Impossible Differential-Linear Cryptanalysis of Reduced-Round CLEFIA-128

Zheng Yuan[1,2], Xian Li[1,2]

[1] Beijing Electronic Science & Technology Institute, Beijing 100070, P. R. China
[2] School of Telecommunications Engineering, Xidian University, Shanxi 710071, P.R. China

Abstract. CLEFIA is a 128-bit block cipher proposed by Sony Corporation in 2007. Our paper introduces a new chosen text attack, impossible differential-linear attack, on iterated cryptosystems. The attack is efficient for 16-round CLEFIA with whitening keys. In the paper, we construct a 13-round impossible differential-linear distinguisher. Based on the distinguisher, we present an effective attack on 16-round CLEFIA-128 with data complexity of $2^{115.52}$, recovering 96-bit subkeys in total. Besides, the results of 15-round CLEFIA-128 are given in the Appendix C. Our attack can also applied to CLEFIA-192 and CLEFIA-256.

Keywords:CLEFIA, impossible differential-linear cryptanalysis, impossible differential cryptanalysis, linear approximation

1 Introduction

CLEFIA [1] is a 128-bit block cipher supporting key lengths of 128, 192 and 256 bits. It achieves enough immunity against known attacks and flexibility for efficient implementation in both hardware and software. As a block cipher proposed by Sony Corporation in 2007, CLEFIA has received a significant amount of cryptanalytic attention. However, except for the evaluation report [2] of the designers, there are only a few significant cryptanalytic results about its security against various cryptanalytic techniques.

At present, the most powerful attack on CLEFIA is a series of impossible differential attacks on reduced rounds of it. The first one is proposed by its designers in the evaluation report of CLEFIA [2]. Then, in FSE 2008, Tsunoo et al. introduced new 9-round impossible differentials for CLEFIA, and presented a 12-round attack on CLEFIA-128 with $2^{118.9}$ chosen plaintexts and 2^{119} encryptions[3] Later, by the same impossible differential distinguisher, Zhang et al. presented an attack on 14-round CLEFIA, in which design team pointed out a flaw and showed that it is not successful[5]. In IndoCrypt 2010, Tezcan proposed improbable differential cryptanalysis and applied it on 13/14/15-round CLEFIA-128/196/256 by the advantage of the relation of round keys [7].

Our Contribution. In this paper, we will propose a new method, impossible differential-linear attack, to analyze the CLEFIA block cipher. By constructing

a 13-round distinguisher, using the new method, and combining with key relations we found, we propose an attack on full-round CLEFIA-128 with data complexity $2^{115.52}$ and time complexity 2^{171}. Besides, for another distinguisher construction, refer to Appendix A. And the attacks to another 16-round and 15-round CLEFIA-128 are also give in Appendix B/C, more efficient compared to the present results. Besides, we provide some key relations we found in Appendix D.

Outline. This paper is organized as follows: Section 2 provides a brief description of CLEFIA, and Section 3 introduces the new method of impossible differential-linear attack. Section 4 gives the 13-round impossible differential-linear distinguisher in detail. Section 5 presents the 16-round impossible differential-linear attack on CLEFIA-128 in detail. Finally, Section 6 concludes the paper.

2 Description of CLEFIA

2.1 Notation

$a\,|b$: The concatenation of a and b;
$a_{(b)}$: b is the bit length of a;
a^T: The transposition of a vector a;
$P = (P_0, P_1, P_2, P_3)$: A 128-bit plaintext, $P_i \in \{0,1\}^{32} (0 \le i \le 4)$;
$C = (C_0, C_1, C_2, C_3)$: A 128-bit ciphertext, $C_i \in \{0,1\}^{32} (0 \le i \le 4)$;
$(X_i^0, X_i^1, X_i^2, X_i^3)$: The i-th round input data, $X_i^j \in \{0,1\}^{32}$
ΔX: The XOR value of X and X^*;

2.2 CLEFIA

CLEFIA is a 128-bit block cipher having a generalized Feistel structure with four data lines, where the width of each data line is 32 bits. For the key lengths of 128, 192, and 256 bits, CLEFIA has 18, 22, and 26 rounds. The encryption function uses four 32-bit whitening keys $WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$ and 2r 32-bit round keys where r is the number of rounds. $K_i \in \{0,1\}^{32} (0 \le i < 2r)$ denotes round key, $WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$ denotes whitening key. We denote d-branch r-round generalized Feistel network employed in CLEFIA as $GFN_{d,r}$. The encryption process can be seen in Fig. 1(a). The detail of $GFN_{4,r}$ is as follows:

- Step 1. $T_0\,|T_1\,|T_2\,|T_3 \leftarrow P_0\,|(P_1 \oplus WK_0)\,|P_2\,|(P_3 \oplus WK_3)$
- Step 2. For $i = 0$ to $r-1$ do the following:
  $T_1 \leftarrow T_1 \oplus F_0(T_0, RK_{2i}), \quad T_3 \leftarrow T_3 \oplus F_1(T_2, RK_{2i+1})$
  $T_0\,|T_1\,|T_2\,|T_3 \leftarrow T_1\,|T_2\,|T_3\,|T_0$
- Step 3. $C_0\,|C_1\,|C_2\,|C_3 \leftarrow T_3\,|\,(T_0 \oplus WK_2\,)\,|\,T_1\,|\,(T_2 \oplus WK_3\,)$

Each round contains two parallel F functions, F_0 and F_1, and their structures are shown in Fig. 1(b) where S_0 and S_1 are 8×8-bit S-boxes. The detail of F_0 is as follows:

– Step 1. $T_0 \,|T_1\, |T_2\, |T_3 \leftarrow RK \oplus x, \quad T_i \in \{0,1\}^8, \;\; x \in \{0,1\}^{32}$
– Step 2. $T_0 \leftarrow S_0(T_0)\ ,\ T_1 \leftarrow S_1(T_1)\ ,\ T_2 \leftarrow S_0(T_2)\ ,\ T_3 \leftarrow S_1(T_3)$
– Step 3. $y = M_0 \cdot (T_0, T_1, T_2, T_3)^T, \;\; y \in \{0,1\}^{32}$

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 two matrices M_0 and M_1 used in the F-functions are defined as follows.

$$M_0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, M_1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}$$

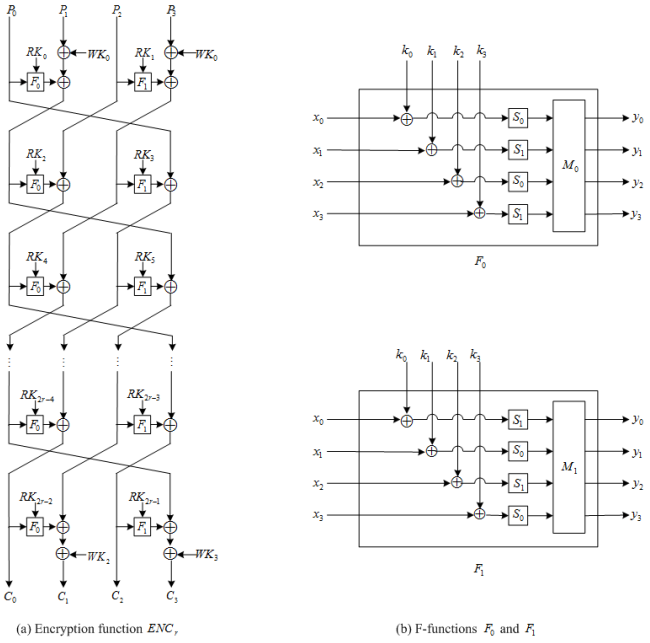

Fig. 1. CLEFIA

2.3 Key Scheduling

The DoubleSwap function $\Sigma : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ is defined as follows:

$$X_{(128)} \mapsto X[7-63]\,|X[121-127]\ |X[0-6]\ |X[64-120]$$

where $X[a-b]$ denotes a bit string cut from the a-th bit to the b-th bit of X.

Let $K = K_0\,|K_1\ |K_2\ |K_3$ be the key and L be an intermediate key, the key scheduling part consists of the following 3 steps:

– Step 1. $L \leftarrow GFN_{4,12}(CON_0, \cdots, CON_{23}, K_0, \cdots, K_3)$
– Step 2.$WK_0 \,|WK_1 \,|WK_2 \,|WK_3 \leftarrow K$
– Step 3. For i=0 to 8 do the following:
$T \leftarrow L \oplus (CON_{24+4i} \,|CON_{24+4i+1} \,|CON_{24+4i+2} \,|CON_{24+4i+3} \,)$
$L \leftarrow \Sigma(L)$
If i is odd: $T \leftarrow T \oplus K$
$RK_{4i} \,|RK_{4i+1} \,|RK_{4i+2} \,|RK_{4i+3} \leftarrow T$

3 The Impossible Differential-Linear Attack

We call this cryptanalytic technique an impossible differential-linear attack, since it combines the impossible differential cryptanalysis and linear cryptanalysis together.The attack is not completely new, for the impossible differential attack and linear attack were typical and widely used in previous attacks on various cryptosystems, but this is the first time that we combine them together.

The basic idea is illuminated from differential-linear attack, first introduced by Langford and Hell-man in [6]. Our attack procedure is described as follows.

we construct an impossible differential-linear distinguisher at first. The block cipher E is represented as $E = E_1 \circ E_0$, where E_0 and E_1 are two subciphers. The distinguisher uses an impossible differential $\Omega_P \not\rightarrow \Omega_T$ with probability 1 for E_0, and a linear approximation $\lambda_P \rightarrow \lambda_T$ with probability $1/2 + q$ for E_1. Then choose a pair of plaintexts (P, P^*) which satisfies $P \oplus P^* = \Omega_P$, and it is obvious that the probability of the impossible differential $E_0(P) \oplus E_0(P^*) \neq \Omega_T$ equals 1. This allows us to get the following one bit equation $\lambda_P \cdot \Omega_T = a$(0 or 1). According to the linear approximation, we can get the equation $\lambda_P \cdot E_0(P) \oplus \lambda_T \cdot E_1(E_0(P)) \oplus \lambda_K \cdot K = 0$ with probability $1/2 + q$. Similarly, we also have $\lambda_P \cdot E_0(P^*) \oplus \lambda_T \cdot E_1(E_0(P^*)) \oplus \lambda_K \cdot K = 0$ with probability $1/2 + q$. Hence, using the piling up lemma presented in [4], we can get $\lambda_T \cdot E_1(E_0(P)) \oplus \lambda_T \cdot E_1(E_0(P^*)) = \lambda_P \cdot (E_0(P) \oplus E_0(P^*)) = a$ with probability $1/2 + 2q^2$. Then we can get $\lambda_T \cdot E_1(E_0(P)) \oplus \lambda_T \cdot E_1(E_0(P^*)) = \lambda_P \cdot \Omega_T = a$ with probability $1/2 - 2q^2$. This can be used as an impossible differential-linear distinguisher. The key recovery attack requires about $O(q^{-4})$ chosen plaintext pairs.

4 The 13-Round Impossible Differential-Linear Distinguisher

4.1 9-round impossible differential characteristic

Paper [3] presented several 9-round impossible differential characteristics. We choose the most efficient which is suitable to our attack as follows:

$$(0, \alpha, 0, 0) \not\rightarrow (0, \beta, 0, 0), \;\; where \;\; \alpha = (0, 0, 0, x), \beta = (y, 0, 0, 0)$$

After the encryption of 9 rounds, the impossible output difference will be

$$\Delta X_9 = (\beta, 0, 0, 0) \tag{1}$$

with probability 1, illustrated in Sect.4.3 Fig.2.

4.2 4-round linear approximation

This subsection we will describe the construction of the 4-round linear approximation used in our attack in detail.

In the 10th round, we get $X_9^0 = X_{10}^3$.

In the 11th round, according to the definition of the round function F_1, we can get the following two equations:

$$X_{10}^3 \oplus F_1(X_{10}^2, RK_{21}) = X_{11}^2, X_{10}^2 = X_{11}^1$$

Then by using linear approximations for the non-linear S-boxes in F_1, we can get the following equation.

$$\lambda_P \cdot F_1(X_{11}^1, RK_{21}) = \lambda_Q \cdot X_{11}^1 \oplus \lambda_Q \cdot RK_{21}$$

Therefore, the linear characteristic of the 11th round can be expressed as follows:

$$\lambda_P \cdot X_{10}^3 = \lambda_P \cdot X_{11}^2 \oplus \lambda_Q \cdot X_{11}^1 \oplus \lambda_Q \cdot RK_{21}, p_1 = 1/2 + q_1 \tag{2}$$

Similarly, the linear characteristics of the 12th round can be expressed as follows.

$$\lambda_Q \cdot X_{11}^1 = \lambda_Q \cdot X_{12}^0 \oplus \lambda_T \cdot X_{12}^3 \oplus \lambda_T \cdot RK_{22}, p_2 = 1/2 + q_2 \tag{3}$$

In the 13th round, we can first get the following equations.

$$X_{12}^1 \oplus F_0(X_{12}^0, RK_{24}) = X_{13}^0, X_{12}^0 = X_{13}^3$$

Then by taking the linear characteristics expressed in Equ. (2) and Equ. (3) into account, we can choose an appropriate pair of values (λ_P, λ_Q), then get the linear characteristic of the 13th round as follows:

$$\lambda_P \cdot X_{12}^1 = \lambda_P \cdot X_{13}^0 \oplus \lambda_Q \cdot X_{13}^3 \oplus \lambda_Q \cdot RK_{24}, p_3 = 1/2 + q_3 \tag{4}$$

Finally, by concentrating the above linear characteristics of round 10-13 together, we can get the following 4-round linear approximation of CLEFIA:

$$\lambda_P \cdot X_9^0 = \lambda_P \cdot X_{10}^3 = \lambda_P \cdot X_{13}^0 \oplus \lambda_T \cdot X_{12}^3 \oplus \lambda_K \cdot K^{'}, p = 1/2 + 2^2 q_1 q_2 q_3 \tag{5}$$

The 4-round linear characteristic is illustrated in Fig.2.

4.3 The 13-Round Impossible Differential-Linear Distinguisher

Here present a property, which can catenate the above two parts together.

Based on the definition of β in 4.1, we get the following computation:

We can choose an input mask as $\lambda_P = (0, \lambda_1, \lambda_1, \lambda_1)$, where $\lambda_1 \in \{01, 02, ...ff\}$. Then we will always have $\lambda_p \cdot \beta = 0$, for $\beta = (y, 0, 0, 0), y \in F_2^8 \backslash \{0\}$.

Therefore, we get a property that when choosing the input mask as $\lambda_P = (0, \lambda_1, \lambda_1, \lambda_1)$, we always have the following equation:

$$\lambda_p \cdot \beta = 0 \tag{6}$$

According to the analysis in Sect.4.1, if choosing a pair of plaintexts (P, P^*) whose difference is $(0, \alpha, 0, 0)$, then based on the 9-round impossible differential expressed as Equ. (1) and (6), we can get the following equation:

$$\lambda_P \cdot \Delta X_9^0 = \lambda_P \cdot (X_9^0 \oplus X_9^{0*}) = 0$$

and it holds with probability 1.Then the 4-round linear characteristic, which is expressed as Equ. (5), can be concatenated to the 10-round impossible differential to form the following 13-round impossible differential-linear distinguisher.

$$\lambda_P \cdot (X_{13}^0 \oplus X_{13}^{0*}) \oplus \lambda_T \cdot (X_{12}^3 \oplus X_{12}^{3*}) = 0 \tag{7}$$

Details of another 13-round impossible differential distinguisher can be seen in Appendix A.

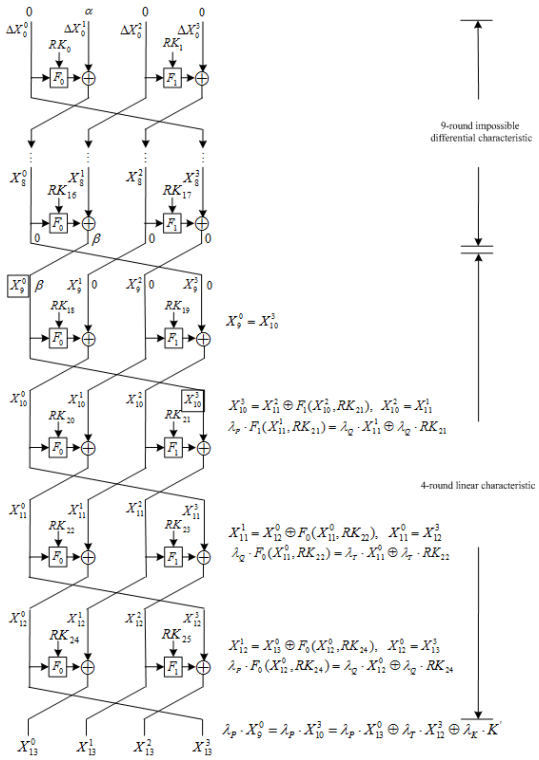

Fig. 2. 13-round impossible differential-linear distinguisher

4.4 Selection of $\boldsymbol{\lambda}$

In this subsection, we show how to select the value of λ_P, λ_Q and λ_T, making the bias of the 4-round linear characteristic as high as possible.

At first, we analyze the linear approximation of F_1 in the 11th round as follows.

$$\lambda_P \cdot F_1(X_{11}^1, RK_{21}) = \lambda_Q \cdot X_{11}^1 \oplus \lambda_Q \cdot RK_{21}$$

The four bytes output of the S-boxes are denoted as (u, v, z, w). Then the round function can be expressed as:

$$F_1(X_{11}^1, RK_{21}) = M_1(S(X_{11}^1 \oplus RK_{21})) = M_1(u, v, z, w)$$

According to the definition in Sect. 2, we can get the following equation:

$$M_1(u, v, z, w)^T = \begin{pmatrix} u \oplus (08 \times v) \oplus (02 \times z) \oplus (0a \times w) \\ (08 \times u) \oplus v \oplus (0a \times z) \oplus (02 \times w) \\ (02 \times u) \oplus (0a \times v) \oplus z \oplus (08 \times w) \\ (0a \times u) \oplus (02 \times v) \oplus (08 \times z) \oplus w \end{pmatrix}$$

Then based on the discussion of the value choice of λ_P in the Sect. 4.3, the left part of the linear approximation can be computed as follows:

$$\lambda_P \cdot F_1(X_{11}^1, RK_{21}) = \{00 \ \ \lambda_1 \ \ \lambda_1 \ \ \lambda_1\} \cdot M_1(u, v, z, w)^T$$

$$= \lambda_1 \cdot (v \oplus (08 \times v) \oplus z \oplus (02 \times z) \oplus w \oplus (0a \times w))$$

Note that the primitive polynomial used in the multiplication is $z^8 + z^4 + z^3 + z^2 + 1$, which can be denoted as a binary string 100011101. Thus we can compute the parity of $\lambda_1 \cdot (02 \times z)$ as follows:

$$\lambda_1 \cdot (02 \times z) = \begin{array}{ll} \lambda_1 \cdot (z << 1), & z_7 = 0 \\ \lambda_1 \cdot (z << 1 \oplus 00011101), & z_7 = 1 \end{array}$$

where z_7 denotes the left-most bit of z. If choosing an appropriate value of λ_1 such that $\lambda_1 \cdot 00011101 = 0$, the above two cases can be transformed both into the following equation:

$$\lambda_1 \cdot (02 \times z) = \lambda_1 \cdot (z << 1) = (\lambda_1 >> 1) \cdot z$$

no matter what the left-most bit of z is.

Similarly, when λ_1 also satisfies $(\lambda_1 >> 1) \cdot 00011101 = 0$, the parity of $\lambda_1 \cdot (08 \cdot v)$ and $\lambda_1 \cdot (0a \cdot w)$ can be computed respectively as follows:

$$\lambda_1 \cdot (08 \times v) = \lambda_1 \cdot (v << 3) = (\lambda_1 >> 3) \cdot v$$

$$\lambda_1 \cdot (0a \times w) = \lambda_1 \cdot ((02 \times w) \oplus (08 \times w)) = ((\lambda_1 >> 1) \oplus (\lambda_1 >> 3)) \cdot w$$

Therefore, the left part of the linear approximation can be transformed into the following equations:

$$\lambda_P \cdot F_1(X_{11}^1, RK_{21})$$

$$= (\lambda_1 \oplus (\lambda_1 >> 3)) \cdot v \oplus (\lambda_1 \oplus (\lambda_1 >> 1)) \cdot z \oplus (\lambda_1 \oplus (\lambda_1 >> 1) \oplus (\lambda_1 >> 3)) \cdot w$$

$$= \{00, \lambda_1 \oplus (\lambda_1 >> 3), \lambda_1 \oplus (\lambda_1 >> 1), \lambda_1 \oplus (\lambda_1 >> 1) \oplus (\lambda_1 >> 3)\} \cdot (u, v, z, w)$$

Then by utilizing the linear distribution table of each S-box, we use the following linear approximation for each S-box (ε denotes the bias of the linear approximation).

$$(\lambda_1 \oplus (\lambda_1 >> 3)) \cdot v = \lambda_2 \cdot (X_{11}^1 \oplus RK_{21})_1, \quad p_4 = 1/2 + \varepsilon_1$$

$$(\lambda_1 \oplus (\lambda_1 >> 1)) \cdot z = \lambda_2 \cdot (X_{11}^1 \oplus RK_{21})_2, \quad p_5 = 1/2 + \varepsilon_2$$

$$(\lambda_1 \oplus (\lambda_1 >> 1) \oplus (\lambda_1 >> 3)) \cdot w = \lambda_2 \cdot (X_{11}^1 \oplus RK_{21})_3, \quad p_6 = 1/2 + \varepsilon_3$$

where $(X_{11}^1 \oplus RK_{21})_j$ denotes the j-th byte of $(X_{12}^1 \oplus RK_{23})(0 \leq j \leq 3)$, and (u, v, z, w) denote the corresponding output of each S-box respectively.

Therefore, we have got the following linear approximation for the function F_1 in the 11th round.

$$\lambda_P \cdot F_1(X_{11}^1 \oplus RK_{21}) = \{00, \lambda_2, \lambda_2, \lambda_2\} \cdot (X_{11}^1 \oplus RK_{21}), \quad p = 1/2 + 2^2\varepsilon_1\varepsilon_2\varepsilon_3$$

Note here we choose λ_Q as the form of $\lambda_Q = \{00, \lambda_2, \lambda_2, \lambda_2\}$, such that we can make use of the property of the linear transformation described in Sect. 4.1.

Similar analysis can be applied to the linear approximation used in the 12th and 13th rounds. Then by running through all the possible values of λ_P, λ_Q and λ_T which satisfies the above conditions, we can choose the following three linear approximation which achieve the highest biases.

$$\{00, f6, f6, f6\} \cdot F_1(X_{11}^1 \oplus RK_{21}) = \{00, eb, eb, eb\} \cdot (X_{11}^1 \oplus RK_{21})$$

whose probability is $p \approx 1/2 - 2^{-11.61}$.

$$\{00, eb, eb, eb\} \cdot F_0(X_{12}^3 \oplus RK_{22}) = \{00, 49, 49, 49\} \cdot (X_{12}^3 \oplus RK_{22})$$

whose probability is $p \approx 1/2 - 2^{-10.83}$.

$$\{00, f6, f6, f6\} \cdot F_0(X_{13}^3 \oplus RK_{24}) = \{00, eb, eb, eb\} \cdot (X_{13}^3 \oplus RK_{24})$$

whose probability is $p \approx 1/2 - 2^{-10.19}$.

Finally, by taking the corresponding values of λ_P, λ_Q and λ_T into the Equations (3)-(6), we can get the following 3-round linear characteristic of CLEFIA.

$$\{00, f6, f6, f6\} \cdot X_{10}^3 = \{00, f6, f6, f6\} \cdot X_{13}^0 \oplus \{00, 49, 49, 49\} \cdot X_{12}^3 \oplus \lambda_K \cdot K^{'} \quad (8)$$

whose probability is $p \approx 1/2 + 2^{-30.63}$.

So the 13-round impossible differential-linear distinguisher can be expressed as follows:

$$\{00, f6, f6, f6\} \cdot (X_{13}^0 \oplus X_{13}^{0*}) \oplus \{00, 49, 49, 49\} \cdot (X_{12}^3 \oplus X_{12}^{3*}) = 0 \quad (9)$$

Its probability can be computed as described in Sect. 3, which means the total probability of the 13-round impossible differential-linear distinguisher is about $1/2 - 2\left(2^{-32.63}\right)^2 \approx 1/2 - 2^{-65.26}$.

5 The Impossible Differential-Linear Attack on 16-Round CLEFIA-128

In this section, we explain our impossible differential-linear attack on 16-round CLEFIA-128 in detail. In the attack, we set the above 13-round impossible differential-linear distinguisher at rounds 3-15, and then mount a key recovery attack by analyzing the first two rounds and the 16th round with whitening keys.

The expression of the distinguisher should be transformed to the following form.

$$\{00, f6, f6, f6\} \cdot (X_{15}^0 \oplus X_{15}^{0*}) \oplus \{00, 49, 49, 49\} \cdot (X_{14}^3 \oplus X_{14}^{3*}) = 0 \qquad (10)$$

and its probability is $1/2 - 2^{-65.26}$.

In the following, we first introduce how to obtain the correct pairs, and then describe the attack procedure in detail, which is also illustrated in Fig.3. In the end, we estimate the data complexity and time complexity of our attack.

5.1 Chosen Plaintext

Based on the analyses in Sect. 3 and [8], we know that approximately $(2^{65.26})^2 \approx 2^{130.52}$ correct pairs are needed to the 13-round impossible linear distinguisher. We choose a structure composed of 2^{72} plaintexts which is defined as follows:

$$S_P = (X_0^0, X_0^1, X_0^2, X_0^3)_j, 1 \leq j \leq 2^{104},$$

Choose plaintext pairs (P, P^*) where $P = (X_0^0, X_0^1, X_0^2, X_0^3)$ and the corresponding plaintext $P^* = (X_0^{0*}, X_0^{1*}, X_0^{2*}, X_0^{3*}) = (X_0^0 \oplus \delta, X_0^1 \oplus \gamma, X_0^2, X_0^3 \oplus \alpha)$, whose difference is of the form $\Delta P = (\delta, \gamma, 0, \alpha)$, where $\alpha = (0, 0, 0, x)$, $\delta = (aw, 2w, 8w, w)$, $w = M_0(S(\alpha))$, $\gamma = (v_0, v_1, v_2, v_3)$, which results to $\Delta X_2 = (0, \alpha, 0, 0)$. The computation of δ, and γ refers to Fig.3. Therefore, we have 255 possible value of α and δ, $2^{32} - 1$ possible values of γ. Then one structure can produce about 2^{119} distinct correct pairs.

Choose a plaintext structure defined as above, then after two rounds encryption, the output difference should be $(0, \alpha, 0, 0)$. After the first round, ΔX_1^0 change to 0, we get the filter probability $\frac{(2^8-1)\cdot 2^{32}/2 \cdot 2^{32}/2}{(2^8-1)\cdot 2^{32}/2 \cdot (2^{32}-1)\cdot 2^{32}/2} \approx 2^{-32}$. From the computation and structure of δ, we know the probability to get ΔX_3^2 is 1. So the filter probability is 2^{-32} in total. After data filter, 2^{87} corrct pairs left.

5.2 Key Recovery

1. For each remaining pair, the first three bytes of α are zero, so the input difference of the first three S-boxes involved in F are zero. Therefore, only the last byte of RK_3 affects F_1. Accordingly, we only need to guess (RK_0, RK_3^3), 40 bits in total, to meet the input difference of impossible differential. For all the 2^{40} guesses, make a table of $K_1, \cdots, K_{2^{40}}$ to record whether the guess is right. If the output is right, the corresponding K_i plus 1.

2. Insert all the ciphertext into another table indexed by $N_1, \cdots N_{2^{56}}$. For every guess of the subkey RK_{30} (32-bit), compute the value of $F_0(X^0_{15}, RK_{30})$ for each X^0_{15}, and we can obtain the value of $X^1_{15} \oplus WK_2 = X^1_{15} \oplus F_0(X^0_{15}, RK_{30})$ for each ciphertext. Then for every guess of the last three bytes of subkey $RK_{29} \oplus WK_2$ (24-bit), we can partially decrypt the function $F_1(X^2_{14}, RK_{29})$ to obtain the value of $\lambda_Q \cdot X^3_{14} = \lambda_Q \cdot (F_1(X^1_{15}, RK_{29}) \oplus X^2_{16})$ for each ciphertext.
   Compute the value of $\lambda_P \cdot X^0_{15} \oplus \lambda_Q \cdot X^3_{14}$. If the pair satisfies equation (10), it's a wrong key that we can filter out, and make N_i plus 1. After running all 2^{56} guesses, output the maximum value of N_i as the 56-bit correct keys.
3. Repeat step 1 with another pair with the 40 bits guessing key obtaining from step 2. Output the 40 bits guess which corresponds to the maximum value of K_i as the correct key.

Complexity Analysis. According to the analysis above, a structure can produce 2^{119} plaintext pairs. The filter probability of first two extention rounds is 2^{-32}, so 2^{87} correct pairs are left. The 13-round distinguisher needs $2^{130.52}$ pairs in total. Then in our key recovery attack, we need about $2^{130.52}/2^{87} = 2^{43.52}$ structures, and the data complexity of our attack is about $2^{72} \cdot 2^{43.52} = 2^{115.52}$.

The time complexity for obtaining the ciphertext is $2^{115.52}$ encryptions. The time complexity of sieving the right key is dominated by Sect.5.2, whose complexity can be estimated separately as follows. The time complexity of Step 1 is about $2^{40} \cdot 2^{72} \cdot 2^{45} = 2^{157}$ S-box operations, which is equal to $2^{157}/8 = 2^{154}$ one round encryption. The time complexity of Step 2 is about $2^{32} \cdot 2^{32} \cdot 2^{32} \cdot 2^{32} \cdot 2^{24} \cdot 2^{24} \approx 2^{176}$ F operations, which is equal to 2^{175} one round encryption. Therefore, the total time complexity of our attack can be estimate as about $(2^{154} + 2^{175})/16 \approx 2^{171}$. Our attack can recover 104-bit subkeys.

Note. Another 13-round impossible differential-linear distinguisher refers to Appendix A, and another 16-round attack to CLEFIA-128 refers to Appendix B. Attacks to 15-round CLEFIA-128 refer to Appendix C. Our attack is also effective to CLEFIA-192 and CLEFIA-256.

6 Conclusion

In this paper, we present a new attack, impossible differential-linear attack, and achieve a result of full-round CLEFIA-128 with $2^{115.52}$ CP, and time complexity is 2^{171}.The comparison of cryptanalytic results to CLEFIA is shown in Table 1, more efficient compared to the present results. The attack is also effective to 15-round CLEFIA-128, given in Appendix C.

References

1. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata.: The 128-bit Blockcipher CLEFIA. In:*Proceedings of Fast Software Encryption 2007*, LNCS, vol. 4593, pp. 181-195. (2007)

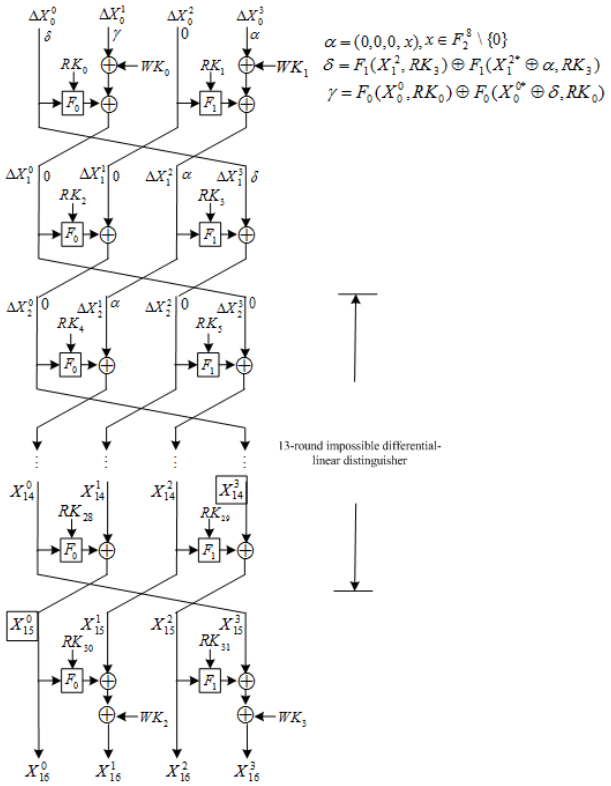

Fig. 3. 16-round impossible differential-linear attack

Table 1. Comparison of Cryptanalysis Results of CLEFIA-128

reference	Rounds	Recover Key	Data Complexity	Time Comlexity
[2]	10	32-bit	$2^{101.7}$	2^{102}
[3]	12	72-bit	$2^{118.9}$	2^{119}
[5]	12	80-bit	$2^{118.9}$	2^{82}
this paper	18	96-bit	$2^{115.52}$	2^{171}

2. Sony Corporation.: The 128-bit blockcipher CLEFIA: Security and performance evaluations. Revision 1.0, On-Line document, 2007.June 1 (2007), http://www.sony.co.jp/Products/clefia/technical/data/clefia-eval-1.0.pdf
3. Y. TsunooE. Tsujihara2M. ShigeriT. SaitoT. Suzaki and H. KUBO.: Impossible Differential Cryptanalysis of CLEFIA. In:*Fast Software Encryption-FSE 2008*LNCS, vol. 5086, pp. 398-411. Springer, Verlag (2008)
4. Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology. In:*Proceedings of EUROCRYPT93*. LNCS, vol. 765, pp. 386-397. Spinger, Heidelberg (1994)
5. Zhang Wenying, Han Jing. Impossible Differential Analysis of Reduced Round CLEFIA. In:*Beijing, China. Proc of Inscrypt'08* . pp. 181-191. (2008)
6. Susan K. Langford, Martin E. Hellman, Differential-Linear Cryptanalysis, Advances in Cryptology. In:*Proceedings of CRYPTO94*. LNCS, vol. 839, pp. 17-25. Springer, Heidelberg (1994)
7. C. Langford, Improbable Differential Attack-Cryptanalysis of Reduced Round CLEFIA, Advances in Cryptology. In:*Proceedings of INDOCRYPT2010*. LNCS, vol. 6498, pp. 197-209. Springer, Heidelberg (2010)
8. Eli Biham, Orr Dunkelman, Nathan Keller, Enhancing Differential-Linear Cryptanalysis, Advances in Cryptology, Proceedings of ASIACRYPT 2002, Lecture Notes in Computer Science 2501, pp. 254-266, Springer, (2002)

Appendix A. Another 13-round impossible differential-linear distinguisher

Another 13-round impossible differential-linear distinguisher concatenate an impossible differential

$$(0,0,0,\alpha) \not\rightarrow (0,0,0,\beta)^{[3]}$$

with a 4-round linear characteristic, details refer to Fig.4.

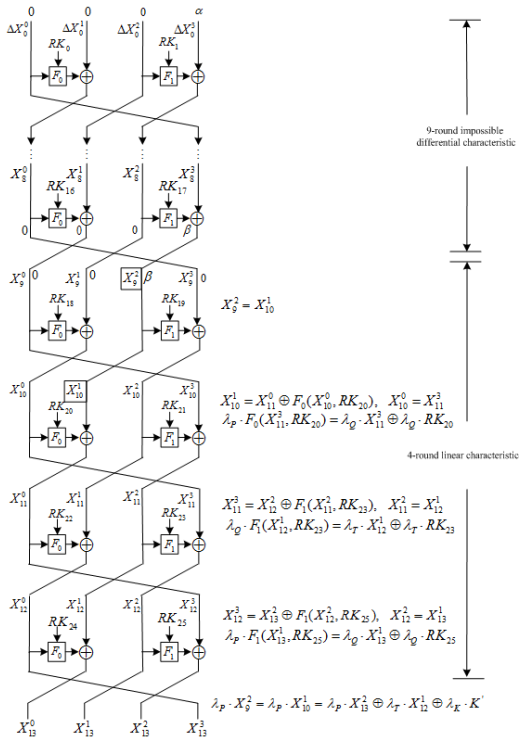

Fig. 4. 13-round impossible differential-linear distinguisher

Appendix B. Another Attack on 16-round CLEFIA-128

The detail of another 16-round attack on CLEFIA-128 is illustrated in Fig.5 with 13-round impossible differential-linear distinguisher in Sect.4, and three rounds extension on plaintext side.

The data complexity is

$$2^{104} \cdot \left[\left(2^{65.26}\right)^2 \Big/ \left(\left(2^{16} \cdot 2^{64} \cdot 2^{64} \cdot 2^{64}/2\right) \cdot 2^{-96} \right) \right] \approx 2^{123.52}.$$

The time complexity is

$$\left[2^{80} \cdot 2^{207}/8 + 2^{24} \cdot 2^{24} \cdot 2^{24}/2\right]/16 \approx 2^{280}.$$

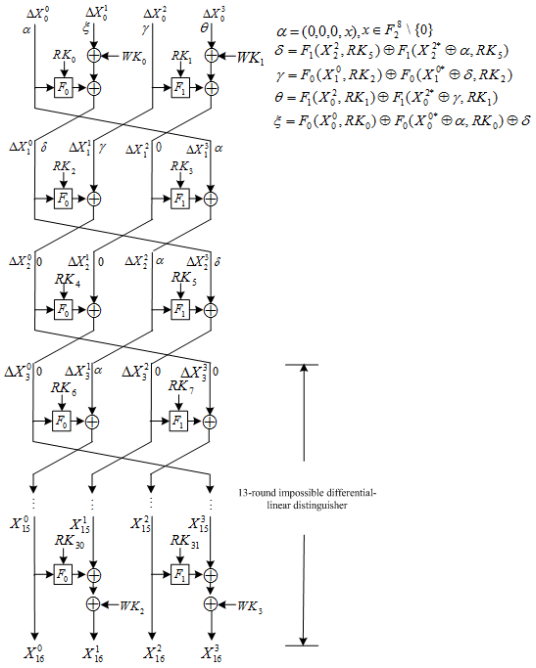

Fig. 5. 16-round impossible differential-linear attack

Appendix C. Attack on 15-round CLEFIA-128

The attacks to 15-round CLEFIA-128 below are all with whitening keys. The detail of the attack can divided into two cases, the first extension case is one rounds on plaintext side, and one round on ciphertext side, which is illustrated in Fig.6. The data complexity is

$$2^{40} \cdot \left[\left(2^{65.26}\right)^2 \Big/ \left(\left(2^{40} \cdot 2^{16}\right) \cdot 2^{-1} \right) \right] \approx 2^{115.52}.$$

The time complexity is

$$\left[\left(2^8 \cdot 2^{40}\right)/8 + \left(2^{32} \cdot 2^{32} \cdot 2^{32}\right) \cdot \left(2^{32} \cdot 2^{24} \cdot 2^{24}\right)/2 \right]/15 \approx 2^{171.09}$$

The second extension is two rounds on plaintext side, illustrated in Fig. 7. The data complexity is

$$2^{72} \cdot \left[\left(2^{65.26}\right)^2 \Big/ \left(\left(2^{72} \cdot \left(2^8 - 1\right)^2 \cdot 2^{32}\right) \Big/ 2 \cdot 2^{-32} \right) \right] \approx 2^{115.52}.$$

The time complexity is the same to the above, i.e. $2^{171.09}$.

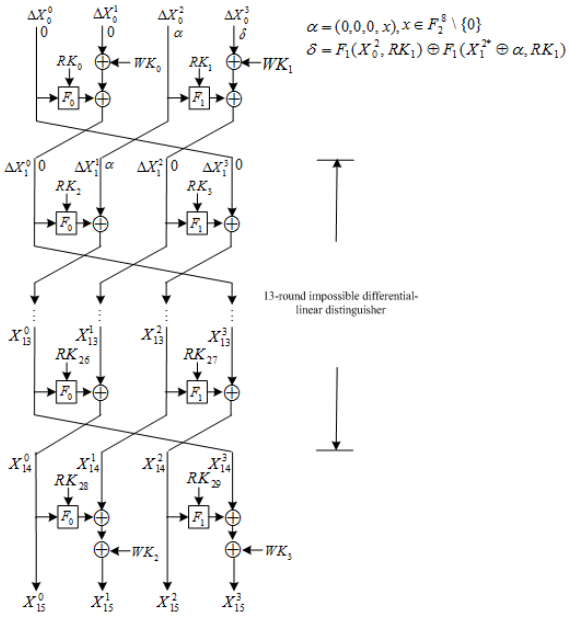

Fig. 6. 15-round impossible differential-linear attack

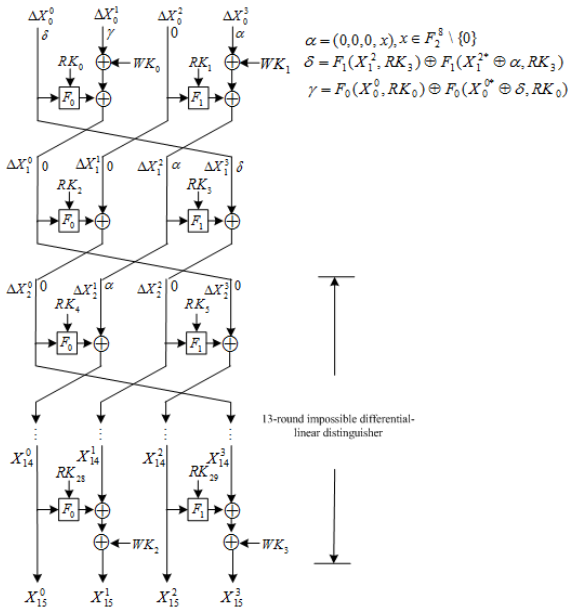

Fig. 7. 15-round impossible differential-linear attack

Appendix D. Round Key Relation

According to the description in Sect. 2, we can get the relationship between generated round keys and related data as follows:

$RK_0 \,|RK_1\, |RK_2\, |RK_3 \leftarrow L \oplus CON_{24}\,|CON_{25}\, |CON_{26}\, |CON_{27}$
$RK_4 \,|RK_5\, |RK_6\, |RK_7 \leftarrow \Sigma(L) \oplus K \oplus CON_{28}\,|CON_{29}\, |CON_{30}\, |CON_{31}$
$RK_8 \,|RK_9\, |RK_{10}\, |RK_{11} \leftarrow \Sigma^2(L) \oplus CON_{32}\,|CON_{33}\, |CON_{34}\, |CON_{35}$
$RK_{12}\,|RK_{13}\, |RK_{14}\, |RK_{15} \leftarrow \Sigma^3(L) \oplus K \oplus CON_{36}\,|CON_{37}\, |CON_{38}\, |CON_{39}$
$RK_{16}\,|RK_{17}\, |RK_{18}\, |RK_{19} \leftarrow \Sigma^4(L) \oplus CON_{40}\,|CON_{41}\, |CON_{42}\, |CON_{43}$
$RK_{20}\,|RK_{21}\, |RK_{22}\, |RK_{23} \leftarrow \Sigma^5(L) \oplus K \oplus CON_{44}\,|CON_{45}\, |CON_{46}\, |CON_{47}$
$RK_{32}\,|RK_{33}\, |RK_{34}\, |RK_{35} \leftarrow \Sigma^8(L) \oplus CON_{56}\,|CON_{57}\, |CON_{58}\, |CON_{59}$

Based on the properties proved in [5], we get the following key relations:

$RK_{32} \oplus C_1 = RK_1[56-63]\,|RK_3[100-102]\,|RK_3[107-127]$
$RK_{33} \oplus C_2 = RK_2[72-95]\,|RK_3[96-99]\,|RK_3[103-106]$
$RK_{34} \oplus C_3 = RK_0[21-24]\,|RK_0[28-31]\,|RK_1[32-55]$
$RK_{35} \oplus C_4 = RK_0[0-20]\,|RK_0[25-27]\,|RK_2[64-71]$

where

$C_1 = CON_{56} \oplus (CON_{25}[56-63]\,|CON_{27}[100-102]\,|CON_{27}[107-127]\,)$
$C_2 = CON_{57} \oplus (CON_{26}[72-95]\,|CON_{27}[96-99]\,|CON_{27}[103-106]\,)$
$C_3 = CON_{58} \oplus (CON_{24}[21-24]\,|CON_{24}[28-31]\,|CON_{25}[32-55]\,)$
$C_4 = CON_{59} \oplus (CON_{24}[0-20]\,|CON_{24}[25-27]\,|CON_{26}[64-71]\,)$

Then we get the following properties from the above derivations:

Property 1. If 32 bits RK_{33} are known, then we can get 24 bits $RK_2[72-95]$, and 8 bits $RK_3[96-99]\,|RK_3[103-106]$.

Property 2. If 32 bits RK_{34} are known, then we can get 8 bits $RK_0[21-24]\,|RK_0[28-31]$, and 24 bits $RK_1[32-55]$.