The Journal of Systems and Software 84 (2011) 1191–1196

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Impossible differential cryptanalysis of 13-round CLEFIA-128

Xuehai Tang[a,*], Bing Sun[a], Ruilin Li[a], Chao Li[a,b]

[a] Department of Mathematics and System Science, Science College of National University of Defense Technology, Changsha, Hunan 410073, PR China
[b] State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100190, PR China

ARTICLE INFO

Article history:
Received 8 July 2010
Received in revised form
15 December 2010
Accepted 12 February 2011
Available online 23 February 2011

Keywords:
Block cipher
CLEFIA
Impossible differential cryptanalysis
Key schedule

ABSTRACT

Block cipher plays an important role in the domain of information security. CLEFIA is a 128-bit block cipher proposed by SONY Corporation in FSE 2007. Using the previous 9-round impossible differentials, the redundancy in the key schedule and the early-abort technique, we present the first successful impossible differential cryptanalysis of 13-round CLEFIA-128 in this paper. The data and time complexities of the attack with the whitening layers are $2^{119.4}$ and $2^{125.52}$, respectively. And for the attack without the whitening layers, more relationships among the subkeys can be used, thus the data and time complexities are reduced to $2^{111.3}$ and $2^{117.5}$, respectively. As far as we know, the presented results are the best compared with the previously published cryptanalytic results on reduced-round CLEFIA-128.

1. Introduction

CLEFIA (Shirai et al., 2007), a 128-bit block cipher proposed by SONY Corporation in FSE 2007, is designed as a well-balanced block cipher between security and performance. The fundamental structure of CLEFIA is a generalized Feistel structure consisting of 4 data lines, in which there are two 32-bit F-functions per round. These two F-functions use two different S-boxes and two different diffusion matrices respectively. CLEFIA supports key length of 128, 192 and 256 bits, these versions of CLEFIA are denoted as CLEFIA-128, CLEFIA-192 and CLEFIA-256. The numbers of rounds for these three versions are 18, 22 and 26 respectively. The security of CLEFIA was analyzed by many cryptographists. At first, some well-known attacks were presented by the designers (Sony, 2007), including differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis, truncated differential cryptanalysis, related-key cryptanalysis, saturation cryptanalysis and some other well-known attacks. Later, more impossible differentials and impossible differential cryptanalysis of CLEFIA were presented by other cryptographists (Wang and Wang, 2007; Tsunoo et al., 2008; Sun et al., 2008; Tsujihara et al., 2008; Wang and Wang, 2009). Moreover, Wang and Wang (2008) and Tang et al. (2009) both found the flaws in the designer's 8-round integral distinguishers and improved the integral cryptanalysis of CLEFIA.

Impossible differential cryptanalysis is a method that reject wrong key candidates by using differentials which hold with probability 0. It was introduced by Biham et al. (1999) and Knudsen (1998), independently. Impossible differential cryptanalysis is one of the most powerful methods used for cryptanalyzing block ciphers. Up to now, the most effective attack on reduced-round CLEFIA is impossible differential cryptanalysis, which can attack 12-round CLEFIA-128, 13-round CLEFIA-192 and 14-round CLEFIA-256. In Zhang and Han (2009), an idea on the impossible differential cryptanalysis of 14-round CLEFIA-128 without the whitening layers was presented. They mainly considered the differential property of S-box and the redundancy in the key schedule. However, they did not give out the attack complexity and could not ensure whether their attack is successful. Therefore, their attack is not so significant though they found the weakness of the key schedule for the first time.

The key schedule is used to generate the subkeys from the master key. Sometimes, we can find the redundancy in the key schedule by analyzing the key schedule in detail. In this paper, we find some common bits between the subkeys used in the first two rounds and the 13th round of CLEFIA-128, so we can guess less subkey bits in the key search phase when we attack 13-round CLEFIA-128. The early-abort technique (Lu et al., 2008) is a useful technique used in the key search phase when we attack block ciphers using differential cryptanalysis or impossible differential cryptanalysis. Its main idea is that we can partially check whether a candidate pair could produce the expected difference by guessing only a small fraction of the unknown required subkey bits at a time, and do a series of partial checks by guessing other fractions of the unknown required subkey bits, instead of guessing all the unknown required subkey bits once. Since some unuseful pairs can be discarded before the next guess for a different fraction of the required subkey bits, we

* Corresponding author. Tel.: +86 13755054594; fax: +86 073184574234.
E-mail address: txh0203@163.com (X. Tang).

0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2011.02.024

can reduce the computational workload for an attack. The round structure of CLEFIA allows us to use the early-abort technique in the impossible differential cryptanalysis of CLEFIA-128.

In this paper, we concentrate on CLEFIA-128. Unlike the attack in Zhang and Han (2009), we use the impossible differentials in Tsunoo et al. (2008), Sun et al. (2008), and Tsujihara et al. (2008). By considering the redundancy in the key schedule, and taking advantage of the early-abort technique, we present the first successful attack on 13-round CLEFIA-128. The data complexity of the proposed attack with the whitening layers is $2^{119.4}$ chosen plaintexts, the time complexity is equivalent to about $2^{125.52}$ encryptions and the memory complexity is less than $2^{119.4}$ blocks. And for the attack without the whitening layers, the data, time and memory complexities are $2^{111.3}$ chosen plaintexts, $2^{117.5}$ encryptions and $2^{111.3}$ blocks, respectively. The results compared with the previously known results on CLEFIA-128 are summarized in Table 1. One can find that our results are better than any previously published cryptanalytic results on CLEFIA-128.

The rest of this paper is organized as follows: In Section 2, we give a brief description of CLEFIA. Some 9-round impossible differentials and some useful observations on the key schedule of CLEFIA-128 are presented in Section 3. Then in Section 4, we propose our attacks on 13-round CLEFIA-128. Finally, Section 5 summarizes this paper.

2. Description of CLEFIA

2.1. Encryption structure

The block length of CLEFIA is 128-bit and the number of rounds for CLEFIA-128 is 18. The data processing part is a four-branch generalized Feistel structure with two parallel F-functions (F_0, F_1) per round. Let $P = (P_0, P_1, P_2, P_3)$ and $C = (C_0, C_1, C_2, C_3)$ be the 128-bit plaintext and ciphertext, respectively, where P_i, $C_i \in \{0,1\}^{32} (0 \le i \le 3)$. The four 32-bit whitening keys and 36 32-bit round subkeys are (WK_0, WK_1, WK_2, WK_3) and $(RK_0, RK_1, \ldots, RK_{35})$. Then the data processing of CLEFIA-128 is shown in Fig. 1.

F_0 and F_1 have 32-bit data x and 32-bit key RK as input and output the 32-bit data y. F_0 is defined as follows:

Step 1. $T \leftarrow x \oplus RK$
Step 2. Let $T = (T_0, T_1, T_2, T_3)$, where $T_i \in \{0,1\}^8$ $(0 \le i \le 3)$. Then $T_0 \leftarrow S_0(T_0), T_1 \leftarrow S_1(T_1), T_2 \leftarrow S_0(T_2), T_3 \leftarrow S_1(T_3)$
Step 3. Let $y = (y_0, y_1, y_2, y_3)$, where $y_i \in \{0,1\}^8$ $(0 \le i \le 3)$. Then $(y_0, y_1, y_2, y_3)^T = M_0(T_0, T_1, T_2, T_3)^T$

And F_1 is defined as:

Step 1. $T \leftarrow x \oplus RK$
Step 2. Let $T = (T_0, T_1, T_2, T_3)$, where $T_i \in \{0,1\}^8$ $(0 \le i \le 3)$. Then $T_0 \leftarrow S_1(T_0), T_1 \leftarrow S_0(T_1), T_2 \leftarrow S_1(T_2), T_3 \leftarrow S_0(T_3)$

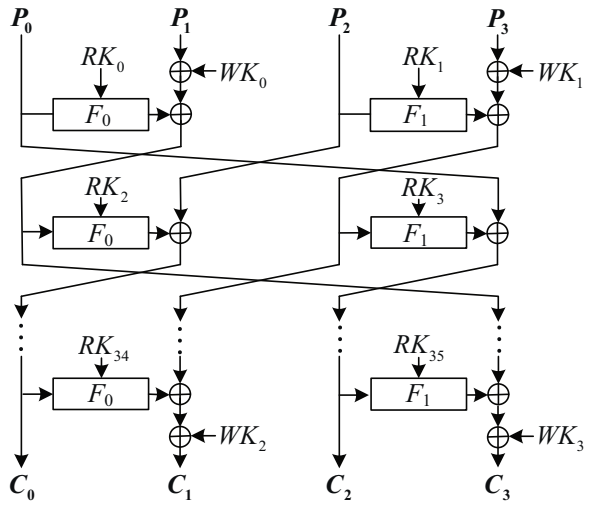

Fig. 1. The Data Processing Structure of CLEFIA-128

Step 3. Let $y = (y_0, y_1, y_2, y_3)$, where $y_i \in \{0,1\}^8$ $(0 \le i \le 3)$. Then $(y_0, y_1, y_2, y_3)^T = M_1(T_0, T_1, T_2, T_3)^T$

Where S_0 and S_1 are non-linear 8-bit S-boxes. The two matrices M_0 and M_1 are MDS (Maximum Distance Separable) matrices, they are defined as:

$$M_0 = \begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{pmatrix}$$

The elements in the matrices are in $GF(2^8)$ and the multiplications of a matrix and a vector are performed in $GF(2^8)$ defined by the lexicographically first primitive polynomial $z^8 + z^4 + z^3 + z^2 + 1$.

2.2. Key schedule of CLEFIA-128

In this subsection, we just describe a part of the key schedule of CLEFIA-128 that will be used in our attacks. We first give the definition of the DoubleSwap function which is used in the key schedule.

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

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

where $X[a-b]$ denotes a bit string cut from the a th bit to the b th bit of X. 0th bit is the most significant bit. The DoubleSwap function is illustrated in Fig. 2.

Table 1
Comparison of attacks on CLEFIA-128.

Attack and source	Whitening	Rounds	Data	Time
Saturation (Sony, 2007)	No	10	$2^{97.6}$	2^{124}
Saturation (Wang and Wang, 2008)	Yes	10	$2^{98.6}$	$2^{98.6}$
Square (Tang et al., 2009)	Yes	10	2^{97}	$2^{92.7}$
Imp. Diff. (Wang and Wang, 2007)	Yes	11	$2^{103.1}$	$2^{98.1}$
Saturation (Wang and Wang, 2009)	Yes	11	$2^{99.8}$	$2^{111.4}$
Imp. Diff. (Wang and Wang, 2007)	Yes	12	$2^{119.3}$	$2^{114.3}$
Imp. Diff. (Tsunoo et al., 2008)	Yes	12	$2^{118.9}$	2^{119}
Imp. Diff. (Sun et al., 2008)	Yes	12	$2^{110.93}$	2^{111}
Imp. Diff. (Wang and Wang, 2009)	Yes	12	$2^{119.1}$	$2^{119.1}$
Imp. Diff. (this paper)	No	13	$2^{111.3}$	$2^{117.5}$
Imp. Diff. (this paper)	Yes	13	$2^{119.4}$	$2^{125.52}$

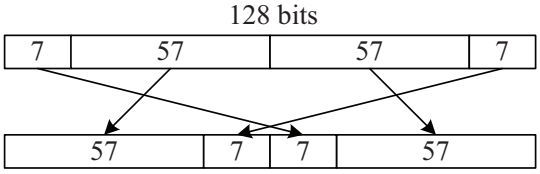

Fig. 2. DoubleSwap Function Σ

Let K be the key and L be an intermediate key, and the key scheduling part consists of the following two steps:

1. Generating L from K.
2. Expanding K and L (Generating WK_i and RK_j).

The relationship between generated round keys and related data is listed as follows:

$$
\begin{aligned}
WK_0||WK_1||WK_2||WK_3 &\leftarrow K\\
RK_0||RK_1||RK_2||RK_3 &\leftarrow L \oplus (CON_{24}||CON_{25}||CON_{26}||CON_{27})\\
RK_4||RK_5||RK_6||RK_7 &\leftarrow \Sigma(L) \oplus K \oplus (CON_{28}||CON_{29}||CON_{30}||\\
&\quad CON_{31})\\
RK_8||RK_9||RK_{10}||RK_{11} &\leftarrow \Sigma^2(L) \oplus (CON_{32}||CON_{33}||CON_{34}||CON_{35})\\
RK_{12}||RK_{13}||RK_{14}||RK_{15} &\leftarrow \Sigma^3(L) \oplus K \oplus (CON_{36}||CON_{37}||CON_{38}||\\
&\quad CON_{39})\\
RK_{16}||RK_{17}||RK_{18}||RK_{19} &\leftarrow \Sigma^4(L) \oplus (CON_{40}||CON_{41}||CON_{42}||CON_{43})\\
RK_{20}||RK_{21}||RK_{22}||RK_{23} &\leftarrow \Sigma^5(L) \oplus K \oplus (CON_{44}||CON_{45}||CON_{46}||\\
&\quad CON_{47})\\
RK_{24}||RK_{25}||RK_{26}||RK_{27} &\leftarrow \Sigma^6(L) \oplus (CON_{48}||CON_{49}||CON_{50}||CON_{51})\\
RK_{28}||RK_{29}||RK_{30}||RK_{31} &\leftarrow \Sigma^7(L) \oplus K \oplus (CON_{52}||CON_{53}||CON_{54}||\\
&\quad CON_{55})\\
RK_{32}||RK_{33}||RK_{34}||RK_{35} &\leftarrow \Sigma^8(L) \oplus (CON_{56}||CON_{57}||CON_{58}||CON_{59})
\end{aligned}
$$

where $CON_{24}, CON_{25}, \ldots, CON_{59}$ are 36 known 32-bit constant values, one can refer to Shirai et al. (2007) for more details.

3. 9-Round impossible differentials and some observations on the key schedule

3.1. 9-Round impossible differentials of CLEFIA

It is known that there are some 9-round impossible differentials of CLEFIA (Tsunoo et al., 2008; Sun et al., 2008; Tsujihara et al., 2008). Here we just list two of them that will be used in our attacks:

$$(0, a000, 0, 0) \nrightarrow_{9r} (0, 0d00, 0, 0) \quad (1)$$

$$(0, ab00, 0, 0) \nrightarrow_{9r} (0, g000, 0, 0) \quad (2)$$

where a, b, d and g are four non-zero bytes, the impossible differential given in (1) is depicted in Fig. 3. One can refer to Tsunoo et al. (2008); Sun et al. (2008); Tsujihara et al. (2008) for the detailed proof.

3.2. Some observations on the key schedule of CLEFIA-128

Let $L \in \{0,1\}^{128}$, from the definition of the DoubleSwap function Σ, we have

$$
\begin{aligned}
&\Sigma^6(L)[0-63]\\
&= L[42-63]||L[121-127]||L[114-120]||L[107-113]||\\
&\quad L[100-106]||L[93-99]||L[86-92].
\end{aligned}
$$

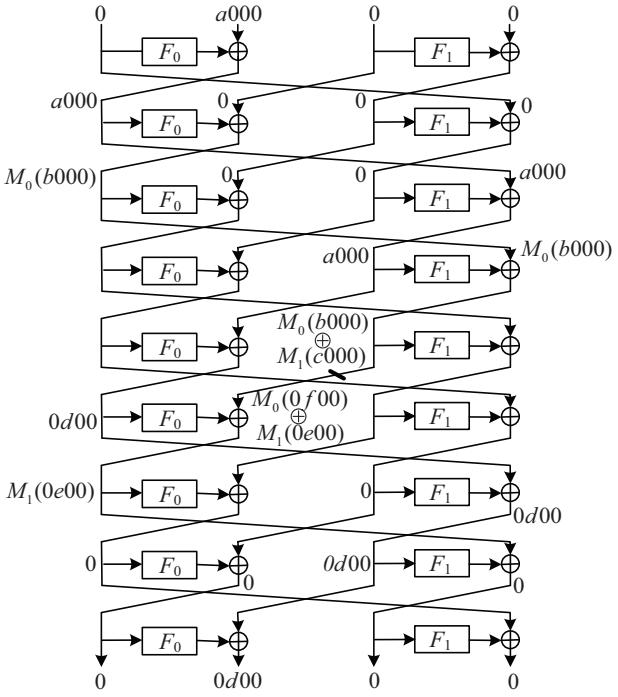

Fig. 3. 9-Round Impossible Differential of CLEFIA

From the key schedule of CLEFIA-128, we know

$$
\begin{aligned}
RK_0||RK_1||RK_2||RK_3 &\leftarrow L \oplus (CON_{24}||CON_{25}||CON_{26}||CON_{27})\\
RK_{24}||RK_{25}||RK_{26}||RK_{27} &\leftarrow \Sigma^6(L) \oplus (CON_{48}||CON_{49}||CON_{50}||CON_{51})
\end{aligned}
$$

thus we can deduce

$$RK_1[10-31] = RK_{24}[0-21] \oplus CON', \quad (3)$$

$$
\begin{aligned}
&RK_{25}[21-24]||RK_{25}[11-17]||RK_{25}[4-8]\\
&\quad = RK_3[0-15] \oplus CON''. \quad (4)
\end{aligned}
$$

where CON' and CON'' are two constant values which are determined by the constant values CON_i s.

4. Key recovery attack on 13-round CLEFIA-128

4.1. Attack with the whitening layers

In this subsection, we present the impossible differential cryptanalysis of 13-round CLEFIA-128 with the whitening layers. This attack is based on the 9-round impossible differential (1) with additional two rounds at the beginning and two rounds at the end as shown in Fig. 4. Notice that we move WK_1 and WK_3 and place them at the proper positions as shown in Fig. 4. Moreover, the whitening keys WK_0 and WK_2 do not affect the corresponding plaintext difference and the ciphertext difference in the attack.

The main idea of the attack is that we first choose one plaintext pair and get the corresponding ciphertext pair, then we guess some subkey to partially encrypt the plaintext pair and partially decrypt the corresponding ciphertext pair, if their differentials match the 9-round impossible differential given in (1), discard the guessed subkey and try another, since the correct subkey cannot lead to the impossible differential. We can repeat the above procedure until there is only one subkey, which can be considered to be the correct subkey.

Let $T^{(i)} = (T_0^{(i)}, T_1^{(i)}, T_2^{(i)}, T_3^{(i)})$ be the output of the i th round and $T_{j,k}^{(i)}$ be the k th byte of $T_j^{(i)}$. $T^{(0)}$ and $T^{(13)}$ are the plaintext and ciphertext, respectively. The attack procedures are as follows:

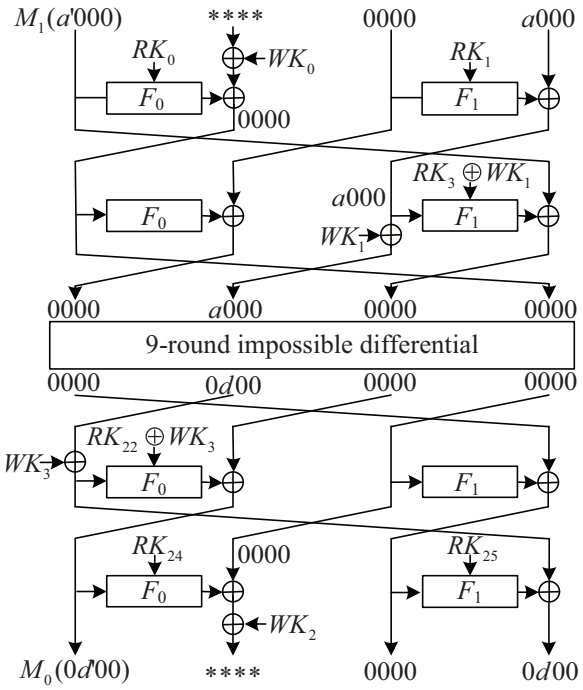

Fig. 4. 13-Round Attack With the Whitening Layers

Step 1. Choose 2^n structures of plaintexts with the form of

$$P = (M_1(x_0||c_0||c_1||c_2), x_1||x_2||x_3||x_4, c_3||c_4||c_5||c_6, x_5||c_7||c_8||c_9),$$

where the 6 bytes $(x_0, x_1, \ldots, x_5)$ take all the possible values, and the 10 bytes $(c_0, c_1, \ldots, c_9)$ are constant values in each structure.

Step 2. For each structure of plaintexts, we can get the corresponding ciphertexts. It is obvious that each structure contains 2^{48} plaintexts and we can obtain 2^{95} plaintext pairs. Keep only the ciphertext pairs and corresponding plaintext pairs which satisfy the difference form: $\Delta P = (M_1(a'000), ****, 0000, a000)$ and $\Delta C = (M_0\,(0d'00), ****, 0000, 0d00)$, where a, a', d and d' denote non-zero bytes and a '$*$' also an unknown byte. The expected number of such pairs is $2^{n+95} \times 2^{-8\times 10} \times (255/256))^4 \approx 2^{n+15}$. The choosing algorithm (Lu et al., 2008; Hamid et al., 2009) is as follows:

Let $C = (C_0, C_1, C_2, C_3)$ be the ciphertext, we first store the ciphertexts of each structure in a hash table indexed by the 1st, 3rd and 4th bytes of $M_0^{-1}(C_0)$, all bytes of C_2, the 1st, 3rd and 4th bytes of C_3. Then, every 2 ciphertexts with the same index in this table have the proper difference: $\Delta C = (M_0\,(0d'00), ****, 0000, 0d00)$. So, we need not to compute each ΔC and compare it with the target difference. Thus the time complexities of this step are mainly obtaining the ciphertexts and computing $M_0^{-1}(C_0)$.

Step 3. In this step, we need to guess RK_0 and partially encrypt every remaining plaintext pair (P and P^*) to keep only the pairs that satisfy the difference $F_0\,(P_0, RK_0) \oplus F_0\,(P_0^*, RK_0) \oplus \Delta P_1 = 0||\,0||\,0||0$.

Method 1: Guess 32-bit value of RK_0 and keep only the pairs that satisfy the difference $F_0\,(P_0, RK_0) \oplus F_0\,(P_0^*, RK_0) \oplus \Delta P_1 = 0||\,0||\,0||0$. The time complexity is about $2 \times 2^{32} \times 2^{n+15} = 2^{n+58}$ F_0 operations.

Method 2: Denote $F_0(P_0, RK_0) = M_0(S(P_0 \oplus RK_0))$ and $F_0(P_0^*, RK_0) = M_0(S(P_0^* \oplus RK_0))$, the condition in method 1 is equivalent to $S(P_0 \oplus RK_0) \oplus S(P_0^* \oplus RK_0) \oplus M_0^{-1}(\Delta P_1) = 0||\,0||\,0||0$. Then we can use the early-abort technique to reduce the time complexity. The detailed procedures are as follows:

Guess the 8-bit value of $RK_{0,k}$ for $k = 0, 1, 2, 3$, compute $\Delta_k = S_0(P_{0,k} \oplus RK_{0,k}) \oplus S_0(P_{0,k}^* \oplus RK_{0,k})$ for $k = 0, 2$ and $\Delta_k = S_1(P_{0,k} \oplus RK_{0,k}) \oplus S_1(P_{0,k}^* \oplus RK_{0,k})$ for $k = 1, 3$. Keep only the pairs that satisfy $\Delta_k = M_0^{-1}(\Delta P_1)_k$, where $M_0^{-1}(\Delta P_1)_k$ is the k th byte of $M_0^{-1}(\Delta P_1)$. The above procedures mean that we guess 8-bit value of RK_0 and discard some unuseful pairs each time, thus we do this event four times instead of guessing 32-bit value of RK_0 once. The probability that $\Delta_k = M_0^{-1}(\Delta P_1)_k$ for each k is 2^{-8} on average (since each Δ_k is a 8-bit value), thus the expected number of remaining pairs is $2^{n+15} \times 2^{-8\times 4} = 2^{n-17}$. The time complexity is less than $2 \times \sum_{i=0}^{3}(2^{n+15-8i} \times 2^{8(i+1)}) = 2^{n+26}$ F_0 operations, it's far less than 2^{n+58} F_0 operations in method 1.

Step 4. This step is similar to step 3. Guess the 8-bit value of $RK_{24,k}$ for $k = 0, 1, 2, 3$, and for each remaining ciphertext pair (C, C^*), compute $\Delta_k = S_0(C_{0,k} \oplus RK_{24,k}) \oplus S_0(C_{0,k}^* \oplus RK_{24,k})$ for $k = 0, 2$ and $\Delta_k = S_1(C_{0,k} \oplus RK_{24,k}) \oplus S_1(C_{0,k}^* \oplus RK_{24,k})$ for $k = 1, 3$. Keep only the pairs that satisfy $\Delta_k = M_0^{-1}(\Delta C_1)_k$, where $M_0^{-1}(\Delta C_1)_k$ is the k th byte of $M_0^{-1}(\Delta C_1)$. The probability of this event for each k is 2^{-8}, thus the expected number of remaining pairs is $2^{n-17} \times 2^{-8\times 4} = 2^{n-49}$.

Step 5. Guess the 32-bit value of RK_1. Notice that according to Eq. (3), $RK_1[10-31]$ is already fixed by previously guessed RK_{24}, so we need only to guess 10-bit value of $RK_1[0-9]$. Partially encrypt each remaining pair to get the exact value of the pair $(T_2^{(1)}, T_2^{(1)*})$. This step does not affect the number of the remaining pairs.

Step 6. Guess 8-bit value $RK'_{3,0}$ as the first byte of $RK_3 \oplus WK_1$, and for each remaining pair, compute $\Delta = S_1(T_{2,0}^{(1)} \oplus RK'_{3,0}) \oplus S_1(T_{2,0}^{(1)*} \oplus RK'_{3,0})$. Keep only the pairs that satisfy $\Delta = a'$. The probability is 2^{-8}, thus the expected number of remaining pairs is $2^{n-49} \times 2^{-8} = 2^{n-57}$.

Step 7. Guess the 32-bit value of RK_{25}. Partially decrypt each remaining pair to get the exact value of the pair $(T_0^{(11)} \oplus WK_3, T_0^{(11)*} \oplus WK_3)$. This step does not affect the number of the remaining pairs.

Step 8. Guess 8-bit value $RK'_{22,1}$ as the second byte of $RK_{22} \oplus WK_3$, and for each remaining pair, compute $\Delta = S_1(T_{0,1}^{(11)} \oplus WK_{3,1} \oplus RK'_{22,1}) \oplus S_1(T_{0,1}^{(11)*} \oplus WK_{3,1} \oplus RK'_{22,1})$ and check if $\Delta = d'$. If there exists a pair that passes this test, then discard the 122-bit guessed subkey and try another.

4.1.1. Analysis of the attack complexity

The main time complexity is in steps 2–8 for recovering the 122-bit value of subkey. In step 8, the probability that $\Delta = d'$ is about 2^{-8}, so after analyzing all of the 2^{n-57} pairs, the expected number of the remaining guessed subkeys is about $r = 2^{122}(1-2^{-8})^{2^{n-57}}$. When $n = 71.4$, we have $r < 1$, thus all wrong guessed subkeys can be excluded. So the data complexity is $2^{n+48} = 2^{119.4}$ chosen plaintexts.

From the encryption algorithm of CLEFIA, we know that one round of CLEFIA encryption is equivalent to four 32-bit (16 8-bit) XOR operations, eight 8-bit S-box operations and two multiplication operations (M_0, M_1). Then the time complexities (in terms of encryption units) in steps 2–8 are as follows:

Step 2: The time complexity of obtaining the ciphertexts is $2^{n+48} = 2^{119.4}$ 13-round CLEFIA encryptions. And one computation of $M_0^{-1}(C_0)$ is less than 1/2 round CLEFIA encryption, then the complexity of computing $M_0^{-1}(C_0)$ is less than $(1/2) \times (1/13) \times 2^n \times 2^{48} \approx 2^{114.7}$ 13-round CLEFIA encryptions. Thus, the total complexity of this step is $2^{119.4} + 2^{114.7} \approx 2^{119.4}$ 13-round CLEFIA encryptions.

Step 3: The complexity of S-box operation is $2 \times (1/(8 \times 13)) \times \sum_{i=0}^{3}(2^{n+15-8i} \times 2^{8(i+1)}) \approx 2^{n+19.3} = 2^{90.7}$, the complexity of XOR operation is $3 \times (1/(16 \times 13)) \times \sum_{i=0}^{3}(2^{n+15-8i} \times 2^{8(i+1)}) + 4 \times (1/(16 \times 13)) \times 2^{n+15} \approx 2^{90.3}$, the complexity of multiplication operation is $(1/(2 \times 13)) \times 2^{n+15} \approx 2^{81.7}$. One can find that the main time complexity of Step 3 is the S-box operations. Thus, the time complexity of Step 3 is less than $2^{90.7}$ 13-round CLEFIA encryptions.

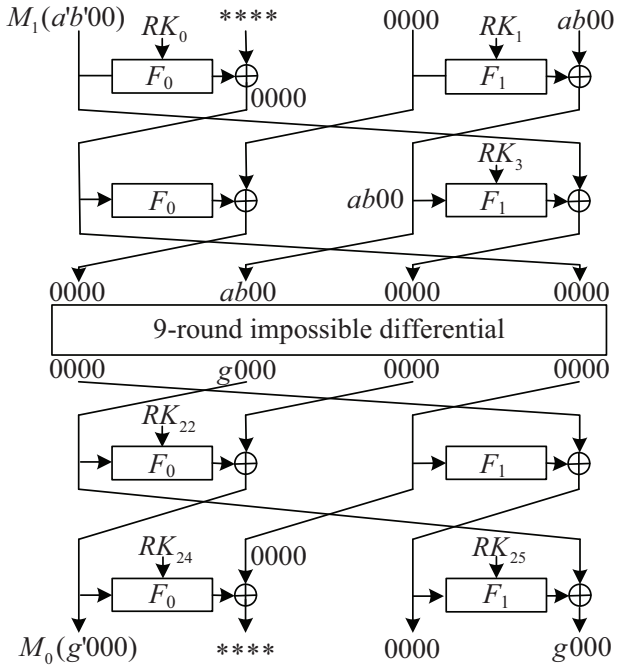

Fig. 5. 13-Round Attack Without the Whitening Layers

Step 4: This step is similar to Step 3 and the time complexity is less than $2 \times (1/(8 \times 13)) \times \sum_{i=0}^{3}(2^{n-17-8i} \times 2^{32+8(i+1)}) \approx 2^{n+19.3} = 2^{90.7}$ 13-round CLEFIA encryptions.

Step 5: In this step, one partial encryption is equivalent to 1/2 round CLEFIA encryption, so the time complexity is $2 \times (1/(2 \times 13)) \times 2^{32+32+10} \times 2^{n-49} \approx 2^{92.7}$ 13-round CLEFIA encryptions.

Step 6: The complexity of S-box operation is $2 \times (1/(8 \times 13)) \times (2^{n-49} \times 2^{74+8}) \approx 2^{98.7}$, the complexity of XOR operation is $3 \times (1/(16 \times 13)) \times (2^{n-49} \times 2^{74+8}) \approx 2^{98.3}$, so the time complexity of step 6 is less than $2^{98.7}$ 13-round CLEFIA encryptions.

Step 7: This step is similar to Step 5 and the time complexity is $2 \times (1/(2 \times 13)) \times 2^{82+32} \times 2^{n-57} \approx 2^{124.7}$ 13-round CLEFIA encryptions.

Step 8: The main time complexity of this step is the S-box operations, and which is less than $2 \times (1/(8 \times 13)) \times 2^{114+8} \times \sum_{i=0}^{2^{n-57}-1}(1-2^{-8})^i \approx 2^{124.3}$ 13-round CLEFIA encryptions.

Thus the time complexity of the attack is about $2^{124.7} + 2^{124.3} \approx 2^{125.52}$ 13-round CLEFIA encryptions. The memory complexity is mainly in step 2, we store the ciphertexts of each structure in a hash table indexed by the 1st, 3rd and 4th bytes of $M_0^{-1}(C_0)$, all bytes of C_2, the 1st, 3rd and 4th bytes of C_3. So the memory complexity is less than $2^{119.4}$ blocks.

4.2. Attack without the whitening layers

In this subsection, we briefly describe the impossible differential cryptanalysis of 13-round CLEFIA-128 without the whitening layers. This attack is based on the 9-round impossible differential (2) with additional two rounds at the beginning and two rounds at the end as shown in Fig. 5. The attack procedures are similar to the above attack.

In step 1, choose 2^n structures of plaintexts such that each structure contains 2^{64} plaintexts with the form

$$P = (M_1(x_0||x_1||c_0||c_1), x_2||x_3||x_4||x_5, c_2||c_3||c_4||c_5, x_6||x_7||c_6||c_7)$$

where the 8 bytes $(x_0, x_1, \ldots, x_7)$ take all the possible values, and the 8 bytes $(c_0, c_1, \ldots, c_7)$ are constant values in each structure. It is clear that we can obtain 2^{127} plaintext pairs in each structure. In step 2, keep only the ciphertext pairs which satisfy the difference form: $\Delta C = (M_0(g'000), ****, 0000, g000)$, where g and g' denote non-zero bytes and a $*$ also an unknown byte. The choosing algorithm is the same as the above one. The expected number of such ciphertext pairs is $2^{n+127} \times 2^{-8\times 10} \times (255/256)^2 \approx 2^{n+47}$.

In steps 3–8, we need to guess 152-bit value of RK_0, RK_1, $RK_{3,0}$, $RK_{3,1}$, RK_{24}, RK_{25} and $RK_{22,0}$. However, we know that there are 38 common bits among the guessed subkeys from Eqs. (3) and (4). Then we need only to guess $152 - 38 = 114$ bits in fact. Analysis of the attack complexity is just like the attack with the whitening layers. In steps 3–7, we can filter out 2^{n-33} satisfying ciphertext pairs. In step 8, after analyzing all of the 2^{n-33} pairs, the expected number of the remaining guessed subkeys is about $r = 2^{114}(1-2^{-8})^{2^{n-33}}$. When $n = 47.3$, we have $r < 1$, thus all wrong guessed subkeys can be excluded. The data complexity is about $2^{111.3}$ chosen plaintexts, the time complexity is about $2^{117.5}$ 13-round CLEFIA encryptions and the memory complexity is less than $2^{111.3}$ blocks.

5. Conclusion

In this paper, new impossible differential cryptanalysis of the block cipher CLEFIA is discussed. By using the previous 9-round impossible differentials, considering the weakness in the key schedule of CLEFIA-128, and taking advantage of the early-abort technique, we present the first successful attacks on 13-round CLEFIA-128 with (without) the whitening layers. The data, time and memory complexities of the attack with the whitening layers are $2^{119.4}$, $2^{125.52}$ and $2^{119.4}$, respectively. And for the attack without the whitening layers, more relationships among the subkeys can be used, thus the data, time and memory complexities are reduced to $2^{111.3}$, $2^{117.5}$ and $2^{111.3}$, respectively. As far as we know, these attacks are the best compared with the existing results on CLEFIA-128. However, our method used in this paper does not apply to CLEFIA-192/256 effectively, since the relations between round subkeys of CLEFIA-192/256 are difficult to be exploited. So, how to improve the existing attacks on CLEFIA-192/256 is worth further studying.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable suggestions and comments. The work in this paper is partially supported by the Natural Science Foundation of China (No: 60803156, 61070215) and the open research fund of State Key Laboratory of Information Security (No: 01-07).

References

Biham, E., Biryukov, A., Shamir, A., (1999). Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: EUROCRYPT 1999. LNCS, vol. 1592. Springer-Verlag, pp. 12–23.

Hamid, M., Mohsen, S., Mohammad, D., Ghadamali, B., 2009. New results on impossible differential cryptanalysis of reduced-round Camellia-128. In: SAC 2009. LNCS, vol. 5867. Springer-Verlag, pp. 281–294.

Knudsen, L., 1998. DEAL—a 128-bit Block Cipher. In: AES Proposal.

Lu, J., Kim, J., Keller, N., Dunkelman, N., 2008. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: CT-RSA 2008. LNCS, vol. 4964. Springer-Verlag, pp. 370–386.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T., 2007. The 128-bit block cipher CLEFIA. In: FSE 2007. LNCS, vol. 4593. Springer-Verlag, pp. 181–195.

Sony Corporation, June 2007. The 128-bit Blockcipher CLEFIA: Security and Performance Evaluation. Revision 1.0.

Sun, B., Li, R., Wang, M., Li, P., Li, C., 2008. Impossible differential cryptanalysis of CLEFIA. In: ePrint 2008/151. http://eprint.iacr.org/2008/151.

Tang, X., Li, C., Xie, D., 2009. Square attack on CLEFIA. Journal of Electronics and Information Technology 31 (9), 2260–2263 (in Chinese).

Tsujihara, E., Shigeri, M. Suzaki, T., Kawabata, T., Tsunoo, Y., 2008. New impossible differentials of CLEFIA. In: Technical Report of IEICE. ISEC, May 2008 (in Japanese).

Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H., 2008. Impossible differential cryptanalysis of CLEFIA. In: FSE 2008. LNCS, vol. 5086. Springer-Verlag, pp. 398–411.
Wang, W., Wang, X., 2007. Improved impossible differential cryptanalysis of CLEFIA. In: ePrint 2007/466. http://eprint.iacr.org2007/466.pdf.
Wang, W., Wang, X., 2009. Impossible differential cryptanalysis of CLEFIA-128/192/256. Journal of Software 20 (9), 2587–2596.
Wang, W., Wang, X., 2008. Saturation cryptanalysis of CLEFIA. Journal of Communication 29 (10), 88–92 (in Chinese).
Zhang, W., Han, J., 2009. Impossible differential analysis of reduced round CLEFIA. In: Inscrypt 2008. LNCS, vol. 5487. Springer-Verlag, pp. 181–191.

Xuehai Tang received his B.S. and M.S. degrees in mathematics from the Science College of National University of Defense Technology, Changsha, China, in 2007 and 2008, respectively. He is a Ph.D. student in the Department of Mathematics and System Science, Science College of National University of Defense Technology since January 2009. His main research interests include information security theory and cryptography.

Bing Sun received the M.S. and Ph.D. degrees in mathematics from the Science College of National University of Defense Technology, Changsha, China, in 2005 and 2009, respectively. He is now a Lecturer with the Department of Mathematics and System Science, National University of Defense Technology. His research fields include cryptography and coding theory.

Ruilin Li received his B.S. and M.S. degrees in mathematics from the Science College of National University of Defense Technology, Changsha, China, in 2005 and 2007, respectively. He is a Ph.D. student in the Department of Mathematics and System Science, Science College of National University of Defense Technology since January 2008. His main research interests include information security theory and cryptography.

Chao Li received the B.A. degree in mathematics from the University of Information Engineering, Zhengzhou, China, in 1987, the M.S. degree in mathematics from the University of Science and Technology of China, Hefei, China, in 1990, and the Ph.D. degree in engineering from the National University of Defense Technology, Changsha, China, in 2002. Since December 2001, he has been a Professor with the Department of Mathematics and System Science, National University of Defense Technology. His research fields include coding theory, cryptography, and sequences.