Mala H, Dakhilalian M, Shakiba M. Impossible differential attacks on 13-round CLEFIA-128. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 26(4): 744–750 July 2011. DOI 10.1007/s11390-011-1173-0

Impossible Differential Attacks on 13-Round CLEFIA-128

Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba

Cryptography and System Security Research Laboratory, Department of Electrical and Computer Engineering Isfahan University of Technology, Isfahan, Iran

E-mail: {hamid_mala@ec, mdalian@cc, m.shakiba@ec}.iut.ac.ir

Received November 9, 2009; revised February 26, 2011.

Abstract CLEFIA, a new 128-bit block cipher proposed by Sony Corporation, is increasingly attracting cryptanalysts' attention. In this paper, we present two new impossible differential attacks on 13 rounds of CLEFIA-128. The proposed attacks utilize a variety of previously known techniques, in particular the hash table technique and redundancy in the key schedule of this block cipher. The first attack does not consider the whitening layers of CLEFIA, requires $2^{109.5}$ chosen plaintexts, and has a running time equivalent to about $2^{112.9}$ encryptions. The second attack preserves the whitening layers, requires $2^{117.8}$ chosen plaintexts, and has a total time complexity equivalent to about $2^{121.2}$ encryptions.

Keywords block cipher, cryptanalysis, impossible differential, CLEFIA

1 Introduction

Diffusion Switching Mechanism (DSM) is a method of designing a Feistel block cipher that can guarantee a large minimum number of active S-boxes[1]. The first block cipher designed based on DSM, CLEFIA[2-3], is a 128-bit block cipher with variable key lengths of n bits, which is denoted as CLEFIA-n, n = 128, 192, 256. The number of rounds for these three variants is 18, 22 and 26, respectively. The designers of CLEFIA claimed that it is designed to achieve sufficient security against all known cryptanalysis techniques. Moreover, [4] proves that 5 rounds of its 4-branch generalized Feistel structure have provable security against differential cryptanalysis. As a new 128-bit block cipher, CLEFIA has received a significant amount of cryptanalytic attention. Among the cryptanalysis methods exploited to analyze this block cipher, the best results are attributed to impossible differential cryptanalysis.

Impossible differential cryptanalysis, an extension of the differential cryptanalysis[5], was first proposed by Biham to analyze the Skipjack block cipher[6]. This method uses differentials that hold with probability zero (impossible differentials) to eliminate the wrong keys and leave the right key. In [2, 7], the designers of CLEFIA found several 9-round impossible differentials for this cipher and mounted a 10-round attack with a data complexity of $2^{101.7}$ and a time complexity of about 2^{102} encryptions. In FSE 2008, [8] introduced new 9-round impossible differentials for CLEFIA, and presented a 12-round attack on CLEFIA-128. This attack requires $2^{118.9}$ chosen plaintexts and performs 2^{119} encryptions. Also in [9-11], impossible differential attacks have been applied to 12 rounds of CLEFIA-128. Recently, using the same impossible differential as that of [8], [12] claimed an attack on 14 rounds of CLEFIA-128 without whitening layers. But, CLEFIA design team pointed out a flaw in their attack and showed that its time complexity is greater than 2^{202} [13]. In fact their attack requires 2^{m+44} plaintexts, and in the attack procedure, after the data filtering, for each of the 2^{m+29} plaintext pairs, about $2^{21} \times 2^{10} \times 2^{-16} = 2^{15}$ values out of the 2^{128} possible values of the target subkeys are removed. To ensure that the number of remaining wrong subkeys is less than 1, we must have $(2^{128}-1) \times (1-\frac{2^{15}}{2^{128}})^{2^{m+29}} < 1$, thus m must be greater than 90.4. As a result, data complexity of the attack becomes greater than $2^{m+44} = 2^{134.4}$, so the attack scenario of [12] is not successful. However, their work is the first attack that considers the weakness in the key schedule of CLEFIA.

In this paper, we reevaluate the security of CLEFIA-128 against impossible differential cryptanalysis. Exploiting a variety of techniques including plaintext structures, key schedule considerations, early abort and hash table techniques, we present the first successful impossible differential attacks on 13-round CLEFIA-128. We summarize our results along with previously known results on CLEFIA-128 in Table 1. In this table, time complexity is measured in encryption units, and data complexity is the number of chosen plaintexts.

Short Paper

Table 1. Summary of the Impossible Differential Attacks on CLEFIA-128

No. Rounds	Whitening	Data Complexity	Time Complexity	Memory (blocks)	Source
10	Yes	$2^{101.7}$	2^{102}	2^{32}	[2, 7]
12	Yes	$2^{119.1}$	$2^{119.1}$	2^{96}	[9]
12	Yes	$2^{118.9}$	2^{119}	2^{73}	[8]
12	Yes	$2^{110.93}$	2^{111}	—	[10]
12	Yes	2^{111}	2^{111}	—	[11]
13	No	$2^{109.5}$	$2^{112.9}$	$2^{94.5}$	This work
13	Yes	$2^{117.8}$	$2^{121.2}$	$2^{86.8}$	This work

The rest of this paper is organized as follows. Section 2 provides a brief description of CLEFIA. 9-round impossible differentials of CLEFIA are reminisced in Section 3. In Section 4, we propose our new impossible differential attacks on 13-round CLEFIA-128 and investigate their complexities. Finally, we conclude the paper in Section 5.

2 Description of CLEFIA

2.1 Data Processing of CLEFIA

In this paper the concatenation of two bit strings a and b is demonstrated by $a|b$. The 128-bit ciphertext $C = C_0|C_1|C_2|C_3$ corresponding to a 128-bit plaintext $P = P_0|P_1|P_2|P_3$ is computed according to the process shown in Fig.1. The encryption process uses a 4-branch generalized Feistel structure with two parallel F functions F_0 and F_1 per round. Also, there are key whitening parts in the beginning and at the end of the cipher. WK_0, WK_1, WK_2 and WK_3 are the 32-bit whitening keys and RK_i, $0 \leqslant i \leqslant 2R-1$ are the 32-bit round subkeys generated by the key schedule for an R-round encryption. In Fig.1, S_0 and S_1 are 8-bit invertible S-boxes, and $\boldsymbol{M}_0$ and $\boldsymbol{M}_1$ are two self-inverse 4×4 matrices with optimal branch number 5[14]. The multiplications between these matrices and vectors are performed in $GF(2^8)$ defined by the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$. Throughout the paper, we use C^r to denote the output of r-th round; C_i^r, $i = 0, 1, 2, 3$ denotes the i-th 32-bit word of C^r. The function F_i, $i = 0, 1$ in round r is denoted by F_i^r. The 32-bit output of S-box layer in F_i^r is denoted by S_i^r, $i = 0, 1$. The j-th byte of the words S_i^r and C_i^r are denoted by $S_{i,j}^r$ and $C_{i,j}^r$, respectively.

2.2 Key Scheduling of CLEFIA-128

Let $X = X_{0\sim127}$ be a 128-bit string indexed from 0 to 127. The DoubleSwap function $DS : \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$ is defined as below:

$$DS(X) = X_{7\sim63}|X_{121\sim127}|X_{0\sim6}|X_{64\sim120}$$

where $X_{a\sim b}$ denotes a bit string cut from the a-th bit to the b-th bit of X. The key scheduling part of CLEFIA-128 first applies a 12-round 4-branch Generalized Feistel Network ($GFN_{4,12}$) on the 128-bit user key K to generate a 128-bit intermediate key L. Then it uses K, L and the DoubleSwap function to generate RK_i, $i = 0, \ldots, 35$ and WK_j, $j = 0, \ldots, 3$ as below:

$$\begin{aligned}
&WK_0|WK_1|WK_2|WK_3 \longleftarrow K,\\
&RK_0|RK_1|RK_2|RK_3 \longleftarrow L \oplus c_1,\\
&RK_4|RK_5|RK_6|RK_7 \longleftarrow DS(L) \oplus K \oplus c_2,\\
&RK_8|RK_9|RK_{10}|RK_{11} \longleftarrow DS^2(L) \oplus c_3,\\
&RK_{12}|RK_{13}|RK_{14}|RK_{15} \longleftarrow DS^3(L) \oplus K \oplus c_4,\\
&RK_{16}|RK_{17}|RK_{18}|RK_{19} \longleftarrow DS^4(L) \oplus c_5,
\end{aligned}$$

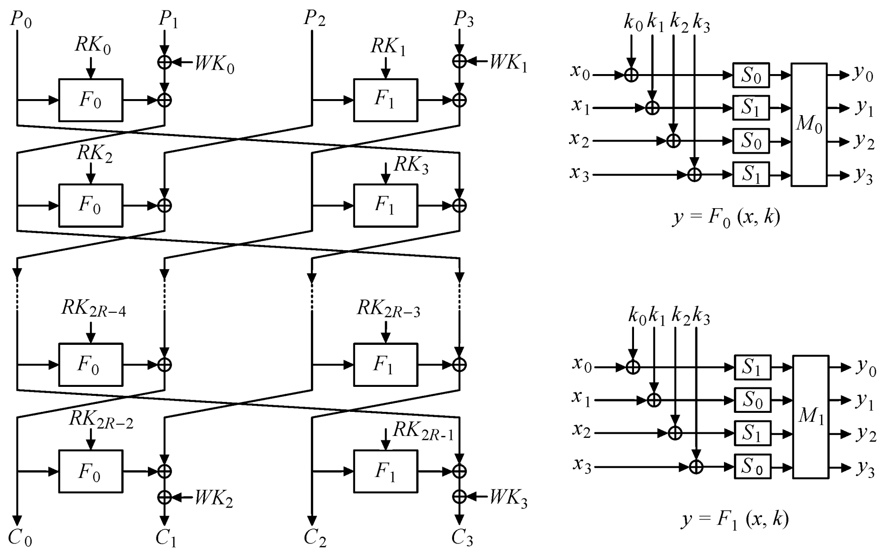

Fig.1. R-round encryption function of CLEFIA and round functions F_0 and F_1.

$$RK_{20}|RK_{21}|RK_{22}|RK_{23} \longleftarrow DS^5(L) \oplus K \oplus c_6,$$
$$RK_{24}|RK_{25}|RK_{26}|RK_{27} \longleftarrow DS^6(L) \oplus c_7,$$
$$RK_{28}|RK_{29}|RK_{30}|RK_{31} \longleftarrow DS^7(L) \oplus K \oplus c_8,$$
$$RK_{32}|RK_{33}|RK_{34}|RK_{35} \longleftarrow DS^8(L) \oplus c_9,$$

where c_i, $i = 1, 2, \ldots, 9$ are 128-bit constants. In our attacks, we need to know the bits of the intermediate key value $L = k_{0\sim127}$ that determine RK_{24} and RK_{25}. After computing the function $DS^6(L)$, it is easy to see that these bits are as follows:

$$RK_{24} : k_{42\sim63}|k_{121\sim127}|k_{114\sim116},$$
$$RK_{25} : k_{117\sim120}|k_{107\sim113}|k_{100\sim106}|k_{93\sim99}|k_{86\sim92}.$$

3 Impossible Differentials of CLEFIA

[7] presents two 9-round impossible differentials of CLEFIA as below:

$$(0|a|0|0) \nrightarrow_{9\,\text{rounds}} (0|a|0|0),$$
$$(0|0|0|a) \nrightarrow_{9\,\text{rounds}} (0|0|0|a),$$

where a is any non-zero 32-bit value. These impossible differentials resulted in attacks on 10-round CLEFIA-128/192/256 and 11-round CLEFIA-192/256 and 12-round CLEFIA-256. In FSE 2008, [8] introduces two new 9-round impossible differentials of CLEFIA with the following forms:

$$(0|a_{in}|0|0) \nrightarrow_{9\,\text{rounds}} (0|a_{out}|0|0),$$
$$(0|0|0|a_{in}) \nrightarrow_{9\,\text{rounds}} (0|0|0|a_{out}).$$

Here, a_{in} and a_{out} are 4-byte values with only one non-zero byte in each. Furthermore, if the non-zero byte in a_{in} is its j-th byte, then the non-zero byte of a_{out} must not be located in the same byte position j. For examples $a_{in} = 0|0|0|s$ and $a_{out} = 0|t|0|0$ satisfy the impossible differential condition, where s and t are non-zero bytes. [10-11] extended these impossible differentials such that the input difference (or the output difference but not both of them) can contain 2 non-zero bytes. One may aggregate impossible differentials of [8, 10-11] as below.

For 9-round CLEFIA excluding the last rotation, given a pair (C^i, C'^i) with the difference $\Delta C^i = 0|a_{in}|0|0$ (or $0|0|0|a_{in}$), the output difference cannot be

Table 2. Values of a_{in} and a_{out}

a_{out} (a_{in})	a_{in} (a_{out})
$s_0|0|0|0$	$*|t_1|0|0$, $*|0|t_2|0$, $*|0|0|t_3$
$0|s_1|0|0$	$t_0|*|0|0$, $0|*|t_2|0$, $0|*|0|t_3$
$0|0|s_2|0$	$t_0|0|*|0$, $0|t_1|*|0$, $0|0|*|t_3$
$0|0|0|s_3$	$t_0|0|0|*$, $0|t_1|0|*$, $0|0|t_2|*$

$\Delta C^{i+9} = 0|a_{out}|0|0$ (or $0|0|0|a_{out}$) where a_{in} and a_{out} are the 4-byte words denoted in Table 2. In this table, t_i and s_j are non-zero byte values, and "$*$" is any arbitrary byte value.

4 Impossible Differential Attack on 13-Round CLEFIA-128

In this section, we present two new impossible differential attacks on 13-round CLEFIA-128. The first attack does not include the whitenings in CLEFIA structure while the second attack does.

4.1 The First Attack Scenario

The first attack illustrated in Fig.2 utilizes the 9-round impossible differential

$$(0|0|0|0|a|0|0|b|0|0|0|0|0|0|0|0) \nrightarrow_{9\,\text{rounds}}$$
$$(x|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0)$$

in rounds 3∼11 (including the word rotation of round 11). The attack procedure is as follows.

1) Take 2^n structures of plaintexts such that each structure contains plaintexts $P = P_0|P_1|P_2|P_3$ of the form:

$$P_0 = C_0^0 = \boldsymbol{M}_1(\beta_1|a_1|a_2|\beta_2),$$
$$P_1 = C_1^0 = (\beta_3|\beta_4|\beta_5|\beta_6),$$
$$P_2 = C_2^0 = (a_3|a_4|a_5|a_6),$$
$$P_3 = C_3^0 = (\beta_7|a_7|a_8|\beta_8),$$

where a_i, $i = 1, \ldots, 8$ are fixed constants, and each β_i, $i = 1, \ldots, 8$ takes all the 8-bit values. It is obvious that each structure contains about 2^{64} plaintexts which can provide about 2^{127} plaintext pairs with the difference

$$\Delta P = \boldsymbol{M}_1(c|0|0|d)|e_0|e_1|e_2|e_3|0|0|0|0|a|0|0|b,$$

where b, d are non-zero, a, c are both zero or both non-zero, and at least one of the 4 bytes e_0, e_1, e_2, e_3 is non-zero byte value. Aggregately, we can collect about 2^{n+127} plaintext pairs.

2) Obtain the ciphertexts of each structure and keep only the pairs that satisfy the difference

$$\Delta C = \boldsymbol{M}_0(y|0|0|0)|z_0|z_1|z_2|z_3|0|0|0|0|x|0|0|0,$$

where x, y, and at least one of the 4 bytes z_0, z_1, z_2, z_3 are non-zero values. The probability of this condition is about 2^{-80}. Thus the expected number of remaining pairs (P, P') and the corresponding ciphertext pairs (C, C') is $2^{n+127} \times 2^{-80} = 2^{n+47}$.

3) For each plaintext pair (P, P'), we immediately obtain the 32-bit difference $\Delta S_0^1 = \boldsymbol{M}_0^{-1}(\Delta C_1^0) = \boldsymbol{M}_0$

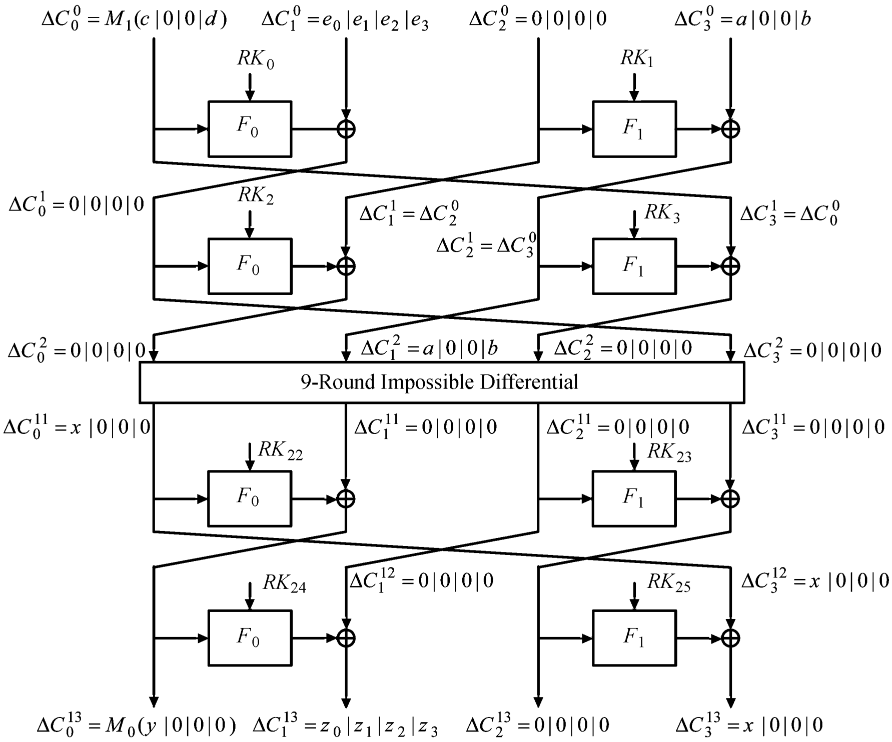

Fig.2. Impossible differential attack on 13-round CLEFIA-128 without whitening.

(ΔC_1^0) (recall that $\boldsymbol{M}_0^{-1} = \boldsymbol{M}_0$). So, for $l = 0, 1, 2, 3$ guess the 8-bit value of $RK_{0,l}$ and partially encrypt every remaining plaintext pair to get the byte difference $\Delta S_{0,l}^1$. Keep only the pairs whose $\Delta S_{0,l}^1$ is equal to the l-th byte of $\boldsymbol{M}_0(\Delta C_1^0)$. The probability of this event for each l is about 2^{-8}, thus the expected number of remaining pairs is $2^{n+47} \times 2^{-8\times 4} = 2^{n+15}$. Note that the operative 32 bits of the intermediate key value $L = k_{0\sim 127}$ in RK_0 include $k_{0\sim 31}$.

4) For each ciphertext pair (C, C') corresponding to a remaining plaintext pair (P, P'), we immediately obtain the 32-bit difference $\Delta S_0^{13} = \boldsymbol{M}_0(\Delta C_1^{13})$. So for $l = 0, 1, 2, 3$ guess the 8-bit value of $RK_{24,l}$ and partially decrypt every remaining ciphertext pair to get the byte difference $\Delta S_{0,l}^{13}$. Keep only the pairs whose $\Delta S_{0,l}^{13}$ is equal to the l-th byte of $\boldsymbol{M}_0(\Delta C_1^{13})$. The probability of this event for each l is about 2^{-8}, thus the expected number of remaining pairs is $2^{n+15} \times 2^{-8\times 4} = 2^{n-17}$. Note that the operative 32 bits of L in RK_{24} include $k_{42\sim 63}|k_{121\sim 127}|k_{114\sim 116}$.

5) In this step, from the 32 bits of L that determine RK_1, 22 bits including $k_{42\sim 63}$ are already known. Based on this fact, perform the following substeps.

(a) Guess the unknown 10 bits $k_{32\sim 41}$ to complete the 32-bit value of RK_1, for each guess partially encrypt all the remaining plaintext pairs through F_1^1 to get the $(C_2^1, C_2'^1)$.

(b) In this stage, from the 8 bits of L that determine $RK_{3,3}$, 7 bits including $k_{121\sim 127}$ are already known. Guess the only unknown bit k_{120} and partially encrypt the last bytes of all the remaining pairs $(C_2^1, C_2'^1)$ through the last S-box of F_1^2. Keep the pairs whose $\Delta S_{1,3}^2$ is equal to d (see Fig.2). The probability of this event is 2^{-8}, thus the expected number of the remaining pairs is $2^{n-17} \times 2^{-8} = 2^{n-25}$.

(c) Guess the 8 bits $k_{96\sim 103}$ of L that determine $RK_{3,0}$ and for each guess partially encrypt the first byte of all the remaining pairs $(C_2^1, C_2'^1)$ through the first S-box of F_1^2. Keep the pairs whose $\Delta S_{1,0}^2$ is equal to c (see Fig.2). The probability of this event is 2^{-8}, thus the expected number of the remaining pairs is $2^{n-25} \times 2^{-8} = 2^{n-33}$.

6) In this step, from the 32 bits of L that determine RK_{25}, 9 bits including $k_{120}|k_{96\sim 103}$ are already known. Guess the other 23 bits and for each guess partially decrypt all the remaining ciphertext pairs through F_1^{13} to get $(C_{0,0}^{11}, C_{0,0}'^{11})$. Now we know the output difference of the S-boxes in F_0^{12}, which is equal to $y|0|0|0$, and also the input pair before the key addition in F_0^{12} (see Fig.2). Thus, by accessing the difference distribution table of the S-box S_0, we obtain on average one 8-bit value for $RK_{22,0}$. The obtained $RK_{22,0}$ along with the 106-bit values guessed in previous steps form a wrong 114-bit subkey. The probability that a wrong 114-bit target subkey $RK_0 \mid RK_1|RK_{3,0}|RK_{3,3}|RK_{24}|RK_{25}|RK_{22,0}$ survives

after analyzing one of the 2^{n-33} remaining pairs in Step 6 is about $1-2^{-8}$. Therefore the expected number of the remaining 114-bit wrong subkeys is about $N=(2^{114}-1)(1-2^{-8})^{2^{n-33}}$. If we accept $N=1$, then n will be 47.3. Hence the attack requires $2^{n+64}=2^{111.3}$ plaintexts.

7) To obtain the whole key, guess the remaining 22 bits of L, including $k_{64\sim 85}$. Then for each guess, according to the key scheduling of CLEFIA-128, run the inverse of $GFN_{4,12}$ to obtain the master key K. Then check the below 8-bit condition on $RK_{22,0}, L$ and K:

$$RK_{22,0}=(DS^5(L)\oplus K\oplus c_6)_{64\sim 71}.$$

Thus there remain about $2^{22}\times 2^{-8}=2^{14}$ guesses for $k_{64\sim 85}$. Then each guess is examined by one or two plaintext/ciphertext pairs. It is obvious that at the end of this process, we obtain the whole 128-bit master key K. The time complexity of this step is about $N\times 2^{22}$ 12-round CLEFIA encryptions to obtain K from L, which, compared with the complexity of previous steps, is negligible. So we can accept a larger value for N without increment of the dominant parts of the time complexity. If we choose $N=2^{81}$, from equation $2^{81}=(2^{114}-1)(1-2^{-8})^{2^{n-33}}$ we obtain $n=45.5$. Consequently the plaintext complexity is reduced to $2^{n+64}=2^{109.5}$ and the time complexity of Step 7 will be about $N\times 2^{22}=2^{103}$ 12-round encryptions.

4.2 Complexity of the Attack

For each plaintext P, consider the corresponding ciphertext as a 16-byte value $C=C_0|C_1|\ldots|C_{15}$. In Step 2, to get the qualified pairs, we first store the ciphertexts of each structure in a hash table H_p indexed by the bytes $C_8, C_9, C_{10}, C_{11}, C_{13}, C_{14}, C_{15}, 2C_0\oplus C_1, 4C_0\oplus C_2$ and $6C_0\oplus C_3$. Note that 1, 2, 4, 6 are elements of matrix $\boldsymbol{M}_0$ (for details of this matrix see [2]). Using this technique, each two ciphertexts with the same index in H_p satisfy a difference of the form

$$\Delta C=\boldsymbol{M}_0(y|0|0|0)|z_0|z_1|z_2|z_3|0|0|0|0|x|0|0|0.$$

This step is performed for each structure in a way independent from the other structures. Thus for each structure we store about $2^{127}\times 2^{-80}=2^{47}$ pairs. The time complexity of this step is composed of two parts. The first part is the time required for encryption of all the 2^{n+64} plaintexts. The second part is the time required for 3 multiplications and 3 XOR operations and one memory access for each ciphertext which, compared to the first part, is negligible. The time complexity of other steps is straightforward and has been mentioned in Table 3.

Each round of CLEFIA encryption can be implemented by 8 memory accesses and 10 XOR operations[7]. If we neglect the XOR operations, 13 rounds of CLEFIA is equivalent to 104 memory accesses. Table 3 shows that Steps 2 and 6 have the dominant parts of the time complexity, so for $n=45.5$ the total complexity of the attack, in encryption unit, is $2^{109.5}+\frac{2^{116.5}}{26}+\frac{2^{118.5}}{104}\approx 2^{112.9}$.

In this attack scenario there is no need to store the discarded values of 114-bit target subkeys. Instead, we store the 2^{n+47} plaintext pairs and their corresponding ciphertext pairs obtained from Step 2, and the N values for the remaining 114-bit target subkeys. For $n=45.5$, the first part requires $4\times 2^{n+47}=2^{94.5}$ blocks of memory and the second part requires about 2^{81} blocks of memory.

4.3 Variant of Attack Including the Whitenings

The proposed attack can be extended to 13-round CLEFIA-128 including the whitening layers. We first move the whitening key WK_0 and place it at the bit-wise XOR with the C_3^2 and bit-wise XOR with RK_2. As depicted in Fig.3, the similar movements for WK_1,

Table 3. Proposed Impossible Differential Attack and Its Complexity

Step	Target Subkeys	No. Remaining Plaintext Pairs	Time Complexity
2	None	$2^{n+47}=2^{92.5}$	2^{n+64} E
3	RK_0	$2^{n+15}=2^{60.5}$	$DS^3_{i=0}2\times 2^{n+47-8i}\times 2^{8(i+1)}=2^{n+58}\ \frac{1}{4}$ F
4	RK_{24}	$2^{n-17}=2^{28.5}$	$DS^3_{i=0}2\times 2^{n+15-8i}\times 2^{32+8(i+1)}=2^{n+58}\ \frac{1}{4}$ F
5(a)	RK_1	$2^{n-17}=2^{28.5}$	$2^{10}\times 2^{64}\times 2\times 2^{n-17}=2^{n+58}$ F
5(b)	$RK_{3,3}$	$2^{n-25}=2^{20.5}$	$2^{1}\times 2^{74}\times 2\times 2^{n-17}=2^{n+49}\ \frac{1}{4}$ F
5(c)	$RK_{3,0}$	$2^{n-33}=2^{12.5}$	$2^{8}\times 2^{75}\times 2\times 2^{n-25}=2^{n+49}\ \frac{1}{4}$ F
6	RK_{25}, $RK_{22,0}$	$2^{n-33}=2^{12.5}$	$2^{23}\times 2^{83}\times 2^{n-33}=2^{n+73}\ \frac{1}{4}$ F $2^{23}\times 2^{83}\times 2^{n-33}=2^{n+73}$ MA
7	$k_{64\sim 75}$	for $N=2^{81}$	$N\times 2^{22}\times\frac{13}{12}=2^{103.1}$ E

Note: E: 13-round CLEFIA encryption; MA: memory access; F: F_0 or F_1 evaluation.

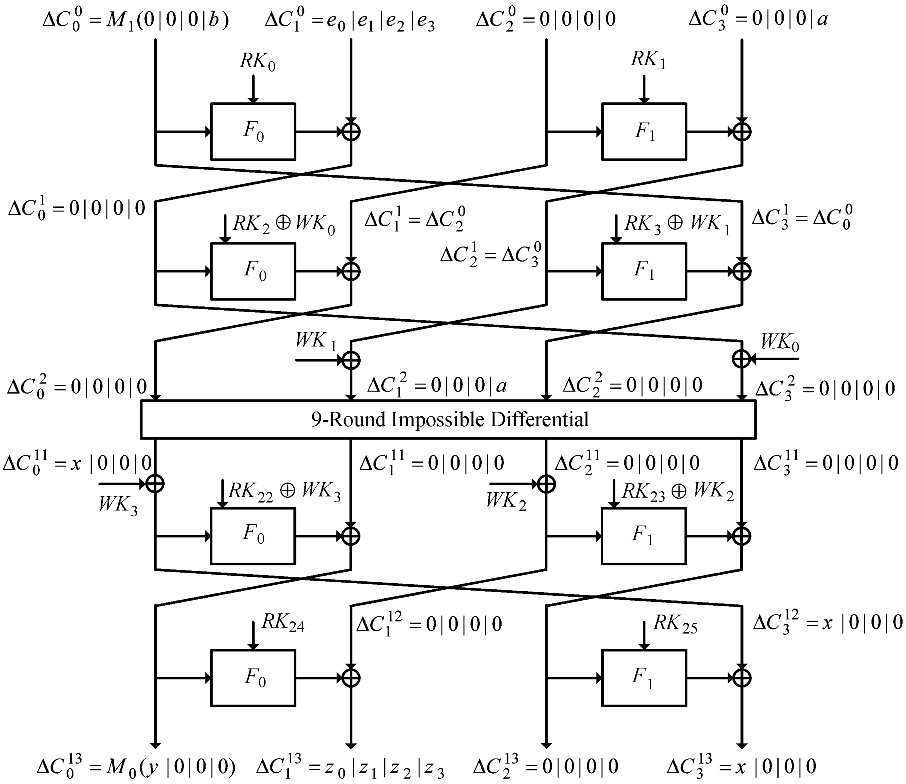

Fig.3. 13-round attack including the whitening layers.

WK_2, and WK_3 are performed. It is easy to see that this is an equivalent structure.

In our analysis we observed that the attack on the complete 13 rounds of CLEFIA-128 works better with the following 9-round impossible differential:

$$(0|0|0|0|0|0|0|a|0|0|0|0|0|0|0|0) \nrightarrow_{9\,\text{rounds}} (x|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0).$$

The attack procedure is similar to that in Subsection 4.2 (only Step 5(c) is removed) and it is demonstrated in Fig.3 and Table 4. In this case each structure contains about 2^{48} plaintexts that can generate a difference of the form

$$\Delta P = \boldsymbol{M}_1(0|0|0|b)|e_0|e_1|e_2|e_3|0|0|0|0|0|0|0|a.$$

Thus each structure contains about 2^{95} plaintext pairs with the above difference. In Step 2 we have an 80-bit filtration, so the number of proper pairs that satisfy the required ciphertext difference is equal to $2^{n+95} \times 2^{-80} = 2^{n+15}$. The target subkeys include $RK_0|RK_1|RK_{3,3} \oplus WK_{1,3}|RK_{24}|RK_{25}|RK_{22,0} \oplus WK_{3,0}$. Based on the key schedule of CLEFIA-128, $RK_0|RK_1|RK_{24}|RK_{25}$ are determined by only 106 bits of the intermediate key value L, including $k_{0\sim63}|k_{86\sim127}$. By including the two bytes $RK_{3,3} \oplus WK_{1,3}$ and $RK_{22,0} \oplus WK_{3,0}$, the target key space contains 122 bits. In Step 6, the probability that a wrong 122-bit target subkey survives after analyzing one of the 2^{n-57} remaining pairs is about $1 - 2^{-8}$. Therefore we expect about $N = (2^{122} - 1)(1 - 2^{-8})^{2^{n-57}}$ wrong

Table 4. Impossible Differential Attack on Complete 13-Round CLEFIA-128 and Its Complexity

Step	Target Subkeys	No. Remaining Plaintext Pairs	Time Complexity
2	None	$2^{n+15} = 2^{84.8}$	$2^{n+48} = 2^{117.8}$ E
3	RK_0	$2^{n-17} = 2^{52.8}$	$DS^3_{i=0} 2 \times 2^{n+15-8i} \times 2^{8(i+1)} = 2^{n+26}\ \frac{1}{4}$ F
4	RK_{24}	$2^{n-49} = 2^{20.8}$	$DS^3_{i=0} 2 \times 2^{n-17-8i} \times 2^{32+8(i+1)} = 2^{n+26}\ \frac{1}{4}$ F
5(a)	RK_1	$2^{n-49} = 2^{20.8}$	$2^{10} \times 2^{64} \times 2 \times 2^{n-49} = 2^{n+26}$ F
5(b)	$RK_{3,3} \oplus WK_{1,3}$	$2^{n-57} = 2^{12.8}$	$2^8 \times 2^{74} \times 2 \times 2^{n-49} = 2^{n+34}\ \frac{1}{4}$ F
6	RK_{25}, $RK_{22,0} \oplus WK_{3,0}$	$2^{n-57} = 2^{12.8}$	$2^{32} \times 2^{82} \times 2^{n-57} = 2^{n+57}\ \frac{1}{4}$ F $2^{32} \times 2^{82} \times 2^{n-57} = 2^{n+57}$ MA
7	$k_{64\sim85}$	for $N = 2^{80}$	$N \times 2^{22} \times \frac{13}{12} = 2^{102.1}$ E

candidates for the 122-bit target subkey remain. If we accept $N = 2^{80}$, then n will be 69.8. Hence the attack requires $2^{n+48} = 2^{117.8}$ plaintexts.

According to what mentioned in Subsection 4.2, if we consider each 13-round encryption equivalent to 104 memory accesses, then the dominant parts of the time complexity are those of Steps 2 and 6. Thus for $n = 69.8$ the total complexity of the attack is $2^{117.8} + \frac{2^{124.8}}{26} + \frac{2^{126.8}}{104} \approx 2^{121.2}$ encryptions. Also we need $4 \times 2^{n+15} = 2^{86.8}$ blocks of memory to store the pairs obtained from Step 2, and about $N = 2^{80}$ blocks of memory to store the subkey candidates obtained from Step 6.

5 Conclusion

In this paper, first, using the properties of the key schedule of CLEFIA-128, we proposed an impossible differential attack on 13 rounds of this new block cipher without the whitening layers. The attack requires $2^{109.5}$ plaintexts, and has a time complexity equivalent to $2^{112.9}$ 13-round encryptions. Then, we presented another attack on 13 rounds of CLEFIA-128, but this time including the whitening layers. This attack requires about $2^{117.8}$ chosen plaintexts, and has a time complexity equivalent to about $2^{121.2}$ encryptions. These attacks are supposed to be the first successful attacks on 13 rounds of CLEFIA-128.

Acknowledgment The authors would like to thank Wen-Ying Zhang for offering us his paper[12], and Professor Vincent Rijmen for his valuable comments.

References

[1] Shirai T, Shibutani K. On feistel structures using a diffusion switching mechanism. In *Proc. FSE 2006,* Graz, Austria, Mar. 15-17, 2006, pp.41-56.

[2] Shirai T, Shibutani K, Akishita T, Moriai S, Iwata T. The 128-bit block cipher CLEFIA (extended abstract). In *Proc. FSE 2007*, Luxembourg, Mar. 26-28, 2007, pp.181-195.

[3] The 128 bit block cipher CLEFIA algorithm specification. Sony Corporation, http://www.sony.net/Products/cryptography/clefia/technical/data/clefia-spec-1.0.pdf, Jun. 1, 2007.

[4] Lee C, Kim J, Sung J, Hong S, Lee S. Provable security for an RC6-like structure and a MISTY-FO-like structure against differential cryptanalysis. In *Proc. ICCSA 2006,* Glasgow, UK, May 8-11, 2006, pp.446-455.

[5] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 1991, 4(1): 3-72.

[6] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In *Proc. EUROCRYPT 1999*, Prague, Czech, May 2-6, 1999, pp.12-23.

[7] The 128-bit block cipher CLEFIA security and performance evaluations. Sony Corporation, http://www.sony.net/Products/cryptography/clefia/technical/data/clefia-eval-1.0.pdf, Jun. 1, 2007.

[8] Tsunoo Y, Tsujihara E, Shigeri M, Saito T, Suzaki T, Kubo H. Impossible differential cryptanalysis of CLEFIA. In *Proc. FSE 2008*, Lausanne, Switzerland, Feb. 10-13, 2008, pp.398-411.

[9] Wang W, Wang X. Improved impossible differential cryptanalysis of CLEFIA. Cryptology ePrint Archive, Report 2007/466, http://eprint.iacr.org/.

[10] Sun B, Ruilin L, Wang M, Li P, Li C. Impossible differential cryptanalysis of CLEFIA. Cryptology ePrint Archive, Report 2008/151, http://eprint.iacr.org/.

[11] Tsujihara E, Shigeri M, Suzaki T, Kawabata T, Tsunoo Y. New impossible differentials of CLEFIA. IEICE Technical Report, ISEC2008-3 (2008-05), pp.15-22. (In Japanese)

[12] Zhang W, Han J. Impossible differential analysis of reduced round CLEFIA. In *Proc. Inscrypt 2008*, Beijing, China, Dec. 14-17, 2008, pp.181-191.

[13] Comments on the impossible differential analysis of reduced round CLEFIA presented at Inscrypt 2008. CLEFIA Design Team, Sony Corporation, Jan. 8, 2009.

[14] The 128-bit block cipher CLEFIA design rationale. Sony Corporation, http://www.sony.net/Products/cryptography/clefia/technical/data/clefia-design-1.0.pdf, Jun. 1, 2007.

Hamid Mala received his B.S., M.S. and Ph.D. degrees in electrical engineering from Isfahan University of Technology (IUT) in 2003, 2006 and 2011, respectively. His research interests are the design and cryptanalysis of block ciphers, digital signatures, and bilinear pairings.

Mohammad Dakhilalian received his B.S. and Ph.D. degrees in electrical engineering from IUT in 1989 and 1998, respectively and M.S. degree in electrical engineering from Tarbiat Modarres University in 1993. He was an assistant professor of Faculty of Information and Communication Technology, Ministry of ICT, Tehran, Iran in 1999∼2001. He joined IUT in 2001 and is an assistant professor in Electrical and Computer Engineering Department. His current research interests are cryptography and data security.

Mohsen Shakiba received his B.S. and M.S. degrees in electrical engineering from Ferdowsi University of Mashhad and Isfahan University of Technology in 2003 and 2008, respectively. Now he is a Ph.D. candidate at IUT. His main research interests include information theory and cryptanalysis of block ciphers.