Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher

Yanjun Li[1,2], Wenling Wu[1], Xiaoli Yu[1], and Le Dong[1]

[1] State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China
Graduate University of Chinese Academy of Sciences, Beijing 100049, P.R. China
[2] Beijing Electronic Science and Technology Institute, Beijing 100070, P.R. China
{liyanjun, wwl,dongle}@is.iscas.ac.cn

Abstract. In this paper a new 9-round integral distinguisher of CLEFIA is proposed based on byte-pattern, which is proved in detail. Then by using the partial sum technique we improve the previous result on 11-round CLEFIA and proposed integral attack on 12-, 13- and 14- round CLEFIA with the whitening keys. The 12-round CLEFIA-128/192/256 is attacked with data complexity 2^{113} and time complexity $2^{116.7}$, 13-round CLEFIA-192/256 is attacked with data complexity 2^{113} and time complexity $2^{180.5}$, and 14-round CLEFIA-256 is breakable with data complexity 2^{113} and time complexity $2^{244.5}$. These results demonstrate that based on the byte-pattern we can improve the integral attacks on CLEFIA two more rounds than those given by the designers.

Key words: Block cipher, Distinguisher, Integral attack, CLEFIA, Partial sum technique

1 Introduction

The block cipher CLEFIA was developed by Sony Corporation [10]. It has the block length of 128 bits and a variable key length of 128/192/256 bits. The security of CLEFIA was initially analyzed by the algorithm designers, including differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and square attack, in which the impossible differential cryptanalysis is most effective[9]. In FSE 2008 Tsunoo *et al.* improved impossible differential cryptanalysis to 12 rounds of CLEFIA-128 with $2^{118.9}$ chosen plaintexts and 2^{119} encryptions [11]. Later by using the same impossible differential distinguisher, Zhang *et al.* presented an attack on 14-round CLEFIA-128 considering the weakness in the key schedule[13]. But CLEFIA design team pointed out a flaw in their attack and showed that it is not successful[2]. In IndoCrypt 2010, Tezcan proposed improbable differential cryptanalysis and applied it on 13-, 14-, and 15-round CLEFIA-128/192/256 by the advantage of the relation of round keys [1]. However, compared with these differential cryptanalysis, integral attack is still an important attack because of its advantages[6, 8, 14]. The basic idea of integral attack comes from square attack, which was first proposed by Daemen

about the analysis of block cipher SQUARE[3,4]. Later Ferguson *et al.* improved this attack to 8 rounds version of Rijndael-128 with the partial sum technique and the herd technique[7]. In the same year Knudsen and Wagner analyzed this cryptanalysis as a dual to differential attacks particularly applicable to block ciphers with bijective components, and they first proposed the definition of integral[5]. So far the best results of square attack on CLEFIA is presented by Wang *et al.*. They has attacked 11-round CLEFIA-128/192/256 with the same distinguisher given by the algorithm designers[12].

In this paper we use the definition of integral attack instead of square attack. According to the structure properties of CLEFIA, a new 9-round integral distinguisher is proposed. Then by using the partial sum technique we proposed integral attacks on 12-, 13- and 14- round CLEFIA. The detail results are as follows: 12-round CLEFIA- 128/192/256 is attacked with data complexity 2^{113} and time complexity $2^{116.7}$, 13-round CLEFIA-192/256 is attacked with data complexity 2^{113} and time complexity $2^{180.5}$, and 14-round CLEFIA-256 is breakable with data complexity 2^{113} and time complexity $2^{244.5}$. The results demonstrate that based on the byte-pattern we can improve the integral attack on CLEFIA two more rounds than those given by the designers. Moreover, the results also present that in the condition of random round keys integral attack is no less effective than differential cryptanalysis on evaluating the security of encryption structure.

This paper is organized as follows: Section 2 provides a brief outline of CLEFIA, the definition of integral attack and the notations used throughout this paper. Section 3 gives the new 9-round distinguisher in detail. Section 4 describes the integral attacks on the reduced-round CLEFIA. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 Description of CLEFIA

CLEFIA is designed based on generalized Feistel structure as shown in Fig.1, and the number of rounds are 18/22/26 corresponding to key length of 128/192/256 bits. The round function of CLEFIA includes two different functions: F_0 and F_1. An N-round CLEFIA iterates the round function N times, and in the first round and the last round there are 4 whitening key bytes.

F_0 and F_1 have the same SP structure and include three basic operations: Round Key Addition, Substitution Layer and Diffusion Layer. However, in the Substitution Layer the order of S_0 and S_1 is different and the Permutation Layers are also different, which are shown in Fig.2. M_0 and M_1 are shown as follows:

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

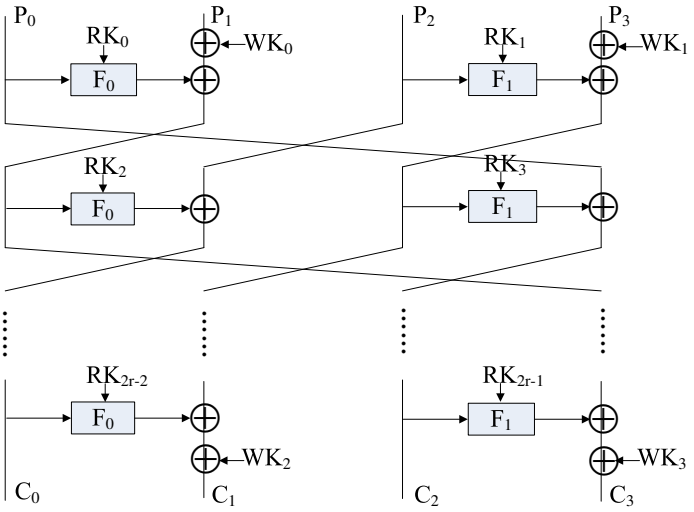

Fig. 1. The Block Cipher: CLEFIA

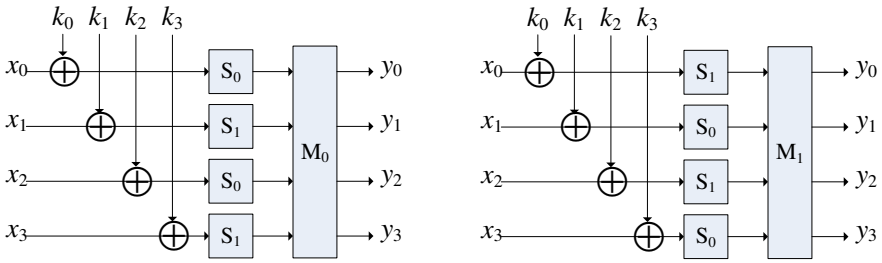

Fig. 2. The Function of F_0 and F_1

In the encryption procedure of CLEFIA, since the relations between the round subkeys will not help in our attacks, we will omit the key scheduling algorithm here and interested readers can refer to [10].

2.2 Integral attack

The integral attack has many interesting features. It can saturate S-Box Layer, and Round Key Addition Layer will not affect this property of saturation. However, Diffusion Layer influences the length of the integral distinguisher. Integral attack considers a particular collection of m bytes in the plaintexts and ciphertexts. The aim of this attack is to predict the values in the sums (i.e. the integral) of the chosen bytes after a certain number of rounds of encryption. In [5], Knudsen and Wagner also generalized this approach to higher order integrals: the original set to consider becomes a set of vectors which differ in d components and where the sum of this set is predictable after a certain number of rounds. The sum of this set is called a d^{th}-order integral. The following definitions are essential:

Active Set. A set $\{x_i | x_i \in F_{2^n}, 0 \leq i \leq 2^n - 1\}$ is active, if for any $0 \leq i < j \leq 2^n - 1$, $x_i \neq x_j$.

Passive Set. A set $\{x_i | x_i \in F_{2^n}, 0 \leq i \leq 2^n - 1\}$ is passive, if for any $0 < i \leq 2^n - 1$, $x_i = x_0$.

Balanced Set. A set $\{x_i | x_i \in F_{2^n}, 0 \leq i \leq 2^n - 1\}$ is balanced, if the sum of all element of the set is 0, that is $\sum_{i=0}^{2^n-1} x_i = 0$.

Usually, Active Set is denoted as A. Passive Set is denoted as C. And Balanced Set is denoted as B.

2.3 Notations

In the following, we introduce some notations used throughout this paper. The plaintext and ciphertext are denoted as $P = P_0|P_1|P_2|P_3$ and $C = C_0|C_1|C_2|C_3$ respectively. WK_0, WK_1, WK_2, WK_3 denote four whitening keys. Other notations that will be used in this paper are described as follows:

$m_{r,i}$: the (i+1)-th byte of the input of the r-th round;
c_i: the (i+1)-th byte of the ciphertext;
$RK_{i,j}$: the (j+1)-th byte of the (i+1)-th round subkey;
$RK'_{i,j}$: This is a simple linear function of the round key $RK_{i,j}$ and WK.
x, y, z, w, v: the active bytes needed in the proofs.

3 New 9-Round Distinguisher of CLEFIA

The integral attack on reduced-round CLEFIA was initially proposed by the algorithm designers, where the text (the data being encrypted) is neatly partitioned into small component words. In this paper we will explore the SP structure of the round function of CLEFIA and partition the text into smaller component bytes. Instead of 8-round integral distinguisher presented by the designers, a new

9-round distinguisher is depicted in Fig.3. In order to prove it, two lemmas are described as follows.

Lemma 1 If $m_{1,4}$ is an active byte and other bytes of the input are constants, after 5 rounds of CLEFIA encryption the c_4, c_5, c_6, c_7 are balance bytes.

Proof. According to Fig.3, 5 rounds of CLEFIA encryption correspond to the rounds from Round 5 to Round 9. The byte $m_{5,4}$ is the only active byte of input of Round 5, which is denoted as x.

After 2 rounds encryption, we will obtain the output state as follows:

$$[y, 2y, 4y, 6y, c, c, c, c, c, c, c, c, x, c, c, c],$$

where $y = s_0(x \oplus RK_{11,0}) \oplus c$, and the value of byte ky is $ky \oplus c, k = 2, 4, 6$.

After 3 rounds encryption, we will obtain the output state as follows:

$$[f_0(y), f_1(y), f_2(y), f_3(y), c, c, c, c, x, c, c, c, y, 2y, 4y, 6y],$$

where $[f_0(y), f_1(y), f_2(y), f_3(y)] = F_0([y, 2y, 4y, 6y], RK_{13})$, and each $f_i(y)$, $0 \leq i \leq 3$ is balance.

After 4 rounds encryption, we will obtain the output state as follows:

$$[?, ?, ?, ?, ?, ?, ?, ?, z \oplus y, 8z \oplus 2y, 2z \oplus 4y, az \oplus 6y, f_0(y), f_1(y), f_2(y), f_3(y)],$$

where $z = s_0(x \oplus RK_{16,0}) \oplus c$. We can easily deduce that each byte of $[z \oplus y$, $8z \oplus 2y, 2z \oplus 4y, az \oplus 6y]$ is balance.

After 5 rounds encryption, only c_4, c_5, c_6, c_7 are balanced bytes, and other bytes are uncertain due to those unknown key bytes.

$$c_4 = z \oplus y, c_5 = 8z \oplus 2y, c_6 = 2z \oplus 4y, c_7 = az \oplus 6y. \square$$

Lemma 2 If $m_{1,4}, m_{1,5}, m_{1,6}$, and $m_{1,7}$ take the values of $v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw$, where v and w are two active bytes, and other 12 bytes of the first round input are active, after 4 rounds of CLEFIA encryption we will obtain 2^{104} sets, and in each set, only byte c_4 is active and other bytes are constant.

Proof. According to Fig.3, $(AAAA)$ denotes 4 active bytes (or an active word), and $(BBBB)$ denotes 4 balanced bytes (or a balanced word). The 4 rounds of CLEFIA encryption described in **Lemma 2** correspond to the rounds from Round 1 to Round 4 in Fig.3. we will proof this lemma in four steps as follows.

1. (Round $4 \rightarrow 5$)Let the input byte pattern be $[c, c, c, c, c, c, c, x, c, c, c, w, 8w$, $2w, aw]$, where x and w are active bytes. After one round encryption we will get 2^8 sets and in each set $c_4 = x$ is active and other bytes are constants.
2. (Round $3 \rightarrow 4$)Let the input byte pattern be $[w, 8w, 2w, aw, u_0, u_1, u_2, u_3, c, c$, $c, c, x, c, c, c]$, where w, u_0, u_1, u_2, u_3 and x are active bytes. After one round encryption we will get 2^{32} sets and in each set the byte pattern is $[c, c, c, c, c, c$, $c, c, x, c, c, c, w, 8w, 2w, aw]$, where x and w are active bytes.

3. (Round 2 → 3)Let the input byte pattern be $[x, c, c, c, v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw, u_0, u_1, u_2, u_3, \lambda_0, \lambda_1, \lambda_2, \lambda_3]$, where x, v, w and $u_i, \lambda_j, 0 \leq i, j \leq 3$ are active bytes. One round encryption can be described as the following equation.

$$P_0 \begin{bmatrix} s_0(x \oplus RK_{3,0}) \oplus v \\ c' \oplus 0 \\ c' \oplus 0 \\ c' \oplus 0 \end{bmatrix} \oplus \begin{bmatrix} w \\ 8w \\ 2w \\ aw \end{bmatrix} = \begin{bmatrix} w \oplus i \\ 8w \oplus 2i \\ 2w \oplus 4i \\ aw \oplus 6i \end{bmatrix} \tag{1}$$

$$P_1 \begin{bmatrix} s_1(u_0 \oplus RK_{4,0}) \\ s_0(u_1 \oplus RK_{4,1}) \\ s_1(u_2 \oplus RK_{4,2}) \\ s_0(u_3 \oplus RK_{4,3}) \end{bmatrix} \oplus \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} c'_0 \\ c'_1 \\ c'_2 \\ c'_3 \end{bmatrix} \tag{2}$$

Without loss of generality, let $c' = 0$. For each value of x, there is $v = v_0$ satisfying the equation (1), and the value of v_0 is unknown due to the unknown RK_3. So when $v = v_0 \oplus t, 0 \leq t \leq 255$ take all 2^8 values, we will obtain 2^8 sets. They are indexed by the value of t. It means that 2^{24} values of $[x, c, c, c, v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw]$ will lead to 2^8 sets, and in each set the byte pattern is $[w, 8w, 2w, aw, x, c, c, c]$. Similarly, 2^{64} values of $[u_0, u_1, u_2, u_3, \lambda_0, \lambda_1, \lambda_2, \lambda_3]$ will lead to 2^{32} sets, and in each set the byte pattern is $[u_0, u_1, u_2, u_3, c, c, c, c]$. The sets are different in 4 constant bytes. Therefore, after one round encryption we will get 2^{40} sets from 2^{88} input values, and in each set the byte pattern is $[w, 8w, 2w, aw, u_0, u_1, u_2, u_3, c, c, c, c, x, c, c, c]$.

4. (Round 1 → 2)Let the input byte pattern be $[\lambda_0, \lambda_1, \lambda_2, \lambda_3, v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8, \lambda_9, \lambda_{10}, \lambda_{11}]$, where v, w and $\lambda_i, 0 \leq i \leq 11$ are active bytes, after one round encryption we will get 2^{24} sets and in each set the byte pattern is $[x, c, c, c, v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw, u_0, u_1, u_2, u_3, \lambda_0, \lambda_1, \lambda_2, \lambda_3]$.

By the steps 1 to 4, we conclude that if $m_{1,4}, m_{1,5}, m_{1,6}$, and $m_{1,7}$ take the values of $v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw$, where v and w are two active bytes, and other 12 bytes of the first round input are active, after 4 rounds of CLEFIA encryption we will obtain 2^{104} sets. In each set, the byte c_4 is active and other bytes are constant.□

In line with Lemma 1 and Lemma 2, we can construct 14th-order 9-round integral distinguisher as depicted in Theorem 1(Fig.3).

Theorem 1 If $m_{1,4}, m_{1,5}, m_{1,6}$, and $m_{1,7}$ take the values of $v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw$, where v and w are two active bytes, and other 12 bytes of the first round input are all active, then after 9 rounds of CLEFIA encryption the bytes of c_4, c_5, c_6, c_7 are balanced.

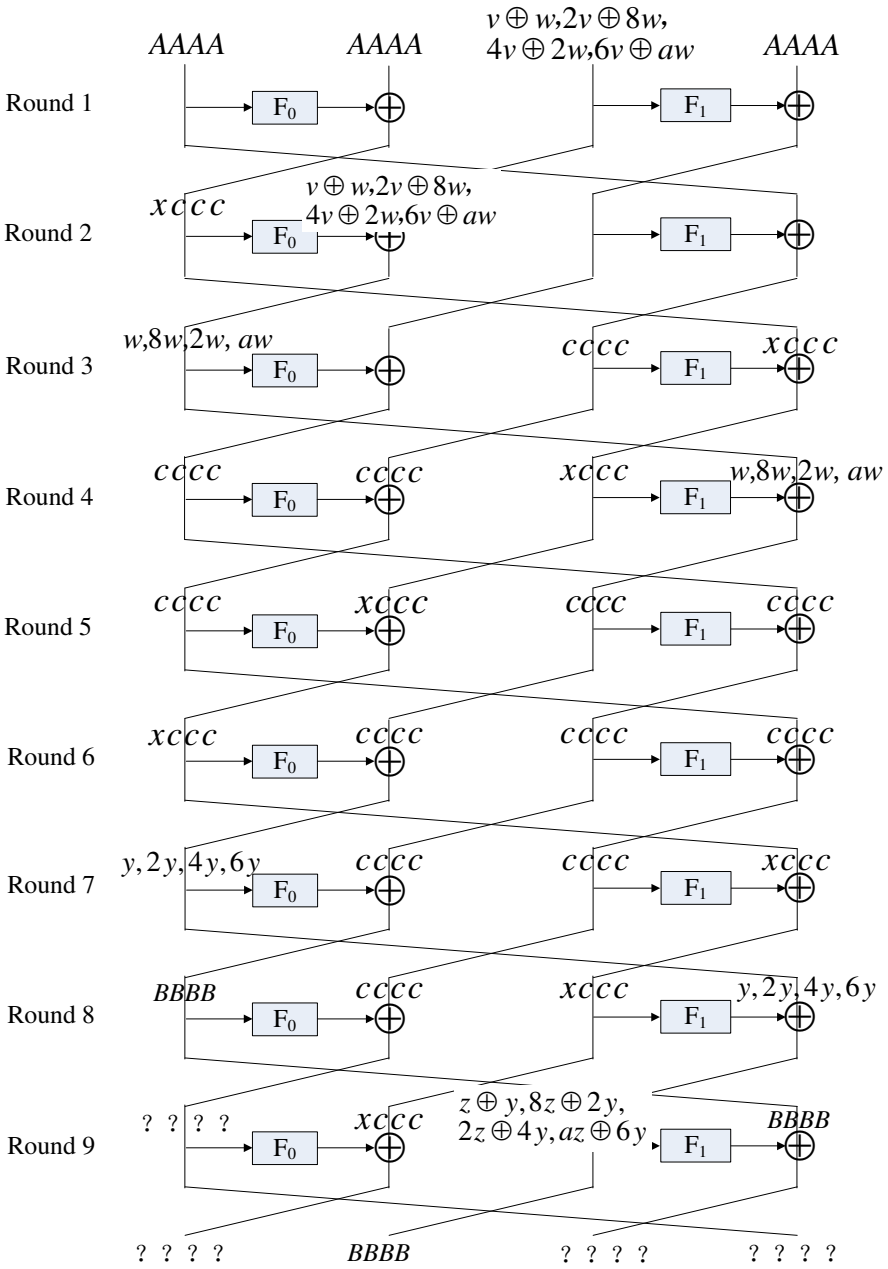

Fig. 3. The 9-Round Integral Distinguisher of CLEFIA

4 Attacks to Reduced Rounds of CLEFIA

4.1 The 11-Round Attack

In this subsection, we describe the integral attack on 11-round CLEFIA based on byte-pattern. It is based on the above 9-round distinguisher with additional two rounds at the end as shown in Fig.4. In the last round there are two whitening keys should be considered. We denote that WK_2 will not affect the attack and $WK_{3,0} \oplus RK_{18,0}$ will be replaced by $RK'_{18,0}$. For 11-round CLEFIA, the following equation can be established:

$$\oplus_{i=1}^{2^{112}} [S_0(S_1(c_8 \oplus RK_{21,0}) \oplus 08S_0(c_9 \oplus RK_{21,1}) \\ \oplus 02S_1(c_{10} \oplus RK_{21,2}) \oplus 0aS_0(c_{11} \oplus RK_{21,3}) \oplus c_{12} \oplus RK'_{18,0})] = \oplus_{i=1}^{2^{112}} c' \tag{3}$$

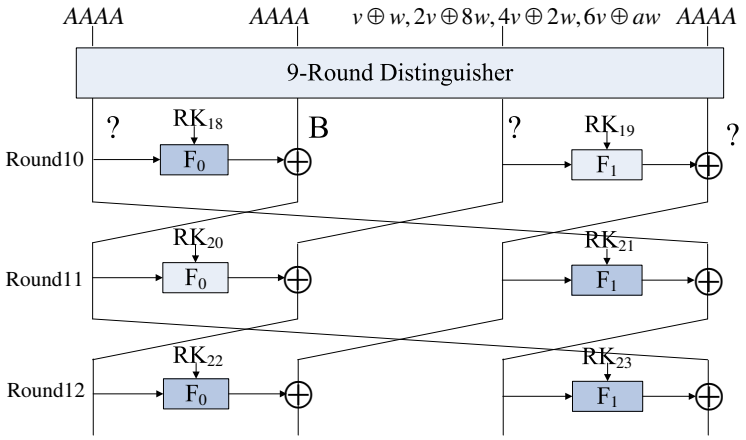

Fig. 4. The Integral Attack on Reduced Rounds of CLEFIA

Using the equation(3), we can attack 11-round CLEFIA as follows:

1. Choose a structure of 2^{112} plaintexts. Let $m_{1,4}, m_{1,5}, m_{1,6}$, and $m_{1,7}$ take the values of $v \oplus w, 2v \oplus 8w, 4v \oplus 2w, 6v \oplus aw$, where v and w are two active bytes, and other 12 bytes of the plaintexts are active. Encrypt all these plaintexts and set 2^{48} counters for six bytes of $c_8, c_9, c_{10}, c_{11}, c_{12}$, and c', where $c' = c_0 \oplus 02c_1 \oplus 04c_2 \oplus 06c_3$, and then the corresponding counter is increased by 1. For all the values of ciphertexts, there are 2^{48} values at most in the six bytes. We choose those values that the counters are odd times ($a \oplus a = 0$).

2. Guess the value of $RK_{21,0}, RK_{21,1}, RK_{21,2}, RK_{21,3}, RK'_{18,0}$, and compute the left value of the equation(3) for all 2^{48} values, where we will use the partial sum technique to compute. Let $t_0, t_1, t_2, \cdots, t_l$ and $r_0, r_1, r_2, \cdots, r_l$ denote the bytes of the ciphertext and the corresponding bytes of RK. We define

$$x_i := \sum_{j=0}^{i} S[t_j \oplus r_j],$$

where i, j satisfy $l \geq i > j \geq 0$.
Now we operate four substeps to compute the left value of the equation(3):

   (a) Guessing the two bytes of $RK_{21,0}$ and $RK_{21,1}$, and computing the partial sum, then we get the corresponding 4 bytes value:

$$(x_1, c_{10}, c_{11}, c_{12}).$$

   (b) Guessing the value of $RK_{21,2}$, and computing the partial sum, then we get 3 bytes value:

$$(x_2, c_{11}, c_{12}).$$

   (c) Guessing the value of $RK_{21,3}$, and computing the partial sum, then we get 2 bytes value:

$$(x_3, c_{12}).$$

   (d) Guessing the value of $RK'_{18,0}$, and computing the partial sum, then we get 1 byte value:

$$(x_4).$$

   The sum of all x_4 is equal to the right value of the equation(3). If the equation(3) holds, the $RK'_{18,0}, RK_{21,0}, RK_{21,1}, RK_{21,2}, RK_{21,3}$ might be right, otherwise it is a wrong guess.
3. Repeat Step 1 and Step 2 until $RK'_{18,0}, RK_{21,0}, RK_{21,1}, RK_{21,2}, RK_{21,3}$ is uniquely determined.

In Step 2, computing the right value of the equation(3) needs 4×2^{32} times XOR operation at most. To get the left value of the equation(3) needs no more than $2^{40} \times 2^{16} \times 4 = 2^{58}$ table lookups. For a wrong key, the probability that it satisfies the equation(3) is 2^{-8}, and thus after analyzing a structure, the number of wrong keys that can pass the equation(3) is $(2^{40} - 1) \times 2^{-8} \approx 2^{32}$. Hence to uniquely determine 5 bytes key, we need to analyze 6 structures. Similarly, the key bytes of $RK'_{18,1}, RK'_{18,2}$ and $RK'_{18,3}$ also can be determined. Accordingly, the data complexity of the attack is about $2^{114.6}$ chosen plaintexts, and the time complexity is $6 \times 2^{58}/(11 \times 2^3) = 2^{54}$ encryptions. Guessing the remaining key bytes of RK_{19} and RK_{20}, the total time complexity is about 2^{64} encryptions (the time cost of searching RK_{19} and RK_{20}).

4.2 The 12-Round Attack

The integral attack on 12 rounds CLEFIA is similar to the attack described above. In the last round there are two white key should be considered. We denote that WK_3 is a constant which will not affect the sum value and $WK_2 \oplus RK_{21}$ will be replaced by RK'_{21}. The equation of integral attack on 12-round CLEFIA is as follows

$$\begin{aligned}\oplus_{i=1}^{2^{112}} \{ & S_0[S_1(b_0 \oplus RK'_{21,0}) \oplus 08S_0(b_1 \oplus RK'_{21,1}) \oplus 02S_1(b_2 \oplus RK'_{21,2}) \\ & \oplus 0aS_0(b_3 \oplus RK'_{21,3}) \oplus c_8 \oplus RK_{18,0}] \oplus [S_1(c_8 \oplus RK_{23,0}) \\ & \oplus S_0(c_9 \oplus RK_{23,1}) \oplus S_1(c_{10} \oplus RK_{23,2}) \oplus S_0(c_{11} \oplus RK_{23,3})]\} = \oplus_{i=1}^{2^{112}} c', \end{aligned} \tag{4}$$

where

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = P_0 \begin{bmatrix} S_0(c_0 \oplus RK_{22,0}) \\ S_1(c_1 \oplus RK_{22,1}) \\ S_2(c_2 \oplus RK_{22,2}) \\ S_3(c_3 \oplus RK_{22,3}) \end{bmatrix} \oplus \begin{bmatrix} c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}.$$

For those 2^{112} ciphertexts just as in Sec 4.1, we need set 2^{104} counters for 13 bytes of C_0, C_1, C_2, and c', where $c' = c_{12} \oplus 02c_{13} \oplus 04c_{14} \oplus 06c_{15}$, and then the corresponding counter plus one. For all the values of ciphertexts, there are 2^{104} values at most in the 13 bytes. We attack 12-round CLEFIA in 2 steps as follows.

1. We need the precomputation of b_0, b_1, b_2, b_3 in the equtions(4). Guessing the four bytes of RK_{22}, and performing $F_0(C_0, RK_{22})$, then Xoring C_1, we will obtain the corresponding 2^{32} values of (b_0, b_1, b_2, b_3).
2. For the 2^{64} values of $(b_0, b_1, b_2, b_3, C_2)$, do the following operations.
   (a) Guess the value of $RK'_{21,0}, RK'_{21,1}$, and compute the partial sum, then we get 2^{56} values of (x_1, b_2, b_3, C_2). Guess the values of $RK'_{21,2}, RK'_{21,3}$ respectively, 2^{40} values of (x_3, C_2) will be obtained after 2 substeps.
   (b) Guess the value of $RK_{18,0}$ and $RK_{23,0}$, and we get 2^{32} values of $(x_4, c_9, c_{10}, c_{11})$. Guess the remaining 3 key bytes of RK_{23} respectively, the only 2^8 values will be obtained after 3 substeps.

In Step 1, for each value of (C_0, C_1, RK_{22}), there is a corresponding (b_0, b_1, b_2, b_3). So 16×2^{96} bytes memory is needed. The time complexity is about $2^{96}/(2 \times 12) \approx 2^{91.4}$, which can be ignored compared with that in Step 2. In Step 2-(a), it cost $2^{32} \times 2^{16} \times [2^{64} + 2^8 \times (2^{56} + 2^8 \times (2^{48} + 2^8 \times 2^{40}))] = 2^{114}$ S-box lookups. In Step 2-(b), the cost is $2^{64} \times 2^{16} \times [2^{40} + 2^8 \times (2^{32} + 2^8 \times (2^{24} + 2^8 \times (2^{16} + 2^8 \times 2^8)))] = 2^{120} \times 5$ S-box lookups, which is the main cost. The Xoring of c' in each step also can be ignored. There are 13 bytes of key needs to be guessed at all, and after analyzing two structures, the number of keys that can pass the equtions(4) is $(2^{104}) \times (2^{-8})^2 = 2^{88}$. We search these 2^{88} and the remaining 2^{24} keys exhaustively. The total time complexity is about $2 \times 2^{120} \times 5/(2^3 \times 12) \approx 2^{116.7}$ encryptions.

4.3 The 13-Round and 14-Round Attacks

For 13-round CLEFIA we decrypt the last round at first, and then attack 12-round. In this attack we guess 8 more key bytes than in the attack on 12-round CLEFIA. If the data complexity is still 2^{113}, we need to search $2^{192-16} = 2^{172}$ keys. The main time complexity is $2^{176} + 2^{64} \times 2^{116.7} \times 12/13 = 2^{180.5}$. This result is fit to CLEFIA with 192 bits key and 256 bits key. For 14-round CLEFIA, our integral attack needs 2^{113} plaintexts and about $2^{256-16} + 2^{128} \times 2^{116.7} \times 12/14 = 2^{244.5}$ encryptions, which is only fit to CLEFIA with 256 bits key.

5 Conclusion

The integral attacks on reduced-round CLEFIA was described in this paper. Firstly, based on byte-pattern a new 9-round integral distinguisher was proposed, which was also be proved in detail. Secondly, by using the partial sum technique we improved integral attack result on 11-round CLEFIA and proposed integral attack on 12-, 13- and 14-round CLEFIA. Table 1 summarizes our integral attacks together with the previously known integral attacks on CLEFIA.

Table 1. Results of integral attacks on CLEFIA

Attack type	D-Rounds	Rounds	Data	Time	Source
Integral Attack	8	10	$2^{97.6}$	$2^{123.7}$	[9]
	8	11	$2^{99.8}$	$2^{111.4}$	[12]
	8	12	$2^{100.5}$	$2^{176.1}$	[12]
	8	13	$2^{100.9}$	$2^{240.3}$	[12]
	9	12	2^{113}	$2^{116.7}$	Sec.4.2
	9	13	2^{113}	$2^{180.5}$	Sec.4.3
	9	14	2^{113}	$2^{244.5}$	Sec.4.3

Time complexity is measured in encryption units.
D-Rounds is Distinguisher Rounds.

According to Table 1, the integral attacks presented in this paper make significant improvements on both data and time complexities. However, the full rounds CLEFIA provides sufficient safety margin against integral attack.

Without considering the relation of round keys the improbable differential and impossible differential cryptanalysis can only attack on 12-, 13-, and 14-round CLEFIA-128/192/256. So our results also present that in the condition of random round keys integral attack is no less effective than the front two kinds of differential cryptanalysis on evaluating the security of encryption structure. For block cipher cryptanalysis, how to study the relation of differential and integral is more significant, which will be our future work.

Acknowledgments

We would like to thank anonymous referees for their helpful comments and suggestions. The research presented in this paper is supported by the National

Natural Science Foundation of China (No.60873259 and No. 60903212), and Knowledge Innovation Project of The Chinese Academy of Sciences.

References

1. Cihangir Tezcan. The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA. INDOCRYPT 2010, LNCS 6498, pp. 197-209. Springer-Verlag, 2010.
2. CLEFIA design team, Sony Corporation, Comments on the Impossible Differential Analysis of Reduced Round CLEFIA Presented at Inscrypt 2008, Jannuary 8, 2009.
3. FIPS 197. Advanced Encryption Standard. Federal Information Processing Standards Publication 197, U.S. Department of Commerce, N.I.S.T, 2001.
4. Joan Daemen, Lars Knudsen , Vincent Rijmen. The block cipher Square. Fast Software Encryption 1997, LNCS 1267, pp. 149-165. Springer-Verlag, 1997.
5. Lars Knudsen, David Wagner. Integral cryptanalysis. Fast Software Encryption 2002, LNCS 2365, pp. 112-127. Springer-Verlag, 2002.
6. Lei Duo, Chao Li, Keqin Feng. Square Like Attack on Camellia. ICICS 2007, LNCS 4861, pp. 269-283. Springer-Verlag, 2007.
7. Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, Doug Whiting. Improved cryptanalysis of Rijndael. Fast Software Encryption 2000, LNCS 1978, pp. 213-230. Springer-Verlag, 2001.
8. Samuel Galice, Marine Minier. Improving integral attacks against Rijndael-256 upto 9 rounds. AFRICACRYPT 2008, LNCS 5023, pp.1-15. Springer-Verlag, 2008.
9. Sony Corporation. The 128-bit Blockcipher CLEFIA. Security and Performance Evaluation. Revision 1.0 June 1, 2007.
10. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata. The 128-bit block cipher CLEFIA. Fast Software Encryption 2007, LNCS 4593, pp. 181-195. Springer-Verlag, 2007.
11. Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, Hiroyasu Kubo. Impossible Differential Cryptanalysis of CLEFIA. Fast Software Encryption 2008, LNCS 5086, pp. 398-411. Springer-Verlag, 2008.
12. Wei Wang, Wang Xiaoyun. Saturation cryptanalysis of CLEFIA. Journal on Communications. Vol.29 No.10, pp. 88-92. 2008.
13. Wenying Zhang, Jing Han. Impossible differential analysis of reduced round CLEFIA. Inscrypt 2008, LNCS 5487, pp. 181-191. Springer-Verlag, 2008.
14. Yanjun Li, Wenling Wu, Lei Zhang. Integral Attacks on Reduced-Round ARIA Block Cipher. ISPEC 2010, LNCS 6047, pp. 19-29. Springer-Verlag, 2010.