Improved Integral and Zero-correlation Linear Cryptanalysis of Reduced-round CLEFIA Block Cipher

Wentan Yi* and **Shaozhen Chen**

State Key Laboratory of Mathematical Engineering and Advanced Computing,
Zhengzhou 450001, China

Abstract. CLEFIA is a block cipher developed by Sony Corporation in 2007. It is a recommended cipher of CRYPTREC, and has been adopted as ISO/IEC international standard in lightweight cryptography. In this paper, some new 9-round zero-correlation linear distinguishers of CLEFIA are constructed with the input masks and output masks being independent, which allow multiple zero-correlation linear attacks on 14/15-rounds CLEAIA-192/256 with the partial sum technique. Furthermore, the relations between integral distinguishers and zero-correlation linear approximations are improved, and some new integral distinguishers over 9-round are deduced from zero-correlation linear approximations. By using these integral distinguishers and the partial sum technique, the previous integral results on CLEFIA are improved. The two results have either one more rounds or lower time complexity than previous attack results by means of integral and zero-correlation linear cryptanalysis.

Keywords: CLEFIA, Integral attack, Zero-correlation linear cryptanalysis, Cryptography.

1 Introduction

The block cipher CLEFIA[1] was proposed in 2007 by Sony Corporation. It was submitted to IETF (Internet Engineering Task Force) and was on the Candidate Recommended Ciphers List of CRYPTREC. Besides, it was one of the only two lightweight block ciphers recommended by the ISO/IEC standard. CLEFIA performs well in both software and hardware and it is claimed to be highly secure. The efficiency comes from the generalized Feistel structure and the byte orientation, while the security is based on the novel technique called DSM (Diffusion Switching Mechanism), which increases resistance against linear and differential attacks. Up to now, a great deal of attention has been paid to CLEFIA and many cryptanalytic methods have been used to evaluate its security, such as integral[2][3][4], truncated differential[5], impossible differential[6][7][8][9], improbable differential[10][11] and zero-correlation linear cryptanalysis[12]. Main results are summarized in Table 1.

[*] Corresponding authors.
E-mail addresses: nlwt8988@gmail.com.

Attack Type	key size	Rounds	Date	Time	Source
Impossible Differential	192	13	$2^{119.8}$CPs	2^{146}Enc	[9]
Improbable Differential	192	14	2^{127}CPs	$2^{183.2}$Enc	[11]
Truncated Differential	192	14	2^{100}CPs	2^{135}Enc	[5]
Integral	192	13	2^{113}CPs	$2^{180.5}$ Enc	[2]
Integral	192	14	2^{128}CPs	$2^{166.7}$ Enc	Sect.4.2
Multidimensional Zero-correlation	192	14	$2^{127.5}$KPs	$2^{180.2}$ Enc	[12]
Multiple Zero-correlation	192	14	$2^{124.5}$KPs	$2^{173.9}$ Enc	Sect.3.2
Impossible Differential	256	14	$2^{120.3}$CPs	2^{212}Enc	[9]
Improbable Differential	256	15	$2^{127.4}$CPs	$2^{247.5}$Enc	[11]
Truncated Differential	256	15	2^{100}CPs	2^{203}Enc	[5]
Integral	256	14	2^{113}CPs	$2^{244.5}$ Enc	[2]
Integral	256	15	2^{128}CPs	$2^{230.7}$ Enc	Sect.4.2
Multidimensional Zero-correlation	256	15	$2^{127.5}$KPs	$2^{244.2}$ Enc	[12]
Multiple Zero-correlation	256	15	$2^{124.5}$KPs	$2^{237.9}$ Enc	Sect.3.2

Table 1: Summary of the attacks on CLEFIA

Since CLEFIA adopts a 4-branch generalized Feistel structure as the fundamental structure, in which there are two 4-byte F-functions per round, the designers[1] showed that there are 9-round impossible differentials in CLEFIA, that is, $(0, \alpha, 0, 0) \nrightarrow (0, \alpha, 0, 0)$ and $(0, 0, 0, \alpha) \nrightarrow (0, 0, 0, \alpha)$, where α are any 32-bit nonzero values. The length of the parts of the plaintext and ciphertext differences are nonzero 32-bit values, however, the plaintext and ciphertext differences must be the same. By observing the inner structure of F-functions, where the branch numbers of the linear transformations are 5, Tsunoo et al. [9] presented that there are some new 9-round impossible differentials, that is, $(0, \alpha000, 0, 0) \nrightarrow (0, 0\beta00, 0, 0)$, where α, β are any nonzero 8-bit values. Although the length of those parts is 8 bits, it is not necessary for the plaintext and ciphertext differences to be the same. Later, Sun et al.[13] found the 9-round impossible differentials with the forms that $(0, \alpha\beta00, 0, 0) \nrightarrow (0, \gamma000, 0, 0)$, where α, β, γ are any nonzero 8-bit values. For the case of the linear distinguishers with zero-correlation of CLEFIA, there only exist $(\alpha, 0, 0, 0) \nrightarrow (\alpha, 0, 0, 0)$ and $(0, 0, \alpha, 0) \nrightarrow (0, 0, \alpha, 0)$ over 9-round, where the input and output masks α are any 32-bit nonzero values. Now, the questions come up, that is, is there any zero-correlation linear distinguishers satisfying the nonzero parts of the input masks and the output masks are different? The question is a part of the motivation of this work.

Integral and zero-correlation distinguishers were established by Bogdanov et al.[14]. They presented that an integral implies a zero-correlation distinguisher and a zero-correlation distinguisher implies an integral under some independent conditions. For a function F, if the input masks α and output masks $\beta \neq 0$ are independent, then the approximation $(\alpha, 0) \rightarrow (\beta, 0)$ of F has correlation zero if and only that for any λ, $\lambda \cdot F(x_0, x_1)$ is balanced with any fixed x_0. Now, if the approximation $(M'\alpha, 0) \rightarrow (M''\beta, 0)$ has correlation zero, where M', M'' are two linear matrixes and α, β are two independent values, whether there exist corresponding integral distinguishers?

In this paper, we investigate the propagation characteristics of the linear masks on the matrixes of F-functions, and propose some new linear distinguishers with zero correlation over 9-round CLEFIA, where the input masks and output masks are independent. Further, with the links in more general case between zero correlation and integral being given, some integral distinguishers are deduced. Further, key recovery attacks on 14/15-round CLEFIA-192/256 are conducted by means of integral and multiple zero-correlation cryptanalysis. Our contributions are summarized as follows.

1. The matrixes M_0, M_1 are MDS (Maximum Distance Separable) matrixes adopted by CLEFIA in the linear transformations of F-functions, the branch numbers of which are 5. By the propagation characteristics of the linear masks, let $\alpha = (\alpha_0, 0, 0, 0)$ and $\beta = (\beta_0, \beta_1, 0, 0)$ are 32-bit values with $M_0 M_1 \beta = (\gamma_0, \gamma_1, \gamma_2, 0)$, where α_0, β_0, β_1 are any nonzero 8-bit values and $\gamma_0, \gamma_1, \gamma_2$ are any 8-bit values, then, the linear approximations $(M_0\alpha, 0, 0, 0) \rightarrow (M_1\beta, 0, 0, 0)$ are zero correlation linear approximation over 9-round CLEFIA. The new linear approximations are 9-round, the same with the existed approximations, however, the input masks and output masks are not required independent. Further, we apply those new linear approximations to key recovery attacks on 14/15-round CLEFIA-192/256 and propose the first multiple zero correlation linear cryptanalysis of CLEFIA.

2. We study the relations between integral and zero-correlation distinguishers in detail, which can be improved to more general case. For the zero correlation linear approximations with the linear transformations operated on the independent input masks and output masks, there exist corresponding integral distinguishers. Then, some integral distinguishers over 9-round CLEFIA are deduced from the zero correlation linear approximations, which have much stronger ability to distinguish the right keys from wrong keys, because the phenomenons of the integral properties emerge in a extremely low probability in the case of wrong keys. By the new integral distinguisher, we present key recovery attacks on 14/15-round CLEFIA-192/256.

The paper is organized as follows: In Sec.2, we give necessary notations, brief description of CLEFIA and concise explanation of zero-correlation linear cryptanalysis. Some zero-correlation linear distinguishers over 9-round are presented in Sec.3, and multiple zero correlation linear attacks are proposed on 14/15-round CLEFIA-192/256. The relations between integral and zero-correlation linear distinguishers are discussed in Sec.4, some 9-round integral distinguishers are deduced, and key recovery attacks on 14/15-round CLEFIA-192/256 are given. Finally, we summarize our work in Sec.5.

2 Preliminaries

2.1 Notations

F_2	: the set of $\{0,1\}$;
F_2^n	: the set of $\{0,1\}^n$;
$\lvert A\rvert$	: the number of the elements of the set A;

$\oplus$: bitwise XOR;
$a \cdot b$: the scalar product of binary vectors by $a \cdot b = \oplus_{i=1}^{n} a_i b_i$;
M^{-1} : the inverse matrix of M;
M^T : the transposition of matrix M;
$z[i]$: the i-th byte of z, and '0' is the most significant byte;
P, C : the plaintexts and the ciphertexts of CLEFIA;
C_j^i : the j-th 32-bit values of the $i+1$-round with $j = 0, 1, 2, 3$;
rk_i : the subkeys in the round functions of CLEFIA;
wk_i : the 32-bit whitening keys with $i = 0, 1, 2, 3$;
$s_i(\cdot)$: the S-box with $i = 0, 1$;
$F_i(\cdot)$: the round function with $i = 0, 1$;
$X \| Y$: the concatenation of X and Y;

2.2 Description of CLEFIA

CLEFIA is a 128-bit block cipher with variable key lengths of 128, 192 and 256 bits, which takes a 4-branch generalized Feistel network with two parallel F-functions (F_0, F_1) per round. See Fig.1(a). The number of rounds are 18/22/26 for CLEFIA-128/192/256, respectively. Firstly, a 128-bit plaintext P is split up into four 32-bit words P_0, P_1, P_2 and P_3. The input state of the first round $(C_0^0, C_1^0, C_2^0, C_3^0) = (P_0, P_1 \oplus wk_0, P_2, P_3 \oplus wk_1)$. For $r = 1$ to n_r, do the following steps:

$$C_0^r = C_1^{r-1} \oplus F_0(C_0^{r-1}, C_1^{r-1}, rk_{2r-2}),\ C_1^r = C_2^{r-1},$$
$$C_2^r = C^{r-1} \oplus F_1(C_1^{r-1}, C_2^{r-1}, rk_{2r-1}),\ C_3^r = C_0^{r-1}.$$

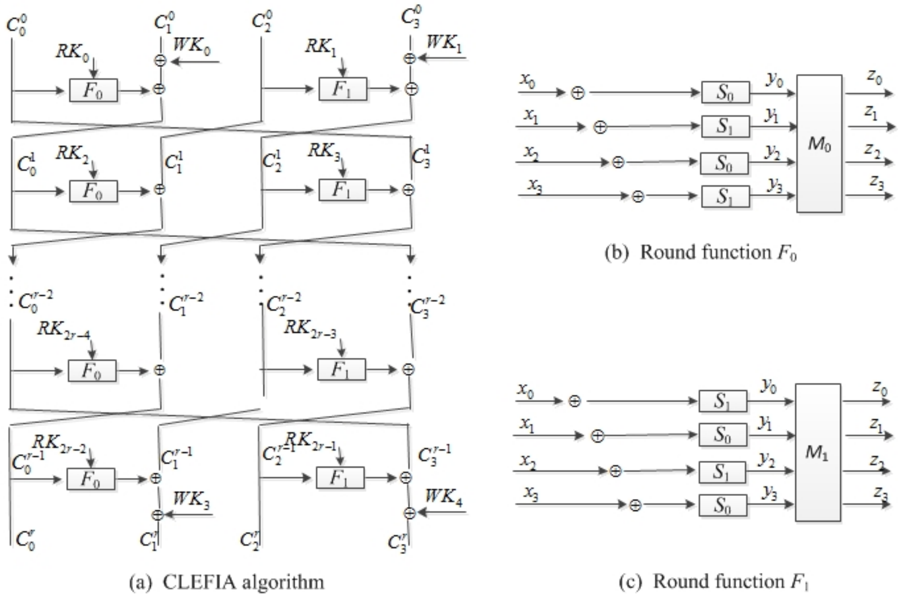
Finally, the 128-bit ciphertext C is computed as $C = (C_0^{nr}, C_1^{nr} \oplus wk_2, C_2^{nr}, C_3^{nr} \oplus wk_3)$.

The round function F_0 and F_1 take the SP structure, see Fig. 1(b)(c). There are two types of byte orientation S-boxes in substitution layer, and the order of s_0 and s_1 is different for both round functions, that is

$$S_0(x_0, x_1, x_2, x_3) = (s_0(x_0), s_1(x_1), s_0(x_2), s_1(x_3)),$$
$$S_1(x_0, x_1, x_2, x_3) = (s_1(x_0), s_0(x_1), s_1(x_2), s_0(x_3)).$$

The diffusion layer uses two different MDS matrix, M_0 and M_1 in functions F_0 and F_1, respectively. The two matrices M_0 and M_1 are defined as

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



(a) CLEFIA algorithm

(b) Round function F_0

(c) Round function F_1

Figure 1: The structure and building blocks of CLEFIA

where the multiplications between these matrices and vectors are performed in F_2^8 defined by the primitive polynomial $x_8 + x_4 + x_3 + x_2 + 1$. By the matrices, we know that $M_0^T = M_0^{-1} = M_0$, $M_1^T = M_1^{-1} = M_1$, and their branch number are both 5.

In addition, our attacks do not utilize the key relation, we omit the details of CLEFIA's key schedule. For the complete specification of CLEFIA, we refer to [1].

2.3 Multiple zero-correlation cryptanalysis

Consider a function $f : F_2^n \mapsto F_2^n$ and let the input of the function be $x \in F_2^n$. The correlation of the linear approximation $x \mapsto \beta \cdot f(x) \oplus a \cdot x$, with an input mask α and an output mask β is defined as follows

$$cor_x(\beta \cdot f(x) \oplus a \cdot x) = 2Pr_x(\beta \cdot f(x) \oplus a \cdot x = 0) - 1.$$

In zero-correlation linear cryptanalysis, the distinguishers use linear approximations with zero correlation. To reduce the data complexity, Bogdanov et al.[15] proposed the multiple zero-correlation linear distinguishers, which use ℓ zero-correlation linear approximations and requires $O(2^n/\sqrt{\ell})$ known plaintexts, where n is the block size of a cipher. Denoted by N, ℓ the number of required known plaintexts and zero-correlation linear approximations for an n-bit block cipher. For each of the given linear approximations, compute the number T_i of times that linear approximation i is fulfilled on N plaintexts and ciphertexts, $i \in \{1, 2, ...\ell\}$.

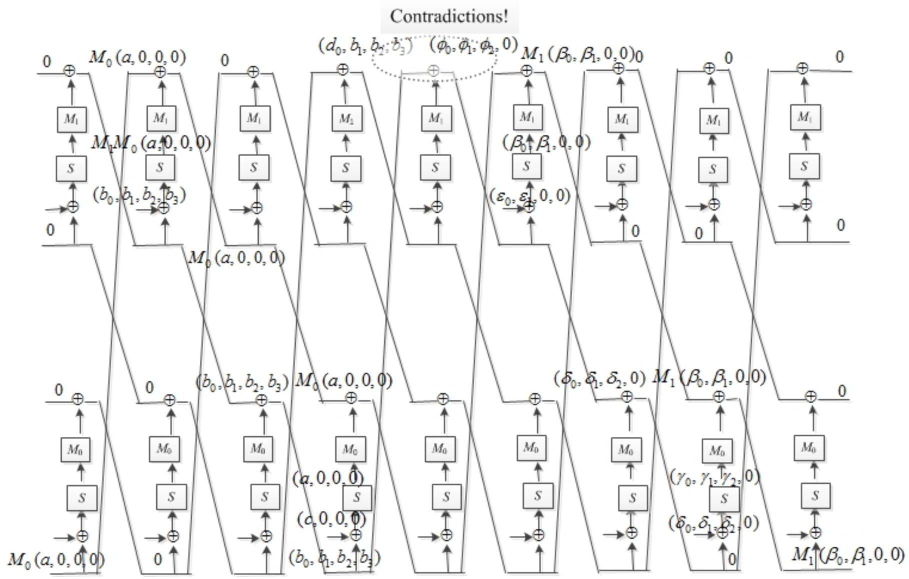

Contradictions!
$M_0\,(a,0,0,0)$
(d_0,b_1,b_2,b_3)
$(\varphi_0,\varphi_1,\varphi_2,0)$
$M_1\,(\beta_0,\beta_1,0,0)$
0
M_1
$M_1 M_0\,(a,0,0,0)$
$(\beta_0,\beta_1,0,0)$
S
(b_0,b_1,b_2,b_3)
$(\varepsilon_0,\varepsilon_1,0,0)$
$M_0\,(a,0,0,0)$
(b_0,b_1,b_2,b_3)
$M_0\,(a,0,0,0)$
$(\delta_0,\delta_1,\delta_2,0)$
$M_1\,(\beta_0,\beta_1,0,0)$
M_0
$(a,0,0,0)$
$(\gamma_0,\gamma_1,\gamma_2,0)$
$(c,0,0,0)$
$(\delta_0,\delta_1,\delta_2,0)$
$M_0\,(a,0,0,0)$
(b_0,b_1,b_2,b_3)
$M_1\,(\beta_0,\beta_1,0,0)$

Figure 2: Zero-correlation linear approximations of 9-round CLEFIA

Each T_i suggests an empirical correlation value $\hat{c}_i = 2T_i/N - 1$. Then, evaluate the statistic:

$$T = \sum_{z=0}^{\ell} \hat{c}_i^2 = \sum_{z=0}^{\ell} (2\frac{T_i}{N} - 1)^2.$$

Under a statistical independency assumption, the statistic T follows a $\mathscr{X}^2$ -distribution with mean $\mu_0 = \ell/N$ and variance $\sigma_0^2 = 2\ell/N^2$ for the right key guess, while for the wrong key guess, it follows a $\mathscr{X}^2$-distribution with mean $\mu_1 = \ell/N + \ell/2^n$ and variance $\sigma_1^2 = 2\ell/(N^2 + 2^{2n} + N2^{n-1})$.

If the probability of the type-I error and the type-II error to distinguish between a wrong key and a right key are denoted as β_0 and β_1, respectively, considering the decision threshold $\tau = \mu_0 + \sigma_0 z_{1-\beta_0} = \mu_1 - \sigma_0 z_{1-\beta_1}$, the number of known plaintexts N should be about

$$N = \frac{2^n(z_{1-\beta_0} + z_{1-\beta_1})}{\sqrt{\ell/2} - z_{1-\beta_1}}, \tag{2.1}$$

where $z_{1-\beta_0}$ and $z_{1-\beta_1}$are the respective quantiles of the standard normal distribution. More details are described in [15].

3 Multiple zero-correlation cryptanalysis of 14/15-round CLEFIA-192/256

3.1 Zero-correlation linear approximations for 9-round CLFEIA

To construct the zero-correlation linear approximations, one adopts the miss-in-the-middle techniques just like to find impossible differential. Any linear approximations with nonzero

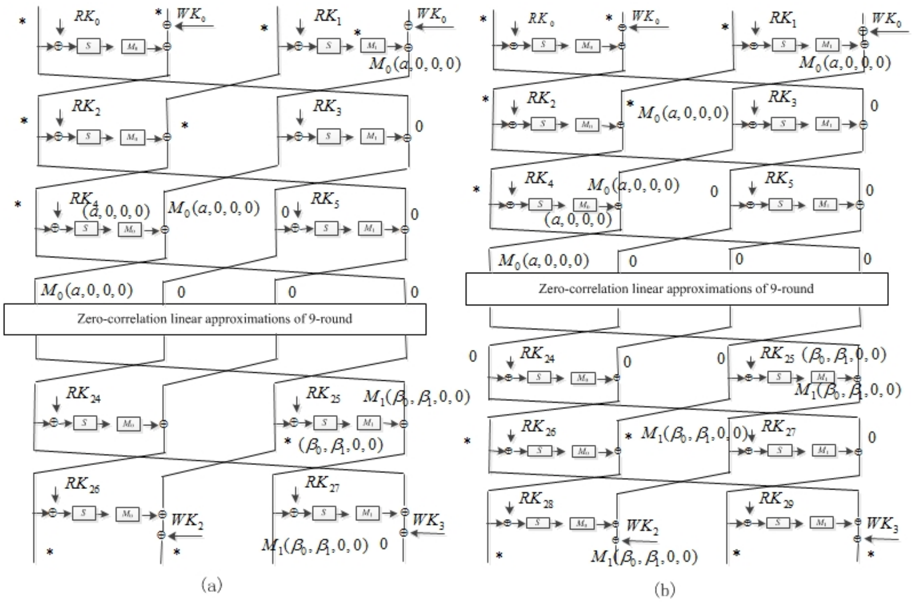


Figure 3: Zero-correlations linear attacks on 14/15-round CLEFIA-192/256

bias is concatenated to any linear approximations with nonzero bias in the inverse direction, where the intermediate masks states contradict with each other. For the propagation characteristics of the linear masks on building element, see [16]. We assert the linear approximations over 9-round CLEFIA (covering rounds 1-9, see Fig.2).

$$\big(M_0(\alpha_0,0,0,0),0,0,0\big) \rightarrow \big(M_1(\beta_0,\beta_1,0,0),0,0,0\big)$$

have zero-correlation, where $M_0M_1(\beta_0,\beta_1,0,0)=(\gamma_0,\gamma_1,\gamma_2,0)$, that is $0x40\gamma_0 \oplus 0x37\gamma_1 = 0$, $\alpha_0,\beta_0,\beta_1 \in F_2^8/\{0\}$ and $\gamma_0,\gamma_1,\gamma_2 \in F_2^8$.

Along the encryption direction: We consider the linear trail with non-zero correlation. Given the mask $\big(M_0(\alpha_0,0,0,0),0,0,0\big)$, the mask of the 4-th branch after 5 rounds must have the form (d_0,b_1,b_2,b_3) if the corresponding 5-round linear trail has non-zero correlation, where $b_1,b_2,b_3 \in F_2^8$ are unknown non-zero values.

Along the decryption direction: Given the mask $\big(M_1(\beta_0,\beta_1,0,0),0,0,0\big)$, the mask of the 4-th branch after 4 rounds must have the form $(\phi_0,\phi_1,\phi_2,0)$ if the corresponding 4-round linear trail has non-zero correlation, as the reason that $M_0M_1(\beta_0,\beta_1,0,0)=(\gamma_0,\gamma_1,\gamma_2,0)$, where $\gamma_0,\gamma_1,\gamma_2,\phi_0,\phi_1,\phi_2$ are unknown values.

Contradiction: We just focus on the linear masks of the 4-th branch of 5-th round function. From the encryption direction, the input masks are (d_0,b_1,b_2,b_3) under the condition the corresponding linear trail has non-zero correlation, where b_1,b_2,b_3 are unknown non-zero values. Similarly, from the decryption direction, the output masks are $(\phi_0,\phi_1,\phi_2,0)$, where

Guess Keys	Counters	Computed States
$rk_0[0]$	$y_4 = P_0[1,2,3]\|P_1\|P_2\|M_0P_3[0]\|M^1$	$P_1[0]+=0x01s_0(P_0[0]\oplus rk_0[0]), P_1[1]+=0x02s_0(P_0[0]\oplus rk_0[0]);$ $P_1[2]+=0x04s_0(P_0[0]\oplus rk_0[0]), P_1[3]+=0x06s_0(P_0[0]\oplus rk_0[0]);$
$rk_0[1]$	$y_5 = P_0[2,3]\|P_1\|P_2\|M_0P_3[0]\|M^1$	$P_1[0]+=0x02s_1(P_0[1]\oplus rk_0[1]), P_1[1]+=0x01s_1(P_0[1]\oplus rk_0[1]);$ $P_1[2]+=0x06s_1(P_0[1]\oplus rk_0[1]), P_1[3]+=0x04s_1(P_0[1]\oplus rk_0[1]);$
$rk_0[2]$	$y_6 = P_0[3]\|P_1\|P_2\|M_0P_3[0]\|M^1$	$P_1[0]+=0x04s_0(P_0[2]\oplus rk_0[2]), P_1[1]+=0x06s_0(P_0[2]\oplus rk_0[2]);$ $P_1[2]+=0x02s_0(P_0[2]\oplus rk_0[2]), P_1[3]+=0x01s_0(P_0[2]\oplus rk_0[2]);$
$rk_0[3]$	$y_7 = P_1\|P_2\|M_0P_3[0]\|M^1$	$P_1[0]+=0x06s_1(P_0[3]\oplus rk_0[3]), P_1[1]+=0x04s_1(P_0[3]\oplus rk_0[3]);$ $P_1[2]+=0x02s_1(P_0[3]\oplus rk_0[3]), P_1[3]+=0x01s_1(P_0[3]\oplus rk_0[3]);$
$rk_1[1]$	$y_8 = P_1\|P_2[0,2,3]\|M_0P_3[0]\|M^1$	$M_0P_3[0]+=0x08s_0(P_2[1]\oplus rk_1[1]);$
$rk_1[2]$	$y_9 = P_1\|P_2[0,3]\|M_0P_3[0]\|M^1$	$M_0P_3[0]+=0x02s_1(P_2[2]\oplus rk_1[2]);$
$rk_1[3]$	$y_{10} = P_1\|P_2[0]\|M_0P_3[0]\|M^1$	$M_0P_3[0]+=0x0as_0(P_2[3]\oplus rk_1[3]);$
$rk_1[0]$	$y_{11} = P_1\|P_2[0]\|M_0P_3[0]\|M^1$	$M_0P_3[0]+=0x01s_1(P_2[0]\oplus rk_1[0]);$
$rk_2[0]\oplus wk_1[0]$	$y_{12} = P_1[1,2,3]\|P_2[0]\|M_0P_3[0]\|M^1$	$P_2[0]+=0x01s_0(P_1[0]\oplus rk_2[0]\oplus wk_1[0]);$
$rk_2[1]\oplus wk_1[1]$	$y_{13} = P_1[2,3]\|P_2[0]\|M_0P_3[0]\|M^1$	$P_2[0]+=0x02s_1(P_1[1]\oplus rk_2[1]\oplus wk_1[1]);$
$rk_2[2]\oplus wk_1[2]$	$y_{14} = P_1[3]\|P_2[0]\|M_0P_3[0]\|M^1$	$P_2[0]+=0x04s_0(P_1[2]\oplus rk_2[2]\oplus wk_1[2]);$
$rk_2[3]\oplus wk_1[3]$	$y_{15} = P_2[0]\|M_0P_3[0]\|M^1$	$P_2[0]+=0x06s_1(P_1[3]\oplus rk_2[3]\oplus wk_1[3]);$
$rk_4[1]$	$y_{16} = M_0P_3[0]\|M^1$	$M_0P_3[0]+=0x01s_0(P_2[0]\oplus rk_4[1]);$

Table 2: Partial encryption and decryption of the attack on 14-round CLEFIA.

ϕ_0, ϕ_1, ϕ_2 are unknown non-zero values, which is contradiction with that $b_3 \neq 0$. Thus, the linear hull is a zero-correlation linear hull. See Figure 2.

3.2 Key Recovery for 14/15-Round CLFEIA-192/256

In this section, we will attack 14-round CLFEIA-192. We mount the 9-round linear approximations from round 4 to round 12, and extend 3 rounds forward and 2 rounds backward respectively, see Fig.3(a). The key-recovery attacks on 14-round CLEFIA-192 are proceeded with the partial-sum technique as follows.

1. Collect all the N plaintext-ciphertext pairs (P, C). Allocate 8-bit counters $N_1[y_1]$ for 2^{160} possible values of

$$y_1 = P_0\|P_1\|P_2\|M_0P_3[0]\|C_0\|C_1[0,1]\|M^1,$$

and initialize them to zero, where M^1 is a 8-bit value with

$$M^1 = 0x34M_1C_2[0] \oplus 0x40M_1C_2[1].$$

For every (P, C) pair, extract the value of y_1 and increase the corresponding counter $N_1[y_1]$.

2. Allocate 8-bit counters $N_2[y_2]$ for 2^{120} possible values of

$$y_1 = P_0\|P_1\|P_2\|M_0P_3[0]\|C_1[1]\|M^1,$$

and initialize them to zero. Guess rk_{26} and $wk_2[0] \oplus rk_{27}[0]$, and partially decrypt y_1 to get the value of y_2, that is,

$$M^1 = M^1 \oplus 0x34 s_1\big(F_0(C_0, rk_{26})[0] \oplus wk_2[0] \oplus rk_{27}[0]\big)$$

then update the corresponding counter by $N_2[y_2] += N_1[y_1]$.

3. Allocate a counter $N_3[y_3]$ for 2^{112} possible values of

$$y_3 = P_0 \| P_1 \| P_2 \| M_0 P_3[0] \| M^1,$$

and initialize them to zero. Guess $wk_2[1] \oplus rk_{27}[1]$, and partially decrypt y_2 to get the value of y_3, that is,

$$M^1 = M^1 \oplus 0x40 \times 0x08 s_0\big(F_0(C_0, rk_{26})[1] \oplus wk_2[1] \oplus rk_{27}[1]\big)$$

then update the corresponding counter by $N_3[y_3] += N_2[y_2]$.

The following steps in the partial encryption and decryption phase are similar to Step 3. Thus, to be consistent, we use Table 2 to show the details of each step of the partial encryption and decryption.

17. Compute the statistic T according to Equation (1). If $T < \tau$, the guessed key value is a right key candidate. After Step 16, 152 key bits have been guessed, then, there are 40 master key bits that we have not guessed, we do exhaustive search for all keys conforming to this possible key candidate.

Complexity of the Attack. In this attack, we set the type-I error probability $\beta_0 = 2^{-2.7}$ and the type-II error probability $\beta_1 = 2^{-20}$. We have $z_{1-\beta_0} = 1$, $z_{1-\beta_1} = 4.2$, $n = 128$, $\ell = 2^{16}$. The date complex N is about $2^{124.5}$ by equation 2.1, and the decision threshold $\tau \approx 2^{6.23}$. The time complexity of steps 1-17 in the described attack is as follows:

(1) Step 1 requires $2^{124.5}$ memory accesses;

(2) Step 2 requires $2^{124.5} \times 2^{40} = 2^{164.5}$ memory accesses, because we should guess 40 bits rk_{26} and $wk_2[0] \oplus rk_{27}[0]$;

(3) Step 3-11 require 9×2^{168} memory accesses;

(4) Step 12-16 require 5×2^{176} memory accesses;

(3) Step 17 requires $2^{152} \times 2^{20}$ 14-round CLEFIA encryption, because only the right key candidates can survive in the wrong key filtration.

If we assume that processing each memory accesse is equivalent to half round encryption, then the total time complexity is about $1/2 \times 5/14 \times 2^{176} \approx 2^{173.9}$ 14-round encryptions. In total, the data complexity is $2^{124.5}$ KPs, the time complexity is about $2^{173.9}$ 14-round encryptions and the memory requirement are 2^{160} bytes for counters.

For the attack on 15-round CLEFIA-256, we mount the 9-round zero-correlation linear approximations from round 4 to round 12, and extend 3 rounds forward and 3 rounds backward, see Fig.3(b). We proceed similar steps to attack 14-round CLEFIA-192. The data complexity of the attack is $2^{124.5}$ KPs. The total time complexity is $2^{237.9}$ encryptions and the memory complexity is about 2^{224} bytes.

4 Integral cryptanalysis of 14/15-round CLEFIA-192/256

In this section, the relations between integral and zero-correlation linear distinguishers are discussed, some 9-round integral distinguishers are deduced, and then, key recovery attacks on 14/15-round CLEFIA-192/256 are given by means of integral.

4.1 Some new integral distinguishers over 9-round CLEFIA

A number of relations have been established among some known attacks methods, so far. Bogdanov et al.[14] presented that an integral implies a zero-correlation distinguisher and a zero-correlation distinguisher implies an integral under some independent conditions.

Theorem 4.1. [14] *Let m, m_1, m_2 be integrals, for the vectorial Boolean function $f : F_2^{m_1} \times F_2^{m_2} \to F_2^m$, the following are equivalent.*

(i) $cor_{x_{m_2}}\big((b_q, 0) \cdot f(x_{m_1}, x_{m_2})\big) = 0$*, for all* $b_q \in F_2^q \setminus \{0\}$*;*

(ii) $cor_{x_{m_1}, x_{m_2}}\big((d_{m_1}, 0) \cdot x \oplus (b_q, 0) \cdot f(x_{m_1}, x_{m_2})\big) = 0$*, for all* $d_{m_1} \in F_2^{m_1}$ *and* $b_q \in F_2^q \setminus \{0\}$*.*

Let M_0, M_1 be two invertible matrices, for any $d_{m_1'} \in F_2^{m_1'}$, $b_{q_1} \in F_2^{q_1}$, and $M_0(d_{m_1'}, 0, ..., 0) \in F_2^{m_1}$, $M_1(b_{q_1}, 0, ..., 0) \in F_2^q$, then we have the following results.

Corollary 4.1. *The following two conditions are equivalent.*

(i) $cor_{x_{(d_{m_1}-d_{m_1'})}, x_{m_2}}\big(b_{q_1} \cdot M_1^T f\big((M_0^{-1})^T x\big)_{q_1}\big) = 0$*, for all* $b_{q_1} \in F_2^{q_1} \setminus \{0\}$*;*

(ii) $cor_x\big((M_0(d_{m_1'}, 0, ..., 0), 0) \cdot (x_{d_{m_1'}}, x_{(d_{m_1}-d_{m_1'})}, x_{m_2}) \oplus (M_1(b_{q_1}, 0, ..., 0), 0) \cdot f(x)\big) = 0$*, for all* $d_{m_1'} \in F_2^{m_1'}$ *and* $b_{q_1} \in F_2^{q_1} \setminus \{0\}$*.*

The corollary can be proved by the fact that $(Ma \cdot x) = (a \cdot M^T x)$, where M is a linear transformation, so we omit the proof here. By Corollary 4.1, an integral distinguisher covering 9-round of CLEFIA can be deduced from zero-correlation linear approximations.

Property 4.1. *Choose a set of 2^{120} input of the r round , where the 32-bit values of C_0^r are set to be a the form $M_0(a, b, c, d)$, C_1^r, C_2^r, C_3^r traversal F_2^{32}, where a is fixed to be any 8-bit values, b, c, d traversal F_2^8. Encrypt the chosen 2^{120} values 9 rounds, then, each of the 2^8 possible values of $0x37(M_1 C_0^{r+9})[0] \oplus 0x40(M_1 C_0^{r+9})[1]$ occurs 2^{112} times.*

Let $F : F_2^{120} \to F_2^8$ be a random vectorial Boolean function and the sets $A_j = \{x_j \in F_2^{120} | F(x_j) = y_j\}$, where $y_j \in F_2^8$, $1 \le j \le 2^8$, then the probability of the random vectorial Boolean function satisfying $|A_j| = 2^{112}$, for each $1 \le j \le 2^8$ is about

$$\big(C_{2^{120}}^{2^{112}} \times C_{2^{120}-2^{112}}^{2^{112}} \times \cdots \times C_{2^{113}}^{2^{112}} \times C_{2^{112}}^{2^{112}}\big)/(2^8)^{2^{120}},$$

which is extremely small, compared with 2^{-192}. Only under the case of the right keys, the phenomenons of the integral properties can emerge, that is, the integral distinguisher has much stronger ability to distinguish the right and wrong keys.

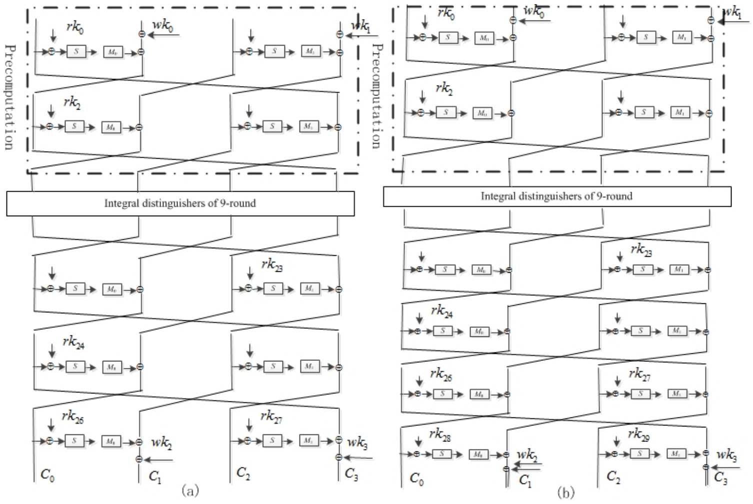


Figure 4: Integral attacks on 14/15-round CLEFIA-192/256

4.2 Key-recovery attacks on 14/15-round CLEFIA-192/256

In this section, the new integral distinguisher is applied to the key-recovery attacks on 14/15-round CLEFIA-192/256. The 9-round integral distinguisher starts from round 3 and end at round 11, see Figure 4(a). In the attack process, we adopt the idea of subkey-dependent chosen plaintexts. We first construct a precomputation table T.

Table T: For each of 2^{160} possible pairs$(P_0, P_1, P_2[1,2,3], P_3, rk_0, wk_0[0] \oplus rk_2[0])$, we calculate $P_2[0] = s_0(F_0(P_0, rk_0)[0] \oplus wk_0[0] \oplus rk_2[0]) \oplus 0x02P_2[1] \oplus 0x04P_2[2] \oplus 0x06P_2[3]$. Store all the 2^{120} pairs (P_0, P_1, P_3, P_4) in a hash table T indexed by 40-bit $(rk_0, wk_0[0] \oplus rk_2[0])$.

Attack Process. The key-recovery attacks on 14-round CLEFIA-192 are proceeded with the partial-sum technique as follows.

1. Guess the subkeys $rk_0, wk_0[0] \oplus rk_2[0]$, by the table T, choose a set of 2^{120} plaintexts to obtain their cipertexts, allocate a 32-bit counter $V_1[x_1]$ for each of 2^{104} possible values of

$$x_1 = C_0 \| C_2 \| C_3 \| M^1,$$

and initialize them to zero, where M^1 is a 8-bit value with

$$M^1 = 0x34M_1C_1[0] \oplus 0x40M_1C_1[1].$$

For each set of the chosen ciphertexts, extract the value of x_1 and increase the corresponding counter $V_1[x_1]$.

2. Allocate 32-bit counters $V_2[x_2]$ for 2^8 possible values of

$$x_2 = C_0 \| C_1[1,2,3] \| C_3 \| M^1,$$

and set them zero. Guess $rk_{27}[0]$ and partially decrypt x_1 to get the value of x_2, then update the corresponding counter $V_2[x_2] += V_1[x_1]$.

3. In the following partial decryption phase, guess $rk_{27}[1]$, $rk_{27}[2]$, $rk_{27}[3]$, $rk_{26}[0]$, $rk_{26}[1]$, $rk_{26}[2]$, $rk_{26}[3]$, $rk_{24}[0]$,$rk_{24}[1]$,$rk_{24}[2]$,$rk_{24}[3]$, $rk_{23}[0]$, $rk_{23}[1]$, compute corresponding values and update the counters, and get $V_3[x_3]$, where

$$x_3 = 0x37(M_1^T C_0^{11})[0] \oplus 0x40(M_1^T C_0^{11})[1].$$

4. After Step 3, 152 key bits have been guessed. If there exists $x_3 \in F_2^8$, $V_3[x_3] \neq 2^{112}$, discard the guessed keys and guess another subkey until we get the correct subkey. As there are 40 master key bits that we have not guessed, we do exhaustive search for all keys conforming to this possible key candidate.

Complexity of the Attack. In this attack,there are 152-bit key value guessed during the encryption phase, and only the right key candidates survive in the wrong key filtration.

(1) Step 1 requires about 2^{160} memory accesses;

(2) Step 2 requires about $2^{104} \times 2^{40} \times 2^8 = 2^{152}$ memory accesses;

(3) Step 3 requires about 10×2^{168} memory accesses;

(4) Step 4 requires 2^{40} 14-round CLEFIA encryption, because only the right key candidates can survive in the wrong key filtration.

If we assume that processing each memory accesse is equivalent to 1/2 round encryption, then the total time complexity is about $2^{168} \times 1/2 \times 10/14 \approx 2^{166.7}$ 14-round encryptions. In total, the data complexity is 2^{128} CPs, the time complexity is about $2^{166.7}$ 14-round encryptions and the memory requirement are 2^{104} bytes for counters.

For the integral attack on 15-round CLEFIA-256, we mount the 9-round zero-correlation linear approximations from round 3 to round 12, see Fig.4(b). We proceed similar steps to attack 14 rounds of CLEFIA-192. The data complexity of the attack is 2^{128} CPs. The total time complexity is $2^{230.7}$ encryptions and the memory complexity is about 2^{128} bytes.

5 Conclusion

In this paper, we have evaluated the security of CLEFIA by means of integral and zero-correlation linear cryptanalysis. Firstly, we investigate the propagation characteristics of the linear masks on the matrixes of F-functions, and propose some new linear distinguishers with zero correlation over 9-round CLEFIA, where the input masks and output masks are independent, then multiple zero-correlation linear attack are conducted on 14/15-round CLEFIA-192/256. Further, the relations between zero correlation and integral are improved, and some integral distinguishers are deduced. Key recovery attacks on 14/15-round CLEFIA-192/256 are conducted by means of integral cryptanalysis. These results are not the best for CLEFIA compared with the truncated differential results, however, the multiple zero-correlation linear attacks are the better compared with the multidimensional zero-correlation linear attacks in terms of both data and time complexity and our integral cryptanalysis can attack one round more than previous integral cryptanalysis.

References

[1] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181-195. Springer, Heidelberg (2007)

[2] Li, Y., Wu, W., Zhang, L.: Improved integral attacks on reduced-round CLEFIA block cipher. In: Jung, S., Yung, M. (eds.) WISA 2011. LNCS, vol. 7115, pp. 28-39. Springer, Heidelberg (2012)

[3] Sasaki, Y., Wang, L.: Meet-in-the-middle technique for integral attacks against feistel ciphers. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 234-251. Springer, Heidelberg (2013)

[4] Wang, W., Wang, X.: Saturation cryptanalysis of CLEFIA. J. Commun. 29(10), pp. 88-92 (2008)

[5] Li, L., Jia, K., Wang, X., Dong, X.: Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia. In G. Leander (Ed.): FSE 2015, LNCS 9054, pp. 48-70, Springer, Heidelberg (2015)

[6] Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon.In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179-199. Springer, Heidelberg (2014)

[7] Mala, H., Dakhilalian, M., Shakiba, M.: Impossible differential attacks on 13-round CLEFIA-128. J. Comput. Sci. Technol. 26(4), pp.744-750 (2011)

[8] Tang, X., Sun, B., Li, R., Li, C.: Impossible differential cryptanalysis of 13-round CLEFIA-128. J. Syst. Softw. 84(7), pp.1191-1196 (2011)

[9] Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible differential cryptanalysis of CLEFIA. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 398-411. Springer, Heidelberg (2008)

[10] Blondeau, C.: Improbable differential from impossible differential: on the validity of the model. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 149-160. Springer, Heidelberg (2013)

[11] Tezcan, C.: The improbable differential attack: cryptanalysis of reduced round CLEFIA. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 197-209. Springer, Heidelberg (2010)

[12] Bogdanov, A., Geng, H., Wang, M., Wen, L., Collard, B.: Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards camellia and CLEFIA. In: Lange, T., Lauter, K., Lison ek, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 306-323. Springer, Heidelberg (2014)

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

[14] Bogdanov,A., Leander, G., Nyberg, K.,Wang, M.: Integral and Multidimensional Linear Distinguishers with Correlation Zero. In Wang, K.,Sako, K., (eds), ASIACRYPT 2012 Vol. 7658, LNCS., pp. 244-261. Springer (2012)

[15] Bogdanov, A., Wang, M.: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. FSE 2012, LNCS, vol.7549, pp. 29-48, Springer-Verlag (2012)

[16] Bogdanov, A., Rijmen,V.: Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography March 2014, Volume 70, Issue 3, pp. 369-383 (2014)