Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA

Andrey Bogdanov[1](✉), Huizheng Geng[2](✉), Meiqin Wang[2](✉), Long Wen[2](✉),
and Baudoin Collard[3]

[1] Technical University of Denmark, Kongens Lyngby, Denmark
anbog@dtu.dk

[2] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
{huizhenggeng,longwen}@mail.sdu.edu.cn, mqwang@sdu.edu.cn

[3] Université Catholique de Louvain, Louvain-la-Neuve, Belgium

Abstract. Zero-correlation linear cryptanalysis is based on the linear approximations with correlation exactly zero, which essentially generalizes the integral property, and has already been applied to several block ciphers — among others, yielding best known attacks to date on round-reduced TEA and CAST-256 as published in FSE'12 and ASIACRYPT'12, respectively.

In this paper, we use the FFT (Fast Fourier Transform) technique to speed up the zero-correlation cryptanalysis. First, this allows us to improve upon the state-of-the-art cryptanalysis for the ISO/IEC standard and CRYPTREC-portfolio cipher Camellia. Namely, we present zero-correlation attacks on 11-round Camellia-128 and 12-round Camellia-192 with FL/FL^{-1} and whitening key starting from the first round, which is an improvement in the number of attacked rounds in both cases. Moreover, we provide multidimensional zero-correlation cryptanalysis of 14-round CLEFIA-192 and 15-round CLEFIA-256 that are attacks on the highest numbers of rounds in the classical single-key setting, respectively, with improvements in memory complexity.

Keywords: Block cipher · Zero-correlation cryptanalysis · FFT · Multidimesional linear cryptanalysis · Camellia · CLEFIA

1 Introduction

Zero-correlation linear cryptanalysis proposed by Bogdanov and Rijmen in [2] has its theoretical foundation in the availability of numerous key-independent unbiased linear approximations with correlation zero for many ciphers. (If p is the probability for a linear approximation to hold, its correlation is defined as $c = 2p - 1$). Though the initial distinguisher of [2] had some limitations in terms of data complexity, they were overcome in the FSE'12 paper [3], where the existence of multiple linear approximations with correlation zero in target ciphers

T. Lange, K. Lauter, and P. Lisoněk (Eds.): SAC 2013, LNCS 8282, pp. 306–323, 2014.
DOI: 10.1007/978-3-662-43414-7_16, © Springer-Verlag Berlin Heidelberg 2014

was used to propose a more data-efficient distinguisher. This resulted in improved attacks on reduced-round TEA and XTEA. The zero-correlation attack on 21 (resp. 23) rounds of TEA remains the attack breaking most rounds of TEA in the single secret-key setting. In a follow-up work at ASIACRYPT'12 [4], zero-correlation cryptanalysis was shown to apply to CAST-256 and to break the highest number of rounds here as well. Moreover, fundamental links of integral cryptanalysis to zero-correlation cryptanalysis have been revealed. Namely, integrals (similar to saturation or multiset distinguishers) have been demonstrated to be essentially a special case of the zero-correlation property. On top of that, a multidimensional distinguisher has been constructed for the zero-correlation property, which removed the unnecessary independency assumptions on the distinguishing side.

While the question of coping with the data requirements of zero-correlation distinguishers has been studied in detail, the *key recovery techniques* used so far on top of those statistical distinguishers remain quite rudimentary. To attack as many rounds as possible, the attackers choose to span the zero-correlation property over a high number of rounds, which usually yields a decrease in the number of zero-correlation linear approximations available. Moreover, for the same reason, the cryptanalysts tend to partially encrypt/decrypt over as many rounds as possible, which gives a high number of (sub)key bits that need to be guessed. Now, in a cryptanalytic effort based on correlation zero, one has to evaluate the sample correlation of all linear approximations (usually, a rather low number) for all plaintext-ciphertext pairs (usually, a significantly higher number) and all key guesses (which can be very high). In terms of computational complexity, this is the bottle neck of zero-correlation attacks so far. And this is exactly the point where the Discrete Fast Fourier Transform comes in handy.

Contributions. The contributions of this paper are three-fold:

Zero-correlation cryptanalysis with FFT: We use Discrete Fast Fourier Transform — that has been previosly used in linear cryptanalysis in [7] — to improve the time complexity of zero-correlation attacks. It relies on eliminating the redundant computations from the partial encryption/decryption in the course of zero-correlation key recovery. For that, an auxiliary $\{-1, 1\}$-matrix with a level-circulant structure is defined such that the evaluation of the sample correlation can be done by matrix-vector multiplication for different keys. By making use of this special structure, the matrix-vector multiplication can be computed efficiently with FFT. This technique is described in Sect. 3.

Improved cryptanalysis of Camellia: We apply this FFT technique to the block cipher Camellia and obtain an improvement in the number of attacked rounds for Camellia-128 and Camellia-192.

Camellia is a block cipher jointly proposed by Mitsubishi and NTT in 2000 [1]. It was adopted as international standard by ISO/IEC [8]. Camellia is a CRYPTREC-recommended cipher for Japanese e-Government applications and is a part of the NESSIE project portfolio. It has a 128-bit block and supports a variable key size. The number of rounds depends on the key size: 18 rounds for 128-bit keys, 24 rounds for 192-bit keys, and 24 rounds for 256-bit keys. The basic Feistel structure is used and a logical keyed transformation layer FL/FL^{-1} is applied every six rounds.

Camellia has received a great deal of attention from cryptanalysts with dozens of attacks on reduced-round variants published alone in the recent years. However, to be able to claim more attacked rounds, most of the existing attacks do not consider FL/FL^{-1} and whitening key. Moreover, some of them only include FL/FL^{-1} but no whitening keys. As opposed to that, in this paper, we only discuss attacks on *Camellia with FL/FL^{-1} and whitening key starting from the first round*. Rather recently, some attacks on reduced-round Camellia with FL/FL^{-1} and whitening key have been introduced [6,11,12]. In this setting, the best attack on Camellia-128 is the impossible differential attack on 10 rounds [11]. A similar attack can break 11 rounds of Camellia-192 [11].

Table 1. Summary of attacks on Camellia with FL/FL^{-1} and whitening key

Key	Attack Type	Rounds	Data	Time (*Ens.*)	Memory (*Bytes*)	Source
128	Imp. Diff	10	$2^{113.8}$CPs	$2^{120.0}$	$2^{84.8}$	[11]
	ZC. FFT	**11**	$2^{125.3}$**KPs**	$2^{125.8}$	$2^{112.0}$	Sect. 4.2
192	Imp. Diff	10	$2^{121.0}$CPs	$2^{175.3}$	$2^{155.2}$	[6]
	Imp. Diff	10	$2^{118.7}$CPs	$2^{130.4}$	$2^{135.0}$	[9]
	Imp. Diff	11	$2^{114.6}$CPs	$2^{184.0}$	$2^{141.6}$	[11]
	ZC. FFT	**12**	$2^{125.7}$**KPs**	$2^{188.8}$	$2^{112.0}$	Sect. 4.3

CPs: Chosen Plaintexts, KPs: Known Plaintexts

In this paper, with the FFT zero-correlation technique, we propose an attack on 11 rounds of Camellia-128. Moreover, we propose an FFT zero-correlation attack on 12-round Camellia-192, while previously only 11 rounds could be attacked. The attacks are given in Sect. 4. Our improvements upon the state-of-the-art cryptanalysis for Camellia are summarized in Table 1.

Improved cryptanalysis of CLEFIA: Multidimensional zero-correlation attacks on 14-round CLEFIA-192 and 15-round CLEFIA-256 with better memory complexities than the currently best published cryptanalysis are reported, while the time and data complexities are almost identical, featuring a rather high data complexity though.

CLEFIA is a block cipher proposed in 2007 by Sony Corporation [15] and has been adopted as ISO/IEC international standard in lightweight cryptography. The block size is 128 bits and the key size is 128, 192, or 256 bits. The numbers of rounds for CLEFIA-128, CLEFIA-192 and CLEFIA-256 are 18, 22 and 26, respectively. Despite CLEFIA's relatively recent publication, the cryptanalysts have been active attacking it [10,17–20] with the best attack to date being the improbable differential cryptanalysis that can break 14-round CLEFIA-192 and 15-round CLEFIA-256 [16].

With the multidimensional zero-correlation cryptanalysis, we can attack 14-round CLEFIA-192 and 15-round CLEFIA-256 with significantly reduced

Table 2. Summary of attacks on CLEFIA

Key size	Attack type	Rounds	Data	Time (*Ens.*)	Memory (*Bytes*)	Source
192	Imp. Diff	13	$2^{111.8}$CPs	2^{155}	2^{116}	[18]
	Imp. Diff	13	$2^{116.6}$CPs	2^{171}	2^{101}	[18]
	Imp. Diff	13	$2^{108.6}$CPs	2^{179}	2^{113}	[18]
	Imp. Diff	13	$2^{108.6}$CPs	2^{171}	2^{109}	[18]
	Integral	13	2^{113}CPs	$2^{180.5}$	N/A	[10]
	Imp. Diff	13	$2^{119.8}$CPs	2^{146}	2^{120}	[17]
	Improbable	14	$2^{127.0}$CPs	$2^{183.2}$	$2^{127.0}$	[16]
	Multidim. ZC	**14**	$2^{127.5}$**KPs**	$2^{180.2}$	2^{115}	Sect. 5.3
256	Imp. Diff	14	$2^{112.3}$CPs	2^{220}	2^{117}	[18]
	Imp. Diff	14	$2^{117.0}$CPs	2^{236}	2^{121}	[18]
	Imp. Diff	14	$2^{109.0}$CPs	2^{244}	2^{113}	[18]
	Imp. Diff	14	$2^{109.0}$CPs	2^{236}	2^{113}	[18]
	Integral	14	2^{113}CPs	$2^{244.5}$	N/A	[10]
	Imp. Diff	14	$2^{120.3}$CPs	2^{212}	2^{121}	[17]
	Improbable	15	$2^{127.4}$CPs	$2^{247.5}$	$2^{127.4}$	[16]
	Multidim. ZC	**15**	$2^{127.5}$**KPs**	$2^{244.2}$	2^{115}	Sect. 5.4

CPs: Chosen Plaintexts, KPs: Known Plaintexts

memory complexities, while keeping the time and data complexities virtually unchanged. The results are given in Sect. 5 and are outlined in Table 2.

Organization of the Paper. The remainder of this paper is organized as follows. Section 2 recalls the techniques of zero-correlation linear cryptanalysis. Section 3 describes how to use Fast Fourier Transform in zero-correlation linear cryptanalysis. Section 4 derives the zero-correlation linear cryptanalysis with FFT of 11-round Camellia-128 and 12-round Camellia-192. Section 5 reports the multidimensional zero-correlation linear cryptanalysis of 14-round CLEFIA-192 and 15-round CLEFIA-256. We conclude in Section 6.

2 Preliminaries

In this section, we briefly recall what zero-correlation linear approximations are (Subsect. 2.1) and how they can be used to build distinguishers for block ciphers with multiple zero-correlation approximations (Subsect. 2.2) and a multidimensional approach (Subsect. 2.3). This summarizes the state-of-the-art of zero-correlation cryptanalysis.

2.1 Basics of Zero-Correlation Linear Cryptanalysis

Consider an n-bit block cipher f_K with key K. Let P denote a plaintext which is mapped to a ciphertext C under key K, $C = f_K(P)$ [2]. If Γ_P and Γ_C are nonzero plaintext and ciphertext linear masks of n bits each, we denote by $\Gamma_P \rightarrow \Gamma_C$ the linear approximation $\Gamma_P^T \cdot P \oplus \Gamma_C^T \cdot C = 0$. Here, $\Gamma_A^T \cdot A$ denotes the multiplication of the transposed bit vector Γ_A by a column bit vector A over $\mathbb{F}_2$. The linear approximation $\Gamma_P \to \Gamma_C$ has probability

$$p_{\Gamma_P,\Gamma_C} = \Pr_{P \in \mathbb{F}_2^n}\{\Gamma_P^T \cdot P \oplus \Gamma_C^T \cdot C = 0\}.$$

The value $c_{\Gamma_P,\Gamma_C} = 2p_{\Gamma_P,\Gamma_C} - 1$ is called the *correlation* of linear approximation $\Gamma_P \to \Gamma_C$. Note that $p_{\Gamma_P,\Gamma_C} = 1/2$ is equivalent to *zero correlation* $c_{\Gamma_P,\Gamma_C} = 0$.

Given a distinguisher of zero-correlation linear approximation(s) over a part of the cipher (detailed upon in the next two subsections), the basic key recovery can be done with a technique similar to that of Matsui's Algorithm 2 [14], partially encrypting/decrypting from the plantext/ciphertext up to the boundaries of the property. This is the key recovery approach used in all zero-correlation attacks so far. In this paper, we aim to improve upon this by using an FFT technique to reduce the computational complexity of attacks.

2.2 Zero-Correlation Linear Cryptanalysis with Multiple Linear Approximations

Let the number of available zero-correlation linear approximations for an n-bit block cipher be denoted by ℓ [3]. Let the number of required known plaintexts be N. For each of the ℓ given linear approximations, the adversary computes the number T_i of times that linear approximation i is fulfilled on N plaintexts and ciphertexts, $i \in \{1, \ldots, \ell\}$. Each T_i suggests an empirical correlation value $\hat{c}_i = 2\frac{T_i}{N} - 1$. Then, the adversary evaluates the statistic:

$$\sum_{i=1}^{\ell} \hat{c}_i^2 = \sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2.$$

Under a statistical independency assumption, the value $\sum_{i=1}^{\ell} \hat{c}_i^2$ for the right key approximately follows a normal distribution with mean $\mu_0 = \frac{\ell}{N}$ and standard deviation $\sigma_0 = \frac{\sqrt{2\ell}}{N}$ while for the wrong key the distribution is approximately a normal distribution with mean $\mu_1 = \frac{\ell}{N} + \frac{\ell}{2^n}$ and standard deviation $\sigma_1 = \frac{\sqrt{2\ell}}{N} + \frac{\sqrt{2\ell}}{2^n}$.

If we denote the probability of false positives and the probability of false negatives to distinguish between a wrong key and a right key as β_1 and β_0, respectively, and we consider the decision threshold $\tau = \mu_0 + \sigma_0 z_{1-\beta_0} = \mu_1 - \sigma_1 z_{1-\beta_1}$ ($z_{1-\beta_0}$ and $z_{1-\beta_1}$ are the quantiles of the standard normal distribution), then the number of known plaintexts N should be approximately:

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

2.3 Multidimensional Zero-Correlation Linear Cryptanalysis

Now we treat the zero-correlation linear approximations available as a linear space spanned by m base zero-correlation linear approximations such that all $\ell = 2^m - 1$ non-zero linear combinations of them have zero correlation [4]. For each of the 2^m data values $z \in \mathbb{F}_2^m$, the attacker initializes a counter $V[z]$, $z = 0, 1, 2, \ldots, 2^m - 1$, to value zero. Then, for each distinct plaintext, the attacker computes the corresponding data value in $\mathbb{F}_2^m$ by evaluating the m basis linear approximations and increments the counter $V[z]$ of this data value by one. Then the attacker computes the statistic T:

$$T = \sum_{i=0}^{2^m-1} \frac{(V[z] - N2^{-m})^2}{N2^{-m}(1 - 2^{-m})}.$$

The statistic T for the right key guess follows a χ^2-distribution with mean $\mu_0 = (\ell - 1)\frac{2^n - N}{2^n - 1}$ and variance $\sigma_0^2 = 2(\ell - 1)\left(\frac{2^n - N}{2^n - 1}\right)^2$, while for the wrong key guess it follows a χ^2-distribution with mean $\mu_1 = \ell - 1$ and variance $\sigma_1^2 = 2(\ell - 1)$.

If we denote the probability of false positives and the probability of false negatives to distinguish between a wrong key and a right key as β_1 and β_0, respectively, and we consider the decision threshold $\tau = \mu_0 + \sigma_0 z_{1-\beta_0} = \mu_1 - \sigma_1 z_{1-\beta_1}$, then the number of known plaintexts N should be about

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

Note that in both (1) and (2), the number of approximations used is the same and equals ℓ. While in the first case we take those individually, the multidimensional treatment considers them as a linear space spanned by m base approximations.

3 Fast Fourier Transform for Zero Correlation

In this section, we describe an FFT-based technique of computational complexity reduction for zero-correlation cryptanalysis. It relies on eliminating the redundant computations from the partial encryption/decryption in the course of zero-correlation linear cryptanalysis. Let $\chi_P \rightarrow \chi_D$ be the linear approximation for the first $R - 1$ rounds of an R-round block cipher f_K.

After partial decryption of the last round, the linear approximation to be evaluated becomes: $\chi_P^T \cdot P \oplus \chi_D^T \cdot S^{-1}(C \oplus K)$, where $S^{-1}(\cdot)$ represents a partial decryption of the last round for the k *bits* of C and K that influence the value of $\chi_D^T \cdot D$.

We define the $2^k \times 2^k$ matrix M as follows:

$$M(C, K) = (-1)^{\chi_D^T \cdot S^{-1}(C \oplus K)}, \text{ for all } C, K \in \{0, \ldots, 2^k - 1\}.$$

Then, the bias of the linear approximation can be evaluated as the matrix vector product $M \cdot x$. As shown in [7], the matrix M has a level-circulant structure and, consequently, this matrix-vector product can be computed efficiently using the Fast Walsh-Hadamard Transform (equivalent to a k-dimensional Fast Fourier Transform) with $\mathcal{O}(3k \cdot 2^k)$ time complexity. The level-circulant structure results from the XOR between the ciphertext and the key guess. Therefore, the matrix can be expressed as a function of $C \oplus K$. The detail of computing matrix-vector product with FFT is shown in Appendix A of the full version of this paper [5].

The objective of using FFT is to compute the correlation for different subkey guesses with matrix-vector multiplications. The key recovery part in zero-correlation linear cryptanalysis can be done with the similar method utilized by Matsui's Algorithm 2 [14], as shown in [3]. Since the zero correlation attack with multiple linear approximations computes the statistic which reveals correlation directly, we can use the FFT speed-up to improve the computational complexity as described above.

4 Zero-Correlation Cryptanalysis of Camellia with FFT

Camellia is a block cipher jointly proposed by Mitsubishi and NTT in 2000 [1] which has been approved for use by ISO/IEC. It features the basic Feistel structure. The block size is 128 bits and the key size is variable. The number of rounds depends on the key size, i.e., 18 rounds for 128-bit key and 24 rounds for 192/256-bit key. Every six rounds, a logical keyed transformation layer FL/FL^{-1} is applied and the round function uses a SPN structure, including the XOR operation with the round subkey, the nonlinear transformation consisting of eight parallel S-boxes (8×8) and the linear permutation P. The cipher also uses input and output key whitening. Encryption process and key schedule are illustrated in Appendix B of the full version of this paper [5].

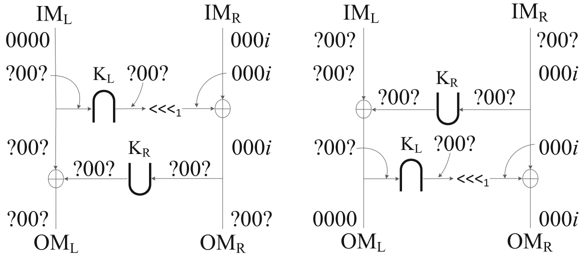
4.1 Zero-Correlation Linear Approximations for 7-Round Camellia

In this subsection, some zero-correlation linear approximations for 7-round Camellia with FL/FL^{-1} are derived. First, we will introduce some properties for FL/FL^{-1} of Camellia.

Property 1. If the input mask of FL is $IM = (0|0|0|0|0|0|0|i)$, then the output mask of FL is $OM = (?|0|0|?|?|0|0|?)$, where '?' is an unknown value, see Fig. 1(a).

Property 2. For the output mask of FL^{-1} is $OM = (0|0|0|0|0|0|0|i)$, then the input mask of FL^{-1} is $IM = (?|0|0|?|?|0|0|?)$, where '?' is an unknown value, see Fig. 1(b).

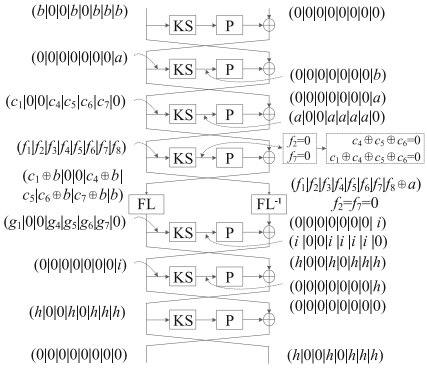
With these properties, we can derive zero-correlation linear approximations for 7-round Camellia.



(a) Property of FL

(b) Property of FL^{-1}

Fig. 1. Property of FL/FL^{-1}



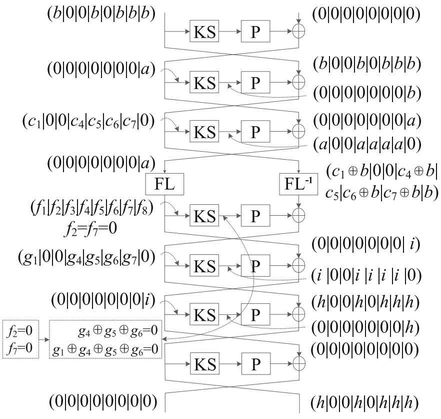


Fig. 2. 4 + 3 rounds

Fig. 3. 3 + 4 rounds

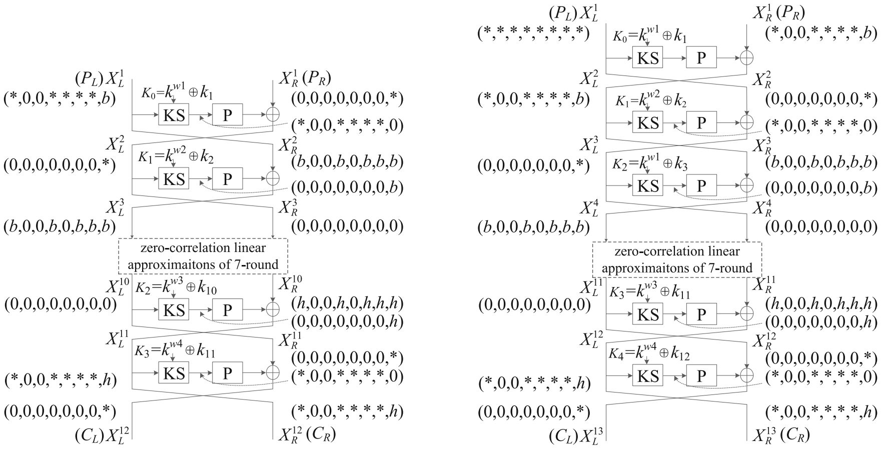
Property 3. For 7-round Camellia consisting of $(F|F|F|F|FL/FL^{-1}|F|F|F)$ as in Fig. 2 or $(F|F|F|FL/FL^{-1}|F|F|F|F)$ as in Fig. 3, if the input mask of the first round is $(b|0|0|b|0|b|b|b, 0|0|0|0|0|0|0|0)$ and the output mask of the last round is $(0|0|0|0|0|0|0|0, h|0|0|h|0|h|h|h)$, then the correlation of the linear approximations is zero, where $b, h \in \mathbb{F}_2^8, b \neq 0, h \neq 0$.

The proofs of Property 1, Property 2 and Property 3 are given in Appendix C of the full version of this paper [5].

4.2 Key Recovery for 11-Round Camellia-128

Using the FFT technique, we can attack 11-round Camellia-128 with FL/FL^{-1} and whitening key starting from the first round by placing the zero-correlation linear approximations of 7-round (4 + 3) Camellia in rounds 3–9 as demonstrated in Fig. 3. This is clarified in Fig. 4(a). Note that in Fig. 4(a), the byte values to be computed are denoted as '$*$' while the bytes denoted as '0' do not require computation.

In the following, we will use some notations. $P^{i_1,i_2,\cdots}$, $C^{i_1,i_2,\cdots}$ and $K^{i_1,i_2,\cdots}$ denote the concatenation of i_1-th, i_2-th,... bytes of the plaintext word, ciphertext word or subkey word respectively. S^j denotes the output of the j-th S-box, F_r denotes the round function for the r-th round and F_r^l is a function and it computes the l-th output byte of the round function for the r-th round. We denote $K_0 = k^{w1} \oplus k_1$, $K_1 = k^{w2} \oplus k_2$, $K_2 = k^{w3} \oplus k_{10}$, and $K_3 = k^{w4} \oplus k_{11}$, where k_1, k_2, k_{10} and k_{11} are 64-bit subkeys for round 1, 2, 10 and 11, respectively, and $k^{wi}, 1 \leq i \leq 4$ is the 64-bit whitening subkey.



(a) Attack on 11-round Camellia-128

(b) Attack on 12-round Camellia-192

Fig. 4. Attacks on 11-round Camellia-128 and 12-round Camellia-192

In our attack, we guess the subkey and evaluate the linear approximation $(\mathbf{b}|0|0|\mathbf{b}|0|\mathbf{b}|\mathbf{b}|\mathbf{b}) \cdot X_L^3 \oplus (\mathbf{h}|0|0|\mathbf{h}|0|\mathbf{h}|\mathbf{h}|\mathbf{h}) \cdot X_R^{10} = 0$ with

$$\begin{aligned} u = {} & \mathbf{b}^T \cdot P_L^8 \oplus \mathbf{h}^T \cdot C_R^8 \oplus \alpha^T \cdot P_L^{1,4,6,7} \oplus \beta^T \cdot C_R^{1,4,6,7} \\ & \oplus \mathbf{b}^T \cdot S^8[P_R^8 \oplus K_1^8 \oplus F_1^8(P_L^{1,4,5,6,7} \oplus K_0^{1,4,5,6,7})] \\ & \oplus \mathbf{h}^T \cdot S^8[C_L^8 \oplus K_2^8 \oplus F_{11}^8(C_R^{1,4,5,6,7} \oplus K_3^{1,4,5,6,7})] = 0, \end{aligned}$$

where $\alpha = (\mathbf{b}, \mathbf{b}, \mathbf{b}, \mathbf{b})$, $\beta = (\mathbf{h}, \mathbf{h}, \mathbf{h}, \mathbf{h})$, $\mathbf{b}$ and $\mathbf{h}$ are non-zero bytes. In order to take the full advantage of the FFT technique to reduce the time complexity, we transform u to v by XORing $\alpha^T \cdot K_0^{1,4,6,7} \oplus \beta^T \cdot K_3^{1,4,6,7}$:

$$\begin{aligned} v = {} & \mathbf{b}^T \cdot P_L^8 \oplus \mathbf{h}^T \cdot C_R^8 \oplus \alpha^T \cdot (P_L^{1,4,6,7} \oplus K_0^{1,4,6,7}) \oplus \beta^T \cdot (C_R^{1,4,6,7} \oplus K_3^{1,4,6,7} \\ & \oplus \mathbf{b}^T \cdot S^8[P_R^8 \oplus K_1^8 \oplus F_1^8(P_L^{1,4,5,6,7} \oplus K_0^{1,4,5,6,7})] \\ & \oplus \mathbf{h}^T \cdot S^8[C_L^8 \oplus K_2^8 \oplus F_{11}^8(C_R^{1,4,5,6,7} \oplus K_3^{1,4,5,6,7})]. \end{aligned} \tag{3}$$

Obviously, the absolute of correlation of the linear approximation $u = 0$ equals to that of the linear approximation $v = 0$, so our attack is equivalent to evaluating the correlation of the linear approximation $v = 0$. As described in Sect. 3, the correlation of the linear approximation $v = 0$ can be evaluated as the matrix vector product where the matrix is:

$$M(P_L^{1,4,5,6,7}|P_R^8|C_L^8|C_R^{1,4,5,6,7}, K_0^{1,4,5,6,7}|K_1^8|K_2^8|K_3^{1,4,5,6,7}) = (-1)^v. \quad (4)$$

To reduce the time complexity, we choose 2^{14} linear approximations where $\mathbf{h}$ takes all possible non-zero values while $\mathbf{b}$ only takes all non-zero values for the six least significant bits and zero value for the two most significant bits. Then the attack is performed as follows:

1. Allocate the vector of counters C_κ of the experimental correlation for every subkey candidate $\kappa = (K_0^{1,4,5,6,7}|K_1^8|K_2^8|K_3^{1,4,5,6,7})$.
2. For each of the 2^{110} values of $i = (P_L^{1,4,5,6,7}|P_L^8[1,2,3,4,5,6]|P_R^8|C_L^8|C_R^{1,4,5,6,7,8})$, define a vector of 2^{110} counters $\mathbf{x}$, where $P_L^8[1,2,3,4,5,6]$ is the six least significant bits of P_L^8.
3. For each of N plaintext-ciphertext pairs, extract the 110-bit value
$$i = (P_L^{1,4,5,6,7}|P_L^8[1,2,3,4,5,6]|P_R^8|C_L^8|C_R^{1,4,5,6,7,8})$$
and increment the counter x_i according to the value of i.
4. For each of the 2^{14} linear approximations
   (a) Perform the data counting phase
      i. For each of the 2^{96} values of $j = (P_L^{1,4,5,6,7}|P_R^8|C_L^8|C_R^{1,4,5,6,7})$, define a vector of 2^{96} counters $\mathbf{y}$.
      ii. For each of the 2^{110} values of $i = (P_L^{1,4,5,6,7}|P_L^8[1,2,3,4,5,6]|P_R^8|C_L^8|C_R^{1,4,5,6,7,8})$, extract 96-bit value $j = (P_L^{1,4,5,6,7}|P_R^8|C_L^8|C_R^{1,4,5,6,7})$ and add x_i to or subtract x_i from the counter y_j according to the parity of $\mathbf{b}^T \cdot P_L^8 \oplus \mathbf{h}^T \cdot C_R^8$.
   (b) Perform the key counting phase
      i. Compute the first column of M using (3) and (4). As M is a 96-level circulant matrix, this information is sufficient to define M completely (requires 2^{96} operations).
      ii. Evaluate the vector $\epsilon = M \cdot \mathbf{y}$ (requires $3 \cdot 96 \cdot 2^{96}$ operations).
      iii. Let $C = C + (\epsilon/N)^2$.
5. If $C_\kappa < \tau$, then the corresponding κ is a possible subkey candidate and all master keys are tested exhaustively.

After Step 4, we obtain 2^{96} counters C_κ which are the sum of squares of correlations for 2^{14} linear approximations under each κ. The correct subkey is then selected from the candidates with C_κ less than the threshold $\tau = \sigma_0 \cdot z_{1-\beta_0} + \mu_0 = \frac{\sqrt{2\ell}}{N} \cdot z_{1-\beta_0} + \frac{\ell}{N}$.

If we set $\beta_0 = 2^{-2.7}$ and $\beta_1 = 2^{-96}$, we get $z_{1-\beta_0} \approx 1$ and $z_{1-\beta_1} \approx 11.3$. Since the block size $n = 128$ and we have $\ell = 2^{14}$ linear approximations, according to Eq. (1) the number of known plaintext-ciphertext pairs N should be about $2^{125.3}$.

In Step 5, only about $2^{96} \cdot 2^{-96} = 1$ guess is expected to survive for the 96-bit target subkey. According to the key schedule of Camellia (e.g. outlined in Appendix B of the full version of this paper [5]), the recovered 96-bit subkey $K_0^{1,4,5,6,7}$, K_1^8, K_2^8 and $K_3^{1,4,5,6,7}$ can be expressed in k_A and k_L as follows,

$$\begin{aligned}
K_0^{1,4,5,6,7} &= [k^{w1} \oplus k_1]^{1,4,5,6,7} &&= [(k_L)_L \oplus (k_A)_L]^{1,4,5,6,7}, \\
K_1^8 &= [k^{w2} \oplus k_2]^8 &&= [(k_L)_R \oplus (k_A)_R]^8, \\
K_2^8 &= [k^{w3} \oplus k_{10}]^8 &&= [(k_A \lll 111)_L \oplus (k_L \lll 60)_R]^8, \\
K_3^{1,4,5,6,7} &= [k^{w4} \oplus k_{11}]^{1,4,5,6,7} &&= [(k_A \lll 111)_R \oplus (k_A \lll 60)_L]^{1,4,5,6,7}.
\end{aligned} \tag{5}$$

One can see that $K_3^{1,4,5,6,7}$ is only related to 61 bits of k_A. So we first guess these 61 bits of k_A and compute $K_3^{1,4,5,6,7}$. Then only about $2^{61} \cdot 2^{-40} = 2^{21}$ values for 61-bit k_A will survive. Second, we guess the other 67 bits of k_A. Then the master key k_L could be computed with four 1-round Camellia encryptions using (6) as proposed in [13]:

$$\begin{aligned}
k_L^R &= F_{C_2}^{-1}(k_A^L \oplus F_{C_4}(k_A^R)) \oplus k_A^R \oplus F_{C_3}(k_A^L \oplus F_{C_4}(k_A^R)), \\
k_L^L &= F_{C_1}^{-1}(k_A^R \oplus F_{C_3}(k_A^L \oplus F_{C_4}(k_A^R))),
\end{aligned} \tag{6}$$

where $C_i, 1 \leq i \leq 4$ is the constant value used in the key schedule. The complexity of this procedure is about $2^{21} \cdot 2^{67} \cdot \frac{4}{11} \approx 2^{86.5}$ 11-round Camellia encryptions.

The complexities for Step 3, Step 4(a), Step 4(b) and Step 5 are $2^{125.3}$ memory accesses, 2^{124} memory accesses, $2^{14} \cdot 4 \cdot 96 \cdot 2^{96} = 2^{118.6}$ 11-round encryptions, $2^{86.5}$ 11-round encryptions, respectively. If we assume that one time of memory access is equivalent to one 11-round Camellia encryption, then the total time complexity is about $2^{125.8}$ encryptions. The memory requirements are about 2^{112} bytes.

All in all, the data complexity is about $2^{125.3}$ known plaintexts, the time complexity is about $2^{125.8}$ encryptions and the memory requirements are 2^{112} bytes.

4.3 Key Recovery for 12-Round Camellia-192

Now we will use the 7-round zero-correlation linear approximations of type (3+4) as given in Fig. 3 to attack 12-round Camellia-192 starting from the first round. By placing these 7-round zero-correlation linear approximations in rounds 4 to 10, we can attack Camellia-192 from round 1 to round 12. This is illustrated in Fig. 4(b).

First, we guess the 64-bit subkey of the first round K_0 and then we proceed with the steps similar as those in the attack on 11-round Camellia-128. Hence, we have to guess 160-bit subkey:

$$K_0^{1,2,3,4,5,6,7,8} = [k^{w1} \oplus k_1]^{1,2,3,4,5,6,7,8} = [(k_L)_L \oplus (k_B)_L]^{1,2,3,4,5,6,7,8}, \tag{7}$$

$$K_1^{1,4,5,6,7} = [k^{w2} \oplus k_2]^{1,4,5,6,7} = [(k_L)_R \oplus (k_B)_R]^{1,4,5,6,7}, \tag{8}$$

$$K_2^8 = [k^{w1} \oplus k_3]^8 = [(k_L)_L \oplus (k_R \lll 15)_L]^8, \tag{9}$$

$$K_3^8 = [k^{w3} \oplus k_{11}]^8 = [(k_B \lll 111)_L \oplus (k_A \lll 45)_L]^8, \tag{10}$$

$$K_4^{1,4,5,6,7} = [k^{w4} \oplus k_{12}]^{1,4,5,6,7} = [(k_B \lll 111)_R \oplus (k_A \lll 45)_R]^{1,4,5,6,7}. \tag{11}$$

Note that in this attack we set $\beta_0 = 2^{-2.7}$ and $\beta_1 = 2^{-160}$, we get $z_{1-\beta_0} \approx 1$ and $z_{1-\beta_1} \approx 14.7$. Since the block size $n = 128$ and we have $\ell = 2^{14}$ linear approximations, then N should be about $\approx 2^{125.7}$ from (1). Similar to the attack on 11-round Camellia-128, only about $2^{160} \cdot 2^{-160} = 1$ guess for the 160-bit target subkey is expected to survive. The complexity of these steps is about $2^{64} \cdot 2^{124.8} = 2^{188.8}$ 12-round Camellia encryptions since the attack on 12-round Camellia-192 is basically the same as the attack on 11-round Camellia-128 except that we have to guess the extra 64-bit $K_0^{1,2,3,4,5,6,7,8}$.

To recover the master key consisting of 128-bit k_L and 64-bit $(k_R)_L$, we first guess 128-bit k_B, compute k'_B according to key schedule. We compute the value of $(k_L)_L$ according to (7). Then we get $(k_R \lll 15)_L^8$ with (9), guess 56-bit $(k_R \lll 15)_L^{1,2,3,4,5,6,7}$ and compute $k_A = k'_B \oplus k_R$. Now we get the value of k_A and k_B according to the key schedule. Using (10, 11), we filter out 2^{-48} values of k_A and k_B. After this step, there are about $2^{128} \cdot 2^{56} \cdot 2^{-48} = 2^{136}$ possible values for k_A, k_B and k_R. k_L can be computed with a cost of four 1-round Camellia encryptions for each of 2^{136} values of k_A, k_B and k_R. With (8), we filter out 2^{-40} wrong candidates. Then we have 2^{96} right key candidates at this time. By verifying with one plaintext-ciphertext pair, only the right key will remain. The dominant time complexity of the above procedure lies in the computation of k_A after guessing 128-bit k_B and 56-bit $(k_R \lll 15)_L^{1,2,3,4,5,6,7}$, which is about 2^{184} XORs of two 128-bit values. Compared to $2^{188.8}$ 12-round Camellia-192 encryptions, this time complexity is negligible.

Thus, the data complexity is $2^{125.7}$ known plaintexts, the memory requirements are about 2^{112} bytes, and the time complexity is $2^{188.8}$ encryptions.

5 Multidimensional Zero-Correlation Cryptanalysis of CLEFIA

CLEFIA is a block cipher proposed in 2007 by Sony Corporation [15] and has been adopted as one of the ISO/IEC international standards in lightweight cryptography. The block size is 128-bit and the key size could be 128, 192 or 256 bits. Accordingly, they are denoted as CLEFIA-128, CLEFIA-192 and CLEFIA-256 and the number of rounds for them are 18, 22 and 26, respectively. CLEFIA employs a four-branch generalized Feistel structure with two parallel F functions (F_0, F_1). The 128-bit ciphertext $(C_0|C_1|C_2|C_3)$ is generated from 128-bit plaintext $(P_0|P_1|P_2|P_3)$ along with $2r$ 32-bit subkey keys $(RK_0, \ldots, RK_{2r-1})$ and four 32-bit whitening keys (WK_0, WK_1, WK_2, WK_3), where r is the total round number. Here we denote a 128-bit value as concatenation of four 32-bit words. The encryption process and key schedule of CLEFIA are shown in Appendix D of the full version of this paper [5].

There are two types of round functions consisting of subkey XOR, S-boxes and the linear transformation, where the linear transformations for them are defined as M_0 and M_1, respectively:

$$M_0 = \begin{pmatrix} 0x1 & 0x2 & 0x4 & 0x6 \\ 0x2 & 0x1 & 0x6 & 0x4 \\ 0x4 & 0x6 & 0x1 & 0x2 \\ 0x6 & 0x4 & 0x2 & 0x1 \end{pmatrix} \text{ and } M_1 = \begin{pmatrix} 0x1 & 0x8 & 0x2 & 0xa \\ 0x8 & 0x1 & 0xa & 0x2 \\ 0x2 & 0xa & 0x1 & 0x8 \\ 0xa & 0x2 & 0x8 & 0x1 \end{pmatrix}.$$

5.1 Zero-Correlation Linear Approximations of 9-Round CLEFIA

In [2], zero-correlation linear approximations of 9-round CLEFIA have been given. If the input mask is $(\mathbf{a}, \mathbf{0}, \mathbf{0}, \mathbf{0})$ and the output mask is $(\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{a})$, then the correlation of the linear approximations is zero. The details of the zero-correlation linear approximations of 9-round CLEFIA are shown in Fig. 5.

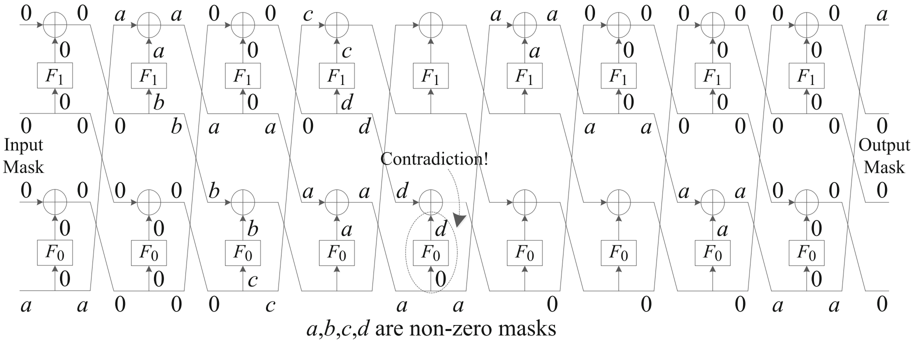


Fig. 5. Zero-correlation linear approximations of 9-Round CLEFIA

5.2 Multidimensional Zero-Correlation Cryptanalysis of 14-Round CLEFIA-192 and 15-Round CLEFIA-256

For the zero-correlation linear approximations of 9-round CLEFIA $(\mathbf{a}, \mathbf{0}, \mathbf{0}, \mathbf{0}) \longrightarrow 9r(\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{a})$, if we take all non-zero values for $\mathbf{a}$, then there are so many guessed subkey bits involved in the key recovery process that the time complexity will be greater than exhaustive search. Therefore, in order to reduce the number of guessed subkey bits, we only use the linear approximations where $\mathbf{a}$ satisfies the following condition:

$$(x,0,0,0),\ (0,x,0,0),\ (0,0,x,0) \text{ or } (0,0,0,x) \longrightarrow M_1\mathbf{a}, x \in \mathbb{F}_2^8, x \neq 0, \mathbf{a} \in \mathbb{F}_2^{32}, \mathbf{a} \neq 0,$$
$$(y_0, y_1, y_2, y_3) \longrightarrow M_0\mathbf{a}, y_i \in \mathbb{F}_2^8, 0 \leq i \leq 3, y_i \neq 0.$$

We will use the above four groups of $\mathbf{a}$ in our attack and there are 255 such linear approximations for each group discovered in our test. In the following, we use $\mathbf{a}_g, 0 \leq g \leq 3$ to denote the four groups where only the g-th byte's input mask of M_1 is nonzero in $\mathbf{a}_g$, e.g. $(x, 0, 0, 0) \in \mathbf{a}_0$ and $(0, 0, x, 0) \in \mathbf{a}_2$. In this way, if the output mask of the round function F_1 is $\mathbf{a}$, then the input mask of the linear

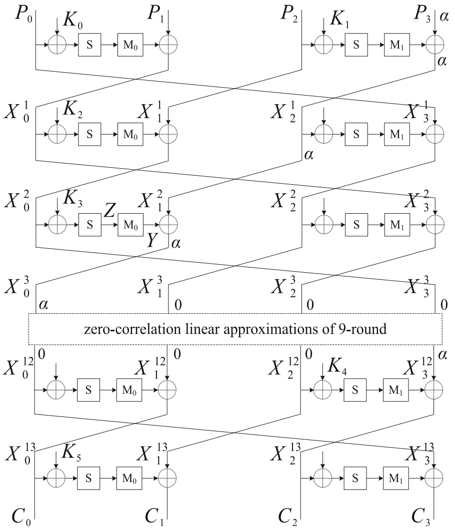


Fig. 6. Attack on 14-round CLEFIA-192

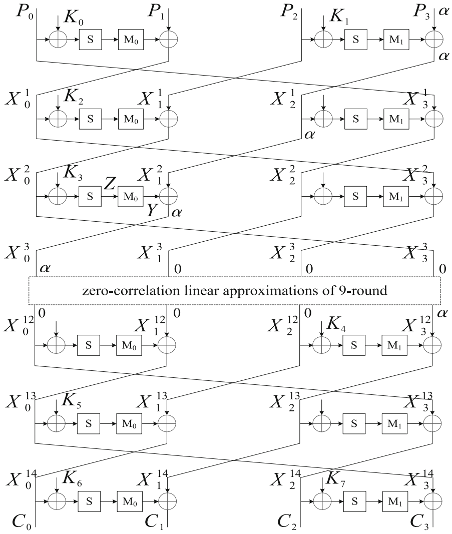


Fig. 7. Attack on 15-round CLEFIA-256

transformation M_1 of this round function is $(x, 0, 0, 0)$, $(0, x, 0, 0)$, $(0, 0, x, 0)$ or $(0, 0, 0, x)$. In this way, there is only one active S-box in F_1 round function in the 1st and 13th rounds, only one subkey byte is required to be guessed instead of four subkey bytes. Four groups of $\mathbf{a}_g$ will be used one by one to sieve wrong subkeys. The right subkey candidates are those survived after the filteration by four groups of $\mathbf{a}$.

5.3 Key Recovery for 14-Round CLEFIA-192

We put the zero-correlation linear approximations of 9-round CLEFIA in rounds 4–12 and attack 14-round CLEFIA-192 starting from the first round, see Fig. 6.

Assume that N known plaintexts are used, the partial encryption and decryption using the partial sum technique are proceeded as in Table 3. Note that X_j^r denotes the j-th branch of the r-th round, the number in square bracket denotes the byte of a 32-bit word, e.g. $P_2[g], 0 \leq g \leq 3$ is the g-th byte of 32-bit P_2. Y and Z are the intermediate states in the third round shown in Fig. 6. In Table 3, the second column stands for the subkey bytes that have to be guessed in each step, the third column denotes the time complexity of corresponding step measured in 1/4 round encryption. In each step, we save the values of the intermediate state $x_{i,g}, 1 \leq i \leq 7, 0 \leq g \leq 3$, during the encryption and decryption process and these are shown in column "Computed States". For each possible value of $x_{i,g}$, the counter (partial sum) $V_{i,g}[x_{i,g}]$ will record how many plaintext-ciphertext pairs can produce the corresponding intermediate state $x_{i,g}$. The counter size for each $x_{i,g}$ is shown in the last column.

Table 3. Partial encryption and decryption on 14-round CLEFIA-192

Step	Guess	Complexity	Computed states	Counter-size
I	K_5	$4 \cdot N \cdot 2^{32}$	$x_{1,g} = (P_0 \mid P_1 \mid P_2 \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{1,g} - 2^{112}$
II	K_0	$4 \cdot 2^{112} \cdot 2^{64}$	$x_{2,g} = (X_0^1 \mid P_2 \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{2,g} - 2^{80}$
III	K_2	$4 \cdot 2^{80} \cdot 2^{96}$	$x_{3,g} = (X_0^2 \mid P_2[g] \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{3,g} - 2^{56}$
IV	$K_3[0]$	$4 \cdot 2^{56} \cdot 2^{104}$	$x_{4,g} = (X_0^2[1,2,3] \mid Z[0] \mid P_2[g] \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{4,g} - 2^{56}$
V	$K_3[1]$	$4 \cdot 2^{56} \cdot 2^{112}$	$x_{5,g} = (X_0^2[2,3] \mid Z[1,0] \mid P_2[g] \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{5,g} - 2^{56}$
VI	$K_3[2]$	$4 \cdot 2^{56} \cdot 2^{120}$	$x_{6,g} = (X_0^2[3] \mid Z[0,1,2] \mid P_2[g] \mid (M_1^{-1}(P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{6,g} - 2^{56}$
VII	$K_3[3]$	$4 \cdot 2^{56} \cdot 2^{128}$	$x_{7,g} = (P_2[g] \mid (M_1^{-1}(Y \oplus P_3 \oplus C_2))[g] \mid X_1^{13}[g])$	$V_{7,g} - 2^{24}$

Since we are going to use four groups $\mathbf{a}_g, 0 \leq g \leq 3$, each step in Table 3 has to be parallelly proceeded for each $\mathbf{a}_g$. To be more clear, we explain the first two steps in Table 3 in detail. In Step I, we allocate four 16-bit counters $V_{1,g}[x_{1,g}]$ and initialize these counters to zero. We then guess 32-bit K_5 and partially decrypt N ciphertexts to compute $x_{1,g}$, and increment the corresponding counters. In Step II, we allocate four 48-bit counters $V_{2,g}[x_{2,g}]$ and initialize them to zero. We then guess 32-bit K_0 and partially encrypt $x_{1,g}$ to compute $x_{2,g}$ and add the corresponding $V_{1,g}$ to $V_{2,g}$.

Key Recovery. We set $\beta_0 = 2^{-4.6}$ and $\beta_1 = 2^{-48}$, then $z_{1-\beta_0} \approx 1.7, z_{1-\beta_1} = 7.8$. Since $n = 128$ and $\ell = 255$, then according to (2), the data complexity N is about $2^{127.5}$. To recover the master key, we perform the following steps.

(A) Partial encryption and decryption for $2^{127.5}$ plaintext-ciphertext pairs as specified by Step I∼VII in Table 3. After Step VII, we get counters $V_{7,0}[x_{7,0}]$, $V_{7,1}[x_{7,1}]$, $V_{7,2}[x_{7,2}]$ and $V_{7,3}[x_{7,3}]$.

(B) Wrong subkeys filteration with $\mathbf{a}_0$ as specified in Algorithm 1. There are 16 new guessed subkey bits involved in this step, and thus about $2^{128+16} \cdot 2^{-48} = 2^{96}$ values for guessed 144-bit subkey will survive after this step.

(C) Wrong subkeys filteration with $\mathbf{a}_1$ as specified in Algorithm 1. After this step, $2^{96+16} \cdot 2^{-48} = 2^{64}$ values for guessed 160-bit subkey will survive.

(D) Wrong subkeys filteration with $\mathbf{a}_2$ as specified in Algorithm 1. $2^{64+16} \cdot 2^{-48} = 2^{32}$ values for guessed 176-bit subkey are expected to survive after this step.

(E) Wrong subkeys filteration with $\mathbf{a}_3$ as specified in Algorithm 1. Only $2^{32+16} \cdot 2^{-48} = 1$ value for guessed 192-bit subkey is supposed to remain.

(F) According to the key schedule of CLEFIA-192, we can recover the master key from this unique 192-bit subkey.

The dominant time complexity in Step (A) lies in Step VII, which is about $4 \cdot 2^{56} \cdot 2^{128} \cdot \frac{1}{4} \cdot \frac{1}{14} \approx 2^{180.2}$ 14-round CLEFIA-192 encryptions. The time complexity of Step (B) is about $(2^{128+8} \cdot 2^{24} + 2^{128+16} \cdot 2^{16}) \cdot \frac{1}{4} \cdot \frac{1}{14} \approx 2^{155.2}$ 14-round CLEFIA-192 encryptions. The time complexity of Step (C) is about $(2^{96+8} \cdot 2^{24} + 2^{96+16} \cdot 2^{16}) \cdot \frac{1}{4} \cdot \frac{1}{14} \approx 2^{123.2}$ 14-round CLEFIA-192 encryptions. The time complexity of Step (D) and (E) is negligible.

For the time complexity of Step (F), we need to consider the key schedule of CLEFIA-192. The six subkeys guessed, $K_i, 0 \leq i \leq 5$ are RK_0, RK_1, $RK_2 \oplus$

Algorithm 1. Filter out wrong subkeys with $\mathbf{a}_g$

```
Allocate 128-bit counter $V_{8,g}$ for 16-bit $x_{8,g} = ((M_1^{-1}(Y \oplus X_2^1 \oplus C_2))[g]|X_1^{13}[g])$ and initialize to zero
Guess 8-bit $K_1[g]$, compute $x_{8,g}$ with $x_{7,g}$, then $V_{8,g}[x_{8,g}] += V_{7,g}[x_{7,g}]$
Allocate 128-bit counter $V_{9,g}$ for 8-bit $x_{9,g} = ((M_1^{-1}(Y \oplus X_2^1 \oplus X_3^{12}))[g])$ and initialize to zero
Guess 8-bit $K_4[g]$, compute $x_{9,g}$ with $x_{8,g}$, then $V_{9,g}[x_{9,g}] += V_{8,g}[x_{8,g}]$
Allocate 128-bit counter $V_g[z]$ for 8-bit $z$ and initialize to zero
{z is the concatenation of evaluations of 8 basis zero-correlation masks}
Compute $z$ from $x_{9,g}$ with 8 basis zero-correlation masks, then $V_g[z] += V_{9,g}[x_{9,g}]$
Compute $T = N \cdot 2^8 \cdot \sum_{z=0}^{2^8-1} \left(\frac{V_g[z]}{N} - \frac{1}{2^8}\right)^2$
if $T < \tau$ then
    Guessed subkey values are possible right subkey candidates
end if
```

WK_0, RK_4, $RK_{25} \oplus WK_2$ and RK_{26}, respectively. According to the key schedule in Appendix D of the full version of this paper [5], RK_0, RK_1 and RK_{26} is only related with the intermediate key value L. Then after Step (E), we obtained 96-bit L since there is only one value for the 192-bit subkey left. To recover the 192-bit key K from the key schedule, we guess other 160-bit L and compute K with cost equivalent to 20 one-round CLEFIA encryptions. K could then be verified with at most two plaintext-ciphertext pairs. The complexity to recover the master key from the 192-bit subkey we obtained after Step (E) is $2^{160} \cdot \frac{20}{14} + 2^{160} + 2^{160-128} \approx 2^{161.3}$ 14-round CLEFIA-192 encryptions.

All in all, the time complexity of our attack on 14-round CLEFIA-192 is about $2^{180.2}$ 14-round CLEFIA-192 encryptions, the data complexity is $2^{127.5}$ known plaintexts and the memory requirements are about 2^{115} bytes to store the counters in Step I.

5.4 Key Recovery for 15-Round CLEFIA-256

We also place the zero-correlation linear approximations of 9-round CLEFIA in rounds 4 to 12 and attack 15-round CLEFIA-256 starting from the first round, see Fig. 7.

For the attack on 15-round CLEFIA-256, we need to guess 32-bit K_6 and 32-bit K_7 and decrypt N pairs of texts to get $(X_0^{14}, X_1^{14}, X_2^{14}, X_3^{14})$. The remaining procedure is similar as the attack on 14-round CLEFIA-192, where we still set $\beta_0 = 2^{-4.6}$ and $\beta_1 = 2^{-48}$.

The time complexity from Step (A) to Step (E) for the attack on 15-round CLEFIA-256 is about 2^{64} times of the time complexity in the corresponding step for the attack on 14-round CLEFIA-192. So the total complexity for Step (A)$\sim$(E) is about $2^{180.2} \cdot 2^{64} \approx 2^{244.2}$ 15-round CLEFIA-256 encryptions.

For the time complexity of Step (F), the key schedule of CLEFIA-256 should be considered. The guessed eight subkeys, $K_i, 0 \le i \le 7$ are RK_0, RK_1, $RK_2 \oplus WK_0$, RK_4, RK_{25}, $RK_{26} \oplus WK_3$, RK_{28} and RK_{29}, respectively. From the key schedule of Appendix D of the full version of this paper [5], the guessed subkey RK_0, RK_1 and RK_{25} are only related with the intermediate key value L. Then after Step (E), we obtained 2^{64} values for 96-bit L since there are 2^{64} guesses for the 256-bit subkey left. To recover the 256-bit key K, we guess other 160-bit L and compute K with cost equivalent to 20 one-round CLEFIA encryptions. K could then be verified with at most two plaintext-ciphertext pairs. The complexity to recover the master key from the 256-bit subkey we obtained after Step (E) is about $2^{64} \cdot 2^{160} \cdot \frac{20}{15} + 2^{64} \cdot 2^{160} + 2^{64} \cdot 2^{160} \cdot 2^{-128} \approx 2^{185.2}$ 15-round CLEFIA-256 encryptions.

All in all, the time complexity of our attack on 15-round CLEFIA-256 is about $2^{244.2}$ 15-round CLEFIA-256 encryptions, the data complexity is $2^{127.5}$ known plaintexts and the memory requirements are about 2^{115} bytes to store the counters in Step I.

6 Conclusion

In this paper, we use the Discrete Fast Fourier Transform to enhance zero-correlation linear cryptanalysis by a faster key recovery. We improve upon the state-of-the-art cryptanalysis for Camellia and CLEFIA by breaking more rounds for Camellia-128 and Camellia-192 than was possible previously as well as by reducing time and memory complexities for CLEFIA-192 and CLEFIA-256.

It is our hope that the FFT zero correlation cryptanalysis will lead to a reevaluation of security level for further ciphers as well.

Acknowledgments. This work has been supported by the National Basic Research 973 Program of China under Grant No. 2013CB834205, the National Natural Science Foundation of China under Grant Nos. 61133013, 61070244, the Program for New Century Excellent Talents in University of China under Grant No. NCET-13-0350, as well as the Interdisciplinary Research Foundation of Shandong University of China under Grant No. 2012JC018.

References

1. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: *Camellia*: a 128-bit block cipher suitable for multiple platforms - design and analysis. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001)
2. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Crypt. **70**(3), 369–383 (2014)
3. Bogdanov, A., Wang, M.: Zero correlation linear cryptanalysis with reduced data complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer, Heidelberg (2012)
4. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and multidimensional linear distinguishers with correlation zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012)

5. 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. IACR ePrint Archive report (2013)
6. Chen, J., Jia, K., Yu, H., Wang, X.: New impossible differential attacks of reduced-round Camellia-192 and Camellia-256. In: Parampalli, U., Hawkes, P. (eds.) ACISP 2011. LNCS, vol. 6812, pp. 16–33. Springer, Heidelberg (2011)
7. Collard, B., Standaert, F.-X., Quisquater, J.-J.: Improving the time complexity of Matsui's linear cryptanalysis. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 77–88. Springer, Heidelberg (2007)
8. ISO/IEC 18033–3:2005 Information technology – Security techniques – Encryption algrithm – Part 3: Block Ciphers (July 2005)
9. Li, L., Chen, J., Jia, K.: New impossible differential cryptanalysis of reduced-round Camellia. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 26–39. Springer, Heidelberg (2011)
10. 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)
11. Liu, Y., Li, L., Gu, D., Wang, X., Liu, Z., Chen, J., Li, W.: New observations on impossible differential cryptanalysis of reduced-round Camellia. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 90–109. Springer, Heidelberg (2012)
12. Liu, Y., Gu, D., Liu, Z., Li, W.: Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256. J. Syst. Softw. **85**(11), 2451–2458 (2012)
13. Mala, H., Shakiba, M., Dakhilalian, M., Bagherikaram, G.: New results on impossible differential cryptanalysis of reduced–round Camellia–128. In: Jacobson Jr, M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 281–294. Springer, Heidelberg (2009)
14. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
15. 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)
16. Tezcan, C.: The improbable differential attack: cryptanalysis of reduced round CLEFIA. In: Gong, G., Gupta, C.K. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 197–209. Springer, Heidelberg (2010)
17. 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)
18. Tsunoo, Y., Tsujihara, E., Shigeri, M., Suzaki, T., Kawabata, T.: Cryptanalysis of CLEFIA using multiple impossible differentials. ISITA **2008**, 1–6 (2008)
19. Wang, W., Wang, X.: Saturation cryptanalysis of CLEFIA. J. Commun. **29**(10), 88–92 (2008)
20. Zhang, W., Han, J.: Impossible differential analysis of reduced round CLEFIA. In: Yung, M., Liu, P., Lin, D. (eds.) INSCRYPT 2008. LNCS, vol. 5487, pp. 181–191. Springer, Heidelberg (2009)