Improved Zero-Correlation Linear Cryptanalysis of Reduced-round Camellia under Weak Keys

Zhiqiang Liu[1,4,⋆], Bing Sun[2,4,⋆], Qingju Wang[1,4,⋆], Kerem Varici[3,4,⋆], and Dawu Gu[1,⋆]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University
800 Dong Chuan Road, Shanghai, 200240, China
[2] Department of Mathematics and System Science, Science College,
National University of Defense Technology, China
[3] ICTEAM-Crypto Group, Universite catholique de Louvain
1348 Louvain-la-Neuve, Belgium
[4] ESAT/COSIC, KU Leuven and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
ilu_zq@sjtu.edu.cn

Abstract. Camellia is one of the widely used block ciphers, which has been included in the NESSIE block cipher portfolio and selected as a standard by ISO/IEC. In this work, we observe that there exist some interesting properties of the FL/FL^{-1} functions in Camellia. With this observation we derive some weak keys for the cipher, based on which we present the first known 8-round zero-correlation linear distinguisher of Camellia with FL/FL^{-1} layers. This result shows that the FL/FL^{-1} layers inserted in Camellia cannot resist zero-correlation linear cryptanalysis effectively for some weak keys since the currently best zero-correlation linear distinguisher for Camellia without FL/FL^{-1} layers also covers 8 rounds. Moreover, by using the novel distinguisher, we launch key recovery attacks on 13-round Camellia-192 and 14-round Camellia-256 respectively. To our knowledge, these results are the best for Camellia-192 and Camellia-256 with FL/FL^{-1} and whitening layers.

Keywords: Cryptanalysis, Zero-correlation Linear Cryptanalysis, Block Cipher, Camellia

1 Introduction

The block cipher Camellia was jointly proposed by NTT and Mitsubishi in 2000 [1]. It was selected as one of the CRYPTREC e-government recommended ciphers in 2002 [2] and included in the NESSIE block cipher portfolio in 2003 [3]. Later in 2005, it was adopted as the international standard by ISO/IEC [4]. Camellia is a 128-bit block cipher which uses the Feistel structure with key-dependent functions FL/FL^{-1} inserted every six rounds. It supports three different key sizes: 128, 192 and 256, and the number of rounds changes according to the key size, i.e., 18 rounds for 128-bit key size (denoted as Camellia-128) and 24 rounds for 192/256-bit key sizes (denoted as Camellia-192/Camellia-256, respectively).

So far there have been many cryptanalytic results for reduced-round Camellia by using different approaches such as differential and linear cryptanalysis [5], truncated differential cryptanalysis [6, 7], integral attack [8–10], meet-in-the-middle attack [11], collision attack [9, 12], impossible differential cryptanalysis [7, 13–19] and zero-correlation linear cryptanalysis [20]. As a matter of fact, most attacks presented before 2011 excluded the FL/FL^{-1} and whitening layers to ease the cryptanalysis, while recent attacks aimed at reduced-round Camellia with FL/FL^{-1} and/or whitening layers. For example, in [13], several 6-round impossible differentials of Camellia with FL/FL^{-1} layers were proposed, based on which some attacks

⋆ Corresponding authors.

were mounted on 10-round Camellia-192 and 11-round Camellia-256. The authors of [14] introduced a 7-round impossible differential of Camellia including FL/FL^{-1} layers, with which they presented improved attacks on 10-round Camellia-128, 10-round Camellia-192 and 11-round Camellia-256. Liu *et al.* [17] constructed some 7 and 8-round impossible differentials of Camellia with FL/FL^{-1} layers and then attacked 11-round Camellia-128, 12-round Camellia-192 and 13-round Camellia-256. In 2013, Bogdanov *et al.* [20] proposed attacks on 11-round Camellia-128 and 12-round Camellia-192 by using 7-round zero-correlation linear distinguishers of Camellia with FL/FL^{-1} layers and the FFT technique.

Zero-correlation linear attack is one of the recent cryptanalytic methods introduced by Bogdanov and Rijmen [21]. The attack is based on linear approximations with zero correlation, which is different from the traditional linear cryptanalysis where linear characteristics (hulls) with high correlations are used. The idea of zero-correlation linear attack can be considered as the projection of impossible differential cryptanalysis to linear cryptanalysis. To construct a zero-correlation linear distinguisher, one always adopts the miss-in-the-middle techniques as that used in impossible differential cryptanalysis. In [22, 23], Bogdanov *et al.* proposed new models that can decrease the data complexity of zero-correlation linear cryptanalysis. We refer to [20, 22–24] for details of zero-correlation linear cryptanalysis on various block ciphers such as CAST, CLEFIA, HIGHT, Skipjack, TEA and XTEA.

In this paper, we first rewrite the FL/FL^{-1} functions within Camellia in matrix forms, which shows that for given keys, FL/FL^{-1} functions are indeed linear (affine) transformations. Thus the correlations of FL/FL^{-1} functions can only be 0 or ± 1. From this we derive some interesting properties of the FL/FL^{-1} functions. Then following these properties we find some weak keys for the cipher, with which the first known 8-round zero-correlation linear distinguisher of Camellia with FL/FL^{-1} layers is presented. Note that this distinguisher covers the same number of rounds as the best known zero-correlation linear distinguisher for Camellia without FL/FL^{-1} layers. Consequently, our result demonstrates that FL/FL^{-1} layers cannot thwart zero-correlation linear cryptanalysis effectively in the case of some specific weak keys. Furthermore, we apply this new distinguisher to attack 13-round Camellia-192 and 14-round Camellia-256 respectively. Although our attacks require certain conditions for 15 subkey bits, they improve the existing cryptanalytic results on Camellia-192/256 with FL/FL^{-1} and whitening layers which can be seen in Table 1.

The remaining of the paper is organized as follows: In Sec. 2, we give necessary notations, brief description of Camellia and concise explanation of Fast Fourier Transform for zero-correlation linear cryptanalysis. In Sec. 3, we present new properties for FL/FL^{-1} functions, some weak keys for Camellia and an 8-round zero-correlation linear distinguisher for the cipher under these weak keys. Then based on this distinguisher, Sec. 4 demonstrates key recovery attacks on reduced-round Camellia-192/256. Finally, we summarize our paper in Sec. 5.

2 Preliminaries

2.1 Notations

General notations: The following notations are used throughout the paper.
– $\oplus$ denotes bitwise exclusive OR (XOR).
– 0x denotes the hexadecimal notation.

Table 1. Summary of the Attacks on Camellia with FL/FL^{-1} and Whitening Layers

Key Size	Cryptanalysis	Rounds	Data	Time(EN)	Memory(Bytes)	Source
192	Imp. Diff.	10	2^{121} CP	$2^{175.3}$	$2^{155.2}$	[13]
	Imp. Diff.	10	$2^{118.7}$ CP	$2^{130.4}$	2^{135}	[14]
	Imp. Diff.	11^*	$2^{112.64}$CP	$2^{146.54}$	$2^{141.64}$	[17]
	Imp. Diff.	11	$2^{114.64}$CP	2^{184}	$2^{141.64}$	[17]
	Imp. Diff.	12	2^{123}CP	$2^{187.2}$	2^{160}	[17]
	Multidim. Zero-Corr.	12	$2^{125.7}$KP	$2^{188.8}$	$2^{112.0}$	[20]
	Zero-Corr.	$\mathbf{13}^*$	2^{128}KP	$2^{169.83}$	$2^{156.86}$	**Sect. 4.1**
256	Higher-order Diff.	11	2^{93}CP	$2^{255.6}$	2^{98}	[25]
	Imp. Diff.	11	2^{121} CP	$2^{206.8}$	2^{166}	[13]
	Imp. Diff.	11	$2^{119.6}$ CP	$2^{194.5}$	2^{135}	[14]
	Imp. Diff.	12^*	$2^{121.12}$CP	$2^{202.55}$	$2^{142.12}$	[17]
	Imp. Diff.	12	$2^{116.17}$CP	2^{240}	$2^{150.17}$	[17]
	Imp. Diff.	13	2^{123}CP	$2^{251.1}$	2^{208}	[17]
	Zero-Corr.	$\mathbf{14}^*$	2^{128}KP	$2^{234.92}$	$2^{212.86}$	**Sect. 4.2**

CP: Chosen Plaintext; KP: Known Plaintext; EN: Encryptions; *: Weak Key

– $\|$ denotes the concatenation operation.
– $\cdot$ denotes bitwise inner product.
– $\cap, \cup$ denote bitwise AND and OR operations, respectively.
– $\overline{X}$ denotes bitwise complement of X, where $X \in \mathbb{F}_2^n$.
– $X \lll_m$ denotes left rotation of X by m bits.
– $X \ggg_m$ denotes right rotation of X by m bits.
– X_L, X_R denote the left and right halves of X, respectively.

Notations for key recovery attacks (i.e., notations used in Section 4):
– P_j, C_j, K_j denote the j-th bytes of plaintext P, ciphertext C and subkey K respectively, numbered from left to right.
– $P_{\{j_1,j_2\}}, C_{\{j_1,j_2\}}, K_{\{j_1,j_2\}}$ denote $P_{j_1}\|P_{j_2}$, $C_{j_1}\|C_{j_2}$ and $K_{j_1}\|K_{j_2}$ respectively.
– $P[j], C[j], K[j]$ denote the j-th bits of plaintext P, ciphertext C and subkey K respectively, numbered from left to right.
– $P[j_1, j_2], C[j_1, j_2], K[j_1, j_2]$ denote $P[j_1]\|P[j_2]$, $C[j_1]\|C[j_2]$ and $K[j_1]\|K[j_2]$ respectively.

2.2 Fast Fourier Transform for Zero-Correlation Linear Cryptanalysis

We briefly recall the FFT-based technique of computational complexity reduction for zero-correlation linear cryptanalysis which was described in [20]. The objective of this technique is to eliminate the redundant computations from the partial encryption/decryption in the course of zero-correlation linear cryptanalysis.

Let $\Gamma_P \to \Gamma_D$ be a zero-correlation linear distinguisher for the first $r-1$ rounds of an r-round block cipher E_K. After partial decryption of the last round, the linear distinguisher to be evaluated becomes: $\Gamma_P \cdot P \oplus \Gamma_D \cdot f^{-1}(K \oplus C)$, where $f^{-1}(\cdot)$ represents a partial decryption of the last round for the k bits of K and C that influence the value of $\Gamma_D \cdot D$.

Let x denote the plaintext-ciphertext bits involved in the linear distinguisher. Now we define the $2^k \times 2^k$ matrix M as follows:

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

Then the bias of the linear distinguisher can be evaluated as the matrix-vector product MZ, where Z is the vector corresponds to the parity of $\Gamma_P \cdot P$ and the number of occurrences of each possible value of x in all given plaintext-ciphertext pairs. As shown in [26], the matrix M has a level-circulant structure resulting from the XOR between the ciphertext and the key guess, thus this matrix-vector product can be computed efficiently by using the Fast Walsh-Hadamard Transform (equivalent to a k-dimensional Fast Fourier Transform) with about $3k \times 2^k$ arithmetic operations. We refer to [20, 26] for more details of the FFT technique for improving the computational complexity in linear cryptanalysis.

2.3 A Brief Description of Camellia

Camellia [1] is a 128-bit block cipher which adopts the Feistel structure with key-dependent functions FL/FL^{-1} inserted every six rounds. It supports variable key sizes and the number of rounds depends on the key size, i.e., 18 rounds for 128-bit key size and 24 rounds for 192/256-bit key sizes. Moreover, pre-whitening and post-whitening layers are included before the first round and after the last round respectively. Fig. 1 gives a schematic description of Camellia-192/256.

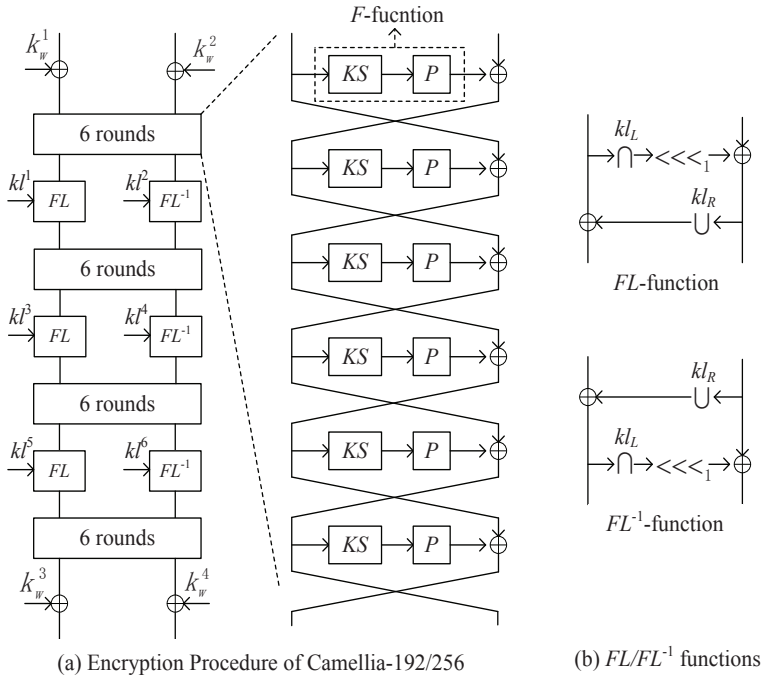


Fig. 1. Schematic description of Camellia-192/256

Let $X_L^i = (X_{L,1}^i, X_{L,2}^i, \ldots, X_{L,8}^i) \in (\mathbb{F}_2^8)^8$, $X_R^i = (X_{R,1}^i, X_{R,2}^i, \ldots, X_{R,8}^i) \in (\mathbb{F}_2^8)^8$ denote the left and right halves of the input for the i-th round of Camellia, respectively. Then the i-th round transformation of Camellia can be described as:

$$\begin{cases} X_L^{i+1} = F(X_L^i, k^i) \oplus X_R^i \\ X_R^{i+1} = X_L^i, \end{cases}$$

where k^i denotes the i-th round key, and the round function F consists of the round key addition, the nonlinear transformation S and the linear transformation P. There are four 8×8 S-boxes S_1, S_2, S_3 and S_4 adopted in S, and each S-box is used twice in the sequence $(S_1, S_2, S_3, S_4, S_2, S_3, S_4, S_1)$. The linear transformation $P : (\mathbb{F}_2^8)^8 \rightarrow (\mathbb{F}_2^8)^8$ and its inverse P^{-1} are defined as follows:

$$
\begin{aligned}
z_1 &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8 & y_1 &= z_2 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8 \\
z_2 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8 & y_2 &= z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8 \\
z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8 & y_3 &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8 \\
z_4 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7 & y_4 &= z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7 \\
z_5 &= y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8 & y_5 &= z_1 \oplus z_2 \oplus z_5 \oplus z_7 \oplus z_8 \\
z_6 &= y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8 & y_6 &= z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8 \\
z_7 &= y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8 & y_7 &= z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7 \\
z_8 &= y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7 & y_8 &= z_1 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8,
\end{aligned}
$$

where $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$ and $(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8)$ are the input and output of P, respectively.

The key schedule algorithm of Camellia-192/256 applies 6-round Feistel structure to derive two 128-bit intermediate variables K_A and K_B from K_L and K_R (See Fig. 2), where K_L, K_R are defined as below:

- For Camellia-192, K_L is set as the left 128-bit value of the master key K, and $K_R = (K_R)_L \| (K_R)_R$, where $(K_R)_L$ is the right 64-bit value of K and $(K_R)_R = \overline{(K_R)_L}$.
- For Camellia-256, the master key K is divided into two 128-bit variables K_L and K_R, i.e., $K = K_L \| K_R$.

All round keys, whitening keys and subkeys used in the FL/FL^{-1} layers can be generated from K_L, K_R, K_A and K_B (See Table 2). We refer to [1] for more details of Camellia.

3 8-round Zero-Correlation Linear Distinguisher of Camellia with FL/FL^{-1} Layers under Weak Keys

3.1 Some Properties of FL^{-1} Function

In this section, we will give some properties of FL^{-1} function, and similar results can be achieved for FL function. We refer to Fig. 1(b) for the definitions of FL/FL^{-1} functions.

Property 1. Let $0 \neq u = (u_L, u_R)$, $v = (v_L, v_R)$ be the input and output masks of the FL^{-1} function respectively, where $u_L, u_R, v_L, v_R \in (\mathbb{F}_2^8)^4$. Let $kl = (kl_L, kl_R)$ be the subkey used in the FL^{-1} function, where $kl_L, kl_R \in (\mathbb{F}_2^8)^4$. Then the correlation of the FL^{-1} function is ± 1 if following conditions are satisfied:

$$
\begin{aligned}
v_R &= u_R \oplus (u_L \cap \overline{kl}_R), \\
v_L &= u_L \oplus ((v_R \ggg_1) \cap kl_L).
\end{aligned}
$$

Otherwise, the correlation is 0.

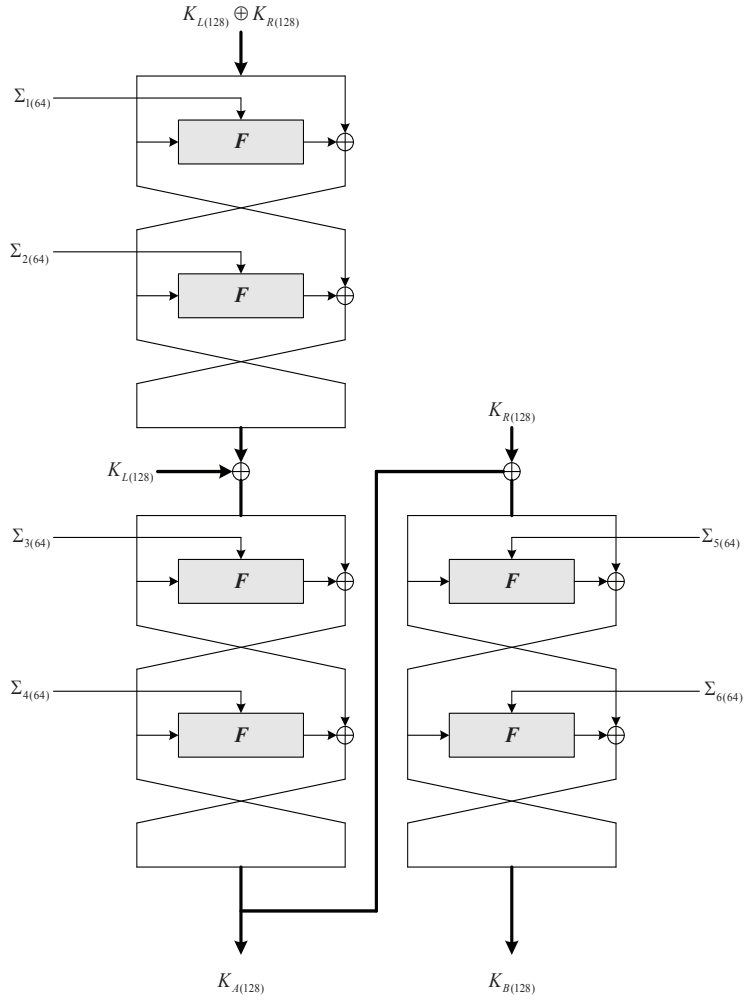


Fig. 2. 6-round Feistel Structure for Generating K_A and K_B

Proof. Let the input and output of FL^{-1} function be

$$I = (I_L, I_R) = (I_L[1], \ldots, I_L[32], I_R[1], \ldots, I_R[32])$$

and

$$O = (O_L, O_R) = (O_L[1], \ldots, O_L[32], O_R[1], \ldots, O_R[32]),$$

respectively. Let $kl_L = (kl_L[1], \ldots, kl_L[32])$, $kl_R = (kl_R[1], \ldots, kl_R[32])$. Since

$$O_L \cap kl_L = \big(O_L[1]\, O_L[2] \cdots O_L[32]\big) \begin{pmatrix} kl_L[1] & 0 & \cdots & 0 \\ 0 & kl_L[2] & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & kl_L[32] \end{pmatrix} \triangleq O_L P_{kl_L}$$

Table 2. Subkeys Used in Camellia-192/256

	subkey	value		subkey	value
Prewhitening	kw^1	$(K_L \lll_0)_L$			
	kw^2	$(K_L \lll_0)_R$			
F(Round 1)	k^1	$(K_B \lll_0)_L$	F(Round 13)	k^{13}	$(K_R \lll_{60})_L$
F(Round 2)	k^2	$(K_B \lll_0)_R$	F(Round 14)	k^{14}	$(K_R \lll_{60})_R$
F(Round 3)	k^3	$(K_R \lll_{15})_L$	F(Round 15)	k^{15}	$(K_B \lll_{60})_L$
F(Round 4)	k^4	$(K_R \lll_{15})_R$	F(Round 16)	k^{16}	$(K_B \lll_{60})_R$
F(Round 5)	k^5	$(K_A \lll_{15})_L$	F(Round 17)	k^{17}	$(K_L \lll_{77})_L$
F(Round 6)	k^6	$(K_A \lll_{15})_R$	F(Round 18)	k^{18}	$(K_L \lll_{77})_R$
FL	kl^1	$(K_R \lll_{30})_L$	FL	kl^5	$(K_A \lll_{77})_L$
FL^{-1}	kl^2	$(K_R \lll_{30})_R$	FL^{-1}	kl^6	$(K_A \lll_{77})_R$
F(Round 7)	k^7	$(K_B \lll_{30})_L$	F(Round 19)	k^{19}	$(K_R \lll_{94})_L$
F(Round 8)	k^8	$(K_B \lll_{30})_R$	F(Round 20)	k^{20}	$(K_R \lll_{94})_R$
F(Round 9)	k^9	$(K_L \lll_{45})_L$	F(Round 21)	k^{21}	$(K_A \lll_{94})_L$
F(Round 10)	k^{10}	$(K_L \lll_{45})_R$	F(Round 22)	k^{22}	$(K_A \lll_{94})_R$
F(Round 11)	k^{11}	$(K_A \lll_{45})_L$	F(Round 23)	k^{23}	$(K_L \lll_{111})_L$
F(Round 12)	k^{12}	$(K_A \lll_{45})_R$	F(Round 24)	k^{24}	$(K_L \lll_{111})_R$
FL	kl^3	$(K_L \lll_{60})_L$	Postwhitening	kw^3	$(K_B \lll_{111})_L$
FL^{-1}	kl^4	$(K_L \lll_{60})_R$		kw^4	$(K_B \lll_{111})_R$

and left rotating a row vector $\gamma \in \mathbb{F}_2^{32}$ by 1 bit can be characterized by

$$\gamma \lll_1 = \gamma \begin{pmatrix} 0\,0\,0 \cdots 0\,1 \\ 1\,0\,0 \cdots 0\,0 \\ 0\,1\,0 \cdots 0\,0 \\ \vdots\,\vdots\,\vdots \cdots \vdots\,\vdots \\ 0\,0\,0 \cdots 1\,0 \end{pmatrix} \triangleq \gamma P_1,$$

therefore,

$$I_R = O_R \oplus ((O_L \cap kl_L) \lll_1) = (O_L(P_{kl_L} P_1)) \oplus O_R.$$

Similarly, since $I_R \cup kl_R = (I_R \cap kl_R) \oplus I_R \oplus kl_R = (I_R \cap \overline{kl}_R) \oplus kl_R$, we have

$$I_L = O_L(E_{32} \oplus P_{kl_L} P_1 P_{\overline{kl}_R}) \oplus O_R P_{\overline{kl}_R} \oplus kl_R,$$

thus

$$(I_L, I_R) = (O_L, O_R) \begin{pmatrix} E_{32} \oplus P_{kl_L} P_1 P_{\overline{kl}_R} & P_{kl_L} P_1 \\ P_{\overline{kl}_R} & E_{32} \end{pmatrix} \oplus (kl_R, \boldsymbol{0}),$$

where E_{32} is the 32×32 identity matrix and $\boldsymbol{0}$ is the 1×32 zero vector.

Notice that $P_{kl_L}^T = P_{kl_L}$ and $P_{kl_R}^T = P_{kl_R}$, accordingly, if the input mask of FL^{-1} is $0 \neq u = (u_L, u_R)$, to make the correlation non-zero (i.e., ± 1), the output mask should be

$$\begin{aligned} (v_L, v_R) &= (u_L, u_R) \begin{pmatrix} E_{32} \oplus P_{kl_L} P_1 P_{\overline{kl}_R} & P_{kl_L} P_1 \\ P_{\overline{kl}_R} & E_{32} \end{pmatrix}^T \\ &= (u_L, u_R) \begin{pmatrix} E_{32} \oplus P_{\overline{kl}_R} P_1^T P_{kl_L} & P_{\overline{kl}_R} \\ P_1^T P_{kl_L} & E_{32} \end{pmatrix}, \end{aligned}$$

which implies

$$v_R = u_R \oplus (u_L P_{\overline{kl}_R}),$$
$$v_L = u_L \oplus v_R P_1^T P_{kl_L},$$

therefore

$$v_R = u_R \oplus (u_L \cap \overline{kl}_R),$$
$$v_L = u_L \oplus ((v_R \ggg_1) \cap kl_L).$$

According to Property 1, we get the following:

Property 2. Let $0 \neq u = (u_L, u_R)$, $v = (v_L, v_R)$ be the input and output masks of the FL^{-1} function as defined in Property 1. Suppose that the correlation of the FL^{-1} function is nonzero (i.e., ± 1), then $u = v$ if and only if

$$0 = u_L \cap \overline{kl}_R,$$
$$0 = (u_R \ggg_1) \cap kl_L.$$

3.2 8-round Zero-Correlation Linear Distinguisher under Weak Keys

By applying miss-in-the-middle technique, we find that

$$\begin{aligned} &((a,a,0,0,a,0,a,a),(0,0,0,0,0,0,0,0)) \\ \rightarrow\ &((0,0,0,0,0,0,0,0),(h,0,0,h,0,h,h,h)) \end{aligned}$$

is an 8-round zero-correlation linear hull for Camellia under some weak keys (covering rounds 6–13, see Fig.3), where $a, h \in \mathbb{F}_2^8$ denote any non-zero values, and the weak keys satisfy the following conditions:

$$\begin{aligned} &(a,a,0,0) \cap \overline{kl_R^2} = 0,\ ((a,0,a,a) \ggg_1) \cap kl_L^2 = 0; \\ &(h,0,0,h) \cap \overline{kl_R^3} = 0,\ ((0,h,h,h) \ggg_1) \cap kl_L^3 = 0. \end{aligned} \tag{1}$$

This is actually the first known 8-round zero-correlation linear distinguisher of Camellia with FL/FL^{-1} layers. Next we will show that the above 8-round linear hull has correlation 0.

According to the correlation matrices results presented in [27], the correlation of a linear hull can be computed as a sum of key-dependent signed products of correlations of linear approximations that are chained over consecutive rounds. Thus for the weak keys satisfying Eq. (1), we will demonstrate that all 8-round linear trails (covering rounds 6–13) with input and output masks being $((a,a,0,0,a,0,a,a),(0,0,0,0,0,0,0,0))$ and $((0,0,0,0,0,0,0,0),(h,0,0,h,0,h,h,h))$ have correlation 0, which indicates that the corresponding 8-round linear hull has correlation 0. The detailed explanation is given below:

– For the linear trails that the input and output masks of FL^{-1} function (Note that the FL function along the encryption direction is regarded as the FL^{-1} function along the decryption direction) are not equal, the correlations of these trails are 0 according to Property 2 given in Section 3.1 and Piling-up Lemma presented in [28].

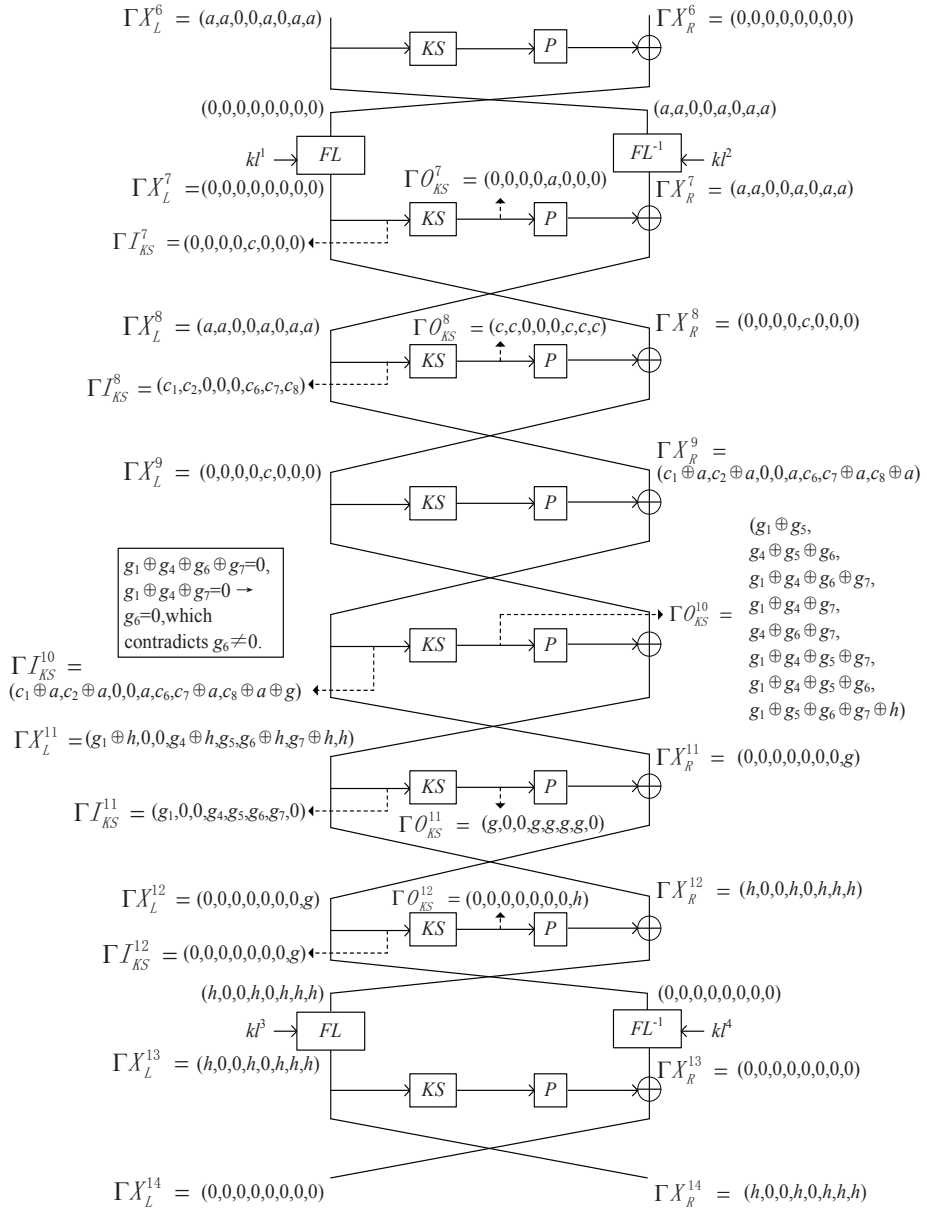


Fig. 3. 8-round zero-correlation linear distinguisher of Camellia with FL/FL^{-1} layers

– As to the linear trails that the input and output masks of FL^{-1} function are equal, we can deduce as follows (the mask evolution can be seen in Fig.3 where $(\Gamma X_L^i, \Gamma X_R^i)$ denotes the input mask of round i, and $\Gamma I_{KS}^i, \Gamma O_{KS}^i$ denote the input and output masks of the KS function in round i):

  - Along the encryption direction: We only consider the linear trail with non-zero correlation. Hence, given the mask $(\Gamma X_L^6, \Gamma X_R^6) = ((a, a, 0, 0, a, 0, a, a), (0, 0, 0, 0, 0, 0, 0, 0))$, the mask after three rounds (i.e., $(\Gamma X_L^9, \Gamma X_R^9)$) must have the form $((0, 0, 0, 0, c, 0, 0, 0)$,

$(c_1 \oplus a, c_2 \oplus a, 0, 0, a, c_6, c_7 \oplus a, c_8 \oplus a))$ if the corresponding 3-round linear trail has non-zero correlation, where $c, c_1, c_2, c_6, c_7, c_8 \in \mathbb{F}_2^8$ are unknown non-zero values.

- Along the decryption direction: Given the mask $(\Gamma X_L^{14}, \Gamma X_R^{14}) = ((0,0,0,0,0,0,0,0), (h,0,0,h,0,h,h,h))$, the mask after three rounds (i.e., $(\Gamma X_L^{11}, \Gamma X_R^{11})$) must have the form $((\mathrm{g}_1 \oplus h, 0, 0, \mathrm{g}_4 \oplus h, \mathrm{g}_5, \mathrm{g}_6 \oplus h, \mathrm{g}_7 \oplus h, h), (0,0,0,0,0,0,0,\mathrm{g}))$ if the corresponding 3-round linear trail has non-zero correlation, where $\mathrm{g}, \mathrm{g}_1, \mathrm{g}_4, \mathrm{g}_5, \mathrm{g}_6, \mathrm{g}_7 \in \mathbb{F}_2^8$ are unknown non-zero values.
- If the upper 3-round linear trail and the lower 3-round linear trail can build up an 8-round linear trail (covering rounds 6–13), then we have:

$$\begin{aligned}
\Gamma X_L^{10} &= (c_1 \oplus a, c_2 \oplus a, 0, 0, a, c_6, c_7 \oplus a, c_8 \oplus a), \\
\Gamma X_R^{10} &= (\mathrm{g}_1 \oplus h, 0, 0, \mathrm{g}_4 \oplus h, \mathrm{g}_5, \mathrm{g}_6 \oplus h, \mathrm{g}_7 \oplus h, h), \\
\Gamma I_{KS}^{10} &= (c_1 \oplus a, c_2 \oplus a, 0, 0, a, c_6, c_7 \oplus a, c_8 \oplus a \oplus \mathrm{g}).
\end{aligned}$$

  Moreover, ΓO_{KS}^{10} can be derived from ΓX_R^{10}. Actually, to make the correlation of the linear approximation of P transformation in round 10 non-zero (Otherwise, the correlation of the whole 8-round linear trail will be 0 according to Piling-up Lemma), ΓO_{KS}^{10} must have the form

$$\begin{aligned}
&(\mathrm{g}_1 \oplus \mathrm{g}_5,\ \mathrm{g}_4 \oplus \mathrm{g}_5 \oplus \mathrm{g}_6,\ \mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_6 \oplus \mathrm{g}_7,\ \mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_7,\ \mathrm{g}_4 \oplus \mathrm{g}_6 \oplus \mathrm{g}_7, \\
&\mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_5 \oplus \mathrm{g}_7,\ \mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_5 \oplus \mathrm{g}_6,\ \mathrm{g}_1 \oplus \mathrm{g}_5 \oplus \mathrm{g}_6 \oplus \mathrm{g}_7 \oplus h).
\end{aligned}$$

- In order to make the correlation of the linear approximation $\Gamma I_{KS}^{10} \to \Gamma O_{KS}^{10}$ non-zero, we have that

$$\mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_6 \oplus \mathrm{g}_7 = 0 \ \text{ and } \ \mathrm{g}_1 \oplus \mathrm{g}_4 \oplus \mathrm{g}_7 = 0.$$

  This implies $\mathrm{g}_6 = 0$, which contradicts the fact that g_6 is a non-zero value. Therefore, we can conclude that all 8-round linear trails (covering rounds 6–13) with input and output masks being $((a,a,0,0,a,0,a,a), (0,0,0,0,0,0,0,0))$ and $((0,0,0,0,0,0,0,0), (h,0,0,h,0,h,h,h))$ have correlation 0 for the weak keys satisfying Eq. (1).

4 Zero-Correlation Linear Attacks on Camellia

Firstly, by setting (a, h) as $(0\text{x}01, 0\text{x}01)$ and $(0\text{x}01, 0\text{x}02)$ respectively in Section 3.2, we obtain two 8-round zero-correlation linear distinguishers of Camellia with FL/FL^{-1} layers under the weak keys satisfying the following 15-bit conditions:

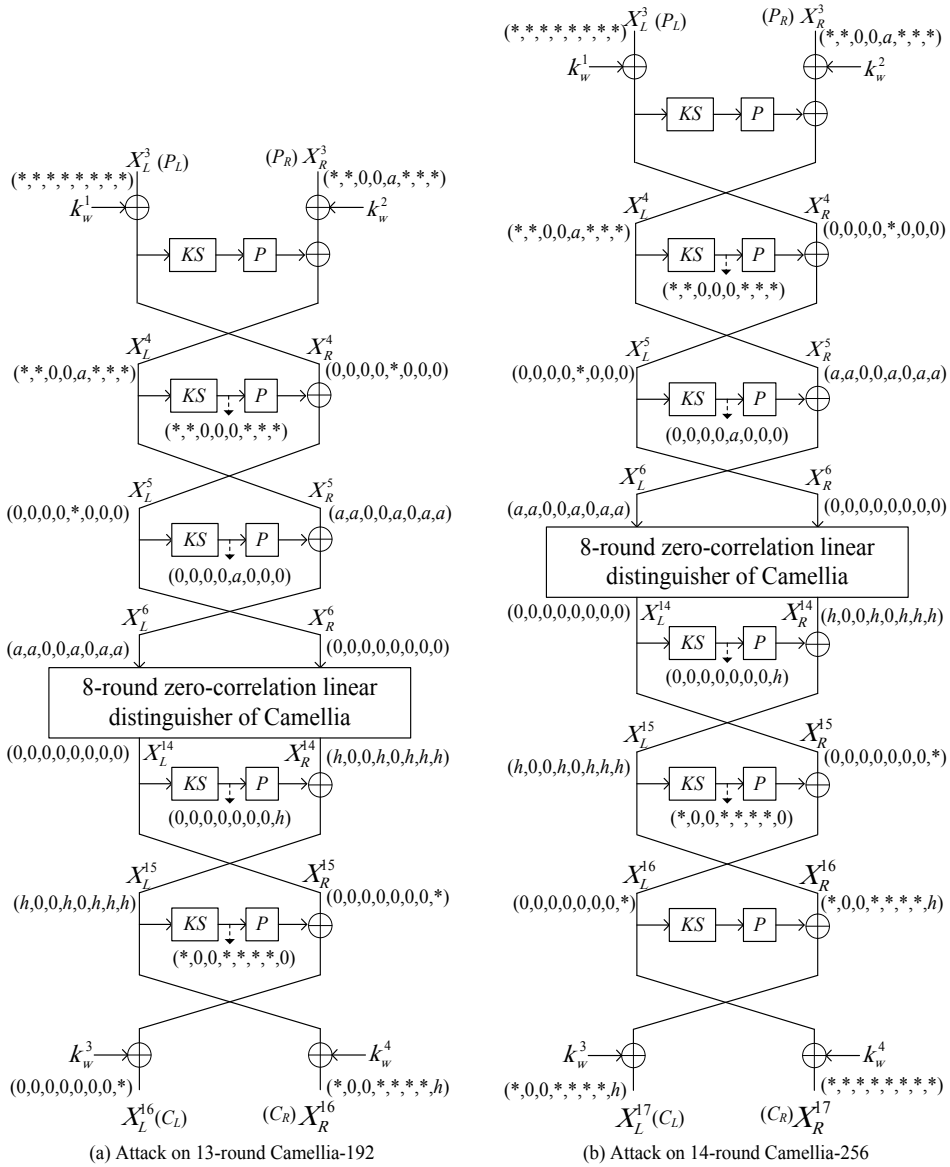
$$\begin{aligned}
&kl_L^2[1] = kl_L^2[9] = kl_L^2[25] = 0,\ kl_R^2[8] = kl_R^2[16] = 1, \\
&kl_L^3[1] = kl_L^3[17] = kl_L^3[25] = 0,\ kl_R^3[8] = kl_R^3[32] = 1, \\
&kl_L^3[16] = kl_L^3[24] = kl_L^3[32] = 0,\ kl_R^3[7] = kl_R^3[31] = 1.
\end{aligned} \tag{2}$$

Then based on these zero-correlation linear distinguishers, we can mount key recovery attacks on 13-round Camellia-192 and 14-round Camellia-256 with FL/FL^{-1} and whitening layers.

4.1 Attacking 13-round Camellia-192

Let E denote the 13-round Camellia-192 with the FL/FL^{-1} and whitening layers from the third round to the fifteenth round, and $P = (P_L, P_R)$, $C = (C_L, C_R)$ represent the plaintext

and ciphertext of E respectively. In the following, we will illustrate the attack on E with the help of the above two 8-round zero-correlation linear hulls (See Fig. 4(a)). Note that in Fig. 4(a), the bytes denoted as $'*'$ need to be computed while the bytes denoted as $'0'$ do not require computation.



(a) Attack on 13-round Camellia-192 (b) Attack on 14-round Camellia-256

Fig. 4. Attacks on 13-round Camellia-192 and 14-round Camellia-256

Before we give the detailed description of our attack, some notations are introduced as follows. Let $k^a = k_w^1 \oplus k^3$, $k^b = k_w^2 \oplus k^4$, $k^c = k_w^1 \oplus k^5$, $k^d = k_w^3 \oplus k^{14}$ and $k^e = k_w^4 \oplus k^{15}$. Then by using the equivalent subkeys k^a, k^b, k^c, k^d and k^e instead of the round keys k^3, k^4, k^5, k^{14} and k^{15}, we can remove the whitening layers. Moreover, let F_j^i denote the

function which computes the j-th output byte of the i-th round function. Let θ, ξ denote $P_L \| P_{R,\{1,2,6,7,8\}} \| C_{L,8} \| C_{R,\{1,4,5,6,7\}}$ and $k^a \| k^b_{\{1,2,6,7,8\}} \| k^d_8 \| k^e_{\{1,4,5,6,7\}}$, respectively. After that, in order to take the full advantage of the FFT technique to reduce the time complexity, we rewrite the linear approximation $(a, a, 0, 0, a, 0, a, a) \cdot X_L^6 \oplus (h, 0, 0, h, 0, h, h, h) \cdot X_R^{14} = 0$ by doing partial encryption and decryption as shown below:

$$\begin{aligned} & a \cdot P_{R,5} \oplus h \cdot C_{R,8} \oplus f(\theta \oplus \xi, k_5^a \oplus k_5^c) \\ = & a \cdot (k_1^b \oplus k_2^b \oplus k_7^b \oplus k_8^b) \oplus h \cdot (k_1^e \oplus k_4^e \oplus k_6^e \oplus k_7^e), \end{aligned} \tag{3}$$

where

$$\begin{aligned} & f(\theta \oplus \xi, k_5^a \oplus k_5^c) \\ = & a \cdot (S_2(\theta_5 \oplus \xi_5) \oplus \theta_{\{9,10,12,13\}} \oplus \xi_{\{9,10,12,13\}}) \\ & \oplus h \cdot (\theta_{\{15,16,18,19\}} \oplus \xi_{\{15,16,18,19\}}) \\ & \oplus h \cdot S_1(F_8^{15}(\theta_{\{15\sim 19\}} \oplus \xi_{\{15\sim 19\}}) \oplus \theta_{14} \oplus \xi_{14}) \\ & \oplus a \cdot S_2(S_1(F_1^3(\theta_{\{1,3,4,6\sim 8\}} \oplus \xi_{\{1,3,4,6\sim 8\}}) \oplus \theta_9 \oplus \xi_9) \oplus \\ & \qquad S_2(F_2^3(\theta_{\{1,2,4,5,7,8\}} \oplus \xi_{\{1,2,4,5,7,8\}}) \oplus \theta_{10} \oplus \xi_{10}) \oplus \\ & \qquad S_3(F_6^3(\theta_{\{2,3,5,7,8\}} \oplus \xi_{\{2,3,5,7,8\}}) \oplus \theta_{11} \oplus \xi_{11}) \oplus \\ & \qquad S_4(F_7^3(\theta_{\{3\sim 6,8\}} \oplus \xi_{\{3\sim 6,8\}}) \oplus \theta_{12} \oplus \xi_{12}) \oplus \\ & \qquad S_1(F_8^3(\theta_{\{1,4\sim 7\}} \oplus \xi_{\{1,4\sim 7\}}) \oplus \theta_{13} \oplus \xi_{13}) \oplus \\ & \qquad \theta_5 \oplus \xi_5 \oplus k_5^a \oplus k_5^c), \end{aligned}$$

θ_j, ξ_j represent the j-th bytes of θ, ξ (numbered from left to right), and $\theta_{\{j_1,j_2\}}$, $\theta_{\{j_1\sim j_2\}}$, $\xi_{\{j_1,j_2\}}$, $\xi_{\{j_1\sim j_2\}}$ $(j_1 < j_2)$ denote $\theta_{j_1} \| \theta_{j_2}$, $\theta_{j_1} \| \theta_{j_1+1} \| \ldots \| \theta_{j_2}$, $\xi_{j_1} \| \xi_{j_2}$, $\xi_{j_1} \| \xi_{j_1+1} \| \ldots \| \xi_{j_2}$ respectively.

Actually, Eq. (3) has zero correlation if and only if the following equation

$$a \cdot P_{R,5} \oplus h \cdot C_{R,8} \oplus f(\theta \oplus \xi, k_5^a \oplus k_5^c) = 0 \tag{4}$$

has zero correlation. Thus we will present a zero-correlation linear attack on E based on Eq. (4). The attack procedure is divided into two phases: *Distillation and Analysis* phase and *Master Key Recovery* phase.

Distillation and Analysis.

1. Collect all the 2^{128} plaintext-ciphertext pairs (P, C) of E.
2. Let $\mu = \theta \| P_{R,5}[8] \| C_{R,8}[8]$ and $\nu = \theta \| P_{R,5}[8] \| C_{R,8}[7]$. Initialize two vectors T and T', each consisting of 2^{154} counters which correspond to all possible values of μ and ν, respectively. Then for each pair (P, C), extract the 154-bit values μ and ν, and increase the corresponding counters T_μ and T'_ν by 1, respectively.
3. Initialize two vectors Z and Z', each composed of 2^{152} counters which correspond to all possible values of θ. Then for each value of μ, extract the 152-bit value θ and add T_μ to the corresponding counter Z_θ if the parity of $P_{R,5}[8] \oplus C_{R,8}[8]$ is 0, and subtract T_μ from Z_θ otherwise. Do similarly for each value of ν and update the vector Z' accordingly.
4. Initialize two vectors Y and Y', each consisting of 2^{152} elements which correspond to all possible values of $\theta \oplus \xi$. Then for each guess of the value of $k_5^a \oplus k_5^c$, do the following:
   - In the case that $(a, h) = (0\text{x}01, 0\text{x}01)$, compute the parity of $f(\theta \oplus \xi, k_5^a \oplus k_5^c)$ for each value of $\theta \oplus \xi$. Set the value of $Y_{\theta \oplus \xi}$ as 1 if the parity is 0, and -1 otherwise. Do similarly for the case that $(a, h) = (0\text{x}01, 0\text{x}02)$ and renew the vector Y' accordingly. Thus two 152-level circulant matrices $M(\xi, \theta)$, $M'(\xi, \theta)$ can be derived from the vectors Y and Y', respectively.

– Compute the vectors $\omega = MZ$ and $\omega' = M'Z'$, respectively.
– Keep the $\xi \| k_5^c$ as a possible subkey candidate if it satisfies $\omega_\kappa = \omega'_\kappa = 0$.

Master Key Recovery. According to [21] and the Wrong-Key Randomization Hypothesis given in [29], for a wrong subkey candidate, the probability that the correlation of Eq. (4) is 0 can be estimated as $\frac{1}{\sqrt{2\pi}} 2^{\frac{4-128}{2}}$. Therefore, the probability that a wrong subkey candidate for $\xi \| k_5^c$ can pass the test in Step 4 of *Distillation and Analysis* phase is approximately $(\frac{1}{\sqrt{2\pi}} 2^{-62})^2 \approx 2^{-126.6}$, thus about $2^{160} \times 2^{-126.6} = 2^{33.4}$ subkey candidates for $\xi \| k_5^c$ will be left after the *Distillation and Analysis* phase. For each of the $2^{33.4}$ values of $\xi \| k_5^c$, do the following to recover the master key consisting of 128-bit K_L and 64-bit $(K_R)_L$:

1. In terms of Table 2, the 160-bit subkey k^a, $k^b_{\{1,2,6,7,8\}}$, k^c_5, k^d_8, $k^e_{\{1,4,5,6,7\}}$ and the 15 bits of kl^2, kl^3 given in Eq. (2) are expressed in K_L, K_R, K_A and K_B as follows:

$$k^a = (K_L)_L \oplus (K_R \lll_{15})_L, \tag{5}$$

$$k^b_{\{1,2,6,7,8\}} = ((K_L)_R \oplus (K_R \lll_{15})_R)_{\{1,2,6,7,8\}}, \tag{6}$$

$$k^c_5 = ((K_L)_L \oplus (K_A \lll_{15})_L)_5, \tag{7}$$

$$k^d_8 = ((K_B \lll_{111})_L \oplus (K_R \lll_{60})_R)_8, \tag{8}$$

$$k^e_{\{1,4,5,6,7\}} = ((K_B \lll_{111})_R \oplus (K_B \lll_{60})_L)_{\{1,4,5,6,7\}}, \tag{9}$$

$$kl^2_L[1,9,25] = (K_R \lll_{30})_R[1,9,25], \tag{10}$$

$$kl^2_R[8,16] = (K_R \lll_{30})_R[40,48], \tag{11}$$

$$kl^3_L[1,16,17,24,25,32] = (K_L \lll_{60})_L[1,16,17,24,25,32], \tag{12}$$

$$kl^3_R[7,8,31,32] = (K_L \lll_{60})_L[39,40,63,64]. \tag{13}$$

2. According to Eq. (10) and (11), we can get five bits of $(K_R \lll_{30})_R$. Guess the other 59 bits of $(K_R \lll_{30})_R$, thus all the bits of $(K_R)_L$ are known. Derive $(K_L)_L$, $(K_L)_{R,\{1,2,6,7,8\}}$ from Eq. (5) and (6), respectively. Check whether $(K_L)_L[61] = (K_L)_R[12] = (K_L)_R[13] = 0$ and $(K_L)_R[59] = (K_L)_R[60] = 1$ hold or not. If not, discard the corresponding key candidate $(K_L)_L \| (K_L)_{R,\{1,2,6,7,8\}} \| (K_R)_L$. After this step, there are about $2^{59} \times 2^{-5} = 2^{54}$ possible values for $(K_L)_L \| (K_L)_{R,\{1,2,6,7,8\}} \| (K_R)_L$.
3. Obtain the five bits $(K_L)_R[20,21,28,35,36]$ according to Eq. (12) and (13), thus only 19 bits of $(K_L)_R$ are unknown. Now we guess these 19 bits of $(K_L)_R$ and compute K_A, K_B according to the key schedule. With Eq. (7), (8) and (9) we filter out 2^{-56} wrong candidates of $K_L \| (K_R)_L$.

Then we have $2^{33.4} \times 2^{54} \times 2^{19} \times 2^{-56} = 2^{50.4}$ key candidates $K_L \| (K_R)_L$ (i.e., the master key) altogether. For each of the $2^{50.4}$ key candidates, verify whether it is correct or not by using one plaintext-ciphertext pair. If not, remove the key candidate. It is expected that only the right key will be left.

Complexity of the Attack. The data complexity of this attack is 2^{128} known plaintexts. The memory complexity is primarily owing to storing the vectors T, T', Z and Z' in the *Distillation and Analysis* phase. Actually, the value of each counter in T is at most $2^{128}/2^{105} = 2^{23}$,

thus the size of each counter in T can be estimated as 23 bits. Similarly, the size of each counter in T', Z, Z' can be approximated as 23, 24, 24 bits respectively. Hence, the memory complexity of this attack can be measured as $2 \times 2^{154} \times 23/8 + 2 \times 2^{152} \times 24/8 \approx 2^{156.86}$ bytes. Regarding the time complexity of this attack, it is mainly dominated by the matrix-vector products MZ and $M'Z'$ in Step 4 of the *Distillation and Analysis* phase, which can be derived as follows. For each possible value of $k_5^a \oplus k_5^c$, the matrix-vector products MZ and $M'Z'$ require $2 \times 3 \times 152 \times 2^{152} \approx 2^{161.83}$ arithmetic operations by applying the FFT technique described in Section 2.2. Accordingly, the time complexity of this attack can be measured as $2^8 \times 2^{161.83} = 2^{169.83}$ 13-round Camellia-192 encryptions (Assume that one arithmetic operation is equivalent to one 13-round Camellia-192 encryption).

4.2 Attacking 14-round Camellia-256

Let E' denote the 14-round Camellia-256 with the FL/FL^{-1} and whitening layers from the third round to the sixteenth round. Now we present a key recovery attack on E' by using the same two 8-round zero-correlation linear hulls as in Section 4.1 (See Fig. 4(b)).

Let $k^a = k_w^1 \oplus k^3$, $k^b = k_w^2 \oplus k^4$, $k^c = k_w^1 \oplus k^5$, $k^d = k_w^4 \oplus k^{14}$, $k^e = k_w^3 \oplus k^{15}$ and $k^f = k_w^4 \oplus k^{16}$. Moreover, let θ, ξ denote $P_L \| P_{R,\{1,2,6,7,8\}} \| C_{L,\{1,4,5,6,7\}} \| C_R$ and $k^a \| k^b_{\{1,2,6,7,8\}} \| k^e_{\{1,4,5,6,7\}} \| k^f$, respectively. After that, in order to take the full advantage of the FFT technique to reduce the time complexity, we rewrite the linear approximation $(a, a, 0, 0, a, 0, a, a) \cdot X_L^6 \oplus (h, 0, 0, h, 0, h, h, h) \cdot X_R^{14} = 0$ by doing partial encryption and decryption as shown below:

$$\begin{aligned} & a \cdot P_{R,5} \oplus h \cdot C_{L,8} \oplus g(\theta \oplus \xi, k_5^a \oplus k_5^c, k_8^d \oplus k_8^f) \\ = {} & a \cdot (k_1^b \oplus k_2^b \oplus k_7^b \oplus k_8^b) \oplus h \cdot (k_1^e \oplus k_4^e \oplus k_6^e \oplus k_7^e), \end{aligned} \tag{14}$$

where

$$\begin{aligned} & g(\theta \oplus \xi, k_5^a \oplus k_5^c, k_8^d \oplus k_8^f) \\ = {} & a \cdot (S_2(\theta_5 \oplus \xi_5) \oplus \theta_{\{9,10,12,13\}} \oplus \xi_{\{9,10,12,13\}}) \\ & \oplus h \cdot (S_1(\theta_{26} \oplus \xi_{26}) \oplus \theta_{\{14,15,17,18\}} \oplus \xi_{\{14,15,17,18\}}) \\ & \oplus a \cdot S_2(S_1(F_1^3(\theta_{\{1,3,4,6\sim 8\}} \oplus \xi_{\{1,3,4,6\sim 8\}}) \oplus \theta_9 \oplus \xi_9) \oplus \\ & \qquad S_2(F_2^3(\theta_{\{1,2,4,5,7,8\}} \oplus \xi_{\{1,2,4,5,7,8\}}) \oplus \theta_{10} \oplus \xi_{10}) \oplus \\ & \qquad S_3(F_6^3(\theta_{\{2,3,5,7,8\}} \oplus \xi_{\{2,3,5,7,8\}}) \oplus \theta_{11} \oplus \xi_{11}) \oplus \\ & \qquad S_4(F_7^3(\theta_{\{3\sim 6,8\}} \oplus \xi_{\{3\sim 6,8\}}) \oplus \theta_{12} \oplus \xi_{12}) \oplus \\ & \qquad S_1(F_8^3(\theta_{\{1,4\sim 7\}} \oplus \xi_{\{1,4\sim 7\}}) \oplus \theta_{13} \oplus \xi_{13}) \oplus \\ & \qquad \theta_5 \oplus \xi_5 \oplus k_5^a \oplus k_5^c) \\ & \oplus h \cdot S_1(S_1(F_1^{16}(\theta_{\{19,21,22,24\sim 26\}} \oplus \xi_{\{19,21,22,24\sim 26\}}) \oplus \theta_{14} \oplus \xi_{14}) \oplus \\ & \qquad S_4(F_4^{16}(\theta_{\{20\sim 25\}} \oplus \xi_{\{20\sim 25\}}) \oplus \theta_{15} \oplus \xi_{15}) \oplus \\ & \qquad S_2(F_5^{16}(\theta_{\{19,20,24\sim 26\}} \oplus \xi_{\{19,20,24\sim 26\}}) \oplus \theta_{16} \oplus \xi_{16}) \oplus \\ & \qquad S_3(F_6^{16}(\theta_{\{20,21,23,25,26\}} \oplus \xi_{\{20,21,23,25,26\}}) \oplus \theta_{17} \oplus \xi_{17}) \oplus \\ & \qquad S_4(F_7^{16}(\theta_{\{21\sim 24,26\}} \oplus \xi_{\{21\sim 24,26\}}) \oplus \theta_{18} \oplus \xi_{18}) \oplus \\ & \qquad \theta_{26} \oplus \xi_{26} \oplus k_8^d \oplus k_8^f). \end{aligned}$$

Then we can mount an attack on E' similarly to that on E given in Section 4.1. The data, memory and time complexities of this attack are about 2^{128} known plaintexts, $2^{212.86}$ bytes and $2^{234.92}$ 14-round Camellia-256 encryptions, respectively.

5 Conclusion

In this paper, we have investigated the security of Camellia by means of zero-correlation linear cryptanalysis. Firstly, some new properties of the FL/FL^{-1} functions in Camellia have been proposed, following which we have observed some weak keys and constructed the first known 8-round zero-correlation linear distinguisher of Camellia with FL/FL^{-1} layers for these weak keys. Since this distinguisher covers the same number of rounds as the best known zero-correlation linear distinguisher for Camellia without FL/FL^{-1} layers, we claim that FL/FL^{-1} layers cannot thwart zero-correlation linear cryptanalysis effectively for some weak keys. Then by using this new distinguisher, we have presented key recovery attacks on 13-round Camellia-192 and 14-round Camellia-256 respectively. Note that our attacks work for weak keys with 15-bit conditions on kl^2 and kl^3 which are actually the 15-bit conditions on the master key, thus the advantages of these attacks over exhaustive search (measured in bits) are about $192 - 169.83 - 15 = 7.17$ and $256 - 234.92 - 15 = 6.08$ bits respectively. Although these results are the currently best for Camellia-192 and Camellia-256 with FL/FL^{-1} and whitening layers in terms of the number of attacked rounds, none of the attacks directly threatens the security of Camellia but they reduce the security margin of the cipher.

References

1. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2000.
2. CRYPTREC. Cryptography Research and Evaluation Committees: report. Archive, 2002. `http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html`.
3. Bart Preneel. NESSIE Project. In *Encyclopedia of Cryptography and Security (2nd Ed.)*, pages 831–836, 2011.
4. International Standardization of Organization (ISO). ISO/IEC 18033-3:2005. Information technology - Security techniques - Encryption algorithms - Part 3: Block Ciphers (July 2005).
5. Taizo Shirai, Shoji Kanamaru, and George Abe. Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia. In Joan Daemen and Vincent Rijmen, editors, *FSE*, volume 2365 of *Lecture Notes in Computer Science*, pages 128–142. Springer, 2002.
6. Seonhee Lee, Seokhie Hong, Sangjin Lee, Jongin Lim, and Seonhee Yoon. Truncated Differential Cryptanalysis of Camellia. In Kwangjo Kim, editor, *ICISC*, volume 2288 of *Lecture Notes in Computer Science*, pages 32–38. Springer, 2001.
7. Makoto Sugita, Kazukuni Kobara, and Hideki Imai. Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis. In Colin Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 193–207. Springer, 2001.
8. Duo Lei, Chao Li, and Keqin Feng. Square Like Attack on Camellia. In Sihan Qing, Hideki Imai, and Guilin Wang, editors, *ICICS*, volume 4861 of *Lecture Notes in Computer Science*, pages 269–283. Springer, 2007.
9. Duo Lei, Chao Li, and Keqin Feng. New Observation on Camellia. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 51–64. Springer, 2005.
10. Jiqiang Lu, Yongzhuang Wei, Pierre-Alain Fouque, and Jongsung Kim. Cryptanalysis of Reduced Versions of the Camellia Block Cipher. *IET Information Security*, 6(3):228–238, 2012.
11. Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic. The Higher-order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher. In Steven D. Galbraith and Mridul Nandi, editors, *INDOCRYPT*, volume 7668 of *Lecture Notes in Computer Science*, pages 244–264. Springer, 2012.

12. Wenling Wu, Dengguo Feng, and Hua Chen. Collision Attack and Pseudorandomness of Reduced-round Camellia. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography*, volume 3357 of *Lecture Notes in Computer Science*, pages 252–266. Springer, 2004.
13. Jiazhe Chen, Keting Jia, Hongbo Yu, and Xiaoyun Wang. New Impossible Differential Attacks of Reduced-round Camellia-192 and Camellia-256. In Udaya Parampalli and Philip Hawkes, editors, *ACISP*, volume 6812 of *Lecture Notes in Computer Science*, pages 16–33. Springer, 2011.
14. Leibo Li, Jiazhe Chen, and Keting Jia. New Impossible Differential Cryptanalysis of Reduced-round Camellia. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *CANS*, volume 7092 of *Lecture Notes in Computer Science*, pages 26–39. Springer, 2011.
15. Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In Tal Malkin, editor, *CT-RSA*, volume 4964 of *Lecture Notes in Computer Science*, pages 370–386. Springer, 2008.
16. Hamid Mala, Mohsen Shakiba, Mohammad Dakhilalian, and Ghadamali Bagherikaram. New Results on Impossible Differential Cryptanalysis of Reduced-round Camellia-128. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 281–294. Springer, 2009.
17. Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen, and Wei Li. New Observations on Impossible Differential Cryptanalysis of Reduced-round Camellia. In Canteaut [30], pages 90–109.
18. Ya Liu, Dawu Gu, Zhiqiang Liu, and Wei Li. Improved Results on Impossible Differential Cryptanalysis of Reduced-round Camellia-192/256. *Journal of Systems and Software*, 85(11):2451 – 2458, 2012.
19. Dongxia Bai and Leibo Li. New Impossible Differential Attacks on Camellia. In Mark Dermot Ryan, Ben Smyth, and Guilin Wang, editors, *ISPEC*, volume 7232 of *Lecture Notes in Computer Science*, pages 80–96. Springer, 2012.
20. Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 306–323. Springer, 2013.
21. Andrey Bogdanov and Vincent Rijmen. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. *Des. Codes Cryptography*, 70(3):369–383, 2014.
22. Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT*, volume 7658 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2012.
23. Andrey Bogdanov and Meiqin Wang. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In Canteaut [30], pages 29–48.
24. Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen. Multidimensional Zero-Correlation Attacks on Lightweight Block Cipher HIGHT: Improved Cryptanalysis of an ISO Standard. *Inf. Process. Lett.*, 114(6):322–330, 2014.
25. Yasuo Hatano, Hiroki Sekine, and Toshinobu Kaneko. Higher Order Differential Attack of Camellia (II). In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 129–146. Springer, 2002.
26. Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Improving the Time Complexity of Matsui's Linear Cryptanalysis. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC*, volume 4817 of *Lecture Notes in Computer Science*, pages 77–88. Springer, 2007.
27. Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation Matrices. In Bart Preneel, editor, *FSE*, volume 1008 of *Lecture Notes in Computer Science*, pages 275–285. Springer, 1994.
28. Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.
29. Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT*, volume 921 of *Lecture Notes in Computer Science*, pages 24–38. Springer, 1995.
30. Anne Canteaut, editor. *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*. Springer, 2012.