New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia

Ya Liu[1], Leibo Li[2,3,*], Dawu Gu[1], Xiaoyun Wang[2,3,4],
Zhiqiang Liu[1], Jiazhe Chen[2,3], and Wei Li[5,6,7]

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{liuya0611,dwgu,ilu_zq}@sjtu.edu.cn
[2] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
[3] School of Mathematics, Shandong University,
Jinan 250100, China
{lileibo,jiazhechen}@mail.sdu.edu.cn
[4] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn
[5] School of Computer Science and Technology, Donghua University,
Shanghai 201620, China
[6] Shanghai Key Laboratory of Integrate Administration Technologies
for Information Security, Shanghai 200240, China
liwei.cs.cn@gmail.com
[7] State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing 100190, China

Abstract. Camellia is one of the widely used block ciphers, which has been selected as an international standard by ISO/IEC. In this paper, by exploiting some interesting properties of the key-dependent layer, we improve previous results on impossible differential cryptanalysis of reduced-round Camellia and gain some new observations. First, we introduce some new 7-round impossible differentials of Camellia for weak keys. These weak keys that work for the impossible differential take 3/4 of the whole key space, therefore, we further get rid of the weak-key assumption and leverage the attacks on reduced-round Camellia to all keys by utilizing the multiplied method. Second, we build a set of differentials which contains at least one 8-round impossible differential of Camellia with two FL/FL^{-1} layers. Following this new result, we show that the key-dependent transformations inserted in Camellia cannot resist impossible differential cryptanalysis effectively. Based on this set of differentials, we present a new cryptanalytic strategy to mount impossible differential attacks on reduced-round Camellia.

Keywords: Block Cipher, Camellia, Impossible Differential Cryptanalysis.

[*] Corresponding author.

A. Canteaut (Ed.): FSE 2012, LNCS 7549, pp. 90–109, 2012.

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 [4] and as a member of the NESSIE block cipher portfolio in 2003 [20]. In 2005, it was adopted as the international standard by ISO/IEC [6]. Camellia is a 128-bit block cipher. It supports variable key sizes and the number of the rounds depends on the key size, i.e., 18 rounds for a 128-bit key size and 24 rounds for 192/256-bit key sizes. For simplicity, they can be usually denoted as Camellia-128, Camellia-192 and Camellia-256, respectively. Camellia adopts the basic Feistel structure with some key-dependent functions FL/FL^{-1} inserted every six rounds, where these key-dependent transformations must be linear and reversible for any fixed key. The goals for such a design are to provide non-regularity across rounds and to thwart future unknown attacks.

Up to now, many cryptanalytic methods were used to evaluate the security of reduced-round Camellia such as linear cryptanalysis, differential cryptanalysis, higher order differential attack, truncated differential attack, collision attack, square attack and impossible differential attack. Before 2011, most attacks focused on the security of simplified versions of Camellia, which did not take the FL/FL^{-1} and whitening layers into account [9–11, 16, 19, 21–24]. Recently, some attacks involved in the study of the original structure of Camellia. For instance, Chen *et al.* constructed a 6-round impossible differential with the FL/FL^{-1} layer to attack 10-round Camellia-192 and 11-round Camellia-256 [3], Lu, Liu and Li independently improved Chen's results to attack on reduced-round Camellia [12, 14, 17], Lu *et al.* proposed higher order meet-in-the-middle attacks on 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 [18].

Impossible differential cryptanalysis was independently proposed by Knudsen [7] and Biham [2]. Its main idea is to use impossible differentials that hold with probability zero to discard the wrong keys until only one key is left. So far, impossible differential cryptanalysis has received much attention and been used to attack a variety of well-known block ciphers such as AES, ARIA, CLEFIA, MISTY1 and so on.

In this paper, we reevaluate the security of reduced-round Camellia with FL/FL^{-1} and whitening layers against impossible differential cryptanalysis from two aspects. On the one hand, we construct some new 7-round impossible differentials of Camellia for weak keys, which work for 75% of the keys. Based on one of them, we mount impossible differential attacks on reduced-round Camellia in the weak-key setting. Then we further propose a multiplied method to extend our attacks for the whole key space. The basic idea is that if the correct key belongs to the set of weak keys, then it will never satisfy the impossible differential. While if the correct key is not a weak key, we get 2-bit conditions about the key. In fact, for the whole key space, we attack 10-round Camellia-128 with about $2^{113.8}$ chosen plaintexts and 2^{120} 10-round encryptions, 11-round Camellia-192 with about $2^{114.64}$ chosen plaintexts and 2^{184} 11-round encryptions as well as 12-round Camellia-256 with about $2^{116.17}$ chosen plaintexts or chosen ciphertexts and 2^{240} 12-round encryptions, respectively. Meanwhile, we can also extend these attacks to 12-round Camellia-192 and 14-round Camellia-256 with two FL/FL^{-1} layers. On the other hand, by studying some properties of key-dependent functions FL/FL^{-1}, we build a set of differentials which contains at least one 8-round impossible differential of Camellia with two FL/FL^{-1} layers. The length of this impossible differential with two FL/FL^{-1} layers is the same as the length of the longest known impossible differential of Camellia without the FL/FL^{-1} layer given by Wu and Zhang [24]. Consequently, we show that the key-dependent transformations inserted in Camellia cannot resist impossible differential cryptanalysis effectively. Based on this set of differentials, we propose a new cryptanalytic strategy to attack 11-round Camellia-128 with about 2^{122} chosen plaintexts and 2^{122} 11-round encryptions, 12-round Camellia-192 with approximately 2^{123} chosen plaintexts and $2^{187.2}$ 12-round encryptions as well as 13-round Camellia-256 with about 2^{123} chosen plaintexts and $2^{251.1}$ 13-round encryptions (not from the first round but with the whitening layers), respectively. All attacks adopt the early abort technique [15]. In table 1, we summarize our results along with the former known ones on reduced-round Camellia.

Table 1. Summary of the attacks on Reduced-Round Camellia

Key Size	Rounds	Attack Type	Data	Time(Enc)	Memory	Source
128 bits	9†	Square	2^{48}CP	2^{122}	2^{53}Bytes	[10]
	10†	Impossible DC	2^{118}CP	2^{118}	2^{93} Bytes	[17]
	10†	HO-MitM	2^{93}CP	$2^{118.6}$	2^{109} Bytes	[18]
	10†	Impossible DC	$2^{118.5}$CP	$2^{123.5}$	2^{127}Bytes	[12]
	10(WK)	Impossible DC	$2^{111.8}$CP	$2^{111.8}$	$2^{84.8}$Bytes	Section 3.2
	10	Impossible DC	$2^{113.8}$CP	2^{120}	$2^{84.8}$ Bytes	Section 3.2
	11	Impossible DC	2^{122}CP	2^{122}	2^{102} Bytes	Section 4.4
192 bits	10	Impossible DC	2^{121}CP	$2^{175.3}$	$2^{155.2}$Bytes	[3]
	10	Impossible DC	$2^{118.7}$CP	$2^{130.4}$	2^{135}Bytes	[12]
	11†	Impossible DC	2^{118}CP	$2^{163.1}$	2^{141}Bytes	[17]
	11†	HO-MitM	2^{94}CP	$2^{180.2}$	2^{174}Bytes	[18]
	11(WK)	Impossible DC	$2^{112.64}$CP	$2^{146.54}$	$2^{141.64}$Bytes	Section 3.3
	11	Impossible DC	$2^{114.64}$CP	2^{184}	$2^{141.64}$Bytes	Section 3.3
	12	Impossible DC	2^{123}CP	$2^{187.2}$	2^{160}Bytes	Section 4.3
	12†	Impossible DC	$2^{120.1}$CP	2^{184}	$2^{124.1}$Bytes	Section 3.5
256 bits	11	High Order DC	2^{93}CP	$2^{255.6}$	2^{98}Bytes	[5]
	11	Impossible DC	2^{121}CP	$2^{206.8}$	2^{166}Bytes	[3]
	11	Impossible DC	$2^{119.6}$CP	$2^{194.5}$	2^{135}Bytes	[12]
	12†	HO-MitM	2^{94}CP	$2^{237.3}$	2^{174}Bytes	[18]
	12(WK)	Impossible DC	$2^{121.12}$CP	$2^{202.55}$	$2^{142.12}$Bytes	Section 3.4
	12	Impossible DC	$2^{116.17}$CP/CC	2^{240}	$2^{150.17}$Bytes	Section 3.4
	13	Impossible DC	2^{123}CP	$2^{251.1}$	2^{208}Bytes	Section 4.2
	14†	Impossible DC	2^{120}CC	$2^{250.5}$	2^{125}Bytes	Section 3.5

DC: Differential Cryptanalysis; CP/CC: Chosen Plaintexts/Chosen Ciphertexts; Enc: Encryptions; †: The attack doesn't include the whitening layers; WK: Weak Key; HO-MitM: Higher Order Meet-in-the-Middle Attack.

The remainder of this paper is organized as follows. Section 2 gives some notations and a brief introduction of Camellia. Section 3 presents several 7-round impossible differentials of Camellia for weak keys. Based on one of them, impossible differential attacks on 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 are elaborated. Section 4 first constructs a set of differentials which contains at least one 8-round impossible differential of Camellia with two FL/FL^{-1} layers, and then proposes impossible differential attacks on 11-round Camellia-128, 12-round Camellia-192 and 13-round Camellia-256, respectively. Section 5 summarizes this paper.

2 Preliminaries

2.1 Some Notations

- P, C: the plaintext and the ciphertext;
- L_{i-1}, R_{i-1}: the left half and the right half of the i-th round input;
- $\Delta L_{i-1}, \Delta R_{i-1}$: the left half and the right half of the input difference in the i-th round;
- $X \mid Y$: the concatenation of X and Y;
- $kw_1|kw_2, kw_3|kw_4$: the pre-whitening key and the post-whitening key;
- k_i: the subkey used in the i-th round;
- $kl_i (1 \leq i \leq 6)$: 64-bit keys used in the functions FL/FL^{-1};
- $S_r, \Delta S_r$: the output and the output difference of the S-boxes in the r-th round;
- $X \lll j$: left rotation of X by j bits;
- $X_{L(\frac{n}{2})}, X_{R(\frac{n}{2})}$: the left half and the right half of a n-bit word X;
- $X_i, X_{\{i,j\}}, X_{\{i\sim j\}}$: the i-th byte, the i-th and j-th bytes and the i-th to the j-th bytes of X;
- $X^i, X^{(i,j)}, X^{(i\sim j)}$: the i-th bit, the i-th and j-th bits and the i-th to j-th bits of X;
- $\oplus, \cap, \cup$: bitwise exclusive-OR (XOR), AND, and OR operations, respectively;
- $0_{(i)}, 1_{(i)}$: consecutive i bits are zero or one.

2.2 Overview of Camellia

Camellia [1] is a 128-bit block cipher. It adopts the basic Feistel structure with keyed functions FL/FL^{-1} inserted every 6 rounds. Camellia uses variable key sizes and the number of rounds depends on the key size, i.e., 18 rounds for a 128-bit key size and 24 rounds for 192/256-bit key sizes. Its round function uses a SPN structure, including the XOR operation with the round subkey, the nonlinear transformation S and the linear permutation P. Please refer to [1] for detailed information.

The key schedule algorithm of Camellia applies a 6-round Feistel structure to derive two 128-bit intermediate variables K_A and K_B from K_L and K_R, and then all round subkeys can be generated by K_L, K_R, K_A and K_B. For Camellia-128, the 128-bit key K is used as K_L and K_R is 0. For Camellia-192, the left

128-bit of the key K is used as K_L, and the concatenation of the right 64-bit of the key K and the complement of the right 64-bit of the key K is used as K_R. For Camellia-256, the main key K is separated into two 128-bit variables K_L and K_R, i.e., $K = K_L \mid K_R$.

3 7-Round Impossible Differentials of Camellia for Weak Keys and Their Applications[1]

In this section, we construct some 7-round impossible differentials of Camellia in weak-key setting. Based on one of them, we present impossible differential attacks on 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 which start from the first round. In addition, we also extend these attacks to 12-round Camellia-192 and 14-round Camellia-256 with two FL/FL^{-1} layers.

3.1 7-Round Impossible Differentials of Camellia for Weak Keys

This section introduces 7-round impossible differentials of Camellia in weak-key setting, which is based on the following lemmas and propositions.

Lemma 1 ([8]). *Let X, X', K be l-bit values, and $\Delta X = X \oplus X'$, then the differential properties of AND and OR operations are:*
$(X \cap K) \oplus (X' \cap K) = (X \oplus X') \cap K = \Delta X \cap K$,
$(X \cup K) \oplus (X' \cup K) = (X \oplus K \oplus (X \cap K)) \oplus (X' \oplus K \oplus (X' \cap K)) = \Delta X \oplus (\Delta X \cap K)$.

Lemma 2 ([3]). *Let ΔX and ΔY be the input and output differences of FL. Then $\Delta Y_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta X_R, \Delta Y_L = \Delta X_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R)$; $\Delta X_L = \Delta Y_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R), \Delta X_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta Y_R$.*

Proposition 1. *If the output difference of FL is $\Delta Y = (0|0|0|0|d|0|0|0)$, where $d \neq 0$ and $d^{(1)} = 0$, then the input difference of FL should satisfy $\Delta X_{\{2,3,4,6,7,8\}} = 0$.*

Proposition 2. *If the output difference of FL^{-1} is $\Delta X = (0|e|e|e|0|e|e|e)$, and the subkeys of FL^{-1} satisfy that $KL_L^{(9)}$ is 0 or $KL_R^{(8)}$ is 1, then the first byte of input difference ΔY should be zero, where e is a non-zero byte.*

Proposition 3. *Given a 7-round Camellia encryption and a FL/FL^{-1} layer inserted between the fifth and sixth round. If the input difference of the first round is $(0|0|0|0|0|0|0|0, a|0|0|0|c|0|0|0)$, and the subkeys of FL^{-1} satisfy $KL_L^{(9)} = 0$ or $KL_R^{(8)} = 1$, then the output difference $(0|0|0|0|d|0|0|0, 0|0|0|0|0|0|0|0)$ with $d^{(1)} = 0$ is impossible, where a and d are non-zero bytes, c is an arbitrary value (see Fig. 1).*

We also obtain three other impossible differentials under different weak-key assumptions:

- $(0|0|0|0|0|0|0|0, 0|a|0|0|0|c|0|0) \nrightarrow (0|0|0|0|0|d|0|0, 0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(17)} = 0$ or $KL_R^{(16)} = 1$, and $d^{(1)} = 0$,

[1] By Leibo Li, Xiaoyun Wang and Jiazhe Chen. See [13] for more details.

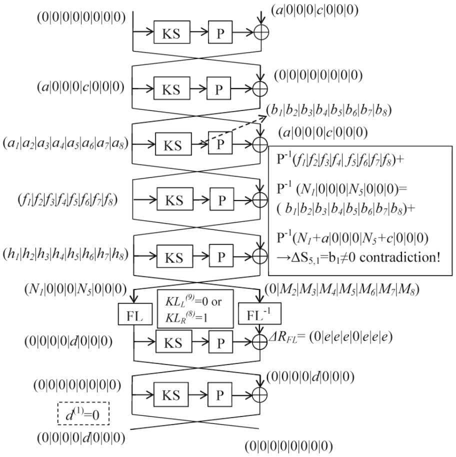
(0|0|0|0|0|0|0|0)
KS
P
$(a|0|0|0|c|0|0|0)$
$(a|0|0|0|c|0|0|0)$
(0|0|0|0|0|0|0|0)
$(b_1|b_2|b_3|b_4|b_5|b_6|b_7|b_8)$
$(a_1|a_2|a_3|a_4|a_5|a_6|a_7|a_8)$
$(a|0|0|0|c|0|0|0)$
$P^{-1}(f_1|f_2|f_3|f_4|f_5|f_6|f_7|f_8)+$
$P^{-1}(N_1|0|0|0|N_5|0|0|0)=$
$(b_1|b_2|b_3|b_4|b_5|b_6|b_7|b_8)+$
$P^{-1}(N_1+a|0|0|0|N_5+c|0|0|0)$
$\rightarrow \Delta S_{5,1}=b_1\neq 0$ contradiction!
$(f_1|f_2|f_3|f_4|f_5|f_6|f_7|f_8)$
$(h_1|h_2|h_3|h_4|h_5|h_6|h_7|h_8)$
$(N_1|0|0|0|N_5|0|0|0)$
$(0|M_2|M_3|M_4|M_5|M_6|M_7|M_8)$
FL
$KL_L^{(9)}=0$ or
$KL_R^{(8)}=1$
FL^{-1}
$(0|0|0|0|d|0|0|0)$
$\Delta R_{FL}=(0|e|e|e|0|e|e|e)$
(0|0|0|0|0|0|0|0)
$(0|0|0|0|d|0|0|0)$
$d^{(1)}=0$
$(0|0|0|0|d|0|0|0)$
(0|0|0|0|0|0|0|0)

Fig. 1. A 7-Round Impossible Differential for Weak Keys

- $(0|0|0|0|0|0|0|0, 0|0|a|0|0|0|c|0) \nrightarrow (0|0|0|0|0|0|d|0, 0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(25)}=0$ or $KL_R^{(24)}=1$, and $d^{(1)}=0$,
- $(0|0|0|0|0|0|0|0, 0|0|0|a|0|0|0|c) \nrightarrow (0|0|0|0|0|0|0|d, 0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(1)}=0$ or $KL_R^{(32)}=1$, and $d^{(1)}=0$.

We denote this type of impossible differentials above as **5+2 WKID** (weak-key impossible differentials). Due to the feature of Feistel structure, we also deduce another type of 7-round impossible differentials with the FL/FL^{-1} layer inserted between the second and the third rounds. We call them **2+5 WKID**, which are depicted as follows.

- $(0|0|0|0|0|0|0|0, 0|0|0|0|d|0|0|0) \nrightarrow (a|0|0|0|c|0|0|0, 0|0|0|0|0|0|0|0)$ with conditions $KL'^{(9)}_L=0$ or $KL'^{(8)}_R=1$, and $d^{(1)}=0$,
- $(0|0|0|0|0|0|0|0, 0|0|0|0|0|d|0|0) \nrightarrow (0|a|0|0|0|c|0|0, 0|0|0|0|0|0|0|0)$ with conditions $KL'^{(17)}_L=0$ or $KL'^{(16)}_R=1$, and $d^{(1)}=0$,
- $(0|0|0|0|0|0|0|0, 0|0|0|0|0|0|d|0) \nrightarrow (0|0|a|0|0|0|c|0, 0|0|0|0|0|0|0|0)$ with conditions $KL'^{(25)}_L=0$ or $KL'^{(24)}_R=1$, and $d^{(1)}=0$,
- $(0|0|0|0|0|0|0|0, 0|0|0|0|0|0|0|d) \nrightarrow (0|0|0|a|0|0|0|c, 0|0|0|0|0|0|0|0)$ with conditions $KL'^{(1)}_L=0$ or $KL'^{(32)}_R=1$, and $d^{(1)}=0$,

where KL' represents the subkey used in FL-function.

3.2 Impossible Differential Attack on 10-Round Camellia-128

We first propose an attack that works for $3\times 2^{126}(=\frac{3}{4}\times 2^{128})$ keys, which is mounted by adding one round on the top and two rounds on the bottom of the **5+2 WKID** (See Fig. 2).

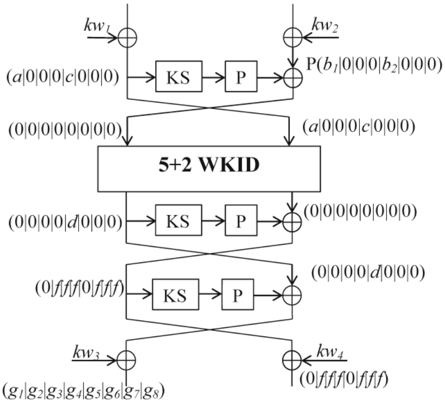

Fig. 2. Impossible Differential Attack on 10-Round Camellia-128 for Weak Keys

Data Collection

1. Choose 2^n structures of plaintexts, and each structure contains 2^{32} plaintexts $(L_0, R_0) = (\alpha_1|x_1|x_2|x_3|\alpha_2|x_4|x_5|x_6, P(\beta_1|y_1|y_2|y_3|\beta_2|y_4|y_5|y_6))$, where x_i and y_i $(i = 1, ..., 6)$ are fixed values in each structure, while α_j and β_j $(j = 1, 2)$ take all the possible values.
2. For each structure, ask for the encryption of the plaintexts and get 2^{32} ciphertexts. Store them in a hash table H indexed by $C_{R,\{1,5\}}$, the XOR of $C_{R,2}$ and $C_{R,3}$, the XOR of $C_{R,2}$ and $C_{R,4}$, the XOR of $C_{R,2}$ and $C_{R,6}$, the XOR of $C_{R,2}$ and $C_{R,7}$, the XOR of $C_{R,2}$ and $C_{R,8}$. Then by birthday paradox, we get 2^{n+7} pairs of ciphertexts with the differences $(\Delta C_L, \Delta C_R) = (g_1|g_2|g_3|g_4|g_5|g_6|g_7|g_8, 0|f|f|f|0|f|f|f)$, and the differences of corresponding plaintext pairs satisfy $(\Delta L_0, \Delta R_0) = (a|0|0|0|c|0|0|0, P(b_1|0|0|0|b_2|0|0|0))$, where a, c, f and b_i $(i = 1, 2)$ are non-zero bytes, and g_i are unknown bytes. For every pair, compute $P^{-1}(\Delta C_L) = P^{-1}(g_1|g_2|g_3|g_4|g_5|g_6|g_7|g_8) = (g'_1|g'_2|g'_3|g'_4|g'_5|g'_6|g'_7|g'_8)$. Keep only the pairs whose ciphertexts satisfy $g'_1 = 0$. The probability of this event is 2^{-8}, thus the expected number of remaining pairs is 2^{n-1}.

Key Recovery

1. For each pair obtained in the data collection phase, guess the 16-bit value $K_{1,\{1,5\}}$, partially encrypt its plaintext $(L_{0,\{1,5\}}, {L'}_{0,\{1,5\}})$ to get the intermediate value $(S_{1,\{1,5\}}, {S'}_{1,\{1,5\}})$ and the difference $\Delta S_{1,\{1,5\}}$. Then discard the pairs whose intermediate values do not satisfy $\Delta S_{1,1} = b_1$ and $\Delta S_{1,5} = b_2$. The probability of a pair being kept is 2^{-16}, so the expected number of remaining pairs is 2^{n-17}.
2. In this step, the ciphertext of every remaining pair is considered.
   (a) Guess the 8-bit value $K_{10,8}$ for every remaining pair, partially decrypt the ciphertext $(C_{R,8}, C'_{R,8})$ to get the intermediate value $(S_{10,8}, S'_{10,8})$ and

   the difference $\Delta S_{10,8}$, and discard the pairs whose intermediate values do not satisfy $\Delta S_{10,8} = g'_8$. The expected number of remaining pairs is 2^{n-25}.

   (b) For $l = 2, 3, 4, 6, 7$, guess the 8-bit value $K_{10,l}$. For every remaining pair, partially decrypt the ciphertext $(C_{R,l}, C'_{R,l})$ to get the intermediate value $(S_{10,l}, S'_{10,l})$ and the difference $\Delta S_{10,l}$, and keep only the pairs whose intermediate values satisfy $\Delta S_{10,l} = g'_l \oplus g'_5$. Since each pair will remain with probability 2^{-40}, the expected number of remaining pairs is 2^{n-65}.

   (c) Guess the 8-bit value $K_{10,1}$, partially decrypt the ciphertext $C_{R,1}$ of every remaining pair to get the intermediate value $S_{10,1}$, which is also the value of $S'_{10,1}$.

   (d) Partially decrypt (S_{10}, S'_{10}) to get the intermediate values $(R_{9,5}, R'_{9,5})$, and discard the pairs whose intermediate values do not satisfy $\Delta R^{(1)}_{9,5} = 0$. As the probability of a pair being discarded is 0.5, the expected number of remaining pairs is 2^{n-66}.

3. For every remaining pair, guess the 8-bit value $K_{9,5}$, partially decrypt the output value $(R_{9,5}, R'_{9,5})$ to get the intermediate value $(S_{9,5}, S'_{9,5})$ and the difference $\Delta S_{9,5}$. If there is a pair satisfying $\Delta S_{9,5} = \Delta C_{R,2}$, we discard the guessed key and try another one. Otherwise we exhaustively search for the remaining 48 bits of the key under this guessed key, if the correct key is obtained, we halt the attack; otherwise, another key guess should be tried.

Complexity. Since the probability of the event $\Delta S_{9,5} = \Delta C_{R,2}$ in step 3 of key recovery phase is 2^{-8}, the expected number of remaining guesses for 72-bit target subkeys is about $\epsilon = 2^{80} \times (1 - 2^{-8})^{2^{n-66}}$. If we choose $\epsilon = 1$, then n is 79.8, and the proposed attack requires $2^{n+32} = 2^{111.8}$ chosen plaintexts. The time and memory complexities are dominated by step 2 of data collection phase, which are about $2^{111.8}$ 10-round encryptions and $2^{n-1} \times 4 \times 2^4 = 2^{84.8}$ bytes.

Extending the Attack to the Whole Key Space. On the basis of the above impossible differential attack for weak keys, we construct a multiplied attack on 10-Round Camellia-128.

- **Phase 1.** Perform an impossible differential attack by using the **5+2 WKID** $(0|0|0|0|0|0|0|0, a|0|0|0|c|0|0|0) \nrightarrow (0|0|0|0|d|0|0|0, 0|0|0|0|0|0|0|0)$. This phase is extremely similar to the weak-key attack that is described above. However, it is slightly different when the attack is finished. That is, if there is a key kept, then the key is the correct key, and we halt the procedure of the attack. Otherwise, we conclude that the correct key does not belong to this set of weak keys, which means that $kl^{(9)}_1 = 1$ and $kl^{(8)}_2 = 0$. In this case, we get 2-bit information of the key and perform the next phase.
- **Phases 2 to 4.** Perform an impossible differential attack by using each **5+2 WKID** in the following:

$$(0|0|0|0|0|0|0|0, 0|a|0|0|0|c|0|0) \nrightarrow (0|0|0|0|0|d|0|0, 0|0|0|0|0|0|0|0),$$

$$(0|0|0|0|0|0|0|0, 0|0|a|0|0|0|c|0) \nrightarrow (0|0|0|0|0|0|d|0, 0|0|0|0|0|0|0|0),$$

$$(0|0|0|0|0|0|0|0, 0|0|0|a|0|0|0|c) \nrightarrow (0|0|0|0|0|0|0|d, 0|0|0|0|0|0|0|0).$$

The procedure is similar to Phase 1, and either recover the correct key or get another 2-bit information about the key and execute the next phase.

- **Phase 5.** Announce the intermediate key $K_A^{(95,103,111,119)} = 0$ and $K_A^{(6,14,22,30)} = 1$, then exhaustively search for the remaining 120-bit value of K_A and recover the key K_L.

The upper bound of the time complexity is $2^{111.8} \times 4 + 2^{120} \approx 2^{120}$. The data complexity is about $2^{113.8}$. The memory could be reused in different phase, so the memory requirement is about $2^{84.8}$ bytes.

3.3 Attack on 11-Round Camellia-192

We add one round on the bottom of 10-round attack and give an attack on 11-round Camellia-192.

Data Collection. Choose $2^{80.64}$ structures of plaintexts. Each structure contains 2^{32} plaintexts satisfying $(L_0, R_0) = (\alpha_1|x_1|x_2|x_3|\alpha_2|x_4|x_5|x_6, P(\beta_1|y_1|y_2|y_3|\beta_2|y_4|y_5|y_6))$, where x_i and y_i $(i = 1, ..., 6)$ are fixed values in each structure, while α_j and β_j $(j = 1, 2)$ take all the possible values. Ask for the encryption of the corresponding ciphertext for each plaintext, compute $P^{-1}(C_R)$ and store the plaintext-ciphertext pairs (L_0, R_0, C_L, C_R) in a hash table indexed by 8-bit value $(P^{-1}(C_R))_1$. By birthday paradox, we get $2^{135.64}$ pairs whose ciphertext differences satisfy $P^{-1}(\Delta C_L) = (h'_1|h'_2|h'_3|h'_4|h'_5|h'_6|h'_7|h'_8)$ and $P^{-1}(\Delta C_R) = (0|g'_2|g'_3|g'_4|g'_5|g'_6|g'_7|g'_8)$, where h'_i and g'_i are unknown values.

Key Recovery

1. For $l = 1, 5$, guess the 8-bit value of $K_{1,l}$, partially encrypt their plaintext $(L_{0,l}, L'_{0,l})$ and discard the pairs whose intermediate value do not satisfy $\Delta S_{1,l} = (P^{-1}(\Delta R_0))_l$. The expected number of remaining pairs is $2^{119.64}$.
2. In this step, we consider the ciphertext of each remaining pair.
   (a) For $l = 1, 2, 3, 4, 6, 7, 8$, guess the 8-bit value of $K_{11,l}$. Partially decrypt the ciphertext $(C_{R,l}, C'_{R,l})$ and keep only the pairs which satisfy $\Delta S_{11,l} = h'_l$. The expected number of remaining pairs is $2^{63.64}$.
   (b) Guess the 8-bit value $K_{11,5}$. Partially decrypt the ciphertext $(C_{R,5}, C'_{R,5})$, then compute the intermediate value (R_{10}, R'_{10}), where $\Delta R_{10} = (0|f|f|f|0|f|f|f)$ and $f = \Delta S_{11,5} \oplus h'_5$.
3. Application of the 10-round attack.
   (a) Guess the 8-bit value $K_{10,8}$, partially decrypt $(R_{10,8}, R'_{10,8})$ and discard the pairs whose intermediate values do not satisfy $\Delta S_{10,8} = g'_8$. The expected number of remaining pairs is $2^{63.64} \times 2^{-8} = 2^{55.64}$.
   (b) For $l = 2, 3, 4, 6, 7$, guess the 8-bit value $K_{10,l}$. Partially decrypt the intermediate value $(R_{10,l}, R'_{10,l})$ and keep only the pairs whose intermediate values satisfy $\Delta S_{10,l} = g'_l \oplus g'_5$. The expected number of remaining pairs is $2^{15.64}$.

(c) Guess the 8-bit value $K_{10,1}$, partially decrypt the intermediate value $R_{10,1}$ and calculate the intermediate values $(R_{9,5}, R'_{9,5})$. Discard the pairs whose intermediate values do not satisfy $\Delta R^{(1)}_{9,5} = 0$. Then the expected number of remaining pairs is $2^{14.64}$.

(d) Guess the 8-bit value $K_{9,5}$, partially decrypt the intermediate value $(R_{9,5}, R'_{9,5})$ to get the difference $\Delta S_{9,5}$. If there is a pair satisfies $\Delta S_{9,5} = \Delta R_{10,2}$, we discard the guessed key and try another one. Otherwise we exhaustively search for the remaining 48 bits of K_L and K_R under this key, if the correct key is obtained, we halt the attack; otherwise, another key should be tried.

Complexity. The data complexity of the attack is $2^{112.64}$ chosen plaintexts. The time complexity is dominated by step 3 (d) which requires about $2^{144} \times (1 + (1-2^{-8}) + (1-2^{-8})^2 + ... + (1-2^{-8})^{2^{13.7}-1}) \times 2 \times \frac{1}{11} \times \frac{1}{8} \approx 2^{146.54}$ 11-round encryptions. The memory complexity is about $2^{133.56} \times 4 \times 2^4 = 2^{141.64}$ bytes.

Reduce the Time Complexity to $2^{138.54}$. Assume 16-bit value α_2 and β_2 are fixed in data collection phase of above attack, then we can collect $2^{n+31} \times 2^{-8} = 2^{n+23}$ pairs, where n represents the number of structures. Nevertheless, it is unnecessary for us to guess 8-bit subkey $K_{1,5}$ in this case. Then there are totally 136-bit values of subkey to be guessed in the attack, therefore, the expected number of remaining guesses of target subkey is about $\epsilon = 2^{136} \times (1-2^{-8})^{2^{n-90}}$ after the attack. If we chose $\epsilon = 1$, n is 104.56. Then the data complexity increases to $2^{n+16} = 2^{120.56}$, but the time complexity reduces to $2^{138.54}$, the memory requirement reduces to $2^{133.56}$ bytes.

Extending the Attack to the Whole Key Space. Similar to 10-round attack on Camellia-128, we mount a multiplied attack on Camellia-192 for the whole key space. The time complexity is about $4 \times 2^{146.54} + 2^{192} \times (1 - \frac{3}{4})^4 = 2^{184}$ 10-round encryptions. The data and memory complexities are approximately $2^{114.64}$ chosen plaintexts and $2^{141.64}$ bytes, respectively.

3.4 The Attack on 12-Round Camellia-256

We add one round on the bottom of 11-round attack, and present a 12-round attack on Camellia-256. The attack procedure is similar to the 11-round attack. First choose $2^{81.17}$ structures and collect $2^{144.17}$ plaintext-ciphertext pairs in data collection phase. After guessing the subkey $K_{1,\{1,5\}}$, we guess the 64-bit value K_{12} and compute the intermediate value (R_{11}, R'_{11}), then apply the 11-round attack to perform the remaining steps. In summary, the proposed attack requires $2^{81.17+32} = 2^{113.17}$ chosen plaintexts. The time complexity is about $2^{210.55}$ 12-round encryptions, and the memory requirement is about $2^{150.17}$ bytes. Similar to the above subsection, the time complexity and memory requirement can also reduce to $2^{202.55}$ and $2^{142.12}$, respectively, but data complexity increases to $2^{121.12}$ in this case.

We also construct another type of impossible differential attack of Camellia-256, which adds four rounds on the top and one round on the bottom of the **2+5 WKID** (see section 3.1). The attack is performed under the chosen ciphertext attack scenario. Similar to the attack based on the **5+2 WKID**, the data and time complexity are about $2^{113.17}$ and $2^{216.3}$, respectively.

Extending the Attack to the Whole Key Space. On the basis of two types of impossible differential attacks for weak keys, we mount a multiplied attack on 12-round Camellia-256 for the whole key space as below.

- **Phases 1 to 8.** Preform impossible differential attacks by using of all conditional impossible differentials **2+5 WKID** list in section 3.1. For each phase, if success, output the actual key, else perform the next phase.
- **Phase 9.** Announce 16-bit value of the master key $K_R^{(31,39,47,55,95,103,111,119)}$ $= 0$ and $K_R^{(6,14,22,30,70,78,86,94)} = 1$, then exhaustively search for the remaining 240-bit value of K_R, K_L and recover the actual key.

The expected time of the attack is $2^{216.3} \times 8 + 2^{256} \times (\frac{1}{4})^8 \approx 2^{240}$ encryptions, and the expected data complexity is about $2^{116.17}$.

3.5 The Attacks Including Two FL/FL^{-1} Layers

If we do not start from the first round, we can take the attacks that include two FL/FL^{-1} layers into account. By exploiting some new properties of FL and FL^{-1}, we mount impossible differential attacks on variants of 14-round Camellia-256 and 12-round Camellia-192. Specifically, we attack 14-round Camellia-256 from round 10 to round 23 with about 2^{120} chosen ciphertexts, $2^{250.5}$ 14-round encryptions and 2^{125} bytes of memory, and 12-round Camellia-192 from round 3 to round 14 with about $2^{120.1}$ chosen plaintexts, $2^{180.1}$ 12-round encryptions and $2^{124.1}$ bytes of memory. The detailed information can be found in [13].

4 8-Round Impossible Differentials of Camellia and Their Applications[2]

In this section, we first present a method to construct a set of differentials, which contains at least one 8-round impossible differential of Camellia with two FL/FL^{-1} layers for any fixed key. Based on this set of differentials, we propose a new strategy to attack on reduced-round Camellia-128/192/256 with the whitening and FL/FL^{-1} layers.

4.1 The Construction of 8-Round Impossible Differentials of Camellia

We first illustrate some properties of FL/FL^{-1}.

[2] By Ya Liu, Dawu Gu, Zhiqiang Liu and Wei Li.

Proposition 4. *If the input difference of FL is $(a|0|0|0|a'|0|0|0)$, where $a^{(1)} = a'^{(8)} = 0$ and*

$$a'^{(i)} = \begin{cases} 0, & kl_L^{(i+1)} = 0; \\ a^{(i+1)}, & kl_L^{(i+1)} = 1; \end{cases} \quad \textit{for } 1 \leq i \leq 7,$$

then the output difference of FL is $(a|0|0|0|0|0|0|0)$.

By Propositions 4, we construct an 8-round impossible differential of Camellia with two FL/FL^{-1} layers for any fixed subkey.

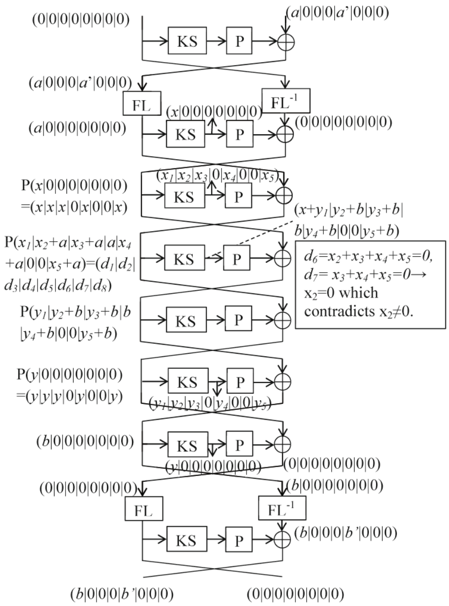

Fig. 3. The Structure of 8-Round Impossible Differential of Camellia

Proposition 5. *For an 8-round Camellia encryption with two FL/FL^{-1} layers inserted after the first and seventh rounds, the input difference of the first round is $(0|0|0|0|0|0|0|0, a|0|0|0|a'|0|0|0)$ and the output difference of the eighth round is $(b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$ with a and b being nonzero bytes and $a^{(1)} = b^{(1)} = a'^{(8)} = a'^{(8)} = 0$. Four subkeys $kl_i (i = 1, \cdots, 4)$ are used in two FL/FL^{-1} layers. If a' and b' satisfy the following equations:*

$$a'^{(i)} = \begin{cases} 0, & \textit{if } kl_1^{(i+1)} = 0; \\ a^{(i+1)}, & \textit{if } kl_1^{(i+1)} = 1; \end{cases} \quad b'^{(i)} = \begin{cases} 0, & \textit{if } kl_4^{(i+1)} = 0; \\ b^{(i+1)}, & \textit{if } kl_4^{(i+1)} = 1; \end{cases} \quad \textit{for } 1 \leq i \leq 7,$$

then $(0|0|0|0|0|0|0|0, a|0|0|0|a'|0|0|0) \nrightarrow_8 (b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$ is an 8-round impossible differential of Camellia with two FL/FL^{-1} layers (See Fig. 3).

For any fixed subkey, an 8-round impossible differential with two FL/FL^{-1} layers can be constructed. Each possible value of $kl_1^{(2\sim8)} \mid kl_4^{(2\sim8)}$ corresponds to the existence of an 8-round impossible differential. All possible values of $kl_1^{(2\sim8)} \mid kl_4^{(2\sim8)}$ are from $0_{(14)}$ to $1_{(14)}$. Denote their corresponding impossible differentials by Δ_i for $0 \leq i \leq 2^{14}-1$. Let A be a set including all differentials $\Delta_i (0 \leq i \leq 2^{14}-1)$, i.e., $A = \{\Delta_i \mid 0 \leq i \leq 2^{14}-1\}$. According to Proposition 5, 8-round differentials of A must have the form: $\Delta = (0|0|0|0|0|0|0|0, a|0|0|0|a'|0|0|0) \nrightarrow_8 (b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$ with a and b being nonzero bytes and $a^{(1)} = b^{(1)} = a'^{(8)} = b'^{(8)} = 0$. Among them, a' and b' are either zero or nonzero bytes. We divide all differentials of A into three cases: (1) $a' = b' = 0$, (2) $a' = 0$ and $b' \neq 0$, or $a' \neq 0$ and $b' = 0$, (3) $a' \neq 0$ and $b' \neq 0$.

By proposition 5, we only know the existence of an 8-round impossible differential of Camellia with two FL/FL^{-1} layers for any fixed key, but cannot distinguish it from other differentials of A. Therefore, we require to propose a new attack strategy to recover the correct key based on this set of differentials.

The Attack Strategy. Select a differential Δ_i from A. Based on it, we mount an impossible differential attack on reduced-round Camellia given enough plaintext pairs.

1. If one subkey will be kept, we recover the secret key by the key schedule and verify whether it is correct by some plaintext-ciphertext pairs. If success, halt this attack. Otherwise, try another differential $\Delta_j (j \neq i)$ of A and perform a new impossible differential attack.
2. If no subkeys or more than one subkeys are left, select another differential of A to execute a new impossible differential attack.

Our attack strategy can really recover the correct key. As a matter of fact, if Δ_i is an impossible differential, we make sure the expected number of remaining wrong keys will be almost zero given enough chosen plaintexts. Therefore, we only consider those differentials which result in one subkey remaining. By Proposition 5, we know the set A contains at least one impossible differential. So we try each differential of A until the correct key is recovered. The worst scenario is that the correct key is retrieved from the last try.

4.2 Impossible Differential Attack on 13-Round Camellia-256

Based on three scenarios of differentials in A, we present an impossible differential attack on 13-round Camellia-256 with the FL/FL^{-1} and whitening layers from rounds 4 to 16. Let $k_a \triangleq kw_1 \oplus k_4, k_b \triangleq kw_2 \oplus k_5, k_c \triangleq kw_4 \oplus k_{16}, k_d \triangleq kw_3 \oplus k_{15}, k_e \triangleq kw_4 \oplus k_{14}$. We use these equivalent subkeys k_a, k_b, k_c, k_d and k_e instead of the round subkeys k_4, k_5, k_{14}, k_{15} and k_{16} so as to remove the whitening layers. In the following, we will illustrate this attack.

Case 1 $a' = b' = 0$**:** The differential $\Delta = (0|0|0|0|0|0|0|0, a|0|0|0|0|0|0|0) \nrightarrow_8 (b|0|0|0|0|0|0|0, 0|0|0|0|0|0|0|0)$, where a and b are nonzero bytes and $a^{(1)} = b^{(1)} = 0$ (See Fig. 4).

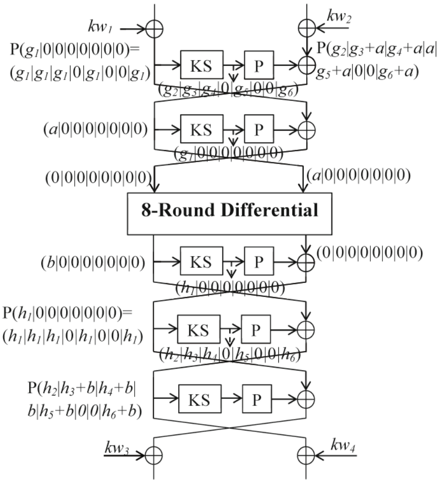

Fig. 4. Impossible Differential Attack on 13-round Camellia-256 for Case 1

Data Collection. Select a structure of plaintexts, which contains 2^{55} plaintexts with the following form:

$$(P(\alpha_1|x_1|x_2|x_3|x_4|x_5|x_6|x_7), P(\alpha_2|\alpha_3|\alpha_4|\alpha_5|\alpha_6|x_8|x_9|\alpha_7)), \qquad (1)$$

where $\alpha_5^{(1)}, x_i(1 \leq i \leq 9)$ are fixed and $\alpha_j(1 \leq j \leq 7, i \neq 5), \alpha_5^{(2\sim8)}$ takes all possible values. Clearly, each structure forms 2^{109} plaintext pairs, the differences of which have the form: $(P(g_1|0|0|0|0|0|0|0), P(g_2|g_3 \oplus a|g_4 \oplus a|a|g_5 \oplus a|0|0|g_6 \oplus a))$ with a and $g_i(1 \leq i \leq 6)$ being nonzero bytes and $a^{(1)}$=0. We take all possible values of $(\alpha_5^{(1)}, x_4, x_8, x_9)$ and 2^{43} different values of $x_i(1 \leq i \leq 7, i \neq 4)$ to derive 2^{68} special structures. In total, there are 2^{123} chosen plaintexts which form 2^{177} plaintext pairs. Encrypt these plaintext pairs to obtain the corresponding ciphertext pairs. If the right halves of their ciphertexts differences have the form: $P(h_1|h_2 \oplus b|h_3 \oplus b|b|h_5 \oplus b|0|0|h_8 \oplus b)$ with $b^{(1)} = 0$, then these pairs will be kept. The expected number of remaining pairs is about 2^{160}.

Key Recovery

1. Guess $k_{a,1}$. For each remaining pair, check whether the equation $\Delta S_{4,1} = (P^{-1}(\Delta P_R))_1$ holds. If $\Delta S_{4,1} \neq (P^{-1}(\Delta P_R))_1$ for some pair, then this pair will be discarded. Next guess each possible value of $k_{a,l}$ for $l = 2, 3, 5, 8$. Keep only the pairs satisfying $\Delta S_{4,l} = (P^{-1}(\Delta P_R))_l \oplus (P^{-1}(\Delta P_R))_4$. The expected number of remaining pairs is about 2^{120}. Finally, guess $k_{a,\{4,6,7\}}$ and compute the inputs of the fifth round for each remaining pair.
2. Guess $k_{b,1}$ and test whether $\Delta S_{5,1}$ is equal to $(P^{-1}(\Delta P_L))_1$ for each remaining pair. If $\Delta S_{5,1} \neq (P^{-1}(\Delta P_L))_1$ for one pair, then this pair will be removed. Finally, about 2^{112} pairs will be kept.

3. Guess $k_{c,l}$ for $2 \leq l \leq 8$. Verify whether $\Delta S_{16,l}$ is equal to $(P^{-1}(\Delta C_L))_l$ for every remaining pair. If $\Delta S_{16,l} \neq (P^{-1}(\Delta C_L))_l$ for some pair, then this pair is discarded. The expected number of remaining pairs is about 2^{56}. Next guess $k_{c,1}$ and compute the outputs of the 15-th round for each remaining pair.
4. Guess $k_{d,l}$ for $l = 1, 2, 3, 5, 8$. For each remaining pair, verify whether the equations $\Delta S_{15,1} = (P^{-1}(\Delta C_R))_1$ and $\Delta S_{15,j} = (P^{-1}(\Delta C_R))_j \oplus (P^{-1}(\Delta C_R))_4$ $(j = 2, 3, 5, 8)$ hold. The probability that to happen is about 2^{-40}. Thus about 2^{16} pairs will be kept. Next guess other bytes of k_d and calculate the outputs of the 14-th round.
5. Guess $k_{e,1}$ and compute the output difference of the S-Boxes in the 14-th round. If $\Delta S_{14,1}$ is equal to $(P^{-1}(\Delta L_{14}))_1$, then we remove this value of $k_{e,1}$ with $(k_a, k_{b,1}, k_c, k_d)$. The probability of this event is about 2^{-8}. After trying all possible values of $(k_a, k_{b,1}, k_c, k_d, k_{e,1})$, if only one joint subkey remains, then Δ is likely to be an impossible differential. At this time, we recover the secret key by the key schedule and verify whether it is correct by some plaintext-ciphertext pairs. If no subkeys or more than one subkeys are left, then Δ is possible to exist. At this time, try another differential of A. As a matter of fact, if Δ is an impossible differential, the expected number of remaining wrong subkeys is about $2^{208} \times (1 - 2^{-8})^{2^{16}} \approx 2^{-161.4}$. We consider that all wrong subkeys are removed and only the correct subkey is left. Therefore, we require to perform the following step only if one subkey will be kept.
6. According to the key schedule of Camellia-256, we can recover the secret key from this unique 208-bit subkey $(k_a, k_{b,1}, k_c, k_d, k_{e,1})$. As a matter of fact, we guess K_B and K_R, and then calculate K_L and K_A by property 4 of [18]. Finally, the number of remaining main keys is approximately 2^{48}. By about 2^{48} trail encryptions, if some key is correct, stop the attack. Otherwise, try another differential of A.

Case 2 $a' = 0$ and $b' \neq 0$, or $a' \neq 0$ and $b' = 0$: We only attack a special scenario, i.e., $a' = 0$ and $b'^{(1\sim7)} = b^{(2\sim8)}$. Others can be attacked in the similar way. At this time, the differential is $\Delta' = (0|0|0|0|0|0|0|0, a|0|0|0|0|0|0|0) \rightarrow_8 (b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$, where a, b and b' are non-zero bytes, $b'^{(1\sim7)} = b^{(2\sim8)}$ and $a^{(1)} = b^{(1)} = b'^{(8)} = 0$.

Data Collection. We apply 2^{68} special structures of above Case 1. Totally, there are 2^{123} chosen plaintexts which form 2^{177} pairs.

Key Recovery

1. Guess $k_{c,l}$ for $2 \leq l \leq 8$ and $l \neq 5$. Verify whether the equation $\Delta S_{16,l} = (P^{-1}(\Delta C_L))_l$ holds for every remaining pair. If $\Delta S_{16,l} \neq (P^{-1}(\Delta C_L))_l$ for some pair, then this pair is discarded. The expected number of remaining pairs is about 2^{129}. Next guess $k_{c,\{1,5\}}$ and compute the outputs of the 15-th round for each remaining pair.

2. We first guess $k_{d,1}$ and check whether the equation $\Delta S_{15,1} = (P^{-1}(\Delta C_R))_1$ holds for each remaining pair. If $\Delta S_{15,1} \neq (P^{-1}(\Delta C_R))_1$ for one pair, then this pair will be removed. Next guess $k_{d,8}$ and keep only the pairs satisfying $\Delta S^{(1)}_{15,8} = (P^{-1}(\Delta C_R))^{(1)}_8$. Finally, guess $k_{d,\{2\sim 7\}}$. Test whether $\Delta S_{15,l} = (P^{-1}(\Delta C_R))_l \oplus (((P^{-1}(\Delta C_R))_8 \oplus \Delta S_{15,8})^{(2\sim 8)}|0)$ for $l = 6, 7$ and $\Delta S_{15,l} = (P^{-1}(\Delta C_R))_l \oplus (P^{-1}(\Delta C_R))_8 \oplus \Delta S_{15,8} \oplus (P^{-1}(\Delta C_R))_7 \oplus \Delta S_{15,7}$ for $l = 2, 3, 4, 5$. The total probability of this step is about 2^{-57}. So the expected number of remaining pairs is approximately 2^{72}. Compute the outputs of the 14-th round for each remaining pair.
3. Guess $k_{e,l}$ for $l = 1, 5$. Verify whether the equation $\Delta S_{14,l} = (P^{-1}(\Delta L_{14}))_l$ holds for each remaining pair. If this equation is correct for some pair, then this pair will be kept. The probability of this event is about 2^{-16}. About 2^{56} pairs will be kept.
4. Guess each possible value of k_a as like Case 1. The expected number of remaining pairs is about 2^{16}. Calculate the inputs of the fifth round.
5. Guess $k_{b,1}$. This step is similar to Step 5 of Case 1. If only one joint subkey is left, then we consider Δ' is an impossible differential and recover the secret key by the key schedule. Otherwise try another differential of A. In fact, the expected number of remaining wrong subkeys is approximately $2^{216} \times (1 - 2^{-8})^{2^{16}} \approx 2^{-153.4}$ if Δ' is an impossible differential.
6. This step is similar to Step 6 of Case 1. Finally, about 2^{40} keys will be left. By about 2^{40} trail encryptions, if some key is correct, stop the attack. Otherwise, try another differential of A.

Case 3 $a' \neq 0$ and $b' \neq 0$: We only discuss an example, i.e., $a'^{(1\sim 7)} = a^{(2\sim 8)}$ and $b'^{(1\sim 7)} = b^{(2\sim 8)}$. The differential is $\Delta'' = (0|0|0|0|0|0|0|0, a|0|0|0|a'|0|0|0) \rightarrow_8 (b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$, where a, b, a' and b' are nonzero bytes and $a^{(1)} = b^{(1)} = a'^{(8)} = b'^{(8)} = 0$.

Data Collection. Continue to adopt 2^{123} chosen plaintexts of Case 1. Because each structure of Case 1 takes all possible values of $\alpha^{(1)}_5, x_4, x_8$ and x_9, 2^{123} chosen plaintexts of Case 1 are equivalent to 2^{43} structures, each of which contains 2^{80} plaintexts with the form: $(P(\beta_1|y_1|y_2|y_3|\beta_2|y_4|\ y_5|y_6), \beta_3|\beta_4|\beta_5|\beta_6|\beta_7|\beta_8|\beta_9|\beta_{10})$, where $y_i (1 \leq i \leq 6)$ are fixed and $\beta_j (1 \leq j \leq 10)$ takes all possible values. It is obvious that one structure generates 2^{159} pairs. Totally, there are approximately 2^{202} plaintext pairs satisfying the input differences.

Key Recovery

1. Guess each byte of $k_c, k_d, k_{e,\{1,5\}}$. This step is similar to above Case 2. After this step, about 2^{81} pairs will be kept.
2. Guess $k_{a,1}$, $k_{a,8}$, $k_{a,\{6,7\}}, k_{a,\{2\sim 5\}}$ and $k_{b,5}$ in turn. The expected number of remaining pairs is about 2^{16}. Compute the inputs of the 5-th round for each remaining pair.
3. Guess $k_{b,1}$ and test whether $\Delta S_{5,1}$ is equal to $(P^{-1}(\Delta P_L))_1$ for each remaining pair. If $\Delta S_{5,1} = (P^{-1}(\Delta P_L))_1$ for some pair, then this guessed key are

removed. After guessing all possible subkeys, if only one joint subkey is left, then we consider Δ'' is an impossible differential. At this moment, we execute the following step. Otherwise try another differential of A. As a matter of fact, the expected number of remaining wrong subkeys is approximately $2^{224} \times (1-2^{-8})^{2^{16}} \approx 2^{-145.4}$ if Δ'' is an impossible differential.

4. Similarly, we recover the secret key from this subkey. The number of remaining main keys is approximately 2^{32}. By about 2^{32} trail encryptions, if some key is correct, stop the attack. Otherwise, try another differential of A.

Complexity. We calculate that the total time complexities of Cases 1 to 3 are about 2^{216} 1-round encryptions, 2^{224} 1-round encryptions and $2^{240.8}$ 1-round encryptions, respectively. Thus the total time complexity is at most $2^{14} \times 2^{240.8} \times \frac{1}{13} \approx 2^{251.1}$ 13-round encryptions. Furthermore, the total data and memory complexities are 2^{123} chosen plaintexts and 2^{208} bytes, respectively.

4.3 Impossible Differential Attack on 12-Round Camellia-192

In this section, we attack 12-round Camellia-192 from rounds 4 to 15 with the 8-round differentials inserted rounds 6 to 13. Some equivalent subkeys k_a and k_b are defined as before. In addition, let $k'_d = kw_4 \oplus k_{15}$ and $k'_e = kw_3 \oplus k_{14}$.

Case 1 $a' = b' = 0$: The differential is Δ.

We select the same plaintexts of Case 1 mentioned in section 4.2, i.e., 2^{123} chosen plaintexts and 2^{177} pairs. Encrypt them and keep those pairs whose ciphertext differences have the form: $(P(h_2|h_3 \oplus b|h_4 \oplus b|b|h_5 \oplus b|0|0|h_6 \oplus b), P(h_1|0|0|0|0|0|0|0))$, where b and $h_i (1 \le i \le 6)$ are nonzero bytes and $b^{(1)} = 0$. The expected number of remaining pairs is about 2^{104}.

Guess all possible values $(k_a, k_{b,1}, k'_d, k'_{e,1})$ and discard those subkeys which acquire the input and output differences of Δ. This step is similar to section 4.2. If Δ is an impossible differential, about $2^{144} \times (1-2^{-8})^{2^{16}} \approx 2^{-225.4}$ wrong subkeys are expected to remain. Therefore, we will recover the secret key by the key schedule of Camellia-192 only if one subkey is left. Otherwise, try another differential of A. By the key schedule of Camellia-192, we derive 2^{48} candidates of the secret key from the 144-bit subkey $(k_a, k_{b,1}, k'_d, k'_{e,1})$. By about 2^{48} trail encryptions, if the correct key is retrieved, halt the attack. Otherwise, try another differential of A.

Case 2 $a' = 0, b' \neq 0$ or $a' \neq 0, b' = 0$: For simplicity, we consider a special differential Δ'.

We still select 2^{123} plaintexts of above Case 1. In total, there are 2^{68} special structures, each of which contains 2^{55} plaintexts. Encrypt these plaintext pairs. If the right halves of their ciphertexts differences have the form: $P(h|0|0|0|h'|0|0|0)$ with h and h' being nonzero bytes, then these pairs will be kept. Consequently, the expected number of remaining pairs is about 2^{129}. Similarly, we can remove some subkeys $(k_a, k_{b,1}, k'_d, k'_{e,\{1,5\}})$ which obtain the input and output differences of Δ' for some pair. If only one subkey is left, we recover the secret key by the key schedule. Otherwise, try another differential of A. In fact, if $\varDelta'$ is an impossible differential, about $2^{-217.4}(\approx 2^{152} \times (1-2^{-8})^{2^{16}})$ wrong subkeys will be left.

Case 3 $a' \neq 0, b' \neq 0$ **:** A special differential $\varDelta''$ will be considered.

The similar attacking procedure can be performed as before. We select 2^{43} structure, each of which contains 2^{80} plaintexts. Totally, they can form 2^{202} pairs. After filtering some pairs by the ciphertext differences, about 2^{154} pairs are expected to remain. The following steps can be preformed in the similar way.

We found that the time complexity of Case 3 is maximal. Therefore, the total time complexity is at most $2^{14} \times 2^{173.2} \approx 2^{187.2}$ 12-round encryptions. The data and memory complexities are 2^{123} chosen plaintexts and 2^{160} bytes, respectively.

4.4 Impossible Differential Attack on 11-Round Camellia-128

For Camellia-128, we put two additional rounds on the top and one additional round on the bottom of 8-round differentials. Based on it, we attack 11-round Camellia-128 from rounds 4 to 14. Similarly, we divide all possible differentials into three different cases as before. For Case 1, we take 2^{67} special structures (1). Totally, the data complexity is 2^{122} chosen plaintexts which form 2^{176} pairs. Encrypt these pairs to acquire the corresponding ciphertext pairs. Then we discard some pairs whose ciphertext differences don't satisfy this form: $(P(h|0|0|0|0|0|0|0), b|0|0|0|0|0|0|0)$ with b and h being non-zero bytes and $b^{(1)} = 0$. The number of remaining pairs after this test is about 2^{63}. Guess $k_{e,1}, k_a$ and $k_{b,1}$ in turn and operate the similar steps. If only one subkey is left, we retrieve the secret key by the key schedule. Otherwise, try anther differential of A. As a matter of fact, if $\varDelta$ is an impossible differential, the expected number of remaining pairs is about $2^{80} \times (1-2^{-8})^{15} \approx 2^{-104.7}$. For other two cases, we execute the similar attack procedure.

We find that the dominant time complexity of all steps in three cases is the data collection. Therefore, the total data, time and memory complexities are 2^{122} chosen plaintexts, 2^{122} 11-round encryptions and 2^{102} bytes, respectively.

5 Conclusion

In this paper, we have presented new insight on impossible differential cryptanalysis of reduced-round Camellia with the FL/FL^{-1} and whitening layers. First, we propose impossible differential attacks on reduced-round Camellia for 75% of the keys, which are then extended to attacks that work for the whole key space. As a matter of fact, we attack 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 which start from the first round and include the whitening layers. Meanwhile, we also attack 12-round Camellia-192 and 14-round Camellia-256 with two FL/FL^{-1} layers. Second, we construct a set of differentials including at least one 8-round impossible differential of Camellia with two layers FL/FL^{-1}. This impossible differential has the same length as the best known impossible differential of Camellia without the FL/FL^{-1} layer.

Therefore, our result shows that the keyed functions cannot thwart impossible differential attack effectively. On the basis of this set of differentials, we propose a new strategy to derive an effective attack on 11-round Camellia-128, 12-round Camellia-192 and 13-round Camellia-256, which do not start the first round but include the whitening and FL/FL^{-1} layers.

Acknowledgements. The authors are grateful to all anonymous reviewers for valuable suggestions and comments. The authors Ya Liu, Dawu Gu, Zhiqiang Liu and Wei Li are supported by the National Natural Science Foundation of China (No. 61073150 and No. 61003278), the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, the open research fund of State Key Laboratory of Information Security and the Fundamental Research Funds for the Central Universities. The authors Leibo Li, Xiaoyun Wang and Jiazhe Chen are supported by the National Natural Science Foundation of China (Grant No. 61133013 and No. 60931160442), and Tsinghua University Initiative Scientific Research Program (2009THZ01002).

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. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
3. 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)
4. CRYPTREC-Cryptography Research and Evaluation Committees: report. Archive (2002), `http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html`
5. Hatano, Y., Sekine, H., Kaneko, T.: Higher order differential attack of *Camellia* (II). In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 129–146. Springer, Heidelberg (2003)
6. International Standardization of Organization (ISO): International standard - ISO/IEC 18033-3. Tech. rep., Information technology - Security techniques - Encryption algrithm - Part 3: Block Ciphers (July 2005)
7. Knudsen, L.R.: DEAL - a 128-bit block cipher. Tech. rep., Department of Informatics, University of Bergen, Norway. technical report (1998)
8. Kühn, U.: Improved Cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
9. Lee, S., Hong, S., Lee, S., Lim, J., Yoon, S.: Truncated Differential Cryptanalysis of Camellia. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 32–38. Springer, Heidelberg (2002)
10. Duo, L., Chao, L., Feng, K.: New Observation on Camellia. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer, Heidelberg (2006)

11. Duo, L., Li, C., Feng, K.: Square Like Attack on Camellia. In: Qing, S., Imai, H., Wang, G. (eds.) ICICS 2007. LNCS, vol. 4861, pp. 269–283. Springer, Heidelberg (2007)
12. 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)
13. Li, L., Chen, J., Wang, X.: Security of Reduced-Round Camellia against Impossible Differential Attack. IACR Cryptology ePrint Archive 2011, 524 (2011)
14. 'Liu, Y., Gu, D., Liu, Z., Li, W., Man, Y.: Improved Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-192/256. Journal of Systems and Software (accepted)
15. Lu, J., Dunkelman, O., Keller, N., Kim, J.-S.: New Impossible Differential Attacks on AES. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 279–293. Springer, Heidelberg (2008)
16. Lu, J., Kim, J.-S., Keller, N., Dunkelman, O.: Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer, Heidelberg (2008)
17. Lu, J., Wei, Y., Kim, J., Fouque, P.-A.: Cryptanalysis of Reduced Versions of the Camellia Block Cipher. In: Preproceeding of SAC (2011)
18. Lu, J., Wei, Y., Kim, J., Pasalic, E.: The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher. In: Presented in Part at the First Asian Workshop on Symmetric Key Cryptography (ASK 2011) (August 2011), https://sites.google.com/site/jiqiang/
19. 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)
20. NESSIE: New European Schemes for Signatures, Integrity, and Encryption, final report of eurpean project IST-1999-12324. Archive (1999), http://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf
21. Shirai, T.: Differential, Linear, Boomerange and Rectangle Cryptanalysis of Reduced-Round Camellia. In: Proceedings of 3rd NESSIE Workshop, Munich, Germany, November 6-7 (2002)
22. Sugita, M., Kobara, K., Imai, H.: Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 193–207. Springer, Heidelberg (2001)
23. Wu, W., Feng, D., Chen, H.: Collision Attack and Pseudorandomness of Reduced-Round Camellia. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 252–266. Springer, Heidelberg (2004)
24. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. J. Comput. Sci. Technol. 22(3), 449–456 (2007)