Improved Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-192/256

Ya Liu[1], Dawu Gu[1], Zhiqiang Liu[1], Wei Li[2], Ying Man[1]

[1]Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, P.R. China
{liuya0611,dwgu,ilu_zq,manying1208}@sjtu.edu.cn
[2]School of Computer Science and Technology,
Donghua University, Shanghai 201620, P.R.China
liwei.cs.cn@gmail.com

Abstract. As an international standard adopted by ISO/IEC, the block cipher Camellia has been used in various cryptographic applications. In this paper, we reevaluate the security of Camellia against impossible differential cryptanalysis. Specifically, we propose several 7-round impossible differentials with the FL/FL^{-1} layers. Based on them, we mount impossible differential attacks on 11-round Camellia-192 and 12-round Camellia-256. The data complexities of our attacks on 11-round Camellia-192 and 12-round Camellia-256 are about 2^{120} chosen plaintexts and $2^{119.8}$ chosen plaintexts, respectively. The corresponding time complexities are approximately $2^{167.1}$ 11-round encryptions and $2^{220.87}$ 12-round encryptions. As far as we know, our attacks are $2^{16.9}$ times and $2^{19.13}$ times faster than the previously best known ones but have slightly more data.

Key words: Block Cipher, Camellia, Impossible Differential Cryptanalysis

1 Introduction

The block cipher Camellia was jointly proposed by NTT and Mitsubishi Electric Corporations [1]. It was then submitted to several standardization and evaluation projects such as the NESSIE Project and the Japanese CRYPTREC Evaluation. In 2002, Camellia was selected to be a CRYPTREC e-government recommended block cipher [4]. In 2003, it was also recommended in the NESSIE block cipher portfolio [19]. Finally, it was adopted as a new international standard by ISO/IEC in 2005 [7]. Camellia is a 128-bit block cipher. It supports 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. For simplicity, they are usually denoted by Camellia-128, Camellia-192 and Camellia-256. Camellia uses the basic Feistel structure with the FL/FL^{-1} layers inserted every 6 rounds. Those transformations FL/FL^{-1} are related to the key value, which is expected to make the cryptanalysis of Camellia much harder.

As one of the most widely used block ciphers, Camellia has drawn a great amount of attention from many researchers. Up to now, a lot of research work has been done to evaluate the security of Camellia by means of various cryptanalytic methods such as linear and differential cryptanalysis, truncated differential cryptanalysis, higher order differential cryptanalysis, collision attacks, square attacks, integral attacks and impossible differential cryptanalysis. Among them, most work [20, 9, 8, 22, 12, 18, 16] focused on the study of the security of a simple version of Camellia (i.e., Camellia without FL/FL^{-1} or whitening layers), and only a few [11, 6, 3, 14] involved in the security analysis of Camellia with the FL/FL^{-1} and whitening layers (Called Camellia for short). For instance, Duo *et al.* presented a square attack on 10-round Camellia-256 which required 2^{48} chosen plaintexts and

2^{210} 10-round encryptions, Hatano *et al.* proposed a higher order differential attack on the last 11 rounds of Camellia-256 with 2^{93} chosen ciphertexts and $2^{255.6}$ 11-round encryptions, Chen *et al.* constructed some 6-round impossible differentials which were used to mount impossible differential attacks on 10-round Camellia-192 with about 2^{121} chosen plaintexts and $2^{175.3}$ 10-round encryptions and 11-round Camellia-256 with approximately 2^{121} chosen plaintexts and $2^{206.8}$ 11-round encryptions, Li *et al* gave some 7-round conditional impossible differentials (i.e., there is a 75% probability that each of them is impossible), which could be used to attack 10-round Camellia-128 with $2^{112.4}$ chosen plaintexts and 2^{120} 10-round encryptions, 11-round Camellia-192 with $2^{113.7}$ chosen plaintexts and 2^{184} 11-round encryptions as well as 12-round Camellia-256 with $2^{114.8}$ chosen plaintexts and 2^{240} 12-round encryptions.

Impossible differential cryptanalysis, which is a variant of differential cryptanalysis, was independently proposed by Knudsen [10] and Biham *et al.* [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. Impossible differential cryptanalysis has received much attention and has been used to attack a variety of well-known block ciphers such as AES, ARIA, CLEFIA and MISTY1 [15, 17, 21, 5].

In this paper, we reappraise the security of Camellia against impossible differential attacks. Firstly, we exploit the properties of the functions FL/FL^{-1} and propose several 7-round impossible differentials of Camellia. Based on them, we successfully mount an impossible differential attack on 11-round Camellia-256. The data, time and memory complexities of our attack are approximately $2^{120.06}$ chosen plaintexts, $2^{196.4}$ 11-round encryptions and $2^{133.06}$ bytes, respectively. Then, we further improve our results and present impossible differential attacks on 11 rounds of Camellia-192 and 12 rounds of Camellia-256. For 11 rounds of Camellia-192, our attack requires about 2^{120} chosen plaintexts, $2^{167.1}$ 11-round encryptions and 2^{149} bytes of memory. For 12 rounds of Camellia-256, our attack needs approximately $2^{119.8}$ chosen plaintexts, $2^{220.87}$ 12-round encryptions and $2^{156.8}$ bytes of memory. Compared with the previously latest results on 11-round Camellia-192 and 12-round Camellia-256, the time complexities of our attacks are reduced by $2^{16.9}$ times and $2^{19.13}$ times and the data and memory complexities are comparable. In table 1, we summarize our results along with the former known ones on Camellia.

Table 1. Summary of the attacks on Camellia-192/256

Cipher	Rounds	Attack Type	Data (Enc)	Time (Bytes)	Memory	Source
Camellia-192	10	Impossible DC	2^{121}CP	$2^{175.3}$	$2^{155.2}$	[3]
	10	Impossible DC	$2^{118.7}$CP	$2^{130.4}$	2^{135}	[13]
	11*	Impossible DC	$2^{119.5}$CP	$2^{138.54}$	$2^{135.5}$	[14]
	11	Impossible DC	$2^{113.7}$CP	2^{184}	$2^{143.7}$	[14]
	11	Impossible DC	2^{120}CP	$2^{167.1}$	2^{149}	Section 5.2
Camellia-256	11	High Order DC	2^{93}CC	$2^{255.6}$	2^{98}	[6]
	11	Impossible DC	2^{121}CP	$2^{206.8}$	2^{166}	[3]
	11	Impossible DC	$2^{119.6}$CP	$2^{194.5}$	2^{135}	[13]
	11	Impossible DC	$2^{120.06}$CP	$2^{196.4}$	$2^{133.06}$	Section 4
	12*	Impossible DC	$2^{119.7}$CP	$2^{202.55}$	$2^{143.7}$	[14]
	12	Impossible DC	$2^{114.8}$CP	2^{240}	$2^{151.8}$	[14]
	12	Impossible DC	$2^{119.8}$CP	$2^{220.87}$	$2^{156.8}$	Section 5.1

DC: Differential Cryptanalysis; CC: Chosen Ciphertext; CP: Chosen Plaintext;
Enc: Encryptions; *: The success probability of that attack is 75%.

The remainder of this paper is organized as follows. Section 2 gives some notations, a brief description of Camellia and some results on impossible differential cryptanalysis of reduced-round Camellia. Section 3 proposes several 7-round impossible differentials of Camellia with the FL/FL^{-1} layers. Section 4 describes an impossible differential attack on 11-round Camellia-256. Section 5 presents impossible differential attacks on 11 rounds of Camellia-192 and 12 rounds of Camellia-256. Section 6 summarizes this paper.

2 Preliminaries

In this section, we first illustrate some notations. Then we briefly describe the encryption procedure and key schedule of Camellia. Finally, we list some results on impossible differential cryptanalysis of reduced-round Camellia.

2.1 Some Notations

- P, C: the 128-bit plaintext and the 128-bit ciphertext;
- $\Delta P, \Delta C$: the differences of a plaintext pair and a ciphertext pair;
- L_{r-1}, R_{r-1}: the left and right halves of the r-th round input;
- $X \mid Y$: the concatenation of X and Y;
- $kw_1 \mid kw_2, kw_3 \mid kw_4$: the pre-whitening and post-whitening keys;
- $kl_i (1 \leq i \leq 6)$: 64-bit key used in the FL/FL^{-1} layers;
- k_r: the r-th round subkey;
- ΔL_{r-1}: the difference of L_{r-1} and L'_{r-1};
- ΔR_{r-1}: the difference of R_{r-1} and R'_{r-1};
- S_r: the output of the S-boxes in the r-th round;
- ΔS_r: 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;
- $X_{l,j}, X_{l,\{i,j\}}, X_{l,\{i\sim j\}}$: the j-th byte, the i-th and j-th bytes and the i-th to the j-th bytes of X_l;
- $\oplus, \cap, \cup$: bitwise exclusive-OR (XOR), AND, and OR operations;

2.2 Overview of Camellia

Camellia, which is a 128-bit block cipher, adopts a Feistel structure with two key-dependent functions FL/FL^{-1} inserted every 6 rounds. It 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. Before the first round and after the last round, the pre-whitening and post-whitening layers are included. Using the notations above, the whole encryption algorithm of Camellia-192/256 can be expressed as below. The basic encryption structure can been seen in Figure 1.

First, a 128-bit plaintext P is XORed with the pre-whitening key $kw_1 \mid kw_2$ to obtain the input of the first round $L_0 \mid R_0$, i.e., $L_0 \mid R_0 = P \oplus (kw_1 \mid kw_2)$. Then, for $r = 1, \cdots, 24$ and $r \neq 6, 12$ and 18,

$$L_r = R_{r-1} \oplus F(L_{r-1}, k_r), \qquad R_r = L_{r-1}.$$

For $r = 6, 12$ and 18,

$$\begin{aligned} L'_r &= R_{r-1} \oplus F(L_{r-1}, k_r), & R'_r &= L_{r-1}; \\ L_r &= FL(L'_r, kl_{r/3-1}), & R_r &= FL^{-1}(L'_r, kl_{r/3}) \end{aligned}$$

Here the round function F uses a SPN structure including the key-addition layer, the nonlinear transformation S and the linear diffusion layer P. The nonlinear transformation S uses four different 8×8 S-boxes s_1, s_2, s_3 and s_4 twice, where three S-boxes s_2, s_3 and s_4 are generated by s_1. Their definitions can be found in [1]. The linear transformation $P : (\{0,1\}^8)^8 \rightarrow (\{0,1\}^8)^8$ maps $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$ to $(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8)$. This transformation and its inverse P^{-1} are defined as follows.

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

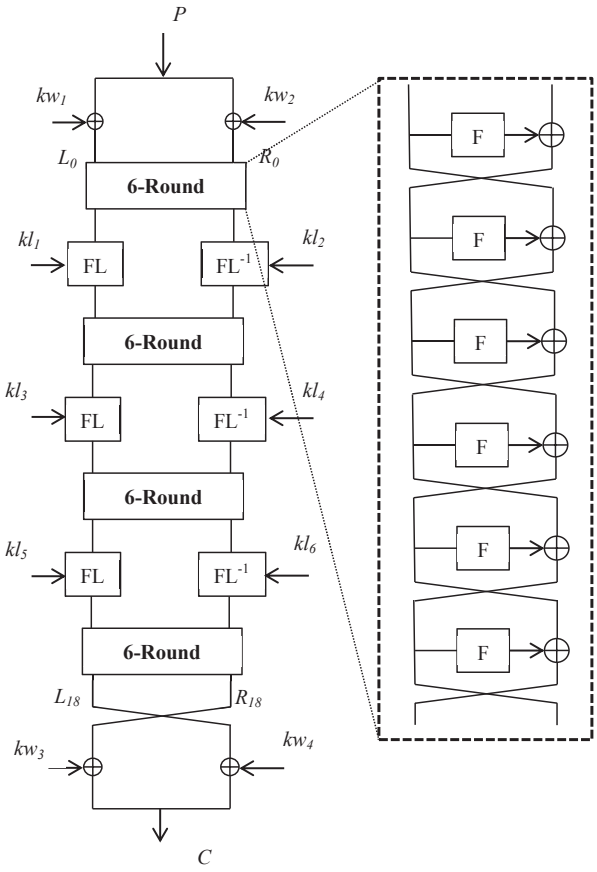

Fig. 1. The Encryption Procedure of Camellia for 192/256-bit Keys

Finally, the ciphertext C is obtained by the XOR of $R_{24} \mid L_{24}$ and the post-whitening key $kw_3 \mid kw_4$, i.e., $C = (R_{24} \mid L_{24}) \oplus (kw_3 \mid kw_4)$.

Key Schedule of Camellia-192/256 The key schedule of Camellia-192/256 applies a 6-round Feistel structure to generate two 128-bit intermediate variables K_A and K_B. These two variables K_A and K_B can be generated from two 128-bit variables K_L and K_R defined by the main key K. For Camellia-192, the left 128 bits of the key K are used as K_L, and the concatenation of the right 64 bits of the key K and the complement of the right 64 bits of the key K are 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., $K = K_L \mid K_R$. One can refer to [1].

2.3 Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia

In 2011, Chen *et al.* gave the first impossible differential cryptanalysis of Camellia [3]. They constructed several 6-round impossible differentials with FL/FL^{-1} inserted in the middle. More concretely, the input and output differences are $(0,0,0,0,0,0,0,0,0,a,0,0,0,0,0,0)$ and $(0,a,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$, which lead to a contradiction in the key-dependent functions FL/FL^{-1}. Based on it, they put three additional rounds on the top and one additional round on the bottom of their 6-round impossible differential to attack 10-round Camellia-192 with 2^{121} chosen plaintexts and $2^{175.3}$ 10-round encryptions. Moreover, they add one additional round on the bottom of 10-round Camellia-192 to attack 11-round Camellia-256 with 2^{121} chosen plaintexts and $2^{206.8}$ 11-round encryptions.

In Nov. 2011, another paper on the security of reduced-round Camellia against impossible differential attack was posted in IACR cryptology eprint archive [14]. They gave several 7-round conditional impossible differentials of Camellia, i.e., the probability that each of them is impossible is 75%. Based on them, they attacked 10-round Camellia-128 with $2^{112.4}$ chosen plaintexts and 2^{120} 10-round encryptions, 11-round Camellia-192 with $2^{113.7}$ chosen plaintexts and 2^{184} 10-round encryptions as well as 12-round Camellia-256 with $2^{114.8}$ chosen plaintexts and 2^{240} 12-round encryptions.

3 7-Round Impossible Differentials of Camellia with the FL/FL^{-1} Layers

In this section, we first give the properties of the key-dependent transformations FL/FL^{-1}. Then we propose some 7-round impossible differentials of Camellia, one of which is elaborated through a proposition as follows.

Lemma 1. *[3] Let ΔX and ΔY the input and output differences of the FL function. Then*

(1) $\Delta Y_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta X_R, \Delta Y_L = \Delta X_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R)$;
(2) $\Delta X_L = \Delta Y_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R), \Delta X_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta Y_R$.

Lemma 2. *If the output difference of the key-dependent function FL^{-1} is $(0,0,0,0,a,0,0,0)$, then its input difference has the form $(y,0,0,0,a,0,0,0)$.*

Proof. Let $(\Delta Y_L, \Delta Y_R) = FL(0,0,0,0,a,0,0,0)$. By Lemma 3.1, we calculate that $\Delta Y_R = (((0,0,0,0) \cap kl_L) \lll 1) \oplus (a,0,0,0) = (a,0,0,0)$ and $\Delta Y_L = (0,0,0,0) \oplus (a,0,0,0) \oplus ((a,0,0,0) \cap kl_R) \triangleq (y,0,0,0)$.

Proposition 1. *If the input difference of the i-th round is* $(0,0,0,0,0,0,0,0,\ 0,0,0,0,a,0,0,0)$ *and the output difference of the* $(i+6)$*-th round is* $(0,0,0,0,\ e,0,0,0,0,0,0,0,0,0,0,0)$ *with a and e being non-zero bytes, then*

$$(0,0,0,0,0,0,0,0,0,0,0,0,a,0,0,0) \rightarrow_7 (0,0,0,0,e,0,0,0,0,0,0,0,0,0,0,0)$$

is an impossible differential of Camellia with the FL/FL^{-1} layers. Here the key-dependent transformations FL/FL^{-1} are inserted after the $(i+5)$-th round. The detailed structure can be seen in Figure 2.

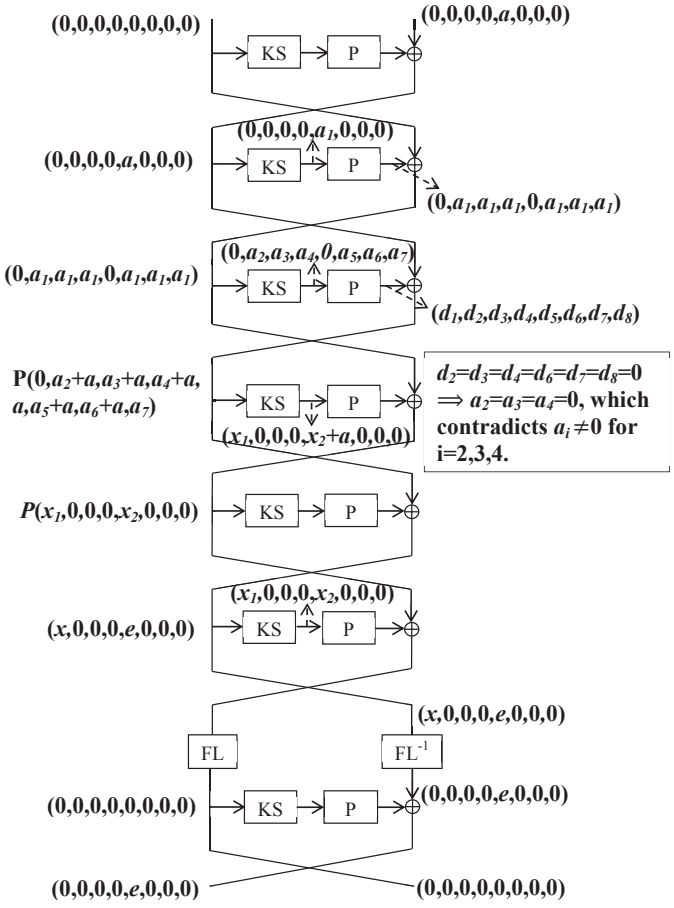

Fig. 2. A 7-Round Impossible Differential of Camellia

Proof. If the input difference of the i-th round is $(0,0,0,0,0,0,0,0,0,0,0,0,0,\ a,0,0,0)$, then the left halves of the input differences in the $(i+2)$-th and $(i+3)$-th rounds are $(0,a_1,a_1,a_1,0,a_1,a_1,a_1)$ and $(0,0,0,0,a,0,0,\ 0) \oplus P(0,a_2,a_3,\ a_4,0,a_5,a_6,a_7)$, respectively. Here $a_i (1 \leq i \leq 7)$ are non-zero bytes. Let $(0,0,0,0,a,0,0,0) \oplus P(0,a_2,a_3,a_4,0,a_5,a_6,a_7) = (z_1,z_2,z_3,z_4,z_5,\ z_6,z_7,z_8)$. By the definition

of P, we can obtain

$$\begin{aligned} z_1 &= a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7; & z_2 &= a_2 \oplus a_4 \oplus a_6 \oplus a_7; \\ z_3 &= a_2 \oplus a_3 \oplus a_5 \oplus a_7; & z_4 &= a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6; \\ z_5 &= a \oplus a_2 \oplus a_5 \oplus a_6 \oplus a_7; & z_6 &= a_2 \oplus a_3 \oplus a_6 \oplus a_7; \\ z_7 &= a_3 \oplus a_4 \oplus a_5 \oplus a_7; & z_8 &= a_4 \oplus a_5 \oplus a_6; \end{aligned}$$

On the other hand, if the output difference of the $(i+6)$-th round is $(0,0,0,0,e,0,0,0,0,0,0,0,0,0,0,0)$, then the output difference after one-round decryption is $(0,0,0,0,0,0,0,0,0,0,0,0,0,e,0,0,0)$. By Lemma 3.2, the output difference of the $(i+5)$-th round is $(0,0,0,0,0,0,0,0,x,0,0,0,e,0,0,0)$. Next decrypt $(0,0,0,0,0,0,0,0,x,0,0,0,e,0,0,\ 0)$. We can obtain the left half of the output difference in the $(i+4)$-th round is equal to $P(x_1,0,0,0,\ x_2,0,0,0)$ with x_2 being non-zero byte. Therefore, the output difference of S-boxes in the $(i+3)$-th round is $(x_1,0,0,0,x_2 \oplus a_1,0,0,0)$.

Up to now, we have obtained that the input and output differences of the S-boxes in the $(i+3)$-th round are $(z_1,z_2,z_3,z_4,z_5,z_6,z_7,z_8)$ and $(x_1,0,0,0,x_2 \oplus a_1,0,0,0)$, respectively. Then we can deduce that $z_2 = z_3 = z_4 = z_6 = z_7 = z_8 = 0$. So $a_2 = a_3 = a_4 = 0$, which contradicts $a_i \neq 0$ for $i = 2,3,4$. To summarize, $(0,0,0,0,0,0,0,0,0,0,0,0,a,0,0,0) \rightarrow_7 (0,0,0,0,e,0,0,0,0,0,0,0,0,0,0,0)$ is a 7-round impossible differential of Camellia.

Similarly, we find some other 7-round impossible differentials of Camellia with the FL/FL^{-1} layers. For example,

$$(0,0,0,0,0,0,0,0,a,0,0,0,0,0,0,0) \nrightarrow_7 (e,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),$$

$$(0,0,0,0,0,0,0,0,0,a,0,0,0,0,0,0) \nrightarrow_7 (0,e,0,0,0,0,0,0,0,0,0,0,0,0,0,0),$$

where the transformations FL/FL^{-1} are inserted between the $(i+5)$-th round and the $(i+6)$-th round. In addition, if the nonlinear layers FL/FL^{-1} are inserted after the i-th round, three differentials above are also impossible. We only demonstrate a part of all possible impossible differentials. Others can be constructed in the same way.

4 Impossible Differential Cryptanalysis of 11-round Camellia-256

Based on the 7-round impossible differentials in section 3, we present an impossible differential attack on 11-round Camellia-256. In the following, we will elaborate the whole attacking procedure.

We add four additional rounds after the 7-round impossible differential. In other words, we mount an impossible differential attack on 11-round Camellia-256 from rounds 1 to 11 by setting the 7-round impossible differential at rounds 1 to 7. The detailed structure can been seen in Figure 3. Before introducing our method, we list some notations used in this section. Let

$$k_a = kw_4 \oplus k_{11}, k_b = kw_3 \oplus k_{10}, k_c = kw_4 \oplus k_9, k_d = kw_3 \oplus k_8.$$

We use these equivalent subkeys k_a, k_b, k_c, and k_d instead of the round subkeys k_{11}, k_{10}, k_9, and k_8 so as to remove the whitening layers. This new cipher acts as the original one.

The Attacking Algorithm 1

1. Select a set of 2^8 plaintexts which has some fixed values in all bytes except for the fifth byte of its right part. Call this special set a structure, which contains some plaintexts with the following form:

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, y_1, y_2, y_3, y_4, \alpha, y_5, y_6, y_7),$$

where $x_i (1 \leq i \leq 8)$ and $y_j (1 \leq j \leq 7)$ are fixed and α takes all possible values of $\mathbb{F}_2^8$. Clearly, each structure forms about 2^{15} plaintext pairs, all bytes of the differences of which are zero except for $\Delta R_{0,5}$. Take 2^n structures. As a result, there are 2^{n+15} plaintext pairs satisfying the input difference of our proposed 7-round impossible differential.

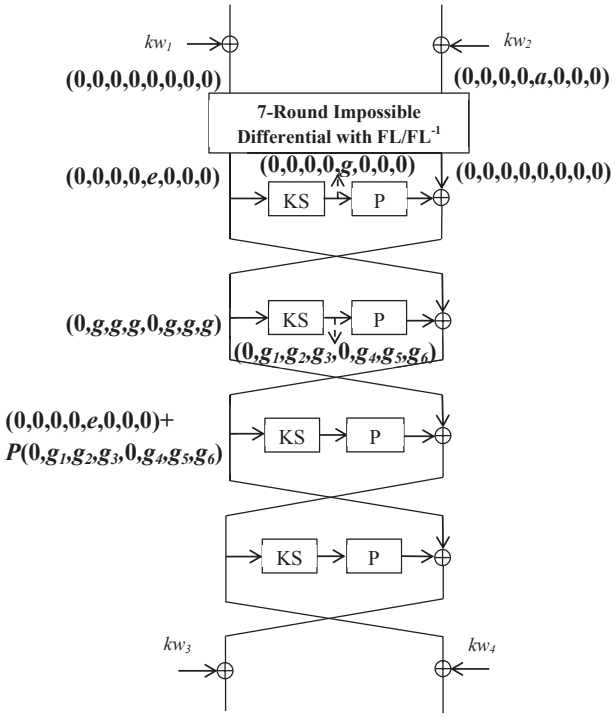

Fig. 3. Impossible Differential Cryptanalysis of 11-Round Camellia-256

2. Guess $k_{a,1}$. For each remaining ciphertext pairs, check whether $\Delta S_{11,1}$ is equal to $(P^{-1}(\Delta C_L))_1$. If $\Delta S_{11,1} \neq (P^{-1}(\Delta C_L))_1$ for some plaintext pair, then this pair is discarded. The probability that a plaintext pair passes this step is 2^{-8}. Therefore, we expect about $2^{n+15} \times 2^{-8} = 2^{n+7}$ pairs to be kept. Next guess the other bytes of k_a, i.e., $k_{a,l}$ for $2 \leq l \leq 8$. For the remaining pairs, compute the outputs of the 10-th round.
3. Guess all possible values of $k_{b,l}$ for $1 \leq l \leq 8$ and $l \neq 5$. For each of the remaining pairs after step 2, check whether the l-th byte of the S-Boxes output difference in the 10-th round $\Delta S_{10,l}$ is equal to $(P^{-1}(\Delta L_{10}))_l$. Keep only the pairs satisfying $\Delta S_{10,l} = (P^{-1}(\Delta L_{10}))_l$. The probability for that to happen is 2^{-8}. Thus, about $2^{n+7} \times 2^{-56} = 2^{n-49}$ will be kept after guessing $k_{b,\{1\sim4\}}$

and $k_{b,\{6\sim8\}}$. Finally, guess $k_{b,5}$ and calculate the outputs of the 9-th round for the remaining pairs.

4. We first guess the byte $k_{c,8}$. Partially decrypt the remaining pairs and keep only the pairs which satisfy $\Delta S_{9,8} = (P^{-1}(\Delta L_9))_8$. The probability of this event is 2^{-8}. So the number of the pairs remaining is about $2^{n-49} \times 2^{-8} = 2^{n-57}$. Then guess the value of $k_{c,l}$ for $2 \leq l \leq 7$ and $l \neq 5$ and check whether the equation $\Delta S_{9,l} = (P^{-1}(\Delta L_9))_l \oplus (P^{-1}(\Delta L_9))_5$ holds for each remaining pairs. If $\Delta S_{9,l} \neq (P^{-1}(\Delta L_9))_l \oplus (P^{-1}(\Delta L_9))_5$ for some pair, then this pair will be removed. The probability that all equations hold is 2^{-40}. The expected number of the pairs remaining is approximately $2^{n-57} \times 2^{-40} = 2^{n-97}$. Finally, guess the value of $k_{c,1}$ and compute $\Delta L_{7,5} = \Delta S_{9,1} \oplus \Delta S_{9,2} \oplus \Delta S_{9,6} \oplus \Delta S_{9,7} \oplus \Delta S_{9,8}$ for the remaining pairs.
5. Guess each possible value of $k_{d,5}$. If $\Delta S_{8,5} = \Delta L_{8,2}$ for some pair, then we remove this value of $k_{d,5}$ with the guessed $(k_a, k_b, k_{c,\{1\sim4\}}, k_{c,\{6\sim8\}})$. The probability of this event is 2^{-8}. Anyway, the correct key will be kept.
6. The main key can be recovered from the remaining 192-bit joint subkey $(k_a, k_b, k_{c,\{1\sim4\}}, k_{c,\{6\sim8\}}$ $k_{d,5})$. According to the key schedule of Camellia-256, we can get the following equations:

$$k_a = kw_4 \oplus k_{11} = (K_B \lll 111)_R \oplus (K_A \lll 45)_L, \tag{1}$$

$$k_b = kw_3 \oplus k_{10} = (K_B \lll 111)_L \oplus (K_L \lll 45)_R, \tag{2}$$

$$k_c = kw_4 \oplus k_9 = (K_B \lll 111)_R \oplus (K_L \lll 45)_L, \tag{3}$$

$$k_d = kw_3 \oplus k_8 = (K_B \lll 111)_L \oplus (K_B \lll 30)_R. \tag{4}$$

Guess each possible value of K_B. By equation (4), we first discard some wrong candidates of K_B. The probability for that to happen is 2^{-8}. For each of the remaining keys K_B, we calculate 64 bits of K_A by equation (1) and 120 bits of K_L by equations (2) and (3). Next, guess 64 remaining unknown bits of K_A. Based on K_B and K_A, we generate all bits of K_R by the key schedule. Finally, guessing eight remaining unknown bits of K_L, we test whether (K_L, K_R, K_A, K_B) can pass the key schedule of Camellia-256. The number of main keys remaining is approximately $2^{128} \times 2^{64} \times 2^8 \times 2^{-8} \times 2^{-128} = 2^{64}$. These remaining keys are considered as the candidates for the correct user key. With about 2^{64} trail encryptions, we can recover the unique user key.

Complexity Let ϵ be the expected number of the wrong subkeys remaining. Clearly,

$$\epsilon = 2^{192} \times (1 - 2^{-8})^{n-97}.$$

If we take $n = 112.06$, then $\epsilon \approx 1$. At this time, about one wrong key is left. In table 2, we will list the time complexity of each step.

Table 2. Time Complexity of Impossible Differential Attacks on 11-Round Camellia-256

Step	Time Complexity (1-round encryptions)
2	$2^{n+15} \times 2 \times 2^8 \times \frac{1}{8} + 2^{n+7} \times 2 \times 2^{64} \times \frac{7}{8} \approx 2^{n+71.8}$
3	$\sum_{i=1}^{8} 2^{n+7-8\cdot(i-1)} \times 2 \times 2^{64} \times 2^{8i} \times \frac{1}{8} = 2^{n+80}$
4	$\sum_{i=1}^{7} 2^{n-49-8\cdot(i-1)} \times 2 \times 2^{128} \times 2^{8i} \times \frac{1}{8} \approx 2^{n+87.8}$
5	$2^{192} \times 2 \times (1 + (1-2^8) + \cdots + (1-2^8)^{2^{n-97}}) \times \frac{1}{8} \approx 2^{198}$
6	$(\epsilon + 1) \times 2^{120} \times 2^{72} \times 6 + \epsilon \times 2^{64} \times 11 \approx 2^{195.6}$

From Table 2, we know the dominant part of time complexity to recover the main key is steps 4 and 5. Therefore, the time complexity of our attack is about $(2^{n+87.8} + 2^{198}) \times \frac{1}{11} \approx 2^{196.4}$ 11-round Camellia-256 encryptions. The data and memory complexities of our attack are approximately $2^{120.06}$ chosen plaintexts and $2^{n+15} \times 4 = 2^{129.06}$ 128-bit blocks, respectively.

5 Impossible Differential Cryptanalysis of 11-Round Camellia-192 and 12-Round Camellia-256

On the basis of our 7-round impossible differentials, we further attack 11-round Camellia-192 and 12-round Camellia-256.

5.1 Impossible Differential Cryptanalysis of 12-Round Camellia-256

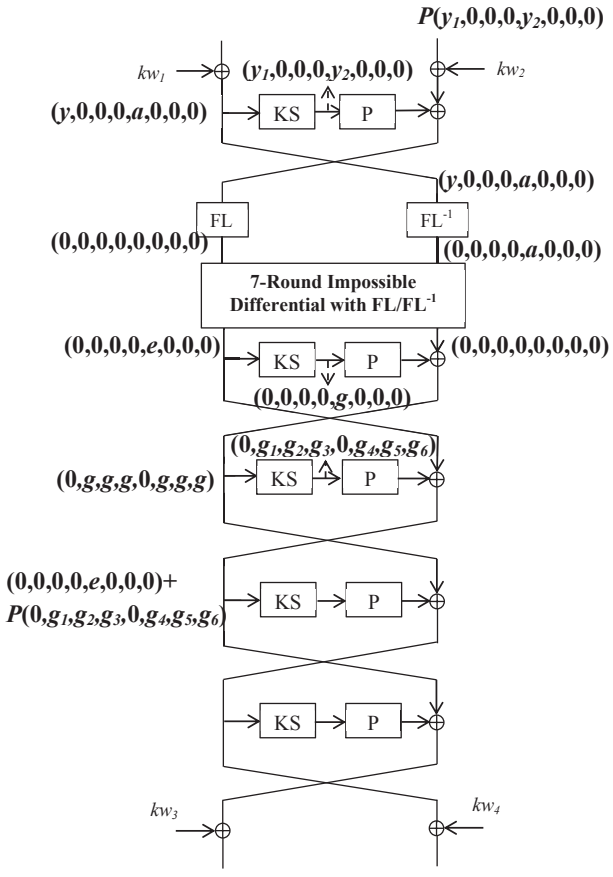

Fig. 4. Impossible Differential Cryptanalysis of 12-Round Camellia-256

We put one additional round on the plaintext side and four additional rounds on the ciphertext side of our proposed 7-round impossible differential to attack 12-round Camellia-256 from rounds

6 to 17. In Figure 4, we illustrate the basic structure of our attack. Some equivalent subkeys need to be given. Let

$$k_e = kw_1 \oplus k_6, k_f = kw_4 \oplus k_{17}, k_g = kw_3 \oplus k_{16}, k_h = kw_4 \oplus k_{15}, k_i = kw_3 \oplus k_{14}.$$

We remove the whitening layers and replace the round keys k_6, k_{14}, k_{15}, k_{16} and k_{17} with the corresponding subkeys k_e, k_i, k_h, k_g and k_f to generate a new cipher, which acts as the original one. The precise attacking procedure can be shown as below.

The Attacking Algorithm 2

1. Data Collection: Choose 2^n structures of plaintexts. Each of them has the following form:

$$(P(\alpha_1, x_1, x_2, x_3, \alpha_2, x_4, x_5, x_6), P(\alpha_3, x_7, x_8, x_9, \alpha_4, x_{10}, x_{11}, x_{12}))$$

   where $\alpha_i (1 \leq i \leq 4)$ takes all possible values and $x_j (1 \leq j \leq 12)$ is fixed in each structure. It is obvious that every structure contains 2^{32} plaintexts and generates 2^{63} plaintext pairs. In total, we collect 2^{n+63} plaintext pairs with the differences $\Delta L_0 = P(y, 0, 0, 0, a, 0, 0, 0)$ and $\Delta R_0 = P(y_1, 0, 0, 0, y_2, 0, 0, 0)$, where y and $y_i (i = 1, 2)$ are non-zero bytes. Encrypt these pairs to obtain the corresponding ciphertexts.
2. Guess $k_{e,1}$ and $k_{e,5}$. Check whether the equations $\Delta S_{6,l} = (P^{-1}(\Delta P_R))_l$ $(l = 1, 5)$ hold for each of remaining pairs. Remove some plaintext pairs satisfying $\Delta S_{6,l} \neq (P^{-1}(\Delta P_R))_l$. The expected number of the pairs remaining is about $2^{n+63} \times 2^{-16} = 2^{n+47}$.
3. Guess $kl_{2,5}$ and keep some plaintext pairs which satisfy the relation $\Delta P_{L,1} \oplus \Delta P_{L,5} \oplus (\Delta P_{L,5} \cap kl_{2,5}) = 0$. The probability of this condition is 2^{-8}. So about $2^{n+47} \times 2^{-8} = 2^{n+39}$ pairs will be left.
4. Guess $k_{f,1}$ and test whether the equation $\Delta S_{17,1} = (P^{-1}(\Delta C_L))_1$ holds for the remaining pairs. If $\Delta S_{17,1}$ is equal to $(P^{-1}(\Delta C_L))_1$ for some pair, then this pair will be kept. The probability of this event is about 2^{-8}. Thus there are about $2^{n+39} \times 2^{-8} = 2^{n+31}$ pairs remain. Next guess other bytes of k_f, i.e., $k_{f,\{2\sim 8\}}$ and compute the outputs of the 16-th round.
5. Guess $k_{g,l}$ for $1 \leq l \leq 8$ and $l \neq 5$. Check whether the equation $\Delta S_{16,l} = (P^{-1}(\Delta L_{16}))_l$ holds for the remaining pairs. Remove some pairs which do not satisfy the equations above. The probability for that to happen is 2^{-56}. Consequently, about $2^{n+31} \times 2^{-56} = 2^{n-25}$ plaintext pairs will be kept. Next guess $k_{g,5}$ and decrypt the ciphertext pairs to get the outputs of the 15-th round.
6. Guess $k_{h,8}$ and check whether $\Delta S_{15,8}$ is equal to $(P^{-1}(\Delta L_{15}))_8$ for the remaining pairs. If $\Delta S_{15,8} = (P^{-1}(\Delta L_{15}))_8$ for some pair, then this pair will be left. The probability of this event is 2^{-8}. Thus there are about $2^{n-25} \times 2^{-8} = 2^{n-33}$ pairs remain. Next guess each possible value of $k_{h,l}$ for $2 \leq l \leq 7 (l \neq 5)$. Keep only the pairs satisfying the equation $\Delta S_{15,l} = (P^{-1}(\Delta L_{15}))_l \oplus (P^{-1}(\Delta L_{15}))_5$. The total probability is about 2^{-40}. The expected number of remaining pairs is about $2^{n-33} \times 2^{-40} = 2^{n-73}$. Finally, guess $k_{h,1}$ and calculate the values of $R_{14,5}$ and $R'_{14,5}$.
7. Guess each possible value of $k_{i,5}$. If $\Delta S_{14,5} = \Delta L_{14,2}$, then we remove this value of $k_{i,5}$ with the guessed $(k_{e,\{1,5\}}, kl_{2,5}, k_f, k_g, k_{h,\{1\sim 4\}}, k_{h,\{6\sim 8\}})$. The probability of this event is 2^{-8}. In any case, the correct key will be kept.

8. The main key can be retrieved from the remaining joint subkeys ($k_{e,\{1,5\}}$, $kl_{2,5}, k_f, k_g, k_{h,\{1\sim4\}}$, $k_{h,\{6\sim8\}}, k_{i,5}$). By the key schedule of Camellia-256, we can obtain:

$$k_e = kw_1 \oplus k_6 = (K_L \lll 0)_L \oplus (K_A \lll 15)_R \tag{5}$$

$$k_f = kw_4 \oplus k_{17} = (K_B \lll 111)_R \oplus (K_L \lll 77)_L \tag{6}$$

$$kl_2 = (K_R \lll 30)_R \tag{7}$$

$$k_g = kw_3 \oplus k_{16} = (K_B \lll 111)_L \oplus (K_B \lll 60)_R \tag{8}$$

$$k_h = kw_4 \oplus k_{15} = (K_B \lll 111)_R \oplus (K_B \lll 60)_L \tag{9}$$

$$k_i = kw_3 \oplus k_{14} = (K_B \lll 111)_L \oplus (K_R \lll 60)_R \tag{10}$$

We first compute the value K_B by equations (8) and (9). There are about 2^8 values of K_B remain. Then we can calculate 64 bits of K_L by the equation (6) and 8 bits of K_R by equation (10). Equation (7) also provides 8 bits of information on K_R. Guess 112 remaining bits of K_R. By the key schedule, we can calculate all bits of K_A. Guessing 64 other bits of K_L, we can discard some wrong values of K_L and K_A according to equation (5). The probability of this event is 2^{-16}. In total, about $2^{168}(= 2^8 \times 2^{112} \times 2^{64} \times 2^{-16})$ keys (K_L, K_R, K_A, K_B) require to be executed the test of the key schedule. Therefore, the expected number of the keys remaining is about $2^{168} \times 2^{-128} = 2^{40}$ and the correct key can be obtained by trial encryptions.

Complexity After step 5, there are about 2^{n+23} plaintext pairs remain. Denote the expected number of wrong 216-bit values $(k_{e,\{1,5\}}, kl_{2,5}, k_f, k_g, k_{h\{1\sim4\}}, k_{h\{6\sim8\}}, k_{i,5})$ surviving after trying all the pairs by ε'. Clearly,

$$\epsilon' = 2^{216} \times (1 - 2^{-8})^{2^{n-73}}.$$

Take $n = 87.8$. Then $\epsilon' \approx 2^{52}$. We list the time complexity of each step in table 3.

Table 3. Time Complexity of Impossible Differential Attacks on 12-Round Camellia-256

Step	Time Complexity (1-round encryptions)
2	$2^{n+63} \times 2 \times 2^8 \times 2 \times \frac{1}{8} = 2^{n+70}$
3	$2^{n+47} \times 2 \times 2^{16} \times 2^8 \times \frac{1}{8} = 2^{n+69}$
4	$2^{n+39} \times 2 \times 2^{32} \times \frac{1}{8} + 2^{n+31} \times 2 \times 2^{88} \times \frac{7}{8} = 2^{n+119.8}$
5	$2^{n+31} \times 2 \times 2^{88} \times 2^8 \times 7 \times \frac{1}{8} + 2^{n-25} \times 2 \times 2^{152} \times \frac{1}{8} = 2^{n+128}$
6	$2^{n-25} \times 2 \times 2^{152} \times 2^8 \times 6 \times \frac{1}{8} + 2^{n-73} \times 2 \times 2^{208} \times \frac{1}{8} \approx 2^{n+135.8}$
7	$2^{216} \times 2 \times (1 + (1-2^8) + \cdots + (1-2^8)^{2^{n-73}} \times \frac{1}{8} \approx 2^{222}$
8	$(\epsilon' + 1) \times 2^{168} \times 6 + \epsilon' \times 2^{40} \times 11 \approx 2^{222.6}$

Clearly, the dominant part of time complexity is steps 6 to 8. Therefore, the total time complexity is about $(2^{n+135.8} + 2^{222} + 2^{222.6}) \times \frac{1}{12} \approx 2^{220.87}$ 12-round Camellia-256 encryptions. The data and memory complexities are $2^{119.8}$ chosen plaintexts and $2^{n+47} \times 4 \times 2^4 = 2^{156.8}$ bytes.

5.2 Impossible Differential Cryptanalysis of 11-Round Camellia-192

On the basis of impossible differential attacks on 12-round Camellia-256 from rounds 6 to 17, we present impossible differential cryptanalysis of 11-round Camellia-192 by removing the 17-th round. Since this attack is similar to the impossible differential attack on 12-round Camellia-256, we only describe some differences between them in the following.

First, we collect the same plaintext pairs as we do in step 1 of section 5.1. In total, we select 2^{n+32} plaintexts, which generate 2^{n+63} pairs satisfying the input differences of the plaintext pairs.

Second, we filter out some wrong plaintext pairs whose ciphertext differences don't satisfy our requirements. Keep only the pairs with the following ciphertext differences:

$$P(0, g_1 \oplus e, g_2 \oplus e, g_3 \oplus e, e, g_4 \oplus e, g_5 \oplus e, g_6),$$

where $g_i (1 \leq i \leq 6)$ are non-zero byte. After this step, we expect about $2^{n+63} \times 2^{-8} = 2^{n+55}$ pairs remain.

Third, we remove the wrong subkeys. We first give some new notations, i.e., $k'_g = kw_4 \oplus k_{16}, k'_h = kw_3 \oplus k_{15}$ and $k'_i = kw_4 \oplus k_{14}$. Then, we guess all possible values of $k_{e,\{1,5\}}, kl_{2,5}, k'_g$ and $k'_{h,l} (1 \leq l \leq 8, l \neq 5)$ in turn so as to keep some plaintext pairs satisfying our requirements. There are approximately $2^{n+55} \times 2^{-16} \times 2^{-8} \times 2^{-56} \times 2^{-48} = 2^{n-73}$ plaintext pairs remain. Finally, guess $k_{i,5}$. If $\Delta S_{14,5} = \Delta L_{14,2}$, then we remove this value of $k_{i,5}$ with the guessed $(k_{e,\{1,5\}}, kl_{2,5}, k'_g, k'_{h,\{1\sim4\}}, k'_{h,\{6\sim8\}})$. The probability of this event is 2^{-8}. Denote the number of the wrong subkeys remaining by ϵ''. Clearly,

$$\epsilon'' = 2^{152} \times (1 - 2^{-8})^{2^{n-73}}.$$

Take $n = 88$. Then $\epsilon'' \approx 2^{-32.7}$. Up to now, the dominant part of time complexity is the step that to guess the values of $(k'_{h,\{1\sim4\}}, k'_{h,\{6\sim8\}})$, i.e., about $2^{n-25} \times 2 \times 2^{88} \times 2^8 \times 7 \times \frac{1}{8} = 2^{n+71.8} = 2^{159.8}$ 1-round encryptions. It is equivalent to approximately $2^{159.8} \times \frac{1}{11} \approx 2^{156.34}$ 11-round Camellia-192 encryptions.

Finally, we recover the main key from the remaining joint subkeys. According to the key schedule of Camellia-192, we obtain the equation:

$$k'_g = kw_4 \oplus k_{16} = (K_B \lll 111)_R \oplus (K_B \lll 60)_R \tag{11}$$

$$k'_h = kw_3 \oplus k_{15} = (K_B \lll 111)_L \oplus (K_B \lll 60)_L \tag{12}$$

$$k'_i = kw_4 \oplus k_{14} = (K_B \lll 111)_R \oplus (K_R \lll 60)_R \tag{13}$$

Combining with equations (5) and (7), we retrieve the main key. First, we calculate 120 bits of K_B by equations (11) and (12). Guessing eight other bits of K_B, we can compute 8 bits of K_R by equation (13). In addition, we know 8 bits of k_R from equation (7). Next, guessing the 48 remaining unknown bits of K_R, we obtain all bits of K_A by the key schedule and 16 bits of K_L by equation (5). Finally, guessing 112 remaining bits of K_L, we test whether (K_L, K_R, K_A, K_B) can pass the key schedule of Camellia-192. Consequently, about $2^8 \times 2^{112} \times 2^{48} \times 2^{-128} = 2^{40}$ keys are kept. The unique correct key can be sieved by trail encryptions. The time complexity of this step is about 2^{168} 6-round encryptions, i.e., $2^{167.1}$ 11-round encryptions.

In conclusion, the total time complexity of impossible differential attacks on 11-round Camellia-192 is about $2^{158.8} + 2^{167.1} \approx 2^{167.1}$ 11-round Camellia-192 encryptions. The data and memory complexities are 2^{120} chosen plaintexts and $2^{88+55} \times 4 \times 2^4 = 2^{149}$ bytes.

6 Conclusion

In this paper, we have presented new results on impossible differential cryptanalysis of Camellia-192 /256. We first exploit some properties of the transformations FL/FL^{-1}. On the basis of them, we construct several 7-round impossible differentials of Camellia with the FL/FL^{-1} layers. Then by adding four additional rounds after one 7-round impossible differential, we propose a new impossible differential attack on 11-round Camellia-256. Our attack requires $2^{120.06}$ chosen plaintexts, $2^{196.4}$ 11-round encryptions and $2^{133.06}$ bytes of memory. Furthermore, we further improve these cryptanalytic results and derive efficient attacks on 11 rounds of Camellia-192 and 12 rounds of Camellia-256. The time complexities of our attacks on 11 rounds of Camellia-192 and 12 rounds of Camellia-256 are about $2^{167.1}$ 11-round encryptions and $2^{220.87}$ 12-round encryptions, which are $2^{16.9}$ times and $2^{19.13}$ times faster than previously best known results but have slightly more data and memory.

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.E. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 2012, pp. 39–56. Springer (2000)
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: EUROCRYPT. pp. 12–23 (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. Lecture Notes in Computer Science, vol. 6812, pp. 16–33. Springer (2011)
4. CRYPTREC-Cryptography Research and Evaluation Committees: report. Archive (2002), http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html
5. Dunkelman, O., Keller, N.: An improved impossible differential attack on MISTY1. In: Pieprzyk, J. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 5350, pp. 441–454. Springer (2008)
6. Hatano, Y., Sekine, H., Kaneko, T.: Higher order differential attack of Camellia (II). In: Nyberg, K., Heys, H.M. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 2595, pp. 129–146. Springer (2002)
7. 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)
8. Jie, G., Zhongya, Z.: Improved collision attack on reduced round Camellia. In: Pointcheval, D., Mu, Y., Chen, K. (eds.) CANS. Lecture Notes in Computer Science, vol. 4301, pp. 182–190. Springer (2006)
9. Kawabata, T., Kaneko, T.: A study on higher order differential attack of Camellia. In: The 2nd open NESSIE workshop (2001)
10. Knudsen, L.R.: DEAL - a 128-bit block cipher. Tech. rep., Department of Informatics, University of Bergen, Norway (1998), technical report
11. Lei, D., Li, C., Feng, K.: New observation on Camellia. In: Preneel, B., Tavares, S.E. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 3897, pp. 51–64. Springer (2005)
12. Lei, D., Li, C., Feng, K.: Square like attack on Camellia. In: Qing, S., Imai, H., Wang, G. (eds.) ICICS. Lecture Notes in Computer Science, vol. 4861, pp. 269–283. Springer (2007)
13. Li, L., Chen, J., Jia, K.: New impossible differential cryptanalysis of reduced versions of Camellia block cipher. In: CANS (2011), to appear
14. Li, L., Chen, J., Wang, X.: Security of reduced-round Camellia against impossible differential attack. IACR Cryptology ePrint Archive 2011, 524 (2011)
15. Lu, J., Dunkelman, O., Keller, N., Kim, J.: New impossible differential attacks on AES. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT. Lecture Notes in Computer Science, vol. 5365, pp. 279–293. Springer (2008)
16. Lu, J., Wei, Y., Kim, J., Fouque, P.A.: Cryptanalysis of reduced versions of the Camellia block cipher. In: SAC (2011), to appear

17. Mala, H., Dakhilalian, M., Rijmen, V., Modarres-Hashemi, M.: Improved impossible differential cryptanalysis of 7-round AES-128. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT. Lecture Notes in Computer Science, vol. 6498, pp. 282–291. Springer (2010)
18. Mala, H., Shakiba, M., Dakhilalian, M., Bagherikaram, G.: New results on impossible differential cryptanalysis of reduced-round Camellia-128. In: Jr., M.J.J., Rijmen, V., Safavi-Naini, R. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 5867, pp. 281–294. Springer (2009)
19. 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
20. 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. Lecture Notes in Computer Science, vol. 2248, pp. 193–207. Springer (2001)
21. Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible differential cryptanalysis of CLEFIA. In: Nyberg, K. (ed.) FSE. Lecture Notes in Computer Science, vol. 5086, pp. 398–411. Springer (2008)
22. Wu, W., Zhang, W., Feng, D.: Impossible differential cryptanalysis of reduced-round aria and camellia. J. Comput. Sci. Technol. 22(3), 449–456 (2007)