Improved Impossible Differential Attack on Reduced Version of Camellia-192/256

Ya Liu[1], Dawu Gu[1], Zhiqiang Liu[1], Wei Li[2,3]

[1] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240 ,China,*
{liuya0611, dwgu, ilu_zq}@sjtu.edu.cn
[2] *School of Computer Science and Technology, Donghua University, Shanghai 201620, China*
[3] *Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai 200240, China*
liwei.cs.cn@gmail.com

Abstract

As an ISO/IEC international standard, Camellia has been used various cryptographic applications. In this paper, we improve previous attacks on Camellia-192/256 with key-dependent layers FL/FL^{-1} by using the intrinsic weakness of keyed functions. Specifically, we present the first impossible differential attack on 13-round Camellia with $2^{121.6}$ chosen ciphertexts and $2^{189.9}$ 13-round encryptions, while the analysis for the biggest number of rounds in previous results on Camellia-192 worked on 12 rounds. Furthermore, we successfully attack 14-round Camellia-256 with $2^{122.1}$ chosen ciphertexts and $2^{229.3}$ 14-round encryptions. Compared with the previously best known attack on 14-round Camellia-256, the time complexity of our attack is reduced by $2^{8.9}$ times and the data complexity is comparable.

Key words: Block Cipher, Camellia, Impossible Differential Cryptanalysis

1. Introduction

The 128-bit block cipher Camellia was jointly developed by NTT and Mitsubishi in 2000 [1]. It supports three kinds of key sizes, i.e., 128 bits, 192 bits and 256 bits. For simplicity, they can be usually denoted as Camellia-128, Camellia-192 and Camellia-256, respectively. Camellia adopts the basic Feistel structure with two key-dependent transformations inserted every six rounds. The goals for such a design are to provide non-regularity across rounds and to thwart future unknown attacks. In 2002, Camellia was selected as one of the CRYPTREC e-government recommended ciphers. In 2003, it was recommended in NESSIE block cipher portfolio. Finally, it was adopted as an international standard by ISO/IEC [4].

So far, a lot of researchers have used various methods to attack Camellia such as linear cryptanalysis, differential cryptanalysis, higher order differential attack, impossible differential attack and so on. Among them, most attacks involved in reduced-round Camellia without FL/FL^{-1} and whitening layers [5, 6, 7, 11, 14, 15, 16, 17, 18], only three attacks focused on the security of reduced-round Camellia with FL/FL^{-1} and whitening layers [3, 9, 10], and four attacks analyzed the security of reduced-round Camellia with FL/FL^{-1} layers [8, 13, 2, 12]. For Camellia with FL/FL^{-1} layers, Li *et al.* attacked 12-round Camellia-192 with $2^{120.1}$ chosen plaintexts and 2^{184} encryptions and 14-round Camellia-256 with 2^{120} chosen ciphertexts and $2^{250.5}$ encryptions [8], lv *et al.* mounted impossible differential attacks on 10-round Camellia-128 with 2^{118} chosen plaintexts and 2^{118} encryptions and 11-round Camellia-192 with 2^{118} chosen plaintexts and $2^{163.1}$ encryptions [13], Bai *et al.* improved Li's results to attack 12-round Camellia-192 with $2^{120.6}$ chosen plaintexts and $2^{171.4}$ encryptions and 14-round Camellia-256 with $2^{121.2}$ chosen plaintexts and $2^{238.2}$ encryptions [2], lv *et al.* gave higher-order meet-in-the-middle attacks on 10-round Camellia-128 with 2^{93} chosen plaintexts and $2^{118.6}$ encryptions, 11-round Camellia-192 with 2^{78} chosen plaintexts and $2^{187.4}$ encryptions as well as 12-round Camellia-256 with 2^{94} chosen plaintexts and $2^{237.3}$ encryptions [12].

Impossible differential cryptanalysis was independently proposed by Knudsen and Biham. Unlike traditional differential cryptanalysis, the adversary requires to construct two truncated differentials with probability one which meet a contradiction in the middle. This new differential with probability zero is called an impossible differential. By using this impossible differential, we can remove all wrong candidates of the secret key until the correct one is left.

Table 1: Summary of attacks on reduced-round Camellia-192/256 without the whitening layers

Key Size	Rounds	Attack Type	Data	Time(Enc)	Memory (Bytes)	Source
Camellia-192	11	Impossible DC	2^{118}CP	$2^{163.1}$	2^{141}	[12]
	11	HO-MitM	2^{94}CP	$2^{180.2}$	2^{174}	[13]
	11	Impossible DC	$2^{120.4}$CP	$2^{121.7}$	$2^{115.5}$	[2]
	12	Impossible DC	$2^{120.1}$CP	2^{184}	$2^{124.1}$	[8]
	12	Impossible DC	$2^{120.6}$CP	$2^{171.4}$	$2^{171.6}$	[2]
	12	Impossible DC	$2^{124.35}$CP	$2^{148.5}$	$2^{132.7}$	Section 3.1
	13	Impossible DC	$2^{121.6}$CC	$2^{189.9}$	$2^{101.6}$	Section 3.2
Camellia-256	12	HO-MitM	2^{94}CP	$2^{237.3}$	2^{174}	[13]
	14	Impossible DC	2^{120}CC	$2^{250.5}$	2^{125}	[8]
	14	Impossible DC	$2^{121.2}$CC	$2^{238.2}$	$2^{180.2}$	[2]
	14	Impossible DC	$2^{122.1}$CC	$2^{229.3}$	$2^{134.1}$	Section 4

DC: Differential Cryptanalysis; CP/CC: Chosen Plaintexts/Chosen Ciphertexts;
HO-MitM: Higher Order Meet-in-the-Middle Attack; Enc: Encryptions;

As one of the most powerful methods, impossible differential cryptanalysis is used to analyze the securities of many block ciphers such as AES, CLEAFIA, ARIA, MISTY1 and so on.

In this paper, we improve previous attacks on Camellia-192/256 with two key-dependent layers FL/FL^{-1} by using the intrinsic weakness of keyed transformations. We first attack 12-round Camellia-192 with $2^{124.35}$ chosen plaintexts, $2^{148.5}$ 12-round encryptions and $2^{132.7}$ bytes. Compared with the previously fastest known attack on 12-round Camellia-192, the time and memory complexities of our attack are reduced by $2^{22.9}$ times and $2^{38.9}$ times and the data complexity is comparable. Second, we further improve our result and derive the first attack on 13-round Camellia-192 with $2^{121.6}$ chosen ciphertexts, $2^{189.9}$ 13-round encryptions and $2^{101.6}$ bytes, while the analysis for the biggest number of rounds in previous results on Camellia-192 worked on 12 rounds. Finally, we propose improved impossible differential cryptanalysis of 14-round Camellia-256 with $2^{122.1}$ chosen ciphertexts, $2^{229.3}$ 14-round encryptions and $2^{134.1}$ bytes, which is $2^{8.9}$ times faster than previously best known attack on 14-round Camellia-256. In table 1, we summarize our results along with the former known ones on Camellia-192/256.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries. Section 3 gives a chosen plaintext attack on 12-round Camellia-192 and a chosen ciphertext attack on 13-round Camellia-192. Section 4 presents an impossible differential attack on 14-round Camellia-256. 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;
- $kw_1|kw_2, kw_3|kw_4$: the pre-whitening key and the post-whitening key;
- $k_i, kl_i (1 \leq i \leq 6)$: the subkey used in the i-th round and 64-bit keys used in the FL/FL^{-1} layers;
- $S_r, \Delta S_r$: the output and the output difference of the S-boxes in the r-th round;
- $X \mid Y, X \lll j$: the concatenation of X and Y, 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. The Block Cipher Camellia

Camellia [1] is a 128-bit block cipher. It adopts the basic Feistel structure with the key-dependent functions FL/FL^{-1} inserted every 6 rounds. Camellia 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. The encryption algorithm of Camellia can be expressed as follows:

1. $L_0|R_0 = P \oplus (kw_1|kw_2)$,
2. For $r = 1$ to Nr:
   if $r \neq 6k$, where $k = 1, \cdots, Nr/6 - 1$, then $L_r = R_{r-1} \oplus F(L_{r-1}, k_r)$, $R_r = L_{r-1}$.
   else $L'_r = R_{r-1} \oplus F(L_{r-1}, k_r)$, $R'_r = L_{r-1}$; $L_r = FL(L'_r, kl_{r/3-1})$, $R_r = FL^{-1}(L'_r, kl_{r/3})$;
3. $C = (R_{N_r} \oplus kw_3)|(LR_{N_r} \oplus kw_4)$.

Here the round function includes an XOR operation with a round key, an nonlinear transformation S and a linear function P. Among it, the linear transformation P and its inverse function P^{-1} are defined as follows:

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

where $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$ and $(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8)$ are the input and output of P. The key-dependent function $FL : (X_L \mid X_R, kl_L \mid kl_R) \mapsto Y_L \mid Y_R$, where $Y_R = ((X_L \cap kl_L) \lll 1) \oplus X_R$, $Y_L = (Y_R \cup kl_R) \oplus X_L$.

Key Schedule of Camellia-192/256. The key schedule of Camellia applies a 6-round Feistel structure to derive two 128-bit intermediate variables K_A and K_B from 128-bit variables 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-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., $K = K_L \mid K_R$.

2.3. 8-Round Impossible Differentials of Camellia

In [10], Liu *et al.* presented 8-round impossible differentials of Camellia with two FL/FL^{-1} layers as follows:

Property 1. *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 $a^{(1)} = b^{(1)} = a'^{(8)} = b'^{(8)} = 0$. Four subkeys $kl_i (i = 1, \cdots, 4)$ are used in two FL/FL^{-1} layers. If a' and b' satisfy the following equations:*

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

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. 1).

For each value of $kl_1^{(2\sim8)}|kl_4^{(2\sim8)}$, denote the corresponding impossible differential by Δ_i. Let $A = \{\Delta_i | 0 \leq i \leq 2^{14} - 1\}$. All differentials of A can be divided into three cases, i.e., (1) $a' = b' = 0$, (2) $a' = 0$ and $b' \neq 0$, or $a' \neq 0$ and $b' = 0$, (3) $a' \neq 0$ and $b' \neq 0$. Since property 1 only gave the existence of an 8-round impossible differential of Camellia for any fixed key value, they proposed an attack strategy to recover the master key in the following:

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.

- 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.

- If no subkeys or more than one subkeys are left, select another differential of A to execute a new impossible differential attack.

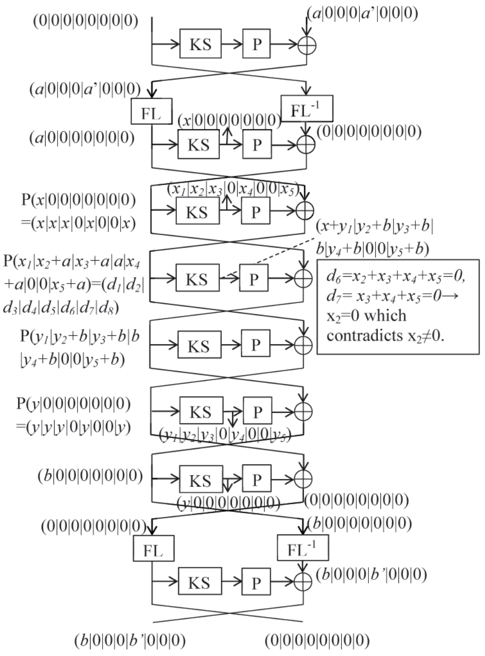

Figure 1: The Structure of 8-Round Impossible Differentials of Camellia

3. Impossible Differential Cryptanalysis of Reduced-Round Camellia-192

In this section, we mount a chosen plaintext attack on 12-round Camellia-192 from rounds 3 to 14 and a chosen ciphertext attack on 13-round Camellia-192 from rounds 3 to 15. Some previous skills such as building hash tables and the early abort technique [11] are also adopted. Moreover, we make full use of the corresponding subkey for each 8-round differential of A to reduce the guessed key space.

3.1. Impossible Differential Cryptanalysis of 12-Round Camellia-192

By setting three rounds at the top and one round at the bottom of 8-round differentials, we attack 12-round Camellia-192 from rounds 3 to 14. We divide all differentials of A into three cases to discuss our attack as follows.

Case 1 $a' = b' = 0$**.** The 8-round impossible differential is $\Delta = (0|0|0|0|0|0|0|0, a|0|0|0|0|0|0|0) \rightarrow_8 (b|0|0|0|0|0|0|0, 0|0|0|0|0|0|0|0)$, where a and b are non-zero bytes and $a^{(1)} = b^{(1)} = 0$. At this time, the corresponding subkey is $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|K_L^{(0\sim3)} = 0_{(14)}$. See Figure 2.

1. Choose $2^{9.5}$ structures of plaintexts. Each structure contains 2^{111} plaintexts with the form: $(P(\alpha_1|\alpha_2|\alpha_3|\alpha_4|\alpha_5|x_1|x_2|\alpha_6), \alpha_7|\alpha_8|\alpha_9|\alpha_{10}|\alpha_{11}|\alpha_{12}|\alpha_{13}|\alpha_{14})$, where $\alpha_4^{(1)}, x_1, x_2$ are fixed and $\alpha_i(1 \le i \le 14, i \ne 4)$, $\alpha_4^{(2\sim8)}$ take all possible values. Clearly, each structure can form 2^{221} plaintext pairs. In total, we collect $2^{230.5}$ plaintext pairs. The left halves of these plaintext differences satisfy $P(g_1|g_2 \oplus a|g_3 \oplus a|a|g_4 \oplus a|0|0|g_5 \oplus a)$ with a and $g_i(1 \le i \le 5)$ being nonzero bytes and $a^{(1)} = 0$. Encrypt them and keep those pairs whose ciphertext differences have the form $(P(h|0|0|0|0|0|0|0), b|0|0|0|0|0|0|0)$ with b and h being nonzero bytes and $b^{(1)} = 0$. The probability of this event is about 2^{-113}. Therefore, the expected number of remaining pairs is about $2^{117.5}$.
2. Guess $K_{3,3} = K_R^{(31\sim38)}$. We have known the value of $K_{3,3}^{(1\sim7)}$ from $kl_1^{(2\sim8)}$. Thus we only guess one bit $K_{3,3}^{(8)}$. For each remaining pair, compute the value of $(S_{3,3}, S'_{3,3})$ and check whether the equation $\Delta S_{3,3} = (P^{-1}(\Delta P_R))_3$ holds. If $\Delta S_{3,3} \ne (P^{-1}(\Delta P_R))_3$ for some pair, then this pair will be discarded. The probability is about 2^{-8}. So the expected number of remaining pairs is approximately $2^{109.5}$. Next guess $K_{3,l}$ for $2 \le l \le 8(l \ne 3)$. For every remaining pair, calculate the value of $(S_{3,l}, S'_{3,l})$. Discard those pairs satisfying $\Delta S_{3,l} \ne (P^{-1}(\Delta P_R))_l$. About $2^{61.5}$ pairs will be kept. Finally, guess $K_{3,1}$ and calculate the inputs of the 4-th round.

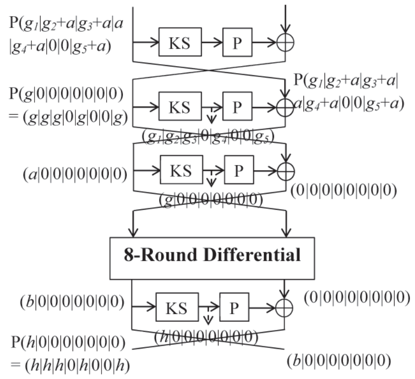

Figure 2: Impossible Differential Attack on 12-Round Camellia for Case 1

3. According to $K_4 = \overline{K_R^{(15\sim63)}}|K_R^{(0\sim14)}$ and $K_{14,1} = \overline{K_R^{(60\sim63)}}|K_R^{(0\sim3)}$, we compute the value of $(S_4, S'_4, \Delta S_{14,1})$ for every remaining pair. Keep those pairs satisfying these equations $\Delta S_{4,1} = (P^{-1}(\Delta P_L))_1$, $\Delta S_{4,l} = (P^{-1}(\Delta P_L))_l \oplus (P^{-1}(\Delta P_L))_4 (l = 2, 3, 5, 8)$ and $\Delta S_{14,1} = (P^{-1}(\Delta C_R))_1$. The probability of this event is about 2^{-48}. The expected number of remaining pairs is approximately $2^{13.5}$. For each remaining pair, calculate the inputs of the 5-th round.
4. Guess $K_{5,1}$. Compute the value of $(\Delta S_{5,1}, (P^{-1}(\Delta R_4))_1)$ for each remaining pair. If $\Delta S_{5,1} = (P^{-1}(\Delta R_4))_1$ for some pair, we remove the guessed subkey. The probability is about 2^{-8}. So the expected number of remaining wrong subkey is approximately $2^{65} \times (1 - 2^{-8})^{2^{13.5}} \approx 1$ if Δ is an 8-round impossible differential. When only one joint subkey is kept, we recover the secret key and verify whether it is correct, else 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 $a' = 0$ 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 $a^{(1)} = b^{(1)} = b'^{(8)} = 0$. The corresponding subkey is $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|K_L^{(0\sim3)} = 0_{(7)}|1_{(7)}$.

1. Select $2^{120.7}$ plaintexts which have the same structure as above Case 1. We totally collect $2^{230.7}$ plaintext pairs. Encrypt them and obtain the corresponding ciphertext pairs. If the ciphertext difference of some pair does not satisfy $(P(h|0|0|0|h'|0|0|0), b|0|0|0|b'|0|0|0)$ with b, b', h and h' being non-zero bytes, $b'^{(1\sim7)} = b^{(2\sim8)}$ and $b^{(1)} = b'^{(8)} = 0$, we get rid of this pair. The expected number of remaining pairs is about $2^{125.7}$.
2. Guess $K_{3,3}, K_{3,2}, K_{3,\{4\sim8\}}$ and $K_{3,1}$ in turn. After this test, about $2^{69.7}$ pairs will be kept.
3. We have known K_4 and $K_{14,l} (l = 1, 5)$. For each remaining pair, we compute the values of (S_4, S'_4) and $(S_{14,l}, S'_{14,l})$. This step is similar to step 3 of Case 1. The expected number of remaining pairs is about $2^{13.7}$.
4. Guess $K_{15,1}$ as before. If Δ' is an 8-round impossible differential, then the expected number of remaining wrong subkeys is approximately $2^{73} \times (1 - 2^{-8})^{2^{13.7}} \approx 1$. We only consider the scenario that one joint subkey will be kept. At this time, we recover the secret key by the key schedule and verify whether it is correct. If this key is correct, then we halt the attack, else try another differential of A.

Case 3 $a' \neq 0$ **and** $b' \neq 0$**.** We only attack an example $a'^{(1\sim7)} = a^{(2\sim8)}$ and $b'^{(1\sim7)} = b^{(2\sim8)}$. 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, a', b and b' are non-zero bytes and $a^{(1)} = b^{(1)} = a'^{(8)} = b'^{(8)} = 0$. The corresponding subkey is $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|K_L^{(0\sim3)} = 1_{(14)}$.

1. Select $2^{124.35}$ plaitexts including those plaintexts in Cases 1 and 2. Encrypt them to obtain the corresponding ciphertexts. Guess 11 bits of K_R, i.e., $K_{14,1} = \overline{K_R^{(60\sim63)}}|K_R^{(0\sim3)}$ and $K_{14,5}^{(1\sim3)} = K_R^{(28\sim30)}$. Since $K_R^{(31\sim35)} = 1_{(5)}$, we can get the value of $K_{14,5}^{(4\sim8)}$. Partially decrypt the ciphertexts to derive the inputs of the 14-th round. Insert these plaintext-ciphertexts into a hash table indexed by 121-bit value of ($L_{13,\{2\sim4\}}$, $L_{13,\{6\sim8\}}$, $L_{13,1}^{(1)}$, $L_{13,5}^{(8)}$, $L_{13,1}^{(2\sim8)} \oplus L_{13,5}^{(1\sim7)}, R_{13}$). Any two plaintext-ciphertexts in the same row of the hash table forms a pair satisfying $(\Delta L_{13}, \Delta R_{13}) = (b|0|0|0|b'|0|0|0, 0|0|0|0|0|0|0|0)$ with $b^{(1)} = b'^{(8)} = 0$ and $b^{(2\sim8)} = b'^{(1\sim7)}$. Finally, the expected number of remaining pairs is about $2^{126.7}$.

Table 2: Time Complexity of Cases 3

Step	Time Complexity (1-round encryptions)
1	$2^{124.35} \times 12 + 2^{124.35} \times 2^{11} = 2^{135.35}$
2	$(2^{126.7} \times 2^{12} + 2^{118.7} \times 2^{15} + 2^{110.7} \times 2^{20} + 2^{102.7} \times 2^{25} + 2^{94.7} \times 2^{33} + 2^{86.7} \times 2^{41} + 2^{78.7} \times 2^{57} \times 2) \times 2 \times \frac{1}{8} = 2^{137}$
3	$2^{78.7} \times 2 \times 2^{57} = 2^{136.7}$
4	$(2^{21.7} \times 2 \times 2^{65} + 2^{73} \times (1 + (1 - 2^{-8}) + \cdots + (1 - 2^{-8})^{2^{13.7}})) \times \frac{1}{8} \approx 2^{84.7}$

2. Guess $K_{3,3} = K_R^{(31\sim38)}$ as before. After this test, about $2^{118.7}$ pairs will be kept. Next guess $K_{3,7}, K_{3,6}, K_{3,2}$ in turn. Because $K_{3,7}^{(1\sim5)} = \overline{K_{14,1}^{(4)}}|K_{14,1}^{(5\sim8)} = \overline{K_R^{(63)}}|K_R^{(0\sim3)}$, $K_{3,6}^{(6\sim8)} = \overline{K_{14,1}^{(1\sim3)}} = \overline{K_R^{(60\sim62)}}$ and $K_{3,2}^{(6\sim8)} = K_{14,5}^{(1\sim3)} = K_R^{(28\sim30)}$, we only guess partial bits of $(K_{3,7}, K_{3,6}, K_{3,2})$. Keep these pairs satisfying $\Delta S_{3,l} = (P^{-1}(\Delta P_R))_l (l = 7, 6, 2)$. The expected number of remaining pairs is about $2^{94.7}$. Finally, guess $K_{3,i}(i = 4, 8)$. For each remaining pair, we compute $(S_{3,i}, S'_{3,i})$ and test whether $\Delta S_{3,i}$ is equal to $(P^{-1}(\Delta P_R))_i$. If $\Delta S_{3,i} \neq (P^{-1}(\Delta P_R))_i$ for some pair, then this pair will be discarded. About $2^{78.7}$ pairs will be kept. Guess $K_{3,\{1,5\}}$ and compute the inputs of the 4-th round.
3. Since $K_4 = (K_R \lll 15)_R$, we can calculate (S_4, S'_4) for each remaining pair. Keep these pairs satisfying these equations $\Delta S_{4,1} = (P^{-1}(\Delta P_L))_1$, $\Delta S_{4,8}^{(1)} = (P^{-1}(\Delta P_L))_8^{(1)}$, $\Delta S_{4,i} = (P^{-1}(\Delta P_L))_i \oplus (\Delta S_{4,8} \oplus (P^{-1}(\Delta P_L))_8)^{(2\sim8)}|0(i = 6, 7)$ and $\Delta S_{4,j} = (P^{-1}(\Delta P_L))_j \oplus \Delta S_{4,8} \oplus (P^{-1}(\Delta P_L))_8 \oplus \Delta S_{4,7} \oplus (P^{-1}(\Delta P_L))_7 (j = 2, 3, 4, 5)$. The probability of this event is approximately 2^{-57}. So about $2^{21.7}$ will be kept.
4. Guess $K_{5,5}$. For each remaining pair, we calculate $(S_{5,5}, S'_{5,5})$ and check whether $\Delta S_{5,5}$ is equal to $(P^{-1}(\Delta R_4))_5$. If $\Delta S_{5,5} \neq (P^{-1}(\Delta R_4))_5$ for one pair, this pair will be discarded. About $2^{13.7}$ pairs will be kept. Next guess $K_{5,1}$ as before. If one subkey is left, we retrieve the master key, else try another differential of A.

Complexity. We list the time complexity of each step for Case 3 in table 2. We find the time complexity of Case 3 is determined by steps 1 and 2, i.e., $2^{138.1}$ 1-round encryptions. Similarly, we compute the time complexities of Cases 1 and 2, i.e., $2^{116.5}$ 1-round encryptions and $2^{124.5}$ 1-round encryptions. Therefore, the whole time complexity is approximately $2^{14} \times 2^{138.1} \times \frac{1}{12} = 2^{148.5}$ 12-round encryptions. The data and memory complexities are $2^{124.35}$ chosen plaintexts and $2^{126.7} \times 4 \times 2^4 = 2^{132.7}$ bytes.

3.2. Impossible Differential Cryptanalysis of 13-Round Camellia-192

By adding one round at the bottom of above 12-round Camellia-192, we mount a chosen ciphertext attack on 13-round Camellia-192 from rounds 3 to 15.

Case 1 $a' = b' = 0$**.** The 8-round differential and the corresponding subkey are Δ and $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|K_L^{(0\sim3)} = 0_{(14)}$, respectively.

1. Choose $2^{66.5}$ structures of ciphertexts. Each structure contains 2^{55} ciphertexts with the form $(P(\alpha_1|\alpha_2|\alpha_3|\alpha_4|\alpha_5|x_1|x_2|\alpha_6), P(\alpha_7|x_3|x_4|x_5|x_6|x_7|x_8|x_9))$, where $\alpha_i(1 \leq i \leq 7, i \neq 4), \alpha_4^{(2\sim8)}$ take all possible values, $x_j(1 \leq j \leq 9), \alpha_4^{(1)}$ are fixed. Clearly, each structure forms 2^{109} ciphertext pairs. We totally collect about $2^{175.5}$ ciphertext pairs whose differences satisfy $(P(h_1|h_2 \oplus b|h_3 \oplus b|b|h_4 \oplus b|0|0|h_5 \oplus b), P(h|0|0|0|0|0|0|0))$ with h, h_i, b being non-zero bytes and $b^{(1)} = 0$.
2. Guess remaining 57 bits of K_R. For each structure, we encrypt plaintexts to derive the inputs of the 5-th round. Insert these plaintext-ciphertexts into a hash table indexed by the value of $(L_{4,1}^{(1)}, L_{4,\{2\sim8\}}, (P^{-1}(R_4))_{\{2\sim8\}})$. Any two plaintexts lying in the same row of the hash table forms a pair whose input difference in the 5-th round satisfies $(a|0|0|0|0|0|0|0, P(g|0|0|0|0|0|0|0))$. So the expected number of remaining pairs is about $2^{62.5}$.
3. Guess $K_{15,1}, K_{15,4}$ and $K_{15,\{2,3,5,8\}}$ in turn. For each remaining pair, compute the value of $(S_{15,i}, S'_{15,i})$ for $1 \leq i \leq 5$ and $i = 8$. Keep these pairs satisfying the equations $\Delta S_{15,1} = (P^{-1}(\Delta C_L))_1$ and $\Delta S_{15,l} = (P^{-1}(\Delta C_L))_l \oplus (P^{-1}(\Delta C_L))_4 (l = 2, 3, 5, 8)$. The expected number of remaining pairs is about $2^{22.5}$. Next guess $K_{15,\{6,7\}}$ and calculate the outputs of the 14-th round.
4. Since $K_{14,1} = \overline{K_R^{(60\sim63)}}|K_R^{(0\sim3)}$, we calculate the value of $\Delta S_{14,1}$ for each remaining pair. Keep these pairs satisfying $\Delta S_{14,1} = (P^{-1}(\Delta C_R))_1$. The expected number of remaining pair is about $2^{14.5}$.
5. Guess $K_{5,1}$ as step 4 of Case 1 in section 3.1. If one joint subkey is left, then we recover the master key, else try another differential of A.

Case 2 $a' = 0$ **and** $b' \neq 0$**, or** $a' \neq 0$ **and** $b' = 0$**.** We attack the same example as Case 2 in section 3.1. The 8-round differential and the corresponding subkey are Δ' and $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|K_L^{(0\sim3)} = 0_{(7)}|1_{(7)}$, respectively.

1. Select $2^{41.6}$ structures of ciphertexts. Each structure contains 2^{80} ciphertexts, the right halves of whose differences have the form $P(h|0|0|0h'|0|0|0)$ with h and h' being non-zero bytes. Decrypt them and obtain the corresponding plaintexts.
2. As step 2 of Case 1, we guess 57 bits of K_R and build $2^{41.6}$ hash tables to collect some plaintext-ciphertext pairs satisfying $(\Delta L_4, \Delta R_4) = (a|0|0|0|0|0|0|0, P(g|0|0|0|0|0|0|0))$ with a and g being non-zero bytes and $a^{(1)} = 0$. The expected number of remaining pairs is about $2^{87.6}$.
3. Guess $K_{15,1}$. For each remaining pair, we calculate the value of $(S_{15,1}, S'_{15,1})$ and verify whether the equation $\Delta S_{15,1} = (P^{-1}(\Delta C_L))_1$ holds. If $\Delta S_{15,1} = (P^{-1}(\Delta C_L))_1$ for some pair, this pair will be kept. Next guess $K_{15,8}$, and compute the value of $(S_{15,8}, S'_{15,8})$ for every remaining pair. If $\Delta S_{15,8}^{(1)} \neq (P^{-1}(\Delta C_L))_8^{(1)}$ for one pair, then this pair will be discarded. Finally, guess $K_{15,l}(2 \leq l \leq 7)$. Keep those pairs satisfying these equations $\Delta S_{15,i} = (P^{-1}(\Delta C_L))_i \oplus (\Delta S_{15,8} \oplus (P^{-1}(\Delta C_L))_8)^{(2\sim8)}|0 (i = 6, 7)$ and $\Delta S_{15,j} = (P^{-1}(\Delta C_L))_j \oplus \Delta S_{15,8} \oplus (P^{-1}(\Delta C_L))_8 \oplus \Delta S_{15,7} \oplus (P^{-1}(\Delta C_L))_7 (j = 2, 3, 4, 5)$. In total, the expected number of remaining pairs is about $2^{30.6}$.
4. Because $K_{14,1} = \overline{K_R^{(60\sim63)}}|K_R^{(0\sim3)}$ and $K_{14,5} = K_R^{(28\sim35)}$, we compute $(S_{14,\{1,5\}}, S'_{14,\{1,5\}})$ for each remaining pair. Discard those pairs satisfying $\Delta S_{14,\{1,5\}} \neq (P^{-1}(\Delta C_R))_{\{1,5\}}$. Finally, about $2^{14.6}$ pairs will be kept.
5. Guess $K_{5,1}$ as before. If Δ' is an impossible differential, the expected number of remaining wrong subkey is about $2^{129} \times (1 - 2^{-8})^{2^{14.6}} \approx 1$. We only recover the secret key if one joint subkey is kept.

Case 3 $a' \neq 0$ **and** $b' \neq 0$**.** We attack an example, i.e., the 8-round differential is Δ''. The corresponding subkey is $kl_1^{(2\sim8)}|kl_4^{(2\sim8)} = K_R^{(31\sim37)}|K_L^{(125\sim127)}|\, K_L^{(0\sim3)} = 1_{(14)}$.

1. Choose the same structures of ciphertexts as Case 2. We totally collect $2^{200.6}$ ciphertext pairs.
2. Like step 2 of Case 2, guess the remaining 57 bits of K_R. For each structure, we build a hash table of plaintext-cphertexts indexed by the value of $(L_{4,1}^{(1)}, L_{4,5}^{(8)}, L_{4,1}^{(2\sim8)} \oplus L_{4,5}^{(1\sim7)}, L_{4,\{2\sim4\}}, L_{4,\{6\sim8\}}, (P^{-1}(R_4))_{\{2\sim4\}}, (P^{-1}(R_4))_{\{6\sim8\}})$. Then any two plaintexts in the same row of one hash table forms a pair whose input difference in the 5-th round has the form $(a|0|0|0|a'|0|0|0, P(g|0|0|0|g'|0|0|0))$ with a, a', g and g' being non-zero bytes, $a^{(2\sim8)} = a'^{(1\sim7)}$ and $a^{(1)} = a'^{(8)} = 0$. Therefore, the expected number of remaining pairs is about $2^{95.6}$.
3. As steps 3 and 4 of Case 2 in this section, guess K_{15} and $K_{14,\{1,5\}}$. Finally, about $2^{22.6}$ pairs will be kept.
4. This step is the same as step 5 of Case 3 in section 3.1. The scenario that one subkey is left will be considered.

Complexity. For three cases, the time complexity of Case 3 is maximal, i.e., about $2^{121.6} \times 2^{57} \times 2 \approx 2^{179.6}$ 1-round encryptions. Therefore, the total time complexity is approximately $2^{14} \times 2^{179.6} \times \frac{1}{13} = 2^{189.9}$ 13-round encryptions. The date and memory complexities are $2^{121.6}$ chosen ciphertexts and $2^{95.6} \times 4 \times 2^4 = 2^{101.6}$ bytes, respectively.

4. Impossible Differential Cryptanalysis of 14-Round Camellia-256

In this section, we mount an impossible differential attack on 14-round Camellia-256 from rounds 10 to 23. Since the attack procedure is similar to above section, we will briefly introduce the whole attack as follows.

Case 1 $a' = b' = 0$**.** The 8-round differential and the corresponding subkey are Δ and $kl_3^{(2\sim8)}|kl_6^{(2\sim8)} = K_L^{(61\sim67)}|K_A^{(14\sim20)} = 0_{(14)}$, respectively.

1. Select 2^{67} structures of plaintexts. Each structure contains 2^{55} plaintexts with the form $(P(\alpha_1|x_1|x_2|x_3|x_4|x_5|x_6|x_7), P(\alpha_2|\alpha_3\alpha_4|\alpha_5|\alpha_6|x_8|x_9|\alpha_7))$, where $\alpha_i (1 \leq i \leq 7, i \neq 5)$ and $\alpha_5^{(2\sim8)}$ take all possible values and $\alpha_5^{(1)}$ and $x_j (1 \leq j \leq 9)$ are fixed.
2. Guess 66 bits of K_L, i.e., $K_L^{(109\sim127)}|K_L^{(0\sim46)}$. Since $K_{10} = (K_L \lll 45)_R = K_L^{(109\sim127)}|K_L^{(0\sim44)}$ and $K_{23} = (K_L \lll 111)_L = K_L^{(111\sim127)}|K_L^{(0\sim46)}$, we partially encrypt plaintexts to obtain inputs of the 11-th round and decrypt corresponding ciphertexts to derive outputs of the 22-nd round. For each structure, we insert plaintext-ciphertexts into a hash table indexed by the value of $(L_{10,\{2\sim8\}}, (P^{-1}(R_{10}))_{\{2\sim8\}}, (P^{-1}(R_{22}))_4^{(1)}, (P^{-1}(R_{22}))_{\{6,7\}})$. Any two plaintext-ciphertexts in the same row of this hash table forms a pair. Its input difference in the 11-th round and the right half

of its output difference in the 22-nd round satisfy $(a|0|0|0|0|0|0|0, P(g|0|0|0|0|0|0|0))$ and $P(h_1|h_2 \oplus b|h_3 \oplus b|b|h_4 \oplus b|0|0|h_5 \oplus b)$ with $a, g, b, h_i (1 \leq i \leq 5)$ being non-zero bytes and $a^{(1)} = b^{(1)} = 0$. Thus the expected number of remaining pairs is about $2^{176} \times 2^{-57} = 2^{119}$.

3. Guess $K_{11,1} = K_A^{(45\sim52)}$. For each remaining pair, we calculate $\Delta S_{11,1}$. Keep these pairs satisfying $\Delta S_{11,1} = (P^{-1}(\Delta R_{10}))_1$. About 2^{111} pairs will be kept.
4. Because $K_{22,3} = K_A^{(46\sim53)}$, we only guess one bit of $K_{22,3}$, i.e., $K_{22,3}^{(8)} = K_A^{(53)}$. For each remaining pair, we calculate the value of $(S_{22,3}, S'_{22,3})$. Keep those pairs satisfying $\Delta S_{22,3} = (P^{-1}(\Delta R_{21}))_3$. The expected number of remaining pairs is about 2^{103}. Next guess $K_{22,2} = K_A^{(38\sim45)}$. In fact, we only guess 7 bits of $K_{22,2}$ because we have known the value of $K_{22,2}^{(8)}$. Keep those pairs satisfying $\Delta S_{22,2} = (P^{-1}(\Delta R_{21}))_2$. The expected number of remaining pairs is about 2^{95}. Finally, guess $K_{22,i}$ for $4 \leq i \leq 8$ in turn. Discard those pairs satisfying $\Delta S_{22,i} \neq (P^{-1}(\Delta R_{21}))_i$. The expected number of remaining pairs is about 2^{55}. Guess $K_{22,1}$ and compute the inputs of the 21-st round.
5. Guess $K_{21,1}$, $K_{21,4}$ and $K_{21,j} (j = 2, 3, 5, 8)$ in turn. For each remaining pair, we compute the value of $(S_{21,j}, S'_{21,j})$. Keep those pairs satisfying $\Delta S_{21,1} = (P^{-1}(\Delta R_{20}))_1$ and $\Delta S_{21,j} = (P^{-1}(\Delta R_{20}))_j \oplus (P^{-1}(\Delta R_{20}))_4$. The expected number of remaining pairs is about 2^{15}. Finally, guess $K_{21,\{6,7\}} = K_A^{(6\sim13)}|K_A^{(14\sim21)}$. As a matter of fact, we only guess 9 bits because we have known the value of $K_A^{(14\sim20)}$. Compute the outputs of the 20-th round.
6. Guess $K_{20,1}$. For each remaining pair, we calculate the value of $(\Delta S_{20,1}, (P^{-1}(\Delta R_{19}))_1)$. Remove these guessed subkeys such that $\Delta S_{20,1}$ is equal to $(P^{-1}(\Delta R_{19}))_1$ for one pair. If Δ is an 8-round impossible differential, the expected number of remaining wrong subkeys is about $2^{195} \times (1 - 2^{-8})^{2^{15}} \approx 1$. We recover the secret key from this guessed subkey when one subkey is left.

Case 2 $a' = 0$ **and** $b' \neq 0$**, or** $a' \neq 0$ **and** $b' = 0$**.** We attack one example, i.e., the 8-round differential is Δ'. The corresponding subkey is $kl_3^{(2\sim8)}|kl_6^{(2\sim8)} = K_L^{(61\sim67)}|K_A^{(14\sim20)} = 0_{(7)}|1_{(7)}$.

1. Choose $2^{67.1}$ structures of plaintexts, which have the same form as above Case 1 in this section.
2. Guess K_{10}, K_{23} and $K_{11,1}$, i.e., 66 bits of K_L and 8 bits of K_A. For each plaintext of any structure, compute outputs of the 11-th and 22-nd rounds. Insert these plaintext-ciphertexts into a hash table indexed by $(L_{11}, R_{11,\{2\sim8\}})$. Any two pairs in the same row of the hash table forms a pair whose output difference in the 11-th round satisfies $(0|0|0|0|0|0|0|0, a|0|0|0|0|0|0|0)$. The expected number of remaining pairs is approximately $2^{67.1+109} \times 2^{-48} = 2^{128.1}$.
3. Guess $K_{22,3}$, $K_{22,2}$, $K_{22,i} (i = 4, 6, 7, 8)$ in turn. For each remaining pair, calculate the intermediate value of $(S_{22,j}, S'_{22,j})$ $(2 \leq j \leq 8, j \neq 5)$. Keep those pairs satisfying $\Delta S_{22,j} = (P^{-1}(\Delta R_{21}))_j$. The expected number of remaining pairs is about $2^{80.1}$. Guess $K_{22,\{1,5\}}$ and compute the outputs of the 21-st round.
4. Guess $K_{21,1}, K_{21,7}, K_{21,l} (2 \leq l \leq 8, l \neq 7)$ in turn. Keep those pairs satisfying these equations $\Delta S_{21,1} = (P^{-1}(\Delta R_{20}))_1$, $\Delta S_{21,7}^{(8)} = (P^{-1}(\Delta R_{20}))_7^{(8)}$, $\Delta S_{21,6} = \Delta S_{21,7} \oplus (P^{-1}(\Delta R_{20}))_7 \oplus (P^{-1}(\Delta R_{20}))_6$, $\Delta S_{21,8} = (P^{-1}(\Delta R_{20}))_8 \oplus 0|(\Delta S_{21,7} \oplus (P^{-1}(\Delta R_{20}))_7)^{1\sim7}$, $\Delta S_{21,i} = (P^{-1}(\Delta R_{20}))_i \oplus \Delta S_{21,7} \oplus (P^{-1}(\Delta R_{20}))_7 \oplus \Delta S_{21,8} \oplus (P^{-1}(\Delta R_{20}))_8 (2 \leq i \leq 5)$. The expected number of remaining pairs is about $2^{23.1}$.
5. Guess $K_{20,5}$. Keep those pairs satisfying $\Delta S_{20,5} = (P^{-1}(\Delta L_{20}))_5$. About $2^{15.1}$ pairs will be left. Next guess $K_{20,1}$. If $\Delta S_{20,1} = (P^{-1}(\Delta L_{20}))_1$ for one pair, we remove this guessed subkey. The expected number of remaining wrong subkeys is about $2^{203} \times (1 - 2^{-8})^{2^{15.1}} \approx 1$ if Δ' is an impossible differential. When one subkey is left, we recover the secret key by the key schedule.

Case 3 $a' \neq 0$ **and** $b' \neq 0$**.** We attack the special example, i.e., the 8-round differential is Δ''. The corresponding subkey is $kl_3^{(2\sim8)}|kl_6^{(2\sim8)} = K_L^{(61\sim67)}|K_A^{(14\sim20)} = 1_{(14)}$.

1. Select $2^{42.1}$ structures of plaintexts. Each structure contains 2^{80} plaintexts with the form $(P(\alpha_1|x_1|x_2|x_3|\alpha_2|x_4|x_5|x_6), \alpha_3|\alpha_4|\alpha_5|\alpha_6|\alpha_7|\alpha_8|\alpha_9|\alpha_{10})$, where $\alpha_i (1 \leq i \leq 10)$ take all possible values and $x_j (1 \leq j \leq 6)$ are fixed.
2. Guess K_{10}, K_{23} and $K_{11,\{1,5\}}$ as before. Partially encrypt the plaintexts to derive outputs of 11-th round and decrypt the corresponding ciphertexts to get outputs of 22-nd round. Insert these plaintext-ciphertexts into the hash table indexed by $(L_{11}, R_{11,1}^{(1)}, R_{11,\{2\sim4\}}, R_{11,5}^{8}, R_{11,\{6\sim8\}}, R_{11,1}^{(2\sim8)} \oplus R_{11,5}^{(1\sim7)})$. Any two plaintext-ciphrtetxs in the same row of the hash table forms a pair whose output difference in the 11-th round have the form $(0|0|0|0|0|0|0|0, a|0|0|0|a'|0|0|0)$ with $a^{(1)} = a'^{(8)} = 0$ and $a^{(2\sim8)} = a'^{(1\sim7)}$. The expected number of remaining pairs is about $2^{42.1+159} \times 2^{-73} = 2^{128.1}$.
3. Guess $K_{22}, K_{21}, K_{20,\{1,5\}}$ as above Case 2. Finally, we recover the secret key by the key schedule when one joint subkey is left. Otherwise try another differential of A.

Complexity. Similarly, we analyze the time complexity of each case. We find that the time complexity of Case 3 is maximal, i.e., $2^{215.3}$ 14-round encryptions. Thus the total time complexity is about $2^{229.3}$ 14-round encryptions. The data and memory complexities are $2^{122.1}$ chosen plaintexts and $2^{134.1}$ bytes.

5. Conclusion

In this paper, we have presented the best known attacks on Camellia-192/256 by making full use of the relation between the 8-round differentials of the set A and the values of the subkey. On the one hand, we mount a chosen plaintext attack on 12-round Camellia-192 from rounds 3 to 14 and a chosen ciphertext attack on 13-round Camellia-192 from rounds 3 to 15. The time complexity of our attack on 12-round Camellia-192 is about $2^{148.5}$ 12-round encryptions, which is $2^{22.9}$ times faster than previously known best results on 12-round Camellia-192. The corresponding memory complexity is about $2^{132.7}$ bytes, which is $2^{38.9}$ times smaller than previously known best results on 12-round Camellia-192. More importantly, the attack on 13-round Camellia-192 is presented for the first time. On the other hand, we successfully mount an improved impossible differential attack on 14-round Camellia-256 with $2^{122.1}$ chosen ciphertexts, $2^{229.3}$ 14-round encryptions and $2^{134.1}$ bytes. Compared with the previously fastest known attack on 14-round Camellia-256, the time and memory complexities of our attack are reduced by $2^{8.9}$ and $2^{46.1}$ times and the data complexity is comparable.

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] Bai, D., Li, L.: New impossible differential attacks on camellia. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC. Lecture Notes in Computer Science, vol. 7232, pp. 80–96. Springer (2012)

[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] 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)

[5] Lee, S., Hong, S., Lee, S., Lim, J., Yoon, S.: Truncated differential cryptanalysis of Camellia. In: Kim, K. (ed.) ICISC. Lecture Notes in Computer Science, vol. 2288, pp. 32–38. Springer (2001)

[6] 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)

[7] 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)

[8] Li, L., Chen, J., Wang, X.: Security of reduced-round Camellia against impossible differential attack. IACR Cryptology ePrint Archive 2011, 524 (2011)

[9] Liu, Y., Gu, D., Liu, Z., Li, W.: Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256. Journal of Systems and Software (2012), accepted

[10] Liu, Y., Li, L., Gu, D., Wang, X., Liu, Z., Chen, J., Li, W.: New observations on impossible differential cryptanalysis of reduced-round Camellia. In: FSE (2012), to appear

[11] Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: Malkin, T. (ed.) CT-RSA. Lecture Notes in Computer Science, vol. 4964, pp. 370–386. Springer (2008)

[12] Lu, J., Wei, Y., Kim, J., Fouque, P.A.: Cryptanalysis of reduced versions of the Camellia block cipher. In: Preproceeding of SAC (2011)

[13] 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) (Augst 2011), a full version is available at https://sites.google.com/site/jiqiang/

[14] 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)

[15] Shirai, T.: Differential, linear, boomerange and rectangle cryptanalysis of reduced-round Camellia. Proceedings of 3rd NESSIE Workshop, Munich, Germany (November 6-7 2002)

[16] 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)

[17] Wu, W., Feng, D., Chen, H.: Collision attack and pseudorandomness of reduced-round Camellia. In: Handschuh, H., Hasan, M.A. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 3357, pp. 252–266. Springer (2004)

[18] Wu, W., Zhang, W., Feng, D.: Impossible differential cryptanalysis of reduced-round ARIA and Camellia. J. Comput. Sci. Technol. 22(3), 449–456 (2007)