New Impossible Differential Attacks on Camellia ⋆

Dongxia Bai[1], Leibo Li[2,3]⋆⋆

[1] Department of Computer Science and Technology,
Tsinghua University, Beijing 100084, China
baidx10@mails.tsinghua.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@mail.sdu.edu.cn

Abstract. Camellia is one of the most worldwide used block ciphers, which has been selected as a standard by ISO/IEC. In this paper, we propose several new 7-round impossible differentials of Camellia with 2 FL/FL^{-1} layers, which turn out to be the first 7-round impossible differentials with 2 FL/FL^{-1} layers. Combined with some basic techniques including the early abort approach and the key schedule consideration, we achieve the impossible differential attacks on 11-round Camellia-128, 11-round Camellia-192, 12-round Camellia-192, and 14-round Camellia-256, and the time complexity are $2^{123.6}$, $2^{121.7}$, $2^{171.4}$ and $2^{238.2}$ respectively. As far as we know, these are the best results against the reduced-round variants of Camellia. Especially, we give the first attack on 11-round Camellia-128 reduced version with FL/FL^{-1} layers.

Key words: Camellia, Impossible Differential, Cryptanalysis, Impossible Differential Attack.

1 Introduction

Camellia is a 128-bit block cipher jointly developed by NTT and Mitsubishi in 2000, and supports 128-, 192-, and 256-bit key lengths [1]. It was adopted by cryptographic evaluation projects such as CRYPTREC [5] and NESSIE [22], as well as the standardization activities at IETF [23]. Then it was accepted by ISO/IEC [9] as an international standard.

Camellia has a Feistel structure with FL/FL^{-1} layers inserted every 6 rounds. The FL/FL^{-1} functions are keyed linear functions which are designed to provide non-regularity across rounds and destroy the differential property [1]. As one of the most widely used block cipher, Camellia has attracted a significant amount of attention of the cryptology researchers. The security of Camellia against various attacks are discussed in many papers, such as linear and differential cryptanalysis [24], higher order differential cryptanalysis [7,11], truncated differential attack [5,10,14,25], impossible differential cryptanalysis [4,16,17,18,20,21,25,26], collision attack [15,27], square attack [8,15,28], square like attack [6] et.al. Among these methods, the impossible differential attack [3,12] is the most efficient.

In recent years, there are a number of results on simple versions of Camellia which exclude the FL/FL^{-1} layers. In [4], the authors present the first 6-round impossible differentials with FL/FL^{-1} functions, and give the impossible differential attacks on Camellia-192/-256 with FL/FL^{-1} functions. Then some 7-round impossible differentials with FL/FL^{-1} functions are introduced in [16,17]. In this paper, we propose some new 7-round impossible differentials including 2 FL/FL^{-1} layers, which are the first 7-round impossible differentials including 2 FL/FL^{-1} layers. Due to our new 7-round impossible differentials including one more FL/FL^{-1}

⋆ Supported by the National Natural Science Foundation of China (Grant No. 60931160442), and the Tsinghua University Initiative Scientific Research Program(2009THZ01002).

⋆⋆ Corresponding author.

layer than all of those impossible differentials above, using our new impossible differentials could achieve better attacks. Combined with the early abort approach [19] and the key schedule considerations, we first present the attack on 11-round Camellia-128, which requires $2^{120.5}$ chosen plaintexts and $2^{123.6}$ 11-round encryptions. Then we give attacks on 11-round Camellia-192, 12-round Camellia-192, and 14-round Camellia-256, and the time complexity are $2^{121.7}$, $2^{171.4}$ and $2^{238.2}$ respectively.

The rest of this paper is organized as follows. We give some notations and briefly describe the block cipher Camellia in Section 2. Some properties of Camellia and 7-round impossible differentials with 2 FL/FL^{-1} layers are given in Section 3. Section 4 presents the impossible differential attacks on reduced-round Camellia with FL/FL^{-1} layers. Finally, we conclude the paper in Section 5.

2 Preliminaries

2.1 Notations

In this paper, we will use the following notations:

L_{r-1}, L'_{r-1}	: the left 64-bit half of the r-th round input,
R_{r-1}, R'_{r-1}	: the right 64-bit half of the r-th round input,
ΔS_r	: the output difference of the S-box layer of the r-th round
K_r	: the subkey used in the r-th round
X_l	: the l-th byte of a 64-bit word X ($l = 1, \ldots, 8$)
$Y_{\{i\}}$	: the i-th bit of a bit string Y ($1 \leq i \leq 128$)
$x\|y$	: the concatenation of x and y
$x \lll_i$	: the left rotation of x by i bits
$\oplus$, $\cap$, $\cup$	: bitwise exclusive-OR(XOR), AND, OR

2.2 Description of Camellia

Camellia [1] is a 128-bit block cipher with Feistel structure. It has 18 rounds for 128-bit key and 24 rounds for 192-/256-bit key. We give the encryption procedure of Camellia-128 as follows, see Fig. 1.

Encryption Procedure. First a 128-bit plaintext M is XORed with subkeys $KW_1\|KW_2$ and separated into two 64-bit intermediate values L_0 and R_0 : $L_0\|R_0 = M \oplus (KW_1\|KW_2)$. Then the following operations are performed from $r = 1$ to 18, except for $r = 6$ and 12:

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

for $r = 6$ and 12, do the following:

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

Finally the 128-bit ciphertext C is calculated as: $C = (R_{18}\|L_{18}) \oplus (KW_3\|KW_4)$.
F is the round function defined below:

$$\begin{aligned} F : GF(2)^{64} \times GF(2)^{64} &\rightarrow GF(2)^{64} \\ (X, K_r) &\mapsto Z = P(S(X \oplus K_r)), \end{aligned}$$

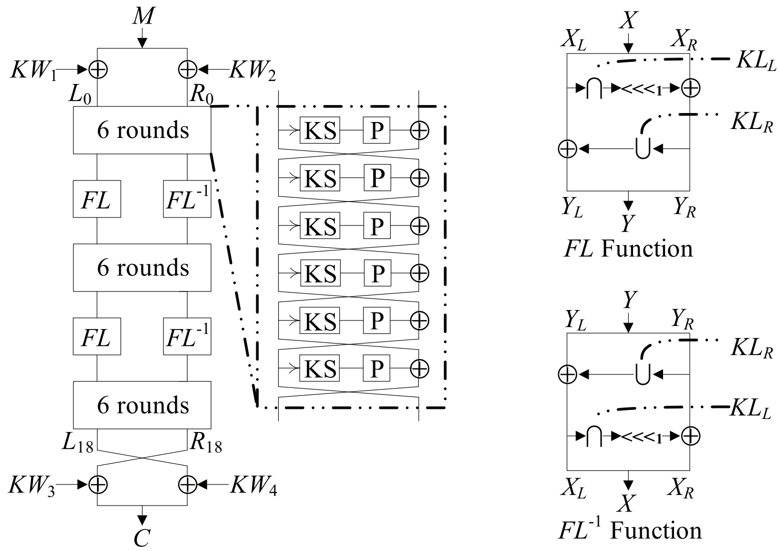

Fig. 1. Encryption procedure of Camellia-128

where S and P are defined as follows:

$$
\begin{gathered}
S : (GF(2)^8)^8 \rightarrow (GF(2)^8)^8 \\
(x_1, x_2, \ldots, x_8) \mapsto (y_1, y_2, \ldots, y_8), \\
y_1 = S_1(x_1),\ y_2 = S_2(x_2),\ y_3 = S_3(x_3),\ y_4 = S_4(x_4), \\
y_5 = S_2(x_5),\ y_6 = S_3(x_6),\ y_7 = S_4(x_7),\ y_8 = S_1(x_8),
\end{gathered}
$$

here S_1, S_2, S_3 and S_4 are the 8×8 S-boxes.

$$
\begin{gathered}
P : (GF(2)^8)^8 \rightarrow (GF(2)^8)^8 \\
(y_1, y_2, \ldots, y_8) \mapsto (z_1, z_2, \ldots, z_8), \\
z_1 = y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8,\ z_5 = y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8, \\
z_2 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8,\ z_6 = y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8, \\
z_3 = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8,\ z_7 = y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8, \\
z_4 = y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7,\ z_8 = y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7.
\end{gathered}
$$

The inverse of P is as follows:

$$
\begin{gathered}
P^{-1} : (GF(2)^8)^8 \rightarrow (GF(2)^8)^8 \\
(z_1, z_2, \ldots, z_8) \mapsto (y_1, y_2, \ldots, y_8), \\
y_1 = z_2 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8,\ y_5 = z_1 \oplus z_2 \oplus z_5 \oplus z_7 \oplus z_8, \\
y_2 = z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8,\ y_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8, \\
y_3 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8,\ y_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7, \\
y_4 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7,\ y_8 = z_1 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8.
\end{gathered}
$$

FL is defined below:

$$FL : GF(2)^{64} \times GF(2)^{64} \rightarrow GF(2)^{64}$$
$$(X_L \| X_R, KL_L \| KL_R) \mapsto (Y_L \| Y_R),$$
$$Y_R = ((X_L \cap KL_L) \lll_1) \oplus X_R,\ Y_L = (Y_R \cup KL_R) \oplus X_L.$$

FL^{-1} is the inverse of FL, and all of them are linear as long as the keys are fixed [2].

Similarly to Camellia-128, Camellia-192/-256 have 24-round Feistel structure with FL/FL^{-1} layers inserted after 6, 12, 18 rounds. Before the first round and after the last round, there are pre- and post-whitening layers which use bitwise exclusive-or operations with 128-bit subkeys, respectively.

Key Schedule. Two 128-bit variables K_A and K_B are generated from the main key $K = K_L \| K_R$. For Camellia-128, K_L is the 128-bit K, and K_R is 0. For Camellia-192, K_L is the left 128-bit of K, and the concatenation of the right 64-bit of K and its complement is used as K_R. For Camellia-256, K_L is the left 128-bit of K, and K_R is the right 128-bit of K. All of the subkeys are derived from rotating K_L, K_R, K_A or K_B, and K_B is only used in Camellia-192/-256. For details of Camellia, we refer to [1].

3 New 7-round Impossible Differentials of Camellia with 2 FL/FL^{-1} layers

In this section, we give some useful properties of Camellia, and then present several new 7-round impossible differentials.

Property 1 *(from [13]) Let x, x', k be 32-bit values, and $\Delta x = x \oplus x'$, then the differential properties of AND and OR operations are:*

$$(x \cap k) \oplus (x' \cap k) = (x \oplus x') \cap k = \Delta x \cap k,$$
$$(x \cup k) \oplus (x' \cup k) = (x \oplus k \oplus (x \cap k)) \oplus (x' \oplus k \oplus (x' \cap k)) = \Delta x \oplus (\Delta x \cap k).$$

Property 2 *For FL^{-1} function, if the input difference is $\Delta Y = (a, 0, 0, 0, 0, 0, 0, 0)$, where a is a non-zero byte whose most significant bit is 0, then the output difference is $\Delta X = (a, 0, 0, 0, A, 0, 0, 0)$, where A is an unknown byte.*

Proof. By Property 1, apparently we can get the output difference below (note that the most significant bit of a is 0):

$$\begin{aligned}\Delta X_L &= X_L \oplus X'_L = (Y_L \oplus (Y_R \cup KL_R)) \oplus (Y'_L \oplus (Y'_R \cup KL_R))\\ &= \Delta Y_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap KL_R) = \Delta Y_L = (a, 0, 0, 0),\\ \Delta X_R &= X_R \oplus X'_R = ((X_L \cap KL_L) \lll_1) \oplus Y_R) \oplus ((X'_L \cap KL_L) \lll_1) \oplus Y'_R)\\ &= \Delta Y_R \oplus ((\Delta X_L \cap KL_L) \lll_1) = (A, 0, 0, 0).\end{aligned}$$

here Y and X are the 64-bit input value and output value of FL^{-1} function, and KL is the 64-bit subkey used in FL^{-1} function, and A is an unknown byte. □

Property 3 *(from [16]) For FL^{-1} function, if the output difference is $\Delta X = (0, 0, 0, 0, b, 0, 0, 0)$, where b is a non-zero byte, then the input difference should satisfy the form $\Delta Y = (B, 0, 0, 0, b, 0, 0, 0)$, where B is an unknown byte.*

Impossible Differential. We now demonstrate that the 7-round differential

$$((0,0,0,0,0,0,0,0);(a,0,0,0,0,0,0,0)) \xrightarrow{7R} ((0,0,0,0,b,0,0,0);(0,0,0,0,0,0,0,0))$$

is impossible, where a is a non-zero byte whose most significant bit is 0, and b is an arbitrary non-zero byte, see Fig. 2.

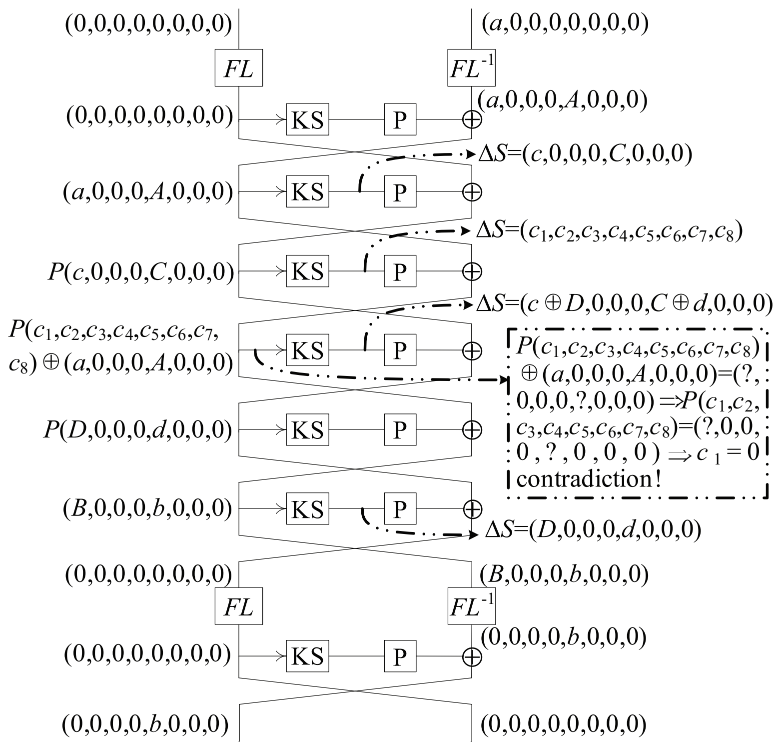

Fig. 2. 7-round impossible differential with 2 FL/FL^{-1} layers

By Property 2, 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 then the output differences of the second and third round are

$$(P(c,0,0,0,C,0,0,0);\ \ (a,0,0,0,A,0,0,0)) \text{ and}$$

$$(P(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8) \oplus (a,0,0,0,A,0,0,0);\ \ P(c,0,0,0,C,0,0,0)),$$

where $(c,0,0,0,C,0,0,0)$ is evolved from $(a,0,0,0,A,0,0,0)$ after key-addition layer and S-box layer, $(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8)$ is evolved from $P(c,0,0,0,C,0,0,0)$ (note that $P(c,0,0,0,C,0,0,0) = (c, c\oplus C, c\oplus C, C, c, C, C, c\oplus C)$), c, c_1, c_5 are unknown non-zero bytes, and C, $c_i (i = 2,3,4,6,7,8)$ are unknown bytes. So we can get that the input difference of S-box layer of the fourth round is

$$P(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8) \oplus (a,0,0,0,A,0,0,0).$$

In the backward direction, the input difference of the seventh round is $((0,0,0,0,0,0,0,0);(0,0,0,0,b,0,0,0))$, and the output difference of the sixth round deduced by Property 3 is $((0,0,0,0,0,0,0,0);(B,0,0,0,b,0,0,0))$. Then the output difference of the fifth round is

$$((B,0,0,0,b,0,0,0);\ \ P(D,0,0,0,d,0,0,0)),$$

where $(D,0,0,0,d,0,0,0)$ is evolved from $(B,0,0,0,b,0,0,0)$ after key-addition layer and S-box layer, d is an unknown non-zero byte, and D is an unknown byte. Hence, the output difference of S-box layer of the fourth round is

$$P^{-1}(P(c,0,0,0,C,0,0,0) \oplus P(D,0,0,0,d,0,0,0)) = (c \oplus D,0,0,0,C \oplus d,0,0,0).$$

Now the input and output differences of S-box layer of the fourth round are all determined. According to the output difference of S-box layer, the input difference of S-box layer should satisfy the form $(?,0,0,0,?,0,0,0)$ (? denotes an unknown byte). So we can get:

$$\begin{aligned}
&P(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8) \oplus (a,0,0,0,A,0,0,0) = (?,0,0,0,?,0,0,0)\\
\Rightarrow\ &P(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8) = (?,0,0,0,?,0,0,0) \oplus (a,0,0,0,A,0,0,0) = (?,0,0,0,?,0,0,0)\\
\Rightarrow\ &c_1 = 0,
\end{aligned}$$

which contradicts with $c_1 \neq 0$. As a result, the differential

$$((0,0,0,0,0,0,0,0);(a,0,0,0,0,0,0,0)) \xrightarrow{7R} ((0,0,0,0,b,0,0,0);(0,0,0,0,0,0,0,0))$$

is impossible. Actually, we can get three more 7-round impossible differentials with 2 FL/FL^{-1} layers, which are:

$$\begin{aligned}
&((0,0,0,0,0,0,0,0);(0,a,0,0,0,0,0,0)) \overset{7R}{\nrightarrow} ((0,0,0,0,0,b,0,0);(0,0,0,0,0,0,0,0)),\\
&((0,0,0,0,0,0,0,0);(0,0,a,0,0,0,0,0)) \overset{7R}{\nrightarrow} ((0,0,0,0,0,0,b,0);(0,0,0,0,0,0,0,0)),\\
&((0,0,0,0,0,0,0,0);(0,0,0,a,0,0,0,0)) \overset{7R}{\nrightarrow} ((0,0,0,0,0,0,0,b);(0,0,0,0,0,0,0,0)),
\end{aligned}$$

where a, b are non-zero bytes, and the most significant bit of a is 0.

4 Impossible Differential Attacks on Camellia with FL/FL^{-1} Layers

In this section, we present some new impossible differential attacks on 11-round Camellia-128, 11-round Camellia-192, 12-round Camellia-192, and 14-round Camellia-256, using the new 7-round impossible differential proposed in Section 3. All of these attacks start from the middle round, and exclude the whitening layers to not change the structure of the algorithm.

4.1 Impossible Differential Attack on 11-round Camellia-128

As illustrated in Fig. 3, the 7-round impossible differential is applied in rounds 7 to 13, and the attack is from round 5 to 15. The attack procedure is as follows.

1. Take 2^n structures of plaintexts $M = (L_4, R_4)$ with following form:

$$(P(x_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\alpha_8);\ P(y_1,y_2,y_3,y_4,y_5,\beta_6,\beta_7,y_8)),$$

   where $\alpha_i\,(i=2,\ldots,8)$, $\beta_j\,(j=6,7)$ are fixed constants, x_1, $y_i\,(i=1,2,3,5,8)$ take all the 8-bit values, and y_4 takes all the 7-bit values with the most significant bit fixed. As a result, each structure contains 2^{55} plaintexts which can provide about 2^{109} plaintext pairs with the difference

$$(P(e,0,0,0,0,0,0,0);P(a_1,a_2,a_3,a,a_5,0,0,a_8)),$$

   where e, a_1, a are non-zero bytes (the most significant bit of a is 0), and $a_i \neq a\,(i=2,3,5,8)$ are unknown bytes. Aggregately, we can collect about 2^{n+109} plaintext pairs.

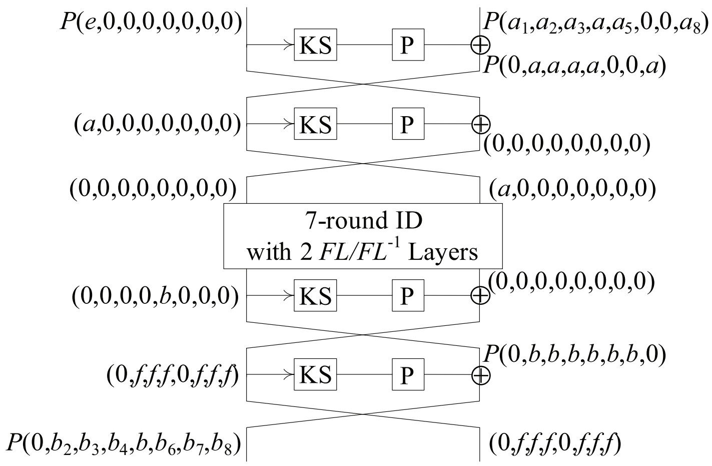

Fig. 3. Attack on 11-round Camellia-128

2. Obtain the ciphertexts of each structure and choose only the pairs that satisfy the following difference by birthday paradox

$$(P(0, b_2, b_3, b_4, b, b_6, b_7, b_8);\ (0, f, f, f, 0, f, f, f)),$$

where b, b_8, f are non-zero bytes, and $b_i \neq b$ $(i = 2, 3, 4, 6, 7)$ are unknown bytes. We expect to have about $2^{n+109-64} = 2^{n+45}$ pairs remaining with this condition.
3. For each plaintext pair, we immediately get the difference $\Delta S_5 = P^{-1}(P(a_1, a_2, a_3, a, a_5, 0, 0, a_8) \oplus P(0, a, a, a, a, 0, 0, a)) = (a_1, a_2 \oplus a, a_3 \oplus a, 0, a_5 \oplus a, 0, 0, a_8 \oplus a)$. So for $l = 1, 2, 3, 5, 8$ guess $K_{5,l}$ and keep only the pairs whose $\Delta S_{5,l}$ is equal to the corresponding value above. The probability of this event is 2^{-40}, thus there remains $2^{n+45-40} = 2^{n+5}$ pairs. Note that $K_{5,l(l=1,2,3,5,8)} = K_{A\{16-39,48-55,72-79\}}$.
4. For each ciphertext pair corresponding to a remaining plaintext pair, obtain the difference $\Delta S_{15} = (0, b_2 \oplus b, b_3 \oplus b, b_4 \oplus b, 0, b_6 \oplus b, b_7 \oplus b, b_8)$. Based on the fact that the bits $K_{A\{16-30\}}$ are already known, perform the following substeps.
   4.1 The value of $K_{15,8}$ $(K_{A\{23-30\}})$ is already known, so use it to partially decrypt every remaining ciphertext pair and keep only the pairs satisfying $\Delta S_{15,8} = b_8$. The probability of this event is 2^{-8}, thus the expected number of remaining pairs is $2^{n+5-8} = 2^{n-3}$.
   4.2 Since $K_{15,7} = K_{A\{15-22\}}$, 7 bits including $K_{A\{16-22\}}$ are already known and guess the only unknown bit $K_{A\{15\}}$. Keep only the pairs satisfying $\Delta S_{15,7} = b_7 \oplus b$. The probability of this event is 2^{-8}, so we expect $2^{n-3-8} = 2^{n-11}$ pairs remain.
   4.3 The values of $K_{15,l(l=2,3,4,6)}$ $(K_{A\{7-14,103-126\}})$ are unknown, so for $l = 2, 3, 4, 6$ respectively guess $K_{15,l}$ and choose only the pairs whose $\Delta S_{15,l}$ is equal to the corresponding value above. The probability of this event is 2^{-32}, thus the expected number of such pairs is $2^{n-11-32} = 2^{n-43}$.
   4.4 Guess $K_{15,1}$ and decrypt every remaining pair to get $(L_{13,5}, L'_{13,5})$, so this step does not effect the number of the remaining pairs.
5. For each remaining pair, obtain the difference $\Delta S_{14} = (0, 0, 0, 0, f, 0, 0, 0)$. Guess $K_{14,5}$ and choose only the pairs satisfying $\Delta S_{14,5} = f$. The probability of this condition is 2^{-8}, thus we expect $2^{n-43-8} = 2^{n-51}$ pairs remain.
6. For $l = 4, 6, 7$ guess $K_{5,l}$ and encrypt every remaining pair to get $(L_{5,1}, L'_{5,1})$.

7. For every remaining pair, guess the 8-bit value of $K_{6,1}$ and calculate the difference $\Delta S_{6,1}$. The probability that $\Delta S_{6,1}$ is equal to a fixed value e is 2^{-8}, where e is already determined by ΔL_4. Such a difference is impossible, so if there exits a pair satisfying this condition, discard the 121-bit wrong subkey guess. Unless the initial assumption on the subkeys K_5, $K_{15,l(l=1,2,3,4,6,7,8)}$ and $K_{14,5}$ is correct, it is expected that we can discard the whole 8-bit value of $K_{6,1}$ for each guessed 113-bit value above since the 121-bit wrong value remains with a very small probability by choosing a proper n. Hence if there remains a value of $K_{6,1}$ after the filtering, we can assume that the guessed value above is right.

Complexity. After analyzing the 2^{n-51} remaining pairs, the expected number of remaining 121-bit wrong keys is $N = (2^{121} - 1)(1 - 2^{-8})^{2^{n-51}}$. In order to let $N \ll 0$, we choose $n = 65.5$. Then the data complexity is $2^{120.5}$ chosen plaintexts. The memory complexity is dominated by storing the $2^{110.5}$ proper pairs in step 2, which requires $2^{115.5}$ bytes. Table 1 shows the time complexity of each step, so the total complexity of the attack, in encryption unit, is about $2^{127}/11 \approx 2^{123.6}$.

Table 1. Time Complexity of the Attack on 11-round Camellia-128

Step	Time Complexity
2	2^{n+55} E
3	$\sum_{i=0}^{4} 2 \times 2^{n+45-8i} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+51} \times 5\ \frac{1}{11}$E
4.1	$2 \times 2^{n+5} \times 2^{40} \times \frac{1}{8} = 2^{n+43}\ \frac{1}{11}$E
4.2	$2 \times 2^{n-3} \times 2^{40} \times 2^{1} \times \frac{1}{8} = 2^{n+36}\ \frac{1}{11}$E
4.3	$\sum_{i=0}^{3} 2 \times 2^{n-11-8i} \times 2^{41} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+38}\ \frac{1}{11}$E
4.4	$2^{n-43} \times 2^{73} \times 2^{8} \times \frac{1}{8} = 2^{n+35}\ \frac{1}{11}$E
5	$2 \times 2^{n-43} \times 2^{81} \times 2^{8} \times \frac{1}{8} = 2^{n+44}\ \frac{1}{11}$E
6	$\sum_{i=0}^{2} 2^{n-51} \times 2^{89} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+43} + 2^{n+51} + 2^{n+59}\ \frac{1}{11}$E
7	$2 \times 2^{113} \times 2^{8} \times (1 + (1 - 2^{-8}) + \ldots + (1 - 2^{-8})^{2^{n-51}-1}) \times \frac{1}{8} \approx 2^{127}\ \frac{1}{11}$E

4.2 Impossible Differential Attack on 11-round and 12-round Camellia-192

In this section, first we give a brief description of the attack on 11-round Camellia-192, and then present the attack on 12-round Camellia-192.

Attack on 11-round Camellia-192. A similar 11-round attack as described in Section 4.1 is equally applicable to Camellia-192 from round 11 to 21, utilizing the 7-round impossible differential in rounds 13 to 19 as shown in Fig.3. According to the key schedule of Camellia-192/-256, we get

$$K_{11} = K_{A\{46-109\}},\ K_{12,1} = K_{A\{110-117\}},$$
$$K_{20,5} = K_{R\{63-70\}},\ K_{21,l(l=1,2,3,4,6,7,8)} = K_{A\{7-30,95-126\}}.$$

Considering the redundancy in $K_{11}, K_{12,1}$ and $K_{21,l(l=1,2,3,4,6,7,8)}$, in fact we only need to guess 113 bits $K_{A\{7-30,46-126\}} \| K_{R\{63-70\}}$. By choosing $n = 65.4$, then $N \ll 0$. Consequently, this attack requires $2^{120.4}$ chosen plaintexts, $2^{115.4}$ bytes of memory and an overall effort of $2^{120.4} + 2^{124.4}/11 \approx 2^{121.7}$ eleven-round Camellia-192 encryptions. The details see Table 3 in Appendix A.

Attack on 12-round Camellia-192. We add one round on the bottom of the 11-round attack, and give a 12-round attack on Camellia-192, which is from round 11 to 22, see Fig. 4. The attack procedure is as follows.

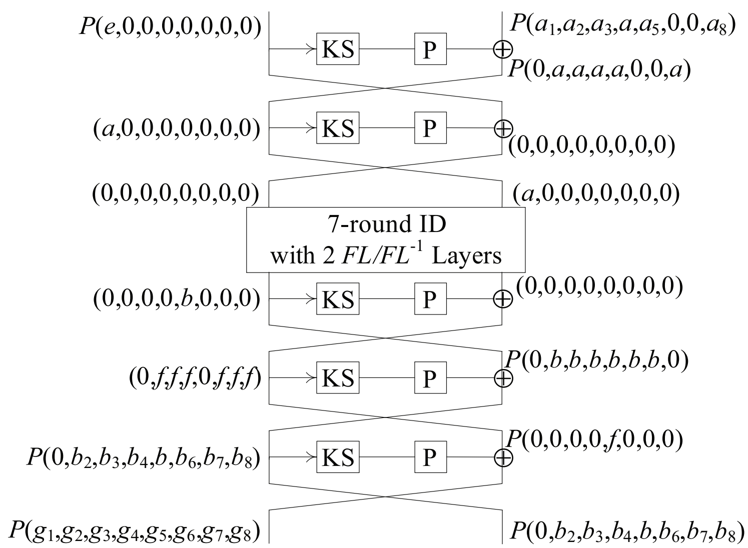

Fig. 4. Attack on 12-round Camellia-192

1. The choice of plaintexts is the same as the 11-round attack, and the ciphertext pairs are sieved by the difference

$$(P(g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8);\ P(0, b_2, b_3, b_4, b, b_6, b_7, b_8)),$$

where b, b_8 are non-zero bytes, and $g_i\,(i = 1, \ldots, 8)$, $b_j \neq b\,(j = 2, 3, 4, 6, 7)$ are unknown bytes. The probability of this condition is about 2^{-8}, so the expected number of remaining pairs is about $2^{n+109-8} = 2^{n+101}$.
2. Obtain the difference $\Delta S_{11} = (a_1, a_2 \oplus a, a_3 \oplus a, 0, a_5 \oplus a, 0, 0, a_8 \oplus a)$, then for $l = 1, 2, 3, 5, 8$ guess $K_{11,l}$ and keep the pairs whose $\Delta S_{11,l}$ is equal to the corresponding value above. So we expect $2^{n+101} \times 2^{-40} = 2^{n+61}$ pairs remain. Note that $K_{11,l(l=1,2,3,5,8)} = K_{A\{46-69,78-85,102-109\}}$.
3. We can get the difference $\Delta S_{22} = (g_1, g_2, g_3, g_4, g_5 \oplus f, g_6, g_7, g_8)$ ($\Delta S_{22,5} \neq g_5$ since $f \neq 0$), and the bits $K_{A\{46-69,78-85\}}$ are already known. Then perform the following substeps.
   - 3.1 The values of $K_{22,l(l=3,4)}$ ($K_{A\{47-62\}}$) are already known, so for $l = 3, 4$ $\Delta S_{22,l}$ can be computed, then choose the pairs satisfying $\Delta S_{22,l} = g_l$. Thus there remains $2^{n+61} \times 2^{-16} = 2^{n+45}$ pairs.
   - 3.2 Since $K_{22,7} = K_{A\{79-86\}}$, guess the only unknown bit $K_{A\{86\}}$ and keep the pairs satisfying $\Delta S_{22,7} = g_7$. Next $K_{22,2} = K_{A\{39-46\}}$, guess the unknown 7 bits $K_{A\{39-45\}}$ and keep the pairs satisfying $\Delta S_{22,2} = g_2$. Similarly, as $K_{22,6} = K_{A\{71-78\}}$, we guess the unknown 7 bits $K_{A\{71-77\}}$ and keep the pairs satisfying $\Delta S_{22,6} = g_6$. Thus the expected number of remaining pairs is $2^{n+45} \times 2^{-24} = 2^{n+21}$.
   - 3.3 The values of $K_{22,l(l=1,8)}$ ($K_{A\{31-38,87-94\}}$) are unknown, so for $l = 1, 8$ guess $K_{22,l}$ and choose the pairs satisfying $\Delta S_{22,l} = g_l$. Then $2^{n+21} \times 2^{-16} = 2^{n+5}$ pairs remain. As $K_{22,5} = K_{A\{63-70\}}$, guess the only unknown bit $K_{A\{70\}}$ and keep only the pairs satisfying

$\Delta S_{22,5} \neq g_5$. The probability of this event is $(2^8-1)/2^8 \approx 1$, thus we expect about 2^{n+5} pairs remain. And now the intermediate values $(L_{21}\|R_{21}, L'_{21}\|R'_{21})$ also can be computed.

4. We can obtain $\Delta S_{21} = (0, b_2 \oplus b, b_3 \oplus b, b_4 \oplus b, 0, b_6 \oplus b, b_7 \oplus b, b_8)$, and the bits $K_{A\{102-109\}}$ are already known. So perform the substeps below.
   4.1 As $K_{21,2} = K_{A\{103-110\}}$, guess the only unknown bit $K_{A\{110\}}$ and keep the pairs satisfying $\Delta S_{21,2} = b_2 \oplus b$. Then we expect $2^{n+5} \times 2^{-8} = 2^{n-3}$ pairs remain.
   4.2 The values of $K_{21,l(l=3,4,6,7,8)}$ $(K_{A\{7-30,111-126\}})$ are unknown, so for $l = 3,4,6,7,8$ guess $K_{21,l}$ and keep only the pairs whose $\Delta S_{21,l}$ is equal to the corresponding value above. Then the expected number of such pairs is $2^{n-3} \times 2^{-40} = 2^{n-43}$.
   4.3 Since $K_{21,1} = K_{A\{95-102\}}$, guess the unknown 7 bits $K_{A\{95-101\}}$ and get $(L_{19,5}, L'_{19,5})$.
5. Obtain the difference $\Delta S_{20} = (0,0,0,0,f,0,0,0)$, then guess $K_{20,5}$ and choose the pairs satisfying $\Delta S_{20,5} = f$. So there remains $2^{n-43} \times 2^{-8} = 2^{n-51}$ pairs.
6. The values of $K_{11,l(l=4,6,7)}$ $(K_{A\{70-77,86-101\}})$ are already known, so we can get $(L_{11,1}, L'_{11,1})$.
7. Since $K_{12,1}$ $(K_{A\{110-117\}})$ are already known, for every remaining pair, $\Delta S_{12,1}$ can be computed. We expect with probability of 2^{-8} that we get a pair with $\Delta S_{12,1} = e$, where e is a fixed value determined by ΔL_{10}. Such a difference is impossible, and every subkey we guessed that proposes such a difference is definitely a wrong key. If there remains a value of $K_{12,1}$ after the filtering, we can assume that the guessed value above is right.

Complexity. The number of remaining 128-bit wrong keys after analyzing all the 2^{n-51} pairs is $N = (2^{128}-1)(1-2^{-8})^{2^{n-51}}$. In order to let $N \ll 0$, we choose $n = 65.6$. Then the data complexity is $2^{120.6}$ chosen plaintexts. The memory complexity is dominated by storing the $2^{166.6}$ pairs in step 2, which is about $2^{171.6}$ bytes. The time complexity is dominated by step 3, which is about $2^{n+107} \times 5/12 = 2^{172.6} \times 5/12 \approx 2^{171.4}$ 12-round encryptions. The details see Table 4 in Appendix A.

4.3 Impossible Differential Attack on 14-round Camellia-256.

We add one more round respectively on the top and bottom of the 12-round attack, and present a 14-round attack on Camellia-256, which is from round 10 to 23 as illustrated in Fig. 5. The attack procedure is below.

1. Take 2^n structures of plaintexts $M = (L_9, R_9)$ with following form:

$$(P(x_1, x_2, x_3, x_4, x_5, \alpha_6, \alpha_7, x_8);\ P(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)),$$

   where α_i $(i = 6,7)$ are fixed constants, x_i $(i = 1,2,3,5,8)$, y_j $(j = 1,\dots,8)$ take all the 8-bit values, and x_4 takes all the 7-bit values with the most significant bit fixed. It is obvious that each structure contains 2^{111} plaintexts which can provide about 2^{221} plaintext pairs with the difference

$$(P(a_1, a_2, a_3, a, a_5, 0, 0, a_8); P(h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8)),$$

   where a_1, a are non-zero byte (the most significant bit of a is 0), and $a_i \neq a$ $(i = 2,3,5,8)$, h_j $(j = 1,\dots,8)$ are unknown bytes. Hence, we can collect about 2^{n+221} plaintext pairs, then obtain the ciphertexts of each structure.
2. We can get that $\Delta S_{10} = (h_1 \oplus e, h_2, h_3, h_4, h_5, h_6, h_7, h_8)$ $(\Delta S_{10,1} \neq h_1$ since $e \neq 0)$, so for $l = 2,\dots,8,1$ respectively guess $K_{10,l}$ and choose only the pairs with $\Delta S_{10,l}$ satisfying the condition above. Then we expect about $2^{n+221} \times 2^{-56} = 2^{n+165}$ pairs remain. Note that $K_{10} = K_{L\{1-45,110-128\}}$. In this step, we can get $(L_{10}\|R_{10}, L'_{10}\|R'_{10})$.

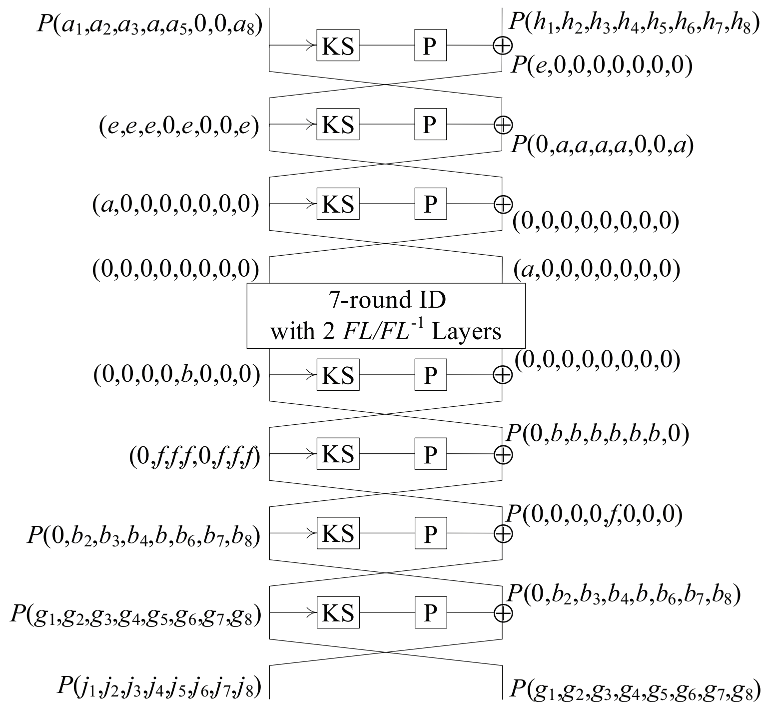

Fig. 5. Attack on 14-round Camellia-256

3. We can obtain the difference $\Delta S_{23} = (j_1, j_2 \oplus b_2, j_3 \oplus b_3, j_4 \oplus b_4, j_5 \oplus b, j_6 \oplus b_6, j_7 \oplus b_7, j_8 \oplus b_8)$ ($\Delta S_{23,5} \neq j_5$ since $b \neq 0$), and the bits $K_{L\{1-45,112-128\}}$ are already known.
   3.1 The values of $K_{23,l(l=1,\ldots,7)}$ ($K_{L\{1-39,112-128\}}$) are already known, so for $l = 1, \ldots, 7$, $\Delta S_{23,l}$ can be computed, then choose only the pairs satisfying $\Delta S_{23,1} = j_1$ and $\Delta S_{23,5} \neq j_5$. The probability of this condition is $2^{-8} \times ((2^8 - 1)/2^8) \approx 2^{-8}$, thus the expected number of remaining pairs is $2^{n+165-8} = 2^{n+157}$.
   3.2 Since $K_{23,8} = K_{L\{40-47\}}$, guess the unknown 2 bits $K_{L\{46,47\}}$ and get the intermediate values $(L_{22} \| R_{22}, L'_{22} \| R'_{22})$.

Next, we perform the steps 4 to 9, which are totally the same as steps 3 to 8 of Section 4.2. Finally we expect 2^{n+5} pairs remain.

Complexity. The expected number of remaining 194-bit wrong keys after analyzing all the 2^{n+5} pairs is $N = (2^{194} - 1)(1 - 2^{-8})^{2^{n+5}}$. In order to let $N \ll 0$, we choose $n = 10.2$. Then the data complexity is $2^{121.2}$ chosen plaintexts. The memory complexity is dominated by storing the $2^{n+165} = 2^{175.2}$ pairs in step 2, which is about $2^{180.2}$ bytes. The time complexity is dominated by step 2 and step 4, which is about $(2^{n+230} + 2^{n+229} \times 5)/14 = 2^{n+228} = 2^{238.2}$ encryptions. Table 5 in Appendix A shows the details of each step.

5 Conclusion

In this paper, we propose some new 7-round impossible differentials including 2 FL/FL^{-1} layers, and then present attacks on 11-round Camellia-128, 11-round Camellia-192, 12-round Camellia-192 and 14-round Camellia-256 without whitening layers. A summary of the previous works and our attacks on Camellia with FL/FL^{-1} layers is given in Table 2.

Table 2. Summary of Attacks on Camellia with FL/FL^{-1} Layers

Cipher	#Rounds	Attack Type	Data	Time	Source
Camellia-128	9$*$	Square Attack	2^{48}CP	2^{122}	[15]
	10$*$	Impossible DC	2^{118}CP	2^{118}	[20]
	10$*$	Impossible DC	$2^{118.5}$CP	$2^{123.5}$	[16]
	10 (Weak Key)	Impossible DC	$2^{110.4}$CP	$2^{110.4}$	[17]
	10	Impossible DC	$2^{112.4}$CP	2^{120}	[17]
	11$*$	Impossible DC	$2^{120.5}$CP	$2^{123.6}$	this paper
Camellia-192	11$*$	Impossible DC	2^{118}CP	$2^{163.1}$	[20]
	11 (Weak Key)	Impossible DC	$2^{119.5}$CP	$2^{138.54}$	[17]
	11	Impossible DC	$2^{113.7}$CP	2^{184}	[17]
	11$*$	Impossible DC	$2^{120.4}$CP	$2^{121.7}$	this paper
	12$*$	Impossible DC	$2^{120.1}$CP	2^{184}	[17]
	12$*$	Impossible DC	$2^{120.6}$CP	$2^{171.4}$	this paper
Camellia-256	12 (Weak Key)	Impossible DC	$2^{119.7}$CP	$2^{202.55}$	[17]
	12	Impossible DC	$2^{114.8}$CP/CC	2^{240}	[17]
	14$*$	Impossible DC	2^{120}CC	$2^{250.5}$	[17]
	14$*$	Impossible DC	$2^{121.2}$CP	$2^{238.2}$	this paper

$*$: the attack does not include the whitening layers;
Weak Key: the weak key space which contains 3×2^{126} keys

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: SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001)
2. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Specification of Camellia–a 128-bit block cipher. version 2.0 (2001), http://info.isl.ntt.co.jp/crypt/eng/camellia/specifications.html
3. 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)
4. Chen, J., Jia, K., Yu, H., Wang, X.,: New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256. In: ACISP 2011, LNCS 6812, pp. 16–33. Springer, Heidelberg (2011)
5. CRYPTREC-Cryptography Research and Evaluation Committees, report, Archive (2002), http://www.cryptrec.go.jp/english/index.html
6. 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)
7. 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)
8. He, Y., Qing, S.: Square Attack on Reduced Camellia Cipher. In: Qing, S., Okamoto, T., Zhou, J. (eds.) ICICS 2001. LNCS, vol. 2229, pp. 238–245. Springer, Heidelberg (2001)
9. International Standardization of Organization (ISO), International Standard-ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms-Part 3: Block ciphers (2005)
10. Kanda, M., Matsumoto, T.: Security of Camellia against Truncated Differential Cryptanalysis. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 119–137. Springer, Heidelberg (2002)
11. Kawabata, T., Kaneko, T.: A Study on Higher Order Differential Attack of Camellia. In: The 2nd open NESSIE workshop (2001)
12. Knudsen, L.R.: DEAL–a 128-bit Block Cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998)
13. Kühn, U.: Improved Cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
14. Lee, S., Hong, S.H., Lee, S.-J., Lim, J.-I., Yoon, S.H.: Truncated Differential Cryptanalysis of Camellia. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 32–38. Springer, Heidelberg (2002)
15. Duo, L., Li, C., Feng, K.: New Observation on Camellia. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer, Heidelberg (2006)
16. Li, L., Chen, J., Jia, K.: New Impossible Differential Cryptanalysis of Reduced-round Camellia. To appear in: CANS 2011.(2011)

17. Li, L., Chen, J., Wang, X.: Security of Reduced-Round Camellia against Impossible Differential Attack, http://eprint.iacr.org/2011/524.pdf
18. Lu, J.: Cryptanalysis of Block Ciphers. PhD Thesis, Department of Mathematics, Royal Holloway, University of London, England (2008)
19. Lu, J., Kim, J.-S., Keller, N., Dunkelman, O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer, Heidelberg (2008)
20. Lu, J., Wei, Y., Kim, J., Fouque, P.A.: Cryptanalysis of Reduced Versions of the Camellia Block Cipher. To appear in: SAC 2011. (2011)
21. 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)
22. NESSIE–New European Schemes for Signatures, Integrity, and Encryption, final report of European project IST-1999-12324. Archive (1999), https://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf
23. NTT Information Sharing Platform Laboratories: Internationally Standardized Encryption Algorithm from Japan "Camellia", http://info.isl.ntt.co.jp/crypt/index.html
24. Shirai, T.: Differential, linear, boomerang and rectangle Cryptanalysis of Reduced-Round Camellia. In: Proceedings of the Third NESSIE Workshop, Munich, Germany, (November 6–7, 2002)
25. 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)
26. Wu, W., Zhang, W., Feng, D.: Impossible differential cryptanalysis of Reduced- Round ARIA and Camellia. Journal of Computer Science and Technology 22(3), 449–456 (2007)
27. 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)
28. Yeom, Y., Park, S., Kim, I.: On the Security of Camellia against the Square Attack. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 89–99. Springer, Heidelberg (2002)

A Time Complexity of Attacks in Section 4

Table 3. Time Complexity of the Attack on 11-round Camellia-192

Step	Time Complexity
2	2^{n+55} E
3	$\sum_{i=0}^{4} 2 \times 2^{n+45-8i} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+51} \times 5\ \frac{1}{11}$E
4.1	$2 \times 2^{n+5} \times 2^{40} \times 2^{1} \times \frac{1}{8} = 2^{n+44}\ \frac{1}{11}$E
4.2	$\sum_{i=0}^{4} 2 \times 2^{n-3-8i} \times 2^{41} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+44} \times 5\ \frac{1}{11}$E
4.3	$2^{n-43} \times 2^{81} \times 2^{7} \times \frac{1}{8} = 2^{n+42}\ \frac{1}{11}$E
5	$2 \times 2^{n-43} \times 2^{88} \times 2^{8} \times \frac{1}{8} = 2^{n+51}\ \frac{1}{11}$E
6.1	$2^{n-51} \times 2^{96} \times 2^{1} \times \frac{1}{8} = 2^{n+43}\ \frac{1}{11}$E
6.2	$\sum_{i=0}^{1} 2^{n-51} \times 2^{97} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+51} + 2^{n+59}\ \frac{1}{11}$E
7	$2 \times 2^{113} \times (1 + (1-2^{-8}) \ldots + (1-2^{-8})^{2^{n-51}-1}) \times \frac{1}{8} \approx 2^{119}\ \frac{1}{11}$E

Table 4. Time Complexity of the Attack on 12-round Camellia-192

Step	Time Complexity
2	2^{n+55} E
3	$\sum_{i=0}^{4} 2 \times 2^{n+101-8i} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+107} \times 5\ \frac{1}{12}$E
4.1	$\sum_{i=0}^{1} 2 \times 2^{n+61-8i} \times 2^{40} \times \frac{1}{8} = 2^{n+99} + 2^{n+91}\ \frac{1}{12}$E
4.2	$2 \times 2^{n+45} \times 2^{40} \times 2^{1} \times \frac{1}{8} = 2^{n+84}\ \frac{1}{12}$E
	$2 \times 2^{n+37} \times 2^{41} \times 2^{7} \times \frac{1}{8} = 2^{n+83}\ \frac{1}{12}$E
	$2 \times 2^{n+29} \times 2^{48} \times 2^{7} \times \frac{1}{8} = 2^{n+82}\ \frac{1}{12}$E
4.3	$\sum_{i=0}^{1} 2 \times 2^{n+21-8i} \times 2^{55} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+83}\ \frac{1}{12}$E
	$2 \times 2^{n+5} \times 2^{71} \times 2^{1} \times \frac{1}{8} = 2^{n+75}\ \frac{1}{12}$E
5.1	$2 \times 2^{n+5} \times 2^{72} \times 2^{1} \times \frac{1}{8} = 2^{n+76}\ \frac{1}{12}$E
5.2	$\sum_{i=0}^{4} 2 \times 2^{n-3-8i} \times 2^{73} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+76} \times 5\ \frac{1}{12}$E
5.3	$2^{n-43} \times 2^{113} \times 2^{7} \times \frac{1}{8} = 2^{n+74}\ \frac{1}{12}$E
6	$2 \times 2^{n-43} \times 2^{120} \times 2^{8} \times \frac{1}{8} = 2^{n+83}\ \frac{1}{12}$E
7	$2^{n-51} \times 2^{128} \times \frac{1}{8} \times 3 = 2^{n+74} \times 3\ \frac{1}{12}$E
8	$2 \times 2^{128} \times (1 + (1-2^{-8}) + \ldots + (1-2^{-8})^{2^{n-51}-1}) \times \frac{1}{8} \approx 2^{134}\ \frac{1}{12}$E

Table 5. Time Complexity of the Attack on 14-round Camellia-256

Step	Time Complexity
1	2^{n+111} E
2	$\sum_{i=0}^{7} 2 \times 2^{n+221-8i} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+230}\ \frac{1}{14}$E
3.1	$2 \times 2^{n+165} \times 2^{64} \times \frac{1}{8} + 2 \times 2^{n+157} \times 2^{64} \times \frac{1}{8} \times 6 = 2^{n+227} + 2^{n+219} \times 6\ \frac{1}{14}$E
3.2	$2 \times 2^{n+157} \times 2^{64} \times 2^{2} \times \frac{1}{8} = 2^{n+221}\ \frac{1}{14}$E
4	$\sum_{i=0}^{4} 2 \times 2^{n+157-8i} \times 2^{66} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+229} \times 5\ \frac{1}{14}$E
5.1	$\sum_{i=0}^{1} 2 \times 2^{n+117-8i} \times 2^{106} \times \frac{1}{8} = 2^{n+221} + 2^{n+213}\ \frac{1}{14}$E
5.2	$2 \times 2^{n+101} \times 2^{106} \times 2^{1} \times \frac{1}{8} = 2^{n+206}\ \frac{1}{14}$E
	$2 \times 2^{n+93} \times 2^{107} \times 2^{7} \times \frac{1}{8} = 2^{n+205}\ \frac{1}{14}$E
	$2 \times 2^{n+85} \times 2^{114} \times 2^{7} \times \frac{1}{8} = 2^{n+204}\ \frac{1}{14}$E
5.3	$\sum_{i=0}^{1} 2 \times 2^{n+77-8i} \times 2^{121} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+205}\ \frac{1}{14}$E
	$2 \times 2^{n+61} \times 2^{137} \times 2^{1} \times \frac{1}{8} = 2^{n+197}\ \frac{1}{14}$E
6.1	$2 \times 2^{n+61} \times 2^{138} \times 2^{1} \times \frac{1}{8} = 2^{n+198}\ \frac{1}{14}$E
6.2	$\sum_{i=0}^{4} 2 \times 2^{n+53-8i} \times 2^{139} \times 2^{8(i+1)} \times \frac{1}{8} = 2^{n+198} \times 5\ \frac{1}{14}$E
6.3	$2^{n+13} \times 2^{179} \times 2^{7} \times \frac{1}{8} = 2^{n+196}\ \frac{1}{14}$E
7	$2 \times 2^{n+13} \times 2^{186} \times 2^{8} \times \frac{1}{8} = 2^{n+205}\ \frac{1}{14}$E
8	$2^{n+5} \times 2^{194} \times \frac{1}{8} \times 3 = 2^{n+196} \times 3\ \frac{1}{14}$E
9	$2 \times 2^{194} \times (1 + (1 - 2^{-8}) + \ldots + (1 - 2^{-8})^{2^{n+5}-1}) \times \frac{1}{8} \approx 2^{200}\ \frac{1}{14}$E