Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis

Makoto Sugita[1], Kazukuni Kobara[2], and Hideki Imai[2]

[1] NTT Network Innovation Laboratories, NTT Corporation
1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847 Japan
sugita@wslab.ntt.co.jp
[2] Institute of Industrial Sciences, The University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo, 153-8505, Japan
{kobara,imai}@imailab.iis.u-tokyo.ac.jp

Abstract. This paper describes truncated and impossible differential cryptanalysis of the 128-bit block cipher Camellia, which was proposed by NTT and Mitsubishi Electric Corporation. Our work improves on the best known truncated and impossible differential cryptanalysis. As a result, we show a nontrivial 9-round byte characteristic, which may lead to a possible attack of reduced-round version of Camellia without input/output whitening, FL or FL^{-1} in a chosen plain text scenario. Previously, only 6-round differentials were known, which may suggest a possible attack of Camellia reduced to 8-rounds. Moreover, we show a nontrivial 7-round impossible differential, whereas only a 5-round impossible differential was previously known. This cryptanalysis is effective against general Feistel structures with round functions composed of S-D (Substitution and Diffusion) transformation.

Keywords: Block Cipher Camellia, Truncated Differential Cryptanalysis, Impossible Differential Cryptanalysis

1 Introduction

Camellia is a 128-bit block cipher proposed by NTT and Mitsubishi Electric Corporation [1]. It was designed to withstand all known cryptanalytic attacks and to provide a sufficient headroom to allow its use over the next $10-20$ years. Camellia supports 128-bit block size and 128-, 192-, and 256-bit key lengths, i.e. the same interface specifications as the Advanced Encryption Standard (AES). Camellia was proposed in response to the call for contributions from ISO/IEC JTC 1/SC27 with the aim of it being adopted as an international standard. Camellia was also submitted to NESSIE (New European Schemes for Signature, Integrity, and Encryption). Furthermore, Camellia was submitted to CRYPTREC (CRYPTography Research & Evaluation Committee) in Japan and it is now being evaluated.

C. Boyd (Ed.): ASIACRYPT 2001, LNCS 2248, pp. 193–207, 2001.

Like E2 [5], which was submitted to AES, Camellia uses a combination of a Feistel structure and the SPN-(Substitution and Permutation Network)-structure, but it also includes new features such as the use of improved linear transformation in SPN-structures, the change of SPN-structures from three layers into two, and the use of input/output whitening, FL and FL^{-1}. The result is improved immunity against truncated differential cryptanalysis, which was applied successfully against reduced-round version of E2 by Matsui and Tokita [12].

Truncated differential cryptanalysis was introduced by Knudsen [4], as a generalization of differential crypanalysis [3]. He defined them as differentials where only a part of the differential can be predicted. The notion of truncated differentials as introduced by him is wide, but with a byte-oriented cipher such as E2 or Camellia, it is natural to study byte-wise differentials as truncated differentials.

The initial analysis of the security of Camellia and its resistance to the truncated and impossible differential cryptanalysis is given in [1], [6]. They state that Camellia with more than 11 rounds is secure against truncated differential cryptanalysis, though they did not indicate the effective truncated differentials. Up to now, the effective cryptanalysis applicable to Camellia has been the higher order differential cryptanalysis proposed by Kawabata, et al.[7], which utilizes non-trivial 6-round higher order differentials, and the differential crypatanalysis which utilizes a 7-round differential [2].

Our analysis improves on the best known truncated and impossible cryptanalysis against Camellia. Our cryptanalysis finds a nontrivial 9-round truncated differential, which may lead to a possible attack of Camellia reduced to 11-rounds without input/output whitening, FL, or FL^{-1} by a chosen plain text scenario. Moreover, we show a nontrivial 7-round impossible differential, whereas only a 5-round impossible differentials were previously known.

The contents of this paper are as follows. In Section 2, we describes the structures of block ciphers, truncated differential probabilities, impossible differential cryptanalysis and the block cipher Camellia. In Section 3, we describe the previous work on the security of block cipher Camellia. In Section 4, we cryptanalyze Camellia by truncated differential cryptanalysis. In Section 5, we cryptanalyze Camellia by impossible differential cryptanalysis. Section 6 concludes this paper.

2 Preliminaries

In this section, we describe the general structures of block ciphers, truncated differential probabilities, impossible differential cryptanalysis and the block cipher Camellia.

2.1 Feistel Structures

Associate with a function $f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^n$, a function $D_{2n,f}(L, R) = (R \oplus f(L), L)$ for all $L, R \in \mathrm{GF}(2)^n$. $D_{2n,f}$ is called the Feistel transformation associated with f. Furthermore, for functions $f_1, f_2, \cdots, f_s : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^n$,

define $\psi_n(f_1, f_2, \cdots, f_s) = D_{2n,f_s} \circ \cdots \circ D_{2n,f_2} \circ D_{2n,f_1}$. We call $F(f_1, f_2, \cdots, f_s) = \psi_n(f_1, f_2, \cdots, f_s)$ the s-round Feistel structure. At this time, we call the functions $f_1, f_2, \cdots, f_s$ the round functions of the Feistel structure $F(f_1, f_2, \cdots, f_s)$.

2.2 SPN-Structures [9]

This structure consists of two kinds of layers: nonlinear layer and linear layer. Each layer has different features as follows.

Nonlinear (Substitution) layer: This layer is composed of m parallel n-bit bijective nonlinear transformations.

Linear (Diffusion) layer: This layer is composed of linear transformations over the field $\mathrm{GF}(2^n)$ (especially in the case of E2 and Camellia, $\mathrm{GF}(2)$), where inputs are transformed linearly to outputs per word (n-bits).

Next for positive integer s, we define the s-layer SPN-structure that consists of s layers. First is a nonlinear layer, second is a linear layer, third is a nonlinear layer, $\cdots$.

2.3 Word Characteristics

We define a word characteristic function $\chi : \mathrm{GF}(2^n)^m \to \mathrm{GF}(2)^m$, $(a_1, \cdots, a_m) \longmapsto (b_1, \cdots, b_m)$ by

$$b_i = \begin{cases} 0 \text{ if } a_i = 0 \\ 1 \text{ otherwise,} \end{cases}$$

Hereafter, we call $\chi(a)$ the word characteristic of $a \in \mathrm{GF}(2^n)^m$. Especially in the case of $n = 8$, we call $\chi(a)$ the byte characteristic.

2.4 Truncated Differential Probability

Definition 1. *Let $\Delta x, \Delta y \in \mathrm{GF}(2^n)^m$ denote the input and output differences of the function f, respectively.*

$$\Delta x = (\Delta x_1, \Delta x_2, \cdots, \Delta x_m)$$
$$\Delta y = (\Delta y_1, \Delta y_2, \cdots, \Delta y_m)$$

We define the input and output truncated differential $(\delta x, \delta y) \in (\mathrm{GF}(2)^m)^2$ of the function f, where

$$\delta x = (\delta x_1, \delta x_2, \cdots, \delta x_m)$$
$$\delta y = (\delta y_1, \delta y_2, \cdots, \delta y_m)$$

by $\delta x = \chi(\Delta x), \delta y = \chi(\Delta y)$.

Let $p_f(\delta x, \delta y)$ denote the transition probability of the truncated differential induced by function f. $p_f(\delta x, \delta y)$ is defined on the truncated differential $(\delta x, \delta y)$. Truncated differential probability $p_f(\delta x, \delta y)$ is defined by

$$p_f(\delta x, \delta y) = 1/c \sum_{\chi(\Delta x)=\delta x, \chi(\Delta y)=\delta y} \Pr(x \in \mathrm{GF}(2^n)^m | f(x) \oplus f(x \oplus \Delta x) = \Delta y),$$

where c is the number of Δx that satisfy $\chi(\Delta x) = \delta x$.

2.5 Block Cipher Camellia

Fig. 1 shows the entire structure of Camellia. Fig. 2 shows its round functions, and Fig. 3. shows FL-function and FL^{-1}-function.

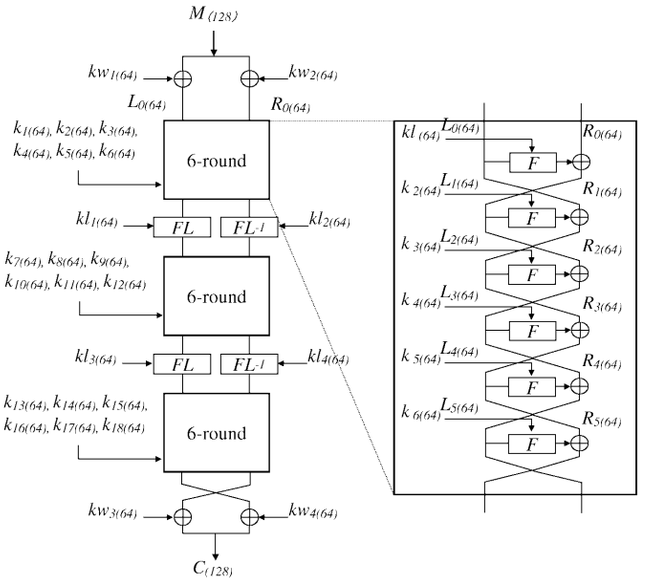

Fig. 1. Block cipher Camellia

3 Previous Security Evaluation of Camellia

3.1 Security Evaluation against Truncated Differential Cryptanalysis [10]

In [10], an algorithm to search for the effective truncated differentials of Feistel ciphers was proposed. This search algorithm consists of recursive procedures.

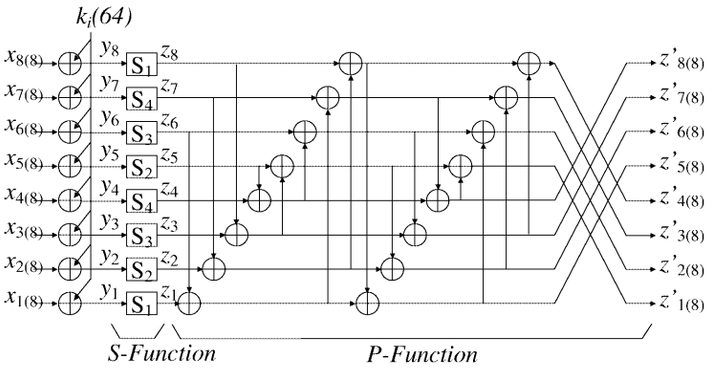

Fig. 2. F function of Camellia

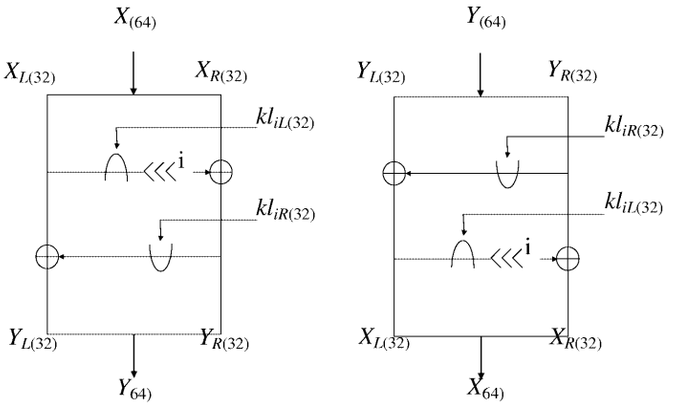

Fig. 3. FL and FL^{-1} functions of Camellia

Feistel ciphers are assumed to have S rounds and input and output block size is $2m$ bits.

Algorithm 1 *[11]*

Let $\Delta X^{(r)}, \Delta Y^{(r)} \in \mathrm{GF}(2)^m$ *be the input and output truncated difference of the* r*-th round functions* f_r*.* $(\Delta L, \Delta R)$ *is the truncated difference of the plaintext. Let* $\Pr((\Delta X^{(0)}, \Delta X^{(1)})|(\Delta L, \Delta R)))$ *be the* r*-round truncated differential probabilities.*

1. *Calculate all the truncated differential probabilities* $p_f(\delta x, \delta y)$ *of the round function* f *for all truncated differentials* $(\delta x, \delta y)$ *and save these probabilities in memory.*
2. *Select and fix* $(\Delta L, \Delta R)$*.* $\Pr((\Delta X^{(0)}, \Delta X^{(1)})|(\Delta L, \Delta R))$ *should be initialized as* 1 *if* $(\Delta X^{(0)}, \Delta X^{(1)}) = (\Delta L, \Delta R)$*, otherwise as* 0*.*

3. *Utilizing the values of* $p_f(\delta x, \delta y)$*, calculate* $\Pr((\Delta X^{(r+1)}, \Delta X^{(r+2)})|(\Delta L, \Delta R))$ *for all* $(\Delta X^{(r+1)}, \Delta X^{(r+2)})$ *from all values of* $\Pr((\Delta X^{(r)}, \Delta X^{(r+1)})|(\Delta L, \Delta R))$*, and save in memory. Repeat this from* $r = 1$ *to* S*. and save the most effective truncated differential probability in memory, where 'most effective' means that the ratio of the obtained probability to the average probability is the maximum.*
4. *Repeat 2-3 for every* $(\Delta R, \Delta L)$*.*
5. *return the most effective truncated differential probability.*

Using this procedure, we can search for all truncated differentials that lead to possible attacks on reduced-round version of Camellia. We cannot find any such truncated differentials for Camellia with more than 6-rounds by this algorithm. The best 6-round truncated differential that leads to possible attacks on reduced-round version of Camellia is shown in Fig. 4.

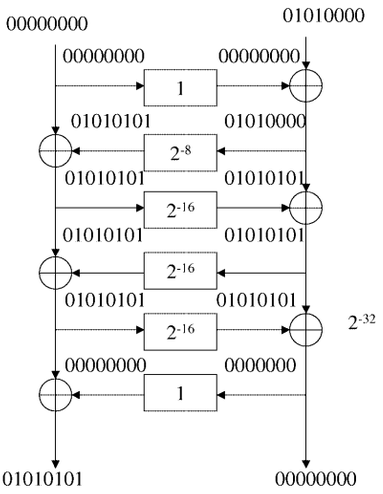

Fig. 4. 6-round truncated differential of Camellia

By this path, total probability $p \simeq 2^{-88}$, whereas the average probability, which can be obtained when entire round function is a random permutation, is 2^{-96}.

This evaluation is accurate if we take the ideal approximation model as is done in [10]. We note that this model is not always appropriate for Camellia, especially because the round function of Camellia is a 2-layer SPN, i.e. S-D (Substitution and Diffusion), not a 3-layer SPN, i.e. S-D-S. In [1] and [6], they upper-bounded the truncated differential probabilities considering this gap, and no effective truncated differentials for Camellia with more than 7-rounds (without input/output whitening, FL or FL^{-1}) are known.

4 Truncated Differential Cryptanalysis of Reduced-Round Version of Camellia without Input/Output Whitening, FL or FL^{-1}

This section indicates the truncated differentials that are effective in the cryptanalysis of reduced version of Camellia. These truncated differences cannot be found by the algorithm described in the previous section. We define notation in Fig. 5.

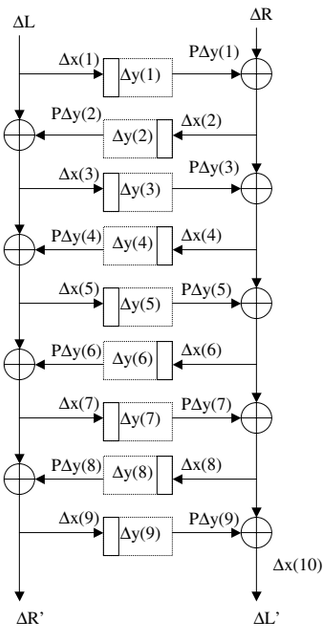

Fig. 5. Notation

First we analyze the round function of Camellia. P-function composing F-function is denoted as follows.

$$\mathrm{GF}(2^8)^8 \to \mathrm{GF}(2^8)^8$$
$$(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8) \mapsto (z'_1, z'_2, z'_3, z'_4, z'_5, z'_6, z'_7, z'_8).$$

This transformation can be expressed by linear transformations represented by matrix P.

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix} \mapsto \begin{pmatrix} z'_1 \\ z'_2 \\ z'_3 \\ z'_4 \\ z'_5 \\ z'_6 \\ z'_7 \\ z'_8 \end{pmatrix} = P \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix}$$

where

$$P = \begin{pmatrix} 1\,0\,1\,1\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,0\,1 \\ 0\,1\,1\,1\,1\,1\,1\,0 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 0\,1\,1\,0\,1\,0\,1\,1 \\ 0\,0\,1\,1\,1\,1\,0\,1 \\ 1\,0\,0\,1\,1\,1\,1\,0 \end{pmatrix}$$

This transformation induces the transformation of the difference as follows.

$$\begin{pmatrix} \Delta z_1 \\ \Delta z_2 \\ \Delta z_3 \\ \Delta z_4 \\ \Delta z_5 \\ \Delta z_6 \\ \Delta z_7 \\ \Delta z_8 \end{pmatrix} \mapsto \begin{pmatrix} \Delta z'_1 \\ \Delta z'_2 \\ \Delta z'_3 \\ \Delta z'_4 \\ \Delta z'_5 \\ \Delta z'_6 \\ \Delta z'_7 \\ \Delta z'_8 \end{pmatrix} = P \begin{pmatrix} \Delta z_1 \\ \Delta z_2 \\ \Delta z_3 \\ \Delta z_4 \\ \Delta z_5 \\ \Delta z_6 \\ \Delta z_7 \\ \Delta z_8 \end{pmatrix}$$

Next we consider the truncated differentials effective for truncated differential cryptanalysis.

When $\Delta z_1, \Delta z_2 \neq 0, \Delta z_3 = \Delta z_4 = \Delta z_5 = \Delta z_6 = \Delta z_7 = \Delta z_8 = 0$, then

$$\begin{pmatrix} \Delta z_1 \\ \Delta z_2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} \Delta z_1 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_2 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_2 \\ 0 \\ \Delta z_1 \oplus \Delta z_2 \end{pmatrix}$$

When $\Delta z_1 \neq \Delta z_2$, this can be expressed in terms of byte characteristics as

$$(11000000) \mapsto (11111101).$$

In this case, this transition probability (truncated differential probability) $p_1 \simeq 1$.

Utilizing the value of

$$P^{-1} = \begin{pmatrix} 0\,1\,1\,1\,0\,1\,1\,1 \\ 1\,0\,1\,1\,1\,0\,1\,1 \\ 1\,1\,0\,1\,1\,1\,0\,1 \\ 1\,1\,1\,0\,1\,1\,1\,0 \\ 1\,1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,0\,1\,1\,0\,1 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 1\,0\,0\,1\,0\,1\,1\,1 \end{pmatrix},$$

when $\Delta z_1, \Delta z_2 \neq 0, \Delta z_1 \neq \Delta z_2, \Delta z_3 = \Delta z_4 = \Delta z_5 = \Delta z_1 \oplus \Delta z_2, \Delta z_6 = \Delta z_1, \Delta z_7 = 0, \Delta z_8 = \Delta z_2$, we obtain

$$\begin{pmatrix} \Delta z_1 \\ \Delta z_2 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_1 \oplus \Delta z_2 \\ \Delta z_1 \\ 0 \\ \Delta z_2 \end{pmatrix} \mapsto \begin{pmatrix} \Delta z_2 \\ \Delta z_1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

which can be expressed in terms of byte characteristics as

$$(11111101) \mapsto (11000000).$$

This transition probability (truncated differential probability) $p_2 \simeq 2^{-40}$

Utilizing these two transition probabilities, we can obtain a 9-round truncated differential that contains two different paths as in Fig. 6.

In total, the first transition probability is approximately 2^{-112} (see the evaluation in Appendix).

Similarly, we consider the other path, which is as effective as the first one. In total, this transition probability is also 2^{-112} (see also the evaluation in Appendix).

Summing the two probabilities, therefore, the truncated differential probability of

$$\begin{aligned} &\Pr(\chi(\Delta L') = (11000000), \chi(\Delta R') = (00000000) | \\ &\quad \chi(\Delta L) = (00000000), \chi(\Delta R) = (11000000)) \simeq 2.0 \times 2^{-112}, \end{aligned}$$

which is approximately twice as large as the average value 2^{-112}.

Our search has not found any truncated differential more effective than this for 9-round Camellia.

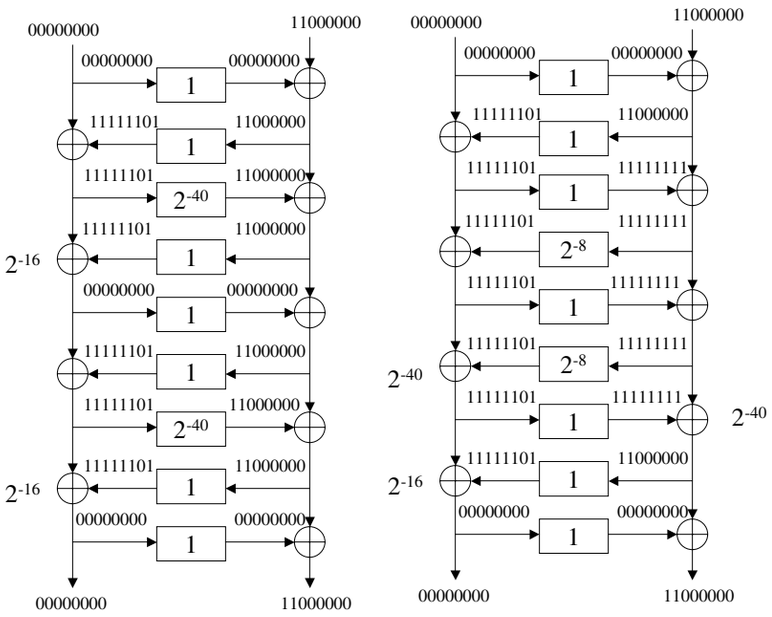

Fig. 6. 9-round byte characteristic of Camellia

5 Impossible Differential Cryptanalysis of Reduced-Round Version of Camellia without Input/Output Whitening, FL or FL^{-1}

5.1 Impossible Differential Cryptanalysis

Impossible differential means the differential that holds with probability 0, or the differential that does not exist. Using such an impossible differential, it is possible to narrow down the subkey candidates. It is known that there is at least one 5-round impossible differential in any Feistel structure with bijective round functions. Since Camellia uses the Feistel structure with FL and FL^{-1} inserted between every 6-rounds and the round function is bijective, Camellia has 5-round impossible differentials.

5.2 Impossible Differential Cryptanalysis of Reduced Camellia

In [1], they state that they have not found impossible differentials for more than 5 rounds. In this subsection, we indicate one impossible differential of a 7-round reduced-round version of Camellia without input/output whitening, FL and FL^{-1} as shown in Fig. 7.

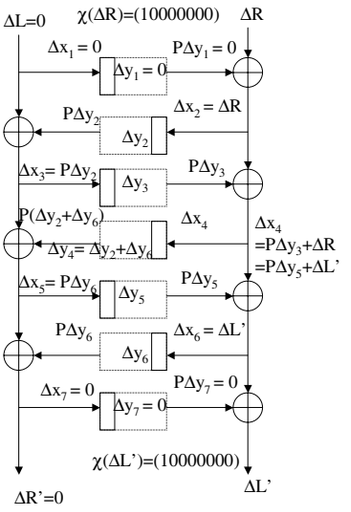

Fig. 7. 7-round impossible differential of Camellia

In this figure, we consider the byte characteristic

$$(0000000010000000) \mapsto (1000000000000000),$$

In this case, we can prove that this is an impossible differential as follows.

First we assume $\chi(\Delta L) = (00000000), \chi(\Delta R) = (10000000)$, $\chi(\Delta R') = (00000000), \chi(\Delta L') = (10000000)$.

This assumption implies that

$$\Delta x_1 = \Delta y_1 = P\Delta y_1 = 0, \Delta x_2 = \Delta R, \Delta x_7 = \Delta y_7 = P\Delta y_7 = 0, \Delta x_6 = \Delta L'.$$

From

$$P\Delta y_4 = P\Delta y_2 \oplus P\Delta y_6,$$

it follows that

$$\Delta y_4 = \Delta y_2 \oplus \Delta y_6,$$

which implies

$$\chi(\Delta x_4) = \chi(\Delta y_4) = \begin{cases} (10000000) \text{ if } \Delta y_2 \neq \Delta y_6 \\ (00000000) \text{ otherwise.} \end{cases}$$

From the definition of P,

$$\chi(\Delta y_3) = \chi(\Delta x_3) = (11101001),$$

where $\Delta y_3 \neq 0$ because $\Delta x_3 \neq 0$ follows from $\Delta y_2 \neq 0$

Similarly,

$$\chi(\Delta y_5) = \chi(\Delta x_5) = (11101001),$$

where $\Delta y_5 \neq 0$ because $\Delta x_5 \neq 0$ follows from $\Delta y_6 \neq 0$.

Since $\chi(\Delta R) = (10000000)$, it holds that

$$\chi(\Delta x_4 \oplus \Delta R) = \begin{cases} (10000000) \text{ if } \Delta x_4 \neq \Delta R \\ (00000000) \text{ otherwise.} \end{cases}$$

Similarly, since $\chi(\Delta L') = (10000000)$, it holds that

$$\chi(\Delta x_4 \oplus \Delta L') = \begin{cases} (10000000) \text{ if } \Delta x_4 \neq \Delta L' \\ (00000000) \text{ otherwise.} \end{cases}$$

From Fig. 7, it holds that

$$P\Delta y_3 = \Delta x_4 \oplus \Delta R, P\Delta y_5 = \Delta x_4 \oplus \Delta L',$$

however, there is no $(t, s) \in (\mathrm{GF}(2^8)^8)^2$ such that $\chi(t) = (11101001)$, $\chi(s) = (10000000)$, $t \neq 0$ and $Pt = s$.

Thus, the truncated differential represented by

$$(0000000010000000) \mapsto (1000000000000000)$$

is impossible.

6 Conclusion

This paper evaluated the security of the block cipher Camellia against truncated and impossible differential cryptanalysis. We introduced a nontrivial 9-round truncated differential that leads to a possible attack of reduced-round version of Camellia without input/output whitening, FL or FL^{-1} in a chosen plain text scenario. Prior studies showed only a 6-round truncated differential for a possible attack against 8-round Camellia. Moreover, we showed a nontrivial 7-round impossible differential, whereas only a 5-round impossible differentials were previously known.

Acknowledgment. We would like to thank Shiho Moriai and the anonymous reviewers for their helpful comments.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platform" `http://info.isl.ntt.co.jp/camellia/`
2. E. Biham, O. Dunkelman, V. Furman, T. Mor, "Preliminary report on the NESSIE submissions Anubis, Camellia, IDEA, Khazad, Misty1, Nimbus, Q," NESSIE public report.

3. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems." Journal of Cryptology, Vol.4, No.1, pp.3-72, 1991. (The extended abstract was presented at CRYPTO'90).
4. L.R. Knudsen and T.A. Berson, "Truncated Differentials of SAFER." In Fast Software Encryption - Third International Workshop, FSE'96, Volume 1039 of Lecture Notes in Computer Science, Berlin, Heidelberg, NewYork, Springer-Verlag, 1996.
5. M. Kanda et al. "A New 128-bit Block Cipher E2," IEICE Trans. fundamentals, Vol.E83-A, No.1, Jan., 2000.
6. M. Kanda and T. Matsumoto, "Security of Camellia against Truncated Differential Cryptanalysis," In Fast Software Encryption - 8th International Workshop, FSE'00.
7. T. Kawabata, Y. Ohgaki, T. Kaneko, "A study on Strength of Camellia against Higher Order Differential Attack," Technical Report of IEICE. ISEC 2001-9, pp.55-62.
8. X. Lai, J.L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptography-EUROCRYPT '91. Lecture Notes in Computer Science, Vol. 576. Springer-Verlag, Berlin, 1992, pp.86-100.
9. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, pp.250-250 (1997).
10. A. Moriai, M. Sugita, K. Aoki, M. Kanda, "Security of E2 against truncated Differential Cryptanalysis" Sixth Annual Workshop on Selected Areas in Cryptography (SAC'99), LNCS 1758 pp.106-117 , Springer Verlag, Berlin, 1999.
11. S. Moriai, M. Sugita and M. Kanda, "Security of E2 against truncated Differential Cryptanalysis" IEICE, Trans. fundamentals, Vol.E84-A NO.1, pp.319-325, January 2001.
12. M. Matsui, and T. Tokita, "Cryptanalysis of a Reduced Version of the Block Cipher E2" in 6-th international workshop, preproceedings FSE'99
13. K. Nyberg and L.R. Knudsen, "Provable security against a differential attack," in Advances in Cryptology - EUROCRYTO'93, LNCS 765, pp.55-64, Springer-Verlag, Berlin, 1994.
14. M. Sugita, K. Kobara, H. Imai, "Pseudorandomness and Maximum Average of Differential Probability of Block Ciphers with SPN-Structures like E2." Second AES Workshop, 1999.
15. M. Sugita, K. Kobara, H. Imai, "Relationships among Differential, Truncated Differential, Impossible Differential Cryptanalyses against Block-Oriented Block Ciphers like RIJNDAEL, E2" Third AES Workshop, 2000.
16. T. Tokita, M. Matsui, "On cryptanalysis of a byte-oriented cipher", The 1999 Symposium on Cryptography and Information Security, pp.93-98 (In Japanese), Kobe, Japan, January 1999.

Appendix: Evaluation of Truncated Differential Probability of Camellia

First we evaluate the transition probability of the first path in Fig. 6.

$$\begin{aligned}\Pr(\chi(P\Delta y(1)) = (00000000) | \chi(\Delta x(1)) = (00000000)) = 1\\ \Pr(\chi(\Delta x(2)) = (11000000) | \chi(P\Delta y(1)) = (00000000),\\ \chi(\Delta R) = (11000000)) = 1\end{aligned}$$

$$\begin{aligned}
&\Pr(\chi(P\Delta y(2)) = (11111101)|\chi(\Delta x(2)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(3)) = (11111101)|\chi(P\Delta y(2)) = (11111101)),\\
&\qquad \chi(\Delta L) = (00000000)) = 1\\
&\Pr(\chi(P\Delta y(3)) = (11000000)|\chi(\Delta x(3)) = (11111101)) \simeq 2^{-40}\\
&\Pr(\chi(\Delta x(4)) = (11000000)|\chi(\Delta x(2)) = \chi(P\Delta y(3)) = (11000000)) \simeq 1\\
&\Pr(\chi(P\Delta y(4)) = (11111101)|\chi(\Delta x(4)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(5)) = (00000000))|\chi(\Delta x(4)) = \chi(\Delta x(2)) = (11000000),\\
&\qquad \chi(\Delta x(1)) = (00000000))\\
&= \Pr(\Delta y(4) = \Delta y(2)|\chi(\Delta x(4)) = \chi(\Delta x(2)) = (11000000)) \simeq 2^{-16}\\
&\Pr(\chi(P\Delta y(5)) = (00000000)|\chi(\Delta x(5)) = (00000000)) = 1\\
&\Pr(\chi(\Delta x(6)) = (11000000)|\chi(P\Delta y(5)) = (00000000),\\
&\qquad \chi(\Delta x(4)) = (11000000)) = 1\\
&\Pr(\chi(P\Delta y(6)) = (11111101)|\chi(\Delta x(6)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(7)) = (11111101)|\chi(P\Delta y(6)) = (11111101),\\
&\qquad \chi(\Delta x(5)) = (00000000)) = 1\\
&\Pr(\chi(P\Delta y(7)) = (11000000)|\chi(\Delta x(7)) = (11111101)) \simeq 2^{-40}\\
&\Pr(\chi(\Delta x(8)) = (11000000)|\chi(P\Delta y(7)) = (11000000),\\
&\qquad \chi(\Delta x(6)) = (11000000)) \simeq 1\\
&\Pr(\chi(P\Delta y(8)) = (11111101)|\chi(\Delta x(8)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(9)) = (00000000)|\chi(\Delta x(8)) = \chi(\Delta x(6)) = (11000000),\\
&\qquad \chi(\Delta x(5) = (00000000))\\
&\qquad = \Pr(\chi(P\Delta y(8) \oplus \Delta x(7)) = (00000000)|\\
&\qquad \chi(\Delta x(8)) = \chi(\Delta x(6)) = (11000000))\\
&= \Pr(\Delta y(8) = \Delta y(6)|\chi(\Delta x(8)) = \chi(\Delta x(6)) = (11000000)) \simeq 2^{-16}\\
&\Pr(\chi(P\Delta y(9)) = (00000000)|\chi(\Delta x(9)) = (00000000)) = 1\\
&\Pr(\chi(\Delta x(10)) = (11000000)|\chi(P\Delta y(9)) = (00000000),\\
&\qquad \chi(\Delta x(8)) = (11000000)) = 1
\end{aligned}$$

In total, the transition probability is approximately 2^{-112}.

Similarly, we consider the other path in Fig. 6, which is as effective as the first one.

$$\begin{aligned}
&\Pr(\chi(P\Delta y(1)) = (00000000)|\chi(\Delta x(1)) = (00000000)) = 1\\
&\Pr(\chi(\Delta x(2)) = (11000000)|\chi(P\Delta y(1)) = (00000000),\\
&\qquad \chi(\Delta R) = (11000000)) = 1\\
&\Pr(\chi(P\Delta y(2)) = (11111101)|\chi(\Delta x(2)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(3)) = (11111101)|\chi(P\Delta y(2)) = (11111101)),\\
&\qquad \chi(\Delta R) = (00000000)) = 1\\
&\Pr(\chi(P\Delta y(3)) = (11111111)|\chi(\Delta x(3)) = (11111101)) \simeq 1
\end{aligned}$$

$$\begin{aligned}
&\Pr(\chi(\Delta x(4)) = (11111111) | \chi(\Delta x(2)) = (11000000),\\
&\qquad \chi(P\Delta y(3)) = (11111111)) \simeq 1\\
&\Pr(\chi(P\Delta y(4)) = (11111101) | \chi(\Delta x(4)) = (11111111)) \simeq 2^{-8}\\
&\Pr(\chi(\Delta x(5)) = (11111101)) | \chi(P\Delta y(4)) = \chi(\Delta x(3)) = (11111101)) \simeq 1\\
&\Pr(\chi(P\Delta y(5)) = (11111101) | \chi(\Delta x(5)) = (11111111)) \simeq 1\\
&\Pr(\chi(\Delta x(6)) = (11111111) | \chi(P\Delta y(5)) = (11111111),\\
&\qquad \chi(\Delta x(4)) = (11111111)) \simeq 1\\
&\Pr(\chi(P\Delta y(6)) = (11111101) | \chi(\Delta x(6)) = (11111111)) \simeq 2^{-8}\\
&\Pr(P^{-1}\Delta x(7) \in \{x \in \mathrm{GF}(2^8)^8 | \chi(x) = (11000000)\}|\\
&\chi(\Delta y(2)) = (11000000), \chi(\Delta y(4)) = \chi(\Delta y(6)) = (11111111),\\
&\qquad \chi(P\Delta y(4)) = \chi(P\Delta y(6)) = (11111101))\\
&= \Pr(\Delta y(4) \oplus \Delta y(6) \in \{x \in \mathrm{GF}(2^8)^8 | \chi(x) = (11000000)\}|\\
&\chi(\Delta y(2)) = (11000000), \chi(\Delta y(4)) = \chi(\Delta y(6)) = (11111111),\\
&\qquad \chi(P\Delta y(4)) = \chi(P\Delta y(6)) = (11111101)) \simeq 2^{-40}\\
&\Pr(\chi(P\Delta y(7)) = (11111111) | \chi(\Delta x(7)) = (11111101)) \simeq 1\\
&\Pr(\chi(\Delta x(8) = (11000000) | \chi(\Delta R) = (11000000),\\
&\qquad \chi(\Delta y(3)) = \chi(\Delta y(5)) = \chi(\Delta y(7)) = (11111101))\\
&= \Pr(\Delta y(3) \oplus \Delta y(5) \oplus \Delta y(7) \in P^{-1}\{x \in \mathrm{GF}(2^8)^8 |\\
&\qquad \chi(x) = (11000000)\}|\\
&\qquad \chi(\Delta y(3)) = \chi(\Delta y(5)) = \chi(\Delta y(7)) = (11111101)) \simeq 2^{-40}\\
&\Pr(\chi(P\Delta y(8)) = (11111101) | \chi(\Delta x(8)) = (11000000)) \simeq 1\\
&\Pr(\chi(\Delta x(9)) = (00000000) | \chi(\Delta y(8)) = (11000000),\\
&\qquad P^{-1}\Delta x(7) \in \{x \in \mathrm{GF}(2^8)^8 | \chi(x) = (11000000)\}) \simeq 2^{-16}\\
&\Pr(\chi(P\Delta y(9)) = (00000000) | \chi(\Delta x(9)) = (00000000)) = 1\\
&\Pr(\chi(\Delta x(10)) = (11000000) | \chi(P\Delta y(9)) = (00000000),\\
&\qquad \chi(\Delta x(8) = (11000000)) = 1
\end{aligned}$$

In total, this transition probability is also approximately 2^{-112}.