The Journal of Systems and Software 85 (2012) 2451–2458

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256

Ya Liu[a], Dawu Gu[a,*], Zhiqiang Liu[a], Wei Li[b,c,d]

[a] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
[b] School of Computer Science and Technology, Donghua University, Shanghai 201620, China
[c] Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai 200240, China
[d] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

ARTICLE INFO

Article history:
Received 13 August 2011
Received in revised form 11 April 2012
Accepted 9 May 2012
Available online 19 May 2012

Keywords:
Block cipher
Camellia
Impossible differential cryptanalysis

ABSTRACT

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

1. Introduction

The block cipher Camellia was jointly proposed by NTT and Mitsubishi Electric Corporations (Aoki et al., 2000). It was then submitted to several standardization and evaluation projects such as the Japanese CRYPTREC Evaluation, the NESSIE Project and ISO/IEC. Specifically, Camellia was selected to be a CRYPTREC e-government recommended block cipher (CRYPTREC, 2002) in 2002. Then, it was recommended in the NESSIE block cipher portfolio (NESSIE, 1999) in 2003. Finally, it was adopted as a new international standard by ISO/IEC in 2005 (ISO, 2005). Camellia is a 128-bit block cipher. It supports variable key sizes and the number of rounds depends on the key size, i.e., 18 rounds for a 128-bit key size and 24 rounds for 192/256-bit key sizes. For simplicity, they are usually denoted as Camellia-128, Camellia-192 and Camellia-256. Camellia uses the basic Feistel structure with the FL/FL^{-1} layer inserted every 6 rounds. Those transformations FL/FL^{-1} are related to the key value, which is expected to make the cryptanalysis of Camellia much harder.

As one of the most widely used block ciphers, Camellia has drawn a great amount of attention from many researchers. Up to now, a lot of research work has been done to evaluate the security of Camellia by means of various cryptanalytic methods such as linear cryptanalysis, differential cryptanalysis, truncated differential cryptanalysis, higher order differential cryptanalysis, collision attacks, square attacks, integral attacks and impossible differential cryptanalysis. Among them, most work (Sugita et al., 2001; Kawabata and Kaneko, 2001; Jie and Zhang, 2006; Wu et al., 2007; Lei et al., 2007; Mala et al., 2009; Lu et al., 2011) focused on the security of a simple version of Camellia (i.e., Camellia without the whitening layer or the FL/FL^{-1} layer), and only a few (Lei et al., 2005; Hatano et al., 2002; Chen et al., 2011; Li et al., 2011a) involved in the security of Camellia with the FL/FL^{-1} and whitening layers (called Camellia for short). For instance, Duo et al. presented a square attack on 10-round Camellia-256 which required 2^{48} chosen plaintexts and 2^{210} 10-round encryptions, Hatano *et al.* proposed a higher order differential attack on the last 11 rounds of Camellia-256 with 2^{93} chosen ciphertexts and $2^{255.6}$ 11-round encryptions, Chen et al. constructed some 6-round impossible differentials which were used to mount impossible differential attacks on 10-round Camellia-192 with about 2^{121} chosen plaintexts and $2^{175.3}$ 10-round encryptions and 11-round Camellia-256 with approximately 2^{121} chosen plaintexts and $2^{206.8}$ 11-round encryptions, Li *et al* gave some 7-round conditional impossible differentials (i.e., there is a 75% probability that each of them is impossible), which could be used to attack 10-round Camellia-128 with $2^{112.4}$ chosen plaintexts and 2^{120} 10-round encryptions, 11-round Camellia-192 with $2^{113.7}$ chosen plaintexts and 2^{184} 11-round encryptions as well as 12-round Camellia-256 with $2^{114.8}$ chosen plaintexts and 2^{240} 12-round encryptions.

[*] Corresponding author.
E-mail addresses: liuya0611@sjtu.edu.cn, liuyaloccs@gmail.com (Y. Liu), dwgu@sjtu.edu.cn (D. Gu), ilu_zq@sjtu.edu.cn (Z. Liu), liwei.cs.cn@gmail.com (W. Li).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.05.051

Impossible differential cryptanalysis, which is a variant of differential cryptanalysis, was independently proposed by Knudsen (1998) and Biham et al. (1999). Its main idea is to use impossible differentials that hold with probability zero to discard the wrong keys until only one key is left. Impossible differential cryptanalysis has received much attention and has been used to attack a variety of well-known block ciphers such as AES, ARIA, CLEFIA and MISTY1 (Lu et al., 2008; Mala et al., 2010; Tsunoo et al., 2008; Dunkelman and Keller, 2008).

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

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

2. Preliminaries

In this section, we will give some notations used throughout the paper, a brief description of Camellia, as well as previous results on impossible differential cryptanalysis of reduced-round Camellia.

2.1. Notations

- P, C: the 128-bit plaintext and the 128-bit ciphertext;
- ΔP, ΔC: the differences of a plaintext pair and a ciphertext pair;
- L_{r-1}, R_{r-1}: the left and right halves of the rth round input;
- ΔL_{r-1}, ΔR_{r-1}: the left and right halves of the rth round input difference;
- S_r: the output of the S-boxes in the rth round;
- ΔS_r: the output difference of the S-boxes in the rth round;
- $X|Y$: the concatenation of X and Y;
- $kw_1|kw_2$, $kw_3|kw_4$: the pre-whitening and post-whitening keys;
- $kl_i (1 \le i \le 6)$: the 64-bit key used in the functions FL/FL^{-1};
- k_r: the rth round subkey;
- $X \lll j$: left rotation of X by j bits;
- $X_{L(n/2)}$, $X_{R(n/2)}$: the left and right halves of a n-bit word X;
- $X_{l,j}$, $X_{l,\{i,j\}}$, $X_{l,\{i\sim j\}}$: the jth byte, the ith and jth bytes and the ith to the jth bytes of X_l;
- $\oplus, \cap, \cup$: bitwise exclusive-OR (XOR), AND, and OR operations.

2.2. Overview of Camellia

Camellia is a 128-bit block cipher which adopts a Feistel structure with the key-dependent functions FL/FL^{-1} inserted every 6 rounds. It supports variable key sizes and the number of rounds depends on the key size, i.e., 18 rounds for a 128-bit key size and 24 rounds for 192/256-bit key sizes. Before the first round and after the last round, the pre-whitening and post-whitening layers are included. The encryption algorithm of Camellia-192/256 can be expressed as below and Fig. 1 gives the basic encryption structure of Camellia.

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

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

For $r = 6$, 12 and 18,

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

Here the round function F uses a SPN structure including the key-addition layer, the nonlinear transformation S and the linear permutation P. The nonlinear transformation S adopts four different 8×8 S-boxes s_1, s_2, s_3 and s_4 twice. Please refer to Aoki et al. (2000) for detailed information about these S-boxes. The linear transformation $P : (\{0, 1\}^8)^8 \to (\{0, 1\}^8)^8$ and its inverse P^{-1} are defined as follows:

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

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, respectively.

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

Key schedule of Camellia-192/256. The key schedule of Camellia-192/256 applies a 6-round Feistel structure to derive 128-bit intermediate variables K_A and K_B from 128-bit variables K_L and K_R, and then all the subkeys can be generated by using K_L, K_R, K_A and K_B. For Camellia-192, the left 128 bits of the key K are used as K_L, and the concatenation of the right 64 bits of the key K and the complement of the right 64 bits of the key K are used as K_R. For Camellia-256, the main key K is separated into two 128-bit variables K_L and K_R, i.e., $K = K_L|K_R$.

2.3. Some results on impossible differential cryptanalysis of reduced-round Camellia

In 2011, Chen et al. gave impossible differential cryptanalysis of Camellia by constructing several 6-round impossible differentials with the functions FL/FL^{-1} inserted in the middle. Specifically, the input and output differences of one of those 6-round impossible differentials are (0, 0, 0, 0, 0, 0, 0, 0, a, 0, 0, 0, 0, 0, 0) and (0, a, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), which meet a contradiction in the key-dependent functions FL/FL^{-1}. Based on this 6-round impossible differential, they put three additional rounds at the top and one additional round at the bottom to attack 10-round Camellia-192 with 2^{121} chosen plaintexts and $2^{175.3}$ 10-round encryptions. Moreover, they mounted an impossible differential attack on 11-round Camellia-256 with 2^{121} chosen plaintexts and $2^{206.8}$ 11-round encryptions.

In November 2011, another paper on the security of reduced-round Camellia against impossible differential attack was posted in