Improved Collision Attack on Reduced Round Camellia

Guan Jie and Zhang Zhongya

The Information Engineer University Electronic Technology Institute
Zhengzhou 450004, China

Abstract. Camellia is a 128-bit block cipher which has been selected as an international standard by ISO/IEC and a European encryption standard by the NESSIE project. Wu Wenling presented the collision attack on reduced-round Camellia in 2004, the 128-bit key of 6 rounds Camellia can be recovered with 2^{10} chosen plaintexts and 2^{15} encryptions. The improved collision attack on 6 rounds Camellia which based on four 4-round distinguishers is presented in this paper. This attack requires less than $2^{10.6}$ chosen plaintexts and $2^{11.5}$ encryptions.

Keywords: Block cipher, Camellia, Collision attack.

1 Introduction

Camellia[1] is a 128-bit block cipher which was announced by NTT and Mitsubishi in 2000, it has been selected as an international standard by ISO/IEC , a European encryption standard by the NESSIE(New European Schemes for Signatures,Integrity,and Encryption) project and a secure E-Government standard of Japan. The security of Camellia against higher-order differential cryptanalysis, truncated differential attack, impossible differential cryptanalysis, Square attack, collision attack et.al. are discussed in [2,3,4,5,6,7,8,9]. The collision attack on reduced-round of Camellia by using collision-searching techniques is presented in [2]. The collision attack on 6-round of 128-bit key Camellia is more efficient than know attacks which requires less than 2^{10} chosen plaintexts and 2^{15} encryptions.

In this paper, we improve the collision attack on 6 rounds Camellia by using the improved collision-searching techniques based on four 4-round distinguishers. The improved collision attack on 6 rounds Camellia requires less than $2^{10.6}$ chosen plaintexts and $2^{11.5}$ encryptions. The time complexity is less than that of collision attack though the data amount is a little more than that of collision attack.

2 Description of the Camellia

Camellia has a 128 bit block size and supports 128, 192 and 256 bit keys. The design of Camellia is based on the Feistel structure. The FL/FL^{-1} function layer is inserted at every 6 rounds. Before the first round and after the last round, there

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 182–190, 2006.

are pre- and post-whitening layers which use bitwise exclusive-or operations with 128 bit subkeys, respectively.

Let L_{r-1} and R_{r-1} be the left and the right halves of the r^{th} round inputs, respectively, and k_r be the r^{th} subkey. Then the Feistel structure of Camellia can be written as

$$\begin{aligned} L_r &= R_{r-1} \oplus F(L_{r-1} \oplus k_r)\,, \\ R_r &= L_{r-1}\,. \end{aligned}$$

here $F = P \circ S$ is the round function defined below:

$$\begin{aligned} F : F_2^{64} \times F_2^{64} &\to F_2^{64}\,, \\ (X_{64}, k_{64}) &\to Y_{64} = P(S(X_{64} \oplus k_{64}))\,. \end{aligned}$$

where S and P are defined as follows:

The substitution $S : F_2^{64} \to F_2^{64}$ is defined by

$$(x_1, \ldots, x_8) \xrightarrow{s} (s_1(x_1), s_2(x_2), s_3(x_3), s_4(x_4), s_2(x_5), s_3(x_6), s_4(x_7), s_1(x_8))\,,$$

where s_1, s_2, s_3 and s_4 are four types of S-boxes over $GF(2^8)$, they are permutation.

The permutation function $P : F_2^{64} \to F_2^{64}$ maps $(z_1, \ldots, z_8)$ to $(z'_1, \ldots, z'_8)$ defined by

$$\begin{pmatrix} z'_8 \\ z'_7 \\ z'_6 \\ z'_5 \\ z'_4 \\ z'_3 \\ z'_2 \\ z'_1 \end{pmatrix} = \begin{pmatrix} 0\,1\,1\,1\,1\,0\,0\,1 \\ 1\,0\,1\,1\,1\,1\,0\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 0\,1\,1\,1\,1\,1\,1\,0 \\ 1\,0\,1\,1\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,0\,1 \end{pmatrix} \begin{pmatrix} z_8 \\ z_7 \\ z_6 \\ z_5 \\ z_4 \\ z_3 \\ z_2 \\ z_1 \end{pmatrix}.$$

The key schedule of Camellia is not described here, details are shown in [1].

3 Improved Collision Attack on 6 Rounds Camellia

The security of reduced Camellia against the collision attack by using collision-searching techniques based on one 4-round distinguisher is presented in [2]. We improve the collision-searching techniques on the foundation of [2], and construct four 4-round distinguishers. The improved collision on the 6 rounds Camellia requires less than $2^{10.6}$ chosen plaintexts and $2^{11.5}$ encryptions.

3.1 4-Round Distinguishers

Firstly, let us review the concept of the active (passive) byte[8].

Let Γ be a collection of state bytes $X = (\chi_1, \chi_2, \ldots, \chi_n)$ where χ_i is the i-th byte of X. If the i-th byte of elements in Γ are different one another, the i-th