Theoretical Computer Science 527 (2014) 102–122

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

The higher-order meet-in-the-middle attack and its application to the Camellia block cipher ☆

Jiqiang Lu [a,1,*], Yongzhuang Wei [b,c], Jongsung Kim [d], Enes Pasalic [e]

[a] Institute for Infocomm Research, Agency for Science, Technology and Research, 1 Fusionopolis Way, Singapore 138632, Singapore
[b] Guilin University of Electronic Technology, Guilin City, Guangxi Province 541004, China
[c] State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[d] Department of e-Business, Kyungnam University, 449 Wolyoung-dong, Masan, Kyungnam, Republic of Korea
[e] University of Primorska FAMNIT, Koper, Slovenia

ARTICLE INFO

Article history:
Received 13 December 2012
Received in revised form 18 November 2013
Accepted 28 January 2014
Communicated by X. Deng

Keywords:
Cryptology
Block cipher
Camellia
Meet-in-the-middle attack
Integral cryptanalysis

ABSTRACT

The Camellia block cipher has a 128-bit block length, a user key of 128, 192 or 256 bits long, and a total of 18 rounds for a 128-bit key and 24 rounds for a 192 or 256-bit key. It is a Japanese CRYPTREC-recommended e-government cipher, a European NESSIE selected cipher and an ISO international standard. The meet-in-the-middle attack is a technique for analysing the security of a block cipher. In this paper, we propose an extension of the meet-in-the-middle attack, which we call the higher-order meet-in-the-middle (HO-MitM) attack; the core idea of the HO-MitM attack is to use multiple plaintexts to cancel some key-dependent component(s) or parameter(s) when constructing a basic unit of "value-in-the-middle". Then we introduce a novel approach, which combines integral cryptanalysis with the meet-in-the-middle attack, to construct HO-MitM attacks on 10-round Camellia with the FL/FL^{-1} functions under 128 key bits, 11-round Camellia with the FL/FL^{-1} functions under 192 key bits and 12-round Camellia with the FL/FL^{-1} functions under 256 key bits. Finally, we apply an existing approach to construct HO-MitM attacks on 14-round Camellia without the FL/FL^{-1} functions under 192 key bits and 16-round Camellia without the FL/FL^{-1} functions under 256 key bits. The HO-MitM attack can potentially be used to cryptanalyse other block ciphers.

☆ This paper was presented in part in an invited talk given by J. Lu at the First Asian Workshop on Symmetric Key Cryptography (ASK 2011, Singapore, 29–31 August 2011), and an extended abstract of this paper was published in Proceedings of the 13th International Conference on Cryptology in India (INDOCRYPT 2012, Kolkata, India, 9–12 December 2012) [28]. As the full version of the work, this paper gives the HO-MitM attacks on 11-round Camellia-192 with FL/FL^{-1} functions and 12-round Camellia-256 with FL/FL^{-1} functions in detail and gives the proof of Propositions 1 and 2. The work was supported by the French ANR project SAPHIR II (No. ANR-08-VERS-014), the Natural Science Foundation of China (No. 61100185, No. 61201250), China Postdoctoral Science Foundation funded project, the National Basic Research 973 Program of China (No. 2013CB338002), Guangxi Experiment Center of Information Science Foundation funded project, the Foundation of Guangxi Key Lab of Wireless Wideband Communication and Signal Processing (No. 11101), and the Basic Science Research Program (3rd year: 2013/5–2014/4) through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2011-0014876).

[*] Corresponding author.

E-mail addresses: lvjiqiang@hotmail.com, jlu@i2r.a-star.edu.sg (J. Lu), walker_wei@msn.com (Y. Wei), jongsung.k@gmail.com (J. Kim), enespasalic@yahoo.se (E. Pasalic).

[1] The author was with École Normale Supérieure (France) when this work was completed.

http://dx.doi.org/10.1016/j.tcs.2014.01.031
0304-3975/© 2014 Elsevier B.V. All rights reserved.

1. Introduction

The Camellia [1] block cipher was published in 2000; it has a 128-bit block length, a user key of 128, 192 or 256 bits long, and a total of 16 rounds when used with a 128-bit key and 24 rounds when used with a 192/256-bit key. Camellia has a Feistel structure with key-dependent logical functions $\mathrm{FL}/\mathrm{FL}^{-1}$ inserted after every six rounds, plus four additional whitening operations at both ends. Camellia became a CRYPTREC e-government recommended cipher [9] in 2002, a NESSIE selected block cipher [33] in 2003, and was adopted as an ISO international standard [20] in 2005. For simplicity, we denote by Camellia-128/192/256 the three versions of Camellia that use 128, 192 and 256 key bits, respectively.

The security of Camellia has been analysed against a variety of cryptanalytic techniques, including differential cryptanalysis [5], higher-order differential cryptanalysis [21,24], truncated differential cryptanalysis [21], impossible differential cryptanalysis [3,22], linear cryptanalysis [32], integral (square [10]) cryptanalysis [19,23], boomerang attack [36], rectangle attack [4], collision attack [35], and meet-in-the-middle attack [13]; and many cryptanalytic results on Camellia have been obtained. In summary, in terms of the numbers of attacked rounds, the best currently known cryptanalytic results on Camellia with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions are the impossible differential attacks on 11-round Camellia-128, 12-round Camellia-192 and 14-round Camellia-256 [2,25], presented recently at FSE 2012 and ISPEC 2012; and the best currently known cryptanalytic results on Camellia without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions are the impossible differential attacks on 12-round Camellia-128 [30], 14-round Camellia-192 [27] and 16-round Camellia-256 [27,31].[2] Besides, Biryukov and Nikolic [6] analysed a reduced Camellia-128 with a modified key schedule.

The meet-in-the-middle (MitM) attack [13] is a technique for analysing the security of a block cipher. In this paper, we propose an extension of the MitM attack, which we call the higher-order meet-in-the-middle (HO-MitM) attack. The core idea of the HO-MitM attack is to use multiple plaintexts to cancel some key-dependent component(s) or parameter(s) when constructing a basic unit of so-called value-in-the-middle. Then we introduce a novel approach, that combines integral cryptanalysis [19,23] with the MitM attack, to construct a few HO-MitM properties for 5-round and 6-round Camellia with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions, and finally apply these properties to conduct HO-MitM attacks on 10-round Camellia-128 with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions, 11-round Camellia-192 with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions and 12-round Camellia-256 with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions. At last, we use an existing approach to construct a few HO-MitM properties for 7-round and 8-round Camellia without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions, and describe HO-MitM attacks on 14-round Camellia-192 without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions and 16-round Camellia-256 without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions. Table 1 summarises previous, our and the newly emerging main cryptanalytic results on Camellia, where CP, CC and KP refer respectively to the numbers of chosen plaintexts, chosen ciphertexts and known plaintexts, Enc. refers to the required number of encryption operations of the relevant reduced version of Camellia, "yes" means "with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions", and "no" means "without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions".

The remainder of the paper is organised as follows. In Section 2, we describe the notation and the Camellia block cipher. We define the HO-MitM attack in Section 3 and present our HO-MitM attacks on Camellia in Sections 4 and 5. Section 6 concludes this paper.

2. Preliminaries

In this section we give the notation used throughout this paper, and briefly describe the Camellia block cipher.

2.1. Notation

The bits of a value are numbered from left to right, starting with 1. We use the following notation throughout this paper.

$\oplus$	bitwise logical exclusive OR (XOR) of two bit strings of the same length
$\cap$	bitwise logical AND of two bit strings of the same length
$\cup$	bitwise logical OR of two bit strings of the same length
$\lll$	left rotation of a bit string
$\parallel$	bit string concatenation
$\circ$	functional composition. When composing functions X and Y, $X \circ Y$ denotes the function obtained by first applying X and then applying Y
$\lvert X\rvert$	the number of bits in a bit string X
$X[i_1, \ldots, i_j]$	the j-bit string of bits $(i_1, \ldots, i_j)$ of a bit string X

[2] When our work was completed, the best previously published cryptanalytic results on Camellia with $\mathrm{FL}/\mathrm{FL}^{-1}$ functions were square attack on 9-round Camellia-128 [15], impossible differential attack on 10-round Camellia-192 [8], and higher-order differential and impossible differential attacks on 11-round Camellia-256 [8,17]; and the best previously published cryptanalytic results on Camellia without $\mathrm{FL}/\mathrm{FL}^{-1}$ functions were impossible differential attacks on 12-round Camellia-128 [30], 12-round Camellia-192 [26] and 15-round Camellia-256 [8]. We incorporate the newly emerging main results in this revised version.