Published in IET Information Security
Received on 14th September 2009
Revised on 2nd June 2010
doi: 10.1049/iet-ifs.2010.0094

ISSN 1751-8709

Impossible differential cryptanalysis of reduced–round Camellia–256

H. Mala M. Dakhilalian M. Shakiba

Cryptography and System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
E-mail: hamid_mala@ec.iut.ac.ir

Abstract: Camellia, a 128-bit block cipher that has been accepted by ISO/IEC as an international standard, is increasingly being used in many cryptographic applications. In this study, the authors present a new impossible differential attack on a reduced version of Camellia-256 without FL/FL^{-1} functions and whitening. First, the authors introduce a new extension of the hash table technique and then exploit it to attack 16 rounds of Camellia-256. When, in an impossible differential attack, the size of the target subkey space is large and the filtration, in the initial steps of the attack, is performed slowly, the extended hash table technique will be very useful. The proposed attack on Camellia-256 requires $2^{124.1}$ known plaintexts and has a running time equivalent to about $2^{249.3}$ encryptions. In terms of the number of attacked rounds, our result is the best published attack on Camellia-256.

1 Introduction

Camellia [1, 2] is a 128-bit block cipher that supports three standard key lengths. For the sake of simplicity, Camellia with n-bit keys is denoted by Camellia-n, $n = 128, 192, 256$. Camellia was jointly proposed in 2000 by NTT and Mitsubishi and then was selected as one of the CRYPTREC e-government recommended ciphers in 2002 and as a member of the NESSIE block cipher portfolio in 2003. Camellia also was selected as an international standard by ISO/IEC in 2005 [3]. As one of the most widely used block ciphers, Camellia has received a significant amount of cryptanalytic attention. The most efficient cryptanalytic results for Camellia include linear and differential attacks [4], truncated differential attack [5–7], higher-order differential attack [8], collision attack [9, 10], square attack [9, 11], a square-like attack [12] and impossible differential attack [7, 13–15].

Impossible differential cryptanalysis [16], an extension of the differential attack, uses differentials that hold with probability zero (impossible differentials) to eliminate the wrong keys and leave the right key. The initial analysis of the security of Camellia against impossible differential cryptanalysis was given in [7]. The authors presented some seven-round impossible differentials for Camellia. In [15] Wu *et al.* introduced a non-trivial eight-round impossible differential that lead to an impossible differential attack on Camellia-192 and Camellia-256. Introducing the early abort technique, Lu *et al.* improved the impossible differential attack on Camellia in [17]. Later in [14] Wu *et al.* found a flaw in [17], and taking the key-scheduling algorithm into account, they presented impossible differential attacks on 12-round Camellia-128 and 16-round Camellia-256. They claimed that their attacks have data complexities of 2^{65} and 2^{89} chosen plaintexts and time complexities of about $2^{111.5}$ and $2^{222.1}$ encryptions, respectively. Recently in [18], Mala *et al.* found a flaw in [14]'s attack on Camellia-128 and by a different filtration process (using a hash table) they proposed the first successful attack on 12 rounds of Camellia-128.

In this paper, first, we point out some flaws in [14]'s attack on Camellia-256 and show that the time complexity of their attack is greater than exhaustive key search. We observed that modifying the filtration step based on the approach in [18] fails to work for Camellia-256. Hence, we introduce an extended hash table technique that can be exploited in impossible differential attacks when the size of the target subkey space is large and the filtration, in the initial steps of the attack, is performed slowly. As an application of this technique, we apply it to present the first successful impossible differential attack on 16-round Camellia-256. We summarise our results along with previously known results on Camellia-256 in Table 1. The results of [14] that are wrong are marked with '$*$', and the correct values that we computed for [14]'s attack are marked by '†'. In this table, time complexity is measured in encryption units and data complexity is the number of required plaintexts.

The rest of this paper is organised as follows: Section 2 provides a brief description of Camellia. We analyse the impossible differential attack of [14] in Section 3. An extended hash table technique and its application to 16 rounds of Camellia-256 is presented in Section 4. 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}	the left 64-bit half of the rth round input
R^{r-1}	the right 64-bit half of the rth round input