New Results on Impossible Differential Cryptanalysis of Reduced–Round Camellia–128

Hamid Mala[1], Mohsen Shakiba[1], Mohammad Dakhilalian[1], and Ghadamali Bagherikaram[2]

[1] Cryptography & System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
{hamid_mala@ec, m.shakiba@ec, mdalian@cc}.iut.ac.ir
[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada
gbagheri@cst.uwaterloo.ca

Abstract. Camellia, a 128–bit block cipher which has been accepted by ISO/IEC as an international standard, is increasingly being used in many cryptographic applications. In this paper, using the redundancy in the key schedule and accelerating the filtration of wrong pairs, we present a new impossible differential attack to reduced–round Camellia. By this attack 12–round Camellia–128 without FL/FL^{-1} functions and whitening is breakable with a total complexity of about $2^{116.6}$ encryptions and $2^{116.3}$ chosen plaintexts. In terms of the numbers of the attacked rounds, our attack is better than any previously known attack on Camellia–128.

1 Introduction

Camellia [1] is a 128–bit block cipher that supports several 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 submitted to several standardization and evaluation projects. It was selected as a winner of CRYPTREC e-government recommended ciphers in 2002 [5], NESSIE block cipher portfolio in 2003 [17] as well as the standardization activities at IETF [18]. Finally Camellia was selected as an international standard by ISO/IEC in 2005 [9]. As one of the most widely used block ciphers, Camellia has received a significant amount of cryptanalytic attention. The most efficient cryptanalytic results on Camellia include linear and differential attacks [19], truncated differential attack [5,10,13,20], higher order differential attack [7,11], collision attack [14,21], square attack [8,14,24], a square like attack [6] and impossible differential attack [15,20,22,23].

Impossible differential cryptanalysis, an extension of the differential attack [4], is one of the most powerful methods used for block cipher cryptanalysis. This method was first introduced by Biham [3] and Knudsen [12] independently. Impossible differential attacks use differentials that hold with probability zero (impossible differentials) to eliminate the wrong keys and leave the right key.

M.J. Jacobson Jr., V. Rijmen, and R. Safavi-Naini (Eds.): SAC 2009, LNCS 5867, pp. 281–294, 2009.