Improved Impossible Differential Cryptanalysis of 7-Round AES-128

Hamid Mala[1], Mohammad Dakhilalian[1],
Vincent Rijmen[2,3,⋆], and Mahmoud Modarres-Hashemi[1]

[1] Cryptography & System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, 8415683111 Isfahan, Iran
{hamid_mala@ec,mdalian@cc,modarres@cc}.iut.ac.ir
[2] COSIC, Dept. of EE, KULeuven and IBBT, Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
[3] IAIK, Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
Vincent.Rijmen@iaik.tugraz.at

Abstract. Using a new 4-round impossible differential in AES that allows us to exploit the redundancy in the key schedule of AES-128 in a way more effective than previous work, we present a new impossible differential attack on 7 rounds of this block cipher. By this attack, 7-round AES-128 is breakable with a data complexity of about 2^{106} chosen plaintexts and a time complexity equivalent to about 2^{110} encryptions. This result is better than any previously known attack on AES-128 in the single-key scenario.

Keywords: AES, block cipher, cryptanalysis, impossible differential.

1 Introduction

The Advanced Encryption Standard (AES)[7] is a 128-bit block cipher with variable key lengths of 128, 192, and 256 bits, which are denoted as AES-128, AES-192 and AES-256, respectively. Since its selection as the standard by NIST in 2001, AES has drawn a great amount of attention from worldwide cryptology researchers. In this paper we reevaluate the security of AES-128 against impossible differential attacks.

Impossible differential cryptanalysis, an extension of the differential attack [4], was first introduced by Knudsen [11] and Biham [2] to analyze DEAL and Skipjack, respectively. Impossible differential attacks use differentials that hold

⋆ This author's work was supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

G. Gong and K.C. Gupta (Eds.): INDOCRYPT 2010, LNCS 6498, pp. 282–291, 2010.