Mala H, Dakhilalian M, Shakiba M. Impossible differential attacks on 13-round CLEFIA-128. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 26(4): 744–750 July 2011. DOI 10.1007/s11390-011-1173-0

Impossible Differential Attacks on 13-Round CLEFIA-128

Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba

Cryptography and System Security Research Laboratory, Department of Electrical and Computer Engineering Isfahan University of Technology, Isfahan, Iran

E-mail: {hamid_mala@ec, mdalian@cc, m.shakiba@ec}.iut.ac.ir

Received November 9, 2009; revised February 26, 2011.

Abstract CLEFIA, a new 128-bit block cipher proposed by Sony Corporation, is increasingly attracting cryptanalysts' attention. In this paper, we present two new impossible differential attacks on 13 rounds of CLEFIA-128. The proposed attacks utilize a variety of previously known techniques, in particular the hash table technique and redundancy in the key schedule of this block cipher. The first attack does not consider the whitening layers of CLEFIA, requires $2^{109.5}$ chosen plaintexts, and has a running time equivalent to about $2^{112.9}$ encryptions. The second attack preserves the whitening layers, requires $2^{117.8}$ chosen plaintexts, and has a total time complexity equivalent to about $2^{121.2}$ encryptions.

Keywords block cipher, cryptanalysis, impossible differential, CLEFIA

1 Introduction

Diffusion Switching Mechanism (DSM) is a method of designing a Feistel block cipher that can guarantee a large minimum number of active S-boxes[1]. The first block cipher designed based on DSM, CLEFIA[2-3], is a 128-bit block cipher with variable key lengths of n bits, which is denoted as CLEFIA-n, n = 128, 192, 256. The number of rounds for these three variants is 18, 22 and 26, respectively. The designers of CLEFIA claimed that it is designed to achieve sufficient security against all known cryptanalysis techniques. Moreover, [4] proves that 5 rounds of its 4-branch generalized Feistel structure have provable security against differential cryptanalysis. As a new 128-bit block cipher, CLEFIA has received a significant amount of cryptanalytic attention. Among the cryptanalysis methods exploited to analyze this block cipher, the best results are attributed to impossible differential cryptanalysis.

Impossible differential cryptanalysis, an extension of the differential cryptanalysis[5], was first proposed by Biham to analyze the Skipjack block cipher[6]. This method uses differentials that hold with probability zero (impossible differentials) to eliminate the wrong keys and leave the right key. In [2, 7], the designers of CLEFIA found several 9-round impossible differentials for this cipher and mounted a 10-round attack with a data complexity of $2^{101.7}$ and a time complexity of about 2^{102} encryptions. In FSE 2008, [8] introduced new 9-round impossible differentials for CLEFIA, and presented a 12-round attack on CLEFIA-128. This attack requires $2^{118.9}$ chosen plaintexts and performs 2^{119} encryptions. Also in [9-11], impossible differential attacks have been applied to 12 rounds of CLEFIA-128. Recently, using the same impossible differential as that of [8], [12] claimed an attack on 14 rounds of CLEFIA-128 without whitening layers. But, CLEFIA design team pointed out a flaw in their attack and showed that its time complexity is greater than 2^{202} [13]. In fact their attack requires 2^{m+44} plaintexts, and in the attack procedure, after the data filtering, for each of the 2^{m+29} plaintext pairs, about $2^{21} \times 2^{10} \times 2^{-16} = 2^{15}$ values out of the 2^{128} possible values of the target subkeys are removed. To ensure that the number of remaining wrong subkeys is less than 1, we must have $(2^{128}-1) \times (1-\frac{2^{15}}{2^{128}})^{2^{m+29}} < 1$, thus m must be greater than 90.4. As a result, data complexity of the attack becomes greater than $2^{m+44} = 2^{134.4}$, so the attack scenario of [12] is not successful. However, their work is the first attack that considers the weakness in the key schedule of CLEFIA.

In this paper, we reevaluate the security of CLEFIA-128 against impossible differential cryptanalysis. Exploiting a variety of techniques including plaintext structures, key schedule considerations, early abort and hash table techniques, we present the first successful impossible differential attacks on 13-round CLEFIA-128. We summarize our results along with previously known results on CLEFIA-128 in Table 1. In this table, time complexity is measured in encryption units, and data complexity is the number of chosen plaintexts.

Short Paper

©2011 Springer Science + Business Media, LLC & Science Press, China