Information Sciences 263 (2014) 211–220

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A unified method for finding impossible differentials of block cipher structures ☆

Yiyuan Luo [a,b], Xuejia Lai [b,*,1], Zhongming Wu [b], Guang Gong [c]

[a] School of Electronics and Information, Shanghai Dian Ji University, China
[b] Department of Computer Science and Engineering, Shanghai Jiao Tong University, China
[c] Department of Electrical and Computer Engineering, University of Waterloo, Canada

ARTICLE INFO

Article history:
Received 31 August 2011
Received in revised form 15 August 2013
Accepted 24 August 2013
Available online 2 September 2013

Keywords:
Cryptography
Block ciphers
Impossible differential cryptanalysis
Differential characteristics

ABSTRACT

In this paper, we propose a systematic method for finding impossible differentials for block cipher structures, which we call the unified impossible differential finding method or UID-method. It is more effective than the $\mathcal{U}$-method introduced by Kim et al. We apply the UID-method to some well-known block cipher structures. Using it, we find a 16-round impossible differential for Gen-Skipjack and a 19-round impossible differential for Gen-CAST256. By this result we can disprove Sung's long standing conjecture that no such differential is possible for 16 or more rounds. On Gen-MARS and SMS4, the impossible differentials found by the UID-method are much longer than those found by the $\mathcal{U}$-method. On the Four-Cell and Gen-RC6 block ciphers, our results are the same as the best results previously obtained.

1. Introduction

Impossible differential cryptanalysis (IDC) was proposed by Biham et al. to attack Skipjack [1] and used by Knudsen against DEAL [7]. It has since been used against many other block ciphers. Ordinary differential cryptanalysis searches for keys which can produce the known differentials. Impossible differential cryptanalysis works the other way, discarding the keys which lead to the impossible differentials.

The key step of impossible differential cryptanalysis is to find the longest impossible differential. Impossible differentials are in the form: $(x_1, \ldots, x_n) \nrightarrow_r (y_1, \ldots, y_n)$ which means that when the input difference is $(x_1, \ldots, x_n)$, the output difference after r rounds cannot be $(y_1, \ldots, y_n)$. Suppose that the block cipher has m rounds, first, the adversary chooses several pairs of plaintexts which satisfy the input of the impossible differential; next he guesses the last $m - r$ round subkeys and decrypts the corresponding ciphertexts to the rth round, and verifies whether one of the decrypted pairs matches the output of the impossible differential. One can conclude that the last $m - r$ round subkey is wrong if any decrypted pair matches an impossible differential [2,17,8,11,12,16].

Usually, the impossible differentials are retrieved manually by observing the structure of the cipher. In [5], Kim et al. first introduced the $\mathcal{U}$-method to find the longest impossible differentials of various block cipher structures. However, there are some limitations in the $\mathcal{U}$-method:

☆ This work was supported by the Key Discipine Funding (Computer Technology) of Shanghai Dian Ji University, No. 13XKJ01.
* Corresponding author. Tel.: +86 2134205440.
E-mail addresses: luoyiyuan@gmail.com (Y. Luo), lai-xj@cs.sjtu.edu.cn (X. Lai), patwu1985@gmail.com (Z. Wu), ggong@uwaterloo.ca (G. Gong).
[1] This work was supported by the National Natural Science Foundation of China (61073149 and 61272440), and Research Fund for the Doctoral Program of Higher Education of China (20090073110027), State Key Laboratory of ASIC and System (11KF0020), Key Lab of Information Network Security, Ministry of Public Security (C11603).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.08.051

- The encryption (decryption) characteristic matrix of the block cipher structure must have the 1-Property [5]. A matrix is a 1-Property matrix if the number of ones in each column is at most one. Thus the $\mathcal{U}$-method is not general; it can only be applied to some special block ciphers.
- Some information is lost in calculating the impossible differentials. The $\mathcal{U}$-method cannot determine some kinds of inconsistencies and some longer impossible differentials cannot be found.

We propose an improved method, which we call the UID-method. It does not require the 1-Property in the characteristic matrix and can find more kinds of inconsistencies. We also describe the UID-method in the theory of finite state machine. We apply the UID-method to some well-known block cipher structures such as Gen-Skipjack [15], Gen-CAST256 [13], Gen-MARS [13], Gen-RC6 [13], Four-Cell [3], and SMS4 [21].

In *Asiacrypt'00* [15], Sung et al. conjectured that no impossible differential exists for Gen-Skipjack or Gen-CAST256 after n^2 rounds where n denotes the number of subblocks. Later in *FSE'09* Rump Session [14], Pudovkina claimed to prove that this conjecture is true. However, we find a 16-round impossible differential of Gen-Skipjack and a 19-round impossible differential of Gen-CAST256 using the UID-method when $n = 4$. By this result we can disprove this conjecture.

On Gen-MARS and SMS4, the impossible differentials found by the $\mathcal{U}$-method are 7-round and 6-round respectively. Using the UID-method, we find 11-round impossible differentials for both Gen-MARS and SMS4, much better than those found by the $\mathcal{U}$-method. In [19], Wu et al. gave an 18-round impossible differential of Four-Cell. Currently this is the longest impossible differential for the Four-Cell block cipher in the literature. Using our UID-method, the result is the same as Wu et al.'s result obtained by case-by-case treatment. All of these impossible differentials found by the UID-method are listed in Table 4.

2. Description of UID-method

In this paper, we assume that a block cipher structure S has n data subblocks, i.e., the input and the output of one round are $(X_1, X_2, \ldots, X_n)$ and $(Y_1, Y_2, \ldots, Y_n)$ respectively. We also assume that the round function F is bijective. Thus a nonzero input difference of F has a nonzero output difference.

Given a block cipher structure S with n subblocks, if the input difference is $U = (u_1, u_2, \ldots, u_n)$, then we call the difference vector U and the difference at the ith subblock u_i, $0 \leqslant i \leqslant n$. We denote the output difference after r rounds for U by U^r, and the value of the ith subblock of U^r by U_i^r. Given an input difference, the possible output difference of each subblock after r rounds is a linear XOR combination of the following four types of differences:

Zero difference. The difference is zero and denoted by 0.

Nonzero fixed difference. The difference is nonzero and fixed and denoted by l_i.

Nonzero varied difference. The difference can be any value except zero and is denoted by m_i.

Varied difference. The difference can be any value and is denoted by r_i.

Among these four types of differences, a nonzero fixed difference l_i and a nonzero varied difference m_i cannot be equal to a zero difference 0; and a varied difference r_i may be equal to either a zero difference or a nonzero difference. In the following, we define the inconsistency of two difference vectors:

Definition 2.1. Two differences vectors $U = (u_1, u_2, \ldots, u_n)$ and $V = (v_1, v_2, \ldots, v_n)$ are inconsistent if there exists a subset $I \subseteq \{1, 2, \ldots, n\}$ such that the XOR of differences in the subset are always unequal: $\oplus_{i\in I} u_i \neq \oplus_{i\in I} v_i$, $\oplus$ denotes the XOR operation.

For example, if $U = (l_1 \oplus m_1, 0)$ and $V = (l_1, 0)$ where l_1 is a nonzero fixed difference and m_1 is a nonzero varied difference, then U and V are inconsistent since $l_1 \oplus m_1$ cannot be equal to l_1. If $U = (u_1, u_2) = (l_1, l_1 \oplus m_1)$ and $V = (v_1, v_2) = (m_2, m_2)$, then $u_1 \oplus u_2 = m_1$ and $v_1 \oplus v_2 = 0$ are always unequal, thus U and V are inconsistent.

For a block cipher structure S, given an input difference vector U^0 and an output difference vector V^0, we can compute difference vector U^i after i rounds encryption and difference vector V^j after j rounds decryption. If U^i and V^j are inconsistent, then there exists an $i + j$ round impossible differential $U^0 \nrightarrow_{i+j} V^0$.

We consider 3 different kinds of transformations in a block cipher structure: the zero transformation **0**, the identity transformation **1** and the nonlinear bijective transformation $\mathbb{F}$. If the input difference is 0, then after the $\mathbb{F}$ transformation, the output difference is 0; If the input difference is a nonzero fixed difference l_i, then after the $\mathbb{F}$ transformation, the output difference is m_j, which is a new nonzero varied difference; otherwise, the output difference is r_j, which means a new varied difference. The three transformations are shown in Table 1.

In Fig. 1, we give an example to demonstrate how to use the inconsistency in Definition 1 to determine the impossible differential of the Feistel structure. If the input difference vector is $U^0 = (l_1, 0)$ where l_1 is a nonzero fixed difference, then from the encryption process: