A Unified Method for Finding Impossible Differentials of Block Cipher Structures

Yiyuan Luo[1,2], Zhongming Wu[1], Xuejia Lai[1] and Guang Gong[2]

[1] Department of Computer Science and Engineering, Shanghai Jiaotong University
luoyiyuan@sjtu.edu.cn
[2] Department of Electrical and Computer Engineering, University of Waterloo.

Abstract. In this paper, we propose a systematic method for finding impossible differentials for block cipher structures, better than the $\mathcal{U}$-method introduced by Kim *et al* [4]. It is referred as a unified impossible differential finding method (UID-method). We apply the UID-method to some popular block ciphers such as Gen-Skipjack, Gen-CAST256, Gen-MARS, Gen-RC6, Four-Cell, SMS4 and give the detailed impossible differentials. By the UID-method, we find a 16-round impossible differential on Gen-Skipjack and a 19-round impossible differential on Gen-CAST256. Thus we disprove the *Conjecture 2* proposed in *Asiacrypt'00* [9] and the theorem in *FSE'09* rump session presentation [8]. On Gen-MARS and SMS4, the impossible differentials find by the UID-method are much longer than that found by the $\mathcal{U}$-method. On the Four-Cell block cipher, our result is the same as the best result previously obtained by case-by-case treatment.

1 Introduction

Impossible differential cryptanalysis (IDC) was proposed by Biham *et al.* and Knudsen respectively to attack Skipjack [1] and DEAL [5]. It is known as one of the most popular attacks on block ciphers. Compared with ordinary differential cryptanalysis, impossible differential cryptanalysis uses impossible differentials to derive the right keys by discarding the wrong keys which lead to the impossible differential.

The key step of impossible differential cryptanalysis is to find the longest impossible differential. Impossible differentials are in the form: $(x_1, \cdots, x_n)_n \nrightarrow_r (y_1, \cdots, y_n)_n$ which means that when the input difference is $(x_1, \cdots, x_n)_n$, the output difference after r rounds cannot be $(y_1, \cdots, y_n)_n$. Suppose that the block cipher has m rounds, firstly, 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 decrypt the corresponding ciphertexts to r-th round, and verifies whether one of decrypted pairs meet the output of the impossible differential. One can conclude that the last $m - r$ round subkey is wrong if any decrypted pairs meet the differences of impossible differential. Usually, the impossible differentials are retrieved manually by observing the structure of the block ciphers. In [4], 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:

- The encryption (decryption) characteristic matrix of the block cipher structure must have 1-Property [4]. Thus the $\mathcal{U}$-method is not very general and can only be applied to some special block ciphers.
- Some information is lost during calculating the impossible differentials. The $\mathcal{U}$-method can not determine some kinds of inconsistencies and some longer impossible differential cannot be found.

In this paper, we propose an improved method to find the longest impossible differential for block cipher structures. We refer to this method as UID-method. The UID-method doesn't require the 1-Property of the encryption(decryption) characteristic matrix and can determine more kinds of inconsistencies. We apply the UID-method to some popular block ciphers such as Gen-Skipjack [9], Gen-CAST256 [7], Gen-MARS [7], Gen-RC6 [7], Four-Cell [2] and SMS4 [12].

In *Asiacrypt'00*[9], Sung *et al.* conjectured that there doesn't exist an impossible differential in Gen-Skipjack and Gen-CAST256 after n^2 rounds where n denotes the number of subblocks. Later in *FSE'09* Rump Session [8], Pudovkina even proved 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 $n = 4$. Thus we disprove this conjecture.

On Gen-MARS and SMS4, the impossible differentials found by $\mathcal{U}$-method are 7-round and 6-round respectively. Using the UID-method, we find a 11-round impossible differential of Gen-MARS and a 11-round impossible differential of SMS4, which are much better than those found by the $\mathcal{U}$-method. In [10], Wu *et al.* gave an 18-round impossible differential of Four-Cell. Currently this is the longest impossible differential for 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.

The rest of this paper is organized as follows. Section 2 describes the UID-method. Section 3 disproves Sung *et al*'s conjecture by the UID-method. Section 4 lists the detailed impossible differential results for some popular block cipher structures and gives a comparison between the UID-method and the $\mathcal{U}$-method. Finally, Section 5 concludes this paper.

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 non-zero input difference of F has a non-zero 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 U is the difference vector and $u_i, 0 \leq i \leq n$

is the difference at the i-th subblock. We denote the output difference after r rounds for U by U^r, and denote the value of the i-th 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 inconsistence of two difference vectors:

Definition 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: $\oplus_{i \in I} u_i \neq \oplus_{i \in I} v_i$.*

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 exist 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 $\mathbb{0}$, the identical transformation $\mathbb{1}$ 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.

Table 1. Three Transformations in a Block Cipher Structure

Trans.	Input	Output	Note
$\mathbb{0}$	$x \in \{0, l_i, m_i, r_i\}$	0	Zero trans.
$\mathbb{1}$	$x \in \{0, l_i, m_i, r_i\}$	x	Identical trans.
$\mathbb{F}$	0	0	m_j denotes a new nonzero varied difference.
	l_i	m_j	
	m_i	m_j	
	Otherwise	r_j	r_j denotes a new varied difference

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

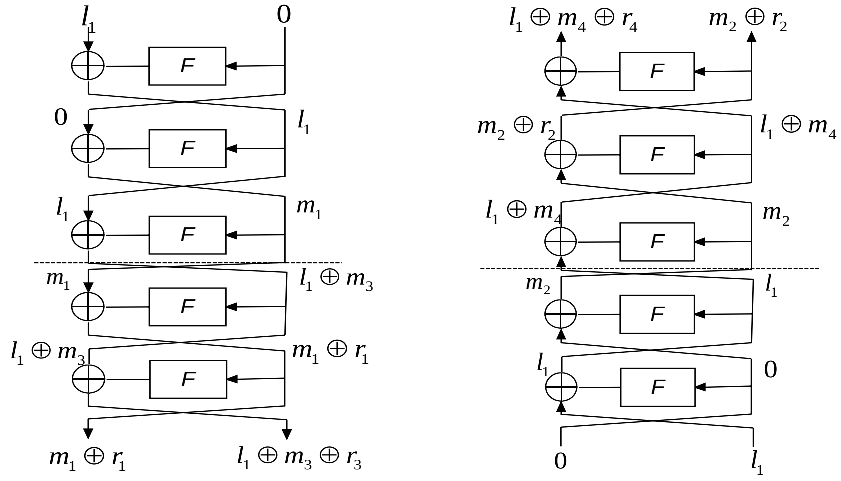


Fig. 1. Differences of 5-round Feistel Structure. The left denotes differences change from the encryption, the right denotes differences change from the decryption.

the input difference vector is $U^0 = (l_1, 0)$ where l_1 is a nonzero fixed difference, then from the encryption process:
1. After the first round, the difference vector $U^1 = (0, l_1)$.
2. After the second round, the difference vector $U^2 = (l_1, m_1)$ where m_1 is a nonzero varied difference. Since a nonzero fixed difference l_1 to $\mathbb{F}$ will result in a nonzero varied difference m_1.
3. After the third round, the difference vector $U^3 = (m_1, l_1 \oplus m_3)$ where m_3 is a new nonzero varied difference.
4. After the fourth round, the difference vector becomes $U^4 = (l_1 \oplus m_3, m_1 \oplus r_1)$ where r_1 is a varied difference. Since $l_1 \oplus m_3$ could be zero, then according to Table 1, applying $\mathbb{F}$ to $l_1 \oplus m_3$ will result in a varied difference r_1.
5. After the fifth round, the difference vector $U^5 = (m_1 \oplus r_1, l_1 \oplus m_3 \oplus r_3)$ where r_3 is a new varied difference.

In the similar way, if the output difference vector is $V^0 = (0, l_1)$, then we can get the difference vectors $V^i (1 \leq i \leq 5)$ from the decryption process. The results are shown in the right of Fig.1.

From Fig.1, we know $U^3 = (U_1^3, U_2^3) = (m_1, l_1 \oplus m_3)$ and $V^2 = (V_1^2, V_2^2) = (m_2, l_1)$. Then according to Definition 2, U^3 and V^2 are inconsistent since $U_2^3 \oplus V_2^2 = m_3$, which cannot be zero. Therefore we get a 5-round impossible differential $(l_1, 0) \nrightarrow_5 (0, l_1)$ for the Feistel structure.

2.1 Matrice Representation of Block Cipher Structures

The encryption and decryption characteristic matrix of block cipher structures are defined as follows.

Definition 2. *If the output $(Y_1, \ldots, Y_n)$ can be expressed in terms of $(X_1, \ldots, X_n)$ in one round of the block cipher structure S in the following* ***UID-form:***

$$\begin{aligned} Y_1 &= F_{11}(X_1) \oplus F_{21}(X_2) \oplus \ldots \oplus F_{n1}(X_n) \\ Y_2 &= F_{12}(X_1) \oplus F_{22}(X_2) \oplus \ldots \oplus F_{n2}(X_n) \\ \vdots \; & \; \vdots \\ Y_n &= F_{1n}(X_1) \oplus F_{2n}(X_2) \oplus \ldots \oplus F_{nn}(X_n) \end{aligned}$$

where $F_{11}, \ldots, F_{nn}$ are transformations in Table 1, then the ***encryption characteristic matrix*** *$\mathcal{E}$ is an $n \times n$ matrix defined as:*

$$\mathcal{E} = \begin{pmatrix} F_{11} & F_{12} & \cdots & F_{1n} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ F_{n1} & F_{n2} & \cdots & F_{nn} \end{pmatrix}$$

Similarly, the ***decryption characteristic matrix*** *of the block cipher structure $\mathcal{D}$ is defined by the decryption process in the similar way.*

Taking the Feistel structure as an example, we have $(Y_1, Y_2) = (X_2, X_1 \oplus F(X_2))$ and $(X_1, X_2) = (F(Y_1) \oplus Y_2, Y_1)$, thus the $\mathcal{E}$ and $\mathcal{D}$ matrices are $\mathcal{E} = \begin{pmatrix} \mathbb{0} & \mathbb{1} \\ \mathbb{1} & \mathbb{F} \end{pmatrix}$ and $\mathcal{D} = \begin{pmatrix} \mathbb{F} & \mathbb{1} \\ \mathbb{1} & \mathbb{0} \end{pmatrix}$.

There are some block cipher structures which cannot be transformed into the UID-form in Definition 2. In this case, we can transform them into a composition of several UID-forms, and for each UID-form there is a corresponding characteristic matrix. For example, assume that $(Y_1, Y_2) = (F(X_1 \oplus X_2), F(X_1 \oplus X_2) \oplus X_2)$, then we can divide the encryption function into the composition of two functions. The first function is $(Z_1, Z_2) = (X_1 \oplus X_2, X_2)$ and the second function is $(Y_1, Y_2) = (F(Z_1), F(Z_1) \oplus Z_2)$. Consequently the characteristic matrix is $\mathcal{E}_1 \cdot \mathcal{E}_2 = \begin{pmatrix} \mathbb{1} & \mathbb{0} \\ \mathbb{1} & \mathbb{1} \end{pmatrix} \cdot \begin{pmatrix} \mathbb{F} & \mathbb{F} \\ \mathbb{0} & \mathbb{1} \end{pmatrix}$.

2.2 Searching the Impossible Differentials.

Definition 3. *The multiplication of a difference vector $U = (u_1, u_2, \ldots, u_n)$ and an encryption (decryption) characteristic matrix $\mathcal{E}$ $(\mathcal{D})$ is defined as $U \cdot \mathcal{E} = (\sum_{i=1}^{n} u_i \cdot \mathcal{E}_{i1}, \sum_{i=1}^{n} u_i \cdot \mathcal{E}_{i2}, \ldots, \sum_{i=1}^{n} u_i \cdot \mathcal{E}_{in})$. Here $u_i \cdot \mathcal{E}_{ij}$ means applying the transformation $\mathcal{E}_{ij}$ to the difference u_i.*

For example, if the input difference of the Feistel structure is $U = (u_1, u_2) = (l_1, 0)$, then $U \cdot \mathcal{E} = (l_1, 0) \cdot \begin{pmatrix} \mathbb{0} & \mathbb{1} \\ \mathbb{1} & \mathbb{F} \end{pmatrix} = (0, l_1)$. After the one-round encryption function and decryption function are converted into matrices, denoted as $\mathcal{E}$ and $\mathcal{D}$, we can compute the difference vector after i-round encryption from the input difference vector U^0 as $U^i = ((U^0 \cdot \underbrace{\mathcal{E}) \cdots \cdot \mathcal{E})}_{i\ times}$ and the difference vector after j-round decryption from the output difference vector V^0 as $V^j = ((V^0 \cdot \underbrace{\mathcal{D}) \cdots \cdot \mathcal{D})}_{j\ times}$. If U^i and V^j are inconsistent, then we find an impossible differential $U^0 \nrightarrow_{i+j} V^0$.

```
 Input: The $n \times n$ encryption characteristic matrix $\mathcal{E}$ , decryption
        characteristic matrix $\mathcal{D}$ and an integer $r = 0$.
Output: The longest impossible differential $\Delta in \nrightarrow_r \Delta out$ where $\Delta in$
        is the input difference vector and $\Delta out$ is the output difference
        vector.
 Step1. For a difference vector pair $(U^0, V^0)$, find the maximum in-
        teger $m = i + j$ such that $U^i = ((U^0 \cdot \underbrace{\mathcal{E}) \cdots \cdot \mathcal{E})}_{i\ times}$ and $V^j =$
        $((V^0 \cdot \underbrace{\mathcal{D}) \cdots \cdot \mathcal{D})}_{j\ times}$ are inconsistent. If $r < m$, let $r \leftarrow m$ and
        $(\Delta in, \Delta out) \leftarrow (U^0, V^0)$.
 Step2. Repeat Step1 until all the cases of $(U^0, V^0)$ have been enu-
        merated.
 Step3. Return $\Delta in \nrightarrow_r \Delta out$.
```

Algorithm 1. Compute the longest impossible differential.

In the UID-method, firstly we choose an input difference vector U^0 and an output difference vector V^0. Then we compute U^i from U^0 forwardly and V^j from V^0 inversely, if U^i and V^j are inconsistent then we get an impossible differential. After achieving a maximum $i+j$ such that U^i and V^j are inconsistent, we find the longest impossible differential based on U^0 and V^0. To find the longest impossible differential for a block cipher structure, we enumerate every possible difference vector of input U^0 and output V^0, and find the maximum $i + j$. Algorithm 1 explains the idea of finding the longest impossible differential.

Toy example. It's well known that there exists a 5-round impossible differential $(l_1, 0) \nrightarrow_5 (0, l_1)$ for the Feistel structure. The input difference vector U^0 and the output difference V^0 can be any one of the difference set $\{(l_1, 0), (0, l_1), (l_1, l_1), (l_1, l_2), (l_2, l_1), (l_2, 0), (0, l_2), (l_2, l_2)\}$ where l_1 and l_2 are different nonzero fixed differences.

- If $U^0 = (l_1, 0)$ and $V^0 = (0, l_1)$, then U^3 and V^2 are inconsistent, we find a $3 + 2 = 5$ round impossible differential $(l_1, 0) \nrightarrow_5 (0, l_1)$.
- If $U^0 = (0, l_1)$ and $V^0 = (0, l_1)$, then U^3 and V^1 are inconsistent, we find a $3 + 1 = 4$ round impossible differential $(0, l_1) \nrightarrow_4 (0, l_1.)$

– After enumerate all of the cases, we cannot find an impossible differential longer than 5. Therefore the longest impossible for Feistel structure found by UID-method is $(l_1, 0) \nrightarrow_5 (0, l_1)$.

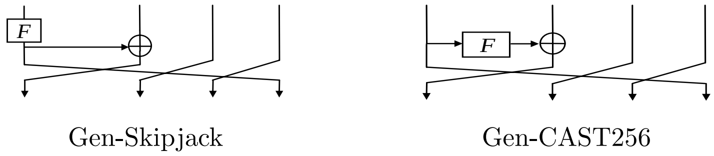
For the Feistel structure, we need to enumerate $8^2 = 64$ cases in order to find the longest impossible differential. It is not hard to write a computer program to do this job. In later sections, we will apply UID-method to some popular block cipher structures when the number of subblocks $n = 4$.

3 Disprove Sung *et al*'s Conjecture

In ref.[9], Sung *et al.* analyzed the impossible differential of (i) the Gen-Skipjack structure whose one-round function is $(y_1, y_2, \ldots, y_n) = (F(x_1) \oplus x_2, x_3, \ldots, x_n, F(x_1))$, and (ii) the Gen-CAST256 structure whose one-round function is $(y_1, y_2, \ldots, y_n) = (F(x_1) \oplus x_2, x_3, \ldots, x_n, x_1)$, where F is a keyed-round bijective function. They proposed the following conjecture:

There does not exist an impossible differential in Gen-Skipjack and Gen-CAST256 after n^2 rounds.

Later in FSE'09 rump session, Pudovkina claimed that this conjecture is true and even gave the proof [8].



Gen-Skipjack

Gen-CAST256

Figure 2. Gen-Skipjack and Gen-CAST256 structure in the case of $n = 4$.

We apply the UID-method on these two structures in the case of $n = 4$ and find a 16-round impossible differential $(0, 0, 0, l_1) \nrightarrow_{16} (l_2, 0, 0, l_2)$ for Gen-Skipjack and a 19-round impossible differential $(0, 0, 0, l_1) \nrightarrow_{19} (l_1, 0, 0, 0)$ for Gen-CAST256. Thus we disprove Sung *et al*'s conjecture. For $n = 4$, the Gen-Skipjack and Gen-CAST256 structure are depicted in Fig.2.

The encryption characteristic matrix $\mathcal{E}$ and decryption characteristic matrix $\mathcal{D}$ of Gen-Skipjack are:

$$\mathcal{E} = \begin{pmatrix} \mathbb{F} & \mathbb{0} & \mathbb{0} & \mathbb{F} \\ \mathbb{1} & \mathbb{0} & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \mathbb{1} & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & \mathbb{1} & \mathbb{0} \end{pmatrix}, \mathcal{D} = \begin{pmatrix} \mathbb{0} & \mathbb{1} & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & \mathbb{1} & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & \mathbb{0} & \mathbb{1} \\ \mathbb{F} & \mathbb{1} & \mathbb{0} & \mathbb{0} \end{pmatrix}$$

In order to find the longest impossible differential for Gen-Skipjack, we implemented **Algorithm 1** and ran it on a laptop with Windows XP2 operating system . We found a 16-round impossible differential $(0, 0, 0, l_1) \nrightarrow_{16} (l_2, 0, 0, l_2)$ less in one minute.

Table 2. 16-round Impossible differential of Gen-Skipjack

R	X_1	X_2	X_3	X_4
0 ↓	0	0	0	l_1
1	0	0	l_1	0
2	0	l_1	0	0
14	m_7	$m_1 \oplus m_6$	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$
13	m_6	$m_4 \oplus r_1$	$m_2 \oplus m_3 \oplus m_5$	m_1
12	r_1	$m_2 \oplus m_3 \oplus m_5$	m_1	m_4
11	m_5	m_1	m_4	$m_2 \oplus m_3$
10	0	m_4	$m_2 \oplus m_3$	m_1
9	m_4	$m_2 \oplus m_3$	m_1	0
8	m_3	m_1	0	m_2
7	0	0	m_2	m_1
6	0	m_2	m_1	0
5	m_2	m_1	0	0
4	0	0	0	m_1
3	0	0	m_1	0
2	0	m_1	0	0
1	m_1	0	0	0
0 ↑	l_2	0	0	l_2

Table 3. 19-round Impossible differential of Gen-CAST256

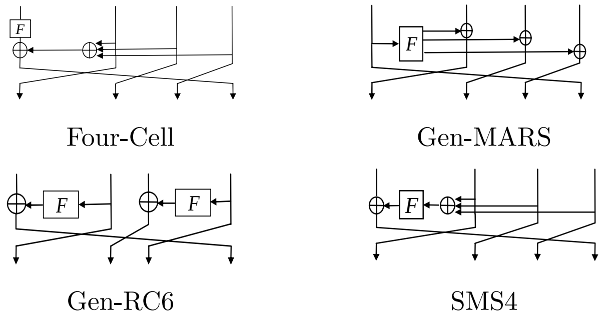
R	X_1	X_2	X_3	X_4
0 ↓	0	0	0	l_1
1	0	0	l_1	0
2	0	l_1	0	0
3	l_1	0	0	0
16	$l_1 \oplus m_{10}$	$m_2 \oplus m_7 \oplus m_9 \oplus r_{13}$	$m_2 \oplus r_5 \oplus r_{11}$	$m_8 \oplus r_9$
15	$m_2 \oplus m_7 \oplus m_9$	$m_2 \oplus r_5 \oplus r_{11}$	$m_8 \oplus r_9$	$l_1 \oplus m_{10}$
14	$m_2 \oplus r_5$	$m_8 \oplus r_9$	$l_1 \oplus m_{10}$	$m_2 \oplus m_7 \oplus m_9$
13	m_8	$l_1 \oplus m_{10}$	$m_2 \oplus m_7 \oplus m_9$	$m_2 \oplus r_5$
12	l_1	$m_2 \oplus m_7 \oplus m_9$	$m_2 \oplus r_5$	m_8
11	$m_2 \oplus m_7$	$m_2 \oplus r_5$	m_8	l_1
10	m_2	m_8	l_1	$m_2 \oplus m_7$
9	0	l_1	$m_2 \oplus m_7$	m_2
8	l_1	$m_2 \oplus m_7$	m_2	0
7	m_2	m_2	0	l_1
6	0	0	l_1	m_2
5	0	l_1	m_2	0
4	l_1	m_2	0	0
3	0	0	0	l_1
2	0	0	l_1	0
1	0	l_1	0	0
0 ↑	l_1	0	0	0

In order to verify the result, let $U^0 = (0, 0, 0, l_1)$ and $V^0 = (l_2, 0, 0, l_2)$, we can see that $U^2 = (0, l_1, 0, 0)$ and $V^{14} = (m_7, m_1 \oplus m_6, m_4 \oplus r_1, m_2 \oplus m_3 \oplus m_5)$ from Table 2, since m_7 cannot be zero, U^2 and V^{14} are inconsistent. Thus a 16 round impossible differential is found.

Using the same method, we find a 19-round impossible differential $(0, 0, 0, l_1) \nrightarrow_{19} (l_1, 0, 0, 0)$ for Gen-CAST256 . In Table 3, if $U^0 = (0, 0, 0, l_1)$ and $V^0 = (l_1, 0, 0, 0)$, then U^3 and V^{16} are inconsistent, since $l_1 \oplus m_{10}$ and l_1 are inconsistent. Note in [11], Yap found a 19-round impossible differential on EFN Type-I (See Table 2 in [11]) by the $\mathcal{U}$-method. Actually this is a 19-round impossible differential of Gen-CAST256, but it seems that they don't know Sung *et al*'s conjecture about Gen-CAST256.

4 Results for Some Other Block Cipher Structures

In this section, we list our results for some other block cipher structures, such as Four-Cell [2], Gen-MARS [7], Gen-RC6 [7] and SMS4 [12]. We assume that the number of subblocks is $n = 4$. These block cipher structures are depicted in Fig.3 and the results are listed in Table 4.



Four-Cell

Gen-MARS

Gen-RC6

SMS4

Figure 3. Some popular block cipher structures.

Table 4. Summary of Impossible differentials of some popular block cipher structures found by $\mathcal{U}$-method and UID-method

Block Cipher	$\mathcal{U}$-method (round)	UID-method (round)	Impossible Differential
Gen-Skipjack [9]	-	16	$(0,0,0,l_1) \not\rightarrow_{16} (l_2,0,0,l_2)$
Gen-CAST256 [7]	15 [4] 19 [3]	19	$(0,0,0,l_1) \not\rightarrow_{19} (l_2,0,0,0)$
Four-Cell [2]	-	18	$(l_1,0,0,0) \not\rightarrow_{18} (l_2,l_2,0,0)$
Gen-MARS [7]	7 [4]	11	$(0,0,0,l_1) \not\rightarrow_{11} (l_1,0,0,0)$
Gen-RC6 [7]	9 [4]	9	$(0,0,l_1,0) \not\rightarrow_{9} (0,l_1,0,0)$ $(l_1,0,0,0) \not\rightarrow_{9} (0,0,0,l_1)$
SMS4 [12]	6 [11]	11	$(l_1,l_1,l_1,0) \not\rightarrow_{11} (0,l_1,l_1,l_1)$

In [10], Wu *et al.* gave an 18-round impossible differential on Four-Cell. Currently this is the longest impossible differential for 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. As shown in Table 5, if $U^0 = (l_1, 0, 0, 0)$ and $V^0 = (l_2, l_2, 0, 0)$, then U^{12} and V^6 are inconsistent, since m_2 cannot be zero.

In [4], Kim *et al.* gave a 7-round impossible differential on Gen-MARS using the $\mathcal{U}$-method. Table 6 shows our result on the Gen-MARS structure, if $U^0 = (0, 0, 0, l_1)$ and $V^0 = (l_1, 0, 0, 0)$, then $U^3 = (u_1, u_2, u_3, u_4) = (l_1, 0, 0, 0)$ and $V^8 = (v_1, v_2, v_3, v_4) = (l_1 \oplus m_4 \oplus r_2 \oplus r_4, m_2 \oplus m_4 \oplus r_2 \oplus r_6, m_2 \oplus m_4 \oplus r_4 \oplus$

Table 5. 18-round Impossible differential of Four-Cell

R	X_1	X_2	X_3	X_4
0 ↓	l_1	0	0	0
1	0	0	0	m_1
2	0	0	m_1	m_1
3	0	m_1	m_1	0
4	m_1	m_1	0	0
5	m_1	0	0	$m_1 \oplus m_3$
6	0	0	$m_1 \oplus m_3$	$m_1 \oplus m_3 \oplus m_5$
7	0	$m_1 \oplus m_3$	$m_1 \oplus m_3 \oplus m_5$	m_5
8	$m_1 \oplus m_3$	$m_1 \oplus m_3 \oplus m_5$	m_5	0
9	$m_1 \oplus m_3 \oplus m_5$	m_5	0	$m_1 \oplus m_3 \oplus r_4$
10	m_5	0	$m_1 \oplus m_3 \oplus r_4$	$m_1 \oplus m_3 \oplus m_5 \oplus r_4 \oplus r_6$
11	0	$m_1 \oplus m_3 \oplus r_4$	$m_1 \oplus m_3 \oplus m_5 \oplus r_4 \oplus r_6$	$m_5 \oplus m_2 \oplus r_6$
12	$m_1 \oplus m_3 \oplus r_4$	$m_1 \oplus m_3 \oplus m_5 \oplus r_4 \oplus r_6$	$m_5 \oplus m_2 \oplus r_6$	$\mathbf{m_2}$
6	r_1	m_4	m_2	$\mathbf{0}$
5	m_4	m_2	0	0
4	m_2	0	0	0
3	0	0	0	l_2
2	0	0	l_2	l_2
1	0	l_2	l_2	0
0 ↑	l_2	l_2	0	0

$r_6, m_2 \oplus r_2 \oplus r_4 \oplus r_6)$. Since $u_1 \oplus u_2 \oplus u_3 = l_1$ and $v_1 \oplus v_2 \oplus v_3 = l_1 \oplus m_4$, which are inconsistent, thus U^3 and V^6 are inconsistent. Therefore an 11-round impossible differential is found, which is much better than Kim *et al.*'s result.

Table 6. 11-round Impossible differential of Gen-MARS

R	X_1	X_2	X_3	X_4
0 ↓	0	0	0	l_1
1	0	0	l_1	0
2	0	l_1	0	0
3	l_1	0	0	0
8	$l_1 \oplus m_4 \oplus r_2 \oplus r_4$	$m_2 \oplus m_4 \oplus r_2 \oplus r_6$	$m_2 \oplus m_4 \oplus r_4 \oplus r_6$	$m_2 \oplus r_2 \oplus r_4 \oplus r_6$
7	$m_2 \oplus m_4 \oplus r_2$	$m_2 \oplus m_4 \oplus r_4$	$m_2 \oplus r_2 \oplus r_4$	$l_1 \oplus m_4 \oplus r_2 \oplus r_4$
6	$m_2 \oplus m_4$	$m_2 \oplus r_2$	$l_1 \oplus m_4 \oplus r_2$	$m_2 \oplus m_4 \oplus r_2$
5	m_2	$l_1 \oplus m_4$	$m_2 \oplus m_4$	$m_2 \oplus m_4$
4	l_1	m_2	m_2	m_2
3	0	0	0	l_1
2	0	0	l_1	0
1	0	l_1	0	0
0 ↑	l_1	0	0	0

For the Gen-RC6 structure, we found two 9-round impossible differentials, the details are shown in Table 8 and Table 9. One of our results is the same as the result in [11].

In ref. [11], Yap found a 6-round impossible differential for the block cipher SMS4 by using the $\mathcal{U}$-method. We find a 11-round impossible differential by the UID-method. The details are shown in Table 7. Our result is one round shorter than Lu's result [6] obtained by case-by-case treatment. This is because Lu used

Table 7. 11-round Impossible differential of SMS4

R	X_1	X_2	X_3	X_4
0 ↓	l_1	l_1	l_1	0
1	l_1	l_1	0	l_1
2	l_1	0	l_1	l_1
3	0	l_1	l_1	l_1
8	$m_2 \oplus r_6$	$l_1 \oplus r_4$	$l_1 \oplus r_2$	$l_1 \oplus m_4$
7	$l_1 \oplus r_4$	$l_1 \oplus r_2$	$l_1 \oplus m_4$	m_2
6	$l_1 \oplus r_2$	$l_1 \oplus m_4$	m_2	l_1
5	$l_1 \oplus m_4$	m_2	l_1	l_1
4	m_2	l_1	l_1	l_1
3	l_1	l_1	l_1	0
2	l_1	l_1	0	l_1
1	l_1	0	l_1	l_1
0 ↑	0	l_1	l_1	l_1

Table 8. 9-round Impossible differential of Gen-RC6 (1)

R	X_1	X_2	X_3	X_4
0 ↓	0	0	l_1	0
1	0	l_1	0	0
2	l_1	0	0	m_1
3	0	m_3	m_1	l_1
6	$m_8 \oplus r_5$	$m_4 \oplus r_2$	$m_2 \oplus m_7 \oplus r_6$	$l_1 \oplus m_{10}$
5	$m_4 \oplus r_2$	$m_2 \oplus m_7$	$l_1 \oplus m_{10}$	m_8
4	$m_2 \oplus m_7$	l_1	m_8	m_4
3	l_1	0	m_4	m_2
2	0	0	m_2	l_1
1	0	0	l_1	0
0 ↑	0	l_1	0	0

Table 9. 9-round Impossible differential of Gen-RC6 (2)

R	X_1	X_2	X_3	X_4
0 ↓	l_1	0	0	0
1	0	0	0	l_1
2	0	m_1	l_1	0
3	m_1	l_1	0	m_3
6	$m_2 \oplus m_8 \oplus r_5$	$l_1 \oplus m_{10}$	$m_7 \oplus r_6$	$m_4 \oplus r_2$
5	$l_1 \oplus m_{10}$	m_7	$m_4 \oplus r_2$	$m_2 \oplus m_8$
4	m_7	m_4	$m_2 \oplus m_8$	l_1
3	m_4	m_2	l_1	0
2	m_2	l_1	0	0
1	l_1	0	0	0
0 ↑	0	0	0	l_1

the details of the S-Box to exhaustively search the impossible differential, while our method considers only the block cipher structure.

Compared with the $\mathcal{U}$-method, the UID-method has the following advantages. *a). UID-method doesn't require the 1-Property of the characteristic matrix.* If the number of $\mathbb{1}$ in each column of the encryption or decryption characteristics matrix is zero or one, then the matrix is a 1-property matrix. $\mathcal{U}$-method requires the characteristic matrix must have the 1-property. The UID-method doesn't need this property. Thus it is more general and can be applied to more block cipher structures. The encryption characteristic matrix of the Four-Cell block cipher doesn't have the 1-property, thus the $\mathcal{U}$-method doesn't work , whereas the UID-method still works.

b). UID-method can determine more kinds of inconsistencies. $\mathcal{U}$-method considers only the inconsistency by the corresponding component of difference vectors. UID-method considers the inconsistency of the XOR sum of several corresponding components, which has more capability to detect the conflict.

Taking the Gen-MARS block cipher structure as example (see Table 6), if $U^0 = (0,0,0,l_1)$ and $V^0 = (l_1,0,0,0)$, then $U^3 = (u_1,u_2,u_3,u_4) = (l_1,0,0,0)$ and $V^6 = (v_1,v_2,v_3,v_4) = (l_1 \oplus m_4 \oplus r_2 \oplus r_4, m_2 \oplus m_4 \oplus r_2 \oplus r_6, m_2 \oplus m_4 \oplus r_4 \oplus r_6, m_2 \oplus r_2 \oplus r_4 \oplus r_6)$. Since $u_1 \oplus u_2 \oplus u_3 = l_1$ and $v_1 \oplus v_2 \oplus v_3 = l_1 \oplus m_4$ are inconsistent, thus U^3 and V^6 are inconsistent. This kind of inconsistency cannot be detected by the $\mathcal{U}$-method.

5 Conclusion

Inspired by the work [4] of automatically retrieving the impossible differentials, we make some improvements based on the $\mathcal{U}$-method and propose a unified impossible differential finding method for block cipher structures. We apply the UID-method to some block cipher structures and get better results than the previous work. Thus, UID-method can be used as a unified tool to evaluate the vulnerability of new block cipher structures against impossible differential cryptanalysis.

References

1. E. Biham, A. Biryukov and A. Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using impossible diffrentials, *EUROCRYPT'99*, LNCS 2595, pp. 12-23, 1999.
2. J. Choy, G. Chew, K. Khoo and H. Yap, Cryptographic properties and application of a generalized unbalanced feistel network structure. *ACISP'2009*, LNCS 5594, pp. 73-89, 2009.
3. J. Choy and H. Yap, Impossible Boomerang Attack for Block Cipher Structures. *IWSEC 2009*, LNCS 5824, pp. 22-37, 2009.
4. J. Kim, S. Hong, J. Sung, S. Lee and J. Lim: Impossible differential cryptanalysis for block cipher structures, *INDOCRYPT 2003*, LNCS 2904, pp. 82-96, 2003.
5. L. Knudsen. DEAL-A 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, Feb.1998.

6. J. Lu, Attacking reduced-round versions of the SMS4 block cipher in the chinese WAPI standard, *ICICS'07*, LNCS 4861, pp. 306-318, 2007.
7. S. Moriai and S. Vaudenay, On the pseudorandomness of Top-Level schemes of block ciphers, *ASIACRYPT'00*, LNCS 1976, pp. 289-302, 2000.
8. Marina Pudovkina, On Impossible Truncated Differentials of Generalized Feistel and Skipjack Ciphers, *FSE 2009 rump session*. Avaiable at: http://fse2009rump.cr.yp.to/e31bba5d1227eac5ef0daa6bcbf66f27.pdf
9. J. Sung, S. Lee, J. Lim, S. Hong, S. Park, Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis, *Advances in Cryptology-ASIACRYPT'00*, LNCS 1976, Springer-Verlag, 2000, pp 274-288.
10. W. Wu, L. Zhang, L. Zhang and W. Zhang: Security analysis of the GF-NLFSR structure and Four-Cell block cipher, *ICICS 2009*, LNCS 5927, pp. 17-31, 2009.
11. H. Yap, Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis. *SecTech 2008*, CCIS 29, pp. 103-121, 2009.
12. Specication of SMS4, block cipher for WLAN products SMS4 (in Chinese), http://www.oscca.gov.cn/UpFile/200621016423197990.pdf.