Hindawi
Security and Communication Networks
Volume 2017, Article ID 5980251, 9 pages
https://doi.org/10.1155/2017/5980251

Research Article

Improvements for Finding Impossible Differentials of Block Cipher Structures

Yiyuan Luo[1] and Xuejia Lai[2,3]

[1]*School of Electronics and Information, Shanghai Dian Ji University, Shanghai, China*
[2]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*
[3]*Westone Cryptologic Research Center, Beijing 100070, China*

Correspondence should be addressed to Yiyuan Luo; luoyy@sdju.edu.cn

Received 30 March 2017; Accepted 17 July 2017; Published 29 August 2017

Academic Editor: Jesús Díaz-Verdejo

We improve Wu and Wang's method for finding impossible differentials of block cipher structures. This improvement is more general than Wu and Wang's method where it can find more impossible differentials with less time. We apply it on Gen-CAST256, Misty, Gen-Skipjack, Four-Cell, Gen-MARS, SMS4, MIBS, Camellia*, LBlock, E2, and SNAKE block ciphers. All impossible differentials discovered by the algorithm are the same as Wu's method. Besides, for the 8-round MIBS block cipher, we find 4 new impossible differentials, which are not listed in Wu and Wang's results. The experiment results show that the improved algorithm can not only find more impossible differentials, but also largely reduce the search time.

1. Introduction

Impossible differential cryptanalysis, introduced by Biham et al. [1] and Knudsen [2] independently, is a special case of differential cryptanalysis that uses differentials with probability zero to sieve the right keys from the wrong keys. It is one of the most powerful attacks for block ciphers and is considered in many block cipher designs [3–10]. The best cryptanalytic results for some block ciphers are obtained by impossible differential cryptanalysis [1, 11]. For example, the currently best attack on the 31-round Skipjack is still the impossible differential cryptanalysis by Biham et al. [1].

The key step in impossible differential cryptanalysis of a block cipher is to find the longest impossible differential. Given two variables $x_1, x_2 \in \mathbb{F}_2^n$, the difference of x_1 and x_2 is usually denoted as $\Delta x = x_1 \oplus x_2$. An impossible differential for an n-subblock block cipher is in the form $(\Delta \text{in} \nrightarrow_r \Delta \text{out})$, where $\Delta \text{in} = (\Delta x_1, \ldots, \Delta x_n)$ and $\Delta \text{out} = (\Delta y_1, \ldots, \Delta y_n)$. $(\Delta \text{in} \nrightarrow_r \Delta \text{out})$ means the probability of the output difference is Δout after r rounds of a block cipher for an input difference Δin is zero. At the first glance, impossible differentials are obtained manually by observing the block cipher structure. However, since the emergence of impossible differential cryptanalysis, automated techniques for finding impossible differentials have been introduced.

The first automated technique is called the Shrinking method introduced by Biham et al. [1]. This method is simple but very useful. It only considers truncated differentials whose differences distinguish only between zero and arbitrary nonzero difference. Given a block cipher, the adversary first designs a mini version of this block cipher, which scales down the block cipher but preserves the global structure. Then the adversary exhaustively searches for this mini cipher and obtains some truncated impossible differentials. Usually these truncated impossible differentials of the mini cipher remain impossible differentials in the normal version. This method can deal with most block ciphers in the real world. However, it becomes very slow if the number of subblocks of a block cipher is as large as 16, since exhaustive search on the mini version of this type of cipher is still a heavy load for most computers.

The second automated technique is based on the miss in the middle approach. This method combines two differentials, one from the input and the other from the output, both with probability 1. However, these two differentials cannot meet in the middle since they can never be equal in the

middle. The $\mathcal{U}$ method [12, 13] and the UID method [14] both belong to this category. In the $\mathcal{U}$ method and the UID method, the adversary first represents the block cipher structure as a matrix; then given a differential pair $(\Delta\text{in}, \Delta\text{out})$, he calculates the m-round intermediate difference from Δin forwardly and the $(r - m)$-round intermediate difference from Δout backwardly by the matrix method. If there is a contradiction for these two intermediate differences, then an impossible differential $(\Delta\text{in} \not\rightarrow_r \Delta\text{out})$ is verified. Representing a block cipher by the matrix has been a popular method in impossible differential and integral and zero correlation linear cryptanalysis [8, 10, 15–20].

In [21], Wu and Wang extend the $\mathcal{U}$-method and UID method to a more generalized method which does not use the miss in the middle approach. They treat the r-round block cipher structure as a system of equations, which describe the propagation behavior of differences in the inner primitives, especially sbox permutations or branch swapping of the block cipher structure. To judge if a truncated differential $(\Delta\text{in}, \Delta\text{out})$ is impossible, they predict information about unknown variables from the known ones iteratively. Finally a truncated differential is verified by checking the constrained conditions in the system. This method is similar to a linear programming method for solving optimization problems.

In [22], Sun et al. show that Wu and Wang's automatic search method can find all impossible differentials of a cipher that are independent of the choices of the inner primitives. However, Wu and Wang's method can only find all truncated impossible differentials since the choice of truncated difference may result in missing some impossible differentials. Wu and Wang's method only considers differences $\Delta\text{in} = (x_1, \ldots, x_n)$ and $\Delta\text{out} = (y_1, \ldots, y_n)$, where x_i and y_i are zero or nonzero values. They assign an indicator to indicate the choice of x_i and y_i, representing by 0 a subblock without difference and by 1 a subblock with a difference. The relationships between nonzero differences have been omitted. For example, y_i may be equal to some x_j, where $1 \le i, j \le n$. If some linear constraints between nonzero variables in Δin and Δout are needed, Wu and Wang claimed their method could still work by translating all linear constraints into the system of equations. However, this method increases the run complexity and implementation of the search method. Since it changes the equation system for every value of $(\Delta\text{in}, \Delta\text{out})$ and if the relationship between Δin and Δout is complicated, the matrix will be very large.

The idea of the UID method is that it represents the differential with symbols and utilizes the propagation property of the linear accumulated symbols. The idea of the Wu-Wang method is to utilize solving linear equations to determine an impossible differential. We show that the Wu-Wang method can be improved by combining the idea of the UID method and Wu-Wang method. Instead of using 1 to represent the nonzero difference, we use a letter symbol to represent a difference and different symbols represent different nonzero values. This method can represent more relationships between these subblocks. For example, if $\Delta\text{in} = (a, 0, 0, a)$ and $\Delta\text{out} = (a, 0, 0, b)$ for a 4-subblock structure where a and b are different nonzero values, then we have $x_1 = x_4 = y_1$ and $y_4 \neq x_1$. In our method, the matrix of the system does not need to be changed with $(\Delta\text{in}, \Delta\text{out})$. We also improve the Wu-Wang method by simplifying the test of whether there are solutions for linear systems. Since the most time consuming part is the matrix operation, our improved method can find more impossible differentials in less time.

We implement the method in java language and apply it to many block cipher structures, including Gen-CAST256 [15], Gen-Skipjack [23], Four-Cell [24], Gen-MARS [12], Gen-RC6 [23], SMS4 [14], Misty [25], MIBS [26], Camellia* [27], LBlock [28], E2 [29], and SNAKE [30] ones. For these block ciphers, we rediscover all known impossible differentials. Especially for the 8-round MIBS cipher, we find 4 new impossible differentials, which are not listed in Wu and Wang's work. Our improvement largely reduced the run time for finding impossible differentials. In [31], the results for MIBS, LBlock, and E2 are obtained in a few hours on a 2.66 GHz processor with MAGMA package. However, our results for MIBS, LBlock, and E2 are obtained within 10 seconds on a 2.20 GHz processor.

2. Preliminaries

In this section we introduce some basic concepts and notions used in this paper. We first introduce the block cipher structures. Next we review the solvability of a system of linear equations.

2.1. Block Cipher Structures. There are mainly two block cipher structures, which are the Feistel structure and its generalizations and the substitute permutation network (SPN). The round function of most of those structures consists of three basic operations: the sbox look-up, the exclusive-or addition (Xor), and the branch swapping, where the only nonlinear component is the sbox look-up operation. In differential cryptanalysis, the Xor differences of plaintext/ciphertext pairs are considered; we omit the key and constant addition since they have no relevance to our analysis. We assume that a block cipher structure has n subblocks (branches), and the input and output differences are denoted by $(\Delta x_1, \ldots, \Delta x_n)$ and $(\Delta y_1, \ldots, \Delta y_n)$, respectively.

2.2. The Solvability of a Linear System. Now we review the basics in linear algebra of determining the solvability of a system of linear equations. Let m, n be two positive integers, $m < n$; let $Ax = b$ be a system of m linear equations with n variables, where A is $m \times n$ matrix over $\mathbb{F}_2$; and $x = (x_1, \ldots, x_n)$ and $b = (b_1, \ldots, b_m)$ are two bit vectors; then the augmented $m \times (n + 1)$ matrix $B = [A \mid b]$ can determine the solvability of the linear system.

A regular method is to deduce the reduced row echelon form (a.k.a. row canonical form) of matrix B by Gauss-Jordan elimination algorithm. The reduced row echelon form of a matrix is unique and denoted by B'. One starts to check B' from the last row to the first, to see if there exists a row in which the first n entries are zeros and the last entry is nonzero. If there are such rows, then the linear system has no solution.

For example, if the augmented matrix B of a linear system in reduced row echelon form is

$$B' = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 0 & 1 & 0 & b_2 \\ 0 & 0 & 0 & b_3 \end{pmatrix}, \quad (1)$$

where b_3 is nonzero, then the linear system has no solution.

3. Mathematical Models for Finding IDs of Block Cipher Structures

Our improvement is based on Wu and Wang's method. If the nonlinear sbox S_i in a block cipher structure is a permutation, then there is a constraint on the input difference x_i and output difference y_i for S_i; that is, x_i and y_i can only both be zero or both be nonzero, denoted by $x_i \sim y_i$. The intermediate value of a block cipher structure is called the state. The state is updated with the round structure. In order to find impossible differential for an r-round block cipher structure, we first set differential variables for the states and then transform the r-round block cipher structure into a system of linear equations and constraints, denoted by $\mathcal{S}$. Then for a given differential $(\Delta\text{in}, \Delta\text{out})$, where $\Delta\text{in} = (a_1, \ldots, a_n)$ and $\Delta\text{out} = (b_1, \ldots, b_n)$, we can check if it is impossible by solving $\mathcal{S}$ with initial values $(a_1, \ldots, a_n, b_1, \ldots, b_n)$; if $\mathcal{S}$ has no solution, then $\Delta\text{in} \nrightarrow_r \Delta\text{out}$.

Here we take the 5-round Feistel structure as an example. We first assign differential variables for 5-round Feistel structure. In Figure 1, F_i, $1 \le i \le 5$ are permutations; the output difference of F_i for input difference X_i is Y_i; thus $X_i \sim Y_i$. According to the computation graph of 5-round Feistel structure, we obtain the following system $\mathcal{S}$ of equations and constraints:

$$\begin{aligned} X_0 \oplus X_2 \oplus Y_1 = 0, \quad & X_1 \sim Y_1, \\ X_1 \oplus X_3 \oplus Y_2 = 0, \quad & X_2 \sim Y_2, \\ X_2 \oplus X_4 \oplus Y_3 = 0, \quad & X_3 \sim Y_3, \\ X_3 \oplus X_5 \oplus Y_4 = 0, \quad & X_4 \sim Y_4, \\ X_4 \oplus X_6 \oplus Y_5 = 0, \quad & X_5 \sim Y_5. \end{aligned} \quad (2)$$

In order to check if $(a, 0) \to (a, 0)$ is an impossible differential where a is a nonzero value, we solve the above system with $X_0 = a$, $X_1 = 0$, $X_5 = 0$, and $X_6 = a$. Since $X_1 \sim Y_1$ and $X_5 \sim Y_5$ we have $Y_1 = 0$ and $Y_5 = 0$. From linear equations of $\mathcal{S}$, we get $Y_3 = 0$; thus $X_3 = 0$ since $X_3 \sim Y_3$; next from linear equations $\mathcal{S}$ we obtain $Y_2 = 0$; however $X_2 = a$ and $X_2 \sim Y_2$; thus the system $\mathcal{S}$ has no solution and $(a, 0) \to (a, 0)$ is an impossible differential for 5-round Feistel structure.

Now we want to find all impossible differentials for 5-round Feistel structure; we enumerate all the possible differential pairs $(\Delta\text{in}, \Delta\text{out}) \in \{(0, a), (a, 0), (a, a), (0, b), (b, 0), (b, b), (b, a), (a, b)\}$, where a and b are two different nonzero values. For each value of $(\Delta\text{in}, \Delta\text{out})$, we judge if it is an impossible differential; after all cases are tested, we will find all impossible differentials.

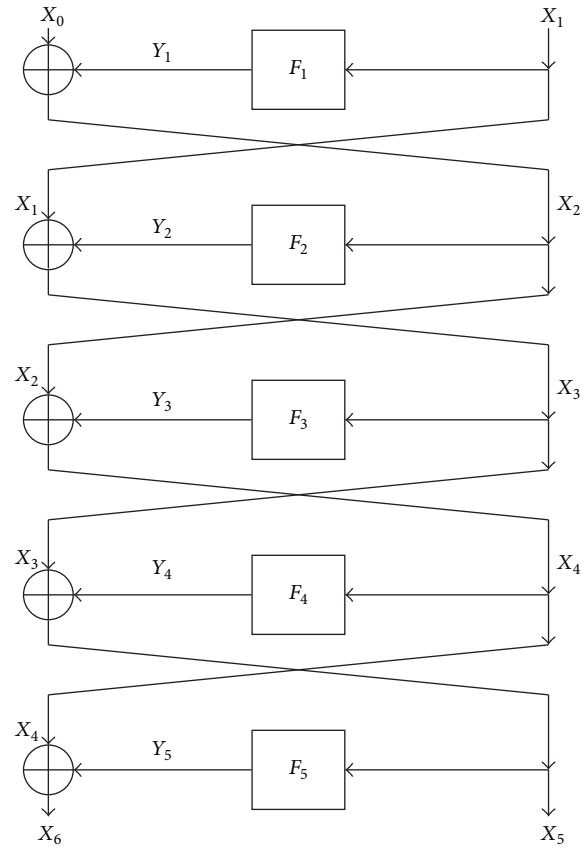

Figure 1: State variables for 5-round Feistel structure.

Thus the general algorithm for finding all r-round impossible differentials for a block cipher structure is outlined as follows:

(1) Generate all the possible differential pairs $(\Delta\text{in}, \Delta\text{out})$ in a set $\mathcal{D}$.

(2) Assign differential variables according to the computation figure of the r-round block cipher structure. Generate the system $\mathcal{S}$ of linear equations and constraints with the differential variables.

(3) For each $(\Delta\text{in}, \Delta\text{out}) \in \mathcal{D}$, solve the system $\mathcal{S}$ with initial value $(\Delta\text{in}, \Delta\text{out})$ and check if $\mathcal{S}$ has no solution. If there is no solution, then $(\Delta\text{in} \to \Delta\text{out})$ is an impossible differential. After all cases are checked we obtain all impossible differentials.

4. The Detailed Algorithm

In this section we describe the detailed algorithm and implementation details.

4.1. Generate All Possible Differential Pairs. We use symbols a_i, b_i, $1 \le i \le n$, to denote different $2n$ as the nonzero values. For a block cipher structure, the input difference is $(\Delta I_1, \ldots, \Delta I_n)$, where $\Delta I_i \in \{0, a_1, \ldots, a_n\}$, and the output difference is $(\Delta O_1, \ldots, \Delta O_n)$, where $\Delta O_i \in \{0, a_1, \ldots, a_n, b_1, \ldots, b_n\}$. Note that the input difference and output difference

Table 1: The 5×13 augmented matrix of 5-round Feistel structure.

	0	1	2	3	4	5	6	7	8	9	10	11	12
	X_0	X_1	X_2	X_3	X_4	X_5	X_6	Y_1	Y_2	Y_3	Y_4	Y_5	**0**
1	1	0	1	0	0	0	0	1	0	0	0	0	0
2	0	1	0	1	0	0	0	0	1	0	0	0	0
3	0	0	1	0	1	0	0	0	0	1	0	0	0
4	0	0	0	1	0	1	0	0	0	0	1	0	0
5	0	0	0	0	1	0	1	0	0	0	0	1	0

will not be zero since this will be trivial in differential cryptanalysis. Thus there are total $((n+1)^n - 1) \cdot ((2n+1)^n - 1)$ differential pairs. This value is large for many block cipher structures.

However, an impossible differential $(\Delta I_1, \ldots, \Delta I_n) \nrightarrow (\Delta O_1, \ldots, \Delta O_n)$ for a block cipher structure is usually simple; that is, there are very few nonzero values in $(\Delta I_1, \ldots, \Delta I_n)$ and $(\Delta O_1, \ldots, \Delta O_n)$. Since the input or output differential are complicate, it will propagate fast due to the round structure of the cipher. Thus it is reasonable to consider simple differential pairs. Actually all the impossible differentials found for block cipher structures in the literature are simple.

In this paper we only consider the input difference $(\Delta I_1, \ldots, \Delta I_n)$, where $\Delta I_i \in \{0, a\}$, and the output difference $(\Delta O_1, \ldots, \Delta O_n)$, where $\Delta O_i \in \{0, a, b\}$. Thus there are total $(2^n - 1)(3^n - 1)$ differential pairs that need to be checked.

4.2. Generate the System $\mathcal{S}$. Given a block cipher structure, we first need to draw the computational figure and assign differential variables, as introduced in the analysis of 5-round Feistel structure. This step is varying according to different block cipher structures. However, since most block cipher structures iterate the same round structure for several times, these variables are regular and easy to implement in a computer program. As in the analysis of 5-round Feistel structure, the input difference of a nonlinear permutation is denoted by variable X_i and the output difference is denoted by variable Y_i. Thus if we see a variable Y_i, it must be some output difference of a nonlinear permutation.

For a block cipher structure with r rounds, there are p variables X_i, $0 \le i \le p$, and q numbers of variables Y_i, $1 \le i \le q$. The numbers p and q are determined by the round structure and the round number r. For the r-round Feistel structure, $p = r + 2$ and $q = r$. We first denote all variables in a variable vector as

$$\overline{X} = \left(X_0, \ldots, X_{p-1}, Y_1, \ldots, Y_q\right), \tag{3}$$

and then linear equations in system $\mathcal{S}$ can be written as $M\overline{X} = \mathbf{0}$, where M is a $kr \times (p+q)$ matrix over F_2 and $\mathbf{0}$ is a $(p+q)$-dimensional zero vector, where k is the number of linear equations in one round of the block cipher structure. The augmented matrix of these linear equations is $B = [M \mid \mathbf{0}]$. For the 5-round Feistel structure, the augmented matrix B is denoted in Table 1.

The set of constraints in $\mathcal{S}$ can be maintained as a map $\mathcal{N}$. Let $\mathrm{id}(X_i)$ denote the index of the variable X_i in vector $\overline{X}$; given a constraint $X_i \sim Y_i$, we add $(\mathrm{id}(X_i), \mathrm{id}(Y_i))$ into the map $\mathcal{N}$. For the 5-round Feistel structure, $\mathcal{N} = \{\langle 1, 7\rangle, \langle 2, 8\rangle, \langle 3, 9\rangle, \langle 4, 10\rangle, \langle 5, 11\rangle\}$. In the real implementation, it is noted that, for most block cipher structures, the distance between constraints X_i and Y_i is fixed and determined by the round structure and the round number; that is, $\mathrm{id}(Y_i) - \mathrm{id}(X_i)$ is a constant. For example, the distance of constraints X_i and Y_i for a r-round Feistel structure is $r+1$. Thus the map $\mathcal{N}$ is not needed to be implemented but only the fixed index distance is needed. This observation facilitates the real implementation of the algorithm.

4.3. Determine the Solvability of $\mathcal{S}$. In the beginning, we assign a symbol "?" to each variable in the variable vector $\overline{X}$, which means every variable is undetermined. Given a differential pair $(\Delta\mathrm{in}, \Delta\mathrm{out})$, we need to check if there exist solutions of the system $\mathcal{S}$ with the initial value $(\Delta\mathrm{in}, \Delta\mathrm{out})$. We first need to initialize the variable vector $\overline{X}$ according to $(\Delta\mathrm{in}, \Delta\mathrm{out})$. As in the 5-round Feistel structure, for a differential pair $\Delta\mathrm{in} = (a, 0)$, $\Delta\mathrm{out} = (a, 0)$, the variable vector $\overline{X}$ is initialized as follows:

X_0	X_1	X_2	X_3	X_4	X_5	X_6	Y_1	Y_2	Y_3	Y_4	Y_5
a	0	?	?	?	0	a	?	?	?	?	?

For a constraint $X_i \sim Y_i$, the algorithm updates (X_i, Y_i) and detects contradictions as follows.

(i) The value X_i is updated:

  (a) If $X_i = 0$ and $Y_i = ?$, then Y_i is set to 0.
  (b) If X_i is a nonzero symbol and $Y_i = ?$, then Y_i is set to the nonzero symbol "$*$."
  (c) If $X_i = 0$ and Y_i is an nonzero symbol, then we obtain a contradiction.

(ii) The value Y_i is updated:

  (a) If $Y_i = 0$ and $X_i = ?$, then X_i is set to 0.
  (b) If $Y_i = 0$ and X_i is an nonzero symbol, then we obtain a contradiction.

We use $\oplus$ to denote the symmetrical difference (Xor) of X_1 and X_2. For example, if $X_1 = \{a_1\}$ and $X_2 = \{b_1\}$, then $X_1 \oplus X_2 = \{a_1, b_1\}$; if $X_1 = \{a_1\}$ and $X_2 = \{0\}$, then $X_1 \oplus X_2 = \{a_1\}$; if $X_1 = \{a_1\}$ and $X_2 = \{a_1, b_1\}$, then $X_1 \oplus X_2 = \{b_1\}$.

The function $\mathsf{UpdateMatrix}(B, \overline{X})$ updates the augmented matrix B according to the variable vector $\overline{X}$. If the ith variable in $\overline{X}$ is 0, then the corresponding ith column of B is set to a zero vector. As in [21], this method keeps solutions

```
// Update the augmented matrix B according to the variable vector X
(1) K ← the size of X;
(2) for i ← 0 to K − 1 do
(3)     t ← X[i];
(4)     if t is 0 then
(5)         Every element of the ith column of B is set to 0.
(6)     else if t is not "?" and t is not "∗" then
(7)         L ← the number of rows of B;
(8)         for r ← 0 to L − 1 do
(9)             if B[r, i] is 1 then
(10)                B[r, i] ← 0;
(11)                B[r, K − 1] ← B[r, K − 1] ⊕ t;
(12)            end
(13)        end
(14)    end
(15) end
```

Algorithm 1: Function UpdateMatrix($B, \overline{X}$).

of the augmented matrix B unchanged. If $\overline{X}_i$ is not in the set $\{0, ?, *\}$, we check each row of B; if the value of the ith column at the rth row $B_{r,i}$ is 1, then we set Xor $\overline{X}_i$ to the last element of the rth row of B and set $B_{r,i}$ to 0 (Algorithm 1).

The function UpdateVector($\overline{X}, \mathcal{N}, j, J$) updates the jth variable $\overline{X}_j$ with the value J; at the same time all constraints in $\mathcal{N}$ are maintained. As described in the beginning of this subsection, the function updates $\overline{X}_j$ with the value J by checking each constraint in $\mathcal{N}$ and returns true if it succeeds or false if there is a contradiction. There are many subcases, as described in the detailed algorithm. During the updating process, there may be contradictions. For example, if $\overline{X}_j = \{a\}$ and $J = \{a, b\}$ which means $J = a \oplus b$, there is a contradiction since $a \oplus b$ can never be a. If J is $\{0\}$ but the corresponding variable which is the sbox output of $\overline{X}_j$ is nonzero or J is $\{0\}$ but the corresponding variable which is the sbox input of $\overline{X}_j$ is nonzero, there will be contradictions (Algorithm 2).

The function ReducedRowEchelon(B) transforms the $\iota \times \kappa$ matrix B into the reduced row echelon form by Gauss-Elimination algorithm. Note that every element in the first $\kappa - 1$ columns of B is in $\mathbb{F}_2$, while elements in the last column of B are represented by a set of symbols. Thus the Xor operation in the last column of B is the symmetrical difference operation. The readers can refer to [32] for the detailed algorithm of transforming a matrix into the reduced row echelon form.

The detailed algorithm for checking if a differential is impossible is described in Algorithm 3. In Algorithm 3, the variable vector $\overline{X}$ is first initialized according to the differential pair $(\Delta\text{in}, \Delta\text{out})$ and the constraint array $\mathcal{N}$. Then the algorithm continues checks if there is a contradiction with a loop test until B and $\overline{X}$ are not updated any more. During the loop the algorithm first updates B according to $\overline{X}$ by the UpdateMatrix($B, \overline{X}$) function and then transforms B into the reduced row echelon form by the ReducedRowEchelon(B) function to see if B has solutions. If B has no solutions, the algorithm obtains a contradiction and stops. Otherwise if there exists a solution for a variable from the reduced row echelon form, the index and the value of the variable are denoted as (j, J). The algorithm updates the variable vector $\overline{X}$ with (j, J) by the UpdateVector($\overline{X}, \mathcal{N}, j, J$) function; if the updating process returns false, a contradiction is obtained and the algorithm stops; otherwise, the algorithm continues to run.

4.4. Complexity. For the $\iota \times \kappa$ matrix B and the $\kappa - 1$ dimension vector $\overline{X}$, the time complexity of the function UpdateMatrix is $\iota \cdot \kappa$, the time complexity of the function ReducedRowEchelon is $\iota^2 \cdot \kappa$, and the time complexity of the function UpdateVector is a constant c, while loop continues running $\kappa/2$ times since there at most $\kappa - 1$ values in $\overline{X}$ and in each loop either 2 variables are updated or there is a contradiction. Thus the total complexity of the algorithm is $(c/2) \cdot \iota^2\kappa^2$, where c is a small constant. The space complexity is dominated by storing the matrix B and is about $\iota \cdot \kappa$. The time complexity of the Wu-Wang method is $T \cdot \iota^2\kappa^2$ and this T is much larger than our c. The Wu-Wang method stores 3 matrices; thus its space complexity is at least triple our method.

4.5. Comparison with Previous Method. In [31], Wu and Wang proved that the $\mathcal{U}$-method and the UID method are specific cases of the Wu-Wang method. They found that their method can find longer impossible differential for the MIBS cipher than by $\mathcal{U}$-method and the UID method. However, in the UID method, for an impossible differential pair $((\Delta I_1, \ldots, \Delta I_n), (\Delta O_1, \ldots, \Delta O_n))$, the relationship between input variables and output variables is considered since UID method uses symbols to denote values. For example, the UID method considers the relation between ΔI_i and ΔO_j and checks if they are equal; however the $\mathcal{U}$-method and Wu-Wang method only use 0 and 1 to denote zero and nonzero

```
// Update the variable vector X̄ according to the variable (j, J) where J is the value
   of the jth variable in X̄. 𝒩 is the array of constraints.
input: the variable vector X̄, the constraint array 𝒩, (j, J).
output: A boolean flag indicates if the update procedure success.
(1) flag ←true;
(2) foreach a ∈ 𝒩 do
(3)     k0 ← a[0]; k1 ← a[1];
(4)     if j is equal to k0 then
(5)         if J ⊕ X̄_k0 is not 0 then
(6)             flag ←false; // Ex. J = a ⊕ b but X̄_k0 = a, a contradiction.
(7)             return flag;
(8)         else if J is 0 and X̄_k0 is ? then
(9)             if X̄[k1] is not 0 then flag ←false;
(10)                return flag;
(11)            end
(12)            X̄_k0 ← 0; X̄_k1 ← 0;
(13)        else if J is a nonzero value then
(14)            X̄_k0 ← J; X̄_k1 ← *;
(15)        end
(16)    else if j is equal to k1 then
(17)        if J ⊕ X̄_k1 is not 0 then flag ←false
(18)            return flag;
(19)        else if X̄_k1 is ? and J is 0 then
(20)            X̄_k1 ← 0; X̄_k0 ← 0;
(21)        end
(22)    end
(23) end
(24) return flag;
```

Algorithm 2: Function UpdateVector($\overline{X}, \mathcal{N}, j, J$).

values, which omit the relationship between input and output differentials.

Our improved method combines the advantages of the UID method and Wu-Wang method. Every impossible differential found by the UID method and Wu-Wang method can be found by our improved method. As Wu and Wang's method, impossible differentials found by our improved method must be correct if the algorithm is implemented correctly. Compared with Wu and Wang's method, our improved method is more complete. The symbol representation of a difference can represent more relationships between different difference values. Thus it can find more impossible differentials and the matrix B does not change with different values of (Δin, Δout) in the beginning of the algorithm, while, in the Wu-Wang method, to add linear relationships between nonzero values in (Δin, Δout), the matrix B must change with different values of (Δin, Δout). This will consume more time during the run of the algorithm.

The most time consuming part in the algorithm is the matrix operation. To check if the augmented matrix has any solutions, the Wu-Wang method needs to compute the rank of the matrices M and B. We show that this step is not required since we can check the solvability of the system from the reduced row echelon form of the matrix B, as introduced in the preliminaries section. Thus our improvement largely reduces the search time of finding impossible differentials of a block cipher structure.

5. Applications and Experiment Results

We implement the algorithm in java language and apply it to many block cipher structures, including Gen-CAST256 [33], Misty [25], Gen-Skipjack [23], Four-Cell [24], Gen-MARS [33], Gen-RC6 [33], SMS4 [34], MIBS [26], Camellia* [27, 31], LBlock [28], E2 [29], and SNAKE [30]. We present the java code of this algorithm and complete impossible differential results in GitHub [35]. To reduce the space of this paper, we present some of the impossible differential results in Table 2. The file *Impossible Differential.txt* in [35] lists the complete impossible differential results for these block cipher structures. Most impossible differentials discovered by our algorithm are the same as the Wu-Wang method.

Moreover, for the 8-round MIBS, we find new 4 impossible differentials, which are not found by the Wu-Wang method since these 4 new impossible differentials are not simple truncated impossible differentials. MIBS is a 16-subblock Feistel structure with substitution and permutation

input: A differential pair (Δin, Δout) and the system $\mathcal{S}$
output: A boolean flag indicates if (Δin, Δout) is an impossible differential
(1) B is the $\iota \times \kappa$ augmented matrix of $\mathcal{S}$;
(2) $\overline{X}$ is the $\kappa - 1$ dimension variable vector;
(3) $\mathcal{N}$ is the map of constraints of $\mathcal{S}$;
(4) flag←false;
(5) index←true;
(6) Initialize every variable in $\overline{X}$ according to (Δin, Δout) and the constraints in $\mathcal{N}$;
(7) **while** *index* **do**
(8) `UpdateMatrix` (B, $\overline{X}$) `// Update` B `according to` $\overline{X}$;
`/* Transform` B `into the reduced-row-echelon form by Gauss-Jordan Elimination */`
(9) `ReducedRowEchelon` (B);
(10) **if** B has no solution **then**
(11) flag←true;
(12) break;
(13) **else**
(14) index ← false;
(15) count← 0;
(16) **for** $i \leftarrow \iota$ **to** 1 **do**
(17) $\overrightarrow{v} \leftarrow$ Row i of B;
(18) **if** the sum of the first $\kappa - 1$ elements of $\overrightarrow{v}$ is 1 **then**
(19) $j \leftarrow$ the index of the element 1 in $\overrightarrow{v}$;
(20) $J \leftarrow$ the last element of $\overrightarrow{v}$; `//` the solution of the jth variable in $\overline{X}$
(21) `/*` update the variable vector $\overline{X}$ with (j, J) and return true if there is no contradiction and return false otherwise. `*/`
(22) $b \leftarrow$`UpdateVector` ($\overline{X}$, $\mathcal{N}$, j, J);
(23) **if** b is false **then**
(24) flag ← true;
(25) **return** flag;
(26) **else**
(27) index ← true;
(28) **end**
(29) **end**
(30) **end**
(31) **end**
(32) **end**
(33) **return** *flag*;

Algorithm 3: The algorithm for checking an impossible differential.

Table 2: Summary of impossible differentials (IDs) of some well-known block ciphers structures found by different methods.

Block cipher	UID [14]	Wu-Wang [31]	This paper
Gen-Skipjack	16: $(0,0,0,a) \nrightarrow_{16} (b,0,0,b)$	—	Same as UID
Gen-CAST256	19: $(0,0,0,a) \nrightarrow_{19} (a,0,0,0)$	—	Same as UID
Four-Cell	18: $(a,0,0,0) \nrightarrow_{18} (b,b,0,0)$	—	Same as UID
Gen-MARS	11: $(0,0,0,a) \nrightarrow_{11} (a,0,0,0)$	—	Same as UID
Gen-RC6	9: $(0,0,a,0) \nrightarrow_{9} (0,a,0,0)$ 9: $(a,0,0,0) \nrightarrow_{9} (0,0,0,a)$	—	Same as UID
SMS4	11: $(0,0,0,a) \nrightarrow_{11} (a,0,0,0)$	—	Same as UID
Misty	—	—	$4 : (0,a) \nrightarrow_{4} (b,b)$
SNAKE	—	—	$11 : (0,0,0,0,0,0,a,0) \nrightarrow_{11} (0,0,b,0,0,0,0,0)$
Camellia*	—	8-round, 4 IDs	Same as Wu-Wang
MIBS	—	8-round, 6 IDs	8-round, 10 IDs
LBlock	—	14-round, 80 IDs	Same as Wu-Wang
E2	—	6-round, 56 IDs	Same as Wu-Wang

Table 3: Impossible differentials for 8-round MIBS. There are 4 new found impossible differentials. a and b are nonzero values and a and b can have the same value.

Number	Δin	Δout	Reference
1	$(0,0,0,0,0,0,0,0;0,0,0,0,0,0,a,0,0)$	$(b,0,0,0,0,0,0,b;0,0,0,0,0,0,0,0)$	This paper
2	$(0,0,0,0,0,0,0,0;0,0,0,0,0,0,a,0,0)$	$(0,0,0,0,b,0,0,b;0,0,0,0,0,0,0,0)$	
3	$(0,0,0,0,0,0,0,0;a,0,0,0,0,0,0,a)$	$(0,0,0,0,0,b,0,0;0,0,0,0,0,0,0,0)$	
4	$(0,0,0,0,0,0,0,0;0,0,0,0,0,a,0,0,a)$	$(0,0,0,0,0,b,0,0;0,0,0,0,0,0,0,0)$	
5	$(0,0,0,0,0,0,0,0;0,0,a,0,0,0,0,0)$	$(0,0,0,0,b,0,0,0;0,0,0,0,0,0,0,0)$	[31]
6	$(0,0,0,0,0,0,0,0;0,0,a,0,0,0,0,0)$	$(0,0,0,0,0,0,0,b;0,0,0,0,0,0,0,0)$	
7	$(0,0,0,0,0,0,0,0;0,0,0,0,0,a,0,0,0)$	$(0,0,b,0,0,0,0,0;0,0,0,0,0,0,0,0)$	
8	$(0,0,0,0,0,0,0,0;0,0,0,0,0,a,0,0,0)$	$(0,0,0,0,0,0,b,0;0,0,0,0,0,0,0,0)$	
9	$(0,0,0,0,0,0,0,0;0,0,0,0,0,0,0,a,0)$	$(0,0,0,0,b,0,0,0;0,0,0,0,0,0,0,0)$	
10	$(0,0,0,0,0,0,0,0;0,0,0,0,0,0,0,0,a)$	$(0,0,b,0,0,0,0,0;0,0,0,0,0,0,0,0)$	

(SP) round function. In the SP round function, the 8 subblocks are first substituted by 8 sboxes; then an 8×8 matrix is applied as the permutation. The permutation matrix P is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}. \quad (4)$$

There are total 10 impossible differentials found for 8-round MIBS by our improved algorithm. The new four 8-round impossible differentials found are listed in Table 3.

Compare with Wu and Wang's algorithm, this improvement is more general since it not only finds more impossible differentials for a block cipher structures, but also has better efficiency. The results for MIBS are obtained on a 2.66 GHz processor with MAGMA package in a few hours by Wu and Wang's algorithm [31]. However, our results for MIBS are obtained on a 2.20 GHz processor in java language in less than 10 seconds. Thus, the algorithm presented in this paper is more efficient than Wu and Wang's algorithm.

6. Conclusion

In this paper we improve Wu and Wang's algorithm for finding impossible differentials of block cipher structures. The improved method is more general than Wu and Wang's method where it can find more impossible differentials with less time. We apply this method to many block cipher structures. The experiment results show that this improvement can largely reduce the search time for the impossible differentials of a block cipher, since there are known relationships between impossible differential and integral and zero correlation linear cryptanalysis [22, 36, 37]. This method can be used as a cryptanalytic tool to evaluate the security of a block cipher against these kinds of cryptanalysis.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Yiyuan Luo was supported by NSFC (61402280) and Academic Discipline Project of Shanghai Dianji University (16YSXK04). Xuejia Lai was supported by NSFC (61272440, 61472251, and U1536101), China Postdoctoral Science Foundation (2013M531174, 2014T70417), National Cryptography Development Fund MMJJ20170105, and Science and Technology on Communication Security Laboratory.

References

[1] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 18, no. 4, pp. 291–311, 2005.

[2] L. R. Knudsen, "DEAL-A 128-bit block cipher," Tech. Rep. 151, Department of Informatics, University of Bergen, 1998.

[3] R. Zong, X. Dong, and X. Wang, "Impossible Differential Attack on Simpira v2," *Science China Information Sciences*, 2017.

[4] L. Cheng, B. Sun, and C. Li, "Revised cryptanalysis for sms4," *Science China Information Sciences*, vol. 60, no. 12, article 122101, 2017.

[5] Y. Dai and S. Chen, "Cryptanalysis of full PRIDE block cipher," *Science China. Information Sciences*, vol. 60, no. 5, 052108, 12 pages, 2017.

[6] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," *Science China Information Sciences*, pp. 1–15, 2015.

[7] G.-Q. Liu and C.-H. Jin, "Algebraic techniques in slender-set differential cryptanalysis of PRESENT-like cipher," *Science China Information Sciences*, vol. 59, no. 9, Article ID 99104, 2016.

[8] T. Lin, X. Lai, W. Xue, and G. Huang, "Discussion on the theoretical results of white-box cryptography," *Science China Information Sciences*, vol. 59, no. 11, Article ID 112101, 2016.

[9] Y. Ding, J. Zhao, L. Li, and H. Yu, "Impossible differential analysis on round-reduced PRINCE," *Journal of Information Science and Engineering*, vol. 33, no. 4, pp. 1041–1053, 2017.

[10] W. Wu, L. Zhang, and X. Yu, "The DBlock family of block ciphers," *Science China Information Sciences*, vol. 58, no. 3, 2015.

[11] C. Boura, M. a. Naya-Plasencia, and V. Suder, "Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon," in *Advances in cryptology—ASIACRYPT 2014. Part I*, vol. 8873 of *Lecture Notes in Comput. Sci.*, pp. 179–199, Springer, Berlin, Germany, 2014.

[12] J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung, "Impossible differential cryptanalysis for block cipher structures," in *Progress in cryptology—INDOCRYPT 2003*, vol. 2904 of *Lecture Notes in Comput. Sci.*, pp. 82–96, Springer, Berlin, Germany, 2003.

[13] J. Kim, S. Hong, and J. Lim, "Impossible differential cryptanalysis using matrix method," *Discrete Mathematics*, vol. 310, no. 5, pp. 988–1002, 2010.

[14] Y. Luo, X. Lai, Z. Wu, and G. Gong, "A unified method for finding impossible differentials of block cipher structures," *Information Sciences*, vol. 263, pp. 211–220, 2014.

[15] H. Yap, "Impossible differential characteristics of extended feistel networks with provable security against differential cryptanalysis," *Communications in Computer and Information Science*, vol. 29, pp. 103–121, 2009.

[16] G. Liu, C. Jin, and Z. Kong, "Key recovery attack for PRESENT using slender-set linear cryptanalysis," *Science China Information Sciences*, vol. 59, no. 3, Article ID 32110, 2016.

[17] R. Zhao, R. Zhang, Y. Li, and B. Wu, "Construction of MDS block diffusion matrices for block ciphers and hash functions," *Science China. Information Sciences*, vol. 59, no. 9, Article ID 99101, 099101, 3 pages, 2016.

[18] T. P. Berger, M. Minier, and G. Thomas, "Extended generalized Feistel networks using matrix representation," in *Selected areas in cryptography—SAC 2013*, vol. 8282 of *Lecture Notes in Comput. Sci.*, pp. 289–305, Springer, Berlin, Germany, 2014.

[19] T. P. Berger and M. Minier, "Some results using the matrix methods on impossible, integral and zero-correlation distinguishers for Feistel-like ciphers," in *Progress in cryptology—INDOCRYPT 2015*, vol. 9462 of *Lecture Notes in Comput. Sci.*, pp. 180–197, Springer, 2015.

[20] C. Blondeau and M. Minier, "Analysis of impossible, integral and zero-correlation attacks on type-II generalized feistel networks using the matrix method," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9054, pp. 92–113, 2015.

[21] S. Wu and M. Wang, "Automatic search of truncated impossible differentials for word-oriented block ciphers," in *Progress in cryptology—INDOCRYPT 2012*, vol. 7668 of *Lecture Notes in Comput. Sci.*, pp. 283–302, Springer, Heidelberg, 2012.

[22] B. Sun, Z. Liu, V. Rijmen et al., "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *Advances in cryptology—CRYPTO 2015. Part I*, vol. 9215 of *Lecture Notes in Comput. Sci.*, pp. 95–115, Springer, Berlin, Germany, 2015.

[23] J. Sung, S. Lee, J. Lim, S. Hong, and S. Park, "Provable security for the Skipjack-like structure against differential cryptanalysis and linear cryptanalysis," in *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, vol. 1976 of *Lecture Notes in Comput. Sci.*, pp. 274–288, Springer, Berlin, Germany, 2000.

[24] J. Choy, G. Chew, K. Khoo, and H. Yap, "Cryptographic properties and application of a generalized unbalanced feistel network structure," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5594, pp. 73–89, 2009.

[25] M. Matsui, "New block encryption algorithm MISTY," in *Fast Software Encryption*, vol. 1267 of *Lecture Notes in Computer Science*, pp. 54–68, Springer-Verlag, 1997.

[26] M. Izadi, B. Sadeghiyan, S. S. Sadeghian, and H. A. Khanooki, "MIBS: A new lightweight block cipher," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5888, pp. 334–348, 2009.

[27] K. Aoki, T. Ichikawa, M. Kanda et al., "Camellia: a 128-bit block cipher suitable for multiple platforms—design and analysis," in *Selected areas in cryptography (Waterloo, ON, 2000)*, vol. 2012 of *Lecture Notes in Comput. Sci.*, pp. 39–56, Springer, Berlin, Germany, 2001.

[28] W. Wu and L. Zhang, "LBlock: A lightweight block cipher," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6715, pp. 327–344, 2011.

[29] M. Kanda, S. Moriai, K. Aoki et al., "E2-A new 128-bit block cipher," *IEICE Transactions Fundamentals - Special Section on Cryptography and Information Security*, vol. E83-A, no. 1, pp. 48–59, 2000.

[30] C. Lee and Y. Cha, "The block cipher: SNAKE with provable resistance against DC and LC attacks," in *JW-ISC 1997*, pp. 3–17, 1997.

[31] S. Wu and M. Wang, "Automatic search of truncated impossible differentials for word-oriented block ciphers," http://eprint.iacr.org/2012/214.pdf.

[32] RosettacodeOrg. How to compute the reduced row echelon form of a matrix. http://rosettacode.org/wiki/Reduced_row_echelon_form.

[33] S. Moriai and S. Vaudenay, "On the pseudorandomness of top-level schemes of block ciphers," in *Advances in cryptology—ASIACRYPT 2000 (Kyoto)*, vol. 1976 of *Lecture Notes in Comput. Sci.*, pp. 289–302, Springer, Berlin, Germany, 2000.

[34] SMS4. Specication of SMS4, block cipher for WLAN products SMS4. Avaiable at: http://www.oscca.gov.cn/UpFile/200621016-423197990.pdf.

[35] Y. Luo, Source codes and results for finding impossible differentials for block cipher structures. https://github.com/ianroo/impossibledifferential.

[36] A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. Steinberger, and E. Tischhauser, "Key-alternating ciphers in a provable setting: encryption using a small number of public permutations (extended abstract)," in *Advances in cryptology—EUROCRYPT 2012*, vol. 7237 of *Lecture Notes in Comput. Sci.*, pp. 45–62, Springer, Berlin, Germany, 2012.

[37] C. Blondeau, A. Bogdanov, and M. Wang, "On the (in)equivalence of impossible differential and zero-correlation distinguishers for Feistel- and Skipjack-type ciphers," in *Applied Cryptography and Network Security*, vol. 8479 of *Lecture Notes in Computer Science*, pp. 271–288, Springer-Verlag, 2014.