Impossible Differential Cryptanalysis on ESF Algorithm with Simplified MILP Model

Xiaonian Wu[1*], Jiaxu Yan[1], Lingchen Li[1], Runlian Zhang[1], Pinghai Yuan[2] and Yujue Wang[3]
[1] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology
Guilin, 541004, China
[e-mail: xnwu@guet.edu.cn, yjx_0629@163.com, llc0208@guet.edu.cn, zhangrl@guet.edu.cn]
[2] School of Computing, National University of Singapore
117417, Singapore
[e-mail: dcsyp@nus.edu.sg]
[3] Hangzhou Innovation Institute, Beihang University
Hangzhou, 310052, China
[e-mail: yjwang@guet.edu.cn]
[*] Corresponding Author: Xiaonian Wu

Received March 31, 2021; revised August 4, 2021; accepted September 21, 2021; published October 31, 2021

Abstract

MILP-based automatic search is the most common method in analyzing the security of cryptographic algorithms. However, this method brings many issues such as low efficiency due to the large size of the model, and the difficulty in finding the contradiction of the impossible differential distinguisher. To analyze the security of ESF algorithm, this paper introduces a simplified MILP-based search model of the differential distinguisher by reducing constrains of XOR and S-box operations, and variables by combining cyclic shift with its adjacent operations. Also, a new method to find contradictions of the impossible differential distinguisher is proposed by introducing temporary variables, which can avoid wrong and miss selection of contradictions. Based on a 9-round impossible differential distinguisher, 15-round attack of ESF can be achieved by extending forward and backward 3-round in single-key setting. Compared with existing results, the exact lower bound of differential active S-boxes in single-key setting for 10-round ESF are improved. Also, 2108 9-round impossible differential distinguishers in single-key setting and 14 12-round impossible differential distinguishers in related-key setting are obtained. Especially, the round of the discovered impossible differential distinguisher in related-key setting is the highest, and compared with the previous results, this attack achieves the highest round number in single-key setting.

Keywords: ESF, MILP, related-key attack, differential active S-box, impossible differential distinguisher

1. Introduction

With the rapid development of Internet technology, information security becomes increasingly important in realizing secure and reliable systems. To this end, many security mechanisms are designed and widely used, such as message authentication [1], communication encryption, and Blockchain [2]. Among the above security technologies, cryptographic algorithm is the cornerstone and dominates the security of the whole system. In recent years, low-power devices have been widely used in real world applications as the rapid development of radio frequency identification (RFID) [3] technology and wireless sensor networks (WSN). With many advantages such as high efficiency, low power consumption and less resource requirements, lightweight block ciphers can be easily implemented in hardware and software. Thus, it can provide security guarantee for Internet of Things (IoT) [4] and resource-constrained environments. At present, many lightweight block ciphers have been proposed, for example, PRESENT [5], LBlock [6], LED [7], Midori [8], GIFT [9], SKINNY [10]. However, there remains a big concern that whether these lightweight block ciphers can resist classic attacks and provide security protection in resource-constrained environments.

The classical cryptanalysis methods include differential cryptanalysis, linear cryptanalysis, related-key analysis, side channel attack and differential fault analysis [11], where differential cryptanalysis and linear cryptanalysis are two most basic cryptanalysis methods. The key for differential analysis is to find a high-probability differential characteristic, and the estimation on the maximum differential characteristic probability can be calculated according to the lower bound of differential active S-box. Impossible differential analysis was independently proposed by Knudsen [12] and Biham [13] from the differential analysis technology. The key of impossible differential analysis is to construct an impossible differential distinguisher to obtain the correct key using the differential with zero probability to filter out wrong keys. The related-key analysis was proposed by Knudsen [14] and Biham [15] independently, which can deduce some information of keys based on the relations of round keys. In order to efficiently find the distinguisher of higher round, many automated search methods have been proposed, where the mixed integer linear programming (MILP) technology is widely used in block cipher analysis. In 2011, Mouha et al. [16] first converted the searching problem for the minimum number of active S-boxes into a MILP problem, which was applied to the word-oriented block ciphers. Then Sun et al. [17] extended the application of MILP to bit-oriented block ciphers, such that the differential characteristic in single-key setting and related-key setting on SIMON48, LBlock, DESL and PRESENT-128 were obtained. Cui et al. [18] constructed the MILP model for impossible difference and zero correlation linear approximation based on existed methods, and proposed a verification algorithm for the searched results. In Eurocrypt 2017, Sasaki et al. [19] proposed an impossible differential search tool for 8-bit S-boxes, as well as a new algorithm for describing S-boxes with less constraint inequalities [20].

Eight-Sided Fortress (ESF) is a lightweight block cipher based on LBlock [21]. In order to achieve faster diffusion and improved security, ESF employs the idea of permutation layer in PRESENT and replaces the nibble replacement method in the LBlock with bit-by-bit replacement method. This paper mainly focuses on analyzing the security of ESF, where the MILP method is employed to automatically search for differential active S-boxes and impossible differential distinguishers. However, there are many problems for the MILP model, such as a large number of constraints, low efficiency of solution finding and difficulty of

verifying impossible difference results.

In this paper, we propose a simplified MILP-based differential distinguisher search model and an improved method to find contradictions of impossible differential distinguishers. Also, the key recovery of ESF is implemented. The contribution of this paper is summarized as follows:

1) With the search model proposed by Sasaki, this paper builds a simplified MILP-based differential distinguisher search model by reducing the number of XOR and S-box operations as well as the number of constraints and variables under the combination of cyclic shift with adjacent operations.
2) For the impossible differential distinguishers verification algorithm proposed by Cui et al., a different method is proposed to find contradictions by indirect transmission of temporary variables, which replaces the direct transmission between the upper and lower rounds.
3) The tested results show that in single-key setting, the more accurate number of lower bounds of 11-round ESF differential active S-box is 14, compared to 10 in related-key setting. Also, 2108 9-round impossible differential distinguishers in single-key setting and 14 12-round impossible differential distinguishers in related-key setting are obtained. The improved verification algorithm is used to find the corresponding contradictions for the obtained impossible differential distinguishers, in this way the searched distinguishers can be verified.
4) With the searched impossible differential distinguishers, 15 rounds of ESF are analyzed, and the data and time complexity of the impossible differential attack in single-key setting are also improved. Specifically, the data complexity is $2^{60.45}$ and the time complexity is $2^{70.02}$.

The rest of the paper is organized as follows. Section 2 mainly introduces the notations and ESF cipher. In section 3, we introduce the basic MILP model and the verification method of the impossible differential distinguisher, and propose an improved MILP model and an improved verification method. In section 4, the exact lower bounds of differential active S-boxes and impossible differential distinguisher of ESF are given, and key recovery of ESF is implemented. The security analysis results are compared in section 5. At last, section 6 concludes the paper.

2. Preliminaries

2.1 Notations

M : 64-bit plaintext

C : 64-bit ciphertext

L_i : The i-th left branch of 32-bit

R_i : The i-th right branch of 32-bit

F : Round function

K : 80-bit master key

RK_i : 32-bit subkey

P : Bit permutation

$||$: Character concatenation

$<<<i$: Left rotation of i-bit

$[i]_2$: Binary representation of i

$\oplus$: Xor

2.2 Description of ESF

ESF is a lightweight block cipher, which adopts the design principles of LBlock and the idea of bit permutation in the linear layer of PRESENT to achieve faster diffusion. As shown in **Fig. 1**, ESF has a 32-round Feistel structure with 64-bit block size and 80-bit key size.

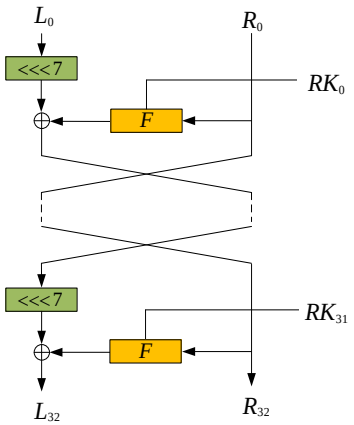

Fig. 1. The structure of ESF

Let L_i and R_i (i=0,1,…,31) respectively be the left and right branches of ESF, $C_i=L_i \,||\, R_i$ be the input for i-th round, $C_{i+1}=L_{i+1} \,||\, R_{i+1}$ be the output, and RK_i be the round key. The update process from (L_i, R_i) to (L_{i+1}, R_{i+1}) is shown as follows:

$$\begin{cases} C_i = L_i \,||\, R_i \\ R_{i+1} = (L_i <<< 7) \oplus F(R_i, RK_i) \\ L_{i+1} = R_i \end{cases} \tag{1}$$

As shown in **Fig. 2**, the round function F of ESF employs the SPN structure, where each round includes a Substitution Layer (S-box_layer), a Permutation Layer (P_Layer), and a Round Key.

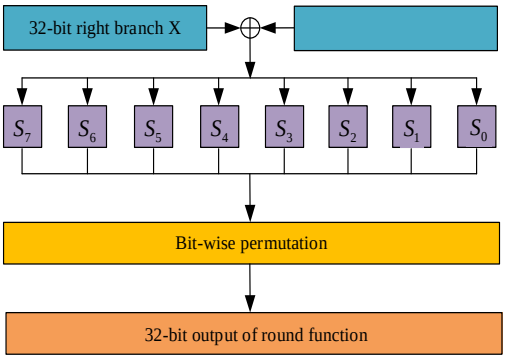

Fig. 2. The round function of ESF

S-box_Layer. ESF uses 8 different 4-bit S−boxes in parallel, which are shown in **Table 1** in hexadecimal.

Table 1. The S-Boxes of ESF

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S_0[x]$	3	8	f	1	a	6	5	b	e	d	4	2	7	0	9	c
$S_1[x]$	f	c	2	7	9	0	5	a	1	b	e	8	6	d	3	4
$S_2[x]$	8	6	7	9	3	c	a	f	d	1	e	4	0	b	5	2
$S_3[x]$	0	f	b	8	c	9	6	3	d	1	2	4	a	7	5	e
$S_4[x]$	1	f	8	3	c	0	b	6	2	5	4	a	9	e	7	d
$S_5[x]$	f	5	2	b	4	a	9	c	0	3	e	8	d	6	7	1
$S_6[x]$	7	2	c	5	8	4	6	b	e	9	1	f	d	3	a	0
$S_7[x]$	1	d	f	0	e	8	2	b	7	4	c	a	9	3	5	6

Permutation Layer P. ESF uses the following method to realize permutation from $(b_{31}\|b_{30}\|...\|b_1\|b_0)$ to $(c_{31}\|c_{30}\|...\|c_1\|c_0)$:

$$b_{4j}\|b_{4j+1}\|b_{4j+2}\|b_{4j+3}\rightarrow c_j\|c_{j+8}\|c_{j+16}\|c_{j+24},\ \ j=0,1,\ldots,7 \tag{2}$$

Key schedule. In order to reduce hardware implementation area and increase the key loading speed, the design of key schedule is simple. Suppose the 80-bit master key is denoted as $K=k_{79}k_{78}k_{77}...k_2k_1k_0$. The master key is stored in the register, so that the 32-bit round key of each round is taken from the leftmost 32-bit in the register for i=1,2,…,31. The key schedule is updated as follows.

$$\begin{cases} K<<<13 \\ [k_{79}k_{78}k_{77}k_{76}]=S_0[k_{79}k_{78}k_{77}k_{76}] \\ [k_{75}k_{74}k_{73}k_{72}]=S_0[k_{75}k_{74}k_{73}k_{72}] \\ [k_{47}k_{46}k_{45}k_{44}k_{43}]=[k_{47}k_{46}k_{45}k_{44}k_{43}]\oplus[i]_2 \end{cases} \tag{3}$$

3. Bit-oriented MILP model

This section introduces the construction method for the basic bit-oriented MILP model, including the search algorithm of the accurate lower bound of the differential active S-box and the impossible differential distinguisher with regard to single-key and related-key. Moreover, the optimization technology for the basic MILP model is proposed, and an improved verification algorithm for impossible differential distinguisher is presented.

3.1 Basic MILP model for searching differential distinguisher

MILP is an optimized production technology in operation research, whose purpose is to solve the maximum or minimum value of the objective function under certain constraints. The automated search method based on MILP has been widely used in the security analysis of cryptographic ciphers. In order to solve the MILP model, the tool of Gurobi [22] is used.

MILP is defined as follows:

Def. 1. Under the constraint conditions $Ax \le b$, find the vector $x = (x_1, x_2, ..., x_n)$ such that $c_1x_1 + c_2x_2 + ... + c_nx_n$ gets the maximum or minimum value, where $A \in \mathrm{R}^{m \times n}$, $b \in \mathrm{R}^m$, $(c_1, c_2, ..., c_n) \in \mathrm{R}^n$, and R is set as an integral domain.

The main operations of lightweight block cipher usually include XOR, S-box, cyclic shift and bit permutation. Among them, the cyclic shift and bit permutation operations only change the position of bits and don't need to construct the any constraints. For S-box and XOR operations, the constraints can be defined as follows.

S-box: a 0-1 variable is used to describe the active state of S-box, where A_t=1 means the S-box is active, otherwise not active. A_t can be described as follows.

$$A_t = \begin{cases} 1, \text{ input differential of S-box is nonzero} \\ 0, \text{ otherwise} \end{cases} \tag{4}$$

Then $\min \sum A_t$ is chosen as the objective function of MILP to determine the lower bound of active S-box.

Suppose $(\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3)$ and $(\Delta y_0, \Delta y_1, \Delta y_2, \Delta y_3)$ are respectively the input and output differences of the 4-bit S-box, and A_t is the active state of S-box. If the input difference is non-zero, that is, at least one bit of $(\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3)$ is active, then $A_t = 1$. The inequality constraints are defined as follows:

$$\begin{cases} \Delta x_0 - A_t \le 0 \\ \Delta x_1 - A_t \le 0 \\ \Delta x_2 - A_t \le 0 \\ \Delta x_3 - A_t \le 0 \end{cases} \tag{5}$$

Conversely, when $A_t = 1$, at least one of $\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3$ is active, for which the inequality constraint can be defined as follows:

$$\Delta x_0 + \Delta x_1 + \Delta x_2 + \Delta x_3 - A_t \ge 0 \tag{6}$$

In order to describe the difference properties of S-box more accurately, according to the method proposed by Sun et al. [17], the SageMath software can be used to generate the convex hull H-expression from all the differential propagation patterns of S-box. Due to the large numbers of the generated constraints, as the dimension of the S-box increases, the constraints grow rapidly. To reduce the redundant constraints, Sun et al. proposed a greedy algorithm to reduce the convex hull H-expression and the numbers of constraints. For the ESF algorithm, the numbers of constraints of S-boxes are summarized in **Table 2**:

Table 2. The Numbers of Constraints of S-Boxes of ESF

S-Box	The Numbers of H-Represetation of the Convex Hulls	The Numbers of Constraints by Greedy Algorithm
S_0	327	21
S_1	327	21
S_2	325	21
S_3	368	27
S_4	321	23
S_5	321	23
S_6	327	21
S_7	368	27

XOR: For $\Delta a_i \oplus \Delta b_i = \Delta c_i$, the inequality constraints are defined as follows:

$$\begin{cases} \Delta a_i + \Delta b_i + \Delta c_i \geq 2d_i \\ d_i \geq \Delta a_i \\ d_i \geq \Delta b_i \\ d_i \geq \Delta c_i \\ \Delta a_i + \Delta b_i + \Delta c_i \leq 2 \end{cases} \tag{7}$$

where $d_i \in \{0,1\}$ is a dummy variable.

According to the above constraints, a MILP model can be constructed to search for the accurate lower bound of the differential active S-box. For the search of impossible differential distinguisher, the objective function needs to be set to null, and the constraint conditions that limiting the input/output differences should be added to the model. Suppose Δin and Δout respectively represent input and output difference sets of cipher. When the solution of the model cannot be found by Gurobi, an impossible difference distinguisher $\Delta in \nrightarrow \Delta out$ will be obtained.

The automated search algorithm is shown in Algorithm 1 [19]:

Algorithm 1: Automatic Search Algorithm of Differential Distinguisher

Input: *r*-round, inequality constraints of nonlinear layer and linear layer, GOAL $\in$ { Differential, Impossible Differential}, Δin and Δout

Output: lower bound of *r*-round differential active S-box, impossible differential distinguisher

```
1)  Initialization;
2)  For ( j = 0 , j < r , j ++ ){
3)    add nonlinear layer constraints;
4)    add linear layer constraints;
5)  }
6)  if (GOAL = Differential){
7)    add objective function;
8)    add initial constraints: at least 1-bit input differential is active;
9)    construct an accurate lower bound search model M for differential active
      S-box;
10)   solve the model with Gurobi;
11) }
```

```
12) else if (GOAL = Impossible Differential){
13)   set the objective function to empty;
14)   For ( input difference Δx_i ∈ Δin ){
15)     For ( output difference Δy_i ∈ Δout ){
16)       Construct impossible differential model M according to the input/output
      differences;
17)       solve the model with Gurobi;
18)       if ( M.status == INFEASIBLE )        // Model has no solution
19)           Record the difference between input and output; //An impossible
      difference
20)         }
21)      }
22)  }
23) return differential lower bound of the number of active S−boxes or impossible
      differential distinguisher Δin ↛ Δout ;
```

By combining difference analysis with related-key analysis, a special key difference can be constructed for XOR offsetting input difference, which can reduce the lower bound of the active S-box and expand the number of distinguisher rounds. To construct the MILP model in related-key setting, it only needs to add the key schedule to the MILP model in single-key setting.

3.2 Improved MILP-based model for searching differential-like distinguisher

Based on the MILP construction method in Section 3.1, the corresponding models can be constructed for different cryptographic ciphers. However, as the search rounds increases, the number of constraints and variables will increase rapidly. To solve this problem, the redundant inequality and variable description operations should be reduced as much as possible under the correct constraints in constructing MILP of ESF. The simplified model enables the solver to efficient find expected solutions.

Firstly, according to [23], the formula (5) can be reduced to obtain the following inequality. Note that 24 constraints can be reduced per round if inequality (8) is used to describe the non-zero state of S-box input difference.

$$\Delta x_0 + \Delta x_1 + \Delta x_2 + \Delta x_3 - 4A_t \leq 0 \tag{8}$$

Secondly, since all variables are 0-1 variables in XOR operations, Cui et al. [18] reduced formula (7) to the following equation. According to this equation, 4 constraints can be reduced for each XOR operation.

$$\Delta a_i + \Delta b_i + \Delta c_i = 2\Delta d_i \tag{9}$$

Thirdly, based on MILP, cyclic shift and bit permutation operations only focus on the change of position and constructing the corresponding equality constraints. The cyclic shift operation and XOR operation in ESF are adjacent operations by analyzing the structure of ESF. MILP for ESF can be constructed as in the following inequality, which takes the constraints of cyclic shift as the input to the XOR operation:

$$(L_i <<< 7) + F(R_i, RK_i) + R_{i+1} = 2\Delta d_i,\ (i = 0,1,...,31) \tag{10}$$

Therefore, since there is no need to construct cyclic shift operations separately, 32 inequality constraints and 32 variables can be reduced in each round, which makes the model structure more compact and the number of constraints and variables reduced.

3.3 Improved verification algorithm for impossible differential distinguisher

In order to obtain the differential propagation path and verify the correctness of the model, the verification on the differential active S-boxes MILP model can be performed by getting the value of each variable through getVars() in Gurobi. However, Gurobi can only determine whether the model has solution in searching impossible differential distinguisher. Thus, it is impossible to obtain the propagation path of the impossible difference and the position of contradiction points, which reduces the reliability of the impossible differential distinguisher searched by this method.

3.3.1 Verification process for impossible differential distinguisher

Based on the miss-in-the-middle technology [24], Cui et al. proposed a verification algorithm to check the correctness of the impossible differential distinguisher [18] searched by MILP. When a r-round impossible differential distinguisher is found, the connection between round $\lceil r/2 \rceil$ and round $\lceil r/2 \rceil+1$ is deleted as much as possible if the model has no solution, and the remain bits are determined as a contradiction. Assuming that the contradiction position has t-bit ($0<t<n$), there must be no intersection between all possible differential set A of t-bit obtained by input differential encryption and all possible differential set B of t-bit obtained by output differential decryption. The specific process is shown in Algorithm 2 [18].

Algorithm 2 Verification method of impossible differential distinguisher

Input: *R*ound R, impossible differential distinguishers $\Delta in \nrightarrow \Delta out$

Output: t-bit contradiction, set A and set B

1) Initialization;
2) Under the premise that the model has no solution, remove the inequalities between round $\lceil r/2 \rceil$ and round $\lceil r/2 \rceil+1$. Assume that after the connection of some bits is cut off, there are remain t-bit connected;
3) Fixed input differential Δin, construct model M_1 for rounds $0\sim\lceil r/2 \rceil$;
4) Traverse all the difference sets of t-bit in model M_1, then add t-bit possible differences into set A;
5) Fixed output differential Δout， construct model M_2 for rounds $\lceil r/2 \rceil+1\sim r$;
6) Traverse all the difference sets of t-bit in model M_2, then add t-bit possible differences into set B;
7) return t-bit contradiction, set A and set B;

3.3.2 Improved verification process for impossible differential distinguisher

Analysis showed that Algorithm 2 has some shortcomings to find contradictions. Firstly, it is easy to make mistakes or miss the inequality to be deleted in the complex MILP model. Secondly, the integrity of the model would be destroyed if the corresponding inequality is removed. To solve these issues, this paper proposes a more effective verification method for the searched impossible differential distinguisher.

In the process of verifying impossible differential distinguisher, let $(\Delta out_0, \Delta out_1, ..., \Delta out_j)$ be the output in round $\lceil r/2 \rceil$, $(\Delta in_0, \Delta in_1, ..., \Delta in_j)$ be the input to round $\lceil r/2 \rceil+1$, and $(\Delta out_0, \Delta out_1, ..., \Delta out_j) \to (\Delta in_0, \Delta in_1, ..., \Delta in_j)$ be the propagation process. In searching for contradictions, our method does not directly delete the relevant inequalities when the model has no solution, but a set of temporary variables $(\alpha_0, \alpha_1, ..., \alpha_j)$ are added so that the direct propagation between the upper and lower rounds can be replaced by the transfer of temporary variables in bit propagation, that is:

$$\begin{cases} (\Delta out_0, \Delta out_1, ..., \Delta out_j) \to (\alpha_0, \alpha_1, ..., \alpha_j) \\ (\alpha_0, \alpha_1, ..., \alpha_j) \to (\Delta in_0, \Delta in_1, ..., \Delta in_j) \end{cases} \tag{11}$$

In searching for contradictions, the temporary variables are removed in sequential. If the model changes from no solution to be solvable after some temporary variables are removed, then the bit position of this temporary variable is considered as the contradictory point.

The improved verification algorithm maintains the integrity of the MILP model by deleting temporary variables instead of directly deleting the inequalities of the model. Also, when sequentially deleting the temporary variables in finding the contradictory points, there is no need to find the position of the inequality as in the original method, which is more efficient and avoids the wrong or missed selection. The detailed improvement operation process is shown in Algorithm 3:

Algorithm 3 Improved method of finding contradictory points

Input: *R*ound r, temporary variable set $A = (\alpha_0, \alpha_1, ..., \alpha_j)$

Output: *t*-bit contradiction

1) Initialization;
2) In the output of *r*-round, that is, the position of input of (*r*+1)-round, add a temporary variable α_j to block the direct transmission between the upper and lower rounds;
3) For ($j = 0$, $j < |A|$, j ++) { // $|A|$ denotes the size of A
4) Delete temporary variables α_j;
5) If (the model has solution)
6) This bit is a contradiction;
7) else if (the model has no solution)
8) This bit is a non-contradictory point;
9) }
10) return *t*-bit contradiction;

4. Security analysis of ESF

In the single-key and related-key setting, an optimized search model for the exact lower bound of differential active S-boxes and impossible differential distinguisher is constructed for ESF,

and Gurobi is used to solve the model. The results are as follows.

4.1 Exact lower bounds of the number of differential active S-boxes

The exact lower bounds of differential active S-boxes in single-key setting and related-key setting of ESF for rounds 1 to 11 are shown in **Table 3**.

Table 3. Results for differential active S-boxes in single-key setting and related-key setting on ESF

Rounds	Single-key	Related-key	Rounds	Single-key	Related-key
1	0	0	7	8	4
2	1	0	8	9	5
3	2	0	9	11	6
4	3	0	10	13	8
5	4	1	11	14	10
6	6	2			

With the proposed method, the accurate lower bound of 11-round differential active S-boxes in single-key setting is 14. Since the optimal differential probability of S-box is 2^{-2}, the maximum differential probability of full-round ESF would be $(2^{-2})^{14+14+13}=2^{-82}<2^{-64}$. Thus, the full-round ESF is sufficiently secure to resist differential attack. In particular, the number of 10-round differential active S-box is 13, which is a more accurate boundary compared with existing results.

4.2 Search results and verification of impossible differential distinguisher

Based on impossible differential MILP in single-key model of ESF, due to high time complexity of traversing all input/output differential sets, the case that a half byte active of input/output differential (excluding zero differentials) is picked. By traversing $(\Delta in \rightarrow \Delta out) = (16\times 15)^2$ times, 2108 9-round impossible differential distinguisher of ESF in single-key setting can be finally found. Some partial searched results are shown in **Table 4**, where Δin and Δout represent input and output differences respectively, the result is expressed in hexadecimal number, and 0 denotes zero difference.

Table 4. The partial results of the impossible differential distinguishers on ESF in single-key setting

$\Delta in \nrightarrow \Delta out$
0000000080000000 $\nrightarrow$ 0000000000000008
0000000080000000 $\nrightarrow$ 0000000000000020
0000000080000000 $\nrightarrow$ 0000000000000040
0000000080000000 $\nrightarrow$ 0000000000000080
0000000080000000 $\nrightarrow$ 00000000000000a0
0000000080000000 $\nrightarrow$ 00000000000000c0

According to the improved algorithm for verification of impossible differential distinguisher presented in Section 3.3, taking the first single-key impossible differential in **Table 4** as example, namely $0000000080000000 \nrightarrow 0000000000000008$, 11 contradictory points can be found at the output of round 5. The specific steps for searching contradictions are as follows:

（1） Fixed input difference Δin=0000000080000000, build model M_1 for rounds 1~5, traverse 2^{11} difference cases, set *A* contains 2046 cases except all zero differences;

（2） Fixed output difference Δout=0000000000000008, build model M_2 for rounds 6~9, traverse 2^{11} difference cases, set *B* only contains all zero differences;

（3） There is no intersection between sets *A* and *B*, thus the current path is an impossible differential distinguisher in single-key setting.

Based on the impossible MILP model in related-key setting of ESF, the case that the master key differential with Hamming weight 1 and the input/output differential with Hamming weight less than or equals to 1 is considered, that is, 80×65×65 times are traversed and 14 impossible differential distinguishers in related-key setting of 12-round ESF are searched. The partial searched results are shown in **Table 5**, where Δin , Δout , ΔK represent input, output and master key differences, respectively, the result is expressed in hexadecimal, and 0 represents zero difference.

Table 5. The partial results for impossible differential distinguisher of ESF in related-key setting

$\Delta in \nrightarrow \Delta out$	ΔK
0000000000000000 $\nrightarrow$ 0004000000000000	0000000000000000008
0000000000000000 $\nrightarrow$ 0008000000000000	0000000000000000010
0000000000000000 $\nrightarrow$ 0010000000000000	0000000000000000020
0000000000001000 $\nrightarrow$ 0000000000000000	0000100000000000000
0000000000000400 $\nrightarrow$ 0000000000000000	0000040000000000000
0000000000000200 $\nrightarrow$ 0000000000000000	0000020000000000000

Similarly, taking the first impossible differential distinguisher in related-key setting in **Table 5** as example for verification, 12 contradictions can be found at the output of round 6. The specific steps to search for contradictions are as follows:

（1） Fixed the master key difference ΔK=0000000000000000008 and the input difference Δin=0000000000000000, build model M_1 for rounds 1~6, traverse all 2^{12} cases, set *A* only contains 0x0001;

（2） Fixed output difference Δout=0004000000000000, build model M_2 for rounds 7~12, set *B* contains the remaining 4095 difference cases;

（3） There is no intersection between sets *A* and *B*, thus the current path is an impossible differential distinguisher in related-key setting.

4.3 Key Recovery

With the first 9-round impossible differential distinguisher in **Table 4**, a 15-round impossible differential attack on ESF can be obtained by extending 3-round forward and 3-round backward, which is shown in **Fig. 3**.

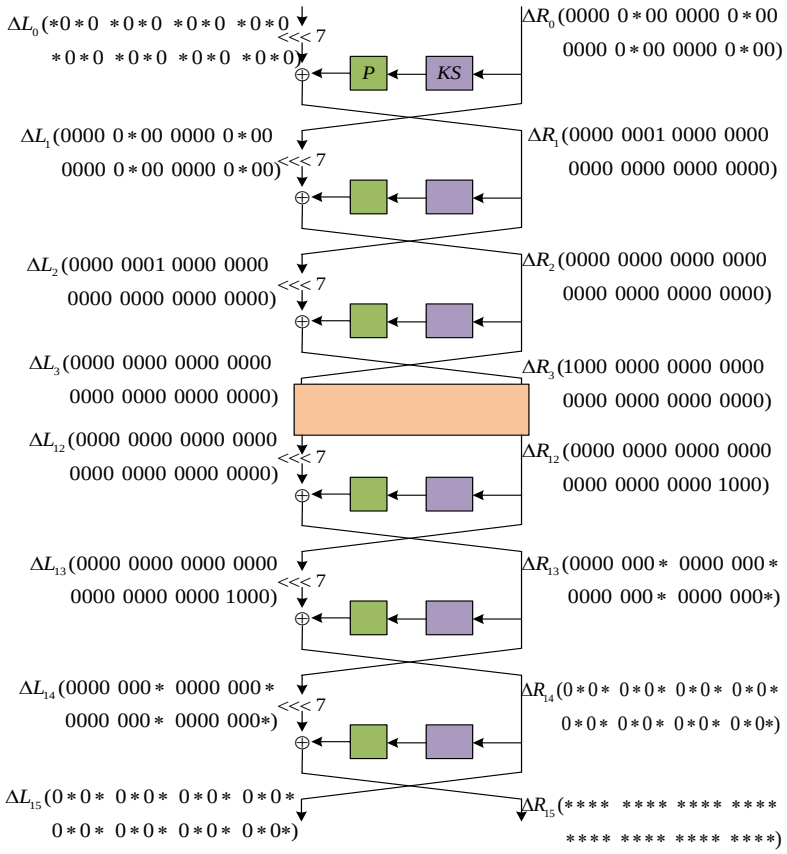

Fig. 3. The 15-round impossible differential attack on ESF

This attack needs to guess 72-bit $K_0^{5\text{-}8}$, $K_0^{13\text{-}16}$, $K_0^{21\text{-}24}$, $K_0^{29\text{-}32}$, $K_1^{5\text{-}8}$, $K_{12}^{29\text{-}32}$, $K_{13}^{5\text{-}8}$, $K_{13}^{13\text{-}16}$, $K_{13}^{21\text{-}24}$, $K_{13}^{29\text{-}32}$ and K_{14}. The relationship of the guessed subkey and the master key is shown in **Table 6**.

Table 6. The relationship of the subkey and master

Subkey to be guessed	Master key corresponding to subkey
$K_0^{5\text{-}8}$, $K_0^{13\text{-}16}$, $K_0^{21\text{-}24}$, $K_0^{29\text{-}32}$	K_{75}, K_{74}, K_{73}, K_{72}, K_{67}, K_{66}, K_{65}, K_{64}, K_{59}, K_{58}, K_{57}, K_{56}, K_{51}, K_{50}, K_{49}, K_{48}
$K_1^{5\text{-}8}$	K_{62}, K_{61}, K_{60}, K_{59}
$K_{12}^{29\text{-}32}$	K_{55}, K_{54}, K_{53}, K_{52}
$K_{13}^{5\text{-}8}$, $K_{13}^{13\text{-}16}$, $K_{13}^{21\text{-}24}$, $K_{13}^{29\text{-}32}$	K_{66}, K_{65}, K_{64}, K_{63}, K_{58}, K_{57}, K_{56}, K_{55}, K_{50}, K_{49}, K_{48}, K_{47}, K_{42}, K_{41}, K_{40}, K_{39}
K_{14}	K_{57}, K_{56}, K_{55}, K_{54}, $K_{53}\cdots K_{26}$

If K_{14} is known, the master key k[57, 56, …, 27, 26] will be available. Thus, $K_0^{29\text{-}32}$, $K_0^{21\text{-}22}$, $K_{12}^{29\text{-}32}$, $K_{13}^{21\text{-}24}$, $K_{13}^{29\text{-}32}$ can be deduced. According to the dependency of the key schedule, only 58-bit subkeys K_{14}, $K_0^{5\text{-}8}$, $K_0^{13\text{-}16}$, $K_0^{23\text{-}24}$, $K_1^{5\text{-}8}$,$K_{13}^{5\text{-}8}$, $K_{13}^{13\text{-}16}$, $K_{13}^{21\text{-}24}$ need to be guessed.

1) Select 2^m plaintext, from which the data pairs satisfying L_0=(*0*0 *0*0 *0*0 *0*0 *0*0 *0*0 *0*0 *0*0) and R_0=(0000 000* 0000 000* 0000 000* 0000 000*) are filtered out, where * indicates that the bit can take any value. Therefore, a structure has 2^{20} plaintexts,

which constitutes $2^{20}\times 2^{20}\times 2^{-1}=2^{39}$ data pairs. After 15 rounds of ESF encryption, 2^{m+39} ciphertext pairs can be obtained.

2) Filter out ciphertexts satisfying ΔL_{15}=(0*0* 0*0* 0*0* 0*0* 0*0* 0*0* 0*0* 0*0*) and ΔR_{15}=(**** **** **** **** **** **** **** ****). $2^{m+39}\times 2^{-16}=2^{m+23}$ data pairs would remain.

3) Guess K_{14}. Filter out the difference satisfying ΔL_{14}= (*000 0000 *000 0000 *000 0000 *000 0000), according to $R_{14}=L_{14}>>>7$ and $L_{14}=\mathrm{P}\cdot\mathrm{S}(R_{14}\oplus K_{14})\oplus R_{15}$, $2^{m+23}\times 2^{-28}=2^{m-5}$ data pairs can be filtered out. Guess the key K_{14}[1-32] bit by bit, taking $K_{14}^{1\text{-}4}$ as an example, check whether all values of ΔL_{14}[1,9,17,25] are 0. If so, the data pairs at the corresponding positions can be filtered out. If it is an uncertain difference, the data pairs cannot be filtered. The number of calculations in this process is about $0.25\times\sum 2^{m+(27-4i)}\times 2^{4i}$, $1\leqslant i\leqslant 8$.

4) Guess $K_{13}^{5\text{-}8}$, $K_{13}^{13\text{-}16}$, $K_{13}^{21\text{-}24}$, $K_{13}^{29\text{-}32}$. From the dependency between the subkeys, $K_{13}^{21\text{-}24}$ and $K_{13}^{29\text{-}32}$ can be obtained through K_{14}. Thus, only $K_{13}^{5\text{-}8}$ and $K_{13}^{13\text{-}16}$ need to be guessed. Filter out the data pairs such that the difference satisfying ΔL_{13}=(0000 0000 0000 0000 0000 0000 0000 1000). According to $K_{13}^{21\text{-}24}$ and $K_{12}^{29\text{-}32}$, check whether ΔL_{13}[6,14,22,30,8,16,24,32]=(0000 0000) holds. If so, then filter out the data pairs. Guess $K_{13}^{5\text{-}8}$ and $K_{13}^{13\text{-}16}$, check whether ΔL_{13}[2,10,18,26,4,12,20,28]=(0000 0000) holds, and continue to filter out data pairs that do not meet the requirements. By two rounds of filtering, there would be $2^{m-5}\times 2^{-16}=2^{m-21}$ data pairs remaining. The amount of calculations is about $2\times(2^{m-5}\times 2^{32}+ 2^{m-13}\times 2^{32}\times 2^{8})/4=2^{m+27}$.

5) Guess $K_{12}^{29\text{-}32}$. From the dependency between the subkeys, $K_{12}^{29\text{-}32}$ can be obtained through K_{14}, check whether ΔL_{12}[8,16,24,32]=(0000) holds, filter data pairs that do not meet the requirements. After filtering, there would be $2^{m-21}\times 2^{-4}=2^{m-25}$ data pairs remaining. The amount of calculations is about $2\times(2^{m-21}\times 2^{32}\times 2^{8})/8 =2^{m+17}$.

6) Guess $K_0^{5\text{-}8}$, $K_0^{13\text{-}16}$, $K_0^{21\text{-}24}$, $K_0^{29\text{-}32}$. Note that $K_0^{23\text{-}24}$ and $K_0^{29\text{-}32}$ can be obtained through K_{14}. It only needs to guess $K_0^{5\text{-}8}$, $K_0^{13\text{-}16}$ and $K_0^{21\text{-}22}$. Filter out the data pairs such that the difference satisfying R_1= (*0*0 *0*0 *0*0 *0*0 *0*0 *0*0 *0*0 *0*0). According to $R_1=\mathrm{P}\cdot\mathrm{S}(R_0\oplus K_0)\oplus L_0<<<7$, filter out the remaining $2^{m-25}\times 2^{-6}=2^{m-31}$ data pairs. The amount of calculations is about $2\times(2^{m-25}\times 2^{32}\times 2^{8}+2^{m-35}\times 2^{32}\times 2^{8}\times 2^{10})/8 =2^{m+14}$.

7) Guess $K_1^{5\text{-}8}$. According to $K_1^{5\text{-}8}$, check whether ΔR_2[2,10,18,26]=(0000) holds, filter out data pairs that do not meet the requirements. After filtering, there would be $2^{m-31}\times 2^{-4}=2^{m-35}$ data pairs remaining. The amount of calculations is about $2\times(2^{m-31}\times 2^{32}\times 2^{8}\times 2^{10})/8=2^{m+17}$.

In the above process, a total of 58-bit subkeys need to be guessed. After screening wrong keys, there are remaining $2^{58}\times(1-2^{-4})^{2^{m-35}}$ candidate keys. When the number of remaining candidate keys is less than or equal to 1, the only correct key can be guaranteed to be recovered, that is, if $2^{58}\times(1-2^{-4})^{2^{m-35}}\leq 1$, the solution $m\approx 40.45$ can be obtained. It can be seen that the data complexity is $2^{20}\times 2^{40.45}=2^{60.45}$.

5. Result comparison and analysis

We found the exact lower bound of the differential active S-boxes in single-key setting. The number of more accurate differential active S-box of 10-round is 13 in our paper, while is 12 in

[23]. The detailed comparison about the exact lower bounds of differential active S-boxes of ESF in single-key setting between our method and [23] is shown in **Table 7**.

Table 7. The exact lower bounds of differential active S-boxes of ESF in single-key setting

Rounds	1	2	3	4	5	6	7	8	9	10	11
Reference [23]	0	1	2	3	4	6	8	9	11	12	14
Our method	0	1	2	3	4	6	8	9	11	13	14

Based on the refined linear MILP model, Yin et al. [23] searched 925 8-round zero-correlation linear approximation distinguishers by adding input and output constraints in each round. Li et al. [27] performed a new 9-round integral distinguisher of ESF based on an automated search method. For the key recovery, Li et al. [26] performed an impossible differential cryptanalysis on 13-round ESF based on the 8-round truncated impossible differential distinguisher, where 48-bit are guessed and the 80-bit master key is recovered. But based on the searched 9-round impossible differential distinguisher in single-key setting, an impossible differential cryptanalysis on 15-round ESF was performed in this paper, where 58-bit are guessed and the master key is recovered.

Furthermore, Xie et al. [25] constructed an 11-round related-key impossible differential path by combining the characteristics of the key schedule with the structure of the round function. And based on a 11-round impossible differential distinguisher in related-key setting, Xie et al. [25] attacked 15-round ESF, where 40-bit key is recovered. In this paper, we obtained 14 12-round related-key impossible differential distinguishers of ESF, which is currently the longest related-key impossible differential distinguisher of ESF. In addition, based on the improved method of finding contradictions, this paper effectively verified the impossible differential distinguisher obtained in single- and related-key setting for the first time.

Compared with existing results, this paper achieves the highest round number of attack in single-key setting and constructs the longest round of the impossible differential distinguisher in related-key setting. The detailed comparison between the existing security analysis results and our method for ESF is shown in **Table 8**.

Table 8. The compared security analysis results of ESF

	Cryptanalysis methods	**Distinguisher Rounds**	**Number**	**Attack Rounds**	**Data complexity**	**Time complexity**	**Reference**
Single-Key	Zero-correlation Linear	8	925	/	/	/	[23]
	Integral Analysis	9	1	/	/	/	[27]
	Truncated Impossible Differential	8	/	13	$2^{61.99}$	$2^{77.39}$	[26]
	Impossible Differential	9	2108	15	$2^{60.45}$	$2^{70.02}$	Our method
Related-Key	Impossible Differential	11	1	15	$2^{61.5}$	$2^{40.5}$	[25]
	Impossible Differential	12	14	/	/	/	Our method

6. Conclusion

This paper proposes a more effective MILP model based on the difference and impossible difference search model proposed by Sasaki et al., which is combined with the greedy algorithm proposed by Sun et al. to simplify the expression of convex hull H-expression, reduces constraints in describing XOR and S-box operations, improves cyclic shift and description method of bit permutation and reduce the numbers of inequality constraints and variables. Also, a new method for finding out the contradictory points of the impossible differential distinguisher using temporary variables is proposed for the first time.

A simplified MILP difference distinguisher search model is constructed for ESF, where a more accurate lower bounds of 1~11 rounds difference active S-boxes in single-key setting can be obtained. The impossible differential distinguisher is searched and verified in single-key/related-key setting. Particularly, the 14 12-round impossible differential distinguisher in related-key setting in this paper is the longest. Moreover, based on the 9-round impossible differential distinguisher in single-key setting, the 15-round impossible differential attack of ESF algorithm also is the highest.

Acknowledgement

This article is supported in part by the National Natural Science Foundation of China (61872103, 62062026, 61862012), the Foundation of Science and Technology on Communication Security Laboratory (6142103190103), the Innovation Research Team Project of Guangxi (2019GXNSFGA245004), the Key Research and Development Plan of Guangxi (guike AB18281019), the scientific research project of young innovative talents of Guangxi (guike AD20238082), the Guangxi Natural Science Foundation (2019GXNSFFA245015), and the Science Research Foundation of Guilin University of Electronic Technology (UF19050Y).

References

[1] Y. Wang, Y. Chen, H. Ahmad, et al., "Message authentication with a new quantum hash function," *CMC-Computers, Materials & Continua*, vol. 59, no. 2, pp. 635-648, 2019. Article (CrossRef Link)

[2] H. L. Chen, G. Xu, Y. L. Chen, X. B. Chen, Y. X. Yang et al., "Cipherchain: a secure and efficient ciphertext blockchain via mpeck," *Journal of Quantum Computing*, vol. 2, no. 1, pp. 57-83, 2020. Article (CrossRef Link)

[3] C. Chu, Z. Huang, R. Xu, G. Wen, L. Liu, "A cross layer protocol for fast identification of blocked tags in large-scale RFID systems," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 1705-1724, 2020. Article (CrossRef Link)

[4] C. T. Poomagal, G. A. Sathish Kumar and D. Mehta, "Multi level key exchange and encryption protocol for internet of things (iot)," *Computer Systems Science and Engineering*, vol. 35, no.1, pp. 51-63, 2020. Article (CrossRef Link)

[5] A. Bogdanov, L.R. Knudsen, G. Leander, "PRESENT: an ultra-lightweight block cipher," in *Proc. of International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 450-466, 2007. Article (CrossRef Link)

[6] W.L. WU, L. Zhang, "LBlock: a lightweight block cipher," in *Proc. of International Conference on Applied Cryptography and Network Security*, pp. 327-344, 2011. Article (CrossRef Link)

[7] J. Guo, T. Peyrin, A. Poschmann, et al., "The LED block cipher," in *Proc. of International International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 326-341, 2011. Article (CrossRef Link)

[8] S. Banik, A. Bogdanov, T. Isobe, et al., "Midori: a block cipher for low energy," in *Proc. of International International Conference on the Theory and Application of Cryptology and Information Security*, pp. 411-436, 2015. Article (CrossRef Link)
[9] S. Banik, S.K. Pandey, T. Peyrin, et al., "GIFT: a small Present," in *Proc. of International International Conference on Cryptographic Hardware and Embedded Systems*, pp. 321-345, 2017. Article (CrossRef Link)
[10] C. Beierle, J. Jean, S. Kölbl, et al., "The SKINNY family of block ciphers and its low-latency variant MANTIS," in *Proc. of International Annual International Cryptology Conference*, pp. 123-153, 2016. Article (CrossRef Link)
[11] M. Long, M. Kong, S. Long and X. Zhang, "An improved differential fault analysis on block cipher klein-64," *Computers, Materials & Continua*, vol. 65, no. 2, pp. 1425-1436, 2020. Article(CrossRef Link)
[12] L. Knudsen, "DEAL-a 128-bit block cipher," *complexity*, vol.258, no.2, pp. 216-225, 1998.
[13] E. Biham, A. Biryukov, A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," in *Proc. of the EUROCRYPT'99*, pp. 12-23, 1999. Article (CrossRef Link)
[14] L.R. Knudsen, "Cryptanalysis of LOKI 91," in *Proc. of International AUSCRYPT'92*, pp. 196-208, 1992. Article (CrossRef Link)
[15] E. Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol.7, no.4, pp.229-246, 1994.
[16] N. Mouha, Q. Wang, D. Gu, et al., "Differential and linear cryptanalysis using mixed-integer linear programming," in *Proc. of International Conference on Information Security and Cryptology*, pp. 57-76, 2011. Article (CrossRef Link)
[17] S. Sun, L. Hu, P. Wang, et al., "Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 158-178, 2014. Article (CrossRef Link)
[18] T.T. Cui, et al., "New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations," *IACR Cryptology ePrint Archive*, pp. 689-707, 2016. Article (CrossRef Link)
[19] Y. Sasaki, Y. Todo, "New impossible differential search tool from design and cryptanalysis aspects," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Cham, pp. 185-215, 2017. Article (CrossRef Link)
[20] Y. Sasaki, Y. Todo, "New algorithm for modeling S-box in MILP based differential and division trail search," in *Proc. of International Conference for Information Technology and Communications*, Springer, Cham, pp. 150-165, 2017. Article (CrossRef Link)
[21] X. Liu, W. Zhang, X. Liu, et al., "Eight-sided fortress: a lightweight block cipher," *The Journal of China Universities of Posts and Telecommunications*, vol. 21, no.1, pp. 104-128, 2014. Article (CrossRef Link)
[22] Gurobi. Gurobi Optimizer Reference Manual, http://www.gurobi.com, 2020.
[23] J. Yin, C.Y. Ma, J. Song, et al., "Security Analysis of LightWeight Block Cipher ESF," *Journal of Computer Research and Development*, vol. 54, no. 10 pp. 2224-2231, 2017. Article (CrossRef Link)
[24] Biham E, Biryukov A, Shamir A, "Miss in the Middle Attacks on IDEA and Khufu," in *Proc. of International Workshop on Fast Software Encryption*, pp. 124-138, 1999. Article (CrossRef Link)
[25] M. Xie, Q.Y. Zeng, "Related-key Impossible Differential Cryptanalysis on Lightweight Block Cipher ESF," *Journal of Electronics and Information Technology*, vol. 41, no.5, pp. 1173-1179, 2019. Article (CrossRef Link)
[26] M.M.Li, J.S.Guo, J.Y.Cui, L.H.Xu, "Truncated impossible difference cryptanalysis of ESF Algorithm," *Journal of Cryptologic Research*, vol. 6, no.5, pp. 585-593, 2019. Article (CrossRef Link)

[27] Li J, Wang H, Qiu X, et al., "Integral analysis of GRANULE and ESF block ciphers based on MILP," in *Proc. of 2021 12th International Conference on Information and Communication Systems (ICICS). IEEE*, pp. 10-16, 2021. Article (CrossRef Link)

Xiaonian Wu is an Associate Professor with School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China. He received the M. degree in Computer science and technology from National University of Defense Technology, Changsha, China. His main research interests include information security, distribution computing.

Jiaxu Yan is a postgraduate student in master's course at School of Computer Science and Information Security in Guilin University of Electronic Technology, Guilin, China. His main research interests include the analysis of cryptographic algorithm.

Lingchen Li is a teacher with School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China. She received the Ph.D. degree in Computer science and technology from the University of Chinese Academy of Sciences, Beijing, China. Her main research interests include the design and cryptanalysis of block cipher.

Runlian Zhang is an Associate Professor with School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China. She received the Ph.D. degree in Computer science and technology from Xi'an Jiaotong University, Xi'an, China. Her main research interests include information security, distribution computing.

Pinghai Yuan is a Research fellow at School of Computing, National University of Singapore. He got his Ph.D. degree at the Department of Computer Science and Technology, Nanjing University. His current research interests focus on software security and system security.

Yujue Wang is a Senior Research Fellow at the Hangzhou Innovation Institute, Beihang University, China. He received the Ph.D. degrees from Wuhan University and City University of Hong Kong under the joint Ph.D. program. His main research interests include applied cryptography and blockchain.