Hindawi
Security and Communication Networks
Volume 2020, Article ID 6789281, 9 pages
https://doi.org/10.1155/2020/6789281

Research Article

Research on SKINNY Optimal Differential Trail Search

Shaoqiang Liu,[1] Chaiyang Peng,[1] and Chunjiang Li[2]

[1]*School of Automation, Central South University, Changsha 410083, China*
[2]*College of Information Science and Technology, Shihezi University, Shihezi 832003, China*

Correspondence should be addressed to Chaiyang Peng; 0904170313@csu.edu.cn

Received 17 December 2019; Revised 15 May 2020; Accepted 4 June 2020; Published 22 June 2020

Academic Editor: Angel M. Del Rey

SKINNY is a tweakable lightweight block cipher algorithm. In order to test its security, this paper performs optimal differential trail search analysis on all SKINNY-64 versions under single-key setting based on the MILP (Mixed Integer Linear Programming) algorithm. Firstly, SKINNY round function is abstracted equivalently by precise constraints, and the objective function is set as the minimum number of active S-box number to optimize SKINNY-64 MILP model. Experiments show the differential trail searched by this method is not necessarily optimal. In order to directly search for the optimal differential trail, the S-box differential probability coding information is added to the optimized SKINNY-64 MILP model, the S-box differential characteristic is reconstructed, and the objective function is set to the minimum value of the probability coding information, which improves the SKINNY-64 MILP model. The results of experimental show that the improved MILP model can directly search for the optimal differential trail, and the complexity is slightly increased, but the search efficiency is significantly improved. Under single-key setting, this method has obvious advantage in searching the optimal differential trails of SKINNY-64 with low round number.

1. Introduction

SKINNY is a SPN-structured tweakable lightweight block cipher algorithm proposed by Beierle [1] at American Cryptography Conference in 2016. SKINNY is divided into six different versions, namely, SKINNY-64-64, SKINNY-64-128, SKINNY-64-192, SKINNY-128-128, SKINNY-128-256, and SKINNY-128-384.

Since the announcement of the SKINNY algorithm, some scholars have used various methods to analyze its security. Tolba et al. [2] performed impossible differential attack analysis on 18, 20, and 22 rounds of SKINNY-n-n, SKINNY-n-2n, and SKINNY-n-3n, respectively. Sadegh Sadeghi et al. [3] obtained the 12-round impossible differential trails of SKINNY-64-64 and SKINNY-64-128 in SKINNY's TK1 and TK2 models, respectively, using the method of intermediate encounter. Hong Dou [4] used the intermediate encounter technology to search out all 16 truncated impossible differential trails of the 11 rounds of the SKINNY encryption algorithm and used one of them to analyze 20 rounds of SKINNY-64-128 using the impossible differential technique under a single key setting. The main approach of these papers is to find trails that are impossible to occur in the ciphertext, leaving only a reasonable number of differential trails to consider.

Unlike methods that search for more impossible differential trails, Mixed integer linear programming(MILP) is a method that can search for differential trails directly. Mouha [5] and Wu [6] converted the minimum active S-boxes number of block ciphers into a MILP problem and applied the MILP method to cryptanalysis. However, this method has two shortcomings. One is that it cannot be directly applied to the SPN block cipher with a bit permutation layer because it does not consider the diffusion effect formed by the S-boxes replacement layer and the bit permutation layer. The second is that, for a given cryptographic algorithm, the MILP constraint set listed cannot fully describe the differential propagation characteristics of the linear diffusion layer [7]. Professor Sun [8] supplemented and optimized the method of Mouha and applied the method of obtaining the minimum number of active S-boxes to a bit-oriented block cipher. A linear inequality was generated based on the differential characteristics of S-boxes. Constraint inequality generated by XOR operation builds an MILP model to search for the differential characteristics of block ciphers under single-key and related-key setting [9], and the MILP model uses only partial linear inequality, making it solvable in real time.

In recent years, some scholars have applied the MILP method to the research of SKINNY cryptographic algorithms. The designers of SKINNY performed a security evaluation of SKINNY. Using the MILP method, they obtained the lower bound of the minimum number of active S-boxes under the single-key and related-key setting. According to the lower limit of the number of differential active S-boxes in SKINNY, they further assumed that each S-box used the maximum differential probability to evaluate the security boundary of SKINNY. However, it is not clear whether such a difference trail with maximum probability that satisfies the lower bound exists. Therefore, Sun et al. [10] proposed a method to obtain stricter boundaries, verified whether the optimal differential trail using the maximum differential probability for all active S-boxes exists, and proposed the method of finding the optimal differential trail of the block cipher algorithm based on MILP. Liu et al. [11] firstly proposed the method of searching the actual differential trail of SKINNY under the relevant tweakable secret key model and used the indirect search method based on MILP to search the optimal differential trail of SKINNY-64 and SKINNY-128. The results show that the probability of the optimal differential trail is much smaller than that obtained from the lower bound of the active S-boxes in SKINNY with the increase of the number of rounds. However, their work is to analyze SKINNY under the related-key setting. Zhang et al. [12] proposed a method based on MILP to automatically search the number of 11 minimum active S-boxes of SKINNY-64/192 and obtained the number of 11 active S-boxes and the corresponding differential trail under this number, but their differential trails are no guarantee that are the optimal trails and other versions of SKINNY-64 are not considered.

In this paper, we analyze the differential propagation characteristics of all SKINNY-64 versions under the single-key setting model by using MILP and obtain the optimal differential trails. The basic method is to establish the MILP model of SKINNY-64 under the single key setting and use the LPSolve optimizer to obtain an optimized solution with the objective function as the minimum number of active S-boxes. Combined with the differential probability coding information of S-boxes, the model was further improved to obtain the optimal differential trail.

The rest of this paper is organized as follows. In Section 2, the MILP model of all SKINNY-64 versions is proposed first. To search the optimal differential trails directly, an improved MILP model of SKINNY-64 and an experimental plan are introduced in Section 3, and also the two experimental results are discussed and analyzed. Finally, Section 4 concludes the work.

2. Analysis of SKINNY Differential Trail Based on MILP

2.1. SKINNY Differential Characteristic Optimization Based on MILP. Due to the differential analysis of single-key setting, the key is assumed to be fixed, the round key difference is not considered, and only the state difference is considered. Therefore, the MILP model of all SKINNY-64 versions can be uniformly optimized by using the S-box constraint part, the Row Shift constraint part, and the column mixed constraint part. MILP model optimization is mainly carried out by reducing constraint inequalities and the number of variables. The specific parameters of a round of difference analysis before and after MILP optimization are shown in Table 1. It can be seen that the optimization reduces the calculation amount and improves the operation efficiency.

In Figure 1, X_i and Y_i represent the state difference of the ith round and Y_{ir} is the state difference of Y_i after Row Shifting, each containing 16 difference cells and a total of 64 bit difference. For example, X_i represents the output difference of the $(i-1)$th or the plaintext pair difference $(x_0, ..K., x_{63})$ when $i=1$. Each state X_i and Y_i contains 16 difference cells, each cell is a nibble, respectively, represented by X_j and Y_j, where $j \in (0, ..K., 15)$. Each difference cell can be expressed as $\mathrm{X}_j = (x_{4\mathrm{j}}, x_{4j+1}, x_{4j+2}, x_{4j+3})$.

2.1.1. S-Box Differential Characteristic Optimization. The 1st round of SKINNY's differential feature changes for each S-box has a total of 97 differential characteristics, as shown in Table 2.

A set of truncated inequality describing these effective difference modes are obtained by computing the finite multipoint convex closure H-representations in a computational geometry system. Through the inequality generator function in the sage.geometry.polyhedron class of the SageMath, a convex closure of a specific S-box can be obtained and 202 inequalities are calculated. Our implementation follows the details presented in Appendix A. To obtain the optimal linear inequalities describing the SKINNY-64 S-box, we use the greedy algorithm to remove the invalid difference to optimize the model. Finally, it only needs 24 valid truncation inequalities (see Table 3) to solve SKINNY-64, which can accurately describe the difference feature of an S-box. The associated source codes of our implementation are listed at Appendix B.

2.1.2. Shift Row Differential Characteristic. In the difference analysis, the Row Shift operation process is the same as the Row Shift process of the SKINNY round function; only the 1st row of the internal state value needs to be fixed, and the 2nd, 3rd, and 4th rows are shifted to the right by 1, 2, and 3 bits, as shown in Figures 1(b) and 1(c).

2.1.3. Mix Column after Optimizing MILP Model. After optimizing the MILP model, the basic process of Column Mixing is shown in Figures 1(c) and 1(d).

Considering the difference of each bit, the 4×4 M matrix of SKINNY is transformed into a 16×16 matrix:

Table 1: Constraint conditions and number of variables of SKINNY-64 differential analysis before and after MILP model optimization.

	Before optimization	The optimized
The constraint inequalities	3712	800
The number of variables	352	288

The *i*th round SKINNY-64 state differential transition after optimization is shown in Figure 1.

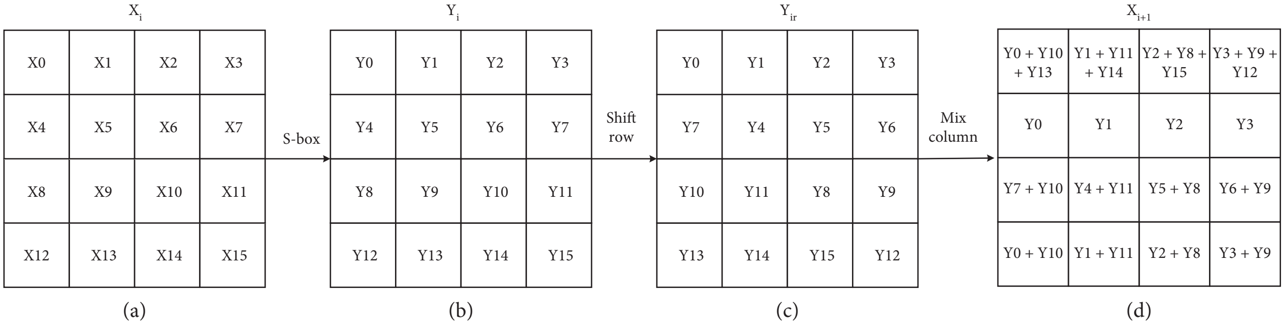

Figure 1: The *i*th round SKINNY-64 state differential transfer diagram after MILP optimization.

Table 2: 97 possible differential characteristics of the 1st round of the SKINNY-64 S-box.

$(x_{4i}, x_{4i+1} + x_{4i+2} + x_{4i+3})$	$(y_{4i}, y_{4i+1}, y_{4i+2}, y_{4i+3}) i \in (0, ..K., 15)$
0000	0000
0001	1000 1001 1010 1011
0010	0001 0011 0101 0110
0011	1000 1001 1010 1011 1100 1101 1110 1111
0100	0010 0110 0111 1011 1100 1101
0101	0010 0110 0111 1010 1100 1101
0110	0001 0011 0100 0111 1000 1010 1101 1110
0111	0001 0011 0100 0111 1001 1011 1100 1111
1000	0100 0101 1100 1101 1110 1111
1001	0100 0101 1100 1101 1110 1111
1010	0101 0110 1000 1001 1010 1011
1011	0001 0011 1100 1101 1110 1111
1100	0010 0110 0111 1000 1110 1111
1101	0010 0110 0111 1001 1110 1111
1110	0001 0011 0100 0111 1001 1011 1101 1110
1111	0001 0011 0100 0111 1000 1010 1100 1111

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

Output difference $X_{i+1} = M \times Y_{ir}$ for the 1st round, corresponding to the 2nd round of input is shown in Table 4.

Based on the XOR method of MILP modeling, the constraint conditions of Column Mixing can be obtained. If the input is tri-XOR, the intermediate variable u_i, $i \in (0, \ldots, 15)$, is introduced. In the column mixed operation, 64 sets of inequalities are generated. Let $a \oplus b = c$, where a and b and c are the input and output differences of the XOR. Virtual variable $d^{\oplus}$ is introduced, when input a and b and output c are all zero, the variable $d^{\oplus}$ is zero. In any other cases, the variable $d^{\oplus}$ is 1. It introduces 64 $d^{\oplus}$.Therefore, a total of 336 constraint inequalities need to be listed in the 1st round of Column Mixing. Due to the large number of linear inequalities involved, representative constraint inequalities are listed in Table 5.

2.2. Analysis of SKINNY-64 4-Round MILP Model Results.

SKINNY-64 1st difference analysis contains 800 constrained inequalities involving 288 variables Therefore, a total of 2864

Table 3: 24 efficient truncation inequalities generated.

24 effective truncation inequalities	Number of invalid difference modes removed/inequalities
$-2x_0 + 3x_1 - 3x_2 - 2x_3 + 5y_0 + 4y_1 + y_2 7y_3 \geq 0$	27
$-x_0 + x_1 = 2x_2 + x_3 + y_0 + 3y_1 - 2y_3 \geq 0$	24
$4x_0 + 3x_1 + 2x_2 + 3x_3 - y_0 - y_1 - y_2 - y_3 \geq 0$	18
$2x_0 - x_1 + 2x_2 + 3y_0 - y_1 + 3y_2 - y_3 \geq 0$	13
$x_0 + 3x_1 + x_2 - 2x_3 + 2y_0 - y_1 - 2y_2 \geq -2$	9
$-3x_0 + 2x_1 + x_2 - 2x_3 - y_0 + 3y_1 + y_3 \geq -3$	8
$x_1 - 2x_2 + 2x_3 - y_0 - 2y_1 + y_2 + y_3 \geq -3$	7
$-2x_0 - 3x_1 + 2x_2 + x_3 + y_0 - y_1 + 3y_2 - y_3 \geq -4$	7
$-x_1 - 2x_2 - x_3 + y_0 - y_1 - 2y_2 + 2y_3 \geq -5$	6
$-x_1 - x_2 - x_3 + y_0 - 2y_1 + 2y_2 - 2y_3 \geq -5$	5
$2x_0 + x_1 + 3x_2 + 4x_3 - 3y_0 + 2y_1 - y_2 + 3y_3 \geq 0$	5
$x_0 - 2x_1 + 2x_2 - 2x_3 - y_0 + y_1 - y_2 - 2y_3 \geq -6$	5
$x_1 - 2x_2 + 2x_3 - y_0 - 2y_1 - y_2 - y_3 \geq -5$	4
$x_0 - x_1 - x_3 + y_0 + 2y_1 + 2y_2 + 2y_3 \geq 0$	3
$x_0 - x_2 + x_3 - y_0 + y_1 - y_3 \geq -2$	3
$-x_0 - x_2 - x_3 - y_0 + y_1 - y_3 \geq -4$	3
$-x_0 - x_1 - x_2 + x_3 + y_1 + y_3 \geq -2$	2
$3x_0 + x_1 + x_2 - 2x_3 + 2y_0 - y_1 + 2y_2 - y_3 \geq -1$	2
$x_1 + x_2 + y_0 - y_2 \geq 0$	2
$x_0 - x_1 - 2x_2 - x_3 + y_0 - 2y_2 + 2y_3 \geq -4$	2
$x_0 + x_1 + x_2 + 2x_3 - 2y_0 + y_1 + y_2 \geq 0$	2
$-x_0 - x_1 + x_2 - y_1 + y_2 \geq -2$	1
$x_0 + x_1 + x_2 - y_1 \geq 0$	1
$x_0 + x_2 - y_0 - y_1 - y_2 \geq -2$	1
Total	159

Table 4: The 2nd round input.

$x_{64} = y_0 + y_{40} + y_{52}$	$x_{80} = y_0$	$x_{96} = y_{28} + y_{40}$	$x_{112} = y_0 + y_{40}$
$x_{65} = y_1 + y_{41} + y_{53}$	$x_{81} = y_1$	$x_{97} = y_{29} + y_{41}$	$x_{113} = y_1 + y_{41}$
$x_{66} = y_2 + y_{42} + y_{54}$	$x_{82} = y_2$	$x_{98} = y_{30} + y_{42}$	$x_{114} = y_2 + y_{42}$
$x_{67} = y_3 + y_{43} + y_{55}$	$x_{83} = y_3$	$x_{99} = y_{31} + y_{43}$	$x_{115} = y_3 + y_{43}$
$x_{68} = y_4 + y_{44} + y_{56}$	$x_{84} = y_4$	$x_{100} = y_{16} + y_{44}$	$x_{116} = y_4 + y_{44}$
$x_{69} = y_5 + y_{45} + y_{57}$	$x_{85} = y_5$	$x_{101} = y_{17} + y_{45}$	$x_{117} = y_5 + y_{45}$
$x_{70} = y_6 + y_{46} + y_{58}$	$x_{86} = y_6$	$x_{102} = y_{18} + y_{46}$	$x_{118} = y_6 + y_{46}$
$x_{71} = y_7 + y_{47} + y_{59}$	$x_{87} = y_7$	$x_{103} = y_{19} + y_{47}$	$x_{119} = y_7 + y_{47}$
$x_{72} = y_8 + y_{32} + y_{60}$	$x_{88} = y_8$	$x_{104} = y_{20} + y_{32}$	$x_{120} = y_8 + y_{32}$
$x_{73} = y_9 + y_{33} + y_{61}$	$x_{89} = y_9$	$x_{105} = y_{21} + y_{33}$	$x_{121} = y_9 + y_{33}$
$x_{74} = y_{10} + y_{34} + y_{62}$	$x_{90} = y_{10}$	$x_{106} = y_{22} + y_{34}$	$x_{122} = y_{10} + y_{34}$
$x_{75} = y_{11} + y_{35} + y_{63}$	$x_{91} = y_{11}$	$x_{107} = y_{23} + y_{35}$	$x_{123} = y_{11} + y_{35}$
$x_{76} = y_{12} + y_{36} + y_{48}$	$x_{92} = y_{12}$	$x_{108} = y_{24} + y_{36}$	$x_{124} = y_{12} + y_{36}$
$x_{77} = y_{13} + y_{37} + y_{49}$	$x_{93} = y_{13}$	$x_{109} = y_{25} + y_{37}$	$x_{125} = y_{13} + y_{37}$
$x_{78} = y_{14} + y_{38} + y_{50}$	$x_{94} = y_{14}$	$x_{110} = y_{26} + y_{38}$	$x_{126} = y_{14} + y_{38}$
$x_{79} = y_{15} + y_{39} + y_{51}$	$x_{95} = y_{15}$	$x_{111} = y_{27} + y_{39}$	$x_{127} = y_{15} + y_{39}$

Table 5: Column hybrid constraint example.

Three XOR inputs	Position replacement	Two XOR inputs
	$x_{80} = y_0$	$x_{96} = y_{28} + y_{40}$ $y_{28} + y_{40} + x_{96} \geq 2d^{\oplus}$ $d^{\oplus} \geq y_{28}, d^{\oplus} \geq y_{40}, d^{\oplus} \geq x_{96}$ $y_{28} + y_{40} + x_{96} \leq 2$
$x_{64} = y_0 + y_{40} + y_{52}$	$x_{81} = y_1$	
$y_0 + y_{40} = u_0$	$x_{82} = y_2$	
$y_0 + y_{40} + u_0 \geq 2d^{\oplus}$	$x_{83} = y_3$	
$d^{\oplus} \geq y_0, d^{\oplus} \geq y_{40}, d^{\oplus} \geq u_0$	...	
$y_0 + y_{40} + u_0 \leq 2$	$x_{92} = y_{12}$	
$x_{64} + y_{52} + u_0 \geq 2d^{\oplus}$	$x_{93} = y_{13}$	
$d^{\oplus} \geq x_{64}, d^{\oplus} \geq y_{52} x_{64} + y_{52} + u_0 \leq 2$	$x_{94} = y_{14}$	
	$x_{95} = y_{15}$	

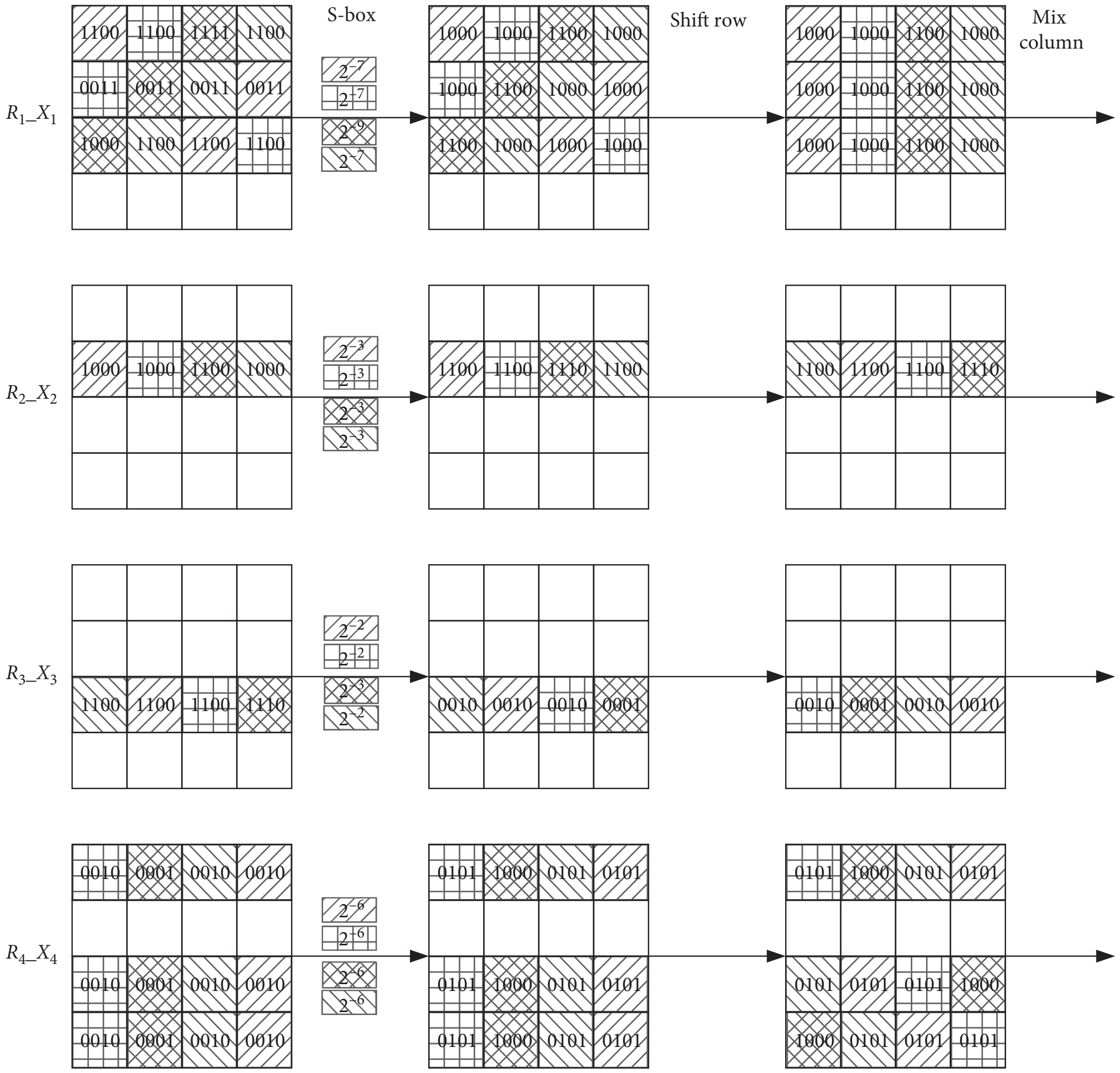

Figure 2: Four 4-round SKINNY-64 differential trails searched after optimizing the model.

constraint inequalities and 816 variables are included in the four rounds of skinny-64 differential trail MILP analysis model.

To find the differential trail, the number of active S-boxes needs to be determined. S-boxes with nonzero input and output differences are called active S-boxes. Generally, when the number of active S-boxes is determined, the greater the state differential probability in the S-box, the higher the probability of the differential trail. Similarly, the smaller the number of the minimum active S-boxes, the higher the probability of the differential trail [13]. In order to solve the minimum number of active S-boxes, the objective function is set:

$$\min \sum_{i=0}^{i=63} A_i. \qquad (2)$$

Among them, $A_i = \begin{cases} 1, & \text{the } S-\text{box is active}, \\ 0, & \text{otherwise}, \end{cases}$, i is the number of the difference units in each round.

Using the LPSolve software to solve the model, the minimum number of active S-boxes for four rounds is finally found to be 8, and the total probabilities of four 4-round differential trails are $2^{-18}(A_0=1)$, $2^{-18}(A_1=1)$, $2^{-21}(A_2=1)$, and $2^{-18}(A_3=1)$, and the result is shown in Figure 2.

The average successful search time is 16.0465s (the main configuration of the computer: Intel i7 8700, CPU frequency 3.2 GHz, memory 32G, hard disk 2 TB 7200RPM + 512 GB SSD). However, the experimental results show that these four trails are not optimal. This method is not conducive to the direct search of the optimal differential trail, which needs further improvement.

3. Improved SKINNY Differential Trail Search Method

The above method can search multiple differential trails with the minimum number of active S-boxes, but the trails with the minimum number of active S-boxes are not all optimal

Table 6: Probability information coding.

(p_i, q_i)	$P_r\,(x_{4i}, \ldots, x_{4i+3}, y_i, \ldots, y_{4i+3}), i \in (0, \ldots, 15)$
(0, 0)	2^{-0}
(0, 1)	2^{-2}
(1, 1)	2^{-3}

Table 7: All possible new differential characteristics for 1st round of SKINNY-64 S-box.

25 effective truncation inequalities	Number of invalid difference modes removed/inequalities
$-x_0 - x_1 - x_3 - y_0 + y_2 - y_3 - p_0 + 5q_0 \geq 0$	484
$-2x_1 - x_2 - x_3 - 2y_1 - y_2 - y_3 + 4p_0 + 4q_0 \geq 0$	127
$x_1 + x_2 + y_0 + y_1 - p_0 - q_0 \geq 0$	97
$x_1 - x_2 + x_3 - 3y_0 - y_1 + 2p_0 + 2q_0 \geq 0$	62
$x_0 - 2x_1 - 4x_2 - x_3 + y_1 + 2y_2 + 3y_3 + 5p_0 + q_0 > \ = 0$	30
$x_0 + 2x_1 + x_2 + y_0 - p_0 - q_0 \geq 0$	24
$2x_2 + y_0 + y_1 + y_2 - p_0 - q_0 \geq 0$	20
$-x_2 + 2y_0 + y_1 - y_2 + 2y_3 - p_0 + q_0 \geq 0$	16
$-3x_0 + 3x_1 + x_2 + 3x_3 - 2y_0 + 2y_1 - 2y_2 - y_3 + 5p_0 + 2q_0 \geq 0$	11
$x_2 + y_1 - p_0 \geq 0$	8
$-3x_1 + 2y_0 - y_1 + y_2 - y_3 + 2p_0 + 2q_0 \geq 0$	7
$3x_0 + 2x_1 + x_2 + 2x_3 - y_0 - y_2 - p_0 \geq 0$	6
$x_1 + y_0 - p_0 \geq 0$	6
$-2x_0 + x_1 - 2x_3 - y_0 + 2y_1 - y_3 - p_0 + 5q_0 \geq 0$	5
$-3x_0 - x_1 - x_2 - 2x_3 - 3y_0 - 2y_1 - y_2 + 2y_3 + 5p_0 + 7q_0 \geq 0$	4
$-x_0 - x_1 + x_2 - y_1 + y_2 + 2q_0 \geq 0$	3
$x_0 - x_1 - 3x_2 - 2x_3 - y_2 + y_3 + 2p_0 + 4q_0 \geq 0$	3
$x_0 - x_1 + x_3 - y_0 + y_1 + 2y_2 - y_3 + p_0 + q_0 \geq 0$	3
$-x_2 + x_3 - y_0 - y_1 - y_2 - y_3 + p_0 + 3q_0 \geq 0$	2
$-x_0 - x_1 - 3x_2 + x_3 - 2y_0 + 2y_1 - 2y_2 + y_3 + 4p_0 + 4q_0 \geq 0$	2
$x_0 + 2x_2 - y_0 - 3y_1 - y_2 + 2p_0 + 2q_0 \geq 0$	2
$-x_0 - x_1 - 3x_2 + x_3 - y_0 + y_2 + y_3 + 2p_0 + 3q_0 \geq 0$	2
$-x_1 - x_2 - x_3 - y_1 + y_2 - y_3 + p_0 + 3q_0 \geq 0$	1
$2x_0 + x_1 + 2x_3 - y_0 - y_2 - y_3 - p_0 + 2q_0 \geq 0$	1
$x_0 - x_2 + x_3 - y_0 - y_1 + 2y_2 + 2y_3 + 2p_0 \geq 0$	1
Total	927

differential trails. Therefore, the MILP model of SKINNY-64 needs to be improved to make it directly find the optimal differential trail.

3.1. New S-Box Differential Characteristic Based on Improved MILP Model. The improved MILP model is mainly to modify the S-box differential feature analysis of the above model, add probability coding information to the optimized MILP model, and reconstruct the S-box differential characteristic.

Each valid differential characteristic of 16 S-boxes $(x_{4i}, \ldots, x_{4i+3}, y_i, \ldots, y_{4i+3}), i \in (0, \ldots, 15)$, in the 1st round is combined with the corresponding probability information coding, to construct a new difference pattern $(x_{4i}, \ldots, x_{4i+3}, y_i, \ldots, y_{4i+3}, p_i, q_i) \in \mathbb{R}^{10}$.The coding method of probability information is shown in Table 6:

According to Table 6, the probability information of the S-box differential characteristic can be expressed as $2^{-(p_i + 2q_i)}$. The main idea of the improved method lies in the constraint of S-box difference mode and the choice of objective function. The constraints of the improved S-box model are combined with the coding information of the difference probability, which is closely related to the probability of the difference trail.

So, set the objective function to

$$\min \sum_{i=0}^{i=63} (p_i + 2q_i). \tag{3}$$

Although the S-box difference mode is changed after the probability coding information is added, the solution method is the same. Ninety seven new differential characteristics are available with the addition of probabilistic coding information, as shown in Table 7:

3.2. Analysis of Improved SKINNY-64 Four-Round MILP Model. After improving the model, the 1st round of SKINNY-64 difference analysis process contains 816 constraint inequalities and 320 variables. Therefore, SKINNY-64 four round differential trail MILP analysis model contains a total of 2928 constraint inequalities and 944 variables.

After the improvement, the optimal differential trail for SKINNY-64 4-round can be found directly. When the minimum number of S-box number in the 4-round is 4, the

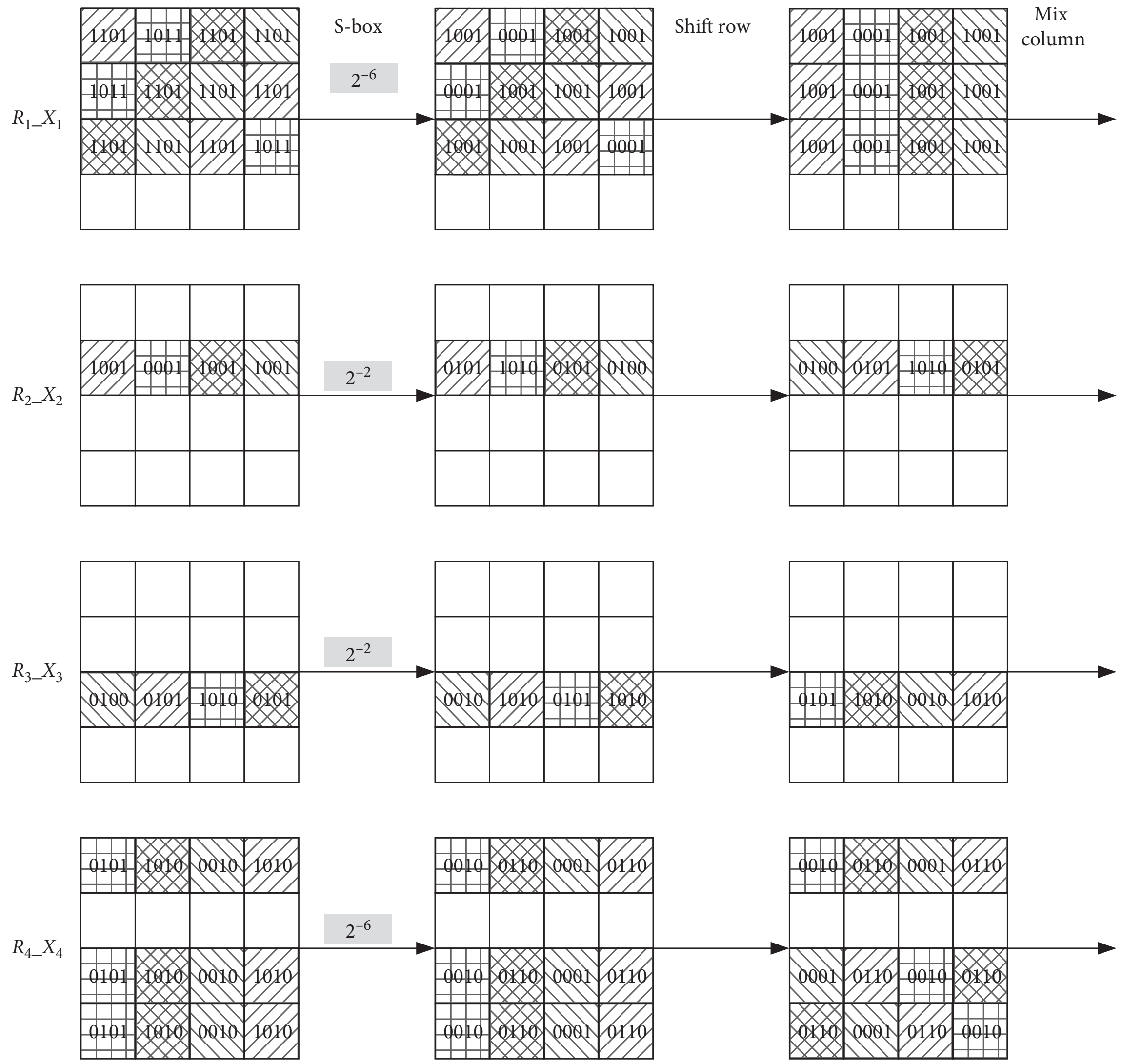

Figure 3: Four 4-round SKINNY-64 optimal differential trails searched after improving the model.

maximum probability of 4 optimal difference trails is 2^{-16}, which just satisfies the upper bound of the differential probability in the 4-round is shown in Figure 3. The experimental results show that the average successful search time is 19.8945s, which is only 3.848s more than the former (the main configuration of the computer: Intel i7 8700, CPU frequency 3.2 GHz, memory 32G, hard disk 2 TB 7200RPM + 512 GB SSD). Obviously, compared with the previous method, this direct search method has advantages in low rounds.

4. Conclusion

In this paper, mainly analyze all SKINNY-64 versions' differential trails under single-key setting. During the differential analysis, the key is assumed to be fixed, the round key difference is not considered, and only the state difference is considered. Therefore, the MILP model of all SKINNY-64 versions can be uniformly constructed. The state difference process of SKINNY is equivalently abstracted by specific constraints and variables to construct a MILP model. In order to improve the operation efficiency, the MILP model was optimized from two aspects: on the one hand, reducing the number of constraint inequalities, and on the other hand, reducing the number of variables. The optimized model reduces the number of constraints by 2912 and the number of variables by 64. However, the optimal trail cannot be searched directly in this scenario. In order to search the optimal trail more accurately, the MILP model is improved. The differential features of the S-box are reconstructed by adding the differential probability coding information of the S-box, and the model under the new difference mode of the S-box is obtained. Finally, the optimal difference trail of skinny-64 4-round is searched successfully. Our model has obvious advantages in searching the low rounds of SKINNY-64 the optimal differential trails under single-key setting.

Appendix

The partial procedure for generating efficient truncation inequality for S-box is given below.

A. Get 202 Linear Inequalities Describing the SKINNY-64 S-Box

Enter these difference vectors in SageMath 8.6 to achieve

```
myPoints=
[
[97 possible difference vectors]
]
poly_test=Polyhedron (vertices=myPoints)
for v in poly_test.inequality_generator():
print v
```

Finally, we can get the result.

B. Obtain the Optimal Linear Inequalities Describing the SKINNY-64 S-Box

//We reduce the 202 linear inequalities describing the SKINNY-64 S-box obtained in A, using the greedy algorithm and finally, we get the optimal linear inequalities describing the SKINNY-64 S-box. And an S-box only needs to be accurately described by 24 linear inequalities.

```
#include <stdio.h>
# define N1 300
# define N2 200
# define M 9
int choose(int x[N1][M],int y[N2][M-1])
{
int i, j, temp=0;
int z[N1]={0};
```

//How many points are not satisfied for each inequality.

```
for (i=0;i<N1;i++)
{
for(j=0;j<N2;j++)
if((x[i][0]*y[j][0]+x[i][1]*y[j][1]+x[i][2]*y[j][2]+x[i]
[3]*y[j][3]+x[i][4]*y[j][4]+x[i][5]*y[j][5]+x[i][6]*y
[j][6]+x[i][7]*y[j][7]+x[i][8])<0)
z[i]++;
}
temp=z[0]; j=0;
```

//Finding the inequality and its count is the largest.
//Number of differential modes removed for each inequality: z [i]

```
for(i=1;i<N1; i++)
{
if(z[i]>temp)
{j=i;temp=z[j];}
}
```

//The maximum number of differential modes removed is saved in temp

```
if(temp!=0)
{
```

//Delete the points corresponding to the largest inequality.

```
for(i=0;i<N2;i++)
{
if(x[j][0]*y[i][0]+x[j][1]*y[i][1]+x[j][2]*y[i][2]+x[j]
[3]*y[i][3]+x[j][4]*y[i][4]+x[j][5]*y[i][5]+x[j][6]*y
[i][6]+x[j][7]*y[i][7]+x[j][8]<0)
{
y[i][0]=0;y[i][1]=0;y[i][2]=0;y[i][3]=0;y[i][4]=0;y[i]
[5]=0;y[i][6]=0; y[i][7]=0;
}
}
```

//A corresponding inequality deletes the corresponding useless difference
//Output inequality and the number of points that are not satisfied.

```
for(i=0; i<8; i++)
{
if(x[j][i]<0||i=0)
printf("%d*x%d",x[j][i],i);
else
printf("+%d*x%d",x[j][i],i);
}
printf("+%d%6d",x[j][8],temp); printf("\n"); x[j][0]=0;
x[j][1]=0; x[j][2]=0; x[j][3]=0; x[j][4]=0; x[j][5]=0; x[j]
[6]=0; x[j][7=0; x[j][8]=0;
return temp;
}
else
return 0;
}
int main()
{
```

//In SageMath, the coefficients of the inequality of the s1-box are obtained.
//202 effective truncation inequalities

```
int  a[N1][M]={{0,-1,0,0,0,0,0,0,1},{-1,0,0,0,0,0,0,0,1},
. . ., {-1,-2,-1,-2,-1,-1,2,-2,8}};
```

//It does not satisfy the s-box.
//Because there are so many points, I'll just list some of them here.

```
int    b[N2][M-1]={{0,0,0,0,0,0,0,1},{0,0,0,0,0,0,1,0},. . .,
{1,1,1,1,1,1,1,0}};
printf(“inequalities counting\n”);
while(choose(a, b)=0)
choose(a, b);
return 0;
}
```

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the Hunan Natural Science Foundation of China (no. 2018JJ2533).

References

[1] C. Beierle, G. Leander, A. Moradi et al., “The SKINNY family of block ciphers and its low-latency variant MANTIS,” in *Proceeedings of the 36th Annual International Cryptology Conference*, pp. 123–153, Santa Barbara, CA, USA, August 2016.

[2] M. Tolba, A. Abdelkhalek, and A. M. Youssef, “Impossible differential cryptanalysis of reduced-round SKINNY,” in *Proceedings of the 9th International Conference on Cryptology in Africa*, pp. 117–134, Dakar, Senegal, May 2017.

[3] S. Sadegh, T. Mohammadi, and N. Bagheri, “Cryptanalysis of reduced round SKINNY block cipher,” *IACR Transactions on Symmetric Cryptology*, vol. 8, no. 2, pp. 124–162, 2018.

[4] H. Dou and S. Chen, “Improved impossible-differential cryptanalysis of reduced-round SKINNY,” *Journal of Cryptologic Research*, vol. 5, no. 2, pp. 126–139, 2018.

[5] N. Mouha, Q. Wang, D. Gu, and B. Preneel, “Differential and linear cryptanalysis using mixed-integer linear programming,” in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 57–76, Beijing, China, November 2012.

[6] S. Wu and M. Wang, “Security evaluation against differential cryptanalysis for block cipher structures,” 2011.

[7] T. Cui, “Security analysis of block cipher and stream ciphers,” Ph.D. thesis, Shangdong University, Jinan, China, 2018.

[8] 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 *Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 158–178, Taiwan, China, December 2014.

[9] E. Biham, O. Dunkelman, and N. Keller, “Related-key boomerang and rectangle attacks,” in *Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques*, Springer-Verlag, Berlin, Germany, 2005.

[10] S. Sun, L. Hu, M. Wang et al., “Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties,” 2014.

[11] G. Liu, M. Ghosh, and L. Song, “Security analysis of SKINNY under related-tweakey setting,” *IACR Transactions on Symmetric Cryptology*, vol. 3, pp. 37–72, 2017.

[12] P. Zhang and W. Zhang, “Differential cryptanalysis on block cipher skinny with MILP program,” *Security and Communication Networks*, vol. 5, pp. 28–39, 2018.

[13] J. Zhao, S. Xu, Z. Zhang et al., “Differential analysis of lightweight block cipher GIFT,” *Journal of Cryptologic Research*, vol. 5, no. 4, pp. 5–13, 2018.