Revisited Security Evaluation on Midori-64 against Differential Cryptanalysis

Guoyong Han[1], and Hongluan Zhao[2,*]
[1]Management School, Tianjin Normal University, Tianjin, China
[e-mail: hgy_126@126.com]
[2] School of Science, Tianjin Chengjian University, Tianjin, China
[e-mail: hongluanzhao@163.com]
*Corresponding author: Hongluan Zhao

Received March 23, 2023; revised November 19, 2023; accepted January 9, 2024; published February 29, 2024

Abstract

In this paper, the Mixed Integer Linear Programming (MILP) model is improved for searching differential characteristics of block cipher Midori-64, and 4 search strategies of differential path are given. By using strategy IV, set 1 S-box on the top of the distinguisher to be active, and set 3 S-boxes at the bottom to be active and the difference to be the same, then we obtain a 5-round differential characteristics. Based on the distinguisher, we attack 12-round Midori-64 with data and time complexities of 2^{63} and $2^{103.83}$, respectively. To our best knowledge, these results are superior to current ones.

Keywords: Midori-64, Block Cipher, Mixed Integer Linear Programming, Differential Distinguisher, Differential Cryptanalysis

1. Introduction

With the development of Information Technology and the improvement of wireless communication technologies, a lot of lightweight cipher algorithms have sprung up, such as LED, Piccolo, Midori [1], SKINNY, PRESENT, GIFT and KLEIN.

At present, some MILP models are used in the cryptanalysis of encryption algorithms, such as differential cryptanalysis, conditional differential cryptanalysis [2] and ID (impossible differential) cryptanalysis. MILP is the most important method in optimization. In 2011, the MILP model was applied to count the total of active S-boxes by Mouha et al. [3]. Then, Sun et al. improved this technique to look for differential paths [4], whose core thought is to depict all differential patterns of nonlinear layer by some linear inequalities, optimize and reduce the number of inequalities in 2014. Xiang et al. put the MILP method to several lightweight block ciphers [5]. Sasaki et al. looked for ID trail at EUROCRYPT 2017 [6]. In 2013, Sun et al. gave a 12-round differential path of PRESENT-80 [7]. Further, Sun et al. gave a method to look for the the high probability differential trail in 2014 [8]. Zhu et al. gave a 19-round differential cryptanalysis about GIFT-64 by a 12-round differential distinguisher [9]. In 2019, Cao et al. presented a 13-round differential trail of related-key based on MILP and attacked on 20-round of GIFT-64 [10].

Midori [1] is a lightweight ciphers presented at Asiacrypt 2015. It has been favored by many cryptographers since its release.

The research work of the distinguisher is as follows. In 2018, Zhang et al. gave a 7-round integral distinguisher [11]. In 2020, Moghaddam et al. showed the truncated differential characteristics for 4/5/6-round Midori-64 with the probability of $2^{-12}/2^{-24}/2^{-52}$ [12]. In 2021, Sun et al. gave a novel model based on SAT to search for the differential distinguisher [13]. Derbez et al. presented 6/7/9-round integral distinguishers with $2^{15}/2^{45}/2^{63}$ chosen plaintexts relying on MILP or SAT solvers [14]. In 2022, Li et al. gave the best valid 5/6-round differential distinguishers based on SAT with the probability of $2^{-46}/2^{-60}$ [15]. Kim et al. demonstrated the optimization of the search algorithm by obtaining the best differential and linear trails of some block ciphers [16]. In 2023, Baksi et al. provided a solution to search for differential distinguishers utilizing neural networks and support vector machines [17].

The above researches only give the solution of search distinguishers, but does not give the specific cryptanalysises of cipher algorithm. Among them, [16] only greatly improves the search speed, and does not give the specific distinguishers. The probabilities of these distinguishers in [12] and [15] are higher than those in this paper, but the characteristics of these distinguishers are not easy to spread and cannot attack more rounds.

In terms of related key attacks： Dong et al. gave a related-key differential cryptanalysis [18]. Gerault et al. attacked a 16-round Midori-64 utilizing a 15-round differential trail of related-key [19]. The related-key attack is weak because it assumes that part of the key could be modified, which might not be suitable for the practical scenario. Contrarily, our attack method is single key attack.

In terms of weak key attacks：Guo et al. presented an invariant subspace attack against full Midori-64 with 2^{32} weak key setting in 2016 [20]. Todo et al. provided an non-linear invariant attack against full Midori-64 with 2^{64} weak key setting [21]. In 2020, Beyne gave a 10-round integral cryptanalysis with 2^{96} weak keys and the data and time complexities of $2^{21.3}$ and 2^{56} [22]. These methods only verify if the key is one of the weak keys that satisfy certain conditions. They are not universal because the true keys may not be one of these weak keys.

The research work on single-key attack is as follows. In 2015, Lin et al. attacked on Midori-64 utilizing MITM distinguisher [23]. In 2016, Chen et al. presented a cryptanalysis using ID distinguisher [24]. In 2019, Li et al. showed an 11-round impossible differential cryptanalysis with data and time complexities of $2^{60.8}$ and $2^{121.4}$ [25]. In 2020, Zhao et al. gave an 11-round differential cryptanalysis with data and time complexities of $2^{55.6}/2^{61.2}$ and $2^{109.35}/2^{100.26}$ [26]. In 2023, Liu et al. gave an 11-round impossible differential cryptanalysis with data and time complexities of 2^{60} and $2^{116.59}$ [27].

In this paper, we listed a 12-round differential cryptanalysis on Midori-64 with data and time complexities of 2^{63} and $2^{103.83}$. We use single key attack which is an efficient attack, and give the details of the attack process and complexity calculation. Compared to [23], their computational complexity of 12-round attack is $2^{125.5}$, and our complexity is $2^{103.82}$, almost 2^{22} times that of ours. So, we have an absolute advantage. Compared to [24,25,27], the maximum number of rounds they attack are 10/11/11-round respectively, and ours is 12-round. At the same time, the computational complexity of our attack is much less than those of [25] and [27]. Compared to [26], we attack more one round than it.

Compared with [18] and [19], especially [19], they have great advantages in terms of the number of rounds, data complexity and computation complexity over us. However, their attack is the related-key attack which is weak. The principle of related key attack is to set the difference on the key, which is not easy to operate in practice. Contrarily, our attack method is single key attack which is a more effective attack method than related-key attack.

All the results of cryptanalysis of Midori-64 are summarized in **Table 1**.

Table 1. Summary of attacks on Midori-64

Rounds	Data	Computations	Attack Type	Reference
* Single-key Attack (full key space)				
10 (16)	$2^{61.5}$	$2^{99.5}$	Meet-In-the-Middle Attack	[23]
11 (16)	2^{53}	2^{122}	Meet-In-the-Middle Attack	[23]
12 (16)	$2^{55.5}$	$2^{125.5}$	Meet-In-the-Middle Attack	[23]
10 (16)	$2^{62.4}$	$2^{80.81}$	Impossible Differential Attack	[24]
11 (16)	$2^{60.8}$	$2^{121.4}$	Truncated Impossible Differential Attack	[25]
11 (16)	2^{60}	$2^{116.59}$	Impossible Differential Attack	[27]
11 (16)	$2^{55.6}$	$2^{109.35}$	Differential Cryptanalysis	[26]
11 (16)	$2^{61.2}$	$2^{100.26}$	Differential Cryptanalysis	[26]
12 (16)	2^{63}	$2^{103.82}$	Differential Cryptanalysis	Section 5.3
*** Related-key Attack (full key space)**				
14 (16)	2^{59}	2^{116}	Related-key Differential Cryptanalysis	[18]
16 (16)	$2^{23.75}$	$2^{35.8}$	Related-key Differential Cryptanalysis	[19]
*** Weak-key Attack (232 weak keys space)**				
16 (16)	2^{1}	2^{16}	Weak Key[invariant subspace]	[20]
16 (16)	2^{1}	2^{16}	Weak Key[non-linear invariant]	[21]
10 (16)	$2^{21.3}$	2^{56}	Integral/invariant[Based on Weak Key]	[22]

1.1 Our Contributions

In this paper, we mostly optimize the MILP model to look for the optimal differential paths in order to attack the longer rounds of cipher algorithms.

(1) We describe accurately the linear layer and the nonlinear layer to look for differential characteristics by some inequalities. Then the objective function is the maximal differential probability.

(2) Four search strategies of differential path are given. We present several 5-round differential distinguishers of Midori-64 with the probability of 2^{-46}, 2^{-52}, 2^{-58}, respectively. We find that different differences can be changed into the same difference through the S-box with a high probability. Then, set 1 S-box on the top of the distinguisher to be active, and set 3 S-boxes at the bottom to be active and the difference to be the same. We find a 5-round differential distinguishers which can be extended back for four rounds, and its probability is no less than 2^{-62}. Through analyzing these four differential search strategies in deep, we find that the fourth differential distinguisher has the highest efficiency, and can attack a 12-round Midori-64.

(3) Taking advantage of the fact that the three differences at the end of the distinguisher are the same, we give a 12-round differential cryptanalysis of Midori-64 with computational complexity of $2^{103.83}$ and data complexity of 2^{63}. We can take the differential cryptanalysis on Midori-64 one round further. Our results have the longest number of rounds, low data complexity and time complexity in single-key attacks.

1.2 Organization

The structure of the paper is as follows. The related works about MILP method are listed in Section 2. The brief description of Midori-64 and its MILP Model are described in Section 3. Section 4 presents some 5-round distinguishers of Midori-64. Differential cryptanalysis on 12-round Midori-64 is discussed in Section 5. Finally, we draw our conclusions.

2. Preliminaries

2.1 Notations

P, C, M : plaintexts, ciphertexts, the internal states.

ΔP, ΔC, ΔM : the difference in plaintexts, ciphertexts, the internal states.

S_i : the i-th S-box.

X_r, Y_r, Z_r, W_r : the internal state of the r-th round.

? : uncertain difference.

* : any non-zero difference.

2.2 Word-Oriented Related Work

Mouha et al.[3] used the MILP model earlier to count the total of active S-boxes. If there is a difference at any position in the word, the word is active.

Definition 1. Let $\Delta=(\Delta_0, \Delta_1, \Delta_2 \cdots, \Delta_{n-1})$, Δ_i is a byte. Then, the difference vector $x=(x_0, x_1, x_2 \cdots, x_{n-1})$, x_i is a bit, corresponding to Δ is as follows:

$$x_i = \begin{cases} 1, & \textit{there is a difference in any bit of } \Delta_i, \\ 0, & \textit{otherwise.} \end{cases} \quad (1)$$

$$S_i = \begin{cases} 1, & \textit{the S-Box marked by } S_i \textit{ is an active,} \\ 0, & \textit{otherwise.} \end{cases} \quad (2)$$

According to Definition 1, they formed the XOR and the linear transformation models.

Modeling the Linear Transformation. Let the input and outpue difference of linear transformation L be $(x_0, x_1, x_2 \cdots, x_{m-1})$ and $(y_0, y_1, \cdots, y_{m-1})$ respectively. In addition, let the differential branch number be B_D. These symbols should comply with the following regulations:

$$\begin{cases} \sum_{i=0}^{m-1} x_i + \sum_{i=0}^{m-1} y_i \geq B_D d_L \\ x_i \leq d_L, \ y_i \leq d_L, \ i \in \{0, 1, 2, \cdots, m-1\} \end{cases} \tag{3}$$

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

2.3 Bit-Oriented Related Work

Sun et al. [4] presented a scheme to describe all differential patterns for the S-box, which improved Mouha's work [3] to bit-oriented ciphers. They constructed the S-box operation model.

Describing the S-Box Operation. Let $(x_0, x_1, x_2 \cdots, x_{m-1})$ and $(y_0, y_1, \cdots, y_{m-1})$ be the input and output bit-level differences respectively. $S = 1$ holds if and only if $(x_0, x_1, x_2 \cdots, x_{m-1})$ are not all zero (i.e. S is active), where $S \in \{0,1\}$, a dummy variable.

$$\begin{cases} S - x_i \geq 0, \ i \in \{0, 1, \cdots, m-1\} \\ \sum x_i - S \geq 0 \end{cases} \tag{4}$$

3. Brief Description of Midori-64 and Its MILP Model

3.1 Description of the Midori-64 Cipher

Midori is a SPN block cipher and its overall structure is shown in **Fig. 1**. The state M (64 bits) of Midori-64 consists of 16 nibbles as follows:

$$M = \begin{bmatrix} m_0 & m_4 & m_8 & m_{12} \\ m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \end{bmatrix}.$$

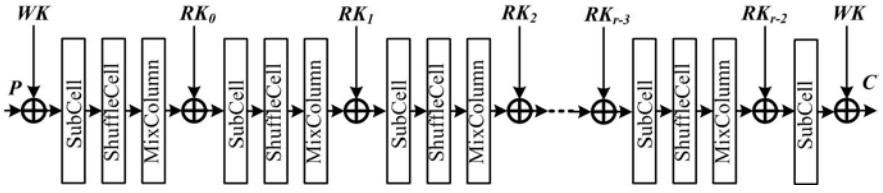

Fig. 1. The Round Function of Midori

Round Function. the round function is composed of the following 4 steps.

(1) SubCell: all 16 nibbles use the same S-box (Sb_0).

(2) ShuffleCell: the shufflecell operation is 16 nibbles out of order, and the rule is as

follows: $(z_0, z_1, z_2, \cdots, z_{15}) \leftarrow (y_0, y_{10}, y_5, y_{15}, y_{14}, y_4, y_{11}, y_1, y_9, y_3, y_{12}, y_6, y_7, y_{13}, y_2, y_8)$.

(3) MixColumn: a 4×4 involution matrix M (almost MDS matrix) is multiplied by 4 columns of the internal state as follows:

$$\begin{bmatrix} w_i \\ w_{i+1} \\ w_{i+2} \\ w_{i+3} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \bullet \begin{bmatrix} z_i \\ z_{i+1} \\ z_{i+2} \\ z_{i+3} \end{bmatrix}.$$

(4) KeyAdd: calculates the bitwise XOR of the internal state M and RK_i. The master Key K contains k_0 and k_1, where $WK = k_0 \oplus k_1$ and $RK_r = k_{r \bmod 2} \oplus \alpha_r, 0 \le r \le 14$. α_r is the round constant.

3.2 A precise description of S-Box

The numbers in Table2 are 16, 4, 2 and 0, i.e., the possible propagation probabilities 1 (16/16), 2^{-2} (4/16 = 1/4), 2^{-3} (2/16 = 1/8) and 0. Let's introduce two variables: (p_0, p_1). The difference pattern can be represented as follows.

$$\begin{cases} (p_0, p_1) = (0,0),\ if\ \ Pr_s[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)] = 16/16 = 1 \\ (p_0, p_1) = (0,1),\ if\ \ Pr_s[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)] = \ 2/16 = 2^{-3} \\ (p_0, p_1) = (1,0),\ if\ \ Pr_s[(x_0, x_1, x_2, x_3) \to (y_0, y_1, y_2, y_3)] = \ 4/16 = 2^{-2} \end{cases} \quad (5)$$

Table 2. DDT of Midori-64 S-Box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	4	0	2	2	2	0	2	0	0	0	0	0	2	0
2	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0
3	0	0	0	0	2	0	4	2	2	2	0	0	0	2	0	2
4	0	2	4	2	2	2	0	0	2	0	0	2	0	0	0	0
5	0	2	0	0	2	0	0	4	0	2	4	0	2	0	0	0
6	0	2	0	4	0	0	0	2	2	0	0	0	2	2	0	2
7	0	0	0	2	0	4	2	0	0	0	0	2	0	4	2	0
8	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
9	0	0	4	2	0	2	0	0	2	2	0	2	2	0	0	0
a	0	0	0	0	0	4	0	0	0	0	4	0	0	4	0	4
b	0	0	0	0	2	0	0	2	2	2	0	4	0	2	0	2
c	0	0	4	0	0	2	2	0	2	2	0	0	2	0	2	0
d	0	0	0	2	0	0	2	4	0	0	4	2	0	0	2	0
e	0	2	0	0	0	0	0	2	2	0	0	0	2	2	4	2
f	0	0	0	2	0	0	2	0	0	0	4	2	0	0	2	4

For example, the ninth row and the ninth column of DDT (**Table 2**) is 2. It means that the probability for $\Delta_{in}(=1001)$ with the corresponding $\Delta_{out}(=1001)$ is 2/16=2^{-3}. We represent it with (1, 0, 0, 1, 1, 0, 0, 1, 0, 1). Similarly, the probability of (0, 0, 0, 1, 0, 0, 1, 0, 1, 0) is 4/16=2^{-2}. Various differential modes of this S-box can be represented with the following 97 points. [0, 0, 0, 0, 0, 0, 0, 0, 0, 0], [0, 0, 0, 1, 0, 0, 0, 1, 0, 1], [0, 0, 0, 1, 0, 0, 1, 0, 1, 0], [0, 0, 0, 1, 0, 1, 0, 0, 0, 1], [0, 0, 0, 1, 0, 1, 0, 1, 0, 1],……, [1, 1, 1, 1, 0, 1, 1, 0, 0, 1], [1, 1, 1, 1, 1, 0, 1, 0, 1, 0], [1, 1, 1, 1, 1, 0, 1, 1, 0, 1], [1, 1, 1, 1, 1, 1, 1, 0, 0, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 0].

We can represent the 97 points above with 1304 linear inequalities whose forms are as follows. Then, 26 inequalities are left by optimizing.

$$\begin{cases} \alpha_{0,0}x_0+\alpha_{0,1}x_1+\alpha_{0,2}x_2+\alpha_{0,3}x_3+\alpha_{0,4}y_0+\alpha_{0,5}y_1+\alpha_{0,6}y_2+\alpha_{0,7}y_3+\alpha_{0,8}p_0+\alpha_{0,9}p_1+\gamma_0 \geq 0, \\ \alpha_{1,0}x_0+\alpha_{1,1}x_1+\alpha_{1,2}x_2+\alpha_{1,3}x_3+\alpha_{1,4}y_0+\alpha_{1,5}y_1+\alpha_{1,6}y_2+\alpha_{1,7}y_3+\alpha_{1,8}p_0+\alpha_{1,9}p_1+\gamma_1 \geq 0, \\ \cdots \\ \alpha_{n-1,0}x_0+\alpha_{n-1,1}x_1+\alpha_{n-1,2}x_2+\alpha_{n-1,3}x_3+\alpha_{n-1,4}y_0+\alpha_{n-1,5}y_1+\alpha_{n-1,6}y_2+\alpha_{n-1,7}y_3+\alpha_{n-1,8}p_0+\alpha_{n-1,9}p_1+\gamma_{n-1} \geq 0. \end{cases} \quad (6)$$

Finally the target function is the maximum probability, i.e., $\sum_{\min}(2\cdot p_0+3\cdot p_1)$.

3.3 Modeling the ShuffleCell Operation (SFC)

Assume the Δ_{in} and Δ_{out} of ShuffleCell operation be $(y_0, y_1, y_2, y_3, ..., y_{61}, y_{62}, y_{63})$ and $(z_0, z_1, z_2, z_3, ..., z_{61}, z_{62}, z_{63})$. 64 equalities can describe the Shuffle operation as follows:.

$$\begin{cases} y_0 - z_0 = 0 \\ y_1 - z_1 = 0 \\ \quad \vdots \\ y_{62} - z_{14} = 0 \\ y_{63} - z_{15} = 0 \end{cases} \quad (7)$$

3.4 Modeling the Multiple Bit XOR Operation

We transform the MC matrix into a bit matrix as follows:

$$\begin{bmatrix} 0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1 \\ 1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1 \\ 1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1 \\ 1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0 \end{bmatrix}$$

Assume the the Δ_{in} and Δ_{out} of MixColumn operation be $(x_0, x_1, x_2, x_3, ..., x_{61}, x_{62}, x_{63})$ and $(y_0, y_1, y_2, y_3, ..., y_{61}, y_{62}, y_{63})$. Since $y_0 = x_4 + x_8 + x_{12}$, we add intermediate variable u_1, $s.t.\ u_1 = x_4 + x_8$, $y_0 = u_1 + x_{12}$. So y_0 can be described by these inequalities as follows:

$$\begin{cases} x_4 + x_8 - u_1 \geq 0 \\ x_4 - x_8 + u_1 \geq 0 \\ -x_4 + x_8 + u_1 \geq 0 \\ x_4 + x_8 + u_1 \leq 2 \\ x_{12} + u_1 - y_0 \geq 0 \\ x_{12} - u_1 + y_0 \geq 0 \\ -x_{12} + u_0 + y_0 \geq 0 \\ x_{12} + u_1 + y_0 \leq 2 \end{cases} \quad (8)$$

4. Experimental Results of 5-Round for Midori-64

We can obtain the solution of the model through the Cplex optimizer. We can get the results of 5-round distinguishers for Midori-64 in 5 minutes, and these results are summarized in **Table 3** to **Table 5**. There are 4 differential distinguishers with the probability of 2^{-46}, 2^{-52}, 2^{-58} and 2^{-62} by different strategies.

Table 3. Summary of Differential Path for Midori-64

Round (all round)	#Variables	#Constraints	Probability
5 (16)	1360+64	4640	2^{-46} / 2^{-52} / 2^{-58} / 2^{-62}

4.1 Strategy I (3 Active S-boxes)

Let three S-boxes be active at the top of these distinguishers, and one S-box is active after one round, where the positions of these three S-boxes are in any set of $\{0,5,10,15\}$, $\{1,4,11,14\}$, $\{3,6,9,12\}$ and $\{2,7,8,13\}$. So there are 16 modes. The feature of the distinguishers is that the three active S-boxes must be on the same column after SFC operation. So, the total of active S-boxes in the first 5 rounds is 3,1,3,9,7, respectively. According to the rule of DDT, the maximum probability of differential transmission can be obtained as follows: $0xa \rightleftharpoons 0xa$, $0xb \rightleftharpoons 0xb$, $0xe \rightleftharpoons 0xe$, $0xf \rightleftharpoons 0xf$, $0x1 \rightleftharpoons 0x2$, $0x2 \rightleftharpoons 0x4$, $0x2 \rightleftharpoons 0x9$, $0x2 \rightleftharpoons 0xc$, $0x3 \rightleftharpoons 0x6$, $0x5 \rightleftharpoons 0x7$, $0x5 \rightleftharpoons 0xa$, $0x7 \rightleftharpoons 0xd$, $0xa \rightleftharpoons 0xd$, and $0xa \rightleftharpoons 0xf$ (14 cases). So, the probability of the distinguishers is $2^{-2*23} = 2^{-46}$.

The characteristics of these distinguishers are as follows. Full diffusion is achieved by extending forward 2 rounds and backward 2 rounds. So, we can attack a 9-round Midori-64 based on these distinguishers which have a high probability and a low number of extended rounds. An example of this type of distinguishers are shown in the left of **Table 4**.

Table 4. Two 5-round Differential Paths with the Probability of 2^{-46} and 2^{-52}

Input Round	Input Differential-1	Probability	Input Differential-2	Probability
1	A000 0A00 00A0 0000	-	A000 0000 00A0 0000	-
2	000A 0000 0000 0000	2^{-6}	AA00 0000 0000 0000	2^{-4}
3	0000 0000 A0AA 0000	2^{-8}	0AAA AAA0 0000 0000	2^{-8}
4	A0AA AA0A 0000 AAA0	2^{-14}	AA0A 0A0A 0A0A AA0A	2^{-20}
5	A0A0 AA00 0AA0 000A	2^{-32}	0A00 00AA 000A AA00	2^{-40}
6	AAAA A0AA 0AAA AA0A	2^{-46}	0000 00AA 00AA AA00	2^{-52}

4.2 Strategy II (2 Active S-boxes)

Let two S-boxes be active at the top of these distinguishers, and they are still active after one round, where the positions of these two S-boxes are in any set of $\{0,5,10,15\}$, $\{1,4,11,14\}$, $\{3,6,9,12\}$ and $\{2,7,8,13\}$. So there are 24 modes. The feature of the distinguishers is that the total of active S-boxes in the first 5 rounds is 2,2,6,10,6, respectively.

The characteristics of these distinguishers are as follows. Two active S-boxes can be transformed into the same column after SFC operation of the first round. After 5 rounds, there is no difference in one column, and there are 2 differences in other columns. Full diffusion is achieved by extending forward 3 rounds and backward 3 rounds. So, we can attack a 11-round Midori-64. An example of the type is shown in the right of **Table 4**.

4.3 Strategy III (1 Active S-boxes)

Let one S-box be active at the top of these distinguishers, and they is no other requirements. The distinguishers can extend forward 3 rounds. So, we can attack an 11-round Midori-64. An example of the type is shown in the left of **Table 5**.

Table 5. Two 5-round Differential Paths with the Probability of 2^{-58} and 2^{-62}

Input Round	Input Differential-3	Probability	Input Differential-4	Probability
1	A000 0000 0000 0000	-	δ 000 0000 0000 0000	-
2	0AAA 0000 0000 0000	2^{-6}	0AAA 0000 0000 0000	2^{-2}
3	0000 5550 A0AA AA0A	2^{-8}	0000 FFF0 5055 FF0F	2^{-8}
4	05AF 0AA0 AA7D 0A0A	2^{-14}	A000 0AA0 00AA D7DA	2^{-26}
5	5000 0077 00A0 5000	2^{-32}	500F A0A0 00AA 5055	2^{-44}
6	AA00 0000 FF5A 0555	2^{-46}	00A0 000A A000 0000	2^{-62}

$\delta \in \{5, A, D, F\}$

4.4 Strategy IV (1 Active S-boxes)

Let one S-box is active at the top of these distinguishers, and there are three active S-boxes after 5-round. These three S-boxes must be transformed into the same column after SFC operation. The distinguisher can extend forward 3 rounds and backward 4 rounds. So, we can attack a 12-round Midori-64. An example of the type is shown in the right of **Table 5** and **Fig. 2**.

Obviously, the positions of the differential cells on the bottom of the distinguisher are special. Then we can choose it to attack Midori-64.

5. Differential Attack on 12-Round Midori-64

5.1 The Property of Round Function

Property 1. Let $P\left((?,?,?,?)\rightarrow(?,?,?,0)\right)$ represent $P\left(SC(?,?,?,?)\rightarrow\left(MC(?,?,?,?)=(?,?,?,0)\right)\right)$, where $*\in\{1,2,3,4,.....,15\}$ (i.e. * is any nonzero difference) and $?\in\{*\cup\{0\}\}$, we can obtain the following probabilities easily.

$$\begin{cases} P\left((?,?,?,?)\rightarrow(?,0,?,?)\right)=\dfrac{1}{16}=2^{-4} \\ P\left((?,?,?,?)\rightarrow\begin{cases}(*,0,*,*)\\(0,*,*,*)\end{cases}\right)=\left(\dfrac{15}{16}\right)^3\times\dfrac{1}{16}\approx 2^{-4.28}\end{cases} \tag{9}$$

$$P\left(\begin{cases}(?,?,*,*)\\(?,*,?,*)\\(?,*,*,?)\end{cases}\rightarrow\begin{cases}(0,0,*,*)\\(0,*,0,*)\\(0,*,*,0)\end{cases}\right)=\left(\frac{1}{16}\right)^2=2^{-8} \tag{10}$$

$$P\left(\begin{cases}(?,?,?,0)\\(?,?,0,?)\\(?,0,?,?)\\(0,?,?,?)\end{cases}\rightarrow\begin{cases}(0,0,0,?)\\(0,0,?,0)\\(0,?,0,0)\\(?,0,0,0)\end{cases}\right)=\left(\frac{1}{16}\right)^2=2^{-8} \tag{11}$$

Property 2. If there is input differences(not necessarily equal) of S-box in 3 nibbles, and the output difference is identical, we can also get the following formulas, where $\Delta_i\in\{1,2,3,4,.....,15\}$.

$$P\left(\begin{cases}(*,*,*,0)\\(*,*,0,*)\\(*,0,*,*)\\(0,*,*,*)\end{cases}\rightarrow\begin{cases}(\Delta_i,\Delta_i,\Delta_i,0)\\(\Delta_i,\Delta_i,0,\Delta_i)\\(\Delta_i,0,\Delta_i,\Delta_i)\\(0,\Delta_i,\Delta_i,\Delta_i)\end{cases}\right)=\left(\frac{1}{15}\right)^2\approx 2^{-7.81} \tag{12}$$

5.2 Attack on 12-Round Midori-64

We can attack 12-round Midori-64 taking the advantage of the 5-round differential characteristic (δ, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) $\rightarrow$ (0, 0, A, 0, 0, 0, 0, A, A, 0, 0, 0, 0, 0, 0, 0) in **Table 5** and **Fig. 2**, where $\delta\in\{5,A,D,F\}$.

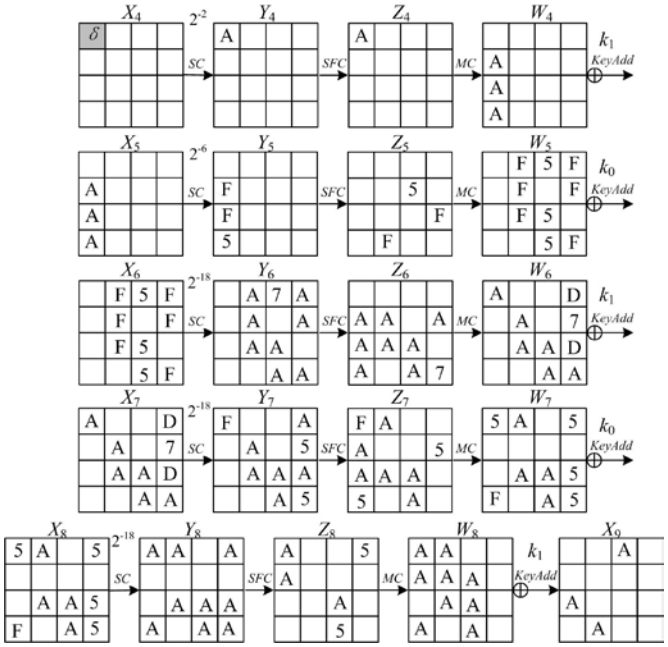

Fig. 2. A 5-round Differential Path of Midori-64 with Probability of 2^{-62}

The biggest advantage of this distinguisher is the positions of 'A' because the three 'A' can be in the same column after the operation of SFC. Then we can extend 4 rounds at the end of the distinguisher. Since only one cell is active at the beginning of the distinguisher, we can extend forward for 3 rounds (**Fig. 3**). The attack steps are as following.

1. Data Collection. Choose any 2^n plaintexts to compose 2^{2n-1} plaintext pairs. We can calculate these plaintext combinations to the intermediate state W_1. Since $P\left((?,?,?,?)\rightarrow(0,*,*,*)\right)=2^{-4.28}$ (Property 1), we can discard some ineligible pairs through $\Delta W_1[0,1,2,3]=\{0,*,*,*\}$ (**Fig. 3**). Similarly, we can discard some pairs through $\Delta W_1[4,5,6,7]=\{0,0,*,*\}$, $\Delta W_1[8,9,10,11]=\{0,*,0,*\}$ and $\Delta W_1[12,13,14,15]=\{0,*,*,0\}$.

Therefore, in the phase, we can obtain $2^{2n-1-4.28-8*3}=2^{2n-29.28}$ plaintext/cipertext combinations without infer any of keys.

2. The Master Key Recovery.

(1) First of all, we guess 12 bits $K_0[2,7,13]$. Since $P\left((*,*,0,*)\rightarrow(\Delta_3,\Delta_3,0,\Delta_3)\right)=2^{-7.81}$ (Property 2), we can throw away some ineligible pairs through $\Delta X_2[2,7,8,13]=\{*,*,0,*\}$ and $\Delta Y_2[2,7,8,13]=\{\Delta_3,\Delta_3,0,\Delta_3\}$ (**Fig. 3**).

Similarly, infer $K_0[1,11,14]$ and $K_0[3,6,9]$. We can discard some pairs through $\left(\Delta X_2[1,4,11,14]=\{*,0,*,*\}\right)\rightarrow\left(\Delta Y_2[1,4,11,14]=\{\Delta_1,0,\Delta_1,\Delta_1\}\right)$ and $\left(\Delta X_2[3,6,9,12]=\{*,*,*,0\}\rightarrow\left(\Delta Y_2[3,6,9,12]=\{\Delta_2,\Delta_2,\Delta_2,0\}\right)\right.$, respectively. So, the total of the left combinations is $2^{2n-29.28-7.81*3}=2^{2n-52.71}$.

(2) Subsequently, infer $K_1[5]$, $K_1[10]$ and $K_1[15]$ one by one in the 3rd round,. We can filter pairs by $\Delta Y_3[5]=\Delta Y_3[10]=\Delta Y_3[15]=\delta$, where $\delta\in\{5,A,D,F\}$ and the probability is $\frac{4}{15}\times\frac{1}{15}\times\frac{1}{15}\approx 2^{-9.72}$. There are $2^{2n-62.43}$ combinations left.

(3) In the 12th round, infer $MC^{-1}(K_1)[0,1,2,3,4,6,7,8,9,11,12,13,14]$. Then decrypt the eligible combinations to the intermediate state W_{11}. We can use the probability 2^{-4} of $\Delta W_{11}[0,1,2,3]=\Delta W_{11}[4,5,6,7]=\Delta W_{11}[8,9,10,11]=\Delta W_{11}[12,13,14,15]=\{?,0,?,?\}$, to filter combinations. After this round, we can obtain $2^{2n-78.43}$ eligible pairs.

(4) Similarly, infer $MC^{-1}(K_0)[0,4,8,10,12,15]$. We can filter pairs by $\Delta W_{10}[0,1,2,3]=\{0,0,0,?\}$, $\Delta W_{10}[4,5,6,7]=\{?,0,0,0\}$, $\Delta W_{10}[8,9,10,11]=\{0,0,?,0\}$ and $\Delta W_{10}[12,13,14,15]=\{0,?,0,0\}$, and the probability of $\left(2^{-8}\right)^4=2^{-32}$ (Property 1). Then we can obtain $2^{2n-110.43}$ eligible pairs.

(5) Decrypt these eligible combinations to the intermediate state W_9 and use the probability $2^{-4.28}$ of $\Delta W_9[12,13,14,15]=\{*,0,*,*\}$ to filter pairs. So, the total of the left combinations is $2^{2n-114.71}$.

(6) Finally, decrypt the remaining combinations to the intermediate state X_9 and we can filter combinations through $\Delta X_9[2,7,8]=\{A,A,A\}$ one by one. The probability of this round is $\frac{1}{15}\times\frac{1}{15}\times\frac{1}{15}=2^{-11.73}$. There are $2^{2n-126.44}$ eligible combinations left.

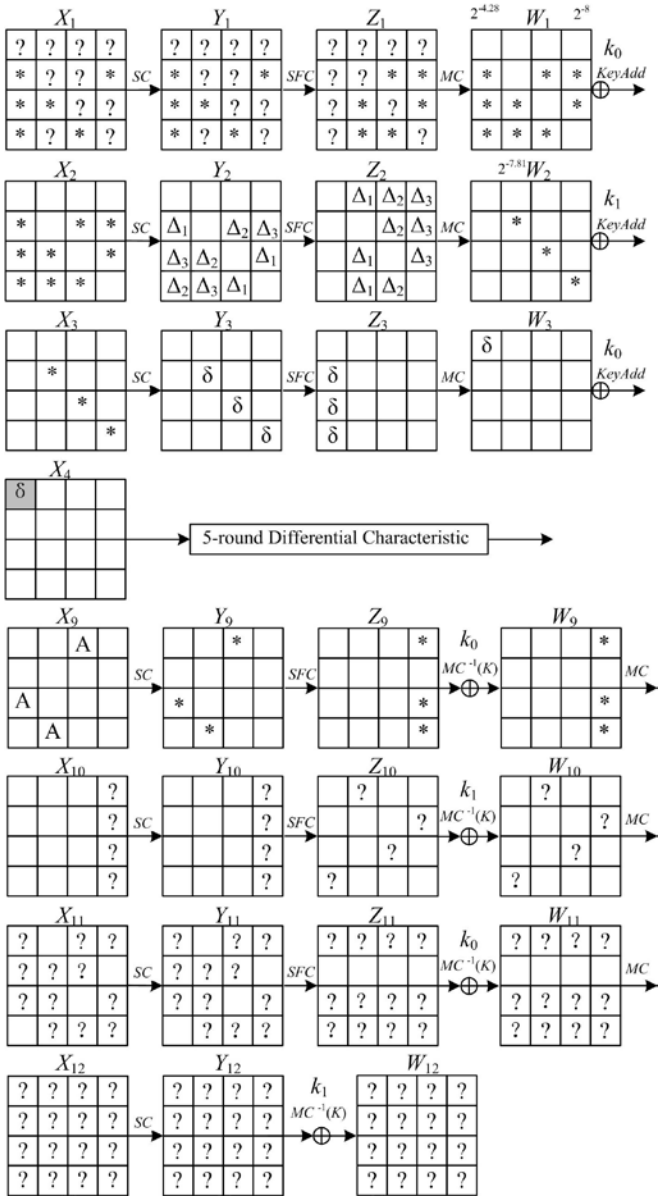

Fig. 3. 12-Round Differential Attack on Midori-64

5.3 Complexity Analysis

1. Data Complexity. Let n = 63, and we can select the correct key from the candidate keys well. For the correct one, there are $2^{2*63-62.43-62} \approx 3$ combinations left. However, $2^{2*63-126.44} \approx 2^{-0.44}$ combinations remain for a random key. This will be able to pick out the correct key. Note: the probability of the 5-round distinguisher and the first three rounds are is 2^{-62} and $2^{-61.43}$, Correspondingly. So, the data complexity is 2^{63} chosen plaintexts..

2. Calculation Complexity.

There are $2^{2n-29.28} = 2^{96.72}$ eligible combinations remained after the step of data collection.

(1) In the first round, guess 12 bits $K_0[1,11,14]$, the computation complexity is $2^{96.72} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{12} \approx 2^{103.82}$ 12-round encryptions. There are $2^{88.91}$ suitable pairs left.

Similarly, guess $K_0[2,7,13]$, and the computation complexity is $2^{88.91} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{12} \approx 2^{95.91}$ 12-round encryptions. There are $2^{81.10}$ suitable pairs left.

Then, guess $K_0[3,6,9]$, and the computation complexity is $2^{88.10}$ 12-round encryptions. There are $2^{73.29}$ suitable pairs left.

(2) Infer 12 bits $K_1[5,10,15]$ in the second round, and the computation complexity is $2^{73.29} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{12} \approx 2^{80.29}$ 12-round encryptions.

Because the complexity of the last four rounds is trivial compared to the first three rounds, we can ignore it. Thus, the total time complexity is $2^{103.83}$ 12-round encryptions.

6. Conclusion

In the paper, we mostly optimize the MILP model to look for the optimal differential paths in order to attack the longer rounds of Midori-64.

(1) We describe accurately the linear layer and the nonlinear layer to look for differential characteristics by some inequalities. Then the objective function is the maximal differential probability.

(2) Four search strategies of differential path are given. We present several 5-round differential distinguishers of Midori-64 with the probability of 2^{-46}, 2^{-52}, 2^{-58}, respectively. We find that different differences can be changed into the same difference through the S-box with a high probability. Then, set 1 S-box on the top of the distinguisher to be active, and set 3 S-boxes at the bottom to be active and the difference to be the same. We obtain a 5-round differential distinguishers which can be extended back for four rounds, and its probability is no less than 2^{-62}.

(3) Taking advantage of the fact that the three differences at the end of the distinguisher are the same, we give a 12-round differential cryptanalysis of Midori-64 with computation complexity of $2^{103.83}$ and data complexity of 2^{63}. We can take the differential cryptanalysis on Midori-64 one round further.

(4) Since the schedule of the round key is particularly simple, and we can easily to get the related-key differential distinguisher through extra 128 bit key variables.

Acknowledgements

This work is partially supported by National Natural Science Foundation of China (Nos. 62272282 and 61802235), and Doctor Foundation of Shandong Jianzhu University(Nos. XNB S20119).

References

[1] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A Block Cipher for Low Energy," in *Proc. of ASIACRYPT 2015, 21st International Conference on the Theory and Application of Cryptology and Information Security*, pp. 411-436, 2015. Article(CrossRefLink)

[2] Z. Xing, W. Zhang, and G. Han, "Improved Conditional Differential Analysis on NLFSR Based Block Cipher KATAN32 with MILP," in *Proc. of International Conference on Security and Privacy in New Computing Environments*, Springer, Cham, 2020. Article(CrossRefLink)

[3] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in *Proc. of International Conference on Information Security and Cryptology*, pp. 57-76, 2011. Article(CrossRefLink)

[4] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "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(CrossRefLink)

[5] Z. Xiang, W. Zhang, Z. Bao, and D. Lin, "Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers," in *Proc. of ASIACRYPT 2016, 22nd International Conference on the Theory and Application of Cryptology and Information Security*, Hanoi, Vietnam, December 4-8, Proceedings, Part I, pp. 648-678, 2016. Article(CrossRefLink)

[6] Y. Sasaki and Y. Todo, "New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers," in *Proc. of Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Paris, France, April 30 - May 4, Proceedings, Part III, pp. 185-215, 2017. Article(CrossRefLink)

[7] S. Sun, L. Hu, L. Song, Y. Xie, and P. Wang, "Automatic security evaluation of block ciphers with s-bp structures against related-key differential attacks," in *Proc. of International Conference on Information Security and Cryptology*, pp. 39-51, 2013. Article(CrossRefLink)

[8] S. Sun, L. Hu, M. Wang, P. Wang, K. Qiao, X. Ma, D. Shi, L. Song, and K. Fu, "Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties," *Cryptology ePrint Archive, Report 2014/747*, 2014. Article(CrossRefLink)

[9] B. Zhu, X. Dong, and H. Yu, "MILP-based Differential Attack on Round-reduced GIFT," *Cryptology ePrint Archive, Report 2018/390*, 2018. Article(CrossRefLink)

[10] M. Cao and W. Zhang, "Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT," *IEEE Access*, vol. 7, 175769-175778, 2019. Article(CrossRefLink)

[11] W. Zhang and V. Rijmen, "Division Cryptanalysis of Block Ciphers with a Binary Diffusion Layer," *IET Information Security*, 13(2), 87-95, 2019. Article(CrossRefLink)

[12] A. Moghaddam and Z. Ahmadian, "New Automatic Search Method for Truncated-Differential Characteristics Application to Midori, SKINNY and CRAFT," *The Computer Journal*, 63(12), 1813-1825, 2020. Article(CrossRefLink)

[13] L. Sun, W. Wang, and M. Wang, "Accelerating linear characteristics with the SAT method," *IACR Transactions on Symmetric Cryptology*, 2021(1), 269-315, 2021. Article(CrossRefLink)

[14] P. Derbez and P.A. Fouque, "Increasing Precision of Division Property," *Cryptology ePrint Archive, Report 2021/022*, 2021. Article(CrossRefLink)

[15] Y. Li and Q. Wang, "The SAT-Based Automatic Searching and Experimental Veriffcation for Differential Characteristics with Application to Midori64," *Cryptology ePrint Archive, Report 2022/1549*, 2022. Article(CrossRefLink)

[16] S. Kim, D. Hong, J. Sung, and S. Hong, "Accelerating the Best Trail Search on AES-Like Ciphers," *Cryptology ePrint Archive, Report 2022/643*, 2022. Article(CrossRefLink)

[17] A. Baksi, J. Breier, V.A. Dasu, X. Hou, H. Kim, and H. Seo, "New Results on Machine Learning Based Distinguishers," *Cryptology ePrint Archive, Report 2023/235*, 2023. Article(CrossRefLink)
[18] X. Dong and Y. Shen, "Cryptanalysis of Reduced-Round Midori64 Block Cipher," *Cryptology ePrint Archive, Report 2016/676*, 2016. Article(CrossRefLink)
[19] D. Gerault, and P. Lafourcade, "Related-Key Cryptanalysis of Midori," in *Proc. of INDOCRYPT 2016*, vol 10095, pp. 287-304, 2016. Article(CrossRefLink)
[20] J. Guo, J. Jean, I. Nikolić, K. Qiao, S. Yu, and S.M. Sim, "Invariant Subspace Attack Against Midori64 and the Resistance Criteria for Sbox Designs," *IACR Transactions on Symmetric Cryptology*, 2016 (1), pp. 33-56, 2016. Article(CrossRefLink)
[21] Y. Todo, G. Leander, and S. Yu, "Nonlinear Invariant Attack: Practical Attack on Full Scream, Iscream, and Midori64," in *Proc. of ASIACRYPT2016*, pp. 3-33, 2016. Article(CrossRefLink)
[22] T. Beyne, "Block Cipher Invariants as Eigenvectors of Correlation Matrices," *Journal of Cryptology*, 33(1), pp. 1156–1183, 2020. Article(CrossRefLink)
[23] L. Lin and W. Wu, "Meet-in-the-middle attacks on reduced-round Midori-64," *Cryptology ePrint Archive, Report 2015/1165*, 2015. Article(CrossRefLink)
[24] Z. Chen and X. Wang, "Impossible differential cryptanalysis of midori," *Cryptology ePrint Archive, Report 2016/535*, 2016. Article(CrossRefLink)
[25] M. Li, J. Guo, J. Cui, and L. Xu, "Truncated impossible differential cryptanalysis of Midori-64," *Journal of Software*, 30(8), pp. 2337-2348, 2019. Article(CrossRefLink)
[26] H. Zhao, G. Han, L. Wang, and W. Wang, "MILP-based Differential Cryptanalysis on Round-reduced Midori64," *IEEE Access*, vol. 8, pp. 95888-95896, 2020. Article(CrossRefLink)
[27] Y. Liu, Z. Xiang, S. Chen, S. Zhang, and X. Zeng, "A Novel Automatic Technique Based on MILP to Search for Impossible Differentials," *Cryptology ePrint Archive, Report 2023/227*, 2023. Article(CrossRefLink)

Guoyong Han received his Ph.D. from the School of Information Science and Engineering, Shandong Normal University, Jinan, China. He received the B.E. (2002) and the M.E.(2006)degrees from Shandong University, Jinan, China. He is an Associate Professor in Management School of Tianjin Normal University. His research interests include information security and analysis and design of block ciphers. He has published over 10 research papers in refereed academic journals and conferences.
(Email: hgy_126@126.com)

Hongluan Zhao received her Ph.D. from the School of Mathematics of the Shandong University in 2007. Currently, she is a Professor in School of Science of Tianjin Chengjian University. Her research interests include computer network and information security.
(Email: hongluanzhao@163.com)