IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

MILP-based Differential Cryptanalysis on Round-reduced Midori64

HONGLUAN ZHAO[1], GUOYONG HAN[2], LETIAN WANG[3], WEN WANG[2]

[1]School of Computer Science and Technology, Shandong Jianzhu University, Jinan, China
[2]School of Management Engineering, Shandong Jianzhu University, Jinan, China
[3]College of Information and Computer Engineering, Northeast Forestry University, Harbin, China

Corresponding author: Guoyong Han (e-mail: hgy_126@126.com).

This work is supported in part by National Natural Science Foundation of China (Nos. 61672330, 61602287, 61672328 and 11771256), and the Key Research Development Project of Shandong Province (No. 2018GGX106006), and Science and Technology Program of Shandong Provincial Education Department(No. J14LN13)

ABSTRACT Mixed integer linear programming (MILP) model was presented by Sun et al. at Asiacrypt 2014 to search for differential characteristics of block ciphers. Based on this model, it is easy to assess block ciphers against differential attack. In this paper, the MILP model is improved to search for differential trails of Midori64 which is a family of lightweight block ciphers provided by Banik et al. at Asiacrypt 2015. We find the best 5-round differential characteristics of Midori64 with MILP-based model, and the probabilities are 2^{-52} and 2^{-58} respectively. Based on these distinguishers, we give key recovery attacks on the 11-round reduced Midori64 with data complexities of $2^{55.6}$ and $2^{61.2}$, and time complexities of $2^{109.35}$ and $2^{100.26}$.

INDEX TERMS Midori, Differential distinguisher, Mixed integer linear programming, Differential cryptanalysis

I. INTRODUCTION

In recent years, a great deal of lightweight block ciphers are widely used in Internet of things and wireless communication because of their uncomplicated structures and efficient execution in low-power and constrained environment. Many lightweight block ciphers have emerged, such as Midori [1], GIFT [3], LED [5], PRESENT [4], PRINCE [6] and SPECK [7].

Differential cryptanalysis is one of the principal attack methods on modern symmetric-key ciphers, which evaluates a chosen-plaintext(ciphertext) attack and studies the effect of a pair of plaintext(ciphertext) differences on the output differences of the subsequent rounds. MILP is a central method, used to solve optimal problems in business and economics because it can diminish the workloads significantly by its efficient optimal results. It has been found that many classical cryptanalysis methods, including differential cryptanalysis, impossible differential, related-key differential characteristics and linear attacks can be converted into mathematical optimal problems. Once the cryptanalytical problem is converted to an MILP problem, it can be solved with MILP solvers such as CPLEX, SAT and SMT. Mouha et al. first introduced the MILP model to count the number of active S-boxes of word-oriented block ciphers in 2011 [8]. In 2013, Sun et al. gave the minimal number of active S-boxes for full-round PRESENT-80 and a 12-round related-key differential characteristics [11]. Further, they presented a novel method based the MILP model to search for the differential trails with the maximal probability, instead of the minimal number of active S-boxes [12]. Meanwhile, they improved this model to automatic search for differential pathes and linear trails [9], whose chief idea is to obtain a number of linear inequalities through the H-Representation of the convex hull of all differential patterns of S-box at ASIACRYPT 2014. Xiang et al. applied a MILP method to search for integral distinguisher [16]. At EUROCRYPT 2017, Sasaki et al. gave a new tool to automatic search for impossible differential trails [10]. Zhu et al. showed a 12-round differential characteristics and proposed a 19-round key-recovery attack for GIFT-64 [17]. Abdelkhalek et al. presented a novel MILP model bit-oriented for 8-bit or larger S-boxes [18]. Their main idea is to divide the difference distribution table (DDT) into several tables on the basis of the probability and control the behavior of these tables through adding conditional constraints. In [19], Canteaut et al. presented an in-depth study into the differential characteristics and introduced the method to attack the block cipher RoadRunneR. The MILP model has been used in cube attacks [25] and [28]. Later, a new MILP model

for searching better or even optimal choices of conditional cubes was proposed in [26]. Cui et al. search impossible differentials and zero-correlation linear approximations by a MILP model [27].

Midori [1] is a family of lightweight block ciphers which was presented at Asiacrypt 2015. However, numerous cryptographers have attacked it utilizing different cryptanalysis methods. In 2015, Lin et al. provided a 10/11/12-round attack on Midori64 based on a MITM distinguisher, with data complexity of $2^{61.5}$/$2^{53.5}$/$2^{55.5}$ chosen plaintexts and computational complexity of $2^{99.5}$/2^{122}/$2^{125.5}$ [13]. Dong et al. introduced an 11-round related-key differential distinguisher and attacked a 14-round on Midori64 with data complexity of 2^{59} and computational complexity of 2^{116} [14]. In 2016, Chen et al. presented a 6-round impossible differential distinguisher to attack 10-round of Midori64 [15], with data complexity of $2^{62.4}$ and computational complexity of $2^{80.81}$. Gerault et al. showed an all round related-key differential attack on Midori64 block cipher with data complexity of $2^{23.75}$ and computational complexity of $2^{35.8}$ [22]. Guo et al. provided an invariant subspace attack on all round Midori64 [23] with 2^{32} weak key setting in 2016.

Our Contributions. In this paper, we generalize an efficient MILP-based model inspired by Sun et al.'s model [9] and mainly concentrate on looking for the longest differential characteristics with the maximal probability. Utilizing this model, the attacker only gives the MILP instance with proper objective function and accurate description of S-box player and linear player by some inequalities. Then the left work can be done by an Optimizer such as CPLEX and Gurobi.

The model is constructed with an exact probability for each possible point in the DDT of S-box for Midori64 to search for the differential characteristics with the maximal differential probability by the optimal inequalities.

We present a 5-round differential characteristics with just two differential cells at the beginning and the maximal probability is no less than 2^{-52}. Based on the difference path, we provide an 11-round difference attack on Midori64 with data complexity of $2^{55.6}$ and computational complexity of $2^{109.35}$. Another 5-round differential characteristics is also shown with just one differential cell at the beginning and the maximal probability is no less than 2^{-58}. Based on the difference path, an 11-round difference attack is provided with data complexity of $2^{61.2}$ and computational complexity of $2^{100.26}$.

The model focuses on the differential characteristics mainly caused by plaintext differences. Since Midori has the little arrangement of the round key, it is effortless to obtain the related-key differential model through increasing 128 key variables into the model above.

A summary of the comparisons of our results with the preceding conclusion on Midori64 is presented in Table 1, where MITM, ID, RKD, IS and NLI represent meet-in-the middle, impossible difference, related-key difference, invariant subspace and non-linear invariant, respectively. We give the feasible and effective single key attack. However the previous invariant subspace attack and nonlinear invariant attack on Midori64 only verify whether the key is one of the weak keys. When the right key is not the weak key, these methods have little advantage. Moreover, the related-key attack is also weak because it supposes that some key bits can be adapted, which might not be easy to operate in the practical attack.

TABLE 1. Summary of key-recovery attacks on Midori64

Target algorithm	Round	Data	Computations	Attack Type	Reference
Midori64	10(16)	$2^{61.5}$	$2^{99.5}$	MITM	[13]
Midori64	11(16)	2^{53}	2^{122}	MITM	[13]
Midori64	12(16)	$2^{55.5}$	$2^{125.5}$	MITM	[13]
Midori64	10(16)	$2^{62.4}$	$2^{80.81}$	ID	[15]
Midori64	14(16)	2^{59}	2^{116}	RKD	[14]
Midori64	16(16)	$2^{23.75}$	$2^{35.8}$	RKD	[22]
Midori64	16(16)	2^{1}	2^{16}	IS	[23]
Midori64	16(16)	2^{1}	2^{16}	NLI	[24]
Midori64	11(16)	$2^{61.2}$	$2^{100.26}$	Differential	Sect. IV

Organization. This paper is organized as follows. The related work and our contribution are in Section I. The particular description of MILP model and Midori are listed in Section II. Applications to the block cipher Midori64 and the differential characteristics are showed in Section III. An 11-round differential attack on Midori64 is showed in Section IV. Finally, we draw our conclusions and summarize this paper.

II. PRELIMINARIES

A. NOTATIONS

P, $\triangle P$: plaintext, the difference in the plaintext.

C, $\triangle C$: ciphertext, the difference in the ciphertext.

M, $\triangle M$: the intermediate state, the difference in the intermediate state.

m_i : the i-th cell of the intermediate state M.

S, S_i : the S-box layer, the i-th S-box.

r : the round number.

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

$\triangle X_r\{i,j\}$: the i-th and j-th cells of the difference in X_r.

RK_r : the r-th round key.

? : any difference in one cell .

$*$, Δ : any non-zero difference in one cell.

$\oplus$: bit-wise exclusive or, that is, XOR.

$\|$: concatenation.

B. DESCRIPTION OF MIDORI

Midori is a lightweight substitution-permutation network (SPN) block cipher. The major frame is shown in Figure 1. The intermediate state M is as follows:

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2995795, IEEE Access

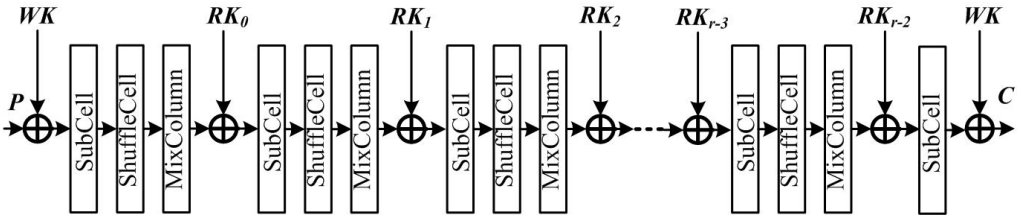

FIGURE 1. Overview of Midori.

TABLE 2. DDT of Midori64 S-box

m_i	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$Sb_0(m_i)$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

There are two versions namely Midori64 and Midori128 whose state sizes are 64 and 128 bits, the round number of 16 and 20, and the sizes of $m_i (0 \leq i \leq 15)$ being 4 and 8 bits, correspondingly. Each version has a key of 128 bit.

Round Function. The round function of Midori includes the following four.

1) SubCell (SC): the same invertible 4-bit S-box Sb_0, the only nonlinear component of the algorithm, is applied to each cell of Midori64, i.e., $Sb_0[m_i] \rightarrow m_i$, where $0 \leq i \leq 15$. (seen in TABLE 2)
2) ShuffleCell (SFC): the shuffle rule is as below: (m_0, m_1, m_2,$\cdots$, m_{13}, m_{14}, m_{15})$\leftarrow$ (m_0, m_{10}, m_5, m_{15}, m_{14}, m_4, m_{11}, m_1, m_9, m_3, m_{12}, m_6, m_7, m_{13}, m_2, m_8).
3) MixColumn (MC): a 4 $\times$ 4 matrix is applied to each column of the intermediate as below:

$$\begin{bmatrix} m_i \\ m_{i+1} \\ m_{i+2} \\ m_{i+3} \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} m_i \\ m_{i+1} \\ m_{i+2} \\ m_{i+3} \end{bmatrix},$$

where $i \in \{0, 4, 8, 12\}$.
Each cell indicates 4-bit and 8-bit for Midori64 and Midori128, correspondingly.
4) KeyAdd (AK): the round key RK_r is XORed with the intermediate M.

The last round function consists of two operations: SubCell and KeyAdd.

Key Schedule. The size of the master key (K)is 128 bits for two versions. For Midori64, K is composed of two 64-bit keys K_0 and K_1; that is, $K = K_0 \| K_1$. Then, $WK = K_0 \oplus K_1$ and $RK_r = K_{r \ mod \ 2} \oplus \alpha_r$, $0 \leq r \leq 14$. For Midori128, $WK = K$ and $RK_r = K \oplus \beta_r$, $0 \leq r \leq 18$. α_r and β_r are the round constants which are discussed at length in [1].

In this paper we mainly study Midori64.

C. MILP MODEL

Mouha et al. [8] first presented the MILP model to calculate the minimal number of active S-boxes for word-oriented block ciphers. Sun et al. [9] constructed the MILP model for bit-oriented block ciphers based on the work of Mouha et al. at Asiacrypt 2014.

Definition 1. For each input and output, we consider bit variable u_i to denote whether the bit has a difference. Then, the differential vector $u = (u_0, u_1, \cdots, u_{n-1})$ is as follows:

$$u_i = \begin{cases} 1, \text{there is a nonzero difference in this bit,} \\ 0, \text{otherwise.} \end{cases} \tag{1}$$

Constraints Describing the XOR Operation. Assume that the input difference for XOR is (u_1, u_2) and the output difference is v, where u_1, u_2 and v be a byte. The XOR operation is shown below:

$$\begin{cases} u_1 + u_2 + v \geq 2d^{\oplus} \\ u_1 \leq d^{\oplus}, \ \ u_2 \leq d^{\oplus}, \ \ v \leq d^{\oplus}, \end{cases} \tag{2}$$

where $d^{\oplus}$ is a dummy variable.

For bit-Oriented Block Ciphers, let the input difference be (u_1, u_2) and the corresponding output difference be v. The XOR operation can be described with the following linear constraints:

$$\begin{cases} u_1 + u_2 - v \geq 0 \\ u_1 - u_2 + v \geq 0 \\ -u_1 + u_2 + v \geq 0 \\ u_1 + u_2 + v \leq 2 \end{cases} \tag{3}$$

Constraints Describing the S-box Operation. Let (x_0, $x_1, \cdots, x_{u-1}$) and (y_0, $y_1, \cdots, y_{v-1}$) denote the input and output differences of a $u \times v$ S-box. S denotes whether the S-box is active or not. S = 0 holds if and only if all x_i are all zero, where $S \in \{0, 1\}$, a dummy variable.

$$\begin{cases} S - x_i \geq 0, \ \ i \in \{0, \cdots, u-1\} \\ \sum_{i=0}^{u-1} x_i - S \geq 0 \end{cases} \tag{4}$$

The Minimal Number of Active S-boxes. The objective function f of the earlier model is $\sum_{min} S_i$, i.e., the minimal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2995795, IEEE Access

number of active S-boxes. For Midori64, the DDT of S-box is seen in TABLE 3, and the numbers of zero points and non-zero points are 159 and 97. The next step is to distinguish these 97 points from the others. With the help of SageMath software, we can obtain 239 inequalities to distinguish these points, whose forms are as below.

$$\begin{cases} \alpha_{0,0}x_0 + \alpha_{0,1}x_1 + \alpha_{0,2}x_2 + \alpha_{0,3}x_3 + \alpha_{0,4}y_0 \\ \qquad +\alpha_{0,5}y_1 + \alpha_{0,6}y_2 + \alpha_{0,7}y_3 + \gamma_0 \geq 0 \\ \alpha_{1,0}x_0 + \alpha_{1,1}x_1 + \alpha_{1,2}x_2 + \alpha_{1,3}x_3 + \alpha_{1,4}y_0 \\ \qquad +\alpha_{1,5}y_1 + \alpha_{1,6}y_2 + \alpha_{1,7}y_3 + \gamma_1 \geq 0 \\ \qquad \cdots \\ \alpha_{n-1,0}x_0 + \alpha_{n-1,1}x_1 + \alpha_{n-1,2}x_2 + \alpha_{n-1,3}x_3 \\ +\alpha_{n-1,4}y_0 + \alpha_{n-1,5}y_1 + \alpha_{n-1,6}y_2 + \alpha_{n-1,7}y_3 \\ \qquad +\gamma_{n-1} \geq 0 \end{cases} \tag{5}$$

The number of inequalities can be reduced remarkably through a greedy algorithm [9]. Finally, 23 linear inequalities remain.

III. APPLICATIONS TO THE BLOCK CIPHER MIDORI64

1. Description of SubCell Operation.

The nonzero number in the DDT of Midori64 is 2,4 and 16. We need to add two extra bit-level variables (p_0, p_1) to represent the new differential pattern: $(x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3, p_0, p_1) \in F_2^{8+2}$. Since the probability of the input difference 0001 with the matching output difference 0001 is 2^{-3}, we indicate it with vector (0,0,0,1,0,0,0,1,0, 1). Analogously, the vector (0,0,0,1,0,0,1,0,1, 0) represents the probability of 2^{-2}.

TABLE 4. Differential Probability of S-box for Midori64

	(p_0, p_1)	probability
0	(0, 0)	1
1	(0, 1)	2^{-3}
2	(1, 0)	2^{-2}
3	(1, 1)	0

Thanks to the SageMath software and the greedy algorithm, there are 26 inequalities left (Equation (6)).

2. Description of ShuffleCell Operation.

According to the rules of ShuffleCell operation: (z_0, z_1, z_2,$\cdots$, z_{13}, z_{14}, 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), this step can be described by these 64 equalities as below:

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

3. Description of MixColumn Operation.

For Midori64, the matrix of MixColumn operation is

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

It is can be converted into a bit matrix with ease as below:

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

Let the input and output of MC operation be $(z_0, z_1, z_2, \cdots, z_{63})$ and $(w_0, w_1, w_2, \cdots, w_{63})$. In order to describe completely the MC operation, we introduced 40 intermediate variables and 448 inequalities. For example, $w_0 = z_4 + z_8 + z_{12}$. We add intermediate variable $t_1 = z_4 + z_8$, then $w_0 = t_1 + z_{12}$. So the expression of w_0 is as below:

$$\begin{cases} z_4 + z_8 - t_1 \geq 0 \\ z_4 - z_8 + t_1 \geq 0 \\ -z_4 + z_8 + t_1 \geq 0 \\ z_4 + z_8 + t_1 \leq 2 \\ z_{12} + t_1 - w_0 \geq 0 \\ z_{12} - t_1 + w_0 \geq 0 \\ -z_{12} + t_1 + w_0 \geq 0 \\ z_{12} + t_1 + w_0 \leq 2 \end{cases} \tag{8}$$

4. The objective function.

The objective function is the minimum $\sum_{min}(2 \cdot p_0 + 3 \cdot p_1 + \cdots + 2 \cdot p_{30} + 3 \cdot p_{31} + \cdots)$. Now, the MILP model is constructed by the above operations. We can obtain the optimal solution by utilizing Algorithm 1.

5. Experimental Results for Midori64.

TABLE 5. 5-round Differential Path of Midori64 with Probabilities 2^{-52} and 2^{-58}

Input Round	Input Differential-1	probability	Input Differential-2	probability
1	α000 0000 00β0 0000	1	δ000 0000 0000 0000	1
2	2200 0000 0000 0000	2^{-4}	0AAA 0000 0000 0000	2^{-2}
3	0444 1110 0000 0000	2^{-8}	0000 5550 A0AA AA0A	2^{-8}
4	2202 0202 0202 2202	2^{-20}	05AF 0AA0 AA7D 0A0A	2^{-26}
5	0400 0011 0001 1100	2^{-40}	5000 0077 00A0 5000	2^{-48}
6	0000 0022 0022 2200	2^{-52}	AA00 0000 FF5A 0555	2^{-58}

α, $\beta \in$ {1,4,9,C} and $\delta \in$ {5,A,D,F}.

The differential trails and probabilities are shown in TABLE 5, FIGURE 2 and FIGURE 3. The MILP instances are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2995795, IEEE Access

TABLE 3. DDT of Midori64 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

$$
\begin{cases}
-p0 - p1 \geqslant -1 \\
-x1 - x3 - y1 - y3 + 4p0 + 3p1 \geqslant 0 \\
-2x0 - x1 - x3 + 2y1 + 6y2 + 2y3 - 2p0 + 3p1 \geqslant 0 \\
3x0 + 3x1 - x2 + 3x3 + y1 - 2y2 + y3 - 2p1 \geqslant 0 \\
+2x1 + 6x2 + 2x3 - 2y0 - y1 - y3 - 2p0 + 3p1 \geqslant 0 \\
+x1 - 2x2 + x3 + 3y0 + 3y1 - y2 + 3y3 - 2p1 \geqslant 0 \\
-5x0 - 4x1 - 7x2 - x3 + 8y0 - y1 - 2y2 + 2y3 + 11p0 + 20p1 \geqslant 0 \\
8x0 + 2x1 - 2x2 - x3 - 5y0 - y1 - 7y2 - 4y3 + 11p0 + 20p1 \geqslant 0 \\
+x1 + 2x2 + x3 - 3y1 - 2y2 - 3y3 + 6p0 + 5p1 \geqslant 0 \\
-3x1 - 2x2 - 3x3 + y1 + 2y2 + y3 + 6p0 + 5p1 \geqslant 0 \\
2x0 + x1 + 4x2 + x3 - 3y0 - 2y1 + y2 - 2y3 + p0 + 3p1 \geqslant 0 \\
-2x0 - x1 - 2x2 + 3x3 - 2y0 + 3y1 - y2 - 3y3 + 7p0 + 8p1 \geqslant 0 \\
-4x0 - 2x1 + x2 - 2x3 + 2y0 + y1 + 5y2 + y3 + p0 + 4p1 \geqslant 0 \\
-x0 + 3x1 - 2x2 - x3 - 2y0 - 2y1 - y2 + 3y3 + 6p0 + 6p1 \geqslant 0 \\
2x0 + 2x2 - 2x3 + y1 - 2y2 - y3 + 4p0 + 3p1 \geqslant 0 \\
-x1 - 2x2 + x3 + 2y0 - 2y1 + 2y2 + 4p0 + 3p1 \geqslant 0 \\
+x1 - 3x2 - 2x3 + 3y0 + y1 + 2y2 - 2y3 + 5p0 + 4p1 \geqslant 0 \\
2x0 - 2x1 + 2x2 - y1 - 2y2 + y3 + 4p0 + 3p1 \geqslant 0 \\
+y1 - y2 + y3 + p0 \geqslant 0 \\
+x1 - 2x2 + x3 + y1 - 2y2 + y3 + 4p0 + p1 \geqslant 0 \\
x0 + 2x1 - x2 + 2x3 + y0 - y1 + y2 - y3 + 2p0 \geqslant 0 \\
-2x0 + x1 - x3 - 2y1 - y2 + y3 + 4p0 + 5p1 \geqslant 0 \\
-2x1 - x2 + x3 - 2y0 + y1 - y3 + 4p0 + 5p1 \geqslant 0 \\
-2x0 - 2x1 + x2 + 2x3 - y0 + y1 - 2y2 - 3y3 + 6p0 + 8p1 \geqslant 0 \\
-3x1 - x2 - x3 + 2y0 - y1 + y2 + 4y3 + 2p0 + 5p1 \geqslant 0 \\
+x1 + 2x2 + x3 - y0 + y1 + y2 + y3 - 2p0 \geqslant 0
\end{cases}
\tag{6}
$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.2995795, IEEE Access

Algorithm 1 The Accurate Difference Probabilities search algorithm based on MILP for Midori64.

Require: the round number r, intermediate state variables x_i, y_i, z_i, w_i, S-box's distribution probability p_j and the non-zero difference of the beginning in only one S-box.

Ensure: the maximal probability of the differential trail

1: Establish an empty MILP model MM.
2: Set x, y, z as the input of the SC, SFC and MC layer, and y, z, w as the output of the SC, SFC and MC layer.
3: p denotes the probability of the DDT.
4: Update MM according to the differential propagation rule of the round function.
5: Set the objective function: $\sum_{min}(2 \cdot p_0 + 3 \cdot p_1)$.
6: According to the conditional inequality obtained in step 4, solve model MM using the MILP optimizer.
7: A feasible solution is found in MM, and save it to a file.

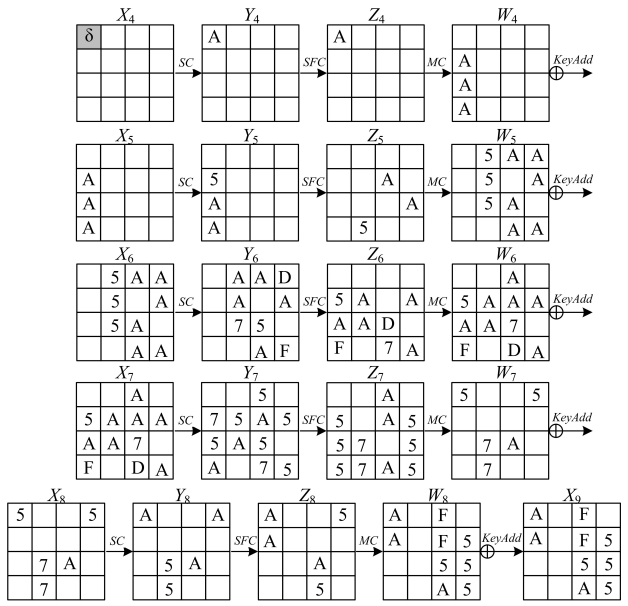

FIGURE 2. A 5-round Differential Path with probability of 2^{-58}.

run by the Cplex12.6 optimizer on a Lenovo Server(X3850 X6) with 64 GB RAM. A 5-round Midori64 model includes 1424 bit variables and 4640 conditional inequalities.

The model focuses on the differential characteristics mainly brought by plaintext differences. Since Midori has the little arrangement of the round key, it is effortless to obtain the related-key differential model through increasing 128 key variables into the model above.

IV. DIFFERENTIAL ATTACK ON 11-ROUND MIDORI64

A. THE PROPERTY OF PROBABILITY FOR ROUND FUNCTION

Property 1. Consider four cells of the intermediate state of SC with any input difference and any output difference. However we want one cell of these four with zero difference after MC operation. For example, let $X\{3, 6, 9, 12\}$ denote the

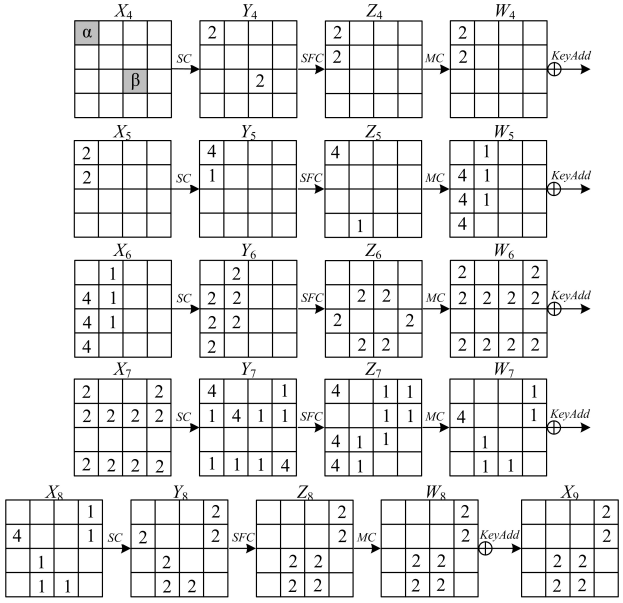

FIGURE 3. Another 5-round Differential Path with probability of 2^{-52}.

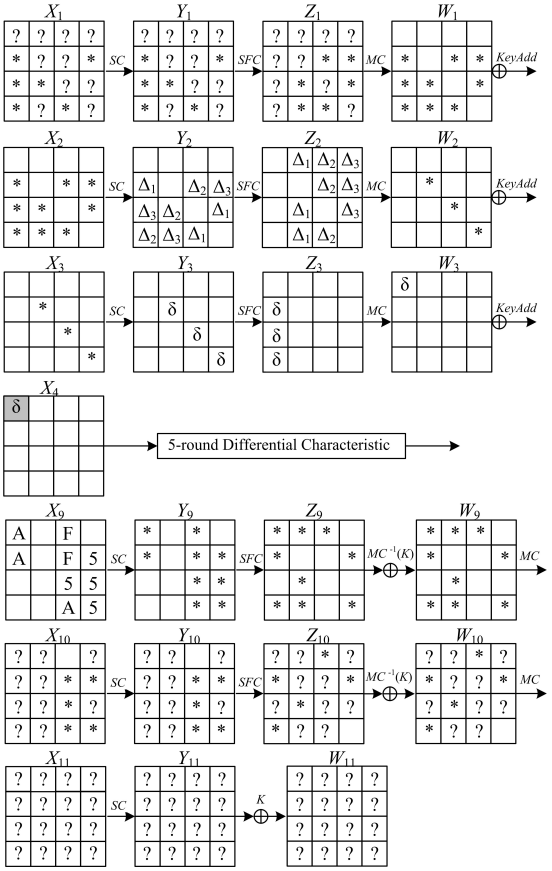

FIGURE 4. An 11-round Differential Attack on Midori64.

position(3,6,9,12) before SC operation and $Y\{3, 6, 9, 12\}$, $Z\{8, 9, 10, 11\}$, $W\{8, 9, 10, 11\}$ denote the corresponding position after SC, SFC, MC operation, respectively. Let

Δw_{11}=0, then $\Delta z_8 = \Delta z_9 \bigoplus \Delta z_{10}$ with the probability of $\frac{1}{16} = 2^{-4}$. Let $P((?,?,?,?) \rightarrow (?,?,?,0))$ denote $P(\ SC(?,?,?,?) \rightarrow (MC(?,?,?,?) = (?,?,?,0))\ )$. So, $P((?,?,?,?) \rightarrow (?,?,?,0)) = 2^{-4}$. Since $? \in \{0,1,2,3,4,5\cdots15\}$ and $* \in \{1,2,3,4,5\cdots15\}$, we can obtain $P((?,?,?,?) \rightarrow (?,?,*,0)) = \frac{15}{16} \times \frac{1}{16} \approx 2^{-4.09}$. Similarly, $P((?,?,?,?) \rightarrow (?,*,*,0)) \approx 2^{-4.19}$, and $P((?,?,?,?) \rightarrow (*,*,*,0)) \approx 2^{-4.28}$.

Property 2. Consider four cells of the intermediate state of SC with any input difference and any output difference. However we want no less than one cell of these four with non-zero difference after MC operation. We can obtain $P((?,?,?,?) \rightarrow (?,?,?,*)) = \frac{15}{16} \approx 2^{-0.09}$. Similarly, $P((?,?,?,?) \rightarrow (?,?,*,*)) \approx 2^{-0.19}$, and $P((?,?,?,?) \rightarrow (?,*,*,*)) \approx 2^{-0.28}$.

Property 3. Consider four cells of SC with two any input differences and two non-zero differences, then we want to get two zero difference after MC operation. We can obtain $P((?,?,*,*) \rightarrow (*,*,0,0)) = \frac{1}{16} \times \frac{1}{16} = 2^{-8}$ and $P((?,?,*,*) \rightarrow (?,?,0,0)) \approx 2^{-7.81}$.

Property 4. If there are three cells with any or any non-zero input differences of SC, and the same non-zero out differences of SC, we can obtain $P((?,?,?,0) \rightarrow (\Delta_1,0,0,0)) = \frac{15}{16} \times \frac{1}{16} \times \frac{1}{16} \approx 2^{-8.09}$ and $P((*,*,*,0) \rightarrow (\Delta_2,0,0,0)) \approx 2^{-7.81}$.

B. ATTACK ON 11-ROUND MIDORI64

Using the 5-round differential characteristic (δ, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)→(A, A, 0, 0, 0, 0, 0, 0, F, F, 5, A, 0, 5, 5, 5) with the probability of 2^{-58} in Table 5 and Figure 2, we could launch a key-recovery attack against 11-round Midori64. We choose the differential-2 rather than the differential-1 because the former is more effective.

Then add 3 rounds in its beginning and at the end respectively to attack 11-round reduced Midori64, shown in Figure 3. The attack procedures are as below.

1. Data Collection. Since the differences of plaintexts are all uncertain bits, plaintexts can not be classified by inactive bits. Choose any 2^n plaintexts and form approximately 2^{2n-1} plaintext pairs. Encrypt these plaintext pairs to state W_1 and use the difference $\triangle W_1\{0,1,2,3\} = \{0,*,*,*\}$ to filter pairs. By Property 1, this provides a filtering probability of $2^{-4.28}$ and there are approximately $2^{2n-5.28}$ pairs left.

Similarly, keep only the pairs such that $\triangle W_1\{4,5,6,7\} = \{0,0,*,*\}$, $\triangle W_1\{8,9,10,11\} = \{0,*,0,*\}$ and $\triangle W_1\{12,13,14,15\} = \{0,*,*,0\}$. By Property 3, the probability of these three cases is 2^{-8} and there are $2^{2n-29.28}$ pairs left. Therefore, in the data collection phase, the remaining number of the plaintext/cipertext pairs is approximately $2^{2n-29.28}$ only by the path choosing without guessing the key.

2. Key Recovery.

(1) Guess 12 bits $K_0\{1,11,14\} \bigoplus \alpha_0\{1,11,14\}$, then partially encrypt these plaintext pairs. As the middle values of right pairs should obey $\triangle X_2\{1,4,11,14\} = \{*,0,*,*\}$ and $\triangle Y_2\{1,4,11,14\} = \{\Delta_1,0,\Delta_1,\Delta_1\}$, the pairs can be filtered with a probability of $2^{-7.81}$ (Property 4), and the number of expected remaining pairs is $2^{2n-37.09}$. Similarly, guess $K_0\{2,7,13\} \bigoplus \alpha_0\{2,7,13\}$, and the right pairs should obey $\triangle Y_2\{2,7,8,13\} = \{\Delta_2,\Delta_2,0,\Delta_2\}$. Then, guess $K_0\{3,6,9\} \bigoplus \alpha_0\{3,6,9\}$, and the right pairs should obey $\triangle Y_2\{3,6,9,12\} = \{\Delta_3,\Delta_3,\Delta_3,0\}$. Totally there are $2^{2n-52.71}$ pairs left.

(2) For every remaining pair, guess 12 bits $K_1\{5,10,15\} \bigoplus \alpha_1\{5,10,15\}$ one by one, then encrypt these pairs. The right pairs should obey $\triangle Y_3\{5,10,15\} = \{\delta,\delta,\delta\}$ where $\delta \in$ {5,A,D,F}, and this round provides a filtering probability of $2^{-7.81} \times \frac{4}{15} \approx 2^{-9.72}$ (Property 4), and there are $2^{2n-62.43}$ pairs left.

(3) Guess $MC^{-1}(K_0 \bigoplus \alpha_{10})\{0,4,5,8,10,12,15\}$ and the rest bits can be obtained by $K_0 \bigoplus \alpha_0$. Then decrypt the left pairs to state W_{10} and use the difference $\triangle W_{10}\{0,1,2,3\} = \{?,*,?,*\}$, $\triangle W_{10}\{4,5,6,7\} = \{?,?,*,?\}$, $\triangle W_{10}\{8,9,10,11\} = \{*,?,?,?\}$ and $\triangle W_{10}\{12,13,14,15\} = \{?,*,?,0\}$ to filter pairs with the probability of $2^{-0.19}$, $2^{-0.09}$, $2^{-0.09}$ (Property 2) and $2^{-4.09}$ (Property 1), respectively. After this round, there are $2^{2n-66.89}$ pairs left.

(4) Similarly, guess $MC^{-1}(K_1 \bigoplus \alpha_9)\{0,1,2,3,4,6,7,8,9,11,12,13,14\}$, and the corresponding conditions in $\triangle W_9\{0,1,2,3\} = \{*,*,0,*\}$, $\triangle W_9\{4,5,6,7\} = \{*,0,*,*\}$, $\triangle W_9\{8,9,10,11\} = \{*,0,0,0\}$ and $\triangle W_9\{12,13,14,15\} = \{0,*,0,*\}$ to filter pairs with the probability of $2^{-4.28}$, $2^{-4.28}$ (Property 1), $2^{-7.81}$ (Property 4) and 2^{-8} (Property 3), respectively. After this round, there are $2^{2n-91.26}$ pairs left.

(5) Finally, decrypt the left pairs to state X_9 and use the difference $\triangle X_9\{0,1,8,9,10,11,13,14,15\} = \{$A,A,F,F,5,A,5,5,5$\}$ one by one to filter pairs with the total probability of $2^{-35.19}$. There are $2^{2n-126.45}$ pairs left.

C. COMPLEXITY ANALYSIS

1. Data Complexity.

In order to distinguish the correct key from the wrong key, choose n = 61.2. For a random key, there are $2^{2\times61.2-126.45} \approx 2^{-4.05}$ pairs left. However, for the right key, there are $2^{2\times61.2-62.43-58} \approx 4$ pairs left as the probability of the 5-round differential Path is 2^{-58}. So, the data complexity is $2^{61.2}$ chosen plaintexts.

2. Time Complexity.

(1) There are $2^{2n-29.28} = 2^{93.12}$ pairs left after the phase of data collection. Guess 12 bits $K_0\{1,11,14\} \bigoplus \alpha_0\{1,11,14\}$, then partially encrypt these plaintext pairs for one round. The time complexity is $2^{93.12} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{11} \approx 2^{100.25}$ 11-round encryptions, and the number of remaining pairs is $2^{85.31}$.

Similarly, guess $K_0\{2,7,13\} \bigoplus \alpha_0\{2,7,13\}$, and the time complexity is $2^{85.31} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{11} \approx 2^{92.44}$ 11-round encryptions, and the number of remaining pairs is $2^{77.5}$.

Then, guess $K_0\{3,6,9\} \bigoplus \alpha_0\{3,6,9\}$, and the time complexity is $2^{84.63}$ 11-round encryptions, and the number of

remaining pairs is $2^{69.69}$.

(2) For every remaining pair, guess 12 bits $K_1\{5,10,15\} \bigoplus \alpha_1\{5,10,15\}$, and the time complexity are $2^{69.69} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{11} \approx 2^{76.82}$ 11-round encryptions, and the number of remaining pairs is $2^{59.97}$.

(3) Guess $MC^{-1}(K_0 \bigoplus \alpha_{10})\{1,2,3,6,7,9,11,13,14\}$ and, for the whole round, the time complexity is $2^{59.97} \times 2 \times 2^{28} \times \frac{1}{11} \approx 2^{85.51}$ 11-round encryptions, and the number of remaining pairs is $2^{55.51}$.

(4) Similarly, guess $MC^{-1}(K_1 \bigoplus \alpha_9)\{1,6,8\}$, and the time complexity is $2^{55.51} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{11} \approx 2^{62.64}$ 11-round encryptions, and the number of remaining pairs is $2^{47.7}$.

Guess $MC^{-1}(K_1 \bigoplus \alpha_9)\{3,4,13\}$, and the time complexity is $2^{47.7} \times 2 \times 2^{12} \times \frac{4}{16} \times \frac{1}{11} \approx 2^{55.24}$ 11-round encryptions, and the number of remaining pairs is $2^{39.7}$.

Guess $MC^{-1}(K_1 \bigoplus \alpha_9)\{0,7,9,14\}$, and the time complexity is $2^{39.7} \times 2 \times 2^{16} \times \frac{4}{16} \times \frac{1}{11} \approx 2^{51.24}$ 11-round encryptions, and the number of remaining pairs is $2^{35.42}$.

Guess $MC^{-1}(K_1 \bigoplus \alpha_9)\{2,11,12\}$, and the time complexity is $2^{35.42} \times 2 \times 2^{12} \times \frac{3}{16} \times \frac{1}{11} \approx 2^{42.55}$ 11-round encryptions, and the number of remaining pairs is $2^{31.14}$.

(5) Finally, the time complexity is $2^{31.14} \times 2 \times \frac{9}{16} \times \frac{1}{11} \approx 2^{27.85}$ 11-round encryptions.

Thus, the total time complexity is $2^{100.26}$ 11-round encryptions.

D. COMPLEXITY ANALYSIS OF ANOTHER DIFFERENTIAL PATH WITH PROBABILITY OF 2^{-52}

Similarly, add 3 rounds in its beginning and at the end of the differential path with probability of 2^{-52} to attack 11-round reduced Midori64. It is easy to get the probability of $2^{-56.18}$ for the top 3 rounds. So we choose n = 55.6. For a random key, there are $2^{2\times55.6-1-56.18-64} \approx 2^{-10}$ pairs left. However, for the right key, there are $2^{2\times55.6-1-56.18-52} \approx 4$ pairs left as the probability of the 5-round differential Path is 2^{-52}. So, the data complexity is $2^{55.6}$ chosen plaintexts, and the time complexity is $2^{109.35}$ 11-round encryptions, Correspondingly.

V. CONCLUSION

In this paper, the MILP method model is improved to search for differential characteristics by considering the probability of differential propagation. Our results are more precise than that of counting the minimal number of active S-boxes.

(1) The model is constructed with an exact probability for each possible point in the DDT of S-box for Midori64 to search for the differential characteristics with the maximal differential probability by the optimal inequalities.

(2) We present a 5-round differential characteristics with just two differential cells at the beginning and the the maximum probability is no less than 2^{-52}. Based on the difference path, we provide an 11-round difference attack on Midori64 with data complexity of $2^{55.6}$ and computational complexity of $2^{109.35}$. Another 5-round differential characteristics is also shown with just one differential cell at the beginning and the maximum probability is no less than 2^{-58}. Based on the difference path, an 11-round difference attack is provided with data complexity of $2^{61.2}$ and computational complexity of $2^{100.26}$.

(3) The model considers only the differential characteristics caused by plaintext differences. However, the schedule of the round key is little arrangement, and it is easy to obtain the related-key differential model by adding 128 key variables into the above model.

REFERENCES

[1] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T. and Regazzoni, F.: Midori: A Block Cipher for Low Energy. ASIACRYPT 2015, 21st International Conference on the Theory and Application of Cryptology and Information Security, LNCS, Springer 2015, vol. 9453, pp. 411-436. (2015)

[2] Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A. and Peyrin, T., et al.: The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. CRYPTO 2016, Springer-Verlag New York Inc., vol. 9815, pp.123-153. (2016)

[3] Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: Cryptographic Hardware and Embedded Systems - CHES 2017. pp. 321-345. https://doi.org/10.1007/978-3-319-66787-4_16. (2017)

[4] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y. and Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2007. pp. 450-466 (2007), https://doi.org/10.1007/978-3-540-74735-2_31. (2007)

[5] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED block cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings. pp. 326-341, http://dx.doi.org/10.1007/978-3-642-23951-9_22. (2011)

[6] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçcin, T.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, pp. 208-225. Springer (2012)

[7] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S.,Weeks, B., Wingers, L.: The simon and speck families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, https://eprint.iacr.org/2013/404. (2013)

[8] Mouha, N., Wang, Q., Gu, D. and Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: International Conference on Information Security and Cryptology. pp. 57-76. (2011)

[9] Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X. and Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 158-178. (2014)

[10] Sasaki, Y. and Todo, Y.: New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers. In: Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III. pp. 185-215, http://dx.doi.org/10.1007/978-3-319-56617-7_7. (2017)

[11] Sun, S., Hu, L., Song, L., Xie, Y. and Wang, P.: Automatic security evaluation of block ciphers with s-bp structures against related-key differential attacks. 2013, 8567:39-51. (2013)

[12] Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., Shi, D., Song, L. and Fu, K.: Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics 16with predefined properties. Cryptology ePrint Archive, Report 2014/747, http://eprint.iacr.org/2014/747. (2014)

[13] Lin, L. and Wu, W.: Meet-in-the-middle attacks on reduced-round Midori64. Cryptology ePrint Archive, Report 2015/1165, http://eprint.iacr.org/2015/1165. (2015)

[14] Dong X. and Shen, Y.: Cryptanalysis of Reduced-Round Midori64 Block Cipher. Cryptology ePrint Archive, Report 2016/676, http://eprint.iacr.org/2016/676. (2016)

[15] Chen, Z. and Wang, X.: Impossible differential cryptanalysis of midori. Cryptology ePrint Archive, Report 2016/535, http://eprint.iacr.org/2016/535. (2016)
[16] Xiang, Z., Zhang, W., Bao, Z. and Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. ASIACRYPT 2016, 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I. pp. 648-678 (2016), http://dx.doi.org/10.1007/978-3-662-53887-6_24. (2016)
[17] Zhu, B., Dong, X. and Yu, H.: MILP-based Differential Attack on Round-reduced GIFT. Cryptology ePrint Archive, Report 2018/390, http://eprint.iacr.org/2018/390. (2018)
[18] Abdelkhalek, A., Sasaki, Y., Todo, Y., Tolba, M., and Youssef, A.: MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics. IACR Transactions on Symmetric Cryptology, Vol. 2017, No. 4, pp. 99-129. (2017)
[19] Canteaut, A., Lambooij, E., Neves, S., Rasoolzadeh, S., Sasaki, Y. and Stevens, M.: Refined probability of differential characteristics including dependency between multiple rounds. IACR Transactions on Symmetric Cryptology, 2017.
[20] CPLEX: IBM software group, CPLEX 12.6. (2011)
[21] Gurobi: Gurobi optimizer reference manual. URL: http://www. gurobi. com. (2012)
[22] Gerault, D., Lafourcade, P.: Related-Key Cryptanalysis of Midori. INDOCRYPT 2016, Lecture Notes in Computer Science, vol 10095, pp. 287-304, https://doi.org/10.1007/978-3-319-49890-4_16. (2016)
[23] Guo, J., Jean, J., Nikolić, I., et al.: Invariant Subspace Attack Against Midori64 and the Resistance Criteria for S-box Designs. IACR Transactions on Symmetric Cryptology, 2016 (1), pp. 33-56. (2016)
[24] Todo, Y., Leander, G., Yu, S.: Nonlinear Invariant Attack: Practical Attack on Full Scream, Iscream, and Midori64. ASIACRYPT 2016, Lecture Notes in Computer Science, Springer, 10031, pp. 3-33. (2016)
[25] Li, Z., Bi, W., Dong, X. and Wang, X.: Improved Conditional Cube Attacks on Keccak Keyed Modes with MILP Method. In Tsuyoshi Takagi and Thomas Peyrin, editors, ASIACRYPT 2017, Part I, LNCS, Springer, vol. 10624, pp. 99-127. (2017)
[26] Song, L., Guo, J., Shi, D. and Ling, S.: New MILP Modeling: Improved Conditional Cube Attacks on Keccak-Based Constructions. In Peyrin T., Galbraith S., editors, ASIACRYPT 2018, LNCS, Springer, vol. 11273, pp. 65-95. (2018)
[27] Cui, T., Chen, S., Jia, K., Fu, K. and Wang, M.: New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations. Cryptology ePrint Archive, Report 2016/689, http://eprint.iacr.org/2016/689. (2016)
[28] Todo, Y., Isobe, T., Hao, Y., et al.: Cube Attacks on Non-Blackbox Polynomials Based on Division Property. IEEE Transactions on Computers, 67 (12), pp. 1720-1736. (2017)

HONGLUAN ZHAO received her PhD from School of Mathematics of Shandong University in 2007. Currently, she is a Professor in School of Computer Science and Technology of Shandong Jianzhu University. Her research interests include computer network and information security.(Email:hongluanzhao@163.com)

GUOYONG HAN received his Ph.D. degree (2019) in School of Information Science and Engineering, Shandong Normal University, Jinan, China. He received B.E. (2002), and M.E. (2006) degrees from Shandong University, Jinan, China. He is an Associate Professor in School of Management Engineering of Shandong Jianzhu 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)

LETIAN WANG is a sophomore in School of Computer Science and Technology, Northeast Forestry University, Harbin, China. He is a member of the NEFU NLP Lab. His research interests include machine learning, knowledge graph, genetic similarity calculation.

WEN WANG received her Ph.D. degree (2011) in School of Information Science and Engineering, Shandong Normal University, Jinan, China. She received B.E. (2001), and M.E. (2004) degrees from Shandong University of Finance and Economics, Jinan, China. She is an Associate Professor in School of Management Engineering of Shandong Jianzhu University. Her research interests include information security and machine learning.