Improved Cryptanalysis of an ISO Standard Lightweight Block Cipher with Refined MILP Modelling

Jun Yin[1,3,4,5(✉)], Chuyan Ma[6], Lijun Lyu[3,4,5], Jian Song[1], Guang Zeng[1], Chuangui Ma[7], and Fushan Wei[1,2]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
yinjun66888@163.com
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[4] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[5] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[6] National University of Defense Technology, Changsha 410073, China
[7] Army Aviation Institute, Beijing 101116, China

Abstract. Differential and linear cryptanalysis are two of the most effective attacks on block ciphers. Searching for (near) optimal differential or linear trails is not only useful for the security evaluation of block ciphers against these attacks, but also indispensable to the cryptanalysts who want to attack a cipher with these techniques. In recent years, searching for trails automatically with Mixed-Integer Linear Programming (MILP) gets a lot of attention. At first, Mouha *et al.* translated the problem of counting the minimum number of differentially active S-boxes into an MILP problem for word-oriented block ciphers. Subsequently, in Asiacrypt 2014, Sun *et al.* extended Mouha *et al.*'s method, and presented a technique which can find actual differential or linear characteristics of a block cipher in both the single-key and related-key models. In this paper, we refine the constraints of the 2-XOR operation in order to reduce the overall number of variables and constraints. Experimental results show that MILP models with the refined constraints can be solved more efficiently. We apply our method to HIGHT (an ISO standard), and we find differential (covering 11 rounds) or linear trails (covering 10 rounds) with higher probability or correlation. Moreover, we find so far the longest differential and linear distinguishers of HIGHT.

Keywords: Lightweight block cipher · Differential attack
Linear attack · HIGHT · MILP

X. Chen et al. (Eds.): Inscrypt 2017, LNCS 10726, pp. 404–426, 2018.
https://doi.org/10.1007/978-3-319-75160-3_24

1 Introduction

In recent years, with the rapid development of the Internet of Things (IoT), the application of micro computing equipment is more and more popular, such as RFID chips and wireless sensor networks. At the same time, how to ensure the security of information stored on or transmitted over such devices with constrained resources attracts more and more attention. Hence, the pursuit of efficient and secure lightweight block ciphers came into being. Researchers have put forward many lightweight block ciphers. Roughly speaking, those lightweight block cipher can be divided into two categories, one type based on small S-boxes, such as LBlock [1], PRESENT [2], SKINNY [3] and RECTANGLE [4]. Another type doesn't use S-boxes. Instead, they adopt the ARX construction, where modular addition, rotation and XOR are used. These operations are easy to implement in software, such as HIGHT [5], TEA [6], SPECK [7], Sparx [8] *etc.*

Differential cryptanalysis [9] and linear cryptanalysis [10] are two main attacks on symmetric-key ciphers. For these attacks, finding an optimal differential or linear trails are important to make an effective attack. Among the methods proposed in the literature on finding optimal differential and linear characteristics, automatic searching is a very popular one, which is relatively easy to implement. Matsui's branch and bound search algorithm is the classic methods for obtaining DES differential characteristics [11]. Recently, with the aim to raise the efficiency of it, Chen *et al.* proposed some variant methods [12,13]. In CT-RSA 2014, Biryukov and Velichkov extended Matsui's algorithm [14], they proposed a new automatic search tool to search for the differential characteristics of ARX ciphers by introducing the new concept of a partial difference distribution table (pDDT). In 2013, Mouha and Preneel proposed an automatic tool to search for the optimal differential characteristic for ARX ciphers Salsa20 [15], The main idea is to convert the problem of searching for differential characteristics to a Boolean satisfiability problem, which only involves writing out simple equations for every operation in the cipher, and applies an off-the-shelf SAT solver. In 2011, Mouha *et al.* translated the problem of counting the number of active S-boxes into an MILP problem which can be solved with MILP solvers [16]. Subsequently, In Asiacrypt 2014, Sun *et al.* extended Mouha *et al.*'s method, and presented methods for searching the differential or linear characteristics of bit-oriented block ciphers both the single-key and related-key models [17]. In FSE 2016, Fu *et al.* proposed an MILP-based tool for automatic search for differential and linear trails in ARX ciphers, through the properties of differential and linear characteristics for modular addition operation, and gave a systematic method to describe the differential and linear characteristics with some constraints [18]. In FSE 2017, automatic search was also conducted based on constraint programming, which was able to analyze ciphers with 8×8 S-boxes [19].

HIGHT [5] was introduced by Hong *et al.* in CHES 2006, which is an ISO standard lightweight block cipher [20]. The designers gave the differential and linear attack results, and found some 11-round differential characteristics with probability 2^{-58} and several 10-round linear approximations with correlation 2^{-26}.[1]

In this paper, we improve Sun *et al.*'s method for automatic search differential and linear trails based on the MILP model. We accurately describe the 2-XOR operations with new constraints. The new constraints can reduce the overall number of variables and constraints in MILP model, which can save the time for solving the MILP model. Subsequently, we apply our refined MILP model to the lightweight block cipher HIGHT. As a result, we not only search the better differential characteristic for 11-round HIGHT and linear approximation for 10-round HIGHT, but also find the optimal differential characteristic for 13-round HIGHT and linear approximation for 11-round HIGHT. These results are shown in Table 1. (The p and cor in the table, represent the probability of differential characteristic and the correlation of linear approximation respectively)

Table 1. Summary of differential characteristics and linear approximations for HIGHT

Differential characteristics			Linear approximations		
Rounds	log_2^p	Reference	Rounds	log_2^{cor}	Reference
11	−58	[5]	10	−26	[5]
11	−45	This paper	10	−25	This paper
12	−53	This paper	11	−31	This paper
13	−61	This paper	-	-	-

Organization. This paper is organised as follows. In Sect. 2, we introduce the related knowledge, and give a brief description of the HIGHT. In Sect. 3, we give a brief introduction the automatic search method of differential and linear trails based on MILP model. In Sect. 4, a refined MILP model is presented. As an application, we utilize the refined MILP model to search the differential and linear characteristics for HIGHT. Then in Sect. 5, the results of differential and linear cryptanalysis of HIGHT are given. Finally, we conclude the paper in Sect. 6.

2 Preliminaries

In this section, we introduce some notations and terms, and briefly describe the lightweight block cipher HIGHT.

[1] In [5], the 10-round linear approximation with $\varepsilon^2 = 2^{-54}$, ε is called bias. Correspondingly, converted into the 10-round linear approximation with correlation 2^{-26}.

2.1 Notations

The following notations are used in this paper:

- $(X_i^7 \| X_i^6 \| \cdots \| X_i^0)$: The 64-bit input of the i-th round is considered as concatenations of 8 bytes X_i^j, $0 \leq j \leq 7$.
- $(SK_{4i+3} \| SK_{4i+2} \| SK_{4i+1} \| SK_{4i})$: The 32-bit subkey of the i-th round is considered as concatenations of 4 bytes SK_{4i+j}, $0 \leq j \leq 3$.
- $\oplus$: Bitwise exclusive OR (XOR)
- $\boxplus$: Addition modulo 2^n
- $x \lll s$: Rotation of x to the left by s positions
- Δx: The XOR difference of x_1 and x_2, $x_1 \oplus x_2 = \Delta x$
- $x[i]$: The bit at position i of word x

2.2 Description of HIGHT

The HIGHT [5] is a lightweight block cipher, it was proposed in CHES 2006, and was adopted as an ISO standard cryptography. The HIGHT utilize an 8-branch Type-II generalized Feistel structure, 64-bit block size and 128-bit key size, consisting of 32 rounds with four parallel Feistel functions in each round. The round function of HIGHT is shown in Fig. 1.[2]

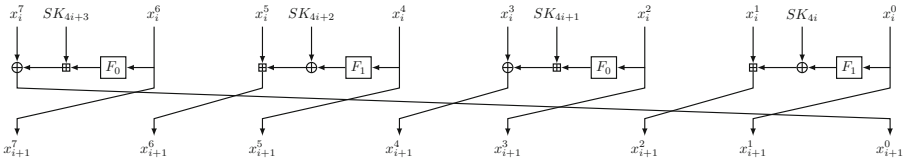

Fig. 1. The round function of HIGHT.

The round function transforms $(x_i^7 || x_i^6 || \cdots || x_i^0)$ into $(x_{i+1}^7 || x_{i+1}^6 || \cdots || x_{i+1}^0)$ as follows:

$$\begin{gathered} x_{i+1}^1 = x_i^0; x_{i+1}^3 = x_i^2; x_{i+1}^5 = x_i^4; x_{i+1}^7 = x_i^6; \\ x_{i+1}^0 = x_i^7 \oplus (F_0(x_i^6) \boxplus SK_{4i+3}); \\ x_{i+1}^2 = x_i^1 \boxplus (F_1(x_i^0) \oplus SK_{4i+2}); \\ x_{i+1}^4 = x_i^3 \oplus (F_0(x_i^2) \boxplus SK_{4i+1}); \\ x_{i+1}^6 = x_i^5 \boxplus (F_1(x_i^4) \boxplus SK_{4i}). \end{gathered}$$

The F_0 and F_1 used in the round function are defined as follows:

$$\begin{aligned} F_0(x) &= (x <<< 1) \oplus (x <<< 2) \oplus (x <<< 7); \\ F_1(x) &= (x <<< 3) \oplus (x <<< 4) \oplus (x <<< 6). \end{aligned}$$

[2] The Figs. 1, 2 and 3 are generated by TikZ for Cryptographers, please refer to http://www.iacr.org/authors/tikz/.

The inner functions F_0 and F_1 provide bitwise diffusion. These functions can be regarded as linear transformations from $GF(2)^8$ to $GF(2)^8$. The two linear transformations selected in the design of the cipher have the best diffusion property.

In this paper, we only consider the single-key model. Therefore, we omit key schedule in this paper. For further details, please refer to [5].

2.3 Security Analysis Results of HIGHT

Since the HIGHT has been put forward, it has received a great deal of attention. At present, there are many cryptanalysis results of HIGHT, which also includes some cryptanalysis results given by the designer.

In [5], the designer gives the differential characteristic probability is 2^{-58} for the 11-round HIGHT, and gave the 13-round HIGHT differential attack result. At the same time, find the 10-round linear approximation with bias $\varepsilon = 2^{-27}$. By using the linear approximation, the designer proposed 13-round linear attack for HIGHT, in the attack process, it requires 2^{57} plaintexts with the success rate 96.7% to recover 36 bits of the subkeys. In addition, the designer use this 14-round impossible differential characteristic to attack 18-round HIGHT. This attack requires $2^{46.8}$ chosen-plaintexts and $2^{109.2}$ encryptions of 18-round HIGHT. Except for some of the above attacks, the designer also presented truncated differential cryptanalysis [21], boomerang attack [22], sliding attack [23] and related key attack [24] and so on. These results indicate that the HIGHT has sufficient security.

Lu et al. [25] gave the first impossible differential cryptanalysis result for 25-round HIGHT, this attack requires 2^{60} chosen-plaintexts and $2^{126.78}$ encryptions. At ACISP 2009, Özen et al. [26] applied the impossible differential technique to attack 26-round HIGHT with data complexity of 2^{61} plaintexts, and time complexity of about $2^{119.53}$ encryptions. Then, At AFRICACRYPT 2012, Chen et al. [27] presented the impossible differential attack on the 27-round HIGHT with data complexity of 2^{58}, and time complexity of about $2^{126.6}$ encryptions, which is smaller than exhaustive search. In 2016, Cui et al. [28] proposed MILP-based automatic tool to search all cases of 17-round impossible differentials that both hamming weights of input and output differences are one, They found 4 impossible differentials for 17-round HIGHT, which are the longest ones until now.

At ICISC 2010, Koo et al. [29] presented the first attack on the full HIGHT using related-key rectangle attack with $2^{123.169}$ encryptions, $2^{57.84}$ data, and 4 related keys.

In 2015, Igarashi et al. [30] gave 19-round HIGTH using meet-in-the-middle attack with Splice-and-Cut technique, the attacked with 2^8 bytes of memory, $2^8 + 2$ pairs of chosen plain and cipher texts, and $2^{120.7}$ times of the encryption operation.

3 MILP-Based Automatic Search for Differential and Linear Trails

In this section, we first introduce the mixed integer linear programming problem, Then we briefly describe the method of constructing constraint inequalities for every operation in the ARX ciphers.

3.1 Mixed Integer Linear Programming (MILP)

MILP: Assume $A \in R^{m \times n}$, $b \in R^m$ and $c_1, c_2, \cdots, c_n \in R^n$, find a vector $x = (x_1, x_2, \cdots, x_n)$, such that the linear function $c_1x_1 + c_2x_2 + \cdots + c_nx_n$ is minimized (or maximized) with respect to the linear constraint $Ax \leq b$.

The MILP problem is a kind of optimization problem, which aims at finding the optimal solution of the objective function under the constraints. This problem can be solved by a lot of commercial software, such as Gurobi [31], CPLEX [32], MAGMA [33], *etc.*

3.2 Differential Constraints for Different Operations

Suppose an ARX cipher is composed of the following three operations:

- Rotations
- XOR
- Modular addition

It is obvious that the differential constraint of rotations operation can be obtained, according to [17], the constraints on the XOR operation as follows.

Constraints for XOR Operation [17]**.** According to Sun *et al.*'s differential automatic search method. For XOR operation with input differences Δa, Δb and output difference Δc, the constraints are presented as follows:

$$\begin{cases} \Delta a + \Delta b + \Delta c \geq 2d_{\oplus} \\ d_{\oplus} \geq \Delta a, d_{\oplus} \geq \Delta b, d_{\oplus} \geq \Delta c \\ \Delta a + \Delta b + \Delta c \leq 2 \end{cases} \tag{1}$$

where $d_{\oplus}$ is a dummy variable.

Constraints for Modular Addition Operation [18]**.** Assume α, β and γ be n-bit XOR differences, α, β are the input differences for modular addition operation, and γ is the output difference. In [18], if $i = 0$, $\alpha[i] \oplus \beta[i] = \gamma[i]$, the constraints are shown in formula (1), if $i \in [1, n-1]$, Fu *et al.* proposed 13 inequalities in formula (2) to express it.

$$\begin{cases} \beta[i] - \gamma[i] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ \alpha[i] - \beta[i] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ -\alpha[i] + \gamma[i] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ -\alpha[i] - \beta[i] - \gamma[i] - T(\alpha[i], \beta[i], \gamma[i]) \geq -3 \\ \alpha[i] + \beta[i] + \gamma[i] - T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ -\beta[i] + \alpha[i+1] + \beta[i+1] + \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ \beta[i] + \alpha[i+1] - \beta[i+1] + \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ \beta[i] - \alpha[i+1] + \beta[i+1] + \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ \beta[i] + \alpha[i+1] + \beta[i+1] - \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq 0 \\ \gamma[i] - \alpha[i+1] - \beta[i+1] - \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq -2 \\ -\beta[i] + \alpha[i+1] - \beta[i+1] - \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq -2 \\ -\beta[i] - \alpha[i+1] + \beta[i+1] - \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq -2 \\ -\beta[i] - \alpha[i+1] - \beta[i+1] + \gamma[i+1] + T(\alpha[i], \beta[i], \gamma[i]) \geq -2 \end{cases} \tag{2}$$

When $\alpha[i] = \beta[i] = \gamma[i]$, $T(\alpha[i], \beta[i], \gamma[i]) = 1$; otherwise, $T(\alpha[i], \beta[i], \gamma[i]) = 0$. the differential probability xdp^+ is calculated as follows:

$$xdp^+ = 2^{-\sum_{i=0}^{n-2} T(\alpha[i], \beta[i], \gamma[i])}$$

Fu *et al.* set the objective function for r-round differential MILP model as the $\sum_{j=0}^{r} \sum_{i=0}^{n-2} T(\alpha[i], \beta[i], \gamma[i])$.

3.3 Linear Constraints for Different Operations

In order to automatically search the linear trial of HIGHT, we must consider the propagation of the linear masks. Notice that the rotations is a simple bit permutation, we can give the corresponding linear constraints. Next, the constraints for the following operations can be given.

- XOR
- Branching
- Modular addition

Constraints for XOR Operation [34]**.** For XOR operation with input masks a, b and output mask c, include the following constraints:

$$a = b = c$$

Constraints for Branching Operation [34]**.** For branching operation with input mask a and output masks b, c, include the following constraints:

$$a \oplus b \oplus c = 0$$

Constraints for Modular Addition Operation [18]**.** Let modular addition operation with input masks $\wedge_\alpha, \wedge_\beta \in F_2^n$ and output mask $\Gamma \in F_2^n$. and

$\wedge_\alpha = (\wedge_\alpha[n-1], \cdots, \wedge_\alpha[0])$, $\wedge_\beta = (\wedge_\beta[n-1], \cdots, \wedge_\beta[0])$, $\Gamma = (\Gamma[n-1], \cdots, \Gamma[0])$. In [18], Fu *et al.* utilize 8 linear inequalities to describe the possible transitions, as shown in formula (3).

$$\begin{cases} s_{i+1} - \Gamma[i] - \Lambda_\alpha[i] + \Lambda_\beta[i] + s_i \geq 0 \\ s_{i+1} + \Gamma[i] + \Lambda_\alpha[i] - \Lambda_\beta[i] - s_i \geq 0 \\ s_{i+1} + \Gamma[i] - \Lambda_\alpha[i] - \Lambda_\beta[i] + s_i \geq 0 \\ s_{i+1} - \Gamma[i] + \Lambda_\alpha[i] - \Lambda_\beta[i] + s_i \geq 0 \\ s_{i+1} + \Gamma[i] - \Lambda_\alpha[i] + \Lambda_\beta[i] - s_i \geq 0 \\ s_{i+1} - \Gamma[i] + \Lambda_\alpha[i] + \Lambda_\beta[i] - s_i \geq 0 \\ -s_{i+1} + \Gamma[i] + \Lambda_\alpha[i] + \Lambda_\beta[i] + s_i \geq 0 \\ s_{i+1} + \Gamma[i] + \Lambda_\alpha[i] + \Lambda_\beta[i] + s_i \leq 4 \end{cases} \tag{3}$$

The correlation of addition modulo 2^n($cor_\boxplus$) can be computed as follows: $|cor_\boxplus(\Gamma, \wedge_\alpha, \wedge_\beta)| = 2^{-\sum_{i=1}^{n-1} s_i}$. Taking the above observation into account, Fu *et al.* set the objective function for r-round linear MILP model as the $\sum_{j=1}^{r}\sum_{i=1}^{n-1} s_i$.

For more details, please refer to [18,35].

4 The Refined MILP Model and Application to HIGHT

In this section, we present our refined MILP model, and then we apply the refined MILP model to the lightweight block cipher HIGHT.

4.1 The Refined MILP Model

It is observed that the number of variables in the MILP model will affect the efficiency of the solver. By analyzing the differential propagation of XOR operation in detail, in Eurocrypt 2017, Sasaki *et al.* gave the following constraints to model XOR operation.[3]

$$\begin{cases} \Delta a + \Delta b + \Delta c \leq 2 \\ \Delta a + \Delta b \geq \Delta c \\ \Delta a + \Delta c \geq \Delta b \\ \Delta b + \Delta c \geq \Delta a \end{cases} \tag{4}$$

where Δa and Δb are the input differences of the XOR operation, and Δc is the output difference.

In the previous work, we obtain the five constraint inequalities by computing the H-representation of the convex hull for the four possible differential propagation modes. Now, we obtain the same four constraint inequalitys with the

[3] The constraints appear in the slide that Sasaki *et al.* were reported in Eurocrypt 2017, please refer to https://eurocrypt2017.di.ens.fr/slides/A09-new-impossible-differential.pdf

greedy algorithm [17]. Compared with/the constraints given in the formula (1), the formula (4) not only introduces no new dummy variables, but also reduces one constraint, which can reduce 16 variables and constraints in just one round HIGHT. Similarly, in the modular addition and the branching operations, the XOR constraints also reduce a part of variables and constraints.

Next, we focus on the functions F_0 and F_1 for HIGHT.

$$F_0(x) = (x <<< 1) \oplus (x <<< 2) \oplus (x <<< 7)$$
$$F_1(x) = (x <<< 3) \oplus (x <<< 4) \oplus (x <<< 6)$$

For the 2-XOR operations in each function, in accordance with the above formula (4), we need to introduce an intermediate variable to generate the constraints, in this case, we convert constrained F_0 and F_1 to the following question.

Let $\Delta a \oplus \Delta b \oplus \Delta c = \Delta d$, where Δa, Δb and Δc are the input differences, and Δd is the output difference. The differential propagation of the 2-XOR operations is shown in Fig. 2.

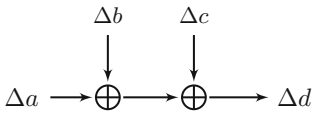

Fig. 2. The differential propagation of the 2-XOR operations.

By analyzing these possible differential patterns in detail, We give the constraints as shown in formula (5). These constraints can be clearly seen from Table 2, we can know the 8 constraints are chosen to describe the possible difference patterns for the 2 XOR operations. In Table 2, the constraint $\Delta a + \Delta b + \Delta c - \Delta d \geq 0$ can remove the impossible differential propagation mode $(0, 0, 0, 1)$. The eight constraint inequalities in formula (5) satisfy all possible input-output differential modes, and also exclude all impossible input-output differential modes.

$$\begin{cases} \Delta a + \Delta b + \Delta c - \Delta d \geq 0 \\ \Delta a + \Delta b + \Delta c - \Delta d \leq 2 \\ \Delta a + \Delta b + \Delta d - \Delta c \geq 0 \\ \Delta a + \Delta b + \Delta d - \Delta c \leq 2 \\ \Delta a + \Delta c + \Delta d - \Delta b \geq 0 \\ \Delta a + \Delta c + \Delta d - \Delta b \leq 2 \\ \Delta b + \Delta c + \Delta d - \Delta a \geq 0 \\ \Delta b + \Delta c + \Delta d - \Delta a \leq 2 \end{cases} \tag{5}$$

By comparing the introduction of the intermediate variable with the constraint given by the formula (4), we can reduce 8 variables in each function by the formula (5). When solving the MILP model with Gurobi, it can save computing time and improve the solving efficiency through the above constraints.

Table 2. Remove all impossible differential propagations for the 2-XOR operations

Δa	Δb	Δc	Δd	Impossible
0	0	0	0	
0	0	0	1	✓ $\Delta a + \Delta b + \Delta c - \Delta d \geq 0$
0	0	1	0	✓ $\Delta a + \Delta b + \Delta d - \Delta c \geq 0$
0	0	1	1	
0	1	0	0	✓ $\Delta a + \Delta c + \Delta d - \Delta b \geq 0$
0	1	0	1	
0	1	1	0	
0	1	1	1	✓ $\Delta b + \Delta c + \Delta d - \Delta a \leq 2$
1	0	0	0	✓ $\Delta b + \Delta c + \Delta d - \Delta a \geq 0$
1	0	0	1	
1	0	1	0	
1	0	1	1	✓ $\Delta a + \Delta c + \Delta d - \Delta b \leq 2$
1	1	0	0	
1	1	0	1	✓ $\Delta a + \Delta b + \Delta d - \Delta c \leq 2$
1	1	1	0	✓ $\Delta a + \Delta b + \Delta c - \Delta d \leq 2$
1	1	1	1	

4.2 Construct the Refined MILP Model for HIGHT

According to the refined constraints given by the XOR and 2-XOR operations, we apply these refined constraints to the MILP model of the HIGHT. According to Sun et al. MILP-based automatic search technology and constraints for modular addition operation, it is easy to construct a refined MILP model for HIGHT.

Without loss of generality, we just give the method of constructing the differential MILP model for 1-round HIGHT in detail. The differential and linear MILP model for r-round HIGHT can be constructed in the similar way.

We assume that the new value introduced in modular addition operation $T(\alpha[i], \beta[i], \gamma[i])$ is denoted by $T_1^{(i)}$, where $i \in [0, 6]$. As there are 4 modular addition operations in a round of HIGHT, the number of the new values $T(\alpha[i], \beta[i], \gamma[i])$ is 28 in total, which is denoted by $(T_1^{(0)}, T_1^{(1)}, \cdots, T_1^{(27)})$. Then the sum of the values: $T_1^{(0)} + T_1^{(1)} + \cdots + T_1^{(27)}$ is chosen as the objective function to be minimized.

Assume that the 64-bit input difference for the 1-round HIGHT is denoted by $\Delta X = (\Delta X_0, \cdots, \Delta X_i, \cdots, \Delta X_7)$, where ΔX_i is an 8-bit differential variable, $\Delta X_i = (\Delta {X_i}^{(0)}, \Delta {X_i}^{(1)} \cdots, \Delta {X_i}^{(7)})$. According to the round function of HIGHT, the 1-8, 17-24, 33-40, 49-56 bits position of the outputs are the same as the corresponding differential positions of the inputs for 1-round HIGHT. So, the 64-bit output difference for the 1-round HIGHT is denoted by $\Delta Y = (\Delta X_1, \Delta Y_0, \Delta X_3, \Delta Y_1, \Delta X_5, \Delta Y_2, \Delta X_7, \Delta Y_3)$, where ΔY_i is an 8-bit differential

variable, $\Delta Y_i = (\Delta {Y_i}^{(0)}, \Delta {Y_i}^{(1)} \cdots, \Delta {Y_i}^{(7)})$. At the same time, the output difference between the four F-functions from left to right is $\Delta Z = (\Delta Z_0, \Delta Z_1)$, ΔZ_i is an 8-bit differential variable, and $\Delta Z_i = (\Delta {Z_i}^{(0)}, \Delta {Z_i}^{(1)} \cdots, \Delta {Z_i}^{(7)})$. The difference between the output of the first and third addition modulo operation from left to right is $\Delta M = (\Delta M_0, \Delta M_1)$, where ΔM_i is an 8-bit differential variable, then $\Delta M_i = (\Delta {M_i}^0, \Delta {M_i}^{(1)}, \cdots, \Delta {M_i}^{(7)})$. These differential variables are shown in Fig. 3.

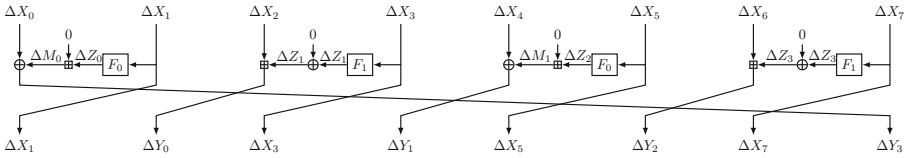

Fig. 3. Differential variable values for the 1-round MILP model of HIGHT.

Firstly, to make sure the non-zero input difference, we should add the constraint:

$$\Delta {X_0}^{(0)} + \Delta {X_0}^{(1)} + \cdots + \Delta {X_0}^{(63)} \geq 1$$

In the first generalized feistel structure, the input difference of the F-function is $(\Delta {X_1}^{(0)}, \Delta {X_1}^{(1)}, \cdots, \Delta {X_1}^{(7)})$, and the output difference is $(\Delta {Z_0}^{(0)}, \Delta {Z_0}^{(1)}, \cdots, \Delta {Z_0}^{(7)})$. When $j = 0$, according to formula (5), we can get the constraints as follows:

$$\begin{cases} \Delta {X_1}^{(1)} + \Delta {X_1}^{(2)} + \Delta {X_1}^{(7)} - \Delta {Z_0}^{(0)} \geq 0 \\ \Delta {X_1}^{(1)} + \Delta {X_1}^{(2)} + \Delta {X_1}^{(7)} - \Delta {Z_0}^{(0)} \leq 2 \\ \Delta {X_1}^{(1)} + \Delta {X_1}^{(2)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(7)} \geq 0 \\ \Delta {X_1}^{(1)} + \Delta {X_1}^{(2)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(7)} \leq 2 \\ \Delta {X_1}^{(1)} + \Delta {X_1}^{(7)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(2)} \geq 0 \\ \Delta {X_1}^{(1)} + \Delta {X_1}^{(7)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(2)} \leq 2 \\ \Delta {X_1}^{(2)} + \Delta {X_1}^{(7)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(1)} \geq 0 \\ \Delta {X_1}^{(2)} + \Delta {X_1}^{(7)} + \Delta {Z_0}^{(0)} - \Delta {X_1}^{(1)} \leq 2 \end{cases} \tag{6}$$

when $j \geq 1$, the constraints can be obtained with the same method. So $8 \times 32 = 256$ linear constraints are proposed to describe the differential property for the 2 XOR operations in the 1-round HIGHT.

The constraints of the modular addition operations are introduced in the following text. In the first generalized feistel structure, the two input differences are $(\Delta {Z_0}^{(0)}, \Delta {Z_0}^{(1)}, \cdots, \Delta {Z_0}^{(7)})$ and 0, the output difference is $(\Delta {M_0}^{(0)}$, $\Delta {M_0}^{(1)}, \cdots, \Delta {M_0}^{(7)})$. When $j = 7$, the constraint is $\Delta {Z_0}^{(0)} - \Delta {M_0}^{(0)} = 0$,

obviously. According to formula (2), when $j = 0$, the constraints are shown in formula (7).

$$\begin{cases} -\Delta M_0^{(1)} + T_0^{(0)} \geq 0 \\ \Delta Z_0^{(1)} + T_0^{(0)} \geq 0 \\ \Delta M_0^{(1)} - \Delta Z_0^{(1)} + T_0^{(0)} \geq 0 \\ -\Delta Z_0^{(1)} + \Delta M_0^{(1)} + T_0^{(0)} \leq 3 \\ -\Delta Z_0^{(1)} + \Delta M_0^{(1)} - T_0^{(0)} \geq 0 \\ \Delta Z_0^{(1)} + \Delta M_0^{(0)} + T_0^{(0)} \geq 0 \\ \Delta Z_0^{(0)} + \Delta M_0^{(0)} \geq 0 \\ -\Delta Z_0^{(0)} + \Delta M_0^{(0)} + T_0^{(0)} \geq 0 \\ \Delta Z_0^{(1)} + \Delta Z_0^{(0)} - \Delta M_0^{(0)} + T_0^{(0)} \geq 0 \\ \Delta M_0^{(1)} + \Delta Z_0^{(0)} - \Delta M_0^{(0)} + T_0^{(0)} \geq -2 \\ \Delta Z_0^{(0)} - \Delta M_0^{(0)} + T_0^{(0)} \geq -2 \\ -\Delta Z_0^{(0)} - \Delta M_0^{(0)} + T_0^{(0)} \geq -2 \\ \Delta M_0^{(0)} - \Delta Z_0^{(0)} + T_0^{(0)} \geq -2 \end{cases} \tag{7}$$

The constraints when $1 \leq j \leq 6$ can be calculated in the similar way. Therefore, we can produce $2 \times (7 \times 13 + 1) + 2 \times (7 \times 13 + 4) = 374$ constraints to represent the differential property for modular addition in the 1-round HIGHT.

Finally, we focus on the XOR operations, whose input difference are $(\Delta {X_0}^{(0)}, \Delta {X_0}^{(1)}, \cdots, \Delta {X_0}^{(7)})$ and $(\Delta {M_0}^{(0)}, \Delta {M_0}^{(1)}, \cdots, \Delta {M_0}^{(7)})$, and the output difference is $(\Delta {Y_3}^{(0)}, \Delta {Y_3}^{(1)}, \cdots, \Delta {Y_3}^{(7)})$. When $j = 0$, the constraints are shown in formula (8).

$$\begin{cases} \Delta X_0^{(0)} + \Delta M_0^{(0)} - \Delta Y_3^{(0)} \geq 0 \\ \Delta X_0^{(0)} + \Delta Y_3^{(0)} - \Delta M_0^{(0)} \geq 0 \\ \Delta Y_3^{(0)} + \Delta M_0^{(0)} - \Delta X_0^{(0)} \geq 0 \\ \Delta X_0^{(0)} + \Delta M_0^{(0)} + \Delta Y_3^{(0)} \leq 2 \end{cases} \tag{8}$$

The constraints when $j \geq 1$ can be calculated in the same way. Thus, we have $2 \times 4 \times 8 = 64$ constraints for XOR operation in the 1-round HIGHT. So far, we construct a complete MILP model for 1-round HIGHT. In total, we have $256 + 374 + 64 + 1 = 695$ constraints to exactly describe the difference $\Delta X \rightarrow \Delta Y$.

4.3 Comparison of Constraints and Variables in the MILP Model

In order to distinguish these two types of MILP models and also for the convenience of our statement in this paper, the MILP model without adding new constraints is named as the original MILP model, and the MILP model with new constraints is named as the refined MILP model.

We establish the differential MILP model for r-round HIGHT. The original MILP model have $776r + 2$ constraints and $214r + 65$ variables for the r-rounds HIGHT, but the refined MILP model for r-round HIGHT only needs $694r + 2$

constraints and $108r+65$ variables, Figs. 4 and 5 show the number of constraints and variables in the original and the refined differential MILP model for the first 12-round HIGHT, respectively.

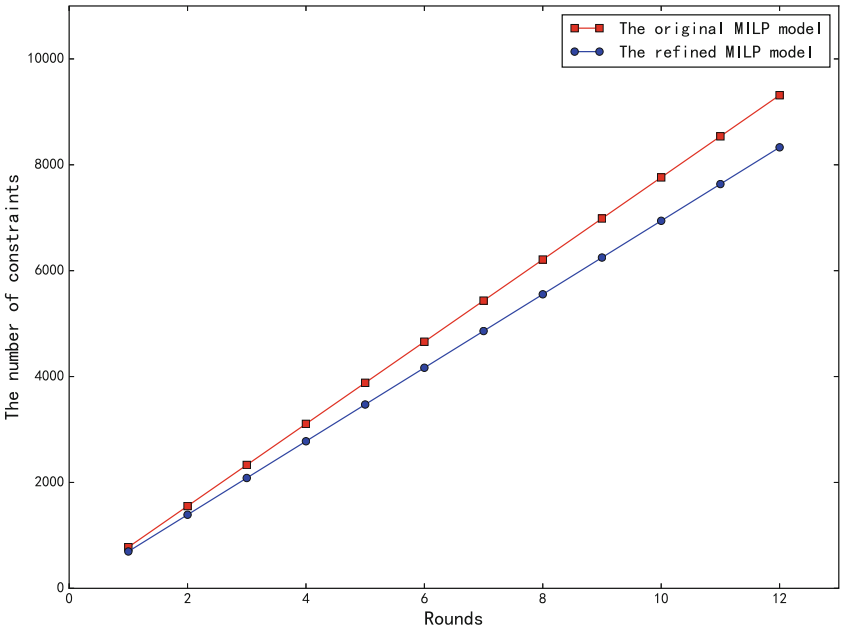

Fig. 4. Comparison of the number of constraints in the original and refined differential MILP model for the first 12-round.

As you can see in Fig. 4, the original model has 7762 constraints for the 10-round HIGHT, while the refined model has only 6942 constraints, in comparison, 820 constraint inequalities are reduced. In Fig. 5, the original model has 2205 variables for the 10-round HIGHT, while the refined model has only 1145 variables, 1060 variables are reduced.

We establish the linear MILP model for r-round HIGHT. The original MILP model have $736r+2$ constraints and $288r+65$ variables for the r-rounds HIGHT, but the refined MILP model for r-round HIGHT only needs $640r+2$ constraints and $192r+65$ variables, Figs. 6 and 7 show the number of constraints and variables in the original and the refined linear MILP model for the first 12-round HIGHT, respectively.

As you can see in Fig. 6, the original model has 7362 constraints for the 10-round HIGHT, while the refined model has only 6402 constraints, in comparison, 960 constraint inequalities are reduced. In Fig. 7, the original model has 2945 variables for the 10-round HIGHT, while the refined model has only 1985 variables, 960 variables are reduced.

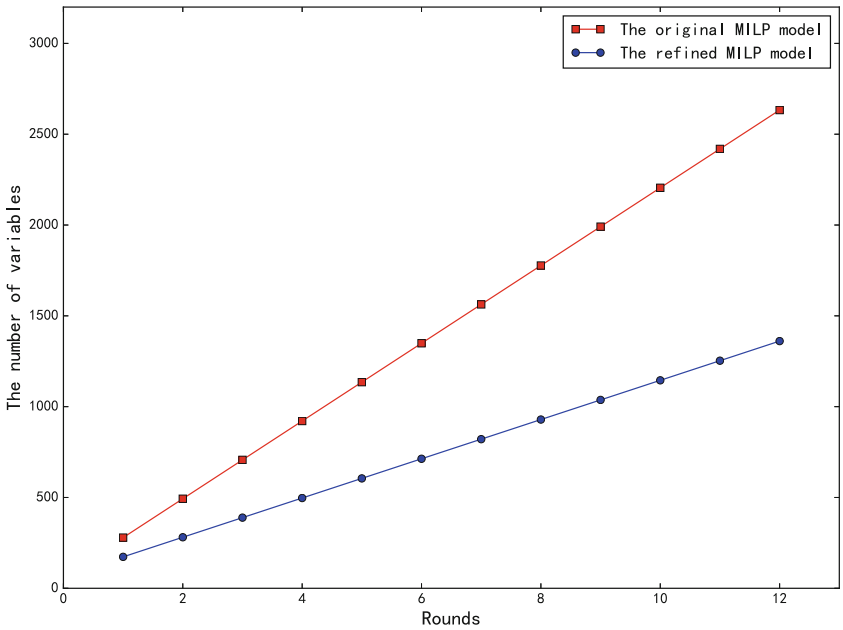

Fig. 5. Comparison of the number of variables in the original and refined differential MILP model for the first 12-round.

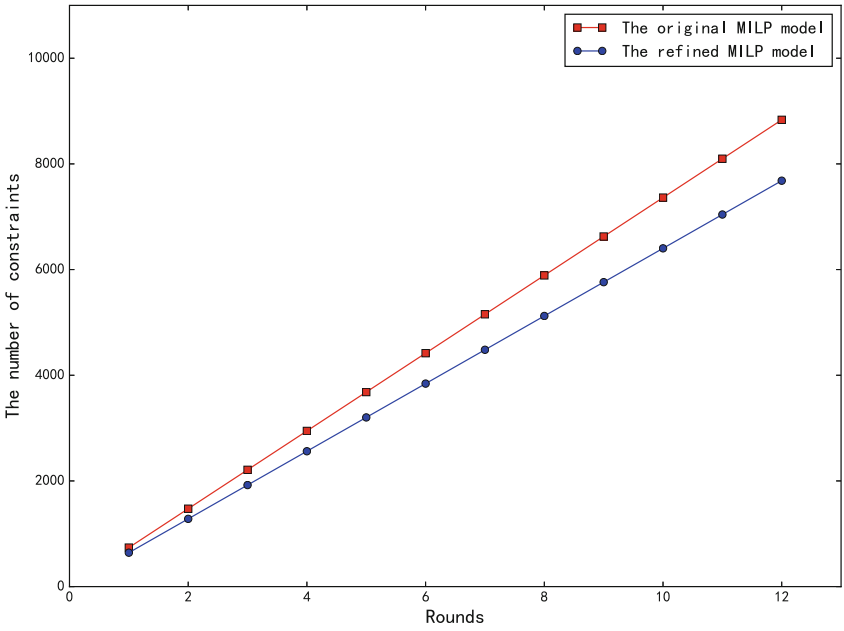

Fig. 6. Comparison of the number of constraints in the original and refined linear MILP model for the first 12-round.

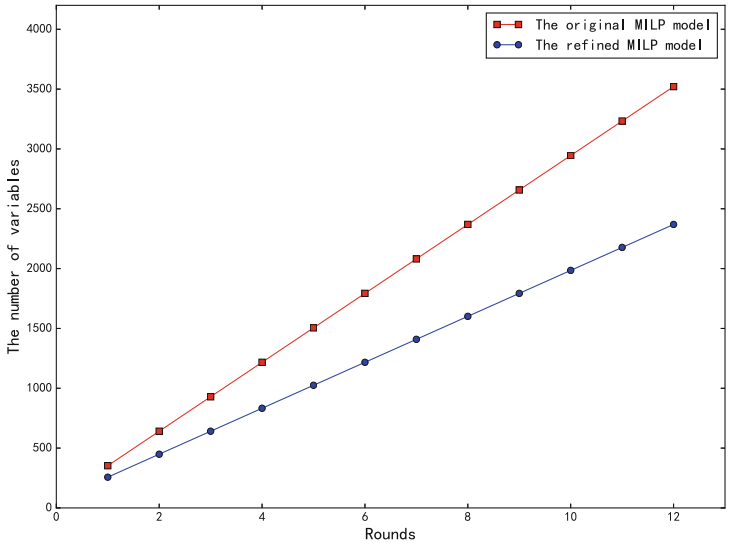

Fig. 7. Comparison of the number of variables in the original and refined linear MILP model for the first 12-round.

5 The Differential and Linear Cryptanalysis for HIGHT

Based on the refined MILP model, according to Sect. 4.2, we generate the differential and linear MILP models in "lp" format [14] for HIGHT through a small python program, and call Gurobi 7.0.2 to solve it. There are $108r + 65$ variables and $694r + 1$ constraints for r-round HIGHT in differential MILP model, and there are $192r + 65$ variables and $640r + 2$ constraints for r-round HIGHT in linear MILP model. The MILP model was solved on a server, the server configuration is shown in Table 3.

Table 3. Experimental environment for solving the MILP model

Item	Configuration
CPU	Intel Xeon E7-4820 v2
RAM	512 GB
OS	Windows Server 2008 R2 Enterprise
Software	Python3.5, Gurobi7.0.2

5.1 The Differential Cryptanalysis for HIGHT

By solving the refined differential MILP model, the probability of differential characteristic for reduced-round HIGHT obtained by our refined MILP model is listed in Table 4, the p_r denotes the probability of differential characteristic for the r-round HIGHT.

Table 4. The differential cryptanalysis results for refined MILP model application to HIGHT

Rounds	#variable	#constraint	$\log_2 p_r$	Timing(s)
1	173	695	0	1
2	281	1389	0	1
3	389	2083	−3	15
4	497	2777	−8	130
5	605	3471	−11	636
6	713	4165	−15	8362
7	821	4859	−19	18456
8	929	5553	−25	41251
9	1037	6247	−30	125565
10	1145	6941	−38	489785
11	1253	7635	−45	1012556
12	1361	8329	−53	1801255
13	1469	9023	−61	2518256
14	1577	9717	<-64	-

From Table 4 we know that the refined MILP model for the 11-round HIGTH consists of 1253 0-1 variables, 7635 constraints. The MILP model can be solved within 1012556 s and we find the better probability of differential characteristic for 11-round HIGHT is 2^{-45}. Note that the probability of the best single-key characteristic previously published covering 11-round is 2^{-58}. Furthermore, using the refined tool, we obtain the new single-key differential characteristics for HIGHT, which cover larger number of rounds. We obtain the 12- and 13-round single-key differential characteristics of HIGHT with probability 2^{-53} and 2^{-61}. For the 14-round HIGHT, the optimal probability for differential characteristic is less than 2^{-64}. The probability of success for an exhaustive search, thus, we concluded that the all-round HIGHT has a sufficient resistance to differential attacks.

Finally, the differential trails for 12 and 13-round HIGHT are listed in Tables 5 and 6, respectively.

In order to clarify that the refined MILP model can solve more efficiently, we establish the MILP model for the first 9-round HIGHT, and solve the MILP model in the same experimental environment. In less than 10 days, the original differential MILP model of the first 9-round HIGHT was solved, and the optimal differential probability is the same as Table 4. But the time expendure of round 1 to 9 is 1 s, 1 s, 123 s, 568 s, 2135 s, 21268 s, 48392 s, 124536 s and 671258 s, respectively. Figure 8 shows a comparison of the solve time between the original and the refined differential MILP model for the first 9-round HIGHT.

Table 5. Differential trail for 12-round HIGHT

Rounds	Difference	$\log_2 p_r$
0	00008227213AEA01	-0
1	000027A03A4E0100	-6
2	0000A0B84E010000	-6
3	0000B8C801000000	-4
4	0000C80100000000	-4
5	0000010000000000	-3
6	0001000000000000	-1
7	0100000000000082	-2
8	00000000009C8201	-3
9	000000039C7A0100	-8
10	00E803BC7A010000	-5
11	E800BCF801000002	-6
12	00B6F801009002E8	-5
Probability	2^{-53}	

Table 6. Differential trail for 13-round HIGHT

Rounds	Difference	$\log_2 p_r$
0	80008AC28A01A0BB	-0
1	0000C2080128BB80	-6
2	000008E528E98000	-10
3	0000E5A8E9800000	-1
4	0000A82C80000000	-8
5	00002C8000000000	-2
6	0000800000000000	-3
7	0080000000000000	-0
8	80000000000000C3	-3
9	000000000072C380	-4
10	0000000C72E98000	-9
11	00A70CF2E9800000	-4
12	A700F22A80000002	-6
13	007B2A80009002A7	-5
Probability	2^{-61}	

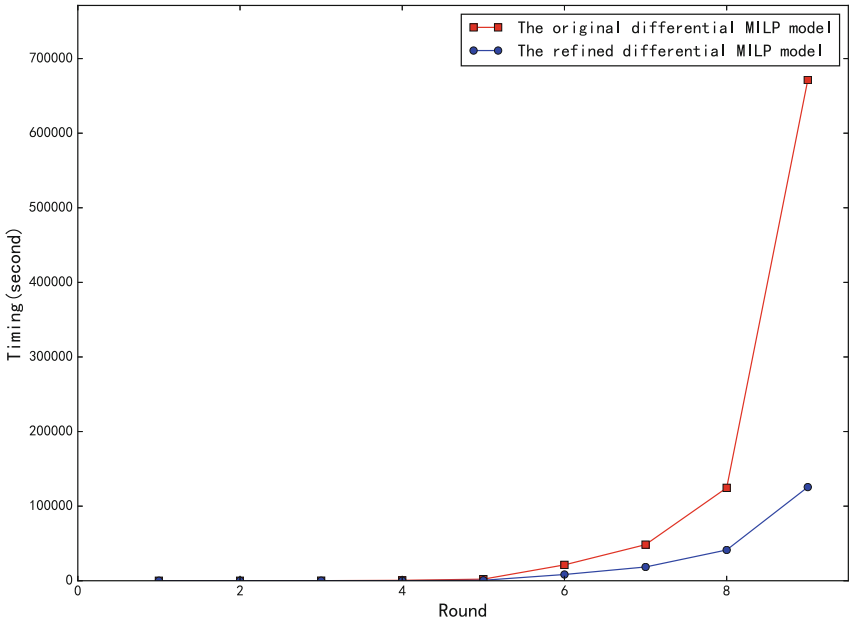

Fig. 8. Comparison of the solve time in the original and refined differential MILP model for the first 9-round HIGHT.

From Fig. 8 we know that the original differential MILP model can be solved within 671258 s for the 9-round HIGHT. Nevertheless, the refined differential MILP model just needed 125565 s. Comparatively speaking, the solve time of the refined MILP model is 5 times faster than the original MILP model.

5.2 The Linear Cryptanalysis for HIGHT

By solving the refined linear MILP model, the correlation of linear approximation for reduced-round HIGHT obtained by our refined MILP model is listed in Table 7, the cor_r denotes the correlation of linear approximation for the r-round HIGHT.

For linear attack, from Table 7 we know that linear approximation for the 10-round HIGHT with correlation 2^{-25}, the correlation of the best linear approximation previously published covering 10-round is 2^{-26}. Moreover, we obtain the new linear approximation for 11-round HIGHT with correlation 2^{-31}, the maximum linear bias is $\varepsilon^2 = 2^{-64}$, then the linear attack on the 11-round HIGHT require 2^{64} known plaintext, but the all-round HIGHT require plaintext is certainly greater than 2^{64}. Therefore, it can be concluded that all-round HIGHT are sufficiently resistant to linear attack. Finally, the linear trail for 11-round HIGHT is listed in Table 8.

In order to clarify that the refined MILP model can solve more efficiently, we establish the MILP model for the first 8-round HIGHT, and solve the MILP

Table 7. The linear cryptanalysis results for refined MILP model application to HIGHT

Rounds	#variable	#constraint	$\log_2 cor_r$	Timing(s)
1	257	642	0	1
2	449	1282	−1	1
3	641	1922	−2	30
4	833	2562	−4	100
5	1025	3202	−6	207
6	1217	3842	−9	970
7	1409	4482	−12	8216
8	1601	5122	−16	165348
9	1793	5762	−22	464156
10	1985	6402	−25	986423
11	2177	7042	−31	1865719
12	2369	7682	-	>30 days

Table 8. Linear trail for 11-round HIGHT

Rounds	Mask	$\log_2 cor_r$
0	3863C24B000001C2	−0
1	01C200000001D638	−5
2	0000000001F65201	−4
3	0000000134530000	−4
4	0000013400000000	−2
5	0001000000000000	−1
6	0100000000000000	−0
7	C200000000000001	−1
8	0C000000000001C2	−3
9	160000000001F60C	−2
10	6000000001A44016	−6
11	B000000166601A60	−3
Correlation	2^{-31}	

model in the same experimental environment. In less than 10 days, the original linear MILP model of the first 8-round HIGHT was solved, and the optimal linear correlation is the same as Table 7. But the time expendure of round 1 to 8 is 1 s, 157 s, 882 s, 5029 s, 18653 s, 79523 s and 4264131 s, respectively. Figure 9 shows a comparison of the solve time between the original and the refined linear MILP model for the first 8-round HIGHT.

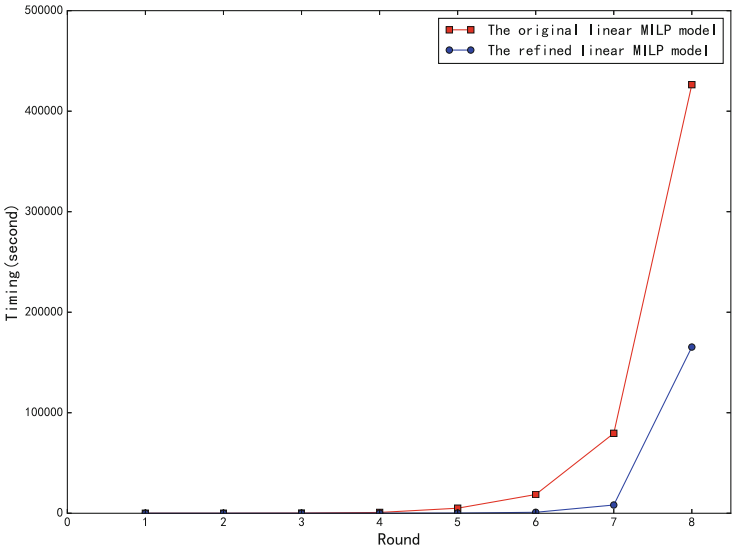

Fig. 9. Comparison of the solve time in the original and refined linear MILP model for the first 8-round.

From Fig. 9 we know that the original linear MILP model can be solved within 426413 s for the 8-round HIGHT. Nevertheless, the refined differential MILP model just needed 165348 s. By contrast, the solve time of the refined MILP model is 2.5 times faster than the original MILP model.

6 Conclusion

In this paper, we analyze the differential propagation for the 2-XOR operations in detail, and improve Sun *et al.*'s method for describing XOR operation with refined constraints. In the refined MILP model, the number of variables and constraints are reduced, which leads to quickly solve for the refined MILP model.

As an application, we implement our refined MILP model to the lightweight block cipher HIGHT. Compared with the existing attack results, the refined MILP model searches the optimal differential characteristic and linear approximation for HIGHT, the differential and linear trails increased to 13-round and 11-round. These results indicate that the refined MILP model is more efficient in practical cryptanalysis.

Acknowledgements. The authors would like to thank the anonymous reviewers for their helpful comments and suggestions. The work of this paper was supported by the National Natural Science Foundation of China (61772519, 61502532, 61379150, 61309016, 61502529), the Open Foundation of the Key State Key Laboratory of Mathematical Engineering and Advanced Computing (2016A02), and the State Key Laboratory of Information Security. The work of Jun Yin and Lijun Lyu is supported by the Youth Innovation Promotion Association of Chinese Academy of Sciences.

References

1. Wu, W., Zhang, L.: LBlock: a lightweight block cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21554-4_19
2. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
3. Beierle, C., et al.: The `SKINNY` family of block ciphers and its low-latency variant `MANTIS`. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5
4. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. Sci. Chin. Inf. Sci. **58**(12), 1–15 (2015). https://doi.org/10.1007/s11432-015-5459-7
5. Hong, D., et al.: HIGHT: a new block cipher suitable for low-resource device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006). https://doi.org/10.1007/11894063_4
6. Wheeler, D.J., Needham, R.M.: TEA, a tiny encryption algorithm. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 363–366. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_29
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 (2013). http://eprint.iacr.org/2013/404
8. Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., Biryukov, A.: Design strategies for ARX with provable bounds: Sparx and LAX. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 484–513. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_18
9. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-38424-3_1
10. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
11. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053451
12. Chen, J., Miyaji, A., Su, C., Teh, J.S.: Accurate estimation of the full differential distribution for general feistel structures. In: Lin, D., Wang, X.F., Yung, M. (eds.) Inscrypt 2015. LNCS, vol. 9589, pp. 108–124. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-38898-4_7
13. Chen, J., Miyaji, A., Su, C., Teh, J.: Improved differential characteristic searching methods. In: IEEE 2nd International Conference on Cyber Security and Cloud Computing, CSCloud 2015, New York, NY, USA, 3–5 November 2015, pp. 500–508 (2015). https://doi.org/10.1109/CSCloud.2015.42
14. Biryukov, A., Velichkov, V.: Automatic search for differential trails in ARX ciphers. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 227–250. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04852-9_12

15. Mouha, N., Preneel, B.: Towards finding optimal differential characteristics for arx: Application to salsa20. Cryptology ePrint Archive, Report 2013/328 (2013). http://eprint.iacr.org/2013/328
16. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 57–76. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34704-7_5
17. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., 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: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_9
18. Fu, K., Wang, M., Guo, Y., Sun, S., Hu, L.: MILP-based automatic search algorithms for differential and linear trails for speck. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 268–288. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_14
19. Sun, S., Gerault, D., Lafourcade, P., Yang, Q., Todo, Y., Qiao, K., Hu, L.: Analysis of aes, skinny, and others with constraint programming. IACR Trans. Symmetric Cryptol. **2017**(1), 281–306 (2017). https://doi.org/10.13154/tosc.v2017.i1.281-306
20. International Organization for Standardization. ISO/IEC 18033-3: 2010. Information technology Security techniques Encryption algorithms Part 3: Block ciphers (2010)
21. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_16
22. Wagner, D.: The boomerang attack. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_12
23. Biryukov, A., Wagner, D.: Slide attacks. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 245–259. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_18
24. Biham, E.: New types of cryptanalytic attacks using related keys. J. Cryptology **7**(4), 229–246 (1994). https://doi.org/10.1007/BF00203965
25. Lu, J.: Cryptanalysis of reduced versions of the hight block cipher from CHES 2006. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 11–26. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76788-6_2
26. Özen, O., Varıcı, K., Tezcan, C., Kocair, Ç.: Lightweight block ciphers revisited: cryptanalysis of reduced round PRESENT and HIGHT. In: Boyd, C., González Nieto, J. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 90–107. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02620-1_7
27. Chen, J., Wang, M., Preneel, B.: Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. In: Mitrokotsa, A., Vaudenay, S. (eds.) AFRICACRYPT 2012. LNCS, vol. 7374, pp. 117–137. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31410-0_8
28. Cui, T., Jia, K., Fu, K., Chen, S., Wang, M.: New automatic search tool for impossible differentials and zero-correlation linear approximations. Cryptology ePrint Archive, Report 2016/689 (2016). http://eprint.iacr.org/2016/689
29. Koo, B., Hong, D., Kwon, D.: Related-key attack on the full HIGHT. In: Rhee, K.-H., Nyang, D.H. (eds.) ICISC 2010. LNCS, vol. 6829, pp. 49–67. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24209-0_4

30. Igarashi, Y., Sueyoshi, R., Kaneko, T., Fuchida, T.: Meet-in-the-middle attack with splice-and-cut technique on the 19-round variant of block cipher HIGHT. In: Kim, K.J. (ed.) Information Science and Applications. LNEE, vol. 339, pp. 423–429. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46578-3_50
31. Gurobi Optimazation, Gurobi optimizer reference manual. http://www.gurobi.com
32. CPLEX, Ibm software group: User-Manual CPLEX 12, https://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/
33. Computational Algebra Group, School of Mathematics and Statistics, University of Sydney: Magma Computational Algebra System, http://magma.maths.usyd.edu.au
34. Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., Shi, D., Song, L.: Automatic enumeration of (related-key) differential and linear characteristics with predefined properties and its applications. IACR Cryptology ePrint Archive 2014, 747 (2014). http://eprint.iacr.org/2014/747
35. Wallén, J.: Linear approximations of addition modulo 2^n. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 261–273. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39887-5_20