MILP-Based Automatic Differential Searches for LEA and HIGHT

Elnaz Bagherzadeh and Zahra Ahmadian
eln.bagherzadeh@mail.sbu.ac.ir, z_ahmadian@sbu.ac.ir

Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran

Abstract. In this paper we use MILP technique for automatic search for differential characteristics of ARX ciphers LEA and HIGHT. We show that the MILP model of the differential property of modular addition with one constant input can be represented with a much less number of linear inequalities compared to the general case. Benefiting from this new developed model for HIGHT block cipher, we can achieve a reduction of $112r$ out of $480r$ in the total number of linear constraints for MILP model of r-round of HIGHT. This saving accelerates the searching process of HIGHT about twice as fast.
We enjoy the MILP model to investigate the differential effect of these ciphers and provide a more accurate estimation for the differential probability, as well. Our observations show that despite HIGHT, LEA exhibits a strong differential effect. The details of differential effects are reflected in a more compact manner using the newly defined notion of probability polynomial. The results gained by this method improve or extend the previous results as follows. For LEA block cipher, we found more efficient 12 and 13-round differentials whose probabilities are better than the best previous 12 and 13-round differentials for a factor of about 2^6 and 2^7, respectively. In the case of HIGHT block cipher, we found two new 12 and 13-round differentials, though with the same best reported probabilities.

Keywords: MILP model · Differential Attack · ARX ciphers.

1 Introduction

symmetric cryptography, ARX structure refers to designs in which only three operations are used: modular addition, XOR and the rotation. This strategy is regarded as an important alternative for SPN structure and contributes a large portion of the existing symmetric schemes. For example, two SHA-3 finalists BLAKE [1] and Skein [2] hash functions, the eStream finalist Salsa20[3], and the NIST released block cipher SPECK[4] are some well-known instances of ARX structure. Some other schemes includes the hash function for short messages SipHash[5]; MAC algorithms Chaskey[6], stream ciphers ChaCha[7] and HC-128[8] and the lightweight block ciphers LEA [9], FEAL[10], Threefish[11], RC5[12] and HIGHT [13].

Table 1. Comparison of our characteristics of LEA with previous ones

Rounds	Characteristic prob.	Differential prob.	Reference
11	2^{-98}	$2^{-91.9}$	[9]
12	2^{-128}	-	[9]
12	2^{-112}	$2^{-101.71}$	[32]
12	$\mathbf{2^{-107}}$	$\mathbf{2^{-95.86}}$	**This paper**
13	2^{-134}	$2^{-123.02}$	[32]
13	$\mathbf{2^{-127}}$	$\mathbf{2^{-115.86}}$	**This paper**

An important step in designing any symmetric scheme is to evaluate its resistance against differential attack. Despite SPN ciphers which enjoy some provable upper bounds for the probability of differential characteristics, such a feature for the ARX structures has not yet been found. Therefore the automatic search algorithms for the optimal differential characteristics have been a focus of cryptographers' concerns. In this regards, a variety of methods have been proposed and applied such as the methods adapted from branch and bound Matsui's algorithm [14, 15], the methods based on Boolean satisfiability problems [16–18], and the method based on mixed integer linear programming problems [26, 27].

In this paper we focus on the third technique which has been explicitly applied for automatic search algorithms for cryptanalysis of symmetric ciphers either SPN or ARX structures [19–27]. Mixed Integer Linear Programming (MILP) is a class of optimization problems derived from Linear Programming which aims to optimize an objective function under certain constrains. Although this problem is NP-complete inherently, there are some open source and commercially availble MILP solvers which can solve not too large MILP problems instances. In order to employ this tool for the purpose of cryptanalysis, the problem of cryptanalysis of a symmetric cipher should be translated to MILP problem and then be solved by an appropriate solver.

The first attempts for employing MILP technique for cryptanalysis of symmetric ciphers belongs to the SPN ciphers where Mouha et al.[19] and Wu et al. [20] translated the problem of finding the minimum number of active Sboxes into a MILP problem. This method then used for finding the specific pattern characteristics for ALE authenticated encryption algorithm and counting the minimal number of active S-boxes of bit-oriented block ciphers by introducing bit-level representations in [28]. Sun et al. [23] extended Mouha et al. method to analyze block ciphers with bitwise permutation diffusion layers (S-bP structures) in the single key and related key models, though without considering the differential properties of Sbox modules. In [21], the differential properties of the Sbox layer has been taken into account in the MILP model and more precise results for differential characteristics derived, consequently.

Table 2. Comparison of our characteristics of HIGHT with previous one.

Rounds	Characteristic prob.	Differential prob.*	Reference
11	2^{-58}	2^{-58}	[13]
11	$\mathbf{2^{-45}}$	$\mathbf{2^{-45}}$	[34] and **This paper**
12	$\mathbf{2^{-53}}$	$\mathbf{2^{-53}}$	[34] and **This paper**
13	$\mathbf{2^{-61}}$	$\mathbf{2^{-61}}$	[34] and **This paper**

* [34] does not provide any analysis for differential probability.

Table 3. Comparison of the number of constraints for MILP models for HIGHT

Model	Number of constraints
Original 1	$776r$
Original 2	$480r$
Yin et al. [34]	$694r$
This paper	**368r**

In case of the ARX ciphers the main challenge is to construct an efficient MILP model to represent differential pattern of modular addition. Although the algorithm proposed in [23] has shown to be effective in constructing MILP model for (at most 4×4) Sbox modules, it can not be used for modular addition as an $2n \times n$ Sbox in $\mathbf{F}_2^n$ (for n typically at least 16). Since it demands too many linear constraints which makes the MILP problem of a typical ARX cipher too complex and hence intractable.

Fu et al. resolved this problem in [26], where the analysis of differential property of modular addition provided in [29] is utilized to derive an efficient MILP model for modular addition. They applied their model to the ARX cipher SPECK which improved the existing results.

In this paper, we modify and use MILP model for ARX structures proposed in [26] to find differential characteristics for ARX ciphers LEA and HIGHT. The design of HIGHT involves some modular additions whose one input is constant (i.e. with zero difference). Although such a scenario can be regarded as a special case of the general form analyzed in [26], it would be modeled much more efficiently with less number of constraints if it is revisited independently. We do this revision and reduced the number of constraints from $13n + 1$ into $5n + 1$ where n is the word size for modular addition. This improvement reduced the number of constraints from $480r$ into $368r$ for r-round HIGHT, which is a considerable improvement and makes the search process of HIGHT twice as fast. Recently, HIGHT has received another differential characteristic search using MILP method [34] with a number of $694r$ constraints for r-round HIGHT. However using this model, new 12 and 13 round characteristics where proposed

for HIGHT. Table 3 compares the number of MILP constraints for the proposed model and the others. From the original model 1 and 2, we mean the MILP model in which the number of XOR constraints is five and one, respectively.

Moreover, we compute the probability of the sub-optimal differential, rather than the sub-optimal characteristic only. The notion of *probability polynomial* is defined to reflect the differential effect for each cipher in a compact form. Our results shows that despite HIGHT, LEA exhibits a strong differential effect which makes the differential probability much bigger than its dominant characteristic probability. A summary of our achievements along with the previous results for LEA and HIGHT are shown in Tab. 1 and Tab. 2, respectively. For LEA, we found new 12 and 13-round differentials with improved probabilities. For HIGHT, using our new model we found new differentials for 11, 12 and 13 rounds, apart from those introduced in [34].

The rest of this paper is organized as follows. Section 2 describes MILP Model for Differential Characteristics in ARX Ciphers, where Fu et al.'s model along with our proposed model for special case of modular addition is presented. In Section 3, we reviewed the concepts of characteristic and differential and the new concept of probability polynomial is presented. Our results on LEA and HIGHT ciphers are detailed in Sections 4 and 5 respectively. Finally, Section 6 concludes our work.

2 MILP Model for Differential Characteristics in ARX Ciphers

The MILP problem is the problem of optimizing the value of a linear objective function of some integer/real-valued variables which satisfy some linear (in)equality constraints.

MILP solvers can be enjoyed to find the best differential characteristic of a cipher if the problem of finding the optimal differential characteristic of a cipher can be translated into a (not too large) MILP problem. To that end, the objective function should be set to an adequate strictly monotonic function of the characteristic probability, and the linear constraints are configured to express the propagation of the difference values in the cipher. Therefore, with respect to the modeled cryptosystem, the optimum differential characteristic probability would be returned by solving the model by an adequate MILP solver.

Fu et al. [26] proposed the first MILP model for the differential characteristic search problem of ARX structures by defining the objective function as well as the linear constraints for ARX structures.

Among the set of modules involved in ARX structures, rotation operation only changes the position of the input bits, so a simple change of variables describes the input difference-output difference relation completely. Since rotation is a linear operation, it does not contribute to the characteristic probability and consequently the objective function. In this section, we first review the MILP model for differential properties of the XOR and modular addition operations

[26], then we propose the new and more concise MILP model for the modular addition when one of its inputs is constant.

2.1 MILP model for XOR

For the XOR operation with bit-level input and output differences, Sun et al. in [21] proposed a model including five inequalities in three input/output binary variables and an extra dummy binary variable that precisely describes the XOR operation. However, considering that all variables in the model are binary, in [27] it was shown that the following single linear equation completely describes the XOR operation.

$$a + b + c = 2d \tag{1}$$

where d is a dummy binary variable. Since XOR is a linear operation, it does not have any effect on the characteristic probability and hence the objective function.

In [34], Yin et al. tried to improve the MILP model for two consecutive XORs which is equivalent to a 3-input XOR. Without noticing 1, they improved the original 10-constraint model for the two consecutive XOR, into a 8-constraint model.

2.2 MILP model for modular addition

Based on two following theorems derived by Lipmaa and Moriai in [29], the feasible differential characteristics for modular addition and their corresponding probabilities are characterized completely. In the following, the notation $x[i]$ is used to show the the i^{th} bit of n-bit word x where the LSB and MSB of x are $x[0]$ and $x[n-1]$, respectively.

Theorem 1. *The differential $(\alpha, \beta \rightarrow \gamma)$ is possible if the following two conditions are satisfied:*

1. $\alpha[0] \oplus \beta[0] \oplus \gamma[0] = 0$, *and*
2. *if* $\alpha[i-1] = \beta[i-1] = \gamma[i-1]$, *then*
   $\alpha[i-1] = \beta[i-1] = \gamma[i-1] = \alpha[i] \oplus \beta[i] \oplus \gamma[i]$, *where* $i = 1, \ldots, n-1$.

Theorem 2. *Assume that $(\alpha, \beta \rightarrow \gamma)$ is a possible differential characteristic, then the xor differential probability of addition (xdp^+) of this differential is*

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

where

$$eq(\alpha[i], \beta[i], \gamma[i]) = \begin{cases} 1 & \alpha[i] = \beta[i] = \gamma[i] \\ 0 & o.w \end{cases} \tag{3}$$

The first feasibility condition $\alpha[0] \oplus \beta[0] \oplus \gamma[0] = 0$ in Theorem 1, can be described in MILP model by the following equation

$$\alpha[0] + \beta[0] + \gamma[0] = 2d$$

where d is a dummy binary variable.
In [26], Fu et. al. observed that the second feasibility condition of Theorem 1 is equivalent to the fact that there are 56 possible vectors of the form

$$(\alpha[i], \beta[i], \gamma[i], \alpha[i+1], \beta[i+1], \gamma[i+1], \neg eq(\alpha[i], \beta[i], \gamma[i]) \tag{4}$$

in total. The SAGE Computer Algebra System [30] returns a set of 65 linear inequalities satisfying all these 56 possible patterns. However, 65 inequalities are too many which makes the MILP model too complicated. In [26], it has been shown that based on the greedy algorithm given in [22], the number of linear inequalities can be reduced from 56 to 13. All these 13 inequalities are shown in Appendix A.

Therefore, for n-bit words, the total number of constraints describing the addition module is $13(n-1)+1$.

The only non-linear module in the ARX structure is modular addition. So, it is the only contributor to the objective function. If there are r modular additions in the cipher in total, with input-output differences $(\alpha_j, \beta_j \rightarrow \gamma_j)$, $j = 1, ..., r$, then according to Theorem 2, the overall characteristic probability is

$$P_D = 2^{-\sum_{j=1}^{r}\sum_{i=0}^{n-2}\neg eq(\alpha[i],\beta[i],\gamma[i])} \tag{5}$$

and the objective function is defined as

$$\sum_{j=1}^{r}\sum_{i=0}^{n-2}\neg eq(\alpha[i], \beta[i], \gamma[i]) \tag{6}$$

which is a linear function and supposed to be minimized.

2.3 MILP model for modular addition with a constant input

Suppose that there is a modular addition in the cipher whose one input is constant. In other words, its corresponding difference is zero. This is exactly the case with HIGHT cipher, where some subkeys are added to the data in each round. One way to handle such a situation, is to use the 13 general inequalities given in Appendix A directly, in which the one input difference, say α have been set to zero i.e. $\alpha[i] = 0$, $i = 0, ..., n-1$.

Here, we propose a more efficient model for this case with much less number of inequalities. Again consider the 7-tuple vector given in (4). The first condition

Table 4. Linear inequalities expressing the differential property of modular addition with a constant input

$$
\begin{aligned}
-\beta[i] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) &\geq 0,\\
-\gamma[i] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) &\geq 0,\\
\beta[i] + \gamma[i] - (\neg eq(\alpha[i], \beta[i], \gamma[i])) &\geq 0,\\
\beta[i+1] - \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) &\geq 0,\\
-\beta[i+1] + \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) &\geq 0.
\end{aligned}
$$

of Theorem 1 is simplified to $\beta[0] = \gamma[0]$, considering $\alpha[0] = 0$. This new form does not need defining any new dummy variable, hence one bit saving in the number of variables of the problem.

To the second condition of Theorem 1, we add the new condition $\alpha[i] = \alpha[i-1] = 0$. So, the number of valid remaining vectors reduces to 14 possible patterns. Using the SAGE Computer Algebra System, we get a number of 10 linear inequalities satisfying all the 14 possible patterns and no impossible patterns. Then, we use the greedy algorithm to make this set smaller and finally the number of inequalities reaches from 10 to 5 inequalities (per bit), which is a great improvement in the number of constraints comparing to 13 inequalities per bit, in general case. In other words, for a n-bit modular addition, the number of constraints decreases by $8(n-1)$ where n is the word size.
This set of inequalities are listed in Table 4. Obviously, the objective function does not change any.

Having defined the objective function and all the constraints for the target ARX cipher, the MILP model is complete and ready to be solved by a MILP solver. It worth mentioning that MILP solvers can return the number of distinct solutions along with the optimum value of the objective function.

3 Characteristic Probability and Differential Probability using MILP method

In order to precisely evaluate the security of block ciphers against differential analysis Lai et. al. first introduced the theory of Markov ciphers and made a distinction between a differential and a differential characteristic [31]. What is essentially important in the differential cryptanalysis is the input-output difference, no matter what the intermediate differences may be. However, for a given differential with fixed input-output differences, there could be potentially many characteristics that share the same input-output differences and so they all contribute to the differential probability. Such an effect is called strong differential effect [31]. In order to calculate the differential probability as accurately as pos-

sible, more characteristics sharing the same input and output difference should be counted in.

Therefore in general, any differential will have a probability greater than that of its most probable characteristic. So, by considering the differential probability rather than the characteristic probability, we calculate the true success rate of the differential cryptanalysis, not just a lower bound for that.

However, the MILP-based search tool finds only the most probable characteristic rather than differential. In the following we explain how to employ the MILP model to find not only the best characteristic, but also to compute the probability of the differential that matches this characteristic.

3.1 Computing differential probability

Assume that the MILP tool has already found the optimum characteristic with input-output difference $(\Delta_{in}, \Delta_{out})$ and probability 2^{-d}. It means that the objective function in the MILP model has optimum value equal to d. We can find other characteristics with the same input-output differences $(\Delta_{in}, \Delta_{out})$ with probabilities equal to or less than 2^{-d}.

We first introduce the notion of *probability polynomial* that we define for a compact and concise representation of probability of a differential and its corresponding characteristics. The probability polynomial of a specific differential with a given input-output difference is defined as follows

$$p(x) = p_0 x^d + p_1 x^{d+1} + p_2 x^{d+2} + \dots \tag{7}$$

Where p_i is the number of distinct characteristics with the probability of $2^{-(d+i)}$, $i = 0, 1, ...$ It is clear that the probability of the corresponding characteristic can be calculated by evaluating $p(x)$ at $x = \frac{1}{2}$. In particular, we consider only the first N monomials of $p(x)$, i.e.

$$p(x) \simeq p_0 x^d + p_1 x^{d+1} + \dots + p_N x^{d+N} \tag{8}$$

where N is actually selected in such way that at $x = \frac{1}{2}$ the last term is negligible comparing to the sum of other terms i.e.,

$$p_{N+1} 2^{-(d+N+1)} < \sum_{i=0}^{N} p_i 2^{-(d+i)} \tag{9}$$

In order to construct the probability polynomial for a cipher using the MILP method, the following steps should be done:

1. build a MILP model for differential characteristic for the target cipher according to Section 2, without any extra constraint. Solve this model to obtain the input and output differences of the optimum differential characteristic $(\Delta_{in}, \Delta_{out})$, along with its probability which is 2^{-d}.
2. For $i = 0$ to $N - 1$,
   Add three new constraints to the original MILP model as follows, then solve it to find p_i.

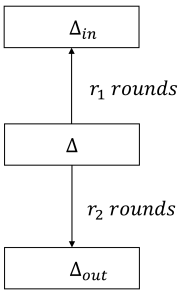

Fig. 1. Obtaining a longer characteristic from two shorter ones.

- Set the input-output difference equal to $(\Delta_{in}, \Delta_{out})$ found in Step 1.
- Add a new constraint that puts the objective function equal to $d + i$.

Despite the first step that we need that the MILP solver returns the optimum solution along with the values of variables, in the second step it is sufficient to configure the MILP solver to return the number of optimum solutions only.

3.2 Sub-optimal solutions

The MILP problem is inherently a NP-complete problem. So, for a differential cryptanalysis with a complex MILP model containing a large number of variables and constraints, it is not unexpected that the problem can not be resolved by a MILP solver. This situation occurs when the number of rounds attacked is increased.

In such problems if the solver fails to solve the problem as a whole, a sub-optimal solution may suffice. To find a sub-optimal solution, it is very conventonal to divide the r-round cipher into two r_1 and r_2-round subciphers ($r = r_1 + r_2$), and solve each problem independently [26, 32]. Definitely, the output difference of the first subcipher must be the same as the input difference of the second subcipher. So, the MILP models of the first r_1-round and second r_2-round subciphers must have an extra constraint which is respectively the out put difference $= \Delta$ and the input difference $= \Delta$. Finally, If the optimum value of the first and second problems are d_1 and d_2 respectively, the sub-optimum value for the full r-round problem would be $d = d_1 + d_2$. This process has been shown in Figure 1. This is exactly equal to the main r-round problem which is subjected to the extra constraint $\Delta_{r_1} = \Delta$.

The only thing that remains is to limit the candidate values of Δ to a small enough set with appropriate values. We should search this set of Δ and choose the one with the highest d value. The differential property of modular addition shows that the more active bits in the input-output differences, potentially the weaker probability of the differential. So, a common choice for Δ is always a low-weight one, e.g. those with only one active bit.

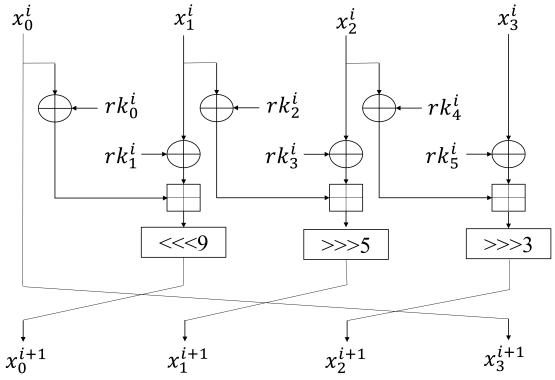

Fig. 2. The round function of LEA.

After finding the best Δ and the associated optimum values d_1 and d_2, we run the above explained algorithm for the two subciphers independently, to construct the two probability polynomials $p_1(x)$ and $p_2(x)$. To derive the probability polynomial of the main r-round cipher, it is needed to consider all possible r-round characteristics by combining each r_1-round characteristic and each r_2-round characteristic. This process is exactly equivalent to multiplying the probability polynomials of the two subciphers. So, the probability polynomial of the main r-round differential would be

$$p(x) = p_1(x)p_2(x) \tag{10}$$

In general, the main problem may be so complex that dividing the r-round cipher into just two subciphers may not be sufficient. So, let the r-round cipher be divided into k subciphers with probability polynomials $p_i(x)$, $i = 1, \ldots, k$. Clearly, the output difference of subcipher i is equal to the input difference of subcipher $i + 1$. Finally, the probability polynomail of the r-round cipher is

$$p(x) = \prod_{i=1}^{k} p_i(x) \tag{11}$$

and the differential probability is $p(x)|_{x=\frac{1}{2}}$.

4 Differntial Analysis of LEA block cipher using MILP method

LEA is an ARX block cipher proposed by Hong et al. in WISA 2009 [9]. It provides a high-speed software encryption on general-purpose processors. It has the block size of 128 bits and the key size of 128, 192, or 256 bits. There are some cryptanalysis on LEA including [35, 36].

In [9] the designers have proposed the first differential analysis of their scheme. Their analysis is confined to finding characteristic probability and not differential probability. The characteristic under consideration has been found by linearizing LEA (replacing modular addition with XOR) and conditioned that the Hamming weight of the difference at the middle of the cipher is small. So, their best findings are 12-round and 11-round characteristics with probabilities 2^{-128} and 2^{-98}, respectively. Song et al [32] used a search method based on SAT solvers and found characteristics and differentials for 12 rounds and 13 rounds of LEA with probability better than 2^{-128}. There is also an informaly published work on 12-round[1] LEA with probability 2^{-121} [33] using a search method based on the Nested Monte-Carlo algorithm. In this section we report our MILP-based results which outperform the previous ones [9, 32]. All results on LEA have been summarized in Tab. 1.

4.1 LEA specification

The encryption algorithm of LEA works as follows. It maps a plaintext of four 32-bit words $(x_0^0, x_1^0, x_2^0, x_3^0)$ into a ciphertext $(x_0^r, x_1^r, x_2^r, x_3^r)$ using a sequence of r rounds, where $r = 24$ for LEA-128, $r = 28$ for LEA-192 and $r = 32$ for LEA-256. The round function for round i, $i = 0, \ldots, r-1$ is defined as follows:

$$\begin{aligned} x_0^{i+1} &\leftarrow ((x_0^i \oplus rk_0^i) + ((x_1^i \oplus rk_1^i)) \lll 9 \\ x_1^{i+1} &\leftarrow ((x_1^i \oplus rk_2^i) + ((x_2^i \oplus rk_3^i)) \ggg 5 \\ x_2^{i+1} &\leftarrow ((x_2^i \oplus rk_4^i) + ((x_3^i \oplus rk_5^i)) \ggg 3 \\ x_3^{i+1} &\leftarrow x_0^i. \end{aligned} \tag{12}$$

One round of LEA cipher has been shown in Fig. 2.

4.2 MILP-based search for characteristics and differentials of LEA

According the MILP model for differential attack on ARX structures described in Section 2, we can construct an MILP model for one-round and hence any arbitrary rounds of LEA cipher. All the XOR operations in LEA are used for key addition which are bypassed in the differential attack. So, for each round of LEA our model includes three modular additions and a bit permutation as for the rotation and words swapping. Therefore, the total number of constrains would be $3(13(n-1)+1)+4n$, where the word size in LEA is $n = 32$. So, the total number of constraints for each rounds of LEA becomes 404.

However, in order to search a r-round LEA without any extra constraint, the MILP model will become too complex to be solved for $r \geq 4$. Therefore, according to the discussion in Section 3.2, we choose the strategy of finding a sub-optimal solution and construct a long characteristic from two short ones.

[1] This work is incorrectly reported as a 13-round characteristic in [33].

Table 5. Sub-optimal characteristic for 12-round LEA

Rounds	12-round	
	$\Delta x_0 \| \| \Delta x_1 \| \| \Delta x_2 \| \| \Delta x_3$	$\log_2 p$
0	$C0000000C0400080404000104040012$	
1	80010000800000044000001440000010	-13
2	02000800820000001000000010010800	-8
3	00100100001000000000200002000800	-4
4	000200000001FF000040030000100100	-15
5	00020000000200000006000000020000	-25
6	**00000000000000000000000000020000**	**-5**
7	00000000000000000000400000000000	-1
8	00000000000006000000080000000000	-3
9	00040000000001000000100000000000	-6
10	08042000800000080000002000040000	-5
11	00401110C40000000000800408002000	-8
12	80222188222004008100140000401110	-14
$\sum_r \log_2 pr$		-107
$\log_2 p_{diff} >$		-95.86

Analysis of 12-round LEA To this end, we first analyse $r = 12$ rounds of LEA by dividing it into two subciphers of $r_1 = r_2 = 6$ rounds. The first subcipher has exactly one active bit, say bit i, in its output difference and the second one has the same difference in its input. The two problems are solved independently and optimum values d_1 and d_2 are derived for $i = 0, ..., 127$. Among all 128 possible cases, the sub-optimal characteristic for 12-round LEA is that with the minimum $d = d_1 + d_2$. So, in this way we found a 12-round characteristic for LEA with the additional constraint that its internal difference at round 6 has Hamming weight equal to one.

A 6-round MILP problem for LEA, which is constrained to Hamming weight one either in input or in output, is solvable by the solver fortunately. Among all 128 possible cases, the best one occurs at $i = 110$ which is equal to a 12-round characteristic with internal difference $\Delta_6 = (00000000, 00000000, 00000000, 00020000)$. For this case $d_1 = 70$ and $d_2 = 37$. So, the corresponding sub-optimum 12-round characteristic has $d = 107$. The details of this characteristic is reflected in Tab. 5.

In order to find the differential probability corresponding to the sub-optimum characteristic, we first find probability polynomials $p_1(x)$ and $p_2(x)$ according

to the algorithm explained in Section 3.1.

$$p_1(x) = 3x^{70} + 9x^{71} + 32x^{72} + 101x^{73} + 245x^{74} + 635x^{75} + 1462x^{76} + 3107x^{77} + 5264x^{78}, \tag{13}$$

$$p_2(x) = 2x^{37} + 0x^{38} + 10x^{39} + 15x^{40} + 24x^{41} + 70x^{42} + 112x^{43} + 254x^{44} + 505x^{45} + 731x^{46}. \tag{14}$$

Now we obtain the probability polynomial for 12-round differential as follows.

$$\begin{aligned} p(x) &= \prod_{i=1}^{2} p_i(x) = p_1(x)p_2(x) \\ &= 6x^{107} + 18x^{108} + 94x^{109} + 337x^{110} + \\ &\quad 1017x^{111} + 3186x^{112} + 8623x^{113} + \\ &\quad 22673x^{114} + 55008x^{115} + 111568x^{116} + \\ &\quad 254616x^{117} + 463615x^{118} + 866416x^{119} + \\ &\quad 1587582x^{120} + 2581241x^{121} + 3974813x^{122} + \\ &\quad 4929537x^{123} + 3847984x^{124} \end{aligned} \tag{15}$$

Finally, by evaluating $p(x)$ at $x = \frac{1}{2}$ we end up with the differential probability of 12-round LEA, which is

$$p(x)\Big|_{x=\frac{1}{2}} = 2^{-95.8629} \tag{16}$$

Analysis of 13-round LEA In order to find a sub-optimum 13-round characteristic, we first examined the scenario of dividing it into 6-round and 7-round subciphers. However, the MILP problem for 7-round is not solvable, even constrained to weight one in the input or output. So, we have to divide the cipher into three subciphers. A good choice, though not necessarily the best one, is to continue the already found 12-round characteristic. So, in case of the 13-round, the first two subciphers would be the two previously found 6-round subciphers and the third one would be a 1-round which is constrained such that its input difference is equal to the output difference of the second subcipher, i.e. $\Delta_{12} = 80222188222004008100140000401110$. This 1-round characteristic along with the two previous 6-rounds are reported in Tab. 6. Comparing Tables 5 and 6, one can realize that two distinct maximal probability characteristics are reported in these tables, but with the same Δ_1 and the same Δ_{12}. The corresponding probability polynomial $p_3(x)$ has only one monomial which is expected due to the shortness of the subcipher.

$$p_3(x) = x^{20} \tag{17}$$

Table 6. Sub-optimal differential characteristics for 13-round LEA

Rounds	13-round	
	$\Delta x_0 \| \| \Delta x_1 \| \| \Delta x_2 \| \| \Delta x_3$	$\log_2 p$
0	$C0000000C0400080404000104040012$	
1	$800100008000000C40000004C0000000$	-13
2	$02001800820000008000000080010000$	-8
3	$00300100001000000000200002001800$	-4
4	$000200000001FF000040010000300100$	-15
5	$00020000000200000002000000020000$	-25
6	**00000000000000000000000000020000**	**-5**
7	$00000000000000000000400000000000$	-1
8	$00000000000002000000080000000000$	-2
9	$00040000000000300000010000000000$	-5
10	$08002000800000080000002000040000$	-7
11	$00401110C4000000000800408002000$	-8
12	$80222188222004008100140000401110$	-14
13	$044911440519008010280 0A180222088$	-20
$\sum_r \log_2 pr$		-127
$\log_2 p_{diff} >$		-115.86

Therefore, the probability polynomial of the proposed sub-optimal 13-round characteristic is

$$\begin{aligned} p(x) &= \prod_{i=1}^{3} p_i(x) = p_1(x)p_2(x)p_3(x) \\ &= 6x^{127} + 18x^{128} + 94x^{129} + 337x^{130} + \\ &\quad 1017x^{131} + 3186x^{132} + 8623x^{133} + \\ &\quad 22673x^{134} + 55008x^{135} + 111568x^{136} + \\ &\quad 254616x^{137} + 463615x^{138} + 866416x^{139} + \\ &\quad 1587582x^{140} + 2581241x^{141} + 3974813x^{142} + \\ &\quad 4929537x^{143} + 3847984x^{144} \end{aligned} \tag{18}$$

Finally, the 13-round differential probability is calculated as

$$p(x)\Big|_{x=\frac{1}{2}} = 2^{-115.8629} \tag{19}$$

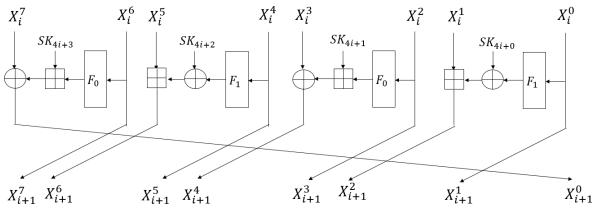

Fig. 3. Round function of HIGHT cipher

5 Differntila Analysis of HIGHT block cipher using MILP method

Hong et al. [13] proposed a new block cipher HIGHT with 64-bit block length and 128-bit key length, which is suitable for low-cost, low-power, and ultra-light implementation. HIGHT is approved by Korea Information Security Agency (KISA) and is adopted as an International Standard by ISO/IEC 18033-3 [13]. This made this cipher an attractive target for cryptanalyses [37–41].

Although HIGHT has been received much attention from the cryptanalysers, few work is focused on finding the best possible differential characteristic. The first one is the designers' analysis [13], where an evaluation of differential attack is provided by linearizing it. According to this analysis, without any discussion about differential probability, the best differential characteristic found for 11-round of HIGHT has been reported with the probability of 2^{-58}. The other one is a recent one [34] in which differential characteristics are found using a so-called refined MILP model for up to 13 rounds of HIGHT. In the rest of this section we introduce new 11-round, 12-round and 13-round differential characteristics/differentials found using our efficient MILP model.

5.1 HIGHT specifications

HIGHT has a 32-round iterative structure which is a variant of generalized Feistel network. Whitening keys are applied before the first round and after the last round. One round of HIGHT is shown in Fig. 3, where $(X_7^i|X_6^i|,...,|X_0^i)$ and $(SK_{4i+3}|SK_{4i+2}|SK_{4i+1}|SK_{4i})$ indicate the 64 bits input and 32 bits subkey of the i-th round respectively. Each word in HIGHT is a byte. Two subkeys SK_{4i+1} and SK_{4i+3} are added to the data in mod 2^8 while the two other ones are XORed to data. F_0 and F_1 are two linear functions with 8 bits input and 8 bits output which work as follows.

$$\begin{aligned} F_0(x) &= (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7) \\ F_1(x) &= (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6) \end{aligned} \tag{20}$$

Table 7. Differential characteristics for 12-round HIGHT

Rounds	First characteristic [34]		Second characteristic (new)	
	$\Delta x_0 \|\| \Delta x_1 \|\| \cdots \|\| \Delta x_6 \|\| \Delta x_7$	$\log_2 p$	$\Delta x_0 \|\| \Delta x_1 \|\| \cdots \|\| \Delta x_6 \|\| \Delta x_7$	$\log_2 p$
0	00008227213*AEE*01		*B*000*C*003000081*E*2	
1	000027*A*03*A*460100	-6	00*E*803000000*E*2*B*0	-3
2	0000*A*0*B*84*E*010000	-6	*E*80700000000*D*002	-8
3	0000*B*8*C*801000000	-4	0*E*00000000000279	-4
4	0000*C*80100000000	-4	0000000000007907	-1
5	0000010000000000	-3	0000000000000700	-5
6	**0001000000000000**	**-1**	**0000000000010000**	**-3**
7	0100000000000082	-2	0000008201000000	-2
8	00000000009*C*8201	-3	009*C*820100000000	-3
9	000000039*C*7*A*0100	-8	9*C*7*A*010000000003	-8
10	00*E*803*BC*7*A*010000	-5	7*A*01000000*E*803*BC*	-5
11	*E*800*BCF*801000002	-6	01000002*E*800*BCF*8	-6
12	00*B*6*F*80100*B*002*E*8	-5	009002*E*800*B*6*F*801	-5
$\sum_r \log_2 pr$		-53		-53

5.2 MILP-based search for characteristics and differentials of HIGHT

The set of operations used in one round of HIGHT is as follows: two modular additions, two modular additions with one constant input (discussed in sec 2.3), two XORs, two F_0 functions, two F_1 functions, and a final swapping. There are also two XOR operations with subkeys which are effectless in differential attack and would be omitted from our model. Summing up all the constraints related to the above operations, our model has a number of $50n - 32$ constraints for one round where $n = 8$. The reader should be noted that by enjoying the new more efficient model giving in Section 2.3, the amount of reduction in the number of constraints is $2(8(n-1)) = 112$, per round.

Similar to LEA, it is impossible to solve a 11-round MILP model as a whole. So, again searching for the sub-optimal solutions explained in 3.2 would be a reasonable strategy here. In the following our results on 11, 12 and 13 rounds of HIGHT are reported.

Analysis of 11 and 12-round HIGHT According to the rule of sub-optimal solution searching, we divide the 12-round cipher into two 6-round subciphers and independently search each of them. The best 12-round differential characteristics have probability 2^{-53} and there are two such characteristics for HIGHT,

Table 8. Differential characteristics for 13-round HIGHT

Rounds	First characteristic		Second characteristic	
	$\Delta x_0 \|\| \Delta x_1 \|\| \cdots \|\| \Delta x_6 \|\| \Delta x_7$	$\log_2 p$	$\Delta x_0 \|\| \Delta x_1 \|\| \cdots \|\| \Delta x_6 \|\| \Delta x_7$	$\log_2 p$
0	01004483E20084F2		01004483E20084F2	
1	000083E20080F201	-3	20005E030000AB3B	-3
2	0000E2C1804A0100	-9	004A030000003B20	-7
3	0000C1184A010000	-6	4A010000000020B8	-10
4	000018C801000000	-6	010000000000B8C8	-4
5	0000C80100000000	-4	000000000000C801	-4
6	0000010000000000	-3	0000000000000100	-3
7	**0001000000000000**	**-1**	**0000000000010000**	**-1**
8	0100000000000082	-2	0000008201000000	-2
9	00000000009C8201	-3	009C820100000000	-3
10	000000039C7A0100	-8	9C7A010000000003	-8
11	00E803BC7A010000	-5	7A01000000E803BC	-5
12	E800BCF801000002	-6	01000002E800BCF8	-6
13	00B6F80100B002E8	-5	009002E800B6F801	-5
$\sum_r \log_2 pr$		-61		-61

one of which was found in [34]. In the first one, reported in [34] too, the internal difference at round six is $(0001, 0000, 0000, 0000)$ and in the other one, reported for the first time in this paper, it is $(0000, 0000, 0001, 0000)$. These two characteristics have been shown in Tab. 8.

Having found the sub-optimum characteristics, we start searching for the other characteristics with the same input/output difference to compute the differential probability. For the second case, the probability polynomials of subciphers are derived as follows.

$$\begin{aligned} p_1(x) &= x^{24} + x^{33} + x^{35} + x^{38} + x^{39} + 3x^{41} + 2x^{42} \\ p_2(x) &= x^{29} + 4x^{40} + 4x^{41} + 4x^{42} + 15x^{43} \end{aligned} \tag{21}$$

and the probability polynomial of the 12-round characteristic is

$$\begin{aligned} p(x) &= p_1(x)p_2(x) \\ &= x^{53} + x^{62} + 5x^{64} + 4x^{65} + 4x^{66} + 16x^{67} + \\ &\quad x^{68} + 3x^{70} + 2x^{71} + 4x^{73} + 4x^{74} + 8x^{75} + \\ &\quad 4x^{76} + 19x^{77} + 19x^{78} + 8x^{79} + 8x^{80} + \\ &\quad 31x^{81} + 35x^{82} + 20x^{83} + 53x^{84} + 30x^{85} \end{aligned} \tag{22}$$

An interesting observation about HIGHT is that, despite LEA, it does not show a strong differential effect. The probability polynomial is sparse and a small number of characteristics with insignificant probabilities matches this differential. Hence, the differential probability is approximately equal to its only dominant characteristic probability which is equal to

$$p(x)|_{x=\frac{1}{2}} \simeq 2^{-53} \tag{23}$$

To have a comparison with 11-round characteristic found in [13], we can omit the last round of these 12-round characteristics to come up with a 11-round characteristics with probability 2^{-47}. However, we repeated the search for sub-optimal solution for the 11-round problem and found a characteristic with probability 2^{-45} which is much more efficient than that found in [13] with probability 2^{-58}.

Analysis of 13-round HIGHT The 13-round sub-optimal characteristic of HIGHT would be found by dividing it into 7 and 6-round subciphers, respectively. These characteristics are reflected in Tab. 7. The best two characteristics constrained to have weight one at the middle (round 7). For the 13-round case, the best found characteristics have the differences $(0000, 0000, 0001, 0000)$ or $(0001, 0000, 0000, 0000)$ at round 7, again. Furthermore, their downward propagation patterns, i.e. in the second subcipher, are exactly the same as the 12-round characteristics. But, their 7-round upward patterns are completely different. It means that sub-optimum 13-round characteristic does not necessarily derived by extending the sub-optimum 12-round characteristic for one round.

Now, we compute the probability polynomials of the two subciphers as follows:

$$\begin{aligned} p_1(x) &= x^{32} + x^{38} + x^{43} + 2x^{44} \\ p_2(x) &= x^{29} + 4x^{40} + 4x^{41} + 4x^{42} + 15x^{43} \end{aligned} \tag{24}$$

And the probability of differential as:

$$p(x)|_{x=\frac{1}{2}} = p_1(x)p_2(x)|_{x=\frac{1}{2}} =\simeq 2^{-61} \tag{25}$$

The above information are related to the 13-round characteristic with the 7-th round difference $(0000, 0000, 0001, 0000)$.

6 Conclusion

This work gave a more precise analysis for the differential property of ARX ciphers using MILP technique. We improved the general MILP model for modular addition in a special case and come up with a simpler and faster solvable model. Two block ciphers LEA and HIGHT were studied as instances of ARX ciphers for both of which the results were improved significantly.

The MILP model constructed to find the (sub-)optimal characteristic intrinsically fits to compute differential probability, as well. We enjoyed this capability

and investigated the differential effect in these two ciphers. Our findings show that despite LEA which has a strong differential effect, HIGHT does not show such an effect.

Bibliography

[1] Aumasson, J.P., Henzen, L., Meier, W. and Phan, R.C.W., 2008. Sha-3 proposal blake. *Submission to NIST*.

[2] Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J. and Walker, J., 2010. The Skein hash function family. *Submission to NIST (round 3)*, 7(7.5), p.3.

[3] Bernstein, D.J., 2008. The Salsa20 family of stream ciphers. In *New stream cipher designs* (pp. 84-97). Springer, Berlin, Heidelberg.

[4] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J. and Wingers, L., 2015, June. The SIMON and SPECK lightweight block ciphers. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE* (pp. 1-6). IEEE.

[5] Aumasson, J.P. and Bernstein, D.J., 2012, December. SipHash: a fast short-input PRF. In *International Conference on Cryptology in India* (pp. 489-508). Springer, Berlin, Heidelberg.

[6] Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B. and Verbauwhede, I., 2014, August. Chaskey: an efficient MAC algorithm for 32-bit microcontrollers. In *International Workshop on Selected Areas in Cryptography* (pp. 306-323). Springer, Cham.

[7] Bernstein, D.J., 2008, January. ChaCha, a variant of Salsa20. In *Workshop Record of SASC* (Vol. 8, pp. 3-5).

[8] Wu, H., 2008. The stream cipher HC-128. In *New stream cipher designs* (pp. 39-47). Springer, Berlin, Heidelberg.

[9] Hong, D., Lee, J.K., Kim, D.C., Kwon, D., Ryu, K.H. and Lee, D.G., 2013, August. LEA: A 128-bit block cipher for fast encryption on common processors. In *International Workshop on Information Security Applications* (pp. 3-27). Springer, Cham.

[10] Shimizu, A. and Miyaguchi, S., 1987, April. Fast data encipherment algorithm FEAL. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 267-278). Springer, Berlin, Heidelberg.

[11] Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J. and Walker, J., 2010. The Skein hash function family. *Submission to NIST (round 3)*, 7(7.5), p.3.

[12] Rivest, R.L., 1994, December. The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86-96). Springer, Berlin, Heidelberg.

[13] Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.S., Lee, C., Chang, D., Lee, J., Jeong, K. and Kim, H., 2006, October. HIGHT: A new block cipher suitable for low-resource device. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 46-59). Springer, Berlin, Heidelberg.

[14] Matsui, M., 1994, May. On correlation between the order of S-boxes and the strength of DES. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 366-375). Springer, Berlin, Heidelberg.

[15] Biryukov, A. and Nikolić, I., 2011, February. Search for related-key differential characteristics in DES-like ciphers. In *International Workshop on Fast Software Encryption* (pp. 18-34). Springer, Berlin, Heidelberg.

[16] Mouha, N. and Preneel, B., 2013. Towards finding optimal differential characteristics for ARX: Application to Salsa20. *Cryptology ePrint Archive, Report 2013/328*.

[17] Aumasson, J.P., Jovanovic, P. and Neves, S., 2014, September. Analysis of NORX: investigating differential and rotational properties. In *International Conference on Cryptology and Information Security in Latin America* (pp. 306-324). Springer, Cham.

[18] Kölbl, S., Leander, G. and Tiessen, T., 2015, August. Observations on the SIMON block cipher family. In *Annual Cryptology Conference* (pp. 161-185). Springer, Berlin, Heidelberg.

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

[20] Wu, S. and Wang, M., 2011. Security Evaluation against Differential Cryptanalysis for Block Cipher Structures. *IACR Cryptology ePrint Archive*, 2011, p.551.

[21] Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X. and Song, L., 2014, December. 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). Springer, Berlin, Heidelberg.

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

[23] Sun, S., Hu, L., Song, L., Xie, Y. and Wang, P., 2013, November. Automatic security evaluation of block ciphers with S-bP structures against related-key differential attacks. In *International Conference on Information Security and Cryptology* (pp. 39-51). Springer, Cham.

[24] Sasaki, Y. and Todo, Y., 2018. Tight Bounds of Differentially and Linearly Active S-Boxes and Division Property of Lilliput. IEEE Transactions on Computers, 67(5), pp.717-732.

[25] Xiang, Z., Zhang, W., Bao, Z. and Lin, D., 2016, December. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 648-678). Springer, Berlin, Heidelberg.

[26] Fu, K., Wang, M., Guo, Y., Sun, S. and Hu, L., 2016, March. MILP-based automatic search algorithms for differential and linear trails for speck. In *International Conference on Fast Software Encryption* (pp. 268-288). Springer, Berlin, Heidelberg.

[27] Cui, T., Jia, K., Fu, K., Chen, S. and Wang, M., 2016. New Automatic Search Tool for Impossible Differentials and Zero-Correlation Linear Approximations. *IACR Cryptology ePrint Archive*, 2016, p.689.

[28] Wu, S., Wu, H., Huang, T., Wang, M. and Wu, W., 2013, December. Leaked-state-forgery attack against the authenticated encryption algorithm ALE. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 377-404). Springer, Berlin, Heidelberg.

[29] Lipmaa, H. and Moriai, S., 2001, April. Efficient algorithms for computing differential properties of addition. In *International Workshop on Fast Software Encryption* (pp. 336-350). Springer, Berlin, Heidelberg.

[30] Winnen, L., Sage S-box MILP toolkit.

[31] Lai, X., Massey, J.L. and Murphy, S., 1991, April. Markov ciphers and differential cryptanalysis. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 17-38). Springer, Berlin, Heidelberg.

[32] Song, L., Huang, Z. and Yang, Q., 2016, July. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In *Australasian Conference on Information Security and Privacy* (pp. 379-394). Springer, Cham.

[33] Dwivedi, A.D. and Srivastava, G., Differential Cryptanalysis in ARX Ciphers, Applications to LEA, *Cryptology ePrint Archive, Report 2018/898* . .

[34] Yin, J., Ma, C., Lyu, L., Song, J., Zeng, G., Ma, C. and Wei, F., 2017, November. Improved Cryptanalysis of an ISO Standard Lightweight Block Cipher with Refined MILP Modelling. In International Conference on Information Security and Cryptology (pp. 404-426). Springer, Cham.

[35] Song, L., Huang, Z. and Yang, Q., 2016, July. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In Australasian Conference on Information Security and Privacy (pp. 379-394). Springer, Cham.

[36] Sun, L., Wang, W. and Wang, M., 2017, December. Automatic search of bit-based division property for ARX ciphers and word-based division property. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 128-157). Springer, Cham.

[37] Zhang, P., Sun, B. and Li, C., 2009, December. Saturation attack on the block cipher HIGHT. In International Conference on Cryptology and Network Security (pp. 76-86). Springer, Berlin, Heidelberg.

[38] Wen, L., Wang, M., Bogdanov, A. and Chen, H., 2014. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: improved cryptanalysis of an ISO standard. Information Processing Letters, 114(6), pp.322-330.

[39] Chen, J., Wang, M. and Preneel, B., 2012, July. Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. In

International Conference on Cryptology in Africa (pp. 117-137). Springer, Berlin, Heidelberg.
[40] Ahmadi, S., Ahmadian, Z., Mohajeri, J. and Aref, M.R., 2014. Low Data Complexity Biclique Cryptanalysis of Block Ciphers with Application to Piccolo and HIGHT. IEEE Trans. Information Forensics and Security, 9(10), pp.1641-1652.
[41] Azimi, S.A., Ahmadi, S., Ahmadian, Z., Mohajeri, J. and Aref, M.R., 2018. Improved impossible differential and biclique cryptanalysis of hight. International Journal of Communication Systems, 31(1), p.e3382.

Appendix A

Table 9. Linear inequalities expressing modular addition in general form

$$
\begin{aligned}
&\beta[i] - \gamma[i] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&\alpha[i] - \beta[i] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&-\alpha[i] + \gamma[i] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&-\alpha[i] - \beta[i] - \gamma[i] - (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq -3,\\
&\alpha[i] + \beta[i] + \gamma[i] - (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&-\beta[i] + \alpha[i+1] + \beta[i+1] + \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&\beta[i] + \alpha[i+1] - \beta[i+1] + \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&\beta[i] - \alpha[i+1] + \beta[i+1] + \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&\alpha[i] + \alpha[i+1] + \beta[i+1] - \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq 0,\\
&\gamma[i] - \alpha[i+1] - \beta[i+1] - \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq -2,\\
&-\beta[i] + \alpha[i+1] - \beta[i+1] - \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq -2,\\
&-\beta[i] - \alpha[i+1] + \beta[i+1] - \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq -2,\\
&-\beta[i] - \alpha[i+1] - \beta[i+1] + \gamma[i+1] + (\neg eq(\alpha[i], \beta[i], \gamma[i])) \geq -2.
\end{aligned}
$$