New Automatic Search Method for Truncated-Differential Characteristics

Application to Midori, SKINNY and CRAFT

AmirHossein EbrahimiMoghaddam and Zahra Ahmadian

Electrical Engineering Department, Shahid Beheshti University, Tehran, Iran,
amirebrahimi18@yahoo.com
z_ahmadian@sbu.ac.ir

Abstract. In this paper, using Mixed Integer Linear Programming, a new automatic search tool for truncated differential characteristic is presented. While the previous MILP models for truncated differential characteristic has been used just as a facilitator for finding the bit-wise differential characteristic with maximum probability, ours considers truncated differential characteristic as an stand-alone distinguisher. Our method models the problem of finding a maximal probability truncated differential characteristic, being able to distinguish the cipher from a pseudo random permutation. Our model enjoys a word-wise variable definitions which makes it much simpler and more easily solvable than its bit-wise counterpart.
Using this method, we analyse Midori64, SKINNY64/X and CRAFT block ciphers, for all of which the existing results are improved. In all cases, the truncated differential characteristic is much more efficient than the (upper bound of) bit-wise differential characteristic proven by the designers, for any number of rounds. More specifically, the highest possible rounds, for which an efficient differential characteristic can exist for Midori64, SKINNY64/X and CRAFT are 6, 7 and 10 rounds respectively, for which differential characteristics with maximum probabilities of 2^{-60}, 2^{-52} and $2^{-62.61}$ (may) exist. However, we introduce new truncated differential characteristics for 6-round of Midori64 with probability 2^{-54}. In case of SKINNY64/X and CRAFT, the gap is much wider. For 7 rounds of Midori64, we find a truncated characteristic with probability 2^{-4}, and even a 10-round truncated characteristic can be found with probability 2^{-40}. Moreover, our result outperforms the only truncated differential analysis that exists on Midori64. For CRAFT we find a 10, 11 and 12 truncated characteristic with probabilities of 2^{-28}, 2^{-32} and 2^{-36}, respectively. This method can be used as a new tool for differential analysis of SPN block ciphers.

Keywords: Truncated Differential · MILP · SPN

1 Introduction

Truncated differential attack is a variant of differential attack introduced by Knudsen in 1994 [11]. Despite the basic differential attack, in which the precise bit-wise value of the input/output (and internal) differences are specified, in truncated differential cryptanalysis, one considers the word-wise differences where the word size can be a nibble, byte, etc., usually equal to the S-box size in the design. Some examples of truncated differential attacks are [17, 12, 13].

Truncated differential characteristics can offer efficient distinguishers for block ciphers, even more efficient than their bit-wise counterpart, in some cases. A well-known instance is KLEIN block cipher, while its security against bit-wise differential attack had been proved in [10], it was broken by some truncated differential attacks [12, 17].

However, while the designers prove upper bounds for bit-wise differential characteristics and greedily try to tighten it more and more, there is no provable method to measure the strength of truncated differential characteristics for block ciphers. Apart from the lack of a provable method, there is not almost any systematic approach for finding efficient truncated differential characteristics. Except a meet in the middle-based method proposed in [13] for finding truncated differential characteristic, which was applied to CLEFIA and Camellia block ciphers and later to MCrypton and CRYPTON v.1 [24].

On the other hand, since the variables are defined word-wise in truncated differential attack, the search space is not as large as that of bit-wise differential attacks. So, it must not be too infeasible to intelligently search the whole space in order to find the best possible truncated differential characteristic by an appropriate search tool. The only work focusing on this problem is a 2 decades old search algorithm proposed by Moriai et al. which was applied to E2 block cipher [14] and later to Midori cipher [8].

Mixed Integer Linear Programming (MILP) has been recently known as an effective automated tool for cryptanalysis of symmetric ciphers such as differential [21], impossible differential [18], zero correlation [7] and integral [23] attacks. The scope of MILP is not confined to SPN structure only, as there are innovative results in cryptanalysis of ciphers with ARX structure, mostly using linear, differential, impossible differential and zero correlation attacks [9, 2, 3, 16].

In case of bit-wise differential cryptanalysis of SPN ciphers, the MILP-based characteristic search problem has progressed from the simple problem of counting the minimum number of active S-boxes [15] into finding the precise maximal probability characteristic for some lightweight ciphers [21, 1]. MILP modeling of S-boxes which is the most challenging part of the MILP modeling of differential attack is now feasible even for 8×8 S-boxes [1]. However, as far as the truncated differential attack is concerned, the existing MILP models work up to finding a characteristic with minimum number of active S-boxes, supposed to be instantiated by a bit-wise characteristic later [21, 1]. Another trace of MILP modeling of truncated differential characteristic is seen in impossible differential characteristic search [18], where the worst case propagation of truncated differentials is modeled. So, there is not any MILP model concentrating on finding the optimal truncated differential characteristic, as an stand-alone distinguisher with maximum probability.

Our contributions. This paper focuses on the problem of MILP modeling of truncated differential characteristic. In this model the variables are defined word-wise, so the number of variables does not grow too fast as the number of rounds grows. Moreover, since truncated differential attack is irrelevant to the S-box specifications, its MILP model is free of modeling the S-boxes which was a bottleneck in its bit-wise counterpart. In this model, using an appropriately defined objective function, we can find the optimum truncated differential characteristic, which covers the most possible number of rounds with highest possible probability, yet distinguishing the cipher from a pseudo random permutation (PRP) .

Having modeled the truncated differential characteristic, we examine our search tool on three remarkable SPN ciphers SKINNY64/X, where $X = 64, 128, 192$ [5], Midori64 [4] and CRAFT [6]. we observe that for all of them, for any rounds that bit-wise differential characteristic works, the truncated differential characteristic has a probability higher than the upper bound of any bit-wise differential characteristic, proven by the designers or third parties. For more details, see Tabs. 1,2 and 3. This shows that, beside the valuable efforts on finding and tightening the upper bound of the bit-wise differential probability, evaluating the strength of the cipher against other kinds of differential attack can be of considerable importance.

This is the first external analysis of CRAFT. SKINNY64/X has not ever been received any internal or external truncated differential analyses. However, for Midori64, a truncated

Table 1: Comparison of bit-wise differential and truncated differential characteristics for Midori64

Number of rounds	4	5	6	Ref.
Upper bound for bit-wise differential characteristic probability	2^{-32}	2^{-46}	2^{-60}	[4]
Truncated differential probability	$\mathbf{2^{-12}}$	$\mathbf{2^{-24}}$	$\mathbf{2^{-54}}$	**Sec. 4**

Table 2: Comparison of bit-wise differential and truncated differential characteristics for SKINNY64/X

Number of rounds	6	7	8	9	10	Ref.
Upper bound for bit-wise differential characteristic probability	2^{-32}	2^{-52}	2^{-72}	2^{-82}	2^{-92}	[5]
Truncated differential probability	$\mathbf{2^{-4}}$	$\mathbf{2^{-4}}$	$\mathbf{2^{-8}}$	$\mathbf{2^{-20}}$	$\mathbf{2^{-40}}$	**Sec. 4**

Table 3: Comparison of bit-wise differential and truncated differential characteristics for CRAFT

Number of rounds	8	9	10	Ref.
Upper bound for bit-wise differential characteristic probability	2^{-52}	2^{-64}	2^{-72}	[6]
The best found differential probability	-	$2^{-54.67}$	$2^{-62.61}$	[6]
Truncated differential probability	$\mathbf{2^{-20}}$	$\mathbf{2^{-24}}$	$\mathbf{2^{-28}}$	**Sec. 4**

Table 4: Summary of 4-round truncated differential characteristics for Midori64

Probability	Method	Reference
2^{-44}	Moriai et. al. [14]	[8]
$\mathbf{2^{-20}}$	**MILP-based, Strategy I**	**Sec. 4**
$\mathbf{2^{-12}}$	**MILP-based, Strategy II**	**Sec. 4**

differential cryptanalysis has been reported [8], in which the automatic search tool of [14] is used. Despite the claim in [8], we found a more probable 4-round truncated characteristic and an efficient 5-round one. For more details see Tab. 4.

Organization of the paper. In Section 2, we bring the preliminaries of the paper, including a brief description of Midori, SKINNY and CRAFT block ciphers and a review of the MILP problem and related work. In Section 3, we present our new method for automatic search for truncated differential characteristic by MILP. In Section 4, we apply our automatic search to Midori, SKINNY and CRAFT where we bring our results and compare them with previous ones. Finally, Section 5 concludes the paper.

2 Preliminaries

In this section we review the structure of Midori, SKINNY and CRAFT block ciphers, which are the ciphers analyzed in this paper. All of them has a AES-like structure with a 4 × 4 state of bytes (nibbles) and a round function composed of a S-box layer, a byte(nibble)-wise permutation, and a column-wise MixColumn operation.

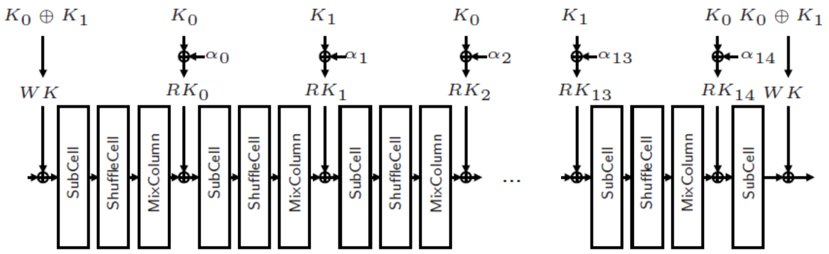

Figure 1: Overview of one round of Midori64 [4]

2.1 Midori Specifications

Midori is a lightweight SPN block cipher proposed in AISACRYPT 2015 [4]. It has two versions Midori64 and Midori128, with 64-bit and 128-bit block sizes, respectively, however both of which work with 128-bit keys. The state of Midori block cipher is expressed as a 4×4 matrix as below:

$$\begin{pmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{pmatrix} \tag{1}$$

for Midori64 each cell of state matrix, $s_i, i = 0, \ldots, 15$, has 4 bits length (nibble) and for Midori128 each cell is 8 bits. At first, a whitening key is added to the state matrix and then the result goes through round functions. Each round function of Midori consist of the following transformations:

- **AddRoundKey (AK)**: The subkey RK_r is added to the intermediate state.
- **SubCell (SC)**: The intermediate state goes through 16 S-boxes (the size of the S-boxes depends on the cipher variant).
- **ShuffleCell (ShC)**: The cells in the state are permuted as follows.

$$(s_0, s_1, ..., s_{15}) \longrightarrow (s_0, s_{10}, s_5, s_{15}, s_{14}, s_4, s_{11}, s_1, s_9, s_3, s_{12}, s_6, s_7, s_{13}, s_2, s_8) \tag{2}$$

- **MixColumn (MC)**: An almost MDS binary matrix M is applied to each column of the intermediate state matrix

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

The S-box used in Midori64 is a 4-bit S-box, while for Midori128, it is a 8-bit one. Number of rounds for Midori64 is 16 and for Midori128 is 20. In the last round, linear layers (SC and MC) are omitted and finally the whitening key is added to state matrix.

Midori128 doesn't employ any key schedule and for Midori64 the key schedule is very simple. For Midori64 the 128 bit secret key is divided into two 64-bit halves K_0, K_1, then the round key is determined by $RK_r = K_{rmod2}$. This keys are XORed with a round constant named α_r before AddRoundKey operation. Whitening key of Midori128 is the same as the secret key while for Midori64 it is $WK = K_0 \oplus K_1$. Fig. 1 shows an overview of Midori64.

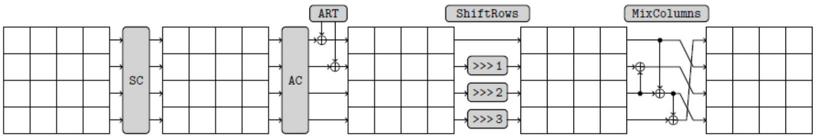

Figure 2: Overview of one round of SKINNY [5]

2.2 SKINNY Specifications

SKINNY is a lightweight SPN cipher proposed in CRYPTO 2016. It takes tweakey rather than the secret key. SKINNY has many variants depending on the block and tweakey sizes which are detailed in [5]. However, in the following we describe SKINNY64/X, the version analyzed in this paper, whose block size is 64 bits and key size can be $X = 64, 128, 192$ bits. All variants of SKINNY initialize plaintext in a 4×4 state matrix, then it goes through round functions. Each round function of SKINNY consists of five transformations of SubCell, AddConstant, AddRoundTweakey, ShiftRows and MixColumn. SKINNY does not have any whitening key.

- **SubCell (SC)**: The state matrix goes through 16 S-boxes.
- **AddConstant (AC)**: A round constant is added to the state matrix.
- **AddRoundTweakey (ART)**: The tweakey TK_r is added to the state matrix.
- **ShiftRows (SR)**: The second, third, and fourth cell rows are rotated by 1, 2 and 3 positions to the right, respectively. The first row remains unchanged.
- **MixColumn (MC)**: A binary matrix M is multiplied by each column of intermediate state matrix

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

Fig. 2 illustrates one round function of SKINNY.

2.2.1 CRAFT

CRAFT block cipher was proposed in IACR TOSC 2018 [6]. This cipher follows an innovative approach, which is protection against differential fault attack in the design phase. It is a lightweight block cipher with a 128-bit key, a 64-bit tweak and a 64-bit block arranged in a 4×4 matrix of nibbles, numbered as follows:

$$\begin{pmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \tag{4}$$

Each round of CRAFT consists of the following transformations, which is applied to the input state according to the following order.

- **MixColumn (MC)**: The following binary matrix M is multiplied to each column of the state.

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{5}$$

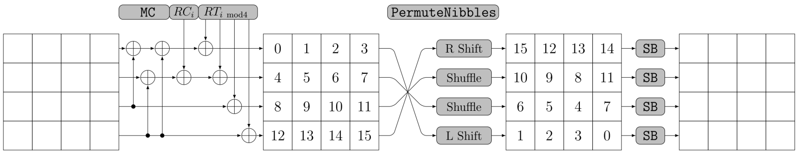

Figure 3: Overview of one round of CRAFT [6]

- **AddConstants (ARC)**: A round Constant is added to the state matrix.
- **AddTweakey (ATK)**: The tweakey TK_r is added to the state matrix.
- **PermuteNibbles (PN)**: The cells in the states are permuted as follows.

$$(s_0, s_1, \ldots, s_{15}) \rightarrow (s_{15}, s_{12}, s_{13}, s_{14}, s_{10}, s_9, s_8, s_{11}, s_6, s_5, s_4, s_7, s_1, s_2, s_3, s_0) \quad (6)$$

- **SubBox (SB)**: The state matrix goes through 16 parallel S-boxes.

For more details about this cipher, one can refer to [6]. Fig. 2.2.1 shows one round of CRAFT.

In Midori and SKINNY, the linear layers come after the nonlinear (S-box) layer in each round. This type of SPN cipher will be called S-then-P structure, in this paper. However, for CRAFT the linear layers are applied first, then the S-box layer comes. We call this SPN structure P-then-S.

2.3 MILP-based differential cryptanalysis

2.3.1 MILP definition

Linear Programming is a class of optimization problems in which the objective function and all constraints are linear functions in decision variables $\mathbf{x} = [x_1, x_2, \ldots, x_n]$. So, an LP problem is as the following form:

$$\begin{aligned} \text{minimize} \quad & \mathbf{c}^T\mathbf{x} \\ \text{subject to} \quad & A\mathbf{x} \leq \mathbf{b} \\ \text{and} \quad & \mathbf{x} \geq 0 \end{aligned} \quad (7)$$

if all or part of the decision variables are integer-valued, the LP problem is called MILP. An MILP problem is inherently NP-complete, however there are either commercial or open source solvers, which are able to solve some not-too-complicated instances of MILP problem. A recent trend in symmetric cryptanalysis is using this tool for finding (sub-)optimal (differential, linear, integral, cube, etc.) characteristics for symmetric primitives.

2.4 Related work

In this section we review the developments of MILP-based techniques in differential cryptanalysis of SPN ciphers. The early work in this area belongs to [15, 22] which searches the minimum number of active S-boxes in SPN ciphers with word-oriented diffusion layers. In these models the differential property of the diffusion layer is taken into account up to its branch number while the information of S-boxes differential properties is not included, at all. The next work, [21], extends the coverage of this method to the SPN ciphers with bit-wise permutation diffusion layers, though with the same objective function and same limitations. A significant work is done in [20], where the differential properties of the S-box along with their probabilities are included in the model. This method enables the cryptanalyst to construct a more accurate feasible set for the MILP problem and set the objective function equal to the precise probability of the differential characteristic, rather than the number of active S-boxes, merely.

However, the method proposed in [20] for modeling S-box is effective for small S-boxes (at most 4×4). Abdelkhalek et al. developed a method for MILP modeling of large S-boxes (up to 8×8) and applied it to SKINNY block cipher and a AES-based MAC [1]. Besides these improvements in differential attack, the problem of searching impossible differential characteristic is also modeled by MILP in [18].

Therefore there are lots of work in employing MILP technique for finding bit-wise differential characteristic for SPN ciphers, but this is not the case with truncated differential cryptanalysis. MILP modeling for truncated differential characteristic is paid attention just in [1] and [18]. In the former, truncated characteristic is treated just as a facilitator to find the optimal bit-wise differential characteristic. In that work, it is targeted to find a minimum active S-box truncated differential characteristic to be instantiated later by a bit-wise characteristic. In the latter, truncated characteristic is used as a tool for fining the impossible differential characteristic. So, a worst-case scenario for propagation of the truncated differential characteristic (i.e. the propagation with probability one) is modeled and utilized for finding impossible differential characteristic.

3 New MILP-based automatic truncated differential search

Despite the bit-wise differential characteristics, there is not any systematic method for proving an upper bound for the probability of the truncated differential characteristic in SPN ciphers. Moreover, the only automatic search algorithm for finding optimal truncated differential characteristic is an exhaustive-type one, dating back two decades [14].

In this section, we propose an efficient technique for MILP modeling the truncated differential characteristic search problem for SPN structures. Due to the word-wise essence of this attack, we use the word-wise variable definition in the MILP-model as well, where the word size is equal to the S-box size in the cipher. In this model all the variables are binary, indicating that the associated word is active (1) or inactive (0).

It is clear that in any kind of (single-key) differential characteristic, XORing with constants, round keys and tweakeys are effectless on the characteristic. In addition, word-wise permutations, such as ShuffleCell in Midori, ShiftRows in SKINNY and PermuteNibbles in CRAFT can be modeled by a simple variable change. Moreover, as we adopted the word-wise variable definition, and assuming bijective S-boxes, the S-box layer would be totally bypassed in our model, hence the input and output of the S-box are indicated by a single binary variable. so, the only layer that plays a decisive and key role in both the propagation pattern of the truncated characteristic and its probability is MixColumn layer.

3.1 MILP model for Diffusion Property of MixColumns

Suppose that the cipher state is a $k \times k$ matrix of m-bit words. So, the MixColumn matrix would be a $k \times k$ matrix M over $GF(2^m)$ and each round contains k parallel MixColumns matrix multiplications. For a single MixColumn, the input and output truncated differential variables are denoted by $\mathbf{x} = (x_0, x_1, \ldots, x_k)^T$ and $\mathbf{y} = (y_0, y_1, \ldots, y_k)^T$, where $\mathbf{x}, \mathbf{y} \in (GF(2))^k$.

It is a straightforward task to compute the probability of all 2^{2k} truncated input/output differentials $P(\mathbf{x} \to \mathbf{y})$ and arrange them in a $2^k \times 2^k$ table called *branching property table* of M, whose rows are hexadecimal form of the input difference vector $\mathbf{x}$ and columns are the hexadecimal form of the output differences vector $\mathbf{y}$. In [14] a recursive method for computing these diffusion probabilities was proposed. Furthermore, these probabilities can be computed by direct analysis or by means of a simple programming. Since the word size is m bits here, the possible values for the probability $P(\mathbf{x} \to \mathbf{y})$ fall into the range

$$\{0, 1, 2^{-m}, 2^{-2m}, \ldots, 2^{-(k-1)m}\}. \tag{8}$$

The branching property tables of Midori, SKINNY and CRAFT MixColumns are shown in Appendix A. For more convenience, in the branching property table, the zero probabilities are shown by 0, the one probabilities are shown by 1, and the other probabilities $p \neq 0, 1$ are shown by $-log_2(p)$.

Those differentials with zero probability are called the impossible differentials that should be excluded from the feasible set of our MILP model. All the remaining differentials should be included in the feasible set, while their probabilities are encoded and defined as decision variables of the MILP model. The process is identical to the method of MILP modeling of differential property of (small) S-boxes [21]. We need to define at most $\lceil log_2(k) \rceil$ decision variables, denoted by $(p_0, p_1, \ldots, p_{\lceil log_2(k) \rceil})$, to encode the probability of all possible differentials of form $p = 2^{-m \sum_{i=0}^{\lceil log_2(k) \rceil} p_i 2^i}$. For example, for the MixColumn matrices of Midori, SKINNY and DRAFT which are 4×4 matrices over $GF(2^4)$, all possible probabilities are $\{0, 1, 2^{-4}, 2^{-8}\}$. The non-zero probabilities are encoded using $\lceil log_2(k) \rceil = 2$ bits (p_0, p_1) as follows.

$$\begin{aligned} 2^0 &\to (0,0) \\ 2^{-4} &\to (1,0) \\ 2^{-8} &\to (0,1) \end{aligned} \tag{9}$$

Finally, each possible differentials can be presented as a $(2k + [log_2(k)])$-tuple of the form

$$(x_0, x_1, \ldots, x_k, y_0, y_1, \ldots, y_k, p_1, \ldots, p_{[log_2(k)]}) \tag{10}$$

Using SAGE computer algebra system [19], one can derive the convex hull of all possible vectors of the form (10). The number of inequalities can be reduced dramatically using the greedy algorithm introduced in [21, 20].

The objective function that should be maximized is the probability of the differential truncated characteristic, which is equal to the product of all MixColumns diffusion probabilities in the characteristic. Equivalently, suppose the cipher under scrutiny has r rounds, each round contains k MixColumn matrix. The objective function, supposed to be minimized, is defined as

$$P_T = \sum_{j=1}^{rk} \sum_{i=0}^{k-1} p_{j,i} 2^i \tag{11}$$

where $p_{j,i}, i = 0, \ldots, k-1$ are the variables encoding the j^{th} MixColumn diffusion probability, $j = 1, \ldots, k$.

3.2 Efficient Characteristics

A truncated differential characteristic will be efficient, if it is able to distinguish the cipher from a Pseudo Random Permutation (PRP). Therefore, the probability of the truncated characteristic $P(\Delta_{in} \xrightarrow{E} \Delta_{out})$ must be greater than that of a PRP which is equal to $P(\Delta_{in} \xrightarrow{PRP} \Delta_{out}) = \frac{|\Delta_{out}|}{2^n}$, where n is the block size of the cipher in bits, here $n = k^2 m$.

3.2.1 Strategy I

A raw way to count $|\Delta_{out}|$, used also in [8], is to count the number of active words in the output difference, i.e. $Hw(\Delta_{out})$. If so, $|\Delta_{out}|$ would be $mHw(\Delta_{out})$. Therefore the

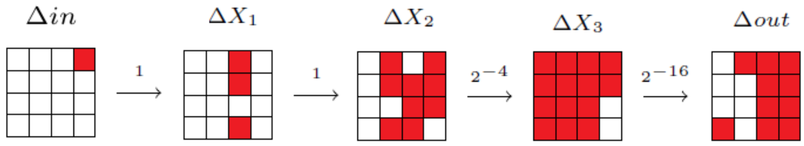

Figure 4: 4-round truncated differential characteristic by strategy I for Midori64.

distinguishability condition in our model is translated into a new linear constraint of the following form

$$P_T > k^2 - Hw(\Delta_{out}) \tag{12}$$

This constraint works correctly for the P-then-S structures, where there is no linear dependency between the active words of the output difference. However, as we will see for the S-then-P structures, this constraint incorrectly excludes some efficient truncated characteristics since $P(\Delta_{in} \xrightarrow{PRP} \Delta_{out})$ has been overestimated in this model.

3.2.2 Strategy II

The objection of Strategy I is that this model is not able to take into account the possible *linear dependencies* that definitely exists between the active words of the output difference, in the S-then-P structures. Linear dependencies, caused due to the last linear layer, makes $|\Delta_{out}|$ smaller than $mHw(\Delta_{out})$. For precise enumeration of $|\Delta_{out}|$, one should actually counts the number of active words in the last round's S-box layer. So, in the MILP model, it suffices that the distingushability constraint (12) be modified into

$$P'_T > k^2 - Hw(\Delta^S_{out}) \tag{13}$$

where Δ^S_{out} is the output difference of the last round's S-box layer and P'_T is the probability of the truncated characteristic excluding the last round's linear layer, i.e. $P'_T = \sum_{j=1}^{(r-1)k} \sum_{i=0}^{k-1} p_{j,i} 2^i$. Note that the objective function is still defined according to P_T in (11).

Although, such an approach finds the truncated differential characteristic with maximal probability, this optimum characteristic may activates *all* the output words. Although the linear relations between the active words of the output difference, along with (13), ensures that it is still an efficient distinguisher, its fully active output state may become challenging in the key recovery phase. Because it typically demands guessing the whole subkey of the next round which definitely is not desirable. To avoid such a situation, we add an extra constraint to the model, enforcing that not all the words in Δ_{out} are active, i.e.

$$Hw(\Delta_{out}) < k^2. \tag{14}$$

Therefore, for a given S-then-P cipher, the truncated differential characteristic derived by Strategy II is one round longer than that derived by Strategy I.

3.2.3 Strategy III

The characteristic found by Strategy I can be extended one round for free for the P-then-S structure, as well. It suffices that a P^{-1} transformation is applied to the input difference of the characteristic found by Strategy I. Here, P represents all the linear layers of one round of the cipher. This extension does not have any cost in the probability of the distinguisher. Clearly, there would be linear dependencies between the input differences of such truncated differential characteristic.

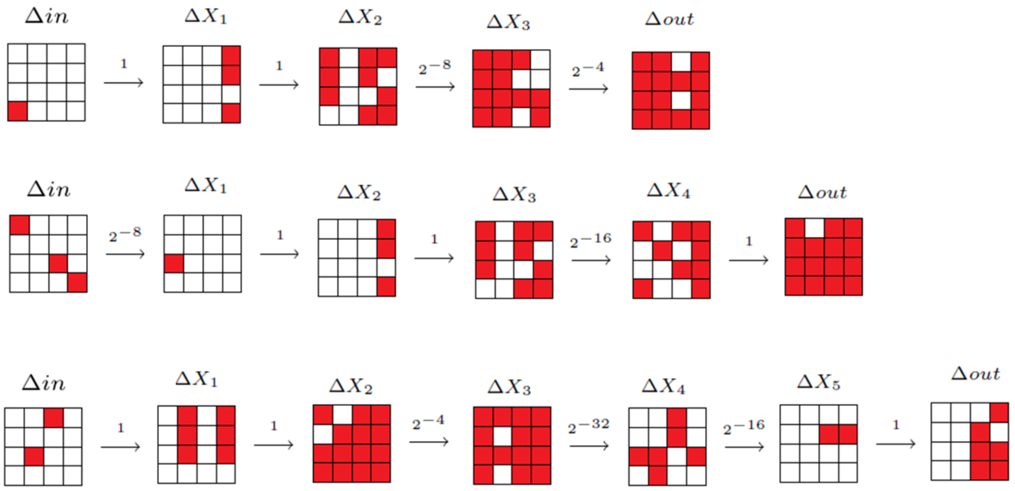

Figure 5: 4,5,6-round truncated differential characteristic by strategy II for Midori64.

4 Application to Midori64, SKINNY64/X and CRAFT

In this section, we report the new truncated differential characteristics we found by applying the proposed search method to three lightweight block ciphers Midori64, SKINNY64/X and CRAFT.

4.1 Midori64 truncated differential characteristics

According the method explained in Sec. 3.2, we first model the truncated differential property of the MixColumn of Midori64. The branching property table of Midori64 MixColumn is shown in Appendix A which can be modeled by 13 linear constraints.

4-round characteristic by Strategy I. In order to compare the MILP-based search method with Moriai et al. automatic search method [14], which was applied to Midori64 in [8], we first examine the less efficient strategy, Strategy I, which is the strategy chosen in [8], too. We found a 4-round characteristic with probability 2^{-20} shown in Fig. 4, while the highest-probability characteristic introduced in [8] is a 4-round one with probability 2^{-44}, claiming "there are no such truncated differentials with more than 4 rounds for Midori64".

4,5,6-round characteristic by Strategy II. Fig. 5, shows the 4,5,6-round characteristics found for Midori64 using Strategy II. The 4-round characteristic has a probability of 2^{-12}. This characteristic demonstrates the large gap that exists between these two strategies. The optimum 5-round characteristic has a probability of 2^{-24}. The highest possible number of rounds for which truncated distinguisher can be proposed is 6 round with probability of 2^{-52}. As it can be compared in Tab. 2, for any round that an efficient bit-wise differential characteristic may exist, there is a more efficient truncated differential characteristic, with better probability. For all above cases, the linear dependencies between Δ_{out} active nibbles are shown in Appendix B.

4.2 SKINNY64/X truncated differential characteristics

The branching property table of SKINNY is shown in Appendix A, which can be modeled using 12 linear inequalities. The branch number of SKINNY MixColumn is smaller than

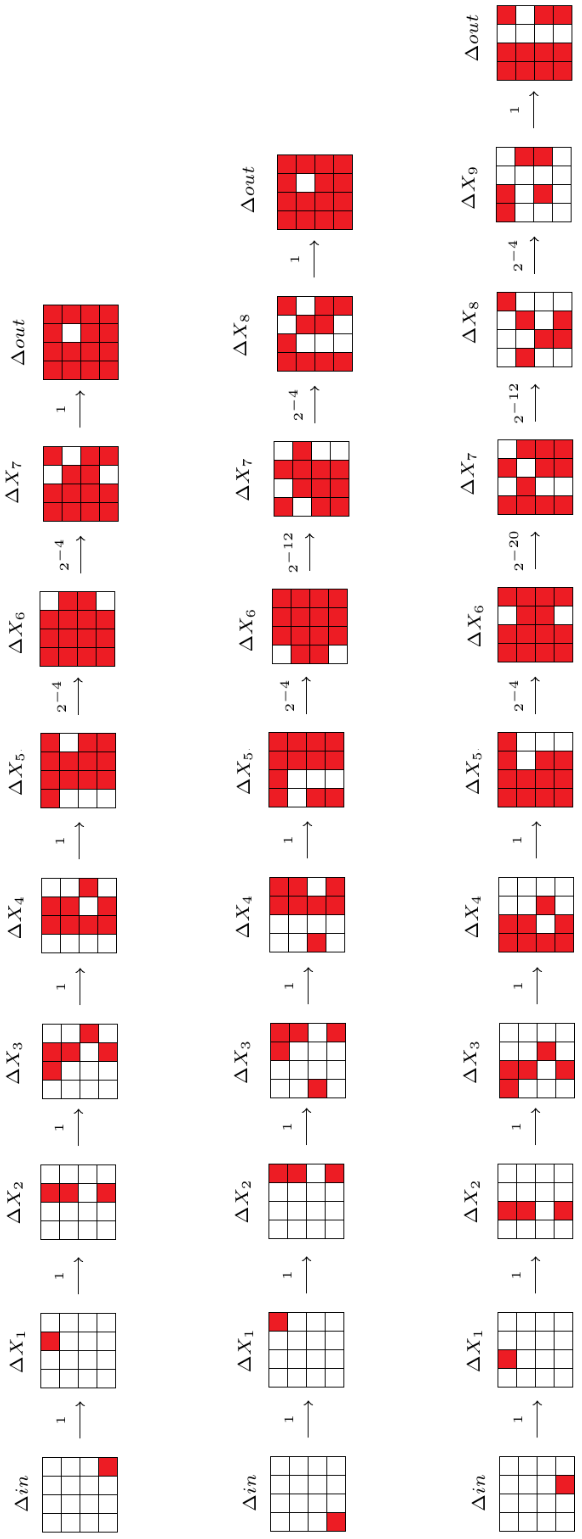

Figure 6: 8,9,10-round truncated differential characteristics by strategy II for SKINNY64/X.

Midori, expectedly resulting in a more sparse branching property table than Midori. In the following, we report our results on 7,8,10 rounds of SKINNY64/X which is considerably much more effective than Midori64, covering more number of rounds with larger probabilities.

8,9,10-round characteristic by Strategy II. SKINNY64/X has not ever been analyzed by truncated differential attack. Using Strategy II, we found efficient 8,9,10-round distinguishers, with probabilities 2^{-8}, 2^{-20} and 2^{-40}, respectively. These characteristics are shown in Fig. 6 and the linear dependencies between active nibbles of Δ_{out} is shown in Appendix C.

Comparing to Midori64, SKINNY64/X exhibits a much wider gap between the truncated and bit-wise differential probabilities, as reflected in Tab. 2, in details. The longest bit-wise differential characteristic that may exist for SKINNY64/X has 7 rounds with probability 2^{-52}, whilst at the same number of rounds, we have found a much stronger truncated differential characteristic with probability of 2^{-4}.

4.3 CRAFT truncated differential characteristics

The branching property table for CRAFT MixColumn is shown in Appendix A, which is modeled by 47 linear constraints. The diffusion property of CRAFT MixColumn is weaker than the two other ones, resulting in longer distinguishers with higher probabilities.

10,11,12-round characteristic by Startegy III. This is the first external analysis of CRAFT cipher. For this cipher, we observed one 1-round and two 2-round iterative truncated differential characteristics with probabilities 2^{-4} and 2^{-8}, respectively. Based on these characteristics, truncated differential distinguishers for 10, 11 and 12 rounds of CRAFT are introduced, which are shown in Fig.7 . Their respective probabilities are 2^{-24}, 2^{-32} and 2^{-36}. The input differences of all of these characteristics are linearly dependent, which are detailed in Appendix D.

Similar to SKINNY64/X, CRAFT shows a wide gap between the truncated and bit-wise differential characteristic probabilities, as it can be noticed in Tab. 3. With the help of strategy III, a 12-round truncated differential characteristic is found with probability of 2^{-36}, while the longest bit-wise one found in [6] has 10-rounds with characteristic probability of 2^{-72} and differential probability $2^{-62.61}$.

5 Conclusion

We proposed a new MILP-based automatic search method for finding truncated differential characteristic for SPN block ciphers. The proposed MILP model maximizes the truncated differential characteristic probability, ensuring its distinguishability from PRP, yet avoiding all output words being active. We applied our proposed method to Midori64, SKINNY64/X and CRAFT block ciphers. Comparing to its bit-wise counterpart, truncated differential attack enjoys a much smaller and less complicated S-box-free MILP model, which makes it much faster to be solved. More importantly, our results on Midori64, SKINNY64/128 and CRAFT shows that the optimal truncated differential characteristics found by this method are much more efficient than the upper bound of bit-wise differential characteristics proven for these three ciphers. This method can be used as a new tool for differential analysis of SPN ciphers.

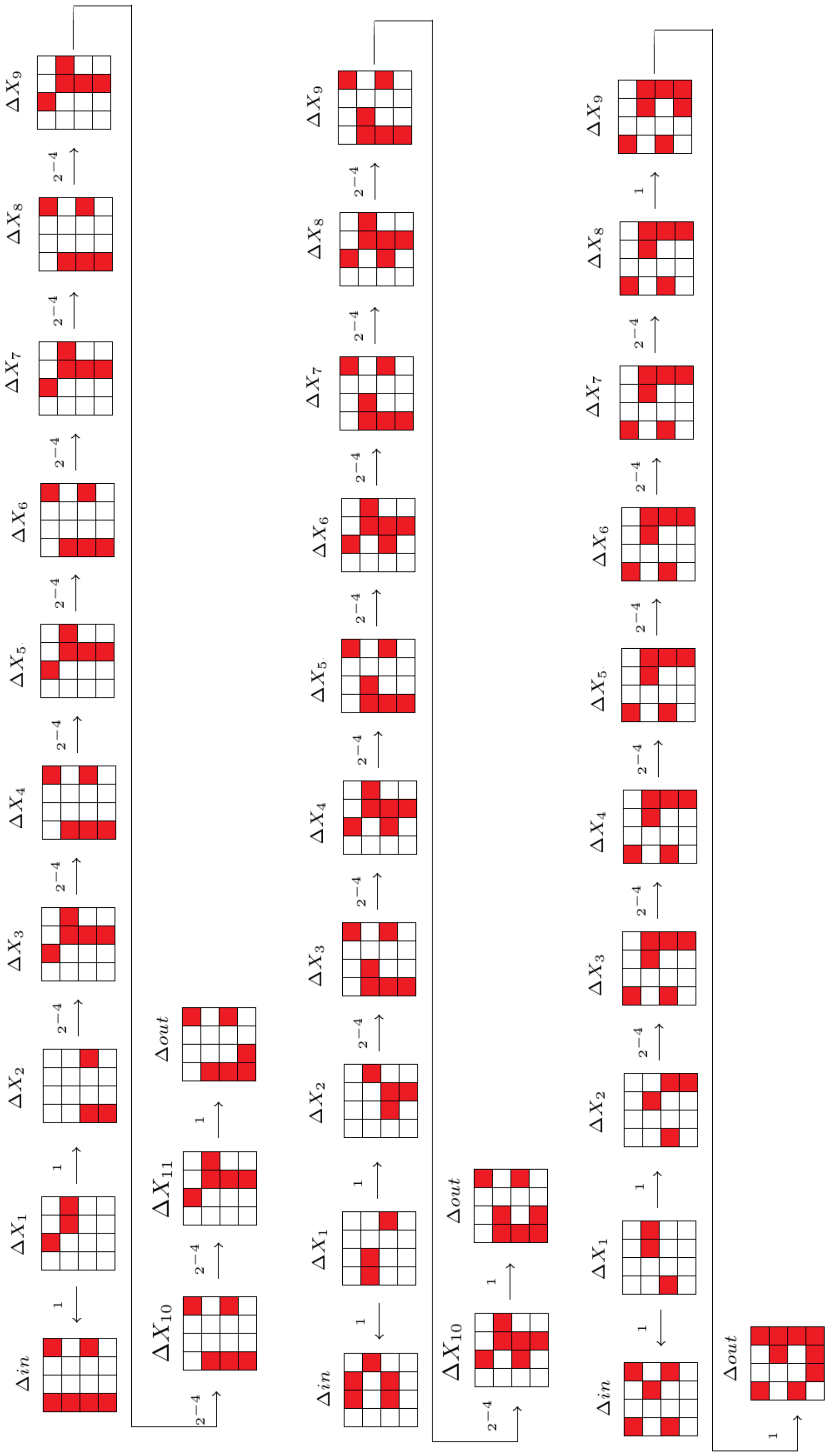

Figure 7: 10,11,112-round truncated differential characteristics by strategy III for CRAFT.

References

[1] Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, and Amr M Youssef. Milp modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Transactions on Symmetric Cryptology*, 2017(4):99–129, 2017.

[2] Ahmed Abdelkhalek, Mohamed Tolba, and Amr M Youssef. Impossible differential attack on reduced round sparx-64/128. In *International Conference on Cryptology in Africa*, pages 135–146. Springer, 2017.

[3] Elnaz Bagherzadeh and Zahra Ahmadian. Milp-based automatic differential searches for LEA and HIGHT. *IACR Cryptology ePrint Archive*, 2018:948, 2018.

[4] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: a block cipher for low energy. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 411–436. Springer, 2014.

[5] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The skinny family of block ciphers and its low-latency variant mantis. In *Annual Cryptology Conference*, pages 123–153. Springer, 2016.

[6] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. Craft: Lightweight tweakable block cipher with efficient protection against dfa attacks. *IACR Transactions on Symmetric Cryptology*, 2019(1):5–45, 2019.

[7] Tingting Cui, Keting Jia, Kai Fu, Shiyao Chen, and Meiqin Wang. New automatic search tool for impossible differentials and zero-correlation linear approximations. *IACR Cryptology ePrint Archive*, 2016:689, 2016.

[8] Xiaoyang Dong and Yanzhao Shen. Cryptanalysis of reduced-round midori64 block cipher. *IACR Cryptology ePrint Archive*, 2016:676, 2016.

[9] Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu. Milp-based automatic search algorithms for differential and linear trails for speck. In *International Conference on Fast Software Encryption*, pages 268–288. Springer, 2016.

[10] Zheng Gong, Svetla Nikova, and Yee Wei Law. Klein: a new family of lightweight block ciphers. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pages 1–18. Springer, 2011.

[11] Lars R Knudsen. Truncated and higher order differentials. In *International Workshop on Fast Software Encryption*, pages 196–211. Springer, 1994.

[12] Virginie Lallemand and María Naya-Plasencia. Cryptanalysis of klein. In *International Workshop on Fast Software Encryption*, pages 451–470. Springer, 2014.

[13] Leibo Li, Keting Jia, Xiaoyun Wang, and Xiaoyang Dong. Meet-in-the-middle technique for truncated differential and its applications to clefia and camellia. In *International Workshop on Fast Software Encryption*, pages 48–70. Springer, 2015.

[14] Shiho Moriai, Makoto Sugita, Kazumaro Aoki, and Masayuki Kanda. Security of e2 against truncated differential cryptanalysis. In *International Workshop on Selected Areas in Cryptography*, pages 106–117. Springer, 1999.

[15] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *International Conference on Information Security and Cryptology*, pages 57–76. Springer, 2011.

[16] Zeynab Namdari, Elnaz Bagherzadeh, and Zahra Ahmadian. Linear and differential-linear distinguishers for lea and hight block cipehrs. *in progress*, 2019.

[17] Shahram Rasoolzadeh, Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. An improved truncated differential cryptanalysis of klein. *Tatra Mountains Mathematical Publications*, 67(1):135–147, 2016.

[18] Yu Sasaki and Yosuke Todo. New impossible differential search tool from design and cryptanalysis aspects. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 185–215. Springer, 2017.

[19] William Stein et al. Sage: Open source mathematical software. *7 December 2009*, 2008.

[20] Siwei Sun, Lei Hu, Meiqin Wang, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Danping Shi, Ling Song, and Kai Fu. Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. *Cryptology ePrint Archive, Report*, 747:2014, 2014.

[21] Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. 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*, pages 158–178. Springer, 2014.

[22] Shengbao Wu and Mingsheng Wang. Security evaluation against differential cryptanalysis for block cipher structures. *IACR Cryptology ePrint Archive*, 2011:551, 2011.

[23] Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. 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*, pages 648–678. Springer, 2016.

[24] Dong Yang, Wen-Feng Qi, and Hua-Jin Chen. Observations on the truncated differential of sp block ciphers and their applications to mcrypton and crypton v1. 0. *IET Information Security*, 12(5):419–424, 2018.

Appendix A

Tabs. 5, 6 and 7 illustrate The branching property tables of Midori64, SKINNY64/128 and CRAFT MixColumns.

Table 5: Branching property table of Midori64 MixColumn

in/out	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0x2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
0x3	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	1
0x4	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0x5	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	1
0x6	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	1
0x7	0	0	0	0	0	0	0	4	8	0	0	4	0	4	4	1
0x8	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0x9	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	1
0xa	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	1
0xb	0	0	0	0	8	0	0	4	0	0	0	4	0	4	4	1
0xc	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	1
0xd	0	0	8	0	0	0	0	4	0	0	0	4	0	4	4	1
0xe	0	8	0	0	0	0	0	4	0	0	0	4	0	4	4	1
0xf	0	0	0	8	0	8	8	4	0	8	8	4	8	4	4	1

Table 6: Branching property table of SKINNY64/X MixColumn

in/out	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0x2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0x3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0x4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x5	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	1
0x6	0	0	0	0	0	0	0	0	0	4	0	1	0	0	0	0
0x7	0	0	8	0	0	0	4	0	0	0	0	4	0	0	0	1
0x8	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x9	0	0	0	0	0	0	0	0	0	0	4	1	0	0	0	0
0xa	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0xb	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	1
0xc	0	0	0	0	0	0	0	0	0	0	0	0	4	1	0	0
0xd	0	0	0	0	0	0	0	4	0	0	0	0	0	0	4	1
0xe	0	0	0	0	0	0	0	0	8	4	0	0	4	1	0	0
0xf	0	0	0	0	0	8	0	4	0	0	0	0	8	4	4	1

Table 7: Branching property table of CRAFT MixColumn

in/out	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
0x2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0x3	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	1
0x4	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0x5	0	0	0	0	0	0	0	0	0	4	0	0	0	1	0	0
0x6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0x7	0	0	0	8	0	0	0	4	0	0	0	4	0	0	0	1
0x8	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0x9	0	0	0	0	0	4	0	0	0	0	0	0	0	1	0	0
0xa	0	0	4	0	0	0	0	0	0	0	1	0	0	0	0	0
0xb	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	1
0xc	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0xd	0	8	0	0	0	4	0	0	0	4	0	0	0	1	0	0
0xe	0	0	0	0	0	0	4	0	0	0	0	0	0	0	1	0
0xf	0	0	0	8	0	0	0	8	0	0	0	4	0	0	0	1

Appendix B

The linear dependencies between active nibbles of Δ_{out} for the proposed 4,5,6-round truncated differential characteristics for Midori64 are as follows.

4-round

$$\begin{array}{ccc}
\Delta^S_{out} & & \Delta_{out} \\
\begin{pmatrix} a & e & i & 0 \\ b & f & 0 & 0 \\ c & g & j & k \\ d & h & 0 & l \end{pmatrix} & \xrightarrow{2^{-4}} & \begin{pmatrix} j \oplus f \oplus l & e \oplus b & 0 & c \oplus i \\ a \oplus f \oplus l & k \oplus b & d & c \oplus h \oplus i \\ a \oplus j \oplus l & k \oplus e \oplus b & 0 & h \oplus i \\ a \oplus j \oplus f & k \oplus e & d & h \oplus c \end{pmatrix}
\end{array}$$

5-round

$$\begin{array}{ccc}
\Delta^S_{out} & & \Delta_{out} \\
\begin{pmatrix} a & 0 & d & f \\ 0 & c & 0 & g \\ 0 & 0 & e & h \\ b & 0 & 0 & i \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} e \oplus c \oplus i & 0 & b \oplus f & d \oplus g \\ a \oplus c \oplus i & h & f & d \\ a \oplus e \oplus i & h & b & d \oplus g \\ a \oplus e \oplus c & h & b \oplus f & g \end{pmatrix}
\end{array}$$

6-round

$$\begin{array}{ccc}
\Delta^S_{out} & & \Delta_{out} \\
\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} 0 & 0 & 0 & b \\ 0 & 0 & a & 0 \\ 0 & 0 & a & b \\ 0 & 0 & a & b \end{pmatrix}
\end{array}$$

Appendix C

The linear dependencies between active nibbles of Δ_{out} for the proposed 8,9,10-round truncated differential characteristics for SKINNY64/X are as follows.

8-round

$$\begin{array}{ccc} \Delta_{out}^{S} & & \Delta_{out} \\ \begin{pmatrix} a & e & 0 & k \\ b & f & i & 0 \\ c & g & j & l \\ d & h & 0 & m \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} a \oplus j \oplus k & e \oplus l & c \oplus m & d \oplus k \oplus g \\ a & e & 0 & k \\ j & b \oplus l & c \oplus f & g \oplus i \\ a \oplus j & e \oplus l & c & k \oplus g \end{pmatrix} \end{array}$$

9-round

$$\begin{array}{ccc} \Delta_{out}^{S} & & \Delta_{out} \\ \begin{pmatrix} a & e & 0 & h \\ b & 0 & f & 0 \\ c & 0 & g & i \\ d & 0 & 0 & j \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} a \oplus g & e \oplus i & c \oplus j & d \oplus h \\ a & e & 0 & h \\ g & b \oplus i & c & f \\ a \oplus g & e \oplus i & c & h \end{pmatrix} \end{array}$$

10-round

$$\begin{array}{ccc} \Delta_{out}^{S} & & \Delta_{out} \\ \begin{pmatrix} a & b & 0 & 0 \\ 0 & 0 & 0 & d \\ 0 & c & 0 & e \\ 0 & 0 & 0 & 0 \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} a & e \oplus b & 0 & c \\ a & b & 0 & 0 \\ d & e & 0 & c \\ a & e \oplus b & 0 & c \end{pmatrix} \end{array}$$

Appendix D

The linear dependencies between active nibbles of Δ_{in} for the proposed 10,11,12-round truncated differential characteristics for CRAFT are as follows.

10-round

$$\begin{array}{ccc} \Delta_{in} & & \Delta_{1} \\ \begin{pmatrix} b & 0 & 0 & c \\ 0 & 0 & a & 0 \\ b & 0 & 0 & c \\ 0 & 0 & 0 & 0 \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & b & c \\ a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

11-round

$$\begin{array}{ccc} \Delta_{in} & & \Delta_{1} \\ \begin{pmatrix} 0 & b & a & 0 \\ 0 & 0 & 0 & c \\ 0 & b & a & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ a & b & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

12-round

$$\begin{array}{ccc} \Delta_{in} & & \Delta_{1} \\ \begin{pmatrix} a \oplus b & 0 & 0 & c \\ a & 0 & 0 & 0 \\ b & 0 & 0 & c \\ a & 0 & 0 & 0 \end{pmatrix} & \xrightarrow{1} & \begin{pmatrix} 0 & a & 0 & 0 \\ 0 & 0 & b & c \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$