Speeding up MILP Aided Differential Characteristic Search with Matsui's Strategy

Yingjie Zhang[1,2,3], Siwei Sun[1,2,3(✉)], Jiahao Cai[1,2,3], and Lei Hu[1,2,3]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{zhangyingjie,sunsiwei,caijiahao,hulei}@iie.ac.cn
[2] Data Assurance and Communication Security Research Center,
Chinese Academy of Sciences, Beijing, China
[3] School of Cyber Security,
University of Chinese Academy of Sciences, Beijing, China

Abstract. Being the first generic algorithm for finding the best differential and linear characteristics, Matsui's branch and bound search algorithm (EUROCRYPT 1994) and its variants have played an important role in the security analysis of symmetric-key primitives. However, Matsui's algorithm is difficult to implement, optimize, and be applied to different ciphers with reusable code. Another approach getting popular in recent years is to encode the search problem as a Mixed Integer Linear Programming (MILP) model which can be solved by open-source or commercially available optimizers. In this work, we show how to tweak the objective functions of the MILP models for finding differential characteristics such that a set of constraints derived from the bounding condition of Matsui's algorithm can be incorporated into the models. We apply the new modeling strategy to PRESENT (S-box based SPN design), SIMON (Feistel structure), and SPECK (ARX construction). For PRESENT, the resolution time is significantly reduced. For example, the time to prove that the exact lower bound of the probabilities of the differential characteristics for 7-round PRESENT is reduced from 48638 s to 656 s. For SIMON, obvious acceleration is also observed, and for the ARX cipher SPECK, the new model is unable to speed up the resolution. In the future, it is interesting to investigate how to integrate other search heuristics proposed in the literature of symmetric-key cryptanalysis into the MILP models, and how to accelerate the resolution of MILP models for finding characteristics of ARX ciphers.

Keywords: Differential characteristic · Linear characteristic
Branch and bound · Matsui's algorithm · MILP

1 Introduction

Differential and linear attacks are two of the most fundamental methods for analyzing symmetric-key primitives, which many advanced cryptanalytic techniques

L. Chen et al. (Eds.): ISC 2018, LNCS 11060, pp. 101–115, 2018.
https://doi.org/10.1007/978-3-319-99136-8_6

are derived from or partly rely on. Performing differential and linear analysis is a tedious routine work for the designers and cryptanalysts of symmetric-key algorithms. Matsui's branch and bound search algorithm [21] is a classical approach for finding the best differential and linear characteristics, and it is extremely efficient for some specific ciphers. But, implementing Matsui's algorithm properly demands for sophisticated programming skills when cipher-specific optimizations are taken into account [5,6,12]. Moreover, there seems to be no obvious way to create highly reusable code for Matsui's algorithm targeting different ciphers.

However, the diversity of cryptographic algorithms is an unstoppable trend. In the case of block ciphers, to have a single algorithm work as a security solution for all scenarios is doomed to fail due to the ever-increasing complexity and diversity of today's communication systems. Over recent years, we have witnessed many new block ciphers designed for lightweight devices or dedicated use cases. These include, to just name a few of them, the ISO standard PRESENT [11], SIMON and SPECK [7] designed by the NSA, the SKINNY family presented in CRYPTO 2016 [8], and Rasta with minimizing AND-related metrics as its main design objective [15]. We refer the reader to [9] for a more comprehensive survey. To meet the requirements of the target applications, these newly designed block ciphers typically use lightweight components with relatively weak local cryptographic properties, consume less resources when implemented and executed, and reserve limited security margins aggressively. This approach makes the design and evaluation more difficult, where the security bounds cannot be derived theoretically.

In such situation, the security evaluation against differential and linear attacks have to be performed with the help of search tools. Matsui's algorithm is obviously not a satisfactory choice not only because of its inconvenience but also that it is unable to get useful results in some cases. Another option getting more and more popular in recent years is the Mixed Integer Linear Programming (MILP) based method, where the problem of searching for characteristics is transformed into an MILP model that can be solved with generic MILP solvers.

Similar to SAT/SMT and CP based methods [4,19,22,26], in the MILP based approach [23,28,29], the cryptanalysts only need to specify the problem in standard modeling languages without mixing in the actual search algorithms. This *decoupling of formulation and resolution* is the key that makes the MILP based approach more attractive than Matsui's algorithm. Unlike Matsui's algorithm, searching heuristics and optimizations can be issued *externally* without touching the sophisticated code powering the search. In addition, cryptanalysts benefit directly from the advancement of MILP resolution techniques. So far, the MILP based approach covers many cryptanalytic techniques, including differential/linear [18,28], impossible differential [25], zero-correlation linear [14], and integral cryptanalysis [30].

Despite all these advantages, there are situations where Matsui's algorithm performs far more better than the MILP based approach (*e.g.*, search for the best characteristics of DES and PRESENT in the single-key model). Moreover, both MILP and Matsui's algorithm rarely work for non-lightweight designs under

today's computational power. Therefore, it is of great importance to improve the efficiency of the MILP based approach, and a natural question to ask is whether it is possible to strengthen the MILP based search with Matsui's algorithm. In this work, we make a first step towards this direction. Finally, before we present our work, we emphasis that all of our analysis are based on the *Markov assumption* [20], where we assume that each round of an iterative cipher is independent.

Motivation and Contribution. One obvious difference between Matsui's algorithm and the MILP based approach is worth to highlight. When we search for the best characteristic of an R-round iterative block cipher, Matsui's algorithm requires the probabilities of the optimal characteristics of the same cipher reduced to r rounds for $1 \leq r < R$. That is, to get the result of R rounds, we must first run Matsui's algorithm for rounds 1, 2, $\cdots$, and $R-1$. These probabilities are employed to prune the search tree according to certain bounding conditions. In contrast, in the MILP based approach, we always set up an R-round model directly, and do not exploit the solutions for lower rounds explicitly. This fact motivates us to enhance the R-round MILP models by taking into account some information of the solutions of lower rounds. We achieve this by adapting the objective function of an R-round model such that constraints encoding Matsui's bounding conditions can be incorporated into the model. In practice, this new modeling strategy leaves many choices for the cryptanalysts, since one can choose to include only a subset of the constraints generated from Matsui's bounding conditions. We perform experiments on PRESENT, SIMON, and SPECK, which shows that the inclusion of the constraints derived from Matsui's algorithm leads to significantly improved resolution performance for PRESENT. For SIMON, obvious improvement is also observed, and for the ARX cipher SPECK, the new model is unable to accelerate the resolution performance. Our work suggests that trying to combine the power of dedicated search algorithms implemented in general purpose programming language and MILP is a valuable endeavor. In the future, it is interesting to see how to integrate other search heuristics [16,17] to speed up the resolution of the MILP models for finding characteristics of ARX ciphers.

Organization. In Sects. 2 and 3, we give a brief introduction of Matsui's algorithm and the MILP based differential and linear analysis. A method for enhancing the MILP models with constraints generated from Matsui's bounding condition is presented in Sect. 4. We then show applications of the enhanced MILP models in Sect. 5. Section 6 concludes the paper and suggests future work.

2 Matsui's Algorithm

At Eurocypt 1994, Matsui presented a branch and bound search algorithm that can be used to identify the maximum probability characteristic of a target block cipher [21]. Matsui's algorithm, together with its variations, has been an important tool in the practice of security evaluation of symmetric-key primitives. It is improved in subsequent work [3,6,13,24] and adapted to ARX constructions in [10,31].

A general description of Matsui's algorithm for an iterative block cipher depicted in Fig. 1 is given in Algorithm 1. Our presentation largely follows the work of Bannier *et al.* [5]. Also note that Algorithm 1 is an over simplification of Matsui's algorithm, which does not exhibit the necessary details (*e.g.*, the technique for controlling the number of initial branches, the order in which candidates are enumerated) in actual implementations.

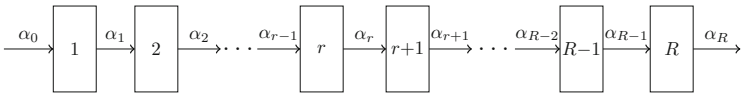

Fig. 1. An R-round iterative cipher, where $\mathcal{T} = (\alpha_0, \cdots, \alpha_R)$ is an R-round differential characteristic with probability $\mathbb{P}(\mathcal{T})$, and the probability of the differential $\alpha_{r-1} \to \alpha_r$ is denoted by $P_{Rd(r)}$.

With the knowledge of the best probabilities $P_{Best}(i)$ of i-round characteristics for $i \in \{1, \cdots, R-1\}$, Matsui's algorithm explores the search space of all possible characteristics in a depth-first approach, and output the optimal R-round characteristic. The search space conceptually forms a tree structure, and at the rth level of the tree, $\mathcal{T}_{[1,r]} = (\alpha_0, \cdots, \alpha_r)$ is assigned to actual values by Matsui's algorithm, and all possible values of $(\alpha_{r+1}, \cdots, \alpha_{R+1})$ form a subtree to be explored. We call $\mathcal{T}_{[1,r]}$ with $r < R$ instantiated with actual values a *partial solution* (corresponding to intermediate node of the search tree), and $\mathcal{T} = \mathcal{T}_{[1,R]}$ instantiated with actual values a *full solution* (corresponding to a leaf node of the search tree). Thus, when Matsui's algorithm goes one level deeper into the search tree, it extends the current partial solution towards a full solution.

The efficiency of Matsui's algorithm comes from the fact that it will not try to extend every partial solution. Before trying to extend the current partial solution, the so-called bounding condition specified in line `24` of Algorithm 1 is tested, which essentially states that if this condition is violated, a better characteristic will never be found by extending the current partial solution, and therefore we should give up the current branch, backtrack to the upper level of the search tree, and try another branch.

The variable P_{Estim} in Matsui's algorithm keeps track of the best characteristic known so far. Only when a strictly better characteristic is encounter during the search, it will be updated (see line `42` of Algorithm 1).

Moreover, in Matsui's algorithm, The first and last rounds receive special treatment (see functions `FirstRound()` and `LastRound()` in Algorithm 1), where the input and output difference is determined directly by the output differences of the round 1 and round $R-1$, without the effort of searching through a set of candidates.

Algorithm 1. Matsui's Algorithm

Input: $R \in \mathbb{Z}^*$, $R \geq 2$; $q > 0$; $P_{Best}(1)$, $P_{Best}(2)$, ..., $P_{Best}(R-1)$
Output: differential characteristic $\mathcal{T} = (\alpha_0, \alpha_1, \ldots, \alpha_{R-1}) \in \mathbb{F}_2^n$ where probability $\mathbb{P}(\mathcal{T}) = P_{Estim}$

Algorithm `OptimalTrail`$(R, q, P_{Best}(1), \ldots, P_{Best}(R-1))$ `// Entry Point`
  for *each non-zero* α_1 **do**
    $\mathcal{T} = ()$, $P_{Estim} \leftarrow q$
    Call `FirstRound()`
  end
  if $\mathcal{T} \neq ()$ **then**
    return $\mathcal{T}$, $P_{Estim} = \mathbb{P}(\mathcal{T})$
  end
end

Function `FirstRound()` `// Subroutine`
  $P_{Rd(1)} \leftarrow \max_\alpha \mathbb{P}(\alpha \rightarrow \alpha_1)$
  $\alpha_0 \leftarrow \alpha,\ s.t\ \mathbb{P}(\alpha \rightarrow \alpha_1) = P_{Rd(1)}$
  if $R > 2$ **then**
    Call `Round(2)`
  else
    Call `LastRound()`
  end
end

Function `Round(r)`$(2 \leq r \leq R-1)$ `// Subroutine`
  for *each candidate* α *for* α_{r-1} **do**
    $P_{Rd(r)} \leftarrow \mathbb{P}(\alpha_{r-1} \rightarrow \alpha)$
    if $\prod_{i=1}^{r} P_{Rd(i)} \cdot P_{Best}(R-r) \geq P_{Estim}$ **then**
      `// Matsui's bounding condition`
      $\alpha_r \leftarrow \alpha$
      if $r + 1 < R$ **then**
        Call `Round(r+1)`
      else
        Call `LastRound()`
      end
    end
  end
end

Function `LastRound()` `// Subroutine`
  for *each candidate* α *for* α_{r-1} **do**
    $P_{Rd(R)} \leftarrow \max_\alpha \mathbb{P}(\alpha_{R-1} \rightarrow \alpha)$
    $\alpha_R \leftarrow \alpha,\ s.t\ \mathbb{P}(\alpha_{R-1} \rightarrow \alpha) = P_{Rd(R)}$
  end
  if $\prod_{i=1}^{R} P_{Rd(i)} > P_{Estim}$ **then** `// A strictly better trail is found`
    $\mathcal{T} \leftarrow (\alpha_0, \alpha_1, \ldots, \alpha_{R-1})$
    $P_{Estim} \leftarrow \prod_{i=1}^{R} P_{Rd(i)}$
  end
end

3 MILP Aided Characteristic Search

At first, MILP was used to determine the minimum number of differentially or linearly active S-boxes of word-oriented ciphers [23,29]. In [28], Sun *et al.* introduced the convex hull computation method which can encode any subset of 0–1 vectors as the solution set of a system of linear inequalities. Thanks to this technique, actual differential and linear characteristics can be found with MILP based method. Subsequently, the MILP aided approach is applied in impossible differential analysis [25], zero-correlation linear analysis [14], and Integral cryptanalysis [30]. It is also extended and adapted to analyze ARX based constructions [18]. In what follows, we give a brief introduction of the MILP modeling technique for finding differential characteristics, which is employed in the following sections.

The key to transfer the problem of searching for differential characteristics into an MILP model is to express the propagation rules of the characteristics as a set of linear inequalities, and encode the overall probability as a linear function.

Objective Function. Since the goal is to find the optimal characteristic, we set the objective function to minimize the probability of the underlying differential characteristic. However, we must be able to express the probability as a linear function at the first place to make it valid in MILP. Such representations are available for SIMON, SPECK, and PRESENT [18,28]. For the sake of simplicity and without loss of generality, we assume the probability (or its equivalence) can be represented by

$$\sum_{i=1}^{R}\sum_{j=1}^{k} A_{i,j},$$

and we call $A_{i,j}$'s are probability weight variables, where $A_{i,j}$ for $j \in \{1, \cdots, k\}$ is the probability weight variables of round i of an iterative cipher. Under this notation, the probability weight contributed by round i is $\sum_{j=1}^{k} A_{i,j}$.

Modeling XOR. Let $a \oplus b = c$, where $a, b, c \in \mathbb{F}_2$ are the bit-level input and output differences of the XOR operation. Then (a, b, c) is a valid differential characteristic of XOR if and only if $a+b+c-2d_{\oplus} = 0$, where a, b, and $c \in \{0, 1\}$, and $d_{\oplus}$ is a 0–1 dummy variable.

Modeling S-box. The exact differential property of an $\omega \times \nu$ S-box S can be modeled by a set of linear inequalities with the convex hull computation method [28]. Let $\mathcal{D} = \{(\mathbf{a}, \mathbf{b}) \in \{0,1\}^{\omega+\nu} : P(\mathbf{a} \rightarrow \mathbf{b}) > 0\}$ be the set of all possible input-output differential patterns of S, where $\mathbf{a} = (a_0, a_1, \ldots, a_{\omega-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{\nu-1})$. Then, we can compute the H-representation of $\mathcal{D} \subseteq \mathbb{R}^{\omega+\nu}$. With the help of the greedy algorithm proposed in [28], we can extract a system of inequalities whose 0–1 solution set is exactly $\mathcal{D}$. Sometimes, it is possible to encode the differential probabilities of $\mathbf{a} \rightarrow \mathbf{b}$ into $\mathcal{D}$, and we refer the reader to [18,27,28] for concrete examples.

Modeling Modular Addition [18]. Suppose $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$ and $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ are the input and output bit-level

XOR-difference of addition module 2^n. The constraints are as follows, where $d_{\oplus}$ is 0–1 dummy variable, $s_i (i = 1, \ldots, n-2)$ are 0–1 active markers and $\sum_{i=1}^{n-2} s_i$ is negative logarithm of the probability $P[(\mathbf{a}, \mathbf{b}) \rightarrow \mathbf{c}]$.

$$
\begin{cases}
a_{n-1} + b_{n-1} + c_{n-1} \leq 2 \\
a_{n-1} + b_{n-1} + c_{n-1} - 2d_{\oplus} \geq 0 \\
d_{\oplus} - a_{n-1} \geq 0 \\
d_{\oplus} - b_{n-1} \geq 0 \\
d_{\oplus} - c_{n-1} \geq 0 \\
-a_i + b_i + s_i \geq 0 \\
-b_i + c_i + s_i \geq 0 \\
a_i - c_i + s_i \geq 0 \\
a_i + b_i + c_i - s_i \geq 0 \\
-a_i - b_i - c_i - s_i \geq -3 \\
c_i + a_{i-1} + b_{i-1} - c_{i-1} + s_i \geq 0 \\
-a_i - b_i - c_i + 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \geq 0 \\
a_i + b_i + c_i - 3a_{i-1} - 3b_{i-1} - 3c_{i-1} + 2s_i \geq -6 \\
-b_i + a_{i-1} - b_{i-1} - c_{i-1} + s_i \geq -2 \\
c_i + a_{i-1} - b_{i-1} + c_{i-1} + s_i \geq 0 \\
-a_i - b_i - c_i - 3a_{i-1} + 3b_{i-1} - 3c_{i-1} + 2s_i \geq -6 \\
-a_i - a_{i-1} - b_{i-1} + c_{i-1} + s_i \geq -2 \\
a_i + b_i + c_i - 3a_{i-1} + 3b_{i-1} + 3c_{i-1} + 2s_i \geq 0 \\
(i = 1, \ldots, n-2)
\end{cases}
\tag{1}
$$

4 Enhancing MILP Based Search with Matsui's Bounding Condition

Firstly, let us recall the bounding condition of Matsui's algorithm (see Algorithm 1):

$$
\prod_{i=1}^{r} P_{Rd(i)} \cdot P_{Best}(R - r) \geq P_{Estim}. \tag{2}
$$

When we run Matsui's algorithm against an R-round cipher, the variable P_{Estim} keeps track of the probability of the best characteristic known by the algorithm so far, and it will be updated dynamically if a strictly better characteristic is encountered during the search. Whenever the algorithm needs to go one level deeper into the search tree, condition (2) is tested. A violation of (2) implies that any extension of the partial solution leads to inferior characteristics with probability less than P_{Estim} (the probability of a known characteristic). Therefore, the entire subtree is pruned.

To integrate Matsui's bounding condition into the MILP models, we introduce a variable named *xobj* acting as the variable P_{Estim} in Matsui's algorithm, and let

$$\text{Minimize } xobj$$

be the objective function of the new model. Note that this is a very natural choice since the variable *xobj* always keeps track of the currently known best

solution during the resolution of the MILP model. To make the $xobj$ correspond to the probability of the identified characteristic, we put an equation

$$xobj = \sum_{i=1}^{R} \sum_{j=1}^{k} A_{i,j}$$

into the constraints section of the model. At this point, the new model is completely equivalent to the original model. What we do is essentially renaming the objective function of the original model.

Assuming we know the probabilities $P_{Best}(1), P_{Best}(2), \cdots, P_{Best}(R-1)$, we are now ready to express the bounding condition (2) as

$$\sum_{t=1}^{i} \sum_{j=1}^{k} A_{t,j} + wt(P_{Best}(R-i)) \leq xobj, \quad i = 1, \ldots, \ R-1 \tag{3}$$

$$\sum_{t=i+1}^{R} \sum_{j=1}^{k} A_{t,j} + wt(P_{Best}(i)) \leq xobj, \quad i = 1, \ldots, R-1 \tag{4}$$

Therefore, for an R-round model, we can generate $2R-2$ more constraints, where $wt(\cdot)$ make $P_{best}(i)$ compatible with the probability weight variables. The most different part of the new model is that it takes into account the solutions of the models of lower rounds. In the following, we present three different modeling strategies, which will be compared in the next section.

- $\mathcal{M}^{I}$: The original model without any modification.
- $\mathcal{M}^{II}$: The model with modified objective function, and $R-1$ additional constraints of (4) generated from Matsui's bounding condition for round 1 to round $R-1$ respectively.

$$\begin{cases} \min \ \ xobj \\ \sum\limits_{i,j} A_{i,j} - xobj = 0 \\ \sum\limits_{t=i+1}^{R} \sum\limits_{j=1}^{k} A_{t,j} + wt(P_{Best}(i)) \leq xobj, \quad i = 1, \ldots, R-1 \end{cases} \tag{5}$$

- $\mathcal{M}^{III}$: The model with modified objective function, and all $2R-2$ additional constraints.

$$\begin{cases} \min \ \ xobj \\ \sum\limits_{i,j} A_{i,j} - xobj = 0 \\ \sum\limits_{t=i+1}^{R} \sum\limits_{j=1}^{k} A_{t,j} + wt(P_{Best}(i)) \leq xobj, \quad i = 1, \ldots, R-1 \\ \sum\limits_{t=1}^{i} \sum\limits_{j=1}^{k} A_{t,j} + wt(P_{Best}(R-i)) \leq xobj, \quad i = 1, \ldots, R-1 \end{cases} \tag{6}$$

5 Applications

In this section, we apply the modeling strategy presented in Sect. 4 to PRESENT, SIMON, and SPECK. The reasons that these ciphers are selected as the experimental targets are twofold. Firstly, the probabilities (or their equivalences) of the differential characteristics of these ciphers can be expressed as linear functions. Secondly, they represent the most common structures for modern block ciphers, where PRESENT is a SPN network, SIMON is a Feistel cipher with pure bitwise operations, and SPECK is an ARX construction.

However, we admit that in our experiments only lightweight primitives are involved. This is because generally MILP based approach (and actually all currently available automatic search tools) is too inefficient to search for characteristics of non-lightweight ciphers directly, and it is sometimes difficult to modeling the components of non-lightweight ciphers at the first place. For example, only recently, Abdelkhalek *et al.* show how to model the differential property of an 8×8 S-box with MILP [2], and even that, the search procedure has to be divided into two steps for a cipher involving 8×8 S-boxes, where only truncated differentials are identified in the first step.

In addition, since the focus of this paper is to improve the MILP based method, we will not give a comparison between Matsui's algorithm and the MILP based approach. Nevertheless, we would like to mention that Matsui's algorithm is much more better than MILP in the case of PRESENT, while for SIMON and SPECK, it is inferior to MILP. Finally, all of the models presented in this paper are solved by the MILP optimizer Gurobi (version 7.0.2) [1] running at 16 threads on a server with Intel® Xeon® E5-2637V3 CPU 3.50 GHz.

5.1 Application to PRESENT

The PRESENT, designed by Bogdanov *et al.*, is an ISO standardized lightweight block cipher [11]. The round function of PRESENT is shown in Fig. 2, and we refer the reader to [11] for more information.

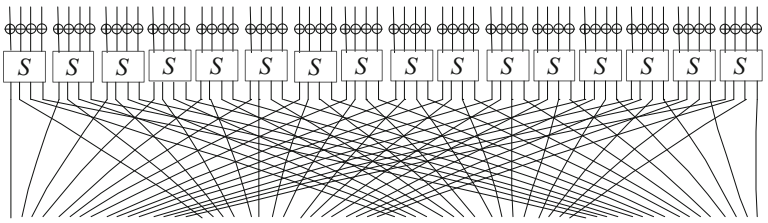

Fig. 2. The round function of PRESENT

We construct three models $\mathcal{M}^I$, $\mathcal{M}^{II}$, and $\mathcal{M}^{III}$ according to the strategies presented in Sect. 4. The resolution time for these models are recorded in Table 1.

Note that what we measure is the time cost for the solver to prove that the solution it identified is *optimal*. This timing information is of most importance since in the design process what we care is the *bound*, and the tighter the bound is, the more accurate the security evaluation.

Table 1. Experimental results of PRESENT

R	p	$\mathcal{M}^I$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
1	2^{-2}	0.01s	0.09s	0.13s
2	2^{-4}	0.95s	0.95s	0.06s
3	2^{-8}	3.70s	2.82s	2.43s
4	2^{-12}	15.78s	10.08s	8.82s
5	2^{-20}	629.83s	114.13s	448.61s
6	2^{-24}	1740.55s	200.03s	74.56s
7	2^{-28}	48638.29s	714.03s	655.36s
8	2^{-32}	>10h	2124.51s	1074.45s

From Table 1 we can see that the resolution time can be significantly improved by using the new modeling strategies. For instance, we can prove that the probability of the optimal characteristic of 8-round PRESENT is 2^{-32} in 1074.45 s by using $\mathcal{M}^{III}$, while for $\mathcal{M}^I$ we can not get this result in less 10 h. Moreover, by using the new models, some interesting phenomenons are observed that we cannot explain. For example, the resolution time of $\mathcal{M}^{III}$ for 6-round PRESENT is faster than that of the 5-round model.

5.2 Application to SIMON

SIMON (depicted in Fig. 3) is a family of lightweight block ciphers with Feistel structure involving only bitwise operations: XOR, AND, and Rotation, which is designed by the National Security Agency of USA. The parameters of different SIMON instances involved in our experiments are summarized in Table 2.

Table 2. Parameters for SIMON32 and SIMON48

Variant $2n/mn$	Block Size $2n$	Key Size mn	Round r
32/64	32	64	32
48/72	48	72	36
48/96	48	96	36

We construct three models $\mathcal{M}^I$, $\mathcal{M}^{II}$, and $\mathcal{M}^{III}$ according to the strategies presented in Sect. 4. The resolution time for these models are recorded in Table 3.

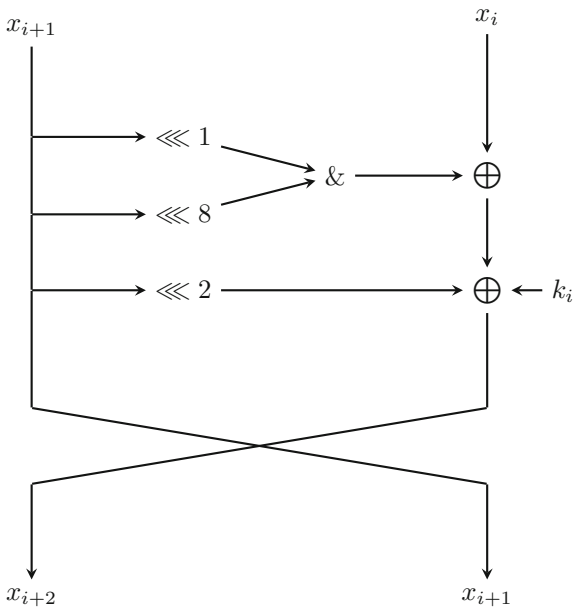

Fig. 3. The round function of SIMON

Table 3. Experimental results of SIMON

Block size $2n$	R	p	$\mathcal{M}^I$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
32	11	2^{-30}	75.05s	79.22s	67.92s
	12	2^{-34}	657.37s	559.83s	209.09s
48	13	2^{-38}	309.58s	376.33s	109.85s
	14	2^{-44}	4627.26s	3577.05s	2942.85s
	15	2^{-46}	31979.80s	3351.41s	2444.28s
	16	2^{-50}	>20h	>15h	26589.96s

From Table 3 we can see that, for larger number of rounds, the improvement is obvious. For example, using $\mathcal{M}^{III}$ we can prove that the probability of the optimal characteristic of 15-round SIMON48 is 2^{-46} in 2444.28 s, while for $\mathcal{M}^I$, the resolution time is 31979.80 s.

5.3 Application to SPECK

The SPECK is a family of ARX Feistel block ciphers (depicted in Fig. 4) designed by the National Security Agency of USA. The parameters of different SPECK instances involved in our experiments are summarized in Table 4.

We construct three models $\mathcal{M}^I$, $\mathcal{M}^{II}$, and $\mathcal{M}^{III}$ according to the strategies presented in Sect. 4. The resolution time for these models are recorded in

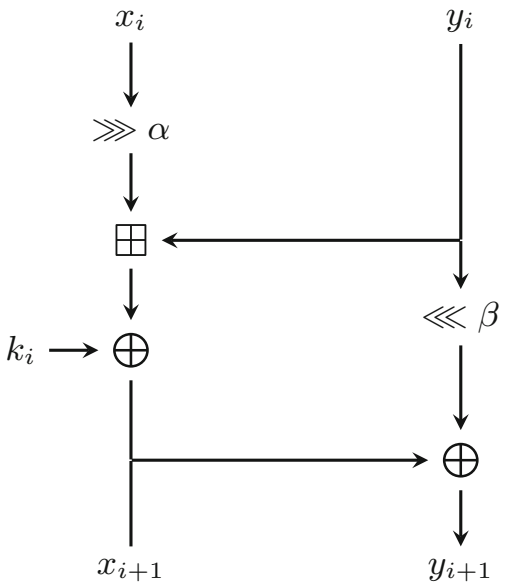

Fig. 4. The round function of SPECK

Table 4. Parameters for SPECK32 and SPECK48

Variant $2n/mn$	Block Size $2n$	Key Size mn	Round r	α	β
32/64	32	64	22	7	2
48/72	48	72	22	8	3
48/96	48	96	23	8	3

Table 5. Experimental results of SPECK

Block size $2n$	R	p	$\mathcal{M}^I$	$\mathcal{M}^{II}$	$\mathcal{M}^{III}$
32	5	2^{-9}	9.78s	17.15s	26.08s
	6	2^{-13}	173.67s	820.82s	390.33s
	7	2^{-18}	7175.87s	>10000s	>10000s
48	5	2^{-10}	32.90s	358.11s	273.98s
	6	2^{-14}	1482.66s	2626.50s	2287.21s
	7	2^{-19}	40860.38s	>100000s	>100000s

Table 5. However, the results show that the new modeling strategies are inferior to the original method. This may somehow implies that adding Matsui's bounding conditions for MILP models of ARX ciphers is not a good choice.

6 Conclusion

Borrowing the ideas from Matsui's algorithm, we tweak the MILP models for differential cryptanalysis by altering the objective functions and introducing in special constraints derived from Matsui's bounding condition. We apply this new modeling strategy to PRESENT, SPECK, and SIMON, which demonstrates that the fusion of Matsui's bounding condition and the MILP approach leads to faster resolution in some cases. Therefore, the new modeling approach is expected to reduce the time cost of differential and linear analysis. In particular, during the design process of symmetric-key schemes, a larger design space may be explored within limited time. Our work shows that it is beneficial to include Matsui's bounding condition in the MILP models for differential analysis. More generally, it is interesting to see how to integrate other search heuristics [16,17] from the literature of symmetric-key cryptanalysis into the MILP models.

Acknowledgments. The authors thank the anonymous reviewers for many helpful comments. The work is supported by the National Natural Science Foundation of China (61732021, 61772519), the Youth Innovation Promotion Association of Chinese Academy of Sciences, the Chinese Major Program of National Cryptography Development Foundation, and the Institute of Information Engineering, CAS (Grant No. Y7Z0341103).

References

1. Gurobi Optimization. Gurobi Optimizer Reference Manual (2013)
2. Abdelkhalek, A., Sasaki, Y., Tolba, M., Youssef, A.M.: MILP modeling for (large) S-boxes to optimize probability of differential characteristics. IACR Trans. Symmetric Cryptol. **2017**(4), 99–129 (2017)
3. Aoki, K., Kobayashi, K., Moriai, S.: Best differential characteristic search of FEAL. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 41–53. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052333
4. Aumasson, J.-P., Jovanovic, P., Neves, S.: Analysis of NORX: investigating differential and rotational properties. In: Aranha, D.F., Menezes, A. (eds.) LATINCRYPT 2014. LNCS, vol. 8895, pp. 306–324. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16295-9_17
5. Bannier, A., Nicolas, B., Eric, F.: Automatic search for a maximum probability differential characteristic in a substitution-permutation network. In: 48th Hawaii International Conference on System Sciences, HICSS 2015, Kauai, Hawaii, USA, January 5–8, 2015, pp. 5165–5174 (2015)
6. Bao, Z., Zhang, W., Lin, D.: Speeding up the search algorithm for the best differential and best linear trails. In: Lin, D., Yung, M., Zhou, J. (eds.) Inscrypt 2014. LNCS, vol. 8957, pp. 259–285. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16745-9_15
7. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. IACR Cryptol. ePrint Arch. **2013**, 404 (2013)

8. Beierle, C., et al.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5
9. Biryukov, A., Perrin, L.: State of the art in lightweight symmetric cryptography. IACR Cryptol. ePrint Arch. **2017**, 511 (2017)
10. Biryukov, A., Velichkov, V., Le Corre, Y.: Automatic search for the best trails in ARX: application to block cipher Speck. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 289–310. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_15
11. Bogdanov, A., et al.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
12. Chen, J., Teh, J., Liu, Z., Chunhua, S., Samsudin, A., Xiang, Y.: Towards accurate statistical analysis of security margins: new searching strategies for differential attacks. IEEE Trans. Comput. **66**(10), 1763–1777 (2017)
13. Collard, B., Standaert, F.-X., Quisquater, J.-J.: Improved and multiple linear cryptanalysis of reduced round serpent. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 51–65. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79499-8_6
14. Cui, T., Jia, K., Kai, F., Chen, S., Wang, M.: New automatic search tool for impossible differentials and zero-correlation linear approximations. IACR Cryptol. ePrint Arch. **2016**, 689 (2016)
15. Dobraunig, C., et al.: Rasta: a cipher with low ANDdepth and few ANDs per bit. IACR Cryptol. ePrint Arch. **2018**, 181 (2018)
16. Dobraunig, C., Eichlseder, M., Mendel, F.: Heuristic tool for linear cryptanalysis with applications to CAESAR candidates. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 490–509. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_20
17. Eichlseder, M., Mendel, F., Schläffer, M.: Branching heuristics in differential collision search with applications to SHA-512. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 473–488. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_24
18. Fu, K., Wang, M., Guo, Y., Sun, S., Hu, L.: MILP-Based automatic search algorithms for differential and linear trails for speck. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 268–288. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_14
19. Gerault, D., Minier, M., Solnon, C.: Constraint programming models for chosen key differential cryptanalysis. In: Proceedings of Principles and Practice of Constraint Programming - 22nd International Conference, CP 2016, Toulouse, France, September 5–9, 2016, pp. 584–601 (2016)
20. Lai, X., Massey, J.L., Murphy, S.: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_2
21. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053451
22. Mouha, N., Preneel, B.: A proof that the ARX cipher Salsa20 is secure against differential cryptanalysis. IACR Cryptol. ePrint Arch. **2013**, 328 (2013)

23. Mouha, N., Wang, Q., Gu, D., Preneel, B.: Differential and linear cryptanalysis using mixed-integer linear programming. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 57–76. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34704-7_5
24. Ohta, K., Moriai, S., Aoki, K.: Improving the search algorithm for the best linear expression. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 157–170. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-44750-4_13
25. Sasaki, Y., Todo, Y.: New impossible differential search tool from design and cryptanalysis aspects. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10212, pp. 185–215. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56617-7_7
26. Sun, S., et al.: Analysis of AES, SKINNY, and others with constraint programming. IACR Trans. Symmetric Cryptol. **2017**(1), 281–306 (2017)
27. Sun, S., et al.: Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. Cryptology ePrint Archive, Report 2014/747 (2014). http://eprint.iacr.org/2014/747
28. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_9
29. Shengbao, W., Wang, M.: Security evaluation against differential cryptanalysis for block cipher structures. IACR Cryptol. ePrint Arch. **2011**, 551 (2011)
30. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 648–678. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_24
31. Yao, Y., Zhang, B., Wu, W.: Automatic search for linear trails of the SPECK family. In: Lopez, J., Mitchell, C.J. (eds.) ISC 2015. LNCS, vol. 9290, pp. 158–176. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23318-5_9