IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

New method to describe the differential distribution table for large S-boxes in MILP and its application

ISSN 1751-8709
Received on 9th June 2018
Revised 5th December 2018
Accepted on 23rd January 2019
E-First on 17th April 2019
doi: 10.1049/iet-ifs.2018.5284
www.ietdl.org

Ling-Chen Li[1,2] ✉, *Wen-Ling Wu*[1], *Lei Zhang*[1], *Ya-Fei Zheng*[1]

[1]*Institute of Software, Chinese Academy of Sciences, South Four Street No.4, Zhong Guan Cun, Haidian District, Beijing 100190, People's Republic of China*

[2]*University of Chinese Academy of Sciences, East Road No. 80, Zhong Guan Cun, Haidian District, Beijing 100049, People's Republic of China*

✉ *E-mail: lilingchen@tca.iscas.ac.cn*

Abstract: Based on the method of the H-representation of the convex hull, the linear inequalities of all possible differential patterns of 4-bit S-boxes in the mix integer linear programming (MILP) model can be generated easily by the SAGE software. Whereas this method cannot be apply to 8-bit S-boxes. In this study, the authors propose a new method to obtain the inequalities for large S-boxes with the coefficients belonging to integer. The relationship between the coefficients of the inequalities and the corresponding excluded impossible differential patterns is obtained. As a result, the number of inequalities can be lower than 4000 for the AES S-box. Then, the new method for finding the best probability of the differential characteristics of 4–15 rounds SM4 in the single-key setting is presented. Especially, the authors found that the 15-round SM4 exists four differential characteristics with 12 active S-boxes. The exact lower bound of the number of differentially active S-boxes of the 16-round SM4 is 15. The authors also found eight differential characteristics of the 19-round SM4 with the probability 2^{-124}.

1 Introduction

Differential cryptanalysis [1] is one of the most important attacks on block ciphers. Over the past decades, lots of meaningful techniques on the differential cryptanalysis have been developed [2–4]. A security evaluation with respect to the differential attacks has become a basic requirement for a newly designed block cipher. Generally speaking, the effective way to evaluate the resistance of a block cipher against the differential attacks is calculating the lower bound of the number of active S-boxes. The most classic method is the Matsui's branch-and-bound depth-first search algorithm [5] which requests the researchers to have a higher programming ability. Recently, the methods based on the solvers become popular. The search problems can be described as mixed-integer linear programming (MILP), satisfiability modulo theory (SAT/SMT) or constraint programming (CP) problems [6–9], which can be automatically solved with the corresponding solvers [10–12]. Among them, the automatic search method based on MILP is simple and practical and has become an important tool.

The automatic search method based on the MILP has attracted increasing attention in recent years. The MILP method can not only search the differential distinguisher, but also the linear trail, impossible differential distinguisher, division property and so on [13–15]. This method was first proposed by Mouha *et al.* [6] and was used for counting the minimum number of differentially active S-boxes of advanced encryption standard (AES) by constructing a word-oriented MILP model. In Asiacrypt 2014, Sun *et al.* [16] proposed an extended bit-oriented framework to search the (related-key) differential characteristic. The key technique is to use the linear inequalities to describe the property of the differential distribution table (DDT) for the 4-bit S-box which can be obtained by using the SAGE software [17] to solve the H-representation of the convex hull of all possible differential patterns. Also then the greedy algorithm is used to remove redundant inequalities. As a result, there are about 30 linear inequalities for a 4-bit S-box. This auxiliary reduction algorithm cannot guarantee minimisation of the number of inequalities, Sasaki and Todo [18] proposed a new algorithm based on MILP for modelling S-boxes. Moreover, it enables the researcher to choose the number of inequalities in the system. The drawback of the Sun's method is impractical to the large S-boxes when the size is larger than 6-bit. Abdelkhalek *et al.* [19] first proposed a method to generate the inequalities of the DDT for the large S-boxes. They converted the problem of generating constraints in logic condition modelling into the problem of minimising the product-of-sum of Boolean functions which is a well-studied problem. The off-the-shelf software Logic Friday [20] can solve this problem automatically. They need more than 8000 inequalities to describe the differential propagation property of the AES S-box. Obviously, these inequalities will lead to a huge model when searching the differential characteristic. In addition, the Logic Friday software is computationally infeasible when the size of the S-box is larger than 8-bit. It is worth noting that the coefficients of inequalities in logical condition model only take {–1, 0, 1}, whereas the coefficients of inequalities in the H-representation of the convex hull belong to integer. In this paper, we mainly focus on how to obtain much fewer inequalities and the coefficients belong to integer even when the size of S-box is larger than 6.

Our Contributions. In this paper, we find the relationship between the coefficients of the inequalities and their excluded impossible differential patterns. Based on this observation, we extend the Sun's method to 8-bit (or more) S-boxes. Our idea is to divide averagely the DDT into multiple parts according to some chosen variables and solve the H-representation of the low dimension of the convex hull for these parts without considering the chosen variables by the SAGE, respectively. By using the new observation, the values of the coefficients of these positions of the chosen variables can be computed. Then we can reduce the number of inequalities by using the greedy algorithm or the MILP method. Based on the new method, we can obtain the inequalities of the differential propagation property of the large S-boxes and the coefficients can be chosen from the full spectrum of integer. As a result, the number of inequalities for the AES S-box is <4000. Moreover, if the probability of the possible nontrivial differential patterns of the S-box takes two values, 2^{-6} and 2^{-7}. We also can add an extra bit to mark the information of the probability and the coefficient can be computed by the same way. These inequalities can be used to search the differential characteristics with the best probability.

As application, we find the best probability of the differential characteristics for 4∼15 rounds SM4 in the single-key model. The results show that the best probability of differential characteristics of the 15-round SM4 is 2^{-82} with 12 active S-boxes. The exact lower bound of the number of differentially active S-boxes of the 16-round SM4 is 15. For the 19-round SM4, we obtain 8 differential characteristics with the probability of 2^{-124}.

Organisation: In Section 2, we introduce the word-oriented and bit-oriented MILP models and the methods to obtain the inequalities of the DDT of the S-box. In Section 3, we introduce the new method to obtain the inequalities of the large S-box. In Section 4, we use the new inequalities to search the differential characteristics with the best probability by using a two-stage algorithm. As application, we give the new results of the differential characteristics for the SM4. We conclude in Section 5.

2 Search frameworks based on MILP

In this section, we give two frameworks. One is the word-oriented MILP model, which is used to search the truncated differential or count the number of differentially active S-boxes. The other is the bit-oriented MILP model, which is used to search the differential characteristics.

2.1 Word-oriented MILP model

Mouha *et al*. [6] proposed the first framework to count the number of differentially active S-boxes for word-oriented block ciphers. The MILP model mainly contains two parts: the objection and the constraints. Obviously, the objection is minimising the number of differentially active S-boxes. Then we should include the constraints imposed by the operations of the cipher. In general, a block cipher is composed of XOR, linear transformation and S-box. We can introduce the 0–1 variables (1 for non-zero difference of one word and 0 otherwise) to mark these operations by word.

For the XOR operation, suppose $z = x \oplus y$, where $x, y, z \in F_2^w$ be the input and output differences. Then $(x, y, z) \in \{(0,0,1),(0,1,0),(1,0,0)\}$ are the impossible differential patterns. Based on the logical condition, the constraints are:

$$\begin{cases} x + y - z \geq 0 \\ x - y + z \geq 0 \\ -x + y + z \geq 0 \end{cases} \tag{1}$$

For the linear transformation, let $(x_0, \ldots, x_{n-1})$ and $(y_0, \ldots, y_{n-1})$ are the word-level input and output differences. B is the branch number of the linear transformation. Then

$$\begin{cases} \sum_i (x_i + y_i) - B \cdot d \geq 0 \\ d - x_i \geq 0, i \in \{0, \ldots, n-1\} \\ d - y_i \geq 0, i \in \{0, \ldots, n-1\} \end{cases} \tag{2}$$

where d is a dummy variable taking values in $\{0, 1\}$.

For the S-box operation, we do not need to give the special constraints. Whereas, we set up the objective function to be the sum of all variables representing the input words of the S-boxes.

2.2 Bit-oriented MILP model

This framework is mainly used to search the exact lower bounds of the number of differentially active S-boxes or the differential characteristics for the bit-oriented block ciphers. The 0–1 variables denote every input and output bit-level difference (1 for non-zero difference for 1 bit and 0 otherwise). In order to count the number of active S-boxes, we need to introduce a new variable A_i for every S-box, such that

$$A_i = \begin{cases} 1, & \text{if the input word of the sbox is non} - \text{zero} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

So the objective function is $\sum_i A_i$ which will be minimised.

For the bit-level XOR operation, the constraint is $z - x - y - 2xy = 0$ when we describe the model in the optimiser pseudo boolean (OPB) file format [21], where $x, y, z \in \{0, 1\}$ are the bit-level input and output differences.

For the S-box operation, the input and output differences are $(x_0, \ldots, x_{n-1})$ and $(y_0, \ldots, y_{m-1})$, respectively. We firstly construct the relationship between A and the input differences $(x_0, \ldots, x_{n-1})$

$$\begin{cases} A - x_i \geq 0, i \in \{0, \ldots, n-1\} \\ x_0 + \ldots + x_{n-1} - A \geq 0 \end{cases} \tag{4}$$

Also for bijective S-boxes, non-zero input differences must result in non-zero output differences and vice versa

$$\begin{cases} ny_0 + \cdots + ny_{m-1} - x_0 - \cdots - x_{n-1} \geq 0 \\ mx_0 + \cdots + mx_{n-1} - y_0 - \cdots - y_{m-1} \geq 0 \end{cases} \tag{5}$$

Most importantly, we need to obtain the linear constraints to describe the DDT of the S-box. There are mainly two methods: the H-representation of the convex hull and the product-of-sum of Boolean function.

(i) *The H-representation of the convex hull*: A polyhedron is the convex set in Euclidean space cut out by a finite set of linear inequalities or linear equations. There are two complementary representations of a polyhedron. One is H(alf-space/Hyperplane)-representation, the other is V(ertex)-representation. The points of the possible differential patterns of the S-box are the V-representations. In addition, we want to know the H-representation which is a set of linear inequalities or equations and can be obtained by using the *inequality-generator*() function in the *sage.geometry.polyhedron* class of the SAGE software. The inequalities obtained by SAGE are too many to construct an efficient MILP model. In order to reduce the number of inequalities, the greedy algorithm has been applied. This reduction problem also can be converted into a MILP problem to obtain the exact minimum number of inequalities or even able to choose the number of inequalities.

(ii) *The product-of-sum of Boolean function*: The product-of-sum representation of the Boolean function f can be written as:

$$f(\vec{x}, \vec{y}) = \bigwedge_{\bar{c} \in \{0,1\}^{2n}} \left(\bigvee_{i=1}^{n} (x_i \oplus c_i) \vee \bigvee_{i=1}^{n} (y_i \oplus c_{n+i}) \right) \tag{6}$$

We can construct a Boolean function $f(\vec{x}, \vec{y})$, where $\vec{x}$ and $\vec{y}$ are the input and output differences, respectively. $f = 1$ if an input and output differential pattern is possible, otherwise $f = 0$. We convert the DDT of the S-box into a truth table. Moreover, then we use the Logic Friday software to minimise the number of terms of the product-of-sum of the Boolean function f. Every term in the product-of-sum represents a linear inequality.

The H-representation of the convex hull is an effective method for 4-bit S-boxes. Nevertheless, the limitation is that it cannot be applied to large (8-bit or more) S-boxes. The method based on the product-of-sum of the Boolean function firstly gives the linear inequalities of differential propagation property for 8-bit S-boxes. However the coefficients of inequalities only take {–1, 0, 1} whereas the coefficients of inequalities in the H-representation of the convex hull belong to integer. Also only one set inequalities can be obtained and the number of the inequalities of the AES S-box is larger than 8000. In the following section, we propose a new method and obtain more than one set inequalities for large S-boxes with the coefficients belonging to integer and the number of inequalities is smaller than previous results.

Table 1 Example

Coefficients	−1	−1	0	−1	0	−1	1	−1	4
impossible differential patterns	1	1	0	1	0	1	0	1	
	1	1	0	1	1	1	0	1	
	1	1	1	1	0	1	0	1	
	1	1	1	1	1	1	0	1	
coefficients	−1	2	−1	1	1	−1	−2	−2	5
impossible differential patterns	0	0	1	0	0	1	1	1	
	1	0	0	0	0	1	1	1	
	1	0	1	0	0	0	1	1	
	1	0	1	0	0	1	1	1	
	1	0	1	0	1	1	1	1	
	1	0	1	1	0	1	1	1	

3 New method to generate the inequalities for large S-boxes

Let $(x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3) \in \{0,1\}^4$ represent the input and output bit-level differences of a 4-bit S-box. We can obtain a set of inequalities such as $\lambda_0 x_0 + \cdots + \lambda_3 x_3 + \lambda_4 y_0 + \cdots + \lambda_7 y_3 + \theta \geq 0$ by the SAGE. Every inequality indicates one or more excluded impossible differential patterns.

First of all, let us look at two examples in Table 1 where two inequalities came from the H-representation of the convex hull of the DDT for the 4-bit S-box of the SKINNY block cipher. The first inequality (–1, −1, 0, −1, 0, −1, 1, −1, 4) can exclude four impossible differential patterns. When the coefficient is −1, the values of the impossible differential patterns in this position are all equal to 1. Similarly, the coefficient is 1, the values of the impossible differential patterns in this position are all equal to 0. It is important that the constant coefficient 4 is equal to $-(-1\times 5+1)$. The second inequality (–1, 2, −1,1,1,–1,–2,–2,5) can exclude six impossible differential patterns. When the coefficient is −2, the values of the impossible differential patterns in this position are all equal to 1. The coefficient is 2, the values of the impossible differential patterns in this position are all equal to 0. Besides, the constant coefficient 5 is equal to $-(-2\times 2+(-1\times 3)+2)$. Some features are reflected in these two inequalities. We conclude in the Observation 1.

Observation 1: Suppose the inequality f, which can exclude m n-dimensional impossible differential patterns. Let δ be the sum of negative coefficients and θ be the constant coefficient. If it exists a position where the impossible differential patterns are all equal to 1 or 0 and the corresponding coefficient is λ or $-\lambda$. Then

$$\lambda = \delta + \theta \tag{7}$$

Based on the Observation 1, we can predict the values of the coefficients for some special variables. Whether there exists a position where the impossible differential patterns are all equality to 1 or 0, we can also get the value of λ through δ and θ when we extend the dimension of the impossible differential patterns by all 1 or 0, as described below.

Observation 2: Suppose the inequality f, which can exclude m n-dimensional impossible differential patterns of the S-boxes. Let δ be the sum of the negative coefficients and θ be the constant coefficient. We extend the impossible differential patterns to n' bits where the values of the extended positions are all equal to 1 or 0. Then the value of the coefficients for the extended positions in the new inequality f' which can exclude the m n'-dimensional impossible differential patterns are equal to $\delta+\theta$ or $-(\delta+\theta)$. Moreover the constant coefficient θ' is equal to $\lambda-\delta'$, where δ' is the sum of the negative coefficients of f'. The rest of coefficients remain unchanged.

Example 1: We have the first inequality f in Table 1. If we want to exclude the impossible differential patterns by extending with 1 in the first position: (111010101), (111011101), (111110101) and (111111101), then the corresponding new inequality is (–1,–1,–1,0,–1,0,–1,1,–1,5).

Due to the limitation of the SAGE software, we cannot obtain the inequalities of the DDT of 8-bit S-boxes directly. Based on the Observation 2, we use the new method to obtain the inequalities for large S-boxes. The procedure is outlined as follows:

Step 1. Partition: According to the solving capability of the SAGE software, we need to divide averagely the DDT to several parts according to some chosen variables. For example, we can obtain the H-representation of the n-dimension convex hull by the SAGE while the input–output differential patterns of the S-box is the N-dimension points $(x_0, \ldots, x_{N-1})$, where $N > n$. We choose any $N-n$ bits as the extended bits and divide the DDT according to the value of these bits in the input–output differential patterns. Then we get 2^{N-n} parts which the $N-n$ bits in input–output differential patterns have the same values.

Step 2. Solving: We do not need to consider the $N-n$ bits in the input–output differential patterns, but only solve separately the H-representation of the 2^{N-n} n-dimension convex hull by the SAGE. Namely, we get the 2^{N-n} sets of inequalities to exclude the n-dimension impossible differential patterns of all parts.

Step 3. Extension: Based on Observation 2, we extend the sets of inequalities to be able to exclude N-dimension impossible differential patterns.

Step 4. ***Exclusion***: Based on the greedy algorithm or the MILP method, the redundant inequalities can be removed.

Obviously, we can change the sequence of Step 3 and 4. In this paper, we apply the extension firstly. For the AES S-box, let $(x_0, \ldots, x_7, y_0, \ldots, y_7)$ is the input–output bit-level differences. According to the solving ability of the SAGE, we chose the first 4-bit (x_0, x_1, x_2, x_3) as the extend variables and obtain 16 parts for the DDT of the AES S-box. Table 2 shows the number of inequalities for each parts by the CaCalc [22] which is an online service for running SAGE computations. The solving time of every part is about 10 min.

After extending all the inequalities, we use the MILP method to remove the redundant inequalities. We have not solved the exact minimised number of the inequalities in some case which would need a lot of time, while the given solution which can be obtained in a few minutes by the Gurobi. The results are shown in Table 3.

Specially, the SAGE works quite well for the dimension up to 12, i.e. each point consists of 12 bits, as the command takes 2–3 min. However, when the dimension increases over 12, the speed of the solving is get really slow and the SAGE will be unable to output the result. Obviously, the dimension is an important factor. At the same time, we found that the size and distribution of points can also decide whether the H-representation of the convex hull can be solved. For example, when we consider the MISTY1 S9 which is a 9-bit S-box, the solvable dimension can be reach 13. Then we need to solve 32 13-dimension rather than 64 12-dimension convex hulls. We chose the first 5-bit positions as the extend variables. As a result, we can obtain 9431 inequalities to describe the DDT of the MISTY1 S9.

Table 2 Number of inequalities of the each part of the DDT of the AES S-box

Structure	$x_0x_1x_2x_3$	#Possible patterns	#Inequalities
AES S-box	0 0 0 0	1906	12,227
	0 0 0 1	2032	9996
	0 0 1 0	2032	9842
	0 0 1 1	2032	9861
	0 1 0 0	2032	9916
	0 1 0 1	2032	10,312
	0 1 1 0	2032	10,149
	0 1 1 1	2032	9859
	1 0 0 0	2032	10,064
	1 0 0 1	2032	1094
	1 0 1 0	2032	9951
	1 0 1 1	2032	10,154
	1 1 0 0	2032	9839
	1 1 0 1	2032	9860
	1 1 1 0	2032	9607
	1 1 1 1	2032	9702

Table 3 Number of inequalities after the exclusion

Structure	Pr	#Inequalities	
		This paper	[19]
AES S-box	Non-zero	<4000	8302
	2^{-6}	108	350
	2^{-7}	<4000	8241
MISTY1 S9	Non-zero	9431	\

Input: the number of active S-boxes n_{tru} in round i;
Output: the best probability of the differential characteristic log_2Pr;
1: $m_0.optimize$(word-oriented-model.opb)
2: **if** $m_0.get$(GRB_IntAttr_Status)==3 **then**
3: Infeasible.
4: **else**
5: $m_1.optimize$(bit-oriented-model.opb, $\triangle^i$)
6: **if** $m_1.get$(GRB_IntAttr_Status)==3 **then**
7: Update(word-oriented-model.opb, $\triangle^i$); Store $\triangle^i$ and back to Step 1.
8: **else if** $n_p == 0$ **then**
9: $log_2Pr = -6 \times n_{tru}$;
10: Stop the search due to the best probability has found.
11: **else**
12: $log_2Pr = -6 \times (n_{tru} - n_p) - 7 \times n_p$ and store.
13: **end if**
14: **end if**

Fig. 1 *Algorithm 1: Search the differential characteristics with the best probability*

Moreover, to search the best probability of the truncated differential characteristic, we use the idea of [19] to separate the DDT to *pd*-DDT according to the probability. We use the new method to obtain the inequalities for each *pd*-DDT. Then we can extend one more bit p to indicate the probability if there are two non-zero probability, 2^{-6} and 2^{-7}. The value of p is as follows:

$$p = \begin{cases} 0, & \text{the probability is } 2^{-6} \\ 1, & \text{the probability is } 2^{-7} \end{cases} \quad (8)$$

So, we need to solve 32 12-dimension convex hulls. The result of AES S-box is shown in Table 3. Then the objective of the search, which is the best probability of the truncated differential characteristic, is to minimise $\sum_i p_i$. Assume the number of the active S-boxes of the truncated differential characteristic is n_{tru} and the minimisation of $\sum_i p_i$ is n_p, the best probability is equal to $2^{-6\times(n_{\text{tru}}-n_p)-7\times n_p}$.

4 Searching for the differential characteristics with the best probability

4.1 Two-stage to search the differential characteristics with the best probability

We adopt a two-stage algorithm [16] to search the differential characteristics with the best probability. Firstly, we need to obtain the number of active S-boxes with the word-oriented model. So we obtain a threshold of the number of active S-boxes. In Algorithm 1, we need to construct two models, m_0 and m_1. In the word-oriented model m_0, the *Callback*() function in Gurobi is to terminate the optimisation when a feasible solution is already appeared. We do not need to wait a long time to prove this solution is the best in each case. The modes of the truncated differential active S-boxes Δ^i in round i namely the output of the model m_0 are detected in one by one and a constraint of a truncated differential mode is used to update the m_0 to exclude the solution which has been detected. After getting the solution of m_0, we import the information about the positions of the active S-boxes Δ^i to the bit-oriented model m_1. We need to add the inequalities obtained by the new method for the active S-boxes while set the input–output variables of the nonactive S-boxes to all zeros. If the objective $\sum_i p_i$ of m_1 is equal to zero, then we have found a differential characteristic with the best probability with all active S-boxes have probability 2^{-6}. We can stop to this round's search or otherwise continue until all the possible truncated differential modes had been detected. We also need to store all invalid truncated differential modes of round i to exclude invalid modes previously in the next round's search. [!t] (Fig. 1).

We employ the C++ interface provided by the Gurobi7.5.2 to automate the whole process of the Algorithm 1. The OPB file format is used to store the MILP instances. The computations are performed on PC (Intel(R) Core(TM) i3–4160 CPU, 3.60 GHz, 4.00 GB RAM, 4 cores, window7).

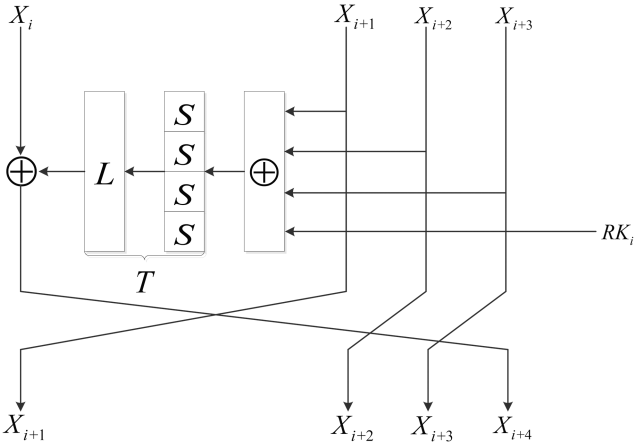

Fig. 2 *Round function of SM4*

Table 4 Lower bounds on the number of active S-boxes of SM4 in single-key setting

Rounds	4	5	6	7	8	9	10	11	12
# Active S-boxes	1	2	2	5	6	7	8	9	10
rounds	13	14	15	16	17	18	19	20	21
# Active S-boxes	10	10	13	14	15	16	18	18	19

4.2 Application to SM4

4.2.1 Description of SM4: SM4 [23] is the first Chinese commercial block cipher standard and mandated for use in protecting wireless networks. The size of block and key are both 128-bit. It consists of 32 rounds. The round's structure of SM4 is modified one of the four 32-bit works that make up the block by XOR it with the keyed function of the other three words, as shown in Fig. 2.

Mixer-substitution T is consists of a non-linear substitution and a linear substitution L, i.e. $T(\cdot) = L(\tau(\cdot))$. The τ applies 4 8-bit S-boxes in parallel. Let $B \in Z_2^{32}$ and $C \in Z_2^{32}$ be the input and output word of the linear substitution L. Then

$$\begin{aligned} C &= L(B) \\ &= B \oplus (B <<< 2) \oplus (B <<< 10) \oplus (B <<< 18) \\ &\quad \oplus (B <<< 24) \end{aligned} \tag{9}$$

The branch number of L is 5. We are mainly interested in the single-key setting and the more details of the key schedule algorithm can be found in [23].

4.2.2 Searching the best differential probability of SM4: We refer to the result of lower bounds on the number of active S-boxes for different rounds of SM4 in single-key setting in [24].

The constraints of the word-oriented MILP model can be referred to [24]. In the bit-oriented MILP model, the constraints of L can be simplified. We need 3 intermediate variables and 4 XOR constraints in bit-level directly. In fact, we only need 2 intermediate variables and 3 XOR constraints owing to the feature of the shift number. Let B be the input L, then (see (10)) is the first intermediate variable, $V = W \oplus (W > > > 14)$ is the second intermediate variable. So the output is $C = V \oplus (B < < < 2)$. This simplification can speed up the solving time.

We use the new method to obtain a set of inequalities to describe the differential propagation property of the SM4 S-box. There are 4146 inequalities in our search. We select a relatively small number of inequalities instead of the exact minimised number of inequalities (Table 4).

4.2.3 Analysis of the results: The result of the search for the differential characteristics with the best probability of SM4 is shown in Table 5. The search starts with 4-round which has only one active S-box. We first finished the full search of the 4–15-round in reasonable time. Table 5 shows the number of possible and impossible truncated differential modes #Possible and #Impossible in our search. For the 15-round SM4, we found 4 differential characteristics with 12 active S-boxes and the probability is 2^{-82}, which indicates that some errors exist in [24]. For the 16-round SM4, we proved that the number of differentially active S-boxes is larger than 14. We also found a valid differential characteristics with 15 active S-boxes of 16-round SM4 with the probability 2^{-105}. The weight of the active S-boxes of this truncated differential characteristic mode is

$$(0, e, 0, 0, a, a, 0, 0, 6, 6, 0, 0, a, a, 0, 0)\,. \tag{11}$$

For the 19-round SM4, we test two active round's modes {(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0), (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)} in Table 6, which have been proved that there are no valid differential characteristic with 17 active S-boxes. In this paper, we obtain 4 valid differential characteristics for each mode with the probability of 2^{-124}. One of the differential characteristics belongs to [25]. The results are shown in Table 7.

5 Conclusion

In this paper, we introduce a new method to obtain the inequalities of the differential propagation property of large S-boxes with the coefficients belonging to integer. We obtain much fewer inequalities to describe the DDT of the 8-bit S-box than before. Moreover, the information of the probability can be treated as an extra variable when we construct a new system of inequalities by the new method to search the differential characteristics with the optimal probability. Also a new insight on the differential characteristics of SM4 is given.

$$W = B \oplus (B < < < 24) = ((B < < < 10) \oplus (B < < < 18)) > > > 14 \tag{10}$$

Table 5 Best differential characteristic of SM4

Rounds	# Possible	# Impossible	$\log_2 Pr$	Time	#Active S-boxes	$\#Pr = 2^{-7}$
4	1	0	−6	1 s	1	0
5	1	0	−12	1 s	2	0
6	1	0	−12	1 s	2	0
7	2	0	−30	3 m	5	0
8	56	344	−38	21 h	6	2
9	16	768	−46	23 h	7	4
10	38	536	−52	36 h	8	4
11	56	48	−60	10 h	9	6
12	12	244	−67	13 h	10	7
13	8	0	−68	1.3 h	10	8
14	4	0	−68	0.8 h	10	8
15	4	0	−82	2.3 h	12	10
16	—	104	—	41 h	14	—

Table 6 Results of the 19-round SM4

Mode	#Possible	#Impossible	Time
1,001,100,110,011,001,100	4	218	≃2 days
0,011,001,100,110,011,001	4	218	≃2 days

Table 7 Differential characteristic of the 19-round SM4 with probability 2^{-124}

Rounds	Input differences				*Pr*
0	33f3f300	33f3f300	fcccf300	cf3f0000	—
1	33f3f300	fcccf300	cf3f0000	33f3f300	1
2	fcccf300	cf3f0000	33f3f300	33f33f00	1
3	cf3f0000	33f3f300	33f33f00	30f30000	2^{-14}
4	33f3f300	33f33f00	30f30000	0300f300	2^{-14}
5	33f33f00	30f30000	0300f300	33f3f300	1
6	30f30000	0300f300	33f3f300	33f3f300	1
7	0300f300	33f3f300	33f3f300	3300cf00	2^{-14}
8	33f3f300	33f3f300	3300cf00	00f33c00	2^{-14}
9	33f3f300	3300cf00	00f33c00	33f3f300	1
10	3300cf00	00f33c00	33f3f300	33f3f300	1
11	00f33c00	33f3f300	33f3f300	00f33c00	2^{-14}
12	33f3f300	33f3f300	00f33c00	3300cf00	2^{-14}
13	33f3f300	00f33c00	3300cf00	33f3f300	1
14	00f33c00	3300cf00	33f3f300	33f3f300	1
15	3300cf00	33f3f300	33f3f300	0300f300	2^{-14}
16	33f3f300	33f3f300	0300f300	30f30000	2^{-14}
17	33f3f300	0300f300	30f30000	33f3f300	1
18	0300f300	30f30000	33f3f300	33f3f300	1
end	30f30000	33f3f300	33f3f300	8ce5992d	2^{-12}

6 References

[1] Biham, E., Shamir, A.: 'Differential cryptanalysis of DES-like cryptosystems'. *J. Cryptol.*, 1991, **4**, (1), pp. 3–72

[2] Wagner, D: 'The boomerang attack'. Proc. Int. Conf. FSE, Rome, Italy, March 1999, pp. 156–170

[3] Knudsen, L.R: 'Truncated and higher order differentials'. Proc. Int. Conf. FSE, Leuven, Belgium, December 1994, pp. 196–211

[4] Bahrak, B., Aref, M.R.: 'Impossible differential attack on seven-round AES-128', *IET Inf. Sec.*, 2008, **2**, (2), pp. 28–32

[5] Matsui, M.: 'On correlation between the order of S-boxes and the strength of DES'. Proc. Int. Conf. EUROCRYPT, Italy, May 1994, pp. 366–375

[6] Mouha, N., Wang, Q., Gu, D., *et al.*: 'Differential and linear cryptanalysis using mixed-integer linear programming'. Proc. Int. Conf. Inscrypt, Beijing China, November 2011, pp. 57–76

[7] Mouha, N., Preneel, B.: 'Towards finding optimal differential characteristics for ARX: application to Salsa20', Cryptology ePrint Archive, May 2013

[8] Gĺęrault, D., Lafourcade, P., Minier, M., *et al.*: 'Revisiting AES related-key differential attacks with constraint programming', Cryptology ePrint Archive, February 2017

[9] Sun, S., Gerault, D., Lafourcade, P., *et al.*: 'Analysis of AES, SKINNY, and others with constraint programming', Cryptology ePrint Archive, February 2017

[10] 'Gurobi Optimizer 7.5.2', http://www.gurobi.com

[11] 'CryptoMiniSat5', https://www.msoos.org/cryptominisat5

[12] 'Choco', http://www.choco-solver.org/

[13] Sasaki, Y., Todo, Y.: 'New impossible differential search tool from design and cryptanalysis aspects'. Proc. Int. Conf. EUROCRYPT, Paris, France, April 2017, pp. 185–215

[14] Xiang, Z., Zhang, W., Bao, Z., *et al.*: 'Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers'. Proc. Int. Conf. ASIACRYPT, Hanoi, Vietnam, December 2016, pp. 648–678

[15] Cid, C., Huang, T., Peyrin, T., *et al.*: 'A security analysis of deoxys and its internal tweakable block ciphers', *IACR Trans. Symmetric Cryptol.*, 2017, **17**, (3), pp. 73–107

[16] Sun, S., Hu, L., Wang, P., *et al.*: 'Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers'. Proc. Int. Conf. ASIACRYPT, Kaoshiung, Taiwan, ROC, December 2014, pp. 158–178

[17] 'SAGE', http://www.sagemath.org/index.html

[18] Sasaki, Y., Todo, Y.: 'New algorithm for modeling S-box in MILP based differential and division trail search'. Proc. Int. Conf. SecITC, Bucharest, Romania, June 2017, pp. 150–165

[19] Abdelkhalek, A., Sasaki, Y., Todo, Y., *et al.*: 'MILP modeling for (large) S-boxes to optimize probability of differential characteristics', *IACR Trans. Symmetric Cryptol.*, 2017, **2017**, (4), pp. 99–129
[20] 'Logic friday', http://sontrak.com/
[21] Li, L., Wu, W., Zhang, L.: 'Improved automatic search tool for Bit-oriented block ciphers and its applications'. Proc. Int. Conf. ICICS, Beijing, China, December 2017, pp. 502–508
[22] 'COCAL', https://cocalc.com/
[23] Diffie, W., Ledin, G.: 'SMS4 encryption algorithm for wireless networks', IACR Cryptology ePrint Archive, July 2008
[24] Zhang, J., Wu, W., Zheng, Y.: 'Security of SM4 against (related-key) differential cryptanalysis'. Proc. Int. Conf. ISPEC, Zhangjiajie, China, November 2016, pp. 65–78
[25] Su, B.Z., Wu, W.L., Zhang, W.T.: 'Security of the SMS4 block cipher against differential cryptanalysis'. *J. Comput. Sci. Technol.*, 2011, **26**, (1), pp. 130–138