Noname manuscript No.
(will be inserted by the editor)

An STP-based model toward designing S-boxes with good cryptographic properties

Zhenyu Lu · Sihem Mesnager · Tingting Cui · Yanhong Fan · Meiqin Wang

Received: date / Accepted: date

Abstract The substitution box (S-box) is an important nonlinear component in most symmetric cryptosystems and thus should have good properties. Its

Zhenyu Lu
School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
E-mail: luzhenyu@mail.sdu.edu.cn

Sihem Mesnager
Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, University Sorbonne Paris Cité, LAGA, UMR 7539, CNRS, 93430 Villetaneuse and Telecom Paris, Polytechnic Institute of Paris, 91120 Palaiseau, France.
E-mail: smesnager@univ-paris8.fr

Tingting Cui
School of Cyberspace, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
E-mail: cuitingting@hdu.edu.cn
This author is supported by the Open Project Program from Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University.
Corresponding author: Tingting Cui.

Yanhong Fan
School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
E-mail: fanyh@mail.sdu.edu.cn

Meiqin Wang
School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
Quan Cheng Shandong Laboratory, Jinan, China
E-mail: mqwang@sdu.edu.cn

difference distribution table (DDT) and linear approximation table (LAT) affect the security of the cipher against differential and linear cryptanalysis. In most previous work, differential uniformity and linearity of an S-box are two primary cryptographic properties to impact the resistance against differential and linear attacks. In some cases, the branch number and fixed point are also be considered. However, other important cryptographic properties such as the frequency of differential uniformity (resp. linearity) and the number of Bad Input and Bad Output (BIBO) patterns in DDT (resp. LAT) are often ignored. These properties substantially affect lightweight cryptography based on substitution bit permutation networks (SbPN) such as PRESENT, GIFT and RECTANGLE. This paper introduces a new method to search for S-boxes satisfying all above criteria simultaneously. In our strategy, we transform the process of searching for S-boxes under certain constraints on cryptographic properties into a satisfiability (SAT) problem. As applications, we use our new approach to search out 4-bit and 5-bit S-boxes with the same or better cryptographic properties compared with the S-boxes from well-known ciphers. Finally, we also utilize our method to verify a conjecture proposed by Boura et al. in the case of all 3-bit and 4-bit S-boxes. We propose a proposition and two corollaries to reduce the search space in this verification.

Keywords Symmetric cryptography · Lightweight cryptography · Block cipher · S-box · Difference Distribution Table (DDT) · Linear Approximation Table (LAT)

Mathematics Subject Classification: 11T71, 14G50, 68P25, 81P94.

1 Introduction

The substitution box (S-box) is the nonlinear component of symmetric cryptography primitives since it provides "confusion" for ciphers. The security of a cipher is strongly dependent on the cryptographic properties of its S-box. Consequently, an S-box used in cryptography should have good properties to resist various attacks.

Differential and linear attacks are two important statistical techniques in cryptanalysis of block ciphers, introduced by Biham and Shamir [11] and Matsui [35] respectively. In order to resist differential and linear attacks, differential uniformity and linearity of an S-box are considered as two primary cryptographic properties in most previous works. They should be as small as possible. In some cases, designers may consider the branch number, fixed points and so on [5,43].

Previous approaches available in the literature for the construction of an S-box can be divided into three main streams:

1. Choose an S-box randomly.
2. Design an S-box by mathematical algebraic or structural constructions.
3. A variety of heuristic approaches to generate an S-box.

The first type of approaches is based on using some pseudo-random generation. However, it is hard to provide good results as the search space is too large and good cryptographic properties are scarce [37]. Hence designers use the second type of approaches more and more, which are mathematical or structural methods to generate S-boxes. The mathematical method consists in finding expressions leading to better properties. For example, AES's S-box [20] is based on inversion in the finite field $GF(2^8)$ and simultaneously optimal with respect to most of desired criteria, such as differential uniformity and linearity. RECTANGLE's S-box [43] is chosen from one of the optimal 4-bit S-box equivalence classes [32]. Besides that, structural methods are also used in cryptography. SKINNY's [9] S-box is designed based on a generalized Feistel structure and Midori's [4] S-box has involution property by utilizing two smaller S-boxes and a bit permutation. So, the inverse of their S-boxes are straightforward deduced and have low hardware implementation cost. The last approach uses heuristic algorithms including the hill climbing method, the simulated annealing method, the genetic algorithm or a combination of these algorithms [26, 28, 42]. All these heuristic algorithms use guided search in order to evolve S-boxes to find even better ones. They described give good results for constructing bijective S-boxes with respect to only one of the main criteria, but it becomes much more challenging when more properties should be considered simultaneously [27].

However, as mentioned above, these approaches are hard to give good results when multiple cryptographic properties are considered simultaneously. Usually, designers divide all the properties that need to be considered into several parts to search for an S-box in steps. For example, designers first search for a set of S-boxes with the optimal differential uniformity and linearity. Then, they exhaust S-boxes from the set to meet other requirements, such as no fixed points, high branch numbers and so on. In the process of a step-by-step search, some good results will be ignored, such as GIFT's S-box that does not have the optimal differential uniformity. Therefore, how to search for an S-box with multiple good cryptographic properties together in a more efficient way is our first motivation in this paper.

Lightweight cryptography has become an extremely active research topic with the development of the Internet of Things (IoT), which aims to provide security in a limited resource environment. The properties of the S-box in lightweight cryptography are considered more carefully than before, especially in substitution bit-permutation networks (SbPN), such as PRESENT [13], GIFT [5], and RECTANGLE [43]. The SbPN ciphers use a bit-permutation as the diffusion layer and thus saving a considerable amount of hardware cost. Consequently, the security of these ciphers greatly depend on the S-boxes. In this case, the frequency of differential uniformity (resp. linearity) in DDT (resp. LAT) has a great effect on multiple differential (resp. linear hull) attacks. In other words, S-boxes that have the same differential uniformity (linearity) but different frequencies of differential uniformity (linearity) may have different performances in terms of resistance against differential (linear) attacks. Meanwhile, a bad input and bad output (BIBO) pattern in DDT (resp. LAT)

may result in a differential or linear trail with a single active S-Box. Here, BIBO means that the hamming weight of both input and output differences (or masks) is exactly one. For instance, PRESENT's DDT has no BIBO pattern, but its LAT has 8 BIBO patterns. As a result, its linear attack is nearly ten rounds longer than its differential attack.

Furthermore, it is almost impossible for an S-box to achieve that all properties above are optimal simultaneously. Designers need to trade off between different cryptography properties. For example, GIFT uses an S-box with sub-optimal differential uniformity so that the total number of BIBO patterns of the S-box is as low as possible. In this case, it can still resist differential attacks very well. The previous approaches for constructing an S-box have limitations on a trade-off between these properties and search for sub-optimal solutions. Thus our second motivation is to efficiently find good S-boxes with a trade-off between all properties above.

Finally, reconstructing S-boxes from a given DDT or LAT is a significant problem. It can be used to recover the secret S-box from DDT or LAT. For example, in the slide attack on GOST proposed by Bar-On et al. [7], the attacker could deduce the secret S-box from its known DDT. Another line of research that will enjoy such efficient reconstruction algorithms is the study of the theoretical properties of DDTs. A recent work by Boura et al. [14] studies a theoretical question — whether two different S-boxes, which do not satisfy some trivial relation, could share the same DDT. To answer the question, Boura et al. proposed a guess-and-determine (GD) algorithm by utilizing a depth-first search strategy. Later, Dunkelman and Huang improved the GD algorithm by using the relationship between DDT and LAT to reduce the search space [23]. Nevertheless, both algorithms have limitations that they can only reconstruct S-boxes from a known DDT and are powerless to support theoretical analysis about non-specific DDT and LAT issues. Therefore, our third motivation is to build a model which can analyze the S-box and its DDT or LAT when we do not know the complete DDT or LAT.

Our Contributions

In view of the above state-of-the-art, our contributions are twofold as follows.

1. **Propose a new method of searching for S-boxes with good cryptographic properties**
   In this paper, we build a model which can consider many cryptographic properties at the same time, such as fixed points, branch number, differential uniformity, linearity, the frequency of differential uniformity (linearity) and the number of BIBO patterns. Firstly, we transform the relationship between an S-box and its DDT and LAT into a satisfiability modulo theories (SMT) problem. Then we add the requirements on cryptographic properties of S-boxes as constraints. Finally, we utilize an SMT solver STP (Simple Theorem Prover) to solve the model and get expected S-boxes.

As applications, for 4-bit S-boxes, we apply this model to search out 3723/947/620 S-boxes which have the same cryptographic properties as the S-boxes used in PRESENT/GIFT/RECTANGLE. We summarize the results in Table 1. In addition, we also trade off difference uniformity against the number of BIBO patterns. As a result, we search out 824 S-boxes to meet different design requirements. Compared with PRESENT/GIFT/RECTANGLE's S-boxes, although these new S-boxes have a slightly higher differential uniformity, there are only 3 BIBO patterns in total. For 5-bit S-boxes, we search out 31/28 S-boxes with the same cryptographic properties as the 5-bit S-box used in KECCAK/ASCON, which are summarized in Table 2. Furthermore, we find out 17 5-bit new S-boxes better than KECCAK/ASCON's S-boxes in terms of the differential uniformity.
In addition, we simplify the above model, replacing the constraints on properties with the values of predetermined DDT or LAT. We use this new model to search for S-boxes that have the same DDT as PRESENT and KECCAK without fixed points. In experiments, we search all 96 out of 256 S-boxes without fixed point corresponding to the DDT of PRESENT's 4-bit S-box within 10 minutes and 672 out of 1024 S-boxes without fixed point corresponding to the DDT from KECCAK's 5-bit S-box within 7.5 hours.

Table 1: Summary of cryptographic properties of PRESENT, GIFT and RECTANGLE's S-boxes and new S-boxes found in our work. $\#\text{BIBO}_{\text{DDT}}$ and $\#\text{BIBO}_{\text{LAT}}$ represent the number of BIBO patterns in DDT and LAT, respectively. Differential uniformity and linearity are denoted as $\mathcal{U}(S)$ and $\mathcal{L}(S)$. The frequency of differential uniformity and linearity in DDT and LAT are represented by $\#\mathcal{U}(S)$ and $\#\mathcal{L}(S)$, respectively.

	$\#\text{BIBO}_{\text{DDT}}$	$\#\text{BIBO}_{\text{LAT}}$	$\mathcal{U}(S)$	$\mathcal{L}(S)$	$\#\mathcal{U}(S)$	$\#\mathcal{L}(S)$	#New S-boxes
PRESENT [13]	0	8	4	8	24	36	**3723**
GIFT [5]	1	3	6	8	2	36	**947**
RECTANGLE [43]	2	2	4	8	24	36	**620**
New S-box[1]	**1**	**2**	**8**	**8**	**2**	**44**	**834**

[1] $\delta_S(\alpha, \beta) = 8$ only occurs twice in the DDT of our new S-box.

Table 2: Summary of cryptographic properties of KECCAK and ASCON's S-boxes and new S-boxes found in our work.

	$\#\text{BIBO}_{\text{DDT}}$	$\#\text{BIBO}_{\text{LAT}}$	$\mathcal{U}(S)$	$\mathcal{L}(S)$	$\#\mathcal{U}(S)$	$\#\mathcal{L}(S)$	#New S-boxes
KECCAK [10]	5	5	8	16	20	40	**31**
ASCON [22]	0	0	8	16	20	40	**28**
New S-box	**0**	**0**	**6**	**16**	**24**	**40**	**17**

2. **Verify the conjecture proposed by Boura et al. in [14]**
In paper [14], Boura et al. propose a conjecture that an S-Box $S(x)$ only has trivially DDT-equivalent S-Boxes of the form $S(x \oplus c) \oplus d$, with $c, d \in \mathbb{F}_2^n$, if and only if the rows in its DDT are pairwise distinct.

In this paper, we first propose a proposition and two corollaries to reduce the search space in the verification. Then we extend our model in Section 3 to verify the conjecture. We use the same way to transform the relationship between two S-boxes and their same DDT into an SMT problem. Finally, we add the conditions mentioned in the conjecture as constraints on the model, such as two S-boxes are not trivially DDT-equivalent and any rows of the DDT are pairwise distinct. Experimentally, we verify the correctness of the conjecture for all 3-bit and 4-bit S-boxes by using our model.

Organization of the article

In Section 2, we recall some preliminaries, including differential and linear properties of an S-box and an overview of STP. Next, we propose a new method of searching for S-boxes with good properties and apply it to 4-bit and 5-bit S-boxes in Sections 3 and 4 respectively. In Section 5, we verify a conjecture about trivially DDT-equivalence class of an S-box proposed by Boura *et al.* Finally, we conclude this paper in Section 6.

2 Preliminaries

In this section, we first recall the basic differential and linear properties of an S-box in Section 2.1. In Section 2.2, we introduce some definitions of other important cryptographic properties of an S-box, such as the frequency of differential uniformity, the frequency of linearity, and the number of BIBO patterns. Then, we briefly introduce the Simple Theorem Prover (STP) solver and its CVC input language formats in Section 2.3.

2.1 Basic differential and linear properties of S-boxes

Often the S-boxes are the only nonlinear components in a block cipher and play an important role in ensuring the cipher's resistance to cryptanalysis. Mathematically, an S-box corresponds to a vectorial Boolean function and an $m \times n$ S-box $S : \mathbb{F}_2^m \to \mathbb{F}_2^n$ is a mapping from m-bit input to n-bit output. For each input $x = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{F}_2^m$, there is one output $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^n$ such that $y = S(x)$.

Differential uniformity and linearity are two important cryptographic properties to impact an S-box's resistance against differential and linear attacks, which should be carefully considered when constructing an S-box. We briefly recall some definitions and properties related to them.

Definition 1 (Difference distribution table) Let $S : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be an S-box. For any $\alpha \in \mathbb{F}_2^m$ and $\beta \in \mathbb{F}_2^n$, $\delta_S(\alpha, \beta)$ is defined as

$$\delta_S(\alpha, \beta) = \#\{x \in \mathbb{F}_2^m | S(x) \oplus S(x \oplus \alpha) = \beta\}.$$

An $2^m \times 2^n$ table T can be built as follow: take α as the row index to traverse $\mathbb{F}_2^m$, β as the column index to traverse $\mathbb{F}_2^n$, as well as the value $\delta_S(\alpha, \beta)$ at the intersection of the α-th row and β-th column. Such table is defined as *differential distribution table* (DDT) of the S-box, in which α denotes the input difference, β denotes the output difference and $\delta_S(\alpha, \beta)$ denotes how many x satisfy this (α, β).

Based on the definition of DDT, the differential uniformity of an S-box is defined as follows.

Definition 2 (Differential uniformity [36]) The differential uniformity of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as

$$\mathcal{U}(S) \triangleq \max_{\alpha \in \mathbb{F}_2^n \setminus \{0\}, \beta \in \mathbb{F}_2^m} \delta_S(\alpha, \beta).$$

It is easy to find that the differential uniformity of any S-box is greater than or equal to 2 ($\mathcal{U}(S) \geq 2$). If $\mathcal{U}(S)$ of an S-box reaches the minimum, i.e. $\mathcal{U}(S) = 2$, we call this S-box *almost perfect nonlinear* (APN).

The existence of n-bit APN permutation is implied by the existence of n-bit almost Bent (AB) functions [18,36] when n is odd. However, when n is even, only one 6-bit APN S-box has been discovered by Dillon et al. in 2009 [15]. Whether an APN S-box exists or not on other even dimensions is still an open problem, named "The Big APN Problem" [17].

Definition 3 (DDT-equivalent) Two different S-boxes $S_0(x)$ and $S_1(x)$ are *DDT-equivalent* if they have the same DDT, and they are *trivially DDT-equivalent* if and only if they satisfy that $S_0(x) = S_1(x \oplus c) \oplus d$ with c, d in $\mathbb{F}_2^n$.

To calculate the number of S-boxes trivial DDT-equivalent to an S-box S, we give Proposition 1. Assume that S is an n-bit bijective S-box. If $\Delta_a S(x) = S(x) \oplus S(x \oplus \alpha)$ is constant for all possible x, we call this $\alpha \in \mathbb{F}_2^n$ a linear structure. The set of all linear structures is a vector space named linear space of S.

Proposition 1 *([14]) Let S be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ and let l denote the dimension of its linear space. Then, the DDT-equivalence class of S contains the 2^{2n-l} distinct functions of the form*

$$x \mapsto S(x \oplus c) \oplus d, \quad c, d \in \mathbb{F}_2^n. \tag{1}$$

We say that a DDT-equivalent class is trivial if its size matches the lower-bound given in Proposition 2.

Definition 4 (Linear approximation table) Let $S : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be an S-box. For any $\alpha \in \mathbb{F}_2^m$ and $\beta \in \mathbb{F}_2^n$, $\lambda_S(\alpha, \beta)$ is defined as

$$\lambda_S(\alpha, \beta) = \#\{x \in \mathbb{F}_2^n | \alpha \cdot x \oplus \beta \cdot S(x) = 0\} - 2^{n-1} = \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x \oplus \beta \cdot S(x)}.$$

Recall that the *Walsh Fourier transform* of S is defined as

$$\mathcal{W}_S(\alpha,\beta) \triangleq \sum_{x\in\mathbb{F}_2^n} (-1)^{\alpha\cdot x\oplus\beta\cdot S(x)}.$$

An $2^m \times 2^n$ table T can be built as follow: Take α as the row index to traverse $\mathbb{F}_2^m$, β as the column index to traverse $\mathbb{F}_2^n$, as well as the value $\lambda_S(\alpha,\beta)$ at the intersection of the α-th row and β-th column. Such table is defined as *Linear Approximation Table* (LAT) of the S-box, in which α denotes the input mask, β denotes the output mask and $\lambda_S(\alpha,\beta)$ denotes how many x satisfy this (α,β).

Based on the definition of LAT, the linearity of an S-box is defined as follows.

Definition 5 (Linearity [36]) The linearity of an S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as

$$\mathcal{L}(S) = \max_{\alpha\in\mathbb{F}_2^n,\beta\in\mathbb{F}_2^m\setminus\{0\}} |\mathcal{W}_S(\alpha,\beta)|$$

Linearity impacts the resistance against linear cryptanalysis. Generally, designers expect that the linearity of an S-box is as low as possible. Note that in some other papers, the authors use nonlinearity rather than linearity. Actually, the nonlinearity and linearity of an S-box are related by:

$$\mathcal{NL}(S) = 2^{n-1} - \frac{1}{2}\mathcal{L}(S)$$

As is well known for bijective S-boxes, the linearity $\mathcal{L}(S) \geq 2^{(n+1)/2}$. Especially, for even dimension n, the smallest linearity is $2^{n/2+1}$ [18]. When the linearity of an S-box S reaches the lower bound, this S is called *almost bent* (AB) function. An AB function contributes to a maximal resistance to both linear and differential cryptanalysis. What's more, an almost Bent (AB) function is almost perfect nonlinear (APN) as well[16].

According to Leander and Poschmann's work on 4-bit S-boxes in [32], the optimal $\mathcal{U}(S)$ is 4 and $\mathcal{L}(S)$ is 8, which means no S-box under dimension 4 that is both APN and AB function. Those bijective S-boxes with optimal $\mathcal{U}(S)$ and $\mathcal{L}(S)$ are called optimal S-boxes. In addition, all optimal 4-bit S-boxes can be classified to 16 differential affine equivalence classes (please refer to Table 11 in Appendix A).

To explain above definitions more clearly, we take the S-box used in GIFT as an example depicted in Table 3. Its DDT and LAT are provided in Appendix B. As seen from Table 12 and 13, the differential uniformity of GIFT's S-box is 6 appearing in cells $(4,7)$ and $(6,3)$, and the linearity is 8. It implies that this S-box is not in any equivalence class of the optimal S-boxes.

Table 3: Specification of GIFT S-box S.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(x)$	1	10	4	12	6	15	3	9	2	13	11	7	5	0	8	E

2.2 Other important differential and linear properties of S-boxes

Besides the properties in Section 2.1, other important differential and linear properties of S-boxes are proposed recently. The number of occurrences of differential uniformity in DDT and linearity in LAT also impact the resistance against differential and linear attacks. Thus, we consider them and define them as the frequency of differential uniformity and linearity, respectively.

Definition 6 (Frequency) The frequency of differential uniformity in DDT is defined as

$$\#\mathcal{U}(S) \triangleq \#\{(\alpha,\beta)|\delta_S(\alpha,\beta) = \mathcal{U}(S), \alpha \in \mathbb{F}_2^n\backslash\{0\}, \beta \in \mathbb{F}_2^n\},$$

while the frequency of linearity in LAT is defined as

$$\#\mathcal{L}(S) \triangleq \#\{(\alpha,\beta)|\mathcal{W}_S(\alpha,\beta) = \mathcal{L}(S), \alpha \in \mathbb{F}_2^n\backslash\{0\}, \beta \in \mathbb{F}_2^n\}.$$

Furthermore, the number of BIBO patterns is also significant and we define it as follows.

Definition 7 (Bad Input and Bad Output (BIBO) pattern) If input/output difference (resp. mask) (α,β) satisfy $wt(\alpha) = wt(\beta) = 1$ and $\delta_S(\alpha,\beta) \neq 0$ (resp. $\lambda_S(\alpha,\beta) \neq 0$), we call this input/output difference (resp. mask) a *Bad Input and Bad Output* (BIBO) pattern.

It can be seen from Definition 7 that a BIBO pattern may result in a differential or linear trail with a single active S-Box. In [5,29,30], the authors proposed some schemes to overcome this case with the mathematical and structural constructions. In our paper, we denote the number of BIBO patterns in DDT as $\#\text{BIBO}_{\text{DDT}}$ and the number of BIBO patterns in LAT as $\#\text{BIBO}_{\text{LAT}}$. All BIBO patterns (α,β) in DDT (or LAT) form a subtable called *1-1 bit table*. As examples, we list the *1-1 bit tables* of GIFT's and RECTANGLE's DDT in Table 4 and Table 5, respectively. There is only 1 BIBO pattern in GIFT (e.g. $\#\text{BIBO}_{\text{DDT}} = 1$) and 2 BIBO patterns in RECTANGLE (e.g. $\#\text{BIBO}_{\text{DDT}} = 2$).

2.3 A constraint solver: STP (Simple Theorem Prover)

In recent years, automatic searching tools are widely used in cryptanalysis. One category of the automatic searches is based on the Boolean satisfiability problem (SAT) or the more general extension called satisfiability modulo theories (SMT) method. SAT is the problem of determining whether there exists an

Table 4: *1-1 bit table* of the S-box's DDT used in GIFT.

α \ β	1000	0100	0010	0001
1000	0	0	0	2
0100	0	0	0	0
0010	0	0	0	0
0001	0	0	0	0

Table 5: *1-1 bit table* of the S-box's DDT used in RECTANGLE.

α \ β	1000	0100	0010	0001
1000	0	0	0	0
0100	0	0	0	2
0010	0	0	0	0
0001	2	0	0	0

evaluation for the binary variables such that the value of the given Boolean formula equals one. An extension of the SAT problem is SMT problem, in which some of the Boolean variables are replaced by a suitable set of binary and (or) non-binary variables [41]. In most previous work, it mainly uses an SAT/SMT solver STP (Simple Theorem Prover) [24] to search for differential or linear trails [1–3, 31, 33, 38, 39, 41]. In STP, CVC formats is one of the commonly used file-based input languages. We list some CVC language references and three examples as follows. For more details, please refer to http://stp.github.io/.

Table 6: A Description for CVC Input Language [24]

Name	Symbol	Example
Concatenation	@	t1@t2@...@tm
Extraction	[i:j]	x[31:26]
Bitwise XOR	BVXOR	BVXOR(t1,t2)
Bitvector Add	BVPLUS	BVPLUS(n,t1,t2,..., tm)
Less Than Or Equal To	BVLE	BVLE(t1,t2)
Greater Than Or Equal To	BVGE	BVGE(t1,t2)
Not Equal to	\=	t1 \= t2

Example 1 Description of GIFT's S-box in CVC formats as follows.

S: ARRAY BITVECTOR(4) OF BITVECTOR(4);
//Statement: the size of the S-box is 2^4 *and each element is a* 4*-bit Boolean variable.*
ASSERT(S[0bin0000] = 0bin1100);
ASSERT(S[0bin0001] = 0bin0101);
...
//Assignment: S[0] = 12; S[1] = 5; ...

Similarly, the DDT and LAT can be described in CVC formats as well.

Example 2 "If condition" can be described in CVC formats. For example, If $a = b$ then $c = 1$ else $c = 0$.

```
a, b, c: BITVECTOR(1);
ASSERT( IF a = b THEN c = 0bin1 ELSE c = 0bin0 ENDIF );
```

Example 3 To describe $x = (a + b) \oplus c$ where $x, a, b \in \mathbb{F}_2^5$ and $c \in \mathbb{F}_2^4$.

```
x: BITVECTOR(5);
a, b: BITVECTOR(5);
c: BITVECTOR(4);
ASSERT( x = BVXOR(BVPLUS(5, a, b), 0bin0@c) );
```

Note that the parameters of BVXOR function must have the same length. So, we add 0 to the most significant bit of c.

3 New method of searching for S-boxes with good properties

From a design perspective, differential uniformity and linearity of an S-box are two primary properties to be considered. However, other properties, such as fixed point, branch number, frequency of differential uniformity, frequency of linearity, and number of BIBO patterns also affect an S-box's resistance against differential attacks and linear attacks. In our new method, we search for S-boxes by considering all of these properties above simultaneously.

For an $n \times n$ S-box, it may have some basic properties, such as it is bijective and nonlinear. In some cases, designers require an S-box without fixed point and so on [25]. In Section 3.1, we show how to describe these basic properties of an S-box as SMT problems.

In Section 3.2, we first propose how to transform the relationship between the S-box and its DDT and LAT into an SMT problem. Then, we add all requirements on the above cryptographic properties as constraints into the same model. Finally, we utilize STP to solve the model. However, it can only get a single result at one time. In order to find more solutions, we add each previous solution as a constraint to avoid the repeated solution.

3.1 Transform basic properties of an S-box into SMT problems

In this section, an n-bit S-box is denoted by $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We transform constraints on the basic properties of S-boxes into SMT problems and use CVC formats to build an STP model. We exemplify four basic properties in the following.

- **Nonlinear.** An S-box is a nonlinear function if and only if there exist two inputs x_1 and x_2 such that

$$S[x_1] \oplus S[x_2] \neq S[x_1 \oplus x_2], \quad \textit{for } \forall x_1, x_2 \in \mathbb{F}_2^n.$$

We can describe this case in the model using $(2^n \times (2^n - 1))/2$ constraints for different x_1 and x_2.

ASSERT(BVXOR(S[x_1], S[x_2]) \ = S[BVXOR(x_1, x_2)]);

– **Bijective.** For any two inputs x_1 and x_2, an S-box is bijective if and only if we have

$$S[x_1] \neq S[x_2], \quad for\ \forall x_1, x_2 \in \mathbb{F}_2^n.$$

It also needs $(2^n \times (2^n - 1))/2$ constraints to describe these equations as follows.

ASSERT(S[x_1] \ = S[x_2]);

– **Without fixed point.** For all possible input x, an S-box has no fixed point if and only if we have

$$S[x] \neq x, \quad for\ \forall x \in \mathbb{F}_2^n.$$

There are 2^n constraints for all possible inputs x.

ASSERT(S[x] \ = x);

– **Branch number.** The differential branch number of an S-box is defined as

$$DBN = \min\{wt(\alpha) + wt(\beta) | \delta_S(\alpha, \beta) \neq 0, 0 \leq \alpha, \beta < 2^n\},$$

while the linear branch number of an S-box is defined as

$$LBN = \min\{wt(\alpha) + wt(\beta) | \lambda_S(\alpha, \beta) \neq 0, 0 \leq \alpha, \beta < 2^n\}.$$

In order to add the requirements on branch number into the STP-based model, we can describe them with CVC language in the following forms:

ASSERT(DDT[α, β] = 0bin0); *//for each* $wt(\alpha) + wt(\beta) <$*DBN.*
ASSERT(LAT[α, β] = 0bin0); *//for each* $wt(\alpha) + wt(\beta) <$*LBN.*

3.2 General STP model to search for S-boxes with good properties

In this part, we first propose how to describe the relationship between an S-box and its DDT and LAT as an SMT problem.

In order to link an S-box with its DDT, we set 2^n dummy variables $IsTrue_{DDT}(\alpha, \beta, x)$ for each input/output difference pair $(\alpha, \beta), 0 \leq \alpha, \beta, x < 2^n$ as follows:

$$IsTrue_{DDT}(\alpha, \beta, x) = \begin{cases} 1, & \textit{if } S(x \oplus \alpha) = S(x) \oplus \beta, \\ 0, & \textit{others.} \end{cases} \tag{2}$$

Each variable aims to record whether an input pair $(x, x \oplus \alpha)$ contributes to item $\delta_s(\alpha, \beta)$ in DDT. By exhausting all possible input x, we can link an S-box and its DDT by

$$\delta_s(\alpha, \beta) = \sum_{x=0}^{2^n-1} IsTrue_{DDT}(\alpha, \beta, x). \tag{3}$$

Equations (2) and (3) can be described as CVC input language as the following forms:

```
ASSERT( IF BVPLUS(S[x], β) = S[BVPLUS( x, α)] THEN
        IsTrue[α, β, x] = 0bin0 ELSE IsTrue[α, β, x] = 0bin1 ENDIF );
ASSERT( DDT[α, β] = BVPLUS( n, IsTrue[α, β, 0], IsTrue[α, β, 1], ··· ) );
```

As mentioned before, the properties of an S-box considered in this paper are $\mathcal{U}(S)$, $\mathcal{L}(S)$, $\#\mathcal{U}(S)$, $\#\mathcal{L}(S)$, $\#\text{BIBO}_{\text{DDT}}$ and $\#\text{BIBO}_{\text{LAT}}$. So, when designers confirm requirements on these properties, we can describe them as constraints in our model.

Firstly, for any $\alpha, \beta < 2^n$,the requirements on differential uniformity $\mathcal{U}(S)$ and linearity $\mathcal{L}(S)$ can be added into our model as:

$$\delta_S(\alpha, \beta) \leq \mathcal{U}(S),$$

$$\lambda_S(\alpha, \beta) \leq \mathcal{L}(S).$$

Note that $\mathcal{U}(S)$ and $\mathcal{L}(S)$ are variables predetermined by designers.

Secondly, some S-boxes of well-known lightweight ciphers like PRESENT, GIFT and RECTANGLE are designed by considering the number of BIBO patterns. We set new dummy variables $IsTrue^{DDT}_{BIBO}(\alpha, \beta)$ as follows where both hamming weight of α and β are 1.

$$IsTrue^{DDT}_{BIBO}(\alpha, \beta) = \begin{cases} 1, & \textit{if } \delta_S(\alpha, \beta) \neq 0 \\ 0, & \textit{others.} \end{cases} \tag{4}$$

This equation describes whether an input/output difference pair (α, β) is a BIBO pattern. Furthermore, we can calculate the number of BIBO patterns in a DDT according to Equation (5).

$$\#\text{BIBO}_{\text{DDT}} = \sum_{wt(\alpha)=wt(\beta)=1} IsTrue^{DDT}_{BIBO}(\alpha, \beta) \tag{5}$$

Similarly, we can calculate the number of BIBO patterns in a LAT by using variables $IsTrue^{LAT}_{BIBO}(\alpha,\beta)$ and $\#\mathrm{BIBO}_{\mathrm{LAT}}$. These constraints according to Equations (4) and (5) can be described in STP-based model as following forms:

ASSERT(*IF* DDT$[\alpha,\beta]$ = 0bin0 *THEN*
BIBO$[\alpha,\beta]$ = 0bin0 *ELSE* BIBO$[\alpha,\beta]$ = 0bin1 *ENDIF*);
ASSERT(#BIBO = *BVPLUS*(n, BIBO$[\alpha_1,\beta_1]$, BIBO$[\alpha_2,\beta_2]$, $\cdots$));

When considering the frequeny of differential uniformity, we set dummy variables $IsTrue^{DDT}_{Freq}(\alpha,\beta)$ with $(\alpha,\beta)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$ as follows:

$$IsTrue^{DDT}_{Freq}(\alpha,\beta)=\begin{cases}1, & if\ \delta_S(\alpha,\beta)=\mathcal{U}(S)\\ 0, & others.\end{cases} \tag{6}$$

We can calculate the frequency of differential uniformity $\#\mathcal{U}(S)$ by the following equation.

$$\#\mathcal{U}(S)=\sum_{\beta=0}^{2^n-1}\sum_{\alpha=0}^{2^n-1}IsTrue^{DDT}_{Freq}(\alpha,\beta). \tag{7}$$

Meanwhile, the frequency of linearity can be described by setting the variables $IsTrue^{LAT}_{Freq}(\alpha,\beta)$ and $\#\mathcal{U}(S)$. These constraints on frequency can be described in STP-basd model as CVC formats:

ASSERT(*IF* DDT$[\alpha,\beta]=\mathcal{U}(S)$ *THEN*
Freq$[\alpha,\beta]$ = 0bin0 *ELSE* Freq$[\alpha,\beta]$ = 0bin1 *ENDIF*);
ASSERT(#Freq = BVPLUS(n, Freq$[\alpha_1,\beta_1]$, Freq$[\alpha_2,\beta_2]$, $\cdots$));

All in all, we can combine all constraints on $\mathcal{U}(S)$, $\mathcal{L}(S)$, $\#\mathcal{U}(S)$, $\#\mathcal{L}(S)$, $\#\mathrm{BIBO}_{\mathrm{DDT}}$ and $\#\mathrm{BIBO}_{\mathrm{LAT}}$ together in our model. After assigning predetermined values to them, we can find out expected S-boxes by STP.

According to Proposition 1, there are many S-boxes mapping to the same DDT, which means there are many solutions for such an STP-based model. To get multiple solutions, once we get a new S-box $S_1(x)$, we remove it out of the solution space by

$$(S(0)\neq S_1(0))\ OR\ (S(1)\neq S_1(1))\ OR\ \cdots\ OR\ (S(2^n-1)\neq S_1(2^n-1)). \tag{8}$$

Equation (8) can be transformed into CVC formats as:

ASSERT((S[0]$\neq$S$_1$[0]) *OR*(S[1]$\neq$S$_1$[1]) *OR*$\cdots$ *OR*(S[2^n-1]$\neq$S$_1$[2^n-1]));

Please note $S_1[x]$ represents previous solution and it is described as a set of constant values in our model.

4 Applications on 4-bit and 5-bit S-boxes

There are two scenarios for applying the new model in Section 3. In the first case, when given some differential and linear properties of an S-box without knowing the whole DDT or LAT, we can use our model to search for expected 4-bit and 5-bit S-boxes directly in Section 4.1 and 4.2. The other case is to search for (reconstruct) S-boxes while we know the DDT or LAT. We simplify the model and replace the constraints on properties with specific DDT or LAT in Section 4.3. As applications, we list the number of S-boxes without fixed points that have the same DDT as PRESENT and KECCAK separately.

4.1 Searching for 4-bit S-boxes

In the design process, designers usually search for an S-box according to the security requirements. In most previous work, differential uniformity and linearity are two primary properties considered when designing a new S-box. However, the frequency of differential uniformity and linearity in DDT and LAT also impacts resistance against multiple differential attacks and linear hull attacks, respectively. More importantly, the frequency of differential uniformity (linearity) in the DDT (LAT) provides a more accurate estimation of the maximum expected differential (linear hull) probability than that provided merely by the differential uniformity. Furthermore, the existence of BIBO patterns will lead to the single active bit path. So, the number of BIBO patterns should be as low as possible.

When considering all above properties, we apply our model to finding new 4-bit S-boxes, which have the same cryptographic properties as current well-known 4-bit S-boxes used in PRESENT, GIFT, and RECTANGLE. We first summarize the cryptographic properties of target S-boxes on differential uniformity, linearity, frequency of differential uniformity, frequency of linearity, and number of BIBO patterns, then assign them to constraint variables in our model to search for S-boxes. For instance, the values of these properties in PRESENT are $\mathcal{U}(S) = 4$, $\mathcal{L}(S) = 8$, $\#\mathcal{U}(S) = 24$, $\#\mathcal{L}(S) = 4$, $\#\text{BIBO}_{\text{DDT}} = 0$ and $\#\text{BIBO}_{\text{LAT}} = 8$, respectively. In the end, we found out 3723/947/620 S-boxes with the same cryptographic properties as PRESENT/GIFT/RECTANGLE's S-boxes within 6 hours. Here, we name these S-boxes as PRESENT/GIFT/RECTANGLE-like S-boxes. The number of S-boxes are summarized in Table 1 and some example S-boxes are shown in Table 7.

In addition, the designers of GIFT select an S-box with $\mathcal{U}(S) = 6$, $\mathcal{L}(S) = 8$, $\#\text{BIBO}_{\text{DDT}} = 1$ and $\#\text{BIBO}_{\text{LAT}} = 3$. As mentioned in section 2.1, this S-box is not in any equivalence class of the optimal S-boxes. However, with a trade-off between differential uniformity and number of BIBO patterns, the whole cipher also has strong resistance against differential attacks. So it is significant to search for new S-boxes with a lower $\#\text{BIBO}_{\text{DDT}}$ at the cost of a higher differential uniformity. These new S-boxes in Table 1 have $\mathcal{U}(S) = 8$ and $\mathcal{L}(S) = 8$, but their total number of BIBO patterns in DDT and LAT is

only 3. Compared with GIFT, they have a lower number of BIBO patterns at the cost of a higher differential uniformity.

Interestingly, we get an observation from the searching results:

Observation 1 *If we pre-determine an optimal S-box with* $\mathcal{U}(S) = 4$, $\mathcal{L}(S) = 8$, *and* $\#BIBO_{DDT} = 0$, *its total number of BIBO patterns existed in DDT and LAT must satisfy*

$$\#BIBO_{DDT} + \#BIBO_{LAT} = \#BIBO_{LAT} > 3.$$

This observation explains that a lower total number of BIBO patterns may be at the cost of higher differential uniformity or linearity.

Table 7: Some PRESENT/GIFT/RECTANGLE-like S-boxes and the new S-box. (*-like S-boxes have the same $\mathcal{U}(S)$, $\mathcal{L}(S)$, $\#\mathcal{U}(S)$, $\#\mathcal{L}(S)$, $\#\text{BIBO}_{\text{DDT}}$ and $\#\text{BIBO}_{\text{LAT}}$ as *.)

	#BIBO	**S(x)**
PRESENT-like S-boxes	4	5,11,8,14,9,2,7,4,3,12,13,1,6,14,0,10
		12,7,1,13,10,0,15,3,5,2,14,8,6,11,9,4
		14,11,0,12,3,6,9,15,2,4,13,7,5,8,10,1
GIFT-like S-boxes	4	15,9,1,2,8,6,7,12,10,4,13,14,3,5,0,11
		2,12,1,7,5,11,8,14,15,10,13,0,9,4,6,3
		15,3,8,4,2,12,1,11,9,0,6,13,5,14,10,7
RECTANGLE-like S-boxes	4	5,13,10,0,11,6,12,3,2,14,1,7,4,9,15,8
		15,2,6,8,1,4,13,11,9,12,0,7,14,3,10,5
		5,2,13,8,6,11,3,4,0,15,14,1,9,12,10,7
New S-box_1	3	5,2,6,8,9,15,12,3,0,13,11,7,14,10,1,4

4.2 Searching for 5-bit S-boxes

Similar to 4-bit S-boxes, we also apply our model to searching for 5-bit S-boxes. The S-boxes' cryptographic properties used in two famous ciphers – KECCAK and ASCON are listed in Table 2. Firstly, we assign them to constraint variables in our model. We found out only 31 and 28 KECCAK-like and ASCON-like S-boxes within 6 hours, respectively.

Furthermore, we also search out some new S-boxes with a trade-off between differential uniformity and its frequency of differential uniformity. We list the properties of these new S-boxes in Table 2. Compared with ASCON, they have lower differential uniformity ($\mathcal{U}(S) = 6$) at the cost of higher frequency of differential uniformity ($\#\mathcal{U}(S) = 24$). In Table 8, we list some examples of KECCAK-like, ASCON-like, and new S-boxes.

Table 8: KECCAK-like, ASCON-like 5-bit S-boxes and the new S-box

	#BIBO	S(x)
KECCAK-like S-boxes	10	23,24,3,14,20,9,30,19,10,17,28,2,11,5,4,29, 8,12,21,6,13,18,1,27,25,22,16,15,0,7,31,26
		12,5,21,14,3,20,30,15,22,1,9,27,26,0,23,28, 24,18,19,11,29,2,8,17,6,31,13,16,7,25,4,10
		22,30,21,25,11,20,31,2,26,5,12,29,4,8,6,7,1, 0,3,13,28,14,16,27,19,10,15,18,24,23,9,17
ASCON-like S-boxes	0	24,9,27,6,3,31,22,1,20,30,8,5,10,21,15,16,4, 19,23,12,28,0,13,26,7,11,25,18,17,14,2,29
		23,28,15,16,2,1,21,30,25,19,18,12,11,8,13, 6,24,14,0,3,5,29,10,27,4,7,31,9,26,22,20,17
		3,13,26,22,17,2,15,21,0,23,12,9,20,25,30, 10,27,14,4,29,28,8,1,18,7,24,16,19,31,6,11,5
New S-box$_2$	0	22,15,16,9,27,3,5,6,1,21,30,18,28,8,10,29, 14,0,13,26,24,20,17,31,19,12,7,25,11,23,4,2

4.3 Reconstruct S-boxes from a given DDT

If we know the complete DDT or LAT, we can simplify our model and replace all constraints on properties with the specific value of DDT or LAT.

For example, if we want to know how many S-boxes without fixed points have the same DDT as PRESENT's S-box, we can transform the relationship between S-box and PRESENT's DDT into an SMT problem. Then, we describe the property of no fixed point as constraint. By using STP, we get the solutions:

- **For 4-Bit S-boxes.** We take the PRESENT's S-box as an example. There are a total of 2^8 different 4-bit S-boxes corresponding to PRESENT's DDT, which are summarized in Table 9. It also verifies the Proposition 1 by experiments. We spent 10 minutes finding all these 256 S-boxes[1] and there are 96 S-boxes left when we add the constraint of no fixed point.

Table 9: The result of the experiments on 4-bit S-boxes

#S-boxes	#S-boxes without fixed point	Percentage	Time
256	96	37.5%	10 mins
With fixed point	10,13,6,11,4,7,1,2,3,14,9,0,15,8,12,5		
	13,14,8,11,10,7,6,1,0,9,3,4,5,12,15,2		
	12,11,10,7,6,5,3,0,15,2,1,8,9,14,4,13		
Without fixed point	10,13,9,0,6,11,12,5,1,2,4,7,15,8,3,14		
	11,8,14,13,1,6,7,10,4,3,9,0,2,15,12,5		
	13,14,8,11,3,4,15,2,6,1,5,12,10,7,0,9		

- **For 5-Bit S-boxes.** The time spent in finding 5-bit S-box's DDT is much more than 4-bit one. As can be seen from Table 10, we found all 1024

[1] All experiments in our paper are implemented in the AMD EPYC 7302 CPU @ 3.0 GHz with eight threads.

S-boxes with the same DDT as KECCAK's S-box in 7.5 hours, and 672 S-boxes have no fixed point. It also verifies the Proposition 1 by experiments.

Table 10: The result of the experiments on 5-bit S-boxes

#S-boxes	#S-boxes without fixed point	Percentage	Time
1024	672	65.6%	7.5 hours
With fixed point	17,18,23,16,13,14,3,4,9,10,15,8,5,6,11,12, 1,0,7,2,29,28,19,22,24,25,30,27,20,21,26,31		
	18,21,16,19,22,17,28,31,10,13,8,11,30,25,20, 23,1,4,3,2,5,0,15,14,24,29,26,27,12,9,6,7		
	4,5,6,3,24,25,18,23,29,28,31,26,17,16,27,30, 22,21,20,19,10,9,0,7,14,13,12,11,2,1,8,15		
Without fixed point	29,24,19,18,9,12,15,14,20,17,26,27,16,21, 22,23,13,10,3,0,25,30,31,28,5,2,11,8,1,6,7,4		
	11,10,5,0,23,22,17,20,2,3,12,9,14,15,8,13, 27,24,21,18,7,4,1,6,19,16,29,26,31,28,25,30		
	16,17,22,19,28,29,18,23,9,8,15,10,21,20,27, 30,1,2,7,0,13,14,3,4,25,26,31,24,5,6,11,12		

5 Verify a Conjecture about trivial DDT-equivalence proposed by Boura et al.

When we find an S-box with good cryptographic properties, we can generate new S-boxes through some equivalent transformations to keep these properties. For example, two S-boxes in the same affine equivalence class have the same differential uniformity and even the whole differential spectrum [6]. So, it is significant to theoretical research the S-boxes in some equivalence classes.

In the paper [14], the authors give a conjecture on the DDT-equivalence classes.

Conjecture 1 [14] The DDT-equivalence class of an S-box S, such that the rows in its DDT are pairwise distinct, only contains S-boxes of the form $S(x \oplus c) \oplus d$, with $c, d \in \mathbb{F}_2^n$ (i.e. is trivial).

To verify the conjecture, one method is to traverse all the S-boxes and classify them according to the same DDT, and then verify whether there exist two non-trivially DDT-equivalent S-boxes in the same class. However, the search space is too large to traverse all the S-boxes and classify them, even though the size of S-boxes is 4-bit.

We give a proposition and two corollaries as follows to reduce the search space. We first classify all n-bit S-boxes into affine equivalence classes.

Proposition 2 *(adapted from [14]) Let F and G be two functions which are affine equivalent, i.e., there exist two affine functions A_0 and A_1, where A_1 and A_2 are bijective such that $G = A_2 \circ F \circ A_1$. Then, the DDT-equivalence classes of F and of G have the same size. Moreover, the class of G is composed of all $A_2 \circ F' \circ A_1$ where F' varies in the class of F.*

Proof Let L_0 and L_1 denote the linear parts of the affine functions A_0 and A_1. It is well-known that the DDT of F amd G are related by

$$\delta_G(a,b) = \delta_F(L_1(a), L_2^{-1}(b)), \forall (a,b) \tag{9}$$

This comes from the fact that

$$\begin{aligned} \Delta_a G(x) &= A_2[F(A_1(x \oplus a))] \oplus A_2[F(A_1(x))], \\ &= L_2[F(A_1(x) \oplus L_1(a)) \oplus F(A_1(x))], \\ &= L_2[\Delta_{L_1(a)} F(A_1(x))]. \end{aligned}$$

Let $F' \in \mathscr{C}_{DDT}F$ be an element in the DDT-equivalence class of F and let us consider $G' = A_2 \circ F' \circ A_1$. Then, the DDT of F' and G' satisfy: for all (a,b)

$$\delta_{G'}(a,b) = \delta_{F'}(L_1(a), L_2^{-1}(b)) = \delta_F(L_1(a), L_2^{-1}(b)),$$

where the last equality comes from the fact F and F' have the same DDT. Then, we deduce from Equation (9) that $\delta_{G'}(a,b) = \delta_G(a,b)$ for all (a,b). It follows that

$$G' = A_2 \circ F' \circ A_1,\ F' \in \mathscr{C}_{DDT}F \subseteq \mathscr{C}_{DDT}G.$$

By exchanging the roles of F and G, we deduce that both sets coincide. □

According to Proposition 2, the DDT-equivalence classes of the S-boxes in an affine equivalence class have the same size.

Corollary 1 *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a single representative S-box of an affine equivalence class $\mathscr{A}_S$. If its DDT has the same rows, then the DDT of any S-box in $\mathscr{A}_S$ has the same rows.*

Proof Let L_0 and L_1 denote the linear parts of the affine functions A_0 and A_1. F and G are affine equivalent functions and $G = A_2 \circ F \circ A_1$. From Proposition 2, we know that

$$\delta_G(a,b) = \delta_F(L_1(a), L_2^{-1}(b)), \forall (a,b) \tag{10}$$

Assume that two rows a_1 and a_2 are the same in the DDT of G, then two rows $L_1(a)$ and $L_2(a)$ are the same in the DDT of F. □

In other words, from Corollary 1, we do not need to verify the representative S-box, whose DDT is same in two rows, of an affine class.

Corollary 2 *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a single representative S-box of an affine equivalence class $\mathscr{A}_S$. If the DDT-equivalence class $\mathscr{C}_S$ of S is trivial, then the DDT-equivalence classes of all S-boxes in $\mathscr{A}_S$ are trivial.*

Proof From Proposition 1, the DDT-equivalence class $\mathscr{C}_S$ of S is trivial if and only if it contains 2^{2n-l} elements. Then the DDT-equivalence classes $\mathscr{C}_{S'}$ of all S-boxes S' in $\mathscr{A}_S$ contains 2^{2n-l} elements too (i.e. are trivial). □

From Corollary 2, if the representative S-box of an affine equivalence class only has trivially DDT-equivalent S-boxes, then all S-boxes in this affine equivalence class also only have trivially DDT-equivalent S-boxes.

In a summary, to verify the conjecture, it is sufficient to traverse a special set of S-boxes. Any element in this set is a single representative S-box of an affine equivalence class and its DDT is pairwise distinct in any two rows. Then, if all these S-boxes in this set only have trivially DDT-equivalent S-boxes, the conjecture is correct.

Extended Model. We extend the model in Section 3 to verify the conjecture. This model can verify whether there exists any S-box $S_2(x)$ that is non-trivially DDT-equivalent to a given S-box $S_1(x)$. We launch it by STP, if it returns that there does not exist an S-box $S_2(x)$, then all S-boxes in the affine equivalence class $\mathscr{A}_S$ only have trivially DDT-equivalent S-boxes.

We build this model as follows. Firstly, we transform the relationship between two S-boxes $S_1(x)$, $S_2(x)$ and their same DDT into SMT problem as Section 3.2, respectively.

Then, we add the constraint that $S_1(x)$ and $S_2(x)$ are non-trivially DDT-equivalent as follows. For any $c, d \in \mathbb{F}_2^n$, there exist an $x \in \mathbb{F}_2^n$ such that

$$S_1(x) \neq S_2(x \oplus c) \oplus d.$$

To implement this inequation by STP, we must exhaust c and d. We can describe this inequation as CVC formats:

```
c, d: BITVECTOR(n);
ASSERT( S1[0] ≠ S2[0 ⊕ c] ⊕ d OR
        S1[1] ≠ S2[1 ⊕ c] ⊕ d OR
        ··· OR
        S1[2^n − 1] ≠ S2[2^n − 1 ⊕ c] ⊕ d
```

Finally, we assign the value of an S-box $S(x)$ to $S_1(x)$.

```
ASSERT( (S1[0] = S[0]) AND ··· AND (S1[2^n − 1]) = S[2^n − 1]) );
```

Experimentally, we traverse all S-boxes in a special set where any S-box is a single representative of an affine equivalence class and its DDT is pairwise distinct in any two rows. Then we assign their values to $S_1(x)$ in our model to verify the conjecture.

Experimental result. We efficiently verify the correctness of the conjecture for all 3-bit S-boxes by using our model in a few minutes.

There are a total of 302 affine equivalence classes for all 4-bit S-boxes (Table 5.2-5.8 in [21]). Note that, for 4-bit S-boxes, a linear structure is one input difference to 16 same output differences. We classify their representative S-boxes into two sets as follows.

The DDT of any S-box in this set does not have the same rows. There are a total of 259 S-boxes in this set. We further classify them according to whether they have a linear structure.

[a] 253 S-boxes do not have linear structure except the input difference 0. We verify that the size of their DDT-equivalence classes are 2^8 (i.e. are trivial).

[b] The representative S-boxes of classes 293, 294, 296, 299, and 300 have only 1 linear structure except the input difference 0. We verify that the size of their DDT-equivalence classes are 2^7 (i.e. are trivial).

[c] The representative S-box of class 302 is the identity function and it has 15 linear structures except the input difference 0. The dimension of its linear space is $l = 4$. We verify that the size of its DDT-equivalence class is 2^4 (i.e. is trivial).

Up to here, we already verify that the conjecture is correct for all 4-bit S-boxes.

The DDT of any S-box in this set has the same rows. For completeness, there are a total of 43 S-boxes in this set, even though we do not need to verify this set. We list their class number in Table 14. The classes 295, 297, 298, and 301 have linear structures except the input difference 0.

[a] The representative S-boxes of classes 276, 277, and 287 do not have linear structure except the input difference 0. We verify that the size of their DDT-equivalence classes are 2×2^8 (i.e. are non-trivial).

[b] The representative S-box of class 289 does not have linear structure except the input difference 0. We verify that the size of its DDT-equivalence class is 4×2^8 (i.e. is non-trivial).

[c] The representative S-boxes of classes 295, 297, and 298 have only 1 linear structure except the input difference 0. The dimensions of their linear spaces are $l = 1$. We verify that the size of their DDT-equivalence classes are 2^7 (i.e. are trivial).

[d] The representative S-box of class 301 has 3 linear structures except the input difference 0. The dimension of its linear space is $l = 2$. We verify that the size of their DDT-equivalence classes are 2^6 (i.e. is trivial).

[e] The representative S-boxes of other 35 classes do not have linear structure except the input difference 0. We verify that the size of their DDT-equivalence classes are 2^8 (i.e. are trivial).

6 Conclusion and future works

This paper proposes a new method to search for S-boxes by considering many cryptographic properties simultaneously, such as fix points, branch number, differential uniformity, linearity, the frequency of differential uniformity (linearity) and the number of BIBO patterns. We search out many 4-bit and 5-bit S-boxes and compare them with some well-known ciphers. Our work provid new insights on the design of S-boxes. We can trade off multiple properties to achieve good resistance against differential and linear attacks rather than

focusing on the optimal S-box with the lowest differential uniformity and linearity.

Furthermore, what our method can do is far more than examples in this paper. Boomerang Connectivity Table (BCT) [19] and Differential-Linear Connectivity Table (DLCT) [8] can also be modeled like our method, and other cryptographic properties related to DDT and LAT can also be added to our model, such as the whole differential spectrum and Walsh spectrum.

On the other hand, some SAT-based works can optimize the implementation of an S-box [12,34,40]. We can combine our method with them to build a SAT-based tool for designing an S-box with good cryptographic properties and efficient hardware implementation.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 62032014, 61902100, 62002201), the National Key Research and Development Program of China (Grant No. 2018YFA0704702), the Major Basic Research Project of Natural Science Foundation of Shandong Province, China (Grant No. ZR202010220025).

References

1. Ankele, R., Kölbl, S.: Mind the gap - A closer look at the security of block ciphers against differential cryptanalysis. In: C. Cid, M.J.J. Jr. (eds.) Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 11349, pp. 163–190. Springer (2018). DOI 10.1007/978-3-030-10970-7_8. URL https://doi.org/10.1007/978-3-030-10970-7_8
2. Aumasson, J., Jovanovic, P., Neves, S.: Analysis of NORX: investigating differential and rotational properties. In: D.F. Aranha, A. Menezes (eds.) Progress in Cryptology - LATINCRYPT 2014 - Third International Conference on Cryptology and Information Security in Latin America, Florianópolis, Brazil, September 17-19, 2014, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 8895, pp. 306–324. Springer (2014). DOI 10.1007/978-3-319-16295-9_17. URL https://doi.org/10.1007/978-3-319-16295-9_17
3. Azimi, S.A., Ranea, A., Salmasizadeh, M., Mohajeri, J., Aref, M.R., Rijmen, V.: A bit-vector differential model for the modular addition by a constant. In: S. Moriai, H. Wang (eds.) Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I, *Lecture Notes in Computer Science*, vol. 12491, pp. 385–414. Springer (2020). DOI 10.1007/978-3-030-64837-4_13. URL https://doi.org/10.1007/978-3-030-64837-4_13
4. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: T. Iwata, J.H. Cheon (eds.) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 9453, pp. 411–436. Springer (2015). DOI 10.1007/978-3-662-48800-3_17. URL https://doi.org/10.1007/978-3-662-48800-3_17
5. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In: W. Fischer, N. Homma (eds.) Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, *Lecture Notes in Computer Science*, vol. 10529, pp. 321–345. Springer (2017). DOI 10.1007/978-3-319-66787-4_16. URL https://doi.org/10.1007/978-3-319-66787-4_16

6. Bao, Z., Guo, J., Ling, S., Sasaki, Y.: PEIGEN - a platform for evaluation, implementation, and generation of s-boxes. IACR Trans. Symmetric Cryptol. **2019**(1), 330–394 (2019). DOI 10.13154/tosc.v2019.i1.330-394. URL https://doi.org/10.13154/tosc.v2019.i1.330-394
7. Bar-On, A., Biham, E., Dunkelman, O., Keller, N.: Efficient slide attacks. J. Cryptol. **31**(3), 641–670 (2018). DOI 10.1007/s00145-017-9266-8. URL https://doi.org/10.1007/s00145-017-9266-8
8. Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis. In: Y. Ishai, V. Rijmen (eds.) Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I, *Lecture Notes in Computer Science*, vol. 11476, pp. 313–342. Springer (2019). DOI 10.1007/978-3-030-17653-2_11. URL https://doi.org/10.1007/978-3-030-17653-2_11
9. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: M. Robshaw, J. Katz (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 9815, pp. 123–153. Springer (2016). DOI 10.1007/978-3-662-53008-5_5. URL https://doi.org/10.1007/978-3-662-53008-5_5
10. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: The keccak sha-3 submission. Submission to NIST (Round 3) **6**(7), 16 (2011)
11. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993). DOI 10.1007/978-1-4613-9314-6. URL https://doi.org/10.1007/978-1-4613-9314-6
12. Bilgin, B., Meyer, L.D., Duval, S., Levi, I., Standaert, F.: Low AND depth and efficient inverses: a guide on s-boxes for low-latency masking. IACR Trans. Symmetric Cryptol. **2020**(1), 144–184 (2020). DOI 10.13154/tosc.v2020.i1.144-184. URL https://doi.org/10.13154/tosc.v2020.i1.144-184
13. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: P. Paillier, I. Verbauwhede (eds.) Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, *Lecture Notes in Computer Science*, vol. 4727, pp. 450–466. Springer (2007). DOI 10.1007/978-3-540-74735-2_31. URL https://doi.org/10.1007/978-3-540-74735-2_31
14. Boura, C., Canteaut, A., Jean, J., Suder, V.: Two notions of differential equivalence on sboxes. Des. Codes Cryptogr. **87**(2-3), 185–202 (2019). DOI 10.1007/s10623-018-0496-z. URL https://doi.org/10.1007/s10623-018-0496-z
15. Browning, K., Dillon, J., McQuistan, M., Wolfe, A.: An apn permutation in dimension six. Finite Fields: theory and applications **518**, 33–42 (2010)
16. Calderini, M., Budaghyan, L., Carlet, C.: On known constructions of apn and ab functions and their relation to each other (2020)
17. Carlet, C.: Open questions on nonlinearity and on APN functions. In: Ç.K. Koç, S. Mesnager, E. Savas (eds.) Arithmetic of Finite Fields - 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 9061, pp. 83–107. Springer (2014). DOI 10.1007/978-3-319-16277-5_5. URL https://doi.org/10.1007/978-3-319-16277-5_5
18. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: A.D. Santis (ed.) Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings, *Lecture Notes in Computer Science*, vol. 950, pp. 356–365. Springer (1994). DOI 10.1007/BFb0053450. URL https://doi.org/10.1007/BFb0053450
19. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: J.B. Nielsen, V. Rijmen (eds.) Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 10821, pp. 683–714. Springer (2018). DOI 10.1007/978-3-319-78375-8_22. URL https://doi.org/10.1007/978-3-319-78375-8_22

20. Daemen, J., Rijmen, V.: The design of Rijndael, vol. 2. Springer (2002)
21. De Cannière, C.: Analysis and design of symmetric encryption algorithms. Doctoral Dissertaion, KULeuven (2007)
22. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon. Submission to the CAESAR competition: http://ascon. iaik. tugraz. at (2014)
23. Dunkelman, O., Huang, S.: Reconstructing an s-box from its difference distribution table. IACR Trans. Symmetric Cryptol. **2019**(2), 193–217 (2019). DOI 10.13154/tosc.v2019.i2.193-217. URL https://doi.org/10.13154/tosc.v2019.i2.193-217
24. Ganesh, V., Dill, D.L.: http://stp.github.io/ (2007)
25. Guo, J., Jean, J., Nikolic, I., Qiao, K., Sasaki, Y., Sim, S.M.: Invariant subspace attack against midori64 and the resistance criteria for s-box designs. IACR Trans. Symmetric Cryptol. **2016**(1), 33–56 (2016). DOI 10.13154/tosc.v2016.i1.33-56. URL https://doi.org/10.13154/tosc.v2016.i1.33-56
26. Isa, H., Jamil, N., Z'aba, M.: Hybrid heuristic methods in constructing cryptographically strong s-boxes. Int. J. Cryptol. Res **6**(1), 1–15 (2016)
27. Ivanov, G., Nikolov, N., Nikova, S.: Cryptographically strong s-boxes generated by modified immune algorithm. In: E. Pasalic, L.R. Knudsen (eds.) Cryptography and Information Security in the Balkans - Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 9540, pp. 31–42. Springer (2015). DOI 10.1007/978-3-319-29172-7_3. URL https://doi.org/10.1007/978-3-319-29172-7_3
28. Ivanov, G., Nikolov, N., Nikova, S.: Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptography and Communications **8**(2), 247–276 (2016)
29. Kim, H., Jeon, Y., Kim, G., Kim, J., Sim, B., Han, D., Seo, H., Kim, S., Hong, S., Sung, J., Hong, D.: A new method for designing lightweight s-boxes with high differential and linear branch numbers, and its application. IACR Cryptol. ePrint Arch. **2020**, 1582 (2020). URL https://eprint.iacr.org/2020/1582
30. Kim, S.G., Hong, D., Sung, J., Hong, S.: Classification of 4-bit s-boxes for BOGI permutation. IEEE Access **8**, 210935–210949 (2020). DOI 10.1109/ACCESS.2020.3039273. URL https://doi.org/10.1109/ACCESS.2020.3039273
31. Kölbl, S., Leander, G., Tiessen, T.: Observations on the SIMON block cipher family. In: R. Gennaro, M. Robshaw (eds.) Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, *Lecture Notes in Computer Science*, vol. 9215, pp. 161–185. Springer (2015). DOI 10.1007/978-3-662-47989-6_8. URL https://doi.org/10.1007/978-3-662-47989-6_8
32. Leander, G., Poschmann, A.: On the classification of 4 bit s-boxes. In: C. Carlet, B. Sunar (eds.) Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings, *Lecture Notes in Computer Science*, vol. 4547, pp. 159–176. Springer (2007). DOI 10.1007/978-3-540-73074-3_13. URL https://doi.org/10.1007/978-3-540-73074-3_13
33. Liu, Y., Liang, H., Li, M., Huang, L., Hu, K., Yang, C., Wang, M.: STP models of optimal differential and linear trail for s-box based ciphers. IACR Cryptol. ePrint Arch. **2019**, 25 (2019). URL https://eprint.iacr.org/2019/025
34. Lu, Z., Wang, W., Hu, K., Fan, Y., Wu, L., Wang, M.: Pushing the limits: Searching for implementations with the smallest area for lightweight s-boxes. In: A. Adhikari, R. Küsters, B. Preneel (eds.) Progress in Cryptology - INDOCRYPT 2021 - 22nd International Conference on Cryptology in India, Jaipur, India, December 12-15, 2021, Proceedings, *Lecture Notes in Computer Science*, vol. 13143, pp. 159–178. Springer (2021). DOI 10.1007/978-3-030-92518-5_8. URL https://doi.org/10.1007/978-3-030-92518-5_8
35. Matsui, M.: Linear cryptanalysis method for DES cipher. In: T. Helleseth (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings, *Lecture Notes in Computer Science*, vol. 765, pp. 386–397. Springer (1993). DOI 10.1007/3-540-48285-7_33. URL https://doi.org/10.1007/3-540-48285-7_33
36. Nyberg, K.: Differentially uniform mappings for cryptography. In: T. Helleseth (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings, *Lecture*

Notes in Computer Science, vol. 765, pp. 55–64. Springer (1993). DOI 10.1007/3-540-48285-7_6. URL https://doi.org/10.1007/3-540-48285-7_6

37. Perrin, L.: Cryptanalysis, reverse-engineering and design of symmetric cryptographic algorithms (2017)
38. Ranea, A., Liu, Y., Ashur, T.: An easy-to-use tool for rotational-xor cryptanalysis of ARX block ciphers. IACR Cryptol. ePrint Arch. **2020**, 727 (2020). URL https://eprint.iacr.org/2020/727
39. Song, L., Huang, Z., Yang, Q.: Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In: J.K. Liu, R. Steinfeld (eds.) Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II, *Lecture Notes in Computer Science*, vol. 9723, pp. 379–394. Springer (2016). DOI 10.1007/978-3-319-40367-0_24. URL https://doi.org/10.1007/978-3-319-40367-0_24
40. Stoffelen, K.: Optimizing s-box implementations for several criteria using SAT solvers. In: T. Peyrin (ed.) Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 9783, pp. 140–160. Springer (2016). DOI 10.1007/978-3-662-52993-5_8. URL https://doi.org/10.1007/978-3-662-52993-5_8
41. Sun, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the SAT method. IACR Trans. Symmetric Cryptol. **2021**(1), 269–315 (2021). DOI 10.46586/tosc.v2021.i1.269-315. URL https://doi.org/10.46586/tosc.v2021.i1.269-315
42. Wang, Y., Zhang, Z., Zhang, L.Y., Feng, J., Gao, J., Lei, P.: A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Information Sciences **523**, 152–166 (2020)
43. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Sci. China Inf. Sci. **58**(12), 1–15 (2015). DOI 10.1007/s11432-015-5459-7. URL https://doi.org/10.1007/s11432-015-5459-7

A Representatives for all 16 classes of optimal 4-bit S-boxes

Table 11: Representatives for all 16 classes of optimal 4 bit S-boxes

G_0	0,1,2,13,4,7,15,6,8,11,12,9,3,14,10,5
G_1	0,1,2,13,4,7,15,6,8,11,14,3,5,9,10,12
G_2	0,1,2,13,4,7,15,6,8,11,14,3,10,12,5,9
G_3	0,1,2,13,4,7,15,6,8,12,5,3,10,14,11,9
G_4	0,1,2,13,4,7,15,6,8,12,9,11,10,14,5,3
G_5	0,1,2,13,4,7,15,6,8,12,11,9,10,14,3,5
G_6	0,1,2,13,4,7,15,6,8,12,11,9,10,14,5,3
G_7	0,1,2,13,4,7,15,6,8,12,14,11,10,9,3,5
G_8	0,1,2,13,4,7,15,6,8,14,9,5,10,11,3,12
G_9	0,1,2,13,4,7,15,6,8,14,11,3,5,9,10,12
G_{10}	0,1,2,13,4,7,15,6,8,14,11,5,10,9,3,12
G_{11}	0,1,2,13,4,7,15,6,8,14,11,10,5,9,12,3
G_{12}	0,1,2,13,4,7,15,6,8,14,11,10,9,3,12,5
G_{13}	0,1,2,13,4,7,15,6,8,14,12,9,5,11,10,3
G_{14}	0,1,2,13,4,7,15,6,8,14,12,11,3,9,5,10
G_{15}	0,1,2,13,4,7,15,6,8,14,12,11,9,3,10,5

B DDT and LAT of GIFT‘s S-box

Table 12: DDT of the GIFT's S-box

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	2	0	2	2	2	2	2	0	0	2
2	0	0	0	0	0	4	4	0	0	2	2	0	0	2	2	0
3	0	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2
4	0	0	0	2	0	4	0	6	0	2	0	0	0	2	0	0
5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4
6	0	0	4	6	0	0	0	2	0	0	2	0	0	0	2	0
7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0
8	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
10	0	4	0	0	0	0	4	0	0	2	2	0	0	2	2	0
11	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0
12	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0
13	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
14	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	0
15	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2

Table 13: LAT of the GIFT's S-box

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	-2	-2	2	4	0	0	-4	-2	-2	-2	-2
2	0	0	0	-4	0	4	0	0	2	2	2	-2	2	-2	2	2
3	0	0	0	-4	-2	-2	2	-2	2	-2	-2	-2	0	4	0	0
4	0	0	0	0	0	0	-4	-4	0	0	0	0	0	0	4	-4
5	0	0	0	0	2	-2	2	-2	0	4	4	0	2	2	-2	-2
6	0	0	0	-4	4	0	0	0	-2	-2	-2	2	2	-2	-2	-2
7	0	0	0	4	2	2	2	-2	2	-2	-2	-2	4	0	0	0
8	0	0	0	0	0	-4	0	-4	0	0	0	0	0	-4	0	4
9	0	0	0	0	-2	-2	2	2	4	0	0	4	2	-2	2	-2
10	0	0	-4	0	0	0	4	0	-2	-2	2	-2	-2	-2	2	-2
11	0	0	4	0	2	-2	2	2	-2	2	-2	-2	0	0	4	0
12	0	4	4	0	0	0	0	0	0	-4	4	0	0	0	0	0
13	0	-4	4	0	-2	2	2	-2	0	0	0	0	-2	-2	-2	-2
14	0	-4	0	0	4	0	0	0	2	-2	2	2	-2	2	2	2
15	0	-4	0	0	-2	-2	-2	2	-2	-2	2	-2	4	0	0	0

C The class number of the affine equivalence classes in [21]

Table 14: The class number of affine equivalence classes in the set where any DDT of an S-box has the same rows.

Class	15	16	26	31	32	33	108	136	137	142
143	190	216	233	248	249	250	251	252	253	254
255	256	257	258	259	262	267	268	272	273	276
277	282	284	287	288	289	291	295	297	298	301