IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 2, 2020, accepted November 16, 2020, date of publication November 19, 2020,
date of current version December 7, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3039273*

# Classification of 4-bit S-Boxes for BOGI Permutation

**SEONGGYEOM KIM[1], DEUKJO HONG[2], JAECHUL SUNG[3], AND SEOKHIE HONG[1], (Member, IEEE)**

[1]Institute of Cyber Security and Privacy (ICSP), Korea University, Seoul 02841, South Korea
[2]Department of Information Technology and Engineering, Chonbuk National University, Jeonju 54896, South Korea
[3]Department of Mathematics, University of Seoul, Seoul 02504, South Korea

Corresponding author: Deukjo Hong (deukjo.hong@jbnu.ac.kr)

This work was supported in part by the Military Crypto Research Center funded by the Defense Acquisition Program Administration (DAPA) and Agency for Defense Development (ADD) under Grant UD170109ED.

**ABSTRACT** Bad Output must go to Good Input (BOGI) is the primary design strategy of GIFT, a lightweight block cipher that was presented at CHES 2017. Because this strategy obviates the need to adhere to the required conditions of S-boxes when adopting bit-permutation, cryptographic designers have more S-box choices. In this paper, we classify all 4-bit S-boxes that support BOGI, called ''BOGI-applicable S-boxes,'' and evaluate them in terms of the cryptographic strength and efficiency. First, we exhaustively show that only 2413 Permutation-XOR-Equivalence (PXE) classes over 4-bit S-boxes are BOGI-applicable. After refining the PXE classes with respect to the differential uniformity ($\mathcal{U}$) and linearity ($\mathcal{L}$), we suggest 20 ''Optimal BOGI-applicable'' PXE classes that provide the best ($\mathcal{U}$, $\mathcal{L}$). Our security evaluations revealed that all optimal BOGI-applicable S-boxes fulfill the security properties considered by the designers of GIFT and that the differences between them exist in the other properties. Moreover, we explore the resistance of GIFT variants against differential and linear cryptanalysis by replacing the existing S-box with other optimal BOGI-applicable S-boxes. Based on the results, we identify the best attainable resistance with the bit-permutation of GIFT-64. Lastly, we suggest notable S-boxes that support competitive performance, jointly considering the cryptographic strength and efficiency for GIFT-64 and GIFT-128 structures, respectively.

**INDEX TERMS** S-box, lightweight implementation, BOGI, equivalence class, cryptography.

## I. INTRODUCTION

A large number of lightweight block ciphers adopt bit-permutation due to its negligible implementation cost in hardware. Among these block ciphers, GIFT presented in [1] outperforms the others with its state-of-the-art design approach. Thus, GIFT is widely used as the main primitive in multiple candidates of NIST lightweight cryptography standardization [2]–[6]. The main novelty of GIFT is a logic named Bad Output must go to Good Input (BOGI). This logic prevents differential and linear trails consisting of only one active S-box in each round even though the round function is composed of a bit-permutation and an S-box whose differential and linear branch numbers are 2. As a result, this simple but effective idea enhances the design strategy of PRESENT [7] and allows GIFT to become faster and lighter. However, not every S-box can support BOGI because such *BOGI-applicable* S-boxes would need to satisfy particular conditions on their Difference Distribution Table (DDT) and Linear Approximation Table (LAT). Indeed, it has already been shown that all the ''Optimal S-boxes'' discussed in [8] are not BOGI-applicable. This implies that related studies that concentrate only on the optimal S-boxes [9] may not be helpful for analyzing the BOGI design strategy thoroughly.

Various aspects of an S-box, which is the main nonlinear component of modern SPN ciphers, have been analyzed. These aspects are mainly related to security strength and efficiency, such as classifying a set of S-boxes in terms of the security strength requirements [8], [10], [11] or implementation cost [12], and finding the optimal implementation of a given S-box [13]–[15]. Because of the infeasible searching space of large S-boxes, these studies tended to concentrate on 4-bit S-boxes. Moreover, for classification purposes, introducing an appropriate equivalence relation is necessarily considered to ensure analysis efficiency. The well-known relations to group $16!(\approx 2^{44.25})$ 4-bit S-boxes into equiv-

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

alence classes are Affine-Equivalence (AE), Permutation-XOR-Equivalence (PXE), and Permutation Equivalence (PE) relations. In two independent reports [16], [17], the number of AE, PXE, and PE classes over 4-bit S-boxes were deduced as 302, 142,090,700($\approx 2^{27.08}$), and 36,325,278,240($\approx 2^{35.08}$), respectively.

As BOGI-applicability is preserved in a PXE class, and it is feasible to analyze the number of PXE classes exhaustively, we present an in-depth analysis of all BOGI-applicable S-boxes. Our analysis includes the security strength of the S-boxes themselves and the extent to which they affect the resistance of GIFT against differential and linear cryptanalysis (DC and LC). We partitioned the BOGI-applicable PXE classes into PE classes to enable us to additionally analyze their implementation costs. Based on our results, we suggest generalized properties of BOGI-applicable S-boxes and notable S-boxes for GIFT.

### A. OUR CONTRIBUTIONS

#### 1) CLASSIFICATION OF ALL BOGI-APPLICABLE 4-BIT S-BOXES

We search for and identify all BOGI-applicable PXE classes and deduce the total number of BOGI-applicable 4-bit S-boxes. Our search showed that only 2,413 PXE classes (186,392,448 S-boxes) are BOGI-applicable over 4-bit S-boxes. We define BOGI-applicable 4-bit S-boxes that provide the best differential uniformity and linearity as being ''Optimal BOGI-applicable'' 4-bit S-boxes with knowledge similar to that of the optimal 4-bit S-boxes discussed in [8]. Following the definition, we provide 20 optimal BOGI-applicable PXE classes out of the entire set of PXE classes.

Using the 20 optimal BOGI-applicable PXE classes, we conduct a detailed cryptographic analysis and generalize their security properties (Observation 1-5). Our investigations revealed that all optimal BOGI-applicable S-boxes fulfill the security properties considered by the designers of GIFT and that the differences among the PXE classes exist with respect to the other cryptographic properties.

We also explore the cost of implementing the optimal BOGI-applicable S-boxes in software and hardware, respectively. This was achieved by adopting two well-known measures – Bitslice Gate Complexity (**BGC**) and Gate Equivalent Complexity (**GEC**). The **BGC** of optimal BOGI-applicable S-boxes ranges from 10 to 13 whereas that of **GEC** ranges from 16 to 21 with the UMC180nm cell library. Our result shows that the (**BGC**, **GEC**) value of the GIFT S-box is (11, 16) implying that there exist S-boxes that provide more efficient implementations in software. However, as the smallest **BGC** = 10 always leads the S-boxes to have fixed points, we can conclude that (11, 16) is the best implementation cost without fixed-points.

#### 2) SUGGESTION OF NOTABLE S-BOXES FOR GIFT

We jointly consider the implementation cost and the resistance against DC and LC, and suggest notable S-boxes for the GIFT[1] structures. This is accomplished by deducing the best differential and linear trails by replacing the existing S-box of GIFT with optimal BOGI-applicable S-boxes.

We first show that an exhaustive investigation of the resistance is possible by using only 1,728 non-DDT-equivalent S-boxes. Then, we deduce the 13-round best differential and linear trails of the 1,728 GIFT−64 variants, where only the existing S-box is replaced by one of the non-DDT-equivalent S-boxes. Our results show that the maximum differential probability and correlation potential at $log_2$ scale can be improved to $(-68.4, -72)$ or $(-70, -68)$ from the current $(-62, -68)$. Although both of the most improved DC and LC resistances cause the implementation cost to increase, we identify 128 (+ 80 with fixed points) notable S-boxes that support the competitive DC and LC resistances within the same implementation cost of the GIFT S-box.

For GIFT−128 structure, we only consider S-boxes already demonstrated to perform competitively in GIFT−64 structure due to the computational intensiveness. Our results show that the maximum differential probability and correlation potential of 12-round trails of GIFT−128 variants can be improved up to $(-76.4, -74)$ from the current $(-60.4, -72)$.

### B. ORGANIZATION

Section II defines the notations used in this paper with brief explanations of BOGI and equivalence relations over S-box. In Section III, all BOGI-applicable S-boxes are classified and we define optimal BOGI-applicable S-boxes. In Section IV, we scrutinize cryptographic properties of optimal BOGI-applicable S-boxes and their implementation costs. In Section V, we investigate how the BOGI-applicable S-boxes influence the security of GIFT against DC and LC, followed by several competitive S-boxes compared to the existing S-box of GIFT. Lastly, the conclusion is given in Section VI. Some of our analysis results are presented in the Appendices.[2]

## II. PRELIMINARY

### A. NOTATIONS

In this paper, all the S-boxes we consider are 4-bit bijective functions. The following notations are used throughout the paper.

- $\cdot\ wt(x)$ : The Hamming weight of a binary vector $x$.
- $\cdot\ x \cdot y$ : The inner product of $x$ and $y$ over $\mathbb{F}_2^4$.
- $\cdot\ \mathrm{DDT}_S$ : The difference distribution table of an S-box $S$. The element $\mathrm{DDT}_S(\Delta i, \Delta o)$ in row $\Delta i$ and column $\Delta o$ is $|\{x \in \mathbb{F}_2^4 | S(x) \oplus S(x \oplus \Delta i) = \Delta o\}|$.
- $\cdot\ \mathrm{LAT}_S$ : The linear approximation table of an S-box $S$. The element $\mathrm{LAT}_S(\lambda i, \lambda o)$ in row $\lambda i$ and column $\lambda o$ is $|\{x \in \mathbb{F}_2^4 \mid \lambda i \cdot x = \lambda o \cdot S(x)\}| - 8$.

[1] Two versions of GIFT exist, GIFT−64 and GIFT−128, depending on the distinct block size.

[2] Our analysis results can be also found in https://github.com/jeffgyeom/classification-bogi-sbox

- $\cdot$ $\mathrm{SQLAT}_S$ : The table derived from the corresponding $\mathrm{LAT}_S$. The element $\mathrm{SQLAT}_S(\lambda i, \lambda o)$ is the square of the corresponding element $(\mathrm{LAT}_S(\lambda i, \lambda o))^2$.
- $\cdot$ $\mathrm{DDT}_S^1$ : The partial $4 \times 4$ table consisting of Hamming weight 1 to Hamming weight 1(i.e., single active bit) differential transitions in the corresponding $\mathrm{DDT}_S$.
- $\cdot$ $\mathrm{LAT}_S^1$ : The partial $4 \times 4$ table consisting of Hamming weight 1 to Hamming weight 1(i.e., single active bit) linear transitions in the corresponding $\mathrm{LAT}_S$.

We also define the following table, which can be deduced by the corresponding $\mathrm{DDT}_S^1$ and $\mathrm{LAT}_S^1$.

*Definition 1: The* BOGI Table *of 4-bit S-box S, denoted by* $\mathrm{BGT}_S$*, is a* $4 \times 4$ *table where each coefficient is* 0 *when the corresponding coefficients of* $\mathrm{DDT}_S^1$ *and* $\mathrm{LAT}_S^1$ *are both* 0*; otherwise, each coefficient in the table is* 1.

If the reference to S-box $S$ is clear from the context, we omit $S$ from the notations.

### B. PREVENTION OF CONSECUTIVE SINGLE ACTIVE BIT TRANSITIONS

For differential and linear cryptanalysis, the differential uniformity [18] and linearity [19] of an S-box are considered to be the most basic but significant measures. The differential uniformity and linearity of an S-box $S$ are denoted by $\mathcal{U}(S)$ and $\mathcal{L}(S)$ and defined as:

$$\mathcal{U}(S) := \max_{\Delta i \in \mathbb{F}_2^4 - \{0\},\ \Delta o \in \mathbb{F}_2^4} \mathrm{DDT}_S(\Delta i, \Delta o),$$
$$\mathcal{L}(S) := \max_{\lambda i \in \mathbb{F}_2^4,\ \lambda o \in \mathbb{F}_2^4 - \{0\}} 2 \times |\mathrm{LAT}_S(\lambda i, \lambda o)|.$$

It is already shown that the smallest $\mathcal{U}$ and $\mathcal{L}$ of 4-bit S-boxes are 4 and 8, respectively. Based on the above properties, "Optimal 4-bit S-boxes" are defined as the follows.

*Definition 2 [8]: A 4-bit S-box S is called an* Optimal S-box *if it fulfills these three conditions:*

1) $S$ *is bijective.*
2) $\mathcal{U}(S) = 4$.
3) $\mathcal{L}(S) = 8$.

However, adopting an optimal S-box cannot always guarantee the optimal resistance of the ciphers against DC and LC, especially when bit-permutation is used for the permutation layer. Thus, Zhang *et al.* additionally considered the number of non-zero entries in $\mathrm{DDT}^1$ and $\mathrm{LAT}^1$ [9]. In other words, the non-zero entries represent single active bit transitions.

*Definition 3 [9]:* $CarD1_S$ *and* $CarL1_S$ *of an S-box S denote the number of non-zero entries in* $\mathrm{DDT}_S^1$ *and* $\mathrm{LAT}_S^1$*, respectively.*

This is because the single active bit differential(linear) transitions of an S-box may cause the differential(linear) trails of bit-permutation based ciphers to have only one single active S-box in each round, and raise a number of efficient trails for DC and LC. Indeed, such linear trails allow multidimensional linear cryptanalysis on PRESENT up to 26 rounds out of 31 rounds.

Direct mitigation for this weakness is to use an S-box that does not have any active transitions both in $\mathrm{DDT}^1$ and $\mathrm{LAT}^1$(i.e., $(CarD1, CarL1) = (0, 0)$). However, it is shown that nonlinear 4-bit S-boxes cannot have such $(CarD1, CarL1)$ values [11].

Indirect mitigation presented in [9] prevents short iterative trails consisting of only single active bit transitions from allowing $(CarD1, CarL1) \neq (0, 0)$. This design approach alters PRESENT and $\mathrm{SPONGENT}_{88}$ [20] by replacing their S-box, and improves the block ciphers in terms of the resistance against DC and LC. Moreover, RECTANGLE [21] is designed with the prevention strategy, and provides the relatively robust resistances in spite of adopting an S-boxes with $(CarD1, CarL1) = (2, 2)$. Nonetheless, this design approach cannot fundamentally solve the problem of presenting consecutive single active bit transitions in trails. To be specific, RECTANGLE allows 2-round trails that consist of only single active bit transitions.

### C. BOGI

BOGI was presented as the first design approach toward the fundamental prevention of consecutive single active bit transitions [1]. The approach reveals $\mathrm{DDT}^1$ and $\mathrm{LAT}^1$ such that it achieves the fundamental prevention. It was successfully applied to the bit-permutation based block cipher, GIFT. Consequently, GIFT supports both DC and LC resistance with even fewer rounds than PRESENT.

Before describing BOGI, we first introduce PRESENT round function, on which BOGI is based. The round function consists of a substitution layer composed of the same 4-bit S-box and a 64-bit permutation layer. The permutation layer is again composed of four independent 16-bit permutations and a nibble-wise permutation followed by key addition. The round function, except for the key-addition, can be described in Fig. 1. $\mathcal{P}_{mix}^j$ denote the four independent 16-bit permutations and $\mathcal{P}_{shuf}$ denotes the nibble-wise permutation while the S-boxes in the $i^{\text{th}}$ round are denoted by $S_0^i, S_1^i, \ldots, S_{15}^i$. The $P_{mix}^j$ can easily be deduced to be a 16-bit mapping from the four S-boxes $\{S_{4j}^i, S_{4j+1}^i, S_{4j+2}^i, S_{4j+3}^i\}$ to the four S-boxes $\{S_j^{i+1}, S_{j+4}^{i+1}, S_{j+8}^{i+1}, S_{j+12}^{i+1}\}$.

Although the structure of PRESENT round function provides full diffusion in 3 rounds, $\mathcal{P}_{mix}^j$ of PRESENT have an Achilles' heel - allowing consecutive single active bit transitions in linear trails. This is because PRESENT S-box has single active bit linear transitions. To overcome the weakness of $\mathcal{P}_{mix}^j$ in PRESENT, BOGI properly crafts $\mathcal{P}_{mix}^j$ to guarantee that an output bit of a single active bit transition (Bad Output) must go to an input bit of a single non-active bit transition (Good Input).

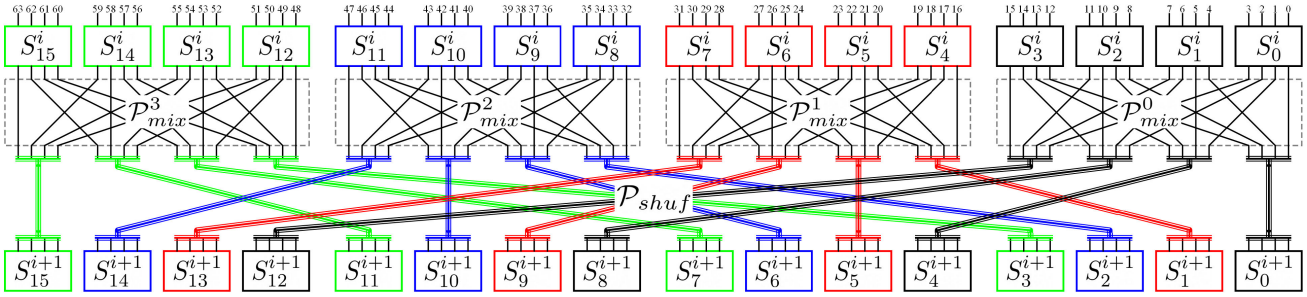


**FIGURE 1.** Round function of PRESENT except for key-addition.

However, to enable BOGI to be used, in addition to well-crafted $\mathcal{P}^j_{mix}$, an S-box has to obtain an appropriate BGT as presented in Lemma 1.

*Lemma 1 [1]: To apply BOGI to an S-box S, the corresponding* $\mathrm{BGT}_S$ *must consist of at least four all-zero rows and columns.*

If an S-box satisfies the above condition, we denote the S-box to be *BOGI-applicable*. As seen in Table 1, PRESENT S-box(*PS*) is not BOGI-applicable because $\mathrm{BGT}_{PS}$ consists of only one all-zero row and column each. On the contrary, $\mathrm{BGT}_{GS}$ of GIFT S-box(*GS*) has four all-zero rows and columns, and thus *GS* is BOGI-applicable.

**TABLE 1.** DDT[1], LAT[1], and BGT of *PS* and *GS*: all zero rows(Good input) and columns (Good output) are indexed with *G*, otherwise (Bad in/output) with *B*.

• $\mathrm{BGT}_{PS}$

| | 1 | 2 | 4 | 8 |
|---|---|---|---|---|
| | *G* | *B* | *B* | *B* |
| 1 *G* | 0 | 0 | 0 | 0 |
| 2 *B* | 0 | 1 | 1 | 1 |
| 4 *B* | 0 | 1 | 1 | 1 |
| 8 *G* | 0 | 1 | 0 | 1 |

• $\mathrm{BGT}_{GS}$

| | 1 | 2 | 4 | 8 |
|---|---|---|---|---|
| | *G* | *G* | *B* | *B* |
| 1 *B* | 0 | 0 | 1 | 1 |
| 2 *B* | 0 | 0 | 0 | 1 |
| 4 *G* | 0 | 0 | 0 | 0 |
| 8 *G* | 0 | 0 | 0 | 0 |

### D. BOGI PERMUTATION

Once an S-box is BOGI-applicable, appropriate 16-bit permutations $\mathcal{P}^j_{mix}$ can be deduced for the S-box. Hereafter, we assume that the four structures of $\mathcal{P}^j_{mix}$ are equal to each other. This equality is not required to apply BOGI but may be preferred for implementation and design consistency. $\mathcal{P}^j_{mix}$ consists of a group mapping ($\rho$) and four individual mappings ($\pi^k$) as presented in Fig. 2. We assume that the group mapping is $\rho$ of GIFT.[3]

The group mapping $\rho$ ensures that the input bits in each S-box originate from four different S-boxes in the previous round. At the same time, the bit orders of the bad ($B$) and good ($G$) outputs of each S-box in the $i^{th}$ round are preserved after passing through $\rho$. Considering the preserved orders,

[3] GIFT-64 and GIFT-128 have the same $\mathcal{P}^j_{mix}$.

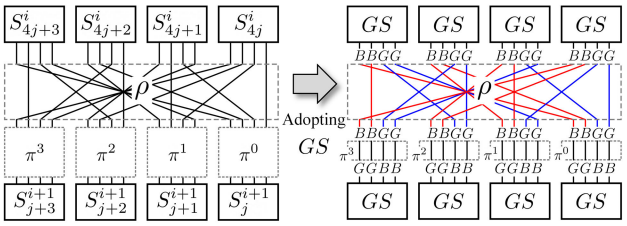


**FIGURE 2.** Structure of $\mathcal{P}^j_{mix}$ and the propagations of *B* and *G* in $\mathcal{P}^j_{mix}$ of GIFT.

the individual mappings $\pi^k$ can be chosen to map the bad outputs to good inputs in the next round. For example, $\mathcal{P}^j_{mix}$ of GIFT adopts identity mappings for $\pi^k$ as presented in Fig. 2. In this case, it should be noted that $B$ cannot propagate to $B$. Likewise, all of the individual mappings that do not produce $B$ - $B$ matches are BOGI permutations for an S-box. Note that such mappings do not exist for non-BOGI-applicable S-boxes.

The number of BOGI permutations of a BOGI-applicable S-box can be deduced by the BOGI-spectrum defined in Definition 4.

*Definition 4: The* BOGI-spectrum $\mathcal{BG}(S)$ *of an S-box S denotes a tuple* $(R_0, C_0)$*, where* $R_0$ *and* $C_0$ *denote the number of all-zero row vectors and column vectors in* $\mathrm{BGT}_S$*, respectively.*

According to Table 1, $\mathcal{BG}(GS) = (2, 2)$. Therefore, four BOGI permutations are available for *GS*.

### E. EQUIVALENCE RELATIONS OVER S-BOX

Various equivalence relations are used when analyzing the S-boxes. The well-studied equivalence relations are XOR Equivalence (XE), PE, PXE, Linear Equivalence (LE), and CCZ relations. In this paper, we mainly deal with XE, PE, PXE, and AE relations over 4-bit invertible S-boxes.

*Definition 5: If an S-box* $S'$ *can be defined from S as*

$$S'(x) = S((x \oplus c_{in})) \oplus c_{out}$$

*for some two vectors* $c_{in}$ *and* $c_{out}$ *over* $\mathbb{F}_2^4$*, S and* $S'$ *are* XOR equivalent (XE).

*Definition 6: If an S-box $S'$ can be defined from $S$ as*

$$S'(x) = P_{out}S(P_{in}(x))$$

*for some two bit-permutation matrices $P_{in}$ and $P_{out}$ over $\mathbb{F}_2^{4\times4}$, $S$ and $S'$ are* Permutation equivalent (PE).

*Definition 7 [10]: If an S-box $S'$ can be defined from $S$ as*

$$S'(x) = P_{out}S(P_{in}(x \oplus c_{in})) \oplus c_{out}$$

*for some two bit-permutation matrices $P_{in}$ and $P_{out}$ over $\mathbb{F}_2^{4\times4}$, and two vectors $c_{in}$ and $c_{out}$ over $\mathbb{F}_2^4$, $S$ and $S'$ are* Permutation-XOR equivalent (PXE).

*Definition 8: If an S-box $S'$ can be defined from $S$ as*

$$S'(x) = L_{out}S(L_{in}(x \oplus c_{in})) \oplus c_{out}$$

*for some two non-singular matrices $L_{in}$ and $L_{out}$ over $\mathbb{F}_2^{4\times4}$, and two vectors $c_{in}$ and $c_{out}$ over $\mathbb{F}_2^4$, $S$ and $S'$ are* Affine equivalent (AE).

The above equivalence relations enable the 4-bit S-boxes to be grouped into equivalence classes, such as the XE, PE, PXE, and AE classes. An algorithm to search all PXE classes over 4-bit S-boxes was first presented by Saarinen [10]. This algorithm was subsequently improved, and it was proved that every PXE class consists of 384 times the number of 4-bit S-boxes [11]. The improved algorithm can provide each representative of PXE classes and their size within several minutes.

## III. CLASSIFICATION OF BOGI-APPLICABLE S-BOXES

In this section, we identify all BOGI-applicable S-boxes and classify them according to their differential uniformity and linearity. Because the BOGI-applicability is invariant in a PXE class as presented by Proposition 1, we only check the BOGI-applicability of the representatives of 142,090,700 PXE classes to investigate the BOGI-applicability of all 4-bit S-boxes.

*Proposition 1 [1]: In a PXE class, BOGI-applicability is preserved. To be specific, if $S$ is BOGI-applicable, $S'(x) = P_{out}S(P_{in}(x \oplus c_{in})) \oplus c_{out}$ for all bit-permutation matrices $P_{in}$, $P_{out}$ over $\mathbb{F}_2^{4\times4}$ and vectors $c_{in}$, $c_{out}$ over $\mathbb{F}_2^4$ is also BOGI-applicable.*

### A. DISTRIBUTION OF BOGI-APPLICABLE PXE CLASSES

Checking the BOGI-applicability of all 4-bit PXE classes required approximately 6 hours with our single-threaded program. The result yielded only 2,413 BOGI-applicable PXE classes. We briefly categorized them according to their cryptographic strength by introducing differential uniformity and linearity. Note that these cryptographic properties are also invariant in the PXE class. Table 2 provides the distribution of the BOGI-applicable PXE classes.

Because each PXE class has a distinct size, the distribution of the 4-bit S-boxes differs from that of the PXE classes. Table 3 provides the distribution of BOGI-applicable S-boxes. The number of BOGI-applicable S-boxes amounts to only $186,392,448 (\approx 2^{27.47})$ out of all 4-bit S-boxes $(\approx 2^{44.25})$.

**TABLE 2. Distribution of 4-bit BOGI-applicable PXE classes: The total number of the PXE classes is 2,413.**

| $\mathcal{U}\backslash\mathcal{L}$ | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 |
|---|---|---|---|---|---|---|---|---|
| 2 | - | - | - | - | - | - | - | - |
| 4 | - | - | - | - | - | - | - | - |
| 6 | - | - | - | 20 | - | 95 | - | - |
| 8 | - | - | - | 106 | - | 26 | - | 604 |
| 10 | - | - | - | - | - | - | - | - |
| 12 | - | - | - | - | - | 20 | - | 538 |
| 14 | - | - | - | - | - | - | - | - |
| 16 | - | - | - | - | - | - | - | 1,004 |

**TABLE 3. Distribution of 4-bit S-boxes that are BOGI-applicable: The total number of BOGI-applicable S-boxes is 186,392,448.**

| $\mathcal{U}\backslash\mathcal{L}$ | 8 | 12 | 16 |
|---|---|---|---|
| 6 | 2,654,208 (1.42%) | 14,008,320 (7.52%) | - |
| 8 | 11,354,112 (6.09%) | 3,538,944 (1.9%) | 59,609,088 (31.98%) |
| 12 | - | 1,474,560 (0.79%) | 58,896,384 (31.6%) |
| 16 | - | - | 34,856,832 (18.7%) |

**TABLE 4. Details of the 20 optimal BOGI-applicable PXE classes. $B_0$ includes `GIFT` S-box and $B_1$ includes `GIFT` inverse S-box.**

| PXE Class | Representative | # S-boxes | Inverse Class |
|---|---|---|---|
| $B_0$ | (0, 7, 3, 4, 5, 2, 14, 13, 9, 12, 6, 11, 15, 10, 8, 1) | 147,456 | $B_1$ |
| $B_1$ | (0, 3, 5, 6, 7, 12, 8, 1, 11, 4, 13, 10, 14, 9, 2, 15) | 147,456 | $B_0$ |
| $B_2$ | (0, 7, 3, 4, 5, 2, 10, 9, 13, 8, 6, 15, 11, 14, 12, 1) | 147,456 | $B_3$ |
| $B_3$ | (0, 3, 5, 6, 7, 8, 10, 1, 14, 4, 9, 15, 13, 11, 2, 12) | 147,456 | $B_2$ |
| $B_4$ | (0, 7, 3, 4, 5, 8, 10, 15, 11, 2, 12, 9, 13, 14, 6, 1) | 147,456 | $B_5$ |
| $B_5$ | (0, 3, 7, 12, 5, 10, 8, 15, 13, 4, 2, 9, 11, 6, 14, 1) | 147,456 | $B_4$ |
| $B_6$ | (0, 3, 7, 8, 4, 13, 15, 2, 9, 6, 10, 5, 14, 11, 1, 12) | 147,456 | $B_7$ |
| $B_7$ | (0, 3, 5, 6, 7, 8, 9, 14, 10, 13, 12, 1, 15, 4, 2, 11) | 147,456 | $B_6$ |
| $B_8$ | (0, 7, 3, 8, 4, 15, 13, 2, 14, 1, 11, 12, 9, 10, 6, 5) | 73,728 | $B_9$ |
| $B_9$ | (0, 3, 5, 13, 6, 15, 10, 8, 11, 4, 14, 2, 9, 12, 7, 1) | 73,728 | $B_8$ |
| $B_{10}$ | (0, 3, 5, 6, 7, 12, 8, 1, 9, 4, 14, 11, 15, 10, 2, 13) | 147,456 | $B_{11}$ |
| $B_{11}$ | (0, 7, 3, 4, 5, 2, 14, 11, 9, 15, 6, 8, 10, 12, 13, 1) | 147,456 | $B_{10}$ |
| $B_{12}$ | (0, 3, 5, 6, 7, 8, 10, 1, 15, 4, 12, 11, 9, 14, 2, 13) | 147,456 | $B_{13}$ |
| $B_{13}$ | (0, 7, 3, 4, 5, 2, 12, 9, 11, 13, 6, 10, 8, 14, 15, 1) | 147,456 | $B_{12}$ |
| $B_{14}$ | (0, 3, 7, 13, 5, 11, 10, 12, 15, 4, 9, 2, 8, 14, 6, 1) | 147,456 | $B_{15}$ |
| $B_{15}$ | (0, 7, 3, 4, 5, 9, 8, 14, 12, 2, 11, 13, 15, 10, 6, 1) | 147,456 | $B_{14}$ |
| $B_{16}$ | (0, 3, 5, 6, 7, 8, 10, 15, 11, 14, 12, 1, 13, 4, 2, 9) | 147,456 | $B_{17}$ |
| $B_{17}$ | (0, 3, 7, 12, 5, 10, 11, 4, 6, 15, 9, 2, 8, 13, 14, 1) | 147,456 | $B_{16}$ |
| $B_{18}$ | (0, 3, 7, 12, 4, 13, 15, 10, 11, 6, 8, 5, 14, 9, 1, 2) | 73,728 | $B_{19}$ |
| $B_{19}$ | (0, 3, 5, 12, 7, 13, 10, 2, 8, 6, 11, 15, 14, 9, 1, 4) | 73,728 | $B_{18}$ |

As already shown in [1], BOGI-applicable PXE classes (S-boxes) that support $\mathcal{U} \leq 4$ do not exist. Therefore, $(\mathcal{U}, \mathcal{L}) = (6, 8)$ can be concluded to be the optimal choice. Based on the optimal choice, we define optimal BOGI-applicable S-boxes.

*Definition 9: A 4-bit S-box $S$ is called an* optimal BOGI-applicable S-box *if it fulfills these four conditions:*

1) *$S$ is bijective.*
2) *$S$ is BOGI-applicable.*
3) *$\mathcal{U}(S) = 6$.*
4) *$\mathcal{L}(S) = 8$.*

There exist only 20 optimal BOGI-applicable PXE classes. Table 4 presents details of all the optimal BOGI-applicable PXE classes. The inverse relations in Table 4 suggest that none of the optimal BOGI-applicable S-boxes is self-permutation-XOR equivalent, from which it can be concluded that they are unable to support involution (self-inverse).

*Observation 1: All optimal BOGI-applicable S-boxes are not involutory.*

### B. BOGI SPECTRUM OF BOGI-APPLICABLE S-BOXES

As already mentioned in subsection II-D, the BOGI-spectrum $\mathcal{BG}$ of a BOGI-applicable S-box can give an insight into the BOGI permutations of the S-box. Especially, the number of BOGI permutations can easily be deduced by $\mathcal{BG}$. The distribution of $\mathcal{BG}$ of BOGI-applicable PXE classes is presented in Table 5. These results lead to the conclusion that $\mathcal{BG}$ of optimal BOGI-applicable 4-bit S-boxes is always (2, 2), and that the number of BOGI-permutations for optimal BOGI-applicable S-boxes is always 4.

**TABLE 5. $\mathcal{BG}$ of BOGI-applicable PXE Classes: Each result shows the number of BOGI-applicable PXE classes with the corresponding $\mathcal{BG}$. For example, 20 optimal BOGI-applicable PXE classes have the $\mathcal{BG}$ as (2, 2).**

| $(\mathcal{U}, \mathcal{L})$ | $\mathcal{BG}$ of the BOGI-applicable PXE Classes |
|---|---|
| (6, 8) | (2, 2): 20 |
| (6, 12) | (1, 3): 3, (2, 2): 76, (2, 3): 6, (3, 1): 3, (3, 2): 6, (3, 3): 1 |
| (8, 8) | (1, 3): 3, (2, 2): 88, (2, 3): 6, (3, 1): 3, (3, 2): 6 |
| (8, 12) | (2, 2): 26 |
| (8, 16) | (1, 3): 54, (2, 2): 377, (2, 3): 59, (3, 1): 54, (3, 2): 59, (3, 3): 1 |
| (12, 12) | (2, 2): 16, (2, 3): 2, (3, 2): 2 |
| (12, 16) | (1, 3): 54, (2, 2): 215, (2, 3): 85, (3, 1): 54, (3, 2): 85, (3, 3): 45 |
| (16, 16) | (1, 3): 39, (2, 2): 414, (2, 3): 101, (3, 1): 39, (3, 2): 101, (3, 3): 238, (4, 4): 72 |

*Observation 2: All optimal BOGI-applicable 4-bit S-boxes have $\mathcal{BG}$ as (2, 2). This implies that there exist only four distinct BOGI permutations($\pi$) for each optimal BOGI-applicable 4-bit S-box.*

### C. BOGI-APPLICABLE S-BOXES THAT FULFILL THE CRITERIA OF THE GIFT DESIGNERS

In this subsection, we traverse every BOGI-applicable S-box satisfying criteria suggested in [1]. Except for the consideration of the implementation, the following conditions are considered by GIFT designers.

- Condition 1 (**GC1**) : An S-box $S$ is BOGI-applicable.
- Condition 2 (**GC2**) : $\mathcal{U}(S)$ values in $\mathrm{DDT}_S$ appear smaller than 3 times.
- Condition 3 (**GC3**) : For $\mathrm{DDT}_S(\Delta i)(\Delta o) = \mathcal{U}(S)$, $wt(\Delta i) + wt(\Delta o) \geq 4$.

Table 6 presents the distribution of PXE classes that fulfill all the conditions **GC1**∼**3**. Only 363 PXE classes(43,118,592 S-boxes) satisfy all three conditions. Note that all optimal BOGI-applicable S-boxes satisfy the conditions.

**TABLE 6. Distribution of 4-bit BOGI-applicable PXE classes that satisfy the conditions specified by the designers of GIFT. The total number of the PXE classes is 363.**

| $\mathcal{U}\backslash\mathcal{L}$ | 8 | 12 | 16 |
|---|---|---|---|
| 6 | 20/20 | 0/95 | - |
| 8 | 24/106 | 16/26 | 24/604 |
| 12 | - | 20/20 | 259/538 |
| 16 | - | - | 0/1,004 |

*Observation 3: All optimal BOGI-applicable S-boxes satisfy the conditions **GC1**∼**3**.*

This observation implies that none of the optimal BOGI-applicable S-boxes make any difference in terms of the previous design criteria considered by GIFT designers. However, as we show in the following section, the differences between optimal BOGI-applicable and non-optimal BOGI-applicable S-boxes manifest themselves in the other security properties and the implementation cost.

## IV. EVALUATIONS OF OPTIMAL BOGI-APPLICABLE S-BOXES

In this section, we evaluate optimal BOGI-applicable S-boxes in terms of their cryptographic strength and implementation cost in more detail than the criteria considered by GIFT designers. Hereafter, we denote each of the 20 optimal BOGI-applicable PXE classes in Table 4 as $B_i$ with the corresponding index $i$. Although most of the cryptographic properties we evaluate are preserved in a PXE class, we sometimes partition each PXE class into the corresponding PE, XE classes for the properties that are not preserved in a PXE class. To be specific, optimal BOGI-applicable PE classes are discussed for the implementation cost in subsection IV-B whereas the XE classes are discussed in Section V.

### A. SECURITY EVALUATIONS

In this subsection, we consider security properties of the 20 optimal BOGI-applicable PXE classes additional to those that were considered by GIFT designers. Although all optimal BOGI-applicable PXE classes satisfy GIFT designers' criteria as shown in Observation 3, our extra security evaluations present some differences between the PXE classes.

**TABLE 7. AE classes that include the 20 optimal BOGI-applicable PXE classes. The $25^{th}$ AE class includes the GIFT S-box whereas the $26^{th}$ AE class includes the GIFT inverse S-box.**

| AE class | PXE class | AE class | PXE class | AE class | PXE class | AE class | PXE class |
|---|---|---|---|---|---|---|---|
| $25^{th}$ | $B_0$ | $26^{th}$ | $B_1$ | $28^{th}$ | $B_{10}$ | $29^{th}$ | $B_{11}$ |
| | $B_2$ | | $B_3$ | | $B_{12}$ | | $B_{13}$ |
| | $B_4$ | | $B_5$ | | $B_{14}$ | | $B_{15}$ |
| | $B_6$ | | $B_7$ | | $B_{16}$ | | $B_{17}$ |
| | $B_8$ | | $B_9$ | | $B_{18}$ | | $B_{19}$ |

#### 1) OPTIMAL BOGI-APPLICABLE AE CLASSES

We first compute the AE classes that include optimal BOGI-applicable PXE classes and present the results in Table 7. We refer to [22] for the index of AE class. Only four distinct

AE classes include optimal BOGI-applicable PXE classes (five each). It is noted that BOGI-applicability is not preserved in an AE class. For example, the S-boxes that are included in the $25^{th}$ AE class but not included in $B_{0,2,4,6,8}$ are not BOGI-applicable.

#### 2) DIFFERENTIAL SPECTRUM AND WALSH SPECTRUM

The differential spectrum of an S-box is related to **GC2**. In addition to the frequency of differential uniformity in DDT, the frequency of the other values in DDT may affect the resistance against DC. Thus, the differential spectrum could be of interest. The differential spectrum $\mathcal{D}_{spec}$ is defined as follows.

*Definition 10 [23], [24]: The* differential spectrum *of an S-box* $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *is the multiset:*

$$\mathcal{D}_{spec}(S) := \{\mathrm{DDT}_S(\Delta i, \Delta o) \mid \Delta i \in \mathbb{F}_2^n - \{0\}, \Delta o \in \mathbb{F}_2^n\}.$$

In the similar concept, the Walsh spectrum of an S-box could be of interest. The Walsh spectrum was not included in the three primary conditions(**GC1** $\sim$ **GC3**). However, the frequency of maximal values may also affect the resistance against LC. In consideration thereof, we evaluate the extended Walsh spectrum $|\mathcal{L}|_{spec}$. The (extended) Walsh spectrum of a Boolean function can be generalized for an S-box as follows.

*Definition 11 [23]: The* Walsh spectrum *of an S-box* $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *is the multiset:*

$$\mathcal{L}_{spec}(S) := \{2 \times \mathrm{LAT}_S(\lambda i, \lambda o) \mid \lambda i \in \mathbb{F}_2^n, \lambda o \in \mathbb{F}_2^n - \{0\}\}.$$

*Moreover, the* extended Walsh spectrum *of an S-box* $|\mathcal{L}|_{spec}(S)$ *is defined as the multiset of the absolute values in* $\mathcal{L}_{spec}(S)$.

Because $\mathcal{D}_{spec}$ and $|\mathcal{L}|_{spec}$ are invariant in an AE class, we only deduce them with the four AE classes in Table 7. Surprisingly, these four AE classes have the same differential, extended Walsh spectrum as Observation 4.

*Observation 4: All optimal BOGI-applicable S-boxes have the differential spectrum* $\mathcal{D}_{spec}$ *and extended Walsh spectrum* $|\mathcal{L}|_{spec}$*:*

$$\mathcal{D}_{spec} = \{0 : 142,\ 2 : 78,\ 4 : 18,\ 6 : 2\},$$
$$|\mathcal{L}|_{spec} = \{0 : 108,\ 4 : 96,\ 8 : 36\}.$$

Although certain optimal 4-bit S-boxes presented previously [8] have a more appropriately extended Walsh spectrum:

$$|\mathcal{L}|_{spec} = \{0 : 96,\ 4 : 112,\ 8 : 32\} \text{ or } \{0 : 90,\ 4 : 120,\ 8 : 30\},$$

the extended Walsh spectrum of optimal BOGI-applicable S-boxes equals to the extended Walsh spectrum of S-boxes in 4-bit S-box based block ciphers (e.g., `PRESENT`, `LBlock`, `PICCOLO`, `RECTANGLE`). This implies that optimal BOGI-applicable S-boxes provide compatible cryptographic strength in terms of nonlinearity.

#### 3) ALGEBRAIC DEGREE OF COMPONENT BOOLEAN FUNCTIONS

The algebraic degree, $\deg(f)$, of a Boolean function $f$ is the degree of the maximum term in the corresponding algebraic normal form. The algebraic degree for an S-box(vectorial Boolean function) $S$ can be generalized as follows:

$$\deg(S) = \max_{a \in \mathbb{F}_2^n - \{0\}} \deg(S_a),$$

where $S_a = a \cdot S$.

In addition to the degree of the maximum term, the following multiset:

$$\deg_{spec}(S) = \{\deg(S_a) | a \in \mathbb{F}_2^n - \{0\}\}$$

could be of interest. Because $\deg_{spec}$ is invariant under affine equivalence, we again utilize the results in Table 7 to investigate $\deg_{spec}$ of all optimal BOGI-applicable S-boxes. The evaluations present that every optimal BOGI-applicable S-box has the same algebraic degree spectrum as presented in Observation 5.

*Observation 5: All optimal BOGI-applicable S-boxes have the algebraic degree spectrum* $\deg_{spec}(S)$*:*

$$\deg_{spec}(S) = \{2 : 3,\ 3 : 12\}.$$

*This also implies that all optimal BOGI-applicable S-boxes have the algebraic degree of 3.*

Clearly, at least two of the coordinate Boolean functions ($S_{e_i}$ for a unit vector $e_i \in \mathbb{F}_2^4$) have the algebraic degree of 3 with the same knowledge of Theorem 3 as in a previous study [9]. This means that at least two non-zero entries are present in $\mathrm{LAT}^1$(i.e., $CarL1 \geq 2$), which corresponds to our results in Table 9.

#### 4) HAMMING WEIGHT ON THE SUB-OPTIMAL DIFFERENTIAL TRANSITION

Related to **GC3**, $wt(\Delta i) + wt(\Delta o)$ for $\mathrm{DDT}(\Delta i, \Delta o) = 6$ should be considered to reduce the occurrence of sub-optimal differential transition in a differential trail. As the Hamming weights are preserved in a PXE class, we compute the following multiset:

$$\mathcal{W}_{D6}(S) := \{wt(\Delta i) + wt(\Delta o) \mid DDT_S(\Delta i, \Delta o) = 6\}.$$

Table 8 presents the value of $\mathcal{W}_{D6}$ of each of optimal BOGI-applicable PXE classes.

All optimal BOGI-applicable PXE classes have only two entries with the differential uniformity 6 as presented in Observation 4. One can notice that there exist better PXE classes than $B_0$ and $B_1$, which include `GIFT` S-box and inverse S-box, respectively. Indeed, $\mathcal{W}_{D6}$ of $B_{4\sim7}$ and $B_{14\sim17}$ are $\{4, 5\}$, and $\mathcal{W}_{D6}$ of $B_{8,9,18,19}$ are $\{5, 5\}$. Thus, `GIFT` S-box may not be the best choice with respect to the prevention of sub-optimal differential transitions in a trail.

**TABLE 8.** Values of $\mathcal{W}_{D6}$ of the 20 optimal BOGI-applicable PXE classes.

| PXE class | $\mathcal{W}_{D6}$ | PXE class | $\mathcal{W}_{D6}$ | PXE class | $\mathcal{W}_{D6}$ | PXE class | $\mathcal{W}_{D6}$ |
|---|---|---|---|---|---|---|---|
| $B_0$ | 4, 4 | $B_5$ | 4, 5 | $B_{10}$ | 4, 4 | $B_{15}$ | 4, 5 |
| $B_1$ | 4, 4 | $B_6$ | 4, 5 | $B_{11}$ | 4, 4 | $B_{16}$ | 4, 5 |
| $B_2$ | 4, 4 | $B_7$ | 4, 5 | $B_{12}$ | 4, 4 | $B_{17}$ | 4, 5 |
| $B_3$ | 4, 4 | $B_8$ | 5, 5 | $B_{13}$ | 4, 4 | $B_{18}$ | 5, 5 |
| $B_4$ | 4, 5 | $B_9$ | 5, 5 | $B_{14}$ | 4, 5 | $B_{19}$ | 5, 5 |

**TABLE 9.** Differential(extended Walsh) spectrum restricted in $\mathrm{DDT}^1(\mathrm{LAT}^1)$. The zeros in each spectrum are omitted.

| PXE class | $\mathcal{D}^1_{spec}$ | $\lvert\mathcal{L}\rvert^1_{spec}$ | PXE class | $\mathcal{D}^1_{spec}$ | $\lvert\mathcal{L}\rvert^1_{spec}$ |
|---|---|---|---|---|---|
| $B_0$ | 2 | 2, 2, 4 | $B_{10}$ | 2 | 2, 2, 4 |
| $B_1$ | 2 | 2, 2, 4 | $B_{11}$ | 2 | 2, 2, 4 |
| $B_2$ | 2 | 2, 2, 2, 4 | $B_{12}$ | 2 | 2, 2, 2, 4 |
| $B_3$ | 2 | 2, 2, 2, 4 | $B_{13}$ | 2 | 2, 2, 2, 4 |
| $B_4$ | 2, 2 | 2, 2, 2 | $B_{14}$ | 2, 2 | 2, 2, 2 |
| $B_5$ | 2, 2 | 2, 2, 2 | $B_{15}$ | 2, 2 | 2, 2, 2 |
| $B_6$ | 2, 2 | 2, 2, 2 | $B_{16}$ | 2, 2 | 2, 2, 2 |
| $B_7$ | 2, 2 | 2, 2, 2 | $B_{17}$ | 2, 2 | 2, 2, 2 |
| $B_8$ | 2, 2, 2, 2 | 2, 2 | $B_{18}$ | 2, 2, 2, 2 | 2, 2 |
| $B_9$ | 2, 2, 2, 2 | 2, 2 | $B_{19}$ | 2, 2, 2, 2 | 2, 2 |

#### 5) DIFFERENTIAL(EXTENDED WALSH) SPECTRUM RESTRICTED IN $\mathrm{DDT}^1(\mathrm{LAT}^1)$

Although the differential and extended Walsh spectrum of optimal BOGI-applicable PXE classes are equal to each other, the differential(extended Walsh) spectrum restricted in $\mathrm{DDT}^1$ and $\mathrm{LAT}^1$, denoted by $\mathcal{D}^1_{spec}$ and $|\mathcal{L}|^1_{spec}$, can be distinct. Table 9 presents the restricted spectrum. One can also deduce $CarD1$ and $CarL1$ from $\mathcal{D}^1_{spec}$ and $|\mathcal{L}|^1_{spec}$.

The PXE classes $B_{0,1,10,11}$ provide the optimal choice of $(CarD1, CarL1) = (1, 3)$. However, the optimal choices cause $|\mathcal{L}|^1_{spec}$ to include 4. On the contrary, $\mathcal{D}^1_{spec}$ and $|\mathcal{L}|^1_{spec}$ of $B_{4\sim7,14\sim15}$ consists only of 2 although they have ($CarD1$, $CarL1$) as (2, 3).

### B. IMPLEMENTATION EVALUATIONS

In this subsection, we evaluate the implementation of optimal BOGI-applicable S-boxes with Peigen [14], which is based on `LIGHTER` [15]. We deduce both the software- and hardware-oriented implementations. This enables us to jointly consider the software and hardware efficiency of the optimal BOGI-applicable S-boxes.

#### 1) IMPLEMENTATION SEARCHING TOOL – PEIGEN

The implementation searching tool Peigen(or `LIGHTER`) can find the efficient(not always best) implementation of a given S-box within a set of the invertible instructions, denoted by $\mathcal{B}$. Such implementations are denoted $\mathcal{B}$-*implementation*. The searching method is based on bi-directional Dijkstra algorithm, and expands the two subgraphs until the predetermined expansion limit is reached (or when a proper stopping rule is satisfied). The expansion limit($\lambda$ in the paper [15] and "$-$l" in the corresponding tool[4]) determines whether the obtained implementation is the best or not. We set an expansion limit to guarantee all the implementations we obtain are the best $\mathcal{B}$-implementation. By tweaking the instruction set $\mathcal{B}$ and the corresponding costs, one can obtain the implementations of S-boxes for different environments. For more details, refer to [14], [15].

#### 2) OPTIMAL BOGI-APPLICABLE PE CLASSES

Because the implementation costs are not invariant under PXE relation, we first partition each of optimal BOGI-applicable PXE classes into the corresponding PE classes. In total, the PE classes amount to 4,608. Moreover, as an S-box and the corresponding inverse S-box have the exactly same implementation complexity due to the searching way of Peigen, we only consider half of the entire number of PE classes (i.e., 2,304 PE classes).

#### 3) SOFTWARE-ORIENTED IMPLEMENTATION

The complexity of the software implementation is measured by mainly using **BGC** [13]. Because **BGC** denotes the number of atomic operations used in the implementation, **BGC** directly determines the required cycle number and code size for bit-slice implementation of an S-box. The set $\mathcal{B}$[5] includes invertible instructions that are constructed by software operations{`AND`, `XOR`, `OR`, `NOT` and `ANDN`}. As the invertible instructions are constructed by at most three of the software operations, $\mathcal{B}$ includes instructions whose cost ranges from 1 to 3. We specify an expansion limit of "8," which implies each subgraph can be expanded until its size becomes $11(=8+3)$. All the implementation costs we obtain are smaller than $15(=2\times(8+1)-3)$; thus, our obtained implementations can be proved to be the best $\mathcal{B}$-implementation.

#### 4) HARDWARE-ORIENTED IMPLEMENTATION

As a measure of the complexity of hardware implementation, **GEC** is mainly used. **GEC** denotes the logic size of implementation and may be affected by the gates to be used. We restrict the logic gates to those supported by the UMC180nm cell library to construct the hardware instruction set $\mathcal{B}$. Each of the available gates and costs can be found in [14], and the cost of invertible instructions in $\mathcal{B}$[6] ranges from 0.67 to 5. Searching tends to be more intensive than finding the software implementation because $\mathcal{B}$ becomes bigger. We apply the expansion limit of "13," which means each subgraph can be expanded until its size becomes $18(=13+5)$. As the implementation costs we obtain are smaller than $22.34(=2\times(13+0.67)-5)$, all the implementations are proved to be the best in the $\mathcal{B}$-implementation.

[4]https://github.com/peigen-sboxes/PEIGEN

[5]The invertible instructions in $\mathcal{B}$ are checked whether they are equivalent to each other. If this is true, then the implementation with the lowest cost is chosen. The number of non-equivalent invertible instructions for **BGC** amounts to 18.

[6]The number of non-equivalent invertible instructions for **GEC** amounts to 35.

**TABLE 10.** Best $\mathcal{B}$-implementation costs and the number of corresponding PE classes. (BGC, GEC) of GIFT S-box including the inverse is (11, 16), and 18 PE classes provide the same implementation cost.

| BGC \GEC | 16 | 16.33 | 16.66 | 16.67 | 16.99 | 17 | 17.32 | 17.33 | 17.34 | 17.66 | 17.67 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | - | - | 6 | 16 | - | 16 | 2 | 10 | 12 | - | 2 |
| 11 | 18* | 34 | 50 | 146 | 34 | 198 | 2 | 76 | 106 | 6 | 22 |
| 12 | - | 24 | 20 | 36 | 6 | 74 | 4 | 46 | 34 | 2 | 16 |
| BGC \GEC | 18 | 18.33 | 18.66 | 18.67 | 18.99 | 19 | 19.32 | 19.33 | 19.34 | 19.66 | 19.67 |
| 11 | 4 | 20 | 20 | 32 | 14 | 32 | - | 4 | 6 | - | - |
| 12 | 78 | 212 | 250 | 430 | 60 | 326 | 4 | 98 | 36 | 6 | 10 |
| 13 | 26 | 56 | 56 | 116 | 22 | 118 | 2 | 70 | 10 | 76 | 124 |
| 14 | - | - | - | - | - | 6 | - | 8 | - | 6 | 6 |
| BGC \GEC | 19.99 | 20 | 20.32 | 20.33 | 20.34 | 20.66 | 20.67 | 20.99 | 21 | 21.32 | 21.33 |
| 12 | 8 | 10 | 2 | 18 | 8 | 12 | 6 | - | - | - | - |
| 13 | 54 | 242 | 8 | 212 | 84 | 66 | 104 | 16 | 36 | 2 | 4 |
| 14 | 6 | 14 | - | 18 | 6 | 16 | 28 | 4 | 28 | - | 64 |
| BGC \GEC | 21.66 | 21.67 | 21.99 | 22 | | | | | | | |
| 13 | 8 | 2 | 2 | - | | | | | | | |
| 14 | 72 | 40 | 22 | 20 | | | | | | | |
| 15 | 2 | 2 | - | - | | | | | | | |

#### 5) TRADE-OFF BETWEEN SOFTWARE AND HARDWARE-ORIENTED IMPLEMENTATIONS

Table 10 shows the best implementation costs of 4,608 optimal BOGI-applicable PE classes. The best options for **BGC** and **GEC** are 10 and 16, respectively. However, both of the minimum costs cannot be provided at the same time. Thus, two options would be the best for (**BGC**, **GEC**): (11, 16) and (10, 16.33).

Considering that the smallest value of **GEC** is only possible with the option (11, 16), which is (**BGC**, **GEC**) of the GIFT S-box, this S-box is indeed the best option in hardware-oriented designs. Moreover, our analysis shows that all the S-boxes whose **BGC** is 10 have at least one fixed point while GIFT S-box does not have any fixed points. A fixed point may cause the entire block cipher to be vulnerable to Invariant Attacks [25]–[27]. Although the weakness can be mitigated by using proper round constants as presented in [28], providing an appropriate round constant could burden designers even further. As a result, we conclude (11, 16) is the best cost for implementing an optimal BOGI-applicable S-box.

Appendix A lists the available implementation options in each optimal BOGI-applicable PXE class. The best options are supported only by $B_{0,1,2,3}$.

## V. NOTABLE S-BOXES FOR GIFT

In this section, we investigate competitive S-boxes compared to the existing S-box for GIFT. To do so, we check the probability of the best differential/linear trails replacing the existing S-box while fixing the diffusion layer as the bit-permutation of GIFT. We apply all optimal BOGI-applicable S-boxes that are available for the bit-permutation of GIFT-64. For GIFT-128, we only consider the promising S-boxes in GIFT-64 instead of all the S-boxes.

Before starting this section, we define the following in order to measure the resistance.

*Definition 12 ($(\mathbf{DR}_i, \mathbf{LR}_i)_\gamma$): $\mathbf{DR}_i$ denotes the maximum probability of differential trails of i-round GIFT-$\gamma$ at the $log_2$ scale while $\mathbf{LR}_i$ denotes the maximum correlation potential of linear trails at the $log_2$ scale.*

Based on the results of $(\mathbf{DR}_i, \mathbf{LR}_i)_\gamma$, the minimum required number of rounds $r_{min}$ for the resistance against DC and LC can also be obtained. $r_{min}$ is defined as follows:

$$r_{min} = \min_i\{\, i \mid \mathbf{DR}_i \le -\gamma \text{ and } \mathbf{LR}_i \le -\gamma\}.$$

Note that if fewer rounds than $r_{min}$ were used, the corresponding cipher would obviously allow DC or LC.

The best differential/linear trails of GIFT-64 are investigated in [29]. The result showed that $r_{min}$ of GIFT-64 is 14. To be specific, GIFT-64 has $(\mathbf{DR}_{13}, \mathbf{LR}_{13})_{64} = (-62, -68)$ and $\mathbf{DR}_{14} = -68$. This implies that GIFT-64 requires at least 14 rounds to prevent single-trail differential and linear cryptanalysis.

### A. OPTIMAL BOGI-APPLICABLE XE CLASSES

Because the trail search is computationally intensive, we decrease the search space by introducing the XE relation. S-boxes that are included in an XE class have the same $(\mathbf{DR}_i, \mathbf{LR}_i)_\gamma$ because the corresponding $\mathrm{DDT}_S$ and $\mathrm{SQLAT}_S$ are invariant in an XE class. Moreover, $\mathrm{SQLAT}_S$ can be deduced from $\mathrm{DDT}_S$ with bijective Walsh transform as follows:

$$\mathrm{SQLAT}_S = \frac{1}{4}\sum_{x,y}(-1)^{a\cdot x \oplus b\cdot y}\mathrm{DDT}_S(x, y) \text{ [30].}$$

As a result, only XE classes whose DDT are distinct can be considered for trail searching. According to our results, 10,368 XE classes are included in optimal BOGI-applicable PXE classes, and all optimal BOGI-applicable XE classes have distinct DDT, and thus SQLAT as well.

However, some of the XE classes cannot interplay with the original bit-permutation of GIFT(i.e., the $B - B$ match occurs). This is because the mapping $\pi^k$ of GIFT is the identity. Among all the XE classes, only 1,728 XE classes can interplay with GIFT bit-permutation.

**TABLE 11.** Best differential probability and correlation potential of 13-round GIFT-64 variants at the $log_2$ scale. The entries denote the number of corresponding $XE_I$ classes.

| $DR_{13}$ \ $LR_{13}$ | -52.0 | -58.0 | -60.0 | -62.0 | -64.0 | -66.0 | -68.0 | -70.0 | -72.0 |
|---|---|---|---|---|---|---|---|---|---|
| -50.8 | 32 | - | - | - | - | - | 16 | 16 | - |
| -52.0 | - | - | - | - | 16 | - | 16 | - | - |
| -56.4 | 32 | - | 32 | - | 32 | - | - | - | - |
| -57.4 | - | - | 32 | - | - | - | - | - | - |
| -60.8 | 64 | - | 16 | 16 | - | 32 | 80 | 16 | - |
| -61.7 | 64 | - | - | - | - | - | - | - | - |
| -61.8 | 16 | - | 16 | - | - | - | 32 | - | - |
| -62.0 | 16 | - | 48 | - | 48 | - | 64* | - | - |
| -62.4 | 48 | - | 16 | - | - | - | 32 | - | - |
| -62.8 | 144 | 16 | 112 | - | 32 | 32 | 32 | 16 | - |
| -63.4 | 16 | - | - | - | - | - | - | - | - |
| -64.0 | 64 | 32 | 32 | - | - | - | - | 32 | - |
| -64.4 | 16 | - | - | - | - | - | - | - | - |
| -65.8 | - | - | 16 | - | - | - | - | - | - |
| -66.4 | - | - | - | 16 | - | - | - | 32 | - |
| -66.8 | 16 | 16 | 32 | - | - | - | 16 | 16 | - |
| -67.8 | - | - | 16 | - | - | - | 16 | - | - |
| -68.0 | 16 | - | - | - | - | 16 | - | - | - |
| -68.4 | - | - | - | - | - | - | 16 | 16 | **16** |
| -70.0 | - | - | - | - | - | - | **16** | - | - |
| -71.8 | 16 | - | - | - | - | - | - | - | - |

*Observation 6: Optimal BOGI-applicable 4-bit S-boxes have one of 10,368 distinct (*DDT, SQLAT*). Among them, only 1,728 distinct (*DDT, SQLAT*) can interplay with a given BOGI-permutation.*

Let $XE_I$ classes denote the corresponding XE classes whose DDT can adopt the BOGI-permutation as an identity. Now, we can consider only 1,728 $XE_I$ classes for every variant of GIFT-64. It should be noted that the considered number is the same for GIFT-128 variants.

### B. RESISTANCE OF GIFT-64 VARIANTS AGAINST DC AND LC

As mentioned above, $r_{min}$ of GIFT-64 is 14. Thus, we focus on 13-round trails to check if the less $r_{min} \leq 13$ can be possible with other BOGI-applicable S-boxes. We searched the best trails based on the Branch&Bound technique presented in [31], which is relatively fast for bit-permutation based SPN ciphers.

Table 11 shows $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ obtained with the 1,728 $XE_I$ classes. One can easily see that 192 $XE_I$ classes provide $\mathsf{DR}_{13}$ and $\mathsf{LR}_{13} \leq -64$ despite of only using 13 rounds(i.e., $r_{min} = 13$). Since there is a trade-off between $\mathsf{DR}_{13}$ and $\mathsf{LR}_{13}$, one can choose the two best options as $(-68.4, -72)$ and $(-70, -68)$.

Appendix B shows $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ which can be supported by each PXE class. Only $B_{4,5,6,7,12,13,16,17}$ have $r_{min} = 13$, and the two best options can be provided by $B_{4,5,12,13}$ among them. Because the bit-permutation of GIFT-64 is not involutory, an S-box $S$ and its inverse $S^{-1}$ do not always have the same $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$. However, despite the asymmetry, a PXE class and the inverse PXE class have the same results of $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ on the whole.

### C. XE-PE INTERSECTION IN A PXE CLASS

In this subsection, we introduce the XE-PE intersection in a PXE class. When selecting the best S-boxes in an optimal BOGI-applicable PXE class, this intersection allows independent consideration of $(\mathsf{DR}_i, \mathsf{LR}_i)_\gamma$, and (BCG, GEC).

According to Proposition 2, a non-empty intersection of an XE class and PE class exists as long as they are included in the same PXE class. Thus, the BOGI-applicable S-boxes can always be selected with any available combinations of $(\mathsf{DR}_i, \mathsf{LR}_i)_\gamma$, and (BGC, GEC).

*Proposition 2: There always exist S-boxes included both in a given XE class and PE class as long as the XE class and PE class are included in the same PXE class. We denote the non-empty intersection as* XE-PE intersection.

*Proof:* Assume that there exists a non-empty PE class $\mathcal{P}$ and an XE class $\mathcal{X}$ in a PXE class $\mathcal{PX}$ such that $\mathcal{P} \cap \mathcal{X} = \emptyset$. Let two S-boxes $S_\mathcal{P} \in \mathcal{P}$ and $S_\mathcal{X} \in \mathcal{X}$. Because $S_\mathcal{P}$, $S_\mathcal{X} \in \mathcal{PX}$, it follows that

$$S_\mathcal{X}(x) = P_{out} S_\mathcal{P}(P_{in}(x \oplus c_{in})) \oplus c_{out}$$

for some two bit-permutation matrices $P_{in}$ and $P_{out}$ over $\mathbb{F}_2^{4\times4}$, and $c_{in}$ and $c_{out}$ over $\mathbb{F}_2^4$. Let $S'_\mathcal{X} \in \mathcal{X}$ be an S-box satisfying

$$S_\mathcal{X}(x) = S'_\mathcal{X}(x \oplus c_{in}) \oplus c_{out}.$$

Because $S'_\mathcal{X}(x \oplus c_{in}) \oplus c_{out} = P_{out} S_\mathcal{P}(P_{in}(x \oplus c_{in})) \oplus c_{out}$, and thus $S'_\mathcal{X}(y) = P_{out} S_\mathcal{P}(P_{in}(y))$ *where* $y = x \oplus c_{in}$, it follows that $S'_\mathcal{X} \in \mathcal{X}$ and $S'_\mathcal{X} \in \mathcal{P}$. This contradicts the assumption that $\mathcal{P} \cap \mathcal{X} = \emptyset$. □

Note that, a non-empty intersection obviates the need to consider non-best options of $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ or (BGC, GEC).

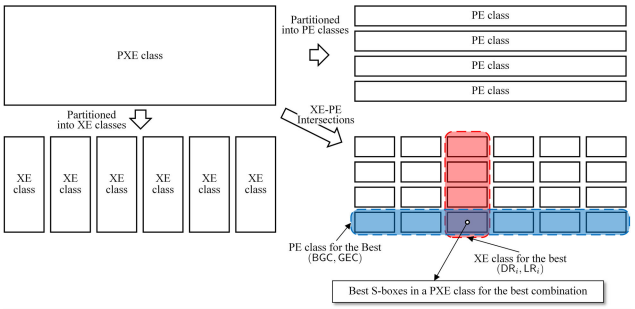


**FIGURE 3.** Method for selecting the best S-boxes in an optimal BOGI-applicable PXE class.

**TABLE 12.** Best options of $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ and (BGC, GEC) and the number of corresponding $\mathrm{XE}_I$, PE classes. The best options of $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ and (BGC, GEC) appear in bold. The highlighted $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ have $r_{min} = 13$.

| PXE class | $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ : # $\mathrm{XE}_I$ classes | (BGC, GEC) : # PE classes |
|---|---|---|
| $B_{0,1}$ | (-62.8, -66.0): 8 | **(10.0, 16.66)**: 1 |
| | (-62.0, -68.0): 16 | **(11.0, 16.0)**: 4 |
| $B_{2,3}$ | (-65.8, -60.0): 8 | **(10.0, 16.66)**: 2 |
| | (-62.8, -70.0): 8 | **(11.0, 16.0)**: 5 |
| $B_{4,5}$ | **(-68.4,-72.0)**: 8 | (11.0, 18.33): 2 |
| | | (12.0, 18.0): 8 |
| $B_{6,7}$ | (-66.8, -68.0): 8 | (11.0, 18.33): 2 |
| | (-64.0, -70.0): 16 | (12.0, 18.0): 4 |
| $B_{8,9}$ | (-62.4, -52.0): 8 | (12.0, 20.33): 4 |
| | (-56.4, -64.0): 16 | (13.0, 20.0): 9 |
| $B_{10,11}$ | (-64.0, -60.0): 8 | (11.0, 18.33): 2 |
| | (-62.8, -68.0): 8 | (12.0, 18.0): 15 |
| $B_{12,13}$ | **(-70.0, -68.0)**: 8 | (11.0, 18.33): 4 |
| | | (12.0, 18.0): 11 |
| $B_{14,15}$ | (-66.8, -60.0): 16 | (12.0, 19.99): 1 |
| | | (13.0, 19.33): 4 |
| $B_{16,17}$ | (-71.8, -52.0): 8 | (12.0, 19.66): 3 |
| | (-68.4, -70.0): 8 | (13.0, 19.0): 3 |
| $B_{18,19}$ | (-64.0, -52.0): 16 | (13.0, 21.33): 2 |
| | | (14.0, 21.0): 9 |

Figure 3 visualizes the XE-PE intersection capable of supporting the best $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ and (BGC, GEC) in a PXE class.

Based on the results in Table 11 and Table 10, we deduce the best combinations of implementation cost and the resistance against differential and linear cryptanalysis. They are summarized in Table 12. Each corresponding XE-$\mathrm{PE}_I$ intersection consists of only 1 or 2 S-boxes depending on the PXE class.

### D. NOTABLE S-BOXES FOR GIFT-64 STRUCTURE

#### 1) TRADE-OFF BETWEEN CRYPTOGRAPHIC STRENGTH AND EFFICIENCY

Table 12 presents that trade-offs exist between $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ and (BGC, GEC). The best options of (BGC, GEC) are supported by $B_{0,1,2,3}$. On the other hand, the optimal BOGI-applicable PXE classes whose $r_{min} = 13$ are $B_{4,5,6,7,12,13,16,17}$.

#### 2) S-BOX PROVIDING THE BEST $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$

$B_{4,5}$ and $B_{12,13}$ provide the best $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-68.4, 72.0)$ and $(-70.0, -68.0)$, respectively. However, all the S-boxes with (BGC, GEC) = (11, 18.33) have at least one fixed point. Thus, as an alternative option, we could suggest 16 S-boxes with (BGC, GEC) = (12, 18) as follows:

(3, 14, 12, 0, 8, 13, 5, 2, 1, 4, 15, 9, 6, 11, 10, 7) in $B_4$
(9, 6, 4, 10, 8, 15, 3, 5, 7, 0, 14, 1, 2, 12, 13, 11) in $B_4$
(6, 8, 9, 5, 11, 13, 0, 2, 4, 3, 15, 10, 1, 14, 12, 7) in $B_4$
(6, 2, 13, 8, 9, 15, 0, 3, 1, 12, 11, 7, 10, 5, 4, 14) in $B_4$
(3, 12, 13, 0, 2, 15, 8, 6, 4, 10, 14, 1, 9, 5, 7, 11) in $B_4$
(12, 2, 4, 9, 11, 7, 1, 14, 3, 5, 15, 10, 0, 8, 6, 13) in $B_4$
(9, 14, 1, 4, 2, 7, 12, 11, 6, 0, 15, 3, 5, 8, 10, 13) in $B_4$
(12, 8, 1, 6, 3, 15, 10, 5, 7, 2, 11, 13, 0, 9, 4, 14) in $B_4$
(12, 6, 1, 8, 2, 9, 14, 5, 13, 3, 11, 4, 0, 15, 7, 10) in $B_5$
(6, 12, 7, 9, 8, 3, 0, 15, 1, 2, 11, 4, 14, 5, 13, 10) in $B_5$
(9, 11, 12, 6, 2, 7, 1, 8, 4, 0, 3, 15, 13, 14, 10, 5) in $B_5$
(3, 11, 4, 0, 8, 13, 7, 14, 6, 12, 9, 15, 1, 2, 10, 5) in $B_5$
(9, 2, 4, 11, 3, 12, 8, 5, 13, 0, 14, 7, 6, 15, 1, 10) in $B_5$
(6, 8, 1, 7, 14, 13, 0, 11, 3, 4, 12, 10, 9, 2, 15, 5) in $B_5$
(3, 8, 7, 0, 9, 6, 12, 15, 4, 11, 14, 13, 2, 5, 1, 10) in $B_5$
(12, 2, 9, 4, 14, 7, 3, 8, 1, 13, 6, 10, 0, 11, 15, 5) in $B_5$.

The above S-boxes support $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-68.4, 72.0)$ and no fixed points. Moreover, in $B_{12,13}$, 48 S-boxes support $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-70.0, 68.0)$, (BGC, GEC) = (12, 18) and have no fixed points. Although the cost of implementation in software increases slightly, these S-boxes can provide the best resistance against DC and LC, and thus the required number of rounds may be reduced relative to the current number of rounds. Because the number of rounds mainly affects the latency and throughput of the block cipher, designers may choose alternatives where speed measures, rather than the implementation costs, become the main consideration.

#### 3) S-BOX PROVIDING THE SAME PERFORMANCE AS THAT OF EXISTING GIFT-64 STRUCTURE

The results in Table 12 indicate a total of 128(=2×16×4) $\mathrm{XE}_I$-PE intersections in which all the S-boxes provide the same performance as that of the current S-box to GIFT-64. Each of the intersections consists of a single S-box, and thus the total number of these S-boxes is 128. Among them, 96 S-boxes without fixed points are presented in Appendix C.

#### 4) S-BOX PROVIDING BETTER PERFORMANCE THAN THAT OF EXISTING GIFT-64 STRUCTURE

Despite the trade-off between the cryptographic strength and efficiency, one can easily see that the $B_{2,3}$ can provide better $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-62.8, -70.0)$ than GIFT S-box within the same (BGC, GEC) = (11, 16). The total number of S-boxes included in these $\mathrm{XE}_I$-PE intersections is 80. Among the S-boxes, only 32 S-boxes have no fixed points. The S-boxes are presented in Appendix D.

**TABLE 13.** Available Implementation Costs (BGC, GEC) of Optimal BOGI-applicable PXE Classes.

| PXE class | Min BGC | Min GEC | (BGC, GEC) : # the corresponding PE classes |
|---|---|---|---|
| $B_{0,1}$ | 10 | 16 | **(10, 16.66)**: 1, (10, 16.67): 4, (10, 17): 5, (10, 17.33): 2, (10, 17.34): 4, **(11, 16)**: 4, (11, 16.33): 9, (11, 16.66): 11, (11, 16.67): 39, (11, 16.99): 10, (11, 17): 46, (11, 17.33): 17, (11, 17.34): 28, (11, 17.66): 2, (11, 17.67): 7, (11, 18): 1, (12, 16.33): 5, (12, 16.66): 6, (12, 16.67): 8, (12, 17): 21, (12, 17.32): 2, (12, 17.33): 14, (12, 17.34): 6, (12, 17.66): 1, (12, 17.67): 3 |
| $B_{2,3}$ | 10 | 16 | **(10, 16.66)**: 2, (10, 16.67): 4, (10, 17): 3, (10, 17.32): 1, (10, 17.33): 3, (10, 17.34): 2, (10, 17.67): 1, **(11, 16)**: 5, (11, 16.33): 8, (11, 16.66): 14, (11, 16.67): 34, (11, 16.99): 7, (11, 17): 53, (11, 17.32): 1, (11, 17.33): 21, (11, 17.34): 25, (11, 17.66): 1, (11, 17.67): 4, (11, 18): 1, (12, 16.33): 7, (12, 16.66): 4, (12, 16.67): 10, (12, 16.99): 3, (12, 17): 16, (12, 17.33): 9, (12, 17.34): 11, (12, 17.67): 5, (12, 18): 1 |
| $B_{4,5}$ | 11 | 18 | **(11, 18.33)**: 2, (11, 18.66): 3, (11, 18.67): 3, (11, 18.99): 1, (11, 19): 6, (11, 19.34): 1, **(12, 18)**: 8, (12, 18.33): 19, (12, 18.66): 26, (12, 18.67): 53, (12, 18.99): 9, (12, 19): 48, (12, 19.32): 1, (12, 19.33): 14, (12, 19.34): 2, (13, 18): 2, (13, 18.33): 7, (13, 18.66): 5, (13, 18.67): 21, (13, 18.99): 3, (13, 19): 18, (13, 19.32): 1, (13, 19.33): 2, (13, 19.34): 1 |
| $B_{6,7}$ | 11 | 18 | **(11, 18.33)**: 2, (11, 18.66): 2, (11, 18.67): 2, (11, 18.99): 3, (11, 19): 5, (11, 19.33): 1, (11, 19.34): 1, **(12, 18)**: 4, (12, 18.33): 21, (12, 18.66): 27, (12, 18.67): 44, (12, 18.99): 6, (12, 19): 45, (12, 19.32): 1, (12, 19.33): 15, (12, 19.34): 11, (13, 18): 5, (13, 18.33): 5, (13, 18.66): 4, (13, 18.67): 19, (13, 18.99): 3, (13, 19): 20, (13, 19.33): 8, (13, 19.34): 2 |
| $B_{8,9}$ | 12 | 20 | **(12, 20.33)**: 4, (12, 20.66): 1, (12, 20.67): 3, **(13, 20)**: 9, (13, 20.33): 19, (13, 20.66): 16, (13, 20.67): 27, (13, 20.99): 4, (13, 21): 14, (13, 21.32): 1, (14, 20): 1, (14, 20.33): 3, (14, 20.66): 7, (14, 20.67): 13, (14, 20.99): 2, (14, 21): 4 |
| $B_{10,11}$ | 11 | 18 | **(11, 18.33)**: 2, (11, 18.66): 2, (11, 18.67): 7, (11, 18.99): 2, (11, 19): 2, (11, 19.34): 1, **(12, 18)**: 15, (12, 18.33): 36, (12, 18.66): 34, (12, 18.67): 52, (12, 18.99): 8, (12, 19): 39, (12, 19.33): 11, (12, 19.34): 1, (13, 18): 2, (13, 18.33): 8, (13, 18.66): 13, (13, 18.67): 10, (13, 18.99): 2, (13, 19): 6, (13, 19.33): 2, (13, 19.34): 1 |
| $B_{12,13}$ | 11 | 18 | **(11, 18.33)**: 4, (11, 18.66): 3, (11, 18.67): 4, (11, 18.99): 1, (11, 19): 3, (11, 19.33): 1, **(12, 18)**: 11, (12, 18.33): 30, (12, 18.66): 38, (12, 18.67): 66, (12, 18.99): 7, (12, 19): 31, (12, 19.33): 9, (12, 19.34): 4, (13, 18): 4, (13, 18.33): 8, (13, 18.66): 6, (13, 18.67): 8, (13, 18.99): 3, (13, 19): 12, (13, 19.33): 2, (13, 19.34): 1 |
| $B_{14,15}$ | 12 | 19.33 | **(12, 19.99)**: 1, (12, 20): 1, (12, 20.32): 1, (12, 20.33): 4, (12, 20.34): 4, (12, 20.66): 5, **(13, 19.33)**: 4, (13, 19.66): 7, (13, 19.67): 18, (13, 19.99): 4, (13, 20): 49, (13, 20.32): 1, (13, 20.33): 59, (13, 20.34): 34, (13, 20.66): 17, (13, 20.67): 25, (13, 20.99): 4, (13, 21): 4, (14, 19.66): 1, (14, 19.99): 1, (14, 20): 2, (14, 20.33): 4, (14, 20.34): 3, (14, 20.66): 1, (14, 20.67): 1, (14, 21): 1 |
| $B_{16,17}$ | 12 | 19 | **(12, 19.66)**: 3, (12, 19.67): 5, (12, 19.99): 3, (12, 20): 4, (12, 20.33): 1, **(13, 19)**: 3, (13, 19.33): 17, (13, 19.66): 31, (13, 19.67): 44, (13, 19.99): 23, (13, 20): 63, (13, 20.32): 3, (13, 20.33): 28, (13, 20.34): 8, (14, 19): 3, (14, 19.33): 4, (14, 19.66): 2, (14, 19.67): 3, (14, 19.99): 2, (14, 20): 4, (14, 20.33): 2 |
| $B_{18,19}$ | 13 | 21 | **(13, 21.33)**: 2, (13, 21.66): 4, (13, 21.67): 1, (13, 21.99): 1, **(14, 21)**: 9, (14, 21.33): 32, (14, 21.66): 36, (14, 21.67): 20, (14, 21.99): 11, (14, 22): 10, (15, 21.66): 1, (15, 21.67): 1 |

**TABLE 14.** Available Resistances $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ of Optimal BOGI-applicable PXE Classes.

| PXE class | Min $\mathsf{DR}_{13}$ | Min $\mathsf{LR}_{13}$ | $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ : # the corresponding $\mathrm{XE}_I$ classes |
|---|---|---|---|
| $B_{0,1}$ | -62.8 | -68 | **(-62.8, -66)**: 8, (-62.8, -52): 8, (-62.4, -60): 8, **(-62, -68)**: 16, (-61.8, -60): 8, (-60.8, -68): 16, (-57.4, -60): 8, (-56.4, -60): 8, (-52, -64): 8, (-50.8, -52): 8 |
| $B_{2,3}$ | -65.8 | -70 | **(-65.8, -60)**: 8, **(-62.8, -70)**: 8, (-62.8, -60): 8, (-62.8, -52): 8, (-62, -68): 8, (-62, -64): 8, (-60.8, -70): 8, (-60.8, -66): 8, (-57.4, -60): 8, (-56.4, -60): 8, (-52, -68): 8, (-50.8, -70): 8 |
| $B_{4,5}$ | -68.4 | -72 | **(-68.4, -72)**: 8, (-68.4, -68): 8, (-68, -66): 8, (-68, -52): 8, (-67.8, -68): 8, (-67.8, -60): 8, (-62.8, -66): 8, (-62.8, -64): 16, (-62.8, -52): 8, (-62, -64): 16 |
| $B_{6,7}$ | -66.8 | -70 | **(-66.8, -68)**: 8, (-66.8, -58): 8, **(-64, -70)**: 16, (-62.8, -60): 16, (-62.8, -52): 16, (-61.7, -52): 32 |
| $B_{8,9}$ | -62.4 | -64 | **(-62.4, -52)**: 8, (-61.8, -52): 8, (-60.8, -60): 8, (-60.8, -52): 8, **(-56.4, -64)**: 1 |
| $B_{10,11}$ | -64 | -68 | **(-64, -60)**: 8, (-64, -58): 8, **(-62.8, -68)**: 8, (-62.8, -60): 8, (-62, -68): 8, (-62, -60): 8, (-61.8, -68): 8, (-60.8, -68): 8, (-60.8, -62): 8, (-60.8, -52): 16, (-50.8, -52): 8 |
| $B_{12,13}$ | -70 | -68 | **(-70, -68)**: 8, (-64, -60): 8, (-64, -58): 8, (-62.8, -68): 8, (-62.8, -60): 8,(-62, -60): 8, (-61.8, -68): 8, (-60.8, -68): 16, (-60.8, -66): 8, (-60.8, -52): 8, (-50.8, -68): 8 |
| $B_{14,15}$ | -66.8 | -60 | **(-66.8, -60)**: 16, (-66.8, -52): 8, (-64, -52): 16, (-62.8, -60): 16, (-62.8, -52): 24, (-62, -60): 8, (-62, -52): 8 |
| $B_{16,17}$ | -71.8 | -70 | **(-71.8, -52)**: 8, **(-68.4, -70)**: 8, (-66.8, -70): 8, (-66.4, -70): 16, (-66.4, -62): 8, (-64.4, -52): 8, (-62.8, -58): 8, (-62.4, -68): 16, (-62.4, -52): 16 |
| $B_{18,19}$ | -64 | -52 | **(-64, -52)**: 16, (-63.4, -52): 8, (-62.8, -52): 8, (-56.4, -52): 16 |

However, we do not insist that GIFT designers should have used those better S-boxes. As presented in Table 9, *CarL*1 of $B_{2,3}$ is worse than $B_{0,1}$. Thus, although the $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$ is improved to $(-62.8, -70.0)$ from the original $(-62.0, -68)$, thorough analyses have to be conducted in order to "well-replace" the GIFT S-box.

### E. NOTABLE S-BOXES FOR GIFT-128 STRUCTURE

The number of $\mathrm{XE}_I$ classes(1,728) is still infeasible for larger block ciphers such as GIFT-128 because trail searching tends to take much more time than 64-bit block ciphers. However, considering only the S-boxes whose performance is not worse than the current S-box in GIFT-64 structure, we can deduce the corresponding $(\mathsf{DR}_i, \mathsf{LR}_i)_{128}$ of GIFT-128 variants with 48 $\mathrm{XE}_I$ classes(16 for the same performance and 32 for better performance).

For GIFT-128 structure, we investigate 12-round trails because searching longer trails requires significant time,[7]

[7]Each searching for the $\mathrm{XE}_I$ classes takes from 5 min to 13 days on a personal computer.

**TABLE 15.** S-box of which the Performance Equals that of the Existing S-box in GIFT-64 Structure.

| In $B_0$, | | In $B_1$, | |
|---|---|---|---|
| • $(DR_{12}, LR_{12})_{128}$ = (-76.4, -74.0) | • $(DR_{12}, LR_{12})_{128}$ = (-60.4, -72.0) | • $(DR_{12}, LR_{12})_{128}$ = (-73.4, -70.0) | (7, 0, 8, 14, 1, 12, 11, 5, 10, 15, 6, 3, 13, 2, 4, 9) |
| (1, 4, 12, 15, 11, 13, 0, 2, 6, 10, 9, 3, 8, 7, 5, 14) | (1, 7, 14, 12, 8, 4, 3, 9, 2, 13, 11, 0, 15, 10, 6, 5) | (3, 4, 7, 8, 9, 2, 12, 15, 0, 11, 14, 13, 10, 5, 1, 6) | (12, 9, 0, 5, 14, 3, 7, 8, 2, 4, 13, 10, 1, 15, 11, 6) |
| (8, 3, 1, 14, 5, 15, 12, 0, 4, 6, 11, 13, 9, 10, 2, 7) | (1, 10, 8, 7, 12, 15, 5, 0, 4, 6, 11, 13, 9, 3, 2, 14) | (7, 8, 11, 12, 0, 3, 13, 6, 2, 1, 4, 15, 9, 14, 10, 5) | (14, 0, 4, 9, 13, 11, 2, 5, 1, 12, 8, 7, 3, 6, 15, 10) |
| (8, 14, 7, 5, 1, 4, 10, 9, 2, 13, 11, 0, 15, 3, 6, 12) | (8, 4, 5, 15, 11, 13, 0, 2, 6, 3, 9, 10, 1, 14, 12, 7) | (14, 5, 8, 11, 0, 15, 3, 4, 1, 6, 13, 2, 7, 12, 10, 9) | (9, 4, 3, 8, 0, 11, 10, 5, 13, 2, 6, 15, 14, 7, 1, 12) |
| (4, 14, 9, 0, 1, 13, 15, 2, 3, 8, 12, 5, 10, 7, 6, 11) | (2, 14, 9, 4, 1, 7, 12, 11, 5, 0, 6, 3, 15, 8, 10, 13) | (6, 12, 7, 9, 1, 2, 8, 15, 0, 10, 11, 4, 14, 5, 13, 3) | (13, 2, 0, 9, 8, 1, 3, 14, 11, 6, 7, 12, 4, 15, 10, 5) |
| (8, 4, 7, 10, 11, 1, 5, 12, 2, 15, 14, 3, 13, 6, 0, 9) | (4, 2, 8, 15, 13, 1, 7, 10, 11, 12, 14, 9, 3, 6, 0, 5) | (7, 0, 14, 13, 8, 6, 9, 3, 2, 12, 1, 10, 4, 11, 15, 5) | (14, 5, 0, 15, 1, 12, 13, 6, 2, 11, 9, 4, 7, 8, 10, 3) |
| (8, 5, 4, 9, 6, 15, 11, 0, 1, 12, 14, 2, 3, 10, 13, 7) | (4, 3, 1, 6, 10, 15, 9, 12, 2, 5, 14, 8, 13, 0, 7, 11) | (11, 0, 8, 6, 5, 15, 14, 1, 4, 7, 13, 10, 3, 9, 2, 12) | (11, 4, 0, 13, 5, 9, 15, 3, 2, 7, 12, 10, 14, 8, 1, 6) |
| (2, 4, 8, 15, 11, 1, 7, 12, 13, 10, 14, 9, 5, 6, 0, 3) | (4, 8, 11, 6, 7, 1, 9, 12, 2, 15, 14, 3, 13, 10, 0, 5) | | (12, 0, 6, 10, 1, 14, 8, 5, 13, 11, 3, 4, 2, 7, 15, 9) |
| (2, 5, 1, 6, 12, 15, 9, 10, 4, 3, 14, 8, 11, 0, 7, 13) | (4, 9, 8, 5, 10, 15, 7, 0, 1, 12, 14, 2, 3, 6, 13, 11) | • $(DR_{12}, LR_{12})_{128}$ = (-73.4, -68.0) | (13, 8, 0, 6, 2, 4, 12, 11, 14, 1, 7, 10, 3, 15, 9, 5) |
| (4, 14, 9, 2, 1, 7, 10, 13, 3, 0, 6, 5, 15, 8, 12, 11) | (8, 14, 5, 0, 1, 13, 15, 2, 3, 4, 12, 9, 6, 11, 10, 7) | (11, 0, 4, 13, 5, 15, 9, 3, 2, 12, 7, 10, 14, 1, 8, 6) | (3, 11, 8, 4, 6, 12, 1, 15, 0, 13, 7, 14, 5, 2, 10, 9) |
| (1, 4, 12, 10, 11, 7, 2, 13, 6, 15, 3, 9, 0, 8, 5, 14) | (1, 10, 4, 12, 6, 15, 3, 9, 2, 13, 11, 7, 5, 0, 8, 14)* | (12, 6, 0, 10, 1, 8, 14, 5, 13, 3, 11, 4, 2, 15, 7, 9) | (11, 7, 4, 12, 0, 14, 3, 9, 1, 8, 2, 15, 6, 5, 13, 10) |
| (2, 9, 4, 12, 5, 15, 3, 10, 1, 14, 11, 7, 6, 0, 8, 13) | (1, 13, 8, 7, 2, 4, 15, 10, 14, 6, 11, 0, 9, 3, 12, 5) | (13, 0, 8, 6, 2, 12, 4, 11, 14, 7, 1, 10, 3, 9, 15, 5)** | (13, 4, 10, 7, 0, 3, 15, 8, 2, 14, 9, 1, 11, 5, 12, 6) |
| (2, 14, 8, 7, 1, 4, 15, 9, 13, 5, 11, 0, 10, 3, 12, 6) | (2, 4, 12, 9, 11, 7, 1, 14, 5, 15, 3, 10, 0, 8, 6, 13) | (9, 4, 0, 11, 3, 8, 10, 5, 13, 2, 14, 7, 6, 15, 1, 12) | (7, 4, 8, 14, 0, 9, 11, 5, 10, 13, 3, 1, 15, 2, 6, 12) |
| | | (13, 2, 8, 1, 0, 9, 3, 14, 11, 6, 4, 15, 7, 12, 10, 5) | (9, 11, 0, 7, 12, 6, 5, 8, 2, 4, 13, 14, 1, 15, 10, 3) |
| • $(DR_{12}, LR_{12})_{128}$ = (-74.8, -74.0) | • $(DR_{12}, LR_{12})_{128}$ = (-59.0, -72.0) | (14, 5, 1, 12, 0, 15, 13, 6, 2, 11, 7, 8, 9, 4, 10, 3) | (11, 13, 1, 2, 0, 14, 12, 5, 4, 6, 8, 15, 9, 3, 7, 10) |
| (4, 8, 10, 6, 2, 13, 12, 1, 9, 7, 15, 0, 3, 14, 5, 11) | (2, 4, 5, 11, 8, 7, 9, 14, 12, 10, 15, 0, 6, 1, 3, 13) | | (6, 0, 7, 11, 1, 14, 8, 13, 12, 10, 9, 4, 2, 5, 15, 3) |
| (4, 11, 8, 5, 1, 13, 15, 3, 7, 10, 2, 12, 14, 0, 9, 6) | (2, 13, 11, 12, 1, 7, 14, 0, 4, 3, 8, 6, 15, 9, 5, 10) | • $(DR_{12}, LR_{12})_{128}$ = (-72.8, -68.0) | (7, 2, 14, 1, 8, 4, 9, 15, 0, 12, 13, 10, 6, 11, 3, 5) |
| (8, 6, 13, 0, 3, 12, 4, 10, 2, 15, 14, 1, 5, 9, 11, 7) | (4, 10, 8, 15, 9, 6, 3, 5, 7, 0, 14, 1, 2, 12, 13, 11) | (6, 0, 8, 7, 14, 13, 1, 11, 3, 5, 4, 10, 9, 2, 15, 12) | (11, 4, 8, 13, 5, 3, 14, 2, 0, 7, 6, 10, 15, 9, 1, 12) |
| (1, 2, 10, 9, 8, 13, 3, 4, 12, 6, 15, 5, 7, 11, 0, 14) | (1, 6, 13, 8, 10, 9, 0, 3, 2, 12, 11, 7, 15, 5, 4, 14) | (13, 2, 10, 12, 1, 11, 7, 4, 0, 14, 15, 9, 6, 5, 8, 3) | (3, 4, 7, 8, 0, 11, 14, 13, 9, 2, 12, 15, 10, 5, 1, 6) |
| (1, 4, 8, 15, 14, 13, 5, 6, 7, 11, 2, 12, 10, 0, 9, 3) | (8, 2, 3, 9, 1, 13, 10, 4, 5, 6, 15, 12, 14, 11, 0, 7) | (14, 4, 1, 2, 7, 8, 9, 15, 0, 3, 6, 13, 11, 5, 12, 10) | (7, 8, 11, 12, 2, 1, 4, 15, 0, 3, 13, 6, 9, 14, 10, 5) |
| (8, 6, 13, 1, 3, 9, 0, 10, 2, 5, 11, 14, 15, 12, 4, 7) | (8, 4, 1, 15, 7, 13, 12, 6, 14, 11, 2, 5, 3, 0, 9, 10) | (3, 11, 8, 4, 0, 13, 7, 14, 6, 12, 1, 15, 5, 2, 10, 9) | (14, 5, 8, 11, 1, 6, 13, 2, 0, 15, 3, 4, 7, 12, 10, 9) |
| (2, 12, 8, 15, 9, 6, 5, 3, 7, 0, 14, 1, 4, 10, 11, 13) | (1, 12, 8, 6, 10, 3, 15, 5, 7, 2, 11, 13, 0, 9, 4, 14) | (11, 7, 4, 12, 1, 8, 2, 15, 0, 14, 3, 9, 6, 5, 13, 10) | |
| (4, 2, 3, 13, 8, 7, 9, 14, 10, 12, 15, 0, 6, 1, 5, 11) | (2, 4, 14, 11, 13, 7, 9, 0, 1, 15, 8, 5, 6, 12, 3, 10) | (13, 4, 10, 7, 2, 14, 9, 1, 0, 3, 15, 8, 11, 5, 12, 6) | • $(DR_{12}, LR_{12})_{128}$ = (-71.4, -70.0) |
| (4, 11, 13, 10, 1, 7, 14, 0, 2, 5, 8, 6, 15, 9, 3, 12) | (2, 8, 5, 12, 1, 7, 14, 11, 9, 3, 15, 6, 10, 4, 0, 13) | | (7, 4, 0, 9, 8, 14, 11, 5, 10, 13, 15, 2, 3, 1, 6, 12) |
| (1, 4, 13, 11, 14, 7, 10, 0, 2, 15, 8, 6, 5, 12, 3, 9) | (4, 10, 13, 0, 3, 12, 8, 6, 2, 15, 14, 1, 9, 5, 7, 11) | • $(DR_{12}, LR_{12})_{128}$ = (-72.8, -64.0) | (9, 11, 12, 6, 0, 7, 5, 8, 2, 4, 1, 15, 13, 14, 10, 3) |
| (1, 8, 6, 12, 2, 7, 13, 11, 10, 3, 15, 5, 9, 4, 0, 14) | (8, 4, 6, 10, 2, 13, 12, 1, 5, 11, 15, 0, 3, 14, 9, 7) | (6, 3, 8, 4, 14, 9, 1, 15, 0, 5, 7, 10, 13, 2, 11, 12) | (11, 13, 0, 14, 1, 2, 12, 5, 4, 6, 9, 3, 8, 15, 7, 10) |
| (2, 12, 8, 5, 9, 3, 15, 6, 7, 1, 11, 14, 0, 10, 4, 13) | (8, 7, 4, 9, 1, 13, 15, 3, 11, 6, 2, 12, 14, 0, 5, 10) | (13, 0, 10, 15, 1, 6, 7, 8, 2, 14, 12, 9, 11, 5, 4, 3) | (7, 8, 0, 14, 1, 11, 12, 5, 10, 6, 15, 3, 13, 4, 2, 9) |
| | | (14, 0, 1, 6, 7, 11, 9, 12, 4, 3, 2, 13, 8, 5, 15, 10) | (12, 0, 9, 5, 14, 7, 3, 8, 2, 13, 4, 10, 1, 11, 15, 6) |
| | | | (14, 4, 0, 9, 13, 2, 11, 5, 1, 8, 12, 7, 3, 15, 6, 10) |

and $(DR_{12}, LR_{12})_{128}$ of GIFT-128 is (−60.4, −72), which implies GIFT-128 requires more than 24 rounds to become resistant against DC.

Appendix C and D present $(DR_{12}, LR_{12})_{128}$ of GIFT-128 variants we consider. The results show that $(DR_{12}, LR_{12})_{128}$ can be improved up to (−76.4, −74.0). Unlike $(DR_{13}, LR_{13})_{64}$, a PXE class and its inverse PXE class have distinct results of $(DR_{12}, LR_{12})_{128}$. Moreover, S-boxes that provide better performance in GIFT-64 structure cannot always guarantee better performance in GIFT-128. This implies that choosing a dedicated S-box for each version of GIFT may guarantee more promising performance.

### F. EXTENSION TO OTHER BOGI-BASED BLOCK CIPHERS

The results of all our analyses except for $(DR_i, LR_i)_\gamma$ can be reused for other BOGI-based block ciphers. However, as we show in Observation 6, only 10,368 BOGI-applicable XE classes can be considered rather than all the S-boxes. Moreover, the number can decrease again to 1,728 after determining the structure of $\mathcal{P}^j_{mix}$. Therefore, our findings are expected to help designers analyze $(DR_i, LR_i)_\gamma$ in their structures.

## VI. CONCLUSION

In this paper, we conducted an exhaustive search for 4-bit BOGI-applicable S-boxes. By classifying the PXE classes with respect to their differential uniformity and linearity, we suggested 20 optimal BOGI-applicable PXE classes. We evaluated these PXE classes, and presented their generalized properties, which have not been analyzed before. Moreover, by partitioning the PXE classes into PE and XE classes, we explored their implementation cost and resistance against single-trail differential and linear cryptanalysis. Based on our investigations, we suggested notable S-boxes for both versions of GIFT. Although we only concentrated on GIFT, we expect our study to form the basis for extensions to other BOGI-based ciphers in future.

## APPENDIX A
## AVAILABLE IMPLEMENTATION COSTS (BGC, GEC) OF OPTIMAL BOGI-APPLICABLE PXE CLASSES

- The implementation cost of GIFT S-box is deduced as (BGC, GEC) = (11, 16).
- The results in boldface are the best results for software or hardware implementations in each PXE class.

See Table 13.

## APPENDIX B
## AVAILABLE RESISTANCES $(DR_{13}, LR_{13})_{64}$ OF OPTIMAL BOGI-APPLICABLE PXE CLASSES

- GIFT S-box has the underlined result **(−62, −68)**.
- The results in boldface are the best resistances against DC or LC in each PXE class.
- The results that reduce the minimum required number of rounds $r_{min}$ to 13 are highlighted.

See Table 14.

## APPENDIX C
## S-BOX OF WHICH THE PERFORMANCE EQUALS THAT OF THE EXISTING S-BOX IN GIFT-64 STRUCTURE

The following S-boxes can provide the same $(DR_{13}, LR_{13})_{64}$, and (BGC, GEC) as GIFT S-box. Moreover, all of the security properties we consider in this study are equivalent to those

**TABLE 16.** S-box of which the Performance is Better than that of the Existing S-box in GIFT-64 Structure.

| In $B_2$, | In $B_3$, |
|---|---|
| • $(DR_{12}, LR_{12})_{128}$ = (-69.8, -66.0) | • $(DR_{12}, LR_{12})_{128}$ = (-61.8, -66.0) | • $(DR_{12}, LR_{12})_{128}$ = (-71.0, -64.0) | (5, 2, 6, 9, 0, 11, 13, 14, 10, 1, 12, 15, 7, 8, 3, 4) |
| (1, 15, 4, 2, 12, 0, 11, 9, 13, 10, 8, 7, 6, 3, 5, 14) | (1, 8, 12, 6, 11, 2, 7, 13, 10, 15, 3, 5, 4, 9, 0, 14) | (7, 8, 3, 4, 10, 1, 12, 15, 0, 11, 13, 14, 5, 2, 6, 9) | (10, 5, 4, 2, 12, 9, 3, 15, 0, 14, 7, 1, 11, 6, 13, 8) |
| (8, 6, 13, 11, 5, 9, 2, 0, 4, 3, 1, 14, 15, 10, 12, 7) | (2, 11, 15, 5, 8, 1, 4, 14, 9, 12, 0, 6, 7, 10, 3, 13) | (14, 0, 1, 7, 6, 11, 8, 13, 5, 10, 2, 4, 9, 12, 15, 3) | (5, 0, 3, 13, 2, 14, 12, 11, 10, 7, 9, 6, 4, 8, 15, 1) |
| (1, 15, 7, 10, 6, 0, 12, 9, 4, 8, 2, 13, 11, 3, 5, 14) | (2, 8, 15, 1, 14, 4, 5, 11, 12, 7, 0, 6, 9, 10, 3, 13) | (7, 10, 6, 9, 8, 4, 1, 15, 0, 5, 13, 3, 14, 2, 11, 12) | (10, 5, 0, 14, 6, 3, 11, 12, 4, 8, 13, 1, 9, 15, 7, 2) |
| (2, 12, 4, 9, 5, 3, 15, 10, 7, 11, 1, 14, 8, 0, 6, 13) | (4, 14, 9, 7, 8, 2, 3, 13, 10, 1, 6, 0, 15, 12, 5, 11) | (14, 0, 5, 10, 12, 11, 3, 6, 1, 13, 8, 4, 2, 7, 15, 9) | (10, 3, 0, 14, 5, 6, 11, 9, 1, 12, 13, 7, 8, 15, 4, 2) |
| (2, 5, 1, 15, 9, 6, 12, 10, 7, 8, 4, 3, 14, 0, 11, 13) | (4, 14, 10, 1, 2, 8, 15, 6, 3, 13, 12, 0, 9, 7, 5, 11) | (11, 9, 5, 6, 0, 14, 10, 3, 4, 2, 8, 15, 13, 7, 1, 12) | (5, 0, 10, 13, 8, 14, 4, 2, 9, 7, 3, 12, 6, 11, 15, 1) |
| (4, 3, 7, 9, 15, 0, 10, 12, 1, 14, 2, 5, 8, 6, 13, 11) | (8, 2, 6, 13, 14, 4, 3, 10, 15, 1, 0, 12, 5, 11, 9, 7) | (13, 10, 0, 5, 2, 4, 14, 8, 12, 3, 7, 9, 1, 15, 11, 6) | (5, 8, 10, 1, 0, 11, 13, 2, 12, 3, 6, 15, 7, 14, 9, 4) |
| (4, 9, 1, 14, 15, 0, 2, 12, 13, 3, 8, 5, 10, 6, 7, 11) | (1, 2, 10, 15, 11, 8, 4, 3, 6, 12, 9, 5, 13, 7, 0, 14) | (13, 2, 0, 11, 10, 1, 5, 8, 9, 4, 7, 14, 6, 15, 12, 3) | (10, 9, 1, 6, 5, 12, 2, 15, 0, 14, 7, 13, 11, 3, 4, 8) |
| (8, 5, 13, 2, 3, 12, 14, 0, 1, 15, 4, 9, 6, 10, 11, 7) | (8, 11, 3, 6, 2, 1, 13, 10, 15, 5, 0, 12, 4, 14, 9, 7) | (11, 3, 4, 8, 0, 14, 7, 13, 5, 12, 2, 15, 10, 9, 1, 6) | |

of GIFT S-box. In other words, the following 96 BOGI-applicable S-boxes provide:

- $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-62.0, -68.0)$
- $(\mathsf{BGC}, \mathsf{GEC}) = (11, 16)$
- No fixed points.

An additional 32 S-boxes that include fixed points provide the same $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$, and (BGC, GEC) as those listed above. Here, * denotes GIFT S-box, and ** denotes its inverse.

See Table 15.

## APPENDIX D
## S-BOX OF WHICH THE PERFORMANCE IS BETTER THAN THAT OF THE EXISTING S-BOX IN GIFT-64 STRUCTURE

The following 32 optimal BOGI-applicable S-boxes provide:

- $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64} = (-62.8, -70.0)$
- $(\mathsf{BGC}, \mathsf{GEC}) = (11, 16)$
- No fixed points.

Note that $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$, $(\mathsf{DR}_{12}, \mathsf{LR}_{12})_{128}$, and (BGC, GEC) of GIFT S-box are $(-62.0, -68.0)$, $(-60.4, -72)$, and $(11, 16)$, respectively. An additional 8 S-boxes that include fixed points provide the same $(\mathsf{DR}_{13}, \mathsf{LR}_{13})_{64}$, and (BGC, GEC) as those listed above.

See Table 16.

## REFERENCES

[1] S. Banik, "GIFT: A small present," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.*, Cham, Switzerland: Springer, 2017, pp. 321–345.
[2] A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi, and Y. Sasaki, "ESTATE: A lightweight and low energy authenticated encryption mode," *IACR Trans. Symmetric Cryptol.*, vol. 2020, pp. 350–389, Jun. 2020.
[3] S. Banik, "GIFT-COFB. Submission to NIST LwC standardization process (round 1)," NIST, Gaithersburg, MD, USA, Tech. Rep., 2019.
[4] A. Chakraborti, N. Datta, A. Jha, S. Mitragotri, and M. Nandi, "From combined to hybrid: Making feedback-based AE even smaller," *IACR Trans. Symmetric Cryptol.*, vol. 2020, pp. 417–445, Jun. 2020.
[5] A. Chakraborti, "Lotus-aead and locus-aead. Submission to NIST LwC standardization process (round 1)," NIST, Gaithersburg, MD, USA, Tech. Rep., 2019.
[6] S. Banik, "SUNDAE-GIFT. Submission to NIST LwC standardization process (round 1)," NIST, Gaithersburg, MD, USA, Tech. Rep., 2019.
[7] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *Proc. Int. workshop Cryptograph. Hardw. Embedded Syst.*, Berlin, Germany: Springer, 2007, pp. 450–466.
[8] G. Leander and A. Poschmann, "On the classification of 4 bit s-boxes," in *Proc. Int. Workshop Arithmetic Finite Fields*. Berlin, Germany: Springer, 2007, pp. 159–176.
[9] W. Zhang, Z. Bao, V. Rijmen, and M. Liu, "A new classification of 4-bit optimal S-boxes and its application to present, rectangle and spongent," in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 2015, pp. 494–515.
[10] M.-J. O. Saarinen, "Cryptographic analysis of all 4×4-bit s-boxes," in *Proc. Int. Workshop Sel. Areas Cryptogr.*, Berlin, Germany: Springer, 2011, pp. 118–133.
[11] L. Cheng, W. Zhang, and Z. Xiang, "A new cryptographic analysis of 4-bit S-boxes," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, Cham, Switzerland: Springer, 2015, pp. 144–164.
[12] M. Ullrich, "Finding optimal bitsliced implementations of 4×4-bit S-boxes," in *Proc. SKEW Symmetric Key Encryption Workshop*, Copenhagen, Denmark, 2011, pp. 16–17.
[13] K. Stoffelen, "Optimizing s-box implementations for several criteria using SAT solvers," in *Proc. Int. Conf. Fast Softw. Encryption*. Berlin, Germany: Springer, 2016, pp. 140–160.
[14] Z. Bao, J. Guo, S. Ling, and Y. Sasaki, "PEIGEN—A platform for evaluation, implementation, and generation of S-boxes," *IACR Trans. Symmetric Cryptol.*, vol. 2019, pp. 330–394, Mar. 2019.
[15] J. Jean, T. Peyrin, S. M. Sim, and J. Tourteaux, "Optimizing implementations of lightweight building blocks," *IACR Trans. Symmetric Cryptol.*, vol. 2017, pp. 130–168, Dec. 2017.
[16] C. S. Lorens, "Invertible Boolean functions," *IEEE Trans. Electron. Comput.*, vol. EC-13, no. 5, pp. 529–541, Oct. 1964.
[17] M. A. Harrison, "On the classification of Boolean functions by the general linear and affine groups," *J. Soc. Ind. Appl. Math.*, vol. 12, no. 2, pp. 285–299, Jun. 1964.
[18] K. Nyberg, "Differentially uniform mappings for cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techniques*. Berlin, Germany: Springer, 1993, pp. 55–64.
[19] K. Nyberg, "S-boxes and round functions with controllable linearity and differential uniformity," in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 1994, pp. 111–130.
[20] A. Bogdanov, M. Kneževic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "Spongent: A lightweight hash function," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Berlin, Germany: Springer, 2011, pp. 312–325.
[21] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms," *Sci. China Inf. Sci.*, vol. 58, no. 12, pp. 1–15, Dec. 2015.
[22] C. de Cannière, "Analysis and design of symmetric encryption algorithms (analyse en ontwerp van symmetrische encryptie-algoritmen," KULeuven, Leuven, Belgium, Tech. Rep., 2007.
[23] A. Canteaut J. Roué, "On the behaviors of affine equivalent sboxes regarding differential and linear attacks," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, Heidelberg, 2015, pp. 45–74.
[24] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149–170, Mar. 2010.
[25] Y. Todo, G. Leander, and Y. Sasaki, "Nonlinear invariant attack," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Berlin, Germany: Springer, 2016, pp. 3–33.
[26] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, and E. Zenner, "A cryptanalysis of PRINTcipher: The invariant subspace attack," in *Proc. Annu. Cryptol. Conf.*, Berlin, Germany: Springer, 2011, pp. 206–221.

[27] Y. Wei, T. Ye, W. Wu, and E. Pasalic, "Generalized nonlinear invariant attack and a new design criterion for round constants," *IACR Trans. Symmetric Cryptol.*, vol. 2018, pp. 62–79, Dec. 2018.
[28] C. Beierle, A. Canteaut, G. Leander, and Y. Rotella, "Proving resistance against invariant attacks: How to choose the round constants," in *Proc. Annu. Int. Cryptol. Conf.*, Cham, Switzerland: Springer, 2017, pp. 647–678.
[29] C. Zhou, W. Zhang, T. Ding, and Z. Xiang, "Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach," *IACR Trans. Symmetric Cryptol.*, vol. 2019, pp. 438–469, Jan. 2020.
[30] O. Dunkelman and S. Huang, "Reconstructing an S-box from its difference distribution table," *IACR Trans. Symmetric Cryptol.*, vol. 2019, pp. 193–217, Jun. 2019.
[31] B. Arnaud, B. Nicolas, and F. Eric, "Automatic search for a maximum probability differential characteristic in a substitution-permutation network," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, Jan. 2015, pp. 5165–5174.
[32] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, p. 958, Sep. 2019.
[33] A. Farhan and M. Ali, "DB protection system depend on modified hash function," in *Proc. 2nd Int. Conf. Cihan Univ.-Erbil Commun. Eng. Comput. Sci.*, Mar. 2017, p. 84.
[34] A. Mohammed Ali and A. Kadhim Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020.

**SEONGGYEOM KIM** received the M.S. degree in information security from Korea University, in 2018, where he is currently pursuing the Ph.D. degree with the Graduate School of Cyber Security. His research interests include symmetric cryptography and random number generators.

**DEUKJO HONG** received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Korea University, in 1999, 2002, and 2006, respectively. From 2007 to 2015, he was with ETRI. He is currently an Associate Professor with the Department of Information Technology and Engineering, Chonbuk National University. His research interest includes symmetric cryptography.

**JAECHUL SUNG** received the Ph.D. degree in mathematics from Korea University, in 2002. From July 2002 to January 2004, he was a Senior Researcher with the Korea Information Security Agency (KISA). He is currently a Professor with the Department of Mathematics, University of Seoul. His research interests include cryptography, symmetric cryptosystems, hash functions, and MACs.

**SEOKHIE HONG** (Member, IEEE) received the M.S. and Ph.D. degrees in mathematics from Korea University, in 1997 and 2001, respectively. From 2000 to 2004, he was with SECURITY Technologies Inc. From 2004 to 2005, he conducted postdoctoral research with COSIC, KU Leuven, Belgium. He joined the Graduate School of Cyber Security, Korea University. His research interests include cryptography, public and symmetric cryptosystems, hash functions, and MACs.