IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 19, 2021, accepted November 2, 2021, date of publication November 8, 2021, date of current version November 12, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3126008*

# A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and Its Application

**HANGI KIM[1], YONGJIN JEON[1], GIYOON KIM[1], JONGSUNG KIM[1,2], BO-YEON SIM[3], DONG-GUK HAN[1,2], HWAJEONG SEO[4], SEONGGYEOM KIM[5], SEOKHIE HONG[5], JAECHUL SUNG[6], AND DEUKJO HONG[7]**

[1]Department of Financial Information Security, Kookmin University, Seoul 02707, Republic of Korea
[2]Department of Information Security, Cryptology, and Mathematics, Kookmin University, Seoul 02707, Republic of Korea
[3]Intelligent Convergence Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon 34129, Republic of Korea
[4]Division of IT Convergence Engineering, Hansung University, Seoul 02876, Republic of Korea
[5]School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea
[6]Department of Mathematics, University of Seoul, Seoul 02504, Republic of Korea
[7]Department of Information Technology and Engineering, Jeonbuk National University, Jeonju 54896, Republic of Korea

Corresponding author: Jongsung Kim (jskim@kookmin.ac.kr)

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00520, Development of SCR-Friendly Symmetric Key Cryptosystem and Its Application Modes).

**ABSTRACT** Bit permutations are efficient linear functions often used for lightweight cipher designs. However, they have low diffusion effects, compared to word-oriented binary and maximum distance separable (MDS) matrices. Thus, the security of bit permutation-based ciphers is significantly affected by differential and linear branch numbers (DBN and LBN) of nonlinear functions. In this paper, we introduce a widely applicable method for constructing S-boxes with high DBN and LBN. Our method exploits constructions of S-boxes from smaller S-boxes and it derives/proves the required conditions for smaller S-boxes so that the DBN and LBN of the constructed S-boxes are at least 3. These conditions enable us to significantly reduce the search space required to create such S-boxes. Using the unbalanced-Bridge and unbalanced-MISTY structures, we develop a variety of new lightweight S-boxes that provide not only both DBN and LBN of at least 3 but also efficient bitsliced implementations including at most 11 nonlinear bitwise operations. The new S-boxes are the first that exhibit these characteristics.

**INDEX TERMS** Lightweight S-boxes, differential and linear branch numbers, higher-order masking.

## I. INTRODUCTION

The fourth industrial revolution encompasses a wide range of advanced technologies. One of its core elements is the Internet of Things (IoT), which binds together people, objects, processes, data, applications, and services. However, trustworthy systems are required to enable secure and reliable IoT-based infrastructures, and an essential building block for such systems is cryptography.

Since most devices in the IoT environment have limited resources and are small, lightweight cryptography is essential to provide their security. ISO/IEC has even standardized some lightweight block ciphers, such as PRESENT [1] and CLEFIA [2]. In addition, a lightweight cryptography standardization project is ongoing at NIST.

In 1996, Paul Kocher first introduced side-channel attacks, which extract secret information by analyzing side-channel information [3]. Since the security against side-channel attacks cannot be provided by the resistance to classical mathematical cryptanalysis, various countermeasures have been studied. As side-channel attacks become more sophisticated and the costs of the associated equipments decrease, the application of side-channel countermeasures to cryptography becomes important. Recently, various studies have been actively conducted on efficient implementations of side-channel countermeasures, especially on efficient masked

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

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

implementations. To minimize the resource overhead used in masked implementations, these studies focus on reducing the number of nonlinear operations. Several lightweight block ciphers, with the design goal of low nonlinear operation count, have been proposed [4]–[6].

### A. MOTIVATION

Constructing cryptographically secure 8-bit S-boxes is a topic that is being actively studied, and S-boxes using various methods such as polynomial or chaotic mappings have been proposed [7]–[9]. A highly secure 8-bit S-box constructed by perfect nonlinear transformation was adopted for the Advanced Encryption Standard (AES) design [10]. However, it is known that at least 35 nonlinear operations are still required to implement the S-box of AES [11]. Although there are many S-box construction methods that guarantee cryptographic security, the implementation efficiency must be considered in order to be used as a component of block cipher. Considering the implementation of side-channel countermeasures, there is a need for the S-box that can be implemented with fewer nonlinear operations.

There were a few lightweight block ciphers such as Zorro, Fantomas, Robin, SKINNY, and FLY that are intended for use in side-channel protected environments. The block cipher Zorro adopted lightweight S-box using a polynomial S-box construction [12]. In Midori and SKINNY, 8-bit S-boxes constructed with two 4-bit S-boxes are adopted [13], [14]. The block ciphers Fantomas, Robin, and FLY use 8-bit S-boxes constructed from three small S-boxes [6], [15].

Based on the S-box construction methods presented so far, we considered that block cipher designers need S-box construction methods that satisfy all four conditions below.

1) It should be possible to efficiently secure the logic of bitsliced implementation.
2) The number of nonlinear operations required for implementation should be small.
3) Both DBN and LBN should be greater than 2.
4) It should have sufficient cryptographic security to be used as a component of block cipher.

The first two conditions are necessary for efficient implementations of side-channel countermeasures in a resource constrained environment. The third condition is to supplement the weak diffusion effect of bit permutation with the characteristic of S-box. High DBN and LBN help to secure resistance to differential and linear attacks in fewer rounds. It is also important that the cryptographic security should not be inferior to the S-boxes used in lightweight block ciphers.

The lightweightness of block ciphers and the efficiency of their side-channel protected implementations depend significantly on their nonlinear functions. Many of lightweight block ciphers use 4-bit S-boxes [1], [4], [16]–[18] or 8-bit S-boxes [2], [6], [14], [15], [19] as nonlinear functions. One of the main design approaches of lightweight 8-bit S-boxes is to use existing structures, such as Feistel, Lai-Massey and MISTY, employing smaller S-boxes (*e.g.,* 3, 4, or 5-bit S-boxes). However, most related studies have focused on the S-box construction to combine with the linear functions such as word-oriented binary or MDS matrices [6], [19], [20].

### B. CONTRIBUTIONS

This paper is an expanded version of the conference paper [21] presented at ICISC 2020. In particular, we generalize and extend the S-box design proposed in [21].

In this paper, we introduce a construction method for a different type of lightweight 8-bit S-boxes that are well-suited to a linear bit permutation layer, based on which we develop many of new S-boxes with both DBN and LBN of at least 3 and with efficient masked software implementations. Our S-box construction methodology enables both DBN and LBN of at least 3, and this property, in combination with a bit permutation, enhances security. It can be used in the construction of a variety of S-boxes from smaller S-boxes. In this study, the Feistel, Lai–Massey, unbalanced-MISTY, and unbalanced-Bridge structures have been analyzed. Our framework eliminates all the input and output differences (or masks) where the sum of their Hamming weights is two, during which some conditions of the employed smaller S-boxes are induced. These conditions could accelerate the S-box search, resulting in more than 10,000 new lightweight 8-bit S-boxes with both DBN and LBN of 3. Some of their bitsliced implementations include 11 nonlinear bitwise operations each. Our methodology was also used to find more than 1,000 8-bit S-boxes with DBN of 4 and LBN of 3. To the best of our knowledge, all the aforementioned S-boxes are the first S-boxes with such properties. Furthermore, we found 6 and 7-bit new S-boxes with both DBN and LBN of 3 which are more efficient than existing ones.

### C. ORGANIZATION

In section II, we introduce a method for constructing S-boxes with DBN and LBN greater than 2. Using this method, section III constructs new S-boxes and provides comparison of our and existing S-boxes. Section III-D shows an appropriate application of our S-box as a block cipher component. Finally, section IV concludes the paper, and suggests future studies.

### D. NOTATION AND DEFINITIONS

The following notations and definitions are used throughout this paper.

DDT Difference Distribution Table of an $n$-bit S-box whose $(\Delta\alpha, \Delta\beta)$ entry is $\#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta\alpha) = \Delta\beta\}$, where $\Delta\alpha, \Delta\beta \in \mathbb{F}_2^n$.

LAT Linear Approximation Table of an $n$-bit S-box whose $(\lambda_\alpha, \lambda_\beta)$ entry is $\#\{x \in \mathbb{F}_2^n | \lambda_\alpha \bullet x = \lambda_\beta \bullet S(x)\} - 2^{n-1}$, where $\lambda_\alpha, \lambda_\beta \in \mathbb{F}_2^n$, and the symbol $\bullet$ denotes the canonical inner product in $\mathbb{F}_2^n$.

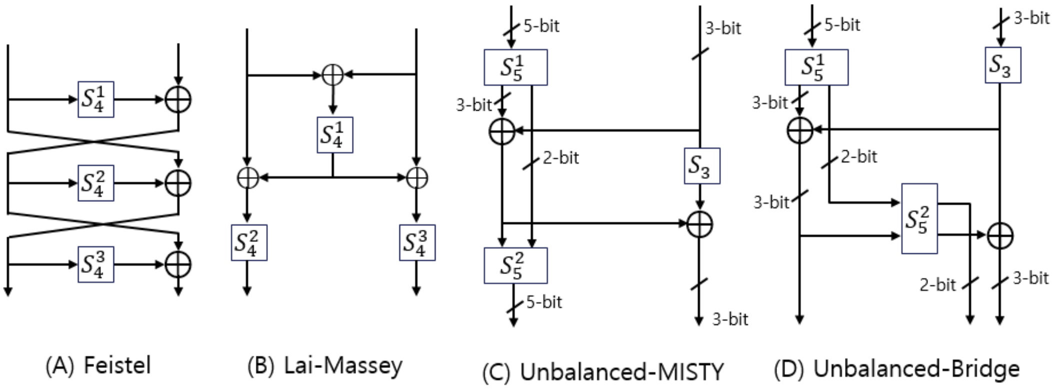


**FIGURE 1.** Constructions of 8-bit S-boxes from smaller S-boxes.

Differential uniformity

$$\max_{\Delta\alpha\neq 0,\Delta\beta} \#\{x\in\mathbb{F}_2^n|S(x)\oplus S(x\oplus\Delta\alpha)=\Delta\beta\}.$$

Non-linearity

$$2^{n-1}-2^{-1}\times\max_{\lambda_\alpha,\lambda_\beta\neq 0}|\Phi(\lambda_\alpha,\lambda_\beta)|, \text{ where } \Phi(\lambda_\alpha,\lambda_\beta) = \sum_{x\in\mathbb{F}_2^n}(-1)^{\lambda_\beta\bullet S(x)\oplus\lambda_\alpha\bullet x}.$$

DBN Differential Branch Number of an S-box defined as $\min_{a,b\neq a}(wt(a\oplus b)+wt(S(a)\oplus S(b)))$.

LBN Linear Branch Number of an S-box defined as $\min_{a,b,\Phi(a,b)\neq 0}(wt(a)+wt(b))$.

## II. CONSTRUCTION OF S-BOXES WITH DIFFERENTIAL AND LINEAR BRANCH NUMBERS GREATER THAN 2

In this section, we describe how to construct S-boxes with DBN>2 and LBN>2. In [22], Ruisanchez proposed algorithm to construct 8-bit S-boxes with a DBN of 3, but did not consider LBN. And Sarkar *et al.* proposed a method for constructing S-boxes with both DBN and LBN of 3 using resilient Boolean functions, and designed such 5 and 6-bit S-boxes [23]. Our method takes a different approach: it uses smaller S-boxes to create S-boxes with DBN>2 (or LBN>2) by eliminating all the input and output differences (or masks) where the sum of their Hamming weights is 2. During this elimination process, relevant conditions of the employed smaller S-boxes can be induced. In this section, we focus on the construction of bijective 8-bit S-boxes.

Several methods have been proposed in the literature to construct 8-bit S-boxes from smaller ones. These methods typically rely on one of the Feistel, Lai-Massey, or (unbalanced-)MISTY structures, as depicted in Fig. 1-(A), (B), and (C), respectively [6], [15], [19], [20], [24]–[26]. The unbalanced-Bridge structure (Fig. 1-(D)) was mentioned in [27], but an S-box constructed using it has not been presented so far. In Fig. 1, $S_i^j$ represents the $j$-th and $i$-bit S-box. Among the structures in Fig. 1, both (A) and (B) use three 4-bit S-boxes and 12 XOR operations on a bit level, whereas both (C) and (D) use one 3-bit and two 5-bit S-boxes and 6 XOR operations.

In this section, we use the following notation.

$\rho_c:\mathbb{F}_2^5\to\mathbb{F}_2^5,\ \ \rho_c(x||y)=y||x,\ \ \text{for } x\in\mathbb{F}_2^3,\ y\in\mathbb{F}_2^2,$

$\tau_n:\mathbb{F}_2^5\to\mathbb{F}_2^n,\ \ \tau_n(x||y)=x,\ \ \text{for } x\in\mathbb{F}_2^n,\ y\in\mathbb{F}_2^{5-n},\ n\in\{1,2,3,4\},$

$\tau'_n:\mathbb{F}_2^5\to\mathbb{F}_2^n,\ \ \tau'_n(x||y)=y,\ \ \text{for } x\in\mathbb{F}_2^{5-n},\ y\in\mathbb{F}_2^n,\ n\in\{1,2,3,4\},$

$\mathfrak{F}_A^1:\mathbb{F}_2^3\to\mathbb{F}_2^5,\ \ \mathfrak{F}_A^1(X)=(S_5^1)^{-1}(X||A)\ \ \text{for } A\in\mathbb{F}_2^2,$

$\mathfrak{F}_A^2:\mathbb{F}_2^3\to\mathbb{F}_2^5,\ \ \mathfrak{F}_A^2(X)=S_5^2(X||A)\ \ \text{for } A\in\mathbb{F}_2^2,$

$0^{(i)}$ : $i$-bit zeros.

The unbalanced-Bridge structure depicted in Fig. 1-(D) can be defined as follows. Let $S_8(X_L||X_R)=C_L(X_L,X_R)||C_R(X_L,X_R)$, where $X_L$ and $X_R$ represent the input variables of $S_8$ which are in $\mathbb{F}_2^5$ and $\mathbb{F}_2^3$, respectively. Then, $C_L(X_L,X_R)=\tau_3(S_5^1(X_L))\oplus S_3(X_R)$ and $C_R(X_L,X_R)=\rho_c(S_5^2(S_5^1(X_L)\oplus(S_3(X_R)||0^{(2)})))\oplus(0^{(2)}||S_3(X_R))$ with $C_L:\mathbb{F}_2^5\times\mathbb{F}_2^3\to\mathbb{F}_2^3$ and $C_R:\mathbb{F}_2^5\times\mathbb{F}_2^3\to\mathbb{F}_2^5$. Proposition 1 shows the conditions for which an 8-bit S-box constructed using Fig. 1-(D) is bijective. The proof of this proposition can be found in [21].

*Proposition 1 [21]: The 8-bit S-box constructed using the unbalanced-Bridge structure of Fig. 1-(D) is bijective if and only if the following three conditions are all satisfied:*

*i) $S_3$ is bijective.*

*ii) $S_5^1$ is bijective.*

*iii) For all $y\in\mathbb{F}_2^3$, $f_y(x)=\tau'_2(S_5^2(y||x))$ is a bijective function with $f_y:\mathbb{F}_2^2\to\mathbb{F}_2^2$.*

In order to guarantee the bijectivity of S-boxes generated from the Lai-Massey and unbalanced-MISTY structures, all the smaller S-boxes except for $S_4^1$ should be bijective, whereas the Feistel structure always offers bijective S-boxes regardless of the smaller S-boxes.

Since all the structures in Fig. 1 have two input branches, S-boxes with DBN>2 can be constructed by eliminating four cases $(\Delta 0||\Delta a,\ \Delta 0||\Delta c)$, $(\Delta 0||\Delta a,\ \Delta d||\Delta 0)$, $(\Delta b||\Delta 0,\ \Delta 0||\Delta c)$, $(\Delta b||\Delta 0,\ \Delta d||\Delta 0)$, where $(\Delta\alpha,\Delta\beta)$

represents the input and output difference pair of the S-boxes, and $wt(\Delta a) = wt(\Delta b) = wt(\Delta c) = wt(\Delta d) = 1$. S-boxes with LBN>2 can be made in the same way. Some conditions of the employed smaller S-boxes are required to rule out these four cases.

The following theorems present the necessary and sufficient conditions of smaller S-boxes so that the 8-bit S-boxes constructed by the **Feistel**, **Lai-Massey**, unbalanced-**MISTY** and unbalanced-**Bridge** structures have both differential and linear branch numbers greater than 2.

*Theorem 1: The DBN of bijective 8-bit S-boxes, constructed using the **Feistel** structure depicted in Fig. 1-(A), is greater than 2 if and only if conditions i) – iv) are all satisfied ($\Delta\alpha$ and $\Delta\beta$ below represent arbitrary 4-bit differences where $wt(\Delta\alpha) = wt(\Delta\beta) = 1$). For each $\Delta\alpha$ and $\Delta\beta$;*

- *i) the entry of the $(\Delta\alpha, \Delta 0)$ in DDT of $S_4^2$ is 0,*
- *ii) at least one entry of the $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^2$ and $(\Delta\beta, \Delta\alpha)$ in DDT of $S_4^3$ is 0,*
- *iii) at least one entry of the $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^1$ and $(\Delta\beta, \Delta\alpha)$ in DDT of $S_4^2$ is 0,*
- *iv) at least one of $S_4^2(Y) \oplus S_4^2(Y \oplus S_4^1(X) \oplus S_4^1(X \oplus \Delta\alpha)) = \Delta\alpha \oplus \Delta\beta$ and $S_4^3(S_4^2(Y) \oplus X) \oplus S_4^3(S_4^2(Y) \oplus X \oplus \Delta\beta) = S_4^1(X) \oplus S_4^1(X \oplus \Delta\alpha)$ has no solution pair $(X, Y)$, where $X, Y \in \mathbb{F}_2^4$.*

*Proof:* The expression of the $C_L$ and $C_R$ is

$$C_L(X_L, X_R) = X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)),$$
$$C_R(X_L, X_R) = X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))).$$

We define the following notation for ease of expression.

$$Y = X_R \oplus S_4^1(X_L), \quad Z = X_L \oplus S_4^2(Y).$$

$\underline{(0^{(4)}||\Delta a, 0^{(4)}||\Delta c)}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta c$. The first equation is expressed as

$$\begin{aligned} &X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)) \oplus X_L \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L)) \\ &= S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L)) = \Delta 0. \end{aligned}$$

By applying $Y$, we obtain

$$S_4^2(Y) \oplus S_4^2(Y \oplus \Delta a) = \Delta 0. \tag{1}$$

Similarly, the second equation is expressed as

$$\begin{aligned} &X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \oplus X_R \oplus \Delta a \\ &\quad \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L))) \\ &= S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \\ &\quad \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L) \oplus \Delta a)) \oplus \Delta a \\ &= \Delta c. \end{aligned}$$

By applying equation (1), we get

$$\Delta a = \Delta c.$$

Therefore, the $(\Delta 0||\Delta a, \Delta 0||\Delta c)$ case is an impossible case if $\Delta a \neq \Delta c$. Otherwise, since the function $(X_L, X_R) \mapsto (X_L, Y)$ is bijective, the $(\Delta 0||\Delta a, \Delta 0||\Delta c)$ case does not happen if and only if there is no $Y$ satisfying equation (1). This means the entries of the $(\Delta a, \Delta 0)$ in DDT of $S_4^2$ have to be zero, which is equivalent to condition *i*) where $\Delta\alpha = \Delta a$.

$\underline{(0^{(4)}||\Delta a, \Delta d||0^{(4)})}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta 0$. The first equation is expressed as

$$\begin{aligned} &X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)) \oplus X_L \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L)) \\ &\quad = S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L)) = \Delta d \end{aligned}$$

By applying $Y$, we have

$$S_4^2(Y) \oplus S_4^2(Y \oplus \Delta a) = \Delta d \tag{2}$$

Similarly, the second equation $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta 0$ is expressed as

$$\begin{aligned} &X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \oplus X_R \oplus \Delta a \\ &\quad \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus \Delta a \oplus S_4^1(X_L))) \\ &= S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \\ &\quad \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L) \oplus \Delta a)) \oplus \Delta a = \Delta 0 \end{aligned}$$

By applying equation (2) and using the definition of $Z$, we obtain

$$S_4^3(Z) \oplus S_4^3(Z \oplus \Delta d) = \Delta a. \tag{3}$$

Since the function $(X_L, X_R) \mapsto (Y, Z)$ is bijective, the $(0^{(4)}||\Delta a, \Delta d||0^{(4)})$ case does not happen if and only if there is no $(Y, Z)$ satisfying both equations ((2 and 3)), which is equivalent to condition *ii*) where $\Delta\alpha = \Delta a, \Delta\beta = \Delta d$.

$\underline{(\Delta b||0^{(4)}, 0^{(4)}||\Delta c)}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta c$. The first equation is expressed as

$$\begin{aligned} &X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)) \\ &\quad \oplus X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) \\ &= S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) \oplus \Delta b \\ &= \Delta 0. \end{aligned}$$

It becomes

$$S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) = \Delta b. \tag{4}$$

Similarly, the second equation $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta c$ is expressed as

$$\begin{aligned} &X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \\ &\quad \oplus X_R \oplus S_4^1(X_L \oplus \Delta b) \\ &\quad \oplus S_4^3(X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b))) \\ &= S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \oplus S_4^1(X_L \\ &\qquad \oplus \Delta b) \oplus S_4^3(X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b))) \\ &= \Delta c. \end{aligned}$$

By applying equation (4), we get

$$S_4^1(X_L) \oplus S_4^1(X_L \oplus \Delta b) = \Delta c. \tag{5}$$

By applying equation (5) and using the definition of $Y$, equation (4) is rewritten as

$$S_4^2(Y) \oplus S_4^2(Y \oplus \Delta c) = \Delta b. \tag{6}$$

Since the function $(X_L, X_R) \mapsto (Y, X_R)$ is bijective, the $(\Delta b || 0^{(4)}, 0^{(4)} || \Delta c)$ case does not happen if and only if there is no $(Y, X_R)$ satisfying both equations (5) and (6), which is equivalent to condition *iii*) where $\Delta\alpha = \Delta b$, $\Delta\beta = \Delta c$.

$(\Delta b || 0^{(4)}, \Delta d || 0^{(4)})$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta 0$. The second equation is expressed as

$$\begin{aligned} & X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \oplus X_R \\ & \quad \oplus S_4^1(X_L \oplus \Delta b) \oplus S_4^3(X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b))) \\ & = S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \oplus S_4^1(X_L \oplus \Delta b) \\ & \quad \oplus S_4^3(X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b))) \\ & = \Delta 0. \end{aligned}$$

It becomes

$$\begin{aligned} & S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \\ & \quad \oplus S_4^3(X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b))) \\ & = S_4^1(X_L) \oplus S_4^1(X_L \oplus \Delta b). \end{aligned} \tag{7}$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ is expressed as

$$\begin{aligned} & X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)) \oplus X_L \oplus \Delta b \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) \\ & = S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) \oplus \Delta b \\ & = \Delta d. \end{aligned}$$

It becomes

$$\begin{aligned} & S_4^2(X_R \oplus S_4^1(X_L)) \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus \Delta b)) \\ & \qquad = \Delta b \oplus \Delta d. \end{aligned} \tag{8}$$

Therefore, $(\Delta b || 0^{(4)}, \Delta d || 0^{(4)})$ case does not happen if and only if there is no $(X_L, X_R)$ satisfying both equations (7) and (8), which is equivalent to condition *iv*). □

*Theorem 2: The LBN of bijective 8-bit S-boxes, constructed using the* Feistel *structure depicted in Fig. 1-(A), is greater than 2 if and only if conditions i) – iv) are all satisfied ($\lambda_\alpha$ and $\lambda_\beta$ below represent arbitrary 4-bit masks where $wt(\lambda_\alpha) = wt(\lambda_\beta) = 1$). For each $\lambda_\alpha$ and $\lambda_\beta$;*

*i)* $\#\{(X, Y) \in (\mathbb{F}_2^4)^2 | (Y \oplus S_4^1(X)) \bullet \lambda_\alpha = (Y \oplus S_4^3(X \oplus S_4^2(Y))) \bullet \lambda_\beta\} = 2^7$,

*ii) at least one entry of the $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^1$ and $(\lambda_\beta, \lambda_\alpha)$ in LAT of $S_4^2$ is* 0,

*iii) at least one entry of the $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^2$ and $(\lambda_\beta, \lambda_\alpha)$ in LAT of $S_4^3$ is* 0,

*iv) the entry of the* $(0, \lambda_\alpha)$ *in LAT of $S_4^2$ is* 0.

*Proof:* We use $C_L$, $C_R$, $Y$, and $Z$ defined in the proof of Theorem 1.

$(0^{(4)} || \lambda_a, 0^{(4)} || \lambda_c)$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_R \bullet \lambda_a = (X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)))) \bullet \lambda_c.$$

It follows

$$\begin{aligned} & (X_R \oplus S_4^1(X_L)) \bullet \lambda_a \oplus S_4^1(X_L) \bullet \lambda_a \\ & \quad = (X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)))) \bullet \lambda_c. \end{aligned}$$

The equation becomes

$$Y \bullet \lambda_a \oplus S_4^1(X_L) \bullet \lambda_a = (Y \oplus S_4^3(X_L \oplus S_4^2(Y))) \bullet \lambda_c \tag{9}$$

by using the definition of $Y$. As mentioned before, the function $(X_L, X_R) \mapsto (X_L, Y)$ is bijective. The $(0 || \lambda_a, 0 || \lambda_c)$ case has zero bias if and only if the equation (9) is not biased. This means $\#\{(X, Y) \in (\mathbb{F}_2^4)^2 | (Y \oplus S_4^1(X)) \bullet \lambda_a = (Y \oplus S_4^3(X \oplus S_4^2(Y))) \bullet \lambda_c\} = 2^7$, which is equivalent to condition *i*) of Theorem 2.

$(0^{(4)} || \lambda_a, \lambda_d || 0^{(4)})$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_R \bullet \lambda_a = (X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \bullet \lambda_d.$$

It follows

$$\begin{aligned} & (X_R \oplus S_4^1(X_L)) \bullet \lambda_a \oplus S_4^1(X_L) \bullet \lambda_a \\ & \qquad = (X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \bullet \lambda_d. \end{aligned}$$

The equation becomes

$$X_L \bullet \lambda_d \oplus S_4^1(X_L) \bullet \lambda_a = Y \bullet \lambda_a \oplus S_4^2(Y) \bullet \lambda_d \tag{10}$$

by using the definition of $Y$. Note that the function $(X_L, X_R) \mapsto (X_L, Y)$ is bijective. The $(0^{(4)} || \lambda_a, \lambda_d || 0^{(4)})$ case has zero bias if and only if the equation (10) is not biased, which is equivalent to condition *ii*) where $\lambda_\alpha = \lambda_d$, $\lambda_\beta = \lambda_a$.

$(\lambda_b || 0^{(4)}, 0^{(4)} || \lambda_c)$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_L \bullet \lambda_b = (X_R \oplus S_4^1(X_L) \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)))) \bullet \lambda_c.$$

It follows

$$\begin{aligned} & (X_R \oplus S_4^1(X_L)) \bullet \lambda_c \oplus S_4^2(X_R \oplus S_4^1(X_L)) \bullet \lambda_b \\ & \quad = (X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \bullet \lambda_b \\ & \qquad \oplus S_4^3(X_L \oplus S_4^2(X_R \oplus S_4^1(X_L)))) \bullet \lambda_c. \end{aligned}$$

The equation becomes

$$Y \bullet \lambda_c \oplus S_4^2(Y) \bullet \lambda_b = Z \bullet \lambda_b \oplus S_4^3(Z) \bullet \lambda_c \tag{11}$$

by using the definition of $Y$ and $Z$. Note that the function $(X_L, X_R) \mapsto (Z, Y)$ is bijective. The $(\lambda_b || 0^{(4)}, 0^{(4)} || \lambda_c)$ case has zero bias if and only if the equation (11) is not biased, which is equivalent to condition *iii*) where $\lambda_\alpha = \lambda_c$, $\lambda_\beta = \lambda_b$.

$\underline{(\lambda_b||0^{(4)}, \lambda_d||0^{(4)})}$: Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_L \bullet \lambda_b = (X_L \oplus S_4^2(X_R \oplus S_4^1(X_L))) \bullet \lambda_d.$$

It follows

$$X_L \bullet (\lambda_b \oplus \lambda_c) = S_4^2(X_R \oplus S_4^1(X_L)) \bullet \lambda_d.$$

The equation becomes

$$X_L \bullet (\lambda_b \oplus \lambda_c) = S_4^2(Y) \bullet \lambda_d \qquad (12)$$

by using the definition of $Y$. Since the left side of the equation is always not biased, only need to consider the right side. The equation (12) is not biased if and only if

$$0 = S_4^2(Y) \bullet \lambda_d \qquad (13)$$

is not biased. The $(\lambda_b||0^{(4)}, \lambda_d||0^{(4)})$ case has zero bias if and only if the equation (13) is not biased, which is equivalent to condition *iv*) where $\lambda_\alpha = \lambda_d$. □

*Theorem 3: The DBN of bijective 8-bit S-boxes, constructed using the* **Lai-Massey** *structure depicted in Fig. 1-(B), is greater than 2 if and only if conditions i) – iv) are all satisfied ($\Delta\alpha$ and $\Delta\beta$ below represent arbitrary 4-bit differences where $wt(\Delta\alpha) = wt(\Delta\beta) = 1$). For each $\Delta\alpha$ and $\Delta\beta$:*

*i) at least one entry of the $(\Delta\alpha, \Delta 0)$ in DDT of $S_4^1$ and $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^3$ is 0,*

*ii) at least one entry of the $(\Delta\alpha, \Delta\alpha)$ in DDT of $S_4^1$ and $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^2$ is 0,*

*iii) at least one entry of the $(\Delta\alpha, \Delta\alpha)$ in DDT of $S_4^1$ and $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^3$ is 0,*

*iv) at least one entry of the $(\Delta\alpha, \Delta 0)$ in DDT of $S_4^1$ and $(\Delta\alpha, \Delta\beta)$ in DDT of $S_4^2$ is 0.*

*Proof:* The expression of the $C_L$ and $C_R$ is

$$C_L(X_L, X_R) = S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)),$$
$$C_R(X_L, X_R) = S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)).$$

We define the following notation for ease of expression.

$$Y = X_L \oplus X_R, \quad Z = X_L \oplus S_4^1(X_L \oplus X_R),$$
$$W = X_R \oplus S_4^1(X_L \oplus X_R).$$

$\underline{(0^{(4)}||\Delta a, 0^{(4)}||\Delta c)}$: It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta c$. The first equation is expressed as

$$S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^2(X_L \oplus S_4^1(X_L \oplus X_R \oplus \Delta a)) = \Delta 0.$$

By applying $(S_4^2)^{-1}$ and using the definition of $Y$, we obtain

$$S_4^1(Y) \oplus S_4^1(Y \oplus \Delta a) = \Delta 0. \qquad (14)$$

Similarly, the second equation $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta c$ is expressed as

$$S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^3(X_R \oplus \Delta a \oplus S_4^1(X_L \oplus X_R \oplus \Delta a)) = \Delta c.$$

By applying equation (14) and using the definition of $W$, we obtain

$$S_4^3(W) \oplus S_4^3(W \oplus \Delta a) = \Delta c. \qquad (15)$$

Since the function $(X_L, X_R) \mapsto (Y, W)$ is bijective, the $(0^{(4)}||\Delta a, 0^{(4)}||\Delta c)$ case does not happen if and only if there is no $(Y, W)$ satisfying both equations (14) and (15), which is equivalent to condition *i*) where $\Delta\alpha = \Delta a$, $\Delta\beta = \Delta c$.

$\underline{(0^{(4)}||\Delta a, \Delta d||0^{(4)})}$: It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta 0$. The second equation is expressed as

$$S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^3(X_R \oplus \Delta a \oplus S_4^1(X_L \oplus X_R \oplus \Delta a)) = \Delta 0.$$

By applying $(S_4^3)^{-1}$ and using the definition of $Y$, we obtain

$$S_4^1(Y) \oplus S_4^1(Y \oplus \Delta a) = \Delta a. \qquad (16)$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ is expressed as

$$S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^2(X_L \oplus S_4^1(X_L \oplus X_R \oplus \Delta a)) = \Delta d.$$

By applying equation (16) and using the definition of $Z$, we obtain

$$S_4^2(Z) \oplus S_4^2(Z \oplus \Delta a) = \Delta d. \qquad (17)$$

Since the function $(X_L, X_R) \mapsto (Z, Y)$ is bijective, the $(0^{(4)}||\Delta a, \Delta d||0^{(4)})$ case does not happen if and only if there is no $(Z, Y)$ satisfying both equations (16) and (17), which is equivalent to condition *ii*) where $\Delta\alpha = \Delta a$, $\Delta\beta = \Delta d$.

$\underline{(\Delta b||0^{(4)}, 0^{(4)}||\Delta c)}$: It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta c$. The first equation is expressed as

$$S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^2(X_L \oplus \Delta b \oplus S_4^1(X_L \oplus \Delta b \oplus X_R)) = \Delta 0.$$

By applying $(S_4^2)^{-1}$ and using the definition of $Y$, we obtain

$$S_4^1(Y) \oplus S_4^1(Y \oplus \Delta b) = \Delta b. \qquad (18)$$

Similarly, the second equation $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta c$ is expressed as

$$S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \oplus S_4^3(X_R \oplus S_4^1(X_L \oplus \Delta b \oplus X_R)) = \Delta c.$$

By applying equation (18) and using the definition of $W$, we obtain

$$S_4^3(W) \oplus S_4^3(W \oplus \Delta b) = \Delta c. \qquad (19)$$

Since the function $(X_L, X_R) \mapsto (Y, W)$ is bijective, the $(\Delta b||0^{(4)}, 0^{(4)}||\Delta c)$ case does not happen if and only if there is no $(Y, W)$ satisfying both equations (18) and (19), which is equivalent to condition *iii*) where $\Delta\alpha = \Delta b$, $\Delta\beta = \Delta c$.

$\underline{(\Delta b||0^{(4)}, \Delta d||0^{(4)})}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta 0$. The second equation is expressed as

$$\begin{aligned} &S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \\ &\qquad \oplus S_4^3(X_R \oplus S_4^1(X_L \oplus X_R \oplus \Delta b)) = \Delta 0. \end{aligned}$$

By applying $(S_4^3)^{-1}$ and using the definition of $Y$, we obtain

$$S_4^1(Y) \oplus S_4^1(Y \oplus \Delta b) = \Delta 0. \tag{20}$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ is expressed as

$$\begin{aligned} &S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \\ &\qquad \oplus S_4^2(X_L \oplus \Delta b \oplus S_4^1(X_L \oplus \Delta b \oplus X_R)) = \Delta d. \end{aligned}$$

By applying equation (20) and using the definition of $Z$, we obtain

$$S_4^2(Z) \oplus S_4^2(Z \oplus \Delta b) = \Delta d. \tag{21}$$

Since the function $(X_L, X_R) \mapsto (Z, Y)$ is bijective, the $(\Delta b||0^{(4)}, \Delta d||0^{(4)})$ case does not happen if and only if there is no $(Z, Y)$ satisfying both equations (20) and (21), which is equivalent to condition *iv*) where $\Delta\alpha = \Delta b$, $\Delta\beta = \Delta d$. □

*Theorem 4: The LBN of bijective 8-bit S-boxes, constructed using the* Lai-Massey *structure depicted in Fig. 1-(B), is greater than 2 if and only if conditions i) – iv) are all satisfied ($\lambda_\alpha$ and $\lambda_\beta$ below represent arbitrary 4-bit masks where $wt(\lambda_\alpha) = wt(\lambda_\beta) = 1$). For each $\lambda_\alpha$ and $\lambda_\beta$;*

*i) at least one entry of the $(0, \lambda_\alpha)$ in LAT of $S_4^1$ and $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^3$ is 0,*

*ii) at least one entry of the $(\lambda_\alpha, \lambda_\alpha)$ in LAT of $S_4^1$ and $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^2$ is 0,*

*iii) at least one entry of the $(\lambda_\alpha, \lambda_\alpha)$ in LAT of $S_4^1$ and $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^3$ is 0,*

*iv) at least one entry of the $(0, \lambda_\alpha)$ in LAT of $S_4^1$ and $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_4^2$ is 0.*

*Proof:* We use $C_L$, $C_R$, $Y$, and $Z$ defined in the proof of Theorem 3.

$\underline{(0^{(4)}||\lambda_a, 0^{(4)}||\lambda_c)}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_R \bullet \lambda_a = S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_c.$$

It follows

$$\begin{aligned} &S_4^1(X_L \oplus X_R) \bullet \lambda_a \\ &\quad = (X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_a \\ &\qquad \oplus S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_c. \end{aligned}$$

The equation becomes

$$S_4^1(Y) \bullet \lambda_a = W \bullet \lambda_a \oplus S_4^3(W) \bullet \lambda_c \tag{22}$$

by using the definition of $Y$ and $W$. Note that the function $(X_L, X_R) \mapsto (Y, W)$ is bijective. The $(0^{(4)}||\lambda_a, 0^{(4)}||\lambda_c)$ case has zero bias if and only if the equation (22) is not biased, which is equivalent to condition *i*) where $\lambda_\alpha = \lambda_a, \lambda_\beta = \lambda_c$.

$\underline{(0^{(4)}||\lambda_a, \lambda_d||0^{(4)})}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_R \bullet \lambda_a = S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_d.$$

It follows

$$\begin{aligned} &(X_L \oplus X_R) \bullet \lambda_a \oplus S_4^1(X_L \oplus X_R) \bullet \lambda_a \\ &\quad = (X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_a \\ &\qquad \oplus S_4^2(X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_d. \end{aligned}$$

The equation becomes

$$Y \bullet \lambda_a \oplus S_4^1(Y) \bullet \lambda_a = W \bullet \lambda_a \oplus S_4^2(W) \bullet \lambda_d \tag{23}$$

by using the definition of $Y$ and $W$. Note that the function $(X_L, X_R) \mapsto (Y, W)$ is bijective. The $(0^{(4)}||\lambda_a, \lambda_d||0^{(4)})$ case has zero bias if and only if the equation (23) is not biased, which is equivalent to condition *ii*) where $\lambda_\alpha = \lambda_a, \lambda_\beta = \lambda_d$.

$\underline{(\lambda_b||0^{(4)}, 0^{(4)}||\lambda_c)}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_L \bullet \lambda_b = S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_c.$$

It follows

$$\begin{aligned} &(X_L \oplus X_R) \bullet \lambda_b \oplus S_4^1(X_L \oplus X_R) \bullet \lambda_b \\ &\quad = (X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_b \\ &\qquad \oplus S_4^3(X_R \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_c. \end{aligned}$$

The equation becomes

$$Y \bullet \lambda_b \oplus S_4^1(Y) \bullet \lambda_b = W \bullet \lambda_b \oplus S_4^3(W) \bullet \lambda_c \tag{24}$$

by using the definition of $Y$ and $W$. Note that the function $(X_L, X_R) \mapsto (Y, W)$ is bijective. The $(\lambda_b||0^{(4)}, 0^{(4)}||\lambda_c)$ case has zero bias if and only if the equation (24) is not biased, which is equivalent to condition *iii*) where $\lambda_\alpha = \lambda_b, \lambda_\beta = \lambda_c$.

$\underline{(\lambda_b||0^{(4)}, \lambda_d||0^{(4)})}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_L \bullet \lambda_b = S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_d.$$

It follows

$$\begin{aligned} &S_4^1(X_L \oplus X_R) \bullet \lambda_b \\ &\quad = (X_L \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_b \\ &\qquad \oplus S_4^2(X_L \oplus S_4^1(X_L \oplus X_R)) \bullet \lambda_d. \end{aligned}$$

The equation becomes

$$S_4^1(Y) \bullet \lambda_b = Z \bullet \lambda_b \oplus S_4^3(Z) \bullet \lambda_d \tag{25}$$

by using the definition of $Y$ and $Z$. Note that the function $(X_L, X_R) \mapsto (Z, Y)$ is bijective. The $(\lambda_b||0^{(4)}, \lambda_d||0^{(4)})$ case has zero bias if and only if the equation (25) is not biased, which is equivalent to condition *iv*) where $\lambda_\alpha = \lambda_b$, $\lambda_\beta = \lambda_d$. □

*Theorem 5: The DBN of bijective 8-bit S-boxes, constructed using the unbalanced-**MISTY** structure depicted in Fig. 1-(C), is greater than 2 if and only if conditions i) and ii) are both satisfied ($\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$ below represent arbitrary 5, 5 and 3-bit differences, respectively, where $wt(\Delta\alpha) = wt(\Delta\beta) = wt(\Delta\gamma) = 1$). For each $\Delta\alpha$, $\Delta\beta$, and $\Delta\gamma$;*

*i) at least one entry of the $(\Delta\gamma, \Delta\gamma)$ in DDT of $S_3$ and $(\Delta\gamma||0^{(2)}, \Delta\alpha)$ in DDT of $S_5^2$ is* 0,

*ii) for each $A, B(\neq A) \in \mathbb{F}_2^2$, at least one of $\mathfrak{F}_A^1(X) \oplus \mathfrak{F}_B^1(X) = \Delta\alpha$ and $\mathfrak{F}_A^2(X) \oplus \mathfrak{F}_B^2(X) = \Delta\beta$ has no solution $X$, where $X \in \mathbb{F}_2^3$.*

*Proof:* The expression of the $C_L$ and $C_R$ is

$$C_L(X_L, X_R) = S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}),$$
$$C_R(X_L, X_R) = \tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R).$$

We define the following notation for ease of expression.

$$Y = S_5^1(X_L), \quad Z = S_5^1(X_L) \oplus X_R||0^{(2)},$$
$$A = \tau_2'(Y) = \tau_2'(Z), \quad Y = Y'||A,\ Z = Z'||A.$$

$\underline{(0^{(5)}||\Delta a, 0^{(5)}||\Delta c)}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta c$. The first equation is expressed as

$$S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \oplus S_5^2(S_5^1(X_L) \oplus (X_R \oplus \Delta a)||0^{(2)}) = \Delta 0.$$

By applying $(S_5^2)^{-1}$, we obtain

$$\Delta a||0^{(2)} = \Delta 0.$$

Since the equation is impossible, the $(0^{(5)}||\Delta a, 0^{(5)}||\Delta c)$ case does not happen.

$\underline{(0^{(5)}||\Delta a, \Delta d||0^{(3)})}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L, X_R \oplus \Delta a) = \Delta 0$. The second equation is expressed as

$$\tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R)$$
$$\oplus \tau_3(S_5^1(X_L)) \oplus X_R \oplus \Delta a \oplus S_3(X_R \oplus \Delta a) = \Delta 0.$$

Clearly,

$$S_3(X_R) \oplus S_3(X_R \oplus \Delta a) = \Delta a. \tag{26}$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L, X_R \oplus \Delta a) = \Delta d$ is expressed as

$$S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \oplus S_5^2(S_5^1(X_L) \oplus (X_R \oplus \Delta a)||0^{(2)}) = \Delta d.$$

By using the definition of $Z$, we obtain

$$S_5^2(Z) \oplus S_5^2(Z \oplus \Delta a||0^{(2)}) = \Delta d. \tag{27}$$

Since the function $(X_L, X_R) \mapsto (Z, X_R)$ is bijective, the $(0^{(5)}||\Delta a, \Delta d||0^{(3)})$ case does not happen if and only if there is no $(Z, X_R)$ satisfying both equations (26) and (27), which is equivalent to condition *i*) where $\Delta\alpha = \Delta a$, $\Delta\beta = \Delta d$.

$\underline{(\Delta b||0^{(3)}, 0^{(5)}||\Delta c)}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta 0$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta c$. The second equation is expressed as

$$\tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R)$$
$$\oplus \tau_3(S_5^1(X_L \oplus \Delta b)) \oplus X_R \oplus S_3(X_R) = \Delta c.$$

Clearly,

$$\tau_3(S_5^1(X_L)) \oplus \tau_3(S_5^1(X_L \oplus \Delta b)) = \Delta c. \tag{28}$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ is expressed as

$$S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \oplus S_5^2(S_5^1(X_L \oplus \Delta b) \oplus X_R||0^{(2)}) = \Delta 0.$$

By applying $(S_5^2)^{-1}$, we obtain

$$S_5^1(X_L) \oplus S_5^1(X_L \oplus \Delta b) = \Delta 0. \tag{29}$$

Since equations (28) and (29) cause contradiction, the $(\Delta b||0^{(3)}, 0^{(5)}||\Delta c)$ case does not happen.

$\underline{(\Delta b||0^{(3)}, \Delta d||0^{(3)})}$*:* It happens if and only if there exists at least one $(X_L, X_R)$ satisfying both $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ and $C_R(X_L, X_R) \oplus C_R(X_L \oplus \Delta b, X_R) = \Delta 0$. The second equation is expressed as

$$\tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R)$$
$$\oplus \tau_3(S_5^1(X_L \oplus \Delta b)) \oplus X_R \oplus S_3(X_R) = \Delta 0.$$

Clearly,

$$\tau_3(S_5^1(X_L)) \oplus \tau_3(S_5^1(X_L \oplus \Delta b)) = \Delta 0.$$

Since $S_5^1$ is bijection, for a non-zero difference $\Delta\omega \in \mathbb{F}_2^2$, the above equation becomes

$$S_5^1(X_L) \oplus S_5^1(X_L \oplus \Delta b) = \Delta\omega. \tag{30}$$

By applying $(S_5^1)^{-1}$, we get

$$X_L \oplus \Delta b = (S_5^1)^{-1}(S_5^1(X_L) \oplus \Delta\omega).$$

By using the definition of $Y$, we obtain

$$(S_5^1)^{-1}(Y) \oplus (S_5^1)^{-1}(Y \oplus \Delta\omega) = \Delta b. \tag{31}$$

Similarly, the first equation $C_L(X_L, X_R) \oplus C_L(X_L \oplus \Delta b, X_R) = \Delta d$ is expressed as

$$S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \oplus S_5^2(S_5^1(X_L \oplus \Delta b) \oplus X_R||0^{(2)}) = \Delta d.$$

By applying equation (30) and using the definition of $Y$, we obtain

$$S_5^2(Y) \oplus S_5^2(Y \oplus \Delta\omega) = \Delta d. \tag{32}$$

For each $A$, the equations (31) and (32) are equivalent to

$$\mathfrak{F}_A^2(Y') \oplus \mathfrak{F}_{A\oplus\Delta\omega}^2(Y') = \Delta b, \tag{33}$$
$$\mathfrak{F}_A^1(Z') \oplus \mathfrak{F}_{A\oplus\Delta\omega}^1(Z') = \Delta d. \tag{34}$$

Here, $\Delta\omega$ is arbitrary nonzero 2-bit difference, and thus we can define $B = A \oplus \Delta\omega$ *i.e.*, $B \neq A$. Since the function $(X_L, X_R) \mapsto (Y', A, Z')$ is bijective, the $(\Delta b||0^{(3)}, \Delta d||0^{(3)})$ case does not happen if and only if there is no $(Y', A, Z')$ satisfying both equations (33) and (34) for all $B(\neq A)$, which is equivalent to condition *ii*) where $\Delta\alpha = \Delta b$, $\Delta\beta = \Delta d$. □

*Theorem 6: The LBN of bijective 8-bit S-boxes, constructed using the unbalanced-**MISTY** structure depicted in Fig. 1-(C), is greater than 2 if and only if conditions i) and ii) are both satisfied ($\lambda_\alpha$, $\lambda_\beta$, and $\lambda_\gamma$ below represent arbitrary 5,5 and 3-bit masks, respectively, where $wt(\lambda_\alpha) = wt(\lambda_\beta) = wt(\lambda_\gamma) = 1$). For each $\lambda_\alpha$, $\lambda_\beta$, and $\lambda_\gamma$;*

- *i) at least one entry of the $(\lambda_\gamma, \lambda_\gamma)$ in LAT of $S_3$ and $(\lambda_\alpha, \lambda_\gamma||0^{(2)})$ in LAT of $S_5^1$ is 0,*
- *ii) $\sum_{A\in\mathbb{F}_2^2} X \cdot Y = 0$ where $X$ is the entry $(0, \lambda_\alpha)$ in LAT of $\mathfrak{F}_A^1$ and $Y$ is the entry $(0, \lambda_\beta)$ in LAT of $\mathfrak{F}_A^2$.*

*Proof:* We use $C_L$, $C_R$, $Y$, and $Z$ defined in the proof of Theorem 5.

$\underline{(0^{(5)}||\lambda_a, 0^{(5)}||\lambda_c)}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_R \bullet \lambda_a = (\tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R)) \bullet \lambda_c.$$

It follows

$$X_R \bullet (\lambda_a \oplus \lambda_c) \oplus S_3(X_R) \bullet \lambda_c = \tau_3(S_5^1(X_L)) \bullet \lambda_c.$$

Clearly,

$$X_R \bullet (\lambda_a \oplus \lambda_c) \oplus S_3(X_R) \bullet \lambda_c = S_5^1(X_L) \bullet \lambda_c||0^{(2)}.$$

Since $S_5^1$ is bijective, the $(0^{(5)}||\lambda_a, 0^{(5)}||\lambda_c)$ case has zero bias.

$\underline{(0^{(5)}||\lambda_a, \lambda_d||0^{(3)})}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_R \bullet \lambda_a = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_R \bullet \lambda_a = S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \bullet \lambda_c.$$

The equation becomes

$$X_R \bullet \lambda_a = S_5^2(Z) \bullet \lambda_c$$

by using the definition of $Z$. Since left side is not biased, the $(0^{(5)}||\lambda_a, \lambda_d||0^{(3)})$ case has zero bias.

$\underline{(\lambda_b||0^{(3)}, 0^{(5)}||\lambda_c)}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_R(X_L, X_R) \bullet \lambda_c$. The equation is expressed as

$$X_L \bullet \lambda_b = (\tau_3(S_5^1(X_L)) \oplus X_R \oplus S_3(X_R)) \bullet \lambda_c.$$

It follows

$$X_R \bullet \lambda_c \oplus S_3(X_R) \bullet \lambda_c = X_L \bullet \lambda_b \oplus \tau_3(S_5^1(X_L)) \bullet \lambda_c.$$

Clearly,

$$X_R \bullet \lambda_c \oplus S_3(X_R) \bullet \lambda_c = X_L \bullet \lambda_b \oplus S_5^1(X_L) \bullet \lambda_c||0^{(2)}. \tag{35}$$

The $(\lambda_b||0^{(3)}, 0^{(5)}||\lambda_c)$ case has zero bias if and only if the equation (35) is not biased, which is equivalent to condition *i*) where $\lambda_\alpha = \lambda_b$, $\lambda_\beta = \lambda_c$.

$\underline{(\lambda_b||0^{(3)}, \lambda_d||0^{(3)})}$*:* Its bias can be calculated by the number of $(X_L, X_R)$ satisfying $X_L \bullet \lambda_b = C_L(X_L, X_R) \bullet \lambda_d$. The equation is expressed as

$$X_L \bullet \lambda_b = S_5^2(S_5^1(X_L) \oplus X_R||0^{(2)}) \bullet \lambda_d.$$

The equation becomes

$$(S_5^1)^{-1}(Y) \bullet \lambda_b = S_5^2(Z) \bullet \lambda_d$$

by using the definition of $Y$ and $Z$. For definition of $A$, the above equation is equivalent to

$$f_A^1(Y') \bullet \lambda_b = f_A^2(Z') \bullet \lambda_d. \tag{36}$$

The $(\lambda_b||0^{(3)}, \lambda_d||0^{(3)})$ case has zero bias if and only if the equation (36) is not biased, which is equivalent to condition *ii*) where $\lambda_\alpha = \lambda_b$, $\lambda_\beta = \lambda_d$. □

The detailed proofs of Theorems 7 and 8 can be found in [21].

*Theorem 7 [21]: The DBN of bijective 8-bit S-boxes constructed using the unbalanced-**Bridge** structure of Fig. 1-(D) is greater than 2 if and only if conditions i), ii), and iii) are all satisfied ($\Delta\alpha$ and $\Delta\beta$ below represent arbitrary differences where $wt(\Delta\alpha) = wt(\Delta\beta) = 1$):*

- *i) For each $\Delta\alpha, \Delta\beta \in \mathbb{F}_2^3$, at least one of the entry $(\Delta\alpha, \Delta\beta)$ in DDT of $S_3$ and the entry $(\Delta\beta||0^{(2)}, \Delta\beta||0^{(2)})$ in DDT of $S_5^2$ is 0,*
- *ii) For each $\Delta\alpha, \Delta\beta \in \mathbb{F}_2^5$, for each $A, B(\neq A) \in \mathbb{F}_2^2$, at least one of $\mathfrak{F}_A^1(X) \oplus \mathfrak{F}_B^1(X) = \Delta\alpha$ and $\mathfrak{F}_A^2(X) \oplus \mathfrak{F}_B^2(X) = \Delta\beta$ has no solution $X$, where $X \in \mathbb{F}_2^3$,*
- *iii) For each $\Delta\alpha \in \mathbb{F}_2^3$ and $\Delta\beta \in \mathbb{F}_2^5$, for each $A, B \in \mathbb{F}_2^2$, at least one of $\mathfrak{F}_A^1(X) \oplus \mathfrak{F}_B^1(X \oplus \Delta\alpha) = \Delta\beta$ and $\mathfrak{F}_A^2(X) \oplus \mathfrak{F}_B^2(X \oplus \Delta\alpha) = \Delta 0$ has no solution $X$, where $X \in \mathbb{F}_2^3$.*

*Theorem 8 [21]: The LBN of bijective 8-bit S-boxes constructed using the unbalanced-**Bridge** structure of Fig. 1-(D) is greater than 2 if and only if conditions i), ii), and iii) are all satisfied ($\lambda_\alpha$ and $\lambda_\beta$ below represent arbitrary masks where $wt(\lambda_\alpha) = wt(\lambda_\beta) = 1$):*

- *i) For each $\lambda_\alpha, \lambda_\beta \in \mathbb{F}_2^3$, at least one of the entry $(\lambda_\alpha, \lambda_\beta)$ in LAT of $S_3$ and the entry $(0, \lambda_\beta||0^{(2)})$ in LAT of $S_5^2$ is 0,*
- *ii) For each $\lambda_\alpha \in \mathbb{F}_2^5$ and $\lambda_\beta \in \mathbb{F}_2^3$, $\sum_{A\in\mathbb{F}_2^2} X \cdot Y = 0$ where $X$ is the entry $(\lambda_\beta, \lambda_\alpha)$ in LAT of $\mathfrak{F}_A^1$ and $Y$ is the entry $(\lambda_\beta, \lambda_\beta||0^{(2)})$ in LAT of $\mathfrak{F}_A^2$,*
- *iii) For each $\lambda_\alpha, \lambda_\beta \in \mathbb{F}_2^5$ satisfying $\tau_3(\lambda_\beta) = 0$, $\sum_{A\in\mathbb{F}_2^2} X \cdot Y = 0$ where $X$ is the entry $(0, \lambda_\alpha)$ in LAT of $\mathfrak{F}_A^1$ and $Y$ is the entry $(0, \lambda_\beta)$ in LAT of $\mathfrak{F}_A^2$.*

In practice, most S-boxes searched from the above theorems have both DBN and LBN of 3. In order to provide higher DBN or LBN of S-boxes, additional conditions are generally required (*e.g.*, a search for S-boxes of DBN of 4 requires additional conditions for eliminating input and output differences where the sum of their Hamming weights is three).

**TABLE 1.** Comparison of bitslice 8-bit S-boxes with respect to cryptographic properties and numbers of operations ('U-' represents 'Unbalanced-').

| | Listing 1 | Listing 2 | Listing 3 | Listing 4 | PIPO | FLY | Fantomas | Robin | Scream v3 | AES |
|---|---|---|---|---|---|---|---|---|---|---|
| DBN | 3 | 3 | 3 | 4 | 3 | 3 | 2 | 2 | 2 | 2 |
| LBN | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 2 |
| Differential uniformity | 16 | 16 | 16 | 64 | 16 | 16 | 16 | 16 | 8 | 4 |
| Non-linearity | 96 | 96 | 96 | 0 | 96 | 96 | 96 | 96 | 96 | 112 |
| Algebraic degree | 6 | 5 | 5 | 5 | 5 | 5 | 5 | 6 | 6 | 7 |
| #(Fixed points) | 16 | 1 | 0 | 2 | 0 | 1 | 0 | 16 | 0 | 0 |
| #(Nonlinear operations)* | 12 | 12 | 11 | 8 | 11 | 12 | 11 | 12 | 12 | 35 |
| #(Linear operations) | 30 | 31 | 24 | 29 | 23 | 24 | 27 | 24 | 27 | 93 |
| Construction method | Feistel | Lai-Massey | U-MISTY | U-Bridge | U-Bridge | Lai-Massey | U-MISTY | MISTY | Feistel | Inversion in $GF(2^8)$ |
| Reference | This paper | This paper | This paper | This paper | This paper, [21] | [15] | [6] | [6] | [19] | [10], [11] |

*Nonlinear (resp. linear) operations represent AND, OR (resp. XOR, NOT).

In the above theorems, conditions of smaller S-boxes are different for each structure, leading to different numbers of the required smaller S-box computations. In order to find an S-box with DBN (or LBN) of 3, then the Feistel, Lai-Massey, unbalanced-MISTY and unbalanced-Bridge structures depicted in Fig. 1 require about 11,200, 1,000, 600, and 1,700 (or 13,300, 1,600, 800, and 900) smaller S-box computations, respectively, which were confirmed in our simulations. Employed smaller S-boxes or their combinations are early aborted once they do not meet any of the conditions in Theorems 1–8. Note that the method described in this section can be applied to any of S-box extension structures.

## III. SEARCHING FOR NEW CRYPTOGRAPHICALLY GOOD AND LIGHTWEIGHT S-BOXES

In this section, we describe the characteristics of balanced and unbalanced structures and the S-box search process. Note that 6, 7 and 8-bit S-boxes constructed in this paper are all bijective. We focus on the following three criteria when constructing the 8-bit S-boxes.

1) It should offer an efficient bitsliced implementation including 12 or fewer nonlinear operations.
2) Its DBN and LBN should both be greater than 2.
3) Its differential uniformity should be 16 or less, and its non-linearity should be 96 or more.

Criterion 1 minimizes the number of nonlinear operations required to implement an S-box, which allows for efficient higher-order masking implementations. Criteria 2 and 3 ensure the cryptographic strengths of the 8-bit S-box against differential cryptanalysis and linear cryptanalysis. The thresholds of the criteria were selected based on the properties of the existing lightweight 8-bit S-boxes (cf. Table 1). In this section, we take into account DBN, LBN, differential uniformity, non-linearity, algebraic degree, and fixed point as the security metrics of an S-box, which are directly necessary for the security analysis of instantiated block cipher. Other cryptographic properties, such as algebraic immunity, strict avalanche criterion (SAC), and bit independence criterion (BIC) are presented in Appendix A.

### A. CONSTRUCTING S-BOXES WITH THE BALANCED STRUCTURES

To construct an 8-bit S-box that satisfies criterion 3 through the balanced structures in Fig. 1, the differential uniformity of each 4-bit S-box must be less than or equal to 4 and the non-linearity must be greater than or equal to 8. It is known that at least 4 ANDs are required to implement such a 4-bit S-box with a differential uniformity of 4 [29]. Therefore, to construct an 8-bit S-box that satisfies criterion 3 using the balanced structures, at least 12 nonlinear operations are required. Block ciphers Robin, Scream v3, and FLY each adopted an S-box constructed using different balanced structures, and 12 nonlinear operations are used to implement one of them (cf. Table 1). Among them, only the Littlun S-box used in the block cipher FLY satisfies criterion 2. We constructed S-boxes with DBN and LBN of 3 by combining 4-bit S-boxes that satisfy the conditions of Theorems 1–4, and presented them in Table 1. Appendix B includes the bitsliced implementations of the S-boxes found from each structure.

### B. CONSTRUCTING S-BOXES WITH THE UNBALANCED STRUCTURES

The S-box adopted in the block cipher Fantomas was constructed using a unbalanced-MISTY structure, and is meaningful because it can be implemented with the fewest nonlinear operations among the 8-bit S-boxes that satisfy criterion 3 proposed so far. This is because the 8-bit S-box satisfies criterion 3 even if only 4 and 3 nonlinear operations are used in the 5-bit S-boxes and the 3-bit S-box of unbalanced structure, respectively. However, Fantomas adopts a word-oriented binary matrix as its linear layer, and thus the designers do not consider the DBN and LBN of the S-box.

Our search process with unbalanced structures is outlined as follows. First, we generated 3-bit and 5-bit S-box sets; for 3-bit S-boxes we ran an exhaustive search with AND, OR, XOR, and NOT instructions while restricting the number of nonlinear (resp. linear) operations to 3 (resp. 4), and for 5-bit S-boxes we ran an exhaustive search with AND, OR, and XOR instruction while restricting the number of nonlinear (resp. linear) operations to 4 (resp. 7) with a differential uniformity of 8 or less. Second, we classified two 5-bit S-boxes and one 3-bit S-box that satisfy the conditions of Theorems 5–8. For the unbalanced-Bridge structure, conditions of Proposition 1 must also be satisfied. During this process, the search space was significantly reduced because the early abort technique was used to select $S_3$, $S_1^5$, and $S_2^5$.

**TABLE 2.** Comparison of 6 and 7-bit S-boxes with respect to cryptographic properties and numbers of operations.

| | 6-bit S-boxes | | | 7-bit S-boxes | |
|---|---|---|---|---|---|
| | Sakar's $S_6$ | Sakar's $S_6$' | Listing 5 | MISTY, KASUMI | Listing 6 |
| DBN | 3 | 3 | 3 | 2 | 3 |
| LBN | 3 | 3 | 3 | 2 | 3 |
| Differential uniformity | 4 | 4 | 4 | 2 | 8 |
| Non-linearity | 24 | 24 | 24 | 56 | 48 |
| Algebraic degree | 3 | 2 | 4 | 3 | 4 |
| #(Fixed points) | 2 | 4 | 2 | 1 | 0 |
| #(Nonlinear operations) | 167 | 36 | 9 | 104 | 11 |
| #(Linear operations) | 119 | 54 | 12 | 77 | 24 |
| Construction method | Cubic function | Toeplitz matrix | Feistel | $A \bullet x^{\alpha}$ over $GF(2^7)$ | U-MISTY |
| Reference | [23] | [23] | This paper | [26], [28] | This paper |

Third, we randomly chose the combination of $S_3$, $S_5^1$, and $S_5^2$ to verify whether the corresponding 8-bit S-boxes satisfy criterion 3.

Through this process, it was possible to construct S-box that satisfy all criteria 1–3 using unbalanced-MISTY structure. Table 1 and Listing 3 show that this S-box can be implemented with fewer operations than the S-box adopted by Fantomas. Also, in [27], it was mentioned that the S-box constructed through unbalanced-Bridge seems to give bad cryptanalytic properties, but we could find more than 8,000 of S-boxes satisfying criteria 1–3. One of them is adopted in the block cipher PIPO [21]. It can be implemented with the fewest operations among all the S-boxes presented so far that satisfy critrion 3.

Since the unbalanced-Bridge structure allows $S_5^2$ to be either bijective or non-bijective, the search pool is larger than that in the unbalanced-MISTY structure.

*Proposition 2: The number of possible combinations of* $S_3, S_5^1$, *and* $S_5^2$ *in the unbalanced-Bridge structure of Fig. 1-(D) is* $32! \times 8! \times 98304^8 \approx 2^{265.6}$, *whereas that in the structure of unbalanced-MISTY of Fig. 1-(C) is* $32! \times 8! \times 32! \approx 2^{250.6}$.

*Proof:* All the smaller S-boxes in (C) and (D) should be bijective except for $S_5^2$ in (D). Condition *iii*) of Proposition 1 should hold for $S_5^2$ in order to make the 8-bit S-box bijective. For a fixed $y \in \mathbb{F}_2^3$, the number of functions $S_5^2(y||\cdot)$ is $4! \times 8^4$. Since $y$ can have any value in $\mathbb{F}_2^3$, the number of possible $S_5^2$ is $(4! \times 8^4)^8 = 98304^8$. □

Furthermore, the unbalanced-Bridge structure enabled us to construct more than 1,000 S-boxes with DBN of 4 and LBN of 3. They were found by using the aforementioned additional conditions, but there is one entry of $-128$ in each of their LATs that might cause ciphers weakened by LC. Its bitsliced implementation can be found in the Listing 4.

## C. CONSTRUCTING 6 AND 7-BIT S-BOXES

Sarkar *et al.* proposed algorithms to search for 5 and 6-bit S-boxes with DBN and LBN greater than 2, and presented several such S-boxes [23]. They have good cryptographic properties. However, they are not efficient in a bitslice manner, since their search algorithms are based on the algebraic methods. Meanwhile, 7-bit S-boxes have been used in KASUMI and MISTY, but DBN and LBN of 7-bit S-boxes have not been studied.

With minor modifications, the theorems presented in Section II can be applied not only to the 6-bit S-boxes but also to the 7-bit S-boxes. We were able to find 6-bit S-boxes with DBN and LBN of 3 using three 3-bit S-boxes in the Feistel structure. Using two 4-bit S-boxes and a 3-bit S-box in the unbalanced-MISTY structure, we were able to find 7-bit S-boxes with DBN and LBN of 3. Since these are based on 3 and 4-bit small S-boxes, it is easy to find their efficient bitsliced implementations (some are described in Appendix B). The 6 and 7-bit S-boxes we found are compared with published ones in Table 2.

## D. APPLICATION OF OUR S-BOX ON BLOCK CIPHER DESIGN

In general, in the SPN structure, the confusion is provided by the substitution function, and a diffusion layer is constructed using an MDS matrix, a binary matrix with a large branch number, or a bit permutation with a low branch number. Although there have been many studies on efficient matrices [6], [12], [30]–[32], bit permutation is a very attractive candidate for diffusion layer in lightweight block ciphers because it does not require any cost in hardware environment. Bit permutation based block ciphers use a large number of rounds to be immune to differential and linear attacks due to the weak diffusion effect. In order to reduce the amount of memory required for the implementation of the diffusion layer and increase the execution speed of block ciphers, PRESENT and GIFT propose new techniques that provide effective diffusions even based on bit permutations [1], [16]. The diffusion layer of the GIFT was chosen to be a BOGI (Bad Output must go to Good Input) bit permutation [16], whereas the PRESENT uses the S-box with DBN of 3 [1]. Since the new S-boxes we present in Tables 1 and 2 have high DBN

**TABLE 3. Comparison of 8-bit S-boxes with respect to cryptographic properties.**

| | Listing 1 | Listing 2 | Listing 3 | Listing 4 | PIPO | FLY | Fantomas | Robin | Scream v3 | AES |
|---|---|---|---|---|---|---|---|---|---|---|
| SAC | 0.5444 | 0.5234 | 0.5103 | 0.5762 | 0.5469 | 0.5400 | 0.4858 | 0.5188 | 0.4985 | 0.5049 |
| BIC for non-linearity | 98.1429 | 98 | 100.5714 | 96 | 98.8571 | 100.5714 | 100.2857 | 99.8571 | 101.8571 | 112 |
| BIC for SAC | 0.5091 | 0.5119 | 0.5135 | 0.5117 | 0.517 | 0.5103 | 0.5099 | 0.5041 | 0.5109 | 0.5046 |
| CI | 1,1,1,1,1,2,2,1 | 1,1,1,1,1,1,1,1 | 1,1,1,1,1,1,1,1 | 1,2,1,1,1,3,3,5 | 1,1,1,1,1,1,1,1 | 1,1,2,1,1,1,2,1 | 0,0,1,0,2,0,0,1 | 0,0,0,2,0,0,0,0 | 0,1,1,1,0,0,0,0 | 0,0,0,0,0,0,0,0 |
| AI | 4,4,4,4,4,3,3,4 | 4,4,3,3,3,3,3,4 | 3,2,3,3,3,4,4,3 | 2,3,3,3,3,2,2,2 | 3,3,4,4,4,3,3,4 | 4,3,3,3,4,3,3,3 | 3,4,4,3,4,3,3,2 | 4,3,3,3,4,4,3,4 | 3,4,3,4,4,4,4,4 | 4,4,4,4,4,4,4,4 |

**TABLE 4. Comparison of 6 and 7-bit S-boxes with respect to cryptographic properties.**

| | 6-bit S-boxes | | | 7-bit S-boxes | |
|---|---|---|---|---|---|
| | Sakar's S6 | Sakar's S6' | Listing 5 | MISTY, KASUMI | Listing 6 |
| SAC | 0.5660 | 0.5694 | 0.5764 | 0.5089 | 0.5721 |
| BIC for non-linearity | 24 | 24 | 24 | 56 | 48.57 |
| BIC for SAC | 0.5097 | 0.5167 | 0.5042 | 0.5102 | 0.5147 |
| CI | 1,1,1,1,1,1 | 1,1,1,1,1,1 | 1,1,1,1,1,1 | 0,0,0,0,0,0,0 | 1,1,1,1,1,1,1 |
| AI | 3,3,3,3,3,3 | 2,2,2,2,2,2 | 3,3,3,3,3,3 | 3,3,3,3,3,3,3 | 2,3,3,3,3,3,3 |

and LBN, if combined with appropriate bit permutations, instantiated block ciphers can be effectively secured.

The block cipher PIPO was designed with the S-box constructed by our method [21]. The ciphsr uses the 64-bit state as an 8 × 8 bit array, applying an S-box to each column and different 8-bit rotations to each row within one round. Therefore, the output bits of one S-box are positioned as inputs of different S-boxes in the next round. This design made it possible to secure cipher against differential and linear attacks with a small number of rounds through the combination of a bit permutation and an S-box with high DBN and LBN.

## IV. CONCLUSION AND FUTURE WORK

In this paper, we presented a widely applicable method for constructing lightweight S-boxes with DBN and LBN greater than 2, from smaller S-boxes. Using structures such as the Feistel, Lai-Massey, unbalanced-MISTY and unbalanced-Bridge structure, we were able to find many lightweight S-boxes with both DBN and LBN of at least 3. We believe that our proposed method can help cipher designers build lightweight S-boxes with high DBN and LBN.

For future work, it would be interesting to investigate the following research questions.

- Are there any other 8-bit S-boxes that have the same level of cryptographic properties as the new S-boxes listed in Table 1 but require fewer nonlinear operations?
- Are there secure and efficient 8-bit S-boxes with both DBN and LBN of 4?

## APPENDIX A
## ADDITIONAL CRYPTOGRAPHIC PROPERTIES OF S-BOXES

In Tables 1 and 2, we presented cryptographic properties that can be directly used for block cipher cryptanalyes. However, there are many other indicators for the cryptographic security of the S-box such as Correlation immunity (CI), Algebraic immunity (AI), SAC (Strict Avalanche Criterion), and BIC (Bit Independence Criterion) [33]–[35]. These indicators are often used when proposing a new S-box with high cryptographic security or an S-box for image encryption [7]–[9]. We define them as follows, and present and compare the corresponding values of the S-boxes in Tables 3 and 4. We can see that there is no significant difference between the values of our new S-boxes and others. Since the new S-boxes we present have high LBN, their correlation immunities are also higher than those of other S-boxes with an LBN of 2.

Let the independence matrix of an $n$-bit S-box $S = (f_1, \cdots, f_n)$ be given by

$$p_{i,j} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f_i(x) \oplus f_i(x \oplus e_j).$$

where $e_j$ is $j$-th standard basis. Then we can define cryptographic properties below.

- The Strict Avalanche Criterion (SAC) of an $n$-bit S-box $S = (f_1, \cdots, f_n)$ is
$$\frac{1}{2^{2n}} \sum_{\substack{1 \le i,j \le n \\ i \ne j}} p_{i,j}.$$
- The Bit Independence Criterion (BIC) for SAC of an $n$-bit S-box $S = (f_1, \cdots, f_n)$ is
$$\frac{1}{2^{2n} - 2^n} \sum_{\substack{1 \le i,j \le n \\ i \ne j}} \frac{1}{2^{2n}} \sum_{\substack{\Delta a \in \mathbb{F}_2^n \\ wt(\Delta a)=1}} \sum_{x \in \mathbb{F}_2^n} g_{i,j}(x) \oplus g_{i,j}(x \oplus \Delta a)$$
where $g_{i,j}(x) = f_i(x) \oplus f_j(x)$.
- The BIC for non-linearity of an $n$-bit S-box $S = (f_1, \cdots, f_n)$ is
$$\frac{1}{2^{2n} - 2^n} \sum_{\substack{1 \le i,j \le n \\ i \ne j}} NL(g_{i,j})$$
where $NL(g_{i,j})$ is non-linearity of $g_{i,j}$ for $g_{i,j}(x) = f_i(x) \oplus f_j(x)$.
- The Correlation Immunity of a Boolean function $f$ is the maximum number $t$ such that
$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \lambda_a \bullet x} = 0$$

where $wt(\lambda_a) \leq t$. The n-bit S-box $S = (f_1, \cdots, f_n)$ has CIs for each of $f_1, \cdots, f_n$.

- Algebraic Immunity (AI) of a Boolean function $f$ is the minimum order $d$ of a polynomial $p(x) \in \mathbb{F}_2[x]$ such that $p(f^{-1}(\{0\})) = \{0\}$ or $p(f^{-1}(\{1\})) = \{0\}$. The n-bit S-box $S = (f_1, \cdots, f_n)$ has AIs for each of $f_1, \cdots, f_n$.

## APPENDIX B
## BITSLICED IMPLEMENTATIONS OF NEW S-BOXES

Listings 1 – 6 represent bitsliced implementations of new S-boxes.

```
//(MSb: x[7], LSb: x[0]) :"b" represents bit
// Input: x[7], x[6], x[5], x[4], x[3],
    x[2], x[1], x[0]
t[0] = x[4]; t[1] = x[5]; t[2] = x[6]; t[3]
    = x[7];
//S4
t[4] = x[6];
x[7] ^= (x[6] | x[5]);
x[6] = (x[5] ^ (x[6] & x[7]));
x[5] = (x[4] ^ x[7]);
x[4] = (x[7] ^ (x[6] | x[5]));
x[7] = (t[4] ^ x[4]);
x[4] ^= (x[7] & x[5]);
//XOR and Swap
x[4] ^= x[0]; x[5] ^= x[1]; x[6] ^= x[2];
    x[7] ^= x[3];
x[0] = t[0]; x[1] = t[1]; x[2] = t[2]; x[3]
    = t[3];
t[0] = x[4]; t[1] = x[5]; t[2] = x[6]; t[3]
    = x[7];
//S4
t[4] = x[6];
x[7] ^= (x[6] | x[5]);
x[6] = (x[5] ^ (x[6] & x[7]));
x[5] = (x[4] ^ x[7]);
x[4] = (x[7] ^ (x[6] | x[5]));
x[7] = (t[4] ^ x[4]);
x[4] ^= (x[7] & x[5]);
//XOR and Swap
x[4] ^= x[0]; x[5] ^= x[1]; x[6] ^= x[2];
    x[7] ^= x[3];
x[0] = t[0]; x[1] = t[1]; x[2] = t[2]; x[3]
    = t[3];
t[0] = x[4]; t[1] = x[5]; t[2] = x[6]; t[3]
    = x[7];
//S4
t[4] = x[6];
x[7] ^= (x[6] | x[5]);
x[6] = (x[5] ^ (x[6] & x[7]));
x[5] = (x[4] ^ x[7]);
x[4] = (x[7] ^ (x[6] | x[5]));
x[7] = (t[4] ^ x[4]);
x[4] ^= (x[7] & x[5]);
//XOR and Swap
x[0] ^= x[4]; x[1] ^= x[5]; x[2] ^= x[6];
    x[3] ^= x[7];
x[4] = t[0]; x[5] = t[1]; x[6] = t[2]; x[7]
    = t[3];
// Output: x[7], x[6], x[5], x[4], x[3],
    x[2], x[1], x[0]
```

**LISTING 1. The bitsliced implementation of the S-box with both DBN and LBN of 3 constructed by the Feistel structure (in C code).**

```
//(MSb: x[7], LSb: x[0]) :"b" represents bit
// Input: x[7], x[6], x[5], x[4], x[3], x[2],
    x[1], x[0]
// XOR
t[0]=x[4]^x[0];t[1]=x[5]^x[1];
t[2]=x[6]^x[2];t[3]=x[7]^x[3];
// S5_1
t[4] = t[2];
t[3] ^= (t[2] | t[1]);
t[2] = (t[1] ^ (t[2] & t[3]));
t[1] = (t[0] ^ t[3]);
t[0] = (t[3] ^ (t[2] | t[1]));
t[3] = (t[4] ^ t[0]);
t[0] ^= (t[3] & t[1]);
// XOR
x[4]^=t[0]; x[5]^=t[1]; x[6]^=t[2];
    x[7]^=t[3];
// S5_2
t[4] = x[6];
x[7] ^= (x[6] | x[5]);
x[6] = (x[5] ^ (x[6] & x[7]));
x[5] = (x[4] ^ x[7]);
x[4] = (x[7] ^ (x[6] | x[5]));
x[7] = (t[4] ^ x[4]);
x[4] ^= (x[7] & x[5]);
// XOR
x[0]^=t[0]; x[1]^=t[1]; x[2]^=t[2];
    x[3]^=t[3];
// S5_3
x[2] ^= (x[1]& x[0]);
x[0] ^= x[2];
x[1] ^= x[3];
x[2] ^= (x[3] | x[1]);
x[3] ^= x[0];
x[0] ^= (x[2]| x[1]);
x[1] ^= (x[2]& x[0]);
// Output: x[7], x[6], x[5], x[4], x[3],
    x[2], x[1], x[0]
```

**LISTING 2. The bitsliced implementation of the S-box with both DBN and LBN of 3 constructed by the Lai-Massey structure (in C code).**

```
//(MSb: x[7], LSb: x[0]) :"b" represents bit
// Input: x[7], x[6], x[5], x[4], x[3], x[2],
    x[1], x[0]
// S5_1
x[6]^=(x[7] & x[3]);
x[7]^=x[6];
x[4]^=(x[7] & x[5]);
x[5]^=x[4];
x[7]^=(x[3] | x[4]);
x[4]^=x[6];
x[3]^=(x[6] | x[5]);
// Extend XOR
x[7] ^= x[0];x[6] ^= x[2];x[5] ^= x[1];
// S3
x[1] = ~x[1];
x[1] ^= x[0] & x[2];
x[0] ^= x[2] | x[1];
x[2] ^= x[0] & x[1];
// Truncated XOR
x[2] ^= x[7];x[1] ^= x[6];x[0] ^= x[5];
// S5_2
x[4] ^= (x[7] & x[5]);
x[7] ^= x[3];
x[3] ^= x[4];
x[6] ^= (x[4] & x[7]);
x[5] ^= x[4];
x[3] ^= (x[6] & x[5]);
x[5] ^= (x[3] | x[6]);
// Output: x[7], x[6], x[5], x[4], x[3],
    x[2], x[1], x[0]
```

**LISTING 3. The bitsliced implementation of the S-box with both DBN and LBN of 3 constructed by the unbalanced-MISTY structure (in C code).**

```
//(MSb: x[7], LSb: x[0]) :"b" represents bit
// Input: x[7], x[6], x[5], x[4], x[3], x[2],
    x[1], x[0]
// S5_1
t[0] = x[7] ^ x[5];
t[1] = x[6] ^ t[0];
t[2] = x[3] ^ x[4];
t[3] = x[7] ^ (t[0] | t[1]);
t[4] = x[5] ^ (x[7] & t[1]);
x[5] = t[3] ^ x[6] ^ t[2];
x[6] = t[1] ^ (x[4] | x[3]);
x[3] = x[4];
x[7] = t[2] ^ x[6];
x[4] = t[4];
// S3
t[0] = x[1] ^ x[2];
t[1] = x[0] ^ t[0];
t[2] = t[1] | x[1];
t[3] = t[1] & t[0];
x[1] = t[3] ^ t[2];
x[0] = x[2] ^ t[3];
x[2] = t[1];
// XOR
x[7] ^= x[2];x[6] ^= x[1];x[5] ^= x[0];
// S5_2
t[0] = x[6] ^ x[7];
t[1] = t[0] ^ x[3];
t[2] = t[1] ^ (x[5] | x[6]);
t[3] = x[4] ^ (t[2] & x[3]);
t[4] = x[6] ^ t[3];
t[1] ^= (x[4] & x[5]);
x[3] = x[5] ^ t[4];
x[4] = x[3] ^ t[2];
t[2] = t[1] ^ x[5];
t[0] ^= x[5];
// XOR
x[2] ^= t[2];x[1] ^= t[1];x[0] ^= t[0];
// Output: x[7], x[6], x[5], x[4], x[3],
    x[2], x[1], x[0]
```

**LISTING 4.** **The bitsliced implementation of the S-box with DBN of 4 and LBN of 3 constructed by the unbalanced-Bridge (in C code).**

```
//(MSb: x[5], LSb: x[0]) :"b" represents bit
// Input: x[5], x[4], x[3], x[2], x[1], x[0]
// S3_1
t[2] = x[4] ^ x[5];
t[1] = x[5] ^ x[3];
t[0] = x[4] | x[3];
t[0] = t[1] ^ t[0];
t[1] = t[1] | t[2];
t[2] = t[2] & x[3];
// XOR
x[0]^=t[0]; x[1]^=t[1]; x[2]^=t[2];
// S3_2
t[2] = x[0] & x[1];
t[2] = t[2] ^ x[2];
t[0] = x[1] | x[2];
t[0] = t[0] ^ x[0];
t[1] = x[2] & t[0];
t[1] = t[1] ^ x[1];
// XOR
x[3]^=t[0]; x[4]^=t[1]; x[5]^=t[2];
// S3_3
t[2] = x[4] & x[3];
t[1] = t[2] ^ x[5];
t[2] = x[5] | x[4];
t[2] = x[3] ^ t[2];
t[0] = t[2] ^ x[4];
t[0] = x[5] & t[0];
// XOR
x[0]^=t[0]; x[1]^=t[1]; x[2]^=t[2];
// Output: x[5], x[4], x[3], x[2], x[1], x[0]
```

**LISTING 5.** **The bitsliced implementation of the 6-bit S-box with both DBN and LBN of 3 constructed by the Feistel structure (in C code).**

```
//(MSb: x[6], LSb: x[0]) :"b" represents bit
// Input: x[6], x[5], x[4], x[3], x[2], x[1],
    x[0]
// S4_1
x[4] ^= x[5] & x[3];
x[5] ^= x[4];
x[3] ^= x[6];
x[4] ^= x[6] | x[3];
x[6] ^= x[5];
x[5] ^= x[3] | x[4];
x[3] ^= x[5] & x[4];
T[0]=x[6]; x[6] = x[3]; x[3] = T[0];
// Extend XOR
x[4]^=x[0]; x[5]^=x[1]; x[6]^=x[2];
// S3
T[0] = x[1] | x[2];
T[2] = x[1];
x[1] = T[0] ^ x[0];
T[1] = ~x[2];
T[0] = x[1] & x[2];
x[2] = T[2] ^ T[0];
T[0] = T[2] | x[1];
x[0] = T[0] ^ T[1];
// Truncated XOR
x[0]^=x[4]; x[1]^=x[5]; x[2]^=x[6];
// S4_2
x[5] ^= x[6]& x[4];
x[6] ^= x[5];
x[4] ^= x[3];
x[5] ^= x[3] | x[4];
x[3] ^= x[6];
x[6] ^= x[4] | x[5];
x[4] ^= x[6] & x[5];
T[0] = x[4]; x[4] = x[3]; x[3] = T[0];
// Output: x[6], x[5], x[4], x[3], x[2],
    x[1], x[0]
```

**LISTING 6.** **The bitsliced implementation of the 7-bit S-box with both DBN and LBN of 3 constructed by unbalanced-MISTY structure (in C code).**

## REFERENCES

[1] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 4727. Berlin, Germany: Springer, 2007, pp. 450–466.

[2] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA (extended abstract)," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 4593. Berlin, Germany: Springer, 2007, pp. 181–195.

[3] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1109. Berlin, Germany: Springer, 1996, pp. 104–113.

[4] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalçin, "Block ciphers—Focus on the linear layer (feat. PRIDE)," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 8616. Berlin, Germany: Springer, 2014, pp. 57–76.

[5] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, "Ciphers for MPC and FHE," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 9056. Berlin, Germany: Springer, 2015, pp. 430–454.

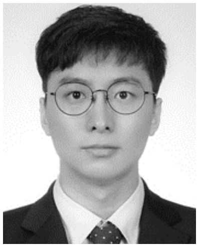
[6] V. Grosso, G. Leurent, F. Standaert, and K. Varici, "LS-designs: Bitslice encryption for efficient masked software implementations," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 8540. Berlin, Germany: Springer, 2014, pp. 18–37.

[7] A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption," *Electronics*, vol. 10, no. 12, p. 1392, 2021.

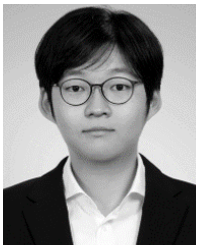
[8] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, 2019.

[9] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, "A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes," *Multimedia Tools Appl.*, vol. 80, no. 16, pp. 24801–24822, 2021.

[10] J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard," in *Information Security and Cryptography*. Berlin, Germany: Springer, 2002.
[11] E. Käsper and P. Schwabe, "Faster and timing-attack resistant AES-GCM," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 5747. Berlin, Germany: Springer, 2009, pp. 1–17.
[12] B. Gérard, V. Grosso, M. Naya-Plasencia, and F. Standaert, "Block ciphers that are easier to mask: How far can we go?" in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 8086, G. Bertoni and J. Coron, Eds. Berlin, Germany: Springer, 2013, pp. 383–399.
[13] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 9453. Berlin, Germany: Springer, 2015, pp. 411–436.
[14] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, "The *SKINNY* family of block ciphers and its low-latency variant *MANTIS*," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 9815. Berlin, Germany: Springer, 2016, pp. 123–153.
[15] P. Karpman and B. Grégoire, "The LITTLUN S-box and the FLY block cipher," in *Proc. Lightweight Cryptogr. Workshop*, 2016, pp. 17–18.
[16] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, "Gift: A small present towards reaching the limit of lightweight encryption," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 10529. Cham, Switzerland: Springer, 2017, pp. 321–345.
[17] B. Bilgin, L. De Meyer, S. Duval, I. Levi, and F. X. Standaert, "Low and depth and efficient inverses: A guide on s-boxes for low-latency masking," *IACR Trans. Symmetric Cryptol.*, vol. 2020, no. 1, pp. 144–184, 2020.
[18] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 6917. Berlin, Germany: Springer, 2011, pp. 326–341.
[19] A. Adomnicai, T. P. Berger, C. Clavier, J. Francq, P. Huynh, V. Lallemand, K. Le Gouguec, M. Minier, L. Reynaud, and G. Thomas, "Lilliput-AE: A new lightweight tweakable block cipher for authenticated encryption with associated data," NIST Lightweight Project, Gaithersburg, MD, USA, 2019.
[20] A. Canteaut, S. Duval, and G. Leurent, "Construction of lightweight S-boxes using feistel and MISTY structures," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 9566. Berlin, Germany: Springer, 2016, pp. 373–393.
[21] H. Kim, Y. Jeon, G. Kim, J. Kim, B. Y. Sim, D. G. Han, H. Seo, S. Kim, S. Hong, J. Sung, and D. Hong, "*PIPO*: A lightweight block cipher with efficient higher-order masking software implementations," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 12593. Cham, Switzerland: Springer, 2020, pp. 99–122.
[22] C. P. Ruisanchez, "A new algorithm to construct S-boxes with high diffusion," *Int. J. Soft Comput., Math. Control*, vol. 4, no. 3, pp. 42–50, 2015.
[23] S. Sarkar, K. Mandal, and D. Saha, "On the relationship between resilient Boolean functions and linear branch number of S-boxes," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 11898. Cham, Switzerland: Springer, 2019, pp. 361–374.
[24] P. Junod and S. Vaudenay, "FOX: A new family of block ciphers," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 3357. Berlin, Germany: Springer, 2004, pp. 114–129.
[25] Y. Li and M. Wang, "Constructing S-boxes for lightweight cryptography with feistel structure," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 8731. Berlin, Germany: Springer, 2014, pp. 127–146.
[26] M. Matsui, "New block encryption algorithm MISTY," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 1267. Berlin, Germany: Springer, 1997, pp. 54–68.
[27] B. Bilgin, L. De Meyer, S. Duval, I. Levi, and F. X. Standaert, "Low and depth and efficient inverses: A guide on S-boxes for low-latency masking," *IACR Trans. Symmetric Cryptol.*, vol. 2020, no. 1, pp. 144–184, 2020.
[28] *Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: Kasumi Specification*, document ETSI. TS 135 202 v7. 0.0, 3GPP, 2014.
[29] P. Zajac and M. Jókay, "Multiplicative complexity of bijective 4×4 S-boxes," *Cryptography Commun.*, vol. 6, no. 3, pp. 255–277, Sep. 2014.
[30] M. T. Sakalli, S. Akleylek, K. Akkanat, and V. Rijmen, "On the automorphisms and isomorphisms of MDS matrices and their efficient implementations," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 28, no. 1, pp. 275–287, Jan. 2020.
[31] M. K. Pehlivanoğlu, M. T. Sakallı, S. Akleylek, N. Duru, and V. Rijmen, "Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography," *IET Inf. Secur.*, vol. 12, no. 4, pp. 348–355, Jul. 2018.
[32] S. Akleylek, V. Rijmen, M. T. Sakallı, and E. Öztürk, "Efficient methods to generate cryptographically significant binary diffusion layers," *IET Inf. Secur.*, vol. 11, no. 4, pp. 177–187, Jul. 2017.
[33] S. Chee, S. Lee, D. Lee, and S. H. Sung, "On the correlation immune functions and their nonlinearity," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1163. Berlin, Germany: Springer, 1996, pp. 232–243.
[34] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3105–3121, Jul. 2006.
[35] Y. Wang, Q. Xie, Y. Wu, B. Du, Y. Wu, Y. Wang, B. Du, and Q. Xie, "A software for S-box performance analysis and test," in *Proc. Int. Conf. Electron. Commerce Bus. Intell.*, Beijing, China, 2009, pp. 125–128.



**HANGI KIM** received the B.S. degree in mathematics and the M.S. degree in financial information security from Kookmin University, Seoul, South Korea, in 2016 and 2018, respectively, where he is currently pursuing the Ph.D. degree in financial information security. His research interests include cryptographic primitives, cryptanalysis, and symmetric cryptosystems.



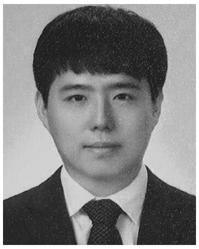
**YONGJIN JEON** received the B.S. degree in mathematics and the M.S. degree in financial information security from Kookmin University, Seoul, South Korea, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree in financial information security. His research interests include cryptographic primitives, cryptanalysis, and symmetric cryptosystems.

**GIYOON KIM** received the B.S. degree in information security, cryptology, and mathematics from Kookmin University, Seoul, South Korea, in 2019, where he is currently pursuing the combined M.S./Ph.D. degree in financial information security. His research interests include cryptographic primitives, cryptanalysis, artificial intelligence, and digital forensics.

**JONGSUNG KIM** received the B.S. and M.S. degrees in mathematics from Korea University, South Korea, in 2000 and 2002, respectively, and the dual Doctoral degree in combined differential, linear, and related-key attacks on block ciphers and MAC algorithms from the ESAT/COSIC Group, Katholieke Universiteit Leuven, Belgium, in 2006, and the Department of Information Security, Korea University, in 2007. He is currently a Full Professor with the Department of Information Security, Cryptology and Mathematics, and the Department Financial Information Security, Kookmin University, South Korea. His research interests include cryptanalysis, symmetric cryptosystems, and digital forensics.

**BO-YEON SIM** received the B.S. degree in mathematics, and the M.S. and Ph.D. degrees in information security from Kookmin University, Seoul, Republic of Korea, in 2013, 2015, and 2020, respectively. In 2020, she worked as a Research Professor with Kookmin University. She is currently working as a Researcher with Electronics and Telecommunications Research Institute (ETRI). Her research interests include side-channel attacks, cryptography, reverse engineering, and implementation of information protection technology for embedded systems.

**DONG-GUK HAN** received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in engineering in information security from Korea University, Seoul, Republic of Korea, in 1999, 2002, and 2005, respectively. He was a Postdoctoral Researcher with Future University Hakodate, Hokkaido, Japan. After finishing his doctoral course, he was then an Exchange Student with the Department of Computer Science and Communication Engineering, Kyushu University, Japan, from April 2004 to March 2005. From 2006 to 2009, he was a Senior Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea. He is currently working as a Professor with the Department of Information Security, Cryptology, and Mathematics, Kookmin University, Seoul, Republic of Korea. He is a member of KIISC, IEEK, and IACR.



**HWAJEONG SEO** received the B.S.E.E., M.S., and Ph.D. degrees in computer engineering from Pusan National University. He is currently an Assistant Professor at Hansung University. His research interests include the Internet of Things and information security.

**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.

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

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

**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 employed at ETRI. He currently holds the position of an Associate Professor with the Department of Information Technology and Engineering, Jeonbuk National University. His research interest includes symmetric cryptography.