Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 6, pp. 1665–1682
DOI : 10.47974/JDMSC-1572

Construction of S-boxes with LBN and DBN ≥ 4

Sonu Pal *
Department of Mathematics
Delhi University
New Delhi 110007
India

Saibal. K. Pal †
Research Scientist
Defence Research and Development Organisation
New Delhi 110054
India

Anupama Panigrahi §
Department of Mathematics
Delhi University
New Delhi 110007
India

Abstract

There is always a need for good and safe S-boxes in block ciphers for secure communication. To improve the security of lightweight block ciphers, S-boxes with high linear and diiferential branch numbers (LBN and DBN) are utilized. Many of these S-boxes have been built in recent years. Sarkar et. al. built S-boxes with LBN and DBN both equal to 3. Kim Hangi et. al. also created 8-bit S-boxes using smaller S-boxes with at least 3 LBN and DBN. In this direction, we narrow the search space of 8 × 8 S-boxes with LBN = DBN = 4. We used the Feistel and Lai-Massey structures to build these S-boxes. We present a detailed explanation of such 8 × 8 S-boxes.

Subject Classification: *94A60.*

Keywords: *Substitution box, Feistel and Lai-massey structures, Linear branch number, Differential branch number.*

* *E-mail:* **sonupal923@gmail.com (Corresponding Author)**
† *E-mail:* **skptech@yahoo.com**
§ *E-mail:* **anupama.panigrahi@gmail.com**

1. Introduction

It was Shannon who identified two important properties of the block ciphers, such as confusion and diffusion [23]. In any cryptographic algorithm, we achieve confusion with a substitution box (S-box) and diffusion with a permutation. Some other properties, like differential probability and linear probability, are also used in an S-box to protect it from differential and linear attacks. Mohammed et. al. suggested several such properties in [19]. Specifically, an S-box has to have high nonlinearity, balancing, bijectivity, low linear approximation probability, low differential probability, or either no or low numbers of fixed and opposite fixed points.

In the literature, many methodologies and programmes are implemented for the construction of such S-boxes. We can broadly classify them into the following three methods:

1. Algebraic Method.
2. Random Search.
3. Heuristic Method.

The first method, "Algebraic," had been implemented by Rijndael (the creator of AES) in 2001 for the construction of an AES S-box using an inverse function in a Galois field $GF(256)$ with 256 elements and then by applying the affine mapping. Currently, this is the best construction of an S-box using the above algebraic method.

The authors in [12] had modified the sequence of operations involving inversion in a Galois field with 256 elements and the affine mapping in it, resulting in an enhancement of the algebraic complexity of the S-box. However, this method reduces the security of the S-box used in the decryption algorithm. In [7, 13, 21, 24], the problem had been solved by applying the affine mapping twice, which maintained the number of terms in the algebraic expressions for both the encryption and decryption sides.In [6], Jie et. al. proposed a new S-box for AES by making suitable changes in the affine mapping step that increased the algebraic complexity of the AES S-box from 9 to 255. The random search approach is generally not preferred due to the vast search space, which increases the infeasibility of finding a cryptographically secure S-box in a given time frame. Consequently, the likelihood of obtaining a favorable S-box is reduced. As demonstrated in the study conducted by the authors in [18], an S-box was proposed utilizing a random binary sequence.

The resulting S-box exhibited cryptographic properties that were deemed weak. The heuristic method is the most preferred method among researchers. In this method, we find the S-box of good cryptographic properties using mathematical methods and iterations.In this approach, varieties of methods have been discussed, such as the chaotic map approach, the coset diagram approach, the evolutionary algorithm approach, and the natural-induced approach. In [17], Mamadolimov et. al. have constructed an S-box using power and binomial functions over some finite field. In [26], Zahid et. al. proposed an 8×8 S-box using cubic polynomial mapping, with an average value of nonlinearity of 106.8. In [9, 11, 20], S-boxes were constructed using the transformations of the form $T(z)=\frac{az+b}{cz+d}$, where $ad-bc\neq0$. However, these methods are not always the best choice for constraint conditions like low implementation costs, reduced area, low power consumption, etc. To overcome this situation, lightweight cryptography has been used, which provides several alternative block ciphers with smaller S-boxes, such as TEA [25], PRESENT [3], PRINCE [4], CRYPTON [15, 16], PRIDE [1], KATAN [8], the LS Designs [10], etc. We concentrate on constructing 8×8 S-boxes with smaller S-boxes.This general approach has been used in various ciphers such as CRYPTON [15] (3–round Feistel), WHIRLPOOL [2] (using 5 smaller S-boxes), LS- Designs [10] (3-round Feistel and Misty network), etc., which depend on Feistel, Lai Massey, and Unbalanced Misty structures. In [14], Kim Hangi et. al. give some conditions that completely characterize 8-bit S-boxes with LBN and DBN of at least three. They construct such S-boxes by eliminating all those input differentials (respectively, masks) and output differentials (respectively, masks) for which the sum of their Hamming weight is 2. In the same direction, but we have deleted all input differentials (respectively, masks) and output differentials (respectively, masks) with Hamming weight sums of 3 or less. In the above process, we characterize all 8×8 S-boxes with LBN and DBN at least 4.

2. Our Contribution

In Section 1 of this paper, we have given a brief introduction to various ways of constructing the S-boxes. We have discussed our work in Section 2. We have given some preliminary definitions and notations that we frequently used in this paper, which are mentioned in Section 3. Section 4 has two subsections. In the first Subsection, 4.1, we have used the Feistel structure to characterize those bijective 8-bit S-boxes for which, LBN and

DBN must be at least 4. In the second Subsection 4.2, we have used the Lai-Massey structure to characterize those bijective 8-bit S-boxes for which, LBN and DBN must be at least 4. After analyzing all four sections, we come to a certain conclusion, which is discussed in the last Section 5.

3. Some Preliminary Definitions and Notations

In this section, we mention a few notations and definitions as defined in [14]. For the sake of convenience, we are rephrasing the definition and notations here as follows:

- Difference Distribution Table (DDT) : Let S be an m-bit S-box, then its DDT is a rectangular array of order $2^m \times 2^m$ whose $(\Delta e, \Delta f)$ entry is given as;

$$\#\{U \in \mathbb{F}_2^m \mid S(U) \oplus S(U \oplus \Delta e) = \Delta f\},$$

  where $\Delta e, \Delta f \in \mathbb{F}_2^m$.
- Linear Approximation Table (LAT) :The LAT of an m-bit S-box is a rectangular array of size $2^m \times 2^m$, where each entry (e, f) is given by the expression

$$\#\{U \in \mathbb{F}_2^m \mid e \cdot U = f \cdot S(U)\} - 2^{m-1}.$$

  Here, e and f are elements of the vector space $\mathbb{F}_2^m$, and the $\cdot$ symbol represents the standard inner product operation.
- Correlation matrix : Let S be an m-bit S-box and $e, f \in \mathbb{F}_2^m$, then its correlation matrix T_S is a $2^m \times 2^m$ matrix whose (e, f) entry is given as

$$T_S(e, f) = \sum_{U \in \mathbb{F}_2^m} (-1)^{e \cdot U \oplus f \cdot S(U)}.$$

- Differential Branch Number (DBN) :Consider a $m \times m$ bijective S-box denoted by S. The DBN of S is given by the expression

$$\min_{e, f \in \mathbb{F}_2^m, f \neq e} (wt(e \oplus f) + wt(S(e) \oplus S(f))),$$

  where $e \oplus f$ represents the input differential and $S(e) \oplus S(f)$ represents the corresponding output differential.
- Linear Branch number (LBN) :The LBN of an $m \times m$ S-box S is defined as

$$\min_{e,f,T_S(e,f)\neq 0} (wt(e)+wt(f)),$$

where e, f are the input and output masks in $\mathbb{F}_2^m$.

- 0^i : a string of 0s of length i.
- S_i : denotes the i^{th} S-box of 4-bits.

4. Constructing 8-bit S-boxes that have LBN and DBN at least 4

We construct 8×8 S-boxes by eliminating those input differentials (respectively, masks) and output differentials (respectively, masks) for which, the sum of their Hamming weight is 3. We are using three smaller 4-bit S-boxes to construct 8-bit S-boxes. Many alternative ways for constructing 8-bit S-boxes can be found in the literature. Most of them possess the **Feistel**, **Massey**, or (unbalanced) **MISTY** structures. However, we use the Feistel and Lai-Massey structure due to its simplicity. We also assume that all smaller S-boxes constituted in these structures are bijective.

We can easily observe from [14, Figure 1-(A) and (B)] that these Feistel and Lai-Massey structures have two inputs and two outputs. The inputs L and R denotes the left and right input of these structures respectively, while the $LO(L,R)$ and $RO(L,R)$ denotes the corresponding left and right outputs of these structures respectively.

According to the research conducted by Kim Hangi et. al. [14], S-boxes that possess a DBN of at least 4 can be generated by eliminating the input

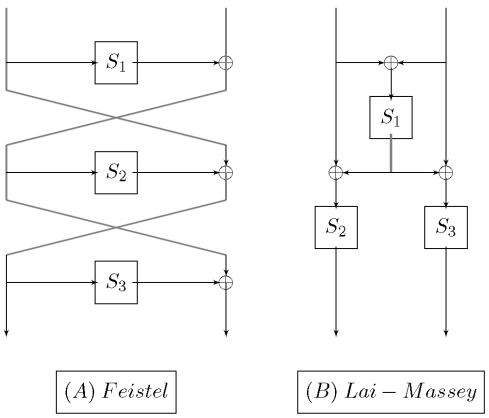

Figure 1

Feistel and Lai-Massey Structures

differential and output differential, provided that the combined Hamming weight of both differentials is equal to 3. This results in the 12 cases stated in Table 1. Let $(\Delta e, \Delta f)$ represent a pair of input and output differentials of the S-box S.

Table 1
Possible Cases Table

(i)	$(\Delta 0 \| \| \Delta e, \Delta 0 \| \| \Delta g)$	(v)	$(\Delta 0 \| \| \Delta e, \Delta 0 \| \| \Delta g)$	(ix)	$(\Delta 0 \| \| \Delta e, \Delta h \| \| \Delta g)$
(ii)	$(\Delta 0 \| \| \Delta e, \Delta h \| \| \Delta 0)$	(vi)	$(\Delta 0 \| \| \Delta e, \Delta h \| \| \Delta 0)$	(x)	$(\Delta f \| \| \Delta 0, \Delta h \| \| \Delta g)$
(iii)	$(\Delta f \| \| \Delta 0, \Delta 0 \| \| \Delta g)$	(vii)	$(\Delta f \| \| \Delta 0, \Delta 0 \| \| \Delta g)$	(xi)	$(\Delta f \| \| \Delta e, \Delta 0 \| \| \Delta g)$
(iv)	$(\Delta f \| \| \Delta 0, \Delta h \| \| \Delta 0)$	(viii)	$(\Delta f \| \| \Delta 0, \Delta h \| \| \Delta 0)$	(xii)	$(\Delta f \| \| \Delta e, \Delta h \| \| \Delta 0)$

- In the first four cases $wt(\Delta e) = (\Delta f) = 2$ and $wt(\Delta g) = wt(\Delta h) = 1$.
- From (v) to (viii) cases $wt(\Delta e) = (\Delta f) = 1$ and $wt(\Delta g) = wt(\Delta h) = 2$.
- From (ix) to (xii) cases $wt(\Delta e) = (\Delta f) = 1$ and $wt(\Delta g) = wt(\Delta h) = 1$.

4.1 *Feistel Structure*

The Feistel structure is used to build an 8-bit S-box S from three smaller 4-bit S-boxes, say $S_1, S_2,$ and S_3. The S-box is defined as

$$S(L \| R) = LO(L, R) \| RO(L, R),$$

where $L,\ R \in \mathbb{F}_2^4$. The input and its corresponding output variables that are used in the Feistel structure are linked with the relation as follows:

$$LO(L, R) = L \oplus S_2(R \oplus S_1(L)),$$
$$RO(L, R) = R \oplus S_1(L) \oplus S_3(L \oplus S_2(R \oplus S_1(L))).$$

The following theorems in this section provide necessary and sufficient conditions on the smaller 4-bit S-boxes to construct the larger 8-bit S-boxes using the Fesitel structure, which have the $DBN \geq 4$ and $LBN \geq 4$.

Theorem 4.1: *The bijective* 8×8 *S-box S, which is constructed by the Feistel structure, has the DBN greater than 3 if and only if the following conditions from (i) to (viii) are satisfied concurrently. Here, in the below conditions* Δe, Δf, *and* Δg *represent 4-bit differences with the possible Hamming weights as stated in Table 1. For each* $\Delta e, \Delta f$, *and* Δg,

(i) *the* $(\Delta e, \Delta 0)$ *entry in the DDT of* S_2 *is zero,*

(ii) *at least one of the* $(\Delta e, \Delta f)$ *and* $(\Delta f, \Delta e)$ *entries in the DDT's of* S_2 *and* S_3 *respectively is zero,*

(iii) *at least one of the* $(\Delta e, \Delta f)$ *and* $(\Delta f, \Delta e)$ *entries in the DDT's of* S_1 *and* S_2 *respectively is zero,*

(iv) *there is no solution pair* (P, Q) *for at least one of* $S_2(Q) \oplus S_2(Q \oplus S_1(P) \oplus S_1(P \oplus \Delta e)) = \Delta e \oplus \Delta f$ *and* $S_3(S_2(Q) \oplus P) \oplus S_3(S_2(Q) \oplus P \oplus \Delta f) = S_1(P) \oplus S_1(P \oplus \Delta e)$, *where* $P, Q \in \mathbb{F}_2^4$,

(v) *at least one of the* $(\Delta e, \Delta f)$ *and* $(\Delta f, \Delta g \oplus \Delta e)$ *entries in the DDT's of* S_2 *and* S_3 *respectively is zero,*

(vi) *there is no solution pair* (P, Q) *for at least one of* $(S_2(Q)) \oplus S_2(Q \oplus S_1(P) \oplus S_1(P \oplus \Delta e) = \Delta e \oplus \Delta g$ *and* $S_3(P \oplus S_2(Q)) \oplus S_3(P \oplus S_2(Q) \oplus \Delta g) = S_1(P) \oplus S_1(P \oplus \Delta e) \oplus \Delta f$, *where* $P, Q \in \mathbb{F}_2^4$,

(vii) *at least one of the* $(\Delta e, \Delta f \oplus \Delta g)$ *and* $(\Delta g, \Delta e)$ *entries in the DDT's of* S_1 *and* S_2 *respectively is zero,*

(viii) *there is no solution pair* (P, Q) *for at least one of* $S_2(Q) \oplus S_2(Q \oplus S_1(P) \oplus S_1(P \oplus \Delta f) \oplus \Delta e) = \Delta f \oplus \Delta g$ *and* $S_3(P \oplus S_2(Q)) \oplus S_3(P \oplus S_2(Q) \oplus \Delta g) = S_1(P) \oplus S_1(P \oplus \Delta f) \oplus \Delta e$, *where* $P, Q \in \mathbb{F}_2^4$

Proof: Some notations are defined for convenience to express the equations as follows:

$$A = R \oplus S_1(L) \text{ and } B = L \oplus S_2(A)$$

The first 8 possible cases are equivalent to the conditions from (i) to (iv) of the Theorem 4.1. For the proof, see [14, Theorem 1]. Now, we consider the other possible cases.

$\underline{(0^4 \,||\, \Delta e, \Delta h \,||\, \Delta g)}$: The necessary and sufficient condition for the existence of this case is the existence of at least one pair (L, R) which satisfies both the equations $LO(L, R) \oplus LO(L, R \oplus \Delta e) = \Delta h$ and $RO(L, R) \oplus RO(L, R \oplus \Delta e) = \Delta g$. Expanding the initial equation, we obtain

$$L \oplus S_2(R \oplus S_1(L)) \oplus L \oplus S_2(R \oplus \Delta e \oplus S_1(L)) = \Delta h.$$

By using the variable A, we get

$$S_2(A) \oplus S_2(A \oplus \Delta e) = \Delta h. \tag{1}$$

Similarly, by applying B and using the Eq.(1), the later equation is reduced as

$$S_3(B) \oplus S_3(B \oplus \Delta h) = \Delta g \oplus \Delta e. \tag{2}$$

As the mapping $(L,R) \mapsto (A,B)$ is bijective, the case $(0^4 \,||\, \Delta e, \Delta h \,||\, \Delta g)$ does not occur if and only if no such pair (A,B) exists meeting Eqs.(1 and 2), which is similar to condition (v) of the Theorem 4.1.

$(\Delta f \,||\, 0^4, \Delta h \,||\, \Delta g)$: The necessary and sufficient condition for the existence of the above case is the existence of at least one pair (L,R) which satisfies both the equations $LO(L,R) \oplus LO(L \oplus \Delta f, R) = \Delta h$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R) = \Delta g$. Expanding the intial equation, we obtain

$$L \oplus S_2(R \oplus S_1(L)) \oplus L \oplus \Delta f \oplus S_2(R \oplus S_1(L \oplus \Delta f)) = \Delta h.$$

It becomes,

$$S_2(R \oplus S_1(L)) \oplus S_2(R \oplus S_1(L \oplus \Delta f)) = \Delta h \oplus \Delta f \tag{3}$$

By using the variable A and Eq.(3) in the later equation, we get

$$S_3(L \oplus S_2(A)) \oplus S_3(L \oplus S_2(A) \oplus \Delta h) = S_1(L) \oplus S_1(L \oplus \Delta f) \oplus \Delta g. \tag{4}$$

Since the mapping $(L,R) \mapsto (L,A)$ is a bijective mapping. So this case will not happen if and only if no such pair (L,A) exists meeting Eqs.(3 and 4), which is similar to condition (vi) of the Theorem 4.1.

$(\Delta f \,||\, \Delta e, 0^4 \,||\, \Delta g)$: The necessary and sufficent condition for the above case is the existence of at least one pair (L,R) which satisfies both the equations $LO(L,R) \oplus LO(L \oplus \Delta f, R \oplus \Delta e) = \Delta 0$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R \oplus \Delta e) = \Delta g$. The initial equation is reduced as

$$S_2(R \oplus S_1(L)) \oplus S_2(R \oplus \Delta e \oplus S_1(L \oplus \Delta f)) = \Delta f. \tag{5}$$

By using Eq.(5) in the later equation, we get

$$S_1(L) \oplus S_1(L \oplus \Delta f) = \Delta e \oplus \Delta g.. \tag{6}$$

Now by using Eq.(6) and variable A in Eq.(5), we get

$$S_2(A) \oplus S_2(A \oplus \Delta g) = \Delta f. \tag{7}$$

Since the mapping $(L,R) \mapsto (L,A)$ is a bijective mapping, so this case $(\Delta f \,||\, \Delta e, 0^4 \,|\, \Delta g)$ will not happen if and only if there does not exists any such pair (L,A) meeting Eq.(6) and Eq.(7), which is similar to condition (vii) of the Theorem 4.1.

$(\Delta f \,||\, \Delta e, \Delta h \,||\, 0^4)$: The necessary and sufficent condition for the above case to be feasable is the existence of at least a pair (L,R) which satisfies both the equations $LO(L,R) \oplus LO(L \oplus \Delta f, R \oplus \Delta e) = \Delta h$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R \oplus \Delta e) = \Delta 0$. The initial equation is reduced as

$$S_2(R \oplus S_1(L)) \oplus S_2(R \oplus \Delta e \oplus S_1(L \oplus \Delta f)) = \Delta f \oplus \Delta h. \quad (8)$$

By applying A and using Eq.(8) in the later equation, we get

$$S_3(R \oplus S_2(A)) \oplus S_3(L \oplus S_2(A) \oplus \Delta h) \oplus \Delta e = S_1(L) \oplus S_1(L \oplus \Delta f). \quad (9)$$

Now, substituting A in Eq.(8), we get

$$S_2(A) \oplus S_2(A \oplus \Delta e \oplus S_1(L) \oplus S_1(L \oplus \Delta f)) = \Delta f \oplus \Delta h. \quad (10)$$

Because the mapping $(L,R) \mapsto (L,A)$ is bijective, the case $(\Delta f \| \Delta e, \Delta h \| 0^4)$ does not occur if and only if no such pair (L,A) exists meeting Eq.(9) and Eq.(10), which is similar to condition (viii) of the Theorem 4.1.

Theorem 4.2: *The bijective 8×8 S-box S which is constructed by the Feistel structure has the LBN greater than 3 if and only if the following conditions from (i) to (viii) are satisfied concurrently. Here, in the below conditions e, f, and g represent arbitrary 4-bit masks with the possible Hamming weights as stated in Table 1. For each e, f, and g,*

(i) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid (Q \oplus S_1(P)) \cdot e = (Q \oplus S_2(Q)) \cdot f\} = 2^7$,

(ii) *a minimum of one of the (e,f) entries in LAT of S_1 and (f,e) entries in LAT of S_2 are both 0,*

(iii) *a minimum of one of the (e,f) entries in LAT of S_2 and (f,e) entries in LAT of S_3 are both 0,*

(iv) *the $(0,e)$ entry in LAT of S_2 is 0,*

(v) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid (Q \cdot (e \oplus f) \oplus S_2(Q) \cdot g \oplus S_3(P \oplus S_2(Q)) \cdot f = (P \cdot g \oplus S_1(P)) \cdot e\} = 2^7$,

(vi) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid P \cdot (e \oplus g) \oplus S_3(P \oplus S_2(Q)) \cdot f = Q \cdot f \oplus S_2(Q) \cdot g\} = 2^7$,

(vii) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid P \cdot g \oplus S_1(P) \cdot e = Q \cdot (e \oplus g) \oplus (S_3(P \oplus S_2(Q))) \cdot g\} = 2^7$,

(viii) *a minimum of one of the $(f \oplus g, e)$ entries in LAT of S_1 and (e,g) entries in LAT of S_2 are both 0.*

Proof: We follow the same notations LO, RO, A, and B as defined in Theorem 4.1.

The first 8 possible cases are equivalent to the conditions from (i) to (iv) of the Theorem 4.1. For the proof see [14, Theorem 2]. Now, we consider the other possible cases.

$\underline{(0^4 \| e, h \| g)}$: The bias in this situation is computed by counting the number of (L, R) pairings that meet the equation. $R \cdot e = LO(L, R) \cdot h \oplus RO(L, R) \cdot g$. After expanding this equation, we get

$$R \cdot e = (L \oplus S_2(R \oplus S_1(L))) \cdot h \oplus (R \oplus S_1(L) \oplus S_3(L \oplus S_2(R \oplus S_1(L))) \cdot g.$$

By using A in above equation, we get

$$A \cdot (e \oplus g) \oplus S_2(A) \cdot h = L \cdot h \oplus S_1(L) \cdot e \oplus S_3(L \oplus S_2(A)) \cdot g. \tag{11}$$

Due to the fact that the mapping $(L, R) \mapsto (L, A)$ is bijective, the case $(0^4 \| e, h \| g)$ has no bias at all if and only if Eq.(11) is not biased, which is similar to holding the condition (v) in Theorem 4.1.

$\underline{(f \| 0^4, h \| g)}$: The bias in this situation is computed by counting the number of (L, R) pairing that meets the equation $L \cdot f = LO(L, R) \cdot h \oplus RO(L, R) \cdot g$. By using the variable A, we obtain

$$L \cdot (f \oplus h) \oplus S_3(L \oplus S_2(A)) \cdot g = A \cdot g \oplus S_2(A) \cdot h. \tag{12}$$

As the mapping $(L, R) \mapsto \hat{A}(L, A)$ exhibits a bijective correspondence. Consequently, the case $(f \| 0^4, h \| g$ has no bias at all if and only if Eq.(12) is not biased, which is similar to holding the condition (vi) in Theorem 4.1.

$\underline{(f \| e, 0^4 \| g)}$: The bias in this case is computed by counting the number of (L, R) pairings that meet the equation $L \cdot f \oplus R \cdot e = RO(L, R) \cdot g$. By using the variable A, we obtain

$$L \cdot f \oplus S_1(L) \cdot e = A \cdot (e \oplus g) \oplus S_3(L \oplus S_2(A)) \cdot g \tag{13}$$

Due to the fact that the mapping $(L, R) \mapsto (L, A)$ is bijective, this case $(f \| e, 0^4 \| g)$ has no bias at all if and only if Eq.(13) is not biased, which is similar to holding the condition (vii) in Theorem 4.1.

$\underline{(f \| e, h \| 0^4)}$: The bias in this case is computed by counting the number of (L, R) pairings that meet the equation $L \cdot f \oplus R \cdot e = LO(L, R) \cdot h$. By using the variable A, we obtain

$$L \cdot (f \oplus h) \oplus S_1(L) \cdot e = A \cdot e \oplus (S_2(A)) \cdot h \tag{14}$$

Because the mapping $(L, R) \mapsto (L, A)$ is bijective, as a result, the case $(f \| e, h \| 0^4)$ has no bias at all if and only if Eq.(14) is not biased, which is similar to holding the condition (viii) in Theorem 4.1.

4.2 *Lai-Massey Structure*

The Lai-Massey structure can be defined as follows:

$$S(L \| R) = LO(L,R) \| RO(L,R),$$

where $L, R \in \mathbb{F}_2^4$ are the input varibales. The connection with the input variables and the associated output variables in the Lai-Massey structure is as follows:

$$LO(L,R) = S_2(L \oplus S_1(L \oplus R)),$$
$$RO(L,R) = S_3(R \oplus S_1(L \oplus R)).$$

In this section, we give necessary as well as sufficient conditions for the construction of 8-bit S-boxes with LBN and DBN at least 4. The subsequent theorems provide the necessary and sufficient conditions for the smaller 4-bit S-boxes to have the $DBN \geq 4$ and $LBN \geq 4$ values for the larger 8-bit S-boxes constructed by the Lai-Massey structure.

Theorem 4.3: *The bijective* 8×8 *S-box S, which is constructed by the Lai-Massey structure, has the* $DBN > 3$ *if and only if the following conditions from (i) to (viii) are satisfied concurrently. In the conditions given below,* Δe, Δf, *and* Δg *represent 4-bit differences with the possible Hamming weights as stated in Table 1. For each* $\Delta e, \Delta f$, *and* Δg,

(i) *at least one of the* $(\Delta e, \Delta 0)$ *and* $(\Delta e, \Delta f)$ *entries in the DDT's of* S_1 *and* S_3 *respectively is zero,*

(ii) *at least one of the* $(\Delta e, \Delta e)$ *and* $(\Delta e, \Delta f)$ *entries in the DDT's of* S_1 *and* S_2 *respectively, is zero,*

(iii) *at least one of the* $(\Delta e, \Delta e)$ *and* $(\Delta e, \Delta f)$ *entries in the DDT's of* S_1 *and* S_3 *respectively, is zero,*

(iv) *at least one of the* $(\Delta e, \Delta 0)$ *and* $(\Delta e, \Delta f)$ *entries in the DDT's of* S_1 *and* S_2 *respectively, is zero,*

(v) *there is no solution pair* (P, Q) *for at least one of the equations* $S_2(P \oplus S_1(P \oplus Q) \oplus S_2(P \oplus S_1(P \oplus Q \oplus \Delta e)) = \Delta g$ *and* $S_3(Q \oplus S_1(P \oplus Q)) \oplus S_3(P \oplus \Delta e \oplus S_1(P \oplus Q \oplus \Delta e)) = \Delta f$, *where* $P, Q \in \mathbb{F}_2^4$,

(vi) *there is no solution pair* (P, Q) *for at least one of the equations* $S_2(P \oplus S_1(P \oplus Q) \oplus S_2(P \oplus \Delta e \oplus S_1(P \oplus Q \oplus \Delta e)) = \Delta g$ *and* $S_3(Q \oplus S_1(P \oplus Q)) \oplus S_3(Q \oplus S_1(P \oplus Q \oplus \Delta e)) = \Delta f$, *where* $P, Q \in \mathbb{F}_2^4$,

(vii) *at least one of the* $(\Delta e \oplus \Delta f, \Delta f)$ *and* $(\Delta e \oplus \Delta f, \Delta g)$ *entries in the DDT's of* S_1 *and* S_3 *respectively, is zero,*

(viii) *at least one of the* $(\Delta e \oplus \Delta f, \Delta e)$ *and* $(\Delta e \oplus \Delta f, \Delta g)$ *entries in the DDT's of* S_1 *and* S_2 *respectively, is zero.*

Proof: Some notations which will be used in this theorem are as follows:

$$A = L \oplus R, B = R \oplus S_1(L \oplus R), \text{and}$$

$$C = L \oplus S_1(L \oplus R).$$

The first 8 possible cases are equivalent to the conditions from (i) to (iv) of the Theorem 4.3. For the proof, see [14, Theorem 3]. Now, we consider the other possible cases.

$\underline{(0^4 \,||\, \Delta e, \Delta h \,||\, \Delta g)}$: The necessary and sufficent conditions for the existence of this case is the existence of at least one pair (L, R) which satisfies both the equations: $LO(L,R) \oplus LO(L, R \oplus \Delta e) = \Delta h$ and $RO(L,R) \oplus RO(L, R \oplus \Delta e) = \Delta g$. By expanding the initial equation, we get

$$S_2(L \oplus S_1(L \oplus R)) \oplus S_2(L \oplus S_1(L \oplus R \oplus \Delta e)) = \Delta h. \tag{15}$$

Similarly by expanding the later equation, we obtain

$$S_3(R \oplus S_1(L \oplus R)) \oplus S_3(R \oplus \Delta e \oplus S_1(L \oplus R \oplus \Delta e)) = \Delta g. \tag{16}$$

The case $(0^4 \,||\, \Delta e, \Delta h \,||\, \Delta g)$ does not occur if and only if there is no such pair (L, R) meeting Eq.(15) and Eq.(16), which is similar to condition (v) of the Theorem 4.3.

$\underline{(\Delta f \,||\, 0^4, \Delta h \,||\, \Delta g)}$: The necessary and sufficent condition for the exitence of this case is the existence of at least one pair (L, R) which satisfies both the equations: $LO(L,R) \oplus LO(L \oplus \Delta f, R) = \Delta h$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R) = \Delta g$. Expanding the initial equation, we obtain

$$S_2(L \oplus S_1(L \oplus R)) \oplus S_2(L \oplus \Delta f \oplus S_1(L \oplus R \oplus \Delta f)) = \Delta h. \tag{17}$$

Similarly by expanding the later equation, we obtain

$$S_3(R \oplus S_1(L \oplus R)) \oplus S_3(R \oplus S_1(L \oplus R \oplus \Delta f)) = \Delta g. \tag{18}$$

The case $(\Delta e \,||\, 0^4, \Delta h \,||\, \Delta g)$ fails to occur if and only if there exists no such pair (L, R) meeting Eq.(17) and Eq.(18), which is equivalent to condition (vi) of the Theorem 4.3.

$\underline{(\Delta f \,||\, \Delta e, 0^4 \,||\, \Delta g)}$: The necessary and sufficent condition for the existence of this case is the existence of at least one pair (L, R) whcih satisfies both the equations: $LO(L,R) \oplus LO(L \oplus \Delta f, R \oplus \Delta e) = \Delta 0$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R \oplus \Delta e) = \Delta g$.

As S_2 is bijective, therefore by applying $(S_2)^{-1}$ and using variable A in initial equation, we get

$$S_1(A) \oplus S_1(A \oplus \Delta e \oplus \Delta f) = \Delta f \tag{19}$$

Similarly, by using Eq.(19) and variable B in the later equation, we obtain

$$S_3(B) \oplus S_3(B \oplus \Delta e \oplus \Delta f) = \Delta g. \tag{20}$$

Because the mappping $(L,R) \mapsto (A,B)$ is bijective, the above case $(\Delta f \,||\, \Delta e, 0^4 \,|\, \Delta g)$ does not occur if and only if no such pair (A,B) exists meeting Eq.(19) and Eq.(20), which is equivalent to condition (vii) of the Theorem 4.3.

$(\Delta f \,||\, \Delta e, \Delta h \,||\, 0^4)$: The necessary and sufficent condition for the existence of this case is the existence of at least one pair (L,R) which satisfies both the equations: $LO(L,R) \oplus LO(L \oplus \Delta f, R \oplus \Delta e) = \Delta h$ and $RO(L,R) \oplus RO(L \oplus \Delta f, R \oplus \Delta e) = \Delta 0$.

As S_3 is bijective, therefore by applying $(S_3)^{-1}$ and by substituting the variable A in the later equation, we obtain

$$S_1(A) \oplus S_1(A \oplus \Delta e \oplus \Delta f) = \Delta e \tag{21}$$

Similarly, by using Eq.(21) and variable C in intial equaion, we get

$$S_2(C) \oplus S_2(C \oplus \Delta e \oplus \Delta f) = \Delta h. \tag{22}$$

Because the mapping $(L,R) \mapsto (A,C)$ is bijective, the above case $(\Delta f \,||\, \Delta e, \Delta h \,||\, 0^4)$ does not occur if and only if no such pair (A,C) exists meeting Eq.(21) and Eq.(22), which is similar to holding condition (viii) in Theorem 4.3.

Theorem 4.4: *The bijective* 8×8 *S-box, constructed using the Lai Massey structure has the LBN at least 4 if and only if all the following conditions from (i) to (viii) holds simultaneously* $(e, f,$ *and* g *below represents arbitrary 4-bit masks with the possible Hamming weights as stated in Table 1)*

(i) *the* $(0,e)$ *entry in LAT of* S_1 *and at least one of the* (e,f) *entries in LAT of* S_3 *are both zero,*

(ii) *a minimum of one of the* (e,e) *entries in LAT of* S_1 *and* (e,f) *entries in LAT of* S_2 *are both zero,*

(iii) *a minimum of one of the* (e,e) *entries in LAT of* S_1 *and* (e,f) *entries in LAT of* S_3 *are both zero,*

(iv) *the* $(0,e)$ *entry in LAT of* S_1 *and at least one of the* (e,f) *entries in the LAT of* S_2 *are both zero,*

(v) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid Q\cdot e \oplus P\cdot e = (S_2(P \oplus S_1(Q))) \cdot g \oplus (S_3(P \oplus Q \oplus S_1(Q))) \cdot f\} = 2^7$,

(vi) $\#\{(P,Q) \in (\mathbb{F}_2^4)^2 \mid Q\cdot e \oplus P\cdot e = S_2(P \oplus Q \oplus S_1(Q)) \cdot g \oplus S_3(P \oplus S_1(Q)) \cdot f\} = 2^7$,

(vii) *a minimum of one of the* $(f, e\oplus f)$ *entries in LAT of* S_1 *and* $(e\oplus f, g)$ *entries in LAT of* S_3 *are both zero,*

(viii) *a minimun of one of the* $(e, e\oplus f)$ *entries in LAT of* S_1 *and* $(e\oplus f, g)$ *entries in LAT of* S_2 *are both zero.*

Proof: We follow the same notations for LO, RO, A, B and C as in Theorem 4.3.

The first 8 possible cases are equivalent to the conditions from (i) to (iv) of the Theorem 4.4. For the proof see [14, Theorem 4].. Now, we consider the other possible cases.

$\underline{(0^4 \| e,h \| g)}$: The bias in this situation is computed by counting the number of (L,R) pairing that meets the equation $R\cdot e = LO(L,R)\cdot h \oplus RO(L,R)\cdot g$.

By expanding and using the variable A in the above expression, we get

$$A\cdot e \oplus L\cdot e = S_2(L\oplus S_1(A))\cdot h \oplus S_3(L\oplus A\oplus S_1(A))\cdot g. \tag{23}$$

Because the mapping $(L,R)\mapsto(L,A)$ is bijective, as a result, the case $(0^4 \| e,h \| g)$ has no bias at all if and only if Eq.(23) is not biased, which is similar to holding the condition (v) in Theorem 4.4.

$\underline{(f \| 0^4,h \| g)}$: The bias in this situation is computed by the number of (L,R) pairing that meets the equation $L\cdot f = LO(L,R)\cdot h \oplus RO(L,R)\cdot g$.

By expanding and using the variable A in the above expression, we get

$$A\cdot f \oplus R\cdot f = S_2(R\oplus A\oplus S_1(A))\cdot h \oplus S_3(R\oplus A\oplus S_1(A))\cdot g. \tag{24}$$

Because the mapping $(L,R)\mapsto(A,R)$ is bijective, as a result, the case $(f \| 0^4,h \| g)$ has no bias at all if and only if Eq.(24) is not biased, which is similar to holding the condition (vi) in Theorem 4.4.

$\underline{(f \| e,0^4 \| g)}$: The bias of this case is computed by conting the number of (L,R) pairing that meets the equation $L\cdot f \oplus R\cdot e = RO(L,R)\cdot g$. By using the variables A and B, we obtain

$$A \cdot (f \oplus e) \oplus S_1(A) \cdot (e \oplus f) = B \cdot (e \oplus f) \oplus S_3(B) \cdot g \tag{25}$$

Since $(L,R) \mapsto (A,B)$ is a bijective mapping, therefore the case $(f \| e, 0^4 \| g)$ has no bias at all if and only if Eq.(25) is not biassed, which is similar to holding the condition (vii) in Theorem 4.4.

$\underline{(f \| e, h \| 0^4)}$: The bias of this case is computed by counting the number of (L,R) pairing that meets the equation $L \cdot f \oplus R \cdot e = LO(L,R) \cdot h$. By using the variables A and C, we obtain

$$A \cdot e \oplus S_1(A) \cdot (e \oplus f) = C \cdot (e \oplus f) \oplus S_2(C) \cdot h. \tag{26}$$

Since $(L,R) \mapsto (A,C)$ is a bijective mapping, therefore the case $(f \| e, h \| 0^4)$ has no bias at all if and only if Eq.(25) is not biassed, which is similar to holding the condition (viii) in Theorem 4.4.

5. Conclusion

We have provided both necessary and sufficient conditions for the construction of 8-bit S-boxes using Feistel and Lai-Massey structures. We have also improves the earlier lower to 4 from 3 in both LBN and DBN cases. The S-boxes exhibit the characteristic of possessing a lower bound of 4 in both LBN and DBN. The aforementioned findings will serve to decrease the search area when seeking the S-box with LBN and DBN equal to 4. In subsequent research, efforts will be made to explore the potential applications of these techniques to other extant structures, including Unbalanced-Misty and Unbalanced-Bridge structures.

Acknowledgement

The authors are extremely thankful to the anonymous referee for their valuable comments and suggestions that led to an overall improvement in quality and presentation for the article.

References

[1] Albrecht, M. R., Driessen, B., Kavun, E. B., Leander, G., Paar, C., & Yalçın, T., Block ciphers–focus on the linear layer (feat. PRIDE). *In Annual Cryptology Conference*, pp. 57-76 (2014, August). Springer, Berlin, Heidelberg.

[2] Barreto, P. S. L. M., & Rijmen, V., The Whirlpool hashing function. *In First Open NESSIE Workshop-CiteSeer, Leuven, Belgium*, Vol. 13, p. 14 (2000, November).

[3] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C., PRESENT: An ultra-lightweight block cipher. *In International workshop on cryptographic hardware and embedded systems*, pp. 450-466 (2007, September). Springer, Berlin, Heidelberg.

[4] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., ... & Yalçın, T., PRINCE–a low-latency block cipher for pervasive computing applications. *In International conference on the theory and application of cryptology and information security*, pp. 208-225 (2012, December). Springer, Berlin, Heidelberg.

[5] Canteaut, A., Duval, S., & Leurent, G., Construction of lightweight S-boxes using Feistel and MISTY structures. *In International Conference on Selected Areas in Cryptography*, pp. 373-393 (2015, August). Springer, Cham.

[6] Cui, J., Huang, L., Zhong, H., Chang, C., & Yang, W., An improved AES S-box and its performance analysis. *International Journal of Innovative Computing, Information and Control*, 7(5), 2291-2302 (2011).

[7] Cui, L., & Cao, Y., A new S-box structure named affine-power-affine. *International Journal of Innovative Computing, Information and Control*, 3(3), 751-759 (2007).

[8] De Canniere, C., Dunkelman, O., & Knežević, M., KATAN and KTANTAN–a family of small and efficient hardware-oriented block ciphers. *In International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 272-288 (2009, September). Springer, Berlin, Heidelberg.

[9] Farwa, S., Shah, T., & Idrees, L., A highly nonlinear S-box based on a fractional linear transformation. *SpringerPlus*, 5(1), 1-12 (2016).

[10] Grosso, V., Leurent, G., Standaert, F. X., & Varıcı, K., LS-designs: Bitslice encryption for efficient masked software implementations. *In International Workshop on Fast Software Encryption*, pp. 18-37 (2014, March). Springer, Berlin, Heidelberg.

[11] Hussain, I., Shah, T., Gondal, M. A., Khan, M., & Khan, W. A., Construction of new S-box using a linear fractional transformation. *World Appl. Sci. J*, 14(12), 1779-1785 (2011).

[12] Jingmei, L., Baodian, W., & Xinmei, W., One AES S-box to increase complexity and its cryptanalysis. *Journal of Systems Engineering and Electronics,* 18(2), 427-433 (2007).

[13] Karaahmetoğlu, O., Sakallı, M. T., Buluş, E., & Tutănescu, I., A new method to determine algebraic expression of power mapping based S-boxes. *Information Processing Letters,* 113(7), 229-235 (2013).

[14] Kim, H., Jeon, Y., Kim, G., Kim, J., Sim, B. Y., Han, D. G., ... & Hong, D., A new method for designing lightweight S-boxes with high differential and linear branch numbers, and its application. *IEEE Access,* 9, 150592-150607 (2021).

[15] Lim, C. H., CRYPTON: A New 128-bit Block Cipher-Specification and Analysis. *NIST AES Proposal-CiteSeer* (1998).

[16] Lim, C. H., A revised version of CRYPTON: CRYPTON V1. 0. *In International Workshop on Fast Software Encryption* (pp. 31-45). Springer, Berlin, Heidelberg (1999, March).

[17] Mamadolimov, A., Isa, H., & Mohamad, M. S., Practical bijective S-box design (2013). arXiv preprint arXiv:1301.4723.

[18] Mroczkowski, P., Generating Pseudorandom S-Boxes-a Method of Improving the Security of Cryptosystems Based on Block Ciphers. *Journal of Telecommunications and Information Technology*, 74-79 (2009).

[19] Mohamed, K., Pauzi, M. N. M., Ali, F. H. H. M., Ariffin, S., & Zulkipli, N. H. N., Study of S-box properties in block cipher. *In 2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, pp. 362-366(2014, September). IEEE.

[20] Qureshi, A., & Shah, T., S-box on subgroup of Galois field based on linear fractional transformation. *Electronics Letters*, 53(9), 604-606 (2017).

[21] Sakallı, M. T., Aslan, B., Buluş, E., Mesut, A. Ş., Büyüksaraçoğlu, F., & Karaahmetoğlu, O., On the algebraic expression of the AES S-box like S-boxes. *In International Conference on Networked Digital Technologies*, pp. 213-227 (2010, July). Springer, Berlin, Heidelberg.

[22] Sarkar, S., Mandal, K., & Saha, D., On the relationship between resilient Boolean functions and linear branch number of S-boxes. *In Progress in Cryptology–INDOCRYPT 2019: 20th International Conference on Cryptology in India, Hyderabad, India, December 15–18, 2019, Proceedings*, pp. 361-374 (2019, November). Cham: Springer International Publishing.

[23] Shannon, C. E., Communication theory of secrecy systems. *The Bell System Technical journal*, 28(4), 656-715 (1949).

[24] Tran, M. T., Bui, D. K., & Duong, A. D., Gray S-box for advanced encryption standard. *In 2008 International Conference on Computational Intelligence and Security*, Vol. 1, pp. 253-258 (2008, December). IEEE.

[25] Wheeler, D. J., & Needham, R. M., TEA, a tiny encryption algorithm. In International workshop on fast software encryption, pp. 363-366 (1994, December). Springer, Berlin, Heidelberg.

[26] Zahid, A., & Arshad, M., An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry*, 11(3), 437 (2019). doi:10.3390/sym11030437.

Received October, 2021

Revised March, 2022