Bounds on Differential and Linear Branch Number of Permutations

Sumanta Sarkar(✉) and Habeeb Syed

TCS Innovation Labs, Hyderabad, India
sumanta.sarkar1@tcs.com, habeeb.syed@tcs.com

Abstract. Nonlinear permutations (S-boxes) are key components in block ciphers. The differential branch number measures the diffusion power of a permutation, whereas the linear branch number measures resistance against linear cryptanalysis. There has not been much analysis done on the differential branch number of nonlinear permutations of $\mathbb{F}_2^n$, although it has been well studied in case of linear permutations. Similarly upper bounds for the linear branch number have also not been studied in general. In this paper we obtain bounds for both the differential and the linear branch number of permutations (both linear and nonlinear) of $\mathbb{F}_2^n$. We also prove that in the case of $\mathbb{F}_2^4$, the maximum differential branch number can be achieved only by affine permutations.

Keywords: Permutation · S-box · Differential branch number
Linear branch number · Block cipher · Griesmer bound

1 Introduction

A basic design principle of a block cipher consists of confusion and diffusion as suggested by Shannon [14]. Confusion layer makes the relation between key and the ciphertext as complex as possible, whereas diffusion layer spreads the plaintext statistics across the ciphertext. So far there have been several constructions of block ciphers, and equal efforts have been made to break them. In the process literature has been enriched by proposals of elegant cryptanalysis techniques, for instance, differential cryptanalysis [3] and linear cryptanalysis [12]. The latter two cryptanalysis methods led to the design known as wide-trail strategy [6]. This design constructs round transformations of block ciphers with efficiency and provides resistance against the differential and the linear cryptanalysis. This strategy also explains how the differential branch number is related to the number of active S-boxes.

Recently lightweight cryptography has gained huge attention from both the industry and academia. There have been several proposals of lightweight ciphers so far, which are mostly based on symmetric cryptography. In this work we are interested in block ciphers. Some examples of lightweight block ciphers are `CLEFIA` [15] and `PRESENT` [4]; both are included in the ISO/IEC 29192 standard. There are many block ciphers which follow the design of Substitution-Permutation-Network (SPN), for example, `AES` [7]. In this model, S-boxes are

W. Susilo and G. Yang (Eds.): ACISP 2018, LNCS 10946, pp. 207–224, 2018.
https://doi.org/10.1007/978-3-319-93638-3_13

used to achieve the confusion property, whereas in general MDS matrices are used as the diffusion layer of a block cipher. MDS matrices generate MDS codes which achieve the highest possible minimum distance, thus MDS matrices have the highest possible diffusion power. In the same note we find the design of PRESENT very interesting. It has removed the usual diffusion layer that is normally implemented by an MDS matrix. Thus saving a considerable amount of hardware cost. It uses a 4 × 4 S-box that has the following properties:

- differential branch number is 3,
- differential uniformity is 4 (the highest possible),
- nonlinearity is 4 (the highest possible),
- algebraic degree is 3.

One round function of PRESENT is comprised of 16 such S-boxes followed by a linear bit-wise permutation $L : \mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$. The role of this linear permutation is to mix up the outputs of the S-boxes which become the input to the next round. As bit-wise permutation can be implemented by wires only, so this reduces the number of gates required for the whole design. Recently a lightweight block cipher GIFT [2] has also appeared which relies on the same design principle as of PRESENT (Fig. 1).

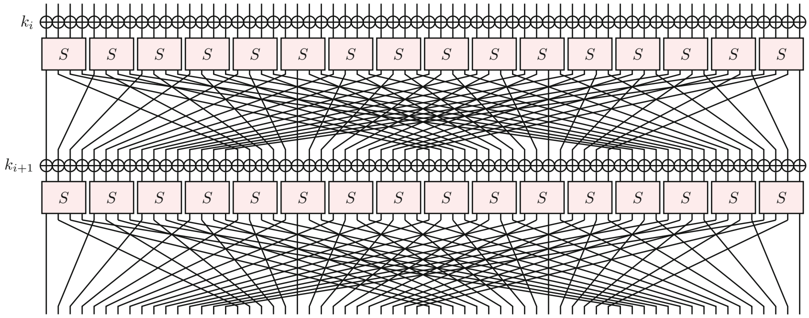

Fig. 1. Round function of PRESENT (image source: [9])

PRESENT (in 2007) used the diffusion property of an S-box. This construction idea will succeed provided the S-box has high differential branch number along with the other cryptographic properties. However after PRESENT, through the last 10 years, no attempt has been made to analyze how far an S-box can diffuse. We consider this problem and provide an upper bound for the differential branch number of permutations in general. To the best of our knowledge this is the first ever work which gives nontrivial bounds on diffusion power of S-boxes. On the other hand it is also crucial to have S-boxes with high linear branch number in order to resist the linear cryptanalysis. So we study the differential branch number of permutations in conjunction with the linear branch number. Below we summarize our contributions.

Our Contributions

In Sect. 4, we present bounds on the differential branch number of any permutation of $\mathbb{F}_2^n$. We completely characterize permutations of $\mathbb{F}_2^4$ in terms of the differential branch number. In [13] huge computational effort was made in order to characterize cryptographic properties of 4×4 S-boxes. In their search they considered 16 optimal 4×4 S-boxes from [10] and showed that the maximum possible differential branch number of such an S-box is 3. However, from this search it is not clear whether 3 is the maximum for all 4×4 S-boxes. In Theorem 4, we prove that if a permutation of $\mathbb{F}_2^4$ has differential branch number 4 then it is affine, which shows (Theorem 5) that in fact for any 4×4 S-box, the maximum possible differential branch number is 3. Further in Theorem 6, we prove that for any permutation over $\mathbb{F}_2^n$, for $n \geq 5$, its differential branch number is upper bounded by $\lceil 2\frac{n}{3} \rceil$. There is a bound known as Griesmer bound [8] which applies only to linear permutations, whereas our bound works on any permutation. We compare these two bounds in Table 3, and observe that values are very close to each other.

We also study bounds on the linear branch number of permutations of $\mathbb{F}_2^n$. It turns out that for a linear permutation of $\mathbb{F}_2^n$, the maximum value of the linear branch number matches with the maximum value of the differential branch number (see Theorem 1). For any permutation of $\mathbb{F}_2^n$, the linear branch number is upper bounded by n (see Theorem 3).

2 Preliminaries

Denote by $\mathbb{F}_2$ the finite field of two elements $\{0, 1\}$ and by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. For any $x \in \mathbb{F}_2^n$ the Hamming weight of x, denoted by $wt(x)$ is the number of 1's in x. Bitwise XOR is denoted by $\oplus$ and for any $x, y \in \mathbb{F}_2^n$ their dot product $x^t \cdot y$ is simply the usual inner product $x_0y_0 \oplus \cdots \oplus x_{n-1}y_{n-1}$.

We now bring in some notations which will be frequently used. For $i = 0, \ldots, n-1$ denote by e_i, the element of $\mathbb{F}_2^n$ which has 1 in the i-th position, and 0 elsewhere. Note that the set $\{e_0, \ldots, e_{n-1}\}$ forms a basis of $\mathbb{F}_2^n$. Further, the element of $\mathbb{F}_2^n$ with all 1 is denoted by $\bar{e}$. To illustrate let $n = 4$, then we have $e_0 = (1, 0, 0, 0),\ e_1 = (0, 1, 0, 0),\ e_2 = (0, 0, 1, 0),\ e_3 = (0, 0, 0, 1),$ and $\bar{e} = (1, 1, 1, 1)$.

An $n \times n$ S-box is a permutation $\mathrm{S} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ which is (strictly) nonlinear. We denote by $\mathbb{GL}(n, \mathbb{F}_2)$ (or simply by $\mathbb{GL}(n)$) the set of linear permutations of $\mathbb{F}_2^n$. Clearly $\mathbb{GL}(n)$ is a proper subset of set of all permutations of $\mathbb{F}_2^n$ and by definition an $n \times n$ S-box is a permutation of $\mathbb{F}_2^n$ which is not in $\mathbb{GL}(n)$. For a secure design, S-box needs to satisfy several properties such as high nonlinearity, high differential uniformity, high algebraic degree, etc. [5]. We now recall the notions of correlation matrices, linear and differential branch numbers. See [7] for detailed discussion on these.

Consider a permutation ϕ of $\mathbb{F}_2^n$.

For any $\alpha, \beta \in \mathbb{F}_2^n$ the correlation coefficient of ϕ with respect to (α, β) is given by

$$\mathtt{C}_\phi(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha^t \cdot x \oplus \beta^t \cdot \phi(x)} \tag{1}$$

It is easy to see that $-2^n \leq \mathtt{C}_\phi(\alpha, \beta) \leq 2^n$. See [7, Chap. 7] for detailed discussion on correlation matrices of Boolean functions and their properties. We define the correlation matrix $\mathtt{C}_\phi$ of ϕ as the $2^n \times 2^n$ matrix indexed by $\alpha, \beta \in \mathbb{F}_2^n$ in which the entry in the cell (α, β) is given by $\mathtt{C}_\phi(\alpha, \beta)$:

$$\mathtt{C}_\phi = [C_{\alpha,\beta}]_{2^n \times 2^n} \quad \text{where } C_{\alpha,\beta} = \mathtt{C}_\phi(\alpha, \beta) \tag{2}$$

Next we recall some definitions related to branch numbers of permutations.

Definition 1. *For any ϕ of $\mathbb{F}_2^n$, its differential branch number (respectively linear branch number) is denoted by $\beta_{\mathtt{d}}(\phi)$ (respectively $\beta_\ell(\phi)$) and defined as*

$$\beta_{\mathtt{d}}(\phi) := \min_{x, x' \in \mathbb{F}_2^n,\, x \neq x'} \{wt(x \oplus x') + wt(\phi(x) \oplus \phi(x'))\},$$

and

$$\beta_\ell(\phi) := \min_{\alpha, \beta \in \mathbb{F}_2^n,\, \mathtt{C}_\phi(\alpha,\beta) \neq 0} \{wt(\alpha) + wt(\beta)\}.$$

where $\mathtt{C}_\phi(\alpha, \beta)$ is the correlation coefficient as in (1).

If ϕ is a linear permutation of $\mathbb{F}_2^n$, then there exists a binary $n \times n$ invertible matrix M such that $\phi(x) = \mathrm{M}x$ for every $x \in \mathbb{F}_2^n$. In this case $\beta_{\mathtt{d}}(\phi)$ and $\beta_\ell(\phi)$ can be simplified as in the following lemma [7, Chap. 9].

Lemma 1. *Let ϕ be a linear permutation of $\mathbb{F}_2^n$ given by $\mathrm{M} \in \mathbb{GL}(n, \mathbb{F}_2)$. Then,*

$$\beta_{\mathtt{d}}(\phi) = \min_{\alpha \in \mathbb{F}_2^n, \alpha \neq 0} \{wt(\alpha) + wt(\mathrm{M}\alpha)\} \tag{3}$$

$$\beta_\ell(\phi) = \min_{\alpha \in \mathbb{F}_2^n, \alpha \neq 0} \{wt(\alpha) + wt(\mathrm{M}^t\alpha)\}. \tag{4}$$

For any $\phi \in \Pi(n)$ it is easy to see that $\beta_{\mathtt{d}}(\phi)$ is ≥ 2 and $\beta_\ell(\phi) \geq 2$. Also,

$$\beta_{\mathtt{d}}(\phi) = \beta_{\mathtt{d}}(\phi^{-1}) \qquad \text{and} \qquad \beta_\ell(\phi) = \beta_\ell(\phi^{-1}).$$

It is interesting to note that the differential branch number is related to the difference distribution table (DDT). DDT of a permutation ϕ of $\mathbb{F}_2^n$ denoted by $\mathcal{D}_\phi$ is a matrix of order $2^n \times 2^n$. Suppose for the input difference δ, the output difference of the permutation ϕ is Δ, i.e., $\phi(x) \oplus \phi(x \oplus \delta) = \Delta$. Let $\mathcal{D}_\phi(\delta, \Delta)$ be the number solutions of $\phi(x) \oplus \phi(x \oplus \delta) = \Delta$, then the (δ, Δ)-th element of DDT is $\mathcal{D}_\phi(\delta, \Delta)$. In Table 1, we present the difference distribution table of the S-box $\phi = 408235\text{B}719\text{A}6\text{CDEF}$.

Then the differential branch number can be redefined as

$$\beta_{\mathtt{d}}(\phi) := \min_{\delta \neq 0, \Delta \neq 0, \mathcal{D}_\phi(\delta, \Delta) \neq 0} \{wt(\delta) + wt(\Delta)\}.$$

Table 1. DDT of S-Box 408235B719A6CDEF

δ	Δ															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	0	0	2	0	2	0	2	0	2	0	4	0	0	0
2	0	0	8	0	0	0	0	0	2	0	0	2	2	0	0	2
3	0	0	0	6	2	0	2	2	2	0	0	0	0	0	2	0
4	0	0	0	2	4	4	0	2	0	2	0	0	0	2	0	0
5	0	2	0	2	0	4	0	0	2	2	0	0	2	0	0	2
6	0	0	0	0	0	0	4	4	0	0	0	4	0	0	0	4
7	0	2	0	2	0	0	0	4	0	0	2	2	0	2	2	0
8	0	0	2	0	2	4	0	0	4	2	0	0	0	0	0	2
9	0	2	0	0	2	0	0	0	2	4	0	0	0	2	4	0
A	0	0	0	0	0	0	2	2	0	2	4	2	0	2	2	0
B	0	2	2	2	0	0	2	0	0	0	2	4	2	0	0	0
C	0	4	2	0	0	0	2	0	2	0	0	0	2	4	0	0
D	0	0	0	0	2	0	0	2	0	2	2	0	4	4	0	0
E	0	0	0	2	2	0	0	0	0	2	4	0	0	0	2	4
F	0	0	2	0	0	4	2	0	0	0	0	2	0	0	4	2

For example, it is clear from the DDT of the differential branch number of 408235B719A6CDEF is 2.

One of the basic notion in the study of permutations is that of *affine equivalence*. This equivalence preserves various cryptographic properties like nonlinearity, differential uniformity, algebraic degree (more than one), etc.

Definition 2 (Affine Equivalence). *Let ϕ, ϕ' be two permutations of $\mathbb{F}_2^n$. We say that ϕ is affine equivalent to ϕ' if there exist A, $B \in \mathbb{GL}(n, \mathbb{F}_2)$, and $c, d \in \mathbb{F}_2^n$ such that*

$$\phi'(x) = B \cdot \phi[A\,x \oplus c] \oplus d, \qquad \textit{for all } x \in \mathbb{F}_2^n. \tag{5}$$

Affine equivalence preserves many properties of S-boxes, such as uniformity, nonlinearity, degree, but it does not preserve branch number in general. For instance, the following two affine equivalent S-boxes (in Table 2) have different differential branch number. Here S and S′ are related as $\mathrm{S}'(x) = B\,\mathrm{S}(x)$, where B is a matrix with the rows $\{(1,0,0,1),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$. Note that $\beta_{\mathtt{d}}(\mathrm{S}) = 3$, whereas $\beta_{\mathtt{d}}(\mathrm{S}') = 2$, although they are affine equivalent. The S-box S is used in PRESENT.

On the other hand, if A and B are permutation matrices[1] then the corresponding affine equivalence class preserves the branch number [13]. We state this as the following lemma.

[1] A matrix obtained by permuting rows (or columns) of an identity matrix.

Table 2. Affine equivalent S-boxes with different differential branch numbers.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
S′(x)	C	D	6	3	1	0	A	5	B	E	7	8	4	F	9	2

Lemma 2. *If ϕ and ϕ_1 are two affine equivalent permutations of $\mathbb{F}_2^n$ such that $\phi_1(x) = B\,\phi[A\,x \oplus c] \oplus d$, for all $x \in \mathbb{F}_2^n$, where A and B are $n \times n$ permutation matrix, and $c, d \in \mathbb{F}_2^n$, then $\beta_{\mathsf{d}}(\phi) = \beta_{\mathsf{d}}(\phi_1)$ and $\beta_{\ell}(\phi) = \beta_{\ell}(\phi_1)$.*

3 Bounds on Linear Branch Number

First we consider the case of linear permutations of $\mathbb{F}_2^n$. In this case we have the following connection between the linear and the differential branch numbers of such permutations.

Theorem 1. *For linear permutations of $\mathbb{F}_2^n$ the maximum differential branch number is equal to the maximum linear branch number.*

Proof. Suppose ϕ be a linear permutation of $\mathbb{F}_2^n$, then there exists a matrix $\mathrm{M} \in \mathbb{GL}(n, \mathbb{F}_2)$ such that $\phi(x) = \mathrm{M}x$ for every $x \in \mathbb{F}_2^n$. Consider the permutation ϕ^t defined as $\phi^t(x) = \mathrm{M}^t x$ for $x \in \mathbb{F}_2^n$. Using Lemma 1 we see that $\beta_{\mathsf{d}}(\phi) = \beta_{\ell}(\phi^t)$ from which the result follows. □

Remark 1. The best known bound for the differential branch number of a linear permutation is Griesmer bound (see Sect. 4). Above theorem suggests that this is also the best bound for the linear branch number of such permutations. Later in Theorem 6 we present new a bound on the differential branch number of more general permutations of $\mathbb{F}_2^n$ which is quite comparable to Griesmer bound in case linear permutations.

It is pertinent to mention here some results similar to Theorem 1 in case of permutations of $\mathbb{F}_q^n$ when $q = 2^m$ for $m > 1$. These results along with proofs can be found in [7]. We present some of them here for sake of completeness. In [7] authors consider a permutation of $\mathbb{F}_q^n$ as a "bundled" permutation of $\mathbb{F}_2^{mn}$ with bundle size m, i.e., if ψ is such permutation then it is defined as

$$\psi(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1}) \tag{6}$$

where $(x_0, \ldots, x_{n-1}), (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{2^m}^n$. The notion of branch numbers (linear and differential) are defined with respect to the bundle size. With these authors prove the following theorem [7, Theorem B.1.2].

Theorem 2. *Let $\psi : \mathbb{F}_2^{mn} \longrightarrow \mathbb{F}_2^{mn}$ be a bundled permutation as in (6). Then ψ has maximal differential branch number if and only if it has maximal linear branch number.*

If ψ is a linear permutation of $\mathbb{F}_q^n$ given by $n \times n$ nonsingular matrix N over $\mathbb{F}_q$, i.e., $\psi(x) = Nx$, then Theorem 2 simply means that the matrix N is MDS if and only if its transpose is also MDS. Note that Theorem 2 goes beyond linear permutations and includes all permutation of $\mathbb{F}_q^n$. However, an important point to be noted here is that Theorem 2 is applicable for bundled permutations of $\mathbb{F}_2^{mn}$ of bundle size $m > 1$ and is not applicable to our results which involve permutations of $\mathbb{F}_2^n$. In the following we will see that such a nice connection is elusive in case of permutations of $\mathbb{F}_2^n$. To continue our results from Theorem 1 we now prove a bound on the linear branch number of general permutations.

To present our results we need some facts related to Boolean functions which we recall here. A n variable Boolean function is map $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. We say that φ is balanced if

$$\#\{x \in \mathbb{F}_2^n : \varphi(x) = 0\} = \#\{x \in \mathbb{F}_2^n : \varphi(x) = 1\} = 2^{n-1}.$$

The map φ is said to be r^{th} order Correlation Immune (r-CI) if

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha^t \cdot x \oplus \varphi(x)} = 0, \tag{7}$$

for all $\alpha \in \mathbb{F}_2^n$ such that $1 \leq wt(\alpha) \leq r$. If φ is balanced and r-CI then it said to be $r-$resilient Boolean function. In our study Boolean functions occur as coordinate functions of a permutation ϕ of $\mathbb{F}_2^n$. The linear branch number of ϕ and the resiliency order of its coordinate functions is interconnected as follows. Suppose that ϕ is a permutation of $\mathbb{F}_2^n$ given by $\phi(x) = (\phi_0(x), \ldots, \phi_{n-1}(x))$ where $x \in \mathbb{F}_2^n$ and each of $\phi_0, \ldots, \phi_{n-1}$ is a coordinate Boolean function. If $\beta_\ell(\phi) = r$ then, by definition for any $\alpha, \beta \in \mathbb{F}_2^n$

$$\mathtt{C}_\phi(\alpha, \beta) = 0 \quad \text{whenever} \quad 2 \leq wt(\alpha) + wt(\beta) \leq r - 1.$$

In particular if we choose $\beta = e_i \in \mathcal{B}_n$, then the above equation implies that

$$\mathtt{C}_\phi(\alpha, e_i) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha^t \cdot x \oplus \phi_i(x)} = 0 \quad \text{whenever} \quad 1 \leq wt(\alpha) \leq r - 2, \tag{8}$$

which means that ϕ_i is $(r-2)-$ CI Boolean function. Also, ϕ_i is balanced since it is a coordinate function of a permutation. Thus we see that each ϕ_i is a $r-2$ resilient Boolean function. In a nutshell this is our observation:

Lemma 3. *Let $\phi = (\phi_0, \ldots, \phi_{n-1})$ be a permutation of $\mathbb{F}_2^n$. For every $0 \leq i \leq n-1$ the coordinate function ϕ_i is $\beta_\ell(\phi) - 2$ resilient Boolean function.*

We also recall the notion of degree of a Boolean function. Given a Boolean function φ of n variables there exist a unique polynomial $P(X_0, \ldots, X_{n-1})$ in n variables over $\mathbb{F}_2$ such that $\varphi(x_0, \ldots, x_{n-1}) = P(x_0, \ldots, x_{n-1})$ for every $(x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$. Such a polynomial is called *Algebraic Normal Form* of φ and the total degree of P is called algebraic degree (or simply degree) of φ. Note that $\deg(\varphi) = 0$ only for constant functions and $\deg(\varphi) = 1$ if φ is affine. For any Boolean function φ its resiliency order and its degree are connected as follows, which is known as Siegenthaler bound [16]. If φ is a n variable $r-$resilient Boolean function then

$$\deg(\varphi) \leq n - 1 - r. \tag{9}$$

Using the connection in Lemma 3 and (9) we obtain bounds on the linear branch number of permutations of $\mathbb{F}_2^n$.

Theorem 3. *For any nonlinear permutation ϕ of $\mathbb{F}_2^n$ we have $\beta_\ell(\phi) \leq n - 1$.*

Proof. First we show that $\beta_\ell(\phi) \leq n$ and then that only linear permutations have $\beta_\ell(\phi) = n$. Let $\phi = (\phi_0, \ldots, \phi_{n-1})$ be a permutation of $\mathbb{F}_2^n$ with coordinate Boolean functions $\{\phi_0, \ldots, \phi_{n-1}\}$. Suppose $\phi_i \in \{\phi_0, \ldots, \phi_{n-1}\}$ be any coordinate function. If $\beta_\ell(\phi) \geq n+1$ then from Lemma 3 it follows that the function ϕ_i is $r-$ resilient where $r \geq (n+1) - 2 = n-1$. By Siegenthaler bound (9) we must have $\deg(\phi_i) \leq (n-1) - (n-1) = 0$. On the other hand, if $\deg(\phi_i) = 0$ then ϕ_i is a constant function which is impossible because ϕ_i a coordinate function of a permutation of $\mathbb{F}_2^n$ and hence need to be balanced. This contradiction shows that $\beta_\ell(\phi) \leq n$. Using same kind of argument one can easily see that if $\beta_\ell(\phi) = n$ then $\deg(\phi_i) \leq 1$ for every $0 \leq i \leq n-1$, which implies that it is affine and hence ϕ itself is affine. As a consequence it follows that if ϕ is a nonlinear permutation of $\mathbb{F}_2^n$ then $\beta_\ell(\phi) \leq n - 1$. □

Next we focus on bounds for the differential branch number of general permutations of $\mathbb{F}_2^n$.

4 Bounds on Differential Branch Number

It is trivial to check that for any permutation ϕ of $\mathbb{F}_2^n$, we have $\beta_{\mathtt{d}}(\phi) \geq 2$. For linear permutations, some upper bound can be easily obtained from coding theory. If $L : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is linear permutation, then the set $\mathcal{C} = \{(x, L(x)) : x \in \mathbb{F}_2^n\}$ forms a $[2n, n]$ linear code, and its minimum distance is actually the differential branch number of L. An $[N, K]$ linear code has minimum distance $d \leq N - K + 1$ (Singleton Bound). The codes which achieve the Singleton Bound are called MDS codes. Therefore, the differential branch number of L is bounded by $n + 1$. However, it is known that there is no nontrivial binary MDS code [11], which means that there is no linear permutation defined over $\mathbb{F}_2^n$ having the differential branch number $n + 1$. Thanks to Griesmer bound we can have further bounds [8].

Lemma 4 (Griesmer Bound). *Let $[N, K]$ be a binary linear code with the minimum distance d then*

$$N \geq \sum_{i=0}^{K-1} \left\lceil \frac{d}{2^i} \right\rceil .$$

In this section we present a bound on the differential branch number of an arbitrary permutation of $\mathbb{F}_2^n$. We begin with following remark which will be useful in our proofs.

Remark 2. Let ϕ be a permutation of $\mathbb{F}_2^n$ such that $\phi(0) = c$ for some $c \neq 0 \in \mathbb{F}_2^n$. Then for the permutation ϕ' defined as $\phi'(x) = \phi(x) \oplus c$ it is easy to see that $\beta_{\mathtt{d}}(\phi) = \beta_{\mathtt{d}}(\phi')$ and $\phi'(0) = 0$. Thus while deriving bounds on the differential branch numbers we can simply consider permutations ϕ such that $\phi(0) = 0$.

Suppose q is a power of prime, and $L : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ is a linear permutation. It is a well known fact [11] that $\beta_{\mathtt{d}}(L) \leq n + 1$ whenever $q \neq 2$.

Next, let ϕ be a arbitrary permutation of $\mathbb{F}_2^n$. If $\beta_{\mathtt{d}}(\phi) = n + 1$ then by Definition 1 and Remark 2 we get

$$wt(e_i \oplus 0) + wt(\phi(e_i) \oplus \phi(0)) = wt(e_i) + wt(\phi(e_i)) \geq n + 1,$$

which implies that $wt(\phi(e_i)) \geq n$ for $i = 0, \ldots n - 1$. However, this is impossible because there is precisely one element $\bar{e} \in \mathbb{F}_2^n$ with $wt(\bar{e}\,) = n$. Hence we must have $\beta_{\mathtt{d}}(\phi) < n + 1$. This gives us a trivial bound on the differential branch number of permutations of $\mathbb{F}_2^n$ as follows.

Lemma 5. *For any permutation ϕ of $\mathbb{F}_2^n$ we have $\beta_{\mathtt{d}}(\phi) < n + 1$.*

In the remaining part of this section we sharpen the bound in Lemma 5. To make proofs easy we consider the case of permutations over $\mathbb{F}_2^4$ and the case of permutations over $\mathbb{F}_2^n, n \geq 5$ separately.

4.1 Differential Branch Number of Permutations of $\mathbb{F}_2^4$

In this section we consider permutations defined on $\mathbb{F}_2^4$ which are used to design 4 × 4 S-boxes. Here we show that if the differential branch number of a permutation of $\mathbb{F}_2^4$ is 4 then it is necessarily affine and hence the differential branch number of any 4 × 4 S-box is bounded above by 3.

Lemma 6. *Suppose $\phi : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ is a permutation with $\phi(0) = 0$ and $\beta_{\mathtt{d}}(\phi) = 4$. Then the following conditions hold for $x \in \mathbb{F}_2^4$*

C1. *if $wt(x) = 4$ then $wt\,(\phi(x)) = 4$,*
C2. *if $wt(x) = 1$ then $wt\,(\phi(x)) = 3$,*
C3. *if $wt(x) = 2$ then $wt\,(\phi(x)) = 2$,*
C4. *if $wt(x) = 3$ then $wt\,(\phi(x)) = 1$.*

Proof. Since $\beta_{\mathtt{d}}(\phi) = 4$, and $\phi(0) = 0$, any nonzero $x \in \mathbb{F}_2^4$ must satisfy

$$wt(x) + wt(\phi(x)) \geq 4. \tag{10}$$

Immediate consequence of this is that $wt(\phi(e_i)) = 3$ or $wt(\phi(e_i)) = 4$ as $wt(e_i) = 1$ for any $0 \leq i \leq 3$. Suppose $wt(\phi(e_i)) = 4$ for some i, then for any $j \neq i$ we have

$$wt(e_i \oplus e_j) + wt(\phi(e_i) \oplus \phi(e_j)) = 3 < 4,$$

contradicting (10). Hence C2 follows.

Next let $x \in \mathbb{F}_2^4$ with $wt(x) = 2$. Then, $2 \leq wt(\phi(x)) \leq 4$ by (10). Since ϕ maps all weight 1 elements to weight 3 elements and ϕ is a permutation, so $wt(\phi(x)) \neq 3$. Suppose that $wt(\phi(x)) = 4$. Choose e_i such that $wt(e_i \oplus x) = 1$, and since $wt(\phi(e_i)) = 3$ we must have

$$wt(e_i \oplus x) + wt(\phi(e_i) \oplus \phi(x)) = 1 + 1 = 2 < 4,$$

again contradicting (10); hence it follows that $wt(\phi(x)) = 2$. This concludes the proof of C3.

Now let's prove C4. Consider x with $wt(x) = 3$. By C2 and C3, we have $wt(S(x)) \neq 2, 3$. This leaves open the possibility that $wt(\phi(x)) = 1$ or 4. If $wt(\phi(x)) = 4$, consider an element x' with $wt(x') = 2$ and $wt(x \oplus x') = 1$. Then

$$wt(x \oplus x') + wt(\phi(x) \oplus \phi(x')) = 1 + 2 < 4,$$

a contradiction. So $wt(\phi(x)) = 1$.

Finally, C2, C3, C4 imply that $wt(\phi(x)) = 4$, when $wt(x) = 4$. □

Above theorem leads to the following characterization of permutations ϕ of $\mathbb{F}_2^4$ for which $\beta_{\mathtt{d}}(\phi) = 4$.

Theorem 4. *Let $\phi : \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$ be a permutation with $\beta_{\mathtt{d}}(\phi) = 4$. Then ϕ is affine.*

Proof. As per Remark 2 we prove the result for $\phi(0) = 0$. Since $\beta_{\mathtt{d}}(\phi) = 4$ and $\phi(0) = 0$, ϕ satisfies C1, C2, C3, C4 (of Lemma 6). Note that the set of 1-weight vectors $\{e_0, e_1, e_2, e_3\}$ form a basis of $\mathbb{F}_2^4$ and by C2 the corresponding image set $\{\phi(e_0), \phi(e_1), \phi(e_2), \phi(e_3)\}$ contains all the 3-weight vectors of $\mathbb{F}_2^4$. Note that $\{\phi(e_0), \phi(e_1), \phi(e_2), \phi(e_3)\}$ also forms a basis of $\mathbb{F}_2^4$. Recall that the permutation ϕ is a linear map iff

$$\phi(c_0e_0 \oplus c_1e_1 \oplus c_2e_2 \oplus c_3e_3) = c_0\phi(e_0) \oplus c_1\phi(e_1) \oplus c_2\phi(e_2) \oplus c_3\phi(e_3)$$

holds for all $(c_0, c_1, c_2, c_3) \in \mathbb{F}_2^4$.

As $wt(\phi(e_0 \oplus e_1 \oplus e_2 \oplus e_3)) = 4$ (by C1 of Lemma 6), and $wt(\phi(e_0) \oplus \phi(e_1) \oplus \phi(e_2) \oplus \phi(e_3)) = 4$, then

$$\phi(e_0 \oplus e_1 \oplus e_2 \oplus e_3) = \phi(e_0) \oplus \phi(e_1) \oplus \phi(e_2) \oplus \phi(e_3).$$

In the following we will use the fact that $\phi(e_i) \oplus \phi(e_j)$ has weight 2, and $\phi(e_i) \oplus \phi(e_j) \oplus \phi(e_k)$ has weight 1. The set $\{\phi(e_0), \phi(e_1), \phi(e_2), \phi(e_3)\}$ forms a basis and $wt(\phi(e_i \oplus e_j)) = 2$ (by C3 of Lemma 6), then $\phi(e_i \oplus e_j)$ can be written as

$$\phi(e_i \oplus e_j) = \phi(e_\ell) \oplus \phi(e_r),$$

for some ℓ and r. If linearity does not hold for $(e_i \oplus e_j)$ then $(i, j) \neq (\ell, r)$.

If $i = \ell$ (and $j \neq r$), then

$$\begin{aligned} wt(e_j \oplus e_i \oplus e_j) + wt(\phi(e_j) \oplus \phi(e_i \oplus e_j)) &= wt(e_i) + wt(\phi(e_j) \oplus \phi(e_i) \oplus \phi(e_r)) \\ &= 1 + 1 < 4, \end{aligned}$$

a contradiction. The case $j = r$ can be treated similarly.

Next if $\ell, r \notin \{i, j\}$, then

$$\begin{aligned} wt(e_j \oplus e_i \oplus e_j) + wt(\phi(e_j) \oplus \phi(e_i \oplus e_j)) &= wt(e_i) + wt(\phi(e_j) \oplus \phi(e_\ell) \oplus \phi(e_r)) \\ &= 1 + 1 < 4, \end{aligned}$$

which contradicts the fact that $\beta_{\mathtt{d}}(\phi) = 4$. Therefore, for any linear combinations of the form $e_i \oplus e_j$ we must have

$$\phi(e_i \oplus e_j) = \phi(e_i) \oplus \phi(e_j).$$

We now consider linear combinations of the form $e_i \oplus e_j \oplus e_k$. By C4 of Lemma 6, we have $wt(\phi(e_i \oplus e_j \oplus e_k)) = 1$. As $\{\phi(e_0), \phi(e_1), \phi(e_2), \phi(e_3)\}$ forms a basis, so we can write

$$\phi(e_i \oplus e_j \oplus e_k) = \phi(e_\ell) \oplus \phi(e_r) \oplus \phi(e_t).$$

Suppose that linearity does not hold for $e_i \oplus e_j \oplus e_k$, then $(i, j, k) \neq (\ell, r, t)$. Note that we must have $|\{i, j, k\} \cap \{\ell, r, t\}| = 2$. Assume that $i = \ell$ and $j = r$. Then

$$\begin{aligned} &wt(e_i \oplus e_k \oplus e_i \oplus e_j \oplus e_k) + wt(\phi(e_i \oplus e_k) \oplus \phi(e_i \oplus e_j \oplus e_k)) \\ &= wt(e_j) + wt(\phi(e_i) \oplus \phi(e_k) \oplus \phi(e_i) \oplus \phi(e_j) \oplus \phi(e_t)) \\ &= wt(e_j) + wt(\phi(e_k) \oplus \phi(e_j) \oplus \phi(e_t)) \\ &= 1 + 1 < 4, \end{aligned}$$

a contradiction. Therefore, for any linear combinations of the form $e_i \oplus e_j \oplus e_k$ we must have

$$\phi(e_i \oplus e_j \oplus e_k) = \phi(e_i) \oplus \phi(e_j) \oplus \phi(e_k).$$

Thus we conclude that ϕ is linear, and the theorem follows. □

Recall that, by definition an $n \times n$ S-box is a strictly nonlinear permutation of $\mathbb{F}_2^n$. Using Lemma 5 and Theorem 4 we get the following strict upper bound on the differential branch number of 4×4 S-boxes.

Theorem 5. *The maximum possible differential branch number of a* 4×4 *S-box is* 3*.*

The paper [13] followed the work of [10] to search for optimal 4×4 S-boxes in the affine equivalent classes. The maximum differential branch number in the affine equivalent classes of the 16 optimal 4×4 S-boxes from [10] is 3. As this search did not consider the so-called non-optimal S-boxes, the question of the maximal differential branch number of any 4×4 S-box remained unanswered. Theorem 5 settles this question.

We now give a family of linear permutations $\mathtt{LS}_n$ of $\mathbb{F}_2^n$ with $\beta_{\mathtt{d}}(\mathtt{LS}_n) = 4$. Definition of these permutations varies slightly depending on whether n is even or odd. Since these permutations are linear we specify their action on basis $\mathcal{B}_n = \{e_0, \ldots, e_{n-1}\}$ of $\mathbb{F}_2^n$ and the maps extend linearly to other elements of $\mathbb{F}_2^n$.

Example 1. Let n be an even integer. The linear permutation $\mathtt{LS}_n$ of $\mathbb{F}_2^n$, defined on the basis $\mathcal{B}_n$ as

$$\mathtt{LS}_n(e_i) = \bar{e} \oplus e_i \tag{11}$$

has $\beta_{\mathtt{d}}(\mathtt{LS}_n) = 4$ and it is also involution. Further, observe that matrix representing the map $\mathtt{LS}_n$ is symmetric from which it follows that $\beta_{\ell}(\mathtt{LS}_n) = 4$.

Next we give a family of linear permutations with the differential branch number 4 defined over $\mathbb{F}_2^n$ for odd values of n

Example 2. Let n be an odd integer. The linear permutation $\mathtt{LS}_n$ of $\mathbb{F}_2^n$, defined on basis $\mathcal{B}_n$ as

$$\mathtt{LS}_n(e_i) = \begin{cases} \bar{e} \oplus e_i \oplus e_{i+1} & \text{if} \quad 0 \le i \le n-2 \\ \\ \bar{e} \oplus e_{n-1} \oplus e_0 & \text{if} \quad i = n-1 \end{cases}$$

has the differential branch number 4.

In both cases it is easy to show that the set $\{\mathtt{LS}_n(e_0), \ldots, \mathtt{LS}_n(e_{n-1})\}$ is a basis of $\mathbb{F}_2^n$ asserting that the maps $\mathtt{LS}_n$ indeed are bijections. The fact that $\beta_{\mathtt{d}}(\mathtt{LS}_n) = 4$ can also be easily checked from the Definition 1 of the differential branch number for linear maps. Next we present bounds for permutations of $\mathbb{F}_2^n$, for $n \ge 5$.

4.2 Differential Branch Number of Permutations of $\mathbb{F}_2^n$, for $n \ge 5$

In this section we present bounds on the differential branch number of a general permutation of $\mathbb{F}_2^n$. In the remainder of this paper we assume that $n \ge 5$ unless specified otherwise. We begin with some initial observations.

Suppose that $x \in \mathbb{F}_2^n$ with $wt(x) = n - \delta$ for some $\delta \ge 1$. Then x can be expressed as $x = \bar{e} \oplus e_{x_1} \oplus \ldots \oplus e_{x_\delta}$ for unique set of elements $e_{x_1}, \ldots e_{x_\delta} \in \mathcal{B}_n$. Using this one can easily see the following fact which we will be using frequently in this paper:

Fact 1 *For x, $x' \in \mathbb{F}_2^m$ with $x \neq x'$, $wt(x) \ge n - \delta$ and $wt(x') \ge n - \delta'$ we have*

$$wt(x \oplus x') \le \delta + \delta'.$$

Lemma 7. *Let ϕ be a permutation of $\mathbb{F}_2^n$ with $\phi(0) = 0$ and the differential branch number $\beta_{\mathtt{d}}(\phi) = n - \beta + 1$ for some $1 \le \beta \le n - 1$. Then we have for $0 \le i \le n - 1$*

$$n - \beta \le wt(\phi(e_i)) \le 2\,\beta + 1 \tag{12}$$

and for $0 \le i \neq j \le n - 1$,

$$n - (\beta + 1) \le wt(\phi(e_i) \oplus \phi(e_j)) \le 2\,\beta. \tag{13}$$

Proof. From the definition of the differential branch number it follows that

$$wt(\phi(e_i)) \geq n - \beta, \tag{14}$$

as $\phi(0) = 0$. Then using $x = \phi(e_i), x' = \phi(e_j)$ in Fact 1 we get

$$wt(\phi(e_i) \oplus \phi(e_j)) \leq 2\beta. \tag{15}$$

Again for every pair of indices $i \neq j$

$$wt(\phi(e_i) \oplus \phi(e_j)) \geq n - (\beta + 1). \tag{16}$$

Using (14) and (16) in Fact 1 we get (12). Further combining (15) and (16) we get (13). □

Lemma 8. *Let δ be an integer such that $1 \leq \delta \leq n$. Denote by $\mathcal{W}^n_\delta$ the following set*

$$\mathcal{W}^n_\delta = \{x \in \mathbb{F}^n_2 : wt(x) = n - \delta\}. \tag{17}$$

Then for any $x, x' \in \mathcal{W}^n_\delta$ we have $wt(x \oplus x') = 2k$ for some $1 \leq k \leq \delta$. Further suppose $\mathcal{V} \subseteq \mathcal{W}^n_\delta$ defined as

$$\mathcal{V} = \{x \in \mathcal{W}^n_\delta : wt(x \oplus x') = 2\delta \text{ for all } x' \in \mathcal{V}\}$$

then $|\mathcal{V}| \leq \left\lfloor \frac{n}{\delta} \right\rfloor$.

Proof. First claim is obvious. To see second part, first observe that given any $x \in \mathcal{W}^n_\delta$ there exist a unique set of elements $\{e_{x_1} \ldots, e_{x_\delta}\} \subseteq \mathcal{B}_n$ such that $x = \bar{e} \oplus e_{x_1} \oplus \cdots \oplus e_{x_\delta}$.

An element $y \in \mathcal{W}^n_\delta$ is in $\mathcal{V}$ if and only if

$$\{e_{y_1} \ldots, e_{y_\delta}\} \cap \{e_{x_1} \ldots, e_{x_\delta}\} = \emptyset$$

for every element x already in $\mathcal{V}$. Consequently, we have $|\mathcal{V}| \leq \left\lfloor \frac{n}{\delta} \right\rfloor$ as required. □

Using the above observations we prove the following bound on the differential branch number of a permutation of $\mathbb{F}^n_2$.

Theorem 6. *If $n \geq 5$ then for any permutation ϕ of $\mathbb{F}^n_2$ we have*

$$\beta_{\mathtt{d}}(\phi) \leq \left\lceil 2\,\frac{n}{3} \right\rceil. \tag{18}$$

Proof. First it is easy to see that

$$\left\lceil 2\,\frac{n}{3} \right\rceil = n - \left\lfloor \frac{n}{3} \right\rfloor,$$

and hence we substitute the bound in (18) by $n - \left\lfloor \frac{n}{3} \right\rfloor$ to make the proof easy.

On the contrary to (18) assume that $\beta_{\mathsf{d}}(\phi) \geq n - \lfloor \frac{n}{3} \rfloor + 1$. Using $\beta = \lfloor \frac{n}{3} \rfloor$ in Lemma 7 we get

$$n - \left\lfloor \frac{n}{3} \right\rfloor \ \leq \ wt(\phi(e_i)) \ \leq 2 \ \left\lfloor \frac{n}{3} \right\rfloor + 1 \tag{19}$$

for $0 \leq i \leq n-1$, and

$$n - (\left\lfloor \frac{n}{3} \right\rfloor + 1) \ \leq \ wt(\phi(e_i) \oplus \phi(e_j)) \ \leq \ 2 \ \left\lfloor \frac{n}{3} \right\rfloor \tag{20}$$

for $0 \leq i \neq j \leq n-1$. Now, recall that the integer n can be written as

$$n = 3 \ \left\lfloor \frac{n}{3} \right\rfloor + r \tag{21}$$

for a unique r such that $0 \leq r \leq 2$. We prove our claim separately for each value of r.

Case 1. $r = 2$**.** From (19) we have

$$n - \left\lfloor \frac{n}{3} \right\rfloor \ \leq \ 2 \ \left\lfloor \frac{n}{3} \right\rfloor + 1$$

and substituting $n = 3 \ \lfloor \frac{n}{3} \rfloor + 2$ in this we get $2 \leq 1$ which is a contradiction.

Case 2. $r = 1$**.** In this case, by substituting $n = 3 \ \lfloor \frac{n}{3} \rfloor + 1$ the inequalities (19) and (20) become the following equalities

$$\begin{aligned} wt(\phi(e_i)) &= n - \left\lfloor \frac{n}{3} \right\rfloor \\ wt(\phi(e_i) \oplus \phi(e_j)) &= 2 \ \left\lfloor \frac{n}{3} \right\rfloor \end{aligned} \tag{22}$$

Note that both identities in (22) must be satisfied by all the elements of the set $\{\phi(e_0), \ldots, \phi(e_{n-1})\}$. We show that this is impossible. Since $wt(\phi(e_i)) = n - \lfloor \frac{n}{3} \rfloor$ for all $0 \leq i \leq n-1$, we are in the situation of Lemma 8 with $\phi(e_i) \in \mathcal{W}^n_\delta$ where $\delta = \lfloor \frac{n}{3} \rfloor$. Consequently, we see that there can be at most $\lfloor \frac{n}{\lfloor \frac{n}{3} \rfloor} \rfloor = 3$ elements $\phi(e_r), \phi(e_s), \phi(e_t)$ for which the latter identity in (22) can hold. On the other hand, since $n \geq 5$, there exists at least two basis elements e_u and e_v apart from e_r, e_s, e_t, and by Lemma 8 we will have

$$wt(\phi(e_u) \oplus \phi(e_v)) \leq 2\,(\delta - 1) < 2 \ \left\lfloor \frac{n}{3} \right\rfloor$$

which contradicts (22).

Case 3. $r = 0$. In this case we have $n = 3 \ \lfloor \frac{n}{3} \rfloor$ and the inequalities (19), (20) simplify to

$$wt(\phi(e_i)) \ = n - \left\lfloor \frac{n}{3} \right\rfloor \ \text{ or } n - \left\lfloor \frac{n}{3} \right\rfloor + 1 \tag{23}$$

$$wt(\phi(e_i) \oplus \phi(e_j)) = n - \left\lfloor \frac{n}{3} \right\rfloor - 1 \text{ or } n - \left\lfloor \frac{n}{3} \right\rfloor \tag{24}$$

Note that for every element of $\{\phi(e_0), \ldots, \phi(e_{n-1})\}$ there are only two possibilities for $wt(\phi(e_i))$ as in (23). First we show that $wt(\phi(e_i)) = wt(\phi(e_j)) = n - \lfloor \frac{n}{3} \rfloor + 1$ cannot hold, for $i \neq j$, otherwise using $x = \phi(e_i), x' = \phi(e_j)$ and $\delta = \delta' = \lfloor \frac{n}{3} \rfloor - 1$ in Fact 1 we get

$$wt(\phi(e_i) \oplus \phi(e_j)) \leq 2(\left\lfloor \frac{n}{3} \right\rfloor - 1) = n - \left\lfloor \frac{n}{3} \right\rfloor - 2 < n - \left\lfloor \frac{n}{3} \right\rfloor - 1$$

contradicting (24). Thus there can be at most one element $\phi(e_i)$ such that $wt(\phi(e_i) = n - \lfloor \frac{n}{3} \rfloor + 1$. Without loss of generality assume that $wt(\phi(e_0)) = n - \lfloor \frac{n}{3} \rfloor + 1$, then it follows from (23) that for $i = 1, \ldots, n-1$ the weights of $wt(\phi((e_i))$ satisfy

$$wt(\phi(e_i)) = n - \left\lfloor \frac{n}{3} \right\rfloor . \tag{25}$$

Thus, we are in situation of Lemma 8 with $\phi(e_1), \ldots, \phi(e_{n-1}) \in \mathcal{W}_\delta^n$ for $\delta = \lfloor \frac{n}{3} \rfloor$. Hence there can be only three elements $\phi(e_r), \phi(e_s), \phi(e_t),\ 1 \leq r \neq s \neq t \leq n-1$ such that for any two indices $i, j \in \{r, s, t\}$

$$wt(\phi(e_i) \oplus \phi(e_j)) \ = \ 2\,\delta \ = \ 2 \left\lfloor \frac{n}{3} \right\rfloor$$

holds. Since $n \geq 5$ there exist at least one element e_k, where $k \neq 0$ and also $k \notin \{r, s, t\}$. Then for any $i \in \{r, s, t\}$ we must have (by Lemma 8) $wt(\phi(e_k) \oplus \phi(e_i)) \ \leq 2(\delta - 1)$, which means that

$$wt(\phi(e_k) \oplus \phi(e_i)) \ \leq \ 2 \ \left\lfloor \frac{n}{3} \right\rfloor - 2 \ < \ n - \left\lfloor \frac{n}{3} \right\rfloor - 1,$$

contradicting (24). This concludes the proof of Case 3 and also of the theorem. □

4.3 Comparison with Griesmer Bound

Recall that Griesmer bound (Lemma 4) is applicable to linear permutations only. Notably our bound as in (18) works for any permutation. The Table 3 shows different n with corresponding values of Griesmer Bound and our bound (18).

It is noticeable that our bound is very close to Griesmer bound, and in fact matching for some small values of n. The Griesmer bound is not sharp, for example for an $[8, 4]$ binary linear code the maximum possible minimum distance d is 5 (see [1]), whereas the Griesmer bound says $d \leq 6$. Our bound for the differential branch number of permutations of $\mathbb{F}_2^8$ is also 6. At this moment we also do not know the existence of any nonlinear permutation with the differential branch number 6, and in general for $\mathbb{F}_2^n$ with $n \geq 5$, it is not known whether there is any nonlinear permutation for which the bound of the differential branch number is achieved. We suspect that like Griesmer bound our bound is also not sharp in general.

Table 3. Comparison between the differential branch number of linear permutations obtained from Griesmer bound and that of general permutations obtained from our bound (18).

n	Griesmer bound	Our bound
4	4	4
5	4	4
6	4	4
7	5	5
8	6	6
9	6	6
10	7	7
11	8	8
12	8	8
13	8	9
14	8	10
15	9	10
16	10	11
17	10	12
18	11	12
19	12	13

5 Conclusions

In this paper we have analyzed the differential and the linear branch numbers of permutations. We have theoretically proved that 4×4 S-boxes can have the maximum differential branch number 3. This is important for the designers who are aiming to construct lightweight block ciphers following the design like PRESENT. We have also presented upper bounds on both the linear and the differential branch number for permutations over $\mathbb{F}_2^n$, for general n. We feel that there is still a scope of improving these bounds. We showed that the maximum differential branch number and the maximum linear branch number of liner permutations match. However, it is not known whether the same happens for nonlinear permutations as well. It will be interesting to pursue the following question.

Question 1. Can an S-box achieve both the maximum linear and differential branch numbers?

As we have seen that the differential branch number is associated with difference distribution table, whereas the linear branch number is associated with the correlation matrix. Therefore, if there is a relation between these two matrices, then probably we have the answer to Question 1. In fact [17] has shown that there is a relationship between the DDT and the correlation matrix (in a

different form). Let $\mathtt{C}^2_\phi$ denote the following matrix which is derived from the correlation matrix of ϕ.
Recall from (1) that the correlation coefficient of ϕ with respect to (α, β) is given by

$$\mathtt{C}_\phi(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha^t \cdot x \oplus \beta^t \cdot \phi(x)}$$

Now define $\mathtt{C}^2_\phi = [\mathtt{C}^2_\phi(\alpha, \beta)]_{2^n \times 2^n}$ as the matrix whose (α, β)-th element is given by $(\mathtt{C}_\phi(\alpha, \beta))^2$. Then we have the following relation as mentioned in [17, Lemma 2 (iii)]

$$\mathtt{C}^2_\phi = \mathcal{H}_n \mathcal{D}_\phi \mathcal{H}_n, \tag{26}$$

where $\mathcal{H}_n$ is the Hadamard matrix of order $2^n \times 2^n$.

It will be interesting to explore (26) in order to establish a relationship between the linear and the differential branch numbers.

References

1. Bounds on the minimum distance of linear codes over GF(2). http://www.codetables.de/BKLC/Tables.php?q=2&n0=1&n1=256&k0=1&k1=256. Accessed 25 Aug 2017
2. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: a small present. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66787-4_16
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-38424-3_1
4. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
5. Carlet, C.: Vectorial Boolean functions for cryptography. In: Crama, P.H.Y. (ed.) Boolean Methods and Models. Cambridge University Press, Cambridge (2010)
6. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_20
7. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, Heidelberg (2002). https://doi.org/10.1007/978-3-662-04722-4
8. Griesmer, J.: A bound for error-correcting codes. IBM J. Res. Dev. **7**, 532–542 (1960)
9. Jean, J.: TikZ for Cryptographers (2016). https://www.iacr.org/authors/tikz/
10. Leander, G., Poschmann, A.: On the classification of 4 bit S-boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73074-3_13
11. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes (North-Holland Mathematical Library). North Holland, January 1983

12. Matsui, M.: Linear Cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
13. Saarinen, M.-J.O.: Cryptographic analysis of all 4 × 4-bit s-boxes. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 118–133. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28496-0_7
14. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
15. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12
16. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.). IEEE Trans. Inf. Theory **30**(5), 776–780 (1984)
17. Zhang, X., Zheng, Y., Imai, H.: Relating differential distribution tables to other properties of of substitution boxes. Des. Codes Crypt. **19**(1), 45–63 (2000)