Bounds on the Differential 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. Differential branch number measures the diffusion power of a permutation. Differential branch number of nonlinear permutations of $\mathbb{F}_2^n$ has not been analyzed, although it is well studied for linear permutations. In this paper we obtain a bound on differential branch number of permutations (both linear and nonlinear) of $\mathbb{F}_2^n$. We also show that in 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, block cipher, Griesmer bound.

1 Introduction

The basic design principle of a block cipher consists of confusion and diffusion as suggested by Shannon [16]. Confusion layer makes the relation between the key and the ciphertext as complex as possible, whereas diffusion layer spreads the plaintext statistics across the ciphertexts. 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 [4] and linear cryptanalysis [14]. The latter two cryptanalysis methods led to the design known as wide-trail strategy [9]. This design constructs round transformations of block ciphers with efficiency and provides resistance against differential and linear cryptanalysis. This also explains how 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 [17] and PRESENT [6]; 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 [10]. In this model, S-boxes are 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 appeared which relies on the same design principle as of PRESENT.

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 upper bound of 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.

Below we summarize our contributions.

Our contributions

In Section 3, 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 differential branch number. In [15] 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 [12] 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 1, we prove that if a permutation of $\mathbb{F}_2^4$ has differential branch number 4 then it is affine, which shows (Theorem 2) that in fact for any 4×4 S-box, the maximum possible differential branch number is 3. Further in Theorem 3, 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 [11] which applies only to linear permutations, whereas our bound works on any permutation. We compare these two bounds in Table 2, and observe that values are very close to each other.

Differential branch number is not invariant under affine equivalence in general. There are 302 affine equivalence classes of 4×4 S-boxes as listed in [5]. After searching through the affine equivalent S-boxes we identify 7 different S-boxes in Table 3 that have differential branch number 3, nonlinearity 4, differential uniformity 4, and degree 3. Our search concluded that there is no involutory S-box with these properties.

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 is the number of 1's in x, and denoted by $wt(x)$. The bitwise XOR is denoted by $\oplus$.

An $n \times n$ S-box is a permutation $\mathrm{S} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ which is (strictly) nonlinear. For a secure design, S-box needs to satisfy several properties such as high nonlinearity, high differential uniformity, high algebraic degree, etc [8]. We now recall the notion of differential branch number [9].

Definition 1. *The differential branch number of a permutation* $\mathrm{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *is defined as*

$$\mathtt{BN}(\mathrm{F}) = \min_{x,x' \in \mathbb{F}_2^n,\, x \neq x'} \{wt(x \oplus x') + wt(\mathrm{F}(x) \oplus \mathrm{F}(x'))\}. \tag{1}$$

In the rest of this paper, we will simply use *branch number* instead of differential branch number. High branch number relates to the Maximum Expected Differential Probability (MEDP) [7]. If F is linear then (1) simplifies to

$$\mathtt{BN}(\mathrm{F}) = \min_{x \neq 0 \in \mathbb{F}_2^n} \{wt(x) + wt(\mathrm{F}(x))\}.$$

Since $x \neq x'$ and F is bijective, so obviously $\mathtt{BN}(\mathrm{F})$ is ≥ 2. Moreover,

$$\mathtt{BN}(\mathrm{F}) = \mathtt{BN}(\mathrm{F}^{-1}).$$

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

$$\mathrm{F}'(x) = B\,\mathrm{F}[A\,x \oplus c] \oplus d, \qquad \textit{for all } x \in \mathbb{F}_2^n. \tag{2}$$

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 have different 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 $\mathtt{BN}(\mathrm{S}) = 3$, whereas $\mathtt{BN}(\mathrm{S}') = 2$, although they are affine equivalent. The S-box S is used in PRESENT.

On the other hand, if A and B are permutation matrices then the corresponding affine equivalence class preserves the branch number [15]. We state this as the following lemma.

Lemma 1. *If* F *and* F_1 *are two affine equivalent permutations of* $\mathbb{F}_2^n$ *such that* $\mathrm{F}_1(x) = B\,\mathrm{F}[A\,x \oplus c] \oplus d$*, 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* $\mathtt{BN}(\mathrm{F}) = \mathtt{BN}(\mathrm{F}_1)$.

Next we focus on branch number of permutations of $\mathbb{F}_2^n$.

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

Table 1. Affine equivalent S-boxes with different branch number.

3 Bounds on Differential Branch Number

It is trivial to check that for any permutation $\mathrm{F} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$, we have $\mathtt{BN}(\mathrm{F}) \geq 2$. For linear permutations, some upper bound can be easily obtained from coding theory. If $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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 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, branch number of L is bounded by $n + 1$. However, it is known that there is no nontrivial binary MDS code [13], which means there is no linear permutation defined over $\mathbb{F}_2^n$ having branch number $n + 1$. Thanks to Griesmer bound we can have further bounds [11].

Lemma 2 (Griesmer Bound). *Let $[N, K]$ be a binary linear code with the minimum distance d then*

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

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 $\bar{e}$. If $n = 4$ then we have $e_0 = (1, 0, 0, 0)$, $e_1 = (0, 1, 0, 0)$, $e_2 = (0, 0, 1, 0)$, $e_3 = (0, 0, 0, 1)$, $\bar{e} = (1, 1, 1, 1)$. We begin with following remark which will be useful in our proofs.

Remark 1. Let F be a permutation of $\mathbb{F}_2^n$ such that $\mathrm{F}(0) = c$ for some $c \neq 0 \in \mathbb{F}_2^n$. Then for the permutation F$'$ defined as $\mathrm{F}'(x) = \mathrm{F}(x) \oplus c$ it is easy to see that $\mathtt{BN}(\mathrm{F}) = \mathtt{BN}(\mathrm{F}')$ and $\mathrm{F}'(0) = 0$. Thus while deriving bounds of branch numbers we can simply consider permutations F such that $F(0) = 0$.

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 [13] that $\mathtt{BN}(L) \leq n + 1$ except when $q \neq 2$.

Suppose F is a permutation of $\mathbb{F}_2^n$. If $\mathtt{BN}(\mathrm{F}) = n + 1$ then by Definition 1 and using Remark 1 we get

$$wt(e_i \oplus 0) + wt(\mathrm{F}(e_i) \oplus \mathrm{F}(0)) = wt(e_i) + wt(\mathrm{F}(e_i)) \geq n + 1$$

which implies that $wt(\mathrm{F}(e_i)) \geq n$, for $i = 0, \ldots n-1$. This is impossible because there is precisely one element $\bar{e} \in \mathbb{F}_2^n$ with $wt(\bar{e}) = n$. So $\mathtt{BN}(\mathrm{F}) < n + 1$. Therefore, we have the trivial bounds of branch number of permutations of $\mathbb{F}_2^n$ as follows.

Lemma 3. *For any permutation* F *of $\mathbb{F}_2^n$ we have $2 \leq \mathtt{BN}(\mathrm{F}) < n + 1$.*

3.1 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 branch number of a permutation of $\mathbb{F}_2^4$ is 4 then it is affine and hence branch number of any 4×4 S-box is bounded above by 3.

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

C1. *if* $wt(x) = 4$ *then* $wt\left(\mathrm{F}(x)\right) = 4$*,*
C2. *if* $wt(x) = 1$ *then* $wt\left(\mathrm{F}(x)\right) = 3$*,*
C3. *if* $wt(x) = 2$ *then* $wt\left(\mathrm{F}(x)\right) = 2$*,*
C4. *if* $wt(x) = 3$ *then* $wt\left(\mathrm{F}(x)\right) = 1$*.*

Proof. Since $\mathtt{BN}(\mathrm{F}) = 4$, and $\mathrm{F}(0) = 0$, then for any nonzero $x \in \mathbb{F}_2^4$ it must satisfy

$$wt(x) + wt(\mathrm{F}(x)) \geq 4. \tag{3}$$

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

$$wt(e_i \oplus e_j) + wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) = 3 < 4,$$

contradicting (3). Hence C2 follows.

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

$$wt(e_i \oplus x) + wt(\mathrm{F}(e_i) \oplus \mathrm{F}(x)) = 1 + 1 = 2 < 4,$$

again contradicting (3), and hence it follows that $wt(\mathrm{F}(x)) = 2$. This concludes the proof of C3.
Now let's prove C4. Consider x with $wt(x) = 3$. By C2 and C3, we have $wt(S(x)) \neq 2$ and 3. This leaves open the possibility that $wt(\mathrm{F}(x)) = 1$ or 4. If $wt(\mathrm{F}(x)) = 4$, take an element x' with $wt(x') = 2$ and $wt(x \oplus x') = 1$. Then

$$wt(x \oplus x') + wt(\mathrm{F}(x) \oplus \mathrm{F}(x')) = 1 + 2 < 4,$$

a contradiction. So $wt(\mathrm{F}(x)) = 1$.
Finally, C2, C3, C4 imply that $wt(\mathrm{F}(x)) = 4$, when $wt(x) = 4$. □

Now we characterize permutations F of $\mathbb{F}_2^4$ that have $\mathtt{BN}(\mathrm{F}) = 4$.

Theorem 1. *Let* $\mathrm{F} : \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$ *be a permutation with* $\mathtt{BN}(\mathrm{F}) = 4$. *Then* F *is affine.*

Proof. As per Remark 1 we prove the result for $F(0) = 0$. Since $\texttt{BN}(\mathrm{F}) = 4$ and $\mathrm{F}(0) = 0$, F satisfies C1, C2, C3, C4 (Lemma 4). Note that the set of 1-weight vectors $\{e_0, e_1, e_2, e_3\}$ form a basis of $\mathbb{F}_2^4$, by the property C2 of Lemma 4, the corresponding image set $\{\mathrm{F}(e_0), \mathrm{F}(e_1), \mathrm{F}(e_2), \mathrm{F}(e_3)\}$ contains all the 3-weight vectors of $\mathbb{F}_2^4$. Note that $\{\mathrm{F}(e_0), \mathrm{F}(e_1), \mathrm{F}(e_2), \mathrm{F}(e_3)\}$ too forms a basis of $\mathbb{F}_2^4$. If

$$\mathrm{F}(c_0e_0 \oplus c_1e_1 \oplus c_2e_2 \oplus c_3e_3) = c_0\mathrm{F}(e_0) \oplus c_1\mathrm{F}(e_1) \oplus c_2\mathrm{F}(e_2) \oplus c_3\mathrm{F}(e_3)$$

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

As $wt(\mathrm{F}(e_0 \oplus e_1 \oplus e_2 \oplus e_3)) = 4$ (by C1 of Lemma 4), and $wt(\mathrm{F}(e_0) \oplus \mathrm{F}(e_1) \oplus \mathrm{F}(e_2) \oplus \mathrm{F}(e_3)) = 4$, then

$$\mathrm{F}(e_0 \oplus e_1 \oplus e_2 \oplus e_3) = \mathrm{F}(e_0) \oplus \mathrm{F}(e_1) \oplus \mathrm{F}(e_2) \oplus \mathrm{F}(e_3).$$

In the following we will use the fact that $F(e_i) \oplus F(e_j)$ has weight 2, and $F(e_i) \oplus F(e_j) \oplus F(e_k)$ has weight 1. The set $\{\mathrm{F}(e_0), \mathrm{F}(e_1), \mathrm{F}(e_2), \mathrm{F}(e_3)\}$ forms a basis and $wt(\mathrm{F}(e_i \oplus e_j)) = 2$ (by C3 of Lemma 4), then $\mathrm{F}(e_i \oplus e_j)$ can be written as

$$\mathrm{F}(e_i \oplus e_j) = \mathrm{F}(e_\ell) \oplus \mathrm{F}(e_r),$$

for some ℓ and r.

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

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

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

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

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

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

$$\mathrm{F}(e_i \oplus e_j) = \mathrm{F}(e_i) \oplus \mathrm{F}(e_j).$$

We now consider linear combinations of the form $e_i \oplus e_j \oplus e_k$. By C4 of Lemma 4, we have $wt(\mathrm{F}(e_i \oplus e_j \oplus e_k)) = 1$. As $\{\mathrm{F}(e_0), \mathrm{F}(e_1), \mathrm{F}(e_2), \mathrm{F}(e_3)\}$ forms a basis, so we can write

$$\mathrm{F}(e_i \oplus e_j \oplus e_k) = \mathrm{F}(e_\ell) \oplus \mathrm{F}(e_r) \oplus \mathrm{F}(e_t).$$

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

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

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

$$\mathrm{F}(e_i \oplus e_j \oplus e_k) = \mathrm{F}(e_i) \oplus \mathrm{F}(e_j) \oplus \mathrm{F}(e_k).$$

Thus we conclude that F 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 3 and Theorem 1 we can prove the upper bound on branch number of 4×4 S-boxes.

Theorem 2. *The maximum possible branch number of a* 4×4 *S-box is* 3.

The paper [15] followed the work of [12] to search for optimal 4×4 S-boxes in the affine equivalent classes. The maximum branch number in the affine equivalent classes of the 16 optimal 4×4 S-boxes from [12] is 3. As this search did not consider the so-called non-optimal S-boxes, the question of the maximal branch number of any 4×4 S-box remained unanswered. Theorem 2 settles this question. Refer to Table 3, which lists S-boxs S that have $\mathtt{BN}(\mathrm{S}) = 3$ along with other optimal cryptographic properties.

We now give a family of linear permutations $\mathtt{LS}_n$ of $\mathbb{F}_2^n$ with $\mathtt{BN}(\mathtt{LS}_n) = 4$. 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

$$\mathtt{LS}_n(e_i) = \bar{e} \oplus e_i \tag{4}$$

has branch number 4 and it is also involution.

We now give family of linear permutations defined over $\mathbb{F}_2^n$ for odd values of n with branch number 4.

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

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

has 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 $\mathtt{BN}(\mathtt{LS}_n) = 4$ can also be easily checked from the Definition 1 of branch number for linear maps. Next we present bounds for permutations of $\mathbb{F}_2^n$, for $n \geq 5$.

3.2 Differential Branch Number of Permutations of $\mathbb{F}_2^n$, $n \geq 5$

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

Suppose that $x \in \mathbb{F}_2^n$ with $wt(x) = n - \delta$ for some $\delta \geq 1$. 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 $wt(x) \geq n - \delta$ and $wt(x') \geq n - \delta'$ we have*

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

Lemma 5. *Let* F *be a permutation of* $\mathbb{F}_2^n$ *with* $F(0) = 0$ *and branch number* $\mathtt{BN}(\mathrm{F}) = n - \beta + 1$ *for some* $1 \leq \beta \leq n - 1$. *Then we have for* $0 \leq i \leq n - 1$

$$n - \beta \leq wt(\mathrm{F}(e_i)) \leq 2\,\beta + 1 \tag{5}$$

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

$$n - (\beta + 1) \leq wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) \leq 2\,\beta. \tag{6}$$

Proof. From the definition of branch number it follows that

$$wt(\mathrm{F}(e_i)) \geq n - \beta, \tag{7}$$

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

$$wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) \leq 2\beta. \tag{8}$$

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

$$wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) \geq n - (\beta + 1). \tag{9}$$

Using (7) and (9) in Fact 1 we get (5). Further combining (8) and (9) we get (6). □

Lemma 6. *Let δ be an integer such that $1 \leq \delta \leq n$. Denote by $\mathcal{W}_\delta^n$ the following set*

$$\mathcal{W}_\delta^n = \{x \in \mathbb{F}_2^n : wt(x) = n - \delta\}. \tag{10}$$

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

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

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 $x \in \mathcal{W}_\delta^n$ there exist unique set of elements $\{e_{x_1} \dots , e_{x_\delta}\} \subseteq \mathcal{B}_n$ such that $x = \bar{e} \oplus e_{x_1} \oplus \cdots \oplus e_{x_\delta}$. An element $y \in \mathcal{W}_\delta^n$ is in $\mathcal{V}$ if and only if

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

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 branch number of a permutation of $\mathbb{F}_2^n$.

Theorem 3. *If $n \geq 5$ then for any permutation* F *of $\mathbb{F}_2^n$ we have*

$$\mathtt{BN}(\mathrm{F}) \leq \left\lceil 2\,\frac{n}{3} \right\rceil . \tag{11}$$

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 (11) by $n - \left\lfloor \frac{n}{3} \right\rfloor$ to make the proof easy.

On the contrary to (11) assume that $\mathtt{BN}(\mathrm{F}) \geq n - \left\lfloor \frac{n}{3} \right\rfloor + 1$. Using $\beta = \left\lfloor \frac{n}{3} \right\rfloor$ in Lemma 5 we get

$$n - \left\lfloor \frac{n}{3} \right\rfloor \ \leq \ wt(\mathrm{F}(e_i)) \ \leq 2 \ \left\lfloor \frac{n}{3} \right\rfloor + 1 \tag{12}$$

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

$$n - (\left\lfloor \frac{n}{3} \right\rfloor + 1) \ \leq \ wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) \ \leq \ 2 \ \left\lfloor \frac{n}{3} \right\rfloor \tag{13}$$

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

$$n = 3 \ \left\lfloor \frac{n}{3} \right\rfloor + r \tag{14}$$

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 (12) we have

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

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

Case 2. $r = 1$. In this case, by substituting $n = 3 \ \left\lfloor \frac{n}{3} \right\rfloor + 1$ the inequalities (12) and (13) become the following equalities

$$\begin{aligned} wt(\mathrm{F}(e_i)) &= n - \left\lfloor \frac{n}{3} \right\rfloor \\ wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) &= 2 \ \left\lfloor \frac{n}{3} \right\rfloor \end{aligned} \tag{15}$$

Note that both the identities in (15) must be satisfied by all the elements of the set $\{\mathrm{F}(e_0), \ldots, \mathrm{F}(e_{n-1})\}$. We show that this is impossible. Since $wt(\mathrm{F}(e_i)) = n - \lfloor \frac{n}{3} \rfloor$ for all $0 \leq i \leq n-1$, we are in the situation of Lemma 6 with $\mathrm{F}(e_i) \in \mathcal{W}_\delta^n$ where $\delta = \lfloor \frac{n}{3} \rfloor$. Consequently, we see that there can be maximum $\lfloor \frac{n}{\lfloor \frac{n}{3} \rfloor} \rfloor = 3$ elements $\mathrm{F}(e_r), \mathrm{F}(e_s), \mathrm{F}(e_t)$ for which the latter identity in (15) can hold. On the other hand, since $n \geq 5$, there exist at least two basis elements e_u and e_v apart from e_r, e_s, e_t, and by Lemma 6 we will have

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

which contradicts (15).

Case 3. $r = 0$. In this case we have $n = 3\, \lfloor \frac{n}{3} \rfloor$ and the inequalities (12), (13) simplify to

$$wt(\mathrm{F}(e_i))\ = n - \left\lfloor \frac{n}{3} \right\rfloor \ \text{ or } n - \left\lfloor \frac{n}{3} \right\rfloor + 1 \tag{16}$$

$$wt(\mathrm{F}(e_i) \oplus \mathrm{F}(e_j)) = n - \left\lfloor \frac{n}{3} \right\rfloor - 1 \text{ or } n - \left\lfloor \frac{n}{3} \right\rfloor \tag{17}$$

for every $0 \leq i \neq j \leq n-1$. Note that for every element of $\{\mathrm{F}(e_0), \ldots, \mathrm{F}(e_{n-1})\}$ there are only two possibilities for $wt(\mathrm{F}(e_i))$ as in (16). First we show that $wt(\mathrm{F}(e_i)) = wt(\mathrm{F}(e_j)) = n - \lfloor \frac{n}{3} \rfloor + 1$ cannot hold, for $i \neq j$, otherwise using $x = \mathrm{F}(e_i), x' = \mathrm{F}(e_j)$ and $\delta = \delta' = \lfloor \frac{n}{3} \rfloor - 1$ in Fact 1 we get

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

contradicting (17). Thus there can be at most one element $\mathrm{F}(e_i)$ such that $wt(\mathrm{F}(e_i) = n - \lfloor \frac{n}{3} \rfloor + 1$. Without loss of generality assume that $wt(\mathrm{F}(e_0)) = n - \lfloor \frac{n}{3} \rfloor + 1$, then it follows from (16) that for $i = 1, \ldots, n-1$ the weights of $wt(\mathrm{F}((e_i))$ satisfy

$$wt(\mathrm{F}(e_i)) = n - \left\lfloor \frac{n}{3} \right\rfloor . \tag{18}$$

Thus, we are in situation of Lemma 6 with $\mathrm{F}(e_1), \ldots, \mathrm{F}(e_{n-1}) \in \mathcal{W}_\delta^n$ for $\delta = \lfloor \frac{n}{3} \rfloor$. Hence there can be only three elements $\mathrm{F}(e_r), \mathrm{F}(e_s), \mathrm{F}(e_t),\ 1 \leq r \neq s \neq t \leq n-1$ such that for any two indices $i, j \in \{r, s, t\}$

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

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 6) $wt(\mathrm{F}(e_k) \oplus \mathrm{F}(e_i))\ \leq 2(\delta - 1)$, which means that

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

contradicting (17). This concludes proof of Case 3 and also of theorem. □

3.3 Comparison with Griesmer Bound

Recall that Griesmer bound (Lemma 2) is applicable to linear permutations only. Notably our bound as in (11) works for any permutation. The Table 2 shows different n with corresponding values of Griesmer Bound and our bound (11).

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

Table 2. Comparison between branch number of linear permutations obtained from Griesmer bound and that of general permutations obtained from our bound (11).

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 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 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 branch number is achieved. We suspect that like Griesmer bound our bound is also not sharp in general.

4 Identifying good 4×4 S-boxes

The set of permutations of $\mathbb{F}_2^4$ is classified into 302 affine equivalent classes as listed in [5]. Affine equivalence relation preserves several cryptographic properties of permutations like algebraic degree, nonlinearity, differential uniformity. There are 16 affine equivalence classes of S-boxes with nonlinearity 4, different uniformity 4 and degree 3. However, none of the S-boxes in this list has branch number 3. As affine equivalence relation does not preserve branch number of a permutation, so we “unwrap” each equivalence class and collect S-boxes having branch number 3. By unwrapping an S-box S we mean enumerating all the S-boxes that are affine equivalent to S. Finally we obtain 7 S-boxes with nonlinearity 4, different uniformity 4, degree 3, and branch number 3. We list them all in Table 3.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\mathcal{S}_1(x)$	2	B	E	0	8	4	5	9	7	C	1	F	D	A	6	3
$\mathcal{S}_2(x)$	1	7	F	8	2	C	9	5	4	B	3	E	D	6	A	0
$\mathcal{S}_3(x)$	5	E	F	8	B	0	2	D	9	3	C	6	4	A	7	1
$\mathcal{S}_4(x)$	4	F	8	6	E	9	3	A	1	2	7	D	B	5	C	0
$\mathcal{S}_5(x)$	2	D	1	A	B	E	4	3	9	7	C	0	6	8	F	5
$\mathcal{S}_6(x)$	7	A	4	F	E	0	9	5	1	D	B	2	8	3	6	C
$\mathcal{S}_7(x)$	5	6	0	9	C	1	A	4	E	8	3	F	7	B	D	2

Table 3. 4×4 S-boxes with Nonlinearity 4, Differential Uniformity 4, Branch Number 3, and Degree 3.

4.1 Involutory S-boxes over $\mathbb{F}_2^4$

The paper [15] presented 4 classes of permutation-xor equivalent S-boxes mentioning them as “Golden S-boxes”. These S-boxes have the same properties as mentioned in Table 3, and with some additional properties. Table 3 gives the designer more choices of such S-boxes if he is only concerned about these four core cryptographic properties. We also considered searching for 4×4 involutory S-boxes with good cryptographic properties.

A permutation F of $\mathbb{F}_2^n$ is called an involution if $\mathrm{F}(\mathrm{F}(x)) = x$ for all $x \in \mathbb{F}_2^n$. Note that in a block cipher if the S-box is an involution then the same S-box can be used for both encryption and decryption. This saves on implementation cost as one does not need to implement both F and F^{-1}. For instance the block cipher `KHAZAD` [3] uses an involutory S-box. We are interested to see if there is any involutory S-box that have the same property as the 7 S-boxes of Table 3 have. Note that affine equivalence relation does not preserve involution property. So we search for involutory S-boxes in each of the 7 classes. Our search does not yield any involution.

On the other hand one can obtain linear involutions of $\mathbb{F}_2^4$ with branch number 4 by using $\mathtt{LS}_n$ as in (4).

5 Conclusions

In this paper we have analyzed differential branch number 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 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.

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: August 25, 2017.
2. S. Banik, S. K. Pandey, T. Peyrin, S. M. Sim, Y. Todo, and Y. Sasaki. GIFT: A small present. *IACR Cryptology ePrint Archive*, 2017:622, 2017.
3. P. S. L. M. Barreto and V. Rijmen. The Khazad Legacy-Level Block Cipher, 2000. `http://www.cryptonessie.org`.
4. E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. In *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '90, pages 2–21, London, UK, UK, 1991. Springer-Verlag.
5. B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, and G. Stütz. Threshold implementations of all 3×3 and 4×4 S-boxes. In E. Prouff and P. Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 76–91. Springer, 2012.
6. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.
7. A. Canteaut and J. Roué. On the behaviors of affine equivalent sboxes regarding differential and linear attacks. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 45–74. Springer, 2015.
8. C. Carlet. Vectorial Boolean functions for cryptography. In P. H. Y. Crama, editor, *Boolean Methods and Models.* Cambridge University Press, 2010.
9. J. Daemen and V. Rijmen. The wide trail design strategy. In B. Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 2001.
10. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.
11. J. Griesmer. A bound for error-correcting codes. *IBM Journal of Research Development*, 7:532–542, 1960.
12. G. Leander and A. Poschmann. On the classification of 4 bit S-boxes. In C. Carlet and B. Sunar, editors, *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*, volume 4547 of *Lecture Notes in Computer Science*, pages 159–176. Springer, 2007.
13. F. J. Macwilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes (North-Holland Mathematical Library).* North Holland, January 1983.

14. M. Matsui. Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, EUROCRYPT '93, pages 386–397, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.
15. M. O. Saarinen. Cryptographic analysis of all 4 × 4-bit S-boxes. In A. Miri and S. Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 118–133. Springer, 2011.
16. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal, Vol 28, pp. 656–715*, October 1949.
17. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In A. Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.