On the Boomerang Uniformity of Cryptographic Sboxes

Christina Boura, Anne Canteaut

On the Boomerang Uniformity of Cryptographic Sboxes

Christina Boura[1,2] and Anne Canteaut[2]

[1] University of Versailles and Inria, France
Christina.Boura@uvsq.fr

[2] Inria, France
Anne.Canteaut@inria.fr

Abstract. The boomerang attack is a cryptanalysis technique against block ciphers which combines two differentials for the upper part and the lower part of the cipher. The dependency between these two differentials then highly affects the complexity of the attack and all its variants. Recently, Cid et al. introduced at Eurocrypt'18 a new tool, called the Boomerang Connectivity Table (BCT) that permits to simplify this complexity analysis, by storing and unifying the different switching probabilities of the cipher's Sbox in one table. In this seminal paper a brief analysis of the properties of these tables is provided and some open questions are raised. It is being asked in particular whether Sboxes with optimal BCTs exist for even dimensions, where optimal means that the maximal value in the BCT equals the lowest known differential uniformity. When the dimension is even and differs from 6, such optimal Sboxes correspond to permutations such that the maximal value in their DDT and in their BCT equals 4 (unless APN permutations for such dimensions exist). We provide in this work a more in-depth analysis of boomerang connectivity tables, by studying more closely differentially 4-uniform Sboxes. We first completely characterize the BCT of all differentially 4-uniform permutations of 4 bits and then study these objects for some cryptographically relevant families of Sboxes, as the inverse function and quadratic permutations. These two families provide us with the first examples of differentially 4-uniform Sboxes optimal against boomerang attacks for an even number of variables, answering the above open question.

Keywords: Sbox · Boomerang Connectivity Table · Boomerang attack · Boomerang uniformity

1 Introduction

The boomerang attack, introduced by Wagner in 1999 [Wag99] is an important cryptanalysis technique against block ciphers. These attacks can be seen as an extension of classical differential attacks [BS91]. Boomerang cryptanalysis can be applied in cases when it is not possible to find a high probability differential trail for the whole cipher and is based on the idea of combining differential properties of smallest parts of the cipher instead. More precisely, in a classical boomerang attack, a cipher E is seen as the composition of two sub-ciphers E_0 and E_1, i.e. $E = E_1 \circ E_0$. Boomerang attacks work by forming a quartet structure based on a differential $a \to d$ for E_0 of probability p and a differential $c \to b$ for E_1 of probability q, as depicted in Figure 1. Using the following estimate

$$\Pr[E^{-1}(E(x) \oplus b) \oplus E^{-1}(E(x \oplus a) \oplus b) = a] = p^2 q^2, \tag{1}$$

the attack consists in mounting a distinguisher with a data complexity corresponding to $(pq)^{-2}$ adaptive chosen plaintexts/ciphertexts.

IACR Transactions on Symmetric Cryptology ISSN 2519-173X, Vol. 2018, No. 3, pp. 290–310
DOI:10.13154/tosc.v2018.i3.290-310

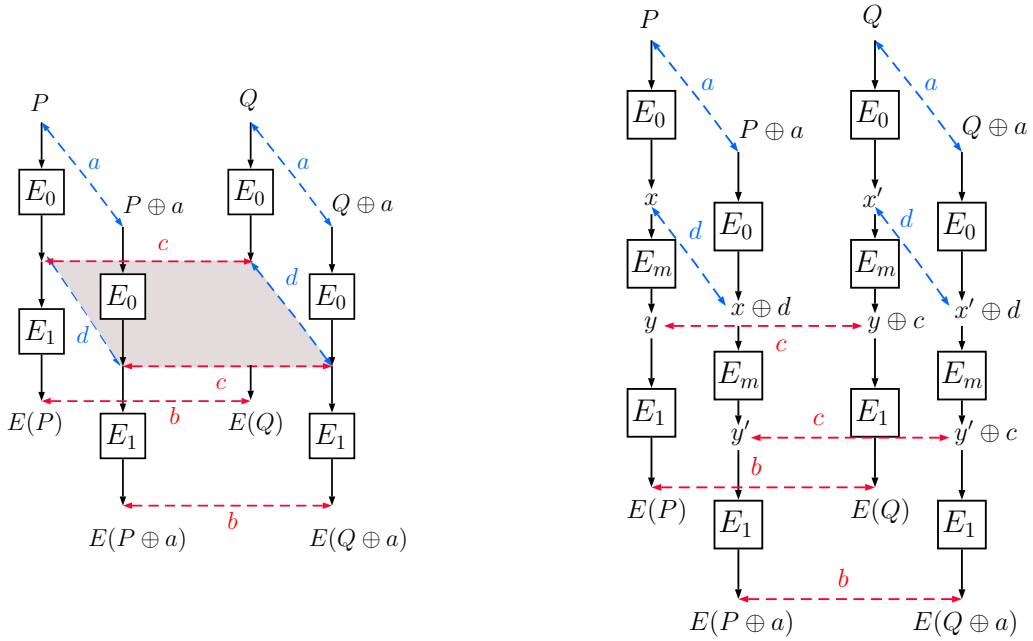


Figure 1: Basic boomerang attack (left) and sandwich attack (right)

Since Wagner's seminal paper, many improvements and variants of boomerang attacks have been proposed [KKS01, BDK01, BDK02, BDD03, BK09, DKS10, KHP+12]. However, Murphy [Mur11] pointed out that the independence assumption used for establishing Eq. (1) may fail: he exhibited some counterexamples for which the probability in (1) is much smaller than this estimate, and some other ones for which this probability is much higher.

A rigorous analysis capturing all these variants has been provided in [DKS14] through the notion of *sandwich attack*. In this case, the cipher is decomposed into three parts, $E = E_1 \circ E_m \circ E_0$, where the middle part E_m is a simple transformation, typically one round (or one S-box layer) of the cipher (see right part of Figure 1). This transition through the middle sub-cipher then formalizes the dependence between the two involved differentials. More precisely, the probability in the previous statistical analysis has to be multiplied by

$$\Pr\left[E_m^{-1}(E_m(x) \oplus c) \oplus E_m^{-1}(E_m(x \oplus d) \oplus c) = d\right]. \tag{2}$$

For instance, the incompatibility exhibited by Murphy corresponds to the situation where this probability vanishes. The so-called *Feistel switch* [BDK05, BK09] refers to the case where E_m is a round of a Feistel cipher. Then, it is easy to see that the Feistel structure implies that the probability (2) is always equal to 1. Similarly, the *ladder switch* introduced by Biryukov and Khovratovich in [BK09] refers to the case where E_m corresponds to the parallel application of smaller transformations, typically to an Sbox layer. Then, if the input difference d_i of the i-th Sbox S_i vanishes, the corresponding contribution to the probability satisfies

$$\Pr[S_i^{-1}(S_i(x_i) \oplus c_i) \oplus S_i^{-1}(S_i(x_i \oplus d_i) \oplus c_i) = d_i] = 1\,.$$

The same property obviously holds if the output difference c_i of the i-th Sbox vanishes.

These observations point out that the value (2) plays a key role when estimating the complexity of boomerang attacks and their generalizations. Recently, in [CHP+18] the authors proposed a new method for evaluating this probability in a more systematic way than by running experiments. This approach consists in studying (2) for a single Sbox

by a method which follows closely what is done for measuring the resistance of a cipher against differential cryptanalysis. Indeed, for differential cryptanalysis, a table called the difference distribution table (DDT) is created for the cipher's Sbox S by recording for each input difference a and for each output difference b the number of solutions of the equation $S(x \oplus a) \oplus S(x) = b$. The smaller the maximal value of the DDT, the better the resistance of the cipher against differential cryptanalysis. In order to evaluate the resistance of a cipher against boomerang attacks, the authors of [CHP+18] introduce a similar table, called the Boomerang Connectivity Table (BCT), to keep for each a and b the number of solutions of the equation

$$S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a.$$

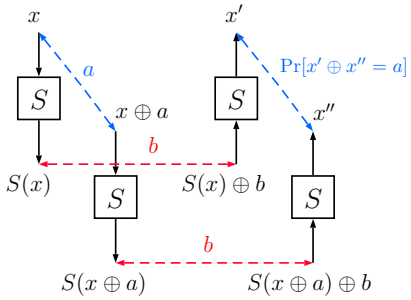
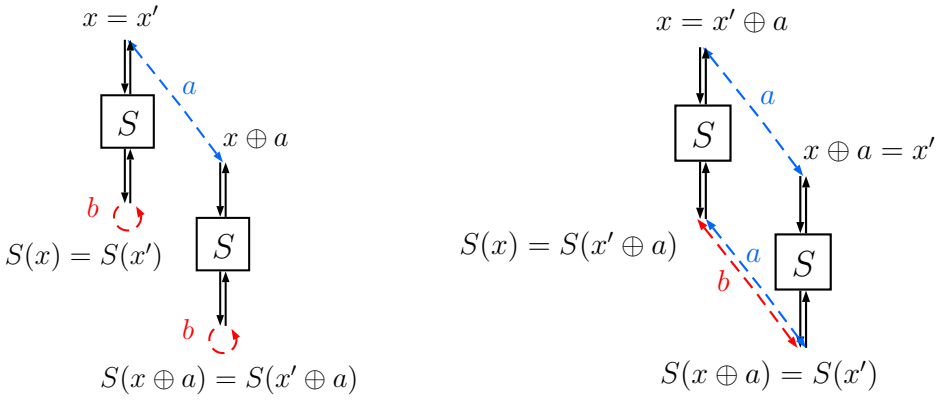


Figure 2: A quartet at the Sbox level

The values of the BCT then record the probability of generating boomerang quartets at the Sbox level (up to a factor 2^{-n}) (see Figure 2). In particular, this representation permits to visualize in a single table both the ladder switch and the Sbox switch (see Figure 3). More importantly, it can reveal in some cases better possible switches. The smaller the maximal value β in the table (excluding the values for a or $b = 0$) the better the resistance of the cipher against boomerang-style attacks. Understanding the properties of such tables allows then designers and cryptanalysts to better evaluate the applicability of boomerang attacks and provides new criteria for designing Sboxes.

The introduction of the Boomerang Connectivity Tables in [CHP+18] was accompanied by a preliminary analysis of their properties and especially of their link with the corresponding DDTs. The authors show notably that the maximum in the BCT, β, is at least equal to the differential uniformity of the Sbox. Moreover, for Almost Perfect Nonlinear (APN) permutations, that are the permutations offering an optimal resistance against differential attacks, the BCT and DDT tables coincide for all values with $a, b \neq 0$. In other words, for APN Sboxes, there are no other switching techniques than the ladder switch and the Sbox switch. On the other hand, it is experimentally shown that, for permutations of $\mathbb{F}_2^4$, a row in a DDT composed only of 0s and 4s leads to an entry equal to 16 in the corresponding row of the BCT. In these cases, there exist some efficient switches other than the ladder switch.

This preliminary analysis therefore raises many important open questions. The case of APN permutations, i.e. permutations with differential uniformity 2, is entirely settled and it was shown, as said before, that such permutations offer an optimal resistance to both differential and boomerang attacks. However, such permutations are only known to exist for odd dimensions, with the only exception being Dillon et al.'s permutation in dimension 6 [BDMW10]. While it is known that for $n = 4$ APN permutations do not exist, for other even dimensions $n \geq 8$, the existence of APN permutations remains an open question, known as the *Big APN Problem* [BDMW10]. Therefore, in even dimensions, notably for $n = 4$ or $n = 8$, designers typically choose Sboxes that offer the next best



(a) Ladder switch **(b)** Sbox switch

Figure 3: Ladder and Sbox switch at the Sbox level

possible resistance to differential cryptanalysis, that is Sboxes with differential uniformity 4. Studying therefore the resistance of such Sboxes against boomerang attacks is an important task. Notably, an open question raised in [CHP+18] is whether optimal differentially 4-uniform Sboxes exist against boomerang attacks, where optimal means that the maximal value in the BCT is 4.

Our contributions. In this paper we study the properties of BCTs, solve some of the problems raised in [CHP+18] and provide results for the BCTs of some important cryptographic families of Sboxes. First, we show that the multi-set composed of all values in the BCT is preserved under affine equivalence and inversion. This very simple result is useful as it restrains the study of BCTs in a given dimension to the study of the properties of a single representative of the affine equivalence class. We then provide a detailed study of the BCTs of all differentially 4-uniform 4-bit permutations and mathematically prove some of the results that were only experimentally verified in [CHP+18]. Next, we entirely determine the boomerang properties for the inverse mapping. In odd dimension this permutation is known to be APN while in even dimension it is differentially 4-uniform. We show here that the maximal value in its BCT is 6 for $n \equiv 0 \mod 4$ and equals 4 for $n \equiv 2 \mod 4$. Therefore, this proves that the inverse mapping has an optimal BCT in such dimensions for a non-APN Sbox. In other words, this solves, for $n \equiv 2 \mod 4$, the open problem raised in [CHP+18]. Finally, we focus on quadratic permutations as these objects present a particular interest for cryptography. Indeed, because of their low multiplicative depth, such functions are good candidates for side-channel resistant and for FHE and MPC-friendly constructions. For example, the Sbox used inside the hash-standard SHA-3 [Dwo15] is a quadratic permutation of $\mathbb{F}_2^5$. We prove first that the maximal value in the BCT of differentially 4-uniform quadratic permutations is at most 12. Also we show that this maximal value is exactly 4 for quadratic power permutations over $\mathbb{F}_{2^n}$ when $n \equiv 2 \mod 4$. Hence, the inverse function and the quadratic differentially 4-uniform power permutations for $n \equiv 2 \mod 4$ provide us with the first examples of optimal non-APN functions against boomerang cryptanalysis.

2 Preliminaries

From now on, the terminology Sbox will refer to a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We introduce here the notions and definitions related to the differential properties of such

functions.

Definition 1 (Derivative of a function)**.** Let S be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. The *derivative of S with respect to $a \in \mathbb{F}_2^n$* is the function

$$\Delta_a S : x \in \mathbb{F}_2^n \mapsto S(x \oplus a) \oplus S(x).$$

The multi-sets corresponding to the images of the derivatives of S are usually represented as a two-dimensional array called the difference distribution table.

Definition 2 (DDT and its characteristics)**.** Let S be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. The *difference distribution table (DDT)* of S is the two-dimensional table defined by

$$\delta_S(a, b) = \#\{x \in \mathbb{F}_2^n : \Delta_a S(x) = b\} \text{ with } a, b \in \mathbb{F}_2^n .$$

The *differential uniformity of S* [Nyb94], denoted by δ_S, is the highest value in the DDT, i.e.

$$\delta_S = \max_{a,b \in \mathbb{F}_2^n, a \neq 0} \delta_S(a, b).$$

A function S with $\delta_S = \delta$ is called *differentially δ-uniform*. Finally, the *differential spectrum* of S is the multi-set

$$\{\delta_S(a, b), a \in \mathbb{F}_2^n \setminus \{0\}, b \in \mathbb{F}_2^n\}.$$

Example 1. When $\mathbb{F}_{2^4}$ is identified with $\mathbb{F}_2^4$ by the primitive polynomial $x^4 + x + 1$, the inverse permutation over $\mathbb{F}_{2^4}$, $S : x \mapsto x^{14}$ has the following value table

$$S = [0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8]$$

and its DDT is provided in Table 1. As it can be seen from this table, S is differentially 4-uniform, i.e. $\delta_S = 4$.

Table 1: DDT of the permutation $x \mapsto x^{2^n-2}$ for $n = 4$

	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	0	0	2	2	0	2	0	2	0	2	2	0
2	0	0	0	2	0	0	0	2	0	4	2	0	2	2	0	2
3	0	0	2	0	0	0	0	2	2	0	2	2	2	0	4	0
4	0	0	0	0	0	2	2	0	2	0	2	0	0	4	2	2
5	0	0	0	0	2	0	2	0	2	2	0	4	2	0	0	2
6	0	2	0	0	2	2	2	4	0	0	2	0	2	0	0	0
7	0	2	2	2	0	0	4	2	2	0	0	0	0	0	0	2
8	0	0	0	2	2	2	0	2	0	0	0	2	0	0	2	4
9	0	2	4	0	0	2	0	0	0	2	0	0	2	0	2	2
a	0	0	2	2	2	0	2	0	0	0	0	0	4	2	2	0
b	0	2	0	2	0	4	0	0	2	0	0	2	2	2	0	0
c	0	0	2	2	0	2	2	0	0	2	4	2	0	0	0	0
d	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
e	0	2	0	4	2	0	0	0	2	2	2	0	0	0	2	0
f	0	0	2	0	2	2	0	2	4	2	0	0	0	2	0	0

The lowest possible value for the differential uniformity of a function from $\mathbb{F}_2^n$ into itself is two and the functions with differential uniformity two are called *almost perfect nonlinear* (APN). While for n odd many families of APN permutations are known [BN15],

for n even only one permutation (up to CCZ equivalence) for $n = 6$, discovered by Dillon et al. in 2009 [BDMW10], is known today. The problem of finding APN permutations for other even dimensions is open and is called *The Big APN Problem*. Therefore, for even dimensions $n \neq 6$, the best choice regarding the differential criterion is the differentially 4-uniform permutations. Such permutations, for both even and odd dimensions, are the object of our study in this article.

We provide now the definition of the Boomerang Connectivity Table (BCT) for a permutation of $\mathbb{F}_2^n$.

Definition 3 ([CHP+18])**.** Let S be a permutation of $\mathbb{F}_2^n$. The *Boomerang Connectivity Table* (BCT) of S is the two-dimensional table defined by

$$\beta_S(a,b) = \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}, \text{ with } a, b \in \mathbb{F}_2^n.$$

The *boomerang uniformity*, denoted by β_S, is the highest value in the BCT without considering the row and the column of index 0:

$$\beta_S = \max_{a,b \in \mathbb{F}_2^n \setminus \{0\}} \beta_S(a,b).$$

Example 2. The BCT of the inverse permutation over $\mathbb{F}_{2^4}$ is provided in Table 2. It can be seen that $\beta_S = 6$.

Table 2: BCT of the permutation $x \mapsto x^{2^n-2}$ for $n = 4$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	4	0	0	0	0	6	6	0	2	0	2	0	2	2	0
2	16	0	0	6	0	0	0	2	0	4	6	0	2	2	0	2
3	16	0	6	0	0	0	0	2	2	0	2	2	6	0	4	0
4	16	0	0	0	0	6	2	0	6	0	2	0	0	4	2	2
5	16	0	0	0	6	0	2	0	2	2	0	4	2	0	0	6
6	16	6	0	0	2	2	6	4	0	0	2	0	2	0	0	0
7	16	6	2	2	0	0	4	6	2	0	0	0	0	0	0	2
8	16	0	0	2	6	2	0	2	0	0	0	6	0	0	2	4
9	16	2	4	0	0	2	0	0	0	2	0	0	6	0	6	2
a	16	0	6	2	2	0	2	0	0	0	0	0	4	2	6	0
b	16	2	0	2	0	4	0	0	6	0	0	2	2	6	0	0
c	16	0	2	6	0	2	2	0	0	6	4	2	0	0	0	0
d	16	2	2	0	4	0	0	0	0	0	2	6	0	2	0	6
e	16	2	0	4	2	0	0	0	2	6	6	0	0	0	2	0
f	16	0	2	0	2	6	0	2	4	2	0	0	0	6	0	0

3 Invariance under some equivalence relations

We show that the multi-set composed of all values in the BCT is preserved under affine equivalence.

Proposition 1. *Let F and G be two permutations of $\mathbb{F}_2^n$ which are affine-equivalent, i.e., there exist two affine permutations A_1 and A_2 such that*

$$G = A_2 \circ F \circ A_1.$$

Then, the BCT of F and G are related by

$$\beta_G(a,b) = \beta_F(L_1(a), L_2^{-1}(b)), \quad \text{for all } a, b \in \mathbb{F}_2^n,$$

where L_1 and L_2 denote the linear parts of A_1 and A_2 respectively.

Proof. Let $x \in \mathbb{F}_2^n$ be a solution of the equation

$$G^{-1}(G(x) \oplus b) \oplus G^{-1}(G(x \oplus a) \oplus b) = a.$$

Equivalently,

$$\begin{aligned} & (A_2 \circ F \circ A_1)^{-1}\left[(A_2 \circ F \circ A_1)(x) \oplus b\right] \oplus (A_2 \circ F \circ A_1)^{-1}\left[(A_2 \circ F \circ A_1)(x \oplus a) \oplus b\right] = a \\ \Leftrightarrow \quad & F^{-1} \circ A_2^{-1}\left[(A_2 \circ F \circ A_1)(x) \oplus b\right] \oplus F^{-1} \circ A_2^{-1}\left[(A_2 \circ F \circ A_1)(x \oplus a) \oplus b\right] = L_1(a) \end{aligned} \quad (3)$$

where this equality is obtained by using that, for any affine function A,

$$A(x_1) \oplus A(x_2) = L(x_1 \oplus x_2)$$

where L is the linear part of A.

Now, by writing $A_2(x) = L_2(x) \oplus \gamma$, we have that $A_2^{-1}(x) = L_2^{-1}(x \oplus \gamma)$. It follows that

$$\begin{aligned} A_2^{-1}\left[(A_2 \circ F \circ A_1)(x) \oplus b\right] &= L_2^{-1}\left[(L_2 \circ F \circ A_1)(x) \oplus \gamma \oplus b \oplus \gamma\right] \\ &= (F \circ A_1)(x) \oplus L_2^{-1}(b)\ . \end{aligned}$$

We then deduce that Equation (3) is equivalent to

$$F^{-1}\left[F(A_1(x)) \oplus L_2^{-1}(b)\right] \oplus F^{-1}\left[F(A_1(x \oplus a)) \oplus L_2^{-1}(b)\right] = L_1(a).$$

By setting $y = A_1(x)$ we get that y is a solution of

$$F^{-1}\left[F(y) \oplus L_2^{-1}(b)\right] \oplus F^{-1}\left[F(y \oplus L_1(a)) \oplus L_2^{-1}(b)\right] = L_1(a).$$

In other words, x belongs to the set involved in $\beta_G(a, b)$ if and only if $y = A_1(x)$ belongs to the set involved in $\beta_F(L_1(a), L_2^{-1}(b))$. □

A similar relation can be exhibited between the BCT of a permutation and the BCT of its inverse.

Proposition 2. *Let S be a permutation of $\mathbb{F}_2^n$. Then, the BCT of S and of S^{-1} are related by*

$$\beta_{S^{-1}}(a, b) = \beta_S(b, a), \quad \textit{for all } a, b \in \mathbb{F}_2^n\ .$$

Proof. Let $x \in \mathbb{F}_2^n$ be a solution of

$$S(S^{-1}(x \oplus a) \oplus b) \oplus S(S^{-1}(x) \oplus b) = a\ .$$

Equivalently,

$$S^{-1}(x \oplus a) \oplus b = S^{-1}\left(S(S^{-1}(x) \oplus b) \oplus a\right)$$

which means that $y = S^{-1}(x)$ is a solution of

$$S^{-1}(S(y) \oplus a) \oplus b = S^{-1}\left(S(y \oplus b) \oplus a\right)\ .$$

In other words x belongs to the set involved in $\beta_{S^{-1}}(a, b)$ if and only if $y = S^{-1}(x)$ belongs to the set involved in $\beta_S(b, a)$. □

We have proved that the multi-set formed by all values in the BCT is invariant under affine equivalence and inversion. In other words, the behaviour of the BCT with respect to these two classes of transformations is exactly the same as the behaviour of the DDT. However, while the differential spectrum of a function is also preserved by the extended-affine (EA) equivalence (i.e. all transformations of the form $A_2 \circ F \circ A_1 \oplus A_0$ where A_1, A_2 are affine permutations and A_0 is an affine function), this is not the case for the BCT. For instance, the two permutations G_4 and G_6 from [LP07] are EA-equivalent, but their boomerang uniformities differ: $\beta_{G_4} = 10$ and $\beta_{G_6} = 8$. Another important equivalence notion between Sboxes is the so-called CCZ-equivalence [CCZ98]. Two functions F and G are said to be CCZ-equivalent if and only if $\{(x, G(x)), x \in \mathbb{F}_2^n\} = \mathcal{A}\{(x, F(x)), x \in \mathbb{F}_2^n\}$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$. As EA-equivalence is a special case of CCZ-equivalence, we deduce that the boomerang uniformity is also not always preserved under CCZ-equivalence.

4 An alternative formulation

Let us define the following two sets of $\mathbb{F}_2^n$:

$$\begin{aligned}\mathcal{U}_{a,b}^S &= \{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus a) = b\},\\ \mathcal{V}_{a,b}^S &= \{S(x) \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus a) = b\}\end{aligned}$$

For the sake of simplicity, Parameter S will be omitted in this notation if the involved mapping is clear from the context. A simple remark is that

$$\mathcal{V}_{a,b}^S = \mathcal{U}_{b,a}^{S^{-1}}.$$

Indeed,

$$\begin{aligned}\mathcal{V}_{a,b}^S &= \{S(x) \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus a) = b\}\\ &= \{y \in \mathbb{F}_2^n : y \oplus S(S^{-1}(y) \oplus a) = b\}\\ &= \{y \in \mathbb{F}_2^n : S^{-1}(y) \oplus S^{-1}(y \oplus b) = a\}\\ &= \mathcal{U}_{b,a}^{S^{-1}}.\end{aligned}$$

We now provide an alternative formula for computing the entries in a BCT of a permutation.

Proposition 3. *For any permutation S of $\mathbb{F}_2^n$, for all $a, b \in \mathbb{F}_2^n$, we have*

$$\beta_S(a,b) = \delta_S(a,b) + \sum_{\gamma \neq 0,b} \#\left(\mathcal{V}_{a,\gamma}^S \cap (\mathcal{V}_{a,\gamma}^S \oplus b)\right) . \tag{4}$$

Proof.

$$\begin{aligned}\beta_S(a,b) &= \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}\\ &= \sum_{\gamma \neq 0} \#\{x : S(x) \oplus S(x \oplus a) = \gamma \text{ and } S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}\\ &= \sum_{\gamma \neq 0} \#\{x : S(x) \oplus S(x \oplus a) = \gamma \text{ and } S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x) \oplus b \oplus \gamma) = a\}\end{aligned}$$

When $\gamma = b$, any x satisfying the first equation satisfies the second one too. Indeed, if $x \in \mathcal{U}_{a,b}$, then

$$S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x)) = S^{-1}(S(x \oplus a)) \oplus S^{-1}(S(x)) = a\,.$$

We then deduce that

$$\begin{aligned}\beta_S(a,b) &= \delta_S(a,b) + \sum_{\gamma \neq 0,b} \#\{x \in \mathcal{U}_{a,\gamma}^S \text{ and } S(x) \oplus b \in \mathcal{U}_{\gamma,a}^{S^{-1}}\}\\ &= \delta_S(a,b) + \sum_{\gamma \neq 0,b} \#\{y \in \mathcal{V}_{a,\gamma}^S \text{ and } y \oplus b \in \mathcal{U}_{\gamma,a}^{S^{-1}}\}\\ &= \delta_S(a,b) + \sum_{\gamma \neq 0,b} \#\{y \in \mathcal{V}_{a,\gamma}^S \text{ and } y \oplus b \in \mathcal{V}_{a,\gamma}^S\}\\ &= \delta_S(a,b) + \sum_{\gamma \neq 0,b} \left(\mathcal{V}_{a,\gamma}^S \cap (\mathcal{V}_{a,\gamma}^S \oplus b)\right).\end{aligned}$$

□

We directly recover from Eq. (4) the following two observations from [CHP+18], corresponding to the *ladder switch* and to the *Sbox switch* respectively:

$$\beta_S(a,0) = 2^n \text{ and } \beta_S(a,b) \geq \delta_S(a,b) \ ,$$

for all $a, b \in \mathbb{F}_2^n$.

Most notably, the highest entry in the BCT β_S is larger than or equal to the differential uniformity of the Sbox. It follows that the lowest possible value for β_S is two, and it is achieved if and only if S is APN. Since no APN permutation of $\mathbb{F}_2^n$ is known for even $n \neq 6$, an optimal BCT in this case corresponds to $\beta_S = 4$, and can only be achieved for differentially 4-uniform Sboxes.

Case of planar permutations. In most practical cases, the Sboxes used in symmetric primitives are *planar* in the sense of the following definition introduced by Daemen and Rijmen.

Definition 4. [DR07] A mapping S from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is called planar if and only if, for all a and b in $\mathbb{F}_2^n$, both sets $\mathcal{U}_{a,b}$ and $\mathcal{V}_{a,b}$ are affine subspaces.

Differentially 4-uniform permutations form an important family of planar mappings. Indeed, since $\mathcal{U}_{a,b}^S$ consists of at most 2 pairs of elements of the form $(x, x \oplus a)$, it is an affine subspace of dimension at most 2. Also, the concatenation of several Sboxes with differential uniformity 4 is planar, implying that the substitution layers in the AES [AES01], in Serpent [BAK98], in Present [BKL+07], Prince [BCG+12] and in many other lightweight ciphers are planar.

For any planar mapping S, we can write $\mathcal{U}_{a,b}^S$ and $\mathcal{V}_{a,b}^S$ as

$$\begin{aligned} \mathcal{U}_{a,b}^S &= u_{a,b} \oplus U_{a,b}^S \\ \mathcal{V}_{a,b}^S &= v_{a,b} \oplus V_{a,b}^S, \end{aligned}$$

where $U_{a,b}^S$ and $V_{a,b}^S$ are linear spaces and $u_{a,b}$ and $v_{a,b}$ are some constants such that $u_{a,b} \in \mathcal{U}_{a,b}^S$ and $v_{a,b} \in \mathcal{V}_{a,b}^S$. Moreover, if $\delta_S(a,b) \neq 0$, we obviously have that $a \in U_{a,b}^S$ and $b \in V_{a,b}^S$.

In the special case of a planar permutation, Proposition 3 can be formulated in a simpler way showing that any entry within Row a in the BCT corresponds to a sum of some entries within Row a in the DDT.

Proposition 4. *For any planar permutation S of $\mathbb{F}_2^n$, for all $a, b \in \mathbb{F}_2^n$, we have*

$$\beta_S(a,b) = \sum_{\gamma \neq 0 : b \in V_{a,\gamma}^S} \delta_S(a,\gamma) \ ,$$

where $V_{a,\gamma}^S$ is the linear space associated to the affine space $\mathcal{V}_{a,\gamma}^S$.

Proof. Proposition 3 involves the cardinality of the intersection

$$\mathcal{V}_{a,\gamma}^S \cap (\mathcal{V}_{a,\gamma}^S \oplus b) \ .$$

When S is planar, $\mathcal{V}_{a,\gamma}^S$ is an affine subspace, $\mathcal{V}_{a,\gamma}^S = v_{a,\gamma} \oplus V_{a,\gamma}^S$. Then, only two situations may occur:

- either $b \in V_{a,\gamma}^S$, which equivalently means that $(\mathcal{V}_{a,\gamma}^S \oplus b) = \mathcal{V}_{a,\gamma}^S$,
- or $b \notin V_{a,\gamma}^S$, which means that $(\mathcal{V}_{a,\gamma}^S \oplus b)$ is a coset of $V_{a,\gamma}^S$ different from $\mathcal{V}_{a,\gamma}^S$. In this case, the intersection between the two cosets of the same linear space is empty.

It follows that

$$\mathcal{V}^S_{a,\gamma} \cap (\mathcal{V}^S_{a,\gamma} \oplus b)$$

equals $\delta_S(a,\gamma)$ when $b \in V^S_{a,\gamma}$ and 0 otherwise. Then,

$$\beta_S(a,b) = \delta_S(a,b) + \sum_{\gamma \notin \{0,b\} : b \in V^S_{a,\gamma}} \delta_S(a,\gamma) \ ,$$

and the result directly follows from the fact that $b \in V^S_{a,\gamma}$. □

Example 3. We illustrate Propositions 3 and 4 by using the Sbox S introduced in Example 1. Let $a = 1$. It can be checked that $\mathcal{V}^S_{1,1} = \{0,1,6,7\}$, $\mathcal{V}^S_{1,6} = \{11,13\}$, $\mathcal{V}^S_{1,7} = \{9,14\}$, $\mathcal{V}^S_{1,9} = \{5,12\}$, $\mathcal{V}^S_{1,11} = \{3,8\}$, $\mathcal{V}^S_{1,13} = \{2,15\}$, $\mathcal{V}^S_{1,14} = \{4,10\}$ and $\mathcal{V}^S_{1,\gamma} = \emptyset$ for all other $\gamma \in \mathbb{F}_2^4$. For the respective linear spaces we have that $V^S_{1,1} = \{0,1,6,7\}$, $V^S_{1,\gamma} = \{0,\gamma\}$ for $\gamma \in \{6,7,9,11,13,14\}$ and $V^S_{1,\gamma} = \emptyset$ for all other $\gamma \in \mathbb{F}_2^4$.

Let $b = 6$. We see that $(\mathcal{V}^S_{1,\gamma} \cap (\mathcal{V}^S_{1,\gamma} \oplus 6)) \neq \emptyset$ only for $\gamma = 1$. In this case, we have $(\mathcal{V}^S_{1,\gamma} \oplus 6) = \mathcal{V}^S_{1,\gamma}$. Therefore, Proposition 3 leads to

$$\beta_S(1,6) = \delta_S(1,6) + \#(\mathcal{V}^S_{1,1} \cap (\mathcal{V}^S_{1,1} \oplus 6)) = 2 + 4 = 6.$$

Alternatively, as S is planar since it has differential uniformity 4, Proposition 4 gives:

$$\beta_S(1,6) = \delta_S(1,6) + \delta_S(1,1) = 2 + 4 = 6.$$

5 BCT tables for 4-bit permutations

5.1 BCT of all 4-bit permutations with $\delta_S = 4$

We have shown that the maximum value in the BCT is preserved under affine equivalence. It is then sufficient to study the BCT for one representative of the affine equivalence class. For $n = 4$ full classifications exist, see for example [DeC07] or [LP07]. Following the classification by De Cannière, we show in Table 3 the spectrum of the BCT for all classes of 4-bit permutations with $\delta_S = 4$, i.e., the values n_i corresponding to the number of times the value i appears in the BCT. This classification includes all optimal permutations with $\delta_S = 4$ and optimal linearity $\mathcal{L}(S) = 8$ listed in [LP07], and also permutations with $\delta_S = 4$ and a higher linearity.

A first important observation from Table 3 is that all 4-bit permutations with $\delta_S = 4$ have boomerang uniformity at least 6. This then proves that 4-bit Sboxes with boomerang uniformity 4 do not exist, as conjectured in [CHP+18, Section 6.1].

Another remark is that the inverse of Permutation 11 in Table 3 belongs to the affine-equivalence class of Permutation 10, implying that their BCTs contain the same values as shown by Proposition 2. Similarly, the inverse of Permutation 16 belongs to the affine-equivalence class of Permutation 13. Then, any two 4-bit permutations with $\delta_S = 4$ that are not related by inversion or affine equivalence have different BCT spectra.

We also notice that for all permutations with $\delta_S = 4$ in four variables $n_{12} = 0$ and $n_{14} = 0$, meaning that the values 12 and 14 never appear in the BCT table.

Table 3: Spectrum of the BCT for all 4-bit permutations with differential uniformity 4. Column 4 mentions the link with the functions of Table 5.2 in [DeC07]. For the first 16 permutations, we also mention the corresponding equivalence class in the Leander-Poschmann classification [LP07].

	Representative	$\mathcal{L}(S)$	[DeC07]	[LP07]	n_0	n_2	n_4	n_6	n_8	n_{10}	n_{16}	β_S
1	[8, 0, 1, 12, 15, 5, 6, 7, 4, 3, 10, 11, 9, 13, 14, 2]	8	3	G_3	120	60	15	30	0	0	0	**6**
2	[2, 0, 1, 8, 3, 11, 6, 7, 4, 9, 10, 15, 12, 13, 14, 5]	8	6	G_5	108	72	27	18	0	0	0	**6**
3	[8, 0, 1, 12, 2, 5, 6, 9, 4, 3, 10, 11, 7, 13, 14, 15]	8	2	G_6	104	80	27	10	4	0	0	**8**
4	[8, 0, 1, 9, 2, 5, 13, 7, 4, 6, 10, 11, 12, 3, 14, 15]	8	8	G_{11}	100	85	30	5	5	0	0	**8**
5	[4, 0, 1, 15, 2, 11, 6, 7, 3, 9, 10, 5, 12, 13, 14, 8]	8	1	G_{13}	105	78	28	11	2	1	0	**10**
6	[2, 0, 1, 8, 3, 13, 6, 7, 4, 9, 10, 5, 12, 11, 14, 15]	8	4	G_4	112	72	23	14	0	4	0	**10**
7	[2, 0, 1, 8, 3, 15, 6, 7, 4, 9, 5, 11, 12, 13, 14, 10]	8	5	G_7	105	80	30	5	0	5	0	**10**
8	[4, 8, 1, 2, 3, 11, 6, 7, 0, 9, 10, 14, 12, 13, 5, 15]	8	7	G_{12}	110	75	25	10	0	5	0	**10**
9	[8, 14, 1, 2, 3, 5, 6, 7, 4, 12, 10, 11, 9, 13, 0, 15]	8	9	G_9	108	69	28	14	5	1	0	**10**
10	[8, 14, 1, 2, 3, 5, 6, 7, 4, 9, 15, 11, 12, 13, 0, 10]	8	10	G_{14}	108	70	27	13	6	1	0	**10**
11	[8, 15, 1, 2, 3, 5, 12, 7, 4, 9, 10, 11, 6, 13, 14, 0]	8	11	G_{15}	108	70	27	13	6	1	0	**10**
12	[8, 15, 1, 2, 3, 5, 6, 13, 4, 9, 10, 11, 12, 7, 14, 0]	8	12	G_{10}	108	69	30	12	3	3	0	**10**
13	[12, 0, 1, 9, 3, 5, 4, 7, 6, 2, 10, 11, 8, 13, 14, 15]	8	13	G_2	107	64	32	8	12	0	2	**16**
14	[12, 11, 1, 2, 3, 5, 4, 7, 6, 9, 10, 0, 8, 13, 14, 15]	8	14	G_1	107	60	36	12	8	0	2	**16**
15	[12, 9, 1, 2, 3, 5, 4, 7, 6, 0, 10, 11, 8, 13, 14, 15]	8	15	G_8	103	72	32	0	16	0	2	**16**
16	[8, 14, 1, 2, 3, 5, 4, 7, 6, 9, 10, 0, 12, 13, 11, 15]	8	16	G_0	107	64	32	8	12	0	2	**16**
17	[8, 15, 1, 2, 3, 12, 6, 7, 4, 9, 10, 11, 5, 13, 14, 0]	12	34	–	112	57	35	14	0	7	0	**10**
18	[8, 0, 1, 12, 2, 5, 11, 7, 4, 9, 10, 6, 3, 13, 14, 15]	12	35	–	109	60	34	15	4	3	0	**10**
19	[8, 0, 1, 12, 2, 5, 13, 7, 4, 9, 10, 11, 3, 6, 14, 15]	12	36	–	109	60	34	15	4	3	0	**10**
20	[12, 0, 1, 2, 3, 15, 6, 7, 4, 9, 10, 11, 8, 13, 14, 5]	12	37	–	110	58	30	14	12	0	1	**16**
21	[12, 0, 1, 2, 3, 5, 6, 13, 4, 9, 10, 11, 8, 7, 14, 15]	12	38	–	106	62	36	8	10	2	1	**16**

5.2 Understanding the results

The previous table confirms several observations on 4-bit Sboxes reported in [CHP+18], which have been obtained experimentally by examining all Sboxes having specific properties. Most of these phenomena can actually be deduced from the following lemma which is very specific to the case of mappings over $\mathbb{F}_2^4$.

Lemma 1. *Let S be a permutation on $\mathbb{F}_2^4$ such that there exist $a, b_1, b_2 \in \mathbb{F}_2^4$ satisfying $\delta_S(a, b_1) = \delta_S(a, b_2) = 4$. Then,*

$$V_{a,b_1} \cap V_{a,b_2} \neq \{0\} .$$

Proof. Since $\delta_S(a, b_1) = \delta_S(a, b_2) = 4$, $\mathcal{V}_{a,b_1}$ and $\mathcal{V}_{a,b_2}$ are two affine subspaces of dimension 2. Let $\mathcal{V}_{a,b_1} = c_1 \oplus \langle b_1, \gamma_1 \rangle$ and $\mathcal{V}_{a,b_2} = c_2 \oplus \langle b_2, \gamma_2 \rangle$. By definition, $\mathcal{V}_{a,b_1}$ and $\mathcal{V}_{a,b_2}$ are disjoint. This means that $c_2 \notin c_1 \oplus \langle b_2, \gamma_2, b_1, \gamma_1 \rangle$. However, if $V_{a,b_1} \cap V_{a,b_2} = \{0\}$, then $\langle b_1, \gamma_1, b_2, \gamma_2 \rangle$ covers the whole space $\mathbb{F}_2^4$, which contradicts the previous property. □

Example 4. We illustrate Lemma 1 on the PRESENT [BKL+07] Sbox. The DDT of this Sbox S is shown in Table 4 while its BCT is shown in Table 5. Let the input difference be $a = 8$. As it can be seen from Table 4, $\delta_S(8, \mathtt{b}) = \delta_S(8, \mathtt{f}) = 4$. It is easy to check that $\mathcal{V}_{8,\mathtt{b}} = \{1, 5, \mathtt{a}, \mathtt{e}\}$ and $\mathcal{V}_{8,\mathtt{f}} = \{2, 3, \mathtt{c}, \mathtt{d}\}$. The corresponding linear spaces are $V_{8,\mathtt{b}} = \{0, 4, \mathtt{b}, \mathtt{f}\}$ and $V_{8,\mathtt{f}} = \{0, 1, \mathtt{e}, \mathtt{f}\}$ and we see that $V_{8,\mathtt{b}} \cap V_{8,\mathtt{d}} = \{0, \mathtt{f}\} \neq \{\mathtt{0}\}$, as expected by Lemma 1.

Table 4: Difference Distribution Table (DDT) of the PRESENT Sbox

	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	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
a	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

The previous lemma implies a strong relationship between the boomerang uniformity of a 4-bit Sbox and the number of values 4 in a row of its DDT. This relationship explains for instance the fact observed in [CHP+18, Lemma 3]: if the DDT of a 4-bit Sbox S has a row with entries 0 and 4 only, then $\beta_S = 16$.

Proposition 5. *Let S be a permutation of $\mathbb{F}_2^4$ with $\delta_s = 4$. Then,*

- *If its DDT has a row with at least two values 4, then $\beta_S \geq 8$;*
- *If each row in its DDT has at most two values 4, then $\beta_S \leq 10$;*
- *If its DDT has a row with four values 4, then $\beta_S = 16$.*

Table 5: Boomerang Connectivity Table of the PRESENT Sbox

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	4	4	0	16	4	4	4	4	0	0	4	4	0	0
2	16	0	0	6	0	4	6	0	0	0	2	0	2	2	2	0
3	16	2	0	6	2	4	4	2	0	0	2	2	0	0	0	0
4	16	0	0	0	0	4	2	2	0	6	2	0	6	0	2	0
5	16	2	0	0	2	4	0	0	0	6	2	2	4	2	0	0
6	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
7	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
8	16	4	0	2	4	0	0	2	0	2	0	4	0	2	4	8
9	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
a	16	0	2	2	0	4	0	0	6	0	2	0	0	6	2	0
b	16	2	0	0	2	4	0	0	4	2	2	2	0	6	0	0
c	16	0	6	0	0	4	0	6	2	2	2	0	0	0	2	0
d	16	2	4	2	2	4	0	6	0	0	2	2	0	0	0	0
e	16	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
f	16	8	0	0	8	0	0	0	0	0	0	8	0	0	8	16

Proof. We know from Proposition 4 that, for any Sbox with differential uniformity 4,

$$\beta_S(a,b) = \sum_{\gamma \neq 0 : b \in V_{a,\gamma}} \delta_S(a,\gamma), \text{ for all } a,b \in \mathbb{F}_2^n .$$

Suppose that the row of index a in the DDT of S is such that there exist γ_1 and γ_2 with $\delta_S(a,\gamma_1) = \delta_S(a,\gamma_2) = 4$. We then deduce from Lemma 1 that there exists a nonzero b in $V_{a,\gamma_1} \cap V_{a,\gamma_2}$. Thus,

$$\beta_S(a,b) \geq \delta_S(a,\gamma_1) + \delta_S(a,\gamma_2) = 8 .$$

Let us now assume that the row of index a contains exactly two values 4, i.e. $\delta_S(a,\gamma) \leq 2$ for all $\gamma \notin \{\gamma_1,\gamma_2\}$. Then, for all $\gamma \notin \{\gamma_1,\gamma_2\}$, $V_{a,\gamma}$ is either empty, or equal to $\{0,\gamma\}$, implying that $b \notin V_{a,\gamma}$ when $\gamma \notin \{0,b\}$. Then, the set of all $\gamma \neq 0$ such that $b \in V_{a,\gamma}$ is always included in $\{b,\gamma_1,\gamma_2\}$. We deduce that, if $b \in \{\gamma_1,\gamma_2\}$, $\beta_S(a,b) = 8$. Otherwise,

$$\beta_S(a,b) \leq \delta_S(a,b) + \delta_S(a,\gamma_1) + \delta_S(a,\gamma_2) \leq 10 .$$

Now we assume that all entries in the row of index a equal 4, i.e. there exist $\gamma_0,\gamma_1,\gamma_2,\gamma_3$ such that $\delta_S(a,\gamma_i) = 4$ for all $0 \leq i \leq 3$, and $\delta_S(a,\gamma) = 0$ otherwise. We will show now that in this special case the above spaces have not only non-trivial pairwise intersections, but on top of that their joint intersection is not trivial i.e. $V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_2} \cap V_{a,\gamma_3} \neq \{0\}$, which directly implies that the BCT uniformity is 16. Indeed, let $b \in V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_2} \cap V_{a,\gamma_3}$, then by Proposition 4, $\beta(a,b) = \delta(a,\gamma_0) + \delta(a,\gamma_1) + \delta(a,\gamma_2) + \delta(a,\gamma_3) = 4 \cdot 4 = 16$. For proving that the above intersection is non-trivial, we first show that any three of these sets have a non-trivial intersection. By contradiction, suppose w.l.o.g. that $V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_2} = \{0\}$. From Lemma 1, we know that $V_{a,\gamma_0} = \langle \gamma_0, b \rangle$ and $V_{a,\gamma_1} = \langle \gamma_1, b \rangle$ for some nonzero b. When $\gamma_1 = \gamma_0 \oplus b$, a trivial intersection between the 3 sets cannot occur: otherwise, $V_{a,\gamma_0} = V_{a,\gamma_1}$ and the intersection between the three sets equals $V_{a,\gamma_0} \cap V_{a,\gamma_2}$ which is non-trivial by Lemma 1. Let us now focus on the case where $\gamma_1 \neq \gamma_0 \oplus b$. Since b does not belong to V_{a,γ_2}, V_{a,γ_2} must be one of the following spaces: $\langle \gamma_0,\gamma_1 \rangle$, $\langle \gamma_0, b \oplus \gamma_1 \rangle$, $\langle b \oplus \gamma_0, \gamma_1 \rangle$ or $\langle b \oplus \gamma_0, b \oplus \gamma_1 \rangle$. In other words, V_{a,γ_2} is a 2-dimensional space $\langle \alpha, \beta \rangle \subset \langle \gamma_0,\gamma_1,b \rangle$ which differs from $\langle \gamma_0, b \rangle$ and from $\langle \gamma_1, b \rangle$. Moreover, by definition, the three affine subspaces $\mathcal{V}_{a,\gamma_0} = c_0 \oplus \langle \gamma_0, b \rangle$, $\mathcal{V}_{a,\gamma_1} = c_1 \oplus \langle \gamma_1, b \rangle$ and $\mathcal{V}_{a,\gamma_2} = c_2 \oplus \langle \alpha, \beta \rangle$ are disjoint. This means that

$$c_0 \notin c_1 \oplus \langle \gamma_0, b, \gamma_1 \rangle$$

and

$$c_0 \notin c_2 \oplus \langle \gamma_0, b, \alpha, \beta \rangle = c_2 \oplus \langle \gamma_0, b, \gamma_1 \rangle \ .$$

The linear space $\langle \gamma_0, \gamma_1, b \rangle$ has dimension 3 since $b \notin \{\gamma_0, \gamma_1\}$ and $\gamma_1 \neq \gamma_0 \oplus b$. Moreover, the two cosets of $\langle \gamma_0, \gamma_1, b \rangle$ defined by c_1 and c_2 are disjoint since $\mathcal{V}_{a,\gamma_1}$ and $\mathcal{V}_{a,\gamma_2}$ are disjoint. Therefore, these two cosets cover the whole space $\mathbb{F}_2^4$, which leads to a contradiction. This proves that any three sets among $V_{a,\gamma_0}, V_{a,\gamma_1}, V_{a,\gamma_2}$ and V_{a,γ_3} have a nontrivial intersection.

Then, the only situation where $V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_2} \cap V_{a,\gamma_3} = \{0\}$ corresponds to the case where there are two distinct nonzero elements b_0 and b_1 which respectively belong to $(V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_2})$ and $(V_{a,\gamma_0} \cap V_{a,\gamma_1} \cap V_{a,\gamma_3})$. This means that $(V_{a,\gamma_0} \cap V_{a,\gamma_1})$ contains two nonzero elements, implying that $V_{a,\gamma_0} = V_{a,\gamma_1}$. But in this case, the intersection between the four subspaces equals the intersection between the last three subspaces, which is known to be nontrivial, a contradiction. □

Example 5. We illustrate Proposition 5 on the PRESENT [BKL+07] Sbox. From Table 4 we first observe that the row corresponding to the input difference $a = 6$ contains two values 4. Then, we can check from Table 5 that $\beta_S(6, 15) = 8$. On the other hand, the row corresponding to $a = 1$ has four values 4. Then, as seen from Table 5, $\beta_S(1, 5) = 16$ and thus $\beta_S = 16$.

This result does not hold anymore for higher even dimensions. For instance, we will exhibit in Section 7 permutations of $\mathbb{F}_2^n$ with differential uniformity 4, for $n \equiv 2 \bmod 4$, such that there is a row in their DDT with entries in $\{0, 4\}$ while their boomerang uniformity equals 4.

Proposition 5 also implies that the values 12 and 14 never appear in the BCT of differentially 4-uniform permutations of $\mathbb{F}_2^4$, as observed in Table 3. Indeed, the DDT of any such permutation does not contain any row with exactly 3 entries equal to 4 (and 2 entries equal to 2). Therefore, the nonzero entries in the BCT belong to $\{2, 4, 6, 8, 10, 16\}$.

6 BCT of the inverse mapping over $\mathbb{F}_{2^n}$

We have proved that the lowest boomerang uniformity that can be achieved for 4-bit permutations is $\beta_S = 6$. This minimum is obtained for the inverse mapping $x \mapsto x^{14}$ over $\mathbb{F}_{2^4}$, which is affine equivalent to the Sbox in the first row of Table 3. We now investigate the properties of the BCT of the inverse mapping $S : x \mapsto x^{2^n-2}$ over $\mathbb{F}_{2^n}$ for larger values of n. It is well-known that the inverse mapping over $\mathbb{F}_{2^n}$ is APN if n is odd. If n is even, then its DDT has exactly one 4 and $(2^{n-1} - 2)$ 2's per row [Nyb94]. We show here that if $n \equiv 0 \mod 4$ then $\beta_S = 6$ and this value is 4 if $n \equiv 2 \mod 4$. This then solves the open problem raised in [CHP+18] on the existence of Sboxes S such that $\beta_S = \delta_S = 4$.

Proposition 6. *Let S be the inverse mapping over $\mathbb{F}_{2^n}$ for n even. Then:*

$$\beta_S = \begin{cases} 4, & \text{if} \quad n \equiv 2 \mod 4 \\ 6, & \text{if} \quad n \equiv 0 \mod 4 \end{cases}$$

Moreover,

- *If $n \equiv 2 \bmod 4$, for any nonzero a, b, we have*

$$\beta_S(a, b) = \begin{cases} 4 & \text{if } b \in \{a^{-1}\omega, a^{-1}(\omega \oplus 1)\} \\ \delta_S(a, b) & \text{otherwise} \end{cases}$$

- *If $n \equiv 0 \bmod 4$, for any nonzero a, b, we have*

$$\beta_S(a, b) = \begin{cases} 6 & \text{if } b \in \{a^{-1}\omega, a^{-1}(\omega \oplus 1)\} \\ \delta_S(a, b) & \text{otherwise} \end{cases}$$

where ω is any element in $\mathbb{F}_4 \setminus \mathbb{F}_2$, i.e. any element[1] *in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $\omega^3 = 1$.*

Proof. Since the inverse mapping on an even number of variables has differential uniformity 4, we use the equivalent formula given in Proposition 4 for computing the BCT entries:

$$\beta_S(a,b) = \sum_{\gamma \neq 0 : b \in V_{a,\gamma}} \delta_S(a,\gamma).$$

As for each row of the DDT there is exactly one 4 per row, there is exactly one γ_a such that $\delta_S(a,\gamma_a) = 4$. Then, for all $\gamma \neq \gamma_a$, $V_{a,\gamma}$ is either empty, or equal to $\{0,\gamma\}$, implying that $b \notin V_{a,\gamma}$ when $\gamma \notin \{0,b\}$. It follows that,

$$\beta_S(a,b) = \begin{cases} \delta_S(a,b) & \text{if } b \notin V_{a,\gamma_a} \\ 4 & \text{if } b = \gamma_a \\ \delta_S(a,b)+4 & \text{if } b \in V_{a,\gamma_a} \setminus \{0,\gamma_a\} \end{cases}.$$

From this, we see already that the boomerang uniformity is at most 6. We will prove now that, for any $a \neq 0$ and any $b \in V_{a,\gamma_a} \setminus \{0,\gamma_a\}$, $\delta_S(a,b) = 0$ if $n \equiv 2 \mod 4$ and 2 if $n \equiv 0 \mod 4$.

We first recall that in the case of the inverse function, for any $a,\gamma \neq 0$, $\delta(a,\gamma) = \delta(1,a\gamma)$. Indeed, consider the equation:

$$(X \oplus a)^{2^n-2} \oplus X^{2^n-2} = \gamma.$$

This equation, by setting $Y = a^{-1}X$, is equivalent to

$$(Y \oplus 1)^{2^n-2} \oplus Y^{2^n-2} = a\gamma,$$

which proves that $\delta(a,\gamma) = \delta(1,a\gamma)$.

Consider the case of $a = 1$. It is well-known that the equation

$$(X \oplus 1)^{2^n-2} \oplus X^{2^n-2} = 1$$

has exactly four solutions. First, $X = 0$ and $X = 1$ are solutions of this equation. The other two solutions are $\alpha^{\frac{2^n-1}{3}}$ and $\alpha^{2\frac{2^n-1}{3}}$ where α is a primitive element of $\mathbb{F}_{2^n}$. If we denote $\omega = \alpha^{\frac{2^n-1}{3}}$ then the four solutions are $\{0,1,\omega,\omega^2\}$ which means that

$$\mathcal{U}_{1,1} = \mathbb{F}_4 = \{0,1,\omega,\omega^2\} = \langle \omega, 1 \rangle.$$

By taking now into account that $\delta(a,\gamma_a) = \delta(1,a\gamma_a)$, this means that $\delta(a,\gamma_a) = 4$ if and only if $a\gamma_a = 1$, or equivalently $\gamma_a = a^{-1}$. By using that $\mathcal{U}_{a,\gamma} = a\mathcal{U}_{1,a\gamma}$ and applying it to $\gamma = a^{-1}$, we deduce that $\mathcal{U}_{a,a^{-1}} = a\mathcal{U}_{1,1} = \langle a, a\omega \rangle$ and then $\mathcal{V}_{a,a^{-1}} = \mathcal{U}_{a^{-1},a} = \langle a^{-1}, a^{-1}\omega \rangle$.

We then need to consider $b \in \langle a^{-1}, a^{-1}\omega \rangle \setminus \{0, a^{-1}\}$, i.e. $b = a^{-1}\omega$ and $b = a^{-1}(\omega \oplus 1)$. We look at the value of $\delta(a,b)$, which is equivalent to looking at the value $\delta(1,ab) = \delta(1,\omega)$ or $\delta(1,\omega \oplus 1)$.

When $X \notin \{0,1\}$, the equations

$$\begin{aligned} (X \oplus 1)^{2^n-2} \oplus X^{2^n-2} &= \omega \\ (X \oplus 1)^{2^n-2} \oplus X^{2^n-2} &= \omega \oplus 1 \end{aligned}$$

are equivalent to the equations

$$\begin{aligned} X^2 \oplus X \oplus \omega &= 0 \\ X^2 \oplus X \oplus \omega \oplus 1 &= 0 \end{aligned}$$

[1] It is worth noticing that there are two elements in $\mathbb{F}_4 \setminus \mathbb{F}_2$, ω and $\omega' = \omega \oplus 1$, and both of them obviously lead to the same condition.

and these last equations have two solutions if $\mathrm{Tr}(\omega) = 0$ (see e.g. [McE87, Page 108]).

$$\begin{aligned}\mathrm{Tr}(\omega) &= \omega \oplus \omega^2 \oplus \omega^4 \oplus \omega^8 \oplus \cdots \oplus \omega^{2^{n-2}} \oplus \omega^{2^{n-1}} \\ &= (\omega \oplus \omega^2) \oplus (\omega^4 \oplus \omega^8) \oplus \cdots \oplus (\omega^{2^{n-2}} \oplus \omega^{2^{n-1}}) \\ &= 1 \oplus 1 \oplus \cdots \oplus 1,\end{aligned}$$

implying

$$\mathrm{Tr}(\omega) = 1 \text{ if and only if } n \equiv 2 \bmod 4\ . \tag{5}$$

This means that $\delta(1,\omega) = 0$ and $\delta(1,\omega \oplus 1) = 0$ if $n \equiv 2 \mod 4$ and $\delta(1,\omega) = 2$ and $\delta(1,\omega \oplus 1) = 2$ if $n \equiv 0 \mod 4$. This completes the proof. □

7 BCT of quadratic permutations with differential uniformity 4

In this section we concentrate on quadratic permutations that are differentially 4-uniform. For an even number of variables, APN quadratic permutations do not exist [Nyb95]. Therefore, $\delta_S = 4$ is the lowest differential uniformity that a quadratic permutation can achieve in this case. Here, we provide an upper bound on the boomerang uniformity of such permutations. More importantly, we exhibit quadratic permutations with optimal BCT, i.e. which have differential uniformity and boomerang uniformity equal to 4.

We first emphasize a behaviour of differentially 4-uniform quadratic permutations that is central in the proofs of the results in this section.

Lemma 2. *Let S be a differentially 4-uniform quadratic permutation and let $\Delta_a S$ be a derivative whose differential spectrum is $\{0,4\}$. Then, for all $\gamma \in \mathrm{Im}(\Delta_a S)$, the affine spaces $\mathcal{U}_{a,\gamma}$ are cosets of the same linear space $\langle a, \alpha\rangle$:*

$$\mathcal{U}_{a,\gamma} = x_\gamma \oplus \langle a, \alpha\rangle \text{ for some } x_\gamma \in \mathbb{F}_2^n.$$

Proof. If S is a quadratic permutation, then all its derivatives have degree at most 1. Since $\Delta_a S$ is an affine (or constant) function, all equations $\Delta_a S(x) = \gamma$ are of the form $L_a(x) = (\gamma \oplus c_a)$ for a given linear function L_a and a given constant c_a. Then, for any γ, the set of solutions of $\Delta_a S(x) = \gamma$ is either empty, or a coset of the linear space $U = \ker L_a$ of dimension d_a. Obviously, $d_a \in \{1,2\}$ when S has differential uniformity 4. This implies that the affine subspaces $\mathcal{U}_{a,\gamma}$ obtained for the different values of γ are all cosets of the same linear space U. The result directly follows from the fact that $a \in U$. □

We now prove a general bound on β_S for differentially 4-uniform quadratic permutations.

Proposition 7. *Let S be a quadratic permutation of $\mathbb{F}_2^n$ with differential uniformity 4. Then $\beta_S \leq 12$.*

Proof. The previous lemma implies that the differential spectrum of a derivative $\Delta_a S$, $a \neq 0$, is either $\{0,2\}$ or $\{0,4\}$, depending on the value of a. For a derivative $\Delta_a S$ whose differential spectrum is $\{0,2\}$, we have that for all $b \in \mathbb{F}_2^n$, $\beta(a,b) \in \{0,2\}$. We then concentrate on derivatives $\Delta_a S$ whose differential spectrum is $\{0,4\}$. Let γ_i, $0 \leq i < 2^{n-2}$ denote the elements in $\mathrm{Im}\,\Delta_a S$. Then, from the previous lemma, we have

$$\mathcal{U}_{a,\gamma_i} = x_i \oplus \langle a, \alpha\rangle \text{ and } \mathcal{V}_{a,\gamma_i} = y_i \oplus \langle \gamma_i, \beta_i\rangle\ .$$

We now show that

$$\{\beta_i, \beta_i \oplus \gamma_i : 0 \leq i < 2^{n-2}\} = \mathrm{Im}\,\Delta_\alpha S \cup \mathrm{Im}\,\Delta_{a\oplus\alpha} S$$

where this equality is an equality between multi-sets (i.e. on elements and their multiplicities). The form of $\mathcal{U}_{a,\gamma_i}$ and $\mathcal{V}_{a,\gamma_i}$ implies that

$$\begin{aligned} S(x_i) \oplus S(x_i \oplus a) &= \gamma_i \\ S(x_i \oplus \alpha) \oplus S(x_i \oplus \alpha \oplus a) &= \gamma_i \ , \end{aligned}$$

and $\beta_i = S(x_i) \oplus S(x_i \oplus \alpha)$, leading to

$$\begin{aligned} S(x_i) \oplus S(x_i \oplus \alpha) &= \beta_i \\ S(x_i \oplus a) \oplus S(x_i \oplus a \oplus \alpha) &= \beta_i \end{aligned}$$

and

$$\begin{aligned} S(x_i) \oplus S(x_i \oplus \alpha \oplus a) &= \gamma_i \oplus \beta_i \\ S(x_i \oplus a) \oplus S(x_i \oplus \alpha) &= \gamma_i \oplus \beta_i \ . \end{aligned}$$

This means that

$$\mathcal{V}_{a,\gamma_i} = \mathcal{V}_{\alpha,\beta_i} = \mathcal{V}_{a\oplus\alpha,\gamma_i\oplus\beta_i} \text{ and } \mathcal{U}_{a,\gamma_i} = \mathcal{U}_{\alpha,\beta_i} = \mathcal{U}_{a\oplus\alpha,\gamma_i\oplus\beta_i}.$$

It follows that, for each γ_i in the image set of $\Delta_a S$, the corresponding β_i and $\gamma_i \oplus \beta_i$ belong to the image set of $\Delta_\alpha S$ and to the image set of $\Delta_{a\oplus\alpha} S$ respectively. Since all $\mathcal{U}_{a,\gamma_i}$ for $0 \leq i < 2^{n-2}$, are disjoint, all $\mathcal{V}_{\alpha,\beta_i}$ are disjoint which implies that all β_i are distinct. The same holds obviously for all the $\beta_i \oplus \gamma_i$.

We now prove the bound on the β_S of such permutations. From Proposition 4, we get that

$$\beta_S(a,b) = \sum_{\gamma \neq 0 : b \in V_{a,\gamma}} \delta_S(a,\gamma) \ ,$$

which in our case can be equivalently written as

$$\beta_S(a,b) = 4\#\{i : b \in \{\gamma_i, \beta_i, \gamma_i \oplus \beta_i\}\} \ .$$

Using that

$$\{\gamma_i, \beta_i, \gamma_i \oplus \beta_i, 0 \leq i < 2^{n-2}\} = \operatorname{Im} \Delta_a S \cup \operatorname{Im} \Delta_\alpha S \cup \operatorname{Im} \Delta_{a\oplus\alpha} S$$

β_S is maximized when b belongs to each one of the three sets $\operatorname{Im} \Delta_a S$, $\operatorname{Im} \Delta_\alpha S$ and $\operatorname{Im} \Delta_{a\oplus\alpha} S$. Then for such a b, $\beta(a,b) = 12$. □

It is worth noticing that this result does not contradict Theorem 5 which states that if the DDT of a 4-bit permutation with $\delta_S = 4$ has a row with four values 4, then $\beta_S = 16$. The reason is that it can easily be checked from Table 3 that quadratic permutations of $\mathbb{F}_2^4$ with differential uniformity 4 do not exist.

For $n = 5$ there are three differentially 4-uniform quadratic permutations up to affine equivalence [BBS17]. For two of them, $\beta_S = 12$ while for the third one $\beta_S = 8$.

We now show that some of the so-called Gold power permutations [Gol68], which are differentially 4-uniform quadratic permutations of $\mathbb{F}_2^n$, also have an optimal BCT when $n \equiv 2 \bmod 4$, i.e. they satisfy $\beta_S = 4$.

Proposition 8. *Let $n \equiv 2 \bmod 4$ and let t be an even integer such that $\gcd(t,n) = 2$. Then $S : x \mapsto x^{2^t+1}$ over $\mathbb{F}_{2^n}$ is a differentially 4-uniform permutation and satisfies $\beta_S = 4$.*

Proof. It is well-known that the power function with Gold exponent x^{2^t+1} over $\mathbb{F}_{2^n}$ has differential uniformity 2^d where $d = \gcd(t, n)$ [Nyb94, Prop. 3]. Moreover, this mapping is bijective if and only if $\gcd(2^t + 1, 2^n - 1) = 1$. Recall that (see e.g. [McE87, Lemma 11.1])

$$\gcd\left(2^t + 1, 2^n - 1\right) = 1 \text{ if and only if } \gcd(t, n) = \gcd(2t, n) \; .$$

It follows that, when $\gcd(t, n) = 2$, x^{2^t+1} is a permutation of $\mathbb{F}_{2^n}$ if and only if $n \equiv 2 \bmod 4$.

It is also known from [BCC10, Lemma 4] that, for any nonzero a and b, the set $\mathcal{U}_{a,b}$ is either empty or a coset of $a\mathbb{F}_4 = \langle a, a\omega\rangle$ where ω is an element in $\mathbb{F}_4 \setminus \mathbb{F}_2$. Then, by applying the same technique as in the proof of the previous proposition, we have that $\max_{b\neq 0} \beta_S(a, b) = 4$ if and only if $\operatorname{Im} \Delta_a S$, $\operatorname{Im} \Delta_{a\omega} S$ and $\operatorname{Im} \Delta_{a(\omega\oplus 1)}$ are disjoint.

Each set $\operatorname{Im} \Delta_a S$ is an affine subspace of codimension 2. We now describe it as a coset of the orthogonal of a 2-dimensional subspace. To this purpose, we use that, for any nonzero $\lambda \in \mathbb{F}_{2^n}$

$$\begin{aligned}
\operatorname{Tr}(\lambda \Delta_a S(x)) &= \operatorname{Tr}\left(\lambda(x \oplus a)^{2^t+1} \oplus \lambda x^{2^t+1}\right) \\
&= \operatorname{Tr}\left(\lambda a x^{2^t} \oplus \lambda a^{2^t} x \oplus \lambda a^{2^t+1}\right) \\
&= \operatorname{Tr}\left(x^{2^t}(\lambda a \oplus \lambda^{2^t} a^{2^{2t}})\right) \oplus \operatorname{Tr}(\lambda a^{2^t+1}) \; .
\end{aligned}$$

It follows that $x \mapsto \operatorname{Tr}(\lambda \Delta_a S(x))$ is constant if and only if

$$\lambda a \oplus \lambda^{2^t} a^{2^{2t}} = 0$$

which equivalently means that

$$\left(\lambda a^{2^t+1}\right)^{2^t-1} = 1 \; .$$

Since $\gcd(2^t - 1, 2^n - 1) = 2^{\gcd(t,n)} - 1 = 3$, this occurs if and only if $\lambda a^{2^t+1} \in \mathbb{F}_4^*$. It follows that, for every $\lambda = a^{-(2^t+1)}\beta$ with $\beta \in \mathbb{F}_4$ and every $x \in \mathbb{F}_{2^n}$,

$$\operatorname{Tr}(\lambda \Delta_a S(x)) = \operatorname{Tr}(\lambda a^{2^t+1}) = \operatorname{Tr}(\beta) \; .$$

For $\beta = \omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have $\operatorname{Tr}(\omega) = 1$ when $n \equiv 2 \bmod 4$ (see (5)), implying that

$$\operatorname{Im} \Delta_a S = \{x \in \mathbb{F}_{2^n} : \operatorname{Tr}(a^{-(2^t+1)}x) = 0 \text{ and } \operatorname{Tr}(a^{-(2^t+1)}\omega x) = 1\} \; .$$

Now, we observe that, since t is even, $\omega^{2^t+1} = \omega^2 \times \omega^{2^t-1} = \omega^2$. Thus

$$(a\omega)^{-(2^t+1)} = a^{-(2^t+1)}(\omega^2)^{-1} = a^{-(2^t+1)}\omega \; ,$$

and we obtain that

$$\begin{aligned}
\operatorname{Im} \Delta_{a\omega} S &= \{x \in \mathbb{F}_{2^n} : \operatorname{Tr}(a^{-(2^t+1)}\omega x) = 0 \text{ and } \operatorname{Tr}(a^{-(2^t+1)}\omega^2 x) = 1\} \\
&= \{x \in \mathbb{F}_{2^n} : \operatorname{Tr}(a^{-(2^t+1)}\omega x) = 0 \text{ and } \operatorname{Tr}(a^{-(2^t+1)} x) = 1\} \; .
\end{aligned}$$

Similarly,

$$\operatorname{Im} \Delta_{a(\omega\oplus 1)} S = \{x \in \mathbb{F}_{2^n} : \operatorname{Tr}(a^{-(2^t+1)}x) = 1 \text{ and } \operatorname{Tr}(a^{-(2^t+1)}\omega x) = 1\} \; .$$

Therefore, for any nonzero a, $\operatorname{Im} \Delta_a S$, $\operatorname{Im} \Delta_{a\omega} S$ and $\operatorname{Im} \Delta_{a(\omega\oplus 1)} S$ are three different cosets of the same linear space, and are then disjoint. We eventually deduce that $\beta_S = 4$. □

As an example of the previous proposition, we get that $S : x \mapsto x^5$ over $\mathbb{F}_{2^n}$ with $n \equiv 2 \bmod 4$ is an Sbox with optimal BCT in the sense of [CHP+18] since it satisfies $\delta_S = \beta_S = 4$. It is worth noticing that, for these dimensions, these quadratic differentially 4-uniform permutations have the same behaviour as the inverse mapping studied in Section 6, while their DDTs are very different. Indeed, the DDTs of the quadratic mappings in Proposition 8 consist of 0 and 4 only, while the DDT of the inverse mapping has a single 4 in each row.

8 Conclusion

Boomerang connectivity tables are newly introduced objects for measuring the resistance of a block cipher against boomerang attacks. Apart from a brief analysis of their properties provided in the introductory paper, very little was known about these tables. In this paper we exhibited some new BCT properties, by showing for example that the boomerang uniformity is invariant up to affine equivalence and inversion and we used this result to entirely determine the value of the boomerang uniformity for all differentially 4-uniform permutations of $\mathbb{F}_2^4$. More importantly, we answered an open question from [CHP+18] on the existence of differentially 4-uniform permutations with optimal boomerang uniformity in even dimensions. Indeed, we exhibited two different families of permutations in $\mathbb{F}_2^n$, with $n \equiv 2 \mod 4$ that are both differentially 4-uniform and have boomerang uniformity 4. These two families then provide a positive answer to the problem in dimensions $n \equiv 2 \mod 4$. However, while we proved that the best possible boomerang uniformity for $n = 4$ is 6, the problem remains open for larger n multiple of 4, notably for $n = 8$. Another open problem is to determine whether the BCT spectrum determines the function up to some simple equivalence. A similar question has been raised for the DDT in [BCJS18]. Here, we showed that, for $n = 4$, differentially 4-uniform Sboxes that are not affine equivalent or inverse of each other have different BCT spectra. But what happens for higher dimensions remains unclear.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, November 2001.

[BAK98] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Serge Vaudenay, editor, *FSE'98*, volume 1372 of *LNCS*, pages 222–238. Springer, Heidelberg, March 1998.

[BBS17] Dusan Bozilov, Begül Bilgin, and Haci Ali Sahin. A Note on 5-bit Quadratic Permutations' Classification. *IACR Trans. Symmetric Cryptol.*, 2017(1):398–404, 2017.

[BCC10] Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential properties of power functions. *International Journal of Information and Coding Theory*, 1(2):149–170, 2010.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, Heidelberg, December 2012.

[BCJS18] Christina Boura, Anne Canteaut, Jérémy Jean, and Valentin Suder. Two notions of differential equivalence on Sboxes. *Designs, Codes and Cryptography*, 2018.

[BDD03] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of SAFER++. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 195–211. Springer, Heidelberg, August 2003.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 340–357. Springer, Heidelberg, May 2001.

[BDK02] Eli Biham, Orr Dunkelman, and Nathan Keller. New results on boomerang and rectangle attacks. In Joan Daemen and Vincent Rijmen, editors, *FSE 2002*, volume 2365 of *LNCS*, pages 1–16. Springer, Heidelberg, February 2002.

[BDK05] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 507–525. Springer, Heidelberg, May 2005.

[BDMW10] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN permutation in dimension six. In *Finite Fields: Theory and Applications*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18. Springer, Heidelberg, December 2009.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, Heidelberg, September 2007.

[BN15] Céline Blondeau and Kaisa Nyberg. Perfect nonlinear functions and cryptography. *Finite Fields and Their Applications*, 32:120–147, 2015.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Heidelberg, August 1991.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 683–714. Springer, Heidelberg, April / May 2018.

[DeC07] Christophe DeCannière. Analysis and Design of Symmetric Encryption Algorithms. PhD thesis, Katholieke Universiteit Leuven, 2007.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 393–410. Springer, Heidelberg, August 2010.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology*, 27(4):824–849, October 2014.

[DR07] Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET Information Security*, 1(1):11–17, 2007.

[Dwo15] Morris J. Dworkin. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. *Federal Information Processing Standards Publication*, NIST FIPS - 202, August 2015.

[Gol68] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Information Theory*, 14(1):154–156, 1968.

[KHP+12] Jongsung Kim, Seokhie Hong, Bart Preneel, Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. *IEEE Trans. Information Theory*, 58(7):4948–4966, 2012.

[KKS01] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 75–93. Springer, Heidelberg, April 2001.

[LP07] Gregor Leander and Axel Poschmann. On the Classification of 4 Bit S-Boxes. In Claude Carlet and Berk Sunar, editors, *WAIFI 2007*, volume 4547 of *LNCS*, pages 159–176. Springer, Heidelberg, June 2007.

[McE87] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.

[Mur11] Sean Murphy. The return of the cryptographic boomerang. *IEEE Trans. Information Theory*, 57(4):2517–2521, 2011.

[Nyb94] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer, Heidelberg, May 1994.

[Nyb95] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 111–130. Springer, Heidelberg, December 1995.

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 156–170. Springer, Heidelberg, March 1999.