Determination of cryptographic tables and properties related to the revised boomerang and its application to a fundamental S-box

Said Eddahmani[1] and Sihem Mesnager[1,2]

[1] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis,
Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France
said.eddahmani@etud.univ-paris8.fr
[2] Telecom Paris, 91120 Palaiseau, France
smesnager@univ-paris8.fr

Abstract. In symmetric cryptography, vectorial Boolean functions over finite fields $\mathbb{F}_{2^n}$ derive strong S-boxes. To this end, the S-box should satisfy a list of tests to resist existing attacks, such as the differential, linear, boomerang, and variants. Several tables are employed to measure an S-box's resistance, such as the difference distribution table (DDT) and the boomerang connectivity table (BCT). Following the boomerang attacks recently revisited in terms of the boomerang switch effect, with a lustration highlighting the power of this technique, a tool called the Boomerang Difference Table (BDT), an alternative to the classical Boomerang BCT, was introduced. Next, two novel tables have been introduced, namely, the Upper Boomerang Connectivity Table (UBCT) and the Lower Boomerang Connectivity Table (LBCT), which are considered improvements over BCT while allowing systematic evaluation of boomerangs to return over multiple rounds.

This paper focuses on the new tools for measuring the revisited version of boomerang attacks and the related tables UBCT, LBCT, as well as the so-called Extended Boomerang Connectivity Table (EBCT). Specifically, we shall study the properties of these novel tools and investigate the corresponding tables. We also study their interconnections, their links to the DDT, and their values for affine equivalent vectorial functions and compositional inverses of permutations of $\mathbb{F}_{2^n}$. Moreover, we introduce the concept of the nontrivial boomerang connectivity uniformity and determine the explicit values of all the entries of the EBCT, LBCT, and EBCT for the important cryptographic case of the inverse function.

Mathematics Subject Classification: 06E30, 05A05, 35F05, 11T06, 11T55, 94A60.

1 Introduction

Let n be a positive integer, and $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A vectorial Boolean function is a map $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ where m is also a positive integer. In most cases, $m = n$ and F is a permutation of $\mathbb{F}_{2^n}$. Vectorial Boolean permutations are intensively used for designing Substitution Boxes (S-boxes). An important reference in this context is the book of Carlet ([7]). A typical example is the Advanced Encryption Standard (AES) [9], which is based on the inverse function. Several criteria are used to test the resistance of an S-box derived from a Boolean vectorial function to cryptanalytic attacks by studying the entries of specific tables. The most known tables are the Difference Distribution Table (DDT) [2], the Boomerang Connectivity Table (BCT) [8], the Differential-Linear Connectivity Table (DLCT) [1], and the Feistel Boomerang Connectivity Table (FBCT) [3]. According to the maximum value of the non-trivial entries in a table, the S-box is more or less resistant to an attack, and the vectorial Boolean function is more or less suitable for cryptographic purposes. It is established that the most secure vectorial Boolean functions are the inverse function[9], the Gold function [16], the Kasami function [17], the Bracken-Leander [5] function, the Welch function [11], the Niho function [12], and the Dobbertin function [13].

In this article, we concentrate on the boomerang attack [27], which is a cryptanalysis technique that allows an attack to concatenate two short differential characteristics. The corresponding tools (the BCT table and the boomerang uniformity) have attracted much attention recently. The reader can consult, for instance, the following references [4,6,8,18,19,20,22,23] and the references therein.

In the meantime, several research results showed that the dependency between these two characteristics at the switching round could significantly impact the attack's complexity or potentially make it invalid. In 2019, Wang and Peyrin [26] introduced two new tables to test the resistance of an S-Box. The two tables are variants of the BCT and were later labelled by Delaune, Derbez and Vavrille [10] as Upper BCT (UBCT) and Lower BCT (LBCT).

The UBCT of a permutation F of $\mathbb{F}_{2^n}$ is a $2^n \times 2^n \times 2^n$ table where the entry at $(a, b, c) \in \mathbb{F}_{2^n}^3$ is given by

$$\mathtt{UBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x+a) = b, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a \end{array} \right.\right\}.$$

Similarly, the LBCT of F is a $2^n \times 2^n \times 2^n$ table where the entry at $(a, b, c) \in \mathbb{F}_{2^n}^3$ is given by

$$\mathtt{LBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x+b) = c, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a \end{array} \right.\right\}.$$

Yet another table called the Extended BCT (EBCT), was proposed in [10]. It is a $2^n \times 2^n \times 2^n \times 2^n$ table where the entry at $(a, b, c, d) \in \mathbb{F}_{2^n}^4$ is given by

$$\mathtt{EBCT}_F(a,b,c,d) = \#\left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x+a) = b, \\ F(x) + F(x+c) = d, \\ F^{-1}(F(x)+d) + F^{-1}(F(x+a)+d) = a \end{array} \right.\right\}.$$

The UBCT, the LBCT, and the EBCT are new and have not been sufficiently studied. Our contribution in this article aligns with our previous study [14] for the classical tables in which we present a first depth-in study of general properties of the former tables and introduce a new uniformity bound for each table. We shall also investigate the behaviours of the crucial case of the inverse function and present the corresponding explicit values of their UBCT, the LBCT, and the EBCT. Below is a summary of our contribution.

- We show that the UBCT and the LBCT of a vectorial Boolean permutation F of $\mathbb{F}_{2^n}$ satisfy
$$\begin{aligned}\mathtt{UBCT}_{F^{-1}}(a,b,c) &= \mathtt{LBCT}_F(c,b,a),\\ \mathtt{LBCT}_{F^{-1}}(a,b,c) &= \mathtt{UBCT}_F(c,b,a),\end{aligned}$$
for all $a, b, c \in \mathbb{F}_{2^n}$ where F^{-1} is the compositional inverse of F. This simplifies the computation of the UBCT and the LBCT of F^{-1}, especially when F is hard to invert (since no expression of the inverse would be needed).
- We show that the values of $\mathtt{UBCT}_F(a,b,c)$ are trivial to compute when $abc = 0$. This enables us to define the nontrivial upper boomerang connectivity uniformity $\overline{\delta}_F$ of F as the maximal value of all $\mathtt{UBCT}_F(a,b,c)$ where $abc \neq 0$. Moreover, we study more properties of the UBCT, especially for power Boolean vectorial functions, and show that the nontrivial upper boomerang connectivity uniformity is invariant by affine transformations.
- Similarly, we show that the values of $\mathtt{LBCT}_F(a,b,c)$ are also trivial to compute when $abc = 0$, leading us to define the nontrivial lower boomerang connectivity uniformity $\underline{\delta}_F$ of F as the maximal value of all $\mathtt{LBCT}_F(a,b,c)$ where $abc \neq 0$. We also study more properties of the LBCT, especially for power Boolean vectorial functions, and show that the nontrivial lower boomerang connectivity uniformity is invariant by affine transformations.
- We also show the values of $\mathtt{EBCT}_F(a,b,c,d)$ are trivial if $abcd = 0$. Moreover, we study the EBCT of a power function and define the nontrivial extended boomerang connectivity uniformity $\underline{\overline{\delta}}_F$ of F as the maximal value of all $\mathtt{EBCT}_F(a,b,c,d)$ where $abcd \neq 0$. We also study the EBCT for power functions and affine equivalent permutations, showing that the nontrivial extended boomerang connectivity is the same for any two affine equivalent permutations.
- Finally, we focus on the inverse function defined over $\mathbb{F}_{2^n}$ by $F(0) = 0$, and $F(x) = \frac{1}{x}$ for $x \neq 0$. We explicitly state all the values of the UBCT, the LBCT, and the EBCT of F. This enables us to compute the nontrivial uniformities of the three tables for the inverse function.

The rest of this paper is organized as follows. Section 2 recalls some basic notions related to some ingredients and concepts, which will be used in subsequent sections. We also present some background related to codes and lattices, which will be employed in the rest of the paper. In Section 3, we review the main tables related to an S-box. Section 4 studies the links between the `UBCT` and the `LBCT` tables. In Section 5, we study the properties of the UBCT table and explicitly its values for the inverse function. In Section 6, we study the properties of the `LBCT` table and determine explicitly its values for the inverse function. Section 7 presents results similar to the `EBCT` table. We conclude the paper in Section 8 and draw new avenues for future work.

2 Preliminaries

This section recalls some terminologies and definitions. It also introduces notation and presents some background in algebra, including valuable results and connections with elements from coding and latices contexts, which will be used in subsequent sections. Throughout the paper, $\#E$ denotes the cardinality of a finite set E.

Definition 1. *Let n and d be two integers with $d < n$ and $d|n$. The trace function of an element $x \in \mathbb{F}_{2^n}$ is given by*

$$Tr_d^n(x) = x + x^{2^d} + x^{2^{2d}} + \cdots + x^{2^{n-d}}.$$

If $d = 1$, we simply set $Tr(x)$.

The following result, in connection with the solvability of a quadratic equation in $\mathbb{F}_{2^n}$, will be used in the present paper.

Lemma 1 (Proposition 1 of [24]). *Let $a, b, c \in \mathbb{F}_{2^n}$. The equation $ax^2 + bx + c = 0$ has*

(i) One root if and only if $b = 0$.
(ii) Two roots if and only if $b \neq 0$ and $Tr\left(\frac{ac}{b^2}\right) = 0$.
(iii) No root if and only if $b \neq 0$ and $Tr\left(\frac{ac}{b^2}\right) = 1$.

Several equivalence relations of vectorial Boolean functions are used to study specific properties. The following definition concerns affine equivalent functions.

Definition 2. *Two vectorial Boolean functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine equivalent if $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$.*

3 Tables for Boolean Vectorial Functions

This section reviews several tables related to S-boxes derived from Boolean vectorial functions.

3.1 The difference distribution table (DDT)

The difference distribution table is used to study the resistance of an S-box to the differential attack and their variants [2,21].

Definition 3. *For $n \geq 2$, let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a vectorial Boolean function. The difference distribution table (DDT) related to F is the $2^n \times 2^n$ table where the element at row $a \in \mathbb{F}_{2^n}$ and column $b \in \mathbb{F}_{2^n}$ is defined by*

$$\mathtt{DDT}_F(a,b) = \#\left\{x \in \mathbb{F}_{2^n} : F(x) + F(x+a) = b\right\},$$

and the differential uniformity of F is defined by

$$\delta_F = \max_{a \neq 0, b \in \mathbb{F}_{2^n}} (\mathtt{DDT}_F(a,b)).$$

Table 1 shows the DDT of the inverse function over $\mathbb{F}_{2^3}$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	0	0	2	2	2	2
3	0	2	0	2	2	0	2	0
4	0	0	2	2	0	0	2	2
5	0	2	2	0	0	2	2	0
6	0	0	2	2	2	2	0	0
7	0	2	2	0	2	0	0	2

Table 1. DDT(a,b) of the inverse function over $\mathbb{F}_{2^3}$.

The following result from [14] gives in detail the entries of the DDT of the inverse function over $\mathbb{F}_{2^n}$.

Theorem 1. *Let S be the inverse function over $\mathbb{F}_{2^n}$. We have the following possibilities for the entries of the DDT of S.*

(i) *if $a = 0$ and $b = 0$, then $\mathtt{DDT}_S(a, b) = 2^n$,*
(ii) *if $a = 0$ and $b \neq 0$, then $\mathtt{DDT}_S(a, b) = 0$,*
(iii) *if $a \neq 0$ and $b = 0$, then $\mathtt{DDT}_S(a, b) = 0$,*
(iv) *if $a \neq 0$, then*

$$\mathtt{DDT}_S\left(a, \frac{1}{a}\right) = \begin{cases} 4 & \textit{if } \mathrm{Tr}(1) = 0, \\ 2 & \textit{if } \mathrm{Tr}(1) = 1, \end{cases}$$

(v) *if $a \neq 0$, $b \neq 0$, and $ab \neq 1$, then*

$$\mathtt{DDT}_S\left(a, b\right) = \begin{cases} 2 & \textit{if } \mathrm{Tr}\left(\dfrac{1}{ab}\right) = 0, \\ 0 & \textit{if } \mathrm{Tr}\left(\dfrac{1}{ab}\right) = 1. \end{cases}$$

3.2 The boomerang connectivity table (BCT)

The boomerang connectivity table plays a central role to study the resistance of an S-box the boomerang attack [25].

Definition 4. *Let F be a permutation of $\mathbb{F}_{2^n}$. The Boomerang Connectivity Table (BCT) of F is a $2^n \times 2^n$ table where the entry at (a, b) with $a, b \in \mathbb{F}_{2^n}$ is given by*

$$\mathtt{BCT}_F(a, b) = \#\left\{x \in \mathbb{F}_{2^n} \mid F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a\right\}.$$

Moreover, the value

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}} \mathtt{BCT}_F(a,b),$$

is called the boomerang uniformity of F.

3.3 The double difference distribution table (DDDT)

The double difference distribution table is a new notion introduced in [15] to study the resistance of an S-box to some variants of the differential attack.

Definition 5. *Let F be a permutation of $\mathbb{F}_{2^n}$. The double difference distribution table (DDDT) of F is a $2^n \times 2^n \times 2^n$ table where the entry at (a,b,c) with $a,b,c \in \mathbb{F}_{2^n}$ is given by*

$$\mathtt{DDDT}_F(a,b,c) = \#\{x \in \mathbb{F}_{2^n} | F(x+a+b) + F(x+a) + F(x+b) + F(x) = c\}.$$

Moreover, the value

$$\varDelta_F = \max_{\substack{(a,b,c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \\ ab(a+b) \neq 0}} \mathtt{DDDT}_F(a,b,c).$$

is called the double differential uniformity of F.

3.4 The Upper, the Lower, and the Extended Boomerang Connectivity Tables

In 2019, Wang and Peyrin [26] introduced two new types of tables: the Boomerang Difference Table (BDT) and its variant BDT'. The two tables were then relabelled by Delaune et al. [10] as the Upper Boomerang Connectivity Table (UBCT), and the Lower Boomerang Connectivity Table (LBCT).

Definition 6. *Let F be a permutation of $\mathbb{F}_{2^n}$. The Upper Boomerang Connectivity Table (UBCT) of F is a $2^n \times 2^n \times 2^n$ table where the entry at (a,b,c) with $a,b,c \in \mathbb{F}_{2^n}$ is given by*

$$\mathtt{UBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x+a) = b, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a \end{array} \right. \right\}.$$

Definition 7. *Let F be a permutation of $\mathbb{F}_{2^n}$. The Lower Boomerang Connectivity Table (LBCT) of F is a $2^n \times 2^n \times 2^n$ table where the entry at (a,b,c) with $a,b,c \in \mathbb{F}_{2^n}$ is given by*

$$\mathtt{LBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x+b) = c, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a \end{array} \right. \right\}.$$

In addition to the UBCT and the LBCT tables, Delaune et al. [10] introduced the so-called Extended Boomerang Connectivity Table as follows.

Definition 8. *Let F be a permutation of $\mathbb{F}_{2^n}$. The Extended Boomerang Connectivity Table (EBCT) of F is a $2^n \times 2^n \times 2^n \times 2^n$ table where the entry at (a,b,c,d) with $a,b,c,d \in \mathbb{F}_{2^n}$ is given by*

$$\mathtt{EBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \;\middle|\; \begin{array}{l} F(x)+F(x+a)=b, \\ F(x)+F(x+c)=d, \\ F^{-1}(F(x)+d)+F^{-1}(F(x+a)+d)=a \end{array} \right\}.$$

4 Links between the UBCT and the LBCT

The following result presents a result relating the UBCT of a permutation and the and LBCT of its compositional inverse.

Proposition 1. *Let F be a permutation of $\mathbb{F}_{2^n}$, and F^{-1} its compositional inverse. Then the LBCT of F and the UBCT of F^{-1} satisfy*

$$\mathtt{UBCT}_{F^{-1}}(a,b,c) = \mathtt{LBCT}_F(c,b,a),$$

for all $a,b,c \in \mathbb{F}_{2^n}$.

Proof. Let $a,b,c \in \mathbb{F}_{2^n}$. Then, $\mathtt{UBCT}_{F^{-1}}(a,b,c)$ is the number of solutions of the equation system

$$\begin{cases} F^{-1}(x)+F^{-1}(x+a)=b, \\ F\left(F^{-1}(x)+c\right)+F\left(F^{-1}(x+a)+c\right)=a. \end{cases}$$

If we set $F^{-1}(x)=y$, then the system is equivalent to

$$\begin{cases} y+F^{-1}(F(y)+a)=b, \\ F\left(y+c\right)+F\left(F^{-1}(F(y)+a)+c\right)=a. \end{cases}$$

The first equation of the system gives $F^{-1}(F(y)+a)=y+b$, and consequently

$$F(y)+F(y+b)=a.$$

The second equation of the system gives $F\left(F^{-1}(F(y)+a)+c\right)=F\left(y+c\right)+a$, and $F^{-1}(F(y)+a)+c=F^{-1}(F\left(y+c\right)+a)$. This implies that

$$F^{-1}(F(y)+a)+F^{-1}(F\left(y+c\right)+a)=c.$$

As a consequence, the original system is equivalent to

$$\begin{cases} F(y)+F(y+b)=a, \\ F^{-1}(F(y)+a)+F^{-1}(F\left(y+c\right)+a)=c, \end{cases}$$

which is related the LBCT of F. This implies that

$$\mathtt{UBCT}_{F^{-1}}(a,b,c) = \mathtt{LBCT}_F(c,b,a).$$

This completes the proof. □

We have the following result as a consequence of Proposition 1.

Proposition 2. *Let F be a permutation of $\mathbb{F}_{2^n}$, and F^{-1} its compositional inverse. Then the UBCT of F and the LBCT of F^{-1} satisfy*

$$\mathtt{LBCT}_{F^{-1}}(a,b,c)=\mathtt{UBCT}_F(c,b,a),$$

for all $a,b,c\in\mathbb{F}_{2^n}$.

Proof. Applying Proposition 1 with F^{-1} gives

$$\mathtt{UBCT}_F(a,b,c)=\mathtt{LBCT}_{F^{-1}}(c,b,a).$$

Rearranging, we get

$$\mathtt{LBCT}_{F^{-1}}(a,b,c)=\mathtt{UBCT}_F(c,b,a).$$

□

We can use Proposition 1 to redefine the UBCT of a permutation F of $\mathbb{F}_{2^n}$ without using its compositional inverse.

Theorem 2. *Let F be a permutation of $\mathbb{F}_{2^n}$. Then*

$$\mathtt{UBCT}_F(a,b,c)=\#\left\{(x,z)\in\mathbb{F}_{2^n}^2\ \middle|\ \begin{array}{l}F(x)+F(x+a)=b,\\ F(x)+F(z)=c,\\ F\left(x+a\right)+F\left(z+a\right)=c\end{array}\right\}.$$

Proof. Using Proposition 1, we have

$$\mathtt{UBCT}_F(a,b,c)=\mathtt{LBCT}_{F^{-1}}(c,b,a).$$

This is the number of solutions of the equation system

$$\begin{cases}F^{-1}(X)+F^{-1}(X+b)=a,\\ F\left(F^{-1}(X)+a\right)+F\left(F^{-1}(X+c)+a\right)=c.\end{cases}$$

Let $x=F^{-1}(X)$, $y=F^{-1}(X+b)$, and $z=F^{-1}(X+c)$. Then, the former system is equivalent to

$$\begin{cases}x+y=a,\\ F(x)+F(y)=b,\\ F(x)+F(z)=c,\\ F\left(x+a\right)+F\left(z+a\right)=c,\end{cases}$$

which can be simplified to

$$\begin{cases}F(x)+F(x+a)=b,\\ F(x)+F(z)=c,\\ F\left(x+a\right)+F\left(z+a\right)=c.\end{cases}$$

This completes the proof. □

We also can use Proposition 1 to redefine the LBCT of a permutation F of $\mathbb{F}_{2^n}$ without using its compositional inverse.

Theorem 3. *Let F be a permutation of $\mathbb{F}_{2^n}$. Then*

$$\mathtt{LBCT}_F(a,b,c) = \# \left\{ (x,y) \in \mathbb{F}_{2^n}^2 \;\middle|\; \begin{array}{l} x+y=b, \\ F\left(x+c\right)+F\left(y+c\right)=a \end{array} \right\}.$$

Proof. Using Proposition 1, we use

$$\mathtt{LBCT}_F(a,b,c) = \mathtt{UBCT}_{F^{-1}}(c,b,a),$$

which is the number of solutions of the equation system

$$\begin{cases} F^{-1}(X)+F^{-1}(X+a)=b, \\ F\left(F^{-1}(X)+c\right)+F\left(F^{-1}(X+a)+c\right)=a. \end{cases}$$

Let $x=F^{-1}(X)$, and $y=F^{-1}(X+a)$. Then, the former system is equivalent to

$$\begin{cases} x+y=b, \\ F\left(x+c\right)+F\left(y+c\right)=a. \end{cases}$$

This completes the proof. □

5 The Upper Boomerang Connectivity Table (UBCT)

In this section, we study the properties of the UBCT and compute its entries for the inverse function.

5.1 Properties of the UBCT

The following result is valid for all permutations of $\mathbb{F}_{2^n}$, and is valid when $abc=0$.

Proposition 3. *For $a,b,c \in \mathbb{F}_{2^n}$ with $abc=0$, we have*

$$\mathtt{UBCT}_F(a,b,c) = \begin{cases} 2^n & \text{if } a=b=0, \\ 0 & \text{if } a=0,\ b\neq 0,\ c\neq 0, \\ \mathtt{DDT}_F(a,b) & \text{if } c=0, \\ 0 & \text{if } a\neq 0,\ b=0,\ c\neq 0. \end{cases}$$

Proof. For $a,b,c \in \mathbb{F}_{2^n}$, consider the equations

$$F(x)+F(x+a)=b, \tag{1}$$

and

$$F^{-1}(F(x)+c)+F^{-1}(F(x+a)+c)=a, \tag{2}$$

Case 1: Suppose that $a = 0$. Then (1) implies that $b = 0$.
Case 1.1: Suppose that $b = 0$. Then (1) is verified for all $x \in \mathbb{F}_{2^n}$. Moreover, (2) gives

$$F^{-1}(F(x) + c) + F^{-1}(F(x) + c) = 0,$$

which is also verified for all $x \in \mathbb{F}_{2^n}$. Then

$$\mathtt{UBCT}_F(0, 0, c) = 2^n.$$

Case 1.2: Suppose that $b \neq 0$. Then

$$\mathtt{UBCT}_F(0, b, c) = 0.$$

In the next cases, we suppose that $a \neq 0$.
Case 2: Suppose that $c = 0$. Then (2) gives

$$F^{-1}(F(x)) + F^{-1}(F(x + a)) = x + x + a = a,$$

which is verified for all $x \in \mathbb{F}_{2^n}$. Then $\mathtt{UBCT}_F(a, b, 0)$ depends only on the equation (1). Hence

$$\mathtt{UBCT}_F(a, b, 0) = DDT(a, b).$$

In the next cases, we suppose that $a \neq 0$ and $c \neq 0$.
Case 3: Suppose that $b = 0$. Then (1) implies that $F(x) + F(x + a) = 0$, that is $x = x + a$ which is not possible. Hence, for all $a \neq 0$ and $c \neq 0$,

$$\mathtt{UBCT}_F(a, 0, c) = 0.$$

In the next cases, we suppose that $a \neq 0$, $b \neq 0$, and $c \neq 0$. □

Observe that Proposition 3 deals with situation $abc = 0$, and the results seem obvious. This allows us to propose a new kind of uniformity for the UBCT.

Definition 9. *Let F be a permutation of $\mathbb{F}_{2^n}$. The nontrivial upper boomerang connectivity uniformity $\overline{\delta}_F$ of F is the maximal value of all $\mathtt{UBCT}_F(a, b, c)$ where $abc \neq 0$, that is*

$$\overline{\delta}_F = \max_{a,b,c \in \mathbb{F}_{2^n}, abc \neq 0} \mathtt{UBCT}_F(a, b, c).$$

The following result concerns the nontrivial upper boomerang connectivity uniformity of power functions.

Proposition 4. *Let d be an integer such that $\gcd(d, 2^n - 1) = 1$. Let F be a power function defined over $\mathbb{F}_{2^n}$ by $F(x) = x^d$. The nontrivial upper boomerang connectivity uniformity of F satisfies*

$$\overline{\delta}_F = \max_{b,c \in \mathbb{F}_{2^n}, bc \neq 0} \mathtt{UBCT}_F(1, b, c).$$

Proof. Let $a \in \mathbb{F}_{2^n}$ with $a \neq 0$. The equation $F(x) + F(x + a) = b$ can be rewritten as $x^d + (x + a)^d = b$, and equivalently

$$y^d + (y + 1)^d = \frac{b}{a^d},$$

where $y = \frac{x}{a}$. Similarly, the equation $F^{-1}(F(x) + c) + F^{-1}(F(x + a) + c) = a$ can be rewritten as

$$\left(x^d + c\right)^{-d} + \left((x + a)^d + c\right)^{-d} = a.$$

This can be simplified to

$$\left(y^d + \frac{c}{a^d}\right)^{-d} + \left((y + 1)^d + \frac{c}{a^d}\right)^{-d} = 1,$$

where $y = \frac{x}{a}$. Since F is a permutation, this implies that

$$\overline{\delta}_F = \max_{b',c' \in \mathbb{F}_{2^n}, b'c' \neq 0} \mathtt{UBCT}_F(1, b', c'),$$

and terminates the proof. □

The following result gives a relation between the UBCT tables of two affine equivalent functions.

Proposition 5. *Let F and G be two affine equivalent permutations of $\mathbb{F}_{2^n}$ such that $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$. Then*

$$\mathtt{UBCT}_G(a, b, c) = \mathtt{UBCT}_F(A_1(a), A_2^{-1}(b), A_2^{-1}(c)).$$

Proof. Let $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$. Then $\mathtt{UBCT}_G(a, b, c)$ is the number of the solutions $x \in \mathbb{F}_{2^n}$ satisfying the system of equations

$$\begin{cases} G(x) + G\left(x + a\right) = b, \\ G^{-1}(G(x) + c) + G^{-1}\left(G(x + a) + c\right) = a. \end{cases}$$

The first equation is equivalent to

$$A_2\left(F(A_1(x)) + F(A_1(x) + A_1(a))\right) = b,$$

and $F(A_1(x)) + F(A_1(x) + A_1(a)) = A_2^{-1}(b)$.
The second equation is equivalent to

$$\begin{aligned} &A_1^{-1} \circ F^{-1} \circ A_2^{-1}\left(A_2 \circ F \circ A_1(x) + c\right) \\ &+ A_1^{-1} \circ F^{-1} \circ A_2^{-1}\left(A_2 \circ F \circ A_1\left(x + a\right) + c\right) = a. \end{aligned}$$

This can be simplified to

$$A_1^{-1} \circ F^{-1}\left(F \circ A_1(x) + A_2^{-1}(c)\right) + A_1^{-1} \circ F^{-1}\left(F \circ A_1\left(x + a\right) + A_2^{-1}(c)\right) = a,$$

and then to

$$A_1^{-1} \circ F^{-1}\left(F(A_1(x)) + A_2^{-1}(c)\right) + A_1^{-1} \circ F^{-1}\left(F\left(A_1(x) + A_1(a)\right) + A_2^{-1}(c)\right) = a.$$

This gives

$$F^{-1}\left(F(A_1(x)) + A_2^{-1}(c)\right) + F^{-1}\left(F\left(A_1(x) + A_1(a)\right) + A_2^{-1}(c)\right) = A_1(a).$$

By setting $A_1(x) = x'$, and since A_1 is a permutation, then x' is a solution of the system

$$\begin{cases} F(x') + F\left(x' + A_1(a)\right) = A_2^{-1}(b), \\ F^{-1}(F(x') + A_2^{-1}(c)) + F^{-1}\left(F(x' + A_1(a)) + A_2^{-1}(c)\right) = A_1(a). \end{cases}$$

This implies that

$$\texttt{UBCT}_G(a, b, c) = \texttt{UBCT}_F(A_1(a), A_2^{-1}(b), A_2^{-1}(c)).$$

and terminates the proof. □

Proposition 5 implies that the nontrivial upper boomerang connectivity uniformity is invariant by affine equivalent transformations.

5.2 The UBCT of the Inverse Function

In this section, we study the UBCT table of the inverse function F defined over $\mathbb{F}_{2^n}$ by $F(0) = 0$ and $F(x) = \frac{1}{x}$ for $x \neq 0$. The following result complements Proposition 3.

Theorem 4. *For $a, b, c \in \mathbb{F}_{2^n}$ with $abc \neq 0$, we have*

$$\texttt{UBCT}_F(a, b, c) = \begin{cases} 4 & \text{if } (a, b, c) \in \mathcal{I}_1 \cup \mathcal{I}_2, \\ 2 & \text{if } (a, b, c) \in \mathcal{I}_3 \cup \mathcal{I}_4, \\ 0 & \text{if } (a, b, c) \notin \mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3 \cup \mathcal{I}_4, \end{cases}$$

where

$$\mathcal{I}_1 = \left\{(a, b, c) : b = c = \frac{1}{a}, Tr(1) = 0\right\},$$
$$\mathcal{I}_2 = \left\{(a, b, c) : b = \frac{1}{a}, (ac)^2 + ac + 1 = 0\right\},$$
$$\mathcal{I}_3 = \left\{(a, b, c) : a = b = c, a \neq 1, Tr\left(\frac{1}{a}\right) = 0\right\},$$
$$\mathcal{I}_4 = \left\{(a, b, c) : b = c, a \neq c, b \neq \frac{1}{a}, Tr\left(\frac{1}{ab}\right) = 0\right\}.$$

Proof. For $a, b, c \in \mathbb{F}_{2^n}$ with $abc \neq 0$, consider the equations

$$F(x) + F(x+a) = b, \tag{3}$$

and

$$F^{-1}(F(x) + c) + F^{-1}(F(x+a) + c) = a, \tag{4}$$

Case 1: Suppose that $x = 0$ is a solution of (3) and (4). Then (3) gives $F(a) = b$, that is $ab = 1$, and (4) gives

$$F^{-1}(F(x) + c) + F^{-1}(F(x+a) + c) = F^{-1}(c) + F^{-1}(F(a) + c).$$

If $F(a) = c$, that is $ac = 1$, then $F^{-1}(c) = a$ is satisfied. If $F(a) \neq c$, then

$$F^{-1}(c) + F^{-1}(F(a) + c) = \frac{1}{c(ac+1)}.$$

Hence, if $\frac{1}{c(ac+1)} = a$, that is $(ac)^2 + ac + 1 = 0$, $x = 0$ is a solution of both (3) and (4).

It follows that $x = 0$ is a solution of (3) and (4) if and only if $b = c = \frac{1}{a}$ or if $b = \frac{1}{a}$, and $(ac)^2 + ac + 1 = 0$.

Case 2: Suppose that $x = a$ is a solution of (3) and (4). Then $F(a) = b$, that is $ab = 1$, and

$$F^{-1}(F(x) + c) + F^{-1}(F(x+a) + c) = F^{-1}(F(a) + c) + F^{-1}(c).$$

If $F(a) = c$, that is $ac = 1$, then $F^{-1}(c) = a$ is satisfied. If $F(a) \neq c$, then

$$F^{-1}(F(a) + c) + F^{-1}(c) = \frac{1}{c(ac+1)}.$$

Hence, if $\frac{1}{c(ac+1)} = a$, that is $(ac)^2 + ac + 1 = 0$, $x = a$ is a solution of both (3) and (4).

It follows that $x = a$ is a solution of (3) and (4) if and only if $b = c = \frac{1}{a}$ or if $b = \frac{1}{a}$, and $(ac)^2 + ac + 1 = 0$.

Case 3: Suppose that $x = \frac{1}{c}$ is a solution of (3) and (4). Then (3) gives

$$c + F\left(\frac{1}{c} + a\right) = b.$$

Case 3.1: If $ac = 1$, then $c = b$. Also, (4) gives

$$F^{-1}\left(F\left(\frac{1}{c} + a\right) + c\right) = a,$$

which is satisfied.

Case 3.2: If $ac \neq 1$, then (3) gives

$$c + F\left(\frac{1}{c} + a\right) = \frac{1}{c(ac+1)} = b.$$

Also, (4) gives

$$\frac{ac+1}{ac^2} = a.$$

that is $(ac)^2 + ac + 1 = 0$.
It follows that $x = \frac{1}{c}$ is a solution of (3) and (4) if and only if $b = c = \frac{1}{a}$ or if $b = \frac{1}{c(ac+1)}$, and $(ac)^2 + ac + 1 = 0$.
Case 4: Suppose that $x = a + \frac{1}{c}$ is a solution of (3) and (4) with $ac \neq 1$ so that $x \neq 0$. Then (3) gives

$$\frac{ac^2}{ac+1} = b.$$

Also, in (4), we have $F(x+a) + c = 0$, and $F^{-1}(F(x) + c) = a$, that is

$$F^{-1}\left(F\left(a + \frac{1}{c}\right) + c\right) = a.$$

Since $ac \neq 1$, then

$$\frac{ac+1}{ac^2} = a,$$

and $(ac)^2 + ac + 1 = 0$. This gives

$$b = \frac{ac^2}{ac+1} = \frac{ac^2}{(ac)^2} = \frac{1}{a}.$$

It follows that $x = a + \frac{1}{c}$ is a solution of (3) and (4) if and only if $b = \frac{1}{a}$, and $(ac)^2 + ac + 1 = 0$.
Case 5: Suppose that $x \neq 0$, $x \neq a$, $x \neq \frac{1}{c}$, $x \neq \frac{1}{c} + a$. Then the equations (3) and (4) can be simplified to the system

$$\begin{cases} bx^2 + abx + a = 0, \\ cx^2 + acx + a = 0. \end{cases}$$

Case 5.1: If $a = c$, then the system is

$$\begin{cases} bx^2 + abx + a = 0, \\ x^2 + ax + 1 \quad = 0. \end{cases}$$

Combining both equations, we get $a = b$. This leads to the unique equation $x^2 + ax + 1 = 0$, which has no solution if $\mathrm{Tr}\left(\frac{1}{a}\right) = 1$, and two solutions if $\mathrm{Tr}\left(\frac{1}{a}\right) = 0$.
Case 5.2: If $a \neq c$, and $b = c$, then the original system gives the unique equation $bx^2+abx+a = 0$. This equation has no solution if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 1$, and two solutions if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$.
Case 5.3: If $a \neq c$, $b \neq c$, then the original system leads to

$$\begin{cases} bcx^2 + abcx + ac = 0, \\ bcx^2 + abcx + ab = 0. \end{cases}$$

Combining the two equations, we get $a(b+c) = 0$ which is impossible.

The former cases can be summarized to find $\mathtt{UBCT}_F(a,b,c)$.

1. If $b = c = a = 1$, and $\mathrm{Tr}\,(1) = 0$, then $\mathtt{UBCT}_F(a,b,c) = 4$. This is true by Case 1, Case 2, and Case 5.1.
2. If $b = c = \frac{1}{a}$, $a \neq 1$, and $\mathrm{Tr}\,(1) = 0$, then $\mathtt{UBCT}_F(a,b,c) = 4$. This is true by Case 1, Case 2, and Case 5.2.
3. If $b = \frac{1}{a}$ and $(ac)^2 + ac + 1 = 0$, then $\mathtt{UBCT}_F(a,b,c) = 4$. This is true by Case 1, Case 2, Case 3, and Case 4.
4. If $a = b = c$, $a \neq 1$, and $\mathrm{Tr}\left(\frac{1}{a}\right) = 0$, then $\mathtt{UBCT}_F(a,b,c) = 2$. This is true by Case 5.1.
5. If $b = c$, $a \neq c$, $b \neq \frac{1}{a}$, and $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, then $\mathtt{UBCT}_F(a,b,c) = 2$. This is true by Case 5.2.
6. In all other cases, $\mathtt{UBCT}_F(a,b,c) = 0$.

This completes the proof. □

Given Proposition 3 and Theorem 4, the following lemma is obvious. It concerns the nontrivial uniformity of the inverse function.

Lemma 2. *For the inverse permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the nontrivial uniformity $\overline{\delta}_F$ of the UBCT is*

$$\overline{\delta}_F = \begin{cases} 4 & \text{if } n \text{ is even,} \\ 2 & \text{if } n \text{ is odd.} \end{cases}$$

In Appendix A, we present the UBCT of the inverse function over $\mathbb{F}_{2^3}$.

6 The Lower Boomerang Connectivity Table (LBCT)

In this section, we study the properties of the LBCT, and give explicit values of its entries for the inverse function.

6.1 Properties of the LBCT

The following result is valid for all permutations of $\mathbb{F}_{2^n}$, and $abc = 0$. Recall that

$$\mathtt{LBCT}_F(a,b,c) = \#\left\{ x \in \mathbb{F}_{2^n} \;\middle|\; \begin{array}{l} F(x) + F(x+b) = c, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a \end{array} \right\}.$$

Proposition 6. *For $a, b, c \in \mathbb{F}_{2^n}$ with $abc = 0$, we have*

$$\mathtt{LBCT}_F(a,b,c) = \begin{cases} 2^n & \text{if } b = c = 0, \\ 0 & \text{if } b = 0,\ c \neq 0, \\ 0 & \text{if } b \neq 0,\ c = 0, \\ \mathtt{DDT}_F(b,c) & \text{if } a = 0. \end{cases}$$

Proof. For $a, b, c \in \mathbb{F}_{2^n}$, consider the equations

$$F(x) + F(x+b) = c, \tag{5}$$

and

$$F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a, \tag{6}$$

Case 1: Suppose that $b = 0$. Then (5) implies that $c = 0$.
Case 1.1: Suppose that $c = 0$. Then (5) is verified for all $x \in \mathbb{F}_{2^n}$. Moreover, (6) gives

$$F^{-1}(F(x)) + F^{-1}(F(x+a)) = x + x + a = a,$$

which is also verified for all $x \in \mathbb{F}_{2^n}$. Then

$$\texttt{LBCT}_F(a, 0, 0) = 2^n.$$

Case 1.2: Suppose that $c \neq 0$. Then

$$\texttt{UBCT}_F(a, 0, c) = 0.$$

In the next cases, we suppose that $b \neq 0$.
Case 2: Suppose that $c = 0$. Then (5) gives $F(x) + F(x+b) = 0$, and $b = 0$ which is not possible.

$$\texttt{LBCT}_F(a, b, 0) = 0.$$

In the next cases, we suppose that $b \neq 0$ and $c \neq 0$.
Case 3: Suppose that $a = 0$. Then (6) implies that

$$F^{-1}(F(x)+c) + F^{-1}(F(x)+c) = 0,$$

which is always satisfied. Hence, (5) implies that

$$\texttt{LBCT}_F(0, b, c) = DDT(b, c).$$

This proves the claim. □

Since Proposition 6 concerns the situation $abc = 0$, we propose a new uniformity concept for the EBCT.

Definition 10. *Let F be a permutation of $\mathbb{F}_{2^n}$. The nontrivial lower uniformity $\underline{\delta}_F$ of the LBCT is the maximal value of all $\texttt{LBCT}_F(a, b, c)$ where $abc \neq 0$, that is*

$$\underline{\delta}_F = \max_{a,b,c \in \mathbb{F}_{2^n}, abc \neq 0} \texttt{LBCT}_F(a, b, c).$$

The following result simplifies the nontrivial lower boomerang connectivity uniformity of power functions.

Proposition 7. *Let d be an integer such that $\gcd(d, 2^n - 1) = 1$. Let F be a power function defined over $\mathbb{F}_{2^n}$ by $F(x) = x^d$. The nontrivial lower boomerang connectivity uniformity of F satisfies*

$$\underline{\delta}_F = \max_{a,c \in \mathbb{F}_{2^n}, ac \neq 0} \texttt{LBCT}_F(a, 1, c).$$

Proof. Let $a, b, c \in \mathbb{F}_{2^n}$ with $abc \neq 0$, and $F(x) = x^d$. The system of equations

$$\begin{cases} F(x) + F(x+b) = c, \\ F^{-1}(F(x)+c) + F^{-1}(F(x+a)+c) = a, \end{cases}$$

can be rewritten as

$$\begin{cases} x^d + (x+b)^d = c, \\ \left(x^d + c\right)^{-d} + \left((x+a)^d + c\right)^{-d} = a. \end{cases}$$

Set $x = by$. Then, the former system gives

$$\begin{cases} b^d y^d + b^d (y+1)^d = c, \\ \left(b^d y^d + c\right)^{-d} + \left((by+a)^d + c\right)^{-d} = a. \end{cases}$$

This equivalent to

$$\begin{cases} y^d + (y+1)^d = \frac{c}{b^d}, \\ \left(y^d + \frac{c}{b^d}\right)^{-d} + \left((y + \frac{a}{b})^d + \frac{c}{b^d}\right)^{-d} = \frac{a}{b}. \end{cases}$$

Hence

$$\underline{\delta}_F = \max_{a,c \in \mathbb{F}_{2^n}, ac \neq 0} \mathtt{UBCT}_F(a, 1, c).$$

This completes the proof. □

The LBCT tables of two affine equivalent functions is presented in the following result.

Proposition 8. *Let F and G be two affine equivalent permutations of $\mathbb{F}_{2^n}$ such that $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$. Then*

$$\mathtt{LBCT}_G(a, b, c) = \mathtt{UBCT}_F\left(A_1(a), A_1(b), A_2^{-1}(c)\right).$$

Proof. Let $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$. The value $\mathtt{LBCT}_G(a, b, c)$ is the number of the solutions $x \in \mathbb{F}_{2^n}$ satisfying the system of equations

$$\begin{cases} G(x) + G\left(x+b\right) = c, \\ G^{-1}(G(x)+c) + G^{-1}\left(G(x+a)+c\right) = a. \end{cases}$$

The first equation can be transformed to

$$A_2\left(F(A_1(x)) + F(A_1(x) + A_1(b))\right) = c,$$

which is equivalent to $F(A_1(x)) + F(A_1(x) + A_1(b)) = A_2^{-1}(c)$.
As in the proof of Proposition 5, the second equation is equivalent to

$$F^{-1}\left(F(A_1(x)) + A_2^{-1}(c)\right) + F^{-1}\left(F\left(A_1(x) + A_1(a)\right) + A_2^{-1}(c)\right) = A_1(a).$$

By setting $A_1(x) = x'$, and since A_1 is a permutation, then x' is a solution of the system

$$\begin{cases} F(x') + F(x' + A_1(b)) = A_2^{-1}(c), \\ F^{-1}\left(F(x') + A_2^{-1}(c)\right) + F^{-1}\left(F\left(x' + A_1(a)\right) + A_2^{-1}(c)\right) = A_1(a). \end{cases}$$

This implies that

$$\mathtt{LBCT}_G(a,b,c) = \mathtt{UBCT}_F\left(A_1(a), A_1(b), A_2^{-1}(c)\right).$$

and terminates the proof. □

Proposition 5 implies that the nontrivial lower boomerang connectivity uniformity is invariant under affine transformations.

6.2 The LBCT of the Inverse Function

In this subsection, we study the LBCT of the inverse function F defined over $\mathbb{F}_{2^n}$. The following result is a continuation of Proposition 6.

Theorem 5. *For $a, b, c \in \mathbb{F}_{2^n}$ with $abc \neq 0$, we have*

$$\mathtt{LBCT}_F(a,b,c) = \begin{cases} 4 & \textit{if } (a,b,c) \in \mathcal{I'}_1 \cup \mathcal{I'}_2, \\ 2 & \textit{if } (a,b,c) \in \mathcal{I'}_3, \\ 0 & \textit{if } (a,b,c) \notin \mathcal{I}_1 \cup \mathcal{I'}_2 \cup \mathcal{I'}_3, \end{cases}$$

where

$$\mathcal{I'}_1 = \left\{(a,b,c) : a = b = \frac{1}{c},\ Tr(1) = 0\right\},$$
$$\mathcal{I'}_2 = \left\{(a,b,c) : b = \frac{1}{c},\ (ac)^2 + ac + 1 = 0\right\},$$
$$\mathcal{I'}_3 = \left\{(a,b,c) : a = b \neq \frac{1}{c},\ Tr\left(\frac{1}{ac}\right) = 0\right\}.$$

Proof. For $a, b, c \in \mathbb{F}_{2^n}$ with $abc \neq 0$, consider the equations

$$F(x) + F(x+b) = c, \tag{7}$$

and

$$F^{-1}(F(x) + c) + F^{-1}(F(x+a) + c) = a, \tag{8}$$

Case 1: Suppose that $x = 0$ is a solution of (7) and (8). Then (3) implies that $F(b) = c$, and $bc = 1$. Also, (8) gives

$$F^{-1}(c) + F^{-1}(F(a) + c) = a.$$

If $F(a) = c$, that is $ac = 1$, then $F^{-1}(c) = a$ is satisfied. If $F(a) \neq c$, then

$$F^{-1}(c) + F^{-1}(F(a) + c) = \frac{1}{c(ac+1)}.$$

Hence, if $\frac{1}{c(ac+1)} = a$, that is $(ac)^2 + ac + 1 = 0$, $x = 0$ is a solution of both (7) and (8).
It follows that $x = 0$ is a solution of (7) and (8) if and only if $a = b = \frac{1}{c}$ or if $b = \frac{1}{c}$, and $(ac)^2 + ac + 1 = 0$.
Case 2: Suppose that $x = b$ is a solution of (7) and (8). Then (7) implies $F(b) = c$, that is $bc = 1$, and (8) implies that

$$F^{-1}(F(b) + c) + F^{-1}(F(b + a) + c) = F^{-1}(F(b + a) + c) = a.$$

Case 2.1: Suppose that $F(b + a) = c$. Then $0 = a$, which is not possible.
Case 2.2: Suppose that $F(b + a) \neq c$. Then, since $bc = 1$, we get

$$F^{-1}(F(b + a) + c) = \frac{b + a}{ca} = a,$$

and $(ac)^2 + ac + 1 = 0$.
It follows that $x = b$ is a solution of (7) and (8) if and only if $b = \frac{1}{c}$, and $(ac)^2 + ac + 1 = 0$.
Case 3: Suppose that $x = \frac{1}{c}$ is a solution of (7) and (8). Then (7) gives

$$c + F\left(\frac{1}{c} + b\right) = c.$$

Case 3.1: If $bc \neq 1$, this is not possible.
Case 3.2: If $bc = 1$, then (7) holds, and (8) gives

$$F^{-1}\left(F\left(\frac{1}{c} + a\right) + c\right) = a,$$

and $F\left(\frac{1}{c} + a\right) + c = F(a) = \frac{1}{a}$.
Case 3.2.1: If $ac = 1$, then this is satisfied.
Case 3.2.2: If $ac \neq 1$, then $F\left(\frac{1}{c} + a\right) + c = \frac{1}{a}$ implies that $(ac)^2 + ac + 1 = 0$.
It follows that $x = \frac{1}{c}$ is a solution of (7) and (8) if and only if $a = b = \frac{1}{c}$, or if $b = \frac{1}{c}$ and $(ac)^2 + ac + 1 = 0$.
Case 4: Suppose that $x = a + \frac{1}{c}$ is a solution of (7) and (8) with $ac \neq 1$ so that $x \neq 0$. Then (8) gives

$$F\left(a + \frac{1}{c}\right) + c = F(a) = \frac{1}{a},$$

and $(ac)^2 + ac + 1 = 0$. Also, (7) gives

$$F\left(a + \frac{1}{c}\right) + F\left(a + \frac{1}{c} + b\right) = c.$$

This is valid if $b = \frac{1}{c}$.
It follows that $x = a + \frac{1}{c}$ is a solution of (7) and (8) if and only if $b = \frac{1}{c}$, and $(ac)^2 + ac + 1 = 0$.
Case 5: Suppose that $x \neq 0$, $x \neq b$, $x \neq \frac{1}{c}$, $x \neq \frac{1}{c} + a$. Then the equations (7) and (8) can be simplified to the system

$$\begin{cases} cx^2 + bcx + b &= 0, \\ cx^2 + acx + a &= 0. \end{cases}$$

Case 5.1: If $a = b$, then the system reduces to $cx^2 + acx + a = 0$. This equation has two solutions of $\mathrm{Tr}\left(\frac{1}{ac}\right) = 0$, and no solution if $\mathrm{Tr}\left(\frac{1}{ac}\right) = 1$. Moreover, when $\mathrm{Tr}\left(\frac{1}{ac}\right) = 0$, one can easily check that 0, b, $\frac{1}{c}$, $\frac{1}{c} + a$ do not satisfy the equation $cx^2 + acx + a = 0$.
Case 5.2: If $a \neq b$, then subtracting the equation in the system, we get

$$(a + b)(cx + 1) = 0,$$

which is impossible since $a \neq b$ and $x \neq \frac{1}{c}$.
The former cases can be summarized to find $\texttt{LBCT}_F(a, b, c)$.

1. If $b = c = a = 1$, and $\mathrm{Tr}(1) = 0$, then $\texttt{LBCT}_F(a, b, c) = 4$. This is true by Case 1, Case 3, and Case 5.1.
2. If $a = b = \frac{1}{c}$, $c \neq 1$, and $\mathrm{Tr}(1) = 0$, then $\texttt{LBCT}_F(a, b, c) = 4$. This is true by Case 1, Case 3, and Case 5.1.
3. If $b = \frac{1}{c}$ and $(ac)^2 + ac + 1 = 0$, then $\texttt{LBCT}_F(a, b, c) = 4$. This is true by Case 1, Case 2, Case 3, and Case 4.
4. If $a = b \neq \frac{1}{c}$, and $\mathrm{Tr}\left(\frac{1}{ac}\right) = 0$, then $\texttt{LBCT}_F(a, b, c) = 2$. This is true by Case 1, Case 3, 5.1.
5. In all other cases, $\texttt{LBCT}_F(a, b, c) = 0$.

This completes the proof. □

By Proposition 6 and Theorem 5, the following lemma gives the nontrivial uniformity of the inverse function.

Lemma 3. *For the inverse permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the nontrivial uniformity $\overline{\delta}_F$ of the LBCT is*

$$\underline{\delta}_F = \begin{cases} 4 & \textit{if } n \textit{ is even}, \\ 2 & \textit{if } n \textit{ is odd}. \end{cases}$$

7 The Extended Boomerang Connectivity Table (EBCT)

In this section, we study some properties of the EBCT, and give all its entries for the inverse function.

7.1 Properties of the EBCT

The following result is valid for all permutations of $\mathbb{F}_{2^n}$, and $abcd = 0$. We recall that

$$\mathtt{EBCT}_F(a, b, c, d) = \# \left\{ x \in \mathbb{F}_{2^n} \left| \begin{array}{l} F(x) + F(x + a) = b, \\ F(x) + F(x + c) = d, \\ F^{-1}(F(x) + d) + F^{-1}(F(x + a) + d) = a \end{array} \right. \right\}.$$

Proposition 9. *For $a, b, c \in \mathbb{F}_{2^n}$ with $abcd = 0$, we have*

$$\mathtt{EBCT}_F(a, b, c, d) = \begin{cases} 2^n & \text{if } a = b = c = d = 0, \\ \mathtt{DDT}_F(c, d) & \text{if } a = b = 0,\ c \neq 0,\ d \neq 0, \\ \mathtt{DDT}_F(a, b) & \text{if } a \neq 0,\ b \neq 0,\ c = d = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Consider the equations

$$F(x) + F(x + a) = b, \tag{9}$$

$$F(x) + F(x + c) = d, \tag{10}$$

and

$$F^{-1}(F(x) + d) + F^{-1}(F(x + a) + d) = a. \tag{11}$$

Case 1. Suppose that $a = 0$. Then (9) gives $0 = b$.
Case 1.1. If $b \neq 0$, then

$$\mathtt{EBCT}_F(0, b, c, d) = 0.$$

Case 1.2. If $b = 0$, then (9) is satisfied. Also, (11) is satisfied. Hence, (11) represents the $\mathtt{DDT}_F(c, d)$, and

$$\mathtt{EBCT}_F(0, 0, c, d) = \mathtt{DDT}_F(c, d).$$

In the next cases, we assume that $a \neq 0$.
Case 2. Suppose that $b = 0$. Then (9) gives $F(x) + F(x + a)$, that is $x = x + a$ and $a = 0$. This is not possible. Hence, for $a \neq 0$, we get

$$\mathtt{EBCT}_F(a, 0, c, d) = 0.$$

In the next cases, we assume that $ab \neq 0$.
Case 3. Suppose that $c = 0$. Then (10) implies that $d = 0$.
Case 3.1. If $d \neq 0$, then

$$\mathtt{LBCT}_F(a, b, 0, d) = 0.$$

Case 3.2. If $d = 0$, then (10) is satisfied. Also, (11) implies that

$$F^{-1}(F(x)) + F^{-1}(F(x + a)) = a,$$

and $F(x+a) = F(x+a)$. Hence (11) is satisfied. Finally, we get

$$\texttt{EBCT}_F(a,b,0,0) = \texttt{DDT}_F(a,b).$$

In the next cases, we assume that $abc \neq 0$.
Case 4. Suppose that $d = 0$. Then (10) implies that $F(x) = F(x+c)$, and $x = x + c$, which is impossible since $c \neq 0$. Hence, for $abc \neq 0$, we get

$$\texttt{EBCT}_F(a,b,c,0) = 0.$$

This completes the proof. □

Proposition 9 gives the values of $\texttt{EBCT}_F(a,b,c,d)$ when $abcd = 0$. This motivates us to propose the following notion.

Definition 11. *Let F be a permutation of $\mathbb{F}_{2^n}$. The nontrivial extended boomerang connectivity uniformity $\overline{\underline{\delta}}_F$ of F is the maximal value of all $\texttt{EBCT}_F(a,b,c,d)$ where $abcd \neq 0$, that is*

$$\overline{\underline{\delta}}_F = \max_{a,b,c,d\in\mathbb{F}_{2^n}, abcd\neq 0} \texttt{EBCT}_F(a,b,c,d).$$

The following result concerns the nontrivial extended boomerang connectivity uniformity of power functions.

Proposition 10. *Let r be an integer such that $\gcd(r, 2^n-1) = 1$. Let F be a power function defined over $\mathbb{F}_{2^n}$ by $F(x) = x^r$. The nontrivial extended boomerang connectivity uniformity of F satisfies*

$$\overline{\underline{\delta}}_F = \max_{b,c,d\in\mathbb{F}_{2^n}, bcd\neq 0} \texttt{EBCT}_F(1,b,c,d).$$

Proof. Let $a \in \mathbb{F}_{2^n}$ with $a \neq 0$. Consider the equation system

$$\begin{cases} F(x) + F(x+a) = b, \\ F(x) + F(x+c) = d, \\ F^{-1}(F(x)+d) + F^{-1}(F(x+a)+d) = a. \end{cases}$$

If $F(x) = x^r$, then the system is equivalent to

$$\begin{cases} x^r + (x+a)^r = b, \\ x^r + (x+c)^r = d, \\ (x^r+d)^{-r} + ((x+a)^r+d)^{-r} = a. \end{cases}$$

Let $x = ay$. Then the system can be reduced to

$$\begin{cases} y^r + (y+1)^r = \frac{b}{a^r}, \\ y^r + \left(y + \frac{c}{a^r}\right)^r = \frac{d}{a^r}, \\ \left(y^r + \frac{d}{a^r}\right)^{-r} + \left((y+1)^r + \frac{d}{a^r}\right)^{-r} = 1. \end{cases}$$

This implies that

$$\mathtt{EBCT}_F(a,b,c,d) = \mathtt{EBCT}_F\left(1, \frac{b}{a^r}, \frac{c}{a^r}, \frac{d}{a^r}\right),$$

and, as a consequence, the nontrivial extended boomerang connectivity uniformity of F satisfies

$$\overline{\underline{\delta}}_F = \max_{b,c,d\in\mathbb{F}_{2^n}, bcd\neq 0} \mathtt{EBCT}_F(1,b,c,d).$$

This completes the proof. □

The following result presents a link between the EBCT and the double difference distribution table (DDDT).

Proposition 11. *Let F be a permutation of $\mathbb{F}_{2^n}$. For any $a,b,c,d \in \mathbb{F}_{2^n}$,*

$$\mathtt{EBCT}_F(a,b,c,d) \leq \mathtt{DDDT}_F(a,c).$$

Proof. Suppose that x is a solution of (9), (10), and (11). Then, Equation (9) implies that $F(x+a) = F(x)+b$, and Equation (10) implies that $F(x)+d = F(x+c)$. Plugging this in Equation (11), we get

$$F^{-1}(F(x+c)) + F^{-1}(F(x)+b+d) = a,$$

and $F^{-1}(F(x)+b+d) = x+a+c$. Then $F(x)+b+d = F(x+a+c)$, and $F(x)+F(x+a+c) = b+d$. On the other hand, adding Equation (9) and Equation (10), we get $b+d = F(x+a)+F(x+c)$. Hence

$$F(x)+F(x+a)+F(x+c)+F(x+a+c) = 0,$$

which implies that

$$\mathtt{EBCT}_F(a,b,c,d) \leq \mathtt{DDDT}_F(a,c).$$

This completes the proof.

□

The following result gives a relation between the EBCT tables of two affine equivalent functions.

Proposition 12. *Let F and G be two affine equivalent permutations of $\mathbb{F}_{2^n}$ such that $G = A_2 \circ F \circ A_1$ where A_1, A_2 are affine permutations of $\mathbb{F}_{2^n}$. Then*

$$\mathtt{EBCT}_G(a,b,c,d) = \mathtt{EBCT}_F(A_1(a), A_2^{-1}(b), A_1(c), A_2^{-1}(d)).$$

Proof. Let $G = A_2 \circ F \circ A_1$ where A_1, A_2 are two affine permutations of $\mathbb{F}_{2^n}$. Then $\mathtt{UBCT}_G(a,b,c,d)$ is the number of the solutions $x \in \mathbb{F}_{2^n}$ satisfying the system of equations

$$\begin{cases} G(x) + G\left(x+a\right) = b, \\ G(x) + G\left(x+c\right) = d, \\ G^{-1}(G(x)+d) + G^{-1}\left(G(x+a)+d\right) = a. \end{cases}$$

The first equation is equivalent to

$$A_2\left(F(A_1(x)) + F(A_1(x) + A_1(a))\right) = b,$$

and $F(A_1(x)) + F(A_1(x) + A_1(a)) = A_2^{-1}(b)$.
The second equation is equivalent to

$$A_2\left(F(A_1(x)) + F(A_1(x) + A_1(c))\right) = d,$$

and $F(A_1(x)) + F(A_1(x) + A_1(c)) = A_2^{-1}(d)$.
The third equation is equivalent to

$$\begin{aligned} &A_1^{-1} \circ F^{-1} \circ A_2^{-1} (A_2 \circ F \circ A_1(x) + d) \\ &+ A_1^{-1} \circ F^{-1} \circ A_2^{-1} (A_2 \circ F \circ A_1 (x + a) + d) = a. \end{aligned}$$

This can be transformed to

$$A_1^{-1} \circ F^{-1} \left(F \circ A_1(x) + A_2^{-1}(d)\right) + A_1^{-1} \circ F^{-1} \left(F \circ A_1 (x + a) + A_2^{-1}(d)\right) = a,$$

and then to

$$A_1^{-1} \circ F^{-1} \left(F \circ A_1(x) + A_2^{-1}(d)\right) + A_1^{-1} \circ F^{-1} \left(F\left(A_1(x) + A_1(a)\right) + A_2^{-1}(d)\right) = a,$$

and finally to

$$F^{-1} \left(F(A_1(x)) + A_2^{-1}(d)\right) + F^{-1} \left(F\left(A_1(x) + A_1(a)\right) + A_2^{-1}(d)\right) = A_1(a).$$

By setting $A_1(x) = x'$, and since A_1 is a permutation, then x' is a solution of the system

$$\begin{cases} F(x') + F(x' + A_1(a)) = A_2^{-1}(b), \\ F(x') + F(x' + A_1(c)) = A_2^{-1}(d), \\ F^{-1}\left(F(x') + A_2^{-1}(d)\right) + F^{-1}\left(F\left(x' + A_1(a)\right) + A_2^{-1}(d)\right) = A_1(a). \end{cases}$$

This implies that

$$\mathtt{EBCT}_G(a, b, c, d) = \mathtt{EBCT}_F(A_1(a), A_2^{-1}(b), A_1(c), A_2^{-1}(d)).$$

and terminates the proof. □

Proposition 12 implies that the nontrivial extended boomerang connectivity uniformity satisfies $\overline{\underline{\delta}}_F = \overline{\underline{\delta}}_G$ whenever F and G are affine equivalent functions.

7.2 The EBCT of the Inverse Function

This section studies the EBCT of the inverse function F. The following result completes Proposition 9 for $abcd \neq 0$.

Theorem 6. *For $a, b, c, d \in \mathbb{F}_{2^n}$ with $abcd \neq 0$, we have*

$$\mathtt{EBCT}_F(a,b,c,d) = \begin{cases} 4 & \text{if } (a,b,c,d) \in \mathcal{I}'_1 \cup \mathcal{I}'_2, \\ 2 & \text{if } (a,b,c,d) \in \mathcal{I}'_3, \\ 0 & \text{if } (a,b,c,d) \notin \mathcal{I}_1 \cup \mathcal{I}'_2 \cup \mathcal{I}'_3, \end{cases}$$

where

$$\mathcal{I}'_1 = \left\{(a,b,c) : c = a, b = d = \frac{1}{a}, n \equiv 0 \pmod 2\right\},$$
$$\mathcal{I}'_2 = \left\{(a,b,c) : b = \frac{1}{a}, c = \frac{1}{d}, (ad)^2 + ad + 1 = 0\right\},$$
$$\mathcal{I}'_3 = \left\{(a,b,c) : c = a, d = b, ab \neq 1, Tr\left(\frac{1}{ab}\right) = 0\right\}.$$

Proof. Let $a, b, c, d \in \mathbb{F}_{2^n}$ with $abcd \neq 0$. Let

$$F(x) + F(x+a) = b, \tag{12}$$

$$F(x) + F(x+c) = d, \tag{13}$$

and

$$F^{-1}(F(x)+d) + F^{-1}(F(x+a)+d) = a. \tag{14}$$

Case 1. Assume that $x = 0$. Then $F(x) = 0$, and (12) gives $ab = 1$, and (13) gives $cd = 1$. Also, (14) gives $F^{-1}(d) + F^{-1}(F(a)+d) = a$.
Case 1.1. If $ad = 1$, then the former equality is satisfied.
Case 1.2. If $ad \neq 1$, then $F(a) + d \neq 0$, and the former equality implies that $(ad)^2 + ad + 1 = 0$.
Hence, $x = 0$ is a solution of the three equations if $b = d = \frac{1}{a}$, $c = a$, or if $b = \frac{1}{a}$, $d = \frac{1}{c}$, $(ad)^2 + ad + 1 = 0$.
Case 2. Assume that $x = a$. Then $F(x+a) = 0$, and (12) gives $ab = 1$, and (14) gives $F^{-1}(F(a)+d) + F^{-1}(d) = a$.
Case 2.1. If $ad = 1$, then $F(a) = d$, and the former equality is satisfied. Moreover, (13) gives $a = c$.
Case 2.2. If $ad \neq 1$, then the former equality gives $(ad)^2 + ad + 1 = 0$.
Case 2.2.1. If $a = c$, then (13) gives $ad = 1$, which is not possible.
Case 2.2.2. If $a \neq c$, then (13) gives

$$c = \frac{a^2 d}{ad+1} = \frac{1}{d}.$$

Hence, $x = a$ is a solution of the three equations if $b = d = \frac{1}{a}$, $c = a$, or if $b = \frac{1}{a}$, $d = \frac{1}{c}$, $a \neq c$, $(ad)^2 + ad + 1 = 0$.
Case 3. Assume that $x = c$. Then $F(x+c) = 0$, and (13) gives $cd = 1$.

Case 3.1. If $a = c$, then (12) gives $bc = 1$, and (14) gives $ad = 1$ which is satisfied.
Case 3.2. If $a \neq c$, then (14) gives $F^{-1}(F(c+a)+d) = a$, and $(ad)^2+ad+1 = 0$. Also, (12) gives

$$b = \frac{a}{(a+c)\,c} = \frac{1}{a}.$$

Hence, $x = c$ is a solution of the three equations if $a = c$, $b = d = \frac{1}{a}$, or if $d = \frac{1}{c}$, $b = \frac{1}{a}$, $a \neq c$, $(ad)^2 + ad + 1 = 0$.
Case 4. Assume that $x = \frac{1}{d}$. Then $F(x) + d = 0$, and (14) gives

$$F^{-1}\left(F\left(\frac{1}{d} + a\right) + d\right) = a.$$

Case 4.1. If $ad = 1$, then the former equality gives $F^{-1}(d) = a$, which is satisfied. Moreover, (12) gives $b = d$, and (13) gives $F\left(\frac{1}{d}\right) + F\left(\frac{1}{d} + c\right) = d$, that is $cd = 1$.
Case 4.2. If $ad \neq 1$, then (14) gives $(ad)^2 + ad + 1 = 0$. Also, (12) gives

$$b = \frac{a}{(a+c)\,c} = \frac{1}{a}.$$

Finally, (13) gives $cd = 1$, that is $\frac{1}{d} = c$. We observe that, in this case $c = \frac{1}{d}$ is also a solution of the system, as in Case 3.2.
Hence, $x = \frac{1}{d}$ is a solution of the three equations if $d = \frac{1}{a}$, $a = c$ or if $b = \frac{1}{a}$, $c = \frac{1}{d}$, and $(ad)^2 + ad + 1 = 0$.
Case 5. Assume that $x = a + \frac{1}{d}$. Then $F(x + a) + d = 0$, and (14) gives

$$F^{-1}\left(F\left(\frac{1}{d} + a\right) + d\right) = a,$$

and $(ad)^2 + ad + 1 = 0$. Next, (12) gives

$$b = \frac{ad^2}{ad+1} = \frac{1}{a}.$$

Case 5.1 If $c = a + \frac{1}{d}$, then (13) gives $F\left(a + \frac{1}{d}\right) = d$, and $a = 0$, which is impossible.
Case 5.2 If $c \neq a + \frac{1}{d}$, then (13) gives

$$c = \frac{a^2d^2+1}{ad^2} = \frac{1}{d}.$$

Hence, $x = a + \frac{1}{d}$ is a solution of the three equations if $(ad)^2 + ad + 1 = 0$, $b = \frac{1}{a}$, $c = \frac{1}{d}$.
Case 6. Assume that $x \neq 0$, $x \neq a$, $x \neq c$, $x \neq \frac{1}{d}$, and $x \neq a + \frac{1}{d}$. Then, combining the equations (12), (13), and (14), we get the system

$$\begin{cases} bx^2 + abx + a = 0, \\ dx^2 + cdx + c = 0, \\ dx^2 + adx + a = 0, \end{cases}$$

Case 6.1 If $a \neq c$, then, adding the last two equations, we get $(a+c)(dx+1) = 0$. This is not possible since $x \neq \frac{1}{d}$.
Case 6.2 If $b \neq d$, then, adding the first and the last equations, we get $(b + d)x(x + a) = 0$. This is not possible since $x \neq a$.
Case 6.3 Assume that $a = c$, and $b = d$. Then, the system reduces to the equation $bx^2 + abx + a = 0$. This equation has two solutions if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, and no solution if $\mathrm{Tr}\left(\frac{1}{ab}\right) \neq 0$.
Moreover, one can easily check that 0, a, c, $\frac{1}{d}$, and $a + \frac{1}{d}$ are not solutions of this equation.
The former cases can be summarized as follows.

1. If $c = a$, $b = d = \frac{1}{a}$, and $\mathrm{Tr}\,(1) = 0$, then $\mathtt{EBCT}_F(a, b, c, d) = 4$. This is true by Case 1, Case 2, Case 3, and case 4.
2. If $b = \frac{1}{a}$, $c = \frac{1}{d}$ $a \neq c$, and $(ad)^2 + ad + 1 = 0$, then $\mathtt{EBCT}_F(a, b, c, d) = 4$. This is true by Case 1, Case 2, Case 3, and Case 5.
3. If $c = a$, $b = d$, and then $\mathtt{EBCT}_F(a, b, c, d) = 2$. This is true by Case 6.3.
4. In all other cases, $\mathtt{EBCT}_F(a, b, c) = 0$.

This completes the proof. □

Theorem 6 implies the following result regarding the nontrivial extended boomerang connectivity uniformity of F.

Lemma 4. *The nontrivial extended boomerang connectivity uniformity of the inverse permutation satisfies*

$$\underline{\overline{\delta}}_F = \begin{cases} 4 & \text{if } n \text{ is even,} \\ 2 & \text{if } n \text{ is odd.} \end{cases}$$

8 Conclusions

The boomerang attack is a cryptanalysis technique that allows an attack to concatenate two short differential characteristics. Given its importance, this research direction has attracted considerable attention. The main crucial tool for quantifying the resistance of a block cypher involving an S-box is the so-called Boomerang Connectivity Table (BCT), which is admitted to be channelling to compete through its system of equations defined by it.

This paper follows the recent advance in boomerang cryptanalysis due to Wang and Peyrin by investigating two appropriate tables introduced recently to measure the resistance of S-boxes derived from vectorial Boolean permutations to cryptanalytic attacks, such as the differential and boomerang attacks: the Upper Boomerang Connectivity Table (UBCT) and the Lower Boomerang Connectivity Table (LBCT). We studied the properties of the UBCT, LBCT, and the Extended Boomerang Connectivity Table (EBCT) for investible S-boxes. We showed that the three tables are interconnected and have various remarkable properties. We also introduced the notion of the nontrivial boomerang connectivity to measure the strengths of these tables. Moreover, we give an explicit value of all the entries of the UBCT, the LBCT, and the EBCT of the significant inverse function. For future work, many directions could be investigated. Still, the natural one would be to study these new tools for other classic popular invertible S-boxes known to have excellent results regarding fundamental attacks in the context of the block cipher in the line of our previous study [14] as well as the depth-in study of the UBCT, LBCT, and EBCT to derive more general results for vectorial permutations at least for quadratic or low-degree functions, in the line of [19].

References

1. Bar-On, A, Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis. Y. Ishai, V. Rijmen (Eds): EUROCRYPT 2019, LNCS 11476, pp. 313-342, 2019.
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, vol.4, no.1, pp.3–72, 1991.
3. Boukerrou, H., Huynh, P., Lallemand, V., Mandal, B., Minier, M.: On the Feistel Counterpart of the Boomerang Connectivity Table: Introduction and Analysis of the FBCT, IACR Transactions on Symmetric Cryptology, Ruhr-University Bochum, 020, Issue 1, pp. 331-362, 2020.
4. Boura C., and Canteaut A.: On the boomerang uniformity of cryptographic S-boxes. IACR Transactions on Symmetric Cryptology, 2018(3):290–310, 2018.
5. Bracken C., Leander G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields Appl. 16, 231-242, 2010.
6. Calderini M., and Villa L.: On the boomerang uniformity of some permutation polynomials. Cryptography and Communications (12) 1161-1178, 2020.
7. Carlet, C.: Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, 2021.
8. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang Connectivity Table: A New Cryptanalysis Tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, Advances in Cryptology - EUROCRYPT 2018 -Proceedings, Part II, volume 10821 of Lecture Notes in Computer Science, 683–714. Springer , 2018.
9. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, Heidelberg, 2002.
10. Delaune, S., Derbez, P., Vavrille, M.: Catching the Fastest Boomerangs: Application to SKINNY. IACR Transactions on Symmetric Cryptology, 2020(4), 104-129, 2020.
11. Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n) : the Welch case. IEEE Trans. Inf. Theory, 45 (4) (1999), 1271-1275.
12. Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): the Niho case. Inf. Comput., 151 (1-2) (1999), 57-72.
13. Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n) : a new case for n divisible by 5. In Jungnickel, D. Niederreiter, H. (Eds.): Proceedings of the Conference on Finite Fields and Applications. Augsburg, 1999, SpringerVerlag, Berlin (2001), pp. 113-121.
14. Eddahmani, S., Mesnager, S.: Explicit values of the DDT, the BCT, the FBCT, and the FBDT of the Inverse, the Gold, and the Bracken-Leander S-boxes. Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, 2022, 14 (6), pp.1301-1344.

15. Eddahmani, S., Mesnager, S.: On the Double Differential Uniformity of Vectorial Boolean Functions, Submitted to Africacrypt 2024.

16. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.), IEEE Transactions on Information Theory, vol.14, issue.1, 154-156, 1968.

17. Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Inf. Control. 18(4), 369-394, 1971.

18. Li K., Qu L., Sun B., and Li C.: New results about the boomerang uniformity of permutation polynomials. IEEE Transactions on Information Theory, 65(11):7542-7553, 2019.

19. Mesnager S., Tang C., and Xiong M.: On the boomerang uniformity of quadratic permutations. Designs, Codes and Cryptography, 88(10):2233-2246, 2020.

20. Mesnager S., Mandal B., and Msahli M.: Survey on recent trends towards generalized differential and boomerang uniformities. Cryptogr. Commun. 14(4): 691-735, 2022.

21. Nyberg. K.: Differentially uniform mappings for cryptography. In: Helleseth T. (eds) Advances in Cryptology - EUROCRYPT'93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. pp. 55-64, Springer, Berlin, Heidelberg, 1994.

22. Song L., Qin X., and L. Hu.: Boomerang Connectivity Table Revisited Application to SKINNY and AES. IACR Transactions on Symmetric Cryptology (1):118-141, 2019.

23. Tian S., Boura C., and, Perrin L .:Boomerang uniformity of popular S-box constructions. Designs, Codes and Cryptography, 88:1959-1989, 2020.

24. Pommerening, K.: Quadratic equations in finite fields of characteristic 2, February 2012. `http://www.staff.uni-mainz.de/pommeren/MathMisc/QuGlChar2.pdf`

25. Wagner, D.: The Boomerang Attack. In Lars R. Knudsen, editor, Fast Software Encryption, volume 1636 of Lecture Notes in Computer Science, pp. 156-170, Springer, 1999.

26. Wang, H. and Peyrin, T.: Boomerang switch in multiple rounds. application to AES variants and deoxys. IACR Trans. Symmetric Cryptol., 2019(1):142-169, 2019.

27. Wagner D.: The boomerang attack.: FSE, LNCS 1636:156-170, 1999.

A Appendix: list of the UBCT of the Inverse Function over $\mathbb{F}_{2^3}$

In this section, we give the list of all values of $\texttt{UBCT}_F(a, b, c)$ for the inverse function F over $\mathbb{F}_{2^3}$. We can check that $\texttt{UBCT}_F(a, b, 0) = DDT(a, b)$, as claimed in Proposition 3, by comparing Table 1 and Table 2.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	0	0	2	2	2	2
3	0	2	0	2	2	0	2	0
4	0	0	2	2	0	0	2	2
5	0	2	2	0	0	2	2	0
6	0	0	2	2	2	2	0	0
7	0	2	2	0	2	0	0	2

Table 2. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 0$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	2	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	2	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	2	0	0	0	0	0	0

Table 3. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 1$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	2	0	0	0	0	0
5	0	0	2	0	0	0	0	0
6	0	0	2	0	0	0	0	0
7	0	0	2	0	0	0	0	0

Table 4. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 2$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	2	0	0	0	0
4	0	0	0	2	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	2	0	0	0	0
7	0	0	0	0	0	0	0	0

Table 5. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 3$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	2	0	0	0
3	0	0	0	0	2	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	2	0	0	0
7	0	0	0	0	2	0	0	0

Table 6. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 4$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	0	2	0	0
2	0	0	0	0	0	2	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	2	0	0
6	0	0	0	0	0	2	0	0
7	0	0	0	0	0	0	0	0

Table 7. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 5$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	2	0
3	0	0	0	0	0	0	2	0
4	0	0	0	0	0	0	2	0
5	0	0	0	0	0	0	2	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0

Table 8. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 6$.

$a\backslash b$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	2
2	0	0	0	0	0	0	0	2
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	2
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	2

Table 9. UBCT(a,b,c) of the inverse function over $\mathbb{F}_{2^3}$ for $c = 7$.