Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-025-01582-3

The revised boomerang connectivity tables and their connection to the difference distribution table

Kirpa Garg[1] · Sartaj Ul Hasan[1] · Constanza Riera[2] · Pantelimon Stănică[3]

Received: 17 July 2024 / Revised: 21 January 2025 / Accepted: 22 January 2025
This is a U.S. Government work and not under copyright protection in the US; foreign copyright protection may apply 2025

Abstract
It is well-known that functions over finite fields play a crucial role in designing substitution boxes (S-boxes) in modern block ciphers. In order to analyze the security of an S-box, recently, three new tables have been introduced: the Extended Boomerang Connectivity Table (EBCT), the Lower Boomerang Connectivity Table (LBCT), and the Upper Boomerang Connectivity Table (UBCT). In fact, these tables offer improved methods over the usual Boomerang Connectivity Table (BCT) for analyzing the security of S-boxes against boomerang-style attacks. Here, we put in context these new EBCT, LBCT, and UBCT concepts by connecting them to the DDT for a differentially δ-uniform function and also determine the EBCT, LBCT, and UBCT entries of three classes of differentially 4-uniform power permutations, namely, Gold, Kasami and Bracken–Leander. We also determine the Double Boomerang Connectivity Table (DBCT) entries of the Gold function. As byproducts of our approach, we obtain some previously published results quite easily.

Keywords Finite fields · Permutation polynomials · Almost perfect non-linear functions · Upper boomerang connectivity table · Lower boomerang connectivity table · Extended boomerang connectivity table · Double boomerang connectivity table.

The work of K. Garg is supported by the University Grants Commission (UGC), Government of India. The work of S. U. Hasan is partially supported by Core Research Grant CRG/2022/005418 from the Science and Engineering Research Board, Government of India. The work of P. Stănică (corresponding author) is partially supported by a grant from the NPS Foundation.

✉ Pantelimon Stănică
pstanica@nps.edu

Kirpa Garg
kirpa.garg@gmail.com

Sartaj Ul Hasan
sartaj.hasan@iitjammu.ac.in

Constanza Riera
csr@hvl.no

[1] Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India

[2] Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway

[3] Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

Mathematics Subject Classification 12E20 · 11T06 · 94A60

1 Introduction

In symmetric cryptography, vectorial Boolean functions over finite fields play a significant role, particularly in designing block ciphers' S-boxes. There are various kinds of cryptanalytic attacks possible on these S-boxes. One well-known attack on S-boxes is the differential attack, introduced by Biham and Shamir [1]. This attack exploits the non-uniformity in the distribution of output differences corresponding to a given input difference. To quantify the degree of resistance of S-Boxes against differential attacks, Nyberg [18] introduced the notion of Difference Distribution Table (DDT) and differential uniformity.

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, by $\mathbb{F}_{2^n}^*$ the multiplicative cyclic group of non-zero elements of $\mathbb{F}_{2^n}$ and by $\mathbb{F}_{2^n}[X]$ the ring of polynomials in one variable X with coefficients in $\mathbb{F}_{2^n}$. For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, and for any $a \in \mathbb{F}_{2^n}$, the derivative of F in the direction a is defined as $D_F(X, a) := F(X + a) + F(X)$ for all $X \in \mathbb{F}_{2^n}$. For any $a, b \in \mathbb{F}_{2^n}$, the Difference Distribution Table (DDT) entry $\mathrm{DDT}_F(a, b)$ at point (a, b) is the number of solutions $X \in \mathbb{F}_{2^n}$ of the equation $D_F(X, a) = b$. Further, the differential uniformity of F, denoted by Δ_F, is given by $\Delta_F := \max\left\{\mathrm{DDT}_F(a, b) \;\middle|\; a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\right\}$. We call a function F an almost perfect nonlinear (APN) function if $\Delta_F = 2$. Notice that Δ_F is always even, because if X is a solution of $D_F(X, a) = b$ then $X + a$ is also a solution of $D_F(X, a) = b$. Functions with low differential uniformity are more resistant to differential attacks, making them desirable for cryptographic applications.

However, it turns out that low differential uniformity is not sufficient to counter some differentials connected attacks. In 1999, Wagner [19] introduced a new attack on block ciphers, called the boomerang attack, which can be seen as an extension of the differential attack. It allows the cryptanalyst to use two unrelated differential characteristics to attack the same cipher by using one differential to defeat the first half and another to defeat the second half of the cipher. The theoretical underpinning of this attack was considered by Cid et al. [9], who introduced the notion of the Boomerang Connectivity Table (BCT) that can be used to more accurately evaluate the probability of generating a right quartet in boomerang-style attacks such that the boomerang incompatibility, ladder switch and S-box switch can easily be detected. For effectively computing the entries in the BCT, Li et al. [16] proposed an equivalent formulation as described below, which avoids computing the inverse of the S-box, and consequently, it can be defined even for non-permutation. For any $a, b \in \mathbb{F}_{2^n}$, the BCT entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, denoted as $\mathcal{B}_F(a, b)$, is the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system

$$\begin{cases} F(X) + F(Y) = b \\ F(X + a) + F(Y + a) = b. \end{cases}$$

The boomerang uniformity of F is defined as $\mathcal{B}_F := \max\left\{\mathcal{B}_F(a, b) \;\middle|\; a, b \in \mathbb{F}_{2^n}^*\right\}$. However, it turns out that the BCT has limitations when evaluating boomerang switches in multiple rounds. This was observed by Wang and Peyrin [20], who showed that the BCT is not applicable effectively in some cases involving multiple rounds by giving an incompatibility example on two rounds of AES. To address this challenge, they introduced a new tool known as the Boomerang Difference Table (BDT) along with its variant BDT′. Later, in 2020, Delaune et al. [11] renamed these tables as the Upper Boomerang Connectivity Table (UBCT) and

the Lower Boomerang Connectivity Table (LBCT), respectively, to highlight the fact that UBCT and LBCT emphasize the upper and lower characteristic, respectively. The Feistel Boomerang Extended Table (FBET), or Boomerang Extended Table (BET) for SPN ciphers, proposed by Boukerrou et al. [3], has been renamed as the Extended Boomerang Connectivity Table (EBCT) by Delaune et al. in [11]. The entries in this table count the number of values such that the boomerang will return on a single S-box, with all the differences fixed.

Further, to study the behavior of two consecutive S-boxes in the boomerang attack, Hadipour et al. [14] introduced the notion of Double Boomerang Connectivity Table (DBCT). It may be noted that Yang et al. [22] illustrated the effect of an S-box on the probability of the 7-round boomerang distinguisher by comparing the DDT, BCT and DBCT entries of different S-boxes. Their findings highlight the importance of investigating the DBCT, in addition to the DDT and BCT, for evaluating an S-box's resistance to a boomerang attack. However, determining the DBCT entries for an S-box (or equivalently, for a vectorial Boolean function) is quite challenging, and rather limited research has been done in this direction.

Recently, Eddahmani and Mesnager [13] studied various properties of the EBCT, LBCT and UBCT. They also determined these entries for the inverse function. In a separate work, Man et al. [17] also gave the DBCT, LBCT and UBCT entries for the inverse function. In this work, we discuss the DBCT entries of the Gold function, and we provide a connection between these new EBCT, LBCT and UBCT concepts and the DDT entries for a differentially δ-uniform function. As a consequence, it turns out that our result covers a particular case of a result of Eddahmani et al. [13] and Man et al. [17] for the inverse function over $\mathbb{F}_{2^n}$. Moreover, we explicitly compute EBCT, LBCT and UBCT entries of three classes of differentially-4 uniform power permutations.

We shall now give the structure of the paper. We first recall some definitions and results in Sect. 2. In Sect. 3, we provide some general results on the EBCT. We also give a generalization for the definitions of the EBCT, LBCT and UBCT for any function over $\mathbb{F}_{2^n}$. In Sect. 4, we discuss the invariance of the EBCT, LBCT and UBCT under the CCZ-equivalence. In Sect. 5, we find a connection between the EBCT, LBCT and UBCT entries of a differentially δ-uniform function and also express them in terms of the DDT entries. Sections 6 and 7 deal with the EBCT, LBCT and UBCT entries of APN functions (leading to a characterization of APN functions) and 4-differential uniform functions, as well as some other well-known functions. We also computed the DBCT entries for the Gold function in Sect. 8. Finally, we conclude the paper in Sect. 9.

2 Preliminaries

We will first recall several definitions and lemmas used in the subsequent sections. Throughout the paper, we shall use Tr_m^n to denote the (relative) trace function from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, i.e., $\mathrm{Tr}_m^n(X) = \sum_{i=0}^{\frac{n-m}{m}} X^{2^{mi}}$, where m and n are positive integers and $m \mid n$. For $m = 1$, we use Tr to denote the absolute trace. As customary, for a set S, we let $a + S = \{a + s \mid s \in S\}$.

Definition 2.1 [11] 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 $a, b, c, d \in \mathbb{F}_{2^n}$ is

$$\mathrm{EBCT}_F(a,b,c,d) = \left| \left\{ X \in \mathbb{F}_{2^n} \,\middle|\, \begin{cases} F(X) + F(X+a) = b \\ F(X) + F(X+c) = d \\ F^{-1}(F(X)+d) + F^{-1}(F(X+a)+d) = a \end{cases} \right\} \right|.$$

Definition 2.2 [20] Let F be a permutation of $\mathbb{F}_{2^n}$. The Lower Boomerang Connectivity Table (LBCT) of F is defined as a $2^n \times 2^n \times 2^n$ table where the entry at $a, b, c \in \mathbb{F}_{2^n}$ is

$$\mathrm{LBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \begin{cases} F(X) + F(X+b) = c \\ F^{-1}(F(X)+c) + F^{-1}(F(X+a)+c) = a \end{cases} \right\} \right|.$$

Definition 2.3 [20] Let F be a permutation of $\mathbb{F}_{2^n}$. The Upper Boomerang Connectivity Table (UBCT) of F is defined as a $2^n \times 2^n \times 2^n$ table where the entry at $a, b, c \in \mathbb{F}_{2^n}$ is

$$\mathrm{UBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \begin{cases} F(X) + F(X+a) = b \\ F^{-1}(F(X)+c) + F^{-1}(F(X+a)+c) = a \end{cases} \right\} \right|.$$

Recently, Eddahmani and Mesnager [13] and, Man et al. [17] redefined the notions of LBCT and UBCT for a function F without involving its compositional inverse ([17] also mentions the non-necessity of the permutation property for the UBCT), as stated in the following lemmas.

Lemma 2.4 [13] *Let F be a permutation of $\mathbb{F}_{2^n}$. Then for $a, b, c \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{LBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists\, Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} X + Y = b \\ F(X+a) + F(Y+a) = c \\ F(X) + F(Y) = c \end{cases} \right\} \right|,$$

and

$$\mathrm{UBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists\, Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} F(X+a) + F(Y+a) = c \\ F(X) + F(Y) = c \\ F(X) + F(X+a) = b \end{cases} \right\} \right|.$$

Definition 2.5 (*Feistel Boomerang Connectivity Table*) [3] Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. The *Feistel Boomerang Connectivity Table* (FBCT) of F is given by a $2^n \times 2^n$ table, of entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ defined by

$$\mathrm{FBCT}_F(a,b) = \left| \left\{ X \in \mathbb{F}_{2^n} \;\middle|\; F(X+a+b) + F(X+b) + F(X+a) + F(X) = 0 \right\} \right|.$$

This is also denoted as $\nabla_F(a, b)$. The maximum of the entries of the FBCT of F, for $a \neq b, ab \neq 0$, is also known as the *second-order zero differential uniformity* of F, denoted as ∇_F, which is defined over any finite field characteristic.

Remark 2.6 If F is a permutation of $\mathbb{F}_{2^n}$, then it is immediate that

$$\mathrm{FBCT}_F(a,b) = \sum_{c \in \mathbb{F}_{2^n}} \mathrm{LBCT}_F(a,b,c).$$

Note that this implies that $\mathrm{LBCT}_F(a,b,c) \leq \mathrm{FBCT}_F(a,b),\ \forall a, b, c \in \mathbb{F}_{2^n}$.

Definition 2.7 (*Double Difference Distribution Table*) [13] 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 $(a, b, c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is given by

$$\mathrm{DDDT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \;\middle|\; F(X+a+b) + F(X+b) + F(X+a) + F(X) = c \right\} \right|.$$

Note that $\mathrm{FBCT}_F(a,b) = \mathrm{DDDT}_F(a,b,0)$.

Moreover, in [13] it was shown that for $a, b, c, d \in \mathbb{F}_{2^n}$ with $abcd = 0$, the values of $\mathrm{EBCT}_F(a, b, c, d)$ are simple to compute if F is a permutation, as are the values of $\mathrm{LBCT}_F(a, b, c)$ and $\mathrm{UBCT}_F(a, b, c)$, for $abc = 0$. We recall these results in the following three lemmas.

Lemma 2.8 [13] *Let F be a permutation of $\mathbb{F}_{2^n}$. Then for $a, b, c, d \in \mathbb{F}_{2^n}$ with $abcd = 0$, we have*

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

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

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

Remark 2.9 If F is not a permutation, some of the results of Lemma 2.8 are not true. We give the generalization of Lemma 2.8 in Sect. 5.

Also, Wagner [19] shows that $\mathrm{UBCT}_F(a, b, b) = \mathrm{DDT}_F(a, b)$, as well as, $\mathrm{BCT}_F(a, c) = \sum_{b\in\mathbb{F}_{2^n}} \mathrm{UBCT}_F(a, b, c)$. Additionally, it is easy to see that $\mathrm{DDT}_F(a, c) = \mathrm{LBCT}_F(a, a, c)$.
Next, we recall the notion of DBCT as follows.

Definition 2.10 [22] Let $F(X)$ be a mapping from $\mathbb{F}_{2^n}$ to itself. The *Double Boomerang Connectivity Table* (DBCT) is a $2^n \times 2^n$ table defined for $(a, d) \in \mathbb{F}_{2^n}^2$ by

$$\mathrm{DBCT}_F(a,d) = \sum_{b,c} \mathrm{dbct}(a,b,c,d),$$

where $\mathrm{dbct}(a, b, c, d) = \mathrm{UBCT}_F(a, b, c)\,\mathrm{LBCT}_F(b, c, d)$. For $a = 0$ or $d = 0$, it can be easily obtained that

$$\mathrm{DBCT}_F(0,d) = \sum_{c} \mathrm{UBCT}_F(0,0,c)\,\mathrm{LBCT}_F(0,c,d) = 2^{2n}, \text{ and}$$
$$\mathrm{DBCT}_F(a,0) = \sum_{b} \mathrm{UBCT}_F(a,b,0)\,\mathrm{LBCT}_F(b,0,0) = 2^{2n}.$$

3 General results on the EBCT

In a similar way as the results in [13] and [17], we can redefine the EBCT for a function F without involving its compositional inverse, as stated in the following lemma.

Lemma 3.1 *Let F be a permutation of $\mathbb{F}_{2^n}$. Then for $a, b, c, d \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_F(a,b,c,d) = \left| \left\{ X \in \mathbb{F}_{2^n} \,\middle|\, \begin{cases} F(X)+F(X+a)=b \\ F(X)+F(X+c)=d \\ F(X+a+c)+F(X+a)=d \end{cases} \right\} \right|.$$

Proof We write

$$\mathrm{EBCT}_F(a,b,c,d) = \left| \left\{ X \in \mathbb{F}_{2^n} \,\middle|\, \begin{cases} (1)\ F(X)+F(X+a)=b \\ (2)\ F(X)+F(X+c)=d \\ (3)\ F^{-1}(F(X)+d)+F^{-1}(F(X+a)+d)=a \end{cases} \right\} \right|.$$

Equation (2) implies $F(X)+d = F(X+c)$. Equation (3) is then equivalent to

$$\begin{aligned} &F^{-1}(F(X+c))+F^{-1}(F(X+a)+d)=a, \\ &F^{-1}(F(X+a)+d)=X+a+c, \\ &F(X+a)+d=F(X+a+c), \end{aligned}$$

completing the proof of the lemma. □

As a consequence, we can derive the connection between the EBCT of a permutation and the EBCT of its compositional inverse.

Corollary 3.2 *Let F be a permutation of $\mathbb{F}_{2^n}$. Then for $a, b, c, d \in \mathbb{F}_{2^n}$, we have* $\mathrm{EBCT}_F(a,b,c,d) = \mathrm{EBCT}_{F^{-1}}(b,a,d,c)$.

Proof We have by Lemma 3.1 that $\mathrm{EBCT}_F(a,b,c,d)$ is given by the following equations:

$$\mathrm{EBCT}_F(a,b,c,d) = \left| \left\{ X \in \mathbb{F}_{2^n} \,\middle|\, \begin{cases} (1)\ F(X)+F(X+a)=b \\ (2)\ F(X)+F(X+c)=d \\ (3)\ F(X+a+c)+F(X+a)=d \end{cases} \right\} \right|.$$

Let $Y = F(X)$. Then, Eq. (1) gives $Y + F(X+a) = b$, which is equivalent to $F(X+a) = Y+b$, and then to $X+a = F^{-1}(Y+b)$, rendering the equation $F^{-1}(Y+b)+F^{-1}(Y) = a$. Similarly, Eq. (2) is equivalent to $F^{-1}(Y+d)+F^{-1}(Y) = c$.

Lastly, inserting Eq. (1) in Eq. (3), we obtain $F(X+a+c) = Y+d+b$, which is equivalent to $F^{-1}(Y+b+d) = X+a+c$. Since $F^{-1}(Y+b)+F^{-1}(Y) = F^{-1}(Y+b)+X = a$, this gives in turn $F^{-1}(Y+b+d) = F^{-1}(Y+b)+c$, equivalent to $F^{-1}(Y+b+d)+F^{-1}(Y+b) = c$. We therefore get the claim. □

Lemmas 2.4 and 3.1 also suggest a generalization of these concepts for the set of all functions over $\mathbb{F}_{2^n}$ (not necessarily permutations).

Definition 3.3 Let F be a function over $\mathbb{F}_{2^n}$. Then, for $a, b, c, d \in \mathbb{F}_{2^n}$, we can define the EBCT, LBCT and UBCT in the following way,

$$\mathrm{EBCT}_F(a,b,c,d) = \left| \left\{ X \in \mathbb{F}_{2^n} \,\middle|\, \begin{cases} F(X)+F(X+a)=b \\ F(X)+F(X+c)=d \\ F(X+a+c)+F(X+a)=d \end{cases} \right\} \right|, \tag{3.1}$$

$$\mathrm{LBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} X+Y=b \\ F(X+a)+F(Y+a)=c \\ F(X)+F(Y)=c \end{cases} \right\} \right|, \tag{3.2}$$

$$\mathrm{UBCT}_F(a,b,c) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} F(X+a)+F(Y+a)=c \\ F(X)+F(Y)=c \\ F(X)+F(X+a)=b \end{cases} \right\} \right|. \tag{3.3}$$

Remark 3.4 Note that if F is a permutation, these definitions are equivalent to the original definitions of these concepts. We preferred to define these concepts this way to avoid over-counting, but we point out that even if we count the number of pairs (X, Y) in each set, all results hold, except for the UBCT in Theorem 5.1, where its expression becomes too cumbersome.

4 Invariance under the CCZ, extended affine and affine-equivalence

We recall that two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are *CCZ-equivalent* [7] if there exists an affine permutation $\mathcal{A}$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$\left\{ \begin{pmatrix} x \\ G(x) \end{pmatrix} \mid x \in \mathbb{F}_{2^n} \right\} = \left\{ \mathcal{A} \begin{pmatrix} x \\ F(x) \end{pmatrix} \mid x \in \mathbb{F}_{2^n} \right\}.$$

As customary, we use the natural identification of the elements in $\mathbb{F}_{2^n}$ with the elements in $\mathbb{F}_2^n$, and, by abuse, we denote by x both an element in $\mathbb{F}_{2^n}$ and the corresponding element in $\mathbb{F}_2^n$. We also decompose the affine permutation $\mathcal{A}$ as an affine block-matrix, for an input vector $u \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$: $\mathcal{A}u = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} u + \begin{pmatrix} C \\ D \end{pmatrix}$, where $\mathcal{A}_{ij} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $i, j \in \{1, 2\}$ and $\begin{pmatrix} C \\ D \end{pmatrix}$ is a column vector in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

When $\mathcal{A}_{12} = 0$, we say that F and G are *extended affine (EA)*-equivalent. This can be also written as $G = F_2 \circ F \circ F_1 + F_0$, for some $F_i(X) = L_i(X) + B_i$ affine functions, where L_i are linearized polynomials, $B_i \in \mathbb{F}_{2^n}$ such that F_1 and F_2 are permutation polynomials.

When $\mathcal{A}_{12} = \mathcal{A}_{21} = 0$, we say that F and G are *affine*-equivalent. This can be also written as $G = F_2 \circ F \circ F_1$, for some $F_i(X) = L_i(X) + B_i$ affine functions, where L_i are linearized polynomials, $B_i \in \mathbb{F}_{2^n}$ such that F_1 and F_2 are permutation polynomials.

Here, we discuss the behavior of the EBCT, LBCT and UBCT of a function F under CCZ, extended affine and affine-equivalence. It is worth noting that Eddahmani and Mesnager [13] proved that the EBCT, LBCT and UBCT of a permutation remain invariant under affine-equivalence.

Theorem 4.1 *Given any functions F, G on $\mathbb{F}_{2^n}$ that are CCZ-equivalent via the affine permutation $\mathcal{A}$ on $\mathbb{F}_{2^{2n}}$, and given any $a, b, c, d \in \mathbb{F}_{2^n}$, then* $\mathrm{EBCT}_F(a,b,c,d) = \mathrm{EBCT}_G(\alpha,\beta,\gamma,\delta)$, *with* $\alpha = \mathcal{A}_{12}b + \mathcal{A}_{11}a$, $\beta = \mathcal{A}_{22}b + \mathcal{A}_{21}a$, $\gamma = \mathcal{A}_{12}d + \mathcal{A}_{11}c$ *and* $\delta = \mathcal{A}_{22}d + \mathcal{A}_{21}c$, *and thus, the EBCT spectrum is preserved under the CCZ-equivalence.*

Proof Let $\left\{\begin{pmatrix} x \\ G(x) \end{pmatrix}, x \in \mathbb{F}_{2^n}\right\} = \left\{\mathcal{A}\begin{pmatrix} x \\ F(x) \end{pmatrix}, x \in \mathbb{F}_{2^n}\right\}$. Then, for every $X, c \in \mathbb{F}_{2^n}$ there exists $y, z \in \mathbb{F}_{2^n}$ such that $\begin{pmatrix} y \\ G(y) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X \\ F(X) \end{pmatrix}$ and $\begin{pmatrix} z \\ G(z) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X+c \\ F(X+c) \end{pmatrix}$, which gives

$$\begin{aligned} y &= \mathcal{A}_{11}X + \mathcal{A}_{12}F(X) + C, \\ G(y) &= \mathcal{A}_{21}X + \mathcal{A}_{22}F(X) + D, \\ z &= \mathcal{A}_{11}(X+c) + \mathcal{A}_{12}F(X+c) + C, \\ G(z) &= \mathcal{A}_{21}(X+c) + \mathcal{A}_{22}F(X+c) + D. \end{aligned}$$

Suppose $F(X+c) + F(X) = d$. Then,

$$\begin{aligned} G(z) + G(y) &= \mathcal{A}_{21}(X+c) + \mathcal{A}_{22}F(X+c) + D + \mathcal{A}_{21}X + \mathcal{A}_{22}F(X) + D \\ &= \mathcal{A}_{22}(F(X+c) + F(X)) + \mathcal{A}_{21}c = \mathcal{A}_{22}d + \mathcal{A}_{21}c. \end{aligned}$$

Taking $z = y + \gamma$ and $\delta = \mathcal{A}_{22}d + \mathcal{A}_{21}c$, we obtain: $G(y+\gamma) + G(y) = \delta$. We can also see that

$$\begin{aligned} \gamma = y + z &= \mathcal{A}_{11}X + \mathcal{A}_{12}F(X) + C + \mathcal{A}_{11}(X+c) + \mathcal{A}_{12}F(X+c) + C \\ &= \mathcal{A}_{12}(F(X+c) + F(X)) + \mathcal{A}_{11}c = \mathcal{A}_{12}d + \mathcal{A}_{11}c. \end{aligned}$$

Therefore, $F(X)+F(X+c) = d \Rightarrow G(y+\gamma)+G(y) = \delta$, where $\gamma = \mathcal{A}_{12}d+\mathcal{A}_{11}c$ and $\delta = \mathcal{A}_{22}d + \mathcal{A}_{21}c$.

Similarly, taking $\begin{pmatrix} u \\ G(u) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X+a \\ F(X+a) \end{pmatrix}$, we can prove that $F(X) + F(X+a) = b \Rightarrow G(y+\alpha) + G(y) = \beta$, where $\alpha = \mathcal{A}_{12}b + \mathcal{A}_{11}a$ and $\beta = \mathcal{A}_{22}b + \mathcal{A}_{21}a$.

Now, we need to see if the third equation, $F(X+a) + F(X+a+c) = d$, transforms into $G(y+\alpha) + G(y+\alpha+\gamma) = \delta$ with the same values of α, γ, and δ. Taking $\begin{pmatrix} w \\ G(w) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X+a+c \\ F(X+a+c) \end{pmatrix}$, we see that

$$\begin{aligned} w &= \mathcal{A}_{11}(X+a+c) + \mathcal{A}_{12}F(X+a+c) + C, \\ G(w) &= \mathcal{A}_{21}(X+a+c) + \mathcal{A}_{22}F(X+a+c) + D, \\ u &= \mathcal{A}_{11}(X+a) + \mathcal{A}_{12}F(X+a) + C, \\ G(u) &= \mathcal{A}_{21}(X+a) + \mathcal{A}_{22}F(X+a) + D. \end{aligned}$$

Then,

$$\begin{aligned} G(w) + G(u) &= \mathcal{A}_{21}(X+a+c) + \mathcal{A}_{22}F(X+a+c) \\ &\quad + D + \mathcal{A}_{21}(X+a) + \mathcal{A}_{22}F(X+a) + D \\ &= \mathcal{A}_{22}(F(X+a+c) + F(X+a)) + \mathcal{A}_{21}c = \mathcal{A}_{22}d + \mathcal{A}_{21}c = \delta. \end{aligned}$$

As before, $u = y + \alpha$, with

$$\begin{aligned} \alpha = y + u &= \mathcal{A}_{11}X + \mathcal{A}_{12}F(X) + C + \mathcal{A}_{11}(X+a) + \mathcal{A}_{12}F(X+a) + C \\ &= \mathcal{A}_{12}b + \mathcal{A}_{11}a, \text{ and} \\ w + u &= \mathcal{A}_{11}(X+a+c) + \mathcal{A}_{12}F(X+a+c) + C \\ &\quad + \mathcal{A}_{11}(X+a) + \mathcal{A}_{12}F(X+a) + C \end{aligned}$$

$$= \mathcal{A}_{12}(F(X+a+c)+F(X+a)) + \mathcal{A}_{11}c = \mathcal{A}_{12}d + \mathcal{A}_{11}c = \gamma.$$

Therefore, we get the desired equation $G(y+\alpha)+G(y+\alpha+\gamma)=\delta$, with the same values of α, γ, and δ.

Finally, we note that

$$\begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\mathcal{A}_{11} & \mathcal{A}_{12} & 0 & 0\\ \mathcal{A}_{21} & \mathcal{A}_{22} & 0 & 0\\ 0 & 0 & \mathcal{A}_{11} & \mathcal{A}_{12}\\ 0 & 0 & \mathcal{A}_{21} & \mathcal{A}_{22}\end{pmatrix}\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix} = \mathcal{B}\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix}$$

and, since $\mathcal{A}$ is invertible, the matrix $\mathcal{B}$ is also invertible. This concludes the proof. □

Below we use again this section's notations.

Theorem 4.2 *The LBCT spectrum is preserved under EA-equivalence. If F and G are EA-equivalent, then* $\mathrm{LBCT}_F(a,b,c) = \mathrm{LBCT}_G(\alpha_L,\beta_L,\gamma_L)$*, where* $\alpha_L = \mathcal{A}_{11}a, \beta_L = \mathcal{A}_{11}b$ *and* $\gamma_L = \mathcal{A}_{22}c + \mathcal{A}_{21}b$.

Proof Here, since $X+Y=b$, we can take $Y=X+b$, and write the second and third equations of the system of $\mathrm{LBCT}_F(a,b,c)$, respectively, as $F(X+a)+F(X+b+a)=c$ and $F(X)+F(X+b)=c$.

There exist $v,t \in \mathbb{F}_{2^n}$ such that $\begin{pmatrix}v\\ G(v)\end{pmatrix} = \mathcal{A}\begin{pmatrix}X+b\\ F(X+b)\end{pmatrix}$ and $\begin{pmatrix}t\\ G(t)\end{pmatrix} = \mathcal{A}\begin{pmatrix}X+b+a\\ F(X+b+a)\end{pmatrix}$. Similarly as in the proof of the previous theorem,

$$v = \mathcal{A}_{11}(X+b) + \mathcal{A}_{12}F(X+b) + C,$$
$$G(v) = \mathcal{A}_{21}(X+b) + \mathcal{A}_{22}F(X+b) + D,$$

gives that

$$F(X)+F(X+b)=c \Rightarrow G(y+\beta_L)+G(y)=\gamma_L,$$

where $\beta_L = \mathcal{A}_{12}c + \mathcal{A}_{11}b$ and $\gamma_L = \mathcal{A}_{22}c + \mathcal{A}_{21}b$.

From

$$t = \mathcal{A}_{11}(X+a+b) + \mathcal{A}_{12}F(X+a+b) + C,$$
$$G(t) = \mathcal{A}_{21}(X+a+b) + \mathcal{A}_{22}F(X+a+b) + D,$$

we obtain $F(X+a)+F(X+a+b)=c \Rightarrow G(y+\alpha_L)+G(y+\alpha_L+\beta_L)=\gamma_L$, where $\alpha_L = \mathcal{A}_{12}(F(X)+F(X+a)) + \mathcal{A}_{11}a$ and $\gamma_L = \mathcal{A}_{22}c + \mathcal{A}_{21}b$, $\beta_L = \mathcal{A}_{12}c + \mathcal{A}_{11}b$.

We see that, in general, α_L is not a constant. However, if $\mathcal{A}_{12}=0$ (i.e. EA-equivalence), we have that α_L is a constant. Therefore, if F and G are EA-equivalent, then $\mathrm{LBCT}_F(a,b,c) = \mathrm{LBCT}_G(\alpha_L,\beta_L,\gamma_L)$, where $\alpha_L = \mathcal{A}_{11}a, \beta_L = \mathcal{A}_{11}b$ and $\gamma_L = \mathcal{A}_{22}c + \mathcal{A}_{21}b$.

Finally,

$$\begin{pmatrix}\alpha_L\\ \beta_L\\ \gamma_L\end{pmatrix} = \begin{pmatrix}\mathcal{A}_{11} & 0 & 0\\ 0 & \mathcal{A}_{11} & 0\\ 0 & \mathcal{A}_{21} & \mathcal{A}_{22}\end{pmatrix}\begin{pmatrix}a\\ b\\ c\end{pmatrix} = \mathcal{C}\begin{pmatrix}a\\ b\\ c\end{pmatrix},$$

and, since $\mathcal{A}$ is invertible, the matrix $\mathcal{C}$ is also invertible. This concludes the proof. □

We use the same notations as in the previous two theorems.

Theorem 4.3 *The UBCT spectrum is preserved under affine equivalence. If F and G are affine equivalent, then* $\mathrm{UBCT}_F(a,b,c) = \mathrm{UBCT}_G(\alpha_U, \beta_U, \gamma_U)$*, where* $\alpha_U = \mathcal{A}_{11}a$, $\beta_U = \mathcal{A}_{22}b$ *and* $\gamma_U = \mathcal{A}_{22}c$.

Proof The relevant equations are here $F(X+a)+F(Y+a)=c$, $F(X)+F(Y)=c$ and $F(X)+F(X+a)=b$. As before,

$$F(X)+F(X+a)=b \Rightarrow G(y+\alpha_U)+G(y)=\beta_U,$$

where $\alpha_U = \mathcal{A}_{12}b + \mathcal{A}_{11}a$ and $\beta_U = \mathcal{A}_{22}b + \mathcal{A}_{21}a$.

Taking as before $\begin{pmatrix} y \\ G(y) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X \\ F(X) \end{pmatrix}$ and $\begin{pmatrix} u \\ G(u) \end{pmatrix} = \mathcal{A}\begin{pmatrix} X+a \\ F(X+a) \end{pmatrix}$, and taking now $\begin{pmatrix} y' \\ G(y') \end{pmatrix} = \mathcal{A}\begin{pmatrix} Y \\ F(Y) \end{pmatrix}$, $\begin{pmatrix} u' \\ G(u') \end{pmatrix} = \mathcal{A}\begin{pmatrix} Y+a \\ F(Y+a) \end{pmatrix}$, we obtain that

$$\begin{aligned}
y &= \mathcal{A}_{11}X + \mathcal{A}_{12}F(X) + C,\\
G(y) &= \mathcal{A}_{21}X + \mathcal{A}_{22}F(X) + D,\\
u &= \mathcal{A}_{11}(X+a) + \mathcal{A}_{12}F(X+a) + C,\\
G(u) &= \mathcal{A}_{21}(X+a) + \mathcal{A}_{22}F(X+a) + D,\\
y' &= \mathcal{A}_{11}Y + \mathcal{A}_{12}F(Y) + C,\\
G(y') &= \mathcal{A}_{21}Y + \mathcal{A}_{22}F(Y) + D,\\
u' &= \mathcal{A}_{11}(Y+a) + \mathcal{A}_{12}F(Y+a) + C,\\
G(u') &= \mathcal{A}_{21}(Y+a) + \mathcal{A}_{22}F(Y+a) + D.
\end{aligned}$$

Then,

$$G(y)+G(y') = \mathcal{A}_{21}(X+Y) + \mathcal{A}_{22}(F(X)+F(Y)) = \mathcal{A}_{21}(X+Y) + \mathcal{A}_{22}c = \gamma_U.$$

Here we see that, in general, γ_U is not constant. Similarly,

$$G(u)+G(u') = \mathcal{A}_{21}(X+Y) + \mathcal{A}_{22}(F(X+a)+F(Y+a)) = \mathcal{A}_{21}(X+Y) + \mathcal{A}_{22}c = \gamma_U.$$

However, if $\mathcal{A}_{21} = 0$, γ_U is constant. Under affine equivalence, $\mathcal{A}_{12} = \mathcal{A}_{21} = 0$, and $\mathrm{UBCT}_F(a,b,c) = \mathrm{UBCT}_G(\alpha_U, \beta_U, \gamma_U)$, with $\gamma_U = \mathcal{A}_{22}c$, $\beta_U = \mathcal{A}_{22}b$ and $\alpha_U = \mathcal{A}_{11}a$.

Finally,

$$\begin{pmatrix} \alpha_U \\ \beta_U \\ \gamma_U \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{11} & 0 & 0 \\ 0 & \mathcal{A}_{22} & 0 \\ 0 & 0 & \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \mathcal{D}\begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

and, since $\mathcal{A}$ is invertible, the matrix $\mathcal{D}$ is also invertible. This concludes the proof. □

The following example shows that the UBCT spectrum is in general not preserved under CCZ equivalence.

Example 4.4 Define $F(X) = X^9$ and $G(X) = X^9 + (X^8 + X)\mathrm{Tr}(X^9 + X)$ over $\mathbb{F}_{2^5}$. Budhagyan et al. [5] showed that while $F(X)$ and $G(X)$ are CCZ equivalent, they are not EA equivalent. Despite of them being CCZ equivalent, their UBCT spectrum differs. Notably, there are 992 tuples $(a,b,c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\mathrm{UBCT}_F(a,b,c) = 2$, while the number of tuples $(a,b,c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ for which $\mathrm{UBCT}_G(a,b,c) = 2$ is 982.

We now present an example illustrating that the UBCT spectrum is in general not even preserved under EA equivalence.

Example 4.5 Let $F(X) = X^5$ and $G(X) = X^5 + X$ be defined over $\mathbb{F}_{2^3}$. Notice that $F(X)$ is a permutation over $\mathbb{F}_{2^3}$ while $G(X)$ is a non-permutation over $\mathbb{F}_{2^3}$. Moreover, $F(X)$ and $G(X)$ are EA equivalent. However, the UBCT spectrum is not preserved under EA equivalence. Specifically, the number of tuples $(a, b, c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ for which $\mathrm{UBCT}_F(a, b, c) = 2$ is 448, whereas the number of tuples $(a, b, c) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $\mathrm{UBCT}_G(a, b, c) = 2$ is 452.

5 EBCT, LBCT and UBCT of a function in terms of its DDT

In this section, we present a general result that gives an intriguing connection between the EBCT, LBCT and UBCT entries of a differentially δ-uniform function F (not necessarily a permutation) with its DDT entries, and between the entries of the EBCT and the LBCT and the UBCT. It also includes a generalization of Lemma 2.8 to arbitrary functions (not necessarily permutations).

Theorem 5.1 *Let F be a differentially δ-uniform function on $\mathbb{F}_{2^n}$, and let $a, b, c, d \in \mathbb{F}_{2^n}$. Let $k \in \left\{1, 2, \ldots, \frac{\delta}{2}\right\}$. If $\mathrm{DDT}_F(a, b) = 2k$, we let $\{x_1, x_1 + a, x_2, x_2 + a, \ldots, x_k, x_k + a\}$ denote the distinct solutions of the equation $F(X + a) + F(X) = b$; if $\mathrm{DDT}_F(b, c) = 2k$, we let $\{y_1, y_1 + b, y_2, y_2 + b, \ldots, y_k, y_k + b\}$ denote the distinct solutions of the equation $F(X + b) + F(X) = c$; if $\mathrm{DDT}_F(c, d) = 2k$, let $\{z_1, z_1 + c, z_2, z_2 + c, \ldots, z_k, z_k + c\}$ be the distinct solutions of the equation $F(X + c) + F(X) = d$. Then, we have*

$$\mathrm{EBCT}_F(a, b, c, d) = \begin{cases} \mathrm{DDT}_F(a, b) & \text{if } c = d = 0, \\ \mathrm{DDT}_F(c, d) & \text{if } ac \neq 0, a = c \text{ and } b = d; \text{ or } a = 0, b = 0 \text{ and } c \neq 0, \\ 4\ell & \text{if } a \neq c, ac \neq 0 \text{ and } \mathrm{DDT}_F(c, d) = 2k = 4r \text{ or } 4r + 2, \\ & \text{where } r > 0 \text{ is an integer,} \\ & 1 \leq \ell \leq r \text{ is the largest integer such that} \\ & (a, b) \in U(i_1, j_1) \cap U(i_2, j_2) \cap \cdots \cap U(i_\ell, j_\ell), \\ & 1 \leq i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \leq k \text{ are distinct integers,} \\ 0 & \text{otherwise,} \end{cases}$$

where $U(i, j) = \{\left(z_i + z_j, F(z_i) + F(z_j)\right), \left(z_i + z_j + c, F(z_i) + F(z_j) + d\right) \mid 1 \leq i \neq j \leq k\} \subseteq \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. Moreover, we have

$$\mathrm{LBCT}_F(a, b, c) = \begin{cases} \mathrm{DDT}_F(b, c) & \text{if } b = c = 0; \text{ or } a = b \text{ and } ab \neq 0; \text{ or } a = 0 \text{ and } b \neq 0, \\ 4\ell & \text{if } a \neq b, ab \neq 0 \text{ and } \mathrm{DDT}_F(b, c) = 2k = 4r \text{ or } 4r + 2, \\ & \text{where } r > 0 \text{ is an integer,} \\ & 1 \leq \ell \leq r \text{ is the largest integer such that} \\ & a \in V(i_1, j_1) \cap V(i_2, j_2) \cap \cdots \cap V(i_\ell, j_\ell), \\ & 1 \leq i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \leq k \text{ are distinct integers,} \\ 0 & \text{otherwise,} \end{cases}$$

where $V(i,j) = \{y_i + y_j, y_i + y_j + b \mid 1 \le i \ne j \le k\} \subseteq \mathbb{F}_{2^n}^*$. *Finally,*

$$\mathrm{UBCT}_F(a,b,c) = \begin{cases} |F^{-1}(c + \mathrm{Im}(F))| & \text{if } a = b = 0, \\ \mathrm{DDT}_F(a,b) & \text{if } b = c \text{ and } a \ne 0, \\ 4\ell & \text{if } c \ne b, a \ne 0 \text{ and } \mathrm{DDT}_F(a,b) = 2k = 4r \text{ or } 4r+2, \\ & \text{where } r > 0 \text{ is an integer,} \\ & 1 \le \ell \le r \text{ is the largest integer such that} \\ & c \in W(i_1,j_1) \cap W(i_2,j_2) \cap \cdots \cap W(i_\ell, j_\ell), \\ & 1 \le i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \le k \text{ are distinct integers,} \\ 0 & \text{otherwise,} \end{cases}$$

where $W(i,j) = \{F(x_i) + F(x_j), F(x_i) + F(x_j) + b \mid 1 \le i \ne j \le k\} \subseteq \mathbb{F}_{2^n}^*$, $\mathrm{Im}(F)$ *is the image of* F *and* $F^{-1}(\cdot)$ *denotes the preimage of the argument.*

Proof It is easy to see that if X is a solution to System (3.1) at (a,b,c) (here and throughout, for easy writing, we refer to the system in the definition of such a cardinality ($\star$) as System ($\star$)), then $\{X, X+c, X+a, X+a+c\}$ are solutions of $F(X) + F(X+c) = d$. Since F is differentially δ-uniform, the equation $F(X) + F(X+c) = d$ can have zero or $2k$ solutions, where $k \in \left\{1, 2, \ldots, \frac{\delta}{2}\right\}$. If $\mathrm{DDT}_F(c,d) = 0$, then System (3.1) has no solutions, and therefore $\mathrm{EBCT}_F(a,b,c,d) = 0$.

Furthermore, it is straightforward to observe that if $a = 0$ (or $c = 0$), then System (3.1) has a solution only when $b = 0$ (or $d = 0$, respectively) and otherwise, no solution. We can now divide the proof into the following five cases as follows

Case 1 If $a = c = 0$, then $b = d = 0$. Therefore for $a = b = c = d = 0$, we get $\mathrm{EBCT}_F(a,b,c,d) = 2^n = \mathrm{DDT}_F(0,0)$.

Case 2 If $a \ne 0, c = d = 0$, we obtain $\mathrm{EBCT}_F(a,b,c,d) = \mathrm{DDT}_F(a,b)$.

Case 3 If $a = b = 0, c \ne 0$, then $\mathrm{EBCT}_F(a,b,c,d) = \mathrm{DDT}_F(c,d)$.

Case 4 If $a = c$ and $ac \ne 0$ then from the first two equations in System (3.1), we obtain $b = d$. Thus, $a = c$ and $b = d$ imply that $\mathrm{EBCT}_F(a,b,c,d) = \mathrm{DDT}_F(c,d)$.

It is easy to observe that when $\mathrm{DDT}_F(c,d) = 2$, System (3.1) will have a solution only if $a = c$ or $a = 0$.

Case 5 Let $a \ne c, ac \ne 0$ and $\mathrm{DDT}_F(c,d) = 2k$, where solutions of $F(X) + F(X+c) = d$ are from the set $S(c,d) := \{z_1, z_2, \ldots, z_k, z_1 + c, z_2 + c, \ldots, z_k + c\}$. Due to the second equation in System (3.1), all solutions of this system must necessarily come from $S(c,d)$ itself. It follows that if z_i is solution to System (3.1), then from the third equation, we have $z_i + a \in S(c,d) \setminus \{z_i, z_i + c\}$, or equivalently, $a \in z_i + S(c,d) \setminus \{z_i, z_i + c\}$. Furthermore, from the first equation, we have $b = F(z_i) + F(z_i + a)$. We consider the following set in $\mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$,

$$U(i,j) = \{\big(z_i + z_j, F(z_i) + F(z_j)\big), \big(z_i + z_j + c, F(z_i) + F(z_j) + d\big) \mid 1 \le i \ne j \le k\}.$$

It easy to check that $z_i, z_j, z_i + c, z_j + c$ are four distinct solutions of System (3.1) if and only if $(a,b) \in U(i,j)$. Note that for a given pair $(a,b) \in U(i,j)$, there may be additional solutions to System (3.1) beyond these four. Thus, we have $\mathrm{EBCT}_F(a,b,c,d) \ge 4$ if $(a,b) \in U(i,j)$ and $\mathrm{DDT}_F(c,d) = 2k$. For $k \ge 4$ and $1 \le i_1 \ne j_1 \ne i_2 \ne j_2 \le k$, let $(a,b) \in U(i_1,j_1)$ and $(a',b') \in U(i_2,j_2)$. If $(a,b) = (a',b')$, then System (3.1) has at least eight solutions, namely, $z_{i_1}, z_{i_2}, z_{j_1}, z_{j_2}, z_{i_1} + c, z_{i_2} + c, z_{j_1} + c, z_{j_2} + c$; otherwise, it will have at least four solutions. Following a similar argument, it is clear that if the pairs (a,b) are equal for three different $U(i,j)$, then System (3.1) will have at least twelve solutions. However, this process must eventually stop, depending on the value of $\mathrm{DDT}_F(c,d)$, which we will describe below.

Depending on whether $2k \equiv 0 \pmod 4$ or $2k \equiv 2 \pmod 4$, we can express $\mathrm{DDT}_F(c,d)$ as $\mathrm{DDT}_F(c,d) = 4r$ or $\mathrm{DDT}_F(c,d) = 4r+2$, respectively, where $r \geq 0$ is an integer. The case $k = 1$ has already been addressed in Case 1. For $k = 2$ or $k = 3$, we have $\mathrm{EBCT}_F(a,b,c,d) \in \{0,4\}$. Now we consider the case $k \geq 4$. Let $1 \leq \ell \leq r$ be the largest integer for which there are distinct integers $i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \in \{1,2,\ldots,k\}$ such that $(a,b) \in U(i_1,j_1) \cap U(i_2,j_2) \cap \cdots \cap U(i_\ell,j_\ell)$, then System (3.1) will have 4ℓ solutions. This proves the result for the EBCT.

Next, we compute the LBCT entries at (a,b,c) for a function F, using System (3.2). If $(X,Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfies System (3.2), then $Y = X+b$ and $\{X, X+b, X+a, X+a+b\}$ are solutions of $F(X)+F(X+b) = c$. As F is differentially δ-uniform, the equation $F(X)+F(X+b) = c$ can have zero or $2k$ solutions, where $k \in \left\{1,2,\ldots,\frac{\delta}{2}\right\}$. Clearly, when $\mathrm{DDT}_F(b,c) = 0$, System (3.2) has no solutions, and therefore $\mathrm{LBCT}_F(a,b,c) = 0$.

Notice that for $b = 0$, System (3.2) has a solution only if $c = 0$ and otherwise, no solution. Moreover, for $b = c = 0$, System (3.2) has 2^n solutions ($= \mathrm{DDT}_F(b,c)$) regardless of whether $a = 0$ or $a \neq 0$. We will now split our analysis into the following cases when $b \neq 0$:

Case 1 Let $a = 0, b \neq 0$, then $\mathrm{LBCT}_F(a,b,c) = \mathrm{DDT}_F(b,c)$.

Case 2 Consider $a = b, ab \neq 0$, then $\mathrm{LBCT}_F(a,b,c) = \mathrm{DDT}_F(b,c)$.

Further, one can see that if $\mathrm{DDT}_F(b,c) = 2$, System (3.2) will have a solution only if $a = b$ or $a = 0$.

Case 3 Next, consider $a \neq b, ab \neq 0$ and $\mathrm{DDT}_F(b,c) = 2k$, where solutions of $F(X)+F(X+b) = c$ are from the set $S(b,c) := \{y_1, y_2, \ldots, y_k, y_1+b, y_2+b, \ldots, y_k+b\}$. If $X = y_i$ is solution to System (3.2), then first equation implies that $Y = y_i+b$ and the second equation implies that $y_i + a \in S(b,c) \setminus \{y_i, y_i+b\}$, or equivalently, $a \in y_i + S(b,c) \setminus \{y_i, y_i+b\}$. We now consider the following set

$$V(i,j) = \{y_i + y_j, y_i + y_j + b \mid 1 \leq i \neq j \leq k\} \subseteq \mathbb{F}_{2^n}^*.$$

One can verify that $(y_i, y_i+b), (y_j, y_j+b), (y_i+b, y_i), (y_j+b, y_j)$ are four distinct solutions of System (3.2) if and only if $a \in V(i,j)$. Therefore, $\mathrm{LBCT}_F(a,b,c) \geq 4$ if $a \in V(i,j)$ and $\mathrm{DDT}_F(b,c) = 2k$. For $k \geq 4$ and $1 \leq i_1 \neq j_1 \neq i_2 \neq j_2 \leq k$, let $a \in V(i_1,j_1)$ and $a' \in V(i_2,j_2)$. If $a = a'$, then System (3.2) has at least eight solutions, namely, $(y_{i_1}, y_{i_1}+b), (y_{j_1}, y_{j_1}+b), (y_{i_1}+b, y_{i_1}), (y_{j_1}+b, y_{j_1}), (y_{i_2}, y_{i_2}+b), (y_{j_2}, y_{j_2}+b), (y_{i_2}+b, y_{i_2}), (y_{j_2}+b, y_{j_2})$; otherwise, it will have at least four solutions. Following a similar argument as in the case of the EBCT, this process must stop somewhere, depending on the value of $\mathrm{DDT}_F(b,c)$.

Again, we can take $\mathrm{DDT}_F(b,c) = 2k \in \{4r, 4r+2\}$, where r is a non-negative integer. We have already discussed the case $k = 1$ in Case 1. For $k = 2,3$, one can see that $\mathrm{LBCT}_F(a,b,c) \in \{0,4\}$. Let us now assume that $k \geq 4$. Let $1 \leq \ell \leq r$ be the largest integer for which there are distinct integers $i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \in \{1,2,\ldots,k\}$ such that $a \in V(i_1,j_1) \cap V(i_2,j_2) \cap \cdots \cap V(i_\ell,j_\ell)$, then System (3.2) will have 4ℓ solutions. This completes the proof for the LBCT.

Finally, we deal with the UBCT at (a,b,c) of a function F by analyzing System (3.3). It is immediate that $F(X)+F(X+a) = F(Y)+F(Y+a) = b$ from the equations of System (3.3). Moreover, $F(X)+F(X+a) = b$ can have zero or $2k$ solutions, where $k \in \left\{1,2,\ldots,\frac{\delta}{2}\right\}$, as F is differentially δ-uniform. Clearly, if $\mathrm{DDT}_F(a,b) = 0$, then System (3.3) has no solutions, and therefore $\mathrm{UBCT}_F(a,b,c) = 0$. Let elements of $S(a,b) := \{x_1, x_2, \ldots, x_k, x_1+a, x_2+a, \ldots, x_k+a\}$ be the solution set of $F(X)+F(X+a) = b$. Next, we consider the following cases:

Case 1 If $a = 0, b \neq 0$, then $\mathrm{UBCT}_F(a,b,c) = 0$.

Case 2 Let $a = b = 0$, $\mathrm{Im}(F) = \{t \in \mathbb{F}_{2^n} \mid \exists\ u \in \mathbb{F}_{2^n}$ satisfying $F(u) = t\}$, and $c + \mathrm{Im}(F) = \{c + t \mid t \in \mathrm{Im}(F)\}$. Then, $\mathrm{UBCT}_F(0, 0, c) = |F^{-1}(c + \mathrm{Im}(F))|$, the cardinality of the preimage of $c + \mathrm{Im}(F)$.
Case 3 If $b = c$ and $a \neq 0$, System (3.3) reduces to

$$\begin{cases} F(X + a) + F(Y + a) = b \\ F(X) + F(Y) = b \\ F(X) + F(X + a) = b. \end{cases}$$

Let $X \in S(a, b)$. Then, $(X, X + a)$ is a solution of the above system. On the other hand, if $X \notin S(a, b)$, then there does not exist any $Y \in \mathbb{F}_{2^n}$ such that (X, Y) is a solution of the above system. Therefore, $\mathrm{UBCT}(a, b, c) = \mathrm{DDT}_F(a, b)$.

If $\mathrm{DDT}_F(a, b) = 2$, then, $S(a, b) := \{x_1, x_1 + a\}$. Without loss of generality, let $X = x_1$. Since $\{X, X + a, Y, Y + a\}$ be solutions of $F(X) + F(X + a) = b$, and since $a \neq 0$, we have that $Y = x_1$ or $Y = x_1 + a$. If $Y = x_1$ and $c \neq 0$, this yields a contradiction (note that, if $c = 0$, we get that (x_1, x_1) and $(x_1 + a, x_1 + a)$ are solutions of the system, and therefore $\mathrm{UBCT}(a, b, c) = \mathrm{DDT}_F(a, b)$). If $Y = x_1 + a$, this yields a contradiction unless $b = c$. Therefore, if $\mathrm{DDT}_F(a, b) = 2$, then System (3.3) has a solution only if $c = 0$ or $b = c$.
Case 4 Now assume that $b \neq c$, $a \neq 0$, and $\mathrm{DDT}_F(a, b) = 2k$, where $k \in \{2, 3, \cdots, \delta/2\}$. For any $X \in S(a, b)$, we have that (X, X) cannot be a solution of System (3.3) unless $c = 0$; similarly, $(X, X + a)$ cannot be a solution of System (3.3) unless $c = b$, which is excluded.

Therefore for $X = x_i \in S(a, b)$, if there exist $Y \in S(a, b) \setminus \{x_i, x_i + a\}$ such that $c = F(x_i) + F(Y) = F(x_i + a) + F(Y + a)$, then (X, Y) is a solution of System (3.3). We now consider the set

$$W(i, j) = \left\{F(x_i) + F(x_j),\ F(x_i) + F(x_j) + b \mid 1 \leq i \neq j \leq k\right\} \subseteq \mathbb{F}_{2^n}^*.$$

It is easy to observe that (x_{i_1}, x_{j_1}), $(x_{i_1} + a, x_{j_1} + a)$, (x_{j_1}, x_{i_1}), $(x_{j_1} + a, x_{i_1} + a)$ are four distinct solutions of System (3.3) if and only if $c \in W(i_1, j_1)$. It is important to see that for a given $c \in W(i_1, j_1)$, there can be more than four solutions to System (3.3), except for these four.

By following a similar analysis as done in the case of the EBCT and LBCT, depending on the value of the DDT entries, we can compute the UBCT entries of F. We can write that $\mathrm{DDT}_F(a, b) = 2k \in \{4r, 4r + 2\}$, where $r \geq 0$ is an integer. If $k = 1$, then using Case 1, we are done, and if $k = 2, 3$, we have $\mathrm{UBCT}_F(a, b, c) \in \{0, 4\}$. Assume that $k \geq 4$. Let $1 \leq \ell \leq r$ be the largest integer for which there are distinct integers $i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \in \{1, 2, \ldots, k\}$ such that $c \in W(i_1, j_1) \cap W(i_2, j_2) \cap \cdots \cap W(i_\ell, j_\ell)$, then System (3.3) will have 4ℓ solutions. This proves the result for the UBCT. □

We now give an example depicting the above Theorem 5.1.

Example 5.2 Let $F(X) = X^{11}$, which is a permutation over $\mathbb{F}_{2^6}$. Let $c = g, d = g^{11}$, where g is primitive element of $\mathbb{F}_{2^6}$. Here, $\mathrm{DDT}_F(c, d) = 10$ and $S(c, d) = \{z_1 = g, z_2 = g^{10}, z_3 = g^{19}, z_4 = g^{22}, z_5 = g^{46}, z_1 + c = 0, z_2 + c = g^{28}, z_3 + c = g^{55}, z_4 + c = g^{43}, z_5 + c = g^{37}\}$. If $i_1 = 1$ and $j_1 = 3$, then for $(a, b) = \left(z_{i_1} + z_{j_1}, F(z_{i_1}) + F(z_{j_1})\right) = (g^{55}, g^{38}) \in U(i_1, j_1)$, we are interested in computing the largest integer $1 \leq \ell \leq 2$ such that $(a, b) \in U(1, 3) \cap U(i_2, j_2) \cap \cdots \cap U(i_\ell, j_\ell)$, where $i_2, i_3, \cdots, i_\ell, j_2, j_3, \cdots, j_\ell \in \{2, 4, 5\}$ are distinct integers. In this example, ℓ is indeed 2. This is because when $i_2 = 2$ and $j_2 = 5$, we get $z_{i_1} + z_{j_1} = z_{i_2} + z_{j_2}$ and $F(z_{i_1}) + F(z_{j_1}) = F(z_{i_2}) + F(z_{j_2})$. Consequently, we have $(a, b) \in U(1, 3) \cap U(2, 5)$, rendering $\mathrm{EBCT}_F(a, b, c, d) = 4\ell = 8$. It also follows

that $(a', b') = (z_{i_1} + z_{i_2} + c, F(z_{i_1}) + F(z_{i_2}) + d) = (g^{19}, g^{20}) \in U(1,3) \cap U(2,5)$, or equivalently for $a' = g^{19}$ and $b' = g^{20}$, we have $\mathrm{EBCT}_F(a', b', c, d) = 8$.

However, $\mathrm{DDT}_F(b, c) = 2$ and $a \neq b$, which gives that $\mathrm{LBCT}_F(a, b, c) = 0$. Moreover, $\mathrm{DDT}_F(a, b) = 10$, and $S(a, b) = \{x_1 = g, x_2 = g^{10}, x_3 = g^{13}, x_4 = g^{28}, x_5 = g^{55}, x_1 + a = g^{19}, x_2 + a = g^{46}, x_3 + a = g^{34}, x_4 + a = g^{37}, x_5 + a = 0\}$. Then, one can check that $c \neq b$ and furthermore, $c \notin W(i, j)$ for all $i \neq j \in \{1, 2, 3, 4\}$, implying that $\mathrm{UBCT}_F(a, b, c) = 0$.

Next, we provide a characterization of the EBCT entries of a differentially δ-uniform function F in terms of UBCT and LBCT entries of F, and vice versa.

Theorem 5.3 *Let F be a function on $\mathbb{F}_{2^n}$. Given any $a, b, c, d \in \mathbb{F}_{2^n}$, the following statements are equivalent:*

(i) $x_0 \in S(c, d) + a$ *is a solution of the system of* $\mathrm{EBCT}_F(a, b, c, d)$.
(ii) $(x_0, x_0 + c)$ *is a solution of the system of* $\mathrm{LBCT}_F(a, c, d)$ and $b = F(x_0) + F(x_0 + a)$.
(iii) $(x_0, x_0 + a)$ *is a solution of the system of* $\mathrm{UBCT}_F(c, d, b)$ (note that this is only possible if $x_0 + a \in S(c, d)$).

Proof We have that

$$\mathrm{EBCT}_F(a, b, c, d) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \begin{cases} (1)\ F(X) + F(X + a) = b \\ (2)\ F(X) + F(X + c) = d \\ (3)\ F(X + a + c) + F(X + a) = d \end{cases} \right\} \right|.$$

On the other hand (replacing the input (a, b, c) by (a, c, d)),

$$\mathrm{LBCT}_F(a, c, d) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists\, Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} (4)\ X + Y = c \\ (5)\ F(X + a) + F(Y + a) = d \\ (6)\ F(X) + F(Y) = d \end{cases} \right\} \right|.$$

By Eq. (4), $Y = X + c$, and we can rewrite Eqs. (5) and (6) as $F(X + a) + F(X + a + c) = d$ and $F(X) + F(X + c) = d$. Since these are, respectively, Eqs. (2) and (3), then, it is clear that x_0 is a solution of the system of $\mathrm{EBCT}_F(a, b, c, d)$ if and only if $(x_0, x_0 + c)$ is a solution of the system of $\mathrm{LBCT}_F(a, c, d)$ and $b = F(x_0) + F(x_0 + a)$.

Furthermore, (replacing the input (a, b, c) by (c, d, b)),

$$\mathrm{UBCT}_F(c, d, b) = \left| \left\{ X \in \mathbb{F}_{2^n} \middle| \exists\, Y \in \mathbb{F}_{2^n} \text{ with } \begin{cases} (7)\ F(X + c) + F(Y + c) = b \\ (8)\ F(X) + F(Y) = b \\ (9)\ F(X) + F(X + c) = d \end{cases} \right\} \right|.$$

Note that Eq. (9) is identical to Eq. (2).

Taking $Y = X + a$, we obtain from Eqs. (7) and (8), $F(X + c) + F(X + a + c) = b$, respectively, $F(X) + F(X + a) = b$. Note that the second equation is identical to Eq. (1). Adding the two equations, we obtain: $F(X) + F(X + c) = F(X + a) + F(X + a + c)$, which, together with Eq. (2), renders $F(X + a) + F(X + a + c) = d$, that is, Eq. (3). From here, we obtain that x_0 is a solution of the system of $\mathrm{EBCT}_F(a, b, c, d)$ if and only if $(x_0, x_0 + a)$ is a solution of the system of $\mathrm{UBCT}_F(c, d, b)$. Note that this forces $x_0 + a \in S(c, d)$, given Eqs. (2) and (3). □

6 Consequences of our results for APN functions

We first state the EBCT, LBCT and UBCT entries of an APN function F and give these entries in terms of the DDT entries of F. It is known that $H(X) = X^{-1}$ over $\mathbb{F}_{2^n}$, where n is odd, is an APN function and the authors in [13, 17] have computed its EBCT, LBCT and UBCT entries, which turns out to be a special case of the following result.

Corollary 6.1 *If F is an APN function over $\mathbb{F}_{2^n}$, then for $a, b, c, d \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_F(a,b,c,d) = \begin{cases} \mathrm{DDT}_F(a,b) & \text{if } c = d = 0, \\ \mathrm{DDT}_F(c,d) & \text{if } ac \neq 0, a = c \text{ and } b = d; \text{ or } a = 0, b = 0 \text{ and } c \neq 0, \\ 0 & \text{otherwise}, \end{cases}$$

$$\mathrm{LBCT}_F(a,b,c) = \begin{cases} \mathrm{DDT}_F(b,c) & \text{if } b = c = 0; \text{ or } a = b \text{ and } ab \neq 0; \text{ or } a = 0 \text{ and } b \neq 0, \\ 0 & \text{otherwise}, \end{cases}$$

$$\mathrm{UBCT}_F(a,b,c) = \begin{cases} |F^{-1}(c + \mathrm{Im}(F))| & \text{if } a = 0 \text{ and } b = 0, \\ \mathrm{DDT}_F(a,b) & \text{if } c = b \text{ and } a \neq 0, \\ 0 & \text{otherwise}, \end{cases}$$

where $\mathrm{Im}(F)$ is the image of F and $F^{-1}(\cdot)$ denotes the preimage of the argument.

Proof The proof of this corollary is straightforward from Theorem 5.1, by setting $\delta = 2$. □

Corollary 6.2 *For any $a, b, c, d \in \mathbb{F}_{2^n}$, $(\mathrm{EBCT}_F(a,b,c,d))^2 \leq \mathrm{LBCT}_F(a,c,d) \cdot \mathrm{UBCT}_F(c,d,b)$. Furthermore, the equality is met for every $a, b, c, d \in \mathbb{F}_{2^n}^*$ if and only if F is APN.*

Proof The inequality follows directly from Theorem 5.3. Suppose that F is APN. Then, by Corollary 6.1, $(\mathrm{EBCT}_F(a,b,c,d))^2 = \mathrm{LBCT}_F(a,c,d) \cdot \mathrm{UBCT}_F(c,d,b)$. Suppose now that F is not APN. Then, for some $c, d \in \mathbb{F}_{2^n}^*$, there exist at least four distinct solutions of the equation $F(X + c) + F(X) = d$, which we denote by $z_1, z_2, z_1 + c, z_2 + c$. Let now $a = z_1 + z_2, b = F(z_1) + F(z_2) + d$. Then, since $a \neq c$ (otherwise $z_2 = z_1 + c$), $(\mathrm{EBCT}_F(a,b,c,d))^2 < \mathrm{LBCT}_F(a,c,d) \cdot \mathrm{UBCT}_F(c,d,b)$. □

7 Consequences of our results for some well-known functions

In this section, we will give the EBCT, LBCT and UBCT entries of the Gold, Kasami and Bracken–Leander functions for those parameters such that the functions are differentially 4-uniform permutations; in the case of the Gold function, we also state and prove the EBCT, LBCT and UBCT entries for any parameters. We can also give a very short proof for the EBCT, LBCT and UBCT entries of the inverse function for n even, which is the main result in [13, 17] (for n odd, see the previous section).

For clarity, we first state the results we will use to compute the EBCT, LBCT and UBCT entries of differentially 4-uniform functions using Theorems 5.1 and 5.3, which we will need for the functions in this section.

Corollary 7.1 *Let F be a differentially 4-uniform function over $\mathbb{F}_{2^n}$. Then, for $a, b, c, d \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_F(a,b,c,d) = \begin{cases} \mathrm{DDT}_F(a,b) & \text{if } c=d=0, \\ \mathrm{DDT}_F(c,d) & \text{if } ac\neq 0, a=c \text{ and } b=d; \text{ or } a=0, b=0 \text{ and } c\neq 0; \text{ or} \\ & \mathrm{DDT}_F(c,d)=4, a=z_1+z_2 \text{ and } b=F(z_1)+F(z_2); \text{ or} \\ & \mathrm{DDT}_F(c,d)=4, a=z_1+z_2+c \text{ and } b=F(z_2)+F(z_2+c), \\ 0 & \text{otherwise}, \end{cases}$$

where z_1, z_1+c, z_2, z_2+c *are the four solutions of the equation* $F(X+c)+F(X)=d$, *if* $\mathrm{DDT}_F(c,d)=4$. *Next,*

$$\mathrm{LBCT}_F(a,b,c) = \begin{cases} \mathrm{DDT}_F(b,c) & \text{if } b=c=0; \text{ or } a=0 \text{ and } b\neq 0; \text{ or} \\ & \mathrm{DDT}_F(b,c)=2, a=b \text{ and } ab\neq 0; \text{ or} \\ & \mathrm{DDT}_F(b,c)=4, ab\neq 0 \text{ and } a\in\{b, y_1+y_2, y_1+y_2+b\}, \\ 0 & \text{otherwise}, \end{cases}$$

where y_1, y_1+b, y_2, y_2+b *are the four solutions of the equation* $F(X+b)+F(X)=c$, *if* $\mathrm{DDT}_F(b,c)=4$. *Further,*

$$\mathrm{UBCT}_F(a,b,c) = \begin{cases} |F^{-1}(c+\mathrm{Im}(F))| & \text{if } a=b=0, \\ \mathrm{DDT}_F(a,b) & \text{if } \mathrm{DDT}_F(a,b)=2, a\neq 0 \text{ and } c=b; \text{ or} \\ & \mathrm{DDT}_F(a,b)=4, a\neq 0 \text{ and} \\ & c\in\{b, F(x_1)+F(x_2), F(x_1)+F(x_2)+b\}, \\ 0 & \text{otherwise}, \end{cases}$$

where x_1, x_1+a, x_2, x_2+a *are the four solutions of the equation* $F(X+a)+F(X)=b$, *if* $\mathrm{DDT}_F(a,b)=4$, $\mathrm{Im}(F)$ *is the image of* F *and* $F^{-1}(\cdot)$ *denotes the preimage of the argument.*

Proof The proof directly follows from Theorem 5.1 by taking $\delta=4$. □

Here, we give an alternative characterization of EBCT of a differentially 4-uniform function F using LBCT and UBCT of F.

Corollary 7.2 *Let* F *be a differentially* 4*-uniform function over* $\mathbb{F}_{2^n}$. *Let* $A = \{(a,c,d) \mid \exists\, b \text{ with } \mathrm{EBCT}_F(a,b,c,d)=4\}$ *and* $B = \{(c,d,b) \mid \exists\, a \text{ with } \mathrm{EBCT}_F(a,b,c,d)=4\}$. *Let* $a,b,c,d\in\mathbb{F}_{2^n}^*$. *Then,* $\mathrm{EBCT}_F(a,b,c,d)=2$ *if and only if* $\mathrm{LBCT}_F(a,c,d)=\mathrm{UBCT}_F(c,d,b)=2$. *Furthermore,* $(a,c,d)\in A$ *if and only if* $\mathrm{LBCT}_F(a,c,d)=4$, *and* $(c,d,b)\in B$ *if and only if* $\mathrm{UBCT}_F(c,d,b)=4$.

Proof Let F be differentially 4-uniform. Then, since $cd\neq 0$, either $\mathrm{DDT}_F(c,d)=0$, $\mathrm{DDT}_F(c,d)=2$ or $\mathrm{DDT}_F(c,d)=4$. One can now proof the result directly from Theorem 5.3. □

We will here use Corollaries 7.1 and 7.2 to compute the concrete values for three infinite classes of differentially 4-uniform power permutations over $\mathbb{F}_{2^n}$ (Table 1) having the best known nonlinearity. For the Gold function, using Theorem 5.1, we will state and prove the result for general parameters, including those for which the Gold function is 4-differential uniform.

We first consider the Gold function $F_1(X)=X^{2^s+1}$, a differentially 2^t-uniform function over $\mathbb{F}_{2^n}$, where $t=\gcd(s,n)$ and compute its EBCT, LBCT and UBCT entries. We will use the relative trace in the following way. For a general s, we do not have in general that $\mathbb{F}_{2^s}\subseteq\mathbb{F}_{2^n}$. However, we can naturally embed the elements of $\mathbb{F}_{2^n}$ in $\mathbb{F}_{2^{sm}}$, since $m=\frac{n}{\gcd(s,n)}$. Then, $\sum_{i=0}^{m-1}\alpha^{2^{si}}=\mathrm{Tr}_s^{sm}(\alpha)$.

Table 1 Differentially 4-uniform permutations X^d over $\mathbb{F}_{2^n}$

Family	d	Condition	LBCT/UBCT
Inverse	2^n-2	$n=2k, k>1$	[13, 17]
Gold	2^s+1	$n=2k$, k odd, $\gcd(s,n)=2$	This paper[a]
Kasami	$2^{2s}-2^s+1$	$n=2k$, k odd, $\gcd(s,n)=2$	This paper
Bracken–Leander	$2^{2s}+2^s+1$	$n=4s$, s odd	This paper

[a]Shown for general parameters

Corollary 7.3 *Let $F_1(X)=X^{2^s+1}$ be the Gold function on $\mathbb{F}_{2^n}$, $1\le s<n$. Let $t=\gcd(s,n)$, and $m=\frac{n}{t}$. Then for $a,b,c,d\in\mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_{F_1}(a,b,c,d)=\begin{cases}2^n & \text{if } a=b=c=d=0,\\ 2^t & \text{if } \mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), c=d=0 \text{ and } a\neq 0; \text{ or}\\ & \mathrm{Tr}_s^{sm}\left(\frac{d}{c^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), a=b=0 \text{ and } c\neq 0; \text{ or}\\ & \mathrm{Tr}_s^{sm}\left(\frac{d}{c^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), a=c, b=d \text{ and } ac\neq 0; \text{ or}\\ & \mathrm{Tr}_s^{sm}\left(\frac{d}{c^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), a=uc, ac\neq 0 \text{ and}\\ & b=(u+u^2)c^{2^s+1}+ud, \text{ where } u\in\mathbb{F}_{2^t}^*\setminus\{1\},\\ 0 & \text{otherwise,}\end{cases}$$

$$\mathrm{LBCT}_{F_1}(a,b,c)=\begin{cases}2^n & \text{if } b=c=0,\\ 2^t & \text{if } \mathrm{Tr}_s^{sm}\left(\frac{c}{b^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), a=0 \text{ and } b\neq 0; \text{ or}\\ & \mathrm{Tr}_s^{sm}\left(\frac{c}{b^{2^s+1}}\right)=\mathrm{Tr}_1^m(1), a\in b\mathbb{F}_{2^t}^* \text{ and } ab\neq 0,\\ 0 & \text{otherwise,}\end{cases}$$

$$\mathrm{UBCT}_{F_1}(a,b,c)=\begin{cases}|F_1^{-1}(c+\mathrm{Im}(F_1))| & \text{if } a=b=0,\\ 2^t & \text{if } a\neq 0, \mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right)=\mathrm{Tr}_1^m(1) \text{ and}\\ & c\in\{b,(u+u^2)a^{2^s+1}+ub, u\in\mathbb{F}_{2^t}^*\setminus\{1\}\},\\ 0 & \text{otherwise,}\end{cases}$$

where $\mathrm{Im}(F_1)$ is the image of F_1 and $F_1^{-1}(\cdot)$ denotes the preimage of the argument. In particular when F_1 is a permutation or equivalently when m is odd, then $|F_1^{-1}(c+\mathrm{Im}(F_1))|=2^n$.

Proof By Theorem 5.1, we have

$$\mathrm{EBCT}_{F_1}(a,b,c,d)=\begin{cases}\mathrm{DDT}_{F_1}(a,b) & \text{if } c=d=0,\\ \mathrm{DDT}_{F_1}(c,d) & \text{if } ac\neq 0, a=c \text{ and } b=d; \text{ or } a=b=0 \text{ and } c\neq 0,\\ 4\ell & \text{if } a\neq c, ac\neq 0 \text{ and } \mathrm{DDT}_{F_1}(c,d)=2k=4r \text{ or } 4r+2,\\ & \text{where } r>0 \text{ is an integer,}\\ & 1\le\ell\le r \text{ is the largest integer such that}\\ & (a,b)\in U(i_1,j_1)\cap U(i_2,j_2)\cap\cdots\cap U(i_\ell,j_\ell),\\ & 1\le i_1,i_2,\ldots,i_\ell,j_1,j_2,\ldots,j_\ell\le k \text{ are distinct integers,}\\ 0 & \text{otherwise,}\end{cases}$$

where $U(i,j) = \{(z_i + z_j, F_1(z_i) + F_1(z_j)), (z_i + z_j + c, F_1(z_i) + F_1(z_j) + d) \mid 1 \le i \ne j \le k\} \subseteq \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ and the set $S(c,d) = \{z_1, z_1+c, z_2, z_2+c, \ldots, z_k, z_k+c\}$ consists of $2k$ solutions of the equation $F_1(X+c) + F_1(X) = d$ when $\mathrm{DDT}_{F_1}(c,d) = 2k$.

It is known from [2, Lemma 4] and [10] that $X^{2^s+1} + (X+c)^{2^s+1} = d$ has 2^t distinct solutions if and only if $\sum_{i=0}^{m-1} D^{2^{si}} = m \equiv \mathrm{Tr}_1^m(1) \pmod 2$, where $D = \frac{d}{c^{2^s+1}}$, with $t = \gcd(s,n)$ and $m = \frac{n}{t}$, and zero solutions otherwise. Moreover, the solutions are of the form $X + cu$, where $u \in \mathbb{F}_{2^t}$.

If $t = 1$, we get that F_1 is APN, and using Corollary 6.1, we are done. Next, let us suppose that $t > 1$. Here, we focus exclusively on the case where $a \ne c$ and $ac \ne 0$, as all other cases are straightforward. Let $\mathrm{DDT}_{F_1}(c,d) = 2k = 2^t = 4r$, where r is a positive integer. Let $z_{i_1} = X + u_{i_1}c$ and $z_{j_1} = X + u_{j_1}c$, where $u_{i_1} \ne u_{j_1} \in \mathbb{F}_{2^t}$ and $u_{i_1} + u_{j_1} \ne c$. Then, for $(a,b) = (z_{i_1} + z_{j_1}, F_1(z_{i_1}) + F_1(z_{j_1})) = ((u_{i_1} + u_{j_1})c, F_1(X + u_{i_1}) + F_1(X + u_{j_1}))$, System (3.1) will have at least four solutions, namely, $\{X + u_{i_1}c, X + u_{j_1}c, X + u_{i_1}c + c, X + u_{j_1}c + c\}$, where X satisfies $X^{2^s+1} + (X+c)^{2^s+1} = d$.

Next, we are required to examine if System (3.1) can have any other solution from the set $S(c,d)$ except for these four, corresponding to the pair (a,b) defined above. Using Theorem 5.1, we know that $z_{i_2} = X + u_{i_2}c \in S(c,d) \setminus \{z_{i_1}, z_{j_1}, z_{i_1} + c, z_{j_1} + c\}$, where $u_{i_2} \in \mathbb{F}_{2^t}$, is a solution of System (3.1) if there exist $z_{j_2} \in S(c,d) \setminus \{z_{i_1}, z_{j_1}, z_{i_1} + c, z_{j_1} + c, z_{i_2}, z_{i_2} + c\}$ such that $a = z_{i_1} + z_{j_1} = z_{i_2} + z_{j_2}$ and $b = F_1(z_{i_1}) + F_1(z_{j_1}) = F_1(z_{i_2}) + F_1(z_{j_2})$. Note that if we choose $z_{j_2} = X + (u_{i_1} + u_{j_1} + u_{i_2})c$, then it is easy to see that $a = z_{i_1} + z_{j_1} = u_{i_1} + u_{j_1} = z_{i_2} + z_{j_2}$ and moreover, the following computations

$$
\begin{aligned}
F_1(z_{i_1}) + F_1(z_{j_1}) &= (X + u_{i_1}c)^{2^s+1} + (X + u_{j_1}c)^{2^s+1} \\
&= ((u_{i_1} + u_{j_1})c)^{2^s} X + (u_{i_1} + u_{j_1})cX^{2^s} + (u_{i_1}^{2^s+1} + u_{j_1}^{2^s+1})c^{2^s+1} \\
&= ((u_{i_1} + u_{j_1})c)^{2^s} X + (u_{i_1} + u_{j_1})cX^{2^s} + (u_{i_1} + u_{j_1})^{2^s+1}c^{2^s+1} \\
&\quad + (u_{i_1}^{2^s} u_{j_1} + u_{j_1}^{2^s} u_{i_1})c^{2^s+1} \\
&= (u_{i_1} + u_{j_1})(c^{2^s} X + cX^{2^s}) + (u_{i_1} + u_{j_1})^2 c^{2^s+1} \\
&= (u_{i_1} + u_{j_1})(c^{2^s+1} + d) + (u_{i_1} + u_{j_1})^2 c^{2^s+1} \\
&= ((u_{i_1} + u_{j_1}) + (u_{i_1} + u_{j_1})^2)c^{2^s+1} + (u_{i_1} + u_{j_1})d, \\
F_1(z_{i_2}) + F_1(z_{j_2}) &= (X + u_{i_2}c)^{2^s+1} + (X + (u_{i_1} + u_{j_1} + u_{i_2})c)^{2^s+1} \\
&= ((u_{i_1} + u_{j_1})c)^{2^s} X + (u_{i_1} + u_{j_1})cX^{2^s} + (u_{i_1} + u_{j_1})^{2^s+1}c^{2^s+1} \\
&\quad + (u_{i_2}^{2^s}(u_{i_1} + u_{j_1}) + (u_{i_1} + u_{j_1})^{2^s} u_{i_2})c^{2^s+1} \\
&= (u_{i_1} + u_{j_1})(c^{2^s} X + cX^{2^s}) + (u_{i_1} + u_{j_1})^2 c^{2^s+1}, \\
&= ((u_{i_1} + u_{j_1}) + (u_{i_1} + u_{j_1})^2)c^{2^s+1} + (u_{i_1} + u_{j_1})d,
\end{aligned}
$$

show that $b = F_1(z_{i_1}) + F_1(z_{j_1}) = F_1(z_{i_2}) + F_1(z_{j_2})$. We have used here that, since $t|s$, if $u \in \mathbb{F}_{2^t}$ then $u^{2^s} = u$, and that $d = (X + u_{i_1}c + c)^{2^s+1} + (X + u_{i_1}c)^{2^s+1} = c^{2^s} X + cX^{2^s} + c^{2^s+1}$. Hence, for $(a,b) = (z_{i_1} + z_{j_1}, F_1(z_{i_1}) + F_1(z_{j_1}))$, we get z_{i_2} as a solution of System (3.1). As $z_{i_2} \in S(c,d) \setminus \{z_{i_1}, z_{j_1}, z_{i_1} + c, z_{j_1} + c\}$ was chosen arbitrarily, so every element in the set $S(c,d)$ will be a solution of System (3.1) for $(a,b) = (z_{i_1} + z_{j_1}, F_1(z_{i_1}) + F_1(z_{j_1}))$. Therefore, for $\mathrm{DDT}_{F_1}(c,d) = 2k$, it turns out that $\ell = r$ is the largest integer such that $(a,b) \in U(i_1,j_1) \cap U(i_2,j_2) \cap \cdots \cap U(i_\ell, j_\ell)$, where $1 \le i_1, i_2, \ldots, i_\ell, j_1, j_2, \ldots, j_\ell \le k$ are distinct integers; or, equivalently, for $\mathrm{DDT}_{F_1}(c,d) = 2k$ and $(a,b) \in \{(uc, (u+u^2)c^{2^s+1} + ud) \mid u \in \mathbb{F}_{2^t}^* \setminus \{1\}\}$, $\mathrm{EBCT}_{F_1}(a,b,c,d) = 4\ell = \mathrm{DDT}_{F_1}(c,d)$.

We now compute LBCT and UBCT entries of F_1. If $t = 1$, then F_1 is APN, and using Corollary 6.1, we are done. Next, let us suppose that $t > 1$, then we will compute the LBCT and UBCT entries via (and using the notations and expressions of LBCT and UBCT) Theorem 5.1.

It is known from Theorem 5.1 that if $a = b, ab \neq 0$ or $a = 0, b \neq 0$, then $\mathrm{LBCT}_{F_1}(a, b, c) = \mathrm{DDT}_{F_1}(b, c) = 2^t$ if and only if $\mathrm{Tr}_s^{sm}\left(\frac{c}{b^{2^s+1}}\right) = \mathrm{Tr}_1^m(1)$; otherwise, it is zero. Now, let $a \neq b$, $ab \neq 0$ and $\mathrm{DDT}_{F_1}(b, c) = 2k = 2^t = 4r$, where r is a positive integer. Consider $S(b, c) = \{y_1, y_1 + b, y_2, y_2 + b, \ldots, y_k, y_k + b\}$ to be the solution set of the equation $F_1(X + b) + F_1(X) = c$. Suppose that $y_{i_1} = X + v_{i_1}b$ and $y_{j_1} = X + v_{j_1}b$, where X satisfies $X^{2^s+1} + (X + b)^{2^s+1} = c$, $v_{i_1} \neq v_{j_1} \in \mathbb{F}_{2^t}$ and $v_{i_1} + v_{j_1} \neq b$. Then, for $a = y_{i_1} + y_{j_1} = (v_{i_1} + v_{j_1})b$, System (3.2) has at least four solutions, namely, $\{(X + v_{i_1}b, X + v_{i_1}b + b), (X + v_{j_1}b, X + v_{j_1}b + b), (X + v_{i_1}b + b, X + v_{i_1}b), (X + v_{j_1}b + b, X + v_{j_1}b)\}$. We now need to investigate that whether System (3.2) has more than these four solutions, corresponding to $a = (v_{i_1} + v_{j_1})b$. From Theorem 5.1, it follows that $(y_{i_2}, y_{i_2} + b)$, where $y_{i_2} = X + v_{i_2}b \in S(b, c) \setminus \{y_{i_1}, y_{j_1}, y_{i_1} + b, y_{j_1} + b\}$ and $v_{i_2} \in \mathbb{F}_{2^t}$, is a solution of System (3.2) if and only if there exists $y_{j_2} = X + v_{j_2}b \in S(b, c) \setminus \{y_{i_1}, y_{j_1}, y_{i_1} + b, y_{j_1} + b, y_{i_2}, y_{i_2} + b\}$, $v_{j_2} \in \mathbb{F}_{2^t}$, such that $a = y_{i_2} + y_{j_2}$. Clearly, one can choose $y_{j_2} = X + (v_{i_1} + v_{i_2} + v_{j_2})$ to ensure $a = y_{i_1} + y_{j_1} = y_{i_2} + y_{j_2}$. Thus, we obtain another set of four solutions $\{(X + v_{i_2}b, X + v_{i_2}b + b), (X + v_{j_2}b, X + v_{j_2}b + b), (X + v_{i_2}b + b, X + v_{i_2}b), (X + v_{j_2}b + b, X + v_{j_2}b)\}$ for System (3.2) when $a = y_{i_1} + y_{j_1}$. Since $y_{i_2} \in S(b, c) \setminus \{y_{i_1}, y_{j_1}, y_{i_1} + b, y_{j_1} + b\}$ was choosen arbitrarily, it renders that every element in the set $S(b, c)$ is a solution of System (3.2) for $a = y_{i_1} + y_{j_1}$. Thus, $\mathrm{LBCT}_{F_1}(a, b, c) = \mathrm{DDT}_{F_1}(b, c)$.

We next compute the UBCT entries for F_1. It is evident from Theorem 5.1 that if $a = b = 0$, then $\mathrm{UBCT}_{F_1}(a, b, c) = |F_1^{-1}(c + \mathrm{Im}(F_1))|$ where $\mathrm{Im}(F_1)$ is the image of F_1 and $F_1^{-1}(\cdot)$ denotes the preimage of the argument. Moreover, if $b = c$ and $a \neq 0$ then $\mathrm{UBCT}_{F_1}(a, b, c) = \mathrm{DDT}_{F_1}(a, b) = 2^t$ if and only if $\mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right) = \mathrm{Tr}_1^m(1)$; otherwise, it is zero. Therefore, assume that $a \neq 0$ and $b \neq c$ and $\mathrm{DDT}_{F_1}(a, b) = 2k = 2^t = 4r$, where r is a positive integer. Define $S(a, b) = \{x_1, x_1 + a, x_2, x_2 + a, \ldots, x_k, x_k + a\}$ as the solution set of the equation $F_1(X + a) + F_1(X) = b$. Suppose $x_{i_1} = X + w_{i_1}a$ and $x_{j_1} = X + w_{j_1}a$, where $w_{i_1} \neq w_{j_1} \in \mathbb{F}_{2^t}$, $w_{i_1} + w_{j_1} \neq a$ and $X^{2^s+1} + (X + a)^{2^s+1} = b$. Then, for $c = F_1(x_{i_1}) + F_1(x_{j_1}) = ((w_{i_1} + w_{j_1}) + (w_{i_1} + w_{j_1})^2)a^{2^s+1} + (w_{i_1} + w_{j_1})b$, System (3.3) will have at least four solutions, namely, $\{(X + w_{i_1}a, X + w_{j_1}a), (X + w_{i_1}a + a, X + w_{j_1}a + a), (X + w_{j_1}a, X + w_{i_1}a), (X + w_{j_1}a + a, X + w_{i_1}a + a)\}$. Using the similar argument as in the case of EBCT, one can ensure that every element in the set $S(a, b)$ is a solution of System (3.3) for $c = F_1(x_{i_1}) + F_1(x_{j_1}) = ((w_{i_1} + w_{j_1}) + (w_{i_1} + w_{j_1})^2)a^{2^s+1} + (w_{i_1} + w_{j_1})b$. Hence, we conclude that $\mathrm{UBCT}_{F_1}(a, b, c) = \mathrm{DDT}_{F_1}(a, b)$. □

We will derive here the FBCT for the Gold function for any parameters a, b (also found in [12], but our proof is significantly shorter). As known, for monomials, one can take $b = 1$.

Corollary 7.4 *Let $F_1(X) = X^{2^s+1}$, with $\gcd(s, n) = t$ and $m = \frac{n}{t}$, where $a \in \mathbb{F}_{2^n}^*$. Then,*

$$\mathrm{FBCT}_{F_1}(a, 1) = \begin{cases} 2^n & \text{if } a \in \mathbb{F}_{2^t}^*, \\ 0 & \text{otherwise.} \end{cases}$$

Proof Observe that

$$\mathrm{LBCT}_{F_1}(a, 1, c) = \begin{cases} 2^t & \text{if } \sum_{i=0}^{m-1} c^{2^{si}} = 1 \text{ and } a \in \mathbb{F}_{2^t}^*, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that, if $a \notin \mathbb{F}_{2^t}^*$, then $\mathrm{FBCT}_{F_1}(a,1) = 0$. Let us now assume that $a \in \mathbb{F}_{2^t}^*$. Note that the condition $\sum_{i=0}^{m-1} c^{2^{si}} = 1$ is equivalent to $\mathrm{DDT}_{F_1}(1,c) = 2^t$. Denoting as is usual $\omega_i = \left|\{c \mid \mathrm{DDT}_{F_1}(1,c) = i\}\right|$, $\mathrm{FBCT}_{F_1}(a,1) = \sum_{c\in\mathbb{F}_{2^n}} \mathrm{LBCT}_{F_1}(a,1,c) = 2^t\omega_{2^t} = \sum_{i=0}^{2^t} i\omega_i = 2^n$. This proves the claim. □

Remark 7.5 Let F be a differentially 4-uniform function over $\mathbb{F}_{2^n}$ such that $\mathrm{DDT}_F(b,c) = 4$ or $\mathrm{DDT}_F(b,c) = 0$ for any $b, c \in \mathbb{F}_{2^n}$. For any b, c such that $\mathrm{DDT}_F(b,c) = 4$, denote by $\{y_1, y_1+b, y_2, y_2+b\}$ the four distinct solutions of the equation $F(X+b)+F(X) = c$. If $y_i + y_j, i \neq j$, is independent of c, then by using a similar argument as in the above corollary, for $a \in \{y_i + y_j, y_i + y_j + b\}$, we obtain

$$\mathrm{FBCT}_F(a,b) = \begin{cases} 2^n & \text{if } a \in \{b, y_i + y_j, y_i + y_j + b\} \\ 0 & \text{otherwise.} \end{cases}$$

Example 7.6 In Table 2, Corollary 7.3 is illustrated by giving explicit values of the EBCT, LBCT and UBCT entries of the Gold function X^{2^s+1} over $\mathbb{F}_{2^n}^* = \langle g \rangle$, where g is a primitive element of $\mathbb{F}_{2^n}$, for some small values of n.

The Kasami function is a well-known nonlinear function over $\mathbb{F}_{2^n}$, given by $F_2(X) = X^{2^{2s}-2^s+1}$. Hertel and Pott [15] showed that for $\gcd(s,n) = 2$, where $n = 2t$, t is odd and $3 \nmid t$, it is a differentially 4-uniform permutation. We next investigate the EBCT, LBCT and UBCT entries of F_2 over $\mathbb{F}_{2^n}$.

Corollary 7.7 *Let $F_2(X) = X^{2^{2s}-2^s+1}$ on $\mathbb{F}_{2^n}$, where $\gcd(s,n) = 2$, $n = 2t$ and t is odd and $3 \nmid t$. Then for $a, b, c, d \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_{F_2}(a,b,c,d) = \begin{cases} 2^n & \text{if } a = b = c = d = 0, \\ 4 & \text{if } \mathrm{DDT}_{F_2}(a,b) = 4, a \neq 0 \text{ and } c = d = 0; \text{ or} \\ & \quad \mathrm{DDT}_{F_2}(c,d) = 4, a = b = 0 \text{ and } c \neq 0; \text{ or} \\ & \quad \mathrm{DDT}_{F_2}(c,d) = 4, ac \neq 0, a = c \text{ and } b = d; \text{ or} \\ & \quad \mathrm{DDT}_{F_2}(c,d) = 4, a = \omega c + \alpha^{2^s+1}, \text{ and } b = \omega d + \alpha^{2^{3s}+1}; \text{ or} \\ & \quad \mathrm{DDT}_{F_2}(c,d) = 4, a = \omega^2 c + \alpha^{2^s+1}, \text{ and } b = \omega^2 d + \alpha^{2^{3s}+1}, \\ 0 & \text{otherwise,} \end{cases}$$

for $\alpha \in \mathbb{F}_{2^n}^*$ with $c^{2^{2s}} + c^{2^s}\alpha^{2^{3s}-2^s} + c\alpha^{2^{3s}+2^{2s}-2^s-1} + d\alpha^{2^{2s}-1} = 0$ and $\mathrm{Tr}_s^{st}\left(1 + \frac{c}{\alpha^{2^s+1}}\right) = 0$,

$$\mathrm{LBCT}_{F_2}(a,b,c) = \begin{cases} 2^n & \text{if } b = c = 0, \\ 4 & \text{if } \mathrm{DDT}_{F_2}(b,c) = 4, a = 0 \text{ and } b \neq 0; \text{ or} \\ & \quad \mathrm{DDT}_{F_2}(b,c) = 4, ab \neq 0 \text{ and } a \in \left\{b, b\omega + \alpha^{2^s+1}, b\omega^2 + \alpha^{2^s+1}\right\}, \\ 0 & \text{otherwise,} \end{cases}$$

for $\alpha \in \mathbb{F}_{2^n}^*$ with $b^{2^{2s}} + b^{2^s}\alpha^{2^{3s}-2^s} + b\alpha^{2^{3s}+2^{2s}-2^s-1} + c\alpha^{2^{2s}-1} = 0$ and $\mathrm{Tr}_s^{st}\left(1 + \frac{b}{\alpha^{2^s+1}}\right) = 0$,

$$\mathrm{UBCT}_{F_2}(a,b,c) = \begin{cases} 2^n & \text{if } a = b = 0, \\ 4 & \text{if } \mathrm{DDT}_{F_2}(a,b) = 4, a \neq 0 \text{ and } c \in \left\{b, b\omega + \alpha^{2^{3s}+1}, b\omega^2 + \alpha^{2^{3s}+1}\right\}, \\ 0 & \text{otherwise,} \end{cases}$$

Table 2 EBCT, LBCT and UBCT entries for the Gold function X^{2^s+1} over $\mathbb{F}_{2^n}$

n	s	a	b	c	d	ω	$\text{EBCT}_{F_1}(a,b,c,d)$	$\text{LBCT}_{F_1}(a,b,c)$	$\text{UBCT}_{F_1}(a,b,c)$
6	2	g^{44}	g^{23}	g^{16}	For any d	g^{21}	0	4	0
6	2	g^{2}	g^{26}	g^{53}	For any d	g^{21}	0	0	4
10	6	g^{351}	g^{692}	g^{2}	For any d	g^{341}	0	0	0
10	4	g^{2}	g^{359}	g^{11}	For any d	g^{682}	0	0	4
6	2	g^{44}	g^{8}	g^{23}	g^{16}	g^{21}	4	0	0
10	4	g^{684}	g^{11}	g^{2}	g^{359}	g^{682}	4	0	0

for $\alpha \in \mathbb{F}_{2^n}^*$ *satisfying* $a^{2^{2s}} + a^{2^s}\alpha^{2^{3s}-2^s} + a\alpha^{2^{3s}+2^{2s}-2^s-1} + b\alpha^{2^{2s}-1} = 0$, $\mathrm{Tr}_s^{st}\left(1 + \frac{a}{\alpha^{2^s+1}}\right) = 0$ *and* ω *is the primitive cube root of unity.*

Proof Since F_2 is a permutation, Lemma 2.8 can be referred for determining EBCT, LBCT and UBCT entries of F_2 in cases where $abcd = 0$. Thus, in what follows, we will assume that $abcd \neq 0$. By Corollary 7.1, for $a, b, c, d \in \mathbb{F}_{2^n}^*$, $\mathrm{EBCT}_{F_2}(a, b, c, d)$ equals

$$\begin{cases} \mathrm{DDT}_{F_2}(c, d) & \text{if } a = c \text{ and } b = d; \text{ or} \\ & \mathrm{DDT}_{F_2}(c, d) = 4, a = z_1 + z_2 \text{ and } b = F_2(z_1) + F_2(z_2); \text{ or} \\ & \mathrm{DDT}_{F_2}(c, d) = 4, a = z_1 + z_2 + c \text{ and } b = F_2(z_1) + F_2(z_2 + c), \\ 0 & \text{otherwise,} \end{cases}$$

where $z_1, z_1 + c, z_2, z_2 + c$ are the four solutions of the equation $F_2(X + c) + F_2(X) = d$ if $\mathrm{DDT}_{F_2}(c, d) = 4$. We write $F_2(X + c) + F_2(X) = d$ as the system

$$\begin{cases} Y + X = c, \\ F_2(Y) + F_2(X) = d. \end{cases} \tag{7.1}$$

Now by using the argument given in [8], and the fact that $\gcd(2^s+1, 2^n-1) = 1$, substituting $X = u^{2^s+1}$, $Y = v^{2^s+1} = (u+\alpha)^{2^s+1}$, for some $\alpha \in \mathbb{F}_{2^n}^*$ such that $v = u+\alpha$ and simplifying System (7.1), we have

$$\begin{cases} \left(\frac{u}{\alpha}\right)^{2^s} + \frac{u}{\alpha} + 1 + \frac{c}{\alpha^{2^s+1}} = 0, \\ \left(\frac{u}{\alpha}\right)^{2^{3s}} + \frac{u}{\alpha} + 1 + \frac{d}{\alpha^{2^{3s}+1}} = 0, \end{cases}$$

or equivalently,

$$\begin{cases} \left(\frac{u}{\alpha}\right)^{2^s} + \frac{u}{\alpha} + 1 + \frac{c}{\alpha^{2^s+1}} = 0, \\ c^{2^{2s}} + c^{2^s}\alpha^{2^{3s}-2^s} + c\alpha^{2^{3s}+2^{2s}-2^s-1} + d\alpha^{2^{2s}-1} = 0. \end{cases}$$

Notice that the first equation of the above system has either 0 or 4 solutions in $\mathbb{F}_{2^n}$, depending on whether $\sum_{i=0}^{t-1}\left(1 + \frac{c}{\alpha^{2^s+1}}\right)^{2^{si}}$ is zero or not, respectively. This first equation is simply the equation for the DDT entry of u^{2^s+1} at (α, c), and if $\mathrm{DDT}_{u^{2^s+1}}(\alpha, c) = 4$, then the four solutions of $\left(\frac{u}{\alpha}\right)^{2^s} + \frac{u}{\alpha} + 1 + \frac{c}{\alpha^{2^s+1}} = 0$ are $\{u, u+\alpha, u+\alpha\omega, u+\alpha\omega^2\}$. This implies that u^{2^s+1}, $(u+\alpha)^{2^s+1}$, $(u+\alpha\omega)^{2^s+1}$, $(u+\alpha\omega^2)^{2^s+1}$ are solutions of $F_2(X)+F_2(X+c) = d$, or equivalently $\{z_1, z_1+c, z_2, z_2+c\} \subseteq \left\{u^{2^s+1}, (u+\alpha)^{2^s+1}, (u+\alpha\omega)^{2^s+1}, (u+\alpha\omega^2)^{2^s+1}\right\}$. Then for $z_1 = u^{2^s+1}$, we have $z_1 + c = (u+\alpha)^{2^s+1}$. Further, we split our analysis in the following two cases:

Case 1 Let $z_2 = (u+\alpha\omega)^{2^s+1}$ Then $z_1 + z_2 = a$ and $F_2(z_1) + F_2(z_2) = b$ can be written as $u^{2^s+1} + (u+\alpha\omega)^{2^s+1} = a$ and $u^{2^{3s}+1} + (u+\alpha\omega)^{2^{3s}+1} = b$.

Also, by using $u^{2^{3s}+1} + (u+\alpha)^{2^{3s}+1} = d$, and the second equation of above system will give us $b = d\omega + \alpha^{2^{3s}+1}$. To compute a, we use $u^{2^s+1} + (u+\alpha)^{2^s+1} = c$ and the first equation of the above system and simplify them to get $a = c\omega + \alpha^{2^s+1}$.

Case 2 Now assume $z_2 = (u+\alpha\omega^2)^{2^s+1}$. By using the same argument as in the above case, we get $a = c\omega^2 + \alpha^{2^s+1}$ and $b = d\omega^2 + \alpha^{2^{3s}+1}$.

Summarizing both cases, we get the EBCT of the Kasami function.

We next compute the LBCT and UBCT entries via (and using the notations of) Corollary 7.2. As $\mathrm{DDT}_{F_2}(c,d)$ is either 0 or 4, then, $\mathrm{LBCT}_{F_2}(a,c,d) \neq 2$, for any $(a,c,d) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ and, $\mathrm{UBCT}_{F_2}(c,d,b) \neq 2$, for any $(c,d,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$.

Now, one can write set

$$A = \left\{ (c,c,d), (\omega c + \alpha^{2^s+1}, c, d), (\omega^2 c + \alpha^{2^s+1}, c, d) \mid \mathrm{DDT}_{F_2}(c,d) = 4 \right\},$$

for $c, d \in \mathbb{F}_{2^n}^*$. This is because, when $\mathrm{DDT}_{F_2}(c,d) = 4$, $(c,c,d) \in A$, for $b = d$, $(\omega c + \alpha^{2^s+1}, c, d) \in A$, for $b = d\omega + \alpha^{2^{3s}+1}$ and $(\omega^2 c + \alpha^{2^s+1}, c, d) \in A$, for $b = d\omega^2 + \alpha^{2^{3s}+1}$. Finally, from Corollary 7.2, we have $\mathrm{LBCT}_{F_2}(a,c,d) = 4$, for $a \in \left\{c, \omega c + \alpha^{2^s+1}, \omega^2 c + \alpha^{2^s+1}\right\}$. Thus, by reordering the indexes, we complete the LBCT case.

Similarly, one can write the set

$$B = \left\{ (c,d,d), (c,d,d\omega + \alpha^{2^{3s}+1}), (c,d,d\omega^2 + \alpha^{2^{3s}+1}) \mid \mathrm{DDT}_{F_2}(c,d) = 4 \right\},$$

as, in the case $\mathrm{DDT}_{F_2}(c,d) = 4$, $(c,d,d) \in B$, for $a = c$, $(c,d,d\omega + \alpha^{2^{3s}+1}) \in B$, for $a = \omega c + \alpha^{2^s+1}$ and $(c,d,d\omega^2 + \alpha^{2^{3s}+1}) \in B$, for $a = \omega^2 c + \alpha^{2^s+1}$. Hence, one can get the UBCT of the Kasami function by reordering the indexes. □

Example 7.8 The examples given in Table 3 (g denotes a primitive element of $\mathbb{F}_{2^{2t}}$) illustrate Corollary 7.7:

Bracken and Leander [4] studied the differential uniformity of $F_3(X) = X^{2^{2s}+2^s+1}$ over $\mathbb{F}_{2^n}$ where $n = 4s$, which is often known as the Bracken–Leander function. They showed that F_3 is differentially 4-uniform, and its nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$. Further, Calderini and Villa [6] investigated the BCT entries and showed that the boomerang uniformity of the Bracken–Leander function is upper bounded by 24. Here, we first recall some results from [21] that will be used to compute the EBCT, LBCT and UBCT entries for the Bracken–Leander function.

Lemma 7.9 [21, Lemma 1] *For any $X \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^n}$, let $t = \mathrm{Tr}_s^n(c+1) \in \mathbb{F}_{2^s}$, $n = 4s$.*

(1) *If $F_3(X) + F_3(X+1) = c$, then $\mathrm{Tr}_s^n(X) = t$.*
(2) *Let $Z = X + X^{2^s}$. Then $F_3(x) + F_3(X+1) = c$ holds if and only if $Z^2 + (t+1)Z + c^{2^s} + c^{2^{2s}} = 0$ and $X^2 + X + Z^{2^s+1} + Z^{2^s} + Z^2 + c + 1 = 0$.*

Next, we define W to be the set of all $X \in \mathbb{F}_{2^n}$ such that there exists $X' \in \mathbb{F}_{2^n} \setminus \{X, X+1\}$ with $X^{2^{2s}+2^s+1} + (X+1)^{2^{2s}+2^s+1} = X'^{2^{2s}+2^s+1} + (X'+1)^{2^{2s}+2^s+1}$. We now recall a result describing W explicitly.

Lemma 7.10 [21, Theorem 2] *Given elements $u \in \mathbb{F}_{2^{2s}} \setminus \{\mathbb{F}_{2^s}\}$ and $v \in \mathbb{F}_{2^n} \setminus \{\mathbb{F}_{2^{2s}}\}$ such that $u + u^{2^s} = 1$, $v + v^{2^{2s}} = 1$, which always exist, then $X \in W$ if and only if $X = (tu+\beta)v + \tau$, where $t \in \mathbb{F}_{2^s} \setminus \{1\}$, $\tau \in \mathbb{F}_{2^{2s}}$, and $\beta \in \mathbb{F}_{2^s}$ satisfies $\beta = (t+1)^{-1}(\alpha^2+\alpha) + (t+1)(u^2+u) + 1$, for some $\alpha \in \mathbb{F}_{2^s}$.*

Remark 7.11 The proof of the above lemma also shows that $X' = X + (t+1)u + \alpha$.

Next, we determine the EBCT, LBCT and UBCT entries for the Bracken–Leander function.

Table 3 EBCT, LBCT and UBCT entries for Kasami function $X^{2^{2s}-2^s+1}$ over $\mathbb{F}_{2^{2t}}$

t	s	a	b	c	d	α	ω	$\mathrm{EBCT}_{F_2}(a,b,c,d)$	$\mathrm{LBCT}_{F_2}(a,b,c)$	$\mathrm{UBCT}_{F_2}(a,b,c)$
5	2	g^6	g	g^{605}	For any d	g^{50}	g^{341}	0	0	4
5	6	g^5	g	g^{774}	For any d	g^{994}	g^{682}	0	0	0
5	2	g^{401}	g^{605}	g^6	g	g^{50}	g^{341}	4	0	0
5	6	g^{84}	g^{24}	g^2	For any d	g^{681}	g^{682}	0	4	0

Corollary 7.12 *Let $F_3(X) = X^{2^{2s}+2^s+1}$ on $\mathbb{F}_{2^n}$, where $n = 4s$. Then for $a, b, c, d \in \mathbb{F}_{2^n}$, we have*

$$\mathrm{EBCT}_{F_3}(a,b,c,d) = \begin{cases} 2^n & \text{if } a=b=c=d=0, \\ \mathrm{DDT}_{F_3}(a,b) & \text{if } c=d=0 \text{ and } a\neq 0, \\ \mathrm{DDT}_{F_3}(c,d) & \text{if } ac\neq 0, a=c \text{ and } b=d; \text{ or } a=0, b=0 \text{ and } c\neq 0; \\ & \text{or } \mathrm{DDT}_{F_3}(c,d)=4, a=c((t+1)u+\alpha) \text{ and} \\ & \quad b=d(\alpha+(t+1)u^{2^s})+F_3(c)\gamma; \\ & \text{or } \mathrm{DDT}_{F_3}(c,d)=4, a=c((t+1)u+\alpha+1) \text{ and} \\ & \quad b=d(\alpha+(t+1)u^{2^s}+1)+F_3(c)\gamma, \\ 0 & \text{otherwise,} \end{cases}$$

where $t = \mathrm{Tr}_s^n\left(\frac{d}{F_3(c)}\right)$, and $F_3((tu+\beta)v+\tau)+F_3((tu+\beta)v+\tau+1) = \frac{d}{F_3(c)}$,

$$\mathrm{LBCT}_{F_3}(a,b,c) = \begin{cases} 2^n & \text{if } b=c=0, \\ \mathrm{DDT}_{F_3}(b,c) & \text{if } a=0 \text{ and } b\neq 0; \text{ or} \\ & \mathrm{DDT}_{F_3}(b,c)=2, ab\neq 0 \text{ and } a=b; \text{ or} \\ & \mathrm{DDT}_{F_3}(b,c)=4, ab\neq 0 \text{ and} \\ & \quad a\in\{b, b((t+1)u+\alpha), b((t+1)u+\alpha+1)\}, \\ 0 & \text{otherwise,} \end{cases}$$

where $t = \mathrm{Tr}_s^n\left(\frac{c}{F_3(b)}\right)$, and $F_3((tu+\beta)v+\tau)+F_3((tu+\beta)v+\tau+1) = \frac{c}{F_3(b)}$, and,

$$\mathrm{UBCT}_{F_3}(a,b,c) = \begin{cases} |F_3^{-1}(c+\mathrm{Im}(F_3))| & \text{if } a=b=0, \\ \mathrm{DDT}_{F_3}(a,b) & \text{if } \mathrm{DDT}_{F_3}(a,b)=2, a\neq 0 \text{ and } c=b; \text{ or} \\ & \mathrm{DDT}_{F_3}(a,b)=4, a\neq 0, \\ & c\in\{b, b(\alpha+(t+1)u^{2^s})+F_3(a)\gamma, \text{ and} \\ & \quad b(\alpha+(t+1)(1+u)+1)+F_3(a)\gamma\}, \\ 0 & \text{otherwise,} \end{cases}$$

where $t = \mathrm{Tr}_s^n\left(\frac{b}{F_3(a)}\right)$, $F_3((tu+\beta)v+\tau)+F_3((tu+\beta)v+\tau+1) = \frac{b}{F_3(a)}$, $\mathrm{Im}(F_3)$ is the image of F_3 and $F_3^{-1}(\cdot)$ denotes the preimage of the argument. In particular, if F_3 is a permutation, or equivalently if s is odd, then $|F_3^{-1}(c+\mathrm{Im}(F_3))| = 2^n$.

In all the computed tables, $\gamma = ((t+1)^{-1}(\alpha^4+\alpha^2)+(t+1)^3(u^4+u^2)+\alpha^2 t+\alpha t+t(t+1)(u+u^2))$, $\tau \in \mathbb{F}_{2^{2s}}$, $u \in \mathbb{F}_{2^{2s}} \setminus \{\mathbb{F}_{2^s}\}$, $v \in \mathbb{F}_{2^n} \setminus \{\mathbb{F}_{2^{2s}}\}$ satisfying $u+u^{2^s}=1$, $v+v^{2^{2s}}=1$, and $\beta \in \mathbb{F}_{2^s}$ satisfying $\beta = (t+1)^{-1}(\alpha^2+\alpha)+(t+1)(u^2+u)+1$, for some $\alpha \in \mathbb{F}_{2^s}$.

Proof By Corollary 7.1, $\mathrm{EBCT}_{F_3}(a,b,c,d)$ is equal to

$$\begin{cases} \mathrm{DDT}_{F_3}(a,b) & \text{if } c=d=0, \\ \mathrm{DDT}_{F_3}(c,d) & \text{if } ac\neq 0, a=c \text{ and } b=d; \text{ or } a=0, b=0, c\neq 0; \text{ or} \\ & \mathrm{DDT}_{F_3}(c,d)=4, a=z_1+z_2 \text{ and } b=F_3(z_1)+F_3(z_2); \text{ or} \\ & \mathrm{DDT}_{F_3}(c,d)=4, a=z_1+z_2+c \text{ and } b=F_3(z_2)+F_3(z_2+c), \\ 0 & \text{otherwise,} \end{cases}$$

where z_1, z_1+c, z_2, z_2+c are the four solutions of the equation $F_3(X+c)+F_3(X)=d$ if $\mathrm{DDT}_{F_3}(c,d)=4$. This is equivalent to $F_3\left(\frac{X}{c}+1\right)+F_3\left(\frac{X}{c}\right) = \frac{d}{c^{2^{2s}+2^s+1}}$ having solutions $\left\{\frac{z_1}{c}, \frac{z_1}{c}+1, \frac{z_2}{c}, \frac{z_2}{c}+1\right\}$. We can simplify $F_3\left(\frac{X}{c}+1\right)+F_3\left(\frac{X}{c}\right) = \frac{d}{F_3(c)}$ as

$$\left(\frac{X}{c}\right)^{2^{2s}+2^s}+\left(\frac{X}{c}\right)^{2^{2s}+1}+\left(\frac{X}{c}\right)^{2^s+1}+\left(\frac{X}{c}\right)^{2^{2s}}+\left(\frac{X}{c}\right)^{2^s}+\frac{X}{c}+1 = \frac{d}{F_3(c)}.$$

Let $\mathrm{Tr}_s^n\left(\frac{d}{F_3(c)}+1\right)=\mathrm{Tr}_s^n\left(\frac{d}{F_3(c)}\right)=t$, where Tr_s^n denotes the relative trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^s}$.

First assume that $t=1$, then from the proof of [4, Theorem 1], we know that $F_3(\frac{X}{c}+1)+F_3(\frac{X}{c})=\frac{d}{F_3(c)}$ can have at most two solutions, a contradiction. Next, for $t\neq 1$, from Lemma 7.10, for $u\in\mathbb{F}_{2^{2s}}\setminus\{\mathbb{F}_{2^s}\}$ and $v\in\mathbb{F}_{2^n}\setminus\{\mathbb{F}_{2^{2s}}\}$ such that $u+u^{2^s}=1$, $v+v^{2^{2s}}=1$, we know that $\frac{z_1}{c}\in W$ if and only if $\frac{z_1}{c}=(tu+\beta)v+\tau$ and $\frac{z_2}{c}\in\left\{\frac{z_1}{c}+(t+1)u+\alpha,\frac{z_1}{c}+(t+1)u+\alpha+1\right\}$, where $\tau\in\mathbb{F}_{2^{2s}}$, and $\beta\in\mathbb{F}_{2^s}$ satisfies the relation $\beta=(t+1)^{-1}(\alpha^2+\alpha)+(t+1)(u^2+u)+1$, for some $\alpha\in\mathbb{F}_{2^s}$. Thus, $F_3(\frac{X}{c}+1)+F_3(\frac{X}{c})=\frac{d}{F_3(c)}$ can be written as $F_3((tu+\beta)v+\tau)+F_3((tu+\beta)v+\tau+1)=\frac{d}{F_3(c)}$.

Again, we divide our analysis into the following two cases:

Case 1 Let $\frac{z_2}{c}=\frac{z_1}{c}+(t+1)u+\alpha$, then we have $a=c((t+1)u+\alpha)$. Now, $b=F_3(z_1)+F_3(z_2)=z_1^{2^{2s}+2^s+1}+z_2^{2^{2s}+2^s+1}=c^{2^{2s}+2^s+1}(F_3(\frac{z_1}{c})+F_3(\frac{z_1}{c}+(t+1)u+\alpha))$. For $y_1=\frac{z_1}{c}$ and $D=\frac{d}{F_3(c)}$, we have

$$
\begin{aligned}
\frac{b}{F_3(c)} &= F_3(y_1)+F_3(y_1+(t+1)u+\alpha)\\
&= (\alpha+(t+1)u)(y_1^{2^{2s}+2^s}+y_1^{2^{2s}+1}+y_1^{2^s+1})+(\alpha+(t+1)u)^2(y_1^{2^{2s}}+y_1^{2^k}+y_1)\\
&\quad+(t+1)(y_1^{2^{2s}+1}+(\alpha+(t+1)u)(y_1+y_1^{2^s}))+(\alpha+(t+1)u)^{2^{2s}+2^s+1}\\
&= ((\alpha+(t+1)u)+(\alpha+(t+1)u)^2)(y_1^{2^{2s}}+y_1^{2^s}+y_1)+(\alpha+(t+1)u)(1+D)\\
&\quad+(t+1)(y_1^{2^{2s}+1}+(\alpha+(t+1)u)(y_1+y_1^{2^s}))+(\alpha+(t+1)u)^{2^{2s}+2^s+1}\\
&= (t+1)(tu+\beta+1)(y_1^{2^{2s}}+y_1^{2^s}+y_1)+(\alpha+(t+1)u)(1+D)\\
&\quad+(t+1)(y_1^{2^{2s}+1}+(\alpha+(t+1)u)(y_1+y_1^{2^s}))+(\alpha+(t+1)u)^{2^{2s}+2^s+1}\\
&= (t+1)(tu+\beta+1)(tu+\beta+(tu^{2^s}+\beta)v^{2^s}+\tau^{2^s})+(\alpha+(t+1)u)(1+D)\\
&\quad+(t+1)((tu+\beta)^2v^{2^{2s}+1}+\tau(tu+\beta)+\tau^2\\
&\quad+(\alpha+(t+1)u)(tu+\beta))+(\alpha+(t+1)u)^{2^{2s}+2^s+1}\\
&= (t+1)(D+tu+\beta+1)+(t+1)(tu+\beta+1)(tu+\beta)+(\alpha+(t+1)u)(1+D)\\
&\quad+(t+1)(\alpha+(t+1)u)(tu+\beta)+(\alpha+(t+1)u)^{2^{2s}+2^s+1}\\
&= (\alpha+(t+1)u^{2^s})D+(t+1)^{-1}(\alpha^4+\alpha^2)+(t+1)^3(u^4+u^2)\\
&\quad+\alpha^2t+\alpha t+t(t+1)(u+u^2).
\end{aligned}
$$

The above expression will give us $b=d(\alpha+(t+1)u^{2^s})+F_3(c)((t+1)^{-1}(\alpha^4+\alpha^2)+(t+1)^3(u^4+u^2)+\alpha^2t+\alpha t+t(t+1)(u+u^2))=d(\alpha+(t+1)u^{2^s})+F_3(c)\gamma$ (say), where $\gamma=((t+1)^{-1}(\alpha^4+\alpha^2)+(t+1)^3(u^4+u^2)+\alpha^2t+\alpha t+t(t+1)(u+u^2))$.

Case 2 Let $\frac{z_2}{c}=\frac{z_1}{c}+(t+1)u+\alpha+1$, then by the same argument as in Case 1, we have $a=c((t+1)u+\alpha+1)$ and $b=d(\alpha+(t+1)u^{2^s}+1)+F_3(c)((t+1)^{-1}(\alpha^4+\alpha^2)+(t+1)^3(u^4+u^2)+\alpha^2t+\alpha t+t(t+1)(u+u^2))$.

Combining both of these cases, we get the EBCT entries for the Bracken–Leander function.

Next, we compute the UBCT and LBCT entries for the Bracken–Leander function. Using Corollary 7.1 the LBCT entries are straightforward to determine when $acd=0$, except the case where $a\neq c, ac\neq 0$ and $d=0$. Furthermore, if $ac\neq 0, a\neq c$ and $d=0$,

the conditions derived for LBCT entries are identical to those obtained for the case where $acd \neq 0$ and $a \neq c$. Similarly, in the case of UBCT entries, we only need to focus on the case when $c \neq 0$ and $bd = 0$ as the other cases are trivial if $bcd = 0$. The conditions in this case are identical to those for $bcd \neq 0$. Therefore, it is sufficient to determine the UBCT and LBCT entries when $a, b, c, d \in \mathbb{F}_{2^n}^*$.

We then use (also its notations) of Corollary 7.2 to compute the LBCT and UBCT entries for the Bracken–Leander function when $abcd \neq 0$. As we have computed $\mathrm{EBCT}_{F_3}(a, b, c, d) = 2$, when $a = c, b = d$ and $\mathrm{DDT}_{F_3}(c, d) = 2$, then $\mathrm{LBCT}_{F_3}(a, c, d) = 2$, for $a = c$ when $\mathrm{DDT}_{F_3}(c, d) = 2$ and, $\mathrm{UBCT}_{F_3}(c, d, b) = 2$, for $b = d$ when $\mathrm{DDT}_{F_3}(c, d) = 2$.

Also, $A = \{(c, c, d), (c((t+1)u+\alpha), c, d), (c((t+1)u+\alpha+1), c, d) \mid \mathrm{DDT}_{F_3}(c, d) = 4\}$, as, in the case $\mathrm{DDT}_{F_3}(c, d) = 4$, $(c, c, d) \in A$, for $b = d$, $(c((t+1)u+\alpha), c, d) \in A$, for $b = d(\alpha + (t+1)u^{2^s}) + F_3(c)\gamma$ and $(c((t+1)u+\alpha+1), c, d) \in A$, for $b = d(\alpha + (t+1)u^{2^s} + 1) + F_3(c)\gamma$. Thus, from Corollary 7.2, we have $\mathrm{LBCT}_{F_3}(a, c, d) = 4$, for $a \in \{c, c((t+1)u+\alpha), c((t+1)u+\alpha+1)\}$. This completes the LBCT case.

Similarly, one can write $B = \{(c, d, d), (c, d, d(\alpha + (t+1)u^{2^s}) + F_3(c)\gamma), (c, d, d(\alpha + (t+1)u^{2^s} + 1) + F_3(c)\gamma \mid \mathrm{DDT}_{F_3}(c, d) = 4\}$, as, in the case of $\mathrm{DDT}_{F_3}(c, d) = 4$, $(c, d, d) \in B$, for $a = c$, $(c, d, d(\alpha + (t+1)u^{2^s}) + F_3(c)\gamma) \in B$, for $a = c((t+1)u+\alpha)$ and $(c, d, d(\alpha + (t+1)u^{2^k} + 1) + F_3(c)\gamma) \in B$, for $a = c((t+1)u+\alpha+1)$.

Hence, we get the LBCT and UBCT of the Bracken–Leander function by just reordering the indexes. □

Example 7.13 To illustrate Corollary 7.12, Table 4 gives explicit values of the LBCT and UBCT entries of Bracken–Leander function over $\mathbb{F}_{2^{4s}}^* = \langle g \rangle$ (g is a primitive element of $\mathbb{F}_{2^{4s}}$).

Via our Corollary 7.1, we can also give a very short proof for the EBCT, LBCT and UBCT entries of the inverse function for n even, which is the main result in [13, 17] (for n odd, see the previous section). Since F_4 is a permutation, the case for $abcd = 0$ follows directly from Lemma 2.8. Therefore, we focus our discussion in the following corollary on the cases where $a, b, c, d \in \mathbb{F}_{2^n}^*$.

Corollary 7.14 *Let $F_4(X) = X^{2^n-2}$ on $\mathbb{F}_{2^n}$, where n is even. For $a, b, c, d \in \mathbb{F}_{2^n}^*$, we have*

$$\mathrm{EBCT}_{F_4}(a, b, c, d) = \begin{cases} 4 & \text{if } a = c = \frac{1}{b} = \frac{1}{d}; \text{ or} \\ & \quad b = \frac{1}{a}, d = \frac{1}{c}, \text{ and } (ad)^2 + ad + 1 = 0, \\ 2 & \text{if } a = c, b = d, d \neq \frac{1}{c} \text{ and } \mathrm{Tr}\left(\frac{1}{cd}\right) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathrm{LBCT}_{F_4}(a, b, c) = \begin{cases} 4 & \text{if } a = b = \frac{1}{c}; \text{ or} \\ & \quad b = \frac{1}{c}, (ac)^2 + ac + 1 = 0, \\ 2 & \text{if } a = b \neq \frac{1}{c}, \mathrm{Tr}\left(\frac{1}{bc}\right) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathrm{UBCT}_{F_4}(a, b, c) = \begin{cases} 4 & \text{if } b = c = \frac{1}{a}; \text{ or} \\ & \quad b = \frac{1}{a}, (ac)^2 + ac + 1 = 0, \\ 2 & \text{if } c = b \neq \frac{1}{a}, \mathrm{Tr}\left(\frac{1}{ab}\right) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof For all three results, we have to study the spectrum of the inverse function, which can be found, for instance, implied in the proofs in [13, 17], but we recall it below for easy reference.

Table 4 EBCT, LBCT and UBCT entries for Bracken–Leander function $X^{2^{2s}+2^s+1}$ over $\mathbb{F}^*_{2^{4s}} = \langle g \rangle$

s	a	b	c	d	α	u	v	τ	$\mathrm{EBCT}_{F_3}(a,b,c,d)$	$\mathrm{LBCT}_{F_3}(a,b,c)$	$\mathrm{UBCT}_{F_3}(a,b,c)$
2	g	g	g	d	–	–	–	–	2	2	2
2	g^{71}	g^3	g^{32}	d	g^{255}	g^{17}	g^{123}	g^{17}	0	4	0
2	g^{54}	g^{37}	g^{26}	d	g^{85}	g^{34}	g^{224}	g^{17}	0	4	0
2	g^{70}	g^3	g^{103}	d	g^{85}	g^{34}	g^{224}	g^{17}	0	0	4
2	g^{36}	g^{103}	g^{70}	g^3	g^{85}	g^{34}	g^{224}	g^{17}	4	0	0

The equation $(X+A)^{2^n-2}+X^{2^n-2}=B$, for $A, B \neq 0$, and n even, gives:

- If $X=0 \text{or} X=A$, then $B=\frac{1}{A}$, otherwise there are no solutions.
- If $X \neq 0, A$, then the equation is equivalent to $X^2+AX+\frac{A}{B}=0$, which has two solutions if and only if $\text{Tr}\left(\frac{1}{AB}\right)=0$, and zero solutions, otherwise.

By Corollary 7.1, $\text{EBCT}_{F_4}(a,b,c,d)$ is equal to

$$\begin{cases} \text{DDT}_{F_4}(c,d) & \text{if } a=c, b=d, \text{ or} \\ & \quad \text{DDT}_{F_4}(c,d)=4, a=z_1+z_2, b=F_4(z_1)+F_4(z_2), \text{ or} \\ & \quad \text{DDT}_{F_4}(c,d)=4, a=z_1+z_2+c, b=F_4(z_1)+F_4(z_2+c) \\ 0 & \text{otherwise,} \end{cases}$$

where z_1, z_1+c, z_2, z_2+c are the four solutions of the equation $F_4(X+c)+F_4(X)=d$, if $\text{DDT}_{F_4}(c,d)=4$.

If $a=c, b=d, d\neq\frac{1}{c}$ and $\text{Tr}\left(\frac{1}{cd}\right)=0$, then $\text{EBCT}_{F_4}(a,b,c,d)=\text{DDT}_{F_4}(c,d)=2$. If $d=\frac{1}{c}$, and without loss of generality, we let $z_1=0, z_2=\omega c$. If $a=c, b=d$, then $\text{EBCT}_{F_4}(a,b,c,d)=\text{DDT}_{F_4}(c,d)=4$. If $a=z_1+z_2=\omega c$ and $b=F_4(z_1)+F_4(z_2)=\frac{1}{\omega c}$, then $\text{EBCT}_{F_4}(a,b,c,d)=\text{DDT}_{F_4}(c,d)=4$. If $a=z_1+z_2+c=\omega^2 c$ and $b=F_4(z_1)+F_4(z_2+c)=\frac{1}{\omega^2 c}$, then $\text{EBCT}_{F_4}(a,b,c,d)=\text{DDT}_{F_4}(c,d)=4$. Note that these last two cases can be summarized as $b=\frac{1}{a}$, $d=\frac{1}{c}$ and $(ad)^2+ad+1=0$. In all other cases, $\text{EBCT}_{F_4}(a,b,c,d)=0$.

We now compute the LBCT and UBCT of the inverse function using Corollary 7.2. As we have seen $\text{EBCT}_{F_4}(a,b,c,d)=2$, when $a=c, b=d, d\neq\frac{1}{c}$ and $\text{Tr}\left(\frac{1}{cd}\right)=0$, we infer that $\text{LBCT}_{F_4}(a,c,d)=2$ if $a=c\neq\frac{1}{d}$ and $\text{Tr}\left(\frac{1}{cd}\right)=0$. Similarly, $\text{UBCT}_{F_4}(c,d,b)=2$ if $b=d\neq\frac{1}{d}$ and $\text{Tr}\left(\frac{1}{cd}\right)=0$.

Clearly, when $d=\frac{1}{c}$, we can write $A=\{(c,c,d),(\omega c,c,d),(\omega^2 c,c,d) \mid \text{DDT}_{F_4}(c,d)=4\}$, as, in the case $\text{DDT}_{F_4}(c,d)=4$, $(c,c,d)\in A$, for $b=d$, $(\omega c,c,d)\in A$, for $b=\frac{1}{\omega c}$ and $(\omega^2 c,c,d)\in A$, for $b=\frac{1}{\omega^2 c}$. Thus, from Corollary 7.2, we have $\text{LBCT}_{F_4}(a,c,d)=4$, for $a\in\{c,\omega c,\omega^2 c\}$ and $d=\frac{1}{c}$. This is equivalent to $\text{LBCT}_{F_4}(a,c,d)=4$ when $d=\frac{1}{c}$ and $(ad)^2+ad=1=0$.

In a similar way, one can write $B=\{(c,d,d),(c,d,\frac{1}{\omega c}),(c,d,b=\frac{1}{\omega c}) \mid \text{DDT}_{F_4}(c,d)=4\}$, as, in the case $\text{DDT}_{F_4}(c,d)=4, (c,d,d)\in B$, for $a=c, (c,d,\frac{1}{\omega c})\in B$, for $a=\omega c$ and $(c,d,\frac{1}{\omega c})\in B$, for $a=\omega^2 c$, and the claim follows. □

Using Remark 2.6 and our results for the inverse function, we can easily compute its FBCT (also found in [12]).

Corollary 7.15 *Let $F_4(X)=X^{2^n-2}$ over $\mathbb{F}_{2^n}$, with n even. Then, for $a,b\in\mathbb{F}_{2^n}^*$,*

$$\text{FBCT}_{F_4}(a,b)=\begin{cases} 2^n, & \text{if } a=b, \\ 4, & \text{if } \left(\frac{a}{b}\right)^2+\frac{a}{b}+1=0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof If $a=b$, then trivially $\text{FBCT}_{F_4}(a,b)=2^n$ for any function F_4. If $a\neq b$, by Corollary 7.14, $\text{LBCT}_{F_4}(a,b,c)$ is nonzero if and only if $b=\frac{1}{c}$, $(ac)^2+ac+1=0$, which is equivalent to $b=\frac{1}{c}$, $\left(\frac{a}{b}\right)^2+\frac{a}{b}+a=0$. In that case, $\text{LBCT}_{F_4}(a,b,c)=4$. The result follows. □

8 DBCT for the Gold function

In this section, we study the DBCT entries for the Gold function. To this end, we need the LBCT and UBCT entries of the Gold function, which we have already computed in Corollary 7.3. Also, if $s|n$, then for any $\alpha \in \mathbb{F}_{2^n}$, we have $\sum_{i=0}^{t-1} \alpha^{2^{si}} = \mathrm{Tr}_s^n(\alpha)$, the relative trace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^s}$. If $s \nmid n$, then the elements of $\mathbb{F}_{2^n}$ can be embedded in $\mathbb{F}_{2^{sm}}$, since $m = \frac{n}{\gcd(s,n)}$.

Theorem 8.1 *Let $F_1(X) = X^{2^s+1}$ over $\mathbb{F}_{2^n}$ where $\gcd(s,n) = t$ and $m = \frac{n}{t}$ is odd. Then,*

$$\mathrm{DBCT}_{F_1}(a,d) = \begin{cases} 2^{2n} & \text{if } ad = 0, \\ 2^{2t}\left((2^t-2) + |N(a,d)|\right) & \text{if } ad \neq 0, \mathrm{Tr}_s^{sm}\left(\frac{d}{(a^{2^s+1})^{2^s+1}}\right) = u^4, u \in \mathbb{F}_{2^t}^* \setminus \{1\}, \\ 2^{2t} \cdot |N(a,d)| & \text{otherwise,} \end{cases}$$

where $|N(a,d)|$ denotes the cardinality of $\left\{b \in \mathbb{F}_{2^n}^* \mid \mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right) = \mathrm{Tr}_s^{sm}\left(\frac{d}{b^{2^s+1}}\right) = m\right\}$.

Proof First, assume that $a = 0$ or $d = 0$, then using definition of DBCT, we can write $\mathrm{DBCT}_{F_1}(a,d) = 2^{2n}$. Here F_1 is a permutation as m is given to be odd. Thus, for $a, d \in \mathbb{F}_{2^n}^*$, we can write

$$\mathrm{DBCT}_{F_1}(a,d) = \sum_{b=c} \mathrm{UBCT}_{F_1}(a,b,c)\,\mathrm{LBCT}_{F_1}(b,c,d) + \sum_{b\neq c} \mathrm{UBCT}_{F_1}(a,b,c)\,\mathrm{LBCT}_{F_1}(b,c,d).$$

Recall, for $a, d \in \mathbb{F}_{2^n}^*$, $t = \gcd(k,n)$ and $m = \frac{n}{t}$,

$$\mathrm{LBCT}_{F_1}(b,c,d) = \begin{cases} 2^t & \text{if } \mathrm{Tr}_s^{sm}\left(\frac{d}{c^{2^s+1}}\right) = \mathrm{Tr}_1^m(1) \text{ and } b \in c\mathbb{F}_{2^t}^* \text{ for } b,c,d \in \mathbb{F}_{2^n}^*, \\ \mathrm{DDT}_{F_1}(c,d) & \text{if } b = 0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathrm{UBCT}_{F_1}(a,b,c) = \begin{cases} 2^t & \text{if } \mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right) = \mathrm{Tr}_1^m(1) \text{ and for } a,b,c \in \mathbb{F}_{2^n}^*, \\ & \quad c \in \left\{b, (u+u^2)a^{2^s+1} + ub, u \in \mathbb{F}_{2^t}^* \setminus \{1\}\right\}, \\ \mathrm{DDT}_{F_1}(a,b) & \text{if } c = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly for $b = 0$, we have $\mathrm{DDT}_{F_1}(a,b) = \mathrm{DDT}_{F_1}(a,0) = 0$ as $a \neq 0$, thus, giving us $\mathrm{UBCT}_{F_1}(a,b,c) = 0$ and similarly for $c = 0$, we get $\mathrm{DDT}_{F_1}(c,d) = \mathrm{DDT}_{F_1}(0,d) = 0$ as $d \neq 0$ giving us $\mathrm{LBCT}_{F_1}(a,b,c) = 0$.

When $b \neq c$, then $\mathrm{UBCT}_{F_1}(a,b,c) = 2^t$ only if $c = (u+u^2)a^{2^s+1} + ub$ and $\mathrm{DDT}_{F_1}(a,b) = 2^t$, where $u \in \mathbb{F}_{2^t}^* \setminus \{1\}$. Also, $\mathrm{LBCT}_{F_1}(b,c,d) = 2^t$ only if $b = vc$ for some $v \in \mathbb{F}_{2^l}^*$ and $\mathrm{DDT}_{F_1}(c,d) = 2^t$. After combining them, we have $c = (u+u^2)a^{2^s+1} + uvc$, and $\mathrm{DDT}_{F_1}(a,b) = \mathrm{DDT}_{F_1}(c,d) = 2^t$. Notice that $v \neq u^{-1}$, because otherwise $a = 0$. Thus, we have $c = \frac{(u+u^2)}{1+uv}a^{2^s+1}$ and therefore, $b = \frac{v(u+u^2)}{1+uv}a^{2^s+1}$. Then $\mathrm{UBCT}_{F_1}(a,b,c) = \mathrm{LBCT}_{F_1}(b,c,d) = 2^t$ if $\mathrm{DDT}_{F_1}(a,b) = \mathrm{DDT}_{F_1}(c,d) = 2^t$ which is the same as $\sum_{i=0}^{m-1} \frac{b^{2^{si}}}{a^{2^{si}(2^s+1)}} = \sum_{i=0}^{m-1} \frac{d^{2^{si}}}{c^{2^{si}(2^s+1)}} = m$, where $m = \frac{n}{t}$. This is equivalent to $\sum_{i=0}^{m-1} \left(\frac{v(u+u^2)}{1+uv}\right)^{2^{si}} = \sum_{i=0}^{m-1} \frac{d^{2^{si}}}{(\frac{(u+u^2)}{1+uv}a^{2^s+1})^{2^{si}(2^s+1)}} = m$. One can see that the first equality $\sum_{i=0}^{m-1} \left(\frac{v(u+u^2)}{1+uv}\right)^{2^{si}} = m$, is nothing but $m\left(\frac{v(u+u^2)}{1+uv}\right) = m$, as $u, v \in \mathbb{F}_{2^t} \subseteq \mathbb{F}_{2^s}$.

Table 5 DBCT entries for the Gold function X^{2^s+1} over $\mathbb{F}_{2^n}$

n	s	a	d	u	$\mathrm{DBCT}_{F_1}(a,d)$
6	2	g^{25}	g^{22}	g^3+g^2+g+1	160
6	2	g^{63}	g^{56}	–	64
10	2	g^4	g^{186}	–	1024
10	4	g^2	g^{868}	g^5+g^3+g+1	1024

This is the same as saying $m\dfrac{u^2v+1}{uv+1}=0$, or equivalently we have $\frac{u^2v+1}{uv+1}=0$ or equivalently, $v=\frac{1}{u^2}$, as m is odd. Then we have $\frac{u^2v+1}{uv+1}=0$ or equivalently, $v=\frac{1}{u^2}$. This will give us $c=u^2(a^{2^s+1})$ and $b=a^{2^s+1}$. Thus, for $b=a^{2^s+1}$ and $c=u^2(a^{2^s+1})$, we have $\sum_{i=0}^{m-1}\frac{b^{2^{si}}}{a^{2^{si}(2^s+1)}}=1(\equiv m \pmod 2)$. Also, $\sum_{i=0}^{m-1}\frac{d^{2^{si}}}{(u^2a^{2^s+1})^{2^{si}(2^s+1)}}=m$ for some $a,d\in\mathbb{F}_{2^t}$. Obviously, such a and d always exist because $\sum_{i=0}^{m-1}\frac{d^{2^{si}}}{(u^2a^{2^s+1})^{2^{si}(2^s+1)}}=1$ if and only if there exists an $A\in\mathbb{F}_{2^{sm}}$ such that $\frac{d^{2^{si}}}{(u^2a^{2^s+1})^{2^{si}(2^s+1)}}=1+A+A^{2^s}$. Finally, we can conclude that for all $u\in\mathbb{F}_{2^t}$, choosing $c=u^2(a^{2^s+1})$ and $b=a^{2^s+1}$, for $\mathrm{UBCT}_{F_1}(a,b,c)=\mathrm{LBCT}_{F_1}(b,c,d)=2^t$, we should have $\sum_{i=0}^{m-1}\frac{d^{2^{si}}}{u^4(a^{2^s+1})^{2^{si}(2^s+1)}}=m$. Therefore, $\mathrm{DBCT}_{F_1}(a,d)=2^{2t}(2^l-2)$ if $\mathrm{Tr}_s^{sm}\left(\frac{d}{(a^{2^s+1})^{2^s+1}}\right)=u^4$, for some $u\in\mathbb{F}_{2^t}^*\backslash\{1\}$.

If $b=c$, then $\sum_{b=c}\mathrm{UBCT}_{F_1}(a,b,c)\,\mathrm{LBCT}_{F_1}(b,c,d)=\sum_b\mathrm{DDT}_{F_1}(a,b)\,\mathrm{DDT}_{F_1}(b,d)$, when $\sum_{i=0}^{m-1}\frac{b^{2^{si}}}{a^{2^{si}(2^s+1)}}=\sum_{i=0}^{m-1}\frac{d^{2^{si}}}{b^{2^{si}(2^s+1)}}=m$. If any of these sums is different from m, then the product of the DDT entries is 0. Hence, we need to compute $|N(a,d)|$, that is,

$$\begin{aligned}N(a,d)&=\left\{b\in\mathbb{F}_{2^n}^*\,\middle|\,\sum_{i=0}^{m-1}\frac{b^{2^{si}}}{a^{2^{si}(2^s+1)}}=\sum_{i=0}^{m-1}\frac{d^{2^{si}}}{b^{2^{si}(2^s+1)}}=m\right\}\\&=\left\{b\in\mathbb{F}_{2^n}^*\,\middle|\,\mathrm{Tr}_s^{sm}\left(\frac{b}{a^{2^s+1}}\right)=\mathrm{Tr}_s^{sm}\left(\frac{d}{b^{2^s+1}}\right)=m\right\},\end{aligned}$$

which completes the proof. □

Example 8.2 To illustrate Theorem 8.1, in Table 5 we give explicit values of the DBCT entries of the Gold function over $\mathbb{F}_{2^n}^*=\langle g\rangle$, where g is a primitive element of $\mathbb{F}_{2^n}$.

9 Conclusion

We have determined the entries of the newly proposed Extended Boomerang Connectivity Table (EBCT), Lower Boomerang Connectivity Table (LBCT) and Upper Boomerang Connectivity Table (UBCT) of a δ-uniform function by establishing connections with the entries of the well-known Difference Distribution Table (DDT), which we consider to be a significant observation. We also give the EBCT, LBCT and UBCT entries of three classes of differentially 4-uniform power permutations, namely, Gold, Kasami and Bracken–Leander. Moreover, it turns out that one of our results covers the result of Eddahmani et al. [13] and Man et al. [17] for the inverse function over $\mathbb{F}_{2^n}$. We also compute the DBCT entries for the

Gold function. We further challenge the community to determine the DBCT entries of other classes of interesting functions, such as Kasami and Bracken–Leander functions over $\mathbb{F}_{2^n}$.

Acknowledgements The authors would like to thank the editor, Prof. Daniele Bartoli, for the prompt handling of our paper, and they extend their appreciation to the very professional referees, who spotted errors/typos (now fixed), and provided beneficial and constructive comments to improve our paper. In particular, the referees challenged us to describe the CCZ/EA/A-equivalence of the considered concepts, which is now part of Sect. 4, or provide examples, whenever possible.

Author contributions All authors contributed equally to the paper. All authors reviewed the manuscript and agreed on the submission.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991).
2. Blondeau C., Canteaut A., Charpin P.: Differential properties of power functions. Int. J. Inf. Coding Theory **1**(2), 149–170 (2010).
3. Boukerrou H., Huynh P., Lallemand V., Mandal B., Minier M.: On the Feistel counterpart of the boomerang connectivity table. IACR Trans. Symmetric Cryptol. **1**, 331–362 (2020).
4. Bracken C., Leander G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields Appl. **16**(4), 231–242 (2010).
5. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inf. Theory **52**(3), 1141–1152 (2006).
6. Calderini M., Villa I.: On the boomerang uniformity of some permutation polynomials. Cryptogr. Commun. **12**, 1161–1178 (2020).
7. Carlet C., Charpin P., Zinoviev V.: Codes, Bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998).
8. Carlet C., Kim K.H., Mesnager S.: A direct proof of APN-ness of the Kasami functions. Des. Codes Cryptogr. **89**, 441–446 (2021).
9. Cid C., Huang T., Peyrin T., Sasaki Y., Song L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen J., Rijmen V. (eds.) Advances in Cryptology, EUROCRYPT 2018, LNCS 10821, pp. 683–714. Springer, Cham (2018).
10. Coulter R.S., Henderson M.: A note on the roots of trinomials over a finite field. Bull. Austral. Math. Soc. **69**, 429–432 (2004).
11. Delaune S., Derbez P., Vavrille M.: Catching the fastest boomerangs: application to SKINNY. IACR Trans. Symmetric Cryptol. **4**, 104–129 (2020).
12. 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. Cryptogr. Commun. **14**, 1301–1344 (2022).
13. Eddahmani S., Mesnager S.: Determination of cryptographic tables and properties related to the revised boomerang and its application to a fundamental *S*-box. Cryptogr. Commun. (2024). https://doi.org/10.1007/s12095-024-00767-2.
14. Hadipour H., Bagheri N., Song L.: Improved rectangle attacks on SKINNY and CRAFT. IACR Trans. Symmetric Cryptol. **2**, 140–198 (2021).
15. Hertel D., Pott A.: Two results on maximum nonlinear functions. Des. Codes Cryptogr. **47**, 225–235 (2008).
16. Li K., Qu L., Sun B., Li C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inf. Theory **65**(11), 7542–7553 (2019).
17. Man Y., Li N., Liu Z., Zeng X.: The explicit values of the UBCT, the LBCT and the DBCT of the inverse function. Finite Fields Appl. **100**, 102508 (2024).
18. Nyberg K.: Differentially uniform mappings for cryptography. In: Helleseth T. (ed.) Advances in Cryptology-EUROCRYPT 1993, LNCS 765, pp. 55–64. Springer, Berlin/Heidelberg (1994).

19. Wagner D.: The boomerang attack. In: Knudsen L.R. (ed.) Fast Software Encryption-FSE 1999. LNCS 1636, pp. 156–170. Springer, Berlin/Heidelberg (1999).
20. Wang H., Peyrin T.: Boomerang switch in multiple rounds. Application to AES variants and Deoxys. IACR Trans. Symmetric Cryptol. **1**, 142–169 (2019).
21. Xiong M., Yan H.: A note on the differential spectrum of a differentially 4-uniform power function. Finite Fields Appl. **48**, 117–125 (2017).
22. Yang Q., Song L., Sun S., Shi D., Hu L.: New properties of the double boomerang connectivity table. IACR Trans. Symmetric Cryptol. **4**, 208–242 (2022).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.