The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials

Sartaj Ul Hasan, Mohit Pal, Pantelimon Stănică

***Abstract*—The Difference Distribution Table (DDT) and the differential uniformity play a major role for the design of substitution boxes in block ciphers, since they indicate the function's resistance against differential cryptanalysis. This concept was extended recently to c-DDT and c-differential uniformity, which have the potential of extending differential cryptanalysis. Recently, a new theoretical tool, the Boomerang Connectivity Table (BCT) and the corresponding boomerang uniformity were introduced to quantify the resistance of a block cipher against boomerang-style attacks. Here we concentrate on two classes (introduced recently) of permutation polynomials over finite fields of even characteristic. For one of these, which is an involution used to construct a 4-uniform permutation, we explicitly determine the c-DDT entries and BCT entries. For the second type of function, which is a differentially 4-uniform function, we give bounds for its c-differential and boomerang uniformities.**

***Index Terms*—Finite fields, permutation polynomials, c-differential uniformity, boomerang uniformity, perfect and almost perfect c-nonlinearity**

MSC 2020: 12E20, 11T06, 11T55, 94A60

I. Introduction

Let $\mathbb{F}_q$ be the (binary) finite field with $q = 2^n$ elements, where n is a positive integer. We denote by $\mathbb{F}_q^*$, the multiplicative cyclic group of non-zero elements of the finite field $\mathbb{F}_q$. Let f be a function from the finite field $\mathbb{F}_q$ to itself. It is well-known that any function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be uniquely represented as a univariate polynomial of degree less than q. Therefore, we shall always consider f as a polynomial in $\mathbb{F}_q[X]$. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the mapping $X \mapsto f(X)$ is a permutation of $\mathbb{F}_q$.

Differential cryptanalysis, introduced by Biham and Shamir [3], is one of the most powerful attacks on block ciphers. To quantify the ability of a given function to resist the differential attack, Nyberg [23] introduced the notion of differential uniformity which is defined as follows. For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and for any $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by $D_f(X, a)$, is defined as

$$D_f(X, a) := f(X + a) + f(X) \text{ for all } X \in \mathbb{F}_q.$$

S. U. Hasan and M. Pal are with Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India; E-mail: {sartaj.hasan,2018RMA0021}@iitjammu.ac.in

Pantelimon Stănică is with Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA; E-mail: pstanica@nps.edu

For any $a, b \in \mathbb{F}_q$, the Difference Distribution Table (DDT) entry at point (a, b), denoted by $\Delta_f(a, b)$, is defined as $\Delta_f(a, b) := |\{X \in \mathbb{F}_q \mid D_f(X, a) = b\}|$. The differential uniformity of f, denoted by Δ_f, is defined as $\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}$. If $\Delta_f = \delta$, we say that the function f is δ-uniform. When $\delta = 1, 2$, we say that the function f is perfect nonlinear (PN) and almost perfect nonlinear (APN), respectively. Denote $w_i := |\{(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q \mid \Delta_f(a, b) = i\}|$. The differential spectrum of f is defined as the multiset $\Omega_f := \{w_0, w_1, \ldots, w_\delta\}$, where δ is the differential uniformity of f. It is easy to see that for finite fields of even characteristic, $w_i = 0$ for odd i. For further details concerning vectorial Boolean functions and their cryptographic properties, one may refer to the recent book of Carlet [8].

Motivated by a practical differential attack based on a new differential as introduced by Borisov et al. [5], Ellingsen et al. [13] proposed a new type of differential known as multiplicative differential defined as follows. For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of f at point a is defined as

$${}_cD_f(X, a) := f(X + a) + cf(X), \text{ for all } X \in \mathbb{F}_q.$$

For any $a, b \in \mathbb{F}_q$, the c-Difference Distribution Table (c-DDT) entry ${}_c\Delta_f(a, b)$ at point (a, b) is the number of solutions $X \in \mathbb{F}_q$ of the equation ${}_cD_f(X, a) = b$. The c-differential uniformity of f, denoted by ${}_c\Delta_f$, is given by ${}_c\Delta_f := \max\{{}_c\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ when } c = 1\}$. When ${}_c\Delta_f = \delta_c$, we say that c-differential uniformity of f is δ_c. When $\delta_c = 1, 2$, we say that the function f is perfect c-nonlinear (PcN) and almost perfect c-nonlinear (APcN), respectively. It is straightforward to see that the classical notion of differential uniformity can be obtained by putting $c = 1$. For some more recent results on c-differential uniformity, one may refer to [1], [14], [22], [27], [28], [31], [34].

In a block cipher, the nonlinearity of a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is also an important property. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. The *Walsh-Hadamard transform* is defined as the integer-valued function

$$\mathcal{W}_F(u) := \sum_{X \in \mathbb{F}_{2^n}} (-1)^{F(X) + \mathrm{Tr}(uX)}, \ u \in \mathbb{F}_{2^n},$$

where $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, given by $\mathrm{Tr}(X) = \sum_{i=0}^{n-1} X^{2^i}$. The (vectorial) Walsh transform

$\mathcal{W}_f(a,b)$ of a function $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ at $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ is the Walsh-Hadamard transform of its component function $\mathrm{Tr}(bf(X))$ at a, that is,

$$\mathcal{W}_f(a,b):=\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(bf(X)+aX)}.$$

The nonlinearity of f, denoted by $\mathrm{NL}(f)$, is defined by

$$\mathrm{NL}(f):=2^{n-1}-\frac{1}{2}\max_{(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}^*}|\mathcal{W}_f(a,b)|.$$

We slightly deviate to discuss about a different type of attack known as boomerang attack. The boomerang attack on block ciphers was proposed by Wagner [32]. Recently, at EUROCRYPT-2018, Cid et al. [10] introduced a systematic approach which is known as the Boomerang Connectivity Table (BCT), to analyze boomerang style attacks. Boura and Canteaut [6] further studied the BCT and coined the term boomerang uniformity, which is essentially the maximum value in the BCT, to quantify the resistance of a function against the boomerang attack. Later, Li et al. [19] proposed an equivalent technique to compute the BCT as follows. For any function $f:\mathbb{F}_q\to\mathbb{F}_q$, the BCT entry $\mathcal{B}_f(a,b)$ at point $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ is the number of solutions $(X,Y)\in\mathbb{F}_q\times\mathbb{F}_q$ of the following system

$$\begin{cases}f(X)+f(Y)=b\\ f(X+a)+f(Y+a)=b.\end{cases}\tag{1}$$

The boomerang uniformity of the function f, denoted by $\mathcal{B}_f$, is given by $\mathcal{B}_f:=\max\{\mathcal{B}_f(a,b)\mid a,b\in\mathbb{F}_q^*\}$. We note that this equivalent formulation does not require the compositional inverse of the function f and hence enables us to compute the BCT for non-permutations as well. It is easy to observe that for a permutation function $f:\mathbb{F}_q\to\mathbb{F}_q$, $\mathcal{B}_f(a,0)=q=\mathcal{B}_f(0,b)$, irrespective of values of a and b, therefore while computing boomerang uniformity, we exclude the first row and the first column of the BCT.

Cid et al. [10, Lemma 4] showed that for APN permutations, the BCT is the same as the DDT, except for the first row and the first column. Thus APN permutations offer an optimal resistance to both differential and boomerang attacks. For any permutation f, Cid et al. [10, Lemma 1] showed that $\mathcal{B}_f(a,b)\geq\Delta_f(a,b)$ for all $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$. Later, Mesnager et al. [21] showed that it holds for non-permutation functions, as well.

Since the seminal work of Cid et al. [10], functions with low boomerang uniformity have attracted a lot of attention in the last couple of years (see [7], [16], [18], [19], [20], [21], [30], [33] and the references therein). It is not quite clear what bounds on the differential and/or boomerang uniformities would allow a (modified) differential attack to work. It is known that the boomerang uniformity is not invariant under (some) linear layers (general EA-equivalence), so there are no general upper bounds on these uniformities to ensure security against a modified differential attack (we want to point out that even a differential uniformity of 8 is encountered in standard ciphers; e.g., the Russian standard, Kyuznechik (GOST R 34.12-2015) – see [4] and the references therein).

We shall now give the structure of the paper. We first recall some definitions and results in Section II. In Section III, we consider the c-differential uniformity of an involution over the finite field $\mathbb{F}_{2^n}$, which has been used to construct a class of differentially 4-uniform functions [2] and we prove that the c-differential uniformity of this involution is bounded above by 2 for all the values of c in the ambient finite field except for 0 and 1. Moreover, in Section IV, we give a complete description of the BCT entries of this involution and show that there are only two different entries in its BCT. The c-differential uniformity of a differentially 4-uniform function studied by Tan et al. [29], has been considered in Section V, and a bound for its boomerang uniformity is discussed in Section VI. Finally, we end with some concluding remarks in Section VII.

II. PRELIMINARIES

In the study of finite fields, permutation polynomials are very important objects as they are used in a variety of theoretical and practical applications. Therefore, the construction of infinite classes of permutation polynomials over finite fields is an interesting problem and a lot of research has been done in this direction in recent years. A permutation polynomial $f(X)$ is called a complete permutation polynomial if both $X\mapsto f(X)$ and $X\mapsto f(X)+X$ are permutations. In view of this, an interesting problem is to add some simple functions in a given permutation polynomial and to check for its permutation behaviour.

Recently, Beierle and Leander [2] considered the perturbation of a linear function by a trace function and showed that it is an involution. More precisely, the authors showed that the function $G(X)=X+\mathrm{Tr}(\alpha X+X^{2^k+1})$, where $\mathrm{Tr}(\alpha)=1$ and $\gcd(k,n)=1$ is an involution of the finite field $\mathbb{F}_{2^n}$, $n\geq 3$ odd. Here, Tr is the absolute trace function. Recall that the power function $f(X)=X^{2^k+1}$ over $\mathbb{F}_{2^n}$, $0\leq k<n$ is the Gold function [12] and if $\gcd(k,n)=\gcd(2k,n)$, then it is a permutation of $\mathbb{F}_{2^n}$. Nyberg [23] showed that when $\gcd(k,n)=s$, the Gold function is differentially 2^s-uniform. Thus, when $\gcd(k,n)=1$ and n odd, the Gold function is an APN permutation. Beierle and Leander [2] considered the composition of the involution $G(X)$ with the monomial X^ℓ, where $\ell=(2^k+1)^{-1}\pmod{2^n-1}$ with $\gcd(k,n)=1$, and showed that it is a differentially 4-uniform permutation with trivial nonlinearity 0. More precisely, the authors proved the following result.

Lemma 1. [2, Proposition 1] *Let $n\geq 3$ be odd, $\alpha\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha)=1$ and $\ell=(2^k+1)^{-1}\pmod{2^n-1}$ with $\gcd(k,n)=1$. Then the function $G_{\alpha,\ell}(X)=X^\ell+\mathrm{Tr}(\alpha X^\ell+X)$ is a differentially 4-uniform permutation with null nonlinearity over $\mathbb{F}_{2^n}$.*

We explicitly determine the c-DDT entries of the involution $G(X)$ for all $c \in \mathbb{F}_{2^n}$ in Section III. Moreover, we compute BCT entries of the involution $G(X)$ in Section IV.

We shall now turn our focus towards another interesting function. A systematic study of the permutation behaviour of the functions of the form $f(X) = g(X)+\gamma \mathrm{Tr}(h(X))$ has been done by Charpin and Kyureghyan [9] where the authors gave necessary conditions on $\gamma \in \mathbb{F}_{2^n}$, $g, h \in \mathbb{F}_{2^n}[X]$ for which $g(X) + \gamma \mathrm{Tr}(h(X))$ is a permutation polynomial. More precisely, authors gave the following two classes of permutation polynomials.

Lemma 2. [9, Corollary 1] *For any $\beta, \gamma \in \mathbb{F}_{2^n}$ and $h(X) \in \mathbb{F}_{2^n}[X]$, the polynomials*

(1) $f_1(X) = X + \gamma \mathrm{Tr}(h(X^2 + \gamma X) + \beta X)$*; and*
(2) $f_2(X) = X + \gamma \mathrm{Tr}(h(X) + h(X + \gamma) + \beta X)$

are permutation polynomials if and only if $\mathrm{Tr}(\beta\gamma) = 0$.

From the above lemma, it is easy to see that if $\beta = 0, \gamma = 1$ and $h(X) = X^{-1}$, the function $f_1'(X) = X + \mathrm{Tr}\left(\frac{1}{X^2+X}\right)$ is a permutation of $\mathbb{F}_{2^n}$. Tan et al. [29] showed that when n is even, the permutation polynomial $H(X) = f_1'(X^{-1}) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ is differentially 4-uniform. With regard to inverses of elements in the finite field, we shall use the convention that for any non-zero $a \in \mathbb{F}_{2^n}$, $a^{-1} := \frac{1}{a}$ and $0^{-1} := 0$ in the definition of $H(X)$ as well as in the rest of the paper. Recall that when n is even, the inverse mapping X^{-1} is a differentially 4-uniform permutation of $\mathbb{F}_{2^n}$ (see [23, Proposition 6]). Thus, the permutation behaviour and differential uniformity remain the same even after adding the term $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ in the inverse mapping X^{-1}. The c-differential uniformity of the inverse function has been studied by Ellingsen et al. [13]. In Section V, we shall consider the c-differential uniformity of the function $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$ for $1 \neq c \in \mathbb{F}_{2^n}$, to see the effect of the addition of the trace term $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ on the c-differential uniformity. We shall also consider the boomerang uniformity of the function $H(X)$ in Section VI.

We shall later use the following result [13, Lemma 11].

Lemma 3. *Let n be a positive integer. The equation $X^2 + aX + b = 0$, with $a, b \in \mathbb{F}_{2^n}, a \neq 0$, has two solutions X in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{b}{a^2}\right) = 0$, and no solutions otherwise.*

In [26] and [28], the authors used a Weil sums technique in computing the c-BCT and c-DDT entries, respectively. Here we recall the general technique to express the number of solutions of a given equation or a system of two equations over finite fields in terms of Weil sums for the convenience of the reader.

Let $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ be the canonical additive character of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) := \exp\left(\frac{2\pi i \mathrm{Tr}(X)}{2}\right) = (-1)^{\mathrm{Tr}(X)}.$$

It is easy to observe (see, for instance [26]) that the number of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ of the equation

$$f(X_1, X_2, \ldots, X_n) = b,$$

denoted by $N(b)$, is given by

$$\begin{aligned} &N(b) \\ &= \frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi_1(\beta(f(X_1, X_2, \ldots, X_n) - b)) \\ &= \frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(\beta(f(X_1, X_2, \ldots, X_n) - b))}. \end{aligned} \tag{2}$$

Similarly, the number of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ of the system

$$\begin{cases} f_1(X_1, X_2, \ldots, X_n) = b_1 \\ f_2(X_1, X_2, \ldots, X_n) = b_2, \end{cases}$$

denoted by $\widehat{N}(b)$, where $b = (b_1, b_2)$, is given by

$$\begin{aligned} &\widehat{N}(b) \\ &= \frac{1}{q^2} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi_1(\beta(f_1(X_1, \ldots, X_n) - b_1)) \\ &\qquad \sum_{\gamma \in \mathbb{F}_q} \chi_1(\gamma(f_2(X_1, \ldots, X_n) - b_2)) \\ &= \frac{1}{q^2} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(\beta(f_1(X_1, \ldots, X_n) - b_1))} \\ &\qquad \sum_{\gamma \in \mathbb{F}_q} (-1)^{\mathrm{Tr}(\gamma(f_2(X_1, \ldots, X_n) - b_2))}. \end{aligned} \tag{3}$$

III. The c-differential uniformity of a class of involutions

In this section, first we shall consider the c-differential uniformity of the involution $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$ over $\mathbb{F}_{2^n}$, where $n \geq 3$ is odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$ and $\gcd(k, n) = 1$. Let $f(X) = \mathrm{Tr}(X^{2^k+1})$ be the trace of the Gold function. For $c \in \mathbb{F}_q$, $c \notin \{0, 1\}$, the following result gives the c-DDT entries of the involution $G(X)$.

Theorem 4. *Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$ and let $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$ with $\gcd(k, n) = 1$. Then for any $a, b, c \in \mathbb{F}_{2^n}$, $c \notin \{0, 1\}$, the c-DDT entry ${}_c\Delta_G(a, b)$ of $G(X)$ at (a, b) is given by*

$${}_c\Delta_G(a, b) = \begin{cases} 0 & \text{if } A = 1 \text{ and } B = 1 \\ 1 & \text{if } B = 0 \\ 2 & \text{if } A = 0 \text{ and } B = 1, \end{cases}$$

where $A = \mathrm{Tr}\left(\frac{(a+b)(a^{2^{-k}} + a^{2^k})}{1+c} + \alpha a + a^{2^k+1}\right)$ and $B = \mathrm{Tr}\left(\frac{a^{2^{-k}} + a^{2^k}}{1+c}\right)$.

Proof. Recall that the c-DDT entry ${}_c\Delta_G(a,b)$ at the point (a,b) of the function $G(X)$ is given by the number of solutions $X \in \mathbb{F}_q$ of the following equation

$$\begin{aligned} b &= G(X+a) + cG(X) \\ &= X + a + \mathrm{Tr}\left(\alpha(X+a) + (X+a)^{2^k+1}\right) \\ &\quad + c\left(X + \mathrm{Tr}(\alpha X + X^{2^k+1})\right) \\ &= (1+c)\left(X + \mathrm{Tr}(\alpha X + X^{2^k+1})\right) + a \\ &\quad + \mathrm{Tr}(\alpha a + a^{2^k+1}) + \mathrm{Tr}(X^{2^k}a + Xa^{2^k}), \end{aligned}$$

which can be further written as

$$(1+c)G(X) + \mathrm{Tr}(X^{2^k}a + Xa^{2^k}) + G(a) + b = 0. \quad (4)$$

Now from (2), the number of solutions $X \in \mathbb{F}_q$ of the above Equation (4) is given by

$$\begin{aligned} &{}_c\Delta_G(a,b) \\ &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(\beta\left((1+c)G(X)+\mathrm{Tr}(X^{2^k}a+Xa^{2^k})+G(a)+b\right)\right)} \\ &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(\beta(1+c)G(X)+\beta\mathrm{Tr}(X^{2^k}a+Xa^{2^k})\right)} \\ &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\ &= \frac{1}{2^n}(M_0 + M_1), \end{aligned}$$

where M_0 and M_1 are the sums corresponding to $\mathrm{Tr}(\beta)=0$ and $\mathrm{Tr}(\beta)=1$, respectively. We shall now compute M_0 and M_1, separately. The first sum M_0 is given by

$$\begin{aligned} M_0 &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))} \\ &= 2^n + \sum_{\substack{\beta\in\mathbb{F}_q^* \\ \mathrm{Tr}(\beta)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))} \\ &= 2^n, \end{aligned}$$

where the last equality holds because $\beta(1+c) \neq 0$ and $G(X)$ is a permutation of $\mathbb{F}_{2^n}$, which makes the inner sum zero. Similarly, we can compute the second sum M_1, which is given by

$$\begin{aligned} &M_1 \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)(X+\mathrm{Tr}(\alpha X+X^{2^k+1})))+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}))} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)X)+\mathrm{Tr}(\beta(1+c))\mathrm{Tr}(\alpha X+X^{2^k+1})+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}))} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c))\mathrm{Tr}(\alpha X+X^{2^k+1})+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))}. \end{aligned}$$

Now we shall consider two cases, namely, $\mathrm{Tr}(\beta(1+c))=0$ and $\mathrm{Tr}(\beta(1+c))=1$, respectively. Equivalently, $\mathrm{Tr}(\beta c)=1$ and $\mathrm{Tr}(\beta c)=0$, respectively. We shall denote the sums corresponding to $\mathrm{Tr}(\beta c)=1$ and $\mathrm{Tr}(\beta c)=0$ by $M_{1,1}$ and $M_{1,0}$, respectively.

Case 1. Let $\mathrm{Tr}(\beta c)=1$. In this case,

$$\begin{aligned} M_{1,1} &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta c)=1=\mathrm{Tr}(\beta)}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta c)=1=\mathrm{Tr}(\beta)}} (-1)^{\mathrm{Tr}((a+b)\beta+\beta\mathrm{Tr}(\alpha a+a^{2^k+1}))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta c)=1=\mathrm{Tr}(\beta)}} (-1)^{\mathrm{Tr}((a+b)\beta)+\mathrm{Tr}(\beta)\mathrm{Tr}(\alpha a+a^{2^k+1})} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta c)=1=\mathrm{Tr}(\beta)}} (-1)^{\mathrm{Tr}((a+b)\beta+\alpha a+a^{2^k+1})} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))}. \end{aligned}$$

Notice that the inner sum will have a contribution if and only if $\beta(1+c) = a^{2^{-k}} + a^{2^k}$. Therefore, we have

$$M_{1,1} = \begin{cases} 0 & \text{if } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right) = 0 \\ 2^n \cdot (-1)^A & \text{if } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right) = 1, \end{cases}$$

where $A = \mathrm{Tr}\left(\frac{(a+b)(a^{2^{-k}}+a^{2^k})}{1+c} + \alpha a + a^{2^k+1}\right)$.

Case 2. Let $\mathrm{Tr}(\beta c) = 0$. In this case,

$$\begin{aligned} M_{1,0} &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1 \\ \mathrm{Tr}(\beta c)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \\ &\quad \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(X^{2^k+1}+X(a^{2^{-k}}+a^{2^k}+\beta(1+c)+\alpha)\right)} \\ &= \sum_{\substack{\beta\in\mathbb{F}_q \\ \mathrm{Tr}(\beta)=1 \\ \mathrm{Tr}(\beta c)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \mathcal{W}_f(u), \end{aligned}$$

where $u = a^{2^{-k}} + a^{2^k} + \beta(1+c) + \alpha$. We now apply an old result of Gold [12] (see also [17, Theorem 4]) which states that when n is odd and $\gcd(k,n) = 1$, the Walsh coefficient of the trace of the Gold function $f : X \mapsto X^{2^k+1}$ is given by

$$\mathcal{W}_f(u) = \begin{cases} 0 & \text{if } \mathrm{Tr}(u) = 0 \\ (-1)^{Tr(\gamma^{2^k+1})}\mathcal{W}_f(1) & \text{if } \mathrm{Tr}(u) = 1, \end{cases}$$

where γ is the unique element in $\mathbb{F}_{2^n}$ of trace 0 such that $u = \gamma^{2^k} + \gamma^{2^{-k}} + 1$, completed with one of Dillon and Dobbertin's results [11] (see also [17, Theorem 5]), which gives the Walsh-Hadamard coefficient

$$\mathcal{W}_f(1) = \begin{cases} +2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 1 \pmod 8 \\ -2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 3 \pmod 8. \end{cases}$$

It is easy to see that $\mathrm{Tr}(u) = \mathrm{Tr}(a^{2^{-k}}+a^{2^k}+\beta(1+c)+\alpha) = 0$. Therefore $M_{1,0} = 0$. This completes the proof. □

The case $c = 0$ is considered in the following remark.

Remark 5. *Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then for $c = 0$, the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where $\gcd(k,n) = 1$, is PcN.*

The following theorem gives the differential uniformity (the case $c = 1$) of the function $G(X)$.

Theorem 6. *Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then the DDT entries $\Delta_G(a,b)$ at point $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ of the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where $\gcd(k,n) = 1$, is given by*

$$\Delta_G(a,b) = \begin{cases} 2^n & \text{if } (a,b) = (1,1) \\ 2^{n-1} & \text{if } (a,b) \neq (1,1),\ G(a) \in \{b, b+1\} \\ 0 & \text{otherwise}. \end{cases}$$

Proof. Recall that the DDT entry $\Delta_G(a,b)$ at the point $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ of the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$ is given by the number of solutions $X \in \mathbb{F}_q$ of the following equation

$$\begin{aligned} & G(X+a) + G(X) = b \\ \iff\ & X + a + \mathrm{Tr}\left(\alpha(X+a) + (X+a)^{2^k+1}\right) \\ & \quad + X + \mathrm{Tr}(\alpha X + X^{2^k+1}) = b \\ \iff\ & a + \mathrm{Tr}(\alpha a + a^{2^k+1}) + \mathrm{Tr}(X^{2^k}a + Xa^{2^k}) = b \\ \iff\ & \mathrm{Tr}(X^{2^k}a + Xa^{2^k}) = G(a) + b \\ \iff\ & \mathrm{Tr}(X(a^{2^{-k}} + a^{2^k})) = G(a) + b \end{aligned}$$

Notice that when $a = 1$, then $G(a) = 1$ and in this case the above equation has 2^n solutions if $b = 1$ and no solution otherwise. For $a \notin \{0,1\}$, we have $a^{2^{-k}} + a^{2^k} \neq 0$ as $\gcd(k,n) = 1$ and n is odd. In this case the above equation has 2^{n-1} solutions if $G(a) \in \{b, b+1\}$ and has no solution, otherwise. □

IV. The boomerang uniformity of a class of involutions

In this section, we shall consider the boomerang uniformity of the involution $G(X)$. The following theorem gives the BCT entries of the involution $G(X)$ over the finite field $\mathbb{F}_{2^n}$.

Theorem 7. *Let $n \geq 3$ be odd and $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then the BCT entry $\mathcal{B}_G(a,b)$ at point $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ of the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where $\gcd(k,n) = 1$, is given by*

$$\mathcal{B}_G(a,b) = \begin{cases} 2^n & \text{if } \mathrm{Tr}((a^k + a^{-k})b) = 0 \\ 0 & \text{if } \mathrm{Tr}((a^k + a^{-k})b) = 1. \end{cases}$$

Proof. Recall that the BCT entry of $G(X)$ at point $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ is the number of solutions $(X,Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system

$$\begin{cases} G(X) + G(Y) = b \\ G(X+a) + G(Y+a) = b, \end{cases}$$

that is,

$$\begin{cases} X + Y + \mathrm{Tr}(\alpha(X+Y)) + \mathrm{Tr}(X^{2^k+1} + Y^{2^k+1}) & = b \\ X + Y + \mathrm{Tr}(\alpha(X+Y)) & \\ \qquad + \mathrm{Tr}((X+a)^{2^k+1} + (Y+a)^{2^k+1}) & = b. \end{cases} \tag{5}$$

Now adding both the equations in the above System (5), we have

$$\begin{aligned} 0 &= \mathrm{Tr}\left((X+a)^{2^k+1} + X^{2^k+1} + (Y+a)^{2^k+1} + Y^{2^k+1}\right) \\ &= \mathrm{Tr}\left(X^{2^k}a + Xa^{2^k} + Y^{2^k}a + Ya^{2^k}\right) \\ &= \mathrm{Tr}\left((X+Y)^{2^k}a + (X+Y)a^{2^k}\right). \end{aligned}$$

Therefore, System (5) is equivalent to the following system

$$\begin{cases} X + Y + \mathrm{Tr}\left(\alpha(X+Y) + X^{2^k+1} + Y^{2^k+1}\right) = b \\ \mathrm{Tr}\left((X+Y)^{2^k}a + (X+Y)a^{2^k}\right) = 0, \end{cases}$$

and so,

$$\begin{cases} X+Y+\mathrm{Tr}\left(\alpha(X+Y)+(X+Y)^{2^k+1}\right) \\ \qquad +\mathrm{Tr}\left(X^{2^k}Y+XY^{2^k}\right)=b \\ \mathrm{Tr}\left((X+Y)^{2^k}a+(X+Y)a^{2^k}\right)=0. \end{cases} \tag{6}$$

Taking $Y=X+Z$, the above System (6) becomes

$$\begin{cases} Z+\mathrm{Tr}\left(\alpha Z+Z^{2^k+1}\right)+\mathrm{Tr}\left(X^{2^k}Z+XZ^{2^k}\right)=b \\ \mathrm{Tr}\left(Z^{2^k}a+Za^{2^k}\right)=0, \end{cases}$$

which can be written as

$$\begin{cases} G(Z)+\mathrm{Tr}\left(X(Z^{2^{-k}}+Z^{2^k})\right)=b \\ \mathrm{Tr}\left(a(Z^{2^{-k}}+Z^{2^k})\right)=0. \end{cases} \tag{7}$$

Now from (3), the number of solutions $(X,Z)\in\mathbb{F}_q\times\mathbb{F}_q$ of the above System (7), denoted as $\mathcal{B}_G(a,b)$, is given by

$$\begin{aligned} &\mathcal{B}_G(a,b) \\ =&\frac{1}{2^{2n}}\sum_{X,Z\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(G(Z)+\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))+b))} \\ &\qquad\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k})))} \\ =&\frac{1}{2^{2n}}\sum_{X,Z\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(G(Z)+b))+\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\frac{1}{2^{2n}}\sum_{\beta,\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta b)} \\ &\qquad\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ =&\frac{1}{2^{2n}}(S_0+S_1), \end{aligned} \tag{8}$$

where S_0 and S_1 are the sums corresponding to $\mathrm{Tr}(\beta)=0$ and $\mathrm{Tr}(\beta)=1$, respectively. We shall now compute S_0 and S_1 separately. We first consider the sum S_0 given by

$$\begin{aligned} S_0=&\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n}} \\ &\qquad\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ =&\ 2^n\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n}} \\ &\qquad\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\ 2^n\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}(S_{0,0}+S_{0,1}), \end{aligned} \tag{9}$$

where $S_{0,0}$ and $S_{0,1}$ are the sums corresponding to $\mathrm{Tr}(\gamma)=0$ and $\mathrm{Tr}(\gamma)=1$, respectively. We shall now compute $S_{0,0}$ and $S_{0,1}$, separately. Consider

$$\begin{aligned} S_{0,0}=&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=0}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=0}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))} \\ =&\ 2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))}. \end{aligned}$$

Similarly,

$$\begin{aligned} &S_{0,1} \\ =&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=1}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=1}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\ 2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta Z+\beta\mathrm{Tr}(\alpha Z+Z^{2^k+1}))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\ 2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta Z)+\mathrm{Tr}(\beta)\mathrm{Tr}(\alpha Z+Z^{2^k+1})+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ =&\ 2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta Z)+\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}))} \\ =&\ 2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))}. \end{aligned}$$

Now putting the values of $S_{0,0}$ and $S_{0,1}$ into Equation (10), we have

$$\begin{aligned} S_0=&\ 2^{2n-1}\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)} \\ &\left(\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))}+\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))}\right) \\ =&\ 2^{2n-1}\left(2^n+\sum_{\substack{\beta\in\mathbb{F}_q^*\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))}\right. \\ &\left.+\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))}\right) \\ =&\ 2^{3n-1} \end{aligned}$$

$$+2^{2n-1}\left(\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=0}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))}\right)$$
$$=2^{3n-1}+2^{3n-1}(-1)^{\mathrm{Tr}(b(a^{2^{-k}}+a^{2^k}))},$$

where the second last equality holds because $G(Z)$ is a permutation of $\mathbb{F}_{2^n}$. The last equality holds as the inner sum will contribute if and only if $\beta=a^{2^{-k}}+a^{2^k}$.

Now, we shall calculate S_1 which is given by

$$\begin{aligned}S_1=&\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=1}}(-1)^{\mathrm{Tr}(\beta b)}\\&\sum_{\gamma\in\mathbb{F}_{2^n}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=1}}(-1)^{\mathrm{Tr}(\beta b)}\\&\sum_{\gamma\in\mathbb{F}_{2^n}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&\sum_{\substack{\beta\in\mathbb{F}_q\\ \mathrm{Tr}(\beta)=1}}(-1)^{\mathrm{Tr}(\beta b)}(S_{1,0}+S_{1,1}),\end{aligned}\tag{10}$$

where $S_{1,0}$ and $S_{1,1}$ are the sum corresponding to $\mathrm{Tr}(\gamma)=0$ and $\mathrm{Tr}(\gamma)=1$, respectively. We shall now compute $S_{1,0}$ and $S_{1,1}$ separately. Consider

$$\begin{aligned}&S_{1,0}\\=&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=0}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=0}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))}\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))}\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&\left(\sum_{\substack{Z\in\mathbb{F}_{2^n}\\ Z\notin\{0,1\}}}(-1)^{\mathrm{Tr}(\beta G(Z))}\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\right)\\&2^{n-1}+2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta G(1))}\\=&2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta(1+\mathrm{Tr}(\alpha+1))}\\=&2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta)},\end{aligned}$$

where the second to last identity holds because $Z^{2^{-k}}+Z^{2^k}=0$, or equivalently, $Z^{2^{2k}}+Z=0$ if and only if $Z\in\{0,1\}$. For $Z\in\mathbb{F}_{2^n}\backslash\{0,1\}$, $Z^{2^{-k}}+Z^{2^k}\neq 0$ and as a consequence, the inner sum will be equal to zero. The last equality holds because $\mathrm{Tr}(\alpha)=1$. Similarly,

$$\begin{aligned}S_{1,1}=&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=1}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&\sum_{\substack{\gamma\in\mathbb{F}_q\\ \mathrm{Tr}(\gamma)=1}}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&2^{n-1}\sum_{Z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta G(1))}\\&+2^{n-1}\sum_{\substack{Z\in\mathbb{F}_{2^n}\\ Z\notin\{0,1\}}}(-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))}\\&\sum_{X\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}\\=&2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta+\beta\mathrm{Tr}(\alpha+1))}\\=&2^{2n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(\beta)}.\end{aligned}$$

Now putting the values of $S_{1,0}$ and $S_{1,1}$ in Equation (12), we have

$$S_1=\sum_{\beta\in\mathbb{F}_q,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\left(2^{2n}+2^{2n}\cdot(-1)^{\mathrm{Tr}(\beta)}\right)=0.$$

Now putting the values of S_0 and S_1 into Equation (8), we have

$$\mathcal{B}_G(a,b)=2^{n-1}+2^{n-1}\cdot(-1)^{\mathrm{Tr}\left(b\left(a^{2^{-k}}+a^{2^k}\right)\right)}.$$

This completes the proof. □

V. The c-differential uniformity of a perturbed inverse function

In this section, we shall consider the c-differential uniformity of the function $H(X)=X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$, for all positive integers n and $1\neq c\in\mathbb{F}_q$. We shall first recall the following lemma (we have slightly modified the statement as per our requirements), which gives the c-differential uniformity of the inverse mapping.

Lemma 8. [13, Theorem 12] *Let n be a positive integer and $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$. For any $a,b\in\mathbb{F}_{2^n}$, the solutions $X\in\mathbb{F}_q$*

of the equation $(X+a)^{-1}+cX^{-1}=b$ *are described as follows:*

$$\begin{cases} \{\frac{ac}{1+c}\} & \text{if } b=0 \\ \{b^{-1}(1+c)\} & \text{if } a=0, b\neq 0 \\ \{0\} & \text{if } ab=1 \text{ and } \mathrm{Tr}(1/c)=1 \\ \{0, \text{ two more solutions}\} & \text{if } ab=1 \text{ and } \mathrm{Tr}(1/c)=0 \\ \{a\} & \text{if } ab=c \text{ and } \mathrm{Tr}(c)=1 \\ \{a, \text{ two more solutions}\} & \text{if } ab=c \text{ and } \mathrm{Tr}(c)=0 \\ \{\left(\frac{ac}{b}\right)^{2^{n-1}}\} & \text{if } ab=1+c \\ \{\text{two solutions}\} & \text{if } ab\neq 1, c, 1+c \\ & \quad \text{and } \mathrm{Tr}\left(\frac{abc}{(ab)^2+c^2+1}\right)=0 \\ \text{no solution} & \text{otherwise}. \end{cases}$$

The following theorem gives a bound for the c-differential uniformity of the function $H(X)$ over $\mathbb{F}_{2^n}$, for all positive integers n and $1\neq c\in\mathbb{F}_q$.

Theorem 9. *Let* $1\neq c\in\mathbb{F}_{2^n}$ *and* $H:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ *be defined by* $H(X)=X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. *We have*:

(i) If $c=0$, *then* $H(X)$ *is PcN;*
(ii) If $\mathrm{Tr}(c)=1=\mathrm{Tr}(1/c)$, *then* ${}_c\Delta_H\leq 8$;
(iii) Otherwise, ${}_c\Delta_H\leq 9$.

Proof. For any fixed $1\neq c\in\mathbb{F}_{2^n}$, the c-differential uniformity of the function $H(X)=X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ equals the maximum number of solutions $X\in\mathbb{F}_q$ of the following equation

$$(X+a)^{-1}+\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)+cX^{-1}+c\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=b, \tag{11}$$

where $a,b\in\mathbb{F}_{2^n}$. Notice that when $c=0$, the above Equation (13) reduces to

$$(X+a)^{-1}+\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=b,$$

which has exactly one solution for each pair $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ as the left hand side is a PP. Let $c\notin\{0,1\}$. For any fixed $c\notin\{0,1\}$, if $a=0$, Equation (13) reduces to

$$X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=b(1+c)^{-1},$$

which has exactly one solution for each $b\in\mathbb{F}_{2^n}$ as the left hand side is a PP. Now for any $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$, to find the solutions of Equation (13), we shall split the analysis into four cases.

Case 1. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=0=\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. In this case, Equation (13) reduces to

$$(X+a)^{-1}+cX^{-1}=b. \tag{12}$$

Notice that if 0 is a solution of Equation (13) then either $ab=1$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=0$ or $a(b+1)=1$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. Similarly, if a is a solution of Equation (13) then either $ab=c$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=0$ or $a(b+c)=c$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. From Lemma 8, we know that if $ab=1$ and $\mathrm{Tr}(1/c)=0$, then the Equation (14) has three solutions and one among them is zero. Similarly, if $ab=c$ and $\mathrm{Tr}(c)=0$, then the Equation (14) has three solutions and one among them is a. In rest of the cases Equation (14) can have at most two solutions. From here we conclude that for any fixed $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$, Equation (13) can have at most three solutions if either $\mathrm{Tr}(1/c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=0$ and $ab=1$, or $\mathrm{Tr}(c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=0$ and $ab=c$. Otherwise, there can be at most two solutions of Equation (13) from this case.

Case 2. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=1=\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. In this case, Equation (13) reduces to

$$(X+a)^{-1}+cX^{-1}=b+c+1. \tag{13}$$

Again, by Lemma 8, if $a(b+c+1)=1$ and $\mathrm{Tr}(1/c)=0$, then the Equation (15) has three solutions and one among them is zero. It is easy to see that when $X=0$, $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=0$. Therefore 0 can not be a solution of Equation (13). Similarly, if $a(b+c+1)=c$ and $\mathrm{Tr}(c)=0$, then Equation (15) has three solutions and one among them is a. Notice that, when $X=a$, we have $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=0$. Therefore a can not be a solution of Equation (13). Thus, we can get at most two solutions of Equation (13) from this case.

Case 3. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=0$ and $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=1$. Then Equation (13) reduces to

$$(X+a)^{-1}+cX^{-1}=b+c. \tag{14}$$

From Lemma 8, we know that if $a(b+c)=1$ and $\mathrm{Tr}(1/c)=0$, then Equation (16) has three solutions and one among them is 0. As we are in the case $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=1$, the solution $X=0$ of Equation (16) will not be a solution of Equation (13). Similarly, if $a(b+c)=c$ and $\mathrm{Tr}(c)=0$, then Equation (16) has three solutions and one among them is a. It is easy to see that the solution $X=a$ of (16) will be a solution of Equation (13) if and only if $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. Thus, for any fixed $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$, if $\mathrm{Tr}(c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$ and $a(b+c)=c$, then there can be at most 3 solutions of Equation (13) from this case, otherwise there can be at most 2 solutions.

Case 4. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=1$ and $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=0$. Then Equation (13) reduces to

$$(X+a)^{-1}+cX^{-1}=b+1. \tag{15}$$

Again, by Lemma 8, if $a(b+1)=1$ and $\mathrm{Tr}(1/c)=0$, then Equation (17) has three solutions and one among them is 0. Notice that the solution $X=0$ of Equation (17) will be a solution of Equation (13) if and only if $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. Similarly, if $a(b+1)=c$ and $\mathrm{Tr}(c)=0$, then Equation (17) has three solutions and one among them is a. Notice that solution $X=a$ of (17) will not be a solution of Equation (13)

as $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) \neq 1$. Thus, for any fixed $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$, if $\mathrm{Tr}(1/c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$ and $a(b+1)=1$ then there can be at most 3 solutions of Equation (13) from this case, otherwise there can be at most 2 solutions. This completes the proof. □

Table I gives the maximum possible value of ${}_c\Delta_H$, where $c \notin \{0,1\}$, of the function $H(X)$ over $\mathbb{F}_{2^n}$ for some small values of n.

Remark 10. *It remains an open question to investigate if the bound for the c-differential uniformity of the perturbed inverse function $H(x)$ in Theorem 9 could indeed be attained.*

VI. The boomerang uniformity of a perturbed inverse function

Boura and Canteaut [6] studied the BCT entries of the inverse mapping and proved the following lemma. We are also including the proof here (however, our technique is slightly different from the one given in [6]), for the convenience of the reader.

Lemma 11. [6, Proposition 6] *Let $f(X)=X^{-1}$ be a map from $\mathbb{F}_{2^n}$ to itself with n even. Then for any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, the boomerang system*

$$\begin{cases} X^{-1}+Y^{-1}=b \\ (X+a)^{-1}+(Y+a)^{-1}=b \end{cases} \tag{16}$$

has the following solutions if $n \equiv 2 \pmod 4$

$$\begin{cases} \{(0,a),(a,0),(a\omega,a\omega^2),(a\omega^2,a\omega)\} \text{ if } ab=1 \\ \{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\} \text{ if } ab=\omega \\ \{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\} \text{ if } ab=\omega^2 \\ \{(X_1,X_1+a),(X_1+a,X_1)\}, X_1^2+aX_1+\frac{a}{b}=0 \\ \qquad \text{if } \mathrm{Tr}(\frac{1}{ab})=0, \text{ and } ab\neq 1,\omega,\omega^2 \\ \text{no solution otherwise,} \end{cases}$$

where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$ is a primitive cube root of unity. When $n \equiv 0 \pmod 4$, then there are the following additional solutions

$$\begin{cases} \{(X_2,X_2+a),(X_2+a,X_2)\}, \\ \quad X_2^2+aX_2+a^2\omega^2=0 \qquad \text{if } ab=\omega \\ \{(X_3,X_3+a),(X_3+a,X_3)\}, \\ \quad X_3^2+aX_3+a^2\omega=0 \qquad \text{if } ab=\omega^2. \end{cases}$$

Proof. It is easy to see that $(0,0)$ and (a,a) can not be a solution of Equation (18) as $b \neq 0$. Now we shall divide our discussion into the following different cases.

Case 1. Let $X=0$. In this case, System (18) reduces to

$$\begin{cases} Y=b^{-1} \\ (b^{-1}+a)^{-1}=b+a^{-1}. \end{cases} \tag{17}$$

It is easy to see that if $ab=1$ then $(0,a)$ is the solution of above System (19). If $ab \neq 1$ then System (19) reduces to

$$\begin{aligned} 0 &= (b^{-1}+a)(b+a^{-1})+1 \\ &= 1+a^{-1}b^{-1}+ab \\ &= (ab)^2+ab+1. \end{aligned}$$

Thus $ab \neq 1$ is a root of $X^3+1=0$, hence a primitive element of $\mathbb{F}_{2^2}$, say ω, ω^2. When $ab=\omega$, Equation (19) has exactly one solution $(0,a\omega^2)$. Similarly, when $ab=\omega^2$, Equation (19) has exactly one solution $(0,a\omega)$. If $ab \notin \{1,\omega,\omega^2\}$, then System (19) has no solution.

Case 2. Let $X=a$. In this case, System (18) reduces to

$$\begin{cases} Y=(b+a^{-1})^{-1} \\ ((b+a^{-1})^{-1}+a)^{-1}=b. \end{cases} \tag{18}$$

It is easy to see that if $ab=1$ then $(a,0)$ is the solution of above System (20). Also notice that if $ab \neq 1$ then $(b+a^{-1})^{-1}+a \neq 0$ as $b \neq 0$. Thus, for $ab \neq 1$ System (20) reduces to

$$\begin{aligned} (b+a^{-1})^{-1} &= a+b^{-1} \\ (a+b^{-1})(a^{-1}+b) &= 1 \\ (ab)^2+ab+1 &= 0. \end{aligned}$$

Thus $ab \neq 1$ is a root of $X^3+1=0$, hence a primitive element of $\mathbb{F}_{2^2}$. When $ab=\omega$, System (20) has exactly one solution $(a,a\omega)$. Similarly, when $ab=\omega^2$, System (20) has exactly one solution $(a,a\omega^2)$. If $ab \notin \{1,\omega,\omega^2\}$, then System (20) has no solution.

Case 3. Let $Y=0$. Since System (18) is symmetric in the variables X and Y, this case directly follows from Case 1. Thus, System (18) has exactly one solution $(a,0),(a\omega^2,0)$ and $(a\omega,0)$ when $ab \in \{1,\omega,\omega^2\}$, respectively. If $ab \notin \{1,\omega,\omega^2\}$, then System (18) has no solution with $Y=0$.

Case 4. Let $Y=a$. Since System (18) is symmetric in the variables X and Y, this case directly follows from Case 2. Thus, System (18) has exactly one solution $(0,a),(a\omega,a)$ and $(a\omega^2,a)$ when $ab \in \{1,\omega,\omega^2\}$, respectively. If $ab \notin \{1,\omega,\omega^2\}$, then System (18) has no solution with $Y=a$.

Case 5. Let $X \notin \{0,a\}$ and $Y \notin \{0,a\}$. Now, System (18) becomes

$$\begin{cases} X+Y=bXY \\ X+Y=b(XY+aX+aY+a^2), \end{cases} \tag{19}$$

which is equivalent to

$$\begin{cases} X+a & =Y \\ X^2+aX+\frac{a}{b} & =0. \end{cases} \tag{20}$$

Now if $ab=1$, then the second equation of System (22) reduces to $X^2+aX+a^2=0$, which has two solutions $a\omega, a\omega^2$. Thus, System (21) has two solutions, namely $(a\omega,a\omega^2)$ and $(a\omega^2,a\omega)$. If $ab=\omega$, then the second equation of System (22) becomes $X^2+aX+a^2\omega^2=0$, which has two solutions if and only if $\mathrm{Tr}(\omega^2)=\mathrm{Tr}(\omega)=0$. Here, one may note that $\mathrm{Tr}(\omega)=0$ if and only if $n \equiv 0$

TABLE I: Maximum value of ${}_c\Delta_H$ over the finite field $\mathbb{F}_{2^n}$.

n	when $\mathrm{Tr}(c)=0=\mathrm{Tr}(\frac{1}{c})$ or $\mathrm{Tr}(c)+\mathrm{Tr}(\frac{1}{c})=1$	when $\mathrm{Tr}(c)=1=\mathrm{Tr}(\frac{1}{c})$
2	1	1
3	3	1
4	5	4
5	6	6
6	7	6
7	7	6
8	8	7

$(\mathrm{mod}\ 4)$. Similarly, if $ab=\omega^2$, the second equation of System (22) becomes $X^2+aX+a^2\omega=0$, which has two solutions if and only if $\mathrm{Tr}(\omega)=0$. Again, $\mathrm{Tr}(\omega)=0$ if and only if $n\equiv 0\ (\mathrm{mod}\ 4)$. When $X,Y\notin\{0,a\}$ and $ab\notin\{1,\omega,\omega^2\}$, then System (22) has two solutions if and only if $\mathrm{Tr}\left(\frac{1}{ab}\right)=0$. □

The following is an immediate corollary of Lemma 11.

Corollary 12. *Let $f(X)=X^{-1}$ be a map from $\mathbb{F}_{2^n}$ to itself with n even. Then the boomerang uniformity of f is given by*

$$\mathcal{B}_f=\begin{cases}4 & \text{if } n\equiv 2 \pmod 4\\ 6 & \text{if } n\equiv 0 \pmod 4.\end{cases}$$

Now we shall consider the boomerang uniformity of the differentially 4-uniform permutation $H(X)=X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$ with n even in the following theorem.

Theorem 13. *Let n be even and $H(X)=X^{-1}+\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ be a map from $\mathbb{F}_{2^n}$ to itself. Then the boomerang uniformity of H is less than or equal to* 12.

Proof. For any $a,b\in\mathbb{F}_{2^n}^*$, the Boomerang Connectivity Table (BCT) entry $\mathcal{B}_H(a,b)$ of H at point (a,b) is the number of solutions $(X,Y)\in\mathbb{F}_q\times\mathbb{F}_q$ of the following system

$$\begin{cases}X^{-1}+Y^{-1}+\mathrm{Tr}\left(\dfrac{X^2}{X+1}+\dfrac{Y^2}{Y+1}\right)=b;\\ (X+a)^{-1}+(Y+a)^{-1}\\ \qquad\qquad +\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)=b.\end{cases}\tag{21}$$

We shall now give the strategy of the proof. Depending upon the values of $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)$ and $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)$, we shall split the analysis of solutions of the above System (23) into two parts. In the first part, we shall consider two cases, namely, Case 1 and Case 2 corresponding to $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)=0=\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)$ and $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)=1=\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)$, respectively. We then compute the maximum number of solutions $(X,Y)\in\mathbb{F}_q\times\mathbb{F}_q$ of the system of equations in each of these cases, individualy. Next, we compute the maximum number of solutions of System (23) that can be obtained from Case 1 and Case 2. In the second part also, we shall consider two cases, namely, Case 3 corresponding to $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)=0$ and $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)=1$, and Case 4 corresponding to $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)=1$ and $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)=0$. We then compute the maximum number of solutions $(X,Y)\in\mathbb{F}_q\times\mathbb{F}_q$ of the system of equations in each of these cases, individualy and then we compute the maximum number of solutions of System (23) that can be obtained from Case 3 and Case 4. Finally, combining the first and second part, we compute the maximum number of solutions of System (23).

Case 1. Let $\mathrm{Tr}\left(\dfrac{X^2}{X+1}+\dfrac{Y^2}{Y+1}\right)=0=\mathrm{Tr}\left(\dfrac{X^2+a^2}{X+a+1}+\dfrac{Y^2+a^2}{Y+a+1}\right)$. In this case, System (23) reduces to

$$\begin{cases}X^{-1}+Y^{-1}=b\\ (X+a)^{-1}+(Y+a)^{-1}=b.\end{cases}\tag{22}$$

From Lemma 11, we know that the above System (24) has four solutions if $ab=1$; four solutions if $ab\in\{\omega,\omega^2\}$ and $n\equiv 2\ (\mathrm{mod}\ 4)$; six solutions if $ab\in\{\omega,\omega^2\}$ and $n\equiv 0\ (\mathrm{mod}\ 4)$; two solutions if $\mathrm{Tr}(\frac{1}{ab})=0$ and $ab\notin\{1,\omega,\omega^2\}$; and no solutions, otherwise.

Case 2. Let $\mathrm{Tr}\left(\dfrac{X^2}{X+1}+\dfrac{Y^2}{Y+1}\right)=1=\mathrm{Tr}\left(\dfrac{X^2+a^2}{X+a+1}+\dfrac{Y^2+a^2}{Y+a+1}\right)$. In this case, System (23)

reduces to

$$\begin{cases} X^{-1}+Y^{-1}=b+1 \\ (X+a)^{-1}+(Y+a)^{-1}=b+1. \end{cases} \tag{23}$$

Again, from Lemma 11, we know that the above System (25) has four solutions if $a(b+1)=1$; four solutions if $a(b+1) \in \{\omega, \omega^2\}$ and $n \equiv 2 \pmod 4$; six solutions if $a(b+1) \in \{\omega, \omega^2\}$ and $n \equiv 0 \pmod 4$; two solutions if $\mathrm{Tr}(\frac{1}{a(b+1)}) = 0$ and $a(b+1) \notin \{1, \omega, \omega^2\}$ and no solutions, otherwise.

We shall now compute the maximum number of solutions of Equation (23) that can be obtained from Case 1 and Case 2.

(i) Let $ab=1$. In this subcase, if $ab+a=1$, $a=0$ which is not possible as $a \neq 0$. If $ab+a=\omega$, we have $(a,b)=(\omega^2,\omega)$. For $(a,b)=(\omega^2,\omega)$, the four solutions of System (24) are $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$. It is easy to verify that all these four solutions are solutions of System (23). For $(a,b)=(\omega^2,\omega)$, System (25) has four solutions $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$, when $n \equiv 2 \pmod 4$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. A simple calculation shows that none of these four solutions satisfies System (23). If $ab+a=\omega^2$, we have $(a,b)=(\omega,\omega^2)$. For $(a,b)=(\omega,\omega^2)$, the four solutions of System (24) are $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$ and one can easily verify that these four solutions are solutions of System (23). For $(a,b)=(\omega,\omega^2)$, we have four solutions of (25), when $n \equiv 2 \pmod 4$, which are given by $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. A routine calculation shows that none of these four solutions are solutions of System (23). If $ab+a \notin \{1,\omega,\omega^2\}$, System (25) has two solutions if $\mathrm{Tr}\left(\frac{1}{1+a}\right)=0$ and no solution, otherwise.

(ii) Let $ab=\omega$. In this subcase, if $ab+a=1$ then $(a,b)=(\omega^2,\omega^2)$. For $(a,b)=(\omega^2,\omega^2)$, System (24) has four solutions $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$ if $n \equiv 2 \pmod 4$ and there are two additional solutions if $n \equiv 0 \pmod 4$. A simple calculation shows that all these four solutions are also a solution of equation (23). For $(a,b)=(\omega^2,\omega^2)$, the four solutions of System (25) are $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$. A simple calculation shows that none of these four solutions satisfies System (23). If $ab+a=\omega$ then $a=0$ which is not possible as $a \neq 0$. Now if $ab+a=\omega^2$, we have $(a,b)=(1,\omega)$. For $(a,b)=(1,\omega)$, System (24) has four solutions $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$ if $n \equiv 2 \pmod 4$ and there will be two additional solutions if $n \equiv 0 \pmod 4$. A simple calculation yields that all these four solutions are solutions of System (23). For $(a,b)=(1,\omega)$, the four solutions of (25), when $n \equiv 2 \pmod 4$, are $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. It is easy to verify that none of these four solutions are solutions of System (23). If $ab+a \notin \{1,\omega,\omega^2\}$, System (25) has two solutions if $\mathrm{Tr}\left(\frac{1}{a+\omega}\right)=0$ and no solution, otherwise.

(iii) Let $ab=\omega^2$. In this subcase, if $ab+a=1$, we have $(a,b)=(\omega,\omega)$. For $(a,b)=(\omega,\omega)$, System (24) has four solutions $\{(0,\omega^2),(\omega^2,0),(\omega,1),(1,\omega)\}$ if $n \equiv 2 \pmod 4$ and there are two additional solutions if $n \equiv 0 \pmod 4$. It can be easily shown that all these four solutions are solutions of System (23). For $(a,b)=(\omega,\omega)$, the four solutions of System (25) are $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$ and a routine calculation shows that none of these four solutions satisfies System (23). If $ab+a=\omega$, we have $(a,b)=(1,\omega^2)$. Now for $(a,b)=(1,\omega^2)$, System (24) has four solutions $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$ if $n \equiv 2 \pmod 4$ and there are two additional solutions if $n \equiv 0 \pmod 4$. It is easy to verify that all these four solutions are solutions of System (23). For $(a,b)=(1,\omega^2)$, the four solutions of (25), when $n \equiv 2 \pmod 4$, are $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. One can easily verify that none of these four solutions are solutions of System (23). If $ab+a=\omega^2$, then $a=0$ which is not possible as $a \neq 0$. Now, if $ab+a \notin \{1,\omega,\omega^2\}$, System (25) has two solutions if $\mathrm{Tr}\left(\frac{1}{a+\omega^2}\right)=0$ and no solution, otherwise.

From the above discussion, we arrive at the following conclusion.

(I) If $ab \in \{1, a+1\}$, we can get at most 6 solutions of System (23) from Case 1 and Case 2.

(II) If $ab \in \{\omega, \omega^2, a+\omega, a+\omega^2\}$, we can get at most 6 (respectively 8) solutions of System (23) from Case 1 and Case 2, if $n \not\equiv 2 \pmod 4$ (respectively $n \equiv 0 \pmod 4$).

(III) If $ab \notin \{1, \omega, \omega^2, a+1, a+\omega, a+\omega^2\}$, we can get at most 4 solutions of System (23) from Case 1 and Case 2.

We shall now move towards the second part of the analysis.

Case 3. Let $\mathrm{Tr}\left(\frac{X^2}{X+1}+\frac{Y^2}{Y+1}\right)=0$ and $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}+\frac{Y^2+a^2}{Y+a+1}\right)=1$. In this case, System (23) reduces to

$$\begin{cases} X^{-1}+Y^{-1}=b \\ (X+a)^{-1}+(Y+a)^{-1}=b+1. \end{cases} \tag{24}$$

It is easy to see that when $b=1$, System (26) is inconsistent, as in this case, the second equation of System (26) would imply $X=Y$ and the first equation of System (26) cannot have solutions of this type as $b \neq 0$. Now, we shall calculate the number of solutions of the above System (26) in the following cases.

Subcase 3.1. Let $X=0$. In this case System (26) reduces to

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

which is equivalent to

$$\begin{cases} Y=b^{-1} \\ (b^{-1}+a)^{-1}=a^{-1}+b+1. \end{cases} \tag{25}$$

Notice that if $ab = 1$, then the above system is inconsistent. If $ab \neq 1$ then $(0, b^{-1})$ will be a solution of System (26) if and only if $a^2b^2 + a^2b + ab + a + 1 = 0$.

Subcase 3.2. Let $X = a$. In this case System (26) reduces to

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

which is equivalent to

$$\begin{cases} Y = (a^{-1} + b)^{-1} \\ ((a^{-1} + b)^{-1} + a)^{-1} = b + 1. \end{cases} \tag{26}$$

Notice that if $ab = 1$ then the equation above is inconsistent. If $ab \neq 1$ then $(a, (a^{-1} + b)^{-1})$ will be a solution of System (26) if and only if $a^2b^2 + a^2b + ab + 1 = 0$.

Subcase 3.3. Let $Y = 0$. As System (26) is symmetric in the variables X and Y, this subcase directly follow from Subcase 3.1. Therefore System (26) has no solution if $ab = 1$ and if $ab \neq 1$ then $(b^{-1}, 0)$ is a solution of System (26) if and only if $a^2b^2 + a^2b + ab + a + 1 = 0$.

Subcase 3.4. Let $Y = a$. This subcase directly follows from Subcase 3.2. Therefore System (26) has no solution if $ab = 1$ and if $ab \neq 1$ then $((a^{-1} + b)^{-1}, a)$ is a solution of System (26) if and only if $a^2b^2 + a^2b + ab + 1 = 0$.

Subcase 3.5. Let $X \notin \{0, a\}$ and $Y \notin \{0, a\}$. In this case, System (26) reduces to

$$\begin{cases} X + Y = bXY \\ X + Y = (b + 1)(X + a)(Y + a). \end{cases} \tag{27}$$

Now adding the first and the second equation of the above system, we have

$$\begin{aligned} XY + (ab + a)(X + Y + a) &= 0 \\ bXY + (ab^2 + ab)(X + Y + a) &= 0 \\ (ab^2 + ab + 1)(X + Y) + a^2b^2 + a^2b &= 0, \end{aligned}$$

when $ab^2 + ab + 1 = 0$, then the above equation will be inconsistent, as $a^2b^2 + a^2b \neq 0$ (since $b \notin \{0, 1\}$). When $ab^2+ab+1 \neq 0$, we let $X+Y = t$, where $t = \dfrac{a^2b^2 + a^2b}{ab^2 + ab + 1}$. Now putting $Y = X + t$, the first equation of System (29) transforms into

$$X^2 + tX + \frac{t}{b} = 0. \tag{28}$$

The above equation has two solutions if and only if $\mathrm{Tr}\left(\frac{1}{tb}\right) = 0$, say X_1 and $X_1 + t$. Thus, we can get at most two solutions, namely, $(X_1, X_1 + t)$ and $(X_1 + t, X_1)$ of System (29), where X_1 is a root of Equation (30).

Case 4. Let $\mathrm{Tr}\left(\dfrac{X^2}{X+1} + \dfrac{Y^2}{Y+1}\right) = 1$ and $\mathrm{Tr}\left(\dfrac{X^2 + a^2}{X + a + 1} + \dfrac{Y^2 + a^2}{Y + a + 1}\right) = 0$. In this case, System (23) reduces to

$$\begin{cases} X^{-1} + Y^{-1} = b + 1 \\ (X + a)^{-1} + (Y + a)^{-1} = b, \end{cases} \tag{29}$$

It is obvious that if (X, Y) is a solution of System (26) then $(X + a, Y + a)$ will be a solution of System (31). Also it is easy to observe that if solution (X, Y) of System (26) is a solution of System (23) then solution $(X + a, Y + a)$ of System (31) will also be a solution of System (23). Thus, in order to compute the maximum number of solutions of System (23) from Case 3 and Case 4, it is sufficient to compute the maximum number of solutions of System (23) obtained from Case 3. The maximum number of solutions of System (23) from Case 3 and Case 4 can be then obtained by just doubling this number.

In the following, we shall compute the maximum number of solutions of System (23) that can be obtained from Case 3.

(i) When $ab \in \{1, \omega, \omega^2\}$, then there is no solution of System (23) from Subcase 3.1, 3.2, 3.3 and 3.4. When $ab \in \{1, \omega, \omega^2\}$, at most two solutions of System (23) can be obtained from Subcase 3.5 if and only if $\mathrm{Tr}\left(\frac{1}{a+1}\right) = 0$, $\mathrm{Tr}\left(\frac{a+1}{a+w}\right) = 0$ and $\mathrm{Tr}\left(\frac{a+1}{a+w^2}\right) = 0$, respectively.

(ii) When $ab \in \{a + 1, a + \omega, a + \omega^2\}$, then there is no solution of System (23) from Subcase 3.1, 3.2, 3.3 and 3.4. When $ab \in \{a+1, a+\omega, a+\omega^2\}$, at most two solutions of System (23) can be obtained from Subcase 3.5 if and only if $\mathrm{Tr}\left(\frac{1}{a^2+1}\right) = 0$, $\mathrm{Tr}\left(\frac{\omega(a+1)}{a^2+\omega^2}\right) = 0$ and $\mathrm{Tr}\left(\frac{a+1}{\omega(a^2+\omega)}\right) = 0$, respectively.

(vii) When $ab \notin \{1, \omega, \omega^2, 1+a, a+\omega, a+\omega^2\}$, then it is easy to see that for any fixed $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, there can be at most two solutions of System (23) from Subcase 3.1, 3.2, 3.3 and 3.4 as $a^2b^2+a^2b+ab+a+1 = a^2b^2+a^2b+ab+1$ implies $a = 0$, a contradiction. As we have seen earlier, we can get at most two solutions of System (23) from Subcase 3.5. Thus, we can get at most 4 solutions of System (23) from Case 3.

Combining the first and the second part of the analysis, the maximum number of solutions of System (23) are listed in Table II.

This completes the proof. □

Table III gives the boomerang uniformity $\mathcal{B}_H$ of the function $H(X)$ over $\mathbb{F}_{2^n}$ with n even, for some small values of n.

Remark 14. *It would be interesting to see if the bound for the boomerang uniformity of the function $H(x)$ in Theorem* 13 *could indeed be attained.*

VII. Concluding remarks

In this paper we compute the c-Difference Distribution Table entries, as well as the Boomerang Connectivity Table entries, for an involution which has been used to construct a class of differentially 4-uniform permutations, by Beierle and Leander [2]. We consider the c-differential uniformity and boomerang uniformity of yet another function which is a differentially 4-uniform function as shown by Tan et

TABLE II: Maximum number of solutions of System (23).

Condition on (a, b)	Maximum number of solutions of System (23) from Case 1 and Case 2	Maximum number of solutions of System (23) from Case 3 and Case 4	Maximum number of solutions of System (23)
$ab = 1$	6	4	10
$ab = \omega$	6 if $n \equiv 2 \pmod 4$ and 8 if $n \equiv 0 \pmod 4$	4	10 if $n \equiv 2 \pmod 4$ and 12 if $n \equiv 0 \pmod 4$
$ab = \omega^2$	6 if $n \equiv 2 \pmod 4$ and 8 if $n \equiv 0 \pmod 4$	4	10 if $n \equiv 2 \pmod 4$ and 12 if $n \equiv 0 \pmod 4$
$ab = a + 1$	6	4	10
$ab = a + \omega$	6 if $n \equiv 2 \pmod 4$ and 8 if $n \equiv 0 \pmod 4$	4	10 if $n \equiv 2 \pmod 4$ and 12 if $n \equiv 0 \pmod 4$
$ab = a + \omega^2$	6 if $n \equiv 2 \pmod 4$ and 8 if $n \equiv 0 \pmod 4$	4	10 if $n \equiv 2 \pmod 4$ and 12 if $n \equiv 0 \pmod 4$
$ab \notin \{1, \omega, \omega^2, a+1, a+\omega, a+\omega^2\}$	4	8	12

TABLE III: Boomerang uniformity of the function $H(X)$ over finite field $\mathbb{F}_{2^n}$.

n	2	4	6	8
$\mathcal{B}_H$	4	6	8	10

al. [29] and we give bounds for its c-differential uniformity and boomerang uniformity. The c-differential uniformity concept, introduced barely a year ago, has proven to be quite interesting and attractive, mathematically, and one expects it will soon be applied in a modification of the differential attack. We hope other classes of functions will be investigated via this concept, and perhaps even via the c-boomerang uniformity notion, as introduced in [24] and further studied in [15], [25], [26].

ACKNOWLEDGEMENTS

We would like to express our sincere appreciation to the Associate Editor Prof. Sihem Mesnager for efficiently handling our paper and to the reviewers for their careful reading, beneficial comments and constructive suggestions. The research of Sartaj Ul Hasan is partially supported by MATRICS grant MTR/2019/000744 from the Science and Engineering Research Board, Government of India. Pantelimon Stănică acknowledges the sabbatical support from Naval Postgraduate School from September 2020 to July 2021.

REFERENCES

[1] D. Bartoli, M. Calderini, *On construction and (non)existence of c-(almost) perfect nonlinear functions,* Finite Fields Appl. 72 (2021), 101835.

[2] C. Beierle, G. Leander, 4*-uniform permutations with null nonlinearity*, Cryptogr. Commun. 12 (2020), 1133–1141.

[3] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptol. 4(1) (1991), 3–72.

[4] A. Biryukov, L. Perrin, A. Udovenko, *Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr*, In: Fischlin M., Coron J. S. (eds), Adv. in Crypt. – EUROCRYPT 2016, LNCS 9665, Springer, Berlin, Heidelberg, pp. 372–402, 2016.

[5] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.), Proc. Fast Software Encryption – FSE 2002, LNCS 2365, Springer, Berlin, Heidelberg, pp. 17–33, 2002.

[6] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic Sboxes,* IACR Trans. Symmetric Cryptol. 3 (2018), 290–310.

[7] M. Calderini, I. Villa, *On the boomerang uniformity of some permutation polynomials*, Cryptogr. Commun. 12 (2020), 1161–1178.

[8] C. Carlet, *Boolean Functions for Cryptography and Coding Theory,* Cambridge University Press, 2021.

[9] P. Charpin, G. M. Kyureghyan, *When does* $G(X) + \gamma \mathrm{Tr}(H(X))$ *permute* $\mathbb{F}_{p^n}$*,* Finite Fields Appl. 15 (2009), 615–63.

[10] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, *Boomerang connectivity table: a new cryptanalysis tool*, In: Nielsen J., Rijmen V. (eds.) Adv. Crypt. – EUROCRYPT 2018, LNCS 10821, Springer, Cham, pp. 683–714, 2018.

[11] J. F. Dillon, H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl. 10 (2004), 342–389.

[12] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *c-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity,* IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.

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

[14] S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.

[15] S. U. Hasan, M. Pal, P. Stănică, *The binary Gold function and its c-boomerang connectivity table*, https://arxiv.org/abs/2009.09340.

[16] S. U. Hasan, M. Pal, P. Stănică, *Boomerang uniformity of a class of power maps*, Des. Codes Cryptogr. 89 (2021), 2627–2636.

[17] J. Lahtonen, G. McGuire, H.N. Ward, *Gold and Kasami-Welch functions, quadratic forms and bent functions,* Adv. Math. Commun. 1:2 (2007), 243–250.

[18] K. Li, C. Li, T. Helleseth, L. Qu, *Cryptographically strong permutations from the butterfly structure*, Des. Codes Cryptogr. 89 (2021), 737–761.

[19] K. Li, L. Qu, B. Sun, C. Li, *New results about the boomerang uniformity of permutation polynomials,* IEEE Trans. Inf. Theory 65:11 (2019), 7542–7553.
[20] N. Li, Z. Hu, M. Xiong, X. Zeng, 4*-uniform BCT permutations from generalized butterfly structure*, https://arxiv.org/abs/2001.00464.
[21] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou, *Investigations on c-(almost) perfect nonlinear functions,* IEEE Trans. Inf. Theory 67:10 (2021), 6916–6925.
[22] S. Mesnager, C. Tang, M. Xiong, *On the boomerang uniformity of quadratic permutations*, Des. Codes Cryptogr. 88 (2020), 2233–2246.
[23] K. Nyberg, *Differentially uniform mappings for cryptography*. In: Helleseth, T. (ed.) Adv. Crypt. – EUROCRYPT 1993, LNCS 765, Springer, Berlin, Heidelberg, pp. 55–64, 1993.
[24] P. Stănică, *Investigations on c-boomerang uniformity and perfect nonlinearity*, Discrete Appl. Math. 304 (2021), 297–314.
[25] P. Stănică, *Low c-differential and c-boomerang uniformity of the swapped inverse function,* Discrete Math. 344(10) (2021), 112543.
[26] P. Stănică, *Using double Weil sums in finding the c-boomerang connectivity table for monomial functions on finite fields,* Appl. Algebra Eng. Commun. Comput. (2021), https://doi.org/10.1007/s00200-021-00520-9.
[27] P. Stănică, A. Geary, *The c-differential behavior of the inverse function under the EA-equivalence*, Cryptogr. Commun. 13 (2021), 295–306.
[28] P. Stănică, C. Riera, A. Tkachenko, *Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function*, Cryptogr. Commun. (2021), https://doi.org/10.1007/s12095-021-00485-z.
[29] Y. Tan, L. Qu, C.H. Tan, C. Li, *New families of differentially* 4*-uniform permutations over* $\mathbb{F}_{2^{2k}}$, In: T. Helleseth, J. Jedwab (Eds.) Proceedings of SEquences and Their Applications – SETA 2012, LNCS 7280, Springer, Heidelberg, vol. 7280, pp. 25–39, 2012.
[30] Z. Tu, N. Li, X. Zeng, J. Zhou, *A class of quadrinomial permutation with boomerang uniformity four*, IEEE Trans. Inf. Theory 66(6) (2020), 3753–3765.
[31] D. Wagner, *The boomerang attack*, In: L. R. Knudsen (ed.) Proc. Fast Software Encryption – FSE 1999, LNCS 1636, Springer, Heidelberg, pp. 156–170, 1999.
[32] Y. P. Wang, Q. Wang, W. G. Zhang, *Boomerang uniformity of normalized permutation polynomials of low degree*, Appl. Algebra Eng. Commun. Comput. 31 (2020), 307–322.
[33] H. Yan, *On* (-1)*-differential uniformity of ternary APN power functions*, Cryptogr. Commun. (2021). https://doi.org/10.1007/s12095-021-00526-7.
[34] Z. Zha, L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Des. Codes Cryptogr. 89 (2021), 1193–1210.

Sartaj Ul Hasan was born in Shahjahanpur, India on July 10, 1981. He received the B.Sc., M.Sc., and Ph.D. degrees in Mathematics from the Mahatma Jyotiba Phule Rohilkhand University, Aligarh Muslim University, and Indian Institute of Technology Bombay in 1999, 2001, and 2010, respectively. He is currently an Assistant Professor at the Indian Institute of Technology (IIT) Jammu. Prior to joining IIT Jammu, he was a Scientist in Defence Research and Development Organisation at Delhi from February 2007 to January 2018. From September 2011 to December 2012, he was a postdoctoral fellow at Carleton University, Ottawa, Canada. His main research interests are in finite fields and applications in cryptography and coding theory.

Mohit Pal received the B.Sc. degree in Mathematics from University of Allahabad, Allahabad, India, in 2014, and M.Sc. degree in Mathematics from Indian Institute of Technology Kharagpur, India, in 2016. He has recently completed his Ph.D. in Mathematics from Indian Institute of Technology Jammu, India. His research interests include finite fields and applications in cryptography and coding theory.

Pantelimon Stănică received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California, USA. He is an associated editor of Advances in Mathematics of Communications, Discrete Applied Mathematics and European Journal of Pure and Applied Mathematics. He was awarded the 2021 George Boole International prize for considerable contributions to the theory of Boolean functions. His research interests are in Cryptology, Coding Theory, Sequence Design, Number Theory and Discrete Mathematics.