Discrete Applied Mathematics 343 (2024) 166–179

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

# Boomerang uniformity of some classes of functions over finite fields[☆]

Kirpa Garg[a], Sartaj Ul Hasan[a,*], Pantelimon Stănică[b]

[a] Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India
[b] Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

ARTICLE INFO

*Article history:*
Received 18 January 2023
Received in revised form 12 October 2023
Accepted 15 October 2023
Available online 29 October 2023

*Keywords:*
Finite fields
Differential uniformity
Boomerang uniformity

ABSTRACT

We give bounds for the boomerang uniformity of the perturbation of some special classes of permutation functions, namely, Gold and inverse functions via trace maps. Consequently, we obtain some classes of functions with low boomerang uniformity, as often required for practical purposes.



## 1. Introduction

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 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 $\mathbb{F}_{2^n}$. Let $F$ be a function from $\mathbb{F}_{2^n}$ to itself. We can uniquely express $F$ as a polynomial in $\mathbb{F}_{2^n}[X]$ of degree at most $2^n - 1$ thanks to Lagrange's interpolation formula. A polynomial $F \in \mathbb{F}_{2^n}[X]$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if the mapping $X \mapsto F(X)$ is a permutation of $\mathbb{F}_{2^n}$. It may be noted that functions over finite fields are very important objects due to their wide range of applications in coding theory and cryptography. For example, in cryptography, these functions are often used in designing what are known as substitution boxes (S-boxes) in modern block ciphers.

One of the most effective attacks on block ciphers is differential cryptanalysis, which was first introduced by Biham and Shamir [1]. The resistance of a function against differential attack is measured in terms of its differential uniformity — a notion introduced by Nyberg [17]. For any 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 $X \in \mathbb{F}_{2^n}$. The Difference Distribution Table (DDT) entry of $F$ at a point $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, denoted by $\Delta_F(a, b)$, is the number of solutions $X \in \mathbb{F}_{2^n}$ of the equation $D_F(X, a) = b$. The differential uniformity of $F$, denoted by $\Delta_F$, is given by $\Delta_F := \max\{\Delta_F(a, b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$. When $\Delta_F = 1, 2$, $F$ is a perfect nonlinear (PN) function, respectively, an almost perfect nonlinear (APN) function. It should be noted that there are no PN functions over finite fields with even characteristic.

The boomerang attack on block ciphers was proposed by Wagner [21]. In Eurocrypt 2018, Cid et al. [9] introduced a systematic approach known as the Boomerang Connectivity Table (BCT), to analyze the boomerang style attack. Boura and Canteaut [2] further studied BCT and coined the term "boomerang uniformity", which is essentially the maximum value of nontrivial entries of the BCT, to quantify the resistance of a function against the boomerang attack. For effectively

☆ 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.

* Corresponding author.
*E-mail addresses:* kirpa.garg@gmail.com (K. Garg), sartaj.hasan@iitjammu.ac.in (S.U. Hasan), pstanica@nps.edu (P. Stănică).

https://doi.org/10.1016/j.dam.2023.10.019
0166-218X/

computing the entries in the BCT, Li et al. [15] proposed an equivalent formulation as described below. For any $a, b \in \mathbb{F}_{2^n}$, the Boomerang Connectivity Table (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 $\mathcal{B}_F := \max\{\mathcal{B}_F(a, b) \mid a, b \in \mathbb{F}_{2^n}^*\}$.

For any permutation $F$, Cid et al. [9, Lemma 1] showed that $\mathcal{B}_F(a, b) \geq \Delta_F(a, b)$ for all $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. It was later proved to be valid for non-permutation functions by Mesnager et al. [16]. According to Cid et al. [9, Lemma 4], the first row and first column are the only places where the BCT and DDT differ for APN permutations. APN permutations therefore offer the most effective defense against differential and boomerang attacks. However, when $n$ is even, the only known instance of an APN permutation over $\mathbb{F}_{2^n}$ is due to Dillon et al. [3] over $\mathbb{F}_{2^6}$. The existence of APN permutations over $\mathbb{F}_{2^n}$, $n \geq 8$ even, is open and often referred to as the Big APN Problem. Thus, over $\mathbb{F}_{2^n}$, the functions with low differential and boomerang uniformity (particularly, the functions with differential and boomerang uniformity of four) are of great interest. As a consequence of the inequality $\mathcal{B}_F(a, b) \geq \Delta_F(a, b)$ for all $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, Cid et al. [9] (see also [16, Theorem 1]) showed that for a permutation $F$, $\mathcal{B}_F \geq \Delta_F$. This does not necessarily hold true for non-permutations as shown in [12]. This is because $D_F(X, a) = b$ may have a solution corresponding to $b = 0$ when $F$ is a non-permutation whereas such a solution is not possible for permutations. Motivated by the work of Cid et al. [9], many functions with low boomerang uniformity have been studied in the last couple of years (see, for example, [5,12,13,15,16,20,22], and the references therein). Hence, the construction of functions (polynomials) with low differential and boomerang uniformities is important for designing S-boxes of many block ciphers. For instance, the inverse function over $\mathbb{F}_{2^8}$ is used to design the S-box of the Advanced Encryption Standard (AES), and it is a differentially 4-uniform and boomerang 6-uniform permutation over $\mathbb{F}_{2^8}$. In this paper, we study the boomerang uniformity of some classes of functions by finding the number of solutions to a system of equations over finite fields. In fact, we provide upper bounds for their boomerang uniformity, and it turns out that these bounds hold true even when these functions are permutations under certain conditions. We want to point out that some of the perturbations we discuss here do have low boomerang uniformity. Ultimately, questions on differential and boomerang uniformity reduce to solving some equations in finite fields, which are notoriously difficult, and very few such allow general methods, most being resolved via ad hoc techniques, depending upon the shape of the function under consideration.

We shall now give the structure of the paper. We first recall a definition and some results in Section 2. In Section 3, we give general bounds for the boomerang uniformity of the perturbed functions over $\mathbb{F}_{2^n}$, and further compute the bounds for the boomerang uniformity of the perturbed Gold function. In Section 4, bounds for the boomerang uniformity of the perturbed inverse function have been computed. An explicit class of permutation polynomials with boomerang uniformity at most 8 is given in Section 5. We conclude the paper in Section 6.

## 2. Preliminaries

We will first provide some background and provide several lemmas that will be used in the subsequent sections. As it is known (and discussed in [6], for instance), a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be represented as $\mathrm{Tr}(R(x))$ for some (not unique) mapping $R : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where Tr denotes the absolute trace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

**Definition 2.1** ([6]). A function $\mathrm{Tr}(R(X))$ is said to have a linear structure $\alpha \in \mathbb{F}_{2^n}^*$ if $\mathrm{Tr}(R(X)) + \mathrm{Tr}(R(X + \alpha)) = \mathrm{Tr}(R(X) + R(X + \alpha))$ is a constant function. We call $\alpha \in \mathbb{F}_{2^n}^*$ a $b$-linear structure if $\mathrm{Tr}(R(X) + R(X + \alpha)) = b$ for all $X \in \mathbb{F}_{2^n}$, where $b \in \mathbb{F}_2$.

We present now a few lemmas, as they will be used later in the paper.

**Lemma 2.2** ([6, Theorem 2]). *Let $G(X), H(X) \in \mathbb{F}_{2^n}[X]$, $\gamma \in \mathbb{F}_{2^n}$ and $G(X)$ be a permutation polynomial. Then $F(X) = G(X) + \gamma \mathrm{Tr}(H(X))$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if $H(X) = R(G(X))$, where $R(X) \in \mathbb{F}_{2^n}[X]$ and $\gamma$ is a 0-linear structure of the function $\mathrm{Tr}(R(x))$.*

**Lemma 2.3** ([10, Theorem 3]). *Let $k$ be a non-negative integer and $F(X) = X^{2^k} + AX + B \in \mathbb{F}_{2^n}[X]$, $A \neq 0$. Let $d = \gcd(k, n)$, $m = n/d$ and $\mathrm{Tr}_d^n$ be the relative trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^d}$. For $0 \leq i \leq m-1$, define $t_i = \sum_{j=i}^{m-2} 2^{k(j+1)}$. Put $\alpha_0 = A$ and $\beta_0 = B$. If $m > 1$, then for $1 \leq r \leq m-1$, we let $\alpha_r = A^{1+2^k+2^{2k}+\cdots+2^{kr}}$ and $\beta_r = \sum_{i=0}^{r} A^{s_i} B^{2^{ki}}$ where $s_i = \sum_{j=i}^{r-1} 2^{k(j+1)}$ for $0 \leq i \leq r-1$ and $s_r = 0$.*

*(i) If $\alpha_{m-1} = 1$ and $\beta_{m-1} \neq 0$ then the trinomial $F$ has no roots in $\mathbb{F}_{2^n}$.*

*(ii) If $\alpha_{m-1} \neq 1$ then $F$ has a unique root, namely $X = \dfrac{\beta_{m-1}}{1 + \alpha_{m-1}}$.*

*(iii) If $\alpha_{m-1} = 1$, $\beta_{m-1} = 0$, $F$ has $2^d$ roots in $\mathbb{F}_{2^n}$ given by $x + \delta\tau$, where $\delta \in \mathbb{F}_{2^d}$, $\tau$ is fixed in $\mathbb{F}_{2^n}$ with $\tau^{2^k-1} = A$ (that is, a $(2^k-1)$-root of $A$), and, for any $c \in \mathbb{F}_{2^n}^*$, satisfying $\mathrm{Tr}_d(c) \neq 0$ then $x = \frac{1}{\mathrm{Tr}_d(c)} \sum_{i=o}^{m-1} \left(\sum_{j=0}^{i} c^{2^{kj}}\right) A^{t_i} B^{2^{ki}}$.*

**Lemma 2.4** (*[7, Theorem 7]*). *Let $F_{s,t,\gamma}(X) = X^s + \gamma \mathrm{Tr}(X^t)$ with $\gamma \in \mathbb{F}_{2^n}^*$. Then $F_{s,t,\gamma}$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if $\gcd(s, 2^n-1) = 1$, $t \equiv 2^j(2^i+1)s \pmod{2^n-1}$ for some $0 \le i, j \le n-1$, $i \ne n/2$, and either of the following holds:*

*(i) $i = 0$ and $\mathrm{Tr}(\gamma) = 0$;*
*(ii) $i > 0$ and $\gamma \in \mathbb{F}_{2^k}$ with $\mathrm{Tr}(\gamma^{2^i+1}) = 0$, where $k = \gcd(2i, n)$.*

*Moreover, if $\mathrm{Tr}(\gamma) = 1$ in Case $(i)$, or $\mathrm{Tr}(\gamma^{2^i+1}) = 1$ in Case $(ii)$, then $F_{s,t,\gamma}$ is a 2-to-1 mapping.*

**Lemma 2.5** (*[7, Proposition 3]*). *Let $F(X) = G(X) + \gamma \mathrm{Tr}(H(X))$, $G(X), H(X) \in \mathbb{F}_q[X]$, where $q$ is a prime power and $\gamma \in \mathbb{F}_q^*$. Then $\Delta_F \le 2\Delta_G$.*

**Lemma 2.6** (*[8, Lemma 5]*). *Let $F(X) = X^{-1} + \gamma \mathrm{Tr}(H(x))$ where $H \in \mathbb{F}_{2^n}[X]$ and $\gamma \in \mathbb{F}_{2^n}^*$. Then*

$$\Delta_F \in \begin{cases} \{2,4\} & \text{if } n \text{ is odd;} \\ \{4,6\} & \text{if } n \text{ is even.} \end{cases}$$

**Lemma 2.7** (*[11, Lemma 11]*). *Let $n$ be a positive integer. The equation $X^2 + aX + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $a \ne 0$, has two solutions in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{b}{a^2}\right) = 0$, and no solution otherwise.*

## 3. Boomerang uniformity of the perturbed gold functions

It is not a new idea to modify a good function via a trace, and we mention here the beautiful APN function $X^3 + \mathrm{Tr}(X^9)$ of [4], which changes a Gold APN function in one component.

Here we shall discuss the boomerang uniformity of the functions of the form $F(X) = G(X) + \gamma \mathrm{Tr}(H(X))$, where $G, H \in \mathbb{F}_{2^n}[X]$ over finite field $\mathbb{F}_{2^n}$. From Lemma 2.5, we know that the differential uniformity of the function $F$ is bounded above by twice the differential uniformity of $G$. The following lemma, whose proof is rather immediate, gives a relation between the BCT entries of the function $F$ and $G$.

**Lemma 3.1.** *Let $F(X) = G(X) + \gamma \mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,*

$$\mathcal{B}_F(a,b) \le \mathcal{B}_G(a,b) + \mathcal{B}_G(a, b+\gamma) + N_1 + N_2,$$

*where*

$$N_1 = \left| \left\{ (X,Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid \begin{cases} G(X+a) + G(Y+a) = b + \gamma \\ G(X) + G(Y) = b \end{cases} \right\} \right| \tag{3.1}$$

*and*

$$N_2 = \left| \left\{ (X,Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid \begin{cases} G(X+a) + G(Y+a) = b \\ G(X) + G(Y) = b + \gamma \end{cases} \right\} \right|. \tag{3.2}$$

**Remark 3.2.** Notice that the permutations displayed in Lemmas 2.2 and 2.4 are a particular case of the function $F$ mentioned in Lemma 3.1. Therefore, also for these specific permutations, the upper bound for the boomerang uniformity remains valid.

We next discuss the particular case of Lemma 3.1 when $G(X) = L_1(X^d)$, where $L_1$ is a linear permutation and $H(X) = L_2(X)$, for a linear map $L_2$ over $\mathbb{F}_{2^n}$. This lemma will be used in the subsequent section.

**Lemma 3.3.** *Let $F(X) = L_1(X^d) + \gamma \mathrm{Tr}(L_2(X)) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$, $L_1$ is a linear permutation and $L_2$ is a linear map over $\mathbb{F}_{2^n}$. Then for any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$*

$$\mathcal{B}_F(a,b) \le \max\{2\mathcal{B}_G, \mathcal{B}_G + (d'-1)(d'-2)\},$$

*where $d' = \gcd(d, 2^n-1)$ and $G(X) = X^d$.*

**Proof.** Let $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, then we have the following system of equations:

$$\begin{cases} L_1(X^d) + L_1(Y^d) + \gamma \mathrm{Tr}(L_2(X+Y)) = b \\ L_1((X+a)^d) + L_1((Y+a)^d) + \gamma \mathrm{Tr}(L_2(X+Y)) = b. \end{cases} \tag{3.3}$$

We first consider the case when $b \ne \gamma$. Now, we deal with two subcases depending upon whether $\mathrm{Tr}(L_2(X+Y))$ is 0 or 1. When $\mathrm{Tr}(L_2(x+y))$ is 0, then we have at most $\mathcal{B}_G(a, L_1^{-1}(b))$ possible solutions, instead when $\mathrm{Tr}(L_2(x+y))$ is 1, there are at most $\mathcal{B}_G(a, L_1^{-1}(b+\gamma))$ possible solutions. Therefore, for any $a, b \in \mathbb{F}_{2^n}^*$ with $b \ne \gamma$, we infer

$\mathcal{B}_F(a,b) \le \mathcal{B}_G(a, L_1^{-1}(b)) + \mathcal{B}_G(a, L_1^{-1}(b+\gamma)) \le 2\mathcal{B}_G$. Next, we consider the case when $b=\gamma$. Then, System (3.3) would further reduce to the following system of equations,

$$\begin{cases} L_1(X^d)+L_1(Y^d)+\gamma \mathrm{Tr}(L_2(X+Y))=\gamma \\ L_1((X+a)^d)+L_1((Y+a)^d)+\gamma \mathrm{Tr}(L_2(X+Y))=\gamma. \end{cases} \tag{3.4}$$

Further if $\mathrm{Tr}(L_2(X+Y))=0$, System (3.4) has at most $B_G(a, L_1^{-1}(\gamma))$ solutions. Now, if $\mathrm{Tr}(L_2(X+Y))=1$, then the first equation of System (3.4) will give us $L_1(X^d)=L_1(Y^d)$ or equivalently, $X^d=Y^d$. If $Z=\frac{X}{Y}$, then $Z^d=1$ has $d'=\gcd(d,2^n-1)$ solutions in $\mathbb{F}_{2^n}$. One, among these $d'$ solutions is $Z=1$, or equivalently $X=Y$, which is not possible. Hence, we are left with $X=\alpha Y$, where $\alpha \in \mathbb{F}_{2^n}\setminus\{1\}$ satisfying $\alpha^{d'}=1$. Now, from the second equation of System (3.4) we have $L_1((X+a)^d)=L_1((Y+a)^d)$, i.e., $(X+a)^d=(Y+a)^d$. Using the same argument, we get $X+a=\beta(Y+a)$, where $\beta\in\mathbb{F}_{2^n}\setminus\{1\}$ satisfying $\beta^{d'}=1$. Now if $\alpha=\beta$, we have $a(1+\alpha)=0$, which is not possible. For $\alpha\ne\beta$, $Y=\dfrac{a(1+\beta)}{(\alpha+\beta)}$ and thus, $X=\dfrac{a\alpha(1+\beta)}{(\alpha+\beta)}$. We have at most $(d'-1)(d'-2)$ choices for $Y=\dfrac{a(1+\beta)}{(\alpha+\beta)}$ in $\mathbb{F}_{2^n}$. Hence, this will give us $\mathcal{B}_F(a,\gamma)\le \mathcal{B}_G(a, L_1^{-1}(\gamma))+(d'-1)(d'-2)\le \mathcal{B}_G+(d'-1)(d'-2)$, where $d'=\gcd(d,2^n-1)$. This completes the proof. □

We shall now use Lemma 3.1 to compute bounds for the boomerang uniformity of the function $F$ for some particular type of functions $G$. The following theorem gives a bound for the function $F$ when the function $G$ is a Gold function.

**Theorem 3.4.** *Let $F(X)=X^{2^k+1}+\gamma\mathrm{Tr}(H(X))\in\mathbb{F}_{2^n}[X]$, where $H\in\mathbb{F}_{2^n}[X]$, $\gamma\in\mathbb{F}_{2^n}^*$ and $\gcd(k,n)=1$. Then $\mathcal{B}_F\le 12$.*

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

$$\begin{cases} X^{2^k+1}+Y^{2^k+1}+\gamma\mathrm{Tr}(H(X)+H(Y))=b, \\ (X+a)^{2^k+1}+(Y+a)^{2^k+1}+\gamma\mathrm{Tr}(H(X+a)+H(Y+a))=b. \end{cases} \tag{3.5}$$

From Lemma 3.1, we know that $\mathcal{B}_F(a,b)\le\mathcal{B}_G(a,b)+\mathcal{B}_G(a,b+\gamma)+N_1+N_2$, where $N_1$ and $N_2$ are given in Eq. (3.1) and (3.2), respectively. It is easy to observe that for $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_{2^n}^*\setminus\{\gamma\}$, we have $\mathcal{B}_F(a,b)\le 2\mathcal{B}_G+N_1+N_2$. We now consider the number of solutions $(X,Y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of the following system:

$$\begin{cases} (X+a)^{2^k+1}+(Y+a)^{2^k+1}=b+\gamma, \\ X^{2^k+1}+Y^{2^k+1}=b, \end{cases}$$

which can be further written as

$$\begin{cases} a(X+Y)^{2^k}+a^{2^k}(X+Y)=\gamma, \\ X^{2^k+1}+Y^{2^k+1}=b. \end{cases}$$

Substituting $X+Y=Z$, we get the following

$$\begin{cases} aZ^{2^k}+a^{2^k}Z=\gamma \\ X^{2^k+1}+(X+Z)^{2^k+1}=b. \end{cases} \tag{3.6}$$

Consider the first equation of System (3.6), that is

$$Z^{2^k}+a^{2^k-1}Z+a^{-1}\gamma=0. \tag{3.7}$$

Since $a\in\mathbb{F}_{2^n}^*$, from Lemma 2.3, Eq. (3.7) can have at most 2 solutions (as $d=\gcd(k,n)=1$). Also notice that since $X^{2^k+1}$, where $\gcd(k,n)=1$, is APN over $\mathbb{F}_{2^n}$, the second equation of System (3.6) can have at most 2 solutions for some fixed $Z\in\mathbb{F}_{2^n}^*$. Thus $N_1\le 4$. Similar arguments can be applied to show that $N_2\le 4$. Hence, for $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_{2^n}^*\setminus\{\gamma\}$, we get $\mathcal{B}_F(a,b)\le 2\mathcal{B}_G+8$.

We shall now compute the BCT entry $\mathcal{B}_F(a,\gamma)$, which is given by the number of solutions $(X,Y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of the following system

$$\begin{cases} G(X+a)+G(Y+a)+\gamma\mathrm{Tr}(H(X+a)+H(Y+a))=\gamma \\ G(X)+G(Y)+\gamma\mathrm{Tr}(H(X)+H(Y))=\gamma. \end{cases} \tag{3.8}$$

We shall now split the analysis of the solutions of the above system in following four cases.

**Case 1**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=0=\mathrm{Tr}(H(X)+H(Y))$, then

$$\begin{cases} (X+a)^{2^k+1}+(Y+a)^{2^k+1}=\gamma \\ X^{2^k+1}+Y^{2^k+1}=\gamma. \end{cases}$$

As $\gamma\ne 0$, we can have at most two solutions for System (3.8) in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

**Case 2**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=1=\mathrm{Tr}(H(X)+H(Y))$, then

$$\begin{cases}(X+a)^{2^k+1}+(Y+a)^{2^k+1}=0\\ X^{2^k+1}+Y^{2^k+1}=0.\end{cases}$$

When $n$ is odd, there does not exist any solution $(X,Y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of the second equation of the above system. This is because $\gcd(k,n)=1$ and hence the second equation will give us $X=Y$, which is not possible. For even $n$, System (3.8) has at most two solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ from this case.

**Case 3**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=1$ and $\mathrm{Tr}(H(X)+H(Y))=0$, then

$$\begin{cases}(X+a)^{2^k+1}+(Y+a)^{2^k+1}=0,\\ X^{2^k+1}+Y^{2^k+1}=\gamma.\end{cases}$$

Similar arguments as in Case 2, for odd $n$, we have no solution of System (3.8) from this case and for even $n$, we have at most two solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

**Case 4**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=0$ and $\mathrm{Tr}(H(X)+H(Y))=1$, then

$$\begin{cases}(X+a)^{2^k+1}+(Y+a)^{2^k+1}=\gamma,\\ X^{2^k+1}+Y^{2^k+1}=0.\end{cases}$$

Similar to the above case, we have at most two solutions of System (3.8) from this case. This completes the proof. □

**Remark 3.5.** Charpin et al. [8] showed that for $n$ odd, $G(X)=X^3+\mathrm{Tr}(X^3+X^9)$ is bijective on $\mathbb{F}_{2^n}$ and satisfies $\Delta_G=4$. Experimentally, we found that over $\mathbb{F}_{2^7}$, $G(X)$ attains the upper bound 12 of the boomerang uniformity.

We now put a restriction on $H(X)$ and take $H(X)=X+X^{2^k+1}$. It is obvious from Lemma 2.5 that the differential uniformity of $F(X)=X^{2^k+1}+\gamma\mathrm{Tr}(X+X^{2^k+1})$ over $\mathbb{F}_{2^n}$, where $\gamma\in\mathbb{F}_{2^n}^*$ and $\gcd(n,k)=1$ is bounded above by 4. Moreover, if $\mathrm{Tr}(\gamma)=0$, $F$ is EA-equivalent to $X^{2^k+1}$, which makes it APN and hence the DDT entry at $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$ and BCT entry at $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$ of $F$ is at most 2. We shall compute the bounds for the boomerang uniformity of the function $F(X)=X^{2^k+1}+\gamma\mathrm{Tr}(X+X^{2^k+1})$ in the next theorem by first finding out the DDT entries in the following lemma.

**Lemma 3.6.** *Let $F(X)=X^{2^k+1}+\gamma\mathrm{Tr}(X+X^{2^k+1})\in\mathbb{F}_{2^n}[X]$, where $\gamma\in\mathbb{F}_{2^n}^*$, $\gcd(n,k)=1$. Then for any $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, the DDT entries of the function $F$ are given by*

$$\Delta_F(a,b)=\begin{cases}0 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right),\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right)=(1,0),\\ 2 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right),\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right)\in\{(1,1),(0,1)\},\\ 4 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right),\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right)=(0,0),\quad \text{where } b':=F(a)+b.\end{cases}$$

*Further, if $\mathrm{Tr}(\gamma)=0$, $\Delta_F(a,b)\in\{0,2\}$.*

**Proof.** For $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_{2^n}$, consider the following equation

$$\begin{aligned}b&=F(X+a)+F(X)\\ &=X^{2^k+1}+(X+a)^{2^k+1}+\gamma\mathrm{Tr}\left(X+X^{2^k+1}+X+a+(X+a)^{2^k+1}\right)\\ &=a^{2^k+1}+aX^{2^k}+Xa^{2^k}+\gamma\mathrm{Tr}\left(a+a^{2^k+1}+aX^{2^k}+Xa^{2^k}\right),\end{aligned}$$

or equivalently,

$$aX^{2^k}+Xa^{2^k}+\gamma\mathrm{Tr}\left(aX^{2^k}+Xa^{2^k}\right)=b', \tag{3.9}$$

where $b'=b+a^{2^k+1}+\gamma\mathrm{Tr}\left(a+a^{2^k+1}\right)=F(a)+b$. Now, we split the analysis of Eq. (3.9) in the following two cases.

**Case 1**. Let $\mathrm{Tr}(aX^{2^k}+Xa^{2^k})=0$. Then Eq. (3.9) reduces to

$$X^{2^k}+Xa^{2^k-1}+b'a^{-1}=0.$$

From Lemma 2.3, $m=n$, and hence $\alpha_{m-1}=1$. Here, $s_i=\frac{2^{kn}-2^{k(i+1)}}{2^k-1}$ and hence

$$\beta_{m-1}=\beta_{n-1}=\sum_{i=0}^{n-1}(a^{2^{kn}-2^{k(i+1)}})(b'a^{-1})^{2^{ki}}=a\sum_{i=0}^{n-1}\frac{(b')^{2^{ki}}}{a^{2^{ki}+2^{k(i+1)}}}=a\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right).$$

Thus, from Lemma 2.3, Eq. (3.9) has the following solutions:

$$\begin{cases} \text{no solutions} & \text{if } \mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right) = 1, \\ \{X, X+a\} & \text{if } \mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right) = 0. \end{cases}$$

**Case 2**. Let $\mathrm{Tr}(aX^{2^k} + Xa^{2^k}) = 1$. In this case Eq. (3.9) reduces to

$$X^{2^k} + Xa^{2^k-1} + (b' + \gamma)a^{-1} = 0.$$

Similar to Case 1, Eq. (3.9) has the following solutions:

$$\begin{cases} \text{no solutions} & \text{if } \mathrm{Tr}\left(\frac{b'+\gamma}{a^{2^k+1}}\right) = 1, \\ \{X, X+a\} & \text{if } \mathrm{Tr}\left(\frac{b'+\gamma}{a^{2^k+1}}\right) = 0. \end{cases}$$

From the above discussion, we infer that

$$\Delta_F(a,b) = \begin{cases} 0 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (1,0), \\ 2 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) \in \{(1,1),(0,1)\}, \\ 4 & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (0,0). \end{cases}$$

Further, if $\mathrm{Tr}(\gamma) = 0$, we have from Eq. (3.9) that $\mathrm{Tr}(b') = 0$ in Case 1 and $\mathrm{Tr}(b') = 1$ in Case 2. Hence, Case 1 and Case 2 cannot occur simultaneously when $\mathrm{Tr}(\gamma) = 0$. This completes the proof of the lemma. □

The following theorem gives the boomerang uniformity of the function $F(X) = X^{2^k+1} + \gamma\mathrm{Tr}(X + X^{2^k+1})$ over $\mathbb{F}_{2^n}$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $\gcd(k,n) = 1$. In case of odd $n$, the bound is refined further.

**Theorem 3.7.** *Let $F(X) = X^{2^k+1} + \gamma\mathrm{Tr}(X + X^{2^k+1}) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $\gcd(k,n) = 1$. Then for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, the BCT entries of the function $F$ are given by*

$$\mathcal{B}_F(a,b) = \begin{cases} 0 & \textit{if } \left(T_\gamma, T_b, T_a, T_Z\right) = (0,1,0,0), \\ 2 & \textit{if } T_\gamma = 1, \\ 4 & \textit{if } \left(T_\gamma, T_b, T_a, T_Z\right) \in \{(0,0,1,0),(0,0,1,1),(0,0,0,1)\}, \\ 8 & \textit{if } \left(T_\gamma, T_b, T_a, T_Z\right) \in \{(0,1,0,1),(0,1,1,0),(0,1,1,1)\}, \\ 12 & \textit{if } \left(T_\gamma, T_b, T_a, T_Z\right) = (0,0,0,0), \end{cases}$$

*where $\left(T_\gamma, T_b, T_a, T_Z\right) := \left(\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{b}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(a)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(Z)}{a^{2^k+1}}\right)\right)$ and $Z$ is a solution of the equation $aZ^{2^k} + a^{2^k}Z + \gamma = 0$. Also, when $\mathrm{Tr}(\gamma) = 0$, we have $\mathcal{B}_F(a,b) \in \{0,2\}$. Moreover, when $n$ is odd, $\mathcal{B}_F \le 8$.*

**Proof.** For $a, b \in \mathbb{F}_{2^n}^*$, the BCT entry $\mathcal{B}_F(a,b)$ is given by the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system

$$\begin{cases} (X+a)^{2^k+1} + (Y+a)^{2^k+1} + \gamma\mathrm{Tr}(X + (X+a)^{2^k+1} + Y + (Y+a)^{2^k+1}) = b, \\ X^{2^k+1} + Y^{2^k+1} + \gamma\mathrm{Tr}(X + X^{2^k+1} + Y + Y^{2^k+1}) = b. \end{cases}$$

After simplifying and substituting $Z = X + Y$, we get

$$\begin{cases} \gamma\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = aZ^{2^k} + a^{2^k}Z, \\ X^{2^k+1} + (X+Z)^{2^k+1} + \gamma\mathrm{Tr}(Z + X^{2^k+1} + (X+Z)^{2^k+1}) = b, \end{cases}$$

or equivalently,

$$\begin{cases} aZ^{2^k} + a^{2^k}Z + \gamma\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 0, \\ XZ^{2^k} + X^{2^k}Z + \gamma\mathrm{Tr}(XZ^{2^k} + X^{2^k}Z) = b + F(Z). \end{cases} \tag{3.10}$$

Now we shall consider the following two cases, namely, $\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 0$ and $\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 1$, respectively.

**Case 1**. Let $\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 0$. Then from the first equation of the above system, we have $aZ^{2^k} + a^{2^k}Z = 0$. As $Z \neq 0$ and $\gcd(2^k - 1, 2^n - 1) = 1$, we have $Z^{2^k-1} = a^{2^k-1}$, which implies that $Z = a$. Substituting $Z = a$ in the second equation in System (3.10), we get

$$Xa^{2^k} + X^{2^k}a + \gamma\mathrm{Tr}(Xa^{2^k} + X^{2^k}a) = b',$$

where $b' = b + F(a)$. From Lemma 3.6, we know that the above equation has

$$\begin{cases} \text{no solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (1, 0), \\ 2 \text{ solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) \in \{(1, 1), (0, 1)\}, \\ 4 \text{ solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b'}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (0, 0). \end{cases}$$

**Case 2**. Let $\mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 1$. Then from the first equation of the above system, we have $aZ^{2^k} + a^{2^k}Z = \gamma$. From Lemma 2.3, we have $m = n$, $\alpha_{n-1} = 1$ and $\beta_{n-1} = a\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)$. When $\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right) = 1$, the equation $aZ^{2^k} + a^{2^k}Z + \gamma = 0$ has no solution $Z \in \mathbb{F}_{2^n}$ and consequently, System (3.10) has no solution $(X, Z) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. When $\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right) = 0$, the equation $aZ^{2^k} + a^{2^k}Z + \gamma = 0$ has two solutions $Z, Z + a \in \mathbb{F}_{2^n}$. When $Z$ is a solution of the equation $aZ^{2^k} + a^{2^k}Z + \gamma = 0$, System (3.10) has

$$\begin{cases} \text{no solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b+F(Z)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (1, 0), \\ 4 \text{ solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b+F(Z)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (0, 0). \end{cases}$$

When $Z + a$ is a solution of the equation $aZ^{2^k} + a^{2^k}Z + \gamma = 0$ then System (3.10) has

$$\begin{cases} \text{no solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b+F(Z)+F(a)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (1, 0), \\ 4 \text{ solutions} & \text{if } \left(\mathrm{Tr}\left(\frac{b+F(Z)+F(a)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right)\right) = (0, 0). \end{cases}$$

From the above discussion, we infer the following,

$$\mathcal{B}_F(a, b) = \begin{cases} 0 & \text{if } \left(T_\gamma, T_b, T_a, T_Z\right) = (0, 1, 0, 0), \\ 2 & \text{if } T_\gamma = 1, \\ 4 & \text{if } \left(T_\gamma, T_b, T_a, T_Z\right) \in \{(0, 0, 1, 0), (0, 0, 1, 1), (0, 0, 0, 1)\}, \\ 8 & \text{if } \left(T_\gamma, T_b, T_a, T_Z\right) \in \{(0, 1, 0, 1), (0, 1, 1, 0), (0, 1, 1, 1)\}, \\ 12 & \text{if } \left(T_\gamma, T_b, T_a, T_Z\right) = (0, 0, 0, 0), \end{cases}$$

where $\left(T_\gamma, T_b, T_a, T_Z\right) = \left(\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{b}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(a)}{a^{2^k+1}}\right), \mathrm{Tr}\left(\frac{F(Z)}{a^{2^k+1}}\right)\right)$. Notice that

$$T_a = \mathrm{Tr}\left(\frac{F(a)}{a^{2^k+1}}\right) = \mathrm{Tr}(1) + \mathrm{Tr}(a + a^{2^k+1})\mathrm{Tr}\left(\frac{\gamma}{a^{2^k+1}}\right).$$

When $T_\gamma = 0$, we get that $T_a = \mathrm{Tr}(1)$. Hence, $\mathcal{B}_F(a, b) \le 8$ for odd $n$. Also, if $\mathrm{Tr}(\gamma) = 0$, Case 2 will have no solutions because $\mathrm{Tr}(\gamma) = \mathrm{Tr}(aZ^{2^k} + a^{2^k}Z) = 1$ and Case 1 can give at most 2 solutions which follow from Lemma 3.6. This completes the proof. □

## 4. Boomerang uniformity of the perturbed inverse function

In this section, we shall give bounds for the boomerang uniformity for the general case of perturbed inverse functions. In fact, we prove in the following theorem that for even $n$, the bound is sixteen and twenty when $n \equiv 2 \pmod 4$ and $n \equiv 0 \pmod 4$, respectively, and twelve for odd $n$. For inverses of elements in the finite field, we shall use the convention that for any nonzero $a \in \mathbb{F}_{2^n}$, $a^{-1} := \frac{1}{a}$ and $0^{-1} := 0$.

**Theorem 4.1.** *Let $F(X) = X^{-1} + \gamma Tr(H(X)) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}^*$. Then the boomerang uniformity $\mathcal{B}_F$ of $F$ is given by*

$$\mathcal{B}_F \le \begin{cases} 12 \textit{ if } n \textit{ is odd}, \\ 16 \textit{ if } n \equiv 2 \pmod 4, \\ 20 \textit{ if } n \equiv 0 \pmod 4). \end{cases}$$

**Proof.** We know, by Lemma 3.1, that $\mathcal{B}_F(a, b) \le \mathcal{B}_G(a, b) + \mathcal{B}_G(a, b + \gamma) + N_1 + N_2$. We first consider the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system when $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}^* \setminus \{\gamma\}$,

$$\begin{cases} (X + a)^{-1} + (Y + a)^{-1} = b + \gamma \\ X^{-1} + Y^{-1} = b. \end{cases} \tag{4.1}$$

We will split the analysis of the solutions of the above system in the following five cases.

**Case 1**. If $X = 0$, the above system reduces to

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

Notice that if $b = a^{-1}$, then the above system is inconsistent. If $b \neq a^{-1}$ then $(0, b^{-1})$ will be a solution of System (4.1) if and only if $a^2b^2 + a^2b\gamma + ab + a\gamma + 1 = 0$.

**Case 2**. If $X = a$, the above system reduces to

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

Notice that if $b = a^{-1}$, then the above system is inconsistent. If $b \neq a^{-1}$ then $(a, (b + a^{-1})^{-1})$ will be a solution of System (4.1) if and only if $a^2b^2 + a^2b\gamma + ab + 1 = 0$.

**Case 3**. Let $Y = 0$. Similar to Case 1, System (4.1) has a solution $(b^{-1}, 0)$ if and only if $a^2b^2 + a^2b\gamma + ab + a\gamma + 1 = 0$.

**Case 4**. Let $Y = a$. Similar to Case 2, System (4.1) has a solution $((b + a^{-1})^{-1}, a)$ if and only if $a^2b^2 + a^2b\gamma + ab + 1 = 0$.

**Case 5**. Let $X, Y \notin \{0, a\}$. In this case System (4.1) reduces to

$$\begin{cases} (ab^2 + ab\gamma + \gamma)(X + Y) + a^2b^2 + a^2b\gamma = 0, \\ X + Y = bXY. \end{cases}$$

Since $ab^2 + ab\gamma + \gamma \neq 0$, as $a^2b^2 + a^2b\gamma$ cannot be zero. Hence, after further solving the system, we get

$$\begin{cases} Y = X + \dfrac{a^2b^2 + a^2b\gamma}{ab^2 + ab\gamma + \gamma} \\ X^2 + \dfrac{a^2b^2 + a^2b\gamma}{ab^2 + ab\gamma + \gamma}X + \dfrac{a^2b^2 + a^2b\gamma}{b(ab^2 + ab\gamma + \gamma)} = 0. \end{cases} \tag{4.2}$$

The above system can have at most two solutions. Hence, for $b = a^{-1}$, we get at most two solutions (from Case 5) of System (4.1). And when $b \neq a^{-1}$, we get at most four solutions, as $a^2b^2 + a^2b\gamma + ab + 1 = 0$ and $a^2b^2 + a^2b\gamma + ab + a\gamma + 1 = 0$ do not hold simultaneously. Thus

$$N_1 \leq \begin{cases} 2 \text{ if } b = a^{-1}, \\ 4 \text{ if } b \neq a^{-1}. \end{cases}$$

Similarly,

$$N_2 \leq \begin{cases} 2 \text{ if } b = a^{-1}, \\ 4 \text{ if } b \neq a^{-1}. \end{cases}$$

Also, from [9] (for $n$ odd) and from [2,14] (for $n$ even), we know that for the inverse function $G(X) = X^{-1}$, the BCT entry $\mathcal{B}_G(a, b)$ at point $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ is given by

$$\mathcal{B}_G(a, b) \leq \begin{cases} 2 \text{ if } n \text{ is odd,} \\ 4 \text{ if } n \equiv 2 \pmod 4, \\ 6 \text{ if } n \equiv 0 \pmod 4). \end{cases}$$

Summarizing the above discussion for $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}^* \setminus \{\gamma\}$, we have

$$\mathcal{B}_F(a, b) \leq \begin{cases} 12 \text{ if } n \text{ is odd,} \\ 16 \text{ if } n \equiv 2 \pmod 4, \\ 20 \text{ if } n \equiv 0 \pmod 4). \end{cases} \tag{4.3}$$

Now, we shall directly compute $\mathcal{B}_F(a, \gamma)$ without making use of Lemma 3.1, by considering the number of solutions of the following system

$$\begin{cases} (X+a)^{-1} + (Y+a)^{-1} + \gamma \mathrm{Tr}(H(X+a) + H(Y+a)) = \gamma \\ X^{-1} + Y^{-1} + \gamma \mathrm{Tr}(H(X) + H(Y)) = \gamma, \end{cases} \tag{4.4}$$

and splitting this analysis in the following four cases.

**Case 1**. Let $\mathrm{Tr}(H(X + a) + H(Y + a)) = 0 = \mathrm{Tr}(H(X) + H(Y))$. In this case, System (4.4) reduces to

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

**Table 1**
Boomerang uniformity of some perturbed inverse functions over $\mathbb{F}_{2^n}$.

| $F(X)$ | $n$ | $\Delta_F$ | $\mathcal{B}_F$ | Ref |
|---|---|---|---|---|
| $X^{-1}+\mathrm{Tr}(X^{2^{n-1}-2})$ | 5 | 4 | 6 | [8, Proposition 5] |
| $X^{-1}+\mathrm{Tr}(X^{-1}+X^{-3})$ | 7 | 4 | 8 | [8, Remark 8] |
| $X^{-1}+(g^3+g^2+g+1)\mathrm{Tr}(X^5)$ | 4 | 4 | 6 | [8, Theorem 8] |
| $X^{-1}+\mathrm{Tr}(X^5)$ | 8 | 4 | 12 | [8, Theorem 8] |
| $X^{-1}+(g^3+g^2+g)\mathrm{Tr}(X^3)$ | 6 | 4 | 8 | [8, Theorem 8] |

The number of solutions of the above system is

$$\begin{cases}\le 2 \text{ if } n \text{ is odd},\\ \le 4 \text{ if } n\equiv 2 \pmod 4,\\ \le 6 \text{ if } n\equiv 0 \pmod 4.\end{cases} \tag{4.5}$$

**Case 2**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=1=\mathrm{Tr}(H(X)+H(Y))$. Then the system further reduces to

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}=0\\ X^{-1}+Y^{-1}=0.\end{cases}$$

For $X,Y\notin\{0,a\}$, the above system is inconsistent. Also, when $X=0$, we get $Y^{-1}=0$, i.e., $Y=0$, but $(X,X)$ cannot be a solution of System (4.4), hence the system is inconsistent. Similarly, when $X=a$, we get $Y=a$, hence the system is inconsistent. As the above system is symmetric with respect to $X$ and $Y$, we get no solutions in this case.

**Case 3**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=1$, $\mathrm{Tr}(H(X)+H(Y))=0$. Similar to Case 2, we do not get any solution of System (4.4) from this case.

**Case 4**. Let $\mathrm{Tr}(H(X+a)+H(Y+a))=0$, $\mathrm{Tr}(H(X)+H(Y))=1$. Similar to Case 2, we do not get any solution of System (4.4) from this case, too.

As $\mathcal{B}_F=\max_{a,b\in\mathbb{F}_{2^n}^*,b\neq\gamma}\{\mathcal{B}_F(a,b),\mathcal{B}_F(a,\gamma)\}$, using System (4.3) and System (4.5), we have our claim. □

The examples given in Table 1 ($g$ denotes a primitive element of $\mathbb{F}_{2^n}^*$) illustrate Theorem 4.1. It is worth noting that the values obtained are strictly smaller than the bounds in Theorem 4.1. It would be interesting to investigate whether these bounds can be reached or not.

Hasan et al. [14] considered the function $F(X)=X^{-1}+\gamma\mathrm{Tr}(H(X))$ where $\gamma=1$ and $H(X)=\frac{X^2}{X+1}$ and they showed that this function has boomerang uniformity at most twelve over $\mathbb{F}_{2^n}$, where $n$ is even. However, in the following theorem, we compute the bounds for the boomerang uniformity for the function $X^{-1}+\gamma\mathrm{Tr}\,(H(X))$ over $\mathbb{F}_{2^n}$, where $H(X)=\frac{X^2+1}{X}$. In fact, we find some conditions on $\gamma$ so as to obtain slightly better bounds for its boomerang uniformity.

**Theorem 4.2.** *Let $F(X)=X^{-1}+\gamma Tr\left(\frac{X^2+1}{X}\right)\in\mathbb{F}_{2^n}[X]$, where $n$ is even, $\gamma\in\mathbb{F}_{2^n}^*$ such that $\mathrm{Tr}(\gamma)=0$. Then the boomerang uniformity of $F$ is given by*

$$\mathcal{B}_F\le\begin{cases}8 & \text{if } n\equiv 2 \bmod 4\\ 12 & \text{if } n\equiv 0 \bmod 4.\end{cases}$$

*Further, if $\mathrm{Tr}(\gamma^{-1})=0$, then $\mathcal{B}_F\le 6$.*

**Proof.** We may write $F(X)=L_1(X^{-1})+\gamma\mathrm{Tr}(L_2(X))$, where $L_2(X)=X$ is a linear map and $L_1(X)=X+\gamma\mathrm{Tr}(X)$ is a linearized permutation polynomial over $\mathbb{F}_{2^n}$ since $\mathrm{Tr}(\gamma)=0$ (see Lemma 2.2). Hence, using Lemma 3.3, we can compute the bounds for the boomerang uniformity of the function $F$. Now in view of Lemma 3.3, we have $d=2^n-2$ and thus $d'=1$. This gives us $\mathcal{B}_F(a,b)\le 2\mathcal{B}_G$ where $G(X)=X^{-1}$, which in turn implies that

$$\mathcal{B}_F(a,b)\le\begin{cases}8 \text{ if } n\equiv 2 \pmod 4,\\ 12 \text{ if } n\equiv 0 \pmod 4).\end{cases}$$

It should be noted that the above bounds for the boomerang uniformity are valid regardless of whether $\mathrm{Tr}(\gamma^{-1})$ is zero or not. However, the bound for the boomerang uniformity can further be reduced under the condition $\mathrm{Tr}(\gamma^{-1})=0$, and we present a detailed proof as follows. For $a,b\in\mathbb{F}_{2^n}^*$, consider the following system of equations

$$\begin{cases}F(X+a)+F(Y+a)=b\\ F(X)+F(Y)=b,\end{cases} \tag{4.6}$$

which further reduces to

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

or,

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}+\gamma\mathrm{Tr}(X^{-1}+(X+a)^{-1}+Y^{-1}+(Y+a)^{-1})=0\\ X^{-1}+Y^{-1}+\gamma\mathrm{Tr}(X+X^{-1}+Y+Y^{-1})=b.\end{cases}$$

From the first equation of the above system, we get that, either $(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=0$ or $(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=\gamma$, but as $\mathrm{Tr}(\gamma)=0$, the only possibility would be $(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=0$. Hence, the above system has solution in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ only if the following system

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=0\\ X^{-1}+Y^{-1}+\gamma\mathrm{Tr}(X+X^{-1}+Y+Y^{-1})=b\end{cases}\tag{4.7}$$

has solution in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. In order to analyze the solutions of this system, we shall consider the following five cases.

**Case 1**. Let $X=0$. Then, System (4.7) reduces to

$$\begin{cases}(Y+a)^{-1}+Y^{-1}=a^{-1}\\ Y^{-1}+\gamma\mathrm{Tr}(Y+Y^{-1})=b.\end{cases}\tag{4.8}$$

Now, $Y=0$ is not the solution of the above system. If $Y=a$, then System (4.8) has the solution $(0,a)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ if $b=a^{-1}+\gamma\mathrm{Tr}(a+a^{-1})$. For $Y\notin\{0,a\}$ we have

$$\frac{1}{Y+a}+\frac{1}{Y}=\frac{1}{a}$$

or,

$$Y^2+aY+a^2=0$$

and this quadratic equation has two solutions in $\mathbb{F}_{2^n}$ as $\mathrm{Tr}(1)=0$, say, $Y_1$ and $Y_2$. Hence, $(0,Y_1)$ and $(0,Y_2)$ are solutions of System (4.8) for $b=Y_1^{-1}+\gamma\mathrm{Tr}(Y_1+Y_1^{-1})$ and $b=Y_2^{-1}+\gamma\mathrm{Tr}(Y_2+Y_2^{-1})$, respectively.

**Case 2**. Let $X=a$. Then, System (4.7) reduces to

$$\begin{cases}(Y+a)^{-1}+Y^{-1}=a^{-1}\\ a^{-1}+Y^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y+Y^{-1})=b.\end{cases}\tag{4.9}$$

Now, $Y=a$, is not the solution of the above system. If $Y=0$ then System (4.9) has solution $(a,0)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ if $b=a^{-1}+\gamma\mathrm{Tr}(a+a^{-1})$. For $Y\notin\{0,a\}$ we know that the quadratic equation

$$Y^2+aY+a^2=0$$

has two solutions $Y_1$ and $Y_2$ in $\mathbb{F}_{2^n}$. Hence, $(a,Y_1)$ and $(a,Y_2)$ are solutions of System (4.7) for $b=a^{-1}+Y_1^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_1+Y_1^{-1})$ and $b=a^{-1}+Y_2^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_2+Y_2^{-1})$, respectively.

**Case 3**. Let $Y=0$. Since System (4.7) is symmetric in $X$ and $Y$, this case follows from Case 1. Hence, $(a,0)$ is a solution of the above system in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ if $b=a^{-1}+\gamma\mathrm{Tr}(a+a^{-1})$. Also, $(Y_1,0)$ and $(Y_2,0)$ are solutions for $b=Y_1^{-1}+\gamma\mathrm{Tr}(Y_1+Y_1^{-1})$ and $b=Y_2^{-1}+\gamma\mathrm{Tr}(Y_2+Y_2^{-1})$ respectively.

**Case 4**. Let $Y=a$. Since, System (4.7) is symmetric in $X$ and $Y$, this case follows from Case 2. Hence, $(0,a)$ is a solution of the above System in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ if $b=a^{-1}+\gamma\mathrm{Tr}(a+a^{-1})$. Also, $(Y_1,a)$ and $(Y_2,a)$ are solutions for $b=a^{-1}+Y_1^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_1+Y_1^{-1})$ and $b=a^{-1}+Y_2^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_2+Y_2^{-1})$ respectively.

Notice that,

$$a^{-1}+Y_1^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_1+Y_1^{-1})=Y_2^{-1}+\gamma\mathrm{Tr}(Y_2+Y_2^{-1})$$

and similarly,

$$a^{-1}+Y_2^{-1}+\gamma\mathrm{Tr}(a+a^{-1}+Y_2+Y_2^{-1})=Y_1^{-1}+\gamma\mathrm{Tr}(Y_1+Y_1^{-1}).$$

Hence, by summarizing Case 1, Case 2, Case 3 and Case 4, we get the solutions for System (4.7) as follows:

$$\begin{cases}\{(0,a),(a,0)\} & \text{if } b=a^{-1}+\gamma\mathrm{Tr}(a+a^{-1})\\ \{(0,Y_1),(Y_1,0),(Y_2,a),(a,Y_2)\} & \text{if } b=Y_1^{-1}+\gamma\mathrm{Tr}(Y_1+Y_1^{-1})\\ \{(0,Y_2),(Y_2,0),(Y_1,a),(a,Y_1)\} & \text{if } b=Y_2^{-1}+\gamma\mathrm{Tr}(Y_2+Y_2^{-1})\\ \text{no solution} & \text{otherwise,}\end{cases}$$

where $Y_1$ and $Y_2$ are solutions of $Y^2+aY+a^2=0$ in $\mathbb{F}_{2^n}$.

**Case 5**. Let $X \notin \{0, a\}$ and $Y \notin \{0, a\}$, then System (4.7) reduces to

$$\begin{cases} \dfrac{1}{X} + \dfrac{1}{X+a} = \dfrac{1}{Y} + \dfrac{1}{Y+a} \\ \dfrac{1}{X} + \dfrac{1}{Y} + \gamma \mathrm{Tr}\left(X + Y + \dfrac{1}{X} + \dfrac{1}{Y}\right) = b \end{cases} \tag{4.10}$$

or,

$$\begin{cases} (X+Y)(X+Y+a) = 0 \\ \dfrac{1}{X} + \dfrac{1}{Y} + \gamma \mathrm{Tr}\left(X + Y + \dfrac{1}{X} + \dfrac{1}{Y}\right) = b. \end{cases}$$

Now $X + Y \neq 0$, and hence, for $X + Y = a$, we get that System (4.10) has solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if

$$\frac{1}{X} + \frac{1}{X+a} + \gamma \mathrm{Tr}\left(\frac{1}{X} + \frac{1}{X+a}\right) = b + \gamma \mathrm{Tr}(a) \tag{4.11}$$

has solution in $\mathbb{F}_{2^n}$. Let $Z = \dfrac{1}{X} + \dfrac{1}{X+a}$, then $Z + \gamma \mathrm{Tr}(Z)$ is a permutation and hence for $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, $Z + \gamma \mathrm{Tr}(Z) = b + \gamma \mathrm{Tr}(a)$ has a unique solution $Z = u \in \mathbb{F}_{2^n}$. This is equivalent to $\dfrac{1}{X} + \dfrac{1}{X+a} = u$, which has at most two solutions $X \in \mathbb{F}_{2^n}$.

Also, notice that if

$$Y_1^{-1} + \gamma \mathrm{Tr}(Y_1 + Y_1^{-1}) = Y_2^{-1} + \gamma \mathrm{Tr}(Y_2 + Y_2^{-1}),$$

then

$$\frac{1}{Y_1} + \frac{1}{Y_2} + \gamma \mathrm{Tr}(Y_1 + Y_2 + \frac{1}{Y_1} + \frac{1}{Y_2}) = 0$$

that is,

$$\frac{1}{a} + \gamma \mathrm{Tr}\left(a + \frac{1}{a}\right) = 0,$$

which has no solution in $\mathbb{F}_{2^n}^*$ if $\mathrm{Tr}(\gamma^{-1}) = 0$. Also, if

$$a^{-1} + \gamma \mathrm{Tr}(a + a^{-1}) = Y_1^{-1} + \gamma \mathrm{Tr}(Y_1 + Y_1^{-1}),$$

then

$$\frac{1}{Y_1} + \frac{1}{a} + \gamma \mathrm{Tr}\left(Y_1 + a + \frac{1}{Y_1} + \frac{1}{a}\right) = 0.$$

As $Y_1 \neq a$, we are left with the case of $\mathrm{Tr}\left(Y_1 + a + \frac{1}{Y_1} + \frac{1}{a}\right) = 1$. Hence, we get

$$\begin{cases} \mathrm{Tr}\left(Y_1 + a + \dfrac{1}{Y_1} + \dfrac{1}{a}\right) = \mathrm{Tr}\left(Y_2 + \dfrac{1}{Y_2}\right) = 1 \\ \dfrac{1}{Y_1} + \dfrac{1}{a} = \dfrac{1}{Y_2} = \gamma. \end{cases}$$

The above system is inconsistent over $\mathbb{F}_{2^n}$ when $\mathrm{Tr}(\gamma^{-1}) = 0$ and therefore we get no common solution. Hence, System (4.7) can have at most six solutions when $\mathrm{Tr}(\gamma^{-1}) = 0$. $\square$

**Example 4.3.** Let $\mathbb{F}_{2^6}$ be the finite field, where $\mathbb{F}_{2^6}^* = \langle g \rangle$. In the aforementioned Theorem 4.2, let $F(X) = X^{-1} + \gamma \mathrm{Tr}(X + X^{-1})$ where $\gamma = g^{32}$ with $\mathrm{Tr}(\gamma) = 0$. According to Theorem 4.2 (or alternatively, Lemma 3.3), it follows that $\mathcal{B}_F \leq 8$. However, computational results using SageMath indicate that $\mathcal{B}_F$ is indeed equal to 8 in this case. This example serves to demonstrate that the bound stated in Lemma 3.3 and Theorem 4.2 can indeed be attained.

## 5. A class of permutations with low boomerang uniformity

It is known from the work of Boura and Canteaut [2] the boomerang uniformity of the inverse function is 6, if $n \equiv 0 \pmod 4$ and 4, if $n \equiv 2 \pmod 4$. In [15], the boomerang uniformity of the 0/1-swapped inverse function was shown to be 10, 8, 6, for $n \equiv 0 \pmod 6$, $n \equiv 3 \pmod 6$, respectively, $n \not\equiv 0 \pmod 3$.

Below, we consider yet another modification of the inverse function. It is clear from Lemma 2.2 that $F(X) = X^{-1} + \mathrm{Tr}(X^{-3} + X^{-5} + vX^{-1})$ is a permutation polynomial over $\mathbb{F}_{2^n}$ for odd $n$ and $v \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(v) = 0$. Moreover, it follows from Lemma 2.5 that the differential uniformity of this function is at most 4. We discuss the boomerang uniformity of $F$ in the following theorem.

**Theorem 5.1.** *Let $F(X)=X^{-1}+\mathrm{Tr}(X^{-3}+X^{-5}+vX^{-1})$ over $\mathbb{F}_{2^n}$, where $n$ is odd and $\mathrm{Tr}(v)=0$, for $v\in\mathbb{F}_{2^n}$. Then $\mathcal{B}_F\le 8$.*

**Proof.** For $a,b\in\mathbb{F}_{2^n}^*$, we consider the following system of equations

$$\begin{cases}F(X+a)+F(Y+a)=b\\ F(X)+F(Y)=b,\end{cases}\tag{5.1}$$

which further reduces to

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+\mathrm{Tr}(X+a)^{-3}+(Y+a)^{-3}+(X+a)^{-5}+(Y+a)^{-5}+v((X+a)^{-1}+(Y+a)^{-1})=b\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b,\end{cases}$$

or,

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+(X+a)^{-3}+Y^{-3}\\ \qquad +(Y+a)^{-3}+X^{-5}+(X+a)^{-5}+(Y+a)^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}+(X+a)^{-1}+(Y+a)^{-1}))=0\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b.\end{cases}$$

From the first equation of the above system, we consider the following two cases:

**Case 1**. Assume that $\mathrm{Tr}(X^{-3}+(X+a)^{-3}+Y^{-3}+(Y+a)^{-3}+X^{-5}+(X+a)^{-5}+Y^{-5}+(Y+a)^{-5}+v(X^{-1}+Y^{-1}+(X+a)^{-1}+(Y+a)^{-1}))=0$. Then the above system further reduces to

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=0\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b.\end{cases}\tag{5.2}$$

We split this case further into the following five subcases.

**Subcase 1.1**. If $X=0$, System (5.2) reduces to

$$\begin{cases}Y^{-1}+(Y+a)^{-1}=a^{-1}\\ Y^{-1}+\mathrm{Tr}(Y^{-3}+Y^{-5}+vY^{-1})=b.\end{cases}$$

Notice that the above system has only one solution $(0,a)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, when $b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1})$, otherwise the system is inconsistent.

**Subcase 1.2**. If $X=a$, System (5.2) reduces to

$$\begin{cases}Y^{-1}+(Y+a)^{-1}=a^{-1}\\ a^{-1}+Y^{-1}+\mathrm{Tr}(a^{-3}+Y^{-3}+a^{-5}+Y^{-5}+v(a^{-1}+Y^{-1}))=b.\end{cases}$$

Notice that the above system has only one solution $(a,0)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, when $b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1})$, otherwise the system is inconsistent.

**Subcase 1.3**. Let $Y=0$. As System (5.2) is symmetric in $X$ and $Y$, then $(a,0)$ is the only possible solution of the system, when $b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1})$.

**Subcase 1.4**. Let $Y=a$. Similarly as in the above case, $(0,a)$ is the only possible solution of System (5.2), when $b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1})$.

**Subcase 1.5**. Let $X,Y\notin\{0,a\}$. Then System (5.2) reduces to

$$\begin{cases}(X+Y)^2+a(X+Y)=0\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b,\end{cases}$$

From the first equation of the above system, we get $Y=X+a$. Substituting in the second equation, we get

$$\left\{X^{-1}+(X+a)^{-1}+\mathrm{Tr}(X^{-3}+(X+a)^{-3}+X^{-5}+(X+a)^{-5}+v(X^{-1}+(X+a)^{-1}))=b\right.$$

which has at most four solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

Also, when $b=a^{-1}+\mathrm{Tr}_1^n(a^{-3}+a^{-5}+va^{-1})$, Subcase 1.5 yields two solutions, say $(X_1,X_2),(X_2,X_1)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(\frac{1}{a+1})=0$, where $X_1$ and $X_2$ are solutions of the equation $X^2+aX+\left(\frac{a^2}{a+1}\right)=0$. Hence, by summarizing all the subcases of Case 1, we get the following solutions of System (5.2):

$$\begin{cases}\{(0,a),(a,0)\} & \text{if } b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1}),\\ & \text{and } \mathrm{Tr}\left(\frac{1}{a+1}\right)\neq 0\\ \{(0,a),(a,0),(X_1,X_2),(X_2,X_1)\} & \text{if } b=a^{-1}+\mathrm{Tr}(a^{-3}+a^{-5}+va^{-1}),\\ & \text{and } \mathrm{Tr}\left(\frac{1}{a+1}\right)=0\\ \text{at most four solutions} & \text{otherwise.}\end{cases}$$

**Case 2**. Assume that $\mathrm{Tr}(X^{-3}+(X+a)^{-3}+Y^{-3}+(Y+a)^{-3}+X^{-5}+(X+a)^{-5}+(Y+a)^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}+(X+a)^{-1}+(Y+a)^{-1}))=1$.

Then the above system reduces to

$$\begin{cases}(X+a)^{-1}+(Y+a)^{-1}+X^{-1}+Y^{-1}=1\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b.\end{cases} \tag{5.3}$$

We consider the following five subcases.

**Subcase 2.1**. If $X=0$, System (5.3) reduces to

$$\begin{cases}Y^{-1}+(Y+a)^{-1}=a^{-1}+1\\ Y^{-1}+\mathrm{Tr}(Y^{-3}+Y^{-5}+vY^{-1})=b.\end{cases}$$

The above system has at most two solutions $(0,Y_1)$ and $(0,Y_2)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ for $b=Y_1^{-1}+\mathrm{Tr}(Y_1^{-3}+Y_1^{-5}+vY_1^{-1})$ or $b=Y_2^{-1}+\mathrm{Tr}(Y_2^{-3}+Y_2^{-5}+vY_2^{-1})$, respectively if and only if $\mathrm{Tr}\left(\frac{1}{a+1}\right)=0$. Here $Y_1$ and $Y_2$ are solutions of $Y^2+aY+\frac{a^2}{a+1}=0$.

We argue that the above subcase is not possible. To this end, suppose $(0,Y_1)$ satisfies System (5.3), then we have

$$\mathrm{Tr}(a^{-3}+Y_1^{-3}+(Y_1+a)^{-3}+a^{-5}+Y_1^{-5}+(Y_1+a)^{-5}+v(a^{-1}+Y_1^{-1}+(Y_1+a)^{-1}))=1,$$

or equivalently,

$$\mathrm{Tr}\left(\frac{1}{a^3}+\frac{1}{a^5}+\frac{1}{Y_1^3}+\frac{1}{Y_1^5}+\frac{1}{(Y_1+a)^3}+\frac{1}{(Y_1+a)^5}+v\left(\frac{1}{a}+\frac{1}{Y_1}+\frac{1}{Y_1+a}\right)\right)=1.$$

As $Y_1$ satisfies $Y_1^2+aY_1+\frac{a^2}{a+1}=0$, we get that $\frac{1}{Y_1}+\frac{1}{Y_1+a}=1+\frac{1}{a}$. Clearly,

$$\frac{1}{Y_1^3}+\frac{1}{(Y_1+a)^3}=\left(\frac{1}{Y_1}+\frac{1}{Y_1+a}\right)^3+\frac{1}{Y_1(Y_1+a)}\left(\frac{1}{Y_1}+\frac{1}{Y_1+a}\right)$$

and,

$$\frac{1}{Y_1^5}+\frac{1}{(Y_1+a)^5}=\left(\frac{1}{Y_1}+\frac{1}{Y_1+a}\right)^5+\frac{1}{Y_1(Y_1+a)}\left(\frac{1}{Y_1^3}+\frac{1}{(Y_1+a)^3}\right).$$

Using the above relations, we obtain

$$\mathrm{Tr}(a^{-3}+Y_1^{-3}+(Y_1+a)^{-3}+a^{-5}+Y_1^{-5}+(Y_1+a)^{-5}+v(a^{-1}+Y_1^{-1}+(Y_1+a)^{-1}))=0,$$

which is a contradiction to our assumption. Hence, $(0,Y_1)$ is not a solution of System (5.3) in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. Similarly, $(0,Y_2)$ is not a solution of System (5.3) in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

**Subcase 2.2**. Let $X=a$. Similar to the above subcase, $(a,Y_1)$ and $(a,Y_2)$ cannot be the solutions of System (5.3).

**Subcase 2.3**. Let $Y=0$. As System (5.3) is symmetric in $X$ and $Y$, hence it is inconsistent in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

**Subcase 2.4**. Let $Y=a$. Similar to the above subcase, System (5.3) has no solution in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

**Subcase 2.5.** Let $X,Y\notin\{0,a\}$, then System (5.3) reduces to

$$\begin{cases}(XY)^2+aXY(X+Y)+a^2(XY)+a(X+Y)^2+a^2(X+Y)=0\\ X^{-1}+Y^{-1}+\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=b.\end{cases}$$

We further analyze this subcase by dividing it into the following two cases.

**Subcase 2.5.1**. Let $\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=0$. After substituting $Z=XY$, the above system further reduces to

$$\begin{cases}(1+ab+ab^2)Z^2+(a^2+a^2b)Z=0\\ X+X^{-1}Z=bZ,\end{cases}$$

which has at most two solutions, $\left(X_1,\frac{a^2(b+1)}{ab^2+ab+1}\right)$ and $\left(X_2,\frac{a^2(b+1)}{ab^2+ab+1}\right)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. Here $X_1$ and $X_2$ are solutions of $X^2+\left(\frac{a^2b(b+1)}{ab^2+ab+1}\right)X+\frac{a^2(b+1)}{ab^2+ab+1}=0$.

**Subcase 2.5.2**. Let $\mathrm{Tr}(X^{-3}+Y^{-3}+X^{-5}+Y^{-5}+v(X^{-1}+Y^{-1}))=1$.

This subcase also has at most two solutions $\left(X_3,\frac{a^2b}{ab^2+ab+1}\right)$ and $\left(X_4,\frac{a^2b}{ab^2+ab+1}\right)$ in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, where $X_3$ and $X_4$ are solutions of $X^2+\left(\frac{a^2b(b+1)}{ab^2+ab+1}\right)X+\frac{a^2b}{ab^2+ab+1}=0$.

Summarizing all the subcases of Case 2, System (5.3) has at most four solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, and hence our claim is shown. □

In Table 2, we provide some computational examples using SageMath that illustrate Theorem 5.1.

**Table 2**
Examples to illustrate Theorem 5.1.

| $n$ | $v$ | $\mathcal{B}_F$ |
|---|---|---|
| 3 | $g^2+g$ | 2 |
| 5 | $g^4+g^3+g^2+1$ | 6 |
| 7 | $g^6$ | 8 |
| 9 | $g$ | 8 |

## 6. Conclusion

We have computed the bounds for the boomerang uniformity of a general class of perturbed functions. Subsequently, we considered special cases of perturbed Gold and inverse functions. We also considered some classes of functions for some specific functions $H(X)$. For instance, we have considered a class of permutations with boomerang uniformity of at most 8. It would be interesting to further investigate the boomerang uniformity (or, even the more difficult concept of $c$-boomerang uniformity [13,18,19]) of the function $F(X) = G(X) + \gamma\mathrm{Tr}(H(X)) \in \mathbb{F}_{2^n}[X]$ by taking different functions $G, H$ and constants $\gamma$.

## Data availability

No data was used for the research described in the article.

## Acknowledgments

We would like to express our sincere appreciation to the editors for handling our paper and to the reviewers for their careful reading, beneficial comments and constructive suggestions. The authors want to thank Mohit Pal for his careful reading of the initial draft and for several useful discussions.

## References

[1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptol. 4 (1) (1991) 3–72.
[2] C. Boura, A. Canteaut, On the boomerang uniformity of cryptographic S-boxes, IACR Trans. Symmetric Cryptol. 3 (2018) 290–310.
[3] K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe, An APN permutation in dimension six, in: G. McGuire, et al. (Eds.), Proceedings of the 9th International Conference on Finite Fields and Applications, Vol. 518, Contemporary Mathematics, 2010, pp. 33–42.
[4] L. Budaghyan, C. Carlet, Constructing new APN functions from known ones, Finite Fields Appl. 15 (2) (2009) 150–159.
[5] M. Calderini, I. Villa, On the boomerang uniformity of some permutation polynomials, Cryptogr. Commun. 12 (6) (2020) 1161–1178.
[6] P. Charpin, G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, in: S.W. Golomb, M.G. Parker, A. Pott, A. Winterhof (Eds.), Proceedings of Sequences and their Applications - SETA 2008, in: Lecture Notes Comput. Sci., Vol. 5203, Springer, Berlin, Heidelberg, 2008, pp. 368–376.
[7] P. Charpin, G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, in: Finite Fields: Theory and Applications, Contemp. Math. 518, 3, (16) Amer. Math. Soc., 2010, pp. 99–111.
[8] P. Charpin, G. Kyureghyan, V. Suder, Sparse permutations with low differential uniformity, Finite Fields Appl. 28 (2014) 214–243.
[9] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, Boomerang connectivity table: a new cryptanalysis tool, in: J. Nielsen, V. Rijmen (Eds.), Advances in Cryptology-EUROCRYPT'18, in: Lecture Notes Comput. Sci., Vol. 10821, Springer, Cham, 2018, pp. 683–714.
[10] R.S. Coulter, M. Henderson, A note on the roots of trinomials over a finite field, Bull. Aust. Math. Soc. 69 (2004) 429–432.
[11] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, $c$-Differentials, multiplicative uniformity, and (almost) perfect $c$-nonlinearity, IEEE Trans. Inform. Theory 66 (6) (2020) 5781–5789.
[12] S.U. Hasan, M. Pal, P. Stănică, Boomerang uniformity of a class of power maps, Des. Codes Cryptogr. 89 (11) (2021) 2627–2636.
[13] S.U. Hasan, M. Pal, P. Stănică, The binary gold function and its $c$-boomerang connectivity table, Cryptogr. Commun. 14 (2022) 1257–1280.
[14] S.U. Hasan, M. Pal, P. Stănică, The $c$-diferential uniformity and boomerang uniformity of two classes of permutation polynomials, IEEE Trans. Inform. Theory 68 (1) (2022) 679–691.
[15] K. Li, L. Qu, B. Sun, C. Li, New results about the boomerang uniformity of permutation polynomials, IEEE Trans. Inform. Theory 65 (11) (2019) 7542–7553.
[16] S. Mesnager, C. Tang, M. Xiong, On the boomerang uniformity of quadratic permutations, Des. Codes Cryptogr. 88 (10) (2020) 2233–2246.
[17] K. Nyberg, Differentially uniform mappings for cryptography, in: T. Helleseth (Ed.), Advances in Cryptology-EUROCRYPT'93, Vol. 765, Springer, Heidelberg, 1994, pp. 55–64.
[18] P. Stănică, Investigations on $c$-boomerang uniformity and perfect nonlinearity, Discrete Appl. Math. 304 (2021) 297–314.
[19] P. Stănică, Using double weil sums in finding the $c$-boomerang connectivity table for monomial functions on finite fields, Appl. Algebra Eng. Commun. Comput. 34 (2023) 581–602.
[20] Z. Tu, N. Li, X. Zeng, J. Zhou, A class of quadrinomial permutations with boomerang uniformity four, IEEE Trans. Inform. Theory 66 (6) (2020) 3753–3765.
[21] D. Wagner, The boomerang attack, in: L.R. Knudsen (Ed.), Fast Software Encryption-FSE 1999, in: LNCS, Vol. 1636, Springer, Berlin, Heidelberg, 1999, pp. 156–170.
[22] Y. Wang, Q. Wang, W. Zhang, Boomerang uniformity of normalized permutation polynomials of low degree, Appl. Algebra Eng. Commun. Comput. 31 (3) (2020) 307–322.