Cryptography and Communications (2020) 12:1161–1178
https://doi.org/10.1007/s12095-020-00439-x

On the boomerang uniformity of some permutation polynomials

Marco Calderini[1] · Irene Villa[1]

Received: 31 July 2019 / Accepted: 6 May 2020 / Published online: 11 June 2020

Abstract

The boomerang attack, introduced by Wagner in 1999, is a cryptanalysis technique against block ciphers based on differential cryptanalysis. In particular it takes into consideration two differentials, one for the upper part of the cipher and one for the lower part, and it exploits the dependency of these two differentials. At Eurocrypt'18, Cid et al. introduced a new tool, called the Boomerang Connectivity Table (BCT), that permits to simplify this analysis. Next, Boura and Canteaut introduced an important parameter for cryptographic S-boxes called boomerang uniformity, that is the maximum value in the BCT. Very recently, the boomerang uniformity of some classes of permutations (in particular quadratic functions) have been studied by Li, Qu, Sun and Li, and by Mesnager, Tang and Xiong. In this paper we further study the boomerang uniformity of some non-quadratic differentially 4-uniform functions. In particular, we consider the case of the Bracken-Leander cubic function and three classes of 4-uniform functions constructed by Li, Wang and Yu, obtained from modifying the inverse functions.

Keywords Vectorial Boolean functions · Boomerang uniformity · Boomerang connectivity table · Boomerang attack

Mathematics Subject Classification (2010) 94C10 · 94A60 · 06E30 · 14G50

1 Introduction

A vectorial Boolean function, or (n, m)-function, is a function F from the vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. When $m = 1$, F is simply called a Boolean function. Vectorial Boolean functions and Boolean functions have a crucial role in the design of secure cryptographic primitives,

✉ Irene Villa
irene.villa@uib.no

Marco Calderini
marco.calderini@uib.no

[1] Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, Norway

such as block ciphers. In this context, a vectorial Boolean function is also called an S-box. Most modern block ciphers, such as the AES, implement S-boxes which are (n, n)-functions permuting the space $\mathbb{F}_2^n$. We refer the reader to [10] for an overview on vectorial Boolean functions.

In the following, we shall identify the vector space $\mathbb{F}_2^n$ to the finite field $\mathbb{F}_{2^n}$ with 2^n elements. Moreover, $\mathbb{F}_{2^n}^\star$ will denote the multiplicative group of $\mathbb{F}_{2^n}$.

Among the most efficient attacks on block ciphers there is the differential attack, introduced by Biham and Shamir [2]. In [19], Nyberg introduced the notion of differential uniformity which measures the resistance of an S-box to this attack. In particular, a vectorial Boolean function F is called differentially δ-uniform if the equation $F(x) + F(x + a) = b$ has at most δ solutions for any non-zero a and for all b. Since if x is a solution, then also $x + a$ is a solution of the equation, the smallest possible value for δ is 2. Functions achieving such differential uniformity are called almost perfect nonlinear (APN). APN functions have optimal resistance to differential attacks.

In 1999, Wagner [22] introduced the boomerang attack, which is an important cryptanalysis technique against block ciphers. This attack can be seen as an extension of classical differential attacks. In fact, it combines two differentials for the upper part and the lower part of the cipher. Since Wagner's seminal paper, many improvements and variants of boomerang attacks have been proposed (see for instance [1, 3, 14]).

In order to evaluate the feasibility of boomerang-style attacks, in EUROCRYPT 2018, Cid et al. [11] introduced a new cryptanalysis tool: the Boomerang Connectivity Table (BCT).

In 2018, Boura and Canteaut [4] introduced a parameter for cryptographic S-boxes called boomerang uniformity which is defined as the maximum value in the BCT.

Boura and Canteaut showed that the boomerang uniformity is invariant only with respect to affine equivalence and inverse transformation. They also gave the classification of all differentially 4-uniform permutations of 4 bits. Moreover, they obtained the boomerang uniformities for two classes of differentially 4-uniform functions, the inverse function and the the Gold functions over $\mathbb{F}_{2^n}$ for n even.

Recently, Li et al. [16] gave an equivalent definition to compute the BCT (and the boomerang uniformity) and provided a characterization by means of the Walsh transform of functions with a fixed boomerang uniformity. Moreover, they gave an upper bound for the boomerang uniformity of quadratic permutations, and provided also a class of quadratic permutations (related to the Gold functions), defined for n even, with differential 4-uniformity and boomerang 4-uniformity. Still in [16], the boomerang uniformity of a 4-uniform permutation obtained from the inverse function swapping the image of 0 and 1 (introduced in [23]) is also obtained.

Another recent paper of Mesnager et al. [18] studies the boomerang uniformity of quadratic permutations. In particular, from their results it is possible to obtain the boomerang uniformity of the Gold functions and the class studied in [16], and also the boomerang uniformity of the binomials studied in [6].

In this paper we further study the boomerang uniformity of certain classes of 4-uniform functions. In particular, we consider the Bracken-Leander cubic function $x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{2^{4k}}$ ([5]) and we show that the boomerang uniformity is upper bounded by 24. Using the software MAGMA it is possible to verify that in small dimension this upper bound can be attained. We also compute the boomerang uniformities for three classes of differentially 4-uniform permutations of maximal algebraic degree $n - 1$, obtained in [17, 23] from modifying the inverse function.

2 Preliminaries

Any function F from $\mathbb{F}_{2^n}$ to itself can be represented as a univariate polynomial of degree at most $2^n - 1$, that is

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i.$$

The *2-weight* of an integer $0 \leq i \leq 2^n - 1$, denoted by $w_2(i)$, is the (Hamming) weight of its binary representation. It is well known that the algebraic degree of a function F is given by

$$\deg(F) = \max\{w_2(i) \mid a_i \neq 0\}.$$

The function F is:

- *linear* if $F(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$;
- *affine* if it is the sum of a linear function and a constant;
- *DO* (Dembowski-Ostrom) *polynomial* if $F(x) = \sum_{0 \leq i < j < n} a_{ij} x^{2^i + 2^j}$, with $a_{ij} \in \mathbb{F}_{2^n}$;
- *quadratic* if it is the sum of a DO polynomial and an affine function.

For any $m \geq 1$ such that $m|n$ we can define the (linear) *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ by

$$\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

When $m = 1$ we will denote $\mathrm{Tr}_1^n(x)$ by $\mathrm{Tr}(x)$.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote the *Walsh transform* in $a, b \in \mathbb{F}_{2^n}$ by

$$\mathscr{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax + bF(x))}.$$

With *Walsh spectrum* we refer to the set of all possible values of the Walsh transform. The Walsh spectrum of a vectorial Boolean function F is strictly related to the notion of nonlinearity of F, denoted by $\mathscr{N}\mathscr{L}(F)$, indeed we have

$$\mathscr{N}\mathscr{L}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\star} |\mathscr{W}_F(a, b)|.$$

The derivative of F in the direction of $a \in \mathbb{F}_{2^n}$ is defined as $D_a F(x) = F(x+a) + F(x)$. Let

$$\delta_F = \max_{a \in \mathbb{F}_{2^n}^\star, b \in \mathbb{F}_{2^n}} |\{x : D_a F(x) = b\}|,$$

the map F is called *differentially* δ_F*-uniform*.

When F is used as an S-box inside a block cipher, the differential uniformity measures its contribution to the resistance to the differential attack [2]. The smaller δ_F is the better is the resistance of F to this attack. In even characteristic, the best resistance belongs to functions that are differentially 2-uniform, these functions are called *almost perfect nonlinear* or APN.

In [11], Cid et al. introduced the concept of Boomerang Connectivity Table for a permutation F over $\mathbb{F}_{2^n}$. Next, in [4] the authors introduced the notion of boomerang uniformity.

Definition 1 Let F be a permutation over $\mathbb{F}_{2^n}$, and a, b in $\mathbb{F}_{2^n}$.

The Boomerang Connectivity Table (BCT) of F is given by a $2^n \times 2^n$ table T, in which the entry for the position (a, b) is given by

$$T(a, b) = |\{x \in \mathbb{F}_{2^n} : F^{-1}(F(x) + a) + F^{-1}(F(x + b) + a) = b\}|.$$

Moreover, for any $a, b \in \mathbb{F}_{2^n}^{\star}$, the value

$$\beta_F = \max_{a,b\in\mathbb{F}_{2^n}^{\star}} |\{x \in \mathbb{F}_{2^n} \ : \ F^{-1}(F(x)+a) + F^{-1}(F(x+b)+a) = b\}|$$

is called the boomerang uniformity of F, or we call F a *boomerang β_F-uniform* function.

We recall that two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- *affine equivalent* if $F' = A_1 \circ F \circ A_2$ where the mappings $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- *extended affine equivalent* (EA-equivalent) if $F' = F'' + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathscr{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of F is the graph of F', that is, $\mathscr{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) \ : \ x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) \ : \ x \in \mathbb{F}_{2^n}\}$.

The nonlinearity and the differential uniformity are invariant for all these equivalence relations, while the boomerang uniformity is invariant for affine equivalence but not for EA- and CCZ-equivalence (see [4]).

It has been proved in [11] that $\delta_F \le \beta_F$ for any function F. Moreover, $\delta_F = 2$ if and only if $\beta_F = 2$. So, APN permutations offer an optimal resistance to both differential and boomerang attacks.

For odd values of n there are known families of APN permutations. While, for n even, no APN permutation exists for $n = 4$ and, up to CCZ-equivalence, there exists only one example of APN permutation over $\mathbb{F}_{2^6}$ ([7]), and with respect to the affine equivalence (for which the boomerang uniformity is invariant) these known APN permutations can be divided in 4 affine equivalence classes [8]. The existence of more APN permutations on an even number of bits remains an open problem.

So, it is interesting to study the boomerang uniformity of non-APN permutations, and in particular of the differentially 4-uniform functions. As is well-known, for an even integer n there are five classes of primarily constructed differentially 4-uniform permutations over $\mathbb{F}_{2^n}$, which are listed in Table 1.

The boomerang uniformity of Gold and Inverse functions have been determined in [4]. For the Bracken-Tan-Tan the boomerang uniformity was obtained from the results in [18].

Table 1 Primarily-constructed differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ (n even)

Name	**F**(**x**)	deg	Conditions	In
Gold	x^{2^i+1}	2	$n = 2k$, k odd $\gcd(i, n) = 2$	[12]
Kasami	$x^{2^{2i}-2^i+1}$	i+1	$n = 2k$, k odd $\gcd(i, n) = 2$	[13]
Inverse	x^{2^n-2}	$n-1$	$n = 2k$, $k \ge 1$	[19]
Bracken-Leander	$x^{2^{2k}+2^k+1}$	3	$n = 4k$, k odd	[5]
Bracken-Tan-Tan	$\zeta x^{2^i+1} + \zeta^{2^m} x^{2^{-m}+2^{m+i}}$	2	$n = 3m$, m even, $m/2$ odd, $\gcd(n, i) = 2$, $3 \mid m+i$ and ζ is a primitive element of $\mathbb{F}_{2^n}$	[6]

As it was noted in [16], the entry $T(a, b)$ of the BCT can be given by the number of solutions of the system

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

Since the BCT of F, T, and the BCT of F^{-1}, T', are such that $T(a, b) = T'(b, a)$, the boomerang uniformity of F is given by the maximum number of solutions of the system

$$\begin{cases} F(x+a) + F(y+a) = b \\ F(x) + F(y) = b, \end{cases} \quad \text{or equivalently} \quad \begin{cases} F(x+a) + F(y+a) = F(x) + F(y) \\ F(x) + F(y) = b. \end{cases}$$

Letting $y = x + \alpha$, it is equivalent to

$$\begin{cases} D_a D_\alpha F(x) = 0 \\ D_\alpha F(x) = b. \end{cases} \tag{1}$$

Thus, the boomerang uniformity of F is given by

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}^\star} |\{(x, \alpha) \in \mathbb{F}_{2^n}^2 \ : \ (x, \alpha) \text{ is a solution of } (1)\}|.$$

Note that, using this equivalent definition for the boomerang uniformity, it is possible to consider also maps which are not permutations. We will denote by $S_{a,b}$ the number of solutions of System (1) for any $a, b \in \mathbb{F}_{2^n}$.

For power functions we have the following.

Proposition 1 ([16]) *Let $F(x) = x^d$ be defined over $\mathbb{F}_{2^n}$. Then the boomerang uniformity of F is given by* $\max_{b \in \mathbb{F}_{2^n}^\star} S_{1,b}$.

Thus, the boomerang uniformity for a power function can be checked fixing $a = 1$.

3 On the Bracken-Leander map

In this section, we will give an upper bound on the boomerang uniformity of the Bracken-Leander permutation. Using the software MAGMA we are able also to show that this upper bound can be attained.

For an odd integer k, let $q = 2^k$ and consider the finite field with 2^{4k} elements $\mathbb{F}_{2^{4k}} = \mathbb{F}_{q^4}$. Over this field consider the differentially 4-uniform permutation

$$F(x) = x^{2^{2k}+2^k+1} = x^{q^2+q+1}.$$

In the following we will show that

Theorem 1 *Let $k > 1$ odd. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{2^{4k}}$ is such that $\beta_F \leq 24$.*

Before proving Theorem 1 we will prove two lemmata.

Lemma 1 *Let $k > 1$ be odd and $q = 2^k$. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{q^4}$ is such that*

$$S_{1,b} \leq \begin{cases} 4 & \text{if } b \in \mathbb{F}^\star_{q^2} \text{ and } Tr_1^{2k}(b) = 0 \\ 6 & \text{if } b \in \mathbb{F}^\star_{q^2} \text{ and } Tr_1^{2k}(b) = 1 \\ 4m+4 & \text{if } b \notin \mathbb{F}_{q^2}, \end{cases}$$

where m is the number of the solutions $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ of

$$b^{q^2} + b = \alpha^{q+1} \frac{(\alpha^{2q} + \alpha)(\alpha + 1)}{(\alpha^q + \alpha)^2}.$$

Proof We want to study the number of solutions, for $b \in \mathbb{F}^\star_{q^4}$, of

$$\begin{cases} D_1 D_\alpha F(x) = 0 \\ D_\alpha F(x) = b. \end{cases}$$

In particular, we have the following

$$\begin{aligned} D_\alpha F(x) &= (x+\alpha)^{q^2+q+1} + x^{q^2+q+1} \\ &= x^{q^2+q}\alpha + x^{q^2+1}\alpha^q + x^{q+1}\alpha^{q^2} + x^{q^2}\alpha^{q+1} + x^q\alpha^{q^2+1} + x\alpha^{q^2+q} + \alpha^{q^2+q+1}. \end{aligned}$$

And therefore

$$\begin{aligned} D_1 D_\alpha F(x) &= (x^{q^2} + x^q + 1)\alpha + (x^{q^2} + x + 1)\alpha^q + (x^q + x + 1)\alpha^{q^2} + \alpha^{q+1} \\ &\quad + \alpha^{q^2+1} + \alpha^{q^2+q} \\ &= y^q(\alpha + \alpha^q) + y(\alpha^q + \alpha^{q^2}) + \alpha + \alpha^q + \alpha^{q^2} + \alpha^{q+1} + \alpha^{q^2+1} + \alpha^{q^2+q}, \end{aligned}$$

where $y = x^q + x$. Hence, we have that $y^q + y = x^{q^2} + x$ is an element of $\mathbb{F}_{q^2}$, so $y^{q^3} = y^{q^2} + y^q + y$. For simplicity, let us denote $R = D_1 D_\alpha F(x) = 0$. Thus

$$R^q = y^{q^2}(\alpha^q + \alpha^{q^2}) + y^q(\alpha^{q^2} + \alpha^{q^3}) + \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \alpha^{q^2+q} + \alpha^{q^3+q} + \alpha^{q^3+q^2},$$

and using the fact that $y^{q^3} = y^{q^2} + y^q + y$

$$R^{q^2} = y^{q^2}(\alpha^{q^2}+\alpha)+y^q(\alpha^{q^2}+\alpha^{q^3})+y(\alpha^{q^2}+\alpha^{q^3})+\alpha^{q^2}+\alpha^{q^3}+\alpha+\alpha^{q^3+q^2}+\alpha^{q^2+1}+\alpha^{q^3+1}.$$

Then

$$\begin{aligned} 0 &= R^q + R^{q^2} \\ &= y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} + \alpha^q + \alpha + \alpha^{q^2+q} + \alpha^{q^3+q} + \alpha^{q^2+1} + \alpha^{q^3+1} \\ &= y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} + \alpha^q + \alpha + (\alpha^q + \alpha)^{q^2+1}. \end{aligned}$$

Since $y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} \in \mathbb{F}_{q^2}$ and $(\alpha^q + \alpha)^{q^2+1} \in \mathbb{F}_{q^2}$ then also $(\alpha^q + \alpha) \in \mathbb{F}_{q^2}$. Then, we can rewrite the equation as

$$\begin{aligned} 0 &= y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha) + \alpha^q + \alpha + (\alpha^q + \alpha)^2 = (\alpha^q + \alpha)(y^{q^2} + y + \alpha^q + \alpha + 1) \\ &= (\alpha^q + \alpha)(x^{q^3} + x^{q^2} + x^q + x + \alpha^q + \alpha + 1). \end{aligned}$$

Therefore one of the following conditions is satisfied:

1. $\alpha^q + \alpha = 0$, that is, $\alpha \in \mathbb{F}_q$;
2. $\mathrm{Tr}_k^{4k}(x) = x^{q^3} + x^{q^2} + x^q + x = \alpha^q + \alpha + 1$.

Case 1: $\alpha \in \mathbb{F}_q$.

We have $R = \alpha + \alpha^2 = 0$, hence $\alpha \in \mathbb{F}_2$. We do not consider the case $\alpha = 0$, therefore for $\alpha = 1$ we know that the equation $D_\alpha F(x) = b$ admits at most 4 solutions. So, for any b the number of solutions of type (x, α) with $\alpha \in \mathbb{F}_q$ is at most 4.

Case 2: $\mathrm{Tr}_k^{4k}(x) = x^{q^3} + x^{q^2} + x^q + x = \alpha^q + \alpha + 1$.

In this case, we need to compute the number of solutions (x, α) with $\alpha \notin \mathbb{F}_q$. Since $\mathrm{Tr}_k^{4k}(x) \in \mathbb{F}_q$, we have that $\alpha^q + \alpha \in \mathbb{F}_q^\star$. Therefore, $\alpha^{q^2} + \alpha = 0$, so we have $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$.

Then, we have $R = (\alpha^q + \alpha)(y^q + y) + \alpha^q + \alpha^2 = (\alpha^q + \alpha)(x^{q^2} + x) + \alpha^q + \alpha^2$, and the system that we have to analyse is the following

$$\begin{cases} \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \\ \mathrm{Tr}_k^{4k}(x) = \alpha^q + \alpha + 1 \\ (\alpha^q + \alpha)(x^{q^2} + x) = \alpha^q + \alpha^2 \\ D_\alpha F(x) = b. \end{cases} \tag{2}$$

It is clear that, for a fixed α, if $\bar{x}$ is a solution of the first three equations in (2), then all the other solutions (for these equations) are $\bar{x} + w$ for any $w \in \mathbb{F}_{q^2}$. Moreover, since $\alpha^q + \alpha \neq 0$, denoting by $\gamma = \frac{\alpha^q + \alpha^2}{\alpha^q + \alpha}$, we have $x^{q^2} = x + \gamma$.
The last equation is

$$\begin{aligned} b = D_\alpha F(x) &= x^{q^2+q}\alpha + x^{q^2+1}\alpha^q + x^{q+1}\alpha + x^{q^2}\alpha^{q+1} + x^q\alpha^2 + x\alpha^{q+1} + \alpha^{q+2} \\ &= (x+\gamma)x^q\alpha + (x+\gamma)x\alpha^q + x^{q+1}\alpha + (x+\gamma)\alpha^{q+1} + x^q\alpha^2 \\ &\quad + x\alpha^{q+1} + \alpha^{q+2} \\ &= x^q\alpha(\gamma+\alpha) + x^2\alpha^q + x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha). \end{aligned}$$

For $w \in \mathbb{F}_{q^2}$, there exist unique $r, s \in \mathbb{F}_q$ such that $w = r\alpha + s$. Hence, we have

$$\begin{aligned} D_\alpha F(x+w) &= (x^q + r\alpha^q + s)\alpha(\gamma+\alpha) + (x^2 + r^2\alpha^2 + s^2)\alpha^q + (x + r\alpha + s)\alpha^q\gamma \\ &\quad + \alpha^{q+1}(\gamma+\alpha) \\ &= D_\alpha F(x) + \gamma(r\alpha^{q+1} + s\alpha + r\alpha^{q+1} + s\alpha^q) + r\alpha^{q+2} + s\alpha^2 \\ &\quad + r^2\alpha^{q+2} + s^2\alpha^q \\ &= D_\alpha F(x) + \gamma s(\alpha + \alpha^q) + \alpha^{q+2}(r + r^2) + s(\alpha^2 + s\alpha^q) \\ &= D_\alpha F(x) + (\alpha^q + \alpha^2)s + \alpha^{q+2}(r + r^2) + s(\alpha^2 + s\alpha^q) \\ &= D_\alpha F(x) + \alpha^q(s + s^2) + \alpha^{q+2}(r + r^2). \end{aligned}$$

Then, $D_\alpha F(x+w) = D_\alpha F(x) = b$ if and only if $\alpha^q(s+s^2) + \alpha^{q+2}(r+r^2) = 0$. Since $\alpha \neq 0$, we have that $(s+s^2) + \alpha^2(r+r^2) = 0$ if and only if both $s+s^2$ and $r+r^2$ are zero ($r, s \in \mathbb{F}_q$ and $\alpha \notin \mathbb{F}_q$). Hence, fixed $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, if $\bar{x}$ is a solution of $D_\alpha F(x) = b$, then we can have only three more solutions, which are $\bar{x} + \alpha, \bar{x} + 1, \bar{x} + \alpha + 1$.

Consider now the following

$$\begin{aligned} b^{q^2} + b &= x^{q^3}\alpha(\gamma+\alpha) + x^{2q^2}\alpha^q + x^{q^2}\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) + x^q\alpha(\gamma+\alpha) \\ &\quad + x^2\alpha^q + x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ &= (x+\gamma)^q\alpha(\gamma+\alpha) + (x+\gamma)^2\alpha^q + (x+\gamma)\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ &\quad + x^q\alpha(\gamma+\alpha) + x^2\alpha^q + x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ &= \gamma^q\alpha(\gamma+\alpha) = \frac{\alpha + \alpha^{2q}}{\alpha^q + \alpha}\alpha\frac{\alpha^q(\alpha+1)}{\alpha^q+\alpha} = \alpha^{q+1}\frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}. \end{aligned}$$

Now, if $b \in \mathbb{F}_{q^2}$ we have either $\gamma = 0$ or $\gamma = \alpha$.

- If $\gamma = 0$, then from (2) we obtain $\alpha^q = \alpha^2$, $x \in \mathbb{F}_{q^2}$ and $\alpha^q + \alpha + 1 = 0$, implying that $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$.
- If $\gamma = \alpha$ then $\frac{\alpha^q+\alpha^2}{\alpha^q+\alpha} + \alpha = \frac{\alpha^q(\alpha+1)}{\alpha^q+\alpha} = 0$. This leads to $\alpha = 1$ (already studied).

Thus, for the case $b \in \mathbb{F}_{q^2}$, we need to count the number of solutions x of the following systems:

$$(I) \begin{cases} D_1 D_1 F(x) = 0 \\ D_1 F(x) = b, \end{cases} \qquad (II) \begin{cases} x^{q^2} + x = 0 \\ D_1 D_\omega F(x) = 0 \\ D_\omega F(x) = b, \end{cases} \qquad (III) \begin{cases} x^{q^2} + x = 0 \\ D_1 D_{\omega^2} F(x) = 0 \\ D_{\omega^2} F(x) = b, \end{cases}$$

where ω is a primitive element of $\mathbb{F}_4$.

Since we have the restriction $x^{q^2} + x = 0$, solving System (II) and (III) is equivalent to solve the systems

$$(II') \begin{cases} D_1 D_\omega G(x) = 0 \\ D_\omega G(x) = b, \end{cases} \qquad (III') \begin{cases} D_1 D_{\omega^2} G(x) = 0 \\ D_{\omega^2} G(x) = b, \end{cases}$$

defined over $\mathbb{F}_{q^2}$, where $G(x) = F_{|\mathbb{F}_{q^2}}(x) = x^{q+2}$.

Note that, for all these systems the equations involving the second derivative are satisfied for any $x \in \mathbb{F}_{q^2}$. Moreover, the function $G : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is a Gold function with boomerang uniformity 4 (see [4]) and we can have that at most one system between (II') and (III') admits 4 solutions.

Suppose now that $b \in \mathbb{F}_{q^2}$ and one between System (II) or (III) admits 4 solutions. We need to determine the number of solutions of System (I), that is, we need to study the number of solutions of $D_1 F(x) = b$. Let us consider, therefore, the proof of Theorem 1 in [5], in which the authors study the differential uniformity of F. According to their notation, we have $c = b + 1 \in \mathbb{F}_{q^2}$ and $t = \mathrm{Tr}(x) = \mathrm{Tr}(c) = 0$. If we consider now Equation (5) in [5] we have the following condition:

$$0 = (x + x^{q^2})^2 + (t+1)(x + x^{q^2}) + c^q + c^{q^3} = (x + x^{q^2})^2 + (x + x^{q^2}).$$

Hence $x + x^{q^2} = 0, 1$. The only possibility is $x^{q^2} = x + 1$, otherwise we would obtain a solution $x \in \mathbb{F}_{q^2}$ of $D_1 G(x) = b$ in contradiction with the boomerang uniformity of G. This restriction leads us to

$$\begin{aligned} D_1 F(x) &= x^{q^2+q} + x^{q^2+1} + x^{q+1} + x^{q^2} + x^q + x + 1 \\ &= (x+1)x^q + (x+1)x + x^{q+1} + x + 1 + x^q + x + 1 = x^2 + x \\ 0 &= x^2 + x + b. \end{aligned}$$

This last equation implies that we have, for $\alpha = 1$, at most 2 solutions. Moreover, since from $x^2 = x + b$ we obtain that $x^{q^2} = x + \mathrm{Tr}_1^{2k}(b)$, we can have these two more solutions if and only if $\mathrm{Tr}_1^{2k}(b) = 1$. Hence, in total we can have at most 6 solutions when $\mathrm{Tr}_1^{2k}(b) = 1$.

On the other hand, if $b \in \mathbb{F}_{q^2}$ and $\mathrm{Tr}_1^{2k}(b) = 0$ we can have only solutions $x \in \mathbb{F}_{q^2}$ for all the three systems. Therefore, since $G(x) = F_{|\mathbb{F}_{q^2}}(x)$ we can have at most only one of the systems admitting 4 solutions.

For $b \notin \mathbb{F}_{q^2}$, let m be the number of roots of the equation $b^{q^2} + b = \alpha^{q+1} \frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}$ such that $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then, for any of these roots we can have 4 possible x plus the 4 possible solutions when $\alpha = 1$. Hence, we have $S_{1,b} \le 4 \cdot (m+1)$. □

Remark 1 For the case $b \in \mathbb{F}_{q^2}$ it is possible to show that six solutions are possible. Consider $b = \omega$, where ω is a primitive element of $\mathbb{F}_4$. First of all, it is easy to check that any $x \in \mathbb{F}_4$ is a solution of System (II) in the proof of Lemma 1. Moreover, we have that $\mathrm{Tr}_1^{2k}(b) = 1$, so there exist two solutions in $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ of System (I) in Lemma 1. So, we have that $S_{1,\omega} = 6$.

Lemma 2 *Let $k > 1$ odd and $q = 2^k$. For any $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ the equation*

$$b^{q^2} + b = \alpha^{q+1}\frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}$$

admits at most 5 solutions $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Proof Consider the equation

$$b^{q^2} + b = \alpha^{q+1}\frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}. \tag{3}$$

Then, we have also the relation

$$\mathrm{Tr}_k^{4k}(b) = \alpha^{q+1}\frac{(\alpha^{q+1}+1)}{\alpha^q+\alpha}. \tag{4}$$

Let $d = b^{q^2} + b$ and $e = \mathrm{Tr}_k^{4k}(b) = d^q + d \in \mathbb{F}_q$.

If $d \in \mathbb{F}_q$, then $e = 0$ and therefore $\alpha^{q+1} = 1$ and $\alpha^q = \alpha^{-1}$. This leads to

$$d = 1 \cdot \frac{(\frac{1}{\alpha^2}+\alpha)(\alpha+1)}{\frac{1}{\alpha^2}+\alpha^2} = \frac{1+\alpha^3}{\alpha^2}(\alpha+1)\frac{\alpha^2}{(1+\alpha)^4} = \frac{1+\alpha^3}{(1+\alpha)^3} = \frac{\alpha^2+\alpha+1}{1+\alpha^2}.$$

Hence $\alpha^2(d+1) + \alpha + 1 + d = 0$, that has at most 2 solutions in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ if and only if $\mathrm{Tr}_1^k(d) = 0$. Indeed, if $\mathrm{Tr}_1^k(d) = 1$ we would have $\mathrm{Tr}_1^k(d^2+1) = 0$ and thus the equation admits 2 solutions in $\mathbb{F}_q$.

Now, consider the case $d \notin \mathbb{F}_q$ and thus $e \neq 0$. Denoting by $\gamma = \frac{\alpha^q+\alpha^2}{\alpha^q+\alpha}$, we have $d = \gamma^q\alpha(\gamma+\alpha)$ and

$$e = d^q + d = \gamma^{q+1}(\alpha^q+\alpha) + \gamma\alpha^{2q} + \gamma^q\alpha^2.$$

Since $d \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ we can write α as $\alpha = rd + s$, with $r, s \in \mathbb{F}_q, r \neq 0$. Therefore, we have $\alpha^q + \alpha = r(d^q + d) = re$. From $d(\alpha^q+\alpha)^2 = \alpha^{q+1}(\alpha^{2q}+\alpha)(\alpha+1)$ (3) we get

$$\begin{aligned} s^5 &= s^4rd^q + s^3(r^2e^2+1) + s^2(r^3d^qe^2 + r^2e^2 + rd^q) \\ &\quad + s(r^4d^{2q+2} + r^3e^3 + r^2d^2) + r^5d^{3q+2} + r^4d^{q+1}e^2 + r^3d^{q+2} + r^2de^2. \end{aligned} \tag{5}$$

From $e(\alpha^q+\alpha) = \alpha^{q+1}(\alpha^{q+1}+1)$ (4) we get

$$s^4 = s^2(r^2e^2+1) + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1}. \tag{6}$$

To simplify the equation, let us introduce the variable $A = re + 1$. Then we can rewrite (5) as

$$\begin{aligned} s^5 &= s^4rd^q + s^3A^2 + s^2(rd^qA^2 + A^2 + 1) + s(r^4d^{2q+2} + r^3e^3 + r^2d^2) \\ &\quad + r^5d^{3q+2} + r^4d^{q+1}e^2 + r^3d^{q+2} + r^2de^2, \end{aligned}$$

and (6) as

$$s^4 = s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1}.$$

Substituting the second one in the first one we obtain

$$\begin{aligned}
0 &= s(s^2A^2+sre+re^2+r^4d^{2q+2}+r^2d^{q+1})+(s^2A^2+sre+re^2+r^4d^{2q+2}\\
&\quad +r^2d^{q+1})rd^q+s^3A^2+s^2(rd^qA^2+A^2+1)+s(r^4d^{2q+2}+r^3e^3+r^2d^2)\\
&\quad +r^5d^{3q+2}+r^4d^{q+1}e^2+r^3d^{q+2}+r^2de^2\\
&= s^3A^2+s^2re+s(re^2+r^4d^{2q+2}+r^2d^{q+1})+s^2A^2rd^q+sr^2d^qe+r^2d^qe^2\\
&\quad +r^5d^{3q+2}+r^3d^{2q+1}+s^3A^2+s^2(rd^qA^2+A^2+1)+s(r^4d^{2q+2}+r^3e^3+r^2d^2)\\
&\quad +r^5d^{3q+2}+r^4d^{q+1}e^2+r^3d^{q+2}+r^2de^2\\
&= s^2(A^2+A)+s(re^2+r^3e^3+r^2e^2)+r^2e^3+r^4d^{q+1}e^2+r^3d^{q+1}e\\
&= s^2reA+sre^2(1+rA)+r^2e(e^2+rd^{q+1}A)\\
&= re[s^2A+se(1+rA)+r(e^2+rd^{q+1}A)].
\end{aligned}$$

Since $r, e \neq 0$, denoting by $B = e(1+rA)$ and by $C = r(e^2+rd^{q+1}A)$ we have

$$0 = s^2A + sB + C. \tag{7}$$

Replacing (7), hence $s^2A = sB + C$, into (6) ($s^4 = s^2A^2 + sre + K$, with $K = re^2 + r^4d^{2q+2} + r^2d^{q+1}$) we have

$$s^4 = A(sB+C)+sre+K = s(AB+re)+AC+K.$$

Thus raising (7) to the power of two and substituing s^4 we obtain

$$s^2B^2 = s(A^3B+A^2re)+A^3C+A^2K+C^2.$$

Using (7) (multiplied by B^2) we obtain

$$As^2B^2 = sB^3+B^2C = s(A^4B+A^3re)+A^4C+A^3K+AC^2,$$

which implies

$$0 = s(B^3+A^4B+A^3re)+B^2C+A^4C+A^3K+AC^2 = s\bar{D}+\bar{E}.$$

Therefore

$$\begin{aligned}
\bar{D} &= B^3+A^4B+A^3re = (e+reA)^3+A^4(e+reA)+A^3re\\
&= e[e^2+Are^2+A^2],\\
\bar{E} &= B^2C+A^4C+A^3K+AC^2\\
&= (e^2+A^2r^2e^2)(re^2+Ar^2d^{q+1})+A^4(re^2+Ar^2d^{q+1})\\
&\quad +A^3(re^2+r^4d^{2q+2}+r^2d^{q+1})+A(r^2e^4+A^2r^4d^{2q+2})\\
&= e[A^2r^2e^2+Ar^2d^{q+1}e+Ar^2e^3+re^3].
\end{aligned}$$

Let $D = \bar{D}e^{-1}$ and $E = \bar{E}e^{-1}$, then $Ds = E$ with

$$D = e^2+Are^2+A^2 \text{ and } E = A^2r^2e^2+Ar^2d^{q+1}e+Ar^2e^3+re^3.$$

Using this last relation inside (7) we have

$$\begin{aligned}
0 &= D^2(s^2A+sB+C)\\
&= D^2s^2A+D^2sB+D^2C\\
&= E^2A+DEB+D^2C.
\end{aligned}$$

Now, since

$$\begin{aligned} AE^2 &= A^5r^4e^4 + A^3r^4d^{2q+2}e^2 + A^3r^4e^6 + Ar^2e^6, \\ BDE &= A^5(r^3e^3 + r^3e^4 + r^2e^4 + d^{q+1}r^2e^2) + A^4(r^3d^{q+1}e^2 + r^2e^3), \\ &\quad +A^3(r^2e^4 + r^2e^5) + A^2re^4 + A(r^2e^6 + r^2d^{q+1}e^4) + re^6, \\ CD^2 &= A^5r^2d^{q+1} + A^4re^2 + A^3r^4d^{q+1}e^4 + A^2r^3e^6 + Ar^2d^{q+1}e^4 + re^6, \end{aligned}$$

we obtain

$$\begin{aligned} 0 &= A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2) \\ &\quad +A^4(r^3d^{q+1}e^2 + re^4) + A^3(r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5) \\ &= A^3rP(r), \end{aligned} \tag{8}$$

with

$$\begin{aligned} P(r) &= A^2(r^3e^4 + r^2e^4 + r^2e^3 + rd^{q+1}e^2 + rd^{q+1} + e^2) \\ &\quad +A(r^2d^{q+1}e^2 + e^4) + r^3d^{2q+2}e^2 + r^3d^{q+1}e^4 + re^5 \\ &= r^5e^6 + r^4(e^5 + e^6) + r^3(e^4 + d^{q+1}(e^2 + e^3) + d^{2q+2}e^2) \\ &\quad +r^2(e^3 + d^{q+1}e^2) + rd^{q+1}(e^2 + 1) + e^4 + e^2. \end{aligned}$$

We need to find solutions of (8) related to some $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ that satisfies (3). Equation (8) is satisfied if either one of the following conditions is true

1. $A = 0$,
2. $r = 0$, not acceptable since $\alpha \notin \mathbb{F}_q$,
3. $P(r) = 0$.

Assume that $A = 0$ is a possible solution, therefore $r = \frac{1}{e}$ (it is related to an α for which (3) holds). From (7) we obtain that $se + re^2 = 0$, therefore $s = 1$. From (6) we have

$$\begin{aligned} s^4 &= s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1} \\ 1 &= 0 + 1 + e + \frac{d^{2q+2}}{e^4} + \frac{d^{q+1}}{e^2} \\ d^{2q+2} &= e^2d^{q+1} + e^5. \end{aligned}$$

Hence, we obtain that

$$\begin{aligned} r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5 &= r^4d^{q+1}e^4 + r^4e^7 + r^4d^{q+1}e^4 + r^2e^5 \\ &= r^2e^5(r^2e^2 + 1) = r^2e^5A^2 \end{aligned}$$

and using this equality we have that (8) becomes

$$\begin{aligned} 0 = E^2A + DEB + D^2C &= A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2) \\ &\quad +A^4(r^3d^{q+1}e^2 + re^4) + A^3(r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5) \\ &= A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2) \\ &\quad +A^4(r^3d^{q+1}e^2 + re^4) + A^5r^2e^5 \\ &= A^4r[A(r^3e^4 + r^2e^4 + r^2e^3 + rd^{q+1}e^2 + rd^{q+1} + e^2 + re^5) \\ &\quad +r^2d^{q+1}e^2 + e^4] \\ &= A^4rQ(r), \end{aligned}$$

where $Q(r)$ is a polynomial of degree at most 4. Therefore, if b is such that among the solution of (3) there is one for which $A = 0$, then at most we have 5 possible solutions r of (8).

Otherwise, if $A = 0$ is not a possible solution, then $P(r)$ can have at most 5 different roots. Hence, in total we have at most 5 different possible r.

We need to check, how many s there exist for any of these r. From the equation $Ds = E$ we know that, given a fixed r, unless $D = 0$, there exists only one possible s. We need to study the case $D = A^2 + Are^2 + e^2 = 0$. From (7), that is, $As^2 + Bs + C = 0$ we obtain that we can have at most two s for any r (in the case $D = 0$).

If $A = 0$, then (7) admits at most one solution since $B = Are + e = e \neq 0$. Also if $A \neq 0$ and $B = 0$, then the equation admits only one solution. In particular, (7) admits two solutions if and only if $B \neq 0$ and $\mathrm{Tr}\left(\frac{AC}{B^2}\right) = 0$. Hence, we need to study the system

$$\begin{cases} 0 \neq A \\ 0 \neq B = Are + e \\ 0 = D = A^2 + Are^2 + e^2 = A^2 + eB \\ 0 = E = A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 = re^2B + eC + B^2 + e^2A. \end{cases}$$

Then, we have $A^2 = Are^2 + e^2$ and (substituting A) $r^2(e^2 + e^3) = re^2 + e^2 + 1$, that leads to the restriction $e \neq 1$. Using these relations inside E we obtain

$$\begin{aligned} 0 &= A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= (Are^2 + e^2)r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= Ar^3e^4 + r^2e^4 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= r^4e^5 + r^3e^4 + r^2e^4 + r^3d^{q+1}e^2 + r^2d^{q+1}e + r^3e^4 + r^2e^3 + re^3 \\ &= re(r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2), \end{aligned} \tag{9}$$

which implies $r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2 = 0$ and thus

$$\begin{aligned} 0 &= (r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2)(e^2 + e) \\ &= re^3r^2(e^2 + e^3) + r(e^5 + e^4) + d^{q+1}r^2(e^3 + e^2) \\ &\quad + rd^{q+1}(e^2 + e) + r(e^4 + e^3) + e^3 + e^4 \\ &= re^3(re^2 + e^2 + 1) + r(e^5 + e^4) + d^{q+1}(re^2 + e^2 + 1) \\ &\quad + rd^{q+1}(e^2 + e) + r(e^4 + e^3) + e^3 + e^4 \\ &= r^2e^5 + d^{q+1}(e^2 + 1) + rd^{q+1}e + e^3(e + 1) \\ 0 &= (r^2e^5 + d^{q+1}(e^2 + 1) + rd^{q+1}e + e^3(e + 1))(e + 1). \end{aligned}$$

Using the substitution $r^2(e^2 + e^3) = re^2 + e^2 + 1$ we have

$$\begin{aligned} 0 &= e^3(re^2 + e^2 + 1) + d^{q+1}(e + 1)^3 + rd^{q+1}(e^2 + e) + e^3(e + 1)^2 \\ &= r(e^5 + d^{q+1}(e^2 + e)) + d^{q+1}(e + 1)^3. \end{aligned}$$

Hence, we have only one possible r that satisfies the system. Now, from $r^2(e^2+e^3)+re^2+e^2+1=0$ we have also

$$\begin{aligned}
0 &= (r^2(e^2+e^3)+re^2+e^2+1)(e^4+d^{q+1}(e+1))\\
&= red^{q+1}(e+1)^3+re^2d^{q+1}(e+1)^3+ed^{q+1}(e+1)^3+e^4(e+1)^2+d^{q+1}(e+1)^3\\
&= (e+1)^2(rd^{q+1}e(e+1)^2+d^{q+1}(e+1)^2+e^4)\\
&= (e+1)^2[(e+1)(re^5+d^{q+1}(e+1)^3)+d^{q+1}(e+1)^2+e^4]\\
&= (e+1)^2[re^5(e+1)+d^{q+1}(e+1)^4+d^{q+1}(e+1)^2+e^4]\\
&= (e+1)^2e^2[re^3(e+1)+d^{q+1}(e+1)^2+e^2]
\end{aligned}$$

and thus $re^3(e+1)=d^{q+1}(e+1)^2+e^2$. Moreover, from $re^3(e+1)+d^{q+1}(e+1)^2+e^2=0$, we can obtain

$$\begin{aligned}
0 &= [re^3(e+1)+d^{q+1}(e+1)^2+e^2](e^4+d^{q+1}(e+1))\\
&= e^2d^{q+1}(e+1)^4+d^{q+1}e^4(e+1)^2+e^6+d^{2q+2}(e+1)^3\\
&\quad +d^{q+1}e^2(e+1)\\
&= e^3d^{q+1}(e+1)+e^6+d^{2q+2}(e+1)^3\\
d^{2q+2}(e+1)^3 &= e^3d^{q+1}(e+1)+e^6.
\end{aligned}$$

From the two equations above we have also $re^3(1+e)=d^{q+1}(1+e)^2+e^2$ and $d^{2q+2}(1+e)^3=d^{q+1}e^3(1+e)+e^6$. We know that $e\neq 0,1$ therefore

$$r=\frac{d^{q+1}(e+1)}{e^3}+\frac{1}{e(e+1)}.$$

Hence,

$$\begin{aligned}
A &= re+1\\
&= \frac{d^{q+1}(e+1)}{e^2}+\frac{e}{(e+1)}\\
A^2 &= \frac{d^{2q+2}(e+1)^2}{e^4}+\frac{e^2}{(e+1)^2}=\frac{d^{q+1}}{e}+\frac{e^3}{(e+1)^2}\\
0 &= D=A^2+Are+e^2\\
&= \frac{d^{q+1}}{e}+\frac{e^3}{(e+1)^2}+\left(\frac{d^{q+1}(e+1)}{e^2}+\frac{e}{(e+1)}\right)\left(\frac{d^{q+1}(e+1)}{e^2}+\frac{1}{(e+1)}\right)+e^2\\
&= \frac{d^{q+1}}{e}+\frac{e^3}{(e+1)^2}+\frac{d^{2q+2}(e+1)^2}{e^4}+\frac{d^{q+1}(e+1)}{e^2}+\frac{e}{(e+1)^2}+e^2\\
&= \frac{d^{q+1}}{e}+\frac{e^3}{(e+1)^2}+\frac{d^{q+1}}{e}+\frac{e^2}{(e+1)}+\frac{d^{q+1}(e+1)}{e^2}+\frac{e}{(e+1)^2}+e^2\\
&= d^{q+1}(\frac{e+1}{e^2})+e+e^2+\frac{e^2}{e+1}=d^{q+1}\cdot\frac{e+1}{e^2}+\frac{e(e^2+e+1)}{e+1}\\
d^{q+1} &= \frac{e^3(e^2+e+1)}{(e+1)^2}.
\end{aligned}$$

Therefore

$$r=\frac{e^2+e+1}{e+1}+\frac{1}{e(e+1)}=\frac{(e+1)^2}{e}$$

and $A = re + 1 = e^2$. Then

$$0 = E = A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 = (e+1)^3 \cdot e^2.$$

This last result is not possible since $e \neq 0, 1$. So, the system admits no solutions.

Therefore we have that when $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, (3) admits at most 5 distinct values. □

Proof of Theorem 1 Since F is a power function, from Proposition 1 we can consider $a = 1$, and thus $\beta_F = \max_{b \in \mathbb{F}^{\star}_{q^4}} S_{1,b}$. From Lemmas 1 and 2 we have immediately that $\beta_{FF} \leq 24$. □

From the proof of Lemmas 1 and 2 we can distinguish five cases for the upper bound on the values $S_{1,b}$. In particular, we obtain the following.

Proposition 2 *Let $k > 1$ be odd and $q = 2^k$. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{q^4}$ is such that*

$$S_{1,b} \leq \begin{cases} 4 & \textit{if } b \in \mathbb{F}^{\star}_{q^2} \textit{ and } Tr_1^{2k}(b) = 0 \\ 6 & \textit{if } b \in \mathbb{F}^{\star}_{q^2} \textit{ and } Tr_1^{2k}(b) = 1 \\ 4 & \textit{if } b \notin \mathbb{F}_{q^2}, Tr_{2k}^{4k}(b) \in \mathbb{F}_q \textit{ and } Tr_1^k(Tr_{2k}^{4k}(b)) = 1 \\ 12 & \textit{if } b \notin \mathbb{F}_{q^2}, Tr_{2k}^{4k}(b) \in \mathbb{F}_q \textit{ and } Tr_1^k(Tr_{2k}^{4k}(b)) = 0 \\ 24 & \textit{otherwise.} \end{cases}$$

Using Lemma 1 we evaluated (with the help of MAGMA) the boomerang uniformity for the Bracken-Leander permutation up to dimension $n = 60$. From Table 2 we can see that for the values $7 \leq k \leq 15$ the upper bound for the boomerang uniformity is attained.

4 On the inverse function modified

In the past years, several constructions of differentially 4-uniform bijective functions, based on modifying the inverse function, have been proposed (see for instance [17, 20, 21, 23, 24]). In particular, in [17, 23], the authors modified the inverse functions composing it with some cycle, and studied when it could be possible to obtain a differentially 4-uniform permutation. In the following we will study the boomerang uniformity of some of the functions studied in [17] and in [23].

Given $m + 1$ pairwise different elements of $\mathbb{F}_{2^n}$, α_i for $0 \leq i \leq m$, consider the cycle $\pi = (\alpha_0, \alpha_1, ..., \alpha_m)$ over $\mathbb{F}_{2^n}$ defined as

$$\pi(x) = \begin{cases} \alpha_{i+1} & x = \alpha_i \\ x & x \notin \{\alpha_i | 0 \leq i \leq m\}, \end{cases}$$

where $\alpha_{m+1} = \alpha_0$.

Table 2 Boomerang uniformity of the function $x^{2^{2k}+2^k+1}$ over $\mathbb{F}_{2^{4k}}$

k :	3	5	7	9	11	13	15
β_F :	14	16	24	24	24	24	24

In [23] the authors study the case of cycle of length two (that is π a transposition), while in [17] they consider the more general case of functions of type

$$\pi(x)^{-1} = \begin{cases} \alpha_{i+1}^{-1} & x = \alpha_i \\ x^{-1} & x \notin \{\alpha_i | 0 \leq i \leq m\}. \end{cases}$$

From [23] we have that:

Lemma 3 *Let $n = 2k$ be an even integer. Then the following statements hold.*

1. *Suppose $\pi = (0, 1)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if k is odd.*
2. *Suppose $\pi = (1, c)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if $Tr(c) = Tr(\frac{1}{c}) = 1$.*

In [17] it has been proved the following:

Lemma 4 *Suppose $\pi = (\alpha_0, \dots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Then the following statements hold.*

1. *If $0 \in \pi$, then $\pi(x)^{-1}$ is affine equivalent to $\pi_1(x)^{-1}$, where π_1 is a cycle over $\mathbb{F}_{2^n}$ of the type $(0, 1, \beta_1, \dots, \beta_{m-1})$.*
2. *If $0 \notin \pi$, then $\pi(x)^{-1}$ is affine equivalent to $\pi_1(x)^{-1}$, where π_1 is a cycle over $\mathbb{F}_{2^n}$ of the type $(1, \beta_1, \dots, \beta_m)$.*

Recalling that the boomerang uniformity is invariant for affine equivalence, when $m = 1$ we need to consider, up to affine equivalence, only two types of permutations $\pi(x)^{-1}$:

- $\pi = (0, 1)$,
- $\pi = (1, c)$, with $c \neq 0, 1$.

In [16] Li et al. studied the boomerang uniformity of $\pi(x)^{-1}$ with $\pi = (0, 1)$. They obtained the following result.

Theorem 2 *Let $F(x) = \pi(x)^{-1}$, for $\pi = (0, 1)$, and $n \geq 3$. Then the boomerang uniformity of F is* $\beta_F = \begin{cases} 10, & if\ n \equiv 0\ (mod\ 6), \\ 8, & if\ n \equiv 3\ (mod\ 6), \\ 6, & if\ n \not\equiv 0\ (mod\ 3). \end{cases}$

Considering the case $\pi = (1, c)$ we obtain the following.

Theorem 3 *Let n be even and $F(x) = \pi(x)^{-1}$ with $\pi = (1, c)$ be a differentially 4-uniform function over $\mathbb{F}_{2^n}$. Then,*

(i) *if $c \notin \mathbb{F}_4$*

$$\beta_F = \begin{cases} 10 & if\ n \equiv 0 \mod 4 \\ 8 & if\ n \equiv 2 \mod 4. \end{cases}$$

(ii) *if $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ (thus $n \equiv 2 \mod 4$) $\beta_F = 6$.*

The proof of Theorem 3 relies just on the study of all the possible cases that we can obtain in System (1) and on the, well-known, characterization of the solutions of the equation $x^{-1} + (x + a)^{-1} = b$ (see for instance [19]). For such a reason the proof is omitted, but we redirect the interested reader to [9].

From Theorems 2 and 3 we obtain the following corollary.

Corollary 1 *Let $n = 2k$ and $\pi = (\alpha_1, \alpha_2)$. Consider the function $F(x) = \pi(x)^{-1}$ defined over $\mathbb{F}_{2^n}$ and suppose that F is differentially 4-uniform. Then,*

(i) *if $0 \in \pi$, then k is odd and*

$$\beta_F = \begin{cases} 10, & \textit{if}\ n \equiv 0\ (\textit{mod}\ 6), \\ 6, & \textit{otherwise}. \end{cases}$$

(ii) *if $0 \notin \pi$, then*

(a) *if $\frac{\alpha_2}{\alpha_1} \notin \mathbb{F}_4^\star$, then*

$$\beta_F = \begin{cases} 10\ \textit{if}\ n \equiv 0 \mod 4, \\ 8\ \ \textit{if}\ n \equiv 2 \mod 4. \end{cases}$$

(b) *if $\frac{\alpha_2}{\alpha_1} \in \mathbb{F}_4^\star$, then k is odd and $\beta_F = 6$.*

Proof If $0 \in \pi$ then from Lemma 4 we have that $F(x) = \pi(x)^{-1}$ is affine equivalent to $\pi_0(x)^{-1}$ where $\pi_0(x) = (0, 1)$. So from Theorem 2 and since in the case $n \equiv 3 \mod 6$ F cannot be differentially 4-uniform we have our claim.

Suppose now that $\alpha_1, \alpha_2 \neq 0$. From Lemma 4 we have that $\alpha_1^{-1}\pi(\alpha_1 x) = \pi_1(x)$ where $\pi_1(x) = (1, \beta_1)$ with $\beta_{F1} = \frac{\alpha_2}{\alpha_1}$, and thus $F(x) = \pi(x)^{-1}$ is affine equivalent to $\pi_1(x)^{-1} = \alpha_1\pi(\alpha_1 x)^{-1}$. From Theorem 3 we obtain the claim. □

In [17], the authors extend the results obtained in [23] by composing the inverse function with cycles of order greater than two. In particular from their results we have the following differentially 4-uniform functions.

Lemma 5 *Let $n = 2k$ with $k > 1$. Let $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then the functions $F(x) = \pi(x)^{-1}$ with $\pi = (0, 1, c)$ and $G(x) = \pi(x)^{-1}$ with $\pi = (1, c, c^2)$ are differentially 4-uniform if and only if k is odd.*

Using a similar analysis as in Theorem 3 we can get the following results.

Theorem 4 *Let $n = 2k$ with $k > 1$ odd. Let $F(x) = \pi(x)^{-1}$ with $\pi = (0, 1, c)$ and $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, be a differentially 4-uniform function over $\mathbb{F}_{2^n}$. Then,*

$$\beta_F = \begin{cases} 8\ \textit{if}\ n \equiv 0 \mod 6, \\ 6\ \textit{otherwise}. \end{cases}$$

Theorem 5 *Let $n = 2k$ with $k > 1$ odd. Let $F(x) = \pi(x)^{-1}$ with $\pi = (1, c, c^2)$ and $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, be a differentially 4-uniform function over $\mathbb{F}_{2^n}$. Then,*

$$\beta_F = \begin{cases} 8\ \textit{if}\ n \equiv 0 \mod 6, \\ 6\ \textit{otherwise}. \end{cases}$$

As for Theorem 3, we redirect the interested reader to [9] for the proofs of Theorems 4 and 5.

Using the same arguments as in the proof of Corollary 1, we have the following.

Corollary 2 *Let $n = 2k$ with k odd and $\pi = (\alpha_1, \alpha_2, \alpha_3)$ with $\alpha_1, \alpha_2, \alpha_3 \in \gamma\mathbb{F}_4$ for some $\gamma \in \mathbb{F}_{2^n}^{\star}$. Consider the function $F(x) = \pi(x)^{-1}$ defined over $\mathbb{F}_{2^n}$ and suppose that F is differentially 4-uniform. Then,*

$$\beta_F = \begin{cases} 8 & \textit{if } n \equiv 0 \mod 6, \\ 6 & \textit{otherwise}. \end{cases}$$

5 Conclusions

In this paper we studied the boomerang uniformity of some classes of differentially 4-uniform permutations defined over $\mathbb{F}_{2^n}$ with n even. In particular, we obtained an upper bound for the boomerang uniformity of the cubic functions introduced by Bracken and Leander [5] and the boomerang uniformity for some of the functions studied in [17, 23].

From the results in [16, 18] we have that from quadratic permutations it is possible to obtain functions with optimal BCT, that is function with $\delta_F = \beta_F$. However, for cryptographic applications, quadratic functions could be weak with respect to higher order differential attacks [15]. So it would be interesting to construct optimal functions with degree greater than two and which are, in particular, 4-uniform.

In [4], it has been proved that if $n \equiv 2 \mod 4$, then the inverse function is optimal ($\delta_F = \beta_F = 4$). However, for the case $n \equiv 0 \mod 4$, which is widely used in cryptographic algorithm, from the results obtained in this paper and in the previous ones [4, 16, 18] we can not find any permutations over $\mathbb{F}_{2^n}$ with boomerang uniformity 4. So, an interesting open problem is to investigate the existence of a permutation having boomerang uniformity 4 over $\mathbb{F}_{2^n}$ with $n \equiv 0 \mod 4$.

Acknowledgments This research was supported by Trond Mohn Stiftelse (TMS) foundation.

Funding Information Open Access funding provided by University of Bergen.

References

1. Biham, E., Dunkelman, O., Keller, N.: New results on boomerang and rectangle attacks. FSE 2002, ser. Lect. Notes Comput. Sci. **2365**, 1–16 (2002)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology **4**(1), 3–72 (1991)
3. Biryukov, A., De Cannière, C., Dellkrantz, G.: Cryptanalysis of SAFER++. CRYPTO 2003, ser. Lect. Notes Comput. Sci. **2729**, 195–211 (2003)
4. Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic Sboxes. IACR Trans. Symmetric Cryptol. **2018**(3), 290–310 (2018)
5. Bracken, C., Leander, G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields Appl. **16**, 231–242 (2010)

6. Bracken, C., Tan, C.H., Tan, Y.: Binomial differentially 4-uniform permutations with high nonlinearity. Finite Fields Appl. **18**(3), 537–546 (2012)
7. Browning, K.A., Dillon, J.F., McQuistan, M.T., Wolfe, A.J.: An APN permutation in dimension six. Finite Fields: Theory Appl. **518**, 33–42 (2010)
8. Calderini, M.: On the EA-classes of known APN functions in small dimensions, Cryptogr. Commun. https://doi.org/10.1007/s12095-020-00427-1 (2020)
9. Calderini, M., Villa, I.: On the boomerang uniformity of some permutation polynomials IACR cryptology ePrint archive 2019: 881 - https://eprint.iacr.org/2019/881 (2019)
10. Carlet, C.: Vectorial Boolean functions for cryptography, encyclopedia of mathematics and its applications, pp. 398–470. Cambridge University Press, Cambridge (2010)
11. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. EUROCRYPT 2018, ser. Lect. Notes Comput. Sci. **10821**, 683–714 (2018)
12. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.) IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
13. Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Inf. Control. **18**(4), 369–394 (1971)
14. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round MARS and Serpent. FSE 2000, ser. Lect. Notes Comput. Sci. **1978**, 75–93 (2001)
15. Knudsen, L.: Truncated and higher order differentials. FSE 1994, ser. Lect. Notes Comput. Sci. **1008**, 196–211 (1995)
16. Li, K., Qu, L., Sun, B., Li, C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inf. Theory **65**(11), 7542–7553 (2019)
17. Li, Y., Wang, M., Yu, Y.: Constructing Differentially 4-uniform Permutations over GF (22k) from the Inverse Function Revisited IACR Cryptology ePrint Archive 2013: 731 - https://eprint.iacr.org/2013/731 (2013)
18. Mesnager, S., Tang, C., Xiong, M.: On the boomerang uniformity of (quadratic) permutations over F_2^n. arXiv preprint arXiv:1903.00501 - https://arxiv.org/pdf/1903.00501.pdf (2019)
19. Nyberg, N.: Differentially uniform mappings for cryptography. EUROCRYPT'93, ser. Lect. Notes Comput. Sci. **765**, 55–64 (1994)
20. Qu, L.J., Tan, Y., Tan, C.H., Li, C.: Constructing differentially 4-uniform permutations over F_2^{2k} via the switching method. IEEE Trans. Inf. Theory **59**(7), 4675–4686 (2013)
21. Tang, D., Carlet, C., Tang, X.: Differentially 4-uniform bijections by permuting the inverse function. Des. Codes. Cryptogr. **77**, 117–141 (2014)
22. Wagner, D.: The boomerang attack. FSE'99, ser. Lect. Notes Comput. Sci. **1636**, 156–170 (1999)
23. Yu, Y., Wang, M., Li, Y.: Constructing differentially 4 uniform permutations from known ones. Chin. J. Electron. **22**(3), 495–499 (2013)
24. Zha, Z., Hu, L., Sun, S.: Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields Appl. **25**, 64–78 (2014)