Noname manuscript No.
(will be inserted by the editor)

On the Boomerang Uniformity of some Permutation Polynomials

Marco Calderini · **Irene Villa**

Received: date / Accepted: date

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, Chunming and Maosheng.

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 · 11T71

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, 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 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 $\mathbb{F}_{2^n}$.

M. Calderini (✉)
E-mail: marco.calderini@uib.no

I. Villa
E-mail: irene.villa@uib.no
Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, Norway

Among the most efficient attacks on block ciphers there is the differential attack, introduced by Biham and Shamir [3]. In [18], 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 [21] 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 [2,4,13]).

In order to evaluate the feasibility of boomerang-style attacks, in EUROCRYPT 2018, Cid et al. [10] introduced a new cryptanalysis tool: the Boomerang Connectivity Table (BCT).

In 2018, Boura and Canteaut [5] 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. [15] 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 [15], the boomerang uniformity of a 4-uniform permutation obtained from the inverse function swapping the image of 0 and 1 (introduced in [22]) is also obtained.

Another recent paper of Mesnager et al. [17] 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 [15], and also the boomerang uniformity of the binomials studied in [7].

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 $\mathbb{F}_{2^{4k}}$ ([6]) 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 [16, 22] 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 $0 \le i \le 2^n-1$, 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 $F(x) = \sum_{0\le i<j<n} a_{ij} x^{2^i+2^j}$, 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 $D_aF(x) = F(x+a)+F(x)$. Let

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

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 [3]. 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 [10], Cid et al. introduced the concept of Boomerang Connectivity Table for a permutation F over $\mathbb{F}_{2^n}$. Next, in [5] 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 [5]).

It has been proved in [10] that $\delta_F \leq \beta_F$ 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 $\mathbb{F}_{2^6}$ ([8]), 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 [9]. 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.

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 $\gcd(i,n) = 2$	[11]
Kasami	$x^{2^{2i}-2^i+1}$	i+1	$n = 2k$, k odd $\gcd(i,n) = 2$	[12]
Inverse	x^{2^n-2}	$n-1$	$n = 2k$, $k \geq 1$	[18]
Bracken-Leander	$x^{2^{2k}+2^k+1}$	3	$n = 4k$, k odd	[6]
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 $\mathbb{F}_{2^n}$	[7]

The boomerang uniformity of Gold and Inverse functions have been determined in [5]. For the Bracken-Tan-Tan the boomerang uniformity was obtained from the results in [17].

As it was noted in [15], 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 **([15])** *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*

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

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 $b \in \mathbb{F}_{q^4}^\star$, 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

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

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

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

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

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

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

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

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:

$$(I)\begin{cases} D_1D_1F(x)=0 \\ D_1F(x)=b, \end{cases} \qquad (II)\begin{cases} x^{q^2}+x=0 \\ D_1D_\omega F(x)=0 \\ D_\omega F(x)=b, \end{cases} \qquad (III)\begin{cases} x^{q^2}+x=0 \\ D_1D_{\omega^2}F(x)=0 \\ D_{\omega^2}F(x)=b, \end{cases}$$

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

$$(II')\begin{cases} D_1D_\omega G(x)=0 \\ D_\omega G(x)=b, \end{cases} \qquad (III')\begin{cases} D_1D_{\omega^2}G(x)=0 \\ D_{\omega^2}G(x)=b, \end{cases}$$

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 [5]) 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 $D_1F(x)=b$. Let us consider, therefore, the proof of Theorem 1 in [6], 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 [6] 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 $D_1G(x)=b$ in contradiction with the boomerang uniformity of G. This restriction leads us to

$$\begin{aligned} D_1F(x)=&x^{q^2+q}+x^{q^2+1}+x^{q+1}+x^{q^2}+x^q+x+1 \\ =&(x+1)x^q+(x+1)x+x^{q+1}+x+1+x^q+x+1=x^2+x \\ 0=&x^2+x+b. \end{aligned}$$

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 $d(\alpha^q + \alpha)^2 = \alpha^{q+1}(\alpha^{2q} + \alpha)(\alpha + 1)$ (Equation (3)) we get

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

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

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

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

$$s^5 = s^4 r d^q + s^3 A^2 + s^2(r d^q A^2 + A^2 + 1) + s(r^4 d^{2q+2} + r^3 e^3 + r^2 d^2) + r^5 d^{3q+2} + r^4 d^{q+1} e^2 + r^3 d^{q+2} + r^2 d e^2,$$

and Equation (6) as

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

Substituting the second one in the first one we obtain

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

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

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

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

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

we obtain

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

with

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

We need to find solutions of Equation (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 Equation (7) we obtain that $se + re^2 = 0$, therefore $s = 1$. From Equation (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

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

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 Equation (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

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

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

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

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 Lemma 1 and Lemma 2 we have immediately that $\beta_F \leq 24$. □

From the proof of Lemma 1 and Lemma 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*

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

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.

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

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

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 [16,19,20,22,23]). In particular, in [16,22], 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 [16] and in [22].

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

In [22] the authors study the case of cycle of length two (that is π a transposition), while in [16] 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 [22] 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 [16] 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 [15] 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*

$$\beta_F = \begin{cases} 10, & if\ n \equiv 0\ (mod\ 6), \\ 8, & if\ n \equiv 3\ (mod\ 6), \\ 6, & if\ n \not\equiv 0\ (mod\ 3). \end{cases}$$

In the following we will consider the case $\pi = (1,c)$. In the proof of Theorem 3 we will use the following well-known result.

Lemma 5 ([18]) *Let $n = 2k$ be an even integer. Then for any $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_{2^n}$, the following statements hold.*

1. *$x^{-1} + (x+a)^{-1} = b$ has no roots in $\mathbb{F}_{2^n}$ if and only if $Tr(\frac{1}{ab}) = 1$.*
2. *$x^{-1} + (x+a)^{-1} = b$ has 2 roots in $\mathbb{F}_{2^n}$ if and only if $ab \neq 1$ and $Tr(\frac{1}{ab}) = 0$.*
3. *$x^{-1} + (x+a)^{-1} = b$ has 4 roots in $\mathbb{F}_{2^n}$ if and only if $b = a^{-1}$. Furthermore, when $b = a^{-1}$ the 4 roots of the above equation in $\mathbb{F}_{2^n}$ are $\{0, a, a\omega, a\omega^2\}$, where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$.*

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 $c \notin \mathbb{F}_4$

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

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

Proof Our function is given by

$$F(x) = \begin{cases} 1 & x = c \\ c^{-1} & x = 1 \\ x^{-1} & x \neq 1, c \end{cases}$$

Since F is differentially 4-uniform we have that $\mathrm{Tr}(c) = \mathrm{Tr}\left(\frac{1}{c}\right) = 1$. Note that, if $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then $n \equiv 2 \mod 4$. In the following ω will denote a primitive element of $\mathbb{F}_4$. Let us study the solutions of System (2) for any $a, b \in \mathbb{F}_{2^n}^\star$. First of all, notice that $x \neq y$, otherwise $b = 0$. Moreover, due to the fact that if (x,y) is a solution, also $(y,x), (x+a, y+a), (y+a, x+a)$ are solutions, we just need to consider one of them for analyzing the solutions.

When $x = 0$ then we have:

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

- If $y = 1$, then $b = c^{-1}$ and $F(a) + F(a+1) = c^{-1}$. This is true if and only if $a = 1$ and also $a = c, c+1$ if $c \in \mathbb{F}_4$. Indeed, $a = 1$ it is obvious and if $a = c$ or $a = c+1$ we obtain the equation $(c+1)^{-1} + c^{-1} = 1$, that implies $c \in \mathbb{F}_4$. For the other values we have $a^{-1} + (a+1)^{-1} = c^{-1}$. But it does not admit solutions since $\mathrm{Tr}(c^{-1}) = 1$.
- If $y = c$, then $b = 1$ and $F(a) + F(a+c) = 1$. Similarly, this is true if and only if $a = c$ and $a = 1, c+1$ if $c \in \mathbb{F}_4$.
- If $y = a$, then $b = a^{-1}$ is a possible solution for any $a \neq 0, 1, c$.
- If $y = a+1$, with $a \neq 1, c+1$, then $b = (a+1)^{-1}$. Moreover, if $a = c$ then $c \in \mathbb{F}_4$. Otherwise $a^{-1} + c^{-1} = (a+1)^{-1}$ does not admits solutions since $\mathrm{Tr}(c) = 1$.
- If $y = a+c$, with $a \neq c, c+1$, then $b = (a+c)^{-1}$ and $a^{-1} + 1 = (a+c)^{-1}$. Moreover, if $a = 1$ we have $c \in \mathbb{F}_4$. But if $a \neq 0, 1, c, c+1$ it does not admits solutions since $\mathrm{Tr}(c^{-1}) = 1$.

- If $y \neq 0,1,c,a,a+1,a+c$, then $b = y^{-1}$. Thus, if $a = 1$ the equation $c^{-1}+(y+1)^{-1} = y^{-1}$ has no solutions. Also if $a = c$, then $1+(y+c)^{-1} = y^{-1}$ has no solutions.
  If $a \neq 1,c$, the equation $a^{-1}+(y+a)^{-1} = y^{-1}$ admits 4 possible solutions for y: $0,a,a\omega,a\omega^2$. From the cases above, only the last two can be considered.
  In particular, if $y = a\omega$ then $b = \omega^2 a^{-1}$ and $a \neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$. While, if $y = a\omega^2$ then $b = \omega a^{-1}$ and $a \neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$.

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

- If $y = c$, then $b = 1+c^{-1}$ and $F(a+1)+F(a+c) = 1+c^{-1}$. If $a = 1$ or $a = c$ then $c \in \mathbb{F}_4$. If $a = c+1$, then the equation is satisfied.
  For the other values we have $(a+1)^{-1}+(a+c)^{-1} = 1+c^{-1}$. Let $z = a+1$, then we have $z^{-1}+(z+1+c)^{-1} = c^{-1}(c+1)$. Since $\frac{(1+c)^2}{c} = 1$ if and only if $c \in \mathbb{F}_4$, then the equation admits four solutions if $c \in \mathbb{F}_4$, that are $\{0,c,c\omega,c\omega^2\} = \{0,1,c,c+1\}$, none of them admissible. Otherwise it admits two solutions that are $a = 0$ and $a = c+1$, both not admissible.
- If $y = a$, with $a \neq 0,1,c$, then $b = c^{-1}+a^{-1}$ and $F(a+1) = c^{-1}+a^{-1}$. When $a = c+1$ we have $1 = c^{-1}+(c+1)^{-1}$, implying $c \in \mathbb{F}_4$.
  If $a \neq 0,1,c,c+1$, then $(a+1)^{-1} = c^{-1}+a^{-1}$ has no solutions.
- If $y = a+1$, then $b = (a+1)^{-1}+c^{-1}$ is a possible solution for any $a \neq 0,1,c+1$.
- If $y = a+c$, with $a \neq 0,c,c+1$, then $b = (a+c)^{-1}+c^{-1}$ and $F(a+1)+1 = (a+c)^{-1}+c^{-1}$.
  If $a = 1$, then $(1+c)^{-1}+c^{-1} = 1$ implies $c \in \mathbb{F}_4$. For the other values we have $(a+1)^{-1}+1 = (a+c)^{-1}+c^{-1}$. Let $z = a+1$, then we have $z^{-1}+(z+1+c)^{-1} = c^{-1}(c+1)$, as explained before the equation admits at most four solutions that are $\{0,1,c,c+1\}$, none of them admissible.
- If $y \neq 0,1,c,a,a+1,a+c$, then $b = y^{-1}+c^{-1}$ and $F(a+1)+(y+a)^{-1} = y^{-1}+c^{-1}$.
  If $a = 1$, then the equation does not admit solutions. For $a = c+1$, the equation $1+(y+c+1)^{-1} = y^{-1}+c^{-1}$ admits at most four solutions: $\{0,1,c,c+1\}$, none of them admissible.
  For the other values we have $(a+1)^{-1}+(y+a)^{-1} = y^{-1}+c^{-1}$. Hence if $\mathrm{Tr}\left(\frac{c(a+1)}{a(c+a+1)}\right) = 0$, since $\frac{c(a+1)}{a(c+a+1)} = 1$ does not admit solutions, it yields two solutions for y. Otherwise, there is no valid y. In particular, we have $y = \frac{c}{bc+1}$ and $b^2ac(a+1)+ba(a+c+1)+c+1 = 0$.

  When $x = c$ we have:
$$\begin{cases} F(a+c)+F(y+a) = b \\ F(y)+1 = b. \end{cases}$$

Since $y \neq 0,1,c$ we have $b = y^{-1}+1$.

- If $y = a$, with $a \neq 0,1,c$, then $b = a^{-1}+1$ and $F(a+c) = a^{-1}+1$. If $a = c+1$ then $c \in \mathbb{F}_4$. In the other cases the equation has no solutions.
- If $y = a+1$, with $a \neq 0,1,c+1$, then $b = (a+1)^{-1}+1$ and $F(a+c)+c^{-1} = (a+1)^{-1}+1$. If $a = c$ then $c \in \mathbb{F}_4$ and $b = c^{-1}$.
  In the other cases we have $(a+c)^{-1}+(a+1)^{-1} = c^{-1}+1$. The equation admits at most four solutions that are $\{0,1,c,c+1\}$, none of them admissible.
- If $y = a+c$, then $b = (a+c)^{-1}+1$ is a possible solution for any $a \neq 0,c,c+1$.

- If $y \neq 0,1,c,a,a+1,a+c$, then $y^{-1}+1 = F(a+c)+(y+a)^{-1}$.
  If $a=c$, then the equation has no solutions.
  If $a=c+1$, then $y^{-1}+1=c^{-1}+(y+c+1)^{-1}$ admits at most four solutions $\{0,1,c,c+1\}$, all not admissible.
  If $a\neq 0,c,c+1$, then $y^{-1}+1=(a+c)^{-1}+(y+a)^{-1}$. Hence if $\mathrm{Tr}\left(\frac{(a+c)}{a(1+a+c)}\right)=0$, since $\frac{(a+c)}{a(1+a+c)}=1$ does not admit a solution, it has two possible values for y. Otherwise none. In particular $y=(b+1)^{-1}$ and $b^2a(a+c)+ba(a+c+1)+c+1=0$.

When $x\neq 0,1,c,a,a+1,a+c$ and $y\neq 0,1,c,a,a+1,a+c,x$ we have:

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

Hence we have $x=\frac{y}{by+1}$, $y\neq b^{-1}$. Therefore $x+a=\frac{y+aby+a}{by+1}$, $y\neq\frac{a}{ab+1}$, and

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

The equation admits two solutions if and only if $\mathrm{Tr}\left(\frac{1}{ab}\right)=0$. Moreover, we have, in order to keep the restriction on y, that $b+ab+a\neq 0$ and $bc^2+abc+a\neq 0$. Assume that $\frac{1}{ab}=r^2+r$, then we have $\frac{y}{a}=r$ or $\frac{y}{a}=r+1$. If $y=ra$ then $\frac{y}{by+1}=a(r+1)$. If $y=(r+1)a$ then $\frac{y}{by+1}=ra$. Since we consider pairs (x,y) up to a swap or the addition of a, we have just one. Therefore we have the following possible solution:

- $(\frac{y}{by+1},y)$ if $\frac{1}{ab}=r^2+r$, $b+ab+a\neq 0$, $bc^2+abc+a\neq 0$ and $y=ra$. Moreover $ra,(r+1)a\neq 0,1,c,a,a+1,a+c$

Considering the case $c\notin\mathbb{F}_4$, from the analysis above (swapping the pairs (x,y) and adding a) we have the following list:

(1) for $a=1$ and $b=c^{-1}$ we have the solutions $\{(0,1),(1,0)\}$,
(2) with $a=c$, and $b=1$, we have the solutions $\{(0,c),(c,0)\}$,
(3) with $b=a^{-1}$ and $a\neq 0,1,c$, we have $\{(0,a),(a,0)\}$,
(4) with $b=\omega^2a^{-1}$ and $a\neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$, we have $\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}$,
(5) with $b=\omega a^{-1}$ and $a\neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$, we have $\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}$,
(6) with $a=c+1$ and $b=c^{-1}+1$ we have $\{(1,c),(c,1)\}$,
(7) with $b=(a+1)^{-1}+c^{-1}$ and $a\neq 0,1,c+1$, we have $\{(1,a+1),(a+1,1)\}$,
(8) if $\mathrm{Tr}\left(\frac{c(a+1)}{a(c+a+1)}\right)=0$, $a\neq 0,1,c+1$ and $b^2ac(a+1)+ba(a+c+1)+c+1=0$, we have $\{(1,\frac{c}{bc+1}),(\frac{c}{bc+1},1),(a+1,a+\frac{c}{bc+1}),(a+\frac{c}{bc+1},a+1)\}$,

(9) with $b=(a+c)^{-1}+1$ and $a\neq 0,c,c+1$, $\{(c,c+a),(c+a,c)\}$,

(10) if $\mathrm{Tr}\left(\frac{a+c}{a(c+a+1)}\right)=0$, $a\neq 0,c,c+1$ and $b^2a(a+c)+ba(a+c+1)+c+1=0$, we have $\{(c,\frac{1}{b+1}),(\frac{1}{b+1},c),(c+a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,c+a)\}$,

(11) if $\frac{1}{ab}=r^2+r$ (that is $\mathrm{Tr}(\frac{1}{ab})=0$), $b+ab+a\neq 0$, $bc^2+abc+a\neq 0$ and $y=ra$, we have $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ Moreover $ra,(r+1)a\neq 0,1,c,a,a+1,a+c$.

We want to study now, for different possible fixed pairs $a,b\in\mathbb{F}_{2^n}^{\star}$ how many solutions (x,y) are possible.

- If $a=1$ the possible cases are
  condition (1) with $b=c^{-1}$,
  condition (9) with $b=(c+1)^{-1}+1$,
  condition (11) if $\mathrm{Tr}(b^{-1})=0$, $b\neq(c^2+c)^{-1}$.
  Obviously case (1) and (9) cannot coexist, since $c\notin\mathbb{F}_4$. Case (1) and (11) cannot either, since $\mathrm{Tr}(c)=1$. The same for (9) and (11). Therefore if $a=1$ there can be at most 2 solutions.
  We do not have to consider case (1) any more.
- If $a=c$ we have
  condition (2) with $b=1$,
  condition (7) with $b=(c+1)^{-1}+c^{-1}$,
  condition (11) if $\mathrm{Tr}((bc)^{-1})=0$, $b^{-1}\neq 1+c^{-1}$.
  Case (2) and (7) cannot coexist since $c\notin\mathbb{F}_4$. Also case (2) and (11) and case (7) and (11) cannot since $\mathrm{Tr}(c)=\mathrm{Tr}(c^{-1})=1$. Therefore if $a=c$ there can be at most 2 solutions.
  We do not have to consider case (2) any more.
- If $a=c+1$ we have
  condition (3) with $b=(c+1)^{-1}$,
  condition (4) with $b=(c+1)^{-1}\omega^2$,
  condition (5) with $b=(c+1)^{-1}\omega$,
  condition (6) with $b=c^{-1}+1$,
  condition (11) if $\mathrm{Tr}((bc+b)^{-1})=0$, $b\neq 1+c^{-1}$. Assume $\frac{1}{b(c+1)}=r+r^2$, with $r\neq 0,1,(c+1)^{-1},(c+1)^{-1}+1$.
  Therefore we have:
  - if $b=(c+1)^{-1}$, then the only possible cases are (3) and (11) with $r=\omega$.
  - if $b=(c+1)^{-1}\omega^2$, then we have case (4). For (6) we need $c^2+\omega^2c+1=0$, that has 2 values only if $\mathrm{Tr}(\omega)=0$. For case (11) we need also that $\mathrm{Tr}(\omega)=0$ but $b\neq c^{-1}+1$ (hence no condition (6)).
  - if $b=(c+1)^{-1}\omega$, then we have case (5). For (6) we need $c^2+\omega c+1=0$, that has 2 values only if $\mathrm{Tr}(\omega)=0$. For case (11) we need also that $\mathrm{Tr}(\omega)=0$ but $b\neq c^{-1}+1$ (hence no (6)).
  - if b is different from the cases already analysed, it is clear that it cannot satisfy more than one pair of cases.

  Therefore if $a=c+1$ there can be at most 6 solutions. Moreover, if $\mathrm{Tr}(\omega)=1$ there can be at most 4 solutions.
  We do not have to consider case (6) any more.
- If $a=b^{-1}\neq 1,c,c+1$ we can have
  condition (3) since the conditions is satisfied,
  condition (11) is possible if $b\neq\omega,\omega^2$ and $bc\neq\omega,\omega^2$ and $by=\omega$ or $by=\omega^2$.
  Therefore if $a=b^{-1}$ we have at most 4 solutions.
  We do not have to consider case (3) any more.
- If $a=b^{-1}\omega$ we have

condition (5) with $b \neq 0,1,\omega,\omega^2,c^{-1},c^{-1}\omega,c^{-1}\omega^2$,
condition (7) is possible if $b^2c+b(c\omega^2+1)+\omega=0$. Hence, we need $\mathrm{Tr}\Big(\frac{c\omega}{c^2\omega+1}\Big)=0$,
condition (8) is possible if $\mathrm{Tr}(c\omega^2)=0$ (hence $\mathrm{Tr}(c\omega)=1$). Moreover, we have $b^2c+b\omega+\omega=0$. If $c\omega^2=r^2+r$, then we have $b=r^{-1}$ or $b=(r+1)^{-1}$,
condition (9) is possible if $b^2c+b(c+\omega^2)+\omega=0$. Hence, we need $\mathrm{Tr}\Big(\frac{c\omega}{c^2+\omega}\Big)=0$,
condition (10) is possible if $\mathrm{Tr}(\frac{1}{c\omega})=0$. If $\frac{1}{c\omega}=r^2+r$, then $b=r\omega$ or $b=(r+1)\omega$.
condition (11) is possible if $\mathrm{Tr}(\omega)=0$.

Hence we have
- case (7) has to satisfy $cb^2+b(c\omega^2+1)+\omega=0$,
- case (8) has to satisfy $cb^2+b\omega+\omega=0$,
- case (9) has to satisfy $cb^2+b(\omega^2+c)+\omega=0$,
- case (10) has to satisfy $cb^2+bc\omega+\omega=0$.

It is clear that we can satisfy at most one condition of the above plus the condition of case (5) and case (11). Therefore if $ab=\omega$ we have at most 10 solutions. Moreover if $\mathrm{Tr}(\omega)=1$ we have at most 8 solutions. While, if $\mathrm{Tr}(c\omega^2)=\mathrm{Tr}(\frac{1}{c\omega})=\mathrm{Tr}(\omega)=1$ we have at most 6 solutions, and if $\mathrm{Tr}(\frac{c\omega}{c^2\omega+1})=\mathrm{Tr}(c\omega^2)=\mathrm{Tr}(\frac{c\omega}{c^2+\omega})=\mathrm{Tr}(\frac{1}{c\omega})=\mathrm{Tr}(\omega)=1$ we have at most 4 solutions.
We do not have to consider case (5) any more.

- If $a=b^{-1}\omega^2$ we have a symmetric set of solutions with the previous case.
In particular we obtain
  - case (7) has to satisfy $cb^2+b(c\omega+1)+\omega^2=0$ and $\mathrm{Tr}(\frac{c\omega^2}{c^2\omega^2+1})=0$,
  - case (8) has to satisfy $cb^2+b\omega^2+\omega^2=0$ and $\mathrm{Tr}(c\omega)=0$,
  - case (9) has to satisfy $cb^2+b(\omega+c)+\omega^2=0$ and $\mathrm{Tr}(\frac{c\omega^2}{c^2+\omega^2})=0$,
  - case (10) has to satisfy $cb^2+bc\omega^2+\omega^2=0$ and $\mathrm{Tr}(\frac{1}{c\omega^2})=0$.

Moreover we have the following relations:

$$\begin{aligned}\mathrm{Tr}\Big(\frac{1}{c\omega}\Big) &=1+\mathrm{Tr}\Big(\frac{1}{c\omega^2}\Big)\\ \mathrm{Tr}(c\omega^2) &=1+\mathrm{Tr}(c\omega)\\ \mathrm{Tr}\Big(\frac{c\omega}{c^2+\omega}\Big) &=\mathrm{Tr}\Big(\frac{c\omega^2}{c^2\omega^2+1}\Big)\\ \mathrm{Tr}\Big(\frac{c\omega}{c^2\omega+1}\Big) &=\mathrm{Tr}\Big(\frac{c\omega^2}{c^2+\omega^2}\Big)\end{aligned}$$

It is clear that we can satisfy at most one condition of the above plus the condition of case (4) and case (11). Therefore if $ab=\omega^2$ we have at most 10 solutions. Moreover, if $\mathrm{Tr}(\omega)=1$ we have at most 8 solutions.
While, if $\mathrm{Tr}(c\omega)=\mathrm{Tr}(\frac{1}{c\omega^2})=\mathrm{Tr}(\omega)=1$ we have at most 6 solutions, and if $\mathrm{Tr}(\frac{c\omega^2}{c^2\omega^2+1})=\mathrm{Tr}(c\omega)=\mathrm{Tr}(\frac{c\omega^2}{c^2+\omega^2})=\mathrm{Tr}(\frac{1}{c\omega^2})=\mathrm{Tr}(\omega)=1$ we have at most 4 solutions.
We do not have to consider case (4) any more.

- If condition (7) is satisfied, that is if $b=(a+1)^{-1}+c^{-1}$, we have
condition (7) for $a\neq 0,1,c+1$,
condition (11) is possible if $\mathrm{Tr}\Big(\frac{c(a+1)}{a(a+1+c)}\Big)=0$.
Therefore if $b=(a+1)^{-1}+c^{-1}$ we have at most 4 solutions.
We do not have to consider case (7) any more.

- If condition (9) is satisfied, that is if $b = (a+c)^{-1}+1$, we have
  condition (9) with $a \neq 0, c, c+1$.
  condition (11) is possible if $\mathrm{Tr}\left(\frac{a+c}{a(1+a+c)}\right) = 0$.
  Therefore if $b = (a+c)^{-1}+1$ we have at most 4 solutions.
  We do not have to consider case (9) any more.
- If condition (8) is satisfied, that is $b^2ac(a+1)+ba(a+1+c)+1+c = 0$, we have
  condition (8) if $\mathrm{Tr}\left(\frac{c(a+1)}{a(c+a+1)}\right) = 0$.
  condition (11) if $\mathrm{Tr}(\frac{1}{ab}) = 0$.
  Therefore if $b^2ac(a+1)+ba(a+1+c)+1+c = 0$ we have at most 6 solutions.
  We do not have to consider case (8) any more.
- If condition (10) is satisfied, that is $b^2a(a+c)+ba(a+1+c)+1+c = 0$, we have
  condition (10) if $\mathrm{Tr}\left(\frac{a+c}{a(c+a+1)}\right) = 0$.
  condition (11) if $\mathrm{Tr}(\frac{1}{ab}) = 0$.
  Therefore if $b^2a(a+c)+ba(a+1+c)+1+c = 0$ we have at most 6 solutions.
  We do not have to consider case (10) any more.
- For the other possible values for a and b we have at most 2 possible solutions coming from case (11).

Therefore we have that for $c \notin \mathbb{F}_4$ $\beta_F \leq 10$. Moreover, if $\mathbb{F}_{2^n} = \mathbb{F}_{2^{2k}}$ with k an odd integer, we have $\mathrm{Tr}(\omega) = 1$ and, in this case, we have $\beta_F = 8$. Indeed, since $\mathrm{Tr}(c\omega^2) = 1+\mathrm{Tr}(c\omega)$ we have that one of them is equal to zero, hence in the case $ab = \omega$ or $ab = \omega^2$ it is possible to reach 8 solutions for k odd. Otherwise, for k even, $\beta_F = 10$.

Now, let us consider the case $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Since we need the restriction $\mathrm{Tr}(c) = \mathrm{Tr}(c^{-1}) = 1$ then we consider $c = \omega$ or $c = \omega^2$ only over $\mathbb{F}_{2^{2k}}$ for k odd. Let us assume, without loss of generality, that $c = \omega$. Hence we have the following list of possible solutions.

(1) with $a = 1$ and $b = \omega^2$, we have the solutions $\{(0,1),(1,0)\}$,
(2) with $a = \omega$ and $b = \omega^2$, we have the solutions $\{(0,1),(1,0),(\omega,\omega^2),(\omega^2,\omega)\}$,
(3) with $a = \omega^2$ and $b = \omega^2$, we have the solutions $\{(0,1),(1,0),(\omega^2,\omega),(\omega,\omega^2)\}$,
(4) with $a = 1$ and $b = 1$, we have the solutions $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$,
(5) with $a = \omega$ and $b = 1$, we have the solutions $\{(0,\omega),(\omega,0)\}$,
(6) with $a = \omega^2$ and $b = 1$, we have the solutions $\{(0,\omega),(\omega,0),(\omega^2,1),(1,\omega^2)\}$,
(7) with $b = a^{-1}$ and $a \neq 0,1,\omega$, we have the solutions $\{(0,a),(a,0)\}$,
(8) with $a = \omega$ and $b = \omega$, we have the solutions $\{(0,\omega^2),(\omega^2,0),(\omega,1),(1,\omega)\}$,
(9) with $a = 1$ and $b = \omega$, we have the solutions $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$,
(10) with $b = \omega^2a^{-1}$ and $a \neq 0,1,\omega,\omega^2$, we have $\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}$,
(11) with $b = \omega a^{-1}$ and $a \neq 0,1,\omega,\omega^2$, we have $\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}$,
(12) with $a = \omega^2$ and $b = \omega$, we have the solutions $\{(1,\omega),(\omega,1)\}$,
(13) with $b = (a+1)^{-1}+\omega^2$ and $a \neq 0,1,\omega^2$, we have the solutions $\{(1,a+1),(a+1,1)\}$,
(14) if $\mathrm{Tr}\left(\frac{\omega(a+1)}{a(\omega^2+a)}\right) = 0, a \neq 0,1,\omega^2$ and $b^2a\omega(a+1)+ba(a+\omega^2)+\omega^2 = 0$, we have $\{(1,\frac{\omega}{b\omega+1}),(\frac{\omega}{b\omega+1},1),(a+1,a+\frac{\omega}{b\omega+1}),(a+\frac{\omega}{b\omega+1},a+1)\}$,
(15) with $b = (a+\omega)^{-1}+1$ and $a \neq 0,\omega,\omega^2$, $\{(\omega,\omega+a),(\omega+a,\omega)\}$.
(16) if $\mathrm{Tr}\left(\frac{a+\omega}{a(\omega^2+a)}\right) = 0, a \neq 0,\omega,\omega^2$ and $b^2a(a+\omega)+ba(a+\omega^2)+\omega^2 = 0$, we have $\{(\omega,\frac{1}{b+1}),(\frac{1}{b+1},\omega),(\omega+a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,\omega+a)\}$.

(17) if $\frac{1}{ab} = r^2 + r$ (that is $\mathrm{Tr}(\frac{1}{ab}) = 0$), $b + ab + a \neq 0$, $b\omega^2 + ab\omega + a \neq 0$ and $y = ra$, we have $\{(\frac{y}{by+1}, y), (y, \frac{y}{by+1})\}$ Moreover $ra, (r+1)a \neq 0, 1, \omega, a, a+1, a+\omega$.

Now we start analysing the possible solutions for different values of a and b in $\mathbb{F}_{2^n}^{\star}$.

- If $a = 1$ we have
  case (1) with $b = \omega^2$,
  case (4) with $b = 1$,
  case (9) with $b = \omega$,
  case (15) with $b = \omega^2$,
  case (17) if $\mathrm{Tr}(b^{-1}) = 0$, $b \neq 1$.
  Therefore if $a = 1$ we have at most 4 solutions. We do not have to consider case (1), (4) and (9) any more.
- If $a = \omega$ we have
  case (2) with $b = \omega^2$,
  case (5) with $b = 1$,
  case (8) with $b = \omega$,
  case (13) with $b = 1$,
  case (17) if $\mathrm{Tr}((\omega b)^{-1}) = 0$, $b \neq \omega + 1$.
  Therefore for $a = \omega$ we have at most 4 solutions. We do not have to consider case (2), (5) and (8) any more.
- If $a = \omega^2$ we have
  case (3) with $b = \omega^2$,
  case (6) with $b = 1$,
  case (7) with $b = \omega$,
  case (12) with $b = \omega$,
  case (17) if $\mathrm{Tr}(\omega b^{-1}) = 0$, $b \neq \omega$.
  Therefore for $a = \omega^2$ we have at most 4 solutions. We do not have to consider case (3), (6) and (12) any more.
- If $ab = 1$ and $a \notin \mathbb{F}_4$ we have
  case (7) since the condition is satisfied,
  case (17) with $r = \omega$ is satisfied.
  Therefore for $ab = 1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (7) any more.
- If $ab = \omega$ and $a \notin \mathbb{F}_4$ we have
  case (11) since the condition is satisfied,
  Therefore for $ab = \omega$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not need to consider (11) any more.
- If $ab = \omega^2$ and $a \notin \mathbb{F}_4$ we have
  case (10) since the condition is satisfied,
  Therefore for $ab = \omega^2$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider (10) any more.
- If $b = (a+1)^{-1} + \omega^2$ and $a \notin \mathbb{F}_4$ we have
  case (13) since the condition is satisfied,
  case (17) if $\mathrm{Tr}((ab)^{-1}) = 0$.
  Therefore for $b = (a+1)^{-1} + \omega + 1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider (13) any more.
- If $b = (a+\omega)^{-1} + 1$ and $a \notin \mathbb{F}_4$ we have
  case (15) since the condition is satisfied,
  case (17) if $\mathrm{Tr}((ab)^{-1}) = 0$.

Therefore for $b=(a+\omega)^{-1}+1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (15) any more.
The last cases that we have to consider are
case (14) if $b^2 a\omega(a+1)+ba(a+\omega^2)+\omega^2=0$,
case (16) if $b^2 a(a+\omega)+ba(a+\omega^2)+\omega^2=0$,
case (17) if $\mathrm{Tr}((ab)^{-1})=0$.
Note that, considering $a \notin \mathbb{F}_4$, the trace conditions in (14) and (16) are equivalent to having solutions for the above equations. So, we will analyze if these equations can be satisfied.
We have that case (14) and (16) cannot happen at the same time since $b^2 a\omega(a+1)=b^2 a(a+\omega)$ cannot be satisfied.
Therefore if $b^2 a\omega(a+1)+ba(a+\omega^2)+\omega^2=0$ or $b^2 a(a+\omega)+ba(a+\omega^2)+\omega^2=0$ we have at most 6 solutions. We will show that there exist a,b satisfying condition (17) and one between (14) and (16).
Let $Tr_0=\{x : \mathrm{Tr}(x)=0\}$ and $k=\frac{1}{ab}$. Then from case (14) and (16) we can obtain the relations:
(a) $a^2k\omega+a(k^2+k+\omega)+\omega^2=0$;
(b) $a^2k\omega+a(k^2+k+\omega^2)+\omega^2=0$.
For any fixed k the equations (a) and (b) admits solutions if and only if

$$\begin{aligned}
0 =&\mathrm{Tr}\left(\frac{k}{(k^2+k+\omega)^2}\right)=\mathrm{Tr}\left(\frac{k^2+\omega}{(k^2+k+\omega)^2}+\frac{1}{k^2+k+\omega}\right)\\
=&\mathrm{Tr}\left(\frac{k+\omega^2}{k^2+k+\omega}+\frac{1}{k^2+k+\omega}\right)=\mathrm{Tr}\left(\frac{k+\omega}{k^2+k+\omega}\right)\\
=&\mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega}+1\right)=\mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega}\right)
\end{aligned} \tag{10}$$

and

$$\begin{aligned}
0 =&\mathrm{Tr}\left(\frac{k}{(k^2+k+\omega^2)^2}\right)=\mathrm{Tr}\left(\frac{k^2+\omega^2}{(k^2+k+\omega^2)^2}+\frac{1}{k^2+k+\omega^2}\right)\\
=&\mathrm{Tr}\left(\frac{k+\omega}{k^2+k+\omega^2}+\frac{1}{k^2+k+\omega^2}\right)=\mathrm{Tr}\left(\frac{k+\omega^2}{k^2+k+\omega^2}\right)\\
=&\mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega^2}+1\right)=\mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega^2}\right)
\end{aligned} \tag{11}$$

Since, we want to exclude cases already studied, we have $k\neq 0,1$ (so $b\neq a^{-1}$) and it is easy to check that from (a) and (b) with this restriction we also have $a\notin\mathbb{F}_4$.
Suppose that for any $k\in Tr_0\setminus\{0,1\}$ the conditions (10) and (11) are not satisfied. Thus, since $k+1\in Tr_0\setminus\{0,1\}$ for any $k\in Tr_0\setminus\{0,1\}$ we have that

$$1=\mathrm{Tr}\left(\frac{k^2+1}{k^2+k+\omega}\right)=\mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega}\right)+\mathrm{Tr}\left(\frac{1}{k^2+k+\omega}\right)=1+\mathrm{Tr}\left(\frac{1}{k^2+k+\omega}\right)$$

and

$$1=\mathrm{Tr}\left(\frac{k^2+1}{k^2+k+\omega^2}\right)=1+\mathrm{Tr}\left(\frac{1}{k^2+k+\omega^2}\right).$$

So, denoting by $S=\{k^2+k : k\in Tr_0\}$ we have that for all $s\in S\setminus\{0\}$

$$\mathrm{Tr}\left(\frac{1}{s+\omega}\right)=\mathrm{Tr}\left(\frac{1}{s+\omega^2}\right)=0.$$

Now, since $\mathrm{Tr}(\omega)=\mathrm{Tr}(\omega^2)=1$ and $1\notin S$, we have that $Tr_1=\{x : \mathrm{Tr}(x)=1\}=(\omega+S)\cup(\omega^2+S)$, where $\omega^i+S=\{\omega^i+s : s\in S\}$.
This means that the inverse function $I(x)=x^{-1}$ maps $Tr_1\setminus\{\omega,\omega^2\}$ onto $Tr_0\setminus\{0,1\}$, and thus $I(Tr_1\setminus\{\omega,\omega^2\})=Tr_0\setminus\{0,1\}$.
Define the map

$$G(x)=\begin{cases}x+\omega & \text{if } x\in\mathbb{F}_4\\ x^{-1} & \text{if } x\notin\mathbb{F}_4.\end{cases}$$

Then, $G(Tr_1)=Tr_0$, so considering $H(x)=G^{-1}(x)+\omega$ we would obtain $H(Tr_0)=Tr_0$ and also $H(0)=0$. Thus, H is such that there exists a vector space of dimension $n-1$ which is sent to another vector space of dimension $n-1$. From Proposition 5.3 in [1] we have that this is equivalent to $\mathscr{NL}(H)=0$. However, H is CCZ-equivalent to the function G which coincides with the inverse function except over the set $U=\mathbb{F}_4$. Then, it is easy to check that for any $\alpha,\beta\in\mathbb{F}_{2^n}$ we have

$$|\mathscr{W}_G(\alpha,\beta)|\le|\mathscr{W}_I(\alpha,\beta)|+2\cdot|U|,$$

implying that $\mathscr{NL}(G)\ge\mathscr{NL}(I)-|U|=2^{n-1}-2^{n/2}-4>0$ since $n\ge 6$. So we obtain a contradiction. Therefore, there should exist a,b with $b\neq a^{-1}$, $a\notin\mathbb{F}_4$ such that case (17) and one between case (14) and case (16) are satisfied.

For all the other cases we have at most 2 solutions. □

From Theorem 2 and Theorem 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

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

(ii) if $0\notin\pi$, then
  (a) if $\frac{\alpha_2}{\alpha_1}\notin\mathbb{F}_4^\star$, then

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

  (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 $\beta_1=\frac{\alpha_2}{\alpha_1}$, 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 [16], the authors extend the results obtained in [22] modifying the inverse function with cycles of order greaten than two. In particular from their results we have the following differentially 4-uniform functions.

Lemma 6 *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 (we give some steps of the proof in the appendix).

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,*

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

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,*

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

With same arguments as in 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,*

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

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 [6] and the boomerang uniformity for some of the functions studied in [16, 22].

From the results in [15, 17] 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 [14]. So it would be interesting to construct optimal functions with degree greater than two and which are, in particular, 4-uniform.

In [5], 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 ([5, 15, 17]) 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 $n \equiv 0 \mod 4$.

References

1. Aragona, R., Calderini, M., Tortora, A., Tota, M.: *Primitivity of PRESENT and other lightweight ciphers*. Journal of Algebra and Its Applications, 17 (2018), 1850115, 16pp.
2. Biham, E., Dunkelman, O., Keller, N.: New results on boomerang and rectangle attacks. FSE 2002, ser. Lect. Notes Comput. Sci **2365**, 1–16 (2002)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology **4**(1), 3–72 (1991)
4. Biryukov, A., De Cannière, C., Dellkrantz, G.: Cryptanalysis of SAFER++. CRYPTO 2003, ser. Lect. Notes Comput. Sci **2729**, 195–211(2003)
5. Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic Sboxes. IACR Transactions on Symmetric Cryptology **2018**(3), 290–310 (2018)
6. 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)
7. Bracken, C., Tan, C.H., Tan, Y.: Binomial differentially 4-uniform permutations with high nonlinearity. Finite Fields Appl. **18**(3), 537–546 (2012)
8. 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)
9. Calderini, M.: On the EA-classes of known APN functions in small dimensions, IACR Cryptology ePrint Archive 2019: 369 - `https://eprint.iacr.org/2019/369` (2019)
10. 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)
11. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.) IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
12. 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)
13. 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)
14. Knudsen, L.: Truncated and higher order differentials. FSE 1994, ser. Lect. Notes Comput. Sci **1008**, 196–211 (1995)
15. 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).
16. 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)
17. Mesnager, S., Chunming, T., Maosheng, X.: On the boomerang uniformity of (quadratic) permutations over F_{2^n}. arXiv preprint arXiv:1903.00501 - `https://arxiv.org/pdf/1903.00501.pdf` (2019).
18. Nyberg, N.: Differentially uniform mappings for cryptography. EUROCRYPT'93, ser. Lect. Notes Comput. Sci **765**, 55–64 (1994)
19. 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)
20. Tang, D., Carlet, C., Tang, X.: Differentially 4-uniform bijections by permuting the inverse function. Des. Codes. Cryptogr. **77**, 117–141 (2014)
21. Wagner, D.: The boomerang attack. FSE'99, ser. Lect. Notes Comput. Sci **1636**, 156–170 (1999)
22. Yu, Y., Wang, M., Li, Y.: Constructing differentially 4 uniform permutations from known ones. Chin. J. Electron. **22**(3), 495–499 (2013)
23. Zha, Z., Hu, L., Sun, S.: Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields Appl. **25**, 64–78 (2014)

A Appendix

Proof (Proof of Theorem 4) Performing a similar analysis as in Theorem 3 we will obtain that, up to swap x and y, and adding $+a$ to both terms, we have the following list of possible solutions:

(1) $\{(0,1),(1,0),(a,a+1),(a+1,a)\}$ with $a=1,c,c^2$ and $b=c$,
(2) $\{(0,c),(c,0),(a,a+c),(a+c,a)\}$ with $a=1,c,c^2$ and $b=1$,
(3) $\{(0,a),(a,0)\}$ with $a\neq 1,c$ and $b=a^{-1}+1$,
(4) $\{(0,c^2),(c^2,0),(1,c),(c,1)\}$ with $a=1,c,c^2$ and $b=c^2$,
(5) $\{(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)\}$ with $a^2b^2+ab(a+1)+1=0$ and $a\neq 1,c,c^2$,
(6) $\{(1,a+1),(a+1,1)\}$ with $a\neq 1,c^2$ and $b=(a+1)^{-1}+c^2$,
(7) $\{(1,\frac{1}{b+c^2}),(\frac{1}{b+c^2},1),(1+a,\frac{1}{b+c^2}+a),(\frac{1}{b+c^2}+a,1+a)\}$ with $ab^2(a+1)+ab(ac^2+c)+c=0$ and $a\neq 1,c,c^2$,
(8) $\{(c,a+c),(a+c,c)\}$ with $a\neq c,c^2$ and $b=(a+c)^{-1}$,
(9) $\{(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)\}$ with $ab^2(a+c)+ab+1$ and $a\neq 1,c,c^2$,
(10) $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ with $by^2+aby+a=0$ and $\mathrm{Tr}(\frac{1}{ab})$=0.

It is easy to verify that if $a=1,c,c^2$ then for any fixed b there are at most 4 different solutions. For example for $a=1$ we consider case (1), (2), (4), (8), (10). When $b=1$ we have $(0,c),(c,0),(1,c^2),(c^2,1)$ from (2). When $b=c$ we have $(0,1),(1,0)$ from 1 and $(c,c^2),(c^2,c)$ from (8). When $b=c^2$ we have $(0,c^2),(c^2,0)(1,c),(c,1)$ from 4. Otherwise when $\mathrm{Tr}(\frac{1}{b})$=0 we have two solutions from (10).

Hence we just need to focus on condition (3), (5), (6), (7), (8), (9) and (10) for $a\neq 1,c,c^2$.

(I) If $b=a^{-1}+1$ then we have
case (3) We have 2 solutions: $(0,a),(a,0)$.
case (7) leads to $a^3c=a+1$, and 4 solutions: $(1,\frac{1}{b+c^2}),(\frac{1}{b+c^2},1),(1+a,\frac{1}{b+c^2}+a),(\frac{1}{b+c^2}+a,1+a)$
case (9) leads to $a^3=a^2c^2+a+c$, and 4 solutions: $(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)$
case (10) is possible if $\mathrm{Tr}(\frac{1}{a+1})$=0, and we have 2 solutions: $(\frac{y}{by+1},y),(y,\frac{y}{by+1})$.

For case (7), we have that $a=c^2$ is a solution of the $a^3c+a+1=0$. In particular we have $a^3c+a+1=(a+c^2)(a^2c+a+c)=0$. Hence no proper solutions are possible. For case (9), considering $a^3=a^2c^2+a+c$, we obtain $a^{2^6}=a$. Since $a\neq 0,1$, it admits solution only if $3|k$. Therefore if $3\nmid k$ we have at most 4 solutions. In the other cases we can have exactly 8 solutions. Indeed, let $k=3m$ and $\mathbb{F}_{2^3}^{\star}=\langle w\rangle$, then $a=w^{13}$ satisfies the relation in 11. Moreover, we have $a+1=w^3$ and $\frac{1}{a+1}=w^{60}$. Therefore, $\mathrm{Tr}(\frac{1}{a+1})$=$\mathrm{Tr}(w^{60})$=$\mathrm{Tr}(w^{15})$=$\mathrm{Tr}(w^7+w^{14})=0$ and we can have exactly 6 solutions from (9) and (10), plus the solutions from (3) we have in total 8 solutions.

(II) If $b=(a+1)^{-1}+c^2$ then we have
case (5) leads to $a^4+a^3c+a^2+ac^2=0$, and 4 solutions: $(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)$.
case (6), we have 2 solutions: $(1,a+1),(a+1,1)$.
case (9) leads to $a^4c+a^2(c^2)+a(c^2)+1=0$ and 4 solutions: $(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)$.
case (10) is possible if $\mathrm{Tr}(\frac{1}{ab})$=0, and we have 2 solutions: $(\frac{y}{by+1},y),(y,\frac{y}{by+1})$.

For case (5), we have that if $a^4=a^3c+a^2+ac+1$ then $a^{2^8}=a$. Since $a\neq 0,1$ then we do not have possible solutions. The same for case (9). Indeed, if $a^4c=a^2c^2+ac^2+1$ then $a^{2^8}=a$. Therefore we have at most 4 solutions.

(III) If $b=(a+c)^{-1}$ then we have
case (5) leads to $a^3+a^2(c^2)+ac+c^2$, and 4 solutions: $(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)$,
case (8), we have 2 solutions: $(c,a+c),(a+c,c)$.
case (10) is possible if $\mathrm{Tr}(\frac{1}{ab})$=0, and we have 2 solutions: $(\frac{y}{by+1},y),(y,\frac{y}{by+1})$.

For case (5) we have that if $a^3=a^2c^2+ac+c^2$ then $a^{2^6}=a$. Therefore we have solutions only if $3|k$. In this case we have at most 8 solutions.

Now we are left with case (5), (7), (9) and (10).

– If condition (5) and (7) are both satisfied, then we have the following constrain on a:

$$a^4=a^3+a^2c+c^2.$$

If we now compute the 2-powers of a we notice that $a^{2^8}=a$, hence $a\in\mathbb{F}_{2^8}$. This is not possible since $a\in\mathbb{F}_{2^{2k}}$ with k odd and $a\notin\mathbb{F}_{2^2}$.

– If case (5) and (9) are both satisfied, then we obtain

$$bc=a \text{ and } b^4=b^3+b^2(c^2)+c.$$

Using the same technique we can verify that $b^{2^8}=b$, hence we get a contradiction.

- If case (7) and (9) are both satisfied then we obtain

$$a^4 = a^3(c^2) + a^2c + c.$$

Again $a^{2^8} = a$, hence a contradiction.

Therefore at most we can have 4 solutions coming from one of these three cases, plus two solutions from (12). Thus, at most 6 solutions.

Assume now case (5). Therefore we have the condition $\mathrm{Tr}(\frac{1}{a+1})$=0. Assume then, $\frac{1}{a+1} = r^2 + r$ for some r. Hence, $b = r^2 \frac{a+1}{a}$ or $b = (r^2+1)\frac{a+1}{a}$. Let us consider the first case, for case (10) we should have:

$$\frac{1}{ab} = \frac{1}{r^2(a+1)} = \frac{1}{r^2}(r^2+r) = 1 + \frac{1}{r}$$
$$\mathrm{Tr}\left(\frac{1}{ab}\right) = \mathrm{Tr}\left(1 + \frac{1}{r^2}\right) = \mathrm{Tr}\left(\frac{1}{r}\right).$$

Then, we just need to consider an element $r \neq 0$ with inverse of null trace and consider $a = \frac{1}{r^2+r} + 1$ and $b = r^2 \frac{a+1}{a}$. So, we will obtain 6 possible solutions. In order to avoid the three cases previously analysed, we just need to consider $r \neq 1$, $r^4 + r^2c + rc + c^2 \neq 0$ and $r^3c + r^2c^2 + r + 1 \neq 0$. Moreover, due to the restrictions on a, we have $r^2 + r \neq 1, c, c^2$. Since $n \geq 6$ there exists such an element r in $\mathbb{F}_{2^n}$. ◻

Proof (Proof of Theorem 5) Consider now $\pi = (1, c, c^2)$ with $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and the function

$$F(x) = \begin{cases} c^2 & \text{if } x = 1, \\ c & \text{if } x = c, \\ 1 & \text{if } x = c^2, \\ x^{-1} & \text{otherwise.} \end{cases}$$

Performing a similar analysis as in Theorem 3 we will obtain that, up to swap and adding a to both terms, we have the following list of possible solutions:

(1) $\{(0,1),(1,0),(c,c^2),(c^2,c)\}$ with $a = 1, c, c^2$ and $b = c^2$,
(2) $\{(0,c),(c,0),(1,c^2),(c^2,1)\}$ with $a = 1, c, c^2$ and $b = c$,
(3) $\{(0,c^2),(c^2,0),(1,c),(c,1)\}$ with $a = 1, c, c^2$ and $b = 1$,
(4) $\{(0,a),(a,0)\}$ with $a \notin \mathbb{F}_4$ and $b = a^{-1}$,
(5) $\{(0,ac),(ac,0),(a,ac+a),(ac+a,a)\}$ with $a \notin \mathbb{F}_4$ and $b = a^{-1}c^2$,
(6) $\{(0,ac+a),(ac+a,0),(a,ac),(ac,a)\}$ with $a \notin \mathbb{F}_4$ and $b = a^{-1}c$,
(7) $\{(1,a+1),(a+1,1)\}$ with $a \notin \mathbb{F}_4$ and $b = c^2 + (a+1)^{-1}$,
(8) $\{(1,(b+c^2)^{-1}),((b+c^2)^{-1},1),(1+a,(b+c^2)^{-1}+a),((b+c^2)^{-1}+a,1+a)\}$ with $a \notin \mathbb{F}_4$ and $b^2(a^2+a) + b(ac+a^2c^2) + c = 0$,
(9) $\{(c,a+c),(a+c,c)$ with $a \notin \mathbb{F}_4$ and $b = c + (a+c)^{-1}$,
(10) $\{(c,(b+c)^{-1}),((b+c)^{-1},c),(c+a,(b+c)^{-1})+a,((b+c)^{-1}+a,c+a)\}$ with $a \notin \mathbb{F}_4$ and $b^2(a^2+ac) + b(ac+a^2c) + c = 0$,
(11) $\{(c^2,a+c^2),(a+c^2,c^2)\}$ with $a \notin \mathbb{F}_4$ and $b = 1 + (a+c^2)^{-1}$,
(12) $\{(c^2,(b+1)^{-1}),((b+1)^{-1},c^2),(a+c^2,a+(b+1)^{-1}),(a+(b+1)^{-1},a+c^2)\}$ with $a \notin \mathbb{F}_4$ and $b^2(a^2+ac^2) + b(a^2+ac) + c = 0$,
(13) $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ with $by^2 + aby + a = 0$, $\frac{y}{by+1}, y \notin \mathbb{F}_4, a + \mathbb{F}_4$, hence $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$.

It is easy to verify that for $a = 1, c, c^2$, for any fixed b, we have at most 4 different solutions. For example for $a = 1$ we consider solutions from 1,2,3,13. When $b = 1$ we have $(0,c^2),(c^2,0),(1,c),(c,1)$ from 3, and none from 13. When $b = c$ we have $(0,c),(c,0),(1,c^2),(c^2,1)$ from 2 and none from 13. When $b = c^2$ we have $(0,1),(1,0),(c,c^2),(c^2,c)$ from 1 and none from 16. When $b \notin \mathbb{F}_4$ and $\mathrm{Tr}\left(\frac{1}{b}\right) = 0$ then we have at most 2 solutions from 13.

Hence we just need to focus on case (4), (5), (6), (7), (8), (9), (10), (11), (12), (13).

- If $b = a^{-1}$ then we have
  case (4), $(0,a)$, $(a,0)$,
  case (13), $\left(\frac{y}{a^{-1}y+1}, y\right)$, $\left(y, \frac{y}{a^{-1}y+1}\right)$,
  hence we have 4 solutions.
- If $b = a^{-1}c^2$ then we have
  case (5), $(0,ac)$, $(ac,0)$, (a,ac^2), (ac^2,a),
  hence 4 solutions.
- If $b = a^{-1}c$ then we have
  case (6), $(0,ac^2)$, $(ac^2,0)$, (a,ac), (ac,a),

hence 4 solutions.

- If $b = c^2 + (a+1)^{-1}$ then we have
  case (7), $(1, a+1)$, $(a+1, 1)$,
  case (10) is possible if $a^3c + a^2c^2 + a + c^2 = 0$, that implies $a^{64} = a$. Hence only possible when k is multiple of 3, and in this case we have 4 solutions,
  case (13), $\left(\frac{y}{by+1}, y\right)$, $\left(y, \frac{y}{by+1}\right)$ if $\mathrm{Tr}\left(\frac{1}{ab}\right)$=0,

  hence at most 4 solutions.
- If $b = c + (a+c)^{-1}$ then we have
  case (9), $(c, a+c)$, $(a+c, c)$,
  case (8) is possible if $a^3 = a^2 + 1$, that implies $a^8 = a$. Hence only possible when k is a multiple of 3, and in this case we have 4 solutions,
  case (12) is possible if $a^3 = a^2c^2 + ac + c$, that implies $a^{64} = a^{2^6} = a$. Hence only possible when k is multiple of 3, and in this case we have 4 solutions,
  case (13) is possible if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, two solutions.

  It is trivial that both case (8) and (12) cannot be verified. Therefore if k is not a multiple of 3 we have at most 4 solutions. Otherwise we have at most 8 solutions.
- If $b = 1 + (a+c^2)^2$ we have
  case (11), $(c^2, a+c^2)$, $(a+c^2, c^2)$,
  case (8) is possible if $a^3 = a^2 + a + c$, that implies $a^{64} = a$. Hence only if k is multiple of 3 we can have at most 4 solutions,
  case (10) is possible if $a^4 = a^3c^2 + a^2c + a + 1$, that implies $a^{64} = a$. Again we have 4 solutions only of k is multiple of 3,
  case (13) is possible if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, two solutions.

  Again, both (8) and (10) cannot be satisfied. Therefore when k is not a multiple of 3 we have at most 4 solutions, otherwise we have at most 8 solutions.
  Hence, we are now left to consider case (8), (10), (12), (13).
- If (8) and (10) are satisfied, then we obtain $b = ac$ and $a^3 = a^2c + ac^2 + c^2$. Then $a^{64} = a$, and it is possible only if k is multiple of 3.
- If (8) and (12) are satisfied, then $b = a$ and $a^3 = a^2 + a + c$. This leads to $a^{64} = a$, hence it is possible only if k is multiple of 3.
- If (10) and (12) are satisfied, then $b = ac^2$ and $a^3 + c^2a^2 + ac + c^2 = 0$. So, $a^{64} = a$, and it is possible only if k is multiple of 3.

Therefore we have that if k is not a multiple of 3 that we can have at most 6 solutions (4 from one among (8), (10), (12) and 2 from (13)). If k is a multiple of 3 that we can have at most 10 solutions.

Let $\mathbb{F}_{2^6}^\star = \langle w \rangle$. For the case when (8) and (10) are satisfied we have $b = ac$ and w^{46}, w^{58}, w^{43} are the solutions of $a^3 = a^2c + ac^2 + c^2$. However, for these values $\mathrm{Tr}(\frac{1}{ab}) = 1$, and so condition (13) is not satisfied.
Similar, when (8) and (12) are satisfied we have $b = a$ and w, w^4, w^{16} are solutions of $a^3 = a^2 + a + c$. Hence a must assume one of these values. But since $\mathrm{Tr}\left(\frac{1}{w}\right) = 1$ we have that case (13) is not possible.
Also for the last case we have $b = ac^2$ and the solutions of $a^3 + c^2a^2 + ac + c^2 = 0$ are w^{22}, w^{25}, w^{37}. For all these cases $\mathrm{Tr}(\frac{1}{ab}) = 1$, implying that (13) cannot happen.
Therefore for k multiple of 3 we have 8 solutions.

Now, as for the the last part of Theorem 3 we will show that if $3 \nmid n$ we have exactly 6 solutions. Then, let $k = \frac{1}{ab}$ of null trace, as in Theorem 3 we consider $k \neq 0, 1$. From condition (8), (10) and (12) we would obtain

(a) $a^2kc + a(k^2 + k + c^2) + c^2 = 0$;
(b) $a^2kc^2 + a(k^2 + k + c^2) + 1 = 0$;
(c) $a^2kc^2 + a(k^2 + k + c^2) + c = 0$.

For (a) and (c) we can have solutions if and only if

$$\begin{aligned}
0 =& \mathrm{Tr}\left(\frac{k}{(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k^2+c^2}{(k^2+k+c^2)^2} + \frac{1}{k^2+k+c^2}\right) \\
=& \mathrm{Tr}\left(\frac{k+c}{k^2+k+c^2} + \frac{1}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{k+c^2}{k^2+k+c^2}\right) \\
=& \mathrm{Tr}\left(\frac{k^2}{k^2+k+c^2} + 1\right) = \mathrm{Tr}\left(\frac{k^2}{k^2+k+c^2}\right)
\end{aligned} \tag{12}$$

and for (b)

$$\begin{aligned}
0 =&\mathrm{Tr}\left(\frac{kc^2}{(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k}{c(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k^2+c^2}{c(k^2+k+c^2)^2}+\frac{1}{c(k^2+k+c^2)}\right)\\
=&\mathrm{Tr}\left(\frac{k+c}{c^2(k^2+k+c^2)}+\frac{1}{c(k^2+k+c^2)}\right) = \mathrm{Tr}\left(\frac{k}{c^2(k^2+k+c^2)}\right)\\
=&\mathrm{Tr}\left(\frac{kc}{k^2+k+c^2}\right) \qquad (13)
\end{aligned}$$

Suppose by contradiction, that for any $k \in Tr_0 \setminus \{0,1\}$ (12) and (13) cannot happen. Then

$$\mathrm{Tr}\left(\frac{k}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{kc}{k^2+k+c^2}\right) = 1,$$

for any k. Since $k+1 \in Tr_0 \setminus \{0,1\}$ for all $k \in Tr_0 \setminus \{0,1\}$, we obtain

$$\mathrm{Tr}\left(\frac{1}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{c}{k^2+k+c^2}\right) = 0,$$

for any $k \in Tr_0 \setminus \{0,1\}$. Now, let $S = \{k^2+k : \mathrm{Tr}(k) = 0\}$. As above, $Tr_1 = (c+S) \cup (c^2+S)$. Now, $\frac{k^2+k+c^2}{c} = c^2s+c$, with $s \in S$, and we have that $c^2S = S$. Indeed, since any $k \in Tr_0$ can be written as $k = d^2+d$ for some $d \in \mathbb{F}_{2^n}$ we have that $S = \{d^4+d : d \in \mathbb{F}_{2^n}\}$. So,

$$c^2s = c^2(d^4+d) = (c^2d)^4 + c^2d = [(c^2d)^2+c^2d]^2 + \underbrace{(c^2d)^2+c^2d}_{\in Tr_0} \in S.$$

Therefore, $c+c^2S = c+S$ implying that all the elements in $Tr_1 \setminus \{c,c^2\}$ are mapped by the inverse function into $Tr_0 \setminus \{0,1\}$ So, as in Theorem 3 we obtain a contradiction and thus, for some $k \in Tr_0 \setminus \{0,1\}$, there exist a,b satisfying (13) and one among (8), (10) and (12). □