



The second-order zero differential spectra of some functions over finite fields

Kirpa Garg¹ · Sartaj Ul Hasan¹ · Constanza Riera² · Pantelimon Stănică³

Received: 6 June 2024 / Accepted: 10 January 2025

This is a U.S. Government work and not under copyright protection in the US; foreign copyright protection may apply 2025

Abstract

It was shown by Boukerrou et al. [IACR Trans. Symmetric Cryptol. 1 (2020), 331–362] that the F -boomerang uniformity (which is the same as the second-order zero differential uniformity in even characteristic) of perfect nonlinear functions is 0 on \mathbb{F}_{p^n} (p prime) and the one of almost perfect nonlinear functions on \mathbb{F}_{2^n} is 0. It is natural to inquire what happens with APN or other low differential uniform functions in even and odd characteristics. Here, we explicitly determine the second-order zero differential spectra of several maps with low differential uniformity. In particular, we compute the second-order zero differential spectra for some almost perfect nonlinear (APN) functions over finite fields of odd characteristic, pushing further the study started in Boukerrou et al. and continued in Li et al. [Cryptogr. Commun. 14.3 (2022), 653–662], and it turns out that our considered functions also have low second-order zero differential uniformity. Moreover, we study the second-order zero differential spectra of certain functions with low differential uniformity over finite fields of even characteristic. We connect this new concept to the sum-freedom and vanishing flats concepts and find some counts for the number of vanishing flats via our methods. We provide detailed analyses on several equations over finite fields that may have an interest outside of the scope of our paper.

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

✉ Pantelimon Stănică
pstanica@nps.edu

Kirpa Garg
kirpa.garg@gmail.com

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

Constanza Riera
csr@hvl.no

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

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

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

Keywords Finite fields · Almost perfect nonlinear functions · Second-order zero differential spectra · Second-order zero differential uniformity

Mathematics Subject Classification (2010) 12E20 · 11T06 · 94A60

1 Introduction

Let n be a positive integer and p be a prime number. We denote by \mathbb{F}_q the finite field with $q = p^n$ elements, by \mathbb{F}_q^* the multiplicative cyclic group of nonzero elements of \mathbb{F}_q and by $\mathbb{F}_q[X]$ the ring of polynomials in one variable X with coefficients in \mathbb{F}_q . It may be noted that functions over finite fields are very important objects due to their wide range of applications in coding theory and cryptography. For example, in cryptography, these functions are often used in designing what are known as substitution boxes (S-boxes) in modern block ciphers (mostly, for $p = 2$, though there are some proposals in odd characteristic such as GMiMC [1]). One of the most effective attacks on block ciphers is differential cryptanalysis, which was first introduced by Biham and Shamir [2]. The resistance of a function against differential attack is measured in terms of its differential uniformity (DU) – a notion introduced by Nyberg [26]. For a function $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$, and any $a \in \mathbb{F}_q$, the derivative of F in the direction of a is defined as $D_F(X, a) := F(X + a) - F(X)$ for all $X \in \mathbb{F}_q$. For any $a, b \in \mathbb{F}_q$, the Difference Distribution Table (DDT) entry $\delta_F(a, b)$ at point (a, b) is the number of solutions $X \in \mathbb{F}_q$ of the equation $D_F(X, a) = b$. Further, the differential uniformity of F , denoted by δ_F , is given by $\delta_F := \max\{\delta_F(a, b) : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$. We call the function F a perfect nonlinear (PN) function, respectively, an almost perfect nonlinear (APN) function, if $\delta_F = 1$, respectively, $\delta_F = 2$. Blondeau, Canteaut, and Charpin [3] introduced the idea of locally APN power functions as a generalization of the APN-ness property. A power function $F(X)$ over \mathbb{F}_{2^n} is said to be locally-APN if $\max\{\delta_F(1, b) : b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\} = 2$.

The boomerang attack on block ciphers is another important cryptanalysis technique proposed by Wagner [29]. It can be considered as an extension of the classical differential attack. At Eurocrypt 2018, Cid et al. [11] introduced a systematic approach known as the Boomerang Connectivity Table (BCT), to analyze the boomerang style attack. Boura and Canteaut [6] further studied BCT and coined the term “boomerang uniformity”, which is essentially the maximum value of nontrivial entries of the BCT, to quantify the resistance of a function against the boomerang attack. Boukerrou et al. [5] pointed out the need for the counterpart of the BCT by extending the idea to Feistel ciphers. They introduced the Feistel Boomerang Connectivity Table (FBCT) as an extension of BCT for Feistel ciphers, where the S-boxes may not be permutations. It is worth emphasizing that Feistel-based ciphers, such as 3-DES and CLEFIA [27], hold just as much importance in the block cipher designs as SPN ciphers.

The authors in [5] investigated the properties of the FBCT for two classes of functions, namely, APN functions and functions based on the inverse mapping over \mathbb{F}_{2^n} . Also, all the nontrivial coefficients of the FBCT are 0 for APN functions over \mathbb{F}_{2^n} (via [9]) and are 0 and 4 for the inverse function over \mathbb{F}_{2^n} , where n is even. In fact, the coefficients of the FBCT are related to the second-order zero differential spectra of the functions. Another important property of the FBCT (sure, it can be derived from [9]) is that F is an APN function over \mathbb{F}_{2^n} if and only if the FBCT of F is 0 for $a, b \in \mathbb{F}_{2^n}$ with $ab(a + b) \neq 0$. Li et al. [21] further studied the second-order zero differential spectra of the inverse function and some APN functions in odd characteristic. The authors of [21] also show that these functions have

low second-order zero differential uniformity. It is worth mentioning that Mesnager et al. gave an excellent survey on generalized differential and boomerang uniformities in [25]. Moreover, Eddahmani and Mesnager [13] determined the FBCT entries of the inverse, the Gold, and the Bracken-Leander functions over finite fields of even characteristic. Their work also indicates that functions with low differential uniformity such as Bracken-Leander function may not have low second-order zero differential uniformity or F -boomerang uniformity. This suggests that, though in some cases (for instance APN in even characteristic, and PN in odd characteristic, as commented above), the coefficients of the FBCT are linked to the DU, this is not the case in general, and therefore, the FBCT is a truly independent measure of the strength of a function, from a cryptographic perspective. That is, low differential uniformity may not be enough, rather one has to combine it with many other criteria, including the F -boomerang uniformity. This motivates us further to investigate the second-order zero differential uniformity of functions that have low differential uniformity. It might seem like an unconnected list of functions, but our goal is to go through some of the known classes of functions with low differential uniformity and distinguish them via the F -boomerang uniformity and the FBCT.

Recently, Garg et al. [14] and Man et al. [23, 24] studied the second-order zero differential uniformity of several classes of functions over finite fields with low differential uniformity. We further extend their work by investigating the second-order zero differential spectra of some more classes of functions with low differential uniformity. In addition, these functions have low second-order zero differential uniformity. The paper is organized as follows. In Section 2, we recall some definitions. A connection between the FBCT, sum-freedom, and vanishing flats is established in Section 3. The second-order zero differential spectrum of four power functions over finite fields of odd characteristic is considered in Section 4. Further, in Section 5, the second-order zero differential spectrum and the number of vanishing flats of some power functions over finite fields of even characteristic are investigated. Section 6 deals with second-order zero differential spectrum of two non-monomial permutations with low differential uniformity over finite field of even characteristic. Finally, we conclude the paper in Section 7. The techniques involve dealing with some delicate equations and systems of equations over finite fields and that may be of independent interest.

2 Preliminaries

In this section, we recall some definitions.

Definition 2.1 [5, 21] For $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$, positive integer n , p an arbitrary prime, and $a, b \in \mathbb{F}_q$, the *second-order zero differential spectra* of F with respect to a, b is defined as

$$\nabla_F(a, b) := \#\{X \in \mathbb{F}_q : F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0\}.$$

If $q = 2^n$, we call $\nabla_F = \max\{\nabla_F(a, b) : a \neq b, a, b \in \mathbb{F}_{2^n} \setminus \{0\}\}$ the second-order zero differential uniformity of F . If $q = p^n$, $p > 2$, we call $\nabla_F = \max\{\nabla_F(a, b) : a, b \in \mathbb{F}_{p^n} \setminus \{0\}\}$ the second-order zero differential uniformity of F .

Definition 2.2 (Feistel Boomerang Connectivity Table) [5] Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. The *Feistel Boomerang Connectivity Table (FBCT)* of F is given by a $2^n \times 2^n$ table, in which the entry for the (a, b) position is given by

$$\text{FBCT}_F(a, b) = \#\{X \in \mathbb{F}_{2^n} : F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0\}.$$

Definition 2.3 (*F*-Boomerang Uniformity) [5, 21] The *F*-Boomerang uniformity corresponds to the highest value in the FBCT without considering the first row, the first column and the diagonal, that is,

$$\beta_F = \max_{a \neq 0, b \neq 0, a \neq b} \text{FBCT}_F(a, b).$$

Note that, when $p = 2$, then $\nabla_F(a, b) = \text{FBCT}_F(a, b)$, and thus the coefficients of the FBCT are exactly the second-order zero differential spectra of functions over \mathbb{F}_{2^n} , and that the *F*-Boomerang uniformity is in fact the second-order zero differential uniformity of *F* in even characteristic.

Definition 2.4 The Kloosterman sum $K(1)$ in the field \mathbb{F}_{2^n} is defined by:

$$K(1) = \sum_{X \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(X^{-1}+X)}$$

with the convention that $(-1)^{\text{Tr}(X^{-1})} = 1$ for $X = 0$. Carlitz [8] gives the following explicit expression of this sum, namely,

$$K(1) = 1 + \frac{(-1)^{n-1}}{2^{n-1}} \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^i \binom{n}{2i} 7^i.$$

We now present some lemmas that will be needed in the subsequent sections.

Lemma 2.5 [5] *Let $n \geq 1$ be an even integer. Let ω and $\omega + 1$ be the solutions of the equation $X^2 + X + 1$ in \mathbb{F}_{2^n} . Let F be the inverse function defined over \mathbb{F}_{2^n} by $F(0) = 0$ and $F(X) = \frac{1}{X}$ for $X \neq 0$. The FBCT of F satisfies*

$$\nabla_F(a, b) = \begin{cases} 0 & \text{if } a \neq 0, b \neq 0, a \neq b \text{ and } a \notin \{b\omega, b(\omega + 1)\} \\ 4 & \text{if } a \neq 0, b \neq 0, a \neq b \text{ and } a \in \{b\omega, b(\omega + 1)\} \\ 2^n & \text{if } ab = 0 \text{ or } a = b. \end{cases}$$

Moreover, $X \in \{0, a, b, a + b\}$ are the four solutions in the above system.

Lemma 2.6 [5] *Let $n \geq 1$ be an odd integer. Let F be the inverse function defined over \mathbb{F}_{2^n} by $F(0) = 0$ and $F(X) = \frac{1}{X}$ for $X \neq 0$. The FBCT of F satisfies*

$$\nabla_F(a, b) = \begin{cases} 0 & \text{if } a \neq 0, b \neq 0, a \neq b \\ 2^n & \text{if } ab = 0 \text{ or } a = b. \end{cases}$$

Recall that for p an odd prime, n a positive integer, and $q = p^n$, we let η be the quadratic character of \mathbb{F}_q defined by $\eta(X) = 1$, respectively, -1 , if X is a square, respectively, a non-square in \mathbb{F}_q^* (we let $\eta(0) = 0$). We use $\#A$ for the cardinality of a set A . As customary, we shall use the convention that for any nonzero $a \in \mathbb{F}_{2^n}$, $a^{-1} := \frac{1}{a}$ and $0^{-1} := 0$, when needed.

3 A connection between vanishing flats, sum-freedom, an alternative definition of APNness for p odd, and the FBCT

In [20], the concept of *vanishing flats* was introduced in the following way. For $n \geq 2$, we define the set of all 2-dimensional flats in $\mathbb{F}_{2^n}^n$ as

$$\mathcal{P}_n = \{\{X_1, X_2, X_3, X_4\} \mid X_1 + X_2 + X_3 + X_4 = 0 \text{ and } X_1, X_2, X_3, X_4 \in \mathbb{F}_{2^n} \text{ are distinct}\}.$$

Conventionally, each subset in \mathcal{P}_n is called a *block*. For a function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, we define the set of *vanishing flats* with respect to F as

$$\mathcal{VP}_{n,F} = \{ \{X_1, X_2, X_3, X_4\} \in \mathcal{P}_n \mid F(X_1) + F(X_2) + F(X_3) + F(X_4) = 0 \}.$$

Clearly, given $\{X_1, X_2, X_3, X_4\} \in \mathcal{VP}_{n,F}$, we can always write $X_2 = X_1 + a$, $X_3 = X_1 + b$, $X_4 = X_1 + X_2 + X_3 = X_1 + a + b$ for some $a, b \in \mathbb{F}_{2^n}$, and X_1 satisfies then the equation $F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0$. However, X_2, X_3, X_4 are also solutions of the equation, while the sets in the vanishing flats are unordered. Obviously, $\text{FBCT}_F(a, a) = 2^n$, and $\text{FBCT}_F(a, b) = \text{FBCT}_F(b, a) = \text{FBCT}_F(a + b, a) = \text{FBCT}_F(a, a + b) = \text{FBCT}_F(a + b, b) = \text{FBCT}_F(b, a + b)$. Thus, the following result holds.

Proposition 3.1 *Given a function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$, $n \geq 2$, then*

$$\sum_{a,b \in \mathbb{F}_{2^n}^*, a \neq b} \text{FBCT}_F(a, b) = 24 \# \mathcal{VP}_{n,F}.$$

Therefore, the knowledge of the vanishing flats implies the knowledge of the Feistel Boomerang Connectivity Table (FBCT)/second-order zero differential spectra, though the vanishing flats shows not only the number of solutions but the actual solutions of the equation. However, the knowledge of the *number* of vanishing flats does not imply the knowledge of the Feistel Boomerang Connectivity Table (FBCT)/second-order zero differential spectra.

Very recently, Carlet [7] introduced a generalization of APNness called *sum-freedom*. Let $2 \leq k \leq n$ and m be positive integers. An (n, m) -function F is called *kth-order sum-free* if, for every k -dimensional affine subspace (i.e. k -flat) A of \mathbb{F}_{2^n} , the sum $\sum_{X \in A} F(X)$ is nonzero. Thus, F is second-order sum free if and only if $\mathcal{VP}_{n,F} = \emptyset$, or equivalently, F is second-order sum free if and only if $\text{FBCT}_F(a, b) = 0$ for $a, b \in \mathbb{F}_{2^n}$ with $ab(a + b) \neq 0$.

In [18], an alternative definition of APNness was given: A function $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ is a *generalized almost perfect nonlinear (GAPN) function* if the equation

$$\tilde{D}_a F(X) = \sum_{i \in \mathbb{F}_p} F(X + ai) = b$$

has at most p solutions X in \mathbb{F}_{p^n} if $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$.

For $p = 2$, this is clearly the notion of APNness, while for p odd the derivative differs from the usual derivative for p odd, which is given by $D_a F(X) = F(X) - F(X + a)$. It would be interesting to study how the functions studied in this paper for p odd (and in general) behave under this generalized derivative. As far as the authors can see, there is no clear connection for p odd between neither the differential uniformity nor the Feistel Boomerang Connectivity table.

4 The second-order zero differential spectrum for power functions over finite fields of odd characteristic

Let p be now odd. Then, a function F is PN if and only if, for any $X_1, a \in \mathbb{F}_{p^n}$ ($a \neq 0$),

$$F(X_1 + a) - F(Y + a) - F(X_1) + F(Y) = 0$$

has exactly one solution, namely $Y = X_1$.

Similarly, F is APN if and only if, for any $X_1, a \in \mathbb{F}_{p^n}$ ($a \neq 0$),

$$F(X_1 + a) - F(Y + a) - F(X_1) + F(Y) = 0$$

has at most two distinct solutions $Y = X_1, X_2$, and there is at least one X_1 such that the equation has exactly two solutions $X_1 \neq X_2$.

We see here that the study of the Feistel Boomerang Connectivity Table (FBCT)/second-order zero differential spectra is closely linked to how far is a function from the PN or the APN property, as is the case with the APN-ness in even characteristic.

Table 1 gives some of the known functions with low second-order zero differential uniformity over finite fields of odd characteristic, in addition to the general results on the PN/APN functions mentioned in [5].

In this section, we first deal with the computation of the second-order zero differential spectrum of the function $F(X) = X^d$, where $d = \frac{2p^n-1}{3}$ over \mathbb{F}_{p^n} , for $p^n \equiv 2 \pmod{3}$. Helleseth et al. [16] showed that F is an APN function over \mathbb{F}_{p^n} , for $p^n \equiv 2 \pmod{3}$.

Theorem 4.1 *Let $F(X) = X^d$ be a function of \mathbb{F}_{p^n} , where $d = \frac{2p^n-1}{3}$, $p^n \equiv 2 \pmod{3}$. Then for $a, b \in \mathbb{F}_{p^n}$,*

$$\nabla_F(a, b) = \begin{cases} 1 & \text{if } ab \neq 0 \\ p^n & \text{if } ab = 0. \end{cases}$$

Moreover, F is second-order zero differential 1-uniform.

Proof For $a, b \in \mathbb{F}_{p^n}$, we consider the equation

$$F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0. \tag{4.1}$$

If $ab = 0$, then $\nabla_F(a, b) = p^n$. If $ab \neq 0$, then we can write the above equation as

$$\begin{cases} Y - X - a = 0 \\ F(Y + b) - F(Y) - F(X + b) + F(X) = 0, \end{cases} \tag{4.2}$$

Table 1 Second-order differential uniformity for functions over finite fields of odd characteristic

p	d	condition	Δ_F	∇_F	Ref
$p > 3$	3	any	2	1	[21, Theorem 3.1]
$p = 3$	$3^n - 3$	$n > 1$ is odd	2	2	[21, Theorem 3.2]
$p > 2$	$p^n - 2$	$p^n \equiv 2 \pmod{3}$	2	1	[21, Theorem 3.3]
$p > 3$	$p^m + 2$	$n = 2m, p^m \equiv 1 \pmod{3}$	2	1	[21, Theorem 3.4]
$p = 3$	$3^n - 2$	any	3	3	[21, Theorem 3.1]
p	$p^n - 2$	$p^n \equiv 1 \pmod{3}$	3	3	[21, Theorem 3.1]
$p > 3$	4	$n > 1$	3	2	This paper
p	$\frac{2p^n-1}{3}$	$p^n \equiv 2 \pmod{3}$	2	1	This paper
$p > 3$	$\frac{p^k+1}{2}$	$\gcd(2n, k) = 1$	$\leq \gcd(\frac{p^k-1}{2}, p^{2n} - 1)$	$\frac{p-3}{2}$	This paper
$p = 3$	$\frac{p^n-1}{2} + 2$	n is odd	4	3	This paper

or equivalently, substituting $Y' = \frac{Y}{b}$ and $X' = \frac{X}{b}$, we have

$$\begin{cases} Y' - X' - ab^{-1} = 0 \\ F(Y' + 1) - F(Y') - F(X' + 1) + F(X') = 0. \end{cases} \tag{4.3}$$

Let $c \in \mathbb{F}_{p^n}^*$ and $F(Y' + 1) - F(Y') = c$. Let $u_{Y'} = (Y')^d$ and $u_{Y'+1} = (Y' + 1)^d$. Then $u_{Y'+1} = c + u_{Y'}$, and since $3d \equiv 1 \pmod{p^n - 1}$, we have $(u_{Y'+1})^3 = (c + u_{Y'})^3$, or equivalently,

$$3c(u_{Y'})^2 + 3c^2u_{Y'} + c^3 - 1 = 0.$$

We get the quadratic equation in terms of $u_{Y'}$ and since $u_{Y'} = (Y')^d$, each of the two solutions gives a maximum of $\gcd(d, p^n - 1) = 1$ solutions in Y' . Solving the above quadratic equation, we have

$$u_{Y'} = \frac{-3c^2 \pm \sqrt{9c^4 - 4(3c)(c^3 - 1)}}{6c} = \frac{-3c^2 \pm \sqrt{-3c^4 + 12c}}{6c},$$

and hence for $\Delta = \sqrt{-3c^4 + 12c}$, we have $(u_{Y'})^3 = Y' = \left(\frac{-3c^2 \pm \Delta}{6c}\right)^3$. This will give us

$$Y'_1 = \frac{\Delta^3 - 27c^6 - 9c^2\Delta^2 + 27c^4\Delta}{(216)c^3} \text{ and } Y'_2 = \frac{-(\Delta^3 + 27c^6 + 9c^2\Delta^2 + 27c^4\Delta)}{(216)c^3}. \text{ Then}$$

$$F(X'+1) - F(X') = c \text{ will also give us the same solutions } X'_1 = \frac{\Delta^3 - 27c^6 - 9c^2\Delta^2 + 27c^4\Delta}{(216)c^3}$$

and, $X'_2 = \frac{-(\Delta^3 + 27c^6 + 9c^2\Delta^2 + 27c^4\Delta)}{(216)c^3}$. Now, from the first equation of System (4.3),

we have $Y'_1 = X'_2 + ab^{-1}$ or $Y'_2 = X'_1 + ab^{-1}$ as $ab^{-1} \neq 0$. We need to show that for every pair $(a, b) \in \mathbb{F}_{p^n}$, with $ab \neq 0$, there exists a unique c for which either $Y'_1 = X'_2 + ab^{-1}$ or $Y'_2 = X'_1 + ab^{-1}$ holds. Now, $Y'_1 - X'_2 = ab^{-1}$ is the same as $2\Delta^3 + 54c^4\Delta = (216)c^3ab^{-1}$. Next, squaring the last expression we get,

$$4\Delta^6 + (54)^2c^8\Delta^2 + 4(54)c^4\Delta^4 = (216)^2c^6(ab^{-1})^2. \tag{4.4}$$

We have, $\Delta^6 = (-3c^4 + 12c)^3 = -(27)c^{12} + (12)^3c^3 - 9(12)^2c^6 + (27)(12)c^9$, and $\Delta^4 = (-3c^4 + 12c)^2 = 9c^8 + 144c^2 - 72c^5$. Substituting all the values, we have (4.4) reduced to

$$4c^{12} - 12c^9 + ((27)(ab^{-1})^2 - 15)c^6 - 4c^3 = 0,$$

or equivalently,

$$4k^3 - 12k^2 + ((27)(ab^{-1})^2 - 15)k - 4 = 0,$$

where $k = c^3$. We can write the above equation as below:

$$(k - 1)^3 + \frac{(27)((ab^{-1})^2 - 1)k}{4} = 0. \tag{4.5}$$

When $(ab^{-1})^2 = 1$, that is $a = \pm b$, then $k = 1$ and hence $c = 1$, or we can say $\Delta = 3$. Thus we have $Y'_1 = X'_1 = 0$ and $Y'_2 = X'_2 = -1$. When $a = b$, $ab^{-1} = 1$ and hence out of the pairs (X'_1, Y'_2) and (X'_2, Y'_1) , we have $Y'_1 - X'_2 = 1$ giving us $X = -b$ as a solution of (4.2) in that case. And similarly for $a = -b$, we have $X = 0$ as a solution of (4.2).

Let us now have $(ab^{-1})^2 \neq 1$. Substituting $k - 1 = Z$ and $A = \frac{(27)((ab^{-1})^2 - 1)}{4}$, we can write the above (4.5) as $Z^3 + AZ + A = 0$. The discriminant D for the cubic equation

is $D = -4A^3 - (27)A^2 = -A^2(4A + 27) = -(27)(ab^{-1})^2A^2$. Let us now assume that $Z^3 + AZ + A = 0$ has one root $Z_1 \in \mathbb{F}_{p^n}$. Then the cubic equation will have other two roots in \mathbb{F}_{p^n} only if D is a square in \mathbb{F}_{p^n} . Clearly D is a square in \mathbb{F}_{p^n} only if $\eta(-27) = \eta(-3) = 1$, where η is the quadratic character of \mathbb{F}_{p^n} . As $p^n \equiv 2 \pmod{3}$, one can see that $\eta(-3) = -1$ (from [22, Exercise 5.22]). Hence D is not a square in \mathbb{F}_{p^n} . Thus, if $Z^3 + AZ + A = 0$ has a root in \mathbb{F}_{p^n} , then the other two roots are not in \mathbb{F}_{p^n} .

Thus we are left to show that $Z^3 + AZ + A = 0$ is reducible over \mathbb{F}_{p^n} . However, that is immediate via a result of Dickson [12, Lemma 2], who showed that a necessary and sufficient condition for a cubic to have one and only one root in \mathbb{F}_{p^n} , $p > 2$, is that the discriminant is a non-square in \mathbb{F}_{p^n} , which is what we showed above. Hence, for every pair $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, the equation $Z^3 + AZ + A = 0$ has exactly one solution $Z \in \mathbb{F}_{p^n}$ or equivalently a unique k , i.e. $k = Z + 1$. Now, $\gcd(3, p^n - 1) = 1$ and hence there exists exactly one c corresponding to each pair of $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, for which Δ exists and $2\Delta^3 + 54c^4\Delta = (216)c^3ab^{-1}$, i.e. $Y'_1 - X'_2 = ab^{-1}$. Notice that $Y'_1 - X'_2 = ab^{-1}$ and $Y'_2 - X'_1 = ab^{-1}$ cannot hold simultaneously. Hence, the proof holds. \square

Next, we consider the power function $F(X) = X^d$, where $d = \frac{p^k+1}{2}$, and compute its second-order zero differential spectrum over \mathbb{F}_{p^n} .

Theorem 4.2 *Let $F(X) = X^d$ be a power function of \mathbb{F}_{p^n} , where $d = \frac{p^k+1}{2}$, and $\gcd(k, 2n) = 1$. Let $p > 3$. Then for $a, b \in \mathbb{F}_{p^n}$,*

$$\nabla_F(a, b) = \begin{cases} 0 & \text{if } ab \neq 0 \text{ and } \eta(D) = -1 \\ 1 & \text{if } ab \neq 0 \text{ and } \eta(D) = 0 \\ \frac{p-3}{2} & \text{if } ab \neq 0 \text{ and } \eta(D) = 1 \\ p^n & \text{if } ab = 0, \end{cases}$$

where $D = \frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}$, u is a primitive $(p-1)$ -th root of unity in $\mathbb{F}_{p^{2n}}^*$. Moreover, F is second-order zero differential $\frac{p-3}{2}$ -uniform.

Proof For $a, b \in \mathbb{F}_{p^n}$, we consider the equation

$$F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0. \tag{4.6}$$

If $ab = 0$, then $\nabla_F(a, b) = p^n$. If $ab \neq 0$, then we split (4.6) in the following system

$$\begin{cases} Y - X - a = 0 \\ F(Y + b) - F(Y) - F(X + b) + F(X) = 0. \end{cases} \tag{4.7}$$

For $Y \in \mathbb{F}_{p^{2n}}^*$, there exist $\alpha, \beta \in \mathbb{F}_{p^{2n}}^*$ such that $Y + b = \alpha^2$ and $Y = \beta^2$. Let $\alpha - \beta = \theta \in \mathbb{F}_{p^{2n}}^*$. Then we have $\alpha + \beta = b\theta^{-1}$, giving us $\alpha = \frac{\theta + b\theta^{-1}}{2}$ and $\beta = \frac{b\theta^{-1} - \theta}{2}$. Thus,

$$\begin{aligned} (Y + b)^d - Y^d &= \left(\frac{\theta + b\theta^{-1}}{2}\right)^{p^k+1} - \left(\frac{b\theta^{-1} - \theta}{2}\right)^{p^k+1} \\ &= \frac{\theta^{p^k}(b\theta^{-1}) + (b\theta^{-1})^{p^k}\theta}{2}. \end{aligned}$$

Using a similar argument as above we can write

$$(X + b)^d - X^d = \frac{\lambda^{p^k}(b\lambda^{-1}) + (b\lambda^{-1})^{p^k}\lambda}{2},$$

where $\lambda = \delta - \gamma \in \mathbb{F}_{p^{2n}}^*$, for $X + b = \delta^2$ and $X = \gamma^2$ such that $\delta, \gamma \in \mathbb{F}_{p^{2n}}^*$. Now, using the second equation of System (4.7), we have

$$(Y + b)^d - Y^d = (X + b)^d - X^d,$$

or equivalently,

$$\frac{\theta^{p^k}(b\theta^{-1}) + (b\theta^{-1})^{p^k}\theta}{2} = \frac{\lambda^{p^k}(b\lambda^{-1}) + (b\lambda^{-1})^{p^k}\lambda}{2}.$$

The above equality will give us either $(\lambda\theta^{-1})^{p^k-1} = 1$ or $(\lambda\theta)^{p^k-1} = b^{p^k-1}$. Since $\gcd(p^k - 1, p^{2n} - 1) = p^{\gcd(k, 2n)} - 1 = p - 1$, we have either $\lambda = u^i\theta$ or $\lambda = bu^i\theta^{-1}$, where u is a primitive $(p - 1)$ -th root of unity in $\mathbb{F}_{p^{2n}}^*$, $1 \leq i \leq p - 1$. Now, we discuss all the possible values of λ .

Note that, if $j = \frac{p-1}{2} + i$, then $u^j = -u^i$. We have then $\lambda = \pm u^i\theta$ or $\lambda = \pm bu^i\theta^{-1}$, where u is a primitive $(p - 1)$ -th root of unity in $\mathbb{F}_{p^{2n}}^*$, $1 \leq i \leq \frac{p-1}{2}$.

If $\lambda = \pm\theta, \pm b\theta^{-1}$, then $X = Y$, but from the first equation of System (4.7), we know $X \neq X + a$. Hence $\lambda \notin \{\pm\theta, \pm b\theta^{-1}\}$.

In general, if $\lambda = \pm u^i\theta, \pm bu^i\theta^{-1}, u^i \neq 1$, then

$$X = \left(\frac{b\lambda^{-1} - \lambda}{2}\right)^2 = \frac{1}{4\lambda^2}(\lambda^4 - 2b\lambda^2 + b^2) = \frac{1}{4u^{2i}\theta^2}(u^{4i}\theta^4 - 2bu^{2i}\theta^2 + b^2).$$

Thus,

$$\begin{aligned} a &= Y - X = \frac{1}{4\theta^2}\left(\theta^4 - 2b\theta^2 + b^2 - \frac{u^{4i}\theta^4 - 2bu^{2i}\theta^2 + b^2}{u^{2i}}\right), \\ 4a\theta^2 &= \theta^4(1 - u^{2i}) + b^2(1 - u^{-2i}), \\ 0 &= \theta^4 - \frac{4a}{1 - u^{2i}}\theta^2 + b^2\frac{1 - u^{-2i}}{1 - u^{2i}}, \\ 0 &= \theta^4 - \frac{4a}{1 - u^{2i}}\theta^2 - b^2\frac{1}{u^{2i}}, \\ \theta^2 &= \frac{\frac{4a}{1-u^{2i}} \pm \sqrt{\frac{16a^2}{(1-u^{2i})^2} + 4\frac{b^2}{u^{2i}}}}{2} = \frac{2a}{1 - u^{2i}} \pm \sqrt{\frac{4a^2}{(1 - u^{2i})^2} + \frac{b^2}{u^{2i}}}. \end{aligned}$$

When $D = \frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}} = 0, \theta^2 = \frac{2a}{1-u^{2i}}$, implying that

$$X = \frac{1}{4}\left(u^{2i}\frac{2a}{1 - u^{2i}} - 2b + b^2u^{-2i}\frac{1 - u^{2i}}{2a}\right).$$

When $\eta(D) = -1$, there is no solution. When $\eta(D) = 1$, there are two solutions for X ,

$$X = \frac{1}{4}\left(u^{2i}\left(\frac{2a}{1 - u^{2i}} \pm \sqrt{\frac{4a^2}{(1 - u^{2i})^2} + \frac{b^2}{u^{2i}}}\right) - 2b + b^2u^{-2i}\frac{1}{\frac{2a}{1-u^{2i}} \pm \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}}}\right).$$

Now, observe that

$$\frac{1}{\frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}}} = \frac{-u^{2i} \left(\frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right)}{b^2}, \text{ and}$$

$$\frac{1}{\frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}}} = \frac{-u^{2i} \left(\frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right)}{b^2}.$$

Let us call $S_i = \{u^i\theta, u^j\theta, bu^i\theta^{-1}, bu^j\theta^{-1}\}$, where $j = \frac{p-1}{2} + i$ and $1 \leq i \leq \frac{p-3}{2}$. Thus for $\lambda \in S_i$, we have the following two solutions,

$$\begin{aligned} X_{i,1} &= \frac{1}{4} \left(u^{2i} \left(\frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) - 2b + b^2 u^{-2i} \frac{1}{\frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}}} \right) \\ &= \frac{1}{4} \left(u^{2i} \left(\frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) - 2b - \frac{2a}{1-u^{2i}} + \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) \\ &= \frac{1}{4} \left(-2a - 2b + (1+u^{2i}) \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) \\ &= \frac{1}{4} \left(-2a - 2b + \frac{(1+u^{2i})}{(1-u^{2i})} \sqrt{4a^2 - b^2(1-u^{2i})(1-u^{-2i})} \right) \\ &= \frac{1}{4} \left(-2a - 2b + \frac{(1+u^{2i})}{(1-u^{2i})} \sqrt{4a^2 + b^2 \frac{(u^{2i}-1)^2}{u^{2i}}} \right) \end{aligned}$$

and

$$\begin{aligned} X_{i,2} &= \frac{1}{4} \left(u^{2i} \left(\frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) - 2b + b^2 u^{-2i} \frac{1}{\frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}}} \right) \\ &= \frac{1}{4} \left(u^{2i} \left(\frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) - 2b - \frac{2a}{1-u^{2i}} - \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) \\ &= \frac{1}{4} \left(-2a - 2b - (1+u^{2i}) \sqrt{\frac{4a^2}{(1-u^{2i})^2} + \frac{b^2}{u^{2i}}} \right) \\ &= \frac{1}{4} \left(-2a - 2b - \frac{(1+u^{2i})}{(1-u^{2i})} \sqrt{4a^2 - b^2(1-u^{2i})(1-u^{-2i})} \right) \\ &= \frac{1}{4} \left(-2a - 2b - \frac{(1+u^{2i})}{(1-u^{2i})} \sqrt{4a^2 + b^2 \frac{(u^{2i}-1)^2}{u^{2i}}} \right). \end{aligned}$$

Now, one can see that $\frac{(u^{2k}-1)^2}{u^{2k}} = \frac{(u^{2l}-1)^2}{u^{2l}}$ for $1 \leq k \neq l \leq \frac{p-3}{2}$ implies that $u^{2k-2l}(u^{2k+2l}-1) = 0$, or equivalently $u^{2k+2l} = 1$. This will give us $u^k = -(u^l)^{-1}$, because being a primitive $(p-1)$ -th root of unity, $u^{k+l} \neq 1$. Also, observe that for $u^k = -(u^l)^{-1}$,

$\frac{(1+u^{2^k})}{(1-u^{2^k})} = -\frac{(1+u^{2^l})}{(1-u^{2^l})}$. The above discussion will give us $X_{k,1} = X_{l,2}$, when $u^k = -(u^l)^{-1}$. Next, we note that

$$(u^{\frac{p-3}{2}-(t-1)})^{-1} = (u^{\frac{p-3}{2}})^{-1}u^{t-1} = u^{\frac{p-1}{2}}u^t = -u^t,$$

where $1 \leq t \leq \frac{p-3}{4}$ when $p \equiv 3 \pmod{4}$ and $1 \leq t \leq \frac{p-5}{4}$ when $p \equiv 1 \pmod{4}$ (notice that $(u^{\frac{p-1}{4}})^{-1} = -u^{\frac{p-1}{4}}$ when $p \equiv 1 \pmod{4}$). Hence, for all the possible values of i in our case, that is $1 \leq i \leq \frac{p-3}{2}$, we have $X_{i,1} = X_{\frac{p-3}{2}-(t-1),2}$ for $1 \leq t \leq i$. Thus for $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ satisfying $\eta(D) = 1$, (4.6) has $\frac{p-3}{2}$ solutions in \mathbb{F}_{p^n} . \square

Remark 4.3 Helleseth et al. in [16] showed that if $d = \frac{5^k+1}{2}$, $\gcd(k, 2n) = 1$, then $F(X) = X^d$ is an APN power function over \mathbb{F}_{5^n} . Hence, from the above Theorem 4.2, we get that F is second-order zero differential 1-uniform over \mathbb{F}_{5^n} . Note also that, if $p = 3$, then F is PN, and therefore, by [21], it is second-order zero differential 0-uniform over \mathbb{F}_{3^n} .

Now, we consider more functions with low (that is, 3, 4) differential uniformity. In the following result, we show that $F(X) = X^4$ is second-order zero differential 2-uniform for all $p, n > 1$.

Proposition 4.4 *Let $F(X) = X^4$ be a power function of \mathbb{F}_{p^n} , where p is an odd prime and $n > 1$. Then for $a, b \in \mathbb{F}_{p^n}$,*

$$\nabla_F(a, b) = \begin{cases} 0 & \text{if } \eta\left(\frac{-a^2 - b^2}{3}\right) = -1 \\ 1 & \text{if } a^2 + b^2 = 0 \\ 2 & \text{if } \eta\left(\frac{-a^2 - b^2}{3}\right) = 1 \\ p^n & \text{if } ab = 0. \end{cases}$$

In particular, F is second-order zero differential 2-uniform.

Proof For $a, b \in \mathbb{F}_{p^n}$, we consider the equation:

$$F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0.$$

If $ab = 0$, then $\nabla_F(a, b) = p^n$. If $ab \neq 0$, then we have the simplified equation as

$$X^2 + (a + b)X + \frac{a^2 + b^2}{3} + \frac{ab}{2} = 0.$$

One can easily observe that the discriminant of the above quadratic equation is $\frac{-(a^2 + b^2)}{3}$. This completes the proof. \square

Helleseth et al. in [17] showed that $F(X) = X^d$, where $d = \frac{3^n-1}{2} + 2$ is a differentially 4-uniform function over \mathbb{F}_{p^n} , for odd n . We compute its second-order zero differential spectrum implying that this function is second-order zero differential 3-uniform.

Theorem 4.5 *Let $F(X) = X^d$ be a function on \mathbb{F}_{3^n} , where $d = \frac{3^n-1}{2} + 2$ and n is odd. Then for $a, b \in \mathbb{F}_{3^n}$,*

$$\nabla_F(a, b) = \begin{cases} 1 & \text{if } \eta(ab) = 1 = \eta(a^2 + b^2) \text{ or } \eta(ab) = -1 \text{ and } \eta(a^2 + b^2) = 1 \\ 3 & \text{if } \eta(ab) = -1 = \eta(a^2 + b^2) \text{ or } \eta(ab) = 1 \text{ and } \eta(a^2 + b^2) = -1 \\ 3^n & \text{if } ab = 0. \end{cases}$$

In particular, F is second-order zero differential 3-uniform.

Proof Now for $a, b \in \mathbb{F}_{3^n}$, we consider the equation:

$$F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0. \tag{4.8}$$

If $ab = 0$, then $\nabla_F(a, b) = 3^n$. If $ab \neq 0$, then we can write the above equation as

$$\eta(X + a + b)(X + a + b)^2 - \eta(X + b)(X + b)^2 - \eta(X + a)(X + a)^2 + \eta(X)X^2 = 0,$$

where η is the quadratic character over \mathbb{F}_{3^n} . Also $\eta(-1) = -1$, because n is odd. Moreover, one can easily see that if X is a solution of (4.8), then $-(X + a + b)$ is also a solution of (4.8). Now, for $X \notin \{0, -a, -b, -(a + b)\}$, we have sixteen possible cases listed in Table 2.

One can discard Case 1 and Case 16, as $ab \neq 0$. Notice that Case 5 is not possible. This is because if $X = \sqrt{ab}$ is a solution with respect to Case 5, then we have $\eta(\sqrt{ab}) = -1$ and $\eta(b + \sqrt{ab}) = \eta(a + \sqrt{ab}) = \eta(a + b + \sqrt{ab}) = 1$. Then we can write

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

This will give us $\eta(a + b + \sqrt{ab})\eta(a + b - \sqrt{ab}) = \eta((a - b)^2) = -1$, which is not true. Hence, $X = \sqrt{ab}$ cannot be a solution of Case 5. Similarly, one can show that $X = -\sqrt{ab}$ is not a solution of Case 5. By similar reasoning, the possibility for Case 12 can also be removed. Also, Case 3, Case 4, Case 13 and Case 14 cannot hold. If $X = -a + \sqrt{-ab}$ is a solution of Case 3, then $\eta(-a + \sqrt{-ab}) = 1 = \eta(b - a + \sqrt{-ab}) = \eta(b + \sqrt{-ab})$ and $\eta(\sqrt{-ab}) = -1$. Thus, we have

$$1 = \eta(b + \sqrt{-ab})\eta(-a + \sqrt{-ab}) = \eta(\sqrt{-ab}(b - a + 2\sqrt{ab})) = -\eta(b - a - \sqrt{ab}).$$

This renders $\eta(b - a + \sqrt{-ab})\eta(b - a - \sqrt{-ab}) = \eta((a + b)^2) = -1$, which is not true.

Now we split our analysis in four cases depending on the values of $\eta(ab)$ and $\eta(a^2 + b^2)$.

Case A Let $\eta(ab) = 1$ and $\eta(a^2 + b^2) = 1$. We can have only one solution possible in this case. If Case 2 holds, then $X_1 = -(a + b) \pm \sqrt{ab}$ is a solution of (4.8) for Case A. But then $-(X_1 + a + b) = \pm\sqrt{ab}$ is also a solution which is not possible. Similarly, Case 15 would also not contribute to Case A. Hence the only possible solution we have is either obtained from Case 10 or Case 11.

Case B Let $\eta(ab) = -1$ and $\eta(a^2 + b^2) = 1$. We have exactly one solution in \mathbb{F}_{3^n} of (4.8), i.e. $X = \frac{-(a+b)}{2}$, which is obtained either from Case 10 or Case 11.

Case C Let $\eta(ab) = 1$ and $\eta(a^2 + b^2) = -1$. This case will have three solutions. One solution would be obtained either from Case 10 or Case 11. Notice that Case 8 and Case 9 can have at most one solution individually. Also, they cannot occur simultaneously.

Hence, if $X_1 = \frac{-(a+b)+\sqrt{-(a^2+b^2)}}{2}$, a solution obtained from Case 8 satisfies (4.8),

then $Y_1 = -(X_1 + a + b) = \frac{-(a+b)-\sqrt{-(a^2+b^2)}}{2}$ is also a solution of (4.8). Observe that Y_1 can be obtained from Case 9. Similarly we have one more possible pair

of solutions, i.e. $X_2 = \frac{-(a+b)-\sqrt{-(a^2+b^2)}}{2}$ and $Y_2 = \frac{-(a+b)+\sqrt{-(a^2+b^2)}}{2}$ satisfying Case 8 and Case 9 respectively. Summarizing all, we have exactly three solutions in Case C.

Case D Let $\eta(ab) = -1$ and $\eta(a^2 + b^2) = -1$. Using similar arguments used in Case C, one can show that there are three solutions in this case as well.

This completes the proof. □

Table 2 Various cases considered when $ab \neq 0$

Case	$\eta(X + a + b)$	$\eta(X + a)$	$\eta(X + b)$	$\eta(X)$	Equation	X
1	1	1	1	1	$2ab = 0$	No solution
2	-1	1	1	1	$X^2 + 2(a + b)X + a^2 + b^2 + ab = 0$	$-(a + b) \pm \sqrt{ab}$
3	1	-1	1	1	$X^2 + 2aX + a^2 + ab = 0$	$-a \pm \sqrt{-ab}$
4	1	1	-1	1	$X^2 + 2bX + b^2 + ab = 0$	$-b \pm \sqrt{-ab}$
5	1	1	1	-1	$X^2 - ab = 0$	$\pm\sqrt{ab}$
6	-1	-1	1	1	$2X + a + b = 0$	$X = \frac{-(a+b)}{2}$
7	-1	1	-1	1	$2X + a + b = 0$	$X = \frac{-(a+b)}{2}$
8	-1	1	1	-1	$2X^2 + 2(a + b)X + a^2 + b^2 + ab = 0$	$\frac{-(a+b) \pm \sqrt{-(a^2 + b^2)}}{2}$
9	1	-1	-1	1	$2X^2 + 2(a + b)X + a^2 + b^2 + ab = 0$	$\frac{-(a+b) \pm \sqrt{-(a^2 + b^2)}}{2}$
10	1	-1	1	-1	$2X + a + b = 0$	$X = \frac{-(a+b)}{2}$
11	1	1	-1	-1	$2X + a + b = 0$	$X = \frac{-(a+b)}{2}$
12	-1	-1	-1	1	$X^2 - ab = 0$	$\pm\sqrt{ab}$
13	-1	-1	1	-1	$X^2 + 2bX + b^2 + ab = 0$	$-b \pm \sqrt{-ab}$
14	-1	1	-1	-1	$X^2 + 2aX + a^2 + ab = 0$	$-a \pm \sqrt{-ab}$
15	1	-1	-1	-1	$X^2 + 2(a + b)X + a^2 + b^2 + ab = 0$	$-(a + b) \pm \sqrt{ab}$
16	-1	-1	-1	-1	$2ab = 0$	No solution

5 The second-order zero differential spectrum for power functions over finite fields of even characteristic

In this section, we first compute the second-order zero differential spectrum of the family of functions $F(X) = X^{2^t-1}$ over \mathbb{F}_{2^n} , whose DDT entries have already been computed by Blondeau et al. in [3]. We then compute the number of vanishing flats. Finally, we consider a few concrete values of t that give low differential uniformity.

Let $F(X) = X^d$ be a monomial. Recall that for any $(a', b') \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, $\nabla_F(a', b')$ is given by the number of solutions $X \in \mathbb{F}_{2^n}$ of the following equation

$$X^d + (X + a')^d + (X + b')^d + (X + a' + b')^d = 0. \tag{5.1}$$

Observe that for $a' = 0, b' = 0$ and $a' = b',$ (5.1) has 2^n solutions in $\mathbb{F}_{2^n}.$ Let $a', b' \neq 0.$ We now rewrite (5.1) as

$$x^d + (x + 1)^d + (x + b)^d + (x + b + 1)^d = 0,$$

where $b = \frac{b'}{a'}, x = \frac{X'}{a'}$ and $a' \neq 0.$ We can, therefore, assume without loss of generality that $a' = 1,$ since $\nabla_F(a', b') = \nabla_F(1, b'/a')$ if $a' \neq 0.$ Moreover, we know that for a monomial $F(X) = X^d,$ the DDT entries of F are determined by $\delta_F(1, b), b \in \mathbb{F}_{2^n}.$ Throughout this paper, we shall denote $\delta_F(1, b)$ by $\delta_F(b),$ and the differential uniformity of F by $\delta_F.$

Theorem 5.1 *Let F be a function over \mathbb{F}_{2^n} defined by $F(X) = X^{2^t-1}.$ Then, for any $b \in \mathbb{F}_{2^n},$*

$$\nabla_F(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_F(B) & \text{if } B = 1, \\ \max(\delta_F(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise,} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 2^{\gcd(t-1, n)} & \text{if } B = 1, \\ 2^{\gcd(t, n)} - 4 & \text{if } B = 0, \\ \max(2^r - 4, 0) & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $B = \frac{b^{2^t} + b}{b(b+1)}$ for $b \neq 0, 1, 1 < r \leq \min(t, n - t + 1),$ and r depends on $B,$ precisely, $r = \dim(\text{Ker}(P_B)), P_B = X^{2^t} + BX^2 + (B + 1).$

NB: Note that $\delta_F(1) = 2^{\gcd(t-1, n)}$ and $\delta_F(0) = 2^{\gcd(t, n)} - 2,$ by [3]. However, given that the relation between b and B is in general not a permutation, $\delta_F(B) \leq \delta_F,$ the differential uniformity, but $\max_b \delta_F(B)$ is not necessarily equal to $\delta_F.$ Therefore, the F -Boomerang uniformity is bounded by the differential uniformity:

$$\beta_F = \max_{a \neq 0, b \neq 0, a \neq b} \text{FBCT}_F(a, b) \leq \delta_F,$$

but the equality may not happen.

Proof Recall that for any $(a', b') \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*,$ $\nabla_F(a', b')$ is given by the number of solutions $X \in \mathbb{F}_{2^n}$ of the following equation

$$X^{2^t-1} + (X + a')^{2^t-1} + (X + b')^{2^t-1} + (X + a' + b')^{2^t-1} = 0. \tag{5.2}$$

Observe that for $a' = 0, b' = 0$ and $a' = b',$ (5.2) has 2^n solutions in $\mathbb{F}_{2^n}.$ We now rewrite the (5.2) as

$$x^{2^t-1} + (x + 1)^{2^t-1} + (x + b)^{2^t-1} + (x + b + 1)^{2^t-1} = 0, \tag{5.3}$$

where $x = \frac{X}{a'}, b = \frac{b'}{a'}.$ Clearly, for $b = 0$ and $b = 1,$ (5.3) has 2^n solutions in $\mathbb{F}_{2^n}.$ We assume $b \in \mathbb{F}_{2^n}^* \setminus \{1\}.$ Then we have the following two cases:

Case 1 Let $x \in \{0, 1, b, b + 1\}$. Then (5.3) reduces to

$$1 + b^{2^t-1} + (1 + b)^{2^t-1} = 0, \text{ that is, } b^2 + b^{2^t} = 0.$$

This is equivalent to $b^{2^t-2} = 1$.

Case 2 Let $x \notin \{0, 1, b, b + 1\}$. Then (5.2) reduces to

$$\frac{x^{2^t}}{x} + \frac{(x + 1)^{2^t}}{x + 1} + \frac{(x + b)^{2^t}}{x + b} + \frac{(x + 1 + b)^{2^t}}{x + 1 + b} = 0,$$

or equivalently,

$$b(b + 1)x^{2^t} + (b^{2^t} + b)x^2 + (b^{2^t} + b^2)x = 0.$$

As $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$, we can rewrite the above equation as

$$P_B(x) = x^{2^t} + Bx^2 + (B + 1)x = 0, \tag{5.4}$$

where $B = \frac{b^{2^t} + b}{b(b + 1)}$. Then, we need to compute the number of solutions to (5.4).

By [3, Theorem 1], $\delta_F(0) = 2^{\gcd(t,n)} - 2$, $\delta_F(1) = 2^{\gcd(t-1,n)}$, $\delta_F(b) = 2^r - 2$, $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, $1 \leq r \leq \min(t, n - t + 1)$. Observe that, when $r = 1$, $\delta_F(b) = 0$, and that $\delta_F(b)$ is the number of solutions other than 0, 1, for $b \neq 1$. The result then follows. Note that, since $B = 0$ if and only if $b^{2^t-1} = 1$, and this is only possible for $b \neq 1$ if $\gcd(2^t - 1, 2^n - 1) = \gcd(t, n) > 1$, then in this case $2^{\gcd(t,n)} - 4 \geq 0$, giving that $\max(2^{\gcd(t,n)} - 4, 0) = 2^{\gcd(t,n)} - 4$. \square

From the above result and Proposition 3.1, we determine the number of vanishing flats of $F(X) = X^{2^t-1}$ over \mathbb{F}_{2^n} , as stated in the following corollary. We point to [20], where some of the vanishing flat counts are also found. A good summary can be found in [20, Table 3], where we find the count for $t = n - 1, n - 2, \frac{n-1}{2}, \frac{n+3}{2}$ (n odd), $\frac{n}{2}, \frac{n}{2} + 1$ (n even). Our next corollary considers arbitrary values of t .

Corollary 5.2 *Let $F(X) = X^{2^t-1}$ over \mathbb{F}_{2^n} , then the number of vanishing flats $\mathcal{VP}_{n,F}$ of F is given by*

$$\frac{1}{24} \left[(2^n - 1)(4^{\gcd(t-1,n)} + 4^{\gcd(t,n)} - 3 \cdot 2^{\gcd(t,n)+1} - 2^{\gcd(t-1,n)+1} + 8) + (2^r - 4)(\#\mathcal{R}_{2^r-4}) \right],$$

where $\#\mathcal{R}_{2^r-4} = (2^n - 1) \cdot \#\left\{ b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^t-2} \neq 1, b^{2^t-1} \neq 1, \delta_F\left(\frac{b^{2^t} + b}{b(b+1)}\right) = 2^r - 2 \right\}$, $1 < r \leq \min(t, n - t + 1)$, $r (= r(B)) = \dim(\text{Ker}(P_B))$, $P_B = X^{2^t} + BX^2 + (B + 1)$.

Proof From Theorem 5.1, we know that for any $b \in \mathbb{F}_{2^n}^*$,

$$\nabla_F(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_F(B) & \text{if } B = 1, \\ \max(\delta_F(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise,} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 2^{\gcd(t-1,n)} & \text{if } B = 1, \\ 2^{\gcd(t,n)} - 4 & \text{if } B = 0, \\ \max(2^r - 4, 0) & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $B = \frac{b^{2^t} + b}{b(b + 1)}$, and $1 < r \leq \min(t, n - t + 1)$. We consider the set

$$\mathcal{S}_i = \{b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid \text{FBCT}_F(1, b) = i\}.$$

Table 3 Various cases when $ab \neq 0$ and $a \neq b$

Case	$\text{Tr}_1^a(X^{2^l+1})$	$\text{Tr}_1^a((X+a)^{2^l+1})$	$\text{Tr}_1^a((X+b)^{2^l+1})$	$\text{Tr}_1^a((X+a+b)^{2^l+1})$	Equation
1	0	0	0	0	$\frac{1}{X} + \frac{1}{X+a} + \frac{1}{X+b} + \frac{1}{X+a+b} = 0$
2	1	0	0	0	$\frac{1}{X+\gamma} + \frac{1}{X+a} + \frac{1}{X+b} + \frac{1}{X+a+b} = 0$
3	0	1	0	0	$\frac{1}{X} + \frac{1}{X+a+\gamma} + \frac{1}{X+b} + \frac{1}{X+a+b} = 0$
4	0	0	1	0	$\frac{1}{X} + \frac{1}{X+a} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b} = 0$
5	0	0	0	1	$\frac{1}{X} + \frac{1}{X+a} + \frac{1}{X+b} + \frac{1}{X+a+b+\gamma} = 0$
6	1	1	0	0	$\frac{1}{X+\gamma} + \frac{1}{X+a+\gamma} + \frac{1}{X+b} + \frac{1}{X+a+b} = 0$
7	1	0	1	0	$\frac{1}{X+\gamma} + \frac{1}{X+a} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b} = 0$
8	1	0	0	1	$\frac{1}{X+\gamma} + \frac{1}{X+a} + \frac{1}{X+b} + \frac{1}{X+a+b+\gamma} = 0$
9	0	1	1	0	$\frac{1}{X} + \frac{1}{X+a+\gamma} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b} = 0$
10	0	1	0	1	$\frac{1}{X} + \frac{1}{X+a+\gamma} + \frac{1}{X+b} + \frac{1}{X+a+b+\gamma} = 0$
11	0	0	1	1	$\frac{1}{X} + \frac{1}{X+a} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b+\gamma} = 0$
12	1	1	1	0	$\frac{1}{X+\gamma} + \frac{1}{X+a+\gamma} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b} = 0$
13	1	0	1	1	$\frac{1}{X+\gamma} + \frac{1}{X+a} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b+\gamma} = 0$
14	0	1	1	1	$\frac{1}{X} + \frac{1}{X+a+\gamma} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b+\gamma} = 0$
15	1	1	0	1	$\frac{1}{X+\gamma} + \frac{1}{X+a+\gamma} + \frac{1}{X+b} + \frac{1}{X+a+b+\gamma} = 0$
16	1	1	1	1	$\frac{1}{X+\gamma} + \frac{1}{X+a+\gamma} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b+\gamma} = 0$

It is obvious that $B = 1$ if and only if $b^{2^t-2} = 1$ for any $b \in \mathbb{F}_{2^n}^*$. Therefore, we get $\#S_{2^{\gcd(t-1,n)}} = \gcd(2^t - 2, 2^n - 1) - 1 = 2^{\gcd(t-1,n)} - 2$. Similarly, $B = 0$ if and only if $b^{2^t-1} = 1$ for any $b \in \mathbb{F}_{2^n}^*$. This will give us $\#S_{2^{\gcd(t,n)-4}} = \gcd(2^t - 1, 2^n - 1) - 1 = 2^{\gcd(t,n)} - 2$.

Next, we need to consider the case when $B \notin \{0, 1\}$ and $\text{FBCT}_F(1, b) = 2^r - 4$ where $1 < r \leq \min(t, n - t + 1)$. Here, we will have $\#S_{2^r-4} = \#\{b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^t-2} \neq 1, b^{2^t-1} \neq 1, \delta_F\left(\frac{b^{2^t}+b}{b(b+1)}\right) = 2^r - 2\}$, $1 < r \leq \min(t, n - t + 1)$. Moreover, if for each $a \in \mathbb{F}_{2^n}^*$,

$$\mathcal{R}_i = \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* \setminus \{a\} \mid \text{FBCT}_F(a, b) = i\},$$

then

$$\#\mathcal{R}_{2^{\gcd(t-1,n)}} = (2^{\gcd(t-1,n)} - 2)(2^n - 1),$$

$$\#\mathcal{R}_{2^{\gcd(t,n)-4}} = (2^{\gcd(t,n)} - 2)(2^n - 1),$$

and $\#\mathcal{R}_{2^r-4} = (2^n - 1) \left(\#\left\{b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^t-2} \neq 1, b^{2^t-1} \neq 1, \delta_F\left(\frac{b^{2^t}+b}{b(b+1)}\right) = 2^r - 2\right\} \right)$, where $1 < r \leq \min(t, n - t + 1)$.

Thus, from Proposition 3.1, the number of vanishing flats $\mathcal{VP}_{n,F}$ of F is given by

$$\frac{1}{24} \left[2^{\gcd(t-1,n)} (2^{\gcd(t-1,n)} - 2)(2^n - 1) + (2^{\gcd(t,n)} - 4)(2^{\gcd(t,n)} - 2)(2^n - 1) + (2^r - 4)(\#\mathcal{R}_{2^r-4}) \right],$$

where $1 < r \leq \min(t, n - t + 1)$, which renders the claim. □

We will next consider some particular classes with low differential uniformity. Firstly, we compute the second-order zero differential spectrum of the locally APN function $F_1(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m}}$, the DDT entries for which have already been computed by Blondeau et al. in [3]. We then consider a few more permutations with low differential uniformity.

Corollary 5.3 *Let $F_1(X) = X^{2^m-1} \in \mathbb{F}_{2^n}[X]$, where $n = 2m$. Then for any $b \in \mathbb{F}_{2^n}$, we have:*

(1) *When m is odd,*

$$\nabla_{F_1}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 4 & \text{if } b \neq 0, 1 \text{ and } b^{2^m-2} = 1, \\ 2^m - 4 & \text{if } b \neq 0, 1 \text{ and } b^{2^m-1} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *When m is even,*

$$\nabla_{F_1}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 2^m - 4 & \text{if } b \neq 0, 1 \text{ and } b^{2^m-1} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the Feistel boomerang uniformity of F_1 is $\beta_{F_1} = 2^m - 4$ for m even or m odd with $m > 2$.

Proof Here, $t = m = \frac{n}{2}$. Then, $\gcd(t - 1, n) = \gcd(m - 1, 2m) = 1$, when m is even and $\gcd(t - 1, n) = \gcd(m - 1, 2m) = 2$ when m is odd, respectively. Moreover, $\gcd(t, n) =$

$\gcd(m, 2m) = m$ for every positive integer m . Let $B = \frac{b^{2^m} + b}{b(b + 1)}$ for $b \neq 0, 1$. Furthermore, from Theorem 7 in [3], $\delta_{F_1}(0) = 2^m - 2$, $\delta_{F_1}(1) = 4$ when m is odd and $\delta_{F_1}(1) = 2$ when m is even. Also, $\delta_{F_1}(B) \leq 2$ for $B \neq 0, 1$. This implies that $\max(\delta_{F_1}(B) - 2, 0) = 0$ for $B \neq 0, 1$. Hence from Theorem 5.1, we have the following:

1. If m is even,

$$\nabla_{F_1}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_1}(B) & \text{if } B = 1, \\ \max(\delta_{F_1}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 2 & \text{if } B = 1, \\ 2^m - 4 & \text{if } B = 0, \\ 0 & \text{otherwise.} \end{cases}$$

2. If m is odd,

$$\nabla_{F_1}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_1}(B) & \text{if } B = 1, \\ \max(\delta_{F_1}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 4 & \text{if } B = 1, \\ 2^m - 4 & \text{if } B = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly,

$$B = 1 \Leftrightarrow B + 1 = \frac{b^{2^m} + b^2}{b(b + 1)} = 0 \Leftrightarrow b^{2^m - 2} = 1, b \neq 1.$$

Now, $\gcd(2^m - 2, 2^{2m} - 1) = 1$ if m is even, and $\gcd(2^m - 2, 2^n - 1) = 3$ if m is odd, implying that $B = 1$ is not possible for m even, while there are exactly two values of b such that $B = 1$ if m is odd.

Thus the proof follows immediately from $\nabla_{F_1}(a, b) = \nabla_{F_1}(1, b/a)$. □

Corollary 5.4 *Let $F_1(X) = X^{2^m - 1}$ over $\mathbb{F}_{2^{2m}}$, then we have*

$$\#\mathcal{VP}_{n, F_1} = \begin{cases} \frac{(2^{m-2} - 1)(2^{m-1} - 1)(2^n - 1)}{3} & \text{if } m \text{ is even,} \\ \frac{((2^{m-2} - 1)(2^{m-1} - 1) + 1)(2^n - 1)}{3} & \text{if } m \text{ is odd.} \end{cases}$$

Proof The number of vanishing flats for $F_1(X) = X^{2^m - 1}$ over $\mathbb{F}_{2^{2m}}$ follows from Corollary 5.2 and Corollary 5.3. □

Blondeau et al. [3] also studied the differential uniformity of $F_2(X) = X^{2^{\frac{n-1}{2}} - 1}$ for n odd, and showed that it is a permutation having differential uniformity at most 8. In the following corollary, we determine its FBCT spectrum and show that its F -boomerang uniformity is at most 8 for $m \not\equiv 1 \pmod{3}$, and is exactly 4 for $m \equiv 1 \pmod{3}$.

Corollary 5.5 *Let $F_2(X) = X^{2^m - 1} \in \mathbb{F}_{2^n}[X]$, where $n = 2m + 1$. Then for any $b \in \mathbb{F}_{2^n}$, we have:*

(1) *When $m \equiv 1 \pmod{3}$,*

$$\nabla_{F_2}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 8 & \text{if } b \neq 0, 1, \text{ and } b^{2^m - 2} = 1, \\ 4 & \text{if } b \in \mathcal{S}_6, \\ 0 & \text{otherwise.} \end{cases}$$

(2) When $m \not\equiv 1 \pmod{3}$,

$$\nabla_{F_2}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 4 & \text{if } b \in S_6, \\ 0 & \text{otherwise,} \end{cases}$$

where $S_6 = \{b \in \mathbb{F}_{2^n}^* \setminus \{1\}, b^{2^m-2} \neq 1, b^{2^m-1} \neq 1 \text{ and } \delta_{F_2}(B) = 6\}$, with $B = \frac{b^{2^m} + b}{b(b+1)}$. Thus, the Feistel boomerang uniformity of F_2 is 8 for $m \equiv 1 \pmod{3}$, and it is 4 for $m \not\equiv 1 \pmod{3}$.

Proof Notice that $t = m = \frac{n-1}{2}$. Then, $\gcd(t - 1, n) = \gcd(m - 1, 2m + 1) = 3$ if $m \equiv 1 \pmod{3}$ and 1 if $m \not\equiv 1 \pmod{3}$, respectively. Additionally, $\gcd(t, n) = \gcd(m, 2m + 1) = 1$, for all positive integers m . For $B = \frac{b^{2^m} + b}{b(b+1)}$ where $b \neq 0, 1$, observe from [3, Theorem 9] that $\delta_{F_2}(1) = 8$ when $m \equiv 1 \pmod{3}$ and otherwise, $\delta_{F_2}(1) = 2$. Moreover, we have $\delta_{F_2}(0) = 0$ and $\delta_{F_2}(B) = 6$ for some $B \in \mathbb{F}_{2^n}^* \setminus \{1\}$. This further implies that $\max(\delta_{F_2}(B) - 2, 0) = 4$ when $B \neq 0, 1$. Therefore from Theorem 5.1, we get:

1. If $m \equiv 1 \pmod{3}$,

$$\nabla_{F_2}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_2}(B) & \text{if } B = 1, \\ \max(\delta_{F_2}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 8 & \text{if } B = 1, \\ 0 & \text{if } B = 0, \\ 4 & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise.} \end{cases}$$

2. If $m \not\equiv 1 \pmod{3}$,

$$\nabla_{F_2}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_2}(B) & \text{if } B = 1, \\ \max(\delta_{F_2}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 2 & \text{if } B = 1, \\ 0 & \text{if } B = 0, \\ 4 & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise.} \end{cases}$$

Since, $\gcd(2^m - 1, 2^n - 1) = 1$, $B = 0$ is not possible. Moreover, $B = 1$ if and only if $b^{2^m-2} = 1, b \neq 1$. Clearly, $\gcd(2^m - 2, 2^n - 1) = 1$ when $m \not\equiv 1 \pmod{3}$, so in that case $B = 1$ is not possible. We then need to consider only the case $m \equiv 1 \pmod{3}$; in this case $\gcd(2^m - 2, 2^n - 1) = 7$, giving us exactly six values of $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $B = 1$.

Next, we have $\nabla_{F_2}(1, b) = 4$, when $\delta_{F_2}(B) = 6$ and $B \neq 0, 1$. More precisely, we can say that $\nabla_{F_2}(1, b) = 4$ when $b \in S_6 = \{b \in \mathbb{F}_{2^n}^* \setminus \{1\}, b^{2^m-2} \neq 1, b^{2^m-1} \neq 1 \text{ and } \delta_{F_2}\left(\frac{b^{2^m} + b}{b(b+1)}\right) = 6\}$. □

In the next corollary, we give the number of vanishing flats of F_2 .

Corollary 5.6 Let $F_2(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m+1}}$, then we have

$$\#\mathcal{VP}_{n, F_2} = \begin{cases} \left(\frac{2^{n-2} + 7}{6} - \frac{K(1)}{8}\right) (2^n - 1) & \text{if } m \equiv 1 \pmod{3} \\ \left(\frac{2^{n-2} + 1}{6} - \frac{K(1)}{8}\right) (2^n - 1) & \text{if } m \not\equiv 1 \pmod{3}, \end{cases}$$

where $K(1)$ is the Kloosterman sum.

Proof From Corollary 5.5, we have $\nabla_{F_2}(1, b) = 4$, when $b \in S_6$. The cardinality of the set S_6 is

$$\begin{aligned} \#S_6 &= \# \left\{ b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^i-2} \neq 1, b^{2^i-1} \neq 1 \text{ and } \delta_{F_2}(B) = \delta_{F_2} \left(\frac{b^{2^i} + b}{b(b+1)} \right) = 6 \right\} \\ &= \# \{ b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^i-2} \neq 1, b^{2^i-1} \neq 1 \\ &\quad \text{and } x^{2^m} + Bx^2 + (B+1)x \text{ has six solutions } \in \mathbb{F}_{2^n} \}. \end{aligned}$$

It is already known from [4, Theorem 5] that for $m \equiv 1 \pmod{3}$,

$$\#\{B \in \mathbb{F}_{2^n}^* \setminus \{1\} \text{ and } \delta_{F_2}(B) = 6\} = \frac{2^{n-2} - 5}{6} - \frac{K(1)}{8}.$$

We thereby only need to count the number of $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $\delta_{F_2}(B) = 6$. Now, for a given $B \in \mathbb{F}_{2^n}^* \setminus \{1\}$ with $\delta_{F_2}(B) = 6$, we can write

$$b^{2^m} + Bb^2 + (B+1)b = 0.$$

Since B is fixed, the above equation will have eight solutions $b \in \mathbb{F}_{2^n}$ including $\{0, 1\}$. Thus, for each $B \in \mathbb{F}_{2^n}^* \setminus \{1\}$ with $\delta_{F_2}(B) = 6$ the above equation will have 6 solutions as $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$. This gives us $\#S_6 = 6 \left(\frac{2^{n-2} - 5}{6} - \frac{K(1)}{8} \right)$ when $m \equiv 1 \pmod{3}$. Hence, the number of vanishing flats for $F_2(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m+1}}$, when $m \equiv 1 \pmod{3}$ follows from Corollary 5.2 and Corollary 5.5.

In a similar way, when $m \not\equiv 1 \pmod{3}$, we get $\#S_6 = 6 \left(\frac{2^{n-2} + 1}{6} - \frac{K(1)}{8} \right)$. This gives us the number of vanishing flats for $F_2(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m+1}}$, for $m \not\equiv 1 \pmod{3}$. □

In terms of the new concept, the authors of [5] show that F is an APN function of \mathbb{F}_{2^n} if and only if the FBCT of F is zero (already known from [9]). Hence, the next best possible value of the FBCT of F over even characteristic of functions with differential uniformity greater than two is four. We now consider a power function $F_3(X) = X^{2^{\frac{n+3}{2}}-1}$, which is a permutation if and only if $n \equiv 0 \pmod{3}$. Blondeau et al. in [4] conclude that the function F_3 is differentially 6-uniform over \mathbb{F}_{2^n} , when n is odd. In the following theorem, we show that the function F_3 attains the best possible value of the FBCT, i.e. four, for odd n .

Corollary 5.7 *Let $F_3(X) = X^d$ be a power function of \mathbb{F}_{2^n} , where $d = 2^{\frac{n+3}{2}} - 1$ and n is odd. Then for $b \in \mathbb{F}_{2^n}$ we have:*

(1) *When $n \equiv 0 \pmod{3}$,*

$$\nabla_{F_3}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 4 & \text{if } b \neq 0, 1, \text{ and } b^{2^m-1} = 1, \\ 4 & \text{if } b \in S_6, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *When $n \not\equiv 0 \pmod{3}$,*

$$\nabla_{F_3}(1, b) = \begin{cases} 2^n & \text{if } b = 0, \text{ or } b = 1, \\ 4 & \text{if } b \in S_6, \\ 0 & \text{otherwise,} \end{cases}$$

$$\text{where } S_6 = \left\{ b \in \mathbb{F}_{2^n}^* \setminus \{1\} \mid b^{2^{\frac{n+3}{2}}-2} \neq 1, b^{2^{\frac{n+3}{2}}-1} \neq 1 \text{ and } \delta_{F_3} \left(\frac{b^{2^{\frac{n+3}{2}}} + b}{b(b+1)} \right) = 6 \right\}.$$

Thus, the Feistel boomerang uniformity of F_3 is 4.

Proof Clearly, $t = \frac{n+3}{2}$ and $\gcd(t, n) = 3$ if $n \equiv 0 \pmod{3}$ and 1 if $n \not\equiv 0 \pmod{3}$, respectively. Moreover, $\gcd(t - 1, n) = 1$ for all positive integers n . Let $B = \frac{b^{2^t} + b}{b(b+1)}$ when $b \neq 0, 1$. Then, from Theorem 9 and Corollary 2 in [3], we have $\delta_{F_3}(0) = 6$ when $n \equiv 0 \pmod{3}$ and $\delta_{F_3}(0) = 0$ when $n \not\equiv 0 \pmod{3}$. Also, we have $\delta_{F_3}(1) = 2$ for every positive integer n and $\delta_{F_3}(B) = 6 = 2^3 - 2$ for some $B \in \mathbb{F}_{2^n}^* \setminus \{1\}$. Therefore, $\max(\delta_{F_3}(B) - 2, 0) = 4$ when $B \neq 0, 1$. Thus, from Theorem 5.1, we get the following:

(1) If $n \equiv 0 \pmod{3}$,

$$\nabla_{F_3}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_3}(B) & \text{if } B = 1, \\ \max(\delta_{F_3}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 0 & \text{if } B = 1, \\ 4 & \text{if } B = 0, \\ 4 & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise.} \end{cases}$$

(2) If $n \not\equiv 0 \pmod{3}$,

$$\nabla_{F_3}(1, b) = \begin{cases} 2^n & \text{if } b = 0, 1, \\ \delta_{F_3}(B) & \text{if } B = 1, \\ \max(\delta_{F_3}(B) - 2, 0) & \text{if } B \neq 1, \\ 0 & \text{otherwise.} \end{cases} = \begin{cases} 2^n & \text{if } b = 0, 1, \\ 0 & \text{if } B = 1, \\ 0 & \text{if } B = 0, \\ 4 & \text{if } B \neq 0, 1, \\ 0 & \text{otherwise.} \end{cases}$$

It is obvious that $B = 1$ if and only if $b^{2^t-2} = 1, b \neq 1$. Since, $\gcd(2^m - 2, 2^n - 1) = 1$, there does not exist $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $B = 1$. Moreover, we have $B = 0$ if and only if $b^{2^t-1} = 1, b \neq 1$. Since, $\gcd(2^t - 1, 2^n - 1) = 1$ when $n \not\equiv 0 \pmod{3}$, so in that case $B = 0$ is not possible. Thus, we are left with the case when $n \equiv 0 \pmod{3}$; in this case $\gcd(2^t - 1, 2^n - 1) = 7$, giving us exactly six values of $b \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $B = 0$.

Next, we have $\nabla_{F_3}(1, b) = 4$, when $\delta_{F_3}(B) = 6, B \neq 0, 1$, or equivalently, when $b \in S_6 = \left\{ b \in \mathbb{F}_{2^n}^* \setminus \{1\}, b^{2^t-2} \neq 1, b^{2^t-1} \neq 1 \text{ and } \delta_{F_3} \left(\frac{b^{2^t} + b}{b(b+1)} \right) = 6 \right\}$. □

We next determine the number of vanishing flats of F_3 .

Corollary 5.8 Let $F_3(X) = X^{2^t-1}$ over \mathbb{F}_{2^n} , where $t = \frac{n+3}{2}$. Then we have

$$\#\mathcal{VP}_{n, F_3} = \frac{2^{n-2} + 1}{6} - \frac{K(1)}{8},$$

where $K(1)$ is the Kloosterman sum.

Proof It is known from Corollary 2 in [3] that $\#S_6$ for $F_3(X) = X^{2^{\frac{n+3}{2}}-1}$ is same as $\#S_6$ for $F_2(X) = X^{2^{n-1}}$. Thus, from Corollary 5.6 we get, $\#S_6 = 6 \left(\frac{2^{n-2} - 5}{6} - \frac{K(1)}{8} \right)$ when $n \equiv 0 \pmod{3}$ and $\#S_6 = 6 \left(\frac{2^{n-2} + 1}{6} - \frac{K(1)}{8} \right)$ when $n \not\equiv 0 \pmod{3}$, respectively. Hence, using Corollary 5.2 and Corollary 5.7, we get the number of vanishing flats for $F_3(X) = X^{2^t-1}$ over \mathbb{F}_{2^n} . □

6 The second-order zero differential spectrum for some differentially low uniform permutation polynomials in even characteristic

Next, we shall consider two differentially low uniform permutation polynomials over the finite field \mathbb{F}_{2^n} . The first one was introduced by Tan et al. [28] who showed that when n is even, the permutation polynomial $F(X) = X^{-1} + \text{Tr}_1^n\left(\frac{X^2}{X+1}\right)$ is differentially 4-uniform. Further, Hasan et al. in [15] studied the c -differential and boomerang uniformities of $F(X)$.

Below, we shall be using the following result of [19]. Let f be the polynomial $f(X) = X^4 + a_2X^2 + a_1X + a_0$ with $a_0a_1 \neq 0$ and $g(Y) = Y^3 + a_2Y + a_1$ be the companion cubic with the roots r_1, r_2, r_3 . When the roots exist in \mathbb{F}_{2^n} , we set $w_i = a_0r_i^2/a_1^2$. We write a polynomial h as $h = (1, 2, 3, \dots)$ over some field to mean that it decomposes as a product of degree 1, 2, 3, \dots , over that field.

Lemma 6.1 [[19]] *Let $f(X) = X^4 + a_2X^2 + a_1X + a_0 \in \mathbb{F}_{2^n}[X]$ with $a_0a_1 \neq 0$. The factorization of $f(X)$ over \mathbb{F}_{2^n} is characterized as follows:*

- (i) $f = (1, 1, 1, 1) \Leftrightarrow g = (1, 1, 1)$ and $\text{Tr}_1^n(w_1) = \text{Tr}_1^n(w_2) = \text{Tr}_1^n(w_3) = 0$;
- (ii) $f = (2, 2) \Leftrightarrow g = (1, 1, 1)$ and $\text{Tr}_1^n(w_1) = 0, \text{Tr}_1^n(w_2) = \text{Tr}_1^n(w_3) = 1$;
- (iii) $f = (1, 3) \Leftrightarrow g = (3)$;
- (iv) $f = (1, 1, 2) \Leftrightarrow g = (1, 2)$ and $\text{Tr}_1^n(w_1) = 0$;
- (v) $f = (4) \Leftrightarrow g = (1, 2)$ and $\text{Tr}_1^n(w_1) = 1$.

In the following theorem, we give the FBCT of $F(X) = X^{-1} + \text{Tr}_1^n\left(\frac{X^2}{X+1}\right)$.

Theorem 6.1 *Let $F(X) = X^{-1} + \text{Tr}_1^n\left(\frac{X^2}{X+1}\right)$ be a function over \mathbb{F}_{2^n} , where n is even. Then for $a, b \in \mathbb{F}_{2^n}$,*

$$\nabla_F(a, b) = \begin{cases} 4 & \text{if } \text{Tr}_1^n(b^{-1}) = \text{Tr}_1^n(b^{-1}\omega) = \text{Tr}_1^n(b^{-1}\omega^2) = 0, \text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^3) = 1, \\ & \text{or } \text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^3) = 0 \text{ and } \text{Tr}_1^n(b^{-1}) = 1, \\ & \text{or } \text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^3) = 0 \text{ and } \text{Tr}_1^n(b^{-1}\omega) = 1, \\ & \text{or } \text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^3) = 0 \text{ and } \text{Tr}_1^n(b^{-1}\omega^2) = 1, \\ & \text{or } \text{Tr}_1^n(w_1) = \text{Tr}_1^n(w_2) = \text{Tr}_1^n(w_3) = \text{Tr}_1^n\left(\frac{ab(a+b)}{a^2+b^2+ab(a+b)+ab+1}\right) = 1, \\ 8 & \text{if } \text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^{-1}) = \text{Tr}_1^n(b^{-1}\omega) = \text{Tr}_1^n(b^{-1}\omega^2) = 0, \text{Tr}_1^n(b^3) = 1, \\ 2^n & \text{if } ab = 0 \text{ or } a = b, \\ 0 & \text{otherwise,} \end{cases}$$

where ω is a cube root of unity, $w_1 = \frac{a}{b(a+b)}, w_2 = \frac{b}{a(a+b)}$ and $w_3 = \frac{a+b}{ab}$. Moreover, F is second-order zero differential 8-uniform (that is, the Feistel boomerang uniformity of F is 8).

Proof For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0. \tag{6.1}$$

If $ab = 0$ and $a = b$, then $\nabla_F(a, b) = 2^n$. If $ab \neq 0, a \neq b$, then we can write it as,

$$(X + a + b)^{-1} + (X + b)^{-1} + (X + a)^{-1} + X^{-1} + \text{Tr}_1^n \left(\frac{X^2}{X + 1} + \frac{X^2 + a^2}{X + a + 1} + \frac{X^2 + b^2}{X + b + 1} + \frac{X^2 + a^2 + b^2}{X + a + b + 1} \right) = 0.$$

Case A $a^2 + ab + b^2 = 0$ (i.e. $a \in \{b\omega, b(\omega + 1)\}$). We can distinguish two subcases.

Subcase a Let $\text{Tr}_1^n \left(\frac{X^2}{X + 1} + \frac{X^2 + a^2}{X + a + 1} + \frac{X^2 + b^2}{X + b + 1} + \frac{X^2 + a^2 + b^2}{X + a + b + 1} \right) = 0$. Then $\nabla_F(a, b) = \nabla_G(a, b)$, where $G(X) = X^{-1}$, and therefore, from Lemma 2.5, there are a priori 4 solutions, namely $X = 0, a, b$ and $a + b$. We have that, for all these,

$$\text{Tr}_1^n \left(\frac{X^2}{X + 1} + \frac{X^2 + a^2}{X + a + 1} + \frac{X^2 + b^2}{X + b + 1} + \frac{X^2 + a^2 + b^2}{X + a + b + 1} \right) = \text{Tr}_1^n \left(\frac{b^3}{b^3 + 1} \right).$$

Therefore, in this subcase, there are four solutions, namely $X = 0, a, b$ and $a + b$, if $\text{Tr}_1^n \left(\frac{b^3}{b^3 + 1} \right) = 0$, and no solutions if $\text{Tr}_1^n \left(\frac{b^3}{b^3 + 1} \right) = 1$.

Subcase b Let $\text{Tr}_1^n \left(\frac{X^2}{X + 1} + \frac{X^2 + a^2}{X + a + 1} + \frac{X^2 + b^2}{X + b + 1} + \frac{X^2 + a^2 + b^2}{X + a + b + 1} \right) = 1$. Then

$$(X + a + b)^{-1} + (X + b)^{-1} + (X + a)^{-1} + X^{-1} = 1.$$

If $X = 0, a, b$ or $a + b$, this renders

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{a + b} = 1,$$

or, equivalently,

$$a^2 + ab + b^2 = ab(a + b).$$

However, $a^2 + ab + b^2 = 0$, gives a contradiction. Assume, then, $X \notin \{0, a, b, a + b\}$. In this case, we obtain

$$\frac{1}{X} + \frac{1}{X + a} + \frac{1}{X + b} + \frac{1}{X + a + b} = 1,$$

which is the same as,

$$X^4 + (a^2 + b^2 + ab)X^2 + ab(a + b)X + ab(a + b) = 0.$$

Since $a \in \{b\omega, b(\omega + 1)\}$, this gives

$$X^4 + b^3X + b^3 = 0. \tag{6.2}$$

Looking at the roots of the resolvent cubic $Y^3 + b^3$, we see that there are three different roots $Y_1 = b, Y_2 = b\omega, Y_3 = b(\omega + 1)$. Equation (6.2) has then four solutions (different than $0, a, b, a + b$) if $\text{Tr}_1^n(b^{-1}) = \text{Tr}_1^n(b^{-1}\omega) = \text{Tr}_1^n(b^{-1}\omega^2) = 0$, and no solutions if $\text{Tr}_1^n(b^{-1}) = 1$ or $\text{Tr}_1^n(b^{-1}\omega) = 1$ or $\text{Tr}_1^n(b^{-1}\omega^2) = 1$. The solutions, if any, have to fulfill the condition $\text{Tr}_1^n \left(\frac{X^2}{X + 1} + \frac{X^2 + a^2}{X + a + 1} + \frac{X^2 + b^2}{X + b + 1} + \frac{X^2 + a^2 + b^2}{X + a + b + 1} \right) = \text{Tr}_1^n(b^3) = 1$.

Summarizing these two subcases, then, we see that (6.1) has 8 solutions if $\text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^{-1}) = \text{Tr}_1^n(b^{-1}\omega) = \text{Tr}_1^n(b^{-1}\omega^2) = 0$ and $\text{Tr}_1^n(b^3) = 1$, 4 solutions if $\text{Tr}_1^n(b^{-1}) = \text{Tr}_1^n(b^{-1}\omega) = \text{Tr}_1^n(b^{-1}\omega^2) = 0$ and $\text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = \text{Tr}_1^n(b^3) = 1$ or $\text{Tr}_1^n\left(\frac{b^3}{b^3+1}\right) = 0, \text{Tr}_1^n(b^{-1}) = 1$ or $\text{Tr}_1^n(b^{-1}\omega) = 1$ or $\text{Tr}_1^n(b^{-1}\omega^2) = 1$ or $\text{Tr}_1^n(b^3) = 0$, and no solutions otherwise.

Case B $a^2 + ab + b^2 \neq 0$ (i.e. $a \notin \{b\omega, b(\omega + 1)\}$). We can distinguish two subcases:

Subcase a Let $\text{Tr}_1^n\left(\frac{X^2}{X+1} + \frac{X^2+a^2}{X+a+1} + \frac{X^2+b^2}{X+b+1} + \frac{X^2+a^2+b^2}{X+a+b+1}\right) = 0$. Then $\nabla_F(a, b) = \nabla_G(a, b)$, where $G(X) = X^{-1}$, and therefore, from Lemma 2.5, there are no solutions.

Subcase b Let $\text{Tr}_1^n\left(\frac{X^2}{X+1} + \frac{X^2+a^2}{X+a+1} + \frac{X^2+b^2}{X+b+1} + \frac{X^2+a^2+b^2}{X+a+b+1}\right) = 1$. Then

$$(X+a+b)^{-1} + (X+b)^{-1} + (X+a)^{-1} + X^{-1} = 1. \tag{6.3}$$

If $X = 0, a, b$ or $a + b$, this renders

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{a+b} = 1,$$

or, equivalently,

$$a^2 + ab + b^2 = ab(a + b).$$

This is possible, and the solutions are valid if

$$\begin{aligned} \text{Tr}_1^n\left(\frac{X^2}{X+1} + \frac{X^2+a^2}{X+a+1} + \frac{X^2+b^2}{X+b+1} + \frac{X^2+a^2+b^2}{X+a+b+1}\right) \\ = \text{Tr}_1^n\left(\frac{ab(a+b)}{a^2+b^2+ab(a+b)+ab+1}\right) = 1. \end{aligned}$$

Because we have $a^2 + ab + b^2 + ab(a + b) = 0$, the above condition will further give us $\text{Tr}_1^n(ab(a + b)) = 1$. We would next show that there does not exist any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $a^2 + b^2 + ab + ab(a + b) = 0$ and $\text{Tr}_1^n(ab(a + b)) = 1$. Let us assume that $a^2 + b^2 + ab + ab(a + b) = 0$ for some $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Then applying the absolute trace on the above equation, we get that

$$\text{Tr}_1^n(ab(a + b)) = \text{Tr}_1^n(a + b + ab). \tag{6.4}$$

Now dividing $a^2 + b^2 + ab + ab(a + b) = 0$ by a and applying the trace again, we get that

$$\text{Tr}_1^n(a) + \text{Tr}_1^n\left(\frac{b^2}{a}\right) + \text{Tr}_1^n(b) + \text{Tr}_1^n(ba) + \text{Tr}_1^n(b^2) = 0,$$

or equivalently,

$$\text{Tr}_1^n(a) + \text{Tr}_1^n\left(\frac{b^2}{a}\right) + \text{Tr}_1^n(ba) = 0. \tag{6.5}$$

Again dividing $a^2 + b^2 + ab + ab(a + b) = 0$ by a^2 and applying the absolute trace, we have

$$\text{Tr}_1^n(1) + \text{Tr}_1^n\left(\frac{b^2}{a^2}\right) + \text{Tr}_1^n\left(\frac{b}{a}\right) + \text{Tr}_1^n(b) + \text{Tr}_1^n\left(\frac{b^2}{a}\right) = 0,$$

which is the same as

$$\text{Tr}_1^n(b) + \text{Tr}_1^n\left(\frac{b^2}{a}\right) = 0. \tag{6.6}$$

From (6.4), (6.5) and (6.6), we get that for even n , there does not exist any (a, b) in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\text{Tr}_1^n(ab(a + b)) = 1$. Hence $0, a, b$ and $a + b$ are not the solutions of (6.3).

If $X \notin \{0, a, b, a + b\}$, we obtain

$$\frac{1}{X} + \frac{1}{X + a} + \frac{1}{X + b} + \frac{1}{X + a + b} = 1,$$

which is same as,

$$X^4 + (a^2 + b^2 + ab)X^2 + ab(a + b)X + ab(a + b) = 0. \tag{6.7}$$

Again, via Lemma 6.1, observe that the companion cubic polynomial is yet again

$$Y^3 + (a^2 + ab + b^2)Y + ab(a + b) = (Y + a)(Y + b)(Y + a + b).$$

We let $a_0 = ab(a + b), a_1 = ab(a + b), a_2 = a^2 + ab + b^2, w_1 = \frac{a_0a^2}{a^2} = \frac{a}{b(a+b)}, w_2 = \frac{a_0b^2}{a^2} = \frac{b}{a(a+b)}$, and $w_3 = \frac{a_0(a+b)^2}{a^2} = \frac{a+b}{ab}$. Since the companion cubic is thus $(1, 1, 1)$, from Lemma 6.1 (i) and (ii), we then see that the polynomial (6.7) is either $(1, 1, 1, 1)$ or $(2, 2)$, and so, it has a root in \mathbb{F}_{2^n} if and only if all the traces of w_1, w_2, w_3 are zero. Thus, (6.7) can have at most four solutions. Hence, (6.1) can have at most four solutions from Subcase b.

In conclusion, (6.1) has at most 8 solutions. □

Next, for t and n , two positive integers, the authors in [32] show that the function $F(X) = \frac{1}{X + \gamma \text{Tr}_1^n(X^{2^t+1})}$ is a permutation of \mathbb{F}_{2^n} with $\delta_F \leq 6$, where γ is an element of $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^{2t}}^*$ with $\text{Tr}_1^n(\gamma^{2^t+1}) = 0$. In the following theorem, we determine the FBCT of this function. We have not explicitly stated the second-order zero differential spectrum of this function in the statement of the theorem due to the large number of conditions required. However, it is readily apparent from the proof of the theorem.

Theorem 6.2 *Let $F(X) = \frac{1}{X + \gamma \text{Tr}_1^n(X^{2^t+1})}$ where t and n are two positive integers with $t < n$, and γ is an element of $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^{2t}}^*$ with $\text{Tr}_1^n(\gamma^{2^t+1}) = 0$. Then for $a, b \in \mathbb{F}_{2^n}, \nabla_F(a, b) \in \{0, 4, 8\}$. Consequently, F has Feistel boomerang uniformity at most 8.*

Proof For $a, b \in \mathbb{F}_{2^n}$, we consider the equation:

$$F(X + a + b) + F(X + b) + F(X + a) + F(X) = 0. \tag{6.8}$$

If $ab = 0$ or $a = b$, then $\nabla_F(a, b) = 2^n$. If $ab \neq 0$, (6.8) can be written as,

$$\frac{1}{X + \gamma \text{Tr}_1^n(X^{2^t+1})} + \frac{1}{X + a + \gamma \text{Tr}_1^n((X + a)^{2^t+1})} + \frac{1}{X + b + \gamma \text{Tr}_1^n((X + b)^{2^t+1})} + \frac{1}{X + a + b + \gamma \text{Tr}_1^n((X + a + b)^{2^t+1})} = 0.$$

Next, we consider sixteen possible cases as pointed out in Table 3.

Let N_i denote the number of solutions in \mathbb{F}_{2^n} for the i^{th} case given in Table 3.

Case 1 For the first case, we need to consider the number of solutions $X \in \mathbb{F}_{2^n}$ of the equation, $\frac{1}{X} + \frac{1}{X+a} + \frac{1}{X+b} + \frac{1}{X+a+b} = 0$, which is the same as the FBCT of the inverse function. From Lemma 2.6, it is clear that for odd n , Case 1 has no solution. When n is even, then Lemma 2.5 would give us only four solutions $X \in \{0, a, b, a + b\}$ of Case 1 if and only if $a \in \{b\omega, b\omega^2\}$ and $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a + b)^{2^t+1}) = 0$.

Case 2 In this case, consider the number of solutions $X \in \mathbb{F}_{2^n}$ of the equation, $\frac{1}{X + \gamma} + \frac{1}{X + a} + \frac{1}{X + b} + \frac{1}{X + a + b} = 0$. It is clear that $X = \gamma$ cannot be a solution of Case 2 as $\text{Tr}_1^n(\gamma^{2^t+1}) = 0$. Moreover, $X = a, b$ and $a + b$ cannot satisfy Case 2, simultaneously. This is because $X = a$ is solution if $a^2 + b^2 + ab + a\gamma = 0$ along with $\text{Tr}_1^n(a^{2^t+1}) = 1$ and $\text{Tr}_1^n(b^{2^t+1}) = 0 = \text{Tr}_1^n((a + b)^{2^t+1})$. Similarly, $X = b$ is solution if $a^2 + b^2 + ab + b\gamma = 0$ and $\text{Tr}_1^n(b^{2^t+1}) = 1$ and $\text{Tr}_1^n(a^{2^t+1}) = 0 = \text{Tr}_1^n((a + b)^{2^t+1})$. Finally, $X = a + b$ is solution if $a^2 + b^2 + ab + (a + b)\gamma = 0$ and $\text{Tr}_1^n((a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n(a^{2^t+1}) = 0 = \text{Tr}_1^n((b^{2^t+1}))$. Summarizing the above, we get at most one solution of Case 2 when $X \in \{a, b, a + b\}$. For the other values of X , one can get a unique solution $X' \in \mathbb{F}_{2^n}$ satisfying $X'^2 = a^2 + b^2 + ab + \frac{ab(a + b)}{\gamma}$, $\text{Tr}_1^n(X'^{2^t+1}) = 1$ and $\text{Tr}_1^n((X' + a)^{2^t+1}) = \text{Tr}_1^n((X' + b)^{2^t+1}) = \text{Tr}_1^n((X' + a + b)^{2^t+1}) = 0$.

Case 3 Here, $N_2 = N_3$, because if X is solution for Case 2, then $X + a$ will satisfy Case 3 and hence Case 3 has at most two solutions.

Case 4 Similar to Case 3, we have $N_2 = N_4$, because if X is a solution for Case 2, then $X + b$ will satisfy Case 4 and hence Case 4 has at most two solutions.

Case 5 Similar to Case 2, we have $N_2 = N_5$.

Summarizing Cases 2–5, we have

$$X \in \begin{cases} \{0, a, b, a + b\} & \text{if } a^2 + b^2 + ab + a\gamma = 0, \text{Tr}_1^n(a^{2^t+1}) = 1 \text{ and } \\ & \text{Tr}_1^n(b^{2^t+1}) = 0 = \text{Tr}_1^n((a + b)^{2^t+1}), \\ & \text{or, if } a^2 + b^2 + ab + b\gamma = 0, \text{Tr}_1^n(b^{2^t+1}) = 1 \text{ and } \\ & \text{Tr}_1^n(a^{2^t+1}) = 0 = \text{Tr}_1^n((a + b)^{2^t+1}), \text{ or,} \\ & a^2 + b^2 + ab + (a + b)\gamma = 0, \text{Tr}_1^n((a + b)^{2^t+1}) = 1 \\ & \text{and } \text{Tr}_1^n(b^{2^t+1}) = 0 = \text{Tr}_1^n(a^{2^t+1}), \\ \{X', X' + a, X' + b, X' + a + b\} & \text{if } \text{Tr}_1^n(X'^{2^t+1}) = 1 \text{ and } \text{Tr}_1^n((X' + a)^{2^t+1}) = 0 \\ & \text{Tr}_1^n((X' + b)^{2^t+1}) = 0 = \text{Tr}_1^n((X' + a + b)^{2^t+1}), \end{cases} \tag{6.9}$$

where $X'^2 = a^2 + b^2 + ab + \frac{ab(a + b)}{\gamma}$ and $\gamma \notin \{a, b, a + b\}$.

Case 6 In this case, we have:

$$\frac{1}{X + \gamma} + \frac{1}{X + a + \gamma} + \frac{1}{X + b} + \frac{1}{X + a + b} = 0, \tag{6.10}$$

where $\text{Tr}_1^n(X^{2^t+1}) = \text{Tr}_1^n((X + a)^{2^t+1}) = 1$ and $\text{Tr}_1^n((X + b)^{2^t+1}) = \text{Tr}_1^n((X + a + b)^{2^t+1}) = 0$. If $\gamma = b$, then $\text{Tr}_1^n(b^{2^t+1}) = 0$, and this will give us $0 = \text{Tr}_1^n((X + b)^{2^t+1}) = \text{Tr}_1^n(X^{2^t+1}) = 1$. Hence, there is no solution corresponding to $\gamma = b$. Similarly, if $\gamma = a + b$, then $\text{Tr}_1^n((a + b)^{2^t+1}) = 0$, but this will give us a contradiction as $0 = \text{Tr}_1^n((X + a + b)^{2^t+1}) = \text{Tr}_1^n(X^{2^t+1}) = 1$.

Now, let $\gamma \notin \{b, a + b\}$, then $X \in \{\gamma, a + \gamma\}$ does not satisfy (6.10) and $X \in \{b, a + b\}$ satisfy (6.10) if $\frac{1}{a} + \frac{1}{b + \gamma} + \frac{1}{a + b + \gamma} = 0$, which is the same as $a^2 + b^2 + \gamma^2 + a(b + \gamma) = 0$. Substituting $b + \gamma = Z$, we can rewrite the previous equation as $Z^2 + aZ + a^2 = 0$, which has no solution when n is odd as $\text{Tr}_1^n(1) \neq 0$. For even n , $a^2 + b^2 + \gamma^2 + a(b + \gamma) = 0$ holds for the pairs $\{(a, \gamma + a\omega), (a, \gamma + a\omega^2)\}$ in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Thus, $X \in \{b, a + b\}$ satisfy (6.10) for the pairs $\{(a, \gamma + a\omega), (a, \gamma + a\omega^2)\}$, where $a \in \mathbb{F}_{2^n}$, n is even and also $\text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n(a^{2^t+1}) = 0$.

Case 7 Due to symmetry in a and b , we have $N_7 = N_6$, and hence it can have at most two solutions $\{a, a + b\}$, when n is even and $a^2 + b^2 + \gamma^2 + b(a + \gamma) = 0$ for the pairs $(a, b) = \{(\gamma + b\omega, b), (\gamma + b\omega^2, b)\}$ in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying $\text{Tr}_1^n(a^{2^t+1}) = 1 = \text{Tr}_1^n((a + b)^{2^t+1})$ and $\text{Tr}_1^n(b^{2^t+1}) = 0$.

Case 8 Here, we have

$$\frac{1}{X + \gamma} + \frac{1}{X + a} + \frac{1}{X + b} + \frac{1}{X + a + b + \gamma} = 0,$$

where $\text{Tr}_1^n(X^{2^t+1}) = \text{Tr}_1^n((X + a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n((X + b)^{2^t+1}) = \text{Tr}_1^n((X + a)^{2^t+1}) = 0$. If $\gamma \in \{a, b\}$, then there does not exist any solution $X \in \mathbb{F}_{2^n}$. Let $\gamma \notin \{a, b\}$, then clearly $X = \gamma$ and $X = a + b + \gamma$ does not satisfy the above equation. Clearly, $X = a$ and $X = b$ are solutions only when $a^2 + b^2 + \gamma^2 + ab + (a + b)\gamma = 0$, $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = 1$ and $\text{Tr}_1^n((a + b)^{2^t+1}) = 0$. Otherwise, there does not exist any solution in this case.

Case 9 By the same arguments as in Case 8, we have $X = 0$ and $X = a + b$ as solutions, when $a^2 + b^2 + \gamma^2 + ab + (a + b)\gamma = 0$, $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = 1$ and $\text{Tr}_1^n((a + b)^{2^t+1}) = 0$.

Case 10 Using a similar approach as in Case 7, we have at most two solutions $\{0, b\}$, only when n is even and $a^2 + b^2 + \gamma^2 + b(a + \gamma) = 0$ for the pairs $(a, b) = \{(\gamma + b\omega, b), (\gamma + b\omega^2, b)\}$ in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying the required trace conditions in this case.

Case 11 Following similar reasoning as in Case 6, there are at most two solutions, $\{0, a\}$, which occur only when n is even and $a^2 + b^2 + \gamma^2 + a(b + \gamma) = 0$. These solutions correspond to the pairs $(a, b) = \{(\gamma + b\omega, b), (\gamma + b\omega^2, b)\}$ in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ that satisfy the trace conditions required for this case.

Summarizing Case 6, Case 7, Case 8, Case 9, Case 10 and Case 11, we get $X \in \{0, a, b, a + b\}$ either if $\gamma \notin \{b, a + b\}$, $(a, b) \in \{(a, \gamma + a\omega), (a, \gamma + a\omega^2)\}$, $\text{Tr}_1^n(b^{2^t+1}) = 1 = \text{Tr}_1^n((a + b)^{2^t+1})$ and $\text{Tr}_1^n(a^{2^t+1}) = 0$, or if $\gamma \notin \{a, a + b\}$, $(a, b) \in \{(\gamma + b\omega, b), (\gamma + b\omega^2, b)\}$, $\text{Tr}_1^n(a^{2^t+1}) = 1 = \text{Tr}_1^n((a + b)^{2^t+1})$ and

$\text{Tr}_1^n(b^{2^t+1}) = 0$, or if $\gamma \notin \{a, b\}$, $a^2 + b^2 + \gamma^2 + ab + (a+b)\gamma = 0$, $\text{Tr}_1^n(a^{2^t+1}) = 1 = \text{Tr}_1^n(b^{2^t+1})$ and $\text{Tr}_1^n((a+b)^{2^t+1}) = 0$.

Case 12 When $\gamma \in \{a, b, a+b\}$, Case 12 has no solutions $X \in \mathbb{F}_{2^n}$. Hence, assume that $\gamma \notin \{a, b, a+b\}$. Then $X \in \{\gamma, a+\gamma, b+\gamma\}$ are not the solutions of Case 12 as $\text{Tr}_1^n(\gamma^{2^t+1}) = 0$, and $X = a+b$ is solution of Case 12 if $a^2 + b^2 + \gamma^2 + ab = 0$ and $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a+b)^{2^t+1}) = 1$. When $X \notin \{\gamma, a+\gamma, b+\gamma, a+b\}$, then Case 12 can have a unique solution X_{12} in \mathbb{F}_{2^n} such that $X_{12}^2 = \gamma^2 + ab + \frac{ab(a+b)}{\gamma}$ and the given conditions on trace are satisfied. Hence, this case has at most two solutions $a+b$ and X_{12} satisfying the above discussed conditions.

Case 13 Consider the following equation

$$\frac{1}{X+\gamma} + \frac{1}{X+a} + \frac{1}{X+b+\gamma} + \frac{1}{X+a+b+\gamma} = 0.$$

Clearly, $X \in \{\gamma, b+\gamma, a+b+\gamma\}$ are not solutions of the above equation. Also, $X = a$ is solution only when $a^2 + b^2 + \gamma^2 + ab = 0$ and $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a+b)^{2^t+1}) = 1$. Otherwise, it can have at most one solution X_{13} satisfying $X_{13}^2 = b^2 + \gamma^2 + ab + \frac{ab(a+b)}{\gamma}$, $\text{Tr}_1^n(X_{13}^{2^t+1}) = \text{Tr}_1^n((X_{13} + b)^{2^t+1}) = \text{Tr}_1^n((X_{13} + a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n((X_{13} + a)^{2^t+1}) = 0$.

Case 14 Similar to Case 12, $X = 0$ is solution only when $a^2 + b^2 + \gamma^2 + ab = 0$ and $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a+b)^{2^t+1}) = 1$. Otherwise, it can have at most one solution X_{14} satisfying $X_{14}^2 = a^2 + b^2 + \gamma^2 + ab + \frac{ab(a+b)}{\gamma}$, $\text{Tr}_1^n((X_{14} + a)^{2^t+1}) = \text{Tr}_1^n((X_{14} + b)^{2^t+1}) = \text{Tr}_1^n((X_{14} + a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n(X_{14}^{2^t+1}) = 0$.

Case 15 Similar to Case 13, we can have at most two solutions $X = b$ when $a^2 + b^2 + \gamma^2 + ab = 0$ and $\text{Tr}_1^n(a^{2^t+1}) = \text{Tr}_1^n(b^{2^t+1}) = \text{Tr}_1^n((a+b)^{2^t+1}) = 1$ and $X = X_{15}$ satisfying $X_{15}^2 = a^2 + \gamma^2 + ab + \frac{ab(a+b)}{\gamma}$, $\text{Tr}_1^n(X_{15}^{2^t+1}) = \text{Tr}_1^n((X_{15} + a)^{2^t+1}) = \text{Tr}_1^n((X_{15} + a + b)^{2^t+1}) = 1$ and $\text{Tr}_1^n((X_{15} + b)^{2^t+1}) = 0$.

Summarizing Case 12, Case 13, Case 14 and Case 15, we have the following,

$$X \in \begin{cases} \{0, a, b, a+b\} & \text{if } a^2 + b^2 + \gamma^2 + ab = 0, \text{Tr}_1^n(a^{2^t+1}) = 1 \text{ and} \\ & \text{Tr}_1^n(b^{2^t+1}) = 1 = \text{Tr}_1^n((a+b)^{2^t+1}), \\ \{X_{12}, X_{13}, X_{14}, X_{15}\} & \text{if } \text{Tr}_1^n(X_{12}^{2^t+1}) = 1 = \text{Tr}_1^n(X_{13})^{2^t+1} \\ & \text{Tr}_1^n(X_{15})^{2^t+1} = 1 \text{ and } \text{Tr}_1^n(X_{14})^{2^t+1} = 0, \end{cases}$$

where $X_{12}^2 = \gamma^2 + ab + \frac{ab(a+b)}{\gamma}$ and $\gamma \notin \{a, b, a+b\}$.

Case 16 This case has no solution $X \in \mathbb{F}_{2^n}$. This is because the only solutions possible are $X \in \{\gamma, a+\gamma, b+\gamma, a+b+\gamma\}$, when n is even, but this would contradict the fact that $\text{Tr}_1^n(\gamma^{2^t+1}) = 0$.

Notice that Case 2 and Case 14 cannot occur together. This is because if X satisfies Case 2, then $X + \gamma$ satisfies Case 14, which would further imply that $\text{Tr}_1^n((X + \gamma)^{2^t+1}) = 0$. But as $\gamma \in \mathbb{F}_{2^{2t}}$ and $\text{Tr}_1^n((\gamma)^{2^t+1}) = 0$, this will give us $\text{Tr}_1^n(X^{2^t+1}) = 0$, which is not possible, as from Case 2, we have $\text{Tr}_1^n(X^{2^t+1}) = 1$.

Hence Case 2 and Case 14 cannot occur together. Similarly, the pairs (Case 3, Case 13), (Case 4, Case 15), (Case 5, Case 12) cannot occur simultaneously. Summarizing, we conclude that we have at most 8 solutions of (6.8) in \mathbb{F}_{2^n} . \square

7 Conclusion

In this paper, we extend the work of Boukerrou et al. [5] and Li et al. [21] by computing the second-order zero differential spectra of some APN power functions over finite fields of odd characteristic and functions with low differential uniformity over finite fields of even and odd characteristic in order to derive additional cryptographic properties of these functions. It is worth noting that all of these maps exhibit a low second-order zero differential uniformity. We also connect this concept with the sum-freedom concept, which extends the vanishing affine subspaces (of dimension 2) concept, in even characteristic. We compute, via our method, the number of vanishing flats, for many of our investigated functions (in even characteristic). Surely, we believe that it is worthwhile to look into more functions with low differential uniformity and investigate their second-order zero differential spectrum, and perhaps even extend the concept of vanishing affine subspaces, or sum-freedom to odd characteristic (though applications are not yet visible, for such an extension).

Acknowledgements The authors would like to thank the editor for the prompt handling of our paper, and they want to extend their thanks and appreciation to the very professional referees, who provided beneficial and constructive comments to improve our paper.

References

- Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schefneger, M.: Feistel structures for MPC, and More. In: Sako, K., Schneider, S., Ryan, P. (eds.) *Computer Security-ESORICS 2019*, LNCS 11736. Springer, Cham (2019)
- Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.* **4**(1), 3–72 (1991)
- Blondeau, C., Canteaut, A., Charpin, P.: Differential properties of $X \rightarrow X^{2^f-1}$. *IEEE Trans. Inf. Theory* **57**(12), 8127–8137 (2011)
- Blondeau, C., Perrin, L.: More differentially 6-uniform power functions. *Des. Codes Cryptogr.* **73**, 487–505 (2014)
- Boukerrou, H., Huynh, P., Lallemand, V., Mandal, B., Minier, M.: On the Feistel counterpart of the boomerang connectivity table. *IACR Trans. Symmetric Cryptol.* **1**, 331–362 (2020)
- Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic S-boxes. *IACR Trans. Symmetric Cryptol.* **3**, 290–310 (2018)
- Carlet, C.: Two generalizations of almost perfect nonlinearity. *Cryptology ePrint Archive* <https://ia.cr/2024/841> (2024)
- Carlitz, L.: Kloosterman sums and finite field extensions. *Acta Arith.* **16**(2), 179–183 (1969)
- Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) *Adv.*, pp. 356–365. *Crypt - EUROCRYPT '94*, LNCS 950, Springer (1995)
- Choi, S., Hong, S., No, J., Chung, H.: Differential spectrum of some power functions in odd prime characteristic. *Finite Fields Appl.* **21**, 11–29 (2013)
- Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen, J., Rijmen, V. (eds.) *Advances in Cryptology-EUROCRYPT'18*, LNCS 10821, pp. 683–714. Springer, Cham (2018)
- Dickson, L.E.: Criteria for the irreducibility of functions in a finite field. *Bull. Amer. Math. Soc.* **13**, 1–8 (1906)
- Eddahmani, S., Mesnager, S.: Explicit values of the DDT, the BCT, the FBCT, and the FBCT of the inverse, the gold, and the Bracken-Leander S-boxes. *Cryptogr. Commun.* **14**, 1301–1344 (2022)
- Garg, K., Hasan, S.U., Riera, C., Stănică, P.: The second-order zero differential spectra of some APN and other maps over finite fields. *arXiv preprint arXiv:2310.13775* (2023)

15. Hasan, S.U., Pal, M., Stănică, P.: The c -Differential Uniformity and Boomerang Uniformity of Two Classes of Permutation Polynomials. *IEEE Trans. Inf. Theory* **68**, 679–691 (2022)
16. Helleseeth, T., Chunming, R., Daniel, S.: New families of almost perfect nonlinear power mappings. *IEEE Trans. Inf. Theory* **45**(2), 475–485 (1999)
17. Helleseeth, T., Sandberg, D.: Some power mappings with low differential uniformity. *Appl. Algebra Eng. Commun. Comput.* **8**, 363–370 (1997)
18. Kuroda, M., Tsujie, S.: A generalization of APN functions for odd characteristic. *Finite Fields and Their Applications* **47**, 64–84 (2017)
19. Leonard, P.A., Williams, K.S.: Quartics over $GF(2^n)$. *Proc. Amer. Math. Soc.* **36**(2), 347–350 (1972)
20. Li, S., Meidl, W., Polujan, A., Pott, A., Riera, C., Stănică, P.: Vanishing Flats: A Combinatorial Viewpoint on the Planarity of Functions and Their Applications. *IEEE Trans. Inf. Theory* **66**(11), 7101–7112 (2020)
21. Li, X., Yue, Q., Tang, D.: The second-order zero differential spectra of almost perfect nonlinear functions and the inverse function in odd characteristic. *Cryptogr. Commun.* **14**(3), 653–662 (2022)
22. Lidl, R., Niederreiter, H.: *Finite Fields*. Cambridge University Press, (1997)
23. Man, Y., Li, N., Xiang, Z., Zeng, X.: On the second-order zero differential spectra of some power functions over finite fields. *Cryptogr. Commun.* (2024) <https://doi.org/10.1007/s12095-024-00740-z>
24. Man, Y., Mesnager, S., Li, N., Zeng, X., Tang, X.: In-depth analysis of S-boxes over binary finite fields concerning their differential and Feistel boomerang differential uniformities. *Discrete Math.* **347**(12) (2024). <https://doi.org/10.1016/j.disc.2024.114185>
25. Mesnager, S., Mandal, B., Msahli, M.: Survey on recent trends towards generalized differential and boomerang uniformities. *Cryptogr. Commun.* **14**, 691–735 (2022)
26. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseeth, T. (ed.) *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, pp. 55–64. Springer, Heidelberg (1994)
27. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract.). In: Biryukov, A. (ed.) *Fast Software Encryption-FSE 2007*, LNCS 4593, pp. 181–195. Springer, Berlin, Heidelberg (2007)
28. Tan, Y., Qu, L., Tan, C.H., Li, C.: New families of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. In: Helleseeth, T., Jedwab, J. (eds.) *Sequences and Their Applications-SETA*, LNCS 7280, pp. 25–39. Springer, Heidelberg, Germany (2012)
29. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) *Fast Software Encryption-FSE 1999*. LNCS, vol. 1636, pp. 156–170. Springer, Berlin, Heidelberg (1999)
30. Yan, H., Zhou, Z., Weng, J., Wen, J., Helleseeth, T., Wang, Q.: Differential spectrum of Kasami power permutations over odd characteristic finite fields. *IEEE Trans. Inf. Theory* **65**(10), 6819–6826 (2019)
31. Zha, Z., Wang, X.: Almost perfect nonlinear power functions in odd characteristic. *IEEE Trans. Inf. Theory* **57**(7), 4826–4832 (2011)
32. Ziran, T., Zeng, X.: Non-monomial permutations with differential uniformity six. *J. Syst. Sci. & Complexity* **31**(4), 1078–1089 (2018)

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