

The second-order zero differential spectra of some APN and other maps over finite fields

Kirpa Garg * and Sartaj Ul Hasan †

*Department of Mathematics
Indian Institute of Technology Jammu
Jammu 181221, India
*kirpa.garg@gmail.com
†sartaj.hasan@iitjammu.ac.in*

Constanza Riera 

*Department of Computer Science
Electrical Engineering and Mathematical Sciences
Western Norway University of Applied Sciences
Bergen 5020, Norway
csr@hvl.no*

Pantelimon Stănică 

*Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, USA
pstanica@nps.edu*

Received 29 February 2024

Accepted 3 October 2024

Published 13 March 2025

Communicated by Mrinmoy Datta

Dedicated to Professor Sudhir R. Ghorpade on the occasion of his 60th birthday.

The Feistel Boomerang Connectivity Table and the related notion of F -Boomerang uniformity (also known as the second-order zero differential uniformity) have been recently introduced by [H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier, On the Feistel counterpart of the boomerang connectivity table, *IACR Trans. Symmetric Cryptol.* **1** (2020) 331–362]. In the same paper, a characterization of almost perfect nonlinear (APN) functions over fields of even characteristic in terms of second-order zero differential uniformity was also given. Here, we find a sufficient condition for an odd or even function over fields of odd characteristic to be an APN function, in terms of second-order zero differential uniformity. Moreover, we compute the second-order zero differential spectra of several APN or other low differential uniform functions, and show that our considered functions also have low second-order zero differential uniformity,

†Corresponding author.

though it may vary widely, unlike the case for even characteristic, when it is always zero.

Keywords: Finite fields; almost perfect nonlinear functions; second-order zero differential spectra; second-order zero differential uniformity.

Mathematics Subject Classification 2020: 12E20, 11T06, 94A60

1. Introduction

In symmetric-key cryptography, the substitution box (S-box) plays a crucial role in most of modern block ciphers. Recall that the S-boxes are functions over finite fields having even characteristic. However, recently, some cryptographic primitives, such as GMiMC [1], have been proposed over finite fields of odd characteristic. This suggests that studying the cryptographic properties of functions over fields with odd characteristic is equally important and useful. There are many cryptographic attacks that are possible on these block ciphers. One of the most powerful attacks introduced by Biham and Shamir [2] in 1991 is known as differential cryptanalysis. Further, to quantify the degree of resistance of these functions against differential attacks, Nyberg [21] introduced the notion of differential uniformity. The smaller the differential uniformity of a function, the stronger its resistance to the differential attack.

Let \mathbb{F}_q denote the finite field with $q = p^n$ elements where n is a positive integer and p is a prime number. We use the notation \mathbb{F}_q^* to represent the multiplicative cyclic group of nonzero elements of \mathbb{F}_q and $\mathbb{F}_q[X]$ to represent the ring of polynomials in one variable X with coefficients in \mathbb{F}_q . Let F be a function from \mathbb{F}_q to \mathbb{F}_q , and a be any element in \mathbb{F}_q , then we define the derivative of F in the direction a as $D_F(X, a) := F(X + a) - F(X)$ for all $X \in \mathbb{F}_q$. The Difference Distribution Table (DDT) entry $\Delta_F(a, b)$ for any $a, b \in \mathbb{F}_q$, at (a, b) is given by the number of solutions $X \in \mathbb{F}_q$ satisfying $D_F(X, a) = b$. 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 say that the function F is a perfect nonlinear (PN) function if $\Delta_F = 1$ and an almost PN (APN) function if $\Delta_F = 2$.

The boomerang attack is another significant cryptanalysis technique introduced by Wagner [25] for analyzing block ciphers. This attack can be seen as a variant of the classical differential attack. At Eurocrypt 2018, Cid *et al.* [9] analyze the boomerang style attack in a better way by introducing a new tool known as the Boomerang Connectivity Table (BCT). To quantify the resistance of a function against the boomerang attack, Boura and Canteaut [5] introduced the concept of boomerang uniformity. However, this was valid only for Substitution–Permutation Network (SPN) ciphers and the obvious question was to define its equivalent for Feistel ciphers. It is important to note that Feistel network-based ciphers, such as 3-DES and CLEFIA [24], are equally significant in block cipher design as SPN. Boukerrou *et al.* [4] addressed the requirement for a counterpart to the BCT, and

extended this concept to Feistel ciphers. They introduced the Feistel BCT (FBCT) as an extension for Feistel ciphers, where the S-boxes may not be permutations. Further, these coefficients of the FBCT are related to the second-order zero differential spectra of the functions over finite fields.

In [4], the authors studied the FBCT entries for some APN and inverse functions over finite fields of even characteristics. Li *et al.* [18] extended this research to odd characteristics, and studied the second-order zero differential spectra of some APN power functions over odd characteristic. Furthermore, Eddahmani and Mesnager [13] investigated the entries of the FBCT for the inverse, Gold, and Bracken–Leander functions over finite fields with even characteristic. Recently, Man *et al.* [19] also computed the FBCT entries for a specific power function, $F(X) = X^{2^{m+1}-1}$ over \mathbb{F}_{2^n} , where $n = 2m$ or $n = 2m + 1$. Further, Garg *et al.* [15] also considered several APN or other low differential uniform functions in both even and odd characteristics and investigated their second-order zero differential spectra.

It was shown in [4] that for the finite field of even characteristic, all the non-trivial coefficients of FBCT of F are 0 if and only if F is APN, or equivalently F is second-order zero differentially 0-uniform if and only if it is APN. In this paper, we show that, for odd characteristic, if an odd or even function F is second-order zero differentially 1-uniform then it has to be an APN function. The converse, however, does not hold. We further compute the second-order zero differential spectra of some other functions that are APN, or have other low differential uniformity over finite fields of both even and odd characteristic. It may be noted that, on the one hand, the Bracken–Leander function given in [13] has low differential uniformity but high second-order zero differential uniformity. On the other hand, PN functions [18, Lemma 2.5] in odd characteristic and APN functions [18, Lemma 2.6] in even characteristic have low second-order differential uniformity. In view of this, it appears that both notions are independent of each other. Thus, to measure the strength of a function from a cryptographic viewpoint, we need to look at several other properties, including second-order zero uniformity, rather than just focusing on low differential uniformity. The reader might wonder why we considered a seemingly non-unified list of functions, but the reason is rather simple: we want to analyze some known classes of functions as far as their second-order zero differential uniformity is concerned.

This paper is structured as follows. In Sec. 2, we recall some definitions and results required later. In Sec. 3, we give the only known constraint with respect to the second-order zero differential uniformity, for functions that are not PN in odd characteristic, namely, we show that an odd or even function F , which is second-order zero differentially 1-uniform must be APN. We also consider the second-order zero differential spectra of some functions (including APNs) over finite fields of odd characteristic. Furthermore, Sec. 4 explores the second-order zero differential spectrum of some (partial) 0-APN functions and extensions. Finally, we conclude the paper in Sec. 5.

2. Preliminaries

In this section, we recall some definitions and results that we will use in subsequent sections.

Definition 2.1. For p an odd prime, n a positive integer, and $q = p^n$, we let χ be the quadratic character of \mathbb{F}_q , χ , be defined for each $X \in \mathbb{F}_q$ by

$$\chi(X) := \begin{cases} 0 & \text{if } X = 0, \\ 1 & \text{if } X \text{ is a square of an element of } \mathbb{F}_q^*, \\ -1 & \text{otherwise.} \end{cases}$$

Definition 2.2 ([6]). Let F be a function from \mathbb{F}_{2^n} to itself. For a fixed $X_0 \in \mathbb{F}_{2^n}$, we call F as X_0 -APN (or partially APN) if all $(X, Y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ satisfying

$$F(X_0) + F(X) + F(Y) + F(X_0 + X + Y) = 0,$$

belong to the curve $(X_0 + X)(X_0 + Y)(X + Y) = 0$.

Definition 2.3 ([4, 18]). For $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $q = p^n$, n a positive integer, 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

$$\nabla_F(a, b) := \#\{X \in \mathbb{F}_q : F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0\}. \quad (1)$$

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

Definition 2.4 (FBCT [4]). Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. The *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 2.5 (F -Boomerang uniformity [4, 18]). 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 the coefficients of 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.

The following lemma gives a characterization of APN functions in terms of their second-order zero differential uniformity.

Lemma 2.6 ([18, Lemma 2.6]). F is an APN function of \mathbb{F}_{2^n} if and only if

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

where $a, b \in \mathbb{F}_{2^n}$. Moreover, F is second-order zero differential 0-uniform.

The characterization of PN functions is given by the following lemma.

Lemma 2.7 ([18, Lemma 2.5]). *F is a PN function of \mathbb{F}_{p^n} if and only if*

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

where $a, b \in \mathbb{F}_{p^n}$. Moreover, *F is second-order zero differential 0-uniform.*

We will be using the following result by Coulter and Henderson [10] to determine the roots of trinomial $X^{p^k} - AX - B$ in some of the results.

Lemma 2.8 ([10, Theorem 3]). *Let k be a non-negative integer and $F(X) = X^{p^k} - AX - B \in \mathbb{F}_{p^n}[X]$, $A \neq 0$. Let $d = \gcd(k, n)$, $m = n/d$ and Tr_d^n be the relative trace from \mathbb{F}_{p^n} to \mathbb{F}_{p^d} . For $0 \leq i \leq m - 1$, define $t_i = \sum_{j=i}^{m-2} p^{k(j+1)}$. Put $\alpha_0 = A$ and $\beta_0 = B$. If $m > 1$, then for $1 \leq r \leq m - 1$, we let $\alpha_r = A^{1+p^k+p^{2k}+\dots+p^{kr}}$ and $\beta_r = \sum_{i=0}^r A^{s_i} B^{p^{k_i}}$ where $s_i = \sum_{j=i}^{r-1} p^{k(j+1)}$ for $0 \leq i \leq r - 1$ and $s_r = 0$.*

- (i) *If $\alpha_{m-1} = 1$ and $\beta_{m-1} \neq 0$ then the trinomial F has no roots in \mathbb{F}_{p^n} .*
- (ii) *If $\alpha_{m-1} \neq 1$ then F has a unique root, namely $X = \frac{\beta_{m-1}}{1-\alpha_{m-1}}$.*
- (iii) *If $\alpha_{m-1} = 1$, $\beta_{m-1} = 0$, F has p^d roots in \mathbb{F}_{p^n} given by $x + \delta\tau$, where $\delta \in \mathbb{F}_{p^d}$, τ is fixed in \mathbb{F}_{p^n} with $\tau^{p^k-1} = A$ (that is, a $(p^k - 1)$ -root of A), and, for any $c \in \mathbb{F}_{p^*}^*$, satisfying $\text{Tr}_d(c) \neq 0$ then $x = \frac{1}{\text{Tr}_d(c)} \sum_{i=0}^{m-1} (\sum_{j=0}^i c^{p^{kj}}) A^{t_i} B^{p^{k_i}}$.*

The following two lemmas discuss the solutions of quadratic and cubic equations, respectively.

Lemma 2.9 ([14, Lemma 11]). *Let n be a positive integer. The equation $X^2 + aX + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, has two solutions in \mathbb{F}_{2^n} if $\text{Tr}(\frac{b}{a^2}) = 0$, and no solution otherwise.*

Lemma 2.10 ([26, Theorem 1]). *The factorization of $F(X) = X^3 + X + a$ over \mathbb{F}_{2^n} with $a \neq 0$ is characterized as follows:*

- (1) *F is a product of three linear factors if and only if $\text{Tr}(\frac{1}{a}) = \text{Tr}(1)$, t_1 and t_2 are cubes in \mathbb{F}_{2^n} (n even), $\mathbb{F}_{2^{2n}}$ (n odd), where t_1, t_2 are roots of $t^2 + at + 1 = 0$.*
- (2) *F is a product of one linear and one quadratic factor if and only if $\text{Tr}(\frac{1}{a}) \neq \text{Tr}(1)$.*
- (3) *F is irreducible if and only if $\text{Tr}(\frac{1}{a}) = \text{Tr}(1)$, t_1 and t_2 are not cubes in \mathbb{F}_{2^n} (n even), $\mathbb{F}_{2^{2n}}$ (n odd), where t_1, t_2 are roots of $t^2 + at + 1 = 0$.*

Recently, Budaghyan and Pal [8] obtained a new class of binomials with low differential uniformity, stated below. In the next section, we will look at its second-order zero differential uniformity.

Lemma 2.11 ([8, Theorem 4.2]). *Let p be an odd prime and n be a positive integer. Then the binomial $F(X) = X^{p^n-1} + uX^2$, $u \in \mathbb{F}_{p^n}^*$ over \mathbb{F}_{p^n} is APN if*

$$\begin{cases} \chi(u) = -1 & \text{and } p^n \equiv 1 \pmod{4}, \\ \chi(u) = 1 & \text{and } p^n \equiv 3 \pmod{4}, \end{cases}$$

and differentially 3-uniform, otherwise.

3. The Second-Order Zero Differential Spectrum for Functions Over Finite Fields of Odd Characteristic

Boukerrou *et al.* [4] showed that all the nontrivial second-order zero differential spectra of APN functions in even characteristic are 0 (see Lemma 2.6). Further, Li *et al.* [18] gave the characterization of PN functions in terms of the second-order zero differential spectra over \mathbb{F}_{p^n} for an odd prime p , as given in Lemma 2.7. Surely, a natural question is whether there are other constraints on the second-order zero differential spectra for APN functions in odd characteristic. In the following theorem, we show that for any odd or even function F over \mathbb{F}_{p^n} , where p is an odd prime, if the second-order differential uniformity is 1, then F must be an APN function. Recall that F is odd if and only if $F(-X) = -F(X) \forall X \in \mathbb{F}_{p^n}$, while F is even if and only if $F(-X) = F(X) \forall X \in \mathbb{F}_{p^n}$. Trivially, all power functions $F(X) = X^d$ are either odd (if d is odd) or even (if d is even), so this result encompasses (but it does not restrict to) power functions.

Theorem 3.1. *Let F be an odd or even function over \mathbb{F}_{p^n} , where p is an odd prime. If the differential uniformity Δ_F of F is strictly greater than 2, then the second-order zero differential uniformity ∇_F of F is never equal to 1. In other words, if $\nabla_F = 1$, then F is an APN function over \mathbb{F}_{p^n} .*

Proof. It is given that the function $F(X)$ has differential uniformity strictly greater than 2. Assume on the contrary that $\nabla_F = 1$. Now, for $a, b \in \mathbb{F}_{p^n} \setminus \{0\}$, we consider the equation

$$F(X + a + b) - F(X + b) - F(X + a) + F(X) = 0. \tag{2}$$

Since F is odd or even, it is straightforward to see that if X is a solution of Eq. (2) then $-(X + a + b)$ is also a solution of Eq. (2). Since $\Delta_F \geq 3$, there exists $(a', b') \in \mathbb{F}_{p^n} \setminus \{0\} \times \mathbb{F}_{p^n}$ such that $\Delta_F(a', b') \geq 3$, that is, the difference equation $F(Z + a') - F(Z) = b'$ has at least three distinct solutions in \mathbb{F}_{p^n} . Suppose X_1, X_2 and X_3 are any three distinct solutions to $F(Z + a') - F(Z) = b'$ in \mathbb{F}_{p^n} . We may write $X_2 = X_1 + u$ and $X_3 = X_2 + v$ for some $u, v \in \mathbb{F}_{p^n}^*$. We now compute $\nabla_F(u, a')$ by simply looking at the solutions to the equation

$$F(X + u + a') - F(X + u) - F(X + a') + F(X) = 0. \tag{3}$$

It follows immediately that $X = X_1$ is a solution to Eq. (3), and as a consequence, $\nabla_F(u, a') \geq 1$. However, by our assumption that the second-order zero differential

uniformity of F is 1, we must have $\nabla_F(u, a') = 1$. As per our earlier observation, $-(X_1 + u + a')$ is also a solution to Eq. (3). Thus, in view of the fact that $\nabla_F(u, a') = 1$, we must have that $X_1 = -(X_1 + u + a')$, i.e. $X_1 = \frac{-(u+a')}{2}$. Hence, $X_2 = X_1 + u = \frac{u-a'}{2}$. Similarly, one can show that $\nabla_F(v, a') = 1$, with X_2 satisfying the equation

$$F(X + v + a') - F(X + v) - F(X + a') + F(X) = 0. \tag{4}$$

This will yield us $X_2 = \frac{-(v+a')}{2}$ by following the similar arguments as before. Now, comparing both expressions for X_2 , we obtain $u = -v$, which implies that $X_1 = X_3$. Thus, we get a contradiction to the fact that X_1 and X_3 are distinct. Together with Lemma 2.5, this gives that, if $\nabla_F = 1$, then F is an APN function over \mathbb{F}_{p^n} . This completes the proof of both statements of the theorem. \square

Remark 3.2. The converse of Theorem 3.1 does not hold in general. However, it holds true for an odd APN function. For instance, consider the function $F(X) = X^{14}$, which is APN over the finite field \mathbb{F}_{53} but has second-order zero differential uniformity 4. Moreover, the statement of Theorem 3.1 does not hold in general. To illustrate this, consider the function $F(X) = X^9 + X^4$, which is a differentially 3-uniform function over \mathbb{F}_{11} . However, it has second-order zero differential uniformity 1.

Remark 3.3. Note that the proof implies that, for F even or odd (p odd), if $\nabla_F = 1$, if for a certain a and b there is a solution X , then the solution is $X = -\frac{a+b}{2}$, since $X = -X - a - b$. Further, we note that, if F is odd, then $X = -\frac{a+b}{2}$ is always a solution.

Corollary 3.4. *If F is an odd function, then F is not PN.*

Proof. It follows directly from Remark 3.3 and Lemma 2.7. \square

Remark 3.5. Note that the proof also implies that, if F is an even function, the number of solutions to the equation is always even, unless $X = -X - a - b$ for some solution X , in which case $X = \frac{-a-b}{2}$. This implies that, unless $X = \frac{-a-b}{2}$ is a solution, the second-order zero differential uniformity of any even function F is even.

Remark 3.6. It is worth noting that since both Δ_F and ∇_F are invariant under extended affine (EA) equivalence [4], the theorem is also true for a function EA-equivalent to an even or odd function. Recall that two vectorial functions F, G on \mathbb{F}_{p^n} (for any characteristic p) are EA-equivalent if that there exist two affine permutations P, Q and an affine function A satisfying $G = P \circ F \circ Q + A$.

We next compute the second-order zero differential spectrum of the differentially low uniform binomial given in Lemma 2.11 (which is APN under some conditions of the parameter u).

Theorem 3.7. *Let p be an odd prime and n be a positive integer. Consider the binomial $F(X) = X^{p^n-1} + uX^2$, $u \in \mathbb{F}_{p^n}^*$ over \mathbb{F}_{p^n} . Then for $a, b \in \mathbb{F}_{p^n}$*

$$\nabla_F(a, b) = \begin{cases} p^n & \text{if } ab = 0, \\ 1 & \text{if } ab \neq 0, p \neq 3, a = -b \text{ and } -1 + abu = 0, \\ 2 & \text{if } ab \neq 0, p \neq 3, a = b \text{ and } -1 + 2abu = 0 \text{ or } 1 + abu = 0, \\ & \text{or } ab \neq 0, p \neq 3, a = -b \text{ and } 1 + 2abu = 0, \\ & \text{or } ab \neq 0, a \neq b, -b \text{ and } -1 + 2abu = 0 \text{ or } 1 + 2abu = 0, \\ 3 & \text{if } ab \neq 0, p = 3, a = -b \text{ and } -1 + abu = 0, \\ 4 & \text{if } ab \neq 0, p = 3, a = b, -1 + 2abu = 0 \text{ and } 1 + abu = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\nabla_F(a, b) \geq 3$ is possible only when $p = 3$. Hence, F is second-order zero differentially 2-uniform if $p \neq 3$ and when $p = 3$ it is second-order zero differential 4-uniform.

Proof. Now, 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 can write the above equation as

$$(X + a + b)^{p^n-1} - (X + b)^{p^n-1} - (X + a)^{p^n-1} + X^{p^n-1} + 2abu = 0. \tag{5}$$

Now, we divide our analysis in the following five cases.

Case 1. Let $X = 0$ satisfy Eq. (5), then

$$(a + b)^{p^n-1} - b^{p^n-1} - a^{p^n-1} + 2abu = 0.$$

For $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$, when $a = -b$, $X = 0$ is a solution if $-1 + abu = 0$. When $a \neq -b$, $X = 0$ is a solution if $-1 + 2abu = 0$.

Case 2. Let $X = -a$ satisfy Eq. (5), then

$$b^{p^n-1} - (-a + b)^{p^n-1} + a^{p^n-1} + 2abu = 0.$$

For $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^*$, when $a = b$, $X = -a$ is a solution if $1 + abu = 0$. When $a \neq b$, $X = -a$ is a solution if $1 + 2abu = 0$.

Case 3. Let $X = -b$. Due to the symmetry in Cases 2 and 3, we have $X = -b$ is a solution of Eq. (5) if $a = b$ and $1 + abu = 0$ or $a \neq b$ and $1 + 2abu = 0$.

Case 4. Let $X = -(a + b) \neq 0$. Then Eq. (5) has a solution only if $-1 + 2abu = 0$. Note that this excludes $a = -b$, in which case we obtain Case 1.

Case 5. Let $X \notin \{0, -a, -b, -(a + b)\}$. Then Eq. (5) has no solution in \mathbb{F}_{p^n} .

Clearly Cases 1-4 simultaneously give a solution of Eq. (5), or $X \in \{0, a, b, a + b\}$ are solutions of Eq. (5) when $a = b$, $-1 + 2abu = 0$ and $1 + abu = 0$. The conditions

further simplify to the equation $3abu = 0$, which is true only when $p = 3$. Thus, we get the desired claim. \square

Dobbertin *et al.* [12] showed that the power function $F(X) = X^{2 \cdot 3^{\frac{n-1}{2}} + 1}$ over \mathbb{F}_{3^n} for odd n is differentially 4-uniform. We next compute its second-order zero differential spectrum.

Theorem 3.8. *Let $F(X) = X^d$, where $d = 2 \cdot 3^{\frac{n-1}{2}} + 1$, be a function over \mathbb{F}_{3^n} , for odd n . Then for $a, b \in \mathbb{F}_{3^n}$*

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

where $m = \frac{n-1}{2}$. Moreover, F is second-order zero differentially 3-uniform.

Proof. For $a, b \in \mathbb{F}_{3^n}$, consider the following equation:

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

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

$$(X + a + b)^d - (X + b)^d - (X + a)^d + X^d = 0,$$

or equivalently

$$(Y + B + 1)^{2 \cdot 3^m + 1} - (Y + B)^{2 \cdot 3^m + 1} - (Y + 1)^{2 \cdot 3^m + 1} + Y^{2 \cdot 3^m + 1} = 0,$$

where $m = \frac{n-1}{2}$, $Y = \frac{X}{a}$ and $B = \frac{b}{a}$. The above equation can be further reduced to

$$(B + B^{3^m})Y^{3^m} + B^{3^m}Y + B^{3^m+1} + B^{3^m} - B^{2 \cdot 3^m} - B = 0,$$

which is equivalent to

$$(B + B^{3^m})Y^{3^m} + B^{3^m}Y - (B^{3^m} - B)(B^{3^m} - 1) = 0. \tag{6}$$

If $B = \pm 1$ (i.e. $a = \pm b$), then Eq. (6) has three solutions, namely, 0, 1 and 2. Let us now assume $a \neq \pm b$ and rewrite Eq. (6) as follows:

$$Y^{3^m} + \left(\frac{B^{3^m}}{B + B^{3^m}} \right) Y - \frac{(B^{3^m} - B)(B^{3^m} - 1)}{B + B^{3^m}} = 0. \tag{7}$$

We know from Remark 3.3 that for every entry $(1, B) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, there exists at least one solution $Y = -\frac{1+B}{2}$, as F is odd. Hence, using Lemma 2.8, we can further characterize the solutions of Eq. (7). In fact, if $\alpha_{n-1} = \left(\frac{-B^{3^m}}{B^{3^m} + B} \right)^{1+3^m+\dots+3^{(n-1)m}} = 1$, Eq. (7) has three solutions in \mathbb{F}_{p^n} , and otherwise one solution in \mathbb{F}_{p^n} . \square

In the following theorem, we consider the second-order zero differential uniformity of an APN function introduced in [17].

Theorem 3.9. *Let p be an odd prime and n be a positive integer. Let the APN function $F(X) = X^d$ over \mathbb{F}_{p^n} , where $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$, if $p^n \equiv 3 \pmod{8}$, or $d = \frac{p^n+1}{4}$, if $p^n \equiv 7 \pmod{8}$. Then the second-order zero differential uniformity of F is given by*

- (1) if $p = 3$, then $\nabla_F \leq 8$;
- (2) if $p > 3$, then $\nabla_F \leq 8$, if $\chi(2) = -1$, and $\nabla_F \leq 18$, if $\chi(2) = 1$.

Note that, under the conditions of our theorem, that is, $p^n \equiv 3, 7 \pmod{8}$, $\chi(2) = 1$ if and only if $p^n \equiv 7 \pmod{8}$.

Proof. The second-order zero differential uniformity equation for F at (a, b) (where $ab \neq 0$, or $a \neq -b$, since those cases are trivial) is

$$(X + a + b)^d - (X + b)^d - (X + a)^d + X^d = 0,$$

which, dividing by b^d and using the relabeling $X/b \mapsto X, a/b \mapsto a$, is equivalent to

$$(X + a + 1)^d - (X + 1)^d - (X + a)^d + X^d = 0. \tag{8}$$

If $X = 0, -1, -a, -a - 1$, then a must satisfy (since d is even) $(a + 1)^d - a^d = 1$, $(a - 1)^d - a^d = 1$, $(a - 1)^d - a^d = 1$, $(a + 1)^d - a^d = 1$, respectively. All of these cases allow only two values of a , since F is APN. In fact, from the proof of the APN-ness of this function in [17], there are no other solutions than $a = 0$, which is excluded. We thus can exclude the solutions $X = 0, -1, -a, -a - 1$.

We now assume that $X \notin \{0, -1, -a, -a - 1\}$. We next divide by X^d and label $Y = 1/X$. We thus get

$$(1 + (a + 1)Y)^d - (1 + Y)^d - (1 + aY)^d + 1 = 0.$$

We set $U_{\alpha Y} = (1 + \alpha Y)^d$, where $\alpha = 1, a, a + 1$. Observe that, as in [17], $2d \equiv \frac{p^n+1}{2} \pmod{p^n - 1}$, and so, $U_{\alpha Y}^2 = \chi(1 + \alpha Y) \cdot (1 + \alpha Y)$. Squaring the second-order zero differential uniformity equation $U_Y + U_{aY} = U_{(a+1)Y} + 1$, we get

$$\begin{aligned} &\chi(1 + Y)(1 + Y) + \chi(1 + aY)(1 + aY) + 2U_Y U_{aY} \\ &= \chi(1 + (a + 1)Y)(1 + (a + 1)Y) + 1 + 2U_{(a+1)Y}. \end{aligned} \tag{9}$$

We now consider 8 (though we combine some of these) cases depending upon the sign vector

$$(\chi(1 + Y), \chi(1 + aY), \chi(1 + (a + 1)Y)) = (\alpha, \beta, \gamma) \in \{\pm 1\}^3.$$

Case 1. Let $(\alpha, \beta, \gamma) = (1, 1, 1)$. Equation (9) becomes

$$1 + Y + 1 + aY + 2U_Y U_{aY} = 1 + (a + 1)Y + 1 + 2U_{(a+1)Y}, \quad \text{that is,}$$

$$U_Y U_{aY} = U_{(a+1)Y}, \quad \text{which, by squaring again, renders}$$

$$(1 + Y)(1 + aY) = 1 + (a + 1)Y, \quad \text{implying (since } Y \neq 0)$$

$$a = 0, \quad \text{an impossibility.}$$

Case 2. Let $(\alpha, \beta, \gamma) = (1, 1, -1)$. Equation (9) becomes

$$\begin{aligned}
 1 + Y + 1 + aY + 2U_Y U_{aY} &= -(1 + (a + 1)Y) + 1 + 2U_{(a+1)Y}, \quad \text{that is,} \\
 U_Y U_{aY} &= -1 - (a + 1)Y + U_{(a+1)Y}, \quad \text{which, by squaring as before, renders} \\
 (1 + Y)(1 + aY) &= (1 + (a + 1)Y)^2 - (1 + (a + 1)Y) - 2(1 + (a + 1)Y)U_{(a+1)Y}, \\
 (a^2 + a + 1)Y^2 - 1 &= 2(1 + (a + 1)Y)U_{(a+1)Y}, \quad \text{and squaring again} \\
 (a^2 + a + 1)^2 Y^4 - 2(a^2 + a + 1)Y^2 + 1 &= -4(1 + (a + 1)Y)^2(1 + (a + 1)Y), \\
 5 + 12(1 + a)Y + 2(5 + 11a + 5a^2)Y^2 + 4(1 + a)^3 Y^3 + (1 + a + a^2)^2 Y^4 &= 0,
 \end{aligned}$$

which has at most four solutions. The discriminant of this equation is $-2^8(-1 + a)^4 a^3(8 + 11a + 8a^2)$. Recall that for any polynomial of any degree m , a necessary condition for the polynomial to be irreducible over \mathbb{F}_{p^n} is to have its discriminant a square (m odd), respectively, non-square (m even) (see [11]). Thus, we have no solutions if $-a(8 + 11a + 8a^2)$ is a non-square.

Case 3. Let $(\alpha, \beta, \gamma) = (1, -1, 1)$. Equation (9) becomes

$$\begin{aligned}
 1 + Y - (1 + aY) + 2U_Y U_{aY} &= 1 + (a + 1)Y + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= U_{(a+1)Y} + 1 + aY, \quad \text{and by squaring,} \\
 -(1 + Y)(1 + aY) &= 1 + (a + 1)Y + 1 + a^2 Y^2 + 2aY + 2(1 + aY)U_{(a+1)Y}, \\
 -3 - 2(1 + 2a)Y - (a + a^2)Y^2 &= 2(1 + aY)U_{(a+1)Y}, \\
 5 + 4(2 + 3a)Y + 2(1 + a)(2 + 5a)Y^2 + 4a(1 + a)^2 Y^3 + a^2(1 + a)^2 Y^4 &= 0,
 \end{aligned}$$

which again has at most four solutions. The discriminant of this equation is $2^8 a^3(1 + a)^4(8 - 11a + 8a^2)$, so we have no solutions if $a(8 - 11a + 8a^2)$ is a non-square.

Case 4. Let $(\alpha, \beta, \gamma) = (1, -1, -1)$. In this case, we have the sequence of implications

$$\begin{aligned}
 1 + Y - (1 + aY) + 2U_Y U_{aY} &= -(1 + (a + 1)Y) + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= U_{(a+1)Y} - Y, \\
 -(1 + Y)(1 + aY) &= -(1 + (a + 1)Y) + Y^2 - 2YU_{(a+1)Y} \\
 (1 + a)Y^2 &= 2YU_{(a+1)Y}, \quad \text{and dividing by } Y \text{ and squaring we get} \\
 (1 + a)^2 Y^2 &= -4(1 + (a + 1)Y), \\
 (2 + (1 + a)Y)^2 &= 0, \quad \text{of solution } Y = \frac{-2}{a + 1}.
 \end{aligned}$$

Case 5. Let $(\alpha, \beta, \gamma) = (-1, 1, 1)$. As before, we get

$$\begin{aligned}
 -(1 + Y) + (1 + aY) + 2U_Y U_{aY} &= (1 + (a + 1)Y) + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= U_{(a+1)Y} + Y + 1,
 \end{aligned}$$

$$\begin{aligned}
 -(1+Y)(1+aY) &= (1+(a+1)Y) + (Y+1)^2 + 2(Y+1)U_{(a+1)Y}, \\
 -3 - 2(2+a)Y - (1+a)Y^2 &= 2(Y+1)U_{(a+1)Y}, \quad \text{and so,} \\
 5 + 4(3+2a)Y + 2(1+a)(5+2a)Y^2 + 4(1+a)^2Y^3 + (1+a)^2Y^4 &= 0,
 \end{aligned}$$

with at most four solutions. The discriminant of this equation is $2^8 a^3(1+a)^4(8-11a+8a^2)$, so we have no solutions if $a(8-11a+8a^2)$ is a non-square.

Case 6. Let $(\alpha, \beta, \gamma) = (-1, 1, -1)$. We have

$$\begin{aligned}
 -(1+Y) + 1 + aY + 2U_Y U_{aY} &= -(1+(a+1)Y) + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= U_{(a+1)Y} - aY, \\
 -(1+Y)(1+aY) &= -(1+(a+1)Y) + a^2Y^2 - 2aYU_{(a+1)Y} \\
 2aYU_{(a+1)Y} &= a(1+a)Y^2, \quad \text{and dividing by } aY \text{ and squaring,} \\
 -4(1+(a+1)Y) &= (1+a)^2Y^2, \quad \text{that is,} \\
 (2+Y+aY)^2, \quad \text{of solution } Y &= \frac{-2}{a+1}.
 \end{aligned}$$

Case 7. Let $(\alpha, \beta, \gamma) = (-1, -1, 1)$. As before, we look at the equation

$$\begin{aligned}
 -(1+Y) - (1+aY) + 2U_Y U_{aY} &= (1+(a+1)Y) + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= 2 + (1+a)Y + U_{(a+1)Y}, \\
 (1+Y)(1+aY) &= (2+(1+a)Y)^2 + (1+(a+1)Y) + 2(2+(1+a)Y)U_{(a+1)Y}, \\
 -4 - 4(1+a)Y + (-1-a-a^2)Y^2 &= 2(2+(1+a)Y)U_{(a+1)Y}, \\
 (-4 - 4(1+a)Y + (-1-a-a^2)Y^2)^2 &= 4(2+(1+a)Y)^2(1+(a+1)Y), \quad \text{and so,} \\
 4(1+a^2) + 4(1+a)(1+a^2)Y + (1+a+a^2)^2Y^2 &= 0,
 \end{aligned}$$

which has at most two solutions.

The discriminant of this equation is $-2^4 a^2(1+a^2)$. Thus, we have no solutions if $\chi(-(a^2+1)) = -\chi(a^2+1) = -1$, that is, a^2+1 is a square and two solutions, otherwise.

Case 8. Let $(\alpha, \beta, \gamma) = (-1, -1, -1)$. We finally have

$$\begin{aligned}
 -(1+Y) - (1+aY) + 2U_Y U_{aY} &= -(1+(a+1)Y) + 1 + 2U_{(a+1)Y}, \\
 U_Y U_{aY} &= U_{(a+1)Y} + 1 = U_Y + U_{aY}, \quad \text{and dividing by } U_Y \\
 U_{aY} - 1 &= \left(\frac{1+aY}{1+Y} \right)^d, \quad \text{and by squaring}
 \end{aligned}$$

$$-(1 + aY) + 1 - 2U_{aY} = \frac{1 + aY}{1 + Y}, \quad \text{that is,}$$

$$-2U_{aY} = \frac{aY^2 + 2aY + 1}{Y + 1},$$

$$5 + 8(1 + a)Y + 2(2 + a)(1 + 2a)Y^2 + 4a(1 + a)Y^3 + a^2Y^4 = 0,$$

which has at most four solutions. The discriminant of this equation is $-2^8(-1 + a)^4a^3(8 + 11a + 8a^2)$, so we have no solutions if and only if $-a(8 + 11a + 8a^2)$ is a non-square.

Recall that $\chi(-1) = -1$ under our conditions on n, p . Surely, Cases 4 and 6 cannot occur simultaneously, and we can see that the conditions on Y in Case 4 (as well, as Case 6) are fulfilled for $a \neq \pm 1$, so one of these cases can happen, but not both.

Note also that the conditions for Cases 2 and 8 are identical, as are the conditions for Cases 3 and 5.

In Cases 4 and 6, the solution is $Y = \frac{-2}{a+1}$. Then

$$\chi(1 + (a + 1)Y) = \chi(-1) = -1,$$

$$\chi(1 + Y) = \chi\left(\frac{a - 1}{a + 1}\right) = \chi(a - 1)\chi(a + 1),$$

$$\begin{aligned} \chi(1 + aY) &= \chi\left(\frac{-a + 1}{a + 1}\right) = \chi(-1)\chi(a - 1)\chi(a + 1) \\ &= -\chi(a - 1)\chi(a + 1) = -\chi(1 + Y). \end{aligned}$$

For any $a \neq \pm 1, 0$, then we have that either $\chi(a - 1) = \chi(a + 1)$ (Case 4) or $\chi(a - 1) = -\chi(a + 1)$ (Case 6), so $Y = \frac{-2}{a+1}$ is always a solution of Eq. (9). However, by replacing $X = \frac{1}{Y} = -\frac{a+1}{2}$ in the original equation $(X + a + 1)^d - (X + 1)^d - (X + a)^d + X^d = 0$, we can see that the latter equation is not satisfied by this value of X

$$\left(-\frac{a + 1}{2} + a + 1\right)^d - \left(-\frac{a + 1}{2} + 1\right)^d - \left(-\frac{a + 1}{2} + a\right)^d + \left(-\frac{a + 1}{2}\right)^d = 0,$$

$$2^{-d+1}((a + 1)^d - (a - 1)^d) = 0, \quad \text{that is,}$$

$$\left(\frac{a - 1}{a + 1}\right)^d = 1.$$

The number of solutions to the equation $z^d = 1$ is given by $\gcd(d, p^n - 1) = 2$. It is easy to see that these solutions are $z = \pm 1$. However, $z = 1$ renders a contradiction, while $z = -1$ renders $a = 0$, which is excluded. This implies that, for $a \neq \pm 1$, Cases 4 and 6 do not contribute to the total number of solutions. It is easy to see that $a = -1$ renders a contradiction on Cases 4 and 6, while, trivially, the solution $a = \pm 1$ cannot fulfill the conditions on these cases.

Therefore, for any $a \in \mathbb{F}_{p^n}^*$, Cases 4 and 6 do not contribute to the total number of solutions of the original equation (8).

We can prune the other cases a bit better in the following way. We express the polynomials in the “variable” a , and compute their discriminant. If a is fixed in \mathbb{F}_{p^n} and Y_i exists for the Case i ($i = 2, 3, 5, 7, 8$), then the corresponding discriminant of the polynomial in a cannot be a square. These discriminants for Cases 2, 3, 5, 7, 8 are

$$2Y_2^{15}(1 + Y_2)^6, Y_3^{15}(1 + Y_3)^3, Y_5^4(1 + Y_5)^3(2 + Y_5)^2, 2Y_7^2(1 + Y_7)^3, 2Y_8^2(1 + Y_8)^3.$$

Since $\chi(Y_i + 1) = 1$ in Cases 2 and 3, and $\chi(Y_i + 1) = -1$ in the other cases, we see that, if $\chi(2) = -1$, we can exclude Cases 7 and 8, since the discriminant is therefore a square, and, since the discriminant (with variable X) for Case 2 is the same as for Case 8, we can also exclude this case; we thus obtain if $\chi(2) = -1$ an upper bound of 8. If $\chi(2) = 1$, then we obtain an upper bound of 18.

If $p = 3$, then we can further refine the distribution of the potential solutions. In this case, since $\chi(2) = -1$, we can exclude Cases 2, 7 and 8. Next, $8a^2 - 11a + 8 = 2(a^2 - a + 1) = 2(1 + a)^2$, which is a square only if $a = -1$.

First, if $p = 3, a = -1$, then in Case 3 the equation reduces to $2 - Y = 0$, which renders as the only solution $Y = 2$. In Case 5 the equation reduces to $2 + Y = 0$, which renders as the only solution $Y = -2$. Therefore, when $a = -1$ there are exactly two solutions.

Next, let $p = 3, a \neq -1$. The maximum number of solutions can only happen for Cases 3 and 5 (when $\chi(a) = -1$). When $\chi(a) = 1$, there are no solutions. \square

Remark 3.10. It is worth noting that, since F is an even function and $X = \frac{-a-1}{2}$ is not a solution, by Remark 3.5 the second-order zero differential uniformity of F is even.

We display in Table 1 some experimental data on the monomial function of our previous theorem, which shows that our bound of 8 (when $\chi(2) = -1$) for the second-order zero differential uniformity is attained for some values of p and n .

Table 1. Experimental results on $X^{\frac{p^n+1}{4} + \frac{p^n-1}{2}}$.

p	n	d	∇_F
3	3	20	2
3	5	182	4
3	7	1640	8
3	9	14,762	6
7	3	86	4
7	5	4202	8
11	3	998	6

4. The Second-Order Zero Differential Spectrum of 0-APN Functions and Extensions

Budaghyan *et al.* [7] considered the function $F(X) = X^{21}$ and showed that it is 0-APN if and only if n is not a multiple of 6 (that is, this function is an almost exceptional partial APN). As a side note, we point out that Pott [23] showed (non-constructively) that there exist partially APN permutations (in even characteristic), for all integers $n \geq 3$, by connecting the problem to Steiner triple systems. We discuss here the second-order zero differential spectrum of $F(X) = X^{21}$ and show that it attains the best possible value of FBCT for a non-APN function when n is odd.

Theorem 4.1. *Let $F(X) = X^{21}$ be a function over \mathbb{F}_{2^n} , where n is odd. Then for $a, b \in \mathbb{F}_{2^n}$*

$$\nabla_F(a, b) = \begin{cases} 2^n & \text{if } ab = 0 \text{ or } a = b, \\ 4 & \text{if } ab \neq 0 \text{ and } a \neq b, \sum_{i=0}^{n-1} v^{s_i} C^{2^{2i}} = 0 \\ & \text{and } \sum_{r=0}^{n-1} \left(\sum_{i=0}^{n-1} (i+1)v^{s_i} C^{2^{2i}} \right)^{2^{2r}} = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where $v = \frac{b}{a}(1 + \frac{b^3}{a^3})$, $C = 1 + \frac{b^{20} + a^4 b^{16} + a^{15} b^5 + a^3 b^{17}}{a^{16} b^4 + a^{19} b}$, $s_i = \sum_{j=i}^{n-2} 2^{2(j+1)}$ for $0 \leq i \leq n-2$ and $s_{n-1} = 0$. Moreover, the Feistel boomerang uniformity of F is 4.

Proof. We consider the following equation for $a, b \in \mathbb{F}_{2^n}$:

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

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

$$(X + a + b)^{21} + (X + b)^{21} + (X + a)^{21} + X^{21} = 0,$$

or equivalently

$$(Y + B + 1)^{21} + (Y + B)^{21} + (Y + 1)^{21} + Y^{21} = 0,$$

where $Y = \frac{X}{a}$ and $B = \frac{b}{a}$. The above equation can be further reduced to

$$(B^4 + B)Y^{16} + (B^{16} + B)Y^4 + (B^4 + B^{16})Y + B^4 + B^{17} + B^5 + B^{16} + B^{20} + B = 0.$$

Note that $B^4 + B \neq 0$, because otherwise we would have $a^3 = b^3$ and as n is odd, we get $\gcd(3, 2^n - 1) = 1$ which would further imply $a = b$. Hence, dividing the

above equation by $B^4 + B$, we have

$$Y^{16} + \left(\frac{B^{16} + B}{B^4 + B}\right)Y^4 + \left(\frac{B^{16} + B^4}{B^4 + B}\right)Y + \frac{B^4 + B^{17} + B^5 + B^{16} + B^{20} + B}{B^4 + B} = 0. \tag{10}$$

One can further reduce the coefficients in the above equation as

$$\frac{B^{16} + B}{B^4 + B} = 1 + B^{12} + B^3 + B^9 + B^6 =: u,$$

$$\frac{B^{16} + B^4}{B^4 + B} = B^{12} + B^3 + B^9 + B^6 = u + 1 =: v.$$

Thus, we can rewrite Eq. (10) as $Y^{16} + uY^4 + vY + C = 0$, where

$$C = \frac{B^4 + B^{17} + B^5 + B^{16} + B^{20} + B}{B^4 + B}.$$

Substituting $u = v + 1$ in the above equation, we get $Y^{16} + Y^4 + vY^4 + vY + C = 0$, which can be further simplified as $Z^4 + vZ + C = 0$ for $Z = Y^4 + Y$. Now using Lemma 2.8, to solve $Z^4 + vZ + C = 0$, we have $k = 2, m = n$ and $\alpha_{m-1} = v^{\frac{2^{2n}-1}{3}} = (B(1+B^3))^{2^{2n}-1} = 1$. This gives us that $Z^4 + vZ + C = 0$ has no solution in \mathbb{F}_{2^n} if $\sum_{i=0}^{n-1} v^{s_i} C^{2^{2i}} \neq 0$, where $s_{n-1} = 0, s_i = \sum_{j=i}^{n-2} 2^{2(j+1)}$ for $0 \leq i \leq n-2$, and two solutions in \mathbb{F}_{2^n} if the sum $\sum_{i=0}^{n-1} v^{s_i} C^{2^{2i}} = 0$, in which case, taking $c = 1$, and given that $\tau^3 = v$, we get $\tau = B(1+B^3)$. Then the two solutions of $Z^4 + vZ + C = 0$ from Lemma 2.8 are $Z_1 = \sum_{i=0}^{n-1} (i+1)v^{t_i} C^{2^{2i}}$ and $Z_2 = \sum_{i=0}^{n-1} (i+1)v^{t_i} C^{2^{2i}} + \tau$, where $t_i = \sum_{j=i}^{n-2} 2^{2(j+1)}$ for $0 \leq i \leq n-1$. Observe that $t_i = s_i$ (for $r = n-1$) in our case.

We are now left with the equation $Y^4 + Y + Z_j = 0$ for $j = 1, 2$. Again using Lemma 2.8, the equation can have either zero or two solutions depending on whether the sum $\sum_{i=0}^{n-1} (Z_j)^{2^{2i}}$ is zero or not. Note that $\sum_{i=0}^{n-1} (Z_1)^{2^{2i}} = \sum_{i=0}^{n-1} (Z_2)^{2^{2i}}$, as the sum $\sum_{i=0}^{n-1} \tau^{2^{2i}} = 0$. Thus, we have either four solutions or no solutions. This will give us our desired claim. \square

Remark 4.2. Note that the equivalent proof for n even gives

$$\nabla_F(a, b) = \begin{cases} 2^n & \text{if } ab = 0 \text{ or } a = b, \\ 16 & \text{if } ab \neq 0 \text{ and } a^3 \neq b^3, \sum_{i=0}^{n/2-1} v^{s_i} C^{2^{2i}} = 0 \\ & \text{and } \sum_{r=0}^{n/2-1} \left(\sum_{i=0}^{n-1} (i+1)v^{s_i} C^{2^{2i}} \right)^{2^{2r}} = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where we have $v = \frac{b}{a}(1 + \frac{b^3}{a^3})$, $C = 1 + \frac{b^{20} + a^4 b^{16} + a^{15} b^5 + a^3 b^{17}}{a^{16} b^4 + a^{19} b}$, $s_i = \sum_{j=i}^{n/2-2} 2^{2(j+1)}$ for $0 \leq i \leq n/2-2$ and $s_{n/2-1} = 0$.

We can generalize the previous function to a much more general cubic polynomial, but, of course, the spectrum is not going to be that explicit. For a linearized polynomial L , we let $\ker(L)$, $\Im(L)$ be the kernel, respectively, the image of L .

Theorem 4.3. *Let $F(X) = \sum_{0 < i < j < n} c_{ij} X^{p^i + p^j + 1}$ be a cubic function in $F_{p^n}[X]$, where p is an arbitrary prime. Then for any $a, b \in \mathbb{F}_{p^n}$, the second-order zero differential spectra are given by*

$$\nabla_F(a, b) = \begin{cases} p^n & \text{if } ab = 0, \\ p^{\dim(\ker L_{a,b})} & \text{if } \delta_{a,b} \in \Im(L_{a,b}), \\ 0 & \text{if } \delta_{a,b} \notin \Im(L_{a,b}), \end{cases}$$

where $L_{a,b}(X) = \sum_{0 < i < j < n} c_{ij} (X(a^{p^i} b^{p^j} + a^{p^j} b^{p^i}) + X^{p^i} (ba^{p^j} + ab^{p^j}) + X^{p^j} (ba^{p^i} + ab^{p^i}))$, and $\delta_{a,b} = \sum_{0 < i < j < n} c_{ij} ((a+b)(a^{p^i} b^{p^j} + a^{p^j} b^{p^i}) + ab^{p^i + p^j} + ba^{p^i + p^j})$.

Proof. We first compute

$$\begin{aligned} F(X) &= \sum_{0 < i < j < n} c_{ij} X^{p^i + p^j + 1}, \\ F(X+a) &= \sum_{0 < i < j < n} c_{ij} (a^{p^i + 1} X^{p^j} + a^{p^j + 1} X^{p^i} + X a^{p^i + p^j} + a^{p^i + p^j + 1} \\ &\quad + a^{p^i} X^{p^j + 1} + a^{p^j} X^{p^i + 1} + a X^{p^i + p^j} + X^{p^i + p^j + 1}), \\ F(X+b) &= \sum_{0 < i < j < n} c_{ij} (b^{p^i + 1} X^{p^j} + b^{p^j + 1} X^{p^i} + X b^{p^i + p^j} + b^{p^i + p^j + 1} \\ &\quad + b^{p^i} X^{p^j + 1} + b^{p^j} X^{p^i + 1} + b X^{p^i + p^j} + X^{p^i + p^j + 1}), \\ F(X+a+b) &= \sum_{0 < i < j < n} c_{ij} (X^{p^i + p^j + 1} + X^{p^j + 1} (a+b)^{p^i} + X^{p^i + 1} (a+b)^{p^j} \\ &\quad + X^{p^j} (a(a+b)^{p^i} + b(a+b)^{p^i}) + X^{p^i} (a(a+b)^{p^j} + b(a+b)^{p^j}) \\ &\quad + X(a+b)^{p^i + p^j} + (a+b)^{p^i + p^j + 1} + X^{p^i + p^j} (a+b)). \end{aligned}$$

The second-order zero differential equation $F(X+a+b) - F(X+b) - F(X+a) + F(X) = 0$ becomes, after simplifying where possible (a straightforward, but rather tedious computation)

$$\begin{aligned} 0 &= \sum_{0 < i < j < n} c_{ij} (-a^{p^i + 1} X^{p^j} - a^{p^j + 1} X^{p^i} - X a^{p^i + p^j} - a^{p^i + p^j + 1} + X^{p^i + 1} (a^{p^j} + b^{p^j}) \\ &\quad + X^{p^j + 1} (a^{p^i} + b^{p^i}) + a X^{p^i} (a^{p^j} + b^{p^j}) + a X^{p^j} (a^{p^i} + b^{p^i}) + b X^{p^i} (a^{p^j} + b^{p^j}) \\ &\quad + b X^{p^j} (a^{p^i} + b^{p^i}) + X (a^{p^i} + b^{p^i}) (a^{p^j} + b^{p^j}) + a (a^{p^i} + b^{p^i}) (a^{p^j} + b^{p^j})) \end{aligned}$$

$$\begin{aligned}
 &+ b(a^{p^i} + b^{p^i})(a^{p^j} + b^{p^j}) + a^{p^i}(-X^{p^j+1}) - a^{p^j}X^{p^i+1} - b^{p^j+1}X^{p^i} - b^{p^i+1}X^{p^j} \\
 &- Xb^{p^i+p^j} - b^{p^i+p^j+1} - b^{p^j}X^{p^i+1} - b^{p^i}X^{p^j+1}) \\
 = &\sum_{0 < i < j < n} c_{ij}((a+b)(a^{p^i}b^{p^j} + a^{p^j}b^{p^i}) + ab^{p^i+p^j} + ba^{p^i+p^j} + X(a^{p^i}b^{p^j} + a^{p^j}b^{p^i}) \\
 &+ X^{p^i}(ba^{p^j} + ab^{p^j}) + X^{p^j}(ba^{p^i} + ab^{p^i})).
 \end{aligned}$$

If the element $\sum_{0 < i < j < n} c_{ij}((a+b)(a^{p^i}b^{p^j} + a^{p^j}b^{p^i}) + ab^{p^i+p^j} + ba^{p^i+p^j})$ belongs to the image of the affine polynomial

$$L_{a,b}(X) = \sum_{0 < i < j < n} c_{ij}(X(a^{p^i}b^{p^j} + a^{p^j}b^{p^i}) + X^{p^i}(ba^{p^j} + ab^{p^j}) + X^{p^j}(ba^{p^i} + ab^{p^i})),$$

then the solutions for the second-order zero differential equation form an affine space of dimension precisely $\dim(\ker L_{a,b})$. The proof is done. \square

Remark 4.4. Surely, one can wonder why we have not considered Dembowski–Ostrom (DO) polynomials, that is, polynomials of the form $F(X) = \sum_{0 \leq i < j < n} a_{ij}X^{p^i+p^j}$ (with or without affine terms) on \mathbb{F}_{p^n} . However, the interested reader can quickly check that the second-order zero differential equation for F at a, b , either has no solutions or it has p^n solutions.

Budaghyan *et al.* [7] also considered $F(X) = X^{2^n-2^s}$ (which coincides with the inverse function X^{-1} extended by $0^{-1} = 0$ for $s = 1$) and showed that it is 0-APN if and only if $\gcd(n, s + 1) = 1$.

Theorem 4.5. *Let $F(X) = X^{2^n-2^s}$ be a function over \mathbb{F}_{2^n} , where s is a positive integer satisfying $\gcd(n, s + 1) = 1$. Then for $a, b \in \mathbb{F}_{2^n}$*

$$\nabla_F(a, b) = \begin{cases} 2^n & \text{if } ab = 0 \text{ and } a = b, \\ 2^{\gcd(s,n)} - 4 & \text{if } ab \neq 0, ab^{2^s} + a^{2^s}b = 0 \text{ and } \gcd(s, n) > 1, \\ 2^{n-s-\text{rank}(E_1)} - 4 & \text{if } ab \neq 0, ab^{2^s} + a^{2^s}b \neq 0, A \neq 1 \\ & \text{and } \text{rank}(E_1) \leq (n - s) - 2, \\ 0 & \text{otherwise,} \end{cases}$$

where $A = \frac{ab^{2^n-s} + a^{2^n-s}b}{a^{2^n-s-2}(ab^2+a^2b)}$, $E_1 = C_T C_T^2 \cdots C_T^{2^{n-1}} - I_{n-s}$, and $C_T^{2^i}$ is the matrix obtained from the $(n - s) \times (n - s)$ matrix

$$C_T = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 + A \\ 1 & 0 & \cdots & 0 & A \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

by applying to each of its entries the automorphism $X \mapsto X^{2^i}$ and I_k is the identity matrix of order k .

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

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

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

$$(X + a + b)^{2^n - 2^s} + (X + b)^{2^n - 2^s} + (X + a)^{2^n - 2^s} + X^{2^n - 2^s} = 0,$$

or equivalently

$$(Y + B + 1)^{2^n - 2^s} + (Y + B)^{2^n - 2^s} + (Y + 1)^{2^n - 2^s} + Y^{2^n - 2^s} = 0, \quad (11)$$

where $Y = \frac{X}{a}$ and $B = \frac{b}{a}$. Let $Y \in \{0, 1, B, B + 1\}$, the above equation has a solution only if $(B + 1)^{2^n - 2^s} + B^{2^n - 2^s} + 1 = 0$, or equivalently, $B^{2^{n-s-1}-1} = 1$. However, this is possible only if $\gcd(s+1, n) > 1$, and hence Eq. (11) has no solution $Y \in \{0, 1, B, B + 1\}$.

Let us assume $Y \notin \{0, 1, B, B + 1\}$. Then Eq. (11) reduced to

$$(B + B^{2^s})Y^{2^{s+1}} + (B + B^{2^{s+1}})Y^{2^s} + (B^{2^s} + B^{2^{s+1}})Y = 0. \quad (12)$$

We have two possible cases here depending on whether $B + B^{2^s} = 0$ or not. One can see that there are $2^{\gcd(s,n)}$ possible values of B for which $B + B^{2^s} = 0$. If $\gcd(s, n) = 1$, then $B \in \{0, 1\}$, which is not possible. Hence, we consider the case $B + B^{2^s} = 0$ when $\gcd(s, n) > 1$, and in this case Eq. (12) is reduced to $Y^{2^s} + Y = 0$ which has $2^{\gcd(s,n)}$ solutions in \mathbb{F}_{2^n} .

We now assume $B + B^{2^s} \neq 0$. Observe that the sum of these coefficients is 1. Raising Eq. (12) to the power 2^{n-s} , we get

$$(B^{2^{n-s}} + B)Y^2 + (B^{2^{n-s}} + B^2)Y + (B + B^2)Y^{2^{n-s}} = 0,$$

or equivalently, dividing by $B^2 + B$ and using the notation $A = \frac{B^{2^{n-s}} + B}{B^2 + B}$

$$Y^{2^{n-s}} + AY^2 + (1 + A)Y = 0. \quad (13)$$

This equation is connected to the known Blondeau–Canteaut–Charpin (BCC) conjecture [3] on $f_t(X) = X^{2^t-1}$ on \mathbb{F}_{2^n} , namely:

- (i) f_t is APN on $\mathbb{F}_{2^{2m}}$ if and only if $t = 2$ (this was shown to be true by Göloğlu [16]).
- (ii) f_t is APN on $\mathbb{F}_{2^{2m+1}}$ if and only if $t \in \{2, m + 1, 2m\}$ (still open).

Writing the differential equation for f_t (for us, $t = n - s$, $\gcd(t - 1, n) = \gcd(s + 1, n) = 1$) at some a' , one can derive the equation (where $Z := 1/X$)

$$Z^{2^t} + A'Z^2 + (1 + A')Z = 0, \quad \text{where } A' = \frac{1 + a'^{2^t-1}}{1 + a'}. \quad (14)$$

While we cannot prove the BCC conjecture, we can derive some conditions for the kernel of Eq. (13). If $A = 1$, that is $B^{2^{n-s}} + B^2 = 0$, Eq. (13) transforms into

$Y^{2^{n-s}} + Y^2 = 0$, that is, $Y^{2^{n-s}-1} + Y = 0$, which has $2^{\gcd(n-s-1, n)} = 2^{\gcd(s+1, n)} = 2$ solutions, (these are precisely $Y = 0, 1$) that we have already excluded. We now let $A \neq 1$. We define the companion matrix of the trinomial $T(Y) = Y^{2^{n-s}} + AY^2 + (1+A)Y$ of (13) be given by the $(n-s) \times (n-s)$ matrix

$$C_T = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1+A \\ 1 & 0 & \cdots & 0 & A \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

We now use McGuire and Sheekey result [20, Theorem 6] (or Polverino and Ferdinando [22, Theorem 1.4]), which, particularized for our linearized trinomial T , implies that the dimension (over \mathbb{F}_2) of the kernel of T (in terms of the rank of a matrix) is given by

$$\dim_{\mathbb{F}_2} \ker T = n - s - \text{rank}(E_1),$$

where $E_1 = C_T C_T^2 \cdots C_T^{2^{n-1}} - I_{n-s}$, where

$$C_T^{2^i} = \begin{pmatrix} 0 & 0 & \cdots & 0 & (1+A)^{2^i} \\ 1 & 0 & \cdots & 0 & A^{2^i} \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

is the matrix obtained from C_T by applying to each of its entries the automorphism $X \mapsto X^{2^i}$ and I_k is the identity matrix of order k . Therefore, the trinomial $T(Y)$ has $2^{n-s-\text{rank}(E_1)}$ solutions in \mathbb{F}_{2^n} or equivalently $2^{n-s-\text{rank}(E_1)} - 4$ solutions in $\mathbb{F}_{2^n} \setminus \{0, 1, B, B+1\}$ if $\text{rank}(E_1) \leq (n-s) - 2$. This will give us the desired claim. \square

To illustrate Theorem 4.5, we give the following example.

Example 4.6. Let $F(X) = X^7$ be a function over the finite field \mathbb{F}_{2^7} , where $\mathbb{F}_{2^7}^* = \langle g \rangle$. Here, $n = 7$, $s = 4$ and $\gcd(n, s+1) = \gcd(7, 5) = 1$. For $(a, b) = (g^2, g)$, we have

$$C_T = \begin{pmatrix} 0 & 0 & g^5 + g^3 + g \\ 1 & 0 & g^5 + g^3 + g + 1 \\ 0 & 1 & 0 \end{pmatrix},$$

and $E_1 = C_T C_T^2 C_T^4 C_T^8 C_T^{16} C_T^{32} - I_3$ is a zero matrix with rank 0. Thus, the above theorem would give us $\nabla_F(g^2, g) = 2^3 - 4 = 4$. Note that $\nabla_F(a, b) \leq 4$ corresponding to any pair $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ with $ab \neq 0$ and $a \neq b$. Thus, we have that the Feistel boomerang uniformity of $F(X) = X^7$ over \mathbb{F}_{2^7} is 4.

Remark 4.7. Some particular cases of Theorem 4.5 have already been addressed, independently. For instance, when $n - s = t = 2$, $X^{2^n - 2^s}$ is an APN function and for APN functions the FBCT spectra are already known in view of Lemma 2.6. Moreover, Garg *et al.* [15] computed the FBCT spectra when $n = 2m$ and $n - s = t = m$, and in fact, they also showed that for $n = 2m + 1$ and $n - s = t = m + 2$, $X^{2^t - 1}$ has the F-Boomerang uniformity at most 4. Recently, Man *et al.* [19] computed the FBCT spectra when $n - s = t = m + 1$.

As a consequence of Theorem 4.5, the following corollary in a special case of $n - s = t = 3$ is almost immediate.

Corollary 4.8. *Let s and n be positive integers such that $\gcd(s, n + 1) = 1$, $n - s = 3$, and $F(X) = X^{2^n - 2^s}$ be a function over the finite field \mathbb{F}_{2^n} . Then the Feistel boomerang uniformity of F is 4.*

Proof. Given the conditions on s and n , one can easily deduce that $\gcd(s, n)$ is either 1 or 3. From Theorem 4.5, it is clear that for $ab \neq 0$, $a \neq b$ and $ab^{2^s} + a^{2^s}b = 0$, $\nabla_F(a, b) = 2^{\gcd(s, n)} - 4 = 4$. We next consider the case when $ab \neq 0$, $a \neq b$ and $A \neq 1$, where $A = \frac{ab^s + a^s b}{a^6(ab^2 + a^2b)}$, then we have $\nabla_F(a, b) = 2^{3 - \text{rank}(E_1)} - 4$ where E_1 is a 3×3 matrix. Since the $\text{rank}(E_1)$ is less than or equal to $n - s - 2$, it is either 0 or 1. In other words, either $\nabla_F(a, b) = 4$ or $\nabla_F(a, b) = 0$, respectively. Thus, the above arguments clearly indicate that $\nabla_F(a, b) \leq 4$ for $ab \neq 0$ and $a \neq b$. Since F is not an APN function (cf. [3, Theorem 5]), it follows from Lemma 2.6 that the Feistel boomerang uniformity of F is 4. □

Note that Corollary 4.8 gives only the Feistel boomerang uniformity of the function $X^{2^n - 2^s}$ over \mathbb{F}_{2^n} when $t = n - s = 3$ and $\gcd(n, s + 1) = 1$. However, we adopt a slightly different approach to determine the complete Feistel boomerang spectra of this function in the following theorem. It may be noted that the differential spectrum of $F(X) = X^7$ was studied in [3, Theorem 5].

Theorem 4.9. *Let $F(X) = X^{2^n - 2^s}$ be a function over \mathbb{F}_{2^n} , where s is a positive integer satisfying $\gcd(n, s + 1) = 1$ and $n - s = 3$. Then for $a, b \in \mathbb{F}_{2^n}$, we have*

$$\nabla_F(a, b) = \begin{cases} 2^n & \text{if } ab = 0 \text{ or } a = b, \\ 4 & \text{if } ab \neq 0, a \neq b, ab^{2^s} + a^{2^s}b = 0 \text{ and } \gcd(s, n) = 3, \\ & \text{or } ab \neq 0, a \neq b, \text{Tr}\left(\frac{a^7(ab^2 + a^2b)}{a^2b^8 + a^8b^2}\right) = 1, \\ & \text{Tr}\left(\frac{a^3}{a^2b + ab^2}\right) = 1; t_1, t_2 \text{ are cubes in } \mathbb{F}_{2^{2n}}, \\ & \text{and } \text{Tr}(Z_1) = \text{Tr}(Z_2) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where Z_1, Z_2 are solutions of $a^6 Z^2 + a^3(ab^2 + a^2b)Z + a^2b^4 + a^4b^2 + a^6 = 0$ and t_1, t_2 are solutions of $a^7(ab^2 + a^2b)t^2 + (a^8b^2 + a^2b^8)t + a^7(ab^2 + a^2b) = 0$. Moreover, the Feistel boomerang uniformity of F is 4.

Proof. It is easy to observe that $n - s = 3$ and $\gcd(s + 1, n) = 1$ would together imply that n is odd. Consider the following equation:

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

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

$$(Y + B + 1)^{2^n - 2^s} + (Y + B)^{2^n - 2^s} + (Y + 1)^{2^n - 2^s} + Y^{2^n - 2^s} = 0, \quad (15)$$

where $Y = \frac{X}{a}$ and $B = \frac{b}{a}$. We know from the proof of Theorem 4.5 that Eq. (15) has no solution in $\{0, 1, B, B + 1\}$. Let us assume $Y \notin \{0, 1, B, B + 1\}$, then one can write Eq. (15) as

$$(B + B^{2^s})Y^{2^{s+1}} + (B + B^{2^{s+1}})Y^{2^s} + (B^{2^s} + B^{2^{s+1}})Y = 0. \quad (16)$$

We first consider the case when $B + B^{2^s} = 0$. Observe that there are $2^{\gcd(s, n)}$ such $B \in \mathbb{F}_{2^n}$ satisfying $B + B^{2^s} = 0$. Note that $\gcd(s, n)$ is either 1 or 3. Thus, when $\gcd(s, n) = 1$, the equation $B + B^{2^s} = 0$ has only two solutions, namely $B = 0$ and $B = 1$, which we have already considered. Hence, we consider the case $B + B^{2^s} = 0$ when $\gcd(s, n) = 3$ and in this case, Eq. (16) has exactly 4 solutions in $\mathbb{F}_{2^n} \setminus \{0, 1, B, B + 1\}$. Next, we consider $B + B^{2^s} \neq 0$, and in this case, we can reduce Eq. (16) as follows:

$$Y^{2^3} + AY^2 + (1 + A)Y = 0, \quad (17)$$

where $A = \frac{B^{2^3} + B}{B^2 + B}$. We can further rewrite Eq. (16) as

$$Y^{2^3} + Y^{2^2} + Y^{2^2} + Y^2 + Y^2 + AY^2 + Y + AY = 0,$$

or equivalently, $(Y^2 + Y)^{2^2} + (Y^2 + Y)^2 + (1 + A)(Y^2 + Y) = 0$. Substitute $Z = Y^2 + Y$ in the above equation to get

$$Z^{2^2} + Z^2 + (1 + A)Z = 0. \quad (18)$$

Clearly, $Z = 0$ and $Z = B^2 + B$ are solutions of Eq. (18). Then the cubic equation $Z^3 + Z + (1 + A) = 0$ would have at least one solution in \mathbb{F}_{2^n} , or more precisely, the cubic equation can have either one or three solutions in \mathbb{F}_{2^n} . From Lemma 2.10, if $\text{Tr}(\frac{1}{1+A}) \neq 1$, then $Z^3 + Z + (1 + A) = 0$ has only one solution, that is, $Z = B^2 + B$. This would further imply that $Y \in \{0, 1, B, B + 1\}$, which is a contradiction to our assumption. Next, let the cubic equation has three solutions in \mathbb{F}_{2^n} . Now, Lemma 2.10 ensures that this is possible only when $\text{Tr}(\frac{1}{1+A}) = 1$ and t_1, t_2 are

cubes in $\mathbb{F}_{2^{2n}}$, where t_1, t_2 are roots of $t^2 + (1 + A)t + 1 = 0$. Let u_1 and u_2 be the two solutions of $Z^3 + Z + (1 + A) = 0$, except $B^2 + B$, then they must satisfy the quadratic equation $Z^2 + (B^2 + B)Z + B^4 + B^2 + 1 = 0$. One can see from Lemma 2.9 that this quadratic equation would have no solution in \mathbb{F}_{2^n} if $\text{Tr}(\frac{1}{B^2+B}) \neq 1$ and exactly two solutions in \mathbb{F}_{2^n} if $\text{Tr}(\frac{1}{B^2+B}) = 1$. Let the two solutions in later case be Z_1 and Z_2 , then it is easy to observe that $\text{Tr}(Z_1) = \text{Tr}(Z_2)$. Now, we look at the equations $Y^2 + Y + Z_i = 0$, for $i = 1, 2$, and in view of Lemma 2.9, we get that the original equation (17) has four solutions in \mathbb{F}_{2^n} when $\text{Tr}(Z_1) = \text{Tr}(Z_2) = 0$, and otherwise has no solution. This completes the proof of the theorem. \square


5. Further Comments

In this paper we concentrate on the second-order zero differential uniformity and spectra, connected to the (coefficients of the) FBCT, the counterpart concept for Feistel network-based ciphers (like 3-DES, CLEFIA, etc.), as introduced by [4]. Recall that it is known that a function is APN in even characteristic, and PN in odd characteristic if and only if the second-order zero differential uniformity is zero. It is natural to inquire what happens for APN functions in odd characteristic. We start with a rather intriguing result, where we show that if an odd or even function F is second-order zero differentially 1-uniform then it has to be an APN function. We then proceed to consider several APN, or other low differential uniform functions and check their Feistel boomerang uniformity, or even compute, for most of them, their FBCT entries. This sheds further light on the constraints between the differential uniformity and the second-order zero differential uniformity and the behavior of the latter concept. Surely, there is much to be done in this direction, and we point out that perhaps some good bounds relating the differential uniformity and the second-order zero differential uniformity would be an avenue of research, as well as investigate how various other classes of functions (besides the ones we considered) behave under this recent concept.

Acknowledgments


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.

ORCID

Kirpa Garg  <https://orcid.org/0009-0003-8680-0235>

Sartaj Ul Hasan  <https://orcid.org/0000-0002-7962-3221>

Constanza Riera  <https://orcid.org/0000-0001-8829-0847>

Pantelimon Stănică  <https://orcid.org/0000-0002-8622-7120>

References

- [1] M. R. Albrecht, L. Grassi, L. Perrin, S. Ramacher, C. Rechberger, D. Rotaru, A. Roy and M. Schafnegger, Feistel structures for MPC, and more, in *Computer Security — ESORICS 2019*, eds. K. Sako, S. Schneider and P. Ryan, Lecture Notes in Computer Science, Vol. 11736 (Springer, Cham, 2019), pp. 683–714.
- [2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology* **4**(1) (1991) 3–72.
- [3] C. Blondeau, A. Canteaut and P. Charpin, Differential properties of $X \rightarrow X^{2^t-1}$, *IEEE Trans. Inform. Theory* **57**(12) (2011) 8127–8137.
- [4] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal and M. Minier, On the Feistel counterpart of the boomerang connectivity table, *IACR Trans. Symmetric Cryptol.* **1** (2020) 331–362.
- [5] C. Boura and A. Canteaut, On the boomerang uniformity of cryptographic S-boxes, *IACR Trans. Symmetric Cryptol.* **3** (2018) 290–310.
- [6] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera and P. Stănică, Partially APN Boolean functions and classes of functions that are not APN infinitely often, *Cryptogr. Commun.* **12**(3) (2020) 527–545.
- [7] L. Budaghyan, N. Kaleyski, C. Riera and P. Stănică, Partially APN functions with APN-like polynomial representations, *Des. Codes Cryptogr.* **88** (2020) 1159–1177.
- [8] L. Budaghyan and M. Pal, Arithmetization-oriented APN functions, *Des. Codes Cryptogr.* (2024), doi:10.1007/s10623-024-01487-7.
- [9] C. Cid, T. Huang, T. Peyrin, Y. Sasaki and L. Song, Boomerang connectivity table: A new cryptanalysis tool, in *Advances in Cryptology — EUROCRYPT 2018*, eds. J. Nielsen and V. Rijmen, Lecture Notes in Computer Science, Vol. 10821 (Springer, Cham, 2018), pp. 683–714.
- [10] R. S. Coulter and M. Henderson, A note on the roots of trinomials over a finite field, *Bull. Austral. Math. Soc.* **69** (2004) 429–432.
- [11] L. E. Dickson, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* **13** (1906) 1–8.
- [12] H. Dobbertin, T. Helleseeth, P. V. Kumar and H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type, *IEEE Trans. Inform. Theory* **47**(4) (2001) 1473–1481.
- [13] S. Eddahmani and S. Mesnager, Explicit values of the DDT, the BCT, the FBCT, and the FBDT of the inverse, the Gold, and the Bracken-Leander S-boxes, *Cryptogr. Commun.* **14** (2022) 1301–1344.
- [14] P. Ellingsen, P. Felke, C. Riera, P. Stănică and A. Tkachenko, c -differentials, multiplicative uniformity, and (almost) perfect c -nonlinearity, *IEEE Trans. Inform. Theory* **66**(6) (2020) 5781–5789.
- [15] K. Garg, S. U. Hasan, C. Riera and P. Stănică, The second-order zero differential spectra of some functions over finite fields, *Cryptogr. Commun.* (2025), doi:10.1007/s12095-025-00776-9.
- [16] F. Göloğlu, A note on the differential properties of $x \mapsto x^{2^t-1}$, *IEEE Trans. Inform. Theory* **58**(11) (2012) 6986–6988.
- [17] T. Helleseeth, C. Rong and D. Sandberg, New families of almost perfect nonlinear power functions, *IEEE Trans. Inform. Theory* **45** (1999) 475–485.
- [18] X. Li, Q. Yue and D. Tang, The second-order zero differential spectra of almost perfect nonlinear functions and the inverse function in odd characteristic, *Cryptogr. Commun.* **14**(3) (2022) 653–662.

- [19] Y. Man, S. Mesnager, N. Li, X. Zeng and X. Tang, In-depth analysis of S-boxes over binary finite fields concerning their differential and Feistel boomerang differential uniformities, *Discrete Math.* **347**(12) (2024) 114185.
- [20] G. McGuire and J. Sheekey, A characterization of the number of roots of linearized and projective polynomials in the field of coefficients, *Finite Fields Appl.* **57** (2019) 68–91.
- [21] K. Nyberg, Differentially uniform mappings for cryptography, in *Advances in Cryptology — EUROCRYPT '93*, ed. T. Helleseeth, Lecture Notes in Computer Science, Vol. 765 (Springer, Heidelberg, 1994), pp. 55–64.
- [22] O. Polverino and Z. Ferdinando, On the number of roots of some linearized polynomials, *Linear Algebra Appl.* **601** (2020) 189–218.
- [23] A. Pott, Partially almost perfect nonlinear permutations, in *LOOPS*, Budapest, Hungary (2019), pp. 1–19. <https://algebra.math.bme.hu/LOOPS19/slides/pott.pdf>.
- [24] T. Shirai, K. Shibutani, T. Akishita, S. Moriai and T. Iwata, The 128-bit blockcipher CLEFIA (extended abstract), in *Fast Software Encryption-FSE 2007*, ed. A. Biryukov, Lecture Notes in Computer Science, Vol. 4593 (Springer, Berlin, 2007), pp. 181–195.
- [25] D. Wagner, The boomerang attack, in *Fast Software Encryption-FSE 1999*, ed. L. R. Knudsen, Lecture Notes in Computer Science, Vol. 1636 (Springer, Berlin, 1999), pp. 156–170.
- [26] K. S. Williams, Note on cubics over \mathbb{F}_{2^n} and \mathbb{F}_{3^n} , *J. Number Theory* **7**(4) (1975) 361–365.