The second-order zero differential spectra of some power maps

Kirpa Garg[*], Sartaj Ul Hasan[*], Constanza Riera[**], and Pantelimon Stănică[***]

[*]Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India
[**]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway
[***]Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

Abstract

It was shown by Boukerrou et al. [3] 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 also 0. It is natural to inquire what happens with APN or other low differential uniform functions in odd characteristics. As a by-product, our work implies that APN functions in odd characteristic may not have zero second-order zero differential spectra, as one might venture to conjecture. 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, and it turns out that these functions also have low second-order zero differential uniformity.

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 $\mathbb{F}_{p^n}^*$ the multiplicative cyclic group of non-zero 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 (mostly, for $p = 2$, though there are some proposals in odd characteristic) are often used in designing what are known as substitution boxes (S-boxes) in modern block ciphers. One of the most effective attacks on block ciphers is differential cryptanalysis, which was first introduced by Biham and Shamir [1]. The resistance of a function against differential attacks is measured in terms of its differential uniformity – a notion introduced by Nyberg [11]. For a function $F : \mathbb{F}_q \to \mathbb{F}_q$, and any $a \in \mathbb{F}_q$, the derivative of F in the direction a is defined as $D_F(X, a) := F(X + a) - F(X)$ for all $X \in \mathbb{F}_q$. 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 [2] 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 $\max\{\mathrm{DDT}_F(1, b) : b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\} = 2$.

The boomerang attack on block ciphers is another important cryptanalysis technique proposed by Wagner [13]. It can be considered as an extension of the classical differential attack. At Eurocrypt 2018, Cid et al. [5] introduced a systematic approach known as the Boomerang Connectivity Table (BCT), to analyze the boomerang style attack. Boura and Canteaut [4] 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. [3] 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 for Feistel ciphers, where the S-boxes may not be permutations.

The authors in [3] investigated the properties of the FBCT for two classes of vectorial functions, namely, APN functions and functions based on inverse mapping over $\mathbb{F}_{2^n}$. They showed that all the non-trivial coefficients at FBCT are 0 for APN functions over $\mathbb{F}_{2^n}$ and are 0 and 4 for the inverse function over $\mathbb{F}_{2^n}$, where n is even. In fact, the coefficients of FBCT are related to the second-order zero differential spectra of the functions. Another important property of the FBCT 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. [10] further studied the second-order zero differential spectra of the inverse function and some APN functions in odd characteristic. The authors of [10] also show that these function also have low second-order zero differential uniformity. Although most of the block ciphers operate in even characteristic, there are proposals, which work in non-binary environments, and we mention here Schroeppel's Hasty Pudding cipher (a candidate for the AES competition) [12], defined on a set of arbitrary size.

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. The second-order zero differential spectra of four power functions over finite fields of odd characteristic have been considered in Section 3. Further, in Section 4 second-order zero differential spectrum of a locally APN function has been studied. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section, we recall some definitions.

Definition 2.1 *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*

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

Definition 2.2 [3, 10] *For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ a function and $a, b \in \mathbb{F}_{p^n}$, the* second-order zero differential spectra *of F with respect to a, b is defined as*

$$\nabla_F(a,b) := \#\{X \in \mathbb{F}_{p^n} : F(X+a+b) - F(X+b) - F(X+a) + F(X) = 0\}. \tag{1}$$

If $p = 2$, 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 $p > 2$, 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 2.3 *(Feistel Boomerang Connectivity Table)* [3] *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ 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 T, in which the entry for the (a, b) position is given by:*

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

Definition 2.4 *(F-Boomerang Uniformity)* [3, 10] *The F-Boomerang uniformity corresponds to the highest value in the FBCT without considering the first row, the first column and the diagonal:*

$$\beta_F = \max_{a \neq 0, b \neq 0, a \neq b} FBCT_F(a,b).$$

Notice that the coefficients of FBCT are related to the second-order zero differential spectra of functions over $\mathbb{F}_{2^n}$. Note that the F-Boomerang uniformity is in fact the second-order zero differential uniformity of F in even characteristic.

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

Table 1 gives some of the known power functions with low second-order zero differential uniformity over finite fields of odd characteristic.

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

p	d	condition	Δ_F	∇_F	Ref
any odd p	any d	any n	1	0	[10, Lemma 2.5]
$p>3$	3	any	2	1	[10, Theorem 3.1]
$p=3$	3^n-3	$n>1$ is odd	2	2	[10, Theorem 3.2]
$p>2$	p^n-2	$p^n\equiv 2 \pmod 3$	2	1	[10, Theorem 3.3]
$p>3$	p^m+2	$n=2m$, $p^m\equiv 1 \pmod 3$	2	1	[10, Theorem 3.4]
$p=3$	3^n-2	any	3	3	[10, Theorem 3.1]
p	p^n-2	$p^n\equiv 1 \pmod 3$	3	3	[10, 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
$p=3$	$\frac{3^n-1}{2}+2$	n is odd	4	3	This paper

In this section, we first deal with the computation of 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. [8] showed that F is an APN function over $\mathbb{F}_{p^n}$, for $p^n\equiv 2 \pmod 3$.

Theorem 3.1 *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 $a,b\in\mathbb{F}_{p^n}$,*

$$\nabla_F(a,b)=\begin{cases}1 & \text{if } ab\neq 0\\ p^n & \text{if } ab=0.\end{cases} \tag{2}$$

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

Next, we considered the power function $F(X)=X^{\frac{p^k+1}{2}}$, which was shown to be an APN power function by Helleseth et al. in [8]. We further compute its second-order zero differential spectrum over $\mathbb{F}_{p^n}$.

Theorem 3.2 *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 $a,b\in\mathbb{F}_{p^n}$,*

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

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.

Remark 3.3 *Helleseth et al. in [8] showed that $F(X)=X^d$ over $\mathbb{F}_{5^n}$, where $d=\frac{5^k+1}{2}$, and $\gcd(k,2n)=1$ is an APN power function. Hence, from the above Theorem 3.2, we get that F is second-order zero differential 1-uniform over $\mathbb{F}_{5^n}$.*

Remark 3.4 *Note that, if $p = 3$, then F is PN function [6]. Therefore, by [10], it is second-order zero differential 0-uniform over $\mathbb{F}_{3^n}$.*

Now, we considered some more functions with low differential uniformity, more precisely of differential uniformity 3 and 4. Dobbertin et al. in [7] show that $F(X) = X^4$ is differentially 3 uniform for all $p > 3$ and $n > 1$. In the following theorem, we show that $F(X) = X^4$ is second-order zero differential 1-uniform for all $p > 3$ and $n > 1$.

Theorem 3.5 *Let $F(X) = X^4$ be a power function of $\mathbb{F}_{p^n}$, where $p > 3, n > 1$. Then for $a, b \in \mathbb{F}_{p^n}$,*

$$\nabla_F(a,b) = \begin{cases} 0 & \text{if } \eta\left(\frac{-a^2-b^2}{3}\right) = -1 \\ 1 & \text{if } a^2+b^2 = 0 \\ 2 & \text{if } \eta\left(\frac{-a^2-b^2}{3}\right) = 1 \\ p^n & \text{if } ab = 0. \end{cases} \tag{4}$$

Moreover, F is second-order zero differential 2-uniform.

Helleseth et al. in [9] 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 and show that it is is second-order zero differential 3-uniform.

Theorem 3.6 *Let $F(X) = X^d$ be a function of $\mathbb{F}_{3^n}$, where $d = \frac{3^n-1}{2} + 2$ and n is odd. Then for $a, b \in \mathbb{F}_{3^n}$,*

$$\nabla_F(a,b) = \begin{cases} 1 & \text{if } \eta(ab) = 1 = \eta(a^2+b^2) \text{ or } \eta(ab) = -1 \text{ and } \eta(a^2+b^2) = 1 \\ 3 & \text{if } \eta(ab) = -1 = \eta(a^2+b^2) \text{ or } \eta(ab) = 1 \text{ and } \eta(a^2+b^2) = -1 \\ 3^n & \text{if } ab = 0. \end{cases} \tag{5}$$

Moreover, F is second-order zero differential 3-uniform.

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

In this section, we compute the second-order zero differential spectrum of the locally APN function $F(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m}}$, the DDT entries for which have already been computed by Blondeau et al. in [2].

Theorem 4.1 *Let $F(X) = X^{2^m-1} \in \mathbb{F}_{2^n}[X]$, where $n = 2m$. Then for any $a, b \in \mathbb{F}_{2^n}$,*

(1) *When m is odd,*

$$\nabla_F(a,b) = \begin{cases} 2^n & \text{if } a = 0, \text{ or } b = 0, \text{ or } a = b \\ 4 & \text{if } a \neq 0, b \neq 0, a \neq b, A \neq 0 \text{ and } B = 0 \\ 2^m - 4 & \text{if } a \neq 0, b \neq 0, a \neq b, A = 0 \text{ and } B \neq 0 \\ 0 & \text{if } a \neq 0, b \neq 0, a \neq b, A = 0 \text{ and } B = 0 \\ 0 & \text{if } a \neq 0, b \neq 0, a \neq b, A \neq 0 \text{ and } B \neq 0. \end{cases}$$

(2) *When m is even,*

$$\nabla_F(a,b) = \begin{cases} 2^n & \text{if } a = 0, \text{ or } b = 0, \text{ or } a = b \\ 0 & \text{if } a \neq 0, b \neq 0, a \neq b, A \neq 0 \text{ and } B = 0 \\ 2^m - 4 & \text{if } a \neq 0, b \neq 0, a \neq b, A = 0 \text{ and } B \neq 0 \\ 0 & \text{if } a \neq 0, b \neq 0, a \neq b, A = 0 \text{ and } B = 0 \\ 0 & \text{if } a \neq 0, b \neq 0, a \neq b, A \neq 0 \text{ and } B \neq 0, \end{cases}$$

where $A = \dfrac{ab^{2^m} + ba^{2^m}}{ab(a+b)}$ *and* $B = \dfrac{a^2b^{2^m} + b^2a^{2^m}}{ab(a+b)}$. *Moreover, the Feistel boomerang uniformity of* F *is* $\beta^F(F) = 2^m - 4$.

5 Conclusion

In this paper, we extended the work of Li et al. [10] by computing the second-order zero differential spectra of some APN power functions over finite fields of odd characteristic in order to derive additional cryptographic properties of APN functions. We also determined the second-order zero differential spectrum of some functions with low differential uniformity. Additionally, all of these functions exhibit a low second-order zero differential uniformity. In our future work, we will look into more functions with low differential uniformity and investigate their second-order zero differential spectrum.

References

[1] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptol. 4:1 (1991), 3–72.

[2] C. Blondeau, A. Canteaut, P. Charpin,*Differential properties of* $X \to X^{2^t-1}$, IEEE Trans. Inf. Theory 57(12), (2011) 8127–8137.

[3] H. Boukerrou, P. Huynh, V. Lallemand, B. Mandal, M. Minier, *On the Feistel counterpart of the boomerang connectivity table,* IACR Trans. Symmetric Cryptol. 1 (2020), 331–362.

[4] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic S-boxes,* IACR Trans. Symmetric Cryptol. 3 (2018) 290–310.

[5] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, *Boomerang connectivity table: a new cryptanalysis tool.* In: J. Nielsen, V. Rijmen (ed) Advances in Cryptology-EUROCRYPT'18, LNCS 10821 683-714, Springer, Cham (2018).

[6] R.S. Coulter, R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II,* Des. Codes Cryptogr. 10(2) (1997) 167–184.

[7] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, W. Willems, *APN functions in odd characteristic*, Discrete Math. 267(1-3) (2003) 95–112.

[8] T. Helleseth, R. Chunming, S. Daniel, *New families of almost perfect nonlinear power mappings,* IEEE Trans. Inf. Theory 45.2 (1999) 475–485.

[9] T. Helleseth, D. Sandberg, *Some power mappings with low differential uniformity*, Appl. Algebra Eng. Commun. Comput. 8 (1997), 363–370.

[10] X. Li, Q. Yue, 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.

[11] K. Nyberg, *Differentially uniform mappings for cryptography,* In T. Helleseth (ed), Advances in Cryptology-EUROCRYPT'93, LNCS 765, pp. 55–64, Springer, Heidelberg (1994).

[12] R. Schroeppel, *Hasty Pudding Cipher Specifications*, `http://richard.schroeppel.name:8015/hpc/hpc-spec`; see also, https://en.wikipedia.org/wiki/Hasty_Pudding_cipher.

[13] D. Wagner, *The boomerang attack,* In: L. R. Knudsen (ed.) Fast Software Encryption-FSE 1999. LNCS 1636, Springer, Berlin, Heidelberg, (1999), pp. 156–170.