A Direct Method for Calculating the Differential Spectrum of an APN Power Mapping

Yongbo Xia*, Furong Bao*, Shaoping Chen†, and Tor Helleseth ‡

Abstract

Let n be a positive integer, p be an odd prime, $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ if $p^n \equiv 3 \pmod 8$ and $d = \frac{p^n+1}{4}$ if $p^n \equiv 7 \pmod 8$. When $p^n > 7$, the power mapping x^d from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ was proved to be almost perfect nonlinear by Helleseth, Rong and Sandberg in IEEE Trans. Inform. Theory, 45(2): 475-485, 1999. By establishing a system of linear equations related to the differential spectrum, Tan and Yan completely determined the differential spectrum of this power mapping in Des. Codes Cryptogr., 91(8): 2755-2768, 2023. In this paper, we directly characterize the conditions on $b \in \mathbb{F}_{p^n}$ under which the differential equation $(x+1)^d - x^d = b$ has exactly i solution(s) for $i = 0, 1, 2$, respectively. Then, using the theory of elliptic curves, the number of those b's in each case is determined and thus the differential spectrum of x^d is obtained. Our method releases more information about the differential equation of x^d, which can be used to describe the DDT of this APN power function.

Keywords Differential spectrum, power mapping, almost perfect nonlinear, elliptic curve.
MSC (2020) 94A60, 11T71, 11T06, 05-08

1 Introduction

Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$, where p is a prime integer and n is a positive integer. Let $F(x)$ be a mapping from $\mathbb{F}_{p^n}$ to itself. The

*Y. Xia and F. Bao are with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China (xia@mail.scuec.edu.cn). Y. Xia is also with the Hubei Key Laboratory of Intelligent Wireless Communications, South-Central University for Nationalities, Wuhan 430074, China.

†S. Chen is with the Hubei Key Laboratory of Intelligent Wireless Communications, South-Central University for Nationalities, Wuhan 430074, China (spchen@scuec.edu.cn).

‡T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (tor.helleseth@uib.no).

derivative function of $F(x)$ at an element $a \in \mathbb{F}_{p^n}$, denoted by $\mathbb{D}_a F$, is given by

$$\mathbb{D}_a F(x) = F(x+a) - F(x).$$

For any a, $b \in \mathbb{F}_{p^n}$, the equation $\mathbb{D}_a F(x) = b$ is called the *differential equation* of $F(x)$ with input difference a and output difference b. Let $\delta_F(a,b) = |\{x \in \mathbb{F}_{p^n} \mid \mathbb{D}_a F(x) = b\}|$, where $|S|$ denotes the cardinality of the set S. The *differential distribution table (DDT)* of $F(x)$ is the two-dimensional table defined by

$$(\delta_F(a,b))_{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}}.$$

The *differential uniformity* of $F(x)$ is defined as

$$\delta(F) = \max\{\delta_F(a,b) \mid a \in \mathbb{F}_{p^n}^*,\ b \in \mathbb{F}_{p^n}\}.$$

The function $F(x)$ is said to be differentially δ-uniform if $\delta(F) = \delta$. In particular, $F(x)$ is called a perfect nonlinear (PN) function if $\delta(F) = 1$, and an almost perfect nonlinear (APN) function if $\delta(F) = 2$.

Differential uniformity is an important concept in cryptography introduced by Nyberg [8], which can be used to quantify the security of the block cipher with respect to the differential attack if $F(x)$ used in the S-box. The lower the differential uniformity of $F(x)$ is, the stronger it is to resist the differential attack. Power functions with low differential uniformity have been extensively studied due to their strong resistance to differential attacks and low implementation cost.

For a power mapping $F(x) = x^d$, it is readily seen that $\delta_F(a,b) = \delta_F(1, b/a^d)$ for all $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$. The *differential spectrum* of $F(x) = x^d$ is defined as $[\omega_0, \omega_1, ..., \omega_\delta]$ with

$$\omega_i = |\{b \mid \delta_F(1,b) = i, b \in \mathbb{F}_{p^n}\}|.$$

Compared to the differential uniformity, the differential spectrum of a power mapping reflects more information about its differential property [1, 2, 3, 4]. The whole differential spectrum and even the form of the DDT play important roles when the resistance against several variants of differential cryptanalysis is quantified. According to the definition,

the differential spectrum of a power mapping $F(x)$ with $\delta(F) = \delta$ satisfies the following identities:

$$\sum_{i=0}^{\delta} \omega_i = p^n \text{ and } \sum_{i=0}^{\delta} i\omega_i = p^n. \tag{1}$$

It is an interesting topic to completely determine the differential spectra of power mappings with low differential uniformity. However, this problem typically involves solving nonlinear equations and is generally challenging. More explanations about this topic can be found in [9, 10] and references therein.

Let p be an odd prime, n be a positive integer and

$$d = \begin{cases} \frac{p^n+1}{4} + \frac{p^n-1}{2}, & \text{if } p^n \equiv 3 \pmod 8, \\ \frac{p^n+1}{4}, & \text{if } p^n \equiv 7 \pmod 8. \end{cases} \tag{2}$$

It was proved that $F(x) = x^d$ is an APN function over $\mathbb{F}_{p^n}$ when $p^n > 7$ [6]. Notice that when $p^n = 7$ or $p^n = 3$, we have $d = 2$ and the function x^d is a PN function. For the case $p = 3$, the APN mapping $F(x) = x^d$ is a special case of the power mapping investigated in [5], for which the differential spectrum has been determined. For $p > 3$, utilizing the theory of elliptic curves, Tan and Yan in [10] determined the number of solutions, denoted by M, to the following equation system

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_1^d - x_2^d + x_3^d - x_4^d = 0, \end{cases}$$

which yields the identity $\sum_{i=0}^{2} i^2\omega_i = \omega_1 + 4\omega_2 = (M - p^{2n})/(p^n - 1)$. Combining this identity and those in (1), they obtained a system of linear equations and derived the differential spectrum $[\omega_0, \omega_1, \omega_2]$ of $F(x) = x^d$. This commonly-used method can provide the differential spectra of certain power functions, nevertheless, it does not provide further insight into solving the differential equation. Accordingly, it gives little information about the DDTs.

In this paper, by directly investigating the differential equation $\mathbb{D}_1 F(x) = (x+1)^d - x^d = b$ of $F(x) = x^d$, we propose an efficient method to solve it. Then, we characterize

the conditions on b under which the differential equation $\mathbb{D}_1F(x) = b$ has exactly zero solution, one solution, and two solutions, respectively. By counting the number of those b's in all cases, we obtain the differential spectrum of $F(x) = x^d$. In this way we release more information about the solutions of the differential equation $\mathbb{D}_1F(x) = b$, which can be used to describe the form of the DDT of this APN power function.

2 Main results and their proofs

In this section, we will investigate the differential equation of the APN function $F(x) = x^d$ with d in (2), and then derive the differential spectrum of $F(x)$. The techniques for investigating the differential equation mainly come from [6, Theorem 4], but additional discussions are required. In the case $p > 3$, the differential spectrum will be expressed in terms of some quadratic character sums. When dealing with the quadratic character sums appeared in this case, we use the theory of elliptic curves and some techniques that are similar to those in [10].

Now we begin to deal with the differential equation of $F(x) = x^d$. Recall that the positive integer d given in (2) has the following two properties:
(i) $\gcd(d, p^n - 1) = 2$, and thus d is even;
(ii) $2d \equiv \frac{p^n+1}{2} \pmod{p^n - 1}$.
In the sequel our discussions are always under the condition that $p^n > 3$. The differential equation $\mathbb{D}_1F(x) = b$ of $F(x) = x^d$ is given by

$$\mathbb{D}_1F(x) = (x + 1)^d - x^d = b. \tag{3}$$

For convenience, let $N(b)$ denote the number of its solutions in $\mathbb{F}_{p^n}$. If $b = 0$, since $\gcd(d, p^n - 1) = 2$ the differential equation $\mathbb{D}_1F(x) = 0$ has only one solution $x = -\frac{1}{2}$. This shows that $N(0) = 1$. Hence, in the sequel we will investigate the differential equation $\mathbb{D}_1F(x) = b$ for $b \in \mathbb{F}_{p^n}^*$.

From (3) we see that when $x = 0$, $b = 1$; when $x = -1$, $b = -1$. This implies that for each $b \in \{\pm 1\}$, the differential equation $\mathbb{D}_1F(x) = b$ has exactly one solution in $\{0, -1\}$. In order to determine $N(1)$ (resp. $N(-1)$), we shall determine how many

solutions $\mathbb{D}_1F(x) = 1$ (resp. $\mathbb{D}_1F(x) = -1$) has in $\mathbb{F}_{p^n} \setminus \{0, -1\}$. Moreover, for each $b \neq \pm 1$, the solutions of $\mathbb{D}_1F(x) = b$ (if they exist) must belong to $\mathbb{F}_{p^n} \setminus \{0, -1\}$. Thus, in what follows we only need to investigate the differential equation $\mathbb{D}_1F(x) = b$ under that conditions that $x \in \mathbb{F}_{p^n} \setminus \{0, -1\}$ and $b \neq 0$. Set

$$v_x = x^d \text{ and } v_{x+1} = (x+1)^d.$$

Then, $v_x^2 = x^{\frac{p^n+1}{2}} = \chi(x)x$ and $v_{x+1}^2 = \chi(x+1)(x+1)$ since $2d \equiv \frac{p^n+1}{2} \pmod{p^n - 1}$, where $\chi(x) = x^{\frac{p^n-1}{2}}$ is the quadratic character of $x \in \mathbb{F}_{p^n}$ [7]. Note that the expression $v_x^2 = \chi(x)x$ implies that x is uniquely determined by v_x and $\chi(x)$.

Lemma 1 *With the notation introduced above, let $v_x = x^d$ and $v_{x+1} = (x+1)^d$. When $x \notin \{0, -1\}$, for each $b \neq 0$, the differential equation* (3) *is equivalent to the following equation system*

$$\begin{cases} (\chi(x+1)\chi(x) - 1)\, v_x^2 - 2bv_x + \chi(x+1) - b^2 = 0, \\ \chi(v_x + b) = 1. \end{cases} \tag{4}$$

Proof: If $x \in \mathbb{F}_{p^n} \setminus \{0, -1\}$ satisfies (3), then we have

$$v_{x+1} = v_x + b. \tag{5}$$

Squaring both sides of (5) yields

$$v_{x+1}^2 = v_x^2 + 2bv_x + b^2. \tag{6}$$

Substituting $v_x^2 = \chi(x)x$ and $v_{x+1}^2 = \chi(x+1)(x+1)$ into the above equation, we have

$$(\chi(x+1) - \chi(x))x + \chi(x+1) - b^2 - 2bv_x = 0, \tag{7}$$

which can be rewritten as

$$(\chi(x+1)\chi(x) - 1)\, \chi(x)x + \chi(x+1) - b^2 - 2bv_x = 0. \tag{8}$$

Furthermore, substituting $x = \chi(x)v_x^2$ into (8), we get the first equation of (4). The second equation $\chi(v_x + b) = 1$ is obvious due to (5) and $v_{x+1} = (x+1)^d$.

Conversely, let $x \in \mathbb{F}_{p^n} \setminus \{0, -1\}$ be a solution of (4). Reversing the process from (6) to (8), we can deduce that

$$-v_{x+1} = v_x + b \text{ or } v_{x+1} = v_x + b.$$

If $v_x + b$ is square, then x will satisfy the differential equation $v_{x+1} = v_x + b$ since -1 is a nonsquare and v_{x+1} is a square. □

Given $b \neq 0$, the differential equation $D_1F(x) = b$ is transformed to the equation system (4), where the first equation can be regarded as a quadratic equation in variable v_x. We have the following method of finding its solutions in $\mathbb{F}_{p^n} \setminus \{0, -1\}$:

- *Step 1:* Pose a restriction on $(\chi(x), \chi(x+1))$, which ranges over the set

$$\{(1,1),\ (1,-1),\ (-1,1),\ (-1,-1)\};$$

- *Step 2:* For each given $(\chi(x), \chi(x+1)) = (\epsilon_1, \epsilon_2)$, solve the first equation in (4) in variable v_x, where $\epsilon_i \in \{\pm 1\}$, $i = 1, 2$;

- *Step 3:* If the solution v_x satisfies

$$\chi(v_x) = 1 \text{ and } \chi(v_x + b) = 1, \tag{9}$$

  then $x = v_x^2\chi(x) = v_x^2\epsilon_1$ is a solution of (4).

- *Step 4:* Repeat the steps 2 and 3 until (ϵ_1, ϵ_2) takes all possible values. Collecting all the x's obtained in the Step 3, we get the solutions of (4) in $\mathbb{F}_{p^n} \setminus \{0, -1\}$.

To validate the above method, we need to verify that each x obtained in Step 3 must be a solution to the equation (4). More precisely, we need to show that for each given (ϵ_1, ϵ_2), the x obtained in Step 3 (if it exists) satisfies $\chi(x) = \epsilon_1$, $\chi(x+1) = \epsilon_2$ and $x^d = v_x$ (here v_x is the solution of the quadratic equation $(\epsilon_2\epsilon_1 - 1)v_x^2 - 2bv_x + \epsilon_2 - b^2 = 0$ for each given (ϵ_1, ϵ_2)). It is obvious that the x satisfies $\chi(x) = \epsilon_1$ since $x = v_x^2\epsilon_1$. Furthermore,

by $v_x^2 = x\epsilon_1$, we get $x^d\epsilon_1^d = x^d = v_x^{2d} = \chi(v_x)v_x$. With the condition $\chi(v_x) = 1$, we can conclude that the x obtained in Step 3 satisfies $v_x = x^d$. Next we verify that satisfies $\chi(x+1) = \epsilon_2$. Note that

$$(\epsilon_2\epsilon_1 - 1)v_x^2 - 2bv_x + \epsilon_2 - b^2 = \epsilon_2(v_x^2\epsilon_1 + 1) - (v_x + b)^2 = 0,$$

which implies

$$\epsilon_2(v_x^2\epsilon_1 + 1) = (v_x + b)^2.$$

Then, it follows that $\chi\left(\epsilon_2(v_x^2\epsilon_1 + 1)\right) = 1$. Since $x = v_x^2\epsilon_1$, we have $\chi(x+1) = \epsilon_2$. Due to the condition $\chi(v_x + b) = 1$ in (9), the obtained x also satisfies the second equation of (4). Therefore, the method described above is valid, and according to Lemma 1, it provides an efficient approach to deal with the differential equation $\mathbb{D}_1 F(x) = b$ in (3).

For the sake of brevity, we introduce the following sets

$$\begin{cases} \mathcal{B}_1 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{1-b^2}{2b}\right) = \chi\left(\frac{1+b^2}{2b}\right) = 1\}, \\ \mathcal{B}_2 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{-1-b^2}{2b}\right) = \chi\left(\frac{-1+b^2}{2b}\right) = 1\}, \\ \mathcal{B}_3 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{-1-b^2}{2}\right) = \chi(-2-b^2) = 1\}, \\ \mathcal{B}_4 := \{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\frac{1-b^2}{2}\right) = \chi(2-b^2) = 1\}, \end{cases} \tag{10}$$

where $p^n > 3$. Generally, these sets have the following relations as illustrated in Figure 1:

(i) $\{0, \pm 1\} \cap \cup_{i=1}^4 \mathcal{B}_i = \emptyset$;

(ii) $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$;

(iii) $\mathcal{B}_i \cap \mathcal{B}_3 \cap \mathcal{B}_4 = \emptyset$, $i = 1, 2$.

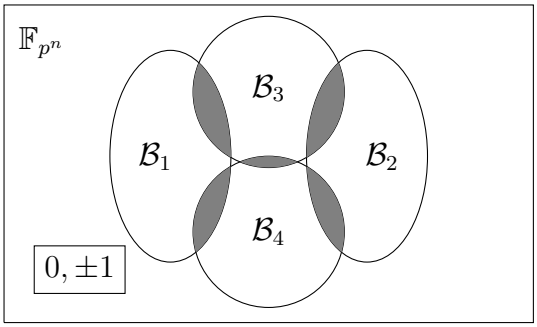
It is easy to verify the properties (i) and (ii). The reason for the property (iii) is given as follows. For $b \in \mathcal{B}_1 \cup \mathcal{B}_2$, we have

$$\chi\left(\frac{1-b^2}{2b}\right)\chi\left(\frac{1+b^2}{2b}\right) = \chi\left(\frac{1-b^2}{2}\right)\chi\left(\frac{1+b^2}{2}\right) = 1,$$

while for $b \in \mathcal{B}_3 \cap \mathcal{B}_4$, we have

$$\chi\left(\frac{1-b^2}{2}\right)\chi\left(\frac{1+b^2}{2}\right) = -1.$$

Figure 1: Diagram of $\mathcal{B}_i$ $(i = 1, 2, 3, 4)$ and their relations



Thus, the intersection is empty.

Set

$$\begin{cases} \mathcal{C}_1 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (1,1)\}, \\ \mathcal{C}_2 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (-1,-1)\}, \\ \mathcal{C}_3 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (1,-1)\}, \\ \mathcal{C}_4 := \{x \in \mathbb{F}_{p^n}^* \mid (\chi(x), \chi(x+1)) = (-1,1)\}. \end{cases}$$

Then, $\mathcal{C}_i$, $i = 1, 2, 3, 4$, are pairwise disjoint and $\cup_{i=1}^4 \mathcal{C}_i = \mathbb{F}_{p^n} \setminus \{0, -1\}$. With these preparations, we give the following proposition.

Proposition 1 *With the notation introduced above, let d be the positive integer defined in (2) with $p^n > 3$, and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$. Then, when $b \neq 0$, the differential equation $(x+1)^d - x^d = b$ has at most one solution in $\mathcal{C}_i$, and it has exactly one solution in $\mathcal{C}_i$ if and only if $b \in \mathcal{B}_i$, $i = 1, 2, 3, 4$.*

Proof: By Lemma 1, for each $b \neq 0$, we only need to consider the number of solutions of (4) in $\mathbb{F}_{p^n} \setminus \{0, -1\}$. We distinguish four cases.

Case 1: $x \in \mathcal{C}_1$, i.e., $(\chi(x), \chi(x+1)) = (1, 1)$. Then (4) becomes

$$\begin{cases} v_x = \frac{1-b^2}{2b}, \\ \chi\left(\frac{1+b^2}{2b}\right) = 1. \end{cases}$$

According to (9), this case contributes one solution if and only if $b \in \mathcal{B}_1$.

Case 2: $x \in \mathcal{C}_2$, i.e., $(\chi(x), \chi(x+1)) = (-1,-1)$. In this case, (4) can be rewritten as

$$\begin{cases} v_x = \frac{-1-b^2}{2b}, \\ \chi\left(\frac{-1+b^2}{2b}\right) = 1. \end{cases}$$

Similarly, this case contributes one solution if and only if $b \in \mathcal{B}_2$.

Case 3: $x \in \mathcal{C}_3$, i.e., $(\chi(x), \chi(x+1)) = (1,-1)$. In this case, (4) becomes

$$\begin{cases} v_x^2 + bv_x + \frac{1+b^2}{2} = 0, \\ \chi(v_x + b) = 1. \end{cases} \tag{11}$$

The first equation in (11) is a quadratic equation in variable v_x and its discriminant is equal to $-2-b^2$. If $\chi(-2-b^2) = 1$, (11) is equivalent to the following two equation systems:

$$\begin{cases} v_{x_1} = \frac{-b+\sqrt{-2-b^2}}{2}, \\ \chi(v_{x_1} + b) = \chi\left(\frac{b+\sqrt{-2-b^2}}{2}\right) = 1, \end{cases} \tag{12}$$

or

$$\begin{cases} v_{x_2} = \frac{-b-\sqrt{-2-b^2}}{2}, \\ \chi(v_{x_2} + b) = \chi\left(\frac{b-\sqrt{-2-b^2}}{2}\right) = 1. \end{cases} \tag{13}$$

Note that $v_{x_i}(v_{x_i}+b) = \frac{-1-b^2}{2}$, $i = 1, 2$. To make sure (12) or (13) contributes one solution to (4), it is necessary to have $\chi\left(\frac{-1-b^2}{2}\right) = 1$, which further implies that $\chi(v_{x_1}v_{x_2}) = \chi\left(\frac{1+b^2}{2}\right) = -1$. So one and only one of v_{x_1} and v_{x_2} is square. Therefore, we can conclude that when $b \in \mathcal{B}_3$, one and only one of (12) and (13) contributes one solution to (4).

Note that if $-2-b^2 = 0$, the first equation in (4) has only one solution v_x, and this solution satisfies $v_x(v_x+b) = \frac{-b^2}{4}$, which is a nonsquare. Thus, the condition in (9) does not hold. So (4) has no solution in this case.

The above discussions show that when $x \in \mathcal{C}_3$, (4) has at most one solution, and it has exactly one solution if and only if $b \in \mathcal{B}_3$.

Case 4: $x \in \mathcal{C}_4$, i.e., $(\chi(x), \chi(x+1)) = (-1, 1)$. In this case, (4) becomes

$$\begin{cases} v_x^2 + bv_x + \frac{-1+b^2}{2} = 0, \\ \chi(v_x + b) = 1. \end{cases} \tag{14}$$

The first equation in (14) is also a quadratic equation in variable v_x and the discriminant is equal to $2 - b^2$. If $\chi(2 - b^2) = 1$, it has two solutions, denoted by $v_{x_1} = \frac{-b+\sqrt{2-b^2}}{2}$ and $v_{x_2} = \frac{-b-\sqrt{2-b^2}}{2}$, which satisfy $v_{x_i}(v_{x_i} + b) = \frac{1-b^2}{2}$, $i = 1, 2$. To make sure that (14) can have solutions, it is necessary to have $\chi\left(\frac{1-b^2}{2}\right) = 1$, which leads to that $\chi\left(\frac{-1+b^2}{2}\right) = \chi(v_{x_1}v_{x_2}) = -1$. This means that one and only one of v_{x_1} and v_{x_2} is square. Therefore, when $b \in \mathcal{B}_4$, (14) can contribute one and only one solution to (4). Moreover, if $2 - b^2 = 0$, we have $v_x(v_x + b) = \frac{-b^2}{4}$, which is a nonsquare. Due to (9), we know that under this condition (14) has no solution. Therefore, we can conclude that this case can contribute exactly one solution if and only if $b \in \mathcal{B}_4$.

Based on the results obtained in Cases 1-4, we get the the desired result. □

According to Proposition 1 and its proof, we can characterize the conditions on b for which the differential equation $(x+1)^d - x^d = b$ has no solution, exactly one solution and two solutions, respectively.

Proposition 2 *With the same notation as in Proposition 1, for each $b \in \mathbb{F}_{p^n}$, let $p^n > 3$ and $N(b)$ denote the number of solutions $x \in \mathbb{F}_{p^n}$ to the differential equation $\mathbb{D}_1 F(x) = (x+1)^d - x^d = b$. Then,*

$$N(b) = \begin{cases} 0, & \text{if } b \in \mathbb{F}_{p^n} \setminus (\{0, \pm 1\} \cup \mathcal{B}), \\ 1, & \text{if } b \in \{0, \pm 1\} \cup \mathcal{B} \setminus \widetilde{\mathcal{B}}, \\ 2, & \text{if } b \in \widetilde{\mathcal{B}}, \end{cases} \tag{15}$$

where $\mathcal{B} = \cup_{i=1}^{4} \mathcal{B}_i$, and $\widetilde{\mathcal{B}} = (\mathcal{B}_1 \cap \mathcal{B}_3) \cup (\mathcal{B}_1 \cap \mathcal{B}_4) \cup (\mathcal{B}_2 \cap \mathcal{B}_3) \cup (\mathcal{B}_2 \cap \mathcal{B}_4) \cup (\mathcal{B}_3 \cap \mathcal{B}_4)$, which corresponds to the gray areas shown in Figure 1.

Proof: Recall that $x = 0$ (resp. $x = -1$) is a solution of $\mathbb{D}_1 F(x) = 1$ (resp. $\mathbb{D}_1 F(x) = -1$). Due to Proposition 1 and the fact $\pm 1 \notin \mathcal{B}$, we know that for each $b \in \{\pm 1\}$, the differential equation $\mathbb{D}_1 F(x) = b$ has no solution in $\cup_{i=1}^{4} \mathcal{C}_i = \mathbb{F}_{p^n} \setminus \{0, -1\}$ and thus $N(\pm 1) = 1$. Together with the fact $N(0) = 1$, we have $N(b) = 1$ for $b \in \{0, \pm 1\}$. On the other hand, for each $b \notin \{\pm 1\}$, the differential equation $\mathbb{D}_1 F(x) = b$ has no solution in $\{0, -1\}$ and its solutions in $\mathbb{F}_{p^n}$ are exactly those in $\mathbb{F}_{p^n} \setminus \{0, -1\}$. Thus, according to Proposition 1, we conclude that $N(b) \geq 1$ if $b \in \mathcal{B}$, and $N(b) = 0$ if $b \notin \{0, \pm 1\} \cup \mathcal{B}$.

Furthermore, note that the properties (ii) and (iii) about the sets $\mathcal{B}_i$ $(i = 1, 2, 3, 4)$ imply that the differential equation cannot have solutions in $\mathcal{C}_1$ and $\mathcal{C}_2$ simultaneously, and cannot have solutions simultaneously in any three sets of $\mathcal{C}_i$, $i = 1, 2, 3, 4$, either. Thus, for each $b \in \mathcal{B}$, $N(b) \leq 2$. Moreover, according to Proposition 1 and its proof, $N(b) = 2$ if and only if b belongs to the intersection of any two sets of $\mathcal{B}_i$, $i = 1, 2, 3, 4$. Thus $N(b) = 2$ if and only if $b \in \widetilde{\mathcal{B}}$. Removing the elements in $\widetilde{\mathcal{B}}$ from the set $\mathcal{B}$ and adding the elements of $\{0, \pm 1\}$, we can get the elements b such that $N(b) = 1$. The relationships between the sets mentioned above can be easily observed with the help of Figure 1. □

Proposition 2 has characterized the sets of elements b for $N(b) = 0$, 1 and 2 , respectively. Next we need to calculate the cardinalities of the sets in Proposition 2, thereby determining the differential spectrum of $F(x) = x^d$. The sets $\mathcal{B}_i$, $i = 1, 2, 3, 4$, are defined in terms of quadratic characters. Hence we use quadratic character sums to calculate the cardinalities of the sets in (15) in Propositions 2. Many quadratic character sums involved can be reduced to a simpler form in the case $p = 3$. Thus, we deal with the cases $p > 3$ and $p = 3$ separately. We first consider the case $p > 3$.

When $p > 3$, for simplicity, we will express the relevant quadratic character sums in terms of the following three quadratic character sums:

$$\Gamma_{p,n}^{(1)} = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(x(x-1)(x-3)\right), \tag{16}$$

$$\Gamma_{p,n}^{(2)} = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(x(x-1)(x+2)\right), \tag{17}$$

and

$$\Gamma_{p,n}^{(3)} = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(x(x-1)(x+3)\right). \tag{18}$$

These three quadratic character sums can be evaluated by the theory of elliptic curves, and the details have been described in [9] and [10]. The following two lemmas evaluate the quadratic character sums derived from Propositions 2, some of which are expressed in terms of $\Gamma_{p,n}^{(i)}$, $i = 1, 2, 3$.

Lemma 2 *Let $p > 3$, and $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$. Then, we have 24 identities in Table 1, where $\Gamma_{p,n}^{(1)}$, $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are defined in* (16), (17) and (18), respectively.

Table 1: Some identities about quadratic character sums

1)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x^2-1)\right) = 0$	2)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x^2+1)\right) = 0$
3)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(1-2x)(2-2x)\right) = 0$	4)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(1+x)(2-2x)\right) = 0$
5)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-1)(x+3)(3x+1)\right) = 0$	6)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x+1)(2x-2)\right) = \chi(2)\Gamma_{p,n}^{(1)}$
7)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(3x+1)\right) = \Gamma_{p,n}^{(2)}$	8)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x-2)(6x-2)\right) = -\Gamma_{p,n}^{(2)}$
9)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(2x-2)(6-2x)\right) = \Gamma_{p,n}^{(2)}$	10)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x-1)(3x+1)\right) = -\Gamma_{p,n}^{(3)}$
11)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(6x-2)\right) = \chi(2)\Gamma_{p,n}^{(3)}$	12)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(6-2x)\right) = \chi(2)\Gamma_{p,n}^{(3)}$
13)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(3x+1)(x+3)\right) = -\Gamma_{p,n}^{(3)}$	14)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)\right) = 1$
15)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+x^2)\right) = \chi(2) + \chi(2)\Gamma_{p,n}^{(1)}$	16)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2-x^2)\right) = -\chi(2)$
17)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2-x^2)\right) = \chi(2) - \chi(2)\Gamma_{p,n}^{(1)}$	18)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2+x^2)\right) = -\chi(2)$
19)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)\right) = 1$	20)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right) = 1 + \Gamma_{p,n}^{(2)} - \Gamma_{p,n}^{(3)}$
21)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2-x^2)\right) = -1 + \Gamma_{p,n}^{(2)} + \Gamma_{p,n}^{(3)}$	22)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)(2+2x^2)\right) = \chi(2) + \chi(2)\Gamma_{p,n}^{(3)} - \Gamma_{p,n}^{(2)}$
23)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-x^2)(2+x^2)(2-2x^2)\right) = -\chi(2) + \chi(2)\Gamma_{p,n}^{(3)} + \Gamma_{p,n}^{(2)}$	24)	$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)(2-x^2)\right) = -1 - \Gamma_{p,n}^{(3)}$

Proof: See Appendix A. □

The conditions that $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$ are equivalent to n being odd and $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$. Note that the element 2 is a nonsquare in $\mathbb{F}_p$ if $p \equiv 3 \pmod 8$ and a square in $\mathbb{F}_p$ if $p \equiv 7 \pmod 8$, and -1 is a nonsquare when $p^n \equiv 3 \pmod 4$. Therefore, the element 2 is a square in $\mathbb{F}_{p^n}$ if $p^n \equiv 7 \pmod 8$, and a nonsquare if $p^n \equiv 3 \pmod 8$; -2 is a nonsquare in $\mathbb{F}_{p^n}$ if $p^n \equiv 7 \pmod 8$, and a square if $p^n \equiv 3 \pmod 8$. In order to present our main results, we need to define the following three sets

$$\mathcal{A}_1 = \begin{cases} \{\pm 1, \pm\sqrt{-2}\}, & \text{if } p^n \equiv 3 \pmod 8, \\ \{\pm 1\}, & \text{if } p^n \equiv 7 \pmod 8, \end{cases} \tag{19}$$

$$\mathcal{A}_2 = \begin{cases} \{\pm 1\}, & \text{if } p^n \equiv 3 \pmod 8, \\ \{\pm 1, \pm\sqrt{2}\}, & \text{if } p^n \equiv 7 \pmod 8, \end{cases} \tag{20}$$

and

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2. \tag{21}$$

Lemma 3 *With the notation introduced above, let $p > 3$, and $p^n \equiv 3 \pmod 8$ or $p^n \equiv 7 \pmod 8$, then we have*

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}_1} \big((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\big) = p^n+1+\chi(2)\Gamma_{p,n}^{(1)}-\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)},$$

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}_2} \big((1+\chi(2-2x^2))(1+\chi(2+2x^2))(1+\chi(2-x^2))\big) = p^n-7-\chi(2)\Gamma_{p,n}^{(1)}+\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)},$$

and

$$\sum_{x \in \mathbb{F}_{p^n} \setminus \mathcal{A}} \big((1+\chi(2-2x^2))(1-\chi(2+2x^2))(1+\chi(2-x^2))(1-\chi(2+x^2))\big) = p^n+1-2\Gamma_{p,n}^{(2)}-3\Gamma_{p,n}^{(3)},$$

where $\Gamma_{p,n}^{(1)}$, $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are defined in (16), (17) and (18), respectively.

Proof: See Appendix B.

□

Keeping the notation introduced above, we have the following main theorem.

Theorem 1 *Let d be defined in (2) and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$. When $p > 3$ and $p^n > 7$, the differential spectrum of $F(x) = x^d$ is given by*

$$[\,\omega_0, \omega_1, \omega_2\,] = [\,\frac{5p^n - 27 - 2\Gamma_{p,n}^{(2)} + \Gamma_{p,n}^{(3)}}{16}, \frac{3p^n + 27 + 2\Gamma_{p,n}^{(2)} - \Gamma_{p,n}^{(3)}}{8}, \frac{5p^n - 27 - 2\Gamma_{p,n}^{(2)} + \Gamma_{p,n}^{(3)}}{16}\,],$$

where $\Gamma_{p,n}^{(2)}$ and $\Gamma_{p,n}^{(3)}$ are given in (17) and (18).

Proof: Determining the differential spectrum of $F(x) = x^d$ requires calculating the cardinalities of the sets in (15). We start with calculating the cardinality of $\widetilde{\mathcal{B}}$, which is exactly the component ω_2 in the differential spectrum of $F(x)$. According to (10), we have

$$\begin{aligned}
|\mathcal{B}_1 \cap \mathcal{B}_3| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi\left(\tfrac{1-b^2}{2b}\right) = 1, \chi\left(\tfrac{1+b^2}{2b}\right) = 1, \chi\left(\tfrac{-1-b^2}{2}\right) = 1, \chi(-2-b^2) = 1\}| \\
&= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = -1, \chi(2+2b^2) = -1, \chi(2+b^2) = -1, \chi(b) = -1\}|, \\
|\mathcal{B}_1 \cap \mathcal{B}_4| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = 1, \chi(2+2b^2) = 1, \chi(2-b^2) = 1, \chi(b) = 1\}|, \\
|\mathcal{B}_2 \cap \mathcal{B}_3| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = -1, \chi(2+2b^2) = -1, \chi(2+b^2) = -1, \chi(b) = 1\}|, \\
|\mathcal{B}_2 \cap \mathcal{B}_4| &= |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = 1, \chi(2+2b^2) = 1, \chi(2-b^2) = 1, \chi(b) = -1\}|,
\end{aligned}$$

and

$$|\mathcal{B}_3 \cap \mathcal{B}_4| = |\{b \in \mathbb{F}_{p^n}^* \mid \chi(2-2b^2) = 1, \chi(2+2b^2) = -1, \chi(2-b^2) = 1, \chi(2+b^2) = -1\}|.$$

Note that the sets $\mathcal{B}_1 \cap \mathcal{B}_3$, $\mathcal{B}_1 \cap \mathcal{B}_4$, $\mathcal{B}_2 \cap \mathcal{B}_3$, $\mathcal{B}_2 \cap \mathcal{B}_4$ and $\mathcal{B}_3 \cap \mathcal{B}_4$ are pairwise disjoint, see Figure 1. Denote the cardinality of $\mathcal{B}_i \cap \mathcal{B}_j$ by $N_{i,j}$, where $i \neq j$. It can be seen that $N_{1,3} = N_{2,3}$ since $b \in \mathcal{B}_1 \cap \mathcal{B}_3$ if and only if $-b \in \mathcal{B}_2 \cap \mathcal{B}_3$. Similarly, $N_{1,4} = N_{2,4}$ since $b \in \mathcal{B}_1 \cap \mathcal{B}_4$ if and only if $-b \in \mathcal{B}_2 \cap \mathcal{B}_4$. Moreover, we have

$$8(N_{1,3} + N_{2,3}) = \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}_1} \left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right),$$

$$8(N_{1,4} + N_{2,4}) = \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}_2} \left((1+\chi(2-2x^2))(1+\chi(2+2x^2))(1+\chi(2-x^2))\right),$$

and

$$16N_{3,4} = \sum_{x \in \mathbb{F}_{p^n}^* \setminus \mathcal{A}} \left((1+\chi(2-2x^2))(1-\chi(2+2x^2))(1+\chi(2-x^2))(1-\chi(2+x^2))\right),$$

where $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}$ being defined in (19), (20) and (21), respectively. By Lemma 3, we

obtain

$$N_{1,3}+N_{2,3}=\frac{p^n+1+\chi(2)\Gamma_{p,n}^{(1)}-\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}-(1-\chi(2))^3}{8},$$
$$N_{1,4}+N_{2,4}=\frac{p^n-7-\chi(2)\Gamma_{p,n}^{(1)}+\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}-(1+\chi(2))^3}{8},$$
$$N_{3,4}=\frac{p^n+1-2\Gamma_{p,n}^{(2)}-3\Gamma_{p,n}^{(3)}}{16}.$$

Then we obtain

$$\omega_2=|\widetilde{\mathcal{B}}|=N_{1,3}+N_{1,4}+N_{2,3}+N_{2,4}+N_{3,4}=\frac{5p^n-27-2\Gamma_{p,n}^{(2)}+\Gamma_{p,n}^{(3)}}{16}. \tag{22}$$

Next we determine the component ω_1 in the differential spectrum of $F(x)$. Based on the properties of $\mathcal{B}_i$, $i=1,2,3,4$, which are illustrated in Figure 1, we have

$$|\{0,\pm1\}\cup\mathcal{B}\setminus\widetilde{\mathcal{B}}|=3+\sum_{i=1}^{4}|\mathcal{B}_i|-2|\widetilde{\mathcal{B}}|. \tag{23}$$

According to the definition of $\mathcal{B}_i$ in (10), $i=1,2,3,4$, we can calculate their cardinalities as follows.

$$\begin{aligned}4|\mathcal{B}_1|&=\sum_{x\in\mathbb{F}_{p^n}\setminus\{0,\pm1\}}\big(1+\chi(2x(1+x^2))\big)\big(1+\chi(2x(1-x^2))\big)\\&=p^n-4+\sum_{x\in\mathbb{F}_{p^n}}\chi(2x(1+x^2))+\sum_{x\in\mathbb{F}_{p^n}}\chi(2x(1-x^2))+\sum_{x\in\mathbb{F}_{p^n}}\chi\big((1-x^2)(1+x^2)\big)\\&=p^n-3,\end{aligned}$$

where we use the identities 1), 2) and 14) in Table 1. Similarly, we have

$$\begin{aligned}4|\mathcal{B}_2|&=\sum_{x\in\mathbb{F}_{p^n}\setminus\{0,\pm1\}}\big(1-\chi(2x(1+x^2))\big)\big(1-\chi(2x(1-x^2))\big)\\&=p^n-3.\end{aligned}$$

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be the sets defined in (19) and (20), respectively. Then

$$\begin{aligned}
4|\mathcal{B}_3| &= \sum_{\mathbb{F}_{p^n}^* \setminus \mathcal{A}_1} \left((1-\chi(2+2x^2))\left(1-\chi(2+x^2)\right)\right) \\
&= \sum_{x\in\mathbb{F}_{p^n}} \left(1-\chi(2+2x^2)\right)\left(1-\chi(2+x^2)\right) - (1-\chi(2))^2 \\
&= p^n + \chi(2) + 1 + \sum_{x\in\mathbb{F}_{p^n}} \chi\left((2+2x^2)(2+x^2)\right) - (1-\chi(2))^2 \\
&= p^n + 1 - (1-\chi(2))^2,
\end{aligned}$$

where we use the identity 18) in Table 1. Similarly,

$$\begin{aligned}
4|\mathcal{B}_4| &= \sum_{x\in\Omega_1=\mathbb{F}_{p^n}^* \setminus \mathcal{A}_2} \left((1+\chi(2-2x^2))(1+\chi(2-x^2))\right) \\
&= \sum_{x\in\mathbb{F}_{p^n}} \left((1+\chi(2-2x^2))(1+\chi(2-x^2))\right) - (1+\chi(2))^2 - 4 \\
&= p^n - 3 - (1+\chi(2))^2.
\end{aligned}$$

Therefore, we get

$$\sum_{i=1}^{4} |\mathcal{B}_i| = p^n - 3. \tag{24}$$

Substituting (24) and (22) into (23), we obtain

$$\omega_1 = \frac{3p^n + 27 + 2\Gamma_{p,n}^{(2)} - \Gamma_{p,n}^{(3)}}{8}.$$

Finally, we determine the component ω_0 in the differential spectrum of $F(x)$. According to (15), (24) and (22), we get

$$\omega_0 = p^n - 3 - |\mathcal{B}| = p^n - 3 - \sum_{i=1}^{4} |\mathcal{B}_i| + |\widetilde{\mathcal{B}}| = \frac{5p^n - 27 - 2\Gamma_{p,n}^{(2)} + \Gamma_{p,n}^{(3)}}{16}.$$

The proof is finished. □

Remark 1 *After we determined the component ω_2 in (22), we actually can utilize the identities (1) to derive ω_1 and ω_0. Here we don't use these identities since we want to give a direct calculation via determining the sizes of the corresponding sets. The reason why we can do this lies in that we successfully characterize the conditions on b under which the differential equation $\mathbb{D}_1F(x) = b$ has exactly i solution(s) in $\mathbb{F}_{p^n}$, $i = 0, 1, 2$. This characterization reveals more essential information about the differential equation $\mathbb{D}_1F(x) = b$ and can be used to describe the form of the DDT of $F(x) = x^d$.*

Remark 2 *When the power function $F(x) = x^d$ in this theorem is APN, we must have $\omega_2 = \frac{5p^n-27-2\Gamma^{(2)}_{p,n}+\Gamma^{(3)}_{p,n}}{16} > 0$. According to the Weil bound in [7, Theorem 5.41], when $p > 3$ we have $-2\sqrt{p^n} \le \Gamma^{(2)}_{p,n}, \Gamma^{(3)}_{p,n} \le 2\sqrt{p^n}$. Thus,*

$$5p^n - 27 - 2\Gamma^{(2)}_{p,n} + \Gamma^{(3)}_{p,n} \ge 5p^n - 6\sqrt{p^n} - 27.$$

To make sure $\omega_2 > 0$, it suffices that $5p^n - 6\sqrt{p^n} - 27 > 0$, which implies $p^n > 9$. When p is odd and n is odd, $p^n > 9$ is equivalent to that $p^n > 7$. This explains again why we need the condition $p^n > 7$ when x^d is APN.

Remark 3 *When $p^n = 7$, by Magma, we get $\Gamma^{(2)}_{p,n} = 4$ and $\Gamma^{(3)}_{p,n} = 0$. Using the the formulas in Theorem 1, we get $\omega_2 = 0$, $\omega_1 = 7$ and $\omega_0 = 0$, which coincides with the fact that x^d is the PN function x^2 when $p^n = 7$. This shows that the formulas of the differential spectrum in this theorem also hold for $p^n = 7$.*

Remark 4 *Note that*

$$\Gamma^{(2)}_{p,n} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-x(-x-1)(-x+2)\right) = -\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-2)\right)$$

and

$$\Gamma^{(3)}_{p,n} = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-x(-x-1)(-x+3)\right) = -\sum_{x\in\mathbb{F}_{p^n}} \chi\left(x(x+1)(x-3)\right).$$

Therefore, Theorem 1 agrees with Theorem 3 in [10].

Next we give the differential spectrum of $F(x) = x^d$ in the case $p = 3$.

Theorem 2 *Let $p = 3$, $n \geq 3$ and $F(x) = x^d$ be the power mapping over $\mathbb{F}_{p^n}$ with d being defined by (2). The differential spectrum of $F(x) = x^d$ is given by*

$$[\,\omega_0, \omega_1, \omega_2\,] = [\,\frac{p^n - 3}{2},\, 3,\, \frac{p^n - 3}{2}\,].$$

Proof: With the same notation in Proposition 2, when $p = 3$, besides the properties displayed in Figure 1, the sets $\mathcal{B}_i$, $i = 1, 2, 3, 4$, in (10) have more special properties as follows:
(a) when $\chi(b) = 1$, $\mathcal{B}_1 \cap \mathcal{B}_3 = \emptyset$, $\mathcal{B}_1 = \mathcal{B}_4$, $\mathcal{B}_2 = \mathcal{B}_3$, and $\mathcal{B}_2 \cap \mathcal{B}_4 = \emptyset$;
(b) when $\chi(b) = -1$, $\mathcal{B}_1 = \mathcal{B}_3$, $\mathcal{B}_1 \cap \mathcal{B}_4 = \emptyset$, $\mathcal{B}_2 \cap \mathcal{B}_3 = \emptyset$, and $\mathcal{B}_2 = \mathcal{B}_4$;
(c) $\mathcal{B}_3 \cap \mathcal{B}_4 = \emptyset$.
From the properties above, we know that

$$\widetilde{\mathcal{B}} = \mathcal{B}_1 \cup \mathcal{B}_2 \text{ and } \mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2.$$

Utilizing the the theory of quadratic character sums, we can get $|\mathcal{B}_1| = |\mathcal{B}_2| = \frac{3^n-3}{4}$. Then, according to Proposition 2, we get $\omega_2 = |\widetilde{\mathcal{B}}| = |\mathcal{B}_1| + |\mathcal{B}_2| = \frac{3^n-3}{2}$, $\omega_1 = |\{0, \pm 1\} \cup \mathcal{B} \setminus \widetilde{\mathcal{B}}| = 3$, and $\omega_0 = p^n - 3 - |\mathcal{B}| = \frac{3^n-3}{2}$. □

As a special case of Theorem 3 in [5], by taking $m = 1$ there, one gets the same result of Theorem 2.

3 Conclusion

In this paper, we study the differential spectrum of the APN function $F(x) = x^d$ over $\mathbb{F}_{p^n}$, where $p^n > 7$, $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ if $p^n \equiv 3 \pmod 8$ and $d = \frac{p^n+1}{4}$ if $p^n \equiv 7 \pmod 8$. We first present an efficient algorithm to find the solutions of the differential equation $\mathbb{D}_1 F(x) = b$, and then characterize the conditions on b under which $\mathbb{D}_1 F(x) = b$ has exactly two solutions, one solution and no solution, respectively. We determine the cardinalities of the associated sets by the theory of elliptic curves, and thus obtain the

differential spectrum of $F(x)$. Compared with the method in [10], we provide a direct method for computing the differential spectrum of $F(x)$. In addition, the obtained results about the differential equation $\mathbb{D}_1 F(x) = b$ can be used to describe the form of the DDT of $F(x)$. Thus, our method explores more information about the differential properties of this APN function. The idea used in this paper may be used to calculate the differential spectra of other power mappings over finite fields of odd characteristic.

Acknowledgment

The authors wish to thank Dr. Chunlei Li for his valuable discussions and suggestions. Y. Xia and F. Bao were supported in part by the National Natural Science Foundation of China under Grant 62171479, and in part by the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities under Grant CZZ23004. S. Chen was supported in part by the National Natural Science Foundation of China under Grant 61971452 and in part by the Fund for Scientific Research Platforms of South-Central Minzu University under Grant PTZ24004. T. Helleseth is supported by the Research Council of Norway under Grant 311646.

References

[1] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149-170, 2010.

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \mapsto x^{2^t-1}$," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8127-8137, 2011.

[3] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions," *Des. Codes Cryptogr.*, vol. 73, no. 2, pp. 487-505, 2014.

[4] C. Boura, A. Canteaut, J. Jean, and V. Suder, "Two notions of differential equivalence on Sboxes," *Des. Codes Cryptogr.*, vol. 87, no. 6, pp. 185-202, 2019.

[5] S. T. Choi, S. Hong, J. S. No, and H. Chung, "Differential spectrum of some power functions in odd prime characteristic," *Finite Fields Appl.*, vol. 21, pp. 11-29, 2013.

[6] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 475-485, 1999.

[7] R. Lidl and H. Niederreiter, *Finite Fields,* Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge U.K: Cambridge University Press, 1997.

[8] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765. Berlin, Germany: Springer-Verlag, 1994, pp. 55-64.

[9] H. Yan, Y. Xia, C. Li, T. Helleseth, M. Xiong, and J. Luo, "The differential spectrum of the power mapping x^{p^n-3}," *IEEE Trans. Inf. Theory*, vol. 68, no. 8, pp. 5535-5547, 2022.

[10] X. Tan and H. Yan. "Differential spectrum of a class of APN power functions," *Des. Codes Cryptogr.*, vol. 91, no. 8, pp. 2755-2768, 2023.

Appendix A

The Proof of Lemma 2: All these identities are required to calculates the sizes of the sets appeared in Proposition 2. The identities 3) to 13) will be used in the proofs of the identities 14) to 24). We only give the proof for identities 1), 13), 14) and 20) in Table 1. The other identities can be similarly proved.

Identity 1): Let $x = -u$, then we have

$$\sum_{x\in\mathbb{F}_{p^n}} \chi(x(x^2-1)) = \sum_{u\in\mathbb{F}_{p^n}} \chi(-u(u^2-1)) = \chi(-1)\sum_{u\in\mathbb{F}_{p^n}} \chi(u(u^2-1))$$

which implies that $\sum_{x\in\mathbb{F}_{p^n}} \chi(x(x^2-1)) = 0$ since $\chi(-1) = -1$.

Identity 13): Note that

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^n}}\chi\left(x(3x+1)(x+3)\right) &= \sum_{x\in\mathbb{F}_{p^n}}\chi\left(3x(3x+1)(3x+9)\right)\\ &= \sum_{u\in\mathbb{F}_{p^n}}\chi\left(u(u+1)(u+9)\right)\\ &= \sum_{u\in\mathbb{F}_{p^n}^*}\chi\left(\frac{(u+1)(u+9)}{u}\right).\end{aligned}$$

For $u\neq 0$, let

$$\frac{(u+1)(u+9)}{u}=v,$$

then each $v\in\mathbb{F}_{p^n}$ corresponds to $1+\chi\left((v-4)(v-16)\right)$ u's. Thus, we obtain

$$\begin{aligned}\sum_{u\in\mathbb{F}_{p^n}^*}\chi\left(\frac{(u+1)(u+9)}{u}\right) &= \sum_{v\in\mathbb{F}_{p^n}}\chi(v)\left(1+\chi((v-4)(v-16))\right)\\ &= \sum_{v\in\mathbb{F}_{p^n}}\chi\left(v(v-4)(v-16)\right)\\ &= \sum_{v\in\mathbb{F}_{p^n}}\chi\left(\frac{v}{4}(\frac{v}{4}-1)(\frac{v}{4}-4)\right).\end{aligned}$$

Furthermore, let $t=\frac{v}{4}-1$ and $w=-t$, then

$$\begin{aligned}\sum_{u\in\mathbb{F}_{p^n}^*}\chi\left(\frac{(u+1)(u+9)}{u}\right) &= \sum_{v\in\mathbb{F}_{p^n}}\chi\left(\frac{v}{4}(\frac{v}{4}-1)(\frac{v}{4}-4)\right)\\ &= \sum_{t\in\mathbb{F}_{p^n}}\chi\left(t(t+1)(t-3)\right)\\ &= \sum_{w\in\mathbb{F}_{p^n}}\chi\left(w(1-w)(w+3)\right)\\ &= -\Gamma_{p,n}^{(3)}.\end{aligned}$$

Identity 14): Note that

$$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)\right) = \sum_{x\in\mathbb{F}_{p^n}} \chi\left((1-x^2)(1+x^2)\right)$$
$$= \sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}\right).$$

Let $\frac{1+x^2}{1-x^2} = u$, then x and u satisfy

$$(u+1)x^2 + 1 - u = 0. \tag{25}$$

When $u \neq -1$, (25) is a quadratic equation in variable x, and its discriminant is $\Delta = 4(u+1)(u-1)$. For each $u \neq -1$, it corresponds to $(1+\chi(\Delta))$ x's via (25). Thus, we obtain

$$\sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}\right) = \sum_{u\neq -1} \chi(u)\left(1+\chi((u+1)(u-1))\right)$$
$$= 1 + \sum_{u\in\mathbb{F}_{p^n}} \chi(u) + \sum_{u\in\mathbb{F}_{p^n}} \chi\left(u(u^2-1)\right).$$

This together with the identity 1) shows that $\sum_{x\in\mathbb{F}_{p^n}} \chi\left((1-x^2)(1+x^2)\right) = 1$.

Identity 20): We have

$$\sum_{x\in\mathbb{F}_{p^n}} \chi\left((2-2x^2)(2+2x^2)(2+x^2)\right) = \sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}} \chi\left(\frac{1+x^2}{1-x^2}(2+x^2)\right).$$

Let $\frac{1+x^2}{1-x^2} = u$, then x and u satisfy

$$(u+1)x^2 + 1 - u = 0. \tag{26}$$

When $u \neq -1$, (26) is a quadratic equation in variable x, and its discriminant is $4(u+1)(u-1)$. For each $u \in \mathbb{F}_{p^n} \setminus \{-1\}$, it corresponds $(1+\chi(\Delta))$ x's via (26). Moreover,

from (26), we have $2+x^2=\frac{3u+1}{u+1}$. Thus,

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{p^n}\setminus\{\pm 1\}}\chi\left(\frac{1+x^2}{1-x^2}(2+x^2)\right)\\
&=\sum_{u\neq -1}\chi\left(u\left(\frac{3u+1}{u+1}\right)\right)(1+\chi(u+1)(u-1))\\
&=\sum_{u\neq -1}\chi(u(u+1)(3u+1))+\sum_{u\neq -1}\chi\left(u(3u+1)(u-1)\right)\\
&=\sum_{u\in\mathbb{F}_{p^n}}\chi(u(u+1)(3u+1))+\sum_{u\in\mathbb{F}_{p^n}}\chi\left(u(3u+1)(u-1)\right)+1.
\end{aligned}$$

Furthermore, utilizing the identities 7) and 10), we have $\sum\limits_{x\in\mathbb{F}_{p^n}}\chi\left((2-2x^2)(2+2x^2)(2+x^2)\right)=$ $1+\Gamma^{(2)}_{p,n}-\Gamma^{(3)}_{p,n}$. □

Appendix B

The Proof of Lemma 3:

For the first equation, we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{p^n}\setminus\mathcal{A}_1}\left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right)\\
&=\sum_{x\in\mathbb{F}_{p^n}}1-\sum_{x\in\mathbb{F}_{p^n}}\chi(2-2x^2)-\sum_{x\in\mathbb{F}_{p^n}}\chi(2+2x^2)-\sum_{x\in\mathbb{F}_{p^n}}\chi(2+x^2)\\
&\quad+\sum_{x\in\mathbb{F}_{p^n}}\chi\left((2-2x^2)(2+2x^2)\right)+\sum_{x\in\mathbb{F}_{p^n}}\chi\left((2-2x^2)(2+x^2)\right)\\
&\quad+\sum_{x\in\mathbb{F}_{p^n}}\chi\left((2+2x^2)(2+x^2)\right)-\sum_{x\in\mathbb{F}_{p^n}}\chi\left((2-2x^2)(2+2x^2)(2+x^2)\right)\\
&\quad-\sum_{\mathcal{A}_1}\left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right).
\end{aligned}$$

Note that $\sum\limits_{\mathcal{A}_1}\left((1-\chi(2-2x^2))(1-\chi(2+2x^2))(1-\chi(2+x^2))\right)=0$, and the character

sums associated with any quadratic polynomial can be evaluated by [7, Theorem 5.48]. Then, by Lemma 2, we can obtain the desired result. The second and third identities can be similarly proved, and we omit the proofs here. □