The Differential Spectrum of the Power Mapping x^{p^n-3}

Haode Yan, Yongbo Xia, Chunlei Li, Tor Helleseth, Maosheng Xiong and Jinquan Luo

Abstract

Let n be a positive integer and p a prime. The power mapping x^{p^n-3} over $\mathbb{F}_{p^n}$ has desirable differential properties, and its differential spectra for $p=2,3$ have been determined. In this paper, for any odd prime p, by investigating certain quadratic character sums and some equations over $\mathbb{F}_{p^n}$, we determine the differential spectrum of x^{p^n-3} with a unified approach. The obtained result shows that for any given odd prime p, the differential spectrum can be expressed explicitly in terms of n. Compared with previous results, a special elliptic curve over $\mathbb{F}_p$ plays an important role in our computation for the general case $p \geq 5$.

Index Terms

Power mapping, Differential cryptanalysis, Differential spectrum, Quadratic character sum, Elliptic curve.

I. 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 number and n is a positive integer. Let $F(x)$ be a function from $\mathbb{F}_{p^n}$ to itself. The *derivative function*, denoted by $\mathbb{D}_a F$, of $F(x)$ at an element a in $\mathbb{F}_{p^n}$ is given by

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

For any $a, b \in \mathbb{F}_{p^n}$, let

$$\delta_F(a,b) = |\{x \in \mathbb{F}_{p^n} | \ \mathbb{D}_a F(x) = b\}|,$$

where $|S|$ denotes the cardinality of a set S, and define

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

A function F is said to be *differentially* δ*-uniform* iff $\delta(F) = \delta$, and δ is called the *differential uniformity* of $F(x)$ accordingly [19]. The *differential spectrum* of $F(x)$ is defined as the multiset

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

H. Yan was partially supported the National Natural Science Foundation of China under Grant 11801468 and the projects of central government to guide local scientific and technological development under Grant 2021ZYD0001. Y. Xia was supported in part by NSFC under Grants 62171479 and 61771021, and in part by the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities under Grant CZT20023. C. Li and T. Helleseth were supported by the Research Council of Norway under Grants 247742 and 311646. M. Xiong was supported by RGC, Hong Kong, under Grant N_HKUST619/17. J. Luo was supported by NSFC under Grant 12171191 and in part by Hubei Provincial Science and Technology Innovation Base (Platform) Special Project 2020DFH002. (*Corresponding author: Yongbo Xia*).

H. Yan is with the School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China (e-mail: hdyan@swjtu.edu.cn).

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

C. Li and T. Helleseth are with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: chunlei.li@uib.no, tor.helleseth@uib.no).

M. Xiong is with the Department of Mathematics, The Hong Kong University of Science and Technology, Hong Kong (e-mail: mamsxiong@ust.hk).

J. Luo is with the Hubei Key Laboratory of Mathematical Sciences, School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China (E-mail: luojinquan@mail.ccnu.edu.cn).

TABLE I
SOME POWER FUNCTIONS $F(x) = x^d$ OVER $\mathbb{F}_{p^n}$ WITH KNOWN DIFFERENTIAL SPECTRUM

p	d	Condition	$\delta(F)$	Ref.
2	2^t+1	$\gcd(t,n)=s$	2^s	[2]
2	$2^{2t}-2^t+1$	$\gcd(t,n)=s$, n/s odd	2^s	[2]
2	2^n-2	$n \geq 2$	2 or 4	[2]
2	$2^{2k}+2^k+1$	$n=4k$	4	[2], [23]
2	2^t-1	$t=3,n-2$	6 or 8	[3]
2	2^t-1	$t=n/2,n/2+1$, n even	$2^{n/2}-2$ or $2^{n/2}$	[3]
2	2^t-1	$t=(n-1)/2,(n+3)/2$, n odd	6 or 8	[4]
2	$2^m+2^{(m+1)/2}+1$	$n=2m$, $m \geq 5$ odd	8	[24]
2	$2^{m+1}+3$	$n=2m$, $m \geq 5$ odd	8	[24]
2	$2^{3k}+2^{2k}+2^k-1$	$n=4k$	2^{2k}	[14]
3	$2 \cdot 3^{(n-1)/2}+1$	n odd	4	[11]
3	3^n-3	n odd, $n \equiv 2 (\text{mod } 4)$, or $n \equiv 0 (\text{mod } 4)$	$2,4$, or 5	[22]
p odd	$(p^k+1)/2$	$e=\gcd(n,k)$	$(p^e-1)/2$ or p^e+1	[10]
p odd	$(p^n+1)/(p^m+1)+(p^n-1)/2$	$p \equiv 3 \pmod 4$, n odd, $m \mid n$	$(p^m+1)/2$	[10]
p odd	$p^{2k}-p^k+1$	$\gcd(n,k)=e$, n/e odd,	p^e+1	[25], [17]

When $F(x)$ is a power mapping, i.e., $F(x) = x^d$ for a positive integer d, one easily sees that $\delta_F(a,b) = \delta_F(1,b/a^d)$ for all $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$. That is to say, the differential spectrum of $F(x)$ is completely determined by the values of $\delta_F(1,b)$ as b runs through $\mathbb{F}_{p^n}$. Therefore, the differential spectrum of a power mapping can be simplified as follows.

Definition 1. *Assume that a power function $F(x) = x^d$ over $\mathbb{F}_{p^n}$ has differential uniformity δ and denote*

$$\omega_i = \left| \left\{ b \in \mathbb{F}_{p^n} \mid \delta_F(1,b) = i \right\} \right|, \ 0 \leq i \leq \delta.$$

The differential spectrum of F is simply defined to be an ordered sequence

$$\mathbb{S} = [\omega_0, \omega_1, \ldots, \omega_\delta].$$

Due to the differential cryptanalysis [1], the differential property is one of the most fundamental parameters of cryptographic primitives in block ciphers. Consequently, it is highly desirable that nonlinear functions for cryptographic applications have low differential uniformity. For example, the AES (Advanced Encryption Standard) uses the inverse function $x \mapsto x^{-1}$ over $\mathbb{F}_{2^n}$, which has differential uniformity 4 for even n and 2 for odd n. Besides the differential uniformity, the differential spectrum of a nonlinear function also reflects its differential property. It is usually taken into consideration when one assesses the resistance of a function against differential cryptanalysis and its variants [2], [3], [4]. Moreover, the differential spectrum of a nonlinear function is also related to the nonlinearity of the function, which is an important parameter of a function with respect to linear cryptanalysis [7], [9], [18].

In addition to its importance in cryptography, the differential spectrum of a nonlinear function also plays a significant role in sequences, coding theory and combinatorial design. In sequences, the differential spectrum of a power mapping can be used to determine the cross-correlation between m-sequences and their decimation sequences [11]; in coding theory, the differential spectrum is highly related to the number of low weight codewords in some linear codes [2], [6], [8]; and in combinatorial designs, some new 2-designs can be constructed from differentially two-valued functions [21]. Therefore, it is an interesting topic to completely determine the differential spectrum of a nonlinear function with low differential uniformity. This problem is, nevertheless, relatively challenging. So far, only a few infinite families of power mappings have known differential spectra, which are listed in TABLE I.

The investigation of differential spectra of power mappings over finite fields, to the best of our knowledge, first appeared in [11], where the authors considered the differential spectrum of x^d over $\mathbb{F}_{3^n}$ with odd n and $d = 2 \cdot 3^{\frac{n-1}{2}} + 1$ (known as the ternary Welch exponent). The result obtained there was then used to resolve the ternary Welch conjecture that the cross-correlation function between an m-sequence of period 3^n-1 and its ternary Welch decimation sequence takes exactly three values. Blondeau, Canteaut and Charpin later in [2] dedicated their research focus to the differential spectra of several power mappings in the binary case, including quadratic power mappings, Bracken-Leander power mapping and Kasami power mapping, and they proposed some conjectures. The differential properties of the power mappings x^{2^t-1} over $\mathbb{F}_{2^n}$ were later investigated in [3] and [4], where the differential spectra of x^{2^t-1} for certain special t's were determined. Xiong et al. in [24] proved one of the conjectures in [2] about the differential spectra of the power functions with Niho exponents. Very recently, for the power mapping $x^{2^{3k}+2^{2k}+2^k-1}$ over $\mathbb{F}_{2^n}$ with $n=4k$, Li et al. [14] determined its differential spectrum, which gives an affirmative answer to the conjecture proposed in [5]. In recent years some research progress has also been made for the nonbinary cases. Choi et. al [10] computed the differential spectra of two power functions $x^{\frac{p^k+1}{2}}$ and $x^{\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}}$, where the conditions on p,n,k,m are listed in TABLE I. The differential spectra of the family of p-ary Kasami power permutation $x^{p^{2k}-p^k+1}$ over $\mathbb{F}_{p^n}$ with $\gcd(n,k)=1$ and its generalized family with $\gcd(n,k)=e$ were investigated in [25] and [17], respectively.

Our study in this paper originates from the work of Helleseth, Rong and Sandberg [13], where they intensively studied the differential properties of a number of power functions and presented several families of APN functions. In particular, the differential properties of the power function x^{p^n-3} were characterized as follows.

Theorem 1. *[13, Theorem 7] Let $d=p^n-3$ and let $F(x)=x^d$ be a mapping over $\mathbb{F}_{p^n}$.*
(i) If $p=2$, then $\delta(F)=2$ when n is odd and $\delta(F)=4$ when n is even.
(ii) If p is an odd prime, then $1\leq\delta(F)\leq 5$.
(iii) If $n>1$ is odd and $p=3$, then $\delta(F)=2$.

Given Theorem 1, a natural question arises: what is the differential spectrum of the power mapping x^{p^n-3} over $\mathbb{F}_{p^n}$? There are some partial answers to this question. By setting $\frac{1}{0}=0$, the above power mapping can be rewritten as $F(x)=x^{-2}$. When $p=2$, it is equivalent to the inverse function x^{-1} over $\mathbb{F}_{2^n}$, of which the differential spectrum has been determined in [2]. Recently, for $p=3$ the differential spectrum of $F(x)=x^{p^n-3}$ was completely determined in [22], where the authors characterized the conditions on b such that the derivative equation $\mathbb{D}_1F(x)=F(x+1)-F(x)=b$ has two and four roots in $\mathbb{F}_{3^n}$, respectively. The method used in [22] relies heavily on the characteristic $p=3$, and it is not clear how it may work for the general prime p.

In this paper, for any odd prime p, we present a unified approach to studying the differential spectrum of x^{p^n-3}, which is different from that used in [22]. In our approach, we investigate several related equations in details, and establish a connection between the differential spectrum of x^{p^n-3} and two quadratic character sums that are associated with two quartic polynomials. For the case $p=3$, the two quartic polynomials are essentially quadratic ones and hence the two quadratic character sums can be evaluated directly; when $p\geq 5$, both of the quadratic character sums are related to a single elliptic curve over $\mathbb{F}_p$, and they can be computed by the theory of elliptic curves. As a result, for any given odd prime p, the differential spectrum of x^{p^n-3} can be derived and expressed explicitly in terms of n. Therefore, our work completely settles the unsolved problem about the differential spectrum of x^{p^n-3} in Theorem 7 of [13].

The rest of this paper is organized as follows. Section II introduces some quadratic character sums and the related theory of elliptic curves over $\mathbb{F}_{p^n}$. In Section III, we will determine the number of solutions to an equation system, which is dependent on a quadratic character sum presented in Section II. With the preparations in Sections II and III, the differential spectrum of x^{p^n-3} is computed in Section IV. Section V concludes this paper.

II. Some quadratic sums and the theory of elliptic curves

From now on, we always assume that p is an odd prime and η is the quadratic multiplicative character of $\mathbb{F}_{p^n}^*$. It is convenient to extend the definition of η to $\mathbb{F}_{p^n}$ by setting $\eta(0)=0$. For an element $\beta\in\mathbb{F}_{p^n}$, if

$\eta(\beta)=1$, then it has exactly two square roots in $\mathbb{F}_{p^n}$, which are denoted by $\pm\sqrt{\beta}$ throughout this paper. In the sequel, for convenience we also frequently adopt the convention that $\frac{1}{0}:=0$.

Let $\mathbb{F}_{p^n}[x]$ denote the polynomial ring over $\mathbb{F}_{p^n}$. We shall consider the sums involving the quadratic character and having polynomial arguments of the form

$$\sum_{x\in\mathbb{F}_{p^n}}\eta(f(x))$$

with $f(x)\in\mathbb{F}_{p^n}[x]$. It is clear that the case of linear $f(x)$ is trivial. When $f(x)$ is quadratic, the explicit formula was given in [15].

Lemma 2. *[15, Theorem 5.48] Let $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_{p^n}[x]$ with p odd and $a_2\neq 0$. Put $d=a_1^2-4a_0a_2$ and let η be the quadratic character of $\mathbb{F}_{p^n}$. Then*

$$\sum_{x\in\mathbb{F}_{p^n}}\eta(f(x))=\begin{cases}-\eta(a_2), & \textit{if } d\neq 0,\\ (p^n-1)\eta(a_2), & \textit{if } d=0.\end{cases}$$

As it will be seen in Sections III and IV, the computation of the differential spectrum of the power mapping x^{p^n-3} over $\mathbb{F}_{p^n}$ boils down to evaluating two specific character sums

$$\lambda_{1,p^n}:=\sum_{x\in\mathbb{F}_{p^n}}\eta\left((x^2-4)(-3x^2-4)\right), \tag{1}$$

and

$$\lambda_{2,p^n}:=\sum_{x\in\mathbb{F}_{p^n}}\eta\left((x^2+1)(x^2+4x+1)\right). \tag{2}$$

Note that in the case of $p=3$ the above character sums can be easily computed. To be more concrete, one has $-3x^2-4=-4$ and $x^2+4x+1=(x+2)^2$, then the polynomials involved in $\lambda_{1,3^n}$ and $\lambda_{2,3^n}$ are essentially quadratic ones. Hence Lemma 2 can be applied directly and we have

$$\lambda_{1,3^n}=-\eta(-1)\ \text{and}\ \lambda_{2,3^n}=-1-\eta(2). \tag{3}$$

When $p\geq 5$, the situation is quite different. The polynomials involved in λ_{1,p^n} and λ_{2,p^n} are of degree 4, these character sums correspond to the elliptic curves $y^2=(x^2-4)(-3x^2-4)$ and $y^2=(x^2+1)(x^2+4x+1)$ over $\mathbb{F}_p$ respectively. Generally speaking, by the theory of elliptic curves in [20], there is no explicit formula for the evaluation of such character sums in general, except for some very special kinds of elliptic curves that are very rare. The following theorem provides an efficient method to evaluate λ_{1,p^n} and λ_{2,p^n} for $p\geq 5$ based on the theory of elliptic curves.

Theorem 3. *Let $p\geq 5$. Denote by N_p the number of $(x,y)\in\mathbb{F}_p^2$ satisfying the equation*

$$E: y^2=x(x-1)(x+3). \tag{4}$$

Define $a=N_p-p$ and let r_1 and r_2 be the two roots of the quadratic polynomial T^2+aT+p in the complex number field. Define

$$\Gamma_{p,n}:=\sum_{x\in\mathbb{F}_{p^n}}\eta(x(x-1)(x+3)). \tag{5}$$

Then

$$\begin{cases}\Gamma_{p,n} &= -r_1^n-r_2^n,\\ \lambda_{1,p^n} &= \Gamma_{p,n}-\eta(-3),\\ \lambda_{2,p^n} &= \Gamma_{p,n}-1.\end{cases} \tag{6}$$

Proof. The equation (4) defines an elliptic curve E over $\mathbb{F}_p$. The quadratic character sum $\Gamma_{p,n}$ defined in (5) is closely related to the number of $\mathbb{F}_{p^n}$-rational points (with the extra point at infinity) on E, which is actually equal to $p^n+1+\Gamma_{p,n}$. By the theory of elliptic curves (see [20, Theorem 2.3.1, Chap. V]), we have

$$\Gamma_{p,n} = -r_1^n - r_2^n.$$

The Weil bound for $\Gamma_{p,n}$ is that $|\Gamma_{p,n}| \leq 2\sqrt{p^n}$ (see [20, Corollary 1.4, Chap. V]). Note that $a = \Gamma_{p,1}$, which is an integer. Thus, we have $a^2 < 4p$ and $r_1 \neq r_2$.

Now using $\Gamma_{p,n}$ we can evaluate λ_{1,p^n} as follows:

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{p^n}} \eta\left((x^2-4)(-3x^2-4)\right) \\
=\ & 1+2\sum_{\eta(u)=1} \eta\left((u-4)(-3u-4)\right) \\
=\ & 1+2\sum_{\eta(u)=1} \eta\left((1-\tfrac{4}{u})(-3-\tfrac{4}{u})\right) \\
=\ & 1+2\sum_{\eta(u)=1} \eta\left((1-u)(-3-u)\right) \\
=\ & 1+\sum_{u\in\mathbb{F}_{p^n}} (1+\eta(u))\eta\left((u-1)(u+3)\right) \\
& -\eta(-3) \\
=\ & \sum_{u\in\mathbb{F}_{p^n}} \eta\left((u-1)(u+3)\right)+\Gamma_{p,n}+1-\eta(-3).
\end{aligned}$$

The first term $\sum_{u\in\mathbb{F}_{p^n}} \eta\left((u-1)(u+3)\right) = -1$ according to Lemma 2. Thus we have the desired result for λ_{1,p^n}.

As for λ_{2,p^n}, let $\frac{x^2+4x+1}{x^2+1} = u$. Then, u and x satisfy

$$(u-1)x^2-4x+(u-1)=0. \tag{7}$$

It is easy to see that $x=0$ if and only if $u=1$. When $u\neq 1$, (7) is a quadratic equation in the variable x, and it has solutions in $\mathbb{F}_{p^n}$ if and only if $\eta(\Delta)=\eta((u+1)(-u+3))=1$ or 0. If $u=-1$ (resp. $u=3$), then $x=-1$ (resp. $x=1$) is the unique solution of (7). If $u\neq 1$ and $\eta((u+1)(-u+3))=1$, there are two distinct x's satisfying (7). Thus we have

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{p^n}} \eta\left(\frac{x^2+4x+1}{x^2+1}\right) &= \eta(1)+\eta(-1) \\
&\quad +\eta(3)+2\sum_{u\in\mathcal{U}}\eta(u),
\end{aligned} \tag{8}$$

where

$$\mathcal{U} = \{u\in\mathbb{F}_{p^n} \mid u\neq 1, \eta((u+1)(-u+3))=1\},$$

and we may adopt the convention that $\frac{1}{0} := 0$. Furthermore,

$$\begin{aligned}
& 2\sum_{u\in\mathcal{U}}\eta(u) \\
= & \sum_{u\neq 1}(1+\eta((u+1)(-u+3)))\eta(u) \\
& -\eta(-1)-\eta(3) \\
= & \sum_{u\in\mathbb{F}_{p^n}}(1+\eta((u+1)(-u+3)))\eta(u) \\
& -2\eta(1)-\eta(-1)-\eta(3) \\
= & \sum_{u\in\mathbb{F}_{p^n}}\eta(u)+\sum_{u\in\mathbb{F}_{p^n}}\eta(u(u+1)(-u+3)) \\
& -2\eta(1)-\eta(-1)-\eta(3) \\
= & \sum_{u\in\mathbb{F}_{p^n}}\eta((-u)(-u+1)(u+3)) \\
& -2\eta(1)-\eta(-1)-\eta(3) \\
= & \Gamma_{p,n}-2\eta(1)-\eta(-1)-\eta(3),
\end{aligned}$$

where the fourth equality holds since $\sum_{u\in\mathbb{F}_{p^n}}\eta(u)=0$. This together with (8) yields

$$\sum_{x\in\mathbb{F}_{p^n}}\eta\left(\frac{x^2+4x+1}{x^2+1}\right)=\Gamma_{p,n}-1.$$

Since

$$\begin{aligned}
\lambda_{2,p^n} &= \sum_{x\in\mathbb{F}_{p^n}}\eta\left(\tfrac{x^2+4x+1}{x^2+1}\right)\eta\left((x^2+1)^2\right) \\
&= \sum_{x\in\mathbb{F}_{p^n}}\eta\left(\tfrac{x^2+4x+1}{x^2+1}\right),
\end{aligned}$$

the desired evaluation of λ_{2,p^n} follows. □

Remark 1. *We emphasize that a unified explicit formula of the character sum $\Gamma_{p,n}$ for all primes $p\geq 5$ and positive integers n may not exist at all; and we have the same situation for λ_{1,p^n} and λ_{2,p^n}. However, Theorem 3 enables us to give a practical and efficient algorithm for evaluating these character sums, which can be described as follows:*

- ***Step 1:*** *For each given $p\geq 5$, compute the quantity N_p, which can be easily computed for most practical values of p by Magma . Then, we get $a=N_p-p$.*
- ***Step 2:*** *Determine the two roots r_1 and r_2 of the polynomial x^2+aT+p in the complex number field, which are*

$$r_1,=\frac{-a+\sqrt{a^2-4p}}{2},\quad r_2=\frac{-a-\sqrt{a^2-4p}}{2}.$$

- ***Step 3:*** *Compute $\Gamma_{p,n}$, λ_{1,p^n} and λ_{2,p^n} according to (6).*

Note that $a=\Gamma_{p,1}$ and thus in Step 1 we can compute the value of a directly according to (5).

Utilizing the above algorithm, one knows that for any given prime $p\geq 5$, the character sums $\Gamma_{p,n}$, λ_{1,p^n} and λ_{2,p^n} can be computed and expressed explicitly in terms of n. The procedure of the above algorithm is illustrated in the following example.

Example 1. *For $p=5$, by using Magma we can obtain $N_5=7$, hence $a=2$. So we have $r_1,r_2=-1\pm 2\sqrt{-1}$, hence*

$$\Gamma_{5,n}=-\left(-1+2\sqrt{-1}\right)^n-\left(-1-2\sqrt{-1}\right)^n.$$

TABLE II
THE VALUES OF $\Gamma_{p,1}$ FOR $p \leq 1000$

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$\Gamma_{p,1}$	2	0	−4	2	−2	4	8	−6	−8	−6	6	−4	0	2
p	59	61	67	71	73	79	83	89	97	101	103	107	109	113
$\Gamma_{p,1}$	−4	2	4	−8	−10	8	4	6	−2	18	−16	12	2	−18
p	127	131	137	139	149	151	157	163	167	173	179	181	191	193
$\Gamma_{p,1}$	8	4	6	12	−14	16	2	−12	−24	−6	−12	−6	0	−2
p	197	199	211	223	227	229	233	239	241	251	257	263	269	271
$\Gamma_{p,1}$	18	−16	20	8	−12	−22	−10	16	−18	−20	−2	8	10	−8
p	277	281	283	293	307	311	313	317	331	337	347	349	353	359
$\Gamma_{p,1}$	26	−26	28	18	−12	24	6	−6	−20	−18	12	−30	−2	24
p	367	373	379	383	389	397	401	409	419	421	431	433	439	443
$\Gamma_{p,1}$	8	10	−20	0	2	−14	30	6	−12	10	−32	14	0	−20
p	449	457	461	463	467	479	487	491	499	503	509	521	523	541
$\Gamma_{p,1}$	14	22	26	−8	36	16	32	12	−12	−24	−6	−26	−4	18
p	547	557	563	569	571	577	587	593	599	601	607	613	617	619
$\Gamma_{p,1}$	−44	26	−28	−10	−36	−2	44	14	−24	38	40	−38	−42	44
p	631	641	643	647	653	659	661	673	677	683	691	701	709	719
$\Gamma_{p,1}$	−16	14	−12	−8	−6	−12	10	−34	2	−4	4	−6	10	32
p	727	733	739	743	751	757	761	769	773	787	797	809	811	821
$\Gamma_{p,1}$	−48	−14	4	8	−24	−38	22	−2	18	−28	−22	−26	−4	−30
p	823	827	829	839	853	857	859	863	877	881	883	887	907	911
$\Gamma_{p,1}$	16	28	50	24	10	−42	12	32	18	−50	4	−8	−4	−16
p	919	929	937	941	947	953	967	971	977	983	991	997		
$\Gamma_{p,1}$	−16	−50	−42	−6	−12	54	16	−36	30	24	−40	26		

For $p = 7$, by using Magma we can obtain $a = 0$ by (5). So we have $r_1, r_2 = \pm\sqrt{-7}$. Then, we get

$$\Gamma_{7,n} = -\left(1 + (-1)^n\right)\sqrt{-7}^{\,n}.$$

The values of $\Gamma_{p,n}$ for other p can be obtained similarly. Once the value of $\Gamma_{p,n}$ is obtained, so are the values of λ_{1,p^n} and λ_{2,p^n}.

Remark 2. *If $a = 0$, then $r_1, r_2 = \pm\sqrt{-p}$, and we have a simple expression of $\Gamma_{p,n}$ as*

$$\Gamma_{p,n} = \begin{cases} 0, & \text{if } n \text{ is odd,} \\ -2\sqrt{-1}^{\,n} p^{n/2}, & \text{if } n \text{ is even.} \end{cases}$$

It was known that $a = 0$ if and only if the elliptic curve E defined over $\mathbb{F}_p$ in (4) is supersingular, and there is an explicit and efficient formula to determine whether or not E is supersingular (see [20, Theorem 4.1, Chap. V]). In particular, for $p \leq 1000$, the elliptic curve E defined over $\mathbb{F}_p$ is supersingular if $p = 7, 47, 191, 383$ and 439, thus in these cases the values $\Gamma_{p,n}$, λ_{1,p^n} and λ_{2,p^n} can be presented in a more compact form.

Remark 3. *In Table II, for all primes $p \leq 1000$ we list the values of $\Gamma_{p,1}$, which are computed with Magma. Let*

$$D_n(x,1) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-1)^i x^{n-2i}$$

be the Dickson polynomial of degree n [16]. Then, we have

$$D_n(y + \frac{1}{y}, 1) = y^n + \frac{1}{y^n}.$$

With this identity and Theorem 3, we have

$$\Gamma_{p,n} = -p^{n/2} D_n\left(-\frac{\Gamma_{p,1}}{\sqrt{p}}, 1\right).$$

III. THE NUMBER OF SOLUTIONS TO AN EQUATION SYSTEM

Let $d = p^n - 3$ with p being an odd prime. Denote by $\mathcal{M}$ the set of solutions $(x_1, x_2, x_3, x_4) \in (\mathbb{F}_{p^n})^4$ of the equation system

$$\left\{ \begin{array}{rcl} x_1 - x_2 + x_3 - x_4 & = & 0, \\ x_1^d - x_2^d + x_3^d - x_4^d & = & 0, \end{array} \right. \tag{9}$$

and $M = |\mathcal{M}|$. In this section we shall compute the value of M, which plays an important role in determining the differential spectrum of the power mapping x^{p^n-3} over $\mathbb{F}_{p^n}$.

To this end, we need to make some preparations. Define

$$\mathcal{M}_i = \left\{(x_1, x_2, x_3, x_4) \in \mathcal{M} \mid x_i = 0\right\}, \, i = 1, 2, 3, 4,$$

and

$$\mathcal{M}^{\circ} = \left\{(x_1, x_2, x_3, x_4) \in \mathcal{M} \mid x_1 x_2 x_3 x_4 \neq 0\right\}.$$

For any $1 \leq i < j < k \leq 4$, it is trivial to see that

$$|\mathcal{M}_i \cap \mathcal{M}_j| = \begin{cases} 1, & \text{if } (i, j) \in \{(1,3), \\ & \qquad\qquad (2,4)\}, \\ p^n, & \text{otherwise}, \end{cases} \tag{10}$$

$$|\mathcal{M}_i \cap \mathcal{M}_j \cap \mathcal{M}_k| = 1 \text{ and } \left|\cap_{i=1}^4 \mathcal{M}_i\right| = 1. \tag{11}$$

Next we compute $|\mathcal{M}_i|$ $(1 \leq i \leq 4)$ and $|\mathcal{M}^{\circ}|$.

The following result about a quartic equation over $\mathbb{F}_{p^n}$ is useful for computing $|\mathcal{M}_i|$ $(1 \leq i \leq 4)$. Before we give the result, we recall from Section II that for any $\beta \in \mathbb{F}_{p^n}$ with $\eta(\beta) = 1$, the two square roots of β are denoted by $\sqrt{\beta}$ and $-\sqrt{\beta}$.

Lemma 4. *Let $p \geq 3$ be an odd prime, and $g_1(x) = x^4 + 2x^3 + x^2 + 2x + 1 \in \mathbb{F}_{p^n}[x]$. Denote by T_1 the number of roots of $g_1(x)$ in $\mathbb{F}_{p^n}$. Then, we have*

$$T_1 = \begin{cases} 0, \text{ if } \eta(2) = -1, \text{ or } \eta(2) = \eta(-7) = 1 \\ \quad \text{but } \eta(-1 + 2\sqrt{2}) = -1, \\ 1, \text{ if } p = 7 \text{ and } n \text{ is odd}, \\ 2, \text{ if } \eta(2) = 1 \text{ and } \eta(-7) = -1, \\ 3, \text{ if } p = 7 \text{ and } n \text{ is even}, \\ 4, \text{ if } \eta(2) = \eta(-7) = \eta(-1 + 2\sqrt{2}) = 1. \end{cases}$$

Proof. Let $x \in \mathbb{F}_{p^n}$ be a solution of $g_1(x)$, then we have

$$\left(x + \frac{1}{x}\right)^2 + 2\left(x + \frac{1}{x}\right) - 1 = 0, \tag{12}$$

which can be regarded as a quadratic equation in variable $z = x + \frac{1}{x}$ with discriminant $\Delta = 2^2 - 4 \cdot (-1) = 8$. If $\eta(\Delta) = -1$, that is, $\eta(2) = -1$, then $T_1 = 0$. Now suppose $\eta(\Delta) = \eta(2) = 1$. Solving (12), we have

$$x + \frac{1}{x} = -1 \mp \sqrt{2},$$

which implies that

$$x^2+(1\pm\sqrt{2})x+1=0. \tag{13}$$

To solve (13) over $\mathbb{F}_{p^n}$, we compute the corresponding discriminants which are $\Delta_1=-1+2\sqrt{2}$, $\Delta_2=-1-2\sqrt{2}$. Noting that $\Delta_1\cdot\Delta_2=-7$, there are two cases to consider:

Case 1: assume $\Delta_1\cdot\Delta_2=0$. This occurs if and only if $p=7$. In this case, $3^2=2$ hence we may take $\sqrt{2}=3$, then we have $(\Delta_1,\Delta_2)=(5,0)$. For $\Delta_2=0$, the corresponding equation (13) is always solvable with a unique solution. As for $\Delta_1=5$, note that 5 is a nonsquare in $\mathbb{F}_7$. Therefore, if n is odd, then $\eta(5)=-1$ and the equation (13) corresponding to Δ_1 is not solvable in $\mathbb{F}_{p^n}$, that is, $T_1=1$. On the other hand, if n is even, then $\eta(5)=1$ and the equation (13) corresponding to Δ_1 has two distinct solutions in $\mathbb{F}_{p^n}$, so in this case we have $T_1=3$.

Case 2: assume $\Delta_1\cdot\Delta_2\neq 0$. Then $p\neq 7$. If $\eta(\Delta_1)=\eta(\Delta_2)=1$, then the equations (13) corresponding to both Δ_1 and Δ_2 are solvable with two distinct solutions, so $T_1=4$. If $\eta(\Delta_1)=\eta(\Delta_2)=-1$, then the equation (13) is not solvable for either Δ_1 or Δ_2, hence $T_1=0$. On the other hand, if $\eta(\Delta_1)\cdot\eta(\Delta_2)=\eta(-7)=-1$, then the corresponding equation (13) is solvable with two distinct solutions in $\mathbb{F}_{p^n}$ for exactly one of Δ_1 and Δ_2, that is, $T_1=2$.

Summarizing all the above cases we obtain the desired formula for T_1. This completes the proof of Lemma 4. □

Remark 4. *For any given odd prime p and positive integer n, in order to get the exact value of* T_1*, one first needs to compute* $\eta(2)$ *and* $\eta(-7)$ *in* $\mathbb{F}_{p^n}$*, which is straightforward according to the Legendre symbols* $\left(\frac{2}{p}\right)$, $\left(\frac{-7}{p}\right)$ *and the parity of n. If* $\eta(2)=\eta(-7)=1$*, then one further needs to check the value of* $\eta(-1+2\sqrt{2})$*. This can be handled efficiently by the following way:*

- *when* $\left(\frac{2}{p}\right)=1$*, then* $-1+2\sqrt{2}$ *is an element in* $\mathbb{F}_p$*, and it is always a square in* $\mathbb{F}_{p^2}$*. Thus, the element* $-1+2\sqrt{2}$ *is a square of* $\mathbb{F}_{p^n}$ *iff* $-1+2\sqrt{2}$ *is a square of* $\mathbb{F}_p$ *or n is even;*
- *when* $\left(\frac{2}{p}\right)=-1$*, then* $-1+2\sqrt{2}$ *is an element in* $\mathbb{F}_{p^2}\setminus\mathbb{F}_p$*, and since* $\eta(2)=1$*, n must be even. Thus,* $\eta(-1+2\sqrt{2})=1$ *iff* $-1+2\sqrt{2}$ *is a square in* $\mathbb{F}_{p^2}$*, or n is a multiple of* 4*.*

An alternative approach to computing $\eta(-1+2\sqrt{2})$ *is based on investigating the polynomial* $(x^2+1)^2-8$*, that is,* x^4+2x^2-7*. We have* $\eta(-1+2\sqrt{2})=1$ *if and only if* x^4+2x^2-7 *has a root in* $\mathbb{F}_{p^n}$*. In order to determine whether the polynomial* $x^4+2x^2-7\in\mathbb{F}_p[x]$ *has a root in* $\mathbb{F}_{p^n}$*, it suffices to verify whether it has roots in* $\mathbb{F}_p$ *and* $\mathbb{F}_{p^2}$*. Then, combined with the parity of n or n/2, we can obtain the desired result. The details are omitted here.*

Lemma 5. *With the notation introduced above, for any* $1\leq i\leq 4$*, we have* $|\mathcal{M}_i|=p^n+(1+T_1)(p^n-1)$*, where* T_1 *is given in Lemma 4.*

Proof. It is easy to see that $|\mathcal{M}_i|=|\mathcal{M}_4|$ for any $1\leq i\leq 4$. So we only consider $\mathcal{M}_4$, that is, $x_4=0$ in (9). If $x_3=0$, then $x_1=x_2$ and (9) has p^n solutions. Now suppose $x_3\neq 0$, let $y_1=\frac{x_1}{x_3}$ and $y_2=\frac{x_2}{x_3}$, then y_1 and y_2 satisfy

$$\begin{cases} y_1-y_2+1 &= 0,\\ y_1^{p^n-3}-y_2^{p^n-3}+1 &= 0. \end{cases} \tag{14}$$

Denote by L_0 the number of solutions $(y_1,y_2)\in(\mathbb{F}_{p^n})^2$ of (14). Thus we have $|\mathcal{M}_4|=p^n+(p^n-1)L_0$.

Note that (14) is equivalent to

$$(y_1+1)^{p^n-3}-y_1^{p^n-3}=1. \tag{15}$$

It is obvious that $y_1=0$ is a solution of (15). If $y_1\neq 0$, then (15) is equivalent to $g_1(x)=0$, which has been investigated in Lemma 4. Thus, $L_0=1+T_1$ and $|\mathcal{M}_4|=p^n+(1+T_1)(p^n-1)$. This proves Lemma 5. □

Lemma 6. *With the notation introduced above, we have*

$$\begin{aligned} \left|\mathcal{M}^{\circ}\right| = (p^n-1)(3p^n-8-2\eta(-1) \\ -\eta(-3)\,(2+\eta(-3))+\lambda_{2,p^n}), \end{aligned} \tag{16}$$

where λ_{2,p^n} is defined as in (2).

Proof. Since $x_4 \neq 0$, putting $y_i = \frac{x_i}{x_4}$ for $i = 1,2$ and 3, we have

$$\begin{cases} y_1 - y_2 + y_3 - 1 & = & 0, \\ y_1^{p^n-3} - y_2^{p^n-3} + y_3^{p^n-3} - 1 & = & 0. \end{cases} \tag{17}$$

Denote by M_0 the number of solutions $(y_1, y_2, y_3) \in \left(\mathbb{F}_{p^n}^*\right)^3$ of the equation system (17). Then we have

$$\left|\mathcal{M}^{\circ}\right| = M_0(p^n-1). \tag{18}$$

Now we compute M_0.

Since $y_i \neq 0$ for all $i \in \{1,2,3\}$, using $y_1y_3 = z$, then (17) becomes

$$\begin{cases} y_1 + y_3 & = & 1 + y_2, \\ y_1 y_3 & = & z, \quad z \in \mathbb{F}_{p^n}^*, \\ y_1^{-2} + y_3^{-2} & = & 1 + y_2^{-2}. \end{cases} \tag{19}$$

From the second and the third equations in (19) we get

$$y_2^{-2} + 1 = \frac{y_1^2 + y_3^2}{y_1^2 y_3^2} = \frac{(y_2+1)^2 - 2z}{z^2},$$

which is equivalent to

$$(y_2^{-2}+1)z^2 + 2z - (y_2+1)^2 = 0.$$

Then, we can conclude that M_0 is equal to the number of solutions $(y, y_2, z) \in \left(\mathbb{F}_{p^n}^*\right)^3$ of the equation system

$$\begin{cases} y^2 - (1+y_2)y + z & = & 0, \\ (y_2^{-2}+1)z^2 + 2z - (y_2+1)^2 & = & 0. \end{cases} \tag{20}$$

For determining M_0, now our strategy is to count the number of pairs $(y,z) \in \left(\mathbb{F}_{p^n}^*\right)^2$ satisfying (20) for each fixed $y_2 \in \mathbb{F}_{p^n}^*$. We distinguish two cases as follows.

Case 1: $y_2^{-2} + 1 = 0$. This case occurs only when $\eta(-1) = 1$. Then $y_2 = \pm\sqrt{-1}$ and it follows that $z = y_2$ from the second equation in (20). Then the first equation in (20) leads to $y = 1$ or $y = y_2$. Thus, for each such y_2 it contributes 2 solutions to M_0.

Case 2: $y_2^{-2} + 1 \neq 0$. Then, the second equation in (20) is a quadratic equation in variable z, and it has two solutions $z = y_2$ and $z = -\frac{y_2(y_2+1)^2}{y_2^2+1}$. There are two subcases that need to be considered.

Subcase 2.1: $z = y_2$. Then the first equation in (20) still has two solutions $y = 1$ or $y = y_2$ if $y_2 \neq 1$; however, it leads to one solution if $y_2 = 1$.

Subcase 2.2: $z = -\frac{y_2(y_2+1)^2}{y_2^2+1}$. Then the first equation of (20) becomes

$$y^2 - (y_2+1)y - \frac{y_2(y_2+1)^2}{y_2^2+1} = 0. \tag{21}$$

This is a quadratic equation in variable y with discriminant given by $\Delta = \frac{(y_2+1)^2(y_2^2+4y_2+1)}{y_2^2+1}$. Note that $y_2 = -1$ will leads to a zero solution $y = 0$ of (21) and $z = 0$, which should be discarded since $y,\, z \in \mathbb{F}_{p^n}^*$.

Therefore, $y_2 \neq -1$. When $y_2 \in \mathbb{F}_{p^n} \setminus \{0,-1\}$, (21) has two solutions in $\mathbb{F}_{p^n}^*$ if $\eta(\Delta)=1$, a unique solution in $\mathbb{F}_{p^n}^*$ if $\eta(\Delta)=0$, and no solution if $\eta(\Delta)=-1$. So this subcase contributes $\left(1+\eta\left(\frac{y_2^2+4y_2+1}{y_2^2+1}\right)\right)$ solutions for $y_2 \in \mathbb{F}_{p^n} \setminus \{0,-1\}$.

Note that when $y_2 = -\frac{y_2(y_2+1)^2}{y_2^2+1}$, the solutions in Subcases 2.1 and 2.2 will overlap, and they need to be excluded in the counting. Since $y_2 \neq 0$, $y_2 = -\frac{y_2(y_2+1)^2}{y_2^2+1}$ is equivalent to that $y_2^2+y_2+1=0$. This holds if and only if when $\eta(-3)=1$ or $\eta(-3)=0$, and for such y_2 the above two subcases are the same. More precisely, when $\eta(-3)=1$, we can solve $y_2 = \frac{-1\pm\sqrt{-3}}{2} \in \mathbb{F}_{p^n}^*$ and each y_2 contributes 2 solutions to M_0; if $\eta(-3)=0$, i.e., $p=3$, then $y_2=1$ and it contributes only one solution to M_0; if $\eta(-3)=-1$, then no such y_2 exists in $\mathbb{F}_{p^n}$. Therefore, there are $\sum_{y_2^2+y_2+1=0}(1+\eta(-3))$ solutions that have been counted twice in Subcases 2.1 and 2.2.

Summarizing the above discussions, we can write the total number of solutions M_0 of the equation system (20) as

$$\begin{aligned}
&\sum_{y_2^{-2}+1=0} 2 + \sum_{\substack{y_2^{-2}+1\neq 0\\ y_2\neq 1,0}} 2 + \sum_{\substack{y_2^{-2}+1\neq 0\\ y_2=1}} 1\\
&+ \sum_{\substack{y_2^{-2}+1\neq 0\\ y_2\neq 0,-1}} \left(1+\eta\left(\frac{y_2^2+4y_2+1}{y_2^2+1}\right)\right)\\
&- \sum_{y_2^2+y_2+1=0} (1+\eta(-3)).
\end{aligned}$$

Noting that

$$\sum_{y_2^{-2}+1=0} 2 = 2(1+\eta(-1)),$$

$$\sum_{y_2^2+y_2+1=0} (1+\eta(-3)) = (1+\eta(-3))^2,$$

and

$$\sum_{y_2^{-2}+1=0} \eta\left(\frac{y_2^2+4y_2+1}{y_2^2+1}\right) = 0,$$

we can obtain

$$\begin{aligned}
M_0 = {} & 3p^n - 8 - 2\eta(-1) - \eta(-3)(2+\eta(-3))\\
& + \sum_{y_2 \in \mathbb{F}_{p^n}} \eta\left(\frac{y_2^2+4y_2+1}{y_2^2+1}\right).
\end{aligned} \tag{22}$$

Then the desired value of $|\mathcal{M}^\circ|$ follows immediately from the fact that $\lambda_{2,p^n} = \sum_{y_2\in\mathbb{F}_{p^n}} \eta\left(\frac{y_2^2+4y_2+1}{y_2^2+1}\right)$ and the relation (18). □

With the above preparations, we can now obtain the value of M easily.

Theorem 7. *Let $p \geq 3$ be an odd prime, T_1 be given in Lemma 4, and λ_{2,p^n} be defined as in (2). Then the number of solutions to the equation system (9), denoted by M, is given by*

$$\begin{aligned}
M = 1 + (p^n-1)(&3p^n + \lambda_{2,p^n} + 4T_1 - 4\\
&-2\eta(-1) - \eta(-3)(2+\eta(-3))).
\end{aligned}$$

Proof. By the inclusion-exclusion principle we have

$$\begin{aligned} M = |\mathcal{M}^{\circ}| + \sum_{i=1}^{4} \left|\mathcal{M}_i\right| - \sum_{1\le i<j\le 4} \left|\mathcal{M}_i \cap \mathcal{M}_j\right| \\ + \sum_{1\le i<j<k\le 4} \left|\mathcal{M}_i \cap \mathcal{M}_j \cap \mathcal{M}_k\right| - \left|\cap_{i=1}^{4} \mathcal{M}_i\right|. \end{aligned}$$

Then using Lemmas 5 and 6 and noting (10) and (11), we obtain the desired result. □

IV. The differential spectrum of x^{p^n-3}

For the power function $F(x) = x^{p^n-3}$ with p being an odd prime in Theorem 1, it is already known that the differential uniformity $\delta(F)$ of $F(x)$ satisfies $1 \le \delta(F) \le 5$ [13]. Recalling Definition 1, we can assume the differential spectrum of $F(x) = x^{p^n-3}$ as

$$\mathbb{S} = [\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5].$$

For $p = 3$, the differential spectrum $\mathbb{S}$ has been completely determined in [22]. However, the method used in [22] heavily depends on the characteristic $p = 3$ and doesn't seem to work for the general case $p \ge 5$. In this section, for any odd prime $p \ge 3$, we will compute $\mathbb{S}$ by a unified approach.

A. Some basic properties about the differential spectrum

Before beginning our computations, we mention some basic properties about the differential spectrum of a power mapping x^d over finite fields. Let x^d be a power mapping over $\mathbb{F}_{p^n}$ with differential uniformity δ, then using the notation in Definition 1 we have

$$\sum_{i=0}^{\delta} \omega_i = \sum_{i=0}^{\delta} i\omega_i = p^n. \tag{23}$$

The identities in (23) are well-known [2], [25], [22], and are useful in computing the differential spectrum. Moreover, the following identity also plays an important role in the computation, which was established in [13].

Lemma 8. *[13, Theorem 10] With the notation introduced in Definition 1, let M denote the number of solutions $(x_1,x_2,x_3,x_4) \in (\mathbb{F}_{p^n})^4$ of the equation system*

$$\begin{cases} x_1 - x_2 + x_3 - x_4 &= 0, \\ x_1^d - x_2^d + x_3^d - x_4^d &= 0. \end{cases} \tag{24}$$

Then, we have

$$\sum_{i=0}^{\delta} i^2 \omega_i = \frac{M - p^{2n}}{p^n - 1}. \tag{25}$$

With the equalities in (23) and (25), our strategy for computing the differential spectrum $\mathbb{S}$ of x^{p^n-3} can be sketched as follows: first we will compute ω_5, ω_3 and ω_2; then we establish a system of linear equations in three variables ω_0, ω_1 and ω_4 by (23) and (25), which enables us to express ω_0, ω_1 and ω_4 in terms of the known ω_5, ω_3 and ω_2. Next we begin with the general setup for investigating the differential spectrum.

B. The general setup

For any $b \in \mathbb{F}_{p^n}$, the derivative equation $\mathbb{D}_1 F(x) = b$ is

$$(x+1)^{p^n-3} - x^{p^n-3} = b. \tag{26}$$

Let $N(b)$ denote the number of its solutions in $\mathbb{F}_{p^n}$. The elements ω_i's for $i \in \{0, 1, \cdots, 5\}$ in the differential spectrum $\mathbb{S}$ are actually the number of $b \in \mathbb{F}_{p^n}$ such that $N(b) = i$.

It can be easily observed that the derivative equation (26) has a solution x if and only if the derivative equation $(x+1)^{p^n-3} - x^{p^n-3} = -b$ has a solution $-x-1$. Thus, $N(b) = N(-b)$ for any b. When $b = 0$, it is easy to verify that $x = -\frac{1}{2}$ is the unique solution of (26). That is ta say, $N(0) = 1$. Moreover, note that in (26) if b is equal to 1 (resp. -1), then $x = 0$ (resp. $x = -1$) is a solution to the corresponding equation (26). Since $N(0)$ is already determined, in the following we only need to consider $N(b)$ for $b \neq 0$.

For $b \in \mathbb{F}_{p^n}^*$, define

$$g_b(x) = x^4 + 2x^3 + x^2 + 2b^{-1}x + b^{-1}, \tag{27}$$

and denote the number of its roots in $\mathbb{F}_{p^n}$ by T_b. Note that for $b = 1$, T_b has already been determined in Lemma 4. This polynomial is closely connected with the derivative equation (26). As a matter of fact, when $x \neq 0, -1$, (26) can be written as $(x+1)^{-2} - x^{-2} = b$, which is equivalent to

$$g_b(x) = x^4 + 2x^3 + x^2 + 2b^{-1}x + b^{-1} = 0.$$

Hence we can arrive at the following result:

$$N(b) = \begin{cases} T_b, & \text{if } b \in \mathbb{F}_{p^n}^* \setminus \{\pm 1\}, \\ T_b + 1, & \text{if } b = \pm 1. \end{cases} \tag{28}$$

Moreover, since $N(b) = N(-b)$ for any b, it follows that

$$T_b = T_{-b} \text{ for any } b \in \mathbb{F}_{p^n}^*. \tag{29}$$

C. The values of ω_5

Note that (27) has at most four roots in $\mathbb{F}_{p^n}$. By (28), it is easy to see that $\delta(F) = 5$ if and only if $N(1) = N(-1) = 5$. Then, we have $\omega_5 \in \{0, 2\}$, and $\omega_5 = 2$ if and only if $T_1 = 4$. The condition for $T_1 = 4$ has already been shown in Lemma 4. Thus, we can determine ω_5 in the differential spectrum $\mathbb{S}$ as follows.

Theorem 9. *With the notation introduced above, we have*

$$\omega_5 = \begin{cases} 2, \text{ if } \eta(2) = \eta(-7) = \eta(-1 + 2\sqrt{2}) = 1, \\ 0, \text{ otherwise.} \end{cases}$$

D. The values of ω_3

Next we investigate the value of ω_3. When $N(b) = 3$, we distinguish the following two cases.

Case 1: $b = \pm 1$. $N(1) = N(-1) = 3$ if and only if $T_1 = 2$. By Lemma 4, this occurs only when $\eta(2) = 1$ and $\eta(-7) = -1$.

Case 2: $b \neq \pm 1$. By (28), $N(b) = 3$ if and only if $T_b = 3$. Thus, we need to characterize when $T_b = 3$ for $b \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\}$. Such results are given below.

Lemma 10. *Let $b \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\}$, and $g_b(x)$ be the polynomial defined as in (27). Then $g_b(x) = 0$ has a multiple root $x_0 \in \mathbb{F}_{p^n}$ if and only if $p \neq 7$ and $\eta(-3) = 1$. In this case, the multiple roots x_0's are $-\frac{1}{2} \pm \frac{1}{6}\sqrt{-3}$, and the corresponding b's are $\mp 3\sqrt{-3}$.*

Proof. If x_0 is a multiple root of $g_b(x) = 0$, then $g_b'(x_0) = 2(2x_0^3 + 3x_0^2 + x_0 + b^{-1}) = 0$, and we have $x_0 \neq 0, -1$. Hence $b^{-1} = -(2x_0^3 + 3x_0^2 + x_0)$. Substituting it into the original equation, we get

$$x_0(x_0+1)(3x_0^2+3x_0+1) = 0.$$

This together with $x_0 \neq 0, -1$ leads to $3x_0^2 + 3x_0 + 1 = 0$. Such x_0 exists if and only if $\eta(-3) = 1$. Then we have $x_0 = -\frac{1}{2} \pm \frac{1}{6}\sqrt{-3}$ and the corresponding b's are $\mp 3\sqrt{-3}$.

Moreover, if $p = 7$, then we may take $\sqrt{-3} = 2$ since $2^2 = -3$, and thus $b = \mp 3\sqrt{-3} = \pm 1$, a contradiction. Therefore, we need the condition $p \neq 7$ holds. □

Lemma 11. *Let $b \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\}$. Then $T_b = 3$ if and only if $p \neq 7$, $\eta(-3) = \eta(-2) = 1$ and $b = \pm 3\sqrt{-3}$.*

Proof. If $T_b = 3$, then $g_b(x) = 0$ must have a multiple root x_0 in $\mathbb{F}_{p^n}$. By Lemma 10, we have $p \neq 7$, $\eta(-3) = 1$ and $(x_0, b) = (-\frac{1}{2} + \frac{1}{6}\sqrt{-3}, -3\sqrt{-3})$ or $(x_0, b) = (-\frac{1}{2} - \frac{1}{6}\sqrt{-3}, 3\sqrt{-3})$. For the former case, the equation $g_b(x) = 0$ can be written as

$$\begin{aligned}(x-x_0)^2(x^2 + (1 + \frac{1}{3}\sqrt{-3})x& \\ +(-\frac{1}{2} + \frac{1}{6}\sqrt{-3})) &= 0,\end{aligned} \tag{30}$$

which has three solutions in $\mathbb{F}_{p^n}$ if and only if $\eta((1+\frac{1}{3}\sqrt{-3})^2 - 4(-\frac{1}{2} + \frac{1}{6}\sqrt{-3})) = \eta(\frac{8}{3}) = 1$, that is, $\eta(6) = 1$. Since $\eta(-3) = 1$, this is equivalent to that $\eta(-2) = 1$. It can be checked that in this case the other two solutions of (30) are $-\frac{1}{2} - \frac{1}{6}\sqrt{-3} \pm \frac{1}{3}\sqrt{6}$, which are different from x_0. For the latter case $(x_0, b) = (-\frac{1}{2} - \frac{1}{6}\sqrt{-3}, 3\sqrt{-3})$, the arguments are almost the same. So we omit the details. □

Based on the above results, we can now obtain the value of ω_3 below.

Theorem 12. *Let* C_1 *denote the condition that* $\eta(2) = -\eta(-7) = 1$ *and* C_2 *denote the condition that* $\eta(-3) = \eta(6) = 1$ *and* $p \neq 7$*. Then, we have*

$$\omega_3 = \begin{cases} 4, & \text{both } \mathrm{C}_1 \text{ and } \mathrm{C}_2 \text{ hold}, \\ 2, & \text{only one of } \mathrm{C}_1 \text{ and } \mathrm{C}_2 \text{ holds}, \\ 0, & \text{otherwise}. \end{cases} \tag{31}$$

Alternatively, the value ω_3 *may be expressed as*

$$\begin{aligned}\omega_3 = \frac{\eta(7)^2\eta(3)^2}{2}\Big(&\big(1+\eta(2)\big)\cdot\big(1-\eta(-7)\big) \\ &+\big(1+\eta(-2)\big)\cdot\big(1+\eta(-3)\big)\Big).\end{aligned} \tag{32}$$

Proof. In order to find the value of ω_3, we need to find the frequency of $b \in \mathbb{F}_{p^n}$ such that $N(b) = 3$. There are two cases to consider.

Case 1: $b = \pm 1$. $N(1) = N(-1) = 3$ if and only if $T_1 = 2$. By Lemma 4, this occurs if and only if $\eta(2) = 1$ and $\eta(-7) = -1$, which is Condition C_1.

Case 2: $b \neq \pm 1$. By Lemma 11, $N(b) = T_b = 3$ if and only if $p \neq 7$, $\eta(-3) = \eta(-2) = 1$ and the corresponding b's are $\pm 3\sqrt{-3}$. Here we get Condition C_2.

Combining these two cases yield the expression of ω_3 in (31). As for the expression of ω_3 in (32), denote

$$f_1 := \eta(7)^2\eta(3)^2 \cdot \big(1+\eta(2)\big)\cdot\big(1-\eta(-7)\big),$$

$$f_2 := \eta(7)^2\eta(3)^2 \cdot \big(1+\eta(-2)\big)\cdot\big(1+\eta(-3)\big).$$

Then (32) follows easily from the observation that

$$f_1 = \begin{cases} 4, & \text{if } \mathrm{C}_1 \text{ holds}, \\ 0, & \text{if } \mathrm{C}_1 \text{ does not hold}, \end{cases}$$

$$f_2 = \begin{cases} 4, & \text{if } \mathrm{C}_2 \text{ holds}, \\ 0, & \text{if } \mathrm{C}_2 \text{ does not hold}, \end{cases}$$

This finishes the proof of Theorem 12. □

E. The value of ω_2

This subsection is devoted to the computation of ω_2. Recall the basic facts in (28) and (29). First, we prove the following useful result.

Lemma 13. *Let* $p \geq 3$ *and let* T_b *be the number of roots of the polynomial* $g_b(x) \in \mathbb{F}_{p^n}[x]$ *defined as in (27). Define two sets*

$$\begin{aligned} \mathcal{A} \;\; = \;\; & \{a \in \mathbb{F}_{p^n} \mid \eta(a^2-4) = 1 \;\text{ and} \\ & \qquad\qquad \eta(-3a^2-4) = -1\}, \end{aligned} \tag{33}$$

and

$$\mathcal{B} = \{b \in \mathbb{F}_{p^n}^* \mid T_b = 2\}. \tag{34}$$

Then, there is a one-to-one correspondence between the elements $b \in \mathcal{B}$ *and the elements* $a \in \mathcal{A}$*. Moreover, if* $\eta(2) = 1$ *and* $\eta(-7) = -1$*, then* $\pm 1 \in \mathcal{B}$ *and the corresponding a's belong to* $\{\pm 2\sqrt{2}\}$*.*

Proof. For $b \in \mathcal{B}$, the proofs of Lemmas 10 and 11 imply that $g_b(x) = 0$ can not have multiple roots, so it has exactly two distinct simple roots in $\mathbb{F}_{p^n}$. Putting $y = 2x+1$ in (27), $g_b(x) = 0$ becomes

$$y^4 - 2y^2 + 16b^{-1}y + 1 = 0, \tag{35}$$

which also has exactly two distinct simple roots in $\mathbb{F}_{p^n}$ for each $b \in \mathcal{B}$. Thus, we can factor (35) into the form

$$(y^2 + ay + c)(y^2 - ay + c^{-1}) = 0, \tag{36}$$

where the pair (a, c) satisfies the following conditions

1) $a \in \mathbb{F}_{p^n}^*$, $c \in \mathbb{F}_{p^n}^*$;
2) $y^2 + ay + c$ is irreducible over $\mathbb{F}_{p^n}$, that is, $\eta(a^2 - 4c) = -1$;
3) $y^2 - ay + c^{-1}$ has two distinct roots in $\mathbb{F}_{p^n}$, that is, $\eta(a^2 - 4c^{-1}) = 1$;
4)

$$\begin{cases} c + c^{-1} & = a^2 - 2, \\ a(c - c^{-1}) & = -16b^{-1}, \end{cases} \tag{37}$$

which is obtained by comparing (35) with (36). This gives the correspondence from $b \in \mathcal{B}$ to the pairs (a, c) satisfying the above conditions. Once $b \in \mathcal{B}$ is given, the two solutions of (35) are uniquely determined and so are the pair (a, c) and the element a. This shows that for each $b \in \mathcal{B}$, there exists a unique a satisfying the conditions in $1) - 4)$. Now we verify that this $a \in \mathcal{A}$. For this a, (37) implies that $c + c^{-1} = a^2 - 2$ has two distinct roots $c \neq c^{-1} \in \mathbb{F}_{p^n}$, so we have $\eta((a^2-2)^2 - 4) = \eta(a^2(a^2-4)) = 1$, that is, $\eta(a^2 - 4) = 1$ and $a \in \mathbb{F}_{p^n}^*$. On the other hand, from

$$\begin{aligned} -1 \;\; &= \;\; \eta((a^2-4c)(a^2-4c^{-1})) \\ &= \;\; \eta(a^4 - 4a^2(c + c^{-1}) + 16) \\ &= \;\; \eta((a^2-4)(-3a^2-4)), \end{aligned} \tag{38}$$

we derive that $\eta(-3a^2-4)=-1$. This shows that a indeed belongs to $\mathcal{A}$.

Now suppose that $a\in\mathcal{A}$. We show that c and b are all uniquely determined by this a according to (36), and $b\in\mathcal{B}$.

First, since $\eta(a^2-4)=1$, the first equation of (37) has two distinct solutions $c_1,c_2\in\mathbb{F}_{p^n}$, and we have $\eta((a^2-4c_1)(a^2-4c_2))=-1$ due to (38). We may assume $\eta(a^2-4c_1)=-1$. Then we take $c=c_1$. This is the desired c in (36) such that y^2+ay+c is irreducible over $\mathbb{F}_{p^n}$ and y^2-ay+c^{-1} is reducible with two distinct roots in $\mathbb{F}_{p^n}$. Choosing b according to the second equation of (37), we can obtain $y^4-2y^2+16b^{-1}y+1=(y^2+ay+c)(y^2-ay+c^{-1})=0$, which has exactly two roots in $\mathbb{F}_{p^n}$. This shows that $b\in\mathbb{F}_{p^n}^*$ is uniquely determined by a and it satisfies $T_b=2$. This finishes the proof of the first part of Lemma 13.

As for the second part, when $\eta(2)=1$ and $\eta(-7)=-1$, by Lemma 4 and (29), we have $T_1=T_{-1}=2$ and thus $\pm1\in\mathcal{B}$. Then from (37) we obtain

$$16^2=(-16b^{-1})^2=a^2(c-c^{-1})^2=a^2((a^2-2)^2-4),$$

that is,

$$(a^2-8)(a^4+4a^2+32)=0,$$

which implies that $a^4+4a^2+32=0$ or $a^2=8$. If $a^4+4a^2+32=0$, then we have $\eta(4^2-4\cdot32)=\eta(-7)=1$, a contradiction. Hence we have $a^2=8$ and it can be easily verified that the corresponding two a's indeed belong to $\mathcal{A}$. This proves the second part of Lemma 13. □

Now we can obtain the value of ω_2 in the following theorem.

Theorem 14. *For $p\geq 3$, we have*

$$\omega_2=\begin{cases}0, & \text{if } p=3 \text{ and } n \text{ is even},\\ \frac{3^n-3}{2}, & \text{if } p=3 \text{ and } n \text{ is odd},\\ A+2, & \text{if } p=7 \text{ and } n \text{ is odd},\\ A-2, & \text{if } \eta(2)=1 \text{ and } \eta(-7)=-1,\\ A, & \text{otherwise}.\end{cases}$$

where $A=\frac{1}{4}\big(p^n-5-\lambda_{1,p^n}-\eta(-3)+2\eta(-1)\big)$ with λ_{1,p^n} being defined as in (1).

Proof. If $N(1)=N(-1)=2$, then $T_1=T_{-1}=1$. By Lemma 4, this occurs only when $p=7$ and n is odd. Now we need to consider the number of $b\in\mathbb{F}_{p^n}\setminus\{0,\pm1\}$ such that $T_b=2$, by Lemma 13 which is related to the cardinality of the set $\mathcal{A}$ defined in (33) or $\mathcal{B}$ in (34). We distinguish the following two cases.

Case 1: $p=3$. Then, we have $T_{\pm1}\neq1$, $\pm1\notin\mathcal{B}$ and the set $\mathcal{A}$ defined in (33) becomes

$$\mathcal{A}=\{a\in\mathbb{F}_{3^n}\mid\eta(a^2-1)=1\text{ and }\eta(-1)=-1\}.$$

Therefore, in this case we have

$$\omega_2=|\mathcal{B}|=|\mathcal{A}|.$$

If n is even, then $\eta(-1)=1$ and thus $|\mathcal{A}|=0$. Otherwise, we have

$$\mathcal{A}=\{a\in\mathbb{F}_{3^n}^*\mid\eta(a^2-1)=1\},$$

and by the cyclotomic numbers used in [22], we have

$$|\mathcal{A}|=\frac{3^n-3}{2}.$$

Thus, in this case, we have

$$\omega_2=\begin{cases}0, & \text{if } n \text{ is even},\\ \frac{3^n-3}{2}, & \text{if } n \text{ is odd}.\end{cases}$$

Case 2: $p \geq 5$. Then, by Lemma 13 we find that

$$\left|\{b \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\} \mid T_b = 2\}\right| =$$
$$\begin{cases} |\mathcal{A}| - 2, & \text{if } \eta(2) = 1 \text{ and } \eta(-7) = -1, \\ |\mathcal{A}|, & \text{otherwise.} \end{cases}$$

This shows that when $p \geq 5$

$$\omega_2 = \begin{cases} |\mathcal{A}| - 2, & \text{if } \eta(2) = 1 \text{ and} \\ & \quad \eta(-7) = -1, \\ |\mathcal{A}| + 2, & \text{if } p = 7 \text{ and } n \text{ is odd}, \\ |\mathcal{A}|, & \text{otherwise.} \end{cases} \tag{39}$$

Now it suffices to determine the cardinality of $\mathcal{A}$. Actually, since $p \geq 5$,

$$\begin{aligned} & |\mathcal{A}| \\ = \ & \frac{1}{4} \sum_{a^2 \neq 4, -\frac{4}{3}} \left(1 + \eta(a^2 - 4)\right)\left(1 - \eta(-3a^2 - 4)\right) \\ = \ & \frac{1}{4} \sum_{a \in \mathbb{F}_{p^n}} \left(1 + \eta(a^2 - 4)\right)\left(1 - \eta(-3a^2 - 4)\right) \\ & -1 + \frac{1}{2}\eta(-1) - \frac{1}{2}\eta(-3) \\ = \ & \frac{1}{4}\Big[\sum_{a \in \mathbb{F}_{p^n}} \eta(a^2 - 4) - \sum_{a \in \mathbb{F}_{p^n}} \eta(-3a^2 - 4) \\ & - \sum_{a \in \mathbb{F}_{p^n}} \eta((a^2 - 4)(-3a^2 - 4)) + \sum_{a \in \mathbb{F}_{p^n}} 1\Big] \\ & -1 + \frac{1}{2}\eta(-1) - \frac{1}{2}\eta(-3). \end{aligned}$$

By using the facts that $\sum\limits_{a \in \mathbb{F}_{p^n}} \eta(a^2 - 4) = -1$ and $\sum\limits_{a \in \mathbb{F}_{p^n}} \eta(-3a^2 - 4) = -\eta(-3)$, and noting that $\sum_{a \in \mathbb{F}_{p^n}} \eta\left((a^2 - 4)(-3a\right.$ is exactly the character sum λ_{1,p^n} evaluated in Theorem 3, we obtain $|\mathcal{A}| = A$. Then the desired result follows from (39). This completes the proof of Theorem 14. □

Based on the previous results and the identities in (23) and (25), we can obtain the following main result about the differential spectrum of x^{p^n-3}.

Theorem 15. *Let $\mathbb{S} = [\omega_0, \omega_1, \ldots, \omega_5]$ be the differential spectrum of $F(x) = x^{p^n-3}$. Then we have*

$$\begin{cases} \omega_0 & = \frac{M - 2p^{2n} + p^n}{4(p^n - 1)} + \frac{1}{2}\omega_2 + \frac{1}{2}\omega_3 - \omega_5, \\ \omega_1 & = \frac{-M + 5p^{2n} - 4p^n}{3(p^n - 1)} - \frac{4}{3}\omega_2 - \omega_3 + \frac{5}{3}\omega_5, \\ \omega_4 & = \frac{M - 2p^{2n} + p^n}{12(p^n - 1)} - \frac{1}{6}\omega_2 - \frac{1}{2}\omega_3 - \frac{5}{3}\omega_5, \end{cases} \tag{40}$$

where ω_5, ω_3 and ω_2 are given in Theorems 9, 12 and 14, respectively, and M is given in Theorem 7.

Remark 5. *Applying Theorem 15, the differential spectrum $\mathbb{S}$ of x^{p^n-3} for any odd prime $p \geq 3$ can be completely determined. To be more concrete, for each given prime $p \geq 3$, one first compute the exact values of ω_5, ω_3, ω_2 and M:*

- *the values of ω_5 and ω_3 can be derived from Theorems 9 and 14 respectively after calculating the quadratic character of some specified elements;*
- *the value of ω_2 is given in Theorem 14. For $p = 3$, it is already given explicitly. For any $p \geq 5$, ω_2 is expressed in terms of the quadratic character sum λ_{1,p^n}, which has been evaluated in Theorem 3.*
- *the value of M shown in Theorem 7 is related to the quadratic character sum λ_{2,p^n}. For any prime $p \geq 3$, one can explicitly express the parameter M in terms of n by utilizing (3), Theorem 3, Lemma 4 and Theorem 7.*

Then, the differential spectrum $\mathbb{S}$ can be computed via (40), and one can express it explicitly in terms of n.

We provide the following results to illustrate Theorem 15. The first one is about the case $p = 3$, which has been investigated in [22] with a different method.

Corollary 16. *Let $p = 3$ and let $\mathbb{S} = [\omega_0, \omega_1, \ldots, \omega_5]$ be the differential spectrum of the power mapping x^{p^n-3} over $\mathbb{F}_{3^n}$. Then, (i) when n is odd,*

$$\begin{aligned}\mathbb{S} = [\omega_0 = \frac{3^n-3}{2},\ \omega_1 = 3,\ \omega_2 = \frac{3^n-3}{2},\\ \omega_3 = 0, \qquad \omega_4 = 0,\ \omega_5 = 0];\end{aligned}$$

(ii) when $n \equiv 2 \pmod 4$,

$$\begin{aligned}\mathbb{S} = [\omega_0 = \frac{3^n-9}{4},\ \omega_1 = 2\cdot 3^{n-1}+3,\ \omega_2 = 0,\\ \omega_3 = 0, \qquad \omega_4 = \frac{3^{n-1}-3}{4}, \qquad \omega_5 = 0];\end{aligned}$$

(iii) when $n \equiv 0 \pmod 4$,

$$\begin{aligned}\mathbb{S} = [\omega_0 = \frac{3^n-1}{4},\ \omega_1 = 2\cdot 3^{n-1}+1, \omega_2 = 0,\\ \omega_3 = 0, \qquad \omega_4 = \frac{3^{n-1}-11}{4},\ \omega_5 = 2].\end{aligned}$$

Proof. For $p = 3$, by Theorem 9, we have $\omega_5 = 0$ if n is odd or $n \equiv 2 \pmod 4$, and $\omega_5 = 2$ if $n \equiv 0 \pmod 4$ since in this case $\left(x^2+1\right)^2 - 8 = x^4 + 2x^2 + 2$ is irreducible over $\mathbb{F}_3$. By (32) in Theorem 12, we have $\omega_3 = 0$. By Theorem 14, we have $\omega_2 = 0$ if n is even, and $\omega_2 = \frac{3^n-3}{2}$ if n is odd. By Theorem 7, we get $M = 1 + (3^n-1)(3^{n+1}-2)$ if n is odd, $M = 1 + (3^n-1)(3^{n+1}-8)$ if $n \equiv 2 \pmod 4$, and $M = 1 + (3^n-1)(3^{n+1}+8)$ if $n \equiv 0 \pmod 4$. Then, we should distinguish three cases and substituting the corresponding values into (40), the differential spectrum $\mathbb{S}$ is derived. □

Remark 6. *For the case $p = 3$, based on the characteristic property, the work of [22] calculated ω_4 directly instead of investigating the parameter M. However, their method in [22] doesn't seem to work for general case $p \geq 5$. The approach in the present paper works for all odd primes.*

Corollary 17. *Let $p = 5$ and $\Gamma_{5,n} = -\left(-1+2\sqrt{-1}\right)^n - \left(-1-2\sqrt{-1}\right)^n$ obtained from Example 1. Then, the differential spectrum $\mathbb{S}$ of x^{p^n-3} is shown as follows:*
(i) when n is odd, $\mathbb{S}$ is given by

$$\begin{aligned}[\omega_0 = \frac{3\cdot 5^n+\Gamma_{5,n}-17}{8}, \omega_1 = \frac{5^n+10}{3},\\ \omega_2 = \frac{5^n-\Gamma_{5,n}-3}{4}, \qquad \omega_3 = 0,\\ \omega_4 = \frac{5^n+3\cdot\Gamma_{5,n}-11}{24}, \quad \omega_5 = 0];\end{aligned}$$

(ii) when $n \equiv 2 \pmod 4$, $\mathbb{S}$ is given by

$$\begin{aligned}[\omega_0 = \frac{3\cdot 5^n+\Gamma_{5,n}-17}{8}, \omega_1 = \frac{5^n+8}{3},\\ \omega_2 = \frac{5^n-\Gamma_{5,n}-3}{4}, \qquad \omega_3 = 2,\\ \omega_4 = \frac{5^n+3\cdot\Gamma_{5,n}-43}{24}, \omega_5 = 0];\end{aligned}$$

*(*iii*) when* $n \equiv 0 \pmod 4$*,* $\mathbb{S}$ *is given by*

$$\begin{aligned}
[\omega_0 &= \frac{3\cdot 5^n + \Gamma_{5,n} - 1}{8}, \omega_1 = \frac{5^n+2}{3},\\
\omega_2 &= \frac{5^n - \Gamma_{5,n} - 3}{4}, \quad \omega_3 = 2,\\
\omega_4 &= \frac{5^n + 3\cdot\Gamma_{5,n} - 91}{24}, \omega_5 = 2].
\end{aligned}$$

Proof. If $p=5$, then $a=\Gamma_{5,1}=2$ and the explicit formula for $\Gamma_{5,n}$ follows from Theorem 3. Next we consider the following two cases:

Case 1: n is odd. Then, the element 2 is a nonsquare in $\mathbb{F}_{5^n}$ since it is a nonsquare in $\mathbb{F}_5$. Thus, we have $\omega_5 = 0$, $\omega_3 = 0$ and $\omega_2 = \frac{5^n - \Gamma_{5,n} - 3}{4}$ according to Theorems 9, 12 and 14, respectively. Furthermore, we have $T_1 = 0$ by Lemma 4 and $M = 5^n + (5^n-1)(3\cdot 5^n + \Gamma_{5,n} - 7)$ by Theorems 7 and 3. Substituting ω_5, ω_3, ω_2 and M into Theorem 15, we obtain the desired result.

Case 2: n is even. Then, the elements ± 2 are squares in $\mathbb{F}_{5^n}$. One needs to decide whether $-1\pm 2\sqrt{2}$ are squares in $\mathbb{F}_{5^n}$ or not. Note that $-1+2\sqrt{2}$ (resp. $-1-2\sqrt{2}$) is a square in $\mathbb{F}_{5^n}$ if and only if $(x^2+1)^2 = 8$ has a solution in $\mathbb{F}_{5^n}$, while the associated polynomial $(x^2+1)^2 - 8$ is an irreducible polynomial over $\mathbb{F}_5$. Thus, $-1+2\sqrt{2}$ (resp. $-1-2\sqrt{2}$) is a square in $\mathbb{F}_{5^n}$ if and only if $n \equiv 0 \pmod 4$. As we have done in Case 1, the desired results then follows from Theorem 15. □

Similarly, for $p=7$, the differential spectrum of the function x^{7^n-3} over $\mathbb{F}_{7^n}$ can be presented as follows.

Corollary 18. *The power mapping* x^{7^n-3} *over* $\mathbb{F}_{7^n}$ *is differentially* 4*-uniform and its differential spectrum* $\mathbb{S}$ *is given as follows:*
*(*i*)*

$$\begin{aligned}
\mathbb{S} = [\omega_0 &= \frac{3\cdot 7^n - 5}{8}, \omega_1 = \frac{7^n+2}{3}, \omega_2 = \frac{7^n+1}{4},\\
\omega_3 &= 0, \qquad \omega_4 = \frac{7^n-7}{24}]
\end{aligned}$$

if n is odd;
*(*ii*)*

$$\begin{aligned}
\mathbb{S} = [\omega_0 &= \frac{3\cdot 7^n - 2(-7)^{n/2} - 1}{8}, \omega_1 = \frac{7^n+2}{3},\\
\omega_2 &= \frac{7^n + 2(-7)^{n/2} - 3}{4}, \quad \omega_3 = 0,\\
\omega_4 &= \frac{7^n - 6(-7)^{n/2} + 5}{24}]
\end{aligned}$$

if n is even.

For other given primes p, one can also obtain similar results as Corollaries 16, 17 and 18 by Theorem 15. Next we provide some numerical experiments to verify our results in previous theorems.

Example 2. *Let* $p=5$*,* $n=4$*,* $d=p^n-3=622$ *and* η *be the quadratic character of* $\mathbb{F}_{5^4}$*. Then, one has* $\eta(2)=\eta(-1\pm 2\sqrt{2})=1$*, and* $\eta(-3)=\eta(6)=1$*. Thus, by Theorems 9 and 12, we have* $\omega_5 = 2$ and $\omega_3 = 2$*. By Theorem 3, we get* $\Gamma_{5,4} = 14$ *and* $\lambda_{1,5^4} = 13$*. Then, by Theorem 14, we obtain* $\omega_2 = 152$*. By Lemma 4 we have* $T_1 = 4$ *and by Theorem 7 one gets* $M = 1182481$*. By Theorem 15, we get* $\omega_0 = 236$*,* $\omega_1 =$ 209 and $\omega_4 = 24$.

The result of the above computation can also be obtained directly by Corollary 17, and it is in accordance with the differential spectrum of the mapping x^{622} over $\mathbb{F}_{5^4}$ calculated directly by Magma, which is

$$\begin{aligned}[\omega_0 = 236,\ \omega_1 = 209,\ \omega_2 = 152,\\ \omega_3 = 2,\quad \omega_4 = 24,\ \omega_5 = 2].\end{aligned}$$

Example 3. *Let $p = 5$, $n = 5$, $d = p^n - 3 = 3122$ and η be the quadratic character of $\mathbb{F}_{5^5}$. Then, one has $\eta(2) = \eta(-3) = -1$. Thus, by Theorems 9 and 12, we have $\omega_5 = 0$ and $\omega_3 = 0$. We get $\Gamma_{5,5} = 82$ and $\lambda_{1,5^5} = 83$ by Theorem 3. Then, by Theorem 14, we obtain $\omega_2 = 760$. By Lemma 4 we have $T_1 = 0$ and by Theorem 7 one gets $M = 29524925$. By Theorem 15, we get $\omega_0 = 1180$, $\omega_1 = 1045$ and $\omega_4 = 140$.*

From Corollary 17, we can get the same result directly. The above result is also in accordance with the numerical result obtained from computer experiments, which is

$$\begin{aligned}[\omega_0 = 1180,\ \omega_1 = 1045,\ \omega_2 = 760,\\ \omega_3 = 0,\quad \omega_4 = 140].\end{aligned}$$

Example 4. *Let $p = 7$, $n = 4$, $d = p^n - 3 = 2398$. By Theorems 9 and 12, we have $\omega_5 = 0$ and $\omega_3 = 0$. By Theorem 3 and Remark 2, we get $\lambda_{1,7^4} = -99$. Then, by Theorem 14, we obtain $\omega_2 = 624$. By Lemma 4 we have $T_1 = 3$ and by Theorem 7 one gets $M = 17056801$. By Theorem 15, we get $\omega_0 = 888$, $\omega_1 = 801$ and $\omega_4 = 88$.*

The above result can also be obtained directly by Corollary 18, and it coincides with the numerical result computed by Magma, which is

$$[\omega_0 = 888,\ \omega_1 = 801,\ \omega_2 = 624,\ \omega_3 = 0,\ \omega_4 = 88].$$

V. CONCLUDING REMARKS

In this paper, we determine the differential spectrum of power function x^{p^n-3} over $\mathbb{F}_{p^n}$ for all primes $p \geq 3$ with a unified approach. It is interesting that the differential spectrum of x^{p^n-3} has a close connection with the quadratic character sums λ_{1,p^n} defined as in (1) and λ_{2,p^n} in (2). When $p \geq 5$, these two quadratic character sums are all related to the quadratic character sum $\Gamma_{p,n}$, which can be evaluated by the theory of elliptic curves over finite fields. As a result, the differential spectrum of x^{p^n-3} over $\mathbb{F}_{p^n}$ is completely determined in the sense that for any given odd prime p, all its coordinates can be expressed explicitly in terms of n. Our result resolves a problem that is left open for twenty years, and includes a recent result in [22] as a special case.

VI. ACKNOWLEDGEMENTS

The authors are very grateful to the associate editor and the anonymous reviewers for careful reading and for many valuable comments that improved the quality of the paper.

REFERENCES

[1] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” *J. Cryptology*, vol. 4, no. 1, pp. 3-72, 1991.

[2] 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.

[3] 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.

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

[5] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. S. Kaleyski, “On two fundamental problems on APN power functions,” *IEEE Trans. Inf. Theory*, doi: 10.1109/TIT.2022.3147060.

[6] C. Carlet, P. Charpin, and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems,” *Des. Codes Cryptogr.*, vol. 15, no. 2, pp. 125-156, 1998.

[7] C. Carlet, “Characterizations of the differential uniformity of vectorial functions by the Walsh transform,” *IEEE Trans. Inf. Theory*, vol. 64, no. 9, pp. 6443-6453, 2018.

[8] P. Charpin and J. Peng, "Differential uniformity and the associated codes of cryptographic functions," *Adv. Math. Commun.*, vol. 13, no. 4, pp. 579-600, 2019.

[9] P. Charpin and J. Peng, "New links between nonlinearity and differential uniformity," *Finite Fields Appl.*, vol. 56, pp. 188-208, 2019.

[10] 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.

[11] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary *m*-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473-1481, 2001.

[12] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials,* Pitman Monographs in Pure and Applied Mathematics, vol. 65. New York: John Wiley & Sons, 1993.

[13] 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.

[14] N. Li, Y. Wu, X. Zeng, and X. Tang, "On the differential spectrum of a class of power functions over finite fields," arXiv:2012.04316, 2020.

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

[16] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials,* Pitman Monographs in Pure and Applied Mathematics, vol. 65. New York: John Wiley & Sons, 1993.

[17] L. Lei, W. Ren, and C. Fan, "The differential spectrum of a class of power functions over finite fields," *Adv. Math. Commun.*, vol. 15, no. 3, pp. 525-537, 2021.

[18] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science)*, vol. 765, T. Helleseth Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 386-397.

[19] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science)*, vol. 765, T. Helleseth Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 55-64.

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition. Heidelberg: Springer, 2009.

[21] C. Tang, C. Ding, and M. Xiong, "Codes, differentially δ-uniform functions, and t-designs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3691-3703, 2020.

[22] Y. Xia, X. Zhang, C. Li, and T. Helleseth, "The differential spectrum of a ternary power mapping," *Finite Fields Appl.*, vol. 64, 2020.

[23] M. Xiong and H. Yan, "A note on the differential spectrum of a differentially 4-uniform power function," *Finite Fields Appl.*, vol. 48, pp. 117-125, 2017.

[24] M. Xiong, H. Yan, and P. Yuan, "On a conjecture of differentially 8-uniform power functions," *Des. Codes Cryptogr.*, vol. 86, no. 8, pp. 1601-1621, 2018.

[25] H. Yan, Z. Zhou, J. Wen, J. Weng, T. Helleseth, and Q. Wang, "Differential spectrum of Kasami power permutations over odd characteristic finite fields," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6819-6826, 2019.

Haode Yan received the B.S. and Ph. D. degree in mathematics from Shanghai Jiao Tong University, Shanghai, China, in 2010 and 2016, respectively. From 2016 to 2017, he was a postdoctoral member in the Department of Mathematics, the Hong Kong University of Science and Technology. Since 2017, he has been in the School of Mathematics, Southwest Jiaotong University, where he is currently an Associate Professor. His research interests include coding theory, cryptography and combinatorics.

Yongbo Xia received the B.S., the M.S. and the Ph.D. degrees in mathematics from the Department of Mathematics, Hubei University, Wuhan, China, in 2003, 2006 and 2009, respectively. From Sept. 2013 to Sept. 2014, and from Jul. 2016 to Aug. 2016, he was a visiting researcher in the Department of Informatics, University of Bergen, Norway. Since 2006, he has been with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan, China, where he is currently a Professor. His research interests include sequence design for wireless communication, coding theory and cryptography.

Chunlei Li (Member, IEEE) received the Ph.D. degree from the University of Bergen, Norway, in 2014. He was a Post-Doctoral Researcher with the University of Stavanger, Norway, from 2015 to 2017, and a Researcher with the University of Bergen from 2017 to 2018. Since 2018, he has been an Associate Professor with the Department of Informatics, University of Bergen. His research interests include sequence design, coding theory, and cryptography. He was the Program Co-Chair of the workshops Mathematical Methods for Cryptography in 2017 and Sequences and Their Applications (SETA) in 2020, and served as a program committee member for several workshops including WAIFI18, SETA18, BFA20/21, IWSDA19/22 and WCC22.

Tor Helleseth received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973 to 1980, he was a Research Assistant with the Department of Mathematics, University of Bergen. From 1981 to 1984, he was with the Chief Head Quarters of Defense in Norway. Since 1984, he has been a Professor with the Department of Informatics, University of Bergen. During the academic years, from 1977 to 1978 and from 1992 to 1993, he was on sabbatical leave with the University of Southern California, Los Angeles. From 1979 to 1980, he was a Research Fellow with the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology. In 1997, he was elected as an IEEE fellow for his contributions to coding theory and cryptography. In 2004, he was elected as a member of Det Norske Videnskaps-Akademi. He was the Program Chairman of Eurocrypt 1993 and the Information Theory Workshop in 1997, Longyearbyen, Norway. He was the Program Co-Chairman of SEquences and Their Applications (SETA) in 1998, 2001, 2004, 2006, 2012, 2018, and 2020, and the IEEE Information Theory Workshop in Solstrand, Norway, in 2007. From 2007 to 2009, he served on the Board of Governors for the IEEE Information Theory Society. He served as an Associate Editor for coding theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1991 to 1993 and from 2012 to 2014.

Maosheng Xiong received the Ph.D. degree in mathematics from the University of Illinois at Urbana-Champaign in 2007. He was a postdoc at Pennsylvania State University from August 2007 to June 2010. He joined the Department of Mathematics, The Hong Kong University of Science and Technology in 2010 and is currently an Associate Professor. His area of research interests is in algebraic coding theory and number theory.

Jinquan Luo was born in Anhui, China, in February 1980. He received the B.S. degree in mathematics from Zhejiang University, Hangzhou, China, in July 2001, and the Ph.D. degree in mathematics from Tsinghua University, Beijing, China, in January 2007. He joined Yangzhou University, China, in 2007. He is currently a Professor with Central China Normal University, China. His major research interests are coding theory, cryptology, and number theory.