The Differential Spectrum of a Ternary Power Mapping

Yongbo Xia*, Xianglai Zhang*, Chunlei Li† and Tor Helleseth†

Abstract

A function $f(x)$ from the finite field $\mathrm{GF}(p^n)$ to itself is said to be differentially δ-uniform when the maximum number of solutions $x \in \mathrm{GF}(p^n)$ of $f(x+a)-f(x)=b$ for any $a \in \mathrm{GF}(p^n)^*$ and $b \in \mathrm{GF}(p^n)$ is equal to δ. Let $p=3$ and $d=3^n-3$. When $n>1$ is odd, the power mapping $f(x)=x^d$ over $\mathrm{GF}(3^n)$ was proved to be differentially 2-uniform by Helleseth, Rong and Sandberg in 1999. For even n, they showed that the differential uniformity Δ_f of $f(x)$ satisfies $1 \le \Delta_f \le 5$. In this paper, we present more precise results on the differential property of this power mapping. For $d=3^n-3$ with even $n>2$, we show that the power mapping x^d over $\mathrm{GF}(3^n)$ is differentially 4-uniform when $n \equiv 2 \pmod 4$ and is differentially 5-uniform when $n \equiv 0 \pmod 4$. Furthermore, we determine the differential spectrum of x^d for any integer $n>1$.

Index Terms Power mapping, Differential cryptanalysis, Differential uniformity, Differential spectrum.

AMS 94B15, 11T71

1 Introduction

Let $\mathrm{GF}(p^n)$ denote the finite field with p^n elements and $\mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) \setminus \{0\}$, where p is a prime. Let $f(x)$ be a mapping from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p^n)$. Define

$$N_f(a,b) = \left| \{x \in GF(p^n) \,|\, f(x+a)-f(x)=b\} \right| \tag{1}$$

where $a, b \in \mathrm{GF}(p^n)$, and let

$$\Delta_f = \max \{N_f(a,b) \mid a \in \mathrm{GF}(p^n)^*, b \in \mathrm{GF}(p^n)\}.$$

Nyberg defined a mapping $f(x)$ to be differentially δ-uniform if $\Delta_f = \delta$ [11]. Differential uniformity is one of the most important notions in symmetric cryptography. It quantifies

*Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China. Y. Xia is 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).

†Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: chunlei.li@uib.no, tor.helleseth@uib.no)

the security of S-boxes used in block ciphers with respect to the differential attack [1]. For practical applications, cryptographic functions are desirable to have low differential uniformity. A function $f(x)$ is said to be almost perfect nonlinear (APN) if $\Delta_f = 2$ and perfect nonlinear (PN) if $\Delta_f = 1$. It is clear that when the finite field has characteristic 2, the solutions in (1) come in pairs. Hence PN functions only exist in finite fields of odd characteristic.

Power mappings with low differential uniformity serve as good candidates for the design of S-boxes since they usually have lower implementation costs in hardware environments. Besides, their particular algebraic structure makes the determination of their differential properties relatively easier. Given a cryptographic function $f(x)$, the differential spectrum of $f(x)$, namely the value distribution of $N_f(a,b)$ for $a \in \mathrm{GF}(p^n)^*$ and $b \in \mathrm{GF}(p^n)$, is also an important notion for estimating its resistance against variants of differential cryptanalysis [2, 3, 5, 6]. For a power mapping $f(x) = x^d$ with some positive integer d, by (1) we have $N_f(a,b) = N_f(1, \frac{b}{a^d})$ for all $a \neq 0$. Thus, the differential spectrum of $f(x)$ can be completely determined by the values of $N_f(1,b)$, $b \in \mathrm{GF}(p^n)$, which enables us to simplify the differential spectrum of a power mapping as follows.

Definition 1 *With the notation introduced above, let $f(x) = x^d$ be a power mapping over $\mathrm{GF}(p^n)$. Denote by ω_i the number of output differences b that occur i times:*

$$\omega_i = |\{b \in \mathrm{GF}(p^n) \mid N_f(1,b) = i\}|.$$

The differential spectrum of $f(x)$ is defined as the multi-set

$$\mathbb{S} = \{\omega_0, \omega_1, \cdots, \omega_\delta\},$$

where δ is the differential uniformity of $f(x)$.

It is easily seen that the differential spectrum defined as above has the following properties

$$\sum_{i=0}^{\delta} \omega_i = p^n \text{ and } \sum_{i=0}^{\delta} (i \times \omega_i) = p^n. \tag{2}$$

Utilizing these properties, the following results can be easily derived.

Proposition 1 *([16, Proposition 1]) (i) If p is odd and $f(x) = x^d$ is PN over $\mathrm{GF}(p^n)$, then its differential spectrum is*

$$\{\, \omega_0 = 0, \omega_1 = p^n \,\};$$

(ii) if $f(x) = x^d$ is APN over $\mathrm{GF}(2^n)$*, then its differential spectrum is*

$$\left\{ \omega_0 = 2^{n-1}, \omega_1 = 0, \omega_2 = 2^{n-1} \right\}.$$

Recently, the differential spectra of several families of power functions over $GF(2^n)$ with differential uniformity 4, 6 and 8 were determined [2, 3, 4, 14, 15]. For power functions defined over finite fields of odd characteristic, there are also some classes of power functions whose differential spectra have been calculated [8, 7, 16]. In [8], for an odd integer n and $d = 2 \cdot 3^{\frac{n-1}{2}} + 1$, the differential spectrum of the ternary power function x^d over $\mathrm{GF}(3^n)$ was determined, and the result was used to study the cross-correlation between two ternary m-sequences of period $3^n - 1$. In this paper, we investigate a ternary power function $f(x) = x^d$ over $\mathrm{GF}(3^n)$ with $d = 3^n - 3$, where $n > 1$. The differential spectrum of this power function is determined. Our main results are given in the following theorem.

Theorem 1 *Let $d = 3^n - 3$ and $f(x) = x^d$ be a power mapping over* $\mathrm{GF}(3^n)$*. When $n > 2$, the differential uniformity Δ_f of $f(x)$ is given by*

$$\Delta_f = \begin{cases} 2, & \text{if } n \text{ is odd,} \\ 4, & \text{if } n \equiv 2 \pmod 4, \\ 5, & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

Furthermore, the corresponding differential spectra are given by

(i) $\left\{ \omega_0 = \frac{3^n-3}{2}, \omega_1 = 3, \omega_2 = \frac{3^n-3}{2} \right\}$ *if n is odd;*

(ii) $\left\{ \omega_0 = \frac{3^n-9}{4}, \omega_1 = 2 \cdot 3^{n-1} + 3, \omega_2 = 0, \omega_3 = 0, \omega_4 = \frac{3^{n-1}-3}{4} \right\}$ *if* $n \equiv 2 \pmod 4$*;*

(iii) $\left\{ \omega_0 = \frac{3^n-1}{4}, \omega_1 = 2 \cdot 3^{n-1} + 1, \omega_2 = 0, \omega_3 = 0, \omega_4 = \frac{3^{n-1}-11}{4}, \omega_5 = 2 \right\}$ *if* $n \equiv 0 \pmod 4$.

In particular, when $n = 2$, x^d is PN over $\mathrm{GF}(3^n)$.

A more general form of the above mapping is $f(x) = x^{p^n-3}$ over $GF(p^n)$ with p being a prime. The differential properties of this power mapping have been discussed in the literature. By the setting $\frac{1}{0^2} := 0$, this power mapping can be written as $f(x) = \frac{1}{x^2}$. When $p = 2$, it is linearly equivalent to the inverse function $\frac{1}{x}$ over $\mathrm{GF}(2^n)$. Hence, the differential spectrum of $f(x)$ is the same as that of the inverse function $\frac{1}{x}$, which has been determined in [2, Example 1]. When p is an odd prime, the differential uniformity of $f(x)$ has been investigated in [9].

More specifically, it is proved in [9, Theorem 7] that the differential uniformity Δ_f satisfies $1 \leq \Delta_f \leq 5$; in particular, for $p = 3$ and odd n, it is proved that $\Delta_f = 2$ by investigating the Gröbner basis of certain equations. In this paper, we use a different approach to further studying the differential property of the power mapping x^{3^n-3} over $\mathrm{GF}(3^n)$. As a result, we not only obtain the exact differential uniformity of this function, but also completely determine its differential spectrum, which settled the open problem in [9].

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries and notation. Section 3 is dedicated to the proof of our main result. The conclusive remarks are given in Section 4.

2 Preliminaries

In order to prove our main result in Theorem 1, we need to make some preparations. Let p be an odd prime, and α a primitive element of $\mathrm{GF}(p^n)$. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ denote the sets of squares and nonsquares in $\mathrm{GF}(p^n)^*$, respectively. The cyclotomic number (i, j) for $i, j \in \{0, 1\}$ is defined as the cardinality of the set $\mathcal{E}_{ij} = (\mathcal{C}_i + 1) \cap \mathcal{C}_j$.

Lemma 1 *([12, Lemma 6]) The cyclotomic numbers (i, j) are given as follows:*
(i) if $p^n \equiv 1 \pmod 4$, then

$$(0,0) = \frac{p^n - 5}{4},\ (0,1) = (1,0) = (1,1) = \frac{p^n - 1}{4};$$

(ii) if $p^n \equiv 3 \pmod 4$, then

$$(0,0) = (1,0) = (1,1) = \frac{p^n - 3}{4},\ (0,1) = \frac{p^n + 1}{4}.$$

Indeed, the elements in $\mathcal{E}_{ij}$ for $i, j \in \{0, 1\}$ can be fully characterized [7]. The following lemma characterizes the elements of $\mathcal{E}_{00}$.

Lemma 2 *([7, Lemma 2]) Let p be an odd prime, and α a primitive element of $\mathrm{GF}(p^n)$. Then, each element x in $\mathcal{E}_{00}$ has the following representation*

$$x = \left(\frac{\alpha^k - \alpha^{-k}}{2}\right)^2,$$

where $k \in \{1, \cdots, \frac{p^n-5}{4}\}$ if $p^n \equiv 1 \pmod 4$ and $k \in \{1, \cdots, \frac{p^n-3}{4}\}$ if $p^n \equiv 3 \pmod 4$.

Let q be a prime power, and denote the polynomial ring over $\mathrm{GF}(q)$ by $\mathrm{GF}(q)[x]$. The following lemma about the quadratic equations over finite fields will be frequently used in this paper, and its proof is trivial.

Lemma 3 *[10, Exercise 5.24] The polynomial $Q(x) = x^2 + ax + b \in \mathrm{GF}(q)[x]$, q odd, is irreducible in $\mathrm{GF}(q)[x]$ if and only if $a^2 - 4b$ is a nonsquare in $\mathrm{GF}(q)$. In particular, if $a^2 - 4b$ is a nonzero square in $\mathrm{GF}(q)$, $Q(x)$ has two distinct roots in $\mathrm{GF}(q)$.*

For a square s in the finite field $\mathrm{GF}(q)$ with odd q, we will use $\sqrt{s}$ and $-\sqrt{s}$ to denote the two square roots of s throughout the paper.

3 The proof of the main theorem

In this section, our main goal is to give the proof of Theorem 1. Let $d = 3^n - 3$ and we shall investigate the following equation

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

in $\mathrm{GF}(3^n)$. For simplicity, we use $N(b)$ instead of $N(1, b)$ to denote the number of solutions of (3) in $\mathrm{GF}(3^n)$. Calculating the differential spectrum of x^d can be reduced to determining the value distribution of $N(b)$ as b runs through $\mathrm{GF}(3^n)$.

For $b \in \mathrm{GF}(3)$, $N(b)$ can be easily determined. For $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, the situation becomes more difficult. If $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, one can immediately conclude that the solutions of (3) are not in $\mathrm{GF}(3)$. Thus, in this case $x(x+1) \neq 0$ and (3) becomes

$$(1+x)^{-2} - x^{-2} = b,$$

which can be rewritten as

$$x^4 + 2x^3 + x^2 + \frac{2}{b}x + \frac{1}{b} = 0.$$

Replacing x by $(x - \frac{1}{2})$, we get the main equation in this paper as follow:

$$x^4 + x^2 - ux + 1 = 0, \tag{4}$$

where $u = \frac{1}{b}$. Note that b (resp. x) $\in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ if and only if u (resp. $x - \frac{1}{2}$) $\in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$. Thus, $N(b)$ is equal to the number of solutions of (4) in $\mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$. Therefore,

in order to determine the value distribution of $N(b)$ for $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, it is equivalent to studying the roots of the polynomial

$$h_u(x) = x^4 + x^2 - ux + 1 \tag{5}$$

in $\mathrm{GF}(3^n)$, where $n > 1$ and $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$.

Note that the derivative $h'_u(x)$ of $h_u(x)$ is $x^3 - x - u$, and $\gcd(h'_u(x), h_u(x)) = \gcd(x^2 - 1, u)$, which is equal to 1 when $u \neq 0$. This implies that $h_u(x)$ has no multiple roots in its splitting field for $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$. Moreover, it is clear that $h_u(x)$ can not have exactly three roots in $\mathrm{GF}(3^n)$ since in that case the fourth root belongs to $\mathrm{GF}(3^n)$ as well. Thus, we have the following proposition.

Proposition 2 *Let $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ and $h_u(x)$ be the polynomial defined as in (5). Then, (i) if r_0 is a root of $h_u(x)$ in $\mathrm{GF}(3^n)$, then r_0 has multiplicity 1 and belongs to $\mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$; (ii) for each $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, the possible numbers of distinct roots of $h_u(x)$ in $\mathrm{GF}(3^n)$ are 0, 1, 2 and 4.*

Next we consider the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has two (resp. four) distinct roots in $\mathrm{GF}(3^n)$. Before we proceed, we give some useful facts as follows. Let α be a primitive root of $\mathrm{GF}(3^n)$. It follows that $-1 = \alpha^{\frac{3^n-1}{2}}$ is a square in $\mathrm{GF}(3^n)$ if and only if n is even, since $3^n \equiv 1 \pmod 4$ for even n and $3^n \equiv 3 \pmod 4$ for odd n. Moreover, when n is even, one has $3^n \equiv 1 \pmod 8$, which implies that $\pm\sqrt{-1} = \pm\alpha^{\frac{3^n-1}{4}}$ are also squares in $\mathrm{GF}(3^n)$. Furthermore, the squares $\pm\sqrt{-1}$ are fourth powers in $\mathrm{GF}(3^n)$ when $n \equiv 0 \pmod 4$ since $3^n \equiv 1 \pmod{16}$ if and only $n \equiv 0 \pmod 4$.

The following results build the foundation to compute the differential spectrum of $f(x)$ in Theorem 1.

Lemma 4 *Let $F(x) = x^3 - x^2 - 1$, $\mathcal{C}_0$ be the set of squares in $\mathrm{GF}(3^n)^*$ and $\mathcal{E}_{00} = (\mathcal{C}_0 + 1) \cap \mathcal{C}_0$.*
(i) When n is odd, the polynomial $F(x)$ has no root in $\mathcal{C}_0$.
(ii) When n is even, the polynomial $F(x)$ has no root in the set

$$\mathcal{A} = \left\{ \frac{(t^2-1)^2}{t^2(t^2+1)} \,|\, t^2 \in \mathcal{T} \right\},$$

where the set $\mathcal{T}$ is given by

$$\mathcal{T} = \begin{cases} \mathcal{E}_{00} \setminus \{1\}, & \text{if } n \equiv 2 \pmod 4, \\ \mathcal{E}_{00} \setminus \{1, 1 \pm c, 1 \pm \sqrt{1-c}, 1 \pm \sqrt{1+c}\}, & \text{if } n \equiv 0 \pmod 4, \end{cases}$$

with $c = \sqrt{-1}$.

Proof: For the polynomial

$$F(x) = x^3 - x^2 - 1 = (x+1)(x^2 - 2x + 2), \tag{6}$$

its divisor $x^2 - 2x + 2 \in \mathrm{GF}(3)[x]$ has discriminant -1. Thus, it is an irreducible polynomial over $\mathrm{GF}(3)$, and all its roots are in $\mathrm{GF}(3^2)$.

(i) When n is odd, $F(x)$ has only one root -1 in $\mathrm{GF}(3^n)$. In this case, -1 is a nonsquare in $\mathrm{GF}(3^n)$, and thus $F(x) \neq 0$ for any $x \in \mathcal{C}_0$.

(ii) When n is even, -1 is a square in $\mathrm{GF}(3^n)$ and $x^2 - 2x + 2$ has two roots $1 \pm \sqrt{-1}$ in $\mathrm{GF}(3^n)$. Then, in this case $F(x)$ has exactly three roots in $\mathrm{GF}(3^n)$, which are -1, $1 + c$ and $1 - c$, where $c = \sqrt{-1}$. Notice that $(1 \pm c)^2 = \mp c$ which are fourth powers in $\mathrm{GF}(3^n)$ if and only if $n \equiv 0 \pmod 4$. Thus, $1 \pm c$ are squares in $\mathrm{GF}(3^n)$ if $n \equiv 0 \pmod 4$ and nonsquares if $n \equiv 2 \pmod 4$. Notice that $\mathcal{A}$ is a subset of $\mathcal{C}_0$. In what follows we will show that none of the three roots of $F(x)$ belongs to the set $\mathcal{A}$. We consider the following two cases:

Case 1: $n \equiv 2 \pmod 4$. Then, $1 \pm c$ are nonsquares in $\mathrm{GF}(3^n)$ and thus they are not in $\mathcal{A}$. By (6), $F(x)$ has only one root -1 in $\mathcal{C}_0$. We observe that $-1 \notin \mathcal{A}$. Otherwise, -1 can be written in the form

$$-1 = \frac{(t^2-1)^2}{t^2(t^2+1)},$$

which implies $t^2(t^2+1) = 1$. Then, we obtain that $t^2 = 1 \pm c$. This leads to a contradiction since $1 \pm c$ are nonsquares in $\mathrm{GF}(3^n)$ in this case. Thus, $-1 \notin \mathcal{A}$ and $F(x) \neq 0$ for any x in $\mathcal{A}$.

Case 2: $n \equiv 0 \pmod 4$. From the above discussion, we know that $F(x)$ has roots -1, $1 + c$ and $1 - c$ in $\mathcal{C}_0$. Next we show that none of these roots belongs to $\mathcal{A}$. Our discussion proceeds with three subcases.

Subcase 2.1: Suppose that the root -1 can be written in the form $-1 = \frac{(t^2-1)^2}{t^2(t^2+1)}$. Then, we have $t^2(t^2+1) = 1$, which implies $t^2 = 1 \pm c$. Note that when $n \equiv 0 \pmod 4$, $1 \pm c$ are

squares in $\mathrm{GF}(3^n)$ and $(1 \pm c) + 1 = -1 \pm c$ are also squares. The elements $1 \pm c$ belong to $\mathcal{E}_{00}$ but not to $\mathcal{T}$. Thus, -1 is not in $\mathcal{A}$.

Subcase 2.2: If the root $1 + c$ can be written in the form $1 + c = \frac{(t^2-1)^2}{t^2(t^2+1)} = 1 + \frac{1}{t^4+t^2}$, then we have $t^4 + t^2 - \frac{1}{c} = t^4 + t^2 + c = 0$, which implies $t^2 = 1 \pm \sqrt{1-c}$. Next we show that $1 \pm \sqrt{1-c} \in \mathcal{E}_{00}$. First, we need to show that $1 \pm \sqrt{1-c}$ are squares in $\mathrm{GF}(3^n)$. Suppose that $1 + \sqrt{1-c} = \gamma^2$ for some $\gamma \in \mathrm{GF}(3^n)$, which can be transformed into $\gamma^2 - 1 = \sqrt{1-c}$. By repeated squaring both sides, we have

$$\gamma^8 + 2\gamma^6 + \gamma^4 + 1 = (\gamma^4 + \gamma^3 + 2)(\gamma^4 - \gamma^3 + 2) = 0.$$

Note that the associated polynomials $x^4 + x^3 + 2$ and $x^4 - x^3 + 2$ are irreducible over $\mathrm{GF}(3)$, and their roots are all in the subfield $\mathrm{GF}(3^4)$ of $\mathrm{GF}(3^n)$ when $n \equiv 0 \pmod 4$. Therefore, there exists a $\gamma \in \mathrm{GF}(3^n)$ such that $1 + \sqrt{1-c} = \gamma^2$. This shows that $1 + \sqrt{1-c}$ is a square in $\mathrm{GF}(3^n)$, and one can further derive that $1 - \sqrt{1-c}$ is also a square in $\mathrm{GF}(3^n)$ since $(1 + \sqrt{1-c})(1 - \sqrt{1-c}) = c$ is a square. Note that $(1 \pm \sqrt{1-c}) + 1 = -(1 \mp \sqrt{1-c})$, which are also squares in $\mathrm{GF}(3^n)$. Thus, $1 \pm \sqrt{1-c} \in \mathcal{E}_{00}$. These two values have been excluded from $\mathcal{E}_{00}$ and are not in $\mathcal{T}$. Hence we have $1 + c \notin \mathcal{A}$.

Subcase 2.3: Suppose that $1 - c$ can be written in the form $1 - c = \frac{(t^2-1)^2}{t^2(t^2+1)}$. Then we can similarly show that the corresponding elements $t^2 = 1 \pm \sqrt{1+c}$ belong to $\mathcal{E}_{00}$ but not to $\mathcal{T}$. Thus $1 - c$ is not in $\mathcal{A}$. □

Lemma 5 *Let $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ and $h_u(x)$ be the polynomial defined as in (5). Then, $h_u(x)$ has two (resp. four) roots in $\mathrm{GF}(3^n)$ if and only if*

$$u = \pm a^2\sqrt{a^2 - 1}, \tag{7}$$

with $a \in \mathrm{GF}(3^n)^*$ satisfying the following three conditions:
(i) $a^2 - 1$ is a square in $\mathrm{GF}(3^n)^*$;
(ii) one and only one of $-1 + \frac{a}{\sqrt{a^2-1}}$ and $-1 - \frac{a}{\sqrt{a^2-1}}$ is a square in $\mathrm{GF}(3^n)^*$ (resp. both $-1 + \frac{a}{\sqrt{a^2-1}}$ and $-1 - \frac{a}{\sqrt{a^2-1}}$ are squares in $\mathrm{GF}(3^n)^*$);
(iii) $a^6 - a^4 - 1 \neq 0$.

Proof: If $h_u(x)$ has two or more roots in $\mathrm{GF}(3^n)$, then $h_u(x)$ has the following factorization over $\mathrm{GF}(3^n)$

$$h_u(x) = \left(x^2 + ax + b\right)\left(x^2 - ax + b^{-1}\right), \tag{8}$$

where $a \in \mathrm{GF}(3^n)$ and $b \in \mathrm{GF}(3^n)^*$ satisfying

$$\begin{cases} b + b^{-1} = a^2 + 1, \\ u = a(b - b^{-1}). \end{cases} \tag{9}$$

The discriminants of the two quadratic polynomials $x^2 + ax + b$ and $x^2 - ax + b^{-1}$ in (8) are $a^2 - b$ and $a^2 - b^{-1}$, respectively. By Proposition 2, $h_u(x)$ has no multiple roots. Thus, neither of the two discriminants can be equal to zero. By Lemma 3, $h_u(x)$ has exactly two roots in $\mathrm{GF}(3^n)$ if one and only one of the two discriminants is a square in $\mathrm{GF}(3^n)^*$, and $h_u(x)$ has exactly four roots in $\mathrm{GF}(3^n)$ if both of them are squares in $\mathrm{GF}(3^n)^*$.

The first equation in (9) is equivalent to

$$\left(b + (a^2 + 1)\right)^2 = a^2(a^2 - 1). \tag{10}$$

If $a^2 = 0$ or 1, then we can derive the equality $b = b^{-1}$ from (10), which leads to $u = 0$, a contradiction to the assumption. Thus, to ensure that (9) holds, $a(a^2 - 1) \neq 0$ and $a^2 - 1$ must be a square in $\mathrm{GF}(3^n)^*$, which is the desired condition (i).

Furthermore, solving the first equation in (9), we obtain

$$b = -(a^2 + 1) \pm a\sqrt{a^2 - 1}. \tag{11}$$

Substituting the above solutions into the second equation of (9), we get

$$u = \pm a^2\sqrt{a^2 - 1},$$

where $a \in \mathrm{GF}(3^n)^*$ satisfies that $a^2 - 1$ is a square in $\mathrm{GF}(3^n)^*$. By (11), the two discriminants $a^2 - b$ and $a^2 - b^{-1}$ become exactly $(a^2 - 1)(-1 \pm \frac{a}{\sqrt{a^2-1}})$, respectively. The desired result (ii) follows immediately since $a^2 - 1$ is already a square.

Since $u \in \mathrm{GF}(3^n) \backslash \mathrm{GF}(3)$, we have $u^2 \neq 1$, which implies that $a^4(a^2-1)-1 = a^6-a^4-1 \neq 0$. Thus, we obtain the desired condition (iii). The proof of the necessity is thus finished.

Conversely, for a given u of the form (7) with $a \in \mathrm{GF}(3^n)^*$ satisfying the conditions (i)-(iii) in this lemma, we can determine b and b^{-1} from (10), and then get the factorization of $h_u(x)$ as (8). Finally, considering the two discriminants of the polynomials x^2+ax+b and x^2-ax+b^{-1}, we obtain the desired result.

□

Based on Lemmas 4 and 5, we can prove the following proposition.

Proposition 3 *Let $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ and $h_u(x)$ be the polynomial defined as in (5). Then, (i) when $n > 1$ is odd, $h_u(x)$ cannot have four roots in $\mathrm{GF}(3^n)$ and in this case the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has exactly two roots in $\mathrm{GF}(3^n)$ is equal to $\frac{3^n-3}{2}$; (ii) when n is even, $h_u(x)$ cannot have exactly two roots in $\mathrm{GF}(3^n)$ and in this case the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has exactly four roots in $\mathrm{GF}(3^n)$ is equal to $\frac{3^{n-1}-3}{4}$ if $n \equiv 2 \pmod 4$ and $\frac{3^{n-1}-11}{4}$ if $n \equiv 0 \pmod 4$.*

Proof: In this proof, we always assume that $h_u(x)$ has two or more roots in $\mathrm{GF}(3^n)$. Using the notation introduced in Lemma 5, we have

$$\left(-1+\frac{a}{\sqrt{a^2-1}}\right)\left(-1-\frac{a}{\sqrt{a^2-1}}\right)=\frac{-1}{a^2-1}. \tag{12}$$

It is convenient to distinguish the cases of even and odd n.

(i) n is odd. Then, -1 is a nonsquare in $\mathrm{GF}(3^n)$, and so is $\frac{-1}{a^2-1}$. It follows from (12) that one of $\{\, -1 \pm \frac{a}{\sqrt{a^2-1}} \,\}$ is a square in $\mathrm{GF}(3^n)$ and the other is a nonsquare. Thus, in this case, $h_u(x)$ cannot have four roots, and moreover, according to Lemma 5, $h_u(x)$ has two roots in $\mathrm{GF}(3^n)$ if and only if $u = \pm a^2\sqrt{a^2-1}$ with $a \in \mathrm{GF}(3^n)^*$ satisfying the conditions (i) and (iii) in Lemma 5.

Let $\mathcal{C}_0$ and $\mathcal{E}_{00} = (\mathcal{C}_0 + 1) \cap \mathcal{C}_0$ be the notation introduced in Lemma 4. Assume that $a^2-1 = t^2 \in \mathcal{C}_0$. Then, it requires that $t^2 \in \mathcal{E}_{00}$. By Lemma 4 (i), when n is odd, $a^6-a^4-1 \neq 0$ for any $a \in \mathrm{GF}(3^n)$. Thus, when n is odd, the condition (iii) in Lemma 5 always holds. Therefore, when n is odd, for $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, $h_u(x)$ has exactly two roots in $\mathrm{GF}(3^n)$ if and only if $u = \pm a^2\sqrt{a^2-1}$ with $a^2 = t^2+1$ and $t^2 \in \mathcal{E}_{00}$.

Now we consider the number of such elements u. Let

$$\mathcal{U}_0 = \{\, u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3) \mid h_u(x) \text{ has exactly two roots in } \mathrm{GF}(3^n) \,\}.$$

Since an element $u \in \mathcal{U}_0$ if and only if $u = \pm a^2\sqrt{a^2-1} = \pm(t^2+1)t$ for some $t \in \mathbb{F}_{3^n}$ with $t^2 \in \mathcal{E}_{00}$, the set $\mathcal{U}_0$ can be rewritten as $\mathcal{U}_0 = \{u \mid u = \pm t(t^2+1),\, t^2 \in \mathcal{E}_{00}\}$. Moreover, if $t_1^3+t_1 = t_2^3+t_2$, then $(t_1-t_2)((t_1-t_2)^2+1) = 0$, which implies $t_1 = t_2$ since -1 is a nonsquare; if $t_1^3+t_1 = -(t_2^3+t_2)$, one similarly obtains $t_1 = -t_2$. This means that each $t^2 \in \mathcal{E}_{00}$ corresponds to two u's $\in \mathcal{U}_0$. Hence, it follows from Lemma 1 that $|\mathcal{U}_0| = 2|\mathcal{E}_{00}| = 2 \times \frac{3^n-3}{4} = \frac{3^n-3}{2}$.

(ii) n is even. Then -1 is a square in $\mathrm{GF}(3^n)$, and so is $\frac{-1}{a^2-1}$. Then from (12), it follows that both $-1+\frac{a}{\sqrt{a^2-1}}$ and $-1-\frac{a}{\sqrt{a^2-1}}$ are squares or nonsquares in $\mathrm{GF}(3^n)^*$. Thus, $h_u(x)$ cannot have exactly two roots in $\mathrm{GF}(3^n)$ in this case. Next we consider the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has exactly four roots in $\mathrm{GF}(3^n)$. Define

$$\mathcal{U} = \{\, u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3) \mid h_u(x) \text{ has exactly four roots in } \mathrm{GF}(3^n) \,\}. \tag{13}$$

According to Lemma 5, $u \in \mathcal{U}$ if and only if $u = \pm a^2\sqrt{a^2-1}$ with $a \in \mathrm{GF}(3^n)^*$ satisfying the corresponding conditions (i)-(iii) in Lemma 5. When n is even, the condition (ii) in Lemma 5 is equivalent to that $1+\frac{a}{\sqrt{a^2-1}}$ is a square in $\mathrm{GF}(3^n)^*$.

Assume that $\frac{a}{\sqrt{a^2-1}}+1 = t^2$ for some $t^2 \in \mathcal{C}_0$. Then, we have

$$a^2 = \frac{(t^2-1)^2}{t^2(t^2+1)} \text{ and } a^2-1 = \frac{1}{t^2(t^2+1)}.$$

To ensure that $a^2 \in \mathcal{C}_0$ and $a^2-1 \in \mathcal{C}_0$, t^2+1 should also belong to $\mathcal{C}_0$ and $t^2 \neq 1$. Then, we conclude that $a \in \mathrm{GF}(3^n)^*$ satisfying the corresponding conditions (i) and (ii) in Lemma 5 if and only if $a^2 = \frac{(t^2-1)^2}{t^2(t^2+1)}$ with $t^2 \in \mathcal{E}_{00} \setminus \{1\}$. In order to ensure that the condition (iii) in Lemma 5 also holds, some additional restrictions on $t^2 \in \mathcal{E}_{00} \setminus \{1\}$ should be imposed as follows.

Let

$$\mathcal{A} = \left\{ a^2 = \frac{(t^2-1)^2}{t^2(t^2+1)} \mid t^2 \in \mathcal{E}_{00} \setminus \{1\} \text{ and } a^6-a^4-1 \neq 0 \right\}.$$

By Lemma 4 (ii), the above set can be rewritten as

$$\mathcal{A} = \left\{ a^2 = \frac{(t^2-1)^2}{t^2(t^2+1)} \mid t^2 \in \mathcal{T} \right\}, \tag{14}$$

where the set $\mathcal{T}$ is given by

$$\mathcal{T} = \begin{cases} \mathcal{E}_{00} \setminus \{1\}, & \text{if } n \equiv 2 \pmod 4, \\ \mathcal{E}_{00} \setminus \{\, 1, 1 \pm c, 1 \pm \sqrt{1-c}, 1 \pm \sqrt{1+c}\,\}, & \text{if } n \equiv 0 \pmod 4, \end{cases} \tag{15}$$

with $c = \sqrt{-1}$. Here one should note that if $n = 2$, then $\mathcal{E}_{00} \setminus \{1\}$ is empty due to Lemma 1. This means that when $n = 2$, $h_u(x)$ cannot have four roots in $\mathrm{GF}(3^n)$.

Summarizing the above discussions, we conclude that $u \in \mathcal{U}$ if and only if $u = \pm a^2\sqrt{a^2-1}$ with $a^2 \in \mathcal{A}$, where $\mathcal{A}$ is given in (14). Notice that

$$u = \pm a^2\sqrt{a^2-1} = \left(\pm\sqrt{a^2-1}\right)^3 + \left(\pm\sqrt{a^2-1}\right).$$

In order to simplify the above expression for u, we define

$$\mathcal{B} = \{\, w \mid w^2 = a^2 - 1 \ \text{ with } a^2 \in \mathcal{A}\,\}. \tag{16}$$

Then, $u \in \mathcal{U}$ if and only if $u = w^3 + w$ with $w \in \mathcal{B}$.

It is obvious that $|\mathcal{B}| = 2|\mathcal{A}|$. Now we consider the relationship between $\mathcal{T}$ and $\mathcal{A}$. For $s^2, t^2 \in \mathcal{T}$, $\frac{(t^2-1)^2}{t^2(t^2+1)} = \frac{(s^2-1)^2}{s^2(s^2+1)}$ if and only if $s^2 = t^2$ or $s^2 + t^2 = -1$. In addition, when n is even, the set $\mathcal{E}_{00} \setminus \{1\}$ has the following property: if $t^2 \in \mathcal{E}_{00}$, then $-1 - t^2$ also belong to $\mathcal{E}_{00}$. Thus, the correspondence $a^2 = \frac{(t^2-1)^2}{t^2(t^2+1)}$ between $t^2 \in \mathcal{T}$ and $a^2 \in \mathcal{A}$ is 2-to-1. This means that $|\mathcal{A}| = |\mathcal{T}|/2$. Moreover, by the definition of $\mathcal{T}$ in (15), we have $|\mathcal{T}| = |\mathcal{E}_{0,0}| - 1$ if $n \equiv 2 \pmod 4$ and $|\mathcal{T}| = |\mathcal{E}_{0,0}| - 7$ if $n \equiv 2 \pmod 4$. Then, by Lemma 1, we have

$$|\mathcal{B}| = |\mathcal{T}| = \begin{cases} \frac{3^n-9}{4}, & \text{if } n \equiv 2 \pmod 4, \\ \frac{3^n-33}{4}, & \text{if } n \equiv 0 \pmod 4. \end{cases} \tag{17}$$

Now we determine the cardinality of $\mathcal{U}$. We will show that the correspondence $u = w^3 + w$ between $\mathcal{B}$ and $\mathcal{U}$ is 3-to-1, and then $|\mathcal{U}| = |\mathcal{B}|/3$. According to the relationship between $\mathcal{U}$ in (13) and $\mathcal{B}$ in (16), for a given $u \in \mathcal{U}$, there exists an element $w \in \mathcal{B}$ such that $u = w^3 + w$. For such given u, the polynomial

$$x^3 + x - u = x^3 + x - (w^3 + w) = (x - w)(x^2 + wx + (w^2 + 1))$$

has exactly three roots in GF(3^n), which are precisely w, $w-c$ and $w+c$, where $c=\sqrt{-1}$. In what follows we will prove that for such given $u \in \mathcal{U}$, $w \pm c$ also belong to $\mathcal{B}$. Combining (14) and (16), the set $\mathcal{B}$ can also be represented as

$$\mathcal{B} = \left\{ w \mid w^2 = \frac{1}{t^2(t^2+1)} \ \text{ with } t^2 \in \mathcal{T} \right\}. \tag{18}$$

To show that $w \pm c$ belong to $\mathcal{B}$, we only need to show that $(w \pm c)^2$ can be written in the form $\frac{1}{t_0^2(t_0^2+1)}$ for some $t_0^2 \in \mathcal{T}$ by (18).

First, we make some preparations. By the definition of $\mathcal{B}$ in (18), we assume that $w^2 = \frac{1}{t^2(t^2+1)}$ for some $t^2 \in \mathcal{T}$. By Lemma 2 and using the notation introduced there, assume $t^2 = (\alpha^k - \alpha^{-k})^2$ for some integer k. Then, we can rewrite w^2 as $\frac{1}{(y^2-y^{-2})^2}$, where $y = \alpha^k$. Without loss of generality, assume that $w = \frac{1}{y^2-y^{-2}}$. Then,

$$w(w-c) = \frac{1}{y^2-y^{-2}}(-c)\left(\frac{c+y^2-y^{-2}}{y^2-y^{-2}}\right) = \frac{1}{(y^2-y^{-2})^2}(-c)\left(y-cy^{-1}\right)^2, \tag{19}$$

which is a nonzero square in GF(3^n) since $-c$ is a square in GF(3^n) when n is even. Now we consider the following equation

$$w + c = \frac{1}{x^2 - x^{-2}}, \tag{20}$$

which is equivalent to

$$x^4 - \frac{1}{w+c}x^2 - 1 = 0. \tag{21}$$

Note that $\Delta = \frac{1}{(w+c)^2} + 1 = \frac{1}{(w+c)^2}w(w-c)$ is a nonzero square in GF(3^n) duo to (19). By Lemma 3, we have

$$\begin{aligned} x^2 &= -\tfrac{1}{w+c} \pm \sqrt{\Delta} \\ &= -\left(\tfrac{1 \mp \sqrt{w(w-c)}}{w+c}\right), \end{aligned} \tag{22}$$

where $\sqrt{\Delta}$ denote a square root of Δ in GF(3^n). In order to show that (22) has solutions in GF(3^n), we need to verify that the right hand side of (22) is a square in GF(3^n). Note that $c = \sqrt{-1}$ is a square in GF(3^n) when n is even. Thus, $\sqrt{c} \in$ GF(3^n). By (19), without loss

of generality, assume that $\sqrt{w(w-c)} = \frac{1}{y^2-y^{-2}} c\sqrt{c}(y - cy^{-1})$. Substituting it into the right hand side of (22), we have

$$\begin{aligned}
& -\left(\frac{1\mp\sqrt{w(w-c)}}{w+c}\right) \\
= & -\left(\frac{1\mp c\sqrt{c}(y-cy^{-1})/(y^2-y^{-2})}{1/(y^2-y^{-2})+c}\right) \\
= & -\left(\frac{(y^2-y^{-2})\mp c\sqrt{c}(y-cy^{-1})}{1+c(y^2-y^{-2})}\right) \\
= & -\left(\frac{y^{-2}}{c}\cdot\frac{(y^4-1)\mp c\sqrt{c}(y^3-cy)}{(y^2-y^{-2})+2c}\right) \\
= & -\left(\frac{1}{cy^2}\cdot\frac{y^4\mp c\sqrt{c}y^3\mp\sqrt{c}y-1}{(y+cy^{-1})^2}\right) \\
= & -\left(\frac{1}{cy^2}\cdot\frac{(y\mp c\sqrt{c})^4}{(y+cy^{-1})^2}\right) \\
= & \frac{1}{(c\sqrt{c}y)^2}\cdot\frac{(y\mp c\sqrt{c})^4}{(y+cy^{-1})^2},
\end{aligned}$$

which is indeed a square in $\mathrm{GF}(3^n)$. Thus, (22) has solutions in $\mathrm{GF}(3^n)$, and the solutions are not equal to ± 1 by (21). Combining (20)-(22), one knows that there exists an element $x \in \mathrm{GF}(3^n)^* \setminus \{\pm 1\}$ such that $(w+c)^2 = \frac{1}{(x^2-x^{-2})^2}$. Let x be the element given by (22) and $t_0^2 = (x-x^{-1})^2$. It is obvious that t_0^2 belongs to $\mathcal{E}_{00}$ due to Lemma 2. Hence $(w+c)^2 = \frac{1}{t_0^2(t_0^2+1)}$. Note that the value $t_0^2 = (x-x^{-1})^2$ must belong to $\mathcal{T}$. Otherwise, it will lead to

$$u = (w+c)^3 + (w+c) = w^3 + w \in \mathrm{GF}(3),$$

a contradiction. By (18), we conclude that $w+c \in \mathcal{B}$. Similarly, we can derive that $(w+c)+c = w-c \in \mathcal{B}$.

The above argument has shown that for each $u \in \mathcal{U}$, there are three w'$s \in \mathcal{B}$ such that $u = w^3 + w$. On the other hand, the polynomial $x^3 + x - u \in \mathrm{GF}(3^n)[x]$ has at most three roots in $\mathrm{GF}(3^n)$. Thus, the correspondence $u = w^3 + w$ between $w \in \mathcal{B}$ and $u \in \mathcal{U}$ is 3-to-1. Together with (17), we have

$$|\mathcal{U}| = \begin{cases} \frac{3^{n-1}-3}{4}, \text{ if } n \equiv 2 \pmod 4, \\ \frac{3^{n-1}-11}{4}, \text{ if } n \equiv 0 \pmod 4. \end{cases} \tag{23}$$

Note that as mentioned before, when $n = 2$, $\mathcal{E}_{00} \setminus \{1\}$ is empty and so is $\mathcal{T}$. Thus $|\mathcal{U}| = 0$, and the formula in (23) is also valid for $n = 2$. □

With the above preparations, we can now give the proof of the main theorem.

Proof of Theorem 1. As stated at the beginning of this section, let $N(b)$ denote the number of solutions of (3) in GF(3^n).

If $b = 0$, then (3) is equivalent to

$$\left(1 + \frac{1}{x}\right)^d = 1,$$

which has only one solution $x = 1$ in GF(3^n). Thus, $N(0) = 1$.

If $b = 1$, in addition to the solution $x = 0$, the other roots of (3) satisfy

$$(1 + x)^{-2} - x^{-2} = 1, \tag{24}$$

where $x \neq 0$ and $x \neq -1$. We can rewrite (24) as

$$x^4 + 2x^3 + x^2 + 2x + 1 = 0. \tag{25}$$

The polynomial on the left hand side of (25) is irreducible over GF(3), and its four roots are all in GF(3^4) but not in any subfield of GF(3^4). Thus, $N(1) = 5$ when $n \equiv 0 \pmod 4$ and $N(1) = 1$ otherwise.

Similarly, if $b = -1$, in addition to the solution $x = -1$, the other roots of (3) satisfy

$$(1 + x)^{-2} - x^{-2} = -1,$$

which can be rewritten as

$$x^4 + 2x^3 + x^2 + x + 2 = 0. \tag{26}$$

The polynomial on the left hand side of (26) is also irreducible over GF(3). Therefore, we have $N(-1) = 5$ when $n \equiv 0 \pmod 4$ and $N(-1) = 1$ otherwise.

Now we consider $N(b)$ when $b \in \text{GF}(3^n) \setminus \text{GF}(3)$. As stated before, in this case, $N(b)$ is equal to the number of solutions of (4) in GF(3^n) $\setminus$ GF(3), where $u = \frac{1}{b}$. We consider the following cases.

Case 1: $n > 1$ is odd. In this case, we already have $N(0) = N(-1) = N(1) = 1$. By Proposition 3, we know that for each $b \in \text{GF}(3^n) \setminus \text{GF}(3)$, $N(b)$ is equal to 0, 1 or 2, and the number of b such that $N(b) = 2$ is equal to $\frac{3^n-3}{2}$. Let ω_i denote the number of $b \in \text{GF}(3^n)$

such that $N(b) = i$, $i \in \{0, 1, 2\}$. By (2), we have

$$\begin{cases} \omega_0 + \omega_1 + \omega_2 = 3^n, \\ \omega_1 + 2\omega_2 = 3^n, \\ \omega_2 = \frac{3^n - 3}{2}. \end{cases}$$

Solving above equation system gives the desired result.

Case 2: $n \geq 2$ and $n \equiv 2 \pmod 4$. Then, $N(b) = 1$ for each $b \in \mathrm{GF}(3)$. By Proposition 3, the possible values of $N(b)$ are 0, 1 or 4 for $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, and the number of $b \in \mathrm{GF}(3^n)$ such that $N(b) = 4$ is $\frac{3^{n-1}-3}{4}$. Similarly, by (2), we have

$$\begin{cases} \omega_0 + \omega_1 + \omega_4 = 3^n, \\ \omega_2 = \omega_3 = 0, \\ \omega_1 + 4\omega_4 = 3^n, \\ \omega_4 = \frac{3^{n-1}-3}{4}, \end{cases}$$

where ω_i is the number of b such that $N(b) = i$, $i \in \{0, 1, \cdots, 4\}$. Solving this equation system, we also get the desired result. Note that when $n = 2$, $w_4 = 0$. Thus, in this case x^d is PN, and its differential spectrum obtained here is in accordance with Proposition 1.

Case 3: $n \equiv 0 \pmod 4$. Then, $N(0) = 1$ and $N(1) = N(-1) = 5$. By Proposition 3, $N(b)$ is equal to 0, 1 and 4 for $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ and $\omega_4 = \frac{3^{n-1}-11}{4}$. Similarly, we have

$$\begin{cases} \omega_0 + \omega_1 + \omega_4 + \omega_5 = 3^n, \\ \omega_1 + 4\omega_4 + 5\omega_5 = 3^n, \\ \omega_2 = \omega_3 = 0, \\ \omega_4 = \frac{3^{n-1}-3}{4}, \\ \omega_5 = 2. \end{cases}$$

Solving the equation above, we obtain the desired result. □

4 Conclusion

In this paper, we conducted a comprehensive investigation on the differential spectrum of x^{p^n-3} for $p = 3$ and settled the open problems in [9]. Nevertheless, the calculation process relies heavily on the characteristic $p = 3$, and we didn't manage to extended the technique to a general odd prime p. It is worth noting that the study of ternary functions with desired cryptographic properties is of practical interest: the IOTA foundation is currently developing new computer chips built around base-3 logic (`https://cryptobriefing.com/iota-new-hash-function/`).

Acknowledgment

Y. Xia and X. Zhang were supported in part by National Natural Science Foundation of China under Grant 61771021, and in part by Natural Science Foundation of Hubei Province under Grant 2017CFB425. The work of C. Li and T. Helleseth was supported by the Research Council of Norway under the grant 247742/O70.

References

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

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Information and 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, Dec. 2011.

[4] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions", *Des. Codes Cryptogr.*, vol .73, pp. 487-505, 2014.

[5] C. Bracken and G. Leander, "A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree," *Finite Fields Appl.*, vol. 16, no. 4, pp. 231-242, 2010.

[6] P. Charpin, G. Kyureghyan, and V. Sunder, "Sparse permutations with low differential uniformity," *Finite Fields Appl.*, vol. 28, pp. 214-243, 2014.

[7] 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.

[8] 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, May 2001.

[9] 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, Mar. 1999.

[10] R. Lidl and H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20. Amsterdam, The Netherlands: Addison-Wesley, 1983.

[11] K. Nyberg, "Differentially uniform mappings for cryptography," In: T. Helleseth (ed.) Advances in cryptology - EUROCRYPT'93. *Lecture Notes in Computer Science*, vol. 765, pp. 55-64. Berlin Heidelberg New York: Springer 1994.

[12] T. Storer, *Cyclotomy and difference sets.* Markham, Chicago, 1967.

[13] K. S. Williams, "Note on cubics over GF(2^n) and GF(3^n)," *Journal of Number Theory*, vol. 7, no. 4, pp. 361-365, Nov. 1975.

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

[15] M. Xiong, H. Yan, and P. Yuan,"On a conjecture of differenially 8-uniform power functions," *Des. Codes Cryptogr.*, vol. 86, pp. 1601-1621, 2018.

[16] H. Yan, Z. Zhou, J. Weng, J. Wen, 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, Oct. 2019.