Differential spectra of a class of power permutations with Niho exponents

Zhen Li and Haode Yan*

School of Mathematics, Southwest Jiaotong University
Chengdu, 611756, China

(Communicated by Sihem Mesnager)

Abstract. Let $m \geq 3$ be a positive integer and $n = 2^m$. Let $f(x) = x^{2^m+3}$ be a power permutation over $\text{GF}(2^n)$, which is a monomial with a Niho exponent. In this paper, the differential spectrum of $f$ is investigated. It is shown that the differential spectrum of $f$ is $S = \{\omega_0 = 2^{2^m-1} + 2^m - 1, \omega_2 = 2^{2^m-2} + 2^{m-1}, \omega_4 = 2^{2^m-3} - 2^{m-1}, \omega_6 = 1\}$ when $m$ is even, and $S = \{\omega_0 = 7 \cdot 2^{2^m-2} + 2^m, \omega_2 = 3 \cdot 2^{2^m-3} - 2^{m-2} - 1, \omega_6 = 2^{2^m-3} - 2^{m-2}, \omega_8 = 1\}$ when $m$ is odd.

1. Introduction

Let $n$ be a positive integer. Denote by $\text{GF}(2^n)$ the finite field with $2^n$ elements. For any function $f : \text{GF}(2^n) \to \text{GF}(2^n)$, the derivative of $f$ with respect to any given $a \in \text{GF}(2^n)$ is a function from $\text{GF}(2^n)$ to $\text{GF}(2^n)$ defined by $D_a f(x) = f(x + a) + f(x), \forall x \in \text{GF}(2^n)$. For any $a, b \in \text{GF}(2^n)$, we denote $\delta(a, b) = \#\{x \in \text{GF}(2^n) \mid D_a f(x) = b\}$, where $\#S$ denotes the cardinality of the set $S$. The differential uniformity of $f$ is defined as $\delta = \max_{a \neq 0, b \in \text{GF}(2^n)} \delta(a, b)$, and $f$ is said to be differentially $\delta$-uniform [16]. Obviously, the solutions of $D_a f(x) = b$ come in pairs ( if $x$ is a solution, then $x + a$ is also a solution), thus $\delta$ is even. In particular, the function $f$ with the lowest differential uniformity $\delta = 2$ is called an almost perfect nonlinear (APN) function. The known results on APN functions can be found in [6, 8, 16, 17].

Differential uniformity is an important concept in cryptography as it quantifies the degree of security of the Substitution box (S-box) used in the cipher with respect to differential attacks [1]. Power permutations with low differential uniformity serve as good candidates for the design of S-boxes, not only because of their strong resistance to differential attacks, but also for the usually low implementation cost.
in hardware. It is worthwhile to study power permutations with low differential uniformity as it provides better resistance towards differential cryptanalysis [16]. For example, the well known AES (advanced encryption standard) [7] employs a differentially 4-uniform power permutation which is extended affine equivalent to the inverse function $x \mapsto x^{-1}$ over $GF(2^n)$, where $n > 0$ is an even integer.

When $f(x) = x^d$ is a power function over $GF(2^n)$, it is easy to see that $\delta(a, b) = \delta(1, \frac{b}{a^n})$ for any $a \in GF(2^n) \setminus \{0\} := GF(2^n)^*$. This implies that the differential properties of $f(x)$ is completely determined by the values of $\delta(1, b)$ as $b$ runs through $GF(2^n)$. From now on, we use the convention $\delta(b) = \delta(1, b)$. The differential spectrum is defined as follows.

**Definition 1.1** ([2]). Let $f(x) = x^d$ be a power function over $GF(2^n)$ with differential uniformity $\delta$. Denote

$$\omega_i = \# \{ b \in GF(2^n) \mid \delta(b) = i \},$$

where $0 \leq i \leq \delta$. The differential spectrum of $f$ is defined to be the collection of $\omega_i$

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

If needed, we exclude the zeroes from $S$. Moreover, the differential spectrum of $f$ over $GF(2^n)$ satisfies the following two identities (see Proposition 7 in [2])

$$\sum_{i=0}^{\delta} \omega_i = \sum_{i=0}^{\delta} i \omega_i = 2^n. \tag{1}$$

The identities in (1) are very useful for computing the differential spectrum of $f$. If $f(x)$ is an APN function, then the nonzero elements in the differential spectrum are $\omega_0$ and $\omega_2$. By (1), we obtain that all APN functions have the same differential spectrum

$$S = \{ \omega_0 = 2^{n-1}, \omega_2 = 2^{n-1} \}.$$

As noted in [2], the entire differential spectrum of an S-box is useful for analysing the resistance of the cipher against differential attacks and its invariants. For example, the inverse function $x^{-1}$ over $GF(2^n)$ with even $n$ has the best resistance to differential cryptanalysis for 4-uniform S-boxes, since the differential spectrum of $x^{-1}$ is $S = \{ \omega_0 = 2^{n-1} + 1, \omega_2 = 2^{n-1} - 2, \omega_4 = 1 \}$, which offers the lowest value of $\omega_4$ among all the differentially 4-uniform functions [2]. Inspired by this pioneering work, the differential spectra of a few infinite families of power mappings over $GF(2^n)$ were determined. In [2], Blondeau et al. studied the differential spectra of several power mappings over $GF(2^n)$, such as quadratic power mappings, Kasami power mappings and Bracken-Leander power mappings. They also presented some conjectures, one of which was proved by Xiong et al. [20]. In [3] and [4], the authors investigated the differential properties of the power mappings $x^{2^t-1}$ over $GF(2^n)$ and determined their differential spectra for certain $t$. Very recently, Li et al. determined the differential spectrum of the power mapping $x^{2^{n/4} + 2^{n/2} + 2^{n/4} - 1}$ over $GF(2^n)$ with $4 \mid n$ [13]. We list the power mappings over $GF(2^n)$ with known differential spectra in Table 1.

Let $n$ and $m$ be positive integers with $n = 2m$. A positive integer $d$ is called a **Niho exponent** with respect to the finite field $GF(2^n)$ if $d \equiv 2^j \pmod{2^n - 1}$ for some nonnegative integer $j$, which was first reported in the study of cross-correlation functions between an $m$-sequence and its decimated sequence [15]. Niho exponents are widely used in cryptography, coding theory, and sequence designs (see
Table 1. Power functions $f(x) = x^d$ over GF($2^n$) with known differential spectra

| $d$           | Conditions                      | $\delta_f$ | Reference |
|---------------|---------------------------------|------------|-----------|
| $2^n - 2$     | $n$ is even                     | 4          | [2]       |
| $2^{2t} - 2^t + 1$ | $\gcd(t, n) = 2$            | 4          | [2]       |
| $2^t + 1$     | $\gcd(t, n) = 2$               | 4          | [2]       |
| $2^{n/2} + 2^{n/4} + 1$ | $4 \mid n$               | 4          | [2, 19]  |
| $2^{n/2} - 1$; | $n \geq 6$ is even             | $2^{n/2} - 2$ | [3]       |
| $2^{n/2 + 1} - 1$; | $t = 3, n - 2$               | 6          | [3]       |
| $2^t - 1$     | $t = (n - 1)/2$, $n$ is odd   | 6 or 8    | [4]       |
| $2^{n/2} + 2^{(n+2)/4} + 1$; | $n \equiv 2 \pmod{4}$, $n \geq 10$ | 8          | [20]      |
| $2^{n/2 + 1} + 3$ | $4 \mid n$               | $2^{n/2}$  | [13]      |
| $2^{3n/4} + 2^{n/2} + 2^{n/4} - 1$ | $n \geq 6$ is even | $2^{n/2}$ or $2^{n/2} + 2$ | This paper |

[5, 11, 12, 18]). Related results can be found in a recent survey [14]. However, the differential properties of some power functions with Niho exponents are unknown. In this paper, we focus on the differential properties of a class of power permutations with Niho exponents. Throughout this paper, let $f(x) = x^d$ be a power permutation over the finite fields GF($2^n$), where $n = 2m \geq 6$ and $d = 2^n + 3$ is a Niho exponent. This kind of Niho exponents was firstly studied by Niho [15], offering at most five-valued cross-correlation functions between $m$-sequence and its decimated sequence. After 4 years, Helleseth found the value distribution of this cross-correlation function [9]. The differential uniformity and the differential spectrum of $f$ are determined in this paper.

The rest of this paper is organized as follows. In Section 2, we introduce the relationship between the differential spectrum of power permutation $f$ and the Walsh spectrum of a related Boolean function. The differential spectrum of $f$ is determined in Section 3. We give some concluding remarks in Section 4.

2. Preliminaries

In this section, we will show the relationship between the differential spectrum of power permutation $x^d$ and the Walsh spectrum of the Boolean function $F : x \mapsto \text{Tr}_1^n(x^d)$ over GF($2^n$), where $\text{Tr}_1^n(y) = \sum_{t=0}^{n-1} y^{2^t}$ is the absolute trace mapping from GF($2^n$) to GF(2).

Let $d$ be a positive integer with $\gcd(d, 2^n - 1) = 1$. For $a \in$ GF($2^n$) we define the following exponential sum

$$W_d(a) = \sum_{x \in \text{GF}(2^n)} (-1)^{\text{Tr}_1^n(x^d + ax)}.$$
The Walsh spectrum of Boolean function $F: x \mapsto \text{Tr}^n_1(x^d)$ over $\mathbb{GF}(2^n)$ is defined as the collection of values $W_d(a)$ as $a$ runs through $\mathbb{GF}(2^n)$, i.e.,

$$W_F = \{ W_d(a) \mid a \in \mathbb{GF}(2^n) \}.$$ 

Moreover, the following lemma can be easily deduced by Theorem 10 in [10].

**Lemma 2.1.** Let $x^d$ be a differentially $\delta$-uniform power permutation with the differential spectrum $\mathbb{S} = \{ \omega_0, \omega_1, \cdots, \omega_{\delta} \}$. We have

$$\sum_{a \in \mathbb{GF}(2^n)} (W_d(a))^4 = 2^{2n} \sum_{i=0}^{\delta} i^2 \omega_i. \tag{2}$$

**Proof.** Recall that $\delta(u, v) = \# \{ x \in \mathbb{GF}(2^n) \mid (x + u)^d + x^d = v \}$, where $u$ and $v \in \mathbb{GF}(2^n)$. Obviously we have

$$\delta(0, v) = \begin{cases} 
2^n, & v = 0, \\
0, & v \neq 0.
\end{cases}$$

Observing that for arbitrary but fixed $u \in \mathbb{GF}(2^n)^*$, one has

$$\{ \delta(v) \mid v \in \mathbb{GF}(2^n) \} = \{ \delta(u, v) \mid v \in \mathbb{GF}(2^n) \}.$$

Therefore, we assert that

$$\sum_{u, v \in \mathbb{GF}(2^n)} (\delta(u, v))^2 = 2^{2n} + \sum_{u \neq 0, v \in \mathbb{GF}(2^n)} (\delta(u, v))^2,$$ 

which equivalently becomes

$$\sum_{u, v \in \mathbb{GF}(2^n)} (\delta(u, v))^2 = 2^{2n} + (2^n - 1) \sum_{v \in \mathbb{GF}(2^n)} (\delta(v))^2. \tag{3}$$

Let $\theta_d(\lambda, a) = \sum_{x \in \mathbb{GF}(2^n)} (-1)^{\text{Tr}^n_1(\lambda x^d + ax)}$ for any $\lambda, a \in \mathbb{GF}(2^n)$. Then

$$\theta_d(0, a) = \begin{cases} 
2^n, & a = 0, \\
0, & a \neq 0.
\end{cases}$$

Noting that $\gcd(d, 2^n - 1) = 1$, then for arbitrary but fixed $\lambda \in \mathbb{GF}(2^n)^*$ one has

$$\{ W_d(a) \mid a \in \mathbb{GF}(2^n) \} = \{ \theta_d(\lambda, a) \mid a \in \mathbb{GF}(2^n) \},$$

which implies that

$$\sum_{\lambda, a \in \mathbb{GF}(2^n)} (\theta_d(\lambda, a))^4 = 2^{4n} + (2^n - 1) \sum_{a \in \mathbb{GF}(2^n)} (W_d(a))^4. \tag{4}$$

By the Theorem 10 in [10], we have

$$\sum_{\lambda, a \in \mathbb{GF}(2^n)} (\theta_d(\lambda, a))^4 = 2^{2n} \sum_{u, v \in \mathbb{GF}(2^n)} (\delta(u, v))^2. \tag{5}$$

Combining with the equalities (3) and (4), the desired result follows. \[\square\]

From now on, let $f(x) = x^d$ be a power mapping over $\mathbb{GF}(2^n)$, where $n = 2m \geq 6$ and $d = 2^n + 3$ is a Niho exponent. As we mentioned before, the Walsh spectrum of $f$ was determined in [9] as follows.
Lemma 2.2 ([9]). The Walsh spectrum of the $f$ is given by

$$\mathcal{W}_f = \begin{cases} 
3 \cdot 2^m, & \text{occurs } \frac{1}{3} \left( 2^{2m-3} + 2^{m-3}((-1)^{m+1} + 1) - 2^{m-1} \right) \text{ times,} \\
2 \cdot 2^m, & \text{occurs } 2^{m-1} \text{ times,} \\
2^m, & \text{occurs } 2^{2m-1} - 2^{2m-2} - 2^{m-2}((-1)^{m+1} + 1) \text{ times,} \\
0, & \text{occurs } \frac{1}{3} \left( 2^{2m} + 2^m((-1)^{m+1} + 1) + 2^{m-1} \right) \text{ times,} \\
-2^m, & \text{occurs } 2^{2m-1} - 2^{2m-3} - 2^{m-3}((-1)^{m+1} + 1) - 2^{m-1} \text{ times.}
\end{cases}$$

We immediately deduce the following corollary by Lemmas 2.1 and 2.2.

Corollary 1. With the notation introduced before, the differential spectrum of $f(x)$ satisfies

$$\sum i^2 \omega_i = \begin{cases} 
2^{2m+2} - 2^{m+2} - 2^{m+1}, & \text{if } m \text{ is even,} \\
2^{2m+2}, & \text{if } m \text{ is odd.}
\end{cases}$$

3. The differential spectrum of $f(x) = x^{2^m+3}$

To determine the differential spectrum of $f$, we will consider the differential equation of the form

$$(x + 1)^{2^m+3} + x^{2^m+3} = b$$

for $b \in \text{GF}(2^n)$. Recall that $\delta(b)$ denotes the number of solutions of (6) in $\text{GF}(2^n)$. Firstly, we determine the values of $\delta(0)$ and $\delta(1)$.

Lemma 3.1. We have

(1): $\delta(0) = 0$;
(2): $\delta(1) = \begin{cases} 
2^m, & \text{if } m \text{ is even,} \\
2^m + 2, & \text{if } m \text{ is odd.}
\end{cases}$

Proof. When $b = 0$, the differential equation

$$(x + 1)^{2^m+3} + x^{2^m+3} = 0$$

has no solution since $\text{gcd}(2^m + 3, 2^m - 1) = 1$. Thus, $\delta(0) = 0$. Now we assume that $b = 1$. Then the equation (6) becomes

$$(x^{2^m} + x)(x^2 + x + 1) = 0,$$

which gives that $x^{2^m} + x = 0$ or $x^2 + x + 1 = 0$. They have solutions $\text{GF}(2^m)$, $\omega$ and $\omega^2$, where $\omega$ is a primitive element in $\text{GF}(2^2)$. If $m$ is even, $\text{GF}(2^2) \subseteq \text{GF}(2^m)$ and subsequently equation (7) has exactly $2^m$ distinct solutions in $\text{GF}(2^m)$. If $m$ is odd and thus $w, w^2 \notin \text{GF}(2^m)$. Hence, (7) has exactly $2^m + 2$ distinct solutions in $\text{GF}(2^m)$. This completes the proof. \hfill $\square$

Let us now consider the values of $\delta(b)$ for $b \in \text{GF}(2^n) \setminus \{0, 1\}$. We observe the following.

Lemma 3.2. For any $b \in \text{GF}(2^n) \setminus \{0, 1\}$, we have

(1): $\delta(b) \leq 6$,
(2): $\delta(b) \neq 6$ when $m$ is even and $\delta(b) \neq 4$ when $m$ is odd.

Proof. For any $b \in \text{GF}(2^n) \setminus \{0, 1\}$, the equation (6) becomes

$$(x^{2^m} + x)(x^2 + x + 1) = b + 1.$$
Raising to the $2^m$-th power on each side of equation (8), we have that
\begin{equation}
(x^{2^m} + x)(x^{2^m+1} + x^{2^m} + 1) = b^{2^m} + 1.
\end{equation}

By summing (8) and (9), we obtain
\begin{equation}
\sum_{i=0}^{m-1} (x^i + x^{i+1}) = \sum_{i=0}^{m-1} (1 + u_x^{-1}(b+1))^2^i = m + \sum_{i=0}^{m-1} (u_x^{-1}(b+1))2^i.
\end{equation}

It is easy to note that $u_x$ contributes two solutions of (11) if and only if
\begin{equation}
u_x = m + \sum_{i=0}^{m-1} (u_x^{-1}(b+1))2^i.
\end{equation}

Let us now prove the second statement of Lemma 3.2. For an arbitrary but fixed $b \in \text{GF}(2^n) \setminus \{0,1\}$ suppose that (10) has three distinct nonzero solutions in $\text{GF}(2^n)$, namely $u_{x_1}, u_{x_2}$ and $u_{x_3}$.

If each $u_{x_j} (j = 1, 2, 3)$ contributes exactly two solutions by (11), then $u_{x_j}$ satisfies (12). By summing these three identities, we obtain that
\begin{equation}
u_{x_1} + u_{x_2} + u_{x_3} = m + \sum_{i=0}^{m-1} ((u_{x_1}^{-1} + u_{x_2}^{-1} + u_{x_3}^{-1})(b+1))2^i.
\end{equation}

Since $u_{x_1}, u_{x_2}$ and $u_{x_3}$ are solutions of (10), we have
\begin{equation}u_{x_1} + u_{x_2} + u_{x_3} = 1,
\end{equation}

and
\begin{equation}u_{x_1}^{-1} + u_{x_2}^{-1} + u_{x_3}^{-1} = \frac{u_{x_1}u_{x_2} + u_{x_2}u_{x_3} + u_{x_1}u_{x_3}}{u_{x_1}u_{x_2}u_{x_3}} = 0.
\end{equation}

Then (13) becomes $m = 1$. If $m$ is even, (13) cannot hold. This implies that $u_{x_1}, u_{x_2}$ and $u_{x_3}$ cannot give two solutions simultaneously, i.e., $\delta(b) \leq 4$ for any $b \in \text{GF}(2^n) \setminus \{0,1\}$. If $m$ is odd, (13) is always satisfied. This implies that if any two of $\{u_{x_1}, u_{x_2}, u_{x_3}\}$ give two solutions, then all three of them contribute exactly two solutions to (11), i.e., $\delta(b) \neq 4$ for any $b \in \text{GF}(2^n) \setminus \{0,1\}$. This completes the proof.

Now we are ready to determine the differential spectrum of $f$. By Lemmas 3.1 and 3.2, when $m$ is even, $\omega_{2^m} = 1$, the remaining nonzero elements in the differential spectrum are $\omega_0, \omega_2, \omega_4$. When $m$ is odd, $\omega_{2^m+2} = 1$, the remaining nonzero elements in the differential spectrum are $\omega_0, \omega_2, \omega_6$. We now present the main result of the paper.
Theorem 3.3. Let \( f(x) = x^{2m+3} \) be a power function over \( \text{GF}(2^n) \), where \( n = 2m \) is an even integer with \( m \geq 3 \). The differential spectrum of \( f \) is
\[
S = \{ \omega_0 = 2^{2m-1} + 2^{2m-3} - 1, \omega_2 = 2^{2m-2} + 2^{m-1}, \\
\omega_4 = 2^{2m-3} - 2^{m-1}, \omega_{2m} = 1 \}
\]
if \( m \) is even, and
\[
S = \{ \omega_0 = \frac{7 \cdot 2^{2m-2} + 2^m}{3}, \omega_2 = 3 \cdot 2^{2m-3} - 2^{m-2} - 1, \\
\omega_6 = \frac{2^{2m-3} - 2^{m-2}}{3}, \omega_{2m+2} = 1 \}
\]
if \( m \) is odd.

Proof. By (1) and Corollary 1, we have that \( \omega_0, \omega_2 \) and \( \omega_4 \) satisfy the following system of equations
\[
\begin{align*}
\omega_0 + \omega_2 + \omega_4 + 1 &= 2^{2m} \\
2\omega_2 + 4\omega_4 + 2^m &= 2^{2m} \\
4\omega_2 + 16\omega_4 + 2^{2m} &= 2^{2m+2} - 2^m - 2^m + 1
\end{align*}
\]
when \( m \) is even, and \( \omega_0, \omega_2 \) and \( \omega_6 \) satisfy the following system of equations
\[
\begin{align*}
\omega_0 + \omega_2 + \omega_6 + 1 &= 2^{2m} \\
2\omega_2 + 6\omega_6 + 2^m + 2 &= 2^{2m} \\
4\omega_2 + 36\omega_6 + (2^m + 2)^2 &= 2^{2m+2}
\end{align*}
\]
when \( m \) is odd. The solutions to the above two systems are exactly the differential spectrum of \( f \) for, respectively, \( m \) even and odd. This completes the proof.

The computational results obtained by the algebra system Magma are consistent with the results in Theorem 3.3 and are listed in the following table:

| \( n \) | \( d = 2^{n/2} + 3 \) | Differential spectra |
|---|---|---|
| 8 | \( d = 19 \) | \( S = \{ \omega_0 = 159, \omega_2 = 72, \omega_4 = 24, \omega_{16} = 1 \} \) |
| 10 | \( d = 35 \) | \( S = \{ \omega_0 = 608, \omega_2 = 375, \omega_6 = 40, \omega_{34} = 1 \} \) |
| 12 | \( d = 67 \) | \( S = \{ \omega_0 = 2559, \omega_2 = 1056, \omega_4 = 480, \omega_{64} = 1 \} \) |
| 14 | \( d = 131 \) | \( S = \{ \omega_0 = 9600, \omega_2 = 6111, \omega_6 = 672, \omega_{130} = 1 \} \) |

4. Concluding remarks

In this paper, we computed the differential spectrum of \( f(x) = x^d \) over \( \text{GF}(2^n) \) with even \( n \geq 6 \), where \( d = 2^{n/2} + 3 \) is a Niho exponent. The main result implies that the equation \((x + 1)^d + x^d = b\) has only a few solutions when \( b \in \text{GF}(2^n) \) \( \setminus \{0, 1\} \). It would be interesting to study the differential spectra of functions with other Niho exponents in finite fields of both even and odd characteristic. It would be also of interest to find the applications of differential spectra of functions with Niho exponents in sequence designs, coding theory and combinatorial designs.
References

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

[2] C. Blondeau, A. Canteaut and P. Charpin, Differential properties of power functions, *Int. J. Inf. Coding Theory*, 1 (2010), 149–170.

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

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

[5] P. Charpin, Cyclic codes with few weights and Niho exponents, *J. Combinat. Theory. Ser. A.*, 108 (2004), 247–259.

[6] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case, *Inform. and Comput.*, 151 (1999), 57–72.

[7] J. Daemen and V. Rijmen, *The Design of Rijndael: AES- The Advanced Encryption Standard*, Springer-Verlag, Berlin, 2002.

[8] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case, *IEEE Trans. Inf. Theory.*, 45 (1999), 1271–1275.

[9] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.*, 16 (1976), 209–232.

[10] T. Helleseth, C. Rong and D. Sandberg, New families of almost perfect nonlinear power mappings, *IEEE Trans. Inf. Theory.*, 45 (1999), 474–485.

[11] H. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary $m$-sequences, *Finite Fields Appl.*, 7 (2001), 253–286.

[12] N. Li, T. Helleseth, A. Kholosha and X. Tang, On the walsh transform of a class of functions from Niho exponents, *IEEE Trans. Inf. Theory.*, 59 (2013), 4662–4667.

[13] N. Li, Y. Wu, X. Zeng and X. Tang, On the differential spectrum of a class of power functions over finite fields, *Computer Science*, 2020, arXiv:2012.04316v1.

[14] N. Li and X. Zeng, A survey on the applications of Niho exponents, *Cryptogr. Commun.*, 11 (2019), 509–548.

[15] Y. Niho, *Multivalued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequence*, PhD Thesis, Univ. of Southern California, Los Angle, 1972.

[16] K. Nyberg, Differentially uniform mappings for cryptography, *Advances in Cryptology–EUROCRYPT’93*, 765 (1993), 55–64.

[17] A. Pott, Almost perfect and planar functions, *Des. Codes Cryptogr.*, 78 (2016), 141–195.

[18] M. Xiong, N. Li, Z. Zhou and C. Ding, Weight distribution of cyclic codes with arbitrary number of generalized Niho type zeroes, *Des. Codes Cryptogr.*, 78 (2016), 713–730.

[19] M. Xiong and H. Yan, A note on the differential spectrum of a 4-uniform power function, *Finite Fields and Appl.*, 48 (2017), 117–125.

[20] M. Xiong, H. Yan and P. Yuan, On a conjecture of differentially 8-uniform power function, *Des. Codes Cryptogr.*, 86 (2018), 1601–1621.

Received August 2021; revised October 2021; early access December 2021.

E-mail address:lz-math@my.swjtu.edu.cn
E-mail address:hdyan@swjtu.edu.cn