PAPER

New Classes of Permutation Quadrinomials Over $\mathbb{F}_{q^3}$

Changhui CHEN[†a)], ***Nonmember***, **Haibin KAN**[††,†††,††††b)], ***Member***, **Jie PENG**[†c)], ***and*** **Li WANG**[†d)], ***Nonmembers***

SUMMARY Permutation polynomials have been studied for a long time and have important applications in cryptography, coding theory and combinatorial designs. In this paper, by means of the multivariate method and the resultant, we propose four new classes of permutation quadrinomials over $\mathbb{F}_{q^3}$, where q is a prime power. We also show that they are not quasi-multiplicative equivalent to known ones. Moreover, we compare their differential uniformity with that of some known classes of permutation trinomials for some small q.

key words: *finite field, cryptography, permutation quadrinomial, resultant, quasi-multiplicative equivalence*

1. Introduction

In this paper, let m be a positive integer, p be a prime and $q = p^m$. Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ be the set of nonzero elements of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a permutation polynomial over $\mathbb{F}_q$ if the associated mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a bijection. Permutation polynomials over finite fields have important applications in many areas of science and engineering such as coding theory, combinatorial designs and cryptography [11]. For instance, in many block ciphers, permutations defined on $\mathbb{F}_{2^m}$ with low differential uniformity are utilized as their S-boxes to provide confusion. Permutation polynomials can also be employed to construct bent functions of the Maiorana-McFarland class, with the form of $f(x, y) = \mathrm{Tr}_m(x \cdot \pi(y) + g(y)) \in \mathbb{F}_{2^m}^2[x, y]$, where π is any permutation over $\mathbb{F}_{2^m}$. More details on properties and applications of permutation polynomials can be found in [8]–[10].

Permutation polynomials with few terms have attracted much attention for their simple algebraic forms. For example, Ding [3] presented novel cyclic codes by using permutation monomials and permutation trinomials. For a monomial x^n, a necessary and sufficient condition for it to permute $\mathbb{F}_q$ is given by $\gcd(n, q-1) = 1$. However, the characterization of permutation binomials and permutation trinomials is much more complicated, we refer to [1], [5], [6], [12], [16], [23]–[25] for more details. Theoretically speaking, the total number of permutation polynomials over $\mathbb{F}_q$ is large. However, it is hard to construct permutation polynomials with a simple algebraic form and some additional extraordinary properties explicitly [7]. In order to solve the Big APN (Almost Perfect Nonlinear) Problem on the existence of APN permutations over $\mathbb{F}_{2^n}$ when $n \geq 8$ is even, Pasalic and Charpin investigated the existence of permutation polynomials of the form $f(x) = x^d + L(x)$ over $\mathbb{F}_{2^n}$ [15]. Motivated by their works, Li and Wang [11] studied permutation polynomials over $\mathbb{F}_{2^n}$ with the form of

$$f(x) = x^{2^i+1} + L(x), \tag{1}$$

where $\gcd(i, n) = 1$ and $L(x)$ is a linearized polynomial. They proved that $x^{2^i+1} + L(x)$ permutes $\mathbb{F}_{2^n}$ if and only if n is odd and $L(x) = a^{2^i}x + ax^{2^i}$, where $a \in \mathbb{F}_{2^n}$. Then Gong et al. [4] investigated permutation polynomials of the form (1) with $\gcd(i, n) > 1$. In 2021, Pang et al. [16] constructed six classes of permutation trinomials over $\mathbb{F}_{2^{3m}}$ with the form $x^d + L(x^s)$ by choosing some suitable integers d, s and linearized polynomials $L(x)$. Very recently, Gupta et al. [5] presented two classes of permutation trinomials of the form $x + Ax^{2^{2m}-2^m+1} + x^{2^{2m}+2^m-1}$ and $x + Ax^{2^{3m}-2^{2m}+2^m} + x^{2^{2m}+2^m-1}$ over $\mathbb{F}_{2^{3m}}$, and a class of permutation trinomials of the form $x + Ax^{q^2-q+1} + A^2x^{q^2}$ over $\mathbb{F}_{p^{3m}}$, where p is odd.

Dobbertin [2] employed the multivariate method to verify the permutation property of particular types of polynomials over finite fields with even characteristics. In addition, the authors in [1], [5], [16], [25] utilized the resultant and the multivariate method to investigate permutation polynomials over finite fields. In this paper, we propose four classes of permutation quadrinomials over $\mathbb{F}_{q^3}$ by the multivariate method and the resultant of two polynomials. More explicitly, there are two classes of permutation polynomials over $\mathbb{F}_{q^3}$ of the form $x + x^q + \xi x^{q^2-q+1} + x^{q^2+q-1}$ and $x + x^q + x^{q^2} + \xi x^{q^2-q+1}$ with $p = 2$, together with another two classes of the form $x \pm x^q + x^{q^2} + x^{q^2-q+1}$ with p being odd. We also show the quasi-multiplicative equivalence between the presented permutation polynomials in this paper and the known ones. Moreover, we compare the differential uniformity of ours permutations with that of some known permutation trinomi-

Manuscript received September 12, 2023.
Manuscript revised November 26, 2023.
Manuscript publicized December 27, 2023.

[†] Mathematics and Science College, Shanghai Normal University, Guilin Road #100, Shanghai, 200234, China.

[††] Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China.

[†††] Shanghai Engineering Research Center of Blockchain, Shanghai 200433, China.

[††††] Yiwu Research Institute, Fudan University, Yiwu, Zhejiang 322000, China.

a) E-mail: cchxuexi@126.com
b) E-mail: hbkan@fudan.edu.cn
c) E-mail: jpeng@shnu.edu.cn
d) E-mail: wlmath@shnu.edu.cn

DOI: 10.1587/transfun.2023EAP1113

als over $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{3^6}$, respectively.

The remainder of the paper is organized as follows. Section 2 provides the definitions of the resultant of two polynomials and quasi-multiplicative (QM) equivalence. In Sect. 3, we present four classes of permutation quadrinomials over $\mathbb{F}_{q^3}$. In Sect. 4, we show that the classes of permutation quadrinomials presented in this paper are QM inequivalent to known ones. In Sect. 5, with the help of the computer software, we compare the differential uniformity of our permutation quadrinomials with that of some konwn permutation trinomials. Finally, Sect. 6 concludes this paper.

2. Preliminaries

The resultant of two polynomials is a useful tool for determining whether two polynomials have a common root or not.

Definition 2.1: [5] Let $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$, $g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n \in \mathbb{F}_q[x]$ be two polynomials of positive degree m and n, respectively. Then the resultant of f and g with respect to x is defined by the determinant

$$R(f,g,x) = \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_m \\ b_0 & b_1 & \cdots & \cdots & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_n & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_n \end{vmatrix}$$

of order $m + n$.

It is well known that f and g have at least one common root if and only if $R(f, g, x) = 0$.

It is well known that, when $f(x)$ is a permutation polynomial and $g(x)$ is quasi-multiplicative equivalent to $f(x)$, then $g(x)$ is also a permutation polynomial.

Definition 2.2: [18] Two permutation polynomials $f(x)$ and $g(x)$ over $\mathbb{F}_q[x]$ are called quasi-multiplicative (QM) equivalent, if there exists an integer $1 \le r \le q-2$ such that $\gcd(r, q-1) = 1$ and $f(x) = c_2 g(c_1 x^r)$, where $c_1, c_2 \in \mathbb{F}_q^*$.

Definition 2.3: Let $f(x) \in \mathbb{F}_q[x]$. If for any $a \in \mathbb{F}_q^*$ and any $b \in \mathbb{F}_q$, the equation $f(x) - f(x+a) = b$ has at most δ solutions in $\mathbb{F}_q$, then $f(x)$ is called differentially δ-uniform.

The S-boxes used in block ciphers should have a low differential uniformity to allow a good resistance to differential attack.

3. Main Results

In this section, we construct four classes of permutation quadrinomials over $\mathbb{F}_{q^3}$.

3.1 The Case $p = 2$

In the following, two classes of permutation quadrinomials with coefficients in $\mathbb{F}_{2^2}$ are given.

Theorem 3.1: Let $q = 2^m$ with $m \not\equiv 1 \pmod 3$ be even and ξ be a primitive element of $\mathbb{F}_{2^2}$. Then $f(x) = x + x^q + \xi x^{q^2-q+1} + x^{q^2+q-1}$ is a permutation polynomial over $\mathbb{F}_{q^3}$.

Proof: In order to prove that $f(x)$ permutes $\mathbb{F}_{q^3}$, it suffices to verify that for any $a \in \mathbb{F}_{q^3}$, $f(x) = a$ has at most one solution in $\mathbb{F}_{q^3}$. We first show that $f(x) = 0$ has a unique solution $x = 0$ in $\mathbb{F}_{q^3}$. Assume that there exists some $x \in \mathbb{F}_{q^3}^*$ such that $f(x) = 0$, then we have

$$1 + x^{q-1} + \xi x^{q^2-q} + x^{q^2+q-2} = 0.$$

Let $u = x^{q-1}$, then it becomes

$$1 + u + \xi u^q + u^{q+2} = 0. \qquad (2)$$

If $\xi + u^2 = 0$, then (2) gives $u = 1$, a contradiction. Hence $\xi + u^2 \neq 0$, and (2) yields $u^q = \frac{u+1}{\xi+u^2}$ and $u^{q^2} = \frac{(\xi+u^2)(\xi^2+u^2+u)}{\xi u^4+u^2}$. Thus we have

$$1 = x^{q^3-1} = u^{q^2+q+1} = \frac{(u+1)(\xi^2+u^2+u)}{\xi u^3+u},$$

which can be rearranged as

$$u^3 + u + 1 = 0 \qquad (3)$$

by using $\xi^2 + \xi + 1 = 0$. So it holds $u^7 = 1$. If $m \equiv 0 \pmod 3$, then $q \equiv 1 \pmod 7$, so that $u^q = u$. Hence we have $u^{q^2+q+1} = u^3 = 1$, and thus $u^{\gcd(7,3)} = u = 1$, which contradicts to (3). If $m \equiv 2 \pmod 3$, then $q \equiv 4 \pmod 7$, so that $u^q = u^4$. Then from (2) we have

$$u^6 + \xi u^4 + u + 1 = 0.$$

Since $u + 1 = u^3$ from (3), then the above equation becomes $u^6 + \xi u^4 + u^3 = 0$, and thus $0 = u^3 + \xi u + 1 = \xi u + u = \xi^2 u$, which is a contradiction.

Below assume that $a \in \mathbb{F}_{q^3}^*$ and we show that

$$f(x) = x + x^q + \xi x^{q^2-q+1} + x^{q^2+q-1} = a \qquad (4)$$

has at most one solution in $\mathbb{F}_{q^3}^*$. Let $y = x^q$, $z = y^q$, $b = a^q$ and $c = b^q$. Then we can get the following system of equations

$$\begin{cases} x + y + \frac{\xi xz}{y} + \frac{yz}{x} = a \\ y + z + \frac{\xi yx}{z} + \frac{xz}{y} = b \\ z + x + \frac{\xi zy}{x} + \frac{xy}{z} = c. \end{cases} \qquad (5)$$

Let $u = \frac{yz}{x}, v = \frac{xz}{y}$, and $w = \frac{xy}{z}$. Then it is clear that

$$\begin{cases} x^2 = vw, \\ y^2 = uw, \\ z^2 = uv. \end{cases}$$

Therefore, squaring both sides of each equation of (5) gives

$$\begin{cases} u^2+\xi^2v^2+vw+uw=a^2\\ v^2+\xi^2w^2+wu+vu=b^2\\ w^2+\xi^2u^2+uv+wv=c^2. \end{cases} \tag{6}$$

Adding these equations together, one obtains that $u^2+v^2+w^2=\xi^2(a^2+b^2+c^2)$, and thus

$$u+v+w=\xi(a+b+c).$$

Let $t=\xi(a+b+c)\in\mathbb{F}_q$. If $t=0$, then $u+v+w=0$, which implies that $u=\xi c$, $v=\xi a$ and $w=\xi b$ by (6). Thus, we obtain that $x=(vw)^{\frac{1}{2}}=\xi(ab)^{\frac{1}{2}}$, which is the unique solution of (4). If $t\neq 0$, we can have

$$\begin{cases} v^2+\xi^2tu+\xi^2tv=\xi^2a^2\\ u^2+v^2+\xi^2tu+\xi t^2=\xi^2b^2 \end{cases} \tag{7}$$

from (6). By adding above two equations together, we have

$$u^2+\xi^2tv+\xi t^2+\xi^2a^2+\xi^2b^2=0. \tag{8}$$

Eliminating the indeterminate v from the second equation of (7) and Eq. (8), we get that

$$u^4+\xi t^2u^2+t^3u+t^2b^2+\xi a^4+\xi b^4=0. \tag{9}$$

Recall that $v=u^q$ and $t\in\mathbb{F}_q$, and replace u by ξtu in the second equation of (7) and Eq. (9), one has

$$\begin{cases} u^{2q}+u^2+\xi u=c_1,\\ \xi u^4+u^2+\xi u=c_2, \end{cases} \tag{10}$$

where $c_1=(\frac{b+\xi t}{t})^2$ and $c_2=\frac{t^2b^2+\xi a^4+\xi b^4}{t^4}$. Assume that $u_1\neq u_2$ are two solutions of (10) and let $U=u_1+u_2$, then we have

$$\begin{cases} U^{2q}+U^2+\xi U=0,\\ \xi U^4+U^2+\xi U=0, \end{cases} \tag{11}$$

which gives that

$$U^{2q}+\xi U^4=0.$$

Note that $U\neq 0$, so we have $U^{2q-4}=\xi$, which implies that $U=\xi$, since $\xi^{2q-4}=\xi$ $(2q-4\equiv 1 \pmod 3)$ and

$$\gcd(2q-4,q^3-1)=\gcd\left(2^{m+1}-4,2^{3m}-1\right)=2^{\gcd(m-1,3m)}-1=1$$

as $m\not\equiv 1 \pmod 3$. But $U=\xi$ contradicts to (11), so that (10) has at most one solution. Therefore, (6) has at most one solution in $\mathbb{F}_{q^3}^*$. This completes the proof.

Theorem 3.2. Let $q=2^m$, m be even and ξ be a primitive element of $\mathbb{F}_{2^2}$. Then $f(x)=x+x^q+x^{q^2}+\xi x^{q^2-q+1}$ is a permutation polynomial over $\mathbb{F}_{q^3}$.

Proof: We first show that $f(x)=0$ has a unique solution $x=0$ in $\mathbb{F}_{q^3}$. Suppose that there exists some $x\in\mathbb{F}_{q^3}^*$ such that $f(x)=0$, then we have

$$1+x^{q-1}+x^{q^2-1}+\xi x^{q^2-q}=0.$$

Let $u=x^{q-1}$, then it becomes

$$1+u+\xi u^q+u^{q+1}=0. \tag{12}$$

If $\xi+u=0$, then (12) gives $u=1$, which is a contradiction. Hence (12) yields $u^q=\frac{u+1}{\xi+u}$ and $u^{q^2}=\frac{1}{u+\xi^2}$. Thus we have

$$1=u^{q^2+q+1}=\frac{u^2+u}{u^2+u+1},$$

which is equivalent to $1=0$, a contradiction. Therefore, $f(x)=0$ has only one solution.

Below for any $a\in\mathbb{F}_{q^3}^*$ we show that

$$f(x)=x+x^q+x^{q^2}+\xi x^{q^2-q+1}=a \tag{13}$$

has at most one solution in $\mathbb{F}_{q^3}^*$. Let $y=x^q$, $z=y^q$, $b=a^q$ and $c=b^q$. Then we can get the following system of equations

$$\begin{cases} x+y+z+\frac{\xi xz}{y}=a,\\ y+z+x+\frac{\xi yx}{z}=b,\\ z+x+y+\frac{\xi zy}{x}=c, \end{cases}$$

which can be rewritten as

$$\begin{cases} y^2+xy+zy+\xi xz=ay,\\ z^2+yz+xz+\xi yx=bz,\\ x^2+zx+yx+\xi zy=cx. \end{cases} \tag{14}$$

Eliminating the indeterminate z in (14), one can obtain that

$$\begin{cases} f_1(y):=(a+b)y^2+(\xi^2(a+b)x+a^2+ab)y\\ \qquad\qquad +\xi^2x^3+\xi(a+b)x^2+\xi abx=0,\\ f_2(y):=\xi y^3+\xi(x+a)y^2+(\xi x^2+(a+c)x)y\\ \qquad\qquad +\xi x^3+\xi cx^2=0. \end{cases}$$

By using the MAGMA software, the resultant of f_1 and f_2 with respect to y is

$$R(f_1,f_2,y)=\xi x^3(x+\xi a)^2(x^4+\alpha),$$

where $\alpha=\xi a^2b^2+\xi a^3b+\xi a^3c+\xi a^2bc+\xi ab^3+\xi ab^2c+\xi b^3c+a^2c^2+b^2c^2$. Since f_1 and f_2 have a common root, then we obtain that

$$R(f_1,f_2,y)=\xi x^3(x+\xi a)^2(x^4+\alpha)=0. \tag{15}$$

So (13) has at most one solution in $\mathbb{F}_{q^3}^*$ if and only if (15) has at most one solution in $\mathbb{F}_{q^3}^*$. Note that if $a=b$ or $b=c$ or $a=c$, then $a=b=c$ from $b=a^q$, $c=b^q$ and $a=c^q$. Therefore, we divide the discussion into the following three cases:

Case 1: $a=b=c$. It is easy to get that $\xi x^3(x+\xi a)^6=0$ from (15). Therefore, $x=\xi a$ is the only possible solution of (15).

Case 2: $a\neq b\neq c$ and $\xi a+b=0$. In this case we have $\xi b+c=0$ and $\xi c+a=0$. Thus we can deduce that $\xi^2(a+b+c)=0$, which implies $a+b+c=0$. Substituting b for $a+c$ in α, we obtain

$$\alpha = \xi a^4 + \xi ac^3 + \xi^2 c^4,$$

which is equivalent to $\alpha = \xi a^4$ since $\xi c + a = 0$. So (15) can be rewritten as $\xi x^3(x + \xi a)^6 = 0$. Therefore, $x = \xi a$ is the only possible solution of (15).

Case 3: $a \neq b \neq c$ and $\xi a + b \neq 0$. If $x = \xi a$, then $y = \xi b$ and $z = \xi c$. Thus we obtain that

$$(\xi a + b)(b + c) = 0$$

from the first equation of (14), which leads to a contradiction that $\xi a + b = 0$ or $b + c = 0$. Therefore, $x = \alpha^{\frac{1}{4}}$ is the only possible solution of (15). This completes the proof.

3.2 The Case p is Odd

In the following, we constructed two classes of permutation quadrinomials with the form of $f(x) = x \pm x^q + x^{q^2} + x^{q^2-q+1}$.

Theorem 3.3: Let $q = p^m$ and p be an odd prime. Then $f(x) = x + x^q + x^{q^2} + x^{q^2-q+1}$ is a permutation polynomial over $\mathbb{F}_{q^3}$.

Proof: We first show that $f(x) = 0$ has a unique solution $x = 0$ in $\mathbb{F}_{q^3}$. Assume that there exists some $x \in \mathbb{F}^*_{q^3}$ such that $f(x) = 0$. Then we have

$$1 + x^{q-1} + x^{q^2-1} + x^{q^2-q} = 0. \tag{16}$$

Let $u = x^{q-1}$, then it becomes

$$1 + u + u^q(u + 1) = 0. \tag{17}$$

If $u + 1 = 0$, then $u = -1$, so that $u^{1+q+q^2} = -1$, which contradicts to $u^{1+q+q^2} = x^{q^3-1} = 1$. Hence (17) yields $u^q = -1$, which also leads to the contradiction $u = -1$.

Below for any $a \in \mathbb{F}^*_{q^3}$ we show that

$$f(x) = x + x^q + x^{q^2} + x^{q^2-q+1} = a \tag{18}$$

has at most one solution in $\mathbb{F}^*_{q^3}$. Let $y = x^q$, $z = y^q$, $b = a^q$ and $c = b^q$. Then we can get the following system of equations

$$\begin{cases} x + y + z + \frac{xz}{y} = a, \\ y + z + x + \frac{yx}{z} = b, \\ z + x + y + \frac{zy}{x} = c, \end{cases}$$

which can be rewritten as

$$\begin{cases} y^2 + xy + zy + xz = ay, \\ z^2 + yz + xz + yx = bz, \\ x^2 + zx + yx + zy = cx. \end{cases} \tag{19}$$

Eliminating the indeterminate z in (19), we can obtain that

$$\begin{cases} f_1(y) := (b-a)y^2 + (2bx + a^2 - ab)y + ax^2 \\ \qquad + bx^2 - abx = 0, \\ f_2(y) := y^2 - ay + cx - x^2 = 0. \end{cases}$$

By using the MAGMA software, the resultant of f_1 and f_2 with respect to y is

$$R(f_1, f_2, y) = x^2(4abcx - a^2b^2 + a^2c^2 - 2abc^2 + b^2c^2).$$

Since f_1 and f_2 have a common root, then we obtain

$$x^2(4abcx - a^2b^2 + a^2c^2 - 2abc^2 + b^2c^2) = 0.$$

Note that $abc \neq 0$ and $x \neq 0$. Therefore, $x = \frac{a^2b^2 - a^2c^2 + 2abc^2 - b^2c^2}{4abc}$ is the only possible solution of (18). This completes the proof.

Theorem 3.4: Let $q = p^m$ and p be an odd prime. Then $f(x) = x - x^q + x^{q^2} + x^{q^2-q+1}$ is a permutation polynomial over $\mathbb{F}_{q^3}$.

Proof: We first show that $f(x) = 0$ has a unique solution $x = 0$ in $\mathbb{F}_{q^3}$. Suppose that there exists some $x \in \mathbb{F}^*_{q^3}$ such that $f(x) = 0$. Then we can get

$$1 - x^{q-1} + x^{q^2-1} + x^{q^2-q} = 0. \tag{20}$$

Let $u = x^{q-1}$, then it becomes

$$1 - u + u^q(u + 1) = 0. \tag{21}$$

Then we have $u^q = \frac{u-1}{u+1}$ and $u^{q^2} = -\frac{1}{u}$. Hence

$$1 = u^{1+q+q^2} = \frac{1-u}{u+1},$$

which gives that $u = 0$, a contradiction.

Below, for any $a \in \mathbb{F}^*_{q^3}$ we show that

$$f(x) = x - x^q + x^{q^2} + x^{q^2-q+1} = a \tag{22}$$

has at most one solution in $\mathbb{F}^*_{q^3}$. Let $y = x^q$, $z = y^q$, $b = a^q$ and $c = b^q$. Then we can get the following system of equations

$$\begin{cases} x - y + z + \frac{xz}{y} = a, \\ y - z + x + \frac{yx}{z} = b, \\ z - x + y + \frac{zy}{x} = c, \end{cases}$$

which can be expressed as

$$\begin{cases} -y^2 + xy + zy + xz = ay \\ -z^2 + yz + xz + yx = bz \\ -x^2 + zx + yx + zy = cx. \end{cases} \tag{23}$$

Eliminating the indeterminate z in (23), we can obtain that

$$\begin{cases} f_1(y) := (4x - a - b)y^2 + (4ax - a^2 - ab)y + x^2a \\ \qquad + bx^2 - abx = 0, \\ f_2(y) := y^2 + ay - cx - x^2 = 0. \end{cases}$$

By using the MAGMA software, the resultant of f_1 and f_2 with respect to y is $R(f_1, f_2, y) = x^2(4x^2 + 4cx - ab - bc - ac)^2$. Since f_1 and f_2 have a common root, then we obtain

$$x(4x^2 + 4cx - ab - bc - ac) = 0. \tag{24}$$

The solutions of $4x^2 + 4cx - ab - bc - ca = 0$ are $x =$

$\frac{-c\pm\sqrt{(c+a)(c+b)}}{2}$. Note that $(c+a)(c+b) = (c+a)^{q^2+1}$, where q^2+1 is even, thus $(c+a)(c+b)$ is a square. Moreover, one can check that $x_1 = \frac{-c+\sqrt{(c+a)(c+b)}}{2}$ is a solution of (22), while $x_2 = \frac{-c-\sqrt{(c+a)(c+b)}}{2}$ is not. This completes the proof.

4. The Quasi-Multiplicative Equivalence

In this section, we discuss the quasi-multiplicative (QM) equivalence between the presented permutations and the known ones.

It is clear that two QM equivalent permutations must have the same number of terms. Thus, we only need to compare the permutations in this paper with all known permutation quadrinomials over $\mathbb{F}_{q^3}$. To the best of the authors' knowledge, there are only four classes of known permutation quadrinomials over finite fields of odd characteristic in [19].

Let $S_{\bmod\ (q^3-1)} = \{s \bmod (q^3-1) \mid s \in S\}$, and via the strategy mentioned in [16] to investigate the QM inequivalence of $f(x) = x + a_1x^{s_1} + a_2x^{s_2} + a_3x^{s_3}$ in this paper and $g(x) = b_1x^{d_1} + b_2x^{d_2} + b_3x^{d_3} + b_4x^{d_4}$ through the following two steps.

1. Prove that there exists no integer $1 \le r \le q-2$ such that $\gcd(r, q^3-1) = 1$ and $\{1, s_1, s_2, s_3\}_{\bmod\ (q^3-1)} = \{d_1, d_2, d_3, d_4\}_{\bmod\ (q^3-1)}$;
2. Compare the coefficients of $c_2 f(c_1 x^r)$ and $g(x)$.

For instance, the permutations in Theorem 3.1 is QM inequivalent to the permutations in Theorem 3.2 from Step 1. Otherwise, there exists an integer r such that $\gcd(r, q^3-1) = 1$ and $\{r, rq, r(q^2-q+1), r(q^2+q-1)\}_{\bmod\ (q^3-1)} = \{1, q, q^2, q^2-q+1\}_{\bmod\ (q^3-1)}$. Clearly, $r = 1$ is impossible. If $r = q$, then $rq = q^2$, $r(q^2-q+1) \equiv q+1-q^2 \bmod (q^3-1)$ and $r(q^2+q-1) \equiv q^2-q+1 \bmod (q^3-1)$. If $r = q^2$, then $rq \equiv 1 \bmod (q^3-1)$, $r(q^2-q+1) \equiv q^2+q-1 \bmod (q^3-1)$ and $r(q^2+q-1) \equiv q+1-q^2 \bmod (q^3-1)$. If $r = q^2-q+1$, then $rq \equiv 1+q-q^2 \bmod (q^3-1)$, $r(q^2-q+1) \equiv 3q^2-q-1 \bmod (q^3-1)$ and $r(q^2+q-1) \equiv 3q-q^2-1 \bmod (q^3-1)$. In conclusion, we have

$$\begin{aligned}&\{r, rq, r(q^2-q+1), r(q^2+q-1)\}_{\bmod\ (q^3-1)}\\ \ne&\{1, q, q^2, q^2-q+1\}_{\bmod\ (q^3-1)}.\end{aligned}$$

Also note that Step 2 is enough to show QM inequivalence between the permutations in Theorem 3.3 and those in Theorem 3.4. By similar discussions, it can be proved that each permutation polynomial over finite fields of odd characteristic in this paper is QM inequivalent to all permutation quadrinomials in [19].

5. The Differential Uniformity

In this section, by using the MAGMA software, we obtain the differential uniformity δ of some known permutation trinomials and the permutation quadrinomials proposed in this paper over $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{3^6}$, respectively. The results are presented in Tables 1, 2 and 3.

Table 1 The differential uniformity of some permutation polynomials over $\mathbb{F}_{2^6}$.

Class	Polynomials	δ	Reference
I	$x^5 + x^8 + x^{32}$	4	[4]
II	$bx+ax^{16}+x^{13}$, $a^{21} = b^{21}$ and $a^4b \in \mathbb{F}^*_{2^2}\backslash\{1\}$	4	[16]
III	$a^{18}x^4 + ax^{16} + x^{13}$, $a^{42} + b^{21} = 1$	4	[16]
IV	$x + ax^{19} + bx^{52}$, $a^{42} + b^{21} = 1$	12	[16]
V	$vx + x^5 + x^{17}$, $v \in \mathbb{F}_{2^2}\backslash\{0, 1\}$	16	[17]
VI	$x + Ax^{52} + x^{19}$, $A \in \mathbb{F}^*_{2^2}$	12	[5]
VII	$x + x^4 + \xi x^{13} + x^{19}$, $\xi\mathbb{F}^*_{2^2}\backslash\{1\}$	12	Theorem 3.1
VIII	$x + x^4 + x^{16} + \xi x^{13}$, $\xi\mathbb{F}^*_{2^2}\backslash\{1\}$	4	Theorem 3.2

Table 2 The differential uniformity of some permutation polynomials over $\mathbb{F}_{2^{12}}$.

Class	Polynomials	δ	Reference
I	$x^2 + x^9 + x^{512}$	16	[4]
II	$x + x^{241} + x^{271}$	48	[20]
III	$x + x^{256} + x^{271}$	16	[20]
IV	$bx + ax^{256} + x^{241}$, $a^{273} = b^{273}$ and $a^4b \in \mathbb{F}^*_{2^4}\backslash\{1\}$	16	[16]
V	$x+ax^{271}+x^{3856}$, $a^{546}+b^{273} = 1$ and $ab = 1$	16	[16]
VI	$vx + x^{17} + x^{257}$, $v \in \mathbb{F}^*_{2^2}\backslash\{1\}$	256	[17]
VII	$x + Ax^{241} + x^{271}$, $A \in \mathbb{F}^*_{2^2}$	48	[5]
VIII	$x + x^{16} + x^{256} + \xi x^{241}$, $\xi \in \mathbb{F}^*_{2^2}\backslash\{1\}$	16	Theorem 3.2

Table 3 The differential uniformity of some permutation polynomials over $\mathbb{F}_{3^6}$.

Class	Polynomials	δ	Reference
I	$-x^{369} + x^{41} + x^{409}$	10	[22]
II	$-x + x^{41} + x^{369}$	10	[13]
III	$x - x^{73} + x^{89}$	28	[21]
IV	$x + x^{81} - x^{89}$	10	[21]
V	$-x + x^9 + x^{89}$	10	[21]
VI	$x + Ax^{73} + A^2x^{81}$, $A \in \mathbb{F}^*_{3^2}$ with $A^3 \ne 1$	10	[5]
VII	$x + x^9 + x^{73} + x^{81}$	10	Theorem 3.3
VIII	$x - x^9 + x^{73} + x^{81}$	10	Theorem 3.4

From the above three tables, one can see that the differential uniformity of our permutations is good compared with other known permutation trinomials.

6. Conclusion

In this paper, we construct two classes of permutation quadrinomials over $\mathbb{F}_{q^3}$ for q even and two classes of permutation quadrinomials over $\mathbb{F}_{q^3}$ for q odd, respectively. We also show that these permutation quadrinomials are QM inequivalent to known permutation quadrinomials. Compared with the differential uniformity of some known permutation trinomials in recent papers, our permutation quadrinomials are good.

Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2101703; in part by the National Natural Science

Foundation of China under Grants 61972258, 62272107 and U19A2066; in part by the Innovation Action Plan of Shanghai Science and Technology under Grants 20511102200 and 21511102200; in part by the Key Research and Development Program of Guangdong Province under Grant 2020B0101090001, and in part by Open Research Program of Shanghai Key Lab of Intelligent Information Processing under Grant IIPL201902.

References

[1] D. Bartoli, "Permutation trinomials over $\mathbb{F}_{q^3}$," Finite Fields Appl., vol.61, p.101597, Jan. 2020.

[2] H. Dobbertin, "Uniformly representable permutation polynomials," Proc. SETA 01, T. Helleseth, P.V. Kumar, and K. Yang, eds., pp.1–22, Springer, London, 2002.

[3] C. Ding, "Cyclic codes from some monomials and trinomials," SIAM J. Discret. Math., vol.27, no.4, pp.1977–1994, Nov. 2013.

[4] X. Gong, G. Gao, and W. Liu, "On permutation polynomials of the form $x^{1+2^k} + L(x)$," Int. J. Comput. Math., vol.93, no.10, pp.1715–1722, Aug. 2016.

[5] R. Gupta, P. Gahlyan, and R.K. Sharma, "New classes of permutation trinomials over $\mathbb{F}_{q^3}$," Finite Fields Appl., vol.84, p.102110, Dec. 2022.

[6] X. Hou, "Permutation polynomials over finite fields — A survey of recent advances," Finite Fields Appl., vol.32, pp.82–119, March 2015.

[7] J. Jeong, C.H. Kim, N. Koo, S. Kwon, and S. Lee, "On cryptographic parameters of permutation polynomials of the form $x^r h(x^{(2^n-1)/d})$," IEICE Trans. Fundamentals, vol.E105-A, no.8, pp.1134–1146, Aug. 2022.

[8] Y. Laigle-Chapuy, "Permutation polynomials and applications to coding theory," Finite Fields Appl., vol.13, no.1, pp.58–70, Jan. 2007.

[9] J. Levine and J.V. Brawley, "Some cryptographic applications of permutation polynomials," Cryptologia, vol.1, no.1, pp.76–92, Jan. 1977.

[10] J. Levine and R. Chandler, "Some further cryptographic applications of permutation polynomials," Cryptologia, vol.11, no.4, pp.211–218, Oct. 1987.

[11] Y. Li and M. Wang, "On EA-equivalence of certain permutations to power mappings," Des. Codes Cryptogr., vol.58, pp.259–269, July 2018.

[12] N. Li and X. Zeng, "A survey on the applications of Niho exponents," Cryptogr. Commun., vol.11, pp.509–548, May 2019.

[13] J. Ma, T. Zhang, T. Feng, and G. Ge, "Some new results on permutation polynomials over finite fields," Des. Codes Cryptogr., vol.83, pp.425–443, May 2017.

[14] A.M. Masuda and M.E. Zieve, "Permutation binomials over finite fields," Trans. Amer. Math. Soc., vol.361, pp.4169–4180, March 2009.

[15] E. Pasalic and P. Charpin, "Some results concerning cryptographically significant mappings over GF(2^n)," Des. Codes Cryptogr., vol.57, pp.257–269, Feb. 2010.

[16] T. Pang, Y. Xu, N. Li, and X. Zeng, "Permutation polynomials of the form $x^d + L(x^s)$ over $\mathbb{F}_{q^3}$," Finite Fields Appl., vol.76, p.101906, Aug. 2021.

[17] Z. Tu, X. Zeng, and L. Hu, "Several classes of complete permutation polynomials," Finite Fields Appl., vol.25, pp.182–193, Jan. 2014.

[18] D. Wu, P. Yuan, C. Ding, and Y. Ma, "Permutation trinomials over $\mathbb{F}_{2^m}$," Finite Fields Appl., vol.46, pp.38–56, July 2017.

[19] Y. Wang, W. Zhang, D. Bartoli, and Q. Wang, "Permutation polynomials and complete permutation polynomials over $\mathbb{F}_{q^3}$," arXiv:1806.05712v1, June 2018.

[20] Y. Wang, W. Zhang, and Z. Zha, "Six new classes of permutation trinomials over $\mathbb{F}_{2^n}$," SIAM J. Discrete Math., vol.32, no.3, pp.1946–1961, Jan. 2018.

[21] Y. Wang, W. Zhang, and Z. Zha, "Six new classes of permutation trinomials over $\mathbb{F}_{3^{3k}}$," Appl. Algebra Eng. Commun. Comput., vol.29, pp.479–499, Dec. 2018.

[22] P. Yuan, "More explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$," Finite Fields Appl., vol.16, no.2, pp.88–95, March 2010.

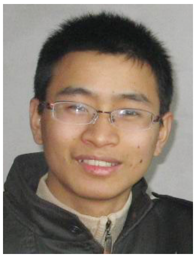
[23] L. Zheng, H. Kan, and J. Peng, "Two classes of permutation trinomials with Niho exponents over finite fields with even characteristic," Finite Fields Appl., vol.68, p.101754, Dec. 2020.

[24] L. Zheng, H. Kan, J. Peng, and D. Tang, "Two classes of permutation trinomials with niho exponents," Finite Fields Appl., vol.70, p.101790, Feb. 2021.

[25] L. Zheng, B. Liu, H. Kan, J. Peng, and D. Tang, "More classes of permutation quadrinomials from Niho exponents in characteristic two," Finite Fields Appl., vol.78, p.101962, Feb. 2022.

Changhui Chen was born in Hunan, China, in 1995. He is now a Ph.D. candidate of Shanghai Normal University. His present research interests include mathematics and cryptograghy.

Haibin Kan received Ph D in the Institute of Mathematics of Fudan University in 1999. Then he was a faculty of School of Computer Science, Fudan University. He is now a Full Professor of Fudan University and the head of the group of Theoretical Computer and Cryptography. His research topics include Cryptography, Information Security and Coding Theory. From June 2002 to February 2006, he was an Assistant Professor of the School of Information, Japan Advanced Institute of Science and Technology.



Jie Peng received Ph. D in Mathematics in 2011 from Fudan University. He is now an Associate Professor of College of Mathematics and Science, Shanghai Normal University. From April 2014 to August 2015, he was with Temasek Laboratories, National University of Singapore as a Visiting Research Scientist. His research interest includes Coding Theory and Information Security.

Li Wang received Ph. D in the Department of Mathematics of East China Normal University in 2006. She is now an Associate Professor of College of Mathematics and Science, Shanghai Normal University. From September 2011 to August 2012, she worked in the Department of Mathematics of the University of Aberdeen, UK, as a visiting scholar. Her research interest includes Algebra, Coding Theory and Information Security.