A NEW FAMILY OF APN MAPPINGS OVER FINITE FIELDS OF ODD CHARACTERISTIC

XIANGYONG ZENG, LEI HU, YANG YANG, AND WENFENG JIANG

Abstract. In this paper, for a prime $p \equiv 3 \pmod 4$ and an odd n such that $p^n \geq 7$, a new family of almost perfect nonlinear mappings over the finite field F_{p^n} is presented. These mappings have the form as $f(x) = ux^{\frac{p^n-1}{2}-1} + x^{p^n-2}$, and contain the ternary APN mappings proposed by Ness and Helleseth as a special case. For $p \geq 7$, these proposed mappings are proven to be CCZ-inequivalent to all known APN power mappings.

1. Introduction And Preliminaries

To efficiently resist against differential attacks [9], cryptographical functions used as S-boxes in block ciphers should have low differential uniformity. In this sense a class of mappings with the smallest possible differential uniformity, almost perfect nonlinear (APN) mappings, is introduced as ones opposing an optimum resistance to the differential cryptanalysis [24].

Let F_{p^n} denote a finite field with p^n elements, where p is a prime. A function f from F_{p^n} to itself is called *almost perfect nonlinear* if, for every $a \neq 0$ and every b in F_{p^n}, the function $f(x+a)-f(x) = b$ admits at most two solutions. Few APN mappings are known, and all known monomial APN power mappings are listed as in Table 1.

Until recently, the known constructions of APN mappings are EA-equivalent to power mappings over finite fields. Two functions f_1 and f_2 are called *extended affine equivalent* (EA-equivalent) if $f_2 = A_1 \circ f_1 \circ A_2 + A$, where mappings A_1, A_2, A are affine and A_1, A_2 are permutations. Up to EA-equivalence, if f_1 is not affine, then f_1 and f_2 have the same algebraic degree. The mappings f_1 and f_2 are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if the graphs of f_1 and f_2, that is, the subsets $\{(x, f_1(x)) \,|\, x \in F_{p^n}\}$ and $\{(x, f_2(x)) \,|\, x \in F_{p^n}\}$ of $F_{p^n} \times F_{p^n}$, are affine equivalent. Hence, f_1 and f_2 are CCZ-equivalent if and only if there exists an affine automorphism $L = (L_1, L_2)$ of $F_{p^n} \times F_{p^n}$ such that

$$y = f_1(x) \Longleftrightarrow L_2(x, y) = f_2(L_1(x, y)).$$

Note that the function $L_1(x, f_1(x))$ has to be a permutation. CCZ-equivalence is a more general equivalent relation of functions than EA-equivalence, and it keeps APN property of functions, i.e., if f_1 and f_2 are CCZ-equivalent, then f_1 is APN if and only if f_2 is APN [10]. By applying CCZ-transformations of functions [10], new classes of binary APN functions EA-inequivalent to power functions are found in [7]. However, these functions are CCZ-equivalent to Gold power mappings. The first examples of APN functions CCZ-inequivalent to power mappings are introduced in [15], and they are two quadratic binomials defined over two specific fields $F_{2^{10}}$ and $F_{2^{12}}$, respectively. Recently, binary APN functions are extensively studied, and some functions

Key words and phrases. Almost perfect nonlinear (APN), differential uniformity, EA-equivalence, CCZ-equivalence.

X. Zeng and Y. Yang are with the Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China (e-mail: xzeng@hubu.edu.cn).

L. Hu and W. Jiang are with the State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing, 100049, China (e-mail: {hu,wfjiang}@is.ac.cn).

are proven to be CCZ-inequivalent to all known APN mappings [1]-[6]. Some nonbinary APN functions are also found in [14, 18, 19].

Table 1 Known monomial APN power mappings over F_{p^n}.

Functions	Exponents d	Conditions	References
Kloosterman	p^n-2	$p=2$ and n is odd, or $p>2$ and $p\equiv 2\,(\mathrm{mod}\,3)$	[8] [24] [19]
Gold	2^i+1	$p=2$, gcd $(i,n)=1$	[17]
Kasami	$2^{2i}-2^i+1$	$p=2$, gcd $(i,n)=1$	[20] [21]
Welch	2^t+3	$p=2$, $n=2t+1$	[11]
Niho	$2^t+2^{t/2}-1$ for even t $2^t+2^{\frac{3t+1}{2}-1}$ for odd t	$p=2$, $n=2t+1$	[13]
Inverse	$2^{2t}-1$	$p=2$, $n=2t+1$	[8] [24]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$p=2$, $n=5i$	[12]
Helleseth Sandberg	$\frac{p^n-1}{2}-1$	$p\equiv 3,7\,(\mathrm{mod}\,20)$, $p^n>7$, $p^n\neq 27$ and n is odd	[19]
Dobbertin et. al. Felke	$\frac{3^{(n+1)/2}-1}{2}$ $\frac{3^{(n+1)/2}-1}{2}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 3\,(\mathrm{mod}\,4)$ $p=3$, $n\equiv 1\,(\mathrm{mod}\,4)$	[14] [16]
Dobbertin et. al.	$\frac{3^{n+1}-1}{8}$ $\frac{3^{n+1}-1}{8}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 3\,(\mathrm{mod}\,4)$ $p=3$, $n\equiv 1\,(\mathrm{mod}\,4)$	[14]
Helleseth Rong Sandberg	$\frac{p^n+1}{4}+\frac{p^n-1}{2}$ $\frac{p^n+1}{4}$ $\frac{2p^n-1}{3}$ p^n-3	$p^n\equiv 3\,(\mathrm{mod}\,8)$ $p^n\equiv 7\,(\mathrm{mod}\,8)$ $p^n\equiv 2\,(\mathrm{mod}\,3)$ $p=3$, $n>1$, n is odd	[18]
Trival	3	$p>3$	[19]

In this paper, for a prime $p\equiv 3\,(\mathrm{mod}\,4)$ and an odd n such that $p^n\geq 7$, we study a class of binomial APN mappings having the form as

$$f(x)=ux^{\frac{p^n-1}{2}-1}+x^{p^n-2} \tag{1}$$

over F_{p^n}, where the element $u\in F_{p^n}$ satisfies

$$\chi(u+1)=\chi(u-1)=-\chi(5u+3),\ \text{or}\ \chi(u+1)=\chi(u-1)=-\chi(5u-3) \tag{2}$$

and the quadratic character χ is defined in Section 2. When $p=3$ and $n\geq 3$, the proposed family is exactly that found in [23]. Furthermore, for $p\geq 7$, these functions are proven to be CCZ-inequivalent to all known APN power mappings.

The remainder of this paper is organized as follows. Section 2 proves the proposed functions are APN. Section 3 studies the inequivalence between these functions and all known APN power mappings. Section 4 concludes the study.

2. A New Family Of APN Mappings Over F_{p^n}

Throughout this paper, it is always assumed that the prime $p\equiv 3\,(\mathrm{mod}\,4)$ and n is odd.

In this section, a family of functions defined by Equality (1) will be proven to be APN. The following lemma in page 225 of [22] will be used in the proof of the result in this paper.

Lemma 1: Let χ be a multiplicative character of F_{p^n} of order $m>1$ and let $f(x)\in F_{p^n}[x]$ be a monic polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over F_{p^n}. Then for every $a\in F_{p^n}$, we have

$$|\sum_{c\in F_{p^n}}\chi(af(c))|\leq (d-1)p^{n/2}.$$

The quadratic character on F_{p^n} is defined by

$$\chi(x) = \begin{cases} 1, & \text{if } x \text{ is a square in } F_{p^n}, \\ -1, & \text{if } x \text{ is a nonsquare in } F_{p^n}, \\ 0, & \text{if } x = 0. \end{cases}$$

In another expression, one has $\chi(x) = x^{\frac{p^n-1}{2}}$.

When $p = 3$ and $n \geq 3$ is odd, one has $-\chi(5u+3) = -\chi(5u-3) = \chi(u)$, and there exist elements $u \in F_{3^n}$ satisfying both formulas in Equality (2) [23]. The number of similar elements u in the case $p \geq 7$ is characterized by the following lemma.

Lemma 2: For a prime $p \geq 7$ with $p \equiv 3 \pmod 4$ and for odd n, let N be the number of elements $u \in F_{p^n}$ satisfying the condition in Equality (2). Then, $N \geq 1$. Furthermore, when $n = 1$ and $p \geq 163$, or $n \geq 3$ and $p \geq 7$, the value of N satisfies

$$\frac{1}{8}(3p^n - 37p^{n/2}) \leq N \leq \frac{1}{8}(3p^n + 37p^{n/2}).$$

Proof: Let N_1 be the number of elements $u \in F_{p^n}$ satisfying

$$\chi(u+1) = \chi(u-1) = -\chi(5u+3) = 1.$$

We first show by a similar method as used in Lemma 1 of [23] that

$$p^n - 5p^{n/2} \leq 8N_1 \leq p^n + 5p^{n/2}.$$

Let $\Gamma = \{1, -1, -3/5\}$ be the set of zeroes of three expressions $u+1$, $u-1$ and $5u+3$. Then,

$$8N_1 = \sum_{u \in F_{p^n} \setminus \Gamma} (1 + \chi(u+1))(1 + \chi(u-1))(1 - \chi(5u+3)).$$

The summation $\sum\limits_{u \in F_{p^n} \setminus \Gamma}$ can be written as $\sum\limits_{u \in F_{p^n}} - \sum\limits_{u \in \Gamma}$, and one can easily get the latter summation. Due to the assumption on p and n, one has $\chi(-1) = -1$. By the property of a multiplicative character that $\chi(a^2 b) = \chi(b)$ and $\chi(a) = \pm 1$ for any $a \neq 0$, one can directly calculate

$$\sum_{u \in \Gamma} (1 + \chi(u+1))(1 + \chi(u-1))(1 - \chi(5u+3)) = 0.$$

Thus,

$$\begin{aligned} & -p^n + 8N_1 \\ = \; & -p^n + \sum_{u \in F_{p^n}} (1 + \chi(u+1))(1 + \chi(u-1))(1 - \chi(5u+3)) \\ = \; & \sum_{u \in F_{p^n}} \chi(u+1) + \sum_{u \in F_{p^n}} \chi(u-1) - \sum_{u \in F_{p^n}} \chi(5u+3) \\ & + \sum_{u \in F_{p^n}} \chi(u^2-1) - \sum_{u \in F_{p^n}} \chi((u+1)(5u+3)) - \sum_{u \in F_{p^n}} \chi((u-1)(5u+3)) \\ & - \sum_{u \in F_{p^n}} \chi((u+1)(u-1)(5u+3)), \end{aligned}$$

and by Lemma 1, one has

$$|8N_1 - p^n| \leq 5p^{n/2}.$$

Similarly, let N_2, N_3 and N_4 be the numbers of elements $u \in F_{p^n}$ satisfying $\chi(u+1) = \chi(u-1) = -\chi(5u+3) = -1$, $\chi(u+1) = \chi(u-1) = -\chi(5u-3) = 1$ and $\chi(u+1) = \chi(u-1) = -\chi(5u-3) = -1$, respectively, and one has for $i = 2, 3, 4$,

$$\tfrac{1}{8}(p^n - 5p^{n/2}) \leq N_i \leq \tfrac{1}{8}(p^n + 5p^{n/2}).$$

Let N_5 and N_6 be the numbers of elements $u \in F_{p^n}$ satisfying $\chi(u+1) = \chi(u-1) = -\chi(5u+3) = -\chi(5u-3) = 1$ and $\chi(u+1) = \chi(u-1) = -\chi(5u+3) = -\chi(5u-3) = -1$, respectively. It can be similarly proven that

$$\tfrac{1}{16}(p^n - 17p^{n/2}) \leq N_i \leq \tfrac{1}{16}(p^n + 17p^{n/2})$$

for $i = 5$, 6.

Thus, the value of $N = N_1 + N_2 + N_3 + N_4 - N_5 - N_6$ can be measured as follows:

$$|N - 3p^n/8| \leq (4 \cdot 5/8 + 2 \cdot 17/16)p^{n/2} = 37p^{n/2}/8.$$

When $n = 1$ and $p \geq 163$, or $n \geq 3$ and $p \geq 7$, a direct calculation shows that $N \geq (3p^n - 37p^{n/2})/8 \geq 1$. When $n = 1$ and $7 \leq p < 163$, with the help of a computer, we can find at least one element $u \in F_p$ satisfying the condition in Equality (2).

This finishes the proof. $\square$

By Lemma 2, when p^n is large enough, N is about as large as $3p^n/8$. The following example gives a concrete value of N in the finite field F_{7^3}.

Example 1: Let $F_{p^n} = F_{7^3}$. With the help of a computer, one can find $N = 128$ elements $u \in F_{7^3}$ satisfying the condition in Equality (2) such that $f(x) = ux^{170} + x^{341}$ is an APN mapping. Among them, there exist 85 elements u satisfying $\chi(u+1) = \chi(u-1) = -\chi(5u+3)$, 85 elements u satisfying $\chi(u+1) = \chi(u-1) = -\chi(5u-3)$, and 42 elements u satisfying $\chi(u+1) = \chi(u-1) = -\chi(5u-3) = -\chi(5u+3)$.

The following lemma is an analog of Lemma 1 in [23]. It will be used to prove the APN property of the presented functions.

Lemma 3: Assume $p \equiv 3 \pmod 4$, n is odd, $p^n \geq 7$, and $u \in F_{p^n}$ satisfies the condition in Equality (2). Further assume $u \neq 4$ and $u \neq 7$ in the case of $p = 11$ and $n = 1$. Then there exists one nonzero element $z \in F_{p^n}$ such that $z \neq 1 \pm u$ and the three elements $z^2 - 4(u+1)z$, $z^2 + 4(u-1)z$ and $z^2 - 4z + 4u^2$ are all nonsquares in F_{p^n}.

Proof: Let N be the number of elements $z \in F_{p^n}$ satisfying the requirements in the lemma, and let $\Gamma' = \{0, x_1 = 4 + 4u, x_2 = 4 - 4u, x_3, x_4, 1 + u, 1 - u\}$ be the multiset consisting of $1 \pm u$ and all zeroes of three polynomials $z^2 - 4(u+1)z$, $z^2 + 4(u-1)z$ and $z^2 - 4z + 4u^2$, here x_3 and x_4 are zeroes of $z^2 - 4z + 4u^2$. Denote

$$h(z) = (1 - \chi(z^2 - 4(u+1)z))(1 - \chi(z^2 + 4(u-1)z))(1 - \chi(z^2 - 4z + 4u^2)).$$

Then

$$8N = \sum_{z \in F_{p^n} \setminus \Gamma'} h(z) = \sum_{z \in F_{p^n}} h(z) - \sum_{z \in \Gamma'} h(z).$$

Note that $h(z)$ takes value 0 at $z = 0$, takes values at most 4 at each x_i $(1 \leq i \leq 4)$, and takes values at most 8 at $z = 1 \pm u$. Therefore, the summation $\sum_{z \in \Gamma'} h(z) \leq 32$. By a direct calculation, one has

$$\begin{aligned}
& \sum_{z \in F_{p^n}} \chi(z^2(z - 4u - 4)(z + 4u - 4)) \\
= \ & (\sum_{z=0} + \sum_{0 \neq z \in F_{p^n}})\chi(z^2(z - 4u - 4)(z + 4u - 4)) \\
= \ & 0 + \sum_{0 \neq z \in F_{p^n}} \chi((z - 4u - 4)(z + 4u - 4)) \\
= \ & 1 + (\sum_{z=0} + \sum_{0 \neq z \in F_{p^n}})\chi((z - 4u - 4)(z + 4u - 4)) \\
= \ & 1 + \sum_{z \in F_{p^n}} \chi((z - 4u - 4)(z + 4u - 4)),
\end{aligned}$$

where the fact $\chi((-4u-4)(4u-4)) = \chi(-1)\chi(u+1)\chi(u-1) = -1$ is used in the last second equality. Similarly, one has

$$\begin{aligned} & \sum_{z\in F_{p^n}} \chi(z^2(z-4u-4)(z+4u-4)(z^2-4z+4u^2)) \\ = & \ 1 + \sum_{z\in F_{p^n}} \chi((z-4u-4)(z+4u-4)(z^2-4z+4u^2)). \end{aligned}$$

With a same analysis as in the proof of Lemma 2, one has

$$\begin{aligned} & \sum_{z\in F_{p^n}} (1-\chi(z^2-4(u+1)z))(1-\chi(z^2+4(u-1)z))(1-\chi(z^2-4z+4u^2)) \\ \geq & \ p^n - 13p^{n/2}, \end{aligned}$$

and hence,

$$8N \geq p^n - 13p^{n/2} - 32.$$

If $p^n > 250$, then $N \geq 1$. For values of parameters $p^n < 250$, with the help of a computer, one can confirm $N \geq 1$ if u satisfies the condition in Equality (2) and satisfies $u \neq 4$ and $u \neq 7$ in the case of $p = 11$ and $n = 1$.

This finishes the proof. □

Remark 1: When $p = 11$ and $n = 1$, both $u = 4$ and 7 satisfy the condition in Equality (2). For $u = 4$, or 7, there is at least one square element in the set

$$\{z^2-4(u+1)z, z^2+4(u-1)z, z^2-4z+4u^2\}$$

for any $z \in F_{11}$.

The functions defined by Equality (1) can be proven to be APN for suitable parameters p, n and u as the following theorem, by applying a similar method as in [19, 23].

Theorem 1: For a prime $p \equiv 3 \pmod 4$ and an odd n such that $p^n \geq 7$, $u \in F_{p^n}$ satisfies the condition in Equality (2), then the mapping $f(x)$ defined by Equality (1) is APN.

Proof: It needs to prove the equation $f(x+a) - f(x) = b$, i.e.,

$$u(x+a)^{\frac{p^n-1}{2}-1} + (x+a)^{p^n-2} - (ux^{\frac{p^n-1}{2}-1} + x^{p^n-2}) = b \tag{3}$$

has at most two solutions for any given $a \neq 0$ and $b \in F_{p^n}$. In the following, the number of solutions to Equation (3) will be investigated.

When $x \neq 0$ and $-a$, multiplying both sides of (3) by $(x+a)x$ implies

$$bx^2 + (ab + u\chi(x) - u\chi(x+a))\, x + a(u\chi(x)+1) = 0. \tag{4}$$

That is to say

1) $(\chi(x+a), \chi(x)) = (1, 1)$:
$$bx^2 + abx + a(1+u) = 0; \tag{5}$$
2) $(\chi(x+a), \chi(x)) = (-1, -1)$:
$$bx^2 + abx + a(1-u) = 0; \tag{6}$$
3) $(\chi(x+a), \chi(x)) = (1, -1)$:
$$bx^2 + (ab-2u)x + a(1-u) = 0; \tag{7}$$
4) $(\chi(x+a), \chi(x)) = (-1, 1)$:
$$bx^2 + (ab+2u)x + a(1+u) = 0. \tag{8}$$

On the other hand,

i) when $x=0$, Equation (3) becomes two equivalent ones as follows:

$$ua^{\frac{p^n-1}{2}-1}+a^{p^n-2}=b \iff 1+u\chi(a)=ab;$$

ii) when $x=-a$, one has

$$-(u(-a)^{\frac{p^n-1}{2}-1}+(-a)^{p^n-2})=b \iff 1-u\chi(a)=ab.$$

The discussion can be divided into the following three subcases: $ab\neq 1\pm u$, $ab=1+u$, and $ab=1-u$.

For a prime $p\equiv 3(\bmod 4)$ and an odd n, one has $\frac{p^n-1}{2}\equiv 1(\bmod 2)$ and $\chi(-1)=-1$. For the element u satisfying the condition in Equality (2), one has $u\neq \pm 1, 0$. Otherwise, $\chi(u+1)=\chi(2)\neq\chi(0)=\chi(u-1)$ for $u=1$, $\chi(u-1)=\chi(-2)\neq\chi(0)=\chi(u+1)$ for $u=-1$, and $\chi(u-1)=\chi(-1)\neq\chi(1)=\chi(u+1)$ for $u=0$, which contradict with the assumption that $\chi(u+1)=\chi(u-1)$.

(1) $ab\neq 1\pm u$.

By i) and ii), neither $x=0$ nor $-a$ is the solution of Equation (3).

When $b=0$, Equations (5) and (6) have no solutions since $u\neq\pm 1$. Each of Equations (7) and (8) has one solution. Thus, Equation (3) has at most two solutions in this case.

When $b\neq 0$, for Equations (5) and (6), one has $\chi(x(x+a))=\chi(x)\chi(x+a)=1$. This shows

$$\chi(\frac{a(1\pm u)}{b})=\chi(-x(x+a))=\chi(-1)=-1. \tag{9}$$

We claim that Equation (5) has at most one solution. Otherwise, if Equation (5) has two solutions x_1 and x_2, then both of them are square elements and $\chi(x_1x_2)=1$. On the other hand, $x_1x_2=\frac{a(1+u)}{b}$ and by Equality (9), $\chi(x_1x_2)=-1$. This is a contradiction. Therefore, Equation (5) has at most one solution. It can be similarly proven that Equation (6) also has at most one solution. Furthermore, if these two equations have solutions simultaneously, by Equality (9), one has

$$\chi(\frac{a(1-u)}{b})=\chi(\frac{a(1+u)}{b})=-1$$

which is impossible since $\chi(1-u)=-\chi(u-1)=-\chi(u+1)$. Thus, Equations (5) and (6) have at most one solution in total.

Assume that each of Equations (7) and (8) has two solutions x_1 and x_2. Then, one has $x_1x_2=\frac{a(1\mp u)}{b}$ and $x_1+x_2=-\frac{ab\mp 2u}{b}$. Hence,

$$\begin{array}{rcl}(x_1+a)(x_2+a) & = & x_1x_2+a(x_1+x_2)+a^2\\ & = & \frac{a(1\mp u)}{b}-a(\frac{ab\mp 2u}{b})+a^2\\ & = & \frac{a(1\pm u)}{b}.\end{array}$$

Since $\chi(u-1)=\chi(u+1)$, one has

$$\begin{array}{rcl}\chi(x_1x_2(x_1+a)(x_2+a)) & = & \chi(-\frac{a^2(u+1)(u-1)}{b^2})\\ & = & \chi(-(u+1)(u-1))\\ & = & -1,\end{array}$$

which implies that

$$\left\{\begin{array}{l}\chi(x_1(x_1+a))=1;\\ \chi(x_2(x_2+a))=-1\end{array}\right. \text{ or } \left\{\begin{array}{l}\chi(x_1(x_1+a))=-1;\\ \chi(x_2(x_2+a))=1.\end{array}\right. \tag{10}$$

On the other hand, by Equations (7) and (8), one has $\chi(x_i(x_i+a))=-1$ for $i=1,2$, and hence $\chi(x_1x_2(x_1+a)(x_2+a))=1$, which contradicts with the fact $\chi(x_1x_2(x_1+a)(x_2+a))=-1$ that can be derived from Equality (10). Therefore, the assumption can not hold and then each of Equations (7) and (8) has at most one solution. If these two equations have solutions simultaneously, denoted by x_1 and y_1 respectively, then one has

$$\chi(x_1+a)=1,\ \chi(x_1)=-1,\ \chi(y_1+a)=-1,\ \text{and}\ \chi(y_1)=1. \tag{11}$$

Let $x_2 \neq x_1$ and $y_2 \neq y_1$ also satisfy Equations $bx^2+(ab-2u)x+a(1-u)=0$ and $bx^2+(ab+2u)x+a(1+u)=0$, respectively, then $(\chi(x_2+a),\chi(x_2)) \neq (1,-1)$ and $(\chi(y_2+a),\chi(y_2)) \neq (-1,1)$. Note that $-(x_1+a)$ and $-(x_2+a)$ are two solutions to Equation $bx^2+(ab+2u)x+a(1+u)=0$, then one has $\{-(x_1+a),-(x_2+a)\}=\{y_1,y_2\}$. By Equality (11), one has

$$x_1+y_2+a=x_2+y_1+a=0.$$

The equalities $\chi(-1)=-1$ and (11) show that

$$1=\chi(x_1(-x_1-a)y_1(-y_1-a))=\chi(x_1y_1x_2y_2)=\chi(\frac{a(1-u)}{b}\cdot\frac{a(1+u)}{b})=-1.$$

This is a contradiction. Thus, Equations (7) and (8) have at most one solution in total. Since it has been proved that Equations (5) and (6) have at most one solution in total, one has Equation (3) has at most two solutions.

(2) $ab=1+u$.

In this subcase, $b=\frac{1+u}{a}\neq 0$ since $u\neq\pm 1$. For given a,b, and u, there exists exactly one solution of Equation (3) in the set $\{0,-a\}$, namely $x=0$ if $\chi(a)=1$ and $x=-a$ if $\chi(a)=-1$.

Assume that Equation (3) has one solution x_0 other than 0 and $-a$. Then, this solution satisfies $(x_0+a)x_0\neq 0$ and it is a solution to Equation (4). We will show that there exists at most one such x_0 in the case of u satisfying the condition in Equality (2).

When $\chi(u+1)=\chi(u-1)=-\chi(5u+3)$, the discriminants of Equations (7) and (8) are equal to

$$\begin{aligned} a^2b^2-4ab+4u^2 &= (u+1)^2-4(u+1)+4u^2 \\ &= 5u^2-2u-3 \\ &= (5u+3)(u-1). \end{aligned}$$

Since $\chi(5u+3)=-\chi(u-1)$, $4u^2+a^2b^2-4ab$ is nonsquare. Thus, x_0 can not satisfy Equation (7) or Equation (8). By previous analysis, Equations (5) and (6) totally have at most one solution. Therefore, in this case, Equation (3) has at most one such x_0 other than 0 and $-a$.

When $\chi(u+1)=\chi(u-1)=-\chi(5u-3)$, if x_0 satisfies Equation (5), one has

$$\chi(x_0(x_0+a))=\chi(-\frac{a(1+u)}{b})=\chi(-a^2)=-1,$$

which contradicts with $\chi(x_0+a)=1$ and $\chi(x_0)=1$. The discriminant of Equation (6) is equal to $a^2b^2+4ab(u-1)=(5u-3)(u+1)$, which is nonsquare. Thus, x_0 can not satisfy Equation (5) or Equation (6). Since Equations (7) and (8) totally have at most one solution, Equation (3) has at most one such x_0 other than 0 and $-a$.

Combining the discussion above, Equation (3) has at most two solutions.

(3) $ab=1-u$.

It can be similarly proven that Equation (3) has at most two solutions.

Finally, we prove that there are values for $a\neq 0$ and b such that $f(x+a)-f(x)=b$ has exactly two solutions, or equivalently, $f(x)$ is not a *perfect nonlinear* or *planar* function in the sense that for every $0\neq a\in F_{p^n}$, the function $\Delta f_a(x)=f(x+a)-f(x)$ induces a permutation mapping over F_{p^n}. To this end, we only need to prove that there are values for $a\neq 0$ and b such that $f(x+a)-f(x)=b$ has no solutions since for any $a\neq 0$ there is on the average one solution for each b.

For u satisfying the condition in Equality (2) and satisfying $u \neq 4$ and $u \neq 7$ if $p = 11$ and $n = 1$, the discriminants of Equations (5), (6), (7) and (8) are

$$a^2b^2 - 4ab(u+1),\ a^2b^2 + 4ab(u-1),\ a^2b^2 - 4ab + 4u^2,\ a^2b^2 - 4ab + 4u^2,$$

respectively. Thus, it is sufficient to show that there exists at least one nonzero element $z = ab \in F_{p^n} \setminus \{1 \pm u\}$ such that all the discriminants are nonsquares, i.e., such that $z^2 - 4(u+1)z$, $z^2 + 4(u-1)z$ and $z^2 - 4z + 4u^2$ are nonsquares. This follows Lemma 3.

For $p = 11$ and $n = 1$, when $u = 4$ or 7, it is directly verified that the equation

$$f(x+1) - f(x) = u(x+1)^4 + (x+1)^9 - ux^4 - x^9 = 1$$

has no solution in F_{11}.

Now we complete the proof of that $f(x)$ is exactly an APN function. □

Remark 2: When $p = 3$, $\chi(5u \pm 3) = \chi(-u) = -\chi(u)$, the condition $\chi(u+1) = \chi(u-1) = -\chi(5u \pm 3)$ is equivalent to $\chi(u+1) = \chi(u-1) = \chi(u)$. Thus, Theorem 1 in [23] is a special case of our result. For $p \geq 7$, the characterization of u is different from the case for $p = 3$ given in [23]. Using this characterization, an analog of the APN mapping family in [23] for $p \geq 7$ can be obtained.

When $p \geq 7$, the constructed functions in this paper are different from those in [23] and they will be proven to be CCZ-inequivalent to all known APN mappings in next section.

3. The Inequivalence With Known APN Power Mappings

In this section, we will discuss the inequivalence between $f(x)$ defined in Equality (1) and all known APN power mappings $g(x) = x^d$ as in Table 1 for $p \geq 7$ and an odd n.

Suppose that $f(x)$ and $g(x) = x^d$ are CCZ-equivalent, then there exists an affine automorphism $L = (L_1, L_2)$ of $F_{p^n} \times F_{p^n}$ such that

$$L_2(x, f(x)) = g(L_1(x, f(x))) \pmod{x^{p^n} - x},$$

where $L_2(x,y) = a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i y^{p^i}$, $L_1(x,y) = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i y^{p^i}$, $a, c, a_i, b_i, c_i, e_i \in F_{p^n}$ and $L_1(x, f(x))$ is a permutation. Thus, one has

$$a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i} = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^d \pmod{x^{p^n} - x}, \tag{12}$$

where $f(x)^{p^i}$ can be calculated as

$$\begin{aligned} f(x)^{p^i} &= (ux^{\frac{p^n-1}{2}-1} + x^{p^n-2})^{p^i} \\ &= u^{p^i} x^{\frac{p^i(p^n-1)}{2} - p^i} + x^{p^i(p^n-1)-p^i} \\ &= u^{p^i} x^{\frac{p^n-1}{2} - p^i} + x^{p^n-1-p^i}. \end{aligned}$$

By Table 1, the power exponent d takes at most five types of values as listed in Propositions 1-2 and Corollary 1 below if $f(x)$ is CCZ-equivalent to a known APN power mapping $g(x) = x^d$. In what follows, we will prove that $f(x)$ is CCZ-inequivalent to these known APN power mappings.

For a given non-negative integer k with p-adic expansion $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$ where $0 \leq k_i < p$, its *p-adic weight* is defined as the integer $k_0 + k_1 + \cdots + k_{n-1}$ and denoted by $wt(k)$. For every non-constant monomial function x^γ on F_{p^n}, where $\gamma \neq 0$, there is a positive integer β with $1 \leq \beta \leq p^n - 1$ such that $x^\gamma = x^\beta \pmod{x^{p^n} - x}$, namely, $\beta \equiv \gamma \pmod{p^n - 1}$ if $\gamma \not\equiv 0 \pmod{p^n - 1}$, and $\beta = p^n - 1$ if $\gamma \equiv 0 \pmod{p^n - 1}$. For a monomial x^γ defined on F_{p^n}, it is sufficient to consider the p-adic weight of such an integer β, and the latter is regarded as the weight of γ. The main technique used in the following proofs is to analyze the weights of the exponents of the monomials in the expansion of some polynomials over F_{p^n}.

In the following proofs to Proposition 1, Corollary 1 and Proposition 2, one will encounter 35 kinds of monomials totally. Their exponents and the possible values of the corresponding weights are carefully but tediously determined as in Table 2.

Lemma 4: Let $0 \leq k, s, t, l, v \leq n-1$, and $q = p-1$. The weights of the 35 kinds of exponents listed in Table 2 are correctly given in that table.

Proof: We show the determination of the weights by illustrating a complicated case, namely how to determine the weight of the last exponent $p^k + p^s + p^n - 1 - p^t - p^l - p^v$. Other kinds of exponents are similarly handled. Without loss of generality, we can assume for this case that $k \geq s$ and $t \geq l \geq v$. We show its weight must be one of the several values listed in the last entry in Table 2.

Firstly, assume $p^k + p^s > p^t + p^l + p^v$. Then one has

$$p^k + p^s + p^n - 1 - p^t - p^l - p^v (\bmod p^n - 1) = p^k + p^s - p^t - p^l - p^v = \beta,$$

and $k > t$, or $k = t$ and $s > l$.

When $k > t$, $p^k - p^v = (p-1)p^{k-1} + \cdots + (p-1)p^v$ and its weight is $(k-v)q$. If $s = k, t, l$ or $s < v$, β has weight $(k-v)q - 1$. If $k > t \geq l > s \geq v$, $p^k - p^l = (p-1)p^{k-1} + \cdots + (p-1)p^l$ has weight $(k-l)q$ and $p^s - p^v = (p-1)p^{s-1} + \cdots + (p-1)p^v$ has weight $(s-v)q$. Thus, β has weight $(k+s-l-v)q - 1$. Similarly, for $k > t > s > l \geq v$, β has weight $(k+s-t-v)q - 1$. If $k > s > t \geq l \geq v$, $p^s - p^v = (p-1)p^{s-1} + \cdots (p-1)p^v$ and then β has weight $(s-v)q - 1$.

When $k = t$ and $s > l$, by the expression of $p^s - p^v$, $\beta = p^s - p^l - p^v$ has weight $(s-v)q - 1$.

Secondly, assume $p^k + p^s < p^t + p^l + p^v$. Then in this case, one has $k \leq t$ and

$$p^k + p^s + p^n - 1 - p^t - p^l - p^v (\bmod p^n - 1) = p^k + p^s + p^n - 1 - p^t - p^l - p^v = \beta.$$

When $k = t$, one has $s \leq l$ and $\beta = p^s + p^n - 1 - p^l - p^v$. If $v < s \leq l$, β has weight $(n+s-l)q - 1$. If $s \leq v$, β has weight $(n+s-v)q - 1$.

When $k < t$, if $k \geq s > l \geq v$, one has $p^n - p^t = (p-1)p^{n-1} + \cdots + (p-1)p^t$ of weight $(n-t)q$ and $p^s - 1 = (p-1)p^{s-1} + \cdots + (p-1)$ of weight sq. Thus, the weight of β is equal to $(n-t+s)q + 1 - 2 = (n+s-t)q - 1$. Similarly, one has

$$wt(\beta) = \begin{cases} (n+k+s-t-l)q - 1, & t > k \geq l \geq s > v; \\ (n+k+s-t-v)q - 1, & t > k > l \geq v \geq s; \\ (n+s-l)q - 1, & t \geq l > k \geq s > v; \\ (n+k+s-l-v)q - 1, & t \geq l \geq k \geq v \geq s; \\ (n+s-v)q - 1, & t \geq l \geq v > k \geq s. \end{cases}$$

All the weight values appeared above are ranged into the set of 10 expressions listed in the last entry of Table 2. □

With the weights in Lemma 4, the following Propositions 1-2 and Corollary 1 can be proved. Another simple fact below will also be used in these proofs.

Lemma 5: Let $u \in F_{p^n}$ satisfy the condition in Equality (2) and $p \geq 7$. Then, none of the two systems of equations

$$\begin{cases} 3u^2 + 1 = 0 \\ u^2 + 3 = 0 \end{cases} \text{ and } \begin{cases} 5u^4 + 10u^2 + 1 = 0 \\ u^4 + 10u^2 + 5 = 0 \end{cases}$$

has solutions.

Table 2. Thirty-five kinds of exponents and their p-adic weights (with notation $q := p-1$)

Exponent	p^k	$\frac{p^n-1}{2}-p^k$	p^n-1-p^k
Weight	1	$\frac{nq}{2}-1$	$nq-1$
Exponent	p^k+p^s	$p^n-1-p^k-p^s$	$p^k+\frac{p^n-1}{2}-p^s$
Weight	2	$nq-2$	$\frac{nq}{2}$
Exponent	$\frac{p^n-1}{2}-p^k-p^s$	$p^k+p^s+p^t$	$p^k+p^s+\frac{p^n-1}{2}-p^t$
Weight	$\frac{nq}{2}-2$	3	$\frac{nq}{2}+1$
Exponent	$p^k+\frac{p^n-1}{2}-p^s-p^t$	$\frac{p^n-1}{2}-p^k-p^s-p^t$	$p^n-1-p^k-p^s-p^t$
Weight	$\frac{nq}{2}-1$	$\frac{nq}{2}-3\,(p^n>7)$ $6\,(p^n=7)$	$nq-3$
Exponent	$p^k+p^n-1-p^s$	$p^k+p^s+p^n-1-p^t$	$p^k+p^n-1-p^s-p^t$
Weight	$(k-s)q$, or $(n+k-s)q$	$(k-t)q+1$, or $(s-t)q+1$, or $(n+\min\{k,s\}-t)q+1$	$(k-\min\{s,t\})q-1$, or $(n+k-s)q-1$, or $(n+k-t)q-1$
Exponent	$p^k+p^s+p^t+p^l$	$\frac{p^n-1}{2}-p^k-p^s-p^t-p^l$	$p^k+\frac{p^n-1}{2}-p^s-p^t-p^l$
Weight	4	$\frac{nq}{2}-4\,(p>7)$ $3n-4$ or $3n+2\,(p=7)$	$\frac{nq}{2}-2$
Exponent	$p^k+p^s+\frac{p^n-1}{2}-p^t-p^l$	$p^k+p^s+p^t+\frac{p^n-1}{2}-p^l$	$p^n-1-p^k-p^s-p^t-p^l$
Weight	$\frac{nq}{2}$	$\frac{nq}{2}+2$	$nq-4$
Exponent	$p^k+p^n-1-p^s-p^t-p^l$	$p^k+p^s+p^n-1-p^t-p^l$	$p^k+p^s+p^t+p^n-1-p^l$
Weight	$(k-\min\{s,t,l\})q-2$, or $(n+k-s)q-2$, or $(n+k-t)q-2$, or $(n+k-l)q-2$	$(k-\min\{t,l\})q$, or $(s-\min\{t,l\})q$, or $(k+s-t-l)q$, or $(n+\min\{k,s\}-l)q$, or $(n+\min\{k,s\}-t)q$, or $(n+k+s-t-l)q$	$(k-l)q+2$, or $(s-l)q+2$, or $(t-l)q+2$, or $(n+\min\{k,s,t\}-l)q+2$
Exponent	$p^k+p^s+p^t+p^l+p^v$	$\frac{p^n-1}{2}-p^k-p^s-p^t-p^l-p^v$	$p^k+\frac{p^n-1}{2}-p^s-p^t-p^l-p^v$
Weight	5	$\frac{nq}{2}-5\,(p\geq 11, p^n>11)$ $10\,(p^n=11)$ $3n-5$ or $3n+1\,(p=7)$	$\frac{nq}{2}-3\,(p>7)$, $3n-3$ or $3n+3\,(p=7)$
Exponent	$p^k+p^s+\frac{p^n-1}{2}-p^t-p^l-p^v$	$p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$	$p^k+p^s+p^t+p^l+\frac{p^n-1}{2}-p^v$
Weight	$\frac{nq}{2}-1$	$\frac{nq}{2}+1$	$\frac{nq}{2}+3\,(p>7)$, $3n+3$ or $3n-3\,(p=7)$
Exponent	$p^n-1-p^k-p^s-p^t-p^l-p^v$	$p^k+p^n-1-p^s-p^t-p^l-p^v$	$p^k+p^s+p^t+p^l+p^n-1-p^v$
Weight	$nq-5$	$(k-\min\{s,t,l,v\})q-3$, or $(n+k-s)q-3$, or $(n+k-t)q-3$, or $(n+k-l)q-3$, or $(n+k-v)q-3$	$(k-v)q+3$, or $(s-v)q+3$, or $(t-v)q+3$, or $(l-v)q+3$, or $(n+\min\{k,s,t,l\}-v)q+3$
Exponent	$p^k+p^s+p^t+p^n-1-p^l-p^v$ $(k\geq s\geq t$ and $l\geq v)$	$p^k+p^s+p^n-1-p^t-p^l-p^v$ $(k\geq s$ and $t\geq l\geq v)$	
Weight	$(k-v)q+1$, or $(s-v)q+1$, or $(t-v)q+1$, or $(k+s-l-v)q+1$, or $(k+t-l-v)q+1$, or $(s+t-l-v)q+1$, or $(n+t-l)q+1$, or $(n+t-v)q+1$, or $(n+s+t-l-v)q+1$, or $(n+k+t-l-v)q+1$	$(k-v)q-1$, or $(s-v)q-1$, or $(k+s-l-v)q-1$, or $(k+s-t-v)q-1$, or $(n+s-t)q-1$, or $(n+s-l)q-1$, or $(n+s-v)q-1$, or $(n+k+s-t-v)q-1$, or $(n+k+s-t-l)q-1$, or $(n+k+s-l-v)q-1$	

With the above preparation, the inequivalence of functions can now be discussed. Since the weights of exponents in Table 2 depend on the parameters p and n, the inequivalent proof of

$f(x)$ and all known APN power mappings can be divided into three subcases: (1) $p \geq 7$ and $n \geq 3$; (2) $p \geq 19$ and $n = 1$; and (3) $p = 7$ or 11, and $n = 1$. We only give the proof of the first case in Propositions 1-2 and Corollary 1, and the second case can be proved in a similar way. The third case can be directly verified with the help of a computer. The reader will find the proof of Proposition 2 is very lengthy (nine pages two of which is devoted to Proposition 2(1) and the other seven to Proposition 2(2)). We can not give a unified proof to these propositions and corollary.

Proposition 1: The function $f(x)$ is CCZ-inequivalent to $g(x) = x^d$ on F_{p^n}, if

(1) $d = 3$; or

(2) $d = p^n - 2$ for $p \equiv 2(\mathrm{mod}\ 3)$.

Proof: (1) Suppose that $f(x)$ and $g(x) = x^3$ are CCZ-equivalent. Then, the right hand side (RHS) of Equality (12) is expanded as

$$\begin{aligned}
& (c+\sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^3 \\
= \ & c^3 + 3\sum_{k=0}^{n-1} c^2 c_k x^{p^k} + 3\sum_{k=0}^{n-1} c^2 e_k u^{p^k} x^{\frac{p^n-1}{2}-p^k} + 3\sum_{k=0}^{n-1} c^2 e_k x^{p^n-1-p^k} \\
& +3\sum_{k,s=0}^{n-1} c c_k c_s x^{p^k+p^s} + 3\sum_{k,s=0}^{n-1} c e_k e_s (u^{p^k+p^s}+1) x^{p^n-1-p^k-p^s} \\
& +6\sum_{k,s=0}^{n-1} c c_k e_s u^{p^s} x^{p^k+\frac{p^n-1}{2}-p^s} + 6\sum_{k,s=0}^{n-1} c c_k e_s x^{p^k+p^n-1-p^s} \\
& +6\sum_{k,s=0}^{n-1} c e_k e_s u^{p^k} x^{\frac{p^n-1}{2}-p^k-p^s} + \sum_{k,s,t=0}^{n-1} c_k c_s c_t x^{p^k+p^s+p^t} \\
& +3\sum_{k,s,t=0}^{n-1} c_k c_s e_t u^{p^t} x^{p^k+p^s+\frac{p^n-1}{2}-p^t} + 3\sum_{k,s,t=0}^{n-1} c_k c_s e_t x^{p^k+p^s+p^n-1-p^t} \\
& +6\sum_{k,s,t=0}^{n-1} c_k e_s e_t u^{p^s} x^{p^k+\frac{p^n-1}{2}-p^s-p^t} \\
& +3\sum_{k,s,t=0}^{n-1} c_k e_s e_t (u^{p^s+p^t}+1) x^{p^k+p^n-1-p^s-p^t} \\
& +\sum_{k,s,t=0}^{n-1} e_k e_s e_t (u^{p^k+p^s+p^t}+3u^{p^k}) x^{\frac{p^n-1}{2}-p^k-p^s-p^t} + \\
& +\sum_{k,s,t=0}^{n-1} e_k e_s e_t (3u^{p^k+p^s}+1) x^{p^n-1-p^k-p^s-p^t}.
\end{aligned} \tag{13}$$

The exponents of indeterminant x in Equality (13) have 15 kinds of possible forms, which are exactly the first 15 kinds of exponents in Table 2.

Consider the exponent $3p^i$ of weight 3, where $i \in \{0, 1, \cdots, n-1\}$. By the weights of the first 15 kinds of exponents in Table 2, for $p \geq 7$ and $n \geq 3$, the exponent $3p^i$ only derives from the form $p^k + p^s + p^t$ with $k = s = t = i$. Therefore, by Equality (13), the coefficient of x^{3p^i} on the RHS of Equality (12) is equal to c_i^3, and it is zero on the left hand side (LHS). This gives $c_i^3 = 0$, i.e., $c_i = 0$.

Considering the exponent $p^n - 1 - 3p^i$, similarly, one has $p^n - 1 - 3p^i = p^n - 1 - p^k - p^s - p^t$ and then $k = s = t = i$. As the case of x^{3p^i}, one can get that the coefficient of $x^{p^n-1-3p^i}$ on the RHS of Equality (12) is equal to $e_i^3(3u^{2p^i} + 1)$, and it is zero on the LHS. Then, one has

$$e_i^3(3u^2+1)^{p^i} = 0. \tag{14}$$

Similarly, the following equality can be obtained by considering the coefficient of $x^{\frac{p^n-1}{2}-3p^i}$,

$$e_i^3(u^3+3u)^{p^i}=0. \tag{15}$$

By Lemma 5, Equalities (14) and (15) imply $e_i=0$ for all $i\in\{0,1,\cdots,n-1\}$. Thus $L_1(x,f(x))=c$ is not a permutation.

Therefore, $f(x)$ and $g(x)=x^3$ are CCZ-inequivalent on F_{p^n}.

(2) Suppose that $f(x)$ and x^{p^n-2} are CCZ-equivalent. By $p\equiv 3(\mathrm{mod}\ 4)$ and $p\equiv 2(\mathrm{mod}\ 3)$, one has $p\geq 11$. Multiplying both sides of Equality (12) by $(c+\sum\limits_{i=0}^{n-1}c_ix^{p^i}+\sum\limits_{i=0}^{n-1}e_if(x)^{p^i})^2$ implies

$$(a+\sum_{i=0}^{n-1}a_ix^{p^i}+\sum_{i=0}^{n-1}b_if(x)^{p^i})(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2=c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i}\ (\mathrm{mod}\, x^{p^n}-x). \tag{16}$$

The LHS of Equality (16) is equal to

$$\begin{aligned}
&(a+\sum_{i=0}^{n-1}a_ix^{p^i}+\sum_{i=0}^{n-1}b_if(x)^{p^i})(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2\\
=\ & ac^2+\sum_{k=0}^{n-1}(2acc_k+a_kc^2)x^{p^k}+\sum_{k=0}^{n-1}(c^2b_k+2ace_k)u^{p^k}x^{\frac{p^n-1}{2}-p^k}\\
&+\sum_{k=0}^{n-1}(c^2b_k+2ace_k)x^{p^n-1-p^k}+\sum_{k,s=0}^{n-1}(ac_kc_s+2ca_kc_s)x^{p^k+p^s}\\
&+\sum_{k,s=0}^{n-1}(ae_ke_s+2b_kce_s)(u^{p^k+p^s}+1)x^{p^n-1-p^k-p^s}\\
&+\sum_{k,s=0}^{n-1}(2ac_ke_s+2a_kce_s+2b_scc_k)u^{p^s}x^{p^k+\frac{p^n-1}{2}-p^s}\\
&+\sum_{k,s=0}^{n-1}(2ac_ke_s+2a_kce_s+2b_scc_k)x^{p^k+p^n-1-p^s}\\
&+\sum_{k,s=0}^{n-1}(2ae_ke_s+2b_kce_s+2b_sce_k)u^{p^k}x^{\frac{p^n-1}{2}-p^k-p^s}\\
&+\sum_{k,s,t=0}^{n-1}a_kc_sc_tx^{p^k+p^s+p^t}+\sum_{k,s,t=0}^{n-1}(2a_kc_se_t+b_tc_kc_s)u^{p^t}x^{p^k+p^s+\frac{p^n-1}{2}-p^t}\\
&+\sum_{k,s,t=0}^{n-1}(2a_kc_se_t+b_tc_kc_s)x^{p^k+p^s+p^n-1-p^t}\\
&+\sum_{k,s,t=0}^{n-1}(2a_ke_se_t+4b_sc_ke_t)u^{p^s}x^{p^k+\frac{p^n-1}{2}-p^s-p^t}\\
&+\sum_{k,s,t=0}^{n-1}(a_ke_se_t+2b_sc_ke_t)(u^{p^s+p^t}+1)x^{p^k+p^n-1-p^s-p^t}\\
&+\sum_{k,s,t=0}^{n-1}b_ke_se_t(u^{p^k+p^s+p^t}+u^{p^k}+2u^{p^s})x^{\frac{p^n-1}{2}-p^k-p^s-p^t}\\
&+\sum_{k,s,t=0}^{n-1}b_ke_se_t(2u^{p^k+p^s}+u^{p^s+p^t}+1)x^{p^n-1-p^k-p^s-p^t}.
\end{aligned} \tag{17}$$

Equalities (17) and (13) have same exponents of the indeterminant x, i.e., the first 15 kinds of exponents as listed in Table 2.

For any i, $0 \le i \le n-1$, by a similar analysis as above for the coefficients of the exponents $3p^i$, $\frac{p^n-1}{2} - 3p^i$, and $p^n - 1 - 3p^i$ in Equality (17), one has

$$\begin{cases} a_i c_i^2 = 0; \\ b_i e_i^2 (u^3 + 3u)^{p^i} = 0; \\ b_i e_i^2 (3u^2 + 1)^{p^i} = 0. \end{cases} \tag{18}$$

By Lemma 5, Equality (18) gives

$$a_i c_i = 0 \text{ and } b_i e_i = 0. \tag{19}$$

Considering the exponent $p^n - 1 - p^i - 2p^j$ $(0 \le i \ne j \le n-1)$, again by the weights of the first 15 exponents in Table 2, one has $p^n - 1 - p^i - 2p^j = p^n - 1 - p^k - p^s - p^t$ and then $k = i$, $s = t = j$, or $s = i$, $k = t = j$, or $t = i$, $k = s = j$. Thus, by Equality (17), the coefficient of $x^{p^n-1-p^i-2p^j}$ on the LHS of Equality (16) is equal to

$$(b_i e_j^2 + 2b_j e_i e_j)(2u^{p^i+p^j} + u^{2p^j} + 1) = b_i e_j^2 (2u^{p^i+p^j} + u^{2p^j} + 1),$$

and it is zero on the RHS. Thus,

$$b_i e_j^2 (2u^{p^i+p^j} + u^{2p^j} + 1) = 0. \tag{20}$$

Similarly as above, from the coefficient of $x^{\frac{p^n-1}{2} - p^i - 2p^j}$ $(i \ne j)$, one has

$$b_i e_j^2 (u^{p^i+2p^j} + u^{p^i} + 2u^{p^j}) = 0. \tag{21}$$

We claim that $b_i e_j = 0$ holds for any $0 \le i \ne j \le n-1$. Otherwise, there exist two integers i_0 and j_0 such that $b_{i_0} e_{j_0} \ne 0$. By Equalities (20) and (21), one has

$$\begin{cases} 2u^{p^{i_0}+p^{j_0}} + u^{2p^{j_0}} + 1 = 0; \\ u^{p^{i_0}+2p^{j_0}} + u^{p^{i_0}} + 2u^{p^{j_0}} = 0. \end{cases} \tag{22}$$

Denote $y = u^{p^{i_0}}$ and $z = u^{p^{j_0}}$. Since $u \ne \pm 1$ and 0, Equality (22) implies

$$y = \frac{z^2+1}{-2z} = \frac{-2z}{z^2+1}.$$

Then, the element z satisfies the following equation

$$z^4 - 2z^2 + 1 = 0, \tag{23}$$

i.e., $z = \pm 1$ and then $u = \pm 1$. It is impossible. Therefore, $b_i e_j = 0$ for any $i \ne j$. This together with Equality (19) shows that $b_i e_j = 0$ for any $i, j \in \{0, 1, \cdots, n-1\}$. That is to say that $b_0 = b_1 = \cdots = b_{n-1} = 0$ or $e_0 = e_1 = \cdots = e_{n-1} = 0$.

Consider the exponent $p^i + 2p^j$ $(i \ne j)$ of weight 3, where $i, j \in \{0, 1, \cdots, n-1\}$. Among the first 15 kinds of exponents in Table 2, the exponent $p^i + 2p^j$ only derives from the form $p^k + p^s + p^t$ with $k = i$ and $s = t = j$, or $s = i$ and $k = t = j$, or $t = i$ and $k = s = j$. Therefore, the coefficient of $x^{p^i+2p^j}$ on the LHS of Equality (16) is equal to $a_i c_j^2 + 2a_j c_i c_j$, and it is zero on the RHS. This gives

$$a_i c_j^2 + 2a_j c_i c_j = 0. \tag{24}$$

By Equalities (19) and (24), one has $a_i c_j = 0$ for any $i, j \in \{0, 1, \cdots, n-1\}$. That is to say that $a_0 = a_1 = \cdots = a_{n-1} = 0$ or $c_0 = c_1 = \cdots = c_{n-1} = 0$.

Assume that $e_j = 0$ for any $j \in \{0, 1, \cdots, n-1\}$. Since $L_1(x, f(x))$ is a permutation, there exists some j_0 such that $c_{j_0} \ne 0$. Thus, one has $a_i = 0$ for any i, and then Equality (16) can be reduced to

$$(a + \sum_{i=0}^{n-1} b_i f(x)^{p^i})(c + \sum_{i=0}^{n-1} c_i x^{p^i})^2 = c + \sum_{i=0}^{n-1} c_i x^{p^i} \pmod{x^{p^n} - x}. \tag{25}$$

By Table 2, the exponent $p^n-1-p^i+2p^j$ $(i \neq j)$ has weight $\alpha(p-1)+1$, where i, $j \in \{0,1,\cdots,n-1\}$ and $1 \leq \alpha \leq n-1$, then the exponent $p^n-1-p^i+2p^j$ $(i \neq j)$ only derives from the form $p^k+p^s+p^n-1-p^t$ with $t=i$, $k=s=j$. Therefore, the coefficient of $x^{p^n-1-p^i+2p^j}$ on the LHS of Equality (16) is equal to $b_i c_j^2 + 2a_j c_j e_i$, and it is zero on the RHS. This together with Equality (19) show

$$b_i c_j^2 = 0. \tag{26}$$

For $j=j_0$, the equation $b_i c_{j_0}^2 = 0$ implies that $b_i = 0$ for any $i \neq j_0$. For $i = j_0$, the equation $b_{j_0} c_j^2 = 0$ implies that $b_{j_0} = 0$ or $c_j = 0$ for any $j \neq j_0$. In other words, one has $b_i = 0$ for any i, or $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$.

When $b_i = 0$ for any $i \in \{0,1,\cdots,n-1\}$, Equality (25) is equal to

$$a = (c + \sum_{i=0}^{n-1} c_i x^{p^i})^{p^n-2} \pmod{x^{p^n}-x}. \tag{27}$$

Since $(p^n-2)^2 = (p^n-1)^2 - 2(p^n-1) + 1 \equiv 1 (\bmod\ p^n-1)$, by Equality (27), one has

$$a^{p^n-2} = c + \sum_{i=0}^{n-1} c_i x^{p^i} \pmod{x^{p^n}-x}. \tag{28}$$

Obviously, one has $c_i = 0$ for any $i \in \{0,1,\cdots,n-1\}$ and then $L_1(x,f(x)) = c$ is not a permutation. That is a contradiction.

When $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$, then Equality (25) is further reduced to

$$(a + b_{j_0} f(x)^{p^{j_0}})(c + c_{j_0} x^{p^{j_0}})^2 = c + c_{j_0} x^{p^{j_0}} \pmod{x^{p^n}-x}. \tag{29}$$

Since the coefficient of $x^{\frac{p^n-1}{2}+p^{j_0}}$ is equal to $b_{j_0} c_{j_0}^2 u^{p^{j_0}}$, one has $b_{j_0} c_{j_0}^2 u^{p^{j_0}} = 0$ which implies $b_{j_0} c_{j_0} = 0$. That is also a contradiction.

Now one should assume that there exists some integer j_0 such that $e_{j_0} \neq 0$. Then $b_j = 0$ for any j. If $a_i = 0$ for any i, then by Equalities (27) and (28), one has $L_1(x,f(x)) = c$. This is impossible, and then there exists at least one nonzero element in $\{a_i \,|\, 0 \leq i \leq n-1\}$. Thus, $c_j = 0$ for any j, and Equality (16) is reduced to

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i})(c + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^2 = c + \sum_{i=0}^{n-1} e_i f(x)^{p^i} \pmod{x^{p^n}-x}. \tag{30}$$

Also by Table 2, the exponent $p^n-1+p^i-2p^j$ $(i \neq j)$ has weight $\alpha(p-1)-1$, where i, $j \in \{0,1,\cdots,n-1\}$ and $1 \leq \alpha \leq n-1$. Then, the exponent $p^n-1+p^i-2p^j$ $(i \neq j)$ only derives from the form $p^n-1+p^k-p^s-p^t$ with $k=i$ and $s=t=j$. Therefore, the coefficient of $x^{p^n-1+p^i-2p^j}$ on the LHS of Equality (16) is equal to $a_i e_j^2 (u^{2p^j}+1)$, and it is zero on the RHS. This gives

$$a_i e_j^2 (u^2+1)^{p^j} = 0, \tag{31}$$

and then

$$a_i e_j^2 = 0, \tag{32}$$

since $u^2+1 \neq 0$.

For $j = j_0$, the equation $a_i e_{j_0}^2 = 0$ implies that $a_i = 0$ for any $i \neq j_0$ since $e_{j_0} \neq 0$. Since there exists at least one nonzero element in $\{a_i \,|\, 0 \leq i \leq n-1\}$, one has $a_{j_0} \neq 0$ and the equation $a_{j_0} e_j^2 = 0$ implies $e_j = 0$ for any $j \neq j_0$. Thus, one has $a_{j_0} e_{j_0} \neq 0$ and $b_j = c_j = 0$ for any j. Equality (30) is reduced to

$$(a + a_{j_0} x^{p^{j_0}})(c + e_{j_0} f(x)^{p^{j_0}})^2 = c + e_{j_0} f(x)^{p^{j_0}} \pmod{x^{p^n}-x}. \tag{33}$$

Considering the coefficient of $x^{p^{j_0}}$ in Equality (33), one has $a_{j_0}c^2 = 0$ and then $c = 0$. From the coefficients of $x^{p^n-1-p^{j_0}}$ and $x^{\frac{p^n-1}{2}-p^{j_0}}$, one has

$$\begin{cases} a_{j_0}e_{j_0}^2(u^2+1)^{p^{j_0}} = e_{j_0}; \\ 2a_{j_0}e_{j_0}^2u^{p^{j_0}} = e_{j_0}u^{p^{j_0}}, \end{cases}$$

which implies $u = \pm 1$ since $a_{j_0}e_{j_0} \neq 0$. This contradicts with $u \neq \pm 1$.

The arguments above prove that $f(x)$ and $g(x) = x^{p^n-2}$ are CCZ-inequivalent on F_{p^n}. □

Corollary 1: The function $f(x)$ is CCZ-inequivalent to $g(x) = x^{\frac{2p^n-1}{3}}$, where $p^n \equiv 2 (\mathrm{mod}\ 3)$.

Proof: For $p^n \equiv 2\,(\mathrm{mod}\ 3)$ and $p \equiv 3\,(\mathrm{mod}\ 4)$, one has $p \geq 11$. If $f(x)$ and $g(x) = x^{\frac{2p^n-1}{3}}$ are CCZ-equivalent on F_{p^n}, then by Equality (12), one has

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i})^3 = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i} (\mathrm{mod}\ x^{p^n} - x). \tag{34}$$

A same analysis as in Proposition 1 (1) gives $a_i = b_i = 0$ for any $0 \leq i \leq n-1$. Equality (34) can be reduced to

$$a^3 = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i} (\mathrm{mod}\ x^{p^n} - x),$$

which implies $c_i = e_i = 0$ for any i. Thus, $L_1(x, f(x)) = c$. This contradicts with that $L_1(x, f(x))$ is a permutation. The contradiction proves CCZ-inequivalence of $f(x)$ and $g(x) = x^{\frac{2p^n-1}{3}}$. □

By analyzing the weights of the exponents in Equality (12), the following proposition can be proved in a similar way to Proposition 1.

Proposition 2: The functions $f(x)$ and $g(x) = x^d$ are CCZ-inequivalent on F_{p^n}, if
(1) $d = \frac{p^n+1}{4}$ for $p^n \equiv 7\,(\mathrm{mod}\ 8)$ and $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ for $p^n \equiv 3\,(\mathrm{mod}\ 8)$; or
(2) $d = \frac{p^n-1}{2} - 1$ for $p \equiv 3, 7\,(\mathrm{mod}\ 20)$.

Proof: (1) Assume that $f(x)$ and $g(x) = x^d$ are CCZ-equivalent. Then, by Equality (12), one has

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i})^4 = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^2 (\mathrm{mod}\ x^{p^n} - x). \tag{35}$$

Then, the LHS of Equality (35) is equal to

$$\begin{aligned} & (a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i})^4 \\ = \ & a^4 + 4\sum_{k=0}^{n-1} a^3 a_k x^{p^k} + 4\sum_{k=0}^{n-1} a^3 b_k u^{p^k} x^{\frac{p^n-1}{2}-p^k} + 4\sum_{k=0}^{n-1} a^3 b_k x^{p^n-1-p^k} \\ & +6\sum_{k,s=0}^{n-1} a^2 a_k a_s x^{p^k+p^s} + 6\sum_{k,s=0}^{n-1} a^2 b_k b_s (u^{p^k+p^s}+1) x^{p^n-1-p^k-p^s} \\ & +12\sum_{k,s=0}^{n-1} a^2 a_k b_s u^{p^s} x^{p^k+\frac{p^n-1}{2}-p^s} + 12\sum_{k,s=0}^{n-1} a^2 a_k b_s x^{p^k+p^n-1-p^s} \\ & +12\sum_{k,s=0}^{n-1} a^2 b_k b_s u^{p^k} x^{\frac{p^n-1}{2}-p^k-p^s} + 4\sum_{k,s,t=0}^{n-1} a a_k a_s a_t x^{p^k+p^s+p^t} \\ & +12\sum_{k,s,t=0}^{n-1} a a_k a_s b_t u^{p^t} x^{p^k+p^s+\frac{p^n-1}{2}-p^t} + 12\sum_{k,s,t=0}^{n-1} a a_k a_s b_t x^{p^k+p^s+p^n-1-p^t} \end{aligned}$$

$$
\begin{aligned}
&+24\sum_{k,s,t=0}^{n-1} aa_kb_sb_tu^{p^s}x^{p^k+\frac{p^n-1}{2}-p^s-p^t}\\
&+12\sum_{k,s,t=0}^{n-1} aa_kb_sb_t(u^{p^s+p^t}+1)x^{p^k+p^n-1-p^s-p^t}\\
&+4\sum_{k,s,t=0}^{n-1} ab_kb_sb_t(u^{p^k+p^s+p^t}+3u^{p^k})x^{\frac{p^n-1}{2}-p^k-p^s-p^t}\\
&+4\sum_{k,s,t=0}^{n-1} ab_kb_sb_t(3u^{p^k+p^s}+1)x^{p^n-1-p^k-p^s-p^t}\\
&+\sum_{k,s,t,l=0}^{n-1} a_ka_sa_ta_lx^{p^k+p^s+p^t+p^l}+4\sum_{k,s,t,l=0}^{n-1} a_ka_sa_tb_lu^{p^l}x^{p^k+p^s+p^t+\frac{p^n-1}{2}-p^l}\\
&+4\sum_{k,s,t,l=0}^{n-1} a_ka_sa_tb_lx^{p^k+p^s+p^t+p^n-1-p^l}\\
&+12\sum_{k,s,t,l=0}^{n-1} a_ka_sb_tb_lu^{p^t}x^{p^k+p^s+\frac{p^n-1}{2}-p^t-p^l}\\
&+6\sum_{k,s,t,l=0}^{n-1} a_ka_sb_tb_l(u^{p^t+p^l}+1)x^{p^k+p^s+p^n-1-p^t-p^l}\\
&+4\sum_{k,s,t,l=0}^{n-1} a_kb_sb_tb_l(u^{p^s+p^t+p^l}+3u^{p^s})x^{p^k+\frac{p^n-1}{2}-p^s-p^t-p^l}\\
&+4\sum_{k,s,t,l=0}^{n-1} a_kb_sb_tb_l(3u^{p^s+p^t}+1)x^{p^k+p^n-1-p^s-p^t-p^l}\\
&+\sum_{k,s,t,l=0}^{n-1} b_kb_sb_tb_l(u^{p^k+p^s+p^t+p^l}+6u^{p^k+p^s}+1)x^{p^n-1-p^k-p^s-p^t-p^l}\\
&+4\sum_{k,s,t,l=0}^{n-1} b_kb_sb_tb_l(u^{p^k+p^s+p^t}+u^{p^k})x^{\frac{p^n-1}{2}-p^k-p^s-p^t-p^l}.
\end{aligned}
\tag{36}
$$

The exponents of indeterminant x in Equality (36) have 24 kinds of possible forms, and they are the first 24 kinds of the exponents in Table 2. From this table, the weight of $\frac{p^n-1}{2}-p^k-p^s-p^t-p^l$ depends on whether the character p is 7 or not. The following discussion is divided into two subcases $p>7$ and $p=7$.

Case 1: $p>7$.

Consider the exponent $4p^i$ of weight 4, where $i\in\{0,1,\cdots,n-1\}$. By Table 2, the exponent $4p^i$ only derives from $p^k+p^s+p^t+p^l$ with $k=s=t=l=i$. Therefore, the coefficient of x^{4p^i} on the LHS of Equality (35) is equal to a_i^4, and it is zero on the RHS. This gives $a_i^4=0$, i.e., $a_i=0$.

Considering the exponent $\frac{p^n-1}{2}-4p^i$ of weight $\frac{n(p-1)}{2}-4$, by Table 2, $\frac{p^n-1}{2}-4p^i=\frac{p^n-1}{2}-p^k-p^s-p^t-p^l$ and then $k=s=t=l=i$. Since the coefficient of $x^{\frac{p^n-1}{2}-4p^i}$ on the LHS of Equality (35) is equal to $b_i^4(4u^3+4u)^{p^i}$, and it is zero on the RHS, one has

$$
b_i^4(4u^3+4u)^{p^i}=0, \tag{37}
$$

which implies that $b_i=0$ since $4u^3+4u=4u(u^2+1)\neq 0$.

Thus, Equality (35) can be rewritten as

$$
a^4=(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2(\bmod\ x^{p^n}-x). \tag{38}
$$

By analyzing the coefficients of monomials x with exponents $2p^i$ and p^n-1-2p^i in the expansion of Equality (38), one has

$$\begin{cases} c_i^2 = 0; \\ e_i^2(u^2+1)^{p^i} = 0. \end{cases} \tag{39}$$

This implies $c_i = 0$ and $e_i = 0$ for any i, and then $L_1(x, f(x)) = c$ is not a permutation. The contradiction proves that $f(x)$ is CCZ-inequivalent to $g(x) = x^d$ for $p > 7$.

Case 2: $p = 7$.

Consider the exponent $3p^i + p^j$ $(i \neq j)$ of weight 4, where $i, j \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $3p^i + p^j$ only derives from $p^k + p^s + p^t + p^l$ with $k = s = t = i$ and $l = j$. Therefore, the coefficient of $x^{3p^i+p^j}$ on the LHS of Equality (35) is equal to $4a_i^3a_j$, and it is zero on the RHS. This gives $4a_i^3a_j = 0$. If $a_{i_0} \neq 0$, then one has $a_i = 0$ for any $i \neq i_0$. That is to say, there exists at most one nonzero element in $\{a_i \mid 0 \leq i \leq n-1\}$.

Considering the exponent $p^n - 1 - 4p^i$ of weight $6n-4$, by Table 2, the exponent has two forms $p^n - 1 - p^k - p^s - p^t - p^l$ with $k = s = t = l = i$, or $p^k + p^s + p^t + p^n - 1 - p^l$ with $k = s = t = i$, $l = i+1$. Since the coefficient of $x^{p^n-1-4p^i}$ on the LHS of Equality (35) is equal to $4a_i^3b_{i+1} + b_i^4(u^4+6u^2+1)^{p^i}$, and it is zero on the RHS, one has

$$4a_i^3b_{i+1} + b_i^4(u^4+6u^2+1)^{p^i} = 0, \tag{40}$$

which implies $b_i = 0\,(i \neq i_0)$ since $a_i = 0$ for any $i \neq i_0$ and

$$u^4 + 6u^2 + 1 = (u^2+2)(u^2+4) = (u^2+3^2)(u^2+2^2) \neq 0. \tag{41}$$

For $i = i_0$, one has $b_{i_0+1} = 0$. Then, the equality $4a_{i_0}^3b_{i_0+1} + b_{i_0}^4(u^4+6u^2+1)^{p^{i_0}} = 0$ implies $b_{i_0} = 0$. Therefore, $b_i = 0$ for any i.

Consider the exponent $4p^i$ of weight 4, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $4p^i$ has the forms as $p^k + p^s + p^t + p^l$ with $k = s = t = l = i$, or $p^k + p^n - 1 - p^s - p^t - p^l$ with $k = i+1$ and $s = t = l = i$. Since the coefficient of x^{4p^i} on the LHS of Equality (35) is equal to $a_i^4 + 12a_{i+1}b_i^3u^{2p^i} + 4a_{i+1}b_i^3$, and it is zero on the RHS. This gives

$$a_i^4 + 12a_{i+1}b_i^3u^{2p^i} + 4a_{i+1}b_i^3 = 0. \tag{42}$$

Then, one has

$$a_i^4 = 0 \tag{43}$$

since $b_i = 0$ for any i. Equality (43) shows $a_i = 0$ for any $i \in \{0, 1, \cdots, n-1\}$. Thus, Equality (35) can be rewritten as

$$a^4 = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^2 \,(\bmod\, x^{p^n} - x). \tag{44}$$

Similar to the analysis after Equality (38), one has $c_i = 0$ and $e_i = 0$ for any i. Thus, $L_1(x, f(x)) = c$. That is to say, the function $f(x)$ is CCZ-inequivalent to $g(x) = x^d$ for $p = 7$.

(2) Assume that $f(x)$ and $g(x) = x^d$ are CCZ-equivalent. Squaring both sides of Equality (12) and multiplying $(c + \sum_{t=0}^{n-1} c_t x^{p^t} + \sum_{t=0}^{n-1} e_t f(x)^{p^t})^3$ for both sides imply

$$\begin{aligned} &(a + \sum_{s=0}^{n-1} a_s x^{p^s} + \sum_{s=0}^{n-1} b_s f(x)^{p^s})^2 (c + \sum_{t=0}^{n-1} c_t x^{p^t} + \sum_{t=0}^{n-1} e_t f(x)^{p^t})^3 \\ &= c + \sum_{t=0}^{n-1} c_t x^{p^t} + \sum_{t=0}^{n-1} e_t f(x)^{p^t} (\bmod\ x^{p^n} - x). \end{aligned} \tag{45}$$

We claim that there exists some integer j_0 such that $e_{j_0} \neq 0$. Otherwise, if $e_j = 0$ holds for any j, Equality (45) can be reduced to

$$(a + \sum_{s=0}^{n-1} a_s x^{p^s} + \sum_{s=0}^{n-1} b_s f(x)^{p^s})^2 (c + \sum_{t=0}^{n-1} c_t x^{p^t})^3 = c + \sum_{t=0}^{n-1} c_t x^{p^t} (\bmod\ x^{p^n} - x). \tag{46}$$

Consider the exponent $\frac{p^n-1}{2} - 2p^i + 3p^j$ $(i \neq j)$ of weight $\frac{n(p-1)}{2} + 1$. By Table 2, the exponent $\frac{p^n-1}{2} - 2p^i + 3p^j$ only has the form $p^k + p^s + p^t + \frac{p^n-1}{2} - p^l - p^v$ with $k = s = t = j$ and $l = v = i$. The coefficient of $\frac{p^n-1}{2} - 2p^i + 3p^j$ on the LHS of Equality (46) is equal to $2b_i^2 c_j^3 u^{p^i}$ and it is zero on the RHS. Thus, $b_i c_j = 0$ for any $i \neq j$.

Since $L_1(x, f(x))$ is a permutation, there exists some integer j_0 such that $c_{j_0} \neq 0$. For $i \neq j$, the equation $b_i c_j = 0$ implies that $b_i = 0$ for any i, or $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$.

When $b_i = 0$ for any i, Equality (46) is equal to

$$(a + \sum_{s=0}^{n-1} a_s x^{p^s})^2 (c + \sum_{t=0}^{n-1} c_t x^{p^t})^3 = c + \sum_{t=0}^{n-1} c_t x^{p^t}\ (\bmod\, x^{p^n} - x).$$

Since the coefficient of x^{5p^i} on the LHS of the above equality is $a_i^2 c_i^3$ and it is zero on the RHS, one has $a_i c_i = 0$. Similarly, from the coefficient of $x^{2p^i + 3p^j}$ $(i \neq j)$ in the equality above, one has $a_i^2 c_j^3 + 6a_i a_j c_i c_j^2 + 3a_j^2 c_i^2 c_j = a_i^2 c_j^3 = 0$ since $a_i c_i = 0$ for any i. Thus, $a_i c_j = 0$ for any i and j. The inequality $c_{j_0} \neq 0$ implies $a_i = 0$ for any i.

We next show $L_1(x, f(x))$ is not a permutation when $a_i = b_i = 0$ for any i.

By $a_i = b_i = 0$, Equality (12) can be reduced to

$$a = (c + \sum_{t=0}^{n-1} c_t x^{p^t} + \sum_{t=0}^{n-1} e_t f(x)^{p^t})^{\frac{p^n-1}{2} - 1} (\bmod\ x^{p^n} - x). \tag{47}$$

Since $\gcd(\frac{p^n-1}{2} - 1, p^n - 1) = 2$, there exists an integer λ such that $\lambda(\frac{p^n-1}{2} - 1) \equiv 2 (\bmod\ p^n - 1)$. Thus, from Equality (47), one has

$$a^\lambda = (c + \sum_{t=0}^{n-1} c_t x^{p^t} + \sum_{t=0}^{n-1} e_t f(x)^{p^t})^2\ (\bmod\ x^{p^n} - x).$$

By the analysis after Equality (38), one has $c_i = 0$ and $e_i = 0$ for any i. Thus $L_1(x, f(x)) = c$ is not a permutation.

When $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$, Equality (46) becomes

$$(a + \sum_{s=0}^{n-1} a_s x^{p^s} + b_{j_0} f(x)^{p^{j_0}})^2 (c + c_{j_0} x^{p^{j_0}})^3 = c + c_{j_0} x^{p^{j_0}} (\bmod\ x^{p^n} - x). \tag{48}$$

Consider the coefficient of $x^{2p^i + 3p^{j_0}}$ $(i \neq j_0)$ in Equality (48), one has $a_i^2 c_{j_0}^3 = 0$. This implies $a_i = 0$ for $i \neq j_0$ since $c_{j_0} \neq 0$. Thus, Equality (48) becomes

$$(a + a_{j_0} x^{p^{j_0}} + b_{j_0} f(x)^{p^{j_0}})^2 (c + c_{j_0} x^{p^{j_0}})^3 = c + c_{j_0} x^{p^{j_0}} (\bmod\ x^{p^n} - x). \tag{49}$$

From the coefficients of $x^{5p^{j_0}}$ and $x^{3p^{j_0}}$ in Equality (49), one has

$$\begin{cases} a_{j_0}^2 c_{j_0}^3 = 0; \\ a^2 c_{j_0}^3 + 6aca_{j_0} c_{j_0}^2 + 3c^2 a_{j_0}^2 c_{j_0} = 0, \end{cases}$$

which implies $a_{j_0} = a = 0$. Furthermore, from the coefficient of $x^{\frac{p^n-1}{2} - 2p^{j_0} + 3p^{j_0}}$, one has $b_{j_0}^2 c_{j_0}^3 = 0$. This is a contradiction.

Therefore, there exists some integer j_0 such that $e_{j_0} \neq 0$.

Since the weights of some exponents in Table 2 depend on the concrete values of p and n, the following discussion will be divided into three subcases: (1) $p > 7$; (2) $p = 7$ and $n \geq 5$; (3) $p = 7$ and $n = 3$.

Case 1: $p > 7$.

Consider the exponent $\frac{p^n-1}{2} - 5p^i$ of weight $\frac{n(p-1)}{2} - 5$, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $\frac{p^n-1}{2} - 5p^i$ only has the form as $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v$ with $k = s = t = l = v = i$. Since the coefficient of $x^{\frac{p^n-1}{2}-5p^i}$ on the LHS of Equality (45) is equal to $b_i^2 e_i^3 (u^5 + 10u^3 + 5u)^{p^i}$, and it is zero on the RHS, one has

$$b_i^2 e_i^3 (u^5 + 10u^3 + 5u)^{p^i} = 0. \tag{50}$$

Similarly, comparing the coefficients of $x^{p^n-1-5p^i}$ on both sides of Equality (45), one has

$$b_i^2 e_i^3 (5u^4 + 10u^2 + 1)^{p^i} = 0. \tag{51}$$

By Lemma 5, Equalities (50) and (51) imply that $b_i e_i = 0$ for any i.

Since $b_i e_i = 0$ for any i, the coefficient of $x^{\frac{p^n-1}{2}-2p^i-3p^j} (i \neq j)$ on the LHS of Equality (45) is

$$\begin{aligned} & (b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}) \\ = \; & b_i^2 e_j^3 ((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}), \end{aligned}$$

and it is zero on the RHS. Thus, one has

$$b_i^2 e_j^3 ((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}) = 0. \tag{52}$$

Similarly, from the coefficient of $x^{p^n-1-2p^i-3p^j} (i \neq j)$, one has

$$\begin{aligned} & (b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)((u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}) \\ = \; & b_i^2 e_j^3 ((u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}) = 0. \end{aligned} \tag{53}$$

By Equalities (52) and (53), we claim that $b_i e_j = 0$ for any $i \neq j$. Otherwise, there exist two integers i, j such that $b_i e_j \neq 0$. Then, one has

$$\begin{cases} (u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j} = 0; \\ (u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j} = 0, \end{cases} \tag{54}$$

which implies

$$\begin{aligned} & ((u^3+3u)(3u^2+1))^{p^j}((u^2+1)^2 - 4u^2)^{p^i} \\ = \; & ((u^3+3u)(3u^2+1))^{p^j}(u^2-1)^{2p^i} = 0. \end{aligned} \tag{55}$$

By Equality (54), if one of u^3+3u and $3u^2+1$ is zero, the other is also zero, which contradicts with Lemma 5. Thus, one has $(u^3+3u)(3u^2+1) \neq 0$. Equality (55) gives $u^2 - 1 = 0$. This is a contradiction with $u \neq \pm 1$. Therefore, $b_i e_j = 0$ holds for any $i \neq j$. By $b_i e_i = 0$, one has $b_i e_j = 0$ for any i and j. Since there exists some integer j_0 such that $e_{j_0} \neq 0$, one has $b_i = 0$ for any i.

Consider the exponent $5p^i$ of weight 5, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $5p^i$ only has the form as $p^k + p^s + p^t + p^l + p^v$ with $k = s = t = l = v = i$. Since the coefficient of x^{5p^i} on the LHS of Equality (45) is equal to $a_i^2 c_i^3$, and it is zero on the RHS, one has $a_i^2 c_i^3 = 0$ for any i. Similarly, considering the coefficient of $x^{2p^i+3p^j} (i \neq j)$, one has

$$a_i^2 c_j^3 + 6a_i a_j c_i c_j^2 + 3a_j^2 c_i^2 c_j = a_i^2 c_j^3 = 0. \tag{56}$$

Thus, $a_i = 0$ for any i or $c_j = 0$ for any j.

Similarly as described in Equality (47), $L_1(x, f(x))$ is not a permutation if $a_i = b_i = 0$ for any i. Thus, there exists a nonzero element in $\{a_i \,|\, 0 \le i \le n-1\}$. Then, $c_j = 0$ for any j. From the coefficients of $x^{p^n-1-3p^j+2p^i} (i \neq j)$ and $x^{\frac{p^n-1}{2}-3p^j+2p^i} (i \neq j)$, one has

$$\begin{cases} (a_i^2e_j^3 + 6a_ib_jc_ie_j^2 + 3b_j^2c_i^2e_j)(3u^2+1)^{p^j} = 0; \\ (a_i^2e_j^3 + 6a_ib_jc_ie_j^2 + 3b_j^2c_i^2e_j)(u^3+3u)^{p^j} = 0. \end{cases}$$

Since $c_j = 0$ for any j, the equality above becomes

$$\begin{cases} a_i^2e_j^3(3u^2+1)^{p^j} = 0; \\ a_i^2e_j^3(u^3+3u)^{p^j} = 0, \end{cases}$$

which implies that $a_ie_j = 0$ for any $i \neq j$ by Lemma 5. Thus, by $e_{j_0} \neq 0$, one has $a_{j_0}e_{j_0} \neq 0$ and $a_j = e_j = 0$ for any $j \neq j_0$. Equality (45) can be reduced to

$$(a + a_{j_0}x^{p^{j_0}})^2(c + e_{j_0}f(x)^{p^{j_0}})^3 = c + e_{j_0}f(x)^{p^{j_0}} \pmod{x^{p^n} - x}. \tag{57}$$

From the coefficients of $x^{\frac{p^n-1}{2}-3p^{j_0}}$ and $x^{p^n-1-3p^{j_0}}$ in Equality (57), one has

$$\begin{cases} a^2e_{j_0}^3(u^3+3u)^{p^{j_0}} = 0; \\ a^2e_{j_0}^3(3u^2+1)^{p^{j_0}} = 0, \end{cases} \tag{58}$$

which implies $a = 0$. Considering the coefficients of $x^{\frac{p^n-1}{2}-p^{j_0}}$ and $x^{p^n-1-p^{j_0}}$, one has

$$\begin{cases} a_{j_0}^2e_{j_0}^3(u^3+3u)^{p^{j_0}} = e_{j_0}u^{p^{j_0}}; \\ a_{j_0}^2e_{j_0}^3(3u^2+1)^{p^{j_0}} = e_{j_0}, \end{cases} \tag{59}$$

which implies

$$a_{j_0}^2e_{j_0}^3u^{p^{j_0}}(-2u^2+2)^{p^{j_0}} = -2a_{j_0}^2e_{j_0}^3u^{p^{j_0}}(u^2-1)^{p^{j_0}} = 0.$$

This gives $a_{j_0}e_{j_0} = 0$ since $u(u^2-1) \neq 0$. It's impossible.

According to the arguments above, $f(x)$ and $g(x) = x^{\frac{p^n-1}{2}-1}$ are CCZ-inequivalent on F_{p^n} when $p > 7$ and n is odd.

Case 2: $p = 7, n \ge 5$.

Consider the exponent $\frac{p^n-1}{2} - 2p^i - 3p^j$ $(i \neq j)$ of weight $3n-5$, where $i, j \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $\frac{p^n-1}{2} - 2p^i - 3p^j$ only has the form as $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v$ for some $k, s, t, l, v \in \{0, 1, \cdots, n-1\}$. Since the coefficient of $x^{\frac{p^n-1}{2}-2p^i-3p^j}$ on the LHS of Equality (45) is equal to

$$(b_i^2e_j^3 + 6b_ib_je_ie_j^2 + 3b_j^2e_i^2e_j)((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j})$$

and it is zero on the RHS, one has

$$(b_i^2e_j^3 + 6b_ib_je_ie_j^2 + 3b_j^2e_i^2e_j)((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}) = 0. \tag{60}$$

Similarly, for the exponent $p^n - 1 - 2p^i - 3p^j$, one has

$$(b_i^2e_j^3 + 6b_ib_je_ie_j^2 + 3b_j^2e_i^2e_j)((u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}) = 0. \tag{61}$$

By the analysis in Case 1, Equalities (60) and (61) imply

$$b_i^2e_j^3 + 6b_ib_je_ie_j^2 + 3b_j^2e_i^2e_j = ((b_ie_j + 3b_je_i)^2 + b_j^2e_i^2)e_j = 0. \tag{62}$$

For $j = j_0$, since $e_{j_0} \neq 0$ and -1 is nonsquare, one has $b_ie_{j_0} + 3b_{j_0}e_i = b_{j_0}e_i = 0$, i.e.,

$$b_ie_{j_0} = b_{j_0}e_i = 0. \tag{63}$$

This implies that $b_i = 0$ for any i, or $b_{j_0} \neq 0$ and $b_i = e_i = 0$ for any $i \neq j_0$.

From the coefficient of the monomial with exponent $2p^i + \frac{p^n-1}{2} - 3p^j$ $(i \neq j)$, one has

$$(a_i^2 e_j^3 + 6a_i b_j c_i e_j^2 + 3b_j^2 c_i^2 e_j)(u^3 + 3u)^{p^j} = 0. \tag{64}$$

Since -1 is a nonsquare element in F_{p^n}, one has $\chi(3) = \chi(-4) = -1$. We say $u^3 + 3u \neq 0$. Otherwise, $u = 2$ or 5 and then $\chi(u+1) \neq \chi(u-1)$. This is a contradiction. Therefore, Equality (64) implies that

$$a_i^2 e_j^3 + 6a_i b_j c_i e_j^2 + 3b_j^2 c_i^2 e_j = ((a_i e_j + 3b_j c_i)^2 + b_j^2 c_i^2) e_j = 0. \tag{65}$$

For $j = j_0$, one has $a_i e_{j_0} + 3b_{j_0} c_i = b_{j_0} c_i = 0$ since -1 is a nonsquare element, i.e., $a_i = 0$ for any $i \neq j_0$. If $b_{j_0} \neq 0$, then $c_i = 0$ for any $i \neq j_0$. If $b_i = 0$ for any i, Equality (65) can be reduced to $a_i e_j = 0$.

According to the discussion after Equalities (63) and (65), we derive that $b_i = 0$ for any i and $a_i e_j = 0$ for any $i \neq j$, or $b_{j_0} \neq 0$ and $a_i = b_i = c_i = e_i = 0$ for any $i \neq j_0$.

Assume that $b_i = 0$ for any i and $a_i e_j = 0$ for any $i \neq j$. If $a_{j_0} = 0$, i.e., $a_i = 0$ for any i since $e_{j_0} \neq 0$, then $L_1(x, f(x)) = c$ is not a permutation. If $a_{j_0} \neq 0$, then $a_{j_0} e_j = 0$ implies $e_j = 0$ for any $j \neq j_0$. Therefore, Equality (45) can be reduced to

$$(a + a_{j_0} x^{p^{j_0}})^2 (c + \sum_{i=0}^{n-1} c_i x^{p^i} + e_{j_0} f(x)^{p^{j_0}})^3 = c + \sum_{i=0}^{n-1} c_i x^{p^i} + e_{j_0} f(x)^{p^{j_0}} \pmod{x^{p^n} - x}. \tag{66}$$

Considering the coefficients of the monomials with exponents $\frac{p^n-1}{2} - 3p^{j_0}$, $p^n - 1 - 3p^{j_0}$, $\frac{p^n-1}{2} - p^{j_0}$ and $p^n - 1 - p^{j_0}$ in Equality (66), one has that Equalities (58) and (59) hold. Then, $a_{j_0} e_{j_0} = 0$, which is impossible.

Assume that $b_{j_0} \neq 0$ and $a_i = b_i = c_i = e_i = 0$ for any $i \neq j_0$. Equality (45) can be reduced to

$$(a + a_{j_0} x^{p^{j_0}} + b_{j_0} f(x)^{p^{j_0}})^2 (c + c_{j_0} x^{p^{j_0}} + e_{j_0} f(x)^{p^{j_0}})^3 = c + c_{j_0} x^{p^{j_0}} + e_{j_0} f(x)^{p^{j_0}} \pmod{x^{p^n} - x}. \tag{67}$$

Considering the coefficients of $x^{\frac{p^n-1}{2} - 5p^{j_0}}$ and $x^{p^n - 1 - 5p^{j_0}}$ in Equality (67), one has

$$\begin{cases} b_{j_0}^2 e_{j_0}^3 (u^5 + 10u^3 + 5u)^{p^{j_0}} = 0; \\ b_{j_0}^2 e_{j_0}^3 (5u^4 + 10u^2 + 1)^{p^{j_0}} = 0, \end{cases}$$

which implies $b_{j_0} e_{j_0} = 0$ by Lemma 5. That's a contradiction with $b_{j_0} e_{j_0} \neq 0$. Therefore, $f(x)$ and $g(x) = x^{\frac{p^n-1}{2} - 1}$ are CCZ-inequivalent on F_{7^n}, where $n \geq 5$ is odd.

Case 3: $p = 7, n = 3$.

For all integers i, j with $0 \leq i \neq j \leq 2$, considering the coefficients of $x^{2p^i + \frac{p^n-1}{2} - 3p^j}$, it can be similarly proven that Equalities (64) and (65) hold. From these two equalities, one has

$$a_i e_j = e_j b_j c_i = 0, \ i \neq j. \tag{68}$$

Considering the exponent $\frac{p^n-1}{2} - 2p^i - 3p^j$ $(i \neq j)$, where $i, j = 0, 1, 2$, it has two forms $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v$, and $p^k + p^s + p^t + p^l$ with $k = i$ and $w \neq i, j$, where $w = s = t = l$. Then, its coefficients on both sides of Equality (45) give

$$\begin{aligned}(b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)[(u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}] \\ + 2aa_i c_w^3 + 6a_i a_w c c_w^2 + 6aa_w c_i c_w^2 + 6a_w^2 c c_i c_w = 0.\end{aligned} \tag{69}$$

For $i, j = 0, 1, 2$, considering the exponent $p^n - 1 - 2p^i - 3p^j$ $(i \neq j)$, it has a unique form $p^n - 1 - p^k - p^s - p^t - p^l - p^v$. Then, its coefficients on both sides of Equality (45) give

$$(b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)[(u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}] = 0. \tag{70}$$

Considering the coefficients of the monomials with exponents $p^n-1-2p^i+3p^{i+1}(=19,133,247)$, one has

$$\left\{\begin{array}{l}(3a_1^2c_1e_0^2+6a_1b_0c_1^2e_0+b_0^2c_1^3)(u^2+1)=0;\\(3a_2^2c_2e_1^2+6a_2b_1c_2^2e_1+b_1^2c_2^3)(u^2+1)^7=0;\\(3a_0^2c_0e_2^2+6a_0b_2c_0^2e_2+b_2^2c_0^3)(u^2+1)^{49}=0.\end{array}\right. \tag{71}$$

Since $u^2+1\neq 0$ and $a_ie_j=0$ for any $i\neq j$, one has

$$b_0^2c_1^3=b_1^2c_2^3=b_2^2c_0^3=0.$$

Therefore, there exist eight possible cases as follows.

1) $c_0=c_1=c_2=0$;
2) $c_1=c_2=b_2=0$, $c_0\neq 0$;
3) $c_2=c_0=b_0=0$, $c_1\neq 0$;
4) $c_0=c_1=b_1=0$, $c_2\neq 0$;
5) $c_1=b_1=b_2=0$, $c_0c_2\neq 0$;
6) $c_2=b_2=b_0=0$, $c_1c_0\neq 0$;
7) $c_0=b_0=b_1=0$, $c_2c_1\neq 0$;
8) $b_0=b_1=b_2=0$, $c_0c_1c_2\neq 0$.

We only give the analysis of Cases 1), 2), 5), and 8). The Cases 3), 4), 6), and 7) can be similarly analyzed.

1) Considering the exponent $\frac{p^n-1}{2}-5p^i\,(=5+2p+3p^2,3+5p+2p^2,2+3p+5p^2)$ of weight 10, it has 4 possible forms as $p^k+p^s+\frac{p^n-1}{2}-p^t$, $p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$, $p^k+p^n-1-p^s-p^t-p^l$, and $\frac{p^n-1}{2}-p^k-p^s-p^t-p^l-p^v$ where $k,s,t,l,v\in\{0,1,2\}$.

If $p^k+p^s+\frac{p^n-1}{2}-p^t\equiv\frac{p^n-1}{2}-5p^i\,(\mathrm{mod}\,p^n-1)$, one has $k=s=i$, $t=i+1$. Then, the coefficient of the monomial with exponent $p^k+p^s+\frac{p^n-1}{2}-p^t$ is

$$3a_i^2c^2e_{i+1}+12aa_icc_ie_{i+1}+6a_ib_{i+1}c^2c_i+3a^2c_i^2e_{i+1}+6ab_{i+1}cc_i^2+6a_ib_{i+1}c^2c_i=0$$

since $c_i=0$ and $a_ie_j=0$. Also by $c_i=0$, the coefficient of the monomial with exponent $p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$ is equal to 0.

If $\frac{p^n-1}{2}-5p^i\equiv p^k+p^n-1-p^s-p^t-p^l\,(\mathrm{mod}\,p^n-1)$, one has $x^{p^k+p^n-1-p^s-p^t-p^l}=x^{\frac{p^n-1}{2}-5p^i}$ and then $x^{p^k+\frac{p^n-1}{2}+5p^i}=x^{p^s+p^t+p^l}$. By a direct calculation, $p^k+\frac{p^n-1}{2}+5p^i\,(\mathrm{mod}\,p^n-1)$ is of weight 9, while the weight of $p^s+p^t+p^l$ is 3. This is impossible.

If $\frac{p^n-1}{2}-p^k-p^s-p^t-p^l-p^v\equiv\frac{p^n-1}{2}-5p^i\,(\mathrm{mod}\,p^n-1)$, one has $k=s=t=l=v=i$. The coefficient of the monomial with such an exponent is equal to $b_i^2e_i^3(u^5+10u^3+5u)^{p^i}$ on the LHS of Equality (45), and it is zero on the RHS.

By the analysis above, the coefficients of $\frac{p^n-1}{2}-5p^i$ on the both sides of Equality (45) satisfy the following equation

$$b_i^2e_i^3(u^5+10u^3+5u)^{p^i}=0.$$

A similar discussion for the exponent p^n-1-5p^i shows

$$b_i^2e_i^3(5u^4+10u^2+1)^{p^i}=0.$$

The two equalities imply $b_ie_i=0$ for any i.

Since $c_i=0$ and $b_ie_i=0$ for any i, Equalities (69) and (70) give

$$\left\{\begin{array}{l}b_i^2e_j^3((u^2+1)^{p^i}(u^3+3u)^{p^j}+2u^{p^i}(3u^2+1)^{p^j})=0;\\b_i^2e_j^3((u^2+1)^{p^i}(3u^2+1)^{p^j}+2u^{p^i}(u^3+3u)^{p^j})=0.\end{array}\right.$$

From Equalities (52) and (53), one has $b_ie_j=0$.

Therefore, one has $b_ie_j = 0$ for any i and j, i.e., $b_i = 0$ for any i since $e_{j_0} \neq 0$.

The exponent $2p^i$ has the possible form as $p^k + p^s$, or $p^k + p^s + p^t + p^n - 1 - p^l$, where $k, s, t, l \in \{0, 1, 2\}$. If $p^k + p^s = 2p^i$, then one has $k = s = i$. If $p^k + p^s + p^t + p^n - 1 - p^l \equiv 2p^i \pmod{p^n - 1}$, then one has $k = s = i$, $t = l$. Since $c_i = 0$ for all i, the coefficient of the monomial $x^{p^k+p^s+p^t+p^n-1-p^l}$ is zero. Therefore, the exponent of x^{2p^i} only has form as $p^k + p^s$ with $k = s = i$. Thus, one has

$$a_i^2c^3 + 6aa_ic^2c_i + 3a^2cc_i^2 = a_i^2c^3 = 0,$$

which implies $c = 0$ or $a_i = 0$ for any i. By Equality (68), there exists at most one nonzero element among a_0, a_1 and a_2. If $a_i = 0$ for any i, then $L_1(x, f(x)) = c$ is not a permutation. If some $a_{j_0} \neq 0$, then $c = 0$ and $a = c^{\frac{p^n-1}{2}-1}$ implying $a = 0$. Thus, Equality (45) is reduced to

$$a_{j_0}^2 x^{2p^{j_0}} (\sum_{i=0}^{n-1} e_i f(x)^{p^i})^3 = \sum_{i=0}^{n-1} e_i f(x)^{p^i} \pmod{x^{p^n} - x}.$$

Comparing the coefficients of $x^{\frac{p^n-1}{2}-p^{j_0}}$ and $x^{p^n-1-p^{j_0}}$ on both sides of equality above, one has

$$\begin{cases} a_{j_0}^2 e_{j_0}^3 (u^3 + 3u)^{p^{j_0}} = e_{j_0} u^{p^{j_0}}; \\ a_{j_0}^2 e_{j_0}^3 (3u^2 + 1)^{p^{j_0}} = e_{j_0}. \end{cases}$$

Since $a_{j_0}e_{j_0} \neq 0$ and $u \neq 0$, one has $u^3 + 3u = (3u^2 + 1)u$, i.e., $u = \pm 1$. This is impossible.

2) In this case, Equality (45) is reduced to

$$\begin{aligned} &(a + \sum_{i=0}^{n-1} a_i x^{p^i} + b_0 f(x) + b_1 f(x)^p)^2 (c + c_0 x + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^3 \\ &\quad = c + c_0 x + \sum_{i=0}^{n-1} e_i f(x)^{p^i} \pmod{x^{p^n} - x}. \end{aligned} \tag{72}$$

By Equality (68), there exists at most one nonzero element among a_0, a_1, a_2.

If $a_1 = a_2 = 0$, the coefficient of x^5 satisfies $a_0^2c_0^3 = 0$ and then $a_0 = 0$ since $c_0 \neq 0$. The coefficient of x^3 satisfies $a^2c_0^3 = 0$, and then $a = 0$. The coefficient of x^{172} satisfies $2b_0^2c_0^3u = 0$, which implies $b_0 = 0$. Thus, the coefficient of x satisfies $c_0 = 0$, and it contradicts with the fact $c_0 \neq 0$.

If $a_1 = 0$ and $a_2 \neq 0$, one also has $a_0 = 0$. By Equality (68), the equality $a_2e_j = 0$ implies $e_0 = e_1 = 0$. Considering the coefficient of x^{101}, one has $a_2^2c_0^3 = 0$. This contradicts with $a_2c_0 \neq 0$.

If $a_1 \neq 0$ and $a_2 = 0$, then one has $a_0 = 0$. By Equality (68), the equality $a_1e_j = 0$ implies $e_0 = e_2 = 0$. Considering the coefficient of x^{17}, one has $a_1^2c_0^3 = 0$. This contradicts with $a_1c_0 \neq 0$.

5) In this case, Equality (45) can be rewritten as

$$\begin{aligned} &(a + \sum_{i=0}^{n-1} a_i x^{p^i} + b_0 f(x))^2 (c + c_0 x + c_2 x^{p^2} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^3 \\ &\quad = c + c_0 x + c_2 x^{p^2} + \sum_{i=0}^{n-1} e_i f(x)^{p^i} \pmod{x^{p^n} - x}. \end{aligned} \tag{73}$$

Considering the coefficient of x^{17}, the coefficient on the LHS of Equality (73) is equal to $a_1^2c_0^3$ and it is zero on the RHS. Thus, one has $a_1^2c_0^3 = 0$ and then $a_1 = 0$ since $c_0 \neq 0$. Similarly, the coefficient of x^{101} satisfies

$$a_2^2c_0^3 + 6a_0a_2c_0c_2^2 + 3a_0^2c_0c_2^2 = ((a_2c_0 + 3a_0c_2)^2 + a_0^2c_2^2)c_0 = 0.$$

Since $c_0 \neq 0$ and -1 is nonsquare, one has $a_2c_0 + 3a_0c_2 = a_0c_2 = 0$, i.e., $a_0 = a_2 = 0$ since $c_0c_2 \neq 0$. Thus, Equality (73) can be reduced to

$$(a+b_0f(x))^2(c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^3 = c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1}e_if(x)^{p^i} \pmod{x^{p^n}-x}. \quad (74)$$

From the coefficient of x^3 in Equality (74), one has $a^2c_0^3 = 0$. Thus, $a = 0$ and then $c = 0$. The coefficient of x^{172} satisfies $2b_0^2c_0^3u = 0$. This gives $b_0 = 0$ and then $a_i = b_i = 0$ for any i. By similar arguments after Equality (47), one has $L_1(x, f(x)) = c$. That's a contradiction.

8) In this case, Equality (45) is rewritten as

$$(a+\sum_{i=0}^{n-1}a_ix^{p^i})^2(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^3 = c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i} \pmod{x^{p^n}-x}. \quad (75)$$

If $a_0 \neq 0$, then $a_1 = a_2 = 0$. By considering the monomial with exponent 53 of weight 5, one has $3a_0^2c_0^2c_2 = 0$, which implies that $a_0 = 0$ since $c_0c_2 \neq 0$. This is impossible.

Similarly, if $a_1 \neq 0$, then $a_0 = a_2 = 0$. By considering the monomial with exponent $29 \equiv 53 \cdot 7 \pmod{342}$, one has $a_1 = 0$. If $a_2 \neq 0$, one has $a_0 = a_1 = 0$. By considering the monomial with exponent $203 \equiv 53 \cdot 7^2 \pmod{342}$, one has $a_2 = 0$.

From the arguments of Cases 1-8, $f(x)$ and $g(x) = x^{\frac{p^n-1}{2}-1}$ are CCZ-inequivalent on F_{7^3}.

This finally finishes the proof of Proposition 2. □

As far as the authors are aware, all known APN functions over finite fields of odd characteristic only include those listed in Table 1 and the family in [23]. By Propositions 1, 2 and Corollary 1, for $p \geq 7$, the proposed functions $f(x)$ are CCZ-inequivalent to all known APN power mappings. Therefore, these functions are also CCZ-inequivalent to all known APN mappings.

4. Conclusion And Further Work

This paper proved an infinite family of mappings over finite fields of odd characteristic is almost perfect nonlinear. For $p \geq 7$, the proposed functions are CCZ-inequivalent to all known APN power mappings. Further work needs for the inequivalence within the proposed family of APN functions, and the inequivalence between the proposed family in fields of characteristic 3 and all known APN functions.

References

[1] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," *Cryptology ePrint Archive:*, Rep. 2007/098, 2007.

[2] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions over F_{2^n}," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4160-4170, Sept. 2006.

[3] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, "An infinite class of quadratic APN functions which are not equivalent to power mappings," *Proceedings of the IEEE International Symposium on Information Theory 2006*, Settle, USA, pp. 2637-2641, July 2006.

[4] L. Budaghyan, C. Carlet, and G. Leander, "Another class of quadratic APN binomials over F_{2^n}: the case n divisible by 4," *Cryptology ePrint Archive:*, Rep. 2006/428, 2006.

[5] L. Budaghyan, C. Carlet, and G. Leander, "A class of quadratic APN binomials inequivalent to power functions," *Cryptology ePrint Archive:*, Rep. 2006/445, 2006.

[6] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," *Cryptology ePrint Archive:*, Rep. 2007/063, 2007.

[7] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[8] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science).* Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 65-76.

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

[10] C. Carlet, P. Charpin and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125-156, 1998.

[11] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): The Welch case," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271-1275, May 1999.

[12] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): A new case for n divisible 5," in *Proceedings of Finite Fields and Applications FQ5*, D. Jungnickel and H. Niederreiter, Eds. Augsburg, Germany: Springer-Verlag, 2000, pp. 113-121.

[13] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): The Niho case," *Inf. Comput.*, vol. 151, pp. 57-72, 1999.

[14] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, and W. Willems, "APN functions in odd characteristic," *Discr. Math.*, vol. 267, pp. 95-112, 2003.

[15] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 744-747, Feb. 2006.

[16] P. Felke, "Computing the uniformity of power mappings: a systematic approach with the multi-variate method over finite fields of odd characteristic," Ph. D. dissertation, University of Bochum, Bochum, Germany, 2005.

[17] R. Gold, "Maximal recursive sequence with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154-156, Jan. 1968.

[18] 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, March 1999.

[19] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, pp. 363-370, 1997.

[20] H. Janwa and R. Wilson, "Hyperplane sections of fermat varieties in P^3 in Char. 2 and some applications to cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 673, pp. 180-194, 1993.

[21] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes," *Inf. Contr.*, vol. 18, pp. 369-394, 1971.

[22] R. Lidl and H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20. Reading, MA: Addison-Wesley, 1983.

[23] G. J. Ness and T. Helleseth, "A new family of ternary almost perfect nonlinear mappings," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2581-2586, July 2007.

[24] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science).* Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 55-64.