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, 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 mapping 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-equivalent, 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 of $\{(x, f_1(x)) \,|\, x \in F_{p^n}\}$ 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

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

CCZ-equivalence is a more general equivalent relation of functions than EA-equivalence, and it keeps APN properties 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-transformation 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 over $F_{2^{10}}$ and $F_{2^{12}}$, respectively. Recently, binary APN functions are extensively studied, and some functions are proven to be CCZ-inequivalent to all known APN functions [1]-[6]. Some nonbinary APN mappings are also found in [14, 18, 19].

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).

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 $p\equiv 2 \pmod 3$	[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	$\frac{p^n-1}{2}-1$	$p\equiv 3,7 \pmod{20}$, $p^n>7$, $p^n\neq 27$ and n is odd	[19]
Dobbertin et. al. Felke	$\frac{3^{(n+1)/2}-1}{2}$ $\frac{3^{(n+1)/2}-1}{2}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 3 \pmod 4$ $p=3$, $n\equiv 1 \pmod 4$	[14] [16]
Dobbertin et. al.	$\frac{3^{n+1}-1}{8}$ $\frac{3^{n+1}-1}{8}+\frac{3^n-1}{2}$	$p=3$, $n\equiv 3 \pmod 4$ $p=3$, $n\equiv 1 \pmod 4$	[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	$p^n\equiv 3 \pmod 8$ $p^n\equiv 7 \pmod 8$ $p^n\equiv 2 \pmod 3$ $p=3$, $n>1$, n is odd	[18]
Trival	3	$p>3$	[19]

In this paper, for a prime $p\equiv 3 \pmod 4$ and an odd n, 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

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

When $p=3$, 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 functions.

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 known APN functions. Section 4 concludes the study.

2. A New Family of APN mapping over F_{p^n}

In this section, a family of functions defined by Equality (1) will be proven to be APN.

The following lemma in [22] on page 223 will be used to prove result in this paper.

Lemma 1: Let $f(x)\in F_{p^n}[x]$ be of degree $d\geq 1$ with $\gcd(d,p^n)=1$ and let χ be a nontrivial character of F_{p^n}. Then

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

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

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

Thus, 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 satisfying the condition in Equality (2) [23]. The number of such elements u for other cases is characterized by the following lemma.

Lemma 2: For an integer $n \geq 3$ and $p \geq 7$, let N be the number of elements $u \in F_{p^n}$ satisfying the condition in Equality (2). Then,

$$\frac{1}{8}(3p^n - 37p^{n/2} - 152) \leq N \leq \frac{1}{8}(3p^n + 37p^{n/2} + 136).$$

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

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

and Γ the set consisting of all zeroes of the three polynomials $u+1$, $u-1$ and $5u+3$. Then, one has $|\Gamma| = 3$. By Lemma 1, one has

$$\begin{aligned}
8N_1 &= \sum_{u \in F_{p^n} \setminus \Gamma} (1+\chi(u+1))(1+\chi(u-1))(1-\chi(5u+3)) \\
&= \sum_{u \in F_{p^n} \setminus \Gamma} 1 + \sum_{u \in F_{p^n} \setminus \Gamma} \chi(u+1) + \sum_{u \in F_{p^n} \setminus \Gamma} \chi(u-1) - \sum_{u \in F_{p^n} \setminus \Gamma} \chi(5u+3) \\
&\quad + \sum_{u \in F_{p^n} \setminus \Gamma} \chi(u^2-1) - \sum_{u \in F_{p^n} \setminus \Gamma} \chi((u+1)(5u+3)) - \sum_{u \in F_{p^n} \setminus \Gamma} \chi((u-1)(5u+3)) \\
&\quad - \sum_{u \in F_{p^n} \setminus \Gamma} \chi((u+1)(u-1)(5u+3)) \\
&\geq (p^n - 3) - 3 \cdot 3 - 3 \cdot (p^{n/2} + 3) - (2p^{n/2} + 3) \\
&= p^n - 5p^{n/2} - 24,
\end{aligned}$$

and

$$\begin{aligned}
8N_1 &\leq (p^n - |\Gamma|) + 3 \cdot |\Gamma| + 3 \cdot (p^{n/2} + |\Gamma|) + (2p^{n/2} + |\Gamma|) \\
&= p^n + 5p^{n/2} + 6|\Gamma| \\
&\leq p^n + 5p^{n/2} + 18.
\end{aligned}$$

Let N_2, N_3 and N_4 be the number 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.

Similarly, one has

$$\tfrac{1}{8}(p^n - 5p^{n/2} - 24) \leq N_i \leq \tfrac{1}{8}(p^n + 5p^{n/2} + 18), \ i = 2, 3, 4.$$

Let N_5 and N_6 be the number 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

$$\tfrac{1}{16}(p^n - 17p^{n/2} - 64) \leq N_i \leq \tfrac{1}{16}(p^n + 17p^{n/2} + 56)$$

for $i = 5$, 6.

Thus, the range of the value N can be measured as follows:

$$\begin{aligned}
N &= N_1 + N_2 + N_3 + N_4 - N_5 - N_6 \\
&\geq 4 \cdot \tfrac{1}{8}(p^n - 5p^{n/2} - 24) - 2 \cdot \tfrac{1}{16}(p^n + 17p^{n/2} + 56) \\
&= \tfrac{1}{8}(3p^n - 37p^{n/2} - 152)
\end{aligned}$$

and

$$\begin{aligned}
N &\leq 4 \cdot \tfrac{1}{8}(p^n + 5p^{n/2} + 18) - 2 \cdot \tfrac{1}{16}(p^n - 17p^{n/2} - 64) \\
&= \tfrac{1}{8}(3p^n + 37p^{n/2} + 136).
\end{aligned}$$

This finishes the proof. □

Remark 1: For $n \geq 3$ and $p \geq 7$, one has

$$\begin{aligned} N &\geq (3p^n - 37p^{n/2} - 152)/8 \\ &> (3 \times 7^{n/2}p^{n/2} - 37p^{n/2} - 152)/8 \\ &= (17p^{n/2} - 152)/8 \\ &> (17 \times 18 - 152)/8 \\ &> 19. \end{aligned}$$

This shows that in this case, there also exist elements u satisfying the condition in Equality (2). When n and p are large enough, N is about as large as $\frac{3p^n}{8}$.

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 an odd $n \geq 3$ and a prime p with $p \equiv 3 (\mathrm{mod}\ 4)$, if $u \in F_{p^n}$ satisfies the condition in Equality (2), then the mapping $f(x)$ defined by Equality (1) is APN.

Proof: To finish the proof, it is sufficient 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) $(\chi(x+a), \chi(x)) = (1, 1)$:

$$bx^2 + abx + a(u+1) = 0; \tag{5}$$

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 $x = 0$, one has

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

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 $ab = 1 - u$.

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

For a prime $p \equiv 3 (\mathrm{mod}\, 4)$ and an odd $n \geq 3$, one has $\frac{p^n-1}{2} \equiv 1 (\mathrm{mod}\, 2)$ and $\chi(-1) = -1$. For the element u satisfying the condition in the theorem, one has $u \neq \pm 1$. Otherwise, $\chi(u+1) = \chi(2) \neq \chi(0) = \chi(u-1)$ for $u = 1$ and $\chi(u-1) = \chi(-2) \neq \chi(0) = \chi(u+1)$ for $u = -1$, which contradicts with $\chi(u+1) = \chi(u-1)$. Thus, neither $x = 0$ nor $-a$ is the zero of Equation (3).

When $b = 0$, Equations (5) and (6) have no solutions. Equations (7) and (8) have only one solution respectively.

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

$$\chi(x_1x_2) = \chi(\frac{a(1 \pm u)}{b}) = \chi(-x(x+a)) = \chi(-1) = -1 \tag{9}$$

and then only one of x_1 and x_2 can be a square, where x_1 and x_2 denote two solutions to Equations (5) and (6). Therefore, both Equations (5) and (6) have at most one solution. If these two equations simultaneously has one solution, 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.

For Equations (7) and (8), one has $x_1x_2 = \frac{a(1\mp u)}{b}$ and $x_1 + x_2 = -\frac{ab\mp 2u}{b}$. Hence,

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

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

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

which implies that

$$\begin{cases} \chi(x_1(x_1+a)) = 1; \\ \chi(x_2(x_2+a)) = -1 \end{cases} \text{ or } \begin{cases} \chi(x_1(x_1+a)) = -1; \\ \chi(x_2(x_2+a)) = 1. \end{cases}$$

Thus, $\chi(x(x+a)) = -1$, and then both Equations (7) and (8) have at most one solution. Suppose that $x_1, x_2 \in F_{p^n}$ are two solutions to Equation (7), and $y_1, y_2 \in F_{p^n}$ are two solutions to Equation (8). Note that $-(x_1+a)$ and $-(x_2+a)$ are two solutions to Equation (8), then one has $\{-(x_1+a), -(x_2+a)\} = \{y_1, y_2\}$. Suppose

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

Then

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

Therefore,

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

This is impossible. Thus, Equations (7) and (8) have at most one solution in total.

(2) $ab = 1 + u$

In this subcase, for given a, b, and u, Equation (3) exactly has a solution $x = 0$ if $\chi(a) = 1$, and $x = -a$ if $\chi(a) = -1$.

Assume that Equation (3) has another 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 discriminant of Equations (7) and (8) is 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 not a square. Thus, x_0 has the only possibility to satisfy Equation (5) or Equation (6). 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 $-a$.

From $u\neq\pm1$, one has $b\neq0$. 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 $a^2b^2+4ab(u+1)=(5u-3)(u+1)$ is not a square. Thus, x_0 is not a solution to Equation (5). Thus, x_0 can not be a solution to 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 $-a$.

Combing 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 $a\neq0$ and b such that $f(x+a)-f(x)=b$ has two solutions, equivalently, we only need to prove that there are values for $a\neq0$ and b such that $f(x+a)-f(x)=b$ has no solutions since for $a\neq0$ there are on the average one solution for each b. 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 exist at least one nonzero value $z=ab\in F_{p^n}$ 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 can be proven by the method used in Lemma 2, and there are such values $z=ab\neq1\pm u$ in F_{p^n}. Then $f(x+a)-f(x)=b$ has no solutions for these particular choices of $a\neq0$ and b. Thus, for some a, there is a b such that Equation (3) has two solutions and therefore the function is APN. □

Remark 2: When $p=3$, $\chi(5u\pm3)=\chi(-u)=-\chi(u)$. Since $\chi(u+1)=\chi(u-1)$ implies $u\neq0$, the condition $\chi(u+1)=\chi(u-1)=-\chi(5u\pm3)$ is equivalent to $\chi(u+1)=\chi(u-1)=\chi(u)$. Thus, in this case, above theorem is exactly Theorem 1 in [23]. For $p>3$, the characterization of u is different from the case for $p=3$ given in [23]. This maybe interprets why the proposed family of APN in [23] does not seem to have an analog for $p>3$.

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

When $p\geq7$, 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 mappings

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

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

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

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

$$a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i} = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^d (\text{mod } x^{p^n} - x) \tag{10}$$

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

In fact, by Table 1, we only need to consider five exponents d in propositions 1-2 and Corollary 1 as follows. The following lemma will be used to prove results in this paper.

Lemma 3: Let $u \in F_{p^n}$ satisfy the condition in Equality (2) and $p \geq 7$. Then, any 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 no zeros.

Proposition 1: The function $f(x)$ is CCZ-inequivalent to $g(x) = x^3$ on F_{p^n}.

Proof: Suppose that $f(x)$ and $g(x) = x^3$ are CCZ-equivalent. Then, the right side of Equality (10) is equal to

$$\begin{aligned}
& (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^3 \\
= \; & c^3 + 3\sum_{k=0}^{n-1} c^2 c_k x^{p^k} + 3\sum_{k=0}^{n-1} c^2 e_k u^{p^k} x^{\frac{p^n-1}{2}-p^k} + 3\sum_{k=0}^{n-1} c^2 e_k x^{p^n-1-p^k} + \\
& 3\sum_{k,s=0}^{n-1} c c_k c_s x^{p^k+p^s} + 3\sum_{k,s=0}^{n-1} c e_k e_s (u^{p^k+p^s} + 1) x^{p^n-1-p^k-p^s} + \\
& 6\sum_{k,s=0}^{n-1} c c_k e_s u^{p^s} x^{p^k+\frac{p^n-1}{2}-p^s} + 6\sum_{k,s=0}^{n-1} c c_k e_s x^{p^k+p^n-1-p^s} + \\
& 3\sum_{k,s=0}^{n-1} c e_k e_s (u^{p^k} + u^{p^s}) x^{\frac{p^n-1}{2}-p^k-p^s} + \sum_{k,s,t=0}^{n-1} c_k c_s c_t x^{p^k+p^s+p^t} + \\
& 3\sum_{k,s,t=0}^{n-1} c_k c_s e_t u^{p^t} x^{p^k+p^s+\frac{p^n-1}{2}-p^t} + 3\sum_{k,s,t=0}^{n-1} c_k c_s e_t x^{p^k+p^s+p^n-1-p^t} + \\
& 3\sum_{k,s,t=0}^{n-1} c_k e_s e_t (u^{p^s} + u^{p^t}) x^{p^k+\frac{p^n-1}{2}-p^s-p^t} + \\
& 3\sum_{k,s,t=0}^{n-1} c_k e_s e_t (u^{p^s+p^t} + 1) x^{p^k+p^n-1-p^s-p^t} + \\
& \sum_{k,s,t=0}^{n-1} e_k e_s e_t (u^{p^k+p^s+p^t} + u^{p^k} + u^{p^s} + u^{p^t}) x^{\frac{p^n-1}{2}-p^k-p^s-p^t} + \\
& \sum_{k,s,t=0}^{n-1} e_k e_s e_t (u^{p^k+p^s} + u^{p^s+p^t} + u^{p^t+p^k} + 1) x^{p^n-1-p^k-p^s-p^t}.
\end{aligned} \tag{11}$$

The exponents of unknown x in Equality (11) have 16 possible forms. Since $p \geq 7$ and $n \geq 3$ is odd, it is not difficult to observe that the first 13 kinds of exponents in Table 2 are less than $p^n - 1$ and their weights are determined as the following table. Now we consider the last three kind exponents having forms $p^k + p^n - 1 + \alpha p^s - p^t$, where $\alpha = 0, \pm 1$. We only give the analysis for the weight of $p^k + p^n - 1 - p^s - p^t \pmod{p^n - 1}$, and other cases of $\alpha = 0$ and 1 can be similarly obtained.

Table 2 Possible forms and weights of exponents in Equality (11)

Exponent	0	p^k	$\frac{p^n-1}{2} - p^k$	$p^n - 1 - p^k$
Weight	0	1	$\frac{n(p-1)}{2} - 1$	$n(p-1) - 1$
Exponent	$p^k + p^s$	$p^n - 1 - p^k - p^s$	$p^k + \frac{p^n-1}{2} - p^s$	$\frac{p^n-1}{2} - p^k - p^s$
Weight	2	$n(p-1) - 2$	$\frac{n(p-1)}{2}$	$\frac{n(p-1)}{2} - 2$
Exponent	$p^k + p^s + p^t$	$p^k + p^s + \frac{p^n-1}{2} - p^t$	$p^k + \frac{p^n-1}{2} - p^s - p^t$	$\frac{p^n-1}{2} - p^k - p^s - p^t$
Weight	3	$\frac{n(p-1)}{2} + 1$	$\frac{n(p-1)}{2} - 1$	$\frac{n(p-1)}{2} - 3$
Exponent	$p^n - 1 - p^k - p^s - p^t$	$p^k + p^n - 1 - p^s$	$p^k + p^s + p^n - 1 - p^t$	$p^k + p^n - 1 - p^s - p^t$
Weight	$n(p-1) - 3$	$(k-s)(p-1)$, or $(n+k-s)(p-1)$	$1+(k-t)(p-1)$, or $1 + (s-t)(p-1)$, or $1+$ $(n-t+\min\{k,s\})(p-1)$	$(k - \min\{s,t\})(p-1) - 1$, or $(n+k-s)(p-1) - 1$, or $(n+k-t)(p-1) - 1$

where $0 \leq k$, s, $t \leq n-1$.

Without loss of generality, we assume $s \geq t$. When $k > s$, one has

$$p^k + p^n - 1 - p^s - p^t \pmod{p^n - 1} = p^k - p^s - p^t.$$

Then, $p^k - p^t = (p-1)p^{n-1} + \cdots + (p-1)p^t$ has weight $(k-t)(p-1)$. Since $k > s \geq t$, the weight of $p^k - p^s - p^t$ is $(k-t)(p-1) - 1$. When $t < k \leq s$, one has

$$p^k + p^n - 1 - p^s - p^t \pmod{p^n - 1} = p^k + p^n - 1 - p^s - p^t.$$

Then,

$$\begin{aligned} & p^k + p^n - 1 - p^s \\ = \; & (p^n - p^s) + (p^k - 1) \\ = \; & (p-1)p^{n-1} + \cdots + (p-1)p^s + (p-1)p^{k-1} + \cdots + (p-1), \end{aligned} \tag{12}$$

whose weight is $(n+k-s)(p-1)$. Since $k - 1 \geq t$, the weight of $p^k + p^n - 1 - p^s - p^t$ is $(n+k-s)(p-1) - 1$. When $k = t$, $p^k + p^n - 1 - p^s - p^t = p^n - 1 - p^s$ has weight $n(p-1) - 1$. When $k < t$, by Equality (12), the weight of $p^k + p^n - 1 - p^s - p^t$ is $(n+k-t)(p-1) - 1$.

Consider the exponent $3p^i$ of weight 3, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $3p^i$ only derives from the form $p^k + p^s + p^t$ with $k = s = t = i$. Therefore, the coefficient of the term x^{3p^i} on right hand of Equality (10) is equal to c_i^3, and it is zero on the left side. This gives $c_i^3 = 0$, i.e., $c_i = 0$.

Considering the exponents $p^n - 1 - 3p^i$, by Table 2, $p^n - 1 - 3p^i = p^n - 1 - p^k - p^s - p^t$ and then $k = s = t = i$. As the case of x^{3p^i}, one can get that the coefficient of the term $x^{p^n - 1 - 3p^i}$ on right hand of Equality (10) is equal to $e_i^3(3u^2 + 1)^{p^i}$, and it is zero on the left side. Then, one has

$$e_i^3(3u^2 + 1)^{p^i} = 0. \tag{13}$$

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

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

By Lemma 3, Equalities (13) and (14) imply $e_i = 0$. Thus $L_2(x, f(x)) = c$ is not a permutation. Therefore, $f(x)$ and $g(x) = x^3$ 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 $p^n \equiv 2(\text{mod } 3)$ and $p \equiv 3(\text{mod } 4)$, 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 (10), one has

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i})^3 = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i} (\text{mod } x^{p^n} - x). \quad (15)$$

A same analysis as in Proposition 1 gives $a_i = b_i = 0$ for any $0 \leq i \leq n-1$. Eq. (15) can be reduced as

$$a^3 = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i} (\text{mod } x^{p^n} - x), \quad (16)$$

which implies $c_i = e_i = 0$ for any i. Thus, $L_2(x, f(x)) = c$. This contradicts with $L_2(x, f(x))$ is a permutation. The contradiction proves CCZ-inequivalence of $f(x)$ and $g(x) = x^{\frac{2p^n-1}{3}}$. □

By analyzing the weight of exponents in Equality (10), the following can be proven in a way similar 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 $p^n \equiv 3(\text{mod } 8)$ and $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ for $p^n \equiv 7(\text{mod } 8)$;
(2) $d = \frac{p^n-1}{2} - 1$ for $p \equiv 3, 7(\text{mod } 20)$;
(3) $d = p^n - 2$ for $p \equiv 2(\text{mod } 3)$.

By Propositions 1, 2 and Corollary 1, for $p \geq 7$, the proposed functions are CCZ-inequivalent to all known APN power mappings.

4. Conclusion

This paper proved an infinite family of mappings over finite fields of odd Characteristic is almost perfect nonlinear. For $p \geq 7$, the constructed mappings are CCZ-inequivalent to all known APN power mappings.

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, 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," *Information Theory, 2006 IEEE International Symposium*, pp. 2637-2641, 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, 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, Mar. 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.