On equivalence between known polynomial APN functions and power APN functions

Qianhong Wan[a], Longjiang Qu[a,b,1], Chao Li[a,2,*]

[a]College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China.
[b]State Key Laboratory of Cryptology, Beijing, 100878, China.

Abstract

Constructions and equivalence of APN functions play a significant role in the research of cryptographic functions. On finite fields of characteristic 2, 6 families of power APN functions and 14 families of polynomial APN functions have been constructed in the literature. However, the study on the equivalence among the aforementioned APN functions is rather limited to the equivalence in the power APN functions. Meanwhile, the theoretical analysis on the equivalence between the polynomial APN functions and the power APN functions, as well as the equivalence in the polynomial APN functions themselves, is far less studied. In this paper, we give the theoretical analysis on the inequivalence in 8 known families of polynomial APN functions and power APN functions.

Keywords: Polynomial APN Function, Power APN Function, EA-equivalence, CCZ-equivalence
MSC: 94A60, 06E30, 11T71

1. Introduction

Cryptographic function is the only nonlinear component of symmetric cryptographic algorithm such as stream cipher, block cipher and Hash function. Researchers have introduced various criteria to measure the resistance of a cryptographic function to different kinds of cryptanalysis, including differential uniformity, nonlinearity, algebraic degree, boomerang uniformity, etc. The lower the differential uniformity of a function is, the better its security against differential cryptanalysis is. Due to practical application, most cryptographic functions are defined over the finite field with even characteristic. The differential uniformity of a cryptographic function is at least 2 over such field, the functions achieving the least differential uniformity are called almost perfect nonlinear(APN) over the field of characteristic 2.

The differential uniformity is preserved under some equivalence relations between cryptographic functions such as affine equivalence, extended affine equivalence (EA-equivalence) and CCZ-equivalence. It is known that affine equivalence is EA-equivalence, EA-equivalence is a simple particular case of CCZ-equivalence, but the converse is not necessarily true.

Constructing new APN functions is one of main topics in the research of cryptography functions, and the new APN function can not be included in the existing families of APN functions in the sense of equivalence. So it is necessary to check the equivalence between APN functions.

It is difficult to find new families of APN functions. Up to now, only 6 families of power APN functions and 14 infinite families of APN polynomials are known since 1990's, which are listed in tables I and II respectively. Recently Budaghyan et al. proved that $f_3(x)$ is equivalent to $f_{11}(x)$, and both of them are included in $f_4(x)$[1].

*Corresponding author
Email addresses: 77927023@qq.com (Qianhong Wan), ljqu_happy@hotmail.com (Longjiang Qu), lichao_nudt@sina.com (Chao Li)

[1]The research of Longjiang Qu is partially supported by the Nature Science Foundation of China (NSFC) under Grant 61722213, 11771451 and the Open Foundation of State Key Laboratory of Cryptology.
[2]The research of Chao Li is partially supported by the Nature Science Foundation of China (NSFC) under Grant 61672530, 11531002.

Table 1: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	2^i+1	$\gcd(i,n)=1$	2	[2]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[3]
Welch	2^t+3	$n=2t+1$	3	[4]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{(3t+1)}{2}}-1$, t odd	$n=2t+1$	$\frac{(t+2)}{2}$ $t+1$	[5]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[6, 7]
Dobbertin	$2^{4i}+2^{3^i}+2^{2^i}+2^i-1$	$n=5i$	$i+3$	[8]

The research of equivalence of APN functions is focused on the equivalence between power functions [9, 10, 11, 12, 13]. In 2018, Dempwolff gave a general result about CCZ-equivalence among power APN functions over the finite field of characteristic p. Let $F=\mathbb{F}_{p^n}$ be a finite field, $f_d(x)=x^d$ and $f_e(x)=x^e$ be two APN power functions over F. Then f_d and f_e are CCZ-equivalent if and only if there exists some $a\in[0,n-1]$ such that $e\equiv dp^a \mod p^n-1$ or $ed\equiv p^a \mod p^n-1$[14]. So the equivalences between any two power APN functions are resolved completely.

The theoretical analysis of equivalence between polynomial APN function and power APN function only be found in literature[15, 16]. For example, Budaghyan et al. proved that their functions are EA-inequivalent to any power APN function, and CCZ-inequivalent to Gold function, inverse function and Dobbertin function for $n\geq 12$. Generally, the equivalence between new family of APN functions and power APN functions is checked by searching the CCZ-equivalent invariants on a small number of variables, but very little theoretical results were known.

In 2012, Yoshiara proved the Edel's conjecture: Let f and g be quadratic APN functions on a finite field $\mathbb{F}_{2^n}$ with $n\geq 2$. Then f is CCZ-equivalent to g if and only if f is EA-equivalent to g [17]. In 2016, she proved: Let $\mathbb{F}_{2^n}$ be a finite field. If a quadratic APN function f and a power APN function g is CCZ-equivalent, then f is EA-equivalent to one of the Gold function($n\geq 3$) [9]. which implies that CCZ-equivalence between a quadratic polynomial APN function and a power APN function can be turned into CCZ-equivalence between a quadratic polynomial APN function and a Gold function. Furthermore, as Gold function is a quadratic function, it can be turned into EA-equivalence. In this paper, we consider the 8 known families of quadratic polynomial APN functions constructed in [15][18, 19], and we prove that all these functions are CCZ-inequivalent to power APN functions, therefore some theoretical results on CCZ-equivalence between quadratic polynomial APN functions and power APN functions are obtained.

We first give the preliminaries needed in this paper, then we give the proofs of CCZ-inequivalence between $f_i(x)$ (in table II) and power APN functions($i=1,2,4,5,6,7,8,9$), which is the main part of our paper. For $f_4(x)$, we discuss CCZ-inequivalence by proving CCZ-inequivalence between $f_i(x)(i=3,11)$ and power APN functions.

2. Preliminaries

Denote by $\mathbb{F}_2$ the finite field with two elements. For a positive integer n, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, which is a linear space with dimension n over $\mathbb{F}_2$, $\mathbb{F}_{2^n}^*$ be the multiplicative group of $\mathbb{F}_{2^n}$. A function from $\mathbb{F}_{2^n}$ to itself is called almost perfect nonlinear(APN) if for any $a\neq 0$, $b\in\mathbb{F}_{2^n}$, the number of solutions in $\mathbb{F}_{2^n}$ of the equation $f(x+a)-f(x)=b$ is at most 2.

A polynomial $L(x)\in\mathbb{F}_{2^n}[x]$ is called a linearized polynomial if $L(x)$ can be written as

$$L(x)=\sum_{i=0}^{n-1}a_i x^{2^i},\ a_i\in\mathbb{F}_{2^n}.$$

A polynomial from $\mathbb{F}_{2^n}$ to itself is called affine, if it is defined by the sum of a linearized polynomial and a constant polynomial over $\mathbb{F}_{2^n}$.

Table 2: Known infinite families of quadratic APN polynomial over $\mathbb{F}_{2^n}$

ID	Functions	Conditions	In
$f_i(x)$ $i=1,2$	$x^{2^s+1}+u^{2^{k-1}}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}, i=sk \mod p, m=p-i$, $n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[15]
$f_3(x)$	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{(2^{2i}+2^i)q}$	$q=2^m, n=2m, \gcd(i,m)=1$, $\gcd(2^i+1,q+1)\neq 1, dc^q+c\neq 0$, $d\notin\{\lambda^{(2^i+1)(q-1)}, \lambda\in\mathbb{F}_{2^n}\}, d^{q+1}=1$	[18]
$f_4(x)$	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m, n=2m, \gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[18]
$f_5(x)$	$x^3+a^{-1}\mathrm{Tr}(a^3x^9)$	$a\neq 0$	[19]
$f_6(x)$	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n, a\neq 0$	[19]
$f_7(x)$	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$	[19]
$f_i(x)$ $i=8,9,10$	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}$ $+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}, vw\neq 1$, $3\mid(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[20, 21]
$f_{11}(x)$	$dx^{2^i+1}+d^qx^{q(2^i+1)}$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_sx^{2^s(q+1)}$	$q=2^m, n=2m, \gcd(i,m)=1, i,m$ odd, $\gamma_s\in\mathbb{F}_{2^m}, c\notin\mathbb{F}_{2^m}$ d not a cube	[21]
$f_{12}(x)$	$(x+x^q)^{2^i+1}+u'(ux+u^qx^q)^{(2^i+1)2^j}$ $+u(x+x^q)(ux+u^qx^q)$	$q=2^m, n=2m, m\geq 2$ even, $\gcd(i,m)=1$ and j even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube	[22]
$f_{13}(x)$	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+$ $ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions in [23, Theorem 6.3]	[23]
$f_{14}(x)$	$u(u^qx+x^qu)(x^q+x)$ $+(u^qx+x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}$ $+b(x^q+x)^{2^i+1}$	$q=2^m, n=2m, \gcd(i,m)=1$, $a,b\in\mathbb{F}_{2^m}$ and $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$	[24]

For any $m\geq 1$ such that $m\mid n$,

$$\mathrm{Tr}_n^m(x)=\sum_{i=0}^{\frac{n}{m}-1}x^{2^{im}}$$

denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. When $m=1$, we denote it by $\mathrm{Tr}(x)$, which is called absolute trace function.

Definition 2.1. *(EA equivalence) Two functions $f, g:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ are extended affine equivalent (EA-equivalent) if there exist two affine permutations $L_1, L_2:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ and an affine function $L:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ such that $g=L_1\circ f\circ L_2+L$.*

Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function, the graph G_f of f is the set $G_f=\{(x,f(x))|x\in\mathbb{F}_{2^n}\}\subseteq\mathbb{F}_{2^n}^2$.

Definition 2.2. *(CCZ equivalence) Two functions $f, g:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ are CCZ-equivalent if there exists an affine permutation $L(x)$ such that $L(G_f)=G_g$.*

We first give the following two important results about EA-equivalence and CCZ-equivalence.

Theorem 2.3 ([17],Theorem 1)**.** *Let f and g be quadratic APN functions on a finite field $\mathbb{F}_{2^n}$ with $n\geq 2$. Then f is CCZ-equivalent to g if and only if f is EA-equivalent to g .*

Theorem 2.4 ([9],Theorem 2)**.** *Let $\mathbb{F}_{2^n}$ be a finite field, f be a quadratic APN function, and $f_d(x) = x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ ($n \geq 3$) be a power APN function. If f and f_d are CCZ-equivalent, then f is EA-equivalent to the Gold function $g_s(x) = x^{2^s+1}$ for some integer s with $1 \leq s < \frac{n}{2}$ coprime to n.*

From Theorem 2.4, it is obvious that if a quadratic APN function is EA-inequivalent to any Gold functions, then it is CCZ-inequivalent to any power APN functions.

Let i, j, s, t be any positive integers, if $2^i + 2^j = 2^s + 2^t$, then $i = s$ and $j = t$, or $i = t$ and $j = s$. Using this conclusion, we have the following lemma.

Lemma 2.5. *Let $i \neq j \mod n$, $s \neq t \mod n$ be any positive integers, $x^{2^i+2^j}$, $x^{2^s+2^t}$ be two monomials over $\mathbb{F}_{2^n}$. Then $x^{2^i+2^j} = x^{2^s+2^t}$ if and only if $i \equiv s \mod n$ and $j \equiv t \mod n$, or $j \equiv s \mod n$ and $i \equiv t \mod n$.*

Proof. The sufficiency is obvious, we just give the proof of the necessity. By choosing integers l_1, l_2, l_3, l_4 suitably, we can assume all of the $i - nl_1$, $j - nl_2$, $s - nl_3$, $t - nl_4$ are in the interval of $[0, n-1]$. As a result, $x^{2^i+2^j} = x^{2^s+2^t}$ can be written as

$$x^{2^{i-nl_1+nl_1}+2^{j-nl_2+nl_2}} = x^{2^{s-nl_3+nl_3}+2^{t-nl_4+nl_4}}.$$

Namely

$$x^{2^{i-nl_1}+2^{j-nl_2}} = x^{2^{s-nl_3}+2^{t-nl_4}}.$$

Since $i - nl_1$, $j - nl_2$, $s - nl_3$, $t - nl_4$ are less than n, then

$$1 < 2^{i-nl_1} + 2^{j-nl_2} < 2^n, \quad 1 < 2^{s-nl_3} + 2^{t-nl_4} < 2^n.$$

So that

$$i - nl_1 = s - nl_3 \text{ and } j - nl_2 = t - nl_4, \quad \text{or } j - nl_2 = s - nl_3 \text{ and } i - nl_1 = t - nl_4.$$

Which is equivalent to

$$i \equiv s \mod n \text{ and } j \equiv t \mod n, \quad \text{or } j \equiv s \mod n \text{ and } i \equiv t \mod n.$$

□

Let $L(x) = \sum_{j=0}^{n-1} c_j x^{2^j}$ be a linearized polynomial over $\mathbb{F}_{2^n}$, $g(x) = x^{2^r+1}$ be a Gold function. Then

$$g(L(x)) = (\sum_{j=0}^{n-1} c_j x^{2^j})^{2^r+1} = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} c_j c_i^{2^r} x^{2^{r+i}+2^j}.$$

If $r + i \neq j$, then there exist only two terms of the type $x^{2^{r+i}+2^j}$ in $g(L(x))$ from Lemma 2.5. And if the subscripts of coefficients of polynomial function belong to the ring $\mathbb{Z}/n\mathbb{Z}$, i.e. $i \equiv j \mod n \Rightarrow c_i = c_j$, then we have the following corollary.

Corollary 2.6. *If $r + i \neq j$, then the coefficient of the term of the type $x^{2^{r+i}+2^j}$ of $g(L(x))$ is $c_j c_i^{2^r} + c_{i+r} c_{j-r}^{2^r}$.*

If we rearrange the terms of $g(L(x))$, then $g(L(x))$ can be expressed as

$$g(L(x)) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} c_j c_{i+j}^{2^r} x^{2^j(2^{r+i}+1)}.$$

Let $\mathbb{Z}$ be the set of all integers. We have the following corollary.

Corollary 2.7. *Let $0 \leq i_1 \neq i_2 \leq n-1$, and $2r + i_1 + i_2 \neq 0 \mod n$. Then $\{x^{2^j(2^{r+i_1}+1)} | j \in \mathbb{Z}\} \cap \{x^{2^{j'}(2^{r+i_2}+1)} | j' \in \mathbb{Z}\} = \varnothing$ over $\mathbb{F}_{2^n}$.*

Proof. If $x^{2^j(2^{r+i_1}+1)} = x^{2^{j'}(2^{r+i_2}+1)}$, then by Lemma 2.5, we have

$$\begin{cases} j+r+i_1 \equiv j'+r+i_2 \mod n \\ j \equiv j' \mod n \end{cases} \quad \text{or} \quad \begin{cases} j+r+i_1 \equiv j' \mod n \\ j \equiv j'+r+i_2 \mod n \end{cases}$$

By solving this congruence equations, we have $i_1 = i_2$ or $2r + i_1 + i_2 = 0 \mod n$, a contradiction.

□

3. Main Conclusion

Without further explanation, the functions in this section are all defined over the finite field $\mathbb{F}_{2^n}$, and the subscripts of the coefficients of polynomial function belong to the ring $\mathbb{Z}/n\mathbb{Z}$, i.e. $i \equiv j \mod n \Rightarrow c_i = c_j$.

Lemma 3.1. *Let $L(x) = \sum_{j=0}^{2k-1} b_j x^{2^j}$ be a linearized polynomial over $\mathbb{F}_{2^{2k}}$. If $b_0 = 1$, $b_k = 0$, $b_j = \frac{r_j}{c^{2^j}+c^{2^{k+j}}}$, $c \in \mathbb{F}_{2^{2k}}$, $r_j \in \mathbb{F}_{2^k}$, $b_{j+k} = b_j\,(1 \le j \le k-1)$, then $L(x)$ is a linear permutation.*

Proof. The fact $r_j \in \mathbb{F}_{2^k}$ implies $b_j^{2^k} = (\frac{r_j}{c^{2^j}+c^{2^{k+j}}})^{2^k} = \frac{r_j^{2^k}}{c^{2^{j+k}}+c^{2^{2k+j}}} = \frac{r_j}{c^{2^{j+k}}+c^{2^j}} = b_j$, $1 \le i \le k-1$. Assume $L(a) = 0$ for some $a \in \mathbb{F}_{2^{2k}}$, that is

$$\sum_{j=0}^{2k-1} b_j a^{2^j} = 0. \tag{1}$$

Since $b_0 = 1$, $b_k = 0$, $b_{j+k} = b_j\,(1 \le j \le k-1)$, from (1), we have

$$a + \sum_{j=1}^{k-1} b_j (a^{2^j} + a^{2^{k+j}}) = 0. \tag{2}$$

Raising both sides of equation (2) to the 2^k−th power leads to

$$a^{2^k} + \sum_{j=1}^{k-1} b_j (a^{2^j} + a^{2^{k+j}}) = 0. \tag{3}$$

It follows from (2) and (3) that

$$a^{2^k} + a = 0. \tag{4}$$

Substituting (4) into (2), we obtain $a = 0$. So $L(x)$ is a linear permutation.

□

Let s, k be odd, $(s,k) = 1$, b, $c \in \mathbb{F}_{2^{2k}}$, $r_j \in \mathbb{F}_{2^k}$. If $c \notin \mathbb{F}_{2^k}$ and b is not a cube, then $f_{11}(x) = bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{j=1}^{k-1} r_j x^{2^{j+k}+2^j}$, $h(x) = bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^k+1}$ are APN functions over $\mathbb{F}_{2^{2k}}$[21], and we have the following proposition (different proof can be found in [1]).

Proposition 3.2. *$f_{11}(x)$ is EA-equivalent to $h(x)$.*

Proof. Let $L(x) = \sum_{i=0}^{2k-1} b_i x^{2^i}$ be defined as in Lemma 3.1. Then

$$\begin{aligned} L(f_{11}(x)) &= \sum_{i=0}^{2k-1} b_i (bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{j=1}^{k-1} r_j x^{2^{j+k}+2^j})^{2^i} \\ &= \sum_{i=0}^{2k-1} b_i b^{2^i} x^{2^i(2^s+1)} + \sum_{i=0}^{2k-1} b_i b^{2^{k+i}} x^{2^{i+k}(2^s+1)} \\ &+ \sum_{i=0}^{2k-1} b_i c^{2^i} x^{2^i(2^k+1)} + \sum_{i=0}^{2k-1} b_i \sum_{j=1}^{k-1} r_j^{2^i} x^{2^{i+j}(2^k+1)}. \end{aligned} \tag{5}$$

Next we will compute (5) item by item.

1) The second term $\sum_{i=0}^{2k-1} b_i b^{2^{k+i}} x^{2^{i+k}(2^s+1)}$ of (5) can be rewritten as

$$\sum_{i=0}^{2k-1} b_{i+k} b^{2^i} x^{2^i(2^s+1)}.$$

Hence the sum of the first and second term of (5) is equal to

$$\begin{aligned}&\sum_{i=0}^{2k-1} b_i b^{2^i} x^{(2^s+1)2^i} + \sum_{i=0}^{2k-1} b_{i+k} b^{2^i} x^{2^i(2^s+1)}\\ &= \sum_{i=0}^{2k-1} (b_i + b_{i+k}) b^{2^i} x^{2^i(2^s+1)}.\end{aligned}$$

As $b_{i+k} = b_i\,(1 \le i \le k-1)$, all the terms are 0 in the above form except $i = 0,\ k$. That is to say, the above form equals to

$$(b_0 + b_k) b x^{2^s+1} + (b_k + b_0) b^{2^k} x^{2^k(2^s+1)}.$$

The fact $b_0 = 1,\ b_k = 0$ implies that the sum of the first and second term of (5) is

$$b x^{2^s+1} + b^{2^k} x^{2^k(2^s+1)}.$$

2) The third term of (5) is

$$\begin{aligned}\sum_{i=0}^{2k-1} b_i c^{2^i} x^{2^i(2^k+1)} &= \sum_{i=0}^{k-1} b_i c^{2^i} x^{2^i(2^k+1)} + \sum_{i=k}^{2k-1} b_i c^{2^i} x^{2^i(2^k+1)}\\ &= \sum_{i=0}^{k-1} b_i c^{2^i} x^{2^i(2^k+1)} + \sum_{i=0}^{k-1} b_{k+i} c^{2^{k+i}} x^{2^i(2^k+1)}.\end{aligned}$$

The fact $b_0 = 1,\ b_k = 0$ and $b_{i+k} = b_i (1 \le i \le k-1)$ implies the third term equals to

$$c x^{2^k+1} + \sum_{i=1}^{k-1} b_i (c^{2^i} + c^{2^{k+i}}) x^{2^i(2^k+1)}.$$

3) The fourth term $\sum_{i=0}^{2k-1} b_i \sum_{j=1}^{k-1} r_j^{2^i} x^{2^{i+j}(2^k+1)}$ of (5) can be transformed into

$$\sum_{j=1}^{k-1} \sum_{i=0}^{2k-1} b_i r_j^{2^i} x^{2^{i+j}(2^k+1)}.$$

Using the similar process to the above form that is used to the third term, the fourth term can be written as

$$\sum_{j=1}^{k-1} (r_j x^{2^{j+k}+2^j} + \sum_{i=1}^{k-1} b_i (r_j^{2^i} + r_j^{2^{i+k}}) x^{2^{i+j}(2^k+1)}).$$

Because $r_i \in \mathbb{F}_{2^k}$, so $r_j^{2^i} + r_j^{2^{i+k}} = 0\,(1 \le i \le k-1)$, as a result, the fourth term is

$$\sum_{j=1}^{k-1} r_j x^{2^{j+k}+2^j}.$$

So the form of (5) is

$$\begin{aligned}
&bx^{2^s+1} + b^{2^k}x^{2^k(2^s+1)} + cx^{2^k+1} + \sum_{i=1}^{k-1} b_i(c^{2^i} + c^{2^{k+i}})x^{2^i(2^k+1)} + \sum_{j=1}^{k-1} r_j x^{2^{j+k}+2^j} \\
&= bx^{2^s+1} + b^{2^k}x^{2^k(2^s+1)} + cx^{2^k+1} + \sum_{i=1}^{k-1}(b_i(c^{2^i} + c^{2^{k+i}}) + r_i)x^{2^i(2^k+1)} \\
&= bx^{2^s+1} + b^{2^k}x^{2^k(2^s+1)} + cx^{2^k+1},
\end{aligned}$$

where the last equality follows from $b_i = \dfrac{r_i}{c^{2^i} + c^{2^{k+i}}}$. So we have $L(f_{11}(x)) = h(x)$, and by Lemma 3.1, $L(x)$ is a linear permutation, so $f_{11}(x)$ is EA-equivalent to $h(x)$.

□

Lemma 3.3 ([13],Corollary 3)**.** *Let $h(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1}$ with $b, c \in \mathbb{F}_{2^{2k}}$. If $c \notin \mathbb{F}_{2^k}$ and b is not a cube, then $h(x)$ is CCZ-inequivalent to Gold function $g(x) = x^{2^r+1}$, where $1 \le r < \frac{n}{2}$ coprime to $n = 2k$.*

By Lemma 3.3 and the transitivity of equivalence, we can obtain the following proposition.

Proposition 3.4. *$f_{11}(x)$ is CCZ-inequivalent to Gold function $g(x) = x^{2^r+1}$.*

Let $n = 2m(m \ge 3)$, $\gcd(s, m) = 1$, $\alpha, \beta \in \mathbb{F}_{2^n}$, and $\beta^{2^m+1} = 1$, $\beta \notin \{\lambda^{(2^s+1)(2^m-1)} | \lambda \in \mathbb{F}_{2^n}\}$, $\beta\alpha^{2^m} + \alpha \ne 0$. Then $f_3(x) = x^{2^{2s}+2^s} + \alpha x^{2^m+1} + \beta x^{2^{2s+m}+2^{s+m}}$ is a quadratic APN function[18]. We can assume $0 < s < 2m$.

Before we give the EA-inequivalence result between $f_3(x)$ and Gold function, we need the following lemma.

Lemma 3.5. *If $m \ge 4$, then*

(1) $\{x^{2^i(2^{m+s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)} | i \in \mathbb{Z}\} = \varnothing$, $\quad \{x^{2^i(2^{m+s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^m+1)} | i \in \mathbb{Z}\} = \varnothing$;

(2) $\{x^{2^i(2^{m+2s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)} | i \in \mathbb{Z}\} = \varnothing$, $\quad \{x^{2^i(2^{m+2s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^m+1)} | i \in \mathbb{Z}\} = \varnothing$.

Proof. We only prove (1), (2) can be proved by the similar way.

We claim $m + s + s \ne 0 \mod n$. In fact $m < m + s + s < 5m$.

If $m + 2s = 2m$, then $m = 2s$, but $(s, m) = 1$, a contradiction;

If $m + 2s = 4m$, then $3m = 2s$ and $2 \mid m$, hence we may assume $m = 2l$. The fact $m \ge 4$ implies $l \ge 2$ and $l \mid m$. On the other hand, by substituting $m = 2l$ into $3m = 2s$, we get $s = 3l$, hence $l \mid s$, but $(s, m) = 1$, a contradiction. Hence by Corollary 2.7, $\{x^{2^i(2^{m+s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)} | i \in \mathbb{Z}\} = \varnothing$.

Because of $2m < m + s + m < 4m$, hence $m + s + m \ne 0 \mod n$. By Corollary 2.7, $\{x^{2^i(2^{m+s}+1)} | i \in \mathbb{Z}\} \cap \{x^{2^i(2^m+1)} | i \in \mathbb{Z}\} = \varnothing$. □

Proposition 3.6. *If $m \ge 4$, then $f_3(x)$ is not EA-equivalent to Gold function $g(x) = x^{2^r+1}$, where $1 \le r < \frac{n}{2}$ coprime to $n = 2m$.*

Proof. We assume $f_3(x)$ is EA-equivalent to Gold function. Because the two functions are quadratic, we can assume there exist linear functions $L_1(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$, $L_2(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$ and affine function $L'(x)$ such that $L_1(f_3(x)) = g(L_2(x)) + L'(x)$, that is

$$\sum_{i=0}^{n-1} b_i(x^{2^{2s}+2^s} + \alpha x^{2^m+1} + \beta x^{2^{2s+m}+2^{s+m}})^{2^i} = (\sum_{i=0}^{n-1} c_i x^{2^i})^{2^r+1} + L'(x). \tag{6}$$

The left hand of equality (6) equals to

$$\sum_{i=0}^{m-1}(b_i + b_{i+m}\beta^{2^{i+m}})x^{2^{i+s}(2^s+1)} + \sum_{i=0}^{m-1}(b_i\alpha^{2^i} + b_{i+m}\alpha^{2^{i+m}})x^{2^i(2^m+1)} + \sum_{i=0}^{m-1}(b_{i+m} + b_i\beta^{2^i})x^{2^{i+m+s}(2^s+1)}.$$

On the left hand of equality (6), we only have the terms of the type

$$x^{2^i(2^{2s}+2^s)},\ x^{2^i(2^m+1)},\ x^{2^i(2^{2s+m}+2^{s+m})}$$

Because $\{x^{2^i(2^{2s}+2^s)}|i \in \mathbb{Z}\} = \{x^{2^i(2^{2s+m}+2^{s+m})}|i \in \mathbb{Z}\} = \{x^{2^i(2^s+1)} \mid i \in \mathbb{Z}\}$, by Lemma 3.5, the terms of the type $x^{2^i(2^{m+s}+1)}$ and $x^{2^i(2^{m+2s}+1)}$ are missing in the left hand of (6). Therefore, for any i, we get the equalities from the right hand of (6)

$$\begin{array}{ll} (a) & c_i c_{i+s+m-r}^{2^r} + c_{i+s+m} c_{i-r}^{2^r} = 0, \\ (b) & c_i c_{i+2s+m-r}^{2^r} + c_{i+2s+m} c_{i-r}^{2^r} = 0. \end{array}$$

We will prove that equality (6) holds only if $b_i = 0$ for all i. Assume, on the contrary, there exists $b_i \neq 0$ for some i.

1) If there exists $b_j\alpha^{2^j} + b_{j+m}\alpha^{2^{j+m}} \neq 0$ for some j, then b_j or b_{j+m} is nonzero, meanwhile we have both $b_j + b_{j+m}\beta^{2^{j+m}}$ and $b_{j+m} + b_j\beta^{2^j}$ are nonzero because of $\beta^{2^m+1} = 1$. As a consequence all the coefficients of the terms of the type $x^{2^j(2^{2s}+2^s)}$, $x^{2^j(2^m+1)}$ and $x^{2^j(2^{2s+m}+2^{s+m})}$ are nonzero on the left hand of equality (6). Hence this is true for the right hand of equality (6), by Corollary 2.6, we have

$$\begin{array}{ll} (c) & c_{j+s} c_{j+2s-r}^{2^r} + c_{j+2s} c_{j+s-r}^{2^r} \neq 0, \\ (d) & c_j c_{j+m-r}^{2^r} + c_{j+m} c_{j-r}^{2^r} \neq 0, \\ (e) & c_{j+s+m} c_{j+2s+m-r}^{2^r} + c_{j+2s+m} c_{j+s+m-r}^{2^r} \neq 0. \end{array}$$

We consider the following cases.

Case 1 When $c_{j+s+m-r} \neq 0$, $c_{j+2s+m-r} \neq 0$, and $c_{j-r} \neq 0$.

Since $c_{j+s+m-r} \neq 0$, $c_{j+2s+m-r} \neq 0$, $c_{j-r} \neq 0$, we get from (a), (b), (e)

$$\begin{array}{l} c_j c_{j-r}^{-2^r} = c_{j+s+m} c_{j+s+m-r}^{-2^r}, \\ c_j c_{j-r}^{-2^r} = c_{j+2s+m} c_{j+2s+m-r}^{-2^r}, \\ c_{j+s+m} c_{j+s+m-r}^{-2^r} \neq c_{j+2s+m} c_{j+2s+m-r}^{-2^r}. \end{array}$$

Hence we come to an obvious contradiction.

Case 2 When $c_{j+s+m-r} \neq 0$, $c_{j+2s+m-r} \neq 0$, and $c_{j-r} = 0$.

Since $c_{j-r} = 0$, we get $c_j \neq 0$ from (d). For $c_j \neq 0$, $c_{j-r} = 0$, we have $c_{j+s+m-r} = 0$ from (a), a contradiction.

Case 3 When $c_{j+s+m-r} \neq 0$, $c_{j+2s+m-r} = 0$.

Since $c_{j+2s+m-r} = 0$, we have $c_{j+2s+m} \neq 0$ from (e). Furthermore, we get $c_{j-r} = 0$ from (b), as a consequence we have $c_j \neq 0$ from (d). Therefore we get $c_{j+s+m-r} \neq 0$, $c_j \neq 0$, $c_{j-r} = 0$, which is contradict with (a).

Case 4 When $c_{j+s+m-r} = 0$.

Since $c_{j+s+m-r} = 0$, we have $c_{j+s+m} \neq 0$ and $c_{j+2s+m-r} \neq 0$ from (e). Furthermore equation (a) implies $c_{j-r} = 0$, hence $c_j \neq 0$ from (d). So we get $c_{j+2s+m-r} \neq 0$, $c_j \neq 0$, $c_{j-r} = 0$, which is contradict with (b).

2) If $b_j\alpha^{2^j} + b_{j+m}\alpha^{2^{j+m}} = 0$ for all j, then the coefficients of the term of the type $x^{2^j(2^m+1)}$ is zero for all j on the left hand of equality (6). Since $b_i \neq 0$ and $\beta^{2^m+1} = 1$, neither $b_i + b_{i+m}\beta^{2^{i+m}}$ nor $b_{i+m} + b_i\beta^{2^i}$ is zero, as a consequence the coefficients of the terms of the type $x^{2^i(2^{2s}+2^s)}$ and $x^{2^i(2^{2s+m}+2^{s+m})}$ are nonzero on the left hand of equality (6). Hence this is true for the right hand of equality (6), by Corollary 2.6, we have

$$\begin{array}{ll} (c') & c_{i+s} c_{i+2s-r}^{2^r} + c_{i+2s} c_{i+s-r}^{2^r} \neq 0, \\ (e') & c_{i+s+m} c_{i+2s+m-r}^{2^r} + c_{i+2s+m} c_{i+s+m-r}^{2^r} \neq 0, \\ (d') & c_j c_{j+m-r}^{2^r} + c_{j+m} c_{j-r}^{2^r} = 0 \text{ for any } j. \end{array}$$

We consider the following cases.

Case 1 When $c_{i+2s+m-r} \neq 0$, $c_{i+2s-r} \neq 0$ and $c_{i+s-r} \neq 0$.

From (a), we have

$$(a') \quad c_{i+s} c_{i+2s+m-r}^{2^r} + c_{i+2s+m} c_{i+s-r}^{2^r} = 0.$$

From (d'), we have

$$(d'') \quad c_{i+2s} c_{i+2s+m-r}^{2^r} + c_{i+2s+m} c_{i+2s-r}^{2^r} = 0.$$

Since $c_{i+2s+m-r} \neq 0$, $c_{i+2s-r} \neq 0$, $c_{i+s-r} \neq 0$, we get from (c'), (d''), (a')

$$c_{i+s}c_{i+s-r}^{-2^r} \neq c_{i+2s}c_{i+2s-r}^{-2^r},$$
$$c_{i+2s}c_{i+2s-r}^{-2^r} = c_{i+2s+m}c_{i+2s+m-r}^{-2^r},$$
$$c_{i+s}c_{i+s-r}^{-2^r} = c_{i+2s+m}c_{i+2s+m-r}^{-2^r}.$$

Thus we come to an obvious contradiction.

Case 2 When $c_{i+2s+m-r} \neq 0$, $c_{i+2s-r} \neq 0$, and $c_{i+s-r} = 0$.

Since $c_{i+s-r} = 0$, we get $c_{i+s} \neq 0$ from (c'). For $c_{i+s-r} = 0$, $c_{i+s} \neq 0$, we have $c_{i+2s+m-r} = 0$ from (a'), a contradiction.

Case 3 When $c_{i+2s+m-r} \neq 0$, $c_{i+2s-r} = 0$.

Since $c_{i+2s-r} = 0$, we have $c_{i+2s} \neq 0$ from (c'), but $c_{i+2s+m-r} \neq 0$, $c_{i+2s-r} = 0$, which is contradict with (d'').

Case 4 When $c_{i+2s+m-r} = 0$.

Since $c_{i+2s+m-r} = 0$, we get $c_{i+2s+m} \neq 0$, $c_{i+m+s-r} \neq 0$ from (e'), therefore $c_{i+2s-r} = 0$ from (d''), moreover $c_{i+2s} \neq 0$, $c_{i+s-r} \neq 0$ from (c'), which is a contradiction with (a').

Therefore the hypothesis that there exists $b_i \neq 0$ for some i is not valid, i.e. $L_1(x) = 0$. whereas $f_3(x)$ is EA-inequivalent to Gold function $g(x) = x^{2^r+1}$.

□

Let $q = 2^m$, $n = 2m$, $\gcd(i, m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ have no solution x such that $x^{q+1} = 1$. Then $f_4(x) = x(x^{2^i} + x^q + cx^{2^iq}) + x^{2^i}(c^qx^q + sx^{2^iq}) + x^{(2^i+1)q}$ is a quadratic APN function[18]. By the transitivity of equivalence and Theorem 3.7 in [1], combing Proposition 3.5 or 3.6, we have the following proposition.

Proposition 3.7. *$f_4(x)$ is CCZ-inequivalent to Gold function $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to $n = 2m$.*

For any n, $f(x) = x^3 + \mathrm{Tr}(x^9)$ is an APN function over $\mathbb{F}_{2^n}$ [16], and this function has the following property.

Proposition 3.8 ([16],Theorem 3)**.** *Let $f(x) = x^3 + \mathrm{Tr}(x^9)$. If $n \geq 7$ and $n > 2p$ ($p \neq 1, 3$ and p is the smallest positive integer with $(p, n) = 1$), then $f(x)$ is CCZ-inequivalent to $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

At the same time, Budaghyan et al. proved that $f(x)$ in Proposition 3.8 is CCZ-inequivalent to any power function over $\mathbb{F}_{2^7}$ ([16],Corollary 4), but for $n > 7$, there are no results.

$f(x) = x^3 + \mathrm{Tr}(x^9)$ is generalized to the form $f_5(x) = x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ with $a \neq 0$ in [19]. Furthermore $f_6(x) = x^3 + a^{-1}\mathrm{Tr}_n^3(a^3x^9 + a^6x^{18})$ and $f_7(x) = x^3 + a^{-1}\mathrm{Tr}_n^3(a^6x^{18} + a^{12}x^{36})$ are constructed when $3|n$ and $a \neq 0$, all of them are quadratic APN functions.

Proposition 3.9. *Let $a \neq 0$, $n \geq 6$. Then $f_5(x) = x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ is CCZ-inequivalent to $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

Proof. We assume $f_5(x)$ is EA-equivalent to some Gold function. Because the two functions are quadratic, we can assume there exist linear permutations $L_1(x) = \sum_{i=0}^{n-1} b_ix^{2^i}$, $L_2(x) = \sum_{i=0}^{n-1} c_ix^{2^i}$ and affine function $L'(x)$ such that $L_1(f_5(x)) = g(L_2(x)) + L'(x)$, that is

$$\sum_{i=0}^{n-1} b_i(x^3 + a^{-1}\mathrm{Tr}(a^3x^9))^{2^i} = (\sum_{i=0}^{n-1} c_ix^{2^i})^{2^r+1} + L'(x),$$

which is equivalent to

$$\sum_{i=0}^{n-1} b_ix^{3\cdot 2^i} + (\sum_{i=0}^{n-1} b_ia^{-2^i})\mathrm{Tr}(a^3x^9) = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} c_jc_i^{2^r}x^{2^{r+i}+2^j} + L'(x). \tag{7}$$

It follows from $L_1(x)$ is a permutation that we have $L_1(a^{-1}) = \sum_{i=0}^{n-1} b_ia^{-2^i} \neq 0$. Then for any j the coefficient of the term of the type $x^{9\cdot 2^j}$ is nonzero on the left hand of equality (7). Hence this is true for the right hand of equality (7), by Corollary 2.6, we have

$$(a) \quad c_{j+3}c_{j-r}^{2^r} + c_jc_{j+3-r}^{2^r} \neq 0, \text{ for any } j.$$

Since $n \geq 6$, there exists integer p with $p \neq 1$, $p \neq 3$, $\gcd(p, n) = 1$. By Lemma 3.5, for any j, the term of the type $x^{2^j(2^p+1)}$ is missing in the left hand of (7), so we get the equality from the right hand of (7)

$$(b) \quad c_{j+p}c_{j-r}^{2^r} + c_j c_{j+p-r}^{2^r} = 0, \text{ for any } j.$$

If for any j, $c_j \neq 0$, then from (a) and (b), we have

$$\begin{aligned} (c) \quad & c_j c_{j-r}^{-2^r} \neq c_{j+3} c_{j+3-r}^{-2^r} \\ (d) \quad & c_j c_{j-r}^{-2^r} = c_{j+p} c_{j+p-r}^{-2^r}. \end{aligned}$$

From (d), we get

$$c_j c_{j-r}^{-2^r} = c_{j+p} c_{j+p-r}^{-2^r} = c_{j+2p} c_{j+2p-r}^{-2^r} = \cdots = c_{j+(n-1)p} c_{j+(n-1)p-r}^{-2^r}.$$

Since $\gcd(n, p) = 1$, we have $c_{j+sp} \neq c_{j+tp}$ if $0 \leq s \neq t \leq n-1$, which implies $c_j c_{j-r}^{-2^r} = c_m c_{m-r}^{-2^r}$ for any m, It contradicts (c).

Thus there exists some j such that $c_j = 0$, which implies $c_{j+p} = 0$ from (a) and (b). Repeating this process, we have $c_{j+kp} = 0$, for any k. But $\gcd(n, p) = 1$ implies $c_j = 0$ for any j. A contradiction. Thus $f_5(x)$ is EA-inequivalent to any Gold function. □

By the similar process of proof in Proposition 3.9, we have the following two propositions.

Proposition 3.10. *Let $a \neq 0$, $3|n$. Then $f_6(x) = x^3 + a^{-1}\mathrm{Tr}_n^3(a^3x^9 + a^6x^{18})$ is CCZ-inequivalent to $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

Proposition 3.11. *Let $a \neq 0$, $3|n$. Then $f_7(x) = x^3 + a^{-1}\mathrm{Tr}_n^3(a^6x^{18} + a^{12}x^{36})$ is CCZ-inequivalent to $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

Let $n = 3k$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3 \mid (k + s)$, u primitive in $\mathbb{F}_{2^n}^*$. Then

$$f_8(x) = ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1}(v \neq 0),$$

$$f_9(x) = ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + wu^{2^k+1}x^{2^s+2^{k+s}}(w \neq 0)$$

are quadratic APN functions. [21, 20]

Similarly as Lemma 3.5, we have the following lemma.

Lemma 3.12. (1) $\{x^{2^i(2^{k+s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)}|i \in \mathbb{Z}\} = \{x^{2^i(2^{k+s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^{2k+s}+1)}|i \in \mathbb{Z}\} = \{x^{2^i(2^{k+s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^k+1)}|i \in \mathbb{Z}\} = \varnothing$;

(2) $\{x^{2^i(2^{k+2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)}|i \in \mathbb{Z}\} = \{x^{2^i(2^{k+2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^{2k+s}+1)}|i \in \mathbb{Z}\} = \{x^{2^i(2^{k+2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^k+1)}|i \in \mathbb{Z}\} = \varnothing$;

(3) $\{x^{2^{i+k-s}(2^{2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^s+1)}|i \in \mathbb{Z}\} = \{x^{2^{i+k-s}(2^{2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^{2k+s}+1)}|i \in \mathbb{Z}\} = \{x^{2^{i+k-s}(2^{2s}+1)}|i \in \mathbb{Z}\} \cap \{x^{2^i(2^k+1)}|i \in \mathbb{Z}\} = \varnothing$;

Proposition 3.13. *$f_8(x)$ is not EA-equivalent to Gold function $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n*

Proof. We assume $f_8(x)$ is EA-equivalent to Gold function. Because the two functions are quadratic, we can assume there exist linear functions $L_1(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$, $L_2(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$ and affine function $L'(x)$ such that $L_1(f_8(x)) = g(L_2(x)) + L'(x)$, that is

$$\sum_{i=0}^{n-1} b_i(ux^{2^s+1} + u^{2^k}x^{2^{2k}+2^{k+s}} + vx^{2^{2k}+1})^{2^i} = (\sum_{i=0}^{n-1} c_i x^{2^i})^{2^r+1} + L'(x). \tag{8}$$

The left hand of equality (8) equals to

$$\sum_{i=0}^{n-1} b_i u^{2^i} x^{2^i(2^s+1)} + \sum_{i=0}^{n-1} b_i u^{2^{i+k}} x^{2^{i+k}(2^k+2^s)} + \sum_{i=0}^{n-1} b_i v^{2^i} x^{2^i(2^{2k}+1)}.$$

On the left hand of equality (8), we only have the terms of the type

$$x^{2^i(2^s+1)},\ x^{2^{i+k}(2^k+2^s)},\ x^{2^i(2^{2k}+1)}.$$

We will prove that equality (8) holds only if $b_i = 0$ for all i. Assume on the contrary there exists $b_i \neq 0$ for some i. As a consequence all the coefficients of the terms of the type $x^{2^i(2^s+1)}$, $x^{2^{i+k}(2^k+2^s)}$ and $x^{2^i(2^{2k}+1)}$ are nonzero on the left hand of equality (8). Hence this is true for the right hand of equality (8), by Corollary 2.6, we have

$$\begin{array}{ll}(a) & c_{i+s}c_{i-r}^{2^r} + c_i c_{i+s-r}^{2^r} \neq 0,\\ (b) & c_{i+2k}c_{i+k+s-r}^{2^r} + c_{i+k+s}c_{i+2k-r}^{2^r} \neq 0,\\ (c) & c_{i+2k}c_{i-r}^{2^r} + c_i c_{i+2k-r}^{2^r} \neq 0,\end{array}$$

By (1) and (2) of Lemma 3.12, the terms of the type $x^{2^i(2^{k+s}+1)}$, $x^{2^i(2^{k+2s}+1)}$ are missing in the left hand of equality (8), we get the equalities from the right hand of equality (8)

$$\begin{array}{ll}(d) & c_i c_{i+s+k-r}^{2^r} + c_{i+s+k}c_{i-r}^{2^r} = 0, \text{ for any } i,\\ (i) & c_i c_{i+2s+k-r}^{2^r} + c_{i+2s+k}c_{i-r}^{2^r} = 0, \text{ for any } i,\end{array}$$

1) If $b_{i+k+s} = 0$, then the coefficient of the term of the type $x^{2^{i+k+s}(2^{2k}+1)}$ is zero on the left hand of equality (8). As a consequence the coefficient of the term of the type $x^{2^{i+k+s}(2^{2k}+1)}$ is zero on the right hand of equality (8). By Corollary 2.6, we have

$$(e) \quad c_{i+s}c_{i+k+s-r}^{2^r} + c_{i+k+s}c_{i+s-r}^{2^r} = 0,$$

We consider the following cases.

Case 1 When $c_{i+s+k-r} \neq 0$, $c_{i+s-r} \neq 0$, and $c_{i-r} \neq 0$.

Since $c_{i+s+k-r} \neq 0$, $c_{i+s-r} \neq 0$, and $c_{i-r} \neq 0$, we get from (d), (e), (a)

$$\begin{array}{l}c_i c_{i-r}^{-2^r} = c_{i+k+s}c_{i+k+s-r}^{-2^r},\\ c_{i+s}c_{i+s-r}^{-2^r} = c_{i+k+s}c_{i+k+s-r}^{-2^r},\\ c_i c_{i-r}^{-2^r} \neq c_{i+s}c_{i+s-r}^{-2^r}.\end{array}$$

Therefore we come to an obvious contradiction.

Case 2 When $c_{i+s+k-r} \neq 0$, $c_{i+s-r} \neq 0$, and $c_{i-r} = 0$.

Since $c_{i-r} = 0$, we get $c_i \neq 0$ from (a). For $c_i \neq 0$, $c_{i-r} = 0$, we have $c_{i+s+k-r} = 0$ from (d), a contradiction.

Case 3 When $c_{i+s+k-r} \neq 0$, $c_{i+s-r} = 0$.

Since $c_{i+s-r} = 0$, we get $c_{i+s} \neq 0$ from (a). For $c_{i+s} \neq 0$, $c_{i+s-r} = 0$, we have $c_{i+s+k-r} = 0$ from (e), a contradiction.

Case 4 When $c_{i+s+k-r} = 0$.

Since $c_{i+s+k-r} = 0$, we have $c_{i+s+k} \neq 0$ from (b). Furthermore, (e) implies $c_{i+s-r} = 0$, hence $c_{i-r} \neq 0$ from (a). The fact $c_{i+s+k} \neq 0$, $c_{i-r} \neq 0$, $c_{i+k+s-r} = 0$ implies a contradiction with (d).

2) If $b_{i+k+s} \neq 0$, then the coefficients of the terms of the type $x^{2^{i+k+s}(2^s+1)}$, $x^{2^{i+2k+s}(2^k+2^s)}$ and $x^{2^{i+k+s}(2^{2k}+1)}$ are nonzero on the left hand of equality (8). As a consequence the coefficients of the terms of the type $x^{2^{i+k+s}(2^s+1)}$, $x^{2^{i+2k+s}(2^k+2^s)}$ and $x^{2^{i+k+s}(2^{2k}+1)}$ are zero on the right hand of equality (8). By Corollary 2.6, we have

$$\begin{array}{ll}(h) & c_{i+k+2s}c_{i+k+s-r}^{2^r} + c_{i+k+s}c_{i+k+2s-r}^{2^r} \neq 0,\\ (f) & c_{i+s}c_{i+2s+2k-r}^{2^r} + c_{i+2k+2s}c_{i+s-r}^{2^r} \neq 0,\\ (g) & c_{i+s}c_{i+k+s-r}^{2^r} + c_{i+k+s}c_{i+s-r}^{2^r} \neq 0.\end{array}$$

We consider the following cases.

Case 1 When $c_{i-r} \neq 0$, $c_{i+k+2s-r} \neq 0$ and $c_{i+k+s-r} \neq 0$.

Since $c_{i-r} \neq 0$, $c_{i+k+2s-r} \neq 0$ and $c_{i+k+s-r} \neq 0$, we get from (i), (d), (h)

$$\begin{array}{l}c_i c_{i-r}^{-2^r} = c_{i+k+2s}c_{i+k+2s-r}^{-2^r},\\ c_i c_{i-r}^{-2^r} = c_{i+s+k}c_{i+s+k-r}^{-2^r},\\ c_{i+k+2s}c_{i+k+2s-r}^{-2^r} \neq c_{i+s+k}c_{i+s+k-r}^{-2^r}.\end{array}$$

So we come to an obvious contradiction.

Case 2 When $c_{i-r} \neq 0$, $c_{i+k+2s-r} \neq 0$, and $c_{i+k+s-r} = 0$.

Since $c_{i+k+s-r} = 0$, we get $c_{i+k+s} \neq 0$ from (b). For $c_{i+k+s} \neq 0$, $c_{i+k+s-r} = 0$, we have $c_{i-r} = 0$ from (d), a contradiction.

Case 3 When $c_{i-r} \neq 0$, $c_{i+k+2s-r} = 0$.

Since $c_{i+k+2s-r} = 0$, we have $c_{i+k+2s} \neq 0$ from (h). For $c_{i+k+2s-r} = 0$, $c_{i+k+2s} \neq 0$, we have $c_{i-r} = 0$ from (i), a contradiction.

Case 4 When $c_{i-r} = 0$.

Since $c_{i-r} = 0$, we get $c_i \neq 0$, $c_{i+s-r} \neq 0$ from (a). Moreover, $c_{i+k+2s-r} = 0$ from (i) and $c_{i+k+s-r} = 0$ from (d), which is a contradiction with (h).

Therefore the hypothesis that there exists $b_i \neq 0$ for some i is not valid, i.e. $L_1(x) = 0$. whereas $f_8(x)$ is EA-inequivalent to Gold function $g(x) = x^{2^r+1}$.

□

Proposition 3.14. *$f_9(x) = ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + wu^{2^k+1}x^{2^s+2^{k+s}}$ $(w \neq 0)$ is CCZ-inequivalent to gold function $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

Proof. We assume $f_9(x)$ is EA-equivalent to some Gold function. Because the two functions are quadratic, we can assume there exist linear permutations $L_1(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$, $L_2(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$ and affine function $L'(x)$ such that $L_1(f_9(x)) = g(L_2(x)) + L'(x)$, that is

$$\sum_{i=0}^{n-1} b_i (ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + wu^{2^k+1}x^{2^s+2^{k+s}})^{2^i} = (\sum_{i=0}^{n-1} c_i x^{2^i})^{2^r+1} + L'(x). \tag{9}$$

The left hand of equality (9) equals to

$$\sum_{i=0}^{n-1} b_i u^{2^i} x^{2^i(2^s+1)} + \sum_{i=0}^{n-1} b_i u^{2^{k+i}} x^{2^{i+k}(2^k+2^s)} + \sum_{i=0}^{n-1} b_i w^{2^i} x^{2^{i+s}(2^k+1)}$$

On the left hand of equality (9), we only have the terms of the type

$$x^{2^i(2^s+1)},\ x^{2^{i+k}(2^k+2^s)},\ x^{2^{i+s}(2^k+1)}.$$

We will prove that equality (9) holds only if $b_i = 0$ for all i. If there exists $b_i \neq 0$ for some i. As a consequence all the coefficients of the terms of the type $x^{2^i(2^s+1)}$, $x^{2^{i+k}(2^k+2^s)}$ and $x^{2^{i+s}(2^k+1)}$ are nonzero on the left hand of equality (9). Hence this is true for the right hand of equality (9), by Corollary 2.6, we have

$$\begin{array}{ll} (a) & c_{i+s}c_{i-r}^{2^r} + c_i c_{i+s-r}^{2^r} \neq 0, \\ (b) & c_{i+2k}c_{i+k+s-r}^{2^r} + c_{i+k+s}c_{i+2k-r}^{2^r} \neq 0, \\ (c) & c_{i+s}c_{i+s+k-r}^{2^r} + c_{i+s+k}c_{i+s-r}^{2^r} \neq 0. \end{array}$$

By (1), (2) of Lemma 3.12, the terms of the type $x^{2^i(2^{k+s}+1)}$, $x^{2^i(2^{k+2s}+1)}$ are missing in the left hand of equality (9), we get the equalities from the right hand of equality (9)

$$\begin{array}{ll} (d) & c_i c_{i+s+k-r}^{2^r} + c_{i+s+k}c_{i-r}^{2^r} = 0, \text{ for any } i, \\ (e) & c_i c_{i+2s+k-r}^{2^r} + c_{i+2s+k}c_{i-r}^{2^r} = 0, \text{ for any } i. \end{array}$$

1) If $b_{i+2k-s} = 0$, then the coefficients of the terms of the type $x^{2^{i+2k-s}(2^s+1)}$, $x^{2^{i-s}(2^k+2^s)}$ and $x^{2^i(2^{2k}+1)}$ are zero on the left hand of equality (9). As a consequence the coefficients of the terms of the type $x^{2^{i+2k-s}(2^s+1)}$, $x^{2^{i-s}(2^k+2^s)}$ and $x^{2^i(2^{2k}+1)}$ are zero on the right hand of equality (9). By Corollary 2.6, we have

$$\begin{array}{ll} (f) & c_{i+2k}c_{i+2k-s-r}^{2^r} + c_{i+2k-s}c_{i+2k-r}^{2^r} = 0, \\ (g) & c_{i+k-s}c_{i-r}^{2^r} + c_i c_{i+k-s-r}^{2^r} = 0, \\ (h) & c_{i+2k}c_{i-r}^{2^r} + c_i c_{i+2k-r}^{2^r} = 0. \end{array}$$

We consider the following cases.

Case 1 When $c_{i+s+k-r} \neq 0$, $c_{i-r} \neq 0$, and $c_{i+2k-r} \neq 0$.

Since $c_{i+s+k-r} \neq 0$, $c_{i-r} \neq 0$, and $c_{i+2k-r} \neq 0$, we get from (d), (h), (b)

$$\begin{aligned} &c_i c_{i-r}^{-2^r} = c_{i+k+s} c_{i+k+s-r}^{-2^r}, \\ &c_{i+2k} c_{i+2k-r}^{-2^r} = c_i c_{i-r}^{-2^r}, \\ &c_{i+2k} c_{i+2k-r}^{-2^r} \neq c_{i+k+s} c_{i+k+s-r}^{-2^r}. \end{aligned}$$

Thus we come to an obvious contradiction.

Case 2 When $c_{i+s+k-r} \neq 0$, $c_{i-r} \neq 0$, and $c_{i+2k-r} = 0$.

Since $c_{i+2k-r} = 0$, we get $c_{i+2k} \neq 0$ from (b). For $c_{i+2k-r} = 0$, $c_{i+2k} \neq 0$, we have $c_{i-r} = 0$ from (h), a contradiction.

Case 3 When $c_{i+s+k-r} \neq 0$, $c_{i-r} = 0$.

Since $c_{i-r} = 0$, we get $c_{i+s-r} \neq 0$, $c_i \neq 0$ from (a). As a consequence we have $c_{i+s+k-r} = 0$ from (d), a contradiction.

Case 4 When $c_{i+s+k-r} = 0$.

Since $c_{i+s+k-r} = 0$, we have $c_{i+s+k} \neq 0$, $c_{i+s-r} \neq 0$ from (c). Furthermore, (b) implies $c_{i+2k-r} \neq 0$ and (d) implies $c_{i-r} = 0$. Because of $c_{i-r} = 0$, we have $c_i \neq 0$ from (a). The fact $c_i \neq 0$, $c_{i+2k-r} \neq 0$, $c_{i-r} = 0$ implies that there is a contradiction with (h).

2) If $b_{i+2k-s} \neq 0$, then the coefficients of the terms of the type $x^{2^{i+2k-s}(2^s+1)}$, $x^{2^{i-s}(2^k+2^s)}$ and $x^{2^i(2^{2k}+1)}$ are nonzero on the left hand of equality (9). As a consequence the coefficients of the terms of the type $x^{2^{i+2k-s}(2^s+1)}$, $x^{2^{i-s}(2^k+2^s)}$ and $x^{2^i(2^{2k}+1)}$ are nonzero on the right hand of equality (9). By Corollary 2.6, we have

$$\begin{aligned} &(i) \quad c_{i+2k} c_{i+2k-s-r}^{2^r} + c_{i+2k-s} c_{i+2k-r}^{2^r} \neq 0, \\ &(j) \quad c_{i+k-s} c_{i-r}^{2^r} + c_i c_{i+k-s-r}^{2^r} \neq 0, \\ &(k) \quad c_{i+2k} c_{i-r}^{2^r} + c_i c_{i+2k-r}^{2^r} \neq 0. \end{aligned}$$

From (3) of Lemma 3.1, the term of the type $x^{2^{i+k-s}(2^{2s}+1)}$ is missing on the left hand of equality (9), it is true for the right hand of equality (9), as a consequence we have

$$(l) \quad c_{i+k+s} c_{i+k-s-r}^{2^r} + c_{i+k-s} c_{i+k+s-r}^{2^r} = 0.$$

We consider the following cases.

Case 1 When $c_{i-r} \neq 0$, $c_{i+k+s-r} \neq 0$ and $c_{i+k-s-r} \neq 0$.

Since $c_{i-r} \neq 0$, $c_{i+k+s-r} \neq 0$ and $c_{i+k-s-r} \neq 0$, we get from (l), (d), (j)

$$\begin{aligned} &c_{i+k+s} c_{i+s+k-r}^{-2^r} = c_{i+k-s} c_{i+k-s-r}^{-2^r}, \\ &c_i c_{i-r}^{-2^r} = c_{i+s+k} c_{i+s+k-r}^{-2^r}, \\ &c_i c_{i-r}^{-2^r} \neq c_{i+k-s} c_{i+k-s-r}^{-2^r}. \end{aligned}$$

Therefore we come to an obvious contradiction.

Case 2 When $c_{i-r} \neq 0$, $c_{i+k+s-r} \neq 0$ and $c_{i+k-s-r} = 0$.

Since $c_{i+k-s-r} = 0$, we get $c_{i+k-s} \neq 0$ from (j). For $c_{i+k-s} \neq 0$, $c_{i+k-s-r} = 0$, we have $c_{i+k+s-r} = 0$ from (l), a contradiction.

Case 3 When $c_{i-r} \neq 0$, $c_{i+k+s-r} = 0$.

Since $c_{i+k+s-r} = 0$, we have $c_{i+k+s} \neq 0$ from (b). For $c_{i+k+s-r} = 0$, $c_{i+k+s} \neq 0$, we have $c_{i-r} = 0$ from (d), a contradiction.

Case 4 When $c_{i-r} = 0$.

Since $c_{i-r} = 0$, we get $c_i \neq 0$, $c_{i+s-r} \neq 0$ from (a). Therefore $c_{i+k+s-r} = 0$ from (d), $c_{i+k+s} \neq 0$ from (c), and $c_{i+k-s-r} \neq 0$ from (j), which is a contradiction with (l).

Therefore the hypothesis that there exists $b_i \neq 0$ for some i is not valid, i.e. $L_1(x) = 0$. whereas $f_9(x)$ is EA-inequivalent to Gold function $g(x) = x^{2^r+1}$.

□

Let s, k, p be positive integers. If $n = pk \geq 12$, $p \in \{3, 4\}$, $\gcd(k, p) = \gcd(s, pk) = 1$, $i \equiv sk \mod p$, $t = p - i$, $\alpha \in F_{2^n}^*$ is a prime element, then $f_i(x) = x^{2^{s+1}} + \alpha^{2^k-1} x^{2^{ik}+2^{kt+s}}$ is an APN function with the following property

$(i = 1, 2)$[15].

Proposition 3.15 ([15],Corollary 4, 5)**.** *If $k \geq l$, then $f_i(x), i = 1, 2$ are CCZ-inequivalent to gold function $g(x) = x^{2^r+1}$, where $1 \leq r < \frac{n}{2}$ coprime to n.*

Theorem 3.16. *The quadratic APN functions $f_i(x)$ $(i = 1, 2, 4, 5, 6, 7, 8, 9)$ are CCZ-inequivalent to power APN functions.*

Proof. It is obvious by combing Theorem 2.4 and Proposition 3.7, 3.9, 3.10, 3.11, 3.13, 3.14 3.15. □

Therefore we give the theoretical proof of the inequivalence between $f_i(x)$ $(i = 1, 2, 4, 5, 6, 7, 8, 9)$ and power APN functions, as a consequence, $f(x)$ in Proposition 3.8 is CCZ-inequivalent to power APN functions on F_{2^n} for any n.

[1] Budaghyan L, Calderini M, Villa I.: On Equivalences between known families of quadratic APN functions. Https://eprint.iacr.org/2019/793.pdf

[2] Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions[J]. IEEE Transactions on Information Theory, 1968, 14(1): 154-156

[3] Kasami T. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes[J]. Information and Control, 1971, 18(4): 369-394

[4] Dobbertin H. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case[J]. IEEE Transactions on Information Theory, 1999, 45(4): 1271-1275

[5] Dobbertin H. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case[J]. Information and Computation, 1999, 151(1-2): 57-72

[6] Beth T, Ding C. On almost perfect nonlinear permutations[C]//Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993: 65-76

[7] Nyberg K. Differentially uniform mappings for cryptography[C]// Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993: 55-64

[8] Dobbertin H. Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5[C]//Finite Fields and Applications. Springer, Berlin, Heidelberg, 2001: 113-121

[9] Yoshiara S. Equivalences of power APN funcitons with power or quadratic APN functions[J]. Journal of Algebraic Combinatorics, 2016, 44(3): 561-585

[10] Budaghyan L. On inequivalence between known power APN functions[C]//Proc. Conference BFCA 2008, Copenhagen. 2008

[11] Lachaud G, Wolfmann J. The weights of the orthogonals of the extended quadratic binary Goppa codes[J]. IEEE Transactions on Information Theory, 1990, 36(3): 686-692

[12] Canteaut A, Charpin P, Dobbertin H. Weight divisibility of cyclic codes, highly nonlinear functions on F_2^m , and crosscorrelation of maximum-length sequences[J]. Society for Industrial and Applied Mathe- matics, 2000, 13 (1) :105-138

[13] Bracken C, Byrne E, Markin N, et al.On the equivalence of quadratic APN funcitons[J].Designs,Code and Cryptography, 2011, 61(3): 261-272

[14] Dempwolff U. CCZ equivalence of power functions[J]. Designs, Codes and Cryptography, 2018, 86(3): 665-692

[15] Budaghyan L, Carlet C, Leander G. Two classes of quadratic APN binomials inequivalent to power functions[J]. IEEE Transactions on Information Theory, 2008, 54(9): 4218-4229

[16] Budaghyan L, Carlet C, Leander G. Constructing new APN functions from known ones[J]. Finite Fields and Their Applications, 2009, 15(2): 150-159

[17] Yoshiara S. Equivalences of quadratic APN functions[J]. Journal of Algebraic Combinatorics, 2012, 35(3): 461-475

[18] Budaghyan L, Carlet C. Classes of quadratic APN trinomials and hexanomials and related structures[J].IEEE Transactions on Information Theory, 2008, 54(5): 2354-2357

[19] Budaghyan L, Carlet C, Leander G. On a construction of quadratic APN functions. In 2009 IEEE Information Theory Workshop, 2009: 374-378

[20] Bracken C, Byrne E, Markin N, et al. A few more quadratic APN functions[J]. Cryptography and Communications, 2011, 3(1): 43-53

[21] Bracken C, Byrne E, Markin N, et al. New families of quadratic almost perfect nonlinear trinomials and multinomials[J]. Finite Fields and Their Applications, 2008, 14(3): 703-714

[22] Zhou Y, Pott A. A new family of semifields with 2 parameters[J]. Advances in Mathematics, 2013, 234: 43-60

[23] Budaghyan L, Calderini C, Carlet R, Coulter R, Villa I. Construting APN functions through iostopic shift. Cryptology ePrint Archive, Report 2018/769

[24] Taniguchi H. On some quadratic APN functions. Des, Codes Cryptogr. 2019, https://doi.org/10.1007/S10623-018-00598-2