A class of quadratic APN binomials inequivalent to power functions[*]

Lilya Budaghyan[†] Claude Carlet[‡] Gregor Leander[§]

November 30, 2006

Abstract

We exhibit an infinite class of almost perfect nonlinear quadratic binomials from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ ($n \geq 12$, n divisible by 3 but not by 9). We prove that these functions are EA-inequivalent to any power function and that they are CCZ-inequivalent to any Gold function and to any Kasami function. It means that for n even they are CCZ-inequivalent to any known APN function, and in particular for $n = 12, 24$, they are therefore CCZ-inequivalent to any power function.

It is also proven that, except in particular cases, the Gold mappings are CCZ-inequivalent to the Kasami and Welch functions.

Keywords. Affine equivalence, Almost bent, Almost perfect nonlinear, CCZ-equivalence, Differential uniformity, Nonlinearity, S-box, Vectorial Boolean function.

1 Introduction

Since the introduction by Biham and Shamir of differential attacks on block ciphers [4] and by Matsui of linear attacks [28], and since the introduction by Nyberg [29] of the related notion of almost perfect nonlinear (APN) mappings, and by Chabaud and Vaudenay of the notion of almost bent (AB) mappings [13], much work has been done on these two notions [1, 3, 6, 8, 9, 10, 12, 15, 16, 17, 18, 23, 24, 25]. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called APN if, for every $a \neq 0$ and every b in $\mathbb{F}_2^n$, the equation $F(x)+F(x+a) = b$ admits at most two (that is, 0 or 2) solutions (it is also called differentially 2-uniform). A function F is called AB if the minimum Hamming distance between all Boolean functions $v \cdot F$, $v \in \mathbb{F}_2^n \setminus \{0\}$ (where "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^n$) and all affine Boolean functions on $\mathbb{F}_2^n$ is maximal

[*] Part of this paper was presented at ISIT 2006 [5].

[†] Department of Mathematics, University of Trento, I-38050 Povo (Trento), ITALY; e-mail: lilia.b@mail.ru

[‡] INRIA, Projet CODES, BP 105, 78153, Le Chesnay, FRANCE; e-mail: claude.carlet@inria.fr; he is also a member of the University of Paris 8.

[§] Department of Mathematics, Ruhr-University, Bochum, D-44780 Bochum, GERMANY; e-mail: leander@itsc.ruhr-uni-bochum.de.

(this distance is called the nonlinearity of F and this maximum equals $2^{n-1} - 2^{\frac{n-1}{2}}$). A comprehensive survey on APN and AB functions can be found in [11].

Until recently, all known constructions of APN and AB functions happened to be EA-equivalent to power functions $x \to x^d$ (where x ranges over the finite field $\mathbb{F}_{2^n}$, identified as a vector space to $\mathbb{F}_2^n$). Recall that two functions F and F' are called extended affine equivalent (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings A, A_1, A_2 are affine, and where A_1, A_2 are permutations. Table 1 (resp. Table 2) gives all known values of exponents d (up to multiplication by a power of 2 modulo $2^n - 1$, and up to taking the inverse when a function is a permutation) such that the power function x^d is APN (resp. AB).

Table 1
Known APN power functions x^d on $\mathbb{F}_{2^n}$.

Functions	Exponents d	Conditions	Proven in
Gold	$2^i + 1$	$\gcd(i, n) = 1$	[22, 29]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[25, 26]
Welch	$2^t + 3$	$n = 2t + 1$	[17]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[16]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[3, 29]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[18]

Table 2
Known AB power functions x^d on $\mathbb{F}_{2^n}$, n odd.

Functions	Exponents d	Conditions	Proven in
Gold	$2^i + 1$	$\gcd(i, n) = 1$	[22, 29]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[26]
Welch	$2^t + 3$	$n = 2t + 1$	[9, 10]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[24]

Every power APN function is a permutation when n is odd [20]. For n even case it is conjectured by Canteaut, Carlet, Charpin, Dobbertin and Zinoviev that there exists no APN permutation. Every AB function is APN [13]. The converse is not true in general since AB functions exist only when n is odd while APN functions exist for n even too. Besides, in the n odd case, the Dobbertin APN function is not AB as proven in [10]. Also, in this same case, the inverse APN function is not AB since it has the algebraic degree $n-1$ while the algebraic degree of any AB function is not greater than $(n+1)/2$ (see [12]). But, if n is odd again, every APN mapping which is quadratic (that is, whose algebraic degree equals 2) is AB [12].

When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [29] and has the best known nonlinearity [27], that is $2^{n-1} - 2^{\frac{n}{2}}$ (see [10, 15]). This function has been chosen as the basic S-box, with $n = 8$, in the Advanced Encryption Standard (AES), see [14].

Several conjectures have been made on APN and AB functions. In particular, it was widely accepted as plausible that all APN functions are EA-equivalent to power functions and as a consequence it was conjectured in [12] that all AB functions are EA-equivalent to permutations, and that all quadratic AB functions are EA-equivalent to Gold functions (this last conjecture was restated for APN functions in [2]). Using the stability properties studied in [12] and more recently called CCZ-equivalence (cf. definition at Section 2), new infinite classes of APN and AB functions have been introduced in [6] (see also [7]) and solved the first two problems.

The new APN and AB functions introduced in [7] are, by construction, CCZ-equivalent to Gold functions. Hence, the problem of knowing whether there exist APN functions which would be CCZ-inequivalent to power functions remained open after their introduction. A recent paper [21] introduces two quadratic functions from $\mathbb{F}_{2^{10}}$ (resp. $\mathbb{F}_{2^{12}}$) to itself. The first one is proved to be CCZ-inequivalent to any power function. The exhibition of this function also solves the third of the problems recalled above.

These two (quadratic) functions are isolated and this leaves open the question of knowing whether a whole infinite class of APN functions being not CCZ-equivalent to power functions can be exhibited.

In the present paper, we introduce an infinite class of quadratic APN functions on every number of variables n, divisible by 3, but not by 9. We show that, for $n \geq 12$, these functions are EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami functions. This implies that for n even they are CCZ-inequivalent to all known APN functions. In particular, for $n = 12, 24$, they are indeed CCZ-inequivalent to any power mappings. Furthermore, we consider an open question about CCZ-inequivalence of two different functions from Table 1 to each other. We prove that, except in particular cases, the Gold functions are CCZ-inequivalent to the Kasami and Welch functions, and that two Gold functions are CCZ-equivalent if and only if they are EA-equivalent.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the field $\mathbb{F}_2$. Any function F from $\mathbb{F}_2^n$ to itself can be uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_2^n$, whose degree with respect to each coordinate is at most 1:

$$F(x_1, ..., x_n) = \sum_{u \in \mathbb{F}_2^n} c(u) \big(\prod_{i=1}^{n} x_i^{u_i} \big), \qquad c(u) \in \mathbb{F}_2^n.$$

This representation is called the *algebraic normal form* of F and its degree $d^\circ(F)$ the *algebraic degree* of the function F.

Besides, the field $\mathbb{F}_{2^n}$, as any n-dimensional vector space over $\mathbb{F}_2$, can be identified with $\mathbb{F}_2^n$, as a vector space. Then, viewed as a function from this field to itself, F has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree smaller than 2^n:

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

For any k, $0 \leq k \leq 2^n - 1$, the number $w_2(k)$ of the nonzero coefficients $k_s \in \{0, 1\}$ in the binary expansion $\sum_{s=0}^{n-1} 2^s k_s$ of k is called the 2-*weight* of k. The algebraic degree of F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is $d^\circ(F) = \max_{0 \leq i \leq n-1, c_i \neq 0} w_2(i)$ (see [12]).

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *linear* if and only if $F(x)$ is a linearized polynomial over $\mathbb{F}_{2^n}$, that is,

$$\sum_{i=0}^{n-1} c_i x^{2^i}, \quad c_i \in \mathbb{F}_{2^n}.$$

The sum of a linear function and a constant is called an *affine function*.

Let F be a function from $\mathbb{F}_2^n$ to itself and A_1, $A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be affine permutations. The functions F and $A_1 \circ F \circ A_2$ are then called *affine equivalent*. Affine equivalent functions have the same algebraic degree (i.e. the algebraic degree is *affine invariant*).

As recalled in introduction, we say that the functions F and F' are *extended affine equivalent* if $F' = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and an affine function A. If F is not affine, then F and F' have again the same algebraic degree.

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and any elements $a, b \in \mathbb{F}_2^n$ we denote

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n : F(x + a) + F(x) = b\}|$$

and

$$\Delta_F = \{\delta_F(a, b) : a, b \in \mathbb{F}_2^n, a \neq 0\}.$$

F is called a *differentially δ-uniform* function if $\max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n} \delta_F(a, b) \leq \delta$, where $\mathbb{F}_2^{n*} = \mathbb{F}_2^n \setminus \{0\}$. For any $a, b \in \mathbb{F}_2^n$, the number $\delta_F(a, b)$ is even since if x_0 is a solution of the equation $F(x + a) + F(x) = b$ then $x_0 + a$ is a solution too. Hence, $\delta \geq 2$. Differentially 2-uniform mappings are called *almost perfect nonlinear*.

For any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the distribution of the values

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, \qquad a, b \in \mathbb{F}_2^n,$$

does not depend on a particular choice of the inner product " $\cdot$ " in $\mathbb{F}_2^n$. If we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ then we can take $x \cdot y = tr(xy)$, where $tr(x) = x + x^2 + x^4 + ... + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$. The set $\Lambda_F = \{\lambda_F(a, b) : a, b \in \mathbb{F}_2^n, b \neq 0\}$ is called the *Walsh spectrum* of F and the value

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^{n*}} |\lambda_F(a, b)|$$

equals the *nonlinearity* of the function F. The nonlinearity of any function F satisfies the inequality

$$\mathcal{NL}(F) \le 2^{n-1} - 2^{\frac{n-1}{2}}$$

([13, 30]) and in case of equality F is called *almost bent* or *maximum nonlinear*. For any AB function F, the Walsh spectrum Λ_F equals $\{0, \pm 2^{\frac{n+1}{2}}\}$ as proven in [13].

For EA-equivalent functions F and F', we have $\mathcal{NL}(F) = \mathcal{NL}(F')$, $\Delta_F = \Delta_{F'}$ and if F is a permutation then $\mathcal{NL}(F) = \mathcal{NL}(F^{-1})$, $\Delta_F = \Delta_{F^{-1}}$ (see [12]).

Two mappings F and G from $\mathbb{F}_{2^n}$ to itself are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if the graphs of F and G, that is, the subsets $\{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $\{(x, G(x)) \mid x \in \mathbb{F}_{2^n}\}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, are affine equivalent. Hence, F and G are CCZ-equivalent if and only if there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$y = F(x) \Leftrightarrow L_2(x, y) = G(L_1(x, y)).$$

Note that the function $L_1(x, F(x))$ has to be a permutation too. Indeed, suppose that there exists $x \neq x'$ such that $L_1(x, F(x)) = L_1(x', F(x'))$, then since $\mathcal{L}$ is a permutation, we would have $L_2(x, F(x)) \neq L_2(x', F(x'))$, a contradiction since $L_2(x, F(x)) = G(L_1(x, F(x)))$ and $L_2(x', F(x')) = G(L_1(x', F(x')))$. Note also that, conversely, if F and $\mathcal{L} = (L_1, L_2)$ are respectively a function and an affine automorphism such that the function $L_1(x, F(x))$ is a permutation, then the relation $L_2(x, F(x)) = G(L_1(x, F(x)))$ defines a function G which is CCZ-equivalent to F.

It is shown in [12] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). As shown in [12] too, EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse.

3 A new family of APN functions

The following theorem introduces a large class of quadratic binomial APN functions.

Theorem 1 *Let s and k be positive integers with* $\gcd(s, 3k) = 1$, *and $t \in \{1, 2\}$, $i = 3 - t$. Furthermore let*

$$\begin{aligned} d &= 2^{ik} + 2^{tk+s} - (2^s + 1), \\ g_1 &= \gcd(2^{3k} - 1, d/(2^k - 1)), \\ g_2 &= \gcd(2^k - 1, d/(2^k - 1)), \end{aligned}$$

and α be a primitive element of $\mathbb{F}^*_{2^{3k}}$. If $g_1 \neq g_2$ then the function

$$F(x) = x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}}$$

is almost perfect nonlinear on $\mathbb{F}_{2^{3k}}$ (and is almost bent when k is odd).

Proof. Let $n = 3k$. We have to show that for every $u, v \in \mathbb{F}_{2^n}$, $v \neq 0$, the equation

$$F(x) + F(x+v) = u$$

has at most 2 solutions. We have

$$\begin{aligned}
& F(x) + F(x+v) \\
= \;& \alpha^{2^k-1}\left(x^{2^{ik}+2^{tk+s}} + (x+v)^{2^{ik}+2^{tk+s}}\right) \\
+ \;& x^{2^s+1} + (x+v)^{2^s+1} \\
= \;& \alpha^{2^k-1} v^{2^{ik}+2^{tk+s}} \left(\left(\frac{x}{v}\right)^{2^{ik}} + \left(\frac{x}{v}\right)^{2^{tk+s}}\right) \\
+ \;& v^{2^s+1}\left(\left(\frac{x}{v}\right)^{2^s} + \left(\frac{x}{v}\right)\right) + \alpha^{2^k-1} v^{2^{ik}+2^{tk+s}} + v^{2^s+1}.
\end{aligned}$$

As this is a linear equation in x it is sufficient to study the kernel. Note furthermore that

$$v^{2^{ik}+2^{tk+s}-(2^s+1)} = v^{(2^k-1)(2^{k+s}+2^s+1-2^k(2^s-1)(i-1))}$$

(this can be checked separately for $i = 1$ and $i = 2$). To simplify notation we define

$$a = \left(\alpha v^{2^{k+s}+2^s+1-2^k(2^s-1)(i-1)}\right)^{2^k-1}.$$

After replacing x by vx and dividing by v^{2^s+1}, we finally see that the equation $F(x) + F(x+v) = u$ admits 0 or 2 solutions for every $v \in \mathbb{F}_{2^n}^*$ if and only if, denoting

$$\Delta_a(x) = a\left(x^{2^{ik}} + x^{2^{tk+s}}\right) + x^{2^s} + x,$$

the equation $\Delta_a(x) = 0$ has at most two zeros or, equivalently, that the only solutions are $x = 0$ and $x = 1$.

From now on we consider the cases $i = 1$ and $i = 2$ separately.

Case 1 $(t = 1, i = 2)$ The following step can be seen as a very basic application of the multivariate method introduced by Dobbertin [19]. If we denote $y = x^{2^k}$, $z = y^{2^k}$ and $b = a^{2^k}$, $c = b^{2^k}$ the equation $\Delta_a(x) = 0$ can be rewritten as

$$a(z + y^{2^s}) + (x^{2^s} + x) = 0.$$

By definition, a is always a $(2^k - 1)$-th power and thus $abc = 1$. Besides, $a \notin \mathbb{F}_2$ (as it is confirmed further). Considering also the conjugated equations we derive the following system of equations

$$\begin{aligned}
f_1 = \;& a(z + y^{2^s}) + x^{2^s} + x = & 0 \\
f_2 = \;& b(x + z^{2^s}) + y^{2^s} + y = & 0 \\
f_3 = \;& \tfrac{1}{ab}(y + x^{2^s}) + z^{2^s} + z = & 0.
\end{aligned}$$

The aim now is eliminating y and z from these equations and finally getting an equation in x only. First we compute

$$\begin{aligned} R_1 &= b(f_1)^{2^s} + a^{2^s} f_2 \\ &= a^{2^s} b y^{2^{2s}} + a^{2^s} y^{2^s} + a^{2^s} y + b x^{2^{2s}} + b x^{2^s} + a^{2^s} b x \end{aligned}$$

and

$$\begin{aligned} R_2 &= \frac{1}{a(b+1)} \left(b f_1 + a f_2 + a b f_3\right) \\ &= y^{2^s} + \frac{a+1}{ab+a} y + \frac{1}{a} x^{2^s} + \frac{ab+b}{ab+a} x \end{aligned}$$

to eliminate z. To eliminate $y^{2^{2s}}$ we compute

$$\begin{aligned} R_3 &= R_1 + a^{2^s} b (R_2)^{2^s} = \frac{a^{2^s}(b+1)^{2^s} + (a+1)^{2^s} b}{(b+1)^{2^s}} y^{2^s} \\ &+ a^{2^s} y + \frac{a^{2^s} b^{2^s+1} + b}{b^{2^s}+1} x^{2^s} + a^{2^s} b x. \end{aligned}$$

Using equations R_2 and R_3 we can eliminate y^{2^s} by computing

$$\begin{aligned} R_4 &= R_3 + \frac{a^{2^s}(b+1)^{2^s} + (a+1)^{2^s} b}{(b+1)^{2^s}} R_2 \\ &= P(a)(y + (b+1)x^{2^s} + bx), \end{aligned}$$

where

$$P(a) = \frac{(ab)^{2^s+1} + (ab)^{2^s} + a^{2^s} b + a^{2^s} + ab + b}{(b+1)^{2^s+1} a}.$$

Computing

$$\begin{aligned} R_5 &= (R_4)^{2^s} + P(a)^{2^s} R_2 = P(a)^{2^s} \\ &\times \left(\frac{a+1}{ab+a} y + (b^{2^s}+1) x^{2^{2s}} + \frac{ab^{2^s}+1}{a} x^{2^s} + \frac{ab+b}{ab+a} x\right) \end{aligned}$$

we finally get our desired equation by

$$\begin{aligned} R_6 &= \frac{a+1}{ab+a} P(a)^{2^s-1} R_4 + R_5 \\ &= P(a)^{2^s} (b+1) \left(x^{2^{2s}} + x^{2^s}\right). \end{aligned}$$

Obviously if x is a solution of $\Delta_a(x) = 0$ then $R_6(x) = 0$. For $P(a)^{2^s}(b+1) \neq 0$ this is equivalent to $x = 0, 1$. Thus to prove the theorem one possibility is to show that $P(a)$ does not vanish for elements a fulfilling the equation

$$a = \left(\alpha v^{2^k+2^s+1}\right)^{2^k-1} \tag{1}$$

Note that, if a satisfies (1), then a is not a $(2^k + 2^s + 1)$-th power. Indeed, $g_2 = \gcd(2^k - 1, 2^k + 2^s + 1)$ is always a divisor of $g_1 = \gcd(2^n - 1, 2^k + 2^s + 1)$. And if a fulfilling (1) is a $(2^k + 2^s + 1)$-th power then α^{2^k-1} is a g_1-th power and then α is a (g_1/g_2)-th power. But as (g_1/g_2) is a nontrivial divisor of $2^n - 1$ this contradicts that α is a primitive element.

Consequently we want to show, that if $P(a) = 0$ then a is a $(2^k + 2^s + 1)$-th power. But for $a \notin \mathbb{F}_2$ the equation $P(a) = 0$ is equivalent to

$$a = \left(\frac{a+1}{c+1}\right)^{2^s+1} c^{2^s+1} \left(\frac{b+1}{a+1}\right) a,$$

as can be easily seen by dividing this equality by a, simplifying it by $(a + 1)$, and then expanding it, using that $c = 1/ab$. Note that the right hand side is always a $(2^k + 2^s + 1)$-th power. This proves the first case.

Case 2 $(t = 2, i = 1)$ In this case the equation $\Delta_a(x) = 0$ can be transformed into the following system of equations

$$\begin{aligned} a(y + z^{2^s}) + (x + x^{2^s}) &= 0 \\ b(z + x^{2^s}) + (y + y^{2^s}) &= 0 \\ \frac{1}{ab}(x + y^{2^s}) + (z + z^{2^s}) &= 0. \end{aligned}$$

Again eliminating y and z similarly as before we get this time

$$P(a)^{2^s} \left(x^{2^{2s}} + x^{2^s}\right) = 0,$$

with

$$P(a) = (ab)^{2^s+1} + (ab)^{2^s} + ab^{2^s} + ab + a + b^{2^s}.$$

Using similar arguments as before it suffices in this case to show that if $P(a) = 0$ then a is a $(2^{k+s} + 2^s + 1)$-th power. For this, note that for $a \notin \mathbb{F}_2$ the equation $P(a) = 0$ is equivalent to

$$a^{2^s} = \left(\frac{a+1}{c+1}\right)^{2^s+1} c^{2^s+1} \left(\frac{b+1}{a+1}\right)^{2^s} a^{2^s}$$

and the right hand side is always a $(2^{k+s} + 2^s + 1)$-th power. □

Remark: Note that in Theorem 1 instead of a coefficient α^{2^k-1} we can take any element of order $4^k + 2^k + 1$.

From Theorem 1 we get the following corollary as a special case.

Corollary 1 *Let s and k be positive integers such that* $\gcd(k, 3) = \gcd(s, 3k) = 1$*, and* $i = sk \mod 3$*,* $t = 2i \mod 3$*,* $n = 3k$*, and α be a primitive element of* $\mathbb{F}_{2^n}^*$*. Then the function*

$$F(x) = x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{tk+s}}$$

is APN on $\mathbb{F}_{2^n}$ (and is AB when n is odd).

Proof. We only have to verify that in this case the greatest common divisors

$$g_1 = \gcd(2^n - 1, 2^{k+s} + 2^s + 1 - 2^k(2^s - 1)(i - 1))$$

$$g_2 = \gcd(2^k - 1, 2^{k+s} + 2^s + 1 - 2^k(2^s - 1)(i - 1))$$

are not the same. Obviously g_2 is always coprime with 7 and it can be easily checked that g_1 is always divisible by 7. Indeed, for instance, if $k \mod 3 = s \mod 3 = 1$ then $i = 1$ and $k = 3k' + 1, s = 3s' + 1$ for some k', s', and we get

$$g_1 = 2^{k+s} + 2^s + 1 = 4(2^{3(k'+s')} - 1) + 2(2^{3s'} - 1) + 7.$$

□

It should be noted that Theorem 1 covers a larger class of APN functions as can be seen by checking the conditions on the greatest common divisors for small values of k and s.

The next proposition shows that the functions from Corollary 1 are permutations if k is odd. Moreover computer investigations show that most probably, if k is odd their inverses have the algebraic degree $(3k + 1)/2$.

Proposition 1 *The APN functions of Corollary 1 are bijective if and only if k is odd.*

Sketch of proof. If k is even then, since $\gcd(s, 3k) = 1$, s must be odd and therefore $2^s + 1$ is divisible by 3 as well as $2^{ik} + 2^{tk+s} = 2^{ik}(1 + 2^{(t-i)k+s})$. We have $F(x) = F(\gamma x)$ for every $\gamma \in \mathbb{F}_4^*$.

To prove that F is bijective when k is odd, we use the same steps as in the proof of Theorem 1. Assume $i = 1$ (the proof for the case $i = 2$ is similar). We have to show that the equation $F(x) + F(x + v) = 0$ does not have a non zero solution v for any x. Doing the same computations as in the proof of Theorem 1 we have this time to look at the following system of equations

$$\begin{array}{rrl} f_1 = & a(z + y^{2^s} + 1) + x^{2^s} + x + 1 = & 0 \\ f_2 = & b(x + z^{2^s} + 1) + y^{2^s} + y + 1 = & 0 \\ f_3 = & \frac{1}{ab}(y + x^{2^s} + 1) + z^{2^s} + z + 1 = & 0. \end{array}$$

Now, doing the same elimination of y and z as before, we end up with

$$P(a)^{2^s}(x^{2^s} + x + 1) = 0,$$

where P is as in the proof of Theorem 1. By taking the power 2^s of $x^{2^s} + x + 1 = 0$ and substituting $x^{2^s} = x + 1$ we get $x^{2^{2s}} = x$ which is equivalent to $x \in F_{2^j}$ where $j = \gcd(2s, 3k)$. If k is odd then $j = 1$ and the only possible solutions could be 0 or 1 but they obviously do not satisfy $x^{2^s} + x + 1 = 0$. □

4 On the CCZ-inequivalence between the introduced APN functions and the Gold and the Kasami functions

We first prove the EA-inequivalence between the APN functions introduced in Corollary 1 and all power functions.

Theorem 2 *Let n be a positive integer and let s, j, q be three nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that $q \neq \pm s$. If one of the following conditions holds*

1. $j \neq \pm s, \pm q, 2s, s \pm q,$
2. $j \neq \pm s, \pm q, \pm s - q, -2q,$
3. $j \neq s, -q, 2s - q, s - 2q, s \pm q, 2s,$
4. $j \neq s, -q, 2s - q, s - 2q, \pm s - q, -2q,$

then the function $F(x) = x^{2^s+1} + ax^{2^j(2^q+1)}$ with $a \in \mathbb{F}_{2^n}^*$ is EA-inequivalent to power functions on $\mathbb{F}_{2^n}$.

Proof. Suppose the function F is EA-equivalent to a power function. Since F is quadratic and EA-transformation does not change the algebraic degree of a function then F is EA-equivalent to x^{2^r+1} for some nonzero $r \in \mathbb{Z}/n\mathbb{Z}$. Therefore, there exist affine permutations L_1, L_2 and an affine function L' such that

$$L_1(x^{2^s+1}) + L_1(ax^{2^j(2^q+1)}) = (L_2(x))^{2^r+1} + L'(x).$$

Expressing $L_1(x)$, $L_2(x)$ and $L'(x)$ as sums of linearized polynomials and constants and reducing the resulting exponents modulo $2^n - 1$ leads to an equation whose degree is at most $2^{n-1} + 2^{n-2}$ (since the 2-weights of the exponents are at most 2) and which has 2^n solutions. Hence the equation must be an identity.

Since the functions are quadratic, we can assume without loss of generality that L_1 and L_2 are linear:

$$\begin{aligned} L_1(x) &= \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m x^{2^m}, \\ L_2(x) &= \sum_{p \in \mathbb{Z}/n\mathbb{Z}} c_p x^{2^p}. \end{aligned}$$

Then we get

$$\begin{aligned} &\sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m x^{2^m(2^s+1)} + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m a^{2^m} x^{2^{m+j}(2^q+1)} \\ &= \sum_{l,p \in \mathbb{Z}/n\mathbb{Z}} c_p c_l^{2^r} x^{2^{l+r}+2^p} + L'(x). \end{aligned} \tag{2}$$

On the left hand side of the identity (2) we have only items of the type $x^{2^m(2^s+1)}$, $x^{2^{m+j}(2^q+1)}$, with some coefficients. Therefore this must be true also for the right hand side of the identity.

We shall show that under some conditions on s, j, q, the equality above is satisfied only if $b_m = 0$ for every $m \in \mathbb{Z}/n\mathbb{Z}$. A contradiction.

If $b_m \neq 0$ for some m, then the coefficients of the items $x^{2^m(2^s+1)}$ and $x^{2^{m+j}(2^q+1)}$ are not zero on the left hand side of the identity (2) since $q \neq \pm s$. Hence this is also true for the right hand side of (2), that is,

$$c_m c_{m+s-r}^{2^r} \neq c_{m+s} c_{m-r}^{2^r}, \tag{3}$$

$$c_{m+j} c_{m+j+q-r}^{2^r} \neq c_{m+j+q} c_{m+j-r}^{2^r}. \tag{4}$$

The items of the type $x^{2^m+2^{m+j}}$ are missing in the left hand side of (2) when $j \neq \pm s, \pm q$. And we have no item of the kind $x^{2^{m+j}+2^{m+s}}$ in the left hand side of (2) when $j-s \neq \pm s, \pm q$, that is, $j \neq 2s, s \pm q$.

Thus, if these conditions are satisfied, then from the right hand side of (2) we get the following equalities with $c_m, c_{m+s-r}^{2^r}, c_{m+s}, c_{m-r}^{2^r}, c_{m+j}, c_{m+j-r}^{2^r}$:

$$c_m c_{m+j-r}^{2^r} = c_{m+j} c_{m-r}^{2^r}, \tag{5}$$

$$c_{m+j} c_{m+s-r}^{2^r} = c_{m+s} c_{m+j-r}^{2^r}. \tag{6}$$

Assume $c_{m+j-r}, c_{m+s-r} \neq 0$. If $c_{m-r} \neq 0$ then we get from (3), (5), (6):

$$c_m c_{m-r}^{-2^r} \neq c_{m+s} c_{m+s-r}^{-2^r},$$

$$c_m c_{m-r}^{-2^r} = c_{m+j} c_{m+j-r}^{-2^r},$$

$$c_{m+j} c_{m+j-r}^{-2^r} = c_{m+s} c_{m+s-r}^{-2^r},$$

and we come to a contradiction. If $c_{m-r} = 0$ then from (5) and since $c_{m+j-r} \neq 0$ we get $c_m = 0$. But $c_{m-r} = c_m = 0$ contradicts (3). Therefore, either c_{m+j-r} or c_{m+s-r} equals 0.

Assume first that $c_{m+j-r} = 0$. Then from (4) we get $c_{m+j} \neq 0$; then from (5), (6) we get $c_{m+s-r} = c_{m-r} = 0$, that is in contradiction with (3). Therefore, $c_{m+j-r} \neq 0$.

Assume now that $c_{m+s-r} = 0$. Then from (3) we get $c_{m+s} \neq 0$; then from (6) we get $c_{m+j-r} = 0$. Then from (4) we get $c_{m+j} \neq 0$ and we arrive to the contradiction $c_{m+s-r} = c_{m-r} = 0$ as above.

Therefore, if $j \neq \pm s, \pm q, 2s, s \pm q$ then F is EA-inequivalent to quadratic power functions.

Using similar arguments we get below other conditions on s, q, j which are also sufficient.

We have no item of the kind $x^{2^{m+j+q}+2^m}$ in the left hand side of (2) when $j+q \neq \pm s, \pm q$, that is, $j \neq \pm s - q, -2q$. Thus, if $j \neq \pm s, \pm q, \pm s - q, -2q$ then we have the equality (5) and from (2) we get the following equality

$$c_m c_{m+j+q-r}^{2^r} = c_{m+j+q} c_{m-r}^{2^r}. \tag{7}$$

Let $c_{m+j+q-r}, c_{m+j-r} \neq 0$. If also $c_{m-1} \neq 0$ then we get from (4), (5), (7)

$$c_{m+j}c_{m+j-r}^{-2^r} \neq c_{m+j+q}c_{m+j+q-r}^{-2^r},$$

$$c_m c_{m-r}^{-2^r} = c_{m+j}c_{m+j-r}^{-2^r},$$

$$c_m c_{m-r}^{-2^r} = c_{m+j+q}c_{m+j+q-r}^{-2^r},$$

and we come to a contradiction. If $c_{m-r} = 0$ then it follows from (5) that $c_m = 0$. But $c_m = c_{m-r} = 0$ contradicts (3). Therefore, either $c_{m+j+q-r} = 0$ or $c_{m+j-r} = 0$.

If $c_{m+j-r} = 0$ then $c_{m+j}, c_{m+j+q-r} \neq 0$ by (4). Since $c_{m+j-r} = 0$ and $c_{m+j} \neq 0$ then it follows from (5) that $c_{m-r} = 0$. Since $c_{m+j+q-r} \neq 0$ and $c_{m-r} = 0$ then $c_m = 0$ by (7). But $c_{m-r} = c_m = 0$ contradicts (3).

If $c_{m+j+q-r} = 0$ then from (4) we get $c_{m+j+q}, c_{m+j-r} \neq 0$. Since $c_{m+j+q-r} = 0$ and $c_{m+j+q} \neq 0$ then $c_{m-r} = 0$ from (7). We have $c_m = 0$ from (5) since $c_{m+j-r} \neq 0$ and $c_{m-r} = 0$. But $c_m = c_{m-r} = 0$ contradicts (3).

Thus, if $j \neq \pm s, \pm q, \pm s - q, -2q$ then the function F is EA-inequivalent to power functions.

The proofs of the third and the fourth claim of the theorem are similar. We have the following equality if $j \neq 2s - q, s, -q, s - 2q$

$$c_{m+s}c_{m+j+q-r}^{2^r} = c_{m+j+q}c_{m+s-r}^{2^r}. \tag{8}$$

The equalities (6) and (8) lead to the condition $j \neq 2s - q, s, -q, s - 2q, s \pm q, 2s$ which is sufficient for F to be EA-inequivalent to power functions. The same is true when we consider the equalities (7) and (8) with the condition $j \neq 2s-q, s, -q, s-2q, \pm s-q, -2q$. □

Corollary 2 *Let s and k be positive integers such that $k \geq 4$, $s \leq 3k - 1$, $\gcd(k, 3) = \gcd(s, 3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. Then the function $F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$ with $a \in \mathbb{F}_{2^n}^*$ is EA-inequivalent to power functions on $\mathbb{F}_{2^n}$.*

Proof. The function F coresponds to the first case in the hypotheses of Theorem 2. Indeed, if $i = 1$ then

$$2^{ik} + 2^{tk+s} \mod (2^{3k} - 1) = 2^k + 2^{2k+s} \mod (2^{3k} - 1)$$

$$= \begin{cases} 2^k(2^{k+s} + 1) & \text{if } s < k \\ 2^{s-k}(2^{2k-s} + 1) & \text{if } k < s < 2k \\ 2^k(2^{s-2k} + 1) & \text{if } s > 2k \end{cases} .$$

If $0 < s < k$ then in terms of Theorem 2 we have $j = k$, $q = k + s$ and the condition $j \neq \pm s, \pm q, s \pm q, 2s$ is equivalent to $k \neq s, 3k - s, k + s, 2k - s, k + 2s, 2k, 2s$ which is satisfied since $k \geq 4$ and $\gcd(k, 3) = \gcd(s, 3k) = 1$.

If $k < s < 2k$ then $j = s - k$, $q = 2k - s$ and $s - k \neq s, 3k - s, 2k - s, k + s, 2k, 2s -$

$2k, 2s, 2s-3k$.
If $s > 2k$ then $j = k$, $q = s - 2k$ and $k \neq s, 3k-s, s-2k, 5k-s, 2s-2k, 2k, 2s-3k$.

Obviously, in all cases the condition $q \neq \pm s$ is satisfied. Hence, the function F is EA-inequivalent to power functions by Theorem 2.

For the case $i = 2$ the proof is similar. □

Corollary 3 *Let s and k be positive integers such that $k \geq 4$, $s \leq 3k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, and $i = sk \mod 3$, $t = 2i \mod 3$, $n = 3k$. If $a \in \mathbb{F}_{2^n}$ has the order $2^{2k}+2^k+1$ then the function*

$$F(x) = x^{2^s+1} + ax^{2^{ik}+2^{tk+s}}$$

is AB on $\mathbb{F}_{2^n}$ when n is odd and APN when n is even and it is EA-inequivalent to power mappings.

The next theorems show that in general the new APN functions introduced in the present paper are not CCZ-equivalent to the Gold functions nor to the Kasami functions.

Without loss of generality a Gold function $F(x) = x^{2^s+1}$ and a Kasami function $K(x) = x^{4^r-2^r+1}$ can be considered under conditions $1 \leq s < \frac{n}{2}$, $2 \leq r < \frac{n}{2}$, since this exhausts all different cases (under EA-equivalence).

Theorem 3 *Let n be a positive integer, let r, s, q be three nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ and j an element of $\mathbb{Z}/n\mathbb{Z}$. Let a be a nonzero element of $\mathbb{F}_{2^n}$. Assume that $s \neq \pm q$ and one of the following two conditions is satisfied*
1) $j \neq s-r$, $j \neq -r$, $j+q \neq s-r$, $j+q \neq -r$;
2) $j \neq s+r$, $j \neq r$, $j+q \neq s+r$, $j+q \neq r$.
If $F(x) = x^{2^s+1} + ax^{2^j(2^q+1)}$ is an APN function which is CCZ-equivalent to the function $G(x) = x^{2^r+1}$ then F and G are EA-equivalent.

Proof. Suppose that $F(x)$ and $G(x)$ are CCZ-equivalent, that is, there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $y = F(x) \Leftrightarrow L_2(x,y) = G(L_1(x,y))$. This implies then $L_1(x, F(x))$ is a permutation and $L_2(x, F(x)) = G(L_1(x, F(x)))$. Writing $L_1(x,y) = L(x) + L'(y)$ and $L_2(x,y) = L''(x) + L'''(y)$ gives

$$L''(x) + L'''(F(x)) = G[L(x) + L'(F(x))].$$

We can write

$$\begin{aligned} L(x) &= b + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m x^{2^m}, \\ L'(x) &= b' + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m}, \\ L''(x) &= b'' + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b''_m x^{2^m}, \end{aligned}$$

$$\begin{aligned} L'''(x) &= b''' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'''_m x^{2^m}, \\ b + b' &= c. \end{aligned}$$

We have

$$\begin{aligned}
& G[L(x) + L'(F(x))] \\
= \; & \Big(L(x) + L'(x^{2^s+1} + a x^{2^j(2^q+1)})\Big) \\
\times \; & \Big(L(x) + L'(x^{2^s+1} + a x^{2^j(2^q+1)})\Big)^{2^r} \\
= \; & (c + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m(2^s+1)} \\
+ \; & \sum_{m\in\mathbb{Z}/n\mathbb{Z}} a^m b'_m x^{2^{j+m}(2^q+1)}) \\
\times \; & (c^{2^r} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m^{2^r} x^{2^{m+r}} \\
+ \; & \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'^{2^r}_m x^{2^{m+r}(2^s+1)} \\
+ \; & \sum_{m\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b'^{2^r}_m x^{2^{r+j+m}(2^q+1)}) \\
= \; & Q(x) + [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^k} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b_m^{2^r} x^{2^{m+r}+2^k(2^s+1)} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'_k b_m^{2^r} x^{2^{m+r}+2^{j+k}(2^q+1)}] \\
+ \; & [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^k(2^s+1)} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k(2^s+1)} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^{j+k}(2^q+1)} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}+2^k} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^{j+k}(2^q+1)}],
\end{aligned}$$

where $Q(x)$ is a quadratic polynomial. Obviously, all terms in the expression above whose exponents have 2-weight strictly greater than 2 must cancel.

If L' is a constant then F and G are EA-equivalent and it proves the statement of the theorem. If the function L' is not a constant then there exists $m \in \mathbb{Z}/n\mathbb{Z}$ such that $b'_m \neq 0$.
If $j \neq s-r$, $j \neq -r$, $j+q \neq s-r$ and $j+q \neq -r$ then $2^{r+j+m}(2^q+1)+2^m(2^s+1)$ has 2-weight 4 and the items with this exponent have to vanish. We get $a^{2^{m+r}} b'^{2^r+1}_m + a^{2^{m+r}} b'_{m+r} b'^{2^r}_{m-r} = 0$ and since $a, b'_m \neq 0$ then $b'_{m+r}, b'_{m-r} \neq 0$ and $b'_m b'^{-2^r}_{m-r} = b'_{m+r} b'^{-2^r}_m$.
If $j \neq s+r$, $j \neq r$, $j+q \neq s+r$ and $j+q \neq r$ then $2^{m+j}(2^q+1)+2^{m+r}(2^s+1)$ has 2-weight 4 and we again get $b'_m b'^{-2^r}_{m-r} = b'_{m+r} b'^{-2^r}_m$.

Since $\gcd(r,n)=1$ for APN functions x^{2^r+1} then applying this observation for $m+r$, $m+2r$,..., instead of m we get $b'_t \neq 0$ and

$$b'_m b'^{-2^r}_{m-r} = b'_{t+r} b'^{-2^r}_t \tag{9}$$

for all $t \in \mathbb{Z}/n\mathbb{Z}$.

Let us consider the sum

$$\sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b'_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^k(2^s+1)}$$

from the last bracket. For any $k, m \in \mathbb{Z}/n\mathbb{Z}$, $k \neq m+r$, the items $b'_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^k(2^s+1)}$ and $b'_{m+r} b'^{2^r}_{k-r} x^{2^k(2^s+1)+2^{m+r}(2^s+1)}$ differ and cancel pairwise because of (9). In the case $k = m+r$ the sum gives items with the exponents of 2-weight not greater than 2.
Considering the sum

$$\sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}+2^k} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^{j+k}(2^q+1)}$$

we get that for any $k, m \in \mathbb{Z}/n\mathbb{Z}$, $k \neq m+r$, the items $a^{2^{r+m}+2^k} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^{j+k}(2^q+1)}$ and $a^{2^{r+m}+2^k} b'_{r+m} b'^{2^r}_{k-r} x^{2^{j+k}(2^q+1)+2^{r+j+m}(2^q+1)}$ differ and cancel pairwise because of (9) and in the case $k = m+r$ the sum gives items with the exponents of 2-weight not greater than 2.
Now we consider the sums

$$\sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k(2^s+1)}$$

and

$$\sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} a^{2^k} b'_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^{j+k}(2^q+1)}.$$

For any $k, m \in \mathbb{Z}/n\mathbb{Z}$ the item $a^{2^{r+m}} b'_k b'^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k(2^s+1)}$ from the first sum cancels with the item $a^{2^{r+m}} b'_{m+r} b'^{2^r}_{k-r} x^{2^k(2^s+1)+2^{r+j+m}(2^q+1)}$ from the second sum and vice versa.

Thus the expression in the last bracket is quadratic and

$$\begin{aligned}
& G[L(x)+L'(F(x))] \\
= \; & Q'(x)+[\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_k b_m'^{2^r} x^{2^{m+r}(2^s+1)+2^k} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b_k b_m'^{2^r} x^{2^{r+j+m}(2^q+1)+2^k} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_k' b_m^{2^r} x^{2^{m+r}+2^k(2^s+1)} \\
+ \; & \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b_k' b_m^{2^r} x^{2^{m+r}+2^{j+k}(2^q+1)}],
\end{aligned}$$

where $Q'(x)$ is a quadratic function.

Because of (9) we can deduce, by denoting $b_r' b_0'^{-2^r} = \lambda$, that $b_{t+r}' = \lambda b_t'^{2^r}$ for all t. Then, introducing μ such that $\lambda = \mu^{2^r-1}$, we deduce that $\mu b_{t+r}' = (\mu b_t')^{2^r}$ for all t and then that $\mu b_{t+1}' = (\mu b_t')^2$ (using that $\gcd(r,n)=1$) and then $\mu b_t' = (\mu b_0')^{2^t}$. This means that $\mu L'(x) = \mu b' + tr(\mu b'_0 x)$. Then obviously L' is not a permutation and since $L_1(x, F(x))$ is a permutation then L is not a constant. Thus $b_t \neq 0$ for some $t \in \mathbb{Z}/n\mathbb{Z}$.
We have $s \neq \pm q$ and if also $r \neq \pm q$, $r+s \neq \pm q$ then we have the items with the exponent $2^{m+r+s} + 2^{m+r} + 2^m$ only in the first and the third sums in the bracket (if the condition $r \neq \pm q$, $r+s \neq \pm q$ is wrong then the claim is true for the exponent $2^{m+r+s} + 2^{m+r} + 2^{m-1}$). We get $b_m b_m'^{2^r} + b_{m+r}' b_{m-r}^{2^r} = 0$. Since $b_m, b_m' \neq 0$ then $b_{m-r} \neq 0$ and $b_m b_{m-r}^{-2^r} = b_{m+r}' b_m'^{-2^r}$. Repeating these steps for $b_{m-r}, b_{m-2r}, \ldots$, because of (9) we get $b_t \neq 0$ for all $t \in \mathbb{Z}/n\mathbb{Z}$ and

$$\lambda = b_m' b_{m-r}'^{-2^r} = b_t b_{t-r}^{-2^r}.$$

Therefore, $\mu L(x) = \mu b + tr(\mu b_0 x)$ and $\mu[L(x) + L'(F(x))] = \mu b' + \mu b + tr(\mu b_0 x + \mu b'_0 F(x))$. Obviously the function $L(x) + L'(F(x))$ is not a permutation and that is a contradiction. Therefore, L' is constant and F and G are EA-equivalent. □

Corollary 4 *The functions from Corollary 3 are CCZ-inequivalent to the Gold mappings.*

Proof. Assume that the Gold function x^{2^r+1}, $\gcd(r,n)=1$, is CCZ-equivalent to F. Then by Corollary 3 and by Theorem 3 one of the conditions $s \neq \pm q$, $j \neq s-r$, $j \neq -r$, $j+q \neq s-r$, $j+q \neq -r$, is not satisfied.

Let consider the case $i=1$. Then in terms of Theorem 3 we have $q = k+s, j = k$. If $s = \pm q$ then we get a contradiction with $k \neq 0$ or $\gcd(s,k)=1$. If $r = -j$ or $r = s-(j+q)$ then $\gcd(r,k) \neq 1$, a contradiction. If $r = s-j$ or $r = -(j+q)$ then r is divisible by 3. Indeed, since $sk = 1 \mod 3$ then $s \mod 3 = k \mod 3$ and $\pm(s-k) = 0 \mod 3$. On the other hand, $r = s-j = s-k$ or $r = -(j+q) = n-(2k+s) = 3k-(2k+s) = k-s$. But $\gcd(r,3k)=1$, a contradiction.
The proof for the case $i=2$ is similar. □

Theorem 4 *Let n be a positive integer, let r, s, q, j be nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that* $\gcd(r,n) = 1$, $n > 4$, $s \neq \pm q$, $s \neq \pm 3q$, $q \neq \pm 3s$, $s \neq \pm j$, $q \neq \pm j$, $3q + j \neq 0$, $j + q \neq \pm s$, $j \neq s + q$, $2q \neq \pm j$, $2q \neq s - j$, $2s \neq j$, $2s \neq j + q$. *Then for $a \in \mathbb{F}_{2^n}^*$ the functions* $F(x) = x^{2^s+1} + ax^{2^j(2^q+1)}$ *and* $K(x) = x^{4^r - 2^r + 1}$ *are CCZ-inequivalent.*

Proof. Let $G(x) = x^{2^r+1}$, $G'(x) = x^{2^{3r}+1}$. Suppose that $F(x)$ and $K(x)$ are CCZ-equivalent. Then, there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L_2(x, F(x)) = K(L_1(x, F(x)))$, which implies, by composition by G

$$G(L_2(x, F(x))) = G'(L_1(x, F(x))),$$

that is, writing again $L_1(x,y) = L(x) + L'(y)$ and $L_2(x,y) = L''(x) + L'''(y)$:

$$\begin{aligned}
0 &= G'[L(x) + L'(F(x))] + G[L''(x) + L'''(F(x))] \\
&= Q(x) + [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_k b'^{2^{3r}}_m x^{2^{m+3r}(2^s+1)+2^k} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{3r+m}} b_k b'^{2^{3r}}_m x^{2^{3r+j+m}(2^q+1)+2^k} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b^{2^{3r}}_m x^{2^{m+3r}+2^k(2^s+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'_k b^{2^{3r}}_m x^{2^{m+3r}+2^{j+k}(2^q+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b''_k b'''^{2^r}_m x^{2^{m+r}(2^s+1)+2^k} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b''_k b'''^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'''_k b''^{2^r}_m x^{2^{m+r}+2^k(2^s+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'''_k b''^{2^r}_m x^{2^{m+r}+2^{j+k}(2^q+1)}] \\
&+ [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b'^{2^{3r}}_m x^{2^{m+3r}(2^s+1)+2^k(2^s+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{3r+m}} b'_k b'^{2^{3r}}_m x^{2^{3r+j+m}(2^q+1)+2^k(2^s+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'_k b'^{2^{3r}}_m x^{2^{m+3r}(2^s+1)+2^{j+k}(2^q+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{3r+m}+2^k} b'_k b'^{2^{3r}}_m x^{2^{3r+j+m}(2^q+1)+2^{j+k}(2^q+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'''_k b'''^{2^r}_m x^{2^{m+r}(2^s+1)+2^k(2^s+1)}
\end{aligned}$$

$$+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}} b'''_k b'''^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^k(2^s+1)}$$
$$+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^k} b'''_k b'''^{2^r}_m x^{2^{m+r}(2^s+1)+2^{j+k}(2^q+1)}$$
$$+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} a^{2^{r+m}+2^k} b'''_k b'''^{2^r}_m x^{2^{r+j+m}(2^q+1)+2^{j+k}(2^q+1)}],$$

where Q is quadratic.

Let $s \neq \pm q$, $s \neq \pm 3q$, $q \neq \pm 3s$. The exponents of the type $2^{3r+j+m+q}+2^{3r+j+m}+2^{k+s}+2^k$ have 2-weight 4 if $k \notin \{3r+j+m, 3r+j+m+q, 3r+j+m+q-s, 3r+j+m-s\}$ and these exponents cannot be equal to any exponent of the type $(2^s+1)(2^l+2^{l'})$ or $(2^q+1)(2^l+2^{l'})$. Since all terms with exponents of 2-weight 4 should vanish we obtain

$$b'_k b'^{2^{3r}}_m + b'_{m+3r} b'^{2^{3r}}_{k-3r} = b'''_k b'''^{2^r}_{m+2r} + b'''_{m+3r} b'''^{2^r}_{k-r} \tag{10}$$

for $m, k \in \mathbb{Z}/n\mathbb{Z}$, $k \notin \{3r+j+m, 3r+j+m+q, 3r+j+m+q-s, 3r+j+m-s\}$.

The equality (10) is also true for the cases $k \in \{3r+j+m, 3r+j+m+q, 3r+j+m+q-s, 3r+j+m-s\}$ if $s \neq \pm j$, $q \neq \pm j$, $3q+j \neq 0$, $j+q \neq \pm s$, $j \neq s+q$, $2q \neq \pm j$, $2q \neq s-j$, $2s \neq j$, $2s \neq j+q$. Indeed, consider the items with the exponents $2^{3r+j+m}(2^q+1)+2^{j+k}(2^q+1)$ for $k \in \{3r+j+m, 3r+j+m+q\}$. With the above written conditions these exponents have 2-weight 4 and they differ from exponents of the type $(2^s+1)(2^l+2^{l'})$ and $2^l(2^q+1)+2^{l'}(2^s+1)$. For $k \in \{3r+j+m+q-s, 3r+j+m-s\}$ we can consider $2^{m+3r}(2^s+1)+2^k(2^s+1)$.

Without loss of generality we can assume that L, L', L'', L''' are linear (since changing the constant terms in these affine mappings results only in a change of the polynomial $Q(x)$ above) and let $L' \neq 0$. The equalities (10) imply

$$(L'''(x))^{2^r+1} + (L'(x))^{2^{3r}+1} = C(x) \tag{11}$$

for some linear function $C(x)$. Besides, it must hold that

$$\ker(L''') \cap \ker(L') = \{0\} \tag{12}$$

since otherwise the system of equations

$$\begin{aligned} L(x) + L'(y) &= 0 \\ L''(x) + L'''(y) &= 0 \end{aligned}$$

has solutions different from $(0,0)$ which is not allowed for CCZ-equivalence.

For any a, derivating equality (11) we get

$$L'''(a)^{2^r} L'''(x) + L'''(a) L'''(x)^{2^r}$$

$$+L'(a)^{2^{3r}} L'(x) + L'(a) L'(x)^{2^{3r}} = 0 \tag{13}$$

We want to show first that L' and L''' have to be bijective. Assume on the contrary that L' is not bijective. Then there exists an element $a_0 \neq 0$ such that $L'(a_0) = 0$, and due to equality (12) $L'''(a_0) \neq 0$. We get for all x that

$$L'''(a_0)^{2^r} L'''(x) + L'''(a_0) L'''(x)^{2^r} = 0.$$

And it follows that

$$L'''(x) = 0 \text{ or } L'''(x) = L'''(a_0),$$

where we used that $\gcd(2^r - 1, 2^n - 1) = 1$. Thus there exists an element d such that

$$L'''(x) = L'''(a_0)\, \mathrm{tr}(dx).$$

If we plug this into equality (13) we get

$$L'(a)^{2^{3r}} L'(x) + L'(a) L'(x)^{2^{3r}} = 0$$

for all x and any a. This implies that $L'(x) = 0$ or

$$L'(x)^{2^{3r}-1} = L'(a)^{2^{3r}-1}$$

which, as $\gcd(3r, n) = 3$, means that

$$L'(x) = L'(a)\gamma$$

where $\gamma \in \mathbb{F}_{2^3}$. In particular we have

$$\dim(\mathrm{im}(L')) \leq 3$$

and therefore we have $\dim(\ker(L') \geq n - 3$. As $\dim(\ker(L''')) = n - 1$ for $n > 4$ the two kernel intersect, a contradiction.

Now assume that L''' is not bijective. Then there exists a_1 such that $L'''(a_1) = 0$ and $L'(a_1) \neq 0$. We get, again

$$L'(a_1)^{2^{3r}} L'(x) + L'(a_1) L'(x)^{2^{3r}} = 0$$

which, using the same arguments as above, contradicts the condition that L' is bijective. We conclude that L''' is bijective.

Now we denote $A = L''' \circ L'^{-1}$, which is again a bijective linear mapping. By replacing x by $L'^{-1}(x)$ in (13), we obtain

$$A(a)^{2^r} A(x) + A(a) A(x)^{2^r} + a^{2^{3r}} x + a x^{2^{3r}} = 0$$

and for $a \in \mathbb{F}_{2^3}^*$ we see that for all $x \in \mathbb{F}_{2^3}$ we get

$$A(a)^{2^r} A(x) + A(a) A(x)^{2^r} = 0$$

which is equivalent to $A(x) = 0$ or $A(x) = A(a)$ which is impossible since A is a bijection. Thus, this contradiction shows that the functions F and K are CCZ-inequivalent. □

Corollary 5 *The functions from Corollary 3 are CCZ-inequivalent to the Kasami mappings.*

Proof. It can be easily checked that the function F from Corollary 3 satisfies all conditions of Theorem 4. □

Conjecture 1 *The function from Corollary 3 is CCZ-inequivalent to any power function.*

5 CCZ-inequivalence of the Gold mappings with other known APN power functions

It is an open question whether Gold, Kasami, Welch and Niho functions are pairwise CCZ-inequivalent. Below we solve this problem for some cases. We prove that two Gold functions are CCZ-equivalent if and only if they are EA-equivalent, and that the Gold functions are CCZ-inequivalent to any Kasami and to the Welch functions (except in particular cases). Note that the inverse and Dobbertin APN functions are CCZ-inequivalent to all known APN mappings. It is obvious because of their unique nonlinearities [10, 27].

Proposition 2 (CCZ-ineq. of two Gold functions) *Let* $F(x) = x^{2^s+1}$, $G(x) = x^{2^r+1}$ *and* $s \neq r$, $1 \leq s, r < \frac{n}{2}$, $\gcd(s, n) = \gcd(r, n) = 1$. *Then* F *and* G *are CCZ-inequivalent on* $\mathbb{F}_{2^n}$.

Proof. Suppose that $F(x)$ and $G(x)$ are CCZ-equivalent, then there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L_2(x, F(x)) = G(L_1(x, F(x)))$. Writing $L_1(x, y) = L(x) + L'(y)$ and $L_2(x, y) = L''(x) + L'''(y)$ gives

$$L''(x) + L'''(F(x)) = G[L(x) + L'(F(x))].$$

We can write $L(x) = b + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m}$, $L'(x) = b' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m}$, $L''(x) = b'' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b''_m x^{2^m}$ and $L'''(x) = b''' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'''_m x^{2^m}$, $b + b' = c$.

We have

$$\begin{aligned}
& G[L(x) + L'(F(x))] \\
= \; & \left(L(x) + L'(x^{2^s+1})\right)\left(L(x) + L'(x^{2^s+1})\right)^{2^r} \\
= \; & \left(c + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m(2^s+1)}\right) \\
\times \; & \left(c^{2^r} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m^{2^r} x^{2^{m+r}} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'^{2^r}_m x^{2^{m+r}(2^s+1)}\right) \\
= \; & Q(x) + \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_k b'^{2^r}_m x^{2^{m+r}(2^s+1)+2^k}
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b_m^{2^r} x^{2^{m+r}+2^k(2^s+1)} \\
&+ \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b_m'^{2^r} x^{2^{m+r}(2^s+1)+2^k(2^s+1)},
\end{aligned}
$$

where $Q(x)$ is a quadratic polynomial. Obviously, all terms in the expression above whose exponents have 2-weight strictly greater than 2 must cancel.

Suppose $L' \neq$ const then there exists $m \in \mathbb{Z}/n\mathbb{Z}$ such that $b'_m \neq 0$. Considering s and r as elements of $\mathbb{Z}/n\mathbb{Z}$ we have $s \neq \pm r$ and $s, r \neq 0$. Then $2^{r+m}(2^s+1) + 2^m(2^s+1)$ has 2-weight 4 and the items with this exponent have to vanish. We get $b_m'^{2^r+1} + b'_{m+r} b_{m-r}'^{2^r} = 0$ and since $b'_m \neq 0$ then $b'_{m+r}, b'_{m-r} \neq 0$ and $b'_m b_{m-r}'^{-2^r} = b'_{m+r} b_m'^{-2^r}$. Since $\gcd(r,n) = 1$ then applying this observation for $m+r$, $m+2r$,..., instead of m we get $b'_t \neq 0$ and there exists a nonzero constant λ such that

$$
b'_{t+r} b_t'^{-2^r} = \lambda \tag{14}
$$

for all $t \in \mathbb{Z}/n\mathbb{Z}$.

Let us consider the sum

$$
\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_k b_m'^{2^r} x^{2^{m+r}(2^s+1)+2^k(2^s+1)}.
$$

For any $k, m \in \mathbb{Z}/n\mathbb{Z}$, $k \neq m+r$, the items $b'_k b_m'^{2^r} x^{2^{m+r}(2^s+1)+2^k(2^s+1)}$ and $b'_{m+r} b_{k-r}'^{2^r} x^{2^k(2^s+1)+2^{m+r}(2^s+1)}$ do not coincide and cancel pairwise because of (14). In the case $k = m+r$ the sum gives items with the exponents of 2-weight not greater than 2.

Because of (14) we can deduce $b'_{t+r} = \lambda b_t'^{2^r}$ for all t. Then, introducing μ such that $\lambda = \mu^{2^r-1}$, we deduce that $\mu b'_{t+r} = (\mu b'_t)^{2^r}$ for all t and then that $\mu b'_{t+1} = (\mu b'_t)^2$ (using that $\gcd(r,n) = 1$) and then $\mu b'_t = (\mu b'_0)^{2^t}$. This means that $\mu L'(x) = \mu b' + tr(\mu b'{}_0 x)$. Then obviously L' is not a permutation and since $L_1(x, F(x))$ is a permutation then L is not a constant. Thus $b_m \neq 0$ for some $m \in \mathbb{Z}/n\mathbb{Z}$.

Since $s \neq \pm r$ then considering the items with the exponent $2^{m+r+s} + 2^{m+r} + 2^m$ we get $b_m b_m'^{2^r} + b'_{m+r} b_{m-r}^{2^r} = 0$ if $r \neq -2s$ (for $r = -2s$ there are more than 2 items with this exponent because the difference between m and $m+r+s$ is the same like between $m+r+s$ and $m+r$). Since $b_m, b'_m \neq 0$ then $b_{m-r} \neq 0$ and $b_m b_{m-r}^{-2^r} = b'_{m+r} b_m'^{-2^r}$. Repeating these steps for $b_{m-r}, b_{m-2r}, \ldots$, because of (14) we get $b_t \neq 0$ for all $t \in \mathbb{Z}/n\mathbb{Z}$ and

$$
b_t b_{t-r}^{-2^r} = \lambda. \tag{15}
$$

For the case $r = -2s$ consider the items with the exponent $2^{m+r} + 2^{m+s} + 2^m$ and get $b'_m b_m^{2^r} + b_{m+r} b_{m-r}'^{2^r} = 0$ which again leads to (15).

The equality (15) implies, $\mu L(x) = \mu b + tr(\mu b_0 x)$ and $\mu[L(x) + L'(F(x))] = \mu b' + \mu b + tr(\mu b_0 x + \mu b'{}_0 F(x))$. Obviously the function $L(x) + L'(F(x))$ cannot be a permutation. Therefore, $L' =$ const and then $L \neq$ const. For some $m \in \mathbb{Z}/n\mathbb{Z}$ we have $b_m \neq 0$ and since $s \neq \pm r$ it is not difficult to note that $b_m^{2^r+1} + b_{m+r} b_{m-r}^{2^r} = 0$. Thus $b_{m+r}, b_{m-r} \neq 0$ and because of $\gcd(r,n) = 1$ we derive $b_t \neq 0$ and $\lambda' = b_m b_{m-r}^{-2^r} = b_t b_{t-r}^{-2^r}$ for all $t \in \mathbb{Z}/n\mathbb{Z}$.

This leads to the equality $\mu' L(x) = \mu' b + tr(\mu' b_0 x)$ with $\lambda' = \mu'^{2^r-1}$. Then L is not a permutation. This contradiction proves CCZ-inequivalence of F and G. $\square$

Theorem 5 (CCZ-ineq. of Gold and Kasami functions) *Let* $F(x) = x^{2^s+1}$, $K(x) = x^{4^r-2^r+1}$ *and* $\gcd(s,n) = \gcd(r,n) = 1$, $1 \le s < \frac{n}{2}$, $2 \le r < \frac{n}{2}$. *If* $3r \neq \pm 1 \mod n$ *then* F *and* K *are CCZ-inequivalent on* $\mathbb{F}_{2^n}$.

Proof. Let $G'(x) = x^{2^{3r}+1}$, $G(x) = x^{2^r+1}$ and let the functions K and F be CCZ-equivalent on $\mathbb{F}_{2^n}$. Then, there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L_2(x, K(x)) = F(L_1(x, K(x)))$, which implies $L_2(G(x), G'(x)) = F(L_1(G(x), G'(x)))$, that is, writing again $L_1(x,y) = L(x) + L'(y)$ and $L_2(x,y) = L''(x) + L'''(y)$:

$$L''(G(x)) + L'''(G'(x)) + F[L(G(x)) + L'(G'(x))] = 0.$$

With the same notation as in the proof of Proposition 2, we have:

$$\begin{aligned}
& L''(G(x)) + L'''(G'(x)) + F[L(G(x)) + L'(G'(x))] \\
= \; & Q(x) + [c + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m x^{2^m(2^r+1)} \\
+ \; & \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m(2^{3r}+1)}][c^{2^s} + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m^{2^s} x^{2^{m+s}(2^r+1)} \\
+ \; & \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b'^{2^s}_m x^{2^{m+s}(2^{3r}+1)}] \\
= \; & Q'(x) + \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b_m b_k^{2^s} x^{2^m(2^r+1)+2^{k+s}(2^r+1)} \\
+ \; & \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b_m b'^{2^s}_k x^{2^m(2^r+1)+2^{k+s}(2^{3r}+1)} \\
+ \; & \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b'_m b_k^{2^s} x^{2^m(2^{3r}+1)+2^{k+s}(2^r+1)} \\
+ \; & \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b'_m b'^{2^s}_k x^{2^m(2^{3r}+1)+2^{k+s}(2^{3r}+1)},
\end{aligned}$$

where Q and Q' are quadratic.

Suppose that L and L' are not constant. Then $b_m, b'_k \neq 0$ for some $m, k \in \mathbb{Z}/n\mathbb{Z}$.

We consider the items in the sum with the exponent $2^m(2^r+1) + 2^{k+s}(2^{3r}+1)$, which has the 2-weight at least 3 if $3r \neq \pm 1 \mod n$, and get the equality $b_m b'^{2^s}_k + b'_{k+s} b^{2^s}_{m-s} = 0$. Since $b_m, b'_k \neq 0$ then $b'_{k+s}, b_{m-s} \neq 0$ and

$$b_m b_{m-s}^{-2^s} = b'_{k+s} b'^{-2^s}_k.$$

Repeating this step for $k+s$, $k+2s$,..., instead of k and for $m-s$, $m-2s$,..., instead of m, because of $\gcd(s,n) = 1$ we get

$$\lambda = b_m b_{m-s}^{-2^s} = b'_{k+s} b'^{-2^s}_k \tag{16}$$

for all $m, k \in \mathbb{Z}/n\mathbb{Z}$.

Like in the proof of Proposition 2 from the equality (16) we get $\mu[L(x) + L'(K(x))] = \mu b' + \mu b + tr(\mu b_0 x + \mu b'_0 K(x))$, where $\lambda = \mu^{2^s-1}$. Thus $L_1(x, K(x))$ is not a permutation, a contradiction. Therefore, L or L' is constant and F is then EA-equivalent to K or to the inverse of K. We know that F and K are not EA-equivalent because of algebraic degree of K is $r+1$ while F is quadratic. Let consider the case $L =$ const and $L' \neq$ const. We have $b'_m \neq 0$ for some m and $2^m(2^{3r}+1) + 2^{m+s}(2^{3r}+1)$ has 2-weight at least 3 except the cases when $s = 1$ and $3r = \pm 1 \mod n$. With the same arguments as above we get that $L_1(x, K(x))$ is not a permutation. □

If n is odd and $s = 1$, $3r = \pm 1 \mod n$ then the inverse of the function K may be EA-equivalent to F in some cases. For instance, $K^{-1} = F^4$ for $s = 1$, $r = 2$, $n = 5$.

Theorem 6 (CCZ-ineq. of Gold and Welch mappings) *Let $F(x) = x^{2^s+1}$ and $G(x) = x^{2^t+3}$ with $\gcd(s, n) = 1$, $1 \le s \le \frac{n-1}{2}$, $t = \frac{n-1}{2} \ge 4$. Then F and G are CCZ-inequivalent on $\mathbb{F}_{2^n}$.*

Sketch of proof. If F and G are CCZ-equivalent then for some affine functions L, L', L'', L''' we have

$$L''(x) + L'''(G(x)) = F[L(x) + L'(G(x))],$$

where $L(x) + L'(G(x))$ is a permutation. With the same notation as in the proof of Proposition 2, we have:

$$\begin{aligned}
& L''(x) + L'''(G(x)) + F[L(x) + L'(G(x))] \\
= \;& Q(x) + \left(c + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m x^{2^m} + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m(2^t+3)}\right) \\
\times \;& \left(c^{2^s} + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b_m^{2^s} x^{2^{m+s}} + \sum_{m \in \mathbb{Z}/n\mathbb{Z}} b'^{2^s}_m x^{2^{m+s}(2^t+3)}\right) \\
= \;& Q'(x) + \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b_m b'^{2^s}_k x^{2^m + 2^{k+s}(2^t+3)} \\
+ \;& \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b'_m b_k^{2^s} x^{2^m(2^t+3) + 2^{k+s}} \\
& + \sum_{m,k \in \mathbb{Z}/n\mathbb{Z}} b'_m b'^{2^s}_k x^{2^m(2^t+3) + 2^{k+s}(2^t+3)}, \qquad (17)
\end{aligned}$$

where Q and Q' are cubic.
Since the algebraic degree of G is 3 for $n > 3$ then F and G are EA-inequivalent. Therefore, $L' \neq$ const and $b'_m \neq 0$ for some m.

Since $t \ge 4$ then $2^m(2^t+3) + 2^{m+s}(2^t+3)$ has 2-weight at least 5 when $s \neq 1, t$. If either $s = 1$ or $s = t$ then $2^m(2^t+3) + 2^{m+s}(2^t+3)$ has 2-weight at least 4 and it differs from the exponents of the items in the first and second sums in (17). The equality (17) implies $b'^{2^s+1}_m = b'_{m+s} b'^{2^s}_{m-s}$ and $b'_{m+s}, b'_{m-s} \neq 0$. Since $\gcd(n, s) = 1$ then we get $b'_m \neq 0$ and

$$\lambda = b'_{m+s} b'^{-2^s}_m = b'_m b'^{-2^s}_{m-s} \tag{18}$$

for any m.

For $m \neq k+s$ the items $b'_m b'^{2^s}_k x^{2^m(2^t+3)+2^{k+s}(2^t+3)}$ and $b'_{k+s} b'^{2^s}_{m-s} x^{2^m(2^t+3)+2^{k+s}(2^t+3)}$ differ and cancel pairwise because of (18). In the case $m = k+s$ the sum gives items with the exponents of 2-weight not greater than 3.

Because of (18) we get $\mu L'(x) = \mu b' + tr(\mu b'_0 x)$, where $\lambda = \mu^{2^s-1}$. Therefore, L' is not a permutation and then $L \neq$ const. We have $b_m \neq 0$ for some m and considering the items with the exponent $2^m + 2^{m+s}(2^t+3)$ of 2-weight 4 we get $b_m b'^{2^s}_m = b'_{m+s} b^{2^s}_{m-s}$ and $b_{m-s} \neq 0$. This leads to the equality $b_m b^{-2^s}_{m-s} = b'_{m+s} b'^{-2^s}_m = \lambda$ for any m. Finally we get $\mu[L(x) + L'(G(x))] = \mu b' + \mu b + tr(\mu b_0 x + \mu b'_0 G(x))$ which means that $L(x) + L'(G(x))$ is not a permutation. Thus F and G are CCZ-inequivalent.

It was checked with a computer that if $1 < t < 4$ then F is EA-equivalent to G^{-1} only in case $n = 5$, $s = 2$. □

6 Conclusion

We have introduced an infinite class of APN (and AB if n is odd) quadratic functions which we conjecture CCZ-inequivalent to power functions, and therefore, new, up to CCZ-equivalence. We showed that they are CCZ-inequivalent to Gold and Kasami functions. This implies that, for n even they are CCZ-inequivalent to any known APN function, and for $n = 12, 24$, they are indeed CCZ-inequivalent to power functions. We leave two open problems:
- proving that the functions introduced in the present paper are CCZ-inequivalent to power functions for every $n \geq 12$;
- finding classes of non-quadratic APN functions which would be CCZ-inequivalent to all known APN functions (or even, CCZ-inequivalent to power functions).

References

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions and distance-regular graphs. *Electron. J. Comb.*, 5(R34), 14, 1998.

[2] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear mappings over F_2^n. *Proceedings of International Symposium on Information Theory ISIT 2005.*

[3] T. Beth and C. Ding. On almost perfect nonlinear permutations. *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, 765, Springer-Verlag, New York, pp. 65-76, 1993.

[4] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.

[5] L. Budaghyan, C. Carlet, P. Felke, 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*, Seattle, USA, Jul. 2006.

[6] L. Budaghyan, C. Carlet, A. Pott. New Constructions of Almost Bent and Almost Perfect Nonlinear Functions. *Proceedings of the Workshop on Coding and Cryptography 2005*, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.

[7] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141- 1152, March 2006.

[8] A. Canteaut, P. Charpin and H. Dobbertin. A new characterization of almost bent functions. *Fast Software Encryption 99, Lecture Notes in Computer Science* 1636, L. Knudsen edt, pp. 186-200. Springer-Verlag, 1999.

[9] A. Canteaut, P. Charpin and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.

[10] A. Canteaut, P. Charpin, H. Dobbertin. Weight divisibility of cyclic codes , highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105-138, 2000.

[11] C. Carlet. Vectorial (multi-output) Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[12] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[13] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis, *Advances in Cryptology -EUROCRYPT'94, Lecture Notes in Computer Science*, Springer-Verlag, New York, 950, pp. 356-365, 1995.

[14] J. Daemen and V. Rijmen. AES proposal: Rijndael. http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.

[15] H. Dobbertin. One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. *Appl. Algebra Eng. Commun. Comput.* 9 (2), pp. 139-152, 1998.

[16] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case. *Inform. and Comput.*, 151, pp. 57-72, 1999.

[17] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45, pp. 1271-1275, 1999.

[18] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. D. Jungnickel and H. Niederreiter eds. *Proceedings of Finite Fields and Applications FQ5*, Augsburg, Germany, Springer, pp. 113-121, 2000.

[19] H. Dobbertin, Uniformly representable permutation polynomials, T. Helleseth, P.V. Kumar and K. Yang eds. *in the Proceedings of "Sequences and their applications–SETA '01"*, Springer Verlag, London, 2002, 1-22.

[20] H. Dobbertin. Private communication. 2004.

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

[22] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14, pp. 154-156, 1968.

[23] T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applic. Alg. Eng., Commun. Comput.*, vol. 8, pp. 363-370, 1997.

[24] H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and Their Applications 7*, pp. 253-286, 2001.

[25] H. Janwa and R. Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. *Proceedings of AAECC-10, Lecture Notes in Computer Science*, vol. 673, Berlin, Springer-Verlag, pp. 180-194, 1993.

[26] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Inform. and Control*, 18, pp. 369-394, 1971.

[27] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[28] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 386-397, 1994.

[29] K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, New York, 765, pp. 55-64, 1994.

[30] V. Sidelnikov. On mutual correlation of sequences, *Soviet Math. Dokl.*, 12(1971), pp. 197-201.