The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions

Lilya Budaghyan

Department of Mathematics, University of Trento, I-38050 Povo (Trento), Italy
lilia.b@mail.ru

Abstract. In 2005 Budaghyan, Carlet and Pott constructed the first APN polynomials EA-inequivalent to power functions by applying CCZ-equivalence to the Gold APN functions. It is a natural question whether it is possible to construct APN polynomials EA-inequivalent to power functions by using only EA-equivalence and inverse transformation on a power APN mapping: this would be the simplest method to construct APN polynomials EA-inequivalent to power functions. In the present paper we prove that the answer to this question is positive. By this method we construct a class of APN polynomials EA-inequivalent to power functions. On the other hand it is shown that the APN polynomials constructed by Budaghyan, Carlet and Pott cannot be obtained by the introduced method.

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

1 Introduction

A function $F : \mathbf{F}_2^m \to \mathbf{F}_2^m$ is called *almost perfect nonlinear* (APN) if, for every $a \neq 0$ and every b in $\mathbf{F}_2^m$, the equation $F(x) + F(x+a) = b$ admits at most two solutions (it is also called *differentially* 2*-uniform*). Vectorial Boolean functions used as S-boxes in block ciphers must have low differential uniformity to allow high resistance to the differential cryptanalysis (see [2,30]). In this sense APN functions are optimal. The notion of APN function is closely connected to the notion of almost bent (AB) function. A function $F : \mathbf{F}_2^m \to \mathbf{F}_2^m$ is called AB if the minimum Hamming distance between all the Boolean functions $v \cdot F$, $v \in \mathbf{F}_2^m \setminus \{0\}$, and all affine Boolean functions on $\mathbf{F}_2^m$ is maximal. AB functions exist for m odd only and oppose an optimum resistance to the linear cryptanalysis (see [28,15]). Besides, every AB function is APN [15], and in the m odd case, any quadratic function is APN if and only if it is AB [14].

The APN and AB properties are preserved by some transformations of functions [14,30]. If F is an APN (resp. AB) function, A_1, A_2 are affine permutations and A is affine then the function $F' = A_1 \circ F \circ A_2 + A$ is also APN (resp. AB); the functions F and F' are called extended affine equivalent (*EA-equivalent*). Another case is the *inverse transformation*, that is, the inverse of any APN

C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp. 177–188, 2007.

(resp. AB) permutation is APN (resp. AB). Until recently, the only known constructions of APN and AB functions were EA-equivalent to power functions $F(x) = x^d$ over finite fields ($\mathbf{F}_{2^m}$ being identified with $\mathbf{F}_2^m$). Table 1 gives all known values of exponents d (up to multiplication by a power of 2 modulo $2^m - 1$, and up to taking the inverse when a function is a permutation) such that the power function x^d over $\mathbf{F}_{2^m}$ is APN. For m odd the Gold, Kasami, Welch and Niho APN functions from Table 1 are also AB (for the proofs of AB property see [11,12,23,24,26,30]).

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

Functions	Exponents d	Conditions	Proven in
Gold	$2^i + 1$	$\gcd(i, m) = 1$	[23,30]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1$	[25,26]
Welch	$2^t + 3$	$m = 2t + 1$	[20]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$m = 2t + 1$	[19]
Inverse	$2^{2t} - 1$	$m = 2t + 1$	[1,30]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$m = 5t$	[21]

In [14], Carlet, Charpin and Zinoviev introduced an equivalence relation of functions, more recently called CCZ-equivalence, which corresponds to the affine equivalence of the graphs of functions and preserves APN and AB properties. EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse [14]. In [8,9], it is proven that CCZ-equivalence is more general, and applying CCZ-equivalence to the Gold mappings classes of APN functions EA-inequivalent to power functions are constructed. These classes are presented in Table 2. When m is odd, these functions are also AB.

Table 2. Known APN functions EA-inequivalent to power functions on $\mathbf{F}_{2^m}$

Functions	Conditions	Alg. degree
$x^{2^i+1} + (x^{2^i} + x + tr(1) + 1)tr(x^{2^i+1} + x\ tr(1))$	$m \geq 4$ $\gcd(i, m) = 1$	3
$[x + tr_{(m,3)}(x^{2(2^i+1)} + x^{4(2^i+1)})$ $+tr(x)tr_{(m,3)}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$	m divisible by 6 $\gcd(i, m) = 1$	4
$x^{2^i+1} + tr_{(m,n)}(x^{2^i+1}) + x^{2^i} tr_{(m,n)}(x) + x\ tr_{(m,n)}(x)^{2^i}$ $+[tr_{(m,n)}(x)^{2^i+1} + tr_{(m,n)}(x^{2^i+1}) + tr_{(m,n)}(x)]^{\frac{1}{2^i+1}}$ $\times(x^{2^i} + tr_{(m,n)}(x)^{2^i} + 1) + [tr_{(m,n)}(x)^{2^i+1}$ $+tr_{(m,n)}(x^{2^i+1}) + tr_{(m,n)}(x)]^{\frac{2^i}{2^i+1}}(x + tr_{(m,n)}(x))$	$m \neq n$ m divisible by n $\gcd(2i, m) = 1$	$n + 2$

These new results on CCZ-equivalence have solved several problems (see [8,9]) and have also raised some interesting questions. One of these questions is whether the known classes of APN power functions are CCZ-inequivalent. Partly the answer is given in [6]: it is proven that in general the Gold functions are CCZ-inequivalent to the Kasami and Welch functions, and that for different parameters $1 \leq i, j \leq \frac{m-1}{2}$ the Gold functions x^{2^i+1} and x^{2^j+1} are CCZ-inequivalent. Another interesting question is the existence of APN polynomials CCZ-inequivalent to power functions. Different methods for constructing quadratic APN polynomials CCZ-inequivalent to power functions have been proposed in [3,4,17,22,29], and infinite classes of such functions are constructed in [3,4,5,6,7]. In the present paper we consider the natural question whether it is possible to construct APN polynomials EA-inequivalent to power functions by applying only EA-equivalence and the inverse transformation on a power APN function. We prove that the answer is positive and construct a class of AB functions EA-inequivalent to power mappings by applying this method to the Gold AB functions. It should be mentioned that the functions from Table 2 cannot be obtained by this method. It can be illustrated, for instance, by the fact that for $m = 5$ the functions from Table 2 and for m even the Gold functions are EA-inequivalent to permutations [8,9,31], therefore, the inverse transformation cannot be applied in these cases and the method fails.

2 Preliminaries

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

$$F(x_1, \ldots, x_m) = \sum_{u \in \mathbf{F}_2^m} c(u) \Big(\prod_{i=1}^{m} x_i^{u_i} \Big), \qquad c(u) \in \mathbf{F}_2^m.$$

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

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

For any k, $0 \leq k \leq 2^m - 1$, the number $w_2(k)$ of the nonzero coefficients $k_s \in \{0, 1\}$ in the binary expansion $\sum_{s=0}^{m-1} 2^s k_s$ 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, $d^\circ(F) = \max_{0 \leq i \leq m-1, c_i \neq 0} w_2(i)$ (see [14]).

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

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

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

Let F be a function from $\mathbf{F}_{2^m}$ to itself and $A_1,\ A_2 : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ 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 the 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.

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

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

Note that since $\mathcal{L}$ is a permutation then the function $L_1(x, F(x))$ has to be a permutation too (see [6]). As shown in [14], EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse.

For a function $F : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ and any elements $a, b \in \mathbf{F}_{2^m}$ we denote

$$\delta_F(a, b) = |\{x \in \mathbf{F}_2^m : F(x + a) + F(x) = b\}|.$$

F is called a *differentially δ-uniform* function if $\max_{a \in \mathbf{F}_{2^m}^*, b \in \mathbf{F}_{2^m}} \delta_F(a, b) \le \delta$. Note that $\delta \ge 2$ for any function over $\mathbf{F}_{2^m}$. Differentially 2-uniform mappings are called *almost perfect nonlinear*.

For any function $F : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ we denote

$$\lambda_F(a, b) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{tr(bF(x)+ax)}, \qquad a, b \in \mathbf{F}_{2^m},$$

where $tr(x) = x + x^2 + x^4 + \cdots + x^{2^{m-1}}$ is the trace function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_2$. The set $\Lambda_F = \{\lambda_F(a, b) : a, b \in \mathbf{F}_{2^m}, b \neq 0\}$ is called the *Walsh spectrum* of the function F and the multiset $\{|\lambda_F(a, b)| : a, b \in \mathbf{F}_{2^n}, b \neq 0\}$ is called the *extended Walsh spectrum* of F. The value

$$\mathcal{NL}(F) = 2^{m-1} - \frac{1}{2} \max_{a \in \mathbf{F}_{2^m}, b \in \mathbf{F}_{2^m}^*} |\lambda_F(a, b)|$$

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

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

([15,32]) and in case of equality F is called *almost bent* or *maximum nonlinear*.

Obviously, AB functions exist only for n odd. It is proven in [15] that every AB function is APN and its Walsh spectrum equals $\{0, \pm 2^{\frac{m+1}{2}}\}$. If m is odd, every APN mapping which is quadratic (that is, whose algebraic degree equals 2) is AB [14], but this is not true for nonquadratic cases: the Dobbertin and the inverse APN functions are not AB (see [12,14]). When m is even, the inverse function x^{2^m-2} is a differentially 4-uniform permutation [30] and has the best known nonlinearity [27], that is $2^{m-1} - 2^{\frac{m}{2}}$ (see [12,18]). This function has been chosen as the basic S-box, with $m = 8$, in the Advanced Encryption Standard (AES), see [16]. A comprehensive survey on APN and AB functions can be found in [13].

It is shown in [14] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). More generally, CCZ-equivalent functions have the same differential uniformity and the same extended Walsh spectrum (see [8]). Further invariants for CCZ-equivalence can be found in [22] (see also [17]) in terms of group algebras.

3 The New Construction

In this section we show that it is possible to construct APN polynomials EA-inequivalent to power functions by applying only EA-equivalence and the inverse transformation on a power APN function. The inverse transformation and EA-equivalence are simple transformations of functions which preserve APN and AB properties. However, applying each of them separately on power mappings it is obviously impossible to construct polynomials EA-inequivalent to power functions. Therefore, our approach for constructing APN polynomials EA-inequivalent to power mappings is the simplest. We shall illustrate this method on the Gold AB functions and in order to do it we need the following result from [8,9].

Proposition 1. ([8,9]) *Let* $F : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$, $F(x) = L(x^{2^i+1}) + L'(x)$, *where* $\gcd(i, m) = 1$ *and* L, L' *are linear. Then* F *is a permutation if and only if, for every* $u \neq 0$ *in* $\mathbf{F}_{2^m}$ *and every* v *such that* $tr(v) = tr(1)$, *the condition* $L(u^{2^i+1}v) \neq L'(u)$ *holds.*

Further we use the following notations for any divisor n of m

$$tr_{(m,n)}(x) = x + x^{2^n} + x^{2^{2n}} \ldots + x^{2^{n(m/n-1)}},$$
$$tr_n(x) = x + x^2 + \cdots + x^{2^{n-1}}.$$

Theorem 1. *Let* $m \geq 9$ *be odd and divisible by* 3*. Then the function*

$$F'(x) = \left(x^{\frac{1}{2^i+1}} + tr_{(m,3)}(x + x^{2^{2i}})\right)^{-1},$$

with $1 \leq i \leq m$, $\gcd(i, m) = 1$, *is an AB permutation over* $\mathbf{F}_{2^m}$. *The function* F' *is EA-inequivalent to the Gold functions and to their inverses, that is, to* x^{2^j+1} *and* $x^{\frac{1}{2^j+1}}$ *for any* $1 \leq j \leq m$.

Proof. To prove that the function F' is an AB permutation we only need to show that the function $F_1(x) = x^{\frac{1}{2^i+1}} + tr_{(m,3)}(x + x^{2^{2i}})$ is a permutation. Since the function x^{2^i+1} is a permutation when m is odd and $\gcd(i,m)=1$ then F_1 is a permutation if and only if the function $F(x)=F_1(x^{2^i+1})=x+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})$, with $s=i \bmod 3$, is a permutation.

By Proposition 1 the function F is a permutation if for every $v\in\mathbf{F}_{2^m}$ such that $tr(v)=1$ and every $u\in\mathbf{F}^*_{2^m}$ the condition $tr_{(m,3)}(u^{2^i+1}v+(u^{2^i+1}v)^{2^{2s}})\neq u$ holds. Obviously, if $u\notin\mathbf{F}^*_{2^3}$ then $tr_{(m,3)}(u^{2^i+1}v+(u^{2^i+1}v)^{2^{2s}})\neq u$. For any $u\in\mathbf{F}^*_{2^3}$ the condition $tr_{(m,3)}(u^{2^i+1}v+(u^{2^i+1}v)^{2^{2s}})\neq u$ is equivalent to $u^{2^i+1}tr_{(m,3)}(v)+(u^{2^i+1}tr_{(m,3)}(v))^{2^{2s}}\neq u$. Therefore, F is a permutation if for every $u,w\in\mathbf{F}^*_{2^3}$, $tr_3(w)=1$ the condition $u^{2^i+1}w+(u^{2^i+1}w)^{2^{2s}}\neq u$ is satisfied. Then F is a permutation if $x+x^{2^i+1}+x^{2^{2s}(2^i+1)}$ is a permutation on $\mathbf{F}_{2^3}$ and that was easily checked by a computer.

We have $d^\circ(x^{2^i+1})=2$ and it is proven in [30] that $d^\circ(x^{\frac{1}{2^i+1}})=\frac{m+1}{2}$. We show below that $d^\circ(F')=4$ for $m\geq 9$. Since the function F' has algebraic degree different from 2 and $\frac{m+1}{2}$ then it is EA-inequivalent to the Gold functions and to their inverses.

Since $F'(x)=F_1^{-1}(x)=[F(x^{\frac{1}{2^i+1}})]^{-1}=[F^{-1}(x)]^{2^i+1}$ then to get the representation of the function F' we need the representation of the function F^{-1}. The following computations are helpful to show that $F^{-1}=F\circ F$.

$$\begin{aligned}
&tr_{(m,3)}[(x+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^i+1}]\\
&\quad=tr_{(m,3)}(x^{2^i+1})+tr_{(m,3)}(x^{2^s})tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&\qquad+tr_{(m,3)}(x)tr_{(m,3)}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&\qquad+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})tr_{(m,3)}(x^{2^i+1}+x^{2^s(2^i+1)}),
\end{aligned}$$

since

$$\begin{aligned}
&tr_{(m,3)}((x^{2^i+1}+x^{2^{2s}(2^i+1)})^{2^i})=tr_{(m,3)}((x^{2^i+1}+x^{2^{2s}(2^i+1)})^{2^s})\\
&\quad=tr_{(m,3)}(x^{2^s(2^i+1)}+x^{2^{3s}(2^i+1)})=tr_{(m,3)}(x^{2^s(2^i+1)}+x^{2^i+1}).
\end{aligned}$$

Then

$$\begin{aligned}
&tr_{(m,3)}[(x+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^i+1}+(x+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{2s}(2^i+1)}]\\
&\quad=tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+tr_{(m,3)}(x^{2^s})tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&\qquad+tr_{(m,3)}(x)tr_{(m,3)}(x^{2^{2s}(2^i+1)}+x^{2^s(2^i+1)})+tr_{(m,3)}(x)tr_{(m,3)}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&\qquad+tr_{(m,3)}(x^{2^{2s}})tr_{(m,3)}(x^{2^{2s}(2^i+1)}+x^{(2^i+1)})\\
&\qquad+tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})tr_{(m,3)}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&\qquad+tr_{(m,3)}(x^{2^{2s}(2^i+1)}+x^{2^s(2^i+1)})tr_{(m,3)}(x^{2^{2s}(2^i+1)}+x^{(2^i+1)})\\
&\quad=tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+tr_{(m,3)}(x+x^{2^s}+x^{2^{2s}})tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&\qquad+(tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2=tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&\qquad+tr_m(x)tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{(m,3)}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2
\end{aligned}$$

and

$$F \circ F(x) = x + tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^2$$

and, since $tr_m(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)})) = 0$,

$$\begin{aligned}(F \circ F) \circ F(x) &= x + tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + tr_m(x)[tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) \\ &\quad + tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^2] \\ &\quad + [tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) \\ &\quad + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^2]^2 = x + tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) \\ &\quad + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^2 + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^4 \\ &= x + tr_3(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)})) = x + tr_m(x^{2^i+1} + x^{2^{2s}(2^i+1)})) = x.\end{aligned}$$

Therefore,

$$F^{-1}(x) = F \circ F(x) = x + tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^2.$$

Thus, we have

$$\begin{aligned}&F'(x) = [F^{-1}(x)]^{2^i+1} = [x + tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + (tr_{(m,3)}(x^{2^i+1} \\ &+ x^{2^{2s}(2^i+1)}))^2]^{2^i+1} = x^{2^i+1} + tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} \\ &+ (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2(2^s+1)} + x^{2^i} tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) \\ &+ x\ tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s} + x^{2^i} tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{2s+1}(2^i+1)}) \\ &+ x\ (tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{2s+1}(2^i+1)}))^{2^s} + tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+2} \\ &+ tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^{s+1}+1} = x^{2^i+1} + (tr_{(m,3)}(x^{2^i+1} \\ &+ x^{2^{2s}(2^i+1)}))^{2(2^s+1)} + x^{2^i} tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) \\ &+ x\ tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^s(2^i+1)}) + x^{2^i} tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{2s+1}(2^i+1)}) \\ &+ x\ tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{s+1}(2^i+1)}) + tr_m(x)[(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} \\ &+ (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+2} + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^{s+1}+1}].\end{aligned}$$

The only item in this sum which can give algebraic degree greater than 4 is the last item. We have

$$\begin{aligned}&(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+2} \\ &\quad + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^{s+1}+1} = (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} \\ &\quad + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{4(2^s+1)} + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^{2s}},\end{aligned}$$

since

$$2^s + 2 = \begin{cases} 4 \text{ if } s = 1 \\ 6 \text{ if } s = 2 \end{cases},$$

$$4(2^s+1) = \begin{cases} 12 = 5 \pmod{2^3-1} \text{ if } s=1 \\ 20 = 6 \pmod{2^3-1} \text{ if } s=2 \end{cases},$$

$$2^{s+1}+1 = \begin{cases} 5 & \text{if } s=1 \\ 9 = 2 \pmod{2^3-1} & \text{if } s=2 \end{cases},$$

$$2^{2s} = \begin{cases} 4 & \text{if } s=1 \\ 16 = 2 \pmod{2^3-1} & \text{if } s=2 \end{cases}.$$

On the other hand,

$$(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} = tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)})$$
$$\times tr_{(m,3)}(x^{2^i+1} + x^{2^s(2^i+1)}) = tr_{(m,3)}(x^{2^i+1})^2 + (tr_{(m,3)}(x^{2^i+1}))^{2^{2s}+1}$$
$$+(tr_{(m,3)}(x^{2^i+1}))^{2^s+1} + (tr_{(m,3)}(x^{2^i+1}))^{2^{2s}+2^s}$$

$$= (tr_{(m,3)}(x^{2^i+1}))^6 + (tr_{(m,3)}(x^{2^i+1}))^5 + (tr_{(m,3)}(x^{2^i+1}))^3 + (tr_{(m,3)}(x^{2^i+1}))^2. \quad (1)$$

Using (1) we get

$$(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^s+1} + (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{4(2^s+1)}$$
$$+ (tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^{2s}} = (tr_{(m,3)}(x^{2^i+1}))^6$$
$$+ (tr_{(m,3)}(x^{2^i+1}))^5 + (tr_{(m,3)}(x^{2^i+1}))^3 + (tr_{(m,3)}(x^{2^i+1}))^2$$
$$+ [(tr_{(m,3)}(x^{2^i+1}))^3 + (tr_{(m,3)}(x^{2^i+1}))^6 + (tr_{(m,3)}(x^{2^i+1}))^5$$
$$+ tr_{(m,3)}(x^{2^i+1})] + (tr_{(m,3)}(x^{2^i+1}))^2 + (tr_{(m,3)}(x^{2^i+1}))^4$$

$$= tr_{(m,3)}(x^{2^i+1}) + (tr_{(m,3)}(x^{2^i+1}))^4. \quad (2)$$

Hence, applying (1) and (2) we get

$$F'(x) = x^{2^i+1} + [(tr_{(m,3)}(x^{2^i+1}))^6 + (tr_{(m,3)}(x^{2^i+1}))^5 + (tr_{(m,3)}(x^{2^i+1}))^3$$
$$+(tr_{(m,3)}(x^{2^i+1}))^2]^2 + x^{2^i} tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)})$$
$$+x\ tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^s(2^i+1)}) + x^{2^i} tr_{(m,3)}(x^{2(2^i+1)}$$
$$+x^{2^{2s+1}(2^i+1)}) + x\ tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{s+1}(2^i+1)})$$
$$+tr_m(x)[tr_{(m,3)}(x^{2^i+1}) + (tr_{(m,3)}(x^{2^i+1}))^4] = x^{2^i+1} + (tr_{(m,3)}(x^{2^i+1}))^6$$
$$+(tr_{(m,3)}(x^{2^i+1}))^5 + (tr_{(m,3)}(x^{2^i+1}))^3 + (tr_{(m,3)}(x^{2^i+1}))^4$$
$$+x^{2^i} tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + x\ tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{2^s(2^i+1)})$$
$$+x^{2^i} tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{2s+1}(2^i+1)}) + x\ tr_{(m,3)}(x^{2(2^i+1)} + x^{2^{s+1}(2^i+1)})$$
$$+tr_m(x) tr_{(m,3)}(x^{2^i+1} + x^{4(2^i+1)}).$$

Below we consider all items in the sum presenting the function F' which may give the algebraic degree 4:

$$[(tr_{(m,3)}(x^{2^i+1}))^6 + (tr_{(m,3)}(x^{2^i+1}))^5 + (tr_{(m,3)}(x^{2^i+1}))^3]$$

$$+[x^{2^i} tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + x\ tr_m(x)(tr_{(m,3)}(x^{2^i+1} + x^{2^s(2^i+1)})].$$

For simplicity we take $i = 1$. Obviously, all the items in the second bracket of the algebraic degree 4 have the form $x^{2^j+2^k+2^l+2^r}$, where $r < l < k < j \leq m-1$, $r \leq 1$. Therefore, if we find an item of algebraic degree 4 in the first bracket of the form $x^{2^j+2^k+2^l+2^r}$, where $2 \leq r < l < k < j \leq m-1$, which does not cancel, then this item does not vanish in the whole sum.

We have

$$\begin{aligned}
tr_{(m,3)}(x^3) &= x^{2+1} + x^{2^4+2^3} + \cdots + x^{2^{m-5}+2^{m-6}} + x^{2^{m-2}+2^{m-3}} \\
&= \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}}, \\
(tr_{(m,3)}(x^3))^2 &= x^{2^2+2} + x^{2^5+2^4} + \cdots + x^{2^{m-4}+2^{m-5}} + x^{2^{m-1}+2^{m-2}} \\
&= \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+2}+2^{3k+1}}, \\
(tr_{(m,3)}(x^3))^4 &= x^{2^3+2^2} + x^{2^6+2^5} + \cdots + x^{2^{m-3}+2^{m-4}} + x^{2^m+2^{m-1}} \\
&= \sum_{k=0}^{\frac{m}{3}-2} x^{2^{3k+3}+2^{3k+2}} + x^{2^{m-1}+1},
\end{aligned}$$

$$(tr_{(m,3)}(x^3))^3 = (tr_{(m,3)}(x^3))^2 tr_{(m,3)}(x^3) = \sum_{i,k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}+2^{3i+2}+2^{3i+1}}, \tag{3}$$

$$(tr_{(m,3)}(x^3))^5 = \sum_{j=0}^{\frac{m}{3}-2}\sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+1}+2^{3k}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+1}+2^{3k}}, \tag{4}$$

$$(tr_{(m,3)}(x^3))^6 = \sum_{j=0}^{\frac{m}{3}-2}\sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+2}+2^{3k+1}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+2}+2^{3k+1}}. \tag{5}$$

Note that all exponents of weight 4 in (3)-(5) are smaller than 2^m. If $m \geq 9$ then it is obvious that the item $x^{2^6+2^5+2^4+2^3}$ does not vanish in (4) and it definitely differs from all items in (3) and (5).

Hence, the function F' has the algebraic degree 4 when $m \geq 9$ and that completes the proof of the theorem. □

It is proven in [6] that the Gold functions are CCZ-inequivalent to the Welch function for all $m \geq 9$. Therefore, the function F' of Theorem 1 is CCZ-inequivalent to the Welch function. Further, the inverse and the Dobbertin APN functions are not AB (see [12,14]) and, therefore, the AB function F' is

CCZ-inequivalent to them. The algebraic degree of the Kasami function $x^{4^i-2^i+1}$, $2 \le i \le \frac{m-1}{2}$, $\gcd(i,m)=1$, is equal to $i+1$. Thus, its algebraic degree equals 4 if and only if $i=3$. Since the function F' is defined only for m divisible by 3 then for $i=3$ we would have $\gcd(i,m) \neq 1$. On the other hand, if Gold and Kasami functions are CCZ-equivalent then it follows from the proof of Theorem 5 of [6] that the Gold function is EA-equivalent to the inverse of the Kasami function which must be quadratic in this case. Thus, if F' was EA-equivalent to the inverse of a Kasami function then F' would be quadratic. Hence, F' cannot be EA-equivalent to the Kasami functions or to their inverses.

Proposition 2. *The function of Theorem 1 is EA-inequivalent to the Welch, Kasami, inverse, Dobbertin functions and to their inverses.*

For $m = 2t+1$ the Niho function has the algebraic degree $t+1$ if t is odd and the algebraic degree $(t+2)/2$ if t is even. Therefore, its algebraic degree equals 4 if and only if $m = 7, 13$.

Proposition 3. *The function of Theorem 1 is EA-inequivalent to the Niho function.*

We do not have a general proof of EA-inequivalence of F' and the inverse of the Niho function but for $m = 9$ the Niho function coincides with the Welch functions and therefore its inverse cannot be EA-equivalent to the function F'.

Corollary 1. *For $m = 9$ the function of Theorem 1 is EA-inequivalent to any power function.*

When m is odd and divisible by 3 the APN functions from Table 2 have algebraic degrees different from 4. Thus we get the following proposition.

Proposition 4. *The function of Theorem 1 is EA-inequivalent to any APN function from Table* 2.

Acknowledgments

We would like to thank Claude Carlet for many valuable discussions and for detailed and insightful comments on the several drafts of this paper. The main part of this work was carried out while the author was with Otto-von-Guericke University Magdeburg and the research was supported by the State of Saxony Anhalt, Germany; also supported by a postdoctoral fellowship of MIUR-Italy via PRIN 2006.

References

1. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 65–76. Springer, Heidelberg (1993)
2. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)

3. Budaghyan, L., Carlet, C.: Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. Preprint, available at `http://eprint.iacr.org/2007/098`
4. Budaghyan, L., Carlet, C., Leander, G.: Constructing new APN functions from known ones. Preprint, available at `http://eprint.iacr.org/2007/063`
5. Budaghyan, L., Carlet, C., Leander, G.: Another class of quadratic APN binomials over $\mathbf{F}_{2^n}$: the case n divisible by 4. In: Proceedings of the Workshop on Coding and Cryptography (2007) (To appear) available at `http://eprint.iacr.org/2006/428.pdf`
6. Budaghyan, L., Carlet, C., Leander, G.: A class of quadratic APN binomials inequivalent to power functions. Submitted to IEEE Trans. Inform. Theory, available at `http://eprint.iacr.org/2006/445.pdf`
7. Budaghyan, L., Carlet, C., Felke, P., Leander, G.: 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 (July 2006)
8. Budaghyan, L., Carlet, C., Pott, A.: New Classes of Almost Bent and Almost Perfect Nonlinear Functions. IEEE Trans. Inform. Theory 52(3), 1141–1152 (2006)
9. Budaghyan, L., Carlet, C., Pott, A.: New Constructions of Almost Bent and Almost Perfect Nonlinear Functions. In: Charpin, P., Ytrehus, Ø., (eds.) Proceedings of the Workshop on Coding and Cryptography 2005, pp. 306–315 (2005)
10. Canteaut, A., Charpin, P., Dobbertin, H.: A new characterization of almost bent functions. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 186–200. Springer, Heidelberg (1999)
11. Canteaut, A., Charpin, P., Dobbertin, H.: Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. IEEE Trans. Inform. Theory 46(1), 4–8 (2000)
12. Canteaut, A., Charpin, P., Dobbertin, H.: Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. SIAM Journal on Discrete Mathematics 13(1), 105–138 (2000)
13. Carlet, C.: Vectorial (multi-output) Boolean Functions for Cryptography. In: Crama, Y., Hammer, P. (eds.) Chapter of the monography Boolean Methods and Models, Cambridge University Press, to appear soon. Preliminary version available at `http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html`
14. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography 15(2), 125–156 (1998)
15. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
16. Daemen, J., Rijmen, V.: AES proposal: Rijndael (1999), `http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf`
17. Dillon, J.F.: APN Polynomials and Related Codes. Polynomials over Finite Fields and Applications, Banff International Research Station (November 2006)
18. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. Appl. Algebra Eng. Commun. Comput. 9(2), 139–152 (1998)
19. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case. Inform. and Comput. 151, 57–72 (1999)
20. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case. IEEE Trans. Inform. Theory 45, 1271–1275 (1999)

21. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. In: Jungnickel, D., Niederreiter, H. (eds.) Proceedings of Finite Fields and Applications FQ5, Augsburg, Germany, pp. 113–121. Springer, Heidelberg (2000)
22. Edel, Y., Kyureghyan, G., Pott, A.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52(2), 744–747 (2006)
23. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory 14, 154–156 (1968)
24. Hollmann, H., Xiang, Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields and Their Applications 7, 253–286 (2001)
25. Janwa, H., Wilson, R.: Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In: Moreno, O., Cohen, G., Mora, T. (eds.) AAECC-10. LNCS, vol. 673, pp. 180–194. Springer, Heidelberg (1993)
26. Kasami, T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. and Control 18, 369–394 (1971)
27. Lachaud, G., Wolfmann, J.: The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. IEEE Trans. Inform. Theory 36, 686–692 (1990)
28. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
29. Nakagawa, N., Yoshiara, S.: A construction of differentially 4-uniform functions from commutative semifields of characteristic 2. In: Proceedings of WAIFI 2007, LNCS (2007)
30. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994)
31. Nyberg, K.: S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. In: Preneel, B. (ed.) Fast Software Encryption. LNCS, vol. 1008, pp. 111–130. Springer, Heidelberg (1995)
32. Sidelnikov, V.: On mutual correlation of sequences. Soviet Math. Dokl. 12, 197–201 (1971)