On the sensitivity of some APN permutations to swapping points

Lilya Budaghyan Nikolay S. Kaleyski
Department of Informatics
University of Bergen
Bergen, Norway
{Lilya.Budaghyan, Nikolay.Kaleyski}@uib.no

Constanza Riera
Department of Computer Science,
Electrical Engineering and Mathematical Sciences
Western Norway University of Applied Sciences Bergen, Norway
csr@hvl.no

Pantelimon Stănică
Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943-5212, U.S.A.
pstanica@nps.edu

Abstract

We define a set called the pAPN-spectrum of an (n, n)-function F, which measures how close F is to being an APN function, and investigate how the size of the pAPN-spectrum changes when two of the outputs of a given function F are swapped. We completely characterize the behavior of the pAPN-spectrum under swapping outputs when $F(x) = x^{2^n-2}$ is the inverse function over $\mathbb{F}_{2^n}$. We also investigate this behavior for functions from the Gold and Welch monomial APN families, and experimentally determine the size of the pAPN-spectrum after swapping outputs for representatives from all known families of APN monomials up to dimension $n = 10$.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements for some positive integer n. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables. The set of all Boolean functions on n variables will be denoted by $\mathcal{B}_n$.

For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, we define the *Walsh-Hadamard transform* to be the integer valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)},$$

where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

A vectorial Boolean function, or (n, m)-function, is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, for some positive integers m and n. When $m = n$, it can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$) of the form

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

The binary weight $w_2(i)$ of a positive integer i is the number of non-zero bits in its binary expansion, i.e. $w_2(i) = \sum_{j=0}^{K} a_j$ where $i = \sum_{j=0}^{K} a_j 2^j$ for some positive integer K and for $a_j \in \{0, 1\}$, with all sums involved being computed over the integers. The algebraic degree of $F(x)$ is then the largest binary weight of an exponent i with $a_i \neq 0$. For an (n, n)-function F and for $a, b \in \mathbb{F}_{2^n}$, we define the Walsh transform $\mathcal{W}_F(a, b)$ of F to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^n(bF(x))$ at a, that is,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(x)+ax)}.$$

For an (n, n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} \mid F(x+a)+F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F \leq \delta$, then we say that F is differentially δ-uniform. Since $x + a$ is a solution to $F(x+a)+F(x) = b$ whenever x is, the differential uniformity is always even and is thus at least 2 for any F. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function.

APN functions correspond to optimal objects in other areas of mathematics and computer science, and are of great practical interest in cryptography, where they are used in the design of block ciphers. A number of characterizations of APN-ness can be found in the literature, and we give some of them below [2, 6, 7, 14].

Lemma 1. *Let F be an (n, n)-function.*

(i) We always have

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^4(a, b) \geq 2^{3n+1}(3 \cdot 2^{n-1} - 1),$$

with equality if and only if F is APN.

(ii) If, in addition, F is APN and satisfies $F(0) = 0$, then

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a, b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1).$$

(*iii*) (*Janwa-Wilson-Rodier Condition*[1]) *F is APN if and only if all the points $x, y, z \in \mathbb{F}_{2^n}$ satisfying*

$$F(x) + F(y) + F(z) + F(x + y + z) = 0$$

belong to the curve $(x + y)(x + z)(y + z) = 0$.

Along with S. Kwon, we introduced in [3] a notion of partial APN-ness in our attempt to resolve a conjecture on the upper bound on the algebraic degree of APN functions [2]. For a fixed $x_0 \in \mathbb{F}_{2^n}$, we call an (n, n)-function a (*partial*) *x_0-APN function* (which we typically refer to as x_0-APN, partially APN, or just pAPN, for short) if all points, x, y satisfying

$$F(x_0) + F(x) + F(y) + F(x_0 + x + y) = 0 \tag{1}$$

belong to the curve

$$(x_0 + x)(x_0 + y)(x + y) = 0. \tag{2}$$

We will refer to the set of points $x_0 \in \mathbb{F}_{2^n}$ for which a function is x_0-APN as the *pAPN-spectrum* of the function. Certainly, a function is APN if and only if it is x_0-APN for all points x_0; that is, it is APN if and only if its pAPN-spectrum is $\mathbb{F}_{2^n}$.

An alternative way to express the fact that a given function F is x_0-APN is to say that for any $a \neq 0$ the equation $F(x+a)+F(x) = F(x_0+a)+F(x_0)$ has only two solutions x, namely $x = x_0$ and $x = x_0 + a$. An interesting approach is taken in [10] where the partial APN concept is connected to the notion of a partial quadruple system (an instance of the much more general class of configurations called packings).

We shall denote by $\frac{1}{a}$ or $1/a$ the multiplicative inverse of a in $\mathbb{F}_{2^n}$, adopting the usual convention $\frac{1}{0} = 1/0 = 0$.

In this paper we show an intriguing property of the inverse, Gold and Welch functions: swapping two of their output values leads to a reduction in the size of their pAPN-spectra; in some cases, this reduction is quite significant. In the case of the inverse function, we completely characterize the cases in which the resulting function has an empty pAPN-spectrum.

2 Swapping outputs

A construction proposed in [16] designed to construct differentially 4-uniform permutations, involving swapping two outputs of a given (n, n)-function, has been the subject of many papers since then (see [5, 11, 12, 13, 18], to cite just a few works; a generalization allowing the modification of any two output values, of which swapping is a special case, is investigated in [9]). This naturally leads to the question of how swapping two outputs of a given function F would affect its pAPN-spectrum. We now describe the Janwa-Wilson-Rodier equation for an (n, n)-function F with two output points swapped. More precisely, given two points $x_0 \neq x_1$ in $\mathbb{F}_{2^n}$, we let $G_{x_0x_1}$ be the $\{x_0, x_1\}$-swapping of F defined by

$$G_{x_0x_1}(x) = F(x) + \left((x + x_0)^{2^n-1} + (x + x_1)^{2^n-1}\right)(y_0 + y_1), \tag{3}$$

[1] We have been calling this, the "Rodier condition", but we realized that it did occur in the literature prior to Rodier's work, for power monomials in [8], so we will now call it by the three names.

where $y_0 = F(x_0), y_1 = F(x_1)$. We will sometimes denote $G_{x_0x_1}$ simply by G if there is no danger of confusion.

Note that $x^{2^n-1} = 1$ in $\mathbb{F}_{2^n}$ unless $x = 0$, and so for any $x, y \in \mathbb{F}_{2^n}$, the expression $(x+y)^{2^n-1}$ is equal to 1 if $x \neq y$, and is equal to 0 if $x = y$.

The Janwa-Wilson-Rodier equation of $G = G_{x_0x_1}$ at $\zeta \in \mathbb{F}_{2^n}$ becomes

$$\begin{aligned} 0 = G(\zeta) + G(x) + G(y) + G(x+y+\zeta) = F(\zeta) + F(x) + F(y) + F(x+y+\zeta) \\ + \left((\zeta+x_0)^{2^n-1} + (\zeta+x_1)^{2^n-1} + (x+x_0)^{2^n-1} + (x+x_1)^{2^n-1} + (y+x_0)^{2^n-1}\right. \\ \left. +(y+x_1)^{2^n-1} + (x+y+\zeta+x_0)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{4}$$

We consider several cases depending on the value of ζ:

- If $\zeta = x_0$ (similarly, for $\zeta = x_1$), then (4) becomes (for $x \neq \zeta \neq y \neq x$)

$$\begin{aligned} 0 = F(x_0) + F(x) + F(y) + F(x+y+x_0) \\ + \left((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_0+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{5}$$

- If $\zeta = x_1$, then (4) becomes (for $x \neq \zeta \neq y \neq x$)

$$\begin{aligned} 0 = F(x_1) + F(x) + F(y) + F(x+y+x_1) \\ + \left((x+x_0)^{2^n-1} + (y+x_0)^{2^n-1} + (x+y+x_0+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{6}$$

  (Surely, Equations (5) and (6) are symmetric, so, we will not treat these similar cases.)

- If $x_0 \neq \zeta \neq x_1$, then (4) becomes (for $x \neq \zeta \neq y \neq x$),

$$\begin{aligned} 0 = F(\zeta) + F(x) + F(y) + F(x+y+\zeta) \\ + \left((x+x_0)^{2^n-1} + (x+x_1)^{2^n-1} + (y+x_0)^{2^n-1}\right. \\ \left. +(y+x_1)^{2^n-1} + (x+y+\zeta+x_0)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{7}$$

The analysis of the pAPN-spectrum of any function obtained via a two-point swap typically follows the cases outlined in (5) and (7).

When studying how swapping outputs affects the pAPN-spectrum, we do not restrict ourselves to APN functions and often drop the conditions on the parameters that guarantee their APN-ness. In a number of cases, the functions in question are differentially two-valued, i.e., there is a positive integer $s > 1$ such that all non-zero derivatives of these functions are 2^s-to-1. Such functions are not ζ-APN for any $\zeta \in \mathbb{F}_{2^n}$, and it is also easy to see that swapping two of their outputs will always result in an empty pAPN-spectrum.

Proposition 2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be such that $\Delta_F(a,b) \geq 4$ whenever $\Delta_F(a,b) \neq 0$. Then F has an empty pAPN-spectrum. Furthermore, for any $x_0, x_1 \in \mathbb{F}_{2^n}$, the pAPN-spectrum of the $\{x_0, x_1\}$-swapping $G_{x_0x_1}$, as defined in* (3)*, is also empty.*

3 Theoretical results

Using (5), (6), and (7), it is possible to derive theoretical conditions for the ζ-APN-ness of G. In this section, we present such results for the inverse, Gold, and Welch functions. We mostly focus on the case of the inverse function $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$, for which we are able to completely characterize the cases in which its pAPN-spectrum becomes empty. As pointed out in Section 4, according to our experimental results on APN functions over $\mathbb{F}_{2^n}$ with $4 \leq n \leq 10$, it appears that the inverse APN function is the only one among them whose pAPN-spectrum can be reduced to the empty set by a two-point swap.

We will use the following theorem [1, 15], which describes the existence of solutions for quadratic and cubic equations over binary finite fields.

Theorem 3. *Let n be a natural number, and consider the finite field $\mathbb{F}_{2^n}$.*

(1) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$.*

(2) *The equation $x^3 + ax + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $b \neq 0$, has (t_1, t_2 are the roots of $t^2 + bt + a^3 = 0$):*

   (*i*) *three solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) = \mathrm{Tr}_1^n(1)$ and t_1, t_2 are cubes in $\mathbb{F}_{2^n}$ for n even, and in $\mathbb{F}_{2^{2n}}$ for n odd;*

   (*ii*) *a unique solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) \neq \mathrm{Tr}_1^n(1)$;*

   (*iii*) *no solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) = \mathrm{Tr}_1^n(1)$ and t_1, t_2 are not cubes in $\mathbb{F}_{2^n}$ for n even, respectively, $\mathbb{F}_{2^{2n}}$ for n odd.*

Our main result describes the pAPN-spectrum of the inverse function $F(x) = x^{2^n-2}$ after swapping two points of its output. In particular, we characterize all cases in which the pAPN-spectrum is empty. To describe the pAPN spectrum, we concentrate on Equation (4). If some expression C is not zero, then C^{2^n-2} can be replaced by its inverse $1/C$. Thus, we need to consider a number of cases depending on which of the various expressions in (4) are non-zero. In each such case, we need to analyze equations of degree 2 or 3 in the finite field $\mathbb{F}_{2^n}$.

Theorem 4. *Let $F(x) = x^{2^n-2}$ be the inverse function on $\mathbb{F}_{2^n}$ and let $G_{x_0x_1}$ be the $\{x_0, x_1\}$-swapping of F for some $x_0, x_1 \in \mathbb{F}_{2^n}$ with $x_0 \neq x_1$. If n is odd, then:*

(*i*) *If $x_0 = 0$ or $x_1 = 0$, then $G_{x_0x_1}$ is not ζ-APN for any $\zeta \in \mathbb{F}_{2^n}$.*

(*ii*) *If $x_0x_1 \neq 0$, then G is not ζ-APN for $\zeta \notin \{0, x_0, x_1\}$. Furthermore:*

   (*a*) *if G is 0-APN, then $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 1$;*

   (*b*) *if G is x_0-APN, then $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 1$;*

   (*c*) *if $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 1$, then G is x_0-APN if and only if there is no $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $\mathrm{Tr}_1^n\left(\frac{t(\alpha+\alpha^{-1})}{t^2+\alpha^2+\alpha^{-2}+1}\right) = 0$, where $t = \frac{x_0}{x_1}$;*

(d) *if G is x_1-APN, then* $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right)=1$;

(e) *if* $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right)=1$, *then G is x_1-APN if and only if there is no* $\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ *such that* $\mathrm{Tr}_1^n\left(\frac{t(\alpha+\alpha^{-1})}{t^2+\alpha^2+\alpha^{-2}+1}\right)=0$, *where* $t=\frac{x_1}{x_0}$.

If n is even (and denoting by ω a primitive element of $\mathbb{F}_4$), then:

(i) *If say* $x_0=0$, *then* G_{0x_1} *is not ζ-APN if* $\zeta\in\{0,x_1\}$, *or* $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=0$, *or* $\mathrm{Tr}_1^n\left(\frac{\zeta^2+\zeta}{x_1^2}\right)=0$.

(ii) *If* $x_0x_1\neq 0$, *then we examine four cases depending on* $\left(\mathrm{Tr}_1^n\left(1/x_0^3\right),\mathrm{Tr}_1^n\left(1/x_1^3\right)\right)$:

(a) *if* $\mathrm{Tr}_1^n\left(1/x_0^3\right)=\mathrm{Tr}_1^n\left(1/x_1^3\right)=1$, *then G is not ζ-APN for* $\zeta\notin\{\omega x_0,\omega x_1,\omega^2x_0,\omega^2x_1\}$;

(b) *if* $\mathrm{Tr}_1^n\left(1/x_0^3\right)=0$ *and* $\mathrm{Tr}_1^n\left(1/x_1^3\right)=1$, *then G is not ζ-APN for* $\zeta\notin\{\omega x_0,\omega^2x_0\}$;

(c) *if* $\mathrm{Tr}_1^n\left(1/x_0^3\right)=1$ *and* $\mathrm{Tr}_1^n\left(1/x_1^3\right)=0$, *then G is not ζ-APN for* $\zeta\notin\{\omega x_1,\omega^2x_1\}$;

(d) *if* $\mathrm{Tr}_1^n\left(1/x_0^3\right)=\mathrm{Tr}_1^n\left(1/x_1^3\right)=0$, *then G is not ζ-APN for any* $\zeta\in\mathbb{F}_{2^n}$.

Proof. Suppose $x_0=0$ and $\zeta=0$. From (5), we have

$$\begin{aligned}0=&F(x)+F(y)+F(x+y)+\left((x+x_1)^{2^n-1}+(y+x_1)^{2^n-1}+(x+y+x_1)^{2^n-1}\right)y_1\\&=x^{2^n-2}+y^{2^n-2}+(x+y)^{2^n-2}\\&\qquad+\left((x+x_1)^{2^n-1}+(y+x_1)^{2^n-1}+(x+y+x_1)^{2^n-1}\right)y_1.\end{aligned}$$

Taking x such that $x\neq 0,x_1$, and letting $y=x+x_1$, we get $x^{2^n-2}+(x+x_1)^{2^n-2}+x_1^{2^n-2}=0$. By Theorem 3, this equation has two solutions if and only if $\mathrm{Tr}_1^n(x_1^2/x_1^2)=\mathrm{Tr}_1^n(1)=0$. Therefore, G_{0x_1} cannot be 0-APN when n is even. If n is odd, then we take $0\neq x\neq x_1\neq x\neq y\neq x+x_1$ and equation (5) becomes $F(x_1)+F(x)+F(y)+F(x+y)=0$, that is, $x^2y+xy^2+x_1y^2+x_1x^2+xyx_1=0$, and taking $a\neq 0,1$, we see that the pair $x=x_1\left(1+\frac{1}{a^2+a}\right)$, $y=x_1\left(a+\frac{1}{a+1}\right)$ is a solution. We can also see that $xy\neq 0$, $x\neq y$, and $y\neq x+x_1$. Thus, G_{0x_1} is not 0-APN when n is odd.

We now consider the case of $x_0=0,\zeta=x_1$. Equation (6) transforms into

$$F(x_1)+F(x)+F(y)+F(x+y+x_1)+\left(x^{2^n-1}+y^{2^n-1}+(x+y+x_1)^{2^n-1}\right)y_1. \tag{8}$$

Let $x,y,a\in\mathbb{F}_{2^n}$ be such that $x\neq y=ax\neq 0$, and $x\neq x_1(a+1)^{-1}$. Then (8) becomes

$$\begin{aligned}0&=x_1^{2^n-2}+x^{2^n-2}+y^{2^n-2}+(x+y+x_1)^{2^n-2}+y_1\\&=x^{2^n-2}+y^{2^n-2}+(x+y+x_1)^{2^n-2},\end{aligned}$$

which is equivalent to $0=x^2+y^2+xy+x_1(x+y)=x^2(a^2+a+1)+x_1x(a+1)$, rendering the solution $x=x_1(a+1)(a^2+a+1)^{-1}$. Thus, G_{0x_1} is not x_1-APN.

Finally, we consider the case of $\zeta \neq 0, x_1$. For $x_0 = 0$, equation (7) becomes

$$\begin{aligned} 0 = {} & F(\zeta) + F(x) + F(y) + F(x+y+\zeta) \\ & + \left(x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1} + (y+x_1)^{2^n-1}\right. \\ & \left. +(x+y+\zeta)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\right) y_1. \end{aligned} \tag{9}$$

We now assume that G_{0x_1} is ζ-APN, and so (9) has no nontrivial solutions. Take $y = 0$ and $x_1 + \zeta \neq x \neq x_1$ in (9). We get $\zeta^{-1} + x^{-1} + (x+\zeta)^{-1} + y_1 = 0$, which is equivalent to $x^2(1 + y_1\zeta) + x\zeta(1 + y_1\zeta) + \zeta^2 = 0$, and moreover, $x^2 + x\zeta + \frac{\zeta^2 x_1}{x_1+\zeta} = 0$. By Theorem 3 this equation has no solution, i.e., G is ζ-APN, if and only if

$$\mathrm{Tr}_1^n\left(\frac{\frac{\zeta^2 x_1}{x_1+\zeta}}{\zeta^2}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) = 1. \tag{10}$$

Now, take $0 \neq y = x_1 \neq x \neq 0$ in (9), as well as $x \neq x_1 + \zeta$, $x \neq \zeta$. We get $\zeta^{-1} + x^{-1} + (x + x_1 + \zeta)^{-1} = 0$, which is equivalent to $x^2 + x(x_1 + \zeta) + x_1\zeta + \zeta^2 = 0$, which has no solutions if and only if

$$\mathrm{Tr}_1^n\left(\frac{\zeta(x_1+\zeta)}{(x_1+\zeta)^2}\right) = \mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right) = 1. \tag{11}$$

Now, put together the conditions from equations (10) and (11). We obtain

$$0 = \mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) + \mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right) = \mathrm{Tr}_1^n(1).$$

When n is odd, $\mathrm{Tr}_1^n(1) = 1$. We obtain a contradiction, and therefore, G_{0x_1} cannot be ζ-APN for n odd.

Now, let $x_0x_1 \neq 0$. Assume that n is odd and $\zeta \neq 0$. Suppose $\zeta = x_0$ (the case when $\zeta = x_1$ is treated in a similar manner). Then equation (5) becomes

$$\begin{aligned} 0 = {} & x_0^{2^n-2} + x^{2^n-2} + y^{2^n-2} + (x+y+x_0)^{2^n-2} \\ & + \left((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_0+x_1)^{2^n-1}\right)\left(x_0^{2^n-2} + x_1^{2^n-2}\right). \end{aligned} \tag{12}$$

If the parenthesized expression vanishes, then an even number of its terms must evaluate to 0, which leads to only trivial solutions. At least one of the terms must therefore evaluate to 1, which leads to several cases. Most of them lead to equations having no solution or implying trivial solutions $x = \zeta$ or $y = \zeta$. In the case when $x, y \neq x_0, x_1$, $y \neq x + x_0 + x_1$, the equation becomes

$$\begin{aligned} 0 &= x_0^{2^n-2} + x^{2^n-2} + y^{2^n-2} + (x+y+x_0)^{2^n-2} + x_0^{2^n-2} + x_1^{2^n-2} \\ &= x^{2^n-2} + y^{2^n-2} + (x+y+x_0)^{2^n-2} + x_1^{2^n-2}. \end{aligned} \tag{13}$$

Suppose $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$. Taking $x = 0$, equation (13) reduces to $0 = y^{2^n-2} + (y+x_0)^{2^n-2} + x_1^{2^n-2}$, which is equivalent to $y^2 + yx_0 + x_0x_1 = 0$; this has solutions in y if and only

if $\mathrm{Tr}_1^n\left(\frac{x_0x_1}{x_0^2}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$. Thus, if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$, the function is not x_0-APN. If $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) \neq 0$, we consider the case $x \neq 0$ (similarly, $y \neq 0$). We can then write $y = \alpha x$, with $\alpha \neq 0, 1$. Equation (13) then reduces to $0 = \alpha(1+\alpha)x^2+(x_0\alpha+x_1(1+\alpha+\alpha^2))x+(1+\alpha)x_0x_1$, which is equivalent to $0 = x^2 + \frac{x_0\alpha+x_1(1+\alpha+\alpha^2)}{\alpha(1+\alpha)}x + \frac{x_0x_1}{\alpha}$. Label $t = x_0/x_1, z = x/x_1$. Dividing both sides by x_1^2, the above equation becomes $z^2 + \frac{t\alpha+\alpha^2+\alpha+1}{\alpha^2+\alpha}z + \frac{t}{\alpha} = 0$, which has a solution if and only if $\mathrm{Tr}_1^n\left(\frac{\frac{t}{\alpha}}{\left(\frac{t\alpha+\alpha^2+\alpha+1}{\alpha^2+\alpha}\right)^2}\right) = \mathrm{Tr}_1^n\left(\frac{t(\alpha+\alpha^{-1})}{t^2+\alpha^2+\alpha^{-2}+1}\right) = 0$.

Consider now the case of $\zeta \neq x_0, x_1$ with $\zeta \neq 0$. Assume first that $xy \neq 0$. Then, we can write $x = \beta\zeta$, and $y = \alpha\zeta$, with $\alpha, \beta \neq 0, 1$ and $\alpha \neq \beta$. Equation (7) then becomes $0 = \zeta^{2^n-2}(1+\alpha^{2^n-2}+\beta^{2^n-2}+(1+\alpha+\beta)^{2^n-2})+P(x_0^{2^n-2}+x_1^{2n-2})$, where $P = (x+x_0)^{2^n-1}+(x+x_1)^{2^n-1}+(y+x_0)^{2^n-1}+(y+x_1)^{2^n-1}+(x+y+\zeta+x_0)^{2^n-1}+(x+y+\zeta+x_1)^{2^n-1}$. Assume that $P = 0$ (which can be achieved, for instance, if all the parenthesized expressions in P are different from zero). The equation becomes $0 = \zeta^{2^n-2}(1+\alpha^{2^n-2}+\beta^{2^n-2}+(1+\alpha+\beta)^{2^n-2})$, which, since $\zeta \neq 0$, is equivalent to $0 = 1 + \alpha^{2^n-2} + \beta^{2^n-2} + (1+\alpha+\beta)^{2^n-2}$. For $\beta = \gamma\alpha$, with $\gamma \neq 0, 1, \frac{1}{\alpha}$, we obtain an equivalent equation which has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{\frac{1}{\gamma}}{\left(\frac{1+\gamma}{\gamma}\right)^2}\right) = \mathrm{Tr}_1^n\left(\frac{\gamma}{1+\gamma^2}\right) = 0$. Since $\frac{\gamma}{1+\gamma^2} = \frac{1}{1+\gamma} + \left(\frac{1}{1+\gamma}\right)^2$, we always have that $\mathrm{Tr}_1^n\left(\frac{\gamma}{1+\gamma^2}\right) = 0$, so this equation always has solutions. The function is thus not ζ-APN if $\zeta \neq 0, x_0, x_1$.

For n even, the conditions from equations (10) and (11) are equivalent, since $\mathrm{Tr}_1^n(1) = 0$, and $\frac{x_1}{x_1+\zeta} + \frac{\zeta}{x_1+\zeta} = 1$. Therefore, when n is even and $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) = 0$, the function G_{0x_1} is not ζ-APN.

Now, suppose $x_0x_1 \neq 0$. If the parenthesized expression in (7) vanishes, and $\zeta = 0$, but $x, y, x+y \neq 0$, then the equation transforms into $x^{-1} + y^{-1} + (x+y)^{-1} = 0$, which is equivalent to (with $y = ax$, $a \neq 0, 1$) $a^2 + a + 1 = 0$, which always has solutions for n even since $\mathrm{Tr}_1^n(1) = 0$. The function is thus never 0-APN for n even. However, for n odd, we have to consider the case where $\zeta = 0$ and the expression in the parentheses in (7) is equal to 1. In that case, we must have that $x = x_0$, or $x = x_1$, or $y = x_0$, or $y = x_1$, or $x + y = x_0$, or $x + y = x_1$. We take first the case $x = x_0$. Equation (7) becomes $0 = x_0^{-1} + y^{-1} + (y + x_0)^{-1} + x_0^{-1} + x_1^{-1}$, which is equivalent to $0 = y^2 + yx_0 + x_0x_1$, which has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{x_0x_1}{x_0^2}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$. In that case, the function is not 0-APN. By symmetry, the case $x = x_1$ gives the condition $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 0$. In that case, the function is not 0-APN. The other five cases lead to the same conditions. We conclude then that the function is not 0-APN, for n odd, when either $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$ or $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 0$, and is 0-APN otherwise.

Consider now $\zeta \neq 0$. If the parenthesized expression in (7) is 0, $\zeta \neq x_0, x_1$, and x, y, $x+y+\zeta \neq 0$, then equation (7) transforms into $\zeta^{-1}+x^{-1}+y^{-1}+(x+y+\zeta)^{-1} = 0$, which is equivalent to $0 = x^2y + xy^2 + x^2\zeta + y^2\zeta + x\zeta^2 + y\zeta^2 = (x+y)(x+\zeta)(y+\zeta)$, rendering trivial solutions.

If the parenthesized expression in (7) is 0, $\zeta \neq x_0, x_1$ and $x = 0$, but $y, y+\zeta \neq 0$, then equation (7) transforms into $\zeta^{-1} + y^{-1} + (y+\zeta)^{-1} = 0$, which is equivalent to $0 = y^2 + \zeta y + \zeta^2$, which has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{\zeta^2}{\zeta^2}\right) = \mathrm{Tr}_1^n(1) = 0$, which is always true for n even. For $\zeta = x_1 + x_0$, the parenthesized expression is always zero, and so the function cannot be ζ-APN.

Take now $x_1 \neq x_0 + \zeta$. We know that $y^2 + \zeta y + \zeta^2 = 0$ has exactly two different roots, $y_0 = \zeta\omega$ and $y_1 = \zeta\omega^2$, where ω is a primitive element of $\mathbb{F}_4$. When $y_j = x_k$ for $j, k = 0, 1$ or $y_j = x_k + \zeta$, these solutions are not valid. Suppose that $y_0 = x_0$. The equation $x_0^2 + \zeta x_0 + \zeta^2 = 0$ has solutions in ζ if and only if $\mathrm{Tr}_1^n(1/x_0^3) = 0$. The other forbidden roots induce the condition $\mathrm{Tr}_1^n(1/x_1^3) = 0$, or $\mathrm{Tr}_1^n(1/x_0^3) = 0$.

So, for $\mathrm{Tr}_1^n(1/x_0^3) = 0$, the function can be ζ-APN for $\zeta_0 = x_0\omega$ and $\zeta_1 = x_0\omega^2$, and similarly for x_1 under the condition $\mathrm{Tr}_1^n(1/x_1^3) = 0$. So we have that:

- If $\mathrm{Tr}_1^n(1/x_0^3) = 0 = \mathrm{Tr}_1^n(1/x_1^3)$, then G can be ζ-APN for at most four values of ζ.
- If $\mathrm{Tr}_1^n(1/x_0^3) = 0$, $\mathrm{Tr}_1^n(1/x_1^3) = 1$, then G can be ζ-APN for at most two values of ζ.
- If $\mathrm{Tr}_1^n(1/x_0^3) = 1$, $\mathrm{Tr}_1^n(1/x_1^3) = 0$, then G can be ζ-APN for at most two values of ζ.
- If $\mathrm{Tr}_1^n(1/x_0^3) = 1 = \mathrm{Tr}_1^n(1/x_1^3)$, then G cannot be ζ-APN for any ζ.

By symmetry, we obtain a similar result in the case of $y = 0$. If the expression in the parentheses in (7) is 0 and $y = x + \zeta$, but $x \neq 0, \zeta$, then (7) transforms into $\zeta^{-1} + x^{-1} + (x+\zeta)^{-1} = 0$, which is equivalent to $x^2 + \zeta x + \zeta^2 = 0$. We have already handled this equation in the case $x = 0$ above, and we do not get any new information from this.

If the parenthesized expression in (7) is 1, we cannot possibly have $x_0 = x_1 + \zeta$. We must then have that $x = x_0$, or $x = x_1$, or $y = x_0$, or $y = x_1$, or $x + y = \zeta + x_0$, or $x + y = \zeta + x_1$. We take first the case $\zeta \neq x_0, x_1, x_0 + x_1$. If $x = x_0$, then the equation becomes $\zeta^{-1} + x_0^{-1} + y^{-1} + (x_0 + y + \zeta)^{-1} + x_0^{-1} + x_1^{-1} = 0$, which is equivalent to $y^2(x_1 + \zeta) + y(\zeta + x_0)(\zeta + x_1) + \zeta x_1(\zeta + x_1) = 0$, which, since $x_1 \neq \zeta$, is equivalent to $y^2 + y(\zeta + x_0) + \zeta x_0 = 0$, that is, $(y + \zeta)(y + x_0) = 0$. However, any solution of this equation leads to a trivial solution of the Janwa-Wilson-Rodier equation. The other cases lead to trivial solutions as well.

Finally, we consider $\zeta \in \{x_0, x_1, x_0 + x_1\}$. Suppose that $\zeta = x_0$, and the parenthesized expression in (5) is 1. Then, we have that $x = x_1$, or $y = x_1$, or $x + y = x_0 + x_1$. On inspection, they either yield trivial solutions, or a contradiction. We have then that the function is ζ-APN. □

Remark 5. In the proof of the last item of the case n odd, $\zeta x_0 x_1 \neq 0$ above, taking $\beta = \alpha + \alpha^{-1}$, we can easily show that $\mathrm{Tr}_1^n\left(\frac{t\beta}{t^2+\beta^2+1}\right) = 0$ has solutions. To see this, we look at the equation $\frac{t\beta}{t^2+\beta^2+1} = t^2 + t$ ($t \neq 0$), which has solutions β if $\beta^2 + \frac{1}{1+t}\beta + (1+t)^2 = 0$, and this last equation, by Theorem 3, has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{(t+1)^2}{\frac{1}{(t+1)^2}}\right) = \mathrm{Tr}_1^n((t+$

$1)^4) = \mathrm{Tr}_1^n(t+1) = 0$, which holds, by our assumption that $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) \neq 0$ and n is odd. Unfortunately, it is not always true that there exists α such that $\alpha + \alpha^{-1} = \beta$ (this last equation has a solution α if and only if $\mathrm{Tr}_1^n(\beta^{-2}) = \mathrm{Tr}_1^n(\beta^{-1}) = 0$).

Using a similar approach, we can obtain comparable results for the Gold APN functions.

Theorem 6. *Let $F(x) = x^{2^k+1}$ be the Gold function on $\mathbb{F}_{2^n}$, where n is odd and $\gcd(k,n) = 1$. Let G_{0x_1} be the $\{0, x_1\}$-swapping of F for some $x_1 \in \mathbb{F}_{2^n}^*$. Then:*

- *G_{0,x_1} is not 0-APN;*
- *G_{0,x_1} is not x_1-APN for $0 \neq x_1 \in \mathbb{F}_{2^n}$ if and only if there exists $0 \neq t \in \mathbb{F}_{2^n}$ such that $\sum_{i=0}^{n-1} t^{2^{ki}} = 0$;*
- *if $0 \neq \zeta \neq x_1$, then G_{0x_1} is ζ-APN if and only if there are no solutions to either of $u^{2^k} + u + (x_1/\zeta)^{2^k+1} = 0$, and $y^{2^k} + y(x_1+\zeta)^{2^k-1} + x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta} = 0$; equivalently, G_{0x_1} is ζ-APN if and only if $\sum_{i=0}^{n-1} \left(\frac{x_1}{\zeta}\right)^{2^{ki}} \neq 0$ and $\sum_{i=0}^{n-1} \left((x_1+\zeta)^{-2^k}\left(x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta}\right)\right)^{2^{ki}} \neq 0$.*

The Welch APN functions can also be approached in the same way. To simplify the notation, we let

$$\begin{aligned} E(\zeta, x_1, x, y) &= \zeta^{2^n-1} + (\zeta + x_1)^{2^n-1} + x^{2^n-1} + (x + x_1)^{2^n-1} + y^{2^n-1} \\ &\quad + (y + x_1)^{2^n-1} + (x + y + \zeta)^{2^n-1} + (x + y + \zeta + x_1)^{2^n-1}, \\ C(\zeta, x, y) &= \zeta^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x + y + \zeta)^{2^k+3} \end{aligned}$$

in $\mathbb{F}_{2^n}$. Certainly, $E(\zeta, x_1, x, y) \in \{0, 1\}$.

Theorem 7. *Let $F(x) = x^{2^k+3}$ be the Welch function on $\mathbb{F}_{2^n}$, where n is odd and let G_{0x_1} be the $\{0, x_1\}$-swapping of F for some $0 \neq x_1 \in \mathbb{F}_{2^n}$. Then:*

- *G_{0x_1} is not 0-APN if $\gcd(2^k + 3, 2^n - 1) = 1$ (which always happens if $n = 2k + 1$), nor x_1-APN in general;*
- *if $\zeta \neq 0, x_1$, then G_{0x_1} is not ζ-APN if and only if there is a solution (x, y) of the system $C(\zeta, x, y) = 0$ and $E(\zeta, x_1, x, y) = 0$, or $C(\zeta, x, y) = x_1^{2^k+3}$ and $E(\zeta, x_1, x, y) = 1$, where $x_1, \zeta \neq x \neq y \neq x_1, \zeta$.*

4 Experimental results

In order to gain further insight into how the operation of swapping two output points affects the pAPN-spectrum of power functions, we ran an exhaustive search over all power functions from the known infinite families over $\mathbb{F}_{2^n}$ with $4 \leq n \leq 10$. In doing this, we relax all restrictions on the parameters, e.g. in the case of the Gold functions x^{2^i+1} over $\mathbb{F}_{2^n}$, we drop the condition that i and n must be coprime, and consider functions of the form x^{2^i+1} for all $1 \leq i \leq n-1$. For each considered function F, we go through all possible pairs $(x_0, x_1) \in \mathbb{F}_{2^n}^2$, and compute the size of the pAPN-spectrum of the function $G_{x_0x_1}$ obtained by swapping the outputs of F at x_0 and x_1.

Due to space limitations, we omit the full experimental results here; they can be found in the preprint of our full paper [4].

With the notable exception of the inverse function, it appears that for any APN function F, the pAPN-spectrum of any function obtained by a two-point swap from F is never empty. In order to check whether this might be true for APN functions in general, we perform the same computations for representatives from all known CCZ-equivalence classes of APN functions over $\mathbb{F}_{2^n}$ for $4 \leq n \leq 10$. In the case of $n = 7$ and $n = 8$, these include around 500 and 8000 functions, respectively [17]. Despite this, all of the tested functions (save for the inverse function) preserve a non-empty pAPN-spectrum after any two-point swap. We thus formulate the following conjecture.

Conjecture 8. Let F be any APN power functions over $\mathbb{F}_{2^n}$, CCZ-inequivalent to the inverse power function x^{2^n-2}, and let $G_{x_0x_1}$ be the (x_0, x_1)-swapping of F for some $(x_0, x_1) \in \mathbb{F}_{2^n}^2$. Then the pAPN-spectrum of G is not empty.

Acknowledgements

The paper was started while the fourth named author visited the Selmer center at University of Bergen and Western Norway University of Applied Sciences in the Spring of 2019. This author thanks these institutions for the excellent working conditions. The research of the first two named authors was supported by the Trond Mohn foundation.

References

[1] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10 (1967), 553–564.

[2] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, B. Sun, *On upper bounds for algebraic degrees of APN functions*, IEEE Trans. Inform. Theory 64:6 (2018), 4399–4411.

[3] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera, P. Stănică, *Partially APN Boolean functions and classes of functions that are not APN infinitely often*, Cryptography & Communications - CCDS 12 (2020), 527–545; preliminary version in Proc. Sequences and Their Applications – SETA 2018, Hong Kong, 2018.

[4] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera, P. Stănică, *On the sensitivity of some APN permutations to swapping points*, Cryptology ePrint Archive, Report 2020/557, 2020, https://eprint.iacr.org/2020/557.

[5] M. Calderini, I.Villa, *On the Boomerang Uniformity of some Permutation Polynomials*, https://eprint.iacr.org/2019/881.pdf.

[6] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[7] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Advances in Cryptology–EUROCRYPT'94, LNCS 950, pp. 356–365, 1995.

[8] H. Janwa and M. Wilson, *Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC10 (G. Cohen, T. Mora and O. Moreno, Eds.), LNCS 673, Springer-Verlag, New York/Berlin, pp. 180–194, 1993.

[9] N.S. Kaleyski, *Changing APN functions at two points*, Cryptography and Communications 11.6 (2019), 1165–1184.

[10] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stănică, *Vanishing Flats: A Combinatorial Viewpoint on the Planarity of Functions and Their Application*, to appear in IEEE Trans. Inf. Theory, 2020.

[11] D. Tang, C. Carlet, X. Tang, *Differentially 4-uniform bijections by permuting the inverse function*, Des. Codes. Cryptogr. 77 (2014), 117–141.

[12] L. Qu, Y. Tan, C. H. Tan, C. Li, *Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method*, IEEE Trans. Inf. Theory 59:4 (2013), 4675–4686.

[13] L. Qu, Y. Tan, C. Li, and G. Gong, *More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$*, Des., Codes Cryptogr. 78 (2016), 391–408.

[14] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman, eds., Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169–181, 2009.

[15] K.S. Williams, *Note on cubics over $GF(2^n)$ and $GF(3^n)$*, J. Number Theory 7 (1975), 361–365.

[16] Y. Yu, M. Wang and Y. Li, *Constructing differentially 4 uniform permutations from known ones*, Chinese Journal of Electronics 22.3 (2013): 495–499.

[17] Y. Yu, M. Wang and Y. Li, *A matrix approach for constructing quadratic APN functions.Designs*, Codes and Cryptography, 73.2 (2014): 587–600.

[18] Z. Zha, L. Hu, S. Sun, *Constructing new differentially* 4*-uniform permutations from the inverse function*, Finite Fields Appl. 25 (2014), 64–78.