# $C$-differentials, multiplicative uniformity and (almost) perfect $c$-nonlinearity

Pål Ellingsen, Patrick Felke, Constanza Riera, Pantelimon Stănică*, Anton Tkachenko

***Abstract*—In this paper we define a new (output) multiplicative differential, and the corresponding $c$-differential uniformity. With this new concept, even for characteristic $2$, there are perfect $c$-nonlinear (PcN) functions. We first characterize the $c$-differential uniformity of a function in terms of its Walsh transform. We further look at some of the known perfect nonlinear (PN) functions and show that only one remains a PcN function, under a different condition on the parameters. In fact, the $p$-ary Gold PN function increases its $c$-differential uniformity significantly, under some conditions on the parameters. We then precisely characterize the $c$-differential uniformity of the inverse function (in any dimension and characteristic), relevant for the Rijndael (and Advanced Encryption Standard) block cipher.**

***Index Terms*—Boolean, $p$-ary functions, $c$-differentials, Walsh transform, differential uniformity, perfect and almost perfect $c$-nonlinearity**

## I. Introduction and motivation

In [3], the authors used a new type of differential that is quite useful from a practical perspective for ciphers that utilize modular multiplication as a primitive operation. It is an extension of a type of differential cryptanalysis and it was used to cryptanalyse some existing ciphers (like a variant of the well-known IDEA cipher). The authors argue that one should look (and some authors did) at other types of differentials for a Boolean (vectorial) function $F$, not only the usual $(F(x+a),F(x))$. In [3], the differential used in their attack was $(F(cx),F(x))$. Drawing inspiration from the mentioned successful attempt, we therefore here start a theoretical analysis of an (output) multiplicative differential. We first connect the differential uniformity (under this new concept) to the Walsh coefficients. We next investigate some of the known perfect nonlinear $p$-ary functions and show that with one exception (under a different condition on the parameters, though) they do not remain perfect nonlinear under the new concept. We also look at the Rijndael inverse function and its $c$-differential uniformity (for example, we show that in some instances the uniformity drops to 3).

The objects of this study are Boolean and $p$-ary functions (where $p$ is an odd prime) and some of their differential properties. We will introduce here only some needed notation, and the reader can consult [4], [5], [6], [12], [15], [18] for more on Boolean and $p$-ary functions.

Let $n$ be a positive integer and $\mathbb{F}_{p^n}$ denote the finite field with $p^n$ elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n}\setminus\{0\}$ (for $a\neq 0$, we often write $\frac{1}{a}$ to mean the inverse of $a$ in the considered finite field). Further, let $\mathbb{F}_p^m$ denote the $m$-dimensional vector space over $\mathbb{F}_p$. We call a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ a *$p$-ary Boolean function* on $n$ variables. The cardinality of a set $S$ is denoted by $\#S$. For $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ we define the *Walsh-Hadamard transform* to be the integer-valued function $\mathcal{W}_f(u)=\sum_{x\in\mathbb{F}_{p^n}}\zeta_p^{f(x)-{\rm Tr}_n(ux)},\ u\in\mathbb{F}_{p^n}$, where $\zeta_p = e^{\frac{2\pi i}{p}}$ and ${\rm Tr}_n:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is the absolute trace function, given by ${\rm Tr}(x)=\sum_{i=0}^{n-1}x^{p^i}$.

Given a $p$-ary Boolean function $f$, the derivative of $f$ with respect to $a\in\mathbb{F}_{p^n}$ is the Boolean function $D_af(x)=f(x+a)-f(x),$ for all $x\in\mathbb{F}_{p^n}$.

For positive integers $n$ and $m$, any map $F:\mathbb{F}_p^n\to\mathbb{F}_p^m$ is called a vectorial $p$-ary Boolean function, or $(n,m)$-function. When $m=n$, $F$ can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ (using the natural identification of the finite field with the vector space) of the form $F(x)=\sum_{i=0}^{p^n-1}a_ix^i,\ a_i\in\mathbb{F}_{p^n}$. The algebraic degree of $F$ is then the largest Hamming weight of the exponents $i$ with $a_i\neq 0$. For an $(n,m)$-function $F$ and $a\in\mathbb{F}_{p^n}, b\in\mathbb{F}_{p^m}$, we define the Walsh transform $\mathcal{W}_F(a,b)$ to be the Walsh-Hadamard transform of its component function ${\rm Tr}_m(bF(x))$ at $a$, that is,

$$\mathcal{W}_F(a,b)=\sum_{x\in\mathbb{F}_{p^n}}\zeta_p^{{\rm Tr}_m(bF(x))-{\rm Tr}_n(ax)}.$$

For an $(n,n)$-function $F$, and $a,b\in\mathbb{F}_{p^n}$, we let $\Delta_F(a,b)=\#\{x\in\mathbb{F}_{p^n} : F(x+a)-F(x)=b\}$. We call the quantity $\Delta_F=\max\{\Delta_F(a,b)\,:\, a,b\in\mathbb{F}_{p^n}, a\neq 0\}$ the *differential uniformity* of $F$. If $\Delta_F\leq\delta$, then we say that $F$ is differentially $\delta$-uniform. If $\delta=1$, then $F$ is called a *perfect nonlinear* (*PN*) function, or *planar* function. If $\delta=2$, then $F$ is called an *almost perfect nonlinear* (*APN*) function. It is well known that PN functions do not exist if $p=2$.

## II. $c$-Differentials

It is natural to reflect about how the functions would respond, not only to the usual derivative, but to a more general

*Corresponding author
P. Ellingsen is with Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway.
E-mail: pel@hvl.no
P. Felke is with University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden, Germany.
E-mail: patrick.felke@hs-emden-leer.de
C. Riera is with Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway.
E-mail: csr@hvl.no
P. Stănică are with Naval Postgraduate School, Monterey, USA;
E-mail: pstanica@nps.edu
A. Tkachenko is with Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway.
E-mail: atk@hvl.no

derivative. Our proposal is inspired by a practical differential attack developed in [3].

**Definition 1.** *Given a $p$-ary $(n,m)$-function $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^m}$, and $c\in\mathbb{F}_{p^m}$, the (multiplicative) $c$-derivative of $F$ with respect to $a\in\mathbb{F}_{p^n}$ is the function*

$$ {}_cD_aF(x)=F(x+a)-cF(x),\ \text{for all } x\in\mathbb{F}_{p^n}. $$

*(Note that, if $c=1$, then we obtain the usual derivative, and, if $c=0$ or $a=0$, then we obtain a shift of the function.)*

For an $(n,n)$-function $F$, and $a,b\in\mathbb{F}_{p^n}$, we let ${}_c\Delta_F(a,b)=\#\{x\in\mathbb{F}_{p^n}: F(x+a)-cF(x)=b\}$. In the following, we call the quantity ${}_c\Delta_F=\max\left\{{}_c\Delta_F(a,b)\,:\,a,b\in\mathbb{F}_{p^n},\text{ and } a\neq 0 \text{ if } c=1\right\}$[1] the *$c$-differential uniformity* of $F$. If ${}_c\Delta_F=\delta$, then we say that $F$ is differentially $(c,\delta)$-uniform. If $\delta=1$, then $F$ is called a *perfect $c$-nonlinear* (*PcN*) function (certainly, for $c=1$, they only exist for odd characteristic $p$; however, one wonders whether they can exist for $p=2$ for $c\neq 1$, and we shall argue later that this is actually true). If $\delta=2$, then $F$ is called an *almost perfect $c$-nonlinear* (*APcN*) function. It is easy to see that if $F$ is an $(n,n)$-function, that is, $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, then $F$ is PcN if and only if ${}_cD_aF$ is a permutation polynomial.

Furthermore, any nonconstant affine function is PcN for any $c\neq 1$. Let $F(x)=Ax+B, 0\neq A,B\in\mathbb{F}_{p^n}$, and let $c\neq 1$. Then ${}_cD_aF(x)=\alpha$ (for some $\alpha$) is equivalent to $A(x+a)+B-Acx-cB=\alpha$, that is, $A(1-c)x=\alpha+(c-1)B-Aa$, which has a unique solution. By a similar argument, the function $F(x)=Ax^{p^k}+B, 0\neq A,B\in\mathbb{F}_{p^n}$ is PcN for any $c\neq 1$. We shall call these *trivial* PcN functions.

The solutions to the differential equation ${}_cD_aF(x)=b$ for various $c,b$ are not independent as the next proposition shows.

**Proposition 2.** *Let $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^m}$, $b_1,b_2\in\mathbb{F}_{p^m}$, and $c_1\neq c_2\in\mathbb{F}_{p^m}^*$. If $x_0$ is a solution for ${}_{c_1}D_aF(x)=b_1$, then $x_0$ is also a solution for ${}_{c_2}D_aF(x)=b_2$ if and only if $F(x_0)=\dfrac{b_1-b_2}{c_2-c_1}$.*

*Proof.* Assume that

$$ {}_{c_1}D_aF(x_0)=b_1 \text{ and } {}_{c_2}D_aF(x_0)=b_2. $$

Then

$$ \begin{aligned} b_1&=F(x_0+a)-c_1F(x_0)\\ b_2&=F(x_0+a)-c_2F(x_0), \end{aligned} $$

which, by subtracting, renders the claimed identity. The reciprocal is immediate. □

## III. Characterizing $c$-differential uniformity via the Walsh transform

In this section, we shall be using a method of Carlet [7] (which generalized the classical result of Chabaud and Vaudenay [9]) connecting the differential uniformity of an $(n,m)$-function to its Walsh coefficients. Since there are some subtle differences between the classical differential uniformity and our concept, we shall be proving (in any characteristic) the following result and some of its consequences, using the techniques of [7], [9]. Generalizing the usual convolution of two functions $f,g$ in two variables over some cartesian product of fields $\mathbb{F}\times\mathbb{K}$, namely, $(f\otimes g)(a,b)=\sum_{x\in\mathbb{F},y\in\mathbb{K}} f(x,y)g(a+x,b+y)$, we define a generalized convolution of the Walsh transforms (with a twist) of $F$ by

$$ \begin{aligned} &(\mathcal{W}_F\mathcal{W}_F^{c})^{\otimes(j+1)}(0,0)\\ &=\sum_{\substack{u_1,\ldots,u_j\in\mathbb{F}_{p^n}\\ v_1,\ldots,v_j\in\mathbb{F}_{p^m}}}\left(\overline{\mathcal{W}_F}\left(\sum_{i=1}^j u_i,\sum_{i=1}^j v_i\right)\mathcal{W}_F\left(\sum_{i=1}^j u_i,c\sum_{i=1}^j v_i\right)\right.\\ &\qquad\left.\cdot\prod_{i=1}^j\mathcal{W}_F(u_i,v_i)\overline{\mathcal{W}_F}(u_i,cv_i)\right) \end{aligned} $$

(observe that it is a convolution since the sum of the variables in each component is 0). We show the next theorem, which extends [7], [9] to odd characteristics, as well as to the $c$-differential context.

**Theorem 3.** *Let $c\in\mathbb{F}_{p^m}$ and $n,m,\delta$ be fixed positive integers. Let $F$ be an $(n,m)$-function, that is, $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^m}$. Let $\phi_\delta(x)=\sum_{j\geq 0}A_jx^j$ be a polynomial over $\mathbb{R}$ such that $\phi_\delta(x)=0$ for $x\in\mathbb{Z}, 1\leq x\leq\delta$, and $\phi_\delta(x)>0$, for $x\in\mathbb{Z}, x>\delta$. We then have*

$$ p^{2n}A_0+\sum_{j\geq 1}p^{-j(m+n)}A_j\left(\mathcal{W}_F\mathcal{W}_F^{c}\right)^{\otimes(j+1)}(0,0)\geq 0, $$

*with equality if and only if $F$ is $c$-differentially $\delta$-uniform.*

*Proof.* Let $a\in\mathbb{F}_{p^n},\gamma\in\mathbb{F}_{p^m}$ be arbitrary elements. Certainly, the set $\{x\in\mathbb{F}_{p^n}\,|\,{}_cD_aF(x)=\gamma\}$ is empty if $\gamma$ is not of the form ${}_cD_aF(b)$, for some $b\in\mathbb{F}_{p^n}$. Therefore, it is enough to consider only the cardinality $n_F(a,b,c)=|\{x\in\mathbb{F}_{p^n}\,|\,{}_cD_aF(x)={}_cD_aF(b)\}|>0$. From the imposed condition on the polynomial $\phi_\delta$, given $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^m}$, for all $a,b\in\mathbb{F}_{p^n}$, then,

$$ \sum_{j\geq 0}A_j\left(n_F(a,b,c)\right)^j\geq 0, $$

with equality if and only if ${}_c\Delta_F(a,b)\leq\delta$. Consequently, running with all $a,b\in\mathbb{F}_{p^n}$, any $(n,m)$-function $F$ satisfies

$$ \sum_{j\geq 0}A_j\sum_{a,b\in\mathbb{F}_{p^n}}\left(n_F(a,b,c)\right)^j\geq 0, $$

with equality if and only of ${}_c\Delta_F\leq\delta$.

Observe that

$$ n_F(a,b,c)=p^{-m}\sum_{x\in F_{p^n},v\in F_{p^m}}\zeta_p^{\mathrm{Tr}_m(v({}_cD_aF(x)-{}_cD_aF(b)))}, $$

since

$$ \sum_{v\in\mathbb{F}_{p^m}}\zeta_p^{\mathrm{Tr}_m(v\alpha)}=\begin{cases}0 & \text{if } \alpha\neq 0\\ p^m & \text{if } \alpha=0.\end{cases} \tag{1} $$

[1]Including $a=0$ for the case $c\neq 1$, the equation $F(x)-cF(x)=b$ is of course, $F(x)=b(1-c)^{-1}$, so we are looking here at how close $F$ is to a permutation polynomial, and similarly in the case $c=0$ for any $a$.

For a fixed $j \geq 1$, we then have

$$\sum_{a,b\in\mathbb{F}_{p^n}} (n_F(a,b,c))^j$$
$$= p^{-jm} \sum_{a,b\in\mathbb{F}_{p^n}} \sum_{\substack{x_1,\ldots,x_j\in\mathbb{F}_{p^n}\\ v_1,\ldots,v_j\in\mathbb{F}_{p^m}}} \zeta_p^{\sum_{i=1}^j \mathrm{Tr}_m(v_i({}_cD_aF(x_i)-{}_cD_aF(b))}$$
$$= p^{-jm} \sum_{a,b\in\mathbb{F}_{p^n}}$$
$$\sum_{\substack{x_1,\ldots,x_j\in\mathbb{F}_{p^n}\\ v_1,\ldots,v_j\in\mathbb{F}_{p^m}}} \zeta_p^{\sum_{i=1}^j \mathrm{Tr}_m(v_i(F(x_i+a)-cF(x_i)-F(b+a)+cF(b))}.$$

We need to insert some factors in the above expressions to make up the Walsh coefficients. By identity (1), $\sum_{u_i\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(u_i(x_i+a-y_i))} = p^n$, if $y_i = x_i+a$ and 0, otherwise. Similarly, $\sum_{u_0\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(u_0(d-a-b))} = p^n$, if $d = a+b$ and 0, otherwise. Therefore,

$$\sum_{a,b\in\mathbb{F}_{p^n}} (n_F(a,b,c))^j = p^{-mj}\ p^{-(j+1)n} \sum_{a,b,d\in\mathbb{F}_{p^n}}$$
$$\sum_{\substack{x_1,\ldots,x_j,y_1,\ldots,y_j\in\mathbb{F}_{p^n}\\ u_0,\ldots,u_j\in\mathbb{F}_{p^n},v_1,\ldots,v_j\in\mathbb{F}_{p^m}}}$$
$$\zeta_p^{\sum_{i=1}^j [\mathrm{Tr}_m(v_i(F(y_i)-F(d)-cF(x_i)+cF(b)))+\mathrm{Tr}_n(u_i(x_i+a-y_i))]+\mathrm{Tr}_n(u_0(d-a-b))}$$
$$= p^{-j(m+n)-n} \sum_{\substack{u_0,u_1,\ldots,u_j\in\mathbb{F}_{p^n}\\ v_1,\ldots,v_j\in\mathbb{F}_{p^m}}} \overline{\mathcal{W}_F}\left(u_0, \sum_{i=1}^j v_i\right)$$
$$\cdot \mathcal{W}_F\left(u_0, c\sum_{i=1}^j v_i\right) \prod_{i=1}^j \left(\mathcal{W}_F(u_i,v_i)\overline{\mathcal{W}_F}(u_i,cv_i)\right)$$
$$\cdot \sum_{a\in\mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n\left(a\left(\sum_{i=1}^j u_i - u_0\right)\right)}$$
$$= p^{-j(m+n)-n}\ p^n \sum_{\substack{u_1,\ldots,u_j\in\mathbb{F}_{p^n}\\ v_1,\ldots,v_j\in\mathbb{F}_{p^m}}} \overline{\mathcal{W}_F}\left(\sum_{i=1}^j u_i, \sum_{i=1}^j v_i\right)$$
$$\cdot \mathcal{W}_F\left(\sum_{i=1}^j u_i, c\sum_{i=1}^j v_i\right) \prod_{i=1}^j \left(\mathcal{W}_F(u_i,v_i)\overline{\mathcal{W}_F}(u_i,cv_i)\right)$$
$$= p^{-j(m+n)} \left(\mathcal{W}_F\mathcal{W}_F^c\right)^{\otimes(j+1)}(0,0).$$

For $j = 0$, $\sum_{a,b\in\mathbb{F}_{p^n}} (n_F(a,b,c))^j = p^{2n}$ and the theorem follows. □

**Remark 4.** *For a fixed $\delta$, an example of such a polynomial $\phi_\delta$ satisfying the conditions of the above theorem is simply $\phi_\delta(x) = (x-1)(x-2)\cdots(x-\delta)$, which certainly satisfies the conditions $\phi_\delta(x) = 0$, for $1 \leq x \leq \delta$, $x \in \mathbb{Z}$ and $\phi_\delta(x) > 0$, for $x > \delta$, $x \in \mathbb{Z}$.*

While we can take other values, we will only consider below the particular cases of perfect and almost perfect $c$-nonlinear functions, as the results are quite nice.

### A. The case $\delta = 1$ – perfect c-nonlinear (PcN)

We can take the polynomial $\phi_1(x) = x-1$, which certainly satisfies the conditions of Theorem 3. Thus $A_0 = -1, A_1 = 1$ and the relation of Theorem 3 simplifies to

$$-p^{2n} + p^{-(m+n)} \sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2 \geq 0.$$

Thus, we obtain the next result.

**Proposition 5.** *Let $m, n$ be fixed positive integers and $c \in \mathbb{F}_{p^m}$, $c \neq 1$. Let $F$ be an $(n,m)$-function. Then*

$$\sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2 \geq p^{3n+m},$$

*with equality if and only if $F$ is a perfect c-nonlinear (PcN) function.*

### B. The case $\delta = 2$ – almost perfect c-nonlinear (APcN)

We can take the polynomial $\phi_1(x) = (x-1)(x-2) = x^2 - 3x + 2$, which certainly satisfies the conditions of Theorem 3. Thus $A_0 = 2, A_1 = -3, A_2 = 1$ and the relation of Theorem 3 simplifies to

$$2\cdot p^{2n} - 3\cdot p^{-(m+n)} \sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2$$
$$+ p^{-2(m+n)} \sum_{\substack{u_1,u_2\in\mathbb{F}_{p^n}\\ v_1,v_2\in\mathbb{F}_{p^m}}} \overline{\mathcal{W}_F}(u_1+u_2, v_1+v_2)$$
$$\cdot \mathcal{W}_F(u_1+u_2, c(v_1+v_2))\mathcal{W}_F(u_1,v_1)$$
$$\cdot \mathcal{W}_F(u_2,v_2)\overline{\mathcal{W}_F}(u_1,cv_1)\overline{\mathcal{W}_F}(u_2,cv_2) \geq 0.$$

We then have the following result.

**Proposition 6.** *Let $m, n$ be fixed positive integers and $c \in \mathbb{F}_{p^m}$, $c \neq 1$. Let $F$ be an $(n,m)$-function. Then*

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_{p^n}\\ v_1,v_2\in\mathbb{F}_{p^m}}} \overline{\mathcal{W}_F}(u_1+u_2, v_1+v_2)\mathcal{W}_F(u_1+u_2, c(v_1+v_2))$$
$$\cdot \overline{\mathcal{W}_F}(u_1,v_1)\overline{\mathcal{W}_F}(u_2,v_2)\mathcal{W}_F(u_1,cv_1)\mathcal{W}_F(u_2,cv_2)$$
$$\geq 3\cdot p^{m+n} \sum_{\substack{u\in\mathbb{F}_{p^n}\\ v\in\mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2 - 2\cdot p^{2(2n+m)},$$

*with equality if and only if $F$ is an almost perfect c-nonlinear (APcN).*

In the spirit of Berger et al. [1] and Carlet [8], we can also express the $c$-differential uniformity of an $(n,m)$-function $F$ in terms of the Walsh transform of the $c$-derivative of $F$. We will omit the proof as it is similar to the one of the classical case.

**Theorem 7.** *Let $1 \neq c \in \mathbb{F}_{p^m}$, $n, m, \delta$ be fixed positive integers, and let $F$ be an $(n,m)$-function. Let $\phi_\delta(x) = \sum_{j\geq 0} A_j x^j$ be a polynomial over $\mathbb{R}$ such that $\phi_\delta(x) = 0$*

*for $x \in \mathbb{Z}, 1 \le x \le \delta$, and $\phi_\delta(x) > 0$, for $x \in \mathbb{Z}, x > \delta$. We then have*

$$p^n A_0 + \sum_{j\ge 1} p^{-jm} A_j \sum_{v_1,\ldots,v_j \in \mathbb{F}_{p^m}} \mathcal{W}_{{}_cD_aF}\left(0, \sum_{i=1}^j v_i\right) \cdot \prod_{i=1}^j \mathcal{W}_{{}_cD_aF}(0, v_i) \ge 0,$$

*with equality if and only if $F$ is $c$-differentially $\delta$-uniform.*

## IV. $c$-Differential uniformity for some known $PN$ classes

If $c = 1$, the following are some of the known classes of PN [11], [13] (recall that they exist if and only if $p$ is odd).

**Theorem 8.** *The following functions $: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are perfect nonlinear:*

(1) $F(x) = x^2$ *on* $\mathbb{F}_{p^n}$.
(2) $F(x) = x^{p^k+1}$ *on* $\mathbb{F}_{p^n}$ *is PN if and only if* $\frac{n}{\gcd(k,n)}$ *is odd.*
(3) $F(x) = x^{10} \pm x^6 - x^2$ *is PN over* $\mathbb{F}_{3^n}$ *if and only if* $n = 2$ *or* $n$ *is odd. In general, for* $u \in \mathbb{F}_{3^n}$, $F(x) = x^{10} - ux^6 - u^2x^2$ *is PN over* $\mathbb{F}_{3^n}$ *if* $n$ *is odd.*
(4) $F(x) = x^{(3^k+1)/2}$ *is PN over* $\mathbb{F}_{3^n}$ *if and only if* $\gcd(k,n) = 1$ *and* $n$ *is odd.*

It is not surprising that the above monomials are the only known planar (PN) functions since it was shown by Rónyai and Szönyi [17] that all planar functions are quadratic and by Zieve [19] that if the degree $n$ of $\mathbb{F}_{p^n}$ is large enough, namely, $p^n \ge (k-1)^4$, then the only PN monomials $x^k$ are in the list above. It is conjectured that these are the only PN power functions.

Below we will investigate the same functions regarding their $PcN$ property for $c \neq 1$. We first start with a lemma, which is possibly known (but we could not find an appropriate reference).

**Lemma 9.** *Let $p, k, n$ be integers greater than or equal to 1 (we take $k \le n$, though the result can be shown in general). Then*

$$\gcd(2^k+1, 2^n-1) = \frac{2^{\gcd(2k,n)}-1}{2^{\gcd(k,n)}-1}, \text{ and if } p > 2, \text{ then,}$$
$$\gcd(p^k+1, p^n-1) = 2, \text{ if } \frac{n}{\gcd(n,k)} \text{ is odd,}$$
$$\gcd(p^k+1, p^n-1) = p^{\gcd(k,n)}+1, \text{ if } \frac{n}{\gcd(n,k)} \text{ is even.}$$

*Consequently, if either $n$ is odd, or $n \equiv 2 \pmod 4$ and $k$ is even, then $\gcd(2^k+1, 2^n-1) = 1$ and $\gcd(p^k+1, p^n-1) = 2$, if $p > 2$.*

*Proof.* We shall use below the well-known identity

$$\gcd(p^r-1, p^n-1) = p^{\gcd(r,n)}-1.$$

Using the above identity, we first write $\gcd(p^{2k}-1, p^n-1) = p^{\gcd(2k,n)}-1$, and since $\gcd(p^k-1, p^k+1) = 2$, unless $p = 2$, in which case $\gcd(2^k-1, 2^k+1) = 1$, then we get

$$\begin{aligned}\gcd(2^{2k}-1, 2^n-1) &= \gcd(2^k-1, 2^n-1)\cdot\gcd(2^k+1, 2^n-1)\\ &= \left(2^{\gcd(k,n)}-1\right)\gcd(2^k+1, 2^n-1),\end{aligned}$$

and the first claim is shown.

We now assume that $p > 2$. If $k = 1$, we observe that

$$\gcd(p+1, p^n-1) = \gcd(p+1, p^n-1+p+1) = \gcd(p+1, p^{n-1}+1).$$

If $n$ is even, then $n-1 = 2r+1$ (for some $r$) is odd and using the decomposition $p^{2r+1}+1 = (p+1)(p^{2r}+p^{2r-1}+\cdots+p+1)$, we see that $\gcd(p+1, p^{n-1}+1) = p+1$. If $n$ is odd, then $n-1 = 2r$ (for some $r$) is even and consequently we continue the displayed reduction and arrive at $\gcd(p+1, p^n-1) = \gcd(p+1, p^{2r}+1) = \gcd(p+1, p^{2r-2}+1) = \cdots = \gcd(p+1, p^0+1) = 2$.

We next let $k \ge 2$, next. Let $d = \gcd(n,k)$ and $n = dm, k = d\ell$, with $\gcd(m,\ell) = 1$. First observe that

$$\begin{aligned}\gcd\left(p^{d\ell}+1, p^{dm}-1\right) &= \gcd\left(p^{d\ell}+1, p^{dm}+p^{d\ell}\right)\\ &= \gcd\left(p^{d\ell}+1, p^{d(m-\ell)}+1\right)\\ &= \gcd\left(p^{d\ell}+1, p^{d(m-\ell)}-p^{d\ell}\right)\\ &= \begin{cases}\gcd\left(p^{d\ell}+1, p^{d(m-2\ell)}-1\right) & \text{if } m \ge 2\ell\\ \gcd\left(p^{d\ell}+1, p^{d(2\ell-m)}-1\right) & \text{if } m < 2\ell.\end{cases}\end{aligned} \tag{2}$$

In both cases, we see that $|m-2\ell| < m$. We continue the process and apply Fermat's descent method below. We consider two cases.

*Case* 1 : *$m$ is odd*. Since $m$ is odd, the process above arrives at

$$\gcd\left(p^{d\ell}+1, p^{dm}-1\right) = \gcd\left(p^{d\ell}+1, p^d-1\right).$$

Now, we switch sides and concentrate on the first expression. We obtain

$$\begin{aligned}\gcd\left(p^d-1, p^{d\ell}+1\right) &= \gcd\left(p^d-1, p^{d\ell}+1-p^{d(\ell-1)}(p^d-1)\right)\\ &= \gcd\left(p^d-1, p^{d(\ell-1)}+1\right) = \cdots\\ &= \gcd\left(p^d-1, p^d+1\right) = 2.\end{aligned}$$

*Case* 2 : *$m$ is even*. Then the reduction from (2) arrives at (recall that now, $\ell$ is odd)

$$\begin{aligned}\gcd\left(p^{d\ell}+1, p^{dm}-1\right) &= \gcd\left(p^{d\ell}+1, p^{2d}-1\right)\\ &= \gcd\left(p^{2d}-1, p^{d\ell}+p^{2d}\right)\\ &= \gcd\left(p^{2d}-1, p^{d(\ell-2)}+1\right) = \cdots\\ &= \gcd\left(p^{2d}-1, p^d+1\right) = p^d+1.\end{aligned} \tag{3}$$

Lastly, if $n$ is odd and $k$ arbitrary, then $\gcd(2k,n) = \gcd(k,n)$, and so identity (3) becomes $\left(2^{\gcd(k,n)}-1\right)\gcd(2^k+1, 2^n-1) = 2^{\gcd(2k,n)}-1 = 2^{\gcd(k,n)}-1$, rendering $\gcd(2^k+1, 2^n-1) = 1$. If $n \equiv 2 \pmod 4$ and $k$ is even, say $n = 4t+2$, and $k = 2\ell$ for some

$t,\ell$, then $\gcd(2k,n)=\gcd(4\ell,4t+2)=2\gcd(\ell,2t+1)=\gcd(2\ell,4t+2)=\gcd(k,n)$, and identity (3) implies $\gcd(2^k+1,2^n-1)=1$. A similar analysis works for $p>2$, as well. □

It is easy to see that if $F(x)=x^n$, then ${}_c\Delta_F(a,b)={}_c\Delta_F(1,b/a^n)$, so we shall be using this often below.

**Theorem 10.** *Let $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be the monomial $F(x)=x^d$, and $c\neq 1$ be fixed. The following statements hold:*

- $(i)$ *If $d=2$, then $F$ is APcN, for all $c\neq 1$.*
- $(ii)$ *If $d=p^k+1$, $p>2$, then $F$ is not PcN, for all $c\neq 1$. Moreover, when $(1-c)^{p^k-1}=1$ and $n/\gcd(n,k)$ is even, the c-differential uniformity ${}_c\Delta_F\geq p^g+1$, where $g=\gcd(n,k)$.*
- $(iii)$ *Let $p=3$. If $d=\dfrac{3^k+1}{2}$, then $F$ is PcN, for $c=-1$ if and only if $\dfrac{2n}{\gcd(2n,k)}$ is odd.*
- $(iv)$ *If $p=3$ and $F(x)=x^{10}-ux^6-u^2x^2$, the c-differential uniformity of $F$ is ${}_c\Delta_F\geq 2$, for $c\neq 1$.*

*Proof.* We first take $d=2$ and consider the equation $cD_aF(x)=b$. Thus,

$$b=F(x+a)-cF(x)=(1-c)x^2+2ax+a^2,$$

and since we have the choice of $b$ (for example, $b=0$), the above equation has two solutions if and only if $c\neq 1$, and therefore it is $APcN$.

We now consider $d=p^k+1$. The equation $cD_aF(x)=b$ becomes

$$\begin{aligned}b&=(x+a)^{p^k+1}-cx^{p^k+1}\\&=x^{p^k+1}+a^{p^k+1}+ax^{p^k}+a^{p^k}x-cx^{p^k+1}\\&=(1-c)x^{p^k+1}+a\,x^{p^k}+a^{p^k}x+a^{p^k+1}.\end{aligned}$$

Assuming $c\neq 1$, and choosing $b=-\frac{c\,a^{p^k+1}}{1-c}$, the equation transforms into

$$((1-c)x+a)\,x^{p^k}+\frac{a^{p^k}}{1-c}\,((1-c)x+a)=0,$$

which is equivalent to

$$\begin{aligned}0&=((1-c)x+a)\left(x^{p^k}+\frac{a^{p^k}}{1-c}\right)\\&=((1-c)x+a)\left(x+\frac{a}{d}\right)^{p^k},\end{aligned}$$

where $r$ is one of the $p^k$-roots of $1-c\neq 0$.

If $1-c=r^{p^k}\neq r$ (which always happens if $\gcd(k,n)=1$) there are at least two roots of the equation $cD_aF(x)=b$ and consequently, $F$ is not $PcN$.

If $1-c=r^{p^k}=d$ (equivalently, for $c\neq 1$, $(1-c)^{p^k-1}=1$), then we write the equation $cD_aF(x)=b$, for some $a\neq 0$, as (we first multiply it by $d/a^{p^k+1}$)

$$(rx/a)^{p^k+1}+(rx/a)^{p^k}+rx/a+r(1-b/a^{p^k+1})=0,$$

and relabeling $y=rx/a$, $b_1=r(1-b/a^{p^k+1})$, we then get

$$y^{p^k+1}+y^{p^k}+y+b_1=0. \tag{4}$$

If $b_1=0$, then the equation becomes $y^{p^k+1}+y^{p^k}+y=y(y^{p^k}+y^{p^k-1}+1)=0$ with the obvious solution $y=0$.

We next consider the roots of the second equation, that is, $y^{p^k}+y^{p^k-1}+1=0$, or equivalently (with $z=1/y$), $z^{p^k}+z+1=0$. In [14] it is shown that a trinomial $z^{p^k}-az-b$ in $\mathbb{F}_{p^n}$ has either zero, one, or $p^g$ roots, where $g=\gcd(n,k)$.

We can perhaps approach this equation directly, but we can be more precise and use the method of [10], which fixed some errors of [14] and made its results more accurate. We will recall what was shown in [10]. Let $f(z)=z^{p^k}-az-b$ in $\mathbb{F}_{p^n}$, $g=\gcd(n,k)$, $m=n/\gcd(n,k)$ and $\mathrm{Tr}_g$ be the relative trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^g}$. For $0\leq i\leq m-1$, we define $t_i=\sum_{j=i}^{m-2}p^{n(j+1)}$, $\alpha_0=a,\beta_0=b$. If $m>1$ (note that, if $m=1$, then $k=n$, so $F(x)=x^2$, treated in case *(i)*), then, for $1\leq r\leq m-1$, we set

$$\alpha_r=a^{1+p^k+\cdots+p^{kr}}\text{ and }\beta_r=\sum_{i=0}^{r}a^{s_i}b^{p^{ki}},$$

where $s_i=\sum_{j=i}^{r-1}p^{k(j+1)}$, for $0\leq i\leq r-1$ and $s_r=0$. The trinomial $f$ has no roots in $\mathbb{F}_{p^n}$ if and only if $\alpha_{m-1}=1$ and $\beta_{m-1}\neq 0$. If $\alpha_{m-1}\neq 1$, then it has a unique root, namely $x=\beta_{m-1}/(1-\alpha_{m-1})$, and, if $\alpha_{m-1}=1,\beta_{m-1}=0$, it has $p^g$ roots in $\mathbb{F}_{p^n}$ given by $x+\delta\tau$, where $\delta\in\mathbb{F}_{p^g}$, $\tau$ is fixed in $\mathbb{F}_{p^n}$ with $\tau^{p^k-1}=a$ (that is, a $(p^k-1)$-root of $a$), and, for any $e\in\mathbb{F}_{p^n}^*$ with $\mathrm{Tr}_g(e)\neq 0$, then $x=\dfrac{1}{\mathrm{Tr}_g(e)}\displaystyle\sum_{i=0}^{m-1}\left(\sum_{j=0}^{i}e^{p^{kj}}\right)a^{t_i}b^{p^{ki}}$. We could easily simplify some of these parameters using the sum of the geometric sequence, namely

$$s_i=\frac{p^{k(r+1)}-p^{k(i+1)}}{p^k-1},\quad \alpha_r=a^{\frac{p^{k(r+1)}-1}{p^k-1}},$$

though, for our case, these closed forms will not be useful.

For our case, $a=b=-1$ and we further compute the involved parameters, splitting the analysis in two cases. We denote by $\sigma_t\equiv t\pmod 2$ the parity of $t$, that is $t\pmod 2\in\{0,1\}$. First, recall that $\alpha_0=\beta_0=-1$.

*Case* 1. $m=\frac{n}{\gcd(n,k)}=2\ell+1$, for some $\ell\in\mathbb{Z}$. Let $r=m-1$. Recall that $s_{m-1}=0$, thus $\sigma_{s_{m-1}}=0$. The parities of $s_i$, $0\leq i\leq m-2$, are $\sigma_{s_i}=(m-2-i+1)\pmod 2=\sigma_i$ (since $m-1$ is even). Further,

$$\begin{aligned}\alpha_{m-1}&=(-1)^{1+p^k+\cdots+p^{k(m-1)}}=(-1)^{\sigma_m}=-1,\\\beta_{m-1}&=\sum_{i=0}^{m-1}(-1)^{s_i+p^{ki}}=\sum_{i=0}^{m-2}(-1)^{s_i+p^{ki}}+(-1)^{s_{m-1}+p^{k(m-1)}}\\&=-1+\sum_{i=0}^{m-2}(-1)^{\sigma_{i+1}}=-1.\end{aligned}$$

Therefore, we conclude that the equation $z^{p^k}+z+1=0$ has a unique solution in $\mathbb{F}_{p^n}$. Thus, when $\frac{n}{\gcd(n,k)}$, then $F(x)=x^{p^k+1}$ is not $PcN$, for all $c\neq 1$ with $(1-c)^{p^k-1}=1$, and consequently, for all $c\neq 1$, given our previous argument.

*Case* 2. $m=\frac{n}{\gcd(n,k)}=2\ell$, for some $\ell\in\mathbb{Z}$. Let $r=m-1$. Recall that $s_{m-1}=0$, thus $\sigma_{s_{m-1}}=0$. The parities of $s_i$,

$0 \le i \le m-2$, are $\sigma_{s_i} = (m-2-i+1) \pmod 2 = \sigma_{i+1}$ (since $m-1$ is odd). Further,

$$\alpha_{m-1} = (-1)^{1+p^k+\cdots+p^{k(m-1)}} = (-1)^{\sigma_m} = 1,$$
$$\beta_{m-1} = \sum_{i=0}^{m-1}(-1)^{s_i+p^{ki}} = \sum_{i=0}^{m-2}(-1)^{s_i+p^{ki}} + (-1)^{s_{m-1}+p^{k(m-1)}}$$
$$= -1 + \sum_{i=0}^{m-2}(-1)^{\sigma_i} = 0.$$

Therefore, we infer that the equation $z^{p^k} + z + 1 = 0$ has $p^g$ solutions in $\mathbb{F}_{p^n}$. Thus, the initial Equation (4) has $p^g + 1$ solutions, and so, the $c$-differential uniformity in this case (under $(1-c)^{p^k-1} = 1$ and $\frac{n}{\gcd(n,k)}$ even) is at least $p^g+1$, where $g = \gcd(n,k)$.

Let us treat now the case of $d = (3^k+1)/2$ under $c = -1$, in $\mathbb{F}_{3^n}$. As used in [10], our function is $PcN$ if and only if the $c$-derivative $(x+1)^{\frac{3^k+1}{2}} - cx^{\frac{3^k+1}{2}}$ is a permutation polynomial if and only if $h_c(x) = (x-1)^{\frac{3^k+1}{2}} - c(x+1)^{\frac{3^k+1}{2}}$ is a permutation polynomial. Since $2|3^n-1$, for all $n$, then we can always write $x = y + y^{-1}$, for some $y \in \mathbb{F}_{3^n}$. Our condition (for general $c \neq 1$) becomes

$$\begin{aligned} h_c(x) &= (y+y^{-1}-1)^{\frac{3^k+1}{2}} - c(y+y^{-1}+1)^{\frac{3^k+1}{2}} \\ &= \frac{(y^2-y+1)^{\frac{3^k+1}{2}} - c(y^2+y+1)^{\frac{3^k+1}{2}}}{y^{\frac{3^k+1}{2}}} \\ &= \frac{(y+1)^{3^k+1} - c(y-1)^{3^k+1}}{y^{\frac{3^k+1}{2}}} \\ &= \frac{(1-c)y^{3^k+1} + (1+c)y^{3^k} + (1+c)y + (1-c)}{y^{\frac{3^k+1}{2}}} \\ &= (1-c)y^{\frac{3^k+1}{2}} + (1+c)y^{\frac{3^k-1}{2}} \\ &\qquad + (1+c)y^{\frac{-3^k+1}{2}} + (1-c)y^{\frac{-3^k-1}{2}} \\ &= (1-c)T_{\frac{3^k+1}{2}}(y) + (1+c)T_{\frac{3^k-1}{2}}(y) \end{aligned}$$

is a permutation polynomial ($T_\ell$ is the Chebyshev polynomial of the first kind). If $c = -1$, we obtain that $T_{\frac{3^k+1}{2}}(y)$ must be a permutation polynomial, and this is equivalent (by [16]) to the condition that $\gcd\left(\frac{3^k+1}{2}, 3^{2n}-1\right) = 1$. This last identity can be further simplified to $\gcd\left(3^k+1, 3^{2n}-1\right) = 2$. By Lemma 9 a necessary and sufficient condition for that to happen is for $\frac{2n}{\gcd(2n,k)}$ to be odd.

We now consider the function $F(x) = x^{10} - ux^6 - u^2x^2$ over $\mathbb{F}_{3^n}$. The equation ${}_cD_aF(x) = b$ becomes

$$\begin{aligned} &(1-c)x^{10} + ax^9 + u(c-1)x^6 + ua^3x^3 + u^2(c-1)x^2 \\ &\qquad + (a^9+au^2)x + a^{10} - ua^6 - u^2a^2 - b = 0. \end{aligned}$$

Taking $a = 0, b = (c-1)(u^2+u-1)$ the above equation will have solutions $x = 1, 2$, and so, ${}_c\Delta_F \ge 2$ (surely, one can take even nonzero values of $a$, in many instances, if not all; for example, for $c = 2$ and $u = 1$, we can take $a = b = 2$, rendering the solutions $x = 0, 1$). □

| n | Gold function, $k=2$ | Kasami function, $k=2$ |
|---|---|---|
| 1 | 2 | 2 |
| 2 | 4 | 4 |
| 3 | 3 | 3 |
| 4 | 5 | 5 |
| 5 | 3 | 3 |
| 6 | 5 | 5 |
| 7 | 3 | 3 |
| 8 | 5 | 5 |

TABLE I: Gold and Kasami functions, $k = 2$.

### A. *Some computational data*

Table 1 shows the maximal $c$-differential uniformity (for $a, c \neq 0$) for the Gold function $F(x) = x^{2^k+1}$ and the Kasami function $G(x) = x^{2^{2k}-2^k+1}$ over $\mathbb{F}_{2^n}$, for $k = 2$. Note that, for $k = 1$, these two functions are equal. The maximal $c$-differential uniformity (for $a, c \neq 0$), taking $k = 1$ for both functions, is equal to 2 for $n \ge 2$, and equal to 3 for $n \ge 3$, which can be argued theoretically. The cases $n = 1, 2$ are straightforward. Let $n \ge 3$. The $c$-derivative of $F(x) = x^3$ over $\mathbb{F}_{2^n}$ is

$${}_cD_1F(x) = (1+c)x^3 + x^2 + x + 1.$$

Taking $b = 1$, the equation ${}_cD_1F(x) = b$ is equivalent to $x((1+c)x^2 + x + 1) = 0$. This equation always has $x = 0$ as a solution, while the quadratic equation has two solutions if and only if $Tr(1+c) = 0$. Taking $c = \alpha^2 + \alpha + 1 \neq 0$ for $n \ge 3$, where $\alpha$ is a primitive root of $\mathbb{F}_{2^n}$, we obtain three solutions to the equation ${}_cD_aF(x) = b$, and therefore the maximal $c$-differential uniformity (for $c \neq 0$) for the Gold/Kasami function $F(x) = x^3$ over $\mathbb{F}_{2^n}$ is 3.

For $k = 2$ and $n \ge 3$, the results for the Gold and Kasami functions (respectively, $F(x) = x^5$ and $G(x) = x^{13}$) show a maximal $c$-differential uniformity (over $a, c \neq 0$) of 3 for $n$ odd (i.e. for $\gcd(n,k) = 1$), and of 5 for $n$ even. Note that, by Theorem 10$(ii)$, taking $p = 2$ and $n \equiv 0 \pmod 4$, the result is shown for the Gold function with $k = 2$, since, for these cases, the lower bound is 5, and, since the degree of the function is also 5, the $c$-differential uniformity must be exactly 5 for all $c$ such that $(1-c)^3 = 1$. Hence, the maximal $c$-differential uniformity (for $c \neq 0$) for the Gold function is 5, when $k = 2$. We simply double checked computationally (for small dimensions) our proof of Theorem 10$(ii)$. It would be interesting to prove theoretically whether our observations hold also for other dimensions, and for $x^{13}$, or perhaps, for the general Kasami functions.

Table II shows the maximal $c-$differential uniformity for the functions $F(x) = x^{10} \pm x^6 - x^2$ over $\mathbb{F}_{3^n}, c \in \mathbb{F}_{3^n} \setminus \{0, 1\}$. The tests indicate the following behaviour for both polynomials: The maximal $c$-differential uniformity (for $c \neq 0, 1$) is 2 if $n = 2$, $n+1$ for $n = 1, 3, 5$ and 10 for $n \ge 7, n$ odd. It would be nice to have a proof for the general case $x^{10} - ux^6 - u^2x^2, u \in \mathbb{F}_{3^n}$ especially showing that the maximal $c$-differential uniformity is 10 for $n \ge 7, u = \pm 1$ and to see the mathematical reason for jump from 6 to 10 in Table II.

| $n$ | $F(x)=x^{10}-x^6-x^2$ | $F(x)=x^{10}+x^6-x^2$ |
|---|---|---|
| 1 | 2 | 2 |
| 2 | 2 | 2 |
| 3 | 4 | 4 |
| 5 | 6 | 6 |
| 7 | 10 | 10 |
| 9 | 10 | 10 |
| 11 | 10 | 10 |

TABLE II: $F(x)=x^{10}\pm x^6-x^2$ over $\mathbb{F}_{3^n}, c\in\mathbb{F}_{3^n}\setminus\{0,1\}$.

## V. $c$-DIFFERENTIAL UNIFORMITY FOR THE INVERSE FUNCTION

Since there has been quite a bit of effort to investigate the inverse function over $\mathbb{F}_{2^n}$ as it is relevant in Rijndael and Advance Encryption Standard, it is natural to wonder how it behaves with respect to $c$-differential uniformity. We will need the following lemma (see [2], for the first part; the second part is probably known and easy to derive by completing the square in the given quadratic equation, that is, writing $(2ax+b)^2 = a^2-4b$).

**Lemma 11.** *Let $n$ be a positive integer. We have:*

- $(i)$ *The equation $x^2+ax+b=0$, with $a,b\in\mathbb{F}_{2^n}$, $a\neq 0$, has two solutions in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{b}{a^2}\right)=0$, and zero solutions otherwise.*
- $(ii)$ *The equation $x^2+ax+b=0$, with $a,b\in\mathbb{F}_{p^n}$, $p$ odd, has (two, respectively, one) solutions in $\mathbb{F}_{p^n}$ if and only if the discriminant $a^2-4b$ is a (nonzero, respectively, zero) square in $\mathbb{F}_{p^n}$.*

### A. The inverse function in even characteristic

We first treat the even characteristic.

**Theorem 12.** *Let $n$ be a positive integer, $1\neq c\in\mathbb{F}_{2^n}$ and $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be the inverse function defined by $F(x)=x^{2^n-2}$. We have:*

- $(i)$ *If $c=0$, then $F$ is PcN (that is, $F$ is a permutation polynomial).*
- $(ii)$ *If $c\neq 0$ and $\mathrm{Tr}_n(c)=\mathrm{Tr}_n(1/c)=1$, the $c$-differential uniformity of $F$ is $2$ (and hence $F$ is APcN).*
- $(iii)$ *If $c\neq 0$ and $\mathrm{Tr}_n(1/c)=0$, or $\mathrm{Tr}_n(c)=0$, the $c$-differential uniformity of $F$ is $3$.*

*Proof.* We start with the $c$-differential uniformity equation at $a$, namely, $(x+a)^{2^n-2}+cx^{2^n-2}=b$.

If $c=0$, we have at most one solution for the $c$-differential equation, since then the above $c$-differential uniformity equation becomes $(x+a)^{2^n-2}=b$. If $b=0$, then $x=a$ is the only solution, otherwise, multiplying by $x+a$, we get $b(x+a)=1$, which has also only one solution. The proof of $(i)$ is done.

So, next, we may assume $c\neq 0$. If $a=0$, the equation becomes $(1+c)x^{2^n-2}=b$. If $b=0$, then $x=0$ is the only solution. If $b\neq 0$ (so $x\neq 0$), multiplying by $x$, the equation becomes $1+c=bx$, which has only one solution.

We next assume that $c\neq 0, a\neq 0$. Recall that, if $F(x)=x^d$ and $a\neq 0$, then ${}_c\Delta_F(a,b)={}_c\Delta_F(1,b/a^d)$, so we can look at the equation

$$(x+1)^{2^n-2}+cx^{2^n-2}=b. \qquad (5)$$

If $b=0$, we easily get only one solution, since the above equation is equivalent to $c(x+1)=x$, so we may assume below that $b\neq 0$.

*Case* 1. Let $b=1\neq c$. Then $x=0$ is a solution of (5). Assume now that $x\neq 0,1$ (certainly, $x=1$ is not a solution). Multiplying (5) by $x(x+1)$ we get $x+c(x+1)=x(x+1)$, which is equivalent to $x^2+cx+c=0$. By Lemma 11$(i)$, this equation has two solutions (we would have only one solution if $c=0$) if and only if $\mathrm{Tr}_n(1/c)=0$. Thus, altogether, we have three solutions for (5) under $\mathrm{Tr}_n(1/c)=0$. If $\mathrm{Tr}_n(1/c)=1$, then (5) has only the solution $x=0$.

*Case* 2. Let $b=c\neq 0,1$. Certainly, $x=1$ is a solution of (5), while $x=0$ is not a solution, so we assume now that $x\neq 0,1$. Again, multiplying (5) by $x(x+1)$ we get $x+c(x+1)=cx(x+1)$, which is equivalent to $x^2+c^{-1}x+1=0$, which has two solutions if and only if $\mathrm{Tr}_n\left(1/c^{-2}\right)=\mathrm{Tr}_n(c^2)=\mathrm{Tr}(c)=0$. Thus, altogether, we have three solutions for (5) under $\mathrm{Tr}_n(c)=0$.

*Case* 3. Let $b\neq 1,c$ (so, $x\neq 0,1$). Multiplying (5) by $x(x+1)$ we get $x+c(x+1)=bx(x+1)$, which has a unique solution if $b=0$, $c\neq 1$; otherwise, Equation (5) is equivalent to $x^2+\left(\frac{b+c+1}{b}\right)x+\frac{c}{b}=0$. If $b=c+1$, then we have a unique solution, otherwise we have two solutions if and only if $\mathrm{Tr}_n\left(\frac{bc}{b^2+c^2+1}\right)=0$. As we saw, it will be enough to consider the case of $\mathrm{Tr}_n(c)=\mathrm{Tr}_n(1/c)=1$, since otherwise, we have three solutions for some $b$. Below, we argue that we always can find some $b\neq 0$ for which this last trace, $\mathrm{Tr}_n\left(\frac{bc}{b^2+c^2+1}\right)=0$.

If $n$ is odd, then we claim that there exists some value of $u$ such that

$$\frac{uc}{u^2+c^2+1}=\frac{c+1}{c}=1+\frac{1}{c},$$

which follows from the fact that this last equation is equivalent to $(c+1)u^2+c^2u+(c+1)^2=0$, that is, $u^2+\frac{c^2}{c+1}u+(c+1)^2=0$, which, by Lemma 11$(i)$, has solutions if and only if $0=\mathrm{Tr}_n\left(\frac{(c+1)^2}{c^4/(c+1)^2}\right)=\mathrm{Tr}_n\left(\frac{(c+1)^4}{c^4}\right)=\mathrm{Tr}_n\left(\frac{c+1}{c}\right)=\mathrm{Tr}_n\left(1+\frac{1}{c}\right)$. Since $\mathrm{Tr}_n(1/c)=1$ and $n$ is odd (thus, $\mathrm{Tr}_n(1)=1$), then $\mathrm{Tr}_n\left(1+\frac{1}{c}\right)=0$. Taking $b=u$ such solution, then the condition $\mathrm{Tr}_n\left(\frac{bc}{b^2+c^2+1}\right)=0$ will hold and consequently, we have two roots of the $c$-differential equation in this case.

We now let $n$ be even and consider the equation $\dfrac{uc}{u^2+c^2+1}=1+c+\dfrac{1}{c}$, which is equivalent to $u^2+\dfrac{c^2}{c^2+c+1}u+(c+1)^2=0$. This last equation has solutions (by Lemma 11$(i)$) if and only if $0=\mathrm{Tr}_n\left(\frac{(c+1)^2}{c^4/(c^2+c+1)^2}\right)=\mathrm{Tr}_n\left(\frac{(c+1)}{c^2/(c^2+c+1)}\right)=\mathrm{Tr}_n\left(\frac{(c+1)(c^2+c+1)}{c^2}\right)=\mathrm{Tr}_n\left(\frac{c^3+1}{c^2}\right)=\mathrm{Tr}_n(c)+\mathrm{Tr}_n(1/c^2)=\mathrm{Tr}_n(c)+\mathrm{Tr}_n(1/c)=0$, which will certainly happen. By taking $b$ to be equal to such a solution $u$, then, $\mathrm{Tr}_n\left(\frac{bc}{b^2+c^2+1}\right)=\mathrm{Tr}_n(1+c+1/c)=0$, and consequently, the $c$-differential equation will have two solutions. □

### B. The inverse function in odd characteristic

We now treat the case of the inverse for odd characteristic. We use the notation $[A]^2$ to denote the squares in any set $A$.

**Theorem 13.** *Let $p$ be an odd prime, $n \geq 1$ be a positive integer, $1 \neq c \in \mathbb{F}_{p^n}$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the inverse $p$-ary function defined by $F(x) = x^{p^n-2}$. We have:*

$(i)$ *If $c = 0$, then $F$ is PcN (that is, $F$ is a permutation polynomial).*
$(ii)$ *If $c \neq 0, 4, 4^{-1}$, $(c^2-4c) \in [\mathbb{F}_{p^n}]^2$, or $(1-4c) \in [\mathbb{F}_{p^n}]^2$, the $c$-differential uniformity of $F$ is $3$.*
$(iii)$ *If $c = 4, 4^{-1}$, the $c$-differential uniformity of $F$ is $2$ (and hence $F$ is APcN).*
$(iv)$ *If $c \neq 0$, $(c^2-4c) \notin [\mathbb{F}_{p^n}]^2$ and $(1-4c) \notin [\mathbb{F}_{p^n}]^2$, the $c$-differential uniformity of $F$ is $2$ (and hence $F$ is APcN).*

*Proof.* The proof for $(i)$ ($c = 0$, as well as $a = 0$) is similar to the one for characteristic 2.

We next assume that $c \neq 0$. For $a = 0$, as in the case of even characteristic, the corresponding equation $(x+a)^{p^n-2} - cx^{p^n-2} = b$ has one solution. We assume now that $a \neq 0$. As in characteristic 2, we only need to investigate the equation

$$(x+1)^{p^n-2} - cx^{p^n-2} = b. \tag{6}$$

If $b = 0$, we easily get only one solution, so we may assume below that $b \neq 0$.

*Case* 1. Let $b = 1 \neq c$. Then $x = 0$ is a solution of (6). Assume now that $x \neq 0$ (also, $x \neq -1$, since then, $1 = b = c$, which is impossible). Multiplying (6) by $x(x+1)$ we get $x - c(x+1) = x(x+1)$, which is equivalent to $x^2+cx+c = 0$. By Lemma 11$(ii)$, this equation has solutions if and only if the discriminant $D_1 = c^2-4c \in [\mathbb{F}_{p^n}]^2$ (that is, $D_1$ is a square in $\mathbb{F}_{p^n}$); we have two solutions if $D_1 \neq 0$ and one solution if $D_1 = 0$. Thus, altogether, we have three solutions for (6) if $0 \neq D_1 \in [\mathbb{F}_{p^n}]^2$. If $D_1 = 0$ (that is, $c = 4$; we operate under $c \neq 0$), then (6) has only the solutions $x = -2$ and the prior $x = 0$.

*Case* 2. Let $b = c \neq 0, 1$. Now, $x = -1$ is a solution of (6), so we next assume that $x \neq -1$ (also, $x \neq 0$, since this is not a solution unless $c = 1$, which is impossible) . Multiplying (6) by $x(x+1)$ we get $x - c(x+1) = cx(x+1)$, which is equivalent to $x^2+(2-c^{-1})x+1 = 0$, which, by Lemma 11$(ii)$ has two (respectively, one) solutions if and only if $D_2 = (2-c^{-1})^2 - 4 = (1-4c)c^{-2} \in [\mathbb{F}_{p^n}]^2$ and $D_2 \neq 0$ (respectively, $D_2 = 0$). Thus, altogether, we have three solutions for (6) under $0 \neq 1-4c \in [\mathbb{F}_{p^n}]^2$ and two solutions if $c = 4^{-1}$.

*Case* 3. Let $c \neq b \neq 0, 1$ (so, $x \neq 0, -1$). Multiplying (6) by $x(x+1)$ we get $x - c(x+1) = bx(x+1)$, that is, $x^2 + \left(\frac{b+c-1}{b}\right)x + \frac{c}{b} = 0$. If $D_3 = \left(\frac{b+c-1}{b}\right)^2 - 4\frac{c}{b} = 0$, that is, $(b+c-1)^2 = 4bc$, then we have a unique solution, otherwise, we have two solutions if and only if $0 \neq D_3 \in [\mathbb{F}_{p^n}]^2$, that is, $0 \neq (b+c-1)^2 - 4bc \in [\mathbb{F}_{p^n}]^2$.

Below, we argue that we always can find some $b \neq 0, 1, c$ for which $(b+c-1)^2 - 4bc \in \left[\mathbb{F}_{p^n}^*\right]^2$, except for $c = -1$, $p = 3$, $n = 2$, where, we can only find some values of $b$ for which $(b+c-1)^2 - 4bc = 0$.

If $c \neq -2, 2, 4$, then we can take $b = 2^{-1}(c-2)$ and consequently, $b \neq 0, 1, c$, and

$$(b+c-1)^2 - 4bc = 2^{-2}(c-4)^2 \neq 0.$$

If $c = 2$, or $c = 4$, and $p \neq 3, 5$, then, we can take $b = 2(c+1)$, and $b \neq 0, 1, c$, and

$$(b+c-1)^2 - 4bc = (1-c)^2 \neq 0.$$

Let $c = 2$, and $p = 3$. Then, $(b+c-1)^2 - 4bc = b^2+1$. If $n > 2$, then we can take $b = \alpha - \alpha^{-1}$, where $\alpha$ is a primitive root of $\mathbb{F}_{3^n}$ (we here avoid the primitive polynomials $x^2 \pm x - 1 = 0$ over $\mathbb{F}_3$, since then, $b \in \{-1, 1\}$). Consequently, $b \neq 0, 1, -1$, and

$$b^2 + 1 = (\alpha + \alpha^{-1})^2 \neq 0.$$

Equation (6) has then, in this case, two or fewer solutions. If $n = 2$, then, we write $\mathbb{F}_{3^2} = \frac{\mathbb{F}_3[x]}{\langle x^2-x-1\rangle} = \mathbb{F}_3(\alpha)$, where $\alpha$ is a root of the primitive polynomial $x^2 - x - 1 = 0$. Note that (recall Case 1) $D_1 = 2^2 - 4\cdot 2 = -4 = 2 = (\alpha+1)^2 \in [\mathbb{F}_{3^n}]^2 \neq 0$. Since, if $b \neq 0, 1, c$, Equation (6) cannot have more than two solutions, we conclude that the $c$-differential uniformity is 3.

Let $c = 2$, and $p = 5$. Then, $C_1 = c^2 - 2c = -4 = 1 = 1^2 \in [\mathbb{F}_{5^n}]^2 \neq 0$. Since, if $b \neq 0, 1, c$, Equation (6) cannot have more than two solutions, the $c$-differential uniformity is 3 in this case.

If $c = 4$, and $p = 3$, then $c = 1$, which is a contradiction with $c \neq 1$.

Let $c = 4$ and $p = 5$. Then, $(b+c-1)^2 - 4bc = b^2 + 4$. If $n > 2$, then, as before, we can take $b = \alpha - \alpha^{-1}$, where $\alpha$ is a primitive root of $\mathbb{F}_{5^n}$, and consequently, $b \neq 0, 1, -1$, and

$$(b-2)^2 + 4b = b^2 + 4 = (\alpha + \alpha^{-1})^2 \neq 0.$$

If $n = 2$, then, we write $\mathbb{F}_{5^2} = \frac{\mathbb{F}_5[x]}{\langle x^2-x+2\rangle} = \mathbb{F}_5(\alpha)$, where $\alpha$ is a root of the primitive polynomial $x^2 - x + 2 = 0$. Taking $b = \alpha + 3 \neq 0, 1, -1$, then (recall that $\alpha^2 - \alpha + 2 - 0$)

$$(b-2)^2 + 4b = (2\alpha+2)^2 \neq 0.$$

Let now $c = -2$. Note that, then $D_2 = \left(\frac{3}{2}\right)^2 \in [\mathbb{F}_{p^n}]^2$. Furthermore, for $p \neq 3$, $D_2 \neq 0$, rendering at least three solutions of (6) for $p \neq 3$. If $p = 3$, $c = -2 = 1$, which is excluded from this theorem, since it is covered by the classical results.

Note that, by Cases 1, 2 and 3, Equation (6) cannot have more than three solutions, so the $c$-differential uniformity is always at most 3.

The proof of the theorem is done. □

**Acknowledgement.** The authors are grateful to the Assoc. Edit. Sihem Mesnager and the three anonymous reviewers for their valuable and constructive comments which have improved the manuscript.

## REFERENCES

[1] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, *On almost perfect nonlinear functions* IEEE Trans. Inf. Theory 52:9 (2006), 4160–4170.
[2] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10 (1967), 553–564.
[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds) Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science, vol 2365. Springer, Berlin, Heidelberg, 2002.
[4] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[5] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[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] C. Carlet, *Characterizations of the Differential Uniformity of Vectorial Functions by the Walsh Transform*, IEEE Trans. Inf. Theory 64:9 (2018), 6443–6453.

[8] C. Carlet, *On APN exponents, characterizations of differentially uniform functions by the Walsh transform, and related cyclic-difference-set-like structures*, Des. Codes Cryptogr. 87:2-3 (2019), 203–224.

[9] F. Chabaud, S. Vaudenay, *Links between differential and linear cryptanalysis*, In: Adv. in Crypt – EUROCRYPT' 94, LNCS 950, pp. 356–365, 1995.

[10] R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.

[11] R. S. Coulter, R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class* II, Des. Codes Cryptogr. 10 (1997), 167–184.

[12] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[13] C. Ding, J. Yuan, *A new family of skew Paley-Hadamard difference sets*, J. Comb. Theory Ser. A 113 (2006), 1526–1535.

[14] J. Liang, *On the solutions of trinomial equations over finite fields*, Bull. Cal. Math. Soc. 70 (1978), 379–382.

[15] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[16] W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. 231 (1968), 215–219.

[17] L. Rónyai, T. Szönyi, *Planar functions over finite fields*, Combinatorica 9:3 (1989), 315–320.

[18] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.

[19] M. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. 75 (2015), 71–80.



**Pål Ellingsen** has a Master's degree in Mathematics from the University of Tromsø, Norway in 1995 and a Ph.D. in Informatics from the University of Bergen, Norway in 2005. He is currently an Associate Professor at Western Norway University of Applied Sciences in Bergen, Norway. His research interests are Cyber Security, Secure Coding Cryptology, and Coding Theory.

**Patrick Felke** received his Master of Science in Mathematics degree in 2001 from TU Dortmund University, Germany. He completed his Ph.D. in Mathematics at Ruhr University Bochum, Germany in 2005. Currently, he is a Professor for IT-Security at the University of Applied Sciences Emden/Leer, in Emden, Germany. His research interests are in Cryptology, Sequence Design, Coding Theory, Random Number Generation, Protocol and Computer Security.

**Constanza Riera** received her Master of Science degree in 2002 from Autonomous University of Madrid, Spain. She completed her Ph.D. in Mathematics at Complutense University of Madrid, Spain in 2006. Currently, she is an Associate Professor at Western Norway University of Applied Sciences in Bergen, Norway. Her research interests are Cryptology, Sequence Design, Coding Theory and Quantum Communications.

**Pantelimon Stănică** received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Coding Theory, Sequence Design, Number Theory and Discrete Mathematics.

**Anton Tkachenko** received his Master of Science degree in 2017 from Beijing University of Chemical Technology, China. Currently, he is a PhD student at Western Norway University of Applied Sciences in Bergen, Norway. His research interests are Quantum Cryptology and Computation, Quantum Control Theory.