

Low c -differential uniformity for functions modified on subfields

Daniele Bartoli¹, Marco Calderini², Constanza Riera³,
Pantelimon Stănică⁴

¹ Department of Mathematics and Informatics, University of Perugia,
Via Vanvitelli, 1, 06123, Perugia;

`daniele.bartoli@unipg.it`

² Department of Informatics, University of Bergen
Postboks 7803, N-5020, Bergen, Norway;

`Marco.Calderini@uib.no`

³Department of Computer Science,
Electrical Engineering and Mathematical Sciences,
Western Norway University of Applied Sciences,
5020 Bergen, Norway; `csr@hvl.no`

⁴Applied Mathematics Department,

Naval Postgraduate School,
Monterey, CA 93943, USA; `pstanica@nps.edu`

Abstract

In this work, we will extend the results of Calderini (2021) on the differential uniformity of some piecewise functions to the case of the c -differential uniformity, recently introduced by Ellingsen et al. (2020). From this generalization, we are also able to improve the upper bound obtained by Stanica (2021) for the case of a Gold APN function in even characteristic modified on a subfield.

1 Introduction

Let p be a prime number and n be a positive integer n . We let \mathbb{F}_{p^n} be the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ be its multiplicative group.

We call a function from \mathbb{F}_{p^n} (or \mathbb{F}_p^n) to \mathbb{F}_p a p -ary function on n variables. For positive integers n and m , any map $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \rightarrow \mathbb{F}_p^m$) is called a *vectorial p -ary function*, or an (n, m) -function. When $m = n$, F can be uniquely represented as a univariate polynomial over \mathbb{F}_{p^n} of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$, $a_i \in \mathbb{F}_{p^n}$, whose *algebraic degree* is then the largest weight in the p -ary expansion of i (that is, the sum of the digits of the exponents i with $a_i \neq 0$).

Motivated by [3], who extended the differential attack on some ciphers by using a new type of differential, in [6], the authors introduced a new differential and Difference Distribution Table, in any characteristic, along with the corresponding perfect/almost perfect c -nonlinear functions (this was also developed independently in [2] where the authors introduce the concept of quasi planarity) and other notions. In [1, 6, 8, 9] various characterizations of the c -differential uniformity were found, and some of the known perfect and almost perfect nonlinear functions were investigated and constructions were proposed.

For a p -ary (n, m) -function $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^m}$, 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

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

For an (n, n) -function F , and $a, b \in \mathbb{F}_{p^n}$, we let the entries of the c -Difference Distribution Table (c -DDT) be defined by ${}_c \Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$. We call the quantity

$$\delta_{F,c} = \max \{ {}_c \Delta_F(a, b) : a, b \in \mathbb{F}_{p^n}, \text{ and } a \neq 0 \text{ if } c = 1 \}$$

the c -differential uniformity of F . If $\delta_{F,c} = \delta$, then we say that F is differentially (c, δ) -uniform (or that F has c -uniformity δ). 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, as proven in [6], there exist PcN functions for $p = 2$, for all $c \neq 1$). 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, $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$, then F is PcN if and only if ${}_c D_a F$ is a permutation polynomial. For $c = 1$, we recover the classical derivative, PN, APN, differential uniformity and DDT. In the last years, several constructions of low differentially uniform permutations have been introduced by modifying some functions on a subfield (see, for instance, [4, 7, 11, 12]).

In this work we will extend some of the results given in [4] to the case of the c -differential uniformity. From this generalization we are also able to improve the upper bound obtained in [10] for the case of a Gold APN function in even characteristic.

2 Some low c -differential uniform functions and upper bounds on the differential uniformity of piecewise functions

Here, we shall give a general result concerning an upper bound for the c -differential uniformity of a piecewise function, thus generalizing a result of [4].

Before considering the case of the c -differential uniformity, we will give a property for some functions having $\delta_{F,1} = 4$ when $p = 2$. This permits to extend the results given in [4] also to the case of the Kasami function.

Proposition 1. *Let $n = sm$, with m odd, and let $F \in \mathbb{F}_{2^s}[x]$ be a 4-uniform function over \mathbb{F}_{2^n} . Then, $F(x + a) + F(x) = b$ does not admit solution $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$, whenever $a, b \in \mathbb{F}_{2^s}$.*

Remark 2. *In [5], a similar result was obtained for the case of APN functions.*

From Proposition 1 we have that all the results given in [4] for the Gold and Bracken-Leander functions can be extended to other functions, such as the Kasami function. Indeed, the assumption on the solutions of the derivatives of the modified function is needed for applying Theorem 4.1 in [4]. In particular, we have the following result.

Theorem 3. *Let $n = sm$ with s even such that $s/2$ and m are odd. Let k be such that $\gcd(k, n) = 2$ and $f(x) = A_1 \circ \text{Inv} \circ A_2(x)$, where $\text{Inv}(x) = x^{-1}$ and A_1, A_2 are affine permutations over \mathbb{F}_{2^s} . Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k-2^k+1}})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k-2^k+1}} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over \mathbb{F}_{2^n} . Moreover, if $s > 2$ then the algebraic degree of F is $n - 1$. Moreover, the nonlinearity of F is at least $2^{n-1} - 2^{\frac{s}{2}+1} - 2^{\frac{n}{2}}$.

Here, we shall give a general result concerning an upper bound for the c -differential uniformity of a piecewise function, thus generalizing a result of [4]. In particular, Theorem 4.1 in [4] can be extended to the case of p -ary functions and $c \neq 1$. In the following result, we do not request any condition on the solutions of the derivatives of our functions.

Theorem 4. *Let p is a prime, $n > 2$ be an integer, s be a divisor of n , $1 \neq c \in \mathbb{F}_{p^n}$ fixed, and $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a p -ary (n, n) -function defined by*

$$F(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{p^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s, s) -function of c' -differential uniformity $\delta_{f,c'}$ (for all c') and $g \in \mathbb{F}_{p^s}[x]$ is an (n, n) -function of c' -differential uniformity $\delta_{g,c'}$ (for all c'). Then, the c -differential uniformity of F is

$$\delta_{F,c} \leq \begin{cases} \delta_{f,0} + \delta_{g,0}, & \text{if } c = 0, \\ \max \{ \delta_{f,c_1} + \delta_{g,c}, \delta_{g,c} + 2p^s \delta_{g,0} \}, & \text{if } c \neq 0, \end{cases}$$

where $c = \sum_{i=1}^m c_i g_i$, with $c_i \in \mathbb{F}_{p^s}$ and $\{g_1 = 1, g_2, \dots, g_m\}$ is a basis of the extension \mathbb{F}_{p^n} over \mathbb{F}_{p^s} .

If we introduce some extra conditions on the solutions of the derivatives of the function g , we can obtain another upper bound on the c -differential uniformity of the modified function.

Theorem 5. *Let p be a prime, $n > 2$ be an integer, s be a divisor of n , $1 \neq c \in \mathbb{F}_{p^s}$ fixed, and $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a p -ary (n, n) -function defined by*

$$F(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{p^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s, s) -function of c -differential uniformity $\delta_{f,c}$ and $g \in \mathbb{F}_{p^s}[x]$ is an (n, n) -function of c -differential uniformity, $\delta_{g,c}$. Suppose that:

(H1) for any $a \in \mathbb{F}_{p^s}^*$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x+a) - g(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.

(H2) for any $a \in \mathbb{F}_{p^s}$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x+a) - cg(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.

Then, the c -differential uniformity of F is

$${}_c\Delta_F(a, b) \leq \begin{cases} \max \{ \delta_{f,c}, \delta_{g,c} \} & \text{if } a \in \mathbb{F}_{p^s} \\ \delta_{g,c} + 2 \cdot \delta_{g,0} & \text{if } a \notin \mathbb{F}_{p^s}. \end{cases}$$

Remark 6. *Removing condition (H2) in Theorem 5 would yield*

$${}_c\Delta_F(a, b) \leq \begin{cases} \delta_{f,c} + \delta_{g,c} & \text{if } a \in \mathbb{F}_{p^s} \\ \delta_{g,c} + 2 \cdot \delta_{g,0} & \text{if } a \notin \mathbb{F}_{p^s}. \end{cases}$$

Moreover, if g permutes \mathbb{F}_{p^s} then we have also that $\delta_{g,0} = 1$.

For a Gold-like function defined over \mathbb{F}_{2^n} , we can observe the following.

Proposition 7. *Let $n = sm$, with n/s odd. For a Gold-like function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = t$ and $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$, we have that*

$$g(x+a) + g(x) = b$$

does not admit solutions in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$, whenever $a \in \mathbb{F}_{2^s}^*$ and $b \in \mathbb{F}_{2^s}$.

Theorem 8. *Let $n = sm$, with n/s odd. For a Gold-like function $g(x) = x^{2^k+1}$, with $\gcd(n, k) = t$, $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$, and n/t odd, we have that, for any fixed $\alpha \in \mathbb{F}_{2^s}^*$, $G(x) = x^{2^k+1} + \alpha(x^{2^s} + x)^{2^n-1} + \alpha$ is such that $\delta_{G,c} \leq 3$, for any $c \in \mathbb{F}_{2^t} \setminus \{1\}$.*

The c -differential uniformity of a Gold-like function $g(x) = x^{2^k+1}$ has been characterized in [9, Theorem 4]. In particular, for $c \neq 1$ we have $\delta_{g,c} \leq 2^{\gcd(k,n)} + 1$. From this, and from Remark 6 we have the following result.

Theorem 9. *Let $n = sm$, with n odd. For a Gold function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = 1$, we have that for any fixed $\alpha \in \mathbb{F}_{2^s}^*$, $G(x) = x^{2^k+1} + \alpha + \alpha(x^{2^s} + x)^{2^n-1}$ is such that $\delta_{G,c} \leq 6$, for any $c \in \mathbb{F}_{2^s} \setminus \{1\}$.*

Remark 10. *Theorem 9 improves (when c is restricted to the subfield \mathbb{F}_{2^s}) the upper bound obtained in [10], where the author studied the modified Gold function, with no restriction on the element c , and obtained that $\delta_{G,c} \leq 9$.*

3 Concatenating functions with low c -differential uniformity

In this section we will show how it is possible to obtain a function over \mathbb{F}_{q^n} , with low c -differential uniformity, concatenating n functions defined over \mathbb{F}_q .

Let $\{\beta_1, \dots, \beta_n\}$ be a basis of \mathbb{F}_{q^n} as vector space over \mathbb{F}_q . Let $A = (a_{ij})_{i,j} = (\beta_i^{q^j-1})$. The matrix A is non-singular, so we can define $A^{-1} = (a'_{i,j})_{i,j}$. Let us denote by e_k the column vector whose entries are all zeros but one in position k , for $1 \leq k \leq n$. We define the linear polynomial $L_k(x) = \sum_{i=1}^n a'_{i,k} x^{q^i-1} = (x, x^q, \dots, x^{q^{n-1}}) \cdot A^{-1} \cdot e_k$.

Any element $x \in \mathbb{F}_{q^n}$ can be written as $x = \beta_1 x_1 + \dots + \beta_n x_n$, with $x_i \in \mathbb{F}_q$. Thus, we have $L_k(x) = x_k$. That is, L_k is the projection on the k -th component of x . So we obtain the following result.

Theorem 11. *Let $c \in \mathbb{F}_q \setminus \{1\}$ and let f_1, \dots, f_n be n functions over \mathbb{F}_q with c -differential uniformity $\delta_1, \dots, \delta_n$, respectively. Let β_1, \dots, β_n , L_k be defined as before. Then $F(x) = \sum_{k=1}^n \beta_k f_k(L_k(x))$ has c -differential uniformity equal to $\prod_{i=1}^n \delta_i$.*

We can construct a PcN function over \mathbb{F}_{q^n} from n PcN functions over \mathbb{F}_q .

Corollary 12. *Let $c \in \mathbb{F}_q \setminus \{1\}$ and let f_1, \dots, f_n be n functions over \mathbb{F}_q that are PcN. Then $F(x) = \sum_{k=1}^n \beta_k f_k(L_k(x))$ is PcN.*

References

- [1] D. Bartoli, M. Calderini, *On construction and (non)existence of c -(almost) perfect nonlinear functions*, Finite Fields Appl. 72 (2021), <https://doi.org/10.1016/j.ffa.2021.101835>.
- [2] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020), 187–213.
- [3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.), Fast Software Encryption, FSE 2002, LNCS 2365, pp. 17–33, Springer, Berlin, Heidelberg, 2002.
- [4] M. Calderini, *Differentially low uniform permutations from known 4-uniform functions*, Des. Codes Cryptogr. 89 (2021), 33–52.
- [5] C. Carlet, *Revisiting some results on APN and algebraic immune functions*, ePrint, 2021.

- [6] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.
- [7] J. Peng, C. H. Tan, *New differentially 4-uniform permutations by modifying the inverse function on subfields*, Cryptogr. Commun. 9 (2017), 363–378.
- [8] S.U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.
- [9] S. Mesnager, C. Riera, P. Stanica, H. Yan, Z. Zhou, *Investigations on c-(almost) perfect nonlinear functions*, <https://arxiv.org/pdf/2010.10023.pdf>, 2021.
- [10] P. Stănică, *Low c-differential uniformity for the Gold function modified on a subfield*, Proceedings ICSP 2020, Springer LNEE 744 (2021), pp. 131–137, https://doi.org/10.1007/978-981-33-6781-4_11.
- [11] G. Xu, and L. Qu, *Two classes of differentially 4-uniform permutations over \mathbb{F}_{2^n} with n even*. Adv. Math. Communic. 14:1 (2019), 97–110.
- [12] Z. Zha, L. Hu, S. Sun, *Constructing new differentially 4-uniform permutations from the inverse function*, Finite Fields Appl. 25 (2014), 64–78.