# Investigations of *c*-Differential Uniformity of Permutations with Carlitz Rank 3

Jaeseong Jeong<sup>1</sup>, Namhun Koo<sup>2</sup>, Soonhak Kwon<sup>1</sup>

Email: wotjd012321@naver.com, nhkoo@ewha.ac.kr, shkwon@skku.edu

<sup>1</sup>Applied Algebra and Optimization Research Center, Sungkyunkwan University, Suwon, Korea <sup>2</sup>Institute of Mathematical Sciences, Ewha Womans University, Seoul, Korea

February 7, 2022

#### Abstract

The c-differential uniformity is recently proposed to reflect resistance against some variants of differential attack. Finding functions with low c-differential uniformity is attracting attention from many researchers. For even characteristic, it is known that permutations of low Carlitz rank have good cryptographic parameters, for example, low differential uniformity, high nonlinearity, etc. In this paper we show that permutations with low Carlitz rank have low c-differential uniformity. We also investigate c-differential uniformity of permutations with Carlitz rank 3 in detail.

Keywords. c-Differential Uniformity, Carlitz rank, Permutation,

Mathematics Subject Classification(2020) 94A60, 06E30

### 1 Introduction

Functions with good cryptographic parameters have many applications in cryptographic purpose. Very recently, Ellinsen et. al. [7] proposed a new cryptographic parameter, c-differential uniformity, which is useful to measure the resistance against some variants of differential attack [4]. Functions with low c-differential uniformity are resistant against differential attacks of this type. Finding functions with low c-differential uniformity has been a good research topic to many researchers, and many classes of functions with low c-differential uniformity were proposed. [2,3,8,16,19–26] It is known [16] that some functions of low differential uniformity have high c-differential uniformity. Hence it is also important to investigate c-differential uniformity of known functions with low differential uniformity.

For even characteristic, some cryptographic properties of permutations of low Carlitz rank have been investigated in several researches, and we can see that they have good cryptographic parameters. For example, the multiplicative inverse function of Carlitz rank 1 has low differential uniformity [17], high nonlinearity [12], low boomerang uniformity [5], low differential-linear uniformity [6], low *c*differential uniformity [7], and low *c*-boomerang uniformity [18]. Furthermore, it is used as the S-box of the AES(Advanced Encryption Standard) cryptosystem. Cryptographic parameters of permutations of Carlitz rank 2 also have been widely investigated. It is known that they have low differential uniformity [14], high nonlinearity [14], low boomerang uniformity [13], low differentiallinear uniformity [10], low c-differential uniformity [19], and low c-boomerang uniformity [19]. Several classes of differentially 4-uniform involutions with low Carlitz rank were proposed in [11].

Permutations with Carlitz rank 3 also have good cryptographic parameters, for example, high nonliearity [14], and low differential-uniformity [10]. Differentially 4-uniform permutations with Carlitz rank 3 are characterized in [9,14]. The boomerang uniformities of permutations with Carlitz rank 3 were investigated in [9]. Permutations with low Carlitz rank are known to have low differential uniformity, but it does not imply low c-differential uniformity as mentioned above.

In this paper, we show that for binary finite fields the *c*-differential uniformity of permutations with Carlitz rank *m* is upper bounded by m+2 with  $c \neq 1$ . Furthermore, we investigate *c*-differential uniformity of permutations of Carlitz rank 3 in detail.

The rest of this paper is organized as follows. In section 2, we introduce some basic preliminaries and previous results which are necessary in subsequent sections. In section 3, we propose an upper bound of c-differential uniformity depending on Carlitz rank of given permutation. We investigate cdifferential uniformity of permutations with Carlitz rank 3 in section 4. Finally we give the concluding remark in Section 5.

### 2 Preliminaries

We only consider the even characteristic case. Throughout this paper, we let :

- $\mathbb{F}_{2^n}$  be the finite field of  $2^n$  elements and  $\mathbb{F}_{2^n}^*$  be the multiplicative group of  $\mathbb{F}_{2^n}$
- Tr :  $\mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$  be the field trace from  $\mathbb{F}_{2^n}$  onto  $\mathbb{F}_2$  given by  $\operatorname{Tr}(x) = x + x^2 + x^{2^2} + \dots + x^{2^{n-1}}$
- Inv be the multiplicative inverse function on  $\mathbb{F}_{2^n}$ , and  $x^{-1} = Inv(x)$  for all  $x \in \mathbb{F}_{2^n}^*$  and  $0^{-1} = 0$

Next we introduce *c*-differential uniformity which is the subject of this paper.

**Definition 2.1.** ([7]) Let  $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$  be a function and  $c \in \mathbb{F}_{2^n}$ . (i) We denote the c-differential of F by  ${}_cD_aF(x) = F(x+a) - cF(x)$ . (ii) Let  $a, b \in \mathbb{F}_{2^n}$ . We denote  ${}_c\Delta_F(a, b)$  by the number of solutions in  $\mathbb{F}_{2^n}$  of  ${}_cD_aF(x) = b$ . (iii) The c-differential uniformity of F is defined by  ${}_c\Delta_F = \max\{{}_c\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n} \text{ and } a \neq 0 \text{ if } c = 1\}$ .

(iv) F is called a perfect c-nonlinear (PcN) function if  $_{c}\Delta_{F} = 1$ .

(v) F is called a almost perfect c-nonlinear (APcN) function if  $_{c}\Delta_{F} = 2$ .

It is known [15] that, for any permutation  $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ , there is  $m \ge 0$  and  $a_i \in \mathbb{F}_{2^n}$   $(0 \le i \le m+1)$  such that

$$F(x) = (\cdots ((a_0 x + a_1)^{2^n - 2} + a_2)^{2^n - 2} \cdots + a_m)^{2^n - 2} + a_{m+1},$$
(1)

where  $a_0, a_2, \dots, a_m \neq 0$ . The above expression means that any permutation on  $\mathbb{F}_{2^n}$  is generated by the inverse function  $x^{2^n-2}$  and linear functions ax + b ( $a \neq 0$ ). The *Carlitz rank* of F is the least nonnegative integer m satisfying the above expression [1].

It is easy to see that if F has the Carlitz rank 1 then F is affine equivalent to Inv. The *c*-differential uniformity of Inv was investigated in [7].

**Theorem 2.2.** ([7]) Let  $c \neq 0, 1$ . Then Inv is APcN if and only if Tr(c) = Tr(1/c) = 1. Otherwise,  $c\Delta_{Inv} = 3$ .

The *c*-differential uniformity of  $Inv \circ (0, 1)$  was investigated in [19], where (0, 1) is the transposition that 0 and 1 are swapped. As observed in [9] that this case is related with permutations of Carlitz rank 2.

**Theorem 2.3.** ([19]) Let  $c \neq 0, 1$  and  $F = Inv \circ (0, 1)$  on  $\mathbb{F}_{2^n}$ . (i) If n = 2, then  ${}_c\Delta_F = 1$ . (ii) If n = 3, then  ${}_c\Delta_F \leq 3$ . (iii) If  $n \geq 4$ , then  ${}_c\Delta_F \leq 4$ .

Next we introduce a well-known lemma about the number of solutions of quadratic equations.

**Lemma 2.4.** Let p = 2,  $a_2 \in \mathbb{F}_{2^n}^*$  and  $a_1, a_0 \in \mathbb{F}_{2^n}$ . Then,

$$\#\{x \in \mathbb{F}_{2^n} : a_2 x^2 + a_1 x + a_0 = 0\} = \begin{cases} 2 & \text{if } a_1 \neq 0 \text{ and } \operatorname{Tr}\left(\frac{a_0 a_2}{a_1^2}\right) = 0, \\ 1 & \text{if } a_1 = 0, \\ 0 & \text{if } a_1 \neq 0 \text{ and } \operatorname{Tr}\left(\frac{a_0 a_2}{a_1^2}\right) = 1. \end{cases}$$

The following lemma is very simple and useful to our results.

**Lemma 2.5.** Let  $c \neq 0$ . Then  ${}_{c}\Delta_{F}(a,b) = {}_{c^{-1}}\Delta_{F}(a,bc^{-1})$  for all  $a \in \mathbb{F}_{2^{n}}^{*}$  and  $b \in \mathbb{F}_{2^{n}}$ . If F is a permutation then  ${}_{c}\Delta_{F} = {}_{c^{-1}}\Delta_{F}$ .

*Proof.* Let  $a \in \mathbb{F}_{2^n}^*$  and  $b \in \mathbb{F}_{2^n}$ . Then, it is easy to see that x is a solution of  ${}_cD_aF(x) = b$  if and only if x + a is a solution of  ${}_{c^{-1}}D_a(x) = bc^{-1}$ . Thus we have  ${}_c\Delta_F(a,b) = {}_{c^{-1}}\Delta_F(a,bc^{-1})$ . If F is a permutation then  ${}_c\Delta_F(0,b) = 1$  for all  $b \in \mathbb{F}_{2^n}$  and hence we get  ${}_c\Delta_F = {}_{c^{-1}}\Delta_F$ .

## 3 Upper bound on *c*-differential uniformity of permutations with low Carlitz rank

There are many differentially 4-uniform permutations obtained from modifying some points in the multiplicative inverse function (see [10] and its references) defined on  $\mathbb{F}_{2^n}$ . In this section we give an upper bound of *c*-differential uniformity of such differentially 4-uniform permutations when  $c \neq 1$ .

**Theorem 3.1.** Let F and G be permutations on  $\mathbb{F}_{2^n}$  such that F(x) = G(x) for all  $x \in \mathbb{F}_{2^n} \setminus P$  for some nonempty  $P \subseteq \mathbb{F}_{2^n}$ . If  $c \neq 1$  then  $c\Delta_F \leq c\Delta_G + \#P$ .

Proof. Let  $P_a = P \cup \{x + a : x \in P\}$ . It is enough to show that  ${}_c\Delta_F(a,b) \leq \frac{\#P_a}{2} + {}_c\Delta_F(a,b)$  for all  $a \in \mathbb{F}_{2^n}^*$  and  $b \in \mathbb{F}_{2^n}$ . Then for  $x \in \mathbb{F}_{2^n} \setminus P_a$ , all solutions of  ${}_cD_aF(x) = b$  are also solutions of  ${}_cD_aG(x) = b$  since  ${}_cD_aF(x) = {}_cD_aG(x)$ . Thus we have  ${}_cD_aF(x) = b$  has at most  ${}_c\Delta_G$  solutions in  $\mathbb{F}_{2^n} \setminus P_a$ .

Let  $x \in P_a$ . If  $_cD_aF(x) = F(x+a) + cF(x) = F(x) + cF(x+a) = _cD_aF(x+a)$  then we have 0 = F(x+a) + cF(x) + F(x) + cF(x+a) = (c+1)(F(x+a) + F(x)). Since F is a permutation, we have c = 1, which contradicts to the assumption. This means that

$${}_{c}D_{a}F(x) \neq {}_{c}D_{a}F(x+a) \text{ for all } x \in P_{a}.$$
 (2)

If there are  $\frac{\#P_a}{2} + 1$  solutions in  $P_a$  of  ${}_cD_aF(x) = b$  for some  $a, b \in \mathbb{F}_{2^n}$  then there is  $x \in P_a$  such that both x and x + a are solutions of  ${}_{c}D_{a}F(x) = b$ , a contradiction to  ${}_{c}D_{a}F(x) \neq {}_{c}D_{a}F(x+a)$  for all  $x \in P_a$ . Hence there are at most  $\frac{\#P_a}{2}$  solutions in  $P_a$  of  ${}_cD_aF(x) = b$ . Therefore,  ${}_c\Delta_F(a,b) \leq {}_c\Delta_G(a,b) + \frac{\#P_a}{2}$  for all  $a,b \in \mathbb{F}_{2^n}$ , which completes the proof.

**Example.** Let  $F = Inv \circ (1, \gamma)$  where  $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ . The differential uniformity of this function is characterized in [14]. We have G = Inv and  $P = \{1, \gamma\}$  and hence we get  $c\Delta_F \leq 5$  by Theorem 2.2 and Theorem 3.2 when  $c \neq 1$ .

By the above theorem, we can see that if G has a low c-differential uniformity and #P is small then F has also a low c-differential uniformity. Next theorem shows that this upper bound can be slightly reduced when G = Inv and  $0 \in P$ .

**Theorem 3.2.** Let F be a permutation on  $\mathbb{F}_{2^n}$  such that F(x) = Inv(x) for all  $x \in \mathbb{F}_{2^n} \setminus P$  for some nonempty  $P \subseteq \mathbb{F}_{2^n}$  with  $0 \in P$ . If  $c \neq 1$  then  ${}_c\Delta_F \leq \#P+2$ .

*Proof.* Let  $P_a = P \cup \{x + a : x \in P\}$ . It is enough to show that

$${}_c\Delta_F(a,b) \le \frac{\#P_a}{2} + 2 \tag{3}$$

for all  $a \in \mathbb{F}_{2^n}^*$  and  $b \in \mathbb{F}_{2^n}$ . By the same argument in Theorem 3.1, there are at most  $\frac{\#P_a}{2}$ solutions in  $P_a$  of  ${}_cD_aF(x) = b$ . For  $x \in \mathbb{F}_{2^n} \setminus P_a$ , we have  ${}_cD_aF(x) = {}_cD_aInv(x)$ . Since  $0, a \in P_a$ ,  ${}_{c}D_{a}F(x) = b$  implies  $bx^{2} + (ab + c + 1)x + ca = 0$  which has at most two solutions. Therefore, we have  $_{c}\Delta_{F}(a,b) \leq \frac{\#P_{a}}{2} + 2$  for all  $a, b \in \mathbb{F}_{2^{n}}$ , which completes the proof. 

It is known [8] that F and  $F \circ A$  has the same c-differential spectrum, where A is an affine permutation. However, it is not trivial to show F and  $A \circ F$  have the same c-differential uniformity, rather, it seems that it does not generally hold. For example, if  $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/\langle X^4 + X + 1 \rangle$  and  $g^4 + g + 1 = 0$  and  $A(x) = x^4 + gx$ , then A is an affine permutation. Then we have  $g\Delta_{A \circ Inv} = 4$ and  ${}_{g}\Delta_{Inv} = 3$  and hence  ${}_{g}\Delta_{A \circ Inv} \neq {}_{g}\Delta_{Inv}$ . However we show that the *c*-differential uniformity is also invariant in some specific affine equivalence. For convenience we call A(x) = ux + v an affine permutation of degree one if  $u \in \mathbb{F}_{2^n}^*$  and  $v \in \mathbb{F}_{2^n}$  (here degree does not mean algebraic degree). We also call two permutations F and  $\overline{F'}$  are affine equivalent of degree one if there are affine permutations  $A_1$  and  $A_2$  of degree one such that  $F = A_1 \circ F' \circ A_2$ . It is clear that affine equivalence of degree one is an equivalence relation. Next we show that two permutations which are affine equivalent of degree one has the same *c*-differential uniformity.

**Lemma 3.3.** Let F and F' be permutations on  $\mathbb{F}_{2^n}$  which are affine equivalent of degree one. Then  $_{c}\Delta_{F} = _{c}\Delta_{F'}$  for all  $c \in \mathbb{F}_{2^{n}}$ .

*Proof.* We denote  $F = A_1 \circ F' \circ A_2$  and  $F'' = F' \circ A_2$ , where  $A_1$  and  $A_2$  are affine permutations of degree one. Then we already see that  $c\Delta_{F''} = c\Delta_{F'}$  in [8]. Hence it is sufficient to show that  ${}_{c}\Delta_{F''} = {}_{c}\Delta_{F}$ . We denote  $A_{1}(x) = u_{1}x + v_{1}$  where  $u_{1} \in \mathbb{F}_{2^{n}}^{*}$  and  $v_{1} \in \mathbb{F}_{2^{n}}$ . Let  $a, b \in \mathbb{F}_{2^{n}}$ . Then  $b = {}_{c}D_{a}F(x)$  implies that

$$b = F(x+a) + cF(x) = (A_1 \circ F'')(x+a) + c(A_1 \circ F'')(x) = A_1(F''(x+a)) + cA_1(F''(x))$$
  
=  $u_1F''(x+a) + v_1 + c(u_1F''(x) + v) = u_1(F''(x+a) + cF''(x)) + (c+1)v_1$ 

Hence we have  ${}_{c}D_{a}F''(x) = u_{1}^{-1}b + u_{1}^{-1}v_{1}(c+1)$ . It is clear that a map from b to  $u_{1}^{-1}b + u_{1}^{-1}v_{1}(c+1)$  is bijective on  $\mathbb{F}_{2^{n}}$  for all  $c \in \mathbb{F}_{2^{n}}$  and therefore we have  ${}_{c}\Delta_{F''} = {}_{c}\Delta_{F}$ .

Now let F be defined as (1). For recurrence relations  $\alpha_i = a_i \alpha_{i-1} + \alpha_{i-2}$  and  $\beta_i = a_i \beta_{i-1} + \beta_{i-2}$ with  $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$  where  $2 \le i \le m+1$ , we denote

$$R_m(x) = \frac{\alpha_{m+1}x + \beta_{m+1}}{\alpha_m x + \beta_m}$$

and  $O_m = \left\{ x_i : x_i = \frac{\beta_i}{\alpha_i}, 1 \le i \le m \right\}$ . Then it is known [1] that  $F(x) = R_m(x)$  for all  $x \in \mathbb{F}_{2^n} \setminus O_m$ . Next we recall Lemma 3.3 of [9] with some additional properties we need.

**Lemma 3.4.** Let F be defined as (1) and  $\alpha_i, \beta_i$  defined as above. (i) If  $\alpha_m \neq 0$  then there is a permutation G such that G is affine equivalent of degree one to F and G(x) = Inv(x) for all  $x \in \mathbb{F}_{2^n} \setminus P$  where  $P \subseteq \mathbb{F}_{2^n}$  with  $\#P \leq m$  and  $0 \in P$ .

(ii) If  $\alpha_m = 0$  then there is a permutation G such that G is affine equivalent of degree one to F and G(x) = x for all  $x \in \mathbb{F}_{2^n} \setminus P$  where  $P \subseteq \mathbb{F}_{2^n}$  with  $\#P \leq m$ .

*Proof.* For (i) we denote  $A_1(x) = \frac{a_0x+\beta_m}{\alpha_m}$  and  $A_2(x) = \alpha_m x + \alpha_{m+1}$  then  $A_1$  and  $A_2$  are affine permutations of degree one. Let  $P = \{y_i : y_i = A_1^{-1}(x_i), x_i \in O_m\}$  then  $\#P \leq m$ . Since  $\alpha_i\beta_{i+1} + \alpha_{i+1}\beta_i = \alpha_i(a_i\beta_i + \beta_{i-1}) + \beta_i(a_i\alpha_i + \alpha_{i-1}) = \alpha_{i-1}\beta_i + \alpha_i\beta_{i-1}$ , we have  $\alpha_m\beta_{m+1} + \alpha_{m+1}\beta_m = \alpha_0\beta_1 + \alpha_1\beta_0 = a_0$  recursively. Using  $a_0 = \alpha_m\beta_{m+1} + \alpha_{m+1}\beta_m$ , for all  $x \in \mathbb{F}_{2^n} \setminus P$ 

$$(F \circ A_{1})(x) = R_{m} (A_{1}(x)) = \frac{\alpha_{m+1} \cdot \frac{a_{0}x + \beta_{m}}{\alpha_{m}} + \beta_{m+1}}{\alpha_{m} \cdot \frac{a_{0}x + \beta_{m}}{\alpha_{m}} + \beta_{m}} = \frac{\alpha_{m+1}(a_{0}x + \beta_{m}) + \alpha_{m}\beta_{m+1}}{a_{0}\alpha_{m}x}$$
$$= \frac{a_{0}\alpha_{m+1}x + (\alpha_{m+1}\beta_{m} + \alpha_{m}\beta_{m+1})}{a_{0}\alpha_{m}x} = \frac{a_{0}\alpha_{m+1}x + a_{0}}{a_{0}\alpha_{m}x} = \frac{1}{\alpha_{m}} \left(\alpha_{m+1} + \frac{1}{x}\right)$$
$$a_{0}\alpha_{m}x = \frac{1}{\alpha_{m}} \left(\alpha_{m+1} + \frac{1}{x}\right) + \alpha_{m+1} = \frac{1}{x} = Inv(x).$$

Since  $A_1(0) = \frac{\beta_m}{\alpha_m}$ , we can see that  $0 = A_1^{-1} \left(\frac{\beta_m}{\alpha_m}\right) \in P$ . The proof of (ii) is clear by substituting  $\alpha_m = 0$  in  $R_m(x)$ .

(A

Now we are ready to get an upper bound on c-differential uniformity of permutations with Carlitz rank m.

**Theorem 3.5.** Let F be a permutation on  $\mathbb{F}_{2^n}$  with Carlitz rank m, and  $c \neq 1$ . Then  ${}_c\Delta_F \leq m+2$ . *Proof.* The case  $\alpha_m \neq 0$  is directly from Theorem 3.2, Lemma 3.3 and Lemma 3.4 (i). If  $\alpha_m = 0$ then there is a permutation G such that G(x) = x for all  $x \in \mathbb{F}_{2^n} \setminus P$  with  $\#P \leq m$ , by Lemma 3.4 (ii). Thus  ${}_cD_aG(x) = b$  has at most  $\frac{\#P_a}{2}$  solutions in  $P_a = P \cup \{x + a : x \in P\}$  similarly with Theorem 3.1. For  $x \in \mathbb{F}_{2^n} \setminus P_a$ ,  ${}_cD_aG(x) = b$  implies (c+1)x = a+b which has exactly one solution if  $c \neq 1$ . Thus we have  ${}_c\Delta_G(a, b) \leq \frac{\#P_a}{2} + 1 \leq m+1$ . Therefore we have  ${}_c\Delta_G \leq m+1 \leq m+2$ , which completes the proof, by Lemma 3.3.

It is easy to see that permutations of Carlitz rank 1 are affine equivalent of degree one to Inv. We observed in [9] that permutations of Carlitz rank 2 are affine equivalent of degree one to  $Inv \circ (0, 1)$ . Using Lemma 3.3, we can see that the upper bound in the above theorem is tight when m = 1 and m = 2 by Theorem 2.2 and Theorem 2.3, respectively. In next section, we show that it is also tight when m = 3.

### 4 *c*-differential uniformity of permutations with Carlitz rank 3

Let F be (1) with m = 3 as follows :

$$F(x) = \left(\left((a_0 x + a_1)^{2^n - 2} + a_2\right)^{2^n - 2} + a_3\right)^{2^n - 2} + a_4 \tag{4}$$

If  $A_1(x) = \frac{x+a_1a_2}{a_0a_2}$  and  $A_2(x) = \frac{x+a_4}{a_2}$  then we can easily check

$$F_3(x) = (A_2 \circ F \circ A_1)(x) = ((x^{2^n - 2} + 1)^{2^n - 2} + a_2 a_3)^{2^n - 2}.$$

Now we denote  $\gamma = a_2 a_3$ . If  $\gamma = 1$ , then  $F_3$  can be expressed by

$$F_3(x) = \begin{cases} x+1 & \text{if } x \notin \{0,1\} \\ x & \text{if } x \in \{0,1\} \end{cases}$$

which is not an interesting case. When  $\gamma \neq 0, 1$ , as observed in [9], if we denote  $A_3(x) = \frac{x+\gamma}{\gamma+1}$  and  $A_4(x) = (\gamma + 1)x + 1$  then we have  $A_4 \circ F_3 \circ A_3 = Inv \circ (0, 1, \gamma)$  where  $(0, 1, \gamma)$  is a cycle of length 3. Thus we can see that F in (4) is affine equivalent of degree one to  $Inv \circ (0, 1, \gamma)$  with  $\gamma = a_2a_3$ . From now on, we investigate *c*-differential uniformity of  $Inv \circ (0, 1, \gamma)$  where  $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ .

**Remark 4.1.** For small n, we obtain the following results from the exhaustive search. (i) If n = 2 then F is PcN for all  $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ (ii) If n = 3 with  $\mathbb{F}_{2^3} = \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$  then we have

$${}_{c}\Delta_{F} = \begin{cases} 2 & \text{if } \gamma^{3} + \gamma + 1 = 0, \\ 3 & \text{otherwise.} \end{cases}$$

We investigate the c-differential uniformity of  $Inv \circ (0, 1, \gamma)$  when  $n \ge 4$ . If c = 0 then  $_0\Delta_F = 1$  since F is a permutation. The case c = 1 was already investigated in [9, 14]. Hence we assume that

$$F = Inv \circ (0, 1, \gamma), \ c, \gamma \notin \{0, 1\}, \ n \ge 4$$
(5)

throughout this section unless otherwise noted. By Theorem 3.2, F has c-differential uniformity at most 5. We investigate c-differential uniformity of F in detail. We denote a set

$$P_a = P \cup \{x + a : x \in P\} = \{0, 1, \gamma, a, a + 1, a + \gamma\}.$$

We first characterize the condition that  ${}_{c}D_{a}F(x) = b$  has two solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ .

**Lemma 4.2.** Let  $a \in \mathbb{F}_{2^n}^*$  and  $b \in \mathbb{F}_{2^n}$ . Then  ${}_cD_aF(x) = b$  has at most two solutions in  $\mathbb{F}_{2^n} \setminus P_a$ . Furthermore,  ${}_cD_aF(x) = b$  has two solutions in  $\mathbb{F}_{2^n} \setminus P_a$  if and only if  $b \neq 0$ ,  $ab + c + 1 \neq 0$ ,  $\operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = 0$ ,  $(b+c)a + b + c + 1 \neq 0$ ,  $(b+1)a + b + c + 1 \neq 0$ ,  $(b\gamma + c)a + \gamma(b\gamma + c + 1) \neq 0$ and  $(b\gamma + 1)a + \gamma(b\gamma + c + 1) \neq 0$ .

*Proof.* If  $x \in \mathbb{F}_{2^n} \setminus P_a$  then  $b = {}_cD_aF(x) = {}_cD_aInv(x)$  implies that  $bx^2 + (ab+c+1)x + ac = 0$  which has at most 2 solutions. Hence  ${}_cD_aF(x) = b$  has at most two solutions in  $\mathbb{F}_{2^n} \setminus P_a$ .

 ${}_{c}D_{a}F(x) = b$  has 2 solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$  implies that  $bx^{2} + (ab + c + 1)x + ac = 0$  has 2 solutions which is equivalent to

$$\operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = 0, \ b \neq 0 \text{ and } ab+c+1 \neq 0.$$
(6)

by Lemma 2.4. If there is a solution  $x_0 \in P_a$  of  $bx^2 + (ab+c+1)x + ac = 0$  then  $x_0$  cannot be a solution of  ${}_cD_aF(x) = b$ . Hence we need to check that there is no solutions of  $bx^2 + (ab+c+1)x + ac = 0$  in  $P_a$ .

- If x = 0 or x = a then we have a = 0 which is a contradiction to  $a \in \mathbb{F}_{2^n}^*$ .
- If x = 1 then we have (b+c)a + b + c + 1 = 0 or equivalently  $a = \frac{b+c+1}{b+c}$ .
- If x = a + 1 then we have (b+1)a + b + c + 1 = 0 or equivalently  $a = \frac{b+c+1}{b+1}$ .
- If  $x = \gamma$  then we have  $(b\gamma + c)a + \gamma(b\gamma + c + 1) = 0$  or equivalently  $a = \frac{\gamma(b\gamma + c + 1)}{b\gamma + c}$ .
- If  $x = a + \gamma$  then we have  $(b\gamma + 1)a + \gamma(b\gamma + c + 1) = 0$  or equivalently  $a = \frac{\gamma(b\gamma + c + 1)}{b\gamma + 1}$ .

Hence we can see that there are no solutions in  $P_a$  of  $bx^2 + (ab + c + 1)x + ac = 0$  if and only if

$$(b+c)a + b + c + 1 \neq 0, \quad (b\gamma + c)a + \gamma(b\gamma + c + 1) \neq 0, (b+1)a + b + c + 1 \neq 0, \quad (b\gamma + 1)a + \gamma(b\gamma + c + 1) \neq 0.$$
 (7)

If all conditions in the above theorem hold, then  $bx^2 + (ab + c + 1)x + ac = 0$  has two solutions in  $\mathbb{F}_{2^n} \setminus P_a$ . Since all solutions are not belong to  $P_a$  we can say that they are also solutions of  ${}_{c}D_{a}F(x) = b$ .

Next we show that F in (5) is not APcN when  $c \neq 0$ .

**Theorem 4.3.** Under the same assumption as in (5) we have  $3 \le c\Delta_F \le 5$ .

Proof. By Theorem 3.2,  $_{c}\Delta_{F} \leq 5$  is straightforward. Next we show that  $_{c}\Delta_{F} \geq 3$ . We set  $b = _{c}D_{a}F(0) = c + a^{-1}$ . Then x = 0 is a solution of  $_{c}D_{a}F(x) = b$ . We use Lemma 4.2 to show that there is  $a \in \mathbb{F}_{2^{n}}$  such that  $_{c}D_{c}F(x) = b$  has two solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ . It is easy to see that  $b \neq 0$  since  $c \neq a^{-1}$ , and  $ab + c + 1 = a(a^{-1} + c) + c + 1 = c(a + 1) \neq 0$  if  $a \neq 1$ . Now we assume that  $a \neq 1$ . We require

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{ac(a^{-1}+c)}{c^2(a^2+1)}\right) = \operatorname{Tr}\left(\frac{ca+1}{c(a^2+1)}\right) = \operatorname{Tr}\left(\frac{c(a+1)+c+1}{c(a^2+1)}\right) = \operatorname{Tr}\left(\frac{1}{a+1} + \frac{1}{(a+1)^2} + \frac{1}{c(a+1)^2}\right) = \operatorname{Tr}\left(\frac{1}{c(a+1)^2}\right).$$

Using  $b + c + 1 = a^{-1} + 1$  and  $b\gamma + c = a^{-1}\gamma + c(\gamma + 1)$  and  $\gamma(b\gamma + c + 1) = a^{-1}\gamma^2 + c\gamma(\gamma + 1) + \gamma$  we check (7)

$$(b+c)a + b + c + 1 = a^{-1} \cdot a + a^{-1} + 1 = a^{-1} (b+1)a + b + c + 1 = a(a^{-1} + c + 1) + a^{-1} + 1 = a^{-1} ((c+1)a^2 + 1)$$

$n \\ c\Delta_F$	4	5	6	7	8	
3	32	10	28	196	672	
4	164	820	3576	15176	62880	
5	0	70	240	504	964	

Table 1: Distribution of  $_{c}\Delta_{F}$  when  $4 \leq n \leq 8$ .

$$(b\gamma + c)a + \gamma(b\gamma + c + 1) = a(a^{-1}\gamma + c(\gamma + 1)) + a^{-1}\gamma^2 + c\gamma(\gamma + 1) + \gamma = a^{-1} (c(\gamma + 1)a^2 + c\gamma(\gamma + 1)a + \gamma^2) (b\gamma + 1)a + \gamma(b\gamma + c + 1) = a(a^{-1}\gamma + c\gamma + 1) + a^{-1}\gamma^2 + c\gamma(\gamma + 1) + \gamma = a^{-1} ((c\gamma + 1)a^2 + c\gamma(\gamma + 1)a + \gamma^2)$$

We set  $S = \{0, \frac{1}{c^{2n-1}+1}\} \cup \{x \in \mathbb{F}_{2^n} : c(\gamma+1)x^2 + c\gamma(\gamma+1)x + \gamma^2 = 0\} \cup \{x \in \mathbb{F}_{2^n} : (c\gamma+1)x^2 + c\gamma(\gamma+1)x + \gamma^2 = 0\}$ . By Lemma 4.2,  ${}_cD_aF(x) = c + a^{-1}$  has two solutions in  $\mathbb{F}_{2^n} \setminus P_a$  if and only if  $\operatorname{Tr}\left(\frac{1}{c(a+1)^2}\right) = 0$  and  $a \in \mathbb{F}_{2^n} \setminus (S \cup \{1\})$ . Since the map  $a \mapsto \frac{1}{c(a+1)^2}$  is an injection from  $\mathbb{F}_{2^n} \setminus \{1\}$  to  $\mathbb{F}_{2^n}^*$  and  $\operatorname{Tr}(\cdot)$  is a balanced map, we have  $\#\left\{a \in \mathbb{F}_{2^n} \setminus \{1\} : \operatorname{Tr}\left(\frac{1}{c(a+1)^2}\right) = 0\right\} = 2^{n-1} - 1$ . Since  $\#S \leq 6$ , we have  $\#\left(\left\{a \in \mathbb{F}_{2^n} \setminus \{1\} : \operatorname{Tr}\left(\frac{1}{c(a+1)^2}\right) = 0\right\} \setminus S\right) \geq 2^{n-1} - 7 \geq 1$  if  $n \geq 4$ . Therefore, there exists  $a \in \left\{a \in \mathbb{F}_{2^n} \setminus \{1\} : \operatorname{Tr}\left(\frac{1}{c(a+1)^2}\right) = 0\right\} \setminus S$  such that  ${}_cD_aF(x) = c + a^{-1}$  has two solutions in  $\mathbb{F}_{2^n} \setminus P_a$  and hence  ${}_c\Delta_F(a, c + a^{-1}) \geq 3$ .

We summarize in Table 1 the distribution of  ${}_{c}\Delta_{F}$  by computing the number of pairs  $(c, \gamma) \in (\mathbb{F}_{2^{n}} \setminus \mathbb{F}_{2}) \times (\mathbb{F}_{2^{n}} \setminus \mathbb{F}_{2})$  such that  ${}_{c}\Delta_{F}$  equals to each value in  $\{3, 4, 5\}$ , where the column sum is  $(2^{n}-2)^{2}$ . We can see that we have  ${}_{c}\Delta_{F} = 4$  in most cases, and the cases  ${}_{c}\Delta_{F} = 3$  or  ${}_{c}\Delta_{F} = 5$  are relatively rare. So we characterize the cases that  ${}_{c}\Delta_{F} = 3$  or  ${}_{c}\Delta_{F} = 5$ . First we give a characterization for the case  ${}_{c}\Delta_{F} = 5$ .

**Theorem 4.4.** Under the same assumption as in (5) we have  ${}_{c}\Delta_{F} = 5$  if and only if at least one of the following conditions is satisfied :

$$\begin{aligned} &(i) \ c \in \left\{\frac{\gamma^3}{(\gamma+1)^2}, \frac{(\gamma+1)^2}{\gamma^3}\right\} \ and \ \mathrm{Tr}\left(\frac{1}{\gamma(\gamma+1)^2}\right) = 0 \ and \ \gamma \notin \mathbb{F}_4 \ and \ \gamma^4 + \gamma^3 + 1 \neq 0 \ and \ \gamma^5 + \gamma^2 + 1 \neq 0. \\ &(ii) \ c \in \left\{\frac{\gamma+1}{\gamma^3+\gamma^2+\gamma}, \frac{\gamma^3+\gamma^2+\gamma}{\gamma+1}\right\} \ and \ \mathrm{Tr}\left(1+\frac{1}{\gamma^3}\right) = 0 \ and \ \gamma \notin \mathbb{F}_4 \ and \ \gamma^5 + \gamma^3 + 1 \neq 0. \\ &(iii) \ c \in \left\{\frac{\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma}{\gamma(\gamma+1)}, \frac{\gamma(\gamma+1)}{\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma}\right\} \ and \ \mathrm{Tr}\left(\frac{\gamma+1}{\gamma^2(\gamma^2+\gamma+1)}\right) = 0 \ and \ \gamma \notin \mathbb{F}_4 \ and \ \gamma^5 \neq 1. \\ &(iv) \ n \equiv 0 \ (\mathrm{mod} \ 8) \ and \ c, \ \gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2. \\ &(v) \ c \in \left\{x \in \mathbb{F}_{2^n} : \gamma^3 x^3 + \gamma^2 x^2 + (\gamma+1)x + 1 = 0\right\} \setminus \left\{\gamma, \frac{1}{\gamma^{2^{n-1}}+\gamma}\right\}, \ \gamma^3 c^2 + (\gamma^2 + \gamma + 1)c + \gamma^2 \neq 0 \ and \\ &\mathrm{Tr}\left(\frac{(c\gamma+c+1)(c^2\gamma+1)}{c(c+\gamma)^2}\right) = 0 \ and \ \gamma \notin \mathbb{F}_4. \\ &(vi) \ c \in \left\{x \in \mathbb{F}_{2^n} : x^3 + (\gamma+1)x^2 + \gamma^2 x + \gamma^3 = 0\right\} \setminus \left\{\gamma^{-1}, \gamma^{2^{n-1}} + \gamma\right\}, \ \gamma^2 c^2 + (\gamma^2 + \gamma + 1)c + \gamma^3 \neq 0. \\ ∧ \ \mathrm{Tr}\left(\frac{(c+\gamma+1)(c^2\gamma\gamma)}{(c\gamma+1)^2}\right) = 0 \ and \ \gamma \notin \mathbb{F}_4. \end{aligned}$$

*Proof.* Assume that  ${}_{c}\Delta_{F} = 5$ . When  $a \in \{0, 1, \gamma, \gamma + 1\}$ , we have  $\#P_{a} = 4$  and hence  ${}_{c}\Delta_{F}(a, b) \leq 4$  by (3). Thus we assume that  $a \in \mathbb{F}_{2^{n}} \setminus \{0, 1, \gamma, \gamma + 1\}$ , and then we have  $\#P_{a} = 6$ . We can see in

the proof of Theorem 3.2 that  ${}_{c}D_{a}(x) = b$  has at most 3 solutions in  $P_{a}$  and at most 2 solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ . Since  ${}_{c}\Delta_{F} = 5$ , there are  $a \in \mathbb{F}_{2^{n}} \setminus \{0, 1, \gamma, \gamma + 1\}$  and  $b \in \mathbb{F}_{2^{n}}$  such that  ${}_{c}D_{a}F(x) = b$  has 3 solutions in  $P_{a}$  and 2 solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ . First we consider that  ${}_{c}D_{a}F(x) = b$  has 3 solutions in  $P_{a}$ . We state  ${}_{c}D_{a}F(x) = F(x+a) + cF(x)$  for each  $x \in P_{a}$ .

$${}_{c}D_{a}F(0) = F(a) + cF(0) = a^{-1} + c \\ {}_{c}D_{a}F(1) = F(1+a) + cF(1) = (a+1)^{-1} + \gamma^{-1}c \\ {}_{c}D_{a}F(\gamma) = F(\gamma+a) + cF(\gamma) = (a+\gamma)^{-1} \\ {}_{c}D_{a}F(a+\gamma) = F(\gamma) + cF(\gamma+a) = c(a+\gamma)^{-1} \\ {}_{c}D_{a}F(a+\gamma) = F(\gamma) + cF(\gamma) +$$

Applying (2), we investigate required conditions such that  ${}_{c}D_{a}F(x) = b$  has at least two solutions in  $P_{a}$ .

- $_{c}D_{a}F(0) = _{c}D_{a}F(1) \Rightarrow c(\gamma+1)a^{2} + c(\gamma+1)a + \gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{\gamma}{c(\gamma+1)}\right) = 1$ ).
- $_{c}D_{a}F(0) = _{c}D_{a}F(\gamma) \Rightarrow ca^{2} + c\gamma a + \gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}(c^{-1}\gamma^{-1}) = 1$ ).
- ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(a+1) \Rightarrow (c\gamma+1)a^{2} + (\gamma+1)a + \gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{\gamma(c\gamma+1)}{(\gamma+1)^{2}}\right) = 1$  and  $c \neq \gamma^{-1}$ ).
- ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(a+\gamma) \Rightarrow ca^{2} + (c\gamma+c+1)a+\gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{c\gamma}{(c\gamma+c+1)^{2}}\right) = 1$  and  $c \neq (\gamma+1)^{-1}$ ).
- ${}_{c}D_{a}F(1) = {}_{c}D_{a}F(\gamma) \Rightarrow ca^{2} + c(\gamma+1)a + \gamma(c+\gamma+1) = 1$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{\gamma(c+\gamma+1)}{c(\gamma+1)^{2}}\right) = 1$  and  $c \neq \gamma + 1$ ).
- ${}_{c}D_{a}F(1) = {}_{c}D_{a}F(a) \Rightarrow (c+\gamma)a^{2} + c(\gamma+1)a + c\gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{\gamma(c+\gamma)}{c(\gamma+1)^{2}}\right) = 1$  and  $c \neq \gamma$ ).
- ${}_{c}D_{a}F(1) = {}_{c}D_{a}F(a+\gamma) \Rightarrow ca^{2} + (c+\gamma)a + \gamma^{2} = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{c\gamma^{2}}{(c+\gamma)^{2}}\right) = 1$  and  $c \neq \gamma$ ).
- ${}_{c}D_{a}F(\gamma) = {}_{c}D_{a}F(a) \Rightarrow a^{2} + (c+\gamma+1)a + c\gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma+1)^{2}}\right) = 1$  and  $c \neq \gamma + 1$ ).
- ${}_{c}D_{a}F(\gamma) = {}_{c}D_{a}F(a+1) \Rightarrow a^{2} + (c\gamma+1)a + c\gamma^{2} = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{c\gamma^{2}}{(c\gamma+1)^{2}}\right) = 1$  and  $c \neq \gamma^{-1}$ ).

• 
$$_{c}D_{a}F(a) = _{c}D_{a}F(a+1) \Rightarrow (\gamma+1)a^{2} + (\gamma+1)a + c\gamma = 0$$
 (has no solutions  $\Leftrightarrow \operatorname{Tr}\left(\frac{c\gamma}{\gamma+1}\right) = 1$ ).

- $_{c}D_{a}F(a) = _{c}D_{a}F(a+\gamma) \Rightarrow a^{2}+\gamma a+c\gamma = 0$  (has no solutions  $\Leftrightarrow \operatorname{Tr}(c\gamma^{-1}) = 1$ ).
- ${}_{c}D_{a}F(a+1) = {}_{c}D_{a}F(a+\gamma) \Rightarrow a^{2} + (\gamma+1)a + (c\gamma+c+1)\gamma = 0$  (has no solutions  $\Leftrightarrow$  $\operatorname{Tr}\left(\frac{(c\gamma+c+1)\gamma}{(\gamma+1)^{2}}\right) = 1$  and  $c \neq (\gamma+1)^{-1}$ ).

Next we investigate all the cases that  ${}_{c}D_{a}F(x) = b$  has 3 solutions in  $P_{a}$ . For each case, we apply Lemma 4.2 to find required conditions that  ${}_{c}D_{a}F(x) = b$  has 2 solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ .

(Case 1) If  ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(1) = {}_{c}D_{a}F(\gamma)$  then *a* is a common solution of  $c(\gamma+1)a^{2} + c(\gamma+1)a + \gamma = 0$ ,  $ca^{2} + c\gamma a + \gamma = 0$  and  $ca^{2} + c(\gamma+1)a + \gamma(c+\gamma+1) = 0$ . We add the first two equations to get  $0 = c\gamma a^{2} + ca = ca(\gamma a + 1)$  and hence we have  $a = \gamma^{-1}$ . We have  $c = \frac{\gamma^{3}}{(\gamma+1)^{2}}$  to substitute  $a = \gamma^{-1}$  to each equation. We set  $b = {}_{c}D_{a}(\gamma) = \frac{\gamma}{\gamma^{2}+1}$  and check Lemma 4.2. Then we have  $b \neq 0$  and

$$ab + c + 1 = \frac{1}{\gamma^2 + 1} + \frac{\gamma^3}{\gamma^2 + 1} + 1 = \frac{\gamma^3 + \gamma^2}{\gamma^2 + 1} = \frac{\gamma^2}{\gamma + 1} \neq 0,$$

since  $\gamma \neq 0$ . And (6) becomes

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{\frac{\gamma^3}{(\gamma+1)^4}}{\frac{\gamma^4}{(\gamma+1)^2}}\right) = \operatorname{Tr}\left(\frac{1}{\gamma(\gamma+1)^2}\right)$$

Using  $b + c + 1 = \frac{\gamma^3 + \gamma}{\gamma^2 + 1} + 1 = \gamma + 1$  and  $\gamma(b\gamma + c + 1) = \frac{\gamma(\gamma^3 + 1)}{(\gamma + 1)^2} = \frac{\gamma(\gamma^2 + \gamma + 1)}{\gamma + 1}$ , (7) becomes

$$\begin{aligned} a(b+c) + b + c + 1 &= \gamma^{-1} \cdot \gamma + \gamma + 1 = \gamma \neq 0 \\ a(b+1) + b + c + 1 &= \gamma^{-1} \cdot \frac{\gamma^2 + \gamma + 1}{\gamma^2 + 1} + \gamma + 1 = \frac{(\gamma^2 + \gamma + 1) + (\gamma^4 + \gamma^3 + \gamma^2 + \gamma)}{\gamma(\gamma + 1)^2} = \frac{\gamma^4 + \gamma^3 + 1}{\gamma(\gamma + 1)^2} \\ (b\gamma + c)a + \gamma(b\gamma + c + 1) &= \gamma^{-1} \cdot \frac{\gamma^3 + \gamma^2}{(\gamma + 1)^2} + \frac{\gamma(\gamma^2 + \gamma + 1)}{\gamma + 1} = \frac{\gamma^2(\gamma + 1)}{\gamma + 1} = \gamma^2 \neq 0 \\ (b\gamma + 1)a + \gamma(b\gamma + c + 1) = \gamma^{-1} \cdot \frac{1}{(\gamma + 1)^2} + \frac{\gamma(\gamma^2 + \gamma + 1)}{\gamma + 1} = \frac{\gamma^2(\gamma^3 + 1) + 1}{\gamma(\gamma + 1)^2} = \frac{\gamma^5 + \gamma^2 + 1}{\gamma(\gamma + 1)^2} \end{aligned}$$

Hence we require  $\gamma^4 + \gamma^3 + 1 \neq 0$  and  $\gamma^5 + \gamma^2 + 1 \neq 0$ . It is easy to check  $a = \gamma^{-1} \notin \{0, 1, \gamma, \gamma + 1\}$  requires  $\gamma \notin \mathbb{F}_4$ . If  $c = \frac{(\gamma+1)^2}{\gamma^3}$ , then we have  $c\Delta_F = c^{-1}\Delta_F = 5$  by Lemma 2.5. We exchange c by  $c^{-1}$  in the above analysis, we also require  $\operatorname{Tr}\left(\frac{1}{\gamma(\gamma+1)^2}\right) = 0, \ \gamma \notin \mathbb{F}_4, \ \gamma^4 + \gamma^3 + 1 \neq 0$  and  $\gamma^5 + \gamma^2 + 1 \neq 0$ .

(Case 2) If  ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(1) = {}_{c}D_{a}F(a+\gamma)$  then a is a common solution of  $c(\gamma+1)a^{2} + c(\gamma+1)a + \gamma = 0$ ,  $ca^{2} + (c\gamma+c+1)a + \gamma = 0$  and  $ca^{2} + (c+\gamma)a + \gamma^{2} = 0$ . We add the first two equation to have  $c\gamma a^{2} + a = 0$  and hence  $ca = \gamma^{-1}$ . Hence the first equation implies  $0 = ca(\gamma+1)a + ca(\gamma+1) + \gamma = \frac{(\gamma+1)a+(\gamma^{2}+\gamma+1)}{\gamma}$  and hence we have  $a = \frac{\gamma^{2}+\gamma+1}{\gamma+1}$  and  $c = \frac{1}{a\gamma} = \frac{\gamma+1}{\gamma^{3}+\gamma^{2}+\gamma}$ . Note that we have a = 0 if  $\gamma \in \mathbb{F}_{4} \setminus \mathbb{F}_{2}$  and hence we require  $\gamma \notin \mathbb{F}_{4}$ . We set  $b = {}_{c}D_{a}F(0) = a^{-1} + c = \frac{\gamma^{2}+1}{\gamma^{3}+\gamma^{2}+\gamma}$  and check Lemma 4.2. Then we have  $b \neq 0$  and

$$\begin{aligned} ab+c+1 &= \frac{\gamma^2+\gamma+1}{\gamma+1} \cdot \frac{\gamma^2+1}{\gamma^3+\gamma^2+\gamma} + \frac{\gamma+1}{\gamma^3+\gamma^2+\gamma} + 1 = \frac{(\gamma^3+1)+(\gamma+1)+(\gamma^3+\gamma^2+\gamma)}{\gamma^3+\gamma^2+\gamma} \\ &= \frac{\gamma^2}{\gamma^3+\gamma^2+\gamma} \neq 0 \end{aligned}$$

since  $\gamma \neq 0, 1$ . And (6) becomes

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{\frac{(\gamma+1)^2}{\gamma^2(\gamma^2+\gamma+1)}}{\frac{\gamma^2}{(\gamma^2+\gamma+1)^2}}\right) = \operatorname{Tr}\left(\frac{\gamma^4+\gamma^3+\gamma+1}{\gamma^4}\right) = \operatorname{Tr}\left(1+\frac{1}{\gamma^3}\right).$$

Using  $b + c + 1 = \frac{\gamma + 1}{\gamma^2 + \gamma + 1} + 1 = \frac{\gamma^2}{\gamma^2 + \gamma + 1}$  and  $\gamma(b\gamma + c + 1) = \gamma\left(\frac{\gamma^3 + 1}{\gamma(\gamma^2 + \gamma + 1)} + 1\right) = \gamma\left(\frac{\gamma + 1}{\gamma} + 1\right) = 1$ , (7) becomes

$$\begin{aligned} a(b+c) + b + c + 1 &= \frac{\gamma^2 + \gamma + 1}{\gamma + 1} \cdot \frac{\gamma + 1}{\gamma^2 + \gamma + 1} + \frac{\gamma + 1}{\gamma^2 + \gamma + 1} + 1 = \frac{\gamma + 1}{\gamma^2 + \gamma + 1} \neq 0 \\ a(b+1) + b + c + 1 &= \frac{\gamma^2 + \gamma + 1}{\gamma + 1} \cdot \frac{\gamma^3 + \gamma + 1}{\gamma(\gamma^2 + \gamma + 1)} + \frac{\gamma^2}{\gamma^2 + \gamma + 1} = \frac{\gamma^5 + \gamma^3 + 1}{\gamma(\gamma^3 + 1)} \\ (b\gamma + c)a + \gamma(b\gamma + c + 1) &= \frac{\gamma^2 + \gamma + 1}{\gamma + 1} \cdot \frac{\gamma + 1}{\gamma} + 1 = \frac{\gamma^2 + 1}{\gamma} \neq 0 \\ (b\gamma + 1)a + \gamma(b\gamma + c + 1) &= \frac{\gamma^2 + \gamma + 1}{\gamma + 1} \cdot \frac{\gamma}{\gamma^2 + \gamma + 1} + 1 = \frac{1}{\gamma + 1} \neq 0 \end{aligned}$$

Hence we require  $\gamma^5 + \gamma^3 + 1 \neq 0$ . It is easy to check  $a = \frac{\gamma^2 + \gamma + 1}{\gamma + 1} \notin \{0, 1, \gamma, \gamma + 1\}$  if  $\gamma \notin \mathbb{F}_4$ . If  $c = \frac{\gamma^3 + \gamma^2 + \gamma}{\gamma + 1}$ , then we have  $c\Delta_F = c^{-1}\Delta_F = 5$  by Lemma 2.5. We exchange c by  $c^{-1}$  in the above analysis, we also require  $\operatorname{Tr}\left(1 + \frac{1}{\gamma^3}\right) = 0$  and  $\gamma \notin \mathbb{F}_4$  and  $\gamma^5 + \gamma^3 + 1 \neq 0$ .

(Case 3) If  ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(a+1) = {}_{c}D_{a}F(a+\gamma)$  then *a* is a common solution of  $(c\gamma+1)a^{2} + (\gamma+1)a + \gamma = 0$ ,  $ca^{2} + (c\gamma+c+1)a + \gamma = 0$  and  $a^{2} + (\gamma+1)a + (c\gamma+c+1)\gamma = 0$ . We add the first equation and the third equation to get  $c\gamma a^{2} + c\gamma(\gamma+1) = 0$  and hence  $a^{2} = \gamma + 1$  so  $a = \gamma^{2^{n-1}} + 1$ . We substitute  $a = \gamma^{2^{n-1}} + 1$  to the third equation to have  $0 = c\gamma(\gamma+1) + \gamma^{2^{n-1}+1} + \gamma^{2^{n-1}} + \gamma$  and hence  $c = \frac{\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma}{\gamma(\gamma+1)} \neq 0$  because  $0 \neq \gamma(\gamma^{2}+\gamma+1) = (\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma)^{2}$  when  $\gamma \notin \mathbb{F}_{4}$ . We set  $b = {}_{c}D_{a}F(a+\gamma) = \frac{\gamma^{2^{n-1}}}{\gamma(\gamma+1)}$  and check Lemma 4.2. Then we have  $b \neq 0$  and

$$ab + c + 1 = \frac{\gamma^{2^{n-1}}(\gamma^{2^{n-1}} + 1) + (\gamma^{2^{n-1}+1} + \gamma^{2^{n-1}} + \gamma) + \gamma^2 + \gamma}{\gamma(\gamma + 1)} = \frac{\gamma^{2^{n-1}+1} + \gamma^2 + \gamma}{\gamma(\gamma + 1)} \neq 0$$

requires  $\gamma \notin \mathbb{F}_4 \setminus \mathbb{F}_2$  because  $0 \neq \gamma(\gamma^2 + \gamma + 1) = (\gamma^{2^{n-1}+1} + \gamma^{2^{n-1}} + \gamma)^2$ . And (6) becomes

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{\frac{\gamma^{2^{n-1}}(\gamma^{2^{n-1}}+1)(\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma)}{\gamma^2(\gamma+1)^2}}{\frac{\gamma^4+\gamma^3+\gamma^2}{\gamma^2(\gamma+1)^2}}\right)$$
$$= \operatorname{Tr}\left(\frac{\gamma^{2^{n-1}}(\gamma^{2^{n-1}}+1)(\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma)}{\gamma^2(\gamma^2+\gamma+1)}\right) = \operatorname{Tr}\left(\frac{\gamma(\gamma+1)(\gamma^3+\gamma^2+\gamma)}{\gamma^4(\gamma^2+\gamma+1)^2}\right)$$
$$= \operatorname{Tr}\left(\frac{\gamma+1}{\gamma^2(\gamma^2+\gamma+1)}\right).$$

Using  $b + c + 1 = \frac{\gamma^{2^{n-1}} + 1}{\gamma + 1} + 1 = \frac{\gamma^{2^{n-1}} + \gamma}{\gamma + 1}$  and  $\gamma(b\gamma + c + 1) = \gamma\left(\frac{\gamma^{2^{n-1}} + \gamma}{\gamma(\gamma + 1)} + 1\right) = \frac{\gamma^{2^{n-1} + 1} + \gamma^3}{\gamma(\gamma + 1)}$ , (7) becomes

$$\begin{aligned} a(b+c)+b+c+1 &= (\gamma^{2^{n-1}}+1) \cdot \frac{\gamma^{2^{n-1}}+1}{\gamma+1} + \frac{\gamma^{2^{n-1}}+\gamma}{\gamma+1} = \frac{\gamma^{2^{n-1}}+1}{\gamma+1} = (\gamma+1)^{2^{n-1}-1} \neq 0 \\ a(b+1)+b+c+1 &= (\gamma^{2^{n-1}}+1) \cdot \frac{\gamma^{2^{n-1}}+\gamma^2+\gamma}{\gamma(\gamma+1)} + \frac{\gamma^{2^{n-1}}+\gamma}{\gamma+1} = \gamma^{2^{n-1}-1}(\gamma+1) \neq 0 \\ (b\gamma+c)a+\gamma(b\gamma+c+1) &= (\gamma^{2^{n-1}}+1) \cdot \frac{\gamma^{2^{n-1}}+\gamma}{\gamma(\gamma+1)} + \frac{\gamma^{2^{n-1}+1}+\gamma^3}{\gamma(\gamma+1)} = \frac{\gamma^{2^{n-1}}+\gamma^3}{\gamma(\gamma+1)} = \frac{(\gamma^6+\gamma)^{2^{n-1}}}{\gamma(\gamma+1)} \\ (b\gamma+1)a+\gamma(b\gamma+c+1) &= (\gamma^{2^{n-1}}+1) \cdot \frac{\gamma^{2^{n-1}+1}+\gamma^2+\gamma}{\gamma(\gamma+1)} + \frac{\gamma^{2^{n-1}+1}+\gamma^3}{\gamma(\gamma+1)} = \gamma^{2^{n-1}}+\gamma+1 \\ &= (\gamma^2+\gamma+1)^{2^{n-1}} \neq 0 \end{aligned}$$

Hence we require  $\gamma^5 \neq 1$ . It is easy to check  $a = \gamma^{2^{n-1}} + 1 \notin \{0, 1, \gamma, \gamma + 1\}$  if  $\gamma \notin \mathbb{F}_4$ . If  $c = \frac{\gamma(\gamma+1)}{\gamma^{2^{n-1}+1}+\gamma^{2^{n-1}}+\gamma}$ , then we have  $c\Delta_F = c^{-1}\Delta_F = 5$  by Lemma 2.5. We exchange c by  $c^{-1}$  in the above analysis, we also require  $\operatorname{Tr}\left(\frac{\gamma+1}{\gamma^2(\gamma^2+\gamma+1)}\right) = 0, \ \gamma \notin \mathbb{F}_4$  and  $\gamma^5 \neq 1$ .

(Case 4) If  $_cD_aF(0) = _cD_aF(\gamma) = _cD_aF(a+1)$  then a is a common solution of  $ca^2 + c\gamma a + \gamma = 0$ ,  $(c\gamma + 1)a^2 + (\gamma + 1)a + \gamma = 0$  and  $a^2 + (c\gamma + 1)a + c\gamma^2 = 0$ . We add the first two equations to obtain  $(c\gamma + c + 1)a^2 + (c\gamma + \gamma + 1)a = 0$ . Hence we have  $c\gamma + c + 1 = c\gamma + \gamma + 1 = 0$  or  $a = \frac{c\gamma + \gamma + 1}{c\gamma + c + 1}$ .

• If  $c\gamma + c + 1 = c\gamma + \gamma + 1 = 0$  then  $c = \gamma$  and  $\gamma^2 + \gamma + 1 = 0$  so  $\gamma \in \mathbb{F}_4$ . And *a* is a solution of  $a^2 + \gamma a + \gamma = 0$  where such *a* exists if and only if  $\operatorname{Tr}(\gamma) = 0$  if and only if  $n \equiv 0 \pmod{4}$ . Since  $a^2 = a\gamma + 1$ , we have

$$a^{4} = a^{2}\gamma^{2} + 1 = (a\gamma + 1)\gamma^{2} + 1 = a + \gamma,$$
  
$$a^{8} = a^{2} + \gamma^{2} = a\gamma + 1 + \gamma^{2} = a\gamma + \gamma.$$

Thus  $a + a^2 + a^4 + a^8 = a + (a\gamma + 1) + (a + \gamma) + (a\gamma + \gamma) = 1$  and hence

$$Tr(a) = \sum_{i=0}^{n-1} a^{2^i} = \sum_{j=0}^{\frac{n}{4}} (a + a^2 + a^{2^2} + a^{2^3})^{2^j} = \sum_{j=0}^{\frac{n}{4}} 1 = \frac{n}{4}$$

We set  $b = {}_{c}D_{a}F(0) = a^{-1} + \gamma$  and check Lemma 4.2. Then we have  $b \neq 0$ , since if  $a = \gamma^{-1} = \gamma^{2}$ then  $0 = a^{2} + \gamma a + 1 = \gamma$  which is a contradiction. We also have  $ab + c + 1 = a(a^{-1} + \gamma) + \gamma + 1 = \gamma(a+1) \neq 0$ , since if a = 1 then  $0 = a^{2} + \gamma a + 1 = \gamma$  which is a contradiction. And (6) becomes

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{a(a^{-1}+\gamma)\gamma}{\gamma^2(a+1)^2}\right) = \operatorname{Tr}\left(\frac{(a\gamma+1)\gamma}{a\gamma^3}\right) = \operatorname{Tr}\left(\frac{a^2\gamma}{a}\right)$$
$$= \operatorname{Tr}(a\gamma) = \operatorname{Tr}(a^2+1) = \operatorname{Tr}(a)$$

if and only if  $n \equiv 0 \pmod{8}$ . We can easily check that  $a \notin \{0, 1, \gamma, \gamma + 1\} = \mathbb{F}_4$  if  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and  $a^2 + a\gamma + 1 = 0$ . Using  $b + c + 1 = a^{-1} + 1$  and  $\gamma(b\gamma + c + 1) = a^{-1}\gamma^2 + \gamma^3 + \gamma^2 + \gamma = a^{-1}\gamma^2$ , (7) becomes

$$\begin{aligned} a(b+c) + b + c + 1 &= a \cdot a^{-1} + a^{-1} + 1 = a^{-1} \neq 0 \\ a(b+1) + b + c + 1 &= a(a^{-1} + \gamma + 1) + a^{-1} + 1 = a\gamma + a + a^{-1} = a^{-1}\gamma^2(a^2 + \gamma) \neq 0 \\ (b\gamma + c)a + \gamma(b\gamma + c + 1) &= a(a^{-1}\gamma + 1) + a^{-1}\gamma^2 = a^{-1}(a^2 + \gamma a + \gamma^2) = a^{-1}\gamma \neq 0 \\ (b\gamma + 1)a + \gamma(b\gamma + c + 1) &= a\gamma(a^{-1} + 1) + a^{-1}\gamma^2 = a^{-1}\gamma(a^2 + a + \gamma) = a^{-1}(a+1) \neq 0 \end{aligned}$$

Note that  $\gamma^2 \Delta_F = \gamma^{-1} \Delta_F = \gamma \Delta_F = 5$  in this case.

• Now we assume that  $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$  and  $a = \frac{c\gamma + \gamma + 1}{c\gamma + c + 1}$ . We substitute  $a = \frac{c\gamma + \gamma + 1}{c\gamma + c + 1}$  to the first equation to get

$$0 = c(c\gamma + \gamma + 1)^2 + c\gamma(c\gamma + c + 1)(c\gamma + \gamma + 1) + \gamma(c\gamma + c + 1)^2$$
  
=  $\gamma^3 c^3 + \gamma^2 c^2 + (\gamma + 1)c + \gamma$ 

We have the same results when we substitute  $a = \frac{c\gamma+\gamma+1}{c\gamma+c+1}$  to the last two equations. We set  $b = {}_{c}D_{a}F(0) = \frac{c^{2}\gamma+1}{c\gamma+\gamma+1}$  check Lemma 4.2. If  $c^{2}\gamma = 1$  then  $= \gamma^{3}c^{3} + \gamma^{2}c^{2} + (\gamma+1)c + \gamma = (\gamma^{2} + \gamma + 1)c$ , which is a contradiction to  $c \neq 0$  and  $\gamma \notin \mathbb{F}_{4}$ . Hence we have  $b \neq 0$ . Moreover,

$$ab + c + 1 = \frac{c^2\gamma + 1 + (c+1)(c\gamma + c + 1)}{c\gamma + c + 1} = \frac{c(c+\gamma)}{c\gamma + c + 1} \neq 0$$

if and only if  $c \neq \gamma$ . And (6) becomes

$$0 = \operatorname{Tr}\left(\frac{abc}{(ab+c+1)^2}\right) = \operatorname{Tr}\left(\frac{\frac{c(c^2\gamma+1)}{c\gamma+c+1}}{\frac{c^2(c+\gamma)^2}{(c\gamma+c+1)^2}}\right) = \operatorname{Tr}\left(\frac{(c\gamma+c+1)(c^2\gamma+1)}{c(c+\gamma)^2}\right).$$

Using  $b + c = \frac{c\gamma + c + 1}{c\gamma + \gamma + 1} = a^{-1}$  and hence  $b + c + 1 = \frac{c + \gamma}{c\gamma + \gamma + 1}$  and  $\gamma(b\gamma + c + 1) = \frac{c^2 \gamma^2(\gamma + 1) + c\gamma + \gamma}{c\gamma + \gamma + 1}$ , (7) becomes

$$\begin{split} a(b+c) + b + c + 1 &= a \cdot a^{-1} + a^{-1} + 1 = a^{-1} \neq 0 \\ a(b+1) + b + c + 1 &= \frac{c\gamma + \gamma + 1}{c\gamma + c + 1} \cdot \frac{\gamma(c^2 + c + 1)}{c\gamma + \gamma + 1} + \frac{c + \gamma}{c\gamma + \gamma + 1} = \frac{\gamma^2 c^3 + c^2 + (\gamma + 1)^2 c + \gamma^2}{(c\gamma + c + 1)(c\gamma + \gamma + 1)} \\ &= \frac{\gamma^3 c^3 + \gamma c^2 + \gamma(\gamma + 1)^2 c + \gamma^3}{\gamma(c\gamma + c + 1)(c\gamma + \gamma + 1)} = \frac{(\gamma^2 + \gamma)c^2 + (\gamma^3 + 1)c + \gamma^3 + \gamma}{\gamma(c\gamma + c + 1)(c\gamma + \gamma + 1)} \\ &= \frac{(\gamma + 1)(c + \gamma)(\gamma c + \gamma + 1)}{\gamma(c\gamma + c + 1)(c\gamma + \gamma + 1)} = \frac{(\gamma + 1)(c + \gamma)}{\gamma(c\gamma + c + 1)} \neq 0 \\ (b\gamma + c)a + \gamma(b\gamma + c + 1) = \frac{c\gamma + \gamma + 1}{c\gamma + c + 1} \cdot \frac{c^2\gamma(\gamma + 1) + c(\gamma + 1) + \gamma}{c\gamma + \gamma + 1} = \frac{(\gamma + 1)\gamma^3 c^3 + (\gamma + 1)\gamma c^2 + (\gamma + 1)^2 c + \gamma^2}{(c\gamma + c + 1)(c\gamma + \gamma + 1)} \\ &= \frac{(\gamma + 1)(\gamma^3 c^3 + \gamma^2 c^2 + (\gamma + 1)c) + \gamma^2(\gamma + 1)c^2 + \gamma^2}{(c\gamma + c + 1)(c\gamma + \gamma + 1)} \\ &= \frac{\gamma^2(\gamma + 1)c^2 + \gamma}{(c\gamma + c + 1)(c\gamma + \gamma + 1)} = \frac{\gamma(\gamma(\gamma + 1)c^2 + 1)}{(c\gamma + c + 1)(c\gamma + \gamma + 1)} \end{split}$$

$$\begin{split} (b\gamma+1)a + \gamma(b\gamma+c+1) &= \frac{c\gamma+\gamma+1}{c\gamma+c+1} \cdot \frac{c^2\gamma^2+c\gamma+1}{c\gamma+\gamma+1} + \frac{c^2\gamma^2(\gamma+1)+c\gamma+\gamma}{c\gamma+\gamma+1} \\ &= \frac{(\gamma^2+\gamma+1)\gamma^2c^3+\gamma c^2+1}{(c\gamma+c+1)(c\gamma+\gamma+1)} = \frac{(\gamma^2+\gamma+1)\gamma^3c^3+\gamma^2c^2+\gamma}{\gamma(c\gamma+c+1)(c\gamma+\gamma+1)} \\ &= \frac{(\gamma^2+\gamma+1)(\gamma^2c^2+(\gamma+1)c+\gamma)+\gamma^2c^2+\gamma}{\gamma(c\gamma+c+1)(c\gamma+\gamma+1)} \\ &= \frac{(\gamma+1)\gamma^3c^2+(\gamma+1)(\gamma^2+\gamma+1)c+\gamma^2(\gamma+1)}{\gamma(c\gamma+c+1)(c\gamma+\gamma+1)} \\ &= \frac{(\gamma+1)(\gamma^3c^2+(\gamma^2+\gamma+1)c+\gamma^2)}{\gamma(c\gamma+c+1)(c\gamma+\gamma+1)} \end{split}$$

Hence we require  $c \neq \frac{1}{\gamma^{2^{n-1}} + \gamma}$  and  $\gamma^3 c^2 + (\gamma^2 + \gamma + 1)c + \gamma^2 \neq 0$ . It remains to check  $a = \frac{c\gamma + \gamma + 1}{c\gamma + c + 1} \notin \{0, 1, \gamma, \gamma + 1\}$ . If a = 0 then we have  $c\gamma = \gamma + 1$  or  $c = \frac{\gamma + 1}{\gamma}$  and hence we have  $0 = (c\gamma)^3 + (c\gamma)^2 + (\gamma + 1)c + \gamma = \frac{(\gamma^2 + \gamma + 1)^2}{\gamma}$  which is a contradiction to  $\gamma \notin \mathbb{F}_4$ . If a = 1 then we have  $c = \gamma$  and then we have  $ab + c + 1 \neq 0$ . If  $a = \gamma$  then we have  $0 = (c\gamma + \gamma + 1) + \gamma(c\gamma + c + 1) = c\gamma^2 + 1$ , but we already see that  $c\gamma^2 + 1 \neq 0$ . If  $a = \gamma + 1$  then we have  $0 = (c\gamma + \gamma + 1) + (\gamma + 1)(c\gamma + c + 1) = c(\gamma^2 + \gamma + 1)$  which is a contradiction to  $\gamma \notin \mathbb{F}_4$ .

• We exchange c by  $c^{-1}$  in the above analysis to have  $a = \frac{c^{-1}\gamma + \gamma + 1}{c^{-1}\gamma + c^{-1} + 1} = \frac{c\gamma + c + \gamma}{c + \gamma + 1}$  and  $b = \frac{(c^{-1})^2\gamma + 1}{c^{-1}\gamma + \gamma + 1} = \frac{c^2 + \gamma}{c^2(\gamma + 1) + c\gamma}$ . Then  $_{c^{-1}}D_aF(x) = b$  has three solutions in  $P_a$  if  $x = c^{-1}$  is a solution of  $\gamma^3 x^3 + \gamma^2 x^2 + (\gamma + 1)x + 1 = 0$  and hence  $c^3 + (\gamma + 1)c^2 + \gamma^2 c + \gamma^3 = 0$ . Similarly, by Lemma 4.2,  $_{c^{-1}}D_aF(x) = b$  has two solutions in  $\mathbb{F}_{2^n} \setminus P_a$  if and only if

$$0 = \operatorname{Tr}\left(\frac{(c^{-1}\gamma + c^{-1} + 1)((c^{-1})^{2}\gamma + 1)}{c^{-1}(c^{-1} + \gamma)^{2}}\right) = \operatorname{Tr}\left(\frac{(\gamma + c + 1)(c^{2} + \gamma)}{(c\gamma + 1)^{2}}\right)$$

and  $c \neq \gamma^{2^{n-1}} + \gamma$  and  $\gamma^2 c^2 + (\gamma^2 + \gamma + 1)c + \gamma^3 \neq 0$ .

By Lemma 2.5,  $b = {}_{c}D_{a}F(u_{1}) = {}_{c}D_{a}F(u_{2}) = {}_{c}D_{a}F(u_{3})$  if and only if  $bc^{-1} = {}_{c^{-1}}D_{a}F(u_{1}+a) = {}_{c^{-1}}D_{a}F(u_{2}+a) = {}_{c^{-1}}D_{a}F(u_{3}+a)$  for all  $u_{1}, u_{2}, u_{3} \in \mathbb{F}_{2^{n}}$ , and hence it is enough to consider the above cases. Therefore, if conditions in this theorem are not satisfied, then  ${}_{c}D_{a} = b$  has at most 2 solutions in  $P_{a}$  or at most 1 solution in  $\mathbb{F}_{2^{n}} \setminus P_{a}$  and hence we have  ${}_{c}\Delta_{F} \leq 4$ .

Conversely, if each condition in this theorem holds, then we set a and b the same as in the above analysis in each case. By the above analysis in each case, we can see that  ${}_{c}D_{a}F(x) = b$  has 3 solutions in  $P_{a}$ . We can also see that  ${}_{c}D_{a}F(x) = b$  has 2 solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$  by Lemma 4.2. Therefore we have  ${}_{c}\Delta_{F}(a,b) = 5$  and hence  ${}_{c}\Delta_{F} = 5$  by Theorem 4.3, which completes the proof.

By Theorem 4.4, we can say that  $3 \leq {}_{c}\Delta_{F} \leq 4$  if and only if all the conditions in Theorem 4.4 do not hold. Next we give a simple characterization for the case  ${}_{c}\Delta_{F} = 3$ .

**Corollary 4.5.** We have 
$$_{c}\Delta_{F} = 3$$
 if  $c \notin \{\gamma, \gamma^{-1}, \gamma + 1, (\gamma + 1)^{-1}\}$  and  $\operatorname{Tr}\left(\frac{\gamma}{c(\gamma+1)}\right) = \operatorname{Tr}(c^{-1}\gamma^{-1}) = \operatorname{Tr}\left(\frac{\gamma(c\gamma+1)}{(\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c\gamma+c+1)^{2}}\right) = \operatorname{Tr}\left(\frac{\gamma(c+\gamma+1)}{c(\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{c\gamma^{2}}{(c+\gamma)^{2}}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{c$ 

n		5	6	7	8
# of $(c, \gamma)$ with $_c\Delta_F = 3$		10	28	196	672
# of $(c, \gamma)$ with $_{c}\Delta_{F} = 3$ satisfying Corollary 4.5	0	0	12	14	64

Table 2: Distribution of  $_{c}\Delta_{F}$  when  $4 \leq n \leq 8$ .

Proof. We can see in the proof of Theorem 4.4 that  ${}_{c}D_{a}F(u_{1}) \neq {}_{c}D_{a}F(u_{2})$  for all  $u_{1}, u_{2} \in P_{a}$  with  $u_{1} \neq u_{2}$  if all the above trace conditions hold. Thus  ${}_{c}D_{a}F(x) = b$  has at most one solution in  $P_{a}$  for all  $a \in \mathbb{F}_{2^{n}}$  and  $b \in \mathbb{F}_{2^{n}}$ . As observed in the proof of Theorem 4.4  ${}_{c}D_{a}F(x) = b$  has at most two solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$  for all  $a \in \mathbb{F}_{2^{n}}$  and  $b \in \mathbb{F}_{2^{n}}$ . Hence we have  ${}_{c}\Delta_{F}(a, b) \leq 3$  for all  $a \in \mathbb{F}_{2^{n}}$  and  $b \in \mathbb{F}_{2^{n}}$ . By Theorem 4.3, we complete the proof.

We already investigated the number of pairs  $(c, \gamma) \in (\mathbb{F}_{2^n} \setminus \mathbb{F}_2) \times (\mathbb{F}_{2^n} \setminus \mathbb{F}_2)$  that  ${}_{c}\Delta_F = 3$  in Table 1. In Table 2 we investigate the number of pairs  $(c, \gamma)$  with  ${}_{c}\Delta_F = 3$  can be obtained from Corollary 4.5. Unfortunately, the number of pairs  $(c, \gamma)$  that can be obtained by Corollary 4.5 is only a fraction of all the pairs  $(c, \gamma)$  with  ${}_{c}\Delta_F = 3$ . However, we need to investigate all the cases that  ${}_{c}D_aF(u_1) = {}_{c}D_aF(u_2)$  where  $u_1, u_2 \in P_a$  with  $u_1 \neq u_2$  to characterize all the pairs with  ${}_{c}\Delta_F = 3$ , which requires very routine computations.

Next we characterize c-differential uniformity of F in a special case that  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ .

**Lemma 4.6.** Let  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ ,  $a \in \mathbb{F}_4$  and  $b \in \mathbb{F}_{2^n}$ . Then,  ${}_c\Delta_F(a, b) = 4$  if and only if a = 1,  $b = \gamma$ ,  $c \neq \gamma^2$  and  $\operatorname{Tr}\left(\frac{c\gamma}{c^2+\gamma}\right) = 0$ . Otherwise,  ${}_c\Delta_F(a, b) \leq 3$ .

Proof. If a = 1 then we get  ${}_{c}D_{1}F(0) = \gamma^{2} + c$ ,  ${}_{c}D_{1}F(1) = {}_{c}D_{1}F(\gamma) = \gamma$  and  ${}_{c}D_{1}F(\gamma^{2}) = c\gamma$ . Since  $c \neq 1$ , we obtain that  $\gamma^{2} + c$ ,  $\gamma$  and  $c\gamma$  are pairwise distinct. If  $b = \gamma$  then x = 1 and  $x = \gamma$  are solutions of  ${}_{c}D_{1}F(x) = b$ . For  $x \notin \mathbb{F}_{4}$ ,  ${}_{c}D_{1}F(x) = b$  implies  $\gamma x^{2} + (c + \gamma^{2})x + c = 0$ . Note that if  $c \neq \gamma^{2}$  then  $\gamma x^{2} + (c + \gamma^{2})x + c = 0$  has no solutions in  $P_{a} = \mathbb{F}_{4} = \{0, 1, \gamma, \gamma + 1\}$ . Hence by Lemma 4.2 it has two solutions if and only if  $c \neq \gamma^{2}$  and  $0 = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^{2})^{2}}\right) = \operatorname{Tr}\left(\frac{c\gamma}{c^{2}+\gamma}\right)$ . Hence we get  ${}_{c}\Delta_{F}(1,\gamma) = 4$  if  $\operatorname{Tr}\left(\frac{c\gamma}{c^{2}+\gamma}\right) = 0$ .

If u = 0 or  $u = \gamma^2$ , then  ${}_cD_1F(x) = {}_cD_1F(u)$  has the unique solution x = u in  $\mathbb{F}_4$ . By Lemma 4.2,  ${}_cD_1F(x) = {}_cD_1F(u)$  has at most two solutions. If  $b \notin \{ {}_cD_1F(u) : u \in \mathbb{F}_4 \}$ , then we get  ${}_c\Delta_F(1,b) = {}_c\Delta_{Inv}(1,b) \leq 3$  by Theorem 2.2. Therefore, we get  ${}_c\Delta_F(\gamma,b) \leq 3$  for all  $b \in \mathbb{F}_{2^n}$  with  $b \neq \gamma$ .

If  $a = \gamma$ , then we get  ${}_{c}D_{\gamma}F(0) = c$ ,  ${}_{c}D_{\gamma}F(1) = \gamma + c\gamma^{2}$ ,  ${}_{c}D_{\gamma}F(\gamma) = 1$  and  ${}_{c}D_{\gamma}F(\gamma^{2}) = \gamma^{2} + c\gamma$ . Since  $c \neq 1$ , we obtain that  $\gamma + c$ ,  $c\gamma^{2}$ ,  $\gamma^{2}$  and  $1 + c\gamma$  are pairwise distinct (because if two of them are same then we get c = 1, a contradiction). Thus  ${}_{c}D_{\gamma}F(x) = {}_{c}D_{\gamma}F(u)$  has the unique solution x = u in  $\mathbb{F}_{4}$  and at most two solutions in  $x \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$ , by Lemma 4.2. Hence we have  ${}_{c}\Delta_{F}(\gamma, b) \leq 3$  for all  $b \in \mathbb{F}_{2^{n}}$ .

If  $a = \gamma^2$  then we get  ${}_cD_{\gamma^2}F(0) = \gamma + c, {}_cD_{\gamma^2}F(1) = c\gamma^2, {}_cD_{\gamma^2}F(\gamma) = \gamma^2$  and  ${}_cD_{\gamma^2}F(\gamma^2) = 1 + c\gamma$ . Since  $c \neq 1$ , we obtain that  $\gamma + c, c\gamma^2, \gamma^2$  and  $1 + c\gamma$  are pairwise distinct (If two of them are same then we get c = 1, a contradiction). Similar with the case  $a = \gamma$ , we have  ${}_c\Delta_F(\gamma^2, b) \leq 3$  for all  $b \in \mathbb{F}_{2^n}$ . **Theorem 4.7.** Let n be even and  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ . If  $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ , then

$${}_{c}\Delta_{F} = \begin{cases} 3 & if \ n \equiv 2 \pmod{4}, \\ 4 & if \ n \equiv 4 \pmod{8}, \\ 5 & if \ n \equiv 0 \pmod{8}. \end{cases}$$

*Proof.* By Theorem 4.4 we have  $_c\Delta_F = 5$  if and only if  $n \equiv 0 \pmod{8}$ . Otherwise we have  $3 \leq _c\Delta_F \leq 4$  by Theorem 4.3 and Theorem 4.4. By Lemma 2.5, it is sufficient to consider the case  $c = \gamma$ .

(Case 1) Assume that  $n \equiv 2 \pmod{4}$ . By Lemma 4.6 we have  ${}_{c}\Delta_{F}(a,b) \leq 3$  for all  $a \in \mathbb{F}_{4}$  and  $b \in \mathbb{F}_{2^{n}}$ , since  $\operatorname{Tr}\left(\frac{c\gamma}{c^{2}+\gamma}\right) = \operatorname{Tr}(\gamma^{2}) = 1$ . Hence it is sufficient to consider the case that  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$ . Using the proof of Theorem 4.4 we have the followings :

- $_{c}D_{a}F(0) \neq _{c}D_{a}F(1)$  since  $\operatorname{Tr}\left(\frac{\gamma(c\gamma+1)}{(\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{\gamma}{\gamma(\gamma+1)}\right) = \operatorname{Tr}(\gamma) = 1$
- $_{c}D_{a}F(0) \neq _{c}D_{a}F(\gamma)$  since  $\operatorname{Tr}(c^{-1}\gamma^{-1}) = \operatorname{Tr}(\gamma) = 1$
- ${}_{c}D_{a}F(0) \neq {}_{c}D_{a}F(a+1)$  since  $\operatorname{Tr}\left(\frac{\gamma(c\gamma+1)}{(\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{\gamma(\gamma^{2}+1)}{(\gamma+1)^{2}}\right) = \operatorname{Tr}(\gamma) = 1$
- ${}_{c}D_{a}F(0) \neq {}_{c}D_{a}F(a+\gamma)$  since if  ${}_{c}D_{a}F(0) = {}_{c}D_{a}F(a+\gamma)$  then we have a = 1, a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$
- $_{c}D_{a}F(1) \neq _{c}D_{a}F(\gamma)$  since  $\operatorname{Tr}\left(\frac{\gamma(c+\gamma+1)}{c(\gamma+1)^{2}}\right) = \operatorname{Tr}\left(\frac{1}{\gamma^{4}}\right) = \operatorname{Tr}(\gamma^{2}) = 1$
- ${}_{c}D_{a}F(1) \neq {}_{c}D_{a}F(a)$  since if  ${}_{c}D_{a}F(1) = {}_{c}D_{a}F(a)$  then we have  $a = \gamma^{2}$ , a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$
- ${}_{c}D_{a}F(1) \neq {}_{c}D_{a}F(a+\gamma)$  since if  ${}_{c}D_{a}F(1) = {}_{c}D_{a}F(a+\gamma)$  then we have  $a = \gamma^{2}$ , a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$

• 
$$_{c}D_{a}F(\gamma) \neq _{c}D_{a}F(a)$$
 since  $\operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma+1)^{2}}\right) = \operatorname{Tr}(\gamma^{2}) = 1$ 

- $_{c}D_{a}F(\gamma) \neq _{c}D_{a}F(a+1)$  since  $\operatorname{Tr}\left(\frac{c\gamma^{2}}{(c\gamma+1)^{2}}\right) = \operatorname{Tr}(\gamma) = 1$
- ${}_{c}D_{a}F(a) \neq {}_{c}D_{a}F(a+1)$  since if  ${}_{c}D_{a}F(a) = {}_{c}D_{a}F(a+1)$  then we have  $a^{2} + a + 1 = 0$ , a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$
- ${}_{c}D_{a}F(a) \neq {}_{c}D_{a}F(a+\gamma)$  since if  ${}_{c}D_{a}F(a) = {}_{c}D_{a}F(a+\gamma)$  then we have  $a^{2} + \gamma a + \gamma^{2} = 0$  and then  $a \in \{1, 1+\gamma\}$ , a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$
- ${}_{c}D_{a}F(a+1) \neq {}_{c}D_{a}F(a+\gamma)$  since if  ${}_{c}D_{a}F(a+1) = {}_{c}D_{a}F(a+\gamma)$  then we have  $a = \gamma + 1$ , a contradiction to  $a \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$

Hence  ${}_{c}D_{a}F(x) = b$  has at most one solution in  $P_{a}$ . Since  ${}_{c}D_{a}F(x) = b$  has at most two solutions in  $\mathbb{F}_{2^{n}} \setminus P_{a}$ , we obtain  ${}_{c}\Delta_{F}(a,b) \leq 3$ .

(Case 2) Assume that  $n \equiv 4 \pmod{8}$ . Then by Lemma 4.6 we have  ${}_{c}\Delta_{F}(1,\gamma) = 4$  since  $\operatorname{Tr}\left(\frac{c\gamma}{c^{2}+\gamma}\right) = \operatorname{Tr}(\gamma^{2}) = 0$ . Therefore, we have  ${}_{c}\Delta_{F} = 4$  in this case.

n		6	8	10	12
# of $(c, \gamma)$ with $_c\Delta_F = 3$	4	0	8	20	136
# of $(c, \gamma)$ with $_{c}\Delta_{F} = 3$ satisfying Corollary 4.8	0	0	8	10	84

Table 3: The number of  $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$  when  $4 \leq n \leq 12$ .

Next we propose a sufficient condition for  ${}_{c}\Delta_{F} = 3$  in case  $\gamma \in \mathbb{F}_{4} \setminus \mathbb{F}_{2}$  using Corollary 4.5.

**Corollary 4.8.** Let n be even and  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ . If  $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ , then  $3 \leq c\Delta_F \leq 4$ . Furthermore,  $c\Delta_F = 3$  if  $\operatorname{Tr}(c\gamma) = \operatorname{Tr}(c\gamma^2) = \operatorname{Tr}(c^{-1}\gamma) = \operatorname{Tr}(c^{-1}\gamma^2) = \operatorname{Tr}\left(\frac{c}{(c+\gamma)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma^2}{(c+\gamma)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^2)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^2)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^2)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^2)^2}\right) = 1.$ 

Proof. By Theorem 4.4 if  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$  then  ${}_c\Delta_F = 5$  if and only if  $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$  and  $n \equiv 0 \pmod{8}$ . Hence if  $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$  then we have  $3 \leq {}_c\Delta_F \leq 4$  using Theorem 4.3. If  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$  and  $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$  then we have  $c \notin \{\gamma, \gamma + 1, \gamma^{-1}, (\gamma + 1)^{-1}\}$ . Using  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$  and  $\operatorname{Tr}(1) = 0$  we check all trace conditions in Corollary 4.5

$$\begin{aligned} \operatorname{Tr}\left(\frac{\gamma}{c(\gamma+1)}\right) &= \operatorname{Tr}(c^{-1}\gamma^{-1}) = 1 & \operatorname{Tr}(c^{-1}\gamma^{-1}) = 1 \\ \operatorname{Tr}\left(\frac{\gamma(c\gamma+1)}{(\gamma+1)^2}\right) &= \operatorname{Tr}(c\gamma+1) = \operatorname{Tr}(c\gamma) = 1 & \operatorname{Tr}\left(\frac{c\gamma}{(c\gamma+c+1)^2}\right) = \operatorname{Tr}\left(\frac{c}{(c+\gamma)^2}\right) = 1 \\ \operatorname{Tr}\left(\frac{\gamma(c+\gamma+1)}{c(\gamma+1)^2}\right) &= \operatorname{Tr}\left(\frac{c+\gamma^2}{c}\right) = \operatorname{Tr}(c^{-1}\gamma^2) = 1 & \operatorname{Tr}\left(\frac{\gamma(c+\gamma)}{c(\gamma+1)^2}\right) = \operatorname{Tr}\left(\frac{c+\gamma}{c}\right) = \operatorname{Tr}(c^{-1}\gamma) = 1 \\ \operatorname{Tr}\left(\frac{c\gamma^2}{(c+\gamma)^2}\right) &= 1 & \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma+1)^2}\right) = \operatorname{Tr}\left(\frac{c\gamma}{(c+\gamma^2)^2}\right) = 1 \\ \operatorname{Tr}\left(\frac{c\gamma^2}{(c\gamma+1)^2}\right) &= \operatorname{Tr}\left(\frac{c}{(c+\gamma^2)^2}\right) = 1 & \operatorname{Tr}\left(\frac{c\gamma}{\gamma+1}\right) = \operatorname{Tr}(c\gamma^2) = 1 \\ \operatorname{Tr}(c\gamma^{-1}) &= \operatorname{Tr}(c\gamma^2) = 1 & \operatorname{Tr}\left(\frac{(c\gamma+c+1)\gamma}{(\gamma+1)^2}\right) = \operatorname{Tr}(c\gamma^2+1) = \operatorname{Tr}(c\gamma^2) = 1 \end{aligned}$$

and hence we have  $_{c}\Delta_{F} = 3$  by Corollary 4.5, which completes the proof.

The trace conditions in Corollary 4.8 are not necessary for  ${}_{c}\Delta_{F} = 3$ . The third row of Table 3 indicates the number of  $c \in \mathbb{F}_{2^{n}} \setminus \mathbb{F}_{4}$  with  ${}_{c}\Delta_{F} = 3$  satisfying all the trace conditions in Corollary 4.8 for each  $4 \leq n \leq 12$ .

### 5 Concluding Remark

In this paper, we study c-differential uniformity of permutations with low Carlitz rank. We show that a permutation of Carlitz rank m has c-differential uniformity at most m+2. Hence we can see that a permutation of low Carlitz rank has low c-differential uniformity. We observe that this upper bound m+2 on c-differential uniformity of permutations with Carlitz rank m is tight when  $1 \le m \le 3$ . In particular, we investigate c-differential uniformity of permutations of the form  $Inv \circ (0, 1, \gamma)$ , which have the same c-differential uniformity with some permutations with Carlitz rank 3. We can see that  $3 \le c\Delta_F \le 5$ , and we characterize the case  $c\Delta_F = 5$  and give a sufficient condition for  $c\Delta_F = 3$ . We also give a refined chracterization of  $c\Delta_F$  for the special case that n is even and  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ .

The proof of an upper bound on c-differential uniformity of permutations with Carlitz rank m is based on the fact that they are affine equivalent (of degree one) to the inverse function with m

modified points. Since all permutations modifying a small set of points from Inv has low Carlitz rank, we already show that they also have low *c*-differential uniformity. In future studies, we investigate the *c*-differential uniformity of them in detail.

Acknowledgements : This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1C1C2003888). Soonhak Kwon was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2016R1A5A1008055, No. 2019R1F1A1058920 and 2021R1F1A1050721).

### References

- E. Aksoy, A. Cesmelioglu, W. Meidl and A. Topuzoğlu, On the Carlitz rank of permutation polynomials, Finite Fields Appl., Vol. 15, pp. 428-440, 2009. DOI: 10.1016/j.ffa.2009.02.006
- [2] D. Bartoli, and M. Calderini, On construction and (non)existence of c-(almost) perfect nonlinear functions, Finite Fields Appl., Vol. 72, 101835, 2021. DOI: 10.1016/j.ffa.2021.101835
- [3] D. Bartoli, M. Calderini, C. Riera, and P. Stănică, Low c-differential uniformity for functions modified on subfields, Cryptogr. Commun., in press. DOI : 10.1007/s12095-022-00554-x
- [4] N. Borisov, M. Chew, R. Johnson, and D. Wagner, *Multiplicative Differentials*, FSE 2002, Lect. Notes Comput. Sci. Vol. 2365, pp.17-33, 2002. DOI: 10.1007/3-540-45661-9\_2
- [5] C. Boura, and A. Canteaut, On the Boomerang Uniformity of Cryptographic Sboxes. IACR Trans. on Symm. Cryptol., Vol. 2018, issue 3, pp. 290-310, 2018. DOI : 10.13154/tosc.v2018.i3.290-310
- [6] A. Canteaut, L. Kölsch, C. Li, C. Li, K. Li, L. Qu, and F. Wiemer, Autocorrelations of Vectorial Boolean Functions, Latincrypt 2021, Lect. Notes Comput Sci. Vol. 12912, pp.233-253, 2021. DOI : 10.1007/978-3-030-88238-9\_12
- [7] P. Ellingsen, P. Felke, C. Riera, P. Stănică, and A. Tkachenko, *c-Differentials, Multiplicative Uniformity, and (Almost) Perfect c-Nonlinearity*, IEEE Trans. Inf. Theory, Vol. 66, No. 9, pp.5781-5789, 2020. DOI: 10.1109/TIT.2020.2971988
- [8] S. U. Hasan, M. Pal, C. Riera, and P. Stănică, On the c-differential uniformity of certain maps over finite fields, Des. Codes Cryptogr., Vol. 89, issue 2, pp.221-239, 2021. DOI : 10.1007/s10623-020-00812-0
- [9] J. Jeong, N. Koo, and S. Kwon, On Boomerang Uniformity of Permutations of Low Carlitz Rank, a preprint, available at http://arxiv.org/abs/2009.08612.
- [10] J. Jeong, N. Koo, and S. Kwon, New differentially 4-uniform permutations from modifications of the inverse function, Finite Fields Appl., Vol. 77, 101931, 2022. DOI: 10.1016/j.ffa.2021.101931
- [11] J. Jeong, N. Koo, and S. Kwon, Constructing differentially 4-uniform involutions over  $\mathbb{F}_{2^{2k}}$  by using Carlitz form, Finite Fields Appl., Vol. 78, 101957, 2022. DOI : 10.1016/j.ffa.2021.101957

- [12] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inf. Theory Vol. 36, No 3, pp. 686-692 ,1990 DOI: 10.1109/18.54892
- [13] K. Li, L. Qu, B. Sun, and C. Li, New Results about the Boomerang Uniformity of Permutation Polynomials, IEEE Trans. Inf. Theory, Vol. 65 (2019) 7542-7553, 2019. DOI : 10.1109/TIT.2019.2918531
- [14] Y. Li, M. Wang and Y. Yu, Constructing Differentially 4-uniform Permutations over  $GF(2^{2k})$ from the Inverse Function Revisited, IACR ePrint Archieve 2013/731.
- [15] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Applied and Computational Mathematics. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-540-70529-1\_192
- [16] S. Mesnager, C. Riera, P. Stănică, H. Yan, and Z. Zhou, *Investigations on c-(Almost) Perfect Nonlinear Functions*, IEEE Trans. Inf. Theory, Vol. 67, No. 10, pp. 6916-6925, 2021. DOI: 10.1109/TIT.2021.3081348
- [17] K. Nyberg, Differentially uniform mappings for cryptography, EUROCRYPT '93, Lect. Notes Comput. Sci. Vol. 765, pp. 55-64, 1994. DOI : 10.1007/3-540-48285-7\_6
- [18] P. Stănică, Investigations on c-boomerang uniformity and perfect nonlinearity, Discrete Appl. Math., Vol. 304, pp.297-314, 2021. DOI : 10.1016/j.dam.2021.08.002
- [19] P. Stănică, Low c-differential and c-boomerang uniformity of the swapped inverse function, Discrete Math., Vol. 344, 112543, 2021. DOI : 10.1016/j.disc.2021.112543
- [20] P. Stănică, Low c-Differential Uniformity for the Gold Function Modified on a Subfield, Security and Privacy, Lecture Notes in Electrical Engineering, Vol. 744, pp.131-137, 2021. DOI: 10.1007/978-981-33-6781-4\_11
- [21] Z. Tu, X. Zeng, Y. Jiang, and X. Tang, A class of APcN power functions over finite fields of even characteristic, a preprint, available at https://arxiv.org/abs/2107.06464v1.
- [22] X. Wang, and D. Zheng, Several classes of PcN power functions over finite fields, a preprint, available at https://arxiv.org/abs/2104.12942v1.
- [23] Y. Wu, N. Li, and X. Zeng, New PcN and APcN functions over finite fields, Des. Codes Cryptogr., Vol. 89, issue 11, pp. 2637-2651, 2021. DOI : 10.1007/s10623-021-00946-9
- [24] H. Yan, On (-1)-differential uniformity of ternary APN power functions, Cryptogr. Commun., in press, 2021. DOI: 10.1007/s12095-021-00526-7
- [25] Z. Zha, and L. Hu, Some classes of power functions with low c-differential uniformity over finite fields, Des. Codes Cryptogr., Vol. 89, Issue 6, pp.1193-1210, 2021. DOI : 10.1007/s10623-021-00866-8
- [26] K. Zhang, and H. Yan, On the c-differential spectrum of power functions over finite fields, a preprint, available at : https://arxiv.org/abs/2201.06172v1