On Differentially 4-uniform Permutations with Low Carlitz Rank

Jaeseong Jeong, Namhun Koo, Soonhak Kwon

Email: wotjd012321@naver.com, komaton@skku.edu, shkwon@skku.edu
Applied Algebra and Optimization Research Center,
Sungkyunkwan University, Suwon, Republic of Korea

Abstract

Finding permutation polynomials with low differential uniformity is an important topic in S-box designs of many block ciphers. For example, AES chooses the differentially 4-uniform inverse function as its S-box. This inverse function has good cryptographic properties with high algebraic degree and nonlinearity. Therefore, many variants of the inverse function has been researched ([5,6,8–10]). In this paper, we characterize the differential uniformity of a permutation polynomial having low Carlitz rank. We show that permutation of low Carlitz rank is affine equivalent to cycle or composition of cycle and the inverse function. As a result, we give a classification of the differential uniformity of the permutation polynomials of Carlitz rank at most 4 and we present new classes of differentially 4-uniform permutation polynomials.

1 Introduction

A **Boolean function** of n variables is a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ and an **vectorial boolean function** ((n, m)**-function** or **S-box**) is a function $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ where $\mathbb{F}_{2^n}$ is denoted by finite field with 2^n elements. For a given function $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, the **difference distribution table**, denoting $\mathtt{DDT}_F$, whose entries are given as

$$\mathtt{DDT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : F(x) + F(x + a) = b\},$$

where $\#A$ denotes the cardinality of a set A. The function F is **differential δ-uniform** if $\Delta_F \leq \delta$ where

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n} \setminus \{0\},\ b \in \mathbb{F}_{2^n}} \mathtt{DDT}(a, b),$$

and Δ_F is called **differential uniformity** of F. It is clear that the smallest value of Δ_F is 2 and such function is called **Almost perfect nonlinear** (**APN**) function. APN permutations play a important role in designing S-box. But finding an APN permutation is very difficult, so finding differential 4-uniform permutation has been studied actively. ([5, 6, 8–10])

Now we introduce the Carlitz rank of permutation. We let denote $[a_0, a_1, \ldots, a_m]$ continued fraction

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

where $a_i \in \mathbb{F}_{2^n}$. We identify x^{2^n-2} with x^{-1} over $\mathbb{F}_{2^n}$ by defining as $0^{-1} = 0$. It is known that for any permutation $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, there is $m \geq 0$ and $a_i \in \mathbb{F}_{2^n}$, $0 \leq i \leq m$ such that

$$\begin{aligned} F(x) &= [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x] \\ &= (\cdots((a_0 x + a_1)^{-1} + a_2)^{-1} \cdots + a_m)^{-1} + a_{m+1}, \end{aligned} \tag{1}$$

where $a_0, a_2, \cdots, a_m \neq 0$([4]). For a given F, the above expression is not unique in general. However there is the least m among all possible expressions of F. The **Carlitz rank** of F is the least integer m satisfying the above expression. Suppose that a permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has Carlitz rank $\leq m$. Then one may write F as the form of Eq.(1). For given F and $0 \leq k \leq m$, we define

$$\begin{aligned} F_k(x) &= [a_{k+1}, a_k, \ldots, a_2, a_1 + a_0 x] \\ &= (\cdots((a_0 x + a_1)^{-1} + a_2)^{-1} \cdots + a_k)^{-1} + a_{k+1} \end{aligned}$$

Then one has $F_0(x) = a_0 x + a_1, F_1(x) = (a_0 x + a_1)^{2^n-2} + a_2, \cdots, F_m = F$. Also we inductively define $R_k(x)$ for $0 \leq k \leq m$ as follows

$$R_k(x) = \frac{\alpha_{k+1} x + \beta_{k+1}}{\alpha_k x + \beta_k}, \tag{2}$$

where

$$\alpha_{k+1} = a_{k+1}\alpha_k + \alpha_{k-1}, \;\; \beta_{k+1} = a_{k+1}\beta_k + \beta_{k-1} \quad (1 \leq k \leq m)$$

with the initial conditions $\alpha_0 = 0, \alpha_1 = a_0$ and $\beta_0 = 1, \beta_1 = a_1$. Then it is known [4] that

$$R_k(x) = F_k(x) \text{ for all } x \notin \mathbf{O}_k \quad \left(\mathbf{O}_k = \left\{ x_i = \frac{\beta_i}{\alpha_i} : i = 1, \ldots, k \right\}, \mathbf{O}_k \subset \mathbb{F}_{2^n} \cup \{\infty\} \right)$$

where $x_i's$ are called **poles** of F_k and $x_i = \infty$ if and only if $\alpha_i = 0$.

2 Carlitz rank and inverse function

Two functions $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ and $F' : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ are called **affine equivalent** if there exist affine permutations A_1, A_2 satisfying $F' = A_1 \circ F \circ A_2$. (for details, see [1–3]) It is well-known that two affine equivalent functions have same differential uniformity.

Lemma 2.1. *A permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with Carlitz rank $\leq m$ is affine equivalent to inverse function Inv with at most m exceptional points. That is, there is a subset $U \subset \mathbb{F}_{2^n}$ with $\#U \leq m$ and affine permutations $\ell_1, \ell_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfying $\ell_2 \circ F \circ \ell_1(x) = \frac{1}{x}$ for all $x \notin U$.*

As a consequence of the above result, cryptographic properties of a permutation of low Carlitz rank are closely related with those of inverse function modified at some small set of points. In subsequent sections, we discuss cryptographic properties of a permutation of low Carlitz rank.

3 Differential uniformity

Before finding the differential uniformity of $F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x]$ on $\mathbb{F}_{2^n}$, we can set $a_0 = 1, a_1 = 0, a_2 = 1$ without loss of generality by the follwing proposition.

Proposition 3.1. *Let $F(x) = [a_{m+1}, a_m, \ldots, a_2, a_1 + a_0 x]$ on $\mathbb{F}_{2^n}$ where $a_0, a_2, \cdots, a_m \neq 0$.*
(i) If $m = 1$ then F is affine equivalent to G, given by $G(x) = x^{-1}$ on $\mathbb{F}_{2^n}$.
(ii) If $m \geq 2$ then F is affine equivalent to G, given by

$$G(x) = [0, \gamma_m, \ldots, \gamma_1, x] = (\cdots((x^{2^n-2} + \gamma_1)^{2^n-2} + \gamma_2)^{2^n-2} \cdots + \gamma_m)^{2^n-2}$$

where $\gamma_1 = 1$ and $\gamma_i = a_2^{(-1)^i} a_{i+1}$ for $i \geq 2$.

From now on we set

$$F(x) = [0, a_m, \ldots, a_3, 1, x], \tag{3}$$

Now we denote

$$A_i = [0, 1, a_3, \cdots, a_i] \text{ for } 1 \leq i \leq m, \tag{4}$$

i.e. $A_1 = [0], A_2 = [0, 1], A_3 = [0, 1, a_3], \cdots, A_m = [0, 1, a_3, \ldots, a_m]$, and

$$A'_u = [0, 1, a_3, \ldots, a_m, u]. \tag{5}$$

Then we have the following lemma:

Lemma 3.2. *Let $F(x) = [0, a_m, \ldots, a_3, 1, x]$ on $\mathbb{F}_{2^n}$ with $a_3, \ldots, a_m \neq 0$. Then*

$$\mathtt{DDT}_F(a, b) = \mathtt{DDT}_{F^{-1}}(b, a) = \#\{u \in \mathbb{F}_{2^n} : A'_u + A'_{u+b} = a\}.$$

For given $a, b \in \mathbb{F}_{2^n} \setminus \{0\}$, we now define 4 partitions of $\{u \in \mathbb{F}_{2^n} : A'_u + A'_{u+b} = a\}$, denoted by $P(a, b)$, as follows :

$$\begin{aligned}
P_A(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \exists\ 1 \leq i, j \leq m\ A'_u = A_i,\ A'_{u+b} = A_j\} \\
P_B(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \nexists\ 1 \leq i \leq m\ A'_u = A_i,\ \exists\ 1 \leq j \leq m\ A'_{u+b} = A_j\} \\
P_{B'}(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \exists\ 1 \leq i \leq m\ A'_u = A_i,\ \nexists\ 1 \leq j \leq m\ A'_{u+b} = A_j\} \\
P_C(a,b) &= P(a,b) \cap \{u \in \mathbb{F}_{2^n} : \nexists\ 1 \leq i, j \leq m\ A'_u = A_i,\ A'_{u+b} = A_j\}
\end{aligned} \tag{6}$$

It is clear that

$$\mathtt{DDT}_F(a, b) = \#P(a, b) = \#P_A(a, b) + \#P_B(a, b) + \#P_{B'}(a, b) + \#P_C(a, b).$$

Moreover we have $\#P_B(a, b) = \#P_{B'}(a, b)$, so

$$\mathtt{DDT}_F(a, b) = \#P(a, b) = \#P_A(a, b) + 2\#P_B(a, b) + \#P_C(a, b).$$

We now use the notation

$$u_i = [0, a_m, a_{m-1}, \ldots, a_{i+1}],$$

which is the root of $[0, 1, a_3, \ldots, a_m, u] = [0, 1, \ldots, a_i]$, i.e $A'_u = A_i$. The following theorem implies how $P_A(a, b), P_B(a, b)$ and $P_C(a, b)$ are constructed.

Theorem 3.3. *Let $F(x) = [0, a_m, \ldots, a_3, 1, x]$ on $\mathbb{F}_{2^n}$ with $a_3, \ldots, a_m \neq 0$. Let $U = \{u_i : 1 \leq i \leq m\}$ of cardinality m' and we have $1 \leq i_1 < i_2 < \cdots < i_{m'} \leq m$ such that $U = \{u_{i_1}, u_{i_2}, \ldots, u_{i_{m'}}\}$. Then the followings are satisfied:*

(i) $\#P_A(a,b) = \begin{cases} 2 & \text{if } (a,b) \in \{(A_{i_j}+A_{i_k}, u_{i_j}+u_{i_k}) : 1 \le j < k \le m'\} \\ 0 & \text{otherwise} \end{cases}$

(ii) $\#P_B(a,b) = \#\left\{1 \le j \le m' : b + u_{i_j} = \dfrac{(a+A_{i_j})\alpha_{m-1} + \beta_{m-1}}{(a+A_{i_j})\alpha_m + \beta_m},\ b + u_{i_j} \notin U\right\}$

(iii) *If* $\alpha_m \neq 0$ *then* $\#P_C(a,b) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\frac{1}{ab\alpha_m^2}) = 1 \text{ or } p(u) = 0 \text{ for some } u \in U \\ 2 & \text{otherwise} \end{cases}$; *and*

If $\alpha_m = 0$ *then* $\#P_C(a,b) = \begin{cases} 2^n - 2m' + \#\{(j,k) : u_{i_j} + u_{i_k} = b\} & \text{if } b = a\alpha_{m-1}^2 \\ 0 & \text{otherwise.} \end{cases}$

where $p(u) = a\alpha_m^2 u^2 + ab\alpha_m^2 u + ab\alpha_m\alpha_{m-1} + a\alpha_{m-1}^2 + b$.

By using the previous thoerem, we get the upper or lower bound of the differential uniformity of F.

Corollary 3.4. *Let* $F(x) = [0, a_m, \ldots, a_3, 1, x]$ *on* $\mathbb{F}_{2^n}$ *with* $a_3, \ldots, a_m \neq 0$. *Let* $m' = \#\{A_i : 1 \le i \le m\}$. *Then the followings are satisfied :*

(i) *If* $\alpha_m \neq 0$ *then* $\Delta_F \le 2m' + 4$.

(ii) *If* $\alpha_m = 0$ *then* $\Delta_F \ge 2^n - 2m' + 2$.

3.1 Carlitz rank of 3

Throughout this section, let $F(x) = [0, c, 1, x]$ on $\mathbb{F}_{2^n}$, which is obtained by setting $m = 3$ and $a_3 = c$ in (3). Note that in case $c = 1$, we can easily show that $\Delta_F = 2^n$. Now we consider $c \neq 1$ case, then we obtain the coefficients given by Table 1.

Table 1: The coefficients related with $F(x) = [0, c, 1, x]$ on $\mathbb{F}_{2^n}$ with $c \neq 1$.

i	0	1	2	3
α_i	0	1	1	$c+1$
β_i	1	0	1	c
A_i		0	1	$\frac{c}{c+1}$
u_i		$\frac{1}{c+1}$	$\frac{1}{c}$	0

Then by theorem 3.3 and Table 1 with $U = \{u_1, u_2, u_3\} = \{\frac{1}{c+1}, \frac{1}{c}, 0\}$, we have

$$
\begin{aligned}
(i)\ \#P_A(a,b) &= \begin{cases} 2 & \text{if } (a,b) \in \{(1,\frac{1}{c(c+1)}),(\frac{1}{c+1},\frac{1}{c}),(\frac{c}{c+1},\frac{1}{c+1})\} \\ 0 & \text{otherwise} \end{cases} \\
(ii)\ \#P_B(a,b) &= \begin{cases} 3 & \text{if } (a,b) \in C_1 := B_1 \cap B_2 \cap B_3 \\ 2 & \text{if } (a,b) \in C_2 := ((B_1 \cap B_2) \cup (B_2 \cap B_3) \cup (B_3 \cap B_1)) \setminus C_1 \\ 1 & \text{if } (a,b) \in C_3 := (B_1 \cup B_2 \cup B_3) \setminus (C_1 \cup C_2) \\ 0 & \text{otherwise} \end{cases} \\
(iii)\ \#P_C(a,b) &= \begin{cases} 0 & \text{if } \mathrm{Tr}(\frac{1}{ab(c^2+1)}) = 1,\ b = \frac{a}{(c+1)a+1} \text{ or } b = \frac{a}{(c^2+c)a+c^2} \\ 2 & \text{otherwise} \end{cases}
\end{aligned} \tag{7}
$$

where $B_1 = \{(a,b) : b = \frac{1}{(c^2+1)a+c^2+c},\ (a,b) \neq (1,\frac{1}{c+1}),(0,\frac{1}{c^2+c}),(\frac{c}{c+1},0)\}$, $B_2 = \{(a,b) : b = \frac{a+1}{(c^2+c)a+c},(a,b) \neq (0,\frac{1}{c}),(1,0)\}$ and $B_3 = \{(a,b) : b = \frac{(c+1)a+1}{(c^2+1)a},\ (a,b) \neq (0,\frac{1}{c+1}),(\frac{1}{c+1},0)\}$.

The next lemma makes it easier to find (a,b) which makes $\mathtt{DDT}_F(a,b)$ maximum.

Lemma 3.5. *In* (7) *with* $F(x) = [0,c,1,x]$ *on* $\mathbb{F}_{2^n}$ *with* $n \geq 3$ *and* $c \neq 1$*, the followings are satisfied:*
(i) $\Delta_F \geq 4$.
(ii) $c \notin \mathbb{F}_4 \setminus \mathbb{F}_2$ *if and only if* $\#P_A(a,b)\#P_B(a,b) = 0$ *for all* $a,b \in \mathbb{F}_{2^n} \setminus \{0\}$*, in other words neither* $\#P_A(a,b)$ *nor* $\#P_B(a,b)$ *can be positive for all* $a,b \in \mathbb{F}_{2^n} \setminus \{0\}$.
(iii) Let us assume that $c \notin \mathbb{F}_4 \setminus \mathbb{F}_2$*. Then*

$$\Delta_F = \max_{(a,b) \in B'} \mathtt{DDT}_F(a,b)$$

where $B' = \{(a,b) : \#P_B(a,b) = \max_{a,b} \#P_B(a,b)\}$.

By using this lemma, we can induce the following proposition and theorem.

Proposition 3.6. *Let* $F(x) = [0,c,1,x]$ *on* $\mathbb{F}_{2^n}$ *with* $c \neq 1$*. Then the followings are satisfied :*
(i) If $c^3 + c^2 + 1 = 0$ *then* $\Delta_F = 8$.
(ii) If $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ *then* $\Delta_F = \begin{cases} 6 & \text{if } n \equiv 0 \pmod 4 \\ 4 & \text{if } n \equiv 2 \pmod 4 \end{cases}$.

Proof. (Sketch of (i)) We first consider $c^3 + c^2 + 1 = 0$ case. If $c^3 + c^2 + 1 = 0$ then we get for

$$B_1 \cap B_2 \cap B_3 = \{(\frac{1}{c^2+c}, 1)\}.$$

It is obvious that $c \notin \mathbb{F}_4$, so $\Delta_F = \mathtt{DDT}_F(\frac{1}{c^2+c}, 1)$ by lemma 3.5. Hence we obtain $\Delta_F = \mathtt{DDT}_F(\frac{1}{c^2+c}, 1) = 6 + \#P_C(\frac{1}{c^2+c}, 1) = 8$. □

Theorem 3.7. *Let* $F(x) = [0,c,1,x]$ *on* $\mathbb{F}_{2^n}$ *with* $c \notin \mathbb{F}_4$ *and* $c^3 + c^2 + 1 \neq 0$*. Then* $\Delta_F \leq 6$ *and the followings are satisifed:*

(i) If $\mathrm{Tr}(\frac{c}{c+1}) = \mathrm{Tr}(\frac{1}{c}) = 1$ *then* $\Delta_F = 4$.

(ii) *If* $\mathrm{Tr}(\frac{c}{c+1}) = 1, \mathrm{Tr}(\frac{1}{c}) = 0$ *then, letting* $\beta^2 + \beta = \frac{1}{c}$ *with* $\beta \in \mathbb{F}_{2^n}$,
– *If* n *is odd then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 0$ *if and only if* $\Delta_F = 4$.
– *If* n *is even then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 1$ *if and only if* $\Delta_F = 4$.

(iii) *If* $\mathrm{Tr}(\frac{c}{c+1}) = 0, \mathrm{Tr}(\frac{1}{c}) = 1$ *then, letting* $\gamma^2 + \gamma = \frac{1}{c+1}$ *with* $\gamma \in \mathbb{F}_{2^n}$,
it holds that $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.

(iv) *If* $\mathrm{Tr}(\frac{c}{c+1}) = \mathrm{Tr}(\frac{1}{c}) = 0$ *then,* $\beta^2 + \beta = \frac{1}{c}$ *and* $\gamma^2 + \gamma = \frac{1}{c+1}$ *with* $\beta, \gamma \in \mathbb{F}_{2^n}$,
– *If* n *is odd then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = 0$ *and* $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.
– *If* n *is even then* $\mathrm{Tr}(\frac{1}{\beta}) = \mathrm{Tr}(\frac{1}{\beta+1}) = \mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$ *if and only if* $\Delta_F = 4$.

Proof. (Sketch) Since $c \notin \mathbb{F}_4$ and $c^3 + c^2 + 1 \neq 0$, $\max_{a,b} \#P_B(a,b) \leq 2$, so $\Delta_F \leq 6$ by lemma 3.5. We now consider claim (i). The assumption implies that $B_1 \cap B_2 = B_2 \cap B_3 = B_3 \cap B_1 = \phi$, so that $\#P_B(a,b) \leq 1$. By lemma 3.5-$(i), (iii)$, we have $\Delta_F = 4$.

We next consider the claim (ii). The assumption implies that $B_1 \cap B_2 = B_2 \cap B_3 = \phi$ and $B_3 \cap B_1 = \{(a,b) : b = \frac{(c+1)a+1}{(c^2+1)a}, a^2 + \frac{c}{c+1}a + \frac{c}{c^2+1} = 0\}$, so we get

$$B' = \{(\tfrac{c}{c+1}\beta, \tfrac{c\beta+1}{(c^2+c)\beta}), (\tfrac{c}{c+1}(\beta+1), \tfrac{c(\beta+1)+1}{(c^2+c)(\beta+1)})\} = \{(\tfrac{\beta}{\beta^2+\beta+1}, \tfrac{\beta^3+\beta^2}{\beta^2+\beta+1}), (\tfrac{\beta+1}{\beta^2+\beta+1}, \tfrac{\beta^3+\beta}{\beta^2+\beta+1})\}.$$

where $\beta^2 + \beta = \frac{1}{c}$. For $(a,b) = (\frac{\beta}{\beta^2+\beta+1}, \frac{\beta+1}{\beta^2+\beta+1}) \in B'$, we get

$$\#P_C(a,b) = \begin{cases} 2 & \text{if } \mathrm{Tr}(\frac{\beta+1}{\beta}) = 0 \\ 0 & \text{if } \mathrm{Tr}(\frac{\beta+1}{\beta}) = 1 \end{cases}$$

by (7). For $(a,b) = (\frac{\beta+1}{\beta^2+\beta+1}, \frac{\beta^3+\beta}{\beta^2+\beta+1}) \in B'$, Therefore

$$\#P_C(a,b) = \begin{cases} 2 & \text{if } \mathrm{Tr}(\frac{\beta}{\beta+1}) = 0 \\ 0 & \text{if } \mathrm{Tr}(\frac{\beta}{\beta+1}) = 1. \end{cases}$$

by (7). Since $\Delta_F = \max_{(a,b)\in B'} \mathtt{DDT}_F(a,b)$ by lemma 3.5, $\Delta_F = 4$ if and only if $\mathrm{Tr}(\frac{\beta+1}{\beta}) = 1$ and $\mathrm{Tr}(\frac{\beta}{\beta+1}) = 1$. Note that $\mathrm{Tr}(1) = 0$ if and only if n is even, so we get the claim (ii). The claim (iii) and (iv) is simlar to the proof of claim (ii). □

Note that Theorem 3.7-(i) has been constructed in [5] but the others are new classes of differentially 4-uniform permutation polynomials.

3.2 Special case on Carlitz rank of 4

Throughout this section, let $F(x) = [0, d, 1, 1, x]$ on $\mathbb{F}_{2^n}$, which is obtained by setting $m = 4$, $a_3 = 1$ and $a_4 = d$ in (3). Similarly to the proof of Carlitz rank 3, we get the following theorem.

Theorem 3.8. *Let* $F(x) = [0, d, 1, 1, x]$ *on* $\mathbb{F}_{2^n}$ *with* $d \notin \mathbb{F}_4$. *Then* $\Delta_F = 4$ *or* $\Delta_F = 6$. *Moreover we get:*
(i) If n *is odd then* $\Delta_F = 4$.
(ii) If n *is even then* $\mathrm{Tr}(\frac{1}{d+1}) = \mathrm{Tr}(\frac{1}{d}) = 1$ *if and only if* $\Delta_F = 4$.

Note that Theorem 3.8-(ii) has been constructed in [5] but the other is new class of differentially 4-uniform permutation polynomials.

4 Conclusion

In this paper, we presented a methodology for calculating differential uniformity for low carlitz rank. As a result we found the bound of differential uniformity, so it was confirmed that the low carlitz rank guarantees a rather low differential uniformity.

We also gave a partial classification of the differential uniformity of the permutation polynomials of Carlitz rank at most 4. As a result, new classes of differentially 4-uniform permutations have been discovered. Since the permutation polynomials of low Carlitz rank are affine equivalent to inverse function except on a small subset in $\mathbb{F}_{2^n}$, and since the other cryptographic properties of the inverse function are well known, we can also find the other cryptographic invariants such as nonlinearity and Walsh spectrum of permutation polynomials with low Carlitz rank in a similar manner.

References

[1] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer International Publishing, DOI : 10.1007/978-3-319-12991-4 (2014)

[2] C. Carlet, Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, Cambridge (2010)

[3] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications 2nd Edition, Academic Press, eBook ISBN: 9780128111307 (2017)

[4] A. Çesmelioglu, W. Meidl, A. Topuzoglu, On the cycle structure of permutation polynomials, Finite Fields Appl. 14 (2008)

[5] Y. Li, M. Wang and Y. Yu, Constructing Differentially 4-uniform Permutations over $GF(2^{2k})$ from the Inverse Function Revisited, eprint.iacr.org/2013/731

[6] J. Peng, and C. Tan, New differentially 4-uniform permutations by modifying the inverse function on subfields, Crypt. Commun. 9 pp 363-378 (2017)

[7] K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 55-64, (1994)

[8] L. Qu, Y. Tan, C. Tan, and C. Li. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Information Theory, 59(7):4675–4686 (2013)

[9] D. Tang, C. Carlet and X. Tang, Differentially 4-uniform bijections by permuting the inverse function, Des. Codes. Cryptogr. 77 pp 117-141 (2015)

[10] Z. Zha, L. Hu and S. Sun, Constructing new differentially 4-uniform permutations from the inverse function, Finite Fields and Their Applications 25, pp 64-78 (2014)