A New Method to Investigate the CCZ-Equivalence between Functions with Low Differential Uniformity

Xi Chen, Longjiang Qu, Chao Li and Jiao Du**

Abstract

Recently, many new classes of differentially 4-uniform permutations have been constructed. However, it is difficult to decide whether they are CCZ-inequivalent or not. In this paper, we propose a new notion called "Projected Differential Spectrum". By considering the properties of the projected differential spectrum, we find several relations that should be satisfied by CCZ-equivalent functions. Based on these results, we mathematically prove that any differentially 4-uniform permutation constructed in [11] by C.Carlet, D.Tang, X.Tang, et al., is CCZ-inequivalent to the inverse function. We also get two interesting results with the help of computer experiments. The first one is a proof that any permutation constructed in [11] is CCZ-inequivalent to a function which is the summation of the inverse function and any Boolean function on $\mathbb{F}_{2^{2k}}$ when $4 \leq k \leq 7$. The second one is a differentially 4-uniform permutation on $\mathbb{F}_{2^6}$ which is CCZ-inequivalent to any function in the aforementioned two classes.

Index Terms

Differentially 4-uniform function, Projected differential spectrum, Substitution boxes, CCZ-inequivalence.

I. Introduction

In many block ciphers, permutations with specific properties are chosen as Substitution boxes (S-boxes for short) to bring the confusion into the cipher in design of cryptographic systems. To prevent various attacks on the cipher, such permutations are required to have low differential uniformity, high nonlinearity and high algebraic degree. Furthermore, for software implementation, such functions are usually required to be defined on the field with even characteristic and even degrees, namely $\mathbb{F}_{2^{2k}}$. We always let $n = 2k$ be an even integer throughout this paper.

In order to resist differential cryptanalysis, the almost perfect nonlinear (APN) functions, whose differential uniformity achieves the lowest possible value on finite fields with even characteristic, may be the best choices for the design of S-boxes. However, it is still an open problem to construct APN permutations over $\mathbb{F}_{2^{2k}}(k \geq 4)$, which is called the *BIG APN* problem. There is only one sporadic APN permutation on $\mathbb{F}_{2^6}$ found by Dillon in 2009 [4]. Since the lack of knowledge about APN permutations on $\mathbb{F}_{2^{2k}}$, a natural trade-off solution is to use differentially 4-uniform permutations as S-boxes.

Recently, many new constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ were presented [5]–[8], [11]–[13], [15]–[20], [22]. Most of them were constructed by adding a properly chosen Boolean function

Xi Chen, Longjiang Qu, Chao Li and Jiao Du are with the College of Science, National University of Defense Technology, Changsha, 410073, China. Jiao Du is also with the College of Mathematics and Information Sciences, Henan Normal University, Xinxiang, 453007, China. E-mail:1138470214@qq.com, ljqu_happy@hotmail.com, lichao_nudt@sina.com, jiaodudj@126.com. This work is supported by the National Basic Research Program of China (Grant No. 2013CB338002), the Nature Science Foundation of China (NSFC) under Grant 61272484, U1404601, 11531002, 61572026, the Program for New Century Excellent Talents in University (NCET) and the Basic Research Fund of National University of Defense Technology (No.CJ 13-02-01).

to the inverse function, see [12], [13], [16]–[19], [21], [22]. For simplicity, we call a differentially 4-uniform permutation constructed by this method a 4-*uniform BI permutation*. As shown in [17], the number of 4-uniform BI permutations on $\mathbb{F}_{2^n}$ is no less than $2^{\frac{2^n+2}{3}}$. Very recently, C.Carlet, D.Tang, X.Tang, et al., presented a new construction of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$, which used the APN property of the inverse function on $\mathbb{F}_{2^{2k-1}}$. They constructed at least $(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1) \cdot 2^{2^{n-1}}$ differentially 4-uniform permutations [11]. Such families can be regarded as adding a properly chosen Boolean function to the CTTL basic differentially 4-uniform permutation (See the precise definition in Section II.B). We call them 4-*uniform BCTTL permutations* for short.

Two (n, n)-functions are considered to be equivalent if one can be obtained from the other by some simple transformations. There are mainly two such equivalence notions, called extended affine equivalence (EA equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence, graph affine equivalence). It is well known that EA equivalence implies CCZ-equivalence, but not vise versa. Proving the CCZ-inequivalence between two functions is mathematically (and also computationally) difficult, unless some CCZ-equivalent invariants can be proved to be different for the two functions. Many CCZ-equivalent invariants are known, such as the extended Walsh spectrum, the differential spectra, Γ-rank, Δ-rank, the order of the automorphism group of the design $dev(G_F)$, $dev(D_F)$, etc. For their detailed definitions, please see [14] or [1, page 43].

By computing the Walsh spectrum, the authors in [11], [19] proved that both 4-uniform BCTTL permutations and 4-uniform BI permutations are CCZ-inequivalent to the Gold functions, the Kasami functions, the Bracken-Leander functions and quadratic functions . With the help of computer, they also checked for $8 \leq n \leq 16$ that any 4-uniform BCTTL permutation is CCZ-inequivalent to the inverse function [11]. There are also some discussions about CCZ-equivalence between different subclasses of 4-uniform BI permutations or 4-uniform BCTTL permutations [11], [16]–[19], [22]. However, we do not know whether a 4-uniform BCTTL permutation can be CCZ-equivalent to a 4-uniform BI permutation. Due to the big cardinality of these two function classes, it seems to be quite difficult to prove or to check the CCZ-equivalence between them even for small fields. Here we say two classes of functions are CCZ-inequivalent if any function in one class is CCZ-inequivalent to each function in the other class. Moveover, given a differentially 4-uniform permutation on a small field, it also seems difficult to judge whether there exists a function in these two classes which is CCZ-equivalent to the given permutation.

In this paper, we propose a new notion called "Projected Differential Spectrum". By considering the properties of the projected differential spectrum, we find several relations that should be satisfied by CCZ-equivalent functions. Based on these results, we mathematically prove that any of the differentially 4-uniform permutations constructed in [11] by C.Carlet, D.Tang, X.Tang, et al., is CCZ-inequivalent to the inverse function. We also get two interesting results with the help of computer experiments as applications of theory results.

The rest of this paper is organized as follows. In Section II we recall some necessary definitions and useful lemmas. The definition of projected differential spectrum is introduced in Section III. By considering the properties of projecting (n, n)-functions on $\mathbb{F}_2^{2n-1}$ and $\mathbb{F}_2^{2n-2}$, we obtain two useful corollaries. In Section IV, with these corollaries, we prove that any 4-uniform BCTTL permutation is CCZ-inequivalent to the inverse function when $n \geq 6$. Then we prove that 4-uniform BCTTL permutations and 4-uniform BI permutations are CCZ-inequivalent when $8 \leq n \leq 14$ with the help of a computer. At the end of Section IV, we present an interesting function on $\mathbb{F}_{2^6}$ which is proved to be CCZ-inequivalent to any 4-uniform BCTTL permutation or any 4-uniform BI permutation. Conclusion and further problems are given in Section V.

II. Preliminaries

A. Necessary definitions and useful lemmas

In this subsection, we give necessary definitions and results which will be used in the paper.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. It can be regarded as a vector space $\mathbb{F}_2^n$ of dimension n over $\mathbb{F}_2$. In fact, assume $\Gamma(x) \in \mathbb{F}_2[x]$ is an irreducible monic polynomial with degree n and α is a root in the splitting field of $\Gamma(x)$, then

$$\mathbb{F}_{2^n} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \big| a_0, a_1, \cdots, a_{n-1} \in \mathbb{F}_2\}.$$

For any $a = a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \in \mathbb{F}_{2^n}$, the mapping $a \to \vec{a} := (a_0, a_1, \cdots, a_{n-1})^{\mathrm{T}}$ is an isomorphism from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^n$. In the following, we will switch between these two points of views without explanation if the context is clear. Moreover, any vector $\vec{a} = (a_0, a_1, \cdots, a_{n-1})^{\mathrm{T}} \in \mathbb{F}_2^n$ can be written as $\vec{a} = \begin{bmatrix} a_0 \\ \vec{a'} \end{bmatrix}$, where $\vec{a'} = (a_1, \ldots, a_{n-1})^{\mathrm{T}} \in \mathbb{F}_2^{n-1}$ can be identified with $a' \in \mathbb{F}_{2^{n-1}}$. We write $a = (a_0, a')$ for convenience.

Given two positive integers n and m, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called an (n, m)-function. Particularly, when $m = 1$, F is called an n-variable Boolean function, or a Boolean function defined on $\mathbb{F}_{2^n}$. Denote by $\mathbb{B}_n$ all the Boolean functions with n variables. Let F be an (n, n)-function. Then F can be expressed uniquely as a polynomial over $\mathbb{F}_{2^n}$ with degree at most $2^n - 1$. It is called a permutation polynomial if it induces a permutation over $\mathbb{F}_{2^n}$. In the rest of this paper, a function is regarded as an (n, n)-function if there is no explanation.

Denote by $\mathbb{F}_{2^n}^*$ the set of all nonzero elements of $\mathbb{F}_{2^n}$. Throughout this paper, for the multiplicative inverse function $I(x) = \frac{1}{x}$, we always define $I(0) = 0$. We define the trace mapping from $\mathbb{F}_{2^n}$ onto its subfield $\mathbb{F}_{2^l}$ as $\mathrm{Tr}_l^n(x) = \sum_{i=0}^{n/l-1} x^{2^{il}}$, where $l|n$, and denote the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by $\mathrm{Tr}(x) = \mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

For any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let us define the differential value of $F(x)$ at (a, b) as:

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\},$$

where for a set S, its cardinality is denoted by $\#S$. It should be noted that in the above definition we remove the usual restriction $a \neq 0$. Clearly, the differential value can also be defined on the vector space equivalently:

$$\delta_F(a, b) = \# \left\{ (x_1, x_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} \right\}.$$

The multiset $\{* \ \delta_F(a, b) | (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \ *\}$ is called the differential spectrum of F. The value

$$\Delta_F := \max_{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \delta_F(a, b)$$

is called the differential uniformity of F, or we call F a differentially Δ_F-uniform function. In particular, we call F an almost perfect nonlinear (APN) function if $\Delta_F = 2$. It is easy to see that APN functions achieve the minimal value of differential uniformity for functions defined on fields with even characteristic.

For the above function F, the Walsh transform $F^{\mathcal{W}} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^* \to \mathbb{C}$ of F is defined by:

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

The multiset $\mathcal{W}_F = \{* \ F^{\mathcal{W}}(a, b) | a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^* \ *\}$ is called the Walsh spectrum of F. The nonlinearity of F is defined as

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*} |F^{\mathcal{W}}(a, b)|.$$

Two functions F and G are called to be Carlet-Charpin-Zinoviev (CCZ) equivalent if there exists an affine permutation $A : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$, such that $A \begin{bmatrix} \vec{y} \\ G(\vec{y}) \end{bmatrix} = \begin{bmatrix} \vec{x} \\ F(\vec{x}) \end{bmatrix}$.

Definition 2.1: Let F and G be two CCZ-equivalent (n, n)-functions. We call L a *linearized permutation corresponding to CCZ-equivalent transformation* from G to F if

$$\begin{bmatrix} \vec{x} \\ F(\vec{x}) \end{bmatrix} = L \begin{bmatrix} \vec{y} \\ G(\vec{y}) \end{bmatrix} + \begin{bmatrix} \vec{\xi} \\ \vec{\eta} \end{bmatrix},$$

where $L : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ is a linearized permutation, and $\vec{\xi}, \vec{\eta}$ are constants on $\mathbb{F}_2^n$.

Clearly L^{-1} is also a linearized permutation, and we define the matrix expression of $L^{-1} := \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix}$, where $L_i, i = 1, 2, 3, 4$ are matrixes of $n \times n$ on $\mathbb{F}_2$. Let the mapping $\mathcal{L}_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, here $\mathcal{L}_i(x)$ is defined by translating its vector expression $\overrightarrow{\mathcal{L}_i(x)} = L_i\vec{x}$ to the finite field.

Particularly, F and G are extended affine (EA) equivalent when $L_2 = 0$.

The following results are useful in our future discussion.

Theorem 2.2: [2, Theorem 5.45] If χ is a nontrivial additive character and $a, b \in \mathbb{F}_q$ are not both 0, then the Kloosterman Sum $K(\chi; a, b)$ satisfies

$$|K(\chi; a, b)| = |\sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1})| \leq 2q^{\frac{1}{2}}.$$

Lemma 2.3: [2] For any $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$, the polynomial $f(x) = x^2 + ax + b \in \mathbb{F}_{2^n}[x]$ has 2 different solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{b}{a^2}) = 0$.

B. Extensions of some known differentially 4-uniform permutations

In this paper, we will not directly investigate the CCZ-equivalence of known differentially 4-uniform permutations. In contrast, we generalize them to a bigger class of functions with low differential uniformity by adding to it a multiple of a Boolean function. Then we investigate the CCZ-equivalence of the functions in these bigger classes. Hence the CCZ-equivalence of the original permutations have been considered naturally.

First, let us recall the construction presented by C.Carlet, D.Tang, X.Tang, et al. [11].

Theorem 2.4: [11] Let $n \geq 6$ be an even integer and let $c' \in \mathbb{F}_{2^{n-1}} \setminus \{0, 1\}$ such that $\mathrm{Tr}_1^{n-1}(c') = \mathrm{Tr}_1^{n-1}(\frac{1}{c'}) = 1$, and let f' be an arbitrary Boolean function defined on $\mathbb{F}_{2^{n-1}}$. Then we define an (n, n)-function $F_P(x)$ as follows:

$$F_P(x) = F_P(x_0, x') = \begin{cases} (f'(x'), \frac{1}{x'}), & \text{if } x_0 = 0; \\ (f'(\frac{x'}{c'}) + 1, \frac{c'}{x'}), & \text{if } x_0 = 1, \end{cases}$$

where $x' \in \mathbb{F}_{2^{n-1}}$ is defined as $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$. Then $F_P(x)$ is a differentially 4-uniform permutation.

There are at least $(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1) \cdot 2^{2^{n-1}}$ differentially 4-uniform permutations in the above construction.

Definition 2.5: Let $n \geq 6$ be an even integer, for any element $c' \in \mathbb{F}_{2^{n-1}} \setminus \{0, 1\}$ satisfying $\mathrm{Tr}_1^{n-1}(c') = \mathrm{Tr}_1^{n-1}(\frac{1}{c'}) = 1$, we define an (n, n)-function $F_C(x)$ called *CTTL basic differentially 4-uniform permutation* as follows:

$$F_C(x) = F_C(x_0, x') = \begin{cases} (0, \frac{1}{x'}), & \text{if } x_0 = 0; \\ (1, \frac{c'}{x'}), & \text{if } x_0 = 1, \end{cases}$$

where $x' \in \mathbb{F}_{2^{n-1}}$ is defined as $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$.

Define the n-variable Boolean function

$$f_P(x) = f_P(x_0, x') = \begin{cases} f'(x'), & \text{if } x_0 = 0; \\ f'(\frac{x'}{c'}), & \text{if } x_0 = 1. \end{cases}$$

The image set of $F_C(x)$ is $\mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$, which is isomorphic to $\mathbb{F}_{2^n}$. Then $F_P(x)$ can be got by adding a Boolean function $f_P(x)$ to the $\mathbb{F}_2$ component of $F_C(x)$. Further, $F_P(x)$ can be generalized as follows: Let $F_f(x) = F_C(x) + f(x)$ be a summation of $F_C(x)$ and an arbitrary n-variable Boolean function $f(x)$, and let $\mathbb{S}_n = \{F_f(x) | f \in \mathbb{B}_n\}$, that is, $\mathbb{S}_n$ denotes the class of all these functions. Similarly as in the proof of [11, Theorem 2], one can prove that any function in $\mathbb{S}_n$ is differentially 4-uniform. Let $\mathbb{SP}_n$ be the subclass of $\mathbb{S}_n$ which are differentially 4-uniform permutations, and we call them 4-*uniform BCTTL permutations* for simplicity. Actually, Theorem 2.4 describes all the functions of this subclass. We will discuss the CCZ-equivalence of 4-uniform BCTTL permutations with the inverse function and other classes of functions in Section IV.

Now let us define $G_f(x) = I(x) + f(x)$ as the function which is the sum of the inverse function and a Boolean function $f(x)$. Clearly, $G_f(x)$ may not be a permutation polynomial and the differential uniformity might be 4 or 6 [13]. Let $\mathbb{T}_n$ be the class of all functions $G_f(x)$ and let $\mathbb{TP}_n$ be its subclass constituting with differentially 4-uniform permutations. We call a function in this subclass *a* 4-*uniform BI permutation* for short. The cardinality of this subclass $\mathbb{TP}_n$ is at least $2^{\frac{2^n+2}{3}}$ [17]. Further, an equivalent condition for a function to be in $\mathbb{TP}_n$ has been given in [12].

Theorem 2.6: [12] Let n be an even integer and f be an n-variable Boolean function. Let ω be an element of $\mathbb{F}_{2^n}$ with order 3. Then $G(x) = \frac{1}{x} + f(\frac{1}{x})$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if and only if $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$, and for arbitrary $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, at least one of the following two equations holds:

$$f(0) + f(z + \frac{1}{z} + 1) + f(\omega z + \frac{1}{\omega z} + 1) + f(\omega^2 z + \frac{1}{\omega^2 z} + 1) = 0,$$
$$f(0) + f(z + \frac{1}{z} + 1) + f(\omega(z + \frac{1}{z} + 1)) + f(\omega^2(z + \frac{1}{z} + 1)) = 1.$$

III. Projected Differential Spectrum and Its Properties

In this section, we propose a new notion called projected differential spectrum. Then we find several relations that should be satisfied by CCZ-equivalent functions. These relations can be served as a new method to investigate the CCZ-equivalence of functions.

A. The projected differential spectrum

Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function, where $1 \le m \le 2n$ is an integer. The kernel of R is the set

$$\mathrm{Ker}(R) = \{(s,t) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | R(s,t) = 0\}.$$

Let $F(x)$ be an (n,n)-function. Then $x \to (x, F(x))$ is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Definition 3.1: For any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, define the *R-projected differential value* of F at (a,b) as

$$\begin{aligned} \delta_{F-R}(a,b) &= \sum_{(s,t) \in \mathrm{Ker}(R)} \delta_F(a+s, b+t) \\ &= \sum_{(s,t) \in \mathrm{Ker}(R)} \#\left\{ (x_1, x_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \overrightarrow{a+s} \\ \overrightarrow{b+t} \end{bmatrix} \right\}. \end{aligned}$$

Moreover, we define the *R-projected differential spectrum* of F as the multiset

$$\{* \ \delta_{F-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\}.$$

The following theorem shows the relation of projected differential value between two CCZ-equivalent functions.

Theorem 3.2: Suppose that two functions F and G are CCZ-equivalent. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from G to F. Then for any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let $\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} = L \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$, we have

$$\delta_{F-R}(a,b) = \delta_{G-R\circ L}(u,v).$$

Proof: According to the definition of CCZ-equivalence, we have

$$\begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \vec{x_1} \\ \vec{F(x_1)} \end{bmatrix} + \begin{bmatrix} \vec{x_2} \\ \vec{F(x_2)} \end{bmatrix} = L \begin{bmatrix} \overrightarrow{y_1 + y_2} \\ \overrightarrow{G(y_1) + G(y_2)} \end{bmatrix}.$$

Thus $\begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix}$ if and only if $\begin{bmatrix} \overrightarrow{y_1 + y_2} \\ \overrightarrow{G(y_1) + G(y_2)} \end{bmatrix} = \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$.

Hence

$$\begin{aligned}
\delta_{F-R}(a,b) &= \sum_{(s_1,t_1)\in \mathrm{Ker}(R)} \# \left\{ x_1, x_2 \in \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \overrightarrow{a + s_1} \\ \overrightarrow{b + t_1} \end{bmatrix} \right\} \\
&= \sum_{(s_1,t_1)\in \mathrm{Ker}(R)} \# \left\{ y_1, y_2 \in \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{y_1 + y_2} \\ \overrightarrow{G(y_1) + G(y_2)} \end{bmatrix} = L^{-1}(\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} + \begin{bmatrix} \vec{s_1} \\ \vec{t_1} \end{bmatrix}) \right\} \\
&= \sum_{(s_1,t_1)\in \mathrm{Ker}(R)} \# \left\{ y_1, y_2 \in \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{y_1 + y_2} \\ \overrightarrow{G(y_1) + G(y_2)} \end{bmatrix} = \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix} + L^{-1} \begin{bmatrix} \vec{s_1} \\ \vec{t_1} \end{bmatrix} \right\} \\
&= \sum_{(s_2,t_2)\in \mathrm{Ker}(R\circ L)} \# \left\{ y_1, y_2 \in \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{y_1 + y_2} \\ \overrightarrow{G(y_1) + G(y_2)} \end{bmatrix} = \begin{bmatrix} \overrightarrow{u + s_2} \\ \overrightarrow{v + t_2} \end{bmatrix} \right\} \\
&= \delta_{G-R\circ L}(u,v).
\end{aligned}$$

We finish the proof. □

Since L is a linearized permutation, (a,b) runs through $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if and only if (u,v) does. Then we obtain the following corollary.

Corollary 3.3: Suppose that two functions F and G are CCZ-equivalent. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be any surjective linear function. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from G to F. Then

$$\{* \ \delta_{F-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\} = \{* \ \delta_{G-R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\}.$$

Here we project the functions with a surjective linear function $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$. According to Corollary 3.3, if one finds a surjective linear function R such that for all of the possible linearized permutations L, the above condition does not hold, then F and G are CCZ-inequivalent. This method may be quite useful to judge whether two functions are CCZ-inequivalent if it is difficult to calculate the differential spectrum of F and G. In the next subsection, we will project the functions on $\mathbb{F}_2^{2n-1}$ and $\mathbb{F}_2^{2n-2}$ with some special surjective linear functions.

B. Special Projections on $\mathbb{F}_2^{2n-1}$ and $\mathbb{F}_2^{2n-2}$

To discuss the case of projecting the functions on $\mathbb{F}_2^{2n-1}$ and $\mathbb{F}_2^{2n-2}$, we first introduce a new notation.

Definition 3.4: For any $\gamma \in \mathbb{F}_{2^n}^*$, $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, define the *$\gamma$-joint differential value of $F(x)$ at (a,b)* as

$$\begin{aligned} J_{F-\gamma}(a,b) &= \delta_F(a,b) + \delta_F(a,b+\gamma) \\ &= \#\{x \in \mathbb{F}_{2^n} | F(x) + F(x+a) = b\} + \#\{x \in \mathbb{F}_{2^n} | F(x) + F(x+a) = b+\gamma\}. \end{aligned}$$

It is clear that $\delta_{F-R}(a,b) = J_{F-\gamma}(a,b)$ when $\mathrm{Ker}(R) = \{(0,0),(0,\gamma)\}$.

Now we show several properties about the γ-joint differential value.

Lemma 3.5: Let $F(x) = F_0(x) + \gamma f(x)$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $f(x)$ is an n-variable Boolean function. Then for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,

$$J_{F_0-\gamma}(a,b) = J_{F-\gamma}(a,b).$$

Proof: According to the definition of the γ-joint different value, we have

$$\begin{aligned} & J_{F-\gamma}(a,b) = \#\{x \in \mathbb{F}_{2^n} | F(x) + F(x+a) = b\} + \#\{x \in \mathbb{F}_{2^n} | F(x) + F(x+a) = b+\gamma\} \\ = \; & \#\{x \in \mathbb{F}_{2^n} | F_0(x) + F_0(x+a) + \gamma(f(x) + f(x+a)) = b\} \\ & + \#\{x \in \mathbb{F}_{2^n} | F_0(x) + F_0(x+a) + \gamma(f(x) + f(x+a)) = b+\gamma\} \\ = \; & \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b \\ f(x) + f(x+a) = 0 \end{cases}\right\} + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b+\gamma \\ f(x) + f(x+a) = 1 \end{cases}\right\} \\ & + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b \\ f(x) + f(x+a) = 1 \end{cases}\right\} + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b+\gamma \\ f(x) + f(x+a) = 0 \end{cases}\right\} \\ = \; & \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b \\ f(x) + f(x+a) = 0 \end{cases}\right\} + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b \\ f(x) + f(x+a) = 1 \end{cases}\right\} \\ & + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b+\gamma \\ f(x) + f(x+a) = 1 \end{cases}\right\} + \#\left\{x \in \mathbb{F}_{2^n} \middle| \begin{cases} F_0(x) + F_0(x+a) = b+\gamma \\ f(x) + f(x+a) = 0 \end{cases}\right\} \\ = \; & \#\{x \in \mathbb{F}_{2^n} | F_0(x) + F_0(x+a) = b\} + \#\{x \in \mathbb{F}_{2^n} | F_0(x) + F_0(x+a) = b+\gamma\} = J_{F_0-\gamma}(a,b). \end{aligned}$$

The proof is completed. □

By Lemma 3.5, if a function is added by a multiplication of γ and a Boolean function, then its γ-joint differential value remains unchanged. Then we have the following theorem.

Theorem 3.6: Let $F(x) = F_0(x) + \gamma f(x)$, where $\gamma \in \mathbb{F}_{2^n}^*$ and $f(x)$ is an n-variable Boolean function. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function and $(0,\gamma) \in \mathrm{Ker}(R)$. Then for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,

$$\delta_{F_0-R}(a,b) = \delta_{F-R}(a,b).$$

Proof: Since $(0,\gamma) \in \mathrm{Ker}(R)$, we have

$$\sum_{(s,t)\in \mathrm{Ker}(R)} \delta_F(a+s,b+t) = \sum_{(s,t+\gamma)\in \mathrm{Ker}(R)} \delta_F(a+s,b+t+\gamma) = \sum_{(s,t)\in Ker(R)} \delta_F(a+s,b+t+\gamma).$$

Similarly,

$$\sum_{(s,t)\in \mathrm{Ker}(R)} \delta_{F_0}(a+s,b+t) = \sum_{(s,t)\in \mathrm{Ker}(R)} \delta_{F_0}(a+s,b+t+\gamma).$$

According to the definition of the R-projected differential value and Lemma 3.5, we have

$$\begin{aligned}
\delta_{F-R}(a,b) &= \sum_{(s,t)\in \mathrm{Ker}(R)} \delta_F(a+s,b+t) \\
&= \frac{1}{2}\left(\sum_{(s,t)\in \mathrm{Ker}(R)} \delta_F(a+s,b+t) + \sum_{(s,t)\in \mathrm{Ker}(R)} \delta_F(a+s,b+t+\gamma)\right) \\
&= \frac{1}{2}\sum_{(s,t)\in \mathrm{Ker}(R)} J_{F-\gamma}(a+s,b+t) \\
&= \frac{1}{2}\sum_{(s,t)\in \mathrm{Ker}(R)} J_{F_0-\gamma}(a+s,b+t) \\
&= \frac{1}{2}\left(\sum_{(s,t)\in \mathrm{Ker}(R)} \delta_{F_0}(a+s,b+t) + \sum_{(s,t)\in \mathrm{Ker}(R)} \delta_{F_0}(a+s,b+t+\gamma)\right) \\
&= \sum_{(s,t)\in \mathrm{Ker}(R)} \delta_{F_0}(a+s,b+t) = \delta_{F_0-R}(a,b).
\end{aligned}$$

We finish the proof. □

We have the following proposition by projecting the functions with $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-1}$, where $\mathrm{Ker}(R) = \{(0,0),(0,\gamma)\}$.

Proposition 3.7: Suppose that the function $F(x) = F_0(x) + \gamma f(x)$ and $G(x)$ are CCZ-equivalent, where $\gamma \in \mathbb{F}_{2^n}^*$ and $f(x)$ is an arbitrary Boolean function defined on $\mathbb{F}_{2^n}$. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-1}$ be a surjective linear function with $\mathrm{Ker}(R) = \{(0,0),(0,\gamma)\}$. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from G to F. For any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let $\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} = L \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$, we obtain $\delta_{F_0-R}(a,b) = \delta_{G-R\circ L}(u,v)$. Then

$$\{*\ \delta_{F_0-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}\ *\} = \{*\ \delta_{G-R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}\ *\}.$$

Proof: It follows from Theorem 3.2 that $\delta_{F-R}(a,b) = \delta_{G-R\circ L}(u,v)$. Hence by Theorem 3.6, we have

$$\delta_{F_0-R}(a,b) = \delta_{F-R}(a,b) = \delta_{G-R\circ L}(u,v),$$

where $\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} = L \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$.

Since L is a linearized permutation, (a,b) runs through $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if and only if (u,v) does, we get

$$\{*\ \delta_{F_0-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}\ *\} = \{*\ \delta_{G-R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}\ *\}.$$

The proof is completed. □

By projecting the functions with a special surjective linear function on $\mathbb{F}_2^{2n-2}$, we have the following proposition.

Proposition 3.8: Suppose that functions $F(x) = F_0(x) + \gamma_1 f_1(x)$ and $G(x) = G_0(x) + \gamma_2 f_2(x)$ are CCZ-equivalent, where $\gamma_1, \gamma_2 \in \mathbb{F}_{2^n}^*$ and $f_1(x), f_2(x)$ are arbitrary Boolean functions defined on $\mathbb{F}_{2^n}$. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-2}$ be a surjective linear function with $\mathrm{Ker}(R) = \{(0,0),(0,\gamma_1),(s,t),(s,t+\gamma_1)\}$, where $\begin{bmatrix} \vec{s} \\ \vec{t} \end{bmatrix} = L \begin{bmatrix} \vec{0} \\ \vec{\gamma_2} \end{bmatrix}$. Let L be a linearized permutation corresponding to CCZ-equivalent transformation

from G to F. For any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let $\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} = L \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$, we have $\delta_{F_0-R}(a,b) = \delta_{G_0-R\circ L}(u,v)$. Then

$$\{* \ \delta_{F_0-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\} = \{* \ \delta_{G_0-R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\}.$$

Proof: Because of Theorem 3.2, we have

$$\delta_{F-R}(a,b) = \delta_{G-R\circ L}(u,v).$$

Since $\begin{bmatrix} \vec{s} \\ \vec{t} \end{bmatrix} = L \begin{bmatrix} \vec{0} \\ \vec{\gamma_2} \end{bmatrix}$, we have $(0,\gamma_2) \in \mathrm{Ker}(R \circ L)$. Notice that $(0,\gamma_1) \in \mathrm{Ker}(R)$, then

$$\delta_{F_0-R}(a,b) = \delta_{F-R}(a,b) = \delta_{G-R\circ L}(u,v) = \delta_{G_0-R\circ L}(u,v)$$

according to Theorem 3.6.

Since L is a linearized permutation, (a,b) runs through $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if and only if (u,v) does, one has

$$\{* \ \delta_{F_0-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\} = \{* \ \delta_{G_0-R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\}.$$

We finish the proof. □

Proposition 3.7 and Proposition 3.8 present two necessary conditions for F and G to be CCZ-equivalent. Hence it is a new method to judge the CCZ-inequivalence between functions by considering their projected differential spectrums. This method may be quite useful if it is difficult to check the differential spectrums of F and G. In the next section, we will use them to derive some CCZ-inequivalent results about functions with low differential uniformity.

IV. Main Results

A. The CCZ-inequivalence between 4-uniform BCTTL permutations and the inverse function

In this subsection, we will mathematically prove the CCZ-inequivalence between 4-uniform BCTTL permutations and the inverse function by considering the projected differential spectrum. We first introduce two lemmas.

Lemma 4.1: Let $n \geq 6$ be an even integer. Then for any $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$, we have $J_{F_C-1}(a,b) \leq 4$.

Proof: Let us write $a = (a_0, a')$ and $b = (b_0, b')$ as $x = (x_0, x')$ does. Without loss of generality, we assume $a_0 = 1$. The case $a_0 = 0$ can be proved similarly.

$$\begin{aligned}
J_{F_C-1}(a,b) &= \#\{x \in \mathbb{F}_{2^n} \big| F_C(x) + F_C(x+a) = b\} + \#\{x \in \mathbb{F}_{2^n} \big| F_C(x) + F_C(x+a) = b+1\} \\
&= \#\{x \in \mathbb{F}_{2^n} \big| F_C(x_0,x') + F_C(x_0+a_0, x'+a') = (b_0,b')\} \\
&+ \#\{x \in \mathbb{F}_{2^n} \big| F_C(x_0,x') + F_C(x_0+a_0, x'+a') = (b_0+1,b')\} \\
&= \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 0 \end{array} \middle| \begin{array}{c} \frac{1}{x'} + \frac{c'}{x'+a'} = b' \\ 1 = b_0 \end{array} \right\} + \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 1 \end{array} \middle| \begin{array}{c} \frac{c'}{x'} + \frac{1}{x'+a'} = b' \\ 1 = b_0 \end{array} \right\} \\
&+ \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 0 \end{array} \middle| \begin{array}{c} \frac{1}{x'} + \frac{c'}{x'+a'} = b' \\ 1 = b_0 + 1 \end{array} \right\} + \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 1 \end{array} \middle| \begin{array}{c} \frac{c'}{x'} + \frac{1}{x'+a'} = b' \\ 1 = b_0 + 1 \end{array} \right\} \\
&= \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 0 \end{array} \middle| \frac{1}{x'} + \frac{c'}{x'+a'} = b' \right\} + \#\left\{ \begin{array}{l} x' \in \mathbb{F}_{2^{n-1}} \\ x_0 = 1 \end{array} \middle| \frac{c'}{x'} + \frac{1}{x'+a'} = b' \right\}.
\end{aligned}$$

If $a'b' \neq 0, 1, c'$, then each of the equations $\frac{1}{x'} + \frac{c'}{x'+a'} = b'$ and $\frac{c'}{x'} + \frac{1}{x'+a'} = b'$ is equivalent to a quadratic equation, which means that the summation of the number of the solutions of these two equations is at most 4, or for simplicity, we say that these two equations have at most 4 solutions together. Note that here and

thereafter, when we talk about a solution of an equation, we always refer to the solution in $\mathbb{F}_{2^n}$. If $a'b'=0$, we can easily check that each of them has exactly one solution. If $a'b'=1$ or c', $\mathrm{Tr}_1^{n-1}(c')=\mathrm{Tr}_1^{n-1}(\frac{1}{c'})=1$ ensures that these two functions have no solutions beside 0 and a' according to Lemma 2.3. Hence

$$J_{F_C-1}(a,b)=\#\left\{\begin{array}{l} x'\in\mathbb{F}_{2^{n-1}} \\ x_0=0 \end{array}\;\middle|\;\frac{1}{x'}+\frac{c'}{x'+a'}=b'\right\}+\#\left\{\begin{array}{l} x'\in\mathbb{F}_{2^{n-1}} \\ x_0=1 \end{array}\;\middle|\;\frac{c'}{x'}+\frac{1}{x'+a'}=b'\right\}\le 4.$$

This completes the proof of Lemma 4.1. □

Lemma 4.2: Let $n\ge 4$ be an even integer. Then for any $r_1,r_2\in\mathbb{F}_{2^n}$, there exist $u,v\in\mathbb{F}_{2^n}$ such that $\delta_I(u,v)+\delta_I(u+r_1,v+r_2)=6$ or 8.

Proof: Without loss of generality, we assume that $u\neq 0,r_1,1/r_2$. According to the definition of differential value, it is equivalent to prove that the following two equations have 6 or 8 solutions together.

$$I(x)+I(x+u)=v, \tag{1}$$

$$I(x)+I(x+u+r_1)=v+r_2. \tag{2}$$

Let u,v satisfy $uv=1$. Then (1) has 4 different solutions $0,u,\omega u,\omega^2 u$, where ω is an element with multiplicative order 3. Hence $\delta_I(u,v)=4$. By substituting $v=\frac{1}{u}$ into (2), we get $I(x)+I(x+u+r_1)=\frac{1}{u}+r_2$, which has the same number of solutions with the following quadratic function except at $x=0$ and $x=u+r_1$.

$$x^2+(u+r_1)x+\frac{u+r_1}{\frac{1}{u}+r_2}=0. \tag{3}$$

It is easy to show that neither $x=0$ nor $x=u+r_1$ is a solution of (3). Now we need to prove that there exists u such that (3) has 2 different solutions. Then (2) has 2 or 4 different solutions, which means $\delta_I(u,v)+\delta_I(u+r_1,v+r_2)=6$ or 8. The following proof is divided into four cases.

Case 1. $r_1r_2=1$. In this case, (3) is equivalent to $x^2+(u+r_1)x+ur_1=0$. Obviously, it has exactly 2 different solutions $x=u,x=r_1$.

Case 2. $r_1=0$. According to Lemma 2.3, (3) has 2 different solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{1}{1+ur_2})=0$. It is easy to see that there exists u such that (3) has 2 different solutions.

Case 3. $r_2=0$. Similarly, (3) has 2 different solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{1}{\frac{1}{u}r_1+1})=0$, which clearly holds for some $u\neq 0,r_1,\frac{1}{r_2}$.

Case 4. $r_1r_2\neq 0,1$. According to Lemma 2.3, it suffices to prove that there exists $u\in\mathbb{F}_{2^n}\setminus\{0,r_1,\frac{1}{r_2}\}$ such that $\mathrm{Tr}(\frac{1}{(\frac{1}{u}+r_2)(u+r_1)})=0$.

Assume, on the contrary, that there exist $r_1,r_2\in\mathbb{F}_{2^n}$ such that $r_1r_2\neq 0,1$ and $\mathrm{Tr}(\frac{1}{(\frac{1}{u}+r_2)(u+r_1)})=1$ for any $u\in\mathbb{F}_{2^n}\setminus\{0,r_1,I(r_2)\}$. Let $u=\phi(z)=r_1\frac{z+1}{z+r_1r_2}$. Then

$$\begin{aligned}
&\mathrm{Tr}\left(\frac{1}{(\frac{1}{u}+r_2)(u+r_1)}\right)=\mathrm{Tr}\left(\frac{1}{r_1}\frac{u}{(r_2u+1)(\frac{1}{r_1}u+1)}\right)\\
=\;&\mathrm{Tr}\left(\frac{1}{(r_2+\frac{1}{r_1})r_1}(\frac{1}{r_2u+1}+\frac{1}{\frac{1}{r_1}u+1})\right)=\mathrm{Tr}\left(\frac{1}{r_1r_2+1}(\frac{1}{r_1r_2\frac{z+1}{z+r_1r_2}+1}+\frac{1}{\frac{z+1}{z+r_1r_2}+1})\right)\\
=\;&\mathrm{Tr}\left(\frac{1}{r_1r_2+1}(\frac{z+r_1r_2}{(r_1r_2+1)z}+\frac{z+r_1r_2}{r_1r_2+1})\right)=\mathrm{Tr}\left(\frac{1}{r_1r_2+1}+\frac{1}{r_1^2r_2^2+1}z+\frac{r_1r_2}{r_1^2r_2^2+1}\frac{1}{z}\right).
\end{aligned}$$

Since u runs over $\mathbb{F}_{2^n}$ if and only if z does, we have

$$\begin{aligned} 2^n-6 &\leq |\sum_{u\in F_{2^n}}(-1)^0|-2|\sum_{u\in\{0,r_1,\frac{1}{r_2}\}}(-1)^{\mathrm{Tr}(\frac{1}{(\frac{1}{u}+r_2)(u+r_1)})}| \\ &\leq |\sum_{u\in F_{2^n}}(-1)^{\mathrm{Tr}(\frac{1}{(\frac{1}{u}+r_2)(u+r_1)})}| = |\sum_{z\in F_{2^n}}(-1)^{\mathrm{Tr}(\frac{1}{r_1r_2+1}+\frac{1}{r_1^2r_2^2+1}z+\frac{r_1r_2}{r_1^2r_2^2+1}\frac{1}{z})}| \\ &\leq |\sum_{z\in F_{2^n}^*}(-1)^{\mathrm{Tr}(\frac{1}{r_1^2r_2^2+1}z+\frac{r_1r_2}{r_1^2r_2^2+1}\frac{1}{z})}|+1 \leq 2^{\frac{n}{2}+1}+1, \end{aligned}$$

where the last inequality follows from Theorem 2.2 with $q=2^n, a=\frac{1}{r_1^2r_2^2+1}, b=\frac{r_1r_2}{r_1^2r_2^2+1}$ and $\chi(c)=(-1)^{\mathrm{Tr}(c)}$.

Clearly, it is a contradiction when $n\geq 4$. The proof is completed. □

Now we introduce the main theorem of this subsection.

Theorem 4.3: Let $n\geq 6$ be an even integer. Then any function in $\mathbb{S}_n=\{F_C(x)+f(x)|f\in\mathbb{B}_n\}$ is CCZ-inequivalent to the inverse function $I(x)$.

Proof: Otherwise, assume that there exists an n-variable Boolean function $f(x)$ such that $F_f(x)=F_C(x)+f(x)$ is CCZ-equivalent to $I(x)$. Let $R:\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\mapsto\mathbb{F}_2^{2n-1}$ be a surjective linear function with $\mathrm{Ker}(R)=\{(0,0),(0,1)\}$. According to Corollary 3.7, there exists a linearized permutation L corresponding to CCZ-equivalent transformation from I to F_f such that

$$\{*\ \delta_{F_C-R}(a,b)|(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\ *\}=\{*\ \delta_{I-R\circ L}(u,v)|(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\ *\}.$$

On one hand, it follows from $\mathrm{Ker}(R)=\{(0,0),(0,1)\}$ and Lemma 4.1 that $\delta_{F_C-R}(a,b)=J_{F_C-1}(a,b)\leq 4$ for any $a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}$. And when $a=0$, it is clear that $\delta_{F_C-R}(a,b)$ is either 0 or 2^n.

On the other hand, since $\mathrm{Ker}(R\circ L)=\{(0,0),(\mathcal{L}_2(1),\mathcal{L}_4(1))\}$, we have $\delta_{I-R\circ L}(u,v)=\delta_I(u,v)+\delta_I(u+\mathcal{L}_2(1),v+\mathcal{L}_4(1))$. Because of Lemma 4.2, there exist $u,v\in\mathbb{F}_{2^n}$ such that $\delta_I(u,v)+\delta_I(u+s,v+t)=6$ or 8. This means for any linearized permutation L, at least one elements in the set $\{*\ \delta_{I-R\circ L}(u,v)|(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\ *\}$ is 6 or 8, a contradiction.

Thus $F_f(x)=F_C(x)+f(x)$ and $I(x)$ are CCZ-inequivalent. □

Since $\mathbb{SP}_n$ is a subclass of $\mathbb{S}_n$, we directly get the following corollary.

Corollary 4.4: Let $n\geq 6$ be an even integer. Then any 4-uniform BCTTL permutation is CCZ-inequivalent to the inverse function.

B. The CCZ-inequivalence between two big classes of differentially 4-uniform functions

Now we consider the CCZ-inequivalence between 4-uniform BCTTL permutations and 4-uniform BI permutations. Due to the huge number of functions in these two classes, it is difficult to prove or to verify the CCZ-inequivalence between them even on small fields. By using the notion of joint differential value, we mathematically transform the problem to a trace equation system, and then verify it when $8\leq n\leq 14$ by Magma [3]. Hence these two huge classes of permutations are CCZ-inequivalent.

Lemma 4.5: Let $n\geq 8$ be an even integer. For arbitrary $s,t\in\mathbb{F}_{2^n}$, if there exists $u\in\mathbb{F}_{2^n}\backslash\{0,1,s,I(t),I(t+1)\}$, such that

$$\mathrm{Tr}(\frac{1}{1+u})=\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t)})=\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t+1)})=0,$$

then for the above u, one has

$$J_{I-1}(u,\frac{1}{u})+J_{I-1}(u+s,\frac{1}{u}+t)=10\ or\ 12.$$

Proof: It suffices to prove that for the above u, the sum of the numbers of the solutions of the following four equations is 10 or 12.

$$I(x)+I(x+u)=\tfrac{1}{u}, \tag{4}$$

$$I(x)+I(x+u)=\tfrac{1}{u}+1, \tag{5}$$

$$I(x)+I(x+u+s)=\tfrac{1}{u}+t, \tag{6}$$

$$I(x)+I(x+u+s)=\tfrac{1}{u}+t+1. \tag{7}$$

Clearly, (4) has 4 different solutions $0, u, \omega u, \omega^2 u$. Neither $x=0$ nor $x=u$ is a solution of (5). Hence (5) is equivalent to the quadratic function $x^2+ux+\frac{u^2}{u+1}=0$. It follows from Lemma 2.3 and the condition $\mathrm{Tr}(\frac{1}{1+u})=0$ that (5) has 2 different solutions. Hence $\delta_I(u,\frac{1}{u})+\delta_I(u,\frac{1}{u}+1)=6$.

Notice that (6) and (7) have no common solutions and each of them has the same number of solutions as a quadratic function when $x\neq 0, u+s$. Since $\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t)})=\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t+1)})=0$, these two quadratic functions have 4 different solutions together, which means $\delta_I(u+s,\frac{1}{u}+t)+\delta_I(u+s,\frac{1}{u}+t+1)=4$ *or* 6.

In conclusion, we have

$$\begin{aligned} & J_{I-1}(u,\frac{1}{u})+J_{I-1}(u+s,\frac{1}{u}+t)\\ = \;& \delta_I(u,\frac{1}{u})+\delta_I(u,\frac{1}{u}+1)+\delta_I(u+s,\frac{1}{u}+t)+\delta_I(u+s,\frac{1}{u}+t+1)\\ = \;& 10 \textit{ or } 12. \end{aligned}$$

We finish the proof. □

Fact 1: Suppose that $8\leq n\leq 14$ is an even integer, it can be verified by Magma that for any $s,t\in\mathbb{F}_{2^n}$, there exists $u\in\mathbb{F}_{2^n}\setminus\{0,1,s,I(t),I(t+1)\}$, such that

$$\mathrm{Tr}(\frac{1}{1+u})=\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t)})=\mathrm{Tr}(\frac{1}{(u+s)(\frac{1}{u}+t+1)})=0.$$

Here is the main result of this subsection.

Proposition 4.6: Suppose that $8\leq n\leq 14$ is an even integer. Then any function in $\mathbb{S}_n=\{F_C(x)+f(x)|f\in\mathbb{B}_n\}$ is CCZ-inequivalent to any function in $\mathbb{T}_n=\{I(x)+f(x)|f\in\mathbb{B}_n\}$.

Proof: On the contrary, assume that there exist n-variable Boolean functions $f_1(x), f_2(x)$ such that $F(x)=F_C(x)+f_1(x)$ and $G(x)=I(x)+f_2(x)$ are CCZ-equivalent. Let $R:\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\mapsto\mathbb{F}_2^{2n-2}$ be a surjective linear function with $\mathrm{Ker}(R)=\{(0,0),(0,1),(s,t),(s,t+1)\}$, where $\begin{bmatrix}\vec{s}\\ \vec{t}\end{bmatrix}=L\begin{bmatrix}\vec{0}\\ \vec{1}\end{bmatrix}$. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from G to F. According to Proposition 3.8, for any $(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, let $\begin{bmatrix}\vec{a}\\ \vec{b}\end{bmatrix}=L\begin{bmatrix}\vec{u}\\ \vec{v}\end{bmatrix}$, then we have

$$\{*\ \delta_{F_C-R}(a,b)|(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\ *\}=\{*\ \delta_{I-R\circ L}(u,v)|(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\ *\}.$$

On one hand, when $\mathrm{Ker}(R)=\{(0,0),(0,1),(s,t),(s,t+1)\}$, we have $\delta_{F_C-R}(a,b)=J_{F_C-1}(a,b)+J_{F_C-1}(a+s,b+t)$. It follows from Lemma 4.1 that $J_{F_C-1}(a,b)\leq 4$ for any $a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}$. And it is easy to show that the joint different value $J_{F_C-1}(0,b)=0$ or 2^n. Thus, for any linearized permutation L and for any $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$,

$$\delta_{F_C-R}(a,b)\leq 8 \textit{ or } \delta_{F_C-R}(a,b)\geq 2^n.$$

On the other hand, since $\mathrm{Ker}(R \circ L) = \{(0,0), (\mathcal{L}_2(1), \mathcal{L}_4(1)), (0,1), (\mathcal{L}_2(1), \mathcal{L}_4(1)+1)\}$, we have

$$\begin{aligned}\delta_{I-R\circ L}(u,v) &= \delta_I(u,v) + \delta_I(u,v+1) + \delta_I(u+\mathcal{L}_2(1), v+\mathcal{L}_4(1)) + \delta_I(u+\mathcal{L}_2(1), v+\mathcal{L}_4(1)+1) \\ &= J_{I-1}(u,v) + J_{I-1}(u+\mathcal{L}_2(1), v+\mathcal{L}_4(1)).\end{aligned}$$

Because of Lemma 4.5 and Fact 1, there exists $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$\delta_{I-R\circ L}(u,v) = 10 \ or \ 12,$$

a contradiction. Thus any function in $\mathbb{S}_n$ is CCZ-inequivalent to any function in $\mathbb{T}_n$. □

We make two comments on Proposition 4.6. First, the classes of 4-uniform BCTTL permutations and 4-uniform BI permutations are also CCZ-inequivalent when $8 \leq n \leq 14$ since they are subclasses of $\mathbb{S}_n$ and $\mathbb{T}_n$ respectively. Second, it is clear that for any $\gamma \in \mathbb{F}_{2^n}^*$ and an arbitrary Boolean function $f_1(x)$, there exists a Boolean function $f_2(x)$ such that $I(x) + \gamma f_1(x)$ is EA-equivalent to $I(x) + f_2(x)$. Therefore any function in $\mathbb{S}_n$ is CCZ-inequivalent to any function of the form of $I(x) + \gamma f(x)$ when $8 \leq n \leq 14$, where f is a Boolean function.

C. A new method to judge the CCZ-inequivalence on small fields

In this subsection, we propose an interesting problem: Given a differentially 4-uniform permutation $P(x)$ on small fields such as $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^8}$, can one check whether or not there exists some function in the classes of 4-uniform BCTTL permutations and 4-uniform BI permutations which is CCZ-equivalent to P? For example, the following is a differentially 4-uniform permutation $P_0(x)$ on $\mathbb{F}_{2^6}$ with nonlinearity 22.

TABLE I
AN EXAMPLE DIFFERENTIALLY 4-UNIFORM PERMUTATION

0	23	6	8	54	15	2	34
16	37	61	41	39	10	52	57
55	59	21	60	48	31	9	45
46	14	63	4	25	47	62	42
5	26	24	30	58	13	29	35
1	53	22	19	7	32	27	43
28	18	50	36	44	11	20	17
38	3	56	51	40	33	12	49

We indicate the example by vector expression. For example, the last element in the first row $34 = 2 + 2^5$ means that $P_0(7) = 34$, more precisely, it means that $P_0(1 + \alpha + \alpha^2) = \alpha + \alpha^5$, where α is a defining element of $\mathbb{F}_{2^6}$.

It is well known that two functions are CCZ-inequivalent if some CCZ-equivalent invariants are different for these two functions. Unfortunately, it is quite difficult to compute a given CCZ-equivalent invariant for all the functions in the classes of 4-uniform BCTTL permutations (its size is 4294967296) and 4-uniform BI permutations (its size is 16198656) on $\mathbb{F}_{2^6}$ due to their big cardinalities. However, the following proposition can help to answer this question.

Proposition 4.7: Let $n \geq 6$ be an even integer and let $P(x)$ be a differentially 4-uniform permutation on $\mathbb{F}_{2^n}$.

1) If

$$\{* \ \delta_P(u,v) + \delta_P(u+s, v+t) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\} \neq \{* \ J_{F_C-1}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ *\},$$

for all $(s,t) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, then $P(x)$ is CCZ-inequivalent to any 4-uniform BCTTL permutation.

2) If

$$\{* \ \delta_P(u,v)+\delta_P(u+s,v+t)|(u,v)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\} \neq \{* \ J_{I-1}(a,b)|(a,b)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\}$$

for all $(s,t)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, then $P(x)$ is CCZ-inequivalent to any 4-uniform BI permutation.

Proof: Here we only prove the first part. The proof for the rest is similar and is left to the interested readers.

Assume that there exists a 4-uniform BCTTL permutation $F_P(x)$ which is CCZ-equivalent to $P(x)$. By its definition, $F_P(x)$ can be got by adding a Boolean function $f_P(x)$ to the $\mathbb{F}_2$-component of $F_C(x)$, that is, $F_P(x)=F_C(x)+f_P(x)$. Let $R:\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}\mapsto\mathbb{F}_2^{2n-1}$ be a surjective linear function with $\mathrm{Ker}(R)=\{(0,0),(0,1)\}$. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from P to F_P. Then according to Corollary 3.7, we have

$$\{* \ \delta_{F_C-R}(a,b)|(a,b)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\} = \{* \ \delta_{P-R\circ L}(u,v)|(u,v)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\}.$$

Since $\mathrm{Ker}(R)=\{(0,0),(0,1)\}$, we have $\mathrm{Ker}(R\circ L)=\{(0,0),(\mathcal{L}_2(1),\mathcal{L}_4(1))\}$. Then

$$\delta_{F_C-R} = \ J_{F_C-1}(a,b)$$

for any $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ and

$$\delta_{P-R\circ L}(u,v)=\delta_P(u,v)+\delta_P(u+\mathcal{L}_2(1),v+\mathcal{L}_4(1))$$

for any $(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. Thus

$$\{* \ J_{F_C-1}(a,b)|(a,b)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\} = \{* \ \delta_P(u,v)+\delta_P(u+\mathcal{L}_2(1),v+\mathcal{L}_4(1))|(u,v)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\}.$$

Contradicts! We finish the proof. □

One can easily verify the following facts by computer.

Fact 2: For any $\gamma\in\mathbb{F}_{2^6}^*$, $\{* \ J_{I-\gamma}(a,b)|(a,b)\in \mathbb{F}_{2^6}\times\mathbb{F}_{2^6} \ *\} = \{*0^{1118} \ 2^{1980} \ 4^{936} \ 6^{60} \ 8^0 \ 64^2*\}$, which means the sum of the multiplicity of 6 and that of 8 in the multiset is 60.

Fact 3: Let $n\geq 6$ be an even integer. Then $\{* \ J_{F_0-1}(a,b)|(a,b)\in \mathbb{F}_{2^n}\times\mathbb{F}_{2^n} \ *\} = \{*0^{k_0} \ 2^{k_2} \ 4^{k_4} \ 6^0 \ 8^0 \ (2^n)^2*\}$, where $k_0,k_2,k_4\in N$.

Fact 4: For any $s,t\in\mathbb{F}_{2^6}$, the sum of the multiplicity of 6 and that of 8 in the multiset $\{* \ \delta_{P_0}(u,v)+\delta_{P_0}(u+s,v+t)|(u,v)\in \mathbb{F}_{2^6}\times\mathbb{F}_{2^6} \ *\}$ is no less then 114.

Then it follows from Proposition 4.7 and the above facts that $P_0(x)$ is CCZ-inequivalent to these two big differentially 4-uniform permutation classes.

V. Conclusion and further problems

A. Conclusion

It seems to be difficult to investigate the CCZ-equivalence relation between 4-uniform BCTTL permutations and 4-uniform BI permutations. One reason may be that the number of the functions in these two classes is too big. In this paper, we proposed a new notion which is called projected differential spectrum and deduce several relations between CCZ-equivalent functions. Based on these results, we mathematically proved that any 4-uniform BCTTL permutation is CCZ-inequivalent to the inverse function, and then proved that 4-uniform BCTTL permutations and 4-uniform BI permutations are CCZ-inequivalent when $8\leq n\leq 14$ with the help of a computer. At last, we presented a 4-uniform permutation on $\mathbb{F}_{2^6}$, which can be proved to be CCZ-inequivalent to any 4-uniform BCTTL permutation or any 4-uniform BI permutation.

As pointed out by a reviewer, our method can also be explained in the context of group rings. One can refer to [10] and the references therein for the definition of group rings and some of their applications to combinatorics and cryptography. Indeed, we consider the graph of the function F, which may be viewed

as an element D_F in the group ring $\mathbb{C}[\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}]$. Then we compute D_F^2 in the group ring and obtain an element A_F. If F and G are CCZ-equivalent, then A_F and A_G are equivalent. The classical way to check inequivalence between two (n, n)-functions F and G is to compare the differential spectrum of them. In this paper, we introduced *projected differential spectrum*, which is the value distribution of the projections of the differential value modulo subspaces. By projecting the function on $\mathbb{F}_2^{n-1}$ with a special surjective linear function, we found the connection of the projected differential spectrum between those functions which are CCZ-equivalent (Proposition 3.7). We computed the bounds for the coefficients of these projections for some classes of differentially 4-uniform functions (Lemma 4.1 and Lemma 4.2) and showed that they yield different coefficients (Theorem 4.3). We also applied the approach by projecting the function on $\mathbb{F}_2^{n-2}$ (Proposition 3.8).

B. Further problems

Some further problems are as follows. If the trace equation system in Lemma 4.5 has a solution for any even integer $n \geq 8$, then the class of 4-uniform BI permutations and that of 4-uniform BCTTL permutations are CCZ-inequivalent on $\mathbb{F}_{2^n}$. However, we can not prove it now and leave it to interested readers.

The projected differential spectrum can also be used to investigate the CCZ-inequivalence between a special function adding a multiple of a Boolean function and other functions. Beside the inverse function and the CTTL basic differentially 4-uniform permutation, APN functions such as the Gold functions, the Kasami functions and other functions with special differential spectrum may also be applicable to this method. And it would be nice to know whether our new approach can be also used to distinguish the CCZ-inequivalence between APN functions. In a word, to find more properties and applications about the projected differential spectrum is an interesting problem.

Our method is not necessary but sufficient, and we still can not investigate the CCZ-equivalence between different subclasses of 4-uniform BI permutations or between different subclasses of 4-uniform BCTTL permutations. It is interesting to find a valid method to solve this problem.

VI. ACKNOWLEDGEMENT

We are greatly indebted to the anonymous reviewers for their valuable comments and insightful observations, which allowed to significantly improve both the technique equality and the editorial equality of the paper. We would also like to thank Dr. Hai Xiong for very helpful discussions and useful information.

REFERENCES

[1] C. Carlet, Vectorial Boolean Functions for Cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Y.Crama and P.L.Hammer Eds) [M], Cambridge University Press, 2010.
[2] R. Lidl and H. Niederreiter. Finite Fields [M]. V2. Cambridge: Cambridge University Press, 1997.
[3] W. Bosma, J. Cannon and C. Playoust, The magma algebra system I: The user language. J.Symbolic Comput, Vol. 24, pp. 235-265, 1997.
[4] K.A. Browning, J.F. Dillon, M.T. McQuistan and A.J. Wolfe, An APN permutation in dimension six. Contemporary Mathematics Journal of American Mathematical Society, Vol. 518, pp. 33-42, 2010.
[5] C. Bracken and G. Leander, A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications, Vol. 16, No. 4, pp. 231-242, 2010.
[6] C. Bracken, C.H. Tan and Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity. Finite Fields and Their Applications, Vol. 18, No. 3, pp. 537-546, 2012.
[7] C. Carlet, On known and new differentially uniform functions. Information Security and Privacy, Vol. 6812, pp. 1-15, 2011.
[8] C. Carlet, More constructions of APN and differentially 4-uniform functions by concatenation. Science China Mathematics, Vol. 56, No. 7, pp. 1373-1384, 2013.
[9] C. Carlet, P. Charpin and V. Zinoviev, Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. Designs, Codes and Cryptography, Vol. 15, No. 2, pp. 125-156, 1998.

[10] C. Carlet and Y. Tan, On group rings and some of their applications to combinatiorics and cryptgraphy. International Journal of Group Theory, Vol. 4, No. 4, pp. 61-74, 2015.
[11] C. Carlet, D. Tang, X.H. Tang and Q.Y. Liao, New Construction of Differentially 4-Uniform Bijections. Information Security and Cryptology, Vol. 8567, pp. 22-38, 2014.
[12] X. Chen, Y.Z. Deng, M. Zhu and L.J. Qu, An Equivalent Condition on the Switching Construction of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$ from the Inverse Function. International Journal of Computer Mathematics, DOI:10.1080/00207160.2016.1167884.
[13] P. Charpin, G.M. Kyureghyan and V. Suder, Sparse permutations with low differential uniformity. Finite Fields and their Applications, Vol. 28, pp. 214-243, 2014.
[14] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic. Advances in Mathematical Communications. Vol. 3, No. 1, pp. 59-81, 2009.
[15] Y.Q. Li, M.S. Wang and Y.Y. Yu, Constructing Differentially 4-uniform Permutations over $F_{2^{2k}}$ from the Inverse Function Revisited. https://eprint.iacr.org/2013/731.pdf.
[16] J. Peng, C. Tan and Q.C. Wang, A new construction of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. http://arxiv.org/abs/1407.4884.pdf.
[17] L.J. Qu, Y. Tan, C. Li and G. Gong, More Constructions of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$. Designs, Codes and Cryptography, Vol. 78, No. 2, pp. 391-408, 2016.
[18] L.J. Qu, Y. Tan, C. Tan and C. Li, Constructing Differentially 4-Uniform Permutations over $\mathbb{F}_{2^{2k}}$ via the Switching Method. IEEE Transactions on Information Theory, Vol. 59, No. 7, pp. 4675-4686, 2013.
[19] D. Tang, C. Carlet and X.H. Tang, Differentially 4-Uniform Bijections by Permuting the Inverse Function. Designs, Codes and Cryptography, Vol. 77, No. 1, pp. 117-141, 2015.
[20] Y.Y. Yu, M.S. Wang and Y.Q. Li, Constructing differential 4-uniform permutations from know ones. Chinese Journal of Electronics, Vol. 22, No. 3, pp. 495-499, 2013.
[21] Z.B. Zha, L. Hu and S.W. Sun, Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields and Their Applications, Vol. 25, pp. 64-78, 2014.
[22] Z.B. Zha, L. Hu, S.W. Sun and J.Y. Shan, Further results on a class of differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$. Science China Mathematics, Vol. 58, No. 7, pp. 1577-1588, 2015.