More Constructions of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$

Longjiang Qu, Yin Tan, Chao Li and Guang Gong

Abstract

Differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with high nonlinearity are often chosen as Substitution boxes in both block and stream ciphers. Recently, Qu et al. introduced a class of functions, which are called preferred functions, to construct a lot of infinite families of such permutations [14]. In this paper, we propose a particular type of Boolean functions to characterize the preferred functions. On the one hand, such Boolean functions can be determined by solving linear equations, and they give rise to a huge number of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. Hence they may provide more choices for the design of Substitution boxes. On the other hand, by investigating the number of these Boolean functions, we show that the number of CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ grows exponentially when k increases, which gives a positive answer to an open problem proposed in [14].

Index Terms

Differentially 4-uniform permutation; Substitution box; preferred function; preferred Boolean function. MSC: 06E30, 11T60, 94A60

I. Introduction

In the design of many block ciphers and stream ciphers, permutations with specific properties are chosen as Substitution boxes to bring the confusion into ciphers. To prevent various attacks to the cipher and for the software implementation, such permutations are required to have low differential uniformity [1], high algebraic degree [9], high nonlinearity [12], and being defined on fields with even degrees, namely $\mathbb{F}_{2^{2k}}$, etc. Throughout this paper, we always let $n = 2k$ be an even integer.

It is well known that the lowest differential uniformity of a function defined on $\mathbb{F}_{2^n}$ can achieve is 2 and such functions are called *almost perfect nonlinear* (APN) functions. However, due to the lack of knowledge of the APN permutation in even dimension, constructions of differentially 4-uniform permutations with high

L. Qu and C. Li are with the College of Science, National University of Defense Technology, ChangSha, 410073, China, email: ljqu_happy@hotmail.com, lichao_nudt@sina.com. C. Li is also with the Science and Technology on Information Assurance Laboratory, Beijing, 100072, China. The research of L. Qu is supported by the National Natural Science Foundation of China (No. 61272484) and the Research Project of National University of Defense Technology under Grant CJ 13-02-01. The research of C. Li is supported by the National Basic Research Program of China 2013CB338002 and the open research fund of Science and Technology on Information Assurance Laboratory (Grant No. KJ-12-02).

Y. Tan and G. Gong are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada, email: {y24tan, ggong}@uwaterloo.ca.

algebraic degree and high nonlinearity over $\mathbb{F}_{2^{2k}}$ have attracted many researchers' interest. One may refer to [2], [3], [6], [7], [13]–[15] for recent progress on this problem. To the best of our knowledge, before [14], not many infinite families of differentially 4-uniform permutations are known. Among them, the multiplicative inverse function perhaps is the most popular one and it is endorsed as the Substitution box in the ciphers like AES, Camellia, SFINK, etc. In [14], the authors used the so-called switching method to construct many infinite families of such functions, which significantly increase the number of them (see [14, Table 1]). More precisely, they introduced a type of functions, which are called *preferred functions*, to discover a lot of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. All obtained functions are with highest algebraic degree $(2k-1)$ and relatively high nonlinearity (see Result 2.3 and Table II).

After obtaining many infinite families of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ as in [14], determining the number of CCZ-inequivalent classes among these functions arises as a natural question. It was observed in [14] that this number grows exponentially when k grows, and they proposed an open problem to determine, or give a lower bound of this number [14, Problem 4.16]. Since more constructions of preferred functions lead to more differentially 4-uniform permutations (Result 2.2 below), a characterization of preferred functions is clearly helpful to solve the above problem. Hence it was proposed in [14] as another open problem to find more or give a characterization of preferred functions [14, Problem 4.15].

The purpose of this paper is to proceed further the research of [14] and to answer the above two problems.

We should mention that a similar question about the number of CCZ-inequivalent classes of APN functions has been proposed in [8]. Recently the results reported in [16], [17] gave a positive evidence (thousands of APN functions are discovered on $\mathbb{F}_{2^7}, \mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$). However, a theoretical proof of this problem currently seems unavailable.

In Section II, we propose a new type of Boolean functions, called *preferred Boolean functions* (Definition 2.4, PBF for short), to characterize preferred functions. Such Boolean functions are shown to be able to construct differentially 4-uniform permutations (Theorem 2.6). More interestingly, these Boolean functions can be efficiently determined. Precisely, it is proven in Theorem 2.7 that the determination of such Boolean functions can be reduced to solving linear equations. By estimating the 2-rank of the coefficient matrix of this linear equation system, we prove that there exist at least $2^{\frac{2^n+2}{3}}$ preferred Boolean functions with n variables. Hence, by Theorem 2.6, we construct at least $2^{\frac{2^n+2}{3}}$ differentially 4-uniform permutations on $\mathbb{F}_{2^n}$. This is a huge number, which shows that, by making use of preferred Boolean functions, we may give much more differentially 4-uniform permutations than those given in [14]. For example, we have 2^{86} preferred Boolean functions on $\mathbb{F}_{2^8}$, and hence construct the same number of differentially 4-uniform permutations on $\mathbb{F}_{2^8}$ (Theorem 2.6), which is a great improvement of the $2^{\frac{n}{2}+7} = 2^{11}$ such permutations constructed in [14] ([14, Remark 4.14]).

Based on the investigation of the number of preferred Boolean functions, in Theorem 2.8, we show that the number of CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ among those constructed in Theorem 2.6, denoted by $N(n)$, is at least $2^{\frac{2^n+2}{3}-4n^2-2n}$. This shows that the number of differentially

4-uniform permutations on $\mathbb{F}_{2^{2k}}$ **does** increase exponentially when k grows.

In Table I below, the value or a lower bound of $N(n)$ is listed for $6 \le n \le 16$. Some remarks on the table are as follows. One may be curious about why $N(6)$ seems to be quite large while the lower bounds of $N(8)$ and $N(10)$ seems to be weak. The reasons are as follows. On the one hand, thanks to Theorem 2.7, it can be shown that there are 2^{22} preferred Boolean functions on $\mathbb{F}_{2^6}$. Hence by Theorem 2.6 we may construct 2^{22} differentially 4-uniform permutations on $\mathbb{F}_{2^6}$. The small number of PBFs on this field enables us to perform an exhaustive search of CCZ-inequivlaent such functions on $\mathbb{F}_{2^6}$, namely to determine the exact value of $N(6)$. The method we distinguish two CCZ-inequivalent functions is to compare whether the codes corresponding to them are equivalent (see [5] or [4, page 43]). On the other hand, when $n = 8, 10$, the authors in [14] only counted the number of differentially 4-uniform permutations with different differential spectrum, which is only an invariant of CCZ-equivalence.

TABLE I
THE NUMBER OF CCZ-INEQUIVALENT DIFFERENTIALLY 4-UNIFORM PERMUTATIONS AMONG THOSE CONSTRUCTED IN THEOREM 2.6 ON $\mathbb{F}_{2^n}$ WHEN $6 \le n \le 16$ (n EVEN)

n	$N(n)$	Ref
6	$11,120$	Exhaustive search
8	≥ 107	[14, Table 1]
10	≥ 183	[14, Table 1]
12	$\ge 2^{766}$	Theorem 2.8(iii)
14	$\ge 2^{4650}$	Theorem 2.8(iii)
16	$\ge 2^{20790}$	Theorem 2.8(iii)

In Section II.C, we relate the lower bound of $N(n)$ to the rank of the coefficient matrix M of certain linear equation system (Problem 2.9), and the problem to determine a lower bound of the number of the functions which are CCZ-equivalent to a given function (Problem 2.10). For Problem 2.9, in Section II.D, we provide a possible method to solve it by relating the rank of the coefficient matrix to the existence of a 3-regular subgraph of the graph determined by the matrix (Definition 2.16). Some properties of this graph are also presented therein.

As known from Theorem 2.7(i), the set of all preferred Boolean functions is a $\mathbb{F}_2$-subspace. In Section III, we investigate the so-called *non-decomposable* preferred Boolean functions. A preferred Boolean function f is called *non-decomposable* if it is not the sum of the other two preferred Boolean functions whose support sets are proper subsets of the support of f. In Theorem 3.2, we present the characterization of these functions in terms of their support sets. Then many explicit constructions of differentially 4-uniform permutations are presented. It is an evidence that preferred Boolean functions is a more efficient tool than preferred functions to construct differentially 4-uniform permutations.

The rest of the paper is organized as follows. In Section II, we first recall some results appeared in [14], and then introduce the definition and the properties of the preferred Boolean functions and its application to construct differentially 4-uniform permutations, and followed by presenting a lower bound of the number of CCZ-inequivalent classes of constructed permutations. In Section III, we focus on the characterization of non-decomposable preferred Boolean functions. Some concluding remarks are given in Section IV.

We end this section by introducing some notations. 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* with n variables. Clearly, a Boolean function may be regarded as a vector with elements on $\mathbb{F}_2$ of length 2^n by identifying $\mathbb{F}_{2^n}$ with a vector space $\mathbb{F}_2^n$ of dimension n over $\mathbb{F}_2$. In the following, we will switch between these two points of view without explanation if the context is clear. Let f be a nonzero Boolean function. Define the set $\mathrm{Supp}(f) = \{x \in \mathbb{F}_{2^n} | f(x) = 1\}$ and call it the *support set* of f. The value $|\mathrm{Supp}(f)|$ is called the *(Hamming) weight* of f. Denote by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Note that for the multiplicative inverse function x^{-1}, we define $0^{-1} = 0$ as usual.

II. Preferred Functions and Preferred Boolean Functions

In this section, we introduce preferred Boolean functions to characterize preferred functions. Then the properties of preferred Boolean functions are investigated. Finally, a lower bound of the number of CCZ-inequivalent differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ is presented.

A. Preferred functions

First, we recall the definition of preferred functions.

Definition 2.1: [14] Let $n = 2k$ be an even integer and R be an (n, n)-function. Define the Boolean function D_R by

$$D_R(x) = \mathrm{Tr}(R(x+1) + R(x)), \tag{1}$$

and define the functions Q_R, P_R by

$$\begin{aligned} Q_R(x, y) &= D_R\left(\frac{1}{x}\right) + D_R\left(\frac{1}{x} + y\right), \text{ and} && (2)\\ P_R(y) &= Q_R(0, y) = D_R(0) + D_R(y). && (3)\end{aligned}$$

Let U be the subset of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ defined by

$$U = \{(x, y) | x^2 + \frac{1}{y}x + \frac{1}{y(y+1)} = 0, y \notin \mathbb{F}_2\}. \tag{4}$$

If

$$Q_R(x, y) + P_R(y) = 0 \tag{5}$$

holds for any pair (x, y) in U, then we call R a *preferred function* (PF for short) on $\mathbb{F}_{2^n}$, or call it *preferred* on $\mathbb{F}_{2^n}$. In particular, if D_R is the zero function, then clearly R is a PF and it is called *trivial*.

Preferred functions may be used to construct differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ as follows.

Result 2.2: [14, Theorem 3.6] Let $n = 2k$ be an even integer, $I(x) = x^{-1}$ be the multiplicative inverse function and R be an (n, n)-function. Define

$$H(x) = x + \mathrm{Tr}(R(x) + R(x + 1)), \text{ and}$$
$$G(x) = H(I(x)).$$

If $R(x)$ is a preferred function, then $G(x)$ is a differentially 4-uniform permutation polynomial on $\mathbb{F}_{2^n}$.

A lower bound of the nonlinearity of the functions defined in the above result is as follows.

Result 2.3: [14, Theorem 5.4] For any positive even integer n, let G be a function as defined in Result 2.2. Then we have $\mathrm{NL}(G) \geq 2^{n-2} - \frac{1}{4}\lfloor 2^{\frac{n}{2}+1} \rfloor - 1$, where $\mathrm{NL}(G)$ denotes the nonlinearity of the function G.

B. Preferred Boolean functions

Now we introduce a new type of Boolean functions, called *preferred Boolean function* below, to characterize preferred functions.

Definition 2.4: Let $n = 2k$ be an even integer and f be an n-variable Boolean function. We call f a *preferred Boolean function* (PBF for short) if it satisfies the following two conditions:

(i) $f(x + 1) = f(x)$ for any $x \in \mathbb{F}_{2^n}$;

(ii) $f\left(\frac{1}{x}\right) + f\left(\frac{1}{x} + y\right) + f(0) + f(y) = 0$ for any pair $(x, y) \in U$, where U is defined by (4) in Definition 2.1.

The following result points out the relationship between preferred functions and preferred Boolean functions.

Proposition 2.5: Let $n = 2k$ be an even integer and R be an (n, n)-function. Define the Boolean function D_R as in (1). Then R is a preferred function if and only if D_R is a preferred Boolean function. Furthermore, for any preferred Boolean function f with n variables, there are $2^{n \cdot 2^n - 2^{n-1}}$ preferred functions R such that $D_R(x) = f(x)$. In particular, there are $2^{n \cdot 2^n - 2^{n-1}}$ trivial preferred functions on $\mathbb{F}_{2^n}$.

Proof: The first part follows directly from the definitions of PF and PBF. Now, given a PBF f on $\mathbb{F}_{2^n}$, suppose that R is an (n, n)-function satisfying $D_R(x) = \mathrm{Tr}(R(x + 1) + R(x)) = f(x)$. Next we count the number of such R. Note that there are 2^{n-1} pairs of $(x, x + 1)$ in $\mathbb{F}_{2^n}$. For each such pair, $R(x)$ can be any value in $\mathbb{F}_{2^n}$, and $R(x + 1)$ can be any value such that $\mathrm{Tr}(R(x + 1) + R(x)) = f(x)$ is fixed, which means that $R(x + 1)$ can take 2^{n-1} different values. Thus we have in total $\left(2^n \cdot 2^{n-1}\right)^{2^{n-1}} = 2^{n \cdot 2^n - 2^{n-1}}$ preferred functions R such that $D_R(x) = f(x)$. The statement about the number of trivial preferred functions then follows. We complete the proof. ■

By Result 2.2 and Proposition 2.5, it is clear that PBFs can be used to construct differentially 4-uniform permutations.

Theorem 2.6: Let $n = 2k$ be an even integer, $I(x) = x^{-1}$ be the multiplicative inverse function and f be a Boolean function with n variables. Define

$$\begin{aligned} H(x) &= x + f(x), \text{ and} \\ G(x) &= H(I(x)). \end{aligned}$$

If $f(x)$ is a preferred Boolean function, then $G(x)$ is a differentially 4-uniform permutation polynomial on $\mathbb{F}_{2^n}$.

C. Number of CCZ-inequivalent differentially 4-uniform permutations

It is clear that f is a preferred Boolean function if and only if so is $f + 1$. For convenience, we assume that $f(0) = 0$ in the rest of the paper. The following result provides a method to tell whether a Boolean function is a PBF.

Theorem 2.7: Let $n = 2k$ 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 f is a preferred Boolean function if and only if it satisfies the following two conditions:

(i) $f(x + 1) = f(x)$ for any $x \in \mathbb{F}_{2^n}$;

(ii) $f\left(\alpha + \frac{1}{\alpha}\right) + f\left(\omega\alpha + \frac{1}{\omega\alpha}\right) + f\left(\omega^2\alpha + \frac{1}{\omega^2\alpha}\right) = 0$ for any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$.

Proof: We first determine the elements in U (recall its definition in (4)). Given any $(x, y) \in U$, we have $x^2 + \frac{1}{y}x + \frac{1}{y(y+1)} = 0$. It is easy to see that this equation has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}\left(\frac{1}{y(y+1)} \cdot y^2\right) = \mathrm{Tr}\left(\frac{y}{1+y}\right) = \mathrm{Tr}(\frac{1}{1+y}) = 0$. Furthermore, by [11, Lemma 4.1], for such y, there exists $\alpha \in \mathbb{F}_{2^n}^*$ such that $y + 1 = \alpha + \alpha^{-1}$.

Next we solve the equation

$$x^2 + \frac{1}{y}x + \frac{1}{y(y+1)} = 0. \tag{6}$$

Let $x = \frac{1}{y}(z + \omega)$. Then we have $z^2 + z + \frac{1}{y+1} = 0$. With $y + 1 = \alpha + \alpha^{-1}$, we get $z = \frac{1}{\alpha+1}$ or $z = \frac{\alpha}{\alpha+1}$. If $z = \frac{1}{\alpha+1}$, then

$$\begin{aligned} \frac{1}{x} &= \frac{y}{z+w} = \frac{\alpha + \alpha^{-1} + 1}{(\alpha+1)^{-1} + w} = \frac{(\alpha+1)^2\alpha + (\alpha+1)}{\alpha(w(\alpha+1)+1)} \\ &= \frac{\alpha^3+1}{w\alpha(\alpha+w)} = \frac{\alpha^2 + w\alpha + w^2}{w\alpha} = \omega^2\alpha + \frac{1}{\omega^2\alpha} + 1. \end{aligned}$$

Hence

$$\left(\frac{1}{x} + 1, \frac{1}{x} + y\right) = \left(\omega^2\alpha + \frac{1}{\omega^2\alpha}, \omega\alpha + \frac{1}{\omega\alpha}\right)$$

If $z = \frac{\alpha}{1+\alpha}$, similar computations give the following result:

$$\left(\frac{1}{x} + 1, \frac{1}{x} + y\right) = \left(\omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}\right).$$

The rest of the proof follows from the definition of PBF, the assumption $f(0) = 0$ and the fact that $y \in \mathbb{F}_2$ if and only if $\alpha \in \mathbb{F}_4$. We complete the proof. ■

The characterization of PBFs in Theorem 2.7 is useful to determine all PBFs. First note that, when $\alpha \notin \mathbb{F}_4$, the elements $\alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}$ are all distinct (since the sum of them is 0, and none of them can be zero). In the following result, we denote the set of all PFs and PBFs by $\mathcal{PF}$ and $\mathcal{PBF}$, respectively.

Theorem 2.8: Let $n = 2k$ be an even integer. Then the following results hold:

(i) The set $\mathcal{PF}$ (resp. $\mathcal{PBF}$) are $\mathbb{F}_2$-subspaces of the set of all (n, n)-functions (resp. the set of all n-variable Boolean functions).

(ii) The dimension of $\mathcal{PBF}$ is $2^n - 1 - \mathrm{rank}(M)$, and the dimension of $\mathcal{PF}$ is $n \cdot 2^n + 2^{n-1} - 1 - \mathrm{rank}(M)$, where M is the matrix defined in (7) below.

(iii) There are at least $2^{\frac{2^n+2}{3} - 4n^2 - 2n}$ CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ among all the functions constructed by Theorem 2.6 or equivalently, by Result 2.2.

Proof: (i) It is clear from the definitions that $\mathcal{PBF}$ and $\mathcal{PF}$ are $\mathbb{F}_2$-subspaces.

(ii) First note that determining f is equivalent to determining all the images $f(x)$ for $x \in \mathbb{F}_{2^n}$. Now let f be a PBF (recall that we assume $f(0) = f(1) = 0$, and therefore we only need to determine the images of f on $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$). By the two conditions in Theorem 2.7, clearly we may obtain all such PBFs by solving linear equations as follows.

Define the following two sets:

$$\begin{aligned} L_1 &= \{\{x, x+1\} : x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\}, \\ L_2 &= \left\{\{\alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}\} : \alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4\right\}. \end{aligned}$$

Clearly $|L_1| = 2^{n-1} - 1$. Note that when $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, the six elements $\alpha, \omega\alpha, \omega^2\alpha, \frac{1}{\alpha}, \frac{1}{\omega\alpha}, \frac{1}{\omega^2\alpha}$ are distinct, and any one leads to the same element of L_2. Hence $|L_2| = \frac{2^n-4}{3\cdot 2} = \frac{2^{n-1}-2}{3}$. Let v_x and v_α be the characteristic function of each $\{x, x+1\} \in L_1$ and $\{\alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}\} \in L_2$, respectively. Define the $(|L_1| + |L_2|) \times (2^n - 2)$ matrix M by

$$M = \begin{bmatrix} v_x \\ v_\alpha \end{bmatrix}, x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2, \alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4, \tag{7}$$

where the columns and rows of M are indexed by the elements in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ and $L_1 \cup L_2$ respectively. It follows from Theorem 2.7 that a Boolean function f is a PBF with $f(0) = 0$ if and only if

$$Mf^{\mathrm{T}} = 0.$$

Note that in the above equation, by abuse of notation, we still use f^{T} to denote the value vector of f on $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$. Therefore the dimension of the set of all PBFs with $f(0) = 0$ is $2^n - 2 - \mathrm{rank}(M)$.

It is clear that $f + 1$ is also a PBF if f is a PBF, hence altogether the dimension of $\mathcal{PBF}$ is $2^n - 2 - \mathrm{rank}(M) + 1 = 2^n - 1 - \mathrm{rank}(M)$. The dimension of $\mathcal{PF}$ then follows from that of $\mathcal{PBF}$ and Proposition

2.5.

(iii) On the one hand, we have

$$\begin{aligned}\mathrm{rank}(M) &\leq \min\{|L_1|+|L_2|, 2^n-2\}\\ &= \min\{\frac{2^{n+1}-5}{3}, 2^n-2\} = \frac{2^{n+1}-5}{3}.\end{aligned}$$

Hence, the dimension of $\mathcal{PBF}$, which is one plus the dimension of the null space of M, is at least $2^n - 2 - \frac{2^{n+1}-5}{3} + 1 = \frac{2^n+2}{3}$. It then follows from Theorem 2.6 that we can obtain at least $2^{\frac{2^n+2}{3}}$ differentially 4-uniform permutations on $\mathbb{F}_{2^n}$.

On the other hand, for any (n,n)-function, there are at most $(2^n)^{4n+2} = 2^{4n^2+2n}$ functions which are CCZ-equivalent to it. Indeed, given two (n,n)-functions F and G. If G is CCZ-equivalent to F, then by definition there exists an affine automorphism L of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$L\left(\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}\right) = \{(y, G(y)) : y \in \mathbb{F}_{2^n}\}. \tag{8}$$

Clearly we may write $L = (L_1, L_2)$, where L_i is an affine function from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Define the functions $\mathcal{L}_i(x) = L_i(x, F(x))$ for $i = 1, 2$, we may rewrite the equation (8) as

$$\begin{aligned}&\{(y, G(y)) : y \in \mathbb{F}_{2^n}\} = L\left(\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}\right)\\ =\;& \{(L_1(x, F(x)), L_2(x, F(x))) : x \in \mathbb{F}_{2^n}\}\\ =\;& \{(\mathcal{L}_1(x), \mathcal{L}_2(x)) : x \in \mathbb{F}_{2^n}\}\\ =\;& \{(x, \mathcal{L}_2(\mathcal{L}_1^{-1}(x)) : x \in \mathbb{F}_{2^n}\}.\end{aligned}$$

which implies that $G = \mathcal{L}_2(\mathcal{L}_1^{-1}(x))$, and then we can see that once $\mathcal{L}_1$ and $\mathcal{L}_2$ are determined, G is determined. Clearly an affine mapping $\varphi : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be represented as the form

$$\varphi(x, y) = \sum_{i=0}^{n-1} a_i x^{2^i} + \sum_{i=0}^{n-1} b_i y^{2^i} + c,$$

where $a_i, b_i, c \in \mathbb{F}_{2^n}$. Therefore, there are at most $(2^n)^{2n+1}$ choices of L_1 and L_2 respectively, and then altogether there are at most $(2^n)^{4n+2}$ functions G which are CCZ-equivalent to F.

Finally, it follows that the number of CCZ-inequivalent differentially 4-uniform permutations on $\mathbb{F}_{2^n}$ is at least

$$\frac{2^{\frac{2^n+2}{3}}}{2^{n(4n+2)}} = 2^{\frac{2^n+2}{3}-4n^2-2n}.$$

We complete the proof. ■

Several remarks on the above theorem are in the sequel.

(i) By MAGMA, when $6 \leq n \leq 14$, we compute the rank of the matrix M defined in (7) and found that they are all equal to $\frac{2^{n+1}-5}{3}$. We cannot prove this and leave it to interested readers, and we will present some possible methods to solve this problem in the next subsection.

Problem 2.9: To prove that the rank of the matrix M defined in (7) is $\frac{2^{n+1}-5}{3}$.

(ii) In the proof of Theorem 2.8(iii), the bound on the number of the functions G which are CCZ-equivalent to a given function F is loose as we do not consider the requirement that L is a permutation. A polished such number would yield a better lower bound of the number of CCZ-inequivalent differentially 4-uniform permutations. We propose it as an open problem.

Problem 2.10: Given an (n,n)-function (or a permutation) F, determine the number, or an upper bound of the number of the functions G which are CCZ-equivalent to F.

(iii) Theorem 2.8(iii) shows that the number of CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ (n even) grows double exponentially when n grows. This has been observed in [14] and proposed as an open problem. To the best of our knowledge, this is the first bound on the number of CCZ-inequivalent classes of differentially 4-uniform permutations on $\mathbb{F}_{2^n}$ with n even.

In the end of this subsection, we give some comments on the nonlinearity of the differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ constructed by Theorem 2.6. Clearly, the lower bound of the nonlinearity in Result 2.3 holds for all these functions. However, as mentioned in [14, page 11], this bound is not tight. To show this, on small fields, we randomly choose some differentially 4-uniform permutations constructed in Theorem 2.6 and compute the average value of their nonlinearity. Thanks to the characterization of PBF by solving linear equation system, we can perform such a random search. The computational results are given in the following table. The sample size means how many differentially 4-uniform permutations we choose, Ave(NL) denotes the average nonlinearity of them, and known maximal value of nonlinearity is the value $2^{n-1}-2^{n/2}$.

TABLE II
AVERAGE NONLINEARITY OF THE DIFFERENTIALLY 4-UNIFORM PERMUTATIONS CONSTRUCTED BY THEOREM 2.6 ON $\mathbb{F}_{2^n}$ WHEN $6 \le n \le 10$ (n EVEN)

n	Sample size	Ave(NL)	Bound in Result 2.3	Known Maximal Value
6	$10,000$	18.395	14	24
8	$10,000$	94.198	55	112
10	$5,000$	434.06	239	480

D. More on the Rank of M

In this subsection, we present a possible method to determine the rank of M using graph theory. For convenience, we first introduce some notations. For any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, we call the set $R_\alpha = \{\alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}\}$ a *triple set* with respect to α (or TS for short). Define the set $\mathcal{TS} = \{R_\alpha | \alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4\}$. It is known from the last subsection that $|\mathcal{TS}| = \frac{2^{n-1}-2}{3}$.

We first present some properties of triple sets defined above.

Lemma 2.11: The set $\mathcal{TS}$ is a partition of the set $S = \{x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 | \mathrm{Tr}\,(1/x) = 0\}$.

Proof: Clearly $\bigcup_{\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4} R_\alpha \subseteq S$. Conversely, for any $y \in S$, there exists $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $y = \alpha + \frac{1}{\alpha}$. It follows that $y \in R_\alpha$. Therefore, $S \subseteq \bigcup_{\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4} R_\alpha$. So $S = \bigcup_{\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4} R_\alpha$.

Furthermore, assume that $a \in R_\alpha \cap R_\beta$, where $R_\alpha, R_\beta \in \mathcal{TS}$. WLOG, assume that $a = \alpha + \frac{1}{\alpha} = \beta + \frac{1}{\beta}$. We have either $\alpha = \frac{1}{\beta}$ or $\alpha = \beta$ as $x + 1/x$ is a 2-to-1 mapping from $\mathbb{F}_{2^n} \setminus \mathbb{F}_4$ to S. It then follows that in each case, we have $R_\alpha = R_\beta$. The proof is finished. ■

Lemma 2.12: Let $R = \{a_1, a_2, a_3\} \in \mathcal{TS}$. Then the following results hold:

(i) $a_1 + a_2 + a_3 = 0$;

(ii) $1 + a_i \notin R$ for any $1 \leq i \leq 3$.

Proof: (i) follows directly from the definition of the triple set. (ii) can be deduced from (i) and the fact that $1 \notin R$. ■

We define the following sets for later usage:

$$\begin{aligned} T_1 &= \{x \in \mathbb{F}_{2^n} | \mathrm{Tr}\left(\frac{1}{x}\right) = \mathrm{Tr}\left(\frac{1}{x+1}\right) = 1\}, \\ T_2 &= \{x \in \mathbb{F}_{2^n} | \mathrm{Tr}\left(\frac{1}{x}\right) + \mathrm{Tr}\left(\frac{1}{x+1}\right) = 1\}, \\ T_3 &= \{x \in \mathbb{F}_{2^n} | \mathrm{Tr}\left(\frac{1}{x}\right) = \mathrm{Tr}\left(\frac{1}{x+1}\right) = 0\}. \end{aligned} \tag{9}$$

It is clear that T_1, T_2 and T_3 is a partition of $\mathbb{F}_{2^n}$ and for any element a of S, either $a \in T_2$ or $a \in T_3$.

Definition 2.13: Let R_1 and R_2 be two TSs. If there exist $a \in R_1$ and $b \in R_2$ such that $a + b = 1$, then we call R_1 and R_2 are *adjacent*, and call R_1, R_2 *neighbours*. More precisely, we call R_2 is adjacent to R_1 at a, and symmetrically, call R_1 is adjacent to R_2 at b.

It follows from Lemma 2.12 that any TS can not be a neighbour of itself. It is also clear that any TS has at most three neighbours.

Lemma 2.14: Let R be a triple set. Then R has either three neighbours or only one neighbour.

Proof: Assume that $R = \{\alpha + \frac{1}{\alpha}, \omega\alpha + \frac{1}{\omega\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha}\}$ for some $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$. For any $0 \leq i \leq 2$, there exists a neighbour of R which is adjacent at $\omega^i\alpha + \frac{1}{\omega^i\alpha}$ if and only if

$$\mathrm{Tr}\left(\frac{1}{\omega^i\alpha + \frac{1}{\omega^i\alpha} + 1}\right) = 0.$$

Further, we have

$$\begin{aligned} & \mathrm{Tr}\left(\frac{1}{\omega^i\alpha + \frac{1}{\omega^i\alpha} + 1}\right) = 0 \\ \Leftrightarrow \quad & \mathrm{Tr}\left(\frac{\omega^i\alpha}{(\omega^i\alpha + \omega)(\omega^i\alpha + \omega^2)}\right) = 0 \\ \Leftrightarrow \quad & \mathrm{Tr}\left(\frac{\omega^i\alpha}{\omega^i\alpha + \omega}\right) = \mathrm{Tr}\left(\frac{\omega^i\alpha}{\omega^i\alpha + \omega^2}\right) \\ \Leftrightarrow \quad & \mathrm{Tr}\left(\frac{1}{1 + \omega^{1-i}\alpha^{-1}}\right) = \mathrm{Tr}\left(\frac{1}{1 + \omega^{2-i}\alpha^{-1}}\right). \end{aligned}$$

Since

$$\sum_{i=0}^{2}\left(\mathrm{Tr}\left(\frac{1}{1+\omega^{1-i}\alpha^{-1}}\right)+\mathrm{Tr}\left(\frac{1}{1+\omega^{2-i}\alpha^{-1}}\right)\right)=0,$$

we know that $\mathrm{Tr}\left(\frac{1}{\omega^i\alpha+\frac{1}{\omega^i\alpha}+1}\right), 0\le i\le 2$ are either all zeros or exactly one zero. Hence R has either three neighbours or only one neighbour. ■

Definition 2.15: Let R be a TS. If R has three neighbours, then we call R an A-type TS. Otherwise, we call it a B-type TS.

By Lemma 2.14, a TS is either A-type or B-type. A TS R_α is an A-type TS if and only if $\mathrm{Tr}(\frac{1}{1+\alpha^{-1}})=\mathrm{Tr}(\frac{1}{1+\omega\alpha^{-1}})=\mathrm{Tr}(\frac{1}{1+\omega^2\alpha^{-1}})$, and if and only if all the elements of R_α are in T_3. For a B-type TS, two of its elements are in T_2 while exactly one element is in T_3.

Definition 2.16: Define the graph $\mathcal{G}=(V,E)$ from TSs as follows:

- The vertices are all TSs R_α, where $\alpha\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4$;
- Two vertices R_α, R_β are joined by an edge if and only if they are adjacent.

We summarize some properties of the graph $\mathcal{G}$ defined above in the following result.

Proposition 2.17: Let $\mathcal{G}$ be the graph defined above. Then the following results hold:

(i) The degree of each vertex is either 1 or 3;

(ii) The rank of M is $\frac{2^{n+1}-5}{3}$ if and only if the graph $\mathcal{G}$ does not have a 3-regular subgraph, i.e. all vertices in the subgraph have degree exactly 3.

Proof: (i) The result follows from Lemma 2.14.

(ii) Note that any row vector of M has Hamming weight either 2 or 3. For a row vector with Hamming weight 3, its support corresponds to a TS; while for a row vector with Hamming weight 2, its support corresponds to a set with form $\{\beta, 1+\beta\}, \beta\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$. Assume that the row vectors of M are linear dependent over $\mathbb{F}_2$. Since the supports of any two vectors of M with the same Hamming weight are disjoint, we have $\xi_1+\cdots+\xi_s=\eta_1+\cdots+\eta_t$, where ξ_i are vectors with Hamming weight 3 and η_j are those with weight 2. Let the corresponding TS of ξ_i be R_i and let $R_1=\{a,b,c\}$. Then a and $1+a$ are in $\bigcup_{j=1}^{t}\mathrm{Supp}(\eta_j)=\bigcup_{j=1}^{s}\mathrm{Supp}(\xi_j)$. Hence $1+a$ is in the support of ξ_i for some $2\le i\le s$. So are $1+b$ and $1+c$. It then follows that R_1 has 3 neighbours and the set of its neighbours is a subset of $\{R_i|2\le i\le s\}$. Denote by $\mathcal{H}$ the subgraph of $\mathcal{G}$ formed by the vertices $R_i, 1\le i\le s$. Then $\mathcal{H}$ is a 3-regular subgraph of $\mathcal{G}$. We complete the proof. ■

We use the following table to list some properties of the graph $\mathcal{G}$ defined above. For the definition of the girth, connected components and diameter, please refer to any textbook on graph theory. The value of diameter in the table refers to the largest diameter of each connected components.

TABLE III

COMPUTATIONAL RESULTS OF THE GRAPH $\mathcal{G}$ ON $\mathbb{F}_{2^n}$ FOR $6\le n\le 12$ WITH n EVEN

n	# of vertices	# of edges	Girth	# of connected components	Diameter
6	10	6	no cycle	4	2
8	42	35	8	8	6
10	170	120	5	51	4
12	682	517	9	170	18

III. Non-decomposable Preferred Boolean Functions

It is known from Proposition 2.5 that the set $\mathcal{PBF}$ is a $\mathbb{F}_2$-subspace. To obtain linear independent PBFs, we focus on non-decomposable PBFs in this section. After introducing its definition, we give a characterization of non-decomposable PBFs. Then a large subspace of PBFs is explicitly constructed, which can lead to many differentially 4-uniform permutations.

Definition 3.1: Let f be a nonzero PBF. If there exist two PBFs f_1 and f_2 such that $f = f_1 + f_2$ and $\mathrm{Supp}(f_i) \subsetneq \mathrm{Supp}(f), 1 \le i \le 2$, then f is called *decomposable*. Otherwise it is called *non-decomposable*.

Before giving the characterization of non-decomposable PBFs, we first state some properties of them. Let f be a non-decomposable PBF with $f(0) = 0$. By Theorem 2.8(ii), we have $Mf^{\mathrm{T}} = 0$. Since $f(x+1) = f(x)$ holds for any $x \in \mathbb{F}_{2^n}$, the weight of f must be even. Assume that $|\mathrm{Supp}(f)| = 2t$ and $\mathrm{Supp}(f) = \{\beta_i, \beta_i + 1 | 1 \le i \le t\}$ for some positive integer t. Let R be a TS. Then $|\mathrm{Supp}(f) \cap R| = 0$ or 2. In the following, assume that there are r $(0 \le r \le t)$ TSs $R_i = \{a_i, b_i, a_i + b_i\}$ such that $\mathrm{Supp}(f) \cap R_i = \{a_i, b_i\}$. Since $\mathcal{TS}$ is a disjoint union of the set $S = \{x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 | \mathrm{Tr}(1/x) = 0\}$, we have $\mathrm{Supp}(f) \cap S = \bigcup_{i=1}^{r} (R_i \cap \mathrm{Supp}(f))$.

Now we present the main theorem in this section. Recall that the sets T_i $(1 \le i \le 3)$ are defined in (9).

Theorem 3.2: Let f be a Boolean function with n variables. Then the following results hold:

(i) If $t = 1$, then f is a non-decomposable PBF if and only if $r = 0$ and there exists $\beta \in T_1$ such that $\mathrm{Supp}(f) = \{\beta, 1 + \beta\}$;

(ii) If $t = 2$, then f is a non-decomposable PBF if and only if $r = 1$ and there exists a B-type TS $R = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$ such that $\mathrm{Supp}(f) = \{\beta_1, \beta_2, 1 + \beta_1, 1 + \beta_2\}$, where $\beta_1, \beta_2 \in T_2$;

(iii) If $t \ge 3$, then either $r = t$ or $r = t - 1$. Furthermore,

  (a) If $r = t$, then f is a non-decomposable PBF if and only if there exist A-type TSs $R_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$, $R_i = \{1 + \beta_{i-1}, \beta_{i+1}, 1 + \beta_{i-1} + \beta_{i+1}\}$, $2 \le i \le t - 1$, and $R_t = \{1 + \beta_{t-1}, 1 + \beta_t, \beta_{t-1} + \beta_t\}$ such that $R_1, \cdots, R_{t-1}$ and R_t form a circle of TSs, and $\mathrm{Supp}(f) = \{\beta_i, 1 + \beta_i | 1 \le i \le t\}$.

  (b) If $r = t - 1$, then f is a non-decomposable PBF if and only if there exist TSs $R_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$, $R_2 = \{1 + \beta_1, \beta_3, 1 + \beta_1 + \beta_3\}$, and $R_i = \{1 + \beta_i, \beta_{i+1}, 1 + \beta_i + \beta_{i+1}\}$, $3 \le i \le r$ such that R_1, R_r are B-type TSs and $R_2, \cdots, R_{r-1}$ are A-type TSs, and $\mathrm{Supp}(f) = \{\beta_i, 1 + \beta_i | 1 \le i \le t\}$.

Proof: (i) Let $t = 1$ and assume $\mathrm{Supp}(f) = \{\beta, 1 + \beta\}$. Then $\mathrm{Supp}(f) \cap S = \emptyset$. Otherwise, there exists a TS R such that $\mathrm{Supp}(f) \subseteq R$. Then it follows that $1 = \beta + (1 + \beta) \in R$, which is a contradiction as

$1 \notin S$. Hence $\beta \in T_1$ and $r = 0$. Conversely, for any $\beta \in T_1$, let g be a vector with $\mathrm{Supp}(g) = \{\beta, 1+\beta\}$. Then clearly g is a non-decomposable PBF by Theorem 2.7.

(ii) First note that, if $t \geq 2$ and f is non-decomposable, we may see from (i) that $\beta_i \notin T_1$ holds for any $1 \leq i \leq t$ (as otherwise assume $\beta_i \in T_1$, then f can be decomposed into the sum of two PBFs, one with support set $\mathrm{Supp}(f) \setminus \{\beta_i, \beta_i+1\}$ and one with support set $\{\beta_i, \beta_i+1\}$). In other words, for any $1 \leq i \leq t$, either $\beta_i \in T_2$ or $\beta_i \in T_3$. Then $\{\beta_i, 1+\beta_i\} \cap S \neq \emptyset$ for any $1 \leq i \leq t$. Hence $r \geq \lceil \frac{t}{2} \rceil \geq 1$.

Now, let $t = 2$. Assume that f is a non-decomposable PBF with support set $\{\beta_1, \beta_1+1, \beta_2, \beta_2+1\}$. Let R_1 be a TS such that $|\mathrm{Supp}(f) \cap R_1| = 2$. Clearly, for any $i = 1, 2$, at most one of β_i and $1+\beta_i$ is in R_1. WLOG, we assume that $\beta_1, \beta_2 \in R_1$. Hence $R_1 = \{\beta_1, \beta_2, \beta_1+\beta_2\}$. Now we claim that $\beta_1 \in T_2$. Otherwise, we have $\beta_1 \in T_3$, which means that $1+\beta_1 \in S \cap \mathrm{Supp}(f)$. Since $1+\beta_1 \notin R_1$, let R_2 be the TS such that $1+\beta_1 \in R_2$. Then $|R_2 \cap \mathrm{Supp}(f)| = 2$, which deduces that $1+\beta_2 \in R_2$. Hence $(1+\beta_1) + (1+\beta_2) = \beta_1 + \beta_2 \in R_2$, which contradicts the fact that different TSs are disjoint. Thus $\beta_1 \in T_2$. Similarly, we can show that $\beta_2 \in T_2$. Therefore, $R_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$ is a B-type TS and $\mathrm{Supp}(f) = \{\beta_1, \beta_1+1, \beta_2, \beta_2+1\}$, which implies that $r = 1$.

Conversely, let $R = \{a, b, a+b\}$ be a B-type TS and $a, b \in T_2$. Then the vector v_g satisfying $\mathrm{Supp}(v_g) = \{a, b, 1+a, 1+b\}$ is a non-decomposable PBF.

(iii) From now on, we assume that $t \geq 3$. Then $r \geq \lceil \frac{t}{2} \rceil \geq 2$ if f is non-decomposable. First assume that f is non-decomposable, we distinguish the following two cases:

(a) All TSs R_i with $R_i \cap \mathrm{Supp}(f) \neq \emptyset$ are A-type TSs. By the notations at the beginning of this section, we assume that there are r such TSs, where $2 \leq r \leq t$;

(b) There exists at least one B-type TS R_i among those $R_i \cap \mathrm{Supp}(f) \neq \emptyset$. Further, for any B-type TS $R_i = \{a_i, b_i, a_i + b_i\}$, $a_i, b_i \in \mathrm{Supp}(f)$, we have $a_i \notin T_2$ or $b_i \notin T_2$, or equivalently, $a_i \in T_3$ or $b_i \in T_3$. Otherwise, if $a_i, b_i \in T_2$, we may decompose f into the sum of f_1 and f_2, where f_1, f_2 are PBFs, one with support set $\mathrm{Supp}(f) \setminus \{a_i, b_i, 1+a_i, 1+b_i\}$ and one with support set $\{a_i, b_i, a_i+1, b_i+1\}$ (by (ii) such a function is a PBF).

Case (a): Assume that $t \geq 3$ and all R_i are A-type TSs for $1 \leq i \leq r$. Assume that $R_1 = \{\beta_1, \beta_2, \beta_1+\beta_2\}$. Since R_1 is A-type, we have $1+\beta_1, 1+\beta_2 \in S \cap \mathrm{Supp}(f)$. Clearly, $1+\beta_1$ and $1+\beta_2$ can not be in one TS. Assume that $1+\beta_1 \in R_2$ and $1+\beta_2 \in R_3$. Denote by β_3 the other element in $R_2 \cap \mathrm{Supp}(f)$. Then $R_2 = \{1+\beta_1, \beta_3, 1+\beta_1+\beta_3\}$. Similarly, we have $1+\beta_3 \in S \cap \mathrm{Supp}(f)$ since R_2 is A-type.

If $t = 3$, then $r \leq 3$. Hence $R_3 = \{1+\beta_2, 1+\beta_3, \beta_2+\beta_3\}$. Then $\mathrm{Supp}(f) = \{\beta_i, 1+\beta_i, 1 \leq i \leq 3\}$ is a non-decomposable PBF. If $t > 3$, then $1+\beta_3 \notin R_3$ since f is non-decomposable. WLOG, assume that $1+\beta_3 \in R_4$ and $\beta_4 \in R_3$. So on and so forth, since f is non-decomposable, we have $r = t$ and $R_1 = \{\beta_1, \beta_2, \beta_1+\beta_2\}$, $R_i = \{1+\beta_{i-1}, \beta_{i+1}, 1+\beta_{i-1}+\beta_{i+1}\}$, $2 \leq i \leq t-1$, $R_t = \{1+\beta_{t-1}, 1+\beta_t, \beta_{t-1}+\beta_t\}$. Then $R_1, \cdots, R_t$ forms a circle of A-type TSs with length t.

Case (b): Assume that $t \geq 3$ and there exists $1 \leq i \leq r$ such that R_i is a B-type TS. WLOG, we assume that $R_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$ is a B-type TS. Then $\beta_1 \in T_3$ or $\beta_2 \in T_3$. WLOG, we assume that $\beta_1 \in T_3$ and $\beta_2, \beta_1 + \beta_2 \in T_2$ (Note that there is one and only one element of an B-type TS in T_3). It follows that $1 + \beta_1 \in S \cap \mathrm{Supp}(f)$ and $1 + \beta_2 \notin S$. WLOG, assume that $1 + \beta_1 \in R_2$ and $\beta_3 \in R_2$. Then $R_2 = \{1 + \beta_1, \beta_3, 1 + \beta_1 + \beta_3\}$.

If R_2 is B-type, then $\beta_3 \in T_2$ and $1 + \beta_3 \notin S$. Hence the vector v such that $\mathrm{Supp}(v) = \{\beta_i, 1 + \beta_i | 1 \leq i \leq 3\}$ is a PBF. Since V_f is non-decomposable, this can only happen when $t = 3$. And in this case, we have $r = 2 = t - 1$.

If R_2 is A-type, then $\beta_3 \in T_3$ and $1 + \beta_3 \in S \cap \mathrm{Supp}(f)$. Similarly, we can assume that $1 + \beta_3 \in R_3$ and $\beta_4 \in R_3$. Hence $R_3 = \{1 + \beta_3, \beta_4, 1 + \beta_3 + \beta_4\}$. Similarly as just discussed, if R_3 is B-type, then $t = 4$, $r = 3 = t - 1$, and $\mathrm{Supp}(f) = \{\beta_i, 1 + \beta_i | 1 \leq i \leq 4\}$ is a non-decomposable PBF. If R_3 is A-type, then we can assume that $R_4 = \{1 + \beta_4, \beta_5, 1 + \beta_4 + \beta_5\}$. So on and so forth, since f is non-decomposable, we have $r = t - 1$. Further, $R_1 = \{\beta_1, \beta_2, \beta_1 + \beta_2\}$, $R_2 = \{1 + \beta_1, \beta_3, 1 + \beta_1 + \beta_3\}$, and $R_i = \{1 + \beta_i, \beta_{i+1}, 1 + \beta_i + \beta_{i+1}\}$, $3 \leq i \leq r$, where R_1, R_r are B-type TSs and $R_2, \cdots, R_{r-1}$ are A-type TSs.

The proof of the converse part is not difficult and we omit it here. We complete the proof. ■

The following proposition follows directly from Theorem 3.2.

Proposition 3.3: Let $n = 2k$ be an even integer and $\mathcal{G}$ be the graph defined in Definition 2.16. Then the following results hold:

(i) The number of type (i) non-decomposable PBFs in Theorem 3.2 is half of the cardinality of T_1;

(ii) The number of type (ii) non-decomposable PBFs is the number of the B-type TSs;

(iii) A type (iii)(a) non-decomposable PBF with weight $2t$ exists if and only if there exists a cycle in $\mathcal{A}$ of length t, where $\mathcal{A}$ is the subgraph of $\mathcal{G}$ generated by all A-type vertices;

(iv) A type (iii)(b) non-decomposable PBF with weight $2t$ exists if and only if there exists a path of $\mathcal{G}$ with length t, where the starting and ending vertices are B-type vertices, and the others are A-type.

Computer experiments on small fields suggest that there exist many non-decomposable PBFs of the type (iii)(b) and much few those of the type (iii)(a). In the following, we give some experiment results about the non-decomposable PBFs of the type (iii)(a). Note that the minimal value of t such that a type (iii)(a) non-decomposable PBF exists is the girth of the subgraph of $\mathcal{G}$ generated by all A-type TSs. Also, the maximal value of such t is $2d + 1$, where d is the maximal diameter of all connected components of this subgraph. We use the following table to list the properties of the subgraph of $\mathcal{G}$ generated by the A-type TSs. The notations are the same as Table III.

TABLE IV

COMPUTATIONAL RESULTS OF THE SUBGRAPH OF $\mathcal{G}$ GENERATED BY THE A-TYPE TSS ON $\mathbb{F}_{2^n}$ FOR $6 \leq n \leq 12$ WITH n EVEN

n	# of vertices	# of edges	Girth	# of connected components	Diameter
6	1	0	no cycle	1	0
8	14	13	8	2	4
10	35	15	5	21	2
12	176	138	9	43	18

Finally, we apply Theorem 3.2 to explicitly construct a large set of PBFs, and hence obtain many differentially 4-uniform permutations.

We first introduce some notations. For any $\beta \in T_1$, define a function f_β as

$$f_\beta(x) = (x+\beta)^{2^n-1} + (x+\beta+1)^{2^n-1}.$$

Let $R = \{a_1, a_2, a_1 + a_2\}$ be a B-type TS, where $a_1, a_2 \in T_2$. Define the function f_R as

$$f_R(x) = \sum_{i=1}^{2} \left((x+a_i)^{2^n-1} + (x+a_i+1)^{2^n-1} \right).$$

Theorem 3.4: Let $\mathcal{U}$ be the set of non-decomposable PBFs with weight 2 or 4. Then

$$\mathcal{U} = \{f_\beta, f_R | \beta \in T_1, R \text{ is a B-type TS}\}$$

and $|\mathcal{U}| = \frac{|T_1|}{2} + |\{R | R \text{ is a B-type TS}\}|$, where f_β, f_R are as defined above. Define the matrix U with each row the value vector of a Boolean function in $\mathcal{U}$. Then the rank of U is $|\mathcal{U}|$. Therefore, the rows of U generate a subspace of $\mathcal{PBF}$ with dimension $|\mathcal{U}|$. Denote this subspace by $\mathcal{PBF}_4$. By Theorem 2.6, for each $f \in \mathcal{PBF}_4$, we can construct a differentially 4-uniform permutation on $\mathbb{F}_{2^n}$. Therefore we explicitly obtain $2^{|\mathcal{U}|}$ such functions.

Proof: The proof is simple and we omit it here. ■

We use the following table to list $\dim(\mathcal{PBF}_4)$, the dimension of the subspace of differentially 4-uniform permutations obtained in Theorem 3.4 for $6 \le n \le 14$. It seems that $\dim(\mathcal{PBF}_4) = |\mathcal{U}| = 2^{n-2}$. This hints that the dimension of $\mathcal{PBF}_4$ is about $\frac{3}{4}$ of that of the whole space $\mathcal{PBF}$.

TABLE V

DIMENSION OF THE DIFFERENTIALLY 4-UNIFORM PERMUTATIONS ON $\mathbb{F}_{2^n}$ OBTAINED IN THOEREM 3.4, $6 \le n \le 14$ AND n EVEN

n	$\dim(\mathcal{PBF}_4)$ (Thm 3.4)	$\dim(\mathcal{PBF})$
6	16	22
8	64	86
10	256	342
12	1024	1366
14	4096	5462

IV. Conclusions

In this paper we propose a particular type of Boolean functions, preferred Boolean functions, to characterize the preferred functions. This enables us to give a more efficient method to construct new differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. Furthermore, it is proven that such Boolean functions can be determined by solving linear equations. Hence the number of them can be determined by computing the rank of the coefficient matrix. As an application, we show that the number of CCZ-inequivalent differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ (n even) is at least $2^{\frac{2^n+2}{3}-4n^2-2n}$, which implies the number of the CCZ-inequivalent classes of such permutations grow exponentially when n grows. This positively answer an open problem proposed in [14]. Finally, we study the non-decomposable preferred Boolean functions, and use them to construct more differentially 4-uniform permutations explicitly. The obtained functions in this paper may provide more choices for the design of Substitution boxes.

V. Acknowledgement

Part of this work was done when the first author visited Hong Kong University of Science and Technology. He would like to thank Prof. Cunsheng Ding for the kind hospitality and discussions during this period.

References

[1] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 4(1): 3-72, (1991).

[2] C. Bracken and G. Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications, 16(4):231-242, 2010.

[3] C. Bracken, C.H. Tan and Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity, Finite Fields and Their Applications 18 (3), 537–546, (2012).

[4] C. Carlet, Vectorial Boolean Functions for Cryptography, www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf.

[5] C. Carlet, P. Charpin, V. Zinoviev, Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems, Des. Codes Cryptography 15(2): 125-156 (1998)

[6] C. Carlet, On known and new differentially uniform functions, Lecture Notes in Computer Science, Vol. 6812, ACISP 2011, 1-15, (2011).

[7] C. Carlet, More constructions of APN and differentially 4-uniform functions by concatenation, Science China Mathematics, 56(7), 1373-1384, (2013).

[8] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematical Communications 3(1), 59-81, (2009).

[9] L. Knudsen, Truncated and higher order differentials, Lecture Notes in Computer Science, Vol 1008, FSE 1994, 196-211, (1995).

[10] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications 20, (1997).

[11] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Transactions on Information Theory, 36(3), 686-692, (1990).

[12] M. Matsui, Linear cryptanalysis method for DES cipher, Lecture Notes in Computer Science, Vol 765, EUROCRYPT 93, 55-64, (1994).

[13] Y. Li and M. Wang, Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$ from quadratic APN permutations over $\mathbb{F}_{2^{2m+1}}$, Des. Codes Cryptogr., DOI 10.1007/s10623-012-9760-9.

[14] L. 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 Inform. Theory, 59(7), 4675-4686, (2013).

[15] L. Qu, H. Xiong and C. Li, A negative answer to Bracken-Tan-Tan's problem on differentially 4-uniform permutations over $\mathbb{F}_{2^n}$, Finite Fields and Their Applications, Vol. 24, 55-65, (2013).

[16] G. Weng, Y. Tan and G. Gong, On Quadratic APN functions and their related algebraic objects, *Proceedings of International Workshop on Coding and Cryptography*, 48–57, (2013).

[17] Y. Yu, M. Wang and Y. Li, A matrix approach for constructing quadratic APN functions, *Proceedings of International Workshop on Coding and Cryptography*, 39–47, (2013).