An Equivalent Condition on the Switching Construction of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$ from the Inverse Function

Xi Chen, Yazhi Deng, Min Zhu and Longjiang Qu**

Abstract

Differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with high nonlinearity are often chosen as Substitution boxes in block ciphers. Recently, Qu et al. used the powerful switching method to construct such permutations from the inverse function [9], [10]. More precisely, they studied the functions of the form $G(x) = \frac{1}{x} + f(\frac{1}{x})$, where f is a Boolean function. They proved that if f is a preferred Boolean function (PBF), then G is a permutation polynomial over $\mathbb{F}_{2^n}$ whose differential uniformity is at most 4. However, as pointed out in [9], f is a PBF is a sufficient but not necessary condition. In this paper, a sufficient and necessary condition for G to be a differentially 4-uniform permutation is presented. We also show that G can not be an almost perfect nonlinear (APN) function. As an application, a new class of differentially 4-uniform permutations where f are not PBFs are constructed. By comparing this family with previous constructions, the number of permutations here is much bigger. The obtained functions in this paper may provide more choices for the design of Substitution boxes.

Index Terms

Differentially 4-uniform function, Substitution box, 4-Uniform BFI, Preferred Boolean function, Permutation function

I. Introduction

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

X. Chen, Y. Deng and L. Qu are with the College of Science, National University of Defense Technology, ChangSha, 410073, China. M. Zhu is with the College of Computer Science, National University of Defense Technology, ChangSha, 410073, China. E-mail: chenxi_1138470214@qq.com, yzdeng_260849586@qq.com, zhumin_zm@nudt.edu.cn, ljqu_happy@hotmail.com. This work is supported in part 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.

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. On this aspect, they are the most ideal choices for the design of Substitution boxes. However, it is very difficult to find APN permutations over $\mathbb{F}_{2^{2k}}$, which is called *BIG APN* Problem. Due to the lack of knowledge on APN permutations on $\mathbb{F}_{2^{2k}}$, a natural trade-off solution is to use differentially 4-uniform permutations as S-boxes. Recently, many constructions of differentially 4-uniform permutations were introduced [1]–[3], [5], [9]–[14]. In 2013, Qu et al. used the powerful switching method [6] to successfully construct many infinite families of such permutations from the inverse function [9], [10]. In the constructions, they introduced a type of functions [9], which they called preferred Boolean functions. More precisely, they studied the functions with the form $G(x) = \frac{1}{x} + f(\frac{1}{x})$, where f is a Boolean function. They proved that if f is a *preferred Boolean function* (PBF), then G is a permutation polynomial over $\mathbb{F}_{2^n}$ whose differential uniformity is at most 4. However, as pointed out in [10], f is a PBF is only a sufficient but not necessary condition.

In this paper, a generalization of PBF which is called 4-*uniform Boolean function with respect to the inverse function* (4-Uniform BFI for short) is presented. Then we find a sufficient and necessary condition for $G(x) = \frac{1}{x} + f(\frac{1}{x})$ to be a differentially 4-uniform permutation. We also show that G can not be an APN function. As an application, a new class of differentially 4-uniform permutations where f are not PBFs are constructed, the number of which is far more than before. Furthermore, we construct a new infinite family of differentially 4-uniform permutations where f is not a PBF but a 4-Uniform BFI. The number of permutations in this family is quite large. These functions may provide more choices for the design of Substitution boxes.

II. Necessary definitions and useful lemmas

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

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 always define $0^{-1} = 0$ below.

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 $\mathbb{F}_{2^n}$. Denote by $\mathbb{F}_{2^n}^*$ the set of all nonzero elements of $\mathbb{F}_{2^n}$. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, define

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

Note that we denote the cardinality of S by $\sharp S$. 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

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

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

The following results are useful in our future discussion.

Result 2.1: [4] Let n be an even integer and f be an n-variable Boolean function. Then $x + f(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$.

Result 2.2: [8] For any $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$, the polynomial $f(x) = x^2 + ax + b \in \mathbb{F}_{2^n}[x]$ is irreducible if and only if $\mathrm{Tr}(\frac{b}{a^2}) = 1$.

Result 2.3: [7, Lemma 4.1] Let $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$. Then $\mathrm{Tr}(\frac{1}{b}) = 0$ if and only if there exists $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $b = \alpha + \alpha^{-1}$.

III. Main Results

In this section, we give the definition of 4-Uniform BFI and an equivalent condition on the switching construction of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ from the inverse function. As an application, we present a new class of differentially 4-uniform permutations which can not be constructed from PBFs. The number of them is far more than those in [9], [10].

A. Definition of 4-Uniform BFI

In [9] the authors introduced a type of functions called preferred Boolean functions, and then constructed many infinite families of permutations whose differential uniformity are at most 4 of the form $G(x) = \frac{1}{x} + f(\frac{1}{x})$.

Theorem 3.1: [9] 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 PBF if and only if it satisfies the following two conditions: (1) $f(x+1) = f(x)$ for any $x \in \mathbb{F}_{2^n}$;
(2) $f(0) + f(\alpha + \frac{1}{\alpha}) + f(\omega\alpha + \frac{1}{\omega\alpha}) + f(\omega^2\alpha + \frac{1}{\omega^2\alpha}) = 0$ for any $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$.

Theorem 3.2: [9] 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

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

If $f(x)$ is a PBF, then $G(x)$ is a permutation polynomial on $\mathbb{F}_{2^n}$ whose differentially uniformity is at most 4.

This theorem builds a bridge from PBFs to permutation polynomials with differentially uniformity at most 4. However, as pointed out in [10], f is a PBF is only a sufficient but not necessary condition. Then a natural question is to search for an equivalent condition. For convenience, we introduce the following definition.

Definition 3.3: Let $n = 2k$ be an even integer and f be an n-variable Boolean function. We call f a *4-uniform Boolean function with respect to the inverse function* (4-uniform BFI for short) when $G(x) = \frac{1}{x} + f(\frac{1}{x})$ is a permutation whose differential uniformity is at most 4.

Then a PBF is a 4-uniform BFI and not vice versa.

B. An Equivalent Condition

Now we introduce the main theorem of this paper. It is an equivalent condition on the switching construction of differentially 4-uniform permutation on $\mathbb{F}_{2^{2k}}$ from the inverse function.

Theorem 3.4: 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 any $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, at least one of the following two equations holds.

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

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

Proof: It follows from Result 2.1 that $G(x)$ is a permutation if and only if $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$. Then we only need to compute the differential uniformity of G.

Sufficiency: Assume that the differential uniformity of $G(x) = \frac{1}{x} + f(\frac{1}{x})$ is more than 4. Then there exists $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$ such that

$$G(x + a) + G(x) = b \tag{3}$$

has more than 4 solutions in $\mathbb{F}_{2^n}$. Since f is a Boolean function, we have

$$\begin{cases} \frac{1}{x} + \frac{1}{x+a} = b \\ f(\frac{1}{x}) + f(\frac{1}{x+a}) = 0, \end{cases} \tag{4}$$

or

$$\begin{cases} \frac{1}{x} + \frac{1}{x+a} = b + 1 \\ f(\frac{1}{x}) + f(\frac{1}{x+a}) = 1. \end{cases} \tag{5}$$

It is clear that Eq. (4) and Eq. (5) have no common solutions and each of them has at most 2 solutions in $\mathbb{F}_{2^n} \setminus \{0, a\}$. Hence 0 is a solution of Eq. (4) or Eq. (5) and each of them has exactly 2 solutions in $\mathbb{F}_{2^n} \setminus \{0, a\}$. The following proof is divided into two cases.

Case 1. 0 is a solution of Eq. (4)

In this case, we have $ab = 1$ and

$$f(0) + f(\frac{1}{a}) = 0. \tag{6}$$

Substituting $ab = 1$ into Eq. (4) and Eq. (5), we get

$$\begin{cases} \frac{1}{x} + \frac{1}{x+a} = \frac{1}{a} \\ f(\frac{1}{x}) + f(\frac{1}{x} + \frac{1}{a}) = 0, \end{cases} \tag{7}$$

or

$$\begin{cases} \frac{1}{x} + \frac{1}{x+a} = \frac{1}{a} + 1 \\ f(\frac{1}{x}) + f(\frac{1}{x} + \frac{1}{a} + 1) = 1. \end{cases} \tag{8}$$

If $x \neq 0$ or a, then Eq. (7.1) is equivalent to $x^2 + ax + a^2 = 0$, which always has 2 solutions $x = \frac{a}{\omega}$ and $x = \frac{a}{\omega^2}$.

Now we consider Eq. (8.1). It is clear that 0 and a are not the solutions of Eq. (8.1) and $a \neq 1$. Hence Eq. (8.1) is equivalent to

$$x^2 + ax + \frac{a^2}{1+a} = 0 \tag{9}$$

It follows from Result 2.2 that Eq. (9) has a solution in $\mathbb{F}_{2^n}$ if and only if $0 = \mathrm{Tr}(\frac{1}{a+1}) = \mathrm{Tr}(\frac{a}{a+1}) = \mathrm{Tr}(\frac{1}{1+\frac{1}{a}})$, where the last second equality holds since n is an even integer. It follows from $a \neq 0, 1$ that $1 + \frac{1}{a} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$. Then according to Result 2.3, $\mathrm{Tr}(\frac{1}{1+\frac{1}{a}}) = 0$ if and only if there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $\frac{1}{a} + 1 = z + \frac{1}{z}$. Hence Eq. (8.1) has a solution in $\mathbb{F}_{2^n}$ if and only if there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $a = \frac{1}{z+\frac{1}{z}+1}$.

Let $x_1 = \frac{1}{\omega z + \frac{1}{\omega z} + 1}$. Then

$$\begin{aligned} \frac{1}{x_1 + a} &= \frac{1}{\frac{1}{\omega z + \frac{1}{\omega z} + 1} + \frac{1}{z + \frac{1}{z} + 1}} = \frac{(\omega z + \frac{1}{\omega z} + 1)(z + \frac{1}{z} + 1)}{\omega^2 z + \frac{1}{\omega^2 z}} \\ &= \frac{\omega z^2 + \frac{1}{\omega z^2}}{\omega^2 z + \frac{1}{\omega^2 z}} + 1 = \omega^2 z + \frac{1}{\omega^2 z} + 1. \end{aligned}$$

Hence

$$\frac{1}{x_1} + \frac{1}{x_1 + a} = (\omega z + \frac{1}{\omega z} + 1) + (\omega^2 z + \frac{1}{\omega^2 z} + 1) = z + \frac{1}{z} = \frac{1}{a} + 1,$$

which means that $x_1 = \frac{1}{\omega z + \frac{1}{\omega z} + 1}$ is a solution of Eq. (8.1). Clearly, $x_2 = x_1 + a = \frac{1}{\omega^2 z + \frac{1}{\omega^2 z} + 1}$ is the other solution of Eq. (8.1).

Substituting $a = \frac{1}{z+\frac{1}{z}+1}$ into Eq. (6), Eq. (7.2) and Eq. (8.2), one get the following equation system.

$$\begin{cases} f(0) + f(z + \frac{1}{z} + 1) &= 0, \\ f(\omega(z + \frac{1}{z} + 1)) + f(\omega^2(z + \frac{1}{z} + 1)) &= 0, \\ f(\omega z + \frac{1}{\omega z} + 1) + f(\omega^2 z + \frac{1}{\omega^2 z} + 1) &= 1. \end{cases} \tag{10}$$

Hence there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that neither Eq. (1) nor Eq. (2) holds, a contradiction.

Case 2. 0 is a solution of Eq. (5)

Similarly as Case 1, we have $a(b+1)=1$ and there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $a = \frac{1}{z+\frac{1}{z}+1}$. Then we get

$$\begin{cases} f(0)+f(z+\frac{1}{z}+1) &= 1, \\ f(\omega(z+\frac{1}{z}+1))+f(\omega^2(z+\frac{1}{z}+1)) &= 1, \\ f(\omega z+\frac{1}{\omega z}+1)+f(\omega^2 z+\frac{1}{\omega^2 z}+1) &= 0. \end{cases} \tag{11}$$

Thus there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that neither Eq. (1) nor Eq. (2) is hold, a contradiction.

Hence the differential uniformity of G is at most 4.

Now we prove that G can not be an APN function. Assume $G(x)=\frac{1}{x}+f(\frac{1}{x})$ is an APN function, then Eq. (3) has at most 2 solutions in $\mathbb{F}_{2^n}$ for any $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$.

As in the proof of Case 1, let $a = \frac{1}{z+\frac{1}{z}+1}$ and $b = z+\frac{1}{z}+1$, where z be any element of $\mathbb{F}_{2^n} \setminus \mathbb{F}_4$. Then we can verify that $x=0$, $x=a$, $x=\frac{a}{\omega}$ and $x=\frac{a}{\omega^2}$ are the solutions of Eq. (4.1), while $x=\frac{1}{\omega z+\frac{1}{\omega z}+1}$, $x=\frac{1}{\omega^2 z+\frac{1}{\omega^2 z}+1}$ are the solutions of Eq. (5.1). Since Eq. (3) has at most 2 solutions in $\mathbb{F}_{2^n}$, at most one equation of (10) holds.

Now we turn to Case 2. Let $a = \frac{1}{z+\frac{1}{z}+1}$ and $b = z+\frac{1}{z}$. Similarly, at most one equation of (11) holds.

Hence at most two of the six equations of (10) and (11) hold. On the other hand, one and only one of Eq. (10.1) and Eq. (11.1) holds since f is a Boolean function. By the same reason, exactly three of these six equations hold, contradicts.

Hence $G(x)=\frac{1}{x}+f(\frac{1}{x})$ is not an APN permutation but a differentially 4-uniform permutation.

Necessity: Assume, on the contrary, that there exists $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that neither Eq. (1) nor Eq. (2) holds. Since f is a Boolean function, we have $f(0)+f(z+\frac{1}{z}+1)=0$ or 1. Here we only prove one case. The proof for the other case is similar and is left to the interested readers.

Assume that $f(0)+f(z+\frac{1}{z}+1)=0$. Then with the assumption that neither Eq. (1) nor Eq. (2) holds, one can get the equation system Eq. (10). Let $a = \frac{1}{z+\frac{1}{z}+1}$ and $b = z+\frac{1}{z}+1$. It is clear that $ab=1$ and $a \neq 0$ since $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$.

It follows from Eq. (10.1), Eq. (10.2) and $a \neq 0$ that $x=0$, $x=a$, $x=\frac{a}{\omega}$ and $x=\frac{a}{\omega^2}$ are four different solutions of Eq. (4). Similarly as in the sufficient part of the proof, one can verify that $x=\frac{1}{\omega z+\frac{1}{\omega z}+1}$ and $x=\frac{1}{\omega^2 z+\frac{1}{\omega^2 z}+1}$ are two different solutions of Eq. (5). Obviously, Eq. (4) and Eq. (5) have no common solutions. Hence Eq. (3) has at least 6 different solutions in $\mathbb{F}_{2^n}$, a contradiction.

We finish the proof. □

We make two comments on Theorem 3.4. First, in the above proof the condition $f(x)=f(x+1)$ is not used in the computation of the differential uniformity of G. Hence if we remove this condition in the theorem, G is also a differentially 4-uniform function but may be not a permutation. This means that Theorem 3.4 can be used to construct more differentially 4-uniform functions. Second, it is proved that

$G(x)=\frac{1}{x}+f(\frac{1}{x})$ constructed by 4-Uniform BFI is not an APN function. In particular, those $G(x)$ construct by PBF can not be APN functions either.

C. A New Infinite Family of Differentially 4-Uniform Permutations

In this subsection we construct a new infinite family of differentially 4-uniform permutations with Boolean functions which are not PBFs but 4-Uniform BFIs. By comparing this family with previous constructions, the number of permutations here is much bigger. We first introduce a lemma.

Lemma 3.5: Let ω be an element of $\mathbb{F}_{2^n}$ with order 3. If $z\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4$, then

$$\frac{1}{z+\frac{1}{z}+1}+\frac{1}{\omega z+\frac{1}{\omega z}+1}+\frac{1}{\omega^2 z+\frac{1}{\omega^2 z}+1}=0.$$

Proof. It is clear that $1+\omega+\omega^2=0$ and $z+\frac{1}{z}\notin\{0,1\}$. Then

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

□

Theorem 3.6: Let n be an even integer. Let $\alpha,\beta\in\mathbb{F}_{2^n}$ satisfying

$$\alpha+\frac{1}{\alpha}+1=\beta+\frac{1}{\beta}\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4, \tag{12}$$

$\mathrm{Tr}(\frac{1}{\omega\alpha+\frac{1}{\omega\alpha}+1})=1$ and $\mathrm{Tr}(\frac{1}{\omega\beta+\frac{1}{\omega\beta}+1})=1$. Define two subsets of $\mathbb{F}_{2^n}$ as follows.

$$\begin{aligned}U:=\{&\alpha+\frac{1}{\alpha},\alpha+\frac{1}{\alpha}+1,\omega\alpha+\frac{1}{\omega\alpha},\omega\alpha+\frac{1}{\omega\alpha}+1,\omega^2\alpha+\frac{1}{\omega^2\alpha},\omega^2\alpha+\frac{1}{\omega^2\alpha}+1,\\&\omega\beta+\frac{1}{\omega\beta},\omega\beta+\frac{1}{\omega\beta}+1,\omega^2\beta+\frac{1}{\omega^2\beta},\omega^2\beta+\frac{1}{\omega^2\beta}+1.\}\\V:=\{&\omega(\omega\alpha+\frac{1}{\omega\alpha}+1),\omega^2(\omega\alpha+\frac{1}{\omega\alpha}+1),\omega(\omega^2\alpha+\frac{1}{\omega^2\alpha}+1),\omega^2(\omega^2\alpha+\frac{1}{\omega^2\alpha}+1),\\&\omega(\omega\beta+\frac{1}{\omega\beta}+1),\omega^2(\omega\beta+\frac{1}{\omega\beta}+1),\omega(\omega^2\beta+\frac{1}{\omega^2\beta}+1),\omega^2(\omega^2\beta+\frac{1}{\omega^2\beta}+1).\}\end{aligned}$$

If $U\cap V=\emptyset$, then we define

$$f(x)=\begin{cases}1, & \text{when}\quad x\in U;\\ 0, & \text{else.}\end{cases} \tag{13}$$

Then $f(x)$ is a 4-Uniform BFI but not a PBF. Hence $G(x)=\frac{1}{x}+f(\frac{1}{x})$ is a differentially 4-uniform permutation in $\mathbb{F}_{2^n}$.

Proof. It is easy to verify that the elements of U are distinct and $0\notin U$. Then $f(0)=0$. Let z be any element of $\mathbb{F}_{2^n}\setminus\mathbb{F}_4$. According to Theorem 3.4, it suffices to prove that at least one of the following two

equations holds.

$$f(0)+f(z+\tfrac{1}{z}+1)+f(\omega z+\tfrac{1}{\omega z}+1)+f(\omega^2 z+\tfrac{1}{\omega^2 z}+1)=0, \tag{14}$$

$$f(0)+f(z+\tfrac{1}{z}+1)+f(\omega(z+\tfrac{1}{z}+1))+f(\omega^2(z+\tfrac{1}{z}+1))=1. \tag{15}$$

It follows from Eq. (12) and Result 2.3 that $\mathrm{Tr}(\frac{1}{\alpha+\frac{1}{\alpha}+1})=\mathrm{Tr}(\frac{1}{\beta+\frac{1}{\beta}+1})=0$. By the assumption $\mathrm{Tr}(\frac{1}{\omega\alpha+\frac{1}{\omega\alpha}+1})=\mathrm{Tr}(\frac{1}{\omega\beta+\frac{1}{\omega\beta}+1})=1$ and Lemma 3.5, we have $\mathrm{Tr}(\frac{1}{\omega^2\alpha+\frac{1}{\omega^2\alpha}+1})=\mathrm{Tr}(\frac{1}{\omega^2\beta+\frac{1}{\omega^2\beta}+1})=1$. Then it follows from Result 2.3 that neither of $\omega\alpha+\frac{1}{\omega\alpha},\omega^2\alpha+\frac{1}{\omega^2\alpha},\omega\beta+\frac{1}{\omega\beta},\omega^2\beta+\frac{1}{\omega^2\beta}$ can equal to $z+\frac{1}{z}+1$. Hence $z+\frac{1}{z}+1\in U$ if and only if $z\in\{\alpha,\frac{1}{\alpha},\beta,\frac{1}{\beta},\omega\alpha,\frac{1}{\omega\alpha},\omega\beta,\frac{1}{\omega\beta},\omega^2\alpha,\frac{1}{\omega^2\alpha},\omega^2\beta,\frac{1}{\omega^2\beta}\}$. It is also clear that $z+\frac{1}{z}+1\in U$ if and only if $\omega z+\frac{1}{\omega z}+1,\omega^2 z+\frac{1}{\omega^2 z}+1\in U$. The rest of the proof is split into two cases according to whether $z+\frac{1}{z}+1\in U$.

Case 1. $z+\frac{1}{z}+1\notin U$

Then $f(z+\frac{1}{z}+1)=f(\omega z+\frac{1}{\omega z}+1)=f(\omega^2 z+\frac{1}{\omega^2 z}+1)=0$ since neither of $z+\frac{1}{z}+1,\omega z+\frac{1}{\omega z}+1,\omega^2 z+\frac{1}{\omega^2 z}+1$ is in U. Hence Eq. (14) holds.

Case 2. $z+\frac{1}{z}+1\in U$

Contrary to Case 1, now Eq. (14) does not hold since $z+\frac{1}{z}+1,\omega z+\frac{1}{\omega z}+1,\omega^2 z+\frac{1}{\omega^2 z}+1\in U$. Hence f is not a PBF. Now we need to prove that Eq. (15) must hold, or equivalently, to prove that

$$f(\omega(z+\frac{1}{z}+1))=f(\omega^2(z+\frac{1}{z}+1)). \tag{16}$$

We distinguish two subcases.

Subcase 2.1. $z\in\{\omega\alpha,\frac{1}{\omega\alpha},\omega\beta,\frac{1}{\omega\beta},\omega^2\alpha,\frac{1}{\omega^2\alpha},\omega^2\beta,\frac{1}{\omega^2\beta}\}$

It is clear that $\omega(z+\frac{1}{z}+1),\omega^2(z+\frac{1}{z}+1)\in V$. Then it follows from the definition of f and the assumption $U\cap V=\emptyset$ that $f(\omega(z+\frac{1}{z}+1))=f(\omega^2(z+\frac{1}{z}+1))=0$, which means Eq. (16) is hold.

Subcase 2.2. $z\in\{\alpha,\frac{1}{\alpha},\beta,\frac{1}{\beta}\}$

Let $U_1=\{\alpha+\frac{1}{\alpha}+1=\beta+\frac{1}{\beta},\alpha+\frac{1}{\alpha}=\beta+\frac{1}{\beta}+1\}$, $U_2=U\backslash U_1$. Then one can easily verify that $u_1+u_2\in U_2$ holds for any $u_1\in U_1,u_2\in U_2$. Since $z+\frac{1}{z}+1\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4$, we have $\omega^i(z+\frac{1}{z}+1)\notin U_1$, $i=1,2$. Then $\omega(z+\frac{1}{z}+1)\in U_2$ if and only if $\omega^2(z+\frac{1}{z}+1)=(z+\frac{1}{z}+1)+\omega(z+\frac{1}{z}+1)\in U_2$, which means $f(\omega(z+\frac{1}{z}+1))=1$ if and only if $f(\omega^2(z+\frac{1}{z}+1))=1$. Hence Eq. (16) holds.

We finish the proof. □

Now we estimate the number of the permutations constructed in Theorem 3.6. Roughly speaking, for a random element $\alpha\in\mathbb{F}_{2^n}$, the probability of $\mathrm{Tr}(\frac{1}{\alpha+\frac{1}{\alpha}+1})=0$ is around $1/2$. If $\mathrm{Tr}(\frac{1}{\alpha+\frac{1}{\alpha}+1})=0$, then there exists $\beta\in\mathbb{F}_{2^n}$ satisfying Eq. (12). Then there are about 2^{n-3} elements (α) in $\mathbb{F}_{2^n}$ satisfying $\mathrm{Tr}(\frac{1}{\alpha+\frac{1}{\alpha}+1})=0$, $\mathrm{Tr}(\frac{1}{\omega\alpha+\frac{1}{\omega\alpha}+1})=1$ and $\mathrm{Tr}(\frac{1}{\omega\beta+\frac{1}{\omega\beta}+1})=1$. Since there are 8 pairs $((\alpha,\beta),(\alpha,\frac{1}{\beta}),(\frac{1}{\alpha},\beta),(\frac{1}{\alpha},\frac{1}{\beta}),(\beta,\alpha),(\frac{1}{\beta},\alpha),(\beta,\frac{1}{\alpha}),(\frac{1}{\beta},\frac{1}{\alpha}))$ corresponding to the same function $f(x)$, any $f(x)$ corresponds to 4 elements (α). Then there are about 2^{n-5} functions $f(x)$ satisfying the conditions of the Theorem 3.6. We use Magma to do an exhaust search for $\mathbb{F}_{2^n}(6\le n\le 18,\ n$ even). The experiment data is listed in the following table. It provides a

positive evidence of this estimate number. We also list the number of the functions $f(x)$ satisfying all the conditions of Theorem 3.6 except $U \cap V = \emptyset$. The result hints that the restriction $U \cap V = \emptyset$ is quite weak.

TABLE I

NUMBER OF 4-UNIFORM PERMUTATIONS CONSTRUCTED BY THEOREM 3.6 FOR $6 \leq n \leq 18$ (n IS EVEN)

n	The number of $f(x)$	$f(x)$ satisfied all conditions except $U \cap V = \emptyset$	2^{n-5}
6	3	0	2
8	6	0	8
10	30	0	32
12	126	1	128
14	525	0	512
16	2076	0	2048
18	8112	0	8192

In the end of this section, we will show that the number of differentially 4-uniform functions constructed by 4-Uniform BFI is much bigger than those for previous constructions.

It is clear that f is a 4-Uniform BFI if and only if so is $f + 1$. For convenience, we assume that $f(0) = f(1) = 0$ in the rest of the paper. Hence to determine f is equivalent to determine all the images $f(x)$ for $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$. By abuse of notation, in the following, we still use f to denote the value vector of f on $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$.

By the two conditions in Theorem 3.4, clearly we may obtain many such 4-Uniform BFIs by solving linear equations as follows.

Define the following two sets:

$$\begin{aligned} L_x &= \{\{x, x+1\} : x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\}, \\ L_z &= \{\{z + \frac{1}{z} + 1, \omega z + \frac{1}{\omega z} + 1, \omega^2 z + \frac{1}{\omega^2 z} + 1\} : z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4\}. \end{aligned}$$

Clearly $|L_x| = 2^{n-1} - 1$. Note that when $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, the elements $z + \frac{1}{z} + 1, \omega z + \frac{1}{\omega z} + 1, \omega^2 z + \frac{1}{\omega^2 z} + 1$ are all distinct (since the sum of them is 1, and none of them can be 1). The six different elements $z, \omega z, \omega^2 z, \frac{1}{z}, \frac{1}{\omega z}, \frac{1}{\omega^2 z}$ leads to the same element of L_z, hence $|L_z| = \frac{2^n - 4}{3 \cdot 2} = \frac{2^{n-1} - 2}{3}$.

Let L be a subset of $\mathbb{F}_{2^n}$. Denote by v_L its characteristic function. Let $\alpha, \beta \in \mathbb{F}_{2^n}$ be a fixed pair satisfying those conditions in Theorem 3.6. Define the following sets: $L_{z_\alpha} = \{\alpha + \frac{1}{\alpha} + 1, \omega\alpha + \frac{1}{\omega\alpha} + 1, \omega^2\alpha + \frac{1}{\omega^2\alpha} + 1\}$, $L_{z_\beta} = \{\beta + \frac{1}{\beta} + 1, \omega\beta + \frac{1}{\omega\beta} + 1, \omega^2\beta + \frac{1}{\omega^2\beta} + 1\} \in L_z$. $L_{y_\alpha} = \{\alpha + \frac{1}{\alpha} + 1, \omega(\alpha + \frac{1}{\alpha} + 1), \omega^2(\alpha + \frac{1}{\alpha} + 1)\}$, $L_{y_\beta} = \{\beta + \frac{1}{\beta} + 1, \omega(\beta + \frac{1}{\beta} + 1), \omega^2(\beta + \frac{1}{\beta} + 1)\}$.

Define a matrix $M_{\alpha,\beta}$ with the size of $(|L_x|+|L_z|+2)\times(2^n-2)$ as follows:

$$M_{\alpha,\beta}=\begin{bmatrix} v_{L_x} \\ v_{L_z\backslash\{L_{z_\alpha},L_{z_\beta}\}} \\ v_{L_{z_\alpha}} \\ v_{L_{z_\beta}} \\ v_{L_{y_\alpha}} \\ v_{L_{y_\beta}} \end{bmatrix}, \tag{17}$$

where the columns and rows of $M_{\alpha,\beta}$ are indexed by the elements in $\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ and $L_x\cup L_z\cup\{L_{y_\alpha},L_{y_\beta}\}$ respectively.

Proposition 3.7: Let $\alpha,\beta,M_{\alpha,\beta}$ be defined as above and let f be an n-variable Boolean function with $f(0)=f(1)=0$. If f satisfies the equation

$$M_{\alpha,\beta}f^{\mathrm{T}}=\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \tag{18}$$

then f is not a PBF but a 4-Uniform BFI. Further, the number of the Boolean functions satisfying (18) is at least $2^{\frac{2^n-4}{3}}$.

Proof. The first result follows directly from Theorem 3.4 and the proof of Theorem 3.6.

Since α,β are, by assumption, satisfying those conditions in Theorem 3.6, the linear equation system (18) has at least one solution. Therefore the dimension of the set of 4-Uniform BFIs constructed above with $f(0)=0$ is $2^n-2-\mathrm{rank}(M_{\alpha,\beta})$. It is clear that $f+1$ is also a 4-Uniform BFI if f is a 4-Uniform BFI. Hence altogether the dimension of 4-Uniform BFIs constructed above with α,β is $2^n-2-\mathrm{rank}(M_{\alpha,\beta})+1=2^n-1-\mathrm{rank}(M_{\alpha,\beta})$. However,

$$\mathrm{rank}(M_{\alpha,\beta})\le\min\{|L_x|+|L_z|+2,2^n-2\}=\min\{\frac{2^{n+1}-5}{3}+2,2^n-2\}=\frac{2^{n+1}+1}{3}.$$

Hence, the dimension of 4-Uniform BFI, which is one plus the dimension of the null space of $M_{\alpha,\beta}$, is at least $2^n-2-\frac{2^{n+1}+1}{3}+1=\frac{2^n-4}{3}$. □

It is clear that L_{z_α} is different from L_{z_β} when $\alpha\neq\beta$. Thus we have about 2^{n-5} different linear equation systems. Clearly, the solution sets for different linear equation systems are pairwise disjoint. Hence, the number of 4-Uniform BFIs is at least $2^{n-5}\times 2^{\frac{2^n-4}{3}}$ (we can get an exactly lower bound from Table I) and none of them is a PBF. Then we find when n tends to infinity, the number of differentially 4-uniform permutation constructed by 4-Uniform BFI is far more than those in [9] (about $2^{\frac{2^n+2}{3}}$). These functions may

provide more choices for the design of Substitution boxes.

IV. Concluding Remarks

In this paper, an equivalent condition for the switching construction of differentially 4-uniform permutations from the inverse function is presented. It is proved that any constructed function can not be an APN function. A new infinite family differentially 4-uniform permutations is also constructed. The newly obtained functions may provide more choices for the design of Substitution boxes. For further research, it is interesting to find subclasses of the functions constructed by Theorem 3.4 with other good cryptographic properties such as high nonlinearity. A more important challenge is the *BIG APN* Problem.

References

[1] 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.

[2] 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).

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

[4] P. Charpin and G. M. Kyureghyan, On a class of permutation polynomials over F_{2^n}, Lecture Notes in Computer Science, Vol 5203, SETA 2008, 368–376, (2008).

[5] C.Carlet, More constructions of APN and differentially 4-uniform functions by concatenation, Science China, Vol.56 No.7,1373-1384,(2013).

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

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

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

[9] L.J. Qu, Y. Tan, C. Li and G. Gong, More Constructions of Differentially 4-uniform Permutations on $F_{2^{2k}}$, Design, Codes and Cryptology, to appear, also avaiable at http://arxiv.org/abs/1309.7423.

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

[11] Y.Q.Li, M.S.Wang a 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.

[12] D.Tang, C.Carlet and X.H.Tang, Differentially 4-Uniform Bijections by Permuting the Inverse Function, https://eprint.iacr.org/2013/639.pdf.

[13] Y.Y.Yu, M.S.Wang and Y.Q.Li, Constructing differential 4-uniform permutations from know ones. Chinese Journal of Electronics, 22(3), 495-499, (2013).

[14] Z. Zha, L. Hu and S. Sun, Constructing new differential 4-uniform permutations from the inverse function. Finite Fields Appl, 2014, 25: 64-78.