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 permutations with low differential uniformity from the inverse function [10], [11] and proposed a sufficient but not necessary condition for these permutations to be differentially 4-uniform. In this paper, a sufficient and necessary condition is presented. We also give a compact estimation for the number of constructed differentially 4-uniform permutations. Comparing with those constructions in [10], [11], the number of functions constructed here is much bigger. As an application, a new class of differentially 4-uniform permutations is constructed. The obtained functions in this paper may provide more choices for the design of substitution boxes.

Index Terms

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

I. Introduction

In the design of many block ciphers, permutations with specific properties are chosen as *substitution box* (S-box) 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.

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. For example, the *Advanced Encryption Standard* (AES) uses the multiplicative inverse function, which is a differentially 4-uniform permutation with known maximal nonlinearity. Hence to provide more choices for the S-boxes, it is important to construct more infinite families of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ with other good cryptographic properties.

Recently, many constructions of differentially 4-uniform permutations were introduced [2]–[4], [6], [10]–[15]. In 2013, Qu et al. used the powerful switching method [7] to construct many infinite families of

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: 1138470214@qq.com, 260849586@qq.com, 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.

such permutations from the inverse function [10], [11]. In the constructions, they introduced a type of function called *preferred Boolean function* (PBF). 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 PBF, then G is a permutation polynomial over $\mathbb{F}_{2^n}$ whose differential uniformity is at most 4. The number n-variable of PBFs is at least $2^{\frac{2^n+2}{3}}$ [11]. However, as pointed out in [11], f to be a PBF is only a sufficient but not necessary condition for f to be a differentially 4-uniform permutation. Thus it is interesting to find an equivalent condition. To decide the number of the functions in this class is another interesting problem.

The rest of this paper is organized as follows. We introduce some necessary definitions and useful lemmas in Section II . In Section III, 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. As an application, a new class of differentially 4-uniform permutations where f are not PBFs is constructed. In Section IV, we give a compact estimation to the number of 4-Uniform BFIs. The estimation indicates that the number of differentially 4-uniform permutations constructed by our equivalent condition is much bigger than those constructed by PBFs. These constructed 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 lemmas which will be used in the paper.

Let $\mathbb{F}_{2^n}$ be a finite field with 2^n elements. It can be regarded as a vector space of dimension n over $\mathbb{F}_2$, and can then be identified with $\mathbb{F}_2^n$. In the following, we will switch between these two points of view without explanation if the context is clear. Let $\omega = \alpha^{\frac{2^n-1}{3}}$ when n is an even integer, where α is a primitive element of $\mathbb{F}_{2^n}$. Then ω is an element of $\mathbb{F}_{2^4} \setminus \mathbb{F}_2$.

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. We denote by $\mathbb{B}_n$ the set of Boolean functions of n variables. The basic representation of any Boolean function $f \in \mathbb{B}_n$ is by its truth table, i.e.,

$$f = [f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{2^n-2}), f(0)].$$

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 $\mathbb{F}_{2^n}$.

Let $\xi = (\xi(1), \cdots, \xi(m))^{\mathrm{T}}$ be a column vector in $\mathbb{F}_2^m$ and $\xi(i)$ be the i-th element of ξ. The Hamming weight of ξ, denoted by $wt(\xi)$, is the size of the support of ξ, where the support of ξ is defined as $\mathrm{Supp}(\xi) = \{1 \le i \le m | \xi(i) = 1\}$. Let $\vec{0}$ be the vector whose all m elements are 0 and $\vec{1}$ be the vector with m same elements 1. Define $e_l \in \mathbb{F}_2^m$ to be the vector whose l-th element is 1 and others are all 0. Suppose that $\xi = (\xi(1), \cdots, \xi(m))^{\mathrm{T}}, \eta = (\eta(1), \cdots, \eta(m))^{\mathrm{T}}$ are two column vectors in $\mathbb{F}_2^m$, define $\xi \preceq \eta$ if and only if $\xi(i) \le \eta(i)$ for any $1 \le i \le m$.

We define the expected value of a random variable X as $\mathbb{E}(X)$. We use $|S|$ to indicate the number of the elements in a set S. Define the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$. Denote by $\mathbb{F}_{2^n}^*$ the set of all nonzero elements of $\mathbb{F}_{2^n}$. Note that for the multiplicative inverse function x^{-1}, we always define $0^{-1} = 0$ in this paper.

For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, define

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

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 lemmas are useful in our further discussion.

Lemma 2.1: [5] 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 $x \in \mathbb{F}_{2^n}$.

Lemma 2.2: [9] 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 $\mathrm{Tr}(\frac{b}{a^2}) = 1$.

Lemma 2.3: [8, 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 $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $b = z + z^{-1}$.

III. An Equivalent Condition which provides more constructions

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.

A. Definition of 4-Uniform BFI

In [11] the authors introduced a type of functions called preferred Boolean functions, and then constructed many infinite families of permutations of the form $G(x) = \frac{1}{x} + f(\frac{1}{x})$, whose differential uniformity are at most 4.

Theorem 3.1: [11] Let $n = 2k$ be an even integer and f be an n-variable Boolean function. Let ω be an element in $\mathbb{F}_{2^n}$ 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) $f(0) + f(z + \frac{1}{z}) + f(\omega z + \frac{1}{\omega z}) + f(\omega^2 z + \frac{1}{\omega^2 z}) = 0$ for any $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$.

Theorem 3.2: [11] Let $n = 2k$ be an even integer, f be a Boolean function with n variables. Define

$$G(x) = \frac{1}{x} + f(\frac{1}{x}).$$

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.

Theorem 3.2 builds a bridge from PBFs to permutation polynomials with differentially uniformity at most 4. However, as pointed out in [10], f to be 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.

Hence a PBF is a 4-Uniform BFI and not vice versa.

B. An Equivalent Condition

Now we introduce the main theorem of this section. It is an equivalent condition on the switching construction of differentially 4-uniform permutation of $\mathbb{F}_{2^{2k}}$ 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 in $\mathbb{F}_{2^n}$ 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 Lemma 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 exist $a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}$ 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 $\mathbb{F}_{2^n}\backslash\{0,a\}$. Hence 0 is a solution of Eq.(4) or Eq.(5) and each of them has exactly 2 solutions in $\mathbb{F}_{2^n}\backslash\{0,a\}$. 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

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

Since n is an even integer, then $\mathrm{Tr}(\frac{1}{a+1})=\mathrm{Tr}(\frac{a}{a+1})=\mathrm{Tr}(\frac{1}{1+\frac{1}{a}})$. It follows from Lemma 2.2 that Eq.(9) has solutions in $\mathbb{F}_{2^n}$ if and only if $0=\mathrm{Tr}(\frac{1}{a+1})$, which is equal to $\mathrm{Tr}(\frac{1}{1+\frac{1}{a}})$. It follows from $a\neq 0,1$ that $1+\frac{1}{a}\in\mathbb{F}_{2^n}\setminus\ \mathbb{F}_2$. Then according to Lemma 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 gets 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 is 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 Eq.(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 Eq.(11) holds.

Hence at most two of the six equations of Eq.(10) and Eq.(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 $f(x) = f(x+1)$ was 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 was proved that $G(x) = \frac{1}{x} + f(\frac{1}{x})$ constructed by 4-Uniform BFI is not an APN function. In particular, those $G(x)$ constructed 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. We first introduce a lemma.

Lemma 3.5: Let n be an even integer and ω be an element in $\mathbb{F}_{2^n}$ 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.

$$U := \{\alpha + \frac{1}{\alpha}, \alpha + \frac{1}{\alpha} + 1, \omega\alpha + \frac{1}{\omega\alpha}, \omega\alpha + \frac{1}{\omega\alpha} + 1, \omega^2\alpha + \frac{1}{\omega^2\alpha}, \omega^2\alpha + \frac{1}{\omega^2\alpha} + 1,$$
$$\omega\beta + \frac{1}{\omega\beta}, \omega\beta + \frac{1}{\omega\beta} + 1, \omega^2\beta + \frac{1}{\omega^2\beta}, \omega^2\beta + \frac{1}{\omega^2\beta} + 1\}.$$

$$V := \{\omega(\omega\alpha + \frac{1}{\omega\alpha} + 1), \omega^2(\omega\alpha + \frac{1}{\omega\alpha} + 1), \omega(\omega^2\alpha + \frac{1}{\omega^2\alpha} + 1), \omega^2(\omega^2\alpha + \frac{1}{\omega^2\alpha} + 1),$$
$$\omega(\omega\beta + \frac{1}{\omega\beta} + 1), \omega^2(\omega\beta + \frac{1}{\omega\beta} + 1), \omega(\omega^2\beta + \frac{1}{\omega^2\beta} + 1), \omega^2(\omega^2\beta + \frac{1}{\omega^2\beta} + 1)\}.$$

Let us define

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

If $U \cap V = \emptyset$, 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 on $\mathbb{F}_{2^n}$.

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 Lemma 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 Lemma 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) holds.

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.

The proof is completed. □

We use Magma [1] to do an exhaust search for $\mathbb{F}_{2^n}(6 \leq n \leq 18, n$ even). The experiment data is listed in Table I. The data suggests that the number of $f(x)$ constructed by Theorem 3.6 is close to 2^{n-5}. 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: The number of $f(x)$ 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

Theorem 3.6 indicates that there exist some functions which are 4-Uniform BFIs but not PBFs. Indeed, the number of 4-Uniform BFIs is much bigger than that of PBFs. We will estimate the number of 4-Uniform BFIs in the next section.

IV. The Number of 4-Uniform BFIs

According to Definition 3.3, $G(x) = \frac{1}{x} + f(\frac{1}{x})$ is a differentially 4-uniform permutation if and only if f is a 4-Uniform BFI. Thus it is interesting to calculate the number of 4-Uniform BFIs. In this section, we first introduce an algorithm to calculate the exact number of 4-Uniform BFIs. As it is difficult to realize the algorithm, even on $\mathbb{F}_{2^8}$, we propose a method to estimate the number of *η-partly 4-Uniform BFIs* (introduced in Definition 4.5) and then discuss the accuracy of our compact estimation. At last we generalize the method to estimate the number of 4-Uniform BFIs.

A. *The Exact Number of 4-Uniform BFIs*

We first consider the number of PBFs. Suppose that $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by $h(z) = z + \frac{1}{z} + 1$. Then Eq.(1) and Eq.(2) in Theorem 3.4 can be written as

$$f(0) + f(h(z)) + f(h(\omega z)) + f(h(\omega^2 z)) = 0,$$
$$f(0) + f(h(z)) + f(\omega h(z)) + f(\omega^2 h(z)) = 1.$$

Define the following three sets:

$$\begin{aligned} L_x &= \{\{x, x+1\} : x \in \mathbb{F}_{2^n}\}, \\ L_z &= \{\{0, h(z), h(\omega z), h(\omega^2 z)\} : z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4\}, \\ L_h &= \{\{0, h(z), \omega h(z), \omega^2 h(z)\} : z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4\}. \end{aligned}$$

Clearly $|L_x| = 2^{n-1}$. 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 pairwise distinct since the sum of them is 1 and none of them can be 1. Then the 6 different elements $z, \omega z, \omega^2 z, \frac{1}{z}, \frac{1}{\omega z}, \frac{1}{\omega^2 z}$ lead to the same element of L_z, hence $|L_z| = \frac{2^n-4}{6} = \frac{2^{n-1}-2}{3}$. It is clear that $|L_h| \leq \frac{2^n-1}{3}$. Since different elements z may lead to the same element in L_h, we can not get $|L_h|$ directly. However, it can be calculated easily for small number of variables with a computer.

Then we define a matrix M_0 with the size of $(|L_z| + |L_x|) \times 2^n$, where the columns of M_0 are indexed by the 2^n elements in $\mathbb{F}_{2^n}$ and the order of rows is decided by the following algorithm:

Algorithm 4.1:

```
input n;
$M_0 := 0; i := 0; Msupp := 0; SetZ := \emptyset; SetX := \emptyset;$
for $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ do
    if $z + \frac{1}{z} + 1 \notin SetZ$ then
        $i := i + 1; M_0[i, 0] := 1;$
        for $j \in \{0, 1, 2\}$ do
            $M_0[i, \omega^j z + \frac{1}{\omega^j z} + 1] := 1; Msupp[i, j + 1] := \omega^j z + \frac{1}{\omega^j z} + 1;$
    $SetZ := SetZ \bigcup \{z + \frac{1}{z} + 1, \omega z + \frac{1}{\omega z} + 1, \omega^2 z + \frac{1}{\omega^2 z} + 1\};$
for $x \in \mathbb{F}_{2^n}$ do
    if $x \notin SetX$ then
        $i := i + 1; M_0[i, x] := 1; M_0[i, x + 1] := 1;$
    $SetX := SetX \bigcup \{x, x + 1\};$
output $M_0$;$Msupp$.
```

Here we use $Msupp$ to save the support of those lines produced by L_z. The elements of M_0 are in $\mathbb{F}_2$ and each line of M_0 save some messages of the condition of PBFs. Then we get the number of PBFs according to the following theorem.

Theorem 4.2: [11] Let M_0 be defined as above and let f be an n-variable Boolean function expressed by its truth table. Then f is a PBF if and only if it satisfies the equation

$$M_0 f^{\mathrm{T}} = \overline{0}. \tag{17}$$

Further, the number of the Boolean functions satisfying (17) is $2^{2^n - \mathrm{Rank}(M_0)}$. Particularly, if M_0 is a full rank matrix, then this number equals to $2^{\frac{2^n+2}{3}}$.

Now we focus on the number of 4-Uniform BFIs. Assume that the n-variable Boolean function f is a 4-Uniform BFI. Let $\xi = (\xi(1), \cdots, \xi(|L_z|))^{\mathrm{T}}$ be a column vector in $\mathbb{F}_2^{|L_z|}$ and $\xi(i)$ be the i-th element of ξ. Replace the vector $\overline{0}$ in Eq.(17) by $(\xi(1), \cdots, \xi(|L_z|), 0, \cdots, 0)^{\mathrm{T}}$, where the last $|L_x|$ elements are 0. Then $f(x) + f(x+1) = 0$ holds for any $x \in \mathbb{F}_{2^n}$. For any $1 \le i \le |L_z|$, assume that $M_0[i, 0] = M_0[i, h(z_i)] = M_0[i, h(\omega z_i)] = M_0[i, h(\omega^2 z_i)] = 1$ and other elements are 0 in the i-th line of M_0 according to Algorithm 4.1, where $z_i \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$. For those i satisfying $\xi(i) = 0$, the equation $f(0) + f(h(z_i)) + f(h(\omega z_i)) + f(h(\omega^2 z_i)) = 0$ holds. And for the other i satisfying $\xi(i) = 1$, the equation above does not hold, which means the following three equations must hold according to Theorem 3.4.

$$f(0) + f(h(z_i)) + f(\omega h(z_i)) + f(\omega^2 h(z_i)) = 1, \tag{18}$$

$$f(0) + f(h(\omega z_i)) + f(\omega h(\omega z_i)) + f(\omega^2 h(\omega z_i)) = 1, \tag{19}$$

$$f(0) + f(h(\omega^2 z_i)) + f(\omega h(\omega^2 z_i)) + f(\omega^2 h(\omega^2 z_i)) = 1. \tag{20}$$

We define the matrix M_ξ which adds the three conditions above as new lines to M_0 for any $i \in \mathrm{Supp}(\xi)$. However, each condition should be considered at most one time although some of them may be derived from different z_i.

Algorithm 4.3:

```
input $\xi, M_0, Msupp$;
$M_\xi := M_0; i_\xi := |L_z| + |L_x|; SetY := \emptyset$
for $i$ in $Supp(\xi)$ do
    for $j$ in $\{0, 1, 2\}$ do
        if $Msupp[i, j+1] \notin SetY$ then
            $i_\xi := i_\xi + 1; M_\xi[i_\xi, 0] := 1; M_\xi[i_\xi, Msupp[i, j+1]] := 1;$
            $M_\xi[i_\xi, \omega Msupp[i, j+1]] := 1; M_\xi[i_\xi, \omega^2 Msupp[i, j+1]] := 1;$
            $SetY := SetY \cup \{Msupp[i, j+1], \omega Msupp[i, j+1], \omega^2 Msupp[i, j+1]\}$
$m_\xi := i_\xi$
output $M_\xi; m_\xi$;
```

Here m_ξ is the row number of M_ξ, which means M_ξ is a matrix of the size $m_\xi \times 2^n$. Due to Algorithm 4.3, $m_\xi = |L_z| + |L_x| + |L_h| \leq |L_z| + |L_x| + \frac{2^n - 1}{3} \leq 2^n$. The columns of M_ξ are indexed by the 2^n elements in $\mathbb{F}_{2^n}$ and the elements of M_ξ are in $\mathbb{F}_2$. It is clear that for any ξ, let $l \in \mathrm{Supp}(\xi)$ then $m_{\xi + e_l} \leq m_\xi + 3$. Define a column vector v_ξ on $\mathbb{F}_2$ with m_ξ elements as follows: The first $|L_z|$ elements of v_ξ are the same as the vector ξ, the next $|L_x|$ elements are 0 and the last $m_\xi - |L_z| - |L_x|$ elements are 1.

Theorem 4.4: Let n be an even integer. For any $\xi \in \mathbb{F}_2^{|L_z|}$, let M_ξ, v_ξ be defined as above and let f be an n-variable Boolean function expressed by its truth table. Then f is a 4-Uniform BFI if and only if there exists a $\xi \in \mathbb{F}_2^{|L_z|}$ such that f satisfies the following equation.

$$M_\xi f^{\mathrm{T}} = v_\xi. \tag{21}$$

Further, the number of 4-Uniform BFIs on $\mathbb{F}_{2^n}$ is

$$BF(n) = \sum_{\xi \in \mathbb{F}_2^{|L_z|}} (\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1) \times 2^{2^n - \mathrm{Rank}(M_\xi)}. \tag{22}$$

Proof: For any $1 \leq i \leq |L_z|$, if $\xi(i) = 0$, then $f(0) + f(h(z_i)) + f(h(\omega z_i)) + f(h(\omega^2 z_i)) = 0$ holds in these lines. And if $\xi(i) = 1$, the last $m_\xi - |L_z| - |L_x|$ elements are 1, which ensures that all of Eq.(18), Eq.(19) and Eq.(20) hold according to Algorithm 4.3. Clearly, $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$ since the $|L_x|$ elements in the middle of v_ξ are 0 ($v_{\xi(|L_z|+1)} = v_{\xi(|L_z|+2)} = \cdots = v_{\xi(|L_x|+|L_z|)} = 0$). Then for any $\xi \in \mathbb{F}_2^{|L_z|}$, the solutions of Eq.(21) are 4-Uniform BFIs due to Theorem 3.4. Since all of the cases in Theorem 3.4 have been considered when ξ runs over $\mathbb{F}_2^{|L_z|}$, thus f is a 4-Uniform BFI if and only if f is the solution of Eq.(21).

Clearly those solutions corresponding to different ξ are pairwise distinct. By the knowledge of linear algebra, for any $\xi \in \mathbb{F}_2^{|L_z|}$, the number of the Boolean functions satisfying $M_\xi f^{\mathrm{T}} = v_\xi$ is $2^{2^n - \mathrm{Rank}(M_\xi)}$ when $\mathrm{Rank}(M_\xi) = \mathrm{Rank}([M_\xi, v_\xi])$. Otherwise, the number is 0. Here the matrix $[M_\xi, v_\xi]$ is the augmented matrix of Eq.(21). Thus the number of 4-Uniform BFIs on $\mathbb{F}_{2^n}$ is

$$\sum_{\xi \in \mathbb{F}_2^{|L_z|}} (\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1) \times 2^{2^n - \mathrm{Rank}(M_\xi)}.$$

This completes the proof of Theorem 4.4. □

With the help of the computer, we get the exact number of 4-Uniform BFIs on $\mathbb{F}_{2^6}$, which is $16198656 \approx 2^{24}$. In [11], it is computed that the number of PBFs on $\mathbb{F}_{2^6}$ is 2^{21}. Hence the number of 4-Uniform BFIs is almost eight times as that of PBFs. It is difficult to calculate the number even on $\mathbb{F}_{2^8}$ since the complexity is over 2^{42}. Thus it is important to estimate the number of 4-Uniform BFIs.

B. The Estimated Number of 4*-Uniform BFIs*

In this subsection, we first define *η-partly* 4*-Uniform BFIs* as a subset of 4-Uniform BFIs. Then we give a heuristic method to estimate the number of η-partly 4-Uniform BFIs. As it is not a rigorous method, we also do some experiments to show the accuracy of our method. Most of the symbols we use here are introduced in Section II and $|L_z| = \frac{2^{n-1}-2}{3}$ is a fixed number as we defined in last subsection.

Definition 4.5: Let n be an even integer and $\eta \in \mathbb{F}_2^{|L_z|}$. We call the n-variable Boolean function f an *η-partly* 4*-Uniform BFI* if there exists $\xi \preceq \eta$ such that f satisfies Eq.(21). Then the number of *η-partly* 4*-Uniform BFIs* is

$$BF(n,\eta) = \sum_{\xi \preceq \eta} (\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1) \times 2^{2^n - \mathrm{Rank}(M_\xi)}, \tag{23}$$

where M_ξ, v_ξ are defined in Theorem 4.4.

In particular, the number of 4-Uniform BFIs equals $BF(n,\vec{1})$ and the number of PBFs equals $BF(n,\vec{0}) = 2^{2^n - \mathrm{Rank}(M_0)}$.

Since M_ξ, v_ξ depend on ξ and the relationships between them are quite complex, it is difficult for us to calculate the value $\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1$ for all of $\xi \in \mathbb{F}_2^{|L_z|}$ when $n \geq 8$. To make the problem simpler, we regard v_ξ as a random column vector of $\mathbb{F}_2^{m_\xi}$, which means only the length m_ξ depends on ξ. Since M_ξ is identified when ξ fixed, $\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1$ only depends on the random variable v_ξ. Then we use the expected value $\mathbb{E}(\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1)$ in Eq.(23) as an approximation, which means

$$BF(n,\eta) \approx \sum_{\xi \preceq \eta} \mathbb{E}(\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1) \times 2^{2^n - \mathrm{Rank}(M_\xi)} \triangleq \overline{BF}(n,\eta).$$

We call $\overline{BF}(n,\eta)$ *the estimation of η-partly* 4*-Uniform BFIs.*

Now we calculate the expected value $\mathbb{E}(\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1)$ for the random variable v_ξ for any $\xi \in \mathbb{F}_2^{|L_z|}$. Clearly there are totally 2^{m_ξ} possible v_ξ. Since $2^{\mathrm{Rank}(M_\xi)}$ of them are linear combinations over $\mathbb{F}_2$ of the column vectors in M_ξ, the probability that v_ξ is $\mathbb{F}_2$-linearly dependent with the column vectors in M_ξ is $2^{\mathrm{Rank}(M_\xi) - m_\xi}$. And in this case, we have $\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1 = 1$. In the other case, v_ξ is $\mathbb{F}_2$-linearly independent of the column vectors in M_ξ, the value $\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1$ will be 0. Then the expected value $\mathbb{E}(\mathrm{Rank}(M_\xi) - \mathrm{Rank}([M_\xi, v_\xi]) + 1)$ equals $2^{\mathrm{Rank}(M_\xi) - m_\xi} \times 1 + (1 - 2^{\mathrm{Rank}(M_\xi) - m_\xi}) \times 0 = 2^{\mathrm{Rank}(M_\xi) - m_\xi}$.

Thus

$$\begin{aligned} BF(n,\eta) &\approx \overline{BF}(n,\eta) \\ &= \sum_{\xi \preceq \eta} 2^{\mathrm{Rank}(M_\xi) - m_\xi} \times 2^{2^n - \mathrm{Rank}(M_\xi)} \\ &= \sum_{\xi \preceq \eta} 2^{2^n - m_\xi}. \end{aligned}$$

Then we need to estimate the value $\overline{BF}(n,\eta)$.

For any $\eta \in \mathbb{F}_2^{|L_z|}$, define *a series of vectors with ascending order from $\vec{0}$ to η*: $\vec{0} = \eta_0 \preceq \eta_1 \preceq \cdots \preceq \eta_{wt(\eta)-1} \preceq \eta_{wt(\eta)} = \eta$ satisfying $wt(\eta_s) = s$ for any $0 \leq s \leq wt(\eta)$. This means for any $1 \leq s \leq wt(\eta)$,

$\eta_{s-1} \preceq \eta_s$ and only one bit of them is different. We first discuss the relationship between $\overline{BF}(n,\eta_s)$ and $\overline{BF}(n,\eta_{s-1})$.

Lemma 4.6: Let n be an even integer. For any $\eta_s \in \mathbb{F}_2^{|L_z|}$, let $l_1 \in \mathrm{Supp}(\eta_s)$, then

$$\sum_{\xi \preceq \eta_s} 2^{2^n - m_\xi} \geq \frac{9}{8} \sum_{\xi \preceq \eta_s - e_{l_1}} 2^{2^n - m_\xi}.$$

The equality happens if and only if $m_{\xi+e_{l_1}} = m_\xi + 3$ holds for any $\xi \preceq \eta_s - e_{l_1}$.

Proof: For any $\xi \preceq \eta_s - e_{l_1}$, it is clear that $m_{\xi+e_{l_1}} \leq m_\xi + 3$ according to the definition in Algorithm 4.3. Then

$$\begin{aligned}\sum_{\xi \preceq \eta_s} 2^{2^n - m_\xi} &= \sum_{\xi \preceq \eta_s - e_{l_1}} 2^{2^n - m_\xi} + \sum_{e_{l_1} \preceq \xi + e_{l_1} \preceq \eta_s} 2^{2^n - m_{\xi+e_{l_1}}} \\ &\geq \sum_{\xi \preceq \eta_s - e_{l_1}} 2^{2^n - m_\xi} + \sum_{\xi \preceq \eta_s - e_{l_1}} 2^{2^n - m_\xi - 3} \\ &= \frac{9}{8} \sum_{\xi \preceq \eta_s - e_{l_1}} 2^{2^n - m_\xi}\end{aligned}$$

Clearly, the equality happens if and only if $m_{\xi+e_{l_1}} = m_\xi + 3$ holds for any $\xi \preceq \eta_s - e_{l_1}$. □

Since $wt(\eta_s - e_{l_1}) = s-1$, let $\eta_{s-1} = \eta_s - e_{l_1}$. Then $\overline{BF}(n,\eta_s) \geq \frac{9}{8}\overline{BF}(n,\eta_{s-1})$ always holds according to Lemma 4.6. Then we can get a rough estimation of the number of η-partly 4-Uniform BFIs immediately since $m_0 = |L_x| + |L_z| = \frac{2^{n+1}-2}{3}$.

Proposition 4.7: Let n be an even integer and $\eta \in \mathbb{F}_2^{|L_z|}$. Then

$$BF(n,\eta) \approx \sum_{\xi \preceq \eta} 2^{2^n - m_\xi} \geq \left(\frac{9}{8}\right)^{wt(\eta)} 2^{\frac{2^n+2}{3}},$$

Equality in the last inequality happens if and only if there exists *a series of vectors with ascending order from* $\vec{0}$ *to* η, satisfying $m_{\eta_s} = m_{\eta_{s-1}} + 3$ for any $1 \leq s \leq wt(\eta)$. This may happens if $wt(\eta)$ is not very large. But it is impossible when $\frac{2^n+2}{9} < wt(\eta) \leq |L_z|$. Otherwise, $m_\eta = |L_x| + |L_z| + 3wt(\eta) > 2^n$, a contradiction. Thus we need to find a better estimation of $\overline{BF}(n,\eta)$.

Lemma 4.8: Let n be an even integer. For any $\eta_s \in \mathbb{F}_2^{|L_z|}$, let $l_1 \in \mathrm{Supp}(\eta_s)$, if $m_{\eta_s} \leq m_{\eta_s - e_{l_1}} + 2$, then there exists $l_2 \in \mathrm{Supp}(\eta_s - e_{l_1})$, such that

$$\sum_{\xi \preceq \eta_s} 2^{2^n - m_\xi} \geq \frac{41}{32} \sum_{\xi \preceq \eta_s - e_{l_1} - e_{l_2}} 2^{2^n - m_\xi}.$$

Proof: Since $m_{\eta_s} \leq m_{\eta_s - e_{l_1}} + 2$, there exists $l_2 \in \mathrm{Supp}(\eta_s - e_{l_1})$ such that

$$\begin{aligned}&\big\{\{Msupp[l_1,1], \omega Msupp[l_1,1], \omega^2 Msupp[l_1,1]\}, \{Msupp[l_1,2], \omega Msupp[l_1,2], \omega^2 Msupp[l_1,2]\},\\ &\{Msupp[l_1,3], \omega Msupp[l_1,3], \omega^2 Msupp[l_1,3]\}\big\} \bigcap \big\{\{Msupp[l_2,1], \omega Msupp[l_2,1], \omega^2 Msupp[l_2,1]\},\\ &\{Msupp[l_2,2], \omega Msupp[l_2,2], \omega^2 Msupp[l_2,2]\}, \{Msupp[l_2,3], \omega Msupp[l_2,3], \omega^2 Msupp[l_2,3]\}\big\} \neq \varnothing\end{aligned}$$

according to Algorithm 4.3. This means $m_{\xi+e_{l_1}+e_{l_2}} \leq m_\xi + 5$ holds for any $\xi \preceq \eta_s - e_{l_1} - e_{l_2}$. It is clear that $m_{\xi+e_{l_1}} \leq m_\xi + 3$ and $m_{\xi+e_{l_2}} \leq m_\xi + 3$ for the other ξ. According to Lemma 4.6, we get

$$\begin{aligned}
&\sum_{\xi\preceq\eta_s} 2^{2^n-m_\xi}\\
= &\sum_{\xi\preceq\eta_s-e_{l_1}} 2^{2^n-m_\xi} + \sum_{e_{l_1}\preceq\xi+e_{l_1}\preceq\eta_s-e_{l_2}} 2^{2^n-m_{\xi+e_{l_1}}} + \sum_{e_{l_1}+e_{l_2}\preceq\xi+e_{l_1}+e_{l_2}\preceq\eta_s} 2^{2^n-m_{\xi+e_{l_1}+e_{l_2}}}\\
= &\sum_{\xi\preceq\eta_s-e_{l_1}} 2^{2^n-m_\xi} + \sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_{\xi+e_{l_1}}} + \sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_{\xi+e_{l_1}+e_{l_2}}}\\
\geq &\frac{9}{8}\sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_\xi} + \sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_\xi-3} + \sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_\xi-5}\\
= &\frac{41}{32}\sum_{\xi\preceq\eta_s-e_{l_1}-e_{l_2}} 2^{2^n-m_\xi}.
\end{aligned}$$

The proof is completed. □

Assume that there exists *a series of vectors with ascending order from* $\vec{0}$ *to* η, satisfying $m_{\eta_s} \geq m_{\eta_{s-1}} + 2$ for any $1 \leq s \leq wt(\eta)$ as an approximation. Following the approximation above, and assuming that $m_s = m_{s-1} + 2$ happens t times, we have $m_\eta = |L_z| + |L_x| + 3wt(\eta) - t$. This means $m_{\eta_s} = m_{\eta_{s-1}} + 2$ happens $3wt(\eta) + |L_z| + |L_x| - m_\eta = 3wt(\eta) - |L_h|$ times and $m_{\eta_s} = m_{\eta_{s-1}} + 3$ happens $|L_h| - 2wt(\eta)$ times. Then we can give a compact estimation of $\overline{BF}(n,\eta)$ according to Lemma 4.6 and Lemma 4.8.

$$\begin{aligned}
\sum_{\xi\preceq\eta} 2^{2^n-m_\xi} &\approx (\frac{41}{32})^{3wt(\eta)-|L_h|}(\frac{9}{8})^{(|L_h|-2wt(\eta))-(3wt(\eta)-|L_h|)}2^{\frac{2^n+2}{3}}\\
&= (\frac{82}{81})^{3wt(\eta)-|L_h|}(\frac{9}{8})^{wt(\eta)}2^{\frac{2^n+2}{3}}.
\end{aligned}$$

Then we give a compact estimation of the number of η-partly 4-Uniform BFIs. Particularly it is a compact estimation of the number of 4-Uniform BFIs when $\eta = \vec{1}$.

Proposition 4.9: Let n be an even integer and $\eta \in \mathbb{F}_2^{|L_z|}$. Then

$$BF(n,\eta) \approx \overline{BF}(n,\eta) \approx (\frac{82}{81})^{3wt(\eta)-|L_h|}(\frac{9}{8})^{wt(\eta)}2^{\frac{2^n+2}{3}}.$$

Particularly, the number of 4-Uniform BFIs is

$$BF(n,\overline{1}) \approx (\frac{82}{81})^{2^{n-1}-2-|L_h|}(\frac{9}{8})^{\frac{2^{n-1}-2}{3}}2^{\frac{2^n+2}{3}}.$$

Since the method that we use to estimate the number of η-partly 4-Uniform BFIs in this subsection is not a rigorous method, we also do some experiments to show the accuracy of the our method. We calculate the exact number of η-partly 4-Uniform BFIs for some η. By observing the trend of η-partly 4-Uniform BFIs when $wt(\eta)$ grows, we check the accuracy of our compact estimation in Proposition 4.9. Experiment results show that our compact estimation of the number of 4-Uniform BFIs is reliable.

Let η_r be the column vector with the first r elements are 1 and others are 0. We have calculated the exact number of $BF(n,\eta_r)$ for some small n, r by Magma to compare with our compact estimation. Here we only list the data of $BF(8,\eta_r)$ when $r \leq 29$ to indicate the accuracy of our compact estimation.

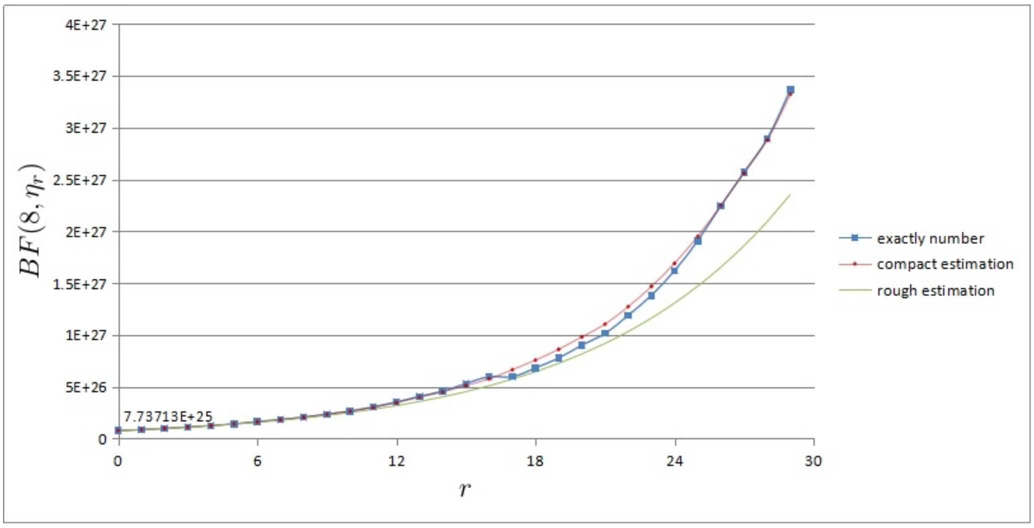

Fig. 1: The trend of $BF(8,\eta_r)$ when r grows

The figure above is the trend of $BF(8,\eta_r)$ and the trend of our compact estimation when r grows from 0 to 29. We also draw the curve $(\frac{9}{8})^r 2^{\frac{2^n+2}{3}}$ as a rough estimation according to Proposition 4.7. As can be seen in figure 1, our compact estimation is further better than the rough estimation and the method we use is reliable. Due to $\text{Rank}(M_\xi) - \text{Rank}([M_\xi, v_\xi]) + 1 = 0$ for any $e_{17} \preceq \xi \preceq \eta_{17}$, the data of $r = 16$ and $r = 17$ is equal. However, our compact estimation still regards v_ξ as a random vector and uses the total expected value $\mathbb{E}(\text{Rank}(M_\xi) - \text{Rank}([M_\xi, v_\xi]) + 1)$ instead as an approximation. This leads to a larger error but this error is counteracted with the growth of r.

Now we list the number of $|L_h|$ when $6 \le n \le 22$ is an even integer. Then the number of 4-Uniform BFIs in our compact estimation is calculated by $BF(n,\overline{1}) \approx (\frac{82}{81})^{2^{n-1}-2-|L_h|}(\frac{9}{8})^{\frac{2^{n-1}-2}{3}} 2^{\frac{2^n+2}{3}}$.

TABLE II: The estimation of $BF(n,\overline{1})$ when $6 \le n \le 22$ is even

n	6	8	10	12	14	16	18	20	22
$\lvert L_h \rvert$	18	69	310	1189	4746	19189	76398	305845	1223266
$BF(n,\overline{1}) \approx$	15780877	$10^{28.34}$	$10^{112.7}$	$10^{450.7}$	10^{1802}	10^{7207}	10^{28831}	10^{115321}	10^{461286}

Here we make two comments. First, according to Proposition 4.9, the number of differentially 4-uniform permutations constructed by 4-Uniform BFIs is much bigger than those constructed by PBFs. Second, $\overline{BF}(n,\eta)$ may be estimated more accurately if one consider more details. It is an interesting problem to enhance the precision of the estimation, or to decide the exact number of 4-Uniform BFIs when $n \ge 8$.

As an application, we can estimate the number of differentially 4-uniform functions constructed in Theorem 3.6. Each of those constructions is corresponding to different ξ with $wt(\xi) = 2$, which means Eq.(21) have solutions for these ξ. Then the number of differentially 4-uniform functions constructed in Theorem 3.6 is at least $T(n) \times 2^{\frac{2^n-13}{3}}$, where $T(n)$ is the exact number of $f(x)$ in Table I.

V. Concluding Remarks

In this paper, a sufficient and necessary condition for the switching construction of differentially 4-uniform permutations from the inverse function is presented. Then we give a compact estimation to the number of this class of differentially 4-uniform permutations. As an application, a new infinite family of 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. To decide the exact number of this class of functions is also an interesting problem. A more important challenge is the *BIG APN* Problem.

VI. ACKNOWLEDGEMENT

We are greatly indebted to Claude Carlet, who has instructed and helped us a lot in revising the last part of the paper. We would also like to thank the editor and the anonymous reviewers for their valuable comments and insightful observations, which allowed to significantly improve the presentation of this paper.

REFERENCES

[1] W.Bosma, J.Cannon and C.Playoust, The magma algebra system.I. The user language, J.Symbolic Comput, 24, 235C265, 1997.

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

[5] 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).

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

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

[8] 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).

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

[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] L.J.Qu, Y.Tan, C.Li and G.Gong, More Constructions of Differentially 4-uniform Permutations on $\mathbb{F}_{2^{2k}}$, Des. Codes Cryptogr. DOI 10.1007/s10623-014-0006-x.

[12] 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.

[13] D.Tang, C.Carlet and X.H.Tang, Differentially 4-Uniform Bijections by Permuting the Inverse Function, Des. Codes Cryptogr. DOI 10.1007/s10623-014-9992-y.

[14] 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).

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