Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 7152657, 10 pages
https://doi.org/10.1155/2020/7152657

Research Article

More Low Differential Uniformity Permutations over $\mathbb{F}_{2^{2k}}$ with k Odd

Yue Leng,[1] **Jinyang Chen**,[2] **and Tao Xie**[1]

[1]*College of Mathematics and Statistics, Hubei Normal University, Huangshi 435002, China*
[2]*College of Mathematics and Statistics, Chongqing Three Gorges University, Chongqing 404130, China*

Correspondence should be addressed to Jinyang Chen; 984121640@qq.com and Tao Xie; 1044806961@qq.com

Received 5 March 2020; Revised 30 May 2020; Accepted 8 June 2020; Published 27 July 2020

Academic Editor: Eric Florentin

Permutations with low differential uniformity, high algebraic degree, and high nonlinearity over $\mathbb{F}_{2^{2k}}$ can be used as the substitution boxes for many block ciphers. In this paper, several classes of low differential uniformity permutations are constructed based on the method of choosing two permutations over $\mathbb{F}_{2^{2k}}$ to get the desired permutations. The resulted low differential uniformity permutations have high algebraic degrees and nonlinearities simultaneously, which provide more choices for the substitution boxes. Moreover, some numerical examples are provided to show the efficacy of the theoretical results.

1. Introduction

Suppose that n be a positive even integer. We always denote by $\mathbb{F}_{2^n}$ the finite field of even characteristic with degree n and $\mathbb{F}_{2^n}^*$ the multiplicative group of nonzero elements of $\mathbb{F}_{2^n}$. Every map from $\mathbb{F}_{2^n}$ to itself is called an (n,n)-function, and bijective (n,n)-function is called a permutation over $\mathbb{F}_{2^n}$. It is well known that confusion introduced by Shannon [1] is one of the most generally accepted design principles for block ciphers and stream ciphers, which means making the relation between the ciphertext and the plaintext as complex as possible for the attacker. The substitution boxes (S-boxes) with good cryptographic properties are used to create confusion in block ciphers and often chosen to be permutations over $\mathbb{F}_{2^n}$. As pointed out in [2], since it needs to resist the differential attack on the block cipher algorithm, the differential uniformity of those permutations as S-boxes is required to be as low as possible. The permutations as S-boxes should also have high algebraic degree to resist the higher order differential attack and high nonlinearity to resist the linear attack (see, for instance, [3, 4]).

It is well known that the lowest differential uniformity of an (n,n)-function over $\mathbb{F}_{2^n}$ is not less than 2. Those (n,n)-functions with differential uniformity 2 are called almost perfect nonlinear (APN) function, which has many interesting properties studied in the last decades (see, for instance, [5–7] and references). However, it is difficult to find APN permutations over the finite field $\mathbb{F}_{2^n}$ for $n \geq 6$. Up to now, a few examples of APN permutations have been found over $\mathbb{F}_{2^6}$ [8–10]. Naturally, people pay more attention to those permutations with differential uniformity 4 or 6 for S-boxes, and a lot of work has been done (see, for instance, [11–25]). Although low differential uniformity permutations are not an optimal choice of S-boxes, they are still an efficient way to against differential attacks. For example, the famous advanced encryption standard (AES) chooses differential 4-uniformity permutation x^{-1} ($0^{-1} := 0$) as its S-box.

The original differential 4-uniformity permutations select Gold functions [12], the Kasami functions [13], the inverse functions [15], and the Bracken–Leander functions [11]. In 2012, Bracken et al. [26] constructed a class of binomials as differential 4-uniformity permutations with high nonlinearity. Inspired by the idea of Carlet [27], Li and Wang [28] obtained a construction of differential 4-uniformity permutations over $\mathbb{F}_{2^n}$ from quadratic APN permutations over $\mathbb{F}_{2^{n+1}}$. The modern method to construct differential 4-uniformity permutation is the switching method proposed by Dillon. In recent years, the power of this method has been shown in the construction of differential 4-uniformity permutations. Qu et al. in [21]

constructed differential 4-uniformity permutations by composing the inverse function and permutations over $\mathbb{F}_{2^n}$ and, in [22], proved that the number of CCZ-inequivalent differential 4-uniformity permutations over $\mathbb{F}_{2^n}$ increases exponentially. For more details, the readers can refer to [14, 19, 23–25, 29, 30].

Different from the above method, in [31, 32], some monomials with differential 6-uniformity over $\mathbb{F}_{2^n}$ for $17 \le n \le 31$ are constructed and in the family of functions:

$$\left\{G_t = x^{2^t-1} \,\middle|\, x \in \mathbb{F}_{2^n}, 1 < t < n\right\}. \tag{1}$$

In 2014, Zha et al. [33] presented three classes of nonmonomial with differential 6-uniformity by modifying the image values of the Gold function. In recent years, more nonmonomial permutations of differential 6-uniformity are proposed. Tu et al. [34, 35] constructed several classes of differential 6-uniformity permutations by selecting the inverse function as a special type of rational functions over $\mathbb{F}_{2^n}$.

Inspired by the idea of [18], we construct some new low differential uniformity permutations. Compared with the previous similar works, our construction can provide a large number of CCZ-inequivalent classes of functions. Precisely, for any $\varepsilon, s \in \mathbb{F}_4$ and some U being a subset of $\mathbb{F}_{2^{2k}}$ with an odd integer k, we prove that the permutations

$$F(x) = \begin{cases} (x+\varepsilon)^{-1} + s, & x \in U, \\ x^{-1}, & x \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{2}$$

have low differential uniformity 4 or 6. It is pointed out here that all of differentially 6-uniform permutations in our construction are CCZ-inequivalent to the existing ones, and it is surprising that there are two new differential 4-uniformity permutations for $k = 3$ CCZ-inequivalent to the previous ones mentioned above. Moreover, all these functions have the optimal algebraic degree and we get a lower bound of the high nonlinearity of F.

The rest of this paper is organized as follows. In the next section, we recall some definitions and general properties of the differential uniformity, algebraic degree, and nonlinearity of (n, n)-functions. In Section 3, we present a new construction of low differential uniformity permutations and discuss the differential uniformity of these permutations over $\mathbb{F}_{2^{2k}}$ with k odd. In Section 4, we consider their other cryptographic properties. Finally, Section 5 concludes the paper.

2. Preliminaries

Let n be a positive even integer and F be an (n, n)-function. We know that any (n, n)-function can be uniquely represented as a univariate polynomial in $\mathbb{F}_{2^n}[x]$:

$$F(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i, \tag{3}$$

where $\alpha_i \in \mathbb{F}_{2^n}$, $0 \le i \le 2^n - 1$. Let $i \in \mathbb{Z}_+$, $t \in \mathbb{N}$ and $i_0, i_1, \ldots, i_t \in \{0, 1\}$. We say that $(i_0, i_1, \ldots, i_t)$ is the binary expansion of i if $i = i_0 2^0 + i_1 2^1 + \cdots + i_t 2^t$ and $wt(i) := |\{j \mid i_j \ne 0, 0 \le j \le t\}|$ is the 2-weight of i. The algebraic degree $\deg(F)$ of $F(x)$ is defined as follows:

$$\deg(F) := \max_{\alpha_i \ne 0} \{wt(i) \mid 0 \le i \le 2^n - 1\}. \tag{4}$$

An (n, n)-function F is affine if $\deg(F) \le 1$. For any (n, n)-permutation F, it is known that $\deg(F) \le n - 1$. If this upper bound is achieved, then F is said to have optimal algebraic degree.

For an (n, n)-function F and $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, denote by $\delta_F(a, b)$ the number of solutions of the equation $F(x + a) + F(x) = b$. We call the multiset

$$\left\{* \delta_F(a, b) \,\middle|\, (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} *\right\}, \tag{5}$$

the differential spectrum of F. The maximum value in the differential spectrum of F is called the differential uniformity of F and denoted by δ, and F is called a differential δ-uniform function [15]. Observe that if x is a solution of $F(x + a) + F(x) = b$, then $x + a$ is also a solution of the equation, and then it follows that δ_F must be an even number greater than or equal to 2.

Let n be a positive integer and k a divisor of n. The trace map $\mathrm{Tr}_k^n(x)$ from $\mathbb{F}_{2^n}$ onto its subfield $\mathbb{F}_{2^k}$ is defined by

$$\mathrm{Tr}_k^n(x) := x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}. \tag{6}$$

In particular, for $k = 1$, $\mathrm{Tr}_k^n(x)$ is called the absolute trace map and denoted by $\mathrm{Tr}(x)$ simply.

For an (n, n)-function $F(x)$, the Walsh transform of the function F is defined as follows:

$$F^W(a, b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(aF(x) + bx)}, \quad (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}. \tag{7}$$

The multisets $\{* F^W(a, b) \mid (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} *\}$ and $\{* |F^W(a, b)| \mid (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} *\}$ are called Walsh spectrum and extended Walsh spectrum of $F(x)$, respectively. The nonlinearity of F is defined as follows:

$$\mathrm{NL}(F) := 2^{n-1} - \frac{1}{2} \max_{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \left|F^W(a, b)\right|. \tag{8}$$

It is well known that $\mathrm{NL}(F) \le 2^{n-1} - 2^{(n-1)/2}$ when n is odd. For the case n even, $2^{n-1} - 2^{n/2}$ is conjectured to be an upper bound of $\mathrm{NL}(F)$ [36].

For two (n, n)-functions $G_1(x)$ and $G_2(x)$, if there exist two affine permutations $A_1(x)$ and $A_2(x)$ such that $G_1(x) = A_1(G_2(A_2(x)))$, then $G_1(x)$ and $G_2(x)$ are called affine equivalent; if there exists an affine function $A(x)$ such that $G_1(x) = A_1(G_2(A_2(x))) + A(x)$, then $G_1(x)$ and $G_2(x)$ are called extended affine (EA) equivalent. If the graphs of $G_1(x)$ and $G_2(x)$ are EA-equivalent, then they are said to be Carlet–Charpin–Zinoviev (CCZ) equivalent, where the graph of $G(x)$ is $\{(x, G(x)) \mid x \in \mathbb{F}_{2^n}\}$. It is known that EA-equivalence implies CCZ-equivalence, and the converse is not always right. Moreover, CCZ-equivalence and EA-equivalence preserve the extended Walsh spectrum and the differential spectrum, and EA-equivalence also preserves the algebraic degree when it is greater than 2 [37, 38].

Definition 1. Let $H(x)$ and $G(x)$ be two permutations over $\mathbb{F}_{2^n}$. Given $\alpha \in \mathbb{F}_{2^n}$, if there exist some positive integer t and some set $C = \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ of $\mathbb{F}_{2^n}$ with $\alpha_1 = \alpha$ such that

$$H(\alpha_1) = G(\alpha_2), \ldots, H(\alpha_{t-1}) = G(\alpha_t), H(\alpha_t) = G(\alpha_1), \tag{9}$$

then the t-subset C is called a t-cycle set of the function H related to the function G and we denote by C_α. Obviously, $\beta \in C_\alpha$ if and only if $C_\beta = C_\alpha$. All the t-cycle sets for $1 \le t \le 2^n$ are also called cycle sets [18].

We still need some helpful lemmas. The following famous lemma reveals that the nonlinearity of the inverse function could achieve the upper bound $2^{n-1} - 2^{n/2}$ of $\mathrm{NL}(F)$.

Lemma 1 (see [39]) *For any positive integer n and any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*$, the value of*

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(ax + bx^{-1}\right)}, \tag{10}$$

can take any integer divisible by 4 in the range $[-2^{(n/2)+1} + 1, 2^{(n/2)+1} + 1]$.

Lemma 2 (see [40]) *Let n be a positive integer. For any $a, b, c \in \mathbb{F}_{2^n}$ with $ab \neq 0$, the equation*

$$ax^2 + bx + c = 0, \tag{11}$$

has two solutions in $\mathbb{F}_{2^n}$ if and only if $Tr(ac/b^2) = 0$.

Lemma 3 (see [18]) *Let $H(x)$ and $G(x)$ be two permutations over $\mathbb{F}_{2^n}$. Then, the function*

$$F(x) = \begin{cases} H(x), & x \in U, \\ G(x), & x \in \mathbb{F}_{2^n} \backslash U, \end{cases} \tag{12}$$

is a permutation over $\mathbb{F}_{2^n}$ if and only if U is a union of some cycle sets of $H(x)$ related to $G(x)$.

3. Construction of Low Differential Uniformity Permutations

In this section, we always assume that $k \ge 3$ is odd. For any $\varepsilon, s \in \mathbb{F}_4$, we select $H(x) = (x + \varepsilon)^{-1} + s$ and $G(x) = x^{-1}$ and define $F(x)$ as

$$F(x) = \begin{cases} (x + \varepsilon)^{-1} + s, & x \in U, \\ x^{-1}, & x \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{13}$$

where U is a disjoint union of the cycle set of $H(x)$ related to $G(x)$.

Firstly, we find all the cycle sets C_α of $H(x)$ related to $G(x)$ for $\alpha \in \mathbb{F}_{2^{2k}} \backslash \mathbb{F}_4$, where C_α is as defined in Definition 1. In what follows, we always write that ω is a primitive element in $\mathbb{F}_4$.

Lemma 4. *For any $\alpha \in \mathbb{F}_{2^{2k}} \backslash \mathbb{F}_4$, the cycle set C_α of $H(x)$ related to $G(x)$ can be expressed as follows:*

(1) If $\varepsilon = 0$,

$$C_\alpha = \begin{cases} \{\alpha\}, & s = 0, \\ \left\{\alpha, \dfrac{\alpha}{1 + s\alpha}\right\}, & s \neq 0. \end{cases} \tag{14}$$

(2) If $\varepsilon = 1$,

$$C_\alpha = \begin{cases} \{\alpha, \alpha + 1\}, & s = 0, \\ \left\{\alpha, 1 + \dfrac{1}{\alpha}, \dfrac{1}{\alpha + 1}\right\}, & s = 1, \\ \left\{\alpha, \dfrac{\alpha + 1}{s^2 + s\alpha}, 1 + \dfrac{s^2}{\alpha}, \dfrac{s^2}{\alpha + 1}, \dfrac{s^2 + s\alpha}{\alpha + s^2}\right\}, & \text{otherwise.} \end{cases} \tag{15}$$

(3) If $\varepsilon = \omega$,

$$C_\alpha = \begin{cases} \{\alpha, \alpha + \omega\}, & s = 0, \\ \left\{\alpha, \dfrac{\alpha + \omega}{\omega^2 + \alpha}, \omega + \dfrac{\omega}{\alpha}, \dfrac{\omega}{\alpha + \omega}, \dfrac{\omega^2\alpha + \omega}{\alpha + 1}\right\}, & s = 1, \\ \left\{\alpha, \dfrac{\alpha + \omega}{\omega + \omega\alpha}, \omega + \dfrac{1}{\alpha}, \dfrac{1}{\alpha + \omega}, \dfrac{\omega + \omega\alpha}{1 + \alpha\omega}\right\}, & s = \omega, \\ \left\{\alpha, \omega + \dfrac{\omega^2}{\alpha}, \dfrac{\omega^2}{\alpha + \omega}\right\}, & s = \omega^2. \end{cases} \tag{16}$$

Proof. By similarity, we only give the details of (1) and (2).

We first prove (1). For $\varepsilon = 0$, obviously, $H(x) = x^{-1} + s$ and $G(x) = x^{-1}$. When $s = 0$, for any $\alpha \in \mathbb{F}_{2^n} \backslash \mathbb{F}_4$, we have $H(\alpha) = G(\alpha)$. Therefore, the cycle set of $H(x)$ related to $G(x)$ is a 1-cycle set, i.e., $C_\alpha = \{\alpha\}$. When $s + t \neq 0$, we let $\alpha_1 := \alpha$ and conclude that $\alpha_2 = \alpha/(1 + s\alpha)$ by $H(\alpha_1) = G(\alpha_2)$. It computes that $H(\alpha_2) = G(\alpha)$ directly. This shows that the cycle set of $H(x)$ related to $G(x)$ is a 2-cycle set and $C_\alpha = \{\alpha, \alpha/(1 + s\alpha)\}$.

To show (2), we set $\alpha_1 = \alpha$. Since $\varepsilon = 1$, we have $H(x) = (x + 1)^{-1} + s$ and $G(x) = x^{-1}$. When $s = 0$, by $H(\alpha_1) = G(\alpha_2)$, we get $\alpha_2 = \alpha + 1$. Then we also get $H(\alpha_2) = G(\alpha)$. Therefore, the cycle set of $H(x)$ related to $G(x)$ is just a 2-cycle set and $C_\alpha = \{\alpha, \alpha + 1\}$. In the case of

$s = 1$, we calculate $\alpha_2 = 1 + (1/\alpha)$ by $H(\alpha_1) = G(\alpha_2)$ and $\alpha_3 = (1/(\alpha + 1))$ by $H(\alpha_2) = G(\alpha_3)$. Furthermore, $H(\alpha_3) = G(\alpha)$. It follows that the cycle set of $H(x)$ related to $G(x)$ is a 3-cycle set $C_\alpha = \{\alpha, 1 + (1/\alpha), 1/(\alpha + 1)\}$. Similarly, we obtain that

$$C_\alpha = \left\{\alpha, \frac{\alpha+1}{s^2+s\alpha}, 1+\frac{s^2}{\alpha}, \frac{s^2}{\alpha+1}, \frac{s^2+s\alpha}{\alpha+s^2}\right\}, \tag{17}$$

either $s = \omega$ or ω^2.

Remark 1. When $\varepsilon = \omega^2$, the cycle sets of $H(x)$ related to $G(x)$ are equivalent to Lemma 4 (3) since ω is a primitive element of $\mathbb{F}_4$ if and only if ω^2 is also a primitive element of $\mathbb{F}_4$.

Some properties of these cycle sets are listed as follows.

Lemma 5. *Let C_α and ε be the same as in Lemma 4. Then*

(a) $C_{\alpha+\varepsilon} = C_\alpha + \varepsilon$.

(b) For any $\eta \in C_\alpha$, $C_\eta = C_\alpha$.

(c) For any $\alpha, \beta \in \mathbb{F}_{2^n}\backslash\mathbb{F}_4$, $C_\alpha = C_\beta$; *otherwise,* $C_\alpha \cap C_\beta = \varnothing$.

Proof. For (a), by similarity, we only prove it for $\varepsilon = 1$. If $s = 0$, it is easy to check that $C_{\alpha+1} = \{\alpha + 1, \alpha + 1 + 1\} = C_\alpha + 1$. If $s = 1$, we have

$$C_{\alpha+1} = \left\{\alpha+1, 1+\frac{1}{\alpha+1}, \frac{1}{\alpha}\right\} = \left\{\alpha+1, 1+\frac{1}{\alpha}+1, \frac{1}{\alpha+1}+1\right\} = C_\alpha + 1. \tag{18}$$

And if $s = \omega$ or $s = \omega^2$,

$$\begin{aligned} C_{\alpha+1} &= \left\{\alpha+1, \frac{\alpha}{1+s\alpha}, 1+\frac{s^2}{\alpha+1}, \frac{s^2}{\alpha}, \frac{1+s\alpha}{\alpha+s}\right\} \\ &= \left\{\alpha+1, \frac{s^2+s\alpha}{\alpha+s^2}+1, 1+\frac{s^2}{\alpha}+1, \frac{s^2}{\alpha+1}+1, \frac{\alpha+1}{s^2+s\alpha}+1\right\} \\ &= C_\alpha + 1. \end{aligned} \tag{19}$$

The proof of (b) is very simple and we omit the details.

To prove (c), we suppose that $C_\alpha \cap C_\beta \neq \varnothing$. Then there exists $\gamma \in C_\alpha \cap C_\beta$, which together with (b) implies $C_\alpha = C_\gamma = C_\beta$. We complete the proof of Lemma 5.

Remark 2. There are 2-cycle sets of $H(x) = (x + \varepsilon)^{-1}$ related to $G(x) = x^{-1}$ over $\mathbb{F}_4^*$, where $\varepsilon \in \mathbb{F}_4^*$. We can define the 2-cycle set as I' and easily get that

$$I' = \begin{cases} \{\omega, \omega^2\}, & \varepsilon = 1, \\ \{1, \varepsilon^2\}, & \varepsilon \neq 1, \end{cases} \tag{20}$$

is closed under addition by ε.

To decompose $\mathbb{F}_{2^{2k}}\backslash\mathbb{F}_4$, we still introduce the set S_α as

$$S_\alpha = \begin{cases} C_\alpha, & s = 0 \text{ or } \varepsilon = 0, \\ C_\alpha \cup C_{\alpha+\varepsilon}, & \text{otherwise}, \end{cases} \tag{21}$$

where C_α is the same as in Lemma 4.

Fix $\varepsilon, s \in \mathbb{F}_4$. For any $\alpha \in \mathbb{F}_{2^{2k}}\backslash\mathbb{F}_4$, each set S_α is a subset of $\mathbb{F}_{2^{2k}}\mathbb{F}_4$. Noticing that, for any $\alpha \in \mathbb{F}_{2^{2k}}\backslash\mathbb{F}_4$ and $k \geq 3$ odd, $|S_\alpha|$ is a positive divisor of $2^{2k} - 4$, by Lemma 5 (c), $\mathbb{F}_{2^{2k}}\backslash\mathbb{F}_4$ could be decomposed into a total of $(2^{2k} - 4)/|S_\alpha|$ such subsets.

Example 1. Let $\varepsilon = \omega, s = \omega$, and α be the primitive element of $\mathbb{F}_{2^6}$. Then, $\mathbb{F}_4 = \{0, 1, \alpha^{21}, \alpha^{42}\}$ and

$$\mathbb{F}_{2^6}\backslash\mathbb{F}_4 = S_\alpha \cup S_{\alpha^2} \cup S_{\alpha^4} \cup S_{\alpha^8} \cup S_{\alpha^{10}} \cup S_{\alpha^{17}}, \tag{22}$$

where

$$\begin{aligned} S_\alpha &= \left\{\alpha^l \,\middle|\, l = 1, 3, 14, 23, 30, 33, 40, 49, 60, 62\right\}, \\ S_{\alpha^2} &= \left\{\alpha^l \,\middle|\, l = 2, 5, 13, 18, 25, 38, 45, 50, 58, 61\right\}, \\ S_{\alpha^4} &= \left\{\alpha^l \,\middle|\, l = 4, 6, 7, 12, 29, 34, 51, 56, 57, 59\right\}, \\ S_{\alpha^8} &= \left\{\alpha^l \,\middle|\, l = 8, 9, 11, 20, 26, 37, 43, 52, 54, 55\right\}, \\ S_{\alpha^{10}} &= \left\{\alpha^l \,\middle|\, l = 10, 15, 16, 24, 28, 35, 39, 47, 48, 53\right\}, \\ S_{\alpha^{17}} &= \left\{\alpha^l \,\middle|\, l = 17, 19, 22, 27, 31, 32, 36, 41, 44, 46\right\}. \end{aligned} \tag{23}$$

If $\mathbb{F}_{2^{2k}}\backslash\mathbb{F}_4 = S_{\alpha_1} \cup S_{\alpha_2} \cup \cdots \cup S_{(2^{2k}-4)/|S_\alpha|}$, we set

$$L = \left\{\alpha_1, \alpha_2, \ldots, \alpha_{(2^{2k}-4)/|S_\alpha|}\right\}, \tag{24}$$

where every α_i is the leading element of S_{α_i}, $i \in \{1, \ldots, (2^{2k} - 4)/|S_\alpha|\}$. By Lemma 5, the sets S_α, $\alpha \in \mathbb{F}_{2^n}\backslash\mathbb{F}_4$, have a nice structure which is stated in the following proposition. The details are omitted.

Proposition 1. *Let $\alpha \in \mathbb{F}_{2^n}\backslash\mathbb{F}_4$. Then S_α is closed under addition by ε.*

Theorem 1. *$F(x)$ is a permutation over $\mathbb{F}_{2^{2k}}$ if the following conditions hold:*

$$U = \begin{cases} \bigcup\limits_{\alpha \in \mathbb{F}_{2^{2k}}\mathbb{F}_4} S_\alpha, & \varepsilon = 0, \\ \bigcup\limits_{\alpha \in J} S_\alpha \cup I', & \varepsilon \neq 0, s = 0, \\ \bigcup\limits_{\alpha \in J} S_\alpha, & \varepsilon \neq 0, s \neq 0, \end{cases} \tag{25}$$

where J is a subset of L and the set I' has been defined in Remark 2.

Proof. By the definition of S_α, we know that all of U is a union of some cycle sets of $H(x)$ related to $G(x)$, which, associated with Lemma 3, implies Theorem 1 holds.

The next step is to study the differential uniformity of $F(x)$. For any $(a, b) \in \mathbb{F}_{2^{2k}}^* \times \mathbb{F}_{2^{2k}}$ and $\varepsilon, s \in \mathbb{F}_4$, the equation $F(x + a) + F(x) = b$ is equivalent to the following four equations on $\mathbb{F}_{2^{2k}}$:

$$\begin{cases} (x+a)^{-1}+x^{-1}=b, \\ x, x+a \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{26}$$

$$\begin{cases} (x+a+\varepsilon)^{-1}+(x+\varepsilon)^{-1}=b, \\ x, x+a \in U, \end{cases} \tag{27}$$

$$\begin{cases} (x+a)^{-1}+(x+\varepsilon)^{-1}=b+s, \\ x \in U, x+a \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{28}$$

$$\begin{cases} (x+a+\varepsilon)^{-1}+x^{-1}=b+s, \\ x \in \mathbb{F}_{2^{2k}} \backslash U, x+a \in U. \end{cases} \tag{29}$$

As the statement of [18], the notations of roots and solutions have different meanings for those equations. For example, we say x_0 is a root of equation (26) if $(x_0+a)^{-1}+x_0^{-1}=b$, and say x_0 is a solution of equation (26) if x_0 is a root of (26) with $x_0, x_0+a \in \mathbb{F}_{2^{2k}} \backslash U$.

Lemma 6. *For the roots of equations (26)–(29), we have the following:*

(a) If x is a root of equation (26), then $x+\varepsilon$ is a root of equation (27), and vice versa. Moreover, $x+a$ is also a root of equation (26).

(b) If x is a root of equation (28), then $x+\varepsilon$ is a root of equation (29), and vice versa. Moreover, $x+a+\varepsilon$ is also a root of equation (28).

Proof. If x is a root of equation (26), then we have $(x+a)^{-1}+x^{-1}=b$, which is equivalent to the equation $(x+\varepsilon+a+\varepsilon)^{-1}+(x+\varepsilon+\varepsilon)^{-1}=b$. This shows that $x+\varepsilon$ is a root of equation (27). Obviously, $x+a$ is another root of equation (26) and $x+a+\varepsilon$ is also a root of equation (27). It finishes the proof of (a) and the proof of (b) can be similarly proved.

We also consider the following equations:

$$\begin{cases} bx^2+abx+a=0, \\ x, x+a \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{30}$$

$$\begin{cases} bx^2+abx+b\varepsilon^2+ab\varepsilon+a=0, \\ x, x+a \in U, \end{cases} \tag{31}$$

$$\begin{cases} (b+s)x^2+(b+s)(a+\varepsilon)x+(b+s)a\varepsilon+\varepsilon+a=0, \\ x \in U, x+a \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{32}$$

$$\begin{cases} (b+s)x^2+(b+s)(a+\varepsilon)x+a+\varepsilon=0, \\ x \in \mathbb{F}_{2^{2k}} \backslash U, x+a \in U. \end{cases} \tag{33}$$

Remark 3. Let $(a,b) \in \mathbb{F}_{2^{2k}}^* \times \mathbb{F}_{2^{2k}}$. When $b \neq a^{-1}$, equations (26) and (27) are equivalent to the following two equations (30) and (31), respectively. When $b \neq (a+\varepsilon)^{-1}+s$, equations (28) and (29) are equivalent to the following two equations (32) and (33), respectively.

If we denote by C_i the set of all solutions of equations (30)~(33), respectively, then we have the following results for the cardinals of C_i, $i=6,7,8,9$.

Lemma 7

(1) $|C_i|=0$ or $|C_i|=2$, $(i=6,7)$ and $|C_6|+|C_7| \leq 2$

(2) $|C_i|=0$ or $|C_i|=1$, $(i=8,9)$ and $|C_8|=1$ if and only if $|C_9|=1$

Proof. We only prove (1) by similarity. If $C_6 \neq \varnothing$, then there exists $\lambda \in C_6$ being the solution of equation (30). So is $\lambda+a$. Noting that equation (30) has at most two solutions for any pair $(a,b) \in \mathbb{F}_{2^{2k}}^* \times \mathbb{F}_{2^{2k}}$, we have $|C_6|=2$. Similarly, if $C_7 \neq \varnothing$, then $|C_7|=2$. Now we prove that $|C_6|+|C_7| \leq 2$. Suppose that $\lambda_1, \lambda_1+a \in C_6$ and $\lambda_2, \lambda_2+a \in C_7$. By Lemma 6 (1), we may write $\lambda_2=\lambda_1+\varepsilon$. However, the fact that $\lambda_1 \notin U$ and $\lambda_2 \in U$ meet a contradiction by Proposition 1. Thus, $|C_6|+|C_7| \leq 2$.

Denoting by T_i the sets of all solutions of equation (26)~(29), $i=2,3,4,5$.

When $\varepsilon=0$, it is obvious that the function in (13) is a differential 4-uniformity permutation over $\mathbb{F}_{2^{2k}}$ if $s=0$. If $s \neq 0$, Zha et al. [24] proved F in (13) is a differential 4-uniformity permutation over $\mathbb{F}_{2^{2k}}$ as a special case. Now, we only need to show that the differential uniformity of the permutation F is as in (13) when $\varepsilon \neq 0$.

Theorem 2. *Let $\varepsilon \neq 0$ and $s=0$. If U as in Theorem 1 satisfies that, for any $x \in U$, $Tr(\varepsilon/x)=1$. Then, the function*

$$F(x)=\begin{cases} (x+\varepsilon)^{-1}+s, & x \in U, \\ x^{-1}, & x \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{34}$$

is of differential 4-uniformity.

Proof. By Theorem 1, it suffices to prove that $F(x+a)+F(x)=b$ has at most 4 solutions. It is equivalent to show that the sum of the numbers of solutions of equations (26) to (29) is less than 4.

Let $(a,b) \in \{\varepsilon\} \times F_{2^{2k}}^*$. The fact that x^{-1} is of differential uniformity 4 implies that the total of the numbers of solutions of equations (26) and (27) is at most 4. Moreover, (28) and (29) have no solutions. Thus, in this case, F is of differential 4-uniformity.

Now we prove that $F(x)+F(x+a)=b$ has at most 4 solutions for $(a,b) \in \mathbb{F}_{2^{2k}}^* \backslash \{\varepsilon\} \times \mathbb{F}_{2^{2k}}^*$. To end this, we consider it to three cases:

(1) $b \neq a^{-1}$ and $b \neq (a+\varepsilon)^{-1}$. From Lemma 7, it follows that

$$\sum_{i=1}^{4} |T_i| = \sum_{i=1}^{4} |C_i| \leq 4, \tag{35}$$

which shows that $F(x)+F(x+a)=b$ has at most 4 solutions.

(2) $b = a^{-1}$. When $a \in U$, by the fact that $0 \notin U$, we know that a is not a solution of equation (26). Neither is 0. The sum of the numbers of equations (26) and (27) is at most 2. Since $b \neq (a+\varepsilon)^{-1}$, by Lemma 7 (2), the sum of the numbers of equations (28) and (29) is also at most 2. And hence, $F(x) + F(x+a) = b$ has at most 4 solutions. When $a \notin U$, obviously, 0 and a are the solutions of equation (26). In addition, since $ab = 1$ and $\mathrm{Tr}(1) = 0$, by Lemma 2, equation (30) has two solutions $a\omega$ and $a\omega^2$, where that ω is a primitive element in $\mathbb{F}_4$. We have $|T_2| = 4$. By $\varepsilon, a+\varepsilon \notin U$ and Lemma 7 (1), we conclude that T_3 is empty. Moreover, we claim that equations (28) and (29) have no solutions. In fact, by Lemma 7, we only need to show that equation (31) or (32) has no solutions. If λ is a solution of equation (32), we get $a^2 + \lambda a + (\lambda\varepsilon + \lambda^2) = 0$. However,

$$\mathrm{Tr}\left(\frac{\lambda\varepsilon + \lambda^2}{\lambda^2}\right) = \mathrm{Tr}\left(\frac{\varepsilon}{\lambda}\right) = 1, \tag{36}$$

which together with Lemma 2 implies that $a^2 + \lambda a + (\lambda\varepsilon + \lambda^2) \neq 0$ for any $a \in \mathbb{F}_{2^{2k}}$. It is a contradiction. Thus, $F(x) + F(x+a) = b$ has 4 solutions.

(3) $b = (a+\varepsilon)^{-1}$. Similar to the statement of the proof of the case $b = a^{-1}$, we also obtain $F(x) + F(x+a) = b$ has at most 4 solutions.

Together with the discussion of the above three cases, we know that F is of differential 4-uniformity. Therefore, it finishes the proof of Theorem 1.

Remark 4

(1) Let $\varepsilon = \omega, s = 0$, and α be the primitive element of $\mathbb{F}_{2^6}$. If we choose $U = S_{\alpha^6} = \{\alpha^l \mid l = 6, 29\}$, then U satisfies all conditions of Theorem 2.

(2) When $\varepsilon = 1$ and $s = 0$, Tang et al. [23] also obtained Theorem 2 and constructed 22 classes of CCZ-inequivalent differential 4-uniformity permutations. In this case, however, we find 27 classes of CCZ-inequivalent differential 4-uniformity permutations based on CCZ-invariant (see Table 1).

Theorem 3. *If $\varepsilon \neq 0$ and $s \neq 0$,*

$$F(x) = \begin{cases} (x+\varepsilon)^{-1} + s, & x \in U, \\ x^{-1}, & x \in \mathbb{F}_{2^{2k}} \backslash U, \end{cases} \tag{37}$$

where $U = \cup_{\alpha \in J} S_\alpha$, then the differential uniformity of the function is of 4 or 6.

Proof. Since the proof of Theorem 3 is very similar to that of Theorem 2, we omit the details.

Remark 5

(1) The permutations F constructed in Theorem 3 are of differential 4-uniformity for all of U if ε and s satisfy one of the following three cases: (1) $\varepsilon = s = 1$; (2) $\varepsilon = \omega$, $s = \omega^2$; and (3) $\varepsilon = \omega^2$, $s = \omega$.

(2) The permutations F are of differential 4-uniformity when $U = \cup_{\alpha \in L} S_\alpha$ (i.e., $U = \mathbb{F}_{2^{2k}}\mathbb{F}_4$), where L has been defined above. In this case, the proof can refer to the case that F in (13) with $\varepsilon = 0$ and $s \neq 0$, since U is closed under addition by ε.

(3) The permutations F constructed in Theorem 3 are of differential 6-uniformity for all of $U = \cup_{\alpha \in J \subset L} S_\alpha$ (J is a proper subset of L) if ε and s satisfy one of the following two cases: (1) $\varepsilon = 1$, $s = \omega$ or ω^2 and (2) $\varepsilon = \omega$ or ω^2, $s = 1$.

(4) When $\varepsilon = s = \omega$ or ω^2, the differential uniformity of the permutations F depends on the choice of $U = \cup_{\alpha \in J \subset L} S_\alpha$. For example, let $\varepsilon = s = \omega$ and $k = 3$, F constructed in Theorem 3 are differential 4-uniformity permutations over $\mathbb{F}_{2^6}$ if $U = S_\alpha \cup S_{\alpha^4} \cup S_{\alpha^{10}}$ or $U = S_\alpha \cup S_{\alpha^2} \cup S_{\alpha^{10}} \cup S_{\alpha^{17}}$, where S_{α^i} comes from Example 1 (see Table 2). Otherwise, F constructed in Theorem 3 are differential 6-uniformity permutations over $\mathbb{F}_{2^6}$ (see Table 3).

4. Other Cryptographic Properties

In this section, we study the algebraic degree and nonlinearity of $F(x)$ over $\mathbb{F}_{2^{2k}}^*$. Moreover, we present some numerical results about the differential spectra, extend Walsh spectra, and nonlinearities of $F(x)$. We also discuss the CCZ-equivalence of $F(x)$ constructed in Section 3.

4.1. Algebraic Degree and Nonlinearity. The aim of this section is to prove that all functions we constructed have the optimal algebraic degree. For any given permutation F over $\mathbb{F}_{2^n}^*$, the algebraic degree of $F(x)$ is at most $n-1$. As noticed in [23] that, for any $(n,1)$-function $h(x)$ (or n-variable Boolean function) with $\deg(h(x)) \leq n-k-1$, if $F(x)$ has algebraic degree at most k, one must have

$$\mathrm{Tr}\left(\sum_{x \in \mathbb{F}_{2^n}} aF(x)h(x)\right) = \sum_{x \in \mathbb{F}_{2^n}} \mathrm{Tr}(aF(x))h(x) = 0, \quad \forall a \in \mathbb{F}_{2^n}^*. \tag{38}$$

It follows that the size of the set $\{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(F(x)h(x)) = 0\}$ must be even from the fact that the algebraic degree of $\mathrm{Tr}(aF(x))h(x)$ is at most $n-1$. Hence, for a permutation $F(x)$ over $\mathbb{F}_{2^n}^*$, if we can show that there exists some Boolean function $h(x)$ with algebraic degree at most 1 such that

$$\sum_{x \in \mathbb{F}_{2^n}} F(x)h(x) \neq 0, \tag{39}$$

then we can conclude that the algebraic degree of F is at least $n-1$.

Table 1: CCZ-inequivalent differential 4-uniformity permutations in Theorem 2 over $\mathbb{F}_{2^6}$ with $\varepsilon = 1, s = 0$.

No.	NL	Extend Walsh spectrum	Differential spectrum
1	22	{*0 [783], 4 [1206], 8 [1024], 12 [798], 16 [209], 20 [12]*}	{*0 [2127], 2 [1794], 4 [111]*}
2	22	{*0 [795], 4 [1210], 8 [1008], 12 [792], 16 [213], 20 [14]*}	{*0 [2139], 2 [1770], 4 [123]*}
3	22	{*0 [794], 4 [1236], 8 [1012], 12 [751], 16 [210], 20 [29]*}	{*0 [2181], 2 [1686], 4 [165]*}
4	20	{*0 [805], 4 [1214], 8 [1014], 12 [774], 16 [195], 20 [28], 24 [2]*}	{*0 [2181], 2 [1686], 4 [165]*}
5	20	{*0 [797], 4 [1240], 8 [998], 12 [755], 16 [219], 20 [21], 24 [2]*}	{*0 [2181], 2 [1686], 4 [165]*}
6	20	{..0 [799], 4 [1242], 8 [999], 12 [748], 16 [217], 20 [26], 24 [1]*}	{*0 [2187], 2 [1674], 4 [171]*}
7	20	{*0 [813], 4 [1244], 8 [991], 12 [737], 16 [211], 20 [35], 24 [1]*}	{*0 [2211], 2 [1626], 4 [195]*}
8	20	{*0 [790], 4 [1252], 8 [1017], 12 [731], 16 [206], 20 [33], 24 [3]*}	{*0 [2211], 2 [1626], 4 [195]*}
9	20	{*0 [804], 4 [1254], 8 [991], 12 [736], 16 [216], 20 [26], 24 [5]*}	{*0 [2217], 2 [1614], 4 [201]*}
10	18	{*0 [841], 4 [1216], 8 [966], 12 [774], 16 [207], 20 [24], 24 [2], 28 [2]*}	{*0 [2217], 2 [1614], 4 [201]*}
11	20	{*0 [810], 4 [1242], 8 [999], 12 [742], 16 [202], 20 [32], 24 [5]*}	{*0 [2223], 2 [1602], 4 [207]*}
12	20	{*0 [831], 4 [1230], 8 [981], 12 [750], 16 [201], 20 [36], 24 [3]*}	{*0 [2223], 2 [1602], 4 [207]*}
13	20	{*0 [803], 4 [1264], 8 [988], 12 [723], 16 [221], 20 [29], 24 [4]*}	{*0 [2223], 2 [1602], 4 [207]*}
14	18	{*0 [808], 4 [1262], 8 [993], 12 [716], 16 [212], 20 [38], 24 [3]*}	{*0 [2235], 2 [1578], 4 [219]*}
15	20	{*0 [815], 4 [1262], 8 [997], 12 [726], 16 [217], 20 [28], 24 [7]**}	{*0 [2241], 2 [1566], 4 [225]*}
16	18	{*0 [815], 4 [1255], 8 [990], 12 [722], 16 [209], 20 [38], 24 [2], 28 [1]*}	{*0 [2241], 2 [1566], 4 [225]*}
17	18	{*0 [822], 4 [1240], 8 [983], 12 [748], 16 [206], 20 [26], 24 [5], 28 [2]*}	{*0 [2241], 2 [1566], 4 [225]*}
18	20	{*0 [801], 4 [1258], 8 [1008], 12 [724], 16 [199], 20 [34], 24 [8]*}	{*0 [2247], 2 [1554], 4 [231]*}
19	20	{*0 [801], 4 [1278], 8 [994], 12 [702], 16 [215], 20 [36], 24 [6]*}	{*0 [2253], 2 [1542], 4 [237]*}
20	18	{*0 [816], 4 [1265], 8 [971], 12 [729], 16 [220], 20 [21], 24 [9], 28 [1]*}	{*0 [2253], 2 [1542], 4 [237]*}
21	20	{*0 [803], 4 [1286], 8 [986], 12 [694], 16 [221], 20 [36], 24 [6]*}	{*0 [2259], 2 [1530], 4 [243]*}
22	18	{*0 [820], 4 [1257], 8 [980], 12 [729], 16 [208], 20 [29], 24 [8], 28 [1]*}	{*0 [2259], 2 [1530], 4 [243]*}
23	18	{*0 [801], 4 [1276], 8 [994], 12 [708], 16 [215], 20 [30], 24 [6], 28 [2]*}	{*0 [2259], 2 [1530], 4 [249]*}
24	18	{*0 [805], 4 [1266], 8 [996], 12 [718], 16 [211], 20 [28], 24 [4], 28 [4]*}	{*0 [2271], 2 [1506], 4 [255]*}
25	22	{*0 [795], 4 [1302], 8 [1008], 12 [654], 16 [213], 20 [60]*}	{*0 [2277], 2 [1494], 4 [261]*}
26	18	{*0 [795], 4 [1284], 8 [1000], 12 [700], 16 [213], 20 [30], 24 [8], 28 [2]*}	{*0 [2277], 2 [1494], 4 [261]*}
27	20	{*0 [783], 4 [1302], 8 [1012], 12 [678], 16 [209], 20 [36], 24 [12]*}	{*0 [2289], 2 [1470], 4 [273]*}

Table 2: CCZ-inequivalent differential 4-uniformity permutations in Theorem 3 over $\mathbb{F}_{2^6}$ with $\varepsilon = s = \omega$.

No.	NL	Extend Walsh spectrum	Differential spectrum
1	22	{*0 [795], 4 [1266], 8 [1008], 12 [708], 16 [213], 20 [42]*}	{*0 [2223], 2 [1602], 4 [207]*}
2	20	{*0 [783], 4 [1254], 8 [1038], 12 [718], 16 [193], 20 [44], 24 [2]*}	{*0 [2223], 2 [1602], 4 [207]*}

Table 3: CCZ-inequivalent differential 6-uniformity permutations in Theorem 3 over $\mathbb{F}_{2^6}$ with $\varepsilon = s = \omega$.

No.	NL	Extend Walsh spectrum	Differential spectrum
1	20	{*0 [803], 4 [1246], 8 [1014], 12 [738], 16 [189], 20 [32], 24 [10]*}	{*0 [2239], 2 [1578], 4 [207], 6 [8]*}
2	18	{*0 [795], 4 [1234], 8 [1040], 12 [738], 16 [181], 20 [40], 24 [0], 28 [4]*}	{*0 [2239], 2 [1578], 4 [207], 6 [8]*}
3	20	{*0 [795], 4 [1258], 8 [1014], 12 [728], 16 [197], 20 [30], 24 [10]*}	{*0 [2239], 2 [1578], 4 [207], 6 [8]*}
4	20	{*0 [765], 4 [1302], 8 [1042], 12 [666], 16 [203], 20 [48], 24 [6]*}	{*0 [2259], 2 [1542], 4 [219], 6 [12]*}
5	20	{*0 [801], 4 [1246], 8 [1026], 12 [726], 16 [183], 20 [44], 24 [6]*}	{*0 [2243], 2 [1566], 4 [219], 6 [4]*}
6	20	{*0 [817], 4 [1278], 8 [976], 12 [702], 16 [215], 20 [36], 24 [8]*}	{*0 [2263], 2 [1530], 4 [231], 6 [8]*}
7	18	{*0 [801], 4 [1268], 8 [1012], 12 [704], 16 [199], 20 [42], 24 [4], 28 [2]*}	{*0 [2263], 2 [1530], 4 [231], 6 [8]*}
8	18	{*0 [805], 4 [1278], 8 [992], 12 [708], 16 [211], 20 [26], 24 [8], 28 [4]*}	{*0 [2279], 2 [1506], 4 [231], 6 [16]*}
9	18	{*0 [813], 4 [1258], 8 [1000], 12 [714], 16 [203], 20 [40], 24 [0], 28 [4]*}	{*0 [2263], 2 [1530], 4 [231], 6 [8]*}
10	18	{*0 [773], 4 [1268], 8 [1038], 12 [720], 16 [195], 20 [26], 24 [10], 28 [2]*}	{*0 [2257], 2 [1536], 4 [237], 6 [2]*}
11	18	{*0 [797], 4 [1264], 8 [1010], 12 [718], 16 [203], 20 [32], 24 [6], 28 [2]*}	{*0 [2257], 2 [1536], 4 [237], 6 [2]*}
12	18	{*0 [815], 4 [1256], 8 [998], 12 [726], 16 [193], 20 [32], 24 [10], 28 [2]*}	{*0 [2273], 2 [1512], 4 [237], 6 [10]*}
13	20	{*0 [791], 4 [1274], 8 [1016], 12 [704], 16 [210], 20 [38], 24 [8]*}	{*0 [2249], 2 [1560], 4 [213], 6 [10]*}
14	20	{*0 [825], 4 [1246], 8 [980], 12 [734], 16 [207], 20 [36], 24 [4]*}	{*0 [2233], 2 [1584], 4 [213], 6 [2]*}
15	20	{*0 [795], 4 [1238], 8 [1018], 12 [750], 16 [197], 20 [28], 24 [6]*}	{*0 [2209], 2 [1632], 4 [189], 6 [2]*}
16	20	{*0 [771], 4 [1270], 8 [1022], 12 [718], 16 [221], 20 [28], 24 [2]*}	{*0 [2159], 2 [1662], 4 [171], 6 [4]*}
17	20	{*0 [817], 4 [1270], 8 [990], 12 [706], 16 [199], 20 [40], 24 [10]*}	{*0 [2277], 2 [1500], 4 [249], 6 [6]*}
18	20	{*0 [779], 4 [1258], 8 [1036], 12 [720], 16 [197], 20 [38], 24 [4]*}	{*0 [2215], 2 [1626], 4 [183], 6 [8]*}
19	20	{*0 [813], 4 [1254], 8 [1006], 12 [722], 16 [187], 20 [40], 24 [10]*}	{*0 [2267], 2 [1518], 4 [243], 6 [4]*}
20	20	{*0 [783], 4 [1274], 8 [1020], 12 [704], 16 [209], 20 [38], 24 [4]*}	{*0 [2229], 2 [1596], 4 [201], 6 [6]*}

Theorem 4. *Let $k \geq 3$ be an odd integer. For any $\varepsilon, s \in \mathbb{F}_4$, $F(x)$ as in (13) has the optimal algebraic degree $2k-1$.*

Proof. When $\varepsilon = 0$, Zha et al. [24] proved Theorem 4 as a special case. Now we turn to prove it for $\varepsilon \neq 0$. To end this, we only need to show that there exists some Boolean function $h(x)$ with algebraic degree at most 1 such that $\sum_{x\in\mathbb{F}_{2^n}} F(x)h(x) \neq 0$.

Let $\varepsilon \neq 0$. Taking $h(x) = \mathrm{Tr}(\varepsilon^{-1}x)$, we know that it is of algebraic degree 1. By $\mathrm{Tr}(\varepsilon^{-1}(x+\varepsilon)) = \mathrm{Tr}(\varepsilon^{-1}x) + \mathrm{Tr}(1)$ and $\mathrm{Tr}(1) = 0$, we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^{2k}}} F(x)h(x) &= \sum_{x\in U} \mathrm{Tr}\left(\varepsilon^{-1}x\right)(x+\varepsilon)^{-1} + s\sum_{x\in U}\mathrm{Tr}\left(\varepsilon^{-1}x\right)\\ &\quad + \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}\mathrm{Tr}\left(\varepsilon^{-1}x\right)x^{-1}\\ &= \sum_{x\in U}\mathrm{Tr}\left(\varepsilon^{-1}(x+\varepsilon)\right)x^{-1} + \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}\mathrm{Tr}\left(\varepsilon^{-1}x\right)x^{-1}\\ &\quad + s\sum_{x\in U}\mathrm{Tr}\left(\varepsilon^{-1}x\right)\\ &= \sum_{x\in\mathbb{F}_{2^{2k}}}\mathrm{Tr}\left(\varepsilon^{-1}x\right)x^{-1} + s\sum_{x\in U}\mathrm{Tr}\left(\varepsilon^{-1}x\right),\end{aligned} \tag{40}$$

where U is the same as in Theorem 1. For any $x \in U$, we have $x + \varepsilon \in U$. Then $\mathrm{Tr}(\varepsilon^{-1}x) + \mathrm{Tr}(\varepsilon^{-1}(x+\varepsilon)) = \mathrm{Tr}(1) = 0$ and so $\sum_{x\in U}\mathrm{Tr}(\varepsilon^{-1}x) = 0$.

Therefore,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^{2k}}} F(x)h(x) &= \varepsilon^{-1}\sum_{x\in\mathbb{F}_{2^{2k}}}\mathrm{Tr}\left(\varepsilon^{-1}x\right)\left(\varepsilon^{-1}x\right)^{-1}\\ &= \varepsilon^{-1}\sum_{x\in\mathbb{F}_{2^{2k}}}\mathrm{Tr}(x)x^{-1} = \varepsilon^{-1}.\end{aligned} \tag{41}$$

We complete the proof of Theorem 4.

Now we consider the nonlinearity of the functions F and obtain the following lower bound.

Theorem 5. *Let $k \geq 3$ be an odd integer. For any $\varepsilon, s \in \mathbb{F}_4$, the nonlinearity of F satisfies $NL(F) \geq 2^{2k-1} - 2^k - |U|$, where U is as in Theorem 1.*

Proof. By the definition of the Walsh transform of the function F, we have, for any $(a,b) \in \mathbb{F}_{2^{2k}} \times \mathbb{F}_{2^{2k}}^*$,

$$\begin{aligned}F^W(a,b) &= \sum_{x\in\mathbb{F}_{2^{2k}}}(-1)^{\mathrm{Tr}[ax+bF(x)]} = \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)}\\ &\quad + \sum_{x\in U}(-1)^{\mathrm{Tr}\left[ax+b\left((x+\varepsilon)^{-1}+s\right)\right]}\\ &= \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)} + \sum_{x\in U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)+\mathrm{Tr}(a\varepsilon+bs)}.\end{aligned} \tag{42}$$

If $\mathrm{Tr}(a\varepsilon + bs) = 0$, then

$$\begin{aligned}F^W(a,b) &= \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)} + \sum_{x\in U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)}\\ &= \sum_{x\in\mathbb{F}_{2^{2k}}}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)}.\end{aligned} \tag{43}$$

And if $\mathrm{Tr}(a\varepsilon + bs) = 1$, then

$$\begin{aligned}F^W(a,b) &= \sum_{x\in\mathbb{F}_{2^{2k}}\setminus U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)} + \sum_{x\in U}(-1)^{\mathrm{Tr}\left[ax+b\left(x^{-1}+t\right)\right]+1}\\ &= \sum_{x\in\mathbb{F}_{2^{2k}}}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)} - 2\sum_{x\in U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)}\\ &= \sum_{x\in\mathbb{F}_{2^{2k}}}(-1)^{\mathrm{Tr}\left(bx^{-1}+ax\right)} - 2\sum_{x\in U}(-1)^{\mathrm{Tr}\left(ax+bx^{-1}\right)}.\end{aligned} \tag{44}$$

Lemma 1 tells us that $\left|\sum_{x\in\mathbb{F}_{2^{2k}}}(-1)^{\mathrm{Tr}(bx^{-1}+ax)}\right| \leq 2^{k+1}$. Therefore, $|F^W(a,b)| \leq 2^{k+1} + 2|U|$, which, according to the definition of $\mathrm{NL}(F)$, implies that

$$\mathrm{NL}(F) = 2^{2k-1} - \frac{1}{2}\max_{(a,b)\in\mathbb{F}_{2^{2k}}\times\mathbb{F}_{2^{2k}}^*}\left|F^W(a,b)\right| \geq 2^{2k-1} - 2^k - |U|. \tag{45}$$

4.2. Numerical Result of CCZ-Inequivalence of $F(x)$. From the primary definition of CCZ-equivalence, it is difficult to check whether two (n,n)-functions are CCZ-equivalent. An alternative method to solve this problem is to compare their CCZ-invariant parameters (such as differential spectrum and extended Walsh spectrum).

We compute the nonlinearity, the extended Walsh spectrum, and the differential spectrum of the constructed functions with different parameters. As we said in Remark 4, we find at least 27 classes of CCZ-inequivalent differential 4-uniformity functions which are listed in Table 1. And as we remarked in Remark 5 (4), there are 2 CCZ-inequivalent differential 4-uniformity classes of functions, which are listed in Table 2. Moreover, CCZ-invariant parameters of the newly differential 6-uniformity functions from Theorem 3 are also computed and listed in Table 3. In these tables, we denote by NL the nonlinearity of a function and the multiset$\{*\, m[t]\, *\}$ the times of t appearing in this multiset which is m.

It is obvious that all of the functions in Table 2 are CCZ-inequivalent to those constructed in [11–13, 15, 26] since they have different nonlinearity. To compare our construction with that described in [14, 16–25], it is found that all of the functions in Table 2 are CCZ-inequivalent to them, since at least one of the extended Walsh spectrum and the differential spectrum is different. Moreover, in Table 3, all of the differential 6-uniformity permutations from Theorem 3 are CCZ-inequivalent to the previously constructed ones in [31–35] when $k = 3$.

5. Conclusions

In this paper, we constructed several classes of low differential uniformity permutations over $\mathbb{F}_{2^{2k}}$ with k odd. All these functions have the optimal algebraic degree, and we get a lower bound of the high nonlinearity of $F(x)$. Moreover, it has been checked by a computer program for $k = 3$ that there are many new CCZ-inequivalent classes of differentially 4- and 6-uniform permutations in our construction. Precisely, all of the differential 6-uniformity permutations are CCZ-inequivalent with the known ones, and there are two new families of differential 4-uniformity permutations.

Data Availability

The data of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This project was supported by the National Natural Science Foundation of China (Grant no. 71701076), Hubei Education Department Key Project (Grant no. D20181902), and Graduate Research Innovation Project of Hubei Normal University (Grant no. 20190108). Tao Xie was supported by the Youth Project of Hubei Province Education Department (Grant no. 2017149) and Doctoral Research Project of Hubei Normal University.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[3] L. R. Knudsen, "Truncated and higher order differentials," *Fast Software Encryption*, vol. 1008, pp. 196–211, 1995.

[4] L. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology-Eurocrypt 93. Lecture Notes in Computer Science*, vol. 765, pp. 386–397, Springer, Berlin, Heidelberg, 1994.

[5] K. Browning, J. Dillon, R. Kibler et al., "Enleadertwodots APN polynomials and related codes," *Journal of Combinatorics, Information & System Sciences*, vol. 34, pp. 135–159, 2009.

[6] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," *Finite Fields and Their Applications*, vol. 14, no. 3, pp. 703–714, 2008.

[7] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009.

[8] L. Perrin, A. Udovenko, and A. Biryukov, "Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem," in *Annual Cryptology Conference*, pp. 93–122, Springer, Berlin, Germany, 2016.

[9] A. Canteaut, S. Duval, and L. Perrin, "A generalisation of dillons APN permutation with the best known differential and linear properties for all fields of size $24k+2$," *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 7575–7591, 2017.

[10] J. F. Dillon, "APN polynomials: an update," in *Proceedings of the Conference Finite Fields and Their Applications Fq9*, Dublin, Ireland, July 2009.

[11] C. Bracken and G. Leander, "A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree," *Finite Fields and Their Applications*, vol. 16, no. 4, pp. 231–242, 2010.

[12] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp)," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[13] T. Kasami, "The weight enumerators for several classes of the 2nd order binary reed-muller codes," *Information and Control*, vol. 18, no. 4, pp. 369–394, 1971.

[14] Y. Q. Li, M. S. Wang, and Y. Y. Yu, "Constructing differentially 4-uniform permutations over F_2^{2k} from the inverse function revisted," 2013, http://eprint.iacr/2013/731.

[15] K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in Cryptology-Eurocrypt 93. Lecture Notes in Computer Science*, vol. 765, pp. 55–64, Springer, Berlin, Heidelberg, 1994.

[16] J. Peng and C. H. Tan, "New explicit constructions of differentially 4-uniformity permutations via special partitions of $F_{2^{2k}}$." *Finite Fields and Their Applications*, vol. 40, pp. 73–89, 2016.

[17] J. Peng, C. H. Tan, and Q. Wang, "A new family of differentially 4-uniformity permutations over $F_{2^{2k}}$ for odd k," *Science China Mathematics*, vol. 59, no. 6, pp. 1221–1234, 2016.

[18] J. Peng, C. H. Tan, and Q. Wang, "New secondary constructions of differentially 4-uniformity permutations over $F_{2^{2k}}$." *International Journal of Computer Mathematics*, vol. 94, no. 8, pp. 1670–1693, 2016.

[19] J. Peng, C. H. Tan, and Q. Wang, "New differentially 4-uniform permutations by modifying the inverse function on subfields," *Cryptography and Communications*, vol. 9, no. 3, pp. 363–378, 2017.

[20] J. Peng, C. H. Tan, Q. Wang, J. Gao, and H. Kan, "More new classes of differentially 4-uniform permutations with good cryptographic properties," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E101.A, no. 6, pp. 945–952, 2018.

[21] L. J. Qu, Y. Tan, and C. Li, "Differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4675–4686, 2013.

[22] L. J. Qu, Y. Tan, C. Li, and G. Gong, "More constructions of differentially 4-uniform permutations on F_2^{2k}." *Designs, Codes and Cryptography*, vol. 78, no. 2, pp. 391–408, 2014.

[23] D. Tang, C. Carlet, and X. Tang, "Differentially 4-uniform bijections by permuting the inverse function," *Designs, Codes and Cryptography*, vol. 77, no. 1, pp. 117–141, 2015.

[24] Z. Zha, L. Hu, and S. Sun, "Constructing new differentially 4-uniform permutations from the inverse function," *Finite Fields and Their Applications*, vol. 25, pp. 64–78, 2014.

[25] Z. Zha, L. Hu, S. Sun, and J. Shan, "Futher results on differentially 4-uniform permutations over $F_{2^{2m}}$." *Science China Mathematics*, vol. 58, no. 7, pp. 1577–1588, 2015.

[26] C. Bracken, C. H. Tan, and Y. Tan, "Binomial differentially 4 uniform permutations with high nonlinearity," *Finite Fields and Their Applications*, vol. 18, no. 3, pp. 537–546, 2012.

[27] C. Carlet, "On known and new differentially uniform functions," in *Information Security and Privacy*, vol. 6812, pp. 1–15, Springer, Berlin, Heidelberg, 2011.

[28] Y. Li and M. Wang, "Constructing differentially 4 uniform power mapping that permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1})," *Designs, Codes and Cryptography*, vol. 72, no. 2, pp. 249–264, 2014.

[29] S. Fu and X. Feng, "Involutory differentially 4-uniform permutations from known constructions," *Designs, Codes and Cryptography*, vol. 87, no. 1, pp. 31–56, 2019.

[30] Y. H. Sin, K. Kim, R. Kim, and S. Han, *Constructing New Differentially 4-uniform Permutations from Known Ones*, Elsevier Inc., Amsterdam, Netherlands, 2020.

[31] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \mapsto x^{2t-1}$." *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 8127–8137, 2011.

[32] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions," *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 487–505, 2014.

[33] Z. Zha, L. Hu, and J. Shan, "Differentially 6-uniform permutations by modifying the gold function," in *Proceedings of the 2014 IEEE International Conference on Information and Automation (ICIA)*, pp. 961–965, Hailar, China, July 2014.

[34] Z. Tu and X. Zeng, "Non-monomial permutations with differential uniformity six," *Journal of Systems Science and Complexity*, vol. 31, no. 4, pp. 1078–1089, 2018.

[35] Z. Tu, X. Zeng, and Z. Zhang, "More permutation polynomials with differential uniformity six," *Science China Information Sciences*, vol. 61, no. 3, pp. 21 9–221, 2018.

[36] H. Dobbertin, "One-to-one highly nonlinear power functions on GF(2^n)," *Applicable Algebra in Engineering, Communication and Computing*, vol. 9, no. 2, pp. 139–152, 1998.

[37] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1141–1152, 2006.

[38] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.

[39] G. Lanchaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Transactions on Information Theory*, vol. 36, no. 3, pp. 686–692, 1990.

[40] F. J. MacWilliams and N. J. Sloane, *The Theroy of Error-Correocting Codes*, North Holland Publishing Codes, Amsterdam, Netherlands, 1977.