New Families of Differentially 4-Uniform Permutations Over $\mathbb{F}_{2^{2k}}$

Yin Tan$^1$, Longjiang Qu$^{2,3}$ *, Chik How Tan$^1$, and Chao Li$^2$ **

$^1$ Temasek Laboratories, National University of Singapore
5A Engineering Drive 1, 09-02, 117411 Singapore
{tslty, tsltch}@nus.edu.sg

$^2$ Department of Mathematics and System Science, Science College, National University of Defense Technology, ChangSha, 410073, China.
ljqu_happy@hotmail.com, lichao_nudt@sina.com

$^3$ Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore.

Abstract. Differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$, especially those with high nonlinearity and high algebraic degree, are cryptographically significant mappings as they are good choices for the substitution boxes (S-boxes) in many symmetric ciphers. For instance, the currently endorsed Advanced Encryption Standard (AES) uses the inverse function, which is a differentially 4-uniform permutation. However, up to now, there are only five known infinite families of such mappings which attain the known maximal nonlinearity. Most of these five families have small algebraic degrees and only one family can be defined over $\mathbb{F}_{2^{2k}}$ for any positive integer $k$. In this paper, we apply the powerful switching method on the five known families to construct differentially 4-uniform permutations. New infinite families of such permutations are discovered from the inverse function, and some sporadic examples are found from the others by using a computer. All newly found infinite families can be defined over fields $\mathbb{F}_{2^{2k}}$ for any $k$ and their algebraic degrees are $2^k - 1$. Furthermore, we obtain a lower bound for the nonlinearity of one infinite family.

Keywords: Permutation polynomial; differentially 4-uniform mapping; S-box; switching method.

1 Introduction

Many symmetric ciphers use the substitution boxes (S-boxes) to bring the confusion and diffusion into the system. Most of such S-boxes are functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. They should have low differential uniformity, high nonlinearity and high algebraic degree so that to be resistant to differential attack ([1]), linear attack ([15]), and higher order differential attack ([10]) respectively. Moreover, for software implementation, it is preferred that S-boxes are permutations on fields with even degree. For example, the Advanced Encryption Standard (AES) uses the inverse function, which is a differentially 4-uniform permutation over $\mathbb{F}_{2^{2k}}$.

* Research of L.J. Qu was supported by the NSFC of China under Grant 60803156, and the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03.

** Research of C. Li was supported by the NSFC of China under Grant 61070215.
As mentioned above, to have optimal resistance to the differential attack, a function chosen to be an S-box should be an almost perfect nonlinear (APN, defined in Section 2), or a differentially 4-uniform permutation over $\mathbb{F}_{2^k}$. However, for APN permutations over fields with even degree, there was only one sporadic example which was discovered in $\mathbb{F}_{2^6}$ until recently [7]. It is a big open problem whether there exist more sporadic, or even infinite families of APN permutations over $\mathbb{F}_{2^k}$. Due to the lack of APN permutations over $\mathbb{F}_{2^k}$, a natural problem motivated by the design of S-boxes is to find more differentially 4-uniform permutations on $\mathbb{F}_{2^k}$, especially those with high nonlinearity and high algebraic degree.

In [3], the authors listed the five known infinite families of such mappings which attain the known maximal nonlinearity (defined in Section 2). But one can find that, except the Kasami and the inverse function, the others have small algebraic degrees (2 or 3), which are then not the ideal choices for S-boxes. Moreover, the inverse function is the only one which can be defined over $\mathbb{F}_{2^k}$ for any positive integer $k$ and its algebraic degree is $2k - 1$. We should mention that there exist also very limited known infinite families of differentially 4-uniform permutations even without the condition to attain the known maximal nonlinearity, see [4] for a recent survey.

The switching method (see details in Section 3.1) was demonstrated to be very powerful to obtain new APN functions, see [2, 9]. In this paper, we apply this method to obtain differentially 4-uniform permutations. More precisely, for a given function $G : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$ and a constant $\gamma$, we consider when the function $G(x) + \gamma \text{Tr}(R(x))$ is a differentially 4-uniform permutation, where $R(x)$ is a function on $\mathbb{F}_{2^k}$ and $\text{Tr}(x) = \sum_{i=0}^{2k-1} x^i$ denotes the absolute trace function. By choosing $G$ to be the functions in [3, Table 1], the computer experiments in small fields show that there exist many differentially 4-uniform permutations, some of which even attain the known maximal nonlinearity. This is a sharp contrast to the short list of the currently known such permutations. We generalize many new infinite families of such permutations with optimal algebraic degree and high nonlinearity from the computational results (Theorems 1, 2). These new families greatly expand the list of differentially 4-uniform permutations. They may provide more choices for the S-boxes.

The rest of this paper is organized as the following. In Section 2, we give necessary definitions used in the paper. In Section 3, we briefly review the switching method and give some preliminary results. New infinite families of differentially 4-uniform permutations are constructed in Section 4. Some conclusion remarks are given in Section 5 and the computational results are given in the Appendix.
2 Preliminaries

An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We can also regard it as a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ by endowing $\mathbb{F}_{2^n}$ with the field structure of $\mathbb{F}_{2^n}$. Denoting by $\mathcal{BF}_n$ the set of all n-variable Boolean functions. It is well known that $(\mathcal{BF}_n, +)$ is a $\mathbb{F}_2$-vector space, where the addition $+$ of two Boolean functions $f, g$ is defined by $(f + g)(x) = f(x) + g(x)$. Moreover, we may define the inner product “$\cdot$” of $f, g$ by $f \cdot g = \sum_{x \in \mathbb{F}_{2^n}} f(x)g(x)$. For a subspace $V$ of $\mathcal{BF}_n$, its dual space $V^\perp$ is defined by

$$V^\perp = \{ h \in \mathcal{BF}_n | h \cdot f = 0 \text{ for all } f \in V \}.$$ 

If $V^\perp = V$, then we call $V$ self-dual. An S-box, or a vectorial Boolean function, is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Through this paper, we always assume $n = m$. An S-box can also be expressed as a polynomial over $\mathbb{F}_{2^n}$. We call it a permutation polynomial (PP) if it induces a bijective mapping on $\mathbb{F}_{2^n}$. For a function $F(x) = \sum_{i=0}^{n-1} a_i x^i$, $a_i \in \mathbb{F}_{2^n}$, its algebraic degree, denoted by $\deg F$, is defined to be the maximal 2-weight of the exponent $i$ such that $a_i \neq 0$, where for an integer $i$, its 2-weight is the number of ones in its binary expression. It is known that if $F$ is a PP on $\mathbb{F}_{2^n}$, then $\deg F \leq n - 1$. If it attains the equality, then we call it a PP with optimal algebraic degree. If $\deg F \leq 1$, then $F(x)$ is called an affine function.

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and any $a, b \in \mathbb{F}_{2^n}, a \neq 0$, define

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

The multiset $\{ \delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0 \}$ is called the differential spectrum of $F$. The value

$$\Delta_F \triangleq \max_{a, b \in \mathbb{F}_{2^n}, a \neq 0} \delta_F(a, b)$$

is called the differential uniformity of $F$, or we call $F$ a differentially $\Delta_F$-uniform function. In particular, we call the function $F$ with $\Delta_F = 2$ an almost perfect nonlinear (APN) function.

Another important method to characterize the nonlinearity of $F$ is as follows. For the above function $F$, the Walsh (Fourier) transform $W_F(a, b) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{C}$ of $F$ is defined as:

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

The set $W_F := \{ W_F(a, b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n} \}$ is called the Walsh spectrum of $F$ and the elements of $W_F$ are called the Walsh coefficients. The nonlinearity $NL(F)$ of $F$ is defined as

$$NL(F) \triangleq 2^{n-1} - \frac{1}{2} \max_{x \in W_F} |x|.$$
It is known that if $n$ is odd, the nonlinearity $NL(F)$ is upper-bounded by $2^{n-1} - 2^n - 1$; and when $n$ is even it is conjectured that $NL(F)$ is upper-bounded by $2^{n-1} - 2^n$. When $n$ is even, we call functions known maximal nonlinear if their nonlinearity attains the aforementioned bound (it is called highly nonlinear in [3]).

Two $(n, n)$-functions $F$ and $G$ are called extended affine (EA) equivalent if there exist affine permutations $L, L' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an affine function $A$ such that $G = L' \circ F \circ L + A$. They are called Carlet-Charpin-Zinoviev (CCZ) equivalent if their graphs $\{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | y = G(x)\}$ are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L_2(x, y) = G(L_1(x, y))$, where $y = F(x)$. It is well known that EA equivalence implies CCZ equivalence, but not vice versa. Moreover, both EA and CCZ equivalence preserve the differential spectrum and the Walsh spectrum up to the signs of the Walsh coefficients, and EA equivalence preserves the algebraic degree.

3 Permutations via switching method

3.1 Switching method

Let $U$ be a subgroup of a group $M$ and $\phi_U : M \to M/U$ be the canonical homomorphism defined by

$$\phi_U(g) = g + U.$$ 

Obviously we may extend the homomorphism $\phi_U$ by linearity to a homomorphism from $\mathbb{F}_{2^n}[M]$ to $\mathbb{F}_{2^n}[M/U]$.

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, define the group ring element

$$G_F = \sum_{g \in \mathbb{F}_{2^n}} (g, F(g)) \in \mathbb{C}[\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}].$$

Now let $F, H$ be two functions over $\mathbb{F}_{2^n}$, and let $U$ be a subgroup of $(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, +)$. We say that $F$ and $H$ are switching neighbours with respect to $U$ if $\phi_U(G_F) = \phi_U(G_H)$. We call $F$ and $H$ switching neighbours in the narrow sense if $U$ is a subgroup of $\{0\} \times \mathbb{F}_{2^n}$ and $\dim(U) = 1$.

The following result in [9, Proposition 3] characterizes the relationship between two functions which are switching neighbours in the narrow sense.

**Result 1** Let $F, H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $U$ is a subgroup of $\{0\} \times \mathbb{F}_{2^n}$. If $\dim(U) = 1$ and $U = \{(0, 0), (0, u)\}$, then $F$ and $H$ are switching neighbours with respect to $U$ if and only if there exists a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $H(x) = F(x) + f(x)u$. 

3.2 Permutations of the form $G(x) + \gamma \text{Tr}(H(x))$

By Result 1 we see that for a given function $G$, the switching neighbours in the narrow sense of $G$ can be represented as the form $G(x) + f(x)v$ for some Boolean function $f$. When will the function with this form be a PP was considered in [5, 6]. Below we give some known results for our future usage.

A Boolean function can be represented, not uniquely, as $\text{Tr}(H(x))$ for some mapping $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. A Boolean function $\text{Tr}(H(x))$ is said to have a $c$-linear structure $\alpha \in \mathbb{F}_{2^n}$ if

$$\text{Tr}(H(x) + H(x + \alpha)) \equiv c$$

for some constant $c \in \mathbb{F}_2$. More details of linear structures can be found in [8, 12, 13]. Linear structures are useful to characterize whether the polynomial of the form $G(x) + \gamma \text{Tr}(H(x))$ is a permutation, see [5, 6]. In particular, when $G$ is a PP, we know the following result from [5, Theorem 2].

**Result 2** Let $G(x), H(x) \in \mathbb{F}_{2^n}[x]$ and $\gamma \in \mathbb{F}_{2^n}$ and $G(x)$ is a PP. Then

$$F(x) = G(x) + \gamma \text{Tr}(H(x))$$

is a PP if and only if $H(x) = R(G(x))$, where $R(x) \in \mathbb{F}_{2^n}[x]$ and $\gamma$ is a 0-linear structure of the Boolean function $\text{Tr}(R(x))$.

Now a natural question arises: for a given PP $G$ and a constant $\gamma$, what is the property of the set of all Boolean functions $\text{Tr}(H(x))$ such that $G(x) + \gamma \text{Tr}(H(x))$ is a PP? The following result is an answer to this question.

**Lemma 1.** Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a PP and $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Let $\gamma \in \mathbb{F}_{2^n}$ be a nonzero constant. Then the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F(x) = G(x) + \gamma h(x)$ is a PP if and only if

$$h(x) + h(y) = 0 \text{ holds for any } x, y \text{ satisfying } G(x) + G(y) = \gamma. \quad (1)$$

Moreover, let

$$S_{G,\gamma} = \{ h \in BF_n | G(x) + \gamma h(x) \text{ is a PP} \}.$$

Then $S_{G,\gamma}$ is a subspace of $(BF_n, +)$ of dimension $2^{n-1}$ and $S_{G,\gamma}$ is self-orthogonal.

**Proof.** Assume that there exist $x, y \in \mathbb{F}_{2^n}$ such that $F(x) = F(y)$, then we get $G(x) + G(y) = (h(x) + h(y))\gamma$. First, assume that (1) is true. Now, if $h(x) + h(y) = 0$, then $G(x) + G(y) = 0$ implies that $x = y$ as $G$ is a permutation. Otherwise, if $h(x) + h(y) = 1$, then $G(x) + G(y) = \gamma$. But this is impossible by (1). Conversely, if $F$ is a permutation, then one can easily see that (1) holds.

Now we show the “Moreover” part. For any $h_1, h_2 \in S_{G,\gamma}$, it is easy to see that $h_1 + h_2$ satisfies (1) and thus $h_1 + h_2 \in S_{G,\gamma}$. Therefore, $S_{G,\gamma}$ is a subspace of...
\( \mathcal{BF}_n \). To determine the dimension of \( S_{G, \gamma} \), first note that we may regard a Boolean function as a vector of length \( 2^n \). By abuse of notations, for a Boolean function \( h \), we still denote by \( h \) its corresponding vector. Define the set \( X = \{ \{x, y\} \subset \mathbb{F}_{2^n} \mid G(x) + G(y) = \gamma \} \), and for each \( t_{xy} = \{x, y\} \in X \), let \( v_{t_{xy}} \) be the characteristic function of \( t_{xy} \). It is clear that the cardinality of \( X \) is \( 2^n - 1 \) since \( G \) is a permutation.

Define the \( 2^n - 1 \times 2^n \) matrix \( R \) by \( R = (v_{t_{xy}}) \), \( t_{xy} \in X \), where the columns and rows of \( R \) are indexed by the elements in \( \mathbb{F}_{2^n} \) and \( X \) respectively. It is also clear that the rank of \( R \) is \( 2^n - 1 \) We may see that, by (1), a Boolean function \( h \in S_{G, \gamma} \) if and only if \( Rh^T = 0 \). Therefore,

\[
\dim(S_{G, \gamma}) = \dim(\mathcal{BF}_n) - \text{rank} R = 2^n - (2^n - 1) = 2^{n-1}.
\]

Now let \( h_1, h_2 \in S_{G, \gamma} \), then \( h_1(x) + h_2(x) = h_1(y) + h_2(y) \) holds for any \( \{x, y\} \in X \), which further leads to \( h_1 \ast h_2 = 0 \). Then with \( \dim S_{G, \gamma} = 2^{n-1} \), we know that \( S_{G, \gamma} \) is self-dual. We finish the proof. \( \square \)

Lemma 1 actually provides a method to find the Boolean function \( h \) such that \( G(x) + \gamma h(x) \) is a PP for a given PP \( G \) and a constant \( \gamma \) by solving linear equations. Using the functions in [3, Table 1], in \( \mathbb{F}_{2^6} \), we found that, by a personal computer, many such PPs exist and many of them were verified to have differential uniformity \( 4 \). Some are even able to attain the known maximal nonlinearity. We list these functions in Table 1 and Table 2 in the Appendix.

By Result 2, two families of PPs were given in [5, Theorem 3]. They will be used to construct differentially \( 4 \)-uniform permutations. We list them below.

\section*{Result 3}

Let \( \gamma, \beta \in \mathbb{F}_{2^n} \) and \( H(x) \in \mathbb{F}_{2^n}[x] \).

1. Then the polynomial \( x + \gamma \text{Tr}(H(x^2 + \gamma x) + \beta x) \) is PP if and only if \( \text{Tr}(\beta \gamma) = 0 \).

2. Then the polynomial \( x + \gamma \text{Tr}(H(x) + H(x + \gamma) + \beta x) \) is PP if and only if \( \text{Tr}(\beta \gamma) = 0 \).

\subsection*{3.3 Useful results}

We will conclude this section by giving some results for later use.

\section*{Result 4 \ [14]} For any \( a, b \in \mathbb{F}_{2^n} \) and \( a \neq 0 \), the polynomial \( p(x) = x^2 + ax + b \in \mathbb{F}_{2^n}[x] \) is irreducible if and only if \( \text{Tr}(b/a^2) = 1 \).

\section*{Result 5 \ [11, Lemma 4.1]} Let \( b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \), then \( \text{Tr}(b^k) = 0 \) if and only if there exists \( \alpha \in \mathbb{F}_{2^n}^* \), such that \( b = \alpha + \alpha^{-1} \).
This subsection will be ended by a brief introduction of the Dickson polynomials. Let $d$ be a positive integer. The Dickson polynomial $D_d(x)$ is defined over $\mathbb{F}_{2^n}$ as

\begin{align}
D_0(x) &= 0, \\
D_1(x) &= x, \quad \text{and} \\
D_d(x) &= xD_{d-1}(x) + D_{d-2}(x).
\end{align}

For any positive integers $u$ and $v$, the Dickson polynomials satisfy:

(i) $D_{uv}(x) = D_u(D_v(x))$,

(ii) $D_u(x + x^{-1}) = x^u + x^{-u}$.

More details about the Dickson polynomials can be found in [14]. We need the following identities of the Dickson polynomials. The proofs can be deduced easily from (3) and (i); and we leave them to the reader.

**Lemma 2.** Let $r$ be a positive integer, then the following identities about the Dickson polynomials hold:

1. $x^{2^r+1} = D_{2^r+1}(x) + D_{2^r-1}(x)$,
2. $x^{2^r+3} = D_{2^r+3}(x) + D_{2^r+1}(x) + D_{2^r-1}(x) + D_{2^r-3}(x)$,
3. $x^{3 \cdot 2^r+1} = D_{3 \cdot 2^r+1}(x) + D_{3 \cdot 2^r-1}(x) + D_{2^r+1}(x) + D_{2^r-1}(x)$.

## 4 New differentially 4-uniform permutations

In this section, we present new infinite families of differentially 4-uniform permutations. Our constructions use Result 3. More precisely, let $L(x)$ be a PP from Result 3. We consider the differential uniformity of the function $L(G(x))$, where $G(x)$ is a known differentially 4-uniform PP. In the following, all the new infinite families are with the form $L(I(x))$, where $I : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ denotes the inverse function. As usual, we extend the definition of $I(x)$ at 0 by $I(0) = 0^{-1} = \frac{1}{0} = 0$. We divide our new found families into two types according to which type $L(x)$ is in Result 3. Finally, since $H(x)$ is any function on $\mathbb{F}_{2^n}$, we can let $x = \gamma y$ and let $H'(x) = H(\gamma^2 x)$ in Result 3(1) or $H'(x) = H(\gamma x)$ in Result 3(2). Thus, to obtain new families of differentially 4-uniform permutations up to CCZ-equivalence, w.l.o.g., we may choose $\gamma = 1, \beta = 0$ in Result 3.

### 4.1 The first type

We give the first infinite family of differentially 4-uniform permutations $L(I(x))$ by using the permutation $L$ in Result 3 (1).

**Theorem 1.** Let $n$ be an even integer and $L$ be a function defined by $L(x) = x + \text{Tr}(x^2 + x^{-1})$. Then $G(x) = L(I(x))$ is a differentially 4-uniform PP. Moreover, the algebraic degree of $G$ is $n - 1$ and the nonlinearity of $G$ satisfies

$\text{NL}(G) \geq 2^{n-1} - \lfloor 2^{\frac{n}{2} + 1} \rfloor - 2.$
Proof. It follows from Result 3 (1) that $G$ is a PP. Now, clearly we have $G(x) = x^{-1} + \text{Tr}(\frac{x^2}{x+1})$. To prove that the differential uniformity of $G$ is 4, we need to show that the equation

$$G(x + a) + G(x) = b$$

(4)

has at most 4 solutions for all $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$. Expressing (4) explicitly we have the following

$$(x + a)^{-1} + x^{-1} = b, \quad \text{Tr}\left(\frac{(x + a)^2}{x + a + 1} + \frac{x^2}{x + 1}\right) = 0; \text{ or}$$

(5)

$$(x + a)^{-1} + x^{-1} = b + 1, \quad \text{Tr}\left(\frac{(x + a)^2}{x + a + 1} + \frac{x^2}{x + 1}\right) = 1.$$  

(6)

If both (5) and (6) have at most two solutions, then clearly (4) has at most four solutions. Otherwise, assume that (5) has four solutions, then we will show that (6) has no solution. Note that if (5) has 4 solutions, then we have $ab = 1$ and $\text{Tr}(\frac{a^2}{a+1}) = 0$. For convenience, we write the first equation of (6) as (6.1) and so on. Hence, Eq. (6.1) can be written as $x^2 + ax + \frac{a^2}{a+1} = 0$. Then by Result 4, Eq. (6.1) has solutions in $\mathbb{F}_{2^n}$ if and only if $\text{Tr}(\frac{1}{a+1}) = 0$. Now let $x_0$ be a solution of (6.1), we have

$$\text{Tr}\left(\frac{(x_0 + a)^2}{x_0 + a + 1} + \frac{x_0^2}{x_0 + 1}\right) = \text{Tr}(a) + \text{Tr}(\frac{1}{x_0 + a + 1} + \frac{1}{x_0 + 1}) = \text{Tr}(a) + \text{Tr}(\frac{a}{x_0 + a + (a + 1)})$$

$$= \text{Tr}(a) + \text{Tr}(a^2 + a) = \text{Tr}(a) = \text{Tr}(\frac{a^2}{a+1}) + \text{Tr}(\frac{1}{a+1}) = 0,$$

which shows that (6) has no solutions in $\mathbb{F}_{2^n}$. Similar arguments may show that (5) has no solutions if (6) has four solutions. Therefore, the differential uniformity of $G$ is 4.

It is not difficult to see that the algebraic degree of $G$ is $n - 1$ and we omit it here.

Finally, we will show the bound of $\text{NL}(G)$. We need to prove that

$$\max_{\alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^n}} |W_G(\alpha, \beta)| \leq 2\lceil 2^{\frac{n}{2}+1} \rceil + 4.$$  

(7)

Firstly, we have

$$W_G(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\alpha(\frac{1}{x} + \text{Tr}(\frac{x^2}{x+1}))) + \beta x}$$

$$= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\frac{1}{x} + \beta x) + \text{Tr}(\alpha) \cdot \text{Tr}(\frac{x^2}{x+1})}.$$
If $\text{Tr}(\alpha) = 0$, then $|W_G(\alpha, \beta)| = |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\frac{x}{\alpha} + \beta x)}| \leq 2^{\frac{n}{2}+1}$ by the well known bound of Kloosterman sum\cite{11}. If $\text{Tr}(\alpha) = 1$, then

$$W_G(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\frac{x}{\alpha} + \beta x + \frac{x^2}{x+1})} = 2|\{x \in \mathbb{F}_{2^n} | \text{Tr}(\frac{a}{x} + \beta x + \frac{x^2}{x+1}) = 0\}| - 2^n.$$ 

Let $S = \{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | y^2 + y = \frac{a}{x} + \beta x + \frac{x^2}{x+1}\}$, and denote by $M$ the cardinality of $S$. Then we have

$$W_G(\alpha, \beta) = M - 2^n.$$ 

(8)

It is easy to see that $(0, 0), (0, 1) \in S$ (Note that 1+0 00 0). If $x = 1$, then we get $y^2 + y = \alpha + \beta$. Thus $S$ contains two points with the first coordinate 1 if and only if $\text{Tr}(\alpha + \beta) = 0$. The following proof requires some knowledge of function fields, one can turn to \cite{16} for reference. Consider the function field $K = \mathbb{F}_{2^n}(x, y)$ with defining equation $y^2 + y = \frac{a}{x} + \beta x + \frac{x^2}{x+1}$. Denote by $N$ the number of the places with degree one of $K/\mathbb{F}_{2^n}$. Then by Serre bound, we have

$$|N - (2^n + 1)| \leq g[2^{\frac{n}{2}+1}],$$

(9)

where $g$ is the genus of $K$. It can be computed that $g = 1$ if $\beta = 1$ and $g = 2$ if $\beta \neq 1$. It can be verified that $K$ has only one pole with degree one. Thus we have

$$N = \begin{cases} M - 3, & \text{if } \text{Tr}(\alpha + \beta) = 0, \\ M - 1, & \text{otherwise}. \end{cases}$$

(10)

Combining (8), (9) and (10), we get the inequality (7). The proof is completed. □

By MAGMA, the differential spectrum and the nonlinearity of $G$ in Theorem 1 are given in Table 3 in the Appendix when $n = 6, 8, 10, 12$. Since their differential spectrum and nonlinearity are different from known ones, they are therefore CCZ-inequivalent to all known such functions. We can see that the nonlinearity of $G$ is less than the known maximal nonlinearity. But we should mention that its distance to the known maximal nonlinearity is very similar to the newly found such function $F_3$ in [4].

Furthermore, the inverse function of $G$ in Theorem 1 can be determined.

**Proposition 1.** The inverse function of the permutation polynomial in Theorem 1 is given by $P(x) = \frac{1}{x + \text{Tr}((x^2 + x)^{-1})}$.
Proof. Let \( R(x) = 1/G(x) \). One may check that
\[
(G \circ R)(x) = G\left(\frac{1}{G(x)}\right)
\]
\[
= G(x) + \text{Tr}\left(\frac{1}{G(x)^2 + G(x)}\right)
\]
\[
= x^{-1} + \text{Tr}\left(\frac{x^2}{x+1}\right) + \text{Tr}\left(\frac{1}{x-2x-1}\right)
\]
\[
= x^{-1}.
\]
Therefore we have
\[
(G \circ R) \circ (G \circ R) = G \circ (R \circ G \circ R) = id,
\]
where \( id \) denotes the identity mapping defined by \( id(x) = x \) for all \( x \in \mathbb{F}_{2^n} \). Clearly, the inverse function \( P \) of \( G \) is \( R \circ G \circ R \). By routine computations, we have
\[
P(x) = \frac{1}{x + \text{Tr}\left((x^2 + x)^{-1}\right)}.
\]
We finish the proof. \( \square \)

4.2 The second type

Now we use \( L \) from the ones in Result 3 (2) to obtain more differentially 4-uniform permutations. In the following, we only consider the case that \( H(x) \) is a power function.

**Theorem 2.** Let \( n = 2k \) be an even integer and \( L(x) = x + \text{Tr}\left(x^d + (x+1)^d\right) \). Define the function \( G(x) = L(I(x)) \). Then \( G \) is a differentially 4-uniform PP if
1. \( d = 2^n - 2, \)
2. \( n = 2k = 4m, d = 2^{2m} + 2^m + 1, \)
3. \( d = 2^t + 1, \) where \( 1 \leq t \leq k - 1, \)
4. \( d = 3(2^t + 1), \) where \( 2 \leq t \leq k - 1. \)

Furthermore, the algebraic degree of \( G \) obtained in (4) is \( n - 1 \) and its inverse function \( P(x) \) is \( 1/G(x^{-1}) \).

**Proof.** By Result 3 (2), we can see that \( G \) is a PP for all exponents \( d \). We will show their differential uniformity is 4 case by case. First, after expanding the function \( G \), it is not difficult to see that (1) is the same as the one in Theorem 1, and (3) is the inverse function. Routine computations may show that (2) is EA-equivalent to the inverse function and hence the differential uniformity is 4. In the following we focus on proving (4).
For any $x$ and $b$, define $P, Q$ by
\[
P(b) = \text{Tr} \left( (b+1)^d + b^d + 1 \right),
\]
\[
Q(x, b) = \text{Tr} \left( \left( \frac{1}{x} \right)^d + \left( \frac{1}{x} + 1 \right)^d + \left( \frac{1}{x} + b \right)^d + \left( \frac{1}{x} + b + 1 \right)^d \right).
\]

We first prove the following claim is true: for any $x \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ satisfying the following two equations:
\[
\text{Tr} \left( \frac{1}{b+1} \right) = 0, \tag{11}
\]
\[
x^2 + \frac{1}{b} x + \frac{1}{b(b+1)} = 0, \tag{12}
\]
we have
\[
P(b) + Q(x, b) = 0. \tag{13}
\]

From (11) and Result 5, we know that there exists $\alpha \in \mathbb{F}_{2^n}^*$, such that $b+1 = \alpha + \alpha^{-1}$. Let $u = \alpha + \alpha^{-1} = 1 + b$, then with $d = 3(2^t + 1)$, we have
\[
P(b) = \text{Tr} \left( (b+1)^d + b^d + 1 \right) = \text{Tr} \left( (u+1)^d + u^d + 1 \right)
= \text{Tr} \left( u^{d-1} + u^{d-2} + u^{d-2t} + u^{d-2t+1} + u^{2t+1} + u^{2t+2} \right)
= \text{Tr} \left( u^{3t+1} + u^{3t+1} + u^{2t+1} + u^{2t+3} + u^{2t+1} + u^{2t-1} \right).
\]
Substitute the identities in Lemma 2 in the above equation, we get
\[
P(b) = \text{Tr} \left( D_{3 \cdot 2^t+1}(u) + D_{3 \cdot 2^t-1}(u) + D_{3 \cdot 2t-1+1}(u) + D_{3 \cdot 2t-1-1}(u) + D_{2 + 1+3}(u) + D_{2 + 1-3}(u) + D_{2 + 3}(u) + D_{2-3}(u) \right).
\]
Let $S = \{3 \cdot 2^t \pm 1, 3 \cdot 2^t-1 \pm 1, 2^t+1 \pm 3, 2^t \pm 3\}$, we can rewrite $P$ as
\[
P(b) = \text{Tr} \left( \sum_{j \in S} D_j(u) \right). \tag{14}
\]

Now we solve $x$ from (12). Let $x = \frac{1}{b} (y + \omega)$, where $\omega \in \mathbb{F}_{2^n}$ with order 3. Then (12) turns to $y^2 + y + \frac{1}{b+1} = 0$. It follows from $b+1 = \alpha + \alpha^{-1}$ that $y = \frac{1}{\alpha + 1}$ or $\frac{\alpha}{\alpha + 1}$. If $y = \frac{1}{\alpha + 1}$, then
\[
x = \frac{1}{b} (y + \omega) = \frac{\alpha}{\alpha^2 + \alpha + 1} \cdot \frac{\omega \alpha + \omega^2}{\alpha + 1} = \frac{\omega \alpha}{(\alpha + \omega^2)(\alpha + 1)} = \frac{\omega \alpha}{\alpha^2 + \omega \alpha + \omega^2}.
\]
Therefore,
\[
\frac{1}{x} + 1 = \frac{\alpha^2 + \omega^2}{\omega \alpha} = \omega^2 \alpha + \frac{1}{\omega^2 \alpha},
\]
and
\[
\frac{1}{x} + b = \omega^2 \alpha + \frac{1}{\omega^2 \alpha} + \alpha + \frac{1}{\alpha} = \omega \alpha + \frac{1}{\omega \alpha}.
\]
Let \( v = \omega^2 \alpha + \frac{1}{\omega^2 \alpha} \), and \( w = \omega \alpha + \frac{1}{\omega \alpha} \). Then we get
\[
Q(x, b) = \text{Tr} \left( (1 + v)^d + v^d + w^d + (1 + w)^d \right).
\]

Similar arguments as those in (14) deduce that
\[
Q(x, b) = \text{Tr} \left( \sum_{j \in S} \left( D_j(v) + D_j(w) \right) \right).
\]

Summarizing (14) and (15) we obtain
\[
P(b) + Q(x, b) = \text{Tr} \left( \sum_{j \in S} \left( D_j(a) + D_j(v) + D_j(w) \right) \right)
= \text{Tr} \left( \sum_{j \in S} \left( \alpha^j (1 + \omega^j + \omega^{2j}) + \frac{1}{\alpha^j} (1 + \omega^j + \omega^{2j}) \right) \right)
= 0.
\]
The last equality uses the fact that \( 1 + \omega^j + \omega^{2j} = 1 \) if \( 3 \mid j \); and 0 otherwise.

Similarly, if \( y = \frac{\alpha}{\alpha + 1} \), we can also show that (13) holds.

Now we are able to determine the differential uniformity of \( G \). For any \( a, b \in \mathbb{F}_{2^n}, a \neq 0 \), we consider the number of the solutions of the equation \( G(x + a) + G(x) = b \), i.e.

\[
\begin{cases}
(x + a)^{-1} + x^{-1} = b, \\
\text{Tr} \left( \left( \frac{1}{x} \right)^d + \left( \frac{1}{x} + 1 \right)^d + \left( \frac{1}{x+a} \right)^d + \left( \frac{1}{x+a+1} \right)^d \right) = 0;
\end{cases}
\]

or

\[
\begin{cases}
(x + a)^{-1} + x^{-1} = b + 1, \\
\text{Tr} \left( \left( \frac{1}{x} \right)^d + \left( \frac{1}{x} + 1 \right)^d + \left( \frac{1}{x+a} \right)^d + \left( \frac{1}{x+a+1} \right)^d \right) = 1.
\end{cases}
\]

Clearly we only need to consider the cases that \( ab = 1 \) or \( a(b + 1) = 1 \).

**Case** \( ab = 1 \). In this case, if (16) has 4 solutions and (17.1) has two zeros, then (11), (12) and \( P(b) = 0 \) holds. Thus by (13), we have \( Q(x, b) = 0 \), which means
that (17) has no zero. Thus \( G(x + a) + G(x) = b \) has at most 4 solutions in this case.

**Case** \( a(b + 1) = 1 \). Now if (17) has 4 solutions and (16.1) has 2 solutions, then we have

\[
\Tr\left(\frac{1}{b}\right) = 0; \tag{18}
\]
\[
x^2 + \frac{1}{b + 1} x + \frac{1}{b(b + 1)} = 0; \tag{19}
\]

Note that if we replace \( b \) with \( b + 1 \), then (18) and (19) turn to (11) and (12), respectively, and \( P(b) \) and \( Q(x, b) \) remains unchanged, which implies that (13) will still hold. Similar arguments as above may show that \( G(x + a) + G(x) = b \) has at most 4 solutions.

Similarly as Theorem 1 and Proposition 1, one can show the statements about the algebraic degree of \( G \) and its inverse function, we omit them here. The proof is completed. □

By MAGMA, when \( k \leq 8 \), we searched all the exponents \( d \) such that \( G(x) = L(I(x)) \) is a differentially 4-uniform PP on \( \mathbb{F}_{2^k} \), where \( L(x) = x + \Tr(x^d + (x + 1)^d) \). We found that, when \( 5 \leq k \leq 8 \), except those exponents \( d \) in Theorem 2, there do not exist any other such exponent. Therefore we conjecture that the list of the exponent \( d \) in Theorem 2 is complete. In Table 4, for small cases, we give the differential spectrum and nonlinearity of the functions in Theorem 2 (4). From these computational results, we see that these functions are CCZ-inequivalent to all differentially 4-uniform PPs, including the ones in Theorem 1. Moreover, one can also observe that, by choosing different \( t \), the functions in Theorem 2 (4) are also CCZ-inequivalent pairwise in small cases. If this is true for any integer \( k \), then Theorem 2 (4) may contribute \( \frac{n}{2} - 2 \) new CCZ-inequivalent differentially 4-uniform PPs over \( \mathbb{F}_{2^k} \). Unfortunately, we can not prove that they are pairwise inequivalent now and leave it as an open problem in Section 5.

5 Conclusions and future work

In this paper, we succeed in using the switching method to construct new differentially 4-uniform permutations over \( \mathbb{F}_{2^k} \). Many new infinite families of such mappings with optimal algebraic degree are found over \( \mathbb{F}_{2^k} \) for any \( k \). One family of such functions are proved to have high nonlinearity. The inverse functions of all new obtained functions are also determined. The computational results and the new obtained infinite families suggest that there may exist many such mappings, which is a sharp contrast to the current short list of such mappings. For the future research, we propose two problems below for interested readers.
Problem 1. Are the new differentially 4-uniform permutations in Theorem 2 (4) CCZ-inequivalent by choosing different \( t \)?

Problem 2. Can one generalize more infinite families of differentially 4-uniform permutations over \( \mathbb{F}_{2^k} \), especially those with the known maximal nonlinearity, like those in Tables 1, 2?

Acknowledgement

The authors would like to thank Prof. Chaoping Xing for guidance and helps to compute the nonlinearity bound of the function \( G \) in Theorem 1. This work was completed when the second author worked as a research fellow in Nanyang Technology University.

References

6. P. Charpin and G. M. Kyureghyan, When does \( G(x) + \gamma \text{Tr}(H(x)) \) permute \( \mathbb{F}_{2^n} \), Finite Fields and Their Applications, 15 (2), 615–632, (2009).
9. Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematical Communications 3(1), 59–81, (2009).
Appendix

In this section, we give the computational results mentioned in the paper. The finite field $\mathbb{F}_{2^k}$ is defined by the primitive polynomial $x^6 + x^4 + x^3 + x + 1$. The notation NL represents the nonlinearity of a function. The multiset $M = \{a_1^{m_1}, a_2^{m_2}, \ldots, a_n^{m_n}\}$ means the elements $a_i$ appears $m_i$ times in $M$ for $1 \leq i \leq n$.

Tables 1, 2 list the switching neighbors we obtained in the narrow sense of the Gold mapping $x^5$ and the Kasami mapping $x^{13}$ respectively. Tables 3, 4 list the differential spectrum and the nonlinearity of the functions in Theorems 1 and 2 (4).

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>NL</th>
<th>Differential spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>$x^5$</td>
<td>24</td>
<td>${0^{2424}, 4^{1008}}$</td>
</tr>
<tr>
<td>1.2</td>
<td>$x^5 + \text{Tr}_2^6(x^y) + \text{Tr}(x^{23} + w^{21}x^{21} + x^{14} + x^{11} + w^{42}x^7 + w^{42}x^5 + x^3 + x)$</td>
<td>24</td>
<td>${0^{2736}, 2^{576}, 4^{720}}$</td>
</tr>
<tr>
<td>1.3</td>
<td>$x^5 + \text{Tr}_2^6(x^y) + \text{Tr}(x^{23} + x^{21} + w^{18}x^{15} + x^{13} + w^{54}x^5)$</td>
<td>24</td>
<td>${0^{2688}, 2^{672}, 4^{672}}$</td>
</tr>
<tr>
<td>1.4</td>
<td>$x^5 + \text{Tr}_2^6(x^y) + \text{Tr}(w^{21}x^{21} + x^{15} + w^{21}x^{14} + w^{53}x^5 + x^3 + x)$</td>
<td>24</td>
<td>${0^{2664}, 2^{720}, 4^{648}}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>NL</th>
<th>Differential spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>$x^{13}$</td>
<td>24</td>
<td>${0^{3024}, 4^{1008}}$</td>
</tr>
<tr>
<td>2.2</td>
<td>$x^{13} + \text{Tr}_2^6(x^{27}) + \text{Tr}(w^{21}x^{15} + w^{21}x^{14} + x)$</td>
<td>24</td>
<td>${0^{2448}, 2^{1152}, 4^{432}}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>NL</th>
<th>Differential spectrum</th>
<th>NL bound in Theorem 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>20</td>
<td>${0^{2091}, 2^{1146}, 4^{285}}$</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>102</td>
<td>${0^{36735}, 2^{24450}, 4^{4995}}$</td>
<td>94</td>
</tr>
<tr>
<td>10</td>
<td>454</td>
<td>${0^{89389}, 2^{392550}, 4^{65613}}$</td>
<td>446</td>
</tr>
<tr>
<td>12</td>
<td>1928</td>
<td>${0^{9432879}, 2^{92993922}, 4^{1046819}}$</td>
<td>1918</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>NL</th>
<th>Differential spectrum</th>
<th>NL bound in Theorem 2(4) over $\mathbb{F}_{2^n}$</th>
</tr>
</thead>
</table>

---

**Table 1.** Switching classes of $x^5$ over $\mathbb{F}_{2^6}$

**Table 2.** Switching classes of $x^{13}$ over $\mathbb{F}_{2^6}$

**Table 3.** Walsh and differential spectrum of functions in Theorem 1 over $\mathbb{F}_{2^n}$

**Table 4.** Nonlinearity and differential spectrum of functions in Theorem 2(4) over $\mathbb{F}_{2^n}$
<table>
<thead>
<tr>
<th>$n$</th>
<th>$d$</th>
<th>NL</th>
<th>Differential spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>15</td>
<td>22</td>
<td>${0^{2223}, 2^{1602}, 4^{207}}$</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>98</td>
<td>${0^{08945}, 2^{21990}, 4^{3855}}$</td>
</tr>
<tr>
<td>27</td>
<td>100</td>
<td></td>
<td>${0^{06351}, 2^{25218}, 4^{371\text{I}}}$</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
<td>446</td>
<td>${0^{087199}, 2^{396930}, 4^{63423}}$</td>
</tr>
<tr>
<td>27</td>
<td>448</td>
<td></td>
<td>${0^{086230}, 2^{398850}, 4^{62464}}$</td>
</tr>
<tr>
<td>51</td>
<td>440</td>
<td></td>
<td>${0^{098919}, 2^{393090}, 4^{65343}}$</td>
</tr>
<tr>
<td>12</td>
<td>15</td>
<td>1884</td>
<td>${0^{132063}, 2^{295554}, 4^{104590}}$</td>
</tr>
<tr>
<td>27</td>
<td>1890</td>
<td></td>
<td>${0^{143743}, 2^{298480}, 4^{105689}}$</td>
</tr>
<tr>
<td>51</td>
<td>1898</td>
<td></td>
<td>${0^{1433711}, 2^{2988298}, 4^{1049151}}$</td>
</tr>
<tr>
<td>99</td>
<td>1900</td>
<td></td>
<td>${0^{1436671}, 2^{19286338}, 4^{1050111}}$</td>
</tr>
</tbody>
</table>