Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$ from quadratic APN permutations over $\mathbb{F}_{2^{2m+1}}$

Yongqiang Li and Mingsheng Wang

The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, China
yongq.lee@gmail.com
mingsheng_wang@yahoo.com.cn

Abstract. In this paper, by means of the idea proposed in [8], differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_{2^{2m}}$ can be constructed by using quadratic APN permutations over $\mathbb{F}_{2^{2m+1}}$. Special emphasis is given for the Gold functions. The algebraic degree of the constructions and their compositional inverse is also investigated. One of the constructions and its compositional inverse have both algebraic degree $m+1$ over $\mathbb{F}_2^{2m}$.

Key words: Permutation, Differential uniformity, Nonlinearity, Algebraic degree

1 Introduction

S(ubstitution)-boxes play an important role in iterated block ciphers since they serve as the confusion part and in most cases are the only nonlinear part of round functions. For efficiency of implementations, S-boxes are often designed as permutations over $\mathbb{F}_{2^{2n}}$ in practice. These boxes should possess low differential uniformity and high nonlinearity to resist differential cryptanalysis [4] and linear cryptanalysis [17] respectively. Therefore, the problem of constructing permutations with low differential uniformity and high nonlinearity over $\mathbb{F}_{2^{2n}}$ is of significant importance in cryptography.

For $F(x) \in \mathbb{F}_{2^n}[x]$, $u, v \in \mathbb{F}_{2^n}$, the Walsh transform of $F(x)$ is defined as

$$\lambda_F(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(vF(x)+ux)}$$

and the Walsh spectrum of $F(x)$ is $\{\lambda_F(u,v) \mid u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^*\}$. The nonlinearity of $F(x)$, which is defined as the minimum distance of the components of $F(x)$ and all affine Boolean functions with n variables, is related to the Walsh transform through the following equality

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_{2^n}^*, u \in \mathbb{F}_{2^n}} |\lambda_F(u,v)|.$$

For odd n and $F(x) \in \mathbb{F}_{2^n}[x]$, $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [9]. The functions such the equality holds are called almost bent (AB) functions. The Walsh spectrum of AB function is $\{0, \pm 2^{\frac{n+1}{2}}\}$ [9]. Gold functions are AB functions [11,18]. For even n and $F(x) \in \mathbb{F}_{2^n}[x]$, the upper bound of the nonlinearity of $F(x)$ is still open. The best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$ [2].

The algebraic degree of $F(x) = \sum_{j=0}^{2^n-1} c_j x^j \in \mathbb{F}_{2^n}[x]$, which is denoted by $d^\circ(F)$, equals the maximum Hamming weight of the binary expansion of j with $c_j \neq 0$ [7]. In other words, $d^\circ(F) = \max_{j,c_j \neq 0}\{\omega_2(j)\}$. The functions with algebraic degree 2 is called quadratic functions. It is demonstrated that an S-box should has algebraic degree at least 4 to resist higher order differential attack [12].

A function $F(x) \in \mathbb{F}_{2^n}[x]$ is called differentially δ-uniform if for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, $F(x) + F(x+a) = b$ has at most δ solutions [18]. The functions with differentially 2-uniform are said to be almost perfect nonlinear (APN). AB functions are all APN functions [9]. APN functions provide the best resistance to differential attack. Then APN permutations over $\mathbb{F}_{2^{2n}}$ would be best choice for S-boxes in cryptography. However, only one APN permutation over $\mathbb{F}_{2^{2n}}$ has been found over $\mathbb{F}_{2^6}$ [10] and the existence of APN permutation over $\mathbb{F}_{2^{2n}}$ with $n \geq 4$ remains open.

Therefore, it is appropriate to choose differentially 4-uniform permutations as S-boxes of block ciphers in real applications. For example, the S-box of AES is affine equivalent to the inversion function over $\mathbb{F}_{2^8}$. The construction of differentially 4-uniform permutation with the highest nonlinearity over $\mathbb{F}_{2^{2m}}$ is also difficult. Only few functions are known as follows.

- Suppose k is odd, $n = 2k$, $\gcd(i, n) = 2$, then x^{2^i+1} and $x^{2^{2i}-2^i+1}$ are differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ [11,13].
- suppose n is even, then x^{2^n-2} is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ [3,18,14].
- Suppose k is odd, $n = 4k$, then $x^{2^{2k}+2^k+1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ [1].

We call $F_1(x)$ is EA-equivalent to $F_2(x)$, if there exist affine permutations $A_1(x), A_2(x) \in \mathbb{F}_{2^n}[x]$ and affine function $A_2(x) \in \mathbb{F}_{2^n}[x]$, such that

$$F_1(x) = A_1(F_2(A_2)(x)) + A_3(x).$$

Differential uniformity, nonlinearity and algebraic degree are invariant under EA-equivalence, but permutation is not. Then it is possible to get permutations by applying EA-equivalence to $F(x)$, where $F(x)$ is a function with low differential uniformity and high nonlinearity, see [15,16,19].

Recently, Carlet give a new method for constructing differentially 4-uniform permutations [8]. The idea is that instead of using the field structure of $\mathbb{F}_{2^n}$, to use that of $\mathbb{F}_{2^{n+1}}$. Suppose H is a linear hyperplane of $\mathbb{F}_{2^{n+1}}$ with dimension n, $\{\alpha_1, \cdots, \alpha_n\}$ is a basis of H over $\mathbb{F}_2$. $F(x)$ is a differentially δ-uniform polynomial

on $\mathbb{F}_{2^{n+1}}$ and $F(H) = H$, where $F(H) = \{F(\alpha) \mid \alpha \in H\}$. Identifying an vector of $(c_1, \cdots, c_n) \in \mathbb{F}_2^n$ as an element of $\alpha \in H$ through $\alpha = \sum_{i=1}^{n} c_i \alpha_i$, then

$$\begin{array}{ccc} \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ (c_1, \cdots, c_n) & \to & (d_1, \cdots, d_n) \end{array}$$

is a differentially δ-uniform over $\mathbb{F}_2^n$, where $\alpha = \sum_{i=1}^{n} c_i \alpha_i$, $F(\alpha) = \sum_{i=1}^{n} d_i \alpha_i$. Carlet illustrate his idea with a construction as follows.

Theorem 1. *[8] Suppose $c = n \mod 2$, $\alpha \in \mathbb{F}_{2^{n+1}}$ and $\mathrm{Tr}(\alpha) = 1$. Identifying an vector of $\mathbb{F}_{2^n}$ as an element of $H = \{u \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}(u) = 0\}$, then the restriction of $x + \frac{1}{x+\alpha+c} + (\frac{1}{x+\alpha+c})^2$ to H is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ and its algebraic degree is $n - 1$.*

The bounds of the nonlinearity of the permutations in Theorem 1 shows that these permutations do not obtain the highest nonlinearity [8]. In the present paper, we show that differentially 4 uniform permutation over $\mathbb{F}_{2^n}$ with n even can be constructed from quadratic APN permutations over $\mathbb{F}_{2^{n+1}}$ by using the similar idea. We also show that permutations constructed posses the best known nonlinearity.

The paper is organized as follows. In Sect. 2, a general construction is given and the nonlinearity is also investigated. In Sect. 3, several constructions are given by using Gold functions. One of our constructions and its compositional inverse have both algebraic degree $\frac{n+2}{2}$. The conclusion is given in Sect. 4.

2 General construction

First, for a function $F(x) \in \mathbb{F}_{2^m}[x]$ and $H \subseteq \mathbb{F}_{2^m}$, $F(H)$ means $\{F(h) \mid h \in H\}$, $a + H$ means $\{a + h \mid h \in H\}$, where $a \in \mathbb{F}_{2^m}$.

Throughout this paper, n is an even integer. If $F(x) \in \mathbb{F}_{2^{n+1}}[x]$ is a quadratic APN permutation with $F(0) = 0$, then it is easy to see that for any $u \in \mathbb{F}_{2^{n+1}}^*$,

$$L_u(x) = F(x) + F(x + u) + F(u)$$

is a linear polynomial with kernel $\{0, u\}$. Thus the image of $L_u(x)$ is a linear subspace of $\mathbb{F}_{2^{n+1}}$ with dimension n. Identify a vector of $\mathbb{F}_2^n$ as an element of the image of $L_u(x)$. Then we have the following result.

Theorem 2. *Let n be even, $F(x) \in \mathbb{F}_{2^{n+1}}[x]$ be a quadratic APN permutation with $F(0) = 0$, $L_u(x) = F(x) + F(x + u) + F(u)$, $H_u = \{L_u(a) \mid a \in \mathbb{F}_{2^{n+1}}\}$. Identify the input x with an element of H_u. Let $F_u(x)$ be the restriction of*

$$L_u(F^{-1}(x))$$

to H_u. Then $F_u(x)$ is a differentially 4-uniform permutation over $\mathbb{F}_2^n$, where $F^{-1}(x)$ is the compositional inverse of $F(x)$.

Proof. Notice that $F_u(H_u) = L_u(F^{-1}(H_u)) \subseteq H_u$, we need only to show that $L_u(F^{-1}(x))$ is injective on H_u. Assume that there exist $x_1 \neq x_2 \in H_u$, such that $L_u(F^{-1}(x_1)) = L_u(F^{-1}(x_2))$. Then

$$F^{-1}(x_1) = F^{-1}(x_2) + u,$$

since $\ker(L_u) = \{0, u\}$. Compose both sides of the above equality with $F(x)$, then we have

$$x_1 = F(F^{-1}(x_2) + u),$$

which is equivalent to

$$x_1 + x_2 = F(F^{-1}(x_2) + u) + F(F^{-1}(x_2)).$$

This means $x_1 + x_2 \in F(u) + H_u$. On the other hand, we have $x_1 + x_2 \in H_u$ since $x_1, x_2 \in H_u$ and H_u is a linear subspace of $\mathbb{F}_{2^{n+1}}$. Hence $x_1 + x_2 \in H_u \cap (F(u) + H_u)$, this contradicts to $H_u \cap (F(u) + H_u) = \varnothing$ for $F(x)$ is a permutation.

The differential uniformity of $L_u(F^{-1}(x))$ is easy to compute. Since $|\ker(L_u)| = 2$ and $F(x)$ is an APN permutation, then $F^{-1}(x)$ is also APN and $L_u(F^{-1}(x))$ is differentially 4-uniform. □

Remark 1. If we replace $L_u(x)$ in Theorem 2 with any other linear polynomial $L(x) \in \mathbb{F}_{2^{n+1}}[x]$ with kernel $\{0, u\}$ and image H_u, Theorem 2 also holds. Notice that there are $\prod_{i=0}^{n-1}(2^n - 2^i)$ different linear polynomials with kernel $\{0, u\}$ and image H_u, which is also the amount of different linear permutations over H_u. Therefore, there exists a linear permutation M over H_u such that $L(x) = M(L_u(x))$. Then the restriction of $L(F^{-1}(x))$ to H_u equals the restriction of $M(L_u(F^{-1}(x)))$ to H_u and EA-equivalent to $F_u(x)$. Thus, it is enough to choose $L_u(x) = F(x) + F(x + u) + F(u)$.

Notice that for a quadratic function, it is APN if and only if it is AB [7]. The we can characterize the nonlinearity of the permutations constructed in Theorem 2 as follows.

Theorem 3. *Let $F_u(x)$ be a function constructed as Theorem 2. Then $\mathcal{NL}(F_u) = 2^{n-1} - 2^{\frac{n}{2}}$, which is the best known nonlinearity over $\mathbb{F}_2^n$.*

Proof. Denote the set of all linear subspaces of $\mathbb{F}_{2^{n+1}}$ with dimension n by LS_n. It is hold that $|LS_n| = \frac{\prod_{i=0}^{n-1}(2^{n+1} - 2^i)}{\prod_{i=0}^{n-1}(2^n - 2^i)} = 2^{n+1} - 1$. Then we have

$$LS_n = \{\{x \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}(\alpha x) = 0\} \mid \alpha \in \mathbb{F}_{2^{n+1}}\}.$$

This means for any $H \in LS_n$, there exists $\alpha \in \mathbb{F}_{2^n}^*$, such that $H = \{x \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}_{n+1}(\alpha x) = 0\}$.

Suppose $\alpha_u \in \mathbb{F}_{2^{n+1}}^*$ such that $H_u = \{L_u(a) \mid a \in \mathbb{F}_{2^{n+1}}\} = \{k \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}_{n+1}(\alpha_u k) = 0\}$. Remember that $F_u(x)$ is the restriction of $L_u(F^{-1}(x))$ to H_u, then

$$\mathcal{NL}(F_u) = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^{n+1}}, b\in\mathbb{F}_{2^{n+1}}\setminus\{0,\alpha_u\}} |\lambda_{F_u}(a,b)|,$$

where $\lambda_{F_u}(a,b) = \sum\limits_{x\in H_u} (-1)^{\mathrm{Tr}(bL_u(F^{-1}(x))+ax)}$. For $a, b \in \mathbb{F}_{2^{n+1}} \setminus \{0, \alpha_u\}$, we have

$$\begin{aligned}
\lambda_{F_u}(a,b) &= \sum_{x\in H_u} (-1)^{\mathrm{Tr}(bL_u(F^{-1}(x))+ax)} \\
&= \sum_{x\in H_u} (-1)^{\mathrm{Tr}(L_u^*(b)F^{-1}(x)+ax)} \\
&= \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^{n+1}}} (-1)^{\mathrm{Tr}(L_u^*(b)F^{-1}(x)+ax)} \\
&\quad + \sum_{x\in\mathbb{F}_{2^{n+1}}} (-1)^{\mathrm{Tr}(L_u^*(b)F^{-1}(x)+(a+\alpha_u)x)}\Big) \\
&= \frac{1}{2}\Big(\sum_{x\in\mathbb{F}_{2^{n+1}}} (-1)^{\mathrm{Tr}(L_u^*(b)x+aF(x))} \\
&\quad + \sum_{x\in\mathbb{F}_{2^{n+1}}} (-1)^{\mathrm{Tr}(L_u^*(b)x+(a+\alpha_u)F(x))}\Big) \\
&= \frac{1}{2}(\lambda_F(L_u^*(b),a) + \lambda_F(L_u^*(b),a+\alpha_u)),
\end{aligned}$$

where L_u^* is the adjoint operator of L_u. Notice that

$$\lambda_{F_u}(0,b) = \lambda_{F_u}(\alpha_u,b) = 0$$

for any $b \in \mathbb{F}_{2^{n+1}} \setminus \{0, \alpha_u\}$, since $F_u(x)$ is a permutation over H_u. Then we have

$$\begin{aligned}
&\max_{a\in\mathbb{F}_{2^{n+1}}, b\in\mathbb{F}_{2^{n+1}}\setminus\{0,\alpha_u\}} |\lambda_{F_u}(a,b)| \\
=& \max_{a,b\in\mathbb{F}_{2^{n+1}}\setminus\{0,\alpha_u\}} |\lambda_{F_u}(a,b)| \\
=& \max_{a,b\in\mathbb{F}_{2^{n+1}}\setminus\{0,\alpha_u\}} \frac{1}{2}|\lambda_F(L_u^*(b),a) + \lambda_F(L_u^*(b),a+\alpha_u)| \\
\le& \max_{a,b\in\mathbb{F}_{2^{n+1}}\setminus\{0,\alpha_u\}} \frac{1}{2}(|\lambda_F(L_u^*(b),a)| + |\lambda_F(L_u^*(b),a+\alpha_u)|) \\
\le& \lambda,
\end{aligned}$$

where $\lambda = \max\{\lambda_F(b,a) \mid b \in \mathbb{F}_{2^{n+1}}, a \in \mathbb{F}_{2^{n+1}}^*\} = 2^{\frac{n+2}{2}}$. Since $F(x)$ is a quadratic AB permutation over $\mathbb{F}_{2^{n+1}}$ and its Walsh spectrum is $\{0, \pm 2^{\frac{n+2}{2}}\}$. Therefore,

$$\mathcal{NL}_{F_u} \ge 2^{n-1} - 2^{\frac{n}{2}}.$$

We claim that the equality holds. Otherwise, as a permutation over $\mathbb{F}_2^n$, the Walsh spectrum of $F_u(x)$ is $\{0, \pm 2^{\frac{n}{2}}\}$. According to Parseval's equality, for any $b \in \mathbb{F}_2^{n*}$, it holds $\sum_{a\in\mathbb{F}_2^n}(\sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F_u(x)+a\cdot x})^2 = 2^{2n}$. Therefore, for any $a \in \mathbb{F}_2^n$, it must holds $\lambda_{F_u}(a,b) = \pm 2^{\frac{n}{2}}$. This contradicts with $\lambda_{F_u}(0,b) = 0$, since $F_u(x)$ is a permutation over $\mathbb{F}_2^n$. Therefore, $\mathcal{NL}(F_u) = 2^{n-1} - 2^{\frac{n}{2}}$. □

3 Constructions from Gold functions

It is well-known that x^{2^i+1} is an AB permutation over $\mathbb{F}_{2^{n+1}}$ when is n even and $\gcd(i, n+1) = 1$. We denote its compositional inverse by $x^{\frac{1}{2^i+1}}$. In this section, we give some constructions of differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_2^n$ by using Gold functions. It is easy to see that for Gold functions and $u \in \mathbb{F}^*_{2^{n+1}}$,

$$L_u(x) = x^{2^i+1} + (x+u)^{2^i+1} + u^{2^i+1} = ux^{2^i} + u^{2^i}x.$$

Then according to Theorem 2 and Theorem 3, we have the following result.

Theorem 4. *Suppose n is even, $\gcd(i, n+1) = 1$, $u \in \mathbb{F}^*_{2^{n+1}}$. Identify a vector of $\mathbb{F}_2^n$ as an element of the n-dimension linear subspace $H_u = \{ua^{2^i} + u^{2^i}a \mid a \in \mathbb{F}_{2^{n+1}}\}$. Let $F_u(x)$ be the restriction of $ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}}$ to H_u, where $x^{\frac{1}{2^i+1}}$ is the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^{n+1}}$. Then the following statements hold.*

1. *$F_u(x)$ is a differentially 4-uniform permutation over $\mathbb{F}_2^n$.*
2. *The nonlinearity of $F_u(x)$ is $2^{n-1} - 2^{\frac{n}{2}}$.*

Next, we will investigate the algebraic degree of $F_u(x)$ and $F_u^{-1}(x)$. The following lemmas are useful.

Lemma 1. *[18] Suppose $\gcd(i, n+1) = 1$, then the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^{n+1}}$ is x^d, where $d = \frac{2^{i(n+2)}-1}{2^{2i}-1} = \sum_{k=0}^{\frac{n}{2}} 2^{2ik}$ mod $(2^{n+1}-1)$. Its algebraic degree is $\frac{n+2}{2}$.*

The 2-weight of an integer $t \in \mathbb{N}$ means the number of nonzero terms in the binary expansion of t, denoted by $\omega_2(t)$. Let us recall the following Lemma.

Lemma 2. *[8] Let $n \le N$, $F' \in \mathbb{F}_{2^N}[x]$, let F be the restriction of F' to an n-dimensional affine space E, and k be a positive integer. Then F has algebraic degree at most k if and only if for every integer i with $\omega_2(i)$ at most $n-k-1$, we have $\sum_{x\in E} x^i F(x) = 0$.*

The following lemma is also needed in the proof of the Proposition 1.

Lemma 3. *Let i be a positive integer,* $\gcd(i, n+1) = 1$, *and* $d(2^i+1) = 1 \bmod (2^{n+1}-1)$. *Then there do not exist* $0 \le k_1, k_2 \le n$, *such that* $d + 2^{k_1} = 2^i d + 2^{k_2} \bmod (2^{n+1}-1)$.

Proof. Assume that there are $0 \le k_1, k_2 \le n$, such that $d + 2^{k_1} = 2^i d + 2^{k_2} \bmod (2^{n+1}-1)$. Multiplying both sides by $2^i + 1$, one obtain

$$1 + 2^{i+k_1} + 2^{k_1} = 2^i + 2^{i+k_2} + 2^{k_2} \bmod (2^{n+1}-1). \tag{1}$$

Let $c_1 = 1 + 2^{i+k_1} + 2^{k_1} \bmod (2^{n+1}-1)$, $c_2 = 2^i + 2^{i+k_2} + 2^{k_2} \bmod (2^{n+1}-1)$. Then $1 \le \omega_2(c_1) = \omega_2(c_2) \le 3$. There are three cases:

Case 1. $\omega_2(c_1) = \omega_2(c_2) = 1$. Notice that $k_1 \ne i + k_1 \bmod (n+1)$, then $\omega_2(c_1) = 1$ if and only if $k_1 = 0, (i+k_1) \bmod n+1 = 1$, or $(i+k_1) \bmod n+1 = 0, k_1 = 1$, from which we get $c_1 = 4$. By the same reasoning, $\omega_2(c_2) = 1$ if and only if $(i+k_2) \bmod n+1 = i, k_2 = i+1$, or $(i+k_2) \bmod n+1 = i+1, k_2 = i$, from which we get $c_2 = 2^{i+2} \bmod (2^{n+1}-1)$. Then (1) is equivalent to

$$4 = 2^i 4 \bmod (2^{n+1}-1).$$

Therefore, $i = 0 \bmod (n+1)$, which is a contradiction because $\gcd(i, n+1) = 1$.

Case 2. $\omega_2(c_1) = \omega_2(c_2) = 2$. $\omega_2(c_1) = 2$ if and only if $k_1 = 0, i \ne 1$ or $i + k_1 \bmod n+1 = 0, i \ne n$, from which we get $c_1 = 2^i + 2$ or $c_1 = 2^{n+1-i} + 2$. Notice that $2^{i+k_1} + 2^{k_1} \ne 2^{i+1} \bmod (2^{n+1}-1)$, then $\omega_2(c_2) = 2$ if and only if $i = k_2, i \ne 1$, from which we get $c_2 = 2^{2i} + 2^{i+1}$. Therefore (1) is equivalent to

$$2^{n+1-i} + 2 = 2^{2i} + 2^{i+1} \bmod (2^{n+1}-1),$$

since $c_2 = 2^i(2^i+2) \ne 2^i + 2 \bmod (2^{n+1}-1)$. Thus $2i = 1 \bmod (n+1)$ and $i + 1 = n + 1 - i \bmod (n+1)$, which are equivalent to $i = \frac{n}{2} + 1$ and $i = \frac{n}{2}$ respectively. This is a contradiction.

Case 3. $\omega_2(c_1) = \omega_2(c_2) = 3$. Then it must have $k_1 \ne 0$ and $i + k_2 = 0 \bmod (n+1)$. Therefore (1) is equivalent to

$$1 + 2^{i+k_1} + 2^{k_1} = 2^i + 2^{n+1-i} + 1 \bmod (2^{n+1}-1).$$

Hence $k_1 = i$, and $n+1-i = k_1 + i \bmod (n+1)$, which is equivalent to $n+1 = 3i$. This is a contradiction since $\gcd(i, n+1) = 1$. □

Proposition 1. *Suppose that $n \ge 4$ is even, $F_u(x)$ is a function constructed in Theorem 4. Then $d^\circ(F_u) = \frac{n+2}{2}$.*

Proof. Without loss of generality, we prove the case of $u = 1$. Suppose $F_1(x)$ is the restriction of $x^d + x^{2^i d}$ to

$$H_1 = \{x + x^{2^i} \mid x \in \mathbb{F}_{2^{n+1}}\} = \{x \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}(x) = 0\},$$

where $d(2^i+1) = 1 \bmod (2^{n+1}-1)$. Then according to Lemma 1,we have $d^\circ(F_1(x)) \le \frac{n+2}{2}$. In the next, we show the equality holds.

Since $\omega_2(d) = \frac{n+2}{2} < n$, we can choose an integer k with $0 \le k \le n$, such that $\omega_2(d+2^k) = \omega_2(d)+1$. Notice that for any x^l, where $1 \le l \le 2^{n+1}-2$, we have

$$\sum_{x\in\mathbb{F}_{2^{n+1}}} x^l = \sum_{j=0}^{2^{n+1}-2} g^{jl} = \frac{1+g^{l(2^{n+1}-1)}}{1+g^l} = 0,$$

where g is a primitive element of $\mathbb{F}_{2^{n+1}}$.

Hence by the choice of k, we have

$$\sum_{x\in\mathbb{F}_{2^{n+1}}} x^{2^{n+1}-1-(d+2^k)}(x^d + x^{2^i d}) = 0.$$

By Lemma 3, there does not exist any j with $0 \le j \le n$, such that

$$(2^i-1)d + 2^j - 2^k = 0 \bmod (2^{n+1}-1).$$

Therefore, we have

$$\begin{aligned}
&\sum_{x\in H_1} x^{2^{n+1}-1-(d+2^k)}(x^d + x^{2^i d}) \\
&= \sum_{x\in\mathbb{F}_{2^{n+1}}} x^{2^{n+1}-1-(d+2^k)}(x^d + x^{2^i d})(\mathrm{Tr}(x)+1) \\
&= \sum_{x\in\mathbb{F}_{2^{n+1}}} x^{2^{n+1}-1-(d+2^k)}(x^d + x^{2^i d})\mathrm{Tr}(x) \\
&= \sum_{x\in\mathbb{F}_{2^{n+1}}} x^{2^{n+1}-1} + \sum_{j=0, j\neq k}^{n} \sum_{x\in\mathbb{F}_{2^{n+1}}} x^{2^j-2^k} + \sum_{j=0}^{n} \sum_{x\in\mathbb{F}_{2^{n+1}}} x^{(2^i-1)d-2^k+2^j} \\
&= 1.
\end{aligned}$$

Thus by Lemma 2,

$$d^\circ(F) \ge n - (\frac{n}{2} - 1) = \frac{n+2}{2},$$

since $\omega_2(2^{n+1}-1-(d+2^k)) = n+1-(\omega_2(d)+1) = \frac{n}{2}-1$. Then the proof is completed. □

Concerning the algebraic degree of the compositional inverse of the function constructed in Theorem 4, we have the following results.

Proposition 2. *Suppose $n \ge 4$ is even, $F_u(x)$ is the function constructed in Theorem 4, then $d^\circ(F_u^{-1}(x)) \le 3$.*

Proof. Without loss of generality, we prove the case of $u = 1$. Suppose $F_1(x)$ is the restriction of $x^{\frac{1}{2^i+1}} + x^{\frac{2^i}{2^i+1}}$ to $H_1 = \{x \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}(x) = 0\}$. We have to determine the roots of

$$x^{\frac{1}{2^i+1}} + x^{\frac{2^i}{2^i+1}} = y. \tag{2}$$

Since $\gcd(i, n+1) = 1$, $\{i \cdot k \bmod (n+1) \mid 1 \le k \le n\} = \{k \mid 1 \le k \le n\}$. Let $L(x) = \sum_{j=0}^{\frac{n-2}{2}} x^{2^{(2j+1)i}}$, then $\forall x \in \mathbb{F}_{2^{n+1}}$,

$$L(x + x^{2^i}) = \sum_{j=0}^{\frac{n-2}{2}} (x^{2^{(2j+1)i}} + x^{2^{(2j+2)i}}) = \sum_{j=1}^{n} x^{2^{ji}} = \mathrm{Tr}(x) + x.$$

This means that $L(b)$ satisfies $x + x^{2^i} = b$ when $\mathrm{Tr}(b) = 0$. Since $\ker(x + x^{2^i}) = \{0, 1\}$, for every $y \in H_1$, two roots of equation (2) are $L(y)^{2^i+1}$ and $(L(y)+1)^{2^i+1}$. Thus the compositional inverse of $F_1(x)$ is

$$F_1^{-1}(x) = \begin{cases} L(x)^{2^i+1} & \mathrm{Tr}(L(x)^{2^i+1}) = 0, \\ (L(x)+1)^{2^i+1} & \mathrm{Tr}(L(x)^{2^i+1}) = 1, \end{cases}$$

which equals the restriction of

$$\begin{aligned} &L(x)^{2^i+1}\mathrm{Tr}(L(x)^{2^i+1} + 1) + (L(x)+1)^{2^i+1}\mathrm{Tr}(L(x)^{2^i+1}) \\ &= L(x)^{2^i+1} + \mathrm{Tr}(L(x)^{2^i+1}) + (L(x)^{2^i} + L(x))\mathrm{Tr}(L(x)^{2^i+1}) \end{aligned}$$

to H_1. Therefore, $d^\circ(F_1^{-1}) \le 3$. □

The above result shows that the compositional inverse of the functions constructed in Theorem 4 do not have a high algebraic degree to resist the higher order differential attack. In order to improve this, we give its modification as follows.

Theorem 5. *Suppose n is even, $\gcd(i, n+1) = 1$, $u \in \mathbb{F}_{2^{n+1}}^*$, $H_u = \{ux^{2^i} + u^{2^i}x \mid x \in \mathbb{F}_{2^{n+1}}\}$. Let $F_u'(x)$ be the restriction of $ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}} + x$ to H_u. Then the following statements hold.*

1. *$F_u'(x)$ is a differentially 4-uniform permutation over $\mathbb{F}_2^n$;*
2. *The nonlinearity of $F_u'(x)$ equals $2^{n-1} - 2^{\frac{n}{2}}$;*
3. *$d^\circ(F_u') = d^\circ(F_u'^{-1}) = \frac{n+2}{2}$.*

Proof. Let $F_u(x)$ be the function constructed in Theorem 4. Then $F_u(x)$ and $F_u'(x)$ are EA-equivalent since $F_u'(x) = F_u(x) + x$. Therefore, $F_u'(x)$ is differentially 4-uniform with nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$ and algebraic degree $\frac{n+2}{2}$. Thus we need only to show that $F_u'(x)$ is a permutation, and $d^\circ(F_u'^{-1}) = \frac{n+2}{2}$.

Let $F_1(x) = ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}}$, $F(x) = ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}} + x$. It has been proved that $F_1(H_u) = H_u$. Since H_u is a linear subspace of $\mathbb{F}_{2^{n+1}}$, then $F(H_u) \subseteq H_u$. On the other hand,

$$F(x) = ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}} + x = (x^{\frac{1}{2^i+1}} + u)^{2^i+1} + u^{2^i+1} \tag{3}$$

is a permutation over $\mathbb{F}_{2^{n+1}}$, then $|F(H_u)| = |H_u|$, which shows that $F(x)$ is a permutation on H_u.

By (3), the compositional inverse of $F_u^{'}(x)$ equals the restriction of

$$\begin{aligned}&((x+u^{2^i+1})^{\frac{1}{2^i+1}}+u)^{2^i+1}\\&=x+u(x+u^{2^i+1})^{\frac{2^i}{2^i+1}}+u^{2^i}(x+u^{2^i+1})^{\frac{1}{2^i+1}}\end{aligned}$$

to H_u. Therefore, its algebraic degree is also $\frac{n+2}{2}$ by applying the same reasoning as Proposition 1. □

It is proven that for a nonzero linear polynomial $L(x) \in \mathbb{F}_{2^n}[x]$, $x^{2^i+1}+L(x)$ is a permutation over $\mathbb{F}_{2^n}$ if and only if n is odd and $L(x) = ux^{2^i}+u^{2^i}x$ for some $u \in \mathbb{F}_{2^n}^*$ [15]. Then there does not exist other linear polynomials are helpful for constructing differentially 4-uniform permutations as Theorem 5 does.

At the end of this subsection, we show that differentially 4-uniform permutations over $\mathbb{F}_2^n$ can also be constructed from APN permutations over $\mathbb{F}_{2^{n+1}}$ with algebraic degree larger than 2. Let us recall the following result:

Lemma 4. *[5] Let $m \geq 9$ be odd and divisible by 3, $\gcd(i,m)=1$, $s=i \bmod 3$. Then*

$$(x^{\frac{1}{2^i+1}}+\mathrm{Tr}_{m/3}(x+x^{2^{2s}}))^{-1}$$

is an AB permutation over $\mathbb{F}_{2^m}$, which is EA-inequivalent to Gold functions and their inverse. Its algebraic degree is 4.

Lemma 5. *Let $m=n+1$ be odd and divisible by 3, $\gcd(i,m)=1$, $s=i \bmod 3$, $F(x)=x^{\frac{1}{2^i+1}}+\mathrm{Tr}_{m/3}(x+x^{2^{2s}})$. Then $\mathrm{Tr}(F^{-1}(x)+F^{-1}(x+1))=1$, where $F^{-1}(x)$ is the compositional inverse of $F(x)$.*

Proof. First, we notice that in order to prove

$$\mathrm{Tr}(F^{-1}(a)+F^{-1}(a+1))=1$$

for all $a \in \mathbb{F}_{2^{n+1}}$, we only need to prove the above equality holds for all $a \in \{\alpha \in \mathbb{F}_{2^{n+1}} \mid \mathrm{Tr}(\alpha)=1\} = \mathrm{Tr}^{(1)}$. This is because if $\mathrm{Tr}(a)=0$, let $b=a+1$, then we have $\mathrm{Tr}(b)=1$ and

$$\mathrm{Tr}(F^{-1}(a)+F^{-1}(a+1))=\mathrm{Tr}(F^{-1}(b+1)+F^{-1}(b)).$$

It is proven in [5] that

$$\begin{aligned}F^{-1}(x)=&x^{2^i+1}+(\mathrm{Tr}_{m/3}(x^{2^i+1}))^6+(\mathrm{Tr}_{m/3}(x^{2^i+1}))^5\\&+(\mathrm{Tr}_{m/3}(x^{2^i+1}))^3+(\mathrm{Tr}_{m/3}(x^{2^i+1}))^4\\&+x^{2^i}\mathrm{Tr}(x)\mathrm{Tr}_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+x\mathrm{Tr}(x)\mathrm{Tr}_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\&+x^{2^i}\mathrm{Tr}_{m/3}(x^{2^(2^i+1)}+x^{2^{2s+1}(2^i+1)})+x\mathrm{Tr}_{m/3}(x^{2(2^i+1)}+x^{2^{s+1}(2^i+1)})\\&+\mathrm{Tr}(x)\mathrm{Tr}_{m/3}(x^{2^i+1}+x^{4(2^i+1)}).\end{aligned}$$

Notice that $\mathrm{Tr}(\mathrm{Tr}_{m/3}(x)^3)=\mathrm{Tr}(\mathrm{Tr}_{m/3}(x)^5)$, then for $a \in \mathrm{Tr}^{(1)}$, we have

$$\begin{aligned}\mathrm{Tr}(F^{-1}(a))=\mathrm{Tr}(&\mathrm{Tr}_{m/3}(a^{2^i+1})^{2^s+1}+a^{2^i}\mathrm{Tr}_{m/3}(a^{2^i+1}+a^{2^s(2^i+1)})\\&+a^{2^i}\mathrm{Tr}_{m/3}(a^{2(2^i+1)}+a^{2^{s+1}(2^i+1)})),\end{aligned}$$

and

$$\mathrm{Tr}(F^{-1}(a+1)) = \mathrm{Tr}(\mathrm{Tr}_{m/3}((a+1)^{2^i+1})^{2^s+1} + (a^{2^i}+1)\mathrm{Tr}_{m/3}((a+1)^{2(2^i+1)} + (a+1)^{2^{s+1}(2^i+1)})).$$

By a long but easy computation, we have

$$\begin{aligned}\mathrm{Tr}(F^{-1}(a)+F^{-1}(a+1)) &= 1+\mathrm{Tr}(\mathrm{Tr}_{m/3}(a^{2^i+1})^{2^s}\mathrm{Tr}_{m/3}(a^{2^s}+a^{2^{2s}}) \\ &\quad +\mathrm{Tr}_{m/3}(a)^{2^{2s}+1}+\mathrm{Tr}_{m/3}(a)^{2^{s+1}} \\ &\quad +a^{2^i}\mathrm{Tr}_{m/3}(a^{2^i+1}+a^{2^s(2^i+1)})+a^{2^i}\mathrm{Tr}_{m/3}(a^2+a^{2^{2s+1}})) \\ &= \mathrm{Tr}_3(\mathrm{Tr}_{m/3}(a)^{2^{2s}+1}+\mathrm{Tr}_{m/3}(a)^{2^s+2}+\mathrm{Tr}_{m/3}(a)^{2^s+2^{2s+1}}) \\ &= \mathrm{Tr}_3(\mathrm{Tr}_{m/3}(a)) = 1,\end{aligned}$$

since

$$\{2^{2s}+1 \bmod 7, 2^s+2 \bmod 7, 2^s+2^{2s+1} \bmod 7\} = \begin{cases}\{5,4,3\}, & s=1;\\ \{3,6,1\}, & s=2.\end{cases}$$

Then we complete the proof. □

Theorem 6. *Let $m = n+1$ be odd and divisible by 3, $\gcd(i,m)=1$, $s = i \bmod 3$. $F(x) = x^{\frac{1}{2^i+1}} + \mathrm{Tr}_{m/3}(x+x^{2^{2s}})$ is an AB permutation over $\mathbb{F}_{2^m}$. Identify a vector of $\mathbb{F}_{2^n}$ as an element of the linear subspace $\mathrm{Tr}^{(0)} = \{a \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_m(a) = 0\}$. Let $F'(x)$ be the restriction of $F(x)+F(x)^{2^i}$ to $\mathrm{Tr}^{(0)}$. Then the following statements hold.*

1. *$F'(x)$ is a differentially 4-uniform permutation over $\mathbb{F}_2^n$;*
2. *Its nonlinearity is $2^{n-1}-2^{\frac{n}{2}}$ and its algebraic degree is $\frac{n+2}{2}$;*
3. *$d^\circ(F'^{-1}) \le 7$.*

Proof. As in the proof of Theorem 5, we have $F'(x)$ is EA-equivalent to the functions constructed in Theorem 4. Thus we need only to prove $F'(x)$ is a permutation over $\mathbb{F}_2^n$ and $d^\circ(F'^{-1}) \le 7$.

First, $F'(\mathrm{Tr}^{(0)}) \subseteq \mathrm{Tr}^{(0)}$. Then we need only to show that $F'(x)$ is injective on $\mathrm{Tr}^{(0)}$. Assume that there exist $x_1 \neq x_2 \in \mathrm{Tr}^{(0)}$, such that $F(x_1)+F(x_1)^{2^i} = F(x_2)+F(x_2)^{2^i}$. Since $F(x)$ is a permutation and $y+y^{2^i}=0$ has only two solutions $\{0,1\}$, it must have

$$x_1^{\frac{1}{2^i+1}} + \mathrm{Tr}_{m/3}(x_1+x_1^{2^{2s}}) = x_2^{\frac{1}{2^i+1}} + \mathrm{Tr}_{m/3}(x_2+x_2^{2^{2s}})+1.$$

By applying F^{-1} to two sides of the above equation, we have

$$x_1 = F^{-1}(F(x_2)+1).$$

Therefore,

$$x_1+x_2 = F^{-1}(F(x_2)+1)+F^{-1}(F(x_2)).$$

By Lemma 5, we get

$$\mathrm{Tr}(x_1+x_2) = \mathrm{Tr}(F^{-1}(F(x_2)+1)+F^{-1}(F(x_2))) = 1.$$

However, since $x_1, x_2 \in \mathrm{Tr}^{(0)}$, $x_1 + x_2 \in \mathrm{Tr}^{(0)}$, that is $\mathrm{Tr}(x_1 + x_2) = 0$. Hence we obtain a contradiction. Thus $F^{'}(x)$ is a permutation on $\mathrm{Tr}^{(0)}$.

Let $L(x) = \sum_{j=0}^{\frac{m-3}{2}} x^{2^{(2j+1)i}}$. By Lemma 5, by a similar argument as Proposition 2, we have

$$F^{'-1}(x) = \begin{cases} F^{-1}(L(x)) & \mathrm{Tr}(F^{-1}(L(x))) = 0, \\ F^{-1}(L(x)+1) & \mathrm{Tr}(F^{-1}(L(x))) = 1, \end{cases}$$

which is equivalent to the restriction of

$$\begin{aligned} & F^{-1}(L(x))(\mathrm{Tr}(F^{-1}(L(x))) + 1) + F^{-1}(L(x)+1)\mathrm{Tr}(F^{-1}(L(x))) \\ = & \mathrm{Tr}(F^{-1}(L(x)))(F^{-1}(L(x)) + F^{-1}(L(x)+1)) + F^{-1}(L(x)) \end{aligned}$$

to $\mathrm{Tr}^{(0)}$. By Lemma 4, $d^{\circ}(F^{-1}) = 4$, algebraic degree of $F^{-1}(L(x)) + F^{-1}(L(x) + 1)$ is less than or equal to 3. Hence, $d^{\circ}(F^{'-1}) \leq 7$. □

Remark 2. With the help of Magma, we have $d^{\circ}(F^{'-1}) = 5$ when $m = 9, 15$. Then it is reasonable to believe that $d^{\circ}(F^{'-1}) = 5$ is true for every odd m divisible by 3. The inverse of the permutations constructed in Theorem 5 and Theorem 6 are EA-inequivalent when $n \geq 14$, since their algebraic degree are not equal.

When $n = 8$, we have $d^{\circ}(F_u^{'-1}) = 5$, where $F_u^{'}(x)$ is the permutation constructed in Theorem 5. Define

$$RD_F(a, 4) = |\{b \in \mathbb{F}_{2^n} \mid F(x) + F(x + a) = b \text{ has 4 roots}\}|.$$

Then it is easy to verify that $RD_F(4) = \{RD_F(a, 4) \mid a \in \mathbb{F}_{2^n}^*\}$ is invariant under EA-equivalence. Let $i = 1$, with the help of Magma, we have

$$RD_{F_u^{'-1}}(4) = \{13, 14, 15, 16, 17, 18, 19, 20, 23\}$$

and

$$RD_{F^{'-1}}(4) = \{11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 28\}.$$

Then $F_u^{'-1}(x)$ and $F^{'-1}(x)$ are EA-inequivalent on $\mathbb{F}_{2^8}$ either.

4 Conclusion

In this paper, we give a method for constructing differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_{2^{2m}}$ from quadratic AB permutations over $\mathbb{F}_{2^{2m+1}}$. We give also some constructions by using the Gold functions. Besides inverse functions, it is first time that differentially 4-uniform permutations over $\mathbb{F}_{2^{2^n}}$ with the highest nonlinearity are constructed. Besides Gold functions, there are other AB permutations over $\mathbb{F}_{2^{2m+1}}$ [6]. Then one can obtain other differentially 4-uniform permutations by applying the same method in the paper. It is our hope that the results presented in this paper will motivate new progress in related areas.

References

1. Bracken C., Leander G.: A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications. 16(4), 231-242 (2010).
2. Dobbertin H.: One-to-one highly nonlinear power functions on $GF(2^n)$, Appl. Algebra Engrg. Comm. Comput. 9(2), 139-152 (1998).
3. Beth T., Ding C.: On almost perfect nonlinear permutations. In: Advances in Cryptology -EUROCRYPT'93. LNCS, Vol. 765, pp. 65-76. Springer-Verlag, New York (1994).
4. Biham E., Shamir A.: Defferential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3-72 (1991).
5. Budaghyan L.: The simplest method for constructing APN polynomials EA-inequivalent to power functions. WAIFI 2007, LNCS 4547, 177-188, 2007.
6. Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. on Inform. Theory IT-54(9), 4218-4229 (2008).
7. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations sutiable for DES-like cryptosystems. Des. Codes Cryptogr. 15(2), 125-156 (1998).
8. Carlet C.: On Known and New Differentially Uniform Functions. ACISP 2011: 1-15.
9. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology -EUROCRYPT'94. LNCS, vol. 950, pp. 356-365. Springer-Verlag, New York (1995).
10. Dillon J.F.: APN polynomials: An Update. In: proceedings of The 9th Conference on Finite Fields and Applications FQ9 (to be published), Dublin, Ireland (2009).
11. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, 14, 154-156 (1968).
12. Knudsen L.: Truncated and higher order differentials. In: Preneel, B.(ed.) FSE 1994. LNCS, vol. 1008, pp. 196-211. Springer, Heidelberg (1995).
13. Kasami T.: The weight enumerators for several classes of subcodes of the second order binary ReedCMuller codes, Inform. Control 18, 369-394 (1971).
14. Lachaud G., Wolfmann J.: The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. IEEE Trans. Inform. Theory 36(3), 686-692 (1990).
15. Li Y., Wang M.: On EA-equivalence of certain permutations to power mappings. Des. Codes Cryptogr. 58(3), 259-269 (2011).
16. Li Y., Wang M.: Permutation polynomials EA-equivalent to the inverse function over $GF(2^n)$. Cryptogr. Commun. 3(3), 175-186 (2011).
17. Matsui M.: Linear cryptanalysis method for DES cipher, in Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in computer Science). New York: Springer-Verlag, vol. 765, pp. 386-397, 1994.
18. Nyberg K.: Differentially uniform mappings for cryptography. In: Advances in Cryptography-EUROCRYPT'93. LNCS, vol. 765, pp. 55-64. Springer-Verlag, New York (1994).
19. Pasalic E., Charpin P.: Some results concerning cryptographically significant mappings over GF(2^n). Des. Codes Cryptogr. 57(3), 257-269 (2010).