Constructing Differentially 4-uniform Permutations over GF(2^{2k}) from the Inverse Function Revisited

Yongqiang Li [a], Mingsheng Wang [a] and Yuyin Yu [b]

[a] The State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
[b] Science and Technology on Communication Security Laboratory, Chengdu 610041, P. R. China
yongq.lee@gmail.com
mingsheng_wang@aliyun.com
yuyuyin@163.com

Abstract. Constructing S-boxes with low differential uniformity and high nonlinearity is of cardinal significance in cryptography. In the present paper, we show that numerous differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ can be constructed by composing the inverse function and cycles over $\mathbb{F}_{2^{2k}}$. Two sufficient conditions are given, which ensure that the differential uniformity of the corresponding compositions equals 4. A lower bound on nonlinearity is also given for permutations constructed with the method in the present paper. Moreover, up to CCZ-equivalence, a new differentially 4-uniform permutation with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$ with k odd is constructed. For some special cycles, necessary and sufficient conditions are given such that the corresponding compositions are differentially 4-uniform.

Keywords: differential uniformity, nonlinearity, permutation polynomial, inverse function

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. In some structures of block ciphers, such as substitution permutation structure, it is necessary for an S-box to be a permutation to decrypt a ciphertext. In real application, S-boxes are often designed as permutations over $\mathbb{F}_{2^{2m}}$ for efficiency of implementations. These boxes should possess good cryptographic properties to resist various attacks. Therefore, the problem of constructing permutations with good cryptographic properties over $\mathbb{F}_{2^{2m}}$ is of significant importance in cryptography.

Differential uniformity and nonlinearity are two primary cryptographic properties which should be considered firstly in the design of S-boxes. They measure the resistance of S-boxes to two main attacks on symmetric cryptography algorithms—differential attack [1] and linear attack [27] respectively. The definition of these properties is introduced as follows.

The differential uniformity of $F(x) \in \mathbb{F}_{2^n}$ is the smallest integer δ, such that $F(x)+F(x+a) = b$ has at most δ solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ [28], and $F(x)$ is called differentially δ-uniform. The lower bound on differential uniformity of $F(x) \in \mathbb{F}_{2^n}[x]$ is 2. Differentially 2-uniform functions are called almost perfect nonlinear (APN). Much work has been done on constructing APN functions [2,4,7,8,9,10,11], since they provide the best resistance to differential attacks.

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 $\{\lambda_F(u,v) : u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^*\}$. The nonlinearity of $F(x)$, which is defined as the minimum distance of the components of $F(x)$ and all affine Boolean

Function	Condition	Walsh spectrum	Ref.
x^{2^i+1}	$n = 2k,\ k$ odd, $\gcd(i, n) = 2$	$\{0, \pm 2^{k+1}\}$	[20,28]
$x^{2^{2i}-2^i+1}$	$n = 2k,\ k$ odd, $\gcd(i, n) = 2$	$\{0, \pm 2^{k+1}\}$	[21]
x^{2^n-2}	$n = 2k$	$\{-2^{\frac{n}{2}+1} < a \leq 2^{\frac{n}{2}+1} : 4\|a\}$	[22,28]
$x^{2^{2k}+2^k+1}$	$n = 4k,\ k$ odd	$\{0, \pm 2^{2k}, \pm 2^{2k+1}\}$	[3]
$\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$	$n = 3k,\ k$ even, $3 \nmid k,\ k/2$ odd, $\gcd(3k, s) = 2,\ 3\|(k + s)$, α is a primitive element of $\mathbb{F}_{2^n}$	$\subseteq \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$	[5]
$L_u(F^{-1}(x))\|_{H_u}$	$n = 2k,\ F(x)$ is a quadratic APN permutation on $\mathbb{F}_{2^{n+1}},\ u \in \mathbb{F}^*_{2^{n+1}}$, $L_u(x) = F(x) + F(x + u) + F(u)$, $H_u = \{L_u(x) \mid x \in \mathbb{F}_{2^{n+1}}\}$	$\subseteq \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$	[26]
$\sum_{i=0}^{2^n-3} x^i$	$n = 2k,\ k$ odd	$\{-2^{\frac{n}{2}+1} \leq a \leq 2^{\frac{n}{2}+1} : 4\|a\}$	[32], this article

Table 1. Differentially 4-uniform permutations with the best know nonlinearity over $\mathbb{F}_{2^{2k}}$ for infinitely many k

functions on 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 $F(x) \in \mathbb{F}_{2^n}[x]$, $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [16]. For even n and $F(x) \in \mathbb{F}_{2^n}[x]$, the upper bound on the nonlinearity of $F(x)$ is still open. The best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$ [19]. For other cryptography properties of Boolean functions and vectorial Boolean functions, one can see [13,14] for details.

The lower of the differential uniformity and the higher of the nonlinearity of an S-box, the better performance it possess in cryptography. APN permutations over $\mathbb{F}_{2^{2m}}$ would be the best choice for S-boxes in cryptography. However, only one APN permutation over $\mathbb{F}_{2^6}$ has been found [18], and the existence of APN permutations over $\mathbb{F}_{2^{2m}}$ with $m \geq 4$ 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 inverse function over $\mathbb{F}_{2^8}$. It is also difficult to construct differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_{2^{2m}}$. Table 1 list permutations over $\mathbb{F}_{2^{2m}}$ with differential uniformity 4 and nonlinearity $2^{2m-1} - 2^m$ for infinitely many m as far as we know, and the drawbacks of some of these permutations can be seen in [15].

A reason for few infinite classes of permutations with good cryptographic properties is known, which is point out by Carlet in [15], is that there are no secondary construction methods. EA-equivalence and CCZ-equivalence can be used for constructing permutations with good cryptographic properties, since differential uniformity and nonlinearity are invariant under these equivalence, but permutations are not. Some works are done with this idea, see [7,18,24,25,30] for more details.

Carlet give a powerful secondary method for constructing differentially 4-uniform permutations [15]. The idea is that instead of using the field structure of $\mathbb{F}_{2^n}$, to use that of $\mathbb{F}_{2^{n+1}}$. A differentially 4-uniform permutation with algebraic degree $n - 1$ over $\mathbb{F}_{2^{2k}}$ is constructed in [15]. However, this permutation does not have the highest nonlinearity. With the above idea, it is shown that differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$ can be constructed from quadratic APN permutations over $\mathbb{F}_{2^{2k+1}}$ [26]. Some constructions are given by using Gold functions [26].

Qu et.al give another secondary construction of differentially 4-uniform permutations, which is changing components of the inverse function [31]. Based on the work of characterization of permutation polynomials of the type $F_1(x)+\mathrm{Tr}(G(x))$ [17], they investigate how to choose $R(x)$, such that the composition of $x+\mathrm{Tr}(R(x)+R(x+1))$ and x^{-1} is of differential uniformity 4.

Comparing with changing components of the inverse function, it is natural to change image values of the inverse function directly. We have given a sufficient and necessary condition for permutations, which are constructed by exchanging two image values of the inverse function, have differential uniformity 4 [32]. By using this idea, new differentially 4-uniform permutations are also constructed in [33] by applying affine transformation to the inverse function on some subfields of $\mathbb{F}_{2^{2k}}$ and maintain the image values of the inverse function unchanged for other elements. The idea of changing image values of a known function is also used in [29] to construct functions with optimal deficiency and ambiguity.

In the present paper, we revisit the above secondary construction method of differentially 4-uniform permutations further. We investigate the composition of the inverse function and cycles (see definition below) over $\mathbb{F}_{2^n}$, which means more image values of the inverse function are changed. It is shown that lots of new differentially 4-uniform permutations can be constructed via this method. Furthermore, a new differentially 4-uniform permutation with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$ is also given.

The paper is organized as follows. In Sect. 2, we give a description of our construction and introduce some preliminary results. In Sect. 3, the compositional inverse and a lower bound on nonlinearity of permutations constructed in the present paper are given. A new differentially 4-uniform permutation with the best known nonlinearity is also given. In Sect. 4, two sufficient conditions are given such that the general constructions are differentially 4-uniform. In Sect. 5, complete characterizations for some special cycles such that the corresponding permutations have differential uniformity 4 are given. In Sect. 6, a short conclusion is given.

2 Preliminaries

A cycle over $\mathbb{F}_{2^n}$ is a permutation defined as

$$\pi(x)=\begin{cases}\alpha_{i+1} & x=\alpha_i\\ x & x\notin\{\alpha_i \mid 0\le i\le m\},\end{cases}$$

where α_i, $0\le i\le m$ are pairwise different elements of $\mathbb{F}_{2^n}$. The subscripts are computed in $\mathbb{Z}_{m+1}$ throughout this paper, which means $\alpha_{m+1}=\alpha_0$.

A cycle defined as above is denoted by $\pi=(\alpha_0,\alpha_1,\ldots,\alpha_m)$. $m+1$ is called the length of π. A Cycle with length 2 is called a transposition. We call $\alpha\in\pi$ if $\alpha=\alpha_i$ for some $0\le i\le m$. It is easy to see that $\alpha\notin\pi$ if and only if $\pi(\alpha)=\alpha$.

Let $\pi(x)^{-1}$ denotes the composition of the inverse function and a cycle $\pi=(\alpha_0,\alpha_1,\ldots,\alpha_m)$ over $\mathbb{F}_{2^n}$. Then it holds

$$\pi(x)^{-1}=\begin{cases}\alpha_{i+1}^{-1} & x=\alpha_i\\ x^{-1} & x\notin\{\alpha_i \mid 0\le i\le m\}.\end{cases}$$

It is obvious that $\pi(x)^{-1}$ is a permutation over $\mathbb{F}_{2^n}$. According to Lagrange interpolation, we have

$$\begin{aligned}\pi(x)^{-1}&=x^{-1}+\sum_{i=0}^{m}((x+\alpha_i)^{2^n-1}+1)(\alpha_i^{-1}+\alpha_{i+1}^{-1})\\&=x^{-1}+\sum_{i=0}^{m}(x+\alpha_i)^{2^n-1}(\alpha_i^{-1}+\alpha_{i+1}^{-1}).\end{aligned}$$

In the present paper, we show that lots of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ of the type $\pi(x)^{-1}$ can be constructed by chosing suitable cycles over $\mathbb{F}_{2^n}$.

Before we present the next result, we first introduce some equivalence relationship of functions over $\mathbb{F}_{2^n}$. Two functions $F_1(x), F_2(x) \in \mathbb{F}_{2^n}[x]$ are called EA-equivalent, if there exist affine permutations $A_1(x)$, $A_2(x) \in \mathbb{F}_{2^n}[x]$ and an affine function $A_3(x) \in \mathbb{F}_{2^n}[x]$, such that

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

If $A_3(x) = 0$, then $F_1(x)$ and $F_2(x)$ are called affine equivalent. A more general framework is introduced by considering graphs of functions [12]. Two functions $F_1, F_2 \in \mathbb{F}_{2^n}[x]$ are called CCZ-equivalent if there exists an affine permutation $\mathcal{L}$ over $\mathbb{F}_{2^n}^2$, such that $\mathcal{L}(G_{F_1}) = G_{F_2}$, where $G_{F_i} = \{(x, F_i(x)) \mid x \in \mathbb{F}_{2^n}\}, i = 1, 2$. For $F(x) \in \mathbb{F}_{2^n}[x]$, the extended code $\tilde{C}_F$ of $F(x)$ is the linear code with parity check matrix

$$\begin{bmatrix} \cdots & 1 & \cdots \\ \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{bmatrix}.$$

For admissible maps $F_1(x), F_2(x) \in \mathbb{F}_{2^n}[x]$, $F_1(x)$ and $F_2(x)$ are CCZ-equivalent if and only if $\tilde{C}_{F_1}$ and $\tilde{C}_{F_2}$ are equivalent [6].

Then we have the following result, which simplify the choice of cycles.

Lemma 1. *Suppose $\pi = (\alpha_0, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Then the following statements hold.*

1. *If $0 \in \pi$, then $\pi(x)^{-1}$ is affine equivalent to $\pi_1(x)^{-1}$, where π_1 is a cycle over $\mathbb{F}_{2^n}$ of the type $(0, 1, \beta_1, \ldots, \beta_{m-1})$.*
2. *If $0 \notin \pi$, then $\pi(x)^{-1}$ is affine equivalent to $\pi_1(x)^{-1}$, where π_1 is a cycle over $\mathbb{F}_{2^n}$ of the type $(1, \beta_1, \ldots, \beta_m)$.*

Proof. 1. Without loss of generality, we suppose $\alpha_0 = 0$ since for any $1 \le k \le m$, cycles $(\alpha_0, \ldots, \alpha_m)$ and $(\alpha_k, \alpha_{k+1}, \ldots, \alpha_{k-1})$ are equal. When $\alpha_1 = 1$, the proof is already completed. When $\alpha_1 \neq 1$, let $\pi_1(x) = \alpha_1^{-1}\pi(\alpha_1 x)$. Then

$$\pi_1(x) = \begin{cases} \frac{\alpha_{i+1}}{\alpha_1} & x = \frac{\alpha_i}{\alpha_1} \\ x & x \notin \{\frac{\alpha_i}{\alpha_1} \mid 0 \le i \le m\}. \end{cases}$$

Hence $\pi_1(x) = (0, 1, \frac{\alpha_2}{\alpha_1}, \ldots, \frac{\alpha_m}{\alpha_1})$ is a cycle and $\pi_1(x)^{-1}$ is affine equivalent to $\pi(x)^{-1}$ since

$$\pi_1(x)^{-1} = \alpha_1 \pi(\alpha_1 x)^{-1}.$$

2. The proof is similar as the above proof. □

A permutation over $\mathbb{F}_{2^4}$ is called optimal if both of its differential uniformity and nonlinearity equal 4. There are exactly 7 CCZ-inequivalent optimal permutations over $\mathbb{F}_{2^4}$ [23]. Table 2 shows that up to CCZ-equivalence, all optimal permutations over $\mathbb{F}_{2^4}$ can be generated by this method. This is done by computer searching. Based on Lemma 1, we only need to search cycles of the type $(0, 1, *, \ldots, *)$ and $(1, * \ldots, *)$. We start from cycles with length 2 of the above types and check the differential uniformity, nonlinearity and CCZ-inequivalence of the corresponding permutations. Then we goto the case of cycles with a bigger length until all 7 classes are got. Representative cycles are listed in Table 2, where g is a root of $x^4 + x + 1 = 0$.

When π is a transposition over $\mathbb{F}_{2^n}$, the differential uniformity of $\pi(x)^{-1}$ is characterized in [32].

cycle	G_i in [23]	cycle	G_i in [23]
$(1, g^3)$	G_4	$(0, 1, g)$	G_9
$(1, g^3, g^6)$	G_7	$(0, 1, g^7, g^5)$	G_{13}
$(1, g, g^7, g^2)$	G_0	$(0, 1, g, g^2, g^{10})$	G_{14}
$(1, g^7, g^3, g)$	G_3		

Table 2. Cycles over $\mathbb{F}_{2^4}$ such that $\pi(x)^{-1}$ is an optimal permutation over $\mathbb{F}_{2^4}$

Theorem 1. *[32] Let $n = 2k$ be an even integer. Then the following statements hold.*

1. *Suppose $\pi = (0, 1)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if k is odd.*
2. *Suppose $\pi = (1, \alpha)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\frac{1}{\alpha}) = 1$.*

The following result is useful in the present paper.

Lemma 2. *[28] Let $n = 2k$ be an even integer. Then for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, the following statements hold.*

1. *$x^{-1} + (x + a)^{-1} = b$ has no roots in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{1}{ab}) = 1$.*
2. *$x^{-1} + (x + a)^{-1} = b$ has 2 roots in $\mathbb{F}_{2^n}$ if and only if $ab \neq 1$ and $\mathrm{Tr}(\frac{1}{ab}) = 0$.*
3. *$x^{-1} + (x + a)^{-1} = b$ has 4 roots in $\mathbb{F}_{2^n}$ if and only if $b = a^{-1}$. Furthermore, when $b = a^{-1}$ the 4 roots of the above equation in $\mathbb{F}_{2^n}$ are $\{0, a, a\omega, a\omega^2\}$, where $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$.*

3 On the compositional inverse and nonlinearity of $\pi(x)^{-1}$

We first characterize the compositional inverse and the nonlinearity of $\pi(x)^{-1}$ in this section. The inverse function over $\mathbb{F}_{2^n}$ is denoted by $Inv(x) = x^{-1} = x^{2^n-2}$.

Theorem 2. *Suppose $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Then the following statements hold.*

1. *The compositional inverse of $\pi(x)^{-1}$ is $\pi_1(x)^{-1}$, where $\pi_1 = (\alpha_m^{-1}, \alpha_{m-1}^{-1}, \ldots, \alpha_0^{-1})$ is a cycle over $\mathbb{F}_{2^n}$.*
2. *$\mathcal{NL}(\pi^{-1}) \geq 2^{n-1} - 2^{\frac{n}{2}} - (m + 1)$.*

Proof. 1. Notice that

$$\pi_1(x)^{-1} = \begin{cases} \alpha_{i-1} & x = \alpha_i^{-1} \\ x^{-1} & x \notin \pi_1, \end{cases}$$

and

$$\pi(x)^{-1} = \begin{cases} \alpha_{i+1}^{-1} & x = \alpha_i \\ x^{-1} & x \notin \pi, \end{cases}$$

then we have

$$\pi(\pi_1(x)^{-1})^{-1} = \begin{cases} \pi(\alpha_{i-1})^{-1} = \alpha_i^{-1} & x = \alpha_i^{-1} \\ \pi(x^{-1}) = x & x \notin \pi_1, \end{cases}$$

since $x^{-1} \notin \pi$ when $x \notin \pi_1$. Thus $\pi(\pi_1(x)^{-1})^{-1} = x$.

2. According to the definition of $\pi(x)^{-1}$, for $b \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}
\lambda_{\pi^{-1}}(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(b\pi(x)^{-1}+ax)} \\
&= \sum_{x\notin\pi} (-1)^{\mathrm{Tr}(bx^{-1}+ax)} + \sum_{i=0}^{m} (-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1}+a\alpha_i)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bx^{-1}+ax)} + \sum_{i=0}^{m} ((-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1}+a\alpha_i)} - (-1)^{\mathrm{Tr}(b\alpha_i^{-1}+a\alpha_i)}) \\
&= \lambda_{Inv}(a,b) + \sum_{i=0}^{m} (-1)^{\mathrm{Tr}(a\alpha_i)}((-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1})} - (-1)^{\mathrm{Tr}(b\alpha_i^{-1})}).
\end{aligned}$$

Therefore,

$$\begin{aligned}
|\lambda_{\pi^{-1}}(a,b)| &\leq |\lambda_{Inv}(a,b)| + |\sum_{i=0}^{m} (-1)^{\mathrm{Tr}(a\alpha_i)}((-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1})} - (-1)^{\mathrm{Tr}(b\alpha_i^{-1})})| \\
&\leq 2^{\frac{n}{2}+1} + \sum_{i=0}^{m} |(-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1})} - (-1)^{\mathrm{Tr}(b\alpha_i^{-1})}| \\
&\leq 2^{\frac{n}{2}+1} + 2(m+1),
\end{aligned}$$

from which we get

$$\mathcal{NL}(\pi^{-1}) \geq 2^{n-1} - 2^{\frac{n}{2}} - (m+1)$$

and we complete the proof. □

The above result means that the permutations constructed by compositing the inverse function and cycles over $\mathbb{F}_{2^n}$ have a relative high nonlinearity when cycles are chosen with small length. The lower bound on nonlinearity can be improved for some special cycles. Furthermore, permutations with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$ can be constructed as shown in the following result.

Theorem 3. *Suppose $n = 2k$, $\pi = (0,1)$ is a transposition over $\mathbb{F}_{2^n}$. Then $\pi(x)^{-1} = \sum_{i=0}^{2^n-3} x^i$ and its nonlinearity equals $2^{n-1} - 2^{\frac{n}{2}}$, which is the best known nonlinearity over $\mathbb{F}_{2^n}$. Moreover, its Walsh spectrum is $\{-2^{\frac{n}{2}+1} \leq y \leq 2^{\frac{n}{2}+1} \mid y \equiv 0 \ mod\ 4\}$.*

Proof. According to Lagrange interpolation, we have

$$\pi(x)^{-1} = x^{2^n-2} + x^{2^n-1} + (x+1)^{2^n-1} = \sum_{i=0}^{2^n-3} x^i,$$

where x^0 means 1. Suppose $F(x) = \pi(x)^{-1} = \sum_{i=0}^{2^n-3} x^i$. Then according to Theorem 2, for $b \in \mathbb{F}_{2^n}^*$, $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}
\lambda_F(a,b) &= \lambda_{Inv}(a,b) + \sum_{i=0}^{m} (-1)^{\mathrm{Tr}(a\alpha_i)}((-1)^{\mathrm{Tr}(b\alpha_{i+1}^{-1})} - (-1)^{\mathrm{Tr}(b\alpha_i^{-1})}) \\
&= \lambda_{Inv}(a,b) + ((-1)^{\mathrm{Tr}(b)} - 1) + (-1)^{\mathrm{Tr}(a)}(1 - (-1)^{\mathrm{Tr}(b)}) \\
&= \lambda_{Inv}(a,b) + ((-1)^{\mathrm{Tr}(b)} - 1)(1 - (-1)^{\mathrm{Tr}(a)}) \\
&= \begin{cases} \lambda_{Inv}(a,b) & \mathrm{Tr}(a) = 0 \text{ or } \mathrm{Tr}(b) = 0 \\ \lambda_{Inv}(a,b) - 4 & \mathrm{Tr}(a) = \mathrm{Tr}(b) = 1. \end{cases}
\end{aligned}$$

Note that the Walsh spectrum of x^{-1} is $\Lambda_{Inv} = \{-2^{\frac{n}{2}+1} + 4 \leq y \leq 2^{\frac{n}{2}+1} \mid y \equiv 0 \bmod 4\}$, then we have

$$\Lambda_F \subseteq \{-2^{\frac{n}{2}+1} \leq y \leq 2^{\frac{n}{2}+1} \mid y \equiv 0 \bmod 4\},$$

where Λ_F is the Walsh spectrum of $F(x)$. Notice that for $b \in \mathbb{F}_{2^n}^*, a \in \mathbb{F}_{2^n}$,

$$\lambda_{Inv}(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bx^{-1}+ax)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{-1}+abx)} = \lambda_{Inv}(ab,1),$$

then for any $\alpha \in \Lambda_{Inv}$, there exists $c \in \mathbb{F}_{2^n}$, such that $\lambda_{Inv}(c,1) = \alpha$. Thus

$$\lambda_F(c,1) = \lambda_{Inv}(c,1) = \alpha$$

since $\mathrm{Tr}(1) = 0$ when n is even. This means $\Lambda_{Inv} \subseteq \Lambda_F$.

At last, we prove that $-2^{\frac{n}{2}+1}$ is in the Walsh spectrum of $\pi(x)^{-1}$. Similar as above, it is easy to see that there exists $d \in \mathbb{F}_{2^n}$, such that

$$\lambda_{Inv}(d,1) = -2^{\frac{n}{2}+1} + 4.$$

Then it must holds $d \neq 0$, since x^{-1} is a permutation and hence $\lambda_{Inv}(0,1) = 0$. Therefore, $\mathrm{Tr}(\frac{d}{x})$ is a balanced Boolean function. Hence $|\{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(\frac{d}{x}) = 0\}| = 2^{n-1}$. Notice that $\mathrm{Tr}(d \cdot 0^{-1}) = 0$, then there exists $a' \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(a') = 1$, such that $\mathrm{Tr}(\frac{d}{a'}) = 1$. Then we have

$$\lambda_F(a', \frac{d}{a'}) = \lambda_{Inv}(a', \frac{d}{a'}) - 4 = \lambda_{Inv}(d,1) - 4 = -2^{\frac{n}{2}+1}.$$

Therefore, we have

$$\Lambda_F = \{-2^{\frac{n}{2}+1} \leq y \leq 2^{\frac{n}{2}+1} \mid y \equiv 0 \bmod 4\},$$

and the nonlinearity of $F(x)$ equals $2^{n-1} - 2^{\frac{n}{2}}$. Then we complete the proof. □

Based on the above results and Theorem 1, we have the following result.

Corollary 1. *Suppose $n = 2k$, k is odd and $F(x) = \sum_{i=0}^{2^n-3} x^i$. Then the following statements hold.*

1. *$F(x)$ is an involution on $\mathbb{F}_{2^n}$, which means $F(F(x)) = x$.*
2. *$F(x)$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$.*
3. *$\mathcal{NL}(F) = 2^{n-1} - 2^{\frac{n}{2}}$ and its Walsh spectrum is $\{-2^{\frac{n}{2}+1} \leq y \leq 2^{\frac{n}{2}+1} \mid y \equiv 0 \bmod 4\}$.*

Remark 1. With the help of Magma, it can be checked that $F(x) = \sum_{i=0}^{2^n-3} x^i$ is CCZ-inequivalent to x^{-1} over $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^{10}}$, since their extended codes are not equivalent. The CCZ-inequivalence of $F(x)$ to other differentially 4-uniform permutations with the best known nonlinearity in Table 1 is obvious, since their extended Walsh spectrum are different. Thus $F(x) = \sum_{i=0}^{2^n-3} x^i$ is a new differentially 4-uniform permutation with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$. Another interesting property of $F(x) = \sum_{i=0}^{2^n-3} x^i$ is that its Walsh spectrum is symmetric, which means if $\alpha \in \Lambda_F$, then $-\alpha \in \Lambda_F$. However, the Walsh spectrum of the inverse function does not have this propertity.

4 Sufficient conditions for $\pi(x)^{-1}$ has differential uniformity 4

Suppose $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$ and $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Then we have the following equality,

$$\pi(x)^{-1} + \pi(x+a)^{-1} = \begin{cases} \alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} & \{x, x+a\} \cap \pi = \{\alpha_i, \alpha_j\} \\ \alpha_{i+1}^{-1} + (a+\alpha_i)^{-1} & \{x, x+a\} \cap \pi = \{\alpha_i\} \\ x^{-1} + (x+a)^{-1} & \{x, x+a\} \cap \pi = \emptyset, \end{cases} \tag{1}$$

which is useful for characterizing the number of roots of equation

$$\pi(x)^{-1} + \pi(x+a)^{-1} = b$$

in $\mathbb{F}_{2^n}$. Let $S(a,b) = \{x_0 \in \mathbb{F}_{2^n} \mid \pi(x_0)^{-1} + \pi(x_0+a)^{-1} = b\}$, which is the set of roots of the above equation in $\mathbb{F}_{2^n}$. Then $S(a,b)$ can be partitioned to the following three sets:

$$S_\pi(a,b) = \{x_0 \in S(a,b) \mid \{x_0, x_0+a\} \subseteq \pi\},$$

$$S_{\pi/2}(a,b) = \{x_0 \in S(a,b) \mid \#(\{x_0, x_0+a\} \cap \pi) = 1\},$$

and

$$S_{\bar{\pi}}(a,b) = \{x_0 \in S(a,b) \mid \{x_0, x_0+a\} \cap \pi = \emptyset\}.$$

It is easy to see that

$$S(a,b) = S_\pi(a,b) \cup S_{\pi/2}(a,b) \cup S_{\bar{\pi}}(a,b)$$

and $S_\pi(a,b), S_{\pi/2}(a,b)$, $S_{\bar{\pi}}(a,b)$ are pairwise disjoint. Therefore, it holds

$$|S(a,b)| = |S_\pi(a,b)| + |S_{\pi/2}(a,b)| + |S_{\bar{\pi}}(a,b)|, \tag{2}$$

which is an elementary equality for characterizing the differential uniformity of $\pi(x)^{-1}$.

Lemma 3. *Suppose $n = 2k$ and $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n} \setminus \{\pi(x)^{-1} + \pi(x+a)^{-1} \mid x \in \pi\}$. Then $|S(a,b)| \leq 4$. Moreover, $|S(a,b)| \leq 2$ when $0 \in \pi$.*

Proof. Notice that $b \notin \{\pi(x)^{-1} + \pi(x+a)^{-1} \mid x \in \pi\}$, then for $0 \leq i \leq m$, α_i and $\alpha_i + a$ do not satisfy equation

$$\pi(x)^{-1} + \pi(x+a)^{-1} = b.$$

Thus $|S_\pi(a,b)| = |S_{\pi/2}(a,b)| = 0$ and

$$|S(a,b)| = |S_\pi(a,b)| + |S_{\pi/2}(a,b)| + |S_{\bar{\pi}}(a,b)| = |S_{\bar{\pi}}(a,b)| \leq 4,$$

since

$$x^{-1} + (x+a)^{-1} = b$$

has at most 4 roots in $\mathbb{F}_{2^n}$ according to Lemma 2.

Moreover, according to Lemma 2, the above equation has 4 roots if and only if $ab = 1$. Furthermore, the 4 roots are $0, a, a\omega, a\omega^2$, where $\omega \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Thus when $0 \in \pi$, it holds that 0 is not a root of

$$\pi(x)^{-1} + \pi(x+a)^{-1} = a^{-1},$$

since $a^{-1} \notin \{\pi(x)^{-1} + \pi(x+a)^{-1} \mid x \in \pi\}$. This means $|S(a,b)| \leq 2$ when $0 \in \pi$ and we complete the proof. □

Lemma 3 means that if equation $\pi(x)^{-1}+\pi(x+a)^{-1}=b$ has more than 4 roots in $\mathbb{F}_{2^{2k}}$, then $b=\pi(\alpha_i)^{-1}+\pi(\alpha_i+a)^{-1}$ for some $0\le i\le m$. Let $b_i(a)$ denotes

$$\pi(\alpha_i)^{-1}+\pi(\alpha_i+a)^{-1}$$

for $a\in\mathbb{F}_{2^n}^*$ and $0\le i\le m$. Then it holds

$$b_i(a)=\begin{cases}\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1} & \alpha_i+a=\alpha_j\in\pi\\ \alpha_{i+1}^{-1}+(a+\alpha_i)^{-1} & \alpha_i+a\notin\pi.\end{cases} \tag{3}$$

If π is chosen such that the number of roots of

$$\pi(x)^{-1}+\pi(x+a)^{-1}=b_i(a)$$

in $\mathbb{F}_{2^n}$ is less than or equals to 4 for all $a\in\mathbb{F}_{2^n}^*$ and $0\le i\le m$, then the differential uniformity of $\pi(x)^{-1}$ is not large than 4.

Lemma 4. *Suppose $\pi=(\alpha_0,\alpha_1,\dots,\alpha_n)$ is a cycle over $\mathbb{F}_{2^n}$ with the property that for $0\le i<j<l\le m$, the system of equations*

$$\begin{cases}x^2+(\alpha_i+\alpha_j)x=(\alpha_i+\alpha_j)(\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1})^{-1}+\alpha_i\alpha_j\\ x^2+(\alpha_i+\alpha_l)x=(\alpha_i+\alpha_l)(\alpha_{i+1}^{-1}+\alpha_{l+1}^{-1})^{-1}+\alpha_i\alpha_l\end{cases}$$

does not has solutions in $\mathbb{F}_{2^n}$. Then the following statements hold.

1. *If $0\notin\pi$ and for $0\le i<j\le m$, $\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1}\ne(\alpha_i+\alpha_j)^{-1}$, then $|S_{\pi/2}(a,b)|\le 4$ for $a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}$.*
2. *If $0\in\pi$, then $|S_{\pi/2}(a,b)|\le 4$ for $a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}$.*

Proof. 1. Assume there exist $a\in\mathbb{F}_{2^n}^*$, $b\in\mathbb{F}_{2^n}$, such that $|S_{\pi/2}(a,b)|\ge 6$. Then there exist $\alpha_{i_1},\alpha_{i_2},\alpha_{i_3}\in\pi$, such that $\alpha_{i_j}+a\notin\pi$ for $j=1,2,3$, and $b_{i_1}(a)=b_{i_2}(a)$, $b_{i_1}(a)=b_{i_3}(a)$. Without loss of generality, we suppose $0\le i_1<i_2<i_3\le m$. Then according to equality (3), we have

$$\begin{cases}\alpha_{i_1+1}^{-1}+(\alpha_{i_1}+a)^{-1}=\alpha_{i_2+1}^{-1}+(\alpha_{i_2}+a)^{-1}\\ \alpha_{i_1+1}^{-1}+(\alpha_{i_1}+a)^{-1}=\alpha_{i_3+1}^{-1}+(\alpha_{i_3}+a)^{-1}.\end{cases}$$

Notice that $\alpha_{i_1}\ne a$, otherwise

$$\alpha_{i_1+1}^{-1}+\alpha_{i_2+1}^{-1}=(\alpha_{i_1}+\alpha_{i_2})^{-1},$$

which contradicts to $\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1}\ne(\alpha_i+\alpha_j)^{-1}$ for $0\le i<j\le m$. Similarly, we have $\alpha_{i_2}\ne a$ and $\alpha_{i_3}\ne a$. Then

$$\alpha_{i_1+1}^{-1}+(\alpha_{i_1}+a)^{-1}=\alpha_{i_2+1}^{-1}+(\alpha_{i_2}+a)^{-1}$$

is equivalent to

$$\alpha_{i_1+1}^{-1}+\alpha_{i_2+1}^{-1}=\frac{\alpha_{i_1}+\alpha_{i_2}}{(\alpha_{i_1}+a)(\alpha_{i_2}+a)}=\frac{\alpha_{i_1}+\alpha_{i_2}}{a^2+(\alpha_{i_1}+\alpha_{i_2})a+\alpha_{i_1}\alpha_{i_2}}.$$

Hence a satisfies equation

$$x^2+(\alpha_{i_1}+\alpha_{i_2})x=(\alpha_{i_1}+\alpha_{i_2})(\alpha_{i_1+1}^{-1}+\alpha_{i_2+1}^{-1})^{-1}+\alpha_{i_1}\alpha_{i_2},$$

since $\alpha_{i_1+1}\ne\alpha_{i_2+1}$. Therefore, a is a solution of the system of equations

$$\begin{cases}x^2+(\alpha_{i_1}+\alpha_{i_2})x=(\alpha_{i_1}+\alpha_{i_2})(\alpha_{i_1+1}^{-1}+\alpha_{i_2+1}^{-1})^{-1}+\alpha_{i_1}\alpha_{i_2}\\ x^2+(\alpha_{i_1}+\alpha_{i_3})x=(\alpha_{i_1}+\alpha_{i_3})(\alpha_{i_1+1}^{-1}+\alpha_{i_3+1}^{-1})^{-1}+\alpha_{i_1}\alpha_{i_3},\end{cases}$$

which is a contradiction.

2. Assume there exist $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$, such that $|S_{\pi/2}(a,b)| \geq 6$. Then there exist $\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3} \in \pi$, such that $\alpha_{i_j} + a \notin \pi$ for $j = 1,2,3$, and $b_{i_1}(a) = b_{i_2}(a)$, $b_{i_1}(a) = b_{i_3}(a)$. It is obvious that $\alpha_{i_j} + a \neq 0$ for $j = 1,2,3$, since $0 \in \pi$. Thus the proof is same as the proof of statement 1. □

Theorem 4. *Let $n = 2k$, $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ be a cycle over $\mathbb{F}_{2^n}$ with $0 \in \pi$ and the nonzero elements of π are linear independent over $\mathbb{F}_2$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if the following conditions are satisfied:*

1. *For $0 \leq i < j < l \leq m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} + \alpha_{l+1}^{-1}) \neq (\alpha_i + \alpha_j + \alpha_l)^{-1}$.*
2. *For $0 \leq i < j < l \leq m$, the system of equations*

$$\begin{cases} x^2 + (\alpha_i + \alpha_j)x = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j \\ x^2 + (\alpha_i + \alpha_l)x = (\alpha_i + \alpha_l)(\alpha_{i+1}^{-1} + \alpha_{l+1}^{-1})^{-1} + \alpha_i\alpha_l \end{cases}$$

does not has solutions in $\mathbb{F}_{2^n}$.

3. *For $0 \leq i < j \leq m$, if $a \in \mathbb{F}_{2^n}$ is a solution of*

$$x^2 + (\alpha_i + \alpha_j)x = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j,$$

with $a + \alpha_i \notin \pi$ and $a + \alpha_j \notin \pi$, then $\mathrm{Tr}(\frac{1}{ab_i(a)}) = 1$, where $b_i(a) = \alpha_{i+1}^{-1} + (a + \alpha_i)^{-1}$.

Proof. For $a \in \mathbb{F}_{2^n}^*$ and $0 \leq i \leq m$, denote $b_i(a) = \pi(\alpha_i)^{-1} + \pi(a + \alpha_i)^{-1}$. According to Lemma 3, we only need to prove that for $a \in \mathbb{F}_{2^n}^*$ and $0 \leq i \leq m$, the number of solutions of equation

$$\pi(x)^{-1} + \pi(x + a)^{-1} = b_i(a)$$

in $\mathbb{F}_{2^n}$ is less than or equals to 4. According to equality (2), this is equivalent to prove

$$|S(a, b_i(a))| = |S_\pi(a, b_i(a))| + |S_{\pi/2}(a, b_i(a))| + |S_{\bar{\pi}}(a, b_i(a))| \leq 4.$$

According to Lemma 2, it is easy to see that

$$|S_{\bar{\pi}}(a, b_i(a))| \leq 2$$

for $a \in \mathbb{F}_{2^n}^*$, $0 \leq i \leq m$, since $0 \in \pi$.

Notice that $\pi = (\alpha_0, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$ and the nonzero elements of π are linear independent over $\mathbb{F}_2$, then

$$\alpha_{i_1} + \alpha_{j_1} \neq \alpha_{i_2} + \alpha_{j_2}$$

for $0 \leq i_1, i_2, j_1, j_2 \leq m$ with $\{i_1, j_1\} \neq \{i_2, j_2\}$. This means

$$|S_\pi(a, b_i(a))| \leq 2$$

for $a \in \mathbb{F}_{2^n}^*$ and $0 \leq i \leq m$. Moreover, for $0 \leq i \leq m$, $a \in \mathbb{F}_{2^n}^*$,

$$|S_\pi(a, b_i(a))| = 2$$

if and only if $a = \alpha_i + \alpha_j$ for some $0 \leq j \leq m$ with $j \neq i$. Then for $a \in \mathbb{F}_{2^n}^*$, $0 \leq i \leq m$, we have the following two cases:

Case 1. $|S_\pi(a, b_i(a))| = 2$. Then $a = \alpha_i + \alpha_j$ for some $0 \le j \le m$ with $j \ne i$. First, we prove that

$$S_{\pi/2}(a, b_i(a)) = 0.$$

Otherwise, there exists $0 \le l \le m$ with $l \ne i$, $l \ne j$, such that $\alpha_l + \alpha_i + \alpha_j \notin \pi$ and

$$\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} = b_i(a) = b_l(a) = \alpha_{l+1}^{-1} + (\alpha_l + \alpha_i + \alpha_j)^{-1}.$$

This contradicts with Condition 1. Hence

$$|S(a, b_i(a))| = |S_\pi(a, b_i(a))| + |S_{\pi/2}(a, b_i(a))| + |S_{\bar{\pi}}(a, b_i(a))| \le 2 + 0 + 2 = 4$$

in the case.

Case 2. $|S_\pi(a, b_i(a))| = 0$. According to Lemma 4, we have $|S_{\pi/2}(a, b_i(a))| \le 4$. Next, we prove that

$$S_{\bar{\pi}}(a, b_i(a)) = 0$$

when $|S_{\pi/2}(a, b_i(a))| = 4$. Otherwise, there exists $0 < j \le m$ with $j \ne i$, such that $\alpha_i + a \notin \pi$, $\alpha_j + a \notin \pi$,

$$\alpha_{i+1}^{-1} + (\alpha_i + a)^{-1} = \alpha_{j+1}^{-1} + (\alpha_j + a)^{-1}$$

and

$$x^{-1} + (x + a)^{-1} = \alpha_{i+1}^{-1} + (\alpha_i + a)^{-1}$$

has solutions in $\mathbb{F}_{2^n}$. According to Condition 1 of Lemma 2, the above equation has solutions in $\mathbb{F}_{2^n}$ is equivalent to $\mathrm{Tr}(\frac{1}{ab_i(a)}) = 0$. Hence a satisfies

$$x^2 + (\alpha_i + \alpha_j)x = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j,$$

$\alpha_i + a, \alpha_j + a \notin \pi$, and $\mathrm{Tr}(\frac{1}{ab_i(a)}) = 0$, which contradicts with Condition 3. Therefore, it holds

$$\begin{aligned} S(a, b_i(a)) &= |S_\pi(a, b_i(a))| + |S_{\pi/2}(a, b_i(a))| + |S_{\bar{\pi}}(a, b_i(a))| \\ &\le \begin{cases} 0 + 4 + 0 & S_{\pi/2}(a, b_i(a)) = 4 \\ 0 + 2 + 2 & S_{\pi/2}(a, b_i(a)) = 2 \end{cases} \\ &\le 4 \end{aligned}$$

in the case.

Then we complete the proof. □

Corollary 2. *Let $n = 2k$, $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ be a cycle over $\mathbb{F}_{2^n}$ with $0 \in \pi$ the nonzero elements of π are linear independent over $\mathbb{F}_2$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if the following conditions are satisfied:*

1. *For $0 \le i < j < l \le m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} + \alpha_{l+1}^{-1}) \ne (\alpha_i + \alpha_j + \alpha_l)^{-1}$.*
2. *For $0 \le i < j \le m$, it holds $\mathrm{Tr}((\alpha_i + \alpha_j)^{-1}(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \frac{\alpha_i\alpha_j}{(\alpha_i+\alpha_j)^2}) = 1$.*

Proof. Similarly as the proof of Theorem 4, for $a \in \mathbb{F}_{2^n}^*$, $b = b_i(a), 0 \le i \le m$, we have

$$|S_\pi(a, b)| \le 2.$$

According to Condition 1, if $|S_\pi(a,b)| = 2$, then

$$|S_{\pi/2}(a,b)| = 0.$$

According to Condition 2,

$$|S_{\pi/2}(a,b)| \le 2.$$

Therefore,

$$\begin{aligned} |S(a,b)| &= |S_\pi(a,b)| + |S_{\pi/2}(a,b)| + |S_{\bar\pi}(a,b)| \\ &\le \begin{cases} 2+0+2=4 & |S_\pi(a,b)| = 2 \\ 0+2+2=4 & |S_\pi(a,b)| = 0 \end{cases} \\ &\le 4. \end{aligned}$$

Then we complete the proof. □

When $0 \notin \pi$, we have the following results.

Theorem 5. *Let $n = 2k$, $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ be a cycle over $\mathbb{F}_{2^n}$ with $0 \notin \pi$ and the elements of π are linear independent over $\mathbb{F}_2$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if the following conditions are satisfied:*

1. *For $0 \le i < j < l \le m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} + \alpha_{l+1}^{-1}) \ne (\alpha_i + \alpha_j + \alpha_l)^{-1}$.*
2. *For $0 \le i < j < l \le m$, the system of equations*

$$\begin{cases} x^2 + (\alpha_i + \alpha_j)x = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j \\ x^2 + (\alpha_i + \alpha_l)x = (\alpha_i + \alpha_l)(\alpha_{i+1}^{-1} + \alpha_{l+1}^{-1})^{-1} + \alpha_i\alpha_l \end{cases}$$

   does not has solutions in $\mathbb{F}_{2^n}$.

3. *For $0 \le i < j \le m$, if $a \in \mathbb{F}_{2^n}$ is a solution of*

$$x^2 + (\alpha_i + \alpha_j)x = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j,$$

   with $a + \alpha_i \notin \pi$ and $a + \alpha_j \notin \pi$, then $\mathrm{Tr}(\frac{1}{ab_i(a)}) = 1$, where $b_i(a) = \alpha_{i+1}^{-1} + (a + \alpha_i)^{-1}$.

4. *For $0 \le i < j \le m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1}) \ne (\alpha_i + \alpha_j)^{-1}$.*
5. *For $0 \le i \le m$, it holds $\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i}) = 1$.*

Proof. According to Lemma 3 and equality (2), we only need to prove that for $a \in \mathbb{F}_{2^n}^*$ and $0 \le i \le m$,

$$|S(a, b_i(a))| = |S_\pi(a, b_i(a))| + |S_{\pi/2}(a, b_i(a))| + |S_{\bar\pi}(a, b_i(a))| \le 4,$$

where $b_i(a) = \pi(\alpha_i)^{-1} + \pi(a + \alpha_i)^{-1}$.

First, we claim that $|S_{\bar\pi}(a, b_i(a))| \le 2$ for $a \in \mathbb{F}_{2^n}^*$, $0 \le i \le m$. Otherwise, there exist $a \in \mathbb{F}_{2^n}^*$ and some $0 \le i \le m$, such that

$$a^{-1} = b_i(a) = \alpha_{i+1}^{-1} + \pi(\alpha_i + a)^{-1},$$

since according to Lemma 2, for $b \in \mathbb{F}_{2^n}$, $|S_{\bar\pi}(a,b)| \le 4$ and $ab = 1$ if $|S_{\bar\pi}(a,b)| = 4$. If $\alpha_i + a = \alpha_j \in \pi$ for some $0 \le j \le m$ with $j \ne i$, then according to equality (3),

$$(\alpha_i + \alpha_j)^{-1} = a^{-1} = \alpha_{i+1}^{-1} + \alpha_{j+1}^{-1},$$

which contradicts with Condition 4. If $\alpha_i + a \notin \pi$, then according to equality (3),

$$a^{-1} = \alpha_{i+1}^{-1} + (a+\alpha_i)^{-1}.$$

Notice that $a \neq \alpha_i$, since according to the definition of cycles over $\mathbb{F}_{2^n}$, $\alpha_i \neq \alpha_{i+1}$. Thus the above equality is equivalent to

$$a^2 + \alpha_i a = \alpha_{i+1}\alpha_i.$$

Hence

$$\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i}) = \mathrm{Tr}((\frac{a}{\alpha_i})^2 + \frac{a}{\alpha_i}) = 0,$$

which contradicts with Condition 5. Then the claim holds.

By a similar reason as the proof of Theorem 4, for $a \in \mathbb{F}_{2^n}^*$, $0 \leq i \leq m$, the following results also hold:

- According to Condition 1 and π is a cycle with $0 \notin \pi$ and the elements of π are linear independent over $\mathbb{F}_2$, we have
$$|S_\pi(a, b_i(a))| \leq 2$$
and
$$|S_{\pi/2}(a, b_i(a))| = 0$$
when $|S_\pi(a, b_i(a))| = 2$.
- According to Condition 2, Condition 4 and Lemma 4, we have
$$|S_{\pi/2}(a, b_i(a))| \leq 4.$$
- According to Condition 3, we have
$$|S_{\bar{\pi}}(a, b_i(a))| = 0$$
when $|S_{\pi/2}(a, b_i(a))| = 4$.

Therefore, for $a \in \mathbb{F}_{2^n}^*$, $0 \leq i \leq m$, we have

$$\begin{aligned}|S(a, b_i(a))| &= |S_\pi(a, b_i(a))| + |S_{\pi/2}(a, b_i(a))| + |S_{\bar{\pi}}(a, b_i(a))| \\ &\leq \begin{cases} 2+0+2, & |S_\pi(a, b_i(a))| = 2 \\ 0+4+0, & |S_\pi(a, b_i(a))| = 0 \text{ and } |S_{\pi/2}(a, b_i(a))| = 4 \\ 0+2+2, & |S_\pi(a, b_i(a))| = 0 \text{ and } |S_{\pi/2}(a, b_i(a))| = 2 \end{cases} \\ &\leq 4.\end{aligned}$$

Then we complete the proof. □

Similar as Corollary 2, we have the following result and we omit the proof.

Corollary 3. *Let $n = 2k$, $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ be a cycle permutation over $\mathbb{F}_{2^n}$ with $0 \notin \pi$ and the elements of π are linear independent over $\mathbb{F}_2$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if the following conditions are satisfied:*

1. *For $0 \leq i < j < l \leq m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1} + \alpha_{l+1}^{-1}) \neq (\alpha_i + \alpha_j + \alpha_l)^{-1}$.*
2. *For $0 \leq i < j \leq m$, it holds $(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1}) \neq (\alpha_i + \alpha_j)^{-1}$.*
3. *For $0 \leq i \leq m$, it holds $\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i}) = 1$.*
4. *For $0 \leq i < j \leq m$, it holds $\mathrm{Tr}(\frac{\delta_{i+1,j+1}+\delta_{i,j}}{\alpha_i+\alpha_j}) = 1$, where $\delta_{i,j} = \frac{\alpha_i\alpha_j}{\alpha_i+\alpha_j}$.*

The conditions of Theorem 4, Corollary 2, Theorem 5 and Corollary 3 can be satisfied by lots of elements in $\mathbb{F}_{2^n}$. With the help of Magma, we list some experiment results in Table 3, where l means the length of π. There are too many cycles over $\mathbb{F}_{2^{10}}$ satisfy the conditions of Theorem 5 and Corollary 3, we just test a small part of those cycles due to our computational restriction. That is why we use the symbol "$\geq$" in the last column of table 3.

	$n=6$			$n=8$		$n=10$
	$l=3$	$l=4$	$l=5$	$l=3$	$l=4$	$l=3$
Theorem 4	3	14	245	12	293	33
Corollary 2	2	3	30	9	64	24
Theorem 5	7	19	89	45	1025	≥ 790
Corollary 3	3	2	2	26	276	≥ 281
Total	377			1375		≥ 823

Table 3. Number of CCZ-inequivalence permutations constructed from above results

5 Some special cycles and corresponding permutations

In this section, we investigate the case of some special cycles with length 3. According to Theorem 2, all permutations constructed in this section have nonlinearity not less than $2^{n-1} - 2^{\frac{n}{2}} - 3$, which is very close to the best known nonlinearity over $\mathbb{F}_{2^n}$ for even n.

Theorem 6. *Suppose $n = 2k$, $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, $\pi = (0, 1, \gamma)$ is a cycle over $\mathbb{F}_{2^n}$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ if and only if k is odd.*

Proof. "$\Rightarrow$" Assume k is even. Firstly, note that $\gamma^2 + \gamma = 1$, since $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Then it can be checked that $0, 1, \gamma, \gamma + 1$ satisfy equation

$$\pi(x)^{-1} + \pi(x+1)^{-1} = (\gamma+1)^{-1}.$$

Furthermore, according to Lemma 2, equation $x^{-1} + (x+1)^{-1} = (\gamma+1)^{-1}$ has two roots x_0 and $x_0 + 1$ in $\mathbb{F}_{2^n}$, since

$$\mathrm{Tr}(\gamma+1) = \mathrm{Tr}(\gamma) = \mathrm{Tr}_{2/1}(\gamma \mathrm{Tr}_{n/2}(1)) = 0$$

when k is even. It is easy to check that $\{x_0, x_0+1\} \cap \pi = \emptyset$, then according to equality (1), x_0, x_0+1 also satisfy

$$\pi(x)^{-1} + \pi(x+1)^{-1} = (\gamma+1)^{-1}.$$

Hence the differential uniformity of $\pi(x)^{-1}$ is large than or equals to 6, since $\{x_0, x_0+1\} \cap \{0, 1, \gamma, \gamma+1\} = \emptyset$. This is a contradiction since the differential uniformity of $\pi(x)^{-1}$ is 4.

"$\Leftarrow$" Suppose k is odd. We need to prove that the differential uniformity of $\pi(x)^{-1}$ equals 4. Let $\alpha_0 = 0, \alpha_1 = 1$ and $\alpha_2 = \gamma$. Then according to Lemma 3 and equality (2), we only need to prove that for $a \in \mathbb{F}_{2^n}^*$, $b = b_i(a) = \pi(\alpha_i)^{-1} + \pi(\alpha_i + a)^{-1}$, $i = 0, 1, 2$, it holds

$$|S(a,b)| = |S_\pi(a,b)| + |S_{\pi/2}(a,b)| + |S_{\bar{\pi}}(a,b)| \leq 4.$$

First, we have

$$|S_\pi(a,b)| \leq 2,$$

since $\pi = (0, 1, \gamma)$ is a cycle with length 3. According to Lemma 2, we also have

$$|S_{\bar{\pi}}(a,b)| \leq 2,$$

since $0 \in \pi$.

We claim that it also holds $|S_{\pi/2}(a,b)| \leq 2$. Otherwise, there exists $a \in \mathbb{F}_{2^n}^*$, such that $a + \alpha_i \notin \pi$, $a + \alpha_j \notin \pi$, and $b_i(a) = b_j(a)$ for some $0 \leq i < j \leq 2$. According to equality (3), we have

$$\alpha_{i+1}^{-1} + (a+\alpha_i)^{-1} = b_i(a) = b_j(a) = \alpha_{j+1}^{-1} + (a+\alpha_j)^{-1},$$

which is equivalent to

$$(\frac{a}{\alpha_i+\alpha_j})^2+\frac{a}{\alpha_i+\alpha_j}=(\alpha_i+\alpha_j)^{-1}(\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1})^{-1}+\frac{\alpha_i\alpha_j}{\alpha_i^2+\alpha_j^2},$$

since $a+\alpha_i\notin\pi$, $a+\alpha_j\notin\pi$ and $\alpha_i\neq\alpha_j$. Let $d_{i,j}$ denotes the formula in the right hand of the above equality. Then the above equality implies $\mathrm{Tr}(d_{i,j})=0$. However, it can be checked that

$$\mathrm{Tr}(d_{0,1})=\mathrm{Tr}((1+\gamma^{-1})^{-1})=\mathrm{Tr}(\gamma+1)=1,$$

$$\mathrm{Tr}(d_{0,2})=\mathrm{Tr}(\gamma^{-1})=\mathrm{Tr}(\gamma+1)=1,$$

and

$$\mathrm{Tr}(d_{1,2})=\mathrm{Tr}((\gamma+1)^{-1}\gamma+\frac{\gamma}{\gamma^2+1})=\mathrm{Tr}(\gamma^2)=1,$$

since

$$\mathrm{Tr}(\gamma+1)=\mathrm{Tr}(\gamma)=\mathrm{Tr}_{2/1}(\gamma\mathrm{Tr}_{n/2}(1))=\gamma^2+\gamma=1$$

when k is odd. The contradiction means the claim holds.

At last, we prove that $|S_{\bar{\pi}}(a,b)|=0$ when $|S_{\pi}(a,b)|=2$. Suppose $|S_{\pi}(a,b)|=2$. Then $a=\alpha_i+\alpha_j$ for some $0\leq i<j\leq 2$ and $b=\pi(\alpha_i)^{-1}+\pi(\alpha_i+a)^{-1}=\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1}$. Let $e_{i,j}=(\alpha_i+\alpha_j)(\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1})$. Then it can be checked that

$$\mathrm{Tr}(e_{0,1}^{-1})=\mathrm{Tr}(\frac{1}{1+\gamma^{-1}})=\mathrm{Tr}(\gamma+1)=1,$$

$$\mathrm{Tr}(e_{0,2}^{-1})=\mathrm{Tr}(\frac{1}{\gamma})=\mathrm{Tr}(\gamma+1)=1,$$

and

$$\mathrm{Tr}(e_{1,2}^{-1})=\mathrm{Tr}(\frac{\gamma}{1+\gamma})=\mathrm{Tr}(\gamma^2)=1.$$

Then we have

$$|S_{\bar{\pi}}(a,b)|=0,$$

since $x^{-1}+(x+a)^{-1}=b$ has no roots in $\mathbb{F}_{2^n}$ according to Lemma 2.

Therefore, it holds

$$\begin{aligned}|S(a,b)|&=|S_{\pi}(a,b)|+|S_{\pi/2}(a,b)|+|S_{\bar{\pi}}(a,b)|\\&\leq\begin{cases}2+2+0 & |S_{\pi}(a,b)|=2\\0+2+2 & |S_{\pi}(a,b)|=0\end{cases}\\&\leq 4\end{aligned}$$

and the proof is completed. □

Similar as the proof of Theorem 6, the following results can also be proved.

Corollary 4. *Suppose $n=2k$, $\gamma\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$. Then for cycle $\pi=(1,\gamma,\gamma^2)$, $\pi(x)^{-1}$ is a differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ if and only if k is odd.*

Corollary 5. *Suppose $\gamma\in\mathbb{F}_{2^{2k}}\setminus\mathbb{F}_2$, $\pi=(0,1,\gamma)$ is a cycle over $\mathbb{F}_{2^n}$. If $\mathrm{Tr}(\frac{1}{\gamma})=\mathrm{Tr}(\frac{1}{\gamma+1})=1$, then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^{2k}}$.*

Proof. When $\gamma \notin \mathbb{F}_{2^2}$, it holds $1+\gamma^{-1} \neq (1+\gamma)^{-1}$, which means Condition 1 of Corollary 2 is satisfied. Moreover, it can be checked that Condition 2 of Corollary 2 is also satisfied since $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$. Then the result follows from Corollary 2.

When $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, the results follows from Theorem 6, since for $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, $\mathrm{Tr}(\gamma) = 1$ if and only if k is odd. □

Next, we give a complete characterization of cycles of the type $\pi = (0, 1, \gamma)$, where $\gamma \in \mathbb{F}_{2^n}$, such that $\pi(x)^{-1}$ is a differentially 4-uniform permutation.

Theorem 7. *Suppose $n = 2k$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ and $\pi = (0, 1, \gamma)$ is a cycle over $\mathbb{F}_{2^n}$. Then $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^{2k}}$ if and only if $\gamma \notin \{\frac{i^2+i+1}{i^4+i+1}, \frac{i^4+i^2}{i^2+i+1} \mid i \in \mathbb{F}_{2^{2k}}\}$.*

Proof. Let $\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = \gamma$, $b_i(a) = \pi(\alpha_i)^{-1} + \pi(\alpha_i + a)^{-1}$, $i = 0, 1, 2$ and

$$S = \{\frac{i^2+i+1}{i^4+i+1}, \frac{i^4+i^2}{i^2+i+1} \mid i \in \mathbb{F}_{2^{2k}}\}.$$

"$\Leftarrow$" Firstly, it should be noticed that $1, \gamma$ are linear independent over $\mathbb{F}_2$, and Condition 1 of Theorem 4 is satisfied since $1 + \gamma^{-1} \neq (\gamma + 1)^{-1}$ for $\gamma \notin \mathbb{F}_{2^2}$.

Secondly, Condition 2 of Theorem 4 holds when $\gamma \notin S$. Let $i = 0, j = 1, l = 2$. Then the system of equations in Condition 2 of Theorem 4 becomes

$$\begin{cases} x^2 + x &= (1+\gamma^{-1})^{-1} \\ x^2 + \gamma x &= \gamma. \end{cases}$$

Adding two equations we get

$$x = \frac{\gamma^2}{\gamma^2+1},$$

and it is the solution of the above system of equations if and only if

$$\gamma = x^2 + \gamma x = \frac{\gamma^4}{\gamma^4+1} + \frac{\gamma^3}{\gamma^2+1} = \frac{\gamma^5+\gamma^4+\gamma^3}{\gamma^4+1},$$

which is equivalent to $\gamma^3 + \gamma^2 + 1 = 0$. Notice that $\gamma \notin \mathbb{F}_{2^2}$, then $\gamma^2 + \gamma + 1 \neq 0$ and

$$\frac{\gamma^4+\gamma^2}{\gamma^2+\gamma+1} = \frac{\gamma^3+\gamma^2+\gamma}{\gamma^2+\gamma+1} = \gamma,$$

which means $\gamma \in S$.

Thirdly, we prove that Condition 3 of Theorem 4 holds when $\gamma \notin S$. For $0 \leq i < j \leq 2$, let

$$A_{i,j} = \{\alpha_i + \alpha : \alpha \in \pi\} \cup \{\alpha_j + \alpha : \alpha \in \pi\},$$

$$S_{i,j} = \{a \in \mathbb{F}_{2^n} \setminus A_{i,j} : a^2 + (\alpha_i + \alpha_j)a = (\alpha_i + \alpha_j)(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1} + \alpha_i\alpha_j\},$$

and

$$\Gamma_{i,j} = \{\gamma \in \mathbb{F}_{2^n} : S_{i,j} \neq \emptyset \text{ and } \mathrm{Tr}((ab_i(a))^{-1}) = 0 \text{ for some } a \in S_{i,j}\},$$

where $b_i(a) = \alpha_{i+1}^{-1} + (a + \alpha_i)^{-1}$. Then we only need to prove that

$$S = \Gamma_{0,1} \cup \Gamma_{0,2} \cup \Gamma_{1,2}.$$

It is easy to see that

$$A_{0,1} = A_{0,2} = A_{1,2} = \{0, 1, \gamma, \gamma + 1\}.$$

Let $A = \{0, 1, \gamma, \gamma + 1\}$. Then we characterize $\Gamma_{i,j}$ for $0 \leq i < j \leq 2$ as follows.

Case 1. $i = 0, j = 1$. Then and $a \in S_{0,1}$ if and only if $a \notin A$ and

$$a^2 + a = (1 + \gamma^{-1})^{-1} = \frac{\gamma}{\gamma + 1},$$

from which we get $\gamma = \frac{a^2+a}{a^2+a+1}$. Note that $\gamma \notin \mathbb{F}_{2^2}$, then it can be checked easily that for $x \in A$, it holds $x^2 + x \neq \frac{\gamma}{\gamma+1}$. Thus,

$$S_{0,1} = \begin{cases} \emptyset & \mathrm{Tr}(\frac{\gamma}{\gamma+1}) = 1 \\ \{a, a+1\} & \mathrm{Tr}(\frac{\gamma}{\gamma+1}) = 0 \text{ and } \frac{\gamma}{\gamma+1} = a^2 + a, \end{cases}$$

Note that $\mathrm{Tr}(\frac{1}{ab_0(a)}) = \mathrm{Tr}(\frac{1}{a(1+a^{-1})}) = \mathrm{Tr}(\frac{1}{a+1})$, then $\mathrm{Tr}(\frac{1}{ab_0(a)}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$ such that $\frac{1}{a+1} = i + i^2$. Therefore, $a = \frac{1}{i+i^2} + 1$ and

$$\gamma = \frac{a^2 + a}{a^2 + a + 1} = \frac{i^2 + i + 1}{i^4 + i + 1}.$$

Similarly, it can be proved that $\mathrm{Tr}(\frac{1}{(a+1)b_0(a+1)}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$ such that $\gamma = \frac{i^2+i+1}{i^4+i+1}$. Thus

$$\Gamma_{0,1} = \{\frac{i^2 + i + 1}{i^4 + i + 1} \mid i \in \mathbb{F}_{2^n}\}.$$

Case 2. $i = 0, j = 2$. Then $a \in S_{0,2}$ if and only if $a \notin A$ and

$$a^2 + \gamma a = \gamma,$$

from which we get $\frac{1}{\gamma} = \frac{1}{a} + \frac{1}{a^2}$. It also can be checked that for $x \in A$, it holds $x^2 + \gamma x \neq \gamma$ since $\gamma \notin \mathbb{F}_{2^2}$. Thus

$$S_{0,2} = \begin{cases} \emptyset & \mathrm{Tr}(\frac{1}{\gamma}) = 1 \\ \{\frac{1}{c}, \frac{1}{c+1}\} & \mathrm{Tr}(\frac{1}{\gamma}) = 0 \text{ and } \frac{1}{\gamma} = c^2 + c. \end{cases}$$

Note that $\mathrm{Tr}(\frac{1}{c^{-1}b_0(c^{-1})}) = \mathrm{Tr}(\frac{c}{(1+(c^{-1})^{-1})}) = \mathrm{Tr}(\frac{c}{c+1}) = \mathrm{Tr}(\frac{1}{c+1})$, then $\mathrm{Tr}(\frac{1}{c^{-1}b_0(c^{-1})}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$ such that $\frac{1}{c+1} = i^2 + i$. Therefore, $c = \frac{1}{i^2+i} + 1$ and

$$\gamma = \frac{1}{c + c^2} = \frac{i^4 + i^2}{i^2 + i + 1}.$$

Similarly, it can be proved that $\mathrm{Tr}(\frac{1}{(c+1)^{-1}b_0((c+1)^{-1})}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$ such that $\gamma = \frac{i^4+i^2}{i^2+i+1}$. Thus

$$\Gamma_{02} = \{\frac{i^4 + i^2}{i^2 + i + 1} \mid i \in \mathbb{F}_{2^n}\}.$$

Case 3. $i = 1, j = 2$. Then $a \in S_{1,2}$ if and only if $a \notin A$ and

$$a^2 + (\gamma + 1)a = \gamma^2,$$

from which we get $(\frac{a}{\gamma+1})^2 + \frac{a}{\gamma+1} = (\frac{\gamma}{\gamma+1})^2$. It also can be checked that for $x \in A$, it holds $x^2 + (\gamma + 1)x \neq \gamma^2$ since $\gamma \notin \mathbb{F}_{2^2}$. Thus

$$S_{12} = \begin{cases} \emptyset & \mathrm{Tr}(\frac{\gamma}{\gamma+1}) = 1 \\ \{(\gamma + 1)c^2, (\gamma + 1)(c^2 + 1)\} & \mathrm{Tr}(\frac{\gamma}{\gamma+1}) = 0 \text{ and } \frac{\gamma}{\gamma+1} = c^2 + c. \end{cases}$$

Note that for $a \in S_{1,2}$, $b_1(a) = b_2(a)$. Let $a = (\gamma+1)c^2$. Then

$$\mathrm{Tr}(\frac{1}{ab_1(a)}) = \mathrm{Tr}(\frac{1}{ab_2(a)}) = \mathrm{Tr}(\frac{1}{a(a+\gamma)^{-1}}) = \mathrm{Tr}(\frac{\gamma}{a}) = \mathrm{Tr}(\frac{\gamma}{(\gamma+1)c^2}) = \mathrm{Tr}(\frac{c^2+c}{c^2}) = \mathrm{Tr}(\frac{1}{c}).$$

Hence $\mathrm{Tr}(\frac{1}{ab_2(a)}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$ such that $\frac{1}{c} = i + i^2$ and

$$\gamma = \frac{c^2+c}{c^2+c+1} = \frac{i^2+i+1}{i^4+i+1}.$$

Similarly, it can be proved that when $a = (\gamma+1)(c^2+1)$, $\mathrm{Tr}(\frac{1}{ab_1(a)}) = 0$ if and only if there exists $i \in \mathbb{F}_{2^n}$, such that $\gamma = \frac{i^2+i+1}{i^4+i+1}$. Thus

$$\mathit{\Gamma}_{1,2} = \{\frac{i^2+i+1}{i^4+i+1} \mid i \in \mathbb{F}_{2^n}\} = \mathit{\Gamma}_{0,1}.$$

Therefore, it holds $S = \mathit{\Gamma}_{0,1} \cup \mathit{\Gamma}_{0,2} \cup \mathit{\Gamma}_{1,2}$. Hence when $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$ and $\gamma \notin S$, $\pi(x)^{-1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}$ according to Theorem 4.

"$\Rightarrow$" Assume $\gamma \in S \setminus \mathbb{F}_{2^2}$, then there exists $i \in \mathbb{F}_{2^n}$ such that $\gamma = \frac{i^2+i+1}{i^4+i+1}$ or $\gamma = \frac{i^4+i^2}{i^2+i+1}$.

We investigate the case of $\gamma = \frac{i^2+i+1}{i^4+i+1}$ firstly. Let $a = \frac{1}{i^2+i}+1$. We will show that $|S(a, b_0(a))| \geq 6$. First, it should be noticed that $i \notin \mathbb{F}_{2^2}$ and $i^4+i+1 \neq 0$ since $\gamma \notin \mathbb{F}_{2^2}$.

Let $A = \{0, 1, \gamma, \gamma+1\}$. Then we have $a \notin A$. Otherwise, without loss of generality, we assume that

$$\frac{i^2+i+1}{i^2+i} = a = \gamma = \frac{i^2+i+1}{i^4+i+1}.$$

Notice that $i \notin \mathbb{F}_{2^2}$, then $i^2+i+1 \neq 0$. Thus the above equality is equivalent to

$$i^2+i = i^4+i+1,$$

which is equivalent to $i^2+i+1 = 0$. This contradicts with $i \notin \mathbb{F}_{2^2}$. The cases of other elements in A do not equal a can be proved similarly. Hence $a \notin \pi$ and $a+1 \notin \pi$. Then according to equality (3), we have

$$b_0(a) = 1 + (\frac{1}{i^2+i}+1)^{-1} = \frac{i^4+i+1}{i^2+i+1} + (i^2+i) = b_1(a).$$

According to equality (1), $0, a, 1, a+1$ satisfy equation

$$\pi(x)^{-1} + \pi(x+a)^{-1} = b_0(a),$$

which means $|S_{\pi/2}(a, b_0(a))| \geq 4$. Moreover, we also have

$$\mathrm{Tr}(\frac{1}{ab_0(a)}) = \mathrm{Tr}(((\frac{1}{i^2+i}+1)\frac{1}{i^2+i+1})^{-1}) = \mathrm{Tr}(i^2+i) = 0,$$

then according to Lemma 2,

$$x^{-1} + (x+a)^{-1} = b_0(a)$$

has two roots x_0, x_0+a in $\mathbb{F}_{2^n}$. Next, we check that

$$\{x_0, x_0+a\} \cap \pi = \emptyset.$$

Note that $b_0(a) = 1 + a^{-1}$, thus $x_0 \neq 0$ and $x_0 \neq 1$. If $x_0 = \gamma$, then $\gamma^{-1} + (\gamma + a)^{-1} = 1 + a^{-1}$ is equivalent to

$$(\frac{a}{\gamma})^2 + \frac{a}{\gamma} = \frac{1}{\gamma + 1}.$$

Note that $\frac{a}{\gamma} = \frac{i^4+i+1}{i^2+i}$, $\gamma + 1 = \frac{i^4+i^2}{i^4+i+1}$, and $i^4 + i + 1 \neq 0$, then the above equality is equivalent to $i^2 + i = 0$, which is a contradiction since $i \notin \mathbb{F}_{2^2}$. It can be checked that $x_0 \neq a + \alpha_i$ for $0 \leq i \leq 2$ similarly.

Then according to equality (1), $x_0, x_0 + a$ also satisfy equation

$$\pi(x)^{-1} + \pi(x + a)^{-1} = b_0(a).$$

Therefore,

$$|S(a, b_0(a))| = |S_\pi(a, b_0(a))| + |S_{\pi/2}(a, b_0(a))| + |S_{\bar{\pi}}(a, b_0(a))| \geq 0 + 4 + 2 = 6.$$

This is a contradiction, since the differential uniformity of $\pi(x)^{-1}$ is 4.

The case of $\gamma = \frac{i^4+i^2}{i^2+i+1}$ is similar as above. Let $a = \frac{i^2+i}{i^2+i+1}$. Then it is easy to see that $a \notin A$, $b_0(a) = b_2(a)$ and $\mathrm{Tr}(\frac{1}{ab_0(a)}) = 0$. Similarly as above, it can be checked that $\{x_0, x_0 + a\} \cap \pi = \emptyset$, where $x_0, x_0 + a$ are two roots of equation $x^{-1} + (x + a)^{-1} = b_0(a)$ in $\mathbb{F}_{2^n}$. Hence $|S(a, b_0(a))| \geq 6$, which is a contradiction.

Then we complete the proof. □

Proposition 1. *Let $n = 2k$, $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$ and $S = \{\frac{i^2+i+1}{i^4+i+1}, \frac{i^4+i^2}{i^2+i+1} \mid i \in \mathbb{F}_{2^{2k}}\}$. Then $\gamma \in S$ if and only if k can be divided by 4.*

Proof. Note that $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, then $\gamma^2 + \gamma + 1 = 0$. $\gamma \in S$ if and only if there exists $i \in \mathbb{F}_{2^n}$, such that $\gamma = \frac{i^2+i+1}{i^4+i+1}$ or $\gamma = \frac{i^4+i^2}{i^2+i+1}$. Let $j = i^2 + i$. Then

$$\gamma = \frac{i^2 + i + 1}{i^4 + i + 1} = \frac{j + 1}{j^2 + j + 1}$$

is equivalent to

$$0 = j^2 + \frac{\gamma + 1}{\gamma} j + \frac{\gamma + 1}{\gamma} = j^2 + \gamma j + \gamma,$$

since $\gamma^2 + \gamma + 1 = 0$. Similar, $\gamma = \frac{i^4+i^2}{i^2+i+1} = \frac{j^2}{j+1}$ is also equivalent to the above equality.

Then $\gamma \in S$ if and only if there exists $j \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(j) = 0$, such that

$$j^2 + \gamma j + \gamma = 0,$$

which means j is a root of equation

$$(\frac{x}{\gamma})^2 + \frac{x}{\gamma} + \frac{1}{\gamma} = 0$$

in $\mathbb{F}_{2^n}$. Note that for $\gamma \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, it holds

$$\mathrm{Tr}(\gamma) = \mathrm{Tr}_{2/1}(\gamma \mathrm{Tr}_{n/2}(1)) = \begin{cases} 0 & k \text{ even} \\ 1 & k \text{ odd.} \end{cases}$$

Then equation $(\frac{x}{\gamma})^2+\frac{x}{\gamma}+\frac{1}{\gamma}=0$ has solutions in $\mathbb{F}_{2^n}$ if and only if k is even. When k is even, there exists $d_1\in\mathbb{F}_{2^n}$, such that $\frac{1}{\gamma}=\gamma+1=d_1+d_1^2$. Hence the solutions of the above equation are $d_1\gamma$ and $d_1\gamma+\gamma$. Note that $\gamma+\gamma^2=1$, then $d_1^4+d_1=1$ and

$$\begin{aligned}\mathrm{Tr}(d_1\gamma+\gamma)=\mathrm{Tr}(d_1\gamma)&=\sum_{i=0}^{2k-1}(d_1\gamma)^{2^i}\\&=\sum_{i=0}^{k-1}(d_1\gamma)^{2^{2i}}+\sum_{i=0}^{k-1}(d_1\gamma)^{2^{2i+1}}\\&=\sum_{i=0}^{\frac{k}{2}-1}(d_1\gamma+(d_1\gamma)^4)^{2^{4i}}+\sum_{i=0}^{\frac{k}{2}-1}(d_1\gamma+(d_1\gamma)^4)^{2^{4i+1}}\\&=\sum_{i=0}^{\frac{k}{2}-1}(\gamma)^{2^{4i}}+\sum_{i=0}^{\frac{k}{2}-1}(\gamma)^{2^{4i+1}}\\&=\sum_{i=0}^{\frac{k}{2}-1}(\gamma^2+\gamma)^{2^{4i}}\\&=\frac{k}{2}\bmod 2.\end{aligned}$$

Thus there exists $j\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}(j)=0$, such that $j^2+\gamma j+\gamma=0$ if and only if k is divided by 4. Then we complete the proof. □

Base on Theorem 6, Theorem 7 and Proposition 1, we have the following result.

Corollary 6. *Suppose $n=2k$, $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, $\pi=(0,1,\gamma)$ is a cycle over $\mathbb{F}_{2^n}$. Let $S=\{\frac{i^2+i+1}{i^4+i+1},\frac{i^4+i^2}{i^2+i+1}\mid i\in\mathbb{F}_{2^{2k}}\}$. Then the following statements hold.*

1. *If k is odd or k can be divided by 4, then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if $\gamma\notin S$.*
2. *If k can be divided by 2 but not 4, then the differential uniformity of $\pi(x)^{-1}$ equals 4 if and only if $\gamma\notin(S\cup\mathbb{F}_{2^2})$.*

At the end of this section, we characterize cycles of the type $\pi=(1,\gamma,\gamma+1)$, such that $\pi(x)^{-1}$ is of differential uniformity 4.

Theorem 8. *Suppose $n=2k$, $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ and $\pi=(1,\gamma,\gamma+1)$ is a cycle over $\mathbb{F}_{2^n}$. Then the differential uniformity of $\pi(x)^{-1}$ is 4 if and only if $\mathrm{Tr}(\gamma)=\mathrm{Tr}(\frac{1}{\gamma})=\mathrm{Tr}(\frac{1}{\gamma+1})=1$.*

Proof. The case of $\gamma\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$ follows from Corollary 4, since for $\gamma\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$, $\mathrm{Tr}(\gamma)=1$ if and only if k is odd. Thus we suppose $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^2}$ hereafter in the proof.

"⇒" Let $\alpha_0=1,\alpha_1=\gamma$, $\alpha_2=\gamma+1$. Note that $\mathrm{Tr}(\frac{\alpha_2}{\alpha_1})=\mathrm{Tr}(\frac{\gamma+1}{\gamma})=\mathrm{Tr}(\frac{1}{\gamma})$, then we only need to prove that $\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i})=1$ for $0\le i\le 2$. Assume there exists $0\le i\le 2$, such that $\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i})=0$. Then equation

$$(\frac{x}{\alpha_i})^2+\frac{x}{\alpha_i}=\frac{\alpha_{i+1}}{\alpha_i}$$

has 2 roots in $\mathbb{F}_{2^n}$, which we denote by a_0 and $a_0+\alpha_i$ respectively. It should be noticed that 0 is not a solution of the above equation since $\alpha_i\neq 0$ for $0\le i\le 2$, then $a_0\neq 0$ and $a_0+\alpha_i\neq 0$. We are going to show that there exists $a\in\{a_0,a_0+\alpha_i\}$, such that $\pi(x)^{-1}+\pi(x+a)^{-1}=a^{-1}$ has at least 6 roots in $\mathbb{F}_{2^n}$.

Firstly, we prove that for $a\in\{a_0,a_0+\alpha_i\}$, it holds

$$\{\alpha_i,a+\alpha_i\}\subseteq S_{\pi/2}(a,a^{-1})$$

and hence $|S_{\pi/2}(a,a^{-1})| \geq 2$. Note that $(\frac{a}{\alpha_i})^2+\frac{a}{\alpha_i}=\frac{\alpha_{i+1}}{\alpha_i}$ is equivalent to

$$\alpha_{i+1}^{-1}+(\alpha_i+a)^{-1}=a^{-1},$$

then according to equality (1), we only need to prove that $\{\alpha_i, a+\alpha_i\}\cap\pi=\{\alpha_i\}$, which is equivalent to prove that for $a\in\{a_0, a_0+\alpha_i\}$, it holds

$$a+\alpha_i\notin\pi=(\alpha_0,\alpha_1,\alpha_2)=(1,\gamma,\gamma+1).$$

Assume $a+\alpha_i\in\pi$, then we have $a+\alpha_i=\alpha_{i+1}$ or $a+\alpha_i=\alpha_{i-1}$ since $a\neq 0$. When $a=\alpha_i+\alpha_{i-1}$, we have

$$\frac{\alpha_{i+1}}{\alpha_i}=(\frac{\alpha_i+\alpha_{i-1}}{\alpha_i})^2+\frac{\alpha_i+\alpha_{i-1}}{\alpha_i}=(\frac{\alpha_{i-1}}{\alpha_i})^2+\frac{\alpha_{i-1}}{\alpha_i},$$

which is a contradiction since the above equality is not hold for $i=0,1,2$. For example, when $i=1$, the above equality becomes $\frac{\gamma+1}{\gamma}=\frac{1}{\gamma^2}+\frac{1}{\gamma}$, from which we get $\gamma=1$. This is a contradiction since $\gamma\notin\mathbb{F}_{2^2}$. The case of $i=0,2$ can be checked similarly. When $a=\alpha_i+\alpha_{i+1}$, we have

$$\frac{\alpha_{i+1}}{\alpha_i}=(\frac{\alpha_i+\alpha_{i+1}}{\alpha_i})^2+\frac{\alpha_i+\alpha_{i+1}}{\alpha_i}=(\frac{\alpha_{i+1}}{\alpha_i})^2+\frac{\alpha_{i+1}}{\alpha_i},$$

which is equivalent to $\alpha_{i+1}=0$ or $\alpha_i=0$. This is a contradiction since $0\notin\pi$.

According to Lemma 2, $x^{-1}+(x+a)^{-1}=a^{-1}$ has 4 roots in $\mathbb{F}_{2^n}$, which are $0, a, a\omega, a\omega^2$ respectively, where $\omega\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$. Next, we prove that there exists $a\in\{a_0, a_0+\alpha_i\}$, such that

$$S_{\overline{\pi}}(a,a^{-1})=\{0,a,a\omega,a\omega^2\}.$$

According to equality (1), we only need to show that there exists $a\in\{a_0,a_0+\alpha_i\}$, such that

$$\{0,a,a\omega,a\omega^2\}\cap\pi=\emptyset.$$

Similar as above, for $a\in\{a_0,a_0+\alpha_i\}$, it is easy to see that $\{0,a\}\cap\pi=\emptyset$. Then we only need to prove that there exists $a\in\{a_0,a_0+\alpha_i\}$, such that

$$\{a\omega,a\omega^2\}\cap\pi=\emptyset,$$

where $\omega\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$. Assume $\{a_0\omega,a_0\omega^2\}\cap\pi\neq\emptyset$ and $\{(a_0+\alpha)\omega,(a_0+\alpha_i)\omega^2\}\cap\pi\neq\emptyset$, then there exist $c\in\{a_0\omega,a_0\omega^2\}$ and $d\in\{(a_0+\alpha_i)\omega,(a_0+\alpha_i)\omega^2\}$, such that

$$c+d\in\varDelta_\pi=\{x+y\mid x,y\in\pi\text{ and }x\neq y\}=\{1,\gamma,\gamma+1\}=\{\alpha_j\mid 0\leq j\leq 2\}.$$

Then we have the following cases:

Case 1. $c=a_0\omega, d=(a_0+\alpha_i)\omega$. Then $c+d=\alpha_i\omega$. Note that $\omega\in\mathbb{F}_{2^2}\setminus\mathbb{F}_2$, then $\alpha_i\omega=\alpha_{i+1}$ or $\alpha_i\omega=\alpha_{i-1}$ when $c+d\in\varDelta_\pi$. If $\alpha_i\omega=\alpha_{i+1}$ for some $0\leq i\leq 2$, then $\omega\in\{\gamma,1+\frac{1}{\gamma},\frac{1}{\gamma+1}\}$, which is a contradiction since $\gamma\notin\mathbb{F}_{2^2}$. Similar, $\alpha_i\omega\neq\alpha_{i-1}$ for $0\leq i\leq 2$.

Case 2. $c=a_0\omega, d=(a_0+\alpha_i)\omega^2$. Then

$$c+d=a_0(\omega+\omega^2)+\alpha_i\omega^2=a_0+\alpha_i\omega^2$$

and we have the following subcases:

Case 2.1 $c+d=\alpha_i$. Then $a_0=\alpha_i(\omega^2+1)=\alpha_i\omega$ and

$$\frac{\alpha_{i+1}}{\alpha_i}=(\frac{\alpha_i\omega}{\alpha_i})^2+\frac{\alpha_i\omega}{\alpha_i}=1,$$

which is a contradiction since $a_i\neq\alpha_{i+1}$ for $0\leq i\leq 2$.

Case 2.2 $c + d = \alpha_{i-1}$. Then $a_0 = \alpha_i\omega^2 + \alpha_{i-1}$ and

$$\frac{\alpha_{i+1}}{\alpha_i} = (\frac{\alpha_i\omega^2 + \alpha_{i-1}}{\alpha_i})^2 + \frac{\alpha_i\omega^2 + \alpha_{i-1}}{\alpha_i} = 1 + (\frac{\alpha_{i-1}}{\alpha_i})^2 + \frac{\alpha_{i-1}}{\alpha_i},$$

which is a contradiction since it can be checked easily that the above equality is not hold for $0 \leq i \leq 2$.

Case 2.2 $c + d = \alpha_{i+1}$. Then $a_0 = \alpha_i\omega^2 + \alpha_{i+1}$ and

$$\frac{\alpha_{i+1}}{\alpha_i} = (\frac{\alpha_i\omega^2 + \alpha_{i+1}}{\alpha_i})^2 + \frac{\alpha_i\omega^2 + \alpha_{i+1}}{\alpha_i} = 1 + (\frac{\alpha_{i+1}}{\alpha_i})^2 + \frac{\alpha_{i+1}}{\alpha_i},$$

which is equivalent to $\alpha_{i+1} = \alpha_i$. This is a contradiction since $a_i \neq \alpha_{i+1}$ for $0 \leq i \leq 2$.

Case 3. $c = a_0\omega^2, d = (a_0 + \alpha_i)\omega$. Then

$$c + d = a_0(\omega^2 + \omega) + \alpha_i\omega = a_0 + \alpha_i\omega$$

and it can be proved similarly as Case 2 that $c + d \notin \Delta_\pi$.

Case 4. $c = a_0\omega^2, d = (a_0 + \alpha_i)\omega^2$. Then $c + d = \alpha_i\omega^2$ and it can be proved similarly as Case 1 that $c + d \notin \Delta_\pi$.

Then $\{a_0\omega, a_0\omega^2\} \cap \pi \neq \emptyset$ and $\{(a_0 + 1)\omega, (a_0 + 1)\omega^2\} \cap \pi \neq \emptyset$ can not hold simultaneously. Choose $a \in \{a_0, a_0 + \alpha_i\}$, such that $\{a\omega, a\omega^2\} \cap \pi = \emptyset$. Then we have

$$|S(a, a^{-1})| = |S_\pi(a, a^{-1})| + |S_{\pi/2}(a, a^{-1})| + |S_{\bar{\pi}}(a, a^{-1})| \geq 0 + 2 + 4 = 6,$$

which is a contradiction since the differential uniformity of $\pi(x)^{-1}$ is 4.

"⇐" Let $\alpha_0 = 1, \alpha_1 = \gamma$, $\alpha_2 = \gamma + 1$ and $b_i(a) = \pi(\alpha_i)^{-1} + \pi(\alpha_i + a)^{-1}$ for $i = 0, 1, 2$. According to Lemma 3 and equality (2), we only need to prove that for $a \in \mathbb{F}_{2^n}^*$, $b = b_i(a)$, $i = 0, 1, 2$, it holds

$$|S(a, b)| = |S_\pi(a, b)| + |S_{\pi/2}(a, b)| + |S_{\bar{\pi}}(a, b)| \leq 4.$$

Firstly, it is easy to see $|S_\pi(a, b)| \leq 2$, since $\pi = (1, \gamma, \gamma + 1)$ is a cycle of length 3.

Secondly, we have $|S_{\bar{\pi}}(a, b)| \leq 2$ for $a \in \mathbb{F}_{2^n}^*$, $b = b_i(a)$, $i = 0, 1, 2$. The proof is similar as the claim in the proof of Theorem 5, since $\mathrm{Tr}(\frac{\alpha_{i+1}}{\alpha_i}) = 1$ for $i = 0, 1, 2$ and $(\alpha_i + \alpha_j)^{-1} \neq \alpha_{i+1}^{-1} + \alpha_{j+1}^{-1}$ for $0 \leq i < j \leq 2$, which can be checked easily.

Thirdly, we prove that $|S_{\pi/2}(a, b)| \leq 2$ for $a \in \mathbb{F}_{2^n}^*$, $b = b_i(a)$, $i = 0, 1, 2$. We only need to show that there do not exist $0 \leq i < j \leq 2$ and $a \in \mathbb{F}_{2^n}^*$ with $a + \alpha_i \notin \pi$, $a + \alpha_j \notin \pi$, such that

$$\alpha_{i+1}^{-1} + (a + \alpha_i)^{-1} = b_i(a) = b_j(a) = \alpha_{j+1}^{-1} + (a + \alpha_j)^{-1}.$$

The above equality is equivalent to

$$(\frac{a}{\alpha_i + \alpha_j})^2 + \frac{a}{\alpha_i + \alpha_j} = \frac{(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1}}{\alpha_i + \alpha_j} + \frac{\alpha_i\alpha_j}{\alpha_i^2 + \alpha_j^2}.$$

Let

$$\theta_{i,j} = \frac{(\alpha_{i+1}^{-1} + \alpha_{j+1}^{-1})^{-1}}{\alpha_i + \alpha_j} + \frac{\alpha_i\alpha_j}{\alpha_i^2 + \alpha_j^2} = \frac{1}{\alpha_i + \alpha_j}(\frac{\alpha_{i+1}\alpha_{j+1}}{\alpha_{i+1} + \alpha_{j+1}} + \frac{\alpha_i\alpha_j}{\alpha_i + \alpha_j}).$$

Then we only need to show that $\mathrm{Tr}(\theta_{i,j}) = 1$ for $0 \leq i < j \leq 2$, which can be checked as follows:

$$\mathrm{Tr}(\theta_{0,1}) = \mathrm{Tr}(\frac{1}{\gamma+1}(\gamma^2+\gamma+\frac{\gamma}{\gamma+1})) = \mathrm{Tr}(\gamma+\frac{1}{\gamma+1}+\frac{1}{\gamma^2+1}) = \mathrm{Tr}(\gamma) = 1,$$

$$\mathrm{Tr}(\theta_{0,2}) = \mathrm{Tr}(\frac{1}{\gamma}(\frac{\gamma}{\gamma+1}+\frac{\gamma+1}{\gamma})) = \mathrm{Tr}(\frac{1}{\gamma+1}+\frac{1}{\gamma}+\frac{1}{\gamma^2}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1,$$

and

$$\mathrm{Tr}(\theta_{1,2}) = \mathrm{Tr}(\frac{\gamma+1}{\gamma}+\gamma^2+\gamma) = \mathrm{Tr}(\frac{1}{\gamma}) = 1.$$

Thus the claim holds.

At last, we show that $|S_{\bar{\pi}}(a,b)| = 0$ when $|S_\pi(a,b)| = 2$ for $a \in \mathbb{F}_{2^n}^*$ and $b = b_i(a)$, $i = 0,1,2$. Note that $|S_\pi(a,b)| = 2$ if and only if there exist $0 \le i < j \le 2$, such that $a = \alpha_i + \alpha_j$ and $b = \alpha_{i+1}^{-1} + \alpha_{j+1}^{-1}$. According to Lemma 2, we only need to show that for $0 \le i < j \le 2$, it holds

$$\mathrm{Tr}(\frac{1}{(\alpha_i+\alpha_j)(\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1})}) = 1.$$

Let

$$\delta_{i,j} = \frac{1}{(\alpha_i+\alpha_j)(\alpha_{i+1}^{-1}+\alpha_{j+1}^{-1})} = \frac{\alpha_{i+1}\alpha_{j+1}}{(\alpha_i+\alpha_j)(\alpha_{i+1}+\alpha_{j+1})}$$

for $0 \le i < j \le 2$. Then it can be checked that

$$\mathrm{Tr}(\delta_{0,1}) = \mathrm{Tr}(\frac{\gamma(\gamma+1)}{1+\gamma}) = \mathrm{Tr}(\gamma) = 1,$$

$$\mathrm{Tr}(\delta_{0,2}) = \mathrm{Tr}(\frac{\gamma}{\gamma(\gamma+1)}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$$

and

$$\mathrm{Tr}(\delta_{1,2}) = \mathrm{Tr}(\frac{\gamma+1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma}) = 1.$$

Thus $|S_{\bar{\pi}}(a,b)| = 0$ when $|S_\pi(a,b)| = 2$.

Therefore, for $a \in \mathbb{F}_{2^n}^*$ and $b = b_i(a)$, $i = 0,1,2$, we have

$$\begin{aligned} |S(a,b)| &= |S_\pi(a,b)| + |S_{\pi/2}(a,b)| + |S_{\bar{\pi}}(a,b)| \\ &\le \begin{cases} 2+2+0 & |S_\pi(a,b)| = 2 \\ 0+2+2 & |S_\pi(a,b)| = 0 \end{cases} \\ &\le 4. \end{aligned}$$

Then we complete the proof. □

6 Conclusion

In the present paper, we further study a secondary construction method of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$, which is composing the inverse function and cycles over $\mathbb{F}_{2^{2k}}$. Up to CCZ-equivalence, all optimal permutations over $\mathbb{F}_{2^4}$ can be constructed with this method and a new differentially 4-uniform permutation with the best known nonlinearity over $\mathbb{F}_{2^{2k}}$ with k odd is given. A lower bound on nonlinearity of permutations constructed with the method in the present paper is given. For general cycles, two sufficient conditions are given such that the differential uniformity of the corresponding compositions equals 4. Over small fields, it is shown that numerous differentially 4-uniform permutation can be constructed with these sufficient conditions. For some special cycles, sufficient and necessary conditions are given such that corresponding permutations are differentially 4-uniform.

References

1. Biham E., Shamir A.: Defferential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3-72 (1991).
2. Bracken C., Byrne E., Markin N., McGuire G.: New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields Their Appl. 14(3), 703-714 (2008)
3. 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).
4. Bracken C., Byrne E., Markin N., McGuire G.: A few more quadratic APN functions. Cryptogr. Commun. 3(1), 43-53(2011).
5. Bracken C., Tan C.H., Tan Y.: Binomial differentially 4 uniform permutations with high nonlinearity. Finite Fields and Their Applications 18(3), 537-546 (2012).
6. Browning K. A., Dillon J. F., Kibler R. E., McQuistan M. T.: APN polynomials and related codes. J. Comb. Inf. Syst. Sci., 34(1-4), 135-159 (2009).
7. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. on Inform. Theory, 52(3), 1141-1152 (2006).
8. Budaghyan L.: The simplest method for constructing APN polynomials EA-inequivalent to power functions. WAIFI 2007, LNCS 4547, 177-188, 2007.
9. Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. on Inform. Theory, 54(9), 4218-4229 (2008).
10. Budaghyan L., Carlet C.: Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. IEEE Trans. Inform. Theory, 54(5), 2354-2357 (2008).
11. Budaghyan L., Carlet C., Leander G.: Constructing new APN functions from known ones, Finite Fields and Applications, 15(2), 150-159 (2009).
12. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations sutiable for DES-like cryptosystems. Des. Codes Cryptogr. 15(2), 125-156 (1998).
13. Carlet C.: Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", publisded by Cambridge University Press, Yves Crama and Perter L. Hammer (eds.), 257-397 (2010).
14. Carlet C.: Vectorial Boolean Functions for Cryptography, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", publisded by Cambridge University Press, Yves Crama and Perter L. Hammer (eds.), 398-469 (2010).
15. Carlet C.: On Known and New Differentially Uniform Functions. ACISP 2011, 1-15.
16. 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).
17. Charpin P., Kyureghyan G.M.: When does $G(x) + \gamma\mathrm{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$? Finite Fields and Their Applications. 15(5), 615-632 (2009).
18. Dillon J.F.: APN polynomials: An Update. In: Conference Finite Fields and Applications Fq9, Dublin, Ireland (2009).
19. Dobbertin H.: One-to-one highly nonlinear power functions on $GF(2^n)$, Appl. Algebra Engrg. Comm. Comput. 9(2), 139-152 (1998).
20. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, 14, 154-156 (1968).
21. Kasami T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, Inform. Control 18, 369-394 (1971).
22. 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).
23. Leander G., Poschmann A.: On the Classification of 4 Bit S-Boxes. WAIFI 2007. LNCS 4547, pp. 159C176 (2007).
24. Li Y., Wang M.: On EA-equivalence of certain permutations to power mappings. Des. Codes Cryptogr. 58(3), 259-269 (2011).
25. Li Y., Wang M.: Permutation polynomials EA-equivalent to the inverse function over $GF(2^n)$. Cryptogr. Commun. 3(3), 175-186 (2011).
26. Li Y., Wang M.: Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1}), Des. Codes Cryptogr. In press, 2013.
27. 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, 386-397 (1994).
28. Nyberg K.: Differentially uniform mappings for cryptography. In: Advances in Cryptography-EUROCRYPT'93. LNCS, vol. 765, 55-64 (1994).
29. Panario D., Sakzad A., Stevens B., Wang Q.: Two New Measures for Permutations: Ambiguity and Deficiency. IEEE Trans. Inform. Theory 57(11): 7648-7657 (2011).

30. Pasalic E., Charpin P.: Some results concerning cryptographically significant mappings over GF(2^n). Des. Codes Cryptogr. 57(3), 257-269 (2010).
31. Qu L., Tan Y., Tan C.H., Li C.: Constructing Differentially 4-Uniform Permutations Over $\mathbb{F}_{2^{2k}}$ via the Switching Method. IEEE Transactions on Information Theory. 59(7), 4675-4686 (2013).
32. Yu Y., Wang M., Li Y.: Constructing low differential uniformity functions from known ones, Chinese Journal of Electronics, 22(3), 495-499, 2013.
33. Zha Z., Hu L., Sun S.: Constructing new differentially 4-uniform permutations from the inverse function, Finite Fields and Their Applications, 25, 6478, 2014.