Involutory Differential 4-Uniform Permutations from Known Constructions

Shihui Fu[a], Xiutao Feng[a]

[a]*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, CHINA*

Abstract

Substitution box (S-box) is an important component of block ciphers for providing confusion into the cryptosystems. The functions used as S-boxes should have low differential uniformity, high nonlinearity and high algebraic degree. Due to the lack of knowledge on the existence of APN permutations over $\mathbb{F}_{2^{2k}}$, which have the lowest differential uniformity, when $k > 3$, they are often constructed from differentially 4-uniform permutations. Up to now, many infinite families of such functions have been constructed. Besides, the less cost of hardware implementation of S-boxes is also an important criterion in the design of block ciphers. If the S-box is an involution, which means that the compositional inverse of the permutation is itself, then the implementation cost for its inverse is saved. The same hardware circuit can be used for both encryption and decryption, which is an advantage in hardware implementation. In this paper, we investigate all the differentially 4-uniform permutations that are known in the literature and determine whether they can be involutory. We found that some involutory differential 4-uniform permutations with high nonlinearity and algebraic degree can be given from these known constructions.

Keywords:
Involution, Differentially 4-uniform permutation, Nonlinearity, Permutation, Algebraic degree

1. Introduction

Many block ciphers use substitution boxes (S-boxes) as the confusion part to bring the confusion into the cryptosystems. To obtain a correct decryption and for the easiness of the implementation, S-boxes are usually chosen to be permutations over a finite field with characteristic 2 and even extension degree, i.e., $\mathbb{F}_{2^{2k}}$. Besides, in order to resist various kinds of cryptographic attacks, S-boxes used in block ciphers should possess good cryptographic properties, for example, low differential uniformity to resist differential attacks [BS91], high nonlinearity to resist linear attacks [Mat93], and high algebraic degree to resist the higher order differential attack [Knu94, Lai94], which is described by Knudsen when the degree is 2.

It is well known that for any function defined over $\mathbb{F}_{2^n}$, the lowest differential uniformity is 2, and these functions achieving this value are called almost perfect nonlinear (APN) functions. On this aspect, they are the most ideal choices for S-boxes. Unfortunately, it is very difficult to construct APN permutations for even n. Up to now, only one sporadic APN permutation over $\mathbb{F}_{2^6}$ was found by Dillon et al [BDMW10]. To find any other APN permutations over $\mathbb{F}_{2^n}$ for even n is called the the BIG APN problem.

[☆]This work was supported by National Natural Science Foundation of China (Grants No. 61572491) and the open project of the SKLOIS in Institute of Information Engineering, CAS (Grant No. 2015-MS-03).

Email addresses: fushihui@amss.ac.cn (Shihui Fu), fengxt@amss.ac.cn (Xiutao Feng)

Therefore, when the input sizes are even, a natural tradeoff method is to use differentially 4-uniform permutations as S-boxes. For instance, the AES block cipher uses a differentially 4-uniform function, namely the multiplicative inverse function as S-box. Hence to provide more choices for the design of block ciphers, it is of significant importance to construction more classes differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ with good cryptographic properties.

The low cost of hardware implementation of S-boxes is also an important criterion in the design of block ciphers. For a block cipher, the S-box as a nonlinear part usually takes a relative high cost in practical hardware implementation. Thus the cost of hardware implementation of an S-box is of significant importance, especially in lightweight cryptography algorithms, which are aiming to provide security in a limited resource environment. With the rapid development of lightweight cryptography, it is of particular interest to investigate the problem of constructing S-boxes with excellent cryptographic properties and low cost hardware implementation. If the S-box is an involution, which means that the compositional inverse of the permutation is itself, then the implementation cost for its inverse is saved. The same hardware circuit can be used for both encryption and decryption, which is certainly an advantage in hardware implementation. For instance, the AES cipher uses the inverse function as its S-box, which is, in fact, an involution as well.

In this paper, we study all the differentially 4-uniform permutations that are known in the literature and determine whether these functions can be involutory or under what kinds of conditions they can be. Some involutory differential 4-uniform permutations with high nonlinearity and algebraic degree can be given from these known constructions. Hence this provides more choices for the design of lightweight block ciphers.

The rest of this paper is organized as follows. In the next section, we recall some basic knowledge about Boolean functions, including some necessary definitions and notations. In Section 3, we examine all the known primarily-constructed differentially 4-uniform permutations. The functions constructed by switching method are examined in Section 4. The functions constructed by expansion and contraction are treated in Section 5 and 6 respectively. Conclusions and some open problems are given in Section 7. All the involutory differentially 4-uniform permutations are presented in Table 1.

2. Preliminaries

Let n be a positive integer, $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and $\mathbb{F}_{2^n}^*$ be the corresponding multiplicative cyclic group of order 2^n-1. $\mathbb{F}_{2^n}$ can also be regarded as a vector space of dimension n over $\mathbb{F}_2$, and can then be identified with $\mathbb{F}_2^n$. In the following, we will switch between these two points of view without explanation if the context is clear. Let $\omega = \alpha^{(2^n-1)/3}$ when n is an even integer, where α is a primitive element of $\mathbb{F}_{2^n}$. Then ω is an element of $\mathbb{F}_4 \backslash \mathbb{F}_2$, and satisfies the equation $\omega^2+\omega+1=0$. For the sake of convenience, we always define $0^{-1}=0$.

Given two positive integers n and m, a mapping F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is called an (n,m)-function or a vectorial Boolean function. Particularly, when $m=1$, F is called an n-variable Boolean function. We denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. The basic representation of any Boolean function $f \in \mathcal{B}_n$ is by its truth table, i.e.,

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

The support of f is defined as $\mathrm{Supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.

A (n,n)-function F can be represented uniquely by a polynomial in $\mathbb{F}_{2^n}[x]/\langle x^{2^n}+x\rangle$ as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

For any l, $0 \leq l \leq 2^n - 1$, the number $w_2(l)$ of the nonzero coefficients $l_j \in \mathbb{F}_2$ in the binary expansion $l = \sum_{j=0}^{n-1} l_j 2^j$ is called the 2-weight of l. The algebraic degree $\deg(F)$ of F is equal to the maximum 2-weight of i such that $c_i \neq 0$. It is known that if F is a permutation polynomial over $\mathbb{F}_{2^n}$, then $\deg(F) \leq n-1$ and we call F haing the maximum algebraic degree if the equality holds.

We define the trace function from $\mathbb{F}_{2^n}$ onto its subfield $\mathbb{F}_{2^k}$ (with $k|n$) as

$$\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}},$$

and denote the absolute trace function from $\mathbb{F}_{2^n}$ onto the binary subfield $\mathbb{F}_2$ by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Definition 1 ([Nyb93]). For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the differential uniformity of $F(x)$ is defined as

$$\Delta_F = \max\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\},$$

where $\delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}|$. The differential spectrum of $F(x)$ is the multi-set

$$\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}.$$

For a given integer δ, F is called differentially δ-uniform if $\Delta_F = \delta$. It is easy to see that if x_0 is a solution of $F(x+a) + F(x) = b$, so is $x_0 + a$. Thus a lower bound of the differential uniformity of F is 2. The functions which achieve this bound are called almost perfect nonlinear (APN) functions.

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the Walsh transform of F is defined as

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)}, \quad a, b \in \mathbb{F}_{2^n}.$$

The multi-set $\Lambda_F = \{\mathcal{W}_F(a,b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*\}$ is called the Walsh spectrum of the function F. And the multi-set $\{|\mathcal{W}_F(a,b)| : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*\}$ is called the extended Walsh spectrum of the function F.

The nonlinearity of F is defined as

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |\mathcal{W}_F(a,b)|.$$

It is known that if n is odd, the nonlinearity of F satisfies the inequality $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [CV94] and when the equality holds F is called almost bent (AB). The Walsh spectrum of AB functions is $\{0, \pm 2^{\frac{n+1}{2}}\}$. The notion of AB functions is closely connected with the notion of APN functions. AB functions exist only for odd n and provide the optimal resistance to linear cryptanalysis. Besides, every AB function is APN, and in the case of odd n, any quadratic APN function is an AB function. A comprehensive survey on APN and AB functions can be found in [Car10, CCZ98].

When n is even, the upper bound of the nonlinearity is still open. The known maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$. It is conjectured that $\mathcal{NL}(F)$ is upper bounded by $2^{n-1} - 2^{\frac{n}{2}}$ for any F over $\mathbb{F}_{2^n}$ [Dob98]. These functions which meet this bound are usually called the best known nonlinear functions.

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called extended affine equivalent (EA-equivalent), if $G(x) = A_1(F(A_2(x))) + A_3(x)$, where $A_1(x)$, $A_2(x)$ are affine permutations over $\mathbb{F}_{2^n}$ and $A_3(x)$ is an affine function over $\mathbb{F}_{2^n}$. Furthermore, if $A_3 = 0$, then they are called affine equivalent. They are called CCZ-equivalent (Carlet-Charpin-Zinoviev equivalent) if there exists an affine permutation over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ which maps $\mathcal{G}_F$ to $\mathcal{G}_G$, where $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and $\mathcal{G}_G$ is the graph of G.

It is well known that EA-equivalence implies CCZ-equivalence, but not vice versa. Differential uniformity, nonlinearity and Walsh spectrum are invariants of both EA-equivalence and CCZ-equivalence.

Algebraic degree is preserved by EA-equivalence, but not CCZ-equivalence. However, neither EA-equivalence nor CCZ-equivalence preserves the permutation property.

In the following sections, we examine all the known differentially 4-uniform permutations over $\mathbb{F}_{2^n}$. In the sequel, we make convention that n is always an even positive integer if without special declaration.

3. Functions Constructed by Primary Construction

There are 5 classes of primarily-constructed differentially 4-uniform permutations. These are listed as follows. The inverse function is an involution obviously. In this section, we show that all the other functions cannot be involutory.

- Gold function [Gol68]: x^{2^i+1}, where $n = 2k$, k is odd and $\gcd(i, n) = 2$.
- Kasami function [Kas71]: $x^{2^{2i}-2^i+1}$, where $n = 2k$, k is odd and $\gcd(i, n) = 2$.
- Inverse function [Nyb93]: x^{-1}, where n is even.
- Bracken-Leander function [BL10]: $x^{2^{2k}+2^k+1}$, where $n = 4k$ and k is odd.
- A class of binomials found by Bracken et al. [BTT12]: $\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$, where $n = 3k$, k even, $k/2$ odd, $\gcd(s, n) = 2$, $3|(k + s)$ and α is a primitive element of $\mathbb{F}_{2^n}$.

Lemma 1 ([Nyb93]). *Suppose k is odd and $n = 2k$. Let i be an integer such that $\gcd(i, n) = 2$. Then the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^n}$ is x^t, where $t = \sum_{j=0}^{\frac{k-1}{2}} 2^{2ji} \pmod{2^n - 1}$. Its algebraic degree is $\frac{k+1}{2}$.*

Lemma 2. *Suppose $n \geq 6$ is even. Let i be an integer such that $\gcd(i, n) = 2$. Then $(2^{2i} - 2^i + 1)^2 \neq 1 \pmod{2^n - 1}$.*

Proof. Otherwise, suppose that $(2^{2i} - 2^i + 1)^2 = 1 \pmod{2^n - 1}$, then we obtain

$$\begin{aligned} 0 &= (2^{2i} - 2^i + 1)^2 - 1 \\ &= (2^{2i} - 2^i)(2^{2i} - 2^i + 2) \\ &= 2^{i+1}(2^i - 1)(2^{2i-1} - 2^{i-1} + 1) \pmod{2^n - 1}. \end{aligned}$$

Since $\gcd(2^i - 1, 2^n - 1) = 2^{\gcd(i,n)} - 1 = 3$ and $\gcd(2^{i+1}, 2^n - 1) = 1$, the above equation can be reduced to that

$$3(2^{2i-1} - 2^{i-1} + 1) = 0 \pmod{2^n - 1}.$$

Let $\bar{l}$ denote the unique integer r, $0 \leq r < n$ such that $l = qn + r$ with $q \in \mathbb{Z}$. Note that $\gcd(i, n) = 2$ and $n \geq 6$, then $0 < i \leq n - 2$, $0 < \overline{2i} \leq n - 2$. Hence, when $i \leq \overline{2i}$,

$$\begin{aligned} 0 < 3(2^{\overline{2i}-1} - 2^{i-1} + 1) &< 4(2^{\overline{2i}-1} - 2^{i-1} + 1) \\ &\leq 2^{n-1} - 2^{i+1} + 4 \\ &< 2^n - 1. \end{aligned}$$

When $i > \overline{2i}$, we have

$$\begin{aligned} 0 < -3(2^{\overline{2i}-1} - 2^{i-1} + 1) &< 4(2^{i-1} - 2^{\overline{2i}-1} - 1) \\ &\leq 2^{n-1} - 2^{\overline{2i}+1} - 4 \\ &< 2^n - 1. \end{aligned}$$

So it is impossible that $3(2^{2i-1} - 2^{i-1} + 1) = 0 \pmod{2^n - 1}$. The conclusion then follows. □

Lemma 3. *Suppose $k \geq 2$ is an integer, then $(2^{2k}+2^k+1)^2 \neq 1 \pmod{2^{4k}-1}$.*

PROOF. Otherwise, suppose that $(2^{2k}+2^k+1)^2 = 1 \pmod{2^{4k}-1}$. Then similarly as the proof of Lemma 2, we have

$$(2^k+1)(2^{2k-1}+2^{k-1}+1) \pmod{2^{4k}-1}.$$

Notice that $2^{4k}-1 = (2^k+1)(2^{3k}-2^{2k}+2^k-1)$, then we get

$$2^{2k-1}+2^{k-1}+1 = 0 \pmod{2^{3k}-2^{2k}+2^k-1}.$$

Since $2^{3k}-2^{2k}-2^{2k-1} = 2^{2k-1}(2^{k+1}-3) > 0$ and $2^k-1-(2^{k-1}+1) = 2^{k-1}-2 \geq 0$, it follows that $0 < 2^{2k-1}+2^{k-1}+1 < 2^{3k}-2^{2k}+2^k-1$, which is a contradiction. □

Theorem 4. *The Gold function, Kasami function, Bracken-Leander function and the class of binomials cannot be involutory over $\mathbb{F}_{2^n}$.*

PROOF. Below we discuss these functions separately.

1. Suppose that Gold function x^{2^i+1} is an involution, then by Lemma 1 we must have $\frac{k+1}{2} = 2$, which implies that $k = 3$ and $n = 6$. Thus we get $i = 2$ or $i = 4$. One can then easily verify that Gold function cannot be involutory in these cases.

2. Suppose that Kasami function $x^{2^{2i}-2^i+1}$ is an involution, then for any $x \in \mathbb{F}_{2^n}$, we obtain

$$\left(x^{2^{2i}-2^i+1}\right)^{2^{2i}-2^i+1} = x \pmod{x^{2^n}+x},$$

   which is equivalent to $(2^{2i}-2^i+1)(2^{2i}-2^i+1) = 1 \pmod{2^n-1}$. Then by Lemma 2, it is impossible.

3. For the Bracken-Leander function, we suppose that it is an involution, namely

$$(2^{2k}+2^k+1)^2 = 1 \pmod{2^{4k}-1}.$$

   When $k = 1$, it can be easily checked that $(2^{2k}+2^k+1)^2 \neq 1 \pmod{2^{4k}-1}$. When $k \geq 3$, it is known that this is impossible by Lemma 3.

4. Finally, we consider the class of binomials. Let $F(x)$ denote this class of binomials and suppose that it is an involution. Since k is even and $k/2$ is odd, then $k = 2 \pmod 4$. In the following, we treat it for two cases according to the value of k.

   When $k = 2$, then we have $n = 6$ and $s = 4$. Now

$$F(x) = \alpha x^{2^4+1} + \alpha^{2^2} x^{2^4+2^6} = (\alpha+\alpha^4)x^{17}.$$

   Furthermore, it is easy to obtain that

$$1 = F(F(1)) = F(\alpha+\alpha^4) = (\alpha+\alpha^4)(\alpha+\alpha^4)^{17} = (\alpha+\alpha^4)^{18},$$

   which is equivalent to that $\alpha+\alpha^4 = 1$. It follows that $\alpha^{15} = 1$, a contradiction with the condition that α is a primitive element of $\mathbb{F}_{2^6}$.

When $k \geq 6$, for any $x \in \mathbb{F}_{2^n}$, it holds that

$$\begin{aligned} x = F(F(x)) &= \alpha\left(\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{2k}+2^{k+s}}\right)^{2^s+1} + \alpha^{2^k}\left(\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{2k}+2^{k+s}}\right)^{2^{2k}+2^{k+s}} \\ &= \alpha^{2^s+2} x^{2^{2s}+2^{s+1}+1} + \alpha^{2^{k+s}+2^k}\left(\alpha + \alpha^{2^{2k}}\right) x^{2^{2k+s}+2^{2k}+2^{k+2s}+2^{k+s}} \\ &\quad + \alpha^{2^k+2^s+1} x^{2^{2k}+2^{k+s}+2^{2s}+2^s} + \alpha^{2^{k+s}+2} x^{2^{2k+s}+2^{k+2s}+2^s+1} \\ &\quad + \alpha^{2^{2k+s}+2^k+1} x^{2^{2k+2s}+2^k+2^{s+1}} + \alpha^{2^{2k+s}+2^{2k}+2^k} x^{2^{2k+2s}+2^{2k+s}+2^{2k}+2^s} \\ &\quad + \alpha^{2^{k+s}+2^k+1} x^{2^{k+2s}+2^{k+s}+2^k+2^s}. \end{aligned}$$

First we consider the weight of $2^{2s} + 2^{s+1} + 1 \pmod{2^{3k}-1}$. Since $\gcd(s, n) = 2$ and $n > 6$, then $2 \leq s \leq n-2$. we can easily get that $2s \neq s+1 \pmod{3k}$, $2s \neq 0 \pmod{3k}$, $s+1 \neq 0 \pmod{3k}$. So the weight of $2^{2s} + 2^{s+1} + 1 \pmod{2^{3k}-1}$ is exactly equal to 3. In a similar manner, it is easy to verify that the weight of other six exponents of x are exactly equal to 4, 4, 4, 3, 4, 4, respectively. However, the above equation holds for any $x \in \mathbb{F}_{2^n}$, which is impossible because that the right hand side does not contain any one of the terms of degree one.

We finish the proof. □

4. Functions Constructed by Switching Method

A number of differentially 4-uniform permutations have been constructed via the switching method. Among the 5 classes of primarily-constructed differentially 4-uniform permutations, only the inverse function is an involution. In the following, we consider the differentially 4-uniform permutations constructed from inverse function.

4.1. By Adding a Boolean Function

Firstly, we list the known differentially 4-uniform permutations which were constructed by adding a properly chosen Boolean function to the inverse function.

- Qu-Tan-Tan-Li [QTTL13]: $x^{-1} + \mathrm{Tr}(x^{-d} + (x^{-1}+1)^d)$, where $d = 2^n - 2$, or $3 \times (2^t + 1)$ for $2 \leq t \leq n/2 - 1$.
- Qu-Tan-Li-Gong [QTLG16]: $x^{-1} + g(x)$, where g is some Boolean function.
- Peng-Tan (I) [PT16]:

$$F(x) = \begin{cases} x^{-1} + 1 & \text{if } x \in T, \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n} \setminus T, \end{cases}$$

  where $T \subset \mathbb{F}_{2^n}$. As there are at least $2^{2^{n-2}-1}$ such T, it is not possible to list them here. For more detail on T, please refer to [PT16].
- Zha-Hu-Sun (I) [ZHSS15]:

$$F(x) = \begin{cases} x^{-1} + 1 & \text{if } x \in S, \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n} \setminus S, \end{cases}$$

  where S satisfies any of the following conditions:

  (1) $S = \mathbb{F}_{2^{k_1}} \cup \mathbb{F}_{2^{k_2}}$, k_1, k_2 are even, $k_1 | n, k_2 | n$, or

  (2) $S = \mathbb{F}_{2^3} \cup \mathbb{F}_{2^{k_1}}$, k_1 is even, $k_1 | n$, $\gcd(3, k_1) = 1$, $6 | n$, $\frac{n}{6}$ is odd.

– Chen-Deng-Zhu-Qu [CDZQ16]: $x^{-1}+g(x^{-1})$, where $g(x)$ is a 4-Uniform BFI (4-uniform Boolean function with respect to the inverse function).

All the above functions can be expressed in the following unified form

$$F(x) = x^{-1} + \mathbf{1}_U(x), \tag{1}$$

where $U \subsetneq \mathbb{F}_{2^n}$, $U \neq \emptyset$, and $\mathbf{1}_U$ is the indicator function of U, i.e., $\mathbf{1}_U(x) = 1$ if $x \in U$ and $\mathbf{1}_U(x) = 0$ otherwise. The following result gives the conditions to be satisfied for the function (1) being involutory.

Proposition 1. *The function $F(x)$ of (1) is an involution over $\mathbb{F}_{2^n}$ if and only if the subset U of $\mathbb{F}_{2^n}$ satisfies any one of the following conditions:*

(1) $U = \{0, 1\}$, or

(2) $U = \{\omega, \omega^2\}$, or

(3) $U = \{0, 1, \omega, \omega^2\}$.

Proof. The sufficiency is obvious. Now we consider the necessity.

First, we claim that the subset $U \subsetneq \mathbb{F}_{2^n}$ satisfies that $x \in U$ holds if and only if $\frac{1}{x^{-1}+1} \in U$. Indeed, assume $x_1, x_2 \in \mathbb{F}_{2^n}$ with $F(x_1) = F(x_2)$. Then we have $x_1^{-1} + \mathbf{1}_U(x_1) = x_2^{-1} + \mathbf{1}_U(x_2)$. If $\mathbf{1}_U(x_1) = \mathbf{1}_U(x_2)$, we get $x_1^{-1} = x_2^{-1}$, which leads to $x_1 = x_2$. If $\mathbf{1}_U(x_1) \neq \mathbf{1}_U(x_2)$, we get $x_1^{-1}+1 = x_2^{-1}$, which implies $x_2 = \frac{1}{x_1^{-1}+1}$ and $\mathbf{1}_U(x_1) \neq \mathbf{1}_U\left(\frac{1}{x_1^{-1}+1}\right)$. But since F is a permutation over $\mathbb{F}_{2^n}$, we must have $\mathbf{1}_U(x) = \mathbf{1}_U\left(\frac{1}{x^{-1}+1}\right)$, for any $x \in \mathbb{F}_{2^n}$.

Now we suppose that F is an involution over $\mathbb{F}_{2^n}$. Thus for any $x \in \mathbb{F}_{2^n}$, we have $F(F(x)) = x$, namely

$$\frac{1}{\frac{1}{x} + \mathbf{1}_U(x)} + \mathbf{1}_U\left(\frac{1}{x} + \mathbf{1}_U(x)\right) = x. \tag{2}$$

Below we consider two cases according as $x = 0, 1$ or not.

Case 1: When $x = 0$ or $x = 1$. Substitute $x = 0$ into Eq.(2), we have

$$\frac{1}{\mathbf{1}_U(0)} + \mathbf{1}_U(\mathbf{1}_U(0)) = 0.$$

If $\mathbf{1}_U(0) = 0$, we have $0 \notin U$, which implies $1 \notin U, \mathbf{1}_U(1) = 0$. Substitute $x = 1$ into Eq.(2), we obtain

$$\frac{1}{1 + \mathbf{1}_U(1)} + \mathbf{1}_U(1 + \mathbf{1}_U(1)) = \frac{1}{1} + \mathbf{1}_U(1) = 1.$$

So Eq.(2) holds also for $x = 1$.

If $\mathbf{1}_U(0) = 1$, we have $0 \in U$, which implies $1 \in U, \mathbf{1}_U(1) = 1$. Substitute $x = 1$ into Eq.(2), we obtain

$$\frac{1}{1 + \mathbf{1}_U(1)} + \mathbf{1}_U(1 + \mathbf{1}_U(1)) = \frac{1}{1+1} + \mathbf{1}_U(1+1) = 1.$$

So Eq.(2) holds for $x = 1$ as well.

Case 2: When $x \neq 0$ and $x \neq 1$. Thus we have $\frac{1}{x} + \mathbf{1}_U(x) \neq 0$. Hence from Eq.(2) we get

$$\mathbf{1}_U(x)x^2 + \mathbf{1}_U(x)\mathbf{1}_U\left(\frac{1}{x} + \mathbf{1}_U(x)\right)x + \mathbf{1}_U\left(\frac{1}{x} + \mathbf{1}_U(x)\right) = 0. \tag{3}$$

If $\mathbf{1}_U(x) = 0$, i.e., $x \notin U$. From Eq.(3), we have $\mathbf{1}_U\left(\frac{1}{x}\right) = 0$, which implies that

$$x \notin U \text{ holds if and only if } \frac{1}{x} \notin U \text{ and } \frac{1}{x^{-1}+1} \notin U.$$

If $\mathbf{1}_U(x) = 1$, i.e., $x \in U$. From Eq.(3), we have

$$x^2 + \mathbf{1}_U\left(\frac{1}{x}+1\right)x + \mathbf{1}_U\left(\frac{1}{x}+1\right) = 0.$$

Suppose that $\mathbf{1}_U\left(\frac{1}{x}+1\right) = 0$, then we must have $x = 0$, which is a contradiction. Hence we have $\mathbf{1}_U\left(\frac{1}{x}+1\right) = 1$, and the above equation becomes

$$x^2 + x + 1 = 0.$$

So $x = \omega$ or $x = \omega^2$. It can be easily verified that for $x = \omega$ or $x = \omega^2$, if $\mathbf{1}_U(x) = 1$, then $\mathbf{1}_U\left(\frac{1}{x}+1\right) = 1$.

Combining the discussion of two cases, we deduce that $U \subseteq \{0, 1, \omega, \omega^2\}$. Therefore, $U = \{0, 1\}$ or $U = \{\omega, \omega^2\}$ or $U = \{0, 1, \omega, \omega^2\}$. We complete the proof. □

In [YWL13], it is shown that, when $U = \{0, 1\}$ or $U = \{\omega, \omega^2\}$, the differentially uniformity of the function of (1) is equal to 4 if and only if $n = 2 \pmod 4$. When $U = \{0, 1, \omega, \omega^2\}$, the function of (1) is proved to be a differentially 4-uniform permutation in [ZHSS15]. Therefore, we have the following corollary.

Corollary 5. *The function $F(x)$ of (1) is a differentially 4-uniform involution over $\mathbb{F}_{2^n}$ if and only if the subset U of $\mathbb{F}_{2^n}$ and n satisfy any one of the following conditions:*

(1) $U = \{0, 1\}$ and $n = 2 \pmod 4$, or

(2) $U = \{\omega, \omega^2\}$ and $n = 2 \pmod 4$, or

(3) $U = \{0, 1, \omega, \omega^2\}$.

By Lagrange interpolation, it is easy to obtain the explicit expressions of function $F(x)$ of (1):

$$\begin{aligned}
U = \{0,1\}: \quad F(x) &= x^{2^n-2} + x^{2^n-1} + (x+1)^{2^n-1} \\
&= \sum_{i=0}^{2^n-3} x^i, \\
U = \{\omega,\omega^2\}: \quad F(x) &= x^{2^n-2} + (x+\omega)^{2^n-1} + (x+\omega^2)^{2^n-1} \\
&= \sum_{\substack{i\geq 1,\\ i\neq 0 \pmod 3}}^{2^n-3} x^i, \\
U = \{0,1,\omega,\omega^2\}: \quad F(x) &= x^{2^n-2} + x^{2^n-1} + (x+1)^{2^n-1} + (x+\omega)^{2^n-1} + (x+\omega^2)^{2^n-1} \\
&= x^{2^n-2} + \sum_{\substack{i\geq 0,\\ i=0 \pmod 3}}^{2^n-4} x^i.
\end{aligned}$$

It is obvious that the algebraic degree is equal to $n-1$. For any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*$, we have

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

It is well known that the extended Walsh spectrum of inverse function is bounded by $2^{\frac{n}{2}+1}$, so the nonlinearity $\mathcal{NL}(F) \ge 2^{n-1} - 2^{\frac{n}{2}} - |U|$. Moreover, in [LWY13], it is showed that when $U = \{0,1\}$ and $n = 2 \pmod 4$, the function $F(x)$ of (1) has the best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$ and its Walsh spectrum is $\{-2^{\frac{n}{2}+1} \le y \le 2^{\frac{n}{2}+1} : y = 0 \pmod 4\}$.

4.2. By Using Some Non-affine Transformations on Some Subfields

Next we consider these functions constructed via modifying the inverse function by using some EA-equivalent transformations (which are not affine) on some subfields by Peng and Tan [PT17].

– Peng-Tan (II) [PT17]:

$$
F(x) = \begin{cases} \beta(x+1)^{-1} + \alpha & \text{if } x \in \mathbb{F}_{2^d} \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n}\setminus\mathbb{F}_{2^d} \end{cases}, \tag{4}
$$

where α, β, d, n satisfy any of the following conditions:

(i) $\alpha \in \mathbb{F}_{2^d}$, $\beta = 1$, d is even, or
(ii) $\alpha = \beta = 1$, d is odd, or
(iii) $\alpha = 0$, $\beta = 1$, $d = 1, 3$, $n/2$ is odd, or
(iv) $\alpha, \beta \in \mathbb{F}_{2^d}$, $\mathrm{Tr}(\beta^{-1}) = 1$, n/d is odd.

Obviously, we have $\alpha, \beta \in \mathbb{F}_{2^d}$ and $\beta \neq 0$. If the function (4) is involutory, then from $F(F(0)) = 0$ and $F(F(1)) = 1$, we obtain the following equations:

$$
\frac{\beta}{\alpha+\beta+1} = \alpha, \tag{5a}
$$

$$
\frac{\beta}{\alpha+1} = \alpha + 1. \tag{5b}
$$

If $\alpha = 0$, then $\beta = 1$. One can easily check that F is an involution in this case.

If $\alpha = 1$, then equations (5a) and (5b) hold. For any $x \in \mathbb{F}_{2^n}\setminus\mathbb{F}_{2^d}$, $F(F(x)) = F\left(\frac{1}{x}\right) = x$ and any $x \in \mathbb{F}_{2^d}\setminus\mathbb{F}_2$, $F(F(x)) = F\left(\frac{\beta}{x+1} + 1\right) = \frac{\beta}{\frac{\beta}{x+1}+1+1} + 1 = x$. Therefore, F is an involution.

If $\alpha \neq 0, 1$, then by (5a) and (5b), we can deduce that $\alpha = \beta = \omega$ or ω^2. It follows that d is even and $n = 2 \mod 4$ because of condition (iv). Actually we can furthermore obtain that $d = 2$. Indeed, when $\alpha = \beta = \omega$, for any $x \in \mathbb{F}_{2^d}\setminus\mathbb{F}_{2^2}$, $F(F(x)) = F(\beta(x+1)^{-1} + \alpha) = F(\frac{\omega x}{x+1}) = \frac{\omega^2 x}{\omega^2 x+1} = x$. This implies $x = \omega^2$, a contradiction. The case $\alpha = \beta = \omega^2$ can be treated similarly.

Proposition 2. *The Peng-Tan (II) function $F(x)$ of (4) is a differentially 4-uniform involution over $\mathbb{F}_{2^n}$ if α, β, d, n satisfy any of the following conditions:*

(i) $\alpha = \beta = 1$, *or*

(ii) $\alpha = 0$, $\beta = 1$, d *is even, or*

(iii) $\alpha = 0$, $\beta = 1$, $d = 1, 3$, $n/2$ *is odd, or*

(iv) $\alpha = \beta = \omega$ *or* ω^2, $d = 2$, $n/2$ *is odd, or*

(v) $\alpha = 1$, $\mathrm{Tr}(\beta^{-1}) = 1$, n/d *is odd.*

In [PT17], it is shown that the function $F(x)$ of (4) has algebraic degree $n-1$, and the nonlinearity $\mathcal{NL}(F) \geq 2^{n-1} - 2^{\frac{n}{2}} - 2^d$.

4.3. By Using Some Affine Transformations on Some Subfields

In [ZHS14], by modifying the values of the inverse function on some subfield and applying affine transformations on the function, two new families of differentially 4-uniform permutations are constructed.

– Zha-Hu-Sun (II) [ZHS14]:

$$F(x) = \begin{cases} x^{-1} + \alpha & \text{if } x \in \mathbb{F}_{2^d} \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^d} \end{cases}, \tag{6}$$

where $\alpha \in \mathbb{F}_{2^d}$; $d|n$; d is even, or $d = 1, 3$; $n/2$ is odd.

The case $\alpha = 0$ is trivial. And when $\alpha = 1$, it is the same with function (1). When $\alpha \neq 0, 1$, $F(F(0)) = F(\alpha) = \frac{1}{\alpha} + \alpha \neq 0$. Hence, it can not be involutory.

– Zha-Hu-Sun (III) [ZHS14]:

$$F(x) = \begin{cases} \beta x^{-1} + \alpha & \text{if } x \in \mathbb{F}_{2^d} \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^d} \end{cases}, \tag{7}$$

where $\alpha, \beta \in \mathbb{F}_{2^d}$; $\mathrm{Tr}(\frac{1}{\alpha}) = 1$; $d|n$; d is even; n/d is odd.

If the function (7) is an involution, then we can easily get that $\alpha = \omega$, $\beta = \omega^2$, or $\alpha = \omega^2$, $\beta = \omega$; $d = 2$; $n/2$ is odd.

Similarly, it is shown that the functions $F(x)$ of (6) and (7) have also algebraic degree $n-1$, and the nonlinearity $\mathcal{NL}(F) \geq 2^{n-1} - 2^{\frac{n}{2}} - 2^d$ in [ZHS14].

4.4. By Applying Constant Multiplication to the Inverse Function on Some Subsets

In [PTW16], by applying constant multiplication to the inverse function on some subsets (a union of some cosets of the group generated by a fixed element), Peng et al. constructed a new family of differentially 4-uniform permutations.

– Peng-Tan-Wang [PTW16]:

$$F(x) = \begin{cases} (\gamma x)^{-1} & \text{if } x \in U \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n} \backslash U \end{cases}, \tag{8}$$

where $\gamma \in \mathbb{F}_{2^n}$ and U is a union of some cosets of the cyclic group $\langle \gamma \rangle$.

If we write $U = \bigcup_{i=1}^{s} g_i\langle\gamma\rangle$, then the compositional inverse of function (8) is

$$F^{-1}(x) = \begin{cases} (\gamma x)^{-1} & \text{if } x \in U^{-1} := \bigcup_{i=1}^{s} g_i^{-1}\langle\gamma\rangle \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n}\backslash U^{-1} \end{cases}.$$

Therefore, the function (8) is involutory if and only if $U = U^{-1}$, i.e., $U = \bigcup_{i=1}^{s} \left(g_i\langle\gamma\rangle \cup g_i^{-1}\langle\gamma\rangle\right)$.

Corollary 6. *Let $U = \bigcup_{g\in G} g\langle\gamma\rangle$, where $G \subseteq \mathbb{F}_{2^n}^*$, $\gamma \in \mathbb{F}_{2^n}^*$ is of order d such that*

(i) If $g \in G$, then $g^{-1} \in G$, and

(ii) $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 1$, and

(iii) $\mathrm{Tr}\left(\frac{\gamma}{(g_i/g_j)\gamma^l + (g_j/g_i)\gamma^{-l}}\right) = 1$, for any $g_i, g_j \in G$, $0 \le l \le \frac{d-1}{2}$ (when $g_i = g_j$, then $1 \le l \le \frac{d-1}{2}$),

then the function F of (8) is a differentially 4-uniform involution over $\mathbb{F}_{2^n}$.

In [PTW16], it is shown that the function (8) has maximum algebraic degree $n-1$, and the nonlinearity satisfies that $\mathcal{NL}(F) \ge 2^{n-1} - 2^{\frac{n}{2}} - d \cdot |G|$.

When $n = 2 \cdot 3^m \cdot t$, where $\gcd(6, t) = 1$. ξ is an element of order 3^{m+1}. For every set $J \subseteq \{0, 1, \ldots, 3^m - 1\}$, let $U = \bigcup_{j\in J} \xi^j\langle\omega\rangle$, then the function (8) is proved to have differentially uniformity 4. However, for any $0 \le j \le 3^m - 1$, the inverse of ξ^j is $\xi^{3^{m+1}-j}$, which is not in the set U since $3^{m+1} - j > 3^m - 1$. Hence, the function in this case cannot be involutory.

4.5. By Permuting the Inverse Function

Based the idea of permuting the inverse function, Tang et al. [TCT15] designed a construction providing a large number of differentially 4-uniform permutation with maximum algebraic degree and high nonlinearity. It is proved that for every even $n \ge 12$, the functions in a subclass of the constructed class are CCZ-inequivalent to known differentially 4-uniform power functions and quadratic functions.

– Tang-Carlet-Tang [TCT15]:

$$F(x) = \begin{cases} (x+1)^{-1} & \text{if } x \in T \\ x^{-1} & \text{if } x \in \mathbb{F}_{2^n}\backslash T \end{cases}, \tag{9}$$

where T satisfies:

(i) if $x \in T$, then $x + 1 \in T$, and

(ii) if $x \in T$, then $\mathrm{Tr}(\frac{1}{x}) = \mathrm{Tr}(\frac{1}{x+1}) = 1$.

It is noticed that a function is an involution if and only if its compositional inverse is an involution as well. The compositional inverse of function (9) is $F^{-1}(x) = x^{-1} + \mathbf{1}_T(x^{-1})$, which is the case of the function (1) we have already treated.

4.6. By Composing the Inverse Function and Some Cycles

In [LWY13], Li et al. investigated the composition of the inverse function and cycles over $\mathbb{F}_{2^n}$, thus more image values of the inverse function are changed. It is shown that lots of differentially 4-uniform permutations can be constructed via this method.

Recall that a cycle over $\mathbb{F}_{2^n}$ is denoted by $\pi = (\alpha_0\ \alpha_1\ \cdots\ \alpha_m)$, where α_i, $0 \le i \le m$ are pairwise different elements of $\mathbb{F}_{2^n}$. We call $\alpha \in \pi$ if $\alpha = \alpha_i$ for some $0 \le i \le m$. The subscripts are computed in $\mathbb{Z}/(m+1)\mathbb{Z}$ throughout this subsection, which means $\alpha_{m+1} = \alpha_0$.

We define the composition of the inverse function and a cycle $\pi = (\alpha_0\ \alpha_1\ \cdots\ \alpha_m)$ over $\mathbb{F}_{2^n}$ as follows:

$$F(x) = \begin{cases} \alpha_{i+1}^{-1} & x = \alpha_i \\ x^{-1} & x \notin \{\alpha_i : 0 \le i \le m\} \end{cases}. \tag{10}$$

Moreover, in [LWY13], the authors gave the compositional inverse of $F(x)$:

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

In fact, the compositional inverse of $F(x)$ is the composition of the inverse function and a cycle $\pi_1 = (\alpha_m^{-1}\ \alpha_{m-1}^{-1}\ \cdots\ \alpha_0^{-1})$. Therefore, it is easy to see that the function $F(x)$ is involutory if and only if the cycles $\pi = (\alpha_0\ \alpha_1\ \ldots\ \alpha_m)$ and $\pi_1 = (\alpha_m^{-1}\ \alpha_{m-1}^{-1}\ \cdots\ \alpha_0^{-1})$ are the same. Then the following conclusion is obvious.

Proposition 3. *The function (10) is an involution over $\mathbb{F}_{2^n}$ if and only if there exist integers i, j, $0 \le i, j \le m$ such that for any $0 \le k \le m$, it holds that $\alpha_{i+k} = \frac{1}{\alpha_{j-k}}$. Especially,*

1. *If $0 \in \pi$, $1 \notin \pi$, or $0 \notin \pi$, $1 \in \pi$, then for any $0 \le k \le m$, it holds that $\alpha_{i+k} = \frac{1}{\alpha_{i-k}}$;*
2. *If $0 \in \pi$ and $1 \in \pi$, then the cycle π has the form $(0\ \alpha_1\ \cdots\ \alpha_l\ 1\ \alpha_l^{-1}\ \cdots\ \alpha_1^{-1})$, where l is an integer.*

It is showed that the nonlinearity of function (10) satisfies that $\mathcal{NL}(F) \ge 2^{n-1} - 2^{\frac{n}{2}-1} - (m+1)$, where $m+1$ is the length of the cycle π. For the property of differentially uniformity, one can refer to [LWY13] for more details on the conditions for π such that $F(x)$ has differential uniformity 4. In the following, we list the case of some special cycles with length 3 such that the corresponding functions have differentially uniformity 4.

- $\pi = (1\ \gamma\ \gamma^2)$, $\gamma = \omega$ or $\gamma = \omega^2$, $n = 2 \pmod 4$;
- $\pi = (0\ 1\ \gamma)$, $\gamma \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$, $\mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$;
- $\pi = (1\ \gamma\ \gamma+1)$, $\gamma \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$, $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\frac{1}{\gamma}) = \mathrm{Tr}(\frac{1}{\gamma+1}) = 1$;
- $\pi = (0\ 1\ \gamma)$, $\gamma \notin \begin{cases} \{\frac{i^2+i+1}{i^4+i+1}, \frac{i^4+i^2}{i^2+i+1} : i \in \mathbb{F}_{2^n}\} & \text{if } k \text{ is odd or can be divided by 4} \\ \{\frac{i^2+i+1}{i^4+i+1}, \frac{i^4+i^2}{i^2+i+1} : i \in \mathbb{F}_{2^n}\} \bigcup \mathbb{F}_{2^2} & \text{if } k \text{ can be divided by 2 but not 4} \end{cases}$.

By Proposition 3, these functions constructed by the cycle $(0\ 1\ \gamma)$ cannot be an involution. For the cycle $(1\ \gamma\ \gamma+1)$, it is easy to obtain that $\gamma = \omega$ or $\gamma = \omega^2$, which is the first case. In this case, the nonlinearity $\mathcal{NL}(F) \ge 2^{n-1} - 2^{\frac{n}{2}-1} - 3$. When $\gamma = \omega$, by Lagrange interpolation, we have

$$\begin{aligned} F(x) &= x^{-1} + (x+1)^{2^n-1}(1+\omega^2) + (x+\omega)^{2^n-1}(\omega+\omega^2) + (x+\omega^2)^{2^n-1}(1+\omega) \\ &= \omega^2 x^{2^n-2} + \omega \sum_{i \ge 2,\ i=2 \pmod 3}^{2^n-5} x^i. \end{aligned}$$

Its algebraic degree is obviously $n-1$. The case of $\gamma = \omega^2$ can be treated similarly.

Next we consider the cycles π with length 2, namely transposition. By Proposition 3, we have that $0 \in \pi$ if and only if $1 \in \pi$. If the cycle $\pi = (0\ 1)$, the corresponding function is actually the special case of function (1) with $U = \{0, 1\}$.

If the cycle $\pi \neq (0\ 1)$, then $\pi = (\gamma\ \gamma^{-1})$, $\gamma \notin \mathbb{F}_2$. In [YWL13], it is proved that in this case these functions always have differentially uniformity at most 6. Moreover, the differentially uniformity is equal to 4 if and only if $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\frac{1}{\gamma}) = 1$. By Lagrange interpolation, we have

$$\begin{aligned} F(x) &= x^{2^n-2} + (x+\gamma)^{2^n-1}(\gamma+\gamma^{-1}) + (x+\gamma^{-1})^{2^n-1}(\gamma+\gamma^{-1}) \\ &= (1+\gamma^2+\gamma^{-2})x^{2^n-2} + (\gamma+\gamma^{-1})\sum_{i=1}^{2^n-3}(\gamma^{2^n-i-1} + \gamma^{-(2^n-i-1)})x^i. \end{aligned}$$

When $\gamma = \omega$ or $\gamma = \omega^2$, the corresponding function is actually the special case of function (1) with $U = \{\omega, \omega^2\}$. When $\gamma \neq \omega$ and $\gamma \neq \omega^2$, $(1+\gamma^2+\gamma^{-2}) \neq 0$, the function $F(x)$ has maximum algebraic degree $n-1$. The nonlinearity $\mathcal{NL}(F) \geq 2^{n-1} - 2^{\frac{n}{2}-1} - 2$.

The number of such transpositions such that the corresponding function is differentially 4-uniform involution is exactly equal to $T(n) + 1 = 2^{n-2} - 2^{\frac{n}{2}-1}\cos(n \arccos \frac{1}{\sqrt{8}}) + \frac{5}{4}$ (see Remark 1).

5. Functions Constructed by Expansion

5.1. From the Inverse Function

In 2013, Carlet et al. [CTTL14] introduced a method to construct differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ from known permutations over $\mathbb{F}_{2^{n-1}}$. The construction is follows.

– Carlet et al. [CTTL14]: Let $n \geq 6$ be an even integer. For any element $c \in \mathbb{F}_{2^{n-1}} \backslash \{0, 1\}$ such that $\mathrm{Tr}_1^{n-1}(c) = \mathrm{Tr}_1^{n-1}(1/c) = 1$, we define an (n, n)-function F as follows:

$$F(x_1, \ldots, x_{n-1}, x_n) = \begin{cases} (1/x', f(x')) & \text{if } x_n = 0 \\ (c/x', f(x'/c) + 1) & \text{if } x_n = 1 \end{cases}, \tag{11}$$

where $x' \in \mathbb{F}_{2^{n-1}}$ is identified with $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$ and $f \in \mathcal{B}_{n-1}$ is an arbitrary Boolean function of $n-1$ variables.

In the following, we show that the above function is involutory if and only of f is the zero function on $\mathbb{F}_{2^{n-1}}$.

Proposition 4. *The function $F(x)$ of (11) is involutory over $\mathbb{F}_{2^n}$ if and only if $f = 0$ on $\mathbb{F}_{2^{n-1}}$.*

Proof. If f is not the zero function on $\mathbb{F}_{2^{n-1}}$, then there exists an element $x_0' \in \mathbb{F}_{2^{n-1}}$ such that $f(x_0') = 1$. We consider the element $(x_0', 0) \in \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2$.

$$F(F(x_0', 0)) = F\left(\frac{1}{x_0'}, f(x_0')\right) = \left(cx_0', f\left(\frac{1}{cx_0'}\right) + 1\right) \neq (x_0', 0),$$

since $c \neq 1$. The converse is obvious. □

Remark 1. *It is mentioned in [CTTL14] that if we define $T(n)$ as the number of $c \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_1^n(c) = \mathrm{Tr}_1^n(1/c) = 1$, then the construction (11) can give $T(n-1) - 1$ differentially 4-uniform involutions. Actually, we have that $T(n) = 2^{n-2} - (-1)^n 2^{\frac{n}{2}-1}\cos(n \arccos \frac{1}{\sqrt{8}}) + \frac{1}{4}$ (see [Hir98, Section 1.4]). Hence, this construction gives $2^{n-3} + 2^{\frac{n-3}{2}}\cos((n-1)\arccos \frac{1}{\sqrt{8}}) - \frac{3}{4}$ differentially 4-uniform involutions.*

The algebraic degree is proved to be $n-1$ in [CTTL14]. For any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*$, we identify a with (a', a_n) and b with (b', b_n), then

$$\begin{aligned}
|\mathcal{W}_F(a,b)| &= \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bF(x)+ax)} \right| \\
&= \left| \sum_{(x',x_n) \in \mathbb{F}_{2^{n-1}} \times \{0\}} (-1)^{\mathrm{Tr}_1^{n-1}(b'/x' + a'x')} + \sum_{(x',x_n) \in \mathbb{F}_{2^{n-1}} \times \{1\}} (-1)^{\mathrm{Tr}_1^{n-1}(b'c/x' + a'x') + a_n + b_n} \right| \\
&= \left| \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{\mathrm{Tr}_1^{n-1}(b'/x' + a'x')} + (-1)^{a_n+b_n} \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{\mathrm{Tr}_1^{n-1}(b'c/x' + a'x')} \right| \\
&\leq 2 \left| \sum_{x' \in \mathbb{F}_{2^{n-1}}} (-1)^{\mathrm{Tr}_1^{n-1}(b'/x' + a'x')} \right| \leq 2 \left\lfloor 2^{\frac{n+1}{2}} \right\rfloor .
\end{aligned}$$

This implies that the nonlinearity of the involution $F(x)$ of (11) satisfies $\mathcal{NL}(F) \geq 2^{n-1} - \lfloor 2^{\frac{n+1}{2}} \rfloor$.

5.2. The Butterfly Structures

Recently, Perrin et al. [PUB16] introduced the so-called butterfly structure, which is a $2k$-bit mapping obtained by concatenating two bivariate functions over $\mathbb{F}_{2^k}$ for odd k. In [CDP16], Canteaut et al. generalised this family of butterflies. Such butterflies have two CCZ-equivalent representations: one is a quadratic function (denoted V_R) and one is degree $k+1$ or k involution (denoted H_R) as described in the following.

- the open butterfly H_R is the involution over $(\mathbb{F}_{2^k})^2$ defined by

$$\mathsf{H}_R(x,y) = \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x) \right),$$

- the closed butterfly V_R is the function over $(\mathbb{F}_{2^k})^2$ defined by

$$\mathsf{V}_R(x,y) = (R(x,y), R(y,x)),$$

where $R_y(x) = R(x,y)$ and $R_y^{-1}(R_y(x)) = x$ for any $x, y \in \mathbb{F}_{2^k}$. A representation of this structure is given in Figure 1.

(a) The open butterfly H_R (involution). (b) The closed butterfly V_R.

Figure 1: The butterfly constructions.

It is showed that the differential uniformity of these functions is at most 4 when α, β, $R(x,y)$ satisfy any one of the following conditions:

– Perrin et al. [PUB16]: $\alpha \in \mathbb{F}_{2^k}$, $\alpha \neq 0$, $R(x,y) = (x+\alpha y)^3 + y^3$;

– Fu et al. [FF16] : $\gcd(i,k) = 1$ and $\alpha \in \mathbb{F}_{2^k}$, $\alpha \neq 0$, $R(x,y) = (x+\alpha y)^{2^i+1} + y^{2^i+1}$;

– Canteaut et al. [CDP16]: $\alpha, \beta \in \mathbb{F}_{2^k}$, $\alpha \neq 0$, $\beta \neq 0$ and $\beta \neq (1+\alpha)^3$, $R(x,y) = (x+\alpha y)^3 + \beta y^3$.

Moreover, in [FF16], it is proved that when $\gcd(i,k) = 1$ and $R(x,y) = (x+y)^{2^i+1} + y^{2^i+1}$, the closed butterfly, namely

$$\mathsf{V}_R(x,y) = \left((x+y)^{2^i+1} + x^{2^i+1}, (x+y)^{2^i+1} + y^{2^i+1}\right)$$

is also a differentially 4-uniform permutation over $(\mathbb{F}_{2^k})^2$. However

$$\mathsf{V}_R(\mathsf{V}_R(x,x)) = \mathsf{V}_R\left(x^{2^i+1}, x^{2^i+1}\right) = \left(x^{(2^i+1)^2}, x^{(2^i+1)^2}\right) = (x,x),$$

which does not hold for any $x \in \mathbb{F}_{2^k}$. This implies that $\mathsf{V}_R(x,y)$ is not involutory.

In all the three cases (in fact, the first case is a special case of the third case), the functions always have the best known nonlinearity, namely $2^{2k-1} - 2^k$. Moreover, when $\alpha = \beta = 1$, their extended Walsh spectrum is $\{0, 2^{k+1}\}$, otherwise, their extended Walsh spectrum is $\{0, 2^k, 2^{k+1}\}$.

6. Functions Constructed by Contraction

In [Car11], Carlet presented a method to construct differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ by using APN permutations over $\mathbb{F}_{2^{n+1}}$. The construction is as follows.

– Carlet [Car11]: Let $c = n \pmod 2$, $\alpha \in \mathbb{F}_{2^{n+1}}$ and $\mathrm{Tr}_1^{n+1}(\alpha) = 1$. Identify a vector of $\mathbb{F}_2^n$ as an element of $H = \{u \in \mathbb{F}_{2^{n+1}} : \mathrm{Tr}_1^{n+1}(u) = 0\}$. Then the restriction of $x + \frac{1}{x+\alpha+c} + \left(\frac{1}{x+\alpha+c}\right)^2$ to H is a differentially 4-uniform permutation over $\mathbb{F}_2^n$.

In our case, $c = 0$ since n is even. Denote the function of the above construction by F, and suppose that F is involutory. Then, for any $\beta \in \mathbb{F}_{2^{n+1}} \backslash H$, we have $\alpha + \beta \in H$,

$$\begin{aligned} F(F(\alpha+\beta)) &= F\left(\alpha + \beta + \frac{1}{\beta} + \frac{1}{\beta^2}\right) \\ &= \alpha + \beta + \frac{1}{\beta} + \frac{1}{\beta^2} + \frac{1}{\beta + \frac{1}{\beta} + \frac{1}{\beta^2}} + \left(\frac{1}{\beta + \frac{1}{\beta} + \frac{1}{\beta^2}}\right)^2 = \alpha + \beta. \end{aligned} \tag{12}$$

Notice that $\beta \neq 0$ and $\beta^3 + \beta + 1 \neq 0$. Otherwise, it can imply that $\mathrm{Tr}_1^{n+1}(\beta) = \mathrm{Tr}_1^{n+1}(\beta^4 + \beta^2) = 0$, a contradiction. So the equation (12) can be furthermore reduced to

$$\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0,$$

which contradicts that β is arbitrary. Therefore, the construction F cannot be an involution.

Based on the above idea, Li and Wang [LW14] constructed several classes differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_2^n$ from quadratic APN permutations (which are also AB permutations) over $\mathbb{F}_{2^{n+1}}$, where n is even.

(i) Suppose $n \geq 4$ 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 $H_u = \{ux^{2^i} + u^{2^i}x : x \in \mathbb{F}_{2^{n+1}}\}$. Let $F_u(x)$ be the restriction of $ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}}$ to H_u, where $x^{\frac{1}{2^i+1}}$ is the compositional inverse of x^{2^i} over $\mathbb{F}_{2^{n+1}}$;

(ii) Suppose $n \geq 4$ 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 $H_u = \{ux^{2^i} + u^{2^i}x : x \in \mathbb{F}_{2^{n+1}}\}$. 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, where $x^{\frac{1}{2^i+1}}$ is the compositional inverse of x^{2^i} over $\mathbb{F}_{2^{n+1}}$;

(iii) Let $m = n+1$ be odd and divisible by 3, $\gcd(i, m) = 1$, $s = i \mod 3$. $F(x) = x^{\frac{1}{2^i+1}} + \mathrm{Tr}_3^m(x + x^{2^{2s}})$ is an AB permutation over $\mathbb{F}_{2^m}$. Identify a vector of $\mathbb{F}_2^n$ as an element of the linear subspace $\mathrm{Tr}^{(0)} = \{x \in \mathbb{F}_{2^m} : \mathrm{Tr}_1^m(x) = 0\}$. Let $F'(x)$ be the restriction of $F(x) + F(x)^{2^i}$ to $\mathrm{Tr}^{(0)}$.

Then $F_u(x)$, $F'_u(x)$ and $F'(x)$ are differentially 4-uniform permutations over $\mathbb{F}_2^n$. Their nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$ and the extended Walsh spectrum is $\{0, 2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}\}$.

In the case of (i) (resp. case of (iii)), in [LW14] it is proved that $\deg(F_u(x)) = \frac{n+2}{2}$, and $\deg(F_u^{-1}(x)) \leq 3$ (resp. $\deg(F'(x)) = \frac{n+2}{2}$, $\deg(F'^{-1}(x)) \leq 7$). If the function is an involution, then we must have that $n = 4$ (resp. $n = 2$ or $n = 8$). One can checked experimentally that the function can not be involutory in these cases.

Next we consider the case of (ii), the compositional inverse of $F'_u(x)$ is the restriction of

$$x + u\left(x + u^{2^i+1}\right)^{\frac{2^i}{2^i+1}} + u^{2^i}\left(x + u^{2^i+1}\right)^{\frac{1}{2^i+1}}$$

to H_u [LW14]. If this function $F'_u(x)$ is an involution, then we must have

$$ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}} + x = x + u\left(x + u^{2^i+1}\right)^{\frac{2^i}{2^i+1}} + u^{2^i}\left(x + u^{2^i+1}\right)^{\frac{1}{2^i+1}},$$

i.e.,

$$ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}} = u\left(x + u^{2^i+1}\right)^{\frac{2^i}{2^i+1}} + u^{2^i}\left(x + u^{2^i+1}\right)^{\frac{1}{2^i+1}},$$

held for any $x \in H_u$. However, by case (i), we know that $ux^{\frac{2^i}{2^i+1}} + u^{2^i}x^{\frac{1}{2^i+1}}$ is a permutation when restricted to H_u, it follows then that $u = 0$, a contradiction. Therefore, $F'_u(x)$ can not be involutory as well.

7. Conclusion and Open Problems

In this paper, we studied the involutory property for S-boxes constructed from differentially 4-uniform permutations. If a function used as an S-box in some ciphers is an involution, then the implementation cost for its inverse is saved. This is an advantage in hardware implementation, especially in lightweight cryptography algorithms. Thus, the property of being involutory is a desired property for a good S-box. We examine all the differentially 4-uniform permutations in the literature and determine whether they can be involutory. Some differentially 4-uniform involutions with good cryptography properties are found, which providing more choices for the design of S-boxes with low hardware implementation. Now the list of all involutory differentially 4-uniform permutations is given in Table 1.

We know that if F is an involution over $\mathbb{F}_{2^n}$, and P is a permutation over $\mathbb{F}_{2^n}$, then $G = P^{-1} \circ F \circ P$ is an involution over $\mathbb{F}_{2^n}$ as well. Moveover, if F is differentially 4-uniform and P is affine, then G, which is affine equivalent to F, is a differentially 4-uniform involution. This construction is trivial. It is an interesting problem to investigate the case where P is not affine. It is also a challenging problem to give a characterization of the involution F and permutation P such that the involution G has lower differential uniformity over $\mathbb{F}_{2^n}$.

Table 1: Involutory Differentially 4-uniform Permutations

Functions	Conditions	References
x^{-1}	n is even	[Nyb93]
$x^{-1}+\mathbf{1}_U(x)$	(1) $U=\{0,1\}$, $n/2$ is odd, or (2) $U=\{\omega,\omega^2\}$, $n/2$ is odd, or (3) $U=\{0,1,\omega,\omega^2\}$	[QTTL13, PT16] [QTLG16, ZHSS15] [CDZQ16]
$F(x)=\begin{cases}\beta(x+1)^{-1}+\alpha & \text{if } x\in\mathbb{F}_{2^d}\\ x^{-1} & \text{if } x\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^d}\end{cases}$	(1) $\alpha=\beta=1$, or (2) $\alpha=0$, $\beta=1$, d is even, or (3) $\alpha=0$, $\beta=1$, $d=1,3$, $n/2$ is odd, or (4) $\alpha=\beta=\omega$ or ω^2, $d=2$, $n/2$ is odd, or (5) $\alpha=1$, $\mathrm{Tr}(\frac{1}{\beta})=1$, n/d is odd	[PT17]
$F(x)=\begin{cases}\beta x^{-1}+\alpha & \text{if } x\in\mathbb{F}_{2^d}\\ x^{-1} & \text{if } x\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^d}\end{cases}$	(1) $\alpha=\omega$, $\beta=\omega^2$, $d=2$, $n/2$ is odd, or (2) $\alpha=\omega^2$, $\beta=\omega$, $d=2$, $n/2$ is odd, or	[ZHS14]
$F(x)=\begin{cases}(\gamma x)^{-1} & \text{if } x\in U\\ x^{-1} & \text{if } x\in\mathbb{F}_{2^n}\backslash U\end{cases}$	$U=\bigcup_{g\in G} g\langle\gamma\rangle$, where $G\subseteq\mathbb{F}_{2^n}^*$, $\gamma\in\mathbb{F}_{2^n}^*$ is of order d such that (i) If $g\in G$, then $g^{-1}\in G$, and (ii) $\mathrm{Tr}(\gamma)=\mathrm{Tr}(\frac{1}{\gamma})=1$, and (iii) $\mathrm{Tr}\left(\frac{\gamma}{(g_i/g_j)\gamma^l+(g_j/g_i)\gamma^{-l}}\right)=1$, for any $g_i,g_j\in G$, $0\le l\le\frac{d-1}{2}$ (when $g_i=g_j$, then $1\le l\le\frac{d-1}{2}$)	[PTW16]
$F(x)=(\pi(x))^{-1}=\begin{cases}\alpha_{i+1}^{-1} & x=\alpha_i\\ x^{-1} & x\notin\pi\end{cases}$	(1) $\pi=(1\ \gamma\ \gamma^2)$, $\gamma\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$, $n/2$ is odd, or (2) $\pi=(0\ 1)$, $n/2$ is odd, or (3) $\pi=(\gamma\ \frac{1}{\gamma})$, $\mathrm{Tr}(\gamma)=\mathrm{Tr}(\frac{1}{\gamma})=1$	[LWY13]
$F(x_1,\ldots,x_{n-1},x_n)=\begin{cases}(1/x',0) & \text{if } x_n=0\\ (c/x',1) & \text{if } x_n=1\end{cases}$	$\mathrm{Tr}_1^{n-1}(c)=\mathrm{Tr}_1^{n-1}(\frac{1}{c})=1$	[CTTL14]
$\mathsf{H}_R(x,y)=\left(R_{R_y^{-1}(x)}(y),R_y^{-1}(x)\right)$	$n=2k$, k is odd, $\alpha\in\mathbb{F}_{2^k}^*$, $R_y(x)=R(x,y)$, (1) $\gcd(i,k)=1$, $R(x,y)=(x+\alpha y)^{2^i+1}+y^{2^i+1}$, or (2) $\beta\in\mathbb{F}_{2^k}^*$, $\beta\neq(1+\alpha)^3$, $R(x,y)=(x+\alpha y)^3+\beta y^3$	[PUB16] [FF16] [CDP16]

References

[BDMW10] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN permutation in demension six. In *Postproceedings of the 9th Intenational Conference on Finite Fields and Their Applications Fq'9*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.

[BL10] Carl Bracken and Gregor Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications*, 16(4):231–242, 2010.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[BTT12] Carl Bracken, Chik How Tan, and Yin Tan. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields and Their Applications*, 18(3):537–546, 2012.

[Car10] Claude Carlet. *Vectorial Boolean functions for cryptography*, volume 134 of *Encyclopedia of Mathematics and its Applications*, chapter 9, pages 398–471. Cambridge University Press, 2010.

[Car11] Claude Carlet. On known and new differentially uniform functions. In *Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, pages 1–15, 2011.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998.

[CDP16] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of Dillon's APN permutation with the best known differential and linear properties for all fields of size 2^{4k+2}. *IACR Cryptology ePrint Archive: Report 2016/887*, 2016. http://eprint.iacr.org/2016/887.

[CDZQ16] Xi Chen, Yazhi Deng, Min Zhu, and Longjiang Qu. An equivalent condition on the switching construction of differentially 4-uniform permutations on from the inverse function. *International Journal of Computer Mathematics*, pages 1–16, 2016.

[CTTL14] Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao. New construction of differentially 4-uniform bijections. In Dongdai Lin et al., editor, *Information Security and Cryptology: 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013*, pages 22–38. Springer International Publishing, 2014.

[CV94] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 356–365, 1994.

[Dob98] Hans Dobbertin. One-to-one highly nonlinear power functions on GF(2^n). *Applicable Algebra in Engineering, Communication and Computing*, 9(2):139–152, 1998.

[FF16] Shihui Fu and Xiutao Feng. Further results of the cryptographic properties on the butterfly structure. *CoRR*, abs/1607.08455, 2016.

[Gol68] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Information Theory*, 14(1):154–156, 1968.

[Hir98] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. Clarendon Press; Oxford University Press Oxford: New York, 2nd edition, 1998.

[Kas71] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information and Control*, 18(4):369–394, 1971.

[Knu94] Lars R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, pages 196–211, 1994.

[Lai94] Xuejia Lai. *Higher Order Derivatives and Differential Cryptanalysis*, volume 276 of *The Springer International Series in Engineering and Computer Science*, pages 227–233. Springer US, Boston, MA, 1994.

[LW14] Yongqiang Li and Mingsheng Wang. Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1}). *Des. Codes Cryptography*, 72(2):249–264, 2014.

[LWY13] Yongqiang Li, Mingsheng Wang, and Yuyin Yu. Constructing differentially 4-uniform permutations over gf(2^{2k}) from the inverse function revisited. *IACR Cryptology ePrint Archive: Report 2013/731*, 2013. https://eprint.iacr.org/2013/731.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 386–397, 1993.

[Nyb93] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 55–64, 1993.

[PT16] Jie Peng and Chik How Tan. New explicit constructions of differentially 4-uniform permutations via special partitions of $\mathbb{F}_{2^{2k}}$. *Finite Fields and Their Applications*, 40:73–89, 2016.

[PT17] Jie Peng and Chik How Tan. New differentially 4-uniform permutations by modifying the inverse function on subfields. *Cryptography and Communications*, 9(3):363–378, 2017.

[PTW16] Jie Peng, Chik How Tan, and Qichun Wang. A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k. *Science China Mathematics*, 59(6):1221–1234, 2016.

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 93–122, 2016.

[QTLG16] Longjiang Qu, Yin Tan, Chao Li, and Guang Gong. More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. *Des. Codes Cryptography*, 78(2):391–408, 2016.

[QTTL13] Longjiang Qu, Yin Tan, Chik How Tan, and Chao Li. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. *IEEE Trans. Information Theory*, 59(7):4675–4686, 2013.

[TCT15] Deng Tang, Claude Carlet, and Xiaohu Tang. Differentially 4-uniform bijections by permuting the inverse function. *Des. Codes Cryptography*, 77(1):117–141, 2015.

[YWL13] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. Constructing differentially 4 uniform permutations from known ones. *Chinese Journal of Electronics*, 22(3):495–499, 2013.

[ZHS14] Zhengbang Zha, Lei Hu, and Siwei Sun. Constructing new differentially 4-uniform permutations from the inverse function. *Finite Fields and Their Applications*, 25:64–78, 2014.

[ZHSS15] Zhengbang Zha, Lei Hu, Siwei Sun, and Jinyong Shan. Further results on differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$. *Science China Mathematics*, 58(7):1577–1588, 2015.