IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2017, No. 2, pp. 228–249. DOI:10.13154/tosc.v2017.i2.228-249

Differentially 4-Uniform Permutations with the Best Known Nonlinearity from Butterflies

Shihui Fu[1], Xiutao Feng*[1,2] and Baofeng Wu[2]

[1] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing, China
{fushihui,fengxt}@amss.ac.cn

[2] State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
wubaofeng@iie.ac.cn

Abstract. Many block ciphers use permutations defined over the finite field $\mathbb{F}_{2^{2k}}$ with low differential uniformity, high nonlinearity, and high algebraic degree to provide confusion. Due to the lack of knowledge about the existence of almost perfect nonlinear (APN) permutations over $\mathbb{F}_{2^{2k}}$, which have lowest possible differential uniformity, when $k > 3$, constructions of differentially 4-uniform permutations are usually considered. However, it is also very difficult to construct such permutations together with high nonlinearity; there are very few known families of such functions, which can have the best known nonlinearity and a high algebraic degree. At Crypto'16, Perrin et al. introduced a structure named butterfly, which leads to permutations over $\mathbb{F}_{2^{2k}}$ with differential uniformity at most 4 and very high algebraic degree when k is odd. It is posed as an open problem in Perrin et al.'s paper and solved by Canteaut et al. that the nonlinearity is equal to $2^{2k-1} - 2^k$. In this paper, we extend Perrin et al.'s work and study the functions constructed from butterflies with exponent $e = 2^i + 1$. It turns out that these functions over $\mathbb{F}_{2^{2k}}$ with odd k have differential uniformity at most 4 and algebraic degree $k + 1$. Moreover, we prove that for any integer i and odd k such that $\gcd(i, k) = 1$, the nonlinearity equality holds, which also gives another solution to the open problem proposed by Perrin et al. This greatly expands the list of differentially 4-uniform permutations with good nonlinearity and hence provides more candidates for the design of block ciphers.

Keywords: S-boxes · APN · butterfly structure · permutation · differential uniformity · nonlinearity

1 Introduction

In block ciphers nonlinear functions over finite fields are usually used as substitution boxes (S-boxes) to provide confusion. For the easiness of implementation and to obtain a permutation, S-boxes are usually chosen to be permutations over the finite field with characteristic 2 and an even extension degree, i.e., $\mathbb{F}_{2^{2k}}$. Besides, in order to resist various kinds of cryptographical attacks, S-boxes used in block ciphers should possess, for example, low differential uniformity (to resist differential attack [BS91]), and high nonlinearity (to resist linear attack [Mat93]).

It is well known that for any function defined over $\mathbb{F}_{2^n}$, its differential uniformity must be even. So a lower bound of the differential uniformity is 2, and the functions achieving this value are called almost perfect nonlinear (APN) functions. Unfortunately, it is very

*Corresponding author

Received: 2016-11-23, Revised: 2017-03-01, Accepted: 2017-05-02, Published: 2017-06-19

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 BIG APN problem.

Therefore, when the input sizes are even, a natural tradeoff is to use differentially 4-uniform permutations as the nonlinear functions. For instance, the AES block cipher uses a differentially 4-uniform permutation, namely the inverse function over $\mathbb{F}_{2^8}$ as S-boxes. Hence, to provide more choices for the design of block ciphers, it is of significant importance to construct more classes of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$.

Besides, the nonlinear functions should have high (or at least not low) algebraic degree to resist the higher-order differential attack [Knu94, Lai94] (which is described by Knudsen when the degree is 2). Qu et al. [QTTL13, QTLG16], Peng et al. [PT16] and Tang et al. [TCT15] proposed several families of differentially 4-uniform permutations with optimal algebraic degree from the inverse function by applying the powerful switching method. Later, Zha et al. [ZHS14, ZHSS15] presented some more families of differentially 4-uniform permutations with optimal algebraic degree by applying affine transformations on the elements of some subfields of the inverse function. In [CTTL14], Carlet et al. built a family of differentially 4-uniform permutations with optimal algebraic degree by concatenating two functions from $\mathbb{F}_{2^{n-1}}$ to $\mathbb{F}_{2^n}$ for even $n \geq 6$.

In [BL10, Table 1], the authors list some differentially 4-uniform permutations with nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$ (the best we have known) over the fields of even extension degree. Up to now, the known such functions are Gold functions, Kasami functions, Inverse function, Bracken–Leander functions [BL10], a class of binomials found by Bracken et al. [BTT12] and those functions constructed from quadratic APN permutations over $\mathbb{F}_{2^{2k+1}}$ [LW14a]. We can see that the list of differentially 4-uniform permutations with the best known nonlinearity and high algebraic degree over the fields of even extension degree is still limited. As pointed out by Carlet [Car10], the alternatives for the inverse function are very rare and it is also a main challenge to find more such functions. Thus, constructing more differentially 4-uniform permutations with high nonlinearity and algebraic degree is very necessary, which is still an open problem up to now.

Recently in [PUB16], Perrin et al. introduced two new structures called open and closed butterflies and showed that these functions constructed from butterflies with exponent $e = 3$ always have differential uniformity at most 4 and algebraic degree $k + 1$ when $n = 2k$ with odd k. The authors also verified experimentally that the nonlinearity of these functions are equal to $2^{2k-1} - 2^k$ for $k = 3, 5, 7$. However, they could not prove it in the general case and conjectured that it is true for every odd k.

In [CDP17], Canteaut et al. generalise the family of butterflies, and showed that when $e = 3$, the generalised butterflies have differential uniformity exactly 4 with one exception which is affine equivalent to the Dillon's APN permutation. They also prove that this family functions have the best known nonlinearity and give their algebraic degree.

In [LW14b], Li and Wang proposed a construction from 3-round Feistel structure, which is actually a particular case of the butterfly with trivial coefficient 1. They proved that these functions have differential uniformity 4 and algebraic degree k.

The low cost of hardware implementation of nonlinear functions is also an important criterion in the design of S-boxes. As the cost of nonlinear functions increases with its input and output size, implementing functions over small subfields often costs much less than implementing functions over the larger field. It is a huge advantage of constructing S-boxes over $(\mathbb{F}_{2^k})^2$ from butterflies since we only need to implement the exponentiation and the multiplication in $\mathbb{F}_{2^k}$. Besides, these functions constructed from open butterflies are actually involutory, which means that the implementation of the inverse does not require additional resources, so it is particularly useful in devices with limited resources. There are many works on efficient techniques for implementing S-boxes, for instance, see [SP04, EKP$^+$07, SD16].

In this paper, we study the functions constructed from butterflies with exponent $e = 2^i + 1$ and prove that these functions also have differential uniformity at most 4 and their algebraic degree are $k+1$ when $n = 2k$ for k odd. Moveover, we prove that their nonlinearity is the best in the sense that no known functions over the field of even extension degree have a higher nonlinearity. Finally, we study the function with trivial coefficient $\alpha = 1$, and show that it also has the best known nonlinearity. Hence, some new infinite families of differentially 4-uniform permutations with the best known nonlinearity and high algebraic degree are obtained. Besides, the function constructed from closed butterfly with trivial coefficient is also a permutation.

The rest of the paper is organized as follows. In the next section, we recall some basic backgrounds, including some necessary definitions and results. In Section 3, we show that these functions with odd branch size k, exponent $e = (2^i + 1)$ and nontrivial coefficient have differential uniformity at most 4 and the best known nonlinearity. In Section 4, we further revisit these functions with coefficient $\alpha = 1$ and show that they have the best known nonlinearity as well. The proof of bijective property of functions constructed from closed butterfly is also given in this section. Conclusions and some open problems are given in Section 5.

2 Preliminaries

Let n be a positive integer, $\mathbb{F}_{2^n}$ be the finite field with 2^n elements, $\mathbb{F}_{2^n}^*$ be its multiplicative group, and $\mathbb{F}_{2^n}[x]$ be the polynomial ring over $\mathbb{F}_{2^n}$. Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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, $0 \le l \le 2^n - 1$, 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. It is well known that the algebraic degree of F is equal to the maximal 2-weight of the exponent i such that $c_i \neq 0$.

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

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

where $\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. 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

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

The Parseval's relation states that, for any $b \in \mathbb{F}_{2^n}^*$:

$$\sum_{a \in \mathbb{F}_{2^n}} (\mathcal{W}_F(a,b))^2 = 2^{2n}.$$

This implies that $\mathcal{NL}(F) \leq 2^{n-1} - 2^{n/2-1}$. Moreover, 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 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 best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$. It is conjectured that $\mathcal{NL}(F)$ is upper bounded by $2^{n-1} - 2^{\frac{n}{2}}$ [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 $A_3 = 0$ (resp. $A_3 = 0$ and A_1, A_2 are linear permutations over $\mathbb{F}_{2^n}$), then they are called affine (resp. linear) 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 invariant of both EA-equivalence and CCZ-equivalence. Algebraic degree is preserved by EA-equivalence, but not by CCZ-equivalence. However, in general, neither EA-equivalence nor CCZ-equivalence preserves the permutation property.

Definition 2 (See [PUB16]). Let k be a positive integer and $\alpha \in \mathbb{F}_{2^k}$, e be an integer such that the mapping $x \mapsto x^e$ is a permutation over $\mathbb{F}_{2^k}$ and $R_z[e,\alpha](x) = (x + \alpha z)^e + z^e$ be a keyed permutation. The *butterfly structures* over $(\mathbb{F}_{2^k})^2$ are defined as follows:

1. the *open butterfly structure* with branch size k, exponent e and coefficient α is a function denoted H_e^α (see Figure 1a) defined by:

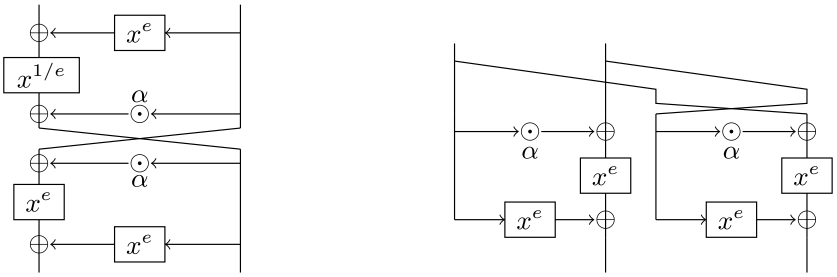
$$\mathsf{H}_e^\alpha(x,y) = \left(R_{R_y^{-1}[e,\alpha](x)}[e,\alpha](y), R_y^{-1}[e,\alpha](x)\right),$$

2. the *closed butterfly structure* with branch size k, exponent e and coefficient α is a function denoted V_e^α (see Figure 1b) defined by:

$$\mathsf{V}_e^\alpha(x,y) = (R_x[e,\alpha](y), R_y[e,\alpha](x)).$$

Note that H_e^α is always a permutation over $(\mathbb{F}_{2^k})^2$, while V_e^α maybe not. Moreover, H_e^α is an involution over $(\mathbb{F}_{2^k})^2$, i.e., $\mathsf{H}_e^\alpha(\mathsf{H}_e^\alpha(x,y)) = (x,y)$, which means that the compositional inverse of H_e^α is itself. Furthermore, the permutation H_e^α and the function V_e^α are CCZ-equivalent [PUB16].

Let L be an extension of a field K and $\mathrm{Gal}(L/K)$ be the Galois group of L over K. For any $\sigma \in \mathrm{Gal}(L/K)$ and any $x \in L$, let $\sigma^0(x) = x, \sigma^j(x) = \sigma(\sigma^{j-1}(x))$. Then for a



(a) Open butterfly H_e^α (bijective).

(b) Closed butterfly V_e^α.

Figure 1: The butterfly structures.

given polynomial $w(t) = \sum_{j=0}^{l} c_j t^j \in L[t]$, $w(\sigma)$ acting on the element x is defined as $w(\sigma)x = \sum_{j=0}^{l} c_j \sigma^j(x)$. The following lemma characterizes the size of solution space of $w(\sigma)x = 0$ and will be of use in the sequel.

Lemma 1 (See [GQ09]). *Let L be a cyclic Galois extension of K of degree n and suppose that σ generates the Galois group of L over K. Let m be an integer satisfying $1 \leq m \leq n$ and $w(t)$ be a polynomial of degree m in $L[t]$. Let*

$$R = \{x \in L : w(\sigma)x = 0\}.$$

Then we have $\dim_K R \leq m$.

It is well known that the Frobenius automorphism $\sigma(x) = x^2$ generates the cyclic group $\mathrm{Gal}(\mathbb{F}_{2^k}/\mathbb{F}_2) \cong \mathbb{Z}/k\mathbb{Z}$. Moveover, if $\gcd(i,k) = 1$, then $\sigma^i(x) = x^{2^i}$ is also a generator. We have the following corollary.

Corollary 1. *Suppose k and i are two integers such that $\gcd(i,k) = 1$. For any $c_1, c_2, c_3 \in \mathbb{F}_{2^k}$ which are not all zero, the following equation*

$$c_1 x^{2^{2i}} + c_2 x^{2^i} + c_3 x = 0$$

has at most 4 solutions in $\mathbb{F}_{2^k}$.

Moreover, if k is an odd integer and $\gcd(i,k) = 1$, then $\gcd(2i,k) = 1$. The next corollary is obvious.

Corollary 2. *Suppose k is an odd integer and $\gcd(i,k) = 1$. For any $c_1, c_2, c_3 \in \mathbb{F}_{2^k}$ which are not all zero, the following equation*

$$c_1 x^{2^{4i}} + c_2 x^{2^{2i}} + c_3 x = 0$$

has at most 4 solutions in $\mathbb{F}_{2^k}$.

3 Butterfly Structures with $\alpha \neq 0, 1$

In this section we shall study the butterfly structures with $\alpha \neq 0, 1$ for odd branch sizes k, and give their differential uniformity, algebraic degree and nonlinearity. Below we make the convention that k is always an odd positive integer unless explicitly mentioned.

For a given non-negative integer i, if $\gcd(i,k) = 1$, then we have also $\gcd(2i,k) = 1$, which implies that $\gcd(2^i \pm 1, 2^k - 1) = 1$. So both mappings $x \mapsto x^{2^i+1}$ and $x \mapsto x^{2^i-1}$ are bijective over $\mathbb{F}_{2^k}$.

3.1 Differential Uniformity

In order to characterize the differential uniformity of the butterfly structures, we first introduce a lemma.

Lemma 2. *Let i be an integer such that $\gcd(i,k)=1$. Then for any $\alpha\in\mathbb{F}_{2^k}$ with $\alpha\neq 0,1$, the equation system in variables u,v*

$$\begin{cases}(\alpha v+u)\left(\alpha(\alpha u+v)^{2^i}+u^{2^i}\right)+(\alpha v+u)^{2^i}\left(\alpha^{2^i}(\alpha u+v)+u\right)=0, & (1)\\ (\alpha v+u)(\alpha u+v)+\left(\alpha^{2^i}(\alpha u+v)+u\right)\left(\alpha^{2^i}(\alpha v+u)+v\right)=0, & (2)\\ (\alpha v+u)(\alpha u+v)^{2^i}+\left(\alpha^{2^i}(\alpha u+v)+u\right)\left(\alpha(\alpha v+u)^{2^i}+v^{2^i}\right)=0 & (3)\end{cases}$$

holds over $\mathbb{F}_{2^k}$ if and only if u,v satisfy both $\alpha v+u=0$ and $\alpha^{2^i}(\alpha u+v)+u=0$.

Proof. The sufficiency is obvious. Now we consider the necessity, and suppose that at least one of $\alpha v+u$ and $\alpha^{2^i}(\alpha u+v)+u$ is not equal to 0. Below we discuss three cases separately.

1. $\alpha v+u=0,\alpha^{2^i}(\alpha u+v)+u\neq 0$. Then $u\neq 0,v\neq 0$, and Eqn. (2) implies $\left(\alpha^{2^i}(\alpha u+v)+u\right)v=0$, which is impossible.

2. $\alpha v+u\neq 0,\alpha^{2^i}(\alpha u+v)+u=0$. Then by Eqn. (2) we get $\alpha u+v=0$. We further have $u=v=0$, which contradicts with $\alpha v+u\neq 0$.

3. $\alpha v+u\neq 0,\alpha^{2^i}(\alpha u+v)+u\neq 0$.

   We first claim that both $u\neq 0$ and $v\neq 0$. This is because: if $u=0$, then $v\neq 0$. By Eqn. (1) we have $(\alpha^{2^i}+\alpha)^2=0$, which is impossible since $\alpha\neq 0,1$ and $\gcd(i,k)=1$. If $v=0$, then $u\neq 0$. By Eqn. (2) and (3), we have $\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha=0$ and $\alpha^{2^i+2}+\alpha^{2^i}+\alpha=0$ respectively. Hence, $\alpha^{2^{i+1}+1}+\alpha^{2^i+2}=\alpha^{2^i+1}(\alpha^{2^i}+\alpha)=0$, which is impossible too.

   Next we claim both $\alpha(\alpha u+v)^{2^i}+u^{2^i}\neq 0$ and $\alpha u+v\neq 0$. Indeed, if $\alpha(\alpha u+v)^{2^i}+u^{2^i}=0$, then by Eqn. (1), we have $\alpha v+u=0$ or $\alpha^{2^i}(\alpha u+v)+u=0$, which contradicts the hypothesis. If $\alpha u+v=0$, then we have $\alpha v+u\neq 0$ and $u\neq 0$. By Eqn. (1), we have $(\alpha v+u)u^{2^i}=(\alpha v+u)^{2^i}u$, which can be reduced to that $u^{2^i-1}=(\alpha v+u)^{2^i-1}$. Recall that x^{2^i-1} is a permutation, we have $u=\alpha v+u$, which is impossible since $\alpha\neq 0$ and $v\neq 0$.

   By Eqn. (1) and (3), we have

$$\frac{(\alpha v+u)^{2^i}}{\alpha(\alpha u+v)^{2^i}+u^{2^i}}=\frac{\alpha v+u}{\alpha^{2^i}(\alpha u+v)+u}=\frac{\alpha(\alpha v+u)^{2^i}+v^{2^i}}{(\alpha u+v)^{2^i}}.$$

   For simplifying the above expressions, we denote $\alpha=\beta^{2^i}$. Then $\beta\neq 0,1$. From the above equation we get

$$\frac{(\alpha v+u)^{2^i}}{(\beta(\alpha u+v)+u)^{2^i}}=\frac{(\beta(\alpha v+u)+v)^{2^i}}{(\alpha u+v)^{2^i}},$$

   which is equivalent to

$$(\alpha v+u)(\alpha u+v)=(\beta(\alpha u+v)+u)(\beta(\alpha v+u)+v). \qquad (4)$$

Compare the above equation with (2), and we get

$$(\beta(\alpha u+v)+u)(\beta(\alpha v+u)+v)=\left(\alpha^{2^i}(\alpha u+v)+u\right)\left(\alpha^{2^i}(\alpha v+u)+v\right),$$

which can be further simplified as

$$(\alpha^{2^i}+\beta)^2(\alpha u+v)(\alpha v+u)+(\alpha^{2^i}+\beta)(u^2+v^2)=0.$$

Note that $\alpha^{2^i}+\beta=\beta^{2^{2i}}+\beta\neq 0$ since $\beta\neq 0,1$ and $\gcd(2i,k)=1$, thus we divide both sides of the above equation by $\alpha^{2^i}+\beta$, and get

$$(\alpha^{2^i}+\beta)(\alpha u+v)(\alpha v+u)+u^2+v^2=0.$$

Let $u=\lambda v$, where $\lambda\neq 0$. So we have

$$(\alpha^{2^i+1}+\alpha\beta+1)\lambda^2+(\alpha^{2^i}+\beta)(\alpha^2+1)\lambda+(\alpha^{2^i+1}+\alpha\beta+1)=0. \tag{5}$$

The coefficient of λ^2 does not vanish. Otherwise, we have $\mathrm{Tr}(\alpha^{2^i+1}+\alpha\beta+1)=\mathrm{Tr}\left((\beta^{2^i+1})^{2^i}+\beta^{2^i+1}+1\right)=\mathrm{Tr}(1)=0$, which is impossible since k is odd. Therefore, divided by $\alpha^{2^i+1}+\alpha\beta+1$, Eqn. (5) is equivalent to

$$\lambda^2+\frac{(\alpha^{2^i}+\beta)(\alpha^2+1)}{\alpha^{2^i+1}+\alpha\beta+1}\lambda+1=0. \tag{6}$$

Further by Eqn. (2), we get

$$(\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha)\lambda^2+(\alpha^{2^{i+1}+2}+\alpha^{2^{i+1}}+\alpha^2)\lambda+(\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha)=0.$$

If $\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha=0$, since $\alpha^{2^{i+1}+2}+\alpha^{2^{i+1}}+\alpha^2=(\alpha+1)^{2(2^i+1)}+1\neq 0$, it follows $\lambda=0$, which is a contradiction. Divided by $\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha$, the above equation becomes

$$\lambda^2+\frac{\alpha^{2^{i+1}+2}+\alpha^{2^{i+1}}+\alpha^2}{\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha}\lambda+1=0. \tag{7}$$

Each equation in the variable λ of (6) and (7), either has two solutions or has no solution in $\mathbb{F}_{2^k}$. Moreover, it is noticed that two solutions of each equation are of the forms λ and λ^{-1}, which means that the sets of solutions of two equations are identical or non-intersected. If their intersection is empty, then at least one of Eqn. (1)-(3) does not hold. If the two solution sets are identical, we must have

$$\frac{(\alpha^{2^i}+\beta)(\alpha^2+1)}{\alpha^{2^i+1}+\alpha\beta+1}=\frac{\alpha^{2^{i+1}+2}+\alpha^{2^{i+1}}+\alpha^2}{\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha}.$$

We replace α with β^{2^i}, and reduce the above equation to

$$\beta^{2^{2i}+2^{i+1}+1}+\beta^{2^{2i}+1}+\beta^{2^{2i}+2^i}+\beta^{2^{i+1}}+\beta^{2^i+1}=0, \tag{8}$$

which is further equivalent to the following equation

$$\beta^{(2^i+1)^2}=(\beta^{2^i}+\beta)^{2^i+1}.$$

Recall that x^{2^i+1} is a permutation over $\mathbb{F}_{2^k}$, hence we have

$$\beta^{2^i+1}+\beta^{2^i}+\beta=(\beta+1)^{2^i+1}+1=0,$$

which contradicts with $\beta\neq 0$. Therefore, at least one of Eqn. (1)-(3) does not hold.

So combining the above three cases, we get the conclusion. □

Theorem 1. *Let i be an integer such that $\gcd(i,k)=1$. For any $0\le t\le k-1$, $\alpha\in\mathbb{F}_{2^k}$ with $\alpha\neq 0,1$, let H_e^α and V_e^α be the open and closed $2k$-bit butterfly structures with exponent $e=(2^i+1)\times 2^t$ and coefficient α respectively. Then the differential uniformity of both H_e^α and V_e^α are at most 4.*

Proof. Since H_e^α and V_e^α are CCZ-equivalent, they have the same differential uniformity. It is sufficient to prove that the differential uniformity of V_e^α is at most 4. Besides, the functions V_e^α with exponent $e=(2^i+1)\times 2^t$ are affine equivalent to the functions V_e^α with exponent $e=2^i+1$. Thus we only consider the case where the exponent is equal to 2^i+1.

Let $u,v,a,b\in\mathbb{F}_{2^k}$, where $(u,v)\neq(0,0)$. Then we need to prove that

$$\mathsf{V}_e^\alpha(x,y)+\mathsf{V}_e^\alpha(x+u,y+v)=(a,b), \tag{9}$$

namely, the equation system

$$\begin{cases} \left(\alpha^{2^i}(\alpha u+v)+u\right)x^{2^i}+\left(\alpha(\alpha u+v)^{2^i}+u^{2^i}\right)x \\ \qquad\qquad +(\alpha u+v)y^{2^i}+(\alpha u+v)^{2^i}y=(\alpha u+v)^{2^i+1}+u^{2^i+1}+a, \\ (\alpha v+u)x^{2^i}+(\alpha v+u)^{2^i}x+\left(\alpha^{2^i}(\alpha v+u)+v\right)y^{2^i} \\ \qquad\qquad +\left(\alpha(\alpha v+u)^{2^i}+v^{2^i}\right)y=(\alpha v+u)^{2^i+1}+v^{2^i+1}+b \end{cases}$$

has at most 4 solutions in $(\mathbb{F}_{2^k})^2$. Notice that this system is affine in variables x,y, then it is enough to prove that the following linear system

$$\begin{cases} \left(\alpha^{2^i}(\alpha u+v)+u\right)x^{2^i}+\left(\alpha(\alpha u+v)^{2^i}+u^{2^i}\right)x+(\alpha u+v)y^{2^i}+(\alpha u+v)^{2^i}y=0, & (10)\\ (\alpha v+u)x^{2^i}+(\alpha v+u)^{2^i}x+\left(\alpha^{2^i}(\alpha v+u)+v\right)y^{2^i}+\left(\alpha(\alpha v+u)^{2^i}+v^{2^i}\right)y=0 & (11)\end{cases}$$

has at most 4 solutions in $(\mathbb{F}_{2^k})^2$. Below we consider two cases depending on whether $\alpha^{2^i}(\alpha u+v)+u=0$ or not.

CASE 1 : $\alpha^{2^i}(\alpha u+v)+u=0$. Then we must have $\alpha u+v\neq 0$, otherwise, we have $u=v=0$, which leads to a contradiction. Further we have

$$\alpha(\alpha u+v)^{2^i}+u^{2^i}=\alpha(\alpha u+v)^{2^i}+\left(\alpha^{2^i}(\alpha u+v)\right)^{2^i}=(\alpha^{2^{2i}}+\alpha)(\alpha u+v)^{2^i}\neq 0,$$

since $\alpha\neq 0,1$ and $\gcd(2i,k)=1$. Then Eqn. (10) can be written as

$$x=\frac{\alpha u+v}{(\alpha^{2^{2i}}+\alpha)(\alpha u+v)^{2^i}}y^{2^i}+\frac{1}{\alpha^{2^{2i}}+\alpha}y. \tag{12}$$

If $\alpha v+u=0$, Eqn. (11) implies $vy^{2^i}+v^{2^i}y=0$. Note that $v\neq 0$, thus $y=0$ or $y=v$. Since Eqn. (12) in x has exactly one solution for each y, thus the total number of solutions of the equation system is equal to 2.

If $\alpha v+u\neq 0$, we replace the x in Eqn. (11) by Eqn. (12) and get

$$A_1y^{2^{2i}}+A_2y^{2^i}+A_3y=0,$$

where $A_1=\frac{(\alpha v+u)(\alpha u+v)^{2^i}}{(\alpha^{2^{2i}}+\alpha)^{2^i}(\alpha u+v)^{2^{2i}}}\neq 0$, and A_2, A_3 are some expressions in α,u,v. By Corollary 1, the above equation in y has at most 4 solutions. From Eqn. (12), x is uniquely determined by y, thus the total number of solutions of the equation system is at most equal to 4.

CASE 2 : $\alpha^{2^i}(\alpha u + v) + u \neq 0$.

If $\alpha v + u = 0$, Eqn. (11) becomes $vy^{2^i} + v^{2^i}y = 0$. Similarly we have $y = 0$ or $y = v$. For each of y, Eqn. (10) in x has at most 2 solutions since the coefficient of x^{2^i} does not vanish. Thus the total number of the solutions of the equation system is at most equal to 4.

If $\alpha v + u \neq 0$, we multiply Eqn. (10) and (11) by $\alpha v + u$ and $\alpha^{2^i}(\alpha u + v) + u$ respectively, and then add them to eliminate x^{2^i}, obtaining

$$A_4 x + A_5 y^{2^i} + A_6 y = 0, \tag{13}$$

where

$$\begin{aligned}
A_4 &= (\alpha v + u)\left(\alpha(\alpha u + v)^{2^i} + u^{2^i}\right) + (\alpha v + u)^{2^i}\left(\alpha^{2^i}(\alpha u + v) + u\right),\\
A_5 &= (\alpha v + u)(\alpha u + v) + \left(\alpha^{2^i}(\alpha u + v) + u\right)\left(\alpha^{2^i}(\alpha v + u) + v\right),\\
A_6 &= (\alpha v + u)(\alpha u + v)^{2^i} + \left(\alpha^{2^i}(\alpha u + v) + u\right)\left(\alpha(\alpha v + u)^{2^i} + v^{2^i}\right).
\end{aligned}$$

By Lemma 2, not all of A_4, A_5, A_6 are equal to zero.

If $A_4 = 0$, Eqn. (13) in y has at most 2 solutions. For each y, Eqn. (10) in x has at most 2 solutions. Hence the total number of solutions of the equation system is at most equal to 4.

If $A_4 \neq 0$ and $A_5 = A_6 = 0$, then $x = 0$. It is easy to observe that not both of $\alpha^{2^i}(\alpha v + u) + v$ and $\alpha(\alpha v + u)^{2^i} + v^{2^i}$ are equal to 0. Otherwise, we get $(\alpha^{2^{2i}} + \alpha)(\alpha v + u)^{2^i} = 0$ implying that $\alpha = 0$ or $\alpha = 1$ since $\gcd(2i, k) = 1$, which has been excluded by the hypothesis. When $x = 0$, since the coefficients in Eqn. (11) cannot simultaneously vanish, Eqn. (11) has at most 2 solutions in y. Hence the total number of the solutions of the equation system is at most equal to 2.

If $A_4 \neq 0, A_5 = 0, A_6 \neq 0$, we combine Eqn. (10) and (13) to eliminate x, and get

$$A_7 y^{2^i} + A_8 y = 0, \tag{14}$$

where A_7 is an expression in α, u, v and $A_8 = \left(\alpha(\alpha u + v)^{2^i} + u^{2^i}\right)\frac{A_6}{A_4} + (\alpha u + v)^{2^i}$. Indeed we have $A_8 \neq 0$ (see Appendix A), so Eqn. (14) in y has at most 2 solutions. For each y, Eqn. (13) in x has exactly one solution. Hence the equation system has at most 2 solutions.

If $A_4 \neq 0$ and $A_5 \neq 0$, similarly we eliminate x from Eqn. (11) and get

$$A_9 y^{2^{2i}} + A_{10} y^{2^i} + A_{11} y = 0, \tag{15}$$

where $A_9 = (\alpha v + u)\left(\frac{A_5}{A_4}\right)^{2^i} \neq 0$ and A_{10}, A_{11} are some expressions in α, u, v. By Corollary 1, Eqn. (15) in y has at most 4 solutions. For each y, Eqn. (13) in x has exactly one solution. Hence Eqn. (9) has at most 4 solutions.

Combining the discussion of all cases, we get that the above linear equation system has at most 4 solutions in $(\mathbb{F}_{2^k})^2$. So the conclusion follows. □

Remark 1. In [PUB16], it has been proved that the 6-bit APN permutation described by Dillon et al. is affine equivalent to the butterfly structure H_6^2, where $2 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2$ is viewed as an element $0 \cdot 1 + 1 \cdot X + 0 \cdot X^2 = X$ in $\mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$. In [CDP17], the authors showed that when $e = 3$, the butterflies do not contain any APN permutation except the foregoing one. However, when $k > 3$, $e \neq 3$, the pairs (e, α) such that H_e^α is APN are not yet found. Perrin et al. verified experimentally that butterfly structures are never differentially 4-uniform for $k = 4, 8, 10$, while for $k = 6$, there does exist α such that H_e^α (e.g., H_5^α) is differentially 4-uniform.

3.2 Algebraic Degree

When $e = 2^i + 1$, the two components of $\mathsf{V}_e^\alpha(x, y)$ are equal to $(\alpha x + y)^{2^i+1} + x^{2^i+1}$ and $(x + \alpha y)^{2^i+1} + y^{2^i+1}$ respectively. It is obvious that they are quadratic. Below we consider the open butterfly structure H_e^α, and we use the same method as in [CDP17] to determine its degree. First the following lemma is needed.

Lemma 3 (See [Nyb93])**.** *Let i be a non-negative integer such that* $\gcd(i, k) = 1$. *Then the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^k}$ is also a power function x^t, and its algebraic degree is $\frac{k+1}{2}$, where $t = \sum_{j=0}^{\frac{k-1}{2}} 2^{2ji} \mod (2^k - 1)$.*

Now we consider the second component of the open butterfly H_e^α, which is equal to $(x + y^{2^i+1})^{\frac{1}{2^i+1}} + \alpha y$. Its algebraic degree is mainly determined by the algebraic degree of the first term. By Lemma 3, we have

$$(x + y^{2^i+1})^{\frac{1}{2^i+1}} = \sum_{J\subseteq[0,(k-1)/2]} \underbrace{\prod_{j\in J} y^{(2^i+1)\cdot 2^{2ji}}}_{\deg\leq 2|J|} \; \underbrace{\prod_{j\in\overline{J}} x^{2^{2ji}}}_{\deg=(k+1)/2-|J|},$$

where $\overline{J}$ is the complement of J in $[0, (k-1)/2]$. The algebraic degree of each term in this sum is at most equal to $(k + 1)/2 + |J| = k + 1 - |\overline{J}|$.

If $\overline{J} = \emptyset$, then x is absent from the term, so the corresponding term is equal to y and has algebraic degree 1.

If $|\overline{J}| = 1$, then the algebraic degree of these terms are at most equal to $k + 1 - 1 = k$. Moveover, if $\overline{J} = \{j\}$ for some j, then the term is equal to

$$x^{2^{2ji}} y^{2^k-(2^i+1)\cdot 2^{2ji}} = x^{2^{2ji}} y^{(2^k-1)-(2^{(2j+1)i}+2^{2ji}-1)}.$$

If $j = 0$, then the term is equal to $xy^{(2^k-1)-2^i}$ and has algebraic degree $1 + k - 1 = k$. If $j = (k-1)/2$, then the term is equal to $x^{2^{(k-1)i}} y^{(2^k-1)-2^{(k-1)i}}$ and has algebraic degree $1 + k - 1 = k$. If $j \neq 0, (k-1)/2$, then $2ji \not\equiv 0 \pmod{k}$, $(2j + 1)i \not\equiv 0 \pmod{k}$ and $2ji \not\equiv (2j + 1)i \pmod{k}$ since $\gcd(i, k) = 1$. For any integer l, $\overline{l}$ denotes the unique integer r, $0 \leq r < k$ such that $l = qk + r$ with $q \in \mathbb{Z}$. Then $0 < \overline{2ji} < k$, $0 < \overline{(2j+1)i} < k$ and $\overline{2ji} \neq \overline{(2j+1)i}$. Hence its algebraic degree is

$$1 + k - w_2(2^{(2j+1)i} + 2^{2ji} - 1) = \begin{cases} k - \overline{2ji} & \text{if } \overline{2ji} < \overline{(2j+1)i}, \\ k - \overline{(2j+1)i} & \text{if } \overline{2ji} > \overline{(2j+1)i}, \end{cases}$$

which is always less than k. Therefore, this component has two terms of degree k, corresponding to $j = 0$ and $j = (k-1)/2$. Notice that $i \pmod{k}$ does not vanish since $\gcd(i, k) = 1$, then those two terms are distinct.

When $|\overline{J}| > 1$, the algebraic degree of these terms are at most equal to $k+1-2 = k-1$. Thus, the second component of H_e^α has algebraic degree k.

Next we consider the first component of H_e^α, which is equal to

$$\left(y + \alpha\left(\left(x + y^{2^i+1}\right)^{\frac{1}{2^i+1}} + \alpha y\right)\right)^{2^i+1} + \left(\left(x + y^{2^i+1}\right)^{\frac{1}{2^i+1}} + \alpha y\right)^{2^i+1}.$$

Let $z = \left(x + y^{2^i+1}\right)^{\frac{1}{2^i+1}}$, then from the above expression we deduce that

$$\begin{aligned} &(y + \alpha\,(z + \alpha y))^{2^i+1} + (z + \alpha y)^{2^i+1} \\ =& \left(1 + \alpha^{2^{i+1}+2} + \alpha^2 + \alpha^{2^{i+1}} + \alpha^{2^i+1}\right) y^{2^i+1} + \left(\alpha^{2^i+1} + 1\right) z^{2^i+1} \\ &+ \left(\alpha^{2^{i+1}+1} + \alpha + \alpha^{2^i}\right) y^{2^i} z + \left(\alpha^{2^i+2} + \alpha^{2^i} + \alpha\right) y z^{2^i}. \end{aligned}$$

The first two terms have algebraic degree at most two. So the terms of highest algebraic degree in this component are of the forms $y^{2^i}z$ or yz^{2^i}.

Since z has algebraic degree k, we deduce that the first component of H_e^α has algebraic degree at most $k+1$. The only terms in this component which may have algebraic degree $k+1$ correspond to terms of algebraic degree k in z, namely (omitting the coefficients):

$$\begin{array}{rrcl}
y^{2^i}z,\ j=0: & y^{2^i}xy^{(2^k-1)-2^i} & = & xy^{2^k-1}, \\
y^{2^i}z,\ j=\frac{k-1}{2}: & y^{2^i}x^{2^{(k-1)i}}y^{(2^k-1)-2^{(k-1)i}} & = & x^{2^{(k-1)i}}y^{(2^k-1)-(2^{(k-1)i}-2^i)}, \\
yz^{2^i},\ j=0: & y\left(xy^{(2^k-1)-2^i}\right)^{2^i} & = & x^{2^i}y^{(2^k-1)-(2^{2i}-1)}, \\
yz^{2^i},\ j=\frac{k-1}{2}: & y\left(x^{2^{(k-1)i}}y^{(2^k-1)-2^{(k-1)i}}\right)^{2^i} & = & xy^{2^k-1}.
\end{array}$$

Only the first and the last terms have algebraic degree $k+1$. Therefore, the term of algebraic degree $k+1$ in the first component of H_e^α is

$$\left(\alpha^{2^{i+1}+1}+\alpha+\alpha^{2^i}\right)xy^{2^k-1}+\left(\alpha^{2^i+2}+\alpha^{2^i}+\alpha\right)xy^{2^k-1}=\left(\alpha^{2^{i+1}+1}+\alpha^{2^i+2}\right)xy^{2^k-1}.$$

When $\alpha\neq 0,1$, then $\alpha^{2^{i+1}+1}+\alpha^{2^i+2}\neq 0$ since $\gcd(i,k)=1$. It follows that the first component of H_e^α thus the whole function has algebraic degree $k+1$. In the case of $\alpha=1$, the coefficient $\alpha^{2^{i+1}+1}+\alpha^{2^i+2}=0$, so the whole function has algebraic degree k because of the second component.

Theorem 2. *Let i be an integer such that $\gcd(i,k)=1$. For any $0\leq t\leq k-1$, $\alpha\in\mathbb{F}_{2^k}^*$, let H_e^α and V_e^α be the open and closed $2k$-bit butterfly structures with exponent $e=(2^i+1)\times 2^t$ and coefficient α respectively. Then*

1. *The closed butterfly V_e^α has algebraic degree 2.*
2. *The open butterfly H_e^α has algebraic degree $k+1$ or k. It is equal to k if and only if $\alpha=1$.*

We will use the following lemma in next section, which gives the connection between the Walsh spectrum and algebraic degree of a function over $\mathbb{F}_{2^n}$.

Lemma 4 (See [Lan90, CCZ98])**.** *Let F be any function over $\mathbb{F}_{2^n}$. If there exists an integer $1\leq l\leq n$ such that $2^l\big|\mathcal{W}_F(a,b)$ for any $a,b\in\mathbb{F}_{2^n}$ with $b\neq 0$, then the algebraic degree of $F(x)$ is at most equal to $n-l+1$.*

3.3 Nonlinearity

In this section we consider the nonlinearity of butterfly structures. We make use of the following lemmata.

Lemma 5. *Let i be an integer such that $\gcd(i,k)=1$ and $\alpha\in\mathbb{F}_{2^k}$ with $\alpha\neq 0,1$. Then for any $c,d\in\mathbb{F}_{2^k}$, the equations $\alpha^{2^i}c+\alpha d=\alpha c+\alpha^{2^i}d=0$ hold over $\mathbb{F}_{2^k}$ if and only if $c=d=0$.*

Proof. The sufficiency is obvious. For the necessity, we have $(\alpha^{2^i}+\alpha)(c+d)=0$. Note that $\alpha^{2^i}+\alpha\neq 0$ since $\alpha\neq 0,1$ and $\gcd(i,k)=1$. Hence, we get $c=d$ and further deduce that $\alpha^{2^i}c+\alpha d=(\alpha^{2^i}+\alpha)c=0$, implying that $c=d=0$. □

Lemma 6. *Let i be an integer such that $\gcd(i,k)=1$. Then for any $\alpha\in\mathbb{F}_{2^k}$ with $\alpha\neq 0,1$, the following equation system in variables c,d*

$$\begin{cases} \left(\alpha^{2^i+1}c+c+d\right)\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha c+\alpha^{2^i}d\right)=0, & (16)\\ \left(\alpha c+\alpha^{2^i}d\right)^{2^i}\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha^{2^i+1}d+c+d\right)^{2^i}=0, & (17)\\ \left(\alpha^{2^i}c+\alpha d\right)\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha^{2^i+1}d+c+d\right)=0 & (18)\end{cases}$$

holds over $\mathbb{F}_{2^k}$ if and only if c,d satisfy both $\alpha^{2^i+1}c+c+d=0$ and $\alpha^{2^i}c+\alpha d=0$.

Proof. The sufficiency is trivial. Below we consider the necessity. Suppose that at least one of $\alpha^{2^i+1}c+c+d$ and $\alpha^{2^i}c+\alpha d$ is not equal to 0.

If $c=0$, by Eqn. (17), we have $d^{2^{i+1}}=0$, which contradicts the assumption. Similarly for the case $d=0$, Eqn. (17) can be written as $c^{2^{i+1}}=0$. So we always assume that $c\neq 0$ and $d\neq 0$.

First we claim that $\alpha^{2^i+1}c+c+d\neq 0$ and $\alpha^{2^i}c+\alpha d\neq 0$. This is because: if $\alpha^{2^i+1}c+c+d=0$, then by Eqn. (18) we have $\alpha^{2^i}c+\alpha d=0$, which contradicts the assumption. Similarly, if $\alpha^{2^i}c+\alpha d=0$, then by Lemma 5, we have $\alpha c+\alpha^{2^i}d\neq 0$. Hence, from Eqn. (16) we have $\alpha^{2^i+1}c+c+d=0$, which contradicts the assumption as well. So we always consider both $\alpha^{2^i+1}c+c+d\neq 0$ and $\alpha^{2^i}c+\alpha d\neq 0$.

Note that $\alpha c+\alpha^{2^i}d\neq 0$ and $\alpha^{2^i+1}d+c+d\neq 0$, otherwise, by Eqn. (16) and (18) we have $\alpha^{2^i+1}c+c+d=0$ or $\alpha^{2^i}c+\alpha d=0$, a contradiction. Thus by Eqn. (16) and (17), we get

$$\frac{\alpha^{2^i+1}c+c+d}{\alpha c+\alpha^{2^i}d}=\frac{\left(\alpha^{2^i+1}c+c+d\right)^{2^i}}{\left(\alpha^{2^i}c+\alpha d\right)^{2^i}}=\frac{\left(\alpha c+\alpha^{2^i}d\right)^{2^i}}{\left(\alpha^{2^i+1}d+c+d\right)^{2^i}},$$

and obtain the following equation

$$\left(\alpha^{2^i+1}c+c+d\right)\left(\alpha^{2^i+1}d+c+d\right)^{2^i}=\left(\alpha c+\alpha^{2^i}d\right)\left(\alpha c+\alpha^{2^i}d\right)^{2^i}.$$

To simplify the expressions in the procedure of deductions, let $c=\lambda d$ and $\gamma=\alpha^{2^i}$, where $\lambda\neq 0$, $\gamma\neq 0,1$. Then the above equation can be rewritten as

$$\lambda^{2^i+1}+(\gamma^2+1)\lambda^{2^i}+(\alpha\gamma^{2^i+2}+\gamma^{2^i+1}+\alpha\gamma^{2^i}+\alpha\gamma+1)\lambda+1=0. \tag{19}$$

Similarly, Eqn. (18) can be rewritten as

$$\lambda^{2^i+1}+(\alpha\gamma^{2^i+2}+\gamma^{2^i+1}+\alpha\gamma^{2^i}+\alpha\gamma+1)\lambda^{2^i}+(\gamma^2+1)\lambda+1=0. \tag{20}$$

We add Eqn. (19) onto Eqn. (20) and get

$$(\alpha\gamma^{2^i+2}+\gamma^{2^i+1}+\alpha\gamma^{2^i}+\alpha\gamma+\gamma^2)\lambda^{2^i}+(\alpha\gamma^{2^i+2}+\gamma^{2^i+1}+\alpha\gamma^{2^i}+\alpha\gamma+\gamma^2)\lambda=0. \tag{21}$$

Recall that $\alpha\gamma^{2^i+2}+\gamma^{2^i+1}+\alpha\gamma^{2^i}+\alpha\gamma+\gamma^2=\alpha^{2^{2i}+2^{i+1}+1}+\alpha^{2^{2i}+2^i}+\alpha^{2^{2i}+1}+\alpha^{2^{i+1}}+\alpha^{2^i+1}\neq 0$ by Eqn. (8). then Eqn. (21) implies $\lambda^{2^i}+\lambda=0$, that is, $\lambda=1$, which means $c=d$. Further by Eqn. (17) we have $\alpha^{2^i+1}+\alpha^{2^i}+\alpha=(\alpha+1)^{2^i+1}+1=0$, which implies $\alpha=0$ and leads to a contradiction. So we can get the desired conclusion. □

Lemma 7. *Let i be an integer such that $\gcd(i,k)=1$. Then for any $(c,d)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ with $(c,d)\neq(0,0)$, the following equation system in the variables u,v*

$$\begin{cases} \left(\alpha^{2^i+1}c+c+d\right)^{2^i}u^{2^{2i}}+\left(\alpha^{2^i+1}c+c+d\right)u \\ \qquad\qquad +\left(\alpha c+\alpha^{2^i}d\right)^{2^i}v^{2^{2i}}+\left(\alpha^{2^i}c+\alpha d\right)v=0, & (22)\\ \left(\alpha^{2^i}c+\alpha d\right)^{2^i}u^{2^{2i}}+\left(\alpha c+\alpha^{2^i}d\right)u \\ \qquad\qquad +\left(\alpha^{2^i+1}d+c+d\right)^{2^i}v^{2^{2i}}+\left(\alpha^{2^i+1}d+c+d\right)v=0 & (23)\end{cases}$$

has at most 4 solutions in $(\mathbb{F}_{2^k})^2$.

Proof. We consider two cases depending on whether $\alpha^{2^i+1}c+c+d=0$ or not.

CASE 1 : $\alpha^{2^i+1}c+c+d=0$. Eqn. (22) can be reduced to

$$\left(\alpha c+\alpha^{2^i}d\right)^{2^i}v^{2^{2i}}+\left(\alpha^{2^i}c+\alpha d\right)v=0. \tag{24}$$

If $\alpha c+\alpha^{2^i}d=\alpha^{2^i}c+\alpha d=0$, then we have $c=d=0$. A contradiction. Hence at least one of $\alpha c+\alpha^{2^i}d$ and $\alpha^{2^i}c+\alpha d$ is nonzero. So Eqn. (24) in v has at most 2 solutions by Corollary 1. Similarly, for each v, Eqn. (23) in u has at most 2 solutions as well. Hence the total numbers of solutions of the equation system is at most equal to 4.

CASE 2 : $\alpha^{2^i+1}c+c+d\neq0$.

If $\alpha^{2^i}c+\alpha d=0$, then $\alpha c+\alpha^{2^i}d\neq0$. Eqn. (23) is reduced to

$$\left(\alpha c+\alpha^{2^i}d\right)u=\left(\alpha^{2^i+1}d+c+d\right)^{2^i}v^{2^{2i}}+\left(\alpha^{2^i+1}d+c+d\right)v. \tag{25}$$

When $\alpha^{2^i+1}d+c+d=0$, then $u=0$. Substitute it into Eqn. (22), and we have $v=0$. Hence the equation system has only the zero solution. When $\alpha^{2^i+1}d+c+d\neq0$, substitute Eqn. (25) into Eqn. (22), and we obtain the following equation

$$B_1v^{2^{4i}}+B_2v^{2^{2i}}+B_3v=0,$$

where $B_1=\frac{\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha^{2^i+1}d+c+d\right)^{2^{3i}}}{\left(\alpha c+\alpha^{2^i}d\right)^{2^{2i}}}\neq0$, and B_2,B_3 are some expressions in α,c,d. By Corollary 2, the above equation in v has at most 4 solutions. For each solution v, Eqn. (25) in u has only one solution. Hence the total numbers of solutions of the equation system is at most equal to 4.

If $\alpha^{2^i}c+\alpha d\neq0$, we multiply Eqn. (22) and (23) by $\left(\alpha^{2^i}c+\alpha d\right)^{2^i}$ and $\left(\alpha^{2^i+1}c+c+d\right)^{2^i}$ respectively, and then add them together to eliminate $u^{2^{2i}}$. Finally we get the following equation

$$B_4u+B_5v^{2^{2i}}+B_6v=0, \tag{26}$$

where

$$\begin{aligned} B_4&=\left(\alpha^{2^i+1}c+c+d\right)\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha c+\alpha^{2^i}d\right),\\ B_5&=\left(\alpha c+\alpha^{2^i}d\right)^{2^i}\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha^{2^i+1}d+c+d\right)^{2^i},\\ B_6&=\left(\alpha^{2^i}c+\alpha d\right)\left(\alpha^{2^i}c+\alpha d\right)^{2^i}+\left(\alpha^{2^i+1}c+c+d\right)^{2^i}\left(\alpha^{2^i+1}d+c+d\right).\end{aligned}$$

By Lemma 6, not all of B_4, B_5, B_6 are equal to zero.

If $B_4 = 0$, Eqn. (26) in v has at most 2 solutions. For each solution v, Eqn. (22) in u has at most 2 solutions. Hence the total number of solutions of the equation system is at most equal to 4.

If $B_4 \neq 0$ and $B_5 = B_6 = 0$, then $u = 0$. Recall that $\alpha^{2^i}c + \alpha c$ and $\alpha c + \alpha^{2^i}d$ cannot be equal to 0 simultaneously. Substitute $u = 0$ into Eqn. (22), and we obtain an equation in v with coefficient not all zero, which has at most 2 solutions. Hence the total number of solutions of the equation system is at most equal to 2.

If $B_4 \neq 0$ and $B_5 = 0, B_6 \neq 0$, then substitute Eqn. (26) into Eqn. (23), and we get

$$B_7 v^{2^{2i}} = 0,$$

where $B_7 = \left(\alpha^{2^i}c + \alpha d\right)^{2^i} B_6^{2^{2i}} + \left(\alpha^{2^i+1}d + c + d\right)^{2^i} B_4^{2^{2i}}$. With a tedious verification (see Appendix B), we have $B_7 \neq 0$. So $v = 0$, which implies that $u = 0$. It is shown that the equation system has only the zero solution.

If $B_4 \neq 0$ and $B_5 \neq 0$, we substitute Eqn. (26) into Eqn. (23) and get

$$B_8 v^{2^{4i}} + B_9 v^{2^{2i}} + B_{10} v = 0, \tag{27}$$

where $B_8 = \left(\alpha^{2^i}c + \alpha d\right)^{2^i} \left(\frac{B_5}{B_4}\right)^{2^{2i}} \neq 0$ and B_9, B_{10} are some expressions in α, c, d. By Corollary 2, Eqn. (27) in v has at most 4 solutions. For each solution v, Eqn. (26) in u has only one solution. Hence the total number of solutions of the equation system is at most equal to 4.

Combining the two cases, we complete the proof. □

Since V_e^α is quadratic, then its Walsh spectrum can be easily determined by the number of constant derivatives of its components, i.e., the dimension of the radical of the corresponding quadratic form (see e.g. [CDP17, Proposition 1], [MS77, Chapter 15] or [CCCF01, Appendix A]). In the following we give the detailed proof.

Theorem 3. *Let i be an integer such that $\gcd(i,k) = 1$. For any $0 \leq t \leq k-1$, $\alpha \in \mathbb{F}_{2^k}$ with $\alpha \neq 0, 1$, let H_e^α and V_e^α be the open and closed $2k$-bit butterfly structures with exponent $e = (2^i + 1) \times 2^t$ and coefficient α respectively. Then the nonlinearity of both H_e^α and V_e^α are $2^{2k-1} - 2^k$. Furthermore, their extended Walsh spectrum are $\{0, 2^k, 2^{k+1}\}$.*

Proof. By the CCZ-equivalent relation of H_e^α and V_e^α, here we only consider V_e^α with $e = 2^i + 1$. For convenience, we denote $F(x,y) = \mathsf{V}_e^\alpha(x,y)$.

Let $a, b, c, d \in \mathbb{F}_{2^k}$, where $(c,d) \neq (0,0)$. Then we have

$$\begin{aligned}\mathcal{W}_F((a,b),(c,d)) &= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}(c(\alpha x+y)^{2^i+1} + cx^{2^i+1} + d(x+\alpha y)^{2^i+1} + dy^{2^i+1} + ax + by)} \\ &= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)},\end{aligned}$$

where

$$\begin{aligned}f(x,y) =& \mathrm{Tr}\Big((\alpha^{2^i+1}c + c + d)x^{2^i+1} + (\alpha^{2^i+1}d + c + d)y^{2^i+1} \\ &+ (\alpha^{2^i}c + \alpha d)x^{2^i}y + (\alpha c + \alpha^{2^i}d)xy^{2^i} + ax + by\Big).\end{aligned}$$

Note that $\mathrm{Tr}(x) = \mathrm{Tr}(x^{2^i})$ for any $x \in \mathbb{F}_{2^k}$, we have

$$\begin{aligned}
&f(x,y) + f(x+u, y+v)\\
=&\mathrm{Tr}\Big[\Big((\alpha^{2^i+1}c+c+d)^{2^i}u^{2^{2i}} + (\alpha^{2^i+1}c+c+d)u + (\alpha c+\alpha^{2^i}d)^{2^i}v^{2^{2i}} + (\alpha^{2^i}c+\alpha d)v\Big)x^{2^i}\\
&\quad + \Big((\alpha^{2^i}c+\alpha d)^{2^i}u^{2^{2i}} + (\alpha c+\alpha^{2^i}d)u + (\alpha^{2^i+1}d+c+d)^{2^i}v^{2^{2i}} + (\alpha^{2^i+1}d+c+d)v\Big)y^{2^i}\Big]\\
&+ f(u,v).
\end{aligned}$$

So

$$\begin{aligned}
(\mathcal{W}_F((a,b),(c,d)))^2 &= \sum_{x,y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)} \cdot \sum_{u,v\in\mathbb{F}_{2^k}} (-1)^{f(x+u,y+v)}\\
&= \sum_{x,y,u,v\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+f(x+u,y+v)}\\
&= 2^{2k} \cdot \sum_{u,v\in R(c,d)} (-1)^{f(u,v)},
\end{aligned}$$

where the radical $R(c,d)$ is the solution set of the following equation system in variables u, v

$$\begin{cases}
\Big(\alpha^{2^i+1}c+c+d\Big)^{2^i}u^{2^{2i}} + \Big(\alpha^{2^i+1}c+c+d\Big)u + \Big(\alpha c+\alpha^{2^i}d\Big)^{2^i}v^{2^{2i}} + \Big(\alpha^{2^i}c+\alpha d\Big)v = 0,\\
\Big(\alpha^{2^i}c+\alpha d\Big)^{2^i}u^{2^{2i}} + \Big(\alpha c+\alpha^{2^i}d\Big)u + \Big(\alpha^{2^i+1}d+c+d\Big)^{2^i}v^{2^{2i}} + \Big(\alpha^{2^i+1}d+c+d\Big)v = 0.
\end{cases}$$

Denote $m = \dim_{\mathbb{F}_2} R(c,d)$. By Lemma 7, we have $0 \le m \le 2$. Note that $f(x,y) + f(x+u, y+v) = f(u,v)$ for $(u,v) \in R(c,d)$ and $(x,y) \in (\mathbb{F}_{2^k})^2$. This implies that $f(u,v)$ is linear over $R(c,d)$. Since $(0,0) \in R(c,d)$, $f(u,v)$ is balanced or constant 0 over $R(c,d)$. Thus

$$(\mathcal{W}_F((a,b),(c,d)))^2 = \begin{cases} 2^{2k+m} & f(u,v) = 0 \text{ over } R(c,d),\\ 0 & \text{otherwise.}\end{cases}$$

As $\mathcal{W}_F((a,b),(c,d))$ is an integer, m must be even, i.e., $m = 0$ or $m = 2$. Hence, $\mathcal{W}_F((a,b),(c,d)) \in \{0, \pm 2^k, \pm 2^{k+1}\}$.

Since H_e^α is a permutation over $(\mathbb{F}_{2^k})^2$, $\mathcal{W}_F((0,0),(c,d)) = 0$ for any $(c,d) \in (\mathbb{F}_{2^k})^2$ with $(c,d) \ne (0,0)$, which means $0 \in \Lambda_F$. Besides we also have $2^{k+1} \in \Lambda_F$ or $-2^{k+1} \in \Lambda_F$. Otherwise, by Parseval's relation we must have $\mathcal{W}_F((a,b),(c,d)) = \pm 2^k$ for any $(a,b),(c,d) \in (\mathbb{F}_{2^k})^2$ with $(c,d) \ne (0,0)$, which is impossible. If $\pm 2^k \notin \Lambda_F$, by Lemma 4, the algebraic degree is at most equal to $2k - (k+1) + 1 = k$, which contradicts that the algebraic degree of H_e^α is $k+1$. Therefore, its extended Walsh spectrum is $\{0, 2^k, 2^{k+1}\}$, and the nonlinearity $\mathcal{NL}(F) = 2^{2k-1} - 2^k$. □

Remark 2. Recall that the Walsh spectrum of Gold function is $\{0, \pm 2^{k+1}\}$, which is different from that of butterfly structures. Hence, the butterfly structures H_e^α and V_e^α are CCZ-inequivalent to the Gold function. Besides, in the proof of Lemma 7, there exists some cases that the solution set $R(c,d)$ has only one solution $(0,0)$ (e.g. the case of $\alpha c + \alpha^{2^i}d = 0$ and $\alpha^{2^i}c + \alpha d \ne 0$), namely, $m = 0$. Hence, we also have $2^k \in \Lambda_F$ or $-2^k \in \Lambda_F$. From the proof of above theorem, we have actually $m = 0$ or $m = 2$, which means that the equation system in Lemma 7 has either one solution or 4 solutions.

4 Butterfly Structures with $\alpha = 1$

In this section we will discuss the butterflies with trivial coefficient $\alpha = 1$. It is known that the butterfly structure H_e^1 is functionally equivalent to the 3-round Feistel structure constructed by Li and Wang [LW14b]. They proved that its differential spectrum is $\{0, 4\}$ and its algebraic degree is k (or see Section 3.2).

Moreover, in [PUB16, Theorem 5], the author showed that when the exponent $e = 2^{2i}+1$ for some i, the closed $2k$-bit butterfly V_e^1 is linear equivalent to the monomial x^e. When k is odd and $\gcd(i, k) = 1$, it is easy to see that x^e is a differentially 4-permutation over $\mathbb{F}_{2^{2k}}$. By the linear equivalence, V_e^1 is a differentially 4-permutation and has the Gold-type Walsh spectrum $\{0, \pm 2^{k+1}\}$.

In this section we give a direct proof of these results. In Section 4.1, when $\gcd(i, k) = 1$ we show that V_e^1 with exponent $e = (2^i + 1) \times 2^t$ is a permutation over $(\mathbb{F}_{2^k})^2$. In Section 4.2, we give a proof that the butterflies with $\alpha = 1$ have the best known nonlinearity. We still suppose that k is an odd positive integer.

4.1 The Bijective Property of the Closed Butterfly Structures

When $\alpha = 1, e = 2^i + 1$, the closed butterfly structure V_e^1 becomes

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

Proposition 1. *Let i be an integer such that $\gcd(i, k) = 1$. For any $0 \le t \le k - 1$, let V_e^1 be the closed $2k$-bit butterfly structure with exponent $e = (2^i + 1) \times 2^t$. Then $\mathsf{V}_e^1(x, y)$ is a permutation over $(\mathbb{F}_{2^k})^2$.*

Proof. Similarly as the proof of Theorem 1, we only consider the case $e = 2^i + 1$. For any $u, v \in \mathbb{F}_{2^k}$ with $(u, v) \neq (0, 0)$, it is sufficient to show that

$$\mathsf{V}_e^1(x, y) + \mathsf{V}_e^1(x + u, y + v) = (0, 0),$$

namely, the system of equations

$$\begin{cases} vx^{2^i} + v^{2^i}x + (u + v)y^{2^i} + (u + v)^{2^i}y = (u + v)^{2^i+1} + u^{2^i+1}, \\ (u + v)x^{2^i} + (u + v)^{2^i}x + uy^{2^i} + u^{2^i}y = (u + v)^{2^i+1} + v^{2^i+1}, \end{cases}$$

has no solution in $(\mathbb{F}_{2^k})^2$. We replace the first equation by the sum of the two equations and consider the following equivalent system of equations

$$\begin{cases} ux^{2^i} + u^{2^i}x + vy^{2^i} + v^{2^i}y = u^{2^i+1} + v^{2^i+1}, & (28) \\ (u + v)x^{2^i} + (u + v)^{2^i}x + uy^{2^i} + u^{2^i}y = (u + v)^{2^i+1} + v^{2^i+1}. & (29) \end{cases}$$

First, if $u = 0$, then $v \neq 0$. So Eqn. (28) can be reduced to

$$vy^{2^i} + v^{2^i}y = v^{2^i+1},$$

which is equivalent to $(v + y)^{2^i+1} = y^{2^i+1}$. Therefore, Eqn. (28) has no solution in $(\mathbb{F}_{2^k})^2$ since x^{2^i+1} is a permutation over $\mathbb{F}_{2^k}$.

Similarly we have the same conclusion for the cases $u \neq 0, v = 0$ and $u = v \neq 0$. Since their proof procedures are almost identical to the above, here we do not repeat them.

Below we suppose that $u \neq 0, v \neq 0$, and $u \neq v$. We multiply Eqn. (28) and Eqn. (29) by u and v respectively, then add them together to eliminate y^{2^i}, and get

$$y = \frac{1}{C_2}(C_1x^{2^i} + C_3x + C_1u^{2^i}),$$

where

$$\begin{aligned} C_1 &= u^2 + uv + v^2, \\ C_2 &= u^{2^i}v + uv^{2^i}, \\ C_3 &= u^{2^i+1} + u^{2^i}v + v^{2^i+1}. \end{aligned}$$

It is easy to see that $C_1 \neq 0$, otherwise we have $(\frac{u}{v})^2 + \frac{u}{v} + 1 = 0$, which is impossible since k is odd. We also have $C_2 \neq 0$ since $u \neq v$. Substitute the above equation into Eqn. (28), multiply both sides by $C_2^{2^i+1}$, and we obtain

$$\begin{aligned} & vC_2C_1^{2^i}x^{2^{2i}} + \left(uC_2^{2^i+1} + (vC_2)^{2^i}C_1 + vC_2C_3^{2^i}\right)x^{2^i} + \left(u^{2^i}C_2^{2^i+1} + (vC_2)^{2^i}C_3\right)x \\ = {} & vC_2C_1^{2^i}u^{2^{2i}} + (vC_2)^{2^i}C_1u^{2^i} + C_2^{2^i+1}\left(u^{2^i+1} + v^{2^i+1}\right), \end{aligned}$$

which can be further reduced to the following equation

$$C_2x^{2^{2i}} + \left(u^{2^{2i}}v + uv^{2^{2i}}\right)x^{2^i} + C_2^{2^i}x = u^{2^{2i}}C_2 + uC_2^{2^i}.$$

Divide both sides by $u^{2^{2i}+2^i+1}$, and we have

$$\begin{aligned} & \left(\frac{v}{u} + \left(\frac{v}{u}\right)^{2^i}\right)\left(\frac{x}{u}\right)^{2^{2i}} + \left(\frac{v}{u} + \left(\frac{v}{u}\right)^{2^{2i}}\right)\left(\frac{x}{u}\right)^{2^i} + \left(\left(\frac{v}{u}\right)^{2^i} + \left(\frac{v}{u}\right)^{2^{2i}}\right)\frac{x}{u} \\ = {} & \frac{v}{u} + \left(\frac{v}{u}\right)^{2^i} + \left(\frac{v}{u}\right)^{2^i} + \left(\frac{v}{u}\right)^{2^{2i}}. \end{aligned} \tag{30}$$

Denote $w = \frac{v}{u} + \left(\frac{v}{u}\right)^{2^i}, z = \frac{x}{u} + \left(\frac{x}{u}\right)^{2^i}$, then we have $w \neq 0$. The above equation is equivalent to

$$w(z+1)^{2^i} + w^{2^i}(z+1) = 0. \tag{31}$$

It is to check that Eqn. (31) has two solutions $z = 1$ and $z = w + 1$ since $\gcd(i, k) = 1$.

If $z = 1$, i.e., $\frac{x}{u} + \left(\frac{x}{u}\right)^{2^i} = 1$. Note that $1 = \mathrm{Tr}(1) \neq \mathrm{Tr}\left(\frac{x}{u} + \left(\frac{x}{u}\right)^{2^i}\right) = 0$, it follows that Eqn. (30) has no solution in $\mathbb{F}_{2^k}$.

If $z = w + 1$, i.e., $\frac{x}{u} + \left(\frac{x}{u}\right)^{2^i} = \frac{v}{u} + \left(\frac{v}{u}\right)^{2^i} + 1$. Thus we have $(\frac{x}{u} + \frac{v}{u}) + (\frac{x}{u} + \frac{v}{u})^{2^i} = 1$. In this case Eqn. (30) has no solution in $\mathbb{F}_{2^k}$ as well.

So the conclusion follows. □

Remark 3. We have also investigated experimentally the bijective property of the closed butterfly structure with other α. However, we could not find an $\alpha \neq 1$ such that V_e^α is also a permutation over $(\mathbb{F}_{2^k})^2$. We conjecture that V_e^α is a permutation over $(\mathbb{F}_{2^k})^2$ if and only if $\alpha = 1$.

4.2 Nonlinearity

First we give a lemma which says that the dimension of the radical of the corresponding quadratic form of V_e^1 is at most equal to 2.

Lemma 8. *Let i be an integer such that $\gcd(i, k) = 1$. Then for any $(c, d) \in (\mathbb{F}_{2^k})^2$ with $(c, d) \neq (0, 0)$, the following system of equations in variables u and v*

$$\begin{cases} du^{2^i} + (du)^{2^{k-i}} + (c+d)v^{2^i} + ((c+d)v)^{2^{k-i}} = 0, \\ (c+d)u^{2^i} + ((c+d)u)^{2^{k-i}} + cv^{2^i} + (cv)^{2^{k-i}} = 0 \end{cases} \tag{32}$$

has at most 4 solutions in $(\mathbb{F}_{2^k})^2$.

Proof. We add the first equation to the second equation and obtain

$$\begin{cases} du^{2^i} + (du)^{2^{k-i}} + (c+d)v^{2^i} + ((c+d)v)^{2^{k-i}} = 0, \\ cu^{2^i} + (cu)^{2^{k-i}} + dv^{2^i} + (dv)^{2^{k-i}} = 0. \end{cases} \tag{33}$$

Then raising both equations to the 2^ith power, we deduce that

$$\begin{cases} d^{2^i}u^{2^{2i}} + du + (c+d)^{2^i}v^{2^{2i}} + (c+d)v = 0, & (34) \\ c^{2^i}u^{2^{2i}} + cu + d^{2^i}v^{2^{2i}} + dv = 0. & (35) \end{cases}$$

If $c = 0$, then $d \neq 0$ and Eqn. (35) in v has 2 solutions. For each solution v, Eqn. (34) in u has at most 2 solutions. Hence the equation system (32) has at most 4 solutions. Similarly we have the same conclusion for the cases $d = 0, c \neq 0$ and $c = d \neq 0$.

Now we suppose that $c \neq 0, d \neq 0$ and $c \neq d$. We multiply Eqn. (34) and (35) by c^{2^i} and d^{2^i} respectively, then add them together to eliminate $u^{2^{2i}}$, finally substitute the expression of u into Eqn. (35) and get

$$D_1 v^{2^{4i}} + D_2 v^{2^{2i}} + D_3 v = 0,$$

where $D_1 = c^{2^i}\frac{(c^2+cd+d^2)^{2^{3i}}}{(c^{2^i}d+cd^{2^i})^{2^i}}$, and D_2, D_3 are some expressions in c, d. From the proof of the Proposition 1, we know $c^2 + cd + d^2 \neq 0$ and $c^{2^i}d + cd^{2^i} \neq 0$, thus $D_1 \neq 0$. By Corollary 2, this equation in v has at most 4 solutions. Since the solution u is uniquely determined by v, the equation system (32) has at most 4 solutions.

Therefore, the whole system has at most 4 solutions. □

Proposition 2. *Let i be an integer such that $\gcd(i,k) = 1$. For any $0 \leq t \leq k-1$, let H_e^1 and V_e^1 be the open and closed $2k$-bit butterfly structures with exponent $e = (2^i+1) \times 2^t$ respectively. Then the nonlinearity of both H_e^1 and V_e^1 are $2^{2k-1} - 2^k$. Furthermore, their Walsh spectrum are $\{0, \pm 2^{k+1}\}$.*

Proof. The proof of nonlinearity of V_e^1 is identical to the proof of the nonlinearity of V_e^α in Theorem 3, here we also have $m \leq 2$ by Lemma 8. It is implied that $\mathcal{W}_{\mathsf{V}_e^1}((a,b),(c,d)) \in \{0, \pm 2^k, \pm 2^{k+1}\}$ for any $a,b,c,d \in \mathbb{F}_{2^k}$ with $(c,d) \neq (0,0)$. Further, since V_e^1 is a permutation, all its nonzero components are balanced, thus cannot be bent. It follows that $\pm 2^k \notin \Lambda_{\mathsf{V}_e^1}$. Therefore, $\Lambda_{\mathsf{V}_e^1} = \{0, \pm 2^{k+1}\}$, and the nonlinearity $\mathcal{NL}(\mathsf{V}_e^1) = 2^{2k-1} - 2^k$. Finally, by CCZ-equivalence, we get the conclusions. □

Remark 4. From the proof of above theorem, we have actually $m = 2$, which means that the equation system in Lemma 8 has exactly 4 solutions for any $(c,d) \in (\mathbb{F}_{2^k})^2$ with $(c,d) \neq (0,0)$.

5 Conclusion and Future Work

In the paper we study the functions of butterflies over $(\mathbb{F}_{2^k})^2$ with odd k and show that these functions with exponent $e = 2^i + 1$ have the differential uniformity at most 4 and the algebraic degree are also very high. Moveover, we prove that their nonlinearity are equal to $2^{2k-1} - 2^k$ in the general case, which also give another complete solution to an open problem raised in [PUB16], which has been independently solved by Canteaut et al. in [CDP17]. Besides, we also study the functions with trivial coefficient $\alpha = 1$, and show that the function constructed from closed butterfly is also bijective. Hence, we obtain many new differentially 4-uniform permutations with the best known nonlinearity and high algebraic degree. These functions provide more choices for the design of S-boxes.

The research of butterfly structures also raise the following problem: To give a characterization of the pair (e, α) such that H_e^α has lower differential uniformity over $(\mathbb{F}_{2^k})^2$ with even k. Besides, how to find more classes of differentially 4-uniform permutations with the best known nonlinearity and high algebraic degree from other functions over subfields or other structures is still very interesting and worthy of a further investigation. The following question is still open: Is there a tuple (k, e, α) where $k > 3$ and $e > 3$ are integers, and α is a nonzero element in $\mathbb{F}_{2^k}$ such that H_e^α is APN over $(\mathbb{F}_{2^k})^2$?

Acknowledgements

The authors would like to thank the anonymous reviewers for their comments and suggestions which significantly improve the quality and presentation of this paper. The works of S.H. Fu and X.T. Feng were supported by the National Natural Science Foundation of China (No. 61572491), the Foundation Science Center project of the National Natural Science Foundation of China (No. 11688101) and the National Key Research and Development Program of China (No. 2016YFB0800401). The work of B.F. Wu was supported by the National Natural Science Foundation of China (No. 61502482).

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.

[CCCF01] Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. On cryptographic properties of the cosets of $R(1,m)$. *IEEE Trans. Information Theory*, 47(4):1494–1513, 2001.

[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.

[CDP17] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Trans. Information Theory*, 2017. https://doi.org/10.1109/TIT.2017.2676807, also available as IACR Cryptology ePrint Archive 2016: 887 (2016).

[Cox12] David A. Cox. *Galois theory*, volume 61 of *The Pure and Applied Mathematics: A Wiley-Interscience Series of Texts, Monographs, and Tracts.* John Wiley & Sons, 2nd edition, 2012.

[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.

[EKP$^+$07] Thomas Eisenbarth, Sandeep S. Kumar, Christof Paar, Axel Poschmann, and Leif Uhsadel. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, 24(6):522–533, 2007.

[GQ09] Rod Gow and Rachel Quinlan. Galois extensions and subspaces of alternating bilinear forms with special rank properties. *Linear Algebra and its Applications*, 430(8):2212–2224, 2009.

[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.

[Lan90] Philippe Langevin. Covering radius of RM(1, 9) in RM(3, 9). In *EUROCODE'90, International Symposium on Coding Theory and Applications, Udine, Italy, November 5-9, 1990, Proceedings*, pages 51–59, 1990.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematica and its Applications.* Cambridge University Press, 2nd edition, 1997.

[LW14a] 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.

[LW14b] Yongqiang Li and Mingsheng Wang. Constructing S-boxes for lightweight cryptography with feistel structure. In *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, pages 127–146, 2014.

[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.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes.* North-Holland mathematical library. North-Holland Pub. Co. New York, Amsterdam, New York, 1977.

[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.

[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.

[SD16] Kirat Pal Singh and Shiwani Dod. An efficient hardware design and implementation of advanced encryption standard (AES) algorithm. *International Journal of Recent Advances in Engineering & Technology*, 4:5–9, 2016.

[SP04] Kai Schramm and Christof Paar. IT security project: Implementation of the advanced encryption standard (AES) on a smart card. In *International Conference on Information Technology: Coding and Computing (ITCC'04), Volume 1, April 5-7, 2004, Las Vegas, Nevada, USA*, pages 176–180, 2004.

[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.

[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.

A The Proof of $A_8 \neq 0$

Suppose that $A_8 = 0$. Then

$$\left(\alpha(\alpha u+v)^{2^i}+u^{2^i}\right)A_6=(\alpha u+v)^{2^i}A_4.$$

Note that $\alpha^{2^i}(\alpha u+v)+u\neq 0$, we substitute A_4 and A_6 into the above equation and get

$$(\alpha v+u)(\alpha u+v)=(\beta(\alpha u+v)+u)(\beta(\alpha v+u)+v), \tag{36}$$

where $\alpha=\beta^{2^i}$.

If $u=0$, then $v\neq 0$. From Eqn. (36) and $A_5=0$, we have $\beta^{2^i+2}+\beta^{2^i}+\beta=0$ and $\alpha^{2^{i+1}+1}+\alpha^{2^i}+\alpha=0$. We add the first equation raised by the 2^ith power to the second equation and get $\alpha^{2^i+1}(\alpha^{2^i}+\alpha)=0$, which is impossible.

Similarly we have the same conclusion for the case $v=0, u\neq 0$. Hence we only consider that $u\neq 0, v\neq 0$. Note that $A_5=0$ and Eqn. (36) are the same as Eqn. (2) and (4), according to the proof of Lemma 2, it is known that this is impossible. So it follows that $A_8\neq 0$.

B The Proof of $B_7 \neq 0$

Otherwise, we suppose that $B_7=0$. Keep the notation $\gamma=\alpha^{2^i}$. Then

$$(\gamma c+\alpha d)B_6^{2^i}=(\alpha\gamma d+c+d)B_4^{2^i}.$$

Substitute B_4 and B_6 into the above equation, and we have

$$\begin{aligned}&(\gamma c+\alpha d)^{2^{2i}}\left[(\gamma c+\alpha d)(\gamma c+\alpha d)^{2^i}+(\alpha\gamma d+c+d)(\alpha\gamma c+c+d)^{2^i}\right]\\ =\;&(\alpha\gamma c+c+d)^{2^{2i}}\left[(\gamma c+\alpha d)(\alpha\gamma d+c+d)^{2^i}+(\alpha\gamma d+c+d)(\alpha c+\gamma d)^{2^i}\right].\end{aligned}$$

Note that $\gamma c+\alpha d\neq 0$ and $\alpha\gamma c+c+d\neq 0$, we deduce that

$$(\gamma c+\alpha d)(\alpha\gamma d+c+d)^{2^i}+(\alpha\gamma d+c+d)(\alpha c+\gamma d)^{2^i}=\frac{(\gamma c+\alpha d)^{2^{2i}}}{(\alpha\gamma c+c+d)^{2^{2i}}}B_6. \tag{37}$$

Since $B_6\neq 0$, it follows that $\alpha\gamma d+c+d\neq 0$ by the above equation. By $B_5=0$, we get

$$\begin{aligned}&(\alpha\gamma d+c+d)(\gamma c+\alpha d)(\alpha c+\gamma d)^{2^i}(\gamma c+\alpha d)^{2^i}\\ =\;&(\alpha\gamma d+c+d)(\gamma c+\alpha d)(\alpha\gamma c+c+d)^{2^i}(\alpha\gamma d+c+d)^{2^i}.\end{aligned}$$

Substitute

$$(\gamma c+\alpha d)(\gamma c+\alpha d)^{2^i}=B_6+(\alpha\gamma c+c+d)^{2^i}(\alpha\gamma d+c+d)$$

into the above equation, and we obtain

$$\begin{aligned}&B_6(\alpha\gamma d+c+d)(\alpha c+\gamma d)^{2^i}\\ =\;&(\alpha\gamma c+c+d)^{2^i}(\alpha\gamma d+c+d)\cdot\left[(\gamma c+\alpha d)(\alpha\gamma d+c+d)^{2^i}+(\alpha\gamma d+c+d)(\alpha c+\gamma d)^{2^i}\right].\end{aligned}$$

By Eqn. (37) and $B_6\neq 0$, we deduce that

$$(\alpha\gamma d+c+d)(\alpha c+\gamma d)^{2^i}=(\alpha\gamma c+c+d)^{2^i}(\alpha\gamma d+c+d)\frac{(\gamma c+\alpha d)^{2^{2i}}}{(\alpha\gamma c+c+d)^{2^{2i}}},$$

which is equivalent to

$$(\alpha c+\gamma d)(\alpha\gamma c+c+d)^{2^i}=(\alpha\gamma c+c+d)(\gamma c+\alpha d)^{2^i}.$$

The last equation implies $B_4=0$. A contradiction. So $B_7\neq 0$.