IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2018, No. 1, pp. 160–179. DOI:10.13154/tosc.v2018.i1.160-179

On the Generalization of Butterfly Structure

Yongqiang Li[1,2], Shizhu Tian[1,2], Yuyin Yu[3] and Mingsheng Wang[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
yongq.lee@gmail.com,{tianshizhu,wangmingsheng}@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[3] School of Mathematics and Information Science, Guangzhou University, Guangzhou, China
yuyuyin@163.com

Abstract. Butterfly structure was proposed in CRYPTO 2016 [PUB16], and it can generate permutations over $\mathbb{F}_{2^n}^2$ from power permutations over $\mathbb{F}_{2^n}$ for odd n. After that, a generalized butterfly structure was proposed in IEEE IT [CDP17], which can generate permutations over $\mathbb{F}_{2^n}^2$ from any permutation over $\mathbb{F}_{2^n}$. There is also another generalization which was given in [FFW17]. Up to now, three constructions based on butterfly structure and Gold type permutations are proposed. In the present paper, we give a construction which contains the three previous constructions as special cases and also generates new permutations with good cryptographic properties. Moreover, we give a characterization of the number of solutions of a special system of linear equations in a more general way, which is useful to investigate the cryptographic properties of quadratic functions obtained with butterfly construction based on Gold exponents.

Keywords: Butterfly structure, differential uniformity, nonlinearity, algebraic degree

1 Introduction

S(ubstitution)-boxes play an important role in symmetric ciphers since they serve as the confusion part and in most cases are the only nonlinear components of round functions. These boxes should possess low differential uniformity and high nonlinearity to resist differential cryptanalysis and linear cryptanalysis respectively. For efficiency of implementations, S-boxes are often designed as permutations over $\mathbb{F}_{2^m}$ in practice, especially over $\mathbb{F}_{2^{2m}}$ in most cases. Then, constructing permutations with low differential uniformity and high nonlinearity is of particular interest in the study of cryptographic functions.

The functions with lower differential uniformity provide better resistance to differential attack. The lower bound for functions on $\mathbb{F}_{2^n}$ is 2, and the functions that achieve this bound are called almost perfect nonlinear (APN) functions. So, APN permutations over $\mathbb{F}_{2^{2m}}$ would be good choices for S-boxes in cryptography. Hou proved that there are no APN permutations over $\mathbb{F}_{2^4}$ and there are no APN permutations over $\mathbb{F}_{2^{2m}}$ with coefficients in $\mathbb{F}_{2^m}$ [Hou06]. Then, the existence of APN permutations over $\mathbb{F}_{2^{2m}}$ is a long-term open problem on vectorial Boolean functions.

The breakthrough is the discovery of an APN permutation over $\mathbb{F}_{2^6}$ [BDMW10], which is still the only known example of an APN permutation over $\mathbb{F}_{2^{2m}}$ so far. It was constructed by using CCZ-equivalence to the Kim function, which is $x^3 + x^{10} + gx^{24}$ and g is a root of $x^6 + x^4 + x^3 + x + 1$. Following this approach, Yu et al. gave a matrix representation of quadratic APN functions and got 8157 new quadratic APN functions over $\mathbb{F}_{2^8}$ [YWL14], but none of them are CCZ-equivalent to permutations. The existence of APN permutations over $\mathbb{F}_{2^{2m}}$ with $m \geq 4$ remains open.

Received: 2017-09-01, Revised: 2017-11-23, Accepted: 2018-01-23, Published: 2018-03-01

In Crypto 2016, Perrin et. al. investigated the only known APN permutation over $\mathbb{F}_{2^6}$ by the method of reverse-engineering. They found that the APN permutation over $\mathbb{F}_{2^6}$ has a simple decomposition relying on x^3 over $\mathbb{F}_{2^3}$. Based on power permutations x^e over $\mathbb{F}_{2^n}$, the open butterfly structure and the closed butterfly structure were proposed respectively [PUB16]. They are functions over $\mathbb{F}_{2^n}^2$ and the open butterfly structure is a permutation over $\mathbb{F}_{2^n}^2$ which is CCZ-equivalent to the closed butterfly structure [PUB16].

As a particular construction, the case of $e = 3 \cdot 2^t$ was discussed in [PUB16]. It was shown that when n is odd, the following quadratic function

$$\mathsf{V}_3^\alpha = \left((x+\alpha y)^3 + y^3, (y+\alpha x)^3 + x^3\right),$$

where $\alpha \in \mathbb{F}_{2^n}^*$, has differential uniformity at most 4. Furthermore, the open butterfly structure is the case of three round Feistel structure with round functions x^3, $x^{1/3}$ and x^3 respectively when $\alpha = 1$[PUB16]. The cryptographic properties of 3-round Feistel structures with round functions x^{2^i+1}, $x^{1/(2^i+1)}$, x^{2^i+1} was also presented in [LW14].

The case of $e = 3$ was generalized to $e = 2^i + 1$ with $\gcd(i, n) = 1$ in [FFW17], and the differential uniformity and nonlinearity of the following function

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

are characterized.

Canteaut et al. generalized the power permutation x^e to any permutation over $\mathbb{F}_{2^n}$. They demonstrated that the open butterfly structure and the closed butterfly structure can be defined via $R(x, y)$, where $R(x, y)$ is a bivariate polynomial over $\mathbb{F}_{2^n}$ such that $R_y : x \mapsto R(x, y)$ is a permutation over $\mathbb{F}_{2^n}$ for all y in $\mathbb{F}_{2^n}$ [CDP17]. The case of

$$R(x, y) = (x + \alpha y)^3 + \beta y^3$$

was studied in [CDP17], and it was proved that the following functions

$$\mathsf{V}_R(x, y) = \left((x+\alpha y)^3 + \beta y^3, (y+\alpha x)^3 + \beta x^3\right),$$

has differential uniformity at most 4 and possesses the best known nonlinearity over $\mathbb{F}_{2^{2n}}$ for $n \geq 3$ and odd, where $\alpha, \beta \in \mathbb{F}_{2^n}^*$ with $\beta \neq (\alpha+1)^3$. Also, it was proved that there is no new APN functions from the above structure except for the quadratic APN function which is CCZ-equivalent to a permutation over $\mathbb{F}_{2^6}$. The algebraic degree of the corresponding open butterfly structure was also given.

The core part of the proof of previous constructions relies on the determination of the number of roots of a system of linear equations of the following type

$$\begin{cases} a_1 x^{2^i} + a_2 x + b_1 y^{2^i} + b_2 y = 0, \\ a_3 x^{2^i} + a_4 x + b_3 y^{2^i} + b_4 y = 0, \end{cases}$$

where $a_j, b_j \in \mathbb{F}_{2^n}, 1 \leq j \leq 4$ are some particular elements derived from the differences of special quadratic functions. This system was studied case by case in previous constructions [LW14, PUB16, CDP17, FFW17].

In this paper, we investigate the number of solutions of the system of linear equations above in a general way. For $a_j, b_j \in \mathbb{F}_{2^n}$ with $\{a_j : 1 \leq j \leq 4\} \neq \{0\}$ and $\{b_j : 1 \leq j \leq 4\} \neq \{0\}$, we give a sufficient and necessary condition on the coefficients such that the above system of equations has at most 2^{2k} solutions over $\mathbb{F}_{2^n}^2$, where $k = \gcd(i, n)$.

With this characterization, we discuss the case of

$$R(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1},$$

which covers the previous constructions as special cases. We show that the functions over $\mathbb{F}_{2^n}^2$ of the following type

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

where $\alpha, \beta \in \mathbb{F}_{2^n}^*$, has differential uniformity at most 4 and also possesses the best known nonlinearity over $\mathbb{F}_{2^n}^2$ when n is odd, $\gcd(i,n) = 1$ and $\beta \neq (\alpha+1)^{2^i+1}$. The algebraic degree of the corresponding permutation $\mathsf{H}_R^{2^i+1}$ is also calculated. The case when i and n that are not coprime is also considered, and we show that differentially 4-uniform functions $\mathsf{V}_R^{2^i+1}$ can be constructed for even n.

The paper is organized as follows. In Sect. 2, some preliminaries are recalled. In Sect. 3, several results concerning the number of solutions of a special system of linear equations are given, which are very helpful to characterize the properties of quadratic functions obtained with butterfly construction based on Gold exponents. In Sect. 4, the differential uniformity, nonlinearity and algebraic degree of our constructions are investigated and the corresponding experiment results are also demonstrated. In Sect. 5, the case when i and n are not coprime is studied. A short conclusion is given in Sect. 6.

2 Preliminaries

Let $F \in \mathbb{F}_{2^n}[x]$, F is called differentially δ-uniform if for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, $F(x) + F(x+a) = b$ has at most δ solutions in $\mathbb{F}_{2^n}$ [Nyb93]. The Walsh transform of F is defined as

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

where $u, v \in \mathbb{F}_{2^n}$. The linearity of F is the highest magnitude of its Walsh coefficients:

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

The nonlinearity of F, which is defined as the minimum distance of the components of F to all affine Boolean functions of n variables, is related to the Walsh transform through the following equality

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\mathcal{L}(F).$$

For $F \in \mathbb{F}_{2^n}[x]$, $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [CV94]. Functions reaching this bound are called AB (Almost Bent) functions and they only exist in $\mathbb{F}_{2^n}$ with odd n. For even n, the upper bound is not tight. Finding the optimal upper bound in this case is still an open problem and the best known nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$ [Dob98].

Let $\omega_2(j)$ denotes the Hamming weight of the binary expansion of j. The algebraic degree of $F(x) = \sum_{j=0}^{2^n-1} c_j x^j \in \mathbb{F}_{2^n}[x]$ is defined as the maximum Hamming weight of the binary expansion of j with $c_j \neq 0$ [CCZ98], i.e., $d^\circ(F) = \max_{j, c_j \neq 0}\{\omega_2(j)\}$. The functions with algebraic degree 2 are called quadratic functions.

$F_1, F_2 \in \mathbb{F}_{2^n}[x]$ are called EA-equivalent, if there exist affine permutations A_1, $A_2 \in \mathbb{F}_{2^n}[x]$ and an affine function $A_3 \in \mathbb{F}_{2^n}[x]$, such that

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

A more general framework is introduced by considering graphs of functions [CCZ98]. Two functions $F_1, F_2 \in \mathbb{F}_{2^n}[x]$ are called CCZ-equivalent if there exists an affine permutation $\mathcal{A}$ over $\mathbb{F}_{2^n}^2$, such that $\mathcal{A}(G_{F_1}) = G_{F_2}$, where $G_{F_i} = \{(x, F_i(x)) \mid x \in \mathbb{F}_{2^n}\}, i = 1, 2$.

Differential uniformity, nonlinearity and Walsh spectrum are invariants of both EA-equivalence and CCZ-equivalence. However, algebraic degree is only preserved by EA-equivalence.

Let $F \in \mathbb{F}_{2^n}[x]$, the extended code $\tilde{C}_F$ of F is the linear code with parity check matrix

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

For admissible maps $F_1, F_2 \in \mathbb{F}_{2^n}[x]$, F_1 and F_2 are CCZ-equivalent if and only if $\tilde{C}_{F_1}$ and $\tilde{C}_{F_2}$ are equivalent [BDKM09].

Definition 1. [PUB16] Let $\alpha \in \mathbb{F}_{2^n}$, e be an integer such that x^e is a permutation over $\mathbb{F}_{2^n}$ and $R_k[e, \alpha]$ be the keyed permutation

$$R_k[e, \alpha](x) = (x + \alpha k)^e + k^e.$$

The following functions

$$\begin{aligned} \mathsf{H}_e^\alpha(x, y) &= (R^{-1}_{R_y[e,\alpha](x)}(y), R_y[e, \alpha](x)), \\ \mathsf{V}_e^\alpha(x, y) &= (R_y[e, \alpha](x), R_x[e, \alpha](y)) \end{aligned}$$

are called the Open Butterfly Structure and Closed Butterfly Structure respectively.

It was shown in [PUB16] that H_e^α is a permutation over $\mathbb{F}_{2^n}^2$ and H_e^α is CCZ-equivalent to V_e^α.

Definition 2. [CDP17] Let R be a bivariate polynomial of $\mathbb{F}_{2^n}$ such that $R_y : x \mapsto R(x, y)$ is a permutation of $\mathbb{F}_{2^n}$ for all y in $\mathbb{F}_{2^n}$. The closed butterfly V_R is the function of $\mathbb{F}_{2^n}^2$ defined by

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

and the open butterfly H_R is the permutation of $\mathbb{F}_{2^n}^2$ defined by

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

where $R_y(x) = R(x, y)$ and $R_y^{-1}(R_y(x)) = x$ for any x, y.

Also, it was proved in [CDP17] that H_R is a permutation over $\mathbb{F}_{2^n}^2$, and H_R is CCZ-equivalent to V_R.

To discuss the nonlinearity of quadratic functions we recall a well-known result in [CDP17] below.

Lemma 1. *[CDP17] Let f be a quadratic Boolean function of n variables. Let* $\mathrm{LS}(f)$ *denote the linear space of f, i.e.*

$$\mathrm{LS}(f) = \{a \in \mathbb{F}_{2^n} : D_a f(x) = \varepsilon, \forall x \in \mathbb{F}_{2^n}\},$$

where $\varepsilon \in \{0, 1\}$. Then, $s = \dim \mathrm{LS}(f)$ has the same parity as n and $\mathcal{L}(f) = 2^{\frac{n+s}{2}}$. Moreover, the Walsh coefficients of f take 2^{n-s} times the value $\pm 2^{\frac{n+s}{2}}$ and $(2^n - 2^{n-s})$ times the value 0.

3 On the number of solutions to a special system of linear equations

The following result is important in the present paper.

Theorem 1. *[Blu04] Let $a, b \in \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1} + ax + b$, and i be an integer with $\gcd(i, n) = k$. Then $N(f) \in \{0, 1, 2, 2^k + 1\}$, where $N(f)$ is the number of roots of f in $\mathbb{F}_{2^n}$.*

Lemma 2. *Let $a, b, c \in \mathbb{F}_{2^n}$ with $\{a, b, c\} \neq \{0\}$, i be an integer with $\gcd(i, n) = k$, $L(x) = ax^{2^{2i}} + bx^{2^i} + cx$. Then the following statements hold.*

1. *If $a \neq 0$, then $L(x) = 0$ has at most 2^{2k} solutions in $\mathbb{F}_2^n$.*
2. *If $a = 0, b \neq 0$, then $L(x) = 0$ has at most 2^k solutions in $\mathbb{F}_2^n$.*
3. *If $a = 0, b = 0, c \neq 0$, then $L(x) = 0$ has exactly 1 solution in $\mathbb{F}_2^n$.*

Proof. 1. $a \neq 0$. Then $ax^{2^{2i}} + bx^{2^i} + cx = 0$ is equivalent to

$$\begin{aligned} 0 &= x^{2^{2i}} + \frac{b}{a}x^{2^i} + \frac{c}{a}x \\ &= x\left(x^{2^{2i}-1} + \frac{b}{a}x^{2^i-1} + \frac{c}{a}\right) \\ &= x\left((x^{2^i-1})^{2^i+1} + \frac{b}{a}x^{2^i-1} + \frac{c}{a}\right). \end{aligned}$$

Let $y = x^{2^i-1}$. According to Theorem 1, equation

$$y^{2^i+1} + a_1 y + b_1 = 0$$

has at most $2^k + 1$ solutions in $\mathbb{F}_{2^n}$ for any $a_1, b_1 \in \mathbb{F}_{2^n}$. Note that, $\gcd(i, n) = k$. Then,

$$\gcd(2^i - 1, 2^n - 1) = 2^{\gcd(i,n)} - 1 = 2^k - 1$$

and hence $x^{2^i-1} = d$ has at most $2^k - 1$ solutions in $\mathbb{F}_{2^n}$ for any $d \in \mathbb{F}_{2^n}$. Therefore, equation $(x^{2^i-1})^{2^i+1} + \frac{b}{a}x^{2^i-1} + \frac{c}{a} = 0$ has at most $(2^k - 1)(2^k + 1) = 2^{2k} - 1$ solutions in $\mathbb{F}_{2^n}$. Thus, $ax^{2^{2i}} + bx^{2^i} + cx = 0$ has at most 2^{2k} solutions in $\mathbb{F}_{2^n}$.

2. $a = 0, b \neq 0$. Then $ax^{2^{2i}} + bx^{2^i} + cx = 0$ is equivalent to

$$0 = x^{2^i} + \frac{c}{b}x = x\left(x^{2^i-1} + \frac{c}{b}\right),$$

which has at most 2^k solutions in $\mathbb{F}_{2^n}$, due to $\gcd(i, n) = k$.

3. $a = 0, b = 0, c \neq 0$. Then $ax^{2^{2i}} + bx^{2^i} + cx = 0$ if and only if $x = 0$. □

According to the result above, we have the following theorem, which is helpful in the characterizations of differential uniformity and nonlinearity of quadratic functions obtained with the butterfly construction based on Gold exponents.

Theorem 2. *Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ be two nonzero matrices over $\mathbb{F}_{2^n}$, and i be an integer with $\gcd(i, n) = k$. Let*

$$L(x, y) = A\begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B\begin{pmatrix} y^{2^i} \\ y \end{pmatrix}$$

be a linear mapping from $\mathbb{F}_{2^n}^2$ *to* $\mathbb{F}_{2^n}^2$*. Then,*

$$|\ker(L(x,y))| \leq 2^{2k}$$

if and only if the following conditions hold.

1. *When* $\mathrm{rank}(A) = 1$*, and* $\mathrm{rank}\left(\begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_3 & a_4 & b_3 & b_4 \end{pmatrix}\right) = 2$.
2. *When* $\mathrm{rank}(A) = 2$*, and there does not exist* $\lambda \in \mathbb{F}_{2^n}^*$*, such that*

$$\begin{pmatrix} a_1\lambda^{2^i} & a_2\lambda \\ a_3\lambda^{2^i} & a_4\lambda \end{pmatrix} = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Proof. Let $L_1(x,y) = a_1x^{2^i} + a_2x + b_1y^{2^i} + b_2y$, $L_2(x,y) = a_3x^{2^i} + a_4x + b_3y^{2^i} + b_4y$, we need to characterize the number of solutions to the system of linear equations below

$$\begin{cases} L_1(x,y) = 0, \\ L_2(x,y) = 0. \end{cases}$$

Note that A is not a zero matrix, we divide the discussion into the following cases.

CASE 1. $\mathrm{rank}(A) = 1$. Then without loss of generality, we suppose $\{a_1, a_2\} \neq \{0\}$ and there exists $\omega \in \mathbb{F}_{2^n}$, such that

$$\begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ 0 & 0 \end{pmatrix}.$$

By adding $\omega L_1(x,y)$ to $L_2(x,y)$, the system of linear equations above is equivalent to

$$\begin{cases} a_1x^{2^i} + a_2x + b_1y^{2^i} + b_2y = 0, & (1) \\ (b_3 + \omega b_1)y^{2^i} + (b_4 + \omega b_2)y = 0. & (2) \end{cases}$$

Then, $L(x_0, y_0) = (0,0)$ if and only if y_0 satisfies Eq. (2) and x_0 is a solution of

$$a_1x^{2^i} + a_2x + b_1y_0^{2^i} + b_2y_0 = 0.$$

According to Lemma 2, the equation above has at most 2^k solutions in $\mathbb{F}_{2^n}$ since $\{a_1, a_2\} \neq \{0\}$ and $\gcd(i,n) = k$. Therefore,

$$|\ker(L(x,y))| \leq 2^k n_0,$$

where n_0 is the number of solutions to Eq. (2). Again, by Lemma 2, $n_0 \leq 2^k$ if and only if

$$\{b_3 + \omega b_1, b_4 + \omega b_2\} \neq \{0\}.$$

Thus, $|\ker(L(x,y))| \leq 2^{2k}$ if and only if there does not exist $\omega \in \mathbb{F}_{2^n}$ such that

$$\omega L_1(x,y) + L_2(x,y) = 0,$$

which is equivalent to

$$\mathrm{rank}\left(\begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_3 & a_4 & b_3 & b_4 \end{pmatrix}\right) = 2.$$

CASE 2. $\mathrm{rank}(A) = 2$. This means that A is non-singular. By multiplying A^{-1} to the following system of linear equations

$$A\begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B\begin{pmatrix} y^{2^i} \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

we get

$$\begin{pmatrix} x^{2^i} \\ x \end{pmatrix} = A^{-1}B \begin{pmatrix} y^{2^i} \\ y \end{pmatrix}.$$

Let $A^{-1}B = C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$. Then we have

$$x^{2^i} = c_1 y^{2^i} + c_2 y \quad \text{and} \quad x = c_3 y^{2^i} + c_4 y, \tag{3}$$

from which we obtain

$$c_3^{2^i} y^{2^{2i}} + (c_1 + c_4^{2^i}) y^{2^i} + c_2 y = 0. \tag{4}$$

Thus, $L(x_0, y_0) = (0, 0)$ if and only if y_0 is a solution to Eq. (4) and x_0 can be derived uniquely by y_0 with Eq. (3). Therefore,

$$|\ker(L(x, y))| = n_0,$$

where n_0 is the number of solutions to Eq. (4). According to Lemma 2, $n_0 \leq 2^{2k}$ if and only if

$$\{c_3, c_1 + c_4^{2^i}, c_2\} \neq \{0\}.$$

Therefore, $|\ker(L(x, y))| > 2^{2k}$ if and only if

$$c_3 = c_2 = 0, c_1 = c_4^{2^i},$$

which is equivalent to the existence of $\lambda \in \mathbb{F}_{2^n}^*$, such that

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} \lambda^{2^i} & 0 \\ 0 & \lambda \end{pmatrix} = AC = B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

We complete the proof. □

Lemma 3. *Let* $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ *be two matrices over* $\mathbb{F}_{2^n}$*, and* i *be an integer with* $\gcd(i, n) = k$*. Let*

$$L(x, y) = A \begin{pmatrix} x^{2^i} \\ x \end{pmatrix} + B \begin{pmatrix} y^{2^i} \\ y \end{pmatrix}$$

be a linear mapping from $\mathbb{F}_{2^n}^2$ *to* $\mathbb{F}_{2^n}^2$*. If*

$$(a_1 b_3 + a_3 b_1) \neq 0 \text{ or } (a_2 b_4 + a_4 b_2) \neq 0,$$

then $|\ker(L(x, y))| \leq 2^{2k}$*.*

Proof. Firstly, it should be noticed that A and B cannot be zero matrix. Suppose

$$a_1 b_3 + a_3 b_1 \neq 0.$$

Then we have

$$\operatorname{rank}\left(\begin{pmatrix} a_1 & b_1 \\ a_3 & b_3 \end{pmatrix}\right) = 2, \tag{5}$$

Therefore, it always holds

$$\operatorname{rank}\left(\begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_3 & a_4 & b_3 & b_4 \end{pmatrix}\right) = 2.$$

Furthermore, equality (5) indicates that there does not exist $\lambda \in \mathbb{F}_{2^n}^*$, such that

$$a_1 \lambda^{2^i} = b_1, \text{ and } a_3 \lambda^{2^i} = b_3.$$

According to Theorem 2, we have

$$|\ker(L(x, y))| \leq 2^{2k}.$$

The case of $a_2 b_4 + a_4 b_2 \neq 0$ can be proved similarly, and we complete the proof. □

4 Cryptographic properties of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$

Throughout this section, we always suppose that n is odd and i is an integer with $\gcd(i,n)=1$. We focus on the cryptographic properties of butterfly structures

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y)=(R_{\alpha,\beta}^{2^i+1}(x,y),R_{\alpha,\beta}^{2^i+1}(y,x)),$$

and

$$\mathsf{H}_{\alpha,\beta}^{2^i+1}(x,y)=(R_{R_y[2^i+1,\alpha,\beta](x)}^{-1}(y),R_y[2^i+1,\alpha,\beta](x)),$$

where $R_{\alpha,\beta}^{2^i+1}(x,y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$ and $R_y[2^i+1,\alpha,\beta](x)=R_{\alpha,\beta}^{2^i+1}(x,y)$.

We only characterize the differential uniformity, nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ and the algebraic degree of $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ in this section since $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ and $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ are CCZ-equivalent. Before the discussion, we should notice that x^{2^i+1} is a permutation over $\mathbb{F}_{2^n}$ when $\gcd(i,n)=1$ and n is odd. Therefore, for any fixed y, $R_{\alpha,\beta}^{2^i+1}$ is a permutation. Firstly, we have the following useful lemma.

Lemma 4. *Let n be odd and i be an integer with $\gcd(i,n)=1$, $\alpha,\beta\in\mathbb{F}_{2^n}^*$. Let $\gamma=\alpha^{2^i+1}+\beta$, $D=\gamma\alpha^{2^i}+\alpha$, $E=(\alpha+1)^{2^i+1}+\beta$, $F=\alpha^{2^i}+\gamma\alpha$. Suppose $E\neq 0$. Then the equations*

$$Dx^2+E^2x+D=0$$

and

$$Fx^{2^{i+1}}+E^2x^{2^i}+F=0$$

do not have common solutions in $\mathbb{F}_{2^n}$.

Proof. Firstly, we claim that D and F cannot both be equal to zero. Otherwise, from

$$\gamma\alpha^{2^i}+\alpha=0=\alpha^{2^i}+\gamma\alpha$$

we have $\gamma=\alpha^{2^i-1}=\alpha^{-(2^i-1)}$. Then $\alpha^{2^i-1}=1$ and hence $\alpha=1$ since $\gcd(i,n)=1$ and n is odd. Therefore, $\gamma=\alpha^{2^i-1}=1$ and

$$\beta=\alpha^{2^i+1}+\gamma=1+1=0.$$

This contradicts $\beta\in\mathbb{F}_{2^n}^*$. Thus, the claim holds.

Assume $z\in\mathbb{F}_{2^n}$ is a common solution to the above equations and we have

$$\begin{cases} Dz^2+E^2z+D=0 & (6)\\ Fz^{2^{i+1}}+E^2z^{2^i}+F=0 & (7)\end{cases}$$

Note that $E\neq 0$, then Eq. (6) is equivalent to

$$\left(\frac{D}{E^2}\right)^{2^i}z^{2^{i+1}}+z^{2^i}+\left(\frac{D}{E^2}\right)^{2^i}=0.$$

Dividing Eq. (7) by E^2 and adding to the equation above, we get

$$\left(\left(\frac{D}{E^2}\right)^{2^i}+\frac{F}{E^2}\right)z^{2^{i+1}}+\left(\frac{D}{E^2}\right)^{2^i}+\frac{F}{E^2}=0.$$

When $\left(\frac{D}{E^2}\right)^{2^i}+\frac{F}{E^2}\neq 0$, we have $z=1$. But $z=1$ does not satisfy Eq. (6) and Eq. (7), since $E\neq 0$. This means that the theorem holds when $\left(\frac{D}{E^2}\right)^{2^i}+\frac{F}{E^2}\neq 0$.

Now, suppose $\left(\frac{D}{E^2}\right)^{2^i} + \frac{F}{E^2} = 0$, which is equivalent to

$$D^{2^i}E^2 + E^{2^{i+1}}F = 0. \tag{8}$$

Substitute $z + \alpha$ to Eq. (6) and Eq. (7), we get

$$\begin{cases} D(z+\alpha)^2 + E^2(z+\alpha) + D + D\alpha^2 + E^2\alpha = 0, \\ F(z+\alpha)^{2^{i+1}} + E^2(z+\alpha)^{2^i} + F + F\alpha^{2^{i+1}} + E^2\alpha^{2^i} = 0. \end{cases} \tag{9}$$

Note that $\gamma = \alpha^{2^i+1} + \beta$, then

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

Hence,

$$\begin{aligned} D + D\alpha^2 + E^2\alpha &= \gamma\alpha^{2^i} + \alpha + \gamma\alpha^{2^i+2} + \alpha^3 + \gamma^2\alpha + \alpha^{2^{i+1}+1} + \alpha^3 + \alpha \\ &= \alpha^{2^i}(\gamma + \alpha^{2^i+1}) + \gamma\alpha(\alpha^{2^i+1} + \gamma) \\ &= (\alpha^{2^i} + \gamma\alpha)(\gamma + \alpha^{2^i+1}) \\ &= F\beta, \end{aligned}$$

and

$$\begin{aligned} F + F\alpha^{2^{i+1}} + E^2\alpha^{2^i} &= \alpha^{2^i} + \gamma\alpha + \alpha^{2^{i+1}+2^i} + \gamma\alpha^{2^{i+1}+1} + \gamma^2\alpha^{2^i} + \alpha^{2^{i+1}+2^i} + \alpha^{2^i+2} + \alpha^{2^i} \\ &= \gamma(\alpha + \gamma\alpha^{2^i}) + \alpha^{2^i+1}(\gamma\alpha^{2^i} + \alpha) \\ &= (\gamma\alpha^{2^i} + \alpha)(\gamma + \alpha^{2^i+1}) \\ &= D\beta. \end{aligned}$$

Therefore, Eqs. (9) become

$$\begin{cases} D(z+\alpha)^2 + E^2(z+\alpha) + F\beta = 0, & (10) \\ F(z+\alpha)^{2^{i+1}} + E^2(z+\alpha)^{2^i} + D\beta = 0. & (11) \end{cases}$$

Eq. (10) is equivalent to

$$D^{2^i}(z+\alpha)^{2^{i+1}} + E^{2^{i+1}}(z+\alpha)^{2^i} + (F\beta)^{2^i} = 0.$$

Multiplying it by F and adding to Eq. (11) multiplied by D^{2^i}, we get

$$(E^{2^{i+1}}F + D^{2^i}E^2)(z+\alpha)^{2^i} = D^{2^i+1}\beta + F^{2^i+1}\beta^{2^i}.$$

According to Eq. (8), we deduce that the previous expression is zero, implying that

$$D^{2^i+1} = F^{2^i+1}\beta^{2^i-1},$$

which is equivalent to

$$D = F\beta^{\frac{2^i-1}{2^i+1}},$$

due to $\gcd(i, n) = 1$ and n being odd. Then, $F \neq 0$. Otherwise, $D = F\beta^{\frac{2^i-1}{2^i+1}} = 0$. A contradiction, since we have proved that D and F cannot both be equal to zero. Substitute it to Eq. (8) and obtain

$$E^2 = F\beta^{\frac{2^i}{2^i+1}}.$$

Plugging the above two equalities into Eq. (10), we have

$$F\beta^{\frac{2^i-1}{2^i+1}}(z+\alpha)^2 + F\beta^{\frac{2^i}{2^i+1}}(z+\alpha) + F\beta = 0,$$

which is equivalent to

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

Dividing by $\beta^{2/(2^i+1)}$, we get

$$\left(\frac{z+\alpha}{\beta^{1/(2^i+1)}}\right)^2 + \frac{z+\alpha}{\beta^{1/(2^i+1)}} = 1,$$

which indicates

$$\mathrm{Tr}(1) = \mathrm{Tr}\left(\left(\frac{z+\alpha}{\beta^{1/(2^i+1)}}\right)^2 + \frac{z+\alpha}{\beta^{1/(2^i+1)}}\right) = 0.$$

This contradicts $\mathrm{Tr}(1) = 1$ for odd n. □

4.1 Differential uniformity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$

Theorem 3. *Let n be odd, i be an integer with $\gcd(i,n) = 1$, $\alpha, \beta \in \mathbb{F}_{2^n}^*$ and $\beta \neq (\alpha+1)^{2^i+1}$. Then the differential uniformity of*

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y) = (R_{\alpha,\beta}^{2^i+1}(x,y), R_{\alpha,\beta}^{2^i+1}(y,x))$$

is at most 4, where $R_{\alpha,\beta}^{2^i+1}(x,y) = (x+\alpha y)^{2^i+1} + \beta y^{2^i+1}$.

Proof. We need to prove that for any $(a,b),(c,d) \in \mathbb{F}_{2^n}^2$ and $(a,b) \neq (0,0)$, the equation

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y) + \mathsf{V}_{\alpha,\beta}^{2^i+1}(x+a,y+b) = (c,d)$$

has at most 4 solutions in $\mathbb{F}_{2^n}^2$. For any fixed $(a,b) \neq (0,0) \in \mathbb{F}_{2^n}^2$, denote $L_{a,b}(x,y) = \mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y) + \mathsf{V}_{\alpha,\beta}^{2^i+1}(x+a,y+b)$. It is clear that $L_{a,b}$ is a linear mapping over $\mathbb{F}_{2^n}^2$ and $L_{a,b}(x,y) = (c,d)$ has no solutions or the same number of solutions as $L_{a,b}(x,y) = (0,0)$. We demonstrate that $L_{a,b}(x,y) = (0,0)$ has at most 4 solutions in $\mathbb{F}_{2^n}^2$, which is equivalent to prove that the following system of linear equations

$$\begin{cases} R_{\alpha,\beta}^{2^i+1}(x,y) + R_{\alpha,\beta}^{2^i+1}(x+a,y+b) + R_{\alpha,\beta}^{2^i+1}(a,b) = 0 \\ R_{\alpha,\beta}^{2^i+1}(y,x) + R_{\alpha,\beta}^{2^i+1}(y+b,x+a) + R_{\alpha,\beta}^{2^i+1}(b,a) = 0 \end{cases}$$

has at most 4 solutions in $\mathbb{F}_{2^n}^*$. Let $\gamma = \alpha^{2^i+1} + \beta$. Then the system of linear equations above equals

$$\begin{cases} (a+\alpha b)x^{2^i} + (a+\alpha b)^{2^i}x + (\alpha^{2^i}a + \gamma b)y^{2^i} + (\alpha a^{2^i} + \gamma b^{2^i})y = 0 \\ (\gamma a + \alpha^{2^i}b)x^{2^i} + (\gamma a^{2^i} + \alpha b^{2^i})x + (\alpha a + b)y^{2^i} + (\alpha a + b)^{2^i}y = 0. \end{cases} \tag{12}$$

Firstly, we claim that

$$\begin{aligned} (a+\alpha b)(\alpha a+b) &= (\gamma a + \alpha^{2^i}b)(\alpha^{2^i}a + \gamma b) \\ (a+\alpha b)^{2^i}(\alpha a+b)^{2^i} &= (\gamma a^{2^i} + \alpha b^{2^i})(\alpha a^{2^i} + \gamma b^{2^i}) \end{aligned}$$

cannot hold simultaneously. By a simple computation, the above equalities become

$$(\gamma\alpha^{2^i}+\alpha)a^2+(\gamma^2+\alpha^{2^{i+1}}+\alpha^2+1)ab+(\gamma\alpha^{2^i}+\alpha)b^2=0$$
$$(\gamma\alpha+\alpha^{2^i})a^{2^{i+1}}+(\gamma^2+\alpha^{2^{i+1}}+\alpha^2+1)a^{2^i}b^{2^i}+(\gamma\alpha+\alpha^{2^i})b^{2^{i+1}}=0.$$

When $b=0$. Then $a\neq 0$, implying that the above equalities cannot hold simultaneously since we have proved that $\gamma\alpha^{2^i}+\alpha$ and $\gamma\alpha+\alpha^{2^i}$ cannot both be zero in Lemma 4.

When $b\neq 0$. Let $y=\frac{a}{b}$ and divide the above two equalities by b^2 and $b^{2^{i+1}}$ respectively, then we get

$$\begin{cases}(\gamma\alpha^{2^i}+\alpha)y^2+(\gamma^2+\alpha^{2^{i+1}}+\alpha^2+1)y+(\gamma\alpha^{2^i}+\alpha)=0,\\ (\gamma\alpha+\alpha^{2^i})y^{2^{i+1}}+(\gamma^2+\alpha^{2^{i+1}}+\alpha^2+1)y^{2^i}+(\gamma\alpha+\alpha^{2^i})=0.\end{cases}$$

According to Lemma 4, the above two equalities do not have common solutions in $\mathbb{F}_{2^n}$. Then the claim holds, and hence Eq. (12) has at most 4 solutions in $\mathbb{F}_{2^n}^2$ by Lemma 3. Thus, $L_{a,b}(x,y)=(c,d)$ has at most 4 solutions in $\mathbb{F}_{2^n}^2$. □

4.2 Nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$

Theorem 4. *Let n be odd, i be an integer with $\gcd(i,n)=1$, $\alpha,\beta\in\mathbb{F}_{2^n}^*$ and $\beta\neq(\alpha+1)^{2^i+1}$. Let $R_{\alpha,\beta}^{2^i+1}(x,y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$. Then the nonlinearity of*

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y)=(R_{\alpha,\beta}^{2^i+1}(x,y),R_{\alpha,\beta}^{2^i+1}(y,x))$$

is equal to $2^{2n-1}-2^n$, which is the best known nonlinearity over $\mathbb{F}_{2^n}^2$.

Proof. We only need to prove that for $(a,b),(c,d)\in\mathbb{F}_{2^n}^2$ with $(a,b)\neq(0,0)$, it holds

$$|\lambda_{\mathsf{V}}((c,d),(a,b))|\leq 2^{n+1},$$

where

$$\lambda_{\mathsf{V}}((c,d),(a,b))=\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}((a,b)\cdot\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y)+cx+dy)}$$
$$=\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}((a+b(\alpha^{2^i+1}+\beta))x^{2^i+1}+(a\alpha+b\alpha^{2^i})x^{2^i}y+(a\alpha^{2^i}+b\alpha)xy^{2^i}+(a(\alpha^{2^i+1}+\beta)+b)y^{2^i+1}+cx+dy)}.$$

Let $\gamma=\alpha^{2^i+1}+\beta$, and

$$A=a+b\gamma, B=a\alpha+b\alpha^{2^i}, C=a\alpha^{2^i}+b\alpha, D=a\gamma+b,$$

and

$$f(x,y)=\mathrm{Tr}(Ax^{2^i+1}+Bx^{2^i}y+Cxy^{2^i}+Dy^{2^i+1}).$$

Then, $\lambda_{\mathsf{V}}((c,d),(a,b))\leq\mathcal{L}(f)$. From Lemma 1, we consider the linear space of f and determine $\dim\mathrm{LS}(f)$. Let $(u,v)\in\mathbb{F}_{2^n}^2$, then

$$\begin{aligned}D_{(u,v)}f(x,y) &= \mathrm{Tr}\left((Au^{2^i}+(Au)^{2^{n-i}}+Cv^{2^i}+(Bv)^{2^{n-i}})x\right)\\ &\quad+\mathrm{Tr}\left((Bu^{2^i}+(Cu)^{2^{n-i}}+Dv^{2^i}+(Dv)^{2^{n-i}})y\right)+c\end{aligned}$$

for some $c\in\mathbb{F}_2$. This implies that $D_{(u,v)}f(x,y)$ is constant if and only if (u,v) satisfies

$$\begin{cases}Au^{2^i}+(Au)^{2^{n-i}}+Cv^{2^i}+(Bv)^{2^{n-i}}=0,\\ Bu^{2^i}+(Cu)^{2^{n-i}}+Dv^{2^i}+(Dv)^{2^{n-i}}=0.\end{cases}$$

which is equivalent to

$$\begin{cases} A^{2^i}u^{2^{2i}} + Au + C^{2^i}v^{2^{2i}} + Bv = 0, \\ B^{2^i}u^{2^{2i}} + Cu + D^{2^i}v^{2^{2i}} + Dv = 0. \end{cases} \tag{13}$$

Firstly, we prove that $A = 0, B = 0, C = 0$ cannot hold simultaneously. Suppose that $B = C = 0$, then there exists $(a, b) \in \mathbb{F}_{2^n}^2$ with $(a, b) \neq (0, 0)$, such that

$$\begin{cases} \alpha a + \alpha^{2^i} b = 0, \\ \alpha^{2^i} a + \alpha b = 0. \end{cases}$$

We deduce that

$$\det\left(\begin{pmatrix} \alpha, & \alpha^{2^i} \\ \alpha^{2^i}, & \alpha \end{pmatrix}\right) = (\alpha + \alpha^{2^i})^2 = 0,$$

i.e. $\alpha = 1$ and $a = b$ since $\gcd(i, n) = 1$. Note that $(a, b) \neq (0, 0)$, we have $b \neq 0$. Thus,

$$A = D = (\gamma + 1)b = \beta b \neq 0.$$

This means $A = B = C = 0$ cannot hold. Also, we can deduce that $B = 0, C = 0, D = 0$ cannot hold at the same time. Then we have the following cases:

CASE 1. $A = 0$. Then $B = 0$ and $C = 0$ cannot hold simultaneously. Therefore,

$$\operatorname{rank}\left(\begin{pmatrix} A^{2^i} & A \\ B^{2^i} & C \end{pmatrix}\right) = \operatorname{rank}\left(\begin{pmatrix} 0 & 0 \\ B^{2^i} & C \end{pmatrix}\right) = 1,$$

and

$$\operatorname{rank}\left(\begin{pmatrix} A^{2^i} & A & C^{2^i} & B \\ B^{2^i} & C & D^{2^i} & D \end{pmatrix}\right) = \operatorname{rank}\left(\begin{pmatrix} 0 & 0 & C^{2^i} & B \\ B^{2^i} & C & D^{2^i} & D \end{pmatrix}\right) = 2.$$

According to Theorem 2, Eq. (13) has at most 4 solutions in $\mathbb{F}_{2^n}^2$ since n is odd and $\gcd(2i, n) = \gcd(i, n) = 1$. It follows that $\dim \mathrm{LS}(f) = 2$.

CASE 2. $A \neq 0$ and $A^{2^i}C + B^{2^i}A = 0$. Then,

$$\operatorname{rank}\left(\begin{pmatrix} A^{2^i} & A \\ B^{2^i} & C \end{pmatrix}\right) = 1.$$

In this case, we claim that

$$\operatorname{rank}\left(\begin{pmatrix} A^{2^i} & A & C^{2^i} & B \\ B^{2^i} & C & D^{2^i} & D \end{pmatrix}\right) = 2. \tag{14}$$

Otherwise, we assume

$$\operatorname{rank}\left(\begin{pmatrix} A^{2^i} & A & C^{2^i} & B \\ B^{2^i} & C & D^{2^i} & D \end{pmatrix}\right) = 1.$$

This means that there exists $\omega \in \mathbb{F}_{2^n}^*$, such that

$$B^{2^i} = A^{2^i}\omega, C = A\omega, D^{2^i} = C^{2^i}\omega, D = B\omega,$$

which is equivalent to

$$B = A\omega^{2^{n-i}}, C = A\omega, D = A\omega^{2^{n-i}+1}.$$

This implies that there exists $(0,0) \neq (a,b) \in \mathbb{F}_{2^n}^2$, such that

$$\begin{aligned}(\omega^{2^{n-i}}+\alpha)a+(\omega^{2^{n-i}}\gamma+\alpha^{2^i})b=0\\(\omega+\alpha^{2^i})a+(\omega\gamma+\alpha)b=0\\(\omega^{2^{n-i}+1}+\gamma)a+(\omega^{2^{n-i}+1}\gamma+1)b=0.\end{aligned}$$

Therefore, the following matrix

$$\begin{pmatrix}\omega^{2^{n-i}}+\alpha, & \omega^{2^{n-i}}\gamma+\alpha^{2^i}\\ \omega+\alpha^{2^i}, & \omega\gamma+\alpha\\ \omega^{2^{n-i}+1}+\gamma, & \omega^{2^{n-i}+1}\gamma+1\end{pmatrix}$$

are not of full rank and hence the determinants of its sub-matrices of order 2 are all equal to zero. By computing the determinants of the sub-matrices formed by the first two rows and the first and last rows respectively, we have

$$(\alpha+\alpha^{2^i}\gamma)\omega^{2^{n-i}}+(\alpha^{2^i}+\alpha\gamma)\omega+\alpha^2+\alpha^{2^{i+1}}=0,$$

$$(\alpha^{2^i}+\alpha\gamma)\omega^{2^{n-i}+1}+(\gamma^2+1)\omega^{2^{n-i}}+\alpha+\alpha^{2^i}\gamma=0.$$

With the above two equations, we deduce

$$\begin{aligned}0 &= \omega^{2^{n-i}}\left((\alpha+\alpha^{2^i}\gamma)\omega^{2^{n-i}}+\alpha^2+\alpha^{2^{i+1}}\right)+(\gamma^2+1)\omega^{2^{n-i}}+\alpha+\alpha^{2^i}\gamma\\ &= (\alpha+\alpha^{2^i}\gamma)\omega^{2^{n-i+1}}+(\gamma^2+\alpha^2+\alpha^{2^{i+1}}+1)\omega^{2^{n-i}}+\alpha+\alpha^{2^i}\gamma.\end{aligned}$$

Similarly, from $C=A\omega$ and $D=B\omega$, we also obtain

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

Let $\omega=\zeta^{2^i}$. Then, ζ satisfies

$$\begin{cases}(\alpha+\alpha^{2^i}\gamma)\zeta^2+(\gamma^2+\alpha^2+\alpha^{2^{i+1}}+1)\zeta+\alpha+\alpha^{2^i}\gamma &= 0\\ (\alpha^{2^i}+\alpha\gamma)\zeta^{2^{i+1}}+(\gamma^2+\alpha^2+\alpha^{2^{i+1}}+1)\zeta^{2^i}+\alpha^{2^i}+\alpha\gamma &= 0.\end{cases}$$

Note that $\gamma^2+\alpha^{2^{i+1}}+\alpha^2+1=(\beta+(\alpha+1)^{2^i+1})^2\neq 0$, then according to Lemma 4, the above system of equations does not have solutions in $\mathbb{F}_{2^n}$, a contradiction. Therefore, equality (14) holds and by Theorem 2, Eq. (13) has at most 4 solutions in $\mathbb{F}_{2^n}^2$, i.e., $\dim \mathrm{LS}(f)=2$.

CASE 3. $A\neq 0$ and $A^{2^i}C+B^{2^i}A\neq 0$. According to Theorem 2, we only need to prove that there does not exist $\kappa\in\mathbb{F}_{2^n}^*$, such that

$$\begin{pmatrix}A^{2^i}\kappa^{2^{2i}} & A\kappa\\ B^{2^i}\kappa^{2^{2i}} & C\kappa\end{pmatrix}=\begin{pmatrix}C^{2^i} & B\\ D^{2^i} & D\end{pmatrix}.$$

which is equivalent to

$$C=A\kappa^{2^i}, B=A\kappa, D=C\kappa.$$

Assume that there exists $\kappa\in\mathbb{F}_{2^n}^*$ satisfying the above equalities, we have

$$A^{2^i}C+B^{2^i}A=A^{2^i+1}\kappa^{2^i}+A^{2^i+1}\kappa^{2^i}=0,$$

which contradicts the case condition that $A^{2^i}C+B^{2^i}A\neq 0$. Again, by Theorem 2, Eq. (13) has at most 4 solutions in $\mathbb{F}_{2^n}^2$, i.e., $\dim \mathrm{LS}(f)=2$.

From the discussions on all the cases above, we always have $\dim \mathrm{LS}(f)=2$. Thus, $\mathcal{L}(f)=2^{\frac{2n+2}{2}}=2^{n+1}$ by Lemma 1. We complete the proof. □

4.3 Algebraic Degree of $\mathsf{H}_{\alpha,\beta}^{2^i+1}$

Note that $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ is CCZ-equivalent to $\mathsf{V}_{\alpha,\beta}^{2^i+1}$, then $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ is a differentially 4-uniform permutation over $\mathbb{F}_{2^n}^2$ with the best known nonlinearity. In this subsection, we characterize the algebraic degree of $\mathsf{H}_{\alpha,\beta}^{2^i+1}$. The inverse of 3 modulo (2^n-1) and its Hamming weight have been determined in [Nyb93] and [KS12], as recalled in the following lemma.

Lemma 5. *[Nyb93, KS12] Let n be odd, i be a non-negative integer such that $\gcd(i,n)=1$. Then the compositional inverse of x^{2^i+1} over $\mathbb{F}_{2^n}$ is also a power function x^d, and its algebraic degree is $\frac{n+1}{2}$, where $d=\sum_{j=0}^{\frac{n-1}{2}} 2^{2ji} \bmod (2^n-1)$.*

We apply a similar method as that in [CDP17] to investigate the algebraic degree and deduce the following result.

Theorem 5. *Let n be odd, i be an integer with $\gcd(i,n)=1$ and $\alpha,\beta\in\mathbb{F}_{2^n}^*$. The algebraic degree of the open butterfly*

$$\mathsf{H}_{\alpha,\beta}^{2^i+1}(x,y) = \Big(\Big(y+\alpha((x+\beta y^{2^i+1})^{\frac{1}{2^i+1}}+\alpha y)\Big)^{2^i+1}+\beta\Big((x+\beta y^{2^i+1})^{\frac{1}{2^i+1}}+\alpha y\Big)^{2^i+1}, \\ (x+\beta y^{2^i+1})^{\frac{1}{2^i+1}}+\alpha y\Big)$$

is equal to n or $n+1$. It is equal to n if and only if

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

The closed butterfly $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ has algebraic degree 2.

Proof. The algebraic degree of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is obviously 2. We only discuss the algebraic degree of $\mathsf{H}_{\alpha,\beta}^{2^i+1}(x,y)=(F_1(x,y),F_2(x,y))$.

Firstly, we consider the right side of the output

$$F_2(x,y)=(x+\beta y^{2^i+1})^{\frac{1}{2^i+1}}+\alpha y.$$

Its algebraic degree is mainly determined by

$$t(x,y)=(x+\beta y^{2^i+1})^{\frac{1}{2^i+1}}.$$

According to Lemma 5, we have

$$t(x,y)=\sum_{J\subseteq[0,(n-1)/2]}\underbrace{\prod_{j\in J}\beta^{2^{2ji}}y^{(2^i+1)2^{2ji}}}_{\deg\le 2|J|}\underbrace{\prod_{j\in\overline{J}}x^{2^{2ji}}}_{\deg=(n+1)/2-|J|},$$

where $\overline{J}$ is the complement of J in $[0,(n-1)/2]$. The algebraic degree of each term is at most equal to $|J|+(n+1)/2$. Thus, if $|J|<(n-1)/2$, then the degree of corresponding term is smaller than n. We focus on the case when $|J|=(n-1)/2$ or $(n+1)/2$, i.e., $\overline{J}=\emptyset$ or $\{j\}$ for some j.

CASE 1. $\overline{J}=\emptyset$, the corresponding term is equal to $\beta^{\frac{1}{2^i+1}}y$ and has degree 1.

CASE 2. $\overline{J}=\{j\}$ for some $j\in[0,(n-1)/2]$, the term is equal to

$$\begin{aligned} T &= x^{2^{2ji}}\times\beta^{\frac{1}{2^i+1}}y\times(\beta y^{2^i+1})^{2^n-1-2^{2ji}} \\ &= \beta^{\frac{1}{2^i+1}-2^{2ji}}\times x^{2^{2ji}}\times y^{(2^n-1)-(2^{(2j+1)i}+2^{2ji}-1)}. \end{aligned}$$

If $j \neq 0, (n-1)/2$, we have

$$2ji \not\equiv 0 \,(\bmod\ n), (2j+1)i \not\equiv 0 \,(\bmod\ n), 2ji \not\equiv (2j+1)i \,(\bmod\ n),$$

since n is odd and $\gcd(i,n) = 1$. Denote $\bar{l}$ the unique integer $r, 0 \leq r < n$ such that $l = qn + r$ with $q \in \mathbb{Z}$. Then T has algebraic degree

$$1 + n - \omega_2(2^{(2j+1)i} + 2^{2ji} - 1) = \begin{cases} n - \overline{2ji}, & \overline{(2j+1)i} > \overline{2ji} \\ n - \overline{(2j+1)i}, & \overline{(2j+1)i} < \overline{2ji}, \end{cases}$$

which is smaller than n.

If $j = 0, (n-1)/2$, the corresponding terms equal to

$$\begin{aligned} m_0(x,y) &= \beta^{\frac{1}{2^i+1}-1} x y^{2^n-1-2^i}, \\ m_1(x,y) &= \beta^{\frac{1}{2^i+1}-2^{(n-1)i}} x^{2^{(n-1)i}} y^{2^n-1-2^{(n-1)i}}, \end{aligned}$$

and both with degree n. Note that $2^{(n-1)i} \not\equiv 1 \,(\bmod 2^n - 1)$, since $\gcd(i,n) = 1$. Thus, F_2 has degree n.

Then consider the left side of the output

$$\begin{aligned} F_1(x,y) &= (y + \alpha(t(x,y) + \alpha y))^{2^i+1} + \beta\,(t(x,y) + \alpha y)^{2^i+1} \\ &= t(x,y)^{2^i+1}(\alpha^{2^i+1} + \beta) + y^{2^i+1}\left((1+\alpha^2)^{2^i+1} + \beta\alpha^{2^i+1}\right) \\ &\quad + y t(x,y)^{2^i}\left(\alpha^{2^i}(1+\alpha^2) + \beta\alpha\right) + y^{2^i} t(x,y)\left((1+\alpha^2)^{2^i}\alpha + \beta\alpha^{2^i}\right). \end{aligned}$$

The degree of terms on the first line is at most 2. Denote the sum of second line by $F'(x,y)$, then

$$\frac{F'(x,y)}{\alpha} = C_0 y t(x,y)^{2^i} + C_1 y^{2^i} t(x,y),$$

where

$$C_0 = \alpha^{2^i-1} + \alpha^{2^i+1} + \beta \text{ and } C_1 = 1 + \alpha^{2^{i+1}} + \beta\alpha^{2^i-1}.$$

Since $t(x,y)$ has degree n, then $\mathsf{H}^{2^i+1}_{\alpha,\beta}$ has degree at most $n+1$ and at least n. We discuss the terms in F_1 which may have degree $n+1$, (omitting the constant factors):

$$y m_0(x,y)^{2^i} = x^{2^i} y^{(2^n-1)-(2^{2i}-1)}, \quad y^{2^i} m_0(x,y) = x y^{2^n-1}$$

$$y m_1(x,y)^{2^i} = x y^{2^n-1}, \quad y^{2^i} m_1(x,y) = x^{2^{(n-1)i}} y^{(2^n-1)-(2^{(n-1)i}-2^i)}.$$

Note that $2i \not\equiv 0 \,(\bmod n)$ and $(n-1)i \not\equiv i (\bmod n)$, since n is odd and $\gcd(i,n) = 1$. Then the term of degree $n+1$ in F_1 is

$$\begin{aligned} C_0 y m_1(x,y)^{2^i} + C_1 y^{2^i} m_0(x,y) &= x y^{2^n-1}\left(C_0 \beta^{\frac{2^i}{2^i+1}-1} + C_1 \beta^{\frac{1}{2^i+1}-1}\right) \\ &= x y^{2^n-1} \beta^{\frac{1}{2^i+1}-1}\left(C_0 \beta^{\frac{2^i-1}{2^i+1}} + C_1\right). \end{aligned}$$

Thus, $\mathsf{H}^{2^i+1}_{\alpha,\beta}$ has degree n if and only if $C_0 \beta^{\frac{2^i-1}{2^i+1}} = C_1$, which is equivalent to

$$C_0^{2^i+1} \beta^{2^i-1} = C_1^{2^i+1}.$$

Then we have

$$\beta^{2^i-1}\left(\alpha^{2^i-1} + \alpha^{2^i+1} + \beta\right)^{2^i+1} = \left(1 + \alpha^{2^{i+1}} + \beta\alpha^{2^i-1}\right)^{2^i+1},$$

and we complete the proof. □

Similar to [CDP17], we also have the following remark to simplify the condition above.

Remark 1. Let $\theta^{2^i+1} = \beta$ then θ is uniquely determined by β and the condition

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

is equivalent to $Z(\alpha, \theta) = 0$, where

$$Z(\alpha,\theta) = \alpha^{2^{i+1}} + \alpha^{2^i-1}(\theta^{2^i-1} + \theta^{2^i+1}) + \theta^{2^i-1}\alpha^{2^i+1} + \theta^{2^{i+1}} + 1.$$

Moreover, Z can be rewritten as

$$\begin{aligned} Z(\alpha,\theta) &= (1+\alpha+\theta)^{2^{i+1}} + (1+\alpha+\theta)^{2^i}\left(\alpha\theta^{2^i-1} + \tfrac{\theta^{2^i-1}+\theta^{2^i+1}}{\alpha}\right) \\ &\quad +(1+\theta^{2^i})\left(\alpha\theta^{2^i-1} + \tfrac{\theta^{2^i-1}+\theta^{2^i+1}}{\alpha}\right) \\ &= (1+\alpha+\theta)^2\left((1+\alpha+\theta)^{2^{i+1}-2} + (\theta\alpha)^{2^i-1}\right). \end{aligned}$$

Hence, if $1+\alpha+\theta \neq 0$, i.e., $(1+\alpha)^{2^i+1} \neq \beta$, $Z(\alpha,\theta) = 0$ if and only if

$$[(1+\alpha+\theta)^2]^{2^i-1} = (\theta\alpha)^{2^i-1}.$$

Since $\gcd(i, n) = 1$, we obtain $\theta^2 + \theta\alpha + \alpha^2 + 1 = 0$ which holds when $\mathrm{Tr}(\alpha^{-1}) = 1$ and each α is linked to two corresponding θ (or β). Therefore, the condition in Theorem 5 holds when $(1+\alpha)^{2^i+1} = \beta$ or $\mathrm{Tr}(\alpha^{-1}) = 1$ for two additional β.

4.4 Experimental results

In this subsection, we give the list of all CCZ-equivalent classes of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ and $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ in the case of $n = 5$ as found with Magma. To classify our constructions and compare them with previous ones, we consider the result for $n = 5$. Indeed, for $n = 3$, $i = 1$ is the unique possible exponent and then our constructions are included in the previous ones.

Again, we focus on the CCZ-equivalent classes of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$. Let $L_i(x, y) = (x^{2^i}, y^{2^i})$, which is a linear permutation over $\mathbb{F}_{2^n}^2$. It holds that

$$L_{n-i}(\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y)) = ((R_{\alpha,\beta}^{2^i+1}(x,y))^{2^{n-i}}, (R_{\alpha,\beta}^{2^i+1}(y,x))^{2^{n-i}}) = \mathsf{V}_{\alpha,\beta^{2^{n-i}}}^{2^{n-i}+1}(x,y),$$

which means $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is EA-equivalent to $\mathsf{V}_{\alpha,\beta^{2^{n-i}}}^{2^{n-i}+1}$. Therefore, we only give the result for $i = 1, 2$ in the case of $n = 5$.

Since $\mathbb{F}_{2^5}$ is a subfield of $\mathbb{F}_{2^{10}}$, $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ can be represented by polynomials over $\mathbb{F}_{2^{10}}$ using Lagrange interpolation. This is convenient for testing the CCZ-equivalence between functions. In our experiment, we use $p(x) = x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ to define the finite field $\mathbb{F}_{2^{10}}$. Let g be a root of $p(x)$, then g is a primitive element of $\mathbb{F}_{2^{10}}$ and g^{33} is a primitive element of $\mathbb{F}_{2^5}$.

Let

$$S = \{\mathsf{V}_{\alpha,\beta}^{2^i+1} : \alpha, \beta \in \mathbb{F}_{2^5}^*, \beta \neq (\alpha+1)^{2^i+1}, i = 1, 2\}.$$

For $f \in S$, we can construct the extended code $\tilde{C}_f$ with Magma. Also, we can determine whether two linear codes are equivalent by using the command "IsEquivalent" in Magma. Then, for a given function $h \in S$, we can obtain the following set

$$S_h = \{f \in S : \mathrm{IsEquivalent}(\tilde{C}_f, \tilde{C}_h) = \mathrm{true}\},$$

which contains all the functions in S that are CCZ-equivalent to h. We store S_h and let $S \coloneqq S \setminus S_h$. Repeat this process until $S = \emptyset$, then we get all CCZ-equivalent classes of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$.

Our results are summarized in Table 1, where we list representative elements of CCZ-equivalent classes of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$. The table shows that 7 classes of functions can be constructed from the work of [PUB16] ($i = 1, \beta = 1$), and 6 new classes can be constructed from the works of [FFW17] ($i = 1, 2, \beta = 1$) and [CDP17] ($i = 1, \beta \neq 0$) respectively. All of the previous constructions are covered by our work, and 7 new classes can be found by our constructions.

Table 1: CCZ-inequivalence functions/permutations over $\mathbb{F}_{2^5}^2$ constructed with butterfly structure

$R(x,y)$ $(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$	Representative elements	Number
$i=1, \beta=1$	$\alpha = 1, g^{33}, g^{99}, g^{165}, g^{231}, g^{363}, g^{495}$	7
$i=2,\ \beta=1$	$\alpha = 1, g^{33}, g^{99}, g^{165}, g^{363}, g^{495}$	6
$i=1,\ \beta\neq 1$	$(\alpha,\beta) = (1,g^{33}), (1,g^{165}), (g^{33},g^{33}),$ $(g^{33},g^{165}), (g^{33},g^{693}), (g^{33},g^{726})$	6
$i=2,\ \beta\neq 1$	$(\alpha,\beta) = (1,g^{99}), (1,g^{363}), (1,g^{495}), (g^{33},g^{99}),$ $(g^{33},g^{132}), (g^{33},g^{198}), (g^{99},g^{165})$	7

5 The case of $\gcd(i,n) = k$

In this subsection, we discuss a more general case of $\gcd(i,n) = k$. Firstly, for $a, b \in \mathbb{F}_{2^n}^*$, the equation

$$ax^2 + bx + a = 0$$

is equivalent to

$$\left(\frac{x}{b/a}\right)^2 + \frac{x}{b/a} + \left(\frac{a}{b}\right)^2 = 0,$$

has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{a}{b}) = 0$.

Theorem 6. *Let n, i be integers with $\gcd(i,n) = k$, $\alpha, \beta \in \mathbb{F}_{2^n}^*$ and $\beta \neq (\alpha+1)^{2^i+1}$. Let $R_{\alpha,\beta}^{2^i+1}(x,y) = (x+\alpha y)^{2^i+1} + \beta y^{2^i+1}$ and*

$$\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y) = (R_{\alpha,\beta}^{2^i+1}(x,y), R_{\alpha,\beta}^{2^i+1}(y,x)).$$

If $\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right) = 1$, then the following statements hold.

1. *The differential uniformity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at most 2^{2k}.*

2. *The nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at least $2^{2n-1} - 2^{n+k_1-1}$, where $k_1 = \gcd(2i,n)$.*

Proof. Note that

$$\begin{aligned}
& \mathrm{Tr}\left(\frac{\alpha+\alpha^{2^i}(\alpha^{2^i+1}+\beta)}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)+\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)\\
= & \mathrm{Tr}\left(\frac{\alpha+\alpha^{2^{i+1}+1}+\beta\alpha^{2^i}+\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)\\
= & \mathrm{Tr}\left(\frac{(\alpha^{2^i}+1)^2+(\alpha^{2^i}+1)(\beta+(\alpha+1)^{2^i+1})}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)\\
= & \mathrm{Tr}\left(\frac{\alpha^{2^i}+1}{\beta+(\alpha+1)^{2^i+1}}+(\frac{\alpha^{2^i}+1}{\beta+(\alpha+1)^{2^i+1}})^2\right)\\
= & 0,
\end{aligned}$$

then the condition

$$\mathrm{Tr}\left(\frac{\beta}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)=1 \tag{15}$$

is equivalent to

$$\mathrm{Tr}\left(\frac{\alpha+\alpha^{2^i}(\alpha^{2^i+1}+\beta)}{\beta^2+(\alpha^2+1)^{2^i+1}}\right)=1. \tag{16}$$

1. As in the proof of Theorem 3, determining the differential uniformity is equivalent to finding the number of solutions of the following system of linear equations:

$$\begin{cases} (a+\alpha b)x^{2^i}+(a+\alpha b)^{2^i}x+(\alpha^{2^i}a+\gamma b)y^{2^i}+(\alpha a^{2^i}+\gamma b^{2^i})y=0\\ (\gamma a+\alpha^{2^i}b)x^{2^i}+(\gamma a^{2^i}+\alpha b^{2^i})x+(\alpha a+b)y^{2^i}+(\alpha a+b)^{2^i}y=0, \end{cases}$$

where $(0,0)\neq(a,b)\in\mathbb{F}_{2^n}^2$ and $\gamma=\alpha^{2^i+1}+\beta$. We claim that the following matrix

$$\begin{pmatrix} a+\alpha b & \alpha^{2^i}a+\gamma b\\ \gamma a+\alpha^{2^i}b & \alpha a+b \end{pmatrix}$$

is always of full rank. Otherwise, the determinant of the above matrix equals 0, i.e.,

$$(\alpha+\alpha^{2^i}\gamma)a^2+(\beta+(\alpha+1)^{2^i+1})^2ab+(\alpha+\alpha^{2^i}\gamma)b^2=0.$$

Suppose $b=0$. From equality (16), we get that $\alpha+\alpha^{2^i}\gamma\neq 0$. Hence we have $a=0$ from the equation above. This contradicts $(a,b)\neq(0,0)$. Thus $b\neq 0$, we divide both sides of the equation above by b^2 and get

$$(\alpha+\alpha^{2^i}\gamma)(a/b)^2+(\beta+(\alpha+1)^{2^i+1})^2(a/b)+(\alpha+\alpha^{2^i}\gamma)=0,$$

which cannot hold for any $a/b\in\mathbb{F}_{2^n}$ by hypothesis (16), a contradiction. Therefore, the differential uniformity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}(x,y)$ is at most 2^{2k} according to Lemma 3,.

2. As the proof of Theorem 4, calculating the nonlinearity is reduced to characterizing the number of the solutions to the following system of linear equations

$$\begin{cases} (a+b\gamma)^{2^i}u^{2^{2i}}+(a+b\gamma)u+(a\alpha^{2^i}+b\alpha)^{2^i}v^{2^{2i}}+(a\alpha+b\alpha^{2^i})v=0,\\ (a\alpha+b\alpha^{2^i})^{2^i}u^{2^{2i}}+(a\alpha^{2^i}+b\alpha)u+(a\gamma+b)^{2^i}v^{2^{2i}}+(a\gamma+b)v=0, \end{cases}$$

where $(0,0)\neq(a,b)\in\mathbb{F}_{2^n}^2$ and $\gamma=\alpha^{2^i+1}+\beta$. Similarly, we claim that the matrix below

$$\begin{pmatrix} a+b\gamma & a\alpha+b\alpha^{2^i}\\ a\alpha^{2^i}+b\alpha & a\gamma+b \end{pmatrix}$$

is always of full rank. Otherwise, the determinant of the above matrix equals 0, i.e.,

$$\beta a^2 + (\beta + (\alpha+1)^{2^i+1})^2 ab + \beta b^2 = 0.$$

If $b = 0$, then the above equation have non-trivial solutions if and only if $\beta = 0$. However, $\beta \neq 0$ according to the equality (15). Then we have $b \neq 0$ and divide both sides of the above equation by b^2, it follows that

$$\beta (a/b)^2 + (\beta + (\alpha+1)^{2^i+1})^2 (a/b) + \beta = 0.$$

which has no solutions in $\mathbb{F}_{2^n}$ by equality (15), a contradiction. From Lemma 3, the system of equations have at most 2^{2k_1} solutions in $\mathbb{F}_{2^n}^2$, where $k_1 = \gcd(2i, n)$. Thus, the nonlinearity of $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ is at least $2^{2n-1} - 2^{n+k_1-1}$. □

Remark 2. According to the theorem above, we can get differentially 4-uniform functions $\mathsf{V}_{\alpha,\beta}^{2^i+1}$ over $\mathbb{F}_{2^n}^2$ for any even n with $\gcd(i, n) = 1$. However, the permutation $\mathsf{H}_{\alpha,\beta}^{2^i+1}$ does not exist in this case since x^{2^i+1} is not a permutation over $\mathbb{F}_{2^n}$ when n is even. So, we cannot get a differentially 4-uniform permutation by this means.

6 Conclusion

In the present paper, we give a more general construction based on butterfly structure, which covers the three previous constructions as special cases. Our construction can generate more new permutations over $\mathbb{F}_{2^{2m+1}}^2$ with differential uniformity 4, the best known nonlinearity, and algebraic degree $2m + 1$ or $2m + 2$. We also give a complete characterization of the number of solutions to a special system of linear equations, and this characterization is useful for investigating the cryptographic properties of quadratic functions obtained with the butterfly construction based on Gold exponents.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions, which have greatly improved the paper. This work was supported by the National Science Foundation of China (No. 61772517, 61772516, 61502113), Youth Innovation Promotion Association CAS, and the Guangdong Provincial NSF (Grant No. 2015A030310174).

References

[BDKM09] K Browning, JF Dillon, RE Kibler, and MT McQuistan. APN polynomials and related codes. *J. Comb. Inf. Syst. Sci*, 34(1-4):135–159, 2009.

[BDMW10] KA Browning, JF Dillon, MT McQuistan, and AJ Wolfe. An APN permutation in dimension six. *Finite Fields: theory and applications- FQ9, ser. Contemporary Mathematics*, 518:33–42, 2010.

[Blu04] Antonia W Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications*, 10(3):285 – 305, 2004.

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

[CDP17] A. Canteaut, S. Duval, and L. 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 Transactions on Information Theory*, 63(11):7575–7591, Nov 2017.

[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}). *Appl. Algebra Eng. Commun. Comput.*, 9(2):139–152, 1998.

[FFW17] Shihui Fu, Xiutao Feng, and Baofeng Wu. Differentially 4-uniform permutations with the best known nonlinearity from butterflies. *IACR Trans. Symmetric Cryptol.*, 2017(2):228–249, 2017.

[Hou06] Xiang-dong Hou. Affinity of permutations of $\mathbb{F}_{2^n}$. *Discrete Applied Mathematics*, 154(2):313–325, 2006.

[KS12] Gohar M. M. Kyureghyan and Valentin Suder. On inverses of APN exponents. In *Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012, Cambridge, MA, USA, July 1-6, 2012*, pages 1207–1211, 2012.

[LW14] 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.

[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.

[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.

[YWL14] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography*, 73(2):587–600, 2014.