Designs, Codes and Cryptography (2021) 89:737–761
https://doi.org/10.1007/s10623-020-00837-5

Cryptographically strong permutations from the butterfly structure

Kangquan Li[1] · Chunlei Li[2] · Tor Helleseth[2] · Longjiang Qu[1,3]

Received: 22 June 2020 / Revised: 15 December 2020 / Accepted: 19 December 2020 /
Published online: 5 February 2021

Abstract

Boomerang connectivity table is a new tool to characterize the vulnerability of cryptographic functions against boomerang attacks. Consequently, a cryptographic function is desired to have boomerang uniformity as low as its differential uniformity. Based on generalized butterfly structures recently introduced by Canteaut, Duval and Perrin, this paper presents infinite families of permutations of $\mathbb{F}_{2^{2n}}$ for a positive odd integer n, which have the best known nonlinearity and boomerang uniformity 4. Both open and closed butterfly structures are considered. The open butterflies, according to experimental results, appear not to produce permutations with boomerang uniformity 4. On the other hand, from the closed butterflies we derive a condition on coefficients $\alpha, \beta \in \mathbb{F}_{2^n}$ such that the functions

$$V_i(x, y) := (R_i(x, y), R_i(y, x)),$$

where $R_i(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ and $\gcd(i, n) = 1$, permute $\mathbb{F}_{2^n}^2$ and have boomerang uniformity 4. In addition, experimental results for $n = 3, 5$ indicate that the proposed condition seems to cover all such permutations $V_i(x, y)$ with boomerang uniformity 4.

Keywords Permutations · Nonlinearity · Differential uniformity · Boomerang uniformity · Butterfly structure

Mathematics Subject Classification 94C10 · 94A60 · 06E30 · 14G50

Communicated by G. Kyureghyan.

The work of Longjiang Qu was supported by the Nature Science Foundation of China (NSFC) under Grants 61722213, 62032009, National Key R&D Program of China (No.2017YFB0802000), and the Open Foundation of State Key Laboratory of Cryptology. The work of Tor Helleseth and Chunlei Li was supported by the Research Council of Norway (No. 247742/O70 and No. 311646/O70). The work of Chunlei Li was also supported in part by the National Natural Science Foundation of China under Grant (No. 61771021). The work of Kangquan Li was supported by China Scholarship Council.

Extended author information available on the last page of the article

1 Introduction

Substitution boxes, known as S-boxes for short, are crucial nonlinear building blocks in modern block ciphers. In accordance with known attacks in the literature, S-boxes used in block ciphers are required to satisfy various cryptographic criteria, including high nonlinearity [6], low differential uniformity [17] and bijectivity. In Eurocrypt'18, Cid, Huang, Peyrin, Sasaki and Song [7] introduced a new tool of S-boxes, so-called the boomerang connectivity table (BCT), which analyzes the dependency between the upper part and lower part of a block cipher in a boomerang attack. This new tool quickly attracted researchers' interest in studying properties and bounds of BCT of cryptographic functions. Boura and Canteaut in [1] investigated the relation between entries in BCT and the difference distribution table (DDT), and introduced the notion of the boomerang uniformity, which is the maximum value in BCT among all nonzero differences of inputs and outputs. They completely characterized the BCTs of 4-bit S-boxes with differential uniformity 4 classified in [10], and also determined the boomerang uniformities of the inverse function and the Gold function. Later, Li, Qu, Sun and Li in [12] provided an equivalent formula to compute the boomerang uniformity of a cryptographic function. Using the new formula, they characterized the boomerang uniformity by means of the Walsh transform, and computed the boomerang uniformities of some permutations with low differential uniformity. Mesnager, Tang and Xiong considered the boomerang uniformity of quadratic permutations in [16], where they presented a characterization of quadratic permutations with boomerang uniformity 4 and showed that the boomerang uniformity of certain quadratic permutations is preserved under extended affine (EA) equivalence. Recently, Calderini and Villa [3] also investigated the boomerang uniformities of some non-quadratic permutations with differential uniformity 4. Very recently, Tian, Boura and Perrin [20] studied the boomerang uniformity of some popular constructions used for building large S-boxes, e.g. for eight variables from smaller ones.

It is shown that the boomerang uniformity of a cryptographic function is greater than or equal to its differential uniformity, and that the lowest possible boomerang uniformity 2 is achieved by almost perfect nonlinear (APN) functions [1,7]. Clearly, APN permutations operating on even number of variables are most interesting. The problem of existence of APN permutations of $\mathbb{F}_{2^{2n}}$ is referred to as the *BIG APN* problem in the community. Nonetheless, by far no other instance for this problem, except for the Dillon APN permutation of $\mathbb{F}_{2^6}$, has been found. Hence it is of great interest to construct permutations of $\mathbb{F}_{2^{2n}}$ that have high nonlinearity, differential and boomerang uniformity 4. Up to now, there are only three infinite and inequivalent families of permutations over $\mathbb{F}_{2^{2n}}$ that have boomerang uniformity 4 for odd integers $n \geq 1$:

(1) $f(x) = x^{-1}$ over $\mathbb{F}_{2^{2n}}$ [1];
(2) $f(x) = x^{2^{2i}+1}$ over $\mathbb{F}_{2^n}$, where $\gcd(i, n) = 1$ [1];
(3) $f(x) = \alpha x^{2^{2s}+1} + \alpha^{2^{2k}} x^{2^{-2k}+2^{2k+2s}}$ over $\mathbb{F}_{2^{2n}}$, where $n = 3k$, $3 \nmid k$, $3 \mid (k+s)$, $\gcd(3k, s) = 1$, and α is a primitive element of $\mathbb{F}_{2^{2n}}$ [16].

In Crypto'16, Perrin, Udovenko and Biryukov [19] investigated the only APN permutation over $\mathbb{F}_{2^6}$ [2] by means of reverse-engineering and proposed the open butterfly and the closed butterfly structures. A generalized butterfly structure was later proposed in [4]. The butterfly structures represent functions over $\mathbb{F}_{2^n}^2$ in terms of bivariate form. It is shown that the open butterfly structure produces permutations of $\mathbb{F}_{2^n}^2$, which are CCZ-equivalent to the functions that are derived from the closed structure and are in simpler forms [19]. Since differential uniformity is an invariant under CCZ-equivalence, one may consider to combine open and closed butterfly structures to construct permutations with low differential uniformity. As a matter of fact, by investigating differential uniformity of functions from the closed butterfly structure, researchers constructed several infinite families of differentially 4-uniform permutations over $\mathbb{F}_{2^n}^2$ with the open butterfly structure [4,5,8,14].

Motivated by recent works on the butterfly structure, this paper aims to construct infinite families of permutations with boomerang uniformity 4 from generalized butterfly structures. The main result of this paper is given as follows.

Theorem 1 *Let* $q = 2^n$ *with* n *odd,* $\gcd(i, n) = 1$ *and* $R_i(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ *with* $\alpha, \beta \in \mathbb{F}_q^*$*, where* $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$*. Then the function*

$$V_i(x, y) := (R_i(x, y), R_i(y, x))$$

from the closed butterfly structure permutes $\mathbb{F}_q^2$ *and has boomerang uniformity* 4 *if* (α, β) *is taken from the following set*

$$\Gamma = \left\{(\alpha, \beta) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : \ \varphi_2^{2^i} = \varphi_1 \varphi_3^{2^i-1} \text{ and } \varphi_3 \neq 0\right\}, \tag{1}$$

where $\varphi_1, \varphi_2, \varphi_3$ *are given by*

$$\begin{cases} \varphi_1 = (\alpha + 1)^{2^{i+1}+2} + \alpha^{2^i+2} + \alpha^{2^i} + \alpha\beta + \beta^2 \\ \varphi_2 = (\alpha + 1)^{2^{i+1}+2} + \alpha^{2^{i+1}+1} + \alpha + \alpha^{2^i}\beta + \beta^2 \\ \varphi_3 = (\alpha + 1)^{2^{i+1}+2} + \beta^2. \end{cases} \tag{2}$$

For the statement in Theorem 1, we will compute the boomerang uniformity by directly investigating the bivariate form $V_i(x, y)$, and prove the permutation property of $V_i(x, y)$ by examining its univariate polynomial representation over $\mathbb{F}_{q^2}$.

The rest of this paper is organized as follows. Section 2 firstly recalls the definitions of differential uniformity, boomerang uniformity, butterfly structure and introduces some auxiliary results. Sections 3 and 4 are devoted to proving the permutation property and the boomerang uniformity in Theorem 1, respectively. Finally, Sect. 5 draws a conclusion of our work.

2 Preliminaries

In this section, we assume n is an arbitrary positive integer and $q = 2^n$. Let $\mathrm{Tr}_q(\cdot)$ denote the absolute trace function over $\mathbb{F}_q$, i.e., $\mathrm{Tr}_q(x) = x + x^2 + \cdots + x^{2^{n-1}}$ for any $x \in \mathbb{F}_q$. For any set E, the nonzero elements of E is denoted by $E\backslash\{0\}$ or E^*.

2.1 Differential uniformity and Boomerang uniformity

The concept of differential uniformity was introduced to reveal the subtleties of differential attacks.

Definition 2 [17] Let $f(x)$ be a function from $\mathbb{F}_q$ to itself and $a, b \in \mathbb{F}_q$. The difference distribution table (DDT) of $f(x)$ is given by a $q \times q$ table D, in which the entry for the (a, b) position is given by

$$DDT(a, b) = \#\{x \in \mathbb{F}_q : \ f(x + a) + f(x) = b\}.$$

The differential uniformity of $f(x)$ is given by

$$\Delta_f = \max_{a\in\mathbb{F}_q^*, b\in\mathbb{F}_q} DDT(a,b).$$

It is straightforward for any function from $\mathbb{F}_q$ to itself, each entry in its DDT takes an even value and its differential uniformity is no less than 2. A function with the minimum possible differential uniformity 2 is called an almost perfect nonlinear (APN) function.

The concept of boomerang connectivity table of a permutation f from $\mathbb{F}_2^n$ to itself was introduced in [7], which clearly is also suitable for the case $\mathbb{F}_{2^n}$. Later, Boura and Canteaut introduced the concept of the boomerang uniformity, which is defined by the maximum value in BCT excluding the first row and column.

Definition 3 [1,7] Let f be an invertible function from $\mathbb{F}_q$ to itself and $a, b \in \mathbb{F}_q$. The boomerang connectivity table (BCT) of f is given by a $q \times q$ table, in which the entry for the (a, b) position is given by

$$BCT(a,b) = \#\left\{x \in \mathbb{F}_q : \ f^{-1}(f(x)+b) + f^{-1}(f(x+a)+b) = a\right\}. \tag{3}$$

The boomerang uniformity of f is defined by

$$\delta_f = \max_{a,b\in\mathbb{F}_q^*} BCT(a,b).$$

It is shown in [1,7] that $BCT(a,b) \geq DDT(a,b)$ for any a, b in $\mathbb{F}_q$. In [12], Li et al. presented an equivalent formula to compute BCT and the boomerang uniformity without knowing $f^{-1}(x)$ and $f(x)$ simultaneously as follows.

Proposition 4 [12] *Let $q = 2^n$ and $f(x) \in \mathbb{F}_q[x]$ be a permutation polynomial over $\mathbb{F}_q$. Then the BCT of $f(x)$ can be given by a $q \times q$ table BCT, in which the entry $BCT(a,b)$ for the (a,b) position is given by the number of solutions (x, y) in $\mathbb{F}_q \times \mathbb{F}_q$ of the following equation system.*

$$\begin{cases} f(x+a) + f(y+a) = b, \\ f(x) + f(y) = b. \end{cases} \tag{4}$$

Equivalently, the boomerang uniformity of $f(x)$, given by δ_f, is the maximum number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of (4) as a, b run through $\mathbb{F}_q^*$.

Let f be a quadratic function from $\mathbb{F}_q$ to itself with $f(0) = 0$. The associated symmetric bilinear mapping is given by $S_f(x, y) = f(x+y) + f(x) + f(y)$, where $x,\ y \in \mathbb{F}_q$. For any $a \in \mathbb{F}_q$, define

$$\mathrm{Im}_{f,a} = \{S_f(a,x) : x \in \mathbb{F}_q\}.$$

Very recently, Mesnager et al. [16] presented a characterization about quadratic permutations with boomerang uniformity 4 using the new formula (4).

Lemma 5 [16] *Let $q = 2^n$ and f be a quadratic permutation of $\mathbb{F}_q$ with differential uniformity 4. Then the boomerang uniformity of f equals 4 if and only if $\mathrm{Im}_{f,a} = \mathrm{Im}_{f,b}$ for any $a, b \in \mathbb{F}_q^*$ satisfying $S_f(a,b) = 0$.*

2.2 The butterfly structure

In Crypto'16, Perrin, Udovenko and Biryukov [19] analyzed the only known APN permutation over $\mathbb{F}_{2^6}$ [2] and discovered that the APN permutation over $\mathbb{F}_{2^6}$ has a simple decomposition relying on x^3 over $\mathbb{F}_{2^3}$. Based on the power permutation x^e over $\mathbb{F}_{2^n}$, they presented the open butterfly structure and the closed butterfly structure, which were later generalized in [4].

Definition 6 [19] Let $q = 2^n$ and $\alpha \in \mathbb{F}_q$, e be an integer such that x^e is a permutation over $\mathbb{F}_q$ and $R_k[e, \alpha]$ be the keyed permutation

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

The following functions

$$H_e^{\alpha}(x, y) = \left(R^{-1}_{R_y[e,\alpha](x)}(y), R_y[e, \alpha](x)\right),$$
$$V_e^{\alpha}(x, y) = \left(R_y[e, \alpha](x), R_x[e, \alpha](y)\right)$$

are called the open butterfly structure and closed butterfly structure respectively.

Definition 7 [4] Let $q = 2^n$ and $R(x, y)$ be a bivariate polynomial of $\mathbb{F}_q$ such that $R_y : x \to R(x, y)$ is a permutation of $\mathbb{F}_q$ for all y in $\mathbb{F}_q$. The closed butterfly V_R is the function of $\mathbb{F}_q^2$ defined by

$$V_R(x, y) = (R(x, y), R(y, x)),$$

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

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

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

Define a bivariate polynomial

$$R_i(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}, \quad \gcd(i, n) = 1, \ \alpha, \beta \in \mathbb{F}_q.$$

Since n is odd, it is clear that the mapping $x \mapsto R_i(x, y)$ is a permutation of $\mathbb{F}_q$ for any fixed $y \in \mathbb{F}_q$. According to experimental results, the permutation $H_{R_i}(x, y)$ from $R_i(x, y)$ and the open butterfly structure seems not to have boomerang uniformity 4 of $\mathbb{F}_{2^3}^2$. Hence this paper concentrates on the closed butterfly structure.

Lemma 8 [14] *Let n be odd, $q = 2^n$, i be an integer with* $\gcd(i, n) = 1$, $\alpha, \beta \in \mathbb{F}_q^*$ *and* $\beta \neq (\alpha + 1)^{2^i+1}$. *Then the function*

$$V_i := (R_i(x, y), R_i(y, x)) \text{ with } R_i(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$$

has differential uniformity at most 4.

Recall that the boomerang uniformity of a function is no less than its differential uniformity. The result about $V_i(x, y)$ in Lemma 8 motivates our study on the coefficients α, β in $\mathbb{F}_q^*$ that can further result in permutations $V_i(x, y)$ with boomerang uniformity 4.

2.3 Useful Lemmas

This subsection summarizes some lemmas that will be used for proving the permutation property of the function in Theorem 1.

Lemma 9 [18,21,22] *Pick $d, r > 0$ with $d \mid (q-1)$, and let $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h\left(x^{(q-1)/d}\right)$ permutes $\mathbb{F}_q$ if and only if both*

(1) $\gcd(r, (q-1)/d) = 1$ *and*
(2) $g(x) = x^r h(x)^{(q-1)/d}$ *permutes μ_d, where $\mu_d := \{x \in \mathbb{F}_q : x^d = 1\}$.*

Let the unit circle of $\mathbb{F}_{q^2}$ be defined by

$$\mu_{q+1} := \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}.$$

The unit circle of $\mathbb{F}_{q^2}$ has the following relation with the finite field $\mathbb{F}_q$.

Lemma 10 [9] *Let γ be any fixed element in $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then we have*

$$\mu_{q+1} \backslash \{1\} = \left\{ \frac{x+\gamma}{x+\gamma^q} : x \in \mathbb{F}_q \right\}.$$

The following lemma is about the solutions of a linear equation. The proof is easy and we omit it.

Lemma 11 *Let $q = 2^n$ and $\gcd(i, n) = 1$. Then for any $a \in \mathbb{F}_q$, the equation $x^{2^i} + x = a$ has solutions in $\mathbb{F}_q$ if and only if $\mathrm{Tr}_q(a) = 0$. Moreover, when $\mathrm{Tr}_q(a) = 0$, the equation $x^{2^i} + x = a$ has exactly two solutions $x = x_0, x_0 + 1$ in $\mathbb{F}_q$.*

Lemma 12 [15] *Let $\mathbb{R}$ be a commutative ring with identity. The Dickson polynomial $D_k(x, a)$ of the first kind of degree k*

$$D_k(x, a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}$$

has the following properties:

(1) $D_k(x_1 + x_2, x_1 x_2) = x_1^k + x_2^k$, *where x_1, x_2 are two indeterminates;*
(2) $D_{k+2}(x, a) = x D_{k+1}(x, a) - a D_k(x, a)$;
(3) $D_{k\ell}(x, a) = D_k\left(D_\ell(x, a), a^\ell\right)$;
(4) *if $\mathbb{R} = \mathbb{F}_{2^n}$, then $D_{2^i}(x, a) = x^{2^i}$.*

By the above lemma, the Dickson polynomial of degree $k = 2^i - 1$ over $\mathbb{F}_{2^n}$ can be explicitly given.

Lemma 13 *For any positive integer i and element $a \in \mathbb{F}_{2^n}$,*

$$D_{2^i-1}(x, a) = \sum_{j=0}^{i-1} a^{2^j-1} x^{2^i-2^{j+1}+1}. \qquad (5)$$

Proof We prove the statement by induction. It is clear that (5) holds for $i = 1$ since $D_1(x,a) = x$. Suppose that (5) holds for $i-1$, namely,

$$D_{2^{i-1}-1}(x,a) = \sum_{j=0}^{i-2} a^{2^j-1} x^{2^{i-1}-2^{j+1}+1}. \tag{6}$$

By Lemma 12 (3) and (4), we have

$$\begin{aligned} D_{2^i-2}(x,a) &= D_{2^{i-1}-1}\left(D_2(x,a), a^2\right) \\ &= D_{2^{i-1}-1}\left(x^2, a^2\right) \\ &= \sum_{j=0}^{i-2} a^{2(2^j-1)} x^{2(2^{i-1}-2^{j+1}+1)} \\ &= \sum_{j=1}^{i-1} a^{2^j-2} x^{2^i-2^{j+1}+2}. \end{aligned}$$

In addition, according to Lemma 12 (2),

$$D_{2^i}(x,a) = xD_{2^i-1}(x,a) + aD_{2^i-2}(x,a).$$

Thus,

$$\begin{aligned} D_{2^i-1}(x,a) &= x^{-1}\left(x^{2^i} + aD_{2^i-2}(x,a)\right) \\ &= x^{-1}\left(x^{2^i} + a\sum_{j=1}^{i-1} a^{2^j-2} x^{2^i-2^{j+1}+2}\right) \\ &= \sum_{j=0}^{i-1} a^{2^j-1} x^{2^i-2^{j+1}+1}, \end{aligned}$$

which implies that (5) holds for the i case. Therefore, the desired conclusion follows. □

Let γ be a primitive element of $\mathbb{F}_{2^2}$, i.e, $\gamma^2 = \gamma + 1$. Let n be a positive odd integer and $q = 2^n$. The finite field $\mathbb{F}_{q^2} = \mathbb{F}_q(\gamma)$ and the basis $1, \gamma$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ induces a one-to-one correspondence between $\mathbb{F}_q^2$ and $\mathbb{F}_{q^2}$ as follows:

$$z = x + \gamma y \leftrightarrow (x, y) = (\gamma^2 z + \gamma z^q, z^q + z).$$

According to the one-to-one correspondence between $\mathbb{F}_q^2$ and $\mathbb{F}_{q^2}$, the closed butterfly structure $V_i(x,y) = (R_i(x,y), R_i(y,x))$ over $\mathbb{F}_q^2$ can be expressed in a univariate $z = x+\gamma y$ as

$$V_i(z) := R_i(x,y) + \gamma R_i(y,x) \text{ with } x = \gamma^2 z + \gamma z^q,\ y = z^q + z.$$

By substituting z with γz when i is odd (resp. $\gamma^2 z$ when i is even), the above univariate polynomial can be transformed into

$$f_i(z) = \epsilon_1 z^{q\cdot(2^i+1)} + \epsilon_2 z^{q\cdot 2^i+1} + \epsilon_3 z^{2^i+q} + \epsilon_4 z^{2^i+1}, \tag{7}$$

where the coefficients

$$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) = \begin{cases} (\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4), & \text{for even } i \\ (\varepsilon_3, \varepsilon_4, \varepsilon_1, \varepsilon_2), & \text{for odd } i, \end{cases} \tag{8}$$

with

$$\begin{cases} \varepsilon_1 = \alpha^{2^i} + \alpha + 1 \\ \varepsilon_2 = \alpha^{2^i+1} + \alpha + \beta + 1 \\ \varepsilon_3 = \alpha^{2^i+1} + \alpha^{2^i} + \beta + 1 \\ \varepsilon_4 = \alpha^{2^i+1} + \alpha^{2^i} + \alpha + \beta. \end{cases} \tag{9}$$

Further, we define

$$\begin{cases} \varphi_1 = \epsilon_1\epsilon_3 + \epsilon_2\epsilon_4 \\ \varphi_2 = \epsilon_1\epsilon_2 + \epsilon_3\epsilon_4 \\ \varphi_3 = \epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2 + \epsilon_4^2 \\ \varphi_4 = \epsilon_1^2 + \epsilon_4^2. \end{cases} \tag{10}$$

It's easy to check that φ_i's, $i = 1, 2, 3$, match the ones defined in (2).

At the end of this section, we provide a lemma about some properties of the elements φ_i's which are characterized in Theorem 1.

This result will be heavily used in the proof of the main theorem.

Lemma 14 *Let $q = 2^n$ with n odd and $\gcd(i, n) = 1$. Let $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ be defined by (10) satisfying $\varphi_2^{2^i} = \varphi_1\varphi_3^{2^i-1}$ and $\varphi_3 \neq 0$. For $\alpha,\ \beta\ \in \mathbb{F}_q^*$, they have the following properties:*

(1) $(\varphi_1 + \varphi_3)(\varphi_2 + \varphi_3)(\varphi_3 + \varphi_4)\varphi_4 \neq 0$ and $\left(\frac{\varphi_3}{\varphi_2+\varphi_3}\right)^{2^i} = \frac{\varphi_3}{\varphi_1+\varphi_3}$;

(2) when i is even, $\mathrm{Tr}_q\left(\frac{\varphi_4}{\varphi_3}\right) = 1$; moreover, the equation

$$x^{2^i} + x + \frac{\varphi_3 + \varphi_4}{\varphi_3} = 0$$

has two solutions $\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha$ and $\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha + 1$ in $\mathbb{F}_q$;

(3) when i is odd, $\mathrm{Tr}_q\left(\frac{\varphi_4}{\varphi_3}\right) = 0$;

(4) $\mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right) = 0$.

Proof Since

$$\begin{cases} \varphi_1 = \alpha^{2^{i+1}+2} + \alpha^{2^{i+1}} + \alpha^{2^i+2} + \alpha^{2^i} + \alpha^2 + \alpha\beta + \beta^2 + 1 \\ \varphi_2 = \alpha^{2^{i+1}+2} + \alpha^{2^{i+1}+1} + \alpha^{2^{i+1}} + \alpha^2 + \alpha + \alpha^{2^i}\beta + \beta^2 + 1 \\ \varphi_3 = \alpha^{2^{i+1}+2} + \alpha^{2^{i+1}} + \alpha^2 + \beta^2 + 1 \end{cases} \tag{11}$$

and

$$\varphi_4 = \begin{cases} \alpha^{2^{i+1}+2} + \beta^2 + 1 & \text{for even } i \\ \alpha^{2^{i+1}} + \alpha^2 & \text{for odd } i, \end{cases} \tag{12}$$

it is clear that

$$\varphi_1 + \varphi_2 = \alpha^{2^i+2} + \alpha^{2^i} + \alpha\beta + \alpha^{2^{i+1}+1} + \alpha^{2^i}\beta + \alpha = (\alpha^{2^i} + \alpha)(\alpha^{2^i+1} + \beta + 1) \tag{13}$$

and

$$\left\{\varphi_4, \varphi_3 + \varphi_4\right\} = \left\{(\alpha^{2^i} + \alpha)^2, (\alpha^{2^i+1} + \beta + 1)^2\right\}. \tag{14}$$

(1) It follows from (13) and (14) that

$$\varphi_4(\varphi_3+\varphi_4)=(\varphi_1+\varphi_2)^2=(\alpha^{2^i}+\alpha)^2(\alpha^{2^i+1}+\beta+1)^2.$$

By the equality $\varphi_2^{2^i}=\varphi_1\varphi_3^{2^i-1}$, if either $\varphi_4(\varphi_3+\varphi_4)=0$ or $(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)=0$, then $\varphi_1+\varphi_2=0$ and $\varphi_1=\varphi_2=\varphi_3$. The equation $\varphi_1+\varphi_2=(\alpha^{2^i}+\alpha)(\alpha^{2^i+1}+\beta+1)=0$ implies $\beta=\alpha^{2^i+1}+1$ or $\alpha^{2^i}+\alpha=0$. In fact, if $\beta=\alpha^{2^i+1}+1$, then $\varphi_1+\varphi_3=\alpha^{2^i+2}+\alpha^{2^i}+\alpha\beta=\alpha^{2^i}+\alpha=0$. Thus we always have $\alpha^{2^i}+\alpha=0$, equivalently $\alpha=0,1$. This implies $\varphi_1+\varphi_3=\alpha^{2^i+2}+\alpha^{2^i}+\alpha\beta=\alpha\beta=0$, which is in contradiction with the assumption $\alpha\beta\neq 0$.

In addition, it is clear that the equality $\varphi_2^{2^i}=\varphi_1\varphi_3^{2^i-1}$ implies

$$\left(\frac{\varphi_3}{\varphi_2+\varphi_3}\right)^{2^i}=\frac{\varphi_3}{\varphi_1+\varphi_3}.$$

(2) From (11) and (12), we have

$$\begin{cases}\varphi_1+\varphi_3=\alpha^{2^i+2}+\alpha^{2^i}+\alpha\beta & \text{(15.1a)}\\ \varphi_2+\varphi_3=\alpha^{2^{i+1}+1}+\alpha^{2^i}\beta+\alpha & \text{(15.1b)}\\ \varphi_3+\varphi_4=\alpha^{2^{i+1}}+\alpha^2. & \text{(15.1c)}\end{cases}$$

It is easy to verify that

$$\alpha\,(\varphi_2+\varphi_3)+\alpha^{2^i}\,(\varphi_1+\varphi_3)=\varphi_3+\varphi_4. \tag{16}$$

Moreover, using $\left(\frac{\varphi_3}{\varphi_2+\varphi_3}\right)^{2^i}=\frac{\varphi_3}{\varphi_1+\varphi_3}$, we have

$$\frac{\varphi_3+\varphi_4}{\varphi_3}=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\frac{\varphi_1+\varphi_3}{\varphi_3}\alpha^{2^i}=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^{2^i}. \tag{17}$$

Thus,

$$\mathrm{Tr}_q\left(\frac{\varphi_3+\varphi_4}{\varphi_3}\right)=\mathrm{Tr}_q\left(\frac{\varphi_4}{\varphi_3}\right)+\mathrm{Tr}_q(1)=0.$$

Furthermore, from Lemma 11, the solutions in $\mathbb{F}_q$ of $x^{2^i}+x=\frac{\varphi_3+\varphi_4}{\varphi_3}$ are $\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha$ and $\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+1$.

(3) From the expressions of φ_3,φ_4 in (11), (12), it is clear that the values of φ_4 for even i and odd i add up to φ_3. The fact that $\mathrm{Tr}_q(1)=1$ for odd integer n implies that the values of $\mathrm{Tr}_q\left(\frac{\varphi_4}{\varphi_3}\right)$ for even i and odd i add up to 1. The desired assertion directly follows from (2) of this lemma.

(4) From (13) and (14), it is easily seen that

$$\left(\frac{\varphi_1}{\varphi_3}\right)^2+\left(\frac{\varphi_2}{\varphi_3}\right)^2=\left(\frac{\varphi_4}{\varphi_3}\right)^2+\frac{\varphi_4}{\varphi_3}. \tag{18}$$

Plugging $\frac{\varphi_1}{\varphi_3}=\left(\frac{\varphi_2}{\varphi_3}\right)^{2^i}$ into Eq. (18), we get

$$\left(\frac{\varphi_2}{\varphi_3}\right)^{2^{i+1}}+\left(\frac{\varphi_2}{\varphi_3}\right)^2=\left(\frac{\varphi_4}{\varphi_3}\right)^2+\frac{\varphi_4}{\varphi_3}=\left(\frac{\varphi_3+\varphi_4}{\varphi_3}\right)^2+\frac{\varphi_3+\varphi_4}{\varphi_3}.$$

By the relation between φ_3 and φ_4 for even and odd i, it is clear that the expression on the right side of the above equation is independent of the parity of the integer i. W.L.O.G., we can assume that i is even, since the case i odd can be proved by just replacing φ_4 by $\varphi_3+\varphi_4$. Together with (17), we have

$$\left(\frac{\varphi_2}{\varphi_3}\right)^{2^{i+1}}+\left(\frac{\varphi_2}{\varphi_3}\right)^2=\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^2\right)^{2^i}+\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^2.$$

Therefore,

$$\left(\frac{\varphi_2}{\varphi_3}\right)^2=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^2$$

or

$$\left(\frac{\varphi_2}{\varphi_3}\right)^2=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^2+1. \tag{19}$$

If Eq. (19) holds, then

$$\left(1+\alpha^2\right)\left(\frac{\varphi_2}{\varphi_3}\right)^2+\alpha\left(\frac{\varphi_2}{\varphi_3}\right)+\alpha^2+\alpha+1=0. \tag{20}$$

If $\alpha=1$, it is easy to obtain that $\beta=1$ from the definition of Γ. Moreover, $\varphi_2=0$ and thus $\mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right)=0$. In the following, we assume that $\alpha\neq 1$. Then after multiplying Eq. (20) by $\frac{\alpha^2+1}{\alpha^2}$ and simplifying, we get

$$\left(\frac{\alpha^2+1}{\alpha}\cdot\frac{\varphi_2}{\varphi_3}\right)^2+\frac{\alpha^2+1}{\alpha}\cdot\frac{\varphi_2}{\varphi_3}=\left(\frac{\alpha^2+1}{\alpha}\right)^2+\frac{\alpha^2+1}{\alpha}$$

and thus

$$\frac{\varphi_2}{\varphi_3}=1\ \text{ or }\ \frac{\alpha^2+\alpha+1}{\alpha^2+1}.$$

It is clear that $\varphi_2+\varphi_3\neq 0$. By $\left(\frac{\varphi_3}{\varphi_2+\varphi_3}\right)^{2^i}=\frac{\varphi_3}{\varphi_1+\varphi_3}$, one has

$$\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\right)^{2^i-1}=\frac{\varphi_1+\varphi_3}{\varphi_3}\cdot\frac{\varphi_3}{\varphi_2+\varphi_3}=\frac{\varphi_1+\varphi_3}{\varphi_2+\varphi_3}=\frac{\alpha^{2^i+2}+\alpha^{2^i}+\alpha\beta}{\alpha^{2^{i+1}+1}+\alpha^{2^i}\beta+\alpha}=\frac{1}{\alpha^{2^i-1}}.$$

Since $\gcd(i,n)=1$, one has $\frac{\varphi_2+\varphi_3}{\varphi_3}=\frac{1}{\alpha}$ and $\frac{\varphi_2+\varphi_3}{\varphi_3}=\frac{1}{\alpha}+1\neq\frac{\alpha^2+\alpha+1}{\alpha^2+1}$.

Therefore, Eq. (19) does not hold and thus

$$\left(\frac{\varphi_2}{\varphi_3}\right)^2=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha+\left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right)^2, \tag{21}$$

which implies $\mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right)=0$. □

3 The permutation property of $V_i(x, y)$

In this section, we firstly give a general necessary and sufficient condition on the permutation property of the function V_i from the closed butterfly. Throughout what follows, we always assume n is an odd integer.

Recall that the univariate representation of V_i have the following form

$$f(x) = \epsilon_1 x^{q\cdot(2^i+1)} + \epsilon_2 x^{q\cdot 2^i+1} + \epsilon_3 x^{2^i+q} + \epsilon_4 x^{2^i+1}, \quad \epsilon_j \in \mathbb{F}_q. \tag{22}$$

Below we first present a necessary and sufficient conditions for $f(x)$ to be a permutation of $\mathbb{F}_{q^2}$ without imposing any additional restrictions on ϵ_j.

The following proposition investigates the permutation property of $f(x)$ defined by (22) over $\mathbb{F}_{q^2}$.

Proposition 15 *Let $q = 2^n$, $f(x)$ be defined by (22), $h(x) = \epsilon_1 x^{2^i+1} + \epsilon_2 x^{2^i} + \epsilon_3 x + \epsilon_4$ and $g(x) = x^{2^i+1}h(x)^{q-1}$. Define $\mu_{q+1} = \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}$ and*

$$T = \left\{ \left(\frac{xy+1}{x+y}, \frac{xy}{x^2+y^2} \right) \quad : \quad x, y \in \mu_{q+1}\backslash\{1\}, y \neq x, x^q \right\} \subset \mathbb{F}_q^2.$$

Then $f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if

(1) $\gcd\left(2^i+1, q-1\right) = 1$*;*
(2) $h(x) = 0$ *has no solution in* μ_{q+1}*;*
(3) $g(x) = 1$ *if and only if* $x = 1$*;*
(4) there does not exist some $(X, Y) \in T$ such that the following equation holds:

$$\varphi_1 X^{2^i} + \varphi_2 X + \varphi_3 \left(\sum_{j=0}^{i-1} Y^{2^j} \right) + \varphi_4 = 0, \tag{23}$$

where φ_j for $j = 1, 2, 3, 4$ are defined by (10).

Proof It is clear that $f(x) = x^{2^i+1}h\left(x^{q-1}\right)$. According to Lemma 9, $f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd\left(2^i+1, q-1\right) = 1$ and

$$g(x) = x^{2^i+1}h(x)^{q-1} = \frac{\epsilon_4 x^{2^i+1} + \epsilon_3 x^{2^i} + \epsilon_2 x + \epsilon_1}{\epsilon_1 x^{2^i+1} + \epsilon_2 x^{2^i} + \epsilon_3 x + \epsilon_4}$$

permutes μ_{q+1}, which obviously implies that $h(x) = 0$ has no solution in μ_{q+1} and $g(x) = 1$ if and only if $x = 1$. In the following, we assume that the conditions (1),(2) and (3) hold. Therefore, $g(x)$ permutes μ_{q+1} if and only if $g(x) + g(y) = 0$ has no solution for $x, y \in \mu_{q+1}\backslash\{1\}$ with $x \neq y$. In fact, if $g(x) + g(y) = 0$ for some $y = x^q$, then we have $g(x) = g(y) = g(x^q) = g(x)^q = g(x)^{-1}$ and thus $g(x) = 1$, which means that $x = 1$. Thus we can only consider the conditions such that $g(x) + g(y) = 0$ has no solution for $x, y \in \mu_{q+1}\backslash\{1\}$ with $y \neq x, x^q$. Next, we prove the necessity and sufficiency of the condition (4).

The sufficiency of (4). Suppose $g(x) + g(y) = 0$, i.e.,

$$\frac{\epsilon_4 x^{2^i+1} + \epsilon_3 x^{2^i} + \epsilon_2 x + \epsilon_1}{\epsilon_1 x^{2^i+1} + \epsilon_2 x^{2^i} + \epsilon_3 x + \epsilon_4} = \frac{\epsilon_4 y^{2^i+1} + \epsilon_3 y^{2^i} + \epsilon_2 y + \epsilon_1}{\epsilon_1 y^{2^i+1} + \epsilon_2 y^{2^i} + \epsilon_3 y + \epsilon_4}.$$

After a routine calculation, we obtain

$$\varphi_1(x+y)(xy+1)^{2^i}+\varphi_2(x+y)^{2^i}(xy+1)+\varphi_4(x+y)^{2^i+1}+\varphi_3\left(x^{2^i}y+xy^{2^i}\right)=0,$$

where φ_j's for $j=1,2,3,4$ are defined as in (10). By the previous discussion, we now only need to consider the case that $(x+y)(xy+1)\neq 0$. Therefore, the above equation is equivalent to

$$\varphi_1\left(\frac{xy+1}{x+y}\right)^{2^i}+\varphi_2\left(\frac{xy+1}{x+y}\right)+\varphi_4+\varphi_3\left(\frac{x^{2^i}y+xy^{2^i}}{(x+y)^{2^i+1}}\right)=0. \tag{24}$$

Note that

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

It follows from Lemma 12 (1) that the coefficient of φ_3 can be expressed in terms of Dickson polynomial as

$$\frac{x^{2^i}y+xy^{2^i}}{(x+y)^{2^i+1}}=D_{2^i+1}\left(1,\frac{xy}{(x+y)^2}\right)+1.$$

In addition, by Lemma 12 (2), (4) and Lemma 13,

$$D_{2^i+1}(x,a)=D_{2^i}(x,a)+aD_{2^i-1}(x,a)=x^{2^i}+\sum_{j=0}^{i-1}a^{2^j}x^{2^i-2^{j+1}+1}. \tag{25}$$

Denote $X=\frac{xy+1}{x+y}$ and $Y=\frac{xy}{(x+y)^2}$. Then the coefficient of φ_3 can be written as

$$D_{2^i+1}(1,Y)+1=1+\sum_{j=0}^{i-1}Y^{2^j}+1=\sum_{j=0}^{i-1}Y^{2^j}.$$

It is straightforward that $g(x)=g(y)$ can be rewritten as

$$\varphi_1X^{2^i}+\varphi_2X+\varphi_3\left(\sum_{j=0}^{i-1}Y^{2^j}\right)+\varphi_4=0. \tag{26}$$

Thus, if there exist some $x,y\in\mu_{q+1}$ with $y\neq x,x^q$ such that $g(x)+g(y)=0$ holds, there must exist some $(X,Y)\in T$ such that Eq. (26) holds. Thus if the condition (4) holds, $g(x)$ permutes μ_{q+1}.

The necessity of (4). On the contrary, if the condition (4) does not hold, which means that there exist some $(X,Y)\in T$ such that Eq. (26) holds, then there must exist some $x,y\in\mu_{q+1}\backslash\{1\}$ with $y\neq x,x^q$ such that $g(x)+g(y)=0$, which implies that $g(x)$ does not permute μ_{q+1}.

On combining the sufficiency and necessity, we have proved the desired conclusion. □

Proof of the permutation part in Theorem 1.

In the following, we will prove the permutation part in Theorem 1 by verifying the conditions in Proposition 15.

First of all, if $\alpha = 1$, it is easy to obtain that $\beta = 1$ from the definition of Γ. In this case, the function

$$f_i(x) = \begin{cases} x^{q\cdot(2^i+1)}, & \text{when } i \text{ is even} \\ x^{2^i+q}, & \text{when } i \text{ is odd,} \end{cases}$$

clearly permutes $\mathbb{F}_{q^2}$. In the following, we assume $\alpha \neq 1$ and will show the four items of Proposition 15.

(1) Since n is odd and $\gcd(i, n) = 1$, we have $\gcd(2^i + 1, 2^n - 1) = 1$ due to the fact $\gcd(2^i + 1, 2^n - 1) \mid \gcd(2^{2i} - 1, 2^n - 1) = 2^{\gcd(2i,n)} - 1 = 1$.

(2) Next we show that $h(x) = 0$ has no solution in $\mu_{q+1}\backslash\{1\}$ ($h(1) = \sqrt{\varphi_3} \neq 0$ according to the definition). Suppose that there exists some $x_0 \in \mu_{q+1}\backslash\{1\}$ satisfying

$$\epsilon_1 x_0^{2^i+1} + \epsilon_2 x_0^{2^i} + \epsilon_3 x_0 + \epsilon_4 = 0. \tag{27}$$

Raising Eq. (27) to the q-th power and re-arranging it according to $x_0^q = x_0^{-1}$, we obtain

$$\epsilon_4 x_0^{2^i+1} + \epsilon_3 x_0^{2^i} + \epsilon_2 x_0 + \epsilon_1 = 0. \tag{28}$$

Summing $\epsilon_4 \times$ (27) and $\epsilon_1 \times$ (28) gives

$$\varphi_1 x_0^{2^i} + \varphi_2 x_0 + \varphi_4 = 0. \tag{29}$$

Computing $\varphi_4 \times (29) + \varphi_1 \times (29)^q \times x_0^{2^i}$ yields

$$\varphi_1\varphi_2 x_0^{2^i-1} + \varphi_2\varphi_4 x_0 + \varphi_1^2 + \varphi_4^2 = 0. \tag{30}$$

Furthermore, by computing $(30) \times x_0 + (29) \times \varphi_2$, we obtain

$$\varphi_2\varphi_4 x_0^2 + \left(\varphi_1^2 + \varphi_2^2 + \varphi_4^2\right) x_0 + \varphi_2\varphi_4 = 0. \tag{31}$$

Note that in the above equation $\varphi_2\varphi_4 \neq 0$. Otherwise, we have $\varphi_1^2 + \varphi_2^2 = \varphi_4^2$. Recall that $\varphi_1^2 + \varphi_2^2 = \varphi_4(\varphi_3 + \varphi_4)$ from (13) and (14). Thus we obtain $\varphi_3\varphi_4 = 0$, which is in contradiction with $\varphi_3 \neq 0$ in the definition of Γ and $\varphi_4 \neq 0$ in Lemma 14 (1). Thus Eq. (31) becomes

$$x_0^2 + \frac{\varphi_1^2 + \varphi_2^2 + \varphi_4^2}{\varphi_2\varphi_4} x_0 + 1 = 0. \tag{32}$$

Note that

$$\mathrm{Tr}_q\left(\frac{\varphi_2\varphi_4}{\varphi_1^2 + \varphi_2^2 + \varphi_4^2}\right) = \mathrm{Tr}_q\left(\frac{\varphi_2\varphi_4}{\varphi_4\varphi_3}\right) = \mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right) = 0.$$

This implies that Eq. (32) has a solution $x_0 \in \mathbb{F}_q$, which contradicts $\mu_{q+1}\backslash\{1\}$. Therefore, $h(x) = 0$ has no solution in μ_{q+1}.

(3) If there exists some $x_0 \in \mu_{q+1}\backslash\{1\}$ such that $g(x_0) = 1$, then we have

$$(\epsilon_1 + \epsilon_4)\, x_0^{2^i+1} + (\epsilon_2 + \epsilon_3)\, x_0^{2^i} + (\epsilon_2 + \epsilon_3)\, x_0 + \epsilon_1 + \epsilon_4 = 0. \tag{33}$$

According to Lemma 10, we know that for any $x_0 \in \mu_{q+1}\backslash\{1\}$, there exists a unique element $y_0 \in \mathbb{F}_q$ such that $x_0 = \frac{y_0+\gamma}{y_0+\gamma^2}$, where $\gamma \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$. By plugging $x_0 = \frac{y_0+\gamma}{y_0+\gamma^2}$ into Eq. (33) and a routine rearrangement, we obtain

$$y_0^{2^i} + y_0 + \frac{\varepsilon_1 + \varepsilon_4}{\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4} = 0, \tag{34}$$

where $\varepsilon_1, \varepsilon_4$ are defined as in (9) satisfying that $\varepsilon_1+\varepsilon_4=\epsilon_1+\epsilon_4$ for even i and $\varepsilon_1+\varepsilon_4=\epsilon_2+\epsilon_3$ for odd i. In other words, $\varepsilon_1+\varepsilon_4$ corresponds to $\sqrt{\varphi_4}$ for even i and $\sqrt{\varphi_3+\varphi_4}$ for odd i. By Lemma 14 (2) and (3), we have

$$\mathrm{Tr}_q\left(\frac{\varepsilon_1+\varepsilon_4}{\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4}\right)=1.$$

This implies (34) has no solution in $\mathbb{F}_q$. Hence $g(x)=1$ if and only if $x=1$.

(4) Recall that $Y=\frac{xy}{x^2+y^2}$ for some $x, y\in\mu_{q+1}\backslash\{1\}$ with $x\neq y$. Note that $\frac{y}{x+y}\in\mathbb{F}_{q^2}\backslash\mathbb{F}_q$ is a solution to the equation $z^2+z+Y=0$. This implies $\mathrm{Tr}_q\,(Y)=1$. It is clear that Eq. (26) required in Proposition 15 is equivalent to

$$\sum_{j=0}^{i-1}Y^{2^j}=\frac{\varphi_1}{\varphi_3}X^{2^i}+\frac{\varphi_2}{\varphi_3}X+\frac{\varphi_4}{\varphi_3}=\left(\frac{\varphi_2}{\varphi_3}X\right)^{2^i}+\frac{\varphi_2}{\varphi_3}X+\frac{\varphi_4}{\varphi_3}.$$

By $\mathrm{Tr}_q(Y)=1$ we have

$$\mathrm{Tr}_q\left(\sum_{j=0}^{i-1}Y^{2^j}\right)=\begin{cases}0, & \text{when } i \text{ is even}\\ 1, & \text{when } i \text{ is odd,}\end{cases} \tag{35}$$

on the other hand, the expression on the right hand side satisfies

$$\mathrm{Tr}_q\left(\left(\frac{\varphi_2}{\varphi_3}X\right)^{2^i}+\frac{\varphi_2}{\varphi_3}X+\frac{\varphi_4}{\varphi_3}\right)=\begin{cases}1, & \text{when } i \text{ is even}\\ 0, & \text{when } i \text{ is odd,}\end{cases}$$

according to Lemma 14. It is clear that Eq. (26) does not hold for any $X, Y\in\mathbb{F}_q$.

Up to now, all the four items in Proposition 15 are confirmed. Hence the function $V_i(x, y)$ in Theorem 1 permutes $\mathbb{F}_q^2$.

4 The boomerang uniformity of $V_i(x, y)$

In this section, we will prove that the function

$$V_i:=(R_i(x, y), R_i(y, x))$$

with $R_i(x, y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$ has boomerang uniformity 4 when the pair (α, β) is taken from the set Γ as in given in Theorem 1. Here and hereafter, we assume that n is odd, $q=2^n$ and $(\alpha, \beta)\in\Gamma$.

First of all, the condition $\beta\neq(\alpha+1)^{2^i+1}$ in Lemma 8 corresponds to the condition $\varphi_3\neq 0$ in Γ. Hence the differential uniformity of V_i with $R_i(x, y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$ is at most 4 for any $(\alpha, \beta)\in\Gamma$. Furthermore, Canteaut, Perrin and Tian [5] showed that if V_i is APN then it operates on 6 bits. Therefore, the differential uniformity of V_i is equal to 4 in other cases. Since V_i in Theorem 1 permutes $\mathbb{F}_q^2$ and has differential uniformity 4, we can use Lemma 5 to show the boomerang uniformity of V_i. For any $(a, b)\in\mathbb{F}_q^2$, denote

$$S_{V_i,(a,b)}(x, y)=V_i(x+a, y+b)+V_i(x, y)+V_i(a, b)$$

and

$$\mathrm{Im}_{V_i,(a,b)}=\left\{S_{V_i,(a,b)}(x, y):\ (x, y)\in\mathbb{F}_q^2\right\}.$$

According to Lemma 5, we need to determine $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_q^2 \backslash \{(0,0)\}$ satisfying $S_{V_i,(a_1,b_1)}(a_2, b_2) = (0, 0)$, and then to prove that for any such pairs the equation $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$ holds.

4.1 The solutions of $S_{V_i,(a_1,b_1)}(a_2, b_2) = (0, 0)$

The solution of the equation $S_{V_i,(a_1,b_1)}(a_2, b_2) = (0, 0)$ is studied in the following proposition.

Proposition 16 *Let V_i be defined as in Theorem 1 with $(\alpha, \beta) \in \Gamma$ and φ_j's for $j = 1, 2, 3, 4$ be defined as in (10). Then the elements $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_q^2 \backslash \{(0, 0)\}$such that*

$$V_i(a_1 + a_2, b_1 + b_2) + V_i(a_1, b_1) + V_i(a_2, b_2) = (0, 0)$$

satisfy $(a_2, b_2) = X \cdot (a_1, b_1)$, where X is a 2×2 matrix taken from the following set

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha + 1 & \frac{\varphi_2+\varphi_3}{\varphi_3} \\ \frac{\varphi_2+\varphi_3}{\varphi_3} & \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha \end{bmatrix}, \begin{bmatrix} \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha & \frac{\varphi_2+\varphi_3}{\varphi_3} \\ \frac{\varphi_2+\varphi_3}{\varphi_3} & \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha + 1 \end{bmatrix} \right\}. \tag{36}$$

Proof Note that the equation

$$S_{V_i,(a_1,b_1)}(a_2, b_2) = V_i(a_1 + a_2, b_1 + b_2) + V_i(a_1, b_1) + V_i(a_2, b_2) = (0, 0)$$

can be rewritten as

$$\begin{cases} (a_1 + \alpha b_1)a_2^{2^i} + (a_1^{2^i} + \alpha^{2^i} b_1^{2^i})a_2 + (\alpha^{2^i} a_1 + (\alpha^{2^i+1} + \beta)b_1)b_2^{2^i} + (\alpha a_1^{2^i} + (\alpha^{2^i+1} + \beta)b_1^{2^i})b_2 = 0 & \text{(37.1a)} \\ ((\alpha^{2^i+1} + \beta)a_1 + \alpha^{2^i} b_1)a_2^{2^i} + ((\alpha^{2^i+1} + \beta)a_1^{2^i} + \alpha b_1^{2^i})a_2 + (\alpha a_1 + b_1)b_2^{2^i} + (\alpha^{2^i} a_1^{2^i} + b_1^{2^i})b_2 = 0. & \text{(37.1b)} \end{cases}$$

Let φ_j's for $j = 1, 2, 3, 4$ be defined as in (10). Eliminating the terms $a_2^{2^i}$ in the above equations by computing $(37.1a) \times \left(\left(\alpha^{2^i+1} + \beta\right) a_1 + \alpha^{2^i} b_1\right) + (37.1b) \times (a_1 + \alpha b_1)$, we obtain

$$\lambda_1 a_2 + \lambda_2 b_2^{2^i} + \lambda_3 b_2 = 0, \tag{38}$$

where the coefficients are given by

$$\begin{cases} \lambda_1 = (\varphi_1 + \varphi_3)\, a_1^{2^i} b_1 + (\varphi_2 + \varphi_3)\, a_1 b_1^{2^i} + (\varphi_3 + \varphi_4) b_1^{2^i+1} \\ \lambda_2 = (\varphi_2 + \varphi_3)\, a_1^2 + \varphi_3 a_1 b_1 + (\varphi_2 + \varphi_3)\, b_1^2 \\ \lambda_3 = (\varphi_1 + \varphi_3)\, a_1^{2^i+1} + \varphi_4 a_1 b_1^{2^i} + (\varphi_2 + \varphi_3)\, b_1^{2^i+1}, \end{cases}$$

$\varphi_1, \varphi_2, \varphi_3$ are defined as in (10) and φ_4 corresponds to the case that i is even. Hereafter, we assume φ_4 is restricted to the case of even i, i.e, $\varphi_4 = (\alpha^{2^i+1} + \beta + 1)^2$.

When $b_1 = 0$, we have $a_1 \neq 0$, $\lambda_1 = 0$, $\lambda_2 = (\varphi_2 + \varphi_3)\, a_1^2$ and $\lambda_3 = (\varphi_1 + \varphi_3)\, a_1^{2^i+1}$. Moreover, Eq. (38) becomes $\lambda_2 b_2^{2^i} = \lambda_3 b_2$. This together with Lemma 14 (1) implies

$$b_2 = 0 \text{ or } b_2 = \left(\frac{\varphi_1 + \varphi_3}{\varphi_2 + \varphi_3}\right)^{\frac{1}{2^i-1}} a_1 = \frac{\varphi_2 + \varphi_3}{\varphi_3} a_1.$$

Note that in the case of $b_1 = 0$, Eq. (37.1a) becomes

$$\left(\frac{a_2}{a_1}\right)^{2^i} + \frac{a_2}{a_1} = \left(\frac{\alpha b_2}{a_1}\right)^{2^i} + \frac{\alpha b_2}{a_1}.$$

Therefore, if $b_2 = 0$, then $a_2 = a_1$; if $b_2 = \frac{\varphi_2+\varphi_3}{\varphi_3}a_1$, then $a_2 = \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha a_1$ or $a_2 = \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha a_1 + a_1$.

When $b_1 \neq 0$, after eliminating the terms $b_2^{2^i}$ by computing (37.1) × $\left((\alpha^{2^i+1} + \beta)a_1^{2^i} + \alpha b_1^{2^i}\right)$ + (37.2) × $\left(a_1^{2^i} + \alpha^{2^i} b_1^{2^i}\right)$, we obtain

$$\eta_1 a_2^{2^i} + \eta_2 b_2^{2^i} + \eta_3 b_2 = 0, \tag{39}$$

where

$$\begin{cases} \eta_1 = \lambda_1 \\ \eta_2 = (\varphi_2 + \varphi_3)\, a_1^{2^i+1} + \varphi_4 a_1^{2^i} b_1 + (\varphi_1 + \varphi_3)\, b_1^{2^i+1} \\ \eta_3 = (\varphi_1 + \varphi_3)\, a_1^{2^{i+1}} + \varphi_3 a_1^{2^i} b_1^{2^i} + (\varphi_1 + \varphi_3)\, b_1^{2^{i+1}}. \end{cases}$$

Furthermore, computing (38)$^{2^i}$ + $\lambda_1^{2^i-1}$ × (39), we eliminate the term $a_2^{2^i}$ and obtain

$$\lambda_2^{2^i} b_2^{2^{2i}-1} + \left(\lambda_1^{2^i-1}\eta_2 + \lambda_3^{2^i}\right) b_2^{2^i-1} + \lambda_1^{2^i-1}\eta_3 = 0. \tag{40}$$

Here we note that $\lambda_2 \neq 0$. Otherwise one has $(\varphi_2 + \varphi_3)\, a_1^2 + \varphi_3 a_1 b_1 + (\varphi_2 + \varphi_3)\, b_1^2 = 0$, i.e.,

$$\left(\frac{\varphi_2 + \varphi_3}{\varphi_3} \cdot \frac{a_1}{b_1}\right)^2 + \frac{\varphi_2 + \varphi_3}{\varphi_3} \cdot \frac{a_1}{b_1} + \left(\frac{\varphi_2 + \varphi_3}{\varphi_3}\right)^2 = 0,$$

which is in contradiction with the fact $\mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right) = 0$ by Lemma 14 (4).

In addition, since the differential uniformity of V_i is 4, Eq. (40) has three nonzero solutions $b_2 = b_1, \bar{b}$ and $\bar{b} + b_1$ and we only need to obtain the expression of $\bar{b}$. Clearly, $\tilde{b}_2 = b_1^{2^i-1}$ is a solution of

$$\lambda_2^{2^i} \tilde{b}_2^{2^i+1} + \left(\lambda_1^{2^i-1}\eta_2 + \lambda_3^{2^i}\right) \tilde{b}_2 + \lambda_1^{2^i-1}\eta_3 = 0. \tag{41}$$

Hence, Eq. (41) can be written as

$$\lambda_2^{2^i}\left(\tilde{b}_2 + b_1^{2^i-1}\right)\left(\tilde{b}_2^{2^i} + b_1^{2^i-1}\tilde{b}_2^{2^i-1} + b_1^{2\cdot(2^i-1)}\tilde{b}_2^{2^i-2} + \cdots + b_1^{(2^i-1)\cdot(2^i-1)}\tilde{b}_2 + c\right) = 0,$$

where $c = \frac{\lambda_1^{2^i-1}\eta_3}{\lambda_2^{2^i} b_1^{2^i-1}}$. Now we consider the equation

$$\tilde{b}_2^{2^i} + b_1^{2^i-1}\tilde{b}_2^{2^i-1} + b_1^{2\cdot(2^i-1)}\tilde{b}_2^{2^i-2} + \cdots + b_1^{(2^i-1)\cdot(2^i-1)}\tilde{b}_2 + c = 0. \tag{42}$$

Let $\hat{b}_2 = \frac{1}{\tilde{b}_2 + b_1^{2^i-1}}$. Then Eq. (42) becomes

$$\hat{b}_2^{2^i} + \frac{b_1^{2^i-1}}{c}\hat{b}_2 + \frac{1}{c} = 0,$$

i.e.,

$$\left(\frac{c^{\frac{1}{2^i-1}}}{b_1}\hat{b}_2\right)^{2^i} + \frac{c^{\frac{1}{2^i-1}}}{b_1}\hat{b}_2 + \frac{c^{\frac{1}{2^i-1}}}{b_1^{2^i}} = 0. \tag{43}$$

In addition, we have

$$\begin{aligned}
c^{\frac{1}{2^i-1}} &= \left(\frac{\lambda_1^{2^i-1}\eta_3}{\lambda_2^{2^i} b_1^{2^i-1}}\right)^{\frac{1}{2^i-1}} \\
&= \frac{\lambda_1}{b_1}\left(\frac{(\varphi_1+\varphi_3)\left(a_1^{2^{i+1}}+\frac{\varphi_3}{\varphi_1+\varphi_3}a_1^{2^i}b_1^{2^i}+b_1^{2^{i+1}}\right)}{(\varphi_2+\varphi_3)^{2^i}\left(a_1^{2^{i+1}}+\frac{\varphi_3^{2^i}}{(\varphi_2+\varphi_3)^{2^i}}a_1^{2^i}b_1^{2^i}+b_1^{2^{i+1}}\right)}\right)^{\frac{1}{2^i-1}} \\
&= \frac{\lambda_1}{b_1}\left(\frac{\varphi_1+\varphi_3}{(\varphi_2+\varphi_3)^{2^i}}\right)^{\frac{1}{2^i-1}} \\
&= \frac{\lambda_1}{b_1\varphi_3},
\end{aligned}$$

where the last two equalities follow from Lemma 14 (1). Moreover,

$$\begin{aligned}
\frac{c^{\frac{1}{2^i-1}}}{b_1^{2^i}} &= \frac{\lambda_1}{\varphi_3 b_1^{2^i+1}} \\
&= \frac{(\varphi_1+\varphi_3)\,a_1^{2^i}+(\varphi_2+\varphi_3)\,a_1 b_1^{2^i-1}+(\varphi_3+\varphi_4)\,b_1^{2^i}}{\varphi_3 b_1^{2^i}} \\
&= \left(\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}\right)^{2^i}+\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+\frac{\varphi_3+\varphi_4}{\varphi_3} \\
&= \left(\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+u\right)^{2^i}+\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+u,
\end{aligned}$$

where $u=\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha$ due to Lemma 14 (2). Hence, from Eq. (43), we have

$$\frac{c^{\frac{1}{2^i-1}}}{b_1}\hat{b}_2 \in \left\{\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+u,\ \frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+u+1\right\},$$

which means that there are exactly two solutions in $\mathbb{F}_q$ for Eq. (42). W.L.O.G., we only consider the first expression here. Namely, we get

$$\hat{b}_2 = \frac{b_1}{c^{\frac{1}{2^i-1}}}\left(\frac{(\varphi_2+\varphi_3)\,a_1}{\varphi_3 b_1}+u\right) = \frac{(\varphi_2+\varphi_3)\,a_1 b_1+\varphi_3 u b_1^2}{\lambda_1}.$$

Thus,

$$\tilde{b}_2 = \frac{1}{\hat{b}_2}+b_1^{2^i-1} = \frac{\lambda_1}{(\varphi_2+\varphi_3)\,a_1 b_1+\varphi_3 u b_1^2}+b_1^{2^i-1}$$

is one solution of Eq. (42). Furthermore, one solution of Eq. (40) is

$$\begin{aligned}
b_2 &= \left(\tilde{b}_2\right)^{\frac{1}{2^i-1}} \\
&= \left(\frac{(\varphi_1+\varphi_3)\,a_1^{2^i}+\varphi_3 u^{2^i} b_1^{2^i}}{(\varphi_2+\varphi_3)\,a_1+\varphi_3 u b_1}\right)^{\frac{1}{2^i-1}}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{\varphi_1+\varphi_3}{\varphi_2+\varphi_3}\right)^{\frac{1}{2^i-1}} \cdot \left(\frac{a_1^{2^i} + \frac{\varphi_3}{\varphi_1+\varphi_3}u^{2^i}b_1^{2^i}}{a_1 + \frac{\varphi_3}{\varphi_2+\varphi_3}ub_1}\right)^{\frac{1}{2^i-1}}\\
&= \frac{\varphi_2+\varphi_3}{\varphi_3}\left(a_1 + \frac{\varphi_3}{\varphi_2+\varphi_3}ub_1\right) \text{ (by Lemma 14(1))}\\
&= \frac{\varphi_2+\varphi_3}{\varphi_3}a_1 + \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha b_1 (\text{recall that } u = \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha).
\end{aligned}
$$

It follows directly from Eq. (38) that

$$
a_2 = \frac{\lambda_2}{\lambda_1}b_2^{2^i} + \frac{\lambda_3}{\lambda_1}b_2 = \left(\frac{\varphi_2+\varphi_3}{\varphi_3}\alpha + 1\right)a_1 + \frac{\varphi_2+\varphi_3}{\varphi_3}b_1.
$$

□

4.2 The proof of $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$

In this subsection, we prove that for any $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_q^2\backslash\{(0, 0)\}$ satisfying $S_{V_i,(a_1,b_1)}(a_2, b_2) = (0, 0)$, $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$.

According to Eq. (37.1), we know that for any $(a_1, b_1) \in \mathbb{F}_q^2$, $S_{V_i,(a_1,b_1)}(x, y)$ can be represented as

$$
S_{V_i,(a_1,b_1)}(x, y) = A_1 \begin{bmatrix} x^{2^i} \\ x \end{bmatrix} + B_1 \begin{bmatrix} y^{2^i} \\ y \end{bmatrix},
$$

where

$$
A_1 = \begin{bmatrix} a_1 + \alpha b_1, & a_1^{2^i} + \alpha^{2^i} b_1^{2^i} \\ (\alpha^{2^i+1} + \beta)a_1 + \alpha^{2^i} b_1, & (\alpha^{2^i+1} + \beta)a_1^{2^i} + \alpha b_1^{2^i} \end{bmatrix} \triangleq \begin{bmatrix} a_{11}, & a_{12} \\ a_{13}, & a_{14} \end{bmatrix}
$$

and

$$
B_1 = \begin{bmatrix} \alpha^{2^i} a_1 + (\alpha^{2^i+1} + \beta)b_1, & \alpha a_1^{2^i} + (\alpha^{2^i+1} + \beta)b_1^{2^i} \\ \alpha a_1 + b_1, & \alpha^{2^i} a_1^{2^i} + b_1^{2^i} \end{bmatrix} \triangleq \begin{bmatrix} b_{11}, & b_{12} \\ b_{13}, & b_{14} \end{bmatrix}.
$$

For the three relations between $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_q^2\backslash\{(0, 0)\}$ presented in Proposition 16 such that $S_{V_i,(a_1,b_1)(a_2,b_2)} = (0, 0)$, it is clear that if $a_2 = a_1$ and $b_2 = b_1$, we have $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$. In addition, if we have proved that $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$ holds for the second relation in Proposition 16, then so does it for the third relation since the sum of two same subspace equals to the subspace. Therefore, it suffices to show that $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$ holds for the second relation in Proposition 16. Below we will again restrict φ_4 to the case of even i.

Let $u = \frac{\varphi_2+\varphi_3}{\varphi_3}\alpha$. Then $u^{2^i} = u + \frac{\varphi_3+\varphi_4}{\varphi_3}$. Moreover, $a_2 = (u + 1)a_1 + \frac{\varphi_2+\varphi_3}{\varphi_3}b_1$ and $b_2 = \frac{\varphi_2+\varphi_3}{\varphi_3}a_1 + ub_1$. Furthermore, we get

$$
a_2^{2^i} = \left(u^{2^i} + 1\right)a_1^{2^i} + \left(\frac{\varphi_2+\varphi_3}{\varphi_3}\right)^{2^i} b_1^{2^i} = \left(u + \frac{\varphi_4}{\varphi_3}\right)a_1^{2^i} + \frac{\varphi_1+\varphi_3}{\varphi_3}b_1^{2^i}
$$

and

$$
b_2^{2^i} = \left(\frac{\varphi_2+\varphi_3}{\varphi_3}\right)^{2^i} a_1^{2^i} + u^{2^i} b_1^{2^i} = \frac{\varphi_1+\varphi_3}{\varphi_3}a_1^{2^i} + \left(u + \frac{\varphi_3+\varphi_4}{\varphi_3}\right)b_1^{2^i}.
$$

Therefore, in $S_{V_i,(a_2,b_2)}(x, y)$, we have

$$A_2 = \begin{bmatrix} a_2 + \alpha b_2, & a_2^{2^i} + \alpha^{2^i} b_2^{2^i} \\ (\alpha^{2^i+1} + \beta)a_2 + \alpha^{2^i} b_2, & (\alpha^{2^i+1} + \beta)a_2^{2^i} + \alpha b_2^{2^i} \end{bmatrix} \triangleq \begin{bmatrix} a_{21}, & a_{22} \\ a_{23}, & a_{24} \end{bmatrix},$$

and

$$B_2 = \begin{bmatrix} \alpha^{2^i} a_2 + (\alpha^{2^i+1} + \beta)b_2, & \alpha a_2^{2^i} + (\alpha^{2^i+1} + \beta)b_2^{2^i} \\ \alpha a_2 + b_2, & \alpha^{2^i} a_2^{2^i} + b_2^{2^i} \end{bmatrix} \triangleq \begin{bmatrix} b_{21}, & b_{22} \\ b_{23}, & b_{24} \end{bmatrix},$$

where the explicit expressions of entries in A_2 and B_2 in terms of a_1, b_1 are given as follows:

$$\begin{aligned} a_{21} &= a_2 + \alpha b_2 \\ &= (u+1)a_1 + \tfrac{\varphi_2+\varphi_3}{\varphi_3} b_1 + \tfrac{\varphi_2+\varphi_3}{\varphi_3}\alpha a_1 + u\alpha b_1 \\ &= \left(u + 1 + \tfrac{\varphi_2+\varphi_3}{\varphi_3}\alpha\right) a_1 + \left(\tfrac{\varphi_2+\varphi_3}{\varphi_3} + u\alpha\right) b_1 \\ &= a_1 + \left(\alpha^2 + 1\right) \tfrac{\varphi_2+\varphi_3}{\varphi_3} b_1 \ \text{(recall that } u = \tfrac{\varphi_2+\varphi_3}{\varphi_3}\alpha), \end{aligned}$$

$$\begin{aligned} a_{22} &= a_2^{2^i} + \alpha^{2^i} b_2^{2^i} \\ &= a_1^{2^i} + \left(\alpha^{2^{i+1}} + 1\right) \tfrac{\varphi_1+\varphi_3}{\varphi_3} b_1^{2^i} \ \text{(due to Lemma 14(1))}, \end{aligned}$$

$$\begin{aligned} a_{23} &= (\alpha^{2^i+1} + \beta)a_2 + \alpha^{2^i} b_2 \\ &= \left(\left(\alpha^{2^i+1} + \beta\right)(u+1) + \alpha^{2^i} \tfrac{\varphi_2+\varphi_3}{\varphi_3}\right) a_1 + \left(\left(\alpha^{2^i+1} + \beta\right) \tfrac{\varphi_2+\varphi_3}{\varphi_3} + \alpha^{2^i} u\right) b_1 \\ &= \left(\tfrac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3} + \alpha^{2^i+1} + \beta\right) a_1 + \tfrac{\varphi_2+\varphi_3}{\varphi_3} \beta b_1, \end{aligned}$$

$$\begin{aligned} a_{24} &= (\alpha^{2^i+1} + \beta)a_2^{2^i} + \alpha b_2^{2^i} \\ &= \left(\left(\alpha^{2^i+1} + \beta\right)\left(u + \tfrac{\varphi_4}{\varphi_3}\right) + \alpha \tfrac{\varphi_1+\varphi_3}{\varphi_3}\right) a_1^{2^i} \\ &\quad + \left(\left(\alpha^{2^i+1} + \beta\right) \tfrac{\varphi_1+\varphi_3}{\varphi_3} + \alpha\left(u + \tfrac{\varphi_3+\varphi_4}{\varphi_3}\right)\right) b_1^{2^i} \\ &= \left(\tfrac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3} + \alpha^{2^i+1} + \beta\right) a_1^{2^i} + \tfrac{\varphi_1+\varphi_3}{\varphi_3} \beta b_1^{2^i} \ \text{(due to(15)and(16))}, \end{aligned}$$

$$\begin{aligned} b_{21} &= \alpha^{2^i} a_2 + (\alpha^{2^i+1} + \beta)b_2 = \left(\alpha^{2^i} + \tfrac{\varphi_2+\varphi_3}{\varphi_3}\beta\right) a_1 + \tfrac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3} b_1, \\ b_{22} &= \alpha a_2^{2^i} + (\alpha^{2^i+1} + \beta)b_2^{2^i} = \left(\alpha + \tfrac{\varphi_1+\varphi_3}{\varphi_3}\beta\right) a_1^{2^i} + \tfrac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3} b_1^{2^i}, \\ b_{23} &= \alpha a_2 + b_2 = \left(\tfrac{\varphi_2+\varphi_3}{\varphi_3}(\alpha^2 + 1) + \alpha\right) a_1, \\ b_{24} &= \alpha^{2^i} a_2^{2^i} + b_2^{2^i} = \left(\tfrac{\varphi_1+\varphi_3}{\varphi_3}(\alpha^{2^{i+1}} + 1) + \alpha^{2^i}\right) a_1^{2^i}. \end{aligned}$$

Note that the determinants of A_1 and B_1 are

$$\begin{aligned} \mathrm{Det}(A_1) &= a_{11}a_{14} + a_{12}a_{13} \\ &= (\varphi_1 + \varphi_3)\, a_1^{2^i} b_1 + (\varphi_2 + \varphi_3)\, a_1 b_1^{2^i} + (\varphi_3 + \varphi_4)\, b_1^{2^i+1}, \end{aligned}$$

and

$$\mathrm{Det}(B_1) = b_{11}b_{14} + b_{12}b_{13}$$

$$= (\varphi_3 + \varphi_4)\, a_1^{2^i+1} + (\varphi_2 + \varphi_3)\, a_1^{2^i} b_1 + (\varphi_1 + \varphi_3)\, a_1 b_1^{2^i}.$$

Now we consider the necessary and sufficient conditions such that $\mathrm{Det}(A_1) = 0$. Clearly, from $\mathrm{Det}(A_1) = 0$, we have $b_1 = 0$ or

$$(\varphi_1 + \varphi_3) \left(\frac{a_1}{b_1}\right)^{2^i} + (\varphi_2 + \varphi_3)\, \frac{a_1}{b_1} + \varphi_3 + \varphi_4 = 0,$$

namely,

$$\left(\frac{\varphi_2 + \varphi_3}{\varphi_3} \cdot \frac{a_1}{b_1}\right)^{2^i} + \frac{\varphi_2 + \varphi_3}{\varphi_3} \cdot \frac{a_1}{b_1} = \frac{\varphi_3 + \varphi_4}{\varphi_3}$$

and thus $a_1 = \alpha b_1$ or $\left(\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3}\right) b_1$ due to Lemma 14. Therefore, $\mathrm{Det}(A_1) = 0$ if and only if $b_1 = 0$ or $a_1 = \alpha b_1$ or $\left(\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3}\right) b_1$. Similarly, $\mathrm{Det}(B_1) = 0$ if and only if $a_1 = 0$ or $b_1 = \alpha a_1$ or $\left(\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3}\right) a_1$.

It is easy to verify that $\mathrm{Det}(A_1) = 0$ and $\mathrm{Det}(B_1) = 0$ holds at the same time if and only if

(i) $\alpha = 1, a_1 = b_1$;
(ii) $\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3} = 1, a_1 = b_1$;
(iii) $\alpha \left(\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3}\right) = 1, a_1 = \alpha b_1$.

If $\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3} = 1$, then $\frac{\varphi_2}{\varphi_3} = \frac{\alpha}{\alpha+1}$. Recall that (21) holds, namely,

$$\left(\frac{\varphi_2}{\varphi_3}\right)^2 = \frac{\varphi_2 + \varphi_3}{\varphi_3}\alpha + \left(\frac{\varphi_2 + \varphi_3}{\varphi_3}\alpha\right)^2.$$

Plugging $\frac{\varphi_2}{\varphi_3} = \frac{\alpha}{\alpha+1}$ into the above equation and simplifying, we obtain $\alpha = 1$, implying $\frac{\varphi_3}{\varphi_2+\varphi_3} = 0$, which is impossible. If $\alpha \left(\alpha + \frac{\varphi_3}{\varphi_2+\varphi_3}\right) = 1$, then $\frac{\varphi_2}{\varphi_3} = \frac{\alpha^2+\alpha+1}{\alpha^2+1} = \frac{1}{\alpha+1} + \frac{1}{\alpha^2+1} + 1$, which is also impossible since $\mathrm{Tr}_q\left(\frac{\varphi_2}{\varphi_3}\right) = 0$. Therefore, $\mathrm{Det}(A_1) = 0$ and $\mathrm{Det}(B_1) = 0$ holds at the same time if and only if $\alpha = 1, a_1 = b_1$, under which it is clear that $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$.

Next, we consider the following two cases:

(I) $\mathrm{Det}(B_1) \neq 0$;
(II) $\mathrm{Det}(A_1) \neq 0$.

It is clear that $\mathrm{Im}_{V_i,(a_1,b_1)} = \mathrm{Im}_{V_i,(a_2,b_2)}$ if there exists some invertible matrix P such that $PA_1 = A_2$ and $PB_1 = B_2$.

As for (i), it suffices to show that

$$B_2 B_1^{-1} A_1 = A_2. \tag{44}$$

After computing, we know that (44) is

$$\begin{bmatrix} b_{21}b_{14}a_{11} + b_{21}b_{12}a_{13} + b_{22}b_{13}a_{11} + b_{22}b_{11}a_{13}, & b_{21}b_{14}a_{12} + b_{21}b_{12}a_{14} + b_{22}b_{13}a_{12} + b_{22}b_{11}a_{14} \\ b_{23}b_{14}a_{11} + b_{23}b_{12}a_{13} + b_{24}b_{13}a_{11} + b_{24}b_{11}a_{13}, & b_{23}b_{14}a_{12} + b_{23}b_{12}a_{14} + b_{24}b_{13}a_{12} + b_{24}b_{11}a_{14} \end{bmatrix}$$
$$= \mathrm{Det}(B_1) \begin{bmatrix} a_{21}, & a_{22} \\ a_{23}, & a_{24} \end{bmatrix}.$$

By plugging the expression of B_1 into the above equation and simplifying, we get

$$\begin{cases} b_{14}a_{11} + b_{12}a_{13} = (\varphi_1+\varphi_3)\, a_1^{2^i+1} + \varphi_4 a_1 b_1^{2^i} + (\varphi_2+\varphi_3)\, b_1^{2^i+1} \\ b_{14}a_{12} + b_{12}a_{14} = (\varphi_1+\varphi_3)\, a_1^{2^{i+1}} + \varphi_3 a_1^{2^i} b_1^{2^i} + (\varphi_1+\varphi_3)\, b_1^{2^{i+1}} \\ b_{13}a_{11} + b_{11}a_{13} = (\varphi_2+\varphi_3)\, a_1^2 + \varphi_3 a_1 b_1 + (\varphi_2+\varphi_3)\, b_1^2 \\ b_{13}a_{12} + b_{11}a_{14} = (\varphi_2+\varphi_3)\, a_1^{2^i+1} + \varphi_4 a_1^{2^i} b_1 + (\varphi_1+\varphi_3)\, b_1^{2^i+1}. \end{cases}$$

Moreover, we have

1.

$$\begin{aligned} &b_{21}b_{14}a_{11} + b_{21}b_{12}a_{13} + b_{22}b_{13}a_{11} + b_{22}b_{11}a_{13} \\ &\quad = (\varphi_3+\varphi_4)\, a_1^{2^i+2} + \left(\varphi_4\alpha^{2^i} + \frac{\varphi_4(\varphi_2+\varphi_3)}{\varphi_3}\beta + \frac{(\varphi_2+\varphi_3)^2(\varphi_1+\varphi_3)}{\varphi_3}\right) a_1^2 b_1^{2^i} \\ &\qquad + \left((\varphi_2+\varphi_3)\,\alpha^{2^i} + \frac{(\varphi_2+\varphi_3)^2}{\varphi_3}\beta + \frac{(\varphi_3+\varphi_4)(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3}\right) a_1 b_1^{2^i+1} \\ &\qquad + \left(\varphi_3\alpha + (\varphi_1+\varphi_3)\,\beta + \frac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)^2}{\varphi_3}\right) a_1^{2^i+1} b_1 \\ &\qquad + \left((\varphi_2+\varphi_3)\,\alpha + \frac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3}\beta\right) a_1^{2^i} b_1^2 \\ &\quad = (\varphi_3+\varphi_4)\, a_1^{2^i+2} + (\varphi_1+\varphi_3)\, a_1^2 b_1^{2^i} + \frac{\left(\alpha^2+1\right)(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3} a_1 b_1^{2^i+1} \\ &\qquad + \frac{(\alpha^4+\beta^2+1)(\varphi_2+\varphi_3)}{\varphi_3} a_1^{2^i+1} b_1 + \frac{\left(\alpha^2+1\right)(\varphi_2+\varphi_3)^2}{\varphi_3} a_1^{2^i} b_1^2, \end{aligned}$$

2.

$$\begin{aligned} &b_{23}b_{14}a_{11} + b_{23}b_{12}a_{13} + b_{24}b_{13}a_{11} + b_{24}b_{11}a_{13} \\ &\quad = \frac{(\varphi_1+\varphi_2)^2\beta}{\varphi_3} a_1^{2^i+2} + \frac{\varphi_4(\varphi_1+\varphi_3)\beta}{\varphi_3} a_1^2 b_1^{2^i} + \frac{(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)\beta}{\varphi_3} a_1 b_1^{2^i+1} \\ &\qquad + (\varphi_2+\varphi_3)\,\beta a_1^{2^i+1} b_1 + \frac{(\varphi_2+\varphi_3)^2\beta}{\varphi_3} a_1^{2^i} b_1^2 \end{aligned}$$

3.

$$\begin{aligned} &b_{23}b_{14}a_{12} + b_{23}b_{12}a_{14} + b_{24}b_{13}a_{12} + b_{24}b_{11}a_{14} \\ &\quad = \frac{(\varphi_1+\varphi_2)^2\beta}{\varphi_3} a_1^{2^{i+1}+1} + (\varphi_1+\varphi_3)\,\beta a_1^{2^i+1} b_1^{2^i} + \frac{(\varphi_1+\varphi_3)^2\beta}{\varphi_3} a_1 b_1^{2^{i+1}} \\ &\qquad + \frac{\varphi_4(\varphi_2+\varphi_3)\beta}{\varphi_3} a_1^{2^{i+1}} b_1 + \frac{(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)\beta}{\varphi_3} a_1^{2^i} b_1^{2^i+1}. \end{aligned}$$

4.

$$\begin{aligned} &b_{21}b_{14}a_{12} + b_{21}b_{12}a_{14} + b_{22}b_{13}a_{12} + b_{22}b_{11}a_{14} \\ &\quad = (\varphi_3+\varphi_4)\, a_1^{2^{i+1}+1} + \left(\varphi_3\alpha^{2^i} + (\varphi_2+\varphi_3)\,\beta + \frac{(\varphi_2+\varphi_3)^2(\varphi_1+\varphi_3)}{\varphi_3}\right) a_1^{2^i+1} b_1^{2^i} \end{aligned}$$

$$
\begin{aligned}
&+\left((\varphi_1+\varphi_3)\alpha^{2^i}+\frac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3}\beta\right)a_1b_1^{2^{i+1}}\\
&+\left(\frac{(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)^2}{\varphi_3}+\varphi_4\alpha+\frac{\varphi_4(\varphi_1+\varphi_3)}{\varphi_3}\beta\right)a_1^{2^{i+1}}b_1\\
&+\left((\varphi_2+\varphi_3)(\varphi_1+\varphi_3)+(\varphi_1+\varphi_3)\alpha+\frac{(\varphi_1+\varphi_3)^2}{\varphi_3}\beta\right.\\
&\left.+\frac{\varphi_4(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3}\right)a_1^{2^i}b_1^{2^i+1}\\
=&(\varphi_3+\varphi_4)a_1^{2^{i+1}+1}+\frac{\left(\alpha^{2^{i+2}}+\beta^2+1\right)(\varphi_1+\varphi_3)}{\varphi_3}a_1^{2^i+1}b_1^{2^i}\\
&+\frac{\left(\alpha^{2^{i+1}}+1\right)(\varphi_1+\varphi_3)^2}{\varphi_3}a_1b_1^{2^{i+1}}\\
&+(\varphi_2+\varphi_3)a_1^{2^{i+1}}b_1+\frac{\left(\alpha^{2^{i+1}}+1\right)(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)}{\varphi_3}a_1b_1^{2^{i+1}},
\end{aligned}
$$

Furthermore, after computing and simplifying, we have

1.

$$
\begin{aligned}
&\mathrm{Det}(B_1)a_{21}\\
&\quad=(\varphi_3+\varphi_4)a_1^{2^i+2}+(\varphi_1+\varphi_3)a_1^2b_1^{2^i}\\
&\qquad+\frac{\left(\alpha^2+1\right)(\varphi_2+\varphi_3)(\varphi_1+\varphi_3)}{\varphi_3}a_1b_1^{2^i+1}\\
&\qquad+\frac{(\alpha^4+\beta^2+1)(\varphi_2+\varphi_3)}{\varphi_3}a_1^{2^i+1}b_1+\frac{\left(\alpha^2+1\right)(\varphi_2+\varphi_3)^2}{\varphi_3}a_1^{2^i}b_1^2,
\end{aligned}
$$

2.

$$
\begin{aligned}
&\mathrm{Det}(B_1)a_{22}\\
&\quad=(\varphi_3+\varphi_4)a_1^{2^{i+1}+1}+\frac{\left(\alpha^{2^{i+2}}+\beta^2+1\right)(\varphi_1+\varphi_3)}{\varphi_3}a_1^{2^i+1}b_1^{2^i}\\
&\qquad+\frac{\left(\alpha^{2^{i+1}}+1\right)(\varphi_1+\varphi_3)^2}{\varphi_3}a_1b_1^{2^{i+1}}\\
&\qquad+(\varphi_2+\varphi_3)a_1^{2^{i+1}}b_1+\frac{\left(\alpha^{2^{i+1}}+1\right)(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)}{\varphi_3}a_1b_1^{2^{i+1}},
\end{aligned}
$$

3.

$$
\begin{aligned}
&\mathrm{Det}(B_1)a_{23}\\
&=\frac{(\varphi_1+\varphi_2)^2\beta}{\varphi_3}a_1^{2^i+2}+\frac{\varphi_4(\varphi_1+\varphi_3)\beta}{\varphi_3}a_1^2b_1^{2^i}+\frac{(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)\beta}{\varphi_3}a_1b_1^{2^i+1}\\
&\quad+(\varphi_2+\varphi_3)\beta a_1^{2^i+1}b_1+\frac{(\varphi_2+\varphi_3)^2\beta}{\varphi_3}a_1^{2^i}b_1^2
\end{aligned}
$$

4.

$$\begin{aligned}&\mathrm{Det}(B_1)a_{24}\\&=\frac{(\varphi_1+\varphi_2)^2\beta}{\varphi_3}a_1^{2^{i+1}+1}+(\varphi_1+\varphi_3)\beta a_1^{2^i+1}b_1^{2^i}+\frac{(\varphi_1+\varphi_3)^2\beta}{\varphi_3}a_1b_1^{2^{i+1}}\\&\quad+\frac{\varphi_4(\varphi_2+\varphi_3)\beta}{\varphi_3}a_1^{2^{i+1}}b_1+\frac{(\varphi_1+\varphi_3)(\varphi_2+\varphi_3)\beta}{\varphi_3}a_1^{2^i}b_1^{2^i+1}.\end{aligned}$$

Hence, it follows that

$$\begin{aligned}&\begin{bmatrix}b_{21}b_{14}a_{11}+b_{21}b_{12}a_{13}+b_{22}b_{13}a_{11}+b_{22}b_{11}a_{13}, & b_{21}b_{14}a_{12}+b_{21}b_{12}a_{14}+b_{22}b_{13}a_{12}+b_{22}b_{11}a_{14}\\ b_{23}b_{14}a_{11}+b_{23}b_{12}a_{13}+b_{24}b_{13}a_{11}+b_{24}b_{11}a_{13}, & b_{23}b_{14}a_{12}+b_{23}b_{12}a_{14}+b_{24}b_{13}a_{12}+b_{24}b_{11}a_{14}\end{bmatrix}\\&=\mathrm{Det}(B_1)\begin{bmatrix}a_{21}, & a_{22}\\ a_{23}, & a_{24}\end{bmatrix}.\end{aligned}$$

and Eq. (44) holds.

As for (ii), we need to show that

$$A_2A_1^{-1}B_1=B_2, \tag{45}$$

whose proof can be obtained through just changing a_1 and b_1 in the proof of (44).

Therefore, for any $(a_1,b_1),(a_2,b_2)\in\mathbb{F}_q^2\backslash\{(0,0)\}$ satisfying $B_{V_i,(a_1,b_1)}(a_2,b_2)=(0,0)$, $\mathrm{Im}_{V_i,(a_1,b_1)}=\mathrm{Im}_{V_i,(a_2,b_2)}$ holds and by Lemma 5, we know that the boomerang uniformity of V_i is 4.

Remark 17 we are aware that Li, Hu, Xiong and Zeng in [13] are independently working on the same problem as in this paper. Their techniques in the proof are different from ours in the early version [11] of this paper.

Remark 18 It's worth pointing out that from the experimental results by MAGMA for $q=2^3,2^5$, the set Γ in Theorem 1 covers all the coefficients $\alpha,\beta\in\mathbb{F}_q^*$ that yield permutations $V_i(x,y)$ with boomerang uniformity 4. We therefore propose the following conjecture and invite interested readers to attack it.

Conjecture 19 *Let $q=2^n$ with n odd,* $\gcd(i,n)=1$ *and $V_i:=(R_i(x,y),R_i(y,x))$ with $R_i(x,y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$. If V_i is a permutation over $\mathbb{F}_q^2$ with boomerang uniformity* 4*, then the coefficients α,β are taken from the set Γ defined as in* (1)*.*

5 Conclusions

In this paper, we applied the butterfly structure in constructing cryptographically strong permuations. The open butterfly does not seem to generate permutations with boomerang uniformity 4 according to numerical results. Based on an intensive study on the coefficients of $R_i(x,y)=(x+\alpha y)^{2^i+1}+\beta y^{2^i+1}$, $\gcd(i,n)=1$, over $\mathbb{F}_{2^n}$, we provided a sufficient condition on α,β such that $V_i(x,y)=(R_i(x,y),R_i(y,x))$ is a permutation over $\mathbb{F}_{2^{2n}}$ with boomerang uniformity 4. The proposed condition seems to be also necessary according to numeric results and a conjecture on the observation was given.

Acknowledgements We would like to thank the editor and the anonymous referees whose valuable comments and suggestions improve both the technical quality and the editorial quality of this paper.

References

1. Boura C., Canteaut A.: On the boomerang uniformity of cryptographic sboxes. IACR Trans. Symm. Cryptol. **2018**(3), 290–310 (2018).
2. Browning K., Dillon J., McQuistan M., Wolfe A.: An APN permutation in dimension six. Finite Fields **518**, 33–42 (2010).
3. Calderini M., Villa I.: On the boomerang uniformity of some permutation polynomials. Cryptogr. Commun. **12**, 1161–1178 (2019).
4. Canteaut A., Duval S., Perrin L.: 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. Inf. Theory **63**(11), 7575–7591 (2017).
5. Canteaut A., Perrin L., Tian S.: If a generalised butterfly is APN then it operates on 6 bits. Cryptogr. Commun. **11**, 1147–1164 (2019).
6. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. Lect. Notes Comput. Sci. **950**, 356–365 (1995).
7. Cid C., Huang T., Peyrin T., Sasaki Y., Song L.: Boomerang connectivity table: A new cryptanalysis tool. Lect. Notes Comput. Sci. **10821**, 683–714 (2018).
8. Fu S., Feng X., Wu B.: Differentially 4-uniform permutations with the best known nonlinearity from butterflies. IACR Trans. Symm. Cryptol. **2017**(2), 228–249 (2017).
9. Lahtonen J.: On the odd and the aperiodic correlation properties of the Kasami sequences. IEEE Trans. Inf. Theory **41**(5), 1506–1508 (1995).
10. Leander G., Poschmann A.: On the classification of 4 bit s-boxes. Lect. Notes Comput. Sci. **4547**, 159–176 (2007).
11. Li, K., Li, C., Helleseth, T., Qu, L.: Cryptographically strong permutations from the butterfly structure. arXiv:1912.02640 (2019)
12. Li K., Qu L., Sun B., Li C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inf. Theory **65**(11), 7542–7553 (2019).
13. Li, N., Hu, Z., Xiong, M., Zeng, X.: 4-uniform BCT permutations from generalized butterfly structure. arXiv:2001.00464 (2020)
14. Li Y., Tian S., Yu Y., Wang M.: On the generalization of butterfly structure. IACR Trans. Symm. Cryptol. **2018**(1), 160–179 (2018).
15. Lidl R., Mullen G.L., Turnwald G.: Dickson polynomials, vol. 65. Chapman & Hall/CRC, New York (1993).
16. Mesnager S., Tang C., Xiong M.: On the boomerang uniformity of quadratic permutations. Des. Codes Cryptogr. **88**, 2233–2246 (2020).
17. Nyberg K.: Differentially uniform mappings for cryptography. Lect. Notes Comput. Sci. **765**, 55–64 (1994).
18. Park Y.H., Lee J.B.: Permutation polynomials and group permutation polynomials. Bull. Aust. Math. Soc. **63**(1), 67–74 (2001).
19. Perrin L., Udovenko A., Biryukov A.: Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. Lect. Notes Comput. Sci. **9815**, 93–122 (2016).
20. Tian S., Boura C., Perrin L.: Boomerang uniformity of popular S-box constructions. Des. Codes Cryptogr. **88**(9), 1959–1989 (2020).
21. Wang, Q.: Cyclotomic mapping permutation polynomials over finite fields. In: S.W. Golomb, G. Gong, T. Helleseth, H. Song (eds.) Sequences, Subsequences, and Consequences, International Workshop,, *Lecture Notes in Comput. Sci.*, vol. 4893, pp. 119–128. Springer (2007)
22. Zieve M.: On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. Proc. Am. Math. Soc. **137**(7), 2209–2216 (2009).

Affiliations

Kangquan Li[1] · Chunlei Li[2] · Tor Helleseth[2] · Longjiang Qu[1,3]

✉ Longjiang Qu
ljqu_happy@hotmail.com

Kangquan Li
likangquan11@nudt.edu.cn

Chunlei Li
chunlei.li@uib.no

Tor Helleseth
tor.helleseth@uib.no

[1] College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China

[2] Department of Informatics, University of Bergen, Bergen 5020, Norway

[3] State Key Laboratory of Cryptology, Beijing 100878, China