Designs, Codes and Cryptography (2022) 90:265–276
https://doi.org/10.1007/s10623-021-00974-5

A note on "Cryptographically strong permutations from the butterfly structure"

Nian Li[1] · Zhao Hu[1] · Maosheng Xiong[2] · Xiangyong Zeng[1]

Received: 25 March 2021 / Revised: 14 September 2021 / Accepted: 5 November 2021 /
Published online: 15 January 2022

Abstract

Very recently, a class of cryptographically strong permutations with boomerang uniformity 4 and the best known nonlinearity is constructed from the closed butterfly structure in Li et al. (Des Codes Cryptogr 89(4):737–761, 2021). In this note, we provide two additional results concerning these permutations. We first represent the conditions of these permutation obtained in Li et al. (Des Codes Cryptogr 89(4):737–761, 2021) in a much simpler form, and then show that they are linear equivalent to Gold functions. We also prove a criterion for solving a new type of equations over finite fields, which is useful and may be of independent interest.

Keywords Boomerang uniformity · Butterfly structure · Differential uniformity · Permutation polynomial

Mathematics Subject Classification 11T06 · 11T71

Communicated by G. Kyureghyan.

✉ Maosheng Xiong
mamsxiong@ust.hk

Nian Li
nian.li@hubu.edu.cn

Zhao Hu
zhao.hu@aliyun.com

Xiangyong Zeng
xzeng@hubu.edu.cn

1 Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

2 Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

1 Introduction

1.1 Background

As a generalization of Dillon's APN permutation in dimension six, butterfly structure was initially proposed by Perrin et al. [14] to generate $2m$-bit mappings by concatenating two bivariate functions over $\mathbb{F}_{2^m}$. Canteaut et al. [3] further studied this structure and generalized it as below. Let $R(x, y)$ be a bivariate polynomial on $\mathbb{F}_{2^m}$ such that $R_y : x \mapsto R(x, y)$ is a permutation of $\mathbb{F}_{2^m}$ for any $y \in \mathbb{F}_{2^m}$. The *closed butterfly* is the function $V_R : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by

$$V_R(x, y) = (R(x, y), R(y, x)), \tag{1.1}$$

and the *open butterfly* is the function $H_R : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by

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

where R_y^{-1} is the compositional inverse of R_y. It is known that H_R is always an involution (and hence a permutation) and the two functions H_R and V_R are CCZ-equivalent, so they share the same differential uniformity, nonlinearity and Walsh spectrum [3].

Let m, k be positive integers such that m is odd and $\gcd(k, m) = 1$. Extending previous work [3,5], Li et al. [11] considered a general bivariate polynomial $R(x, y)$ of the form

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

for any $\alpha, \beta \in \mathbb{F}_{2^m}^* := \mathbb{F}_{2^m} \backslash \{0\}$ and proved that the corresponding butterflies H_R and V_R are differentially 4-uniform and have the best known nonlinearity when $\beta \neq (\alpha + 1)^{2^k+1}$. Under this condition, however, the closed butterfly V_R may not be a permutation.

Since $\gcd(2^k + 1, 2^m - 1) = 1$, any $\beta \in \mathbb{F}_{2^m}^*$ can be written as $\beta = \beta_1^{2^k+1}$ for some $\beta_1 \in \mathbb{F}_{2^m}^*$. So equivalently, the general bivariate polynomial $R(x, y)$ may be written as

$$R(x, y) = (x + \alpha y)^{2^k+1} + (\beta y)^{2^k+1}, \quad \alpha, \beta \in \mathbb{F}_{2^m}^*. \tag{1.2}$$

In an interesting recent paper [8], the authors not only provided conditions under which the closed butterfly V_R is a permutation, but also proved that under these conditions the boomerang uniformity of V_R is 4, a new and important cryptographic property which was discovered to be useful in analyzing the boomerang attack. Interested readers may refer to [2,4,17] for more details. These functions V_R may be considered as the sixth known family of permutations with boomerang uniformity 4 over the field $\mathbb{F}_{2^{2m}}$ in the literature. Observe that for $R(x, y)$ given in (1.2), if k is even, letting $k' := m - k$, then k' is odd and $\gcd(k', m) = 1$. It is easy to see that for any $x, y, \alpha, \beta \in \mathbb{F}_{2^m}$ we have

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

So the case of k being even is equivalent to that of k' which is odd now. For this reason, using the new definition of $R(x, y)$ in (1.2), we may state the main result of [8] as follows:

Theorem 1 [8, Theorem 1] *Let* m, k *be odd with* $\gcd(m, k) = 1$ *and* $q = 2^m$. *The closed butterfly function* $V_R(x, y)$ *given by (1.1) where the function* $R(x, y)$ *is given in* (1.2) *permutes* $\mathbb{F}_q^2$ *and has boomerang uniformity 4 if* (α, β) *is taken from the following set*

$$\Gamma = \left\{(\alpha, \beta) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : \varphi_2^{2^k} = \varphi_1 \varphi_3^{2^k-1} \text{ and } \varphi_3 \neq 0\right\}, \tag{1.3}$$

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

$$\begin{cases} \varphi_1 = (\alpha+1)^{2^{k+1}+2} + \alpha^{2^k+2} + \alpha^{2^k} + \alpha\beta^{2^k+1} + \beta^{2^{k+1}+2}, \\ \varphi_2 = (\alpha+1)^{2^{k+1}+2} + \alpha^{2^{k+1}+1} + \alpha + \alpha^{2^k}\beta^{2^k+1} + \beta^{2^{k+1}+2}, \\ \varphi_3 = (\alpha+1)^{2^{k+1}+2} + \beta^{2^{k+1}+2}. \end{cases} \tag{1.4}$$

Two natural questions arise from Theorem 1. First, the set Γ given in (1.3) looks quite complicated. *Is there a simpler way to represent* Γ? Second, two functions F and F' over $\mathbb{F}_{2^n}$ are called linear (resp. affine) equivalent if $F = A_1 \circ F' \circ A_2$ holds for some linear (resp. affine) permutations A_1 and A_2 over $\mathbb{F}_{2^n}$. It was observed in [8] by numerical computation that when $m = 3, 5$ and $(\alpha, \beta) \in \Gamma$, the closed butterfly function $V_R(x, y)$ is affine equivalent to the Gold function. *Is this true in general?* In this note, we answer these two questions.

1.2 Statement of the main results

Theorem 2 *Let m, k be odd integers with* $\gcd(m, k) = 1$.

(1) $(\alpha, \beta) \in \Gamma$ *if and only if* $\alpha, \beta \in \mathbb{F}_{2^m}^*$ *satisfy* $\alpha^2 + \beta^2 + \alpha\beta + 1 = 0$.
(2) If $(\alpha, \beta) \in \Gamma$*, then the closed butterfly function* $V_R(x, y)$ *over* $\mathbb{F}_{2^m}^2$ *given in* (1.1) *is linear equivalent to the Gold function* $x^{2^{k-m}+1}$ *over* $\mathbb{F}_{2^{2m}}$.

Remark 1 According to [8, Conjecture 19], the closed butterfly V_R is a permutation with boomerang uniformity 4 if and only if $(\alpha, \beta) \in \Gamma$. Hence if this conjecture is true, then Theorem 2 shows that all closed butterfly functions V_R which are permutations with boomerang uniformity 4 are linear equivalent to the Gold function. We also remark that [8, Conjecture 19] is a consequence of a much more general conjecture concerning permutation properties of general quadrinomials of the form (3.2) in [10, Sect. VI]. This conjecture has been proved to be true for $k = 1$ in [7] but remains open for $k > 1$.

Remark 2 It seems fitting to summarize here what we have known about the open butterfly function H_R. The setting is the same as in Theorem 2.

(1) H_R is always an involution (and hence a permutation) and the two functions H_R and V_R are CCZ-equivalent, so they share the same differential uniformity, nonlinearity and Walsh spectrum. The open butterfly function H_R is particularly interesting. Interested readers may refer to [3,5,11] for some of their cryptographic properties.
(2) Theorem 2 shows that H_R is CCZ-equivalent to the Gold function $x^{2^{k-m}+1}$ when $(\alpha, \beta) \in \Gamma$. Experimental results show however that for $m = 3$, H_R is not EA-equivalent to general Gold functions when $(\alpha, \beta) \in \Gamma$.
(3) When $(\alpha, \beta) \notin \Gamma$, experimental results show that for $m = 3, 5$, H_R (and also V_R) is CCZ-inequivalent to general Gold functions.
(4) As for the boomerang uniformity of H_R, experimental results show that for $m = 3$, the boomerang uniformity of H_R is at least 12 for any $(\alpha, \beta) \in \mathbb{F}_{2^3}^2$, except when H_R becomes APN, which are CCZ-equivalent to the only known APN permutation over $\mathbb{F}_{2^6}$. It was known that H_R is not APN whenever $m > 3$.

Next, in view of [8] and [10], there is no need to publish the arxiv paper [9], which proved essentially the same result as [8]. Instead we take this opportunity to present from [9] a criterion for solving a new type of equations over finite fields. We believe this criterion is useful and is of independent interest. In fact it played an essential role in the proofs of [10], which substantially extends the work [8,15,16]. A special case of this criterion for $k = 1$ has appeared in [15]. Similar criteria were well-known in the literature for equations over finite fields such as $x^2 + ax + b = 0$ [12], $x^{2^k+1} + x + a = 0$ [6] and $x^{q+1} + ax + b = 0$ [1].

Theorem 3 *Let m, k be odd integers with $\gcd(k, m) = 1$ and $n = 2m$. For any $\mu, \nu \in \mathbb{F}_{2^n}$, define*

$$L_{\mu,\nu}(x) = x^{2^k} + \mu\overline{x} + (\mu + 1)x + \nu.$$

Here $\overline{x} = x^{2^m}$ for any $x \in \mathbb{F}_{2^n}$. Then the equation $L_{\mu,\nu}(x) = 0$ has either 0, 2 or 4 solutions in $\mathbb{F}_{2^n}$. More precisely, let $\xi, \Delta \in \mathbb{F}_{2^m}$ and $\lambda \in \mathbb{F}_{2^n}$ be defined by the equations

$$\xi^{2^k-1} = 1 + \mu + \overline{\mu}, \quad \Delta = \frac{\nu + \overline{\nu}}{\xi^{2^k}}, \quad \lambda^{2^k} + \lambda = \mu\xi. \tag{1.5}$$

Then

(1) $L_{\mu,\nu}(x) = 0$ has two solutions in $\mathbb{F}_{2^n}$ if and only if one of the following conditions is satisfied:

(i) $1 + \mu + \overline{\mu} = 0$ and $\sum_{i=0}^{m-1} (\mu^{2^k}(\nu + \overline{\nu}) + \nu^{2^k})^{2^{ki}} = \nu + \overline{\nu}$;
(ii) $1 + \mu + \overline{\mu} \neq 0$, $\mathrm{Tr}_1^m(\Delta) = 0$ and $\overline{\lambda} + \lambda = \xi + 1$.

(2) $L_{\mu,\nu}(x) = 0$ has four solutions in $\mathbb{F}_{2^n}$ if and only if

$$1 + \mu + \overline{\mu} \neq 0, \mathrm{Tr}_1^m(\Delta) = 0, \overline{\lambda} + \lambda = \xi, \text{ and } \mathrm{Tr}_1^n\left(\frac{\lambda^{2^k}\overline{\nu}}{\xi^{2^k}}\right) = 0.$$

(3) If $\nu = 0$, $1 + \mu + \overline{\mu} \neq 0$ and $\lambda + \overline{\lambda} = \xi$, then $L_{\mu,\nu}(x) = 0$ has four solutions in $\mathbb{F}_{2^n}$, and these four solutions are $0, 1, \lambda, \lambda + 1$.

We remark that Theorem 3 can be used to study the number of solutions of equations of the form $c_1x^{2^k+1} + c_2\bar{x}^{2^k+1} + c_3x^{2^k}x^{2^m} + c_4xx^{2^{m+k}}$ over $\mathbb{F}_{2^{2m}}$, where m, k are odd, $\gcd(m, k) = 1$ and $c_1, c_2, c_3, c_4 \in \mathbb{F}_{2^{2m}}$.

This note is organized as follows: we prove (1) and (2) of Theorem 2 in Sects. 2 and 3 respectively; we prove Theorem 3 in Sect. 4. Finally we conclude this note in Sect. 5.

2 Proof of part (1) of Theorem 2

To simplify our computation a little bit, we use

$$\alpha \mapsto \alpha + 1, \quad \sigma := 2^k.$$

Under this new α and symbol σ, we can rewrite φ_1, φ_2 and φ_3 as

$$\begin{cases} \varphi_1 = \alpha^2(1 + \alpha + \alpha^2)^\sigma + \beta^{\sigma+1}\left(\beta^{\sigma+1} + \alpha + 1\right), \\ \varphi_2 = \alpha^{2\sigma}(1 + \alpha + \alpha^2) + \beta^{\sigma+1}\left(\beta^{\sigma+1} + \alpha^\sigma + 1\right), \\ \varphi_3 = \left(\alpha^{\sigma+1} + \beta^{\sigma+1}\right)^2. \end{cases} \tag{2.1}$$

Now assume

$$\alpha, \beta \in \mathbb{F}_{2^m}, \alpha \neq 1, \beta \neq 0. \tag{2.2}$$

To prove (1) of Theorem 2, it is equivalent to proving

$$\varphi_3 \neq 0, \varphi_2^\sigma \varphi_3 + \varphi_1 \varphi_3^\sigma = 0 \text{ if and only if } \alpha^2 + \beta^2 + (1+\alpha)\beta = 0. \tag{2.3}$$

It is easy to see that $\varphi_3 \neq 0$ if and only if $\alpha \neq \beta$. Denote

$$F := \varphi_2^\sigma \varphi_3 + \varphi_1 \varphi_3^\sigma.$$

Plugging the values of $\varphi_1, \varphi_2, \varphi_3$ from (2.1) into F, expanding and then collecting common terms, we can obtain

$$F = \alpha^2(1+\alpha)^\sigma \beta^{2\sigma^2+2\sigma} + (1+\alpha)\beta^{2\sigma^2+3\sigma+1} + (1+\alpha)^{\sigma^2}\beta^{\sigma^2+3\sigma+2} + \alpha^{2\sigma+2}(1+\alpha)^{\sigma^2}\beta^{\sigma^2+\sigma} + \alpha^{2\sigma^2}(1+\alpha)^\sigma \beta^{2\sigma+2} + \alpha^{2\sigma^2+2\sigma}(1+\alpha)\beta^{\sigma+1}.$$

Denote

$$Y = \alpha^2 + \beta^2 + (\alpha+1)\beta. \tag{2.4}$$

The right hand side of F above can be further simplified, and we have

$$F = \beta^\sigma \left(\varphi_3 Y^{\sigma^2} + \left(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2}\right)^2 Y^\sigma + \varphi_3^\sigma Y\right). \tag{2.5}$$

Now suppose $Y = 0$. It is clear that $F = 0$. Moreover, if $\alpha = \beta$, then from $Y = 0$ we have $\alpha = 1$ or $\beta = 0$, contradicting (2.2). So $\alpha \neq \beta$ and hence $\varphi_3 \neq 0$ as α, β satisfy (2.2).

On the other hand, suppose $F = 0$ and $\alpha \neq \beta$. Since $\beta \neq 0$, we have

$$\varphi_3 Y^{\sigma^2} + \left(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2}\right)^2 Y^\sigma + \varphi_3^\sigma Y = 0. \tag{2.6}$$

To study (2.6), we quote a result of Bluher:

Lemma 1 [1, Theorem 5.4] *Let* $\gcd(m,k) = 1, b \in \mathbb{F}_{2^m}$ *and* $f(x) = x^{2^k+1} + bx + b$. *Suppose* $\gamma \in \mathbb{F}_{2^m}$ *is a root of* $f(x)$. *Then* γ *is the only root of* $f(x)$ *in* $\mathbb{F}_{2^m}$ *if and only if* $\mathrm{Tr}_1^m(\xi) = 1$. *Here* ξ *is the unique element in* $\mathbb{F}_{2^m}$ *satisfying the relation* $\xi^{2^k-1} = \frac{1}{\gamma+1}$.

Then we can prove

Lemma 2 *Let* m*,* k *be odd integers with* $\gcd(m,k) = 1$*,* $\sigma = 2^k$*,* $\alpha, \beta \in \mathbb{F}_{2^m}$ *and* $\alpha \neq \beta$. *Assume that* $\varphi_3 = \left(\alpha^{\sigma+1} + \beta^{\sigma+1}\right)^2$. *Then the equation*

$$\varphi_3 Y^{\sigma^2} + \left(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2}\right)^2 Y^\sigma + \varphi_3^\sigma Y = 0 \tag{2.7}$$

has exactly two solutions $Y = 0$ *and* $Y = \alpha^2 + \beta^2$ *in* $\mathbb{F}_{2^m}$.

Proof It can be readily verified that both 0 and $\alpha^2+\beta^2$ are solutions of (2.7). Thus, it suffices to show that

$$\varphi_3 Y^{\sigma^2-1} + \left(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2}\right)^2 Y^{\sigma-1} + \varphi_3^\sigma = 0 \tag{2.8}$$

has the unique solution $Y = \alpha^2 + \beta^2$ in $\mathbb{F}_{2^m}$. Let $y = Y^{\sigma-1}$, then (2.8) becomes

$$\varphi_3 y^{\sigma+1} + \left(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2}\right)^2 y + \varphi_3^\sigma = 0,$$

which can be further written as

$$y^{\sigma+1} + ay + b = 0$$

due to the fact that $\varphi_3 \neq 0$, where

$$a = \frac{(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2})^2}{\varphi_3}, \quad b = \varphi_3^{\sigma-1}.$$

Note that $a, b \neq 0$. Substituting y with $\frac{b}{a}x$ leads to

$$x^{\sigma+1} + b^{'}x + b^{'} = 0 \tag{2.9}$$

where $b^{'} = a^{\sigma+1}/b^{\sigma}$.

To complete the proof, we use Lemma 1. Since $\gcd(\sigma - 1, 2^m - 1) = 1$, it suffices to prove that (2.9) has the unique solution $\gamma = \frac{a}{b}(\alpha^2 + \beta^2)^{\sigma-1}$.

With a straightforward calculation, we have

$$\xi^{\sigma-1} = \frac{1}{\gamma+1} = \frac{\varphi_3^{\sigma}(\alpha+\beta)^2}{(\alpha\beta^{\sigma^2} + \beta\alpha^{\sigma^2})^2(\alpha+\beta)^{2\sigma} + \varphi_3^{\sigma}(\alpha+\beta)^2} = \frac{\varphi_3^{\sigma-1}}{(\alpha+\beta)^{2(\sigma^2-1)}},$$

which gives

$$\xi = \frac{\varphi_3}{(\alpha+\beta)^{2(\sigma+1)}}.$$

Further, we can obtain

$$\mathrm{Tr}_1^m(\xi) = \mathrm{Tr}_1^m\left(\frac{\alpha^{\sigma+1} + \beta^{\sigma+1}}{(\alpha+\beta)^{\sigma+1}}\right) = 1 + \mathrm{Tr}_1^m\left(\frac{\alpha\beta^{\sigma} + \beta\alpha^{\sigma}}{(\alpha+\beta)^{\sigma+1}}\right).$$

Let $\epsilon = \alpha + \beta$. Then we have

$$\mathrm{Tr}_1^m\left(\frac{\alpha\beta^{\sigma} + \beta\alpha^{\sigma}}{(\alpha+\beta)^{\sigma+1}}\right) = \mathrm{Tr}_1^m\left(\frac{\alpha(\alpha+\epsilon)^{\sigma} + (\alpha+\epsilon)\alpha^{\sigma}}{\epsilon^{\sigma+1}}\right) = \mathrm{Tr}_1^m\left(\frac{\alpha}{\epsilon} + \frac{\alpha^{\sigma}}{\epsilon^{\sigma}}\right) = 0.$$

This shows that $\mathrm{Tr}_1^m(\xi) = 1$ and hence according to Lemma 1, the Eq. (2.9) has the unique solution $\gamma \in \mathbb{F}_{2^m}$. This completes the proof of Lemma 2. □

Now we resume our proof of (1) in Theorem 2. From (2.6) and Lemma 2, we find that either $Y = 0$ or $Y = \alpha^2 + \beta^2$. On the other hand, since $Y = \alpha^2 + \beta^2 + (\alpha+1)\beta$ (see (2.4)), $\alpha \neq 1$ and $\beta \neq 0$, it is clear that $Y \neq \alpha^2 + \beta^2$. Thus we conclude that $Y = 0$. This proves (2.3) and hence concludes the proof of part (1) of Theorem 2.

3 Proof of part (2) of Theorem 2

We first derive a univariate polynomial expression of V_R (see also [8,9]). Let $n = 2m$ and ω be a root of $x^2 + x + 1 = 0$ in $\mathbb{F}_{2^n}$. Since m is odd, $\{1, \omega\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^m}^2$ is isomorphic to $\mathbb{F}_{2^n}$ under the map

$$z = (x, y) \mapsto x + \omega y, \qquad \forall x, y \in \mathbb{F}_{2^m}.$$

Hence every element $z \in \mathbb{F}_{2^n}$ can be uniquely represented as $z = x + \omega y$ with $x, y \in \mathbb{F}_{2^m}$. This together with $\overline{z} = x + \overline{\omega}y$, where $\overline{z} := z^{2^m}$, one obtains

$$x = \overline{\omega}z + \omega\overline{z}, \quad y = z + \overline{z}.$$

Substituting z with $\omega^2 z$ gives

$$V_R(x, y) = V_R(z) = \omega^2\left(e_1 z^{2^k+1} + e_2\overline{z}^{2^k+1} + e_3 z^{2^k}\overline{z} + e_4 z\overline{z}^{2^k}\right),$$

where

$$e_1 = 1+\alpha+\alpha^{2^k+1}+\beta^{2^k+1},\ e_2 = 1+\alpha^{2^k}+\alpha^{2^k+1}+\beta^{2^k+1},$$
$$e_3 = 1+\alpha+\alpha^{2^k},\qquad e_4 = \alpha+\alpha^{2^k}+\alpha^{2^k+1}+\beta^{2^k+1}.$$

Thus, the closed butterfly V_R defined by (1.1) is linear equivalent to the polynomial

$$f(x) = e_1x^{2^k+1} + e_2\overline{x}^{2^k+1} + e_3x^{2^k}\overline{x} + e_4x\overline{x}^{2^k}. \tag{3.1}$$

Since $(\alpha, \beta) \in \Gamma$, by (1) of Theorem 2, $\alpha, \beta \in \mathbb{F}_{2^m}^*$ satisfy $\alpha^2 + \beta^2 + \alpha\beta + 1 = 0$. Using $\beta = \theta\alpha + 1$ for some $\theta \in \mathbb{F}_{2^m}^*$, we find that a common solution of $(\alpha, \beta) \in \Gamma$ is given by

$$(\alpha, \beta) = \left(\frac{1}{1+\theta+\theta^2}, \frac{\theta^2}{1+\theta+\theta^2}\right), \quad \theta \in \mathbb{F}_{2^m}^*.$$

Using the above expression, the quadrinomial (3.1) is linear equivalent to

$$F(x) := c_1x^{2^k+1} + c_2\overline{x}^{2^k+1} + c_3x^{2^k}\overline{x} + c_4x\overline{x}^{2^k}, \tag{3.2}$$

where the coefficients $c_i = e_i\alpha^{-(2^k+1)}$ and are explicitly given by

$$\begin{cases} c_1 = 1+\theta+\theta^2+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}, \\ c_2 = (1+\theta+\theta^2)^{2^k}+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}, \\ c_3 = 1+(\theta+\theta^2)^{2^k+1}, \\ c_4 = (1+\theta+\theta^2)^{2^k+1}+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}. \end{cases} \tag{3.3}$$

Thus we can conclude that the closed butterfly $V_R(x, y)$ defined by (1.1) is linear equivalent to $F(x)$ defined by (3.2). Then, we can complete the proof of (2) of Theorem 2 by proving Lemma 3.

Lemma 3 *Let $n = 2m$, m odd, $\gcd(n, k) = 1$, $\theta \in \mathbb{F}_{2^m}^*$ and $F(x)$ be the polynomial defined by (3.2) and (3.3). Then $F(x)$ is linear equivalent to the Gold function $x^{2^{k-m}+1}$ on $\mathbb{F}_{2^n}$.*

Proof Denote $g(x) = x^{2^k}\overline{x}$, $L_1(x) = Ax+B\overline{x}$ and $L_2(x) = Cx+D\overline{x}$, where the coefficients $A, B, C, D \in \mathbb{F}_{2^n}$. First, we need to find $A, B, C, D \in \mathbb{F}_{2^n}$ such that

$$Cg\left(Ax + B\overline{x}\right) + D\overline{g\left(Ax + B\overline{x}\right)} = F(x). \tag{3.4}$$

Denote the left hand side of (3.4) to be $H(x)$, we can obtain

$$H(x) = (CA^{2^k}\overline{B} + DA\overline{B}^{2^k})x^{2^k+1} + (C\overline{A}B^{2^k} + D\overline{A}^{2^k}B)\overline{x}^{2^k+1} +$$
$$(CA^{2^k}\overline{A} + DB\overline{B}^{2^k})x^{2^k}\overline{x} + (CB^{2^k}\overline{B} + DA\overline{A}^{2^k})x\overline{x}^{2^k}.$$

Now take the values

$$\begin{cases} A = 1, \\ B = 1+\theta, \\ C = \theta+\theta^{2^k}+\theta^{2^k+1}, \\ D = 1+\theta^{2^k+1}. \end{cases} \tag{3.5}$$

It can be readily verified that

$$\begin{cases} CA^{2^k}\overline{B}+DA\overline{B}^{2^k} = 1+\theta+\theta^2+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}, \\ C\overline{A}B^{2^k}+D\overline{A}^{2^k}B = (1+\theta+\theta^2)^{2^k}+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}, \\ CA^{2^k}\overline{A}+DB\overline{B}^{2^k} = 1+(\theta+\theta^2)^{2^k+1}, \\ CB^{2^k}\overline{B}+DA\overline{A}^{2^k} = (1+\theta+\theta^2)^{2^k+1}+(\theta+\theta^2)^{2^k+1}+\theta^{2(2^k+1)}. \end{cases}$$

Hence under the values of (3.5), Eq. (3.4) holds. Then, to complete the proof, it suffices to prove that both $L_1(x)$ and $L_2(x)$ are permutations. Note that $L_1(x)$ and $L_2(x)$ are permutations if and only if $A \neq B$ and $C \neq D$ respectively. Obviously $A \neq B$ since $\theta \in \mathbb{F}_{2^m}^*$. On the other hand, if $C = D$, then we have $1+\theta+\theta^{2^k} = 0$. Noting that m is odd, taking trace on both sides, we have

$$0 = \mathrm{Tr}_1^m\left(1+\theta+\theta^{2^k}\right) = \mathrm{Tr}_1^m(1) = 1,$$

which is a contradiction. Thus $C \neq D$. So both $L_1(x)$ and $L_2(x)$ are permutations on $\mathbb{F}_{2^n}$. This shows that $F(x)$ is linear equivalent to $g(x)$. Clear $g(x)$ is linear equivalent to the Gold function $x^{2^{k-m}+1}$. □

4 Proof of Theorem 3

First recall the following lemma:

Lemma 4 [13] *Let n, k be positive integers with $\gcd(n,k)=1$. For any $a \in \mathbb{F}_{2^n}$, the equation $x^{2^k}+x=a$ has either 0 or 2 solutions in $\mathbb{F}_{2^n}$. Moreover, it has two solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a)=0$.*

Now we start the proof of Theorem 3. Let $z = x+\overline{x}$, then the equation $L_{\mu,\nu}(x)=0$ becomes

$$x^{2^k}+x+\mu z+\nu = 0. \tag{4.1}$$

Taking 2^m-th power on both sides of (4.1) and adding them together gives

$$z^{2^k}+(1+\mu+\overline{\mu})z+\nu+\overline{\nu} = 0. \tag{4.2}$$

Taking 2^k-th power consecutively on both sides of (4.1), one can also obtain

$$x+x^{2^{km}} = x+\overline{x} = \sum_{i=0}^{m-1}(\mu z+\nu)^{2^{ki}}.$$

Hence solving $L_{\mu,\nu}(x)=0$ for $x \in \mathbb{F}_{2^n}$ is equivalent to solving the system of equations (4.1), (4.2) and

$$\sum_{i=0}^{m-1}(\mu z+\nu)^{2^{ki}}+z = 0 \tag{4.3}$$

for $x \in \mathbb{F}_{2^n}$ and $z \in \mathbb{F}_{2^m}$. Note that $\sum_{i=0}^{m-1}(\mu z+\nu)^{2^{ki}}+z \in \mathbb{F}_2$.

Without checking the solvability of (4.3), since $\gcd(n,k)=1$, for any μ and ν, (4.2) has at most two solutions for $z \in \mathbb{F}_{2^m}$, and for each such z, (4.1) has at most two solutions for

$x \in \mathbb{F}_{2^n}$, hence the equation $L_{\mu,\nu}(x) = 0$ has at most 4 solutions. Also observe that whenever $z \in \mathbb{F}_{2^m}$ is a solution to (4.2) that satisfies (4.3), one always has

$$\mathrm{Tr}_1^n(\mu z + \nu) = \mathrm{Tr}_1^m\left(\mu z + \nu + \overline{\mu z + \nu}\right) = z + \overline{z} = 0,$$

hence for such z, by Lemma 4, (4.1) is always solvable with two solutions $x \in \mathbb{F}_{2^n}$. We conclude that the number of solutions of $L_{\mu,\nu}(x) = 0$ equals two times the number of $z \in \mathbb{F}_{2^n}$ satisfying (4.2) and (4.3).

Now we study in more details the solvability of (4.2) and (4.3).

Case 1 $1 + \mu + \overline{\mu} = 0$.

In this case, (4.2) has a unique solution z such that $z^{2^k} = \nu + \overline{\nu}$, and (4.3) is equivalent to

$$\sum_{i=0}^{m-1}\left(\mu^{2^k} z^{2^k} + \nu^{2^k}\right)^{2^{ki}} = z^{2^k},$$

and this proves part (1) (i) of Theorem 3.

Case 2 $1 + \mu + \overline{\mu} \neq 0$.

Let ξ, Δ be defined by (1.5) and $z = \xi\rho$, then (4.2) becomes

$$\rho^{2^k} + \rho = \Delta \tag{4.4}$$

which has solutions for $\rho \in \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\Delta) = 0$.

We now assume that $\mathrm{Tr}_1^m(\Delta) = 0$. The two solutions $z_1, z_2 \in \mathbb{F}_{2^m}$ to (4.2) satisfy the relation

$$z_1 + z_2 = \xi.$$

Using $\lambda^{2^k} + \lambda = \mu\xi$, we have

$$\sum_{j=1}^{2}\left(\sum_{i=0}^{m-1}(\mu z_j + \nu)^{2^{ki}} + z_j\right) = \sum_{i=0}^{m-1}(\mu\xi)^{2^{ki}} + \xi = \lambda + \overline{\lambda} + \xi \in \mathbb{F}_2.$$

Subcase 2.1 $\lambda + \overline{\lambda} = \xi + 1$. In this case it is easy to see that among z_1 and z_2, exactly one element satisfies (4.3), hence the Eq. $L_{\mu,\nu}(x) = 0$ has two solutions. This proves part (1) (ii) of Theorem 3.

Subcase 2.2 $\overline{\lambda} + \lambda = \xi$. In this case, either both z_1 and z_2 satisfy (4.3) or neither satisfy (4.3), hence the equation $L_{\mu,\nu}(x) = 0$ has either 4 or 0 solution. We will prove below that these z_i's satisfy (4.3) if and only if

$$\mathrm{Tr}_1^n\left(\frac{\lambda^{2^k}\overline{\nu}}{\xi^{2^k}}\right) = 0,$$

hence verifying part (2) of Theorem 3.

Let $z = \xi\rho$ be a solution to (4.2) where $\rho \in \mathbb{F}_{2^m}$ satisfies (4.4). Denote by $h(z)$ the left hand side of Eq. (4.3). We have

$$h(z) = \sum_{i=0}^{m-1}(\mu\xi\rho + \nu)^{2^{ki}} + \xi\rho.$$

The quantity $h(z)$ can be simplified further: using (4.4) and the relation $\sum_{i=0}^{m-1}(\mu\xi)^{2^{ki}} = \lambda+\overline{\lambda}=\xi$ we can obtain

$$\begin{aligned}\sum_{i=0}^{m-1}(\mu\xi\rho)^{2^{ki}} &= \sum_{i=1}^{m-1}(\mu\xi)^{2^{ki}}\rho^{2^{ki}}+\mu\xi\rho = \sum_{i=1}^{m-1}(\mu\xi)^{2^{ki}}\left(\rho+\sum_{j=0}^{i-1}\Delta^{2^{kj}}\right)+\mu\xi\rho\\ &= \rho\sum_{i=0}^{m-1}(\mu\xi)^{2^{ki}}+\sum_{i=1}^{m-1}(\mu\xi)^{2^{ki}}\sum_{j=0}^{i-1}\Delta^{2^{kj}}\\ &= \rho\xi+\sum_{i=1}^{m-1}(\mu\xi)^{2^{ki}}\sum_{j=0}^{i-1}\Delta^{2^{kj}}. \qquad (4.5)\end{aligned}$$

As for the second term on the right side of (4.5), using $\mathrm{Tr}_1^m(\Delta)=\sum_{i=0}^{m-1}\Delta^{2^{ki}}=0$, one obtains

$$\begin{aligned}\sum_{i=1}^{m-1}\sum_{j=0}^{i-1}(\mu\xi)^{2^{ki}}\Delta^{2^{kj}} &= \sum_{j=0}^{m-2}\Delta^{2^{kj}}\sum_{i=j+1}^{m-1}(\mu\xi)^{2^{ki}} = \sum_{j=0}^{m-2}\Delta^{2^{kj}}\sum_{i=j+1}^{m-1}(\lambda^{2^k}+\lambda)^{2^{ki}}\\ &= \sum_{j=0}^{m-2}\Delta^{2^{kj}}(\lambda^{2^{k(j+1)}}+\lambda^{2^{km}})\\ &= \sum_{j=0}^{m-2}(\lambda^{2^k}\Delta)^{2^{kj}}+\Delta^{2^{k(m-1)}}\lambda^{2^{km}}\\ &= \sum_{j=0}^{m-1}(\lambda^{2^k}\Delta)^{2^{kj}}. \qquad (4.6)\end{aligned}$$

Combining (4.5) and (4.6) we can easily find

$$h(z)=\sum_{i=0}^{m-1}\left(\lambda^{2^k}\Delta+\nu\right)^{2^{ki}}.$$

Observing that

$$\lambda^{2^k}\Delta+\nu=\frac{\lambda^{2^k}}{\xi^{2^k}}(\overline{\nu}+\nu)+\nu=\frac{\lambda^{2^k}\overline{\nu}+\overline{\lambda}^{2^k}\nu}{\xi^{2^k}},$$

we obtain

$$h(z)=\mathrm{Tr}_1^n\left(\frac{\lambda^{2^k}\overline{\nu}}{\xi^{2^k}}\right).$$

Hence Eq. (4.3) is equivalent to

$$\mathrm{Tr}_1^n\left(\frac{\lambda^{2^k}\overline{\nu}}{\xi^{2^k}}\right)=0,$$

and in this case, the equation $L_{\mu,\nu}(x)=0$ has 4 solutions. This completes the proof of part (2) of Theorem 3.

Case 3 $\nu = 0$, $1 + \mu + \overline{\mu} \neq 0$ and $\lambda + \overline{\lambda} = \xi$. In this final case, Eq. (4.2) has two solutions $z_1 = 0$, $z_2 = \xi$ which both satisfy (4.3). Returning to (4.1), the corresponding four roots of $L_{\mu,\nu}(x) = 0$ are given by $0, 1, \lambda, \lambda + 1$. This proves part (3) of Theorem 3. Now Theorem 3 is proved.

5 Conclusion

In this note we further studied the cryptographically strong permutations obtained from the closed butterfly function in [8]. We represented the conditions in [8] in a much simpler way and showed that these cryptographically strong permutations are linear equivalent to Gold functions. Moreover, we proved a criterion for solving a new type of equations over finite fields, which is of independent interest.

Acknowledgements The authors would like to thank Dr. Chunming Tang and Haode Yan for helpful discussions. This work was supported by the National Natural Science Foundation of China (Nos. 62072162, 61761166010, 12001176), the Research Grants Council (RGC) of Hong Kong (No. N_HKUST619/17), the National Key Research and Development Project (No. 2018YFA0704702) and the Application Foundation Frontier Project of Wuhan Science and Technology Bureau (No. 2020010601012189).

References

1. Bluher A.W.: On $x^{q+1} + ax + b$. Finite Fields Appl. **10**(3), 285–305 (2004).
2. Boura C., Canteaut A.: On the boomerang uniformity of cryptographic Sboxes. IACR Trans. Symmetric Cryptol. **3**, 290–310 (2018).
3. 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).
4. Cid C., Huang T., Peyrin T., Sasaki Y., Song L.: Boomerang Connectivity Table: A New Cryptanalysis Tool, Advances in Cryptology-EUROCRYPT 2018, Part II, pp. 683–714, Lecture Notes in Comput. Sci., vol. 10821. Springer, Cham (2018).
5. Fu S., Feng X., Wu B.: Differentially 4-uniform permutations with the best known nonlinearity from butterflies. IACR Trans. Symmetric Cryptol. **2**, 228–249 (2017).
6. Helleseth T., Kholosha A.: On the equation $x^{2^l+1}+x+a$ over GF(2^k). Finite Fields Appl. **14**(1), 159–176 (2008).
7. Li K., Qu L., Li C., Chen H.: On a conjecture about a class of permutation quadrinomials. Finite Fields Appl. **66**, 101690 (2020).
8. Li K., Li C., Helleseth T., Qu L.: Cryptographically strong permutations from the butterfly structure. Des. Codes Cryptogr. **89**(4), 737–761 (2021).
9. Li N., Hu Z., Xiong M., Zeng X.: 4-Uniform BCT permutations from generalized butterfly structure, arXiv:2001.00464.
10. Li N., Xiong M., Zeng X.: On permutation quadrinomials and 4-uniform BCT. IEEE Trans. Inf. Theory **67**(7), 4845–4855 (2021).
11. Li Y., Tian S., Yu Y., Wang M.: On the generalization of butterfly structure. IACR Trans. Symmetric Cryptol. **2**, 160–179 (2018).
12. Lidl R., Niederreiter H.: Finite Fields, Encyclopedia of Mathematics, vol. 20. Cambridge University Press, Cambridge (1997).
13. Mesnager S., Kim K., Choe J., Lee D., Go D.: Solving $x + x^{2^l} + \cdots + x^{2^{ml}} = a$ over $\mathbb{F}_{2^n}$. Cryptogr. Commun. **12**(4), 809–817 (2020).
14. Perrin L., Udovenko A., Biryukov A.: Cryptanalysis of a Theorem: Decomposing the only known solution to the big APN problem. In: Robshaw M., Katz J. (eds.) LNCS, vol. 9816, pp. 93–122. Springer (2016).
15. Tu Z., Li N., Zeng X., Zhou J.: A class of quadrinomial permutation with boomerang uniformity four. IEEE Trans. Inf. Theory **66**(6), 3753–3765 (2020).

16. Tu Z., Liu X., Zeng X.: A revisit of a class of permutation quadrinomial. Finite Fields Appl. **59**, 57–85 (2019).
17. Wagner D.: The boomerang attack. In: Knudsen L.R. (ed.) FSE'1999, LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999).