Noname manuscript No.
(will be inserted by the editor)

On the boomerang uniformity of quadratic permutations over $\mathbb{F}_{2^n}$

Sihem Mesnager · **Chunming Tang** · **Maosheng Xiong**

Received: date / Accepted: date

Abstract At Eurocrypt'18, Cid, Huang, Peyrin, Sasaki, and Song introduced a new tool called Boomerang Connectivity Table (BCT) for measuring the resistance of a block cipher against the boomerang attack which is an important cryptanalysis technique introduced by Wagner in 1999 against block ciphers. Next, Boura and Canteaut introduced an important parameter related to the BCT for cryptographic Sboxes called boomerang uniformity.

The purpose of this paper is to present a brief state-of-the-art on the notion of boomerang uniformity of vectorial Boolean functions (or Sboxes) and provide new results. More specifically, we present a slightly different but more convenient formulation of the boomerang uniformity and prove some new identities. Moreover, we focus on quadratic permutations in even dimension and obtain general criteria by which they have optimal BCT. As a consequence of, two previously known results can be derived, and many new quadratic permutations with optimal BCT (optimal means that the maximal value in the Boomerang Connectivity Table equals the lowest known differential uniformity) can be found. In particular, we show that the boomerang uniformity of the binomial differentially 4-uniform permutations presented by Bracken, Tan, and Tan equals 4. Finally, we show a link between the boomerang uniformity and the nonlinearity for some special quadratic permutations.

Keywords Vectorial functions · Block ciphers · Boomerang uniformity · Boomerang Connectivity Table · Boomerang attack · Symmetric cryptography

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

S. Mesnager
LAGA, UMR 7539, CNRS, University Paris XIII - Sorbonne Paris Cité, University Paris VIII (Department of Mathematics) and Telecom ParisTech, France. E-mail: smesnager@univ-paris8.fr

C. Tang
School of Mathematics and Information, China West Normal University, Nanchong 637002, China, and Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China. E-mail: tangchunmingmath@163.com

M. Xiong
Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China. E-mail: mamsxiong@ust.hk

1 Introduction

Substitution boxes (Sboxes) are fundamental parts of block ciphers. Being the only source of nonlinearity in these ciphers, they play a central role in their robustness by providing confusion. Mathematically, Sboxes are vectorial (multi-output) Boolean functions, that is, functions from the vector space $\mathbb{F}_2^n$ of all binary vectors of length n to the finite field $\mathbb{F}_2^r$, for given positive integers n and r. These functions are called (n,r)-functions and include the single-output Boolean functions which correspond to the case $r = 1$. When they are used as Sboxes in block ciphers, the number r of output bits equals or approximately equals the number n of input bits. We shall identify the vector space $\mathbb{F}_2^n$ to the finite field $\mathbb{F}_{2^n}$ of order 2^n. A nice survey on Boolean and vectorial Boolean functions for cryptography can be found in [10] and [11], respectively.

In 1999, Wagner [23] introduced the *boomerang attack* which is an important cryptanalysis technique against block ciphers involving Sboxes. These attacks can be seen as an extension of classical differential attacks [5]. In fact, they combine two differentials for the upper part and the lower part of the cipher. The dependency between these two differentials then highly affects the complexity of the attack and all its variants (we refer for example to [3,4,6,7,15,17,18] and the references therein).

At Eurocrypt 2018, Cid, Huang, Peyrin, Sasaki, and Song [13] introduced the concept of *Boomerang Connectivity Table* (BCT for short) of a permutation F. Such a notion allows one to simplify the complexity analysis by storing and unifying the different switching probabilities of the cipher's Sbox in one table. Very recently (2019), Song, Qin and Hu [21] proposed a generalized framework of BCT. They applied their new framework to two block ciphers SKINNY and AES which are two typical block ciphers using weak and strong round functions respectively.

In 2018, Boura and Canteaut [2] introduced a parameter for cryptographic Sboxes called *boomerang uniformity* which is defined as the maximum value in BCT and provided a more in-depth analysis of boomerang connectivity tables by studying more closely differentially 4-uniform Sboxes. They completely characterized the BCT of all differentially 4-uniform permutations of 4 bits and then studied these objects for some cryptographically relevant families of Sboxes as the inverse function and quadratic permutations. These two families provide the first examples of differentially 4-uniform Sboxes optimal against boomerang attacks for an even number of variables. Later, Li, Qu, Sun and Li [19] gave an essentially equivalent definition to compute the BCT and the boomerang uniformity and provided a characterization of functions having a fixed boomerang uniformity by means of the Walsh transform and finally exhibited a class of differentially 4-uniform permutation for which the boomerang uniformity equals 4. Not long ago, Boura, Perrin and Tian studied in [9] the boomerang uniformity of some popular constructions used for building large S-boxes. The aim of this manuscript is to increase our knowledge on boomerang uniformity of (quadratic) Sboxes in the line of the recent articles [2] and [19].

The paper is structured as follows. In Section 2, we introduce the needed definitions related to the differential uniformity and boomerang uniformity of vectorial functions and briefly discuss these notions. In Section 3, we present shortly the state-of-the-art on boomerang uniformity of Sboxes. Here we present a slightly different but more convenient formulation of the boomerang uniformity and show that the row sum and the column sum of the boomerang connectivity table is related to the differential spectrum and can be expressed in terms of the zeros of the second-order derivative of the permutation or its inverse. Next, in Section 4, we specialize our study of boomerang uniformity to quadratic permutations in even dimension and generalize the results presented in [2] and [19] on quadratic permutation with optimal BCT (optimal means that the maximal value in the Boomerang Connectivity Table equals the lowest known differential uniformity). Consequently, we recover these known results and provide many new families of optimal Sboxes. In particular, we show that that the boomerang uniformity of the binomial differentially 4-uniform permutations presented by Bracken, Tan, and Tan [8] equals 4. We also give a connection between the boomerang uniformity and the nonlinearity for some special quadratic permutations.

2 Preliminaries

In this section, we recall some notations, definitions and results related to the differential properties and boomerang uniformity of vectorial Boolean functions.

Throughout this article, $\#E$ denotes the cardinality of a finite set E. The binary field is denoted by $\mathbb{F}_2$ and the finite field of order 2^n (resp. q) is denoted by $\mathbb{F}_{2^n}$ (resp. $\mathbb{F}_q$). The multiplicative group $\mathbb{F}_{2^n}^*$ is a cyclic group consisting of 2^n-1 elements. The terminology Sbox refer to an (n,n)-vectorial function, that is, a function from $\mathbb{F}_{2^n}$ to itself.

Any function F from $\mathbb{F}_{2^n}$ to itself admits a unique representation as a polynomial over $\mathbb{F}_{2^n}$ in one variable with degree at most 2^n-1:

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

For any k, $0\le k\le 2^n-1$, the number $w_2(k)$ of the nonzero coefficients $k_s\in\{0,1\}$ in the binary expansion of k is called the 2-weight of k. The algebraic degree of F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $\delta_i\neq 0$, that is, $\deg(F)=\max_{0\le i\le n-1,\delta_i\neq 0} w_2(i)$. A function F from $\mathbb{F}_{2^n}$ to itself is said to be quadratic if $\deg(F)=2$.

We use the following terminology: a permutation polynomial over $\mathbb{F}_q$ is a polynomial $F(x)\in\mathbb{F}_q[x]$ for which the function $a\mapsto F(a)$ defines a permutation of $\mathbb{F}_q$.

Recall that for any positive integers k and r such that $r|k$, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as

$$\mathrm{Tr}_r^k(x):=\sum_{i=0}^{\frac{k}{r}-1}x^{2^{ir}}=x+x^{2^r}+x^{2^{2r}}+\cdots+x^{2^{k-r}}.$$

In particular, the *absolute trace* over $\mathbb{F}_2$ of an element $x\in\mathbb{F}_{2^n}$ equals $\mathrm{Tr}_1^n(x)=\sum_{i=0}^{n-1}x^{2^i}$.

Definition 1 Given an (n,n)-function F, the derivative of F with respect to $a\in\mathbb{F}_{2^n}$ is the function $D_aF:x\mapsto F(x+a)+F(x)$. For $(a,b)\in(\mathbb{F}_{2^n})^2$, the second order derivative of F with respect to $a\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_{2^n}$ is the function $D_aD_bF:x\mapsto F(x+a)+F(x+b)+F(x+a+b)+F(x)$. For $(a,b)\in(\mathbb{F}_{2^n})^2$, the entries of the difference distribution table (DDT) are given by

$$\mathrm{DDT}_F(a,b)=\#\{x\in\mathbb{F}_{2^n}\mid D_aF(x)=b\}.$$

The differential uniformity of F is defined as

$$\Delta(F)=\max_{a,b\in\mathbb{F}_{2^n}^*}\mathrm{DDT}_F(a,b).$$

Differential uniformity is an important concept in cryptography as it quantifies the degree of security of a Substitution box used in the cipher with respect to differential attacks. APN (Almost Perfect Nonlinear) functions F are those such that their differential uniformity equals 2 (i.e. $\Delta(F) = 2$).

Definition 2 Let F be a permutation of $\mathbb{F}_{2^n}$. For $(a,b) \in (\mathbb{F}_{2^n})^2$, we define the entries of the *boomerang connectivity table* (BCT) as

$$\mathrm{BCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid F^{-1}(F(x)+b) + F^{-1}(F(x+a)+b) = a\},$$

where F^{-1} denotes the compositional inverse of F. The boomerang uniformity of F is defined as

$$\beta(F) = \max_{a,b \in \mathbb{F}_{2^n}^\star} \mathrm{BCT}_F(a,b).$$

Observe that $\mathrm{DDT}_F(a,b)$ is equal to 0 or 2^n when $ab = 0$. Likewise, $\mathrm{BCT}_F(a,b) = 2^n$ when $ab = 0$.

It is well-known that F and F^{-1} have the same differential uniformity since

$$\begin{aligned} F^{-1}(x) + F^{-1}(x+a) = b &\iff x + a = F(F^{-1}(x) + b) \\ &\iff F(F^{-1}(x)) + F(F^{-1}(x) + b) = a, \end{aligned}$$

yielding that $\mathrm{DDT}_{F^{-1}}(a,b) = \mathrm{DDT}_F(b,a)$ for any $(a,b) \in (\mathbb{F}_{2^n}^\star)^2$. Not surprising, as shown in [2, Proposition 2], it is also true for the boomerang uniformity since

$$\begin{aligned} &F^{-1}(F(x)+b) + F^{-1}(F(x+a)+b) = a \\ &\iff F(x) + F(F^{-1}(F(x+a)+b)+a) = b \\ &\iff F(F^{-1}(F(x+a))+a) + F(F^{-1}(F(x+a)+b)+a) = b, \end{aligned}$$

that is,

$$\mathrm{BCT}_F(a,b) = \mathrm{BCT}_{F^{-1}}(b,a), \quad \forall (a,b) \in (\mathbb{F}_{2^n}^\star)^2. \tag{2}$$

3 On boomerang uniformity of Sboxes

For vectorial Boolean functions, the most useful concepts of equivalence are the extended affine EA-equivalence and the CCZ-equivalence. Two (n,r)-functions F and F' are called EA-equivalent if there exist affine permutations L from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and L' from $\mathbb{F}_{2^r}$ to $\mathbb{F}_{2^r}$ and an affine function L'' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$ such that $F' = L' \circ F \circ L + L''$. EA-equivalence is a particular case of CCZ-equivalence [12]. Two (n,r)-functions F and F' are called CCZ-equivalent if their graphs $G_F := \{(x,F(x)),\ x \in \mathbb{F}_{2^n}\}$ and $G'_F := \{(x,F'(x)),\ x \in \mathbb{F}_{2^n}\}$ are affine equivalent, that is, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^r}$ such that $\mathcal{L}(G_F) = G'_F$.

As explained in [2], the multi-set formed by all values in the BCT is invariant under affine equivalence and inversion. In other words, the behavior of the BCT with respect to these two classes of transformations is the same as that of the DDT. However, while the differential spectrum of a function is also preserved by the extended affine (EA) equivalence, this is not the case for the BCT. As EA-equivalence is a special case of CCZ equivalence, the boomerang uniformity is also not always preserved under CCZ-equivalence.

In [13], it was indicated that $\mathrm{BCT}(a,b)$ is greater than or equal to $\mathrm{DDT}_F(a,b)$ yielding

Theorem 1 *([13]) Let F be a permutation of* $\mathbb{F}_{2^n}$. *Then,* $\beta(F) \geq \Delta(F)$.

It was also proved that

Theorem 2 *([13]) Let F be a permutation of* $\mathbb{F}_{2^n}$. *Then,* $\Delta(F) = 2$ *if and only if* $\beta(F) = 2$.

In [2], Boura and Canteaut established an alternative formulation of the boomerang uniformity as follows:

Theorem 3 *([2]) Let F be a permutation of* $\mathbb{F}_{2^n}$. *Then, for any a and b in* $\mathbb{F}_{2^n}^{\star}$

$$\mathrm{BCT}_F(a,b) = \mathrm{DDT}_F(a,b) + \sum_{\gamma \in \mathbb{F}_{2^n}^{\star}, \gamma \neq b} \#\left(\mathcal{U}_{\gamma,a}^{F^{-1}} \cap \left(b + U_{\gamma,a}^{F^{-1}} \right) \right)$$

where

$$\mathcal{U}_{\gamma,a}^{F^{-1}} = \{x \in \mathbb{F}_{2^n} \mid D_\gamma F^{-1}(x) = a\}.$$

In this paper, we shall use a slightly different formulation of Theorem 3.

Theorem 4 *Let F be a permutation of* $\mathbb{F}_{2^n}$. *Then, for any a and b in* $\mathbb{F}_{2^n}^{\star}$

$$\mathrm{BCT}_F(a,b) = \sum_{\gamma \in \mathbb{F}_{2^n}^{\star}} \#\left(\mathcal{U}_{\gamma,b}^{F} \cap \left(a + \mathcal{U}_{\gamma,b}^{F} \right) \right), \tag{3}$$

where

$$\mathcal{U}_{\gamma,b}^{F} = \{x \in \mathbb{F}_{2^n} \mid D_\gamma F(x) = b\}.$$

Proof Observing that $\mathrm{BCT}_F(a,b) = \mathrm{BCT}_{F^{-1}}(b,a)$, we can prove Equation (3) by directly applying Theorem 3. Here we mention another method. It was proved in [19] that the quantity $\mathrm{BCT}_F(a,b)$ equals the number of solutions $(x,y) \in (\mathbb{F}_{2^n})^2$ satisfying the equations $F(x)+F(y) = b$ and $F(x+a)+F(x+a) = b$ simultaneously. Letting $x+y = \gamma$, then $y = x+\gamma$, so we have

$$\begin{aligned} \mathrm{BCT}_F(a,b) &= \#\left\{ (x,\gamma) : \begin{array}{c} F(x)+F(x+\gamma) = b \\ F(x+a)+F(x+\gamma+a) = b \end{array} \right\} \\ &= \sum_{\gamma} \#\left\{ x : \begin{array}{c} F(x)+F(x+\gamma) = b \\ F(x+a)+F(x+\gamma+a) = b \end{array} \right\}. \end{aligned}$$

It is easy to see that the set in the inner sum for each subscript γ is $\mathcal{U}_{\gamma,b}^{F} \cap \left(a + \mathcal{U}_{\gamma,b}^{F} \right)$. Moreover, $\mathcal{U}_{0,b}^{F} = \emptyset$ since $b \neq 0$. This completes the proof of Theorem 4. □

The new formulation (3) seems more convenient to use than Theorem 3 which involves F^{-1}. Moreover, in (3), the condition that F is a permutation is not required, that is, we may define the boomerang uniformity for any (n,n) function F, even though it may not be a permutation. This is similar to the concept of differential uniformity, which may be of future interest. Finally, in (3), since $\mathcal{U}_{a,b}^{F} = a + \mathcal{U}_{a,b}^{F}$, we have

$$\mathrm{BCT}_F(a,b) = \mathrm{DDT}_F(a,b) + \sum_{\gamma \neq a,0} \#\left(\mathcal{U}_{\gamma,b}^{F} \cap \left(a + \mathcal{U}_{\gamma,b}^{F} \right) \right),$$

from which we can immediately derive $\mathrm{BCT}_F(a,b) \geq \mathrm{DDT}_F(a,b)$.

In the following, we show that the row sum and the column sum of the boomerang connectivity table can be expressed in terms of the zeros of the second-order derivative of the permutation or its inverse.

Proposition 1 *For any a and b in $\mathbb{F}_{2^n}^\star$, we have*

$$\sum_{c\in\mathbb{F}_{2^n}^\star} \mathrm{BCT}_F(a,c) = \sum_{c\in\mathbb{F}_{2^n}^\star} \#\{x\in\mathbb{F}_{2^n} \mid D_aD_cF(x)=0\} \tag{4}$$

$$= \sum_{c\in\mathbb{F}_{2^n}^\star} \mathrm{DDT}_F(a,c)^2 - 2^n, \tag{5}$$

and

$$\sum_{c\in\mathbb{F}_{2^n}^\star} \mathrm{BCT}_F(c,b) = \sum_{c\in\mathbb{F}_{2^n}^\star} \#\{x\in\mathbb{F}_{2^n} \mid D_bD_cF^{-1}(x)=0\}$$

$$= \sum_{c\in\mathbb{F}_{2^n}^\star} \mathrm{DDT}_F(c,b)^2 - 2^n.$$

Proof Let a and b be in $\mathbb{F}_{2^n}^\star$. According to (3)

$$\sum_{c\in\mathbb{F}_{2^n}^\star} \mathrm{BCT}_F(a,c) = \sum_{c\in\mathbb{F}_{2^n}^\star}\sum_{\gamma\in\mathbb{F}_{2^n}^\star} \#\{x\in\mathbb{F}_{2^n} \mid D_\gamma F(x) = D_\gamma F(x+a) = c\}$$

$$= \sum_{\gamma\in\mathbb{F}_{2^n}^\star} \#\{x\in\mathbb{F}_{2^n} \mid D_\gamma F(x) = D_\gamma F(x+a)\}.$$

Here we have used the fact that $D_\gamma F(x)\neq 0$ for any $x\in\mathbb{F}_{2^n}$ and $\gamma\in\mathbb{F}_{2^n}^\star$ since F is a permutation. Now, the identity (4) follows immediately from the fact that $D_\gamma F(x) = D_\gamma F(x+a)$ if and only if $D_aD_\gamma F(x)=0$.

As for (5), first we observe

$$\begin{aligned}
&\sum_{c\in\mathbb{F}_{2^n}} \mathrm{BCT}_F(a,c)\\
&= \sum_{c\in\mathbb{F}_{2^n}} \#\left\{(x,y)\in(\mathbb{F}_{2^n})^2 : \begin{array}{l} F(x)+F(y)=c\\ F(x+a)+F(y+a)=c\end{array}\right\}\\
&= \#\left\{(x,y)\in(\mathbb{F}_{2^n})^2 : F(x)+F(y) = F(x+a)+F(y+a)\right\}\\
&= \sum_{c\in\mathbb{F}_{2^n}} \#\left\{(x,y)\in(\mathbb{F}_{2^n})^2 : \begin{array}{l} F(x)+F(x+a)=c\\ F(y)+F(y+a)=c\end{array}\right\} = \sum_{c\in\mathbb{F}_{2^n}} \mathrm{DDT}_F(a,c)^2.
\end{aligned}$$

Noting that $\mathrm{BCT}_F(a,0)=2^n$ and $\mathrm{DDT}_F(a,0)=0$, we obtain the desired identity. The proof of the second assertion is similar, by using $\mathrm{BCT}_F(c,b) = \mathrm{BCT}_{F^{-1}}(b,c)$. This completes the proof of Theorem 1. $\square$

4 On the boomerang uniformity of quadratic permutations

In this section, we specialize our study of boomerang uniformity to quadratic permutations in even dimension. In even dimension, it is known that the best differential uniformity of a quadratic permutation is 4. Note that in even dimension, APN quadratic permutations F do not exist [20]. Therefore, $\Delta(F)=4$ is the lowest differential uniformity that a quadratic permutation F can achieve.

In [2], Boura and Canteaut exhibited a family of quadratic permutations with optimal BCT, i.e. permutations which have differential uniformity and boomerang uniformity both equal to 4. In [19] Li et al. provided another family of quadratic permutations with optimal BCT. These two families of permutations are related to the so-called Gold power permutations [16]. In this section we obtain a vast generalization of these results.

Theorem 5 *Let q be a power of 2 and m be a positive integer. Let $F : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ be a quadratic function of the form*

$$F(x) = \sum_{0 \le i \le j \le m-1} c_{ij} x^{q^i + q^j}, \quad \forall c_{ij} \in \mathbb{F}_{q^m}. \tag{6}$$

Then $\Delta(F) \ge q$. Moreover, if F is a permutation on $\mathbb{F}_{q^m}$ and $\Delta(F) = q$, then $\beta(F) = q$.

Proof For any $\gamma \in \mathbb{F}_{q^m}^{\star}$, let

$$H_\gamma(x) = F(x+\gamma) + F(x) + F(\gamma).$$

We have

$$\begin{aligned} H_\gamma(x) &= \sum_{0 \le i \le j \le m-1} c_{ij} \left((x+\gamma)^{q^i+q^j} + x^{q^i+q^j} + \gamma^{q^i+q^j} \right) \\ &= \sum_{0 \le i < j \le m-1} c_{ij} (x^{q^i} \gamma^{q^j} + x^{q^j} \gamma^{q^i}). \end{aligned}$$

We apply Theorem 4. The set $\mathcal{U}_{\gamma,b}^F$ is given by

$$\mathcal{U}_{\gamma,b}^F = \left\{ x \in \mathbb{F}_{q^m} : H_\gamma(x) = b + F(\gamma) \right\}.$$

Since F is a quadratic function, if $\mathcal{U}_{\gamma,b}^F \neq \emptyset$, that is, $\mathrm{DDT}_F(\gamma, b) > 0$, then $\mathcal{U}_{\gamma,b}^F$ is an affine subspace of $\mathbb{F}_{q^m}$ obtained by a translation of the vector space $K_F(\gamma)$ where

$$K_F(\gamma) = \left\{ x \in \mathbb{F}_{q^m} : H_\gamma(x) = 0 \right\}.$$

It is easy to see that $K_F(\gamma)$ is a vector space over $\mathbb{F}_q$ and $\gamma \cdot \mathbb{F}_q \subset K_F(\gamma)$. Thus we have $\Delta(F) \ge \# K_F(\gamma) \ge q$.

Now suppose that F is a permutation and $\Delta(F) = q$. Then we have

$$K_F(\gamma) = \gamma \cdot \mathbb{F}_q.$$

Thus

$$\mathcal{U}_{\gamma,b}^F \cap (a + \mathcal{U}_{\gamma,b}^F) = \begin{cases} \emptyset & : \text{ if } \mathrm{DDT}_F(\gamma,b) = 0 \text{ or } a \notin \gamma \cdot \mathbb{F}_q, \\ \mathcal{U}_{\gamma,b}^F & : \text{ if } \mathrm{DDT}_F(\gamma,b) > 0 \text{ and } a \in \gamma \cdot \mathbb{F}_q, \end{cases}$$

and from Theorem 4 we have

$$\mathrm{BCT}_F(a,b) = \sum_{\gamma \in \mathbb{F}_q^{\star}} \mathrm{DDT}_F(a\gamma, b). \tag{7}$$

Now suppose there exist $\gamma_1 \neq \gamma_2 \in \mathbb{F}_q^{\star}$ such that

$$\mathrm{DDT}_F(a\gamma_i, b) \neq 0, \quad \forall i = 1, 2,$$

then the equations

$$H_{a\gamma_i}(x) = b + F(a\gamma_i), \quad x \in \mathbb{F}_{q^m}$$

are solvable for both $i = 1, 2$. Noting that for $i = 1, 2$, since $\gamma_i \in \mathbb{F}_q$,

$$H_{a\gamma_i}(x) = \gamma_i H_a(x), \quad F(a\gamma_i) = \gamma_i^2 F(a),$$

we have

$$\frac{b}{\gamma_i} + \gamma_i F(a) \in \mathrm{Im} H_a, \quad i = 1, 2.$$

Here $\mathrm{Im}H_a$ is the image of the function $H_a(x)$ on $\mathbb{F}_{q^m}$. It is easy to see that the set $\mathrm{Im}H_a$ is a vector space over $\mathbb{F}_q$. Thus we have

$$b+\gamma_i^2 F(a) \in \mathrm{Im}H_a, \quad i=1,2,$$

and

$$(b+\gamma_1^2 F(a)) - (b+\gamma_2^2 F(a)) = (\gamma_1-\gamma_2)^2 F(a) \in \mathrm{Im}H_a,$$

and hence $F(a) \in \mathrm{Im}H_a$. However, this means that the equation

$$F(x+a)+F(x)=0$$

is solvable for $x \in \mathbb{F}_{q^m}$, which is impossible because F is a permutation and $a \neq 0$.

So we have proved that in (7) there is at most one $\gamma \in \mathbb{F}_q^\star$ such that $\mathrm{DDT}_F(a\gamma,b) \neq 0$. Noting that actually

$$\mathrm{DDT}_F(a,b) \in \{0,q\} \quad \forall (a,b) \in (\mathbb{F}_{q^m}^\star)^2,$$

we obtain $\mathrm{BCT}_F(a,b) \leq q$ for any $(a,b) \in (\mathbb{F}_{q^m}^\star)^2$. So we conclude that $\beta(F)=q$. This completes the proof of Theorem 5. □

Remark 1 Let F be a quadratic permutation given by (6) with $\Delta(F)=q$. From the proof of Theorem 5, $\mathrm{DDT}_F(a,b) \in \{0,q\}$, where $(a,b) \in (\mathbb{F}_{q^m}^\star)^2$.

We remark that a general quadratic function $F(x)$ of the form (6) may be written as

$$F(x) = f(x) + \phi(x),$$

where

$$f(x) = \sum_{0\leq i<j\leq m-1} c_{ij} x^{q^i+q^j}, \quad \phi(x) = \sum_{0\leq i\leq m-1} c_i x^{2q^i}.$$

Noting that the function ϕ is linear, so $\Delta(F)=\Delta(f)$.

As applications of Theorem 5, we show here how two previous results of quadratic permutations with optimal BCT from [2] and [19] can be derived.

(1). Let $n \equiv 2 \pmod 4$ and let t be an even integer such that $\gcd(t,n)=2$. It was known that the function $F(x)=x^{2^t+1}$ is a permutation on $\mathbb{F}_{2^n}$ and $\Delta(F)=4$ (see [1]). Theorem 5 implies that $\beta(F)=4$. This is [2, Proposition 8].

(2). Let $n=2m$ where m is an odd integer. Let $\gamma \in \mathbb{F}_{2^n}^\star$ be an element such that the order of λ^{2^m-1} is 3. Define $F(x)=x^{2^m+2}+\lambda x$. It was known that $F(x)$ is a permutation on $\mathbb{F}_{2^n}$ with $\Delta(F)=4$ [22]. We may write $F(x)=f(x)^2$ where $f(x)=x^{2^{m-1}+1}+\lambda^{2^{-1}} x^{2^{n-2}+2^{n-2}}$, hence Theorem 5 implies that $\beta(F)=4$. This is [19, Theorem 5.3].

Next we exhibit another family of quadratic permutations with optimal BCT. To this end, we mention that it has been found in [8] a highly nonlinear 4-differential uniform permutation of $\mathbb{F}_{2^n}$ with $n=3k$, $k \equiv 2 \pmod 4$, $3 \nmid k$:

$$F(x) = \beta x^{2^s+1} + \beta^{2^k} x^{2^{-k}+2^{k+s}} \tag{8}$$

where $\gcd(n,s)=2$, $3|k+s$ and β is a primitive element of $\mathbb{F}_{2^n}$. It was proved that $\Delta(F)=4$. So from Theorem 5 we obtain

Corollary 1 *Let F be an (n,n)-function (permutation) defined by (8). Then,* $\beta(F)=4$.

Finally, we show by numerical computation that many new quadratic permutations with optimal BCT can be found by Theorem 5. Here we focus only on the quadratic function $F(x)$ of the form

$$F(x) = x^{2^{s+1}+2} + Ax + Bx^4 + Cx^{16}, \quad A,B,C \in \mathbb{F}_{2^n}, \tag{9}$$

where $n \equiv 2 \pmod 4$ and $\gcd(n,s) = 2$. It was known that $\Delta(F) = 4$. Noting that $F(x) = f(x)^2$ where

$$f(x) = x^{2^s+1} + A^{2^{-1}}x^{2^{n-1}} + B^{2^{-1}}x^2 + C^{2^{-1}}x^8, \quad A,B,C \in \mathbb{F}_{2^n},$$

by Theorem 5, if F is a permutation, then $\beta(F) = 4$. For simplicity we only consider the case $n = 6$ and search via **Magma** triples $(A,B,C) \in (\mathbb{F}_{2^6})^3$ such that F is a permutation, the number of which is given in the tables below. For comparison, we also indicate the number of such F's implied by [2, Proposition 8] and [19, Theorem 5.3]. This really shows that there is a abundance of quadratic permutations with optimal BCT which can be obtained from Theorem 5.

Table 1: The number of quadratic permutations $F(x)$ of the form (9) on $\mathbb{F}_{2^6}$ with optimal BCT

	Theorem 5 (this paper)	[2, Proposition 8]	[19, Theorem 5.3]
$s = 2$	960	1	15

Next, we will present a connection between the boomerang uniformity and the nonlinearity for the quadratic permutation F given by (6). For any function F from $\mathbb{F}_{q^m}$ to itself, the *Walsh transform* of F at $(\lambda,\mu) \in \mathbb{F}_{q^m}^{\star} \times \mathbb{F}_{q^m}$ is defined as

$$\mathcal{W}_F(\lambda,\mu) = \sum_{x \in \mathbb{F}_{q^m}} (-1)^{\mathrm{Tr}(\lambda F(x)+\mu x)},$$

where $\mathrm{Tr}(\cdot)$ is the absolute trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_2$. The *component functions* of F are the Boolean functions $\mathrm{Tr}(\lambda F(x))$, where $\lambda \in \mathbb{F}_{q^m}$. A component function $\mathrm{Tr}(\lambda F(x))$ is said to be *bent* if $\mathcal{W}_F(\lambda,\mu) = \pm q^{\frac{m}{2}}$, for all $\mu \in \mathbb{F}_{q^m}$. In this case, $\mathrm{Tr}(\lambda F(x))$ is also called a *bent component* of F.

The *nonlinearity* $\mathcal{NL}_F$ of F is defined as

$$\mathcal{NL}_F = \frac{1}{2}\left(q^m - \max\left\{|\mathcal{W}_F(\lambda,\mu)| : (\lambda,\mu) \in \mathbb{F}_{q^m}^{\star} \times \mathbb{F}_{q^m}\right\}\right).$$

Theorem 6 *Let $q = 2^t$ and F be a quadratic permutation defined by (6). Then $\beta(F) = 2^t$ if and only if $\mathcal{W}_F(\lambda,\mu) \in \{0, \pm 2^{\frac{tm+t}{2}}\}$, where $(\lambda,\mu) \in \mathbb{F}_{q^m}^{\star} \times \mathbb{F}_{q^m}$. In particular, if $\beta(F) = 2^t$, $\mathcal{NL}_F = \frac{1}{2}\left(2^{tm} - 2^{\frac{tm+t}{2}}\right)$.*

Proof Using Theorem 5, $\beta(F) = 2^t$ is equivalent to $\mathrm{DDT}_F(a,b) \in \{0, 2^t\}$, where $(a,b) \in \mathbb{F}_{q^m}^{\star} \times \mathbb{F}_{q^m}$. Since F is a permutation, F has no bent component. Hence the desired results follow from [14, Theorem 3].

5 Conclusions

We have pushed further the study of boomerang uniformity of cryptographic Sboxes. More specifically, we have presented a slightly different (and more convenient) formulation of the boomerang uniformity and showed that the row sum and the column sum of the boomerang connectivity table can be expressed in terms of the zeros of the second-order derivative of the permutation or its inverse. Most importantly, we have specialized our study of boomerang uniformity to quadratic permutations in even dimension and generalized the previous results on quadratic permutation with optimal BCT. As a consequence of our general result, we derived many new quadratic permutations with optimal BCT. In particular, we showed that the boomerang uniformity of the binomial differentially 4-uniform permutations presented by Bracken, Tan, and Tan equals 4. Finally, we derived a connection between the boomerang uniformity and the nonlinearity for some special quadratic permutations.

Acknowledgement. We thank Nian Li and Haode Yan for their interesting discussions in Hong Kong. C. Tang was supported by National Natural Science Foundation of China (Grant No. 11871058) and China West Normal University (14E013, CXTD2014-4 and the Meritocracy Research Funds). M. Xiong was supported by The Hong Kong Research Grants Council, Project No. NHKUST619/17.

References

1. Celine Blondeau, Anne Canteaut, Pascale Charpin. Differential properties of power functions. Int. J. Inf. Coding Theory, 1 (2) (2010) 149-170.
2. Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3), pages 290-310, Sep. 2018.
3. Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, EUROCRYPT 2001, volume 2045 of LNCS, pages 340-357. Springer, Heidelberg, May 2001.
4. Eli Biham, Orr Dunkelman, and Nathan Keller. New results on boomerang and rectangle attacks. In Joan Daemen and Vincent Rijmen, editors, FSE 2002, volume 2365 of LNCS, pages 1-16. Springer, Heidelberg, February 2002.
5. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, CRYPTO'90, volume 537 of LNCS, pages 2-21. Springer, Heidelberg, August 1991.
6. Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of SAFER++. In Dan Boneh, editor, CRYPTO 2003, volume 2729 of LNCS, pages 195-211. Springer, Heidelberg, August 2003.
7. Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, ASIACRYPT 2009, volume 5912 of LNCS, pages 1-18. Springer, Heidelberg, December 2009.
8. Carl Bracken, Chik How Tan, and Yin Tan. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields and Their Applications*, 18(3), pages 537-546, 2012.
9. Christina Boura, Leo Perrin, and Shizhu Tian. Boomerang Uniformity of Popular S-box Constructions. Proceedings of The Eleventh International Workshop on Coding and Cryptograph (WCC) 2019.
10. Claude Carlet. Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, In Crama, Y., Hammer, P., (eds), pp. 257–397. Cambridge University Press, 2010.
11. Claude Carlet. Vectorial Boolean Functions for Cryptography, Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Crama, Y., Hammer, P., (eds), pp. 398–469, Cambridge University Press, 2010.
12. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. Des. Codes Cryptography, 15(2), pages 125-156, 1998.
13. Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 683-714, Cham, 2018. Springer International Publishing.

14. Pascale Charpin and Jie Peng. New links between nonlinearity and differential uniformity. Finite Fields and Their Applications, Elsevier, 56, pp.188-208, 2019.
15. Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, CRYPTO 2010, volume 6223 of LNCS, pages 393-410. Springer, –Heidelberg, August 2010.
16. Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inform. Theory, 14(1):154-156, 1968.
17. John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, FSE 2000,
18. Jongsung Kim, Seokhie Hong, Bart Preneel, Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. IEEE Trans. Information Theory, 58(7):4948-4966, 2012.
19. Kangquan Li, Longjiang Qu, Bing Sun, and Chao Li. New results about the boomerang uniformity of permutation polynomials. Cryptology ePrint Archive, Report 2019/079, 2019. https://eprint.iacr.org/2019/079.
20. Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In Bart Preneel, editor, FSE'94, volume 1008 of LNCS, pages 111-130. Springer, Heidelberg, December 1995.
21. Ling Song, Xianrui Qi, and Lei Hu. Boomerang Connectivity Table Revisited-Application to SKINNY and AES. *https://eprint.iacr.org/2019/146.pdf*
22. Michael E. Zieve. Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, *arXiv: 1312.1325v3, 2013*.
23. David Wagner. The boomerang attack. In Lars R. Knudsen, editor, FSE'99, volume 1636 of LNCS, pages 156-170. Springer, Heidelberg, March 1999.