A Class of Power Mappings with Low Boomerang Uniformity

Haode Yan[1], Ziying Zhang[1(✉)], and Zhengchun Zhou[2]

[1] School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China
hdyan@swjtu.edu.cn,
zzy.swjtu.edu.cn@my.swjtu.edu.cn
[2] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China
zzc@swjtu.edu.cn

Abstract. Let $f(x) = x^{\frac{q-3}{2}}$ be a power mapping over $\mathbb{F}_q$, where q is an odd prime power. The differential uniformity of f was determined by Helleseth and Sandberg [14] in 1997. In this paper, we study the boomerang uniformity of f via its differential properties. It is shown that f has low boomerang uniformity when $q \equiv 3 \pmod 4$.

Keywords: Power function · Differential uniformity · Boomerang uniformity

1 Introduction

Substitution boxes (S-boxes for short) play a crucial role in the field of symmetric block ciphers. Let $\mathbb{F}_q$ be the finite field with q elements. For a function f from $\mathbb{F}_q$ to itself, the main tools to handle f regarding the differential attack are the difference distribution table (DDT for short) introduced by Biham and Shamir [2] and the differential uniformity which was introduced by Nyberg [21] in 1994. For any $a, b \in \mathbb{F}_q$, the DDT entry at point (a, b), denoted by $\delta_f(a, b)$, is defined as

$$\delta_f(a,b) = \big|\{x \in \mathbb{F}_q : \ f(x+a) - f(x) = b\}\big|,$$

where $|S|$ denotes the cardinality of the set S. The differential uniformity of the function f, denoted by δ_f, is defined as

$$\delta_f = \max\{\delta_f(a,b) : \ a \in \mathbb{F}_q^*, \ b \in \mathbb{F}_q\},$$

where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. When f is used as an S-box inside a cryptosystem, the smaller the value δ_f is, the better the contribution of f to the resistance against differential attack. When $\delta_f = 1$ (respectively, $\delta_f = 2$), the function f is called a perfect nonlinear (PN) function (respectively, an almost perfect nonlinear (APN) function). The recent results on cryptographic functions with low differential

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
S. Mesnager and Z. Zhou (Eds.): WAIFI 2022, LNCS 13638, pp. 288–297, 2023.
https://doi.org/10.1007/978-3-031-22944-2_18

uniformity can be found in [1,3,5,6,13,18,22,23,25,27,29,30,34] and their references. More precisely, the readers can refer to a recent monograph [8], Chapter 11, which is written by Carlet.

Another important cryptanalytical technique on block ciphers is the boomerang attack introduced by Wagner [28], which is a variant of differential cryptanalysis. In order to analyze the boomerang attack of block ciphers in a better way, analogous to the DDT concerning differential attack, Cid *et al*. [9] firstly proposed the boomerang connectivity table (BCT). Let f be a permutation from $\mathbb{F}_{2^n}$ to itself. For $a, b \in \mathbb{F}_{2^n}$, the BCT entry at point (a, b), denoted by $\beta_f(a, b)$, is defined as

$$\beta_f(a,b) = \left|\{x \in \mathbb{F}_{2^n} : \ f^{-1}(f(x+a)+b) + f^{-1}(f(x)+b) = a\}\right|.$$

Further, to quantify the resistance of a function against the boomerang attack, Boura and Canteaut [4] introduced the concept of boomerang uniformity, which is the maximum value in the BCT excluding the first row and the first column. That is, the boomerang uniformity of the permutation f, denoted by β_f, is given by

$$\beta_f = \max\left\{\beta_f(a,b) : \ a, b \in \mathbb{F}_q^*\right\}.$$

Similarly, the smaller the value β_f is, the better the contribution of f to the resistance against boomerang attack. Recently, Li *et al*. in [16] generalized the definition of $\beta_f(a, b)$ for any function f (not necessarily being a permutation) over $\mathbb{F}_q$. The BCT entry of f at point (a, b), denoted by $\beta_f(a, b)$, is the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following system of equations

$$\begin{cases} f(x) - f(y) &= b, \\ f(x+a) - f(y+a) &= b, \end{cases}$$

where $a, b \in \mathbb{F}_q^*$. The research on cryptographic functions with low boomerang uniformity has been a hot issue in recent years, see for example [4,9,11,16,17, 20,26,33]. More precisely, for recent progress of cryptographic functions with known boomerang uniformity, the readers can refer to the survey article [19], which is written by Mesnager, Mandal and Msahli.

Power functions with low differential uniformity serve as good candidates for the design of S-boxes not only because of their strong resistance to differential attacks but also for the usually low implementation cost in hardware. The differential properties of power functions can be studied more easily due to their particular algebraic structures. Hence, the study on the boomerang uniformity of power mappings attracts a lot of attention. More precisely, when f is a power function, i.e., $f(x) = x^d$ for an integer d, one easily sees that $\beta_f(a, b) = \beta_f(1, \frac{b}{a^d})$ for any $a, b \in \mathbb{F}_q^*$. The boomerang properties of f are completely determined by the values of $\beta_f(1, b)$ as b runs through $\mathbb{F}_q^*$. Equivalently, we need to consider the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following equation system

$$\begin{cases} x^d - y^d &= b \\ (x+1)^d - (y+1)^d &= b \end{cases}$$

for $b \in \mathbb{F}_q^*$. Although the power functions have good algebraic structures, there are only a few classes of power mappings with known boomerang uniformity in the literature. We list them in Table 1.

In this paper, we mainly study the boomerang uniformity of the power mapping $x^{\frac{q-3}{2}}$ over $\mathbb{F}_q$ via its differential properties, where $q \equiv 3 \pmod 4$ is an odd prime power. The rest of this paper is organized as follows. Section 2 first introduces some frequently-used notation, and then gives some lemmas which will be used later. Section 3 investigates the boomerang uniformity of $x^{\frac{q-3}{2}}$. Section 4 concludes this paper.

Table 1. Power functions with known boomerang uniformity over $\mathbb{F}_{p^n}$

p	d	Conditions	β_f	Reference
2	2^n-2	$n \equiv 2 \pmod 4$	4	[4]
2	2^n-2	$n \equiv 0 \pmod 4$	6	[4]
2	2^k+1	$e=\gcd(n,k)$, n/e is odd	2^e	[10,12]
2	2^k-1	$\gcd(n,k)=1$, δ_f is not a power of 2	$\delta_f \le \beta_f \le 2\delta_f-2$	[33]
2	2^m-1	$n=2m$, m be odd (resp. even)	2 (resp. 4)	[11]
2	$2^{m+1}-1$	$n=2m$, $m \ge 2$	2^m+2	[32]
2	$2^{2k}+2^k+1$	$n=4k$, k is odd	$\le$24	[7]
3	$\frac{3^n+3}{2}$	n is odd	3	[15]
odd	p^n-2	any n	$\le$5	[15]
odd	p^k+1	$e=\gcd(n,k)$, n/e is odd	p^e	[24]
odd	p^k+1	$e=\gcd(n,k)$, n/e is even	$p^e(p^e-1)$	[24]
odd	p^m-1	$n=2m$, $p^m \not\equiv 2 \pmod 3$	2	[31]
odd	$\frac{(p^m-1)(p^m+3)}{2}$	$n=2m$, $p^m \not\equiv 2 \pmod 3$, $p^m \equiv 3 \pmod 4$	2	[31]
odd	$\frac{p^n-3}{2}$	$p^n \equiv 3 \pmod 4$, 5 is a nonsquare	$\le$4	This paper
odd	$\frac{p^n-3}{2}$	$p^n \equiv 3 \pmod 4$, 5 is a square	$\le$6	This paper

2 Preliminaries

In this section, we introduce some frequently-used notation in this paper and give some lemmas which will be used in the following.

- q is an odd prime power.
- $\mathbb{F}_q$ is the finite field with q elements.
- Let $f(x)=x^{\frac{q-3}{2}}$ be a power mapping over $\mathbb{F}_q$.
- $\Delta(x)=f(x+1)-f(x)=(x+1)^{\frac{q-3}{2}}-x^{\frac{q-3}{2}}$.

- For any $b \in \mathbb{F}_q$, let $\Delta^{-1}(b) = \{x : \Delta(x) = b\}$ and $\delta(b) = |\Delta^{-1}(b)|$.
- Let $\chi(\cdot)$ be the quadratic multiplicative character over $\mathbb{F}_q^*$, i.e., for any $x \in \mathbb{F}_q^*$,

$$\chi(x) = x^{\frac{q-1}{2}} = \begin{cases} 1, & \text{if } x \text{ is a square element,} \\ -1, & \text{if } x \text{ is a nonsquare element.} \end{cases}$$

- For $i, j \in \{1, -1\}$, we define

$$C_{i,j} = \{x \in \mathbb{F}_q \backslash \{0, -1\} : \chi(x) = i \text{ and } \chi(x+1) = j\}.$$

The differential uniformity of f was determined by Helleseth and Sandberg in [14]. We have the following theorem.

Theorem 1. *Let $q \equiv 3 \pmod 4$ be a prime power. For $q > 7$, the differential uniformity of $f(x) = x^{\frac{q-3}{2}}$ is given by*

$$\delta_f = \begin{cases} 1, & \text{if } q = 27, \\ 2, & \text{if } \chi(5) = -1, \\ 3, & \text{if } \chi(5) = 1. \end{cases}$$

Moreover, the following lemma was shown in the proof of Theorem 1 in [14].

Lemma 1. *Let $q \equiv 3 \pmod 4$ be a prime power. With the notation introduced as above, we have*

- *(i) $\Delta^{-1}(0) = \{-\frac{1}{2}\}$ and $\delta(0) = 1$.*
- *(ii) If $\chi(5) = -1$, then $\Delta^{-1}(1) = \{0\}$, $\Delta^{-1}(-1) = \{-1\}$ and $\delta(1) = \delta(-1) = 1$.*
- *(iii) If $\chi(5) = 1$, then $\delta(b) = 3$ if and only if $b = \pm 1$. Moreover, $\Delta^{-1}(1) = \{0, \frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\}$, $\Delta^{-1}(-1) = \{-1, \frac{-\sqrt{5}-1}{2}, \frac{-\sqrt{5}-3}{2}\}$ with $\chi(\frac{-1+\sqrt{5}}{2}) = -1$, $\Delta^{-1}(1) = \{0, \frac{-\sqrt{5}-1}{2}, \frac{1-\sqrt{5}}{2}\}$, $\Delta^{-1}(-1) = \{-1, \frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}-3}{2}\}$ with $\chi(\frac{-1+\sqrt{5}}{2}) = 1$.*
- *(iv) For $b \neq \pm 1$, we have $\delta(b) \leq 2$. More precisely, if $\delta(b) = 2$, i.e., the equation $\Delta(x) = b$ has two distinct solutions, namely x_1 and x_2, then one of x_1 and x_2 is in $C_{1,1} \cup C_{-1,-1}$, and the other is in $C_{1,-1} \cup C_{-1,1}$.*

3 The Boomerang Uniformity of the Power Function $x^{\frac{q-3}{2}}$ Over $\mathbb{F}_q$

In this section, we investigate the boomerang uniformity of the power mapping f via its differential properties. We denote by β_f the boomerang uniformity of f. Our main result is shown as follows.

Theorem 2. *Let q be an odd prime power with $q \equiv 3 \pmod 4$. For $q \neq 7$ and $q \neq 27$, we have,*

$$\beta_f \leq \begin{cases} 4, & \text{if } \chi(5) = -1, \\ 6, & \text{if } \chi(5) = 1. \end{cases}$$

Proof. For any $b \in \mathbb{F}_q^*$, we consider the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the following equation system

$$\begin{cases} x^{\frac{q-3}{2}} - y^{\frac{q-3}{2}} & = b, \\ (x+1)^{\frac{q-3}{2}} - (y+1)^{\frac{q-3}{2}} & = b. \end{cases} \tag{1}$$

If (x, y) is a solution of (1), we have $x \neq y$ since $b \neq 0$. Moreover, we have $\Delta(x) = \Delta(y)$ from (1).We assert that $\delta(\Delta(x)) = 2$ or 3 by Lemma 1 and $x \neq y$. We discuss in the following two cases.

Case 1. $\delta(\Delta(x)) = 2$. It is clear that $\Delta(x) \neq \pm 1$ by Lemma 1, then we have $x, y \neq 0, -1$. The equation system (1) becomes

$$\begin{cases} \chi(x)x^{-1} - \chi(y)y^{-1} & = b, \\ \chi(x+1)(x+1)^{-1} - \chi(y+1)(y+1)^{-1} & = b. \end{cases} \tag{2}$$

By Lemma 1 (iv), for each $x \in C_{i,j}$, $i, j \in \{1, -1\}$, there are two possible sets of y. We have the following 8 subcases, which we summarize in Table 2.

Table 2. Eight subcases from equation system (2)

	(x, y)	Equation system
I	$(x, y) \in C_{1,1} \times C_{1,-1}$	$\begin{cases} x^{-1} - y^{-1} = b, \\ (x+1)^{-1} + (y+1)^{-1} = b. \end{cases}$
II	$(x, y) \in C_{1,1} \times C_{-1,1}$	$\begin{cases} x^{-1} + y^{-1} = b, \\ (x+1)^{-1} - (y+1)^{-1} = b. \end{cases}$
III	$(x, y) \in C_{1,-1} \times C_{1,1}$	$\begin{cases} x^{-1} - y^{-1} = b, \\ -(x+1)^{-1} - (y+1)^{-1} = b. \end{cases}$
IV	$(x, y) \in C_{1,-1} \times C_{-1,-1}$	$\begin{cases} x^{-1} + y^{-1} = b, \\ -(x+1)^{-1} + (y+1)^{-1} = b. \end{cases}$
V	$(x, y) \in C_{-1,1} \times C_{1,1}$	$\begin{cases} -x^{-1} - y^{-1} = b, \\ (x+1)^{-1} - (y+1)^{-1} = b. \end{cases}$
VI	$(x, y) \in C_{-1,1} \times C_{-1,-1}$	$\begin{cases} -x^{-1} + y^{-1} = b, \\ (x+1)^{-1} + (y+1)^{-1} = b. \end{cases}$
VII	$(x, y) \in C_{-1,-1} \times C_{1,-1}$	$\begin{cases} -x^{-1} - y^{-1} = b, \\ -(x+1)^{-1} + (y+1)^{-1} = b. \end{cases}$
VIII	$(x, y) \in C_{-1,-1} \times C_{-1,1}$	$\begin{cases} -x^{-1} + y^{-1} = b, \\ -(x+1)^{-1} - (y+1)^{-1} = b. \end{cases}$

Subcase I. $(x, y) \in C_{1,1} \times C_{1,-1}$. After a simple calculation, we obtain two quadratic equations as follows.

$$\begin{cases} b(b-2)x^2 + (b^2 - 4b + 2)x - (b-2) & = 0, \quad (3) \\ b^2(y+1)^2 - (b^2+2)(y+1) + b & = 0. \quad (4) \end{cases}$$

It is easy to see that $b \neq 2$ and $b \neq 0$, otherwise, we have $x = 0$ or $y = -1$, a contradiction. If (3) has two solutions, namely x_1 and x_2, then $x_1x_2 = -\frac{1}{b}$. We mention that -1 is a nonsquare element. When b is a square element, then $\chi(x_1x_2) = -1$, and at most one of x_1 and x_2 satisfies $x \in C_{1,1}$. Similarly, if (4) has two solutions, namely y_1 and y_2, then $(y_1 + 1)(y_2 + 1) = \frac{1}{b}$. When b is a nonsquare element, then $\chi((y_1 + 1)(y_2 + 1)) = -1$, and at most one of y_1 and y_2 satisfies $y \in C_{1,-1}$. By a discussion as above, we conclude that for any $b \in \mathbb{F}_q^*$, this subcase contributes at most 1 solution.

Subcase II. $(x, y) \in C_{1,1} \times C_{-1,1}$. In this subcase, we obtain two quadratic equations as follows.

$$\begin{cases} b(b+2)(x+1)^2 - (b^2+4b+2)(x+1) + b + 2 = 0, & (5) \\ b^2y^2 + (b^2+2)y - b = 0. & (6) \end{cases}$$

It is easy to see that $b \neq -2$ and $b \neq 0$. If (5) (respectively, (6)) has two solutions, namely x_1 and x_2 (respectively, y_1 and y_2), then $(x_1 + 1)(x_2 + 1) = \frac{1}{b}$ (respectively, $y_1y_2 = -\frac{1}{b}$). By a similar proof as for subcase I, we conclude that for any $b \in \mathbb{F}_q^*$, this subcase contributes at most 1 solution.

Subcase III. $(x, y) \in C_{1,-1} \times C_{1,1}$. We obtain two quadratic equations as follows.

$$\begin{cases} b^2(x+1)^2 - (b^2+2)(x+1) - b = 0, \\ b(b+2)y^2 + (b^2+4b+2)y + b + 2 = 0. \end{cases}$$

Similar to the proof of subase I, this subcase contributes at most 1 solution.

Subcase IV. $(x, y) \in C_{1,-1} \times C_{-1,-1}$. Since $\frac{q-3}{2}$ is even, then (x, y) is a solution of (1) if and only if $(-x-1, -y-1)$ is a solution of (1). For any $y \in \mathbb{F}_q \setminus \{0, -1\}$, $y \in C_{1,1}$ if and only if $-y - 1 \in C_{-1,-1}$, $y \in C_{1,-1}$ (respectively, $C_{-1,1}$) if and only if $-y - 1 \in C_{1,-1}$ (respectively, $C_{-1,1}$). We conclude that the number of the solutions in this subcase is the same to that of subcase III.

Subcase V. $(x, y) \in C_{-1,1} \times C_{1,1}$. We obtain two quadratic equations as follows.

$$\begin{cases} b^2x^2 + (b^2+2)x + b = 0, & (7) \\ b(b-2)(y+1)^2 - (b^2-4b+2)(y+1) - (b-2) = 0. & (8) \end{cases}$$

Similar to the proof of subcase I, this subcase contributes at most 1 solution.

For subcases VI, VII and VIII, we assert that the numbers of solutions in subcases VI and V (respectively, subcases VII and I, subcases VIII and II) are the same, similar to subcases IV and III. We conclude that the equation system (2) has at most one solution in each subcase.

Next we show that the equation system (2) cannot have solutions in subcase I and subcase V simultaneously. Otherwise, let $(x_1, y_1) \in C_{1,1} \times C_{1,-1}$ be a solution of (2) in subcase I and $(u_1, v_1) \in C_{-1,1} \times C_{1,1}$ be a solution of (2) in subcase V. Then

$$\chi(x_1) = 1,\ \chi(x_1 + 1) = 1,\ \chi(y_1) = 1,\ \chi(y_1 + 1) = -1,$$

and

$$\chi(u_1) = -1,\ \chi(u_1+1) = 1,\ \chi(v_1) = 1,\ \chi(v_1+1) = 1.$$

When we discard the condition on the values of the quadratic character, there is the other solution (x_2, y_2) (respectively, (u_2, v_2)) of equations (3) and (4) (respectively, (7) and (8)). Considering quadratic equations (3) and (8), only one of their coefficients has a different sign. More precisely, we have

$$x_1 + x_2 = -\frac{b^2 - 4b + 2}{b(b-2)} = -((v_1+1) + (v_2+1))$$

and

$$x_1 x_2 = -\frac{1}{b} = (v_1+1)(v_2+1).$$

Then $x_1 = -(v_2+1)$ and $x_2 = -(v_1+1)$ since $x_1, v_1 \in C_{1,1}$. Consequently,

$$\chi(b) = \chi(\frac{1}{b}) = \chi(-(v_1+1)(v_2+1)) = \chi(v_1+1)\chi(x_1) = \chi(x_1) = 1.$$

Similarly, considering quadratic equations (4) and (7), we have

$$u_1 + u_2 = -\frac{b^2+2}{b^2} = -((y_1+1) + (y_2+1))$$

and

$$u_1 u_2 = \frac{1}{b} = (y_1+1)(y_2+1).$$

Then $u_1 = -(y_2+1)$ and $u_2 = -(y_1+1)$ since $u_1 \in C_{-1,1}$ and $y_1 \in C_{1,-1}$. Hence

$$\chi(b) = \chi(\frac{1}{b}) = \chi((y_1+1)(y_2+1)) = \chi(-(y_1+1)u_1) = -\chi(y_1+1)\chi(u_1) = -1,$$

which is a contradiction. Therefore, for any $b \in \mathbb{F}_q^*$, subcase I and subcase V cannot give solutions simultaneously, so they contribute at most one solution altogether. Similarly, subcases II and III contribute at most one solution altogether. That is to say, for any $b \in \mathbb{F}_q^*$, there are at most four solutions of (1) in this case.

Case 2. $\delta(\Delta(x)) = 3$. By Lemma 1, we know that this case only occurs when $\chi(5) = 1$ and $\Delta(x) = \pm 1$. Note that $\frac{-1+\sqrt{5}}{2} \cdot \frac{-1-\sqrt{5}}{2} = -1$, without loss of generality, we assume that $\chi(\frac{-1+\sqrt{5}}{2}) = -1$. Then we can obtain $\Delta^{-1}(1) = \{0, \frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\}$ and $\Delta^{-1}(-1) = \{-1, -\frac{\sqrt{5}+1}{2}, -\frac{\sqrt{5}+3}{2}\}$ by Lemma 1 (iii).

We can list all possible pairs (x, y) with $\Delta(x) = \Delta(y) = \pm 1$. Plugging all pairs (x, y) into the first equation of the system (1), the corresponding b's are obtained. We have the following table (Table 3).

Table 3. The Solutions of $\Delta(x) = \Delta(y) = \pm 1$ and Corresponding b

(x, y) with $\Delta(x) = \Delta(y) = \pm 1$	The Corresponding b
$(0, \frac{\sqrt{5}-1}{2}), (-1, \frac{-\sqrt{5}-1}{2})$	$b = \frac{\sqrt{5}+1}{2}$
$(\frac{\sqrt{5}-1}{2}, 0), (\frac{-\sqrt{5}-1}{2}, -1)$	$b = -\frac{\sqrt{5}+1}{2}$
$(0, \frac{\sqrt{5}+1}{2}), (-1, \frac{-\sqrt{5}-3}{2})$	$b = \frac{\sqrt{5}-1}{2}$
$(\frac{\sqrt{5}+1}{2}, 0), (\frac{-\sqrt{5}-3}{2}, -1)$	$b = -\frac{\sqrt{5}-1}{2}$
$(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}), (\frac{-\sqrt{5}-1}{2}, \frac{-\sqrt{5}-3}{2})$	$b = 1$
$(\frac{\sqrt{5}+1}{2}, \frac{\sqrt{5}-1}{2}), (\frac{-\sqrt{5}-3}{2}, \frac{-\sqrt{5}-1}{2})$	$b = -1$

It is obvious that, for each $b \in \{\pm 1, \ \pm \frac{\sqrt{5}+1}{2}, \ \pm \frac{\sqrt{5}-1}{2}\}$, the equation system (1) has two solutions in this case. For $b \in \mathbb{F}_q^* \backslash \{\pm 1, \ \pm \frac{\sqrt{5}+1}{2}, \ \pm \frac{\sqrt{5}-1}{2}\}$ the equation system (1) has no solution in this case. Note that Case 2 only occurs when $\chi(5) = 1$, the desired results follow.

Remark 1. By making a computer investigation, we have the boomerang uniformity of f is equal to 4 with $q = 3^5$. In addition, the boomerang uniformity of f is equal to 6 with $q = 131$. Therefore, we can conclude that our bound is tight.

4 Conclusion

In this paper, we mainly study the boomerang uniformity of the power function $x^{\frac{q-3}{2}}$ over $\mathbb{F}_q$ via their differential properties, where $q \equiv 3 \pmod 4$ is an odd prime power. It is shown that the power function has low boomerang uniformity. We mention that our approach may be used in determining the boomerang uniformity of other power mappings. It is worthy finding applications of power mappings with low boomerang uniformity in sequence designs, coding theory and combinatorial designs.

Acknowledgements. The authors would like to thank the anonymous reviewers for giving us invaluable comments and suggestions that greatly improved the quality of this paper. H. Yan's research was supported by the Natural Science Foundation of Sichuan (Grant No. 2022NSFSC1805) and the Fundamental Research Funds for the Central Universities of China (Grant No. 2682021ZTPY076).

References

1. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 65–76. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_7

2. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
3. Blondeau, C., Perrin, L.: More differentially 6-uniform power functions. Des. Codes Cryptogr. **73**(2), 487–505 (2014). https://doi.org/10.1007/s10623-014-9948-2
4. Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic Sboxes. IACR Transactions on Symmetric Cryptology, pp. 290–310 (2018)
5. Budaghyan, L., Carlet, C., Helleseth, T., Li, N., Sun, B.: On upper bounds for algebraic degrees of APN functions. IEEE Trans. Inf. Theory **64**(6), 4399–4411 (2017)
6. Budaghyan, L., Carlet, C., Leander, G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inf. Theory **54**(9), 4218–4229 (2008)
7. Calderini, M., Villa, I.: On the boomerang uniformity of some permutation polynomials. Cryptogr. Commun. **12**(6), 1161–1178 (2020). https://doi.org/10.1007/s12095-020-00439-x
8. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021)
9. Cid, C., Huang, T., Peyrin, T., Sasaki, Yu., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 683–714. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_22
10. Eddahmani, S., Mesnager, S.: Explicit values of the tables DDT, BCT, FBCT, and FBDT of the inverse, the gold, and the Bracken-Leander functions
11. Hasan, S.U., Pal, M., Stănică, P.: Boomerang uniformity of a class of power maps. Des. Codes Cryptogr. **89**(11), 2627–2636 (2021). https://doi.org/10.1007/s10623-021-00944-x
12. Hasan, S., Pal, M., Stănică, P.: The binary gold function and its c-boomerang connectivity table. Cryptogr. Commun., 1–24 (2022)
13. Helleseth, T., Rong, C., Sandberg, D.: New families of almost perfect nonlinear power mappings. IEEE Trans. Inf. Theory **45**(2), 475–485 (1999)
14. Helleseth, T., Sandberg, D.: Some power mappings with low differential uniformity. Appl. Algebra Eng. Commun. Comput. **8**(5), 363–370 (1997)
15. Jiang, S., Li, K., Li, Y., Qu, L.: Differential and boomerang spectrums of some power permutations. Cryptogr. Commun. **14**(2), 371–393 (2021). https://doi.org/10.1007/s12095-021-00530-x
16. Li, K., Qu, L., Sun, B., Li, C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inf. Theory **65**(99), 7542–7553 (2019)
17. Li, N., Hu, Z., Xiong, M., Zeng, X.: 4-uniform BCT permutations from generalized butterfly structure. arXiv preprint arXiv:2001.00464 (2020)
18. Li, Y., Wang, M.: Constructing differentially 4-uniform permutations over $\mathbb{GF}(2^{2m})$ from quadratic APN permutations over $\mathbb{GF}(2^{2m+1})$. Des. Codes Cryptogr. **72**(2), 249–264 (2014)
19. Mesnager, S., Mandal, B., Msahli, M.: Survey on recent trends towards generalized differential and boomerang uniformities. Cryptogr. Commun., 1–45 (2021)
20. Mesnager, S., Tang, C., Xiong, M.: On the boomerang uniformity of quadratic permutations. Des. Codes Cryptogr. **88**(10), 2233–2246 (2020). https://doi.org/10.1007/s10623-020-00775-2
21. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_6
22. Qu, L., Tan, Y., Li, C., Gong, G.: More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. Des. Codes Cryptogr. **78**(2), 391–408 (2016)

23. Qu, L., Tan, Y., Tan, C., Li, C.: Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Inf. Theory **59**(7), 4675–4686 (2013)
24. Stănică, P.: Using double Weil sums in finding the c-boomerang connectivity table for monomial functions on finite fields. Applicable Algebra in Engineering, Communication and Computing, pp. 1–22 (2021)
25. Tang, D., Carlet, C., Tang, X.: Differentially 4-uniform bijections by permuting the inverse function. Des. Codes Cryptogr. **77**(1), 117–141 (2015)
26. Tu, Z., Li, N., Zeng, X., Zhou, J.: A class of quadrinomial permutations with boomerang uniformity four. IEEE Trans. Inf. Theory **66**(6), 3753–3765 (2020)
27. Tu, Z., Zeng, X.: Non-monomial permutations with differential uniformity six. J. Syst. Sci. Complex. **31**(4), 1078–1089 (2018)
28. Wagner, D.: The boomerang attack. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_12
29. Xiong, M., Yan, H.: A note on the differential spectrum of a differentially 4-uniform power function. Finite Fields Their Appl. **48**, 117–125 (2017)
30. Xiong, M., Yan, H., Yuan, P.: On a conjecture of differentially 8-uniform power functions. Des. Codes Cryptogr. **86**(8), 1601–1621 (2018)
31. Yan, H., Li, Z., Song, Z., Feng, R.: Two classes of power mappings with boomerang uniformity 2. Adv. Math. Commun. (2022)
32. Yan, H., Zhang, Z., Li, Z.: Boomerang spectrum of a class of power functions. In: International Workshop on Signal Design and its Applications in Communications (IWSDA), pp. 1–4 (2022)
33. Zha, Z., Hu, L.: The boomerang uniformity of power permutations x^{2^k-1} over $\mathbb{F}_{2^n}$. In: 2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA), pp. 1–4. IEEE (2019)
34. Zha, Z., Hu, L., Sun, S.: Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields Their Appl. **25**, 64–78 (2014)