New Results about the Boomerang Uniformity of Permutation Polynomials

Kangquan Li, Longjiang Qu, Bing Sun and Chao Li

Abstract

In EUROCRYPT 2018, Cid et al. [16] introduced a new concept on the cryptographic property of S-boxes: Boomerang Connectivity Table (BCT for short) for evaluating the subtleties of boomerang-style attacks. Very recently, BCT and the boomerang uniformity, the maximum value in BCT, were further studied by Boura and Canteaut [4]. Aiming at providing new insights, we show some new results about BCT and the boomerang uniformity of permutations in terms of theory and experiment in this paper. Firstly, we present an equivalent technique to compute BCT and the boomerang uniformity, which seems to be much simpler than the original definition from [16]. Secondly, thanks to Carlet's idea [15], we give a characterization of functions f from $\mathbb{F}_2^n$ to itself with boomerang uniformity δ_f by means of the Walsh transform. Thirdly, by our method, we consider boomerang uniformities of some specific permutations, mainly the ones with low differential uniformity. Finally, we obtain another class of 4-uniform BCT permutation polynomials over $\mathbb{F}_{2^n}$, which is the first binomial.

Index Terms

Finite Field, Boomerang Connectivity Table, Boomerang Uniformity, Permutation Polynomial

1. Introduction

Let p be a prime, n any positive integer. We denote by $\mathbb{F}_{p^n}$ the finite field with p^n elements and by $\mathbb{F}_p^n$ the n-dimensional vector space over $\mathbb{F}_p$. For any set E, we denote the nonzero elements of E by $E\backslash\{0\}$ or E^*. In this paper, we always identify the vector space $\mathbb{F}_p^n$ with $\mathbb{F}_{p^n}$ and consider functions from $\mathbb{F}_p^n$ to itself as polynomials over $\mathbb{F}_{p^n}$ for convenience. A polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is called a *permutation polynomial* if the induced mapping $x \to f(x)$ is a permutation over $\mathbb{F}_{p^n}$. S-box (over $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$) is an important component for block ciphers and it is often crucial to require S-boxes to be permutations. For the resistance against known attacks, several criteria should be satisfied. For example, the Difference Distribution Table (DDT for short) and the differential uniformity of an S-box characterise the resistance of the cryptographic

Kangquan Li, Longjiang Qu, Bing Sun and Chao Li are with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, 410073, China. Longjiang Qu is also with the State Key Laboratory of Cryptology, Beijing, 100878, China. E-mail: likangquan11@nudt.edu.cn, ljqu_happy@hotmail.com, happy_come@163.com, lichao_nudt@sina.com. This work is supported by the Nature Science Foundation of China (NSFC) under Grant 61722213, 11531002, 61572026, 61772545, National Key R&D Program of China (No.2017YFB0802000), and the Open Foundation of State Key Laboratory of Cryptology.

component against differential cryptanalysis [13]. Furthermore, the differential uniformity, along with many other cryptographic properties of the S-boxes has been extensively studied these years. And a number of results with both theoretical and practical significance have been obtained. It is well known that for any f over $\mathbb{F}_{2^n}$, the elements of DDT are all even and the minimum of differential uniformities of f is 2. The functions with differential uniformity 2 are called Almost Perfect Nonlinear (APN for short) functions.

The Boomerang attack was proposed by Wagner [40] in 1999 and variants of the boomerang attack were later presented [11, 25]. In order to evaluate the subtleties of boomerang-style attacks, in EUROCRYPT 2018, Cid et al. [16] introduced a new cryptanalysis tool: Boomerang Connectivity Table and Boomerang Uniformity (see Definition 2.1). In [16], the authors analyzed the properties of BCT theoretically, especially the relationship between BCT and DDT. They proved that S-boxes having 2-uniform DDT always have 2-uniform BCT and for any choice of (a, b), the value in the BCT is greater than or equal to the one in the DDT. Therefore, for S-boxes, 2-uniform BCT permutations are equivalent to APN permutations. Very recently, BCT and the boomerang uniformity were further studied by Boura and Canteaut [4]. Through showing that boomerang uniformity is only an affine equivalent invariant and the classification [27] about all differentially 4-uniform permutations of 4 bits, Boura and Canteaut completely characterized the BCT of such permutations. In addition, they also obtained the boomerang uniformities of the inverse function and the Gold function over $\mathbb{F}_{2^n}$.

To better reveal the guidance of the newly proposed cryptographic criteria on how to design S-boxes, in this paper, we further explore novel properties about BCT and the boomerang uniformity of permutations over $\mathbb{F}_{2^n}$ theoretically and experimentally. Firstly, we give a new method about computing BCT and the boomerang uniformity of permutations, which is much simpler than the original one. In detail, our definition transforms the problem solving an extremely complicated equation with a permutation and its inverse into that of solving an equation system including two simpler equations with only the permutation in order to compute the BCT and the boomerang uniformity of the permutation. After this transformation, not only can we compute BCT and the boomerang uniformity of permutations more simply, but we can study their properties, such as the characterization of the boomerang uniformity by the Walsh transform and so on, more easily. Moreover, using our new method, we compute boomerang uniformities of some specific permutations, mainly the ones with low differential uniformity and obtain another class of 4-uniform BCT permutation polynomials over $\mathbb{F}_{2^n}$, which is the first binomial up to now.

The rest of this paper is organized as follows. In Section 2, we first recall the original definition about BCT and the boomerang uniformity of permutations from [16]. Moreover, in consideration of the complexity of computing BCT and the boomerang uniformity, we give an equivalent formula to compute them, which seems simpler and can be generalized (not restricted to permutations). Section 3 gives a characterization of δ_f-uniform BCT functions by the Walsh transform. Next, we compute boomerang uniformities of some permutation polynomials with low differential uniformity over $\mathbb{F}_{2^n}$ theoretically and experimentally and obtain another class of 4-uniform BCT permutations in Sections 4 and 5, respectively. Finally, Section 6 is a conclusion.

2. New method of computing BCT and Boomerang Uniformity

In [16], Cid et al. introduced the concept of Boomerang Connectivity Table of a permutation f from $\mathbb{F}_2^n$ to itself as follows, which is also suitable for the case $\mathbb{F}_{2^n}$ clearly.

Definition 2.1. *[16] Let f from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ be an invertible function, and $a, b \in \mathbb{F}_2^n$. The Boomerang Connectivity Table (BCT) of f is given by a $2^n \times 2^n$ table T, in which the entry for the (a, b) position is given by*

$$T(a,b) = \#\{x \in \mathbb{F}_2^n | f^{-1}(f(x)+a) + f^{-1}(f(x+b)+a) = b\}. \tag{1}$$

Moreover, for any $a, b \in \mathbb{F}_2^n \backslash \{0\}$, the value

$$\delta_f = \max_{a,b \in \mathbb{F}_2^n \backslash \{0\}} \#\{x \in \mathbb{F}_2^n | f^{-1}(f(x)+a) + f^{-1}(f(x+b)+a) = b\},$$

is called the boomerang uniformity of f, or we call f is a δ_f-uniform BCT function.

We note that Definition 2.1 is only suitable for invertible functions, i.e., permutations. According to the definition of BCT and the boomerang uniformity, for a permutation $f(x)$ over $\mathbb{F}_{2^n}$, it is necessary to obtain the compositional inverse $f^{-1}(x)$ of $f(x)$ over $\mathbb{F}_{2^n}$ if we want to compute BCT and the boomerang uniformity of $f(x)$. However, given a permutation polynomial $f(x)$ over $\mathbb{F}_{p^n}$, it is in general a hard problem to compute the compositional inverse with explicit form of $f(x)$ over $\mathbb{F}_{p^n}$. Besides many classical classes such as monomials, linearized polynomials, and Dickson polynomials, there are few classes of permutation polynomials whose compositional inverses have been obtained in explicit forms. Some results about compositional inverses can be referred to [28, 37, 39, 41]. In addition, it is general that the compositional inverse of a permutation polynomial f with a simple form has a complex form, increasing the difficulty of computing BCT and the boomerang uniformity of f. Therefore, it seems interesting and meaningful to compute BCT and the boomerang uniformity of $f(x)$ without $f^{-1}(x)$.

In the following, we present an equivalent formula to compute BCT and the boomerang uniformity without knowing $f^{-1}(x)$ and $f(x)$ simultaneously.

Let $a, b \in \mathbb{F}_{2^n}^*$ and $f(x)$ be a permutation polynomial over $\mathbb{F}_{2^n}$. Let $y = x + b$ in (1). Then the following equation system

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

has $T(a, b)$ solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Furthermore, let $X = f(x)$ and $Y = f(y)$. Then we have

$$\begin{cases} f^{-1}(X+a) + f^{-1}(Y+a) = b, \\ f^{-1}(X) + f^{-1}(Y) = b \end{cases} \tag{3}$$

from the equation system (2) and the numbers of solutions of equation systems (2) and (3) are the same since f is a permutation polynomial over $\mathbb{F}_{2^n}$. Hence, it is sufficient to compute the solutions of the equation system (3) if we want to obtain BCT and the boomerang uniformity of a given permutation polynomial

$f(x) \in \mathbb{F}_{2^n}[x]$.

Theorem 2.2. *Let $f(x) \in \mathbb{F}_{2^n}[x]$ be a permutation polynomial over $\mathbb{F}_{2^n}$, $f^{-1}(x)$ be the compositional inverse of $f(x)$ over $\mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. Then the BCT of $f(x)$ can be given by a $2^n \times 2^n$ table T, in which the entry $T(a,b)$ for the (a,b) position is given by the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the equation system (3).*

Let $f(x) \in \mathbb{F}_{2^n}[x]$ be a permutation polynomial over $\mathbb{F}_{2^n}$, $f^{-1}(x)$ be the compositional inverse of $f(x)$ over $\mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$. Assume that T and $T^{'}$ are the BCTs of $f(x)$ and $f^{-1}(x)$, respectively. From [4, Proposition 2], we know that for any $a, b \in \mathbb{F}_{2^n}^{*}$, $T(a,b) = T^{'}(b,a)$. Together with Theorem 2.2, we have

Theorem 2.3. *Let $f(x)$ be a permutation polynomial over $\mathbb{F}_{2^n}$. Then the boomerang uniformity of $f(x)$, given by δ_f, is the maximum of numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system*

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

for any $a, b \in \mathbb{F}_{2^n}^{*}$.

Remark 2.4. About out new method to compute BCT and the boomerang uniformity, the first advantage is that we do not have to figure out the compositional inverse of $f(x)$. In addition, in the original definition about BCT and the boomerang uniformity of $f(x)$ over $\mathbb{F}_2^n$ by Cid et al. [16], i.e., Definition 2.1, it is assumed that $f(x)$ is a permutation. Nevertheless, it is clear from Theorem 2.3 that the condition with permutation property is not necessary. Finally, the boomerang uniformity can be generalized to any vector space, i.e., $\mathbb{F}_p^n$ with p odd, where we should notice that the equation system (4) becomes

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

However, in this paper, we mainly consider the boomerang uniformity of permutations over $\mathbb{F}_{2^n}$.

Remark 2.5. If (x_0, y_0) is a solution in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the equation system (4), then $y_0 \neq x_0$ since $b \neq 0$. Hence (y_0, x_0) must be a distinct solution of (4). Thus for any f, the elements in BCT of f must be even. Moreover, $(x_0 + a, y_0 + a)$ and $(y_0 + a, x_0 + a)$ are another two solutions of (4) if $x_0 + a \neq y_0$. That is to say, $(x_0, y_0), (y_0, x_0), (x_0 + a, y_0 + a)$ and $(y_0 + a, x_0 + a)$ are four different solutions of (4) if $x_0 + a \neq y_0$ and the boomerang uniformity of f, we think, is probably more than four. In other words, constructing 4-uniform BCT permutations seems not so easy.

From Theorem 2.3, it is easy to see that BCT is an affine equivalent invariant, but is nor an EA and CCZ equivalence invariant, as already shown in [4]. Recall that two functions f and $f^{'}$ from $\mathbb{F}_2^n$ to itself are called EA equivalent if $f^{'} = A_1 \circ f \circ A_2 + A$, where A is affine and A_1, A_2 are affine permutations. In particular, when $A = 0$, f and $f^{'}$ are called affine equivalent. Assume that A is affine and A_1, A_2 are affine permutations. If $f'(x) + f'(y) = b$, then we have $A_1 \circ f \circ A_2(x) + A(x) + A_1 \circ f \circ A_2(y) + A(y) = b$, and

$f \circ A_2(x) + f \circ A_2(y) + L_1^{-1} \circ L(x+y) = L_1^{-1}(b)$, which is equivalent to $f(X) + f(Y) = L_1^{-1}(b)$ if $L = 0$, where L_1 and L are the linear part of A_1 and A, respectively, $X = A_2(x)$ and $Y = A_2(y)$. Therefore, BCT is an affine equivalent invariant. However, it is clear that one can not build a similar equation if $L \neq 0$. Hence BCT is nor an EA or CCZ equivalence invariant.

At the end of this section, let us investigate the boomerang uniformities of permutation polynomials with special forms, such as monomials and quadratic permutations.

Definition 2.6. *[1] A function f from $\mathbb{F}_{p^n}$ to itself is*

1) linearized if

$$f(x) = \sum_{0 \le i < n} a_i x^{p^i}, \qquad a_i \in \mathbb{F}_{p^n};$$

2) affine if f is a sum of a linearized function and a constant;

3) Dembowski-Ostrom polynomial (DO polynomial) if

$$f(x) = \sum_{0 \le k < j \le n-1} a_{kj} x^{p^k + p^j}, \qquad a_{kj} \in \mathbb{F}_{p^n};$$

4) quadratic if it is a sum of a DO polynomial and an affine function.

Proposition 2.7. *Let $f(x) = x^d \in \mathbb{F}_{2^n}[x]$. Then the boomerang uniformity of $f(x)$ is $\delta_f = \max_{b \in \mathbb{F}_{2^n}^*} T(1,b)$, where $T(1,b)$ is the number of solutions over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system*

$$\begin{cases} f(x+1) + f(y+1) = b \\ \qquad f(x) + f(y) = b. \end{cases}$$

Proof. Let $x = aX$ and $y = aY$. Then the result follows directly from Theorem 2.3 and $f(x) = x^d$. □

Proposition 2.8. *Let $f(x)$ be a quadratic differentially Δ-uniform permutation polynomial over $\mathbb{F}_{2^n}$. Then the boomerang uniformity δ_f of f satisfies $\Delta \le \delta_f \le \Delta(\Delta - 1)$. Particularly, if $\Delta = 2$, then $\delta_f = 2$; if $\Delta = 4$, then $4 \le \delta_f \le 12$.*

Proof. we only prove the first inequality and it suffices to prove its right part. From Theorem 2.3, we know that $\delta_f = \max_{a,b \in \mathbb{F}_{2^n}^*} T(a,b)$, where $T(a,b)$ is the number of solutions over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system

$$\begin{cases} f(x+a) + f(y+a) = f(x) + f(y) & (6.1) \\ \qquad\qquad f(x) + f(y) = b. & (6.2) \end{cases}$$

Let $D_a f(x) = f(x+a) + f(x)$. Then for any $a \in \mathbb{F}_{2^n}^*$, $D_a f(x)$ is linearized since $f(x)$ is quadratic. Moreover, $D_a f(x)$ is Δ-to-1 since the differential uniformity of $f(x)$ is Δ. Together with (6.1), i.e., $D_a f(x) = D_a f(y)$, we have $y = x + \alpha_i$, where $i = 1, \cdots, \Delta - 1$ and $\alpha_i \neq \alpha_j$ for any $i \neq j$. For any $1 \le i \le \Delta - 1$, (6.2), i.e., $f(x) + f(x + \alpha_i) = b$ has at most Δ solutions in $\mathbb{F}_{2^n}$. Therefore, the equation system (6) has at most $\Delta(\Delta-1)$ solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$. That is to say, $\delta_f\leq\Delta(\Delta-1)$. We finish the proof. □

Remark 2.9. Proposition 2.8 is a generalization of [4, Proposition 7], which only gave the result for the case $\Delta=4$. Moreover, even for this case, our proof seems to be much simple.

3. CHARACTERIZATIONS OF δ_f-UNIFORM BCT FUNCTIONS BY THE WALSH TRANSFORM

It is well known that for any $u\in\mathbb{F}_2^n$ and $v\in\mathbb{F}_2^n\backslash\{0\}$, the Walsh transform of f is a real-valued function, whose value at (u,v) is defined by

$$W_f(u,v)=\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x+v\cdot f(x)}.$$

In this section, we consider the characterizations of δ_f-uniform BCT functions by the Walsh transform. The main idea is from Carlet [15] who characterized the differential uniformity of vectorial functions by means of the Walsh transform. Let

$$T(a,b)=\#\{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n|f(x+a)+f(y+a)=b\ \text{ and }\ f(x)+f(y)=b\}.$$

It is clear that f is an at most δ_f-uniform BCT function if and only if, for any $a,b\in\mathbb{F}_2^n\backslash\{0\}$, we have $T(a,b)\in\{0,2,\cdots,\delta_f\}$. Let $\phi(x)=\sum_{j\geq0}A_jx^j$ be any polynomial over $\mathbb{R}$ such that $\phi(x)=0$ for $x=0,2,\cdots,\delta_f$ and $\phi(x)>0$ for every even $x\in\{\delta_f+2,\cdots,2^n\}$. Hence for any f and $a,b\in\mathbb{F}_2^n\backslash\{0\}$, we have

$$\sum_{j\geq0}A_j(T(a,b))^j\geq0,$$

and f is an at most δ_f-uniform BCT function if and only if this inequality is an equality for any $a,b\in\mathbb{F}_2^n\backslash\{0\}$. Furthermore, for any f, we have

$$\sum_{j\geq0}A_j\sum_{a,b\in\mathbb{F}_2^n\backslash\{0\}}(T(a,b))^j\geq0,$$

and f is an at most δ_f-uniform BCT function if and only if this inequality is an equality. We now characterize δ_f-uniform BCT functions by the Walsh transform.

Lemma 3.1. *For any $j\geq1$, we have*

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_2^n\backslash\{0\}}(T(a,b))^j\\ =\;&2^{2n-4nj}\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ \gamma_1,\cdots,\gamma_j,\eta_1,\cdots,\eta_j\in\mathbb{F}_2^n\\ \sum_{i=1}^j(\alpha_i+\beta_i)=0,\sum_{i=1}^j(\gamma_i+\eta_i)=0}}\prod_{i=1}^jW_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)-2^{nj}(2^{n+1}-1).\end{aligned}$$

Proof. Firstly, it is clear that

$$T(a,b)=2^{-2n}\sum_{\alpha,\beta,x,y\in\mathbb{F}_2^n}(-1)^{\alpha\cdot(f(x+a)+f(y+a)+b)+\beta\cdot(f(x)+f(y)+b)}$$

since $\sum_{\alpha\in\mathbb{F}_2^n}(-1)^{\alpha\cdot(f(x+a)+f(y+a)+b)}$ (or $\sum_{\beta\in\mathbb{F}_2^n}(-1)^{\beta\cdot(f(x)+f(y)+b)}$) is nonzero for $f(x+a)+f(y+a)=b$ (resp. $f(x)+f(y)=b$) only and takes 2^n. Moreover, we have

$$\begin{aligned}
T(a,b) &= 2^{-4n}\sum_{\substack{\alpha,\beta,\gamma,\eta\in\mathbb{F}_2^n\\ x,y,z,w\in\mathbb{F}_2^n}}(-1)^{\alpha\cdot(f(z)+f(w)+b)+\beta\cdot(f(x)+f(y)+b)+\gamma\cdot(z+x+a)+\eta\cdot(w+y+a)}\\
&= 2^{-4n}\sum_{\substack{\alpha,\beta,\gamma,\eta\in\mathbb{F}_2^n\\ x,y,z,w\in\mathbb{F}_2^n}}(-1)^{\gamma\cdot z+\alpha\cdot f(z)}(-1)^{\eta\cdot w+\alpha\cdot f(w)}(-1)^{\gamma\cdot x+\beta\cdot f(x)}(-1)^{\eta\cdot y+\beta\cdot f(y)}(-1)^{(\alpha+\beta)\cdot b+(\gamma+\eta)\cdot a}\\
&= 2^{-4n}\sum_{\alpha,\beta,\gamma,\eta\in\mathbb{F}_2^n}W_f(\gamma,\alpha)W_f(\eta,\alpha)W_f(\gamma,\beta)W_f(\eta,\beta)(-1)^{(\alpha+\beta)\cdot b+(\gamma+\eta)\cdot a},
\end{aligned}$$

Similarly, for an integer $j\geq 1$,

$$\sum_{a,b\in\mathbb{F}_2^n}(T(a,b))^j=2^{-2nj}\sum_{a,b\in\mathbb{F}_2^n}\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ x_1,\cdots,x_j,y_1,\cdots,y_j\in\mathbb{F}_2^n}}(-1)^{\sum_{i=1}^j\alpha_i\cdot(f(x_i+a)+f(y_i+a)+b)+\beta_i\cdot(f(x_i)+f(y_i)+b)}$$

and

$$\begin{aligned}
&2^{4nj}\sum_{a,b\in\mathbb{F}_2^n}(T(a,b))^j\\
=&\sum_{a,b\in\mathbb{F}_2^n}\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ x_1,\cdots,x_j,y_1,\cdots,y_j\in\mathbb{F}_2^n\\ \gamma_1,\cdots,\gamma_j,\eta_1,\cdots,\eta_j\in\mathbb{F}_2^n\\ z_1,\cdots,z_j,w_1,\cdots,w_j\in\mathbb{F}_2^n}}(-1)^{\sum_{i=1}^j\alpha_i\cdot(f(z_i)+f(w_i)+b)+\beta_i\cdot(f(x_i)+f(y_i)+b)+\gamma_i\cdot(z_i+x_i+a)+\eta_i\cdot(w_i+y_i+a)}\\
=&\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ \gamma_1,\cdots,\gamma_j,\eta_1,\cdots,\eta_j\in\mathbb{F}_2^n}}\prod_{i=1}^j W_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)\left(\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\sum_{i=1}^j(\alpha_i+\beta_i)\cdot b+(\gamma_i+\eta_i)\cdot a}\right).
\end{aligned}$$

Because $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{\sum_{i=1}^j(\alpha_i+\beta_i)\cdot b+(\gamma_i+\eta_i)\cdot a}$ is nonzero only when $\sum_{i=1}^j(\alpha_i+\beta_i)=0$ and $\sum_{i=1}^j(\gamma_i+\eta_i)=0$ hold at the same time and takes 2^{2n}, we have

$$\begin{aligned}
&2^{4nj}\sum_{a,b\in\mathbb{F}_2^n}(T(a,b))^j\\
=&\ 2^{2n}\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ \gamma_1,\cdots,\gamma_j,\eta_1,\cdots,\eta_j\in\mathbb{F}_2^n\\ \sum_{i=1}^j(\alpha_i+\beta_i)=0,\sum_{i=1}^j(\gamma_i+\eta_i)=0}}\prod_{i=1}^j W_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)
\end{aligned}$$

On the other hand,

$$\sum_{a,b\in\mathbb{F}_2^n}(T(a,b))^j=\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^j+2^{nj}(2^{n+1}-1).$$

Thus

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^j\\ =\ &2^{2n-4nj}\sum_{\substack{\alpha_1,\cdots,\alpha_j,\beta_1,\cdots,\beta_j\in\mathbb{F}_2^n\\ \gamma_1,\cdots,\gamma_j,\eta_1,\cdots,\eta_j\in\mathbb{F}_2^n\\ \sum_{i=1}^j(\alpha_i+\beta_i)=0,\sum_{i=1}^j(\gamma_i+\eta_i)=0}}\prod_{i=1}^j W_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)-2^{nj}(2^{n+1}-1).\end{aligned}$$

□

Note that for $j=0$, we have $\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^j=(2^n-1)^2$. Therefore, we have the following theorem.

Theorem 3.2. *Let n,δ be positive integers, where δ is even, and let f be any permutation over $\mathbb{F}_{2^n}$. Let $\phi(x)=\sum_{j\geq 0}A_jx^j$ be any polynomial over $\mathbb{R}$ such that $\phi(x)=0$ for $x=0,2,\cdots,\delta$ and $\phi(x)>0$ for every even $x\in\{\delta+2,\cdots,2^n\}$. Then we have*

$$(2^n-1)^2A_0+\sum_{j\geq 1}A_j\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^j\geq 0,$$

where $\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^j$ is given in Lemma 3.1 for any $j\geq 1$. Furthermore, this inequality is an equality if and only if the boomerang uniformity of f is at most δ.

A. Characterizations of 2-uniform BCT functions by the Walsh transform

Let $\phi(x)=x(x-2)=x^2-2x$, which satisfies that $\phi(x)=0$ for $x=0,2$ and $\phi(x)>0$ for every even $x\in\{4,6,\cdots,2^n\}$. Then

$$\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^2-2\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}T(a,b)\geq 0,$$

and f is a 2-uniform BCT function if and only if the above inequality is an equality.

From Lemma 3.1, we have

$$\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}T(a,b)=2^{-2n}\sum_{\alpha,\gamma\in\mathbb{F}_2^n}W_f(\alpha,\gamma)^4-2^n(2^{n+1}-1).$$

and

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_2^n\setminus\{0\}}(T(a,b))^2\\ =\ & 2^{-6n}\sum_{\substack{\alpha_1,\alpha_2,\beta_1,\beta_2\,\in\,\mathbb{F}_2^n\\ \gamma_1,\gamma_2,\eta_1,\eta_2\,\in\,\mathbb{F}_2^n\\ \sum_{i=1}^2(\alpha_i+\beta_i)=0,\sum_{i=1}^2(\gamma_i+\eta_i)=0}}\prod_{i=1}^{2}W_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)-2^{2n}(2^{n+1}-1)\end{aligned}$$

Theorem 3.3. *Let f be any function from $\mathbb{F}_2^n$ to itself. Then*

$$\begin{aligned}&\sum_{\substack{\alpha_1,\alpha_2,\beta_1,\beta_2\,\in\,\mathbb{F}_2^n\\ \gamma_1,\gamma_2,\eta_1,\eta_2\,\in\,\mathbb{F}_2^n\\ \sum_{i=1}^2(\alpha_i+\beta_i)=0,\sum_{i=1}^2(\gamma_i+\eta_i)=0}}\prod_{i=1}^{2}W_f(\gamma_i,\alpha_i)W_f(\eta_i,\alpha_i)W_f(\gamma_i,\beta_i)W_f(\eta_i,\beta_i)\\ \geq\ & 2^{4n+1}\sum_{\alpha,\gamma\,\in\,\mathbb{F}_2^n}W_f(\gamma,\alpha)^4+2^{9n+1}-5\cdot 2^{8n}+2^{7n+1}.\end{aligned}$$

Moreover, f is a 2-uniform BCT function if and only if the above inequality is an equality.

Suppose f is a function from $\mathbb{F}_2^n$ to itself. Since the differential uniformity of f is 2 if and only if f is a 2-uniform BCT function from [16], Theorem 3.3 gives another characterization of APN functions by means of the Walsh transform.

4. The boomerang uniformity of some permutation polynomials with low differential uniformity

Before this section, we introduce some notations that will be used in the following. Let ω be an element of $\mathbb{F}_{2^2}\backslash\mathbb{F}_2$ and $\mathrm{Tr}_{2^n}(\cdot)$ denote the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For any $\gamma\in\mathbb{F}_{2^n}^*$, we assume $\mathrm{Ord}(\gamma)$ is the order of γ, i.e., the minimum positive integer k such that $\gamma^k=1$.

A. APN permutations

From [16], we know that the differential uniformity of permutation f over $\mathbb{F}_{2^n}$ is 2 if and only if f is a 2-uniform BCT permutation. Thus constructing 2-uniform BCT permutations over $\mathbb{F}_{2^n}$ is equivalent to constructing APN permutations over $\mathbb{F}_{2^n}$. In the case n is even, there is only a sporadic APN permutation over $\mathbb{F}_{2^6}$ presented by Dillon et al. [10] up to now and we call it as Dillon's Permutation. Therefore, when n is even, there is also one 2-uniform BCT permutation (Dillon's Permutation) over $\mathbb{F}_{2^n}$. As for the case n is odd, there are many infinite classes of APN permutations as follows and thus also 2-uniform BCT permutations. In fact, [5] proved that if x^d over $\mathbb{F}_{2^n}$ is an APN, then

$$\gcd(d,2^n-1)=\begin{cases}1, & \text{if } \ n \ \text{ is odd;}\\ 3, & \text{if } \ n \ \text{ is even.}\end{cases}$$

The above result shows that APN power functions over $\mathbb{F}_{2^n}$ must be permutations when n is odd while those can not be permutations when n is even. In Table I, we list all current APN functions, i.e., 2-uniform BCT permutation monomials over $\mathbb{F}_{2^n}$, where n is odd.

TABLE I
2-UNIFORM BCT PERMUTATION MONOMIALS OVER $\mathbb{F}_{2^n}$, n ODD

Function	Expression	Conditions	Ref.
Gold	x^{2^i+1}	$\gcd(n,i)=1$	[22, 32]
Kasami	$x^{2^{2i}-2^i+1}$	$\gcd(n,i)=1$	[24]
Welch	x^{2^k+3}	$n=2k+1$	[18]
Niho-1	$x^{2^k+2^{k/2}-1}$	$n=2k+1$, k even	[19]
Niho-2	$x^{2^k+2^{(3k+1)/2}-1}$	$n=2k+1$, k odd	[19]
Inverse	x^{-1}	n odd	[9, 22]
Dobbertin	$x^{2^{4k}+2^{3k}+2^{2k}+2^k-1}$	$n=5k$	[20]

In addition, there are also many APN functions with dominant expressions over $\mathbb{F}_{2^n}$, such as [2, 3, 6, 7, 21]. However, these results are not permutations to our knowledge. Certainly, we may transform them to permutations by CCZ equivalence. However, the research seems to be quite difficult and is not suitable to expand in the present paper.

B. 4*-uniform DDT permutations*

As is well-known, there are five classes of primarily constructed 4-uniform DDT permutations over $\mathbb{F}_{2^n}$, which are listed in Table II. In Table II, "some conditions" for Bracken-Tan-Tan function refer to that $n=3k$, k is even, $3 \nmid k$, $k/2$ is odd, $\gcd(3k,s)=2$, $3 \mid k+s$ and α is a primitive element of $\mathbb{F}_{2^n}$.

TABLE II
4-UNIFORM DDT PERMUTATIONS OVER $\mathbb{F}_{2^n}$

Function	Expression	Conditions	Ref.
Gold	x^{2^i+1}	$n=2k, k$ odd, $\gcd(n,i)=2$	[22]
Kasami	$x^{2^{2i}-2^i+1}$	$n=2k, k$ odd, $\gcd(n,i)=2$	[24]
Inverse	x^{-1}	n even	[9, 32]
Bracken-Leander	$x^{2^{2k}+2^k+1}$	$n=4k$, k odd	[12, 17]
Bracken-Tan-Tan	$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{-k}+2^{k+s}}$	some conditions	[14]

In the subsection, we mainly consider boomerang uniformities of these permutation monomials over $\mathbb{F}_{2^n}$ listed in Table II. In fact, the boomerang uniformities of Gold and Inverse functions have been determined in [4, Proposition 8] and [4, Proposition 6], respectively. As for Kasami, Bracken-Leander and Bracken-Tan-Tan functions, we list boomerang uniformities of these functions in small finite fields.

TABLE III
THE BOOMERANG UNIFORMITY OF THE KASAMI FUNCTION OVER $\mathbb{F}_{2^{2k}}$

Conditions	Functions	Uniformities	Conditions	Functions	Uniformities
$k=3, i=2$	x^{13}	4	$k=5, i=6$	x^{4033}	44
$k=3, i=4$	x^{241}	4	$k=7, i=2$	x^{13}	24
$k=5, i=2$	x^{13}	44	$k=7, i=4$	x^{241}	16
$k=5, i=4$	x^{241}	44	$k=7, i=6$	x^{4033}	16

TABLE IV
THE BOOMERANG UNIFORMITY OF THE BRACKEN-LEANDER FUNCTION OVER $\mathbb{F}_{2^{4k}}$

Conditions	Functions	Uniformities
$k=1$	x^{7}	4
$k=3$	x^{73}	14

From Tables III and IV, we can see that boomerang uniformities of Kasami and Bracken-Leander functions become very high as the value of k increases and it is the reason why we do not give theoretical result about boomerang uniformities of those two classes of functions. As for Bracken-Tan-Tan function defined over $\mathbb{F}_{2^{3k}}$ [14], when $k=2$, we have $s \equiv 4 \pmod 6$ and $f(x) = \left(\alpha + \alpha^4\right) x^{15}$, which is one case of Gold functions and whose boomerang uniformity is 4. While, when k is bigger, like $k=10$, we can not compute the boomerang uniformity of $f(x)$ by Personal Computer within an acceptable time. However, it follows from Proposition 2.8 that the boomerang uniformity of Bracken-Tan-Tan function is smaller than 12.

C. 4-*uniform DDT permutations constructed from the inverse function*

Recently, there were some 4-uniform DDT permutations constructed from the inverse function, like [29, 33–36] and the references therein. In this section, we mainly consider the function over $\mathbb{F}_{2^n}$

$$f(x) = \begin{cases} 1, & \text{if} \quad x = 0, \\ 0, & \text{if} \quad x = 1, \\ \dfrac{1}{x}, & \text{otherwise.} \end{cases} \tag{7}$$

In [29], the authors proved that the differential uniformity of $f(x)$ over $\mathbb{F}_{2^n}$ defined by (7) is at most equal to 6 and it is equal to 4 if and only if $n \equiv 2 \pmod 4$. Furthermore, $f(x)$ is with the best known nonlinearity. In the following, we consider the boomerang uniformity of $f(x)$, i.e., the maximum of numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system for any $a, b \in \mathbb{F}_{2^n}^*$,

$$\begin{cases} f(x+a) + f(y+a) = b, \\ f(x) + f(y) = b. \end{cases} \tag{8}$$

Lemma 4.1. *Let $f(x)$ be defined by (7) and $a \notin \{1, \omega, \omega^2\}$. Then*

(1) $(0, y)$ and $(y, 0)$ are two solutions of (8) if and only if $b = \frac{1+a}{a}$ or $a^2b^2 + a^2b + ab + 1 = 0$. In the case, $y = \frac{1}{b+1}$.

(2) $(1, y)$ and $(y, 1)$ are two solutions of (8) if and only if $b = \frac{1}{1+a}$ or $a^2b^2 + ab^2 + ab + 1 = 0$. In the case, $y = \frac{1}{b}$.

(3) (a, y) and (y, a) are two solutions of (8) if and only if $a^2b^2 + a^2b + ab + 1 = 0$. In the case, $y = \frac{ab+a+1}{b+1}$;

(4) $(a + 1, y)$ and $(y, a + 1)$ are two solutions of (8) if and only if $a^2b^2 + ab^2 + ab + 1 = 0$. In the case, $y = \frac{ab+1}{b}$.

Proof. (1) If $(0, y)$ is a solution of (8), then we have

$$\begin{cases} \dfrac{1}{a} + f(y + a) = b & (9.1) \\ 1 + f(y) = b. & (9.2) \end{cases}$$

Thus $f(y) = b + 1$.

If $b = 1$, then $y = 1$ and $\frac{1}{a} + \frac{1}{1+a} = 1$, leading to $a = \omega$ or ω^2. Contradictions! Hence in the case $b \neq 1$ and $y = \frac{1}{b+1}$.

In the following, we let $b \neq 1$. If $y = a$ holds at the same time, $b = \frac{1+a}{a}$. On the other hand, when $b = \frac{1+a}{a}$, it is easy to check that $(0, a)$ and $(a, 0)$ do satisfy (9). If $y = a+1$ in the meantime, $a+1 = \frac{1}{b+1}$. Moreover, $\frac{1}{a} = b$ holds according to (9.1). Therefore, $a = b = 1$, which is a contradiction. If $y \neq a, a + 1$, we have $\frac{1}{a} + \frac{1}{y+a} = b$ from (9.1). Plugging $y = \frac{1}{b+1}$ into $\frac{1}{a} + \frac{1}{y+a} = b$, we obtain $a^2b^2 + a^2b + ab + 1 = 0$. Furthermore, when $a^2b^2 + a^2b + ab + 1 = 0$ holds, we can also check that $(0, \frac{1}{b+1})$, $(\frac{1}{b+1}, 0)$ are two solutions of (9).

(2) If $(1, y)$ is a solution of (8), we have

$$\begin{cases} \dfrac{1}{a+1} + f(y + a) = b & (10.1) \\ \qquad f(y) = b. & (10.2) \end{cases}$$

If $b = 1$, from (10), we have $y = 0$ and $\frac{1}{1+a} + \frac{1}{a} = 1$, which is a contradiction. Thus $b \neq 1$ and $y = \frac{1}{b}$ from (10.1).

In the following, we let $b \neq 1$. If $y = a$, we have $\frac{1}{a+1} = b + 1$ from (10.1). Together with $\frac{1}{b} = a$ and $\frac{1}{a+1} = b + 1$, $a = 1$, which is contradictory. If $y = a + 1$, we have $b = \frac{1}{a+1}$. Furthermore, when $b = \frac{1}{a+1}$, $(1, a+1), (a+1, 1)$ are two solutions of (10). If $y \neq a, a+1$, we have $\frac{1}{1+a} + \frac{1}{y+a} = b$ from (10.1). Plugging $y = \frac{1}{b}$ into $\frac{1}{1+a} + \frac{1}{y+a} = b$, we get $a^2b^2 + ab^2 + ab + 1 = 0$. Moreover, when $a^2b^2 + ab^2 + ab + 1 = 0$ holds, $(0, \frac{1}{b})$, $(\frac{1}{b}, 0)$ are two solutions of (10).

(3) If (a, y) is a solution of (8), we have

$$\begin{cases} 1 + f(y+a) = b & (11.1) \\ \dfrac{1}{a} + f(y) = b. & (11.2) \end{cases}$$

If $b = 1$, from (11), we have $y = a + 1$ and $\frac{1}{a} + \frac{1}{a+1} = 1$, which is a contradiction. Thus $b \neq 1$ and $y = \frac{1}{b+1} + a = \frac{ab+a+1}{b+1}$. Together with (11.2), we get

$$b + \frac{1}{a} = f(y) = \frac{b+1}{ab+a+1},$$

i.e.,

$$a^2b^2 + a^2b + ab + 1 = 0.$$

Moreover, when $a^2b^2 + a^2b + ab + 1 = 0$, $(a, \frac{ab+a+1}{b+1})$ and $(\frac{ab+a+1}{b+1}, a)$ are two solutions of (11).

(3) If $(a+1, y)$ is a solution of (8), we have

$$\begin{cases} f(y+a) = b & (12.1) \\ \dfrac{1}{a+1} + f(y) = b. & (12.2) \end{cases}$$

If $b = 1$, from (12), we have $y = a$ and $\frac{1}{a} + \frac{1}{a+1} = 1$, which is a contradiction. Thus $b \neq 1$ and $y = \frac{1}{b} + a = \frac{ab+1}{b}$. Together with (12.2), we get

$$b + \frac{1}{a+1} = f(y) = \frac{ab+1}{b},$$

i.e.,

$$a^2b^2 + ab^2 + ab + 1 = 0.$$

Moreover, when $a^2b^2 + ab^2 + ab + 1 = 0$, $(a+1, \frac{ab+1}{b})$ and $(\frac{ab+1}{b}, a+1)$ are two solutions of (12). □

Let sets $S_i (i = 1, \cdots, 4)$ be the conditions of Lemma 4.1, respectively, i.e.,

$$S_1 := \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | b = \frac{1+a}{a} \quad \text{or} \quad a^2b^2 + a^2b + ab + 1 = 0\};$$

$$S_2 := \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | b = \frac{1}{1+a} \quad \text{or} \quad a^2b^2 + ab^2 + ab + 1 = 0\};$$

$$S_3 := \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^2b^2 + a^2b + ab + 1 = 0\};$$

$$S_4 := \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^2b^2 + ab^2 + ab + 1 = 0\}.$$

What should be noticed is that $a \notin \{1, \omega, \omega^2\}$ for $S_i (i = 1, \cdots, 4)$ and there are at least two solutions of (8) if $(a, b) \in S_i$, where $i = 1, 2, 3, 4$. Moreover, if (a, b) belongs to some S_i at the same time, there are more solutions of (8). Therefore, it is worthwhile to consider the intersections of S_i and the following lemma can answer the problem, whose proof is omitted since it is easy to prove.

Lemma 4.2. *1)* $S_1 \cap S_2 = \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3+a+1=0 \ \ and \ \ b = a, \frac{1+a}{a}, \frac{1}{a+1}\}$*;*

2) $S_1 \cap S_3 = S_3$*;*

3) $S_1 \cap S_4 = \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3+a+1=0 \ \ and \ \ b = a, \frac{1+a}{a}\}$*;*

4) $S_2 \cap S_3 = \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3+a+1=0 \ \ and \ \ b = a, \frac{1}{a+1}\}$*;*

5) $S_2 \cap S_4 = S_4$*;*

6) $S_3 \cap S_4 = \{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3+a+1=0 \ \ and \ \ b = a\}$.

7) $S_1 \cap S_2 \cap S_3 \cap S_4 = \{(a,b) | a^3+a+1=0 \ \ and \ \ b = a\}$.

Remark 4.3. It is clear that $a^3+a+1=0$ has solutions in $\mathbb{F}_{2^n}$ if and only if $n \equiv 0 \pmod 3$. Thus when $n \equiv 0 \pmod 3$, there exist some a, b such that $a^3+a+1=0$ and $b=a$. Together with Lemmas 4.1 and 4.2, for such a, b satisfying $a^3+a+1=0$ and $b=a$, (8) has at least eight solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. And when $n \not\equiv 0 \pmod 3$, there exist some $a, b \in \mathbb{F}_{2^n}$ satisfying $a^2b^2+a^2b+ab+1=0$ or $a^2b^2+ab^2+ab+1=0$, when which (8) has at least four solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

In the following, we give the main theorem of this section, determining the boomerang uniformity of $f(x)$ defined by (7). However, the proof is extremely tedious and we only introduce the prime idea here. The detailed and complete proof can be found in the Appendix.

Theorem 4.4. *Let $f(x)$ be defined by (7) and $n \geq 3$. Then the boomerang uniformity of f is*

$$\delta_f = \begin{cases} 10, & \textit{if} \ \ n \equiv 0 \pmod 6, \\ 8, & \textit{if} \ \ n \equiv 3 \pmod 6, \\ 6, & \textit{if} \ \ n \not\equiv 0 \pmod 3. \end{cases}$$

Proof. It suffices to compute $\max\limits_{a,b \in \mathbb{F}_{2^n}^*} T(a,b)$, where $T(a,b)$ is the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system for $a, b \in \mathbb{F}_{2^n} \backslash \{0\}$,

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

We divide the problem into three cases:

(1) $a = 1$, $b \in \mathbb{F}_{2^n}^*$;

(2) $a = \omega$ or ω^2, $b \in \mathbb{F}_{2^n}^*$;

(3) $a \in \mathbb{F}_{2^n}^* \backslash \{1, \omega, \omega^2\}$, $b \in \mathbb{F}_{2^n}^*$.

For the details proof of each case, please see the Appendix. We only mention that Lemmas 4.1 and 4.2 play important roles in cases (3) and for each case, the maximum of numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the above equation system is listed here:

Therefore, the boomerang uniformity of f is as claimed. □

Cases	$\max\limits_{a,b\in\mathbb{F}_{2^n}^*} T(a,b)$
$a=1$	2 if $n\equiv 1\pmod 2$, 4 if $n\equiv 2\pmod 4$, 6 if $n\equiv 0\pmod 4$
$a=\omega$ or ω^2	4 if $n\equiv 2\pmod 4$, 6 if $n\equiv 0\pmod 4$
$a\in\mathbb{F}_{2^n}^*\backslash\{1,\omega,\omega^2\}$	10 if $n\equiv 0\pmod 6$, 8 if $n\equiv 3\pmod 6$, 6 if $n\not\equiv 0\pmod 3$

Example 1. In order to test the correctness of Theorem 4.4, we compute the boomerang uniformity δ_f of f defined by (7) when $3\le n\le 9$ by Magma and the results are listed as follows.

n	3	4	5	6	7	8	9
δ_f	8	6	6	10	6	6	8

From the proof of Theorem 4.4, we see that computing boomerang uniformity is generally more complicated than computing differential uniformity and it seems quite complicated to obtain the boomerang uniformity of all 4-uniform DDT permutations constructed from inverse function.

5. A class of 4-uniform BCT permutations

In [16], Cid et al. discussed that obtaining 4-uniform BCT S-boxes appears to be hard, especially as the size of the S-box increases. In the following, we present a class of 4-uniform BCT permutation polynomials over $\mathbb{F}_{2^n}$.

In [42], Zieve obtained some classes of permutation polynomials with the form of $x^r h\left(x^{q+1}\right)\in\mathbb{F}_{q^2}[x]$, where q is an arbitrary prime power by using all low-degree (≤ 5) permutation polynomials over $\mathbb{F}_q$ (cf. [26, P352, Table 7.1]). The following theorem is one of these permutation polynomials and we can prove that it is a 4-uniform BCT function (Theorem 5.3) when q is even. By the way, the permutation polynomial in Theorem 5.3 is also a 4-uniform DDT function which has been showed in [43].

Lemma 5.1. *[42] Pick $\gamma\in\mathbb{F}_{q^2}^*$, and write $f(x)=x^{q+2}+\gamma x$. Then f permutes $\mathbb{F}_{q^2}$ if and only if one of the following occurs:*

(1) $q\equiv 5\pmod 6$ and γ^{q-1} has order 6;

(2) $q\equiv 2\pmod 6$ and γ^{q-1} has order 3; or

(3) $q\equiv 0\pmod 3$ and $\gamma^{q-1}=-1$.

Leonard and Williams characterized the factorization of a quartic polynomial over $\mathbb{F}_{2^n}$ in [30] and the result is useful to compute the boomerang uniformity of $f(x)$ in Theorem 5.3.

Lemma 5.2. *[30] Let $q=2^n$ and $f(x)=x^4+a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$, where $a_0a_1\ne 0$. Let $g(x)=x^3+a_2x+a_1$ and r_1,r_2,r_3 be three roots in $\mathbb{F}_q$ if they exist in $\mathbb{F}_q$. Then $f(x)$ has four solutions in $\mathbb{F}_q$ if and only if $g(y)$ has three solutions in $\mathbb{F}_q$ and $\mathrm{Tr}_q\left(\frac{a_0r_1^2}{a_1^2}\right)=\mathrm{Tr}_q\left(\frac{a_0r_3^2}{a_1^2}\right)=\mathrm{Tr}_q\left(\frac{a_0r_3^2}{a_1^2}\right)=0$.*

Theorem 5.3. *Let $q = 2^n$, n be odd and $f(x) = x^{q+2} + \gamma x \in \mathbb{F}_{q^2}[x]$, where* $\operatorname{Ord}\left(\gamma^{q-1}\right) = 3$. *Then $\delta_f = 4$.*

Proof. It suffices to prove that for $a, b \in \mathbb{F}_{q^2}^*$, the equation system

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

i.e.,

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

has at most 4 solutions in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$. Thanks to

$$f(x+a) = (x+a)^{q+2} + \gamma(x+a) = x^{q+2} + a^2x^q + a^qx^2 + a^{q+2} + \gamma x + \gamma a,$$

simplifying the above equation system, we have

$$\begin{cases} a^2(x+y)^q + a^q(x+y)^2 = 0 & (13.1) \\ x^{q+2} + \gamma x + y^{q+2} + \gamma y = b. & (13.2) \end{cases}$$

Let $z = x + y$. Then from (13.1), we obtain $z = \beta a$, where $\beta = 1, \omega$ or ω^2, since $\gcd\left(q-2, q^2-1\right) = 3$ when n is odd. Moreover, $y = x + z = x + \beta a$. Plugging it into (13.2), we have

$$\beta^2a^2x^q + a^q\beta^2x^2 + \beta a^{q+2} + \gamma\beta a + b = 0.$$

Let $x = aX$. Then the above equation becomes

$$X^q + X^2 = c, \tag{14}$$

where $c = \frac{\beta a^{q+2}+\gamma\beta a+b}{\beta^2a^{q+2}}$. Let $L(x) = x^q + x^2$. Since $L(x) = 0$ has 4 solutions in $\mathbb{F}_{q^2}$, $L(x)$ is a 4-to-1 polynomial over $\mathbb{F}_{q^2}$. Thus Eq. (14) has 4 or 0 solutions in $\mathbb{F}_{q^2}$ for a given β. In the following, we show that given any $a, b \in \mathbb{F}_{q^2}^*$, for three cases $\beta = 1, \omega, \omega^2$, Eq. (14) can not have solutions at the same time. First of all, we show that equations $x^q + x^2 = c$ and $x^4 + x = c$ have solutions or no solutions in $\mathbb{F}_{q^2}$ at the same time. On one side, if $x_0 \in \mathbb{F}_{q^2}$ is a solution of $x^4 + x = c$, let $x_1 = x_0^q + x_0^2$. Then $x_1^q + x_1^2 = x_0 + x_0^{2q} + x_0^{2q} + x_0^4 = c$, which means that x_1 is a solution of $x^q + x^2 = c$. On the other side, if x_0 is a solution of $x^q + x^2 = c$, let $x_1 = x_0^{2^{n-2}} + x_0^{2^{n-4}} + \cdots + x_0^2$. Then $x_1^4 + x_1 = x_0^{2^n} + x_0^2 = c$, claiming that x_1 is a solution of $x^4 + x = c$. Therefore, given any $a, b \in \mathbb{F}_{q^2}^*$, we suffice to consider equation

$$x^4 + x = c \tag{15}$$

can not have solutions at the same time in $\mathbb{F}_{q^2}$ for three cases $\beta = 1, \omega, \omega^2$, where $c = \frac{\beta a^{q+2}+\gamma\beta a+b}{\beta^2a^{q+2}}$. Let $c_1 = \frac{a^{q+2}+\gamma a+b}{a^{q+2}}$, $c_2 = \frac{\omega a^{q+2}+\gamma\omega a+b}{\omega^2a^{q+2}}$ and $c_3 = \frac{\omega^2a^{q+2}+\gamma\omega^2a+b}{\omega a^{q+2}}$.

Let $g(x) = x^3 + 1$. Then it is trivial that $g(x)$ has three roots $x = 1, \omega, \omega^2$ in $\mathbb{F}_{q^2}$. Moreover, according to

Lemma 5.2, Eq. (15) has four solutions in $\mathbb{F}_{q^2}$ if and only if $\mathrm{Tr}_{q^2}(c) = \mathrm{Tr}_{q^2}(\omega c) = \mathrm{Tr}_{q^2}(\omega^2 c) = 0$. Without loss of generality, we assume that equations $x^4+x = c_1$ and $x^4+x = c_2$ has four solutions in the meantime. Thus we have $\mathrm{Tr}_{q^2}(c_1) = \mathrm{Tr}_{q^2}(\omega c_1) = \mathrm{Tr}_{q^2}(c_2) = \mathrm{Tr}_{q^2}(\omega c_2) = 0$. In addition, $\mathrm{Tr}_{q^2}(c) = 0$ if and only if there exist some $z \in \mathbb{F}_{q^2}$ such that $c = z+z^2$. Therefore, there exist $z_1, z_2, z_3, z_4 \in \mathbb{F}_{q^2}$ such that $c_1 = z_1+z_1^2$, $\omega c_1 = z_2 + z_2^2$, $c_2 = z_3 + z_3^2$ and $\omega c_2 = z_4 + z_4^2$. Moreover, we have $\omega(z_2 + z_2^2) = (z_1 + z_2) + (z_1 + z_2)^2$ and $\omega(z_3 + z_3^2) = z_4 + z_4^2$. Plugging $c_1 = \frac{a^{q+2}+\gamma a+b}{a^{q+2}}$, $c_2 = \frac{\omega a^{q+2}+\gamma\omega a+b}{\omega^2 a^{q+2}}$ into $\omega c_1 = z_2 + z_2^2$ and $c_2 = z_3 + z_3^2$, we have

$$\frac{\omega\gamma}{a^{q+1}} + \frac{\omega b}{a^{q+2}} = z_2 + z_2^2 + \omega \tag{16}$$

and

$$\frac{\omega^2\gamma}{a^{q+1}} + \frac{\omega b}{a^{q+2}} = z_3 + z_3^2 + \omega^2. \tag{17}$$

Adding Eq. (16) and Eq. (17), we obtain

$$\frac{\gamma}{a^{q+1}} = z_2 + z_2^2 + z_3 + z_3^2 + 1. \tag{18}$$

Since $\mathrm{Ord}\left(\gamma^{q-1}\right) = 3$, $\gamma^{3q} = \gamma^3$. Furthermore, $\gamma^q = \beta\gamma$, where $\beta = \omega$ or ω^2. In the following, we assume $\beta = \omega$ and the other case is similar. Raising Eq. (18) into its q-th power, we have

$$\frac{\omega\gamma}{a^{q+1}} = z_2^q + z_2^{2q} + z_3^q + z_3^{2q} + 1. \tag{19}$$

Adding $\omega\times$(18) and (19), we get

$$\omega\left(z_2 + z_2^2 + z_3 + z_3^2 + 1\right) = z_2^q + z_2^{2q} + z_3^q + z_3^{2q} + 1,$$

i.e.,

$$(z_1 + z_2) + (z_1 + z_2)^2 + z_4 + z_4^2 + \omega = z_2^q + z_2^{2q} + z_3^q + z_3^{2q} + 1.$$

Thus

$$\mathrm{Tr}_{q^2}\left((z_1 + z_2) + (z_1 + z_2)^2 + z_4 + z_4^2 + \omega\right) = \mathrm{Tr}_{q^2}\left(z_2^q + z_2^{2q} + z_3^q + z_3^{2q} + 1\right).$$

Since $\mathrm{Tr}_{q^2}(\omega) = 1$ and $\mathrm{Tr}_{q^2}(1) = 0$, we have $1 = 0$ from the above equation. Contradictions!

Therefore, Eq. (13) has at most 4 solutions in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$. That is to say, $\delta_f = 4$.

We have finished the proof. □

It is well known that given a permutation polynomial over $\mathbb{F}_q$, it is very hard to compute its explicit compositional inverse. In [28], the authors introduced an approach to compute the explicit expression for compositional inverses of permutation polynomials of the form $x^r h\left(x^s\right)$ over $\mathbb{F}_q$, where $s \mid (q-1)$ and $\gcd(r, q-1) = 1$. Their main idea is to transform the problem of computing the compositional inverses of permutation polynomials of the form $x^r h\left(x^s\right)$ into that of computing the compositional inverses of two restricted permutation mappings, i.e., x^r over $\mathbb{F}_q$ and $x^r h(x)^s$ over the set of $(q-1)/s$-th roots of unity in $\mathbb{F}_q^*$. Furthermore, they computed the explicit compositional inverses of the permutation polynomials in Theorem 5.1 for arbitrary q.

Lemma 5.4. *[28] Let $f(x) = x^{q+2} + \gamma x \in \mathbb{F}_{q^2}[x]$ be a permutation polynomial over $\mathbb{F}_{q^2}$.*
(1) If $q \equiv 2 \pmod 3$, then the compositional inverse of $f(x)$ over $\mathbb{F}_{q^2}$ is

$$f^{-1}(x) = x^{q^2-q-1}\left(\left(x^{q+1}+\epsilon^3\right)^{2\cdot 3^{-1}} - (2\epsilon - \gamma^q)\left(x^{q+1}+\epsilon^3\right)^{3^{-1}} + \epsilon^2 - \epsilon\gamma^q\right),$$

where $\epsilon = \frac{\gamma^q+\gamma}{3}$ and $3^{-1} = \frac{2q-1}{3}$ is the compositional inverse of 3 modulo $q-1$.
(2) If $q \equiv 0 \pmod 3$, i.e., $q = 3^n$, then the compositional inverse of $f(x)$ over $\mathbb{F}_{q^2}$ is

$$f^{-1}(x) = -\left(\sum_{i=0}^{n-1} \gamma^{-3^{i+1}+1} x^{3^i(q+1)} + \gamma\right)\left(\sum_{i=0}^{n-1} \gamma^{-3^{i+1}+1} x^{3^i(q+1)-q}\right).$$

Together with Theorem 5.3 and Lemma 5.4, we can obtain the following result.

Corollary 5.5. *Let $q = 2^n$, n be odd and*

$$f(x) = x^{q^2-q-1}\left(\left(x^{q+1}+\epsilon^3\right)^{2\cdot 3^{-1}} + \gamma^q\left(x^{q+1}+\epsilon^3\right)^{3^{-1}} + \epsilon^2 + \epsilon\gamma^q\right) \in \mathbb{F}_{q^2}[x],$$

where $\mathrm{Ord}\left(\gamma^{q-1}\right) = 3$, $\epsilon = \gamma^q + \gamma$ and $3^{-1} = \frac{2q-1}{3}$ is the compositional inverse of 3 modulo $q-1$. Then $\delta_f = 4$.

6. Conclusion

Boomerang Connectivity Table (BCT for short) is a new cryptanalysis tool introduced by Cid et al. [16] in EUROCRYPT 2018, to evaluate the subtleties of boomerang-style attacks. In this paper, we give some new properties about BCT and the boomerang uniformity. Firstly, we give an equivalent and simple formula to compute BCT and the boomerang uniformity. The advantage of our new method is not only that the compositional inverse is not needed, but also that the definition of BCT and the boomerang uniformity can be generalized. Secondly, we give a characterization of δ_f-uniform BCT functions by means of the Walsh transform. In particular, a new equivalent characterization about APN functions is presented. Thirdly, we consider boomerang uniformities of some special permutations with low differential uniformity. Finally, we obtain a new class of 4-uniform BCT permutations over $\mathbb{F}_{2^n}$, which is the first binomial. It is worth mentioning that it seems not easy to compute the boomerang uniformity of this class of binomial from the original definition directly .

From [4] and our results, we can see that there exist 2-uniform BCT permutation over $\mathbb{F}_{2^n}$, where n is odd and 4-uniform BCT permutations over $\mathbb{F}_{2^n}$, where $n \equiv 2 \pmod 4$. However, for the case $n \equiv 0 \pmod 4$, which are very widely used in cryptographic algorithm, we can not find any permutations over $\mathbb{F}_{2^n}$ with boomerang uniformity 4 up to now and it is our next goal.

Acknowledgment 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] L. Budaghyan, Construction and analysis of cryptographic functions, *New York, NY, USA: Springer-Verlag*, 2014.

[2] C. Bracken, E. Byme, N. Markin and et al., New families of quadratic almost perfect nonlinear trinomials and multinomials, *Finite Fields Appl.*, 14 (2008), pp. 703-714.

[3] C. Bracken, E. Byme, N. Markin and et al., A few more quadratic APN functions, *Cryptogr. Commun.*, 3 (2011), pp. 43-53.

[4] C. Boura, A. Canteaut, On the boomerang uniformity of cryptographic sboxes, *IACR Trans. Symmetric Cryptol.*, 3 (2018), pp. 290-310.

[5] T. P. Berger, A. Canteaut, P. Charpin and et al., On almost perfect nonlinear functions over F_2^n, *IEEE Trans. Inf. Theory*, 52 (2006), pp. 4160-4170.

[6] L. Budaghyan, C. Carlet and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inf. Theory*, 54 (2008), pp. 4218-4229.

[7] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN functions from known ones, *Finite Fields Appl.*, 15 (2009), pp. 150-159.

[8] L. Budaghyan, C. Carlet and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inf. Theory*, 52 (2006), pp. 1141-1152.

[9] T. Beth, C. Ding, On almost perfect nonlinear permutations, *in: EUROCRYPT,* 1993, pp. 65-76.

[10] K.A. Browning, J.F. Dillon, M.T. McQuistan and et al., An APN permutation in dimension six, *Finite Fields Appl.*, 518 (2010), pp. 33–42.

[11] A. Biryukov, D. Khovratovich, Related-key cryptanalysis of the full AES-192 and AES-256, *In: ASIACRYPT 2009*, in: LNCS, vol. 5912, 2009 pp. 1–18.

[12] C. Bracken, G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, *Finite Fields Appl.*, 16 (2010), pp. 231–242.

[13] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology*, 4 (1991), pp. 3–72.

[14] C. Bracken, C. H. Tan and Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity, *Finite Fields Appl.*, 18(2012), pp. 537-546

[15] C. Carlet, Characterizations of the differential uniformity of vectorial functions by the Walsh transform, *IEEE Trans. Inf. Theory*, 64 (2018), pp. 6443-6453.

[16] C. Cid, T. Huang, T. Peyrin and et al., Boomerang Connectivity Table: A New Cryptanalysis Tool, *in: Advances in Cryptology - EUROCRYPT 2018*, in: LNCS. vol. 10821, 2018, pp. 683–714.

[17] H. Dobbertin, One-to-one highly nonlinear power functions on GF(2^n), *Appl. Algebra Engrg. Comm. Comput.*, 9 (1998), pp. 139–152.

[18] H. Dobbertin, Almost perfect nonlinear power functions on $\mathbb{F}_{2^n}$: the Welch case, *IEEE Trans. Inf. Theory*, 45 (1999), pp. 1271-1275.

[19] H. Dobbertin, Almost perfect nonlinear power functions on $\mathbb{F}_{2^n}$: the Niho case, *Information and Computation*, 151 (1999), pp. 57-72.

[20] H. Dobbertin, Almost perfect nonlinear power functions on $\mathbb{F}_{2^n}$: a new case for n divisible by 5, *Finite Fields and Applications, Springer, Berlin, Heidelberg*, 2001, pp. 113-121.

[21] Y. Edel, A. Pott, A new almost perfect nonlinear function which is not quadratic, *Advances in Mathematics of Communications*, 3 (2009), pp. 59-81.

[22] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.), *IEEE Trans. Inf. Theory*, 14 (1968), pp. 154-156.

[23] X. Hou, Permutation polynomials over finite fields–A survey of recent advances, *Finite Fields Appl.*, 32 (2015), pp. 82-119.

[24] T. Kasami, The Weight enumerators for several classes subcodes of the 2nd order binary Reed-Muller codes, *Inf. Control*, 18 (1971), pp. 369-394.

[25] J. Kelsey, T. Kohno and B. Schneier, Amplified boomerang attacks against reduced-round MARS and serpent, *In: FSE 2000*, in: LNCS, vol. 1978, 2001, pp. 75–93.

[26] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed. *Cambridge Univ. Press, Cambridge*, 1997.

[27] G. Leander, A. Poschmann, On the Classification of 4 Bit S-Boxes, *In: WAIFI 2007*, in: LNCS. vol. 4547, 2007, pp. 159–176.

[28] K. Li, L. Qu and Q. Wang, Compositional inverses of permutation polynomials of the form $x^r h\left(x^s\right)$ over finite fields, *Cryptogr. Commun.*, doi: 10.1007/s12095-018-0292-7, 2018.

[29] Y. Li, M. Wang and Y. Yu, Constructing differentially 4-uniform permutations over $\mathrm{GF}(2^{2k})$ from the inverse function revisited, *IACR Cryptology ePrint Archive: Report 2013/731, 2013. https://eprint.iacr.org/2013/731.*

[30] P. A. Leonard, K. S. Williams, Quartics over $\mathrm{GF}(2^n)$, *Proc. Am. Math. Soc.*, 36 (1972), pp. 347-350.

[31] M. Matsui, Linear cryptanalysis method for DES cipher, *in: Advances in Cryptology - EUROCRYPT 1993*, in: LNCS. vol. 765, 1993, pp. 386–397.

[32] K. Nyberg, Differentially uniform mappings for cryptography, *in: Advances in Cryptology-EUROCRYPT'93*, Lofthus, 1993, in LNCS. vol. 765, 1994, pp. 55-64.

[33] J. Peng, C. Tan, New differentially 4-uniform permutations by modifying the inverse function on subfields, *Cryptogr. Commun.*, 9 (2017), pp. 363-378.

[34] L. Qu, Y. Tan, C. H. Tan and et al., Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method, *IEEE Trans. Inf. Theory*, 59 (2013), pp. 4675-4686.

[35] L. Qu, Y. Tan, C. Li and et al., More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$, *Des. Codes. Cryptogr.*, 78 (2016), pp. 391-408.

[36] D. Tang, C. Carlet and X. Tang, Differentially 4-uniform bijections by permuting the inverse function, *Des. Codes. Cryptogr.*, 77 (2015), pp. 117-141.

[37] A. Tuxanidy, Q. Wang, On the inverse of some classes of permutations of finite fields, *Finite Fields Appl.* 28 (2014), pp. 244-281.

[38] Z. Tu, X. Zeng and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.*, 25 (2014), pp. 182-193.

[39] B. Wu, Z. Liu, The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2,*Finite Fields Appl.* 24 (2013), pp. 136-147.

[40] D. Wagner, The boomerang attack, *In: FSE 1999*, in: LNCS, vol. 1636, 1999, pp. 156–170.

[41] Y. Zheng, P. Yuan and D. Pei, Piecewise constructions of inverses of some permutation polynomials, *Finite Fields Appl.* 36 (2015), pp. 151-169.

[42] M. E. Zieve, Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares,*arXiv: 1312.1325v3,* 2013.

[43] X. Zhu, X. Zeng and Y. Chen, Some binomial and trinomial differentially 4-uniform permutation polynomials, *International Journal of Foundations of Computer Science*, 26 (2015), pp. 487-497.

Appendix

The whole proof of Theorem 4.4

Proof. It suffices to consider the numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following equation system for $a, b \in \mathbb{F}_{2^n}^*$,

$$\begin{cases} f(x+a) + f(y+a) = b, \\ f(x) + f(y) = b. \end{cases} \tag{20}$$

Case 1: $a = 1$**.**

Subcase 1.1: $a = 1, b = 1$**.** In the subcase, (20) becomes

$$\begin{cases} f(x+1) + f(y+1) = 1, \\ f(x) + f(y) = 1. \end{cases} \tag{21}$$

(i) If $x = 0$ or 1, $y = 1$ or 0, respectively. Thus $(x, y) = (0, 1), (1, 0)$ are two solutions of (21);

(ii) If $x \neq 0, 1$, $y \neq 0, 1$, either. Then (21) becomes

$$\begin{cases} \frac{1}{x+1} + \frac{1}{y+1} = 1, \\ \frac{1}{x} + \frac{1}{y} = 1. \end{cases} \tag{22}$$

After simplifying (22), we obtain $x^2 + x + 1 = 0$. Therefore, when $n \equiv 1 \pmod 2$, (22) has no solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. When $n \equiv 0 \pmod 2$, (22) has two solutions $(x, y) = (\omega, \omega^2)$ and (ω^2, ω).

Hence, in the subcase $a = 1, b = 1$, the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is 2 (when $n \equiv 1 \pmod 2$) or 4 (when $n \equiv 0 \pmod 2$).

Subcase 1.2: $a = 1$**,** $b = \omega$ **or** ω^2**.** What should be noticed is that the subcase is under the case n even. In the subcase, we only consider the case $b = \omega$ since the other case is similar. Obviously, (20) becomes

$$\begin{cases} f(x+1) + f(y+1) = \omega, \\ f(x) + f(y) = \omega. \end{cases} \tag{23}$$

(i) If $x = 0$, $f(y+1) = \omega$ and $f(y) = \omega + 1 = \omega^2$ from (23), which means $y = \omega$. Similarly, when $x = 1$, $y = \omega^2$. Thus $(0, \omega), (\omega, 0), (1, \omega^2)$ and $(\omega^2, 1)$ are four solutions of (23).

(ii) If $x \neq 0, 1$, (23) becomes

$$\begin{cases} \frac{1}{x+1} + \frac{1}{y+1} = \omega, \\ \frac{1}{x} + \frac{1}{y} = \omega. \end{cases} \tag{24}$$

After simplifying (24), we have $x^2 + x + \omega^2 = 0$, which has two solutions $x_0, x_0 + 1$ in $\mathbb{F}_{2^n}$ if and only if $n \equiv 0 \pmod 4$. Moreover, when $n \equiv 0 \pmod 4$, $(x_0, x_0 + 1)$ and $(x_0 + 1, x_0)$ are two solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (24).

Hence, in the subcase $n \equiv 0 \pmod 2$, $a = 1, b = \omega$ or ω^2, the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is 4 (when $n \equiv 2 \pmod 4$) or 6 (when $n \equiv 0 \pmod 4$).

Subcase 1.3: $a = 1$, $b \neq \{1, \omega, \omega^2\}$. In the subcase, (20) becomes

$$\begin{cases} f(x+1) + f(y+1) = b, \\ f(x) + f(y) = b. \end{cases} \tag{25}$$

(i) If $x = 0$, $f(y) = b + 1$ and $f(y+1) = b$. Furthermore, $y = \frac{1}{b+1}$ and $y = \frac{1}{b} + 1$, which means $\frac{1}{b+1} = \frac{1}{b} + 1$ and $b = \omega, \omega^2$. Contradictions! Thus $x \neq 0$. Similarly, we also can obtain $x \neq 1$, $y \neq 0, 1$.

(ii) If $x \neq 0, 1$ and $y \neq 0, 1$, we have

$$\begin{cases} \frac{1}{x+1} + \frac{1}{y+1} = b, \\ \frac{1}{x} + \frac{1}{y} = b. \end{cases} \tag{26}$$

From the above equation system, we get $bx^2 + bx + 1 = 0$, which at most two solutions in $\mathbb{F}_{2^n}$. Moreover, in the subcase, (20) has at most two solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Therefore, in the case $a = 1$, the maximum of numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is

$$\begin{cases} 2, & \text{if} \quad n \equiv 1 \pmod 2, \\ 4, & \text{if} \quad n \equiv 2 \pmod 4, \\ 6, & \text{if} \quad n \equiv 0 \pmod 4. \end{cases}$$

Case 2: $a = \omega, \omega^2$. In the case, we should notice that $n \equiv 0 \pmod 2$ and only consider $a = \omega$ since the other case $a = \omega^2$ is similar.

Subcase 2.1: $b = 1$. In the subcase, (20) becomes

$$\begin{cases} f(x+\omega) + f(y+\omega) = 1, \\ f(x) + f(y) = 1. \end{cases} \tag{27}$$

(i) If $x = 0, 1$, $y = 1, 0$ respectively. Thus $(0, 1)$ and $(1, 0)$ are two solutions of (27).

(ii) If $x = \omega, \omega^2$, $y = \omega^2, \omega$ respectively. Thus (ω, ω^2) and (ω^2, ω) are two solutions of (27).

(ii) If $x \neq 0, 1, \omega, \omega^2$, (27) becomes

$$\begin{cases} \frac{1}{x+\omega} + \frac{1}{y+\omega} = 1, \\ \frac{1}{x} + \frac{1}{y} = 1. \end{cases} \tag{28}$$

After simplifying (28), we have $y = \frac{x}{x+1}$ and $x^2 + \omega x + \omega = 0$, which has two solutions $x_0, x_0 + \omega$ in $\mathbb{F}_{2^n}$ if and only if $n \equiv 0 \pmod 4$. Moreover, when $n \equiv 0 \pmod 4$, due to $\frac{x_0}{x_0+1} = x_0 + \omega$, $(x_0, x_0 + \omega)$ and $(x_0 + \omega, x_0)$ are two solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (28).

Hence, in the subcase $n \equiv 0 \pmod 2$, $a = \omega, b = 1$, the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is 4 (when $n \equiv 2 \pmod 4$) or 6 (when $n \equiv 0 \pmod 4$).

Subcase 2.2: $b = \omega$**.** In the subcase, (20) becomes

$$\begin{cases} f(x + \omega) + f(y + \omega) = \omega, \\ f(x) + f(y) = \omega. \end{cases} \tag{29}$$

(i) If $x = 0, 1, \omega, \omega^2$, $y = \omega, \omega^2, 0, 1$ respectively. Thus $(0, \omega), (\omega, 0), (1, \omega^2)$ and $(\omega^2, 1)$ are four solutions of (29).

(ii) If $x \neq 0, 1, \omega, \omega^2$, we have

$$\begin{cases} \frac{1}{x+\omega} + \frac{1}{y+\omega} = \omega, \\ \frac{1}{x} + \frac{1}{y} = \omega. \end{cases} \tag{30}$$

After simplifying (30), we have $y = \frac{x}{\omega x+1}$ and $x^2 + \omega x + 1 = 0$, which has two solutions $x_0, x_0 + \omega$ if and only if $n \equiv 0 \pmod 4$. Furthermore, when $n \equiv 0 \pmod 4$, $(x_0, x_0 + \omega), (x_0 + \omega, x_0)$ are two solutions of (30) and when $n \equiv 2 \pmod 4$, (30) has no solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Hence, in the subcase $n \equiv 0 \pmod 2$, $a = \omega, b = \omega$, the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is 4 (when $n \equiv 2 \pmod 4$) or 6 (when $n \equiv 0 \pmod 4$).

Subcase 2.3: $b = \omega^2$**.** In the subcase, (20) becomes

$$\begin{cases} \frac{1}{x+\omega} + \frac{1}{y+\omega} = \omega, \\ \frac{1}{x} + \frac{1}{y} = \omega. \end{cases} \tag{31}$$

(i) If $x = 0, 1, \omega, \omega^2$, $y = \omega^2, \omega, 1, 0$ respectively. Thus $(0, \omega^2), (\omega^2, 0), (1, \omega)$ and $(\omega, 1)$ are four solutions of (31).

(ii) If $x \neq 0, 1, \omega, \omega^2$, we have

$$\begin{cases} \frac{1}{x+\omega} + \frac{1}{y+\omega} = \omega^2, \\ \frac{1}{x} + \frac{1}{y} = \omega^2. \end{cases} \tag{32}$$

After simplifying (32), we get $y = \frac{x}{\omega^2 x+1}$ and $x^2 + \omega x + \omega^2 = 0$. Then $x = 1$ or ω^2, which is a contradiction.

Subcase 2.4: $b \neq 1, \omega, \omega^2$**.** In the subcase, (20) becomes

$$\begin{cases} f(x + \omega) + f(y + \omega) = b, \\ f(x) + f(y) = b. \end{cases} \tag{33}$$

(i) If $x = 0$, we get $f(y) = b + 1$ and $f(y + \omega) = b + \omega^2$. Thus $y = \frac{1}{b+1} = \frac{1}{b+\omega^2} + \omega$, which means $b^2 + \omega b + \omega = 0$. Similarly, if $x = 1$, we can get $y = \frac{1}{b}$ and $b^2 + \omega b + 1 = 0$. Also, if $x = \omega$, we obtain $y = \frac{1}{b+\omega^2}$ and $b^2 + \omega b + \omega = 0$. In addition, if $x = \omega^2$, we have $y = \frac{1}{b+\omega}$ and $b^2 + \omega b + 1 = 0$.

Hence, when $b^2 + \omega b + \omega = 0$, $(0, \frac{1}{b+1})$, $(\frac{1}{b+1}, 0)$, $(\omega, \frac{1}{b+\omega^2})$ and $(\frac{1}{b+\omega^2}, \omega)$ are four solutions of (33); when $b^2 + \omega b + 1 = 0$, $(1, \frac{1}{b})$, $(\frac{1}{b}, 1)$, $(\omega^2, \frac{1}{b+\omega})$, $(\frac{1}{b+\omega}, \omega^2)$ are four solutions of (33).

(ii) If $x \neq 0, 1, \omega, \omega^2$, (33) becomes

$$\begin{cases} \frac{1}{x+\omega} + \frac{1}{y+\omega} = b, \\ \frac{1}{x} + \frac{1}{y} = b. \end{cases} \tag{34}$$

After simplifying (34), we get $y = \frac{x}{bx+1}$ and $bx^2 + b\omega x + \omega = 0$, which has at most two solutions in $\mathbb{F}_{2^n}$. Moreover, (34) has at most two solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Therefore, in the case, $a = \omega$ or ω^2, the maximum of numbers of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of (20) is

$$\begin{cases} 4, & \text{if } n \equiv 2 \pmod 4, \\ 6, & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

Case 3: $a \notin \{1, \omega, \omega^2\}$.

(i) If $x = 0, 1, a, a+1$, according to Remark 4.3, when $n \equiv 0 \pmod 3$, (20) has at most eight solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and when $n \not\equiv 0 \pmod 3$, (20) has at most four solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

(ii) If $x \neq 0, 1, a, a+1$, (20) becomes

$$\begin{cases} \frac{1}{x+a} + \frac{1}{y+a} = b, \\ \frac{1}{x} + \frac{1}{y} = b. \end{cases} \tag{35}$$

After simplifying (35), we get $y = \frac{x}{bx+1}$ and $x^2 + ax + \frac{a}{b} = 0$, which has two solutions $x_0, x_0 + a$ in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_{2^n}(\frac{1}{ab}) = 0$ and when $\mathrm{Tr}_{2^n}(\frac{1}{ab}) = 0$, $(x_0, x_0 + a)$ and $(x_0 + a, x_0)$ are two solutions of (35).

From Lemma 4.2, (20) has eight solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if and only if $n \equiv 0 \pmod 3$ and $(a, b) \in \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3 + a + 1 = 0 \text{ and } b = a\}$. From the above (ii), $(x_0, x_0 + a)$ and $(x_0 + a, x_0)$ are two solutions of (35) if and only if $\mathrm{Tr}_{2^n}(\frac{1}{ab}) = 0$ holds. In the following, we consider when the above two conditions hold at the same time. Plugging $b = a, a^3 + a + 1 = 0$ into $\mathrm{Tr}_{2^n}(\frac{1}{ab}) = 0$, we get

$$\mathrm{Tr}_{2^n}\left(\frac{1}{a}\right) = \mathrm{Tr}_{2^n}\left(1 + a^2\right) = \mathrm{Tr}_{2^n}(1 + a) = 0.$$

On the other hand, since $a^3 + a + 1 = 0$, i.e., $a^4 + a^2 + a = 0$, $\mathrm{Tr}_{2^n}(a) = (a + a^2 + a^4) + (a + a^2 + a^4)^{2^3} + \cdots + (a + a^2 + a^4)^{2^{n/3-1}} = 0$. Thus $\{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^3 + a + 1 = 0 \text{ and } b = a\} \cap \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | \mathrm{Tr}_{2^n}\left(\frac{1}{ab}\right) = 0\} \neq \emptyset$ if and only if $n \equiv 0 \pmod 3$ and $\mathrm{Tr}_{2^n}(1) = 0$, i.e., $n \equiv 0 \pmod 6$. In other words, in the case, for any $n \equiv 0 \pmod 6$, (35) has at most ten solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and for any $n \equiv 3 \pmod 6$, (35) has at most eight solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

In addition, (20) has four solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ if and only if $(a, b) \in (S_3 \cup S_4) \backslash (S_3 \cap S_4)$, where $S_3 := \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^2 b^2 + a^2 b + ab + 1 = 0\}$ and $S_4 := \{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^* | a^2 b^2 + ab^2 + ab + 1 = 0\}$.

In the following, we consider $S\cap\{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*|\mathrm{Tr}_{2^n}\left(\frac{1}{ab}\right)=0\}$, where $S=(S_3\cup S_4)\backslash(S_3\cap S_4)$ and $n\not\equiv 0 \pmod 3$. Since $\mathrm{Tr}_{2^n}\left(\frac{1}{ab}\right)=0$ holds if and only if there exists $z\in\mathbb{F}_{2^n}$ such that $\frac{1}{ab}=z+z^2$, i.e., $ab=\frac{1}{z}+\frac{1}{z+1}$. Plugging $ab=\frac{1}{z}+\frac{1}{z+1}$ into $a^2b^2+a^2b+ab+1=0$, we have $\frac{1}{z^2}+\frac{1}{z^2+1}+(\frac{1}{z}+\frac{1}{z+1})(1+b)+1=0$, i.e.,

$$b=\frac{z^4+z+1}{z^2+z}.$$

Let $b=\frac{z^4+z+1}{z^2+z}$ and $a=\frac{1}{z^4+z+1}$. Obviously, for any $n\not\equiv 0 \pmod 3$, there exist some $z\in\mathbb{F}_{2^n}$ such that a,b exist. Therefore, $S\cap\{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*|\mathrm{Tr}_{2^n}\left(\frac{1}{ab}\right)=0\}\neq\emptyset$. That is to say, for any $n\not\equiv 0 \pmod 3$, in the case, (35) has at most six solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$.

Therefore, in this case $a\notin\{1,\omega,\omega^2\}$, the maximum of numbers of solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of (20) is

$$\begin{cases}10, & \text{if} \quad n\equiv 0 \pmod 6,\\ 8, & \text{if} \quad n\equiv 3 \pmod 6,\\ 6, & \text{if} \quad n\not\equiv 0 \pmod 3.\end{cases}$$

To sum up, together with Cases 1, 2 and 3, we know that the maximum of numbers of solutions in $\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of (20) is

$$\begin{cases}10, & \text{if} \quad n\equiv 0 \pmod 6,\\ 8, & \text{if} \quad n\equiv 3 \pmod 6,\\ 6, & \text{if} \quad n\not\equiv 0 \pmod 3.\end{cases}$$

□