A Class of Quadrinomial Permutations With Boomerang Uniformity Four

Ziran Tu, Nian Li, Xiangyong Zeng, and Junchao Zhou

***Abstract*—In Eurocrypt'18, Cid et al. proposed a new cryptanalysis tool called Boomerang Connectivity Table (BCT), to evaluate S-boxes of block ciphers. Later, Boura and Canteaut further investigated the new parameter Boomerang uniformity for cryptographic S-boxes. It is of great interest to find new S-boxes with low Boomerang uniformity for even dimensions. In this paper, we prove that a class of permutation quadrinomials over $\mathbb{F}_{2^{2m}}$ with m odd has Boomerang uniformity four, which gives the fifth class of such kind of permutation polynomials. Further, the occurrences of 0 and 4 in the BCTs of the investigated permutation polynomials are also completely determined.**

***Index Terms*—Finite field, boomerang uniformity, differential uniformity, permutation polynomial.**

I. Introduction

THE Substitution-boxes (S-boxes), which actually refer to vectorial cryptographic Boolean functions, play important roles in block ciphers. To resist known attacks, these functions are often required to meet various safety criteria including the permutation property, high nonlinearity, low differential uniformity, etc. The synthesis of these criteria makes finding qualified S-boxes a challenging task.

Wagner proposed the so-called Boomerang attack in 1999 [20], and soon afterwards several variants of this attack also arose [2]–[4], [8], [9]. Seen as extensions of differential cryptanalysis techniques, the Boomerang-style attacks have become popular to assess the security of block ciphers in recent years. The ideas of such attacks are to regard a block cipher as the composition of two sub-ciphers E_0 and E_1, and then select different characteristics for them. In 2018, Cid, Huang, Peyrin, Sasaki and Song introduced in [6] a new cryptanalysis tool known as Boomerang Connectivity Table (BCT), to evaluate the subtleties of boomerang-style attacks. The authors gave some theoretical analysis on the new BCT property, as well as some relations between BCT and DDT (Differential Distribution Table) properties. They showed that the value of the BCT entry was greater than the one in the DDT, and that for a given permutation, its BCT was 2-uniform if and only if its DDT was 2-uniform. Later, Boura and Canteaut further investigated BCT properties and the new parameter Boomerang uniformity [5], they showed that the Boomerang uniformity was preserved under an affine equivalence and inversion, but not invariant under Extended affine (EA) or Carlet-Charpin-Zinoviev (CCZ) transformations [5]. Since no APN permutation of $\mathbb{F}_{2^n}$ with even dimension $n > 6$ is known, we can deduce that the permutation with Boomerang uniformity four becomes actually optimal. To the best of our knowledge, currently over finite fields with even dimension (say $\mathbb{F}_{2^n} = \mathbb{F}_{2^{2m}}$) there are only four classes of permutations with optimal Boomerang uniformity, which are listed as follows:

1) $f(x) = x^{-1}$, $n \equiv 2 \pmod 4$ [5];
2) $f(x) = x^{2^i+1}$, $\gcd(i, n) = 2$ and $m \equiv 2 \pmod 4$ [5];
3) $f(x) = x^{2^t+2} + \gamma x$, $m = 2t$ and $\operatorname{ord}(\gamma^{2^t-1}) = 3$ [10];
4) $f(x) = \alpha x^{2^s+1} + \alpha^{2^t} x^{2^{-t}+2^{t+s}}$, $n = 3t$, $t \equiv 2 \pmod 4$, $\gcd(n, s) = 2$, $3 \,|\, (t + s)$ and α is a primitive element of $\mathbb{F}_{2^n}$ [12].

The first two monomials with optimal Boomerang uniformity were found by Boura and Canteaut [5] and the first binomial with optimal Boomerang uniformity was found by Li *et al.* [10]. Very recently, Mesnager, Tang and Xiong described in [12] more exactly the relation between BCT and DDT properties of quadratic permutations. As a consequence, they showed that the Boomerang uniformity of the Bracken-Tan-Tan binomial permutations equals four and pointed out that the quadratic permutations with optimal Boomerang uniformity obtained in [5], [10] can be readily confirmed by their results.

The purpose of this paper is to find new permutations with optimal Boomerang uniformity for even dimensions. To this end, we investigate the Boomerang uniformity of a class of quadratic quadrinomials over $\mathbb{F}_{2^n}$ with the form

$$f(x) = x^{2^{m+1}+2^m} + a_1 x^{2^{m+1}+1} + a_2 x^{2^m+2} + a_3 x^3, \qquad (1)$$

where $n = 2m$, m is odd and $a_1, a_2, a_3 \in \mathbb{F}_{2^n}$. This class of quadratic quadrinomials over $\mathbb{F}_{2^n}$ was firstly studied by Tu *et al.* [17] as permutations and then was investigated more completely by Tu *et al.* [16]. Note that the Boomerang uniformity of the above quadratic quadrinomials cannot be determined by using the relation between BCT and DDT properties of quadratic permutations obtained by Mesnager, Tang and Xiong in [12, Theorem 5] (see Remark 2) which makes the determination of its Boomerang uniformity a hard problem. In this paper, by adopting the equivalent characterization of Boomerang uniformity via the maximal number of solutions to a two-equation system obtained in [10] and employing special treatments and certain techniques

Manuscript received June 28, 2019; accepted December 10, 2019. Date of publication January 27, 2020; date of current version May 20, 2020. The work of Nian Li was supported in part by the National Natural Science Foundation of China under Grant 61702166. The work of Xiangyong Zeng was supported in part by the National Natural Science Foundation of China under Grant 61761166010.

Ziran Tu is with the School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471003, China (e-mail: tuziran@yahoo.com).

Nian Li, Xiangyong Zeng, and Junchao Zhou are with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China (e-mail: nian.li@hubu.edu.cn; xiangyongzeng@aliyun.com; zhoujunchao@hbeu.edu.cn).

Communicated by A. Canteaut, Associate Editor for Cryptography.

Digital Object Identifier 10.1109/TIT.2020.2969578