Commun. Math. Res.
doi: 10.4208/cmr.2020-0532

Vol. **38**, No. 2, pp. 223-245
May 2022

On the Differential Uniformity and Nonlinearity of a Class of Permutation Quadrinomials Over $\mathbb{F}_{2^{2m}}$

Mengyu Hu, Nian Li and Xiangyong Zeng*

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

Received 13 December 2020; Accepted 23 July 2021

Abstract. Permutation polynomials with low differential uniformity and high nonlinearity are preferred in cryptographic systems. In 2018, Tu, Zeng and Helleseth constructed a new class of permutation quadrinomials over the finite field $\mathbb{F}_{2^{2m}}$ for an odd integer m. In this paper, we aim to investigate the differential uniformity and nonlinearity of this class of permutation polynomials so as to find 4-uniform permutation polynomials with high nonlinearity.

AMS subject classifications: 05A05, 11T06, 11T23, 11T55
Key words: Differential uniformity, finite field, nonlinearity, permutation polynomial.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q^*$ denote its multiplicative group. A polynomial $f(x)$ over $\mathbb{F}_q$ is called a permutation polynomial if the induced mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a bijection. The security of most modern block ciphers relies on cryptographic properties of their S-boxes since S-boxes usually are the only nonlinear elements of these cryptosystems. Permutation polynomials over finite fields with even characteristic can be used as candidate functions of S-boxes [4]. In addition, these permutations are required to possess low differential uniformity and high nonlinearity, in order to resist differential and linear attacks.

*Corresponding author. *Email addresses:* mengyu_hu@aliyun.com (M. Hu), nian.li@hubu.edu.cn (N. Li), xzeng@hubu.edu.cn (X. Zeng)

Definition 1.1. *Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to itself. The differential uniformity of $f(x)$ is defined as follows:*

$$\delta(f)=\max_{a\in\mathbb{F}_{2^n}^*,b\in\mathbb{F}_{2^n}}\mathrm{DDT}_f(a,b),$$

where the entry of the difference distribution table (DDT) at point $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$ is given by

$$\mathrm{DDT}_f(a,b)=\#\{x\in\mathbb{F}_{2^n}:f(x)+f(x+a)=b\}.$$

Definition 1.2. *Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to itself. The nonlinearity of $f(x)$ is defined as follows:*

$$\mathcal{NL}(f)=2^{n-1}-\frac{1}{2}\mathcal{L}(f),$$

where

$$\mathcal{L}(f)=\max_{u\in\mathbb{F}_{2^n}^*,v\in\mathbb{F}_{2^n}}|\lambda_f(u,v)|,$$
$$\lambda_f(u,v)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(uf(x)+vx)}.$$

A function with low differential uniformity is believed to have enough ability to resist difference attacks [19]. Note that the lowest differential uniformity of functions over $\mathbb{F}_{2^n}$ is 2, and such functions are called APN (almost perfect nonlinear) functions. The reader is referred to [2,3,6–8] for some known constructions of APN functions. Nevertheless, almost all known APN permutations are found to be in odd dimensions and only one example is known for even dimensions (Dillon's permutation in dimension 6, see [5]). The existence of APN permutations for even dimension n ($n\geq 8$) remains an open problem (which is the well-known Big APN Problem [5]). Therefore, for even dimensions, permutations $f(x)$ with $\delta(f)=4$ offer an optimal resistance to differential attack. On the other hand, for $f\in\mathbb{F}_{2^n}[x]$, it is known that $\mathcal{NL}(f)\leq 2^{n-1}-2^{\frac{n-1}{2}}$ [9]. Functions reaching this bound are called AB (almost Bent) functions and they only exist in $\mathbb{F}_{2^n}$ for odd n. For even n, the upper bound is not tight. Finding the optimal upper bound in this case is still an open problem and the best known nonlinearity is $2^{n-1}-2^{\frac{n}{2}-1}$ [10]. Functions with high nonlinearity provide good resistance to linear attack [18]. Therefore, it is extremely significant to seek and construct 4-uniform permutation polynomials over $\mathbb{F}_{2^n}$ with high nonlinearity for even n.

In 2018, Tu *et al.* [22] initially investigated the permutation property of a class of quadrinomials with the form

$$f(x)=\bar{x}^3+a\bar{x}^2x+b\bar{x}x^2+cx^3 \tag{1.1}$$