Finite Fields and Their Applications 48 (2017) 117–125

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A note on the differential spectrum of a differentially 4-uniform power function [☆]

Maosheng Xiong [a], Haode Yan [b,*]

[a] *Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong*
[b] *School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China*

ARTICLE INFO

Article history:
Received 17 January 2017
Received in revised form 26 June 2017
Accepted 26 July 2017
Available online xxxx
Communicated by Pascale Charpin

MSC:
11T06
94A60
11T71

Keywords:
Power functions
Differential uniformity
Differential spectrum

ABSTRACT

Let $F(x) = x^{2^{2k}+2^k+1}$ be a power function over the finite field $\mathrm{GF}(2^n)$, where k is a positive integer and $n = 4k$. It is known by a recent result of Bracken and Leander that $F(x)$ is a highly nonlinear differentially 4-uniform function. Building upon this work, in this paper we determine the differential spectrum of $F(x)$.

1. Introduction

Let F be a function on the finite field $\mathrm{GF}(2^n)$. The *derivative* of F with respect to any $a \in \mathrm{GF}(2^n)$ is the function $\mathbb{D}_a F$ from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^n)$ given by

[☆] M. Xiong's research was supported by RGC No. 609513 from Hong Kong. H. Yan's research was supported by National Cryptography Development Fund under Grant MMJJ20170119.

[*] Corresponding author.
E-mail addresses: mamsxiong@ust.hk (M. Xiong), hdyan@sjtu.edu.cn (H. Yan).

http://dx.doi.org/10.1016/j.ffa.2017.07.008
1071-5797/© 2017 Elsevier Inc. All rights reserved.

$$\mathbb{D}_a F(x) = F(x+a) + F(x), \quad \forall\, x \in \mathrm{GF}(2^n).$$

For any $a \in \mathrm{GF}(2^n)^* := \mathrm{GF}(2^n) \setminus \{0\}$ and $b \in \mathrm{GF}(2^n)$, we denote

$$\delta_F(a,b) = \#\{x \in \mathrm{GF}(2^n) : \mathbb{D}_a F(x) = b\}.$$

The differential uniformity of F is defined as

$$\delta(F) = \max_{a \neq 0, b \in \mathrm{GF}(2^n)} \delta_F(a,b).$$

If $\delta(F) = \delta$, then F is said to be *differentially δ-uniform*. In particular, if $\delta(F) = 2$, then F is called almost perfect nonlinear (APN).

Differential uniformity is an important concept in cryptography as it quantifies the degree of security of the *Substitution box* used in the cipher with respect to differential attacks [1]. Power permutations of the form x^d with low uniformity serve as good candidates for the design of S-boxes not only because of their strong resistance to differential attacks but also the usually low implementation cost in hardware environment.

Let $F(x) = x^d$ for some positive integer d, then for all $a \neq 0$ we have $\delta_F(a,b) = \delta_F(1, b/a^d)$. Hence the differential characteristics of F are determined by the values $\delta_F(b) := \delta_F(1,b)$ for all $b \in \mathrm{GF}(2^n)$. The differential spectrum of F is defined in [2] as follows.

Definition 1. Let $F(x) = x^d$ be a monomial on $\mathrm{GF}(2^n)$. Denote by ω_i the number of output differences b that occur i times, that is,

$$\omega_i = \#\left\{b \in \mathrm{GF}(2^n) : \delta_F(b) = i\right\}.$$

The differential spectrum of F is the set $\mathbb{S}$ of the ω_i where i is even and $0 \leq i \leq \delta(F)$ (it is easy to see that $\omega_i = 0$ if i is odd):

$$\mathbb{S} = \left\{\omega_0, \omega_2, \cdots, \omega_{\delta(F)}\right\}.$$

As was pointed out in [2], the whole differential spectrum $\mathbb{S}$ of S-boxes is useful to analyse the resistance of the cipher to differential attacks and to its variants. Hence it is of interest to obtain the differential spectrum of power functions with low uniformity. Moreover, the problem of computing differential spectrum is also interesting and challenging from mathematical point of view and deserves some attention from researchers. Recently in [2], [3] and [4], among many other things, the differential spectra of several families of power functions with uniformity 4 and 6 have been computed.

Let $F(x) = x^{2^{2k}+2^k+1}$ be a power function over $\mathrm{GF}\,(2^n)$ where $n = 4k$. This interesting function was discovered by Dobbertin [6] to meet the conjectured nonlinearity bound and hence is called a highly nonlinear function. In an interesting paper [5] Bracken and Leander showed that the differential uniformity of $F(x)$ is 4 for any k. The purpose of