Finite Fields and Their Applications 53 (2018) 254–266

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Three new classes of generalized almost perfect nonlinear power functions

Zhengbang Zha [a,c,*], Lei Hu [b,d], Zhizheng Zhang [a]

[a] *School of Mathematical Sciences, Henan Key Laboratory of Big Data Processing and Analysis, Luoyang Normal University, Luoyang 471934, China*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[c] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*
[d] *School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China*

ARTICLE INFO

Article history:
Received 29 August 2017
Received in revised form 20 April 2018
Accepted 26 June 2018
Available online 18 July 2018
Communicated by Gary McGuire

MSC:
94A60
11T71
14G50

Keywords:
Almost perfect nonlinear function
Differential uniformity
Algebraic degree

ABSTRACT

Generalized almost perfect nonlinear (GAPN) functions are algebraic generalization of almost perfect nonlinear functions and have important applications in cryptography and finite geometry. Based on the well known binomial theorem and some combinatory formulas, the conjecture proposed by Kuroda is partially disproved and three new classes of GAPN power functions for odd characteristic are presented.

© 2018 Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail addresses: zhazhengbang@163.com (Z. Zha), hu@is.ac.cn (L. Hu).

https://doi.org/10.1016/j.ffa.2018.06.011
1071-5797/© 2018 Elsevier Inc. All rights reserved.

1. Introduction

Let p be a prime and n a positive integer. Define $\mathbb{F}_{p^n}$ be a finite field with p^n elements. Kuroda and Tsujie [11] introduced the concept of generalized almost perfect nonlinear (GAPN) function as follows:

Definition 1.1 *([11]).* A function $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ is a generalized almost perfect nonlinear (GAPN) function if the equation

$$\sum_{i \in \mathbb{F}_p} f(x + ia) = b \tag{1}$$

has at most p solutions x in $\mathbb{F}_{p^n}$ for all $a \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^n}$.

A GAPN function is a formal generalization of an almost perfect nonlinear (APN) function in characteristic 2 [1–3,6,8,13,14] to odd characteristic $p > 2$. In [11], algebraic properties and examples of GAPN functions were presented, and the applications of GAPN functions to generalized almost bent functions and dual arcs were also investigated. However, there are not many known examples of GAPN functions.

For an integer $0 \leq d \leq p^n - 1$ with base p expansion $d = \sum_{j=0}^{n-1} b_j p^j$, $0 \leq b_j < p$, its Lie weight is defined to be $\omega_p(d) = \sum_{j=0}^{n-1} b_j$. The algebraic degree of a function $f(x) = \sum_{i=0}^{p^n-1} a_i x^i \in \mathbb{F}_{p^n}[x]$ is defined as $d^o(f) = \max_{i, a_i \neq 0} \omega_p(i)$. If $d^o(f) \leq 1$, then f is called an affine function.

Two functions $f, g : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ are called extended affine (EA) equivalent if $g = A_1 \circ f \circ A_2 + A_0$ for two affine permutations A_1 and A_2 and an affine function A_0. Nonconstant EA equivalent functions have the same algebraic degree. It is shown in [4] that EA equivalence is a particular case of Carlet–Charpin–Zinoviev (CCZ) equivalence and that every invertible function (namely a permutation over $\mathbb{F}_{p^n}$) is CCZ equivalent to its inverse. However, it was showed by Kuroda and Tsujie [11] that for some invertible GAPN functions, their inverses are not GAPN functions, which means a function CCZ equivalent to a GAPN function may be not again a GAPN function, and it seems very complicated to study the CCZ equivalence of GAPN functions. Below we only consider the equivalence of GAPN functions in terms of EA equivalence, which has the following properties:

Proposition 1.2 *([11]). Let $f, g : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ be EA equivalent functions. Then f is a GAPN function if and only if g is a GAPN function.*

Proposition 1.3 *([5]). Let k and l be integers with $0 \leq k, l < p^n - 1$. Define $p_k(x) = x^k$ and $p_l(x) = x^l$ be power functions on $\mathbb{F}_{p^n}$. Then p_k and p_l are EA equivalent if and only if there exists an integer $0 \leq a < n$, such that $l \equiv p^a k \pmod{p^n - 1}$.*

Download English Version:

https://daneshyari.com/en/article/8895609

Download Persian Version:

https://daneshyari.com/article/8895609

Daneshyari.com