Finite Fields and Their Applications 40 (2016) 73–89

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

New explicit constructions of differentially 4-uniform permutations via special partitions of $\mathbb{F}_{2^{2k}}$

Jie Peng [a,b,*,1], Chik How Tan [c]

[a] School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Luoyu Road #152, Wuhan 430079, PR China
[b] Shanghai Key Laboratory of Intelligent Information Processing, PR China
[c] Temasek Laboratories, National University of Singapore, 5A Engineering Drive 1, 09-02, 117411 Singapore

ARTICLE INFO

Article history:
Received 11 August 2015
Received in revised form 1 December 2015
Accepted 10 March 2016
Available online 25 March 2016
Communicated by Gary McGuire

MSC:
94A60
11T71
14G50

Keywords:
Differentially 4-uniform
Permutation function
S-box
Coset of subgroup
ω-Congruent

ABSTRACT

In this paper, we further study the switching constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ from the inverse function and propose several new explicit constructions. In our constructions, we first partition the finite field $\mathbb{F}_{2^{2k}}$ into some minimal subsets that are closed under both mappings $x \mapsto \frac{1}{x^{-1}+1}$ and $x \mapsto \omega x$, where $\omega \in \mathbb{F}_{2^{2k}}^*$ is of order 3. Then, by utilizing some properties of such subsets to extend differentially 4-uniform permutations over the subfield $\mathbb{F}_4$ or $\mathbb{F}_{2^4}$ to that over $\mathbb{F}_{2^{2k}}$, we give new constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for the cases k odd, $k/2$ odd and $k/2$ even respectively. As compared to previous constructions, our new constructions explicitly give large numbers (at least $2^{2^{2k-2}-1}$) of functions.

[*] Corresponding author.
E-mail addresses: jiepeng@mail.ccnu.edu.cn (J. Peng), tsltch@nus.edu.sg (C.H. Tan).
[1] Now the author is visiting Temasek Laboratories, National University of Singapore.

http://dx.doi.org/10.1016/j.ffa.2016.03.003
1071-5797/© 2016 Elsevier Inc. All rights reserved.

1. Introduction

Throughout this paper, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements and $\mathbb{F}_{2^n}^*$ be the corresponding cyclic group of order $2^n - 1$. For ease of implementation and to have good cryptographic properties to resist various kinds of cryptographic attack, substitution boxes (S-boxes) used in block ciphers are often chosen from permutation functions over $\mathbb{F}_{2^{2k}}$ with low differential uniformity [1], high nonlinearities [23] and high algebraic degrees [18]. It is known that for any function F over $\mathbb{F}_{2^n}$, its differential uniformity is always a positive even integer. If its differential uniformity is 2, then the function F is said to be an almost perfect nonlinear function (APN function for short).

Although many APN functions have been found over $\mathbb{F}_{2^n}$ for n odd and for n even respectively (see [2,3,6–9,12,15]), it is very hard to construct APN permutations for n even. Until now, only one APN permutation over $\mathbb{F}_{2^6}$ has been found by Dillon et al. in [13]. To find any other APN permutations for even n is called the BIG APN problem. Therefore, people have to use differentially 4-uniform permutations as S-boxes. For instance, the S-box of the Advanced Encryption Standard (AES) is constructed from the inverse function x^{-1} $(0^{-1} := 0)$ over $\mathbb{F}_{2^8}$, which is differentially 4-uniform with the known maximum nonlinearity and the optimal algebraic degree.

There are 5 primarily constructed infinite classes of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ which have been proved to possess the known maximum nonlinearity. They are 4 classes of power functions, namely the Gold functions [16], the Kasami functions [17], the inverse functions [24] and the Bracken–Leander functions [4], together with a class of binomials [5]. Besides, many secondary construction methods have been proposed and studied to obtain more differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via known differentially 2/4-uniform functions, for instance, the switching method [25–30], the contraction method (from $\mathbb{F}_{2^{2k+1}}$ to $\mathbb{F}_{2^{2k}}$) [10,20] and the expansion method (from $\mathbb{F}_{2^{2k-1}}$ to $\mathbb{F}_{2^{2k}}$) [11], etc.

The switching method has attracted much attention recently and a lot of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ have been constructed by modifying the inverse function in some special subsets of $\mathbb{F}_{2^{2k}}$. In [29], the authors applied some affine transformations to the inverse function on some particular subfields of $\mathbb{F}_{2^{2k}}$ and obtained two classes of differentially 4-uniform permutations. In [21], the authors investigated the construction of differentially 4-uniform permutations by composing the inverse function and a cycle. In particular, the research on constructing differentially 4-uniform permutations of the form

$$F(x) = x^{-1} + f(x), \text{ where } f(x) \text{ is an } n\text{-variable Boolean function,} \tag{1}$$

is more active. A lot of such differentially 4-uniform permutations were found in [26]. In addition, it was proved in [26] that all the permutations of the form (1) have the optimal algebraic degree and high nonlinearity that is not less than $2^{n-2} - \frac{1}{4}\lfloor 2^{\frac{n}{2}+1} \rfloor - 1$. The authors of [27] generalized the technique of [26] and further proved that if $F(x)$