Finite Fields and Their Applications 47 (2017) 309–329

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the construction of differentially 4-uniform involutions

Yuwei Xu [a,b], Yongqiang Li [a,c,b,*], Chuankun Wu [a], Feng Liu [a]

[a] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*
[b] *School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*
[c] *Science and Technology on Communication Security Laboratory, Chengdu, China*

ARTICLE INFO

Article history:
Received 16 August 2016
Received in revised form 28 February 2017
Accepted 14 June 2017
Available online xxxx
Communicated by Gary McGuire

MSC:
06E30
11T06
94A60

Keywords:
Involution
Differential uniformity
Nonlinearity
Algebraic degree

ABSTRACT

An involution is a permutation whose compositional inverse is itself. Differentially 4-uniform involutions with high algebraic degree and high nonlinearity are important for the design of block ciphers because they possess good cryptographic properties and the same component can be used in both encryption circuit and decryption circuit. A well known differentially 4-uniform involution is the multiplicative inverse function, which is used as the S-boxes in AES and Camellia. Although many differential 4-uniform permutations have been constructed, there are only a few classes of differentially 4-uniform involutions. Recently, Charpin et al. presented an idea of constructing involutions, which is called piece by piece construction. With this method, we construct a family of differentially 4-uniform involutions with optimal algebraic degree and high nonlinearity. It is also shown with the help of computer that such involutions which are CCZ-inequivalent to the known differentially 4-uniform permutations in small number of even dimensions are constructed. Furthermore, the

* Corresponding author at: State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.
E-mail addresses: xuyuwei@iie.ac.cn (Y. Xu), yongq.lee@gmail.com (Y. Li).

http://dx.doi.org/10.1016/j.ffa.2017.06.004

number of CCZ-inequivalent classes of our involutions over $\mathbb{F}_{2^n}$ increases exponentially when n increases.

1. Introduction

In symmetric cryptography, permutation polynomials are often chosen as substitution boxes (S-boxes) to serve as the confusion components in symmetric algorithms. For the ciphers designed with substitution–permutation (SP) structures (*e.g.* AES), it needs to implement the compositional inverses of S-boxes to decrypt a ciphertext. An involution G is a permutation which is its own compositional inverse, i.e., $G \circ G$ is the identity function. For more details of involutions, we refer the reader to [8]. Then the circuit of an involution S-box can be used in both encryption circuit and decryption circuit. This means the implementation of decryption algorithm does not require additional resources. Hence involutions are important for the design of block cipher algorithms, especially for the ciphers used in the resource limited environment.

For the efficiency of implementation, S-boxes are often designed as permutations over $\mathbb{F}_{2^n}$ with n even. To resist various attacks, S-boxes should also possess good cryptographic properties, such as low differential uniformity, high algebraic degree and high nonlinearity. The lower bound of differential uniformity of the functions over $\mathbb{F}_{2^n}$ is 2, and the functions with differential uniformity 2 are called almost perfect nonlinear (APN) functions. However, only one APN permutation over $\mathbb{F}_{2^6}$ was found [10], which is CCZ-equivalent to a quadratic function and not suitable for an S-box. It is a big open problem that whether there exists an APN permutation over $\mathbb{F}_{2^n}$ with even $n \geq 8$.

Thus the construction of differentially 4-uniform permutations with high algebraic degree and high nonlinearity is crucial for the design of block ciphers, and has attracted attentions of many researchers. For the convenience of readers, we list the known differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ for even n as follows.

– **Power functions**
  - The *(multiplicative) inverse function* $I(x) = x^{2^n-2}$ (i.e., x^{-1} with the convention $0^{-1} = 0$) [15]. It has the optimal algebraic degree $n-1$ and the best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$.
  - The Gold function $G_1(x) = x^{2^s+1}$ with $\gcd(s,n) = 2$, $n = 2k$ and k odd [11,15]. It has the best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$, but it is quadratic.
  - The Kasami function $G_2(x) = x^{2^{2s}-2^s+1}$ with $\gcd(s,n) = 2$, $n = 2k$ and k odd [2]. It has the best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$, and its algebraic degree is less than $n-1$.
  - The function $G_3(x) = x^{2k+k+1}$ with $n = 4k$ and k odd [3]. It has the best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$, and its algebraic degree is 3.