Constructions of Complete Permutation Polynomials *

Chunlei Li

Department of Informatics,
University of Bergen, Norway

A polynomial $f(x)$ over $\mathbb{F}_q$ is called a *complete permutation polynomial* (CPP) if both $f(x)$ and $f(x)+x$ are permutations of $\mathbb{F}_q$. These polynomials were introduced by Mann in the construction of orthogonal Latin squares. Niederreiter and Robinson later gave a detailed study of CPPs over finite fields. CPPs over finite fields $\mathbb{F}_q$ in even characteristic are the same as the orthomorphisms, which have a single fixed point and map each maximal subgroup of the additive group of $\mathbb{F}_q$ half into itself and half into its complement. Moreover, nonlinear orthomorphisms also have good bit independence and avalanche characteristics. CPPs (or orthomorphisms) with these properties are of cryptographic interest and were firstly utilized by Mittenthal in the design of nonlinear dynamic substitution device. Researchers later investigated the applications of CPPs in the Lay-Massey scheme, the block cipher SMS4, the stream cipher Loiss, the design of Hash functions, quasigroups, and also in the constructions of some cryptographically strong functions. However, CPPs are rare objects and there are a limited number of known constructions.

The Feistel structure and MISTY structure, in which inputs are divided into small units and the units are further manipulated to produce outputs, have been widely used in the context of block cipher design. The internal transformations in the Feistel and MISTY structures together with the feature of known CPPs motivate the study of this paper.

In this talk, we will introduce new construction methods of CPPs over finite fields with the Feistel and MISTY structures and discuss the properties of the constructed CPPs.

*Joint work with Xiaofang Xu, Xiangyong Zeng and Tor Helleseth