Relevant classes of polynomial functions with applications to Cryptography

Daniele Bartoli

Università degli Studi di Perugia - Dipartimento di Matematica e Informatica

Abstract

A number of different polynomial functions over finite fields have relevant applications in applied areas of Mathematics, as Cryptography or Coding Theory. Among them, APN functions, PN functions, APN permutations, permutation polynomials have been widely studied in the recent years.

In order to investigate non-existence of such functions or to provide constructions of infinite families, algebraic varieties over finite fields are a useful tool. In this direction, a key ingredient is an estimate of the number of rational points of such algebraic varieties and therefore Hasse-Weil type theorems (Lang-Weil, Serre,...) play a fundamental role.

The aim of this talk is to summarize recent results in this direction.