APN functions and their links to geometry

Yves Edel
Department of Pure Mathematics and Computer Algebra
Ghent University
Krijgslaan 281, S22, B-9000 Ghent, Belgium

Abstract

A function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is called almost perfect nonlinear (APN) iff for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ the equation $f(x + a) - f(x) = b$ has at most two solutions. APN functions arose in the context of cryptography. We present selected recent results and point out links to finite geometry.