Some New Results on the Conjecture on APN Functions and Absolutely Irreducible Polynomials

Moises Delgado and Heeralal Janwa* (UPR-Cayey, UPR-Rio Piedras, Puerto Rico)

Almost Perfect Nonlinear (APN) functions are very useful in cryptography, when they are used as S-Boxes, because of their good resistance to differential cryptanalysis. An APN function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is called exceptional APN if it is APN on infinitely many extensions of $\mathbb{F}_{2^n}$. Aubry, McGuire and Rodier conjectured that the only exceptional APN functions are the Gold and the Kasami-Welch monomial functions. They established that a polynomial function of odd degree is not exceptional APN provided the degree is not a Gold number (2^k+1) or a Kasami-Welch number $(2^{2k}-2^k+1)$. When the degree of the polynomial function is a Gold number, Partial results have been obtained by several authors including us.

In this talk, we will present some new results towards the resolution of the stated conjecture.

We also show absolute irreducibility of several classes of multivariate polynomials over finite fields and discuss their applications.

Keywords: APN functions, exceptional APN functions, Janwa-McGuire-Wilson conjecture, absolutely irreducible polynomials, S-Boxes, Differential Cryptanalysis.

2000 Mathematics Subject Classification: 94A60, 20C05, 05B10, 11T71