Resolution of the Exceptional APN Conjecture for the Gold Degree Case

Carlos Agrinsoni[1],
(Joint work with **Heeralal Janwa**[2] and **Moises Delgado**[3])

A function $f : \mathbb{F}_q \to \mathbb{F}_q$, is called an *Almost Perfect Nonlinear* (APN) function if the equation $f(x + a) - f(x) = b$ have at most 2 solutions for every $b, a \in \mathbb{F}_q$, with a nonzero. APN functions arise in cryptography as functions that minimize the probability of success of the differential cryptanalysis. A function is called an exceptional APN if it is APN on infinitely many extensions of $\mathbb{F}_q$. This problem was reduced by Janwa and Wilson and then by Rodier to the study analysis of the absolute irreducibility of the corresponding multivariate polynomial $\phi_f(x, y, z)$. Aubry, McGuire, and Rodier (AMR) conjectured that the only exceptional APN functions up to CCZ equivalence are the monomials of degrees (2^k+1) or $(2^{2k}-2^k+1)$ (called the Gold case or the Kasami-Welch case). AMR established that that odd degree exceptional APN functions necessarily must begin with said monomials. The AMR result was refined further by several authors, and partial results on the resolution of the conjecture have been given.

In this seminar, we will present our recent resolution of the Gold degree case of the exceptional APN conjecture.

Keywords: Almost Perfect Nonlinear (APN) Conjecture, Absolute Irreducibility, Lang-Weil, Deligne, and Ghorpade-Lachaud bounds on rational points on varieties over finite fields

[1]Mathematics
Purdue University
150 N University St, West Lafayette, Indiana, 47907-2067, USA
`cagrinso@purdue.edu`

[2]Mathematics
University of Puerto Rico Rio Piedras
14 Ave Universidad Ste 1401 San Juan PR 00925-2534
`heeralal.janwa@upr.edu`

[3]Mathematics and Physics
University of Puerto Rico Cayey
205 Calle Antonio R. Barcelo, Cayey, 00736
`moises.delgado@upr.edu`