Recent Advances Towards the Conjecture of Exceptional APN Functions

Moises Delgado, Universsity of Puerto Rico at Cayey

Almost perfect nonlinear (APN) functions defined over finite fields $\mathbb{F}_q$, where $q = 2^n$, are called exceptional APN if they are APN on infinitely many extensions of $\mathbb{F}_q$. A conjecture of Janwa-Wilson and McGuire-Janwa-Wilson (1993/1996), settled in 2011, was that the only monomial exceptional APN functions were x^{2^k+1} or $x^{2^{2k}-2^k+1}$ (the Gold or the Kasami-Welch functions respectively). A subsequent conjecture, stated by Aubry, McGuire and Rodier (2009), states that any exceptional APN function is one of the monomials described above. Recently we proved several results including that polynomial functions of the form $f(x) = x^{2^k+1} + h(x)$ (with some conditions in h) can not be exceptional APN, extending substantially several recent results towards the resolution of this conjecture. In this talk we give some background and show some techniques used to obtain our results.

Keywords: APN function, Exceptional APN function, Exceptional APN conjecture, Gold number.