Extensions of some Results on the Conjecture on Exceptional APN Functions and Absolutely Irreducible Polynomials: the Gold Case

Moises Delgado UPR-Cayey, Heeralal Janwa, UPR Rio Piedras

An almost perfect nonlinear (APN) function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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 $(2^{2k} - 2^k + 1)$. Several partial results have been obtained by several authors including us. In the culmination of a series of articles, we proved the exceptional APN conjecture in the Gold degree case when $f(x) = x^{2^k+1} + h(x)$, where $\deg(h(x))$ is odd, except for a few remaining cases and showed exactly when the corresponding multivariate polynomial $\phi(x, y, z)$ is absolutely irreducible. We also improved the sole known result when $\deg(h(x))$ is even. Now we will present further extension of this last result, thus making progress in this relatively difficult Gold degree case.