XI XIE, Hubei University & Carleton Univeresity

On the Niho type locally-APN power functions and their boomerang spectrum

In this talk, we focus on the so-called locally-APN power functions introduced by Blondeau, Canteaut and Charpin, which generalize the well-known notion of APN functions and possibly more suitable candidates against differential attacks. Specifically, given two coprime positive integers m and k such that $\gcd(2^m+1, 2^k+1) = 1$, we investigate the locally-APN-ness property of the Niho type power function $F(x) = x^{s(2^m-1)+1}$ over the finite field $\mathbb{F}_{2^{2m}}$ for $s = (2^k+1)^{-1}$, where $(2^k+1)^{-1}$ denotes the multiplicative inverse modulo 2^m+1. By employing finer studies of the number of solutions of certain equations over finite fields, we prove that $F(x)$ is locally-APN and determine its differential spectrum. We emphasize that computer experiments show that this class of locally-APN power functions covers all Niho type locally-APN power functions for $2 \leq m \leq 10$. In addition, we also determine the boomerang spectrum of $F(x)$ by using its differential spectrum, which particularly generalizes a recent result by Yan, Zhang and Li.