GOHAR KYUREGHYAN, University of Rostock

New and old insights on APN maps

An APN map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by the property that for every non-zero $a \in \mathbb{F}_{2^n}$ the set $D_a = \{f(x+a) + f(x) \mid x \in \mathbb{F}_{2^n}\}$ contains exactly 2^{n-1} elements. The APN maps provide optimal resistance against differential attacks in cryptological applications, and they yield constructions for special codes. In this talk we show that to check the APN property for a generic map it is enough to consider the sets D_a for elements a from a hyperplane. We present some results on the image sets of APN maps, which indicate that a better understanding of the image sets of APN maps will allow progressing on some of main challenges in the research area.

The talk is based on joint works with Pascale Charpin and Lukas Kölsch, Björn Kriepke.