New Generalized APN functions of the lowest algebraic degree

Noureddine El-Asri*[1]

[1]Université de Rouen Normandie – Normandie Université – France

Résumé

Noureddine El-Asri : New Generalized APN functions of the lowest algebraic degree
Almost Perfect Nonlinear (APN) functions are the functions that resist the best against differential cryptanalysis of block ciphers in characteristic two. Due to their properties, APN functions have applications in other domains such as finite geometry and coding theory. Kuroda and Tsujie generalized this notion to fields of arbitrary characteristic by defining the notion of Generalized APN (Almost Perfect Nonlinear) functions.

Not much is known about GAPN functions in the litterature, and most of the constructions are for functions of Hamming degree 2 and with the lowest algebraic degree possible, which coincides with the field characteristic. In this talk, we first present new constructions for monomial GAPN functions for arbitrary Hamming degree, and, for a special case of such monomial functions, we give necessary and sufficient conditions so that they are GAPN. Then, we present new constructions for multinomial GAPN functions of Hamming degree 2, 3 and 5.

Collaboration avec Valentin Suder

*Intervenant