New Efficient Differentially δ-Uniform Functions

Roberto Reyes Carranza[1]*, Heeralal Janwa[2], 1) UPR Mayagüez, 2)UPR Rio Piedras.

this talk, we present constructions of new differentially δ-uniform vectorial Boolean functions. Our families have a univariate polynomial representations with very few terms. Thus our Boolean functions can be efficiently implemented in cryptographic applications.

We present a new theorem that yields us a two parametric family of functions. As a particular case, we generalize the well known theorems of Budaghyan and Carlet, which involve the absolute trace. This way, we also obtain new cubic APN functions. Different parameters generalize other known results, and others yield new families with strong nonlinearity and algebraic degrees. Our functions offer strong resistance to both first and second order Fourier transform analysis.

We include tables of the values of Walsh Spectrum and other cryptographic properties of the Gold family over finite fields up to degree 15. These include values that have not been computed by others. We thus show that there are cases where Gold families are weak with respect to some cryptographic protocols such as nonlinearity profile, where our aforementioned two parametric families are better.

We give a variation of the idea of switching neighbor of Pott, Pott-Budaghyan (also known as Dillon's Method), which yields further generalizations, leading to another new δ-uniform family of functions.

Keywords: differentially δ-uniform functions; APN functions; Nonlinearity.