

KARIN ARIKUSHI
Carleton University

Almost perfect nonlinear polynomials

Cryptographic systems such as AES and DES, which utilize S-boxes, must be resistant to differential cryptanalysis in order to be effective. Almost Perfect Nonlinear (APN) functions are, by definition, optimally resistant to differential attacks and are good candidates for use in S-boxes. However, it is still an open problem to find and classify all APN functions over finite fields.

Until recently, the only known APN polynomials were power functions, i.e. functions of the form $f(x) = x^d$. In the last five years, new binomial and multinomial examples have also been found. We will consider a recent class of APN binomials over \mathbb{F}_{3^n} found by Ness and Helleseth. They proved the APN property using quadratic characters, so we will present a modified approach using different characters. This is still work in progress, but we hope that this method will yield a new class of APN multinomials.