Differential uniformity and exceptional APN polynomials

Ali Issa

Institut de Mathématiques de Marseille - I2M
Aix-Marseille University

Abstract

The differential uniformity is introduced by Nyberg to get a resistance against differential attacks. In our context the differential uniformity of a polynomial $f \in \mathbb{F}_{2^n}[x]$ is the greatest number of solutions can have the equation $f(x) + f(x+\alpha) = \beta$ in $\mathbb{F}_{2^n}$ where α and β belong to $\mathbb{F}_{2^n}$ with α non zero:

$$\delta_{\mathbb{F}_{2^n}}(f) = \max_{(\alpha,\beta)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \text{card}\{x \in \mathbb{F}_{2^n} | f(x) + f(x+\alpha) = \beta\}.$$

A particular interest is being placed on APN (for Almost Perfect Nonlinear) polynomials. That is polynomials f such that $\delta_{\mathbb{F}_{2^n}}(f) = 2$, the smallest value $\delta_{\mathbb{F}_{2^n}}$ can have. APN polynomials which are APN over infinitely many extensions of $\mathbb{F}_{2^n}$ are called exceptional APN polynomials. Aubry, McGuire and Rodier have conjectured that (under an equivalence condition) the only exceptional APN polynomials are the monomials $x^{2^l}+1$ and $x^{4^l-2^l+1}$. This conjecture has been proved for monomials by Hernando and McGuire and still open for polynomials. In this talk, we contribute to the exceptional APN conjecture in the trinomials case. More precisely we introduce an infinite set of even degree m for which no trinomials of the form $f(x) = a_0x^m + a_1x^{m-1} + a_2x^{m-2}$ can be exceptional APN. This is a joint work with **Yves Aubry** and **Fabien Herbaut**.