Maximal differential uniformity of polynomials of some given degrees

Yves Aubry, Fabien Herbaut and Ali Issa

Institut de Mathématiques de Toulon - IMATH, Université de Toulon

In what follows we will consider integers n, $q = 2^n$, and polynomials $f \in \mathbb{F}_q[x]$ of degree m. Kaisa Nyberg has defined in [1] the differential uniformity $\delta(f)$ of a polynomial $f \in \mathbb{F}_q[x]$ as the greatest number of solutions of the set of equations $f(x+\alpha) + f(x) = \beta$ where α and β belong to $\mathbb{F}_q$ with α non-zero. When $\delta(f) = 2$ the associated functions are called APN (Almost Perfectly Nonlinear): these functions have been extensively studied as they offer good resistance against differential attacks. Among them, those which are APN over infinitely many extensions of $\mathbb{F}_q$ have attracted special attention.

In the opposite direction, Felipe Voloch has proven in [3] that most polynomials $f \in \mathbb{F}_q[x]$ of degree $m \equiv 0$ or $3 \pmod 4$ have differential uniformity equal to $m-1$ or $m-2$, the largest possible for polynomials of degree m. Precisely, he proved that for a given integer $m > 4$ such that $m \equiv 0 \pmod 4$ (respectively $m \equiv 3 \pmod 4$), if $\delta_0 = m-2$ (respectively $\delta_0 = m-1$) then

$$\lim_{n\to\infty} \frac{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m,\ \delta(f) = \delta_0\}}{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m\}} = 1.$$

In [2], Yves Aubry, Fabien Herbaut and Felipe Voloch have improved this result for certain degrees. They describe a set of specific degrees m such that for q sufficiently large, all polynomials $f \in \mathbb{F}_q[x]$ of degree m have a maximal differential uniformity.

But the results of [2] require to consider a very specific condition on the degree m. Furthermore, the methods only apply to odd degrees m. The aim of our work is to obtain results and to develop methods that also apply for even degrees.
First we will discuss the case of some specific trinomials of degree $m \equiv 0 \pmod 4$. Later we treat the polynomials of degree 3.2^k and 5.2^k. Precisely we prove the following theorems:

Theorem 0.1. *Let $r \geq 2$ and $m = 3.2^r$ or $m = 5.2^r$. For n sufficiently large and for all polynomials $f(x) = \sum_{k=0}^{m} a_{m-k}x^k \in \mathbb{F}_{2^n}[x]$ such that $a_1 \neq 0$ the differential uniformity $\delta(f)$ is maximal, that is $\delta(f) = m-2$.(And so f is not exceptional APN)*

Bibliography

[1] Kaisa Nyberg, *Differentially uniform mappings for cryptography.* In *Advances in cryptology, Eurocrypt 93, Springer (1994), 55-64.*

[2] Yves Aubry, Fabien Herbaut, and José Felipe Voloch, *Maximal differential uniformity polynomials, Acta Arithmetica,* vol *188 no. 4 (2019), 345-366.*

[3] José Felipe Voloch, *Symmetric cryptography and algebraic curves.* In *Proceedings of the First SAGA Conference, Papeete, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, (2008), 135-141*

Yves Aubry, Institut de Mathématiques de Toulon - IMATH,
Université de Toulon and Institut de Mathématiques de Marseille - I2M,
Aix Marseille Université, CNRS, Centrale Marseille, UMR 7373, France
E-mail address: yves.aubry@univ-tln.fr

Fabien Herbaut, INSPE Nice-Toulon, Université Côte d'Azur,
Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
E-mail address: fabien.herbaut@univ-cotedazur.fr

Ali Issa, Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
E-mail address: ali.issa@univ-tln.fr