Crooked and weakly crooked functions

Pascale Charpin
INRIA-Paris, France.

Abstract

Crooked functions were introduced by Bending and Fon-Der-Flass (1998). These authors called *crooked function* a bijective function F, from $\mathbb{F}_{2^n}$ to itself, whose derivatives have as image set a complement of hyperplane. A generalisation to the non-bijective crooked functions is due to Kuyreghyan (2007). Furthermore, Canteaut and Naya-Plasencia extended this concept to the so-called *crooked function of codimension* k (2009). In this case, the image set of any derivative is an affine subspace of codimension k.

We extend these definitions to functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, where p is any prime. Recall that the *derivative* of F in point $a \in \mathbb{F}_{p^n}$, $a \neq 0$, is the function

$$D_aF \ : \ x \mapsto F(x+a) - F(x), \text{ from } \mathbb{F}_{p^n} \text{ to } \mathbb{F}_{p^n}.$$

We will say that F is a *weakly crooked* function when the image set of any function D_aF is an affine subspace, *i.e.,* these image sets may have different sizes.

The set of weakly crooked functions includes the functions F, which are quadratic, *i.e.,* of algebraic degree equal to 2 or, equivalently, whose derivatives are linear or constant. Furthermore the *planar functions* are crooked function of codimension 0. However it remains an open problem to construct other classes of (weakly) crooked functions.

We point out that *partially-bent* functions provide a relevant tool to describe weakly crooked functions. Moreover, the existence of linear structures for component functions, of the given F, are decisive factors to construct weakly crooked functions. We show how to determine linear structures by a symbolic computation. We later come back to the binary case and present some properties of crooked functions.

Keywords: crooked, vectorial function, partially-bent, bent, APN functions, plateaued, Boolean function, permutation, image set of functions