On relations between CCZ and EA-equivalences

Marco Calderini

Department of Informatics, University of Bergen, Norway
joint work with: Lilya Budaghyan, Irene Villa

Let F and F' be two vectorial Boolean function from $\mathbb{F}_{2^n}$ to itself. We say that F and F' are EA-equivalent if there are affine mapping A and affine permutations A_1, A_2 such that $F'(x) = A_2 \circ F \circ A_1(x) + A(x)$. They are called CCZ-equivalent if there exists an affine permutation $\mathcal{L} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ such that $G_{F'} = \mathcal{L}(G_F)$, where $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$.

The nonlinearity and differential uniformity are properties of a vectorial Boolean function measuring its resistance to linear and differential attacks. APN and AB functions provide optimal resistance against these attacks.

The CCZ-equivalence is the most general known equivalence relation of functions for which the nonlinearity and the differential uniformity (and, therefore, APNness and ABness) are invariant. The notion of CCZ-equivalence is difficult to handle, indeed checking whether two given functions are CCZ-equivalent or not is hard. Also building functions CCZ-equivalent (but not EA-equivalent) to a given function is hard.

On the contrary, EA-equivalence is simpler to check and, given some function, building EA-equivalent ones is very easy. Hence, identifying situations in which CCZ-equivalence reduces to EA-equivalence is useful.

For quadratic APN (AB) functions, in particular for Gold functions, it is possible, by using CCZ-equivalence, to construct functions EA-inequivalent to the starting function and its inverse (when it exists), and more generally to any power function.

In the first part of this talk, we will discuss some properties of the CCZ-equivalence and EA-equivalence and their relations. Then, we will show a procedure which allows, at least in small dimension, to investigate if the CCZ-equivalence leads to more functions than applying EA-equivalence and inverse transformation (when it is possible), for the case of non quadratic functions. This procedure permits, also, to investigate the problem of determining if a given function F is EA-equivalent to a permutation.

In the last part of the talk we will focus on the classification of APN functions. There are twelve classes of APN functions which are CCZ-inequivalent to power functions. We will show that of these twelve classes, only ten are distinct. In particular, we will show that two of these families (defined for n even) are a particular case of the hexanomials introduced by Budaghyan and Carlet.