On Sboxes sharing the same DDT

Anne Canteaut
(Joint work with Christina Boura, Jérémy Jean and Valentin Suder)

This work focuses on two different equivalence notions for vectorial Boolean functions, that we call DDT and γ-equivalence. The first one applies to functions sharing the same difference distribution table while the second applies more generally to functions whose DDT have the same support. The γ-equivalence classes for quadratic APN functions have been recently studied by Gorodilova. She most notably proved that the size of the γ-class for any function is invariant under extended-affine equivalence, and she then wondered whether something similar could be proved for CCZ-equivalence. Here, we give an answer to this question by proving that the number of elements in the differential equivalence class of a function is invariant under CCZ-equivalence.

In parallel, we also provide an algorithm for computing the differential equivalence class corresponding to a prescribed DDT. We applied this algorithm to find several equivalence classes. Most notably, one of the main problems we focus on is to determine whether the differential equivalence class of a permutation over $\mathbb{F}_2^n$ can contain more than 2^{2n} elements. In other words, we wonder whether two permutations F and G with the same DDT necessarily satisfy $G(x) = F(x \oplus c) \oplus d$ for some $c, d \in \mathbb{F}_2^n$. As a result, we found permutations F whose differential equivalence classes contain other elements than the functions $x \mapsto F(x \oplus c) \oplus d$. However, we conjecture that this is only the case when some rows of the corresponding DDT are equal.