On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting

Leo Perrin

Two vectorial Boolean functions are "CCZ-equivalent" if there exists an affine permutation mapping the graph of one to the other. It preserves many of the cryptographic properties of a function such as its differential and Walsh spectra, which is why it could be used by Dillon et al. to find the first APN permutation on an even number of variables. However, the meaning of this form of equivalence remains unclear. In fact, to the best of our knowledge, it is not known how to partition a CCZ-equivalence class into its Extended-Affine (EA) equivalence classes; EA-equivalence being a simple particular case of CCZ-equivalence.

In this talk, we characterize CCZ-equivalence as a property of the zeroes in the Walsh spectrum of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ or, equivalently, of the zeroes in its difference distribution table. We use this framework to show how to efficiently upper bound the number of distinct EA-equivalence classes in a given CCZ-equivalence. More importantly, we prove that it is possible to go from a specific member of any EA-equivalence class to a specific member of another EA-equivalence class in the same CCZ-equivalence class using an operation called *twisting*; so that CCZ-equivalence can be reduced to the association of EA-equivalence and twisting. Twisting a function is a simple process and its possibility is equivalent to the existence of a particular decomposition of the function considered.

Using this knowledge, we revisit several results from the literature on CCZ-equivalence and show how they can be interpreted in light of our results. We also provide simple criteria for the existence of a permutation in the CCZ-equivalence class of any function. In the case of APN quadratic function, it is computationally very efficient and allows us to experimentally show that a 16-bit APN quadratic function cannot be CCZ-equivalent to a permutation using several hours on a regular desktop computer.