Exploring the Set of APN Functions in Practice

Pierre Galissant*[1]

[1]Inria – Inria Paris – France

Abstract

In this work, we investigate known structures in the set of APN functions by establishing new results about the structure of the CCZ-equivalence class of APN functions, in particular quadratic ones. These advances allow us to build a tinySQL database containing exactly one representative of each extended-affine class of APN function over 6 bits and 7 bits.

We also provide and new results about the structure of the set of switching neighbours and improved algorithms to compute them, which allows us to experimentally investigate what the switching neighbours of known functions are. The code and databases will be made available in sboxU.

Having a representative of all known EA-classes means it becomes practical to test if a new function is actually new. Furthermore, a better understanding of the notion of switching neighbors from the theoretical and the computational point of view allows us to efficiently move out of CCZ classes. Thus, we were able to check if new functions could be found in the switching neighbours of all known EA-classes for 6 and 7-bits. For 8-bits, due to the amount of computation, we only focused on quadratic functions.

*Speaker