ANNE CANTEAUT, Inria Paris

Searching for APN permutations with the butterfly construction

The existence of APN permutations operating on an even number of variables was a long-standing open problem, until an example with six variables was exhibited by Dillon et al. in 2009. However it is still unknown whether this example can be generalized to any even number of inputs. This talk investigates the cryptographic properties of butterflies: they form a family of involutions operating on (4k+2) variables and with differential uniformity at most 4, which contains the Dillon permutation. We will also prove that this generalized family does not contain any APN permutation besides the Dillon permutation.