EA-equivalence classes of known APN functions in small dimensions

Marco Calderini

Department of Informatics, University of Bergen, Norway

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.

Among the equivalence relations for (vectorial) Boolean functions preserving the nonlinearity and differential uniformity we have *affine equivalence*, *EA-equivalence* and the more general relation *CCZ-equivalence*.

Classification of Boolean functions, and in particular of APN functions, is a hard open problem. Recently, Brinkmann gave the full classification of all functions defined over $\mathbb{F}_{2^n}$ for $n \leq 4$ with respect to EA- and CCZ-equivalence [1].

A complete classification for APN functions, up to EA- and CCZ-equivalence, is known only for $n \leq 5$ [3], and for $n = 6$ it is known only the CCZ-classification of APN functions with algebraic degree at most 3 [4].

Recently, in [2] it has been introduced a procedure for investigating some relations between CCZ-equivalence and EA-equivalence together with the inverse transformation.

In this talk we will show how it is possible to use this procedure for investigating the EA-classes contained in the CCZ-class of a given function F. In particular, for the case $n = 6$ we are able to give all the EA-classes of the known APN functions.

We extend our study also to dimension 7 and 8, giving an upper bound on the number of the EA-classes for the known APN functions.

Up to dimension 9, for the case of APN non-Gold power functions and the inverse function we obtained that we have at most two EA-classes in any CCZ-class.

References

[1] M Brinkmann, *Extended Affine and CCZ Equivalence up to Dimension 4*, `https://eprint.iacr.org/2019/316.pdf`.

[2] Budaghyan, L., Calderini, M., Villa, I. *On relations between CCZ- and EA-equivalences.* Cryptogr. Commun. (2019).

[3] M. Brinkmann, G. Leander, *On the classification of APN functions up to dimension five.* Designs, Codes and Cryptography, 49(1-3), 273-288, 2008.

[4] P. Langevin, Z. Saygi, and E. Saygi. *Classification of APN cubics in dimension 6 over GF(2).* `http://langevin.univ-tln.fr/project/apn-6/apn-6.html`.

[5] Leander, G., Poschmann, A., *On the Classification of 4 bit S-boxes.* In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007)