Recent Results on the Search for APN Functions in Small Dimension

Christof Beierle[*]

[*]Ruhr University Bochum

Abstract

This talk summarizes the results of the following three papers:

- C. Beierle, M. Brinkmann, G. Leander. Linearly Self-Equivalent APN Permutations in Small Dimension. IEEE Trans. Inf. Theory 67(7), 2021.
- C. Beierle, G. Leander. New Instances of Quadratic APN Functions. (submitted)
- C. Beierle, C. Carlet, G. Leander, L. Perrin. A Further Study of Quadratic APN Permutations in Dimension Nine. (submitted)

In particular, we explain the approach for finding APN functions (APN permutations) using a recursive tree search. By restricting the search space to quadratic functions admitting non-trivial linear self-equivalences, several new instances of APN functions in small dimension $n <= 10$ have been found recently. We explain how the search was implemented and how one can search in the set of possible self-equivalences in a systematic way. Finally, we focus on the two new instances of quadratic APN permutations in dimension $n = 9$ and we highlight the recently-discovered trivariate representation of those permutations.