Search for APN permutations among known APN functions

Faruk Göloğlu* and Jiří Pavlů*

*Department of Algebra, Charles University in Prague

Almost perfect nonlinear (APN) permutations are of great interest to cryptographers, as they offer optimal resistance against differential cryptanalysis when used as S-Boxes. When functions over an odd number of bits ($\mathbb{F}_2^{2m+1}$) are considered, examples of APN permutations are plentiful — indeed, all monomial APN functions are permutations. On the other hand, only one example (up to equivalence) of an APN permutation over an even number of bits ($\mathbb{F}_2^{2m}$) — the "Kim" κ-function over $\mathbb{F}_2^6$[1] presented by Dillon 10 years ago. For higher dimensions the existence of APN permutations remains an open question.

Nevertheless, a steadily increasing number of APN function families over $\mathbb{F}_2^{2m}$ are known. As being APN is an invariant under CCZ-equivalence, whereas being a permutation is not, one of the possible ways to search for APN permutations is to check whether functions from these families are CCZ-equivalent to permutations. A method for cheking whether an APN function is CCZ-equivalent to a permutation is given in [1]. Indeed, it was this algorithm which was used by the authors of [1] when they found the only known such permutation. They also showed that none of the known families (at that time) leads to permutations up to $n = 10$. The algorithm is basically checking existence of two $2m$-dimensional subspaces U, V in the Walsh zeroes of the function, which is defined by

$$Z_F = \{(a, b) \ : \ \widehat{F}(a, b) = 0\} \cup \{(0, 0)\}$$

such that

$$U \cap V = \{(0, 0)\}.$$

This is a necessary and sufficient condition. In this note we give a necessary condition which allows us to completely check equivalence of all members of all known families up to and including dimension $n = 12$, and checking many representatives from all (componentwise-plateaued) families when $n = 14$ up to even $n = 18$. As a result, we can state that none of the known families (to authors) are equivalent to permutations.

Complexity of the original algorithm is that of finding two trivially intersecting $2m$-dimensional subspaces in a set with cardinality approximately 2^{4m-2}, whereas our algorithm requires finding two trivially intersecting m-dimensional subspaces in a set with cardinality 2^{2m-1}.

As a by-product we give a very fast affine-invariant which leads to an algorithm to check equivalence of two functions on large extensions. We also discuss some partial inequivalence results for infinite families as it was done in [2] for Gold (completely) and Kasami (partially) families.

References

[1] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. *An APN permutation in dimension six.* Postproceedings of the 9th International Conference on Finite Fields and Their Applications, 518:33–42, 2010.

[2] F. Göloğlu and P. Langevin. APN families which are not equivalent to permutations, submitted, 2019.