Changing Points in APN Functions

Nikolay Kaleyski
(joint work with Lilya Budaghyan, Claude Carlet and Tor Helleseth)
University of Bergen
nikolay.kaleyski@uib.no

A construction involving changing the value of a given function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ at precisely one point was investigated in [1] in the context of finding an upper bound on the algebraic degree of an APN function. The authors showed that e.g. changing one point of a power or plateaued function (which practically covers all known APN functions) in this manner does not yield an APN function. The problem of changing two points of a given APN function was studied in [3] and similar nonexistence results were obtained for this case as well.

We consider a generalized construction in which we change the value of a given vectorial Boolean function F over $\mathbb{F}_{2^n}$ on a given set of points $u_1, u_2, \cdots u_K$ from $\mathbb{F}_{2^n}$ for some positive integer K: for each point u_i we choose a difference v_i and define a new function G which satisfies $G(u_i) = F(u_i)+v_i$ for $i = 1, 2, \cdots, K$ and $G(x) = F(x)$ for $x \neq u_1, u_2, \cdots, u_K$.

We investigate the relationship between the properties of F and G, devoting particular attention to possibility of obtaining an APN function G when F itself is APN. In the general case, we characterize the APN-ness of G in terms of the derivatives of F and obtain an efficient way of filtering out useless candidate values for $v_1, v_2, \cdots, v_K$ when the points $u_1, u_2, \cdots, u_K$ themselves are fixed. We also define a characteristic m_F for any given function F and derive a lower bound on the Hamming distance between F and its closest APN neighbor in terms of m_F. The number m_F is CCZ-invariant and can be computed efficiently over fields of relatively small dimension. Furthermore, we demonstrate that in the case of quadratic functions, the computation time for m_F can be significantly reduced. We show how a formula for m_F can be derived for the function $F(x) = x^3$ over any field $\mathbb{F}_{2^n}$ and experimentally compute m_F (and the lower bound on the Hamming distance that follows from it) for all functions from [2].

If all of the differences are the same, i.e. if $v_1 = v_2 = \cdots = v_K$, we describe how all APN functions that can be obtained from a given F (not necessarily APN itself) can be efficiently computed by solving a system of linear equations.

References

[1] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, B. Sun, "On upper bounds for algebraic degrees of APN functions", "IEEE Transactions on Information Theory", 2017

[2] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," Adv. in Math. of Comm., vol. 3, no. 1, pp. 59-81, 2009.

[3] N. Kaleyski, "Changing APN Functions at Two Points", "To be submitted to Sequences and their Applications 2018"