Generalized Binomial APN Functions

Lilya Budaghyan, Nikolay Kaleyski
University of Bergen

Binomials are among the classes of vectorial Boolean functions that have been most intensely studied i.a. from the point of view of differential uniformity. Up to now, two infinite families and one sporadic example in dimension 10 of almost perfect nonlinear (APN) binomials have been discovered [1, 2]. The relative simplicity of their polynomial expression makes them an attractive object of study, and it is natural to advance the investigation of APN functions by examining functions which can be described in a similar manner.

We study functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of the form $F(x) = L_1(x^a) + L_2(x^b)$, where L_1 and L_2 are linear functions over $\mathbb{F}_{2^n}$ and x^α and x^β are power functions. We concentrate on the particular case of combining two Gold functions x^{2^i+1} and x^{2^j+1} using linear binomials L_1 and L_2 in this way. This allows us to construct several APN quadrinomials which constitute extensions of the APN function $x^3 + c \cdot x^{36}$ over $\mathbb{F}_{2^{10}}$ (the latter binomial is the earliest example of an APN function that is CCZ-inequivalent to a power function, and has not been classified into any infinite family as of yet). We characterize the APN-ness of these extended quadrinomials in terms of the solvability of a system of equations, from which we derive conditions that allow us to efficiently search for such APN quadrinomials in fields $\mathbb{F}_{2^n}$ of dimension n, with $n = 4k+2$. Our methods allow us to construct APN quadrinomials and obtain non-existence results in dimensions up to $n = 30$, with three of the quadrinomials constructed for $n = 10$ being CCZ-inequivalent to any known APN function.

References

[1] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[2] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52(2):744–747, 2006.