On Isotopic Construction of APN Functions

Irene Villa
joint work with
Lilya Budaghyan, Marco Calderini, Claude Carlet and Robert Coulter

University of Bergen
Irene.Villa@uib.no

Abstract

In our work we suggest a new approach for construction of APN functions over the fields of even characteristic which are of interest for many areas of mathematics and information theory and, in particular, for cryptography. This approach is based on the notion of isotopic equivalence introduced in [1] and defined only for quadratic planar functions. Recall that two quadratic planar functions are called isotopic equivalent if they define isotopic commutative presemifields [1, 3]. In [2] it is proven that CCZ-equivalence (the most general equivalence relation of functions which preserves APN property) is a particular case of this isotopic equivalence in case of quadratic planar functions. It is an open problem whether isotopic equivalence of quadratic planar functions can induce an equivalence relation for APN functions more general than CCZ-equivalence [2]. The present work is dedicated to that problem.

We first prove that quadratic planar functions F and F' are isotopic equivalent if and only if F' is affine equivalent to $F(x + L(x)) - F(L(x)) - F(x)$ for some linear permutation L. Then we study the analogue of isotopic equivalence applied to APN functions. That is, starting from known APN functions F defined over $\mathbb{F}_{2^n}$ we analyse the possible functions of the form

$$F'(x) = F(x + L(x)) + F(L(x)) + F(x)$$

for L a linear function. We analyse the properties of the linear functions L that generate APN maps F'. Moreover, we construct a new family of quadratic APN functions and give some computational results in low dimensions using for F a Gold power function. An interesting fact is that in $\mathbb{F}_{2^6}$ all quadratic APN functions can be generated, up to CCZ-equivalence, with the mentioned construction both with $F(x) = x^3$ and $F(x) = x^3 + \alpha^{-1} Tr(\alpha^3 x^9)$ (with $\alpha \in \mathbb{F}^\star_{2^6}$ primitive) and both with the restriction for L as a linear permutation and with the restriction as a 2-to-1 linear map.

References

[1] L. Budaghyan. Construction and Analysis of Cryptographic Functions. Springer Verlag, 2014.

[2] L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. *Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences*, v. 3(1), pp. 1-16, 2011.

[3] R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Advances in Math.* 217, pp. 282-304, 2008.