On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property

Enrico Piccione[1]

[1]University of Bergen, [2]University of Paris 8

(Joint work with Claude Carlet[1,2])

Abstract

We study those (N, M)-functions $\mathcal{F}$ which map at least one n-dimensional affine subspace $A \subseteq \mathbb{F}_2^N$ to (a subset of) an m-dimensional affine subspace $A' \subseteq \mathbb{F}_2^N$. This leads to (n, m)-functions $\mathcal{F}_A$. We study the cryptographic properties of $\mathcal{F}_A$ by means of the ones of $\mathcal{F}$. We then focus on the case $M = N = m + 1 = n + 1$, resulting in $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ (or $\psi(\mathcal{G}(x)) + x$) where ψ is a linear function with a kernel of dimension 1. We are interested in the case where $\mathcal{G}$ is *almost perfect nonlinear (APN)*. We say that $\mathcal{G}$ has the *strong D-property* if $\mathcal{G}_A$ has the *D-property* [1] for all affine hyperplanes A whose contrary allows the APNness of $\mathcal{F}_A$. We study the strong D-property for crooked functions and we prove that the Gold APN function has the strong D-property in large dimension. Then we give a partial result on the Dobbertin APN function. We then consider the case where $\mathcal{F}_A$ and $\mathcal{G}$ are permutations. We prove that some of the known families [2, 3] of 4-uniform permutations corresponding to this framework are not APN in even dimension.

References

[1] H. Taniguchi, *D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$*, Cryptography and Communications (2023).

[2] Y. Li and M. Wang, *Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$*, Designs, codes and cryptography (2014).

[3] C. Carlet, *On known and new differentially uniform functions*, ACISP, 2011.