Further investigations on the QAM method for finding new APN functions

Nadiia Ichanska
University of Bergen

Abstract

APN functions are vital for the development of cryptographic algorithms that can resist differential cryptanalysis, enhancing the security of digital communications and information. Their study is fundamental, therefore investigations of algorithms for producing and classifying them become practical. We collect algorithms that were already used [1], [2] for the QAM method and improve them for use in different dimensions (n, m) for the homogeneous quadratic functions $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j}$ in the subfield $\mathbb{F}_{2^m}$.

References

[1] Diana Davidova and Nikolay Kaleyski. Classification of all DO planar polynomials with prime field coefficients over $GF(3^n)$ for n up to 7. Cryptology ePrint Archive, Paper 2022/1059, 2022. https://eprint.iacr.org/2022/1059.

[2] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.