Classificaiton of quadratic APN functions with coefficients in $\mathbb{F}_2$

Lilya Budaghyan[a], Nikolay Kaleyski[a], Yongqiang Li[b], Yuyin Yu[c,*]

[a] *Department of Informatics, University of Bergen*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences*
[c] *School of Mathematics and Information Science, Guangzhou University*

The class of almost perfect nonlinear (APN) functions provides optimal resistance to differential cryptanalysis, and as such their study and classification is an important research direction with practical applications to the design of secure cryptographic ciphers. The investigation of APN functions has proven to be quite difficult in general, which is why particular classes of APN functions are typically considered. Quadratic APN functions, i.e. APN functions of algebraic degree two, are among some of the most thoroughly studied; despite their relative simplicity, even this particular class of APN functions is far from being understood, and attempts to characterize and classify quadratic APN functions are ongoing.

In this paper, we recall that there is a one-to-one correspondence between quadratic homogeneous APN functions over $\mathbb{F}_{2^n}$ and a particular class of matrices with elements from $\mathbb{F}_{2^n}$ called quadratic APN matrices (QAMs). We concentrate on the case of quadratic functions f over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$, and show that the QAM H corresponding to any such function must satisfy $H[u+1, v+1] = H[u, v]^2$ for any u, v. This condition enables us to design an efficient algorithm for searching for such functions, and the latter allows us to give a complete classification, up to CCZ-equivalence, of all quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions $4 \leq n \leq 8$, and a (so-far) partial classification for dimension $n = 9$.

Based on the observed data, we conjecture that any quadratic APN over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ is CCZ-equivalent to a quadratic APN over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ having no more than n non-zero terms.

*Corresponding author. Email: yuyuyin@163.com (Yuyin Yu).

Email addresses: Lilya.Budaghyan@uib.no (Lilya Budaghyan), Nikolay Kaleyski (Nikolay Kaleyski), yongq.lee@gmail.com (Yongqiang Li)

May 8, 2019