Opinion on "On a matrix approach for constructing quadratic almost perfect nonlinear functions"

This thesis is about a matrix representation (QAM) of quadratic vectorial Boolean functions, introduced in Yu et al. (2014). Vectorial Boolean functions are frequently used in cryptography. Almost perfect nonlinear (APN) functions are optimal Boolean functions with respect to an important cryptographic attack called differential cryptanalysis. Thus, finding new APN functions is a cryptographically important mathematical problem. There are several known APN functions for infinitely many parameters. Finding APN functions (or families of functions) which are "inequivalent" to the known ones is a difficult problem. The approach in Yu et al. (2016) characterizes almost perfect nonlinearity of a quadratic vectorial Boolean function by a rank property of its corresponding matrix representation. This matrix is then modified by an algorithm to give new APN functions on relatively small degree extensions.

In this thesis it is shown that the QAM matrix representation of quadratic APN functions is in one-to-one correspondence to the well-known algebraic normal form (ANF) representation of Boolean functions, which to the best of our knowledge has not been noted before.

The thesis in review first explains the preliminary notions concisely in Chapter 1. Then the approach of Yu et al. is explained in Chapter 2 with expanded proofs and in a very detailed manner. Then in Chapter 3, it is shown that the ANF representation is in one-to-one correspondence with the QAM approach. Chapter 4 is devoted to two important families of APN functions and their QAM and ANF representations. The author does a very good job to show how these two functions are related when represented as QAM and ANF. This explanation could be useful to give theoretical methods for finding new APN families, i.e., for infinitely many extension degrees.

I believe the thesis in review is a very good one and deserves the best grade (1.0).

Faruk Göloğlu
Prague, September 1st, 2020