Opinion on “APN functions with non-classical Walsh spectra”

Almost Perfect Nonlinear (APN) functions are one of the most interesting mathematical objects in the study of symmetric cryptographic primitives. Most of the researchers would agree that one of the interesting open problems in the study of APN functions is finding a quadratic APN family with so-called non-classical Walsh spectrum. Many of the classical examples of APN functions are quadratic and has a specific spectrum. These include the famous Gold functions X^{2^k+1}.The only thing we can say about the Walsh spectrum of a quadratic function is that they can only have powers of 2 and 0. One sporadic example found in [9] has a different Walsh spectrum than other quadratic APN functions. This example have resisted the attempts to generalizations.

The author of this thesis first introduces the observation that the sporadic non-classical example in $GF(2^6)$ can be written in a nice bivariate form consisting of two functions $f, g : GF(2^3) \times GF(2^3) \to GF(2^3)$, where f is very simple: $f : (x, y) \mapsto x^2y + xy^2 + xy$. This function when defined on larger fields may also lead to non-classical APN functions, when coupled with a suitable g. But even with this observation finding an example is quite hard. That is to say the search space for such g is quite large. The mathematical analysis on f prunes the search space for g and then the exhaustive search becomes feasible on $GF(2^8)$. Then the author implements computer programs to effect the search on $GF(2^8)$ and deduces that such a generalization with that f is not possible. Moreover, he also employs the function $f : (x, y) \mapsto x^2y + y^2x$, which is also a possibility on $GF(2^4) \times GF(2^4)$ (but not on $GF(2^3)$), and repeats the process to deduce such generalization is not possible. He also proves that the generalization is not possible for very large infinite values of n on $GF(2^n)$ where $n > 14$ (Theorem 21).

This thesis contains very nice ideas and their careful implementations. There are many questions/ideas came out of the research which will provide basis for further research. It contains a nice theoretical result for infinite values of n which has a rather nice combinatorial/algebraic proof. I think the thesis deserves the best grade.

Faruk Göloğlu
Prague, June 10th, 2019