Opinion on "Search for APN permutations among known APN functions"

A very interesting question on the subject of mathematical cryptography is the existence of optimal permutations suitable for the use in symmetric ciphers. These permutations are called "almost perfect nonlinear (APN)". The existence of such permutations is an important problem. They exist on every odd extension of the two-element field. Dillon et al. [2] presented in 2009 that there exists APN permutations of $GF(2^6)$, i.e., the extension degree 6. This is the only even extension degree in which the existence is known (in the extensions $GF(2^2)$ and $GF(2^4)$ they do not exist). There are many known families of APN functions which are not necessarily permutations. In the same work, authors show by means of an algorithm (Algorithm 2 of the present work) that within those known families there are no APN functions equivalent to a permutation up to and including the extension degree 10. To that end, they use a necessary and sufficient condition (Lemma 14 of the present thesis) as the basis for their algorithm.

In this thesis, the author gives another proof of Lemma 14. This approach to the proof helps to get a condition (Theorem 15), for so-called componentwise plateaued functions which comprise all known APN functions with the exception of a few exponential functions. This approach was used in a very compact form in [2, 24], the author expands them in a nice way as a part of the project. Using these observations, the author presents one of the main results of the thesis: An algorithm (Algorithm 3) which is theoretically a lot faster that Algorithm 2, as it improves the latter in the region of square-root complexity. Indeed, implemented even in the rather slow mathematical programming language SAGE, the author is able to clear the case $GF(2^{12})$ which was open for some time. He also gives a theoretical result (Theorem 19) which shows that a specific family of APN multinomials cannot be equivalent to permutations in infinitely many doubly-even extensions. This is the first non-monomial, negative result of its kind for infinitely many extensions (in [24], the Gold and Kasami exponential functions were shown to be inequivalent to permuations for infinitely many fields).

I can safely say that the results and the approach of the thesis under review are very good. The author is currently importing the programs to the much faster C Programming Language, where one can hopefully resolve degrees up to 18. Unfortunately, the thesis gives the impression that it was written hastily and as it is, it contains several typos and indeed some errors. But the author gives "Errata and clarifications" which rectify the problems.

Nevertheless, my opinion on this thesis is very high. I still believe that the work deserves acceptance with highest distinction. Mark (1.0).

Faruk Göloğlu
Prague, August 29th, 2018