Review of "Constructions of APN permutations"

Almost Perfect Nonlinear functions are one of the most important theoretical research areas in symmetric cryptography. Many block and stream ciphers employ highly nonlinear functions -functions which are 'far away' from linear functions- to introduce 'confusion' to the system. The specific problem which is studied in this thesis is the question of existence of APN permutations on even degree extension of $GF(2)$, the finite field with two elements.

APN permutations does not exist on $GF(2^2)$ and $GF(2^4)$. It was widely believed that they did not exist on any even degree extension $GF(2^{2m})$ until Dillon provided a counter-example on $GF(2^6)$. Since then researchers have been trying to generalize that case (i.e., the Kim function) to some even extension other than 6.

This Master's Thesis is a meticulous study on whether generalizing the Kim function to some other even extension is possible. Kim function is APN and CCZ-equivalent to a permutation and it is a function of a very specific form. It satisfies a "subfield property". Author analyses two things:

- When do functions in this specific form are APN?
- When do functions in this specific form are equivalent to permutations?

Author deals with these two uneasy tasks and provides characterizations on when these functions are APN (Chapter 3, Theorem 3.2) and when they are equivalent to permutations (Chapter 4, Theorem 4,5).

The author then combines in the conclusion that in the next case (when m is odd, i.e., on $GF(2^{10})$) such generalization is impossible by using computer programs and her Theorems 3.2 and 4.5.

I believe both the idea and the work has been done to write this thesis are very good. She also supports her research with computer simulations. The work also leads to some interesting new research questions.

In my opinion, the thesis certainly deserves awarding of a MSc title with the best grade (1.0).