Report on “Computational methods for finding cryptographic functions”

The thesis is on computational methods for finding examples of interesting nonlinear functions that satisy certain other properties as well. Almost Perfect Nonlinear (APN) functions are important in cryptography as they are optimal against differential attacks. There are many theoretical construction techiques for APN functions however for those satisfying these extra properties (such as being bijective, having certain Fourier transform values, having certain automorphism groups etc.) there are no known theoretical constructions. The thesis provides an understanding of the computational methods (that also employs theoretical background) tailored for such specialized aims.

The thesis starts with an introduction that explains the necessary background nicely. One of the aims of the thesis is to provide the background for the mathematical parts of these highly “algorithmic” papers [2,3,5]. This includes the so-called *rational canonical form* of $\mathbb{F}_2$-matrices that uses the theory of $\mathbb{F}[x]$-modules. The author introduces these in Chapter 1. The treatment follows the standard textbook [Dummit and Foote, 4]. The introduction also contains a background for Boolean functions which was done nicely as well.

Chapter 2 is on the recursive algorithm that aims to find *any* quadratic APN functions and putting them into equivalence classes. Such algorithms create many APN instances which helps, among other things, theoretical understanding. The author first introduces the background. Then the algorithm is explained in very good detail. One of the strongest points of the thesis is the careful implementation of the algorithms and detailed explanations of them. Section 2.3.1 also includes some information on the corrections of some inaccuracies of the original algorithms and some improvements on them.

Chapter 3 is on APN functions that contain non-trivial automorphishms. First, details on the module approach is given and then the algorithms from [2,3] are explained. Although it does not contain all the details and proofs, Section 3.2 gives a good overview of the rational canonical form of matrices using the theory of modules.

The remaining chapters of the thesis are on restricting APN functions on subspaces and conversely, constructing APN functions on larger vector spaces from an APN function on a small vector space. These are called *trims* and *extensions* respectively. Similar to the previous chapters, first the theory is explained and then the algorithm is presented. Certain mathematical parts that are skipped in the original papers are explained in detail.

Topic of the thesis: The topic is very suitable for a thesis. It includes both interesting theory and applications.

Mathematical content: The mathematical content including modules, Boolean functions is adequate.

Citations/References: The citations are done carefully and extensively.

Student’s contribution: Student explained both the theory and algorithms quite well and also implemented the algorithms meticulously and provided independent implementations. However, improvements on the algorithms remain at a superficial level, e.g., faster algorithms that can work on slighly larger dimensions, corrections of simple errors.

Summary: The strength of the thesis is the careful and extensive implementation of the complicated algorithms of three recent papers [2,3,5]. Detailed explanations of mathematical aspects that are omitted from original papers should also be taken into account. However, these explanations stay at a level that cannot be viewed as "contributions". The student mostly follows the original papers and textbook [2,3,4,5] and sometimes gives detailed proofs of some theorems. Although these proofs are sometimes not the optimal ones, it represents the way the student understands them. In my opinion this should not be viewed as a negative aspect.

In my opinion, after all the hard work of implementing all of these algorithms and understanding the theory in detail, the author should have spent a little bit more time to contribute more deeply by finding a good construction method either algorithmically or theoretically. This would have made this an excellent thesis. The thesis could also have benefited from a few more rounds of revision. Having said these, I do believe that the thesis should be deemed successful.

Comments on formal issues:

- Lemma 29 is true for any quadratic function.
- (p. 64) We can see from the proof, that also G(x) + G(x + a) is also a linear mapping. This implies that the image of mapping the G(x) + G(x + a) is a linear subspace. (This is inaccurate, the image is an affine subspace.)
- (p. 66) This implies that it consists of some quadratic coordinate functions. (They can also be degree 1 or 0.)
- (p. 66–67) wlog assume that it is of degree 3. (One cannot do that wlog. I understand that the proof is almost the same for higher degree terms, but this is technically wrong.)
- Lemma 34: One should give an argument why A is nonsingular.
- (p. 76) "a quadratic element" is not good. Should be "term" or "monomial".
- (p. 80) Delete $(xy)^T$ (equation on line 6)

The use of English is good overall the thesis but could be improved. For instance:

- (p. 14) One of the most important properties for us is that the vectorial Boolean func- tion can be APN.
- (p. 14) Following definition (should be "preceding")
- (p. 15) Look in the table
- (p. 18) This is an important contribution to the future chapters of this thesis. (reform the sentence, e.g., This will be used extensively in forthcoming chapters.)
- (p. 20) on the [2, Section 3] (delete "the")
- (p. 37) representative (set of representatives)

- (p. 50) vecotrial
- (p. 56) being an affine (let B be an affine)
- (p. 63) This [chapter] focuses
- (p. 63) In the this chapter
- (p. 67) Such a defined matrix
- (p. 67) be [a] quadratic, exists [a] quadratic
- (p. 74) then it means from the definition it follows that (sentence should be reformed)
- (p. 74) separable (should be "separate")
- (p. 75) this three solutions
- (p. 76) coordination ("coordinate")
- (p. 81) assume that $rank(L)$ (should be $= n$)

Conclusion: In my opinion, despite the few shortcomings explained above the thesis deserves to be recognized as "successful". I will inform the committee of my suggested grade.