Oponent's assessment of the diploma thesis

Title: Computational methods for finding cryptographic functions
Author: Jaroslav Kroutil

Content of the thesis

The author begins with an overview of basic concepts, defines Boolean, vectorial Boolean functions, and their algebraic normal forms. Further, he defines equivalence relations on the class of vector Boolean functions, namely linear equivalence, affine equivalence, extended-linear equivalence and CCZ-equivalence, and prove that they are ordered by inclusion.

In Chapter 2 the author describes how to find coeficients of algebraic normal forms of Boolean functions. He investigates properties of Boolean functions that are invariant with respect to the EA-equivalence. Finally he analyzes and implements an algorithm that searches for Boolean APN functions of a given dimension and sorts them into EA-equivalence classes.

In the third chapter, the author studies groups of automorphisms and affine automorphisms of vector Boolean functions $\mathbb{F}^n \to \mathbb{F}^n$. He will show that Boolean functions of the above form can be represented by pairs of matrices in the rational canonical form, subject to appropriate equivalence. At the end of the chapter, he describes an algorithm that searches for pairs of matrices in the rational canonical form and classifies the corresponding equivalences classes of Boolean functions.

The last two chapters are devoted to methods of finding almost perfect nonlinear Boolean functions, namely trimming and extending to functions with maximum linearity. Both methods are algorithmically implemented.

Evaluation of the thesis

The length of the thesis exceeds what is expected of diploma theses. It can be divided into two parts; the theory of Boolean functions and the implementation of the theoretical part. The first part is a comprehensive compilation from a number of sources. The author refines proofs that are omited or incomplete in the literature. His argumentation often sufferes minor mistakes and inaccuracies. Fortunately, they are not fundamental. Purely mathematical text is slightly stilistically clumsy. On the other hand, the algorithmical implementation and its description are very good.

I like the thesis. The student did a large amount of work. I definitely recommend it to be accepted as a diploma thesis.

The proposed classification will be communicated to the examination committee.

Pavel Růžička
Katedra Algebry MFF UK
3.6.2024