Daniel Joščák: *Algebraic and combinatorial methods in study of hash functions*

opponent's report

The thesis contains results of three published papers (chapters 2, 3 and 4) and an unpublished research (chapter 1). We will first successively discuss the content of individual chapters.

The subject of the first chapter are equations arising from analysis of particular cryptographic constructions. Among standard constructions of symmetric cryptography belongs alternate application of heterogeneous algebraic operations on message data. This makes the resulting data transformation hardly describable within classical algebraic structures. This chapter presents interesting results for the class of AX-equations of depth 1, that is equations in modular addition and xor, where modular additions are not nested.
Basic classification of these equations is achieved by splitting the class to trivial and non-trivial cases, the latter with quadratic and linear subcases. Main part of the research concerns the last mentioned case, so called linear AX-equations, where the corresponding quadratic form is diagonal.
To investigate solvability of equations an inductive construction of solutions is introduced together with a set of solvability conditions. These conditions are applied to partial solutions at each iterative step. Main result of this part is Theorem 1.14 which gives necessary and sufficient condition for solvability of certain class of linear AX-equations. In this class of equations, probability of being a solution is also enumerated. This result covers several important cases which come from cryptanalysis of different hash function proposals.
The first chapter is concluded with an outline of possible recursive application of solvability conditions. The idea is demonstrated on one of the motivating examples but general theory is not further elaborated.

In the second chapter the proposed 3C and 3C+ enhancements of iterated hash functions are analyzed. A simple method of finding multi-block collisions for these constructions is described. As prerequisite, multi-block collision construction for the underlying iterated hash function should be known and it should be of similar type as the construction of Wang et al for the MD5 function. Examples are provided for this particular case.

Major part of the next chapter is a survey of published results on collision searching algoritms. The section analyzing the proposal of feedback ring-iterative construction seems to be new. Again, a simple multi-block collisions based on Wang's method are found for single feedback ring-iterative construction. Idea of finding collisions for multiple feedback ring-iterative construction is just indicated without a rigorous proof. Unfortunately, the precise definition of studied constructions is missing here.

The final chapter describes the construction of new collisions in MD5 hash function. Independent implementations of Stevens algorithm and Klima's algorithm are used to construct full differential paths in MD5 and to find corresponding colliding messages respectively. Interesting modifications are made in extending partial

differential paths, where the choices of binary signed digit representations of differences diverge from Stevens approach. Example of differential path and found collision ends the chapter.

In general, the style of the thesis is good and author tries to explain the notions and ideas. Nevertheless, more rigorous approach would be appropriate at some steps. This concerns proper introduction of used notions (e.g. missing definition of feedback ring-iterative construction) and also proper formulation of results (e.g. strange formulation of Proposition 1.9).
On the other hand, the thesis presents interesting results. Namely the results of the first chapter are promising more systematic treatment of AX-equations, however, in both cases of quadratic and linear equations, the research should proceed further.

The thesis proofs authors ability of independent scientific work. I recommend to accept the work as doctoral dissertation.

Doporučuji práci přijmout jako doktorskou disertaci.

V Praze dne 27. srpna 2015 Robert El Bashir