Title: Applications of Gröbner bases in cryptography

Author: Aleš Fuchs

Department: Department of Algebra

Supervisor: Mgr. Jan Šťovíček Ph.D., Department of Algebra

Abstract: In the present paper we study admissible orders and techniques of multivariate polynomial division in the setting of polynomial rings over finite fields. The Gröbner bases of some ideal play a key role here, as they allow to solve the ideal membership problem thanks to their properties. We also explore features of so called reduced Gröbner bases, which are unique for a particular ideal and in some way also minimal. Further we will discuss the main facts about Gröbner bases also in the setting of free algebras over finite fields, where the variables are non-commuting. Contrary to the first case, Gröbner bases can be infinite here, even for some finitely generated two-sided ideals. In the last chapter we introduce an asymmetric cryptosystem Polly Cracker, based on the ideal membership problem in both commutative and noncommutative theory. We analyze some known cryptanalytic methods applied to these systems and in several cases also precautions dealing with them. Finally we summarize these precautions and introduce a blueprint of Polly Cracker reliable construction.

Keywords: noncommutative Gröbner bases, Polly Cracker, security, cryptanalysis