Title: Goppa codes and their applications

Author: Bc. Jaroslav Kotil

Department: Department of algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc.

Abstract: In this diploma paper we introduce Goppa codes, describe their parametres and inclusion in Alternant codes, which are residual Generalized Reed–Solomon codes, and Algebraic–geometry codes. Aftewards we demonstrate decoding of Goppa codes and introduce Wild Goppa codes. We also describe post–quantum cryptography member: McEliece cryptosystem for which no effective attacks with quantum computers are known. We outline a usage of this cryptosystem with Goppa codes and describe the security of the cryptosystem together with possible attacks of which the most effective ones are based on information–set decoding.

Keywords: Goppa codes, Generalized Reed–Solomon codes, Algebraic–geometry codes, Post–quantum cryptography, McEliece cryptosystem