Title: Analysis of the stream cipher QUAD

Author: Marcel Čurilla

Department: Katedra algebry

Supervisor: doc. Mgr. Štěpán Holub, Ph.D.

Abstract: Stream cipher QUAD was introduced in 2006 on Eurocrypt by Côme Berbain, Henri Gilbert a Jacques Patarin cite quad. The authors showed a reduction of this cipher for the problem of solving m quadratic equations of n variables over finite fields known as the MQ problem. For simplicity, they considered only the case of the field GF(2).

In this thesis I introduce this stream cipher. I show the proof (reduction) of safety ciphers QUAD for MQ problem over any finite field GF(q). I describe the basic methods for the solution of system of quadratic equations over finite fields, linearization and relinearization. I focus on XL algorithm - which is currently the fastest algorithm for solving quadratic systems. This algorithm was designed precisely to deal with overdefined quadratic systems. While analyzing the cipher QUAD I show for what instance is a cipher QUAD breakable and vice versa for what instance is the security guaranteed.

Keywords: stream cipher, QUAD, MQ problem, algorithm XL,