

Motivation

Public key cryptosystems are based on difficult mathematical problems and usually slow compared to symmetric crypto systems. However, especially in small devices there is a demand in ultra-fast public key crypto systems like MQQ-Crypt.

MQQ-Crypt is based on a specific class of quasigroups. In this project, the mathematical background of multivariate quadratic quasigroups (MQQ) should be elaborated. Furthermore, possible attacks and implementation techniques are considered and partially implemented.

Goals and Tasks

- ▶ Acquire the necessary background on multivariate quadratic quasigroups
- ▶ Understand MQQ-Crypt and its security
- ▶ Implement MQQ-Crypt or parts of an attack on it

Literature

- ▶ D. Gligoroski, S. Markovski, and S. J. Knapskog. Public Key Block Cipher Based on Multivariate Quadratic Quasigroups. *Cryptology ePrint Archive, Report 2008/320*, 2008. <http://eprint.iacr.org/>.
- ▶ M. S. E. Mohamed, J. Ding, and J. Buchmann. Algebraic Cryptanalysis of MQQ Public Key Cryptosystem by MutantXL. *Cryptology ePrint Archive, Report 2008/451*, 2008. <http://eprint.iacr.org/>.

Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

Project Schedule

- ▶ Start Immediately
- ▶ Month 1 Reading literature
- ▶ Month 2 Implementing
- ▶ Month 3 Final deliverables

Studies

INF SW TEL TM

Prerequisites

- ▶ C programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at