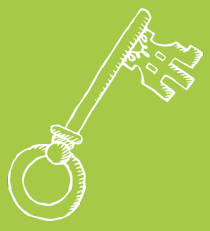

Exploring the Algebraic Security in Lightweight Schemes

Advisor: **Markus Schofnegger**

Motivation

In some of the recent cryptographic research areas (e.g., modern zero-knowledge proof systems), schemes are often built in order to have a clear algebraic structure and to be lightweight with respect to the total number of multiplications or the multiplication depth.

To meet this target, the number of rounds of a construction is sometimes chosen to be very close to its minimum for security. In these cases, slightly wrong theoretical estimations about the strength of the algorithm may lead to attacks. For example, the block cipher in consideration may fail to reach the advertised degree or a certain polynomial density.

The goal of this Bachelor's thesis is to practically investigate the validity of these theoretical estimations using reduced-round versions of existing and already used constructions. This can be done by using tools like Sage.

Goals and Tasks

- Get familiar with the target cipher
- Get familiar with algebraic representation of ciphers
- Model the cipher in Sage
- Evaluate the growth and structure of the polynomials

Literature

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in cryptography and math basics
- Programming (Python/Sage)

Advisor / Contact

markus.schofnegger@iaik.tugraz.at