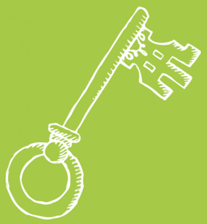
ISEC | Institute of Information Security

TU Graz



Exploring Gröbner Basis Attack Software: A Framework for Efficient Tool Integration with SageMath

Advisor: **Katharina Koschatko**

Motivation

In the realm of advanced cryptographic protocols like Zero-knowledge (ZK) proofs, widely used in blockchain technologies, there is a demand for cryptographic hash functions that are efficient over large finite fields. Responding to this demand, the cryptographic community has introduced so-called *arithmetization-oriented* (AO) hash functions.

Due to the algebraic nature of AO hash functions, they are susceptible to algebraic attacks like the Gröbner basis attack. For this type of attack, the underlying primitive of the hash function is modeled as a system of polynomial equations over a finite field. The goal is then to transform this system into a simpler form from which solutions can be extracted more easily.

There exist several software packages (e.g. MAGMA [2]) and libraries (e.g. FGb [1]) for computing Gröbner bases. Your goal is to research different software tools used for performing Gröbner basis attacks and to develop a framework to facilitate the application of these tools on equation systems generated in SageMath.

Goals and Tasks

- Get a rough understanding of the individual steps of the Gröbner basis attack.
- Research and familiarize yourself with software tools used for performing Gröbner basis attacks.
- Develop a framework to facilitate the application of these tools on equation systems generated in SageMath.

Literature

- J.-C. Faugère
  FGb: A Library for Computing Gröbner Bases
  Mathematical Software - ICMS 2010
  https://www-polsys.lip6.fr/~jcf/FGb/index.html
- The Magma algebra system.
  https://magma.maths.usyd.edu.au/magma/handbook/groebner_bases

Courses & Deliverables

☑ **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 the topic area
- Programming (C/C++, SageMath)

Advisor Contact

katharina.koschatko@tugraz.at