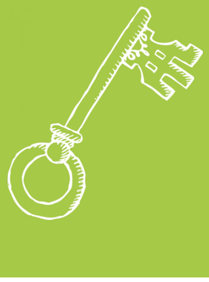


Exploring Gröbner Basis Attack Software: Application to AO hash functions

Advisor: **Katharina Koschatko**

Motivation

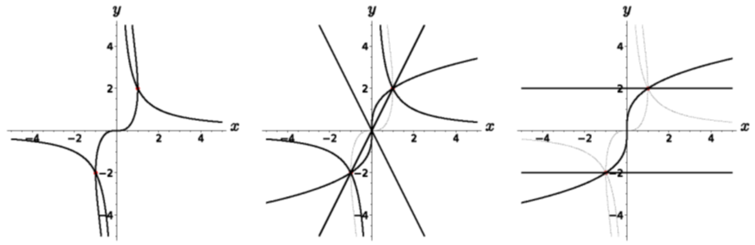
In the realm of advanced cryptographic protocols like Zero-knowledge (ZK) proofs, widely used in blockchain technologies, there is a demand for cryptographic hash functions that are efficient over large finite fields. Responding to this demand, the cryptographic community has introduced so-called *arithmetization-oriented* (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) and libraries (e.g. FGb [2]) for computing Gröbner bases. Your goal is to research different software tools used for performing Gröbner basis attacks and to run and compare Gröbner basis attacks on equation systems stemming from different AO primitives.

Goals and Tasks

- Understand the individual steps of the Gröbner basis attack.
- Research and familiarize yourself with software tools used for performing Gröbner basis attacks.
- Run and compare Gröbner basis attacks on equation systems stemming from different AO primitives.



Literature

- R. Walch
  What's the deal with hash functions in Zero Knowledge?
  https://blog.taceo.io/whats-the-deal-with-hashes-in-zk/
- J.-C. Faugère
  FGb: A Library for Computing Gröbner Bases
  Mathematical Software - ICMS 2010
  https://www-polsys.lip6.fr/~jcf/FGb/index.html

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
+ DiplomandInnenseminar (CS)
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Programming (C/C++, SageMath)

Advisor Contact

katharina.koschatko@iaik.tugraz.at