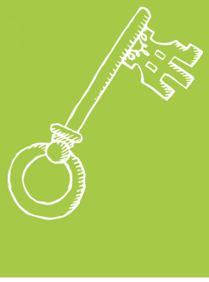
ISEC | Institute of Information Security



Computing the (minimal) multihomogeneous Bézout bound

Advisor: **Katharina Koschatko**

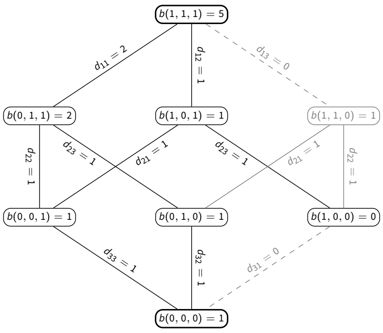
Motivation

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. One important metric to estimate the security against this type of attack is the number of solutions to the (multivariate) polynomial equation system. A well-known upper bound is the so-called Bézout bound. While it is simple to compute, it ofter vastly overestimates the number of solutions. By considering so-called multihomogeneous systems, Bézout's bound might further decrease.

Goals and Tasks

- Understand the number of solutions computed from the Bézout bound.
- Efficiently implement the *Row expansion algorithm* [2] in C/C++.
- Improve the computation of the *minimal* multihomogeneous Bézout bound, addressing the inefficiencies of exhaustive enumeration.



Literature

- K. Koschatko, R. Lüftenegger, and C. Rechberger
  Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi
  IACR Cryptol. ePrint Arch. 2024
  https://eprint.iacr.org/2024/250
- C. W. Wampler
  Bezout number calculations for multi-homogeneous polynomial systems
  Applied Mathematics and Computation 1992

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++)

Advisor Contact

katharina.koschatko@tugraz.at