Motivation

Block ciphers play a crucial role in the cryptographic world and have a large variety of use cases. Very recently, zero-knowledge proof systems such as SNARKs or STARKs make use of block ciphers with certain properties. Specifically, constructions with a “nice” algebraic structure are considered as good choices in these scenarios. Because of this separation, different algorithms tailored towards these new use cases have recently been proposed. Examples include FRIDAY [1] and STARKAD [2].

However, precisely due to their algebraic structure, some of them have been attacked using so-called Gröbner bases [3] – an attack vector whose main approach consists in simplifying a given equation system. Unfortunately, the strength of this technique is hard to estimate without doing experiments.

Your task is to get familiar with concrete constructions (e.g., STARKAD) and with the basics necessary to conduct experiments with Gröbner bases, and to then apply these methods to obtain new results.

Goals and Tasks

- Get familiar with a concrete construction
- Experiment with equation systems and Gröbner bases in a certain framework (e.g., Sage)
- Perform some experiments and evaluate them
- Try to find new results for algebraic constructions

\[
g_1 = x_1^d + h_1(x_1),
g_2 = x_2 + h_2(x_1),
\vdots
\]
\[
g_n = x_n + h_n(x_1).
\]

Literature

- T. Ashur and S. Dhooghe
  MARVELlous: a STARK-Friendly Family of Cryptographic Primitives
  IACR Cryptology ePrint Archive 2018
- L. Grassi et al.
  Starkad and Poseidon: New Hash Functions for Zero Knowledge Proof Systems
  IACR Cryptology ePrint Archive 2019
- M. R. Albrecht et al.
  Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC
  ASIACRYPT (1)

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you’re studying

- CS
- ICE
- SEM

Prerequisites

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

Advisor / Contact

markus.schofnegger@iaik.tugraz.at