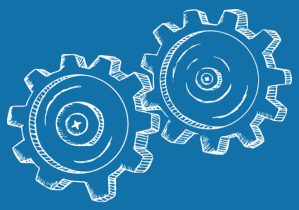

AVX Implementation for Polynomial Commitment Schemes

Advisor: **Florian Krieger**

Motivation

Zero-Knowledge Proofs are recent developments in cryptography. They allow an untrusted party (the prover) to demonstrate the validity of a statement to another party (the verifier) without revealing additional information. Within ZKPs, Polynomial Commitment Schemes (PCS) are important building blocks and cause a major performance bottleneck.

Goals and Tasks

Brakedown is a particularly interesting PCS and the target of this project. Brakedown involves two suboperations, which are linear encoding and Merkle Tree construction. Your task would be to combine an existing implementation of AVX-based linear encoding with your developed Merkle Tree implementation, also on AVX. Specific steps are:

- Learn how the Brakedown PCS works
- Implement a performant AVX software for Merkle Tree construction
- Combine existing linear encoding and Merkle Tree software
- Benchmark and compare your implementation to related work

Literature

- A. Golovnev et al.
  Brakedown: Linear-time and field-agnostic SNARKs for R1CS
  Cryptology ePrint Archive 2021
  https://eprint.iacr.org/2021/1043

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 optimizing software implementations and cryptography
- Basic C/C++ courses, Optional: Cryptography on Software Platforms

Advisor Contact

florian.krieger@tugraz.at