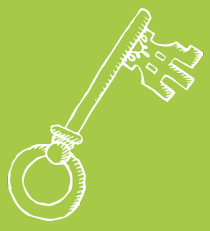

Implementing the Sumcheck Protocol in Hardware or Software

Advisor: **Florian Krieger**

Motivation

Zero-Knowledge Proofs (ZKPs) allow a prover to convince a verifier that a statement is true without revealing anything beyond its validity. This enables applications like privacy-preserving age verification, anonymous credentials, or the verifiable outsourcing of computations. Many modern ZKP systems build on the Sumcheck protocol. Since the Sumcheck protocol dominates the prover's runtime in ZKP systems, implementing it efficiently is key to making ZKPs practical.

The goal of this thesis is to investigate the Sumcheck protocol and to speed up its computation. Depending on your interests, you can implement and optimize the protocol in software or on GPUs. If you are interested in FPGA acceleration, you can design a dedicated hardware accelerator for the Sumcheck protocol using high-end datacenter FPGAs.

Goals and Tasks

- Learn the details of the Sumcheck protocol
- Investigate existing implementations
- Optimize and implement Sumcheck using AVX, GPU, or FPGA
- Evaluate and compare your implementation

Literature

- A. Fan et al.
  GPU Acceleration of the Sum-Check Protocol Over Towers of Binary Fields for Verifiable Computing
  DATE 2026
  doi:10.23919/DATE69613.2026.11539722
- K. Wang et al.
  PipeSC: A Resource-efficient and Pipelined Hardware Accelerator for Sumcheck Protocol
  ePrint 2026
  https://eprint.iacr.org/2026/691

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

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

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in ZKPs
- AVX, GPU, or FPGA experience

Advisor Contact

florian.krieger@tugraz.at