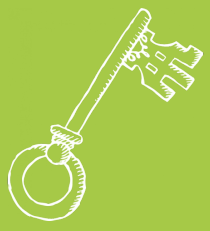


MPC-friendly Post-Quantum Signatures

Advisor: **Verena Schröppel**

Motivation

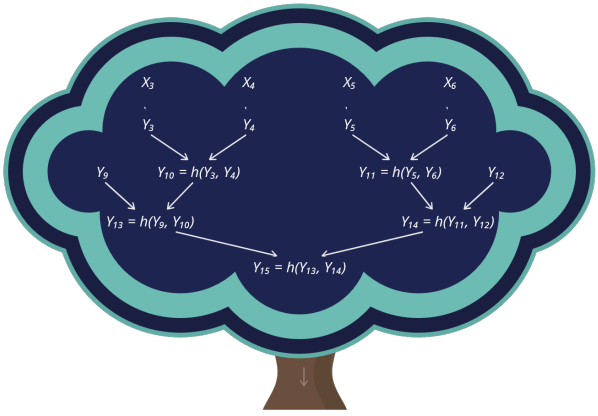
Hash-based cryptographic schemes are an important class of post-quantum constructions, offering security based on the well-established foundations of cryptographic hash functions. At the same time, secure **multi-party computation** (MPC) enables cryptographic operations to be performed collaboratively while keeping the underlying secret keys distributed and private.

Combining these two approaches is particularly relevant for applications where **post-quantum security** and distributed trust are required simultaneously. Cryptographic constructions efficient in conventional settings may not remain efficient in MPC, where algorithmic structure, hashing, primitives, and communication overhead can significantly impact performance.

In this thesis you will study hash-based signatures and modern MPC protocols, focusing on the performance of such threshold signing designs.

Goals and Tasks

- Study PQ secure, hash-based signatures such as SPHINCS$^+$ and the basics of MPC.
- Identify the MPC bottlenecks of hash-based signing and compare candidate hash functions.
- Prototype threshold signing and evaluate design tweaks that reduce communication and rounds.



Literature

- D. J. Bernstein et al.
  The SPHINCS+ Signature Framework
  ACM CCS 2019
- J. Drake et al.
  Hash-Based Multi-Signatures for Post-Quantum Ethereum
  Cryptology ePrint Archive 2025

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 post-quantum signatures and MPC
- Motivation to implement and benchmark modern protocols

Advisor Contact

verena.schroeppel@tugraz.at