

They sign, we prove — Hash-Based Multi-Signatures in Post Quantum Settings.

Advisor: **Fabian Schmid**

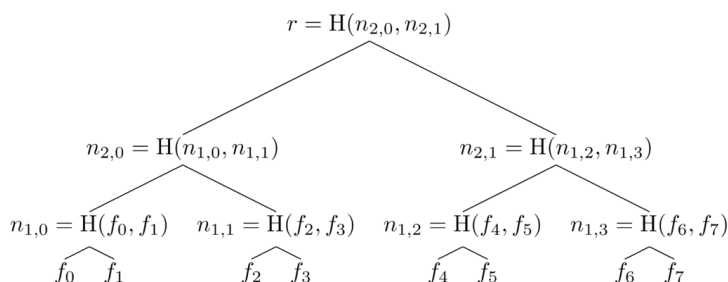
Motivation

A multi-signature scheme allows many parties to sign messages individually and for their signatures to be compactly aggregatable. As a prominent example, these multi-signatures are used in the block validation procedure of Ethereum. Similar to many cryptographic protocols, the existing schemes are threatened by adversaries with sufficiently powerful quantum computers. Recently, there was a proposal to instantiate such a multi-signature with the help of the hash-based signature scheme XMSS and a modern zero-knowledge proof system.

Within this topic, there is a little bit of everything. With hashes, there are fundamental cryptographic primitives; with XMSS, we have a post-quantum signature scheme, and with zero-knowledge proofs, we have cutting-edge privacy technologies.

Goals and Tasks

- 📖 Study the XMSS signature scheme and selected arithmetization-oriented hash functions.
- 📖 Understand how classical signatures can be made aggregatable using zero-knowledge proofs.
- 🔧 Implement parts of the XMSS scheme in a proof system framework.



The eXtended Merkle Signature Scheme (XMSS).

Literature

- > [J. Drake et al.](#)
Hash-based multi-signatures for post-quantum ethereum
[Cryptology ePrint Archive 2025](#)
- > [A. Huelsing et al.](#)
XMSS: eXtended Merkle Signature Scheme
2018
[doi:10.17487/RFC8391](https://doi.org/10.17487/RFC8391)

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 cryptography and privacy, motivation to implement modern protocols.

Advisor Contact

fabian.schmid@tugraz.at