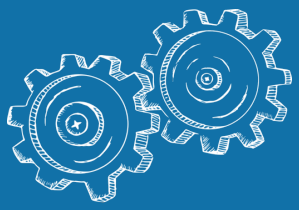

Merkle Tree in Hardware for Post-Quantum Cryptography

Advisor: **Maciej Czuprynko and Sujoy Sinha Roy**

Posted on: Sep, 2025

Motivation

Merkle trees are widely used in cryptographic applications such as digital signatures (e.g., CROSS, FAEST), blockchain, and verifiable data structures. Their security relies on the collision resistance of the underlying hash function, while their performance depends heavily on efficient computation of large numbers of hash values.

In software, Merkle tree construction can become a bottleneck, especially when many hashes need to be computed and stored. Hardware acceleration offers an opportunity to speed up this process by exploiting parallelism and memory hierarchies. The tree shrinks towards the tree and thus having many parallel cores becomes less effective in a simple implementation.

The goal of this project is to explore and implement efficient hardware designs for Merkle tree construction, with a particular focus on digital signature algorithm context, such as CROSS and/or FAEST. The project will evaluate different architectural approaches (e.g., pipelining, parallel hash units, memory management strategies) and quantify their impact on performance, area, and energy efficiency.

Goals and Tasks

- Get familiar with cryptographic hash functions and Merkle tree construction.
- Study the parallel processing methods.
- Implement and evaluate hardware architectures for Merkle Tree.

Literature

- Merkle Tree basics
  https : / / en . wikipedia . org / wiki / Merkle_tree

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 cryptographic hardware design
- Programming and SystemVerilog

Advisor Contact

{maciej.czuprynko,sujoy.sinharoy}@tugraz.at