

# Hardware Implementation of Raccoon Post-Quantum Signature Scheme





Advisor: **Florian Krieger**

## Motivation

The recent advances in quantum computing threatens the fundamentals of classical cryptography. Established signature schemes such as RSA will immediately be broken once a powerful quantum computer is developed. The Raccoon signature scheme is an interesting post-quantum signature scheme that has a strong focus on side-channel resistance.

## Goals and Tasks

Since the Raccoon scheme is brand new, there is no hardware implementation published yet. Hence, this project aims to investigate hardware-specific optimizations either for a high-performance or a low-area Raccoon implementation.

-  Get familiar with the Raccoon signature scheme and related works
-  Propose & implement optimizations for efficient hardware acceleration of Raccoon
-  Optional: Evaluate the side-channel resistance of your implementation
-  Compare your results to other PQ signature hardware accelerators



## Literature

- > Raccoon resources  
<https://raccoonfamily.org/>
- > R. del Pino et al.  
Raccoon: A Masking-Friendly Signature Proven in the Probing Model  
[Cryptology ePrint Archive, Paper 2024/1291](https://eprint.iacr.org/2024/1291) 2024  
<https://eprint.iacr.org/2024/1291>

## Courses & Deliverables

- Master Project**
  - Project code
  - Report
  - Presentation
- OR –
- Master's Thesis + DiplomandInnenseminar (CS)**
  - Initial presentation
  - Project code
  - Thesis (60+ pages)
  - Final presentation

## Recommended if you're studying

- CS
- ICE
- SEM

## Prerequisites

- > Interest in hardware design and PQ-Cryptography
- > "Crypto on Hardware" course is recommended

## Advisor Contact

[florian.krieger@tugraz.at](mailto:florian.krieger@tugraz.at)