

# Hardware Implementation of Raccoon Post-Quantum Signature Scheme






Advisor: **Aikata**

## Motivation

The rapid progress in quantum computing poses a serious threat to the core principles of classical cryptography. Traditional signature schemes like RSA will become vulnerable and can be broken instantly once sufficiently advanced quantum computers are created. The lattice-based Raccoon signature scheme offers a promising alternative in the realm of post-quantum cryptography, with a particular emphasis on resisting side-channel attacks.

## Goals and Tasks

The Raccoon scheme claims to enable cheap SCA resistance. We will analyze this claim theoretically as well as via implementation.

-  Get familiar with the Raccoon signature scheme and related works
-  Analyze Raccoon against the existing SCA attacks on Dilithium or similar schemes.
-  Mount an attack (or Mask the Raccoon subroutine implementations.)
-  If masked, evaluate its side-channel resistance
-  Compare your results to similar work on other PQ signature schemes



## 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

[aikata@iaik.tugraz.at](mailto:aikata@iaik.tugraz.at)