




# Side-channel Analysis of Exotic PQC Signature Schemes

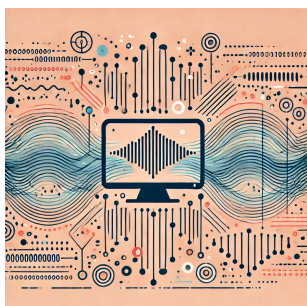
Advisor: **Rishub Nagpal**

## Motivation

The National Institute of Standards and Technology (NIST) has placed an extended call for quantum-resistant digital signature schemes based on different mathematical primitives (Code-based, Oil and Vinegar, Multivariate schemes etc.). The goal of this thesis is to select one (or a few candidates) and analyze the scheme's susceptibility to side-channel attacks. The scope of the project may include (but not limited to): implementing a scheme on a selected software/hardware platform, creating a novel attack tailored to a particular scheme in simulation or on a real device, developing countermeasures to protect against attacks. For more details, contact the linked email.

## Goals and Tasks

-  Get familiar with the state-of-the-art in post-quantum cryptography.
-  Get familiar with state-of-the-art in side-channel analysis.
-  Perform a real attack, in simulation or with real equipment



1

## Literature

- > [National Institute of Standards and Technology \(NIST\) Lightweight Cryptography Standardization Process](https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures-2024)  
<https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures-2024>

## Courses & Deliverables

- Master's Thesis + Diplomandinenseminar (CS)**
  - Initial presentation
  - Project code
  - Thesis (60+ pages)
  - Final presentation

## Recommended if you're studying

- CS
- ICE
- SEM

## Prerequisites

- > Interest in PQC and Side-channel attacks
- > Programming in C/x86/ARM Assembly/Verilog/Your favorite language

## Advisor Contact

[rishub.nagpal@tugraz.at](mailto:rishub.nagpal@tugraz.at)