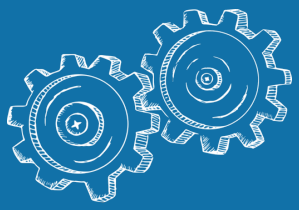

Investigating Backdoors in Post-Quantum Cryptography Implementations

Advisor: **Sujoy Sinha Roy**

Posted on: Sep, 2025

Motivation

With the standardization of post-quantum cryptography (PQC) by NIST and other government agencies, PQC algorithms are expected to be widely deployed in hardware and software platforms. However, even if a PQC scheme is mathematically secure, its real-world implementation may be compromised by backdoors or hardware Trojans introduced at the design or fabrication stage.

Recent works (e.g., REPQC and Kleptographic Backdoors in PQC) have demonstrated that stealthy modifications in PQC implementations can leak secret information without significantly affecting performance or area. This raises urgent questions on how such backdoors can be designed, detected, and mitigated.

The goal of this project is to investigate the feasibility of backdoors in PQC implementations, evaluate their detectability, and explore possible countermeasures. The project aims at analysing one PQC algorithm and its implementation as experimental case studies to provide information on the insertion of backdoors and the detectability of such backdoors.

Goals and Tasks

- Study existing Trojan and kleptographic backdoors.
- Get familiar with one or two PQC algorithms to understand how and where backdoors can be inserted.
- Develop proof of concept and perform experimentations.

Literature

- Pagliarini, Aikata, Malik, Roy
  REPQC: Reverse Engineering Post-Quantum Cryptography Hardware to Insert Trojans
  https://arxiv.org/pdf/2403.09352
- Ravi, Bhasin, Chattopadhyay, Roy
  Backdooring Post-Quantum Cryptography: Kleptographic Attacks on Lattice-based KEMs
  https://eprint.iacr.org/2022/1681

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 design
- Programming (C, C++, SystemVerilog or other hardware language)

Advisor Contact

sujoy.sinharoy@tugraz.at