



Machine Learning + Side-channel Analysis

Advisor: **Rishub Nagpal**

Motivation

Side-channel analysis remains a credible threat to the security of all computing devices. In the last decade, Machine learning and Deep-learning techniques have gained a lot of traction in solving side-channel problems, yet several questions remain unanswered regarding the best use-cases, explainability and performance of these strategies. This project/thesis will take a look at applying the latest techniques in ML/DL to solving side-channel problems on relevant side-channel targets.

Goals and Tasks

-  Get familiar with state-of-the-art DLSCA
-  Develop/Apply attacks on real devices
-  Compare and evaluate your results with the state-of-the-art



Literature

- > [K. et al.](#)
SoK: Deep Learning-based Side-channel Analysis Trends and Challenges
<https://eprint.iacr.org/2025/1309.pdf>

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: ML/DL, SCA
- > Programming (C/C++, Python, whatever you like)
- > Interest in taking physical measurements is a plus

Advisor Contact

rishub.nagpal@tugraz.at