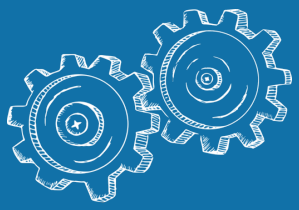

Side-Channel Security of Edge AI Accelerators

Advisor: **Sujoy Sinha Roy**

Motivation

Edge AI devices process sensitive data locally using specialized neural-network accelerators. Although this reduces the need to transmit private data to the cloud, the hardware may leak information through its power consumption. Recent research has shown that such leakage can reveal the architecture and parameters of a neural network, or even information about its inputs. However, the influence of implementation choices on this leakage is not yet sufficiently understood.

The goal of this thesis is to investigate power side-channel leakage from a small FPGA-based AI accelerator using the ChipWhisperer platform. You will implement a quantized neural network on a small FPGA and analyze whether its architecture or model parameters can be recovered from power traces. Based on the results, you will investigate countermeasures such as randomization of operation and evaluate their security and implementation overhead.

Goals and Tasks

- Get familiar with neural-network accelerators and power side-channel analysis
- Implement a small FPGA-based AI accelerator, perform a selected side-channel attack, and apply suitable countermeasures
- Evaluate how implementation choices affect leakage and analyze the security–performance trade-off

Literature

- P. Horvath et al.
  BarraCUDA: Edge GPUs do Leak DNN Weights
  USENIX Security 2025

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 hardware security and machine learning
- Basic knowledge of digital design

Advisor Contact

sujoy.sinharoy@tugraz.at