

Reproducing Deep Learning-based Side-Channel Attacks on Masked AES

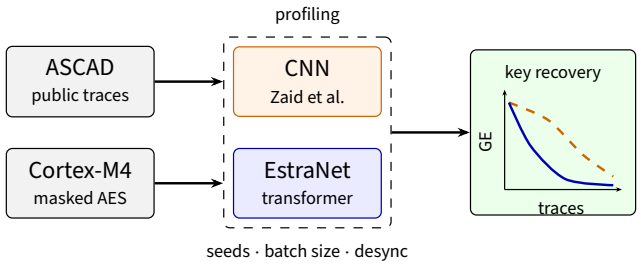
Advisor: **Maciej Czuprynko**

Motivation

Embedded cryptographic implementations must resist side-channel attacks that exploit physical leakage such as power consumption. Deep learning has become the state of the art for such attacks, breaking masked and desynchronized implementations without manual preprocessing. A recent example is EstraNet, a shift-invariant transformer that scales linearly with trace length and outperforms earlier models on traces with random delays and misalignment. However, deep learning results are often hard to reproduce, as they depend strongly on hyperparameters, random initialization and dataset preparation. In this project, we reproduce EstraNet, compare it to a lightweight CNN baseline, and test whether its results carry over to our own measurements.

Goals and Tasks

- Get familiar with profiled side-channel attacks, masking and deep learning-based side-channel analysis.
- Reproduce EstraNet and a CNN baseline on the public ASCAD datasets.
- Record power traces of a masked AES on a Cortex-M4 microcontroller and attack them with both models.



Literature

- S. Hajra, S. Chowdhury, and D. Mukhopadhyay
  EstraNet: An Efficient Shift-Invariant Transformer Network for Side-Channel Analysis
  CHES 2023
- G. Zaid et al.
  Methodology for Efficient CNN Architectures in Profiling Attacks
  CHES 2019

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in Deep Learning
- Knowledge of Python

Advisor Contact

maciej.czuprynko@tugraz.at