
Project Title: “*Side Channel Analysis Testbench for Evaluation of Trace Preprocessing Techniques*”

This project is suitable for both BSc and MSc students.

Contact Information

- Konstantinos Paraskevopoulos, MSc (UT-EEMCS)
 - k.paraskevopoulos@utwente.nl
 - Dr. ir. Nikolaos Alachiotis (UT-EEMCS)
 - n.alachiotis@utwente.nl
-
-

Project Description

The goal of this project is to design and implement a testbench to evaluate trace preprocessing techniques in the context of Side Channel Analysis (SCA).

- The testbench will allow systematic evaluation of different trace preprocessing methods, such as **trace alignment**, which are commonly used to improve the quality of SCA measurements.
- Evaluation will be based on SCA-relevant metrics, including Guessing Entropy, Key Rank, and other indicators of attack success.
- The primary attack methodology will be CNN-based SCA (CNN-SCA), reflecting the current state-of-the-art. Traditional SCA methods such as CPA can also be included for comparison.
- For automated CNN architecture generation and training, **Reinforcement Learning for SCA** will be used, enabling automatic CNN design and optimization for side-channel attacks without requiring prior machine learning expertise.
- Trace acquisition is not part of this project; publicly available trace datasets will be used for experimentation.

Expected outcomes:

- A **fully functional experimental testbench** capable of evaluating comparing various trace pre-processing techniques.

- **Quantitative insights** into whether trace preprocessing enhances CNN-based SCA performance.
-

Tasks

- **Survey and Literature Review:** Conduct a survey of existing technologies and literature in side channel analysis, existing SCA testbenches and publicly available trace datasets.
- **Review of “Reinforcement Learning for SCA” tool:** Experiment with the tool, as it will be the main way of evaluation of the different pre-processing methods.
- **Complete workflow design:** Design the complete workflow of the evaluation testbench. From loading the power traces, to SCA results comparison, there should be a complete system that handles the whole toolchain (Trace Loaders, Trace Pre-processing, CNN inference, Results Comparison, etc.).
- **Experiment Design:** Design of a demonstration experiment that showcases how the testbench work and how it can be used for different pre-processing methods, different datasets, or SCA methods (scalability).

Theory: 20%

Coding/Implementation: 30%

Evaluation: 30%

Writing: 20%