Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Assistant (Student)

Measurement Setup Validation Framework

Our chair has a Side Channel Analysis (SCA) group analysing the side channel properties of mainly cryptographic implementations. Implementations are realized either on a microcontroller or FPGA based target. Since measurements often require similar setups on different lab desktops, ensuring a correctly working measurement setup is crucial. Thus, validation tests to verify the correctness of the newly build up measurement setup are required. Those tests perform SCA on a known target configuration before switching the target to a new crypto-implementation under test.

Within this position, you should implement a test methology for both microcontroller and FPGA. The test crypto-function as well as the framework for both is already present. Also measurements can be taken automatically. Thus, concretely you put all those parts together in a script for easy validation.

Prerequisites

- Interest in side channel analysis
- Interest in hands-on development of SCA-tools
- Microcontroller Programming in C
- VHDL
- Python 3 knowledge
- Fluency in German or English

The position is not strictly limited to a number of weakly working hours.

Advisors

Matthias Probst