Multiple Bachelor/Master Theses
Machine-Learning based Side-channel Tampering-detection and Countermeasure

Side-channel analysis is a major threat for embedded systems. Unintended side-channels of the system can be used to extract encryption keys. Analyzing the power fluctuations (power analysis) or the electromagnetic radiation (electromagnetic analysis) are the most prominent in this area. This analysis requires tampering of the system.

For power analysis, a shunt resistor is placed on the power line to measure power fluctuations. For electromagnetic analysis, removing the fan, heat sink, and casing is done to place field probes close to the chip to measure its electromagnetic radiations.

Here at CES, a machine-learning (ML) based detection of side-channel tampering was already developed as a first step for a full framework to detect and successfully prevent side-channel attacks. It will be used as basis for the thesis topics described below.

Possible Thesis Topics
- Improving the ML solution to work under noisy environments
- Choosing and developing a successful state-of-the-art side channel countermeasure

Tasks of the student
Tasks will vary according to the thesis topic. Both hardware development and software development are performed. The focus depends on the selected topic, e.g. when working on the ML solution or integrating the detection and countermeasure to the bigger system.

Skills beneficial for the thesis
- Programming Skills (C, C++, Python)
- Knowledge of VHDL

Skills acquired with the Thesis
- Work in a research environment
- Hands-on experience in Hardware and Software development
- In depth knowledge of Hardware Security

Contact
Hassan Nassar, M.Sc., hassan.nassar@kit.edu
http://ces.itec.kit.edu/~nassar

Dr.-Ing. Lars Bauer, lars.bauer@kit.edu
http://ces.itec.kit.edu/~bauer