SCA of AI Hardware Accelerator
Neural Networks are inevitable in everyday life. Speech and face recognition as well as driverless cars are just some examples where Artificial Neural Networks (ANN) are used. Training a deep ANN is very time-consuming and computational expensive. Thus, the intellectual property stored in an ANN is an asset worth to protect. Additionally, implementations on edge devices need to be power-efficient whilst maintaining a high throughput. [1] or [2] are examples for frameworks aiming to fulfill these requirements.

A side-channel attack can be used to extract the network parameters such as the number or type of layers, as well as weights and bias values. In [3, 4] side-channel attacks on different implementations of ANNs are performed.

In this work, a side-channel attack on autogenerated implementations of different ANNs should be performed. This includes a detailed analysis of the side-channel properties of the different implementations.

Start of Thesis: Anytime

References:


Prerequisites

- VHDL/Verilog Knowledge
- Sichere Implementierung Kryptographischer Verfahren (SIKA)
- Python Skills

Contact

manuel.brosch@tum.de or matthias.probst@tum.de

Advisors

Manuel Brosch, Matthias Probst