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

Master's Thesis

SCA of Neural Networks

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 as ANN is an asset worth to protect.

An possible attack scenario would be to extract the network parameters such as the layer structure, weights and biases to build a copy of the network. Since there is a trend to perform neural network based classification on edge devices possible hardware attacks like Side-Channel Analysis must be considered.

Some attacks are already present. Batina et al. completely retrieve an ANN executed on an ARM Cortex microcontroller [1] . Since it is more common to execute an ANN on a more parallel HW to increase performance attacking FPGA implementations is also worthwise. Dubey et al. published an attack on a binary neural network (BNN) implemented on a FPGA and furthermore masked the network in order to counter their network [2, 3].

In this work, possible side-channel based attack vectors should be investigated. Based on these attack vectors, possible attacks should be performed on hardware accelerators for neural networks.

References

1. L. Batina, S. Bhasin, D. Jap, and S. Picek, “{CSI}{NN}: Reverse engineering of neural network architectures through electromagnetic side channel,” in 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 515–532, 2019.
2. A. Dubey, R. Cammarota, and A. Aysu, “Maskednet: A pathway for secure inference against power side-channel attacks,” arXiv preprint arXiv:1910.13063, 2019.
3. A. Dubey, R. Cammarota, and A. Aysu, “Bomanet: Boolean masking of an entire neural network,” arXiv preprint arXiv:2006.09532, 2020.

Prerequisites

- Knowledge about Side-Channel Analysis (attending “Sichere Implementierung kryptographischer Verfahren” or something similar is a must)
- Knowledge about VHDL or Verilog and FPGAs
- Good Programming Skills in Python

Advisors

Manuel Brosch, Matthias Probst