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

Forschungspraxis, Master's Thesis

SCA of Neural Network HW-Implementations

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 ANNs 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 extract the network parameters such as number of type of layers as well as weights and bias values to build up his own copy of the network. Since neural networks are also very integrated in edge devices an attack often has physical access to the network. This means that Side Channel Attacks (SCA) are possible and must be considered as a thread.

Some attacks were already published. In [3] they completely retrieve an ANN executed on an ARM Cortex microcontroller. Since it is more common to execute an ANN on a more parallel HW to increase performance attacking FPGA implementations is also worthwhile. 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 [4,5].

In this work, the Side-Channel properties of different model implementations should be analyzed and compared.

Start of Thesis: Jan 2022 or later

References:

[1] M. Blott, T. B. Preußer, N. J. Fraser, G. Gambardella, K. O'brien, Y. Umuroglu, M. Leeser, and K. Vissers, "Finn-r: An end-to-end deep-learning framework for fast exploration of quantized neural networks," ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 11, no. 3, pp. 1–23, 2018.
[2] Y. Umuroglu and M. Jahre, "Streamlined deployment for quantized neural networks," arXiv preprint arXiv:1709.04060, 2017.
[3] 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.
[4] A. Dubey, R. Cammarota, and A. Aysu, "Maskednet: A pathway for secure inference against power side-channel attacks," arXiv preprint arXiv:1910.13063, 2019.
[5] A. Dubey, R. Cammarota, and A. Aysu, "Bomanet: Boolean masking of an entire neural network," arXiv preprint arXiv:2006.09532, 2020.

Prerequisites

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

Advisors

Manuel Brosch, Matthias Probst