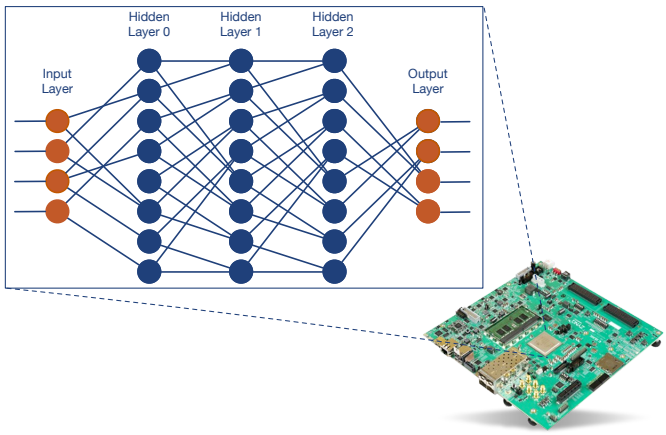
Chair of
„Secure Digital Circuits“

der Bundeswehr Universität München

Side-Channel Attacks on Neural Networks

Introduction



Neural networks are showing a lot of momentum especially thanks to many new potential applications in the realm of the Internet-of-Things. With neural networks starting to find their way into many electronic devices such as smart phones or earbuds an important question arises immediately: Are neural networks secure?

Short Project Description

A new field of research tries to answer the question by applying side-channel attacks on such neural networks. The goal of this project is to first realize a neural network for audio recognition on an FPGA platform and try to reproduce the audio track using power side-channel attacks. In a second part of the project, first countermeasures to minimize this vulnerability shall be developed and applied.

Prerequisites

- Interest in neuronal networks and their hardware implementation
- Experience in Hardware Description Languages (VHDL / Verilog) is helpful

What you will learn

You will get a deep understanding of neuronal networks as well as their implementation and contribute to a new field of research.

Contact

matthias.korb@unibw.de