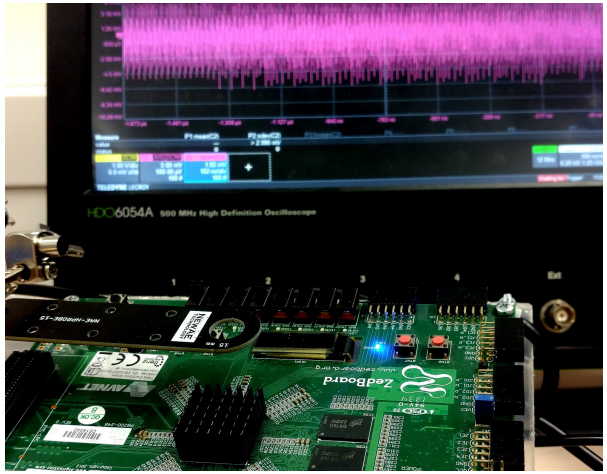
Using machine learning to apply SCA in a real world scenario



Side-channel analysis (SCA) of embedded hardware devices can be of great help for attackers or forensic investigators on a crime scene. SCA can be used to retrieve data and assess the state of a device. Furthermore it can be used to break encryption algorithms running on said device. In a **real world scenario** this is rather hard, because one can only monitor a specific time frame that hopefully contains some evidence of an encryption algorithm like AES. Those encryptions will occur in a bulk and are tough to analyze without separation.
Therefore, it is mandatory to split the recorded measurements into single encryption cycles. This separation could be done by using **machine learning (ML)** due to significant differences in the frequency domain. The goal of this project or thesis is to investigate how well ML works on finding recurring patterns of encryption algorithms in side-channel measurements.
In the future, such an ML algorithm could be a significant part of an FPGA-based analyzer for crypto-devices which could aid forensic investigators at crime scenes to gather valuable data in a useful form.

The amount of work can be adjusted to fit a *project* or *master thesis* but **preferably both** sequentially.
Please feel free to ask for details!

Prerequisites:	Programming skills in Python or C/C++ (experience with machine learning or signal processing is preferred but not mandatory)
Type of Work:	Theory (30%), Conception (20%), Implementation (50%)
Supervisor:	Jens Schlumberger (jens.schlumberger@fau.de)

@design

Lehrstuhl für Informatik 12
Hardware-Software-Co-Design
Cauerstraße 11
91058 Erlangen

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT