

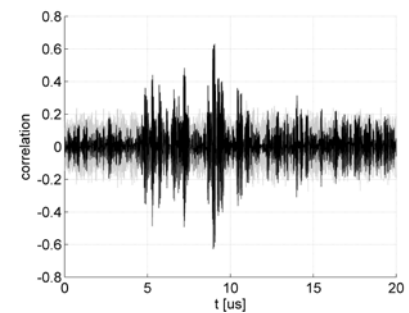
Evaluating Preprocessing Techniques for Power-Analysis Attacks

Motivation

Many hardware devices such as RFID tags have cryptographic algorithms implemented. One way to reveal the secret keys used by these devices are side-channel attacks. Here, e.g. the power consumption or the electromagnetic emanation of the device is recorded during the cryptographic operation. Afterwards the recorded traces are analyzed and in many cases parts of the secret key can be revealed. In order to get satisfying results several preprocessing steps such as filtering or aligning have to be conducted.

Project description

- Goals
 - Analysis of the influence of preprocessing techniques (filtering, aligning) on the result of DPA attacks.
- Tasks
 - Literature research and basic knowledge about DPA attacks.
 - Analyze the impact of filtering
 - Analyze the impact of alignment
 - Automate the search for the best parameters for filtering and aligning.



Literature

- S. Mangard, E. Oswald, T. Popp, „Power Analysis Attacks – Revealing the Secrets of Smart Cards“

Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately
- Month 1 Reading, planning, preparing
- Month 2 FPGA programming
- Month 3 Final deliverables

Master Project

Studies: INF SEW TEL

Prerequisites

- MATLAB

Advisor / contact

Thomas.Korak@iaik.tugraz.at