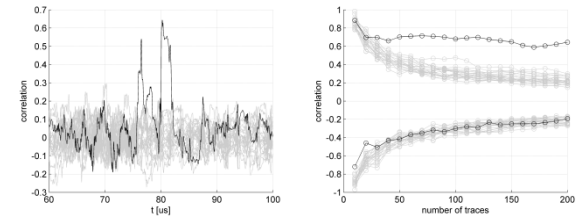


# Measurement Setups for DPA/DEMA Attacks on RFID Tags



## Motivation

DPA attacks are powerful attacks to reveal the used secret key of a cryptographic device by analyzing the power traces recorded during the cryptographic operation. RFID and NFC are contactless communication techniques and the tags used in such systems often have cryptographic algorithms implemented. The goal of this project is to evaluate different measurement methods for DPA attacks targeting such tags.

## Project description

- Goals
  - Successful DPA attack on RFID tag
  - Comparison of different measurement methods
- Tasks
  - Literature research
  - Basic knowledge about DPA attacks
  - Record power traces for DPA attacks
    - Using the Helmholtz antenna arrangement
    - Design a filter for reader signal suppression
    - Zoom into the traces using the oscilloscope
  - Perform DPA attack with the recorded traces
  - Evaluate the methods

## 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 Conduct the measurements
- Month 3 Final deliverables

## Master Project

Studies:  INF  SEW  TEL

## Prerequisites

- MATLAB scripts
- Measuring with an oscilloscope

## Advisor / contact

[Thomas.Korak@iaik.tugraz.at](mailto:Thomas.Korak@iaik.tugraz.at)