

# EM Attacks on Mobile Phones



## Motivation

The signal leakage of mobile phones can be measured at a distance of several meters (even when they are in airplane mode). In this project, an attack has to be performed on a Nexus S mobile phone that runs Elliptic-Curve Cryptography (ECC). Goal is to demonstrate the electromagnetic (EM) side-channel leakage over a large distance.

## Project description

- Goals
  - Get ECC running on the mobile phone (implementations already exist)
  - Identify EM leakage of the phone using appropriate measurement equipment
- Tasks
  - Literature research
  - Use a test receiver to filter frequencies
  - Use an antenna to measure the EM signals
  - Identify the leakage of the phone

## 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

- Interests in side-channel attacks and EM measurements

## Advisor / contact

[Michael.Hutter@iaik.tugraz.at](mailto:Michael.Hutter@iaik.tugraz.at)