

Power Consumption Characterization of Microcontrollers

Motivation

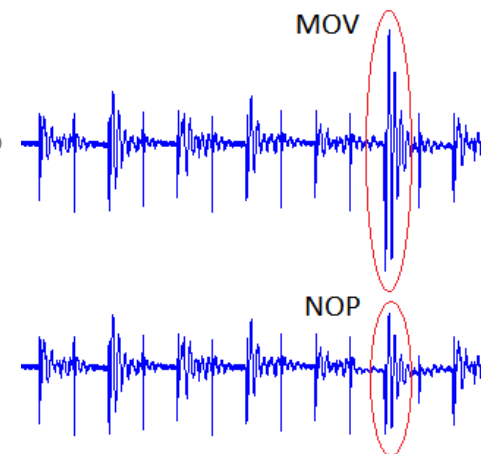
Side-channel attacks exploit small data dependencies in the power consumption of cryptographic devices, whereby the power consumption is measured during the operation of the attacked device (so-called power traces).

In order to evaluate the resistance of a device and/or a cryptographic implementation in an earlier stage, we want to create a power simulator using MATLAB. In a first step, the power consumption of various operations processing different data values on a target device (e.g. 8051 microcontroller) is characterized and stored in a database.

In a second step using this database, we can analyze the side-channel resistance of an implementation based on simulated power traces without the need to program and measure the actual device.

Project description

- Goals
 - Characterize the power consumption of one or more devices
 - Create simulated power traces of the device(s)
- Tasks
 - Get familiar with the IAIK MATLAB toolbox
 - Perform measurements of different devices



Deliverables

- Project files (.zip, cleaned)
- Documentation (paper)
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately or in autumn
- Block 1 Get familiar with the MATLAB toolbox and power measurements
- Block 2 Perform measurements of different operations on one or more devices

Bachelor Project

Studies: INF SEW TEL

Prerequisites

- One or more of the following: MATLAB, oscilloscopes, Assembly

Advisor / contact

Mario.Kirschbaum@iaik.tugraz.at
(Idea by Thomas Plos)