Power Analysis using Low-Cost Hardware: Lab Setup & Simple Targets

Colin O'Flynn & Zhizhang (David) Chen, Dalhousie University

coflynn@dal.ca

The objective of this tutorial is to introduce the participant to setting up a power analysis laboratory with very low-cost hardware. This hardware that will be demonstrated can be built for approximately $200USD, and one may even already have the required components on-hand. Beyond the hardware setup, some basic attacks will be demonstrated to validate the hardware and target environment and communication.

This hardware setup will include details of building the analog capture hardware, differential probe, magnetic field probe, and low-noise amplifier. This hardware is available quasi-commercially for students that are not interested in building their own from scratch.

A demonstration of the use of the SASEBO-W board with this special capture hardware will also be part of the tutorial. The SASEBO-W is anticipated to be used in the DPA Contest v4, thus this tutorial will provide a timely demonstration for participants interested in this contest, but without previous experience in physically capturing power traces used in side-channel analysis.

A summary of this work has previously been presented at several Blackhat conferences, this tutorial substantially elaborates on these previous talks.