DPAContest V3 Entry

Submitter Colin O'Flynn
Affiliation Dalhousie University
Contact coflynn@dal.ca
Entries 2 (TWO) additional entries based on a single acquisition

Acquisition Methodology

A python application controls the SASEBO-GII in addition to the acquisition hardware. This application will be released in an open-source manner, but if there is interest I can send the source code. The two entries contained here would fall in the category of "lowest total acquisition cost", if such a category in the contest existed.

In total there are **TWO (2)** entries into the DPA Contest V3 contained in this .zip.

Probe Setup

The probe setup used is an inductive pickup. A single VINT decoupling capacitor (C46, 100nF part number GRM15561A104KA01, 0402 size) is mounted on the SASEBO-GII board to try and shunt the most possible current through this capacitor. The inductive pickup is 7 wraps of 34AWG magnetic wire around that capacitor.

Oscilloscope

The oscilloscope used is my OpenADC, an open-hardware platform containing an ADC + LNA. The acquisition rate is 96 MSPS, which is derived from the 24 MHz AES clock. This low acquisition rate should work because it is perfectly synchronized with the AES clock.

Detail of the OpenADC platform are available at http://www.assembla.com/spaces/openADC . Total cost for the entire acquisition HW is around $200 in single-unit quantity. While these results are unlikely to provide the best possible results, the extremely low cost of the acquisition HW is noteworthy.

The AES FPGA was clocked at 24 MHz for these acquisitions, which seemed to provide the best results with the inductive pickup.

Capture 1

capture-2012.06.27-16.45.59

This is the 'raw' capture file containing 40K traces, each trace being 64 points.

capture-2012.06.27-16.45.59_windowed

This capture is windowed to only contain points 51-56, which is the data around the round 10 key only