DPAContest V3 Entry

Submitter Colin O'Flynn
Affiliation Dalhousie University
Contact coflynn@dal.ca

Entries Seven (7), based on Three (3) separate acquisitions

Acquisition Methodology

The publically available AIST acquisition tool was used to capture the traces. There is three sets of traces captured, using a similar technique but under slightly different environments. In addition each of the three sets is subject to different post-processing.

In total there are **SEVEN (7)** entries into the DPA Contest V3 contained in this .zip. Many of them are very short (<10 points/trace), so processing time should be negligible. The total entry size is still < 100 MB.

Probe Setup

The probe setup used is an inductive pickup. A single VINT decoupling capacitor (C46, 22nF part number C0603C223Z3VAC) is mounted on the SASEBO-GII board to try and shunt the most possible current through this capacitor. The inductive pickup is 11 wraps of 34AWG magnetic wire around that capacitor.

Oscilloscope

The Oscilloscope used is an Agilent 54831D sampling at 2 GS/second in all captures. The modified source code for the AIST application is available at https://www.assembla.com/spaces/sasebofork which adds support for the 54831D scope.

The AES FPGA was clocked at 24 MHz for these acquisitions, which provided the best results in the inductive pickup.

Capture 1

Capture 1 was performed with the inductive pickup directly feeding the oscilloscope. Vertical sensitivity was 5mV/div.

wf_gii_2012_02_23_220623

This is the 'raw' capture file. It contains 3000 traces, each of 1250 points.

wf_gii_2012_02_23_220623_window

This capture is windowed to only contain points 930-939, which is the data around the round 10 key only.

Capture 2

Capture 2 was performed with the inductive pickup feeding a MiniCircuits ZFL-1000LN Low Noise amplifier, which then connected to the oscilloscope. Vertical sensitivity was 50 mV/div.

wf_gii_2012_02_26_145258

This is the 'raw' capture file. It contains 4000 traces, each of 1250 points.

wf_gii_2012_02_26_145258_average

This is a trace-file where each data-point consist of the averages of point 935 to 938, the data points around round 10. The result is a file consisting of 4000 traces, each of 1 point.

wf_gii_2012_02_26_145258_window

This capture is windowed to only contain points 934-943 of wf_gii_2012_02_26_145258, which is the points around the round 10 key. The result is a file consisting of 4000 traces, each of 10 points.

wf_gii_2012_02_26_145258_lowpasswindow

This capture passes the data through a low-pass IIR filter, of order N=5, Wc=0.5. Then only the data around the round 10 key is written to wave.txt (points 947-952).

Capture 3

Capture 3 was performed with the inductive pickup feeding a MiniCircuits ZFL-1000LN Low Noise amplifier, which then connected to the oscilloscope. The VINT of the AES FPGA was set to 0.744V instead of the normal 1.000V. Vertical sensitivity was 20 mV/div. The supply voltage for the LNA was adjusted to result in the output signal of the LNA being close to full-scale (actual VCC for LNA was about 10.5V).

wf_gii_2012_02_26_143222_averaged

This is a trace-file where each data-point consist of the average of point 935 to 940, the data points around round 10 calculations. The result is a file consisting of 2500 traces, each of 1 point. Note the raw capture file is not provided, as without this post processing it seemed to provide poor results. I can send this raw capture file though if you wish to confirm the data.