A Power Analysis Report for the DPA Contest V3

July 31, 2012

Matsumoto Laboratory
Graduate School of Environment and Information Sciences
Yokohama National University

With 800 traces we successfully extracted the hidden 128-bit key as

0xD481EAE9D7512D595408EA77F630B0C3

from the given AES circuit implemented on the Virtex-5 FPGA of a SASEBO-GII.

- Figure 1 shows the configuration for the final result.
- Figure 2 depicts the environment of experiment for the final result.
- Table 1 shows features of each hardware component for the final result.
- Table 2 shows the measurement setup for the final result.
- Table 3 indicates the history of experiment with the number of traces required to obtain the key.
- Figure 3 shows typical waveform of the 10^{th} round.
- Figure 4 shows the number of right estimation bytes with the CPA tool.

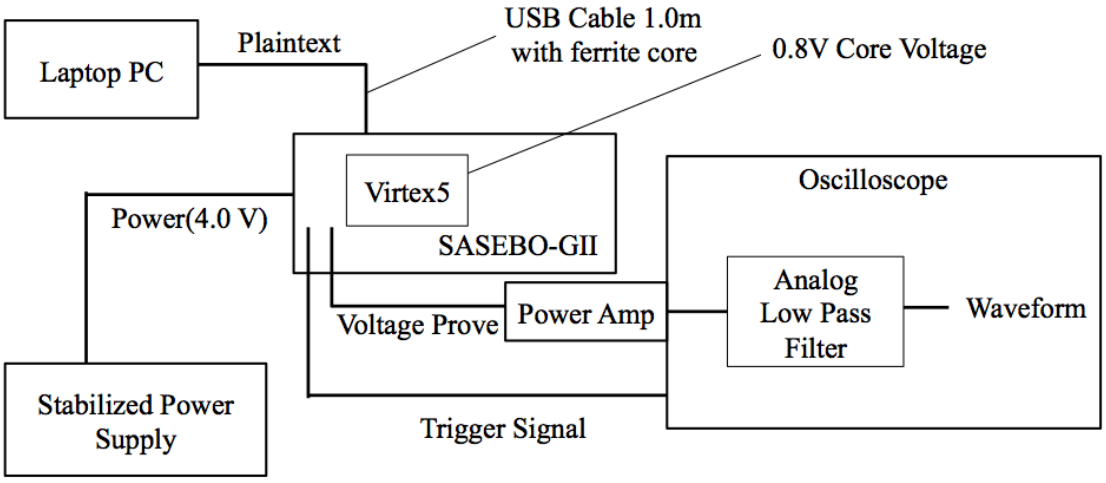

Figure 1. Configuration for the Final Result

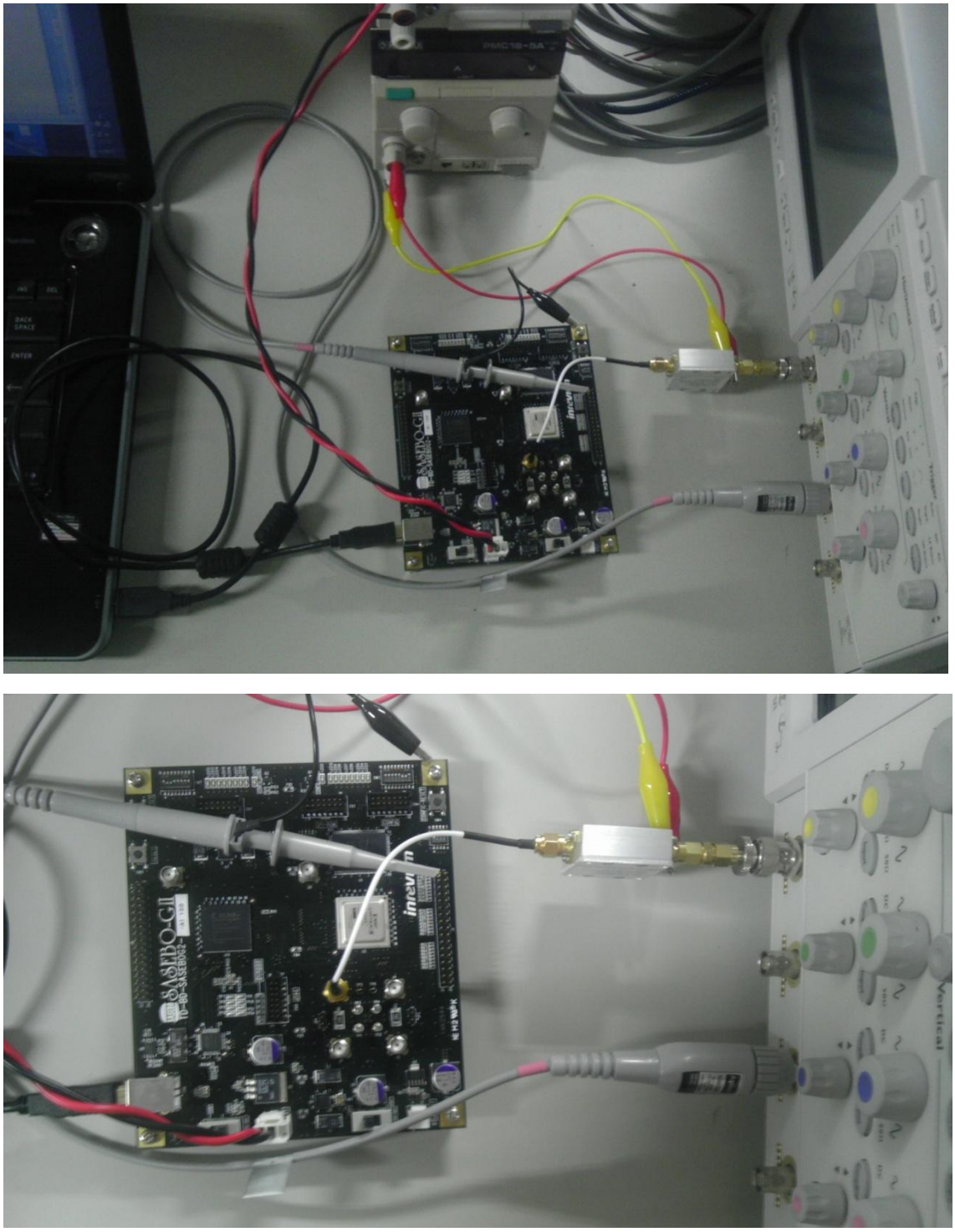

Figure 2. Environment of Experiment for the Final Result

Table 1. Hardware Environment for the Final Result

Equipment	Feature
Board	SASEBO-GII (TD-BD-SASEBOG2-A1)
Control PC	Toshiba Laptop PC Dynabook TX/66HBL Core2Duo P8600 4GB memory
Power supply	KIKUSUI PMC18-5 Stabilized power supply
Oscilloscope	Agilent DSO8104A
Voltage probe for trigger signal	Agilent 10073C
Power Amp	COSMOWAVE LNA270WS
USB cable	1.0m with ferrite core

Table 2. Measurement Setup for the Final Result

Item	Setup
Plaintext	random text (SASEBO Waveform Acquisition)
Virtex-5 FPGA Core voltage	0.8V
Spartan-3 FPGA Core voltage	4.0V
Operating Freq	2 MHz
Measurement position	1Ω shunt resistance side of the core power
Resolution	1G samples/sec (2,000 samples/clock)
Number of Sample points	3,500 points
Jumper pin	JP1-open, JP2-open, JP3-place a jumper
Post-treatments	None

Table 3. History of Experiment with Number of Traces Required to Obtain the Key

Number of Traces	Setup
2,000	Initial setup with AIST's data acquisition program, 1.0V power supply for the FPGA core, without analog filter
4,000	1.0V power supply for the FPGA core, without analog filter, increment text from 00…0, 2.0m USB cable without ferrite core, without power amp, Power supply from Desktop PC
2,700	Power supply from Laptop PC through 2.0m USB cable, random plain text (SASEBO Waveform Acquisition)
1,900	1.0m ferrite core USB cable
1,800	Analog filter was applied
1,000	Reduce the Virtex-5 core voltage down to 0.8V
800	changed to the other random plain text (SASEBO Waveform Acquisition), with Power Amp, Reduce the Spartan-3 core voltage down to 0.8V

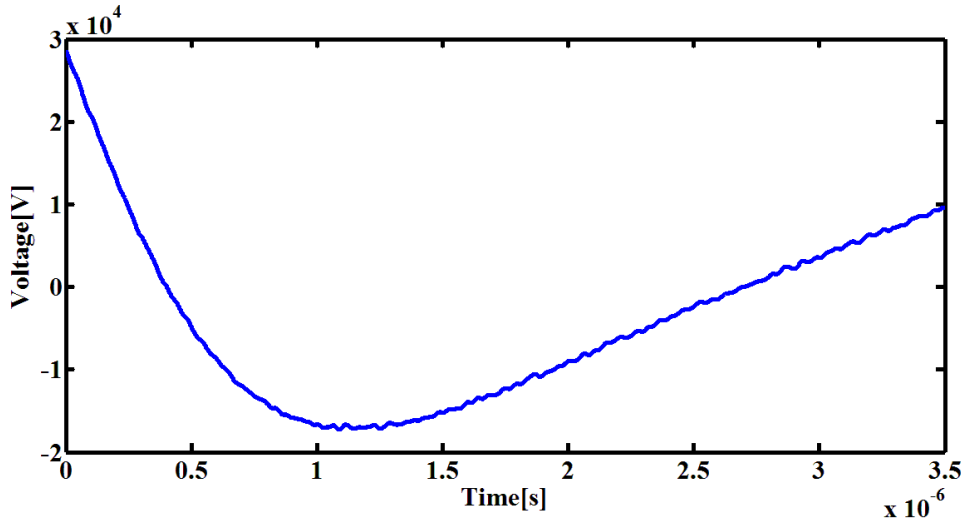

Figure 3. Typical Waveform of the 10th Round

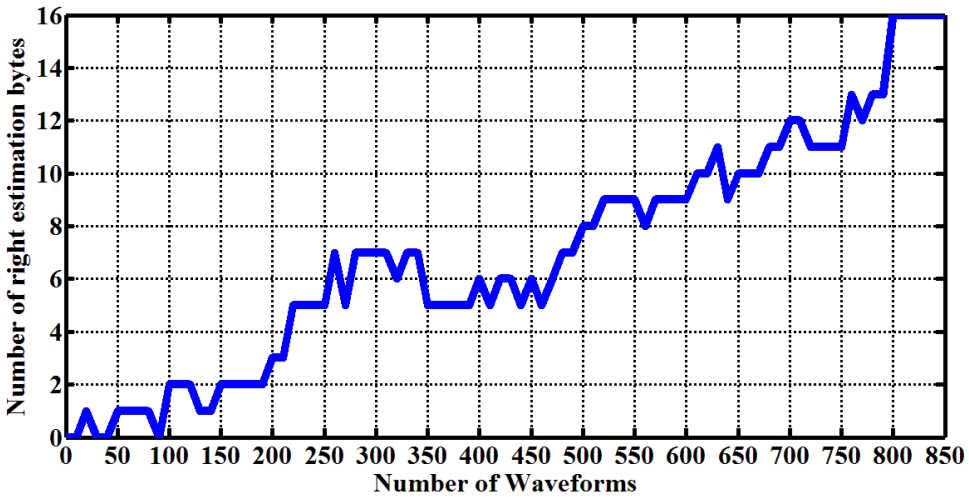

Figure 4. Number of Right Estimation Bytes