Detail Description for the submission

Yongdae Kim (kimyd@ensec.re.kr)

1. Measurement environment

We measured power traces using SMA-BNC cable without any special filters. Moreover, we utilize exactly sample equipment and setup as SASEBO Waveform Acquisition Quick Start Guide Ver. 1.0 [1] except a digital oscilloscope. Table1 shows more detail information for the acquisition. Using the setting, we captured 100k traces at first. By adjusting the delay, we captured 1000 sampling points for the last round power consumption trace (See Fig. 1.)

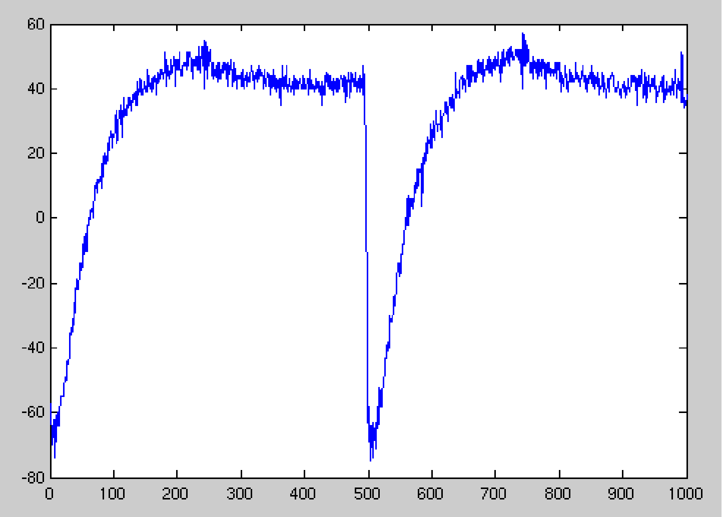

Figure1 Measured Power Consumption Trace

Table1 Experimental Environment

Module	SASEBO-GII (LX30)
Number of points	1000
Digital Oscilloscope	LeCroy WaveRunner 640 Zi
Sampling Frequency	1GSa/s
Power Supply	From USB
Oscillator	24MHz (Set by SW7)

2. Post-processing

Firstly, we adapted low-pass filter and choosing 4k traces from 100k to be biased. Refer to [2] for more information of the method to choose the traces. This can help increase correlation factor for CPA.

References

[1] http://www.risec.aist.go.jp/project/sasebo/download_preb/SASEBO-GII_QuickStartGuide_Ver1.0_English.pdf, September 2009

[2] Yongdae Kim, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki and Akashi Satoh, “Biasing power traces to improve correlation in power analysis attacks”, COSADE 2010, February 2010