DPAContest V3 - ULB Team

Stephane Fernandes Medeiros & Lerman Liran & Nikita Veshchikov

February 6, 2012

We collected power traces using *Tektronix TPS 2024B 200MHz, 2GS/s* oscilloscope. We used *Coax Cable ; RG-59U ; BNC PLUG On Both Side* probe in order to measure the power consumption and *Tektronix TPP0201 Voltage Probe; 200MHz; 10MOhm / >12pF; 300V CAT II* probe for the trigger. The SASEBO-GII (TD-BD-SASEBOG2) was used without modification of the design of the control FPGA.

We used 500 different plaintexts and we collected 100 single acquisitions per plaintext. Let T_i^j be the i^{th} ($i \in \{1, 2, ..., 100\}$) trace linked to the j^{th} ($j \in \{1, 2, ..., 500\}$) plaintext. All traces were aligned thanks to the trigger.

In order to reduce the size of the archive, as post-processing method, we realized a filter noise by averaging 20 different traces linked to the same plaintext in order to estimate the average:

$$\frac{1}{20} \sum_{i=k}^{(k+20)\text{mod}100} T_i^j$$

where $k = \{0, 5, 10, 15, ..., 95\}$ for each plaintext j. The result is 20 traces per plaintext.