Leakage Assessment Report for Ascon_DOM_1st_order

Cankun Zhao Hang Zhao Bohan Yang Wenping Zhu Leibo Liu

August 14, 2022

1. Target implementation
   (a) Algorithm: **Ascon.**
   (b) Team: **IAIK, Graz University of Technology, Austria.**
   (c) Variant name: **Ascon_v1.**
   (d) Protection method: **Domain-oriented Masking (DOM).**
   (e) Protection: **1.**
2. Experimental setup
   (a) Measurement platform and device-under-evaluation: **Design-under-evaluation was instantiated on the Xilinx Spartan-6 (XC6SLX75-2CSG484C) FPGA on SAKURA-G board. The other Xilinx Spartan-6 (XC6SLX9-2CSG225C) FPGA on SAKURA-G was used for control.**
   (b) Description of measurements: **The design-under-evaluation power consumption is measured at the output of the SAKURA-G's on-board amplifier (AD8000YRDZ), that amplifies the voltage drop across the on-board 1 Ω shunt resistor.**
   (c) Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **N/A.**
   (d) Frequency of operation: **4 MHz.**
   (e) Oscilloscope and its major characteristics: **Teledyne LeCroy WaveRunner 8404M with 4 GHz bandwidth was used to collect traces.**
   (f) Sampling frequency and resolution: **Sampling rate of 100 MS/s and 8-bit sample resolution were used.**
   (g) Are sampling clock and design-under-evaluation clock synchronized? **No.**
3. Leakage assessment characteristics
   (a) Leakage assessment type: **Fixed vs. random t-test at first order [GGR11] and second order [SM15].**
   (b) Number of traces used: **10,000,000 traces for the protected and 100,000 for the unprotected implementation.**
   (c) Source of random and pseudorandom inputs: **Trivium-based DRBG.**
   (d) Trigger location relative to the execution start time of the algorithm: **Scope trigger is set at the beginning of the algorithm execution.**
   (e) Time required to collect data for a given leakage assessment: **About 4 hours.**
   (f) Total time of the attack/assessment: **About 6 hours.**
   (g) Total size of all traces (if stored): **37.4 GB.**
   (h) Availability of raw measurement results: **Per request.**
4. Results of leakage assessment
   (a) Graphs illustrating the obtained results: **T-test results are shown in Figure 2, Figure 4. The raw waveform of 50 traces is provided in Figure 1 as a reference to understand the leakage in t-test.**

(b) Attack scripts: **N/A.**

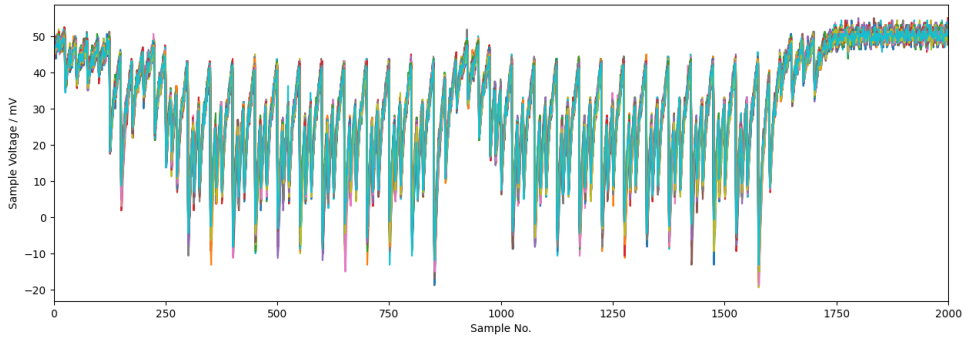

Figure 1: Waveform of 50 traces.

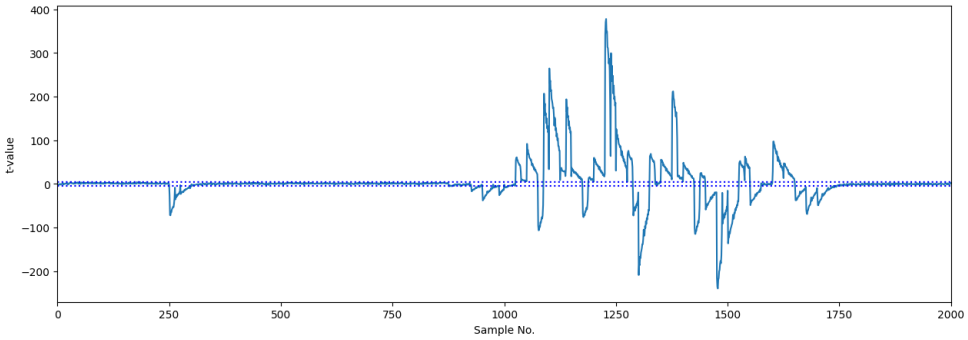

Figure 2: Unprotected design first-order t-test results (100,000 traces).

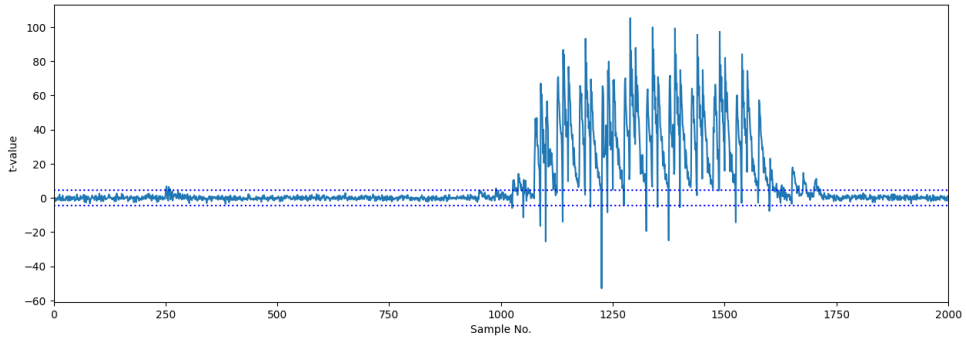

Figure 3: Unprotected design second-order t-test results (100,000 traces).

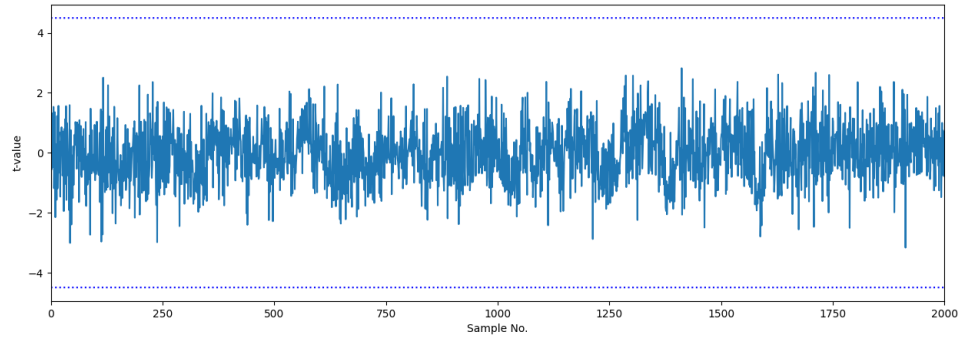

Figure 4: Protected design first-order t-test results (10 million traces).

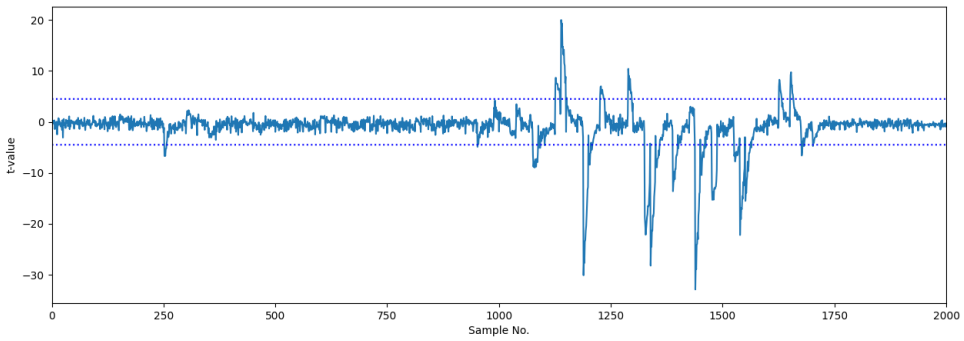

Figure 5: Protected design second-order t-test results (10 million traces).

References

[GGR11] Josh Jaffe Gilbert Goodwill, Benjamin Jun and Pankaj Rohatgi. A testing methodology for side-channel resistance validation. In *NIST Non-Invasive Attack Testing Workshop*, Nara, Japan, 2011.

[SM15] Tobias Schneider and Amir Moradi. Leakage assessment methodology - A clear roadmap for side-channel evaluations. In Tim Güneysu and Helena Handschuh, editors, *CHES 2015*, volume 9293 of *LNCS*, pages 495–513. Springer, Heidelberg, September 2015.