Leakage Assessment Report for Xoodyak_R3_first_order

Cankun Zhao Hang Zhao Bohan Yang Wenping Zhu Leibo Liu

September 5, 2022

1. Target implementation
   (a) Algorithm: **Xoodyak.**
   (b) Team: **Ruhr-University Bochum, Germany.**
   (c) Variant name: **Xoodyak_R3_first_order.**
   (d) URL: **https://github.com/Chair-for-Security-Engineering/LWC-Masking/tree/main/Xoodyak/Xoodyak_R3_first_order.**
   (e) GitHub commit hash: **4e954f283f0bf7ec25ca49f811e51df32fb2e9f0.**
   (f) Protection method: **Hardware Private Circuits 2.**
   (g) Protection: **1.**
2. Experimental setup
   (a) Measurement platform and device-under-evaluation: **Design-under-evaluation was instantiated on the Xilinx Kintex-7 (XC7K160T-1FBG676C) FPGA on SAKURA-X board. The other Xilinx Spartan-6 (XC6SLX45-2FG484C) FPGA on SAKURA-X was used for control.**
   (b) Description of measurements: **The design-under-evaluation power consumption is measured at the output of the amplifier (PA 303N), that amplifies the voltage of SAKURA-X board's measurement point.**
   (c) Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **N/A.**
   (d) Frequency of operation: **6 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 1000 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 150,000 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 7 hours.**
   (f) Total time of the attack/assessment: **About 15 hours.**
   (g) Total size of all traces (if stored): **186 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 3, Figure 4, and Figure 5. 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.**

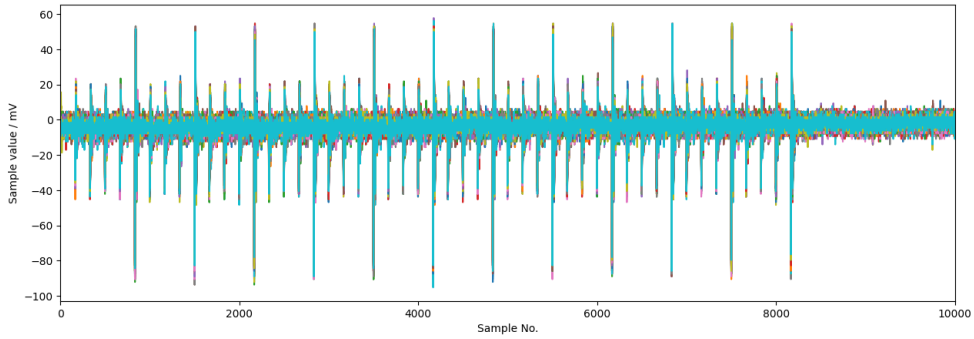

Figure 1: Waveform of 50 traces.

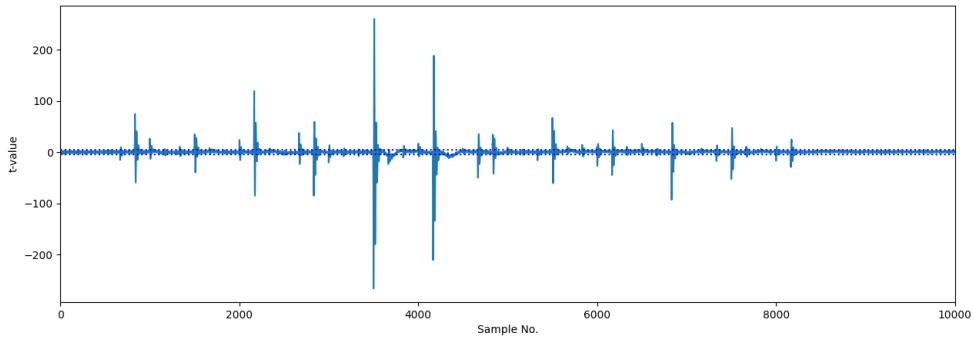

Figure 2: Unprotected design first-order t-test results (150,000 traces).

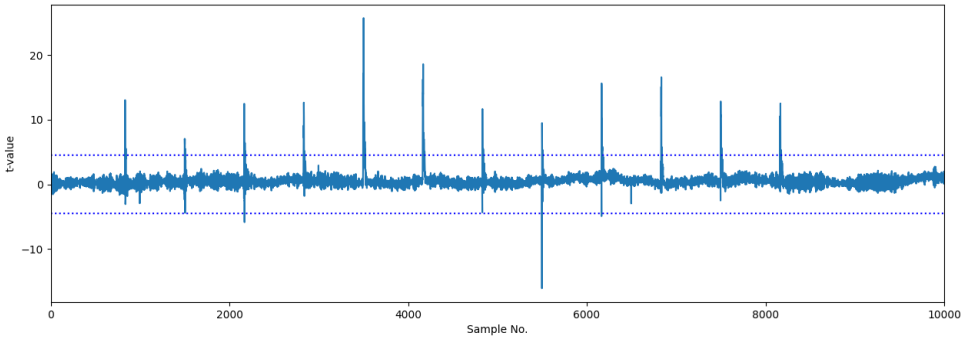

Figure 3: Unprotected design second-order t-test results (150,000 traces).

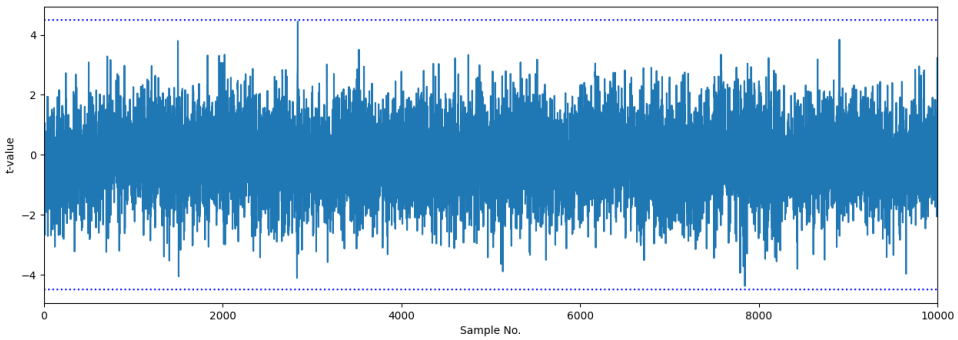

Figure 4: Protected design first-order t-test results (10 million traces).

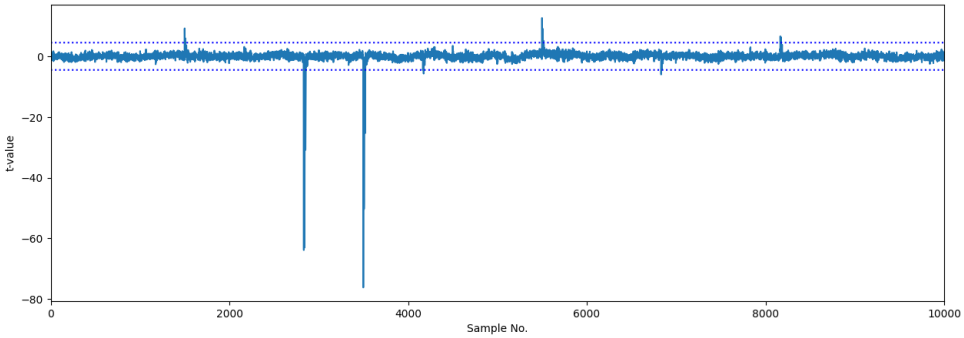

Figure 5: Protected design second-order t-test results (10 million traces).

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.