Documentation of Xoodyak_DOM_first_order (v0.2.1)

Shuohang Peng Shuying Yin Cankun Zhao Hang Zhao

May 10, 2022

1. Protection Method
   (a) Name of the applied countermeasure: **Domain-oriented Masking (DOM).**
   (b) Corresponding primary reference describing this countermeasure (when applied to an arbitrary cryptographic algorithm): **Primary reference is the paper by Gross et al. [GMK16].**
2. Results of the Preliminary Security Evaluation 1
   (a) Attack/leakage assessment type: **Fixed vs. random t-test at first order [GGR11] and second order [SM15].**
   (b) Number of traces used: **One million traces for the protected and 10,000 for the unprotected implementation.**
   (c) Experimental setup
      i. 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.**
      ii. 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.**
      iii. Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **N/A.**
      iv. Frequency of operation: **3 MHz.**
      v. Oscilloscope and its major characteristics: **Teledyne LeCroy WaveRunner 8404M with 4 GHz bandwidth was used to collect traces.**
      vi. Sampling frequency and resolution: **Sampling rate of 100 MS/s and 8-bit sample resolution were used.**
      vii. Are sampling clock and design-under-evaluation clock synchronized? **No.**
   (d) Attack/leakage assessment characteristics
      i. Data inputs and performed operations: **Tested operation is the Xoodoo permutation with 12 rounds. Input test vectors are initially shared on the control FPGA. The data input for the fixed data-set is chosen to make the state bits after the third round all zero.**
      ii. Source of random and pseudorandom inputs: **Trivium-based DRBG.**
      iii. Trigger location relative to the execution start time of the algorithm: **Scope trigger is set at the beginning of the algorithm execution.**
      iv. Time required to collect data for a given attack/leakage assessment: **About 70 minutes.**
      v. Total time of the attack/assessment: **About 80 minutes.**
      vi. Total size of all traces (if stored): **1.9 GB.**
      vii. Availability of raw measurement results: **Per request.**
   (e) Attack-specific characteristics
      i. Power model: **N/A.**
      ii. Attack point: **N/A.**
   (f) Documentation of results

i. 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.**

ii. Attack scripts: **N/A.**

3. Results of the Preliminary Security Evaluation 2

(a) Attack/leakage assessment type: **Fixed vs. random χ^2-test [MRSS18].**

(b) Number of traces used: **1,000,000 traces for the protected and 1,000 for the unprotected implementation.**

(c) Experimental setup: The same as the above t-test experiment.

(d) Attack/leakage assessment characteristics

i. **This χ^2-test is done over the same traces collected in the above t-test experiment.**

ii. **The bit width of sample value used in χ^2-test: 8 bits.**

iii. **Time required to run the χ^2-test per 10,000 traces (600 Samples/trace): About one minute.**

iv. Availability of raw measurement results: **Per request.**

(e) Attack-specific characteristics

i. Power model: **N/A.**

ii. Attack point: **N/A.**

(f) Documentation of results

i. **The χ^2-test results are represented in terms of $-log_{10}(p)$, where p is the p-value of this test. We choose a threshold for p-value of $\alpha = 10^{-5}$, which leads to a confidence of $>$ 0.99999 to reject the null hypothesis.**

ii. Graphs illustrating the obtained results: **For the unprotected design, only result on 1000 traces is given, as shown in Figure 6, as it already has very small p-values. For the protected design, 10k traces show no leakage, 20k traces show some leakage, and 100k traces show significant leakage, as shown in Figure 7, Figure 8, and Figure 9, respectively.**

iii. Attack scripts: **N/A.**

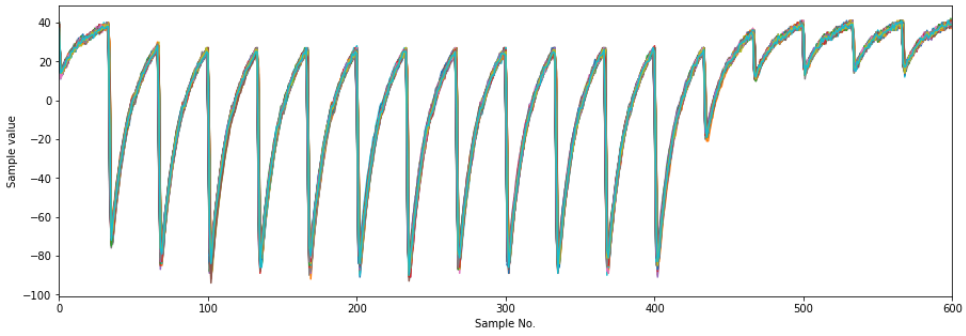

Figure 1: Waveform of 50 traces.

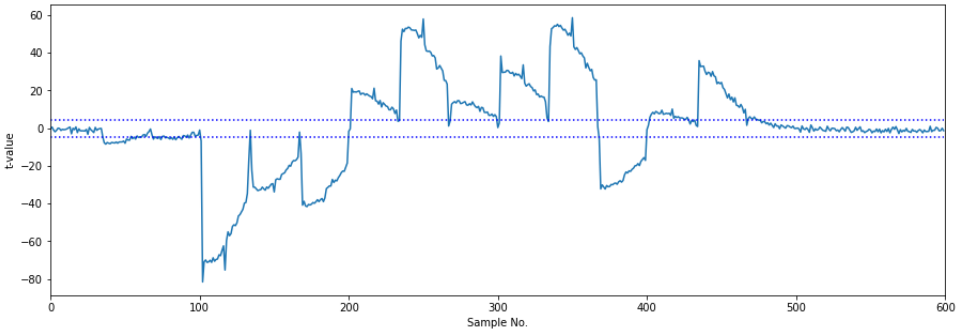

Figure 2: Unprotected design first-order t-test results (10,000 traces).

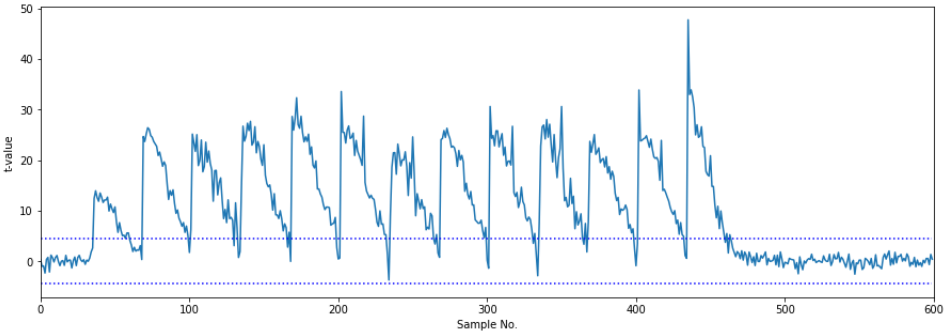

Figure 3: Unprotected design second-order t-test results (10,000 traces).

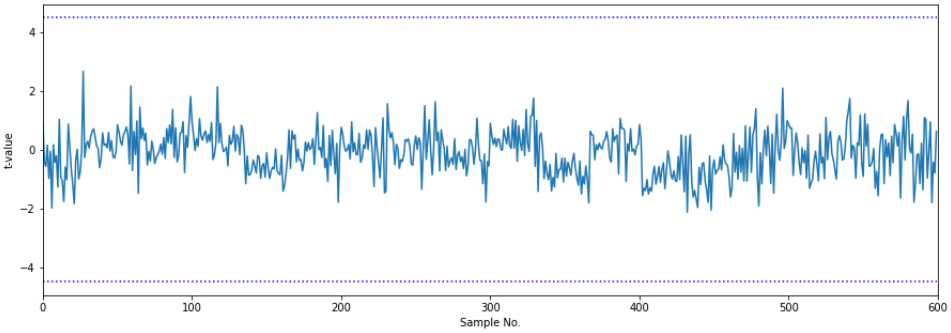

Figure 4: Protected design first-order t-test results (1 million traces).

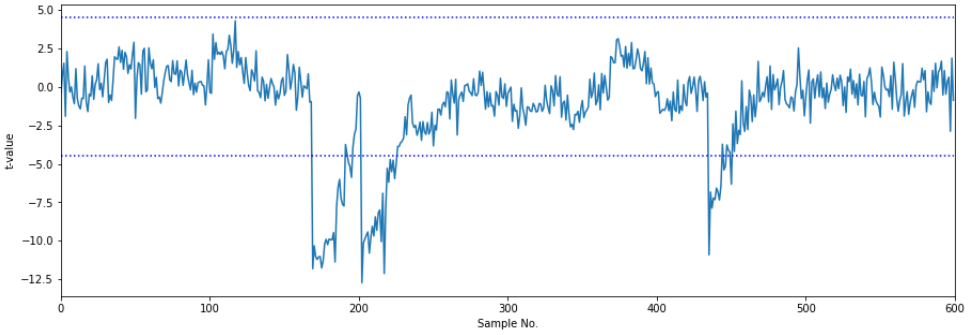

Figure 5: Protected design second-order t-test results (1 million traces).

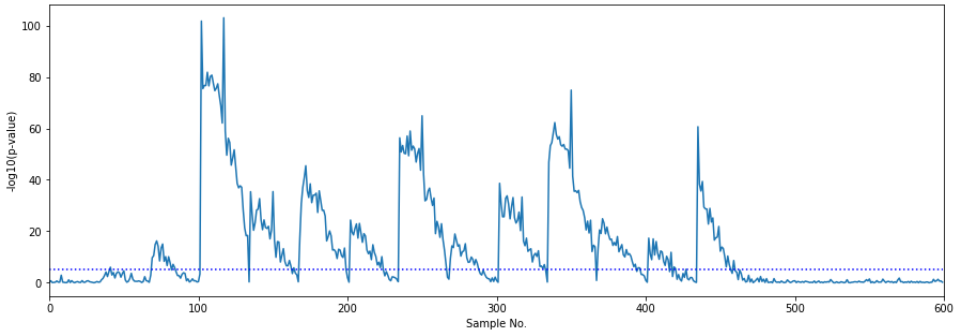

Figure 6: Unprotected design χ^2-test results (1,000 traces).

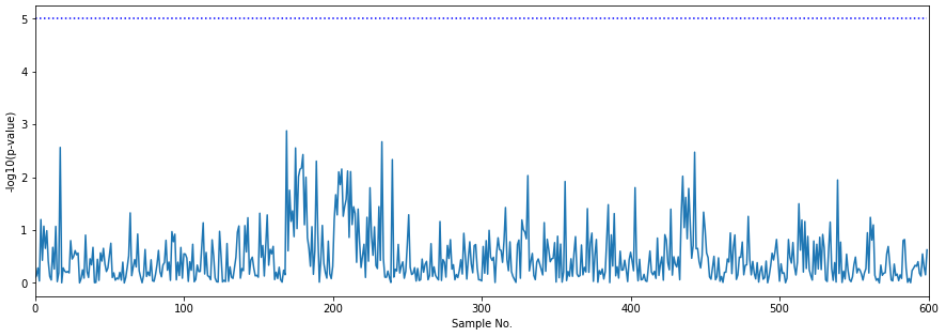

Figure 7: Protected design χ^2-test results (100,000 traces).

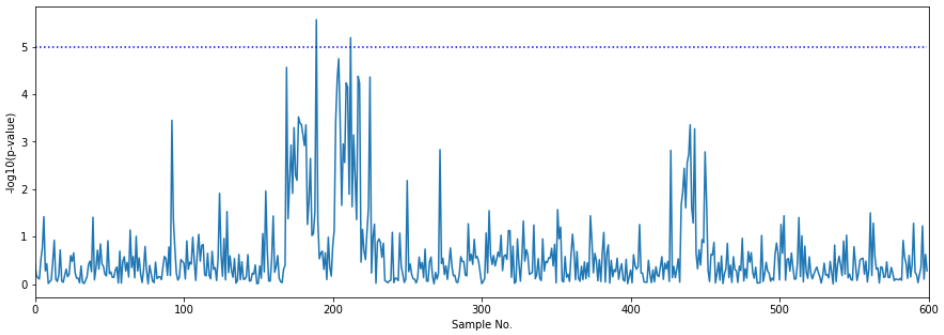

Figure 8: Protected design χ^2-test results (200,000 traces).

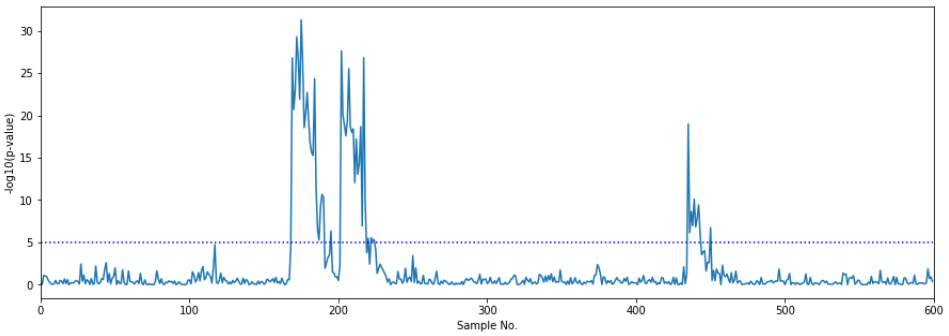

Figure 9: Protected design χ^2-test results (1,000,000 traces).

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.

[GMK16] Hannes Groß, Stefan Mangard, and Thomas Korak. Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. In Begül Bilgin, Svetla Nikova, and Vincent Rijmen, editors, *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*, page 3. ACM, 2016.

[MRSS18] Amir Moradi, Bastian Richter, Tobias Schneider, and François-Xavier Standaert. Leakage detection with the χ^2-test. *IACR TCHES*, 2018(1):209–237, 2018. `https://tches.iacr.org/index.php/TCHES/article/view/838`.

[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.