# Leakage Assessment on Xoodyak_R3_first_order

9/15/2022

Abubakr Abdulgadir Jens-Peter Kaps Kris Gaj

1. Target

a) Algorithm: **Xoodyak**
b) Implementer: **Ruhr-University Bochum, Germany**
c) Variant: **Xoodyak_R3_first_order**
d) URL: **https://github.com/Chair-for-Security-Engineering/LWC-Masking**
e) Commit hash: **4e954f283f0bf7ec25ca49f811e51df32fb2e9f0**
f) Protection method: **Hardware Private Circuits 2 (HPC2)**
g) Protection order: **1**

2. Equipment and Software Used

(a) General type of the evaluation platform: **Control board is FOBOS3 board for control. This board uses a PYNQ-Z1 board with a Zynq SoC (XC7Z020-1CLG400C) and a custom board that hosts an ADC for power measurement. The target board is NewAE CW305 Aritx7 (xc7a100tftg256)**
(b) Oscilloscope and its major characteristics: **We utilized OpenADC with 40 MHz bandwidth and a maximum sampling rate of 100 MS.**
(c) Current and electromagnetic probes: **N/A**
(d) Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **Power was measured at the output of the CW305's onboard amplifier which amplifies the voltage drop across the board's 0.1 Ω shunt resistor.**
(e) Are sampling clock and design-under-evaluation clock synchronized? **Yes**
(f) Names and versions of programs used for evaluating side-channel resistance: **FOBOS3 analysis software.**
g) Clock frequency of target: **10 MHz**
h) Sampling frequency and resolution: **50 M Sample/sec sampling frequency and 10 bit resolution.**

3. Leakage Assessment Method

a) Type of the method: **Fixed-vs-random Test Vector Leakage Assessment [GJJR11 ,SM15].**
b) Number of traces: **10 million traces.**
c) Source of randomness: **Trivium-based DRBG.**
**Before each test vector is processed, the DRBG is run to store the required number of random words in a FIFO. The design-under-evaluation then consume randomness from the FIFO and the DRBG is disabled while the design-under-evaluation is running. The goal of this is to eliminate the effect of the DRBG power consumption on the measurements.**
d) Trigger location relative to the execution start time of the algorithm: **Triggered ADC at the start of the algorithm.**
e) Time required to collect data for a given attack/leakage assessment: **About 19 hours.**
f) Total time of the attack/assessment: **About 19 hours.**
g) Total size of all traces (if stored): **19 GB.**
h) Availability of raw measurement results: **Per request.**

i) Test vector generation:
**The test vectors used and the scripts used for generation are available in the attached file.**

**The procedure is as follows:**

**1- Generate a short unshared test vector using cryptotvgen.**

**2- Convert it into a shared format using gen_shared.py.**

**3- Generate the FOBOS-ready fixed-vs-random test vectors using lwc_2_fobos_tv.py. The SDI is kept similar in all test vectors, and the PDI section is fixed in fixed test vectors and random in the random test vectors. Fresh sharing on the PDI section is generated in all test vectors.**

4. Results:

a) Documentation of results: **Figure 1 shows first-order TVLA using 10 million traces. Figure 2 shows t-values vs. number of traces processed. Listing 1 shows the clock cycles where t-values exceed the threshold for the test vectors attached.**

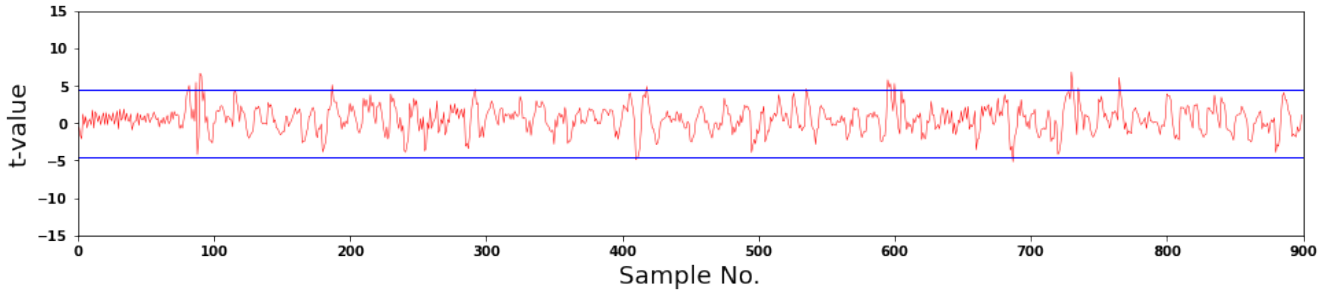


**Figure 1**: TVLA results for Xoodyak_R3_first_order (10 million)

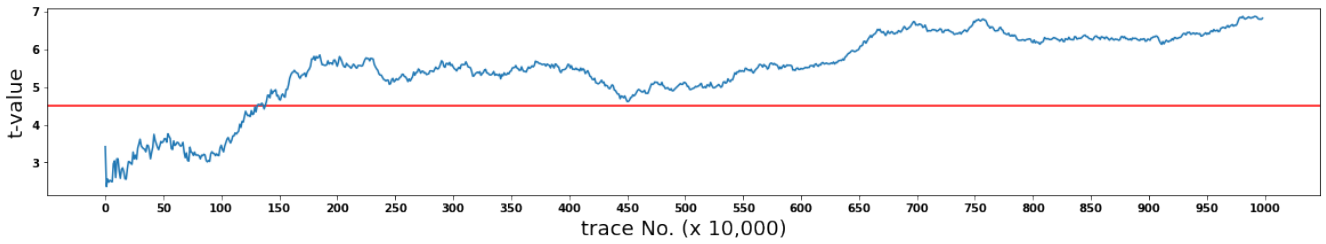


**Figure 2:** Xoodyak_R3_first_order maximum t-value vs. number of traces (x 10,000)

**Listing 1**: Samples that exceed the 4.5 threshold

```
82 --16 -- 5.0
87 --17 -- 5.4
90 --18 -- 6.7
91 --18 -- 6.3
187 --37 -- 5.1
292 --58 -- 4.5
410 --82 -- -4.9
411 --82 -- -4.7
418 --83 -- 4.9
535 --107 -- 4.6
595 --119 -- 5.8
596 --119 -- 4.8
597 --119 -- 5.3
600 --120 -- 5.3
687 --137 -- -5.2
730 --146 -- 6.8
731 --146 -- 4.7
735 --147 -- 4.7
765 --153 -- 6.1
```

## Test Using Picoscope

We ran another TVLA test using the same settings as the previous test with the following exceptions. We used the Picoscope oscilloscope for power measurement and the sampling rate used was 125 M Sample /sec, and the resolution is 8-bit. The sampling clock and target clock are not in sync. In this case we observe no spikes above the threshold. The results of this test is shown in Figure 3 and 4. The difference between the two sets of results is likely related to the usage of the synchronized clock and the higher resolution in the first test. The effect of the synchronized clock was previously observed in [Oflynn17].

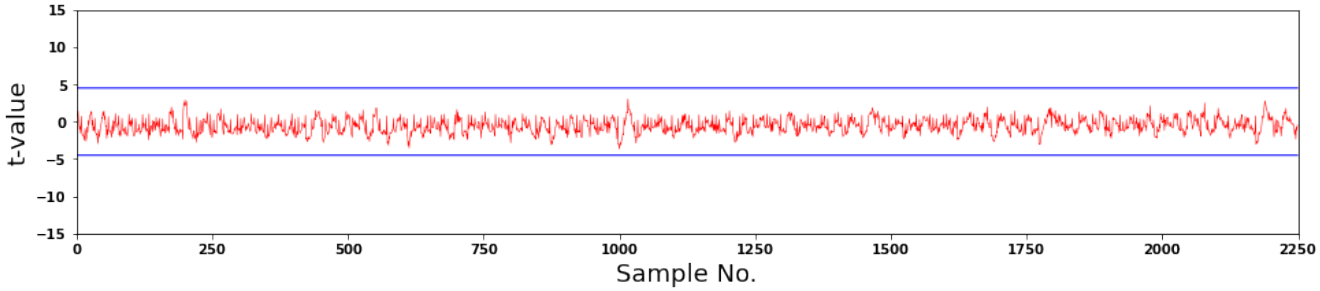


Figure 3: TVLA results for Xoodyak_R3_first_order using Picoscope (10 million)

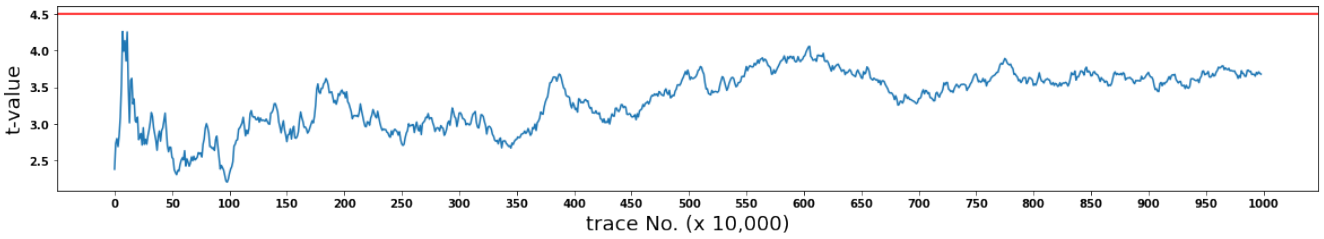


Figure 2: Xoodyak_R3_first_order maximum t-value vs. number of traces using Picoscope (x 10,000)

## References

[GJJR11] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, “A testing methodology for side-channel resistance validation,” Nara, Japan, 2011.

[SM15] T. Schneider and A. Moradi, “Leakage Assessment Methodology - a clear roadmap for side-channel evaluations,” Cryptology ePrint Archive 2015/207, Jun. 2015. Accessed: Dec. 31, 2021. [Online]. Available: https://eprint.iacr.org/2015/207

[Oflynn17] C. O’Flynn, “A Framework for Embedded Hardware Security Analysis,” Ph.D. Thesis, Dalhousie University, Halifax, Nova Scotia, 2017.