SMAesH: preliminary evaluation report

SIMPLE-Crypto

Contents

1 Overview

This document presents the findings of the preliminary evaluation of the resistance of the SMAesH (`aes_enc128_32bits_hpc2`) hardware IP to power analysis attacks. The evaluation has been performed the the developers of SMAesH (SIMPLE-Crypto).

The terminology for this report is defined in the SMAesH technical documentation [SC23].

2 History

2023-05-01 Initial evaluation covering SMAesH v1.0.0, $d = 2$.

3 Evaluation scope

The IP `aes_enc128_32bits_hpc2` allows selecting the amount of shares d at synthesis time. For this preliminary evaluation, we use exclusively $d = 2$.

This evaluation investigates exclusively first-order leakage comparatively to second order leakage. Assessment of other metrics (such as amount of information leakage or number of traces needed for key recovery) are outside of the scope of this report.

4 Measurement Setup and Traces Pre-processing

We synthesize the `aes_enc128_32bits_hpc2` IP on a Xilinx Artix 7 FPGA (package xc7a100tftg256-2) and run it with, at each execution, a fresh sharing of the key and of the plaintext. The PRNG is initialized with a fresh 80-bit seed.

We perform a power analysis of this implementation using a CW305-A100 evaluation board from NewAE.[1] A continuous supply voltage of 1 V is provided to VCC-INT by a low noise Keysight E36102B[2] power supply through the dedicated banana jacks of the board, and the FPGA clock frequency is 1.5625 MHz (it is generated by the on-board PLL from the onboard crystal). We probe the shunt measurement at the dedicated low noise amplified signal point X4 with a digital oscilloscope Picoscope 6424E from PICO TECHNOLOGY.[3] The measurements are performed at 5 GS/s with an enhanced vertical resolution of 10 bits. The clock of the oscilloscope is synchronized to the clock of the FPGA using a 10 MHz clock derived from the PLL on the CW305 board.[4] The size of traces is then reduced by aggregating (i.e., summing) 16 measurements samples into a single one, resulting in a practical sampling rate of 312.5 MHz and an equivalent vertical resolution of 14 bits.

5 Evaluation Methodology

We follow the TVLA methodology [GGJR+11]: we perform non-specific fixed-vs-random Welch's T-tests (with 1 million traces). In particular, first- and second-order univariate T-tests have been conducted over the full execution with the traces set divided in two partitions: one for which the value of the unmasked key k is fixed and the other for which it is random. For both sets, the two shares of the plaintext are fixed to 0 and the key sharing is fresh for each execution. Following [DZD+17], we set the significance threshold to 5.034, corresponding to a significance threshold $\alpha = 0.01$ for $n_L = 21000$ leakage points in the trace (this only includes the 10 AES rounds). The t-value computation was performed using the student T-test implementation of SCALib.[5]

[1] `https://rtfm.newae.com/Targets/CW305%20Artix%20FPGA/`

[2] `https://www.keysight.com/us/en/product/E36102B/dc-power-supply-6v-5a-30w.html`

[3] `https://www.picotech.com/oscilloscope/6000/picoscope-6000-overview`

[4] This synchronization, combined with the high sampling rate, ensures good trace alignment. To further reduce the trace misalignment caused by clock phase drift, a simple trace re-alignment is applied: the acquired traces are shifted by the (small) integer number of samples that maximizes the correlation to a reference trace.

[5] `https://scalib.readthedocs.io/en/stable/source/_generated/scalib.metrics.Ttest.html`

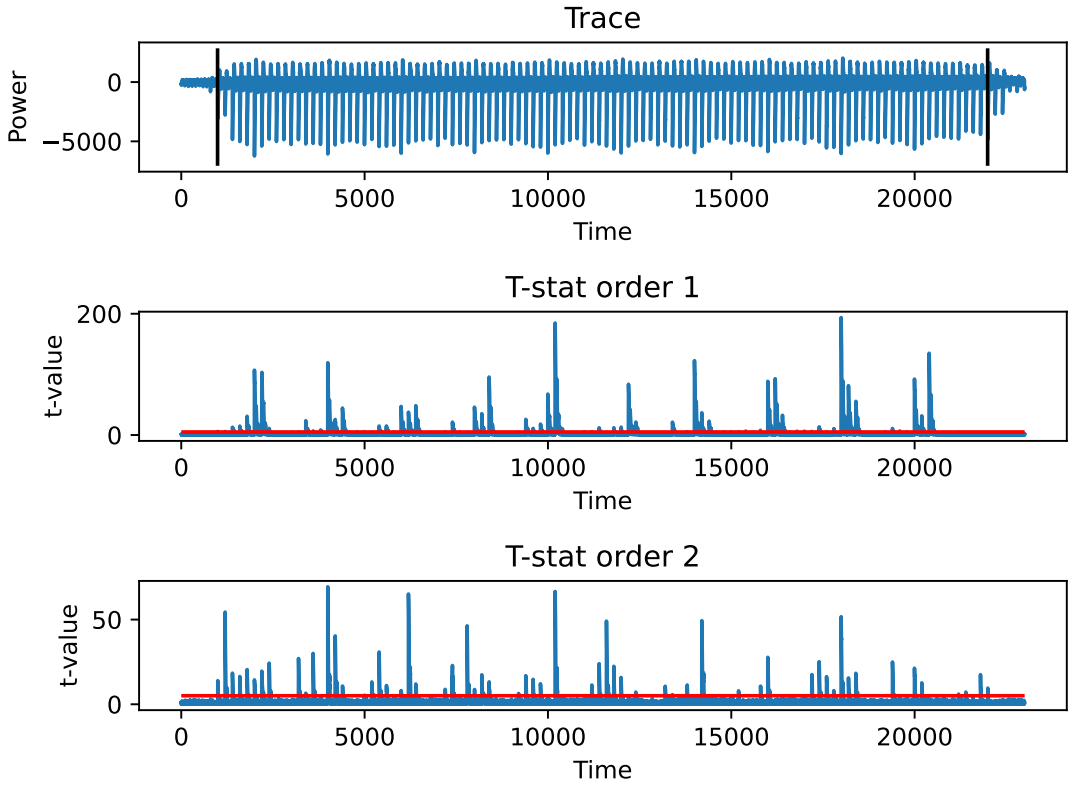

Figure 1: TVLA with PRNG disabled. The vertical black delimiters mark the range of 21000 samples corresponding to one AES encryption.

6 Results

We first performed a T-test with the countermeasure disabled, that is, when the PRNG seed is the same for all the traces. The result is shown in Figure 1. Significant first-order and second-order leakage can be observed in this setting (for all the AES rounds). Besides, the T statistic at first order is larger than the one observed at second order (around 5 times larger).

Second, Figure 2 shows the T-test results when the PRNG is enabled. In that configuration, no more leakage is detected with the T-test at first order, while peaks of T-value above the threshold are still observable along the time frame of an execution at second-order.

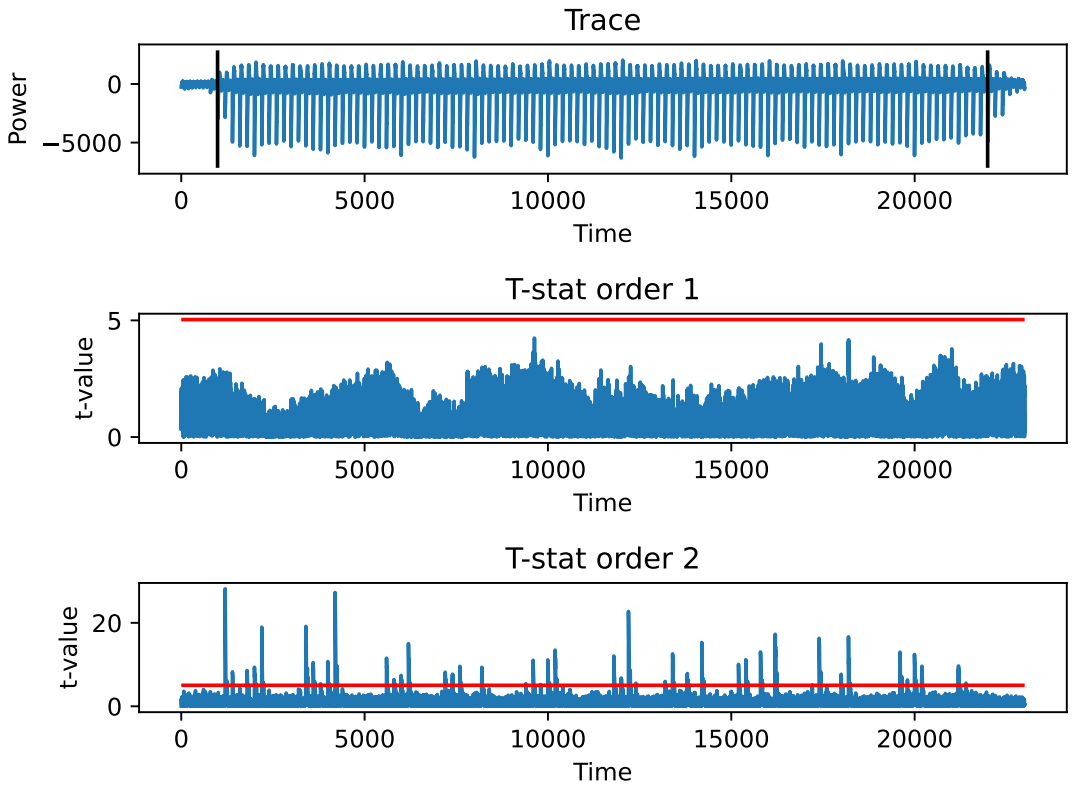

Figure 2: TVLA with PRNG enabled.

7 Conclusion

We do not detect first-order leakage after 1 million traces, while a significant amount of second-order leakage is detected. As usual with leakage detection, this preliminary result does not guarantee that first-order leakage cannot be detected with more traces. Yet, it allows us to conclude that that masking is effective for the noise level of our implementation and that the best attacks will exploit second-order leakage.

8 Copyright

References

[DZD+17] A. Adam Ding, Liwei Zhang, François Durvaux, François-Xavier Standaert, and Yunsi Fei. Towards sound and optimal leakage detection procedure. In *CARDIS*, volume 10728 of *Lecture Notes in Computer Science*, pages 105–122. Springer, 2017.

[GGJR+11] Benjamin Jun Gilbert Goodwill, Josh Jaffe, Pankaj Rohatgi, et al. A testing methodology for side-channel resistance validation. In *NIST non-invasive attack testing workshop*, volume 7, pages 115–136, 2011.

[SC23] SIMPLE-Crypto. SMAesH: technical documentation, 2023.