Documentation of a protected implementation

1 Protection Method

Our hardware implementation of TinyJAMBU-128 uses Domain Oriented Masking [5] to resist first-order Differential Power Analysis (DPA) [6].

The state register is duplicated as well as the logic needed to compute the NLFSR feedback bits. The rest of the datapath, which is responsible for implementing the mode of operation and performs data selection (multiplexing), FrameBits bit addition, etc., is also duplicated with constant addition performed in one copy of the datapath. We instantiate a DOM-dep multiplier [4] instead of the AND gates used in the NLFSR. More detailed description of the design can be found in [2].

2 Results of the Preliminary Security Evaluation

To validate the SCA resistance of our protected implementations, we utilized the Test-vector Leakage Assessment methodology (TVLA) [3].

We utilized the Flexible Opensource workBench fOr Side-channel analysis (FOBOS) [1] platform, and the DUT was instantiated in a NewAE CW305 board, which is a low-noise SCA target board that uses Artix-7 (xc7a100tftg256-3) FPGA. The DUT power consumption is measured at the output of the CW305's Low-Noise Amplifier (LNA), that amplifies the voltage drop across the on-board 0.1 Ω shunt resistor. We clocked the DUT with a low frequency of 1.25 MHz. A USB3-based oscilloscope (Picoscope 5244D) with 200 MHz bandwidth was used to collect traces at a sampling rate of 125 MS/s and 8-bit sample resolution. The sampling clock and the DUT clock were not synchronized. Random data was generated using Trivium.

TVLA results are shown in Figure 1 and 2. For the unprotected baseline design, the t values exceed the threshold, which indicates a significant leakage as expected. This leakage is observed even at only 10,000 traces. On the other hand, the TVLA for the protected implementations shows no observable leakage even when 1 million traces are analyzed.

References

[1] Abubakr Abdulgadir, William Diehl, and Jens-Peter Kaps. *An Open-Source Platform for Evaluating Side-Channel Countermeasures in Hardware Implementations of Cryptography.* Hardware Demo. Cancun, Mexico, 2019.

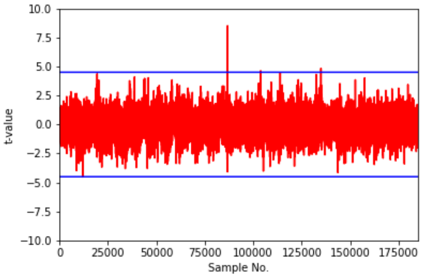

Fig. 1. Unprotected design TVLA results

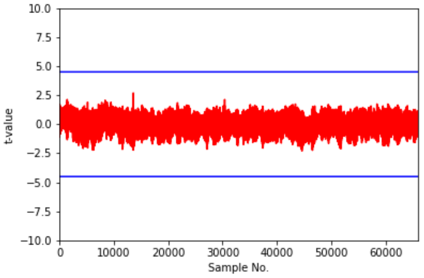

Fig. 2. Unprotected design TVLA results (1 million traces)

[2] Abubakr Abdulgadir, Sammy Lin, Farnoud Farahmand, Jens-Peter Kaps, and Kris Gaj. "Side-Channel Resistant Implementations of a Novel Lightweight Authenticated Cipher with Application to Hardware Security". In: *2019 Great Lakes Symposium on VLSI, GLSVLSI 2021*. Virtual, June 2021.

[3] Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi. "A Testing Methodology for Side–Channel Resistance Validation". In: *NIST Non-Invasive Attack Testing Workshop*. Nara, Japan, 2011.

[4] Hannes Groß. "Domain-Oriented Masking - Generically Masked Hardware Implementations". PhD thesis. Austria: Graz University of Technology, June 2018.

[5] Hannes Gross, Stefan Mangard, and Thomas Korak. "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order". In: *Proceedings of the 2016 ACM Workshop on Theory of Implementation Security - TIS'16*. Vienna, Austria: ACM Press, 2016, pp. 3–3. ISBN: 978-1-4503-4575-0. DOI: 10.1145/2996366.2996426.

[6] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Diferential Power Analysis". In: *CRYPTO '99 - 19th International Conference on Cryptology*. Santa Barbara, CA, Aug. 1999.