Documentation of a protected implementation

1. Protection Method
   - (a) Name of the applied countermeasure: **Domain-oriented Masking (DOM). More detailed description of our implementation can be found in [2].**
   - (b) Corresponding primary reference describing this countermeasure (when applied to an arbitrary cryptographic algorithm): **Primary reference is the paper by Gross et al. [4].**
2. Results of the Preliminary Security Evaluation
   - (a) Attack/leakage assessment type : **Test Vector Leakage Assessment (TVLA) [3].**
   - (b) Number of traces used : **1 Million traces for the protected and 10,000 for the unprotected implementation.**
   - (c) Experimental setup
     - i. Measurement platform and device-under-evaluation (e.g., ChipWhisperer, CW305 FPGA board): **Design-under-evaluation was instantiated on NewAE CW305 board, which features a Xilinx Artix-7 (xc7a100tftg256-3) FPGA. FOBOS [1] used for control and analysis.**
     - ii. Description of measurements, e.g., shunt resistor value, current probe specification, electromagnetic probe specification and placement: **The design-under-evaluation power consumption is measured at the output of the CW305's Low-Noise Amplifier (LNA), that amplifies the voltage drop across the on-board $0.1\,\Omega$ shunt resistor.**
     - iii. Usage of bandwidth limiters, filters, amplifiers, etc. and their specification: **N/A.**
     - iv. Frequency of operation: **1.25 MHz.**
     - v. Oscilloscope and its major characteristics (e.g., bandwidth): **A USB3-based oscilloscope (Picoscope 5244D) with 200 MHz bandwidth was used to collect traces.**
     - vi. Sampling frequency and resolution: **Sampling rate of 125 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: **Input test vectors initially shared in software. Tested operation is authenticated encryption.**
     - ii. Source of random and pseudorandom inputs (e.g., TRNG type, hardware implementation of Trivium, etc.): **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: **Five hours.**

v. Total time of the attack/assessment: **Data collection and analysis were performed simultaneously.**

vi. Total size of all traces (if stored): **N/A.**

vii. Availability of raw measurement results: **Not available.**

(e) Attack-specific characteristics

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

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

(f) Documentation of results

i. Graphs illustrating the obtained results, e.g., Test Vector Leakage Assessment (TVLA) graphs, minimum traces to disclosure (MTD) graphs, guessing entropy (GE), etc.: **See Fig 1 and Fig 2**.

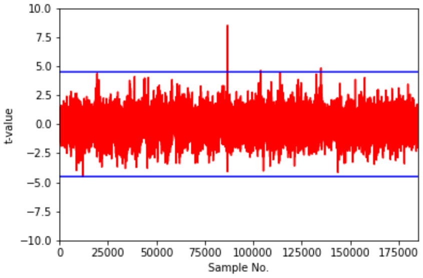

Fig. 1. Unprotected design TVLA results (10,000 traces)

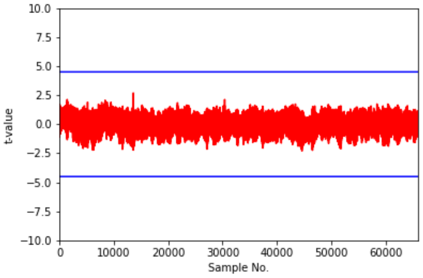

Fig. 2. Unprotected design TVLA results (1 million traces)

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

References

[1] Abubakr Abdulgadir, William Diehl, and Jens-Peter Kaps. "An Open-Source Platform for Evaluation of Hardware Implementations of Lightweight Authenticated Ciphers". In: *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*. Cancun, Mexico: IEEE, Dec. 2019, pp. 1–5. ISBN: 978-1-72811-957-1. DOI: `10.1109/ReConFig48160.2019.8994788`.

[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, 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`.