TVLA On Selected NIST LWC Finalists

Thomas Steinbauer
thomas.steinbauer@student.tugraz.at

Rishub Nagpal
rishub.nagpal@lamarr.at

Robert Primas
robert.primas@iaik.tugraz.at

Stefan Mangard
stefan.mangard@iaik.tugraz.at

August 1, 2022

1 Introduction

We summarize the findings of our SCA Security Evaluation lab on selected NIST Lightweight Cryptography finalist implementations submitted to the "Call for Protected [NIST LWC] Hardware Implementations" [Cry]. For our evaluation, we adopted the TVLA metholodolgy proposed by [SM16] and examined five SCA first-order protected implementations developed by Mueller et. al. [MM]. These implementations were generated with the AGEMA tool [Kni+22] and masked with HPC gadgets [Cas+21].

1.1 Outcomes/Contributions

We performed TVLA with 10 million traces for the selected finalists listed in Table 1. In summary, no detectable leakage was found i.e. the maximum absolute t-score was less than 4.5 for all candidates.

Table 1: Summary of Results. All designs were synthesized for a 1-MHz target clock on an Artix-7 xc7a100t FPGA. Area results for LWC-SCA only includes the CryptoCore and LWC API interface.

Cipher	Reference	Verif. Result	Samples per Trace	Measurement Time	Online Randomness	LUT Area (LWC-SCA)	LUT Area (cw305-top)
Ascon [MM]	ascon128v12	✔	4100	14.76h	320	6143	37978
Elephant [MM]	elephant160v1	✔	55300	29.56h	280	4587	31044
GIFT-COFB [MM]	giftcofb128v1	✔	15500	21.91h	192	3852	28879
Romulus [MM]	romulusn1v1	✔	18000	22.26h	128	2978	27483
Xoodyak [MM]	xoodyakv1	✔	11700	21.81h	384	4551	31143

Table 2: Used Hardware For Test Setup

Type	Name	Reference
Target Board	NewAE CW305 Artix FPGA Target with XC7A100T-2FTG256	NewAE
Oscilloscope	PicoScope 6404C	PicoTech

2 Methodology

2.1 Hardware

Table 2 lists the used hardware to perform the power analysis. The Target Board features a AMD-Xilinx Atrix-7 xc7a100t FPGA which runs the cipher implementation, I/O and trigger logic. All designs were synthesized for a 1-MHz target clock frequency. The PicoScope 6404C oscilloscope runs at 22 MHz sampling rate at 8-bit resolution. Power traces are measured via a single-ended AC-coupled probe set to 100mV/div. The number of gathered samples is dependent on the execution time of the cipher, see Table 1. Figure 1 gives a high-level overview of the evaluation setup.

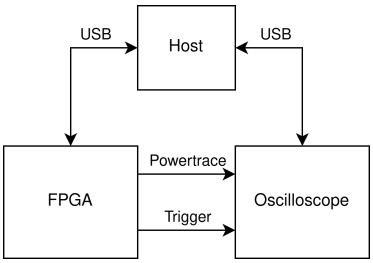

Figure 1: basic overview of test setup

2.2 Software

We created several Python scripts to orchestrate synthesis of bitstreams, TV generation, I/O and updating of the T-test with the help of several third-party tools (summarized in Table 3). The reference implementations for TV generation were taken from SUPERCOP [BL]. Our scripts are optimized to minimize measurement time. We briefly visualize the test flow in Figure 2.

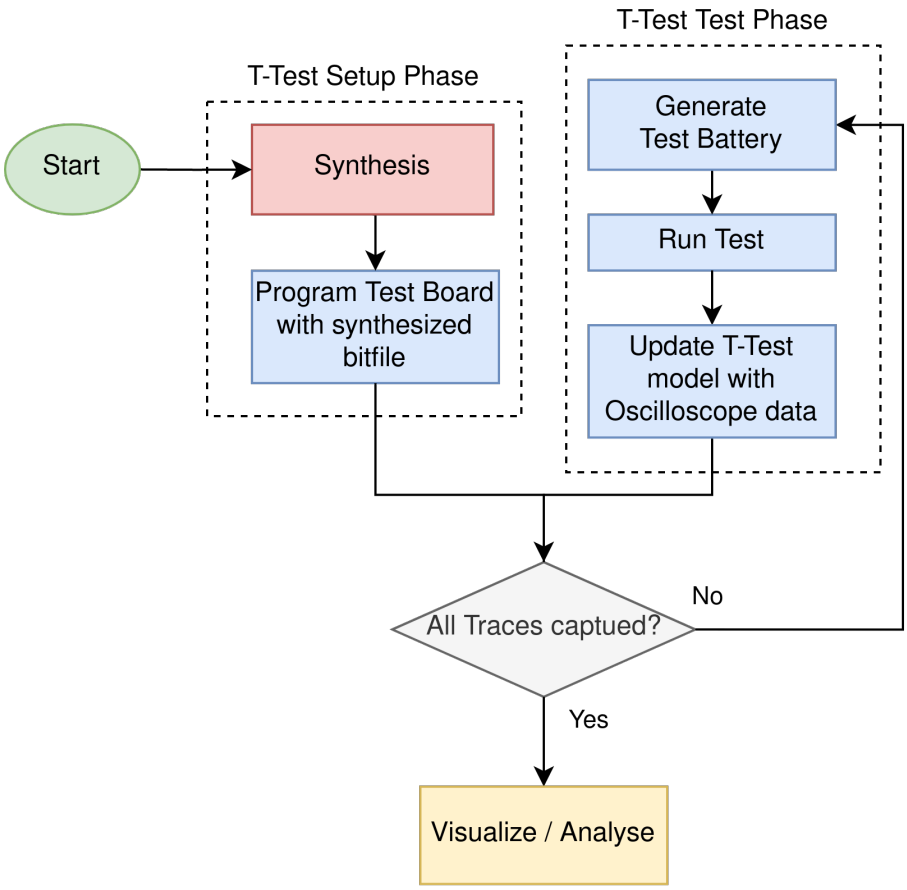

Figure 2: Test Flow Diagram

Hardware Model To decrease the evaluation time, we implemented several hardware optimizations to minimize I/O between the host and FPGA i.e. the identified throughput bottleneck. Figure 3 is an overview of the hardware model used. The FIFOs buffer several hundred encryption blocks and are read in batches by the cipher. Note, no I/O between the host and FPGA is conducted during measurements to minimize power noise. Overall, using FIFO buffers drastically improves evaluation time by several orders of magnitude.

Table 3: Used Software For Test Setup

Type	Name	Version	Reference
Framework Interpreter	Python	3.10.4	python.org
Synthesis Tool	Xilinx Vivado	2021.2	Xilinx
Cipher Software Implementation	SUPERCOP	20220506	bench.cr.yp.to
EDA Automation	Xeda	0.1.0	github.com
Hardware/Software API	LWC Hardware API Development Package	1.2.0	github.com
Simulation Tool	QuestaSim	2020.4	Siemens
Target Board	Chipwisperer	5.6.1	github.com
Oscilloscope SDK	PicoSDK Python Wrapper	1.0	pypi.org
Analysis	SCALib	0.4.2	pypi.org

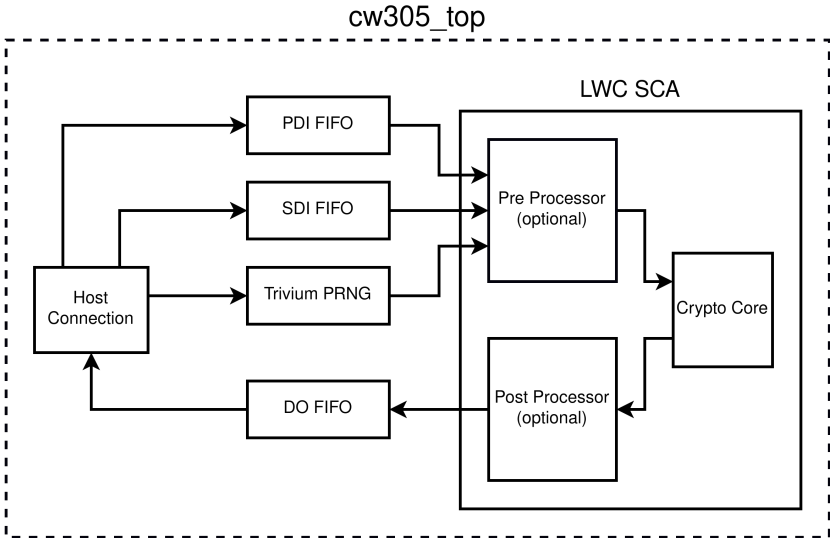

Figure 3: Overview of Hardware Model

Summary of Testing parameters

- First-order masked implementation targets.
- Authenticated Encryption with AD/PT inputs of 1 block length.
- 10 Million fixed vs. random univariate (Welch's) T-test.
- Fixed sets: All PDI inputs are fixed.
- Random sets: All PDI inputs are random.
- In both sets, the key is fixed.
- Execution order of fixed/random TVs is random.
- RNG Source: Trivium [Can06].
- Randomness is generated in parallel with cipher execution.

Randomness For the test series we used a Trivium [Can06] based PRNG implementation [Geo]. The particular implementation generates parallel instances of Trivium and can provide up to 384 bits of randomness from a 768-bit seed. See Table 1 for the amount of randomness required for each implementation.

3 First-Order TVLA Results (10M Traces)

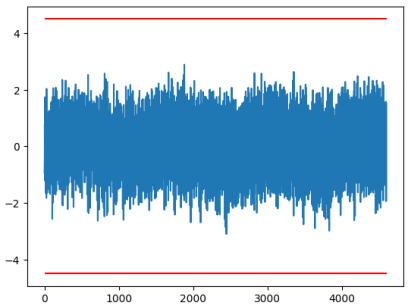

Figure 4: Ascon

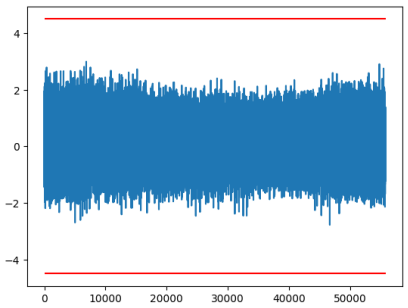

Figure 5: Elephant

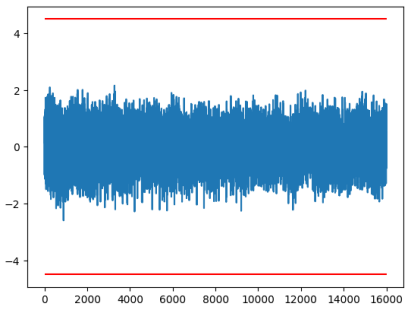

Figure 6: GIFT-COFB

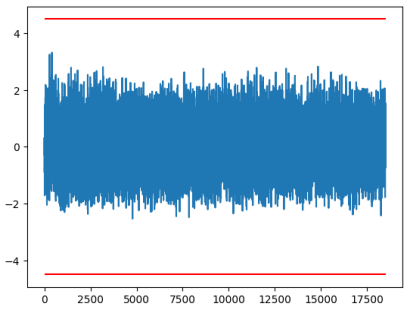

Figure 7: Romulus

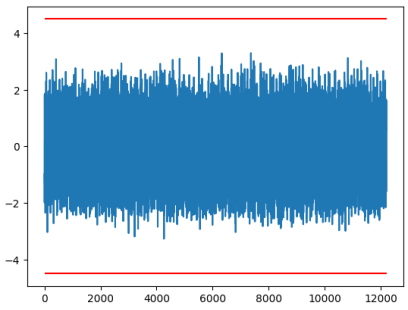

Figure 8: Xoodyak

4 Discussion

The results of our testing are shown in Figure 4, Figure 5, Figure 6, Figure 7, Figure 8. All tested ciphers show T-Test values below 4.5.

5 Conclusion

All tested ciphers passed TVLA on our setup. We plan to continue our measurements for each first-order implementation of the finalist group. We will also integrate new methods to reduce measurement time. For some implementations, the output CT+Tag was incorrect on some test vectors. Once the issue is resolved, we will re-evaluate all implementations and notify designers of any change (if any). We plan to continually refine our evaluations and add results for all NIST LWC finalists.

References

[BL] D.J. Bernstein and T. Lange. *SUPERCOP*. URL: https://bench.cr.yp.to/supercop.html (visited on 07/28/2022).

[Can06] Christophe De Cannière. "Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles". In: *Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings*. Ed. by Sokratis K. Katsikas, Javier López, Michael Backes, Stefanos Gritzalis, and Bart Preneel. Vol. 4176. Lecture Notes in Computer Science. Springer, 2006, pp. 171–186. DOI: 10.1007/11836810_13. URL: https://doi.org/10.1007/11836810%5C_13.

[Cas+21] Gaëtan Cassiers, Benjamin Grégoire, Itamar Levi, and François-Xavier Standaert. "Hardware Private Circuits: From Trivial Composition to Full Verification". In: *IEEE Trans. Computers* 70.10 (2021), pp. 1677–1690. DOI: 10.1109/TC.2020.3022979. URL: https://doi.org/10.1109/TC.2020.3022979.

[Cry] George Mason University Cryptographic Engineering Research Group. *Call for Protected Hardware Implementations*. URL: https://cryptography.gmu.edu/athena/LWC/Call_for_Protected_Hardware_Implementations.pdf.

[Geo] Cryptographic Engineering Research Group at George Mason University. *Hardware implementation of Saber*. URL: https://github.com/GMUCERG/SABER-SCA (visited on 07/28/2022).

[GMK16] Hannes Groß, Stefan Mangard, and Thomas Korak. "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order". In: *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*. Ed. by Begül Bilgin, Svetla Nikova, and Vincent Rijmen. ACM, 2016, p. 3. DOI: 10.1145/2996366.2996426. URL: https://doi.org/10.1145/2996366.2996426.

[Kni+22] David Knichel, Amir Moradi, Nicolai Müller, and Pascal Sasdrich. "Automated Generation of Masked Hardware". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.1 (2022), pp. 589–629. DOI: 10.46586/tches.v2022.i1.589-629. URL: https://doi.org/10.46586/tches.v2022.i1.589-629.

[MM] Nicolai Mueller and Amir Moradi. *LWC Masked Implementations*. URL: https://github.com/Chair-for-Security-Engineering/LWC-Masking/commit/4244b255e282e2d309aa270960bcd5a594c2db03 (visited on 07/28/2022).

[PN] Robert Primas and Rishub Nagpal. *Implementation of Ascon-128 with W=32 and CCW=32, 1st-order DOM, low-register*. URL: https://ascon.iaik.tugraz.at/ (visited on 07/28/2022).

[SM16] Tobias Schneider and Amir Moradi. "Leakage assessment methodology - Extended version". In: *J. Cryptogr. Eng.* 6.2 (2016), pp. 85–99. DOI: 10.1007/s13389-016-0120-y. URL: https://doi.org/10.1007/s13389-016-0120-y.