

Open-Source Framework for Secure Hardware Design with Simulation-based Leakage Assessment

Pablo Navarro-Torrero, Francisco J. Rubio-Barbero, Eros Camacho-Ruiz,
Macarena C. Martinez-Rodriguez and Piedad Brox-Jiménez
Instituto de Microelectrónica de Sevilla (IMSE-CNM), CSIC/US, Seville, Spain

Abstract—Side-channel resilience is a critical requirement for cryptographic accelerators. However, current validation approaches rely heavily on costly, measurement-based testing, which is typically applicable only at the final stages of the design flow. This reliance on physical prototypes is aggravated by the lack of integrated security analysis in fragmented toolchains. To address these challenges, we introduce the HWSEC-OSS Framework, a comprehensive open-source platform designed to streamline the security validation of hardware designs. The framework integrates a complete digital design flow with a pre-silicon Side-Channel Analysis (SCA) module based on Hamming-distance power modeling. We demonstrate the effectiveness of the framework by identifying leakage sources in an EdDSA25519 implementation, exhibiting a strong correlation between simulation-based results and measurements from a physical FPGA prototype. Furthermore, we apply the flow to a hardware implementation of ML-KEM, demonstrating scalability to Post-Quantum Cryptography (PQC). By providing an integrated environment for early security feedback, this work constitutes a fast, cost-effective solution for hardware security validation.

Index Terms—Hardware security, side-channel analysis, design automation, pre-silicon validation, post-quantum cryptography

I. INTRODUCTION

The deployment of cryptographic hardware in security-critical applications renders resistance to Side-Channel Attacks (SCAs) a mandatory design constraint [1]. Attacks such as Differential Power Analysis (DPA) [2] have been successfully demonstrated against a diverse range of devices, necessitating rigorous validation. Traditionally, this validation is performed post-silicon using the Test Vector Leakage Assessment (TVLA) methodology [3]. While accurate, this approach requires costly hardware prototypes and specialized measurement setups [4]. Crucially, validation at this late stage offers limited opportunity for corrective design changes, as resynthesis and refabrication are prohibitively expensive.

These limitations have motivated the development of pre-silicon methodologies. Previous efforts, such as RTL-PSC [5] or RTL-PAC [6], utilize proprietary toolchains to estimate leakage. While academic solutions like VeriSide [7] address simulation speed, they often lack full-flow integration. Bridging platforms like Saidoyoki [8] provide valuable validation testbeds but do not automate the design-to-analysis transition. To the best of our knowledge, no existing solution offers a fully end-to-end, open-source workflow.

This research was supported in part by QUBIP Project with Grant Agreement No. 101119746 under the EU Horizon Europe research and innovation programme.

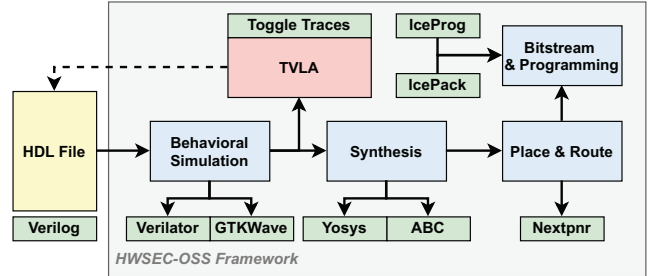


Fig. 1. Design flow of the HWSEC-OSS framework

In this work, we present the **HWSEC-OSS Framework** [9]. Unlike prior point solutions, this framework unifies the entire hardware design stack, integrating front-end simulation, synthesis, and physical implementation with a native side-channel evaluation module. By embedding security validation directly into the design process, our framework enables researchers to assess and mitigate vulnerabilities iteratively prior to silicon fabrication.

II. THE HWSEC-OSS FRAMEWORK ARCHITECTURE

The framework provides a unified, Makefile-driven environment that orchestrates open-source tools to create a complete flow, from RTL to bitstream (Fig. 1).

A. Simulation-Based Leakage Assessment

The framework utilizes **Verilator** [10] for high-performance cycle-accurate simulation. To model power consumption, we employ a Hamming Distance (HD) leakage model. The framework assumes that instantaneous power P_t is proportional to the number of signal toggles between consecutive clock cycles \mathbf{x}_t and \mathbf{x}_{t+1} :

$$P_t \propto \text{HD}(\mathbf{x}_t, \mathbf{x}_{t+1}) = \sum_{i=1}^n \left(x_t^{(i)} \oplus x_{t+1}^{(i)} \right) \quad (1)$$

A custom utility based on [11] processes the simulation VCD files to compute this metric, generating compact toggle traces. These traces are subsequently analyzed using an integrated Jupyter Notebook that applies Welch’s t-test (TVLA) to detect data-dependent leakage.

B. Physical Implementation Flow

The framework includes a complete implementation path. It leverages **Yosys** [12] for synthesis, **Nextpnr** [13] for place-and-route, and **Project IceStorm** [14] for bitstream generation. This guarantees that the code analyzed in the simulation is identical to the physical implementation.

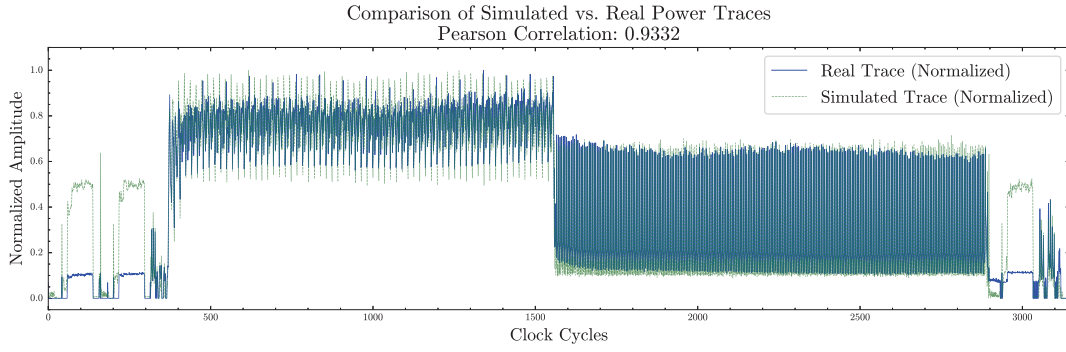


Fig. 2. Comparison of a simulated trace (blue) from HWSEC-OSS and the averaged real power trace (green) from an FPGA for EdDSA25519

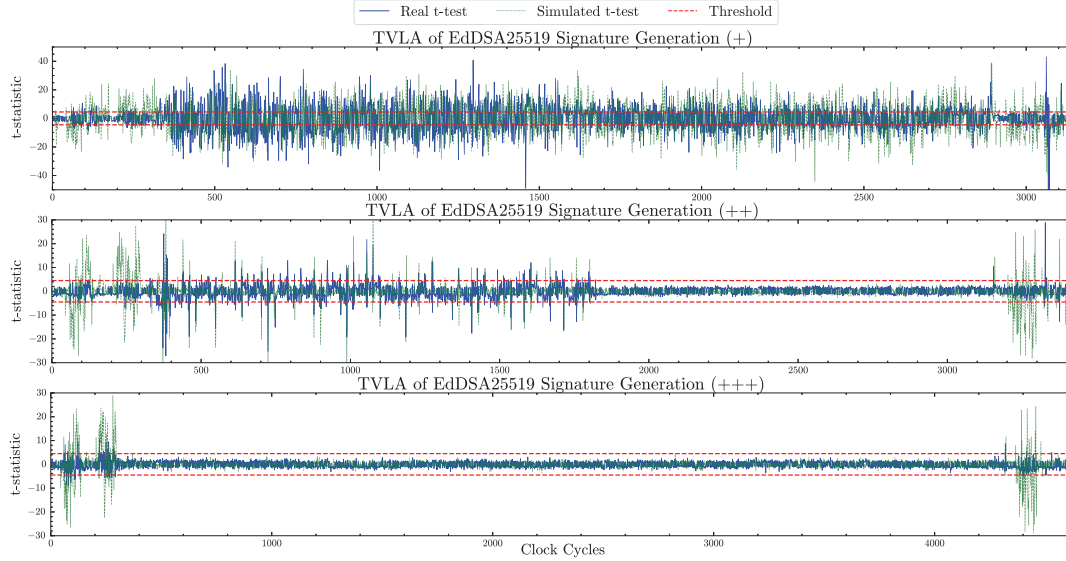


Fig. 3. Comparison of TVLA t-tests on real (green) and simulated (blue) power traces for the three EdDSA25519 security levels

III. EXPERIMENTAL VALIDATION: EDDSA25519

To validate the framework’s predictive capabilities, we conducted a case study on a side-channel protected hardware implementation of EdDSA25519 [15].

We compared the simulation results against physical measurements taken from a SAKURA-X board [16] utilizing a PicoScope 5444D [17]. Fig. 2 illustrates the alignment between the simulated HD trace and the averaged physical power trace. The Pearson correlation coefficient is **0.9332**, indicating a very strong linear relationship. The global shape and operational phases are clearly mirrored in both traces. A notable discrepancy appears in the relative amplitude of the core ECC operations versus the SHA-512 hashes. This occurs because the physical FPGA employs hardened DSP blocks for multiplication which possess a different leakage profile than the generic gates inferred by the simulator. Despite this architectural artifact, the framework successfully models the critical dynamic behavior.

A. Comparative Leakage Assessment

We evaluated three versions of the core with progressive hardening: (+) constant-time, (++) randomized projective coordinates, and (+++) scalar blinding. The simulation results show

a remarkable correspondence with physical reality, see Fig. 3. For the (+) and (++) versions, both methods correctly identify significant leakage. Crucially, regarding the fully hardened (+++) version, the physical evaluation required **one million traces** to reveal residual leakage in the SHA-512 operations due to measurement noise. Remarkably, our simulation-based test identified these exact leakage points with only **2,000 traces**. This superior sensitivity allows subtle, deterministic leakages to be detected early without the noise floor inherent to physical setups.

IV. SCALABILITY AND CONCLUSION

To demonstrate generality, the framework was applied to a hardware accelerator for **ML-KEM** (NIST FIPS 203) [18]. The flow successfully identified leakage during the message decoding phase using 1,000 simulated traces, proving its scalability to complex PQC designs [19].

In summary, the HWSEC-OSS Framework bridges the gap between formal design and empirical validation. By providing an integrated, open-source environment for early security feedback, this work empowers designers to identify and remediate vulnerabilities early, accelerating secure hardware development.

REFERENCES

- [1] M. Tehranipoor and C. Wang, *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.
- [2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.
- [3] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.
- [4] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, 1st ed. Springer Publishing Company, Incorporated, 2010.
- [5] M. He, J. Park, A. Nahiyan, A. Vassilev, Y. Jin, and M. Tehranipoor, "RTL-psc: Automated power side-channel leakage assessment at register-transfer level," in *2019 IEEE 37th VLSI Test Symposium (VTS)*. IEEE, 2019, pp. 1–6.
- [6] N. Pundir, J. Park, F. Farahmandi, and M. Tehranipoor, "Power side-channel leakage assessment framework at register-transfer level," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1207–1218, 2022.
- [7] B. Farnaghinejad, A. Porsia, A. Ruospo, A. Savino, S. Di Carlo, and E. Sanchez, "Late contribution: Veriside: A modified verilator for leakage assessment at the rtl level," in *2025 IEEE 26th Latin American Test Symposium (LATS)*, 2025, pp. 1–2.
- [8] P. Kiaei, Z. Liu, R. K. Eren, Y. Yao, and P. Schaumont, "Saidoyoki: Evaluating side-channel leakage in pre-and post-silicon setting," *Cryptology ePrint Archive*, 2021.
- [9] Pablo Navarro-Torrero, Eros Camacho-Ruiz, "hwsec_oss_framework: Hardware security open source framework," https://github.com/HWSec-CSIC/hwsec_oss_framework, 2025.
- [10] Wilson Snyder, "Verilator," <https://www.veripool.org/verilator/>, (accessed Sep. 13, 2025).
- [11] M.-J. O. Saarinen, "Pre-silicon trace generator for the Adam's Bridge PQC (Dilithium) hardware accelerator from Caliptra 2.0 / Chips Alliance," <https://github.com/ml-dsa/abr-sim>, 2025, accessed: 2025-09-09.
- [12] C. Wolf, J. Glaser, and J. Kepler, "Yosys-a free verilog synthesis suite," in *Proceedings of the 21st Austrian Workshop on Microelectronics (Austrochip)*, 2013, p. 97.
- [13] D. Shah, E. Hung, C. Wolf, S. Bazanski, D. Gisselquist, and M. Milanovic, "Yosys+ nextpnr: an open source framework from verilog to bitstream for commercial fpgas," in *2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. IEEE, 2019, pp. 1–4.
- [14] Clifford Wolf, "Project IceStorm," <https://clifford.at/icestorm>, (accessed Jul. 25, 2025).
- [15] P. Navarro-Torrero, E. Camacho-Ruiz, M. C. Martínez-Rodríguez, and P. Brox-Jiménez, "A side-channel protected and high-performance hardware implementation for eddsa25519," *IEEE Access*, 2025.
- [16] U. S. Lab, "Side-channel attack user reference architecture," <http://sato.h.cs.ucc.ac.jp/SAKURA/index.html>, accessed: 2025-01-05.
- [17] P. Technology, "Picoscope 5444d flexible resolution oscilloscope," <https://www.picotech.com/oscilloscope/5000/flexible-resolution-oscilloscope?kit=5444D>, accessed: 2025-01-05.
- [18] "Module-Lattice-Based Key-Encapsulation Mechanism Standard," National Institute of Standards and Technology, NIST FIPS PUB 203, U.S. Department of Commerce, Aug. 2024.
- [19] Y. Xing and S. Li, "A compact hardware implementation of cca-secure key exchange mechanism crystals-kyber on fpga," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 2, p. 328–356, Feb. 2021. [Online]. Available: <https://tches.iacr.org/index.php/TCHES/article/view/8797>