Abolfazl Sajadi

Digital Hardware Engineer · Hardware Security

a.sajadi@liacs.leidenuniv.nl +31 6 81183983 linkedin.com/in/abisj
abolfazlsajadi.ir Google Scholar Alphen aan den Rijn, The Netherlands

Profile

Digital hardware engineer finishing a PhD in computer science at LIACS, Leiden University, on **hardware security** and digital IC design. On the **PROACT** dual-core RISC-V cryptographic SoC he designed the peripheral RTL (SPI, configurable UART, control/status registers and a PRNG) and integrated the full chip around its **AES, Ascon and Xoodyak** co-processors, first prototyping it on **Xilinx Zynq FPGAs** and then taking it to a **22 nm** ASIC — synthesis in Cadence Genus for GlobalFoundries 22FDX, functional and gate-level verification, and place-and-route and sign-off with the imec team, through to tape-out. He also developed the chip's software stack — C and Python libraries and a control GUI — and its documentation, and designed a ChipWhisperer CW308 target board in Altium with an automated CPA/TVLA side-channel flow. Strongest in the **front-end** (RTL design, synthesis, functional verification), with hands-on **FPGA prototyping**, software and side-channel board experience, looking for a role in **RTL/SoC design, HW/SW co-design, FPGA prototyping, ASIC physical design, or cryptographic hardware**.

Experience

Aug 2022 – Feb 2027 ● ONGOING

Doctoral Researcher — Digital IC & Hardware Security — Leiden University, LIACS · Leiden, NL

- Designed the peripheral RTL — SPI, configurable UART, control/status registers and a PRNG — and integrated the **PROACT dual-core RISC-V cryptographic SoC** around its **AES, Ascon and Xoodyak** co-processors, from RTL to full chip.
- First prototyped and validated the SoC on **Xilinx Zynq FPGAs** (ZYBO, PYNQ-Z2) over SPI/UART, and developed its **software stack** — C and Python libraries, a control GUI, and user documentation.
- Then took the design to a **22 nm ASIC** — synthesized with **Cadence Genus** (GlobalFoundries 22FDX) and ran **functional and gate-level verification** (SDF-annotated **Xcelium** simulation, per-block testbenches).
- Contributed to the **imec back-end** — place-and-route, sign-off and **GDSII**; designed the 28-pin DIL bonding diagram; chip **taped out (MPW)**.
- Built a **ChipWhisperer CW308** target board (Altium) and automated **CPA/TVLA** side-channel evaluation of AES on the RISC-V core.

2018 – 2021

Research Assistant — Embedded Systems (full-time) — University of Tehran, DVD-ES Lab · Tehran, IR

- Designed and evaluated **ML-resistant PUF authentication** protocols (DC-PUF, SQ-PUF) on FPGA; implemented CNN/SVM modeling attacks in Python (published in *J. Network & Computer Applications*).

Selected Projects

Python · PyG

FLASH-Trace — GNN pre-silicon power-trace generation

- A spatiotemporal **Graph Neural Network** (GCN + dilated TCN) that predicts gate-level power traces **up to 9× faster than Cadence Joules**, accurately enough for full **AES-128 key recovery** by CPA.

Open-source

ASSESS — pre-silicon side-channel leakage analysis — ACM CF'26

- A cycle-accurate methodology that localizes **gate-level side-channel leakage** from toggle activity, fast enough for routine checks during iterative **ASIC design**; benchmarked against RTL-PAT, PATCH and ACA on RISC-V/AES designs.

Vivado HLS

Real-time object detection & tracking on Zynq-7000 — B.Sc. thesis

- HW/SW co-design on an ARM+FPGA SoC: HDMI video in, filtering/tracking synthesized via **High-Level Synthesis**, output over VGA/UART.

Cyclone II

CNN accelerator on FPGA — RTL / Quartus

- RTL implementation of a convolutional-network accelerator, validated against a Keras reference model and brought up on an Altera Cyclone II board.

Verilog · VHDL

Hand-written RTL building blocks

- RTL implementations of a simple CPU, an FIR filter and a VGA controller — all hand-written in HDL.

ESP32 · AVR **Home meter monitoring device** Altium · 2020

- Embedded design on ESP32 and AVR (ATmega8) microcontrollers, with a custom PCB designed in Altium Designer.

Education

Aug 2022 – Feb 2027 **Ph.D. in Computer Science** Leiden University (LIACS) · Leiden, NL

ONGOING

Hardware security & digital IC design (PROACT). Dissertation: pre/post-silicon side-channel leakage evaluation in lightweight cryptographic circuits.

2018 – 2021 **M.Sc. in Electrical Engineering — Digital Electronic Systems** University of Tehran · GPA 18.28/20

Ranked 1st in class. Thesis: ML-based modeling attacks on Physical Unclonable Functions (PUFs).

2014 – 2017 **B.Sc. in Electrical Engineering — Electronic Technology** Mohajer Technical University (MTU) · GPA 16.87/20

Top of class. Thesis: real-time object detection & tracking on a Zynq-7000 SoC.

Selected Publications

- **A. Sajadi**, N. Zidarič, T. Stefanov, N. Mentens. *Systematic Comparison and Improvement of Pre-silicon Leakage Analysis Tools.* ACM Computing Frontiers (CF Companion '26), 2026. [doi]
- **A. Sajadi**, N. Zidarič, T. Stefanov, N. Mentens. *A Systematic Comparison of Side-channel Countermeasures for RISC-V-based SoCs.* IEEE NorCAS, 2024. [doi]
- **A. Sajadi**, S. Shiri, N. Zidarič, T. Stefanov, N. Mentens. *FLASH-Trace: Fast & Learning-based Pre-Silicon Power Trace Generation with GNNs.* Under submission, IACR TCHES.
- **A. Sajadi**, A. Shabani, B. Alizadeh. *DC-PUF: ML-Resistant PUF-Based Authentication for Resource-Constrained IoT.* J. Network & Computer Applications, vol. 217, 2023. [doi]
- A. Adhikary *et al.* (incl. **A. Sajadi**). *PROACT — Physical Attack Resistance of Cryptographic Algorithms and Circuits with Reduced Time to Market.* Applied Reconfigurable Computing (ARC), LNCS, Springer, 2024. [doi]
- J. Anders *et al.* (incl. **A. Sajadi**). *A Survey of Developments in Testability, Safety and Security of RISC-V Processors.* IEEE ETS, 2023. [doi]

Technical Skills

Hardware Languages	VHDL, Verilog, SystemVerilog, Verilog-A, High-Level Synthesis (HLS)
Programming	Python, C/C++, Tcl (EDA scripting)
ASIC Front-End	RTL design, RISC-V (Ibex) integration, logic synthesis (Cadence Genus), SDC constraints, STA, gate-level simulation
Back-End	Place-and-route, sign-off, GDSII, bonding diagram, GlobalFoundries 22FDX *(contributed, with imec)*
Verification	Functional & coverage-driven verification (CDV), testbench development, gate-level simulation (Cadence Xcelium), FPGA validation, hardware debug
FPGA & Embedded	Xilinx Zynq-7000 (ZYBO, PYNQ-Z2), Vivado & Vivado HLS, Catapult HLS, SPI/UART, ESP32, AVR
Hardware Security	CPA, DPA, TVLA, SNR/NICV, ChipWhisperer, pre-silicon leakage analysis, PUFs
Design Methods	HW/SW co-design, continuous integration (CI), test & testability design (DfT), fault-tolerant system design
ML & EDA	PyTorch, PyTorch Geometric (GNN/TCN), Keras; Cadence (Genus, Joules, Xcelium), Altium, MATLAB

Teaching, Supervision & Activities

- **Teaching Assistant**, *System & Software Security*, Leiden University (2022–present); **co-supervised 6+ B.Sc. theses** on AES/RISC-V side-channel analysis and chip-prototype leakage assessment.
- **Reviewer**, *IEEE Trans. Computer-Aided Design (TCAD)*; **Cadence certified** — RTL-to-GDSII Flow, Genus Physical Synthesis, Tcl for EDA (2024–25).
- **Summer schools**: CPS Summer School 2023 (Sardinia); Real-World Crypto & Privacy 2023; PROACT Hardware-Security Training Schools (2023, 2025).

Honors & Languages

- **Honors**: Ranked 102nd of 30,000+ in Iran's national M.Sc. entrance exam; 1st place, provincial WorldSkills electronics competition (2013).
- **Languages**: Persian (native) · English (professional working) · Dutch (A2).