Rogerio Paludo

rogeriopaludo.com

✉: rogeriopld@gmail.com
✆: +971 58 276 2152

Experience

- **Infineon Technologies** — Munich, Germany
  Formal Security Verification Engineer – CSS Division — May 2025 – Present
  - Formal Verification: Performing formal security verification of protected cryptographic implementations within the CSS division.
- **Technology Innovation Institute** — Abu Dhabi, UAE
  Lead Hardware Engineer (R&D) – Cryptography Research Center — Jan. 2023 – Present
  - Research: Designed high-bandwidth FPGA accelerators for privacy-preserving machine learning, efficiently utilizing PCIe and HBM2.0. Led architecture, implementation, verification, validation, and software stack integration.
  - Development: Developed national-security–grade cryptographic hardware covering asymmetric (ECDSA, ECDH), symmetric (FIPS 202–SHA3), and post-quantum cryptography (PQC).
- **Crypto Quantique** — London, UK
  Frontend ASIC and FPGA Design Engineer – Contract/Remote — Aug. 2022 – Nov. 2022
  - Physical-Unclonable Functions (PUF): Designed interface controllers and error-correction logic for a mixed-signal PUF system. Fully responsible for the digital frontend architecture, RTL implementation, and verification of multiple test-chip tape-outs.
- **Astrolight** — Vilnius, Lithuania
  Research Consultant – Contract/Remote — Jun. 2022 – Aug. 2022
  - FPGA Testbed for Satellite Communications: Conducted early-stage research and FPGA implementation of satellite communication modulation schemes, contributing to system-level architectural decisions and experimental validation.
- **Altran / Capgemini Engineering** — Lisbon, Portugal
  FPGA R&D Engineer – Contract — Feb. 2022 – Aug. 2022
  - Quantum-Key Distribution (QKD): Developed the physical-layer FPGA design for a QKD proof-of-concept system, overseeing architecture, implementation, verification, and integration of all FPGA-related components.
- **INESC-ID** — Lisbon, Portugal
  Post-doctoral Researcher – Contract/Scholarship — Mar. 2020 – Jan. 2022
  - Research: Designed efficient NTT accelerators for fully homomorphic encryption; extended a Linux-ready RISC-V processor with custom FHE instruction-set extensions and full GCC compiler support. Nominated for Best Paper Award at ASAP 2021.
  - European Projects: Contributed to FutureTPM and the European Processor Initiative (EPI), developing a quantum-resistant TPM 2.0 emulator and an efficient lattice-based autonomous attestation scheme aligned with emerging European secure-processor ecosystems.

Education

- **Federal University of Santa Catarina** — Florianopolis, Brazil
  PhD in Electrical Engineering; GPA: (9.7/10) — Mar. 2016 – Mar. 2020
  - PhD Thesis: Developed efficient arithmetic circuits using alternative forms of numeric representation for high-performance digital signal processing and cryptography systems.
- **Federal University of Santa Catarina** — Florianopolis, Brazil
  Masters in Electrical Engineering; GPA: (9.6/10) — Mar. 2014 – Mar. 2016
  - Master Thesis: Developed a framework for early semi-formal verification of mission-critical embedded software in the Master Thesis. Used the https://floripasat.ufsc.br/ as a study case.

Skills

- Working Knowledge: Cadence: Xcelium, JasperGold, Genus, and Innovus; Synopsys: VCS and DesignCompiler; Siemens: Questa and Visualizer; Xilinx: Vivado and Vitis; Intel: Quartus; Operating Systems: Windows/Linux; CI/CD Jenkins and GitLab Pipelines.
- Languages: HDLs and Verification: VHDL, Verilog, SystemVerilog, SystemVerilog Assertions, SystemC (arch. modeling); Programming/Scripting: Bash, Makefiles/CMake, TCL, Perl, Python, C, ASM x86, ASM RISC-V, Matlab, SageMath.