Rogerio Paludo

rogeriopaludo.com

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

Experience

- **Technology Innovation Institute** — Abu Dhabi, UAE
  Lead Hardware Engineer (R&D) – Cryptography Research Center — Jan. 2023 – Present
  - **Research:** Designing FPGA accelerators for privacy-preserving machine learning taking advantage of maximum PCIe and HBM2.0 bandwidth. Responsible for architecture, implementation, verification, validation, and, integration of the accelerators into the software stack.
  - **Development:** Working at the national security level developing cryptographic hardware for i) asymmetric cryptography (ECDSA & ECDH); ii) symmetric cryptography (FIPS202–SHA3); iii) post-quantum cryptography (PQC). Complete ownership of high-assurance PQC key-encapsulation (FIPS203) and digital signatures (FIPS204) implementations - from architecture specifications, formal verification, validation over the board, to final delivery to clients.
- **Crypto Quantique** — London, UK
  Frontend ASIC and FPGA Design Engineer – Contract/Remote — Aug. 2022 – Nov. 2022
  - **Physical-Unclonable Functions (PUF):** Worked on the interface controller and error correction codes for a mixed-signal PUF. Responsible for all the digital frontend design of the test chips.
- **Astrolight** — Vilnius, Lithuania
  Research Consultant – Contract/Remote — Jun. 2022 – Aug. 2022
  - **FPGA testbed for satellite communications:** Conducted early-stage research and implementation of the modulation system.
- **Altran/Capgemini Engineering** — Lisbon, Portugal
  FPGA R&D Engineer – Contract — Feb. 2022 – Aug. 2022
  - **Quantum-key Distribution (QKD):** Worked on the development of the physical layer for a QKD proof-of-concept system, overseeing all technical aspects related to FPGA design.
- **INESC-ID** — Lisbon, Portugal
  Post-doctoral Researcher – Contract/Scholarship — Mar. 2020 – Jan. 2022
  - **Research:** Efficient Number-Theoretic Transform implementations for Fully-Homomorphic Encryption. Extended a linux-ready customized RISC-V processor for FHE acceleration - full-stack work from novel accelerator to full instruction-set extension in the GCC compiler. Nominated for best paper award in the ASAP2021 conference.
  - **European Projects:** Worked on the FutureTPM and EPI projects. The bulk of the work was to develop a quantum-resistant TPM2.0 emulator and an efficient lattice-based direct autonomous attestation implementation based on the TPM2.0.

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. Implemented a framework for design automation of the specialized arithmetic circuits targeting applications in digital signal processing and cryptography.
- **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. Participated in a R&D project with Freescale Semiconductors for the design of a mixed-signal verification library used in the tapeout of a power-management IP.

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.