ANDRÉ BARBOSA

ASIC Digital Design Engineer · Embedded Systems & Hardware Security

theandrebarbosa@gmail.com · +351 915 274 575 · Porto, PT
linkedin.com/in/andre3barbosa · github.com/andre3barbosa

SUMMARY

ASIC Digital Design Engineer at Synopsys, working on the HDMI/DisplayPort IP RTL implementation team. MSc in Electrical and Computer Engineering (University of Minho) with a research focus on software-based microarchitectural side-channel attacks against MCUs. Experienced across the digital design flow — RTL design, simulation/debug, synthesis, and lint/CDC — and bring a hardware-security mindset shaped by cryptographic and embedded-systems research.

EXPERIENCE

ASIC Digital Design Engineer — Synopsys Dec 2024 – Present

HDMI/DisplayPort IP RTL Implementation team

- Design, implement, and debug RTL in Verilog/SystemVerilog for high-speed connectivity IP: micro-architecture, RTL, simulation/debug, synthesis, and lint/CDC sign-off.
- Contributed to automotive safety-related RTL development for UFS4 IP under ISO 26262-compliant design practices, working to functional-safety requirements.
- Work daily with industry-standard EDA flows (VCS, Verdi, Design Compiler/Fusion Compiler, SpyGlass, Formality) in a Linux/Perforce/Jira environment.

Earlier as a Summer Intern (Jul – Sep 2023): developed a DisplayPort video-packetization RTL module.

Researcher — neXt Sense (Safety Connected and Automated Vehicles) Jan 2024 – Nov 2024

- Investigated side-channel attacks against automotive sensors and identified realistic threat models for connected/automated vehicles.

EDUCATION

MSc, Electrical and Computer Engineering — University of Minho Sep 2022 – Jun 2024

Specialization: Embedded Systems and Computers

Thesis: *Multi-Run Software-Based Microarchitectural Side-Channel Attacks Against MCUs* — practical software-based side-channel attacks against cryptographic routines on ARM Cortex-M IoT devices.

BSc, Electrical and Computer Engineering — University of Minho Sep 2019 – Jun 2022

SELECTED RESEARCH & PROJECTS

WiP Paper: BUSted Second Stop! A First Step for Breaking Cryptographic Applications on MCU-based IoT Devices ***(EWSN'24 Paper)***

Software-based side-channel attacks against cryptographic implementations on ARM Cortex-M IoT devices, exploiting microarchitectural leakage to recover secrets without physical access.

Twofish IP on FPGA SoC

Hardware implementation of the Twofish cryptographic algorithm in a FPGA SoC, balancing performance, area, and resilience against known vulnerabilities.

8051 Assisted Computer System (FPGA SoC)

Pipelined 8051 SoC in Verilog with a custom acceleration module for image processing, plus VGA and PS/2 controllers in a FPGA.

Driver Drowsiness Detection (D3)

Embedded computer-vision system on Raspberry Pi using multi-threaded ML for real-time drowsiness detection, with a companion mobile app and database.

SKILLS

- **Hardware Design** — RTL design, Verilog, SystemVerilog, FPGA prototyping, ASIC flow, uArch
- **Verification** — SystemVerilog testbenches, functional coverage, familiarity with UVM methodologies
- **EDA/Synopsys Tools** — VCS, Verdi, Design Compiler, Fusion Compiler, SpyGlass (lint/CDC), Formality
- **FPGA Tools** — Xilinx Vivado, Vitis
- **Hardware Security** — Side-channel analysis, cryptographic IP, MCU threat modeling, ARM Cortex-M security
- **Embedded Systems** — ARM Cortex-M, STM32, RTOS, low-level systems programming
- **Software** — C, C++, Assembly, Python, bash
- **Workflow** — Linux, Git, Perforce, Jira

LANGUAGES & EXTRACURRICULAR

Portuguese — Native · **English** — Fluent

Roller hockey player (15 years) · Half-marathon runner