Athanasios Moschos

amoschos3@gatech.edu
https://0ena.github.io

SHORT SKILL SET AND RESEARCH INTRODUCTION

I am implementing different open-source RISC-V micro-architectures either through FPGA prototyping (Xilinx/AMD FPGAs) or as ready for tape-out ASIC blocks, to examine their susceptibility to hardware trojan attacks. My concrete understanding of CPU architectures allows me to perform modifications in the original RTL code or design custom add-on modules, while maintaining the native design functionality and performance metrics. To evaluate the performance impact of RTL modifications in the physical implementation of the design, I have created a fully automated RTL-to-GDII flow for synthesis and physical implementation of complex RTL designs. I have experience with C/C++, Python and Matlab programming, as I have employed them both in industry and research projects. During my Masters, I have taken relevant coursework in advanced computer architecture and memory technologies, where I designed simulators in C/C++ for cache memories, branch predictors, FOCO architecture (Tomasulo's algorithm) and cache coherence protocols. I also employ Sed/AWK/Python scripting for the processing and analysis of large database files (e.g., core/memory dumps, ASIC netlists). Lastly, I have setup and maintain my own Linux servers with a variety of industry EDA tools (Cadence, Synonpsys, Mentor) necessary for my research.

EDUCATION

Ph.D. in Electrical and Computer Engineering — January 2020 - Present
Georgia Institute of Technology, COEUS Center — Atlanta, GA
Advisor: Dr. Angelos Keromytis

M.S. in Electrical and Computer Engineering — December 2021
Georgia Institute of Technology — Atlanta, GA

Diploma in Electrical and Computer Engineering (B.Eng. & M.Eng.) — July 2017
University of Patras, VLSI Design Laboratory — Patras, Greece
Advisors: Dr. Odysseas Koufopavlou and Dr. Apostolos Fournaris

SKILL SET

EDA Tools: Vivado, Genus/Innovus/Tempus, VCS, Questasim, Virtuoso, LEC, Spectre
Programming: System Verilog, VHDL, Python, C/C++, Matlab, TCL, Assembly, Sed/Awk, Bazel
Engineering: FPGA prototyping, measurements with oscilloscopes, spectrum analyzers and EM probes. Linux servers & EDA tools setup and management.
Languages: Greek, English and German.

PROFESSIONAL EXPERIENCE

CPU Design Verification Engineer - RISCV Team — May 2024 - December 2024
Tenstorrent — Austin, Texas

- Identified simulation bottlenecks caused by the RTL or the design verification logic in RISCV HPC uArchs, using VCS profiler and Linux Perf for Verilator. Performed optimizations that led to significant reductions in simulation time (up to 14%), across different test-benches and uArch modules, thus lowering the simulation licensing costs. Automated through scripting the discovery of commits in the RTL codebase that throttle simulation performance.
- Reduced ZeBu server's resource utilization to increase emulation capacity. In particular, I performed optimizations in the RTL and C++ API of the Performance Monitor Unit (PMU) used in HPC uArchs, that led to a 40% reduction in the utilization of FPGA resources related to waveform capturing. The optimizations enable dynamic reconfiguration of the PMU's performance counter widths, depending on the needs of the verification team.
- Worked on establishing the infrastructure for gate-level simulations of RISC-V HPC uArchs. Reconfigured and enhanced the existing Bazel-based automation framework, to strip the test-bench platform from DV related logic (e.g., XMRs) and allow execution of verification testing on the bare DUT. The enhanced features provided plug-n-play capabilities, where the RTL logic of the DUT could be swapped with the DUT's gate-level netlist.

Mixed-Signal/Digital IC Design Engineer April 2018 - December 2019
weasic Microelectronics Athens, Greece

- Participation in **5 first pass silicon success** tape-outs of RF/mixed-signal chips as a Digital IC Design Engineer and Analog Layout Engineer.
- Established the Company's first RTL-to-GDSII digital design flow and implemented the front-end and back-end of various digital blocks (including a 32-bit RISC-V microarchitecture) used in the Company's products .
- Performed layout in different technology processes (55nm SiGE BiCMOS, 45nm GF RF-SOI, 22nm GF FD-SOI) on top-chips, individual analog blocks and custom cells used in the digital design flow. My ability in solving fast DRC and LVS errors in complex top-chip/analog layouts enabled the Company to meet all of its tight tape-out deadlines.
- Digital front-end/back-end experience: RTL coding, design synthesis, floor planning, power planning, place and route, clock tree synthesis, static timing analysis (STA), sign-off timings, physical verification, equivalence checking, ECOs.
- Created Sed and Awk scripts to adjust the gate-level netlists of mixed-signal top-chip blocks, to fit the client's digital-on-top flow for functional testing/simulations.

Embedded Systems Software Engineer November 2017 - April 2018
TELETEL S.A. Athens, Greece

- Co-leading a small team instructed with the implementation of a testing-suite for the validation of the Xtratum hypervisor on the LEON3 microprocessor. The project was funded by the European Space Agency [media].
- Implementation of software modules in C and C++ that facilitated the communication between the XtratuM hypervisor and a custom-made Python testing-suite.
- Acquired experience in the implementation of uni-tests for the validation of software modules running on the SPARC-V8 architecture.

RESEARCH EXPERIENCE

Graduate Research Assistant January 2020 - Present
Georgia Institute of Technology Atlanta, GA

My research interests lie in the fields of hardware trojans and side-channel analysis. More specifically, I am interested in the discovery of weaknesses inherent in complex IC designs (i.e. RISC-V, x86 microarchitectures) that enable the insertion of malicious functionalities (hardware trojans) or the extraction of sensitive information through side-channels.

I utilize Linux-capable, 64-bit RISC-V microarchitectures as my test-bed for the creation and testing of hardware trojan attacks (e.g., denial of service, unauthorized access of privileged memory sections). Through FPGA prototyping (on Xilinx/AMD Kintex-7 chips), I test the effectiveness of different trojan functionalities and examine the interaction between the hardware trojans and the OS. Moreover, I collect side-channel measurements during the CPU's operation to evaluate the stealthiness characteristics of the trojan implementations. Using TSMC's 28nm HPC+ process I have implemented the digital front-end and back-end of different RISC-V microarchitectures. I use the finalized sign-off microprocessor layouts to examine the susceptibility of complex ICs to the insertion of hardware trojans inside foundries.

Parallel to the above, under the guidance of Professor Daniel Genkin, I investigated the susceptibility of Intel's AES-NI x86 instruction set extension to side-channel attacks and especially to correlation power analysis (CPA) attacks. I created signal processing scripts for pattern recognition, extraction and alignment, as well as filtering, denoising and discartion of measurements. Moreover, I performed CPA attacks on post-processed measurements of AES-NI encryption operations and successfully recovered the encryption keys.

I look forward for my research to enhance our understanding of hardware vulnerabilities in modern silicon solutions and help protect the chips' life cycle and supply chains.

Diploma Thesis Researcher June 2015 - April 2017
University of Patras Patras, Greece

I conducted research on side-channel attacks and cryptanalysis methods (e.g. CPA) to evaluate the protections of several hardware security modules. I designed and implemented a digital controller IP (FPGA prototyping on Xilinx/AMD Spartan-6 chips) that enabled very fast collection of electromagnetic power measurements from different cryptographic modules implemented inside FPGAs. The digital controller is parametric and can be easily reconfigured during compile time to accommodate a variety of cryptographic modules. I used the collected measurements to evaluate the side-channel resistance of several cryptographic modules. Part of my Diploma Thesis led to 3 publications.

TEACHING

Graduate Teaching Assistant, Georgia Institute of Technology
ECE 4115: Introduction to Computer Security Spring & Fall 2021
Preparing the lab exercises, grading and holding students' office hours.

HONORS & AWARDS

Young DAC Fellow *fellowship from the 61st DAC Conference* June 2024

CSAW Finalist *- AI Hardware Attack Challenge* *November 2023*
Advanced in the final round of the competition with an AI-generated hardware trojan design crafted for a Linux-capable RISC-V microarchitecture.

Young DAC Fellow *fellowship from the 60th DAC Conference* July 2023

Acknowledgment *from the 32nd EUROCRYPT Conference* May 2013
One of the team members helping organizing Eurocrypt 2013 Conference in Athens, Greece.

Travel Grants
DAC 2023/2024, CSAW 2023, CHES 2022, EUROCRYPT 2014/2015

PUBLICATIONS

1. A. Moschos, F. N. Monrose, A. D. Keromytis,"Towards Practical Fabrication Stage Attacks Using Interrupt-Resilient Hardware Trojans", 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2024.
2. G. Kokolakis, A. Moschos, A. D. Keromytis, "Harnessing the Power of LLMs in Hardware Trojan Design", 2024 Artificial Intelligence in Hardware Security, Applied Cryptography and Network Security Workshops (ACNS), 2024.
3. A. Moschos, K. Valakuzhy, A. D. Keromytis, "On the Feasibility of Remotely Triggered Automotive Hardware Trojans", 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2022, [media1] [media2].
4. A. Fournaris, A. Moschos, N. Sklavos, "Side Channel Assessment Platforms and Tools for Ubiquitous Systems", In: Avoine G., Hernandez-Castro J. (eds) Security of Ubiquitous Computing Systems, 2021, Springer, Cham. https://doi.org/10.1007/978-3-030-10591-4_9
5. A. Fournaris, Charalambos Dimopoulos, A. Moschos, O. Koufopavlou. "Design and leakage assessment of side channel attack resistant binary edwards Elliptic Curve digital signature algorithm architectures", Microprocessors and Microsystems 64: 73-87, 2019.1
6. A. Moschos, A. Fournaris, O. Koufopavlou, "A flexible leakage trace collection setup for arbitrary cryptographic IP cores", 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST): 138-142, 2018.

POSTERS

1. A. Moschos, A. D. Keromytis, "Considering the Future of Hardware Trojan Attacks", DAC Young Fellows Poster Session - 60th Design Automation Conference (DAC), 2023.
2. A. Moschos, A. D. Keromytis, "The Design and Implementation of an Open-Source Hardware Trojan for a 64-bit RISC-V CPU Design", Poster Session - IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), 2022.

SERVICE

U.S. Open-Source Software Security Initiative Workshop August 2022
Scribe for the "Memory-Safe Language Adoption in OSS" session.

INVITED TALKS

Athecrypt 2018 January 2018
Talk on "Automated Functional Validation and Security Evaluation Setup for Arbitrary Cryptographic IP cores".

ADDITIONAL SCHOOLS & TRAINING

TRUDEVICE 2014 July 2014
Training School on Trustworthy Manufacturing and Utilization of Secure Devices in Lisbon, Portugal.

EXTRA-CURRICULAR ACTIVITIES

Sailing 2015 - Present

I hold a Skipper's license since 2015 and I have been involved in yacht racing with large keel boats (35ft–40ft).

Free-diving 2019 - Present

I hold a free-diving 1st level certification (depths up to 18m) from the Greek Diving Association and I enjoy spearfishing.