Ognjen **Glamočanin**

COMPUTER SCIENCE PH.D. GRADUATE

☎ (+41) 078-948-15-35 | ✉ o.glamocanin@gmail.com | OgacNS94

Education

EPFL, Ecole Polytechnique Fédérale de Lausanne — *Lausanne, Switzerland*

PH.D. IN COMPUTER SCIENCE — ***Graduated: August 2023***

- Thesis: Evaluating, Exploiting, and Hiding Power Side-Channel Leakage of Remote FPGAs
- Research focus: FPGA security and power side-channel attacks, cloud FPGAs, and multi-tenant FPGAs
- Thesis advisors: Dr. Mirjana Stojilović and Prof. Babak Falsafi
- Relevant experience: RTL design and verification, FPGA design, C/C++, Python for ML (Pandas, Keras, WandB), scripting, power analysis

Sorbonne Université, Paris VI — *Paris, France*

M.S. IN COMPUTER SCIENCE — *2017 – 2018*

University of Novi Sad, Faculty of Technical Sciences — *Novi Sad, Serbia*

B.S. WITH HONOURS IN ELECTRICAL ENGINEERING — *2013 – 2017*

Work Experience

Synthara AG — *Zurich, Switzerland*

HARDWARE ENGINEER — *Sep 2023 – ongoing*

- Integrating Synthara's ComputeRAM™ in-memory computation IP into future generations of edge devices and SoCs.
- Used **SystemVerilog** to design and integrate AXI4-Full router, allowing maximal throughput communication a source and multiple destinations.
- **Verification lead** for the ComputeRAM™ IP, used **SystemVerilog** and **UVM** to build an object-oriented functional verification environment.

ARM — *Sophia Antipolis, France*

CPU MICROARCHITECTURE AND DESIGN INTERN — *Mar 2018 – Aug 2018*

- Analyzed CPU microarchitectural events for the purposes of **power consumption estimation** during cycle-accurate simulation.
- Used **Python sklearn** to model the correlation between CPU events and power consumption simulated in **Cadence Joules**.
- Enabled power estimation in early microarchitecture design stages by integrating power prediction in a **C/C++** cycle-accurate simulator.

FROBAS D.O.O. — *Novi Sad, Serbia*

MACHINE LEARNING HARDWARE ACCELERATION INTERN — *Nov 2016 – Jun 2017*

- Used **VHDL** to design and verify a hardware accelerator for multi-layer perceptron (MLP) artificial neural networks (ANNs).

ELSYS EASTERN EUROPE — *Belgrade, Serbia*

HARDWARE FUNCTIONAL VERIFICATION INTERN — *Jul 2016 – Oct 2016*

- Used **SystemVerilog** and the **UVM** methodology to build a functional verification environment for an OCP2UART bridge.

Technical Skills

Digital design and FPGA development:	RTL design, FPGA design (AMD 7-series, UltraScale+ in Alveo boards), RTL verification (UVM)
Programming and scripting languages:	C/C++ (10yrs), Python (6yrs), SystemVerilog (3 years), Bash (8yrs), TCL(8yrs)
Hardware description languages:	VHDL (9yrs), Verilog (5 years), SystemVerilog (3 years), SystemC
CAD EDA tools:	Xilinx ISE, Vivado, and Vitis, QuestaSim, Cadence Xcelium, Synopsys VCS
ML tools:	Python (Keras, TensorFlow, Weights and Biases, Pandas), Docker, Kubernetes
Cloud frameworks:	AWS EC2, Microsoft Azure, Google Cloud, CoreWeave

Publications

Instruction-Level Power Leakage Evaluation of Soft-Core CPUs on Shared FPGAs — *HaSS*

O. GLAMOČANIN, S. SHRIVASTAVA, J. YAO, N. ARDO, M. PAYER, M. STOJILOVIĆ — *2023*

- Evaluated the instruction-level power leakage of **RISC-V softcore CPUs** in shared FPGAs using deep learning techniques in **Python Keras**.
- Used **Python WandB**, **Bash**, **Docker**, and **Kubernetes** to streamline and automate the training and exploration of ML model hyperparameters.
- Evaluated of the impact of the **FPGA** family, code template structure, preprocessing, and trace averaging on the model accuracy.

Active Wire Fences for Multi-Tenant FPGAs (Best Paper Award Nomination) — *DDECS*

O. GLAMOČANIN, A. KOSTIĆ, S. KOSTIĆ, M. STOJILOVIĆ — *2023*

- Created a novel wire-based **FPGA** power waster architecture using **VHDL** and **XDC**, with no resource overhead compared to the state of the art.
- Deployed a **CUDA**-accelerated power analysis attack on CoreWeave cloud instances with Nvidia A100-80GB GPUs.
- Demonstrated that wire wasters, when used as active fences, outperform the state of the art against remote power analysis attacks.

RDS: FPGA Routing Delay Sensors for Effective Remote Power Analysis Attacks

TCHES

D. Spielmann*, **O. Glamočanin***, M. Stojilović (* equal contribution) *2023*

- Designed a novel routing-based FPGA voltage sensor architecture using **VHDL** and **Vivado**, with superior sensing than the state of the art.
- Designed an AXI4-Full **Vitis RTL kernel** for the **Alveo U200 FPGA card**, used for recording and saving encryption power traces.
- Implemented a **C++** interface for the RTL kernel to record millions of power traces and a **Bash** script to automate the trace collection process.

Temperature Impact on Remote Power Side-Channel Attacks on Shared FPGAs

DATE

O. Glamočanin, H. Bazaz, M. Payer, M. Stojilović *2023*

- Analyzed the temperature impact on **FPGA** voltage sensors and remote power analysis attacks.
- Quantified the impact of temperature effects on statistical (CPA on AES encryption) and ML profiling power analysis attacks.

The Side-Channel Metrics Cheat Sheet

CSUR

K. Papagiannopoulos*, **O. Glamočanin***, M. Azouaoui*, D. Ros*, F. Regazzoni*, M. Stojilović* (* equal contribution) *2022*

- Analyzed and compared methods for power side-channel security evaluation, both theoretically and experimentally.
- Contributed to MetriSCA, a **C++** open-source library of metrics for power side-channel analysis accompanying the publication.

Improving First-Order Threshold Implementations of SKINNY

INDOCRYPT

A. Caforio, D. Collins, **O. Glamočanin**, and S. Banik *2021*

- Worked on an efficient threshold implementation protection against power side-channel attacks for the SKINNY cipher, written in **VHDL**.
- Implemented and evaluated the design on **FPGA** using **Xilinx Vivado**, showing no existence of first-order power side-channel leakage.

Shared FPGAs and the Holy Grail: Protections Against Side-Channel and Fault Attacks

DATE

O. Glamočanin*, D. G. Mahmoud*, F. Regazzoni, and M. Stojilović (* equal contribution) *2021*

- Analyzed recently proposed methods for protection against side-channel and fault attacks in shared FPGAs.
- Provided insights on the versatility and inter-operability of the countermeasures, with an emphasis on future research directions.

Are Cloud FPGAs Really Vulnerable to Power-Analysis Attacks?

DATE

O. Glamočanin, L. Coulon, F. Regazzoni, and M. Stojilović *2020*

- Implemented an **FPGA** voltage sensor on state-of-the-art cloud FPGAs (**Xilinx UltraScale+** on **AWS EC2 F1 instances**) using **VHDL** and **Vivado**.
- Demonstrated the first remote power side-channel attack on cloud-scale FPGAs.

Built-In Self-Evaluation of First-Order Power Side-Channel Leakage for FPGAs

ISFPGA

O. Glamočanin, L. Coulon, F. Regazzoni, and M. Stojilović *2020*

- Used **SystemC** and **VHDL** to implement a fixed-point DSP system on **FPGA** to calculate the statistical *t*-test.
- Showed that FPGA-based voltage sensors and the *t*-test can be used for remote power side-channel leakage estimation.
- Designed the first remote power side-channel leakage assessment system, allowing side-channel security reevaluation on deployed devices.

Honors & Awards

2023	**Nomination for the EPFL Doctoral Program Thesis Distinction**, Award for the best 8% theses, 30% nomination rate	*Switzerland*
2018	**EPFL EDIC Fellowship**, Fellowship for first-year Ph.D. students	*Switzerland*
2017	**French Government Scholarship for International Students**, Full scholarship for master studies in France	*France*
2016	**Dr Vladan Desnica Award**, Best student of the microcomputer electronics track	*Serbia*

Languages

Serbian:	Mother tongue
English:	fluent (level C2)
French:	fluent (level C1)
German:	beginner (level A1)