Ognjen **Glamočanin**

Computer Science PhD Student

(+41) 078-948-15-35 | ognjen.glamocanin@epfl.ch | OgacNS94 | ognjen-glamocanin

Research Interests

I am a PhD student in Computer Science at EPFL, and my research interests include FPGAs (security, cloud integration, AI acceleration), hardware security, and machine learning applications. My current research focuses on cloud FPGA security and exploring vulnerabilities introduced by multiple users sharing the same FPGA.

Education

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

PhD in Computer Science — ***Expected grad: August 2023***

- Power side-channel security of shared FPGAs in the cloud
- Thesis advisors: Dr. Mirjana Stojilović and Prof. Babak Falsafi

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

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 ML techniques to model correlation between events and simulated layout-level power consumption
- Enabled power estimation in early microarchitecture design stages by integrating power prediction in a cycle-accurate simulator

FROBAS D.O.O. — *Novi Sad, Serbia*

Machine Learning Hardware Acceleration Intern — *Nov 2016 – Jun 2017*

- Design and verification of an ML 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

Publications

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

(under review)

O. Glamočanin, Shashwat Shrivastava, Jinwei Yao, Nour Ardo, Mathias Payer, M. Stojilović — *2023*

- Evaluation of instruction-level power side-channel leakage of soft-core CPUs in shared FPGAs using deep-learning profiling techniques.
- Evaluation of the impact of parameters, such as ML model choice, profiling templates, and averaging, on the accuracy.

Active Wire Fences for Multi-Tenant FPGAs — *DDECS*

O. Glamočanin, Anđela Kostić, Staša Kostić, M. Stojilović — *2023*

- Novel FPGA-based power waster architecture using routing resources, with no resource overhead compared to the state of the art.
- In active fences, the wire wasters outperform the state-of-the-art and provide superior protection against remote power analysis attacks.

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

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

- Novel FPGA-based voltage sensor architecture using routing resources.
- Evaluation showing superior sensing capabilities than the state of the art, even on datacenter accelerator cards (Alveo U200).

Temperature Impact on Remote Power Side-Channel Attacks on Shared FPGAs — *DATE*

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

- Analysis of temperature impact on FPGA-voltage sensors and remote power-analysis attacks.
- 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*

- Analysis and comparison of methods for power side-channel security evaluation, with extensive experimental examples.
- Work accompanied with an open-source library of metrics for side-channel analysis.

Improving First-Order Threshold Implementations of SKINNY *INDOCRYPT*

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

- An efficient threshold implementation protection against power side-channel attacks for the SKINNY cipher.
- Experimental evaluation showing no existence of first-order power side-channel leakage on an FPGA implementation.

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*

- Analysis of recently proposed methods for protection against side-channel and fault attacks in shared FPGAs.
- 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*

- Implementation of an FPGA-based voltage sensor on the state-of-the-art cloud FPGAs: Xilinx UltraScale+ on AWS F1 instances.
- Demonstration that remote power side-channel attacks are possible on cloud-scale FPGAs, and pose a serious threat to FPGA multitenancy.

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

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

- Demonstration that FPGA-based voltage sensors can be leveraged for remote power side-channel leakage estimation using the *t*-test.
- Design of a first remote power side-channel leakage assessment system, allowing side-channel security reevaluation on deployed devices.

Honors & Awards

2018 **EPFL EDIC Fellowship,** *Switzerland*
Fellowship for first-year PhD students

2017 **French Government Scholarship for International Students,** *France*
Full scholarship for master studies in France

2016 **Dr Vladan Desnica Award,** *Serbia*
Best student of the microcomputer electronics track

Teaching Experience

EPFL *Lausanne, Switzerland*

Teaching Assistant *Feb 2019 – ongoing*

- **Computer Architecture**: Head TA, managing the course and lab sessions in CPU micro-architecture for 2nd year B.S. students
- **System Programming Project**: Leading lab sessions in C for 2nd year B.S. students
- **Information, Computation, Communication**: Head TA, managing the course and leading lab sessions in Python and C for 1st year B.S. students

University of Novi Sad *Novi Sad, Serbia*

Teaching Assistant *Sep 2016 – Jun 2017*

- **Electrical Circuit Theory**: Leading computer lab sessions in MATLAB for 2nd year B.S. students
- **Systems and Signals**: Leading computer lab sessions in MATLAB for 2nd year B.S. students

Technical Skills

Programming languages:	C/C++ (10yrs), Python (6yrs), SystemVerilog, MATLAB
Scripting languages:	Python, Bash, TCL
Hardware description languages:	VHDL (9yrs), Verilog, SystemVerilog, SystemC
CAD EDA tools:	Xilinx ISE, Xilinx Vivado and Vitis, Cadence NCSim
ML tools:	Python (Keras, TensorFlow, Weights and Biases, Pandas), Docker

Languages

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