

# Ognjen Glamočanin

COMPUTER SCIENCE PHD GRADUATE

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

## Education

### EPFL, Ecole Polytechnique Fédérale de Lausanne

PHD IN COMPUTER SCIENCE

- Thesis topic: Power side-channel security of remote FPGAs
- Thesis advisors: Dr. Mirjana Stojilović and Prof. Babak Falsafi

Lausanne, Switzerland

Graduated: August 2023

### Sorbonne Université, Paris VI

M.S. IN COMPUTER SCIENCE

Paris, France

2017 – 2018

### University of Novi Sad, Faculty of Technical Sciences

B.S. WITH HONOURS IN ELECTRICAL ENGINEERING

Novi Sad, Serbia

2013 – 2017

## Work Experience

### ARM

CPU MICROARCHITECTURE AND DESIGN INTERN

Sophia Antipolis, France

Mar 2018 – Aug 2018

- Analyzed CPU microarchitectural events for the purposes of **power consumption estimation** during cycle-accurate simulation
- Used **Python sklearn** to model 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.

MACHINE LEARNING HARDWARE ACCELERATION INTERN

Novi Sad, Serbia

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

HARDWARE FUNCTIONAL VERIFICATION INTERN

Belgrade, Serbia

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), UVM

**Programming and scripting languages:** C/C++ (10yrs), Python (6yrs), SystemVerilog, MATLAB, Bash, TCL

**Hardware description languages:** VHDL (9yrs), Verilog, SystemVerilog, SystemC

**CAD EDA tools:** Xilinx ISE, Xilinx Vivado and Vitis, QuestaSim, Cadence NCSim

**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, SHASHWAT SHRIVASTAVA, JINWEI YAO, NOUR ARDO, MATHIAS PAYER, M. STOJILLOVIĆ

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 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, ANĐELA KOSTIĆ, STAŠA KOSTIĆ, M. STOJILLOVIĆ

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

DAVID SPIELMANN\*, O. GLAMOČANIN\*, M. STOJILLOVIĆ (\* 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. STOJILLOVIĆ

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. AZOUAOU\*, D. ROS\*, F. REGAZZONI\*, M. STOJILLOVIĆ\* (\* 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. STOJILLOVIĆ (\* 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. STOJILLOVIĆ

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. STOJILLOVIĆ

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

## 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 2<sup>nd</sup> year B.S. students
- **System Programming Project:** Leading lab sessions in C for 2<sup>nd</sup> year B.S. students
- **Information, Computation, Communication:** Head TA, managing the course and leading lab sessions in Python and C for 1<sup>st</sup> 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 2<sup>nd</sup> year B.S. students
- **Systems and Signals:** Leading computer lab sessions in MATLAB for 2<sup>nd</sup> year B.S. students

## Languages

- |                 |                     |
|-----------------|---------------------|
| <b>Serbian:</b> | Mother tongue       |
| <b>English:</b> | fluent (level C2)   |
| <b>French:</b>  | fluent (level C1)   |
| <b>German:</b>  | beginner (level A1) |