UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Seminar announcement

Friday 27th June 2025, Time: 11:00 - 12:00
Meeting Room, Floor 1, Building 3, DIETI - Via Claudio, 21 - NAPOLI

Prof. Jakub Szefer

Northwestern University, Evanston, IL, US

Department of Electrical and Computer Engineering

https://caslab.io/jakub/ – Email: jakub.szefer@northwestern.edu

Trusted Execution Environments for QPUs

Abstract: Quantum computing systems continue to advance rapidly in their size and fidelity. In parallel, there is an increasing number of deployments of these quantum computing systems into cloud-based services for use by researchers and the public. More and more of these quantum computing systems are becoming available as cloud-based services thanks to IBM Quantum, Amazon Braket, Microsoft Azure, and other cloud providers. Ease of access to these computing systems by almost anybody can help democratize quantum computing, democratize development of algorithms or compilers, as well as democratize research, since people can experiment with quantum computation on real devices without themselves having a physical quantum computer. However, cloud-based access may make these systems vulnerable to novel security threats, both for users and the cloud providers. Trusted, secure quantum computer architectures are one solution and defense against number of security threats faced by cloud-based quantum computing systems. This seminar will present a number of architectures for secure quantum computing systems under different threat models, along with the security protections they can offer. The goal of this seminar will be to introduce audience to recent research on architectures for secure quantum computing systems, as well as in general to make the audience aware of the need to protect quantum computing systems, of what can be achieved today, and of the many open research directions in security of quantum computing systems.

Lecturer short bio: *Jakub Szefer is an Associate Professor in the Electrical and Computer Engineering Department at Northwestern University where he leads the Computer Architecture and Security Lab (CASLAB). His research focuses on security attacks and defenses at the computer architecture and hardware levels of computer systems. His work encompasses security of processor architectures, reconfigurable logic, post-quantum cryptographic accelerators, and most recently, quantum computers. He is the author of the "Principles of Secure Processor Architecture Design" book, published in 2018, and co-editor of the "Security of FPGA-Accelerated Cloud Computing Environments" book, published in 2023. He received his BS degree with highest-honors in Electrical and Computer Engineering from University of Illinois at Urbana-Champaign, and MA and PhD degrees in Electrical Engineering from Princeton University.*

For information: Prof. Edo Giusto (DIETI, UniNA) – edoardo.giusto@unina.it *(organizer)*