SIMONE PERRIELLO

Date of birth	25th July 1989	*Email*	simone.perriello@polimi.it
Citizenship	Italian	*Phone*	(+39) 02 2399 9047
Current location	Milan, Italy	*Website*	https://perriello.faculty.polimi.it

EDUCATION

Politecnico di Milano since November 2019
Ph.D. candidate *Milan*

- Thesis title: *Quantum Computing Algorithms for Cryptography: design, validation and complexity assessment*
- Advisors: Prof. *Gerardo Pelosi*; Prof. *Alessandro Barenghi*

Politecnico di Milano April 2019
M.Sc. degree *Milan*

- Thesis title: *Design and developments of quantum circuits to solve the Information Set Decoding problem*
- Advisors: Prof. *Gerardo Pelosi*; Prof. *Alessandro Barenghi*
- Grade: 110/110

IELTS February 2016
English certificate

- Thesis title: *Quantum Computing Algorithms for Cryptography: design, validation and complexity assessment*
- Grade: 7.5/9 (equivalent to C1 of CEFR)

RESEARCH INTERESTS

My research spans the domains of *quantum computing* and *cryptography*, with a primary focus on designing quantum algorithms based on the gate model to attack code-based cryptosystems.

During my Master's program, I embarked on a self-guided exploration of quantum computing. This journey culminated in my thesis, during which I developed a quantum adaptation of the *Information Set Decoding (ISD)* strategy, the most efficient kind of attack against cryptosystems based on linear codes. The implementation of those attacks was based on IBM's open source Qiskit framework, to which I also contributed several patches.

During my internship at Atos, I extended my research by enhancing quantum algorithm simulations for Noisy Intermediate-Scale Quantum (NISQ) architectures. I created a versatile quantum simulation library capable of simulating systems with hundreds of qubits, targeted for the Atos' *Quantum Learning Machine (QLM)* environment. The library was extensively used to replicate state of the art experimental results related to the challenging *barren plateau problem* in quantum neural networks.

My Ph.D. research centered on *quantum cryptanalysis* of post-quantum cryptography. I proposed the first complete design of quantum circuits tailored to attack the hardness assumptions in code-based cryptography, evaluating the computational complexity of attacking all the code-based cryptosystems under international scrutiny. Comprehensive assessments and comparisons, which considered both theoretical and practical implementations for quantum ISD introduced in the years following my initial work, confirmed the substantial advantage of my contribution, with performance surpassing other approaches by a significant margin, ranging from 2^{19} to 2^{30}.

During this process, I also designed a range of practical quantum circuits that can be of independent interests — to sort bitstrings, to permute matrix columns, to perform Gauss-Jordan Elimination on a matrix, and to check the weight of a given bitstring.

WORK EXPERIENCE

Atos: Bull SAS R&D Labs February to July 2020
Quantum computing researcher *Les Clayes-sous-Bois*

- *Supervisors*: *Bertrand Marchand* and *Cyril Allouche*
- Implemented novel simulation strategies for quantum circuits targeting NISQ architecture.
- Explored the *barren plateau problem* in quantum neural network.

Atos: HPC & Quantum team July 2019 to January 2020
Quantum computing researcher *Milan*

- Configured hardware/software stack of the *Atos QLM* appliance.
- Implemented well-known quantum algorithms on the *Atos QLM* framework.
- Lectured external customers on the *Atos QLM* framework.

TEACHING EXPERIENCE

Teaching assistant at Politecnico di Milano February to March 2022
Introduction to Quantum Computing (Ph.D. course) *Prof. Gerardo Pelosi, Prof. Alessandro Barenghi*

- Presentation of the Atos myQLM and QLM frameworks.
- Showcase code implementation of renowned quantum algorithms using QLM framework.

Teaching assistant at Politecnico di Milano November 2020 to January 2024
Computer Architectures and Operating Systems *Prof. Gerardo Pelosi*

- Exercise lectures: Linux Operating Systems.
- Topics addressed (partial): parallel programming (processes, threads), task scheduler, system calls and interrupt routines, memory management, file systems and I/O.

Teaching assistant at Politecnico di Milano November 2022 to January 2024
Computer Architectures and Operating Systems *Prof. Cristina Silvano*

- Exercise lectures: Linux Operating Systems.
- Topics addressed (partial): parallel programming (processes, threads), task scheduler, system calls and interrupt routines, memory management, file systems and I/O.

Teaching assistant at Politecnico di Milano November 2023 to January 2024
Computer Architectures and Operating Systems *Prof. Federico Terraneo*

- Exercise lectures: Linux Operating Systems.
- Topics addressed (partial): parallel programming (processes, threads), task scheduler, system calls and interrupt routines, memory management, file systems and I/O.

Teaching assistant at Politecnico di Milano November 2021 to June 2022
Informatica (per Aerospaziali) *Prof. Gerardo Pelosi*

- Exercise lectures: computer science for Aerospace Engineering.
- Topics addressed (partial): Boolean logic and basics of C programming.

Teaching tutor at Politecnico di Milano November 2018 to January 2019
Informatica (per Ambientali) *Prof. Andrea Bonarini*

- Theory lectures and laboratory exercises on the C programming language.

Teaching tutor at Politecnico di Milano November 2016 to January 2017
Computer Architectures and Operating Systems *Prof. Anna Maria Antola*

- Exercise lectures: Linux Operating Systems.
- Topics addressed (partial): parallel programming (processes, threads), task scheduler, system calls and interrupt routines, memory management, file systems and I/O.

LIST OF PUBLICATIONS

Journals

J1. Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. “Improving the Efficiency of Quantum Circuits for Information Set Decoding”. In: *ACM Transactions on Quantum Computing* 4.4 (Aug. 2023). ISSN: 2643-6809. DOI: `10.1145/3607256`. URL: `https://doi.org/10.1145/3607256`

Conferences

C1. Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. “A Complete Quantum Circuit to Solve the Information Set Decoding Problem”. In: *IEEE International Conference on Quantum Computing and Engineering, QCE 2021, Broomfield, CO, USA, October 17-22, 2021.* Ed. by Hausi A. Müller et al. IEEE, 2021, pp. 366–377. DOI: `10.1109/QCE52317.2021.00056`. URL: `https://doi.org/10.1109/QCE52317.2021.00056`

C2. Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. “A Quantum Circuit to Speed-up the Cryptanalysis of Code-Based Cryptosystems”. In: *Security and Privacy in Communication Networks - 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6-9, 2021, Proceedings, Part II*. ed. by Joaquín García-Alfaro et al. Vol. 399. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, 2021, pp. 458–474. DOI: `10.1007/978-3-030-90022-9_25`. URL: `https://doi.org/10.1007/978-3-030-90022-9_25`

SCIENTIFIC COMMUNITY ROLES

Reviewer

- Paolo Mori, Gabriele Lenzini, and Steven Furnell, eds. *9th International Conference on Information Systems Security and Privacy, ICISSP 2023*
- Leonie Simpson and Mir Ali Rezazadeh Baee, eds. *Information Security and Privacy - 28th Australasian Conference, ACISP 2023*. Lecture Notes in Computer Science
- *IEEE/ACM International Conference On Computer Aided Design, ICCAD 2021*

ADDITIONAL SCIENTIFIC ACTIVITIES

2021 Poster presenter at *International Summer School on Advanced Computer Architecture and Compilation for High-performance Embedded Systems* with title *A Quantum Circuit to Speed-up the Cryptanalysis of Code-based Cryptosystems*.

AWARDS AND RECOGNITION

2021 Grant winner for *International Summer School on Advanced Computer Architecture and Compilation for High-performance Embedded Systems*.