SIMONE PERRIELLO

Email	simone.perriello@polimi.it	*Website*	https://perriello.faculty.polimi.it
ORCID	0000-0001-9656-7252	*Lab Website*	https://www.heaplab.deib.polimi.it

ACADEMIC EXPERIENCE

Politecnico di Milano since May 2024
Postdoctoral Researcher *Milan*

- Project 1: Quantum Cryptanalysis of Symmetric and Asymmetric Cryptosystems
- Project 2: Quantum Acceleration of Clique Problems

Politecnico di Milano May 2024
Ph.D. *Milan*

- Thesis title: *Quantum Circuits for Information Set Decoding: Quantum Cryptanalysis of Code-Based Cryptosystems*
- Advisors: Prof. *Gerardo Pelosi*; Prof. *Alessandro Barenghi*

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.

EDUCATION

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

Unisannio July 2015
B.Sc. Degree *Benevento*

- Thesis title: *Un algoritmo per il social tagging di mashup*
- Advisor: Prof. *Eugenio Zimeo*
- Grade: 110/110 cum laude

RESEARCH INTERESTS

My research focuses on *quantum computing* and *quantum cryptanalysis*, with a particular emphasis on code-based cryptography. During my Master's thesis, I designed quantum circuits adapting the *Information Set Decoding (ISD)* strategy, the most efficient known attack on code-based cryptosystems, implementing and benchmarking these techniques using IBM's Qiskit framework. I expanded this work during my Ph.D. by designing optimized quantum circuits to evaluate the complexity of attacking all major code-based cryptographic schemes under international evaluation. The research led to significant reductions in attack complexity, improving efficiency by factors ranging from 2^{19} to 2^{30} compared to previous approaches.

During my time at Atos' R&D laboratories, I developed a quantum simulation library for Noisy Intermediate-Scale Quantum (NISQ) architectures, enabling large-scale simulations on the *Quantum Learning Machine (QLM)*. This tool was instrumental in reproducing state-of-the-art results on quantum neural networks, particularly in studying the *barren plateau problem*.

As a Postdoctoral researcher, I continue to explore the intersection of quantum algorithm design and cryptographic security, contributing to the study of post-quantum cryptographic resilience. My current research also extends to the design of quantum algorithms for graph-related problems, such as clique detection, and optimizing input state preparation techniques.

TEACHING EXPERIENCE

Teaching assistant at Politecnico di Milano November 2023 to January 2025
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 2022 to January 2025
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 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 2025
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 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

Refereed International 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`

Refereed International Conferences

[C6] Simone Perriello. "Quantum Circuit Design for Finding k-Cliques via Quantum Amplitude Amplification Strategies". In: *Proceedings of the 22nd ACM International Conference on Computing Frontiers, CF 2025, Cagliari, Italy, May 28-30, 2025.* to appear. ACM, 2025. DOI: `10.1145/3719276.3725200`

- [C5] Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. "A Quantum Circuit to Execute a Key-Recovery Attack Against the DES and 3DES Block Ciphers". In: *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montréal, Québec, Canada, September 15-20, 2024.* Ed. by Candace Culhane et al. IEEE, 2024, pp. 1–12. DOI: `10.1109/QCE60285.2024.00011`
- [C4] Giacomo Lancellotti, Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. "Design of a Quantum Walk Circuit to Solve the Subset-Sum Problem". In: *61st ACM/IEEE Design Automation Conference, DAC 2024, San Francisco, CA, USA, July 23-27, 2024.* ACM, 2024. DOI: `10.1145/3649329.3657337`
- [C3] Simone Perriello, Alessandro Barenghi, and Gerardo Pelosi. "Quantum Circuit Design for the Lee-Brickell Based Information Set Decoding". In: *Applied Cryptography and Network Security Workshops - ACNS 2024 Satellite Workshops, ACNS.* Lecture Notes in Computer Science. Abu Dhabi, UAE: Springer, 2024, pp. 8–28. DOI: `10.1007/978-3-031-61489-7_2`
- [C2] 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, Greg Byrd, Candace Culhane, and Travis Humble. IEEE, 2021, pp. 366–377. DOI: `10.1109/QCE52317.2021.00056`
- [C1] 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`

Non-Refereed

- [N1] Poster 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.*

REVIEWER FOR INTERNATIONAL JOURNALS AND CONFERENCES

2025

- *IEEE International Conference on Quantum Computing and Engineering, QCE 2025, Albuquerque, New Mexico, USA, August 31-September5, 2025.* 2025
- *IEEE International Conference on Quantum Software, QSW 2025, Helsinki, Finland, July 7-12.* 2025
- *Foundations Of Reliable Classical-quantum Engineering (FORCE) 2025, co-located with IEEE/IFIP DSN 2025, Naples, Italy, June 26 2025.* 2025
- *Future Generation Computer Systems* (2025). ISSN: 1872-7115, Impact Factor: 6.2, SCImago Journal Rank (SJR) 2023: 1.95 (Q1)
- *ACM International Conference on Computing Frontiers, CF 2025.* 2025

2024

- Candace Culhane et al., eds. *IEEE International Conference on Quantum Computing and Engineering, QCE 2024.* 2024. ISBN: 979-8-3315-4137-8
- Mauro Conti, ed. *IEEE Transactions on Information Forensics and Security* (2024). ISSN: 1556-6021, Impact Factor: 6.8, SCImago Journal Rank (SJR) 2023: 2.89 (Q1)
- **tetc24**, Impact Factor: 5.9, SCImago Journal Rank (SJR) 2023: 1.57 (Q1)

2023

- Paolo Mori, Gabriele Lenzini, and Steven Furnell, eds. *9th International Conference on Information Systems Security and Privacy, ICISSP 2023.* 2023. ISBN: 978-989-758-624-8
- Leonie Simpson and Mir Ali Rezazadeh Baee, eds. *Information Security and Privacy - 28th Australasian Conference, ACISP 2023.* Lecture Notes in Computer Science. 2023. ISBN: 978-3-031-35485-4

2021

- *IEEE/ACM International Conference On Computer Aided Design, ICCAD 2021.* 2021. ISBN: 978-1-6654-4507-8

PROGRAM COMMITTEE MEMBER

2025

- *IEEE International Conference on Quantum Computing and Engineering, QCE 2025, Albuquerque, New Mexico, USA, August 31-September5, 2025.* 2025
- *Foundations Of Reliable Classical-quantum Engineering (FORCE) 2025, co-located with IEEE/IFIP DSN 2025, Naples, Italy, June 26 2025.* 2025

2024

- Candace Culhane et al., eds. *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montréal, Québec, Canada, September 15-20, 2024*. 2024

AWARDS AND RECOGNITION

2024 HiPEAC Paper Award, *European Network of Excellence on High Performance and Embedded Architecture and Compilation*

2024 Grant winner for *61st ACM/IEEE Design Automation Conference, DAC 2024, San Francisco, CA, USA, July 23-27, 2024*.

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

OTHER ACADEMIC ACHIEVEMENTS, HONORS, AND ACTIVITIES

2024

- Session chair for the session titled *Application for Data Analysis* at Candace Culhane et al., eds. *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montréal, Québec, Canada, September 15-20, 2024*. 2024