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

EDUCATION

Politecnico di Milano since May 2024
PostDoc *Milan*

· Project 1: Quantum Cryptanalysis of Symmetric and Asymmetric Cryptosystems

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*

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 journey has evolved from my B.Sc. thesis on *recommender systems* to my current focus on *quantum computing* and *cryptography*. My current focus revolves around the meticulous design of quantum algorithms within the gate-based model, specifically aimed at addressing challenges in code-based cryptosystems.

During my Bachelor's studies, I specialized in designing a recommendation system tailored for enhancing social tagging of mashups — web applications that integrate data and functionalities from diverse sources to enhance the overall user experience. The principal goal of this project was to enhance the core of the mashup tagging process by optimizing the recommender system. This optimization was achieved through systematic social data merging and the discernment of potential user relationships.

Building on this foundation, my Master's program became a platform for 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 centred 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

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. URL: https://doi.org/10.1145/3607256

Refereed International Conferences

[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. URL: https://doi.org/10.1109/DAC56929.2023

[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. URL: https://doi.org/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. URL: https://doi.org/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

2024

- Candace Culhane et al., eds. *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montréal, Québec, Canada, September 15-20, 2024*. SciTePress, 2023. ISBN: 979-8-3315-4137-8
- Mauro Conti, ed. *IEEE Transactions on Information Forensics and Security* (2024). ISSN: 1556-6021. URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206, Impact Factor: 6.8, SCImago Journal Rank (SJR) 2023: 2.89 (Q1)
- Paolo Montuschi, ed. *IEEE Transactions on Emerging Topics in Computing* (2024). ISSN: 2376-4562. URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6245516, 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*. SciTePress, 2023. ISBN: 978-989-758-624-8. DOI: 10.5220/0000168400003405
- Leonie Simpson and Mir Ali Rezazadeh Baee, eds. *Information Security and Privacy - 28th Australasian Conference, ACISP 2023*. Lecture Notes in Computer Science. Springer, 2023. ISBN: 978-3-031-35485-4. DOI: 10.1007/978-3-031-35486-1

2021

- *IEEE/ACM International Conference On Computer Aided Design, ICCAD 2021*. IEEE, 2021. ISBN: 978-1-6654-4507-8. DOI: 10.1109/ICCAD51958.2021

PROGRAM COMMITTEE MEMBER

2024

· Candace Culhane et al., eds. *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montréal, Québec, Canada, September 15-20, 2024*. ISBN: 979-8-3315-4137-8

AWARDS AND RECOGNITION

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*. ISBN: 979-8-3315-4137-8