SIMONE PERRIELLO

Academic email	simone.perriello@polimi.it
Personal email	sperriello@proton.me
Phone number	(+39) 02 2399 9047
Website	https://perriello.faculty.polimi.it

EDUCATION

Ph.D. Candidate *since November 2019*
Enrolled in Ph.D program in Information Technology at *Politecnico di Milano*
Thesis title: *Quantum Computing Algorithms for Cryptography: design, validation and complexity assessment*
Advisor Prof. *Gerardo Pelosi*; Co-Advisor Prof. *Alessandro Barenghi*

M.Sc. degree *April 2019*
Master of Science in Computer Science and Engineering at *Politecnico di Milano*
Thesis title: *Design and developments of quantum circuits to solve the Information Set Decoding problem*
Advisor Prof. *Gerardo Pelosi*; Co-Advisor Prof. *Alessandro Barenghi*; Grade: 110/110

IELTS *February 2016*
Grade 7.5/9 (equivalent to C1 of the 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 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 (PQC). I proposed the first complete design of quantum circuits tailored to attack the hardness assumptions in code-based crpytography, 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 *Milano*

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

TEACHING EXPERIENCE

Teaching assistant 2020-21; 21-22; 22-23; 23-24
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 2021-22; 22-23; 23-24
Computer Architectures and Operating Systems *Prof.ssa 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 2023-24
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 2021-22; 22-23
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 2019
Informatica (per Ambientali) *Prof. Andrea Bonarini*

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

Teaching tutor 2018
Computer Architectures and Operating Systems *Prof.ssa Anna Maria Antola*

- Theory lectures and lab exercises regarding both the architectures of modern computers (ranging from the assembly language to the logic gates) and the structure of an operating system (including the theory of parallel programming and threads management in Linux)

LIST OF PUBLICATIONS

Journals

J1. Perriello, S.; Barenghi, A.; Pelosi, G. Improving the Efficiency of Quantum Circuits for Information Set Decoding. *ACM Transactions on Quantum Computing*. 2023, vol. 4, no. 4. ISSN 2643-6809. Available from DOI: 10.1145/3607256

Conferences

C1. Perriello, S.; Barenghi, A.; Pelosi, G. A Complete Quantum Circuit to Solve the Information Set Decoding Problem. In: Müller, H. A.; Byrd, G.; Culhane, C.; Humble, T. (eds.). *IEEE International Conference on Quantum Computing and Engineering, QCE 2021, Broomfield, CO, USA, October 17-22, 2021*. IEEE, 2021, pp. 366–377. Available from DOI: 10.1109/QCE52317.2021.00056

C2. Perriello, S.; Barenghi, A.; Pelosi, G. A Quantum Circuit to Speed-up the Cryptanalysis of Code-Based Cryptosystems. In: García-Alfaro, J.; Li, S.; Poovendran, R.; Debar, H.; Yung, M. (eds.). *Security and Privacy in Communication Networks - 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6-9, 2021, Proceedings, Part II*. Springer, 2021, vol. 399, pp. 458–474. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Available from DOI: 10.1007/978-3-030-90022-9_25

SCIENTIFIC COMMUNITY ROLES

Reviewer

- Mori, P.; Lenzini, G.; Furnell, S. (eds.). *Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22-24, 2023*. SciTePress, 2023. ISBN 978-989-758-624-8. Available from DOI: 10.5220/0000168400003405
- Simpson, L.; Baee, M. A. R. (eds.). *Information Security and Privacy - 28th Australasian Conference, ACISP 2023, Brisbane, QLD, Australia, July 5-7, 2023, Proceedings*. Vol. 13915. Springer, 2023. Lecture Notes in Computer Science. ISBN 978-3-031-35485-4. Available from DOI: 10.1007/978-3-031-35486-1
- *IEEE/ACM International Conference On Computer Aided Design, ICCAD 2021, Munich, Germany, November 1-4, 2021*. IEEE, 2021. ISBN 978-1-6654-4507-8. Available from DOI: 10.1109/ICCAD51958.2021

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*