Léo Colisson

PhD student in Computer Science,
LIP6 – Sorbonne Université

5 Rue Jean-Pierre Thimbaud
75011 Paris
☎ *+33 6 79 12 48 58*
✉ *leo.colisson@lip6.fr*
leo.colisson.me
in *Léo Colisson*
22 August 1994

RESEARCH INTERESTS

I'm interested in *quantum cryptography*, with a particular focus on classical-client delegated blind quantum computing, composable security, and lattice-based cryptography.

EDUCATION

2018–2021 **PhD student in Computer Science**, *Sorbonne Université*.
Supervised by Elham Kashefi and Antoine Joux. Graduation expected in September 2021.
Thesis entitled "*Study of protocols between classical clients and a quantum server*".

2016–2018 **Parisian Master of Research in Computer Science (MPRI)**, *École Normale Supérieure Paris-Saclay*.
Research-oriented master in computer science, run jointly by French most prestigious schools (École Polytechnique, Université Paris-Saclay, ENS de la rue d'Ulm…). Major in cryptography and quantum computing. With High(est) Honors.

2015–2016 **Bachelor of Computer Science**, *École Normale Supérieure Paris-Saclay*.
With Highest Honors.

2014–2015 **Bachelor of Physics**, *École Normale Supérieure Paris-Saclay*, PHYTEM.
With Honors.
École Normale Supérieure (ENS) Paris-Saclay: highly-selective higher education institution, member of Paris-Saclay University (in 2020: ranked first in the world for Mathematics in the Shanghai Ranking).

2012–2014 **Classes Préparatoires (CPGE) MPSI/MP***, *Lycée du Parc*, Lyon.
Undergraduate program to prepare nationwide highly competitive exams to enroll in "Grandes Écoles" (most prestigious graduate schools). Major in Mathematics, Physics, and Computer Science.

HONORS & AWARDS

2018 **Awarded a Contrat Doctoral Specifique pour Normaliens (CDSN)**.
CDSN: independent doctoral fellowship funded by the French Ministry in charge of Higher Education and Research.

2014 **Normalien**, *École Normale Supérieure Paris-Saclay*.
Normalien: student awarded, via a Ministerial Order, a four-years full scholarship and a status of civil servant.

TEACHING EXPERIENCE

Spring 2021 **C Programming**, *Sorbonne Université*, Licence 1, Teaching assistant.

2019–2020 **Introduction to cryptology**, *Sorbonne Université*, Licence 3, Teaching assistant.

Fall 2019 **Discrete Mathematics**, *Sorbonne Université*, Licence 2, Teaching assistant.

Fall 2018 **Python Programming**, *Polytech Sorbonne*, Licence 2, Teaching assistant.

WORK EXPERIENCE

2018 **Master 2 Internship**, *École Normale Supérieure de la rue d'Ulm, CASCADE Team*.
5 months internship in the cryptography team of ENS Ulm, supervised by Céline Chevalier, on the *design of 2-regular trapdoor functions from post-quantum cryptographic assumptions*.

2017 **Master 1 Internship**, *University of Edinburgh, LFCS.*
5 months internship, supervised by Elham Kashefi and Aggelos Kiayias. Thesis entitled "*Classically Driven Delegated Blind Quantum Computing*".

2016 **Licence 3 Internship**, *École Normale Supérieure de Lyon, LIP, MC2 Team.*
6 weeks internship, supervised by Omar Fawzi. Thesis entitled "*Quantum analog of Differential Privacy in term of Rényi divergence*".

2015 **Licence 3 Internship**, *Sorbonne Université, IN2P3, LPNHE.*
6 weeks internship with Pierre Astier. I studied the role of gases in atmospheric extinction to improve the usability of the Large Synoptic Survey Telescope.

PUBLICATIONS & TALKS

Papers

- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**,
  Manuscript, arXiv:2104.04742.
  Coauthors: F. Grosshans, E. Kashefi.
- **Security Limitations of Classical-Client Delegated Quantum Computing**,
  ASIACRYPT 2020, Presented at Q-Turn 2020, arXiv:2007.01668.
  Coauthors: C. Badertscher, A. Cojocaru, E. Kashefi, D. Leichtle, A. Mantri, P. Wallden.
- **QFactory: classically-instructed remote secret qubits preparation**,
  ASIACRYPT 2019, arXiv:1904.06303
  Coauthors: A. Cojocaru, E. Kashefi, P. Wallden.
- **On the possibility of classical client blind quantum computing**,
  Cryptography (Selected Issue Cover), Presented at QCrypt 2018, arXiv:1802.08759.
  Coauthors: A. Cojocaru, E. Kashefi, P. Wallden.

Talks

- **Security Limitations of Classical-Client Delegated Quantum Computing**,
  Speaker at ASIACRYPT 2020, online (initially Daejeon, South Korea).
- **On the possibility of classical client blind quantum computing**,
  Speaker at:
  - QCrypt 2018, Shanghai, China.
  - JIQ 2018, Nancy, France.

Invited Talks

- **Quantum Introduction Tutorial (3h)**, Spring School EPIT 2021.

Posters

- **Security Limitations of Classical-Client Delegated Quantum Computing**,
  QCrypt 2020 (Online) and QIP 2021 (Online).
- **On the possibility of classical client blind quantum computing**,
  GdR-IQFA 2018 (Montpellier, France) and ICoCQ 2018 (Paris, France).

MISCELLANEOUS

Reviewer For CRYPTO 2021, QIP 2020, QIP 2019, Cryptography, Quantum.

Organizer Of QuRLInG 2019, a one week workshop in Grenoble (Les 7 Laux).

PROFESSIONAL SKILLS

Softwares LaTeX/TikZ, git, emacs, LibreOffice, Gimp, Blender, Inkscape, Kdenlive, Word, Excel.

Programming Ocaml, C(++), Python, Haskell, Bash, Web, Fortran, SQL Databases…

OS Technical use of Linux (Debian, NixOS), Windows.

INTERESTS

Hobbies Salsa, Piano, Saxophone, Volley-ball, Tennis, Astronomy, Photography, Hiking, Biking.

Associative life Member of the Student Union Office 2015–2016, head of the Salsa Club, co-creator of two Salsa choreographies, responsible for the website of "La Nuit aNormale 2016" (gala ball), in charge of the security organization during the inter-school weekend event "InterENS 2015" (24 security guards in rush hours).

Travel Road trips in Sri-Lanka, Cuba, China, and Germany–Sweden–Norway. And more ecological/local long distance hikes and bike rides.