Léo Colisson

QuSoft/CWI, Amsterdam
Postdoc in Quantum Cryptography

De la Reijstraat, 25
1091 NZ Amsterdam
☎ *+33 6 79 12 48 58*
✉ *leo.colisson@cwi.nl*
🌐 *leo.colisson.me*
in *Leo Colisson*
22 août 1994

RESEARCH INTERESTS

I am working in *quantum cryptography*: my research notably focuses on exploring various aspects of blind quantum computing with classical clients, composable security, lattice based cryptography, multipartite computing, diagrammatic reasoning and ZX-calculus.

EDUCATION

2018 2022 **PhD in computer science**, *LIP6, Sorbonne Université*, Paris.
Supervised by Elham Kashefi and Antoine Joux. Thesis entitled:

« *Study of Protocols Between Classical Clients and a Quantum Server* »

Publicly defended on March 28, 2022, before a jury composed of:

- Albrecht Martin,
  University of London (Royaume-Uni), Reporter
- Fawzi Omar,
  ENS de Lyon (France), Examiner
- Jeffery Stacey,
  Centrum Wiskunde & Informatica (Pays-Bas), Reporter
- Joux Antoine,
  CISPA Helmholtz Center for Information Security (Allemagne), PhD supervisor
- Kashefi Elham,
  Sorbonne Université (France) et University of Edinburgh (Royaume-Uni), PhD supervisor
- Magniez Frédéric,
  IRIF (France), Examiner
- Naya-Plasencia María,
  INRIA Paris (France), Examiner
- Renner Renato,
  ETH Zürich (Suisse), Examiner

2016 2018 **Master of Computer Science (MPRI)**, *École Normale Supérieure Paris-Saclay*.
Parisian Master of Research in Computer Science (MPRI), with highest & great honors.

2015 2016 **Licence 3 Informatique**, École Normale Supérieure Paris-Saclay.
With highest honors.

2014 2015 **Licence 3 de Physique**, *PHYTEM*, École Normale Supérieure Paris-Saclay.
Parcours "PHYTEM" (PHYsique, Théorie, Expérience, Modèle), with honors.

2012 2014 **Classes Préparatoires (CPGE) MPSI/MP***, Lycée du Parc, Lyon.
With highest honors.

AWARDS & FELLOWSHIPS

2022 **Quantum Software Consortium (QSC) fellowship**.
Postdoctoral fellowship (1 year), submitted during the Quantum Software Consortium (QSC) 2022's call. Funded by the Ministry of Education, Culture and Science through the Dutch Research Council (NWO).

2018 **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[1], a four-years full scholarship and a status of civil servant.

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000030213856

WORK EXPERIENCE

2022 **Postdoc in quantum cryptography**, *CWI and QuSoft*, Amsterdam.
Postdoctoral researcher (2 years), supervised by Stacey Jeffery, Christian Schaffner et Florian Speelman.

2022 **Postdoc en cryptographie quantique**, *LIP6, Sorbonne Université*, Paris.
Postdoctoral researcher (3 months), supervised by Elham Kashefi.

2018 **Internship Master 2**, *École Normale Supérieure Ulm, CASCADE team.*
5 months internship, supervised by Céline Chevalier. Thesis[2] entitled: « *Classical client blind quantum computing* ».

2017 **Internship Master 1**, *University of Edinburgh, LFCS.*
5 months internship, supervised by Elham Kashefi and Aggelos Kiayias. Thesis[3] entitled « *Classically Driven Delegated Blind Quantum Computing* ».

2016 **Internship Licence 3**, *École Normale Supérieure de Lyon, LIP, MC2 Team.*
Stage de 6 semaines, supervisé par Omar Fawzi. Mémoire[4] intitulé « *Quantum analog of Differential Privacy in term of Rényi divergence* ».

2015 **Internship Licence 3**, *Sorbonne Université, IN2P3, LPNHE.*
6 months internship, supervised by Pierre Astier. I studied the role of gases in atmospheric extinction to enhance the Large Synoptic Survey Telescope.

PUBLICATIONS & PRÉSENTATIONS

Publications

Conferences with proceedings

- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
Léo Colisson, Garazi Muguruza, Florian Speelman,
Advances in Cryptology – ASIACRYPT 2023, 2023, Lecture Notes in Computer Science, Volume 14445, pages 3–38, edited by J. Guo, R. Steinfeld, Springer, Cham.
https://doi.org/10.1007/978-981-99-8742-9
- **Security Limitations of Classical-Client Delegated Quantum Computing**.
Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, Petros Wallden,
Advances in Cryptology – ASIACRYPT 2020, 2020, Lecture Notes in Computer Science, Volume 12492, pages 667–696, edited by S. Moriai, H. Wang, Springer, Cham.
https://doi.org/10.1007/978-3-030-64834-3_23
- **QFactory: Classically-Instructed Remote Secret Qubits Preparation**.
Alexandru Cojocaru, Léo Colisson Elham Kashefi et Petros Wallden,
Advances in Cryptology – ASIACRYPT 2019, 2019, Lecture Notes in Computer Science, Volume 11921, pages 615–645, edited by S. Galbraith et S. Moriai, Springer, Cham.
https://doi.org/10.1007/978-3-030-34578-5_22

Journals

- **On the possibility of classical client blind quantum computing**.
Alexandru Cojocaru, Léo Colisson Elham Kashefi et Petros Wallden,
Cryptography, 2021, Volume 5, Issue 1, 50 pages.
First online appearance in 2018 (presented at QCRYPT 2018), article selected for the issue cover[5].
https://doi.org/10.3390/cryptography5010003

[2] https://leo.colisson.me/presentations/2018_internship_M2.html
[3] https://leo.colisson.me/presentations/2017_internship_M1.html
[4] https://leo.colisson.me/presentations/2016_internship_L3.html
[5] https://www.mdpi.com/2410-387X/5/1

Pre-prints

- **All graph state verification protocols are composably secure**.
  Léo Colisson, Damian Markham, Raja Yehia,
  Pre-print on the arXiv, 2024.
  https://arxiv.org/abs/2402.01445
- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, Frédéric Grosshans, Elham Kashefi,
  In submission, 2021.
  https://arxiv.org/abs/2104.04742

Présentations

Conferences without proceedings

- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, Garazi Muguruza, Florian Speelman,
  QCRYPT 2023, 2023, University of Maryland, États-Unis.
  https://2023.qcrypt.net/accepted-papers/
- **Security Limitations of Classical-Client Delegated Quantum Computing**.
  Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, Petros Wallden,
  Q-Turn 2020, 2020, Online.
- **QFactory: Classically-Instructed Remote Secret Qubits Preparation**.
  Alexandru Cojocaru, Léo Colisson Elham Kashefi et Petros Wallden,
  QCRYPT 2018, 2018, Shanghai International Conference Center, Chine.
  https://www.youtube.com/watch?v=u8gUPcLyuPo

Présentations

I was in charge of presenting our works to the following international conferences:

- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson,
  ASIACRYPT 2023, 2023, Guangzhou, Chine.
  https://asiacrypt.iacr.org/2023/program.php
- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson,
  QCRYPT 2023, 2023, University of Maryland, États-Unis.
  https://www.youtube.com/watch?v=FKLAodM85jM
- **Security Limitations of Classical-Client Delegated Quantum Computing**.
  Léo Colisson,
  ASIACRYPT 2020, 2020, Online.
  https://www.youtube.com/watch?v=R0qk9tZ_VxA
- **On the possibility of classical client blind quantum computing**.
  Léo Colisson,
  QCRYPT 2018, 2018, Shanghai International Conference Center, Chine.
  https://www.youtube.com/watch?v=u8gUPcLyuPo

Invited tutorials

- **Tutorial: Basics of quantum information (3h)**.
  Léo Colisson,
  Spring School in Theoretical Computer Science EPIT, Marseille, 2021.
  https://conferences.cirm-math.fr/2341.html

Invited seminars

- **Oblivious Transfer from Zero-Knowledge Proofs, or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, *Quantum seminar QuasarLab, uOttawa*, 2023.
- **Oblivious Transfer from Zero-Knowledge Proofs, or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, *LIP6, Sorbonne Université*, 2023.
- **Oblivious Transfer from Zero-Knowledge Proofs, or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, *Séminaire RISC*[6]*, CWI Cryptology Group*, 2024.
  Finally cancelled due to schedule constraints
- **Diagrammatic reasoning, cryptography, and verification**.
  Léo Colisson, *Oxford ZX-Calculus Seminar, University of Oxford*, 2023.
  Video[7] (Password: DpD7P&C4).
- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, *Quantum Information Theory Seminar, UCL*, 2021.

Workshops

- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, *Workshop QuPa, Collègue de France, Paris*, 2021.
  Vidéo[8].
- **Quantum Analogue of Differential Privacy**.
  Léo Colisson, *Workshop Université d'Édimbourg, UK*, 2019.
- **Classical Simulation of Quantum Channels and Applications**.
  Léo Colisson, *Workshop QuRLInG, Prapoutel, France*, 2019.
- **On the possibility of classical client blind quantum computing**.
  Léo Colisson, *JIQ 2018, LORIA, Nancy*, 2018.

Lab Visits

I gave these presentations while visiting the following research groups:

- **Round-Optimal Quantum Oblivious Transfer and Diagrammatic Proofs of Security**.
  Léo Colisson, *Laboratoire d'Informatique de Grenoble (LIG) quantum seminars*, 2024.
- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, *QURIOSITY Team Seminar, Télécom, Saclay*, 2023.
- **Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States**.
  Léo Colisson, *GT Info-Quantique Seminars, LaBRI, Bordeaux*, 2023.
- **Round-Optimal Quantum Oblivious Transfer and Statistical Zero-Knowledge proofs on Quantum States**.
  Léo Colisson, *MOCQUA Seminars, LORIA, Nancy*, 2022.

[6] https://projects.cwi.nl/crypto/risc.php?y=2024

[7] https://bham-ac-uk.zoom.us/rec/share/SM743S9LzCmegIoYRs3ElFIy0iDxLN22w7ea3KtbLye0WyfBHUUUebyqhtozRVL_.DTwFHD0Vl3i2v9iE

[8] https://www.college-de-france.fr/fr/agenda/colloque/recent-advances-on-quantum-computing/non-destructive-zero-knowledge-proofs-on-quantum-states-and-multi-party-generation-of-authorized

- **Efficient and Provably Secure One-Time Memories Without Trusted Hardwares**.
  Léo Colisson, *QINFO Seminars, LIP, ENS Lyon*, 2022.
- **Study of Protocols Between Classical Clients and a Quantum Server**.
  Léo Colisson, *QuSoft Seminars, CWI, Amsterdam, Pays-Bas*, 2022.
- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, *Information Security Group (ISG) Seminars, Royal Holloway, University of London, UK*, 2020.
- **Classical simulation of quantum channel, and applications to blind quantum computing**.
  Léo Colisson, *Cryptography and Quantum Seminar, LIP, ENS Lyon*, 2019.

Posters

- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, *QCRYPT 2022*.
- **Non-Destructive Zero-Knowledge Proofs on Quantum States, and Multi-Party Generation of Authorized Hidden GHZ States**.
  Léo Colisson, *GDR IQFA 2021*.
- **Security Limitations of Classical-Client Delegated Quantum Computing**.
  Léo Colisson, *QCRYPT 2020 and QIP 2021*.
- **On the Possibility of Blind Quantum Computing**.
  Léo Colisson, *GDR IQFA 2018*.

SUPERVISION

2024 **Internship supervision**, *University of Amsterdam*, Master.
Supervisor of Yilun Wang (ongoing), student in the Master of Logic of the University of Amsterdam, on *Round-efficient Oblivious Transfer from one-way functions.*

2023 **Internship co-supervision**, *University of Amsterdam*, Bachelor.
Co-supervisor (50%), with Christian Schaffner of Ayed Ben Youb, student in Bachelor of Mathematics, on *Evaluating the practicality of Easycrypt by formally proving the security of CPA-secure encryption schemes.*

COLLECTIVE & ADMINISTRATIVE RESPONSIBILITIES

Workshop Organization

- **Workshop « QuRLInG »**, 2019.
  ↪ **Duration**: 5 days.
  ↪ **My role**: I was in charge of the **complete organization** of the workshop (searching for service providers, quotes, buses, accommodations, communication. . .).
  ↪ **Participants**: 25 researchers and students from 3 groups in Sorbonne Université, ENS Ulm and the LFCS (Laboratory for Foundations of Computer Science, Scotland).

Reviews STOC 2023, CRYPTO 2021, QIP (2019, 2020, 2023, 2024), QCRYPT (2022, 2023), Quantum (2022, 2023), Cryptography, TQC (2023), ITCS (2023)

Associative life Former head of the Salsa association at ENS Paris-Saclay, member of the Student Union Office (2015 – 2016, with responsibilities during the organisation of inter-ENS events), in charge of the website "La Nuit aNormale 2016" (gala ball).

TEACHING

2021
2023 **Modern Cryptography**, *University of Amsterdam*, Bachelor (3rd years).
Teaching assistant in a **flipped classroom** course given by Christian Schaffner. 46h per year (total: 92h).

- 2022-2023: https://datanose.nl/#course[110035]
- 2023-2024: https://datanose.nl/#course[120186]

2020
2021
Programmation C, *Sorbonne Université*, Bachelor (1st year).
Teaching assistant in the course given by Isabelle Mounier, 38.5h.

2019
2020
Introduction to cryptology, *Sorbonne Université*, Bachelor (3rd year).
Teaching assistant in the course given by Valérie Ménissier-Morain and Jeremy Berthomieu, 38.5h

2019
2020
Discrete mathematics, *Sorbonne Université*, Bachelor (2nd year).
Teaching assistant in the course given by Béatrice Bérard, 38.5h.

2018
2019
Introduction to cryptology, *Sorbonne Université*, Bachelor (3rd year).
Teaching assistant in the course given by Valérie Ménissier-Morain and Jeremy Berthomieu, 38.5h

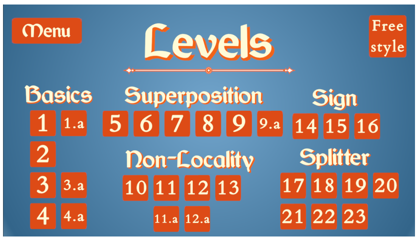
2018
2019
Programmation Python, *Polytech Sorbonne*, Bachelor (3rd year).
Teaching assistant in the course given by Xavier Tannier, 38.5h.

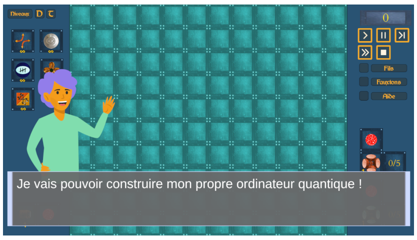
2018
2019
Programmation Python, *Polytech Sorbonne*, Bachelor (3rd year).
Teaching assistant in the course given by Xavier Tannier, 38.5h.

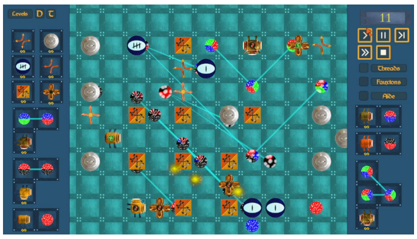
MEDIATION & VALORISATION

Mediation

- OptiQraft: Thanks to the QICS[9] (Quantum Information Center Alliance Sorbonne Université), I participated in the creation and development of the video game OptiQraft[10] with three other doctoral students and a professional designer (budget: 2000€). This game invites players to build a quantum computer through a series of 29 puzzles. In doing so, players can explore the basics of quantum information (superposition, entanglement, measurement, etc.) in a playful manner. The game was showcased during the Fête de la Science, 2021 edition[11], and the Festives[12] festival.




Je vais pouvoir construire mon propre ordinateur quantique !



I also developed other interactive mini-games to assist me during various tutorials I gave:

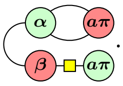
- a QKD mini-game[13],
- a mini-game[14] illustrating quantum pseudo-telepathy using Mermin-Peres's magic square[15].

[9] https://qics.sorbonne-universite.fr/
[10] https://tatawanda.itch.io/optiqraft
[11] http://www.fetedelascience.upmc.fr/
[12] https://www.sorbonne-universite.fr/lesfestives
[13] https://leo-colisson.github.io/qkd-game/
[14] https://github.com/tobiasBora/mermin-peres-magic-square
[15] https://en.wikipedia.org/wiki/Quantum_pseudo-telepathy

Valorisation Creation of multiple LaTeX library, useful to the community:

- zx-calculus[16]: LaTeX library generating ZX-calculs diagrams. For instance, the following code:

  ```
  \begin{ZX}
    \zxZ{\alpha} \dar[C] \rar[o'] \rar[o.] & [\zxHCol] \zxX*{a\pi} \\
    \zxX{\beta} \rar[H]                     & \zxZ*{a\pi}
  \end{ZX}
  ```

  will produce the following picture: .

- robust-externalize[17]: LaTeX library to cache images (generated via Ti*k*z, `zx-calculus`, python. . .) or arbitrary code:

  The for loop

  ```
  for name in ["Alice", "Bob"]:
      print(f"Hello {name}")
  ```

  Output:

  ```
  Hello Alice
  Hello Bob
  ```

- proof-at-the-end[18]: LaTeX library to easily move a proof in appendix, generating a link between the theorem and the proof.

PROFESSIONAL SKILLS

Softwares LaTeX/Ti*k*Z, Git, Emacs, Gimp, Blender, Inkscape, Kdenlive, LibreOffice.

Programmation Python, Ocaml, C(++), Haskell, Bash, Web, Fortran, SQL databases, LaTeX, etc.

OS Linux: NixOs maintainer (link to my Pull Requests[19])

INTERESTS

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

Travel Road-trips in Sri-Lanka, Cuba, China, Europe, United-Stated & more ecological local long distance hikes.

[16] https://github.com/leo-colisson/zx-calculus

[17] https://github.com/leo-colisson/robust-externalize

[18] https://github.com/leo-colisson/proof-at-the-end/

[19] https://github.com/NixOS/nixpkgs/pulls?q=is%3Apr+author%3AtobiasBora