PhD project at University Grenoble Alpes:

Formal cryptographic security proofs in a quantum world

Supervision: Mnacho Echenim[1], Andreas Bluhm[1], and Léo Colisson Palais[2]

[1]Laboratoire d'Informatique de Grenoble, Université Grenoble Alpes,
andreas.bluhm@univ-grenoble-alpes.fr mnacho.echenim@grenoble-inp.fr
[2]Laboratoire Jean Kuntzman (LJK), Université Grenoble Alpes,
leo.colisson-palais@univ-grenoble-alpes.fr

Application deadline: December 1st, 2026.
Starting date: January 1st 2027, at the latest.

Context. The continuous increase in the complexity of mathematical proofs, and the fact that Large Language Models (LLM) start to be able to write plausible complex proofs, urges us to develop formal proof systems that can automatically verify the veracity of a proof. While well established generic formal proof systems already exist (Lean, Rocq, Isabelle...), they lack libraries taking into account the specificities of cryptographic protocols, for instance to quantify over multiple arbitrary polynomial-time communicating quantum Turing machines, oracles... While more specialized tools exist (Easycrypt, CryptoVerif...), they are unable to model the specificities that occur when adversaries are allowed to be quantum[1], or when the protocol itself involves quantum parties. Moreover, the proofs obtained in these frameworks are typically fairly complex to write and understand, and bring an extra layer of complexity.

The thesis. The goal of this thesis will be to explore a different approach to write formal security proofs, inspired by the ZX-calculus [1, 3], a diagrammatic language originally used to reason more efficiently about quantum processes. The goal of this framework (currently in construction) will be to allow users to write security proofs, not only taking into account the subtleties of quantum computing, but also allowing users to design cryptographic protocols more efficiently. More precisely, the hired PhD student will be involved (at various degrees) in:

- the design of this formal security framework,
- the implementation of this framework in the web software that is currently under being built, which involves compiling proofs to other existing formal proof systems,
- the automatic generation of such security proofs based on automated reasoning techniques tailored to reason about graphs, extending methods introduced in [2].

Candidate profile. We are looking for a PhD candidate who is highly motivated to work on problems at the intersection of mathematics, quantum computing, and computer science. The candidate must have a master degree in either mathematics or computer science. Some familiarities with formal proof systems, quantum computing and/or cryptography are highly welcome. Moreover, the candidate should have a good working knowledge of linear algebra, be able to write rigorous mathematical proofs, and be motivated to acquire any mathematical skills they might need during the course of the project. If you have any questions, please don't hesitate to get in touch!

Application procedure. Please send an email containing a letter of motivation and your CV to Mnacho Echenim (contacts above). Moreover, please ask a suitable reference to send a letter of recommendation directly to the same address.

[1]E.g. it is impossible to model a simple oracle that can be queried in superposition.

References

[1] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.

[2] Rachid Echahed, Mnacho Echenim, Mehdi Mhalla, and Nicolas Peltier. A strict constrained superposition calculus for graphs. In Orna Kupferman and Pawel Sobocinski, editors, *Foundations of Software Science and Computation Structures - 26th International Conference, FoSSaCS 2023.*, volume 13992 of *Lecture Notes in Computer Science*, pages 135–155. Springer, 2023.

[3] John van de Wetering. ZX-calculus for the working quantum computer scientist. 2020.