Theory and simulation of secure delegated quantum computation protocol in a network perspective

Type : Theoretical & numerical
Supervisors : Maxime Garnier and Harold Ollivier
Contact : qat-hiring@inria.fr

Introduction

Within the development of quantum technologies (quantum computing and quantum networks), secure delegated computing stands out as a promising application. The aim of delegating a computation is to allow a Client with few ressources to have its computation securely executed by a more powerful Server. In the quantum setting, studying its feasibility is both interesting and timely as it is unlikely that end-users will own and operate quantum computers on premises in the near future. Thus, it is reasonable to suppose that most near-term quantum computations will be delegated.

The Quantum Internet Alliance (QIA) is a European project aiming at developing and deploying the first pan-European quantum communication network, linking nodes separated by several kilometers to more than 100 km. To this end, all aspects from the hardware, the control software as well as the potential applications are considered. In this perspective, quantum delegated computation has been chosen, among others, as a guiding tool to develop both the network and the protocols. Among the variety of protocols available, it is the robust, verifiable and blind (rVBQC) protocol[1] that has been targeted due to its robustness to noise as well as its low verification overheads leading to its potential applicability to noisy devices.

Practical aim of the project

The main objective of our work is to design photonic Clients with as few quantum ressources as possible. This requires both a precise understanding of the theoretical aspect of the protocols and a knowledge of the current hardware limitations. Hence, the task is more a co-design one: hardware limitations can suggest protocol modifications (retaining its guarantees) while theoretical aspects can also inform hardware implementation. The final aim being the real-life implementation of the Clients delegating a secure quantum computation within QIA.

Concrete tasks

To do so, we plan to use detailed high-level modeling (noise and imperfections included) and simulation of the setup that allows to investigate the main functionalities of the protocol. In a nutshell, several tasks will be conducted:

- High-level modeling of the setup and its imperfections

[1] Leichtle, Music, Kashefi and Ollivier for the original proposal and subsequent work for extensions.

- Investigating modifications to both the setup and the protocol in order to increase feasability while retaining the theoretical guarantees
- Assessing the performances of all the versions of the protocol and the hardware via quantum information theory tools as well as numerical simulations
- Numerical calculations and simulation at several levels will be carried out:
    - Density matrix numerical calculations using simulation frameworks such as graphix or strawberryfields,
    - Global network simulations using SquidASM (provided and developed by QIA) which aims at developing and assessing applications for QIA's quantum network.

Environment

The succesful applicant will work within the newly created Quantum Applications and Theory QAT Inria team working at the interface between computer science, quantum information theory and physics. The team is located in the Computer Science of École Normale Supérieure, 45 rue d\'Ulm, Paris, France. The successful candidate will be working with researchers from diverse backgrounds such as computer scientists and theoretical and experimental physicists. The project may also lead to interaction with other stakeholders (startup companies, end-users, ...) within the QIA project. You will participate in a truly ambitious and vibrant European project.

Profile

- Applications from students trained in quantum information, theoretical physicists or computer science will be considered.
- Master-level quantum background mandatory, quantum information training appreciated.
- Taste and skills for programming required (mostly Python).
- Open-mindedness and communication skills necessary to interface with others.

Depending on the results and the candidate, the internship may lead to a PhD or a software engineer position.