

Appel à candidature pour un stage : Expériences sur l'algorithme de Shor et améliorations

L'algorithme de Shor est un algorithme quantique permettant de calculer efficacement la période d'une fonction dans un groupe abélien. Son application la plus connue et la plus préoccupante concerne la factorisation des entiers : cet algorithme pourrait résoudre ce problème en temps polynomial, rendant ainsi obsolètes les cryptosystèmes actuels largement déployés. Les agences de régulation estiment qu'un risque majeur existe à l'horizon 2035.

L'implémentation pratique de cet algorithme se heurte toutefois à deux difficultés majeures. D'une part, le ratio entre le nombre de qubits physiques nécessaires et celui de qubits logiques disponibles constitue un frein important. D'autre part, la profondeur du circuit quantique doit rester compatible avec le temps de cohérence des qubits : au-delà de cette limite, le phénomène de décohérence entraîne une perte d'information rendant l'exécution impossible.

L'approche proposée ici relève du calcul hybride combinant calcul quantique et calcul classique (HQI/HPI).

Objectifs du stage

Ce stage vise à proposer une implémentation de l'algorithme de Shor et à étudier puis développer des améliorations pratiques sous forme de circuits quantiques, en utilisant un langage de programmation tel que Qiskit. Le défi principal consiste à concevoir un circuit capable d'exécuter l'ensemble de ses portes quantiques dans le temps de cohérence disponible, répondant ainsi à la seconde difficulté évoquée précédemment.

La conception de circuits quantiques réalistes représente une étape cruciale pour le développement de l'informatique et de la programmation quantique.

Déroulement du stage

Le stage commencera par la réalisation d'une implantation de l'algorithme de Shor.

Dans un deuxième temps, on adaptera une méthode algorithmique appelée « fenêtre glissante » (« sliding windows ») qui permet de garder des valeurs sous forme de tables qui, bien qu'elle ne soit pas en complexité constante, est suffisamment efficace pour réduire significativement le nombre de portes du circuit quantique.

Enfin, on étudiera l'implantation d'une version améliorée qui distribue l'ensemble des portes quantiques du circuit en plusieurs exécutions s'exécutant chacune dans le temps de cohérence des qubits. Les résultats des différentes exécutions sont alors combinées par du calcul classique après coup.

Modalités du stage

Il s'agit d'un stage de 5 à 6 mois. La gratification est de 660 € par mois.

Encadrements : Razvan Barbulescu (équipe-projet CANARI INRIA Bordeaux) et Olivier Ruatta (équipe CRYPTIS MATHIS/XLIM et équipe-projet CANARI INRIA Bordeaux).

Le ou la stagiaire sera basé-e à Bordeaux et une mobilité est prévue à Limoges.

Compétences attendues

Les compétences attendues sont les bases de l'informatique quantique (notions de qubits, portes etc), l'algorithmique et la programmation `Python`.

Il conviendra d'avoir un goût pour l'algorithmique et la programmation en plus d'une formation minimale sur l'algorithmique quantique. Néanmoins la maîtrise d'un langage comme Qiskit n'est pas un préalable indispensable.

Contact : Pour postuler, contacter olivier.ruatta@unilim.fr et razvan.barbulescu@u-bordeaux.fr

Bibliographie

- [Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS'94), pages 124–134. IEEE, 1994.
- [CFS25] Clémence Cheignard, Pierre-Alain Fouque, André Schrottenloher. [Reducing the number of qubits in quantum factoring](#). Annual International Cryptology Conference. Springer Nature Switzerland, pages 384–415, 2025.