COMITE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Conseil scientifique de l'Institut des sciences de l'information et de leurs interactions (INS2I)

Recommandations résultant du séminaire « Calcul et cryptographie quantique »

Le Conseil Scientifique de l'Institut CNRS des Sciences de l'Information et de leurs Interactions (INS2I) a organisé le 28 septembre 2022 un séminaire sur calcul quantique et cryptographie quantique, afin de comprendre les nouveaux défis de l'informatique quantique, qui est devenue l'un des axes scientifiques stratégiques dans le pays et en Europe, et de dégager des recommandations pour l'institut.

Quatre intervenants se sont exprimés : Frédéric Magniez (DR CNRS, IRIF) : « Algorithmes quantiques : état de l'art et perspectives», Elham Kashefi (Professeur à l'University of Edinburgh, DR CNRS au LIP6 Sorbonne University) : « Quantum Computing as a Service: Secure and Verifiable », Romain Alléaume (PR Telecom Paris, LTCI) : « La cryptographie quantique à la croisée des chemins », et enfin Olivier Blazy (PR Ecole Polytechnique, LIX) : « Panorama des approches et enjeux de la cryptographie post-quantique ».

Au cours des dernières décennies, il a été établi que la possibilité d'encoder des informations sur des supports physiques quantiques, et de les manipuler en tant que tels, apporte des avantages importants pour l'échange de clés cryptographiques (à court terme), ainsi qu'en termes de simulation (à moyen terme) et d'algorithmique quantique (à plus long terme). Certaines applications ont déjà été développées (par exemple la métrologie quantique), et d'autres commencent à émerger (par exemple le *green computing*). Au-delà des applications fascinantes et des méthodes nécessaires pour les réaliser, ce domaine interroge la nature même de l'information et son rôle dans les fondements de la physique. Conscients des obstacles technologiques et scientifiques, et des immenses bénéfices qu'il y aurait à les lever, de nombreux états investissent massivement dans ce domaine. Deux grandes stratégies semblent se dessiner. Le Canada, Singapour, les Pays-Bas et le Royaume-Uni ont successivement opté pour la création de grands centres de recherche internationaux (IQC, PI, CQT, QuTech, UK Quantum hubs). En mettant en place une communication scientifique passionnante et des salaires attractifs, ces centres attirent les grands noms de la recherche en information quantique et alimentent de nombreuses startups (ex : D-Wave, Riverlane, CQC...). À leur manière, la Chine et les États-Unis ont annoncé des "plans quantiques" massifs. La Chine mène une politique de grands projets, comme la mise en place du premier réseau de cryptographie quantique par satellite, QUESS. Les États-Unis, en plus de leur National Quantum Initiative Act, bénéficient de l'engagement des majors. Microsoft et IBM mènent depuis des années des recherches de pointe, tant sur le plan théorique (MS Station Q) que pratique (IBM Q Experience). Arrivé plus récemment dans la course, Google a declaré de pouvoir franchir la barrière de la suprématie quantique en 2019 : pour la première fois, un ordinateur quantique a exécuté une tâche algorithmique de manière spectaculairement plus rapide que les algorithmes classiques les plus connus. Les projets de Google visent désormais à construire, d'ici dix ans, un ordinateur quantique avec des milliers de qubits

physiques, et mettre en œuvre la correction quantique des erreurs afin d'obtenir quelques centaines de qubits logiques parfaits. La France, quant à elle, compte un certain nombre de résultats de recherche marquants en physique expérimentale : démonstration de l'intrication par Alain Aspect, piégeage de l'atome par Claude Cohen-Tannoudji, maîtrise de leur interaction par Serge Haroche, tous trois lauréats du prix Nobel de Physique. Mais elle compte également des contributions importantes en informatique : en algorithmique quantique (*binary welded trees*, *recommendation systems*, ...), en cryptographie quantique (*key exchange*, *secret sharing*, *blind computing*, ...), ou encore en simulation quantique. Du côté de la recherche privée, Atos, leader mondial des logiciels, a annoncé en 2016 la création de sa division Atos Quantum. Cette division vise précisément à développer des logiciels intermédiaires pour optimiser les ressources nécessaires à l'informatique quantique, et se positionne rapidement comme un leader mondial de la simulation classique et quantique. Elle est actuellement la seule "major" européenne dans ce secteur. Quelques start-ups émergent également, comme CryptoNext, Alice&Bob, Pasqal, Quandela, QuantFi et Veriqloud. Récemment, le gouvernement a annoncé un plan stratégique national pour rattraper le retard de la France dans ce domaine, ainsi que pour en faire un leader mondial. Cela se traduit par un investissement de plusieurs millions d'euros qui a permis de lancer plusieurs appels à projets nationaux (e.g. PEPR) sur tous les piliers fondamentaux de l'informatique et des technologies quantiques. Un autre point qui a été également souligné lors du séminaire est l'interdisciplinarité. Dans ce domaine, physique et informatique sont étroitement liées. Cela est dû principalement à la faible indépendance de l'informatique quantique par rapport au matériel ("hardware Independence"), qui rend encore plus difficile la compréhension de l'informatique quantique.

Pour la première fois dans l'histoire de l'informatique, le sacro-saint principe de "hardware Independence" a été ébranlé. Le matériel physique est redevenu fondamental, car il conditionne toute la logique de l'algorithme. Il faut donc être très attentif au choix du système physique, à son initialisation et à sa mesure. Alors que l'informatique classique a rapidement réussi à s'affranchir de la machine physique, dans l'informatique quantique cela semble difficile, voire impossible. Une collaboration étroite entre les deux communautés est nécessaire, car les nouvelles questions posées se situent précisément à la frontière entre l'informatique et la physique. En effet, si avec l'avènement des ordinateurs modernes on a assisté à une séparation progressive des informaticiens, des physiciens et des mathématiciens, l'informatique quantique soulève de nouvelles questions intimement à la frontière entre la physique et l'informatique théorique.

Comme dans toute révolution scientifique, il est nécessaire que les universités forment et mènent des recherches dans ce domaine. Et cela implique en particulier que ces liens forts entre physique et informatique soient présents dès la formation des futurs chercheurs ou ingénieurs. Récemment, un projet d'envergure a été approuvé par le gouvernement, QuantEduFrance, qui distribue plus de vingt millions d'euros pour développer de nouvelles formations entre les départements de physique et informatique, à tous les niveaux, de la formation initiale à la formation continue. Dans les années à venir, ce genre de projets permettront de développer des formations de haut niveau à cheval sur les départements de physique et d'informatique, comme le master "Information quantique" de la Sorbonne inauguré il y a deux ans.

COMITE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

A la lumière de ce séminaire, le CSI formule les recommandations suivantes à destination de l'INS2I:

- L'informatique quantique touche toutes les disciplines classiques de l'informatique qui sont du ressort de différents GDRs. Malgré cela, il semble nécessaire de proposer des formations à tous les personnels de la recherche afin de sensibiliser aux questions du calcul quantique et ses conséquences techniques et sociétales, de façon à pouvoir intervenir aussi bien dans l'espace public/médiatique que dans le monde de l'éducation et de la recherche.

- Face aux différents acteurs privés et aux autres organismes de recherche, le CNRS peine encore à recruter, laissant souvent nos meilleurs étudiants s'échapper ailleurs. Il est donc nécessaire de suivre les besoins exprimés localement et de proposer un plan de recrutement adéquat au niveau national.

- Compte tenu de la nature interdisciplinaire de l'informatique quantique, prévoir des espaces de discussion et de coordination avec d'autres instituts intéressés (tels que l'INP) sur les politiques de recrutement, la formation du personnel et les projets de vulgarisation.

- Bien que l'algorithmique et les codes quantiques soient représentés ponctuellement dans des groupes de travail de certains GDRs dépendant de l'INS2I, il n'y a qu'un seul GDR en France qui traite pleinement de la technologie et de l'informatique quantiques, le GDR TEQ, qui n'a pour l'instant pas de lien avec l'INS2I. Il semble nécessaire que l'INS2I se rapproche de ce GDR et du principal institut de référence (INP) afin de jouer un rôle moteur dans le développement de l'informatique quantique en France.

- Les décideurs (politiques) devraient prendre l'avis des scientifiques en priorité sur l'avis des entreprises.

Gilles SASSATELLI
Président du Conseil scientifique de l'INS2I

Recommandation adoptée le 8 décembre 2023

Vote : 20 oui / 20 votants

Destinataires :

- M. Antoine PETIT, président-directeur général du CNRS
- M. Alain SCHUHL, directeur général délégué à la science du CNRS
- Mme Adeline NAZARENKO, directrice de l'Institut des sciences de l'information et de leurs interactions (INS2I)
- M. Olivier COUTARD, président du Conseil scientifique du CNRS
- M. Fabien JOBARD, président de la Conférence des présidents du Comité national (CPCN)

- Mme Christine ASSAIANTE, porte-parole de la Coordination des responsables des instances du CoNRS (C3N)
- Mme Claudine GILBERT, présidente du CSI de l'Institut de physique (INP), M. Olivier DRAPIER, président du CSI de l'Institut national de physique nucléaire et de physique des particules (IN2P3), M. Serge SIMOENS, président du CSI de l'Institut des sciences de l'ingénierie et des systèmes (INSIS), Mme Beatrice MARTICORENA, présidente du CSI de l'Institut national des sciences de l'Univers (INSU), M. Olivier SANDRE, président du CSI de l'Institut de chimie (INC), Mme Nathalie VIENNE-GUERRIN, présidente du CSI de l'Institut des sciences humaines et sociales (INSHS), M. Yaël GROSJEAN, président du CSI de l'Institut des sciences biologiques (INSB), M. Remi CARLES, président du CSI de l'Institut national des sciences mathématiques et de leurs interactions (INSMI), Mme Patricia GIBERT, présidente du CSI de l'Institut écologie et environnement (INEE)