

Quantique et codes secrets : la course contre la montre

(Enregistré le 06 novembre 2026)

Introduction

Les transactions bancaires en ligne, les valeurs échangées et stockées sur des blockchains, les communications militaires et les secrets d'État reposent sur des codes secrets, des codes mathématiques si complexes qu'il faudrait des milliards d'années aux ordinateurs actuels pour les casser. Mais un ordinateur quantique pourrait venir à bout de certains d'entre eux en quelques heures. Personne ne sait quand une telle machine verra le jour, ni même si elle le verra. Mais les experts parlent tout de même d'une course contre la montre. En effet, des données volées aujourd'hui pourraient être déchiffrées demain. Alors que des entreprises annoncent régulièrement progresser vers un avantage quantique, d'autres acteurs imaginent des parades, et la physique quantique elle-même promet de nouveaux codes secrets écrits avec de la lumière.



Ordinateur quantique, la fin des codes secrets ? Pour en discuter, je reçois Olivier Lantran, responsable du Lab, le Centre d'Innovation de la Banque de France. Bienvenue dans Dialogue Eco.

Qu'est-ce que le quantique ?

LUCILE RIVES : Pour nous accompagner dans ce défi de parler de quantique le plus simplement possible, j'ai choisi Serge Haroche qui est physicien et co-lauréat du prix Nobel de physique en 2012. Je vous propose d'écouter un passage de la leçon inaugurale qu'il a donnée au Collège de France le 13 décembre 2001.

SERGE HAROCHE : Monsieur l'administrateur, mes chers collègues, Mesdames et Messieurs, « Personne ne comprend vraiment la physique quantique ». Ce jugement du physicien Richard Feynman exprime une vérité paradoxale sur la théorie scientifique qui a révolutionné notre compréhension du monde et qui a enrichi d'une façon extraordinaire nos moyens d'action et d'information sur lui. Dans cette première leçon, je vous parlerai donc de physique quantique, en

tentant de résoudre ce paradoxe, et si je n'y parviens pas, la boutade de Feynman nous laissera au moins la consolation de nous sentir en nombreuse compagnie.

LUCILE RIVES : Olivier Lantran, c'est ma première question : pourquoi personne ne comprend vraiment la physique quantique ?

OLIVIER LANTRAN : Si personne ne comprend, c'est une sacrée gageure pour moi d'essayer de l'expliquer à tout le monde ! Ce qu'il y a d'un peu vertigineux avec la physique quantique, c'est qu'elle fait appel à des choses qui ne sont pas naturelles dans notre quotidien. Ce sont des règles qui régissent l'infiniment petit et qui ont des répercussions sur l'infiniment grand, mais que l'on ne voit pas dans notre vie de tous les jours : nous sommes dans une sorte d'entre-deux, entre la particule et les astres. Les manifestations quantiques ne se perçoivent pas. Autant les effets de la physique newtonienne, avec les pommes qui tombent des arbres, peuvent se constater, autant, pour les différents états d'une particule, il faut un peu d'imagination et certaines preuves physiques concrètes qui ne s'observent qu'en laboratoire.

LUCILE RIVES : Ce sont donc des lois qui ne sont pas observables. Pouvez-vous nous dire ce qu'est la superposition des états en physique quantique ?

OLIVIER LANTRAN : Il y a deux propriétés très importantes en physique quantique : la superposition et l'intrication, sur laquelle nous reviendrons sans doute plus tard. Un bon exemple pour la superposition est celui de la pièce de monnaie. Vous prenez une pièce, vous la regardez : il y a un côté pile et un côté face. Mais si vous la faites tourner sur la table, tant qu'elle tourne, elle n'est ni pile ni face, elle est potentiellement un peu des deux. Ce n'est que lorsqu'elle s'arrête de tourner et tombe d'un côté ou de l'autre que l'on peut observer l'état dans lequel elle se trouve, et c'est à ce moment-là que sa valeur est fixée. La physique quantique s'appuie sur ces différents états : le pile, le face, et cet état où l'on superpose les deux tant que la pièce n'a pas fini de tourner. C'est avec ces modèles mathématiques de probabilité que l'on parvient à gérer plusieurs états superposés, ce qui a une influence considérable sur la façon d'appréhender certains systèmes complexes et de réaliser des calculs complexes.

LUCILE RIVES : Vous avez mentionné un autre grand concept associé à la physique quantique : l'intrication. Qu'est-ce que l'intrication ?

OLIVIER LANTRAN : Je pense que l'intrication est un concept encore moins intuitif que le précédent. Il peut se comprendre, même si l'on se demande comment cela peut fonctionner. Je reste avec mes pièces de monnaie. Imaginez que vous avez deux pièces et que vous êtes capable de dire que, lorsque vous les faites tourner, si l'une tombe sur pile, l'autre aussi, systématiquement, qu'elles soient l'une à côté de l'autre ou à des centaines de millions de kilomètres. C'est ce qu'on appelle des états intriqués de la matière : on dit que les deux pièces sont intriquées et qu'elles vont avoir un comportement similaire. Je disais que ce n'était pas forcément intuitif : figurez-vous qu'Einstein trouvait cela inacceptable, il n'y croyait pas. Ce n'est qu'assez récemment qu'Alain Aspect a démontré expérimentalement le fonctionnement de l'intrication, ce qui lui a valu le prix Nobel en 2022.

Une application : l'informatique quantique

LUCILE RIVES : Qu'apporte la connaissance de ces propriétés des objets atomiques, en termes d'applications, dans les objets que l'on utilise tous les jours ?

OLIVIER LANTRAN : Cela ouvre des perspectives très intéressantes. Prenons l'informatique que l'on connaît : elle repose sur quelque chose d'assez simple. Soit le courant passe dans les circuits, soit il ne passe pas. On a donc des composants qui sont soit à 0, pas de courant, soit à 1, il y a du courant, et avec cela on modélise le monde entier. Tous les traitements qui tournent aujourd'hui, l'intelligence artificielle de n'importe quelle génération, reposent à la base sur des zéros et des uns. Avec les théories quantiques, on peut dépasser cette limitation du 0 et du 1. Si l'on dit que 0, c'est pile, et 1, c'est face, pour reprendre mon analogie de la pièce de monnaie, on va avoir des unités élémentaires de calcul qui pourront valoir soit 0, soit 1, soit une superposition probabiliste des deux. C'est justement ce qui permet de paralléliser beaucoup plus facilement des calculs complexes. Si, en plus, vous avez la capacité de répliquer cela avec l'intrication à plus ou moins grande échelle, vous pouvez démultiplier ces calculs avec une consommation de ressources, et notamment d'énergie, beaucoup plus faible que ce que l'on sait faire aujourd'hui. Pour autant, ce n'est pas magique. Présenté ainsi, on a l'impression que cette deuxième révolution quantique dont nous parlons est de nature à tout changer. Ses capacités et ses propriétés physiques sont très pertinentes pour certains types de calculs : comme je le disais, des calculs très complexes, avec des données et des informations très distribuées. Elles ne présentent pas forcément d'avantage significatif pour le calcul classique. En revanche, le quantique, en complément, va être capable de traiter des sujets que l'on considérait comme hors d'atteinte pour les systèmes numériques et automatisés dont on disposait jusqu'à présent.

LUCILE RIVES : Qu'est-ce qui fait la différence entre la première et la deuxième révolution quantique ? Pourquoi parle-t-on de deuxième révolution quantique ?

OLIVIER LANTRAN : Lors de la première révolution quantique, on a utilisé les propriétés quantiques et physiques telles que la matière les offre naturellement. Ces propriétés contribuent à des mécanismes physiques que l'on a utilisés tels quels pour transmettre des signaux, se connecter à des satellites ou faire des examens médicaux avec une IRM. Avec la deuxième révolution quantique, on va au-delà : on travaille directement sur des atomes, sur des photons, les particules élémentaires de lumière, et l'on joue sur ces particules pour forcer des comportements et, finalement, les manipuler comme des objets que l'on manipulerait au quotidien. On est vraiment à l'échelle atomique de la matière, et c'est là la grande différence : avant, on ne savait pas faire cela.

LUCILE RIVES : On entend beaucoup parler de révolution technologique en ce moment. L'intelligence artificielle, c'est l'autre révolution technologique du moment, et il serait assez facile de confondre les deux. Qu'est-ce qui distingue l'intelligence artificielle de l'informatique quantique ? En quoi ces deux technologies sont-elles très différentes ?

OLIVIER LANTRAN : Ce sont effectivement des technologies très différentes. L'intelligence artificielle générative calcule la réponse la plus probable lorsque vous lui posez une question. Ce sont donc des probabilités. Elle infère des réponses à partir de modèles pré-entraînés, avec des algorithmes, et elle

est en plus branchée sur l'ensemble des masses de données dont on dispose aujourd'hui via Internet et d'autres sources plus spécialisées. Mais on reste sur des objets mathématiques classiques et des capacités de calcul classiques. Le quantique, lui, se situe sur le segment du matériel, du « composant électronique », qui va permettre de faire tourner des algorithmes. On parlait tout à l'heure du photon : il existe différents types de machines quantiques, basées sur la lumière, sur le silicium. Il y a aujourd'hui différentes familles de machines, et elles permettent de faire des calculs. Elles ne permettent pas, intrinsèquement, de répondre aux demandes qu'on leur adresse, comme le fait l'intelligence artificielle. C'est donc le matériel contre le logiciel.

LUCILE RIVES : Oui, l'informatique quantique, c'est du hardware.

OLIVIER LANTRAN : Oui, mais pas seulement. C'est avant tout du hardware, du matériel. Mais la nature de ce matériel et la façon dont il fonctionne – superposition, intrication, etc. – ont une influence sur la façon dont on l'utilise. On ne programme pas une machine quantique comme on programme un ordinateur classique. La façon d'écrire les programmes et les algorithmes est différente : il existe des algorithmes pour le quantique qui ne sont pas ceux de l'informatique classique. On se dit souvent : « C'est formidable, l'informatique quantique ! On va prendre tout ce qu'on a aujourd'hui, le faire tourner sur des ordinateurs quantiques, et ça ira plus vite, ce sera plus pertinent. » Pas du tout ! On ne peut pas prendre ce qui tourne sur un ordinateur classique pour le faire tourner sur un ordinateur quantique. Ce que l'on fait tourner sur un ordinateur quantique, ce sont des programmes conçus spécialement pour lui. Il y a donc aussi une partie logicielle qui accompagne ce hardware quantique et qui doit être conçue de façon spécifique.

Opportunités et risques de l'informatique quantique

La simulation de la nature

LUCILE RIVES : Et alors, quel genre de problèmes vise-t-on à résoudre avec un ordinateur quantique ?

OLIVIER LANTRAN : On parle souvent de vitesse, mais l'ordinateur quantique ne va pas faire plus vite tout ce que font nos ordinateurs. La vraie rupture, c'est qu'il va ouvrir des calculs qui sont aujourd'hui hors de portée. En pratique, un ordinateur quantique est capable de prendre en compte la complexité d'un système. Prenons les molécules : ce sont beaucoup d'interactions, beaucoup de composants atomiques. Pour un ordinateur classique, c'est trop, il ne peut pas calculer cela. L'ordinateur quantique, lui, le peut, puisque ses ressorts et ses mécanismes de fonctionnement sont en quelque sorte le miroir des systèmes sur lesquels on le fait travailler.

L'usage le plus solide exploré aujourd'hui, c'est tout ce qui relève de la simulation de la nature, pour ainsi dire : concevoir de nouveaux médicaments, travailler sur les prochaines générations de batteries ou, dans le domaine agricole, sur des engrais plus vertueux que par le passé. Pour tout cela, les machines quantiques sont pertinentes, alors qu'avec des ordinateurs classiques, il faudrait des batteries de machines en parallèle qui, comme je le disais, n'arriveraient pas forcément au bout, étant donné la complexité de tout ce qu'il faut gérer.

LUCILE RIVES : Si je nous replace dans notre position de banque centrale, ce que vous décrivez me fait beaucoup penser aux stress tests. Est-ce une application possible si, un jour, on dispose d'un ordinateur quantique ? C'est aussi un sujet qu'il faudra aborder.

OLIVIER LANTRAN : C'est un vrai sujet, et c'est déjà un sujet d'étude pour les banques centrales : la façon de faire de l'analyse de risques et des stress tests à l'aide de machines quantiques. Toute problématique qui nécessite des calculs intensifs mérite d'être examinée sous l'angle des capacités d'une machine quantique. Tout ne sera pas forcément optimal, et sur certains sujets, c'est peut-être une combinaison d'ordinateurs classiques et d'ordinateurs quantiques qui répondra le mieux au problème. Mais oui, la mesure du risque par la simulation de milliers de scénarios, c'est intéressant. Tous les travaux d'optimisation, qu'il s'agisse de l'optimisation de portefeuille ou du traitement des transactions dans les systèmes de règlement, sont intéressants.

Cela dit, soyons honnêtes : les gains sont encore incertains, ils n'ont pas encore été complètement démontrés. Les machines quantiques qui permettent de faire ces calculs à l'échelle, on ne les a pas encore, et beaucoup d'usages que l'on identifie aujourd'hui ne résisteront probablement pas à l'épreuve quand on disposera de ces machines. C'est normal, c'est une technologie naissante. Notre travail, c'est justement d'anticiper ces éléments pour pouvoir ensuite faire un tri efficace.

Je reviens rapidement sur un point : quand on dit qu'on n'a pas d'ordinateur quantique, en réalité, il en existe. Aujourd'hui, à la Banque de France, nous travaillons avec des collègues du centre de calcul du CEA pour faire tourner de premiers algorithmes sur des machines quantiques. Mais il reste du chemin pour avoir des machines utilisables de façon industrielle, en production et à l'échelle. Je ne me lancerai pas dans une projection en disant qu'elle sera disponible à telle date, parce que des gens beaucoup plus experts que moi en la matière n'avancent pas de date. Ce n'est donc pas moi qui vais le faire. Il existe toutefois aujourd'hui un consensus sur le fait que cette machine sera accessible quelque part entre 2030 et 2035.

LUCILE RIVES : C'est un consensus ?

OLIVIER LANTRAN : Oui, cela fait aujourd'hui partie des éléments qui figurent dans les roadmaps institutionnelles, au niveau du G7 et au niveau des instituts nationaux de sécurité.

Mais pour revenir à la machine quantique elle-même, l'enjeu aujourd'hui, c'est la correction d'erreurs. Les machines quantiques telles qu'elles sont conçues aujourd'hui s'appuient vraiment sur les états de la matière. Or, travailler sur cette matière nécessite de maintenir des conditions physiques très particulières : des froids très intenses ou des environnements sous un vide parfait et absolu. Ce sont des états très difficiles à atteindre et surtout à maintenir dans le temps. On peut donc avoir des variations d'état qui génèrent du bruit, de nature à fausser les calculs. Cela me permet d'ailleurs de faire un lien, que nous n'avons pas évoqué tout à l'heure, avec l'intelligence artificielle. Car l'intelligence artificielle peut aussi se mettre au service du quantique : elle peut jouer un rôle très pertinent dans la gestion de ces erreurs, de ce bruit, pour renforcer la performance et la pertinence des calculs de ces machines quantiques.

LUCILE RIVES : En préparant l'épisode, j'ai eu l'occasion de regarder à quoi ressemble un ordinateur quantique aujourd'hui. C'est très beau, c'est doré, on dirait un grand lustre.

OLIVIER LANTRAN : Oui, je vois l'image que vous avez en tête. Mais il faut savoir qu'il existe plusieurs formes de machines quantiques, selon la technologie, le hardware sous-jacent utilisé.

La cryptographie

LUCILE RIVES : Et quand bien même nous n'aurions pas encore d'ordinateur quantique, une autre application est souvent évoquée et inquiète : la cryptographie, et la capacité qu'auront – je ne dis même pas « qu'auraient », parce que j'ai l'impression que c'est une certitude – les ordinateurs quantiques à casser les codes secrets qui existent aujourd'hui. Est-ce une vraie menace, peut-être en priorité dans le domaine économique et bancaire ?

OLIVIER LANTRAN : En fait, tout ce qui repose aujourd'hui sur du chiffrement, sur de la cryptographie, peut être concerné par cette « menace quantique ».

LUCILE RIVES : On parle donc beaucoup de la blockchain, mais en fait, tout le monde est concerné.

OLIVIER LANTRAN : Tout le monde est concerné : quand vous payez par carte, quand vous vous connectez à votre banque sur votre espace client ou quand deux banques s'envoient des ordres de paiement, tout cela est protégé par de la cryptographie. Elle sert à deux choses : chiffrer les échanges et signer, c'est-à-dire prouver son identité, prouver qui l'on est. Cette sécurité a toujours reposé sur des problèmes mathématiques réputés très difficiles. Par exemple, multiplier deux grands nombres premiers, c'est facile. En revanche, si on vous donne le résultat de cette multiplication, retrouver les nombres qui ont servi à la multiplication est beaucoup plus compliqué avec des ordinateurs classiques. Ce n'est pas impossible, mais c'est extrêmement long.

Ce qui s'est passé en 1994, c'est qu'un mathématicien américain, Peter Shor, a conçu un algorithme qui, avec un ordinateur quantique suffisamment puissant, est capable de faire ces décompositions en nombres premiers de façon très rapide. Ce qui aurait pris des milliards d'années pourrait se faire en quelques jours, voire moins avec les optimisations en cours. C'est là que la menace devient réelle, d'où la fenêtre 2030-2035 que j'évoquais tout à l'heure. Ne serait-ce qu'en France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a émis des recommandations : d'ici à 2030, il faut avoir mis en place des systèmes permettant de se protéger de ce type de menace, et faire en sorte que les fournisseurs soient challengés afin de bénéficier de niveaux de protection qui permettent de se prémunir contre ce genre de risques.

Pour autant, cette menace est réelle dès aujourd'hui, même si la machine suffisamment puissante n'est pas encore là, et même si l'on ne connaît pas exactement la date à partir de laquelle cet ordinateur sera disponible, ce qu'on appelle le Q-Day. Le risque est déjà présent. Pourquoi ? Parce que, parmi toutes les données protégées par du chiffrement, il y en a qui ont une durée de vie longue, potentiellement plus de 10 ou 15 ans. Si l'on considère qu'en 2030-2035 on disposera de ces machines, ces données seront encore exploitables, et elles sont déjà exposées. Pourquoi ? Dans les reportages télévisés, on représente souvent de vilains hackers en capuche devant des écrans qui défilent à la Matrix. Eh bien, ces groupes de hackers sont d'ores et déjà en train de collecter et de mettre de côté des données chiffrées, auxquelles ils n'ont pas accès aujourd'hui, mais dont ils savent

que, lorsque la machine quantique sera disponible, ils auront tout ce qu'il faut pour les déchiffrer et exploiter les informations encore pertinentes et utiles qu'elles contiennent.

LUCILE RIVES : C'est le fameux « Harvest Now, Decrypt Later », c'est ça ?

OLIVIER LANTRAN : En bon anglais, c'est exactement ça : collecter maintenant pour exploiter plus tard. D'où l'enjeu de se protéger dès à présent, et d'où les recommandations de l'ANSSI et des institutions internationales que j'évoquais : prendre en compte ce risque dès maintenant et prioriser les données les plus sensibles et à la durée de vie la plus longue.

Comment se préparer au déploiement de l'informatique quantique

LUCILE RIVES : En préparant l'épisode, j'ai aussi entendu que la physique quantique apportait des solutions en matière de cryptographie, et que l'on pourrait créer des codes secrets grâce à elle, notamment grâce à la lumière. La physique quantique peut-elle être une solution à la menace qu'elle représente par ailleurs ? Où en est-on de la cryptographie post-quantique ?

OLIVIER LANTRAN : C'est assez amusant d'évoquer ces sujets-là, parce que, pour la plupart d'entre nous, le quantique relève déjà d'un sujet un peu « waouh », on se demande comment ça va marcher. Et sous l'angle de la cryptographie, on est déjà dans le post-quantique, c'est-à-dire encore plus loin ! Cependant, on n'a pas forcément besoin de technologie quantique pour se protéger de la menace quantique. La technologie quantique, comme vous l'avez souligné, va apporter de nouvelles capacités de chiffrement demain, et, comme on l'a évoqué, de nombreuses opportunités dans beaucoup de domaines. Mais la bonne nouvelle, c'est qu'aujourd'hui, on sait d'ores et déjà protéger nos informations les plus sensibles de ces machines quantiques qui n'existent pas encore. Comment ? Tout simplement grâce à de nouveaux algorithmes de chiffrement, qui reposent sur des problèmes mathématiques différents de la décomposition en facteurs premiers que l'on a évoquée, et qu'un ordinateur quantique aura du mal à résoudre. Ces algorithmes ont même fait l'objet d'une standardisation, notamment par le NIST, l'organisme américain qui normalise les sujets de chiffrement et de sécurité. L'une des priorités est donc d'identifier ces éléments et d'en faire l'inventaire pour ensuite, comme on l'évoquait, prioriser les données à traiter en premier et mettre en place les algorithmes aujourd'hui standardisés et disponibles sur le marché qui permettent de les protéger. Cette mise en place doit se faire intelligemment, en recherchant ce qu'on appelle la crypto-agilité. Qu'est-ce que la crypto-agilité ? C'est ce qui permettra demain de continuer à adapter simplement ces algorithmes de chiffrement, pour soutenir cette course entre ceux qui sécurisent et ceux qui attaquent, dont on parlait tout à l'heure, et ainsi se prémunir contre les évolutions technologiques d'après-demain, et même au-delà.

LUCILE RIVES : Que peut la Banque de France, et que peut le Lab en particulier, pour préparer l'avènement de l'informatique quantique, de l'ordinateur quantique, et protéger les flux financiers ? Rien de moins !

OLIVIER LANTRAN : C'est vrai que ce n'est pas un petit sujet. Modestement, ce que le Lab, le centre d'innovation de la Banque de France, peut faire et a fait, c'est anticiper, détecter tôt ce risque pour que l'on puisse s'en saisir. La Banque de France s'est donc saisie de ces sujets il y a quelques années

maintenant – je crois que nous avons commencé pendant le Covid. Nous nous sommes rapidement rendu compte que, seuls, nous parviendrions à nous protéger nous-mêmes, mais que cela ne suffirait pas. Nous avons donc porté ce sujet à l'échelle de l'Eurosystème, puis plus largement à l'international, au travers de travaux d'innovation avec la Banque des règlements internationaux (BRI). C'est grâce à ces expérimentations que nous avons pu nous forger, à la Banque de France, une conviction sur la nature exacte du risque, sur ce que l'on pouvait faire pour le traiter et sur la manière d'y remédier collectivement.

D'ailleurs, une fois que le centre d'innovation a fait ce travail, cela ouvre la voie à des chantiers qui ne relèvent plus vraiment de l'innovation : nos collègues de la Banque de France chargés de la sécurité des systèmes d'information et de la prévention des risques s'en emparent pour mettre en place cette fameuse crypto-agilité que j'évoquais, afin de protéger les ressources de la banque centrale.

Ces travaux ont permis à la Banque de France d'être identifiée comme pionnière dans le secteur financier sur ces problématiques. À ce titre, nous avons pu porter cette voix dans le cadre des travaux du G7, notamment au sein d'un groupe de travail sur les technologies quantiques que je copréside avec Maryam Haghighi, de la Banque du Canada, et qui réunit des participants de l'ensemble des banques centrales et des institutions financières des pays du G7. L'objectif est à la fois d'identifier ces risques et de préparer la façon de nous coordonner pour bénéficier des opportunités des ordinateurs quantiques, mais aussi de mieux évaluer et préparer l'impact que ces nouvelles technologies auront, comme on l'a vécu avec l'IA, sur le secteur financier, sur l'économie au sens large et, par ricochet, sur la société.