Elham Kashefi

Comment se manifeste l'avènement du quantique ?

Prisme N°29
Septembre 2014

La Fondation et le Centre Cournot

La Fondation et le Centre Cournot

Association reconnue d'intérêt général, le Centre Cournot contribue à développer et à rendre plus accessibles les théories des sciences économiques, sociales, politiques et leur épistémologie. Comme le Centre, la Fondation poursuit un travail de catalyse dans la filiation d'Augustin Cournot, accélérant ou sélectionnant des formulations théoriques concurrentes. Sous égide de la Fondation de France, la Fondation met ainsi en perspective le basculement probabiliste qui atteint progressivement les disciplines et promeut les recherches qui élaborent et utilisent les probabilités.

Comment se manifeste l'avènement du quantique ?[1]

Elham Kashefi

Prisme N°29

Septembre 2014

[1] Ce texte a été traduit de l'anglais par Nathalie Ferron. L'original est une transcription de la présentation d'Elham Kashefi lors du séminaire Cournot, « *Quantum Turing Testing* » en avril 2014. Il contient également les commentaires de Damian Markham et les questions de l'auditoire. La vidéo du séminaire est disponible sur le site du Centre Cournot : www.centre-cournot.org.

Résumé

Ce texte retrace brièvement l'histoire de l'informatique quantique afin de replacer dans son contexte le champ nouveau de la technologie quantique, avec tous les défis qui l'accompagnent. L'un des défis particulièrement difficiles à relever dans le domaine de l'informatique quantique est celui de la vérification et de la validation : d'une part, dans la mesure où les méthodes de calcul classiques ne peuvent rivaliser avec la puissance de calcul de la mécanique quantique, il est difficile de vérifier l'exactitude d'un calcul de type quantique ; d'autre part, la structure quantique sous-jacente résiste aux analyses classiques. Le texte fait le point sur les derniers procédés mis en place en vue d'évaluer les dispositifs de calcul quantique d'aujourd'hui afin que nous soyons en mesure d'exploiter pleinement ceux de demain.

Je voudrais évoquer dans ce texte divers aspects de la théorie quantique et raconter brièvement comment j'en ai fait mon domaine. Je commencerai par ma propre histoire pour ensuite effectuer un rapide survol de l'histoire de la technique quantique et enfin proposer une présentation détaillée de la méthode que nous employons pour effectuer nos tests. J'ai d'abord entrepris des études de mathématiques et j'envisageais de quitter l'Iran pour le Canada afin de m'y spécialiser dans l'analyse combinatoire lorsque, juste avant mon départ, l'occasion se présenta d'entrer à l'*Imperial College*. C'était une façon comme une autre d'apprendre un peu d'anglais, aussi ai-je accepté l'offre et j'ai préparé et soutenu une thèse de doctorat en mathématiques et en sciences de l'information et de la communication. Je me demandais si je m'étais engagée sur la bonne voie lorsqu'un beau jour une amie me conseilla d'aller voir du côté de l'informatique quantique. « L'informatique *quoi* ? » Très rapidement, elle me présenta à celui qui allait devenir mon directeur : un physicien (et non un informaticien) qui me fit découvrir toutes les possibilités de l'informatique quantique, de la factorisation, etc. Cela me parut proprement merveilleux. Je ne compris pas grand-chose de ce qu'il me dit mais il semblait y avoir de l'algèbre partout et pour avoir étudié l'analyse combinatoire en Iran, j'avais commencé l'algèbre au berceau. Je saisissais parfaitement l'aspect mathématique de ce dont il me parlait, sans avoir la moindre idée des applications possibles. Il m'a fallu dix ans pour comprendre dans quel piège je m'étais fourrée, mais c'est ainsi que je suis arrivée à l'informatique quantique.

Qu'est-ce que l'informatique quantique ? Tout a commencé en 1982 avec Richard Feynman qui, en véritable visionnaire, eut une idée : puisqu'il était apparemment si difficile de simuler des systèmes quantiques, de la physique et des particules quantiques sur des ordinateurs classiques, pourquoi ne pas construire un ordinateur quantique ? Son approche plus qu'audacieuse s'apparentait à de la science-fiction, et pourtant depuis, les progrès dans le domaine ont été fulgurants. Au cours des quarante dernières années, de la théorie des systèmes complexes à la cryptographie, de la simulation à l'échantillonnage, de la tomographie à sa mise en œuvre, de la fondation de la mécanique quantique à son interprétation, les progrès ont été immenses. Chacun de ces termes mériterait un article en soi, mais mon but ici est de vous faire parcourir l'histoire de ce domaine de recherche jusqu'à ce que j'appelle la « boucle de Feynman ». Nous en sommes aujourd'hui au stade

passionnant où nous cherchons à prouver que ce que nous mettons en œuvre et observons relève bien de la physique quantique. À l'origine, la question était la suivante : « Est-il possible de construire quelque chose de quantique ? » Eh bien nous pouvons aujourd'hui répondre affirmativement à cette question. Nous pouvons construire une machine quantique et je vais essayer de vous le montrer. La question que nous nous posons à présent est : « A-t-on bien affaire à du quantique ? » Et si nous ne finissons pas par trouver réponse à cette question-test – si nous ne parvenons pas à vérifier notre hypothèse – on pourra dire que Feynman nous a joué un bon tour : il a eu une idée prophétique, nous l'avons mise en œuvre mais sommes incapables de prouver sa validité. Nous ne sommes pas actuellement en mesure de prouver littéralement que l'on a affaire à du quantique. Je reviendrai sur cette question fondamentale, mais je voudrais d'abord reprendre les choses depuis le début.

Le quantique possède de nombreux aspects, je ne retiendrai que les notions de calcul et d'algorithme. La première fois que je me suis penchée sur la question, j'ai cru qu'il suffisait de trouver un nouvel algorithme, or je le cherche encore aujourd'hui ! Nous disposons donc d'une machine, dont je ne dirai rien de très précis pour l'instant, qui permet des gains en vitesse dépassant tout ce que l'on peut normalement attendre des ordinateurs classiques. Il ne faut pas croire qu'il s'agit de monter un nouveau type d'ordinateur, de construire un modèle et de l'accélérer : ici, le modèle vole en éclats purement et simplement. Au fondement de l'analyse numérique, on trouve la formulation forte de la thèse de Church–Turing. Selon cette thèse, tout modèle conçu par un humain équivaut à une machine de Turing classique[2], dans la limite de coûts raisonnables. Cependant, le modèle de calcul quantique invalide cette thèse. En raison de caractéristiques propres à la mécanique quantique, comme la superposition, les corrélations non locales, l'interférence… nous pensons qu'il y a une accélération. En fait, au bout de quarante années, on ne connaît toujours pas vraiment les causes de cette accélération, mais on sait que certains éléments donnent lieu à cette accélération exponentielle, qui reste du domaine de l'inconnu. Devant ce modèle qui leur donnait une accélération

[2] En 1936, un modèle de calcul proposé par Alan Turing s'est imposé comme modèle. Capable de tout ce que n'importe quel ordinateur physique peut calculer, la « machine de Turing » est devenue un outil indispensable en informatique fondamentale.

exponentielle, n'étant ni spécialistes de la physique expérimentale ni ingénieurs mais théoriciens, les premiers disciples de Feynman cherchèrent à en trouver la cause. Ils furent la première génération de scientifiques à s'intéresser au calcul quantique.

Pour donner une représentation très grossière de ce type de calcul : dans les méthodes de calcul normales, on suit les étapes de l'algorithme dans l'ordre. Ensuite intervient la notion de probabilité, à travers le jeu de pile ou face qui introduit du hasard. Dans le calcul quantique, au lieu de suivre une ligne unique, on suit un faisceau de lignes, ce qui pourrait être à l'origine de l'accélération (bien que l'on s'interroge encore sur la pertinence de cette idée d'accélération). Par ailleurs, il semble que les probabilités quantiques nous permettent d'obtenir des annulations : comme si on avait une distribution normale, mais avec des nombres non réels, des nombres complexes capables de s'annuler les uns les autres. En raison de l'interférence entre ces lignes aléatoires, le calcul s'effectue plus rapidement. Cela semble contre-intuitif, comme si en explorant un espace plus restreint, on obtenait quelque chose de plus grand. La figure 1 (mise au point par Richard Cleve) illustre cette caractéristique :

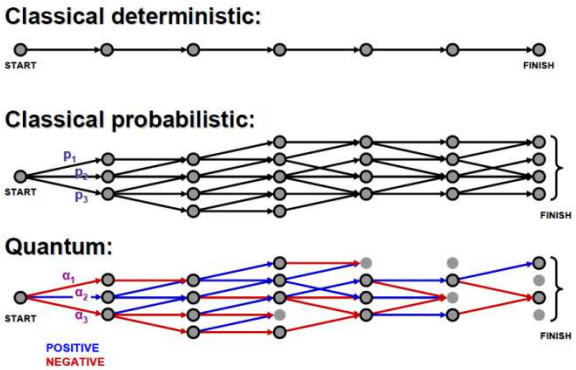

Figure 1 : Comparaison entre modèles de calcul déterministe, probabiliste classique et quantique.

Pour retracer très rapidement l'histoire de la discipline, je rappellerai qu'en 1985, l'un de ses pionniers, David Deutsch, présentait le premier algorithme quantique, qui fut développé un peu plus tard (en 1992), par Richard Jozsa. Ce

premier algorithme marqua un changement radical dans la structure mentale et les modes de pensée de la communauté scientifique concernée :

$$f : \{0,1\}^n \rightarrow \{0,1\}.$$

Cet algorithme n'a en réalité aucun usage pratique. En fait, on suppose une fonction booléenne assignant les valeurs 0 et 1 à des séquences de *n* valeurs binaires. Certaines séquences peuvent être bonnes, d'autres pas ; en tout cas, on obtient 0 ou 1. Ce dont on peut être sûr, c'est que cette fonction booléenne est soit constante – pour toutes les entrées, on obtient toujours 0 ou 1 – soit équilibrée – elle prend autant de fois la valeur 0 que la valeur 1. Imaginons une boîte noire, à chaque fois que l'on entre, par exemple, « quelle est la valeur de 00111010 ? » un nombre sort. Et il vous incombe de déterminer – sans regarder à l'intérieur de la boîte, mais simplement en appuyant sur un bouton pour lui poser des questions – si elle est constante ou équilibrée. En suivant la méthode classique, à l'aide d'un algorithme classique, combien de temps la tâche vous prendra-t-elle ? Quel processus vous permettra de résoudre ce problème ? D'un point de vue déterministe, si l'on veut savoir avec certitude si cette fonction est équilibrée ou constante, il faut jouer sans discontinuer. On ne vous demande pas de donner toutes les valeurs – les valeurs ne nous intéressent pas, ce que nous cherchons à savoir, c'est si la fonction est équilibrée ou constante – mais vous n'avez pas d'autre solution que de calculer toutes les valeurs pour découvrir si elles sont constantes ou équilibrées. Plus précisément, pour en décider, il faudra poser à votre boîte 2^{n-1} questions, à partir de toutes les suites possibles. Il n'existe pas d'autre solution, en dehors peut-être des probabilités. Avec la théorie quantique en revanche, il est prouvé que ce problème se résout à l'aide d'une seule question. La théorie quantique vous permet littéralement d'accomplir les tâches que vous vous assignez, et c'est là, à mes yeux, l'un de ses plus grands mérites. La théorie quantique ne vous donnera pas toutes les valeurs, approchées ou exactes, mais elle vous permet de répondre, avec beaucoup d'économie et de précision, à la question qui vous est posée.

$$|f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

En fait, rien qu'avec une seule et unique question (grâce à la superposition entre autres), on peut créer un état physique – un état quantique, selon la formule ci-dessus – tel que, si la fonction est constante, on trouvera un élément donné dans l'espace vectoriel, et si elle est équilibrée, on en trouvera un autre, orthogonal au premier. Nous savons en outre qu'en théorie quantique, on peut déterminer l'état orthogonal. Peu importe les détails, ce qu'il faut comprendre, c'est que grâce aux outils quantiques, le problème en question peut être résolu exponentiellement plus vite. Et c'est cette simple observation qui a donné naissance à quelques nouveaux algorithmes quantiques bien utiles, fondés sur le principe de l'accélération quantique. Par exemple l'algorithme de Shor (d'après le nom du mathématicien, Peter Shor) qui permet de factoriser des nombres – exponentiellement plus vite qu'avec n'importe quel autre algorithme classique connu – en sorte que tout crypto-système devient vulnérable et les systèmes de sécurité caducs. Entre-temps, Daniel Simon conçut un autre algorithme en 1994, dans le but de déterminer la périodicité d'une fonction, avec cette structure :

1994 – problème de Simon

Soit une fonction $f : \{0,1\}^n \rightarrow \{0,1\}^n$ permet de trouver a tel que $f(x+a) = f(x)$

On obtient une vitesse de calcul accrue par rapport à toute autre solution classique (du type algorithme de Deutsch–Josza) dans la mesure où il n'est pas nécessaire d'évaluer toutes les valeurs de la fonction. L'algorithme de Simon donne une autre accélération. La discipline en était à ses débuts et l'article de Simon fut soumis à Peter Shor, lequel observant cette démonstration comprit qu'on pouvait appliquer la même idée, non pour résoudre ce problème – ce qui n'avait pas grand intérêt – mais pour résoudre le problème de la factorisation. Il s'agit du problème de recherche de période de Shor : soit un nombre entier de n-unités binaires, trouver la factorisation en nombres premiers qui permette de déchiffrer le cryptosystème RSA[3].

[3] Du nom de Ron Rivest, Adi Shamir et Leonard Adleman qui furent les premiers à présenter cet algorithme au public en 1977. RSA a été l'un des premiers cryptosystèmes à clef publique utilisable. Il est largement utilisé pour la transmission de données sécurisées. Dans un tel cryptosystème, la clé de codage est publique tandis que la clé de décodage reste secrète. Dans le système RSA, cette asymétrie repose sur le fait qu'il est difficile de factoriser le produit de deux grands nombres premiers.

C'est ainsi que Shor a révolutionné la discipline : d'un seul coup, tout le monde – tous les gouvernements, la NSA, et toutes les autres agences de sécurité – a compris qu'il était désormais possible de factoriser des nombres pour décrypter une clef RSA, et qu'il valait donc mieux surveiller de près ce qui se passait dans ce domaine. C'est ainsi que nous nous retrouvons aujourd'hui avec un zoo pour algorithmes.

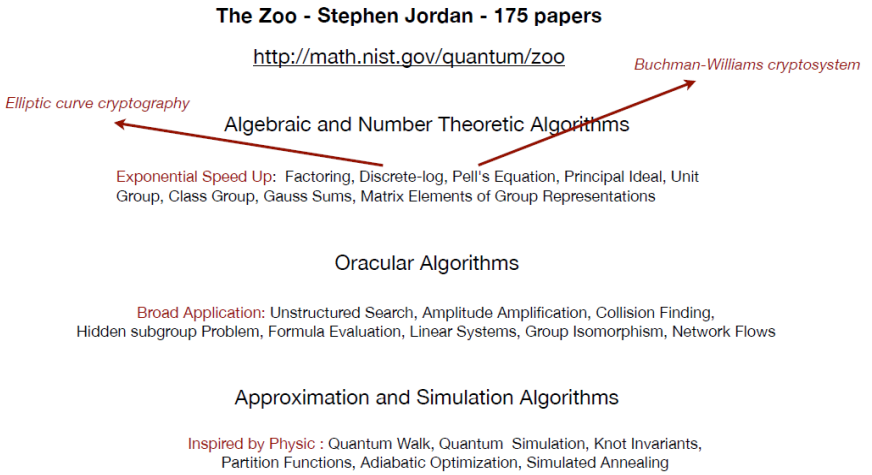

Figure 2 : Zoo pour algorithmes

Ce zoo contient des centaines de travaux et toutes sortes d'algorithmes quantiques très intéressants, qui sont autant de démonstrations de divers types d'accélérations. Ce qui mérite réellement de retenir notre attention, c'est le fait que le calcul quantique permet de résoudre une quantité de problèmes propres à la théorie des nombres, problèmes que l'on a beaucoup de mal à résoudre classiquement (difficulté sur laquelle reposent tous les systèmes de cryptages). D'où la nécessité de trouver un nouveau système de cryptage. J'y reviendrai, mais pour finir sur les algorithmes, rappelons-nous qu'au départ, Feynman a construit un système quantique en vue de simuler la physique car cela lui semblait être le meilleur champ d'application. Et c'est ce qui se passe effectivement aujourd'hui. On sait construire de petits dispositifs physiques pour mettre en œuvre l'algorithme de factorisation de Shor, dans son principe, mais là où les choses sont vraiment intéressantes, c'est dans

le domaine de la simulation quantique : nous disposons enfin d'un dispositif capable de simuler des systèmes qu'il était impossible de simuler auparavant.

Bien qu'il soit difficile de prouver qu'un ordinateur quantique soit réellement plus puissant que n'importe quel système informatique classique (problème équivalent à l'un des grands problèmes non résolus de l'informatique : P *versus* NP), on a tout de même de sérieuses preuves que, pour certains échantillonnages, notre hypothétique ordinateur quantique serait plus puissant sous une certaine hypothèse de complexité. Cette voie d'exploration pourrait nous permettre de réfuter la formulation forte de la thèse de Church–Turing, c'est-à-dire de remettre en question les fondements mêmes de l'informatique. L'autre intérêt de l'ordinateur quantique, c'est qu'il permettrait de venir à bout de la plupart des cryptosystèmes les plus couramment utilisés. Cela signifie que les technologies actuellement utilisées pour assurer la sécurité seraient obsolètes à partir du moment où nous serions en mesure de construire un ordinateur quantique à grande échelle. Comment ne pas s'enthousiasmer : on parle déjà de « cryptographie post-quantique », on tient des réunions où l'on cherche à concevoir un cadre d'analyse pour garantir la sécurité dans un monde à venir, d'ici 50 ou 100 ans, où l'informatique quantique sera devenue réalité.

On dit de la technique quantique que ce qu'elle prend d'une main, elle le redonne de l'autre. Imaginons que la cryptographie quantique remplace le modèle classique. Tandis que la cryptographie classique repose sur la difficulté de certains problèmes, la cryptographie quantique repose pour sa part sur les axiomes de la physique. Si ce que l'on croit savoir de la mécanique quantique est exact – et en 100 ans, la théorie quantique n'a jamais été réfutée – cela veut dire qu'on peut élaborer un cryptosystème dont la sécurité repose sur la théorie quantique et non plus sur la difficulté à résoudre un problème. Ainsi, d'un côté nous disposons d'un cryptosystème fondé sur le fait que les mathématiciens, pourtant si intelligents, n'ont pas encore réussi à résoudre un problème, de l'autre d'un cryptosystème fondé sur une théorie que les physiciens, pourtant très intelligents eux aussi, n'ont pas encore réussi à réfuter ! Le terme servant à désigner la cryptographie quantique est « sécurité inconditionnelle ». Dans le domaine de la cryptographie quantique, on ne s'appuie plus sur la théorie des nombres, on se sert de caractéristiques quantiques, telles que l'impossibilité du clonage (il est impossible de cloner parfaitement un système

physique), ou l'impossibilité d'effectuer une mesure sans entraîner un changement d'état du système. Il est en effet impossible de mener une observation sans modifier l'objet observé. Ce principe peut être utilisé, par exemple, pour contrer les indiscrétions : si un espion cherche à s'introduire dans le système, il provoquera une modification de celui-ci. On ne saurait rêver d'une protection plus efficace. Quant aux utilisateurs du système, ils sont informés de l'événement. La cryptographie classique n'offre pas cette garantie : elle ne permet pas de savoir si une opération non-sécurisée a été effectuée. Telle est donc la promesse de la cryptographie quantique, qui est l'autre fleuron de notre discipline.

La définition de la sécurité change-t-elle dans un cadre global ? On a beaucoup réfléchi à la question. Le cadre mathématique qui permet de penser la notion de sécurité est celui de la théorie des probabilités : quelle est la probabilité pour que la variable correspondant à ce que sait l'espion soit indépendante de la variable aléatoire correspondant à l'information secrète détenue par les parties ? Leur indépendance l'une de l'autre étant la garantie d'une sécurité maximale. Telle est la définition de la sécurité en cryptographie classique et c'est précisément ce que permet la cryptographie quantique. Ce qui compte, en somme, c'est l'indépendance de ces variables aléatoires, autrement dit la quantité d'informations ayant fuité. Les spécialistes du quantique se sont servi de la théorie de Shannon pour trouver un cadre unifié permettant de définir une sorte de protocole de sécurité. Comme dans le scénario classique, on se trouve toutefois confronté à une immense difficulté : comment prouver que les dispositifs quantiques répondent effectivement à l'exigence d'une sécurité inconditionnelle alors que subsiste un écart entre preuve théorique et démonstrations expérimentales ? Nous pensons néanmoins que grâce à nos efforts conjoints et soutenus, nous parviendrons bientôt à résoudre ce problème.

La cryptographie quantique est née grâce à Stephen Wiesner, qui publia en 1983[4] un article dans lequel il émettait l'idée que personne ne pouvait détecter si un photon aléatoire avait été préparé (un photon étant un système physique à l'état aléatoire). Quiconque cherche à observer l'état du photon est voué à le modifier et cette modification est détectable. La trouvaille était belle mais l'auteur dut attendre dix ans avant que son article soit publié. Il est vrai que personne n'avait entendu parler de cryptographie quantique à l'époque. Wiesner était trop en avance sur son

[4] Wiesner, S. J. (1983), "Conjugate Coding", *SIGACT News* 15:1, pp. 78–88.

temps, et on commence seulement aujourd'hui à reparler de son idée de monnaie quantique impossible à reproduire par des faux-monnayeurs. Il s'agit encore une fois d'une idée très simple, mais pleine de prescience. On raconte que certains scientifiques se servirent de son idée loufoque pour l'adapter à la cryptographie classique et jeter les bases de la cryptographie informatique classique. Par la suite, Charles Bennett et Gilles Brassard (1984)[5], puis Artur Ekert (1991)[6] se sont attaqué au problème de distribution des clefs publiques, ce qui ouvrit de tout nouveaux horizons. Pour des raisons évidentes, gouvernements et agences de sécurité sont intéressés au premier chef. Mais il y a aussi cette idée fondamentale qu'en fondant la sécurité sur un axiome de la physique plutôt qu'un axiome mathématique, on aborde un autre monde, et de fait, le fondement même de la physique théorique s'en trouve affecté aujourd'hui. Depuis, bien d'autres protocoles quantiques ont été introduits et divers résultats d'impossibilité démontrés. Le domaine s'est considérablement développé au cours des dix dernières années et on trouve même des entreprises qui vendent des dispositifs de distribution quantique de clef.

Quel avenir envisager pour la cryptographie quantique ? Nous en sommes aujourd'hui à installer de vastes réseaux de distribution de clef quantique. En 2008, le projet SECOQC (***Secure Communication based on Quantum Cryptography project***) a utilisé 200 km de fibre optique standard pour connecter entre eux six nœuds entre Vienne et St-Pölten. Télécom ParisTech fait partie des pionniers de l'installation de ce type de réseaux, et de nombreux autres pays européens se sont lancés dans l'aventure. Le réseau quantique à 10 nœuds de la DARPA (***Defense Advanced Research Projects Agency***) fonctionne depuis 2004, il relie la société BBN Technologies, les universités d'Harvard et de Boston ainsi que la société QinetiQ. Le réseau de distribution quantique de clefs (QKD) de Tokyo compte sept partenaires : NEC, Mitsubishi Electric, NTT, NICT, Toshiba Research Europe Ltd. (RU), Id Quantique (Suisse) et All Vienna. Et plus récemment, l'Europe et la Chine ont pris la tête de la course pour le développement des communications quantiques de la terre vers les satellites.

---

[5] Bennett, C. H. et G. Brassard (1984), "Quantum cryptography: Public key distribution and coin tossing", Actes du colloque international de l'*IEEE: Ordinateurs, Systèmes et traitement du signal (Computers, systems and Signal Processing)*, volume 175, p. 8, New York.

[6] Ekert, Artur (1991), thèse de doctorat, Oxford, *Physical Review Letters*, 67, pp. 661–663.

En résumé, la théorie de l'information et du calcul quantiques – et plus précisément la formalisation de la machine quantique de Turing et du modèle quantique – fut développée à partir des années 1980 par des théoriciens. À l'époque, les spécialistes des sciences expérimentales et les ingénieurs étaient extrêmement sceptiques à l'égard de ce qu'ils considéraient comme de la science-fiction. Ils ont commencé à s'y intéresser au cours des années 1990 à travers l'observation des photons, des électrons libres et ainsi de suite. C'est à partir de ce moment que cette théorie est passée du domaine de la science-fiction à celui du possible : une partie de la communauté scientifique se rendit compte que les idées de Deutsch, Bennett et Brassard pouvaient être mises en pratique. Et dans les années 2000, de nouvelles applications ont vu le jour grâce aux premières start-ups, qui ont encore avancé par rapport à l'idée première qui avait déjà changé notre point de vue. Désormais, on pourrait trouver de réelles applications, faire des simulations réelles, au lieu de se contenter de chercher à savoir si telle fonction est constante ou équilibrée ou si l'on est à l'abri du secret. Le quantique suscite toujours autant d'intérêt : les jeunes étudiants sont fascinés quand on leur parle de l'aventure quantique, et dès qu'ils en savent un peu plus long, ils ne veulent plus faire autre chose. Même si nous ne maîtrisons pas encore tout à fait notre sujet, il a déjà bien avancé, en sorte qu'à mesure que nous progressons, de nouveaux défis, de nouvelles questions se posent, de nouveaux horizons s'ouvrent.

En fait, le domaine se réinvente tous les dix ans. Une nouvelle ère se profile à présent : celle de la « technologie quantique ». En guise d'explication, je vous donnerai un exemple de projet auquel je participe. En décembre 2013, le gouvernement britannique a lancé un ***Programme national en faveur des technologies quantiques***, avec un investissement de £270 millions à la clef. Ceci n'est pas tout à fait surprenant dans la mesure où la Grande-Bretagne a été pionnière dans le domaine de l'information quantique dès ses balbutiements, et plus récemment, de fortes pressions ont été exercées sur le gouvernement pour que soit renforcé le rôle de leader de la Grande-Bretagne. Personne, cependant, ne s'attendait à une telle somme, dont une bonne partie (£150m) est directement allouée à la recherche sous forme de bourses. Le calendrier est serré : l'annonce de l'allocation de £270m a eu lieu en décembre, les pré-propositions étaient attendues pour le 1er février, la soumission des projets, y compris la désignation des membres

de l'équipe et des partenaires industriels, pour le mois de mars, et la date limite d'enregistrement des projets finals était fixée au mois de juin. Les entretiens et les décisions ont eu lieu en septembre et le centre devait fonctionner dès le mois de décembre 2014. Ce programme a bénéficié de l'attitude volontariste du gouvernement qui attend en échange un plan de développement : il s'agit de « développer des technologies nouvelles », d'une « initiative concernant de multiples acteurs, axée sur le déploiement de technologies et prévue pour une durée initiale de cinq ans ». Les technologies en question touchent les domaines des capteurs, de la métrologie, des transactions sécurisées, du calcul, de la simulation, etc. : le programme britannique pour le développement des technologies quantiques (*UK National Quantum Technologies Programme*) n'est pas axé sur la science quantique mais sur l'exploitation de cette science au profit de la technologie. On pourrait s'attendre à ce que la plupart des spécialistes des sciences théoriques s'élève contre une telle proposition, qu'ils ne la prennent pas au sérieux et qu'ils s'en détournent. Comment pourtant résister à une offre aussi généreuse et à une occasion aussi belle et rare ? Dans une certaine mesure, il nous faut changer de voie, pour aborder un problème très intéressant : la construction de la machine. Il n'est plus question de preuve de principe, il faut qu'à la fin des cinq années, nous présentions un prototype suffisamment convaincant pour que l'industrie reprenne le projet. Je ne sais pas quelles seront les conséquences pour la science quantique, mais tous ceux qui ont travaillé sur les aspects théoriques de ce domaine s'intéressent sans doute désormais à la technologie quantique. L'objectif central de mes recherches est d'explorer de bout en bout tous ces thèmes. En particulier, je piloterai une approche bien particulière de la vérification de la technologie quantique, qui constitue à l'heure actuelle le principal défi à relever pour passer de la théorie à la pratique.

Quand notre spécialité est née dans les années 1980, nous nous posions la question suivante : « Qu'est-ce qu'un ordinateur quantique ? » – quelle définition en donner, quelle est sa structure, quelles sont ses applications, etc. ? Dix ans plus tard, selon la formule de Feynman : « On ne comprend pas la mécanique quantique, on s'y habitue. » Et la question que nous nous posons à présent est la suivante : « Est-ce un ordinateur quantique ? » Et même cette question plus intéressante encore : est-ce une boîte quantique ? En effet le terme « ordinateur » – cette machine universelle qu'on emporte partout et qui sert à tout – n'est plus vraiment approprié. La question n'a

rien d'irréaliste. Une entreprise à Vancouver prétend avoir mis au point un dispositif de recuit quantique. Leur machine se présente sous la forme d'une boîte gigantesque, s'agit-il d'un ordinateur quantique ? Il importe de le savoir car l'entreprise en question ne se contente pas de jouer avec deux ou trois photons, elle met en vente un ordinateur quantique doté d'un processeur de 1000 qubits. A-t-on affaire à une boîte quantique ? Son fabricant ne prétend pas qu'il s'agit d'une machine à tout faire : elle est conçue pour effectuer des simulations spécifiques. Je voudrais insister sur le fait que cette question n'est pas triviale. Il ne suffit pas de dire : « nous avons là un algorithme de factorisation qui fonctionne mieux que toutes les machines classiques, c'est donc sûrement quantique. » Cela ne constitue pas une preuve que ce qui se passe à l'intérieur de cette boîte est d'ordre quantique. En l'occurrence, la question du caractère quantique du dispositif ne se pose même pas, la seule question à se poser est : « Cette machine fait-elle quelque chose de juste ? »

Cette question est devenue d'un coup la question centrale, car quels que soient les résultats obtenus en fin de compte grâce à la technologie quantique, c'est la question à laquelle les chercheurs voudront trouver une réponse. En raison de l'ampleur de l'investissement financier et du grand nombre de laboratoires de recherche impliqués dans la construction de cette machine, il est essentiel de savoir si c'est quantique, si c'est correct et si elle répond à la spécification demandée. Si l'on regarde du côté de l'informatique classique, on constate qu'au cours des 30 dernières années, certains des chercheurs qui ont reçu le prix Turing s'intéressaient exactement aux mêmes problèmes : vérification des systèmes complexes et méthodes de test.

Le problème du quantique, c'est que ce qui fait qu'une machine est quantique rend la vérification elle-même quantique. Nous pensons que l'informatique quantique est exponentiellement plus puissante que l'informatique classique, ce qui signifie qu'on ne peut lancer une simulation quelconque en appliquant les méthodes de vérification classiques en vue d'en tirer la conclusion que notre résultat est correct. La raison pour laquelle on peut supposer précisément que notre boîte est quantique, c'est qu'aucune des méthodes employées auparavant ne s'appliquent, il faut tout reprendre à zéro. Le problème auquel nous sommes confrontés à présent, et qui a un sens dans le contexte de la technologie quantique, c'est de trouver une formalisation adéquate. Quelle structure, quelle méthodologie utiliser pour formaliser l'idée de ce qu'est une boîte quantique ? Je vais vous proposer une réponse.

Pour la trouver, il faut remonter au test de Turing. En 1950, Alan Turing eut l'idée de tester l'intelligence artificielle. Son test consiste à placer une personne dans une première pièce, une autre personne dans une deuxième pièce et un ordinateur dans une troisième, le but étant de savoir si on peut faire la différence entre un humain et une machine. Les règles à suivre au fil de la conversation sont préétablies.

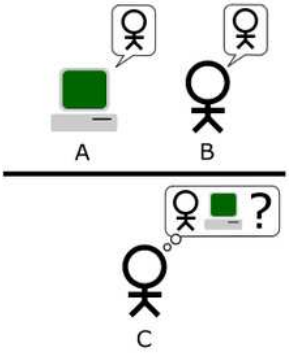

Figure 3 : Une illustration du test de Turing classique : C interroge A et B et tente de déterminer lequel est humain, lequel est une machine.

Pour un ordinateur quantique, la situation est pratiquement la même : nous dialoguons avec une machine, mais nous ne savons pas si elle est de type classique ou bien quantique, c'est aussi simple que cela. Mais pour savoir si une machine est quantique, faut-il utiliser un type de communication d'ordre quantique ou bien classique ? L'autre grande question étant : « Notre machine est-elle efficace ? » Dans la mesure où nous pensons que l'ordinateur quantique est plus puissant qu'un ordinateur classique, cela signifie-t-il qu'il est impossible de tester avec efficacité l'exactitude de ses résultats ? Ou bien la correction des réponses ne peut-elle être testée que par un autre ordinateur lui-même superpuissant ? Cela ne fait que trois ou quatre ans que nous nous posons ces questions.

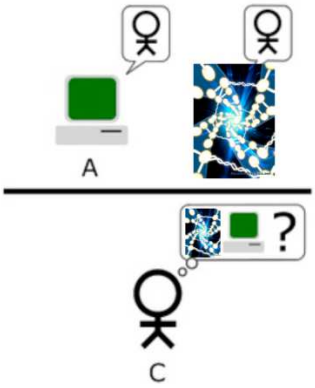

Figure 4 : Test de Turing appliqué au quantique ; © EQUINOX GRAPHICS

En résumé, ce qui fait qu'une machine quantique n'est pas classique rend également sa vérification non-classique. Mais, d'un certain point de vue, elle n'est pas à ce point éloignée du classique. J'ai dit plus haut qu'il fallait oublier tout ce qui avait été fait dans le domaine théorique et repartir de zéro, mais cela n'est pas tout à fait vrai. La meilleure chose à faire, c'est de revenir sur ce que nos prédécesseurs ont fait, repérer la question à laquelle ils ont cherché à répondre dans un contexte classique et qui se rapproche le plus de celle que nous nous posons afin de l'adapter à l'environnement quantique. Les systèmes de preuve interactive sont l'un des joyaux de la théorie des sciences de l'information dans le domaine de la vérification et des tests sur systèmes complexes. Ils sont un bon moyen de formaliser le problème de la constitution d'une preuve. On peut par exemple se servir d'une preuve mathématique pour ensuite la tester, mais une telle preuve ne nous fera pas avancer beaucoup : si vous me posez une question en réponse à laquelle je suis censée vous fournir une preuve, et que notre échange s'arrête là, vous vous bornez à une classe de problèmes très spécifique, comme la factorisation. Si je veux vous prouver que je sais factoriser, vous me donnerez un très grand nombre, je vous en donnerai deux autres, vous multiplierez ces nombres entre eux et vous verrez le résultat. La beauté de la preuve interactive réside dans le fait qu'elle repose sur le hasard et la communication (l'interaction), ce qui permet de faire bien davantage qu'une simple vérification du résultat de la factorisation.

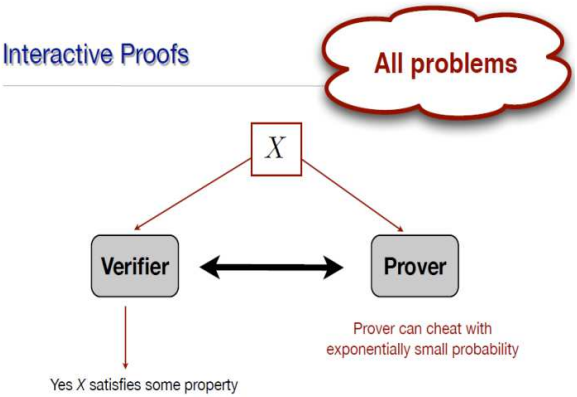

Figure 5 : Preuves interactives

Cette figure présente un démonstrateur, qui correspond à un serveur non fiable, la nature, un dispositif, la technologie quantique, une entité quelconque en tous cas capable de réaliser une tâche très complexe mais qui n'est pas fiable – et un vérificateur, très limité, qui ne peut faire que des calculs très simples. Le démonstrateur peut se servir de n'importe quelle classe de complexité, tandis que le vérificateur cherche à se limiter à un calcul en temps polynomial borné, à ce que sait faire son ordinateur en somme. Le vérificateur pose une question au démonstrateur, consulte sa réponse, effectue des calculs, pose une deuxième question plus difficile, consulte la réponse, et ainsi de suite. La conversation doit être limitée, de même que l'ordinateur du vérificateur. En informatique théorique, on peut vérifier ainsi toute la classe des théorèmes. Cette approche est vraiment efficace. Il y a une petite part d'aléatoire, en sorte que le démonstrateur a la possibilité de tricher, mais avec une probabilité très faible. Parfois, le démonstrateur peut avoir de la chance et démontrer quelque chose qui n'est pas correct, mais en tenant compte de cette part d'aléatoire ! La façon la plus naturelle de formaliser le problème de notre capacité à tester la puissance de calcul quantique serait d'adapter cette technique à l'environnement quantique.

Nous sommes donc dans la position du vérificateur classique ne disposant que d'une machine classique et de dispositifs classiques. Par ailleurs, il y a cette « boîte » (qui sera miraculeusement construite grâce à l'allocation de £50 millions, par l'un des centres de recherches britanniques), à laquelle nous voulons poser des

questions et dont nous espérons obtenir des réponses, sous forme d'un échange, afin de prouver qu'elle fonctionne correctement). Il faut se montrer prudent, aussi ne parlerai-je pas pour l'instant de quantique : la première étape est celle de la correction du calcul. Cette question a été posée pour la première fois en 2004 : la théorie quantique est-elle réfutable par des méthodes classiques ? Puis-je utiliser la logique classique, la théorie classique pour tester la correction des résultats ? La question est simple, me direz-vous, il suffit de faire l'expérience. Alain Aspect, l'un des pionniers de la physique quantique, a mené une extraordinaire expérience mettant en évidence l'effet quantique, mais il reste des lacunes. Alors comment procéder ?

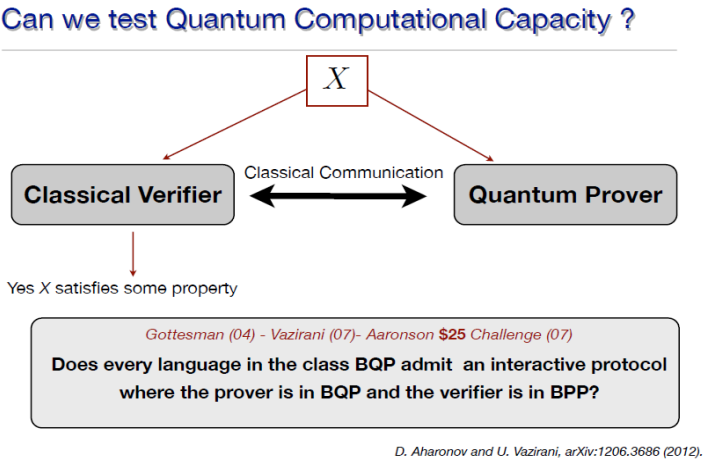

Figure 6 : Comment tester la puissance de calcul quantique ?

Nous cherchons à vérifier ce qu'un ordinateur quantique est supposé faire avec efficacité. Dans la figure 6, BQP correspond à « ***Bounded-error Quantum Polynomial*** » (un problème à erreur bornée, quantique, temps polynômial), ce que les ordinateurs quantiques semblent tout à fait aptes à faire. BPP, « ***Bounded-error Probabilistic, Polynomial*** » (erreur bornée, probabiliste, temps polynomial), correspond à ce que savent faire nos ordinateurs portables avec une dose d'aléatoire classique. Ainsi, si j'ai un BPP, c'est-à-dire si je tire à pile ou face pour ensuite effectuer des calculs, ce qui m'intéresse, c'est de savoir si je suis en mesure de valider un démonstrateur du type BQP en me servant du vérificateur classique. Nous pensons

que le BQP est plus complexe que le BPP, c'est pourquoi nous procédons ainsi, l'ordinateur quantique étant capable de faire des choses impossibles à faire pour des machines classiques. Et on y arrive :

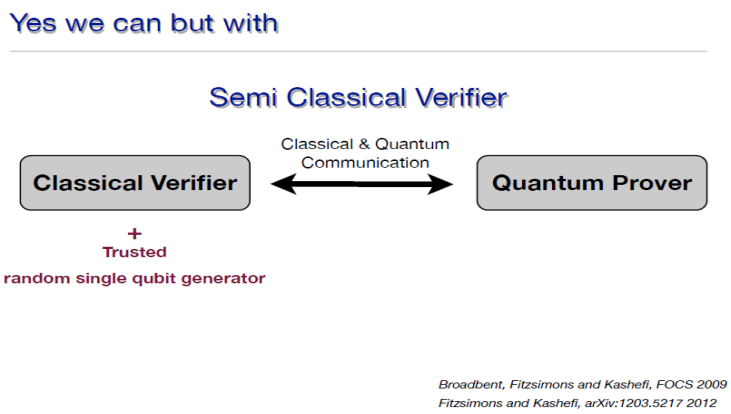

Figure 7 : Vérificateur semi classique

La figure 7 illustre des travaux que j'ai menés il y a quelques années avec Anne Broadbent au Canada et Joseph Fitzsimons à Singapour. L'expérience est réalisable, mais pas dans un cadre intégralement classique. Nous ne sommes pas dans un cadre exclusivement BPP – la question reste ouverte. En tout cas, nous avons gagné les dix dollars que nous avait promis Scott Aaronson, chercheur de pointe à Harvard, si nous relevions le défi qu'il nous avait lancé et qui nous avait si bien motivés… Le principe de notre expérience est le suivant : l'ordinateur du vérificateur est de type classique, mais on y introduit un peu d'aléatoire quantique grâce à un dispositif qui nous permet d'envoyer un photon aléatoire dans une certaine direction autant de fois qu'on le souhaite. Ce dispositif peut être construit par n'importe quel physicien : il ne s'agit pas d'un ordinateur quantique mais d'une machine à photons très simple (comme cela a été démontré à Vienne). C'est comme si on disposait d'une mini « pièce quantique » en quelque sorte, grâce à laquelle on peut tester avec efficacité la fiabilité d'une machine. Une équipe nord-américaine (Reichardt *et al.*) a

par ailleurs publié un article l'an dernier, dans lequel elle explique qu'il existe une autre façon d'introduire la probabilité[7] :

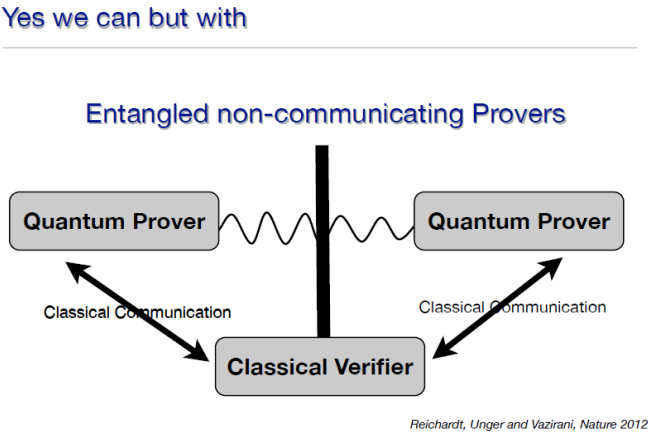

Figure 8 : Démonstrateurs intriqués sans communication entre eux

Nous disposons ici de deux serveurs quantiques et d'un vérificateur classique, en sorte que nous avons perdu notre pièce quantique. Les deux serveurs ne peuvent pas communiquer entre eux, en sorte qu'ils ne peuvent pas « tricher ». Il existe un phénomène appelé « intrication quantique », qui est plus puissant encore que le caractère aléatoire de la mécanique quantique, mais qui produit exactement les mêmes effets. Si deux particules ayant communiqué entre elles avant d'être séparées sont observées ensuite par deux observateurs distincts, à chaque fois que l'un des observateurs tire au sort pour émettre un bit aléatoire, l'autre observateur obtiendra le même bit aléatoire : on a affaire à des phénomènes aléatoires corrélés, ce qu'on ne voit jamais dans le contexte classique. Si cette configuration est alors donnée aux deux serveurs, cela permet encore de tester avec efficacité la fiabilité de la machine. Ainsi, on constate une sorte d'équivalence entre les deux aspects aléatoires, le premier sous forme d'intrication, partagé par les démonstrateurs, parties non fiables, et le second, sous forme de « pièce quantique », confiée au vérificateur, partie fiable. Et ces deux aspects apportent tous deux une solution au problème.

[7] Reichardt, Ben, Falk Unger et Umesh Vazirani (2013), "Classical command of quantum systems", *Nature* 496, pp. 456–460, 25 avril.

Nous n'en sommes qu'au début des études sur les liens entre ces deux approches et la question que nous nous posons est la suivante : « Pouvons-nous nous débarrasser de cet étrange phénomène d'intrication lors des tests ? Pouvons-nous mettre de côté notre pièce quantique ? » En d'autres termes, parviendrons-nous à mettre en place un type de test parfaitement classique ? Cette question est à mes yeux des plus intéressantes. Par ailleurs, en raison de l'ampleur de l'investissement consacré à la technologie quantique (£270m), il est nécessaire de pouvoir procéder à des vérifications, or le protocole de vérification que je viens de présenter n'est encore que théorique. Il y a vingt ans, nous nous serions contentés de ce résultat, mais aujourd'hui, à l'heure où nous cherchons à construire des machines quantiques, il faut trouver des solutions suffisamment optimales pour qu'on puisse les appliquer aux dispositifs pratiques qui verront sans doute bientôt le jour. Il faut poursuivre dans cette voie car, comme nous l'avons montré, il y a des possibilités. Cependant, dans l'immédiat, il faut trouver le moyen de rendre cette technique de vérification applicable à l'industrie.

Voici un peu plus précisément comment fonctionne notre protocole : d'abord, il faut revenir un peu en arrière, à l'époque où Damian Markham (qui sera mon discutant aujourd'hui) et moi cherchions à répondre à la question suivante : « Qu'est-ce qu'un ordinateur quantique ? » L'une des façons de formaliser le problème consiste à établir un modèle de calcul quantique fondé sur la mesure :

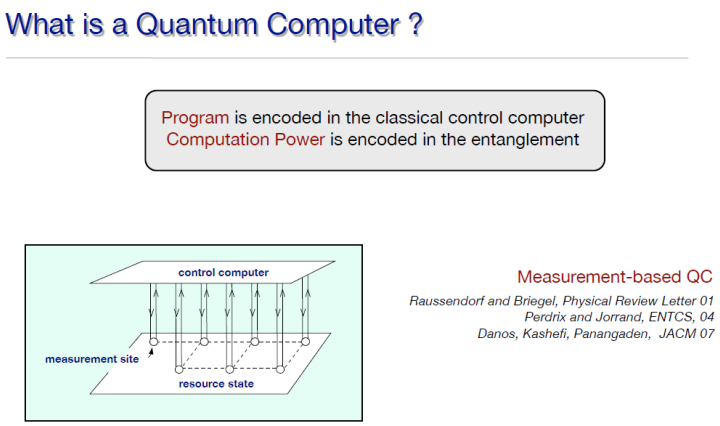

Figure 9 : Qu'est-ce qu'un ordinateur quantique ?

Le dispositif est bizarre : le programme consiste à placer une sorte de contrôle classique par-dessus l'intrication quantique, puis de manœuvrer en sorte que nous puissions bénéficier de toute la puissance du système quantique. Il s'agit en quelque sorte du langage « d'assemblage » des ordinateurs quantiques, sans le jargon quantique – d'une sorte de carte perforée quantique qui agit sur les particules. Il nous a fallu dix années pour comprendre et formaliser ce flux d'information ainsi que beaucoup d'autres choses très intéressantes. Se pose ensuite une nouvelle question : avons-nous réellement affaire à un ordinateur quantique ? Comme je l'ai dit plus haut, je me sers de la théorie de la preuve interactive pour formuler cette nouvelle question. Quelle était la configuration ? Le vérificateur doit être aussi simple et classique que possible. La façon la plus naturelle de procéder est donc de placer ce vérificateur – sous la forme de cette jeune femme fiable et dépourvue de superpouvoirs – dans le rôle de contrôle classique tandis que le démonstrateur – cet homme non fiable doté de superpouvoirs – représentera le dispositif quantique.

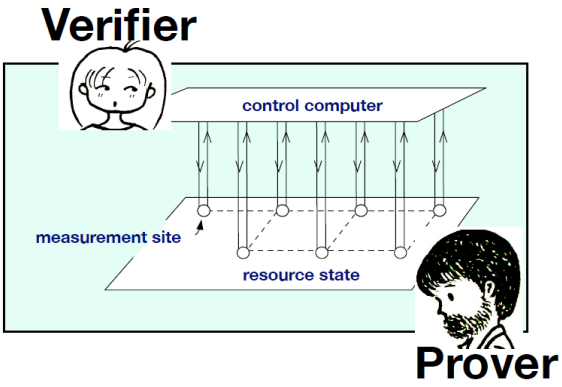

Figure 10 : Vérificateur et démonstrateur

Comme je l'ai déjà dit, avec ce modèle, tout coïncide. En jouant un peu avec, nous nous sommes rendu compte que la preuve interactive coïncidait parfaitement avec lui. Un autre type de modèle de calcul quantique n'aurait sans doute pas aussi bien répondu à la question. Le contrôle de type classique est donc censé jouer le rôle de vérificateur – lequel consiste à poser les questions et prendre l'initiative des échanges – tandis que la personne qui pilote le dispositif quantique – qui gère

l'intrication – sera mon démonstrateur quantique. Dans notre langage d'assemblage, les lignes allant du contrôle à l'état ressource représentent les bits classiques, lesquels indiquent l'angle de mesure. Chacun de ces qubits unitaires est un vecteur unitaire dans un espace vectoriel complexe de dimension 2 (C2). On envoie un signal indiquant dans quelle direction on a l'intention d'effectuer la mesure (on s'arrange pour obtenir un ensemble discret) en choisissant parmi huit angles possibles sur le plan. On procède ensuite à une observation, laquelle constitue une mesure quantique de type probabiliste. On a donc un vecteur unitaire en C2, que l'on projette avec une certaine probabilité qu'il aille dans une certaine direction et une certaine probabilité qu'il aille dans la direction orthogonale à la première. S'il va dans une direction, on lui attribuera la valeur 0, s'il va dans l'autre, la valeur 1. Cette valeur est ensuite resoumise au contrôle classique, et en fonction de ce bit, de valeur 0 ou 1, le contrôle classique décide de l'orientation de la prochaine mesure. On répète l'opération. Le modèle est configuré comme suit : on met en place cet ensemble d'états intriqués, on effectue le premier niveau de mesure, on obtient les données probabilistes classiques, on procède à quelques mystérieux calculs et on décide ensuite dans quelle direction on projette le suivant. Et ce processus est universel, il fonctionne pour n'importe quel type de calcul quantique, pour la factorisation ou tout autre type.

Si je souhaite prouver ce dispositif, mais que je n'ai pas confiance dans l'agent aux superpouvoirs, le moyen le plus facile pour effectuer mon test sera de le saturer : je veux être sûre qu'il ne comprend pas ce qu'il fait en sorte qu'il devienne mon esclave au sens propre. Je lui fais effectuer les calculs, mais j'introduis un peu de cryptographie ordinaire, en sorte qu'il effectue les mesures et les calculs sans savoir à quel type de mesure il se livre, ni même connaître les résultats de ses calculs. La seule chose que j'ajoute, c'est que je le rends aveugle. Je fais en sorte qu'il effectue des mesures correctes, mais sans porter à sa connaissance ce nombre magique qu'est l'angle de mesure. Par ailleurs, même s'il connaît les résultats de ses mesures, ces derniers sont également rendus aléatoires à l'aide d'un masque jetable invisible, qui doit son inviolabilité à son usage unique. Il suffit d'appliquer au message un bit aléatoire, en sorte qu'il devienne parfaitement randomisé. Une fois ce message envoyé, le résultat devient lui aussi aléatoire. C'est le principe du masque jetable classique.

Je rappelle que notre protocole de vérification repose sur le caractère aléatoire du quantique. Je cherche à m'assurer que le démonstrateur effectue les bons calculs, sans pour autant qu'il comprenne ce qui se passe. Ainsi, la sécurité est garantie dans la mesure où la variable aléatoire correspondant à l'information reçue par le démonstrateur est totalement indépendante de la variable aléatoire correspondant à l'information secrète.

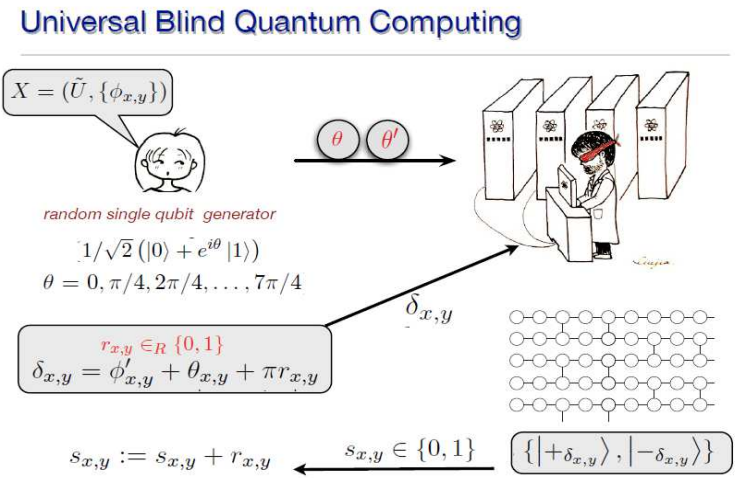

Figure 11 : Calcul quantique universel aveugle

L'équation en haut à gauche de la figure représente la variable aléatoire correspondant au secret détenu par le vérificateur, muni d'un masque jetable : cette variable aléatoire est la clef du message codé envoyé au démonstrateur. En-dessous figure la variable aléatoire quantique, qui est une pièce quantique uniformément aléatoire. On a donc un qubit unique, vecteur dans l'espace de dimension 2, et il s'agit de choisir une structure régulière. θ devient un paramètre, mais selon la théorie quantique, lorsque je vous présente tel état quantique après y avoir encodé mon paramètre aléatoire θ, faute de savoir de quelle manière je l'ai préparé, vous n'en tirerez quasiment aucune information. Cet élément est le plus important (rappelez-vous l'idée très originale de Wiesner sur la cryptographie quantique). Aussi, lorsque je confie ce système physique au démonstrateur – cette boîte magique dotée d'une clef secrète – il est si puissant que tout ce qu'il me faudra par la suite,

c'est que le calcul que je souhaite effectuer corresponde à cette clef. Le masque jetable quant à lui permet premièrement d'envoyer la clef et deuxièmement d'encoder le message. D'ordinaire, on sélectionne un message, on lui ajoute de l'aléatoire, puis on envoie la clef. Ici au contraire, on commence par envoyer la clef puis on y ajoute le message après-coup, l'ensemble étant bien entendu encodé. On envoie donc ces qubits qui sont tous randomisés, en sorte que le démonstrateur ne sait pas du tout à quoi il a affaire. Grâce à la formule magique – mon secret – je m'assure qu'il ne découvre rien. Le message est parfaitement classique : il s'agit de mon message secret et d'une chaîne aléatoire que je combine en sorte qu'ils parviennent au démonstrateur sous une forme totalement confuse dont il ne peut tirer aucune information. Mais ce qui est amusant, c'est que quand je place cet état au-dessus du dispositif physique qui détient la clef, il est décodé : la clef du vérificateur et celle du démonstrateur s'annulent, ce qui signifie que mes calculs sont corrects. J'envoie donc mon élément aléatoire secret, qui ne semble pas correspondre au calcul auquel j'avais pensé, la clef est déjà là, les deux éléments s'annulent en passant par la machine et le démonstrateur n'obtient aucune information.

La première étape se déroule avant même que j'aie connaissance du calcul à effectuer. Soit une entreprise qui vend du matériel quantique et me propose ses services. Je lui achète 100 qubits aléatoires, à titre d'investissement. Je dispose donc désormais de ce petit dispositif qu'on a construit pour moi et à chaque fois que je le sollicite, il me sort une sorte de pièce quantique. Il m'informe : « votre θ est $\pi/4$, et voici le qubit qui encode $\pi/4$ », que j'envoie à l'entreprise. Je sollicite à nouveau ma machine, qui me répond : « votre θ est $\pi/2$, et voici un qubit avec la clef de chiffrement de $\pi/2$ », et ainsi de suite. J'envoie 100 messages de ce type et je garde classiquement en mémoire la séquence $\pi/4$, $\pi/2$, $\pi/8$, et ainsi de suite. Par la suite, peut-être dix ans plus tard, ces qubits sont toujours là qui attendent patiemment, bien intriqués au sein de cette structure. Je n'ai donné aucune information au démonstrateur, dont l'unique rôle consiste à conserver ces pièces pour mon propre usage ; jusqu'au moment où j'ai envie de factoriser. « Pour factoriser, les angles sont censés être les suivants : $3\pi/8$, $5\pi/8$, et $3\pi/4$… », je prends donc $3\pi/8$, l'ajoute à $\pi/4$ (pour obtenir $5\pi/8$), et je demande à l'entreprise de me mesurer ce premier qubit selon un angle de $5\pi/8$. Or $5\pi/8$ ne signifie rien dans la mesure où il n'est pas corrélé à mes données initiales. L'étape suivante consiste à poursuivre les envois d'information. À chaque fois que j'envoie un message, la rotation précédente

s'annule et la rotation correcte se met en place. Il s'agit d'une sorte de décodage : je passe le message à l'entreprise, elle effectue des mesures et me renvoie les résultats, je renouvelle l'opération.

Qu'en est-il de la vérification ? Une fois que je suis en possession de ce petit gadget qui m'assure que le serveur ne sait rien (sinon la dimension du calcul, mais rien de plus), il m'est très facile de le tester puisque je peux m'assurer qu'il effectue des calculs sans se rendre compte de ce qu'il fait. Le reste n'a rien de mystérieux. Puisqu'il agit sans savoir ce qu'il fait exactement, je peux commencer à poser des pièges ici et là. Et puisque je sais où sont les pièges et en quoi consiste le calcul, je peux recoller les informations. Ainsi, pour effectuer à la fois la vérification et les calculs, je continue à glisser des pièges conçus de manière à ce qu'ils ne gênent pas les calculs ; ils en font en fait littéralement partie. C'est comme quand ma mère me testait au retour de l'école. Elle avait des informations sur certains événements survenus tel jour, et lorsque je rentrais à la maison, elle me posait des questions pour voir si je donnais des réponses correctes à propos des événements dont elle avait eu connaissance. Elle en tirait la conclusion que je donnais sans doute des réponses exactes à toutes les questions, car je ne savais pas quelles étaient les questions dont elle avait déjà la réponse. Dans un cas comme celui-là, la probabilité pour que tout soit correct est donc élevée.

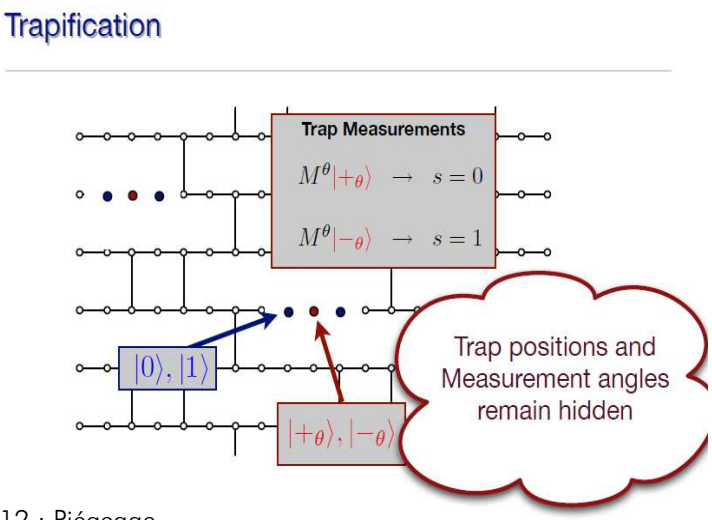

Figure 12 : Piégeage

Dans ce diagramme, les points du milieu représentent des pièges isolés, des états particuliers que j'ai préparés et qui ne sont pas intriqués avec le reste. Les résultats de leurs mesures sont de type déterministe. En général, la mesure d'un état quantique est en fait de type probabiliste, mais si je mesure un état quantique correspondant aux états propres de la mesure observable par l'opérateur, le résultat est de type déterministe. Ainsi, dans mon modèle, toutes les mesures effectuées dans le cadre du calcul général sont de type probabiliste, et je n'ai aucun moyen de vérifier leur exactitude. Mais j'introduis mes pièges, qui sont de type déterministe, pour en faire un champ de mines, et si cette machine non fiable me donne malgré tout la bonne réponse concernant les champs de mines, je puis être sûre que le calcul probabiliste dans son ensemble est correct. Tel est le principe de base. Le cadre dans lequel on établit la preuve de cela est celui de la théorie des probabilités : variables aléatoires, opérateurs de densité, calcul des différences statistiques, etc.

Pour finir, je vous présenterai un aspect de mes recherches actuelles. En suivant le protocole que je viens de vous présenter, pour effectuer un calcul avec 3 bits (ce qui n'est vraiment rien), le nombre de qubits nécessaires est de l'ordre de 300. Ce qui signifie que, dans la réalité, pour s'assurer que ce calcul est correct, il faudrait fixer une limite exponentielle, ce qui nécessiterait d'immenses ressources. Voici donc où nous en sommes : en théorie, le problème est résolu et la question qui se pose désormais est la suivante : avons-nous vraiment besoin d'une limite exponentielle pour prouver l'exactitude du calcul ou bien pouvons-nous faire des compromis là-dessus ?

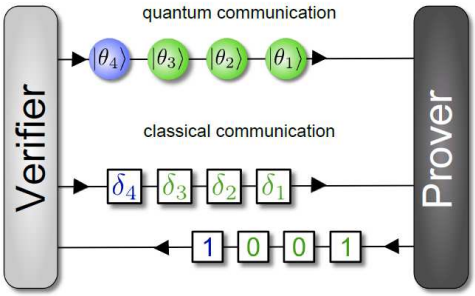

Figure 13 : Que peut-on faire avec 4 qubits ?

Je vais à présent vous rendre compte de travaux que j'ai menés il y a un an, conjointement avec un laboratoire expérimental, le groupe de Vienne sous la direction de Philip Walther. Le nombre de qubits (pas plus de 4) et de rotations mis à notre disposition était limité. Que faire avec cela ? L'enjeu ne se rapporte pas seulement à la technologie quantique, il est également de montrer que théorie et expériences doivent aller de pair : nous ne vivons pas dans un monde différent de celui-ci, et ceci est propre au domaine quantique (et peut-être aussi à celui de la biologie). Nous nous adressons aux équipes d'expérimentation, qui nous félicitent d'avoir trouvé un protocole mais nous demandent de revenir les voir lorsque nous aurons quelque chose à leur proposer qui entre dans le cadre de leur dispositif d'expérimentation. Par la suite, lorsque nous voulons réitérer les expériences, il faut ajuster chacune des preuves. Les preuves doivent être établies dès le départ, et surtout, la question est la suivante : « Ce que nous cherchons à démontrer présente-t-il un intérêt ? » Avant de vous présenter le déroulement de nos travaux, il me semble indispensable de vous donner quelques explications préliminaires.

Partons de ce théorème fondamental qui a révolutionné notre spécialité dans les années 1960 : les inégalités de Bell[8]. Son auteur, John Stewart Bell, a trouvé une recette mathématique permettant de vérifier si tel dispositif est quantique ou

[8] Bell, John (1964), "On the Einstein Podlsky Rosen Paradox", Physics 1(3) : pp. 195–200.

classique. Ce théorème est à mes yeux le plus beau théorème fondamental de tous les temps. L'idée d'intrication quantique est difficile à admettre : comment deux personnes pourraient-elles indépendamment l'une de l'autre lancer deux pièces différentes et obtenir à chaque fois le même résultat, comme ce qui se passe avec l'intrication quantique ? Pour certains penseurs, (voir le paradoxe EPR (Einstein, Podolsky et Rosen, 1935[9]), l'explication tient au fait que physiciens et mathématiciens n'ont pas été capables de fournir une théorie aboutie. Cette corrélation est forcément due à une « variable cachée locale » – une chose cachée à l'intérieur de ma main et de celle de l'autre lanceur de pièce, que la théorie quantique ne décrit pas. Afin de réfuter cette critique, Bell propose un jeu dans lequel l'arbitre donne un bit aléatoire, 0 or 1, à chacun des deux joueurs, Alice et Bob, lesquels doivent répondre par un nombre, 1 ou -1. A et B peuvent utiliser n'importe quelle variable locale cachée et n'importe quelle théorie probabiliste, mais ils ne sont pas autorisés à communiquer l'un avec l'autre au moment de choisir la réponse qu'ils vont transmettre.

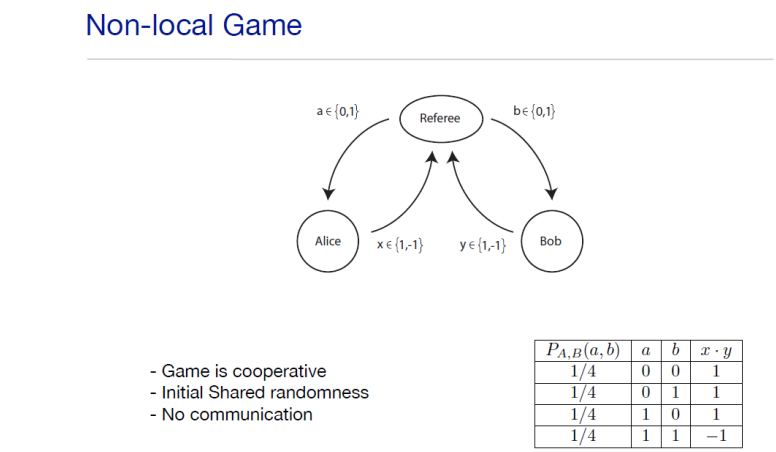

Figure 14 : Jeu non-local

Le tableau inclus dans la figure ci-dessus donne la recette gagnante : si les questions posées à Alice et à Bob sont 0 et 0, le résultat (x fois y) doit être 1, et ainsi

[9] Einstein, Albert, Boris Podolsky, et Nathan Rosen (1935), *Can quantum-mechanical description of physical reality be considered complete? Phys. Rev.* **47** 777.

de suite. On appelle ce jeu extrêmement simple « jeu non-local ». En nous appuyant sur la théorie probabiliste pour déterminer les chances de gain, quelle est la meilleure stratégie corrélée à adopter dans ce jeu si l'on veut que les réponses x et y données par les joueurs à ces bits d'information 0 et 1 correspondent aux réponses gagnantes du tableau (en l'absence de communication entre les joueurs) ? Quelle est la probabilité de gagner dans ce jeu coopératif ? Si les deux joueurs pensent de manière optimale, cette probabilité est de 3/4, soit 75 pour cent. Cela tient au fait que dans la stratégie déterministe optimale, on peut satisfaire trois équations, mais pas la quatrième :

$$\begin{aligned} x &= f(a) \\ y &= g(b) \end{aligned} \qquad \left.\begin{aligned} f(0)g(0) &= 1 \\ f(0)g(1) &= 1 \\ f(1)g(0) &= 1 \\ f(1)g(1) &= -1 \end{aligned}\right\} \Rightarrow \left\{\begin{aligned} f(0) &= g(0) \\ f(0) &= g(1) \\ f(1) &= g(0) \\ f(1) &= -g(1) \end{aligned}\right.$$

Quelle que soit la stratégie probabiliste utilisée, quelle que soit la théorie des variables locales, la probabilité est toujours de 75 pour cent. Ce que Bell a démontré, c'est qu'il existe bel et bien une stratégie quantique, pourvu que les joueurs partagent l'intrication :

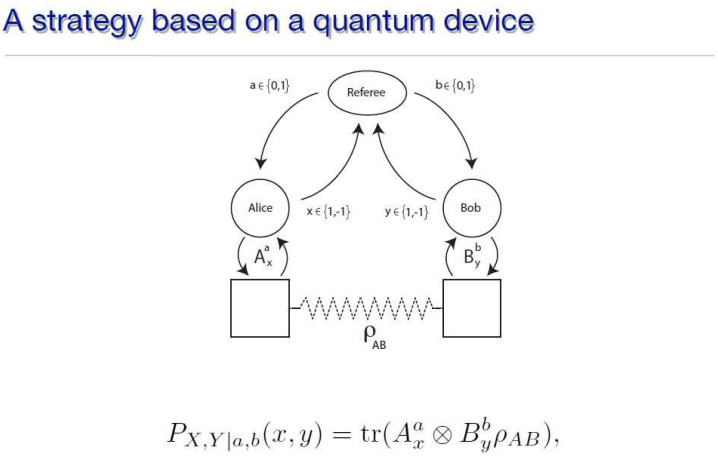

Figure 15 : Stratégie fondée sur un dispositif quantique

dans laquelle, si l'on fait les calculs (voir ci-dessous), la probabilité de gagner est de 85 pour cent. C'est incroyable ! Classiquement, la probabilité de gagner est de 75 pour cent, mais « quantiquement », elle est de 85 pour cent, pour la seule raison qu'existe cette corrélation quantique.

A strategy based on a quantum device

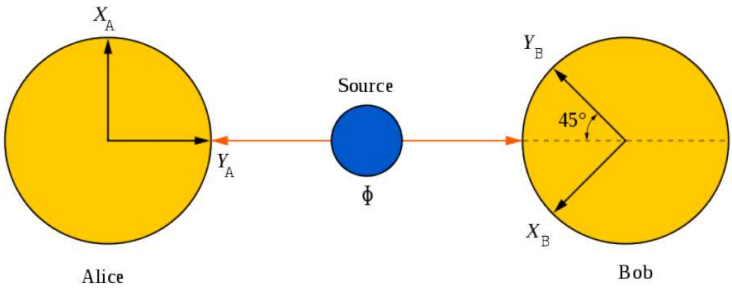

Figure 16 : Stratégie fondée sur un dispositif quantique

$$\rho_{AB} = |\psi\rangle\langle\psi|, \quad |\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

$$\begin{aligned} |\phi_1(\theta)\rangle &= \cos(\theta)|0\rangle + \sin(\theta)|1\rangle, \\ |\phi_{-1}(\theta)\rangle &= -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle. \end{aligned}$$

$$\begin{aligned} A_1^0 &= |\phi_1(0)\rangle\langle\phi_1(0)|, & A_{-1}^0 &= |\phi_{-1}(0)\rangle\langle\phi_{-1}(0)|, \\ A_1^1 &= |\phi_1(\pi/4)\rangle\langle\phi_1(\pi/4)|, & A_{-1}^1 &= |\phi_{-1}(\pi/4)\rangle\langle\phi_{-1}(\pi/4)|. \end{aligned}$$

$$\begin{aligned} B_1^0 &= |\phi_1(\pi/8)\rangle\langle\phi_1(\pi/8)|, & B_{-1}^0 &= |\phi_{-1}(\pi/8)\rangle\langle\phi_{-1}(\pi/8)|, \\ B_1^1 &= |\phi_1(-\pi/8)\rangle\langle\phi_1(-\pi/8)|, & B_{-1}^1 &= |\phi_{-1}(-\pi/8)\rangle\langle\phi_{-1}(-\pi/8)|. \end{aligned}$$

$$
\begin{aligned}
P_{\text{win}} =& \frac{1}{4} \sum_{(a,b,x,y)\in\mathcal{W}} \text{tr}(A_x^a \otimes B_y^b \rho_{AB}) \\
=& \frac{1}{8} \sum_{(0,0,x,y)\in\mathcal{W}} \left| \langle\phi_x(0)|0\rangle\langle\phi_y(\pi/8)|0\rangle + \langle\phi_x(0)|1\rangle\langle\phi_y(\pi/8)|1\rangle \right|^2 \\
&+ \frac{1}{8} \sum_{(0,1,x,y)\in\mathcal{W}} \left| \langle\phi_x(0)|0\rangle\langle\phi_y(-\pi/8)|0\rangle + \langle\phi_x(0)|1\rangle\langle\phi_y(-\pi/8)|1\rangle \right|^2 \\
&+ \frac{1}{8} \sum_{(1,0,x,y)\in\mathcal{W}} \left| \langle\phi_x(\phi/4)|0\rangle\langle\phi_y(\pi/8)|0\rangle + \langle\phi_x(\pi/4)|1\rangle\langle\phi_y(\phi/8)|1\rangle \right|^2 \\
&+ \frac{1}{8} \sum_{(1,1,x,y)\in\mathcal{W}} \left| \langle\phi_x(\pi/4)|0\rangle\langle\phi_y(-\pi/8)|0\rangle + \langle\phi_x(\pi/4)|1\rangle\langle\phi_y(-\pi/8)|1\rangle \right|^2 \\
=& \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \\
\approx& 0.85
\end{aligned}
$$

Alain Aspect fut le premier à réaliser expérimentalement un dispositif satisfaisant les hypothèses du théorème de Bell. Si, quand on joue à ce jeu, il y a une intrication, les données transmises montrent qu'on n'est pas dans le cas d'une théorie de la variable cachée locale. La théorie quantique est donc complète au sens où elle décrit cette corrélation – même si elle demeure incomplète dans sa façon de rendre compte de la gravité, etc. La chose est aussi simple et belle que cela.

Revenons à présent à notre test. Le fait de pouvoir gagner à ce jeu avec une probabilité magique supérieure à 75 pour cent indique que l'on est passé dans le domaine du quantique, et qu'on a quitté l'univers classique. Pour débuter le test, nous disposons donc de 4 qubits : nous mettons en place ce test de Bell, à l'aveugle. Nous avons décidé que si nous disposions d'une boîte construite par une entreprise, nous appliquerions notre technique de vérification après l'avoir adaptée au dispositif, afin de mesurer le pourcentage de gains réalisés par la boîte fournie par cette entreprise. S'il est supérieur à un certain seuil, c'est sans doute qu'il relève du quantique. Rien ne prouve qu'on affaire à du quantique ni à de l'intrication quantique, mais on a la preuve qu'on n'est plus dans le domaine classique. Tel est donc notre point de départ : nous disposons d'un test capable de nous dire si on a affaire à une machine classique magique conçue pour simuler la théorie quantique ou bien s'il s'agit d'une machine authentiquement quantique.

Pour conclure, le calcul quantique universel n'est pas pour demain, mais on voit se développer de nombreux modèles intermédiaires construits sur mesure. Ils ne

sont pas aussi puissants qu'un ordinateur quantique, mais ils effectuent des tâches impossibles à effectuer classiquement, comme de l'estimation de parcours pour le modèle à un qubit pur ou de l'échantillonnage de bosons pour le modèle optique linéaire. De manière générale, tous les « simulateurs quantiques » ne font peut-être pas tout le hamiltonien de la théorie quantique, mais ils font autre chose. Ce que j'aimerais vraiment, ce serait de voir si on peut adapter notre dispositif de vérification quantique à ces modèles. Nous pouvons espérer que, lorsque nous aurons adapté nos dispositifs à ces modèles, nous n'aurons plus besoin des 300 qubits que nous ne pouvons obtenir de toute façon. Une chose est de vérifier l'exactitude des données obtenues, une autre de savoir si ces données proviennent réellement d'un élément quantique. Les inégalités de Bell ne sont qu'un aspect du quantique : il en existe d'autres, comme la corrélation non-classique, les notions de contextualité, de dimensionnalité et de superposition. Notre but est d'identifier avec certitude lequel de ces aspects a été mis en œuvre dans notre boîte quantique.

Commentaires de Damian Markham et questions du public

Je ne suis pas vraiment un expérimentateur. Je fais le lien entre les travaux d'Elham et les expérimentateurs. Nous n'avons pas participé aux expériences décrites par Elham, même s'il existe une équipe à Paris et une autre à Bristol qui mènent des expériences similaires. Mon parcours est un peu différent de celui d'Elham. La question sur laquelle nous travaillons tous deux, à la fois du point de vue de la physique et des sciences de l'information et de la communication, est le suivant : « Cette boîte est-elle ou non quantique ? » Comme l'a signalé Elham, cette question est vaste car, du point de vue de la physique, le problème relève de la physique : si cette boîte représente l'univers, l'intérieur de cette boîte est-il quantique ? L'univers est-il quantique ? Quant à la science de l'information et de la communication, elle s'intéresse à toutes ces applications dont Elham a parlé et à tout ce que l'on pourrait faire de nouveau avec une boîte quantique. À propos de ces millions d'euros mis à notre disposition sous forme de bourses, nous devons en échange nous poser des questions d'ingénieurs : savoir si je veux mettre mon invention sur le marché, si je veux parler de ce que je fais. Ma trajectoire a croisé celle d'Elham à l'endroit même où sa route a croisé celle de l'informatique quantique : dans le bureau de notre directeur, Vlatko Vedral. J'étais physicien de formation. Comme la plupart des personnes qui se lancent dans des études de physique, le goût pour la matière m'est venu en regardant des films de science fiction et en me posant des questions sur le fonctionnement de l'univers. Je ne m'intéressais pas au fonctionnement des ordinateurs, ils n'étaient que des instruments au service de ma passion. En somme, du terme « ordinateur quantique », Elham et moi avons retenu celui qui nous intéressait. Il nous a fallu des années de dispute et de bagarre avant de comprendre que les deux étaient imbriqués. Avant, l'informatique se résumait pour moi à de la programmation, ce qui n'est pas très intéressant, mais j'ai découvert que le domaine était d'une très grande richesse. J'appartiens d'ailleurs aujourd'hui au Laboratoire Traitement et Communication de l'Information (LTCI) du CNRS.

Les questions portant sur ce qui constitue un modèle de calcul et sur la façon de s'interroger sur la puissance d'un ordinateur, etc. – tout cela rejoint les questions des physiciens puisqu'il s'agit de décrire ce qui se passe à l'intérieur. Les questions posées par Elham : « Cette boîte est-elle quantique ? » ou même « cette boîte est-elle

bonne ? » pour parler d'un type de modèle de calcul, rejoignent les questions des physiciens, pour qui elles se posent exactement dans les mêmes termes, par exemple la question du hasard en mécanique quantique dont Elham a parlé à propos du jeu non-local. De manière générale, avant la mécanique quantique, les physiciens pensaient que les probabilités étaient le reflet de notre incapacité à comprendre les choses. Ce point de vue a donné le paradoxe EPR. En physique statistique par exemple, on dira que les particules se répartissent dans la boîte selon une distribution de Boltzmann. On a recours à cette loi de probabilité parce qu'on ne connaît ni la position ni la vitesse de toutes les particules contenues dans la boîte : si c'était le cas, on n'aurait plus besoin de distribution de probabilité, on aurait la force exercée sur les parois, force que l'on peut calculer. En mécanique quantique, en revanche, les probabilités semblent authentiques. L'une des interprétations des inégalités de Bell consiste à dire que, localement, la mécanique quantique est bel et bien probabiliste. Et ceci n'est pas dû à notre ignorance, mais à la nature elle-même. On peut aussi expliquer ce qui se passe dans le calcul quantique et en cryptographie quantique en disant que nous nous servons des effets probabilistes que l'on trouve dans la nature. En particulier, ces effets – ces probabilités que l'on peut partager en mécanique quantique – sont encore plus étranges quand on se les partage à distance. Les termes « contextualité », « dimensionnalité » et « superposition » renvoient tous à la même question : « Comment décrire réellement ce qui se passe ? » En physique, nous avons la chance de voir toutes ces questions se résumer à une seule en quelque sorte. En apparence, il s'agit de questions très différentes les unes des autres : « l'univers est-il aléatoire ou non ? », « Comment procéder pour vérifier si un dispositif est quantique ou non ? », mais en réalité elles sont étroitement liées entre elles. La rencontre de ces deux problèmes, de ces deux trajectoires est, à mes, yeux, ce dont nous a parlé Elham.

Q : Où en sont les machineries quantiques, comme celle que Google a rachetée ?

Elham : Le rachat récent de la machine D-Wave ne signifie pas si elle est quantique ou non, ni même quantique du tout, nous ne savons pas si elle produit une accélération quantique. Pour Google, vingt millions d'euros ne représentent pas une très grosse somme, si bien qu'ils ont acheté ce dispositif. Ils ont un laboratoire dans

lequel ils développent l'apprentissage automatique à des fins d'optimisation. Je suppose que Google veut mettre à l'essai ce dispositif, comme ils le font avec beaucoup d'autres, pour voir s'il y a quelque avantage à en tirer. Mais la communauté scientifique est très partagée à propos de ce dispositif quantique, car certains modèles fondés sur le recuit quantique correspondent aux statistiques des cordes, tandis que d'autres, fondés sur le recuit simulé classique, correspondent aux données. La question est donc de savoir si cela est dû à un modèle quantique ou classique. Google parle d'une machine de 1000 qubits, mais seules sont authentiquement quantiques des unités de 8 qubits.

Le projet reste intéressant à mes yeux : une entreprise commerciale a construit une machine (à l'origine, la propriété intellectuelle devait être très protégée, en sorte que l'entreprise ne devait révéler aucune des données contenues dans la machine, mais par la suite, ils ont changé d'avis). C'est fascinant pour les ingénieurs : des qubits supraconducteurs fonctionnant à des températures proches de zéro, c'est très impressionnant, mais on ne sait toujours pas si l'on a affaire à un phénomène quantique ou classique. S'il est quantique, est-il plus rapide ? Et même si la machine n'était pas quantique, grâce aux investissements privés cette entreprise aura tout de même fait avancé la recherche à un point que les laboratoires de recherche scientifique n'auraient pas pu atteindre. Il semble donc que des partenariats commencent à se former avec certains scientifiques qui cherchent à comprendre le chemin parcouru, là où des améliorations pourraient être apportées, où se trouve exactement la transition entre classique et quantique, etc. et je crois que ce que cherche à faire Google, ainsi que tous ceux qui peuvent s'offrir ce type de machine, c'est de voir ce qu'elle a dans le ventre. Il faut s'imaginer une boîte noire géante dans laquelle on entre des données pour les récupérer à la sortie. Étant donné que la machine est analogique, et non digitale, et qu'il existe toutes sortes de modèles différents, on peut se demander quel domaine est le plus propre à l'évaluer et à en faire la description ?

Q : L'avènement de l'informatique quantique est souvent lié aux changements d'échelle, le fait qu'à une échelle inférieure au nanomètre, les lois de la physique changeaient. Cette association est-elle correcte ?

Elham : il existe en effet un vrai problème technique. Meilleurs sont les ordinateurs, meilleures sont les puces qui les composent. C'est un peu le même combat : en un sens, nous cherchons à construire un effet quantique et à le protéger tandis que l'architecte classique cherche à protéger le soubassement classique contre les effets quantiques. Nous voulons nous assurer que l'effet quantique se produit et qu'il est protégé, tandis que du côté du classique, on cherche à se débarrasser de l'effet quantique. Je pense que l'on arrivera à un point de passage. C'est une question de taille, les machines sont de plus en plus petites. En ce moment, le calcul parallèle intéresse beaucoup de monde. Et c'est vrai aussi pour l'architecture : notre bâtiment à Édimbourg compte cinq étages. Je suis au cinquième, occupée à des choses qui ne servent à rien, des choses théoriques, tandis que les architectes sont au premier. Ces derniers savent qu'il ne reste plus beaucoup de place pour la miniaturisation, aussi y a-t-il eu cet engouement pour le calcul parallèle. Cela nous procurera de la place pour un bon bout de temps, mais la question de la taille se pose aussi avec la parallélisation. Nous en sommes déjà au point où la technique a suscité un intérêt pour la programmation parallèle, l'architecture parallèle, le parallèle sur Internet, la toile parallèle…, c'est un domaine en ébullition. En même temps, personne n'ignore la possibilité du quantique, mais pour exister au sein de cet espace, il faut construire un ordinateur quantique. Si l'on demande aux gens d'investir dans le calcul parallèle parce que cela résoudra nos problèmes pour les dix à vingt années à venir, on passe à la construction ; quant à savoir si la puissance quantique remplacera la puissance parallèle, cela reste à voir.

Q : D'un point de vue conceptuel, pourquoi le quantique devrait-il être plus rapide ?

Elham : Grâce à la superposition, à l'intrication, à toutes les choses qui n'existent pas dans le calcul classique. Si on me posait cette question cocasse : « Croyez-vous en un univers parallèle ? » Eh bien je répondrais oui ! Pour effectuer un calcul, il ne fait aucun doute que le calcul parallèle est plus rapide que le calcul classique. La réponse n'est pas satisfaisante, mais c'est le début de l'explication. Si vous demandez à un million d'ordinateurs de répondre à une question, le calcul s'effectuera plus vite grâce à la puissance apportée par la mise en parallèle. Le calcul quantique s'apparente un peu à cela, parce que nous sommes dans l'univers parallèle : nous transposons chaque mesure de la distribution dans l'univers

parallèle, pour effectuer les calculs dans le cadre d'un parallélisme à grande échelle, et faire ensuite recoïncider cet univers avec le monde classique. C'est comme si un quantique en traitait 1000 autres – ce n'est pas vraiment comme cela que les choses se passent, mais c'est comme si.

Damian : Je crois que ton premier exemple fonctionne comme cela d'un point de vue formel. En rédigeant l'algorithme, on effectue de fait une vérification de type boîte noire sur chacune des entrées. Votre entrée est une superposition de chacune de ces entrées. Et à la fin, il suffit d'effectuer une mesure pour vérifier qu'elles sont identiques.

Q : Si j'ai bien compris, étant donné que chaque qubit se présente dans une superposition d'états, si l'on a n qubits, ayant chacun 2 états, on a alors 2^n états, et à la clef une puissance de représentation exponentielle. En sorte qu'avec 10 qubits, on peut faire l'équivalent de ce que l'on ferait avec 1000 bits classiques.

Elham : Malheureusement, le monde n'est pas si parfait : on ne peut pas faire tout ce que l'on veut avec ces qubits : ils appartiennent à un monde quantique qui ne nous est pas accessible. Tous ces calculs sont miraculeusement effectués, mais au moment de mesurer, on ne retrouve qu'une seule des chaînes (figure 9). Il y en a 1000, mais on ne peut en mesurer qu'une. Si on fait une corrélation habile – grâce à l'amplification et à l'annulation (en raison de nombres complexes négatifs) – et que l'on combine avec bonheur ces chaînes, on peut obtenir une accélération pour un calcul donné. Quelles sont alors les propriétés de ces valeurs ? Grâce au calcul quantique, on pourrait évaluer les relations qui existent entre elles plus vite qu'avec un calcul classique.

Q : Quel est le calcul le plus complexe ayant été effectué expérimentalement à ce jour ?

Damian : Je crois que c'est la factorisation de 21 en 2012.

Elham : Ce qui est vraiment impressionnant, c'est la simulation quantique. Avec la factorisation – c'est un problème classique – si vous voulez faire quelque chose d'utile, il faut prendre le problème au sens pratique, mais on en perd une partie en raison de la présence d'autres éléments. Mais si on dit la chose suivante : « Pour l'instant, mon but n'est pas de vous donner une chose qui ait un sens, une

application utile, pour l'instant je cherche simplement à prouver un principe en vous montrant une véritable application quantique » – alors je crois qu'on peut aller jusqu'à 10 qubits. On arrive à obtenir 10 qubits, la tomographie complète d'une partie du dispositif, et à faire un certain type de simulation hamiltonienne. Mais cela présente-t-il un intérêt ? Comme nous n'en sommes qu'au stade exploratoire, nous ne pouvons répondre catégoriquement. Ce qu'affirment les physiciens – et je pense que s'ils nous promettent 50 ou 100 qubits d'ici cinq ans, ce n'est pas irréaliste car il n'y a pas d'obstacle en vue – c'est qu'une fois qu'on a les 10 qubits, arriver à 50 ou 100 n'est qu'une question d'argent. Aller jusqu'à 1000 serait sans doute plus difficile, mais passer de 10 à 100 est une question de temps de cohérence, de détection à améliorer, etc. Ce n'est pas si facile, mais des idées ont été proposées, comme de faire des paquets de 10, puis 10 et encore 10. C'est ce que nous avons prévu de faire dans l'une des plateformes technologiques britanniques dirigées par Oxford. En les connectant, on améliore le système, mais dans ce rôle intermédiaire, on peut faire des choses qui ne nécessitent pas une totale connectivité, ni la totale cohérence de la factorisation de nombres à dix chiffres, par exemple. Disons qu'on a déjà vu ce que c'était que de présenter des expériences qui ne sauraient être menées classiquement, et qu'on le verra de plus en plus. L'effectuation et la démonstration expérimentale de calculs qui ne peuvent être effectués selon les méthodes classiques : nous y sommes déjà. Que ce type de calcul soit utile, c'est une autre histoire. Mais nous avons déjà dépassé le stade élémentaire de la machine qui « fait mieux que les meilleurs simulateurs classiques ».

Damian : Pour revenir sur les exemples, de l'interprétation des inégalités de Bell en termes de jeu : même si on ne sait pas faire un ordinateur de 10 qubits, on peut quand même jouer à toutes sortes de jeux. Pour prendre l'exemple des communications en réseau, nous disposons de beaucoup de procédés qui ne relèvent pas du calcul, mais qui sont très puissants, comme le protocole de « l'élection du leader » par exemple, sur lequel nous travaillons entre autres choses à Telecom ParisTech.

Elham : Les pressions exercées sur le gouvernement britannique ont porté leurs fruits pour une bonne raison, ces immenses sommes d'argent ne sont pas tombées du ciel. Les économistes le savent : quelles que soient la puissance et l'habileté des lobbies, au fond ce sont les scientifiques qui ont su faire valoir leur

cause auprès des politiques. Beaucoup d'études et de recherches étaient menées au Royaume-Uni comme sur le continent et ailleurs, et c'est cela qui les a convaincus que le moment était venu d'agir.

Q : Des brevets ont-ils été déposés ?

Elham : Bien sûr, en grand nombre ! Je pense que le véritable retour sur investissement de la D-Wave viendra des brevets. Et certainement pas de la vente d'ordinateurs quantiques. Je ne connais pas leur plan de développement, bien entendu, mais ils ont fait breveter tant d'inventions techniques… La toute première entreprise quantique s'appelait *Quantum Magic* ; Je crois qu'elle était implantée à New York… il y a presque vingt ans, bien avant qu'on ait réalisé quoi que ce soit d'un peu concret. Leur projet était d'aider les scientifiques à obtenir des brevets. Nous rédigions des articles pour tenter d'expliquer ce que nous faisions, personne n'y croyait, mais cette entreprise avait flairé quelque chose. Elle a tout de même mis au point une clef de distribution chiffrée, mais son activité principale et la source escomptée de ses revenus étaient fondées sur le partenariat avec le monde scientifique, à travers l'obtention de brevets.

Q : Quels sont les aspects du quantique pouvant faire l'objet de brevets ?

Elham : Je peux vous donner un exemple car je viens justement d'en déposer un. Au début nous ne savions pas comment nous y prendre, mais nous pensions que si nous pouvions commercialiser quelque chose, ce serait dans le domaine de la sécurité, c'est donc de ce côté que nous avons orienté notre stratégie. L'Université d'Édimbourg a donc fait breveter un prototype. Il s'agit en réalité d'un protocole : le protocole BB84 relatif à la distribution de clefs faisant déjà l'objet d'un brevet, nous avons déposé une demande de brevet pour une variante de ce protocole. Notre prototype est destiné à un usage spécial : effectuer un calcul en toute sécurité à partir d'une sorte de support, pour le dire en termes simples. On ne peut pas faire breveter un algorithme, il faut pouvoir présenter une machine. Ne faisant pas d'expérimentation, nous avons fait des schémas, proposé des instructions de montage, puis nous nous sommes adressé à des juristes. Il nous a fallu configurer notre projet en fonction de l'atome, du photon et de notre propre dispositif. Nous avons fait vingt schémas différents. À cette occasion, nous avons pu constater la différence entre la rédaction d'un article et celle d'un dépôt de brevet : tout ce qui est

inutile dans la perspective de l'article doit figurer dans le dépôt de brevet, toutes les possibilités d'exploitation par exemple. Il n'y a rien de quantique dans notre brevet, il s'agit dans un prototype comme les autres. Ensuite, il nous a fallu soumettre notre projet à une entreprise locale employée par l'Université d'Édimbourg pour étudier les potentialités de notre dispositif. L'entreprise en question n'a pas vu en quoi la première idée venue de notre part mériterait les services d'un juriste et le versement de £10,000 pour le dépôt de brevet, en sorte que nous leur avons présenté notre projet, sans rien attendre en échange. Il y a une espèce de hiérarchie : on présente d'abord le projet à un représentant de l'entreprise, qui le présente à une entreprise commerciale, laquelle décide si le produit est susceptible de satisfaire un marché potentiel. Le cas échéant l'université vous donne la somme nécessaire pour faire appel à un juriste qui rédigera le brevet, et ainsi de suite. On ne sait pas à quoi tout cela va aboutir, mais nous avons joué le jeu.

Q : Du point de vue mathématique, quelle est la différence entre une machine classique et une machine quantique ?

Elham : Mathématiquement, la seule chose qui diffère entre les deux, c'est qu'avec le quantique, les nombres sont complexes. Si j'ai un vecteur avec un nombre complexe, le carré de ce nombre est une probabilité. Je peux extraire la probabilité de ce nombre complexe, et obtenir une évolution probabiliste. Lorsque les chaînes passent dans l'univers parallèle, on a toujours affaire à des nombres complexes, positifs ou négatifs. Par exemple, $-\alpha$ et α s'annulent, alors qu'on ne peut avoir de probabilités négatives. Pour utiliser la terminologie de la physique, c'est cette interférence (qu'on retrouve dans les ondes classiques), cette annulation, qui donne au calcul son caractère quantique.

Q : Peut-on prouver qu'un ordinateur ou une boîte est ou non quantique, en suivant un processus purement déterministe, ou bien ne peut-on se passer de cette part d'aléatoire ?

Elham : Je pense qu'on finira par résoudre cette question très intéressante : faut-il une part de quantique pour tester le quantique ? Mais le quantique que nous utilisons pour nos tests est en quelque sorte de type « déterministe ». Je vous donne une paire de particules dans un état de Bell : il n'y a pas d'aléatoire. Nous sommes dans un cadre déterministe et je peux le vérifier. Même dans un tel protocole, j'ai

besoin des probabilités classiques pour le cacher – Donc, non, même si je mets cette ressource à votre disposition de manière quantique, ce qui créera de l'aléatoire par la suite, je suis contrainte de recourir à une forme classique d'aléatoire dans mon protocole… c'est BPP versus P, c'est toujours de l'aléatoire... on ne peut pas se passer de l'aléatoire, on ne peut pas se passer du Centre Cournot pour l'instant !

La collection *Prismes*

La collection *Prismes* rassemble des textes originaux qui traitent de questions théoriques contemporaines. Ses auteurs sont des contributeurs aux conférences, aux débats ou aux séminaires du Centre et de la Fondation.

Dernières parutions

35. Les big data changent-ils la donne en finance ?
Mathieu Rosenbaum

34. Saturation et croissance : Quand la demande en matières premières stagne
Raimund Bleischwitz et Victor Nechifor

33. Une analyse temps-fréquence des données des prix de pétrole
Josselin Garnier et Knut Sølna

32. Les raisons du (quasi-) succès du traitement automatique de la parole
Mark Liberman

31. ***Comment fuir le long d'une droite***
Laure Dumaz

La liste complète des publications se trouve sur le site
www.centre-cournot.org

Elham Kashefi est informaticienne, professeure associée à la faculté d'informatique d'Edimbourg et chercheuse au CNRS, au Laboratoire traitement et communication de l'information (LTCI) de Télécom ParisTech. Elle est directrice adjointe du « Pivot des techniques de l'information quantique en réseau » (NQIT), dont elle assure le développement des applications, entre théorie et expérimentation. Elle est également membre du Centre parisien pour l'informatique quantique (CPIQ) et de l'Académie junior des sciences d'Ecosse. Depuis ses études, Elham Kashefi s'investit dans l'exploration des champs transdisciplinaires du traitement quantique de l'information, de leurs perspectives les plus abstraites à leurs déclinaisons les plus appliquées.

Damian Markham est un physicien quantique, spécialiste d'informatique, chargé de recherches au CNRS en informatique théorique, dans le laboratoire LTCI. Il a participé à la création du groupe interdisciplinaire qui travaille sur les aspects de l'information quantique, de la conceptualisation à la mise en pratique. Cette démarche bénéficie du soutien du nouveau Centre parisien pour l'informatique quantique (PCQC), qui coordonnent les meilleures recherches des physiciens et des informaticiens du quantique.

Publication sous la direction de Jean-Philippe Touffut
Illustration : NiboR / Mise en page : Sophie Otrage