

L'ESSENTIEL

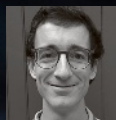
> Selon le principe de localité, toute information ou influence se propage continuellement à une vitesse inférieure ou égale à celle de la lumière. La physique quantique s'est révélée incompatible avec ce principe.

> Dans l'expérience GHZ consistant à mesurer l'état de photons issus d'une source unique, on a montré que les corrélations entre les résultats obtenus ne peuvent s'expliquer en préservant le principe de localité.

> Un futur internet quantique mettra en œuvre de nombreuses sources indépendantes de photons, ce qui amène à étudier la non-localité dans un réseau formé de plusieurs sources.

> Les physiciens étudient les scénarios les plus simples avec deux ou trois sources, des systèmes déjà complexes à analyser.

LES AUTEURS



MARC-OLIVIER RENO
postdoctorant à l'institut des sciences photoniques de Barcelone



NICOLAS GISIN
professeur à l'université de Genève et à l'institut de technologie de Schaffhausen, à Genève



NICOLAS BRUNNER
professeur à l'université de Genève

La non-localité quantique à l'ère des réseaux

Les lois de la physique quantique semblent incompatibles avec le principe de localité, selon lequel deux objets distants ne peuvent pas s'influencer instantanément. Assez bien comprise pour des photons émis par une source unique, cette non-localité reste à cerner dans le cas d'un internet quantique, réseau où de nombreuses sources indépendantes de photons seront à l'œuvre.

Aujourd'hui, une partie sensible de nos vies circule sur internet : nos données bancaires ou médicales, nos courriers électroniques, nos messages sur les réseaux sociaux, nos photos, etc. Pour garantir une transmission sécurisée de ces informations sans qu'elles soient volées, lues ou altérées, des techniques de chiffrement ont été développées. Elles s'appuient sur des problèmes mathématiques qui, sans la clé de déchiffrement, ne sont pas résolus en un temps raisonnable par des ordinateurs classiques. Par exemple, certains algorithmes reposent sur le fait que la décomposition en facteurs premiers de très grands nombres entiers est un tel problème.

Cependant, le développement d'ordinateurs quantiques à l'horizon de quelques années pourrait rendre obsolètes ces techniques de chiffrement. Des algorithmes, qualifiés de quantiques, exploiteraient toute la puissance de la physique quantique afin de résoudre rapidement des problèmes inaccessibles à leurs concurrents classiques. C'est le cas de l'algorithme proposé en 1994 par le mathématicien américain Peter Shor, qui est en théorie capable de factoriser très vite de très grands nombres entiers. Ainsi, quand les ordinateurs quantiques auront été mis au point, les transmissions de coordonnées bancaires lors d'achats en ligne ne seront plus à l'abri d'une attaque. Quelles seront alors les solutions ? Les phénomènes quantiques, à l'origine des capacités de déchiffrement de



La non-localité est au cœur de la mécanique quantique. Elle devient très difficile à étudier dans un réseau muni de plusieurs sources de photons indépendantes. L'analyser dans ce cadre permet cependant d'avoir une compréhension encore plus fondamentale de ce phénomène contre-intuitif.

cette future génération d'ordinateurs, pourraient aussi être la clé pour construire un «internet quantique» hautement sécurisé.

Le concept d'internet quantique recouvre de nombreux dispositifs et idées, dont le développement est un défi à la fois technologique et théorique (voir l'entretien avec Nicolas Gisin, pages 22 à 27). En particulier, la propriété importante qui nous intéresse ici et qui se manifeste dans les systèmes quantiques, des plus simples manipulant juste des paires de photons (les particules élémentaires de lumière) aux plus complexes tels que l'internet quantique, est celle de la non-localité. Et si la physique quantique a la réputation d'être contre-intuitive, c'est surtout en raison de son caractère non local.

UN PRINCIPE ÉVIDENT ?

Pour comprendre cette non-localité, rappelons ce qu'est le principe de localité. D'après celui-ci, toute information ou influence se propage continûment, de proche en proche, à une vitesse finie inférieure ou égale à celle de la lumière, en vertu des lois de la théorie de la relativité restreinte. Le principe de localité semble *a priori* évident pour notre intuition, forgée à partir de notre expérience du monde classique et macroscopique. Pourtant, il n'en est rien à l'échelle microscopique.

Pour être plus précis, le principe de localité ne s'accorde pas avec la physique quantique si l'on admet une hypothèse, celle de l'indépendance du choix de la mesure. Selon cette hypothèse, il est possible de choisir la façon de mesurer un système indépendamment du système lui-même, et il n'existe pas une cause qui soit à la fois à l'origine du choix de cette façon de mesurer et à l'origine de l'état du système (voir l'encadré page ci-contre).

En passant du monde macroscopique à l'univers microscopique et quantique, certains des principes fondamentaux de la physique classique ne s'appliquent plus et doivent être abandonnés. Imaginons un détective armé de son intuition «classique». Il serait bien en peine de percer à jour certaines énigmes du monde microscopique. Il serait confronté à des situations où, par exemple, raisonner simultanément sur la position et la vitesse d'un suspect au moment du crime n'a pas de sens, où l'auteur du crime pourrait être à deux endroits en même temps et où la victime pourrait être à la fois morte et vivante !

Depuis la naissance de la mécanique quantique il y a presque un siècle, les physiciens ont démontré expérimentalement la solidité de cette théorie. Bien que les lois quantiques heurtent l'intuition, ils ont appris à se forger une «intuition quantique» qui leur permet d'en être familiers et de mieux les comprendre. La non-localité quantique a ainsi une histoire riche, ponctuée de débats, de percées théoriques et

d'expériences de pointe. Les physiciens ont mis à l'épreuve leurs idées à ce sujet dans des expériences faisant appel à des sources émettant deux ou trois photons. Or les résultats de ces tests ne pouvaient s'expliquer qu'en remettant en cause le principe de localité (ou alors, celui de l'indépendance du choix de la mesure).

Si l'on peut dire aujourd'hui que la non-localité dans les expériences impliquant une source unique de photons est bien comprise, l'internet quantique bouleverse cette notion. En effet, concevoir un réseau pour l'internet quantique n'est possible qu'en introduisant de multiples sources indépendantes de photons. Le fait de passer d'une source unique à deux sources, trois, etc., change complètement l'analyse du système et la façon dont la non-localité se manifeste.

Depuis une dizaine d'années, alors que l'intérêt pour l'internet quantique grandit, les physiciens théoriciens se sont aussi penchés sur ces systèmes à plusieurs sources de photons. Ils commencent seulement à entrevoir la façon de repenser la notion de non-localité. La formulation de cette dernière ne serait pas unique, mais dépendrait du contexte où elle se manifeste. À terme, une compréhension plus fine des subtilités de la non-localité en réseau débouchera certainement sur de nouvelles applications, voire contribuera à améliorer l'internet de demain.



L'internet quantique bouleverse la notion de non-localité



Pour saisir les enjeux de la non-localité quantique, il est nécessaire de comprendre comment les physiciens sont parvenus à appréhender progressivement cette notion au cours des cent dernières années.

Très tôt dans l'exploration des fondements de la mécanique quantique, les physiciens ont rencontré des difficultés à penser et à formuler cette situation paradoxale. Comment deux principes qui semblaient évidents pour les scientifiques du début du xx^e siècle (la localité et l'indépendance du choix de la mesure) pouvaient-ils être incompatibles avec la physique quantique ? Dans les années 1930, Albert Einstein et deux collègues, Boris Podolsky et Nathan Rosen, ont lancé le débat dans un article resté célèbre, qui s'étonnait d'une «mystérieuse action à distance» incluse dans le