La mécanique quantique, clé de la sécurité des échanges

Omar Fawzi

Puis-je chiffrer mes données en utilisant un appareil dont je ne connais pas l'origine ? Oui, à condition qu'il soit quantique. Mode d'emploi.

Dans sa nouvelle *Le Scarabée d'or*, parue en 1843, l'écrivain Edgar Allan Poe écrivait : « On peut affirmer sans ambages que l'ingéniosité humaine ne saurait concocter un code secret que l'ingéniosité humaine ne puisse résoudre. » Et de fait, depuis leur apparition il y a plusieurs millénaires, peu de codes ont résisté à l'ingéniosité de ceux qui ont voulu les percer. Ces temps sont peut-être révolus avec l'irruption dans le monde de la cryptographie de la physique quantique et ses étranges propriétés qui défient le sens commun. Mais certaines conditions doivent être respectées.

Pour qu'Alice et Bob puissent s'envoyer des données de façon confidentielle, ils ont besoin d'échanger une clé secrète sans laquelle il est impossible déchiffrer le message transmis. Cependant, cette clé ne doit pas être interceptée… Cette clé secrète peut être générée par un protocole quantique d'échange de clé comme l'ont montré en 1984 Charles Bennett, chez IBM, et Gilles Brassard, alors à l'université Cornell, aux États-Unis. La sécurité de l'échange est garantie par le principe d'incertitude de Heisenberg, selon lequel certaines paires de propriétés physiques, telles la position et la quantité de mouvement d'une particule, sont complémentaires et ne peuvent être connues avec précision simultanément.

Dans le protocole quantique d'échange de clé secrète, Alice et Bob utilisent chacun un dispositif quantique avec lequel ils encodent l'information qu'ils se transmettent. La sécurité de ce protocole est mathématiquement prouvée, mais sa mise en pratique impose que les dispositifs quantiques soient correctement implémentés. Dans le cas contraire, le protocole serait vulnérable. Des défauts peuvent être involontaires (bruit, négligence…) ou intentionnels, de la part d'un adversaire ayant eu accès au dispositif, par exemple le constructeur ou le vendeur. Peut-on s'assurer que le protocole, même imparfaitement implémenté, reste sûr ? Est-il possible de garantir la sécurité d'un protocole sans connaître les détails de l'implémentation des dispositifs utilisés ? Étonnamment, la réponse est oui, grâce à justement à une propriété de la mécanique quantique. Ainsi, à condition que les dispositifs soient bien isolés, on obtient un protocole dit « device-independent », c'est-à-dire dont la sécurité ne dépend pas des détails d'implémentation des dispositifs utilisés.

> Depuis leur apparition, il y a des millénaires, peu de codes ont résisté à l'ingéniosité de ceux qui ont voulu les percer

JOUONS AVEC ALICE ET BOB

La brique de base des protocoles « device-independent » est un jeu collaboratif à deux joueurs, Alice et Bob, avec un arbitre. Détaillons-le. Avant la partie, Alice et Bob peuvent décider d'une stratégie commune qui dépend des règles du jeu, mais dès que la partie commence, ils

© Darkfoxelixir/Shutterstock

La physique quantique, garante de la sécurité des échanges sur des appareils inconnus.

ne peuvent plus communiquer. L'arbitre choisit au hasard une question x, parmi deux choix (notés 0 ou 1) qu'il envoie à Alice et une question y du même type à destination de Bob. Chacun des joueurs renvoie à l'arbitre une réponse (a pour Alice et b pour Bob, a et b étant là aussi égal à 0 ou 1). L'arbitre, ayant accès aux questions et aux réponses, décide alors si les joueurs ont gagné ou perdu en fonction des règles du jeu.

Voyons un exemple avec les règles suivantes:

Les règles du jeu		
x	y	Conditions pour gagner
0	0	$a = b$
0	1	$a = b$
1	0	$a = b$
1	1	$a \neq b$

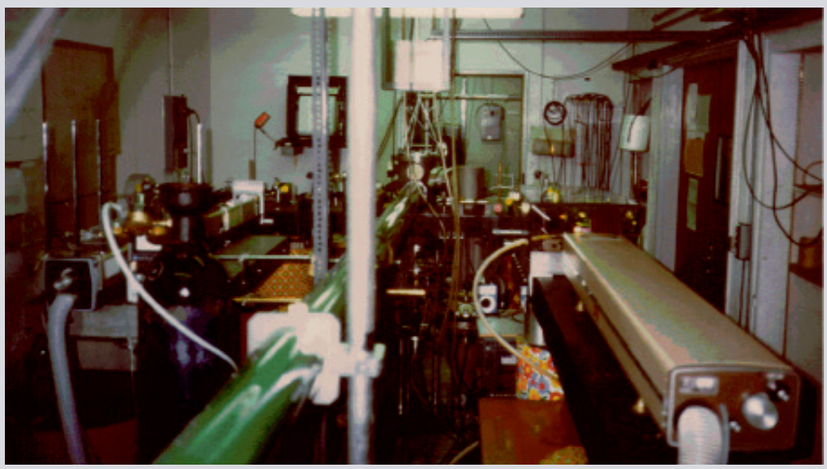
D'après la première ligne, lorsque Alice reçoit $x = 0$ et Bob reçoit $y = 0$ alors les réponses $(a = 0, b = 0)$ et $(a = 1, b = 1)$ sont gagnantes alors que les deux autres paires de réponses $(a = 0, b = 1)$ et $(a = 1, b = 0)$ sont perdantes puisque la condition pour gagner est que $a = b$.
Ici, Alice et Bob peuvent en amont décider de renvoyer la valeur 0 quelle que soit la question. Ainsi, ils gagnent dans tous les cas sauf lorsque $x = y = 1$ (puisque la condition pour gagner est que $a \neq b$), c'est-à-dire avec une probabilité de 3/4, soit 0,75. Peuvent-ils faire mieux? Il faut bien garder en tête qu'Alice et Bob ne peuvent pas communiquer après avoir reçu leurs questions et donc Bob ne connaît pas la valeur de x. Ainsi, lorsqu'il reçoit la question $y = 1$, il ignore si Alice a reçu $x = 0$ auquel cas il faut satisfaire $a = b$ pour gagner ou bien si $x = 1$ valeur pour laquelle la condition pour gagner est $a \neq b$.
Il est assez facile de se convaincre qu'il est impossible de gagner avec une probabilité supérieure à 0,75. En effet, si on note A_0 et A_1 les réponses d'Alice lorsqu'elle reçoit respectivement $x = 0$ et $x = 1$, et B_0 et B_1 les réponses de Bob lorsqu'il reçoit respectivement $y = 0$ et $y = 1$, il suffit d'observer que pour tous les choix possibles de A_0, A_1, B_0 et B_1 (toutes les stratégies déterministes possibles), au plus trois des quatre conditions sont satisfaites.

INTRIGANTE INTRICATION

Que se passe-t-il quand Alice et Bob ont recours aux lois de la mécanique quantique? Dans ce cas, ils ont chacun une particule quantique, par exemple un photon, et vont se mettre d'accord sur une stratégie quantique. Pour Alice, celle-ci est définie mathématiquement par deux bases orthonormées du plan: $(\vec{A}_0(0), \vec{A}_0(1))$ pour l'entrée $x = 0$ et $(\vec{A}_1(0), \vec{A}_1(1))$ pour $x = 1$.
Et de même pour Bob, sa stratégie est définie par $(\vec{B}_0(0), \vec{B}_0(1))$ pour l'entrée $x = 0$ et $(\vec{B}_1(0), \vec{B}_1(1))$.
Avec une telle stratégie, Alice et Bob jouent au jeu de la façon suivante. Lorsqu'elle reçoit la question x, Alice «mesure» sa particule dans la base $(\vec{A}_x(0), \vec{A}_x(1))$ et obtient un résultat a (0 ou 1) qui correspond à sa réponse. Dans le cas d'un photon, cette mesure est celle de sa polarisation avec un polariseur aligné avec la base $(\vec{A}_x(0), \vec{A}_x(1))$ et la réponse a est 0 si le photon passe et 1 sinon. Bob utilise la même procédure, sur sa particule et en utilisant la base $(\vec{B}_y(0), \vec{B}_y(1))$ s'il reçoit la question y.
La découverte très surprenante du physicien John Bell est que si les particules d'Alice et Bob sont préparées dans un état quantique particulier, dit intriqué, alors ils peuvent gagner à ce jeu avec une probabilité égale à $\cos^2(\pi/8)$, soit environ 0,85,

BELL VS. EINSTEIN

Bien qu'il ait contribué à son développement, Albert Einstein n'a jamais complètement admis ce qu'impliquait la physique quantique, et notamment l'intrication, cet état de deux particules, comme des photons polarisés, pour lesquels le formalisme prédit de très fortes corrélations quelle que soit la distance les séparant. En 1935, il publie avec Boris Podolsky et Nathan Rosen l'article «La description quantique de la réalité physique peut-elle être considérée comme complète?». Selon les trois physiciens, l'intrication quantique implique soit que les deux particules échangent des informations qui se propagent plus vite que la lumière (ce qui violerait la théorie de la relativité restreinte), soit que la physique quantique est incomplète et que des «variables cachées», inconnues, donnent l'illusion de l'intrication quantique: c'est le paradoxe EPR.
En 1964, le physicien irlandais John Bell démontre que pour deux particules intriquées, il est impossible d'invoquer des «variables cachées».



Dispositif de l'expérience d'Alain Aspect en 1982.

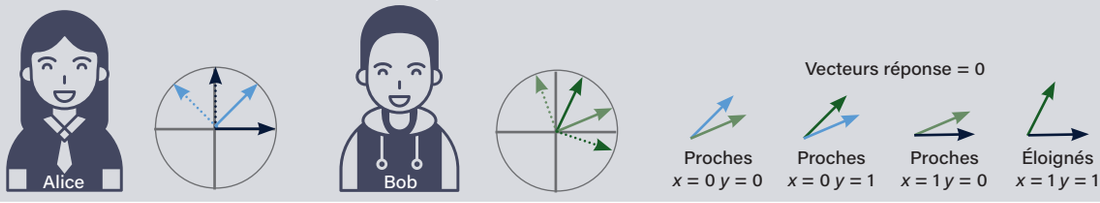
© A. Aspect

Et sa démonstration passe par la définition d'inégalités qui, si Einstein, Podolsky et Rosen ont tort, ne devraient pas être vérifiées. C'était la porte à l'expérimentation, et elle sera franchie en 1982 par Alain Aspect et son équipe qui parvinrent à montrer que l'intrication implique bien une corrélation à distance. La vision dite «réaliste locale» du monde que défendait Einstein n'est pas valide.

INTRICATION ET PROBABILITÉS

Si les particules d'Alice et de Bob sont préparées dans le bon état intriqué, alors pour les questions x et y, la probabilité d'obtenir les réponses a et b est donnée par $\frac{1}{2}|\langle\vec{A}_x(a)|\vec{B}_y(b)\rangle|2$. Prenons un exemple simple : si les 4 bases définissant les deux stratégies sont les mêmes, alors pour tout x et y, on obtient toujours $a = b$. En effet, en utilisant l'orthogonalité de la base, on a $\langle\vec{A}_x(a)|\vec{B}_y(b)\rangle = 0$ lorsque $a \neq b$ et $\langle\vec{A}_x(a)|\vec{B}_y(b)\rangle = 1$ quand $a = b$; puisque $a = b$ recouvre les deux cas $a = b = 0$ et $a = b = 1$ qui sont équiprobables, la probabilité d'obtenir les réponses $a = b = 0$ ou $a = b = 1$ est ½. Cette stratégie est donc gagnante dans tous les cas sauf lorsque $x = y = 1$, ce qui donne encore une probabilité de gagner de 0,75.

Pour faire mieux que, il faut construire des vecteurs tels que $\vec{A}_x(0)$ est « proche » de $\vec{B}_y(0)$ lorsque $x = y = 0$, ou $x = 0$ et $y = 1$, ou encore $x = 1$ et $y = 0$, mais « éloigné » lorsque $x = y = 1$ *(voir ci-dessous)*. On obtient pour tout x et y, si a et b satisfont les conditions gagnantes décrites dans le texte, $|\langle\vec{A}_x(a)|\vec{B}_y(b)\rangle|2 = \cos^2(\pi/8)$, soit environ 0,85, ce qui correspond à la probabilité de gagner.



Les deux bases d'Alice sont représentées en bleu et celles de Bob en vert. La base en couleur claire correspond à la question 0 et la couleur foncée à la question 1. Le vecteur en continu correspond à la réponse 0 et le vecteur en pointillé correspond à la réponse 1. Deux vecteurs sont « proches » lorsque le cosinus au carré de leur angle vaut $\cos^2 \pi/8$ (l'angle est $\pi/8$ ou $7\pi/8$) et « éloignés » si le cosinus au carré de leur angle vaut $\cos^2 3\pi/8$.

ce qui est notablement supérieur à 0,75 (*voir l'encadré x2x*). Deux particules quantiques sont intriquées lorsqu'elles ont une forme de corrélation forte permise par les lois de la mécanique quantique. Dans les années 1930, la nature étrange de l'intrication n'avait pas été acceptée par Albert Einstein, mais en 1964 le physicien John Bell a montré qu'il fallait faire avec lorsqu'il a exploité ce phénomène de manière précise à travers un jeu semblable à celui d'Alice et Bob (*voir l'encadré page ci-contre*).

FABRIQUER DE L'ALÉA

Comment utiliser un tel jeu pour construire un protocole « device-independent » ? L'observation importante ici est qu'un gain au jeu avec une probabilité strictement supérieure à 0,75 certifie que les dispositifs utilisés ne peuvent pas être déterministes, et sont donc quantiques. En effet, comme on l'a vu, on sait que pour toute stratégie déterministe, la probabilité de gagner est bornée par 0,75.

Avec des dispositifs quantiques, on ne peut pas a priori exactement caractériser leur fonctionnement, mais on peut assurer que s'ils sont bien isolés pendant le jeu, alors les réponses a et b générées par les joueurs doivent contenir de l'aléa utilisable pour construire la clé secrète.

Concrètement, Alice et Bob utilisent leurs dispositifs quantiques pour jouer au jeu n fois de façon séquentielle avec les questions $x_1, x_2..., x_n$ et $y_1, y_2..., y_n$ qui sont générées au hasard. Alice obtient les réponses $a_1, a_2..., a_n$ et Bob les réponses $b_1, b_2..., b_n$. Ensuite, Alice choisit au hasard un ensemble de parties et envoie les x_i et les a_i de chacune à Bob. Ce dernier peut ensuite déterminer la fraction η de ces parties qui ont été gagnées. Si $\eta \leq 0{,}75$, Bob annonce l'abandon du protocole (les dispositifs ne sont pas bons). En revanche, quand $\eta > 0{,}75$, Alice et Bob peuvent garantir que les séquences $a_1, a_2..., a_n$ et $b_1, b_2..., b_n$ contiennent de l'aléa privé. La génération de la clé secrète se fait à l'aide d'un algorithme classique (non de quantique) que l'on ne décrira pas ici.

Aujourd'hui, les travaux en cryptographie quantique « device-independent » restent encore théoriques et les réalisations expérimentales se limitent à des preuves de principe. La difficulté réside dans la réduction au maximum les différentes sources d'erreurs. Mais avec le développement des technologies quantiques, nul doute que nous verrons ces protocoles d'échange de clé mis en pratique. Alors peut-être l'affirmation d'Edgar Allan Poe sera-t-elle contredite…

Omar Fawzi
Directeur de recherche Inria au sein du Laboratoire de l'informatique du parallélisme, à l'École Normale Supérieure de Lyon

W. Zhang et al., A device-independent quantum key distribution system for distant users, Nature, 2022.
D. Nadlinger et al., Experimental quantum key distribution certified by Bell's theorem, Nature, 2022.

Retrouvez l'original de cet article ici : https://bit.ly/Interstices-MecaQCryp