POUR LA SCIENCE
Édition française de Scientific American

HORS-SÉRIE

COMPLÉTEZ VOTRE COLLECTION DÈS MAINTENANT !

N° 106 (févr. 20)
réf. DO106

N° 105 (nov. 19)
réf. DO105

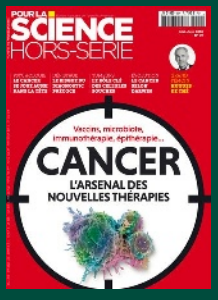
N° 104 (juil. 19)
réf. DO104

N° 103 (avr. 19)
réf. DO103

N° 102 (fév. 19)
réf. DO102

N° 101 (nov. 18)
réf. DO101

N° 100 (août 18)
réf. DO100



N° 99 (mai 18)
réf. DO099

N° 98 (févr. 18)
réf. DO098

N° 97 (nov. 17)
réf. DO097

N° 96 (août 17)
réf. DO096

N° 95 (avr. 17)
réf. DO095

RETROUVEZ L'ENSEMBLE DES ANCIENS NUMÉROS SUR **BOUTIQUE.POURLASCIENCE.FR/HORS-SERIE.HTML**

À retourner accompagné de votre règlement à :
Pour la Science – Service VPC – 19 rue de l'Industrie – BP 90053 – 67402 Illkirch Cedex – email : pourlascience@abopress.fr

☑ **OUI, je commande des numéros de Pour la Science Hors-série, au tarif unitaire de 10,90 €.**

1 / JE REPORTE CI-DESSOUS LES RÉFÉRENCES à 5 chiffres correspondant aux numéros commandés :

1re réf. 0 1 x 10,90 € = 1 0 9 0 €
2e réf. ____ x 10,90 € = ____ €
3e réf. ____ x 10,90 € = ____ €
4e réf. ____ x 10,90 € = ____ €
5e réf. ____ x 10,90 € = ____ €
6e réf. ____ x 10,90 € = ____ €

TOTAL À RÉGLER ____ €

Offre valable jusqu'au 31/12/20 en France Métropolitaine. Pour une livraison à l'étranger, merci de consulter **boutique.pourlascience.fr**

Les informations que nous collectons dans ce bon de commande nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société *Pour La Science*. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. *Pour la Science* ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à *Pour la Science*. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante : https://rebrand.ly/charte-donnees-pls Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit « RGPD ») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse protection-donnees@pourlascience.fr.

2 / J'INDIQUE MES COORDONNÉES

☐ M. ☐ Mme
Nom : .....
Prénom : .....
Adresse : .....
.....
Code postal ____ Ville : .....
Téléphone ____
J'accepte de recevoir les offres de Pour la Science ☐ OUI ☐ NON

3 / JE CHOISIS MON MODE DE RÈGLEMENT

☐ **Par chèque à l'ordre de** *Pour la Science*
☐ **Carte bancaire**
N° ____ ____ ____ ____
Date d'expiration ____ ____
Clé (les 3 chiffres au dos de votre CB) ____

Signature obligatoire :

Groupe Pour la Science – Siège social : 170 bis, boulevard du Montparnasse, CS20012, 75680 Paris Cedex 14 – Sarl au capital de 32000 € – RCS Paris B 311 797 393 – Siret : 311 797 393 000 23 – APE 5814 Z

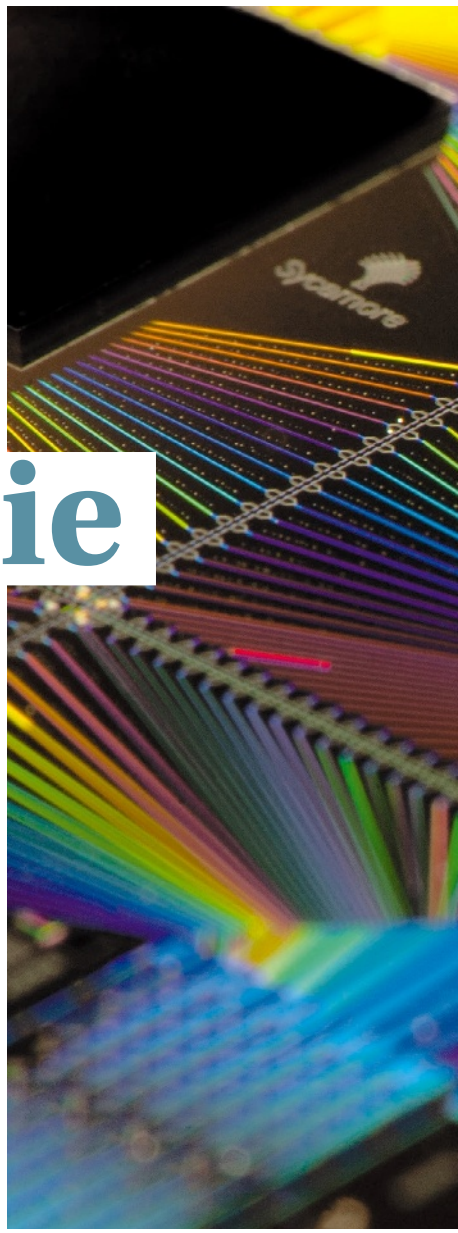
PLUS SIMPLE, PLUS RAPIDE
ABONNEZ-VOUS SUR BOUTIQUE.POURLASCIENCE.FR

L'ESSENTIEL

- L'ordinateur quantique Sycomore, de Google, aurait calculé en 200 secondes ce qu'il aurait fallu 10000 ans à un calculateur classique.
- Cette annonce, signifiant que la « suprématie quantique » est atteinte, ne fait pas consensus, notamment chez IBM, détenteur du plus rapide supercalculateur classique.
- Le débat porte essentiellement sur ce qu'il faut entendre par cette expression, et sur la nature des problèmes résolus.
- Il n'empêche, ce n'est de toute façon qu'une question de temps pour que l'ordinateur quantique dame le pion aux machines classiques.

L'AUTEUR

KEVIN HARTNETT est journaliste à *Quanta Magazine*.



Une suprématie contestée

Google et IBM, les deux principaux rivaux dans le domaine des calculateurs quantiques, s'opposent à coup d'annonces spectaculaires et contradictoires. Comment démêler le vrai du faux ?

Quanta magazine

Cet article a d'abord été publié en anglais par *Quanta Magazine*, une publication en ligne indépendante soutenue par la Simons Foundation afin de favoriser la diffusion des sciences: http://bit.ly/QM-IBMGOO

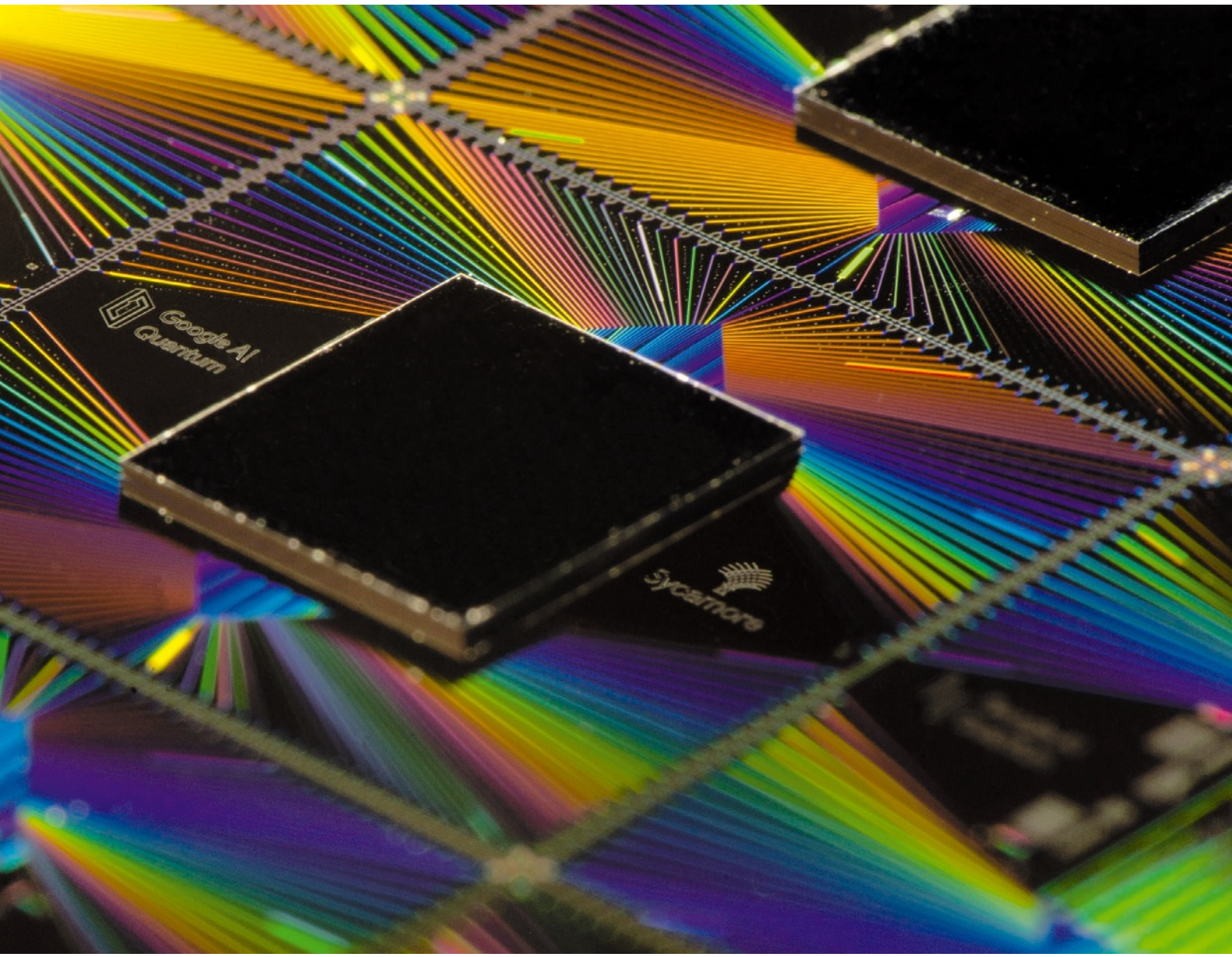
Par un matin du mois d'octobre 2019, des chercheurs de Google sont officiellement rentrés dans l'histoire de l'informatique. Ou pas...

Le géant de la technologie avait annoncé avoir atteint une étape majeure et depuis longtemps anticipée, nommée « suprématie quantique ». Il s'agit du tournant décisif à partir duquel un ordinateur quantique devient capable d'exécuter un calcul qu'aucun ordinateur ordinaire ne peut effectuer dans un temps raisonnable.

NON DE CODE SYCAMORE

Dans une étude publiée dans *Nature*, Google décrit une telle prouesse, accomplie par leur machine quantique dernier cri, au nom de Sycamore. Les ordinateurs quantiques ne sont pas encore développés au point d'être utilisables à des fins pratiques, mais ces résultats montrent qu'ils ont un avantage inhérent par rapport aux ordinateurs normaux pour certaines tâches.

Pourtant, IBM, le rival principal de Google dans ce domaine conteste l'annonce et affirme



© Google

Sycamore, le calculateur quantique de Google, a-t-il atteint la suprématie quantique ?

que le seuil de la suprématie quantique n'aurait pas encore été franchi. Dans un article posté en ligne, la société d'informatique avance des preuves montrant que le supercalculateur le plus puissant du monde peut quasiment suivre le rythme de la nouvelle machine quantique de Google. Par conséquent, IBM a fait valoir que la déclaration de Google devrait être reçue «avec une grande dose de scepticisme».

Pourquoi tant de confusion? Des accomplissements majeurs, comme celui-ci, ne sont-ils pas censés prendre la forme de succès retentissants et sans ambiguïté? Cet épisode rappelle que les révolutions scientifiques ne se font pas du jour au lendemain, et que la suprématie quantique, en particulier, implique plus de nuances que ne le laissent paraître les manchettes tonitruantes des médias.

De quoi parle-t-on? Les calculateurs quantiques sont en développement depuis des décennies. Les ordinateurs ordinaires, ou classiques, exécutent des calculs en utilisant des bits, chacun prenant une valeur définie, (0 ou 1). Les calculateurs quantiques quant à eux encodent l'information à l'aide de bits quantiques, ou qubits, qui se comportent selon les règles étranges de la mécanique quantique. Ces ordinateurs visent à exploiter ces caractéristiques particulières pour effectuer rapidement des calculs à un niveau dépassant de loin les capacités de n'importe quelle machine ordinaire. Mais, pendant des années, les ordinateurs quantiques parvenaient à peine à égaler la puissance de calcul d'une simple calculatrice de poche.

En 2012, John Preskill, chercheur en physique théorique à l'institut de technologie de >

Google a annoncé que son ordinateur quantique *(à gauche)* a atteint la suprématie quantique. Pour certaines tâches, il surclasserait donc le supercalculateur le plus rapide du monde, le Summit d'IBM *(à droite)*. IBM remet en question cette affirmation.

> Californie, a inventé l'expression « suprématie quantique » pour décrire le moment à partir duquel un ordinateur quantique surpasse même le meilleur des supercalculateurs. Le terme a marqué les esprits, mais les experts en sont venus à interpréter différemment sa signification. Ces divergences expliquant la situation qui nous intéresse ici : Google prétend avoir atteint ce seuil, et IBM lui dénie cette victoire.

Avant d'expliquer ce que la suprématie quantique signifie, clarifions ce qu'elle ne signifie pas : le moment à partir duquel un ordinateur quantique est capable d'exécuter un calcul impossible pour un ordinateur classique. En effet, on sait depuis Alan Turing qu'un ordinateur classique peut effectuer n'importe quel calcul, ce n'est qu'une question de temps. « Si on leur en donne assez, les ordinateurs, qu'ils soient classiques ou quantiques, peuvent résoudre les mêmes problèmes », explique Thomas Wong, de l'université Creighton, à Omaha, dans le Nebraska, aux États-Unis.

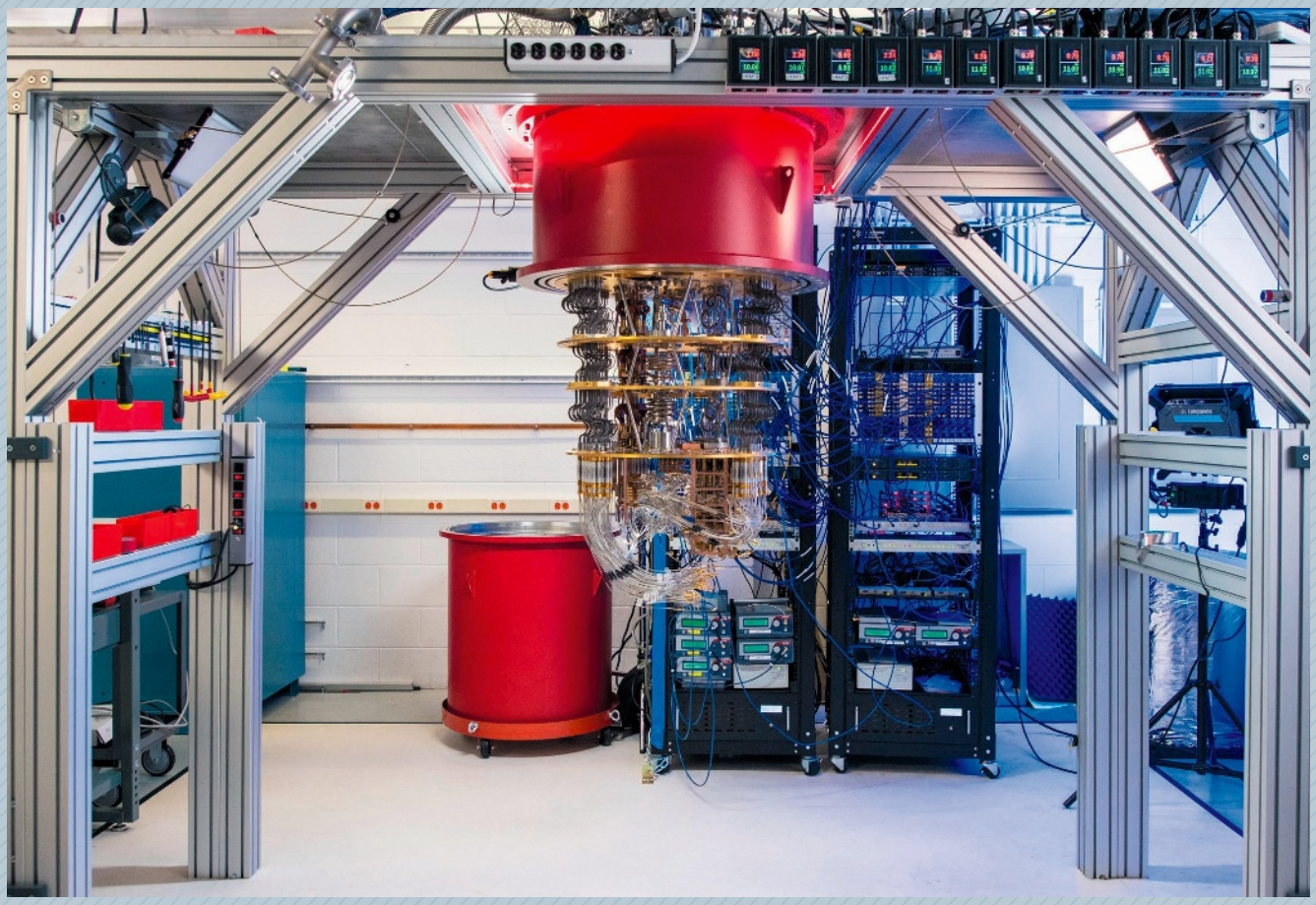
La plupart des experts interprètent la suprématie quantique comme le seuil à partir duquel un ordinateur quantique exécute un calcul qui, à toutes fins pratiques, ne peut être égalé par un ordinateur classique. L'essentiel du désaccord entre Google et IBM porte sur ce qu'il faut entendre par « pratique ».

10 000 ANS CONTRE 60 HEURES

Dans son étude, Google prétend qu'il a fallu 200 secondes à son processeur Sycamore pour effectuer un calcul pour lequel le meilleur supercalculateur actuel du monde – le Summit d'IBM – aurait besoin de 10000 ans, ce qui n'est pas très « pratique ». Cependant, IBM prétend que Summit, qui occupe un espace correspondant à deux terrains de basketball au Laboratoire national d'Oak Ridge, dans le Tennessee, peut exécuter ce calcul en deux jours et demi.

Google maintient son estimation de 10000 ans, bien que plusieurs experts en informatique soutiennent qu'IBM a probablement raison sur ce point. « La déclaration d'IBM me paraît plus plausible », nous a écrit Scott Aaronson, de l'université du Texas à Austin.

En supposant qu'IBM ait raison, peut-on considérer deux jours et demi comme un délai pratique ? Peut-être pour quelques tâches, mais certainement pas pour d'autres. Pour cette raison, les scientifiques ont généralement une



idée plus précise en tête lorsqu'ils parlent de suprématie quantique. Ils font la distinction entre les programmes exécutés en un temps polynomial « rapide » et en un temps exponentiel « lent ». Les programmes rapides le restent, même lorsqu'on leur soumet un très grand nombre. Les programmes lents ralentissent exponentiellement à mesure que la taille des problèmes posés augmente.

Dans son étude, Google démontre que son ordinateur quantique de 53 qubits effectue un calcul spécialisé (appelé « échantillonnage de circuit aléatoire ») en temps polynomial rapide. Or, pour l'heure, un ordinateur classique ne peut effectuer pareille tâche qu'en un temps exponentiel lent. Pour William Fefferman, de l'université de Chicago, ce constat est bien plus important que n'importe quel délai impliqué, qu'il s'agisse de deux jours et demi ou de 10 000 ans. « L'estimation du temps n'est pas très importante, précise-t-il. Je pense qu'IBM ne devrait pas invalider les déclarations principales de Google, en dehors de l'estimation de 10 000 ans. »

Ce qui compte, c'est que la machine de Google résout un problème de calcul d'une façon fondamentalement différente de celle dont un ordinateur classique est capable. Cette différence signifie que, à chaque fois que son ordinateur quantique croît d'un simple qubit, un ordinateur classique aura besoin de voir sa taille doubler pour suivre le rythme. Lorsqu'un ordinateur quantique aura atteint les 70 qubits – probablement d'ici aux deux prochaines années – un supercalculateur classique aura besoin d'un espace équivalent à celui d'une ville pour l'égaler.

ÉCHEC ET MAT

Scott Aaronson – empruntant l'analogie d'un ami – explique que la relation entre les ordinateurs quantiques et classiques, à la suite de l'annonce de Google, ressemble beaucoup à celle, dans les années 1990, entre le champion d'échecs Garry Kasparov et le supercalculateur Deep Blue… d'IBM. Le champion arrivait à suivre les premières versions qui allaient s'améliorant, mais il apparaissait clairement qu'il allait être inéluctablement dépassé par son adversaire algorithmique. IBM, désormais à la place de Garry Kasparov, « peut faire son baroud d'honneur durant l'ère de transition qui durera peut-être un an ou deux, explique Scott Aaronson. Mais, fondamentalement, il est mat. » ■

BIBLIOGRAPHIE

F. ARUTE *ET AL.*, Quantum supremacy using a programmable superconducting processor, *Nature*, vol. 574, pp. 505-510, 2019.

E. PEDNAULT *ET AL.*, Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits, 2019. https://arxiv.org/abs/1910.09534

L'ESSENTIEL

- Les ordinateurs quantiques communiqueront *via* un internet tout aussi quantique qui reste à inventer.
- Les premières pierres sont d'ores et déjà posées et l'on imagine de nombreuses applications que l'internet classique n'autorise pas.
- Ces réseaux quantiques reposeront également la question de la sécurité des transmissions.
- Garantir la confidentialité des communications quantiques impose de réfléchir à de nouveaux protocoles et à de nouvelles hypothèses sur lesquelles les fonder.

L'AUTRICE

NATALIE WOLCHOVER
est journaliste
à *Quanta Magazine*.

Inventer l'internet du futur

L'internet que nous connaissons depuis quarante ans est fondé sur des machines « classiques ». À quoi ressemblera celui qui reliera les ordinateurs quantiques ? Stephanie Wehner apporte quelques éléments de réponse.

Quanta magazine

Cet article a d'abord été publié en anglais par *Quanta Magazine*, une publication en ligne indépendante soutenue par la Simons Foundation afin de favoriser la diffusion des sciences: http://bit.ly/QM-Wehner

Ce soir-là, des informaticiens de l'université de Californie, à Los Angeles, étaient au téléphone avec leurs homologues de l'Institut de recherche Stanford à Menlo Park, situé à quelque 560 kilomètres de là. La conversation était surréaliste se rappelle Leonard Kleinrock, chercheur en informatique à l'université de Californie. « Avez-vous bien reçu le L ? » « Oui », a répondu l'autre équipe. « Vous avez reçu le O ? » « Oui. » De même pour le G… et puis c'est le crash ! Le serveur de l'Institut avait planté.

C'était le 29 octobre 1969. Les trois premières lettres du mot « LOGIN », tel a été le premier message transmis par l'Arpanet, le précurseur d'une révolution, ce que nous appelons aujourd'hui internet.

TROP DE CRÉATIVITÉ NUIT

La capacité des réseaux à transmettre des données, ainsi que leur tendance à planter, sinon à se comporter de façon imprévue, a toujours fasciné Stephanie Wehner. « Dans un ordinateur, tout se passe bien et reste ordonné », explique cette physicienne et informaticienne à l'université de technologie de Delft, aux Pays-Bas. « Dans un réseau, en revanche, de nombreux imprévus surviennent parfois. » Et c'est vrai pour deux raisons. D'abord, quand les programmes sur les ordinateurs connectés interfèrent, ce qui engendre des effets surprenants. Et ensuite, lorsque la créativité des utilisateurs de réseaux déborde. Au départ, « les gens pensaient que nous utiliserions internet pour

Stephanie Wehner, à l'université de technologie de Delft, aux Pays-Bas, où elle pose les premières pierres d'un futur internet quantique.

envoyer des fichiers un peu partout», remarque la physicienne.

Stephanie Wehner s'est connectée pour la première fois en ligne en 1992, quelques années avant que cela ne devienne largement accessible. À l'époque adolescente en Allemagne, elle s'y connaissait déjà en programmation et est vite devenue une pirate informatique sur l'internet naissant. À 20 ans, elle a obtenu un poste de «corsaire», c'est-à-dire de pirate pour le bien : sa tâche consistait à détecter les vulnérabilités du réseau pour un fournisseur d'accès à internet. Puis elle s'est lassée et a cherché à comprendre plus en profondeur les réseaux et les systèmes de transmission d'information.

Aujourd'hui, Stephanie Wehner fait partie des meneurs du mouvement visant à créer une toute nouvelle forme d'internet. Elle travaille à la conception d'un «internet quantique», un réseau qui transmettrait – au lieu des bits classiques ayant soit une valeur de 0, soit de 1 – des bits quantiques dans lesquels les deux possibilités, 0 et 1, coexistent. Ces «qubits» pourraient être faits de photons qui sont une combinaison de deux différentes polarisations. La capacité d'envoyer des qubits d'un endroit à un autre *via* des câbles de fibres optiques ne bouleversera peut-être pas la société aussi profondément que ne l'a fait l'internet classique, mais elle pourrait révolutionner de nombreux aspects de la science et de la culture, de la sécurité à l'informatique, en passant par l'astronomie.

UN ARPANET QUANTIQUE

Stephanie Wehner coordonne la *Quantum Internet Alliance*, une initiative de l'Union européenne pour élaborer un réseau de transmission d'information quantique à travers le continent. Dans un article paru dans la revue *Science* en octobre 2018, elle et deux collègues ont dévoilé leur plan pour la création d'un internet quantique en six étapes, chacune d'elle devant se traduire par de nouveaux algorithmes et applications. >

La première étape est en cours, elle consiste en la construction d'un réseau quantique de démonstration qui connectera quatre villes aux Pays-Bas, une sorte d'analogue quantique de l'Arpanet. Tracy Northup, de l'université d'Innsbruck et membre de la *Quantum Internet Alliance* loue « l'ampleur de la vision de Stephanie et son engagement pour construire le genre de structure nécessaire à la réalisation d'un tel projet. »

Après le piratage, Stephanie Wehner est allée à l'université pour étudier l'informatique et la physique. À Leyde, elle a entendu le théoricien de l'information quantique John Preskill donner une conférence, durant laquelle il décrivait les avantages des bits quantiques pour communiquer. Quelques années plus tard, après avoir son doctorat, elle a abandonné les bits classiques et rejoint le groupe de John Preskill à l'institut de technologie de Californie (Caltech), aux États-Unis, pour un postdoctorat.

Là, en plus d'avoir démontré plusieurs théorèmes notables sur l'information quantique, la cryptographie quantique et la nature de la mécanique quantique elle-même, Stephanie Wehner s'est naturellement imposée comme une « meneuse naturelle », raconte John Preskill ; elle « était souvent le lien qui unissait les gens ». En 2014, après avoir occupé un poste de professeuse à Singapour, elle a déménagé à Delft, où elle a commencé à collaborer avec des expérimentateurs pour poser les fondations de l'internet quantique.

Afin d'en savoir plus, nous avons rencontré Stephanie Wehner en août 2019.

« Nous travaillons à un réseau quantique à travers toute l'Europe »

L'internet quantique est un réseau de transmission de qubits entre deux lieux distants. Pourquoi en a-t-on besoin ?

Stephanie Wehner : L'idée n'est pas de remplacer l'internet que nous utilisons tous aujourd'hui, mais plutôt d'y ajouter des fonctionnalités nouvelles et spéciales. Les réseaux quantiques ont toutes sortes d'applications encore à imaginer, mais nous en connaissons déjà un certain nombre. Bien sûr, la plus célèbre est la communication sécurisée : le fait que l'on puisse utiliser la communication quantique pour distribuer des clés quantiques de cryptographie, garantissant la sécurité, même si l'attaquant est équipé d'un ordinateur quantique. Or une telle machine pourrait vaincre de nombreux protocoles de sécurité existant aujourd'hui.

Qu'est-ce qui rend ces clés quantiques si sûres ?

Stephanie Wehner : Une bonne manière de comprendre ce que l'internet quantique peut faire est de penser à « l'intrication quantique » (*voir Pas d'échappatoire pour l'intrication, par R. Hanson, page 26*), une propriété qui unit deux bits quantiques. La première propriété de l'intrication est sa « coordination maximale » : si j'avais un bit quantique ici, à Delft, et un autre à New York, j'utiliserais l'internet quantique pour les intriquer. Dès lors, une mesure de mon qubit ici et celle du qubit de New York donneraient toujours le même résultat, alors même qu'il n'était pas prédéterminé. Donc, intuitivement, grâce à cette première propriété de l'intrication quantique, l'internet quantique serait très utile pour des tâches nécessitant une coordination à distance.

On peut alors se demander : « Ne serait-ce pas génial de partager cette intrication avec des centaines de personnes ? » Peut-être, mais c'est impossible, car la seconde propriété de l'intrication est son caractère intrinsèquement privé. Si mon qubit d'ici est intriqué avec le vôtre à New York, alors nous savons que rien d'autre ne peut partager cette intrication. C'est pour cela que la communication quantique est si pratique pour les problèmes requérant un certain niveau de sécurité.

La distribution quantique de clé est l'une des applications les plus simples de la communication quantique, et elle pourrait être disponible dès cette année sur le réseau de démonstration que vous construisez. Quelles applications plus lointaines peut-on imaginer ?

Stephanie Wehner : De nouvelles formes d'informatique à distance deviendront possibles. Supposez que vous avez un concept de matériau breveté dont vous aimeriez tester les propriétés dans une simulation. Pour ce faire, un ordinateur quantique sera bien meilleur qu'un ordinateur classique. Mais tout le monde n'aura pas un ordinateur quantique dans son salon dans un futur proche – et probablement même pas de notre vivant.

Une solution serait de m'envoyer votre concept et que j'exécute les simulations sur l'ordinateur quantique du laboratoire. Promis, je vous enverrai les résultats, mais je dispose désormais de toutes les informations sur votre invention. Grâce au réseau quantique, vous pourriez de chez vous utiliser un appareil quantique très simple – en fait, il peut ne faire qu'un qubit à la fois – et transférer les qubits de votre appareil jusqu'à mon ordinateur quantique plus puissant. Il fera alors tourner les simulations sans rien livrer des caractéristiques de votre nouveau matériau. Vous serez tranquillisée grâce au réseau quantique.

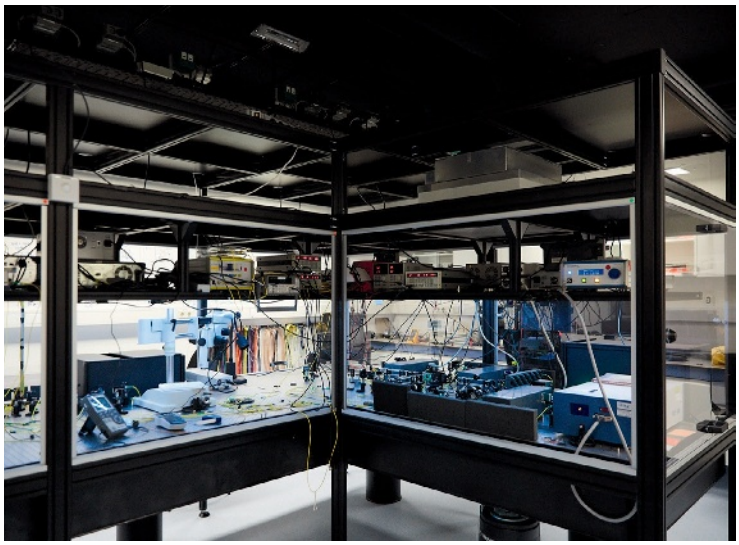
Pour donner un autre exemple, on a aussi montré que l'intrication rend plus précise la synchronisation de deux horloges situées en deux endroits différents. Un tel résultat aura de nombreuses applications, par exemple en géolocalisation.

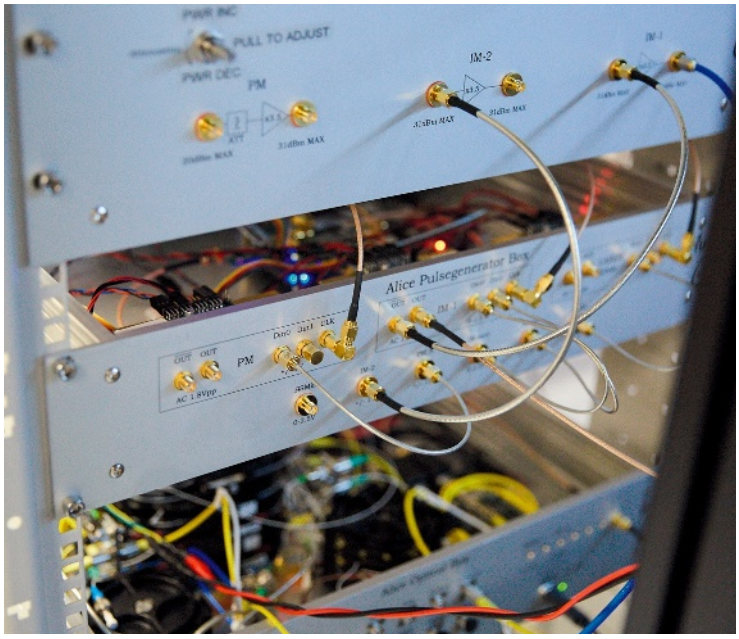
Un internet quantique aiderait aussi à créer un meilleur télescope, en combinant plusieurs télescopes séparés. Les états des particules de lumière captées par un premier télescope seraient téléportés, grâce à l'intrication quantique, vers un second télescope, où ils seraient combinés à ceux de ses photons perçus.

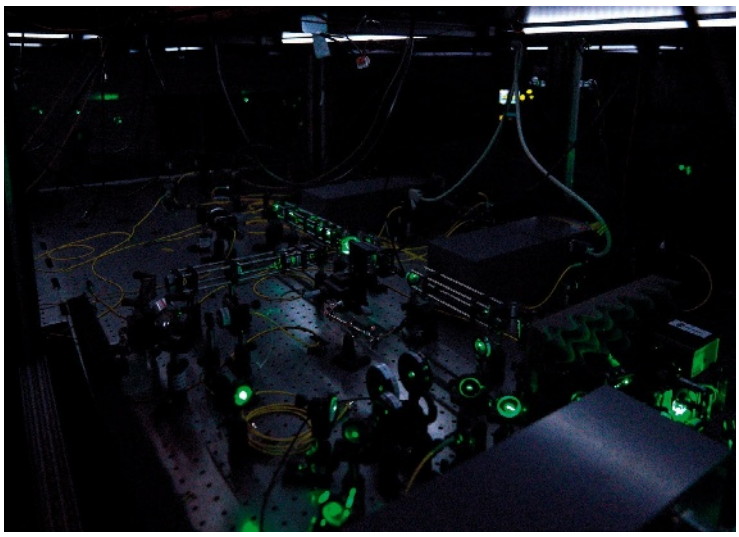
Vous travaillez aussi sur la simulation du futur internet quantique. Pourquoi est-ce nécessaire ?

Stephanie Wehner : Avec la plateforme de simulation très performante que nous avons construite et qui est désormais installée dans un supercalculateur, nous pouvons explorer différentes configurations du réseau quantique et comprendre des propriétés autrement plus difficiles à prédire par des méthodes analytiques classiques. De cette façon, nous espérons mettre au point un concept modulable qui puisse permettre les communications quantiques à travers toute l'Europe.

L'aspect imprédictible des réseaux m'a toujours fascinée. Les ordinateurs sont intéressants, mais ce qui m'importe vraiment, c'est la >







Un laboratoire à l'institut de technologie de Delft, aux Pays-Bas, abrite un cristal spécial, une mémoire quantique servant de nœud de réseau pour la communication quantique à longue distance.

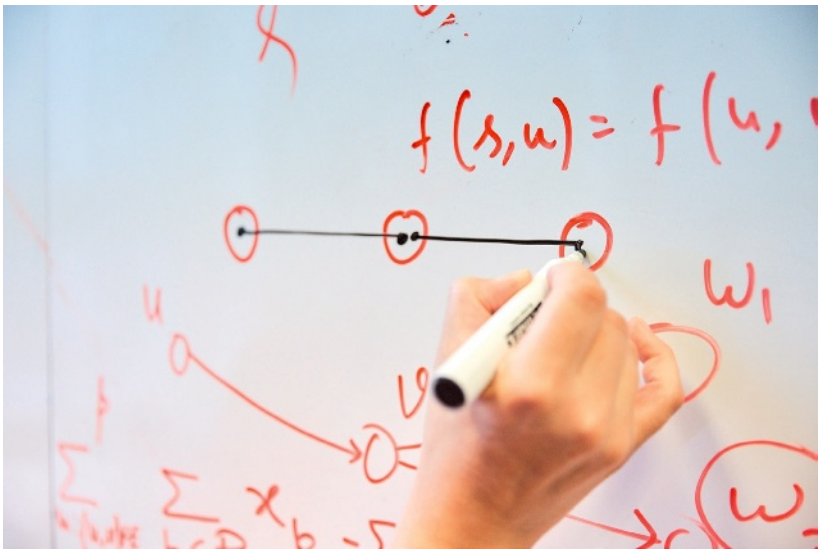
transmission de données d'un point à un autre. C'est pour cette raison que je me suis lancée dans le piratage puis intéressée à l'internet classique. Fondamentalement, comprendre ce qui se passe dans un réseau est très difficile, en raison du nombre important de facteurs non caractérisés. Par exemple, quand vous envoyez un message, vous ne pouvez pas prédire exactement au bout de combien de temps il parviendra au destinataire. Le message peut se perdre, un ordinateur planter, être trop lent, voire corrompre les données. Le protocole de transmission peut se heurter à une vieille version d'un logiciel, une nouvelle version ou une version maligne.

Étiez-vous une méchante pirate avant de devenir une corsaire ?
Stephanie Wehner : Ce n'est pas le genre de révélation que l'on peut faire en public ! Je pense juste qu'à l'époque le monde était un endroit plus sympathique qu'aujourd'hui. Voilà tout…

Pourquoi avez-vous décidé d'arrêter le piratage et de devenir une scientifique ?
Stephanie Wehner : Je sais que le piratage semble très excitant, mais je pratiquais cette activité depuis un certain temps. Bien sûr, on peut améliorer ses méthodes, mais cela reste toujours un peu la même chose. J'ai fini par m'ennuyer et j'ai décidé de me lancer dans une nouvelle aventure. Puis, j'ai découvert la théorie de l'information quantique qui m'a immédiatement fascinée.

L'un des théorèmes que vous avez prouvés sur l'information quantique est le théorème du stockage avec bruit. De quoi s'agit-il ? Et quelles en sont les implications pour la communication quantique ?
Stephanie Wehner : Le stockage avec bruit concerne la cryptographie, avec une hypothèse physique. Dans le monde de l'informatique classique, on formule souvent une hypothèse de départ. Par exemple, on part du principe qu'il est difficile de déterminer les facteurs premiers de grands nombres, et si cette supposition est vraie, alors mon protocole est sûr. Ces preuves de sécurité sont bonnes et elles sont utilisées partout aujourd'hui, mais il ne faut pas oublier qu'elles peuvent être invalidées plus tard.

Demain, ou plus tard, quelqu'un peut inventer une méthode intelligente pour résoudre le problème informatique sur lequel votre sécurité se fonde : elle devient immédiatement obsolète, et de façon rétroactive. Par exemple, grâce à l'algorithme développé par le mathématicien américain Peter Shor, des ordinateurs quantiques factoriseront aisément de grands nombres et réduiront à néant l'efficacité des méthodes de sécurité actuelles fondées sur la factorisation. Quelqu'un enregistrant votre message aujourd'hui pourra le décrypter plus tard.



Les nœuds d'un futur réseau quantique, de la main de Stephanie Wehner.

QUELQU'UN ENREGISTRANT VOTRE MESSAGE SÉCURISÉ AUJOURD'HUI POURRA LE DÉCRYPTER PLUS TARD

Les travaux sur le stockage avec bruit posent la question : peut-on formuler une hypothèse physique qui ne peut pas être rétroactivement rendue caduque ? L'hypothèse physique est ici qu'il est difficile de stocker beaucoup d'états quantiques sans bruit, ce qui n'a besoin d'être vrai que pour un tout petit délai. En partant du principe que, maintenant, vous ne pouvez stocker que jusqu'à un million de qubits avec bruit, je peux modifier les paramètres du protocole de transmission pour augmenter la sécurité en envoyant plus d'informations que n'en peut capturer ce million de qubits. C'est efficace, parce que, si demain vous achetez de la mémoire quantique à hauteur de 2 millions de qubits, il sera trop tard, l'information aura déjà été envoyée de façon sécurisée.

Sur la base de cette idée, toutes sortes de protocoles de communication quantique sont envisageables. Supposons que deux personnes veuillent comparer leur mot de passe sans jamais le révéler. C'est complètement différent de ce que nous faisons aujourd'hui, lorsque nous saisissons notre code à quatre chiffres sur le clavier d'un distributeur de billets. À la place, nous entrerons notre code secret dans notre propre appareil, et il ne sera jamais révélé au distributeur, qui néanmoins nous donnera les billets demandés. Ce protocole devient possible avec l'hypothèse du stockage avec bruit.

La quête de cet internet quantique pourrait-elle nous permettre d'approfondir nos connaissances sur les lois de la nature ?
Stephanie Wehner : En science, on distingue parfois des questions dites « fondamentales »

et d'autres plutôt « pratiques », et donc banales. Je pense qu'apporter au monde réel quelque chose d'utilisable par tout le monde n'est jamais banal. C'est extrêmement difficile. Il y a un bond de géant entre : « J'ai une idée géniale, par exemple un écran tactile, discutons-en sur le tableau blanc » et le smartphone que j'utilise actuellement. Avec l'internet quantique, nous sommes dans la même situation, nous essayons de le construire en partant de rien.

Nous partons d'une expérience préliminaire en laboratoire pour essayer de mettre en place un système étendu à tous les Pays-Bas, fonctionnant à distance et utilisable par des individus, qui, à terme, n'auront pas besoin de s'y connaître en physique pour le faire. Si une partie du système existait déjà, nous pourrions simplement dire « améliorons-la ». Mais créer *ex nihilo* est une autre affaire. Passer de rien à une première version est très long.

En faisant cela, je pense que nous accéderons à une compréhension plus fondamentale dans plusieurs domaines. Nous en apprendrons plus sur la physique en rendant possibles ces réseaux parce que, actuellement, nous ne savons pas exactement comment le faire. Nous testons encore différents types de nœuds et de répéteurs quantiques, des appareils qui relaient l'intrication sur de plus grandes distances. Et, dans le domaine des sciences informatiques, nous découvrirons de nouvelles façons de programmer et contrôler de tels réseaux grâce aux différences fondamentales qui existent entre les communications quantique et classique.

Mais je pense aussi que nous obtiendrons des informations sur les processus créatifs et la sociologie en suivant la façon dont les usagers s'empareront de ces nouveaux réseaux. Souvenez-vous des débuts de l'internet classique, la plupart pensaient qu'il ne servirait qu'à envoyer des fichiers un peu partout. Mais la société a fait preuve de bien plus d'imagination !

Il est difficile de définir un calendrier, mais espérez-vous voir de votre vivant cet internet quantique ?

Stephanie Wehner : Je suis assez optimiste à ce propos, je pense que oui. ■

BIBLIOGRAPHIE

G. MURTA *ET AL.*, Towards a realization of device-independent quantum key distribution, *Quantum Physics*, 2019. https://arxiv.org/abs/1811.07983

S. WEHNER *ET AL.*, Quantum internet: A vision for the road ahead, *Science*, vol. 362(6412), eaam9288, 2018.

D. CASTELVECCHI, The quantum internet has arrived (and it hasn't), *Nature*, vol. 554(7692), pp. 289-292, 2018.

S. WEHNER *ET AL.*, Cryptography from Noisy Storage, *Phys. Rev. Lett.*, vol. 100, 220502, 2008.

PASCALE SENELLART-MARDON

« Les Chinois ont mis un grand coup d'accélérateur avec des moyens considérables »

En quelques mots, qu'est-ce qu'un ordinateur quantique ?

Pascale Senellart-Mardon : C'est une machine « intriquante », c'est-à-dire un dispositif qui exploite la possibilité de superposer et d'intriquer les états quantiques de plusieurs systèmes physiques (*voir Pas d'échappatoire pour l'intrication, par R. Hanson, page 26*) – c'est-à-dire de les lier de façon très étroite, spécifique à la physique quantique – afin de mettre en œuvre des calculs hors de portée des ordinateurs actuels.

D'où vient la puissance calculatoire particulière que vous évoquez ?

Pascale Senellart-Mardon : Pour le faire ressentir, j'aime bien utiliser cette métaphore : rechercher la solution d'un problème revient à essayer de faire traverser un labyrinthe complexe à un personnage. Si c'est un ordinateur classique qui aide ce personnage, il lui fera, à chaque embranchement, essayer successivement toutes les voies, rebrousser chemin au bout de chaque cul-de-sac, puis recommencer jusqu'à trouver la sortie. Il se peut que, par chance, le personnage trouve vite comment traverser, mais il se peut aussi qu'il meure avant que l'exploration systématique ne lui ait révélé la sortie du labyrinthe…

Si c'est un ordinateur quantique qui assiste le personnage, il le « superposera », à chaque embranchement, à un *alter ego* qui explorera l'autre voie. En d'autres termes, on aura simultanément l'état représenté par le personnage allant à gauche et l'état d'un *alter ego* allant à droite. Résultat : en une étape, l'ordinateur quantique fait essayer en parallèle toutes les voies au personnage. Il construit ainsi un état qui superpose tous les états d'*alter ego* effectuant tous les parcours possibles, y compris celui qui permet de traverser. Un témoin présent

BIO EXPRESS

Pascale Senellart-Mardon est directrice de recherche au CNRS et chercheuse au Centre de nanosciences et de nanotechnologies du CNRS et de l'université Paris-Saclay.

Elle a cofondé la société Quandela (grand prix i-Lab 2018), qui produit des sources de photons pour ordinateur et communications quantiques.

© J. Senellart

à la sortie permettra alors d'extraire, parmi la multitude d'*alter ego*, celui qui aura traversé le labyrinthe – autrement dit la solution au problème posé.

Cela revient en somme à une forme de parallélisme massif…

Pascale Senellart-Mardon : Exactement, un parallélisme massif et inhérent à une propriété subtile du monde quantique : l'existence d'états qui sont des superpositions de plusieurs états quantiques de base d'un certain système physique. Une autre façon de paralléliser consiste à « intriquer » l'état d'un système physique avec celui d'un autre, l'intrication étant un lien spécifiquement quantique, qui subsiste quelle que soit la distance séparant les deux systèmes. J'insiste sur un point : puisqu'il fonctionne sur un principe différent, l'ordinateur quantique ne remplacera pas l'ordinateur classique, mais il le complétera quand un problème sera hors de sa portée…

Quels types de problèmes dépassent l'ordinateur classique ?

Pascale Senellart-Mardon : Si nous disposions d'un ordinateur quantique, nous pourrions, de manière générale, résoudre bien plus vite tous les problèmes d'optimisation, ceux où il faut rechercher une solution parmi un très grand nombre de possibilités. Par exemple, cette capacité pourrait nous aider à développer bien plus vite des molécules thérapeutiques, à réaliser des simulations pour trouver enfin la formule d'un supraconducteur à vraiment haute température, à faire de meilleures prévisions météorologiques, à optimiser les investissements financiers…

Mais l'exemple emblématique est un problème arithmétique : avec un ordinateur quantique, on pourrait décomposer un très grand nombre en ses facteurs premiers beaucoup plus vite. Cela bouleverserait la cryptographie, puisque la sécurité du chiffrement RSA, le plus utilisé aujourd'hui, repose sur l'impossibilité, avec un ordinateur classique, d'effectuer la même tâche en un temps raisonnable.

Et où en sommes-nous ? Quels sont les obstacles à surmonter pour construire un ordinateur quantique ?

Pascale Senellart-Mardon : Vaste question ! Disons pour commencer que les théoriciens qui développent l'algorithmique quantique supposent de pouvoir disposer d'un certain nombre de bits quantiques, ou qubits (pour *quantum bits*). Un qubit est l'équivalent concret du personnage superposable que j'évoquais plus haut. Un bit classique ne peut valoir que 0 ou 1. Un qubit, lui, a deux états de base notés $|0\rangle$ et $|1\rangle$, et il peut être dans une superposition des deux, c'est-à-dire dans un état de la forme $a|0\rangle+b|1\rangle$. Ensuite, l'étage de calcul va créer des liens d'intrications multiples entre différents qubits, liens qui contribuent au parallélisme et permettent d'aboutir au résultat très efficacement.

Un ordinateur quantique consiste donc en un étage constitué d'un ensemble de qubits et en un étage qui effectue un calcul ?

Pascale Senellart-Mardon : Oui, comme dans un ordinateur classique, dans un ordinateur quantique, le calcul suppose l'assemblage d'un certain nombre de portes logiques, mais les portes logiques quantiques intriquent les qubits entre eux… Aujourd'hui, la difficulté technique essentielle à franchir pour obtenir un ordinateur quantique est triple : 1) disposer d'un grand nombre de qubits ; 2) parvenir à les combiner en des états intriqués ; 3) maintenir la cohérence de ces états assez longtemps pour que les calculs puissent aller à leur terme.

Ainsi, il faut d'abord avoir des qubits. Par quelles techniques y parvient-on ?

Pascale Senellart-Mardon : Il en existe de l'ordre d'une vingtaine, je crois, mais quatre filières font l'objet d'un développement intense. La plus avancée est celle des ions piégés, dans laquelle deux groupes mènent la course en tête : celui de Rainer Blatt, à l'université d'Innsbruck, en Autriche, et celui de Chris Monroe, à l'université du Maryland, aux États-Unis.

La technologie des ions piégés est la mise en pratique de nos anciennes expériences de pensée de physique quantique : on réalise des dispositifs où des champs électriques et magnétiques piègent des ions disposés en série les uns à côté des autres ; chaque ion, *via* l'état d'énergie d'un électron, constitue un qubit. Une impulsion laser appropriée permet de modifier l'état électronique d'un ion, pour en faire une superposition des états $|0\rangle$ et $|1\rangle$. Ensuite, l'enjeu est de construire des portes logiques quantiques qui, en pratique, intriquent les états des ions entre eux en jouant sur leurs fréquences d'oscillation dans leur piège commun.

Il faut maintenir la cohérence quantique assez longtemps pour réaliser un calcul

Cette filière est très avancée puisque, pour faire des calculs, on dispose de temps de cohérence de quelques minutes, ce qui est très long. En théorie, cela permet d'empiler beaucoup de portes logiques… ce qui veut dire beaucoup d'opérations.

Combien de qubits contiennent les ensembles d'ions piégés que l'on a ainsi obtenus ?

Pascale Senellart-Mardon : Des annonces tapageuses dans les médias ont fait état de 70 qubits, mais seul est pertinent le nombre de qubits que l'on peut combiner tout en maintenant la cohérence quantique assez longtemps pour réaliser un calcul. De ce point de vue, le bon chiffre serait plutôt entre une quinzaine et une vingtaine… ce qui est aussi vrai des autres filières avancées d'aujourd'hui, que celles-ci exploitent des atomes ou des atomes artificiels.

Des atomes artificiels ? C'est-à-dire ?

Pascale Senellart-Mardon : Dans la filière des ions piégés, les qubits sont des états d'énergie d'électrons atomiques. Dans les autres filières dominantes, il s'agit aussi d'états d'énergie d'électrons, mais d'électrons liés à des « atomes artificiels », c'est-à-dire à de petits dispositifs microscopiques conçus pour lier une telle particule. Dans >

> deux des autres filières, par exemple, les électrons sont liés soit au sein de petites boucles de courant en milieu supraconducteur, soit au sein de «boîtes quantiques» réalisées dans du silicium – de minuscules structures où l'électron est confiné.

Tandis que Google et IBM mènent la danse dans la première filière, des équipes des Pays-Bas, d'Australie et des États-Unis la mènent dans la deuxième. Des chercheurs du CEA et du CNRS à Grenoble s'y sont aussi lancés en 2016. Bref, dans ces filières, on a reconstitué au sein d'atomes artificiels l'équivalent d'une échelle des états d'énergie d'électrons atomiques. La très grande subtilité technique de la construction et du maintien en cohérence des superpositions d'états en milieu solide a limité jusqu'à présent le nombre de qubits atteint: il est d'environ 20 dans le cas des dispositifs supraconducteurs, et de 2 dans le cas des boîtes quantiques en silicium...

Seulement 2 ? Pourquoi alors poursuivre dans cette voie ?

Pascale Senellart-Mardon : Ce nombre modeste de qubits du côté du silicium reflète le grand défi à relever pour que cette technologie soit viable: trouver le moyen d'augmenter le nombre de qubits intriqués. Pour autant, comme cette filière s'appuie sur la technologie CMOS qui sert à produire les microprocesseurs actuels, son potentiel industriel est grand et il est donc important de l'explorer. Si l'on parvenait à intriquer un grand nombre de qubits réalisés en semi-conducteurs, on aurait toute facilité pour les produire par millions...

Mais les intriquer en grand nombre ne suffit pas ; ne faut-il pas aussi réussir à conserver la cohérence des états correspondants ?

Pascale Senellart-Mardon : Oui, il y a aussi un défi du côté de la cohérence, comme dans tout système à l'état solide, mais le défi est aussi du côté de la «connectivité», c'est-à-dire la capacité à intriquer des qubits qui sont distants les uns des autres. Pour l'instant, l'état de l'art avec le silicium consiste à intriquer une boîte quantique avec sa plus proche voisine seulement!

Existe-t-il une autre filière où l'on peut espérer intriquer un grand nombre de qubits sans perdre trop rapidement leur cohérence ?

Pascale Senellart-Mardon : La mienne, peut-être, celle de l'ordinateur quantique optique. Dans cette voie, les qubits sont par exemple les états de polarisation de photons uniques, photons que l'on combine en les introduisant simultanément à l'entrée d'un circuit optique effectuant le calcul. Les portes logiques quantiques peuvent être réalisées à base de miroirs, de lames semi-transparentes, c'est-à-dire de séparateurs de faisceau et autres déphaseurs, le tout relié à des détecteurs *via* un réseau de fibres optiques. Or les états photoniques peuvent voyager très loin sans perdre leur cohérence; donc, si l'on parvient à éviter les pertes, on peut réaliser un grand nombre de portes logiques. Et, ce qui ne gâche rien, les ordinateurs quantiques optiques sont évidemment compatibles avec les réseaux de communication optique.

Tout semble donc aller pour le mieux dans ce monde photonique ?

Pascale Senellart-Mardon : Sauf qu'il y a une difficulté de taille... Lorsqu'on effectue un calcul, il existe une probabilité élevée de n'aboutir à aucun résultat. Cela tient au principe des portes logiques qui utilisent des séparateurs de faisceau. Comme, à chaque séparateur, les photons intriqués ont 50% de chance de ne pas être transmis par la voie qui, après beaucoup d'autres embranchements, mènera au détecteur, il se peut qu'aucun signal ne sorte. Pour reprendre l'image de tout à l'heure, tout se passe comme si l'étage de calcul était un labyrinthe dont la traversée résout un problème difficile, mais qu'à chaque embranchement, le candidat perd la moitié de sa substance – de son intensité lumineuse utile – quand il se dédouble en un état superposé de son *alter ego* et de lui-même... Autrement dit, au bout d'un moment, on va perdre trop de lumière pour parvenir à faire le calcul.

C'est un obstacle sérieux...

Pascale Senellart-Mardon : Oui, mais nous avons des solutions pour affronter cette difficulté. Des théoriciens ont trouvé d'autres moyens de faire des calculs à grande échelle: on ne partira plus d'états à un photon, mais, pour limiter le nombre de portes logiques, d'états intriqués à plusieurs photons. Cette autre façon de calculer repose sur une autre architecture de calcul quantique, dite «fondée sur la mesure».

Finalement, cette filière de l'ordinateur quantique et optique est-elle prometteuse ?

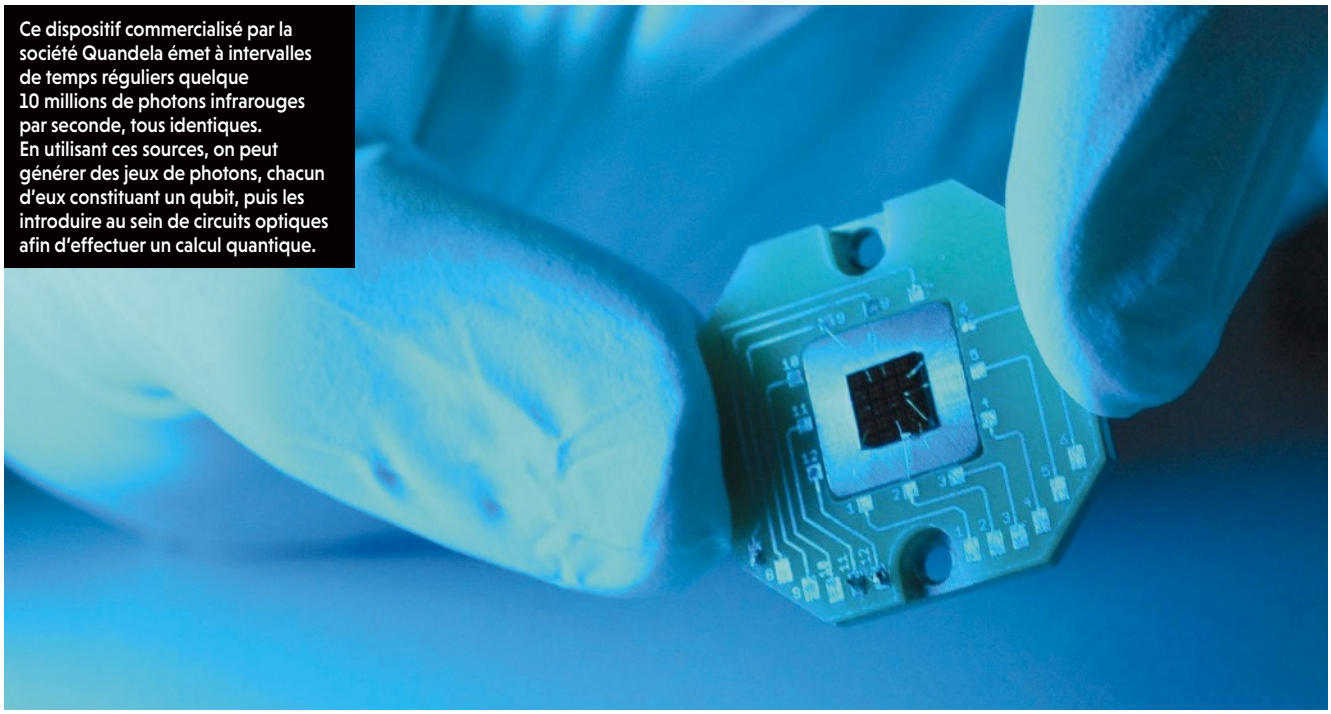
Pascale Senellart-Mardon : Elle a semblé au point mort pendant longtemps, parce que pour produire les états superposés de départ, il faut des sources de photons à la fois uniques – arrivant seuls – et absolument identiques – de même fréquence. Or les sources dont nous disposions dans le passé étaient si peu efficaces qu'il fallait pratiquement deux ou trois ans, le temps d'une thèse de doctorat, avant de parvenir à exécuter un petit calcul.

Pourquoi la situation a-t-elle changé ?

Pascale Senellart-Mardon : Parce que mon équipe au Centre de nanosciences et de nanotechnologies a réussi à mettre au point un petit composant presse-bouton, qui peut émettre à volonté des photons un par un. Pour aller vite, nous avons mis une boîte quantique – un atome artificiel donc, où un électron ne peut occuper que certains niveaux d'énergie – à l'intérieur d'une cavité optique. Comme pour tous les atomes, si on excite cet atome artificiel, il va en se désexcitant émettre un seul photon, mais dans une direction quelconque. Ici, la cavité et les miroirs qui la constituent ont été choisis de telle façon qu'ils augmentent la probabilité que la lumière se concentre dans une direction donnée. En d'autres termes, grâce à la cavité, on contrôle l'«émission spontanée» de l'atome.

Sans cavité optique, tout se passe comme si l'énergie lumineuse émise par

Des spécialistes des algorithmes commencent à envisager la programmation d'ordinateurs quantiques



Ce dispositif commercialisé par la société Quandela émet à intervalles de temps réguliers quelque 10 millions de photons infrarouges par seconde, tous identiques. En utilisant ces sources, on peut générer des jeux de photons, chacun d'eux constituant un qubit, puis les introduire au sein de circuits optiques afin d'effectuer un calcul quantique.

l'atome artificiel sortait d'une grande baignoire par une infinité de petits trous. Avec la cavité optique, on ajoute en pratique un énorme trou dans la baignoire… et naturellement la majorité de l'énergie lumineuse va maintenant s'écouler par ce trou. Il nous suffit alors de la collecter, avec une fibre optique. Notre « baignoire », les miroirs qui la constituent et la boîte quantique qu'elle contient forment une petite structure monolithique en semi-conducteur de 20 micromètres de diamètre (*voir la photo ci-dessus*).

Ce qui a relancé la voie optique ?

Pascale Senellart-Mardon : Oui. En 2016, nous avons publié dans la revue *Nature Photonics* un article qui a eu un grand impact, puisqu'en deux ans, il a été cité plus de 400 fois. Depuis, nous sommes assaillis de demandes de chercheurs qui veulent utiliser nos sources de photons uniques pour faire du calcul quantique…

Comment réagissez-vous à ce succès ?

Pascale Senellart-Mardon : Comme nous ne pouvions pas faire face à toutes les demandes, avec Valérian Giesz et Niccolo Somaschi, nous avons créé la société Quandela. Mon rôle au CNRS consiste à faire de la recherche, et non à fabriquer des sources pour tous les chercheurs du monde qui en ont besoin. Maintenant, grâce à Quandela, nous pouvons leur fournir des sources qui, par rapport aux anciennes, réduisent le temps de calcul de un milliard pour neuf qubits, c'est-à-dire ici neuf photons… Nous en avons déjà vendu en Australie, mais nous avons aussi des collaborations avec des chercheurs qui viennent dans notre laboratoire avec leur puce optique pour effectuer des calculs.

Si je comprends bien, l'aspect matériel de l'ordinateur quantique en est encore à ses débuts, bien que l'on progresse. Et pour l'aspect logiciel ? Existe-t-il déjà des algorithmes ou des programmes pour ordinateurs quantiques ?

Pascale Senellart-Mardon : Les recherches dans ce domaine ont très longtemps été une activité de physiciens d'un côté, et de théoriciens faisant de l'algorithmique quantique de l'autre. Actuellement, quelque chose de nouveau apparaît : des informaticiens spécialistes des algorithmes commencent à envisager la programmation d'ordinateurs quantiques. Corrélativement, de grandes entreprises essaient de les encourager : en 2019, au CES de Las Vegas, le plus grand salon d'électronique grand public du monde, IBM a ainsi présenté Q System One, un système à 20 qubits mis sur le réseau. Contre un abonnement onéreux, les gens qui s'intéressent au développement de logiciels quantiques peuvent s'en servir pour tester des algorithmes… La société Atos, en France, a une autre approche : en préparation de l'avènement du calcul quantique, elle a dédié un gros calculateur classique à la simulation d'un ordinateur quantique, ce qui permet aussi de s'habituer aux calculs quantiques, de repérer les erreurs les plus dommageables, d'étudier la façon dont les utilisateurs s'y prennent…

L'Union européenne a lancé fin 2018 un *Quantum Flagship*, un programme phare sur l'ordinateur et le calcul quantique. Un tournant pour la recherche européenne ?

Pascale Senellart-Mardon : Ce programme va financer à hauteur de un milliard d'euros sur dix ans des projets pour développer l'ordinateur quantique, les simulateurs, les communications et les capteurs quantiques, tout en maintenant un effort de recherche fondamentale. Cet investissement financier n'est finalement pas énorme, si l'on songe que la somme va se répartir sur l'ensemble de la communauté européenne. L'attribution des financements est démocratique, ce qui a du bon, mais cela empêche de concentrer l'investissement dans les projets les plus avancés.

Il semble donc que la cavalerie européenne arrive, sans se presser… Comment cela se passe-t-il ailleurs ?

Pascale Senellart-Mardon : Je connais par exemple le cas des Chinois. En 2017, ils ont déjà secoué la communauté >

quantique internationale en mettant en œuvre une communication quantique depuis un satellite, alors que l'idée de faire cela avait été évoquée en Europe, notamment par Anton Zeilinger, de l'université de Vienne.

Ils ont récidivé en 2020 en établissant une communication entre un satellite quantique (*Quess*), surnommé *Mozi*, et la toute première station quantique mobile terrestre du monde. La communication aurait duré près de huit minutes.

Les Chinois déploient déjà un réseau de communications quantiques sur des milliers de kilomètres. Au fil de nos progrès sur les sources de photons uniques, qui nous ont permis de relancer les travaux sur l'ordinateur optique, des équipes chinoises se sont engouffrées dans cette filière. Elles avancent extrêmement vite, sont fortes, ont de gros effectifs et n'ont apparemment pas de limites aux moyens qu'elles peuvent demander…

Depuis peu, le chef de l'une de ces équipes explique dans les conférences que la Chine va démontrer l'avantage d'un ordinateur quantique par rapport aux plus gros calculateurs classiques grâce la technologie optique. Clairement, les Chinois ont mis un grand coup d'accélérateur sur les technologies quantiques.

Pour autant, l'ordinateur quantique est-il un objectif réaliste ? Pensez-vous que l'on arrivera à intriquer des millions de qubits et que l'on saura maintenir la cohérence quantique assez longtemps pour effectuer de gros calculs ? Selon certains physiciens éminents, le Prix Nobel Serge Haroche notamment, cela restera une utopie…

Pascale Senellart-Mardon : Comme tous les physiciens qui travaillent à maîtriser les effets quantiques subtils – l'intrication, la décohérence – pour rendre possible le calcul quantique, je vois l'énormité des obstacles à franchir et ils m'intimident. Quand j'y pense, j'ignore ce qui va se passer. Mais ça, c'est de la pensée linéaire, alors que nous sommes, avec tout ce qui est technologique, dans un domaine non linéaire, où l'on avance par des ruptures, comme l'illustrent les progrès permis par nos nouvelles sources de photons uniques.

Vos confrères pensent-ils comme vous ?

Pascale Senellart-Mardon : En 2015, j'ai participé aux États-Unis à un séminaire de réflexion sur la construction des futurs réseaux quantiques, où étaient invités des physiciens développant comme moi les composants quantiques, des théoriciens des réseaux quantiques et des gens des grandes entreprises de télécommunication, qui ont vécu la révolution de l'internet à haut débit. Quand ils nous ont entendus rivaliser de prudence en évoquant nos difficultés pour avancer, leur message a été : « Mais arrêtez de vous prendre la tête ! Vous verrez. » De fait, même si l'on m'avait dit il y a dix ans que mon domaine ressemblerait à ce qu'il est aujourd'hui, je n'y aurais pas cru.

Les équipes chinoises avancent très vite et n'ont apparemment pas de limites en termes de moyens

Si l'on se rappelle où en étaient les télécommunications dans les années 1960, quand des opératrices connectaient les gens à l'aide de fiches dans des standards téléphoniques, est-ce que quelqu'un de cette époque aurait cru qu'aujourd'hui nous aurions tous à la main un petit ordinateur supercommunicant, capable de télécharger sans contact des films en quelques secondes, de synchroniser son horloge, de se connecter à un réseau mondial appelé internet, de faire calculer à distance un trajet, de payer… ?

Nous pouvons donc croire aux ordinateurs quantiques ?

Pascale Senellart-Mardon : Comment dire ? Le chemin que nous avons suivi pour aller du stade où nous en étions à l'époque des communications par sémaphores, au XVIII^e siècle, à celles de notre quotidien a aussi été une succession de promesses faites, d'échecs à les satisfaire, puis d'inventions d'alternatives ouvrant sur de nombreuses possibilités auparavant insoupçonnées. J'ai l'impression que dans la quête de l'ordinateur quantique, la même chose se passe… à un rythme effréné. ■

PROPOS RECUEILLIS PAR FRANÇOIS SAVATIER

BIBLIOGRAPHIE

B. ZYGELMAN, ***A First Introduction to Quantum Computing and Information*****, Springer, 2018.**

P. SENELLART *ET AL.*, High-performance semiconductor quantum-dot single-photon sources, *Nature Nanotechnology*, vol. 12, pp. 1026-1039, 2017.

M. A. NIELSEN ET I. L. CHUANG, ***Quantum Computation and Quantum Information*****, Cambridge University Press, 2010.**

D. MERMIN, ***Calculs et algorithmes quantiques*****, EDP Sciences et CNRS Éditions, 2010.**

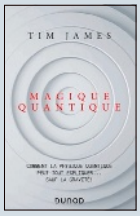
À LIRE EN PLUS

Einstein et les révolutions quantiques
ALAIN ASPECT
CNRS, 2019
(**80 PAGES, 8 EUROS**)

La première révolution quantique a bouleversé notre vision du monde et conduit à des inventions majeures: le transistor, le laser, les ordinateurs. Moins connue est la deuxième révolution quantique engagée en 1935 par le débat entre Albert Einstein et Niels Bohr. Cette révolution repose sur la notion étrange de particules intriquées qui pourrait déboucher à terme sur des technologies nouvelles comme l'informatique quantique.
Cet ouvrage raconte une magnifique histoire de science, dans laquelle l'expérimentation a permis de trancher des débats philosophiques.

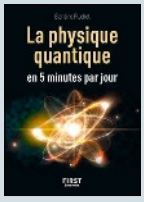
Petit voyage dans le monde des quanta
ÉTIENNE KLEIN
FLAMMARION, 2016
(**194 PAGES, 8 EUROS**)

En 1905 apparaissait une nouvelle physique qui allait révolutionner la façon de décrire la matière et ses interactions: la physique quantique. Elle obligea ses pères fondateurs, Einstein, Bohr, Heisenberg et Schrödinger notamment, à rediscuter le déterminisme et les critères de réalité de la physique classique. Pour la première fois dans l'histoire des sciences, une discipline exigeait un travail d'interprétation afin d'être comprise et appliquée. D'où provient l'incroyable efficacité de la physique quantique?



Magique quantique
TIM JAMES
DUNOD, 2020
(**240 PAGES, 19,90 EUROS**)

Au début du XX^e^ siècle, la science semblait complète et les lois de la nature toutes découvertes, mais des chercheurs intrépides ont réveillé un géant endormi, la mécanique quantique. Dans le monde quantique, les objets peuvent se trouver en deux endroits à la fois, voyager dans le temps est non seulement possible, mais nécessaire, la cause et l'effet peuvent s'inverser et l'observation de quelque chose change son état. Des univers parallèles à l'antimatière, laissez-vous guider par le facétieux Tim James à la découverte des bizarreries du monde de l'infiniment petit!



La Physique quantique en 5 minutes par jour
BLANDINE PLUCHET
FIRST, 2019
(**160 PAGES, 2,99 EUROS**)

Un petit livre pour tous ceux qui, curieux de physique, mais néophytes en la matière, souhaitent enfin comprendre ce qui se cache derrière cette notion de «quantique», dont on entend régulièrement parler sans bien savoir ce qu'elle signifie, souvent d'ailleurs utilisée à tort et à travers. Pour tous ceux qui, curieux, ont envie de faire un voyage dans la pensée des scientifiques, pour y découvrir un monde insaisissable à nos sens, celui de l'infiniment petit, où les lois qui régissent les phénomènes n'ont rien à voir avec celles du monde à notre échelle.

BANDE DESSINÉE

Quantix – La physique quantique et la relativité en BD
LAURENT SCHAFER
DUNOD, 2019
(**176 PAGES, 18,90 EUROS**)

Nos sens nous mentent: temps, matière et énergie n'existent pas tels que nous les percevons. Découvrez cette réalité cachée en suivant les aventures d'une famille ordinaire, et partez à la rencontre de ces chercheurs dont les idées ont révolutionné notre vision du réel: Einstein, Schrödinger, Bohr... et bien d'autres! Le physicien spécialiste de physique quantique Carlo Rovelli a trouvé cet ouvrage «Amusant et fascinant!», tandis que Zep, le créateur de Titeuf, y a trouvé une excuse pour ne plus faire de jogging...

RENDEZ-VOUS