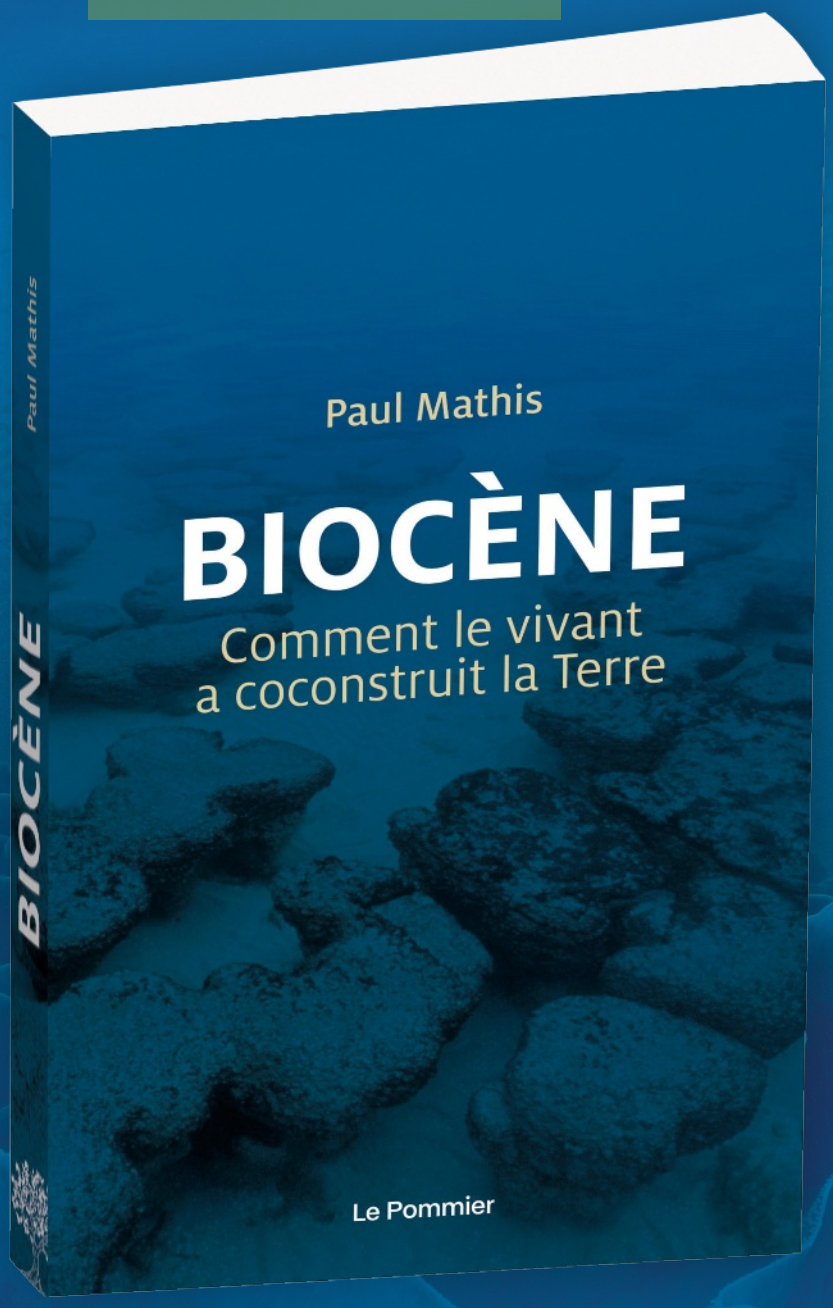
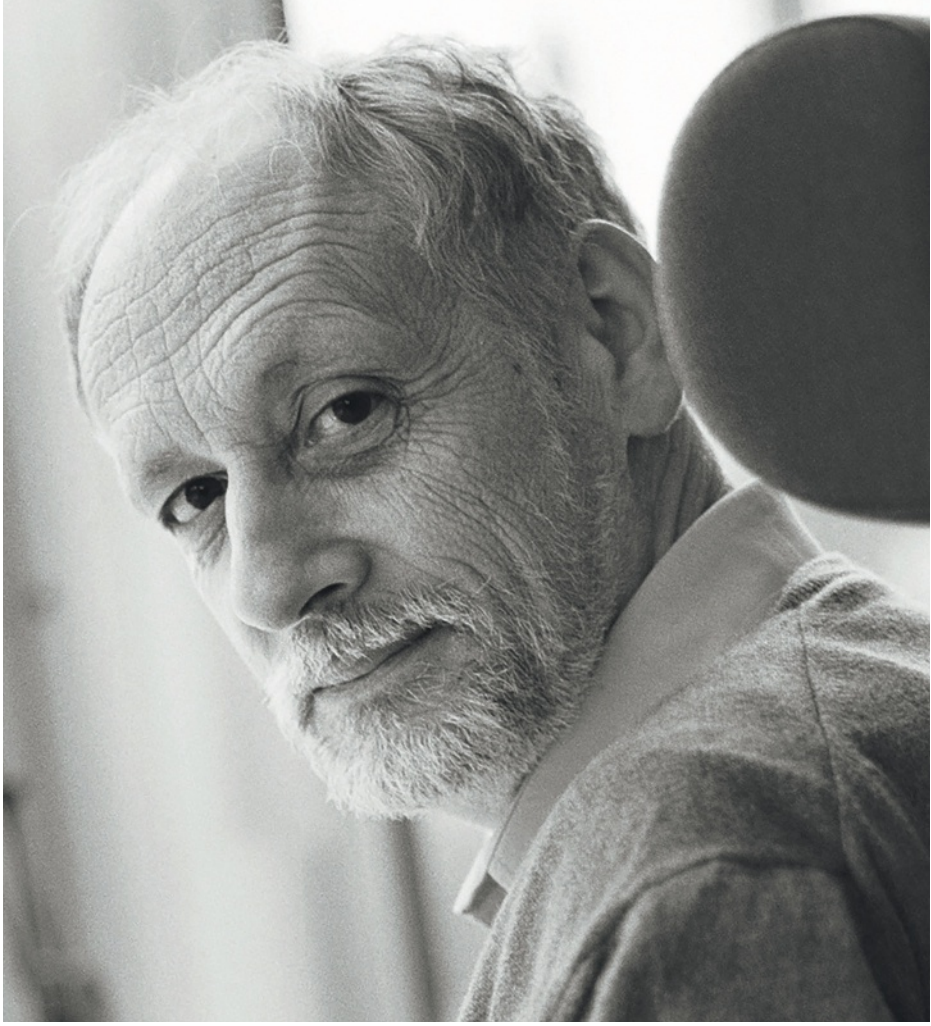
« Un passionnant défrichage de voies nouvelles pour aborder et approfondir quelques enjeux majeurs de notre temps. »

Le Monde des Livres



Éditions
Le Pommier

NICOLAS GISIN
est physicien spécialiste de mécanique quantique et professeur émérite au département de physique appliquée de l'université de Genève. Il est également professeur à l'institut de technologie de Schaffhausen, institut international fondé en 2019 et dont le siège est en Suisse. Nicolas Gisin est par ailleurs cofondateur de la société ID Quantique, créée en 2001 et pionnière dans le développement et la commercialisation des systèmes de cryptographie quantique.



L'internet quantique est pour le physicien un défi fascinant

Comment sécuriser les communications numériques ?
Un internet du futur mettant à profit les lois de la physique quantique offrirait une solution infaillible. À condition de surmonter de nombreuses difficultés techniques et théoriques…
Les explications du spécialiste Nicolas Gisin, qui nous décrit aussi les progrès les plus récents.

© C. Parodi

En quoi consiste l'internet quantique ?

Le réseau internet actuel est un succès technique incroyable qui a connu une croissance explosive ces dernières décennies. On estime qu'en janvier 2021, près de 60% de la population mondiale, soit 4,6 milliards d'individus, y ont accès. Internet fait partie de notre vie. Nous l'utilisons tous les jours pour échanger divers types de données, des textes, des images, des vidéos. Il est difficile d'imaginer comment le monde fonctionnerait sans ce réseau.

D'un point de vue technique, l'internet classique est un réseau décentralisé bâti sur des nœuds répartis à travers le globe et reliés par des fibres optiques. Les unités d'information, les bits, sont transmises sous la forme d'impulsions lumineuses, chacune contenant de l'ordre du million de photons. Selon qu'on reçoit un signal ou non, le bit prend la valeur «1» ou «0».

Ce réseau fonctionne très bien. Mais, d'un point de vue conceptuel, on peut se poser la question suivante: jusqu'où peut-on réduire l'intensité lumineuse? La limite ultime est de n'avoir qu'un seul photon par impulsion. À une telle échelle, les règles de la physique classique ne s'appliquent plus et on entre dans le monde fascinant de la physique quantique. Notamment, le photon peut être dans un état dit «de superposition des états "0" et "1"», c'est-à-dire qu'il peut être, dans un sens mathématiquement précis, dans ces deux états à la fois. Ce phénomène quantique confère une grande richesse au système: le bit classique est remplacé par le bit quantique, ou qubit, qui porte alors une «information quantique». L'idée de l'internet quantique est d'utiliser le réseau actuel de fibres optiques pour échanger des qubits.

Notons que l'on retrouve la même idée de réduction avec l'ordinateur. Pour remplacer les paquets d'électrons qui circulent dans les transistors, de nombreux laboratoires et entreprises travaillent sur le concept d'un ordinateur quantique qui manipulerait des qubits. De telles machines seraient très intéressantes, car on a montré qu'elles pourraient réaliser certains calculs exponentiellement plus vite que les ordinateurs classiques.

Et quels sont les avantages de l'internet quantique ?

Le premier concerne les volumes de données que l'on pourra faire circuler sur le réseau. Les besoins ont décuplé ces dernières années. En réduisant l'information à des photons uniques, on voit tout de suite qu'il sera possible d'augmenter les débits.

Cette idée de photon unique conduit à un deuxième argument en faveur de l'internet quantique. Mais il faut le prendre avec précaution et le considérer comme un idéal à atteindre. À terme, l'internet quantique pourrait être moins énergivore que le réseau actuel.

> En manipulant des photons uniques soumis aux lois de la physique quantique, on obtient automatiquement la sécurité de l'information

Le principe est tout simple: on dépense moins d'énergie à émettre un photon unique qu'un paquet de ces particules de lumière. L'argument s'applique aussi à l'ordinateur quantique, qui pourrait, en principe, un jour réaliser des calculs en consommant moins d'énergie qu'un ordinateur classique.

On est encore loin de cet idéal. Les qubits sont des objets fragiles. S'ils interagissent avec leur environnement, ils perdent leur état de superposition et tous les avantages associés. C'est le phénomène de «décohérence». Cette situation est surtout critique dans les ordinateurs quantiques. La solution pour maintenir l'état quantique du qubit le plus longtemps possible consiste à refroidir l'ordinateur à des températures d'une fraction de degré au-dessus du zéro absolu. Or les dispositifs cryogéniques dépensent beaucoup d'énergie. Mais les progrès dans le domaine de l'ordinateur quantique laissent espérer qu'il sera possible d'en concevoir qui fonctionnent à température ambiante. L'internet quantique est un peu moins sensible à ces problèmes de décohérence, mais certains éléments envisagés pour ce réseau de demain demandent aussi d'être refroidis et ils consomment pour l'instant encore beaucoup d'énergie.

La sécurité est censée être un atout majeur de l'internet quantique. Pourquoi ?

Le fait de manipuler des photons uniques soumis aux lois de la physique quantique procure un avantage qui n'est pas évident *a priori*: on obtient automatiquement la sécurité de l'information. C'est pour moi l'argument principal, il est indiscutable, nous sommes déjà capables de l'exploiter et il n'y a pas d'autre solution aussi efficace.

Tous les dispositifs numériques omniprésents dans notre quotidien (l'ordinateur, les téléphones portables et l'internet classique) ont ouvert de nombreuses portes à des espions, gouvernementaux ou non, capables d'intercepter ou de dérober des données sensibles. La solution actuelle pour protéger ces informations consiste à les rendre illisibles grâce à des algorithmes de chiffrement. Sans la clé de chiffrement, l'espion ne peut pas lire les messages.

Les algorithmes de chiffrement reposent sur des problèmes mathématiques qui sont *a priori* difficiles à résoudre en un temps raisonnable. Par exemple, le chiffrement RSA développé en 1977 par les cryptologues américains Ronald Rivest et Leonard Adleman et l'Israélien Adi Shamir est utilisé pour sécuriser les échanges dans le commerce électronique. Cet algorithme exploite la décomposition en facteurs premiers d'un nombre très grand (actuellement d'au moins 1024 bits, soit des nombres décimaux à 309 chiffres) pour définir la clé de chiffrement. Or, bien que ce nombre très grand ne soit pas secret (d'où la terminologie de clé publique),