Les lois nouvelles de l'information quantique

JEAN-PAUL DELAHAYE

Principe de non-duplication, téléportation, cryptographie inviolable, codes correcteurs, parallélisme illimité : l'informatique quantique est née.

Quand, en 1937, George Stibitz fabrique dans sa cuisine un additionneur binaire à relais qui fonctionne avec deux chiffres (et qui ne fait donc que 4 additions différentes, 0+0, 0+1, 1+0 et 1+1), il ne suscite aucun enthousiasme. Quelques années plus tard, les descendants de sa machine, les ordinateurs, ont envahi le monde.

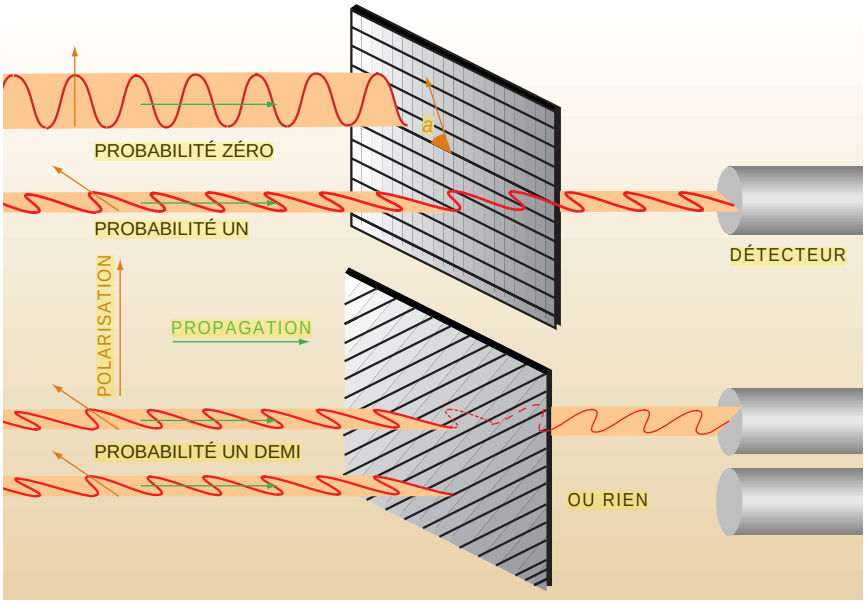
Les physiciens quantiques viennent de fabriquer l'équivalent quantique de l'additionneur de Stibitz et la théorie du calcul quantique prouve que, si l'on progresse normalement, les ordinateurs quantiques seront plus puissants que ne pourrait l'être un ordinateur classique de la taille du système solaire fonctionnant à la vitesse de la lumière avec des unités de mémoire de la taille de l'atome : nous vivons la naissance d'une technologie fondée sur les miracles théoriques du monde quantique, et qui projette ceux-ci dans notre réalité quotidienne.

Parallèlement à nos premiers pas vers ces calculateurs de rêve, une révolution modifie notre conception de l'information. Naïvement, nous avons trop longtemps adopté une vue préquantique de l'information. Pourtant ce qui «va de soi» concernant l'information est erroné si le monde est régi par la mécanique quantique. Le traitement de l'information dans un monde quantique est différent de sa manipulation dans un monde classique : il nous faut découvrir et pratiquer de nouvelles règles pour acquérir de l'information, la copier, la cacher, la mémoriser, la combiner, etc. En conséquence, la définition et la pratique du calcul changent et remettent en cause les fondements de l'informatique théorique.

Nous allons passer en revue dans cet article, en complément du précédent, quelques unes des différences entre information classique et information quantique. Précisons, avant cet examen, que nous adopterons une vue «physicienne» de l'information et que nous ne traitons évidemment pas d'information sémantique (le sens d'un mot, d'un texte, d'une musique, etc.) ou d'autres notions d'information destinées à cerner des contenus non symboliques.

Le lecteur quantique modifie le livre

Dans le monde classique, la consultation de l'information n'en modifie pas la teneur : lire un livre n'en change pas le texte, consulter un site Internet le laisse inchangé. Dans le monde classique, un objet est le même, qu'il soit connu ou pas. En revanche, l'ac-



1. INFORMATION ALÉATOIRE ET DUPLICATION INTERDITE. Un photon se propage selon une direction de polarisation perpendiculaire à son axe de propagation. Cette direction de polarisation est caractérisée par un angle *a*, qu'aucune mesure ne peut déterminer entièrement. Si, pour tenter de connaître cet angle, on place sur le trajet du photon un filtre polarisant d'angle 0, suivi d'un détecteur, alors le photon passera certainement si *a* égale 0, sera intercepté si *a* égale 90°, et passera avec une probabilité $\cos^2 a$ pour les angles intermédiaires. La détection ou non du photon est donc insuffisante pour connaître l'angle *a*. Dans une suite de photons ayant chacun un angle de polarisation égal à 45 degrés, la probabilité que chaque photon soit détecté après passage par le filtre est 1/2. En passant par le filtre polarisant, le photon perd son orientation primitive, ce qui rend l'angle *a* définitivement inconnaissable et le photon impossible à dupliquer.

quisition de l'information sur certains systèmes quantiques les perturbe irrémédiablement. C'est une conséquence du principe d'incertitude d'Heisenberg : mesurer une grandeur associée à un objet interdit d'en connaître d'autres ; plus grave, elle en fait un autre objet. L'information quantique a une réalité physique différente de l'abstraction de l'information classique.

Cette propriété quantique selon laquelle la mesure modifie l'objet mesuré trouble depuis longtemps ceux qui tentent de comprendre la mécanique quantique. Un exemple de cette difficulté, la détermination de la direction de polarisation d'un photon, est détaillée sur la figure 1.

Informations aléatoires et indéterminisme

Cet exemple du photon montre aussi que l'information quantique est parfois authentiquement aléatoire : si, après avoir polarisé un photon selon une direction *a*, on le fait passer dans un filtre polarisant dont l'axe fait un angle de 45° avec *a*, on le détectera exactement une fois sur deux. En envoyant dans le dispositif une série de photons identiques, on obtient une suite de détections symbolisée par une suite de 1 et de 0 (1 pour une détection ; 0 pour une absence de détection) qui possède toutes les propriétés attendues d'une suite de 0 et de 1 parfaitement aléatoire. De telles suites sont intéressantes pour des méthodes de calcul comme la méthode de Monte-Carlo ou le cryptage des informations. Aussi cette propriété a-t-elle conduit à proposer des générateurs de bits aléatoires fondés sur des mécanismes quantiques *(voir la rubrique* Logique et calcul *du mois de mars 1998, qui traite des suites aléatoires en informatique)*.

Copier l'information

Les moines du Moyen Âge, nos photocopieuses et les lecteurs de disquette de nos ordinateurs copient des informations sans rencontrer d'obstacles fondamentaux. Dupliquer l'information classique et en faire de multiples versions est facile et ne coûte presque rien. Comme cette information n'est pas de nature physique, elle n'est pas liée à son support, et elle est donc copiable. Dans le monde quantique, la copie n'est pas toujours possible. Le principe de non-duplication («no-cloning principle») énoncé par W. Wootters, W. Zurek et D. Dieks en 1982 exprime cette impossibilité : un état quantique inconnu ne peut pas être dupliqué.

Reprenons l'exemple du photon : vous ne réussirez jamais à dupliquer un photon dont vous ne savez rien, car vous ne pourrez jamais connaître complètement son état quantique. Si vous essayez, dès que vous commencez à mesurer certaines quantités observables (la polarisation selon une direction par exemple), vous détruisez l'état quantique du photon et vous ne pouvez mesurer d'autres observables. Cette impossibilité interdit la duplication. Notons quand même que le principe de non-duplication n'empêche pas la création de plusieurs objets identiques (par exemple, plusieurs photons de même polarisation) lorsque l'information liée aux objets est connue, car elle résulte du moyen de fabrication.

Cacher l'information, et distribuer des clefs secrètes

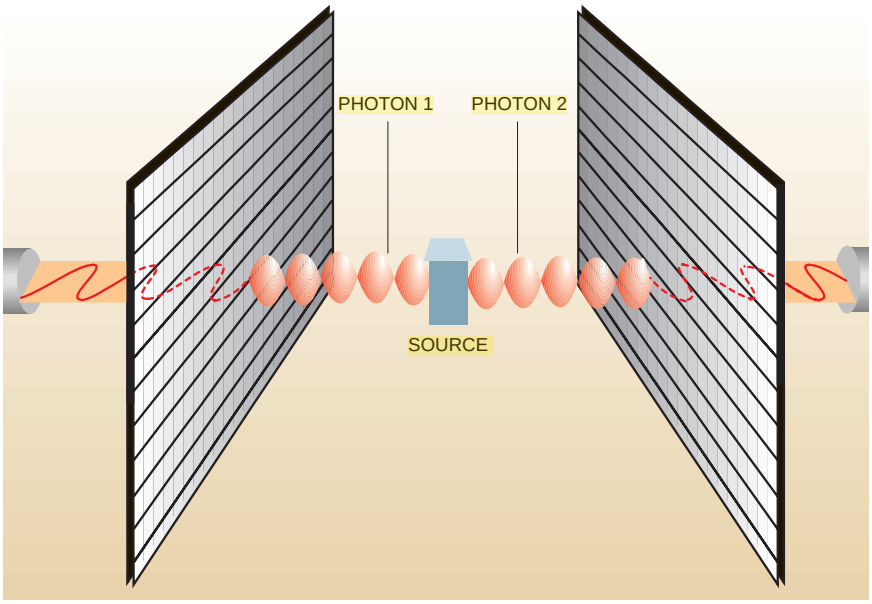
Cacher de l'information classique – ce qui est le but de la cryptographie – est théoriquement difficile : la plus grande partie des méthodes de cryptographie mathématique utilisées aujourd'hui se fonde sur des conjectures non démontrées et sont donc incertaines. Cet état de fait arrange les agences de renseignements, qui laissent croire que les codes légalement autorisés sont inviolables, alors qu'elles savent déchiffrer certains d'entre eux.

En revanche, la cryptographie quantique, qui utilise le principe de non-duplication des photons quantiques, propose des méthodes de distribution de clefs secrètes sûres et sans équivalent classique. Ces méthodes garantissent absolument le secret des échanges.

La cryptographie quantique est aujourd'hui suffisamment développée pour qu'avec des fibres optiques on sache distribuer des clefs secrètes entre des points distants de plusieurs dizaines de kilomètres. L'utilisation commerciale ou militaire de ces méthodes est sur le point de se faire (et a peut-être déjà eu lieu... de manière secrète).

Isoler l'information : la non-localité

Une autre propriété singulière de l'information quantique, étrange et difficile à comprendre, est la non-localité :



2. PHOTONS CORRÉLÉS ET INFORMATION ÉTALÉE. On sait produire des paires de photons corrélés, c'est-à-dire dont les directions de polarisation sont inconnues, mais identiques. Une telle paire contient une information non locale, possibilité exclue dans le monde classique. Cette non-localité de l'information se manifeste de la manière suivante : si l'on dispose sur le trajet des photons des filtres polarisants de même orientation, les deux photons corrélés émis par une source seront tous les deux interceptés ou tous les deux transmis, quelle que soit la distance qui sépare les photons au moment de la mesure (on a mené des expériences où les photons sont séparés l'un de l'autre de 10 kilomètres). Tout se passe comme si le premier photon savait comment l'autre se comporte : aussi faut-il admettre que deux photons corrélés forment un objet physique unique qui contient une information étalée dans tout l'espace.