

La mécanique quantique révolutionne l'informatique

CLAUDE LAFLEUR

Édition [du mercredi 28 mai 2008](#)

Mots clés : mécanique quantique, physique, Prix, Informatique, Québec (province)

La physique newtonienne qu'on enseigne à l'école est «fausse»!

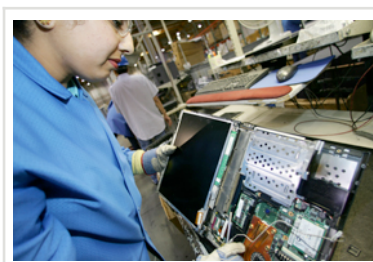


Photo: Agence France-Presse

Gilles Brassard est tout un personnage... c'est le moins qu'on puisse dire! Enfant surdoué, il amorce ses études universitaires dès l'âge de 13 ans. Passionné d'informatique, il crée une nouvelle branche: le traitement quantique de l'information. Il invente même la méthode à toute épreuve pour coder des messages: la cryptologie quantique. Et voici qu'il préconise l'enseignement de la physique quantique dès le secondaire, étant donné que «la physique traditionnelle est tout bonnement fausse!»

Professeur au département d'informatique et de recherche opérationnelle de l'Université de Montréal, Gilles Brassard est titulaire de la Chaire de recherche du Canada en informatique quantique. «Je travaille avant tout sur les fondements de la mécanique quantique afin de comprendre mieux comment fonctionnent l'Univers et le monde physique et, dans un certain sens, pourquoi...», dit-il d'une voix douce.

Comme tout bon roman d'espionnage nous l'enseigne, la cryptographie sert à communiquer des messages à l'insu d'espions éventuels. Mais voilà qu'elle suscite du coup la curiosité du contre-espionnage, qui essaie par tous les moyens de décoder ces messages. Bien entendu, on assiste à un duel entre encrypteurs et perceurs de codes.

«Ma contribution la plus connue consiste à avoir découvert, en collaboration avec Charles Bennett, que l'utilisation judicieuse de la mécanique quantique permet de communiquer avec une garantie de confidentialité impossible à obtenir par toute approche classique», explique M. Brassard.

De plus, ses collègues et lui ont montré que la mécanique quantique permet de réaliser des tâches qui sont hors du commun. Par exemple, un ordinateur quantique pourrait faire davantage de calculs que la réunion de tous les ordinateurs fabriqués à ce jour!

À l'épreuve de tout espion et du temps

«Pour l'instant, l'application la plus pratique de la mécanique quantique est la cryptographie, précise Gilles Brassard. C'est par là que j'ai commencé ma carrière.» En fait, le physicien Bennett et lui ont abordé le problème «sans trop se prendre au sérieux, dit-il. Mais, une chose menant à une autre, il nous a fallu trois ans pour en venir à penser à utiliser la mécanique quantique pour faire de la cryptographie.»

Le duo invente ainsi en 1984 une clé d'encryptage baptisée BB-84 (pour Bennett-Brassard 1984). C'était en soi un prodige puisque, pour la première fois, la mécanique quantique était utilisée pour réaliser une tâche en traitement d'information. Qui plus est, les chercheurs ont démontré que celle-ci permet d'effectuer une tâche impossible à réaliser selon la mécanique classique. «La cryptographie quantique offre une sécurité dont on peut démontrer qu'elle est impossible à briser, indique le chercheur, ce qui n'est nullement le cas avec la cryptographie traditionnelle.»

La création de la clé BB-84 mène à la mise au point (cinq ans plus tard) d'un prototype d'encryptage. «Notre système fonctionne très bien puisque, par la suite, des "gens sérieux" ont pu s'en servir», relate M. Brassard. Entendons là que les services secrets américains se sont intéressés à cette invention. Toutefois, le chercheur

ignore si la clé est réellement en usage. «Je ne sais pas si elle est utilisée par les services secrets, mais, si je le savais, je ne pourrais vous le dire!», laisse-t-il filer.

«D'autre part, il y a un autre aspect intéressant, enchaîne-t-il. Peut-être qu'aujourd'hui personne n'est en mesure de déchiffrer les messages codés de façon traditionnelle, mais rien ne prouve qu'on n'y parviendra pas un jour ou l'autre.» Il est même très possible qu'on découvrira de nouvelles façons de procéder «révolutionnaires» qui permettront de percer les systèmes traditionnels. «Il se peut même que quelqu'un possède déjà les clés nécessaires mais qu'il ne le dise à personne...»

Une autre possibilité: les messages indéchiffrables aujourd'hui sont stockés dans l'espoir de les décoder ultérieurement. «Par exemple, rien n'empêche un malfaiteur ou un gouvernement de conserver les données cryptographiques qui circulent dans Internet en se disant qu'un jour il pourrait y avoir de nouvelles façons de le briser, explique M. Brassard. Ainsi, non seulement on ne possède aucune protection contre le présent, mais rien ne garantit qu'à l'avenir on ne dévoilera pas les secrets d'aujourd'hui.»

Par contre, les systèmes de cryptage quantique seront toujours inviolables. «En fait, pour parvenir à briser un tel système, il faudrait démontrer que la physique quantique est fausse!», résume le chercheur, qui s'empresse d'ajouter qu'un tel prodige «serait une formidable révolution scientifique... ce qui serait en soi fort intéressant!»

Pourquoi enseigne-t-on la «fausse» physique?

Après trente ans de recherches, Gilles Brassard n'est jamais à court d'idées étonnantes. Ainsi, il préconise l'enseignement de la mécanique quantique dès l'école secondaire. Pourquoi? «Parce que la physique newtonienne [qu'on enseigne] est à toutes fins pratiques fausse!»

À ses yeux, c'est comme si on enseignait que tout tourne autour de la Terre, y compris le Soleil, parce que c'est plus facile à comprendre. «Mais ce qu'on enseignerait alors serait faux, tranche-t-il, comme la physique de Newton!»

En fait, les lois de la physique classique s'appliquent aux objets qui se déplacent à faible vitesse -- ce qui est le cas de ce qui se passe au quotidien. Toutefois, comme l'a démontré Einstein avec la relativité, tout change grande vitesse, dont le concept même du temps immuable. Lorsque des corps se déplacent, il faut par conséquent apporter des corrections aux lois de Newton.

«La relativité, si vous voulez, offre une correction à la physique de Newton, explique le professeur. Mais elle n'en demeure pas moins une correction, tandis que la mécanique quantique est un changement complet de perspective. Il ne s'agit pas de corriger la physique selon Newton, mais de tout recommencer.»

De surcroît, poursuit-il, la physique quantique n'a jusqu'à présent jamais été prise en défaut, quelles qu'aient été les expériences faites pour la mettre à l'épreuve. «Il n'y a jamais eu la moindre déviation, insiste-t-il. Ainsi bien qu'on ne puisse absolument être certain qu'elle est parfaitement conforme à la réalité, la mécanique quantique semble plus conforme que la mécanique de Newton... dont on sait qu'elle est fausse!»

Pourquoi donc ne pas enseigner le véritable fonctionnement de l'Univers dès le secondaire?, se demande en conséquence le chercheur, qui se voyait d'ailleurs reconnaître samedi soir dernier comme personnalité de l'année par la Fédération de l'informatique du Québec lors de la soirée de remise des Octas.

Collaborateur du Devoir

Vos réactions

[Du journalisme tout ça...](#) - par Eschbach 59
Le mercredi 28 mai 2008 09:00

[Constat d'échec du système scolaire](#) - par Serge Grenier (serge.grenier@gmail.com)
Le mercredi 28 mai 2008 09:00

[Ne pas mélanger science et enseignement de la science](#) - par Robert Mainville
Le mercredi 28 mai 2008 08:00

[C'est ben beau mais comment ça marche?](#) - par Daniel Creusot
Le mercredi 28 mai 2008 05:00

[Bien entendu](#) - par Georges Allaire
Le mercredi 28 mai 2008 00:00

Réagissez à ce texte

Pour ajouter un commentaire,
identifiez vous :

adresse électronique

ok

Lire aussi

Transformation des processus
organisationnels - La vie est plus
simple à la campagne
[/2008/05/28/191580.html]

Relève étudiante collégiale -
Sainte-Foy triomphe au Grand Prix du
Nunavut [/2008/05/28/191581.html]

Technologies au service de la
collectivité - Internet sans fil gratuit
pour qui habite ou visite Sherbrooke
[/2008/05/28/191582.html]

Octas de l'excellence - Revenu
Québec a les fraudeurs à l'oeil
[/2008/05/28/191583.html]

Octas 2008 - Revenu Québec a de
quoi fêter [/2008/05/28/191584.html]

Publicité - Un produit ou un service ?

Recherche 