Date: 02.03.2018

ENTREPRISE ROMANDE

UNIVERSITÉ DE GENÈVE

Entreprise romande
1211 Genève 11
058/ 715 32 44
www.fer-ge.ch

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 21'376
Parution: 23x/année

Page: 5
Surface: 75'277 mm²

Ordre: 1094772
N° de thème: 377.116

Référence: 68738862
Coupure Page: 1/3

Processeurs quantiques: ils vont bouleverser l'informatique

Un processeur quantique pourrait montrer dès 2018 sa supériorité par rapport à un ordinateur classique sur quelques problèmes bien choisis, estime Nicolas Gisin, professeur à l'Université de Genève. Cela ouvre des perspectives vertigineuses.

PROPOS RECUEILLIS PAR
PIERRE CORMON

Les ordinateurs quantiques? «Ils vont changer notre savoir, la vie économique et le monde aussi radicalement que la première génération d'ordinateurs l'a fait depuis les années 1960.» C'est ce qu'affirme Mike Osborne, chercheur en sécurité au laboratoire IBM de Zurich, dans la *Wirtschaftswoche*. Les processeurs quantiques, dont on annonce l'arrivée imminente, auront en effet une capacité de calcul beaucoup plus grande que les processeurs traditionnels, ce qui permettra de développer toutes sortes d'applications impossibles à faire tourner sur les ordinateurs actuels.

Des entreprises et des chercheurs annoncent régulièrement des percées dans ce domaine et une start-up canadienne, D-Wave, commercialise déjà ce qu'elle présente comme un ordinateur quantique. Qu'en est-il réellement? Le point avec Nicolas Gisin, chef du Group of Applied Physics Optique à l'Université de Genève et cofondateur de l'entreprise ID Quantique, qui commercialise des solutions de cryptage fondées sur la physique quantique.

Où en est le développement de l'ordinateur quantique?

Cela fait environ cinq ans que l'on croit vraiment qu'on pourra le réaliser. Au début 2017, j'ai annoncé, comme beaucoup de mes collègues, qu'un processus quantique pourrait montrer dans le courant de l'année sa supériorité sur un ordinateur classique, sur quelques problèmes choisis. Cela n'a pas été le cas. Je reprends le pari pour 2018.

Mais la startup D-Wave commercialise déjà un ordinateur muni d'un processeur quantique!

C'est ce qu'elle prétend, et ce qu'elle a réalisé est remarquable. Elle a mis au point un processeur qui fonctionne, en investissant cent millions de dollars, alors que le développement d'un nouveau processeur coûte un milliard chez Intel. D-Wave a apporté un changement significatif, avec une autre manière de traiter l'informatique. Mais sa machine ne fonctionne pas mieux qu'un ordinateur traditionnel et sa fonctionnalité quantique n'a pas été démontrée. Je ne connais aucun physicien sérieux qui y croie. Je n'aime d'ailleurs pas beaucoup le terme d'ordinateur quantique. Il faudrait plutôt parler de processeur quantique.

Pourquoi?

Parce que le processeur est le cœur de l'ordinateur. On rajoute ensuite des éléments autour, mais c'est le processeur qui fait la différence. Ceux que l'on utilise actuellement suivent des idées des années 1950, leur architecture n'a pas vraiment changé depuis. Ils sont devenus beaucoup plus rapides, beaucoup plus puissants, beaucoup plus petits, mais en fonctionnant toujours de la même manière.

Laquelle?

Ils traitent une information après l'autre, avec des bits qui ne peuvent prendre que deux valeurs, 0 ou 1. Un processeur quantique pourrait en revanche traiter une quantité phénoménale d'informations en parallèle, sur un même processeur, en exploitant le parallélisme quantique (contrairement au bit traditionnel, un bit quantique (qubit) peut prendre d'innombrables valeurs – *ndlr*). On est déjà parvenu à construire des processeurs quantiques qui montrent que le principe fonctionne et IBM permet d'accéder à l'un d'eux en ligne, de 16 qubits. Mais c'est encore trop peu pour dépasser les possibilités des ordinateurs traditionnels.

Combien de qubits faudrait-il pour faire une vraie différence?

Je pense que le seuil critique se situe entre cinquante et cent. On pourra alors faire des choses dont les ordinateurs traditionnels, même les plus puissants, ne sont pas capables. Alors que dans un processeur traditionnel, ajouter un bit ne fait pas

Date: 02.03.2018

ENTREPRISE ROMANDE

Entreprise romande
1211 Genève 11
058/ 715 32 44
www.fer-ge.ch

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 21'376
Parution: 23x/année

Page: 5
Surface: 75'277 mm²

UNIVERSITÉ DE GENÈVE

Ordre: 1094772
N° de thème: 377.116

Référence: 68738862
Coupure Page: 2/3

une grande différence, ajouter un qubit à un processeur quantique double sa capacité.

Quels pourraient être les usages des processeurs quantiques?

J'en vois trois. Le premier, que l'on cite toujours, est de déchiffrer des données cryptées. Tous les systèmes de cryptage actuels fondés sur des méthodes traditionnelles seront morts, car les processeurs quantiques les casseront très facilement (lire ci-contre – *ndlr*). Mais je crois que les processeurs quantiques ne seront jamais utilisés pour cela.

Pourquoi?

Parce qu'ils auraient besoin de milliers, voire de centaines de milliers de qubits pour le faire et que d'ici qu'ils atteignent cette puissance, on aura déjà changé les systèmes de cryptage, par exemple pour de la cryptographie quantique qui résistera à tout progrès en puissance de calcul, même des ordinateurs quantiques.

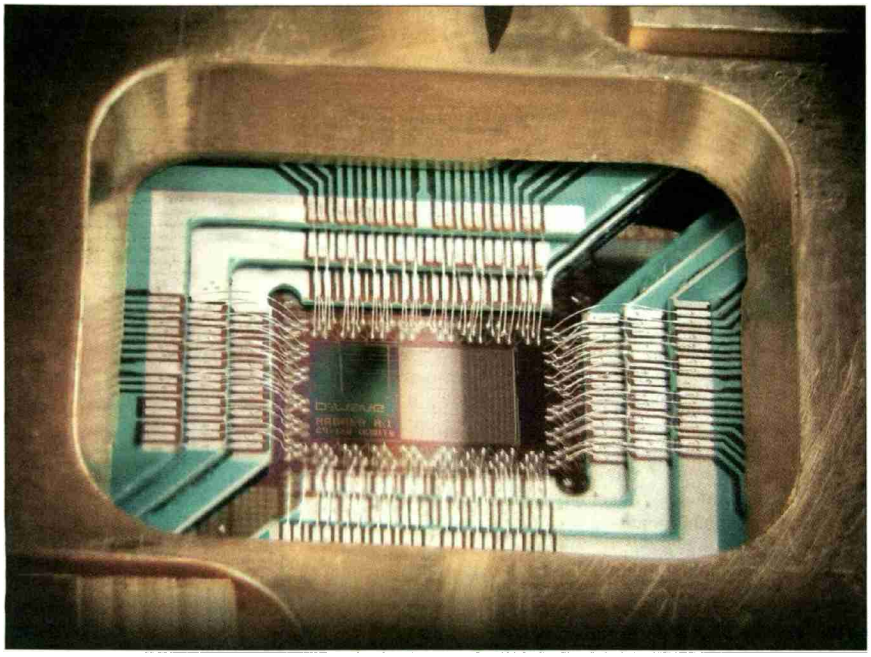
Qu'en est-il du deuxième type d'usage?

Dans de multiples secteurs, on développe déjà des produits grâce à des simulations sur ordinateur – c'est même le cas des bombes atomiques. Dans d'autres, comme la chimie, la pharmacie ou les matériaux, cela demanderait des puissances de calcul phénoménales, que les ordinateurs traditionnels ne sont pas capables de fournir. Avec des processeurs quantiques de quelques centaines de qubits, cela devrait en revanche être possible, permettant d'accélérer le développement de nouveaux médicaments, de nouveaux matériaux, etc.

Et le troisième type d'usage?

C'est l'essentiel: c'est celui dont personne n'a encore la moindre idée! Croyez-vous que la génération des Turing et Von Neumann, où se sont développés les premiers ordinateurs, imaginait qu'ils allaient servir pour jouer ou pour créer des sites de rencontres?

Les prototypes d'ordinateurs quantiques ont aujourd'hui la taille d'une colonne Morris. Aura-t-on un jour des ordinateurs quantiques personnels? Je n'en sais rien, mais rien n'empêche de l'imaginer. Je pense cependant que je verrai les ordinateurs quantiques de mon vivant, pas que j'en aurai un à la maison. ■



CIRCUIT INTÉGRÉ PRODUIT PAR LA FIRME CANADIENNE D-WAVE. *Elle affirme commercialiser un ordinateur quantique, ce qui laisse les physiciens sceptiques.*

Date: 02.03.2018

ENTREPRISE ROMANDE

Entreprise romande
1211 Genève 11
058/ 715 32 44
www.fer-ge.ch

Genre de média: Médias imprimés
Type de média: Presse spécialisée
Tirage: 21'376
Parution: 23x/année

Page: 5
Surface: 75'277 mm²

UNIVERSITÉ DE GENÈVE

Ordre: 1094772
N° de thème: 377.116

Référence: 68738862
Coupure Page: 3/3

«Il faut changer notre approche du cryptage»

L'arrivée des processeurs quantiques pose un gros défi aux systèmes de cryptage traditionnels. Ces derniers sont en effet fondés sur des problèmes mathématiques très complexes, que les ordinateurs traditionnels auraient besoin de parfois plusieurs années pour résoudre. Avec leur puissance de calcul phénoménale, les processeurs quantiques n'auront aucune peine à le faire très rapidement.

«Une solution consiste à protéger les systèmes de cryptage par des problèmes mathématiques encore plus complexes», remarque Nicolas Gisin. «On sera protégé pendant dix ans et avec la progression de la puissance des processeurs quantiques, il faudra de nouveau tout changer. Ce sera très vite invivable. On peut aussi complètement changer de philosophie et fonder les systèmes de sécurité sur la cryptographie quantique. L'investissement de base est plus élevé, mais on n'a pas besoin de renouveller l'équipement tous les dix ans: ce type de système est inviolable. Sa limite est qu'il ne fonctionne encore que sur de courtes distances, entre Genève et Lausanne ou Berne et Zurich.»