Les ordinateurs quantiques seront bientôt là mais sommes-nous prêts à la révolution qu'ils vont entraîner ?

L'ordinateur quantique, bien plus qu'un fantasme, suscite l'intérêt de grandes firmes telles qu'IBM, Microsoft ou Google. Ses capacités de calcul impressionnantes pourraient cependant représenter un danger pour la sécurité de nos données.

Avec Jean-Gabriel Ganascia

Atlantico : L'ordinateur quantique pourrait, de toute évidence, bousculer le monde dans lequel nous évoluons aujourd'hui. Tant et si bien que de plus en plus de firmes (IBM, Microsoft, Google, etc.) s'intéressent à son développement. Dans quelle mesure un tel bouleversement pourrait représenter un danger ? A l'heure où de plus en plus de données personnelles sont collectées, faut-il craindre une faille ?

Jean-Gabriel Ganascia : Ce n'est pas tellement une faille qu'il faut craindre : si l'ordinateur quantique se développe, il disposera de capacités de calcul autrement plus élevées et considérables que les machines actuelles. Par conséquent, il sera en mesure de casser un certain nombre de mesures de protection, de cryptage. Aujourd'hui, la protection est intimement liée à la capacité de calcul des ordinateurs qui vont tenter de décrypter les informations. Si des ordinateurs quantiques, d'une puissance incomparable à celle des ordinateurs contemporains, s'essayent à décrypter ces modèles de protection, ils seront nécessairement beaucoup plus efficaces.

Il va de soi, cependant, que si nous avons affaire à des ordinateurs quantiques, nous aurons également accès à des capacités de cryptages plus importantes et donc à des clés plus grandes. Cela signifie que pour se prémunir de tels risques, les gens devront s'équiper d'ordinateurs quantiques. Cela signifie également que les données anciennes, cryptées avec des méthodes traditionnelles, risquent d'être accessibles à l'ensemble de la population. Quand on sait qu'il s'agit actuellement de toutes nos données, de l'état civil à la santé en passant, par exemple, par les données bancaires, on imagine bien quel bouleversement cela peut représenter. Socialement, cela peut clairement avoir des côtés assez néfastes.

Le risque, c'est bien que toutes ces données soient visibles, piratées ou même falsifiées. Dans la mesure où elles seront accessibles à une majorité, cette majorité pourrait les transformer… sans que cela ne soit très facile de s'en rendre compte. Cela pourrait être utilisé par tout type d'individus malhonnêtes.

Attention, néanmoins. Ce qui constitue un danger considérable n'est pas le régime stable, qu'il s'agisse de l'ordinateur quantique ou de nos machines actuelles. C'est la transition, ce moment où l'on passe d'un monde à un autre. C'est pour cela qu'il faut être très attentif à ce qui va se produire, pour pouvoir anticiper quelques temps avant le changement. Cela soulève évidement certaine

questions : sommes-nous prêts ? En l'état, non, certainement pas. Cependant, il est important de garder à l'esprit que l'ordinateur quantique n'arrivera pas demain, ni même l'année prochaine. Nous avons encore un peu de temps devant nous. Il n'est pas possible de se préparer à quelque chose qui demeure encore très improbable (à savoir son arrivée prochaine, pas son arrivée dans l'absolu). D'autant plus que nous disposons encore d'informations au sujet de son développement.

Si l'ordinateur quantique est aussi efficace pour décoder des données et rendre nos mécanismes de protection actuels obsolètes, peut-on espérer que sa capacité à crypter les données sera à la hauteur de sa capacité à les décrypter ? Quels sont les points de différences entre la cryptographie actuelle et la cryptographie quantique ?

Oui, bien sûr. Un ordinateur quantique permet des méthodes de cryptage qui sont plus robustes que les actuelles.

Il est important de réaliser que la cryptographie quantique n'est pas nécessairement liée à l'ordinateur quantique : il est possible d'avoir une cryptographie quantique sans ordinateur quantique. Il se peut donc que de telles méthodes de cryptographie précèdent les ordinateurs quantiques. Cela nous permettrait de mieux crypter les données et de les rendre plus difficiles à décrypter pour un ordinateur actuel certes, mais également pour un ordinateur quantique. Le principe de cette méthode consiste à transmettre des clés de cryptages sous forme quantique. Par conséquent, les deux individus qui échangent s'envoient la même clé (générée aléatoirement, ce qui lui permet d'être à la fois très longue et particulièrement robuste). Si un tiers en venait à décrypter cette clé, la propriété des objets quantique est telle que les individus engagés dans l'échange pourraient se rendre compte qu'un observateur a dérobé la clé. C'est la raison pour laquelle il s'agit d'une méthode aussi efficace et qu'elle diffère des principes de cryptages actuellement utilisés.

Ceux-ci se divisent en deux catégories : le cryptage symétrique et le cryptage asymétrique. Concrètement, la cryptographie symétrique correspond à une clé de codage unique, qui est la même pour celui qui code et celui qui décode. La cryptographie asymétrique consiste à séparer ces deux clés : la clé publique et la clé privée. Une fois que le message est codé, il faut avoir accès à la clé privée, laquelle n'est pas envoyée, pour pouvoir décoder le message. C'est ce sur quoi reposent les méthodes de codages actuelles les plus puissantes.

Concrètement, la meilleure protection contre un ordinateur quantique, pour des données qui ont été cryptées selon les modèles symétriques ou asymétriques, c'est de les crypter à nouveau, de façon à ce qu'elles répondent au modèle quantique. Ce que nous pensions être des protections fiables – et qui le sont dans le cadre des ordinateurs actuels – sont tout simplement mises en échec face à la capacité de calcul ô combien supérieure d'un ordinateur quantique. Elles ne sont tout simplement plus fiables. Le problème étant que ces données sont très nombreuses et que nous ne penserons probablement pas à toutes les crypter de nouveau.

Cela soulève de nombreuses questions intéressantes, notamment celle des crypto-monnaies comme le Bitcoin. Ces crypto-monnaies reposent sur les techniques de cryptages. Elles sont liées à la confiance, elle-même liée à ces techniques de cryptage, qui garantit l'absence de nécessité d'une autorité référente pour la monnaie : tout le monde peut observer les choses. Une capacité de calcul beaucoup plus élevée, comme cela pourrait être le cas avec un ordinateur quantique, remettrait en cause les principes de cryptages sur lesquels reposent ces monnaies. De là à dire que cela signerait l'arrêt de mort du Bitcoin, ce n'est pas impossible. La question est ouverte.

Quelles sont les autres applications éventuelles de l'ordinateur quantique ? Quels sont les champs des possibles qu'il pourrait ouvrir ?

L'ordinateur quantique est en mesure de rendre des services considérables. L'intelligence artificielle dépend en grande partie de la puissance de calcul. Les techniques d'apprentissage des machines ont fait des progrès considérables grâce à l'augmentation des capacités des processeurs. Si cela continue, nous devrions pouvoir être en mesure de traiter plus encore de données. Cela pourrait servir à mettre en place de la reconnaissance des formes, de la vision, de la reconnaissance de la parole ; où pour traiter des données scientifiques, biologiques par exemple. Cela contribuerait à l'avancée des connaissances de manière tout à fait considérable.

Tous les domaines qui nécessitent d'importantes ressources de calculs pourraient profiter de l'ordinateur quantique. Qu'il s'agisse de l'informatique (reconnaissance des formes, traitement de quantités massives de données), des domaines scientifiques… tous pourraient y trouver un intérêt. Avec des ordinateurs quantiques, nous serions en mesure d'explorer l'ensemble des données génomiques. Il serait possible de faire de la simulation relative au climat, de comprendre certains modèles de la nature… C'est pour toutes ces raisons que ces calculateurs pourraient représenter une avancée considérable.

Le développement de la loi de Moore devrait se poursuivre avec l'ordinateur quantique. Ce n'est pas du tout certain : il est possible que l'ordinateur quantique n'arrive pas à temps et que cette loi se poursuive infiniment, puisqu'il ne s'agit que d'une simple hypothèse de travail. Cela ne signifie pas pour autant qu'à l'arrivée de l'ordinateur quantique, les machines seront devenues plus intelligentes que les hommes. Quand bien même les capacités de calculs sont plus considérables, que cela change énormément de choses dans la vie de tous les jours, jusqu'à la compréhension de la nature, cela ne signifie pas que les machines seront plus intelligentes. Tout juste joueraient-elles un rôle différent dans l'organisation de la société. Cela induirait des bouleversements considérables. Mais les machines qui se substituent à l'homme demeurent une illusion.

Au vu de l'intérêt que génère l'ordinateur quantique, peut-on estimer son arrivée proche ?

Les informations que j'aies, recueillies auprès de physiciens, laissent entendre que nous en sommes encore loin. Cela étant, on ne sait jamais : en matière de technologie, il existe des ruptures. Cependant, il se peut aussi que cela soit finalement une déception : c'est un domaine très complexe. Dans tous les cas, il est évident que l'ordinateur quantique n'arrivera pas d'ici 3 ou 4 ans. Passée

cette estimation, il devient peu prudent de s'avancer. Cependant, il est clair que nous n'y sommes pas encore.