POINT FORT

Les promesses de la cryptographie quantique

Face aux besoins accrus en matière de protection des données et à l'apparition prochaine des ordinateurs quantiques, de nouvelles applications de cryptage, très prisées, voient le jour.

LEILA UEBERSCHLAG

Dans un monde où la collecte de données personnelles est toujours plus importante, les questions liées à leur protection animent de vifs débats. Les récents développements de la cryptographie quantique ont permis de mettre au point des applications de cryptage visant à protéger les informations sensibles sur le long terme. Prometteur, le secteur est en plein boom et cette technologie pourrait devenir incontournable dans les années à venir. Un engouement renforcé par la haute probabilité de l'apparition d'ordinateurs quantiques (à la force de calcul décuplée et qui menacent les méthodes de chiffrement traditionnelles) dans les décennies à venir.

ID QUANTIQUE WINTERSCHOOL. *De gauche à droite: Nicolas Gisin, Artur Ekert, Gilles Brassard, Charles Bennett et Grégoire Ribordy.*

La Suisse est très bien positionnée

Dans le domaine de la cryptographie quantique, le leader mondial est la société genevoise ID Quantique. Pépite issue des laboratoires de physique appliquée de l'Université de Genève, elle a été fondée en 2001. L'entreprise, qui connaît une croissance annuelle de 30% et emploie une soixantaine de collaborateurs sur son site à Carouge (*lire L'Agefi du 15 décembre 2017*), a récemment ouvert une coentreprise en Chine. Elle organise, cette semaine aux Diablerets (Vaud), la dixième édition de sa «Winter-School». Un rendez-vous incontournable pour en apprendre davantage sur les dernières avancées en matière de technologies quantiques. «Notre but est de participer à la création d'un écosystème et de soutenir le développement de ce marché», confie Grégoire Ribordy, cofondateur et CEO d'ID Quantique. «Cet événement est un moyen de multiplier notre force de frappe et de renforcer les liens avec nos partenaires.» Les pères de la cryptographie quantique, Charles Bennett, Gilles Brassard et Artur Ekert, font notamment partie des invités cette année (*lire encadré ci-dessous*).

Un marché qui vaudra 2 milliards en 2021

ID Quantique compte désormais plus d'une centaine de clients pour la partie sécurité, qui représente 50% de ses activités – l'autre moitié étant le développement de capteurs quantiques. «Au niveau global, le marché est de l'ordre de 50 à 100 millions, avec une très forte croissance. Il devrait atteindre 2 milliards en 2021», affirme Grégoire Ribordy. «J'estime à un millier le nombre d'équipements de cryptographie quantique, dont le prix s'élève aujourd'hui à environ 100.000 francs, vendus dans le monde l'an dernier.» Les concurrents de l'entreprise genevoise se comptent, pour le moment, sur les doigts de la main. «Nous avons deux concurrents sérieux qui sont Chinois», ajoute le CEO. Et ce n'est pas un hasard. La Chine est devenue un acteur majeur dans le développement de la cryptographie quantique, qui est l'un des cinq axes du 13e plan quinquennal de Pékin (définis comme étant d'importance stratégique cruciale pour la nation), et investit massivement pour le développement de cette technologie.

Des communications hautement sécurisées

De manière générale, le marché devient de plus en plus mûr. «Le secteur des technologies quantiques reçoit actuellement beaucoup de soutien, en Europe également, avec de grands projets de recherche qui sont lancés. Démystifié, le quantique devient mainstream», ajoute-t-il. «Cela nous a permis d'élargir la base de nos clients, au-delà des early adopters.» Selon lui, de grands groupes actifs dans les télécommunications – à l'instar de Toshiba ou du Huawei – commencent aussi à adopter des solutions de cryptographie quantique, mais attendent que le marché ait atteint une taille suffisante pour le pénétrer. Une des spécialités d'ID Quantique, dans les applications qu'elle propose, est d'utiliser les propriétés quantiques des photons pour distribuer des clés de cryptage (distribution quantique de clés ou quantum key distribution) afin de garantir que personne ne puisse intercepter la clé entre l'émetteur et le récepteur de l'information ainsi transmise. Contrairement aux transmissions classiques d'information (qui peuvent être interceptées sans modification de la teneur du message, donc sans que personne ne puisse s'en rendre compte), dans le cas de la cryptographie quantique, si une personne intercepte la communication, le message est alors automatiquement modifié. Ce qui rend donc l'observation indésirable facilement détectable.

Les produits mis au point par ID Quantique sont utilisés par des gouvernements, pour sécuriser les communications dans des réseaux métropolitains, mais également par diverses entreprises actives dans la finance ou toute autre industrie sensible où la propriété intellectuelle est critique; et pour qui la confidentialité des données doit être préservée sur plusieurs décennies.■

L'ordinateur quantique, c'est pour quand?

Il y a une dizaine d'années, les ordinateurs quantiques relevaient davantage de la science-fiction que d'une réalité à laquelle l'humanité devrait bientôt faire face. Aujourd'hui, si les experts peinent à se mettre d'accord quant à la date exacte de leur apparition, un consensus existe néanmoins dans la branche. Ces machines, qui fascinent autant qu'elles effraient, vont bien voir le jour.

C'est quoi un ordinateur quantique?

Ces ordinateurs utilisent les propriétés quantiques de la matière (comme la superposition et l'intrication) pour effectuer des opérations sur des données; à la différence d'un ordinateur classique basé sur des transitors qui travaille sur des données binaires (0 ou 1), l'ordinateur quantique – aussi appelé calculateur quantique – travaille sur des qubits dont l'état quantique peut posséder plusieurs valeurs. Sa force de calcul est démultipliée, ce qui le rend beaucoup plus puissant que les ordinateurs existants. Si l'entreprise canadienne D-Wave se targue d'avoir développé un tel ordinateur, de nombreux spécialistes remettent en question le caractère quantique de ces machines. Selon les experts, la démarche de D-Wave s'inscrit dans le développement d'une telle technologie, mais pour le moment aucune machine n'a encore fait l'unanimité dans la profession.

Pour Michele Mosca, le cofondateur de «The Institute of Quantum Computing» de l'Université de Waterloo au Canada et CEO de la société EvolutionQ, les ordinateurs quantiques devraient faire leur apparition d'ici 10 à 15 ans (avec 50% de probabilité). «La technologie quantique est déjà présente et utilisée pour de nombreuses applications. Ce n'est plus qu'une question de temps avant qu'un tel ordinateur fasse son apparition», assure ce spécialiste de la gestion des risques liés aux technologies quantiques.

MICHELE MOSCA. *Expert des risques liés au quantique.*

Une vulnérabilité sans précédent

Si les promesses d'une telle machine sont nombreuses, le calculateur quantique représente aussi une sérieuse menace en matière de cybersécurité. «S'ils faisaient leur apparition aujourd'hui, internet et tous les systèmes de communication ou de paiements s'effondreraient. Ce serait une catastrophe sans précédent», prévient-il. Les techniques de chiffrement traditionnelles, qui sont utilisées dans pratiquement tous les ordinateurs ou les smartphones ne résisteront pas à une telle puissance de calcul. «Nous devons entamer une phase de transition sans attendre, car cela va prendre beaucoup de temps», assure-t-il. «Malheureusement, en tant que société nous ignorions souvent les risques jusqu'à ce que les dégâts soient tellement importants que nous soyons dans l'obligation de réagir», note-t-il avant d'ajouter: «Un tel paradigme est particulièrement inquiétant dans le cyber monde. Les technologies modernes ont une portée mondiale à très faible coût. Dans un tel contexte, notre vulnérabilité est beaucoup plus systémique et profonde qu'elle ne l'a jamais été.»

Vers une combinaison des méthodes

La cryptographie, telle qu'on la connaît aujourd'hui, ne résistera pas à l'ordinateur quantique. «Il faut développer de nouvelles méthodes, et la cryptographie quantique en est une», nous apprend Grégoire Ribordy. L'autre méthode est le développement d'une cryptographie appelée «post-quantique», qui revient à complexifier la cryptographie traditionnelle (en modifiant les problèmes mathématiques sur lesquels cette dernière se base). Selon le CEO d'ID Quantique, la cryptographie quantique ne va pas être amenée à remplacer la cryptographie traditionnelle à terme. Après l'évolution de cette dernière, les deux méthodes vont être utilisées conjointement. «Pour les informations qui devront être protégées sur de nombreuses années, l'utilisation d'un système physique de protection est appropriée.» Il rappelle néanmoins que si la cryptographie quantique garantit un très haut niveau de sécurité, elle possède également des contraintes – la technologie s'utilise sur des fibres optiques principalement, ce qui n'est évidemment pas pratique pour un smartphone par exemple – d'où l'intérêt de la combiner avec les algorithmes « post-quantiques». – (LU)

De grands bouleversements sont attendus

«Les fondations de la physique quantique ont été posées il y a près d'un siècle», confie Artur Ekert, un des pères de la cryptographie quantique. «Ce n'est cependant seulement maintenant que nous avons une technologie qui peut contrôler les phénomènes quantiques avec une grande précision», note-t-il. «Et nous savons que cela a déjà - et va continuer à - avoir un impact dans des domaines tels que le calcul, les capteurs ou encore la communication.»

L'aube d'un nouveau monde

L'inventeur du protocole E91, basé sur l'intrication des photons, ajoute que dans 20 ou 30 ans, il y aura des applications dont il ne peut pas parler aujourd'hui, parce que personne n'y pense encore. De ce point de vue, il est, selon lui, difficile de dire quel sera exactement l'impact de la technologie quantique dans le futur. «Nous pouvons néanmoins spéculer», explique-t-il. «Un des domaines qui va certainement prendre de l'ampleur est celui de la cryptographie quantique, où des phénomènes quantiques sont utilisés pour une communication sécurisée. C'est un secteur très intéressant qui est en pleine expansion.»

Il faut garder la tête froide

Il met cependant en garde contre un engouement qui pourrait être excessif, notamment autour de l'ordinateur quantique. «Tout le monde pense qu'ils sont au coin de la rue, mais ce n'est certainement pas encore le cas», rétorque-t-il. «Ils ne vont pas arriver avant au moins cinq ans et il est difficile de fixer une date», ajoute-t-il.

ARTUR EKERT. *Un des pères de la cryptographie quantique.*

«C'est intéressant de relever que, dans le milieu des affaires, ces considérations scientifiques peuvent être mises – entièrement ou partiellement – de côté. Si tout le monde commence à croire qu'un tel ordinateur sera construit demain, même si c'est irrationnel

ON NE SAIT PAS EXACTEMENT QUEL SERA L'IMPACT DES TECHNOLOGIES QUANTIQUES.

et même si ça va à l'inverse de ce que dit la science, les investisseurs vont alors se mettre à injecter massivement de l'argent sur la base d'une simple croyance.»

Une révolution similaire à l'invention de l'électricité

Il souligne néanmoins le caractère disruptif des technologies quantique. «Avant l'invention de l'électricité, ou juste à ses débuts, il était probablement impossible d'imaginer les applications que nous connaissons aujourd'hui. Une révolution de même envergure, liée aux technologies quantiques, est en marche» prévoit-il. «C'est par curiosité que j'ai commencé mes recherches au début des années 90, et, à l'époque, je n'ai pas imaginé à un seul moment qu'elles pourraient donner lieu à des applications pratiques. Plus de 20 ans après, c'est une grande surprise. J'aime l'idée que ce que je pensais être une idée folle, une idée qui ne pourrait jamais être implémentée, l'est devenue.»

Autre pionner de la cryptographique quantique, le physicien Charles Bennett (père du protocole BB84 avec Gilles Brassard) va dans le même sens concernant la forte hype autour du calculateur quantique. «Il y a, à l'heure actuelle, un grand enthousiasme autour de ce que l'ordinateur quantique pourrait être en mesure de faire. Et ceci, particulièrement dans le monde des affaires», commente-t-il. «Nous verrons, d'ici cinq ou dix ans si la technologie est assez mature.» Il fait une analogie avec l'intelligence artificielle (IA).

«Un bon exemple est le boom de l'IA et du deep-learning. Quand j'étais enfant, les ordinateurs, qui étaient aussi qualifiés de cerveaux électroniques, suscitaient de nombreux espoirs, dans le domaine de la traduction notamment. Or, il s'est avéré que c'était un problème très difficile à résoudre», se rappelle-t-il. «Tombée dans l'oubli après les sixties, l'IA revient aujourd'hui en force, car les développements des technologies permettent désormais de le faire.»

Selon lui, la recherche scientifique fondamentale a des conséquences énormes, mais tout le monde s'attend à ce qu'elles se produisent plus tôt que ce qu'elles se produisent réellement. «Nous devons rester patients.» – (LU)