Le physicien Nicolas Pulido devant le prototype d'un ordinateur quantique à Brunswick, en Allemagne.

PERSPECTIVES ET RISQUES de l'informatique quantique

Les ordinateurs quantiques pourraient déchiffrer la cryptographie qui sous-tend la stabilité financière

José Deodoro, Michael Gorbanyov, Majid Malaika et Tahsin Saadi Sedik

Dans la Grèce antique, les soldats envoyaient des dépêches secrètes en enroulant une bande de parchemin autour d'un bâton régulier et en écrivant dessus. Leurs messages ne pouvaient être déchiffrés que par une personne disposant d'un bâton de même diamètre. Il s'agit de l'un des premiers exemples de cryptographie. Les secrets d'aujourd'hui, par exemple la communication par Internet, les services bancaires en ligne et le commerce électronique, sont protégés des regards indiscrets par de puissants algorithmes informatiques. Cependant, ces codes cryptographiques jusqu'ici impénétrables pourraient bientôt appartenir au passé.

Les ordinateurs quantiques peuvent atteindre un niveau d'optimisation qui déchiffrerait bon nombre des clés de chiffrement actuelles en moins de temps qu'il n'en faut pour les générer en utilisant des ordinateurs numériques classiques. Les établissements financiers devraient protéger leurs systèmes de cybersécurité et les adapter aux évolutions futures sans tarder, faute de quoi ils mettront en péril la stabilité financière.

Une révolution quantique

L'informatique quantique est l'utilisation de phénomènes quantiques comme la *superposition* et l'*intrication* pour effectuer des calculs. L'unité de base d'un ordinateur quantique est le bit quantique (ou *qubit* en abrégé). Il est généralement créé par les propriétés quantiques des particules subatomiques, comme le spin des électrons ou la polarisation

Grâce à leurs capacités de traitement, les ordinateurs quantiques sont susceptibles de surpasser massivement les ordinateurs numériques qui obéissent aux lois classiques de la physique.

des photons. Alors que chaque bit binaire utilisé dans les ordinateurs numériques actuels représente une valeur de zéro ou un, les qubits représentent le zéro et le un (ou une combinaison des deux) simultanément. Ce phénomène est désigné sous le nom de superposition. L'intrication quantique est une liaison particulière entre des paires ou des groupes d'éléments quantiques. Le changement d'état d'un élément influe instantanément sur les autres éléments enchevêtrés, quelle que soit la distance qui les sépare.

Une hausse du nombre de qubits se traduit par une augmentation exponentielle de la vitesse de traitement des calculs. Deux bits binaires classiques sont nécessaires pour égaler la puissance d'un seul qubit ; il faut quatre bits pour faire jeu égal avec deux qubits ; huit bits sont requis pour équivaloir à trois qubits, etc. Il faudrait environ 18 billiards de bits de mémoire traditionnelle pour modéliser un ordinateur quantique avec seulement 54 qubits. Un ordinateur quantique de 100 qubits nécessiterait plus de bits qu'il n'y a d'atomes sur notre planète. Et un ordinateur de 280 qubits demanderait plus de bits qu'il n'y a d'atomes dans l'univers connu.

Grâce à leurs capacités de traitement, les ordinateurs quantiques sont susceptibles de surpasser les ordinateurs numériques qui obéissent aux lois classiques de la physique. William Phillips, physicien lauréat du prix Nobel, a comparé les progrès entre les technologies actuelles et les ordinateurs quantiques au saut technologique entre le boulier et l'ordinateur numérique lui-même. Jusqu'à une date récente, cet *avantage quantique* ou cette *suprématie quantique* était simplement une théorie. Toutefois, en 2019, Google a utilisé un ordinateur quantique pour effectuer une tâche de calcul particulière en seulement 200 secondes. Selon le groupe, il aurait fallu 10 000 ans au supercalculateur numérique le plus puissant à l'époque pour réaliser la même tâche.

Les perspectives

Effectuer des tâches informatiques complexes s'apparente à trouver la sortie d'un labyrinthe. Un ordinateur classique tenterait de s'évader en suivant chaque chemin l'un après l'autre jusqu'à atteindre la sortie. En revanche, la superposition permet à un ordinateur quantique d'essayer tous les chemins simultanément, ce qui réduit sensiblement le délai nécessaire pour trouver une solution.

En résolvant les problèmes plus précisément et rapidement que les ordinateurs numériques, les ordinateurs quantiques ont la possibilité d'accélérer les découvertes et innovations scientifiques, de révolutionner la modélisation et les simulations des marchés financiers, et de renforcer l'apprentissage automatique et l'intelligence artificielle. Ils pourraient servir à modéliser les particules subatomiques, les interactions moléculaires et les réactions chimiques. Cela pourrait révolutionner le génie chimique et la science des matériaux, et permettre la conception de nouveaux matériaux, par exemple des batteries à électrolyte solide. Les ordinateurs quantiques pourraient aussi nous aider à comprendre les changements climatiques.

Les ordinateurs quantiques pourraient également transformer le système financier. Ils pourraient réaliser des simulations de Monte Carlo, qui permettent de prédire le comportement des marchés à travers des simulations de prix et de risques, plus précises et pratiquement en temps réel. Il ne serait pas nécessaire de simplifier ces modèles à l'aide d'hypothèses irréalistes. Les ordinateurs quantiques pourraient aussi accomplir des tâches d'optimisation, par exemple répartir le capital, décider des investissements de portefeuille ou gérer les espèces dans les réseaux de guichets automatiques de banque (GAB), en beaucoup moins de temps que les ordinateurs numériques. Les ordinateurs quantiques pourraient par ailleurs accélérer la formation aux algorithmes d'apprentissage automatique. Les délais d'exécution de ces tâches par les ordinateurs numériques s'allongent de manière exponentielle chaque fois qu'une composante est ajoutée. Rien de tel avec les ordinateurs quantiques.

Et les risques

Des risques existent néanmoins. La puissance de calcul de ces machines quantiques imposantes pourrait menacer la cryptographie moderne. Cela a de profondes répercussions pour la stabilité financière et la confidentialité. Actuellement, la cryptographie repose sur trois principaux types d'algorithmes : les *clés symétriques*, les *clés asymétriques* (aussi appelées *clés publiques*) et les *fonctions de hachage*. S'agissant des clés symétriques, la même clé est utilisée pour chiffrer et décrypter un message. La cryptographie asymétrique utilise une paire de clés liées entre elles (une privée et l'autre publique). Un message chiffré par une clé peut être décrypté uniquement par l'autre clé de la paire. Ces algorithmes sont largement utilisés pour l'authentification numérique, les signatures numériques et la sécurité des données. Les fonctions de hachage transforment des entrées numériques en un ensemble unique d'octets de taille fixe. Elles servent à stocker les mots de passe de manière sécurisée et font office de support pour les identités numériques.

Pour l'essentiel, ces algorithmes de chiffrement sont parvenus à sauvegarder des données. Même les supercalculateurs numériques et les techniques de crypto-analyse

PHOTO: GETTY IMAGES/PICTURE ALLIANCE/JULIAN STRATENSCHULTE

Les établissements financiers doivent prendre des mesures immédiates pour se préparer à une transition cryptographique.

les plus perfectionnés d'aujourd'hui ne peuvent pas les déchiffrer suffisamment vite. En revanche, les ordinateurs quantiques pourront résoudre des problèmes mathématiques ardus bien plus rapidement que les supercalculateurs numériques. De fait, la cryptographie asymétrique deviendra obsolète et les autres clés et hachages cryptographiques seront inadaptés. En théorie, un ordinateur quantique qui tourne à plein régime pourrait déchiffrer une clé asymétrique en quelques minutes. Les clés publiques sont particulièrement vulnérables, car elles reposent pour la plupart sur le problème de la factorisation : les ordinateurs numériques peinent à retrouver deux nombres premiers à partir de leur produit. Les ordinateurs quantiques peuvent quant à eux le faire facilement.

Les clés asymétriques sont largement utilisées pour sécuriser les communications sur Internet. Des attaques réussies contre ces algorithmes compromettraient les connexions utilisées par le système financier, dont les services bancaires mobiles, le commerce électronique, les transactions de paiement, les retraits d'espèces aux GAB et les communications via un réseau privé virtuel (RPV), pour n'en citer que quelques-unes. Les applications vulnérables qui reposent sur la cryptographie par clé publique comprennent aussi des actifs numériques très prisés comme Bitcoin et Ethereum, ainsi que des applications Web protégées par mot de passe. Le plus connu de ces protocoles, à savoir HTTPS, est utilisé par 97 des 100 premiers sites Internet au monde.

Pour certaines applications, il est peut-être déjà trop tard. Toute information supposée sûre aujourd'hui pourrait être interceptée et stockée pour être déchiffrée ultérieurement, une fois que des ordinateurs quantiques suffisamment puissants auront été mis au point. En réalité, pratiquement tous les messages cryptés de nature personnelle ou financière envoyés et stockés aujourd'hui pourraient être déchiffrés rétroactivement par un puissant ordinateur quantique. La plupart des établissements financiers et des autorités de contrôle n'a pas encore conscience de ces risques inédits.

La course contre la machine

La course pour élaborer de nouveaux algorithmes et normes de chiffrement post-quantiques a déjà débuté. Aux États-Unis, le National Institute of Standards and Technology organise un concours pour mettre au point des algorithmes de chiffrement post-quantiques. Il espère annoncer un gagnant d'ici à 2024. L'Institut européen des normes de télécommunications prend lui aussi l'initiative. Ces tentatives inspirent les activités d'autres organismes de normalisation. Toutefois, compte tenu des risques rétroactifs, les établissements financiers disposent d'un créneau restreint pour appliquer les nouvelles normes.

Les établissements financiers doivent prendre des mesures immédiates pour se préparer à une transition cryptographique. Ils devraient commencer par évaluer les risques rétroactifs et futurs liés aux ordinateurs quantiques, y compris ceux qui découlent des informations qui ont peut-être déjà été interceptées et pourraient être exploitées des années plus tard. Les établissements financiers devraient ensuite concevoir des projets de migration de la cryptographie actuelle vers des algorithmes post-quantiques. Cela suppose de procéder à un inventaire de la cryptographie par clé publique utilisée par eux-mêmes, mais aussi de celle employée par tous les fournisseurs tiers. Il faudra abandonner les algorithmes vulnérables au profit de la cryptographie post-quantique. Les établissements financiers devraient aussi renforcer l'agilité cryptographique, afin que les algorithmes puissent être améliorés de manière fluide. Les exemples passés de remplacements d'algorithmes, même s'ils sont beaucoup plus simples que la transition vers des normes post-quantiques, montrent qu'ils peuvent causer des perturbations extrêmes. Il faut souvent des années, voire des décennie, pour qu'ils soient menés à bien.

Le FMI a un rôle important à jouer pour sensibiliser ses membres aux risques que les ordinateurs quantiques font peser sur la stabilité financière et pour promouvoir les normes et pratiques post-quantiques. Le FMI devrait encourager les pays membres à collaborer étroitement pour mettre au point des normes de chiffrement post-quantiques, de façon à garantir l'interopérabilité et à adopter des projets de migration du chiffrement pour leur secteur financier.

Les ordinateurs quantiques actuels sont très sensibles. La moindre perturbation dans leur environnement, par exemple la chaleur, la lumière ou une vibration, fait sortir les qubits de leur état quantique et les transforme en bits classiques. Cela donne lieu à des erreurs de calcul. Pour autant, les machines qui calculent en commettant moins d'erreurs et sont capables de déchiffrer des codes ne sont pas très loin. Les établissements financiers devraient prendre conscience des risques et sécuriser leurs systèmes avant qu'il ne soit trop tard. Après tout, l'histoire regorge de récits édifiants de codes en principe indéchiffrables, qui sont décryptés par une nouvelle technologie. FD

JOSÉ DEODORO est le propriétaire de la plateforme de recueil de données et **MAJID MALAIKA** est expert principal en transformation numérique et en risques de cybersécurité au département des technologies de l'information du FMI. **MICHAEL GORBANYOV** est économiste principal au département de la stratégie, des politiques et de l'évaluation du FMI et **TAHSIN SAADI SEDIK** est chef de division adjoint au département Asie et Pacifique du FMI.

Cet article s'inspire du document de travail du FMI 21/71 intitulé « Quantum Computing and the Financial System: Spooky Action at a Distance? ».