Faire et défaire la sécurité des données avec des machines quantiques

Les caractéristiques de l'univers quantique ne sont pas très intuitives lorsqu'elles sont basées sur les observations de la physique de tous les jours, ce qui peut expliquer pourquoi même le physicien théorique Albert Einstein a trouvé les phénomènes « effrayants ».[1] Bien que la discipline soit assez complexe, il est important que les professionnels de l'informatique, en particulier les experts en sécurité informatique, se familiarisent avec les notions fondamentales de la cryptographie quantique en tant que moyen émergent de renforcer la confidentialité et la sécurité des données dans le monde d'aujourd'hui.

Qu'est-ce que la mécanique quantique ?

Richard Feynman, physicien lauréat du prix Nobel, a dit un jour « Si vous pensez comprendre la mécanique quantique, vous ne la comprenez pas ».[2]

La mécanique quantique est une branche de la physique basée sur la façon dont des éléments extrêmement petits, tels que les molécules, les atomes, les électrons et les photons, se comportent dans l'univers. Les particules quantiques présentent deux caractéristiques principales qu'il est utile de connaître : la superposition et l'intrication.

Superposition

Les particules quantiques peuvent se trouver dans différentes positions (ou états) en même temps et ne s'effondrent en une seule position que lorsqu'elles sont observées. Ce phénomène est connu sous le nom de superposition. On parle de superposition lorsqu'une particule se trouve dans les positions A et B en même temps, comme une pièce de monnaie lancée en l'air. La particule ne s'effondre en pile ou face que lorsqu'elle est mesurée (ou, dans le cas de l'analogie, attrapée), et le résultat dépend de probabilités aléatoires (souvent 50:50). Autre exemple, les cours de sciences élémentaires enseignent aux enfants comment les électrons tournent autour du noyau des atomes, tout comme les planètes tournent autour du soleil. Les électrons

DALIA KHADER | PH.D., CISSP, GSEC

Elle est Directrice de la sécurité de l'information (CISO) pour la division internationale de Swiss Life et membre de WomenCyberForce. Elle a plus de 15 ans d'expérience dans le domaine de la cybersécurité, notamment en travaillant dans le milieu universitaire, où elle a effectué des recherches approfondies sur la cryptographie moderne, en travaillant comme associée de recherche à l'Université du Luxembourg (Kirchberg, Luxembourg) et en travaillant comme architecte de sécurité pour un fournisseur de services de télécommunications. Khader a remporté le prix CISO de l'année 2021, Luxembourg. Ses travaux ont été publiés par le World Economic Forum et Usenix et lors de conférences RSA. Son objectif est de rendre les concepts complexes de cybersécurité accessibles à tous. Elle peut être jointe à l'adresse *https://lu.linkedin.com/in/dalia-khader-2b13b6a.*

HUSNA SIDDIQI

Elle est responsable de la gestion de l'assurance technologique dans une organisation mondiale. Elle a plus de 16 ans d'expérience dans la sécurité de l'information, la protection des données, le risque informatique et la gestion de programmes de transformation dans plusieurs secteurs, notamment le pétrole et le gaz, l'énergie et les services publics, les biens de consommation, la fabrication et les services professionnels. Avant de devenir consultant, Mme Siddiqi était professeur d'informatique et ingénieur logiciel. Elle préside le conseil consultatif indépendant du Centre britannique de recherche et d'innovation pour une intelligence artificielle responsable et transparente (ART-AI) à l'université de Bath (Angleterre). Elle contribue au Forum économique mondial et a publié des articles dans plusieurs forums réputés. Elle s'efforce de sensibiliser des publics divers à la sécurité et à la protection de la vie privée à l'aide d'exemples pertinents et participe activement à des initiatives mondiales visant à promouvoir la diversité et l'inclusion et à lutter contre les préjugés inconscients. Elle peut être jointe à l'adresse *https://uk.linkedin.com/in/husna-siddiqi-5466158.*

tournent aussi (vers le haut ou vers le bas selon l'orientation de la rotation), tout comme la Terre tourne sur son propre axe. En appliquant le principe de superposition, les électrons peuvent tourner vers le haut et vers le bas en même temps jusqu'à ce qu'ils soient mesurés. Une fois mesuré, un électron va s'effondrer en une particule dans l'une ou l'autre direction de rotation.

Enchevêtrement

Les particules quantiques peuvent être enchevêtrées de telle manière que l'effondrement de l'une a un impact sur l'autre, même si elles se déplacent extrêmement loin l'une de l'autre.

Les particules peuvent être imaginées comme deux vagues qui se croisent l'une l'autre. Alors qu'elles s'éloignent, une ficelle invisible les lie à jamais, de sorte que le déplacement de l'une aura toujours un impact sur l'autre. Des particules quantiques enchevêtrées pourraient être éloignées de plusieurs années-lumière les unes des autres mais auraient quand même un impact les unes sur les autres. Si un électron est observé et s'effondre pour tourner vers le haut, l'autre s'effondrerait immédiatement pour tourner vers le bas.

Qu'est-ce que l'informatique quantique ?

Avant de décrire les ordinateurs quantiques, il est utile de revoir les éléments de base des ordinateurs classiques/modernes.

> « Ils peuvent améliorer la sécurité des données mais peuvent aussi être utilisés pour briser la sécurité des ordinateurs classiques, à moins que les protocoles ne soient résistants aux quanta. »

Les ordinateurs classiques fonctionnent à l'électricité et, dans leur forme la plus simple, ils stockent des informations sur la base de deux états : le courant qui passe (c'est-à-dire l'allumage) ou le courant qui ne passe pas (c'est-à-dire l'arrêt). Ces états sont représentés mathématiquement sous la forme de chiffres binaires (bits). Un bit peut se trouver dans l'un des deux états possibles : 1 ou 0. S'il y a deux bits, il y a quatre combinaisons de bits possibles (c'est-à-dire 00, 01, 10, 11). Un octet (8 bits) peut avoir 256 combinaisons de 1 ou de 0. Les combinaisons de bits possibles augmentent de manière exponentielle avec le nombre d'octets.

Tous les problèmes mathématiques, qu'il s'agisse de la simple addition de deux nombres ou de calculs astronomiques complexes, peuvent finalement être décomposés par les ordinateurs classiques en séquences de bits (0 et 1). La capacité de mémoire des ordinateurs, qui est basée sur le nombre de bits, a un impact sur la vitesse de calcul pour résoudre les problèmes.

Au fil du temps, la taille des mémoires a augmenté de façon exponentielle en raison des progrès de la technologie. L'époque où les octets, les kilo-octets ou les méga-octets étaient évoqués dans les conversations est révolue. Aujourd'hui, même lorsqu'on choisit un bus série universel (USB), la discussion tourne autour des gigaoctets ou des téraoctets. Ce volume extrêmement élevé de données non structurées peut mettre à rude épreuve les processeurs des ordinateurs classiques, qui ont du mal à suivre en termes de vitesse. Entrer dans les ordinateurs quantiques.

L'équivalent des bits dans les ordinateurs quantiques est appelé bits quantiques (qubits). Cependant, les ordinateurs quantiques sont différents des ordinateurs classiques. Contrairement aux bits classiques, un bit quantique peut se trouver dans les deux états 1 et 0 en même temps grâce à la superposition. Lorsque les électrons sont utilisés pour l'informatique quantique, chaque qubit peut effectuer un spin up et un spin down au même moment.

La possibilité même de se trouver dans plusieurs états en même temps augmente radicalement la vitesse de résolution des problèmes. Imaginez un groupe d'amis essayant de trouver un bijou dans un labyrinthe complexe dans le temps le plus court possible. La chose la plus logique à faire serait de se séparer et de prendre des routes différentes pour augmenter la probabilité de le trouver plus tôt. Comme indiqué, il peut y avoir 256 combinaisons de bits dans un octet. Cependant, un octet de qubits peut se trouver dans toutes les 256 positions en même temps. Imaginez la rapidité avec laquelle un tel ordinateur peut trouver la meilleure route vers le trésor, par rapport à l'ordinateur classique le plus rapide qui tente chaque route à la fois. Si deux des amis sont « enchevêtrés » de telle sorte que lorsque l'un trouve le trésor, l'autre cesse immédiatement de le chercher, cela pourrait permettre de gagner du temps et de l'énergie. Le fait que les particules quantiques telles que les électrons puissent être enchevêtrées de cette manière permet d'accélérer le temps de traitement et d'éliminer plus rapidement les résultats erronés.

L'informatique quantique et ses relations avec la cybersécurité

Les ordinateurs quantiques peuvent être utilisés comme outils et comme armes. Ils peuvent améliorer la sécurité des données mais peuvent également être utilisés pour briser la sécurité des ordinateurs classiques à moins que les protocoles ne soient résistants aux quanta.

La cryptographie (l'art et les mathématiques de l'écriture et de la résolution de codes) est la discipline clé sous-jacente aux techniques qui protègent les données. Le chiffrement s'apparente à placer des données dans une boîte fermée à clé ; il est facile de verrouiller la boîte mais l'objectif est de rendre son déverrouillage extrêmement difficile pour quiconque n'est pas en possession de la clé.

« Des applications plus complexes de la cryptographie quantique, notamment l'utilisation de particules quantiques pour générer le message réel, sont encore en cours de création. »

La cryptographie moderne repose sur des calculs qui ne peuvent pas être inversés en un temps raisonnable compte tenu de la puissance de calcul d'un ordinateur classique. L'un des algorithmes les plus utilisés aujourd'hui pour sécuriser les courriers électroniques et les transactions sur Internet - RSA (qui utilise 2048 bits) - nécessiterait 300 trillions d'années pour casser la sécurité en utilisant des ordinateurs classiques. Cependant, en utilisant des ordinateurs quantiques puissants et sans erreur, il pourrait être brisé en 10 secondes.

En fait, la menace quantique touche l'ensemble du monde numérique , de la navigation sur Internet au courrier électronique en passant par l'accès à distance des systèmes et la communication mobile. L'infrastructure de systèmes tels que l'infrastructure à clé publique (PKI), la sécurité de la couche de transport (TLS), les réseaux privés virtuels (VPN), les bibliothèques cryptographiques de base et les modules matériels sécurisés est basée sur des algorithmes tels que la factorisation, les courbes elliptiques et les logs discrets. Imaginez l'ampleur de l'effort nécessaire pour déployer de nouveaux algorithmes dans l'ensemble de l'écosystème et de la chaîne d'approvisionnement de l'Internet tel qu'il est connu aujourd'hui.

En 2016, le National Institute of Standards and Technology (NIST) américain a commencé à créer de nouvelles normes cryptographiques pour résister à l'informatique quantique. Les nouvelles normes devraient être publiées d'ici 2024.[3]

Même si les ordinateurs quantiques d'aujourd'hui ont un important travail de mise à l'échelle à faire, les experts en protection de l'information tentent de garder une longueur d'avance pour protéger les données en utilisant des méthodes comme celles-ci :

- **Cryptographie quantique -** S'appuie sur les propriétés de la physique quantique pour élaborer de nouveaux algorithmes de cryptographie .
- **Cryptographie résistante aux quanta -** Continue de s'appuyer sur les mathématiques ; cependant, le choix des mathématiques sous-jacentes est difficile à résoudre même avec une puissance de calcul et une capacité de mémoire élevées et, par conséquent, la cryptographie basée sur les mathématiques est incassable avec l'informatique quantique.

Cryptographie quantique

L'informatique quantique peut renforcer la sécurité et la confidentialité des données d'une manière qu'un ordinateur classique ne peut pas faire. Une application moderne de la cryptographie quantique est la distribution quantique des clés.

Dans le cadre de la cryptographie traditionnelle, une partie (Alice) envoie à une autre partie (Bob) la clé de la boîte verrouillée séparément dans un canal sécurisé, puis met la boîte verrouillée en évidence, sachant que seul Bob peut l'ouvrir avec la clé. Mais si une espionne rusée (Jane) parvient à intercepter la communication et à faire une copie de la clé, elle peut imiter la communication entre Alice et Bob.

Les chercheurs ont conçu un algorithme d'échange de clés, BB84, qui implique la transmission de qubits par des canaux quantiques utilisant des photons.[4] Les valeurs des photons et le filtre par lequel ils ont été polarisés sont générés au hasard par Alice, et à la réception des photons, Bob utilise ses propres filtres générés au hasard pour déterminer les valeurs. Comme les filtres sont alignés soit verticalement/ horizontalement, soit en diagonale (c'est-à-dire avec une rotation de +/- 45 degrés), un filtre mal adapté fournira aléatoirement un 1 ou un 0, tandis qu'un filtre adapté fournira la valeur exacte envoyée par Alice. Une fois la transmission terminée, Alice indique à Bob les filtres qu'elle a utilisés. Ils conviennent d'écarter les valeurs pour lesquelles leurs filtres ne correspondent pas (Bob n'est pas devin, il peut donc y en avoir plusieurs) et de conserver les valeurs restantes pour former une clé aléatoire forte.

Si Jane tente d'intercepter la communication, elle se fera attraper car les informations quantiques ne peuvent pas être copiées ou clonées. En raison des caractéristiques de la physique quantique, telles que le théorème de non-clonage (contrairement aux bits numériques, un état quantique ne peut être copié à l'identique)[5] et le principe d'incertitude de Heisenburg (il n'est pas possible de connaître à la fois la vitesse et la position d'un matériau quantique ; l'acte de mesurer l'une rend l'autre inconnue),[6] ses tentatives de mesurer les valeurs perturberont la communication et feront du bruit, ce qui incitera Alice et Bob à réaliser ce qui s'est passé, à interrompre l'échange de clés et à recommencer le processus. Ce n'est que lorsqu'ils pourront générer la clé sans aucun soupçon d'interception qu'Alice enverra le véritable message crypté par un canal classique que seul Bob pourra décrypter.

Un protocole de distribution de clés quantiques reposant sur les propriétés d'intrication des photons a été conçu. [7] Des applications plus complexes de la cryptographie quantique, y compris l'utilisation de particules quantiques pour générer le message réel, sont encore en cours de création.

Les défis de la cryptographie quantique

L'idée nouvelle de concevoir des systèmes cryptographiques basés sur l'informatique quantique pose de nombreux problèmes.

L'un d'eux est que l'infrastructure de communication du réseau actuel n'est pas compatible avec la communication quantique. La question de savoir comment transférer efficacement les états quantiques reste posée. Un autre problème est que la cryptographie quantique a encore de la marge pour se développer en termes de schémas cryptographiques sophistiqués. Entre-temps, la cryptographie traditionnelle (basée sur les mathématiques) s'est améliorée, et sa maturité relative a augmenté rapidement, faisant de la cryptographie à résistance quantique une solution plus réalisable pour résister aux attaques quantiques.

Cryptographie résistante aux quanta

La cryptographie moderne repose sur des problèmes mathématiques (par exemple, la factorisation des nombres entiers, les problèmes de logarithme discret, les problèmes de logarithme discret à courbe elliptique) qui peuvent être résolus, mais qui nécessitent une quantité massive de puissance de calcul lorsqu'on utilise des ordinateurs classiques, ce qui peut prendre des billions d'années. Ceux-ci peuvent encore être brisés en un temps raisonnable avec un ordinateur quantique parfait.

Cependant, il existe encore certains problèmes mathématiques pour lesquels une solution n'a pas encore été découverte ou qui peuvent être réduits aux pires scénarios au lieu d'une puissance de calcul spécifique. Par exemple, la factorisation est utilisée dans la cryptographie actuelle parce que sa résolution nécessite une meilleure puissance de calcul et une capacité de mémoire dans les ordinateurs classiques ; alors qu'un bon mot de passe à usage unique est cassable en essayant de deviner chaque permutation de ce mot de passe, le pire scénario est indépendant de la technologie. Des exemples plus concrets de cryptographie résistante aux quanta comprennent la cryptographie en treillis,[8] multivariée[9] et basée sur le hachage[10].

Les défis de la cryptographie résistante aux quanta

L'un des défis des algorithmes qui ont fait l'objet d'efforts de normalisation par le NIST est la réduction de l'efficacité due à des facteurs tels que la taille des clés, du texte chiffré et des signatures.

Un autre défi lié à l'utilisation de la cryptographie post-quantique est que la sécurité moderne repose essentiellement sur des algorithmes pré-quantiques et que le passage à la cryptographie post-quantique impliquerait une transformation à grande échelle et un coût d'adaptation élevé.

Prenons par exemple le modèle Open Systems Interconnection (OSI).[11] La plupart des protocoles et chacune des couches du modèle devraient être repensés pour prendre en compte les données en transit, comme la sécurité de la couche de transport (TLS), la sécurité du protocole Internet (IPsec), l'accès protégé Wi-Fi 2 (WPA2), les extensions de messagerie Internet sécurisées et polyvalentes (SMIME) et le protocole Secure Shell (SSH). Il faudrait également modifier les modules de sécurité matérielle et tous les systèmes qui assurent la sécurité des données au repos.

Quantum Today

Les ordinateurs quantiques actuels ne peuvent contenir qu'un petit nombre de qubits, et il est difficile de passer à l'échelle supérieure car des conditions environnementales très précises sont nécessaires pour que les particules restent dans les états de superposition ou intriqués souhaités (par exemple, une température extrêmement basse). De plus, le fait que l'information quantique ne puisse pas être copiée de la même manière que l'information numérique pose des obstacles supplémentaires à l'évolutivité.

Néanmoins, la capacité en qubits des ordinateurs quantiques a connu une augmentation remarquable au cours de ce millénaire, passant du processeur expérimental de Yale à 2 qubits en 2009[12] au processeur IBM à 127 qubits en 2021.[13] En ce qui concerne la transmission de photons pour la distribution de clés quantiques, la longueur des liaisons par fibre optique a été multipliée par dix au cours de la dernière décennie (des bobines de 200 km à la distribution par satellite de 1200 km).[14, 15]

> « Le fait que les informations quantiques ne puissent pas être copiées de la même manière que les informations numériques pose des obstacles supplémentaires à l'évolutivité. »

Il existe aujourd'hui de nombreux acteurs sur le marché de l'informatique quantique (par exemple, IonQ, PsiQuantum, D-wave), en plus des géants technologiques pionniers tels que Google,[16] IBM[17] et Intel,[18] qui sont dans la course pour construire un jour des ordinateurs quantiques utiles (à un million de qubits).

En termes de sécurité, la cryptographie résistante aux quanta étant orientée vers les mathématiques, elle donne au monde une plus grande chance de succès dans la préparation du jour où l'informatique quantique deviendra une réalité pratique. La conception de tels algorithmes est indépendante des progrès réalisés dans le domaine de l'informatique quantique. D'autre part, les éléments constitutifs de l'informatique quantique et de la cryptographie quantique reposent sur les mêmes principes physiques fondamentaux, ce qui rend le rythme des progrès comparables et les défis à relever pour assurer la sécurité entrelacés. En outre, tous les algorithmes qui ont fait l'objet de la troisième série d'efforts de normalisation du NIST en 2021 étaient axés sur les mathématiques et utilisaient des techniques de résistance quantique.[19]

Conclusion

Les développements dans le domaine quantique au cours du siècle dernier ont été phénoménaux : de la découverte de la nature étrange des particules quantiques à la visualisation d'un ordinateur capable de simuler l'environnement quantique, en passant par l'émergence d'ordinateurs quantiques très puissants (bien qu'à petite échelle), qui ont un immense potentiel pour faire ou défaire la cybersécurité. La prochaine décennie promet encore plus de développements passionnants de ce mariage de la physique et de l'informatique, et 2022 devrait être l'année des percées quantiques.[20]

Note des auteurs

Les opinions exprimées dans cet article ne reflètent pas celles des employeurs des auteurs.

Bibliographie

1 *MIT Technology Review, «* Einstein's 'Spooky at a Distance' Paradox Older Than Thought », *8 mars 2012, https://www.technologyreview.com/2012/03/08/20152/einsteins-spooky-action-at-a-distance-paradox-older-than-thought*

2 Gleick, J.; « Richard Feynman », *Encyclopedia Britannica,* 7 mai 2022, *https://www.britannica.com/ biography/Richard-Feynman*

3 US National Institute of Standards and Technology (NIST), « NIST Asks Public to Help Future-Proof Electronic Information », États-Unis, 20 décembre 2016, *https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information*

4 Bennett, C. H.; G. Brassard; « Quantum Cryptography: Public Key Distribution and Coin Tossing », *Theoretical Computer Science,* vol. 560, p.175-179

5 Wootters, W. K.; W. H. Zurek; « A Single Quantum Cannot Be Cloned », *Nature,* vol. 299, iss. 5886, 1982, p.802-803

6 Heisenberg, W.; *The Physical Principles of the Quantum Theory,* Dover Publications, États-Unis, 1949

7 Ekert, A. K.; « Quantum Cryptography Based on Bell's Theorem », *Physical Review Letters,* vol. 67, 5 août 1991

8 Ajtai, M.; « Generating Hard Instances of Lattice Problems », Actes du 28e symposium annuel de l'ACM sur la théorie de l'informatique juillet 1996, p. 99-108

9 Wolf, C.; B. Preneel; « Asymmetric Cryptography: Hidden Field Equations », *Congrès européen sur les méthodes computationnelles dans les sciences appliquées et l'ingénierie,* 2004

10 Preneel, B.; « Design Principles for Hash Functions Revisited, » Atelier sur le hachage cryptographique, National Institute of Standards and Technology, 2005, *https://csrc.nist.gov/CSRC/media/Events/ First-Cryptographic-Hash-Workshop/documents/ preneel_nist_v2.pdf*

11 Forcepoint, « The OSI Model Defined », *https://www.forcepoint.com/cyber-edu/ osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems,between%20different%20products%20and%20software*

12 Quantum Thought, « History of Quantum Computing: A Timeline », 29 juin 2020, *https://www.quthought.com/post/history-of-quantum-computing-a-timeline*

13 IBM, « IBM Unveils Breakthrough 127-Qubit Quantum Processor », 16 novembre 2021, *https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor*

14 Homeland Security News Wire, « Quantum Keys Sent Over 200-km Fiber-Optic Link », 5 juin 2007, *https://www.homelandsecuritynewswire.com/quantum-keys-sent-over-200-km-fiber-optic-link#:~:text=In%20an%20experiment%20conducted%20at%20a%20Stanford%20lab%2C,been%20sent%20over%20a%20record-setting%20200-kilometer%20fiber-optic%20link*

15 Yin, J.; Y. Cao; Y.-H. Li; *et al.;* « Satellite-Based Entanglement Distribution Over 1200 Kilometers », *Science,* vol. 356, iss. 6343, 16 juin 2017, p. 1140-1144, *https://www.science.org/doi/10.1126/science.aan3211*

16 Porter, J.; « Google Wants to Build a Useful Quantum Computer by 2029 », *The Verge,* 19 mai 2021, *https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits- quantum-transistor*

17 IBM, « The Quantum Decade, » *https://www.ibm.com/thought-leadership/institute-business-value/report/quantum-decade*

18 Martin, D.; « Turning A Million-Qubit Quantum Computing Dream Into Reality », The Next Platform, 10 mai 2022, *https://www.nextplatform.com/2022/05/10/turning-a-million-qubit-quantum-computing-dream- into-reality/amp/*

19 National Institute of Standards and Technology, « Post-Quantum Cryptography (PQC) », États-Unis, *https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions*

20 Samhitha; « Quantum Computing in 2022: A Leap Into the Tremendous Future Ahead," *Analytics Insight,* 2 janvier 2022, *https://www.analyticsinsight.net/quantum-computing-in-2022-a-leap-into-the-tremendous-future-ahead/*