Communiqués de presse

Des algorithmes développés par IBM sont annoncés comme les premières normes de cryptographie résistante aux ordinateurs quantiques publiées par le NIST

Alors que les ordinateurs quantiques progressent rapidement, l'Institut national américain des normes et de la technologie (NIST) publie de nouveaux algorithmes, dont ceux développés par IBM, en collaboration avec des partenaires industriels, pour sécuriser les données contre les potentielles attaques quantiques.

YORKTOWN HEIGHTS, N.Y., le 03 septembre 2024 : Deux algorithmes développés par IBM (NYSE: IBM) ont été officiellement publiés parmi les trois premières normes de cryptographie résistante aux ordinateurs quantiques annoncées par l'Institut national des normes et de la technologie (NIST) du ministère américain du commerce.

Les normes comprennent trois algorithmes de cryptographie résistante aux ordinateurs quantiques : deux d'entre eux, ML-KEM (initialement connu sous le nom de CRYSTALS-Kyber) et ML-DSA (initialement CRYSTALS-Dilithium) ont été développés par des chercheurs d'IBM en collaboration avec plusieurs partenaires industriels et universitaires. Le troisième algorithme publié, SLH-DSA (initialement soumis sous le nom de SPHINCS+) a été co-développé par un chercheur qui a depuis rejoint IBM. En outre, un quatrième algorithme développé par IBM, FN-DSA (initialement appelé FALCON), a été sélectionné pour une future normalisation.

La publication officielle de ces algorithmes marque une étape cruciale dans l'avancée de la protection des données chiffrées du monde entier contre les cyberattaques qui pourraient être tentées grâce à la puissance unique des ordinateurs quantiques, qui progressent rapidement vers une pertinence cryptographique. C'est à ce moment-là que les ordinateurs quantiques atteindront une puissance de calcul suffisante pour casser les normes de chiffrement qui sous-tendent la plupart des données et des infrastructures mondiales actuelles.

« La mission d'IBM dans le domaine de l'informatique quantique est double : mettre l'informatique quantique utile à la

disposition du monde et rendre le monde sûr sur le plan quantique. Nous sommes ravis des progrès incroyables que nous avons réalisés avec les ordinateurs quantiques d'aujourd'hui, qui sont utilisés dans des industries mondiales pour explorer des problèmes alors que nous nous dirigeons vers des systèmes à correction d'erreurs », a déclaré **Jay Gambetta, Vice President, IBM Quantum**. *« Cependant, nous comprenons que ces avancées pourraient annoncer un bouleversement dans la sécurité de nos données et de nos systèmes les plus sensibles. La publication par le NIST de ses trois premières normes de cryptographie résistante aux ordinateurs quantiques marque une étape importante dans les efforts visant à construire un avenir sans risque quantique parallèlement à l'informatique quantique ».*

En tant que branche entièrement nouvelle de l'informatique, les ordinateurs quantiques évoluent rapidement vers des systèmes utiles et à grande échelle, comme en témoignent les étapes matérielles et logicielles franchies et prévues dans la feuille de route de développement quantique d'IBM. Par exemple, IBM prévoit de livrer son premier système quantique à correction d'erreur d'ici 2029. Ce système devrait exécuter des centaines de millions d'opérations quantiques afin d'obtenir des résultats précis pour des problèmes complexes et utiles qui sont actuellement inaccessibles aux ordinateurs classiques. À plus long terme, la feuille de route d'IBM prévoit d'étendre ce système pour exécuter plus d'un milliard d'opérations quantiques d'ici à 2033. Pour atteindre ces objectifs, IBM a déjà doté des experts des secteurs de la santé et des sciences de la vie, de la finance, du développement de matériaux, de la logistique et d'autres domaines de systèmes à une échelle utile[1] pour commencer à appliquer et à transposer leurs défis les plus urgents aux ordinateurs quantiques au fur et à mesure qu'ils progressent.

Toutefois, l'avènement d'ordinateurs quantiques plus puissants pourrait présenter des risques pour les protocoles de cybersécurité actuels. À mesure que leur vitesse et leurs capacités de correction d'erreur augmentent, ils sont également susceptibles d'être en mesure de casser les systèmes cryptographiques les plus utilisés aujourd'hui, tels que RSA, qui protège depuis longtemps les données mondiales. À partir de travaux entamés il y a plusieurs décennies, l'équipe d'IBM, composée des plus grands experts en cryptographie au monde, continue d'être à la pointe du secteur dans le développement d'algorithmes destinés à protéger les données contre les menaces futures, et qui sont désormais en mesure de remplacer les systèmes de chiffrement actuels.

Les normes nouvellement publiées par le NIST sont conçues pour protéger les données échangées sur les réseaux publics, ainsi que les signatures numériques pour l'authentification des identités. Désormais formalisées, elles serviront de référence aux gouvernements et aux entreprises du monde entier pour commencer à adopter des stratégies de cybersécurité résistante aux ordinateurs quantiques.

En 2016, le NIST a demandé aux cryptographes du monde entier de développer et de soumettre de nouveaux systèmes cryptographiques résistants aux ordinateurs quantiques en vue d'une future normalisation. En 2022, quatre des 69 algorithmes soumis pour examen ont été retenus pour une future normalisation : CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon et SPHINCS+.

Outre la poursuite des évaluations visant à publier Falcon comme quatrième norme officielle, le NIST continue d'identifier et d'évaluer d'autres algorithmes pour diversifier sa panoplie d'algorithmes cryptographiques résistants aux ordinateurs quantiques, dont plusieurs autres développés par des chercheurs d'IBM. Les cryptographes d'IBM sont parmi les pionniers de l'expansion de ces outils, y compris trois systèmes de signatures numériques récemment soumis qui ont déjà été acceptés pour examen par le NIST et qui font l'objet d'un premier cycle d'évaluation.

Dans le cadre de sa mission visant à rendre le monde sûr sur le plan quantique, IBM continue à intégrer la cryptographie résistante aux ordinateurs quantique dans un grand nombre de ses propres produits, tels que l'IBM z16 et IBM Cloud. En 2023, la compagnie a dévoilé la feuille de route IBM Quantum Safe, un plan en trois étapes pour tracer les jalons vers une technologie résistante aux ordinateurs quantique de plus en plus avancée, et définie par les phases de découverte, d'observation et de transformation. Parallèlement à cette feuille de route, la compagnie a également présenté la technologie IBM Quantum Safe et les services de transformation IBM Quantum Safe afin d'aider les clients à se doter d'une sécurité résistante aux ordinateurs quantiques. Ces technologies comprennent l'introduction du Cryptography Bill of Materials (CBOM), une nouvelle norme permettant de capturer et d'échanger des informations sur les actifs cryptographiques dans les logiciels et les systèmes.

Pour en savoir plus sur la technologie et les services IBM Quantum Safe : https://www.ibm.com/quantum/quantum-safe.

À propos d'IBM

IBM est un leader mondial du Cloud hybride et de l'IA, ainsi que des services aux entreprises, qui aide ses clients dans plus de 175 pays à capitaliser sur les connaissances issues de leurs données, à rationaliser leurs processus métier, à réduire leurs coûts et à acquérir un avantage concurrentiel dans leurs secteurs d'activité. Près de 4 000 entités gouvernementales et entreprises dans des domaines d'infrastructures critiques tels que les services financiers, les télécommunications et les soins de santé font confiance à la plateforme Cloud hybride d'IBM et à Red Hat OpenShift pour impacter leurs transformations numériques rapidement, efficacement et en toute sécurité. Les innovations révolutionnaires d'IBM en matière d'IA, d'informatique quantique, de solutions Cloud spécifiques à certains secteurs et de services aux entreprises offrent des options ouvertes et flexibles à nos clients. Tout cela est soutenu par l'engagement légendaire d'IBM en matière de confiance, de transparence, de responsabilité, d'inclusivité et de service.

Pour en savoir plus : www.ibm.com/fr-fr

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

[1] IBM considère que nous sommes rentrés dans l'ère de l'utilité quantique depuis juin 2023, ère dans laquelle le matériel quantique peut exécuter des circuits quantiques plus rapidement et avec plus de précision qu'un ordinateur classique simulant un ordinateur quantique.