Prêt pour l'avenir

Le parcours vers la sécurité post-quantique

Rapport Vanguard

Avril 2022

Sur demande de

IBM

451 Research

S&P Global
Market Intelligence

À propos de l’auteur

John Abbott

Analyste principal en recherche, 4SIGHT

John Abbott travaille sur les systèmes, le stockage et les infrastructures logicielles pour 451 Research, qui fait partie de S&P Global Market Intelligence. Au cours de sa carrière de plus de 30 ans, il a été un pionnier dans des domaines tels que les technologies spécialisées pour Unix, le calcul intensif, les architectures système, le développement logiciel et le stockage.

Cofondateur de The 451 Group en octobre 1999, John Abbott a dirigé les opérations d’analyse de l’entreprise depuis les bureaux de San Francisco. Il a été l’auteur principal de nombreux rapports spéciaux de 451 Research, notamment ceux sur la virtualisation du stockage et les serveurs lames, les premières enquêtes complètes sur le sujet jamais publiées. Plus récemment, John Abbott s’est concentré sur les infrastructures convergées, les nouvelles architectures systèmes, l’IA et les accélérateurs de l’apprentissage en profondeur. Il a contribué à la mise en place de 4SIGHT, le cadre de 451 Research pour la couverture prospective et à long terme des technologies émergentes.

John Abbott a commencé à s’intéresser au secteur des technologies en 1984 en s’appuyant sur son expérience passée en tant qu’auteur technique et sur son implication directe dans l’utilisation des mainframes, des premiers PC et des stations de travail Unix. En tant que journaliste indépendant, il a contribué à des publications dans Computing, Computer Weekly, The Financial Times et The Times. En 1987, il a été nommé rédacteur du bulletin d’information Unix hebdomadaire pour ComputerWire, Unigram.X. Il est ensuite devenu rédacteur du service international quotidien de l’entreprise, Computergram, d’abord à Londres, puis à San Francisco. Il a mis en place le bureau 451 Research à San Francisco, où il a vécu pendant plus de dix ans.

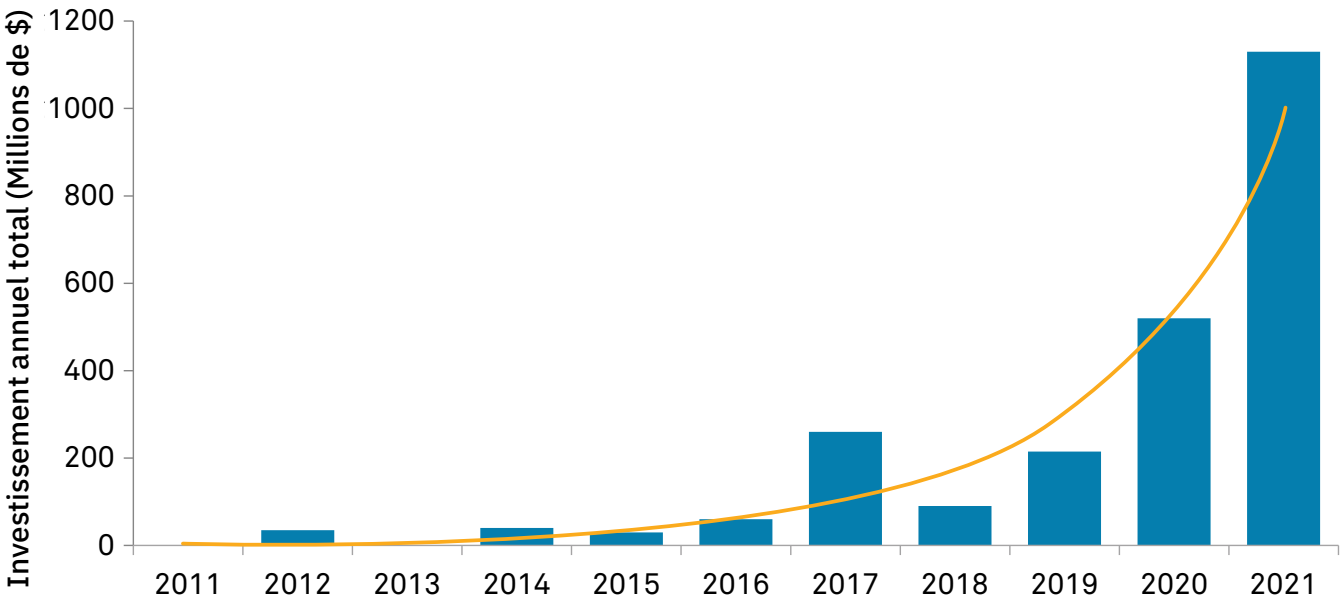
John a étudié la musique à l’Université de Keele et il possède une maîtrise es lettres en littérature anglaise moderne de l’Université de Londres.

Introduction

De nos jours, l'informatique quantique peut être décrite comme étant un investissement à haut risque, mais à fort rendement. Nous ne pouvons pas garantir qu'un ordinateur quantique universel pratique pourra concrètement être fabriqué de notre vivant. Mais des laboratoires de recherche, ainsi que de plus en plus d'entreprises privées du secteur des technologies, franchissent de nouveaux obstacles chaque jour et créent des innovations scientifiques de pointe. Et les retombées pourraient être phénoménales, notamment grâce à la résolution de problèmes qui, aujourd'hui, dépassent les capacités d'un supercalculateur (classique). Il est donc aisé de comprendre pourquoi les revendeurs autant que les utilisateurs tentent leur chance avec cette technologie au pouvoir révolutionnaire. Les données de S&P Capital IP Pro (Figure 1) montrent que les start-ups dans le domaine de l'informatique quantique ont obtenu 2,4 milliards de dollars d'investissements au cours de la dernière décennie. L'année 2021 a vu un important regain d'intérêt avec des investissements de 1,1 milliard de dollars dans les sociétés impliquées dans la recherche quantique. Et encore ces chiffres n'intègrent-ils pas les investissements massifs réalisés par les entreprises informatiques déjà bien établies que sont IBM, Amazon, Google et Honeywell.

Cette opportunité soulève cependant quelques questions importantes. La plus urgente est peut-être celle de la menace pour les pratiques de sécurité actuelles. Armés de l'informatique quantique, les utilisateurs malveillants seraient en mesure de contrefaire des signatures et de déchiffrer les niveaux actuels de cryptographie et de chiffrement, notamment l'infrastructure à clés publiques profondément ancrée dans les systèmes informatiques du monde entier. Pire encore, même les données chiffrées actuellement protégées pourraient être conservées pour déchiffrement ultérieur une fois l'informatique quantique effectivement mise en pratique. Cette question ne peut pas être remise à plus tard. Plus nous attendons, plus nous créons de données exposées à ce risque.

Figure 1 : Investissements dans des start-ups d'informatique quantique



Source : S&P Capital IQ Pro

Intégration 451

Il est impossible de prévoir exactement quand un ordinateur quantique exécutant l'algorithme de Shor avec efficacité sera si largement disponible qu'un utilisateur malveillant pourra y avoir accès. À ce jour, aucun fournisseur informatique n'a indiqué de chronologie précise quant à la possibilité pour l'informatique quantique de dépasser de manière pertinente les ordinateurs classiques. Toutefois, l'accélération des avancées technologiques de ces cinq dernières années, associée aux investissements conséquents désormais en place, laisse penser que ce jour arrivera peut-être avant la fin de la décennie. Lorsque cela se produira, toutes les informations actuellement protégées par des algorithmes à clés publiques seront menacées d'exposition. Pour les agences gouvernementales de renseignement et de défense, ainsi que pour les fournisseurs de services cloud et les constructeurs de systèmes dont les clients appartiennent à des secteurs réglementés, le risque est déjà trop important pour être ignoré. Malgré les fausses alertes du passé (repensons par exemple au bogue de l'an 2000, quand un raccourci de programmation informatique largement utilisé menaçait de semer la pagaille lors du passage de l'année 1999 à l'année 2000) et les inconnues de l'avenir, une chose est sûre : les dangers des cyberattaques sont un problème grave aujourd'hui et la nature des menaces et des vulnérabilités évolue de manière incessante. Les politiques de sécurité doivent être sans cesse revues et mises à jour, et les technologies cryptographiques à sécurité post-quantique, parallèlement à la mise en œuvre d'une crypto-agilité et d'un inventaire cryptographique, formeront le cœur de cette équation.

Scénarios de sécurité résistant aux attaques quantiques et de sécurité post-quantique

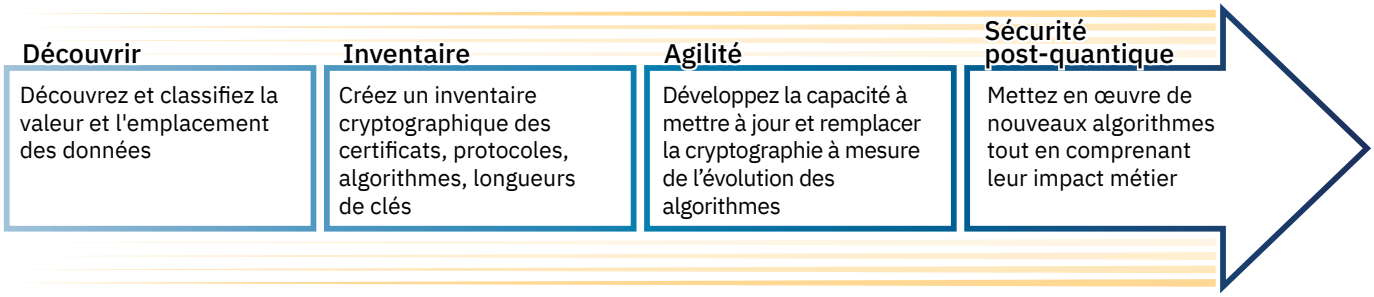
Le problème se présente ainsi : la génération actuelle des algorithmes de sécurité largement utilisés est fondée sur des problèmes mathématiques difficiles… trop difficiles pour être résolus par un ordinateur classique. En revanche, ces mêmes problèmes pourraient être facilement résolus par un ordinateur quantique de puissance suffisante, un postulat largement accepté depuis 1994, lorsque le mathématicien américain Peter Shor a découvert l'algorithme de temps polynomial, désormais appelé algorithme de Shor. Le premier ordinateur quantique a été fabriqué trois ans plus tard. Le développement d'algorithmes de sécurité post-quantique a bien progressé au cours des dix dernières années. Mais le passage des systèmes cryptographiques à clés publiques largement utilisés aujourd'hui dans les gouvernements et industries vers un nouvel ensemble d'algorithmes pourrait prendre plusieurs dizaines d'années.

C'est pourquoi des organisations telles que le NIST (National Institute of Standards and Technology) et le ministère de la Sécurité intérieure (Homeland Security) des États-Unis travaillent sur le processus de normalisation des algorithmes eux-mêmes et sur des recommandations visant à aider les entreprises à se préparer à la transition vers la cryptographie post-quantique. Ces travaux ont incité la Maison Blanche à produire un mémo au mois de janvier pour imposer aux services de défense et de renseignement de commencer à mettre en place ce changement.

Décoder un nombre entier composé de 2 048 bits (par la recherche des facteurs premiers) sur les ordinateurs les plus puissants actuels prendrait des millions d'années. Sur un ordinateur quantique, cette tâche ne durerait en théorie que quelques heures. Les schémas à clés publiques actuels cassés par l'algorithme de Shor incluent le vénérable algorithme RSA (existant depuis 45 ans, mais toujours utilisé dans pratiquement toutes les transactions Internet), ainsi que la norme DSS (Data Security Standard), le cryptosystème de Paillier, l'algorithme de signature numérique à courbe elliptique, le chiffrement Diffie-Hellman basé sur les courbes elliptiques et le chiffrement ElGamal. La liste des normes établies par le NIST, l'ISO/la CEI, l'ETSI et l'IETF concernées s'allonge, ce qui démontre que ce problème est international ; par exemple, en Chine, l'algorithme de signature numérique SM2 et la norme de cryptographie nationale SM9 sont également cassés.

Le processus de normes NIST, initié en 2016 avec un appel à propositions, a identifié un nouvel ensemble de candidats résistant à l'informatique quantique. Regroupés selon différentes approches (cryptographie en treillis, multivariée, basée sur hachage ou sur code), ces candidats incluent notamment le mécanisme d'encapsulation de clé (KEM) CRYSTALS-Kyber basé sur treillis, McEliece (KEM basé sur code) et les schémas de signature post-quantiques Falcon (basé sur treillis) et Rainbow (à plusieurs variables). Ces éléments prometteurs, et d'autres, s'orientent vers une ébauche de normalisation après le troisième cycle de la compétition, désormais achevé. Le quatrième cycle, qui comprendra des algorithmes alternatifs et un appel à des schémas de signature supplémentaires, débute cette année et s'achèvera à la fin de l'année 2024.

Figure 2 : Jalons de la maturité sur le parcours vers la sécurité post-quantique



Source : 451 Research

Parcours vers la cryptographie post-quantique

Quelles actions les organisations doivent-elles entreprendre aujourd'hui pour se préparer à l'intégration de la cryptographie post-quantique dans leurs architectures de sécurité des informations au cours des dix prochaines années ? La première étape, déjà entamée, consiste à participer au processus de normalisation. Il est important que toute organisation ayant un intérêt dans la prévention des authentifications frauduleuses, la protection de l'intégrité du chiffrement et la lutte contre la compromission des signatures numériques participe activement à ce processus pour s'assurer que ses exigences propres seront satisfaites par la liste approuvée des algorithmes, processeurs et outils finalisés. Malgré les progrès réalisés par les organismes de normalisation, il reste beaucoup à faire et d'autres algorithmes seront nécessaires. En outre, les jalons de maturité suivants conduiront à la sécurité post-quantique.

- **Détection des données et classification :** dresser un inventaire des données critiques. Quelles données présentent la plus forte valeur ? Où se trouvent les données ? Quelles sont les exigences de conformité ? Comprendre ces informations est un impératif, car de nombreuses organisations ignorent en partie ce qu'elles possèdent ou la valeur des éléments en leur possession. Sans ces connaissances, elles ne sont pas en mesure d'identifier leurs vulnérabilités les plus graves. Elles doivent créer et gérer un inventaire de données dont la propriété est clairement définie.
- **Crypto-inventaire :** un inventaire cryptographique détaille l'emplacement et les modes d'utilisation de la cryptographie à clés publiques vulnérable et contient des éléments tels que les certificats, les protocoles de chiffrement, les algorithmes et les longueurs de clés. L'inventaire doit être géré de façon à couvrir l'ensemble du cycle de vie des certificats et clés de chiffrement.
- **Crypto-agilité** : à mesure de l'avancement de leurs plans et de leur transition, les organisations doivent réfléchir à la crypto-agilité de manière à pouvoir effectuer des ajustements sans douleur, en fonction de l'évolution des technologies et des circonstances. Elles doivent concevoir et mettre en place des processus permettant de mettre à jour ou de remplacer la cryptographie actuelle, puis la tester, avec plus de facilité, dans des délais d'exécution bien définis.
- **Sécurité post-quantique** : les organisations doivent mettre en œuvre de nouveaux algorithmes tout en connaissant l'impact possible, en termes de performance, de la cryptographie post-quantique sur l'entreprise.

Chaque organisation est unique et toutes ne sont pas en mesure de, ou disposées à, tout changer, notamment en raison des frais ou des problèmes de gestion du cycle de vie. Il demeure cependant essentiel de concevoir des moyens de mettre à jour ou de remplacer les protocoles de sécurité à court aussi bien qu'à long terme. Parce qu'elle est étroitement liée à l'infrastructure système, la démarche visant à devenir crypto-agile nécessite la coopération des concepteurs de systèmes, des développeurs d'applications et des experts en sécurité. Aujourd'hui, les outils manquent pour faciliter ce processus.

Les organisations feront appel à divers facteurs pour établir leurs priorités dans le remplacement cryptographique post-quantique : la valeur des actifs protégés, la vulnérabilité des éléments protégés (c'est-à-dire les magasins de clés et les mots de passe), les systèmes connectés potentiellement concernés (c'est-à-dire le partage d'informations avec des entités extérieures, notamment les agences fédérales) et la durée de protection des données. Des organisations hybrides associant algorithmes classiques et algorithmes post-quantiques seront nécessaires pendant la longue période de transition.

Mise en œuvre, motivation et éléments moteurs

Les fournisseurs de systèmes et les grands prestataires de services cloud, dont les équipements et les infrastructures hébergent des charges de travail essentielles pour les entreprises, ne peuvent s'offrir le luxe d'attendre que les normes de cryptographie à sécurité post-quantique soient parfaitement achevées. Ils travaillent sur ces questions depuis plusieurs années et ont apporté leur contribution au choix des algorithmes et protocoles arrivant en tête de la sélection pour figurer dans la liste des normes finalisées en 2024. Un certain nombre de services de gestion des clés basés sur le cloud prennent déjà en charge les algorithmes des cycles deux et trois. Les clients commencent à utiliser ces services pour mesurer l'impact possible sur les performances de leurs applications en raison d'une surcharge supplémentaire possible sur l'utilisation de la bande passante et la latence, ainsi que pour amoindrir les effets des pannes de connexion probables au niveau des couches de proxy TLS (Transport Level Security). Mais tous s'accordent à dire que la transition vers la sécurité post-quantique demandera plusieurs années alors que les normes et les technologies évoluent, et que ce parcours commence par le renforcement de la sécurité des infrastructures centrales.

Dans le monde des systèmes, les mainframes sont encore très largement utilisés en tant qu'infrastructures centrales sécurisées et hautement disponibles par les plus grandes banques, compagnies d'assurance, sociétés de télécommunications et entreprises de vente et de transport, une position acquise et conservée depuis plus d'un demi-siècle. Les mainframes de dernière génération seront équipés de modules matériels à sécurité post-quantique, complétés par des composants de systèmes d'exploitation actualisés, des API de gestion des clés et la prise en charge d'une suite d'algorithmes émergents résistant aux attaques quantiques. Une technologie d'amorçage à sécurité post-quantique et une racine de confiance matérielle seront utilisées pour protéger l'intégrité du microprogramme d'amorçage du système. En outre, des interfaces de programmation des applications offrant des mécanismes de sécurité post-quantique seront proposées pour sécuriser l'échange de clés cryptographiques avec des partenaires commerciaux.

Les prestataires de services cloud et les fournisseurs doivent jouer un rôle central pour aider leurs clients à passer à la cryptographie post-quantique. Les prises de position réglementaires à titre individuel ne suffisent pas, notamment parce qu'elles ne sont jamais suffisamment normatives pour apporter des directives claires aux organisations utilisatrices sans expertise pertinente propre. Les fournisseurs déjà au cœur de l'infrastructure stratégique peuvent simplifier le processus en proposant une protection métier centrale sans modifications supplémentaires au niveau du système. Ils peuvent également fournir les outils de reconnaissance si attendus pour l'analyse des applications cryptographiques. Les organisations responsables des données doivent s'assurer que leurs données sont protégées pendant toute la durée de leur cycle de vie, aujourd'hui et demain, car les données chiffrées selon des algorithmes classiques aujourd'hui pourraient être déchiffrées par un ordinateur quantique avancé à l'avenir. Si la sécurité de ces données doit être assurée pour 20 ans, cela nous amène rapidement jusque dans les années 2040. Même les sceptiques qui pensent que l'informatique quantique pratique est encore loin devant nous doivent reconnaître qu'au rythme actuel des avancées, la probabilité de sa généralisation aura alors fortement augmenté.

Conclusions

Le dossier en faveur de l'informatique quantique est solide : un ordinateur quantique pleinement développé permettrait des avancées en chimie, en apprentissage automatique, en finance, en transports, en soins de santé et bien plus. Les ordinateurs quantiques accéléreraient de manière exponentielle le traitement d'équations aujourd'hui impossibles à exécuter sur un ordinateur déterministe classique actuel.

Mais cette médaille a un revers. L'informatique quantique pourrait renforcer la menace déjà croissante des cyberattaques contre la protection des données. Alors que la valeur commerciale des données augmente, il en va de même de l'échelle et du coût des exigences de protection des données. En outre, parce que les données conservent longtemps leur valeur, il faut tenir compte de la probabilité croissante de l'avènement réel des ordinateurs quantiques dans un avenir proche. Mieux vaut agir sans attendre afin de proposer une évolution plus sûre et plus contrôlée vers une infrastructure centrale à sécurité post-quantique, la mise en œuvre d'outils capables de reconnaître les vulnérabilités actuelles sur les couches d'applications, la protection des systèmes d'échange de clés utilisés dans les organisations et la protection continue des secrets durables contenus dans les données.

CONTACTS

Amériques
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Moyen-Orient et Afrique
+44 20 7176 1234
market.intelligence@spglobal.com

Asie-Pacifique
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence