CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Février 2025 | ITSAP.00.017

Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie

Avoir recours à la cryptographie est un moyen efficace d'assurer la confidentialité et l'intégrité de l'information et de protéger les systèmes informatiques contre les auteurs de menace. L'informatique quantique menace de détruire une grande partie de la cryptographie que nous utilisons actuellement. Les ordinateurs quantiques utiliseront la physique quantique pour traiter l'information et résoudre des problèmes qu'il est difficile de solutionner au moyen des capacités de traitement actuelles.

Les ordinateurs quantiques actuels ne sont pas suffisamment puissants pour casser la cryptographie à clé publique. Toutefois, un auteur de menace pourrait un jour disposer d'un ordinateur quantique suffisamment puissant pour accéder aux systèmes ou pour déchiffrer et lire l'information sensible. Les organisations devront donc mettre à jour leurs systèmes informatiques pour se protéger de la menace quantique.

En quoi la cybersécurité est-elle touchée?

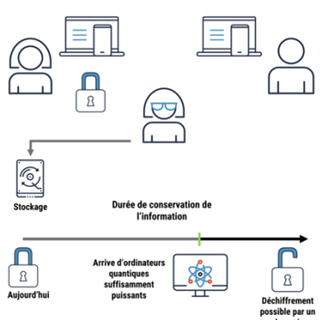
Les progrès réalisés dans le domaine de l'informatique quantique mettent à risque la cybersécurité de votre organisation. Bien que les ordinateurs quantiques actuels n'aient pas la puissance nécessaire pour venir à bout des techniques de cryptographie actuelles, un ordinateur suffisamment puissant pourrait être disponible dès 2030.

La cryptographie protège l'information et les systèmes informatiques en faisant appel au chiffrement et à l'authentification.

Incidence potentielle sur le chiffrement

Le chiffrement protège la confidentialité de l'information stockée sur un dispositif, comme un téléphone intelligent ou une clé USB, et celle transmise à partir de ce dernier. Les auteurs de menace peuvent stocker l'information chiffrée aujourd'hui afin de la déchiffrer plus tard, à l'arrivée d'ordinateurs quantiques suffisamment puissants. Par conséquent, l'information chiffrée ayant une longue durée de conservation pourrait être à risque. Il s'agit d'une menace immédiate de type « récolter maintenant, déchiffrer plus tard » (HNDL pour *Harvest Now, Decrypt Later*).

Figure 1 : Un auteur de menace intercepte et stocke de l'information chiffrée pour la déchiffrer ultérieurement



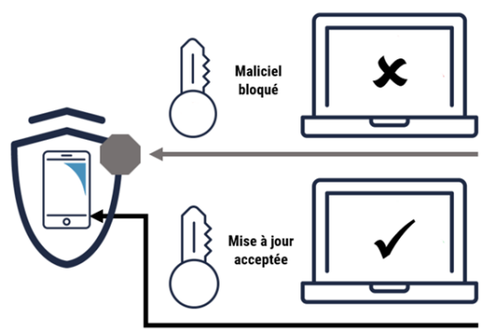
Dans le diagramme, un auteur de menace intercepte et stocke de l'information chiffrée dans le but de la déchiffrer plus tard, à l'arrivée d'ordinateurs quantiques suffisamment puissants.

Incidence potentielle sur l'authentification

L'authentification protège l'intégrité de l'information et pose les bases de la confiance numérique en ligne. Elle permet de s'assurer que l'information n'a pas été modifiée lorsqu'elle est en transit ou en stockage, et qu'elle provient de la source appropriée, qu'il s'agisse d'un système ou de personnes. Des auteurs de menace pourraient utiliser un ordinateur quantique suffisamment puissant de manière à se faire passer pour un système fiable, comme une boutique d'applications ou un fournisseur de confiance, dans le but de distribuer de fausses mises à jour logicielles et d'accéder aux systèmes qui les intéressent. Ils pourraient également contrefaire les certificats utilisés par les sites Web sécurisés pour faire en sorte de diriger le trafic légitime vers leurs sites non valides.

La figure 2 illustre la manière dont les auteurs de menace peuvent utiliser des ordinateurs quantiques puissants de manière à se faire passer pour un système de confiance dans le but de distribuer de fausses mises à jour logicielles et d'accéder aux systèmes qui les intéressent.

Figure 2 : Un auteur de menace utilise des ordinateurs quantiques puissants pour personnifier d'autres systèmes



Comme l'illustre la figure 2, le téléphone bloque le maliciel, puisqu'il ne contient pas de certificat valide. Toutefois, si une mise à jour est signée au moyen d'un certificat valide et est soumise au téléphone, ce dernier l'acceptera et procédera à son installation. Si un ordinateur quantique peut aider à contrefaire le certificat et que ce faux certificat est ensuite utilisé pour signer le maliciel, le téléphone ne saura pas qu'il faut le bloquer et le maliciel arrivera à s'installer.

Contrairement à la confidentialité, l'authentification ne sera à risque qu'après l'arrivée d'ordinateurs quantiques suffisamment puissants.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada
Cat. No. D97-1/00-017-2025F-PDF ISBN 978-0-660-75600-4

Canada

Transition vers la cryptographie post-quantique

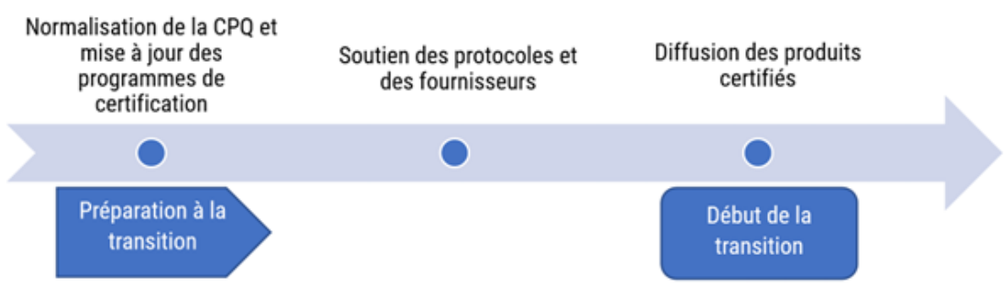
On considère qu'un algorithme de chiffrement offre une résistance quantique s'il ne peut être cassé par un ordinateur quantique. Par cryptographie post-quantique (CPQ), on entend les algorithmes qui sont conçus pour fournir une résistance quantique et qui peuvent être exécutés sur un ordinateur traditionnel.

La cryptographie post-quantique comprend les algorithmes qui établissent les clés nécessaires au chiffrement et aux schémas de signature numérique servant à l'authentification. Ces derniers doivent être en mesure de fonctionner avec les protocoles de communication, les logiciels et les réseaux existants.

Pour assurer la sécurité quantique, on recommande aux organisations d'adopter les solutions de cybersécurité existantes et d'avoir recours à la cryptographie post-quantique. Plusieurs fournisseurs de logiciels et de services infonuagiques planifient déjà de prendre en charge une telle cryptographie dans leurs systèmes et leurs produits. Les organisations devraient confirmer les feuilles de route de la cryptographie post-quantique auprès des fournisseurs et rechercher les façons de migrer vers des solutions informatiques personnalisées.

Avant que les solutions de cryptographie post-quantique puissent être adoptées, il sera toutefois nécessaire de finaliser les normes associées aux algorithmes CPQ et les protocoles de communications Internet qui les intègrent. Les produits des fournisseurs qui mettent en œuvre ces normes devraient également être validés et certifiés. Le National Institute of Standards and Technology (NIST) des États-Unis a publié son ensemble initial de normes pour les algorithmes CPQ en août 2024. On s'attend à ce que des organisations comme l'Internet Engineering Task Force (IETF) prennent bientôt en charge le protocole.

Figure 3 : Progression de la cryptographie post-quantique



Cette figure décrit les phases de la progression de la cryptographie post-quantique. Au cours de la phase de préparation, la progression de la cryptographie post-quantique comprend la mise à jour des programmes de normalisation et de certification, ainsi que le soutien des protocoles et des fournisseurs. Une fois que les produits certifiés auront été lancés, on encourage les organisations à les utiliser et à commencer la transition vers la cryptographie post-quantique.

Ce que votre organisation peut faire

On recommande à votre organisation de prendre les mesures ci-dessous pour aider à pallier les risques liés aux progrès réalisés dans le domaine de l'informatique quantique et de planifier sa transition vers la cryptographie post-quantique.

- Déterminez les systèmes (internes et destinés à la clientèle), les applications, les passerelles et les composantes de sécurité connexes qui seront ciblés lors de la transition.
    - Le soutien des composantes de sécurité peut comprendre ce qui suit :
        - l'infrastructure à clé publique (ICP);
        - les serveurs Web;
        - les mécanismes d'autorisation;
        - les répertoires d'authentification;
        - le système d'adressage par domaine (DNS) de protection.
    - Accordez une attention particulière aux systèmes personnalisés, ainsi qu'aux logiciels conçus en interne ou fournis par de petits fournisseurs.
    - Ces efforts visent généralement à développer un inventaire des produits cryptographiques.
- Déterminez les systèmes patrimoniaux qui ne peuvent être compris dans la transition et développez une approche axée sur la gestion des risques pour les protéger. La tunnellisation du trafic par l'entremise d'un réseau privé virtuel protégé par la cryptographie post-quantique est un exemple d'une telle solution.
- Évaluez le niveau de sensibilité et la durée de conservation de l'information de votre organisation afin de déterminer l'information qui pourrait être à risque (en tant qu'élément des processus d'évaluation continue des risques). Cela vous aidera à hiérarchiser le travail à faire pour assurer la transition.
- Passez en revue votre gestion du cycle de vie des produits informatiques et mettez en place un plan pour faciliter l'adoption de la cryptographie post-quantique dès son arrivée.
- Prévoyez un budget pour des mises à jour matérielles et logicielles potentiellement considérables (y compris le personnel de soutien) lorsque viendra le temps de procéder aux remplacements nécessaires.
- Assurez-vous que vos équipes et vous êtes au courant des nouvelles menaces et des futures technologies quantiques.
- Demandez à vos fournisseurs s'ils planifient de mettre en place la cryptographie post-quantique ou de l'intégrer à de futures mises à jour afin de déterminer si votre organisation devra se procurer du nouveau matériel ou de nouveaux logiciels.
- Assurez-vous que votre fournisseur a recours à des mécanismes cryptographiques normalisés et validés, comme l'accréditation Federal Information Processing Standards (FIPS).
- Tenez un inventaire des produits cryptographiques pour assurer l'adoption de pratiques cryptographiques agiles et faciliter les changements à apporter à la cryptographie des systèmes déployés. Pour obtenir de plus amples renseignements, consultez le document Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018).

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada
Cat. No. D97-1/00-017-2025F-PDF ISBN 978-0-660-75600-4

Canada

Autres solutions à résistance quantique

Le Centre pour la cybersécurité recommande aux organisations de faire la migration vers la cryptographie post-quantique normalisée, car elle offre une meilleure protection contre la menace quantique. D'autres solutions à résistance quantique décrites ci-dessous peuvent fournir une plus grande assurance cryptographique lorsqu'on les combine avec la CPQ. Cependant, ces solutions peuvent faire augmenter considérablement la complexité opérationnelle et les coûts de mise en œuvre. Concrètement, il pourrait donc être difficile pour certaines organisations de procéder à ces remplacements dans leurs systèmes cryptographiques actuels. De plus, il n'y a pas d'options d'accréditation de sécurité basées sur des normes reconnues pour ces remplacements.

L'établissement de clés symétriques

L'établissement de clés symétriques (SKE pour *Symmetric Key Establishment*) exige que les clés cryptographiques secrètes soient prépartagées avec l'ensemble des utilisatrices et utilisateurs (points terminaux) par l'entremise d'un mécanisme hors bande, et non d'un mécanisme d'établissement de clés comme celui de la cryptographie post-quantique. Dans de vastes réseaux, une autorité centrale de confiance établit en ligne des paires de clés secrètes. L'adoption de ce principe est sujette à des limitations, comme la distribution sécurisée de clés prépartagées et la confiance accordée à l'autorité centrale.

La distribution quantique de clés

La distribution quantique de clés (QKD pour Quantum Key Distribution) tire avantage de la physique de la lumière pour établir une clé secrète entre les nœuds d'un réseau. Les nœuds exigent du matériel quantique dédié et une connexion directe (fibre optique ou optique sans fil). Avec la technologie actuelle, les distances entre les nœuds se limitent à quelques centaines de kilomètres de fibres optiques. De plus, les points terminaux typiques des utilisatrices et utilisateurs (par exemple, les téléphones, les portables et les modems) ne prennent pas en charge la fonctionnalité des nœuds par QKD. Il est difficile d'évaluer la robustesse des systèmes de QKD et les organisations internationales de normalisation s'efforcent d'élaborer les normes en la matière.

Les organisations qui souhaitent utiliser d'autres solutions à résistance quantique devront effectuer leur propre analyse coûts-avantages. Pour la plupart des organisations, la voie la plus facile et rentable d'accéder à la résistance quantique est de mettre en place une technologie CPQ agile.

Efforts déployés par le Centre pour la cybersécurité

En tant qu'autorité technique de la cryptographie au sein du gouvernement du Canada, le Centre pour la cybersécurité prend les mesures suivantes pour aider à assurer la résistance quantique du Canada :

- prodiguer des conseils à tous les ordres de gouvernement, aux infrastructures essentielles et aux autres secteurs sur les questions liées à la menace quantique et les mesures à prendre pour se préparer à la transition vers la cryptographie post-quantique;
- jouer un rôle de premier plan dans la transition vers la cryptographie post-quantique sur les systèmes informatiques du gouvernement du Canada en collaboration avec les autres ministères du gouvernement;
- collaborer avec le NIST et d'autres partenaires pour évaluer la sécurité des algorithmes CPQ considérés et mettre à jour les programmes de certification des produits, comme le Programme de validation des modules cryptographiques (PVMC), pour tester les mises en œuvre de la cryptographie post-quantique;
- prendre part aux activités des organisations internationales de normalisation pour s'assurer que les normes associées aux protocoles de communications Internet (comme les protocoles TLS et IPsec) répondent aux besoins des Canadiennes et Canadiens en matière de sécurité cryptographique et de respect de la vie privée;
- collaborer avec les fournisseurs pour les inciter à adopter la cryptographie post-quantique recommandée par le NIST dans les produits commerciaux et pour créer des outils qui soutiennent la transition vers la cryptographie post-quantique.

Learn More

- Guidance on becoming cryptographically agile (ITSAP.40.018)
- Addressing the quantum computing threat to cryptography (ITSE.00.017)
- Cyber Centre celebrates new NIST post-quantum standards
- Post-Quantum Cryptography
- Cryptographic Module Validation Program (CMVP)
- Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111)
- Guidance on securely configuring network protocols (ITSP.40.062)
- Government of Canada's Enterprise Cyber Security Strategy

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada
Cat. No. D97-1/00-017-2025F-PDF ISBN 978-0-660-75600-4

Canada