Quantum Computing Security Issues For Public Key Cryptography

MAY 2017 | EXECUTIVE SERIES | ITSE.00.017

IT Security is essential to government and commercial business activities in Canada. Public Key Cryptography (PKC) is used to protect the confidentiality and integrity of information and is robust in today's computer environment. However, a new computer technology, quantum computing, promises a significant increase in computational capabilities that could compromise PKC.

Quantum computing, based on the properties of quantum physics, is still in its infancy but is expected to mature in the next 10 to 20 years. At that time, quantum computing could put today's PKC at risk, and the confidentiality and integrity of encrypted information may no longer be assured.

This timeframe provides a window of opportunity to create new PKC standards that are resistant to attacks from quantum computers; this is referred to as Quantum Resistant Cryptography (QRC). Adopting QRC will ensure that encrypted information is adequately protected for duration of time that it remains sensitive.

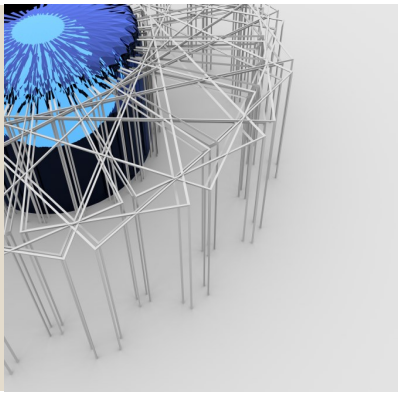
Lifespan Impact

The GC has requirements to protect its sensitive information for its defined lifespan. A threat actor could collect encrypted sensitive information today, and hold onto it in order to decrypt it when quantum computing matures in 10 to 20 years. Information with a lifespan of more than 10 years could still be at risk of decryption.

Technology

The strength of current PKC encryption is based on mathematical problems that are virtually impossible to solve using current technology. Quantum computers will make solving these mathematical problems orders of magnitude faster than today's computers, thus reducing the effectiveness of current PKC encryption.

When using current technology, the effort required to break today's PKC far exceeds the lifespan of the sensitive information it is protecting. With quantum computing, the effort might be measured in days, weeks or a number of years well within the sensitive information's lifespan.



If your department has PKC-encrypted sensitive information with a long lifespan, CSE can address your questions and assist you in being better prepared to protect your sensitive information.

Managing the Risk

The risk that quantum computing could be used to break encryption is a compelling reason to strengthen today's security posture. What should your department do to ensure the protection of your information?

- Evaluate your department's information holdings
- Determine the sensitive lifespan of the information
- Contact CSE for recommendations on how to protect sensitive information with a lifespan of more than 10 years

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

Enjeux de sécurité de l'informatique quantique pour la cryptographie à clé publique

MAI 2017 | SERIE HAUTS DIRIGEANTS | ITSE.00.017

La sécurité des TI est essentielle aux activités organisationnelles du gouvernement et des entreprises au Canada. La cryptographie à clé publique (CCP) sert à protéger la confidentialité et l'intégrité de l'information; c'est d'ailleurs sur sa robustesse que repose la sécurité de l'environnement informatique actuel. L'information quantique, qui constitue une toute nouvelle technologie, se veut aussi la promesse d'une croissance importante des capacités computationnelles susceptibles de compromettre la CCP.

Basée sur les propriétés de la physique quantique, l'informatique quantique en est encore à ses balbutiements. On s'attend toutefois à ce qu'elle parvienne à maturité dans les 10 à 20 prochaines années. Elle posera alors un risque pour la CCP actuelle, puisqu'il sera impossible de garantir la confidentialité et l'intégrité de l'information chiffrée.

D'ici là, il s'offre à nous l'occasion unique de créer de nouvelles normes de CCP capables de résister aux attaques des ordinateurs quantiques; une capacité désignée sous le nom de « cryptographie à résistance quantique ». L'adoption de la cryptographie à résistance quantique permettra d'assurer une protection adéquate de l'information chiffrée aussi longtemps que cette information sera classifiée.

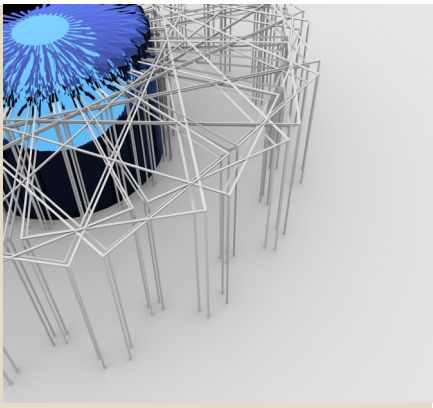
Incidence sur la durée de conservation

Il incombe au GC de protéger son information sensible conformément à la durée de conservation établie. Un auteur de menace pourrait soutirer de l'information sensible aujourd'hui, puis la conserver de manière à la déchiffrer dans 10 à 20 ans, une fois que l'informatique quantique parviendra à maturité. On s'expose donc au risque que l'information faisant l'objet d'une durée de conservation de plus de 10 ans soit éventuellement déchiffrée.

Technologie

De nos jours, la robustesse du chiffrement par CCP repose sur des problèmes mathématiques qui sont virtuellement impossibles à résoudre au moyen de la technologie actuelle. Les ordinateurs quantiques permettront d'accélérer de façon exponentielle la vitesse de résolution de ces problèmes mathématiques par rapport aux ordinateurs d'aujourd'hui, réduisant du coup l'efficacité du chiffrement par CCP actuel.

Avec la présente technologie, le temps nécessaire pour déchiffrer l'information chiffrée par CCP dépasse largement la durée de conservation de l'information sensible que l'on tente de protéger. Grâce à l'informatique quantique, la durée des efforts nécessaires se mesurera en jours, en semaines ou en un nombre d'années bien inférieur à la durée de conservation de l'information sensible visée.



Si votre ministère ou organisme possède de l'information sensible chiffrée par CCP qu'il doit conserver pour de longues périodes, le CST peut répondre à vos questions et vous aider à prendre les mesures nécessaires pour la protéger.

Gestion du risque

Le risque que l'informatique quantique puisse servir à percer le chiffrement constitue une raison valable de renforcer la posture de sécurité actuelle. Quelles mesures votre ministère ou organisme devrait-il prendre pour assurer la protection de votre information?

- Évaluez les fonds de renseignement de votre ministère ou organisme.
- Déterminez la durée de conservation de l'information sensible.
- Communiquez avec le CST pour obtenir des recommandations sur la façon de protéger l'information sensible assujettie à une durée de conservation supérieure à 10 ans.

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modifcation, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

Canada