Preparing your organization for the quantum threat to cryptography

CANADIAN CENTRE FOR CYBER SECURITY
February 2025 | ITSAP.00.017

Cryptography is an effective way to protect the confidentiality and integrity of information and to protect IT systems from threat actors. Quantum computing threatens to break much of the cryptography we currently use. Quantum computers will use quantum physics to process information and solve problems that are impractical to solve using current computing capabilities.

Existing quantum computers are not yet powerful enough to break public key cryptography. However, a threat actor could take advantage of a sufficiently powerful quantum computer in the future to access systems or to decrypt and read sensitive information. Organizations will need to update their IT systems to protect them from the quantum threat.

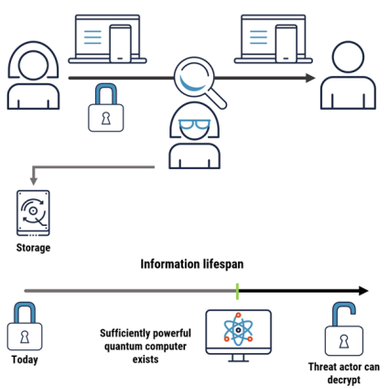
How cyber security is affected

Your organization's cyber security is at risk as quantum computing advances. Although quantum computers cannot break cryptography now, a sufficiently powerful device could be available as early as the 2030s. Cryptography secures information and IT systems in two main ways: encryption and authentication.

Potential impact on encryption

Encryption protects the confidentiality of information being transmitted or stored on a device, such as a smartphone or USB drive. Threat actors can store encrypted information now to decrypt in the future when a sufficiently powerful quantum computer exists. Therefore, encrypted information with a long lifespan could be at risk. This immediate threat is called the Harvest Now, Decrypt Later (HNDL) threat.

Figure 1: Interception of encrypted information and storing it for future decryption

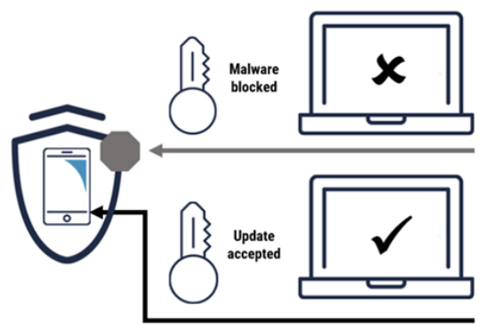


The figure shows a threat actor intercepting encrypted information and storing it over time to decrypt in the future, when sufficiently powerful quantum computers exist.

Potential impact on authentication

Authentication protects the integrity of information and forms the foundation of digital trust online. It ensures that information has not been altered while in transit or in storage, and that it has originated from the correct source, either system or individuals. Threat actors could use a sufficiently powerful quantum computer to impersonate trusted systems, such as an app store or a trusted vendor, to deliver fake software updates or to gain access to systems of interest. Additionally, threat actors could forge certificates used by secure websites, which could allow them to direct legitimate traffic to their invalid sites. Figure 2 demonstrates how threat actors could use powerful quantum computers to impersonate trusted systems to deliver fake software updates and gain access to systems of interest.

Figure 2: Use of powerful quantum computers for impersonation



As shown in Figure 2, the phone blocks malware as it does not contain a valid certificate. However, when an update is signed by a valid certificate and presented to the phone, it accepts and installs it. If a quantum computer can help forge the certificate and that certificate is then used to sign malware, the phone would not know to block it, and the malware would be successfully installed.

Unlike confidentiality, authentication will only be at risk when a sufficiently powerful quantum computer is available.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/00-017-2025E-PDF ISBN 978-0-660-75599-1

Post-quantum cryptography transition

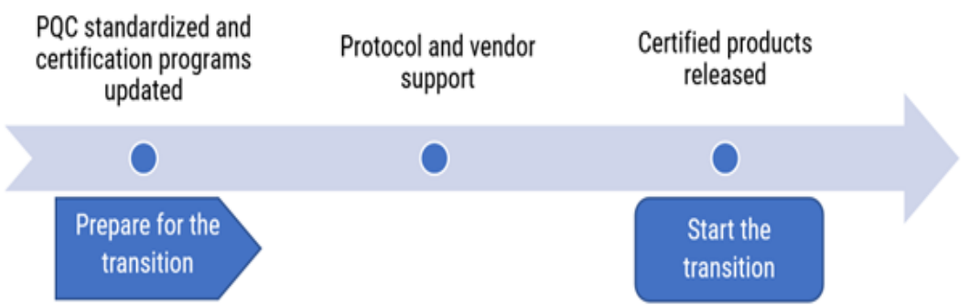
A cryptographic algorithm is quantum-safe if it is secure against a quantum computer. Post-quantum cryptography (PQC) refers to algorithms that are designed to be quantum-safe but that can be run on a conventional computer.

PQC includes algorithms that establish keys for encryption and digital signature schemes for authentication. These are intended to be interoperable with existing communication protocols, software and networks.

To achieve quantum safety, we recommend that organizations transition existing cyber security solutions to use PQC. Many software vendors and cloud service providers are already planning to support PQC in their systems and products. Organizations should confirm PQC roadmaps with vendors and investigate how to transition any custom IT solutions.

However, before PQC solutions can be adopted, the standards for PQC algorithms and the Internet communication protocols that incorporate them need to be finalized. Vendor products implementing these standards should also be validated and certified. The U.S. National Institute of Standards and Technology (NIST) published its initial set of standards for PQC algorithms in August 2024. Organizations such as the Internet Engineering Task Force (IETF) are expected to provide protocol support soon.

Figure 3: Post-quantum cryptography progression



This figure describes the timeline of the PQC progression. During the preparation stage, PQC progression includes standardization and certification program updates, as well as protocol and vendor support. Once certified products are released, organizations are encouraged to leverage those products and to start the PQC transition.

What your organization can do

We recommend that your organization take the following steps to help manage the risks associated with quantum computing advancements and to plan the transition to PQC.

- Identify systems (internal and client-facing), applications, gateways and supporting security components that will need to be cryptographically transitioned
    - Supporting security components can include
        - public key infrastructure (PKI)
        - web servers
        - authorization frameworks
        - authentication directories
        - protected domain name system (DNS)
    - Pay close attention to custom systems and to software developed in-house or provided by smaller vendors
    - This effort is generally called developing a cryptographic inventory
- Identify legacy systems that cannot be transitioned or replaced and develop a risk-managed approach to protect them. An example of a solution would be tunnelling traffic through a PQC-protected virtual private network
- Evaluate the sensitivity and lifespan of your organization's information to identify information that may be at risk (as part of ongoing risk assessment processes). This will help you prioritize the transition work
- Review your IT lifecycle management and develop plans to transition to PQC when available
- Budget for potentially significant software and hardware updates (including support staff) as the timeframe for necessary replacement approaches
- Educate yourself and your teams on the emerging quantum threat and future quantum technologies
- Ask your vendors about their plans to implement PQC or to include PQC in future updates to determine if your organization will need to acquire new hardware or software
- Ensure that your vendor is using standardized, validated cryptography, such as possessing Federal Information Processing Standards (FIPS) accreditation
- Leverage a cryptographic inventory to become cryptographically agile and allow for easier changes to cryptography in deployed systems. For more information refer to Guidance on becoming cryptographically agile (ITSAP.40.018)
- Update and patch systems frequently

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/00-017-2025E-PDF ISBN 978-0-660-75599-1

Alternate quantum-safe solutions

The Cyber Centre recommends migrating to standardized PQC as the best option for organizations to achieve quantum safety. There are alternative quantum-safe solutions, described below, that could provide further cryptographic assurances when combined with PQC. However, these alternatives can significantly increase operational complexity and implementation costs. This means that they might not be feasible replacements for some organizations' current cryptographic systems. Furthermore, these alternatives lack security accreditation options based on recognized standards.

Symmetric key establishment

Symmetric key establishment (SKE) requires secret cryptographic keys to be pre-shared among all users (endpoints) via an out-of-band mechanism, as opposed to a key establishment mechanism such as PQC. In large networks, an online trusted central authority establishes pairwise secret keys. The secure distribution of pre-shared keys and trust in central authority are limitations to SKE adoption.

Quantum key distribution

Quantum key distribution (QKD) exploits the physics of light to establish a secret key between nodes in a network. Nodes require dedicated quantum hardware and direct (fibre-optic or free-space) connection. With current technology, inter-node distances are limited to a few hundred kilometres in optical fibre. Moreover, typical user endpoints (for example, phones, laptops, modems) cannot support QKD-node functionality. Assessing the robustness of QKD systems is a challenge, and international standards bodies are working to develop QKD standards.

Organizations considering the use of alternative quantum-safe solutions should perform their own cost-benefit analyses. For most organizations, the easiest and most cost-effective path to becoming quantum-safe is to implement PQC that supports cryptographic agility.

Cyber Centre efforts

As the technical authority on cryptography in the Government of Canada, the Cyber Centre is taking the following actions to help make Canada quantum safe:

- advising all levels of government, critical infrastructure and other sectors on the quantum threat and the steps to be taken to prepare for the transition to PQC
- taking a lead role in the PQC transition for Government of Canada IT systems in collaboration with other government departments
- working with NIST and other partners to evaluate the security of candidate PQC algorithms and updating product certification programs, such as the Cryptographic Module Validation Program (CMVP), to test PQC implementations
- participating in international standards bodies to ensure standards for Internet communication protocols (for example, TLS and IPsec) meet the cryptographic security and privacy needs of Canadians
- working with vendors to encourage them to adopt NIST-recommended PQC in commercial products and to create tools to support the PQC transition.

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

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada

Cat. No. D97-1/00-017-2025E-PDF ISBN 978-0-660-75599-1