Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Planning for post-quantum cryptography

First published: July 2022
Last updated: August 2023

Introduction

A cryptographically relevant quantum computer (CRQC) will render most contemporary public key cryptography insecure, thus making ubiquitous secure communications based on current public key cryptography technology infeasible. As the creation of a CRQC presents new cybersecurity risks, organisations are encouraged to consider anticipating future requirements and dependencies of vulnerable systems during the transition to post-quantum cryptography (PQC) standards.

Post-quantum cryptography

PQC is a field of cryptography dedicated to the creation and analysis of cryptographic algorithms that derive their security from mathematical problems considered difficult for both classical and quantum computers. PQC offers a low-cost practical path to maintaining the properties of secure communications in the presence of a CRQC.

Selection of PQC algorithms are informed by a National Institute of Standards and Technology (NIST) process. In doing so, candidate PQC algorithms are evaluated and scrutinised in successive rounds to ensure they will meet requirements to protect sensitive or classified data.

The Australian Signals Directorate (ASD) will continue to monitor PQC standardisation efforts, including evaluating the parameters for PQC standardisation. The outcome of these activities will result in updates to ASD-Approved Cryptographic Algorithms in the *Information security manual* (ISM). At this stage, ASD assesses that currently approved cryptography within the ISM provides effective communications security.

ASD will also continue to monitor alternate methods of securing communications in the presence of a CRQC, such as quantum key distribution (QKD). However, the practical limitations of QKD (including transmission distances, specialised hardware requirements and concerns around availability) mean that ASD does not support its use for secure communications at this time.

ASD encourages research, testing and practical trials of PQC algorithms. Research into the further development of PQC algorithms will be a practical and cost-effective step towards securing real-world communications in the presence of a CRQC. More broadly, including outside of cryptographic applications, Australian industry is encouraged to continue research and development of quantum technologies. This should include practical vulnerability research to better understand the risks associated with employing quantum technologies.

Planning for post-quantum cryptography

In planning for a post-quantum computing environment, organisations are encouraged to:

- identify and create an inventory of all applications, IT equipment and OT equipment within their environment that uses public key cryptography
- determine the value of all data within their environment that is currently protected by public key cryptography
- create a transition plan for the use of PQC algorithms within their environment, including the testing and adoption of new PQC algorithms as well as the decommissioning of legacy cryptographic algorithms
- discuss anticipated PQC requirements with vendors or those involved in post-quantum cryptographic research
- educate relevant areas of their organisation on the eventual transition to the use of PQC algorithms and provide any necessary training.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Additional information on post-quantum cryptography is available from the United States' Cybersecurity & Infrastructure Security Agency (CISA)'s Post-Quantum Cryptography Initiative.

Additional information on migrating to post-quantum cryptography is available within the joint CISA, National Security Agency and NIST *Quantum-Readiness: Migration to Post-Quantum Cryptography* factsheet.

Additional information on the PQC standardisation process is available from NIST.

Australia's strategy for the quantum industry and quantum technologies can be found in the Department of Industry, Science and Resources' *National Quantum Strategy*.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate