Migrating to post-quantum cryptography

New guidance from the NCSC helps system and risk owners plan their migration to post-quantum cryptography (PQC).

John H

In 2020, the NCSC published a white paper on Preparing for Quantum-Safe Cryptography. This paper explained the threat that a possible future quantum computer – one much larger, and much more capable, than any that exist today – would pose to a large class of widely deployed cryptography. That cryptography is known as public-key cryptography (PKC). PKC is the enabling technology for secure communication at scale, on the internet and many other networks.

The same white paper also explains why NCSC's recommended mitigation of the quantum computing threat is quantum-safe cryptography, or post-quantum cryptography (PQC). PQC is cryptography that is resistant to attack by quantum computers, and also to today's digital, or classical, computers. Furthermore, PQC offers broadly equivalent functionality to the quantum-vulnerable PKC currently in use, and can be deployed in many of today's devices (including PCs, smartphones etc.) with a software update.

This seems like a simple solution to the threat from a potentially disruptive technology. And conceptually, it is - but the migration to PQC is a very complicated undertaking. This blog explains why.

The quantum computing threat to traditional PKC has been known for decades, and cryptographers in academia, industry and government have been researching PQC intensively since at least the mid-2000s. PQC uses different kinds of mathematics from traditional PKC in the computational problems that underpin its security, but this long period of study has allowed for rigorous analysis of the algorithms that will see widespread adoption.

In 2016, the US National Institute of Standards and Technology (NIST) began a process to select PQC algorithms for standardisation, and that process has just reached a major milestone: the publication of draft standards. Though fundamental security research into PQC will continue, this marks the beginning of

a shift in PQC transition activity from largely a research effort, into a global IT migration project.

Availability of draft standards will enable organisations who manage their own cryptographic estates to take the next steps in PQC migration (for example, by experimenting with implementations of new PQC algorithms to assess performance in important use cases). To support such activities, the NCSC is publishing additional guidance on algorithm choices and protocol considerations.

Migration to PQC requires more than just new algorithms. Protocols and services need to be re-engineered, because PQC typically places greater demands on devices and networks than traditional PKC. This is especially true of the amount of data that needs to be communicated between parties using PQC to secure their communications. International bodies have been working to update protocol standards in parallel with the development of algorithm standards, which is enabling test deployments of PQC by major service providers to understand the potential impacts of the transition.

While not straightforward, upgrading many major internet services (and the apps that access those services) will likely be one of the 'easier' parts of PQC transition. Many legacy and sector-specific protocols, including those used in critical national infrastructure (CNI) will also need to transition to PQC. Additional challenges in these use cases include having to run cryptography on devices with constrained resources, and on legacy systems that are hard to upgrade.

Fortunately, much research in academia and industry has focussed on these difficult use cases, and solutions exist for many situations. For devices or infrastructure that can't be upgraded to PQC, system owners will need to plan for PQC transition as a part of scheduled technology refresh cycles. Over the coming years, NCSC will provide tailored advice to sectors of national importance to support transition to PQC.

Notwithstanding the undertaking that PQC transition represents, nobody should lose sight of the fact that for *many* use cases, PQC is 'just software'. And a lot of *these* use cases are internet services or apps developed and managed by major service providers. In such situations, PQC transition will happen through a software update issued by the provider in question. Individuals and organisations

who rely on major service providers for their cryptography should follow NCSC guidance on keeping software and devices up to date, and PQC transition will happen largely behind the scenes.

For such users, there actually is a fairly simple solution to the quantum threat, but only because of the years of work already done by cryptographers, software engineers, hardware designers, security architects, and many other cyber security specialists worldwide.

John H
Head of Crypt Research

WRITTEN BY

John H
Head of Crypt Research

PUBLISHED

3 November 2023

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

NCSC publications