Preparing for Quantum-Safe Cryptography

An NCSC whitepaper about mitigating the threat to cryptography from development in Quantum Computing.

This white paper sets out the NCSC position on mitigating the threat to cryptography posed by developments in Quantum Computing. It is intended to help technical policymakers make informed decisions as they prepare for quantum-safe cryptography.

Quantum computers

Quantum computers are not just "more powerful supercomputers". They represent a new paradigm in computing.

Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today's digital, "classical", computers. They are, theoretically, capable of performing certain computations that would not be feasible for classical computers.

Quantum computers exist today, but are small and suffer from relatively high error rates in each operation they perform. Current devices are early examples of *Noisy Intermediate-Scale Quantum (NISQ) Computers*, and these are starting to find important applications in quantum simulation and quantum chemistry.

Quantum computers are one of several quantum technologies with applications to cyber security. The NCSC positions on Quantum Key Distribution and Quantum Random Number Generation are set out in the NCSC White Paper on Quantum Security Technologies.

Public-key cryptography

The security of nearly all Internet communications today is based on public-key cryptography.

Public-key cryptography (PKC) is the technology that enables secure communication at scale, on the Internet and other networks.

The principal functions of PKC are:

- *key agreement* – used to establish a shared cryptographic key for secure communication
- *digital signatures* – used to underpin proof-of-identity and trust on a network

The security of all widely-used, "conventional", PKC today relies on the difficulty of the mathematical problems of integer factorisation and calculating *discrete logarithms*. These problems have been extensively studied for decades, and, when suitably parametrised, provide long-term security against classical computers.

However, it has been shown that these mathematical problems would be easy to solve on a large, general-purpose quantum computer, known as a *Cryptographically Relevant Quantum Computer (CRQC)*.

Quantum threat to cryptography

A quantum computer will allow the attacker to read information that has been encrypted in the past, and forge information in the future.

Quantum computers that exist today are not a threat to PKC. Many engineering, physical and mathematical challenges must be overcome before the construction of a CRQC will become possible. Industry, governments and academia around the world are devoting significant resources to research in quantum computing, but there are competing technology choices and the commercial drivers for research are still emerging. As such, it is impossible to

predict with confidence how progress towards large-scale general-purpose quantum computing will evolve.

The threat to key agreement is that an adversary collecting encrypted data today would be able to decrypt it in future, should they have access to a CRQC. Therefore, although a CRQC does not exist today, the possibility of one is a relevant threat now to organisations that need to provide long-term cryptographic protection of data.

Given the amount of old data that would need to be stored by an attacker working today, and the cost of doing so, such an attack is only likely to be worthwhile for very high-value information.

The threat to digital signatures is that an adversary *in possession* of a CRQC could "forge" signatures and impersonate the legitimate private key owner, or tamper with information whose authenticity is protected by a digital signature. This attack should be considered before a CRQC exists, when deploying high-value, root-level public keys that are intended to have a long operational lifetime.

In contrast with PKC, the security of *symmetric cryptography* is not significantly impacted by quantum computers, and with suitable key sizes, existing symmetric algorithms - such as AES - can continue to be used.

Mitigations to the quantum computing threat

Quantum-safe cryptography provides the best mitigation for the quantum computing threat.

Quantum Key Distribution (QKD) mitigates the quantum threat to key agreement using properties of quantum mechanics, rather than hard mathematical problems, to provide security. However, QKD requires specialist hardware, and does not provide a way of doing digital signatures. For these reasons, the NCSC does not endorse QKD for any government or military applications.

It is also possible to mitigate the threat to key agreement by using pre-placed symmetric keys in addition to key agreement with conventional PKC. However,

this approach brings key management and usability challenges, and is not suitable as a general-purpose solution for Internet communications.

Quantum-safe cryptography (QSC) replaces the quantum-vulnerable mathematical problems used in PKC with mathematical problems that are believed to be intractable for both classical and quantum computers. Both key agreement and digital signatures can be made quantum-safe, and QSC can be implemented in both software and hardware. The NCSC believes that adoption of QSC will provide the most effective mitigation for the quantum computing threat.

Quantum-safe cryptography

There is unlikely to be a single quantum-safe algorithm suitable for all applications.

Many algorithms for QSC have been proposed. There is large variation in performance characteristics between different algorithms, more so than for conventional PKC. This means that some algorithms will be more suited to particular use-cases than others. Add to this the ever-expanding set of requirements for cryptography, including deployment in constrained devices, and it seems unlikely there will be a single algorithm suitable for all applications.

The drive to standardise QSC algorithms is encouraging much research on all options for QSC, but the security against classical and quantum computing attacks is still better understood for some candidate algorithms than others.

Standardisation of quantum-safe cryptography

NIST standards for quantum-safe cryptography will be available from 2022-24.

In 2016, The National Institute of Standards and Technology (NIST) started a process to standardise quantum-safe algorithms for key agreement and digital signatures. The field of candidate algorithms has been narrowed down and draft

standards are expected in 2022–24. This long period allows for thorough public scrutiny of the various proposals.

There are existing stateful hash-based signature algorithms, like XMSS and LMS, that have niche applications, such as signing firmware. However, these are not suitable for general-purpose use. The NIST process aims to standardise digital signature algorithms suitable for other use cases.

The NIST process draws on cutting-edge research from academia, industry, and government worldwide. NCSC guidance for quantum-safe algorithms will follow the outcome of the NIST process by recommending specific algorithms for representative use cases.

Preparation for transition

Large organisations should factor the threat of quantum computer attacks into their long-term roadmaps.

The NCSC expects that major commercial products and services will transition to QSC once NIST standards are available and protocols (IPSec, TLS, etc.) are updated to support QSC. The recommended course of action for the majority of users is to follow normal cyber security best practice and wait for the development of standards-compliant QSC products.

Organisations that manage their own cryptographic infrastructure should factor quantum-safe transition into their long-term plans and conduct investigatory work to identify which of their systems will be high priority for transition. Priority systems could be those that process sensitive personal data, or the parts of the public-key infrastructure that have certificate expiry dates far into the future and would be hardest to replace.

For organisations needing long-term cryptographic protection, the NCSC can advise on the deployment of suitable mitigations.

There is likely to be a period during which organisations will be required to operate both conventional and quantum-safe cryptography, in order to ease

transition between the two. It will therefore be necessary to continue support for conventional PKC for the interim period.

Additional considerations

Early adoption of non-standardised QSC is not recommended.

Transition to any form of new cryptographic infrastructure is an inherently complex and expensive process that must be planned and managed with care. There are risks to security as systems and cryptographic keys are changed, and risks to business continuity if there are unforeseen dependencies on cryptographic components that require replacement.

Standards bodies such as NIST and ETSI are working with industry to develop guidance for the transition to QSC, which will allow organisations to mitigate risks in QSC transition effectively.

The NCSC cautions against early adoption of non-standardised QSC. The security level may be unverifiable if the product is not based on a standardised algorithm, and such products are unlikely to inter-operate with future standards-compliant products. This could lead to unnecessary expenditure in having to transition a second time to standards-compliant QSC.

Summary

The NCSC recognises the serious threat that quantum computers pose to long-term cryptographic security. QSC using standards-compliant products is the recommended mitigation for the quantum threat, once such products become available.

The NCSC has confidence in the research activity underpinning NIST's QSC standardisation work. Our guidance for QSC algorithms will follow the outcome of

the NIST process, recommending specific algorithms for representative use cases.

Organisations that manage their own cryptographic infrastructure should note the work of ETSI and NIST on planning QSC transition when making long-term investment decisions. Robust and secure transition will take time to plan and deliver, and there is risk in beginning transition to QSC before standards-compliant products are available.

Further reading

Further information and reading materials:

- NCSC White Paper on Quantum Security Technologies
- Getting ready for post-quantum cryptography (NIST Cybersecurity White Paper)
- Migration strategies and recommendations to Quantum Safe schemes (ETSI Technical Report)

PUBLISHED

11 November 2020

VERSION

2.0

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals