WHITEPAPER

Quantum-safe cryptography

This white paper is intended for those who use or build cryptographic products and systems. It describes the threat to cryptography posed by the emergence of quantum computing, and includes guidance for transitioning to systems that will resist this threat.

Long-term cryptographic security

When assessing the security of a cryptographic system it is necessary to consider how long it will be deployed and the lifetime of the data that it will protect.

It is then necessary to determine whether the computational resources that may become available within the lifetime of the system will undermine the required level of security.

For many systems, and particularly for government systems that protect long-lived data, this means looking ahead several decades.

Asymmetric cryptography

The security of current approaches to asymmetric cryptography, as deployed in real-world systems, usually relies on either the difficulty of factoring integers (RSA) or calculating discrete logarithms (Diffie-Hellman, including Elliptic Curve Diffie-Hellman).

These problems have been intensively studied for many years and are believed to be hard to solve using “conventional” computers of the kind that we have available today. Moreover, for appropriate parameter choices they will remain hard to solve using conventional computers well into the future, even when using Moore's Law to predict advances in computational resources.

However, these problems have been shown to be "easy" to solve given a large enough quantum computer.

The quantum threat

There is no guarantee as to when large-scale quantum computers will become a reality, but NIST estimates that the first cryptographically relevant quantum computer could be built by 2030 for a cost of about one billion US dollars [0]. We expect the cost of building a quantum computer to fall rapidly in the years following the development of the first operational machine.

Consequently, quantum computation must be considered as a significant threat when assessing the security of systems that will protect long-lived data.

With that in mind, the NCSC recognises the need to end reliance upon asymmetric cryptography that will become vulnerable to quantum computation, and hence the need to transition to "quantum-safe cryptography": cryptographic primitives and protocols that cannot efficiently be broken using either a conventional or a quantum computer.

Symmetric cryptography

Symmetric cryptography, and also forms of asymmetric cryptography built entirely from symmetric primitives, such as hash-based signatures, are not regarded as being vulnerable to quantum computation, as the best attacks are considered to be infeasible provided one uses large enough key (and block) sizes. In particular, when used with 256-bit keys, the AES block-cipher is currently considered to be safe from attack by any future conventional or quantum computer.

Key agreement a priority

We note that the quantum threat against public-key digital signatures differs from the threat against key agreement algorithms, in the sense that an adversary would need to perform an active attack (which would require access to a quantum computer) to forge a signature, but may passively collect data now and

then break key agreements (to disclose session keys) in the future once a quantum computer becomes available.

This means that transitioning current systems to use quantum-safe key agreement schemes should be considered as a higher priority than transitioning to quantum-safe digital signatures.

Quantum-safe cryptography

Broadly speaking, there are two very different approaches to protecting against the threat posed by quantum computation.

One is quantum key distribution, or QKD, which exploits quantum properties of physical systems, and so requires specialised hardware.

The other is post-quantum cryptography, or PQC, which, as with existing forms of asymmetric cryptography, exploits the intractability of certain mathematical problems, and so can be implemented in hardware or software.

Based on current understanding, we believe that for most real-world communications systems, and particularly for government systems, PQC will offer much more effective and efficient security mitigations than QKD [1].

A range of PQC proposals exist, based on mathematical problems such as finding short or close vectors in lattices, decoding error-correcting codes that have hidden structure, and inverting hash functions. Each of these problems is believed to provide resistance to attacks from both conventional and quantum computers. More specifically, it is possible to construct instances of each of these problems that are believed to be intractable, regardless of the sort of computers an adversary has at their disposal.

No one-size-fits-all solution

Because cryptography is used in such a wide range of situations, and because new requirements continue to arise, it is unlikely that there will be a "one-size-fits-all" solution to the global question of quantum-safe transition, but rather that different approaches will be more or less suited to different scenarios.

Although there is much academic research into the security and efficiency properties of various post-quantum cryptographic schemes, currently it is only possible to make broad statements rather than specific recommendations.

Quantum-safe key agreement

Post-quantum key agreement schemes based on error-correcting codes, such as McEliece, seem to offer conservative levels of security, but at the expense of very large keys. Consequently, such approaches are unlikely to be appropriate for applications where bandwidth or memory is constrained.

By comparison, lattice-based cryptography, which includes various approaches based on the learning with errors paradigm, seems to offer a good balance between security, key sizes, and computational efficiency.

Other approaches to post-quantum key agreement, including those based on multi-variate systems of equations, and isogenies between elliptic curves, are less well understood.

Quantum-safe signing

General purpose quantum-safe digital signatures (that is, signature schemes that can be used to efficiently sign an arbitrary number of messages under a particular public key) are currently less well developed than quantum-safe key agreement algorithms.

For niche cases where signing keys may be long-lived and of high equity, such as firmware signing, we recommend the use of hash-based signatures, as their security is well understood. However, hash-based signatures work best in scenarios where it is possible to anticipate or bound the number of items to be signed by any given key in order to make sensible decisions about computational trade-offs.

Standardisation and transition

Work towards standardising post-quantum public-key primitives and protocols is underway in international standards bodies such as NIST [2] and ETSI [3].

For the majority of users, waiting for the emergence of such standards and protocols is the recommended approach.

The NCSC will provide additional guidance for those protecting long-lived or highly classified national security information.

Don't jump too soon

We urge caution against transitioning too soon: given the current lack of clarity around which variants will offer the best balance of security and performance, and which specific parameter sets to use, a considered upgrade process will allow time for researchers and other stakeholders to reach consensus on which options and timescales are most appropriate for various applications.

Complex communications systems take a long time to develop and are difficult to upgrade. Unnecessary haste and over-reliance on new approaches to cryptography may introduce costly security weaknesses.

During the transition phase we expect there to be a significant period of time where traditional approaches to asymmetric cryptography will be deployed in conjunction with post-quantum cryptography. Consequently, it will be necessary to continue to support traditional approaches to asymmetric cryptography for the foreseeable future.

Summary

The NCSC acknowledges the serious threat posed by quantum computation to currently used forms of asymmetric cryptography, particularly key agreement algorithms.

We strongly recommend a considered approach to transitioning to quantum-safe cryptography, as and when algorithms and parameter sets become stable and are standardised.

Further Reading

For more information about different quantum-safe cryptographic primitives readers are referred to the ETSI white paper, "Quantum Safe Cryptography and Security" [4]. For more information on quantum technologies, including quantum computation and the threat it poses to cryptography, readers are referred to the recent Blackett review, "The Quantum Age: Technological Opportunities" [5].

References

[0] NIST Interagency Report (NISTIR) 8105: Report on Post-Quantum Cryptography, April 2016

[1] NCSC White Paper: Quantum Key Distribution, October 2016

[2] NIST Post-Quantum Crypto Project, August 2016

[3] ETSI Quantum-Safe Cryptography (QSC) Industry Specification Group (ISG)

[4] ETSI White Paper No. 8 Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, June 2015

[5] Government Office for Science, Quantum Technologies: Blackett review, November 2016

PUBLISHED

30 November 2016

VERSION

1.0

WRITTEN FOR ⓘ

Cyber security professionals