Next steps in preparing for post-quantum cryptography

Guidance to help organisations and CNI providers think about how to best prepare for the migration to post-quantum cryptography (PQC).

This guidance helps system and risk owners in commercial enterprises, public sector organisations and critical national infrastructure providers to think about how to best prepare for the migration to post-quantum cryptography.

Background

In our 2020 white paper, Preparing for Quantum Safe Cryptography, we set out the threat that quantum computers pose to current cryptography, and the work by organisations such as the US National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI) to counter this threat.

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. Although advances in quantum computing technology continue to be made, quantum computers today are still limited, and suffer from relatively high error rates in each operation they perform.

In the future, it is possible that error rates can be lowered such that a large, general-purpose quantum computer could exist. It is, however, impossible to predict when this may happen as many engineering and physical challenges must be overcome first. If such a computer could exist in the future, most traditional public key cryptography (PKC) algorithms in use today will be vulnerable to attacks from it. A quantum computer that will be able to run these attacks is referred to as a cryptographically-relevant quantum computer (CRQC).

These traditional PKC algorithms include:

- algorithms based on integer factorisation such as RSA

- algorithms based on the discrete logarithm problem such as Finite Field Diffie-Hellman, ECDH, DSA, ECDSA, EdDSA

These algorithms are primarily used for key establishment (used to agree a shared cryptographic key for secure communication) and digital signatures (used to underpin proof-of-identity and trust on a network).

For key establishment and encryption, there is a risk from an attacker collecting and storing data today and decrypting it at some point in the future. Given the cost of storing vast amounts of old data for decades, such an attack is only likely to be worthwhile for very high-value information. This means that for organisations that need to provide long-term cryptographic protection of very high-value data, the possibility of a CRQC in the future is a relevant threat now.

The threat to digital signatures is that an adversary in possession of a CRQC could forge signatures to 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, particularly when deploying keys for high-value trust anchors 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 existing symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. The security of hash functions such as SHA-256 is also not significantly affected, and secure hash functions can also continue to be used.

The NCSC advice remains that the best mitigation against the threat of quantum computers to traditional PKC is post-quantum cryptography (PQC), also called quantum-safe cryptography or quantum-resistant cryptography. PQC algorithms will replace the vulnerable PKC algorithms used today for both key establishment and digital signatures. The security of PQC algorithms is based on mathematical problems that are believed to be intractable for both classical and quantum computers. These algorithms will not necessarily be drop-in replacements for the current PKC algorithms in protocols or systems, so system owners should begin planning for the migration to PQC.

Implications of PQC migration for users and system owners

For users of commodity IT, such as those using standard browsers or operating systems, the switchover to PQC will be delivered as part of a software update and should happen seamlessly (ideally without end-users even being aware). To ensure devices are updated to PQC when it is available, system owners should ensure they follow the NCSC's guidance on keeping devices and software up to date.

System owners of enterprise IT, such as those who own IT systems designed to meet the demands of a large organisation, should communicate with their IT system suppliers about their plans for supporting PQC in their products.

For a minority of systems with bespoke IT or operational technology, such as those that implement PKC in proprietary communications systems or architectures, choices will need to be made by system and risk owners as to which PQC algorithms and protocols are best to use.

Technical system and risk owners of both enterprise and bespoke IT should begin or continue financial planning for updating their systems to use PQC. **PQC upgrades can be planned to take part within usual technology refresh cycles once final standards and implementations of these standards are available**.

Towards PQC standardisation

Since 2016, NIST has been running a process to standardise PQC algorithms, backed up by academic scrutiny from the international cryptography community. This process has been followed closely by standards-defining organisations including:

- the Internet Engineering Task Force (IETF), who have been working on updating their protocols to be resistant against a quantum computer
- ETSI, who have been producing migration and deployment guidance

NIST has selected one algorithm for key establishment:

- ML-KEM (CRYSTALS-Kyber)

and three algorithms for digital signatures:

- ML-DSA (CRYSTALS-Dilithium)

- SLH-DSA (SPHINCS+)
- FALCON

There are also two already standardised stateful hash-based signature algorithms, which also offer protection against a quantum computer but can only be used in a subset of use cases. These are Leighton-Micali Signatures (LMS) and eXtended Merkle Signature Scheme (XMSS).

The draft standards for ML-KEM, ML-DSA and SLH-DSA were released in August 2023. Final standards for these algorithms are expected in 2024. The draft standards for FALCON will be released in the future.

The NIST draft standards will allow developers to test these algorithms in their systems and develop plans for deploying these algorithms when the final standards are released. The draft standards are subject to changes before the final standards are released, so there is a risk that implementations based on draft standards may not be compatible with the final standards. **For this reason, the NCSC strongly advises that operational systems should only use implementations based on the final NIST standards**.

These algorithms will need to be implemented in protocols before they can be used on the internet and in other networks. The IETF is in the process of updating the most widely-used security protocols. This includes ensuring that PQC algorithms can be incorporated into key exchange and signature mechanisms in existing protocols such as TLS and IPsec. IETF implementations of post-quantum protocols are subject to change until they are published as RFCs. The NCSC strongly advises that operational systems should use protocol implementations based on RFCs, and not on Internet Drafts.

Choosing algorithms and parameters for your use cases

The following table gives the NCSC recommended algorithms, their functions, and specifications:

ML-KEM Key establishment algorithm NIST Draft - FIPS 203	
ML-DSA Digital signature algorithm NIST Draft - FIPS 204	
SLH-DSA Digital signature algorithm for use cases such as signing firmware and software NIST Draft - FIPS 205	
LMS Digital signature algorithm for use cases such as signing firmware and software NIST SP 800-208	
XMSS Digital signature algorithm for use cases such as signing firmware and software NIST SP 800-208	

The above algorithms support multiple parameter sets that offer different levels of security. The smaller parameter sets generally require less power and bandwidth, but also have lower security margins. Conversely, the larger parameter sets provide higher security margins, but require greater processing power and bandwidth, and have larger key sizes or signatures. The level of security required can vary according to the sensitivity and the lifetime of the data being protected, the key being used, or the validity period of a digital signature. The highest security level may be useful for key establishment in cases where the keys will be particularly long lived or protect particularly sensitive data that needs to be kept secure for a long period of time. It may also be useful for digital signatures where the keys have a particularly long lifetime, such as in a root of trust.

Note that:

- **All of these parameter sets provide an acceptable level of security for personal, enterprise and OFFICIAL-tier government information.**

- ML-KEM and ML-DSA are algorithms suitable for general purpose use. **The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases**.
- Users may wish to use the smaller parameter sets in situations where key/signature size is a consideration, or where it may help address performance issues, such as in constrained devices.

Hash-based signatures

Hash-based signatures such as SLH-DSA, LMS and XMSS rely on different security assumptions than ML-DSA and FALCON. They are **not** suitable for general purpose use as the signatures are large and the algorithms are much slower than ML-DSA. However, these algorithms may be a good fit for use cases such as signing firmware and software where speed is not a bottleneck.

For LMS and XMSS, the security of these algorithms critically depends on users correctly managing the state (that is, knowing which one-time keys have been used for signing so it can be guaranteed that they are never used again). Cases where state management is a more tractable problem include firmware and software signing. ETSI have created advice on how to do this in their Technical Report TR 103 692 v1.1.1 . LMS and XMSS should only be used in situations where it is possible to manage state in a trusted manner for the lifetime of the signing key.

SLH-DSA provides a more robust alternative for situations where it may be difficult or impossible to guarantee a one time key is not re-used, as state management is not straightforward and mistakes can be detrimental to security. This increased robustness comes with significantly larger signature sizes and greater signing time than either LMS or XMSS, although the verification performance is similar.

LMS and XMSS are available as final standards, whereas, as of August 2023, SLH-DSA is available as a draft standard.

Post-quantum traditional (PQ/T) hybrid schemes

A PQ/T hybrid scheme (as defined in this IETF Draft) is one that combines one (or more) PQC algorithms with one (or more) traditional PKC algorithms where all component algorithms are of the same type (for example, a PQC signature algorithm combined with a traditional PKC signature algorithm to give a PQ/T hybrid signature).

There are greater costs to PQ/T hybrid schemes than those with a single algorithm. PQ/T hybrid schemes will be more complex to implement and maintain and will also be less efficient. However, there may sometimes be a need for a PQ/T hybrid scheme, due to **interoperability**, **implementation security**, or constraints imposed by a **protocol** or system:

Interoperability

In a large network, it will be necessary to adopt a phased approach to the introduction of PQC. This will lead to a period where both PQC and traditional PKC algorithms need to be supported simultaneously. Flexible protocols incorporating PQ/T hybrid schemes will make it possible for systems with different security policies to interoperate, and should also allow for a migration to a PQC-only future.

Implementation security

PQC is an emerging technology and, while NIST has a robust process to ensure the security of the PQC algorithms, it will take time for assurance in implementations of these algorithms within protocols and systems to be developed. Therefore, users may wish to consider using PQC in combination with traditional PKC with the aim of building a system which remains secure, even if one of the implementations is insecure.

Protocol constraints

Some protocols may have technical constraints that mean it is difficult to remove the traditional PKC algorithm when adding support for PQC. An example of this is the need to avoid IP layer fragmentation in IKEv2.

Additional considerations for PQ/T hybrid schemes

There are many ways to combine a PQ key establishment algorithm with a traditional key establishment algorithm to obtain a PQ/T hybrid key establishment scheme. For example, using a PQ/T hybrid key establishment mechanism such as in the draft for Hybrid TLS (draft-ietf-tls-hybrid-design-09) or at the protocol level such as in the design for IKE (RFC 9370). These two protocols have been modified to incorporate PQ/T hybrid schemes in a relatively simple and backwards-compatible way.

PQ/T hybrid key establishment mechanisms should be designed carefully to ensure the hybridisation mechanism does not allow additional attacks. As of November 2023, advice on how to do this is currently in development by ETSI.

Proposed PQ/T hybrid schemes for authentication can be significantly more complex than those used for confidentiality, due to the need to make sure both signatures verify in a robust way. There has also been significantly less research activity into PQ/T schemes for authentication than for confidentiality, and there is not yet guidance or a consensus on how to do this in a secure way.

Public key infrastructures (PKIs) make use of authentication algorithms to create, store, verify and revoke digital certificates. Within a PKI, it is difficult to change an individual signature algorithm in isolation. PQ/T hybrid authentication within a PKI requires either a PKI which can generate and sign traditional and post-quantum digital signatures, or two parallel PKIs (one for traditional and one for post-quantum digital signatures). This additional complexity and the difficulty in migrating PKIs mean that a single migration to a fully post-quantum PKI is preferred to adopting an intermediate PQ/T hybrid PKI.

Recommendations on PQ/T hybrid schemes

In the future, if a CRQC exists, traditional PKC algorithms will provide no additional protection against an attacker with a CRQC. At this point, a PQ/T hybrid scheme will provide no more security than a single post-quantum algorithm but with significantly more complexity and overhead. **If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure, and it should be used within a flexible framework that enables a straightforward migration to PQC-only in the future**.

With this in mind, technical system and risk owners should weigh the reasons for and against PQ/T hybrid schemes including interoperability, implementation security, and protocol constraints, as well as the complexity, cost of maintaining a more complex system, and the need to complete the migration twice (once to a PQ/T hybrid scheme and again to PQC-only algorithms as a future end state).

Summary

- Most PKC algorithms in use today will be vulnerable to a CRQC. The best mitigation against the threat of quantum computers to traditional PKC is PQC.
- The security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with appropriate key sizes can continue to be used.

- PQC upgrades can be planned to take place within usual technology refresh cycles.
- ML-KEM (Kyber) and ML-DSA (Dilithium) are algorithms selected for standardisation by NIST that are suitable for general purpose use. All proposed parameter sets provide an acceptable level of security for personal, enterprise and OFFICIAL-tier government information. The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases.
- The NCSC strongly advises that operational systems should only use implementations based on final standards.
- If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure that allows a straightforward migration to PQC-only in the future.

PUBLISHED

3 November 2023

VERSION

1.0

WRITTEN FOR

Public sector

Large organisations

Cyber security professionals