Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

8 December 2025

Technology brief

Quantum computers and post-quantum cryptography

1 Introduction

For several years, the media has reported extensively on quantum computers, their potential risks to current cryptographic methods and the need for quantum-secure cryptography. This coverage has sparked uncertainty and concern that current cryptographic methods might no longer be secure. Against this backdrop, this document outlines what a quantum computer is and why it poses challenges to the security of certain cryptographic methods. It also explains what is meant by post-quantum cryptography (PQC), what progress has been made in this field, and where further action is needed.

2 Quantum computers

While conventional computers are based on classical physics, quantum computers rely on the principles of quantum mechanics. The processing of quantum mechanical states is based on quantum mechanical principles, such as superposition or entanglement. Rather than using bits, which can have a value of zero or one, quantum computers use quantum bits, or qubits. A qubit is the simplest non-trivial quantum system. Its state can be described as a superposition of the basis states zero and one. Due to their ability to form superpositions, registers made up of several qubits can represent and process many basis states simultaneously, i.e. in 'quantum parallel'. This opens up new approaches and possibilities for computation.

Due to their intricate design and unique characteristics, quantum computers excel at solving problems that leverage quantum parallelism and are beyond – or extremely costly to solve using – the capabilities of traditional computers. These problems include simulation tasks in the natural and engineering sciences, optimisation problems in logistics and finance, and machine learning in artificial intelligence. Of particular relevance for this technology brief are the mathematical problems on which the security of certain cryptographic methods is based.

Although quantum computers that can be used for a wide range of applications (known as 'universal quantum computers') are still largely theoretical, major efforts are being made to develop them. This research and development is not only taking place in major technology

companies such as IBM, Google, Microsoft, Amazon and Intel, but also in universities, spin-offs and start-ups. Current systems can incorporate a few hundred qubits (e.g. IBM's 2022 Osprey processor with 433 qubits), or up to a few thousand (e.g. Caltech's 6,100-qubit array).[1] IBM plans to build a quantum computer with 100,000 qubits by 2033.[2] If this ambitious target is met, it would mark a significant step towards a cryptographically relevant quantum computer (CRQC). However, it is not yet clear how powerful a quantum computer must be to qualify as a CRQC. One reason for this uncertainty is that many quantum algorithms require fault-tolerant qubits (also known as logical qubits). Because the physical qubits currently in use are highly prone to errors, one approach to error correction is to combine many physical qubits into a single logical qubit. This process is known as quantum error correction (QEC), and significant progress has been made in this area in recent years. Another approach seeks to create fault-tolerant qubits directly using quantum-optical methods. Because several different development paths are being pursued, it is currently not possible to make reliable predictions about when a CRQC will actually become available.

In any case, the development and construction of a CRQC would have far greater consequences than the 'quantum supremacy' often proclaimed in the media. This term, 'quantum supremacy', simply means that a quantum computer can solve a specific mathematical problem more efficiently than a conventional supercomputer. How significant such a result is depends heavily on the problem in question and cannot be generalised. Likewise, the claims made by D-Wave Systems should be taken with a grain of salt.[3] Although the computers marketed by this company are equipped with thousands of qubits, these computers are not universal ('gate-based') quantum computers. Rather, D-Wave Systems computers can only be used for certain optimisation tasks, achieving hardly discernible performance gains over conventional computers.[4]

3 The challenge

As the name suggests, a CRQC could be used to solve the mathematical problems on which the security of certain cryptographic methods is based. This primarily affects asymmetric cryptosystems such as Rivest–Shamir–Adleman (RSA), which is based on the difficulty of factoring large numbers, as well as systems such as the Diffie–Hellman key exchange, the Digital Signature Algorithm (DSA) and related cryptosystems, which rely on the difficulty of the discrete logarithm problem, including on elliptic curves. As early as 1994, Peter W. Shor demonstrated how these mathematical problems could be solved using a sufficiently powerful quantum computer, thereby compromising the cryptosystems built on them [1]. Unlike conventional computers, Shor’s algorithms run in polynomial time on a quantum computer and are therefore considered efficient in terms of complexity theory.

Because the asymmetric cryptosystems affected by Shor's algorithms are now used almost everywhere, the emergence of a CRQC would have far-reaching consequences for their security. In this context, the term 'Q-Day' is sometimes used to describe the point in time when CRQCs become available to attackers.

In order to solve cryptographically relevant problems, quantum algorithms require at least a number of logical qubits that grows linearly with the bit length of the corresponding keys. In

[1] It should be noted that different technologies also have different properties in terms of qubit stability and error correction capabilities, meaning that the number of qubits cannot always be directly compared. This applies in particular to Caltech's 6,100 qubits. The corresponding qubit array is not comparable to a quantum computer.

[2] https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[3] https://www.dwavesys.com

[4] https://dl.acm.org/doi/10.1145/3459606

the case of RSA, this is typically a few thousand. However, because of the error-correction methods currently available, the number of physical qubits required is many times higher. If IBM can realise its vision, the quantum computer planned for 2033 (with its 100,000 qubits) could potentially become relevant for asymmetric cryptosystems.

Although a quantum computer can in principle also be used to break symmetric cryptography, the known methods have less serious consequences for security. In 1996, Lov K. Grover proposed an algorithm that would reduce the effort required for a brute-force search of an n-bit key from 2^n to $2^{n/2}$ [2]. While this would essentially create vulnerabilities for pseudorandom number generators, Message Authentication Codes and symmetric encryption, doubling key length would be a relatively easy way to mitigate this problem. The same applies to cryptographic hash functions, which do not use keys but whose collision resistance is also affected by Grover's algorithm. Here too, the risk can be mitigated by doubling the hash length. As a result, the security of symmetric cryptosystems and cryptographic hash functions is only marginally affected by the existence of a CRQC. Moreover, Grover's algorithm has only been demonstrated in theory so far, and it is proven to be optimal – meaning that no faster quantum algorithm exists for solving unstructured search problems.[5] In practice, however, it seems that achieving the theoretical speed-up (i.e. reducing from 2^n to $2^{n/2}$ on a real quantum computer is extremely difficult. This makes the recommendation to double key and hash lengths less compelling.

Although a CRQC does not yet exist, attackers may already be collecting encrypted data on a large scale with the intention of decrypting it once suitable quantum computers become available. This type of attack is known as a 'harvest now, decrypt later' (HNDL) attack. The possibility of such attacks is the primary motivation for developing practical countermeasures as soon as possible. There is also a risk that authentication keys could be broken in the future. This would allow attackers to impersonate other users and to forge digital signatures. Such attacks are known as 'trust now, forge later' (TNFL). However, because authentication processes are usually short-lived and digital signatures can be renewed at any time using new keys, TNFL attacks are considered less critical. Current efforts therefore focus primarily on preventing HNDL attacks.

4 Solutions

In view of the extensive research and development activities of the aforementioned technology companies to advance the construction of universal quantum computers, and given the possibility of HNDL (and, in some cases, TNFL attacks), it is sensible to consider how cryptosystems can be designed to resist quantum computers. This subfield of cryptography is known as post-quantum cryptography (PQC). It is currently attracting considerable interest. PQC focuses on asymmetric cryptography. There is barely any need for action with regard to symmetric cryptography since – as mentioned above – all symmetric cryptosystems in use today can continue to be used if the key size is doubled.[6] This doubling compensates for the implications arising from Grover's algorithm. In other words, the resulting security would remain largely intact. Specifically, this means that the AES-256 encryption protocol should be used instead of AES-128. There are minimal disadvantages in day-to-day use, if any. In particular, the speed of encryption and decryption does not depend decisively on the key length.

[5] https://arxiv.org/abs/quant-ph/9701001

[6] Of course, such doubling is only useful up to a certain key length. For example, once a key length of 256 bits is reached, doubling is no longer required, because even if the effective key length were halved it would still be more than 128 bits.

The aim of PQC is therefore to design asymmetric cryptosystems that rely on mathematical problems recognised as difficult and practically unsolvable, even for quantum computers, but that are nevertheless efficient to implement. To this end, the United States' National Institute of Standards and Technology (NIST) has been running a widely observed international competition since 2017.[7] In 2022, NIST announced the first four winners for asymmetric encryption or key encapsulation mechanisms (KEMs) and for digital signatures.[8] The corresponding standards are FIPS 203[9] for ML-KEM (CRYSTALS-Kyber), FIPS 204[10] for ML-DSA (CRYSTALS-Dilithium) and FIPS 205[11] for SLH-DSA (SPHINCS+), or are still being finalised for FALCON (the names in brackets and FALCON refer to the original identifiers of the corresponding PQC algorithms). However, this work is far from complete. The competition is ongoing, and in 2025, for example, NIST selected HQC as an alternative to ML-KEM for standardisation. In addition, NIST launched a second competition for digital signatures in 2023. It is therefore currently unclear whether, and when, other methods may also come into play as potential standards. In addition to the NIST, other organisations such as the Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO) are also working to standardise quantum-resistant algorithms.

From today's perspective, it would certainly be wrong to replace all the asymmetric methods currently in use with PQC methods, as only time will tell how secure they really are. Many PQC methods and algorithms are based on relatively new cryptographic ideas that are not yet fully understood. In addition, PQC methods are more complex to implement, which means that weaknesses and vulnerabilities, including to side-channel attacks, must be expected. Rather than replacing conventional methods entirely, it is advisable to choose a complementary approach that combines conventional methods with PQC methods. These are often referred to as hybrid methods or combiners. For instance, the end-to-end encrypted messaging services Signal and iMessage use a combination of the traditional elliptic-curve-based Diffie–Hellman key exchange and ML-KEM. Hybrid approaches are also being developed for digital signatures and the associated certificates, although the technical challenges in this area are greater.

Quantum cryptography (in particular quantum key distribution, which is virtually its only practical application), and quantum random number generators, are explicitly not considered solutions to the problem discussed in this document. Both technologies are thematically related and can also be used for commercial products. However, there have been so many practical problems associated with quantum cryptography and, in particular, quantum key distribution, that neither the US National Security Agency (NSA)[12] nor a consortium of four European authorities[13] recommends their use. By contrast, there are areas of application for quantum random number generators in which they offer certain advantages over the pseudo-random number generators that are normally used.

---

[7] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[8] The abbreviation KEM stands for 'key encapsulation mechanism'. This is a mechanism that enables a cryptographic key to be sent securely to a party. The key to be transferred is selected at random and packaged (or 'encapsulated') with the sender's public key in such a way that it can only be unpacked again with the recipient's private key. Ideally, a key exchange method would be needed that can be used in a non-interactive way, like Diffie–Hellman. However, no such method is currently available, which is why KEMs are used instead.

[9] https://csrc.nist.gov/pubs/fips/203/final

[10] https://csrc.nist.gov/pubs/fips/204/final

[11] https://csrc.nist.gov/pubs/fips/205/final

[12] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[13] https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution

5 Recommendations and next steps

Given the formidable technical challenges associated with building a CRQC, we do not consider it to be an immediate concern.[14] Nevertheless, the risk of large-scale HNDL (an in certain cases TNFL) attacks argues strongly in favour of implementing PQC. However, any migration should be approached carefully.[15] Implementing short-term or hasty solutions too quickly would likely weaken overall security, even if they initially appear to offer protection against attacks by quantum computers. A corresponding migration is a lengthy process that must be planned accordingly in the context of the current standardisation of quantum-resistant algorithms.[16]

Work is being done on several fronts to standardise PQC algorithms and to integrate them into security protocols and products. Signal and iMessage were already mentioned earlier. As early as the mid-2010s, Google attempted to integrate Frodo (a predecessor of Kyber and ML-KEM) into Transport Layer Security (TLS) and has been working on various PQC extensions for its products ever since.[17] Similar efforts can be seen at Microsoft, Cloudflare and other tech companies, which means that a significant share of internet traffic secured with TLS is already protected using PQC algorithms. Finally, developers of open-source software are also working to integrate PQC algorithms, as illustrated by the example of OpenSSH.[18] Essentially, the more open the system is, the more challenging and time-consuming adding PQC becomes. In this sense, the use of PQC in standardised security protocols for the Internet (e.g. IPsec, TLS) also poses major challenges for the IETF and its working groups. Nevertheless, good progress is being made, with PQC-specific extensions already available for many internet security protocols.

All efforts in the direction of PQC ultimately serve the interests of achieving cryptographic agility and should also be viewed in this light. Systems and applications must be designed and implemented in such a way as to ensure that a variety of cryptographic protocols and algorithms can be run and supported. This form of agility is already important today and will probably become even more crucial in the future. Cryptographic agility requires a software architecture designed for it. In the case of hardware implementations, which are typically used where performance and or security requirements are higher, the scope for agility is generally limited. From the perspective of cryptographic agility, software implementations therefore have an advantage. In any case, it makes sense to document cryptographic components, methods and algorithms in a software bill of materials (SBOM) or cryptography bill of materials (CBOM). This type of inventory is also important regardless of PQC considerations, given the growing prevalence of supply chain attacks. Without understanding an organisation's reliance on cryptographic methods, algorithms and their implementations, it will not be possible to establish and implement an effective security strategy. Therefore, creating an SBOM or CBOM is a sensible first step in addressing this topic. Everything else then depends on the CBOM and on the specific characteristics and objectives of the organisation or company in question.

---

[14] Many scientific publications overstate the progress made in building a CRQC by relying on unrealistic and contrived numerical examples (see, for example, the article on the Cryptology ePrint Archive at https://eprint.iacr.org/2025/1237.pdf).

[15] During a panel discussion on Migrating to Post-Quantum Schemes held at the 2023 RSA Conference, panellist Adi Shamir gave a fitting suggestion: "If you want to switch to post-quantum algorithms, walk, don't run" (https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes).

[16] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[17] https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

[18] https://www.openssh.org/pq.html

Abbreviations

AES	Advanced Encryption Standard
NCSC	National Cyber Security Centre
CBOM	Cryptography Bill of Materials
CRQC	Cryptographically Relevant Quantum Computer
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIDO2	Fast IDentity Online 2
FIPS	Federal Information Processing Standards (US)
HNDL	Harvest Now, Decrypt Later
HQC	Hamming Quasi-Cyclic
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
KEM	Key Encapsulation Mechanism
ML	Module Lattice
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PQC	Post-Quantum Cryptography
RSA	Rivest–Shamir–Adleman
SBOM	Software Bill of Materials
SLH	Stateless Hash
SSH	Secure Shell
TLS	Transport Layer Security
TNFL	Trust Now, Forge Later
DDPS	Federal Department of Defence, Civil Protection and Sport

References

[1] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 1994, Santa Fe, NM, pp. 124–134

[2] Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, May 1996, pp. 212–219