Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

16 May 2024

Technology brief

Quantum computers and post-quantum cryptography

1 Introduction

In 2019, the scientific journal Nature ran an article that proclaimed quantum supremacy[1]. It was most likely at this point that the media began extensive coverage of quantum computers, alerting us to the dangers and threats to current cryptographic protocols and highlighting the need for more secure, quantum-resistant cryptography. Some of this reporting also stoked considerable uncertainty and fears that existing cryptographic protocols are inadequate. Against this backdrop, the present technology brief will explain what a quantum computer is, why its existence may affect the security of certain cryptographic protocols, what the term post-quantum cryptography (PQC) means and where action can be taken.

2 Quantum computers

While conventional computers obey the laws of classical physics, quantum computers operate under the laws of quantum mechanics. The processing of quantum mechanical states is based on quantum mechanical principles, such as superposition or entanglement. Instead of using binary digits (bits) as a unit of information, quantum computers use quantum bits (qubits). One qubit represents the simplest non-trivial quantum system, which can essentially take on an infinite number of different states and even be in these states simultaneously (i.e. 'quantum parallel'). This opens up new computation prospects and approaches.

[1] https://www.nature.com/articles/s41586-019-1666-5

Due to its complex design and characteristic features, a quantum computer can be used primarily to solve tasks that would otherwise be too complex or impossible to perform with conventional computers (e.g. simulation tasks in the field of natural sciences and engineering, optimisation tasks in logistics and finance, machine learning in the context of artificial intelligence and solving mathematical problems that underly the security of certain cryptographic protocols). While universal quantum computers are still mostly a theoretical construct, intensive and generously funded efforts are being made to build them. The corresponding R&D work is not only being pursued by large technology companies such as IBM, Google, Microsoft and Intel, but also by universities, spin-offs and start-ups. Although the number of qubits that can be placed on a chip today is still in the range of a few hundred (e.g. 433 qubits in the case of the Osprey quantum processor presented by IBM in 2022), IBM is planning to build a 100,000-qubit quantum computer by 2033.[2] If this ambitious target can be reached, we will be in the realm of what can be referred to as a cryptographically-relevant quantum computer (CRQC). We do not yet know how big a quantum computer needs to be in order to qualify as a CRQC. This is partly due to that fact that the physical qubits currently being used are highly error-prone and require many quantum algorithms to correct for these errors. The main approach adopted thus far has been to group multiple physical qubits together into a single error-tolerant qubit, referred to as a logical qubit. This process is referred to as quantum error correction (QEC) and considerable progress has been made fairly recently in this area. A competing approach uses quantum optics methods to create error-tolerant qubits directly.

Regardless of how it comes about, the development and creation of a CRQC will have more far-reaching implications than the quantum supremacy proclaimed back in 2019, which we mentioned earlier. After all, the term quantum supremacy only means that a quantum computer can solve a mathematical problem faster than a conventionally operating supercomputer. Of course, the import of this statement depends on the underlying problem to a large extent and is therefore not applicable in all cases. Likewise, the claims made by the company D-Wave Systems[3] should also be taken with a grain of salt. Although the computers marketed by this company use processors comprised of thousands of qubits, these computers are not universal 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 Problems

As the name suggests, a CRQC would be able to solve mathematical problems that form the basis for the security of certain cryptographic approaches. This would include asymmetric cryptosystems, such as Rivest-Shamir-Adleman (RSA), which rely on the fact that factorisation of large prime numbers requires significant computing power (i.e. ‘the factoring problem’). It would also include approaches, such as Diffie-Hellman key exchange, Digital Signature Algorithm (DSA) and analogous cryptosystems, which rely on the staying power of elliptic curves (i.e. ‘the discrete logarithm problem’). As early as 1994, Peter W. Shor demonstrated how a sufficiently large quantum computer or CRQC would be able to solve these mathematical problems and thus crack the cryptosystems based on them [1]. Unlike with conventional computers, Shor’s algorithms on a quantum computer would run in polynomial time and thus be efficient in terms of computational complexity theory.

---

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

3 https://www.dwavesys.com

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

Because the asymmetric cryptosystems affected by Shor's algorithms are practically ubiquitous, the emergence of a CRQC would have grave security implications. The term 'Q-Day' is sometimes used in this context, referring to the moment in time when CRQCs are built and become available to hackers.

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 the case of RSA, this is typically a few thousand. Given the error correction methods available today, the number of physical qubits required is a multiple of this. However, if IBM manages to achieve its vision, the quantum computer planned for 2033 (with its 100,000 qubits) will pose a problem for many asymmetric cryptosystems.

Although a quantum computer can in theory also be used to break symmetric cryptography, the impact on the security of the corresponding protocols is less serious. In 1996, Lov K. Grover proposed an algorithm that could speed up the exhaustive search of a key n-bit in length from 2^n to $2^{n/2}$ [2]. While this would essentially create vulnerabilities for pseudorandom number generators (PRNGs), Message Authentication Codes (MACs) and symmetric encryption, doubling key sizes would be a relatively easy way to mitigate this problem. The security of symmetric cryptography would therefore only marginally be affected by the existence of a CRQC. Moreover, Grover's algorithm is optimal, i.e. no further improvements are expected here.

Although it is currently not possible to build a CRQC, the large-scale collection of encrypted data still poses a problem as a CRQC could be used at a later date to decrypt this data. In this context, the expression 'Harvest Now, Decrypt Later' (HNDL) is used. The potential existence of HNDL attacks is the main reason why practicable approaches and solutions need to be found as quickly as possible.

4 Solutions

Given the amount of R&D being done by the aforementioned technology companies to build universal quantum computers, and the possibility of HNDL attacks, it makes sense to think about how to construct cryptosystems that would be resistant to quantum computers. This branch of cryptography is known as post-quantum cryptography (PQC) and 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 remain in use if the key size is doubled.[5] 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. The disadvantages in terms of practical use - if any - are very slight (in particular, encryption and decryption throughput is not heavily dependent on key size).

[5] Of course, such doubling is only useful and necessary up to a certain key size. From 256 bits, doubling is no longer needed in any case.

The aim of PQC is therefore to construct asymmetric protocols and cryptosystems that rely on mathematical problems recognised as difficult and practically unsolvable, even for quantum computers, but that are nevertheless efficient to implement. In 2017, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) launched a competition that has been very closely observed worldwide.[6] In 2022, the NIST announced the first four winning algorithms for asymmetric encryption schemes, key encapsulation mechanisms (KEMs[7]) and digital signatures, namely: CRYSTALS–KYBER, CRYSTALS–Dilithium, SPHINCS+ and FALCON. These four algorithms will become part of the NIST's post-quantum cryptographic (PQC) standards, which are now in the final stages of completion: FIPS 203 for ML-KEM and FIPS 204 for ML-DSA, which specify the lattice-based algorithms CRYSTALS-Kyber and CRYSTALS-Dilithium; FIPS 205 for SLH-DSA, which specifies the hash-based signature algorithm SPHINCS+; and finally, the digital signature algorithm FALCON, which is also lattice-based, will be standardised at a later point in time. Several code-based algorithms will now be pitted against each other in a new competition round for KEMs. And last but not least, the NIST launched a second competition for digital signatures in 2023. It is therefore not clear at present whether and when other primitives will also be taken into account 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.

As things currently stand, it would be wrong to replace all asymmetric cryptographic primitives used today with PQC-based ones. Only the time will tell how secure they really are, as many PQC protocols and quantum-resistant algorithms are based on cryptographic ideas that are still relatively new and not yet fully understood. Instead, supplementing and complementing these primitives would be a more sensible and expedient option. Here reference is made to 'hybrid' approaches and 'hybrid combiners'. For example, instant messaging services Signal and iMessage provide end-to-end encryption by combining the post-quantum key encapsulation mechanism CRYSTALS-Kyber with a conventional Elliptic-curve Diffie-Hellman (ECDH) key exchange scheme. Hybrid protocols should also be considered in the future for digital signatures and corresponding certificates.

Quantum cryptography (or quantum key distribution as the best-known or even the sole quantum-cryptographic task) and quantum random number generators (QRNGs) are expressly not presented as possible solutions to the problems discussed in this technology brief. 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 that neither the U.S. National Security Agency[8] (NSA) nor a grouping of four European agencies[9] advocate their use. Because QRNGs are only one of a number of possible technical implementations for random number generators, there is insufficient added value here that would justify mandating their use.

---

6 https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

7 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. A key exchange method similar to Diffie-Hellman (also non-interactive) would actually be preferrable. However, such a method is not yet available and KEMs are therefore used instead.

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

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

5 Recommendations and action steps

Given the formidable technical challenges associated with building a CRQC, we do not consider it to be an immediate concern. Nevertheless, the risk of large-scale HNDL attacks argues strongly in favour of implementation of PQC. However, a cautious and well-considered approach is advisable here.[10] The rapid deployment of short-term and possibly hasty solutions, or rather incomplete solutions, would weaken security in a way that would outweigh the benefits of achieving superficial resistance to attacks from 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.[11]

Work is being done on several fronts to standardise quantum-resistant algorithms and to bake these algorithms into security protocols and products. Signal and iMessage were already mentioned earlier. Google also attempted to incorporate Frodo (a predecessor algorithm to Kyber) into Transport Layer Security (TLS) back in the mid-2010s and has been working on various PQC extensions for its products ever since. The same applies to Microsoft, Cloudflare and other technology companies. 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 constitutes a major challenge for the IETF and its working groups.

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. The scope for agility is usually more limited in hardware implementations, where higher performance and/or more stringent security are needed. In any case, it makes sense to document cryptographic primitives, protocols and algorithms in a software (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.

[10] 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).

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

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
FIPS	Federal Information Processing Standards (US)
HNDL	Harvest Now, Decrypt Later
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
TLS	Transport Layer Security
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