General Intelligence and
Security Service
*Ministry of the Interior and
Kingdom Relations*

Prepare for the threat of quantum computers

How do you prepare for the threat of quantum computers?

For years, the advent of the quantum computer has been predicted to be able to break certain cryptography. This poses risks in the area of information security. The Netherlands National Communications Security Agency (NLNCSA) of the General Intelligence and Security Service (AIVD) is closely monitoring developments and conducting research in order to provide timely products and solutions to these security risks.

Do you work with sensitive information? In this publication, the NLNCSA shares its views on the threat posed by quantum computers and tells you what measures you can take to protect yourself against it. In our earlier publication from 2014 [1], we already advised to be vigilant for the development of the quantum computer.

What is the NLNCSA?

The NLNCSA aims to keep the Netherlands digitally secure from state threats and other Advanced Persistent Threats (APTs). We are unique in that we combine our specialist security knowledge with the special intelligence position we have as part of the General Intelligence and Security Service (AIVD). We work closely with our security partners Military Intelligence and Security Service (Dutch: Militaire Inlichtingen- en Veiligheidsdienst, MIVD), National Coordinator for Security and Counterterrorism (Dutch: Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV) and National Cyber Security Centre (Dutch: Nationaal Cyber Security Centrum, NCSC). Together we help the central government and the vital sector to protect special and sensitive information such as state secrets.

Quantum computers: a genuine risk?

For decades, it has been known that insights from quantum mechanics can be used to attack the most commonly used asymmetric cryptography with a quantum computer. For example, RSA and elliptic curves commonly used in HTTPS. In this paper we refer to this form of cryptography as “classical cryptography”. The current quantum computers do not yet have enough computing power to be a serious threat to the current cryptography. By the term quantum computer, we mean an advanced quantum computer that can break classical cryptography.

Experts consider the probability small but real that quantum computers will already be powerful enough by 2030 [2,3] to break current cryptographic standards. For sensitive information, the NLNCSA considers a small chance sufficient reason to take appropriate measures. Until then, there are also risks for today's cryptography. The data you send or store now in encrypted form can be intercepted and decrypted at a later time by a quantum computer. Data that will still be sensitive in 2030 and must remain secret should therefore already be encrypted with cryptography that protects against attacks with a quantum computer.

Therefore, we advise you to work on a migration plan for a quantum-resistant solution in time. Migrating to new cryptographic mechanisms is a complex process that takes time. If you do not take this into account and take measures too late, then you risk that your sensitive or confidential information will still be decrypted.

Store now, decrypt later

Because confidential information often has a long period of confidentiality, the threat of a quantum computer is real. Encrypted data that is intercepted and stored now can be decrypted by a quantum computer at a later date. This could happen before the confidentiality period of your information expires.

How do you protect yourself against the threat of quantum computers?

- Prepare now to migrate to quantum-resistant cryptography.
- Use key lengths of 256 bits for symmetric cryptography.
- Migrate to Post-Quantum Cryptography as soon as the standards are available. In the meantime, study hybrid constructions.
- With Quantum Key Distribution alone, you can't protect sensitive information against quantum computers.

How can you protect your organisation against the threat of quantum computers?

The NLNCSA recommends the use of PQC

To safeguard your sensitive or confidential data, the Netherlands National Communications Security Agency recommends the use of Post-Quantum Cryptography (PQC) in combination with an existing asymmetric algorithm (hybrid construction, see box). We see this as the best way to protect against attacks from quantum computers.

The NLNCSA has great confidence in the security and application of this form of cryptography, even though there are no international standards yet. Where implementing PQC is not yet possible, we recommend adding symmetric cryptography to existing applications as an interim solution.

***Post-Quantum Cryptography* (PQC)**

Post-Quantum Cryptography (PQC) is a form of cryptography based on mathematical problems that cannot effectively be cracked by a quantum computer. New PQC standards are currently being developed that could replace the current asymmetric standards.

To be sure of the security of these new standards, these forms of cryptography need time to mature. With scientific research, confidence in the security of these standards is increased. This is a process that takes time. The National Institute of Standards and Technology (NIST) in the United States started an open process to develop international standards back in 2016. These standards are expected around 2024. Research program PQCRYPTO-EU is also investigating forms of Post-Quantum Cryptography.

It is also possible to use PQC in combination with classical cryptography. We call this a hybrid construction (see box).

Switching to a quantum-proof solution too soon can cost a lot of time and money. Too late is also not an option either because of the risk that your sensitive information is vulnerable. That is why the NLNCSA recommends working out a migration strategy now. You can read how to do this below.

Hybrid constructions

There is sufficient confidence in protection through the PQC algorithms, but the implementations are still very immature. This means that it is not yet certain that there are no errors in the implementations that could break the algorithm.

One solution to better protect against threats from a quantum computer right now, without losing protection, is a hybrid construction. This is a combination of classical cryptography (elliptic curves or RSA) with PQC. The PQC part provides resistance to quantum attacks, while the classical part ensures that the security is never weakened.

How do you prepare a migration to PQC?

Before you migrate to PQC, it is important to make an inventory of your data to be protected, its confidentiality period and the cryptography you use. This will give you a good understanding of your assets and systems.

What information should you keep secret or confidential? How long should it remain secret? And is it protected by asymmetric or symmetric cryptography, or a combination of the two? This helps you to determine which cryptographic solution is best suited to your organisation.

You can also make an estimate of the time it will take to switch to PQC and check whether the equipment your organisation uses can be transferred to PQC. In addition, you can map out what is required for this and what bottlenecks you encounter. Examples include: equipment that is difficult to update, required interoperability with different parties, low bandwidth, or limited computing power. The last two examples can cause bottlenecks because PQC algorithms are often less efficient than classical algorithms. For most applications, this does not present insoluble problems.

Finally, you can take into account the transition to PQC as part of your lifecycle management when purchasing new equipment. Discuss in advance with your vendor whether there are solutions that support PQC or have an additional layer of symmetric cryptography. When purchasing new equipment, also consider the *crypto-agility* of this equipment. This is very important because it indicates how flexibly the equipment can handle different cryptographic algorithms and key lengths.

The American NIST has written a comprehensive whitepaper on PQC migration [4].
TNO and the NCSC also have a handy guide on migration to PQC [5, 6].

What if my data needs to be quantum secure now?

Have you determined that your confidential information needs to be stored in a quantumproof manner right now? If so, we recommend the following:

1. Supplement all systems whose security depends on asymmetric cryptography with a layer of symmetric cryptography.
2. If this not possible, or is your information so sensitive that an extra layer of symmetric cryptography does not provide sufficient security, then switch to PQC in a hybrid construction (see page 7). You can use many different algorithms that vary in performance, efficiency and security. For PQC, we recommend the most secure algorithms, such as Frodo [7] or McEliece [8]. This is in line with what BSI, the German equivalent of the NLNCSA, recommends [9], among others. These algorithms provide the most protection against new attacks in the future, but are not the most efficient.
3. Do the above options offer no or insufficient solution? Then you can consider whether the risk of taking your systems offline outweigh the security risk you run with a quantum computer.

What other security options are there?

Symmetric Cryptography
With symmetric cryptography (such as AES), your information is less vulnerable to attack by a quantum computer. With a strong algorithm like AES, symmetric cryptography with a key length of 256 bits provide sufficient cryptographic resistance against a quantum computer. Within your organisation, you can increase existing symmetric key lengths to 256 bits. Symmetric cryptography can also be used to supplement your existing security. With some VPN products, it is possible to add an extra layer of security with a symmetric shared secret. You can also tunnel connections secured by asymmetric cryptography through a symmetrically secured connection. In this way, any intercepted information is still protected against an attacker with a quantum computer. What is important here is that the shared symmetric secret is exchanged in a quantum-proof manner, for example by exchanging it offline. The NLNCSA can offer government organisations advice on approved and other products

Quantum Key Distribution (QKD)
Quantum Key Distribution (QKD) exchanges digital keys using techniques from quantum mechanics. With this method of key exchange, eavesdropping by a third party is always detected.

With QKD, the identity of the sender and receiver is not established. So you have a secure connection, but you do not know with whom. Adding authentication is a must, because otherwise you run the risk of a so-called man-in-the-middle attack. Adding authentication is possible with PQC or symmetric cryptography and effectively makes QKD obsolete.

QKD is cited as a provably secure method for key exchanges. Currently, there are no QKD implementations with appropriate security proof. For example, this may be an incomplete proof by proving only part of the application. Sometimes assumptions are made about the hardware that are not realistic or that the hardware cannot meet.

In addition, for QKD, distance is limited by requiring an optical point-to-point connection. This can be solved in practice by using networks with trusted points or in the future with quantum repeaters. These are not attractive alternatives to PQC in terms of cost and scalability.

Finally, QKD is not a full-fledged alternative to PQC because it focuses only on key exchange and not on other applications such as digital signatures.

Due to the limitations in functionality and the current immaturity of the technology, QKD without PQC is unsuitable for securing sensitive information against the threat of quantum computing, according to the NLNCSA. The NLNCSA's position against QKD is more broadly supported by international counterparts of the NLNCSA, as shown, for example, in the paper on QKD by the French ANSSI [10] but also in [11, 12, 13].

Any questions?

Do you have questions about securing sensitive information from the threat of quantum computing? Call us at: +31 79 3205050 and ask for NLNCSA. We'd love to help you make your organisation more resistant.

References

1 AIVD. ‘Informatieblad Quantumcomputers’ (2014).

2 M. Mosca, M. Piani. ‘Quantum threat Timeline report 2020’ (2021).

3 TNO. ‘Migration to quantum-safe cryptography. About making decisions on when, what and how to migrate to a quantum-safe situation.’ (2020).

4 NIST. ‘Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.’ (2021).

5 NCSC. ‘Factsheet Postkwantumcryptografe. Bescherm uw data van vandaag tegen de dreiging van morgen.’ (2017)

6 TNO. ‘Migration to quantum-safe cryptography. About making decisions on when, what and how to migrate to a quantum-safe situation.’ (2020).

7 E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila. ‘FrodoKEM. Learning With Errors Key Encapsulation’, https://frodokem.org (version 4 June 2021).

8 M.R. Albrecht, D.J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurisch, R. Misoczki, R. Niederhagen, K.G. Paterson, E.Persicheti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C.J. Tjhai, M. Tomlinson, W. Wang. ‘Classic McEliece: conservative code-based cryptography’, https://classic.mceliece.org (version 10 October 2020).

9 Bundesamt für Sicherheit in der Informationstechnik. ‘BSI – Technical Guideline. Cryptographic Mechanisms: Recommendations and Key Lengths’. (2021).

10 ANSSI. ‘Technical position paper: QKD. Should Quantum Key Distribution Be Used for Secure Communications?’. (2020).

11 BSI, ‘Quantenkryptografe’,https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie.html (version 14 July 2021). (German)

12 NCSC, ‘Whitepaper Quantum security technologies’, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, version 1.0, 24-03-2020.

13 NSA, ‘Quantum Key Distribution (QKD) and Quantum Cryptography (QC)’, https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/ (version 14 July 2021).

General Intelligence and Security Service (AIVD)

PO Box 20010
2500 EA The Hague
T (079) 320 50 50

September 2021