National Cyber Security Centre
Ministry of Security and Justice

Post-quantum cryptography

Protect today's data against tomorrow's threats

Factsheet FS-2017-02 | version 1.1 | 31 August 2017

The arrival of quantum computers could have large consequences for organisations that work with encrypted data. Using a quantum computer, it becomes possible to decrypt data that is secured with the most popular forms of cryptography. After the arrival of quantum computers, data that is currently sufficiently secured will not be so anymore. The consequences are even more serious than that: encrypted data could be intercepted now, in order to decrypt it with a quantum computer in the future. The NCSC recommends organisations to draft a plan of action. This plan of action should clarify in which timeframe measures need to be taken to protect data against quantum computers.

What is a quantum computer?

A quantum computer is a new type of computer that is based on quantum mechanical principles. They are still in development, but the concept of quantum computers dates back to the eighties. Several parties are working to build advanced quantum computers.[1]

The inner workings of a quantum computer are fundamentally different from a classical computer. For example, a quantum computer will be much faster at solving some problems than a classical computer. This makes the development of quantum computers valuable for solving complicated scientific problems.

Target audience

Information security officers
IT managers

The following parties have contributed to this factsheet:

Betaalvereniging Nederland, KPN CISO, Ministry of Security and Justice, NL-NCSA, Peter Schwabe (RU), PQCRYPTO-EU (Tanja Lange)

[1] Source: https://www.aivd.nl/publicaties/publicaties/2014/11/20/informatieblad-over-quantumcomputers

The properties of quantum computers also enable breaking the most popular forms of cryptography.

Cryptographic algorithms used for key exchange and generating digital signatures are based on mathematical problems that are supposedly hard to solve. A classical computer has a hard time solving these problems, but to a quantum computer they are significantly less complicated. An attacker with a quantum computer can therefore decrypt a large part of the encrypted information that is sent via the internet.[2] Using a quantum computer, it is also possible to compromise the integrity of digital signatures.

Quantum computers that are advanced enough to perform these tasks do not yet exist. The TU Delft expects to build an advanced quantum computer between 2030 and 2040. Companies like Google, Microsoft, IBM and Intel are also working to develop quantum computers, and it appears large intelligence services are interested as well.[3]

At first, governments and scientists will be the primary users of this new technology. The probability that consumers will have a physical quantum computer in their living room is - also given the cost - very small.

On the other hand, it's quite probable that quantum computers will become available as cloud applications soon after their arrival. This makes the technology - including its capacity for breaking popular cryptography - available to individuals.

In the rest of this factsheet, the term 'quantum computer' will denote an advanced quantum computer, which is capable of breaking the most popular forms of cryptography.

What does the arrival of quantum computers mean for my organisation?

The arrival of quantum computers has large consequences for organisations that work with encrypted data. More specifically, this holds for data that can be intercepted by a third party. This is data, for example, that is transmitted via the internet or that is published online after a data breach.

Using a quantum computer, data that is encrypted using the most popular forms of cryptography can be decrypted. Therefore, data that is currently sufficiently secured will not be so anymore after the arrival of quantum computers.

Using a quantum computer, it will also become possible to compromise the integrity of digital signatures. An attacker with a quantum computer can work out the private key that is used for a digital signature. Using this private key, the attacker can generate new signatures and thereby impersonate someone else.

To ensure the continued confidentiality of data and integrity of digital signatures after the arrival of quantum computers, forms of cryptography are necessary that are resistant to quantum computers.

Quantum algorithms

Breaking cryptography on a quantum computer is done with special algorithms that can only run on a quantum computer: quantum algorithms.

Shor's algorithm is a quantum algorithm that breaks popular cryptographic algorithms for key exchange and digital signatures (asymmetric cryptography). Cryptographic algorithms such as RSA, ECDSA and Diffie-Hellman are no longer safe then.

Using *Grover's algorithm*, another quantum algorithm, attackers can search faster for encryption keys or passwords.[4] Grover's algorithm, however, is relatively slow. When sufficiently long keys or passwords are used, Grover's algorithm is not effective. Research project PQCRYPTO-EU therefore recommends the use of 256 bit keys for AES.[5]

Why should my organisation care today about the arrival of quantum computers?

Encrypted data may be intercepted already today, in order to decrypt it with a quantum computer in the future. This data is stored awaiting the quantum computer, for example by parties that are interested in your organisation. After the arrival of quantum computers, this data is no longer sufficiently secured, as the cryptographic algorithm that was used can be broken. Data that exists today and that should be protected after the arrival of quantum computers, should therefore already be additionally secured.

What does the NCSC recommend?

The NCSC recommends organisations to draft a plan of action. This plan of action should clarify in which timeframe measures need to be taken to protect data against quantum computers.

Does the plan of action state that your organisation should already start additionally securing data? Take a look at the latest

[2] Source: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
[3] Source: https://www.aivd.nl/publicaties/publicaties/2014/11/20/informatieblad-over-quantumcomputers

[4] The term 'encryption' covers all forms of symmetric encryption, such as AES, Salsa20, 3DES and RC4.
[5] See https://pqcrypto.eu.org/recommend.html for the most recent recommendations.

recommendations of PQCRYPTO-EU.[6] This project researches forms of cryptography that remain secure after the arrival of quantum computers.

Does no data exist within your organisation that should be secured until after the arrival of quantum computers? In that case, wait before switching to new forms of cryptography. Waiting has the advantage that better and better forms of cryptography that can resist attacks with a quantum computer will become available.

Digital signatures

In some cases, digital signatures should already be additionally protected as well.

Digital signatures are used in products that will still be used after the arrival of quantum computers. Devices in the Internet of Things are an example, in the sense that they may verify external commands using digital signatures.

When quantum computers exist, these products can no longer reliably verify digital signatures. An attacker with a quantum computer can forge a digital signature in order to give these devices malicious instructions.

It is important to switch to stronger forms of cryptography for generating and verifying these signatures, because of the long service life of these products.

The plan of action depends on several factors

- **The estimated moment upon which quantum computers become available.** No one knows exactly when people will succeed in building a quantum computer. Nevertheless, estimate the moment when you think quantum computers will exist. Choosing this moment is, in essence, a form of risk acceptance. The later the moment you choose, the more likely it is that quantum computers will exist before that date.

- **The time during which data has to remain secure.** Differences exist between organisations and between types of data in how long they have to remain secure. Some data has a lifetime until after the moment that the first quantum computer becomes available. This data has to be protected with cryptography that cannot be broken by a quantum computer. Other data has a shorter lifetime or is no longer sensitive by the time quantum computers arrive.

- **The way in which data is used.** Different types of data are used and secured in different ways. Every type of data will have different performance demands on the cryptography that is used. Consider for example the difference between data exchange between two computers and the data exchange of a smartcard.

- **The implementation time.** This is the time the organisation needs to switch to new forms of cryptography. This time is needed to for example formulating policy and replacing hardware and software.

- **The availability of new forms of cryptography.** Research is currently underway into the development of cryptography that is secure after the arrival of quantum computers. It will be some time yet until cryptography that is secure against quantum computers is standardised and is implemented in hardware and software.

[6] See https://pqcrypto.eu.org/recommend.html for the most recent recommendations.

Perspective for action

- Gather involved people in your organisation. Determine together the norms to which secured data and/or digital signatures should adhere. This differs between different types of data. Determine which types of data are exchanged within your organisation, how long these should be protected and in which way these are exchanged. Connect these efforts to existing methods for data classification within your organisation.
- Determine the moment upon which you expect quantum computers to become available.
- For each type of data, make a timeline that clarifies when the organisation should start additional data protections. When making this decision, consider the time that data should be protected, the estimated moment at which suitable, new cryptography that is secure against quantum computers becomes available, the time necessary to implement this solution and the period left to wait before acting.
- Determine the plan of action. In it, establish the suitable form of cryptography for each category of data in your organisation.

How can data already be protected against quantum computers?

The development of cryptographic algorithms that are secure against quantum computers yields - in time - better and better solutions.

Post-quantum cryptography is the collective noun for all forms of cryptography that remain secure after the arrival of quantum computers. This includes both symmetric and asymmetric forms of cryptography.

Beside the research of the aforementioned European research project PQCRYPTO-EU, the National Institute of Standards and

Technology (NIST) of the United States has opened a request[7] to develop standardised forms of post-quantum cryptography.

Encryption

When encrypting data, a larger key is needed to make the cryptographic algorithm that is used secure against quantum computers. AES-128 is, for example, strong enough to secure against an attacker with classical means, but not against an attacker with a quantum computer. Research project PQCRYPTO-EU therefore recommends 256 bit keys for AES.[8]

Key exchange

All popular forms of cryptography that are used for key exchange are no longer secure after the arrival of quantum computers.

Exchanging keys manually can be a good solution if it is necessary to start additionally protecting data today. However, this solution is not always feasible. In the case of communication between two data centers, one can imagine using manual key exchange - with smartcards, for example. For regular internet communications, this solution is less suitable.

In addition to full replacement, you can also supplement existing cryptographic key exchange with manual key exchange. The outer layer of encryption is done with the cryptographically exchanged key. Within this layer, encryption is performed with the manually exchanged key. The outer layer protects against attackers with classical means, whereas the inner layer protects against attackers with a quantum computer.

Digital signatures

Methods of post-quantum cryptography used for digital signatures and key exchange currently know several limitations. These limitations concern the performance or usability of these methods.[9] Furthermore, the security of many proposals for these methods of post-quantum cryptography are not yet sufficiently supported by mathematical research.[10] Finally, these forms of post-quantum cryptography need to be implemented in popular hardware and software.

Research project PQCRYPTO-EU recommends the use of SPHINCS-256 as a method for *stateless* digital signatures and XMSS as a method for *stateful* digital signatures.[11]

The cryptographic algorithms used to generate digital signatures can be *stateful* or *stateless*. *Stateful* algorithms are only usable to securely generate digital signatures in a limited number of cases. They require faithfully maintaining a so-called state, an internal status value, which makes their application much more complex. *Stateless* algorithms do not have this limitation.

Quantum Key Distribution

At this time, Quantum Key Distribution is not a suitable alternative to post-quantum cryptography.[12]

In contrast to traditional cryptography, which is based on hard-to-solve mathematical problems, Quantum Key Distribution is a form of cryptography that is based on physical principles.

However, Quantum Key Distribution still has several limitations.[12] The security properties of Quantum Key Distribution are currently insufficiently understood. Also, Quantum Key Distribution requires the use of very costly hardware, which both the sender and the receiver of the data need to possess. Finally, the geographic range of this hardware is limited.

Finally

The arrival of quantum computers may seem like a long way off, but the consequences for organisations that work with sensitive data are present today. Even though the supply of alternative forms of cryptography is still limited, it is essential to start thinking today about forms of cryptography that your organisation has to implement, and the time that it needs to do so.

[7] See http://csrc.nist.gov/groups/ST/post-quantum-crypto/workshops.html
[8] See https://pqcrypto.eu.org/recommend.html for the most recent recommendations.
[9] Bron: https://www.aivd.nl/publicaties/publicaties/2015/04/15/bereid-u-voor-op-de-komst-van-de-quantum-computer
[10] Bron: https://www.aivd.nl/actueel/nieuws/2014/11/20/quantumcomputer-vereist-nieuwe-cryptografische-oplossingen
[11] See https://pqcrypto.eu.org/recommend.html for the most recent recommendations and further specifications.
[12] See further https://www.ncsc.gov.uk/information/quantum-key-distribution

Publication
Nationaal Cyber
Security Centrum (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-02 | version 1.1 | 31 August 2017