POSITION PAPER

MIGRATION TO QUANTUM-SAFE CRYPTOGRAPHY

ABOUT MAKING DECISIONS ON WHEN, WHAT AND HOW TO MIGRATE TO A QUANTUM-SAFE SITUATION.

TNO innovation for life

AUTHORS
Ir. F. Muller
drs. ir. M.P.P. van Heesch

CONTENTS

1. MANAGEMENT SUMMARY

Globally, great effort is being put into building a quantum computer. Quantum computers are anticipated to outperform conventional (super)computers in solving mathematical problems that lie at the foundation of commonly used cryptosystems. An efficient algorithm to solve the problem of the factorisation of large integers, for example, renders the RSA cryptosystem insecure and, for this reason, quantum computers form a very serious threat against this widely used cryptosystem. Similar conclusions can be drawn for many other cryptosystems that are currently deployed. The advent of a quantum computer will therefore have an enormous impact on cryptography, whereby the migration to quantum-safe solutions is inevitable. TNO has drawn up this report to assist organisations in making decisions on when, what and how to migrate to a quantum-safe situation.

Quantum computers already exist today. The existing technology is, however, not yet powerful enough to break cryptography. Although it is extremely difficult to predict future technological developments, some leading experts estimate that there is a likelihood of 50% or more that RSA-2048 will be broken by a quantum computer in 15 years' time; see [GRI19]. Events that will be useful in monitoring the advances in quantum computing are the improvements in the quality of quantum gates and in error correction on quantum bits along with so-called quantum supremacy, i.e. the quantum computer actually solving a problem faster than a classical computer.

Besides the technological developments, two additional factors play an important role in determining the urgency of mitigating this threat. First, one must determine how long information must remain private. In particular, if an attacker is only capable of decrypting private information tomorrow, it does not mean that our IT infrastructure is secure today; with a store-now-decrypt-later attack the information will still get compromised. Second, migrating an IT infrastructure is a complex task that takes time. All in all, even though the threat of a quantum computer may still be more than a decade away, action is already required today.

Various steps need to be taken in order to prepare your IT infrastructure for the advent of the quantum computer. We have clustered them into three stages:

1. **The ramping-up stage.** In this stage you prepare your organisation to get started with the transition to a quantum-safe IT infrastructure by getting acquainted with the subject and forming a dedicated project group.
2. **The initial no-regret moves.** These include consulting the asset inventory, drawing up a migration plan and updating the symmetric cryptography and hash functions that are not strong enough to withstand the quantum computer.
3. **The replace-asymmetric-crypto stage.** In this last stage you select the quantum-safe asymmetric algorithms that you want to replace currently used algorithms, and migrate the IT infrastructure to either hybrid (i.e. combined classical and quantum-safe algorithms) or quantum-safe only solutions.

This is summarised in Figure 1 on the next page.

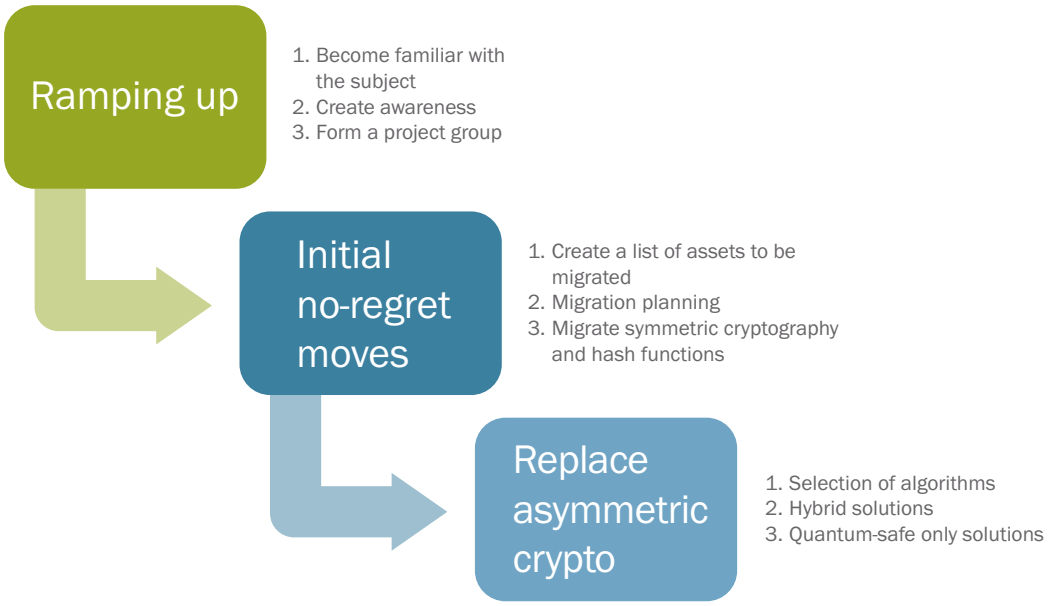


Figure 1: Plan of action for successful migration

There are various types of quantum-safe algorithms, also called post-quantum algorithms, that are currently being developed and tested. Additional to the research that is being conducted, standardisation of post-quantum cryptography is an important process. Various standardisation bodies are working towards the standardisation of post-quantum cryptography; the efforts led by NIST are the most important at this moment; see [NIST PQC]. The first draft standards of NIST are expected to be available between 2022 and 2024.

To conclude, although quantum computers that can break currently used cryptography are still years away, actions to mitigate this threat are already required. Steps you can take now are to start with the ramping-up phase and the initial no-regret moves mentioned above. We advise starting with these two steps as soon as possible to avoid failing to comply with requirements on data confidentiality by migrating too late.

The costs of the entire process can be minimised by expressing interest in quantum-safe products to vendors at an early stage and requiring crypto agility (flexibility in cryptographic algorithms and key lengths) for all products to be purchased from now on.

2. INTRODUCTION

In many locations in the world research is being conducted on building quantum computers. Quantum computers promise the ability to compute solutions to problems that are currently regarded to be infeasible, such as factoring very large numbers. This ability poses a threat to many cryptographic systems that are currently believed to be secure.

The basic building blocks of quantum computers are qubits (or quantum bits). Contrary to 'classical' bits, that can only assume the values '0' and '1', qubits can be in the states '0' or '1', but also in infinitely many superposition states of '0' and '1'. Moreover, qubits display the property that they can have so-called entanglement with each other, a particular correlation, which enables computations to be done with qubits in parallel. These properties enable a quantum computer to solve particular problems exponentially faster than classical computers.

The number of qubits on which current versions of quantum computers can operate is ever increasing. At the time of writing this document, a record number of 72 computing qubits has been reported; see [Google QC]. The estimates of how fast this number is going to rise vary roughly between doubling once every two years to doubling every year.

The future abilities of the quantum computer present a serious threat for many of the currently used cryptographic algorithms. Attacks on secret key (i.e. symmetric) algorithms become quadratically faster by running Grover's algorithm on a quantum computer; see [Grover]. Thus this algorithm halves the present security level. All currently standardised public key (i.e. asymmetric) algorithms, such as RSA, DSA and Elliptic Curve algorithms, can be broken by running Shor's algorithm on a sufficiently large quantum computer; see [Shor94]. As a consequence, all secret key algorithms will have to be used with at least a 256-bit key and, much more seriously, all public key algorithms currently in use will have to be replaced by algorithms that are resistant to the attacks enabled by the quantum computer. Currently cryptosystems that are conjectured to be resistant against attacks using quantum computers are being standardised. They are known as post-quantum cryptography (PQC), quantum-safe cryptography (QSC) or sometimes as quantum-resistant cryptography (QRC).

TNO has drawn up this report to assist organisations in making decisions on when, what and how to migrate to a quantum-safe situation. When the migration should take place is the subject of Chapter 3 below. The 'what' will be discussed in detail in Chapter 4. Chapters 5 and 6 deal with the 'how'. Chapter 7 contains the summary.

3. TIMING OF MIGRATION

3.1 WHEN WILL CURRENT PUBLIC KEY CRYPTO BE BROKEN?

The number of qubits that quantum computers have available for computations is ever increasing. At the time of writing this document, the reported record number of qubits is 72; see for example [Google QC]. The estimates of how fast this number is going to rise vary roughly between doubling every two years to doubling every year, see e.g. [NAS19] and [QCR20].

To attempt to estimate when current public key cryptography will be broken, an example of 2048-bit RSA has been worked out below. To break 2048-bit RSA, using the best implementation of Shor's algorithm, requires $2n+2 \approx 4100$ qubits [Takahashi06]. However, this is strongly dependent on the lifetime of the qubits. The quality of a qubit degrades quickly over time; therefore error correction is necessary, which requires many more qubits. The factor that is usually taken for this is 1000; a thousand times the number of qubits needed to do a computation (logical qubits) is necessary for the error correction; see e.g. [Franke19]. Therefore, to break 2048-bit RSA, around 4,000,000 (physical) qubits are needed.

In Table 1 below an estimate is made of when this many physical qubits will be available in a quantum computer, using the assumptions, for the two columns, that the number of qubits doubles every two years, or every year. The year in which RSA-2048 under a particular assumption is broken is highlighted.

Year	Number of qubits in quantum computer in case of doubling every two years	Number of qubits in quantum computer in case of doubling every year
2019	72	72
2021	144	288
2023	288	1,152
2025	576	4,608
2027	1,152	18,432
2029	2,304	73,728
2031	4,608	294,912
2033	9,216	1,179,648
2035	18,432	**4,718,592**
2037	36,864	
2039	73,728	
2041	147,456	
2051	**4,718,592**	

Table 1: Estimate of growth of number of qubits of quantum computers

Table 1 shows, for example, that if the number of qubits doubles every year (as is currently reported by D-Wave systems, one of the main players, see [D-Wave19]), in around 15 years' time a quantum computer would have enough qubits to break RSA-2048. The table also shows how different the results are, depending on the assumed growth of the number of qubits.

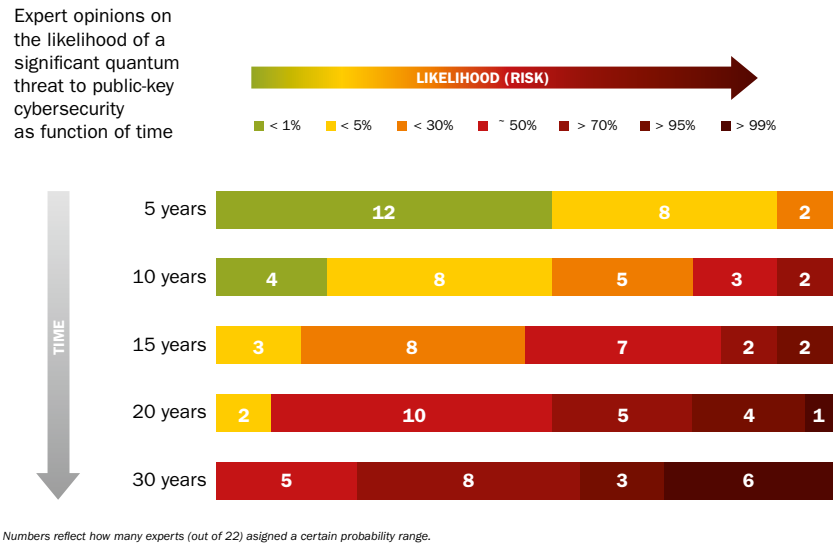
Besides the number of qubits, other factors have an influence too. For example, the quantum computer must be able to run Shor's algorithm to factor the RSA modulus. Some quantum computers report high numbers of qubits, but their principle makes them unsuitable for running Shor's algorithm. One example is the computer of D-Wave Systems, which is based on the principle of quantum annealing, which makes it unsuitable for Shor's algorithm; see [D-Wave14].[1]

Other factors that are important for the efficiency of a quantum computer are:

- **long coherence times**, i.e. qubit lifetimes, the time a qubit stays in superposition before it spontaneously reverts to either 0 or 1; the longer the coherence time, the less error correction is necessary.
- **high gate fidelities**, i.e. the accuracy of logical operations;
- **large connectivity**, i.e. the number of other qubits that qubits can interact with.

Because of all these factors and the immense technological hurdles to be overcome, it is very difficult to predict the development of quantum computers.

To aid in this respect, two scientists recently interviewed 22 global thought leaders in quantum science and technology, asking them about the likelihood that the quantum computer would be able to break RSA-2048, as a function of time; see [GRI19]. Figure 2 below, taken from [GRI19], shows the results of those interviews.



Numbers reflect how many experts (out of 22) asigned a certain probability range.

Figure 2: Expert opinions on breaking RSA-2048 with a quantum computer

1. D-Wave, however, is working on making its system suitable to solve the factorisation problem. It is not known how much acceleration can be gained solving this problem on the D-Wave system; hence the impact D-Wave will have on security cannot be estimated at this moment.

The figure shows, for example, that half of the experts (7+2+2, the red and brown bars in the '15 YEARS' row) think there is a likelihood of 50% or more that RSA-2048 will be broken by a quantum computer in 15 years' time. Note that five experts are even of the opinion that there is a more than 50% likelihood that this will take place in 10 years' time.

[GRI19] mentions the following events to monitor the advances in quantum computing and judge whether or not the expectations above might be met:

- the experts improving the quality of quantum gates;
- demonstrating experimentally that error correction can be used to prolong the storage and manipulation of logical qubits;
- quantum supremacy; this means demonstrating that a quantum computer can actually solve particular problems faster than a classical computer. Coincidentally, this was claimed to have been achieved a few weeks after the publication of [GRI19], see [Google QS].

3.2 MIGRATION DECISION MAKING PROCESS

In the decision making process, there are three factors to be taken into account. Besides the estimated year of the advent of the quantum computer (the first factor), a second crucial factor in determining when to migrate is the security shelf-life of the organisation's confidential data; that is, for how many years the encrypted information must remain confidential. On data that is not yet secured with quantum-safe cryptography attackers can perform a so-called 'harvest attack', also known as 'store-now-decrypt-later'. In this attack, an eavesdropper stores the encrypted data, even though at the time of gathering the information, he is not able to decrypt it. However, when the quantum computer arrives, he is nevertheless able to decrypt the gathered information. For example, if the information is highly confidential and supposed to stay protected for 20 years, but the quantum computer is realised after 15 years, then a lot of confidential material is compromised.

The third factor to take into account here is the time it takes to complete the migration process.

The figure below, taken from [Mosca18], depicts the relationship between the factors mentioned. In this figure:
- X is the security shelf-life, the time the information must stay confidential;
- Y is the migration time;
- Z is the collapse time, the time until a functioning quantum computer is realised.

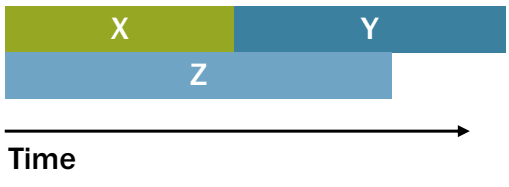


Figure 3: Quantum migration time components

The message that Mosca's figure conveys is that if X + Y > Z, the organisation needs to take measurements very urgently. In other words, if the time the information must stay confidential plus the time it takes to migrate exceeds the time for the realisation of the quantum computer, information is bound to get compromised, a situation that obviously must be avoided.

3.3 THE TIME IT TAKES TO MIGRATE

The time it takes to carry out the migration process depends on: the organisation's number of cryptographic assets, their vulnerability to the quantum computer, their crypto agility (i.e. whether or not the assets support changes in cryptographic algorithms and key lengths) and the budget the organisation invests in the migration.

An effective migration scenario consists of the following steps[2]; they need to be counted in the migration time (the value Y in Section 3.2):

Ramping up
1. become familiar with the subject;
2. create awareness;
3. form a project group;

Initial no-regret moves
4. (draw up and) consult the asset inventory to create a list of assets to be migrated and the estimated time it takes to migrate them;
5. draw up a migration plan;
6. migrate the symmetric cryptography and hash functions (i.e. where necessary increase symmetric key lengths and output lengths of hash functions);

Replace asymmetric crypto
7. select quantum-safe asymmetric algorithms;
8. move to hybrid solutions;
9. move to quantum-safe only solutions.

This is summarised in Figure 4 below.

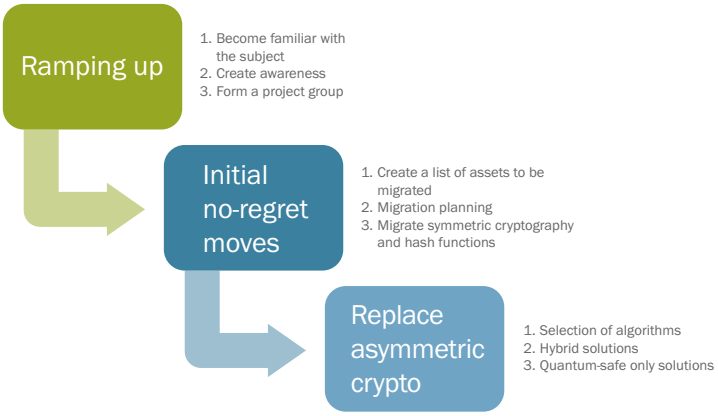


Figure 4: Plan of action for successful migration.

2. Many of these steps can be found in [GRI17] and [CCC19].

There are two boundary conditions:
1. Quantum-safe asymmetric algorithms need to be available to be able to migrate. A big advantage of using a standardised algorithm is that during the standardisation process the algorithm receives much scrutiny by the cryptographic community, which gives faith in its cryptographic strength; see Chapter 6. If the standardisation would not be in time for an organisation, for example because the data needs to stay confidential for a very long time, another choice needs to be made. That, however, involves multiple risks:
   a. there may be weaknesses in the algorithm[3];
   b. there may be errors in the implementation.
2. The migration needs to be completed in time; see Section 3.2. If that is not possible, emergency measures need to be taken to mitigate the risks in another way, for example by quarantining the data, or getting an insurance.

Note that the steps 1 to 6 in the list above can already be taken before any quantum-safe algorithms have been standardised. TNO recommends taking the steps 1 to 6 as soon as possible.

There are tools that can help in replacing the asymmetric crypto; see for example [TNO20].

3.4 RESPONSIBILITIES

As shown in Section 3.3, one of the first steps to take in a migration scenario is to install a project group responsible for the migration. This project group is bound to exist for several years and members must have the skills to fully grasp the complex problem, but requirements on the particular expertise may shift depending on the phase of the migration. Essential expertise includes:
- cryptographic knowledge;
- legal knowledge (with respect to the requirements on the required duration of the protection by the cryptography);
- knowledge of the network architecture of the organisation;
- knowledge of the organisation's assets (hardware, software and data);
- purchasing experience.

Depending on the nature of the organisation, more expertise may be needed. Outsourcing part of the tasks of the project group may be required.

The project group is not responsible, for example, for the standardisation of new X.509 certificates or new public-key algorithms.

3. A way forward out of this situation could be choosing the McEliece system; it has been around for a fairly long time, since 1978, which generates trust in its security. However, the system has impractical values, with private key lengths up to 1 Mbyte.

3.5 COSTS

For the migration costs, a balance has to be found between:

1. **Moving early.** Especially if an organisation moves before the standardisation process has been completed, there is the risk of getting the solution wrong, which involves costs. And, in general, costs incurred early are less favourable than costs incurred later, because in the latter case the amount involved can, in the meantime, be invested in assets that earn returns. An advantage of moving early is that the organisation is not rushed into taking decisions, with the inherent risk of them turning out to be costly mistakes.
2. **Moving late.** When the deadline for the migration to quantum-safe crypto approaches, there may be a significant increase in costs for hiring implementation specialists because they will be in great demand. And, much more seriously, if the migration is initiated too late, severe damage may result from data compromise and the resulting tarnished reputation.

To minimise the costs, ETSI recommends a gradual, standards-based approach; see [ETSI15]. This involves waiting for quantum-safe cryptography standards to emerge and adding a layer of quantum safety to an existing system. Other favourable measures are careful planning and expressing interest in quantum-safe products to vendors at an early stage.

3.6 SUMMARY

It is extremely difficult to predict when a quantum computer will be realised that can break today's cryptography. However, to give an indication, half of a group of 22 leading quantum technology experts estimates that there is a likelihood of 50% or more that RSA-2048 will be broken by a quantum computer in 15 years' time.

To determine the migration urgency for a particular organisation, not only must it take into account the time it takes to build a quantum computer, but also the time the organisation's data must remain confidential and the time it takes to migrate. This is important to prevent so-called store-now-decrypt-later attacks.

We have clustered the necessary migration steps into three stages; (1) the ramping up stage, in which an organisation needs to get acquainted with the subject and form a dedicated and knowledgeable project group, (2) the initial no-regret moves, which include consulting the asset inventory, drawing up a migration plan and updating the symmetric cryptography and hash functions if they are not strong enough to withstand the quantum computer and (3) the replace-asymmetric-crypto stage in which the organisation selects the quantum-safe asymmetric algorithms to replace currently used algorithms, and migrate the IT infrastructure. The time it takes to migrate depends on the organisation's number of cryptographic assets and the budget the organisation invests in the migration.

Costs can be minimised by choosing standardised quantum-safe cryptography solutions, expressing interest to vendors in an early stage and requiring crypto agility for all products to be purchased from now on.

4. ASSESSMENT OF CRYPTO MEANS TO BE MIGRATED

4.1 ASSET INVENTORY

The migration towards a quantum-safe situation starts with the investigation into what assets should be migrated. This can be determined by organisations drawing up (or if it already exists: consulting) an inventory containing all the organisation's assets. Relevant assets for the migration assessment are:

1. Assets containing cryptography: listed in the inventory should be all software and hardware assets and their corresponding cryptographic properties. The inventory should show properties such as:

a. type of cryptography (symmetric/asymmetric);
b. algorithms used;
c. key sizes and/or output lengths;
d. cryptographic agility of the asset, that is whether or not the asset supports changes in cryptographic algorithms and key lengths;
e. the cryptographic dependencies of the assets, i.e. the dependency on suppliers. For example, purchased Hardware Security Modules or apps might require much effort from the supplier to be able to migrate to a quantum-safe situation.

The inventory should keep track of all updates, for example software updates.

2. **Data**: data is also an asset to be regarded in this respect. The organisation needs to be aware of all encrypted or signed data and also of the length in years the encryption needs to stay intact or the signature needs to remain valid.

4.2 CRYPTOGRAPHY

For all assets using symmetric cryptography, the key size should be made at least 256 bits, otherwise the security level drops below the currently required 112-bit strength[4]; and this needs to be done in time. For example AES-128 needs to be migrated to AES-256. For the timing see Section 3.2.

All assets using asymmetric cryptography need to be updated in time with quantum-safe algorithms. A non-exhaustive list of much-used protocols and programs containing asymmetric cryptography is the following: TLS, SSL, HTTPS, IPSec, IKE, X.509 certificates, SSH, S/MIME, PGP/GPG, DNSSEC, ZRTP, DSS, PCIDSS, signatures of apps and Federated Authorisation (a method of 'single sign on').

Cryptographic hash functions suffer from the advent of the quantum computer in combination with Grover's algorithm, but can still be used as long as the length of the output is 3b-bit long, where b is the level of security that is required expressed in a

4. Note that security strength is a different notion than key length.

number of bits; see [Mavroedis18]. For example, if a 112-bit security level is required, the hash function must have at least 336 bits of output to be quantum-safe. Both SHA-2 and SHA-3, currently often-used algorithms, are able to deliver 128-bit quantum security.

Figure 5 below shows a flow chart to do a first quick assessment of the presence of vulnerable cryptography in an organisation.

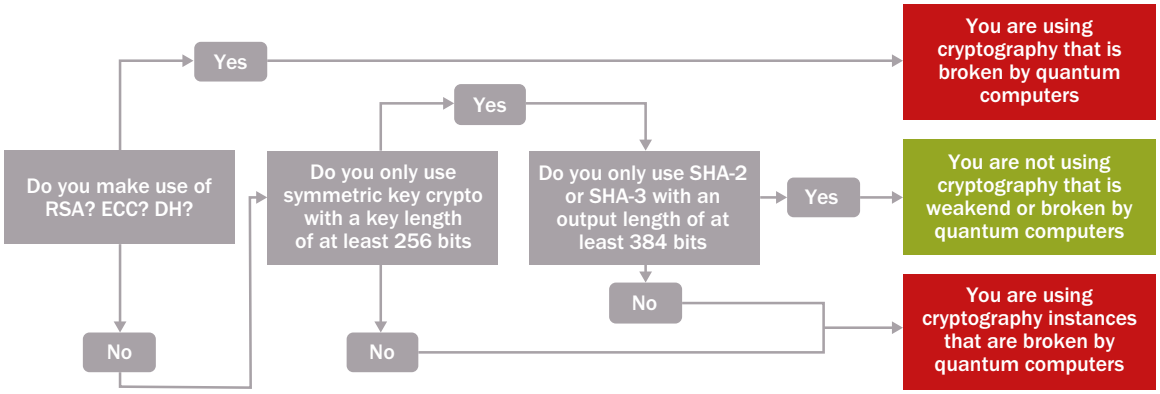


Figure 5: Do you only use quantum-safe cryptography?

Table 2 below shows the strength of various algorithms, against attackers using conventional computers, and attackers assumed to be in possession of a future quantum computer. Variants shown in red should be replaced in time, because, as described in Chapter 2, they can be broken using Grover's algorithm or Shor's algorithm on a (sufficiently large) quantum computer.

Type	Algorithm	(Key) Size	Effective Security Level	
			Conventional Computing	Quantum Computing
Symmetric	AES-128	128 bits	128 bits	64 bits[5]
Symmetric	AES-256	256 bits	256 bits	128 bits
Asymmetric	RSA-1024	1024 bits	80 bits	0 bits
Asymmetric	RSA-2048	2048 bits	112 bits	0 bits
Asymmetric	ECC-256	256 bits	128 bits	0 bits
Asymmetric	ECC-384	384 bits	192 bits	0 bits
Asymmetric	ECDSA-256	256 bits	128 bits	0 bits
Hash	SHA-2	256 bits	128 bits	85 bits
Hash	SHA-2	384 bits	192 bits	128 bits

Table 2: Conventional and quantum security

5 There are various challenges to overcome before quantum computers improve the adversary's capabilities of breaking symmetric ciphers such as AES-128. Taking these challenges into account, an alternative view is that AES-128 will remain secure for the coming decades (https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs).

All elements of a Public Key Infrastructure (PKI) need to be updated; this concerns Certification Authorities (CAs), Registration Authorities (RAs) and end-entities. They all must be provided with new certificates and the ability to issue and/or verify quantum-safe Certificate Signing Requests (CSRs), certificates and Certificate Revocation Lists (CRLs). In this respect, the Root CA needs to be updated first; then the migration moves down the PKI hierarchy. End-entities must be provided with a quantum-safe trust anchor, for example a root certificate. Old certificates need to be revoked.

4.3 DATA

Encrypted data that needs to be confidential for a long time (see Section 3.2) must be re-encrypted. Note that removing the non-quantum-safe encryption prior to applying the quantum-safe encryption may be unacceptable, because during the time the data is unprotected, it may get compromised. If the data is no longer actively needed but needs to remain confidential, it must be quarantined, that is, be taken offline and stored in a physically protected location.

Signed data on which the signature needs to remain valid for a long time, such as signed firmware, needs to be (re-)signed with a quantum-safe algorithm or a hash-based signature using a hash function with a sufficiently long output.

4.4 SUMMARY

An organisation can determine which crypto means must be migrated by (drawing up and) consulting its asset inventory.

The following must be migrated:
- all symmetric cryptography that has a security strength less than 256 bits;
- all hash functions that have an output length that is less than 336 bits;
- all asymmetric cryptography that is based on prime factorisation or discrete logarithms. Also all elements of a Public Key Infrastructure (PKI) need to be updated; this concerns Certification Authorities (CAs), Registration Authorities (RAs) and end-entities;
- all data protected with cryptography mentioned in the previous items; this concerns both confidentiality and integrity protection.

An organisation can determine which crypto means must be migrated by (drawing up and) consulting its asset inventory.

5. CRYPTO MIGRATION

Chapter 3 already listed all the steps involved in the migration. Those involving the migration of the crypto are:
6. migrate the symmetric cryptography and hash functions;
7. select quantum-safe asymmetric algorithms;
8. move to hybrid solutions;
9. move to quantum-safe only solutions.

The items 6 and 8 are discussed below in sections 5.1 and 5.2, respectively. Point 8 can be skipped by an organisation if it can do a 'big bang' introduction of the quantum-safe solution. Item 7 is discussed in detail in Chapter 6. Item 9 is an extension of item 8 by phasing out the vulnerable crypto, and will not be discussed here any further.

5.1 MAKING SYMMETRIC CRYPTOGRAPHY AND HASH FUNCTIONS QUANTUM-SAFE

With the aid of Table 2 in Section 4.2 above, an organisation can check whether or not its symmetric cryptography and hash functions are vulnerable to attacks with a quantum computer. If the organisation uses algorithms not listed in Table 2, the verification needs to be done using other sources. Then, where the check has proven the organisation vulnerable, the organisation needs to increase symmetric key lengths (to reach a security strength of at least 256 bits) and output lengths of hash functions (to at least 336 bits). New algorithms may need to be chosen, for example to phase out TDES.

Such a transition might be as simple as selecting different parameters (key size, output length), but might also involve the introduction of new algorithms. In the former case it needs to be thoroughly investigated whether all parts of the system can deal with these different formats. In the latter case (new algorithms) important aspects are:
1. pre-implementation evaluation: strong cryptography may be poorly implemented;
2. testing.

5.2 HYBRID SOLUTIONS

5.2.1. Goal

A hybrid solution is a solution where multiple algorithms, classical and quantum-safe are used in parallel. When migrating, there are two reasons for combining classical algorithms with quantum-safe ones:

1. **Assurance of cryptographic strength.** The new, supposedly quantum-safe algorithms have received much less analysis by the cryptographic community than the classical ones, simply because they are newer. Therefore, the assurance that they are indeed safe algorithms is lower, and will remain so until after more years of analysis. As long as the quantum computer has not yet arrived, the classical algorithms can function as fall-back solutions in case flaws are discovered in the new algorithms. The resulting solution will at least have the strength of the classical algorithms.

2. **Backwards compatibility.** Communication parties that have already migrated to quantum-safe algorithms can use that solution; the ones that have not, can use the classical algorithms. This needs to be done in cases where a 'big bang' introduction of quantum-safe crypto is not possible. An example is a Public Key Infrastructure where some parties take longer to implement new crypto than others. Also, the replacement of all client applications that use PKI will not be possible in a single go.

When using a hybrid solution, care must be taken to do this in a correct way. This is described in two examples below, for key establishment solutions and for signatures.

5.2.2 For key establishment

For key establishment, for example for the establishment of a session key, a possible solution is as follows. The two communicating parties carry out both a classical key establishment protocol and a quantum-safe one. If more assurance is desired, multiple different quantum-safe algorithms can also be used. Then the session key is derived by both parties from the determined keys by applying a Key Derivation Function (KDF) on them, for example a cryptographic hash function, as shown in Figure 6 below.

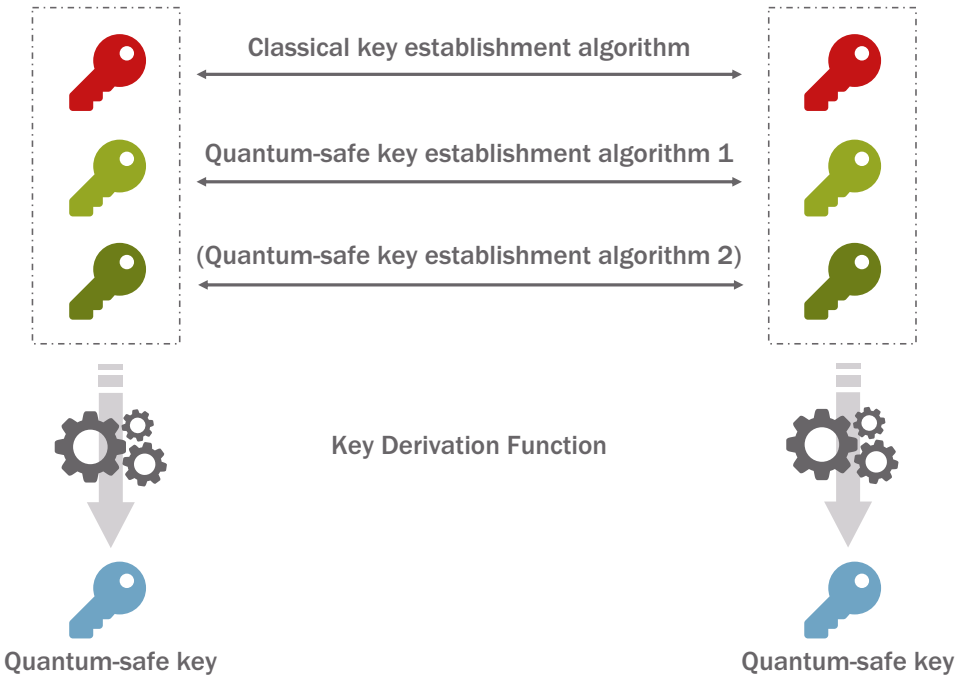


Figure 6: Hybrid encryption for key establishment

Even though part of the input of the KDF is generated using a classical algorithm, the resulting key is quantum-safe. This key therefore provides post-quantum security, yet it at least provides the strength of the classical algorithm, if the quantum-safe algorithms later prove to be insecure. The key thus has at least the strength of the strongest algorithm of the three.

The classical algorithm can also provide backwards compatibility; all parties that have not yet migrated can carry out the key establishment using only the classical cryptography. Note that care must be taken to avoid downgrade attacks, attacks in which a man-in-the-middle manipulates the messages to force the receiver to use the weaker security of a classical algorithm, while both sender and receiver are actually able to use quantum-safe cryptography.

5.2.3 For signatures

For signatures, important properties of the hybrid solution are that they must be both unforgeable and non-separable; see [Bindel17]. The first property means that an attacker must not be able to generate signatures without knowledge of both private keys, the one for the classical algorithm and the one for the quantum-safe algorithm. The second property means that it must not be possible for an attacker to separate the classical signature from the quantum-safe one, and pretend to the receiver that the signer only used classical cryptography; this is a downgrade attack.

In [Bindel17] a scheme is presented in which the two mentioned properties unforgeability and non-separability can be achieved. It is depicted in Figure 7 below.

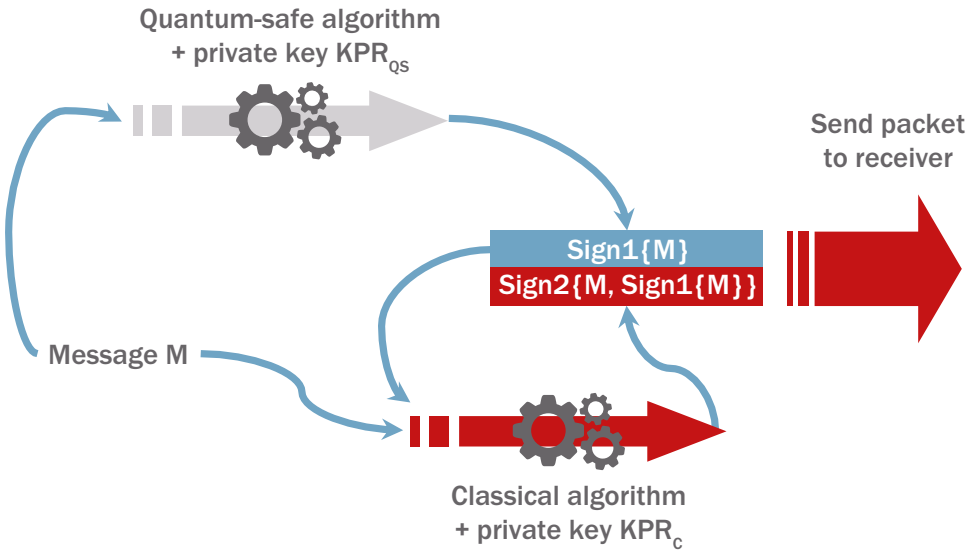


Figure 7: Hybrid signature scheme

The message M is signed with a quantum-safe algorithm; this is signature Sign1 in the figure. Then this signature Sign1 together with (again) the message M are signed with a classical algorithm; the result is signature Sign2.

The signatures on message M can both be checked with:

1. the public key PUQS corresponding to the private key PRQS used for signing with the quantum-safe algorithm (signature Sign1, blue part), and
2. the public key PUC corresponding to the private key PRC used for signing with the classical algorithm (signature Sign2, red part).

The signature Sign2 provides backwards compatibility; all parties that have not yet migrated can check the signature Sign2 using classical cryptography. Note that this part also provides the non-separability, as by the structure it can be recognised that, besides the message M, a signature Sign1 is also involved, the quantum-safe one. An attacker will thus not succeed in making the verifier believe (in a downgrade attack) that only classical cryptography was used.

The signature Sign1 provides post-quantum security. Yet signature Sign2 provides the strength of the classical algorithm, if the quantum-safe algorithm later proves to be insecure. This mechanism thus has at least the strength of the strongest algorithm of the two.

5.3 SUMMARY

Migration of the cryptography vulnerable to attacks using the quantum computer involves the following four steps:

1. When vulnerable to the quantum computer: making the symmetric crypto and hash functions quantum-safe by increasing symmetric key lengths to a security strength of at least 256 bits and increasing output lengths of hash functions to at least 336 bits.
2. Selecting quantum-safe asymmetric algorithms.
3. Optionally implementing a hybrid solution, i.e. mixing classical and quantum-safe algorithms to give assurance of cryptographic strength and backwards compatibility. When using a hybrid solution, care must be taken to do this in a correct way.
4. Moving to quantum-safe algorithm only solutions.

A hybrid solution is a solution where multiple algorithms, classical and quantum-safe are used in parallel.

6. QUANTUM-SAFE CRYPTOGRAPHY

Quantum-safe cryptography refers to the study of cryptographic algorithms that are (assumed to be) secure against attacks by both conventional and quantum computers. Quantum-safe cryptography can be divided into the following two categories:

1. **Quantum Cryptography:** Leveraging quantum mechanical properties to construct cryptographic protocols. The main example in this category is Quantum Key Distribution (QKD); see for example [NIST QKD].
2. **Post-Quantum Cryptography:** The study of 'conventional' cryptographic algorithms, i.e., algorithms not based on quantum mechanics that are assumed to be secure against attacks by a quantum computer.

In this work, we focus on cryptographic algorithms that can be executed on conventional computers, i.e., on *post-quantum cryptography*.

6.1 POST-QUANTUM PUBLIC-KEY CRYPTOGRAPHY

This section focuses on public-key (i.e. asymmetric) algorithms. Public-key algorithms rely on the (assumed) hardness of certain mathematical problems. Traditionally, public-key algorithms are typically based on the integer factorisation problem or the discrete log problem. The advent of the quantum computer renders these schemes insecure, requiring cryptographic algorithms to be based on alternative hardness assumptions.

Cryptographic algorithms are often categorised on the basis of their underlying hardness assumptions. In turn, these assumptions influence important performance measures of the resulting protocols, such as:

- Computational efficiency of the key generation and the public- and private-key operations;
- Size of keys, ciphertexts and signatures.

Below we summarise the main mathematical hardness assumptions encountered in the field of post-quantum cryptography.

- **Code-based cryptography** builds upon error-correcting codes. In this technique the message is turned into a code word with an error-correcting code unknown to the attacker, and errors are deliberately introduced into the result. The ciphertext can be decrypted by running the decoding algorithm for the chosen error-correcting code. The security is derived from the assumption that it is hard to decode a noisy codeword obtained from a random linear code. The cryptographic schemes are set up in such a way that encoding a message can be done with public information (a public key), while decoding requires secret information (the corresponding secret key).

- **Lattice-based cryptography** refers to cryptographic algorithms that rely on the hardness of lattice problems, e.g. the Closest Vector Problem (CVP). Many cryptographic schemes in this category share similarities with code-based cryptography. For example, an encryption of a message can be obtained as a lattice-point to which an error vector has been added. Decryption entails finding the closest lattice point to a ciphertext. The security is derived from the following assumption. From a bad representation (public key) of a lattice it is hard to find the closest vector, whereas from a good representation (private key) the closest vector is easily found.
- **Hash-based cryptography** relies on certain one-way properties of hash functions; these functions can be evaluated efficiently, but are hard to invert. A pre-image of a hash value can therefore only be revealed by someone that knows this pre-image in advance. In contrast to the other categories, hash-based cryptography only comprises signature schemes.
- **Multivariate cryptography** is based on the hardness of solving certain multivariate systems of quadratic equations. Unless additional information (the secret key) about the system is known, solving them is assumed to be infeasible. Multivariate cryptography stands out in that it provides short digital signatures.
- **Supersingular elliptic-curve isogeny based cryptography** relies on the hardness of finding an isogeny between two arbitrary elliptic curves, i.e. a mapping between the two curves that has certain properties. Isogenies between elliptic curves allow for a Diffie-Hellman like key exchange protocol.

This text will not go into these techniques any further; instead the reader is referred to [NIST PQC] or [Fraunhofer17].

6.2 STANDARDISATION

It is common practice to deploy only cryptographic protocols that are standardised. Standardised cryptography has often endured many years of cryptanalysis, which increases the confidence in these systems.

At the time of writing, there are various standardisation bodies working on the standardisation of post-quantum cryptography and its deployment including NIST, IETF, ETSI, ISO and ITU. These bodies are all located in either Europe or the US. China is also active in this area and is planning to present its own cryptographic standards.

The most important standardisation process to follow with respect to the quantum-safe algorithms is that of NIST, the U.S. National Institute of Standards and Technology. In 2016, NIST started a worldwide standardisation process for quantum-safe public-key cryptography; see [NIST PQC]. The outcome of the process will be one or more algorithms for digital signature schemes and key encapsulation mechanisms. Draft NIST standards on quantum-safe public-key cryptography are expected between 2022 and 2024.

There are already some standards available in addition to the standards that are being developed by NIST. Within the IETF there are standards on stateful hash-based signatures and IETF considers how multiple cryptographic schemes can be deployed on the internet in order to easily adopt quantum-safe algorithms. ETSI has published various reports on how to deal with post-quantum cryptography in various use case scenarios such as VPNs.

6.3 SUMMARY

Various asymmetric cryptographic algorithms exist that have an assumed mathematical hardness that makes them resistant to attacks by a quantum computer. The ones that are especially under investigation are code-based cryptography, lattice-based cryptography, hash-based cryptography, multivariate cryptography and supersingular elliptic-curve isogeny based cryptography.

It is common practice to deploy only cryptographic protocols that are standardised. The standardisation of quantum-safe cryptography takes place in standardisation bodies such as NIST, IETF, ETSI, ISO and ITU. The most important standardisation process is that of NIST, the U.S. National Institute of Standards and Technology. Draft NIST standards on quantum-safe public-key cryptography are expected between 2022 and 2024.

It is common practice to deploy only cryptographic protocols that are standardised. Standardised cryptography has often endured many years of cryptanalysis, which increases the confidence in these systems.

7. SUMMARY

The advent of a quantum computer is going to have to have an enormous impact on cryptography. By running the appropriate algorithms on a sufficiently large quantum computer, attacks on secret key (i.e. symmetric) algorithms will become quadratically faster and all currently standardised public key (i.e. asymmetric) algorithms, such as RSA, DSA and Elliptic Curve algorithms, will be broken.

It is extremely difficult to predict when a quantum computer of that scale will be realised, but to give an indication, half of a group of leading experts in the field of quantum technology estimates that there is a likelihood of 50% or more that RSA-2048 will be broken by a quantum computer in 15 years' time; see [GRI19]. Events that will be useful in monitoring the advances in quantum computing are the improvements in the quality of quantum gates and in error correction on qubits, and quantum supremacy. To determine the migration urgency for a particular organisation, not only must the organisation take into account the time it takes to build a quantum computer, but also the time the organisation's data must remain confidential and the time it takes to migrate. This is important, for example, to prevent so-called store-now-decrypt-later attacks.

To migrate to a quantum-safe situation an organisation needs to take the following steps:

Ramping up

1. become familiar with the subject;
2. create awareness;
3. form a project group;

Initial no-regret moves

4. (draw up and) consult the asset inventory to create a list of assets to be migrated and the estimated time it takes to migrate them. The following must be migrated:

a. all symmetric cryptography that has a security strength less than 256 bits;
b. all hash functions that have an output length that is less than 336 bits;
c. all asymmetric cryptography. Also, all elements of a Public Key Infrastructure (PKI) need to be updated. This concerns Certification Authorities (CAs), Registration Authorities (RAs) and end-entities;
d. all data protected with cryptography mentioned in the items a to c. This concerns both confidentiality and integrity protection;

5. draw up a migration plan;
6. migrate the symmetric cryptography and hash functions (i.e. where necessary, increase symmetric key lengths and output lengths of hash functions; see item 4 above);

Replace asymmetric crypto

7. select quantum-safe asymmetric algorithms. A big advantage of using *standardised* algorithms is that during the standardisation process the algorithms receive much scrutiny by the cryptographic community, which gives faith in their cryptographic strength. The most important standardisation process is that of NIST, the U.S. National Institute of Standards and Technology; see [NIST PQC]. Draft NIST standards on quantum-safe public-key cryptography are expected between 2022 and 2024;
8. move to hybrid solutions that mix classical and quantum-safe algorithms to give assurance of cryptographic strength and backwards compatibility;
9. move to quantum-safe only solutions by removing the classical algorithms.

TNO recommends taking steps 1 to 6 as soon as possible; organisations cannot afford failure to comply with data confidentiality requirements by migrating too late.

Costs can be minimised by expressing interest to vendors in an early stage and requiring crypto agility (flexibility in cryptographic algorithms and key lengths) for all products to be purchased from now on.

8. REFERENCES

[Bindel17] N. Bindel e.a., *Transitioning to a Quantum-Resistant Public Key Infrastructure*, May 2017

[CCC19] Computing Community Consortium, *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*, 2019.

[D-Wave14] https://www.dwavesys.com/blog/2014/11/response-worlds-first-quantum-computer-buyers-guide

[D-Wave19] https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware

[ETSI15] ETSI, *Quantum Safe Cryptography and Security*, White Paper no. 8, June 2015

[Franke19] D.P. Franke e.a., *Rent's rule and extensibility in quantum computing*, QuTech, 2019

[Fraunhofer17] R. Niederhagen and M. Waidner, *Practical PostQuantum Cryptography*, Fraunhofer Institute for Secure Information Technology, White Paper, August 2017

[Google QC] https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

[Google QS] Google, *Quantum supremacy using a programmable superconducting processor*, September 2019

[GRI17] M. Mosca and J. Mulholland, *A Methodology for Quantum Risk Assessment*, Global Risk Institute, 2017

[GRI19] M. Mosca and M. Piani, *Quantum Threat Timeline Report*, Global Risk Institute, 2019

[Grover] L.K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212

[Mavroedis18] V. Mavroedis et al., *The Impact of Quantum Computing on Present Cryptography*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018

[NAS19] National Academies of Sciences, *Quantum Computing: Progress and Prospects*, The National Academies Press, 2019

[NIST PQC] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[NIST QKD] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[Mosca18] M. Mosca, *Preparing for the quantum era – Quantum-safe Cryptography for Industry*, August 2018

[RFC 5280] IETF, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008*

[Shor94] *P.W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, IEEE, 1994

[Takahashi06] Y. Takahashi and N. Kunihiro, *A quantum circuit for Shor's factoring algorithm using 2n + 2 qubits*, Quantum Information and Computation, vol. 6, no. 2, pp. 184-192, 2006.

[TNO20] https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/quantum/quantum-safe-crypto/

[QCR20] https://quantumcomputingreport.com/moores-law-for-qubits-revisited/

9. ABBREVIATIONS

AES	Advanced Encryption Standard, symmetric key cryptography algorithm
CA	Certificate Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVP	Closest Vector Problem
DNSSEC	Domain Name System Security Extensions
DSA	Digital Signature Algorithm, FIPS standard
DSS	Digital Signature Standard, FIPS standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GPG	GNU Privacy Guard
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology (U.S.)
PCIDSS	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography (PQC)
QKD	Quantum Key Distribution
QRC	Quantum-Resistant Cryptography
QSC	Quantum-Safe Cryptography
RA	Registration Authority
RSA	Rivest, Shamir, Adelman, public key cryptography algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Socket Layer
TDES	Triple DES (Data Encryption Standard)
TLS	Transport Layer Security
X.509	ITU-T standard for public key certificates
ZRTP	Zimmerman Real-time Transport Protocol

Contact
Drs. Ir. Maran van Heesch
QUANTUM SECURITY SPECIALIST
maran.vanheesch@tno.nl

Ir. F. Muller
SENIOR SECURITY SPECIALIST
frank.muller@tno.nl