Post-Quantum Migration

Table of contents

1. Introduction

Quantum computing will offer new means to solve otherwise intractable computational problems. Some known computational “hard” problems for solving on current “classical” computers can supposedly be solved significantly faster on future quantum computers. This opens new avenues with immense potential, for example for developing new chemical processes, new drugs, and new communication security protocols. At the same time, it may impact the security offered by currently deemed unbreakable cryptographic algorithms, which would have major consequences for the protection of data confidentiality, integrity and authenticity.

The security of cryptographic algorithms is constantly challenged by increases in computing power and the sophistication of cryptanalytic techniques. In general, cryptographic algorithms raise an unsurmountable computational barrier, but the unsolvable hard computational problems of classical cryptography are tailored to the currently available classical computation power. Some of these hard problems turn out to be solvable with quantum computing.

Well-known quantum algorithms with high impact on current classical cryptography are Grover’s algorithm and Shor’s algorithms. Both quantum algorithms and their impact on contemporary cryptography are briefly described below.

1.1. Grover’s algorithm impact on contemporary cryptography

Grover’s algorithm, named after the Indian-American computer scientist Lov Kumar Grover, is a quantum search algorithm formulated in 1996 that finds, with high probability, the unique input to a black box function that produces a particular output value. Grover’s algorithm provides a quadratic speedup over classical computer search algorithms. Although not as impressive as exponential speedup, the quadratic speedup is considerable and affects the security levels provided by cryptographic hash algorithms, Message Authentication Codes (MACs) and symmetric encryption algorithms.

Currently widely used cryptographic hash functions such as for example SHA-2 and SHA-3 (Box 1.1), MACs such as for example HMAC and Poly1305 (Box 1.2), and symmetric cryptographic algorithms such as for example the AES block cipher and the ChaCha20 stream cipher (Box 1.3), are deemed to be resistant to future attacks by means of powerful quantum computers, provided that sufficiently large (underlying) hash values, MAC codes and cryptographic keys are being used.

A cryptographic hash function is a mathematical algorithm that maps data of an arbitrary size to a bitstring of a fixed size (the “hash” or "hash value"), by means of a one-way function. Ideally it should have the following properties:

- it is fast to compute the hash value for any given piece of data;

- the computed hash value is always the same for given piece of data, i.e. the hash function is deterministic;
- it is (practically) infeasible to generate a piece of data that yields a given hash value, i.e. it is impossible to reverse the process that generated the given hash value (pre-image resistance);
- for any given piece of data, it is (practically) infeasible to find another piece of data that has the same hash value (second pre-image resistance);
- it is (practically) infeasible to find (at least) two different pieces of data that have the same hash value (collision resistance);
- a small change to a piece of data should change its hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect).

Box 1.1: Cryptographic hash function

A Message Authentication Code (MAC) is used to verify the authenticity (and at the same time, to protect the integrity) of a piece of data (a file, a document, a message, etc.). A MAC provides message authentication provided that there exists mutual trust, but will not resist repudiation (because the mutual trust relationship breaks with repudiation).

Box 1.2: Message Authentication Code (MAC)

Symmetric cryptography uses only one cryptographic key (known as the "secret key") for both the encryption of plaintext and the decryption of the corresponding ciphertext. For some algorithms, the key value used for decryption is derived from the key value used for encryption by a simple transformation.

Box 1.3: Symmetric cryptography

1.2. Shor's algorithms impact on contemporary cryptography

For the Integer Factorization Problem (IFP) underlying RSA cryptography the best-known classical problem solving algorithm, i.e. General Number Field Sieve (GNFS), has a sub-exponential complexity. For the Discrete Logarithm Problem (DLP) problem underlying Diffie-Hellman (DH) cryptography (which is almost exclusively used for secret key exchange purposes) the best-known classical problem solving algorithm, i.e. Index-Calculate Method (ICM), also has a sub-exponential complexity. For the Elliptic Curve Discrete Logarithm Problem (ECDLP) problem underlying Elliptic Curve Cryptography (ECC) the best-known classical solving algorithm, i.e. Pollard's Rho, has an exponential complexity[1].

Shor's integer factoring algorithm and Shor's dlog algorithm, named after the American mathematician Peter Williston Shor, are quantum algorithms formulated in 1994 for performing integer factorisation and for solving the DLP and ECDLP problems. Shor's quantum algorithms provide exponential speedup over their classical counterparts. This implies that almost all

[1] The lack of known solving algorithms of sub-exponential complexity has made ECC cryptography more attractive than RSA cryptography, because it means that its cryptographic keys can have much smaller sizes than those of RSA for the same level of n-bit security.

currently widely used public-key cryptographic algorithms are in danger of being broken using Shor's algorithms, unless extremely large and totally impractical[2] cryptographic keys are used. It is generally believed that Cryptographically Relevant Quantum Computers (CRQCs)[3] will become available in the (not so far) future that are capable of breaking many widely used classical state-of-the-art public-key cryptographic schemes (Box 1.4), including secret key exchange mechanisms and digital signature mechanisms.

Public-key cryptography uses pairs of cryptographic keys. Each pair consists of a public key (which may be known to others) and a private key (which must not be known by anyone except the owner). The generation of such key pairs depends on asymmetric cryptographic algorithms, which are based on hard mathematical problems (one-way functions).

Box 1.4: Public-key cryptography

Significant damage could be caused by future CRQCs by breaking secret key exchange mechanisms (Box 1.5) based on current public-key encryption. Current publicly known quantum computers are certainly not capable of doing so. Nonetheless, by intercepting and recording data encrypted with secret keys established by means of key exchange mechanisms based on current public-key encryption, CRQCs could be used in the future to decrypt encrypted data that has been recorded earlier on ("harvest-now, decrypt-later" aka "store-now, decrypt-later" attack). Significant damage could thus be caused retrospectively if no action is taken to mitigate this risk, e.g. by migrating to quantum-resistant key exchange schemes before the CRQC threat becomes reality, taking into account the amount of time during which the confidentiality of the previously encrypted data must be ensured.

A secret key exchange mechanism (aka secret key establishment mechanism) is a method by which symmetric cryptographic keys are exchanged between two or parties. Key transport (aka key distribution) is the process whereby one entity generates a secret key and then transfers that secret key by secure means to the other entity. Key agreement is the process of establishing a shared secret key between two entities in such a way that neither of them can predetermine the value of the shared secret key. Key transport usually involves non-interactive techniques while key agreement usually involves interactive techniques. Key transport protocols and key agreement protocols can be based on either symmetric or asymmetric cryptographic techniques.

Note
In many cases, the shared secret key that is established by a key transport or key agreement mechanism is not directly used, but is subject to further processing in order to derive the cryptographic key(s) that is (are) used for subsequent encryption and/or decryption.

Box 1.5: Key exchange mechanism

[2] For example (according to the American mathematician, cryptologist and computer scientist Daniel Julius Bernstein), a 2^{43}-bit (8 TB) key, consisting of 2^{31} primes with 4,096 bits each, would be needed for RSA to remain secure against such quantum computing attacks.

[3] CRQC is used to specifically describe powerful future quantum computers that are capable of actually attacking real world cryptographic schemes that would be infeasible to attack with a classical computer.

Significant damage could also be caused by future CRQCs by forging digital signatures (Box 1.6) based on classical public-key cryptography. Digital signatures are used for different purposes, including signing of public-key certificates, which in turn is used for a variety of purposes: identity authentication, privilege authorisation, etc. Migrating to quantum-resistant digital signature schemes before the CRQC threat becomes reality is needed for mitigating this risk.

A digital signature is the electronic analogue of a hand-written signature and must satisfy the following requirements:

- the receiver should be able to validate the sender's signature;
- the signature must not be forgeable;
- the sender must not be able to successfully repudiate the signing of a message.

Most digital signatures are based on public-key cryptography schemes, many of which are based on specialised algorithms that are not suitable for encipherment purposes. It is usually not desirable to apply a digital signature directly to a possibly long piece of data, given the inefficiency of public-key encryption. Nonetheless, the entire piece of data should be protected by the signature. A way of satisfying both requirements is to use a cryptographic hash function as an intermediary. The hash function takes the entire piece of data and produces a fixed-length message digest (hash value), which is then digitally signed.

Box 1.6: Digital signature

Classical public-key cryptography mechanisms are used in many contemporary cryptographic security protocols (Box 1.7) for the purpose of "on-the-fly" entity authentication or privilege authorisation. Unlike "store-now, decrypt-later" attacks on key exchange mechanisms and attacks on digital signature mechanisms, attacking such entity authentication and privilege authorisation mechanisms will require a much more powerful quantum computer since the time available for performing the attacks is severely constrained, as the entity authentication and the privilege authorisation is done in real-time.

A cryptographic security protocol is an abstract or concrete protocol that performs security-related functions by applying cryptographic methods, often by means of a sequences of cryptographic primitives. It describes how the cryptographic algorithms should be used and includes details about data structures and representations.

Box 1.7: Cryptographic security protocol

1.3. Quantum computing cyberattack taxonomy

A structured list of examples of various types of cyberattacks enabled by the malicious use of quantum computing is provided below. These attacks could be performed in the future when CRQCs will be available, if at that time cryptographic schemes are still being used that are not quantum-resistant. Some attacks, the so-called "harvest now, decrypt later" attacks, could already be attempted today if non-quantum-resistant cryptography is being used.

- Harvesting of encrypted data for malicious purposes:

- harvesting of encrypted *data-in-transit*:
  - mass data harvesting;
  - event-based data harvesting;
  - target-based data harvesting (targeting specific organisations or individuals);
  - etc.

- harvesting of encrypted *data-at-rest*:
  - application data files and databases;
  - snapshots and backups;
  - archival data;
  - etc.

- harvesting of encrypted *data-in-use*:
  - application-level data encryption;
  - Virtual Machine Image (VMI) encryption;
  - etc.

- Malicious signing of digital artefacts:

  - malicious code signing:
    - fake[4] firmware/software and updates;
    - fake malware fingerprints;
    - etc.

  - fraudulent manipulation of digital legal documents:
    - fake passports, birth certificates, driving licences, etc.;
    - fake ownership records;
    - fake mortgage and loan contracts;
    - fake intellectual property (patents and trademarks);
    - etc.

  - fraudulent manipulation of digital evidence:
    - fake audit records (financial, legal, etc.);
    - fake forensic records;
    - fake criminal records;
    - etc.

  - malicious signing of other digital artefacts:
    - fake diplomas and licences;
    - fake insurance policies and claims;

[4] The word “fake” refers to “malicious modification or malicious fabrication”.

- fake invoices;
- fake tax records;
- fake compliance certificates (quality, security, etc.);
- etc.

- Malicious data origin authentication: modification or fabrication of integrity proofs associated with digital artefacts.

- Malicious entity authentication:
  - issuing of fake credentials;
  - impersonation;
  - privilege escalation;
  - etc.

Many of these attacks could be performed offline and may take several hours for execution on a future on-premises quantum computer or even much more time to complete using a shared-access quantum computing service. However, some types of attack must be performed online in just a few seconds, thus requiring real-time dedicated access to very powerful quantum computers which are still a long way off.

2. Post-quantum migration

Every year, evolutionQ and GRI collect the opinion of renowned quantum computing experts on the potential advent of a quantum threat to public-key cryptography (Figure 2.1).

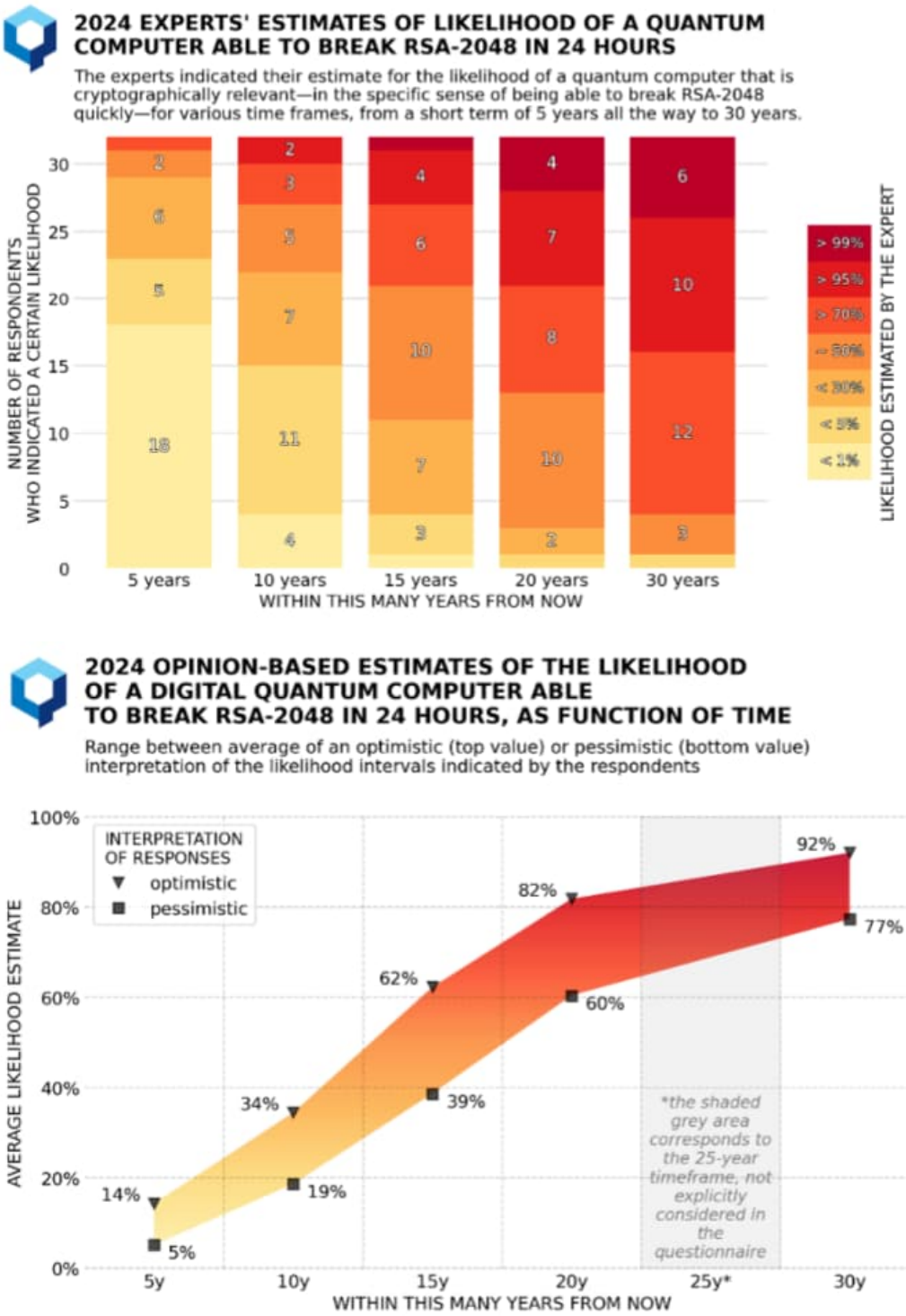

Figure 2.1: Quantum threat estimates (source: evolutionQ/GRI 2024)

Note

Some renown scientists, including the Dutch theoretical physicist and Nobel Prize winner Gerardus 't Hooft, the Russian physicist Mikhail Dyakonov and the Israeli mathematician and computer scientist Gil Kalai, caution that building a universal quantum computer is most probably unfeasible because it is not an engineering problem but rather a fundamental scientific problem for which there exists no solution.

On the Heffalump Threat

Peter Gutmann
University of Auckland
pgut001@cs.auckland.ac.nz

Abstract

Over the last few years a new type of attack has been receiving a lot of attention. Unfortunately the technical details can be quite confusing to laypeople. This paper explains it in easy-to-understand terms.

Discussion

A long time ago, in a faraway kingdom… well actually not that long ago, about thirty years to be precise, one of the king's wizards — and he had a lot of wizards, because wizarding was a profession that attracted plenty of funding — announced that he'd come up with a way for heffalumps to knock down castle walls. Now no-one had ever seen a heffalump and in any case it was much easier to knock down castle walls with catapults so like a lot of the stuff the wizards said it was ignored by everyone except other wizards, some of whom got quite excited about it.

Then about seven years later a group of wizards actually managed to come up with a way to breed a sort of micro-heffalump that could do what the first wizard had described. However when it was pointed out that fifteen bricks piled on top of each other didn't really constitute a castle they went back to their towers and applied for more funding because, you know, heffalumps.

Eleven years after that, some new wizards came up with another toy heffalump that could knock over 21 bricks piled on top of each other, the same as a toddler or an enthusiastic puppy. And now a lot more people got excited about it because, as the wizards pointed out, once someone actually produced a proper heffalump no castle would be safe.

This gradually led to an increase in funding and, eventually, work on post-heffalump fortifications that required even more funding. Still no-one had seen an actual heffalump, but that didn't mean that, like ghosts and goblins and trolls, there couldn't be one out there somewhere.

And now, every few months, one or another of the groups of wizards would announce that they had achieved heffalump supremacy, in which a low wall of bricks that was carefully constructed to be easy to knock down by a heffalump but hard to knock down by a catapult had been knocked down by a heffalump, or at least a simulation of a heffalump. Unfortunately for the wizards since heffalump supremacy was announced every few months, over and over again, people began to doubt it about the tenth or twentieth time that it was announced anew. And still no-one had seen an actual heffalump.

Eventually this came to the king's attention and, while he didn't really understand any of it, he understood that the wizards were saying that none of his castles would be safe when someone produced a heffalump, and so he issued royal decree 7535 which required that all of his subjects switch to living in post-heffalump castles. This upset some people who pointed out that they'd already invested billions of thalers in building castles to resist catapults, and it was hard enough the first time round particularly since some of the castles leaked and were difficult to live in, and now they were expected to spend billions more thalers building new, even more awkward post-heffalump castles, some of which fell down once they were built, but the king had decreed it so there was no going back. In any case all the masons who had set themselves up to build post-heffalump castles were beside themselves with glee at all the thalers this royal decree guaranteed them, as were the wizards who now had guaranteed employment for life dreaming up new types of post-heffalump castles and telling each other about them at wizards conclaves.

And still no-one had ever seen a real heffalump.

A heffalump is an elephant-like creature in the Winnie-the-Pooh stories by A. A. Milne.

A thaler is one of the large silver coins minted by the Holy Roman Empire and the Habsburg monarchy.

Post-quantum migration refers to updating systems and applications to use only implementations of quantum-resistant cryptographic hash functions, MACs, cryptographic algorithms, key exchange schemes, and digital signature schemes.

The Mosca theorem (Figure 2.2) , named after the Canadian mathematician and computer scientist Michele Mosca, helps to understand the timeline for post-quantum migration.

Figure 2.2: Mosca theorem (source: Bosch Research blog 2022)

- **x** is the security shelf life; it refers to how long data encrypted with this particular cryptographic scheme must remain secure against quantum computing attacks after post-quantum migration has been completed;
- **y** is the migration time; it refers to how much time will be needed to migrate from this particular cryptographic scheme to a quantum-secure cryptographic scheme;
- **z** refers to the time when a quantum computer will be available that is capable of breaking this particular cryptographic scheme.

If **(x + y) < z** for a particular cryptographic scheme, i.e. a cryptographic algorithm using a set of particular parameters such as the cryptographic key size, **z - (x + y)** is the maximum time available for migration.

If **(x + y) > z** for a particular cryptographic scheme, it will be vulnerable to "harvest-now, decrypt-later" attacks during **(x + y) - z** time (this is sometimes referred to as the Mosca inequality).

Current Quantum-Resistant Cryptography (QRC) solutions for public-key cryptography mostly focus on several different approaches, including MPCitH-based cryptography, code-based cryptography, lattice-based cryptography, multivariate-based cryptography, isogeny-based cryptography and hash-based cryptography. These QRC approaches are described in Appendix A.

The goal of the US National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) competition is to develop and standardise replacements for public-key cryptographic primitives which are widely used in practice, but are vulnerable to attacks performed with quantum computers. NIST will develop and standardise both quantum-resistant cryptographic primitives that provide authenticity and quantum-resistant cryptographic

primitives that provide secrecy. The current status of NIST's PQC competition is described in Appendix B.

2.1. Post-quantum migration scenarios

First of all, any cryptographic hash function (such as for example MD5), MAC scheme (such as for example CBC-MAC) or symmetric encryption algorithm (such as for example TDES) that is not quantum-resistant should either be upgraded to use a larger (underlying) hash value, authentication code or cryptographic key size (if at all possible) or else replaced by a quantum-resistant mechanism.

One approach for mitigating the risks posed by the future availability of CRQCs to vulnerable public-key cryptographic schemes (including key exchange and digital signature mechanisms) is to physically isolate and strongly protect critical data assets, to prevent eavesdropping and unauthorised manipulation. A major issue with this approach is that physically isolating data usually makes it far less valuable.

There are several other approaches for mitigating these risks that mainly large organisations can choose from (in contrast, small organisations and consumers often have little choice other than relying on their ICT technology providers to migrate to quantum-resistant cryptography):

- Using secure physical distribution of secret keys, e.g. by means of physical transport using cryptographic hardware tokens. This approach is very cumbersome, extremely slow and precludes many use cases.

- Using Quantum Key Distribution (QKD) or QKD Network (QKDN) solutions for the establishment of shared secret keys (see Appendix C). This approach is (very) expensive and, in the case of QKD, currently mostly limited to point-to-point secret key establishment using fibre-optic cables (over relatively short geographical distances) or free-space (satellite) communication channels. Furthermore, in general, QKD(N) is not considered a direct solution to the quantum computing cryptanalysis threat (though it could be part of such a solution) because QKD(N) security is inherently tied to the physical layer and QKDN cannot be used to protect information sent through its network nodes hence these nodes have to be trusted ("trusted relays"). Consequently, QKD(N) is not aligned with modern information security principles, such as end-to-end encryption and zero-trust. It is also important to note that QKD(N) updates will typically require changing hardware and/or firmware of QKD(N) equipment, whereas QRC upgrades will typically be delivered as software updates. QKD(N) solutions will mostly only be used for specific use cases such as for example encryption of communication links between data centres.

- Using a Key Derivation Function (KDF, Box 2.1), to mix keying material obtained from different sources, such as Pre-Shared Keys (PSKs, Box 2.2), QKD(N) keys, classic key exchange schemes

and QRC key exchange schemes, into shared secret keys. When using PSKs, this approach necessitates keeping pairwise shared cryptographic key material, which is very cumbersome to implement and is therefore only an option for use cases where a limited set of entities is involved. This is also the case when using QKD(N) keys.

A Key Derivation Function (KDF) is used in cryptography to derive multiple secrets (KDF outputs) from one or more other secrets (KDF inputs). A KDF is often used in security protocols that require participants to rederive the same key several times and is therefore expected to be deterministic. A KDF is usually not designed to produce a lot of derived secrets.

Box 2.1: Key Derivation Function (KDF)

A Pre-Shared Key (PSK) is a secret key which was previously shared between two parties using a secure (typically out-of-band) communication channel, before it is put into use by some cryptographic mechanism.

Box 2.2: Pre-Shared Key (PSK)

- Replacing key exchange schemes based on vulnerable public-key cryptography with PSK-based schemes (note that the PSK could be a QKD key). Many cryptographic security protocols, including IPsec, TLS and SSH, support the use of PSK-based key exchange schemes. This approach has the same disadvantage as the KDF approach.

- Using key exchange or digital signature QRC schemes that have been standardised by NIST (see Appendix B) and for which vendor-supported or open-source products are available.

- Using other QRC schemes (see Appendix A) for which vendor-supported or open-source products are available. A major issue with this approach is that, in many cases, the security of such QRC schemes and/or products has not been independently verified.

- Using a combination of two or more key exchange or digital signature schemes. At least one of the schemes defends against classical attacks and at least one of the schemes (the same one or another one) defends against CRQC attacks.

  In common practise, this will be hybrid classical/quantum schemes, where one of the schemes is a “proven” classical scheme (to withstand classical cryptanalysis) and (one of) the other scheme(s) is a QRC scheme (to withstand quantum cryptanalysis using CRQCs). This can be implemented in such a way that backwards compatibility is achieved for entities that do not yet support QRC schemes. However, in this case, care should be taken to prevent downgrade attacks (i.e. attacks where an attacker makes a party supporting QRC believe that the other party doesn’t).

  Notes

  1. Hybrid classical/QRC schemes may involve using hybrid public-key certificates that contain multiple sets of public keys and their signatures.

2. Several widely-used classical key exchange mechanisms allow for negotiation of cryptographic schemes and could thus be adapted for the use of hybrid classical/QRC schemes. For example, an IETF standard for hybrid key exchange in TLS1.3 has already been developed.

3. The combined classical/QRC scheme approach could be used to maintain the security certification obtained for a specific application or system if certification (or compliance) mandates the use of (a) specific classical scheme(s).

- Using quantum-resistant hash-based signature schemes, such as XMSS, XMSSMT, LMS or HSS, which have already been standardised by NIST and for which vendor-supported or open-source products are available. However, the security of these particular signature schemes is dependent on careful state management to ensure that signatures are only used once or a few times. They are therefore limited to specific use cases. An example is the use of XMSS for code signing.

- Waiting until standardised QRC signature schemes become available to replace classical signature schemes that are not quantum-resistant. The public keys used by the classical signature schemes must be revoked before the advent of CRQCs, so as to render all their signatures invalid before the CRQC threat becomes manifest. This may also require replacing existing classical signatures with quantum-resistant signatures.

Because an appropriate post-quantum risk mitigation technique depends on several factors, which may be different for various use cases, it is very likely that organisations will need to follow an hybrid mitigation scenario by selecting multiple mitigation approaches from the list above.

In some cases, ii may also be possible to implement application/system specific post-quantum solutions. For example, if highly sensitive data is transferred that is protected by means of vulnerable classical cryptography and it is not feasible or not practical to change the sending and/or receiving application, an option may be to set up a quantum-safe VPN through which the application traffic is routed.

2.2. Post-quantum migration considerations

A particular quantum-resistant public-key cryptographic scheme will most likely support only a limited set of use cases and it is therefore expected that NIST will standardise different QRC schemes for different types of applications and usage contexts.

Furthermore, existing cryptographic security protocols need to be modified to accommodate the particular characteristics of quantum-resistant public-key cryptographic schemes, e.g. long cryptographic keys, long ciphertexts or long digital signatures. So called “drop-in replacements” are not likely to be feasible in many cases for adapting these security protocols and (partial) protocol redesign will be required.

In some cases, replacing cryptography schemes might even be impossible. Examples: legacy systems that are no longer supported by their vendors, hardwired systems that cannot be changed/updated and systems with restricted accessibility (e.g. satellite systems), resource constraints that prohibit the concurrent use of multiple cryptographic schemes. For environments where the update of cryptographic functions is not possible, it is important to consider the use of state-of-the-art cryptography to include implementations of the best and most conservative variants for each cryptographic function.

Migrating to new cryptographic schemes typically requires changing or replacing the following components: cryptographic libraries, implementation validation and certification tools, hardware that implements cryptographic algorithms or accelerates cryptographic algorithm performance, cryptography supporting operating system and application code, communications equipment, etc.

Furthermore, security procedures need to be adapted and also, installation, configuration and system administration documentation needs to be changed or replaced.

Removing support for deprecated and obsolete cryptographic algorithms is very challenging. Once an algorithm is determined to be weak, it is very difficult to eliminate all uses of that algorithm because many applications and environments may rely on it. Since algorithm transitions can introduce interoperability problems, protocol designers and implementers may be inclined to delay the removal of support for such algorithms.

Organisations must inventory their critical data assets, including the desired level of cryptographic protection and the duration of that protection.

It is important for organisations to ensure that all use cases of cryptographic schemes currently deployed to protect (critical) data assets are documented, together with the cryptographic parameters being used (algorithm domain parameters, cryptographic key lengths, etc.). Any dependencies between these cryptographic schemes must also be documented.

Cryptographic schemes that are deemed vulnerable to CRQCs need to be identified, and availability of potential solutions need to be investigated and documented. For each potential solution, it must be determined how it will affect the ICT infrastructure and the applications, to identify potential future infrastructure shortcomings and, if needed, to develop plans for addressing them.

Based on the information gathered, migration scenarios can be worked out and their priorities determined, preferably using a risk-based approach. Also, it is of vital importance that post-quantum cryptography considerations are discussed with (potential) vendors, service providers, contractors, business partners and other relevant third parties; these vendors and service providers should have a post-quantum roadmap in place.

It goes without saying that a lot of effort is required to accomplish all of the above. However, most of it is in fact always required when cryptography solutions are deployed, to ensure that there are

adequate plans for smooth migration to new cryptographic schemes whenever currently used schemes are compromised or run the risk of being compromised in the near future.

Today, very few organisations have such plans readily available; most of them have only recently become aware of this issue due to the enormous amount of publicity given to the emerging quantum computer threats to existing cryptography in (social) media and professional journals.

Furthermore, few organisations have a centralised policy in place for the use of cryptography because it has become very easy to implement and use cryptographic solutions. Consequently, these organisations are neither aware of the types of encryption used by their IT infrastructure and applications, nor where such cryptography is being is used.

Therefore, organisations should immediately implement so-called “low-regret moves”:

- create awareness about the extent of information security that is provided by cryptography (crypto visibility);
- create awareness for emerging quantum computing threats to cryptography (quantum computer threat awareness);
- monitor progress of quantum computing, quantum security and quantum-resistant cryptography technologies;
- develop a strategy for adopting and integrating new cryptographic schemes (crypto agility).

Cryptographic (crypto) agility describes the capabilities needed to replace and adapt cryptographic algorithms for security protocols, applications, software, hardware and infrastructures without interrupting the flow of running systems. Properly designed operational mechanisms that incorporate crypto agility considerations are needed to facilitate transition to newer algorithms in a fast and smooth way without introducing security breaches or operational disruptions. Achieving crypto agility is not only a task for product designers or implementors but also for practitioners, security policy makers and ICT administrators.

In general, migration to quantum-resistant public-key cryptographic schemes will take a significant amount of time. For example, NIST cautions that, after publication of the first set of PQC standards in 2024 (see Appendix B), five to fifteen more years will be needed for completing migration to PQC cryptography.

In some cases, migration to new cryptographic schemes will take a very long time to implement because there are many parties involved. Examples: Public Key Infrastructure (PKI) infrastructures operated by Trust Service Providers (TSPs), Distributed Ledger Technology (DLT) infrastructures and electronic payment infrastructures.

Migration to quantum-resistant cryptography as described above should not be considered to constitute a long-term cryptographic solution for an organisation, for several reasons:

- Though using hybrid key-establishment schemes or hybrid signature schemes can be a good strategy for preserving security in the face of uncertainty while transitioning from traditional public-key cryptography to post-quantum cryptography, the use of hybrid schemes increases protocol complexity and the amount of resources consumed. Note that protocol complexity can lead to portions of the implementation being rarely used, thus increasing the opportunity for undiscovered, exploitable implementation bugs.

- There is no guarantee that the proposed QRC schemes will be capable of withstanding classical attacks for a reasonable amount of time, as these schemes have been subjected to far less classical cryptanalysis than the widely used pre-quantum public-key cryptographic schemes they are meant to replace. Several proposed QRC schemes have already been successfully attacked by classical cryptanalysis (see § B.3 for some examples).

  Successful classical cryptanalysis of a QRC scheme could annihilate the protection provided by hybrid classical/quantum key exchange or digital signature schemes (see § 2.1), e.g. by breaking the classical scheme with quantum cryptanalysis by means of a CRQC and breaking the QRC scheme with classical cryptanalysis.

  Note
  The threats posed by hybrid classical/quantum cryptanalysis are often overlooked in publications related to hybrid classical/quantum key exchange and digital signature schemes.

- QRC protection against quantum computing threats is currently focused on providing resistance against Shor's and Grover's quantum algorithms. However, many a time a new quantum algorithm is discovered that could potentially be used to attack cryptographic schemes. Examples: Abelian hidden shift algorithm, BDD algorithm, BHT algorithm, claw finding attack algorithm, dHSP algorithm, EDCP algorithm, HHL algorithm, Kuperberg's algorithm, Tami's algorithm, etc. In principle, such a quantum algorithm could be adapted so as to be capable of breaking a specific type of QRC scheme.

  Furthermore, cryptographic schemes can be attacked by means of NISQ quantum computers (Box 2.3) or Quantum Annealers (QAs, Box 2.4). For example, lattice-based QRC schemes have been attacked because the hard problem of lattice-based cryptography is merely an optimisation problem that could be solved by NISQ quantum computers or QAs.

Noisy Intermediate-Scale Quantum (NISQ) applies to current state-of-the-art quantum computers. The term “noisy” refers to the fact that these quantum computers are very sensitive to the surrounding environment and may lose their quantum state due to quantum decoherence (loss of quantum coherence) because they are not sophisticated enough to implement quantum error correction. The term “intermediate-scale” refers to the not-so-large number of qubits of contemporary quantum computers.

Box 2.3: Noisy Intermediate-Scale Quantum (NISQ)

Quantum annealing is a restricted form of adiabatic quantum computing, consisting of slowly evolving a quantum system from its ground state to its final state, which encodes a computational problem. It is used for finding the global minimum of a given objective function over a given set of candidate solutions. An objective function is either a cost function or a profit function, which an optimisation solution seeks to minimise (cost function) or maximise (profit function).

Box 2.4: Quantum annealing

Successful quantum cryptanalysis of a QRC scheme (by means of a CRQC) could annihilate the protection provided by hybrid classical/quantum key exchange or digital signature schemes (see § 2.1).

Successful quantum cryptanalysis (by means of a CRQC) of a currently widely used cryptographic hash function, MAC or symmetric cryptographic algorithm could have far-reaching consequences for post-quantum migration as the assumptions in § 1.1 would be no longer valid.

- Quantum computing based cryptanalysis is severely constrained because neither currently available quantum computers nor quantum emulators are powerful enough to enable performing meaningful attacks on the proposed quantum-resistant public-key cryptographic schemes.

- Even if the quantum algorithm(s) for breaking a particular QRC scheme would be known, it is very difficult to determine the computing and memory costs of (a) quantum computer(s) capable of running the quantum algorithm(s), given the current state-of-the-art of quantum computing. It is therefore still unclear how to choose QRC scheme parameter settings that are needed for resistance against attacks by future quantum computers. The parameter settings of cryptographic schemes often have a profound effect on the cryptographic key size, on the ciphertext size or signature size, and on the encryption/decryption or signature generation/verification time.

- Last but not least: cheaper, improved or entirely new quantum security technologies might and probably will emerge that could possibly be used as viable replacements for the quantum-resistant solutions (or parts thereof) described above.

As can be seen from the list above, there are still a lot of uncertainties that organisations must cope with. It can be expected that organisations will assess these uncertainties differently and consequently make different choices for their post-quantum migration strategy.

Appendix A - Quantum-resistant cryptography

A.1 MPC-in-the-Head cryptography

Unlike most other public-key cryptography, MPC-in-the-Head (MPCitH) cryptography is not based on hard problems from number theory. Instead, it is based on a proving algorithm that simulates a MPC protocol (Box A.1).

Multi-Party Computation (MPC), also known as secure computation or privacy-preserving computation, relates to the use of cryptography for creating methods for parties to jointly compute a function over their inputs, while keeping those inputs private. Unlike most traditional usage of cryptography, where adversaries are outside the system of participants (such as an eavesdropper on the sender and receiver), MPC cryptography protects participants' privacy from each other.

By revealing the views of a random subset of MPC parties, a Zero-Knowledge Proof (ZKP) is formed, where one party can convince another party that it knows a secret without disclosing the secret itself. ZKP is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while the prover avoids conveying any additional information apart from the fact that the statement is indeed true. The essence of ZKPs is that it is trivial to prove that one possesses knowledge of certain information (e.g. by simply revealing it); the challenge is of ZKP to prove such possession without revealing the information itself or any additional information about it.

In practice, most zero-knowledge proofs are based on the following three-step mechanism:

1. the prover generates some random value (the commitment) and sends it to the verifier;
2. the verifier responds with a challenge value generated uniformly at random;
3. the prover computes the final proof based on both the commitment and challenge.

Most ZKP mechanisms are interactive, meaning that the provers require a response from the verifiers before they can complete their proof, which is not suitable for many applications. Fortunately, provers can avoid this by using the Fiat-Shamir (FS) heuristic, named after the Israeli cryptographer Adi Shamir and the Israeli computer scientist Amos Fiat, a well-known technique for taking an interactive ZKP and creating a digital signature based on it (sometimes referred to as the FS transformation). The idea behind the FS heuristic is that instead of having the verifier send a random challenge value to the prover, the prover can compute this value itself by using a random function, such as a cryptographic hash function.

Box A.1: Multi-Party Computation (MPC)

For QRC purposes, the MPC/ZKP concept is combined with symmetric cryptography, hash functions and block ciphers, to create a novel digital signature scheme. The hard problems that MPCitH relies on therefore relate only to hash functions and block ciphers, which are thought to be secure against quantum computer attacks.

An example is the Picnic digital signature scheme, which has been selected as an alternate candidate for the third round of the NIST PQC competition (see Appendix B) but will not be

standardised by NIST. Picnic was developed in collaboration with researchers and engineers from Microsoft Research and various research institutes and universities in Europe and the US.

Other MPCitH examples are Mirath, MQOM, PERK, RYDE and SDithH, which have been selected by NIST as second-round candidates in October 2024 to move forward to the next stage of the standardisation process for additional quantum-resistant signature schemes (see Appendix B).

A.2 Code-based cryptography

Code-based cryptography relies on the properties of error-correcting codes. For some specially constructed codes it is possible to correct many errors, but for random linear codes this is a hard problem. Examples of code-based cryptography are the McEliece encryption algorithm (based on random Goppa codes, Box A.2) developed by by the American mathematician Robert J. McEliece, the Niederreiter encryption algorithm (based on Reed-Solomon codes, Box A.3) developed by the Austrian mathematician Harald G. Niederreiter, and the related CFS digital signature scheme developed by the French cryptographers Nicolas Tadeusz Courtois, Matthieu Finiasz and Nicolas Sendrier. The original McEliece signature using random Goppa codes has withstood scrutiny for several decades. However, many variants of the McEliece scheme, which aim to introduce more structure into the code used in order to reduce the size of the keys, have been shown to be insecure.

A Goppa code is a type of error-correcting code and is based on modular arithmetic, which is when a series of numbers increases towards a certain number and upon reaching that number, starts back over at zero again.

Box A.2: Goppa code

Reed–Solomon codes are a group of error-correcting codes that operate on a block of data treated as a set of finite-field elements called symbols. Reed–Solomon codes are able to detect and correct multiple symbol errors.

Box A.3: Reed–Solomon codes

Other examples of code-based cryptography are Hamming Quasi-Cycle (HQC), which is based on Hamming codes (Box A.4) and was developed by Worldline and French universities, and Bit Flipping Key Encapsulation (BIKE), which is based on Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) codes and was developed by Google, Intel, Worldline, INRIA and French, German, Israeli and US universities.

Hamming codes are a family of linear error-correcting codes. Hamming codes can detect one-bit and two-bit errors, or correct one-bit errors without detection of uncorrected errors.

Box A.4: Hamming codes

QC-MDPC codes are variants of Moderate Density Parity-Check (MDPC) codes (Box A.5). MDPC allows for fast encoding and decoding while also being able to correct a lot of errors. The name originates from the appearance of the parity-check matrix. MDPC codes have parity-check matrices which contain a lot of zeroes and very few ones. The density of these parity-check matrices equal the percentage of ones in the entire matrix. MDPC codes have densities in the order of approximately 0.5% or more.

Hamming codes are a family of linear error-correcting codes. Hamming codes can detect one-bit and two-bit errors, or correct one-bit errors without detection of uncorrected errors.

Box A.5: MDPC codes

A.3 Lattice-based cryptography

Lattice-based (Box A.6) cryptography algorithms is based on hard problems in the lattice vector space.

A lattice is a poset (a poset is a partially ordered set), in which every pair of elements has both a least upper bound and a greatest lower bound. In other words, it is a structure with two binary operations: join and meet.

Box A.6: Lattice

A lattice is a poset (a poset is a partially ordered set), in which every pair of elements has both a least upper bound and a greatest lower bound. In other words, it is a structure with two binary operations: join and meet.

The most well-known of these hard problems are:

- the Shortest Vector Problem (SVP): find the shortest non-zero vector in a lattice;
- the Closest Vector Problem (CVP): for a coordinate that is not on the lattice, find the closest point to that coordinate on the lattice.

There exist algorithms such as the Lenstra–Lenstra–Lovász (LLL) and the Block-Korkine-Zolotarev (BKZ) algorithms to solve both of these problems (CVP can be reduced to SVP). These algorithms reduce the basis of a lattice, attempting to find a base set of vectors that are shorter than the ones given to produce the given lattice. However, these algorithms are not at all efficient or even practical. Thus, the SVP and CVP problems are considered to be hard until an efficient and practical solution will be discovered.

Lattice-based cryptography includes cryptographic systems such as the Learning With Errors (LWE) and Ring Learning With Errors (Ring-LWE) encryption schemes, the Ring-LWE key exchange scheme, the Learning With Rounding (LWR) encryption scheme, the older N-th Degree Truncated

Polynomial Ring Units (NTRU) and Goldreich–Goldwasser–Halevi (GGH) encryption schemes, and the newer NTRU-Prime and Bimodal Lattice Signature Scheme (BLISS) signature schemes.

Lattice-based cryptography began in 1996 from a seminal work by the Hungarian-American computer scientist Miklós Ajtai who presented a family of one-way functions based on the Short Integer Solution (SIS) problem. Also in 1996, GGH was introduced by Goldreich, Goldwasser and Halevi.

NTRU was also introduced in 1996 by Hoffstein, Pipher and Silverman. In 1988, it was presented as an alternative to RSA and ECC, offering higher speed at the expense of larger key size and larger ciphertext size. NTRU-Prime was introduced by Daniel Bernstein, Tanja Lange, Christine van Vreedendaal and others in 2016.

Olev Regev introduced LWE in 2005. LWE and Ring-LWE key exchange schemes were first proposed in 2012 by Jintai Ding. Ding's idea was expanded in 2014 by Chris Peikert and in 2015, an authenticated key exchange scheme with provable forward security was presented at Eurocrypt.

IEEE 1363.1 (IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices) was published in 2008. This standard provides specifications of common public-key cryptographic techniques based on hard problems over structured lattices, including mathematical primitives for secret value (key) derivation, public-key encryption, identification and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys are also included.

LWR was introduced by Abhishek Banerjee, Chris Peikert and Alan Rosen in 2012. It is a variant of LWE, where random errors are replaced by deterministic rounding.

"Module" variants of LWE, Ring-LWE, LWR and Ring-LWR were introduced to address some shortcomings in these cryptographic schemes.

BLISS was introduced by Ducas, Durmus, Lepoint and Lyubashevsky in 2013.

Many proposed QRC algorithms use structured lattice-based cryptography and about half of NIST's PQC round 3 finalists and alternate candidates were based on it:

- CRYSTALS-Kyber key encapsulation scheme (Cyclotomic Module-LWE problem);
- CRYSTALS-Dilithium digital signature scheme (Cyclotomic Module-LWE and Module-SIS problem);
- FALCON digital signature scheme (Cyclotomic Ring-SIS problem);
- Frodo-KEM key encapsulation scheme (LWE problem);
- NTRU key encapsulation scheme (Cyclotomic NTRU problem);
- NTRU-Prime key encapsulation scheme (Non-cyclotomic NTRU or Ring-LWE problem);
- SABER key encapsulation scheme (Cyclotomic Module-LWR problem).

Both the CRYSTALS-Kyber key exchange scheme and the CRYSTALS-Dilithium digital signature scheme are based on the Cryptographic Suite for Algebraic Lattices (CRYSTALS) algorithm.

The main advantage of the Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) digital signature scheme is that its signatures are smaller than those of CRYSTALS-Dilithium.

A.4 Multivariate-based cryptography

Multivariate-based cryptography is based on the difficulty of solving systems of multivariate equations (Box A.7).

Multivariate equations are equations containing more than one variable. When faced with a multivariate equation, one may either wish to find a numeric value for each variable, or solve the equation for one variable in terms of the other variables.

Box A.7: Multivariate equation

Attempts to develop secure multivariate-based based encryption schemes have failed until now. However, multivariate digital signature schemes like Unbalanced Oil and Vinegar (UOV), Rainbow (a variation of UOV), Hidden Field Equations vinegar minus (HFEv-) and Great Multivariate Short Signature (GeMSS) are deemed suitable as QRC digital signature schemes. Rainbow was successfully attacked using only a laptop computer for a couple of days, and has therefore been withdrawn.

A.5 Isogeny-based cryptography

Isogeny-based (Box A.8) cryptographic schemes are based on the mathematics of isogenies of supersingular elliptic curves (a specific subclass of elliptic curves) over finite fields, which can be used to create key exchange schemes that can serve as a quantum-resistant replacement for the widely used classical Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) classical key exchange schemes.

An elliptic curve isogeny is a non-constant function, defined on an elliptic curve, that takes values on another elliptic curve and preserves point addition. Elliptic curve endomorphisms (i.e. morphisms from a mathematical object to itself) are isogenies from an elliptic curve to itself. These isogenies are a source of exponentially-sized graphs, which connects nodes on a ring, with each node represents a particular endomorphism. These graphs are well connected so that any node in the graph can be reached in a few steps from (almost) any other node (this is called “rapid mixing”); these steps constitute a (short) path. There are no known efficient classical or quantum algorithms to recover such paths from endpoints; this is the hard problem on which isogeny-based cryptography relies.

Box A.8: Elliptic curve isogeny

Isogeny-based cryptographic schemes have small public key and ciphertext sizes. Supersingular Isogeny Diffie-Hellman (SIDH), Commutative Supersingular-Isogeny Diffie-Hellman (CSIDH) and Supersingular-Isogeny Key Encapsulation (SIKE) are the best known such schemes.

The SIDH key exchange scheme was published in 2011 by Luca De Feo, David Jao, and Jérôme Plut. In 2012, Xi Sun, Haibo Tian and Ymin Wang extended the work of De Feo, Jao, and Plut, to create quantum secure digital signature schemes based on supersingular elliptic curve isogenies. The public key length of the original schemes was quite long but subsequent optimisations reduced it to roughly the same size as for non-quantum DH schemes at the same level of security.

The CSIDH key exchange scheme was published in 2011 by researchers Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny and Joost Renes of TU/e, Radboud University and KU Leuven.

The SIKE encryption scheme evolved from the need to make SIDH resistant to Chosen-Ciphertext Attacks (CCAs). SIKE was developed by researchers from Amazon, Microsoft, Texas Instruments, the University of Waterloo, Université de Versailles and Radboud University. It was subsequently successfully attacked and has therefore been withdrawn.

A.6 Hash-based cryptography

All practical digital signature schemes use cryptographic hash functions as one of their components, to enable efficient signing of messages and documents of arbitrary sizes. But it is also possible to design digital signature schemes that are solely based on hash functions. Such schemes tend to rely only on the pre-image resistance and not on the collision resistance of the hash function for their security proofs, which is very attractive because several solid and well-understood hash functions providing strong pre-image resistance have already been developed.

Hash-based digital signatures were introduced by Ralph Merkle in 1979 with the publication of the Merkle Signature Scheme (MSS). Also in 1979, Leslie Lamport published the concept of a One-Time Signature (OTS) scheme, which uses key pairs that can only be used to sign once.

The eXtended Merkle Signature Scheme (XMSS) is a stateful hash-based signature scheme, which is specified in RFC 8391 and has been standardised by NIST (SP 800-208). It adds a number of optimisations to the MSS scheme. It reduces the size of the private key by deterministically generating each one-time signature in the tree using a seed and the leaf position in the tree. The seed is stored as a private key, instead of all the one-time signature private keys, and it is possible to quickly regenerate any one-time signature key pair from its position in the tree and the seed. To keep track of which leaf one-time signature was used last, the private key also contains a counter that is incremented every time it is used to sign. However, the larger the Merkle tree, the longer it takes to regenerate the tree in order to be able to produce a signature, because all the leaves must be regenerated to produce a Merkle proof; this obviously limits the number of

signatures for which the same key pair can be used. The solution is to use a smaller tree where the one-time signatures in its leaves are not used to sign messages but instead used to sign the root hash of other Merkle trees of one-time signatures. This transforms the Merkle tree into a hypertree (a tree of trees) and is one of the variants of XMSS called Multi-tree XMSS (XMSSMT). With XMSSMT, only the trees involved in the path of a one-time signature need to be regenerated.

Many of the proposed hash-based signature schemes build on the foundations created by Lamport, to allow for many more signatures (sometimes practically unlimited), stateless private keys (but some proposed schemes are still stateful) and more practical parameter sizes. Shortly after Lamport's publication, Robert S. Winternitz proposed the Winternitz One-Time Signature (WOTS) scheme. In WOTS, in order to optimise the size of the private key, hashes of hashes of a secret h(h(...h(x))) = hw(x) are published instead of multiple digests of multiple secrets.

Few-Time Signatures (FTS) schemes were developed to overcome the limits imposed on the number of times a key pair can be used. These schemes rely on low probabilities of reusing the same combination of secrets from a pool of secrets and will protect against signature forgeries unless the key pairs are used too many times.

A major drawback of most hash-based digital signatures is that there is a limit on the number of signatures that can be signed using the same private key; many of them are one-time or bounded-time signatures. This limitation could be overcome by generating a large number of one-time key pairs instead of a single one and discarding a key pair after it has been used. However, this would not only require the public key size to fit the number of signatures that will be used, but would also require keeping track what key pairs have been used, i.e. the scheme has to be "stateful".

The statefulness of digital signature schemes might not be an issue in some use cases, but it is not a desirable property since it requires that users of these signature schemes keep track of a counter. This requirement can lead to signature forgery if the counter mechanism is not correctly implemented. For example, rollback to a previous state of a filesystem, or multiple servers that are concurrently using the same signing key, might induce the same path in the hypertree being used twice to produce signatures.

To overcome the statefulness problem of XMSSMT, the Stateless Practical Hash-based Incredibly Nice Cryptographic Signatures plus (SPHINCS+) signature scheme was developed for NIST's PQC competition (see Appendix B). The stateless SPHINCS+ signature scheme augments XMSSMT with three major changes:

1. The path used in the hypertree is deterministically derived, based on the private key and the message. This ensures that signing the same message twice leads to the same signature and also, because the private key is used, attackers are also unable to predict which path will be taken to sign an attacker's message.

2. To do this, SPHINCS+ simply uses a much larger amount of one-time-signatures, reducing the probability of reusing the same one twice when it chooses a path on a (pseudo)random basis. Because SPHINCS+ also uses a hypertree, this translates into more trees.

3. SPHINCS+ replaces the final one-time-signature mechanism used to sign messages by a few-times signature mechanism. This way, reusing the same path to sign two different messages still doesn't directly contribute to a break of the signature scheme.

The main disadvantages of SPHINCS+ are that it slow and that its signatures are large compared to those of the FALCON and CRYSTALS-Dilithium PQC digital signature schemes.

Appendix B – Post-Quantum Cryptography (PQC)

Public-key cryptographic primitives consist of:

1. Authenticity cryptographic primitives: relate to digital signature schemes, which consist of:
   - a key generation algorithm to generate a private/public key pair;
   - a signature algorithm to generate a signature from a message and the private key;
   - a verification algorithm to verify the message signature with the public key.

2. Secrecy cryptographic primitives: relate to public-key cryptographic schemes, key encapsulation schemes or key exchange schemes.

   A public-key cryptographic scheme consists of:
   - a key generation algorithm to generate a private/public key pair;
   - a public-key encryption algorithm to generate a ciphertext from a plaintext with either the public key or the private key;
   - a public-key decryption algorithm to generate the plaintext from the ciphertext with the corresponding private or public key.

   A key encapsulation scheme consists of:
   - a key generation algorithm to generate a private/public key pair;
   - an encapsulation algorithm to generate a session key and a ciphertext with the either the public key or the private key;
   - a decapsulation algorithm to generate the session key from the ciphertext with the corresponding private or public key.

   A key exchange scheme consists of a protocol that provides a session key to the protocol participants.

   NIST decided to only standardise key encapsulation schemes, called Key-Encapsulation Mechanisms (KEMs), because it is possible to construct both key exchange schemes and public key cryptographic schemes with KEMs.

B.1 NIST first call for PQC proposals

In December 2016, NIST issued an open Call for Proposals for PQC algorithm submissions, together with the specification of mathematical, security and performance capabilities required for candidate algorithms, and the different types of use cases that are considered. This resulted in 82 initial submissions at the end of 2017, of which 69 were deemed suitable PQC candidates.

The retained candidate PQC algorithms were subjected to two rounds of cryptanalysis (including use of quantum algorithms) and performance testing, and their suitability for currently used (classic) computing platforms was investigated.

At the beginning of 2019, 28 PQC proposals survived the first round. In July 2020, 7 finalists and 8 alternative candidates that survived the second round were selected for entry into the third PQC competition round.

The finalists selected for the third PQC competition round were:

- Classic McEliece (code-based KEM scheme);
- CRYSTALS-Dilithium (lattice-based signature scheme);
- FALCON (lattice-based signature scheme);
- CRYSTALS-Kyber (lattice-based KEM scheme);
- NTRU (lattice-based KEM scheme);
- Rainbow (multivariate-based signature scheme);
- SABER (lattice-based KEM scheme).

The alternate candidates selected for the third PQC competition round were:

- BIKE (code-based KEM scheme);
- Frodo-KEM (lattice-based KEM scheme);
- GeMSS (multivariate-based signature scheme);
- HQC (code-based KEM scheme);
- NTRU-Prime (lattice-based KEM scheme);
- Picnic (signature scheme based on zero-knowledge proofs and a block cipher);
- SIKE (isogeny-based KEM scheme);
- SPHINCS+ (hash-based signature scheme).

The following evaluation criteria have been used to select these finalists and alternate candidates:

- security (e.g. security proof, classical and quantum cryptanalysis resistance and side channel resistance);
- key size;
- ciphertext/digital signature size;
- performance (e.g. execution speed and memory requirements);
- algorithm and implementation characteristics (e.g. simplicity and flexibility).

NIST PQC defines five levels of security (i.e. resistance against both classical and quantum attacks):

1. At least as hard to break as AES-128 exhaustive key search: any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES-128).

2. At least as hard to break as SHA-256 collision search: any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA-256 or SHA3-256).

3. At least as hard to break as AES-192 exhaustive key search: any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES-192).

4. At least as hard to break as SHA-384 collision search: any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA-384 or SHA3-384).

5. At least as hard to break as AES-256 exhaustive key search: any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES-256).

In July 2022, NIST selected four PQC schemes for standardisation. NIST recommends two primary algorithms to be implemented for most use cases: CRYSTALS-Kyber (lattice-based KEM scheme) and CRYSTALS-Dilithium (lattice-based digital signature scheme). CRYSTALS-Kyber and CRYSTALS-Dilithium were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications.

In addition, the digital signature schemes FALCON (lattice-based) and SPHINCS+ (hash-based) will also be standardised. FALCON was selected since there may be use cases for which CRYSTALS-Dilithium digital signatures are too large. SPHINCS+ was selected to avoid relying only on the security of structured lattices for digital signature schemes.

The following PQC schemes were selected to advance to the fourth PQC round: BIKE (code-based), Classic McEliece (code-based), HQC (code-based) and SIKE (isogeny-based). BIKE, Classic McEliece and HQC use code-based cryptography, and either would be suitable as a general-purpose KEM that is not based on structured lattices.

In August 2024, NIST released FIPS standards for the first three PQC algorithms:

1. FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), based upon the CRYSTALS-Kyber algorithm;

2. FIPS 204 - Module-Lattice-Based Digital Signature Algorithm (ML-DSA), based upon the CRYSTALS-Dilithium algorithm;

3. FIPS 205 - Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), based upon the SPHINCS+ algorithm.

A fourth standard, FIPS 206 - FFT over NTRU-Lattice-Based Digital Signature Algorithm (FN DSA), based upon the FALCON algorithm, is expected to be released later.

In March 2025, NIST announced that the HQC code-based KEM scheme will be standardised. HQC was selected for standardisation because its security analysis was found to be more mature and stable than that of the BIKE code-based KEM scheme.

The SIKE isogeny-based KEM scheme was not selected for standardisation because several security weaknesses have been discovered.

The Classic McEliece code-based KEM scheme was not selected for standardisation because NIST does not anticipate it being widely used due to its large public key size.

B.2 NIST second call for PQC proposals

NIST issued a call for proposals for additional quantum-resistant signature schemes in September 2022. NIST is primarily looking to diversify its signature portfolio, so general-purpose signature schemes that are not based on structured lattices are of greatest interest, but NIST is also interested in additional signature schemes that have short signatures and fast verification. Any submission based on structured lattices is expected to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

In July 2023, NIST announced that it received 50 submissions (from 28 countries), of which 40 candidate signature schemes are deemed to satisfy all submission requirements. These candidate schemes fall in the following categories:

- MCPitH-based cryptography: 7 digital signature schemes;
- code-based cryptography: 5 digital signature schemes;
- lattice-based cryptography: 7 digital signature schemes;
- multivariate-based cryptography: 11 signature schemes;
- isogeny-based cryptography: 1 digital signature scheme;
- symmetric cryptography-based: 4 digital signature schemes;
- other: 5 digital signature schemes.

NIST initiated a new process for evaluation of these digital signature schemes, which is expected to be much smaller in scope than the 2016 PQC process. Nevertheless, the signature schemes will need to be thoroughly analysed, which will likely take several years.

Based on the public feedback and internal reviews of the first-round candidates, NIST announced the selection of 14 digital signature algorithms as second-round candidates in October 2024 to move forward to the next stage of the standardisation process. These candidates are:

- MCPitH schemes: Mirath (merger of MIRA and MiRitH), MQOM, PERK, RYDE and SDithH;
- code-based schemes: CROSS and LESS;
- lattice-based scheme: HAWK;
- multivariate-based schemes: MAYO, QR-UOV, SNOVA and UOV;
- isogeny-based scheme: SQIsign;

- symmetric cryptography-based scheme: FAEST[5].

B.3 NIST PQC standardisation prognosis

After standardisation of the first set of PQC schemes, NIST's PQC effort will continue for many years to come. This effort will not only consist of updating and refining the selected PQC standards, but also intends to identify potential new PQC schemes and to ensure that there are strong back-ups for selected PQC standards, as the full extent of what might emerge in the area of CRQCs and their associated quantum algorithms remains unknown.

NIST's current view is that structured lattice-based cryptographic schemes appear to be the most promising general-purpose schemes. This is particularly true for digital signature schemes where the best PQC schemes that are not lattice-based have a substantial performance penalty for general-purpose use. Nonetheless, NIST believes it is prudent to continue to study PQC schemes that are not lattice-based as a hedge against unexpected progress in cryptanalysis.

NIST also recognises that current and future cryptographic research may lead to promising schemes which were not part of the NIST PQC standardisation project.

It is important to recognise that most of the proposed PQC schemes have not received nearly as much scrutiny from the cryptographic community as the currently widely used public-key cryptographic schemes. Further analysis and research may uncover that these PQC schemes are not secure enough for replacement of the current public-key cryptographic schemes. For example:

- A classical attack on the Rainbow multivariate-based PQC scheme has been discovered by IBM Research Zürich and this attack, which can be performed on a laptop during a weekend, has resulted in the abandonment of this NIST PQC third round finalist.

- A classical attack on the SIKE elliptic curve isogeny-based PQC scheme was discovered by researchers from KU Leuven. The attack can be performed on a single-core PC in about one hour. Consequently, SIKE has been removed from the fourth round of the NIST PQC competition.

[5] FAEST is a digital signature scheme constructed via a relatively new technique called VOLEitH. This technique is related to the MPCitH approach: both MPCitH and VOLEitH can be used to construct digital signature schemes whose unforgeability relies only on the security of some symmetric-key cryptographic algorithm (in the case of FAEST, this is AES).

- Researchers from NIST and KU Leuven discovered a new classical attack on the SPHINCS+ hash-based PQC scheme with parameter settings that provide level 5 security, when the SHA 256 hash function is being used.

- Researchers from the Center for Encryption and Information security of the Israel Defense Forces (IDF) have successfully performed so-called dual-lattice attacks on NTRU, LWE and LWR NIST PQC schemes.

- Researchers from the Dutch Centrum Wiskunde & Informatica (CWI) have solved the SVP problem for lattices with 180 dimensions in 52 days, using graphics cards on a single (classical) computer, while the record established four years ago for a 150 dimensional lattice involved several (classical) supercomputers working together for more than a year.

- Cryptoanalysis results during the third NIST PQC round have raised some concerns about the security of multivariate PQC schemes.

- Several NIST PQC schemes have been found to provide less than optimal resistance against Side-Channel Attacks (SCAs, Box B.1) and this will exclude them from certain use cases.

Side-Channel Attacks (SCAs) are based on information gained from the implementation of a cryptographic scheme, rather than exploiting weaknesses in the cryptographic scheme itself. Execution time, power consumption, electromagnetic emanation, or even heat, light, sound and vibrations that are produced by a cryptographic system can be exploited to perform side-channel attacks. Side-channel attacks may require (in depth) technical knowledge of the internal operation of an implementation, but so-called "black-box attacks" do not require such knowledge. Some types of side-channel attacks require physical access to the cryptographic system or its communication facilities, while others do not.

Note that electromagnetic emanation should not be confused with ElectroMagnetic Compatibility (EMC) and ElectroMagnetic Interference (EMI), which refer to technologies and standards for avoiding interference of all kinds of equipment with one another and with regulated radio waves such as broadcast radio/TV signals, mobile network radio signals, GPS signals, etc.

Box B.1: Side-Channel Attack (SCA)

Appendix C – Quantum Key Distribution (QKD)

Quantum cryptography (a misnomer for “secure quantum communication”) involves encoding of information transmitted from place to place in quantum states of qubits, as opposed to classical communication's use of bits. These qubits are sometimes called “flying qubits”, whereas the term “stationary qubits” represent the physical qubits used for local computation by a quantum device.

Already in the late 1960s, the concept of using quantum encoding of photons (Box C.1) for secure transmission of information was proposed by the Israeli-American physicist Stephen J. Wiesner.

The photon is an elementary subatomic particle. It is the quantum of the electromagnetic field (including electromagnetic radiation such as light and radio waves), and it is the force carrier for the electromagnetic force. Photons do not have electrical charge, they have zero mass and zero rest energy, and they only exist as moving particles. Photons move at 299,792,458 metres per second in a vacuum, the so-called “speed of light” denoted by c (from the Latin celeritas). The speed of photons in a medium depends upon the medium and is always slower than the speed in vacuum c.

Box C.1: Photon

Qubit quantum states encoded either in the polarisation (Box C.2) or in the spatial wave function of photons are the preferred flying qubits, because light transmission through optical fibres and through free space are well-developed technologies that are reliable enough for the transmission of photonic qubits even over long distances.

Polarisation is a property of transverse waves which specifies the geometrical orientation of their oscillations. In a transverse wave, the direction of the oscillation is perpendicular to the direction of motion of the wave (in contrast, in a longitudinal wave, the displacement of the particles in the oscillation is always in the direction of propagation, so these waves do not exhibit polarisation). Transverse waves that exhibit polarisation include electromagnetic waves such as light waves and radio waves. An electromagnetic wave consists of a coupled oscillating electric field and magnetic field which are always perpendicular to each other; by convention, the polarisation of electromagnetic waves refers to the direction of the electric field. In linear polarisation, the fields oscillate in a single direction. In circular or elliptical polarisation, the fields rotate at a constant rate in a plane as the wave travels. The rotation can have two possible directions; if the fields rotate in a right-hand sense with respect to the direction of wave travel, it is called right circular polarisation, while if the fields rotate in a left-hand sense, it is called left circular polarisation. The spin of the photon spin is the quantum-mechanical description of light polarisation, where spin +1 and spin −1 represent two opposite directions of circular polarisation. Light of a defined circular polarisation consists of photons with the same spin.

Box C.2: Polarisation

Using single photons for transmission of encoded quantum states is very attractive because they undergo very little decoherence, even over large distances; they are, however, susceptible to loss and/or dispersion. Optical fibre is intrinsically lossy. Free space is either very low loss (in the atmosphere) or lossless (in free space), but is subject to dispersion. In optical fibres and in the

atmosphere, the photon loss rate increases exponentially with the distance. In vacuum, the photon dispersion rate grows quadratically with the distance.

C.1 Generic QKD protocol

Currently, the best-known application of secure quantum communication is Quantum Key Distribution (QKD). QKD exploits quantum mechanics phenomena to establish a shared secret key between two parties without a (malicious) third party learning anything about that key, even if it can eavesdrop on all communication. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a quantum communication system can be implemented between two parties.

A QKD key exchange protocol (Figure C.1) requires that sender and receiver dispose of a quantum communication channel which allows quantum states to be transmitted; this channel is either an optical fibre or free space. Sender and receiver also need to be able to communicate via a classical communication channel; this channel can range from a dedicated transmission link to the public internet.

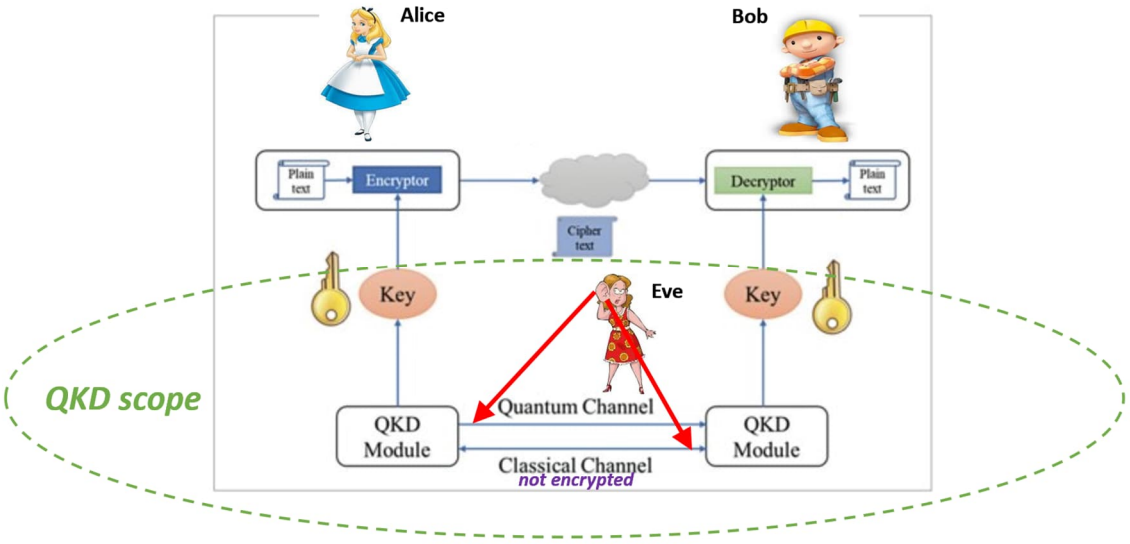

Figure C.1: QKD principle (adapted from Arka Mukherjee 2023)

An important and unique property of QKD is the ability of the two communicating parties to detect the presence of any third party (eavesdropper) trying to gain knowledge of the shared secret key. This results from a fundamental law of quantum mechanics: the process of measuring a quantum system disturbs the quantum system's state. A third party trying to eavesdrop on the key must somehow measure it, thus causing a disturbance that can be detected by the communicating

legitimate parties. Provided that the disturbance caused by eavesdropping remains below a certain threshold, a shared secret key can be produced that is guaranteed to be secure, i.e. the eavesdropper has no information about it. QKD security thus relies on the laws of quantum mechanics and has provable information-theoretic security. In contrast, classical public-key cryptography used for secret key establishment relies on the computational difficulty of certain hard one-way functions, without any mathematical proof whatsoever that these one-way functions cannot be reversed.

QKD protocols are designed under the assumption that eavesdroppers have unlimited computing and storage resources and can interfere in any way with either communication channel. This requires guaranteed authenticity and integrity of messages exchanged over the classical communication channel to prevent man-in-the middle attacks. A small pre-shared key (secured in hardware of a QKD appliance pair), expansion of the pre-shared key based on QKD key exchange results and message authentication based on Wegman-Carter Authentication (WCA, Box C.3) are typically used for this purpose. QKD implementations often use a transactional message authentication scheme where message authentication is performed repeatedly.

Wegman-Carter Authentication (WCA) message authentication, named after the American computer scientists J. Lawrence Carter and Mark N. Wegman, is based on secretly selecting a hash function (using a salt) from a library of Universal Hash Functions (UHFs) and sending its output to a Pseudo-Random Function (PRF), to create a Message Authentication Code (MAC). The WCA scheme is information-theoretically secure (i.e. secure against adversaries with unlimited computing and storage capabilities), provided that the authentication key is uniformly distributed. Universal hashing refers to selecting a hash function at random from a family of hash functions with a certain mathematical property, which guarantees a low number of collisions in expectation, even if the data is chosen by an adversary. Many UHF families are known for hashing integers, vectors and strings; their evaluation is often very efficient.

Box C.3 : Wegman-Carter Authentication (source Wikipedia 2025)

QKD protocols perform a number of functions, which are described in sequential order below, but which would typically be performed in overlap or in parallel in actual QKD implementations. There are many variants of this generic QKD protocol.

Quantum exchange

Upon establishment of the quantum and classical communication channels, a quantum exchange protocol is executed, in which a sequence of photonic qubits is exchanged between sender and receiver through the quantum communication channel.

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. Measuring an unknown quantum state changes that state in some way. This is a consequence of quantum indeterminacy (Box C.4) and can be exploited to detect any eavesdropping on quantum communication (which necessarily involves measurement) and, even more importantly, it can also be exploited to calculate the amount of information that has been intercepted.

Quantum indeterminacy (aka Heisenberg uncertainty principle, named after the German theoretical physicist Werner Karl Heisenberg) is a fundamental principle of quantum mechanics which postulates that there is a lower limit to the precision with which one can measure two independent parameters relating to the same object such as its speed and position or the energy emitted and the duration of emission.

Box C.4 : Quantum indeterminacy

Classical post-processing

The quantum exchange protocol is in fact the only quantum part of a QKD protocol. The remaining parts of a QKD protocol consist of classical post-processing of the measurements obtained by the quantum exchange protocol, in concert with the execution of classical post-processing protocols over the classical communication channel (Figure C.2).

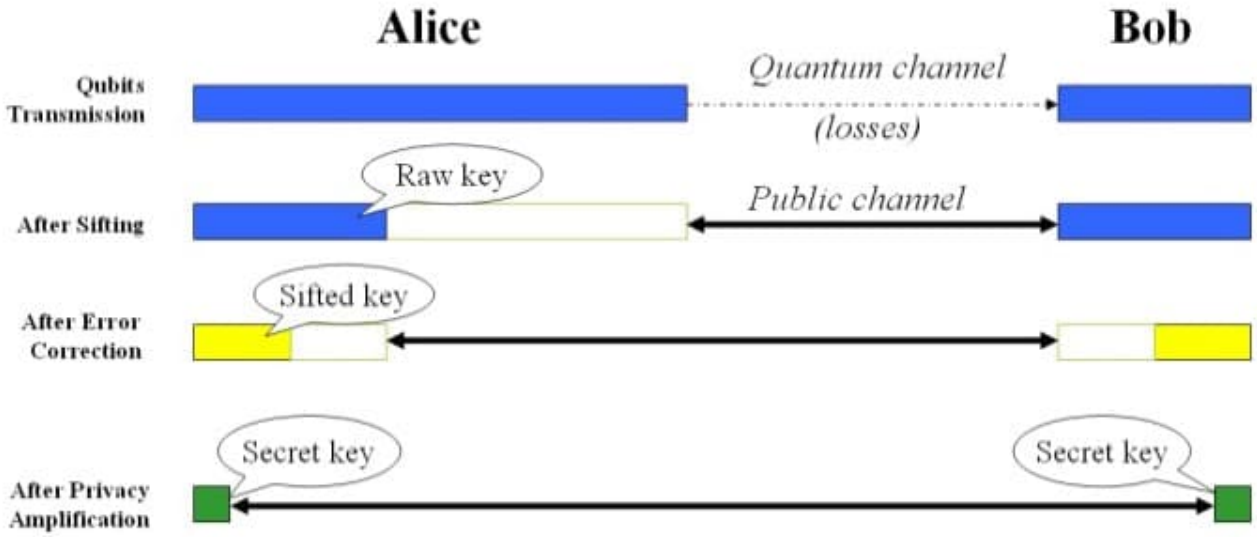

Figure C.2: QKD key determination (source: springer.com 2023)

Raw cryptographic key calculation

First, sender and receiver announce which bases they have used to prepare/measure the qubits exchanged over the quantum channel. The bits corresponding with qubits for which sender and receiver have used different bases are then discarded. The retained bits constitute the so-called raw cryptographic key (aka “sifted key”).

Quantum exchange error rate calculation

Next, an estimate of the quantum exchange error rate is calculated. Typically, a small percentage of the bits of the raw secret key are selected and compared between sender and receiver to calculate this estimate.

Differences between the sender's quantum state preparations/measurements and the receiver's measurements (i.e. quantum exchange errors) may be caused by measurements made by an eavesdropper or by unfavourable environmental conditions (e.g. imperfections in the transmission line and photon detectors or physical disturbances during quantum exchange) that might also cause errors. Because it is impossible to distinguish between these two types of errors (malicious interference and noise), guaranteed QKD security requires the assumption that all errors are due to eavesdropping. If the quantum exchange error rate exceeds a certain predetermined threshold, the established raw cryptographic key must be discarded. Typically, the QKD protocol is then restarted.

Error reconciliation

If the quantum exchange error rate remains below the predetermined threshold, there are typically still errors in the raw cryptographic key that need to be identified, and the affected bits need to be corrected (or discarded). Error reconciliation is performed to correct any such errors and to minimise the amount of information leaked to eavesdroppers on the classical communication channel. This results (with a very high probability) in a perfectly matched and error-free secret key shared between sender and receiver, and also in determination of the Quantum Bit Error Rate (QBER). If the QBER exceeds a certain predetermined threshold, the established secret key must be discarded and the QKD protocol is then typically restarted.

Error reconciliation is done by means of specialised bi-directional correction mechanisms, e.g. the Cascade protocol, Low-Density Parity-Check (LDPC) codes or the Winnow Machine Learning (WML) algorithm. Error reconciliation is highly resource demanding and typically takes the major part of QKD protocol post-processing. It may therefore have considerable impact on the QKD key generation rate, depending on actual implementation choices (LDPC demands larger computational and memory resources than either the Cascade protocol or WML, but it requires less communication resources).

New error reconciliation techniques, for example Tree Parity Machine (TPM), a type of Artificial Neural Network (ANN) inspired by biological neural networks, have been shown to demand less computing and communication resources. This would result in higher key generation rates, which is attractive given the increasing interest in satellite and global QKD connections.

Entropy estimation

If the determined QBER value remains below the predetermined threshold, entropy estimation is performed, to account for the amount of secret key information leaked, i.e. how much information the eavesdropper could have gained about the shared secret key (this is known because of the errors that were introduced by eavesdropping). Key information may have been leaked when executing the quantum exchange protocol over the quantum channel (e.g. by the use of non-ideal optical transmitters that produce insecure multi-photon pulses) or when performing error reconciliation over the classical communication channel. In general, conservative entropy estimations are made though QKD implementations may differ considerably in this respect.

Privacy amplification

The entropy estimation is input for the privacy amplification process. Privacy amplification is a method for reducing (and effectively eliminating) an eavesdropper's partial information about the established shared secret key, which could have been gained both by eavesdropping on the quantum communication channel and on the public communication channel. Privacy amplification transforms the established shared secret key into a new one, in such a way that the eavesdropper has only negligible information about it. This is done by means of universal hashing, i.e. randomly choosing a hash function from a publicly known set. The chosen hash function takes as its input the established shared secret key and outputs a new and shorter shared secret key. The amount by which the key is shortened is determined based on the entropy estimation value. Privacy amplification ensures that the probability of an eavesdropper having any knowledge of the new cryptographic key can be reduced to an arbitrary low value (albeit at the cost of shortening the new shared secret key).

Key comparison

In the last step of the QKD protocol, sender and receiver each calculate a hash of their instance of the (new) shared secret key. If these hashes match, the QKD protocol is considered to have completed successfully. If they do not match, the established (new) secret key must be discarded and the QKD protocol is then typically restarted.

C.2 QKD protocol taxonomy

The American physicist Charles Henry Bennett and the Canadian computer scientist Gilles Brassard embraced the concept proposed by Wiesner in the late 1960s and worked it out as the BB84 QKD protocol (see § C.3). In 1989, they demonstrated the first BB84 based QKD implementation, in which the photon detector produced different audible signals ("clicks"), depending on whether a "0" or "1" bit had been encoded in the photon (it was therefore said to be "fully secure against deaf eavesdroppers"). The term "clicking" is still used in the description of modern photonic equipment, though this equipment no longer produces audible signals.

Many other QKD protocols have been proposed and designed after BB84. There are several different approaches for quantum exchange protocols, but they can be divided into two main categories depending on which quantum mechanics properties they exploit:

1. **Prepare and Measure (P&M) based quantum exchange protocols**

   Prepare and Measure (P&M) quantum exchange protocols are based on the superposition of quantum states of photonic qubits.

2. **Entanglement-based quantum exchange protocols**

   The quantum states of two (or more) separate quantum systems can become linked together in such a way that they must be described by a combined quantum state, not as individual quantum systems. This is known as quantum entanglement and implies that performing a measurement on one quantum system affects the other.

   Quantum teleportation is a communication method that involves transmitting quantum state by exploiting the properties of quantum entanglement. It works by first creating pairs of entangled photons and then sending one photon of each pair to the sender and the other one to the recipient. The sender measures the state of the qubits that hold the quantum information and the state of the entangled photons at the same time. These interactions change the state of its photons, and because they are entangled with the receiver's photons, the interactions instantaneously change the state of the receiver's photons too. In effect, this "teleports" the quantum state of the sender's qubits to the receiver's photons. However, the receiver cannot reconstruct the quantum information until the sender sends the result of its quantum state measurements over the classical communication channel in the form of bits.

   An advantage of entanglement-based quantum exchange protocols is that they can produce shared secret keys which are true random numbers, based on underlying quantum mechanics properties.

The two main approaches for quantum exchange protocols described above can each be further divided into three families of QKD protocols based on the method used for coding:

1. **Discrete Variable QKD (DV-QKD) protocols**

   Discrete Variable (DV) coding uses the polarisation quantum states of single photons.

2. **Distributed Phase Reference QKD (DPR-QKD) protocols**

   Distributed Phase Reference (DPR) coding uses the phase or arrival times of single photons.

3. **Continuous Variable QKD (CV-QKD) protocols**

   Continuous Variable (CV) coding uses the quadrature of the quantised electromagnetic field using coherent states and homodyne or heterodyne detection techniques (Box C.5).

Homodyne detection is a method of extracting information encoded as modulation of the phase and/or frequency of an oscillating signal, by comparing that signal with a standard oscillation that would be identical to the signal if it carried null information. "Homodyne" relates to the use of a single frequency, in contrast to the dual frequencies employed in heterodyne detection.

Box C.5 : Homodyne versus heterodyne detection

CV-QKD technology offers a superior pathway forward in terms of cost and form factor because it can be realised using low-cost off-the-shelf optical components compatible with current telecom fibre technology. Though CV-QKD protocols are attractive for implementation reasons, their security is quite involved. The GG02 CV-QKD protocol (see below) has attracted a lot of interest and various other CV QKD protocols have subsequently been proposed and implemented. Some well-known DV QKD protocols, such as for example B92 (see below) can be transformed to CV-QKD and such variants are also being researched and implemented.

C.3 QKD protocol examples

A few widely implemented used QKD protocols are described below. It should be noted that several other QKD protocols have been proposed and developed, some of which have been implemented in commercially available QKD products. For example, current QKD protocols and QKD implementations are mostly optimised for use with state-of-the-art fibre optic communications technology and often use readily available optical components that implement parts of the QKD technology. There is a growing interest for QKD use cases in satellite networks. QKD systems that must be able to operate over Free-Space Optical (FSO) communication channels need to mitigate several problems that exist in this environment, such as for example atmospheric turbulence. This requires optimisation and even modification of the QKD protocols that are being used and furthermore, their actual implementations need to be tailored to the FSO environment as well.

B92 QKD protocol

The B92 QKD protocol, named after its inventor Charles Bennett and the year of publication (1992), is a modified version of the BB84 QKD protocol. While the BB84 QKD protocol uses four different photon polarisation states, the B92 QKD protocol only uses two. The B92 protocol is easier to implement than the BB84 protocol but is considered less secure. It can also be implemented as a CV QKD protocol where the two different states just differ by phase and homodyne detection is used to measure these states.

BB84 QKD protocol

The BB84 QKD protocol, named after its inventors Charles Bennett and Gilles Brassard, and the year of publication (1984), is a P&M DV-QKD protocol. It was originally described using photon polarisation states to transmit the information. However, any two pairs of conjugate photon quantum states can be used for the protocol. Indeed, many optical fibre-based QKD products that are labelled as BB84 implementations use phase-encoded instead of polarisation-encoded photon quantum states.

BBM92 QKD protocol

The BBM92 QKD protocol, named after its inventors Charles Bennett, Gilles Brassard and Nathaniel David Mermin, and the year of publication (1992), is a simplified version of the E91 QKD protocol. The photon source must still produce EPR-entangled pairs of photons, but the need to perform a Bell inequality test is removed.

E91 QKD protocol

The E91 QKD protocol, named after its inventor Artur Ekert and the year of publication (1991), is an entanglement-based DV-QKD protocol, which uses Einstein-Podolski-Rosen (EPR, see § C.4) entangled pairs of photons. These photon pairs are created by a common source and then distributed so that sender and receiver each end up with one photon from each EPR-entangled pair.

GG02 QKD protocol

The GG02 QKD protocol, named after its inventors Frédéric Grosshans and Philippe Grangier, and the year of introduction (2022), was the first of a series of CV-QKD protocol proposals.

SARG04 QKD protocol

The SARG04 QKD protocol, named after its inventors Valerio Scarani, Antonio Acín, Grégoire Ribordy and Nicolas Gisin, and the year of publication (2004), was derived from the BB84 protocol. It uses different qubit encodings with the objective to provide more robustness when used with multi-photon (faint laser) sources than the BB84 protocol (which was developed for use with single-photon sources). In particular, SARG04 provides more resistance to Photon Number Splitting (PNS) attacks but its QBER is significantly higher than that of BB84 when used over noisy quantum channels.

SSP99 QKD protocol

The Six-State Protocol 1999 (SSP99) QKD protocol, which was proposed by Andrea Pasquinucci and Nicolas Gisin in 1999, is a modified version of the BB84 QKD protocol. While the BB84 QKD protocol uses four different photon polarisation states, the SSP99 QKD protocol uses six and is therefore considered more secure than the original BB84 QKD protocol.

C.4 QKD implementation issues

Implementation of QKD faces several practical challenges. This is predominantly due to limits imposed on the optical transmission distance and on cryptographic key generation rate (which is typically several orders of magnitude lower than the maximum optical transmission rate). In

particular, the propagation of photons through optical fibres or free space is subject to photon loss or dispersion, the extent of which increases with distance. The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) repeaterless bound is a fundamental limit on the quantum capacity of direct quantum communication, i.e. communication without repeaters. For optical fibres, the effective operational distance of QKD products is limited to a few 100 km at the current state of optics technology.

A way to overcome the distance limitation and at the same time achieve much higher key generation rates consists of employing an intermediate node in the quantum channel connecting the parties, which also implements a limited form of device-independent quantum cryptography (see below). Examples of this approach are Measurement Device Independent QKD (MDI-QKD) and Twin-Field QKD (TF-QKD).

In MDI-QKD (Figure C.3), neither endpoint (sender or receiver) is configured as an optical receiver (as is done in conventional QKD protocols), but rather both endpoints are configured as optical transmitters. The two optical transmitters send photons to an intermediate node, called mid-station, which couples and measures the photons. The endpoints can distil a shared secret key from the two-photon interference measurement results disclosed by the mid-station. The MDI-QKD protocol is protected against a malicious attempt by someone compromising the mid-station to gain information about the secret key because the legitimate endpoints can always detect any attempt to alter the correct operation of the ("untrusted") mid-station, as this would manifest as a form of regular eavesdropping.

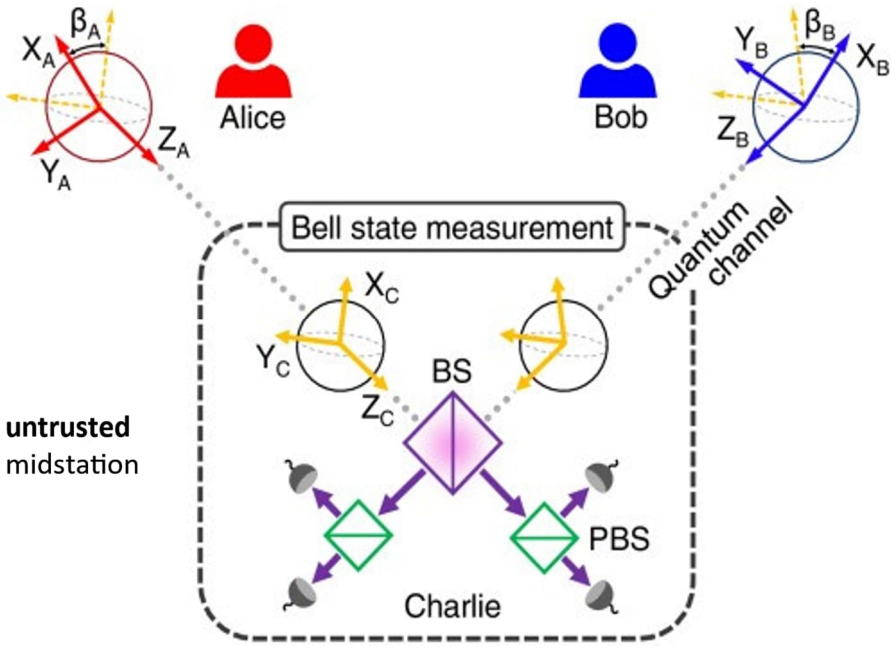

Figure C.3 MDI-QKD principle (source: ResearchGate 2022)

With MDI-QKD it is no longer necessary to take special measures to protect optical receivers of endpoints from outside attacks. The focus shifts to protecting the optical transmitters of

endpoints (where the optical pulses are prepared locally by a trusted user), which is much easier than protecting the optical receivers of endpoints (where optical pulses are received from the outside, prepared by someone who is potentially untrusted and possibly interested in breaking the security of the system).

The advantage of TF-QKD, compared to MDI-QKD, is that it is designed to generate key bits from single-photon interference in the intermediate node, thus removing the need to remedy photon losses via sophisticated techniques.

Chinese scientists have recently successfully implemented Mode-Pairing QKD (MP-QKD). MP-QKD does not require the technically challenging "phase locking" step. It is claimed to achieve an improvement in QKD key-rate of three orders of magnitude on longer distances (300 to 400 km) compared to MDI-QKD. Furthermore, MP-QKD can be implemented using readily available optical fibre technology.

QKD protocol implementations must ensure that the quantum mechanics properties on which their information-theoretic security relies are not compromised in any way by the implementation of the QKD devices; this is often easier said than done.

Quantum cryptographic protocols are device-independent if their security does not rely on trusting that the quantum devices used to implement the protocol are truthful (the security analysis of these protocols includes scenarios of imperfect or even malicious devices).

Device-independence is based on "self-testing" quantum devices, the internal operations of which can be uniquely determined by their input-output statistics. Bell inequality tests (Box C.6) are typically used for checking the “honesty” of the quantum devices. Several unconditionally secure device-independent QKD protocols have been proposed, even taking into account that the actual devices performing the Bell inequality tests may not be ideal (i.e. “noisy”).

Bell's theorem is used to prove that quantum mechanics is incompatible with “local hidden-variable” theories. It was introduced by the British physicist John Stewart Bell in a 1964 in response to the EPR paradox. The EPR paradox refers to a thought experiment that the Swiss-American physicist Albert Einstein, the Russian-American physicist Yakovlevitch Boris Podolsky and the Israeli-American physicist Nathan Rosen formulated in 1935, in order to argue that quantum mechanics was an incomplete theory. In their view (shared by many other leading physicists at the time), quantum particles carry physical attributes (later called “local hidden-variables”) not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes.

Bell carried out an analysis of quantum entanglement and deduced that if measurements are performed independently on the two separated halves of a pair of entangled particles, then the assumption that the outcomes depend upon “local hidden-variables” within each half implies a constraint on how the outcomes on the two halves are correlated. This constraint would later be named the “Bell inequality”. Quantum mechanics predicts correlations that violate this inequality and multiple variations on Bell's theorem have been tested experimentally in physics laboratories many times. All these “Bell tests have found that the hypothesis of “local hidden-variables” is inconsistent with the way that quantum entanglement works.

While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Box C.6 : Bell's theorem

Absolute protection against attackers that have unlimited computing and storage resources, as claimed by QKD proponents, requires that the actual data must be protected by an absolutely secure encryption scheme, i.e. OTP (Box C.7). Given the very low keyrates that are realistically achievable with QKD, this excludes fully secure exchange of data by means of QKD for most practical applications. They will need to protect their data by means of symmetric cryptographic schemes without absolute security (such as for example AES).

The One-Time Pad (OTP) is the only encryption scheme which has been proven unconditionally secure. This symmetric-key encryption scheme, which was first invented at AT&T by Gilbert Sandford Vernam (Vernam cipher) and amended (adding randomness) by US Army Chief Signal Officer Joseph O. Mauborgne, requires a key that is as long as the message to be encrypted and which can be used only once. A different key is needed for each message to be encrypted, i.e. for every plaintext, there is a key that produces that plaintext from a given ciphertext.

Box C.7 : One-Time Pad (OTP)

A problem with QKD's claim that any attempt at eavesdropping is detected, is that such attempts (or more generally, any interference with the quantum channel) will in practice lead to Denial-of-Service (DoS).

C.5 Quantum key distribution networks

Limits are imposed on the range of optical transmission over point-to-point optical links because the propagation of photons through optical fibres or free space is subject to photon loss or dispersion, the extent of which increases with distance. For optical fibres, the effective operational distance of QKD products is limited to a few 100 km at the current state of optics technology.

The QKD distance limitation can be overcome by deploying an intermediate node between the communicating parties. Examples of this approach are optical switch technology or "untrusted" QKD intermediate station technology (either MDI-QKD, TF-QKD or MP-QKD; see § C.4), or a combination of these technologies. This approach is suitable for the implementation of Quantum Metropolitan Area Networks (QMANs) of limited geographical size.

A fully scalable QKD network architecture, which includes specialised "trusted" QKD relays to connect cascaded point-to-point QKD systems, extends the practical range of this technology and allows for secure key exchange over much longer distances in Quantum Wide Area Networks (QWANs). QKD trusted relay technology is expected to form the basis of global Quantum Key Distribution Networks (QKDNs, Figure C.4), including both fibre-based and free FSO-based QKD links. ITU-T is currently developing a series of Recommendations for QKDNs.

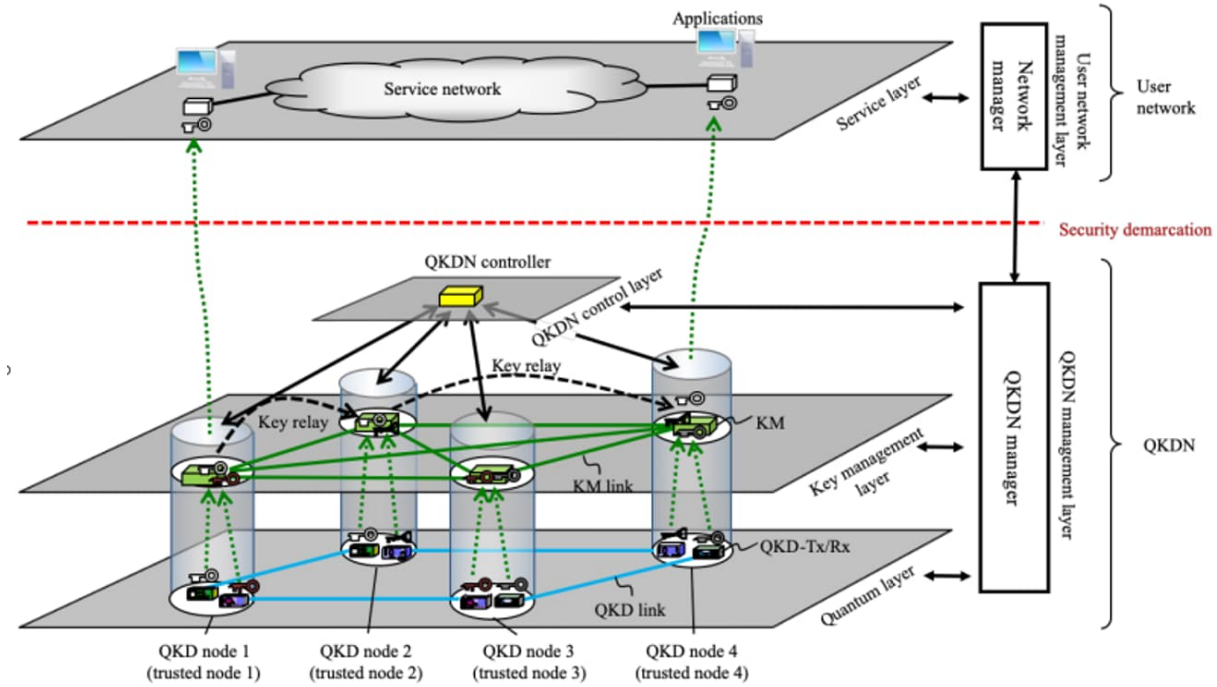

Figure C.4: QKDN network architecture (source: ITU-T 2020)

Trusted QKD relays are based on a simple concept: each relay executes the QKD protocol to securely exchange secret keys with its neighbouring relay(s), thus extending the key exchange capability over distances that are much larger than a single execution of the point-to-point QKD protocol could ever cope with (this is similar to the use of optical repeaters in classical optical fibre networks). To ensure the security of the secret keys that are exchanged in this manner, the QKD relays must be trusted devices (aka “trusted repeaters”), which are protected against intrusion and attacks by unauthorised parties. It goes without saying that this requirement precludes many use cases.

“Untrusted” quantum repeaters based on quantum entanglement are being actively researched. The use of such quantum repeaters would remove the requirement to trust intermediate nodes (such as the trusted QKD relays of QKDN) and would at the same time drastically simplify the architecture of QKD networks. Such networks are still a long way off.

Appendix D – References

[ANSSI 2022] ANSSI views on the Post-Quantum Cryptography transition

[ETSI 2020] TR 103 619 - Migration strategies and recommendations to Quantum Safe schemes

[evolutionQ/GRI 2024] Quantum Threat Timeline Report 2024

[Ezratty 2024] Understanding Quantum Technologies Seventh Edition

[IETF 2005] RFC 4279 - Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)

[IETF 2009] RFC 5487 - Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode

[IETF 2020] RFC 8784 - Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

[IETF 2024] Hybrid key exchange in TLS 1.3 draft

[ITU-T 2020] Security framework for quantum key distribution networks

[Gartner 2022] Preparing for the Quantum World With Crypto-Agility

[GRI/evolutionQ 2024] Quantum Threat Timeline Report 2024

[Michiels 2025] Introduction to cryptography Version 9.3

[NCSC 2022] Guidelines for quantum-safe transport-layer encryption

[NIST 2021] Getting Ready for Post-Quantum Cryptography

[NIST 2025] Considerations for Achieving Crypto Agility initial public draft

[NOREA 2024] Quantum Annealing Explained

[NOREA 2025] Quantum Algorithms

[NOREA 2025] Quantum Computing Explained

[TNO/CWI 2019] Towards Quantum-Safe VPNs and Internet

[TNO/CWI/AIVD 2024] The PQC Migration Handbook

[WEF 2022] Transitioning to a Quantum Secure Economy

[Wikipedia 2025]

NIST PQC Project website

Appendix E - Acronyms and abbreviations

ac	academia
AES	Advanced Encryption Standard
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
aka	also known as
ANN	Artificial Neural Network
ANSSI	Agence nationale de la sécurité des systèmes d'information
AT&T	American Telephone and Telegraph
B92	Bennett 1992
BB84	Bennett and Brassard 1984
BBM92	Bennett, Brassard and Mermin 1992
BDD	Bounded-Distance-Decoding
BHT	Brassard, Høyer and Tapp
BIKE	Bit Flipping Key Encapsulation
bit	binary digit
BKZ	Block-Korkine-Zolotarev
BLISS	Bimodal Lattice Signature Scheme
blog	web log
BS	Beam Splitter
c	celeritas
CBC	Cipher Block Chaining
CCA	Chosen Ciphertext Attack
CFS	Courtois, Finiasz and Sendrier
com	commercial
CROSS	Codes and Restricted Objects Signature Scheme
CRQC	Cryptographically Relevant Quantum Computer
CRYSTALS	Cryptographic Suite for Algebraic Lattices
cs	computer science
CSIDH	Commutative Supersingular-Isogeny Diffie-Hellman
CV	Continuous Variable
CV-QKD	Continuous Variable Quantum Key Distribution
CVP	Closest Vector Problem

CWI	Centrum Wiskunde & Informatica
DES	Data Encryption Standard
DH	Diffie-Hellman
dHSP	dehedral Hidden Subgroup Problem
dlog	discrete logarithm
DLP	Discrete Logarithm Problem
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DPR	Distributed Phase Reference
DPR-QKD	Distributed Phase Reference Quantum Key Distribution
DV	Discrete Variable
DVR	Discrete Variable Quantum Key Distribution
e.g.	exempli gratia
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
EDCP	Extrapolated Dihedral Coset Problem
EDP	Electronic Data Processing
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
EPR	Einstein-Podolsky-Rosen
etc.	et cetera
ETSI	European Telecommunications Standards Institute
FALCON	F*a*st-*F*ourier Lattice-based C*o*mpact *S*ignatures over NTRU
FFT	Fast Fourier Transform
FN-DSA	FFT over NTRU-*L*attice-*B*ased Digital Signature Algorithm
FS	Fiat-Shamir
FSO	Free-Space Optical
FTQC	Fault-Tolerant Quantum Computer
FTS	Few-Time Signatures
GeMSS	Great Multivariate Short Signature
GG02	Grosshans and Grangier 2002

GGH	Goldreich–Goldwasser–Halevi
GNFS	General Number Field Sieve
GPS	Global Positioning System
GRI	Global Risk Institute
HAWK	*a pun on "FALCON"*
HHL	Harrow, Hassidim and Lloyd
HMAC	Hash-based Message Authentication Code
HQC	Hamming Quasi-Cyclic
	High-performance Quantum Computing
HRSS	Hülsing - Rijneveld - Schanck - Schwabe
HSS	Hierarchical Signature System
i.e.	id est
IBM	International Business Machines
ICM	Index-Calculate Method
ICT	Information and Communication Technology
IDF	Israel Defense Forces
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFP	Integer Factorization Problem
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPsec	IP security
ITU-T	International Telecommunication Union - Telecommunication *S*tandardization *S*ector
KDF	Key Derivation Function
KEM	Key-Encapsulation Mechanism
KM	Key Management
KU	Katholieke Universiteit
LDPC	Low-Density Parity-Check
LESS	Linear Equivalence Signature Scheme
LLL	Lenstra–Lenstra–Lovász
LMS	Leighton-Micali Scheme

LWE	Learning With Errors
LWR	Learning With Rounding
MAC	Message Authentication Code
MAYO	*a pun on "Oil and Vinegar"*
MD5	Message Digest 5
MDI-QKD	Measurement Device-Independent Quantum Key Distribution
MDPC	Moderate Density Parity-Check
MIRA	MInRAnk
MiRitH	M*i*nR*A*nk-in-the-Head
ML-DSA	Module-Lattice-*B*ased Digital Signature Algorithm
ML-KEM	Module-Lattice-*B*ased Key-Encapsulation Mechanism
MP-QKD	Mode-Pairing QKD
MPC	Multi-Party Computation
MPCitH	MPC-in-the-Head
MQ	Multivariate Quadratic
MQOM	MQ-*o*n-my-Mind
MSS	Merkle Signature Scheme
NCCoE	National Cybersecurity Center of Excellence
NCSC	Nationaal Cyber Security Centrum
NISQ	Noisy Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
nonce	number used only once
NOREA	Nederlandse Orde van Register EDP-Auditors
NOVA	Noncommutative Oil and Vinegar with Alignment
NTRU	N-th Degree Truncated *P*olynomial Ring Units
nz	*N*ew-*Z*ealand
OQS	Open Quantum Safe
OTP	One-Time Pad
OTS	One-Time Signature
P&M	Prepare & Measure
PBS	Polarizing Beam Splitter
PC	Personal Computer

PERK	PERmuted Kernel
PKI	Public Key Infrastructure
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PNS	Photon Number Splitting
poset	partially ordered set
PQC	Post-Quantum Cryptography
PRF	Pseudo-Random Function
PSK	Pre-Shared Key
QA	Quantum Annealer Quantum Annealing
QBER	Quantum Bit Error Rate
QC-MDPC	Quasi-Cyclic Moderate Density Parity-Check
QED-C	Quantum Economic Development Consortium
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QMAN	Quantum Metropolitan Area Network
QR-UOV	Quotient Ring UOV
QRC	Quantum-Resistant Cryptography
qubit	quantum bit
QWAN	Quantum Wide Area Network
RFC	Request *f*or Comments
RSA	Rivest-Shamir-Adleman
RSA-2048	2048-bit RSA
Rx	Receive
SARG04	Scarani, Acin, Ribordy and Gisin 2004
SCA	Side-Channel Attack
SDitH	Syndrome Decoding-in-the-Head
SHA	Secure Hash Algorithm
SHA-2	Secure Hash Algorithm 2
SHA-3	Secure Hash Algorithm 3
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solution

SLH-DSA	State*l*ess Hash-*B*ased Digital Signature Algorithm
SNOVA	Simple NOVA
SP	Special Publication
SPHINX+	Stateless Practical Hash-based Incredibly Nice *C*ryptographic *S*ignatures plus
SQIsign	Short Quaternion and Isogeny signature
SSH	Secure SHell
SSP99	Six-State Protocol 1999
SVP	Shortest Vector Problem
TB	TeraByte
TDES	Triple DES
TF-QKD	Twin-Field Quantum Key Distribution
TLS	Transport Layer Security
TLS1.3	TLS version 1.3
TNO	*N*ederlandse *O*rganisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TPM	Tree Party Machine
TR	Technical Report
TSP	Trust Service Provider
TU/e	Technische Universiteit *E*indhoven
TV	Tele*vi*sion
Tx	Transmit
UHF	Universal Hash Function
UOV	Unbalanced Oil and Vinegar
US	United States
VMI	Virtual Machine Image
VOLE	Vector Oblivious Linear Evaluation
VOLEitH	VOLE-in-the-Head
VPN	Virtual Private Network
WCA	Wegman-Carter Authentication
WEF	World Economic Forum
WML	Winnow Machine Learning

WOTS	Winternitz One-Time Signature
XMSS	eXtended Merkle Signature Scheme
XMSSMT	Multi-*t*ree eXtended Merkle Signature Scheme
y	year
ZKP	Zero-Knowledge Proof