Quantum-Resistant Cryptography

Table of contents

1. Introduction

Current Quantum-Resistant Cryptography (QRC) solutions mostly focus on several different approaches, including code-based cryptography, lattice-based cryptography, multivariate-based cryptography, isogeny-based cryptography and hash-based cryptography. These QRC approaches are briefly described below.

But first a look at a radically different QRC approach called the Picnic digital signature scheme. Picnic has been selected as an alternate candidate for the third round of the US National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) competition (see Chapter 2) 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. Unlike most other public-key cryptography, Picnic is not based on hard problems from number theory. Instead, it is based on a proving algorithm that simulates a Multi-Party Computation (MPC, see Box 1.1) protocol. By revealing the views of a random subset of MPC parties, an interactive Zero-Knowledge Proof (ZKP, see Box 1.2) is formed, where one party can convince another party that it knows a secret without disclosing the secret itself. This ZKP is transformed into a signature scheme by using a Fiat-Shamir (FS) heuristic (Box 1.3), a well-known technique for taking an interactive ZKP and creating a digital signature based on it. The Picnic ZKP concept was combined with symmetric cryptography, hash functions and block ciphers, to create a novel digital signature scheme. The hard problems that Picnic relies on therefore relate only to hash functions and block ciphers, which are thought to be secure against quantum computer attacks.

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.

Box 1.1: Multi-Party Computation (MPC)

A Zero-Knowledge Proof (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.

Box 1.2: Zero-Knowledge Proof (ZKP)

Most Zero-Knowledge Proof (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 heuristic (sometimes referred to as the Fiat-Shamir transformation). The idea behind the Fiat-Shamir 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 1.3: Fiat-Shamir (FS) heuristic

1.1. 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, see Box 1.4) developed by Robert McEliece, the Niederreiter encryption algorithm (based on Reed-Solomon codes, see Box 1.5) developed by Harald Niederreiter, and the related CFS digital signature scheme developed by Nicolas 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 1.4: 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 1.5: Reed-Solomon code

Other examples of code-based cryptography are Hamming Quasi-Cycle (HQC), which is based on Hamming codes (Box 1.6) 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, see Box 1.7) 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 1.6: Hamming code

Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) codes are variants of Moderate Density Parity-Check (MDPC) codes. 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.

Box 1.7: Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) code

Classical McEliece (a variant of the McEliece algorithm) was selected as a finalist, and BIKE and HQC were selected as alternate candidates for the third round of the NIST PQC competition and they will all advance to the fourth round.

1.2. Lattice-based cryptography

Lattice-based cryptography algorithms is based on hard problems in the lattice (Box 1.8) 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 1.8: Lattice

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 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, which were selected by NIST for standardisation after the third round of the PQC competition, are based on the Cryptographic Suite for Algebraic Lattices (CRYSTALS) algorithm.

The Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) digital signature scheme was also selected by NIST for standardisation after the third round of the PQC competition. The main advantage of FALCON is that its signatures are smaller than those of CRYSTALS-Dilithium.

1.3. Multivariate-based cryptography

Multivariate-based cryptography is based on the difficulty of solving systems of multivariate equations (Box 1.9).

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 1.9: Multivariate equation

Attempts to develop secure multivariate-based based encryption schemes have failed until now. However, multivariate digital signature schemes like UOV (Unbalanced Oil and Vinegar), Rainbow (a variation of UOV), HFEv- (Hidden Field Equations vinegar minus) and GeMSS (Great Multivariate Short Signature) are deemed suitable as QRC digital signature schemes.

GeMSS was selected as an alternate candidate for the third round of the NIST PQC competition.

Rainbow was also selected as a NIST PQC third round finalist but it was successfully attacked later on, using only a laptop computer for a couple of days.

Neither GEMSS nor Rainbow will be standardised by NIST.

1.4. Isogeny-based cryptography

Isogeny-based cryptographic schemes are based on the mathematics of isogenies of supersingular elliptic curves (a specific subclass of elliptic curves, see Box 1.10) 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 1.10: 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, see Box 1.11). SIKE was developed by researchers from Amazon, Microsoft, Texas Instruments, the University of Waterloo, Université de Versailles and Radboud University. It has been selected as an alternate candidate for the third round of the NIST PQC competition and was selected to advance to the fourth round, but it was subsequently successfully attacked and has therefore been withdrawn.

A Chosen-Ciphertext Attack (CCA) is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

Box 1.11: Chosen Ciphertext Attack (CCA)

1.5. Hash-based cryptography

All practical digital signature schemes use cryptographic hash functions (Box 1.12) 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.

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 1.12: Cryptographic hash function

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 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. The stateless SPHINCS+ signature scheme augments XMSSMT with three major changes:

- 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.

- 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.

- 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.

SPHINCS+ was selected by NIST for standardisation after the third round of the PQC competition. 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.

2. NIST Post-Quantum Cryptography (PQC) competition

The goal of the NIST PQC competition is to promote replacements for public-key cryptographic primitives, which are widely used in practice, but are vulnerable to attacks performed with quantum computers, i.e. to develop quantum-resistant cryptographic primitives that provide authenticity and quantum-resistant cryptographic primitives that provide secrecy.

Authenticity cryptographic primitives

Primitives that provide authenticity relate to digital signature schemes, which consist of:

- a key generation algorithm to generate private/public key pairs;
- 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.

Secrecy cryptographic primitives

Primitives that provide secrecy relate to either key exchange, public key encryption or key encapsulation schemes.

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

A **public key encryption scheme** consists of:

- a key generation algorithm to generate private/public key pairs;
- an encryption algorithm to generate a ciphertext from a message and the public key;
- a decryption algorithm to generate the plaintext (message) signature with the private key.

A **key encapsulation scheme** consists of:

- a key generation algorithm to generate private/public key pairs;
- an encapsulation algorithm to generate a session key and a ciphertext with the public key;
- a decapsulation algorithm to generate a session key from the ciphertext with the public key.

NIST decided to only standardise Key Encapsulation Mechanisms (KEMs) because it is possible to construct both key exchange and public-key encryption primitives with KEMs.

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 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, after careful consideration during the third round of the NIST PQC standardisation process, NIST has identified four candidate PQC schemes for standardisation. NIST will recommend two primary algorithms to be implemented for most use cases: CRYSTALS-Kyber (KEM scheme) and CRYSTALS-Dilithium (digital signature scheme). In addition, the digital signature schemes FALCON and SPHINCS+ will also be standardised.

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.

FALCON will be standardised by NIST since there may be use cases for which CRYSTALS-Dilithium digital signatures are too large.

SPHINCS+ will be standardised to avoid relying only on the security of structured lattices for digital signature schemes. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

In August 2023, NIST released draft FIPS standards for three PQC algorithms:

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

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

3. FIPS 205 - Stateless Hash-Based Digital Signature Standard: Stateless Hash-Based Digital Signature Algorithm (SHB-DSA); based upon SPHINCS+.

It is expected that these FIPS standards will be formally approved in 2024.

The draft FIPS standard for FALCON is expected to be released in 2024.

The following candidate KEM schemes will advance to the fourth round: BIKE, Classic McEliece and HQC.

Both BIKE and HQC use code-based cryptography, and either would be suitable as a general-purpose KEM that is not based on structured lattices. NIST expects to select at most one of these two candidates for standardisation at the conclusion of the fourth round.

Classic McEliece was a finalist but is not being standardised by NIST at this time. Although Classic McEliece is widely regarded as secure, NIST does not anticipate it being widely used due to its large public key size. NIST may however still choose to standardise Classic McEliece at the end of the fourth round.

For the KEM schemes moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). NIST will review the proposed modifications and publish the accepted submissions. As a general guideline, NIST expects any modifications to be relatively minor.

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 (according to the NIST PQC website):

- code-based cryptography (see § 1.1): 5 signature schemes;
- structured lattice-based cryptography (see § 1.2): 7 signature schemes;
- multivariate-based cryptography (see § 1.3): 11 signature schemes;
- isogeny-based cryptography (see § 1.4): 1 signature scheme;
- MPC-in-the-Head-based cryptography (a new category which would also include the Picnic PQC signature scheme selected as an alternate candidate for the third round of the 2016 NIST PQC competition, see Chapter 1 for details): 7 signature schemes;
- other: 9 signature schemes.

NIST will initiate a new process for evaluation of these 40 candidate signature schemes, which is expected to be much smaller in scope than the 2016 PQC process. Nevertheless, the submitted signature scheme candidates will need to be thoroughly analysed, which will likely take several years.

The first phase of the NIST PQC standardisation process (publication of FIPS standards for the first set of four PQC schemes) will probably be completed in 2024. It is however expected that many vendors and open-source development groups will start implementation of PQC schemes before the standardisation by NIST will be completed. It is also expected that standards bodies such as for example the IETF will start working on modifications and extensions of existing cryptographic security protocol standards that are required in order to support the new PQC cryptographic schemes.

After standardisation of the first set of four 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 Cryptographically Relevant Quantum Computers (CRQCs, see Box 2.1) 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.

The term Cryptographically Relevant Quantum Computer (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.

Box 2.1: Cryptographically Relevant Quantum Computer (CRQC)

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 used public-key cryptographic schemes. Further analysis and research may uncover that these PQC schemes are not secure enough for replacement of the currently deployed public-key cryptographic schemes. For example:

- A new 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 new classical attack on the SIKE elliptic curve isogeny-based PQC scheme was discovered by 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.

- 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 (see above), 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 recently solved the Shortest Vector Problem (SVP) 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, see Box 2.2) 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. Some types of side-channel attacks require physical access to the cryptographic system or its communication facilities, while others do not. 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. 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 2.2: Side-Channel Attack (SCA)

Appendix A - References

NIST PQC Project

Open Quantum Safe (OQS) project

Tanja Lange's TU/e post-quantum cryptography course

[Bernstein et al 2021] Risks of lattice KEMs

[ENISA 2021] Post-Quantum Cryptography – Current state and quantum mitigation

[ETSI 2015] Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges

[IEEE 2008] 1363.1 – IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices

[NOREA 2024] Quantum Computing and Cryptography

Appendix B - Acronyms and abbreviations

AES	Advanced Encryption Standard
BIKE	B*i*t *F*lipping Key Encapsulation
BKZ	Block-Korkine-Zolotarev
BLISS	Bimodal Lattice Signature Scheme
CCA	Chosen Ciphertext Attack
CFS	Courtois, Finiasz and Sendrier
CRQC	Cryptographically Relevant Quantum Computer
CRYSTALS	C*ry*ptographic Sui*t*e for Algebraic Lattice*s*
CSIDH	Commutative Supersingular-Isogeny Diffie-Hellman
CVP	Closest Vector Problem
CWI	Centrum Wiskunde & Informatica
DH	Diffie-Hellman
e.g.	exempli gratia
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
etc.	et cetera
ETSI	European Telecommunications Standards Institute
FALCON	Fast-*F*ourier Lattice-based Compact *Si*gnatures *o*ver NTRU
FIPS	Federal Information Processing Standards
FS	Fiat-Shamir
FTS	Few-Time Signatures
GeMSS	Great Multivariate Short Signature

GGH	Goldreich–Goldwasser–Halevi
GPS	Global Positioning System
HFEv-	Hidden Field Equations vinegar minus
HQC	Hamming Quasi-Cyclic
i.e.	id est
IBM	International Business Machines
IDF	Israel Defense Forces
IEEE	Institute of Electrical and Electronics Engineers
IFP	Integer Factorisation Problem
INRIA	Institut *n*ational de *r*echerche en sciences et technologies du numérique
KEM	Key Encapsulation Mechanism
KU	Katholieke Universiteit
LLL	Lenstra–Lenstra–Lovász
LWE	Learning With Errors
LWR	Learning With Rounding
MDPC	Moderate Density Parity-Check
ML-DSA	Module-Lattice-*B*ased Digital Signature Algorithm
ML-KEM	Module-Lattice-*B*ased Key-Encapsulation Mechanism Standard
MPC	Multi-Party Computation
MSS	Merkle Signature Scheme
NIST	National Institute of Standards and Technology
NTRU	N-th Degree Truncated Polynomial Ring Units
OQS	Open Quantum Safe
OTS	One-Time Signature
poset	partially ordered set
PQC	Post-Quantum Cryptography

QC-MDPC	Quasi-Cyclic MDPC
QRC	Quantum-Resistant Cryptography
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SCA	Side-Channel Attack
SHA	Secure Hash Algorithm
SHB-DSA	Stateless Hash-Based Digital Signature Algorithm
SIDH	Supersingular Isogeny Diffie-Hellman
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solution
SP	Special Publication
SPHINCS+	Stateless Practical Hash-based Incredibly Nice Cryptographic Signatures plus
SVP	Shortest Vector Problem
TU/e	Technische Universiteit Eindhoven
TV	Television
UOV	Unbalanced Oil and Vinegar
US	United States
WOTS	Winternitz One-Time Signature
XMSS	eXtended Merkle Signature Scheme
XMSSMT	Multi-tree XMSS
ZKP	Zero-Knowledge Proof