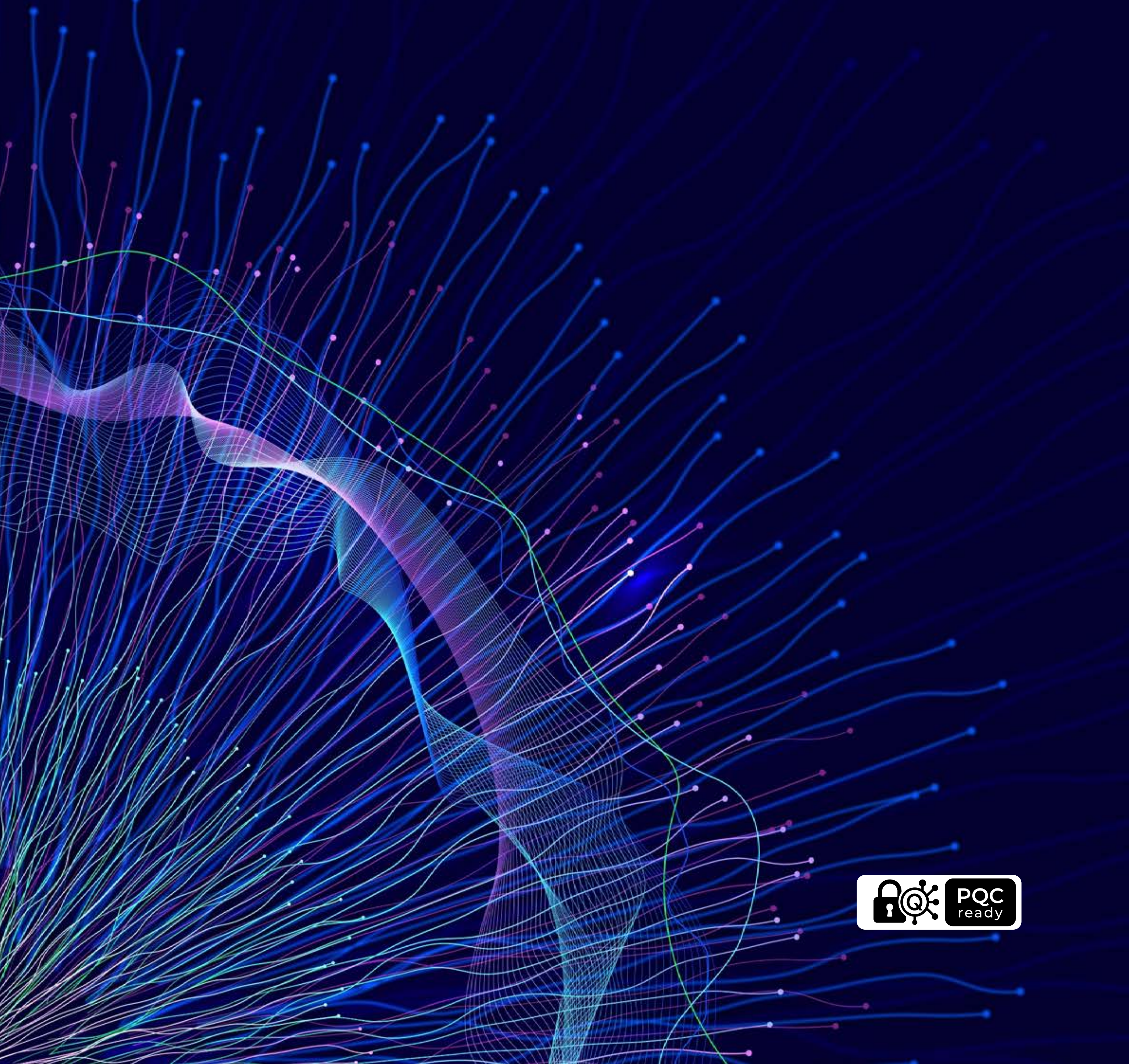
EVIDEN

An Introduction to Post-Quantum Cryptography



PQC ready

Preface: The post-quantum age is dawning

The quantum apocalypse is approaching. We therefore need to urgently look for quantum-safe alternatives to some of the current crypto methods.

Imagine that a hacker could access millions of online bank accounts and make transfers at will. Assume that the same hacker can read all encrypted emails that fall into his hands. And, in addition, imagine that this criminal person would be able to penetrate almost any corporate network to spy on it.

An unrealistic scenario? Not at all, because that's exactly how it could turn out if one day there are powerful quantum computers. Because these devices can be used to crack the RSA, Elliptic-Curve Cryptography (ECC) and Diffie-Hellman methods—three crypto methods that are used billions of times in web-browsers, email clients, wired and wireless networks, business applications, smartphones and ATMs. The digital apocalypse would become reality.

Fortunately, we're not there yet. Although quantum computers already exist, they can so far only decompose smaller numbers into their factors. To threaten RSA, ECC or Diffie-Hellman, they would have to manage a similar operation with a 700-digit number. They won't be able to do that today or tomorrow.

But numerous experts are currently conducting intensive research on quantum computers and ensuring constant improvements—so the apocalypse is drawing closer. We must therefore look in good time for alternatives to RSA, ECC, and Diffie-Hellman that can be used in our existing systems and are not vulnerable to quantum computers. Such methods do exist, and they are grouped under the term "Post-Quantum Cryptography."

Since our last version of this whitepaper, many of those Post-Quantum Cryptography methods have been standardized and researchers have tested them in different conditions, providing good news about their efficiency, as long as enough memory and computation power is available. While most Post-Quantum Cryptography methods are still too little researched to be used without hesitation, progress is being made here as well, and several post-quantum algorithms have now emerged with which we can venture into the post-quantum age.

In addition, high level protocols (SSH, S/MIME, IKE.IPSEC, OpenPGP, X.509, etc.) and standards (EUCC, PCI DSS, GCB, ...) are being adapted. Cyber agencies have set tentative timelines for PQC adoption, though their dates could be subject to change (longer or shorter), and the pace of real-world implementation might vary significantly by region and sector. One thing is sure though, it is not too early to start preparing for this transition. Many companies have started this process in the meantime.

In any case, we will have to migrate to Post-Quantum Cryptography in the coming years. Indeed, Cybersecurity agencies across the world (EU Member States[1], UK NCSC[2], US NIST[3], AU ASD[4]...) have provided either depreciation dates for RSA, ECC and Diffie-Hellman or target dates for migration to Post-Quantum Cryptography, all of them with severe consequences—regulatory and in terms of business operations disruption—for those who won't be ready in time. This will be far from easy. The various methods are diverse and not all world regions have made the same choices. If most of the proposed target dates are met, they will still be extremely ambitious—nearly half the minimum lead time observed in previous, much simpler migrations. Moreover, implementing Post-Quantum Cryptography will bring numerous additional challenges. There is clearly a great deal of work ahead.

This whitepaper is intended to help a wider audience understand Post-Quantum Cryptography. Deeper mathematical knowledge is not necessary to read it.

Eviden hopes you enjoy reading it!

[1] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
[2] https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
[3] https://csrc.nist.gov/pubs/ir/8547/ipd
[4] https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography

Table of contents

Chapter 1 - Introduction

Chapter 2 - Quantum computers

Chapter 3 – Post-Quantum Cryptography

Chapter 4 – What's next?

Chapter 1 – Introduction

How is encryption used today?

The legendary Enigma looked like a typewriter. The encryption device converted the typed letters into a jumbled mess of characters that could only be unraveled with an identical machine and a correctly set combination of numbers (key). The Germans used the Enigma, of which almost 40,000 were produced, to encrypt their Morse code during World War II.

Today, Morse code has been replaced by emails and Internet connections. These also have to be encrypted. This is done using methods such as the Advanced Encryption Standard (AES), which, like the Enigma, processes a key without which it is impossible to unravel the encryption code.

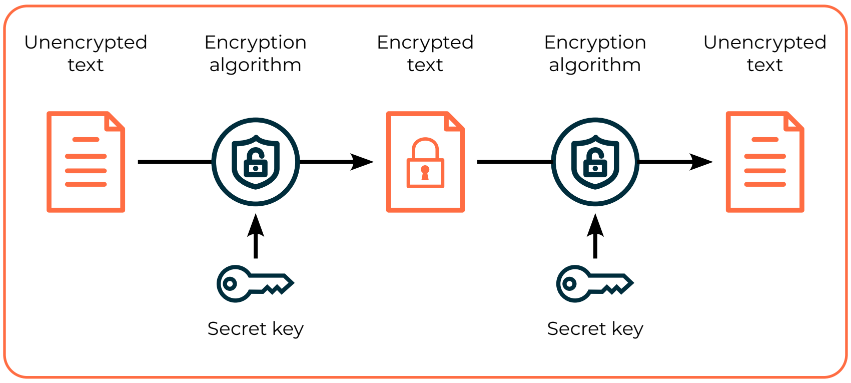


Figure 1: Symmetric encryption uses the same key for encryption and decryption. The sender and receiver must agree on this key in advance.

The AES and the Enigma are examples of symmetric encryption. They each use the same key for encryption and decryption. The sender and receiver must agree on this key in advance.

What is asymmetric cryptography?

The fact that sender and receiver have to know the same key repeatedly causes logistical problems and security gaps—this is referred to as the "key exchange problem". In World War II, for example, submarines had to take key books with them on their voyages so that the radio operator knew the Enigma keys needed for each day. Of course, such books sometimes fell into the hands of the enemy, allowing them to decrypt without authorization. On the worldwide Internet, it can already be a challenge to agree on a key with each communication partner individually.

In the 1970s, mathematicians developed a surprisingly effective solution to the key exchange problem. This envisaged special procedures in which special keys are used in pairs. One key is secret, the other public. Asymmetric cryptography was born.

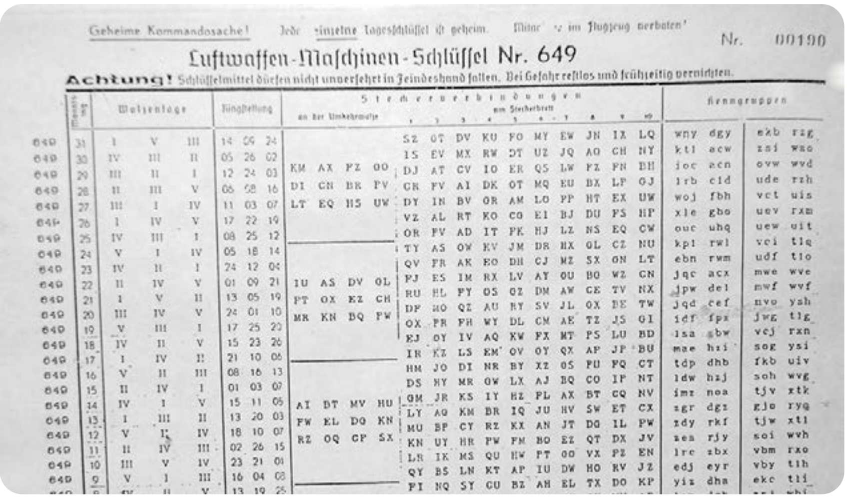

Geheime Kommandosache!
Nr. 00190
Luftwaffen-Maſchinen-Schlüſſel Nr. 649
Achtung! Schlüſſelmittel dürfen nicht unverſehrt in Feindeshand fallen. Bei Gefahr reſtlos und frühzeitig vernichten.
Walzenlage
Ringſtellung
Steckerverbindungen
Kenngruppen

Figure 2: Key lists and key books, as they were necessary for the Enigma, are no longer needed with asymmetric cryptography.

On one hand, asymmetric cryptography enables asymmetric encryption. This can be imagined like a mailbox with a snap lock: Anyone can drop a message in, but only the owner of the key can get it out. Mathematically, this is implemented with two keys belonging to one user: with the public key, anyone can encrypt a message for this person, and with the help of the associated private key, only this person can decrypt the message again. Of course, the user must keep his private key secret. The public key should be accessible to everyone.

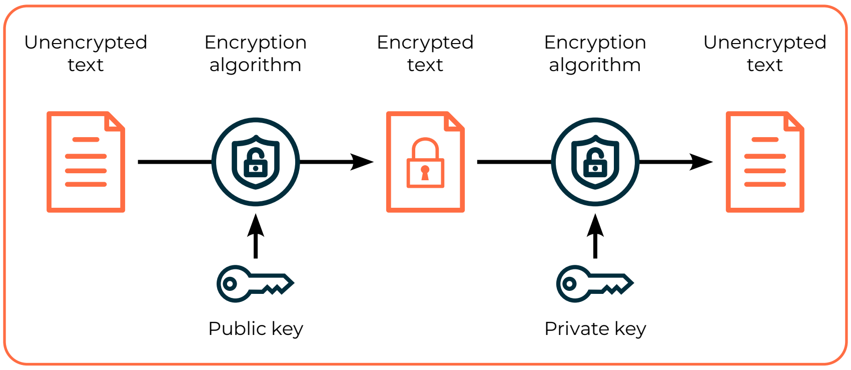


Figure 3: Asymmetric cryptography uses a public key for encryption and a private key for decryption.

On the other hand, asymmetric cryptography enables digital signatures. This is not a scanned signature, but a document digest created with a private key. Only the owner of this private key can generate it, but anyone can verify it with the help of the public key.

How do RSA and Diffie-Hellman work?

The best-known and most widely used asymmetric encryption method is **RSA**. This was developed in 1978 and is named after the initials of its inventors Ron Rivest, Adi Shamir and Leonard Adelmann.

RSA, like all asymmetric methods, is based on a one-way function. This is the name given to a mathematical function that is quick to compute, while the inverse requires a very large amount of computation. In the case of RSA, the one-way function used is the multiplication of two prime numbers. Even if the numbers used have hundreds of decimal places, such an arithmetic operation can be done in seconds with a computer. The inverse, on the other hand, i.e., the decomposition of the prime number product into its factors (also known as factorization), is not nearly feasible within the lifetime of a human being, even with the best computers available today.

The exact operation of RSA is not for discussion here. However, it is important to know: In the RSA process, the private key consists of two prime numbers (in practice, these have 300 to 700 digits), while the product of these forms the public key. It is therefore quite easy to calculate the public key from the private key, but this does not work the other way around.

Some other asymmetric methods—among them **Diffie-Hellman**—are based on the fact that the calculation of the exponential function is simple in certain mathematical structures, while the inverse (i.e. the logarithm) is very complex. This concept is called the discrete logarithm. The exponential function in question is a one-way function.

Diffie-Hellman is not suitable for encryption, but two communication partners can use it to securely agree on a common secret key. They can then use this key for AES, for example. The Diffie-Hellman method thus solves the key exchange problem. Factorization and the discrete logarithm are mathematically related. If it is possible to solve one problem that is, to invert the corresponding one-way function—then the other problem is also solved. This means that all popular asymmetric crypto methods ultimately depend on the same one-way function.

The RSA method can also be used for digital signatures, and it is even possible to use the same pair of keys. The private RSA key is used for signing, the public RSA key for verification.

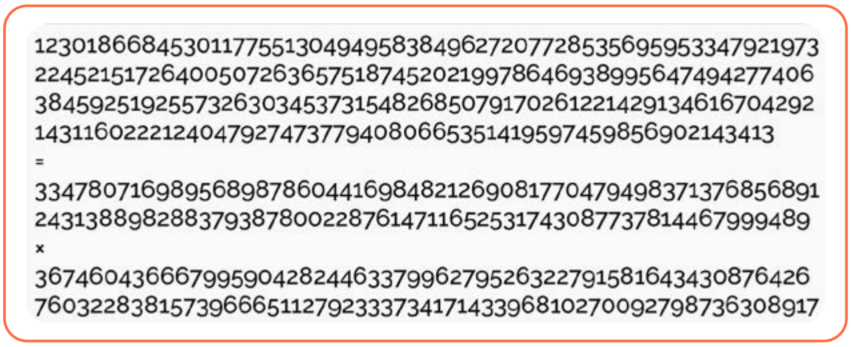

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413
=
33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489
×
36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

Figure 4: This 232-digit prime number product was decomposed into its two factors in 2009 after several years of computation. An entire cluster of computers needed 1500 processor years for this. The prime number products used for the RSA process typically have over 600 digits.

Chapter 2 – Quantum computers

What is a quantum computer?

Conventional computers, as they are used today, function according to the laws of classical physics. A bit can assume two states in such a computer, either 0 or 1 (see Figure 5).

A quantum computer, on the other hand, is based on quantum mechanical phenomena. Such a device uses quantum bits (qubits) that can assume the states 0 and 1 simultaneously. Quantum computers can therefore perform certain computational steps in parallel rather than sequentially. This quantum effect allows computing power to increase significantly and ensures that quantum computers can—at least in theory—perform some tasks orders of magnitude faster than conventional computers.

For example, quantum computers are able to search huge databases in a short time or pick out a particularly advantageous one from a large number of options. However, quantum computers have one disadvantage: although they can perform numerous calculations simultaneously, they can only ever deliver one result—for example, a database entry or an optimized operation. For example, a quantum computer is therefore not very fast at sorting a list alphabetically, since the result here is not a single list entry but the entire list.

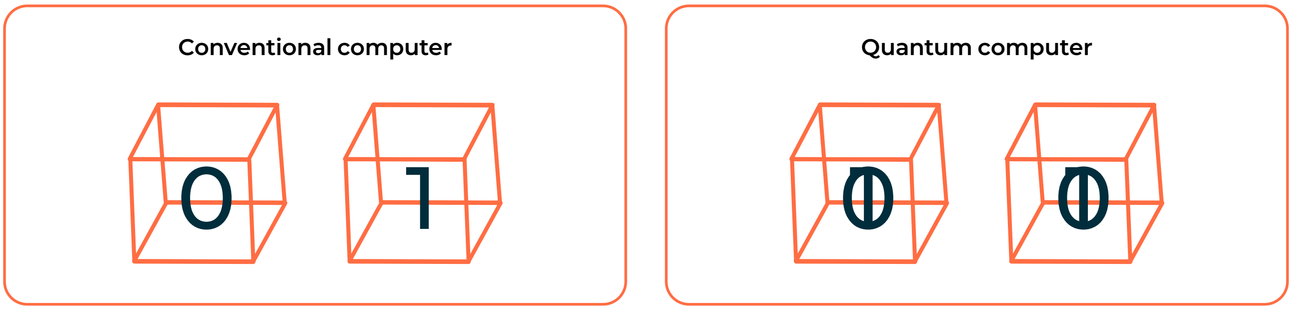


Figure 5: A bit of a conventional computer can only ever assume the value 0 or 1. In a quantum computer bit (qubit), on the other hand, both states are possible at the same time. Qubits can therefore be used to perform several calculations simultaneously.

What encryptions can be solved with quantum computers?

One of the tasks that a quantum computer can handle particularly effectively is the decomposition of a prime number product into the two associated primes. Since the RSA algorithm is based on precisely this mathematical principle, it is true that RSA can be cracked with a quantum computer. Diffie-Hellman and some other asymmetric crypto algorithms, like ECC, are also vulnerable to quantum computers.

Considering that RSA, ECC and Diffie-Hellman are used billions of times in web-browsers, smartphones, VPN clients and elsewhere, the current development is alarming. For example, a hacker with a quantum computer could empty online accounts at will or decrypt encrypted emails —to name just a few examples. A catastrophe of apocalyptic proportions is looming.

But there is no reason to panic yet. The quantum computers that have been realized so far are not particularly powerful and are also error-prone. To break an RSA key, a quantum computer needs about twice as many qubits as there are bits in the key. So with a key length of 2,048 bits, about 4,096 qubits are needed. However, these are error-free qubits, which do not exist in practice. The number of qubits needed in real terms for an RSA key could be 10 to 100 million. Today's quantum computers do not even come up with 100 qubits.

So, we are still a long way from a quantum apocalypse. But that can change, because intensive research is being carried out. For example, the NSA is working on quantum computers. The European Union has announced a "Quantum Technology Flagship Project," while the German government has included two billion euros in its budget to promote quantum technology.[5] Google has already succeeded in building practical quantum computers, even if they are not suitable for factorization and therefore do not pose a threat to cryptography. Hundreds of quantum computer start-ups have been founded.

Symmetric encryption schemes such as the AES can also be solved with quantum computers. However, the advantage that quantum technology brings here is much smaller than for asymmetric methods. The AES, for example, has a minimum key length of 128 bits—an order of magnitude that a quantum computer could just about manage in the distant future. If, on the other hand, 192 or 256 key bits are used, which the AES also supports, then even the best quantum computer will probably never stand a chance. So those who switch to longer AES keys in the next few years don't have too much to worry about. Many AES implementations have long since taken this step.

[5] https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/Technologie/quantentechnologien.html

Chapter 3 – Post-Quantum Cryptography

What is Post-Quantum Cryptography?

Fortunately, there are numerous other asymmetric crypto methods besides RSA and Diffie-Hellman. Some of them are not susceptible to quantum computers according to current knowledge. These are grouped together under the term **Post-Quantum Cryptography.**

In recent years, a wide range of post-quantum cryptographic schemes has emerged, driven largely by the need to prepare for the era of practical quantum computing. Many of these approaches were developed within the last decade, reflecting rapid progress but also significant churn in the field. As research matured, numerous candidates were proven insecure or turned out to be impractical for real-world deployment due to performance, implementation complexity, or resource constraints.

At the same time, several algorithms have demonstrated strong security properties and practical viability. These frontrunners have progressed through rigorous evaluation processes, leading to the first official standards, with additional standardization efforts currently underway. Early commercial implementations have already reached the market, providing organizations with tangible options to begin their transition.

The current focus lies in integrating these post-quantum schemes into operational systems and infrastructures. This transition must occur swiftly and comprehensively: the ultimate goal is to replace RSA, ECC, and Diffie–Hellman wherever feasible before powerful quantum computers materialize, ensuring that today's data remains secure against tomorrow's adversaries.

What is quantum cryptography?

Post-Quantum Cryptography should not be confused with quantum cryptography. The latter aims to use laser light for cryptographic tasks, especially to agree a secret key between two stations without the possibility of eavesdropping on the line—a concept also known as quantum key distribution (QKD). Quantum cryptography thus offers a solution to the key exchange problem. The data is usually transmitted using optical fiber.

Quantum cryptography has nothing to do with quantum computers, except that quantum physics is the base in both cases. In particular, quantum computers are not suited to perform or attack quantum cryptography. However, as quantum cryptography cannot be attacked with a quantum computer, it is sometimes regarded as a part of Post-Quantum Cryptography.

Compared to quantum computers, quantum cryptography is much easier to implement and is already being offered commercially in some cases. However, its usefulness is controversial. Since key exchange can be performed securely without quantum cryptography thanks to asymmetric cryptography, the former is only useful in some special scenarios.

What are the families of Post-Quantum Cryptography methods?

Over the past decades, well over 100 crypto methods have been developed that are considered quantum secure. Many of them showed security vulnerabilities that can be exploited without quantum computing or proved impractical. Some other post-quantum methods, on the other hand, have so far withstood all attempts at attack.

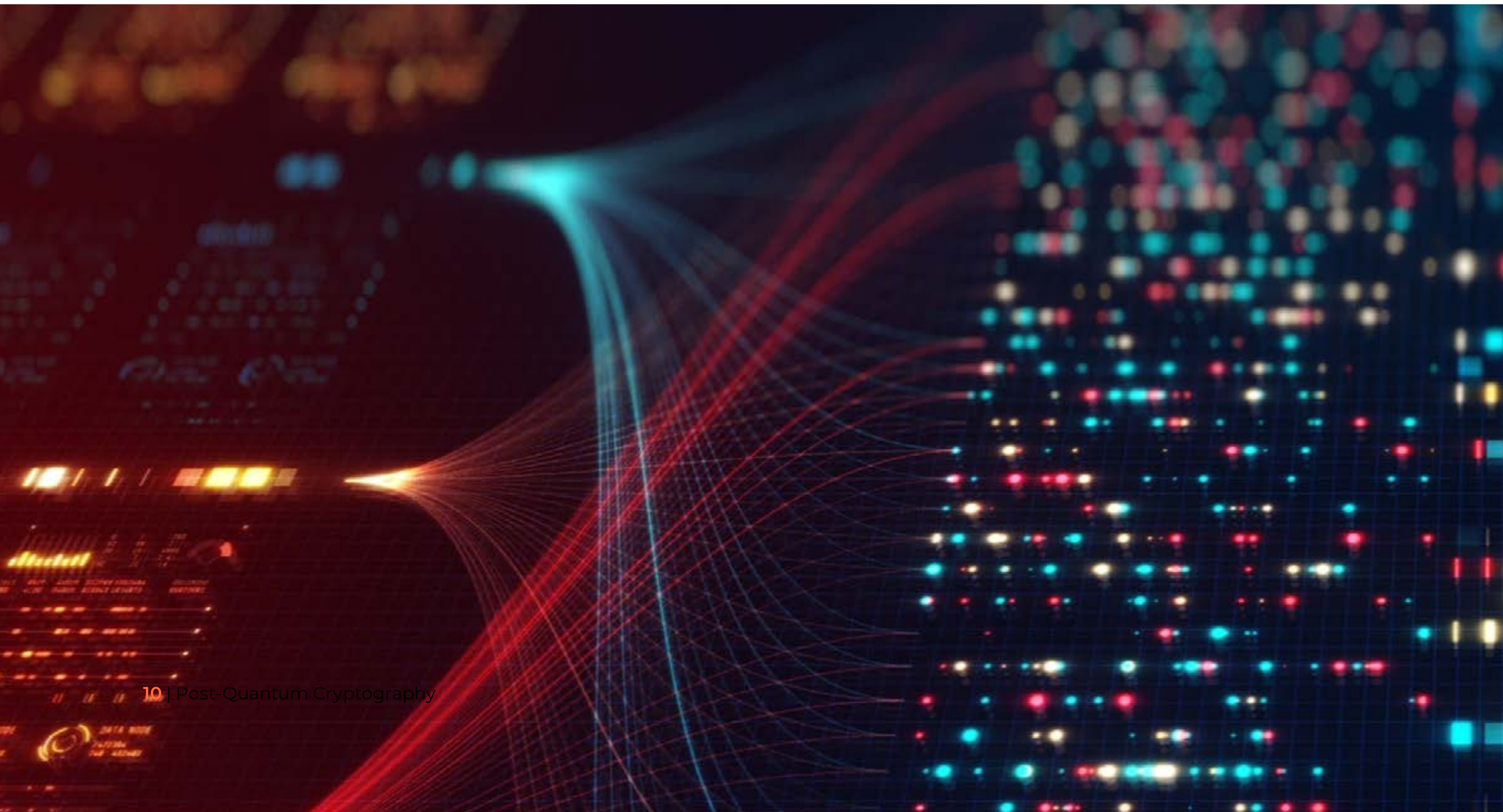
It turned out that almost all post-quantum methods that are to be taken seriously belong to one of six families that differ in their mathematical foundations:

- **Lattice-based algorithms:** These methods operate in high-dimensional lattices.
- **Hash-based algorithms:** These algorithms are based on cryptographic hashing functions.
- **Code-based algorithms:** Methods from this family use error-correcting codes.
- **Multi-party computation in the head (MPC in the head): Here, multi-party computing protocols form the base.**
- **Multivariate algorithms:** Multivariate polynomials form the base of these algorithms.
- **Isogeny-based algorithms:** Methods from this family use isogenies between elliptic curves.

Post-Quantum Cryptography is currently a very active area of research. It is therefore not surprising that there has been considerable upheaval in recent years. Most multivariate crypto methods did not stand up to the critical eye of the experts. In August 2022, SIKE, the most important isogeny method, was completely unexpectedly broken.

Code and hash-based methods have good security properties, but many of them require long keys or generate long signatures and are quite slow. MPC-in-the-head systems are still too new to be trustworthy. The most promising algorithms are undoubtedly the lattice-based ones, some of which have proven to be equally secure and practical. Still, the keys of these methods are in most cases significantly longer than those of RSA, ECC and Diffie-Hellman.

It is important to note that everything could turn out differently in the end—after all, no one knows which weak points in which methods the experts will discover tomorrow.



What was the first NIST post-quantum competition?

The U.S. authority NIST (National Institute for Standards and Technology) has held several competitions in recent decades to find the best possible cryptographic method for a specific purpose. The goal in each case was to standardize the winning algorithm. The NIST competitions always had a great influence on the development of cryptography. For example, the aforementioned AES spread worldwide after it emerged as the winner of a NIST competition in 2000.

In 2017, NIST launched another competition. This time, the aim was to pit post-quantum crypto methods against each other. Experts from all over the world were invited to submit suitable algorithms for this purpose, from which the best methods were to be selected in a process lasting several years. The aim was to identify a portfolio of high-quality post-quantum methods for different purposes and with different mathematical foundations. Both signature and encryption/key-exchange methods were eligible to participate.

NIST admitted 69 of the submitted methods to the competition. Many of the methods proved to be insecure or unsuitable on closer examination and were therefore eliminated from the race. After three rounds of evaluation, NIST finally announced four winners in July 2022. After an additional evaluation round, a fifth algorithm was added to this selection in March 2025. The five winners of the first NIST post-quantum competition are listed in the following:

- CRYSTALS-Kyber, standardized as **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism): This is a lattice-based method for asymmetric encryption.

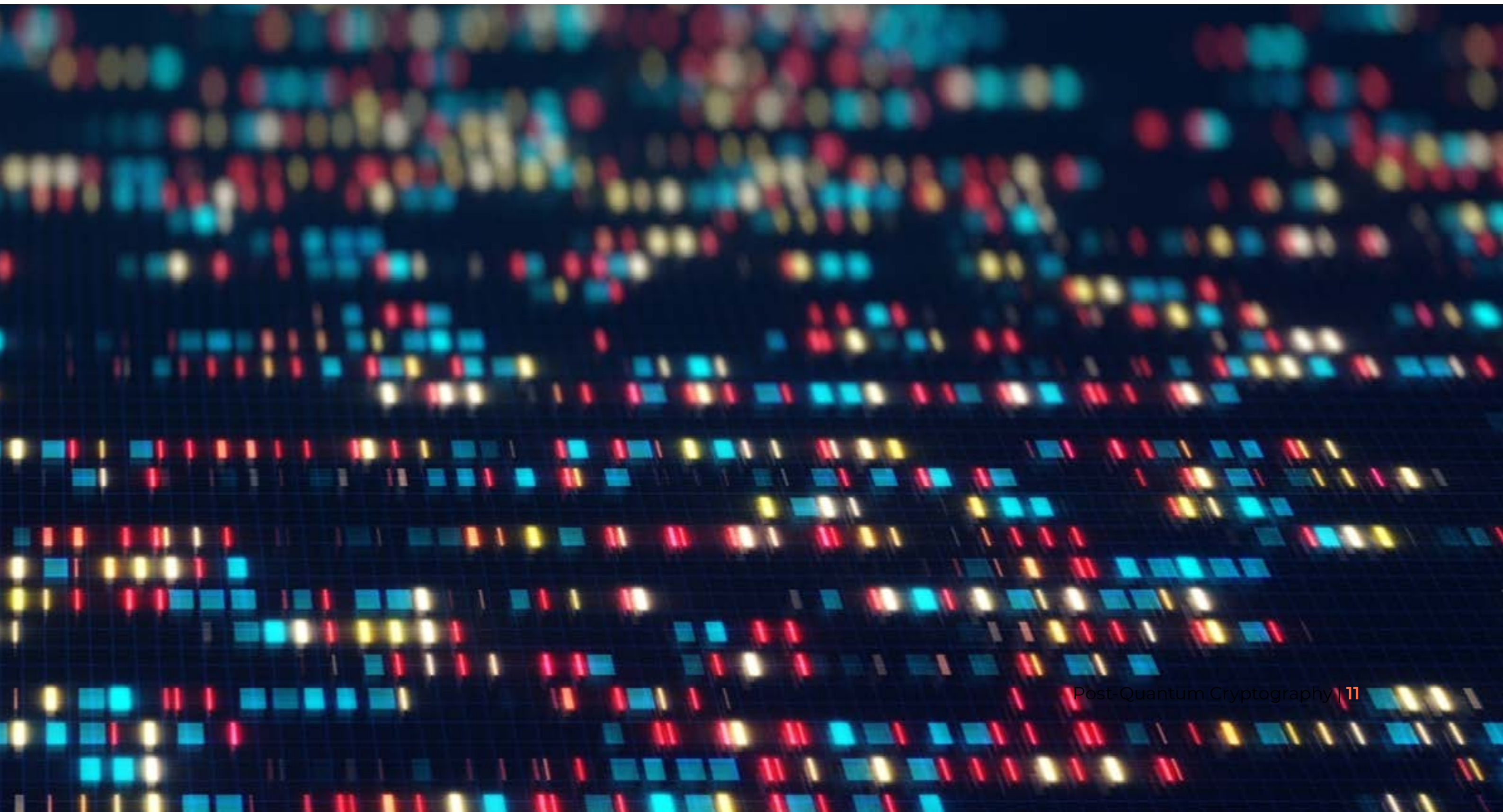
- CRYSTALS-Dilithium, standardized as **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm): Another lattice-based method, it is used for digital signatures.

- SPHINCS+, standardized as **SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm): The hash-based SPHINCS+ is another signature method.

- FALCON, to be standardized as **FN-DSA** (Fast-Fourier transform over NTRU-Lattice-Based Digital Signature Algorithm): This signature method is based on lattices, too.

- HQC, to be standardized as **HQC-KEM** (Hamming Quasi-Cyclic Key Encapsulation Mechanism): This is an asymmetric encryption scheme based on error-correcting codes.

ML-KEM, ML-DSA, and SLH-DSA have meanwhile been standardized by the NIST. The respective standard names are FIPS 203, FIPS 204, and FIPS 205. It is expected that FN-DSA and HQC-KEM will follow soon as FIPS 206 and FIPS 207.



What is the second NIST post-quantum competition?

Though the first NIST post-quantum competition concluded with the selection of five promising algorithms, many cryptographers remained unsatisfied with the outcome. A key concern was the strong dependence on lattice-based signature schemes, which dominated the field. In addition, experts emphasized the need for a practical, everyday digital signature scheme that would provide short signatures with fast verification times—features not delivered by the initial set of winners.

In response to these concerns, NIST announced a second post-quantum competition dedicated exclusively to digital signature algorithms. The official call for proposals was published in September 2022. Research teams from across the globe submitted candidate algorithms. On July 17 of the same year, NIST released the list of 40 approved submissions that would enter the competition. Notably, NIST refrained from specifying either the total number of expected finalists or a fixed competition timeline. Instead, it emphasized that the process would evolve depending on the quality and resilience of the candidate algorithms. Out of the 40 initial submissions, 14 advanced to the second round, which commenced in October 2024. At the time of writing, the further progression and final outcome of the second NIST post-quantum competition remain open.

As in the past, NIST's decisions are expected to have a major impact in the IT world. Undoubtedly, the various winning procedures will also be incorporated into numerous standards and products outside the United States.

Are there other PQC standards?

The Internet Engineering Task Force (IETF), the Internet's standardization body, will undoubtedly also take its cue from the NIST competition. In addition, there are already two "Requests for Comments" (RFCs) that specify post-quantum procedures. These are the stateful hash-based procedures **XMSS** (RFC 8391) and **Leighton-Micali** (RFC 8554), published in 2018 and 2019. As stateful algorithms were not accepted to the NIST competitions, neither XMSS nor Leighton-Micali took part in these contests. The IETF's choice is considered conservative, as hash-based methods are least likely to have security vulnerabilities discovered at some point. In return, one accepts a low level of efficiency.

The ISO, the International Organization for Standardization, is standardizing Post-Quantum Cryptography, too.[6] The first three systems on their list are the following:

- **ML-KEM:** This algorithm is one of the winners of the first NIST competition.
- **FrodoKEM:** This lattice-based system is considered secure, but could not hold its own in the NIST competition due to a lack of efficiency.
- **Classic McEliece:** This code-based scheme took part in the first NIST competition, but was not chosen as a winner. Classic McEliece is already over 40 years old, making it one of the oldest asymmetric methods ever. Since no one has found a weak point in over four decades, it can be assumed that it is secure. For this, one has to accept that the public keys are almost 700 times as long as with RSA.

[6] https://secdev.ieee.org/wp-content/uploads/2022/10/LaMacchia-Keynote-IEEESecDev2022.pdf

What do the national IT security authorities say?

The European Union Agency for Cybersecurity (ENISA) has published recommendations regarding Post-Quantum Cryptography mechanisms. In its document Agreed Cryptographic Mechanisms, ENISA extends its guidance beyond traditional schemes such as Diffie–Hellman (DH) and RSA to include PQC-based approaches.[7] Specifically, the agency highlights the key exchange mechanisms ML-KEM and **FrodoKEM,** as well as the digital signature schemes XMSS, Leighton–Micali, and SLH-DSA.

The German Federal Office for Information Security (BSI) is also keeping a close eye on current developments in quantum computing and Post-Quantum Cryptography. Of course, the experts there are initially guided by the NIST competition, the outcome of which will also have a major impact in the German-speaking world. The BSI in its document Kryptographische Verfahren: Empfehlungen und Schlüssellängen recommends NIST-winner ML-KEM as well as ClassicMcEliece and FrodoKEM.[8] The latter two are considered conservative choices. Neither method is among the most practical, but they have performed very well in security considerations.

[7] https://theinternetofthings.eu/wp-content/uploads/2025/05/ENISA_Report_1747792503.pdf
[8] BSI TR-02102 Kryptographische Verfahren: Emp-fehlungen und Schlüssellängen. January 2022

How does lattice-based cryptography work?

Lattices

Figure 6 shows what is meant by a lattice in mathematics. In two-dimensional space, the definition of a lattice requires two vectors, which are called A and B here. A and B together are also called the base of the lattice. Points that can be reached with the help of the vectors are called lattice points.

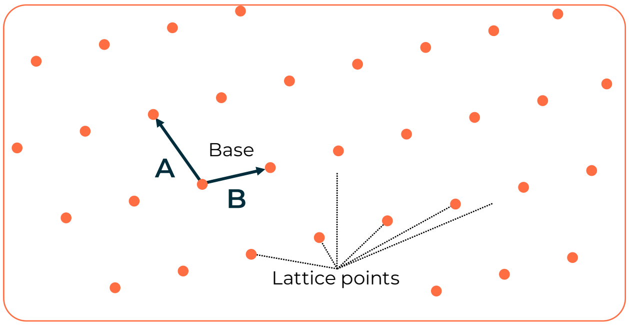


Figure 6: This lattice is defined with the two vectors A and B, which together are also called the base. Points that are reached via multiples of A and B are called lattice points.

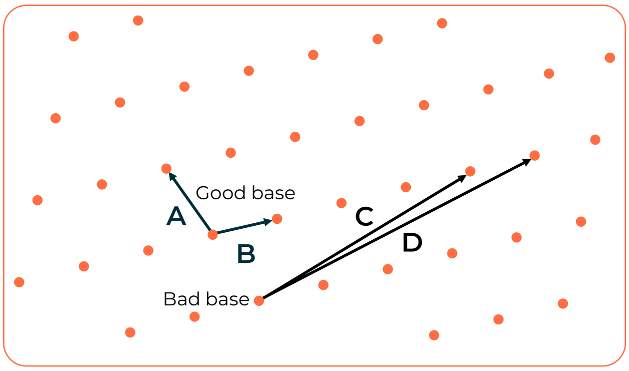


Figure 7: A lattice can always be defined with different bases. If the vectors of a base are approximately perpendicular to each other, it is called a good base; if the vectors are approximately parallel, it is called a bad base.

As shown in Figure 7, there are always several bases that produce the same lattice. If the base vectors are nearly perpendicular to each other, this is called a good base. If, on the other hand, they are almost parallel, we are dealing with a bad base. Of course, you can also define a lattice in three dimensions. For this, one needs a base with three vectors, whereby the third one must not lie in a plane with the other two. In mathematics one is not satisfied with two or three dimensions, but knows for example also four-, five- or six-dimensional spaces. One cannot imagine anything under it, but one can calculate in such spaces quite well.

In Post-Quantum Cryptography, we even have to deal with several hundred dimensions. For example, lattices in 500-dimensional space play a role there, for whose definition one needs accordingly a base with 500 vectors. In such a high-dimensional environment, one can simply calculate a bad base from a good one. The opposite way, on the other hand, is so complex that it would take billions of years even with the best computer.

How does ML-KEM work?

ML-KEM is one of the five post-quantum methods declared winners of the first NIST post-quantum competition. It is an encryption method and intended as a post-quantum alternative to RSA. ML-KEM is a lattice-based method and uses the so-called closest-vector problem (see Figure 8). In this, one assumes that a point P is given within a lattice, but it is not a lattice point. The question is: What is the closest lattice point to P?

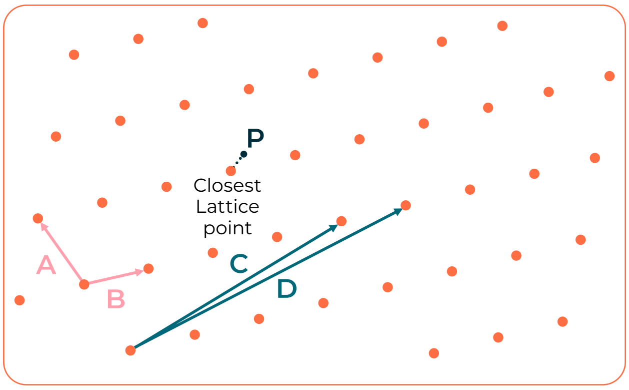


Figure 8: In the closest-vector problem, a point P is given. The goal is to find the closest lattice point to P. In two-dimensional space, this is very easy. In 500-dimensional space, however, such a search is only practical with the help of a good base.

In the two-dimensional case, the closest vector problem is very easy to solve—P has only four neighboring points, and one of them must be the closest. In a 500-dimensional lattice, however, things look different. Here, an off-lattice point has no less than 2500 neighbors—a number with 150 digits. Fortunately, you don't have to try all of them to find the next one, because there are more effective methods.

The following applies: If a good base of the lattice is known, a computer can find the closest lattice point in a fraction of a second, even in high-dimensional spaces. If, on the other hand, only a poor base is available, then even the strongest computer will fall to its knees.

GGH (Goldreich-Goldwasser-Halewi), a lattice-based asymmetric encryption algorithm, uses this principle (Figure 9). A good lattice base serves as the private key, while the public key is given by a bad base of the same lattice. To encrypt, the sender chooses a non-lattice point P in the immediate vicinity of a lattice point. The vector between the two points is the message. In 500-dimensional space, this vector has 500 components, which is enough to encode a 256-bit message, for example. The non-lattice point P is the ciphertext.

ML-KEM is another asymmetric encryption algorithm based on lattices. It is based on a computational problem that can be reduced to the closest-vector problem.

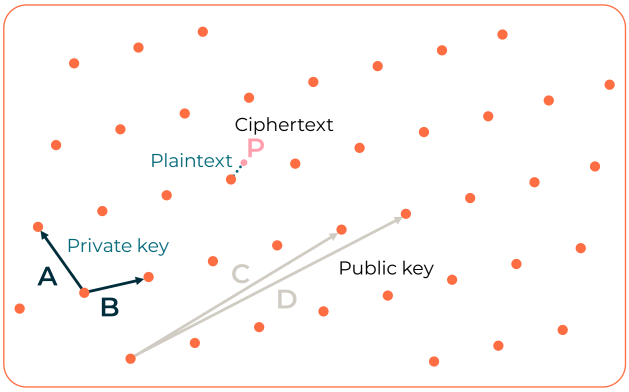


Figure 9: To encrypt with GGH, the sender chooses a non-lattice point P next to a lattice point. The vector between the two points is the message. P is the ciphertext. The receiver can easily reconstruct the message and thus decrypt the ciphertext, knowing a good base with which to compute the lattice point closest to the ciphertext. An attacker, on the other hand, has only a poor base available for this purpose, which makes it almost impossible to determine the lattice point in question.

How does ML-DSA work?

ML-DSA is also one of the four winners of the NIST competition. It is a digital signature method that, like ML-KEM, belongs to the lattice methods. However, the differences between ML-KEM and ML-DSA are greater than the common name suggests.

ML-DSA is also based on the closest-vector problem. The public key of the receiver is a non-lattice point P that is close to a lattice point. The latter forms the private key. Note that an attacker can compute the private key from the public key only if he solves the Closest Vector Problem, which is de facto impossible. In this case, the message m to be signed is a number, say 3. To sign, the sender chooses a second off-lattice point Q (see Figure 10), which is also close to said lattice point, and computes S=Q+m·P. The resulting point S is the signature.

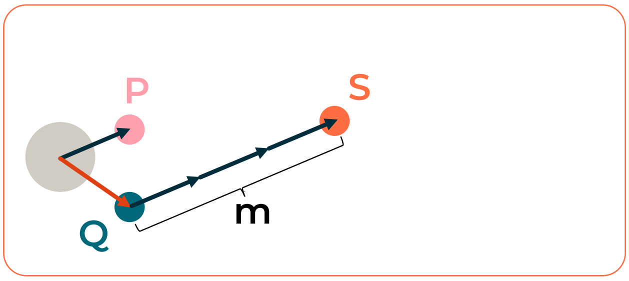


Figure 10: In this case, the message to be signed is a number, for example 3. For signing, the sender chooses a second non-lattice point Q, which is also close to the said lattice point, and calculates S=Q+m·P. The resulting point S is the signature.

To verify the signature, the receiver first checks whether S=Q+m·P holds. This is possible with a bad base. Furthermore, he measures the distance between S and the lattice point—if this is so small that the lattice point must be the closest to S, the signature is genuine.

In the figure, this scheme works only with small numbers for m. If you take m=10, for example, you get too close to other lattice points. Therefore, one should think of the distances between lattice points in this case as being on the order of several kilometers, while points P and Q are only millimeters away from the lattice point in question.

In this case, the near density m to be signed can also have a value of 100 without coming too close to other lattice points. Furthermore, it is relatively easy for the receiver to judge whether the distance between S and the lattice point is short enough. For example, if the distance is less than 50 centimeters, then the signature is most likely genuine, since a randomly chosen point would have been expected to be several hundred meters away. In practice, the differences are not between centimeters and kilometers, but several dozen orders of magnitude more.

How does FN-DSA work?

FN-DSA is the third lattice-based method to be selected as the winner in the NIST competition. It is a signature method. FN-DSA is based on a problem described in Figure 11. In addition to the base vectors A and B, vectors X, Y and Z are added here. The number of the additional vectors must be larger than the number of the base vectors.

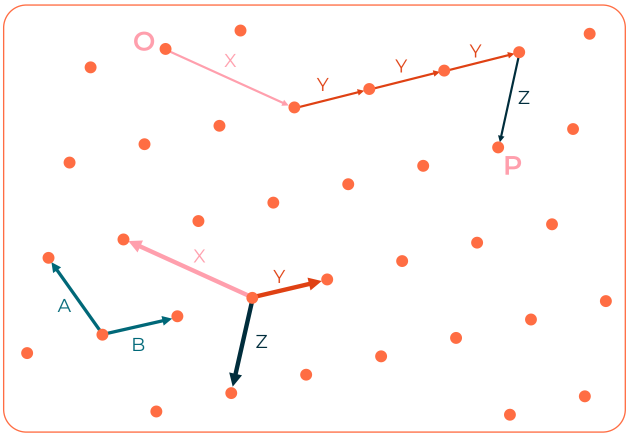


Figure 11: Here the question is: What is the shortest connection between 0 and P if only the vectors X, Y and Z are allowed as intermediate steps?

This principle can be used to explain the FN-DSA signature procedure (see Figure 12). In this case, the sender's private key is a lattice with an associated good base. The sender's public key is given by a bad base of the same lattice. Now, if the sender wants to sign a message, he converts it into a lattice point P. To create the signature, the sender calculates the shortest path between 0 and P, which is quite easy since he knows a good base. In the example, this shortest path is -X+3Y+Z, so the signature is -1, 3. 1.

If one considers now a starting point 0 on the lattice as well as another lattice point P, then the question is: Which is the shortest connection between 0 and P, if only the vectors X, Y and Z are permitted as intermediate steps? In two-dimensional space, the answer is easy to find. In the 500-dimensional case, on the other hand: With a good base, the shortest path is relatively easy to calculate. With a bad base, even the strongest computer needs billions of years and more.

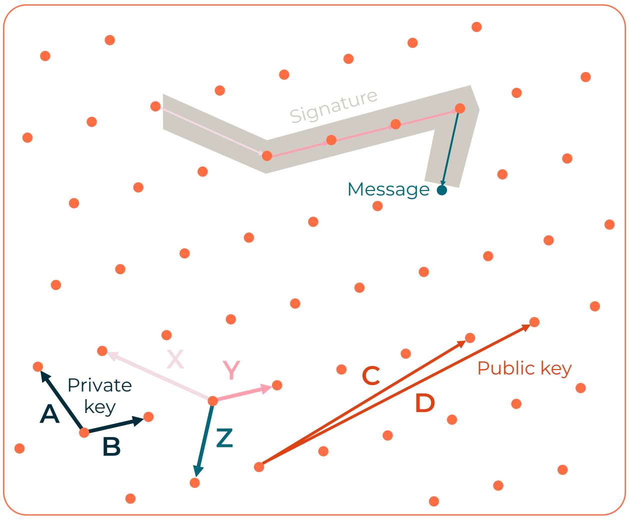


Figure 12: To create the signature, the sender calculates the shortest path between 0 and P, which is quite easy since they knows a good base. This shortest path results in the example from -X+3Y+Z, so the signature is -1, 3. 1.

The receiver of the message can use the bad base to verify that the signature does indeed lead from 0 to P. Unfortunately, they cannot directly verify that it is indeed the shortest path. However, they can estimate the length of the shortest path based on an easy-to-compute formula and compare it with the determined actual length of the path present as a signature. If the difference is small enough, the signature is genuine.

How do hash-based methods work?

The family of hash-based crypto methods differs in several respects from the other five post-quantum families described. Hash-based methods are comparatively simple mathematically. However, they can only be used for digital signatures, while they are not suitable for encryption. Another special feature is that a part of the private key must be made public for each signature, which limits the number of signatures per key.

Security considerations are the main arguments in favor of hash-based methods. Since the methods in this family originated back in the 1970s and are thus among the oldest asymmetric methods, they have been well studied. They are even provably secure under realistic conditions.

For this, hash-based signatures are considered unwieldy. Either the length of the signature or the length of the keys or the computing effort is too great for everyday use. Such methods are therefore particularly suitable when signing is performed infrequently, but particularly high and long-term security is required—for example, as a security anchor for communication with satellites.

The basic principle of hash-based signatures is comparatively simple:

1. The sender specifies two arbitrary constants X and Y, each consisting of 256 bits, for example. X and Y form the private key.
2. The sender applies a cryptographic hash function H to X and Y respectively. The results A=H(X) and B=H(Y) form the public key.
3. The sender now signs a bit as follows: If the bit has the value 0, he publishes X; if, on the other hand, it has the value 1, Y is published. The receiver verifies this signature as follows: If the signed bit has the value 0, then it checks whether A=H(X). In the other case it checks whether B=H(Y).

However, this process is quite time-consuming for the fact that only a single bit is signed. For example, if 256 bits are signed, then the sender must generate 256 values each for X and Y, apply the hash function to each of them, and publish the 512 results as a public key. In our example, this would give a length of over 131,000 bits each for the private and public keys, and this may then only be used for this one message. The signature itself is half as long as the key, i.e. about 65,500 bits. By comparison, RSA gets by with 2,048 bits of key and signature length, and a key can be used any number of times. There are various tricks to make this procedure more effective. However, these usually drive up the required computing time.

Another disadvantage: Since each value of X and Y may only be used once, the sender must remember which values have been used up and therefore keep a corresponding list. There is no such list for the crypto methods currently in use.

Signing with SLH-DSA

The hash-based signature method SLH-DSA is another winner in the NIST competition. SLH-DSA uses the principle described in the previous chapter to generate signatures. Through various optimizations, the developers have succeeded in reducing the size of the public and private keys to a few hundred bits. In return, the signature is two orders of magnitude longer than with RSA, and the performance is among the worst of all post-quantum methods.

As a hash-based method, SLH-DSA would actually need a used-key list. However, NIST wanted to avoid the difficulties associated with such a list from the outset and therefore only allowed signature algorithms without used-key lists for the competition. SLH-DSA therefore works with an additional trick: It provides a very large number of values for X and Y and provides that these are each selected randomly. If the number is large enough, the probability of a key being used twice becomes negligible. As a result, no used-key list is needed. SLH-DSA therefore complies with the NIST specifications.

Signing with XMSS and Leighton-Micali

The Internet Standards Body IETF has now also published two hash-based signature schemes:

- XMSS: The eXtended Merkle Signature Scheme (XMSS) is described in RFC 8391.
- Leighton-Micali: This procedure is specified in RFC 8554.

Both procedures were published as Informational RFC, which means that they do not have official standard status. However, they can be considered as quasi-standards. XMSS and Leighton-Micali require a list on which already consumed keys are noted. The two methods would therefore not have been eligible for the NIST competition.

How do code-based methods work?

Code-based algorithms belong to the oldest asymmetric crypto schemes, with origins dating back to the 1970s. Among the earliest and most notable examples is the McEliece cryptosystem, which demonstrated that public-key encryption could be based on the mathematical hardness of decoding general linear error-correcting codes. Despite its strong theoretical security, the McEliece system and related algorithms saw limited practical adoption for decades—primarily because they required extremely large public keys, often measured in hundreds of kilobytes. In recent years, however, new variants have emerged that significantly reduce key sizes while preserving or even enhancing security. The most prominent of these is the HQC (Hamming Quasi-Cyclic) encryption scheme, which represents the leading candidate among code-based cryptosystems in the ongoing standardization efforts for Post-Quantum Cryptography.

At the core of code-based cryptography lie error-correcting codes, mathematical constructs designed to detect and correct transmission errors in digital communication. To illustrate this concept, consider a simple scenario in which one party transmits radio messages as sequences of bits (for example, 01011001 00110101). Due to noise in the channel, some bits may flip—zeros might become ones and vice versa.

In this scenario, transmission typically occurs in fixed-size blocks of bits, such as eight bits per block. Each such block is referred to as a data word. Certain codes can correct transmission errors by introducing redundancy: they multiply the data word by a so-called generator matrix, resulting in a longer code word. The additional bits encode redundancy, which can later be used to detect and correct errors.

A well-known example is the Hamming code. In one of its standard forms, it encodes 4-bit data words into 7-bit code words. For instance, given the data word 1011 multiplying the data word with the generator matrix yields the code word 1011010:

$$\begin{pmatrix}1 & 0 & 1 & 1\end{pmatrix}.\begin{pmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 0\end{pmatrix}$$

While such codes can effectively correct small numbers of bit errors, the computational effort for decoding can become enormous when larger code lengths and higher error-correction capacities are involved. For example, a code that produces 1000-bit code words and can reliably correct 50 errors would require an infeasible amount of computation—even for the most powerful modern computers.

Fortunately, there exist families of error-correcting codes for which decoding can be performed much more efficiently. This difference in decoding complexity is precisely what code-based cryptography exploits: the public key encodes a code that appears hard to decode for an adversary, while the legitimate key owner possesses a hidden structure that allows for efficient decoding. This asymmetry between “hard for others, easy for me” forms the foundation of secure, code-based public-key cryptosystems.

McEliece encryption

A good matrix is defined as the generator matrix of a code that allows for fast error correction. Conversely, if error correction is computationally demanding, the matrix is referred to as a bad matrix. Randomly generated matrices are almost always bad, so a good matrix must be constructed or selected deliberately. It is possible, however, to transform a good matrix G into a bad one B. This is achieved by multiplying G on the left by a randomly generated, invertible matrix M, called the blend matrix. For example:

$$B = M \cdot G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Performing this multiplication—i.e., blending a good matrix with a scrambling matrix—can be done easily using suitable software. However, reversing this process, meaning decomposing a bad matrix B into its factors M and G, is computationally infeasible for large matrices, even with the most powerful computers. This makes the operation a one-way function.

Let us assume that the bad matrix B generates an error-correcting code with long codewords (for example, 1000 bits) capable of reliably correcting a fixed number of errors (say, 25).

To encrypt, a data word representing the plaintext is multiplied by the public (bad) matrix B, resulting in a codeword. Then, 25 random bit errors are deliberately introduced into the codeword.

Decrypting the message requires correcting those 25 errors and transforming the resulting codeword back into the original data word. With only the bad matrix, this is practically impossible. However, if one knows the decomposition of the bad matrix into its components B=M.G, the process becomes straightforward: one can first remove the scrambling matrix M and then use the good matrix G to efficiently correct the errors.

Currently, the McEliece system is considered secure when the generator matrix has 2048 columns and 1751 rows, and is capable of correcting 27 errors. In this configuration, the public key size is roughly 0.5 megabytes. If McEliece proves to be a viable Post-Quantum Cryptography scheme, it is expected that even larger parameters will be used, resulting in public keys of around 1 megabyte or more in size.

Encryption with HQC

In addition to the McEliece encryption scheme, another significant code-based cryptographic algorithm has emerged in recent years: **HQC,** which stands for Hamming Quasi-Cyclic. HQC was selected as one of the five winners of the first Post-Quantum Cryptography Standardization competition organized by NIST. HQC is based on the Learning Parity with Noise (LPN) problem. The LPN problem can be described as follows: given a binary system of linear equations that admits many possible solutions, the task is to find a solution vector containing as few ones as possible. Consider the following example:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot e = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

A valid solution with a minimal number of ones is, for example, e=(0 0 1 1 0 0 0 0 0).

In the context of error-correcting codes, the vector e represents the error pattern that may occur during data transmission—the ones indicate the positions of incorrectly transmitted bits. The goal is therefore to identify the bit positions where transmission errors occurred, under the assumption that only a small number of errors are present.

HQC introduces a second code into the system, also defined by a publicly known generator matrix. A randomly generated codeword from this code, combined with a controlled amount of noise (errors), constitutes the private key. The public key is derived from this in such a way that reconstructing the private key from the public key would require solving the LPN problem — a task believed to be computationally infeasible, even for quantum computers.

The plaintext message is first encoded as a data word, which is transformed into a codeword using the generator matrix G and subsequently perturbed by adding a small amount of noise. The resulting word is then masked using the second code. Upon receiving the ciphertext, the legitimate receiver uses the private key to remove the masking and applies the decoding algorithm associated with the good matrix G to correct the errors, thereby recovering the original plaintext.

A common drawback of code-based cryptosystems is their typically large public key sizes. HQC, however, achieves surprisingly compact public keys—approximately 36,000 bits for a medium security level. This reduction is possible because HQC does not require the public key to include a full generator matrix; instead, it uses a matrix structure that can be stored efficiently. Nevertheless, 36,000 bits are still significantly larger than the 2,048 bits typically required for RSA public keys.

The private key in HQC can be stored efficiently as well, with a size of about 500 bits, while the ciphertext for medium security levels has a length of approximately 72,000 bits. HQC also offers faster decryption than RSA, which makes it attractive for applications where quick message recovery is essential. However, encryption performance remains a relative weakness, as the process of adding and masking noise is computationally more intensive than RSA encryption.

Which other PQC families do exist?

MPC-in-the-head algorithms

MPC-in-the-head (Multi-party computation in the head) signatures represent a novel and elegant class of post-quantum digital signature schemes. The fundamental concept is derived from secure multi-party computation (MPC), where several participants jointly compute a function on private inputs without revealing those inputs to one another. In MPC-in-the-head, this paradigm is simulated "inside the signer's head". Instead of performing the computation among multiple parties, the signer emulates the behavior of all participants. The signature is then constructed by selectively revealing parts of this simulated computation to convince a verifier that the computation was performed correctly, without exposing the secret key itself. Despite their robustness and elegant design, MPC-in-the-Head signatures also face practical challenges. The main drawback lies in their relatively large signature sizes—often tens of kilobytes—and moderately high verification costs compared to classical schemes. As research continues, MPC-in-the-Head schemes remain one of the most promising approaches to achieving efficient digital signatures in the post-quantum era.

Multivariate algorithms

Multivariate cryptography represents one of the oldest branches of Post-Quantum Cryptography. Its security is based on the computational hardness of solving systems of multivariate quadratic equations over finite fields. As an example, the following equation system containing quadratic polynomials is hard to solve:

$$2x^2+3y^2+5xy+3x+3y=6 \pmod 7$$
$$3x^2+3y^2+4xy+2x+2y=5 \pmod 7$$

If the numbers and variables involved become larger, even the most powerful computer can't solve the problem in a reasonable amount of time. In a multivariate cryptosystem, two such systems of equations are typically employed: a public system and a secret one. The secret system is used for signing or decrypting messages, while the public system serves for verification and encryption. The transformation from the secret to the public system constitutes a one-way function.

Overall, multivariate algorithms are relatively easy to understand and well-studied. However, they face significant challenges. Many proposed systems have been broken over time, seriously undermining their credibility. In addition, their public keys are typically quite large—often reaching several hundred kilobytes.

Isogeny-based algorithms

Isogeny-based cryptography is one of the youngest branches of Post-Quantum Cryptography. While the theory of elliptic curves has long been used in classical cryptography, isogeny-based approaches shift the focus from scalar multiplication to the structure of the isogeny graph itself, where each node represents an elliptic curve and each edge corresponds to an isogeny between them. Its security is founded on the computational hardness of finding isogenies—that is, algebraic mappings—between elliptic curves. Two elliptic curves are isogenous if there exists a certain mapping from one to the other.

The most prominent example of this family is the Supersingular Isogeny Diffie–Hellman (SIDH) protocol and its derivative, Supersingular Isogeny Key Encapsulation (SIKE). Unlike lattice-, code-, or multivariate-based schemes, isogeny-based cryptography offers very small key sizes—often in the range of just a few hundred bytes—comparable to pre-quantum elliptic-curve cryptography.

However, this field has recently faced significant challenges. In 2022, the SIKE scheme was broken by a classical attack. While this was a major setback, it did not invalidate the broader potential of isogeny-based cryptography. Research is now focusing on new directions, such as isogenies on higher-genus curves and alternative hard problems within isogeny graphs that may resist similar attacks.

Chapter 4 – What's next?

Continued standardization and optimization

Further PQC algorithms

The standardization of post-quantum algorithms is on-going. As mentioned in Chapter 3, the second post-quantum competition (currently 14 candidates remaining) is expected to render a number of additional digital signature algorithms in the near future. The ISO standardization work is on-going, too.

It is also worth looking at other regions. On the one hand, Canada, UK, Australia, New Zealand, Japan amongst other countries are adopting NIST-selected algorithms, while the European Union (from where most of the NIST-selected algorithms are from) leverage them but are additionally promoting their own implementations. Some other regions and countries, such as China, Russia, Ukraine or South Korea, have chosen to perform their own assessment and selection, on top of or instead of (depending on the cases) the NIST schemes. Few of those countries have announced yet their final selection but the algorithms they were announcing are mostly rooted, with some tweaks, on the cryptographic schemes which were finalists of the NIST competition (ML-KEM, ML-DSA, NTRU, SIKE, SLH-DSA, FN-DSA…)[9].

Amongst those, South Korea announced, end of 2024, their selection[10], with domestic post-quantum schemes: the key-encapsulation mechanism (KEM) algorithms **SMAUG T** and **NTRU+**, and the signature algorithms **HAETAE** and **AIMer.** The South Korean government has announced a "PQC Master Plan" targeting a full transition of its national cryptographic system by 2035, aligning with other regions targets.

Crypto agility

Even when the first encryption formats for the Internet were developed more than three decades ago (it was initially a matter of emails), it was clear: the encryption methods used must be interchangeable. The manufacturers of crypto software were expected to enable the user to select his preferred crypto algorithms via a configuration setting and to being able to incorporate additional procedures into their products in a simple manner. In this way, it was possible to react quickly, especially if a method turned out to be insecure.

This principle is now widely used and known as **crypto agility.** For instance, most protocols used on the Internet, such as TLS or IPsec, are crypto-agile, which means that implementations may allow switching from one crypto method to another at the click of a mouse. Crypto agility is achieved primarily by the fact that the crypto processes used are not a fixed component of the respective solution, but are implemented in independent modules and called via precisely defined interfaces.

In the age of Post-Quantum Cryptography, crypto agility is more important than ever. In view of the threat posed by quantum computers and the fact that many a vulnerability has been discovered in post-quantum procedures in recent years, it must be possible to switch from one procedure to the other without major effort.

However, in the age of Post-Quantum Cryptography, it is also more challenging than ever to ensure crypto agility. This is because the various post-quantum methods have different properties than RSA and Diffie-Hellman. This is most noticeable in the keys, which are often many times longer in Post-Quantum Cryptography than in conventional methods. Many a protocol cannot handle this so far. For a crypto manufacturer, therefore, it is not enough just to include another library function. In resource-poor environments, the low performance of post-quantum methods also stands in the way of crypto agility.

The aforementioned used-key lists required by some of the hash-based methods are another challenge. This is because many crypto solutions are not set up to store data that will be queried in future crypto operations. This could affect the proliferation of such methods.

The use of Post-Quantum Cryptography is thus inextricably linked to the crypto-agility paradigm. Undoubtedly, the market will more and more demand crypto-agile solutions, and manufacturers will have to adapt to this. Standards, benchmarks, and certifications need to be developed.

[9] Some of the schemes being favoured included: Forzitsiya, Skelya, Aigis-enc, Lac.PKE… for KEMs, Shipovnik, Kryzhovnik, Vershina, Sokil, Aigis-sig… for signatures

[10] South Korea selection https://kpqc.or.kr/competition_02.html

In addition, the increasing necessity for crypto agility will make enterprise-wide key management even more important. If a new crypto algorithm shall be introduced or an existing one abolished, it is crucial to have an overview on which application uses which methods and to have the means to easily change this.

More information about crypto agility is provided in the NIST document Considerations for Achieving Cryptographic Agility: Strategies and Practices."

Hybridization

Many experts advocate using conventional encryption techniques and post-quantum processes in parallel during a transition phase. Crypto systems that follow this approach by combining a conventional and a post-quantum scheme are referred to as hybrid algorithms. Hybrid algorithms make it possible to live with any security gaps in the latter methods. After a few years, one could then switch over completely.

However, hybrid approaches remain a subject of debate. Proponents emphasize the increased security such schemes provide in case a post-quantum algorithm is eventually compromised. Critics, on the other hand, point to the added complexity that comes with implementing and maintaining two cryptographic systems in parallel. The German Federal Office for Information Security (BSI)[12] and the French National Cybersecurity Agency (ANSSI)[13] are among the advocates of the hybrid approach, whereas it is viewed more critically in the United States.

High level protocols

While the standardization of the algorithms is making progress, organizations and standards bodies are accelerating efforts to embed post-quantum schemes across network protocols and data-format infrastructure. Key activities currently include:

- Bodies such as the Internet Engineering Task Force (IETF) are working on Internet Drafts and extensions that introduce post-quantum primitives in protocols, such as TLS 1.3 or IKEv2.

- Academic and industry teams are integrating post-quantum systems into frameworks such as OpenSSL and Open Quantum Safe.

- Beyond protocol handshakes, many systems are examining how to update crypto formats (e.g., certificate profiles, key encapsulation formats, signed message formats) to accommodate larger key sizes, different parameter sets, and hybrid structures required for Post-Quantum Cryptography. For constrained environments (IoT, embedded, automotive) the differences in size, performance and memory are significant challenges.

In summary, the community is showing strong momentum: protocols are being adapted, implementations prototyped, migration frameworks defined, and standards calls issued. The remaining hurdles are mainly practical–performance, interoperability, existing-infrastructure compatibility and rollout in constrained systems.

Facilitating and optimizing implementations

In the coming years, it will continue to be important to study the procedures of Post-Quantum Cryptography. Cryptologists will undoubtedly find many more improvements, and they will discover vulnerabilities in procedures previously considered secure.

And then numerous challenges await when it comes to implementing Post-Quantum Cryptography. Current smart card chip architectures, for example, are mostly designed for RSA, ECC or Diffie-Hellman keys and have a corresponding coprocessor. In contrast, they are not designed to perform lattice or code operations, certainly not with the necessary key lengths. The revision of current chip architectures is therefore an important challenge for the coming years.

[12] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf

[13] www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition

There have long been numerous research projects investigating the use of the new methods in practice. Among the most important is the Aquorypt project ("Applicability of Quantum Computer-Resistant Cryptographic Methods"), which is concerned with the implementation of post-quantum methods on chip cards and in embedded systems.[14] It is supported by the German Federal Ministry of Education and Research. Meanwhile, at the IETF, there are several activities aimed at integrating post-quantum methods into Internet protocols.

Public key infrastructures (PKI), including X.509 and card-verifiable certificates, must also become post-quantum capable. The long keys alone make this a challenging undertaking. Several research projects are also underway in this area.

Atos/Eviden positioning

Who are Atos/Eviden

Atos Group is a global leader in digital transformation with c. 63,000 employees and annual revenue of c. €8 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

The Atos Group, supported by its Eviden cryptographic products R&D and its quantum computing division, is an ideal partner to help its customers:

- **Manage complex cybersecurity programs:** Atos Cybersecurity Services have managed the Olympic Games from Barcelona 1992 to Paris 2024[15] and concluded several major cybersecurity contracts with the European Union.[16]
- **Understand the threat:** Our Qaptiva[17] quantum computing experts provide advice on quantum programming. They support our Cybersecurity teams by deciphering for them the news on quantum computing and helping them filter out what is relevant in terms of quantum risk.
- **Design and tailor highly certified cryptographic products:** Our Cybersecurity Products[18], fully designed and developed in Europe, comply with the strictest international standards and certifications. We included post-quantum algorithms very early on and we have an ambitious roadmap with respect to crypto agility.

In 2021, Eviden acquired the German cryptography specialist **cryptovision.** Since its founding in 1999, cryptovision has focused exclusively on encryption technologies and has earned a global reputation for secure yet user-friendly security solutions. Today, the company possesses substantial expertise in Post-Quantum Cryptography.

What is Eviden doing in the area of Post-Quantum Cryptography?

Eviden is already preparing for the next generation of encryption technologies, including Post-Quantum Cryptography. Traditionally, the company has placed great emphasis on crypto agility. Thus, the company's products typically support multiple crypto methods for the same purpose, with the ability to switch between them at the click of a mouse (see Figure 13).

[14] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aquorypt

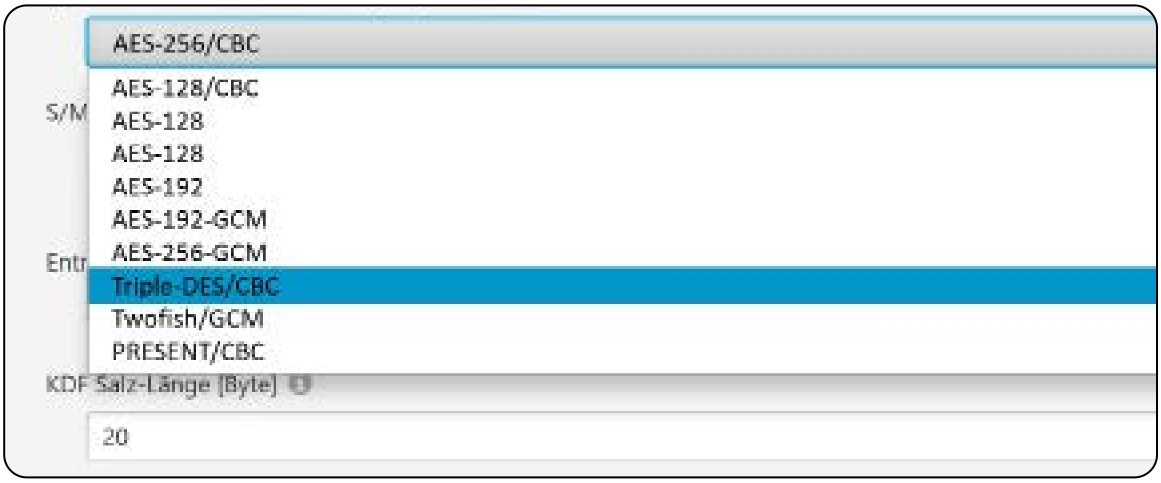
[15] https://atos.net/en/client-stories/securing-the-olympic-and-paralympic-games-paris-2024

[16] Illustration, on september 2025, with the European Commission :
https://atos.net/en/2025/press-release_2025_09_24/atos-secures-major-european-commission-cybersecurity-contract-for-technical-operations-services

[17] https://eviden.com/solutions/quantum-computing/

[18] https://eviden.com/solutions/cybersecurity/

In addition, obsolete methods can be easily deactivated and new ones incorporated. In this way, Eviden is managed the transition from RSA to ECC and from DES to AES. The transition to quantum-safe cryptography is carried out using the same mechanisms. When a post-quantum method is standardized and ready for use, Eviden integrates it into the existing products.



KDF Salz-Länge [Byte]

20

Figure 13: Eviden places great emphasis on crypto agility. The company's solutions typically support multiple crypto methods for the same purpose, with the user able to switch between them at the click of a mouse.

Eviden Cybersecurity Products in detail

Eviden Cybersecurity Products aims to develop future-proof products for digital trust, taking into consideration newest evolution in technology. Eviden Cybersecurity Products covers the whole product spectrum:

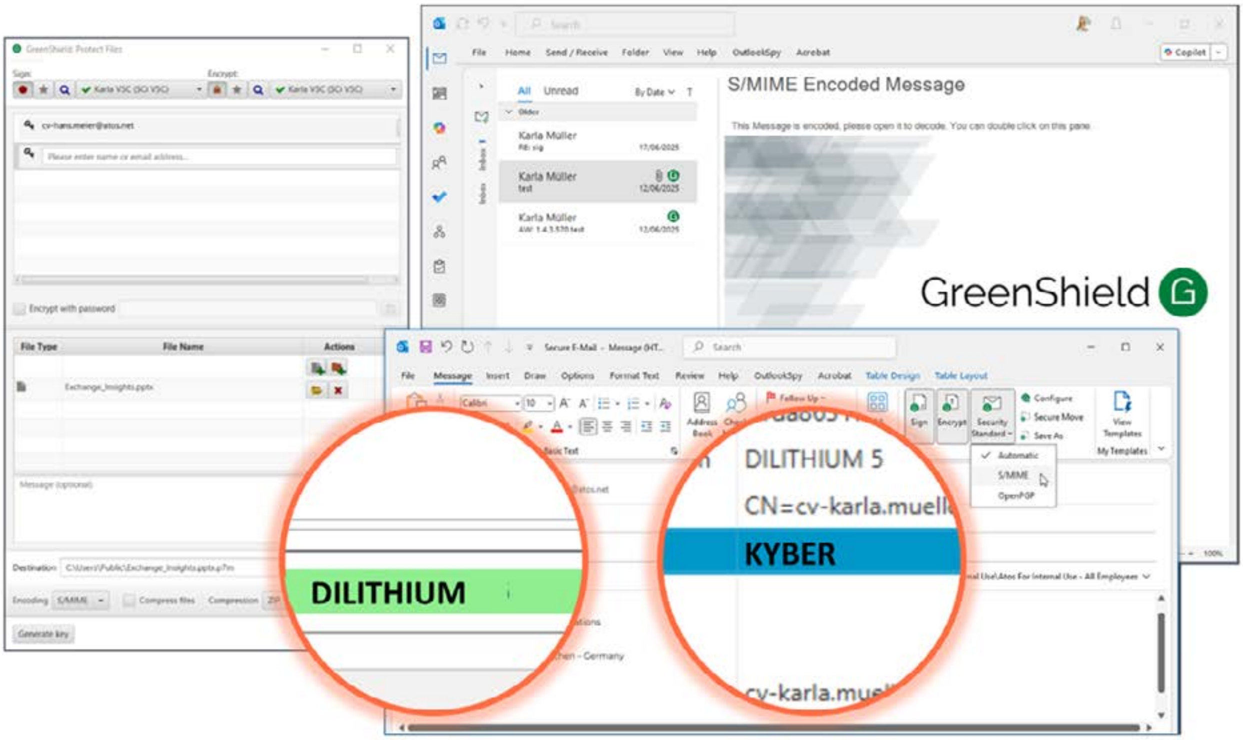
- Cryptographic key generation and usage in a highly protected environment by means of **Eviden Proteccio HSM** (Figure 14) and on-chip with **CardOS** in conjunction with our partners from the smart card industry.
- Post-quantum-ready IPsec network solution confidentiality and integrity of IP flows. **Eviden IP Protect** supports hybrid and Post-Quantum Cryptography, enabling a progressive migration toward quantum-safe communications.

Figure 14: Eviden Proteccio HSMs protect cryptographic key. They are highly certified and PQC ready.

- Next-generation Key Management System, **Eviden DataProtect,** integrates **Covercrypt**[19] an advanced encryption library supporting post-quantum algorithms. Based on the KEMAC (Key Encapsulation and Message Authentication Code) scheme, it enables fine-grained access control to specific data. The solution also implements hybrid PQ/T (pre-quantum and post-quantum) schemes. This innovative approach has been standardized by ETSI.

[19] Covercrypt is standardised by ETSI under TS 104 015 https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=68585

- **Eviden PKI** implements crypto agility and able to issue hybrid/composite and post-quantum only digital certificates.
- Smart card middleware **Eviden SCinterface** and credential management system **Eviden CMS** deploy post-quantum credentials on all kinds of devices.
- **Eviden's Identity and Access Management (IAM)** suite—including Enterprise Access Manager (EAM), Web Access Manager (WAM), Orbion Access & Governance (IDaaS), and Identity Governance & Administration (IGA)—are critical enforcement layers in our customer's transition to quantum-safe architectures. Our assessment confirmed that they present a lower direct exposure to the quantum risk. In response to these findings, Eviden has strategically aligned its IAM PQC integration roadmap, ensuring seamless compatibility with Eviden cryptographic products. As post-quantum standards are adopted by higher level protocols such as SAML 2.0, OpenID Connect, OAuth 2.0, and FIDO2/passwordless authentication, those will be adopted in the Eviden IAM suite.
- PQC-ready end-to-end protection for email and files—from government agencies to companies—with **Eviden GreenShield** (see Figure 15). Eviden GreenShield offers protection with approval up to VS-NfD and NATO/EU-restricted.
- Digital signatures with **Eviden Sign,** a platform that implements digital identities based on Post-Quantum Cryptography.



S/MIME Encoded Message

This Message is encoded, please open it to decode. You can double click on this pane.

Sign: Karla VSC (SO VSC)

Encrypt: Karla VSC (SO VSC)

cv-hans.meier@atos.net

Please enter name or email address...

File Type	File Name	Actions
	Exchange_Insights.pptx	

Destination: C:\Users\Public\Exchange_Insights.pptx.p7m

Encoding: S/MIME

Karla Müller
RE: sig
17/06/2025

Karla Müller
test
12/06/2025

Karla Müller
AW: 1.4.3.570 test
12/06/2025

DILITHIUM

DILITHIUM 5

CN=cv-karla.muell

KYBER

cv-karla.mue

Figure 15: Eviden GreenShield encrypts and signs emails in a user-friendly way. It also supports file encryption and signature. Among other systems, the post-quantum algorithms CRYSTALS-Dilithium (ML-DSA) and CRYTALS-Kyber (ML-KEM) are supported.

How does Eviden explain Post-Quantum Cryptography?

Eviden is aware that Post-Quantum Cryptography will only succeed when developers, consultants, IT managers, administrators and IT executives all come to grip with it. Because crypto literacy is not widely prevalent, Eviden is actively involved in many activities that aim to help explain Post-Quantum Cryptography to non-specialists in many diverse ways. Eviden has developed explanatory models for Post-Quantum Cryptography based on cartoons and everyday analogies (See Figures 16 and 17). They have already been presented at numerous events—including the RSA Conference in San Francisco, Dragon Con in Atlanta, 44CON in London, Trustech in Paris, and DEF CON in Las Vegas.

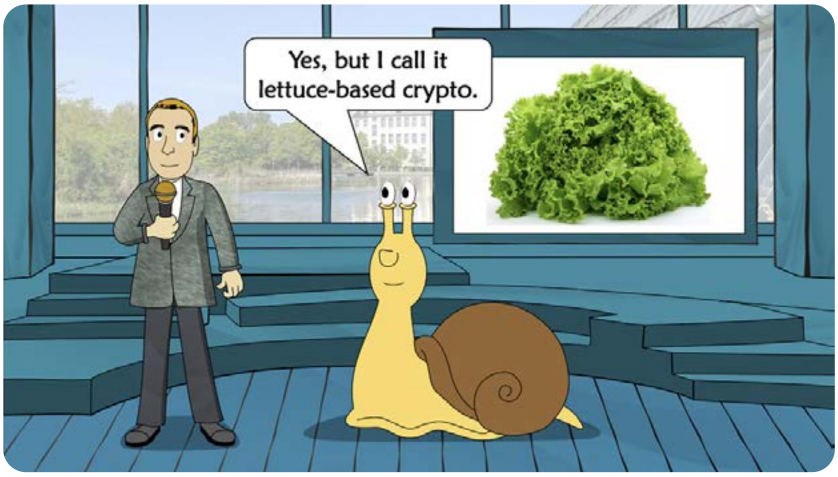


Figure 16: Eviden works with models based on comics and everyday analogies that vividly explain Post-Quantum Cryptography.

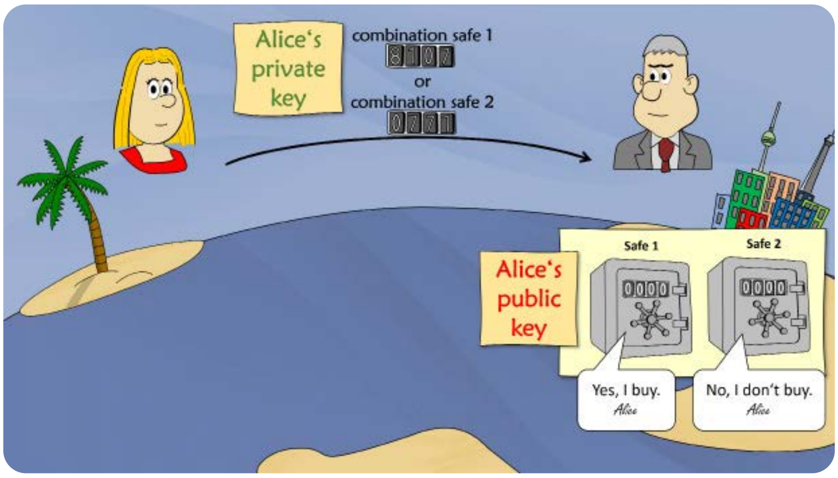


Figure 17: Eviden' comic explanations have already been presented at numerous international events with great success.

Migrating to Post-Quantum Cryptography

Recommended Reading

As organisations embark on the journey of migrating to Post-Quantum Cryptography, it is essential to rely on practical and up-to-date guidance. To learn more, check Eviden's Post Quantum Migration Guide[20].

In addition, we recommend the reading of two fundamental documents: the PQC Migration Handbook[21] (December 2024, 2nd edition) from TNO and the PQC Migration Roadmap[22] (May 2025) from the PQC Coalition.

The TNO PQC Migration Handbook stands out for its technical rigour and practical advice. Developed by AIVD, CWI and TNO, it offers a comprehensive approach to post-quantum migration, structured in three phases: quantum vulnerability diagnosis, migration planning and execution. The handbook stands out for its detailed treatment of cryptographic asset discovery and quantum risk assessment. It also addresses standards and offers lessons learned from real-world migrations. However, its technical detail may be intimidating for readers seeking an overview or quick-start guide.

The PQC Migration Roadmap, developed by the Post-Quantum Cryptography Coalition, complements the TNO handbook with a clear framework suitable for a wide range of organisations. It organises the migration process into four categories: preparation, basic understanding, planning and execution, and monitoring and evaluation. The roadmap is particularly effective in its emphasis on organisational preparation, stakeholder engagement and strategic communication, areas that are sometimes overlooked in more technical guides. Its practical checklists make it particularly useful for project managers and decision-makers. Its main limitation is that it is less detailed on technical migration strategies.

The EU Coordinated Implementation Roadmap

The EU's Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography[23] is a strategic recommendation, published in June 2025 by the PQC Workstream within the NIS Cooperation Group, upon request from the European Commission[24]. Its purpose is to guide Member States in preparing for the quantum threat. Unlike technical handbooks, this roadmap focuses on what must be done, not how to do it. The document sets out a milestone-driven approach for all EU Member States, with clear deadlines:

- **By end of 2026:** All member states should have implemented "First Steps", including establishing national PQC transition roadmaps, identifying stakeholders, creating cryptographic asset inventories, mapping dependencies, and launching pilots for high- and medium-risk use cases.
- **By end of 2030:** The transition for high-risk use cases should be completed, with quantum-safe upgrades enabled by default and planning for medium-risk use cases finalized.
- **By end of 2035:** The transition for medium- and low-risk use cases should be completed as far as feasible.

The roadmap is grounded in risk management principles and aligns with EU regulations such as the NIS2 Directive, DORA, and the Cyber Resilience Act. This means that, while this document is aimed at the Member States, its objectives will apply to organizations that have to comply with those EU regulations.

The document emphasizes the need for coordinated action, regular updates, and knowledge sharing at national and EU levels. It also recommends integrating PQC into risk management, supply chain engagement, and awareness programs, but leaves the technical "how-to" details to other guidance.

In summary, the EU roadmap sets out what actions are required and by when, to ensure a synchronized transition to Post-Quantum Cryptography across European Union.

[20] https://www.cryptovision.com/en/resources/download-access-2/

[21] https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

[22] https://pqcc.org/post-quantum-cryptography-migration-roadmap/

[23] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[24] https://eur-lex.europa.eu/eli/reco/2024/1101/oj

Use Eviden Products to facilitate your migration

Eviden products completely align with the above approaches. Most importantly, we provide an end-to-end solution suite guaranteeing for our customers future-proof products. As concrete examples of end-to-end Post-Quantum Cryptography use cases, in close cooperation between our Innovation and R&D departments, Eviden is setting up several proofs-of-concept demonstrating a complete real-life example of Post-Quantum Cryptography implementation. The intention is to showcase typical daily life use cases such as strong authentication and email signature, making use of almost the complete product portfolio[25].

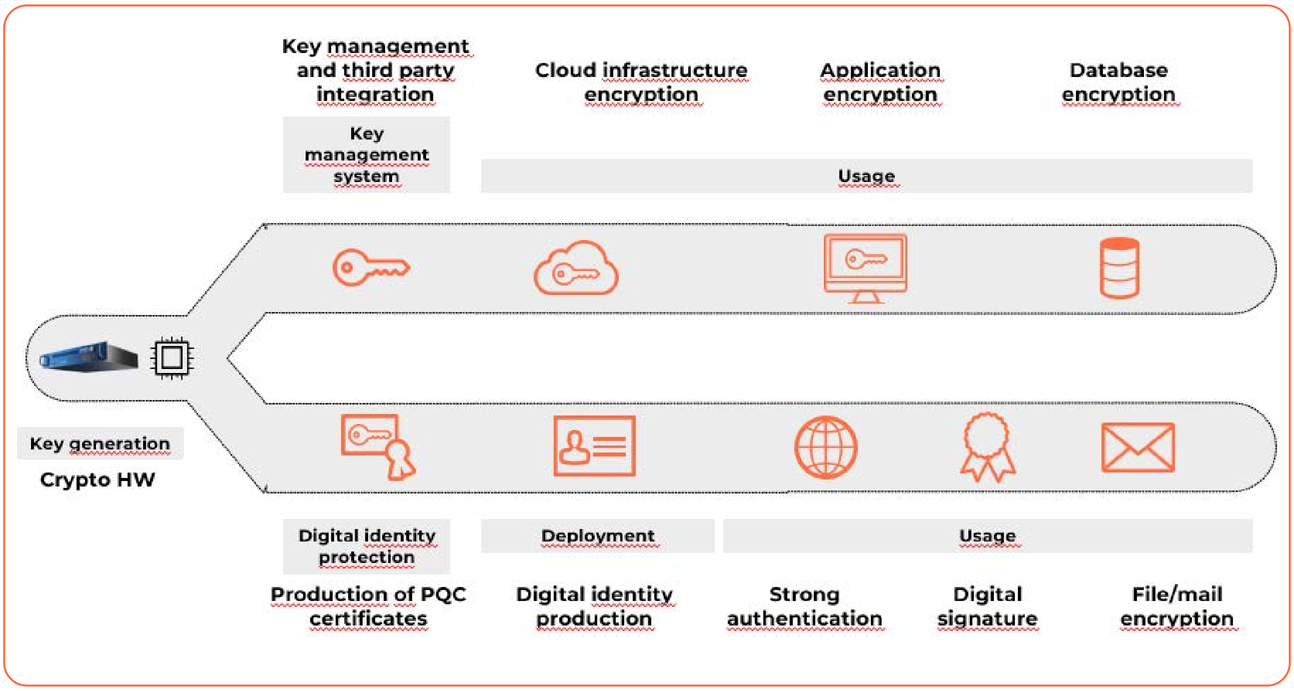


Figure 18: With Eviden Cybersecurity Products you can, in the one hand create , manage and use your PQC keys in Hybrid Cloud deployments while, in the other hand, create, deploy, manage, and use PQC digital identities

Our solutions provide a solid cryptographic foundation to the customers' production environment. By already integrating the NIST standardized post-quantum algorithms, they allow the earliest possible migration. In addition, our customers need to test the post-quantum algorithms at the business application layer. Before moving their applications to production, they'll have to do end-to-end functional tests integrating all the cryptographic layers (including PKI, KMS and HSM, amongst others). Delegating the cryptographic functions to central tools is one of the steps towards crypto agility, without even mentioning resilience, control, cybersecurity strength and certifications. It is worth highlighting that our solutions are available for customer deployment (aka "on premise") as well "as a service". Particularly, you can request access to Eviden's virtual HSMaaS[26] and test the use of highly secure Post-Quantum Cryptography keys in your business applications.

[25] More information: https://www.cryptovision.com/en/post-quantum-cryptography-2/

[26] https://page.eviden.com/pqc-free-trial.html

Appendix 1:

Further information

Links and books

https://www.cryptool.org/en/links-and-books/

NIST competition

Official website: csrc.nist.gov/Projects/post-quantum-cryptography

Lattice-based cryptography

Vinod Vaikuntanathan: Lattices and Cryptography: A Match Made in Heaven.
youtube.com/watch?v=5LGwaICJ5sw

Appendix 2:

Editor:
cv cryptovision (an Eviden company) GmbH, Veronica von Preysing

Source of supply:
cv cryptovision GmbH (an Eviden company) Munscheidstr. 14
45886 Gelsenkirchen, Germany

Published in spring 2026
Layout: Shared Design Center

Concept and editing:
cv cryptovision GmbH (an Eviden company)

Figures:
cryptovision GmbH,

Note: This whitepaper is part of Eviden' public relations efforts.
It is distributed free of charge and is not for sale.

www.eviden.com

cv cryptovision GmbH (an Eviden company)
Munscheidstr. 14
D 45886 Gelsenkirchen

T:+49 209 16724-50 F: +49 209 16724-61

More information:

2026-02-19