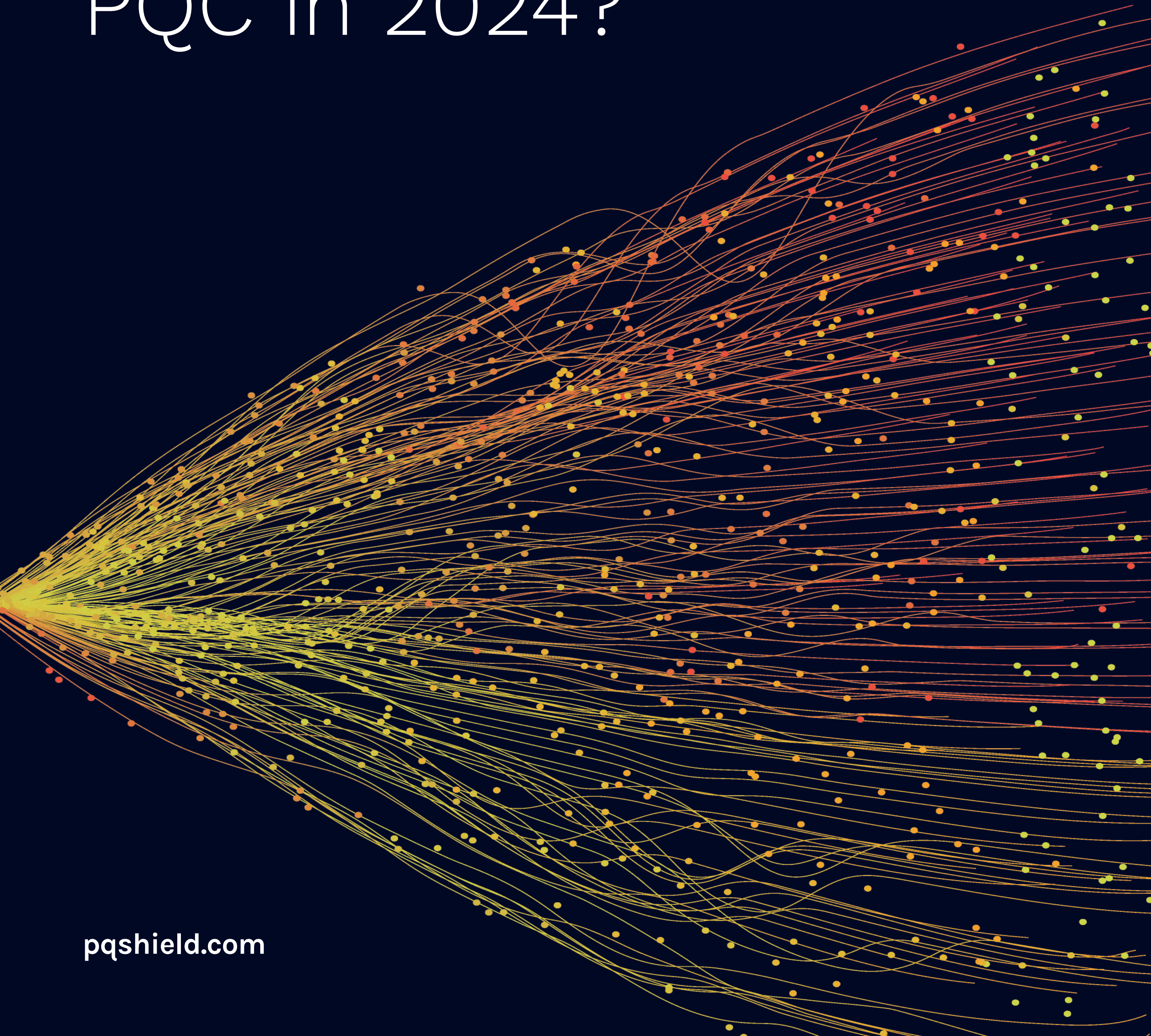
PQ SHIELD

The new NIST standards are here: what does it mean for PQC in 2024?



pqshield.com

Contents

Introduction 3

A brief history of PQC 3

- Early pioneers 4
- The push towards conformity 4
- NIST standardization project 5

The new NIST standards 7

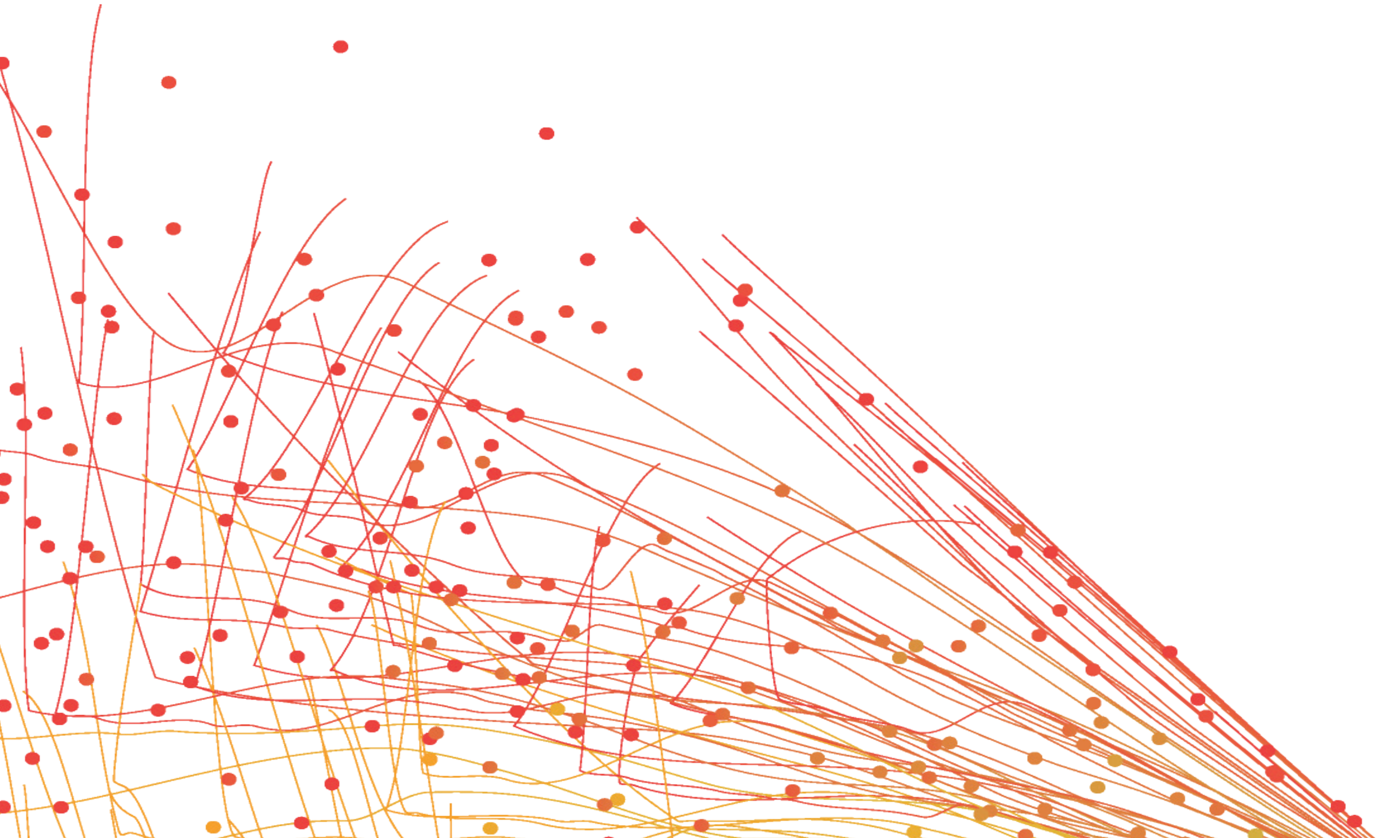
- A quick introduction to Lattices 8
  - FIPS 203 ML-KEM - Post-quantum key exchange 8
  - FIPS 204 ML-DSA - Digital signatures 9
  - FN-DSA - Digital signatures 9
- What about hash-based signature schemes (HBSS)? 10
  - LMS and XMSS 10
  - FIPS 205 SLH-DSA 10

Are there further PQC standards to come? 11

- What happened to the NIST Round 4 candidates? 11
- Additional call for digital signature schemes 12

PQC moves mainstream. What happens next? 13

- PQShield - at the forefront 14



Introduction

In early August, NIST published their finalized post-quantum cryptography (PQC) FIPS standards, the culmination of an eight-year cycle of competitive submission, research and analysis.

This long-awaited announcement marks a significant milestone in the history of PQC. It's set to impact the cryptography deployed in every industry, affecting everything from machines transferring data across a network, to online financial transactions, hardware infrastructure, and military devices. As a result of announcement, chips, devices, software applications, and cryptographic components in supply chains will all now need to be PQC-compliant with the framework of standards announced.

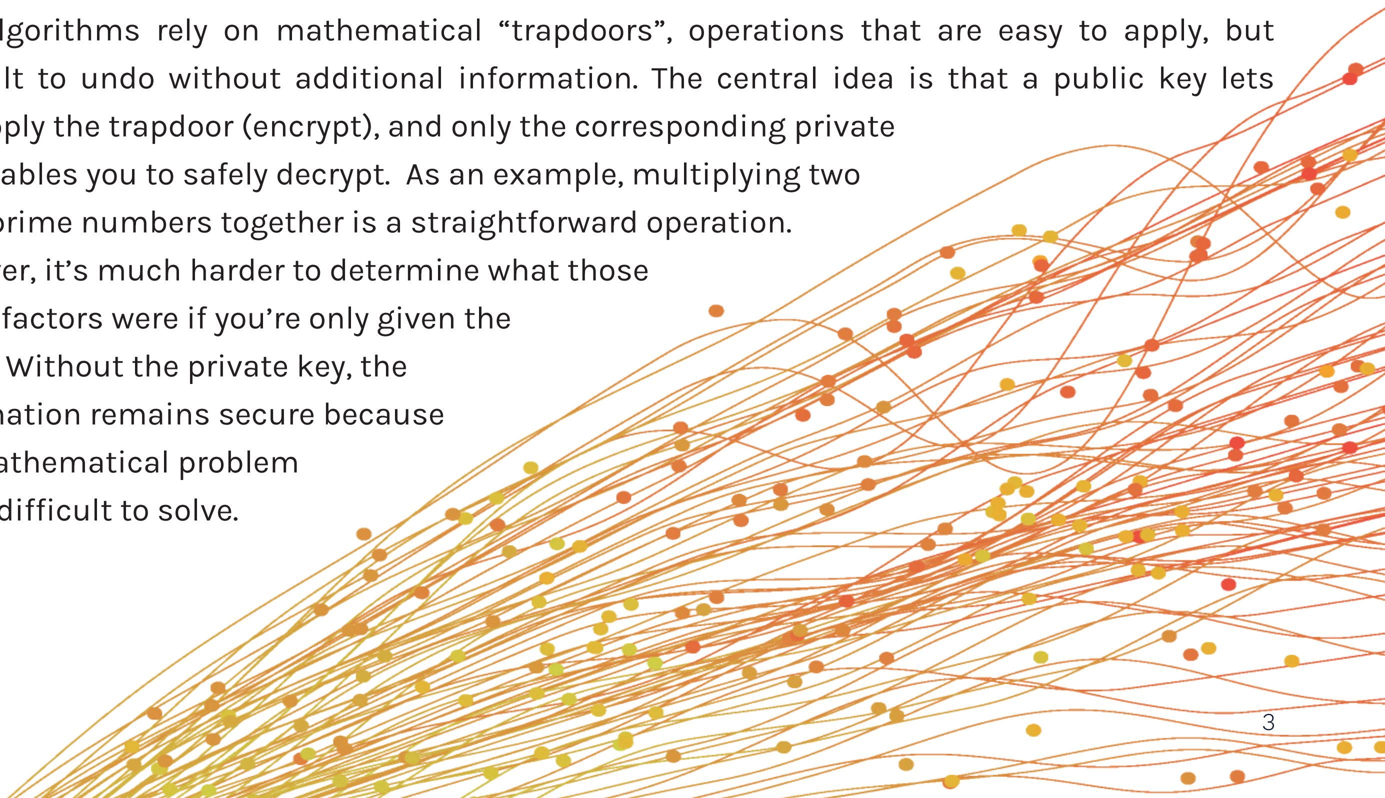
In this paper, we take an in-depth look at the FIPS standards for post-quantum cryptography. *What are the selected algorithms, and why were they chosen? How did the world wake up to the threat of quantum computing? What's the view of companies like PQShield, working with government and security agencies around the world? And importantly, what happens next?*

To answer these questions, we should take a look back at the story of post-quantum cryptography.

A brief history of PQC

One of the mechanisms behind the way we communicate today is the use of Public Key Cryptography (PKC). PKC is an idea that's been around for a long time. In fact, for decades, it has been the primary method for protecting our digital information.

PKC algorithms rely on mathematical "trapdoors", operations that are easy to apply, but difficult to undo without additional information. The central idea is that a public key lets you apply the trapdoor (encrypt), and only the corresponding private key enables you to safely decrypt. As an example, multiplying two large prime numbers together is a straightforward operation. However, it's much harder to determine what those prime factors were if you're only given the result. Without the private key, the information remains secure because the mathematical problem is too difficult to solve.



Early pioneers

In the 1990s, mathematicians began developing new techniques to figure out how to solve some of these 'hard' problems. Peter Shor, in particular, worked on multiple algorithms that were, in theory, able to solve the prime factorization problem, and others. Shor's algorithms were major breakthroughs, showing for the first time, a path towards breaking currently-deployed public-key cryptography. The only issue was that, in order to run those algorithms, a computer would have required a vast amount of processing power - far more than was physically possible for any known machine.

At the time, the basic idea of a quantum computer was not new. The physicist Richard Feynman had proposed the idea of using quantum systems to simulate physical processes in the early 1980s, and throughout that decade there had been a number of elegant models for quantum computation. In 1985, British physicist, David Deutsch proposed the idea of a quantum Turing machine - showing that quantum computers could perform any computation that classical computers could, but in a way that could be efficiently optimized for certain problems.

Quantum computers would be, in theory, much more efficient than classical machines at specific tasks. They rely on quantum effects in subatomic particles such as electrons. Rather than electrical signals that can generate sequential 1s and 0s, a quantum machine uses the superposition of states to open up a huge increase in its ability to perform calculations.

By the mid 1990s, it was becoming evident that a real-world, practicable quantum computer could be extremely effective. As we know today, these machines might be able to accelerate computations in chemistry, engineering, financial-modeling, weather prediction, and countless more applications. Theoretical breakthroughs continued to show the huge potential of quantum computing, both its opportunities, and its power to threaten traditional cryptographic methods.

The growing realization that a quantum computer might be able to use techniques like Shor's algorithms, and break cryptographic protocols, led to a rapid acceleration in the development of so-called quantum-resistance. It wasn't long before this field soon became known as 'post-quantum' cryptography.

The push towards conformity

As we've seen, even in the 1990s and early 2000s, the potential threat of a Cryptographically Relevant Quantum Computer (CRQC) was evident.

While development went into the incredible potential of quantum computing, even further effort was applied to finding new techniques that could defend against a CRQC.

Work in the late 1990s, for example, set the framework for lattice-based cryptography schemes, among others. There was a renewal of interest in cryptosystems based on mathematical problems considered sufficiently difficult. Existing cryptosystems included those based on error-correcting codes, hash-based signatures, isogenies between elliptic curves, and multivariate equations, while new families of cryptosystems, based on isogenies between elliptic curves or multiparty computation, emerged.

As with many technological developments, leaps forward in post-quantum cryptography rarely took a connected or predictable path. Many academics, mathematicians and cryptographers worked on multiple streams of fast-paced research, and it became clear that eventually these ideas would need to coalesce.

Inevitably, interest in standardizing PQC algorithms grew more acute.

What's more, the world of the early 2000s was now rapidly becoming dependent on digital security, and it added urgency to the effort of drawing these streams into one river. The roadmap to quantum resistance was quickly tightening - and a standardized set of verified PQC algorithms was now not only a sensible way forwards for academics, but a necessity for everyone.

NIST standardization project

That's why, in 2016, the United States National Institute of Standards and Technology (NIST), launched the formal process to develop and standardize a set of post-quantum algorithms, submitted by the post-quantum cryptography community.

The aim was to evaluate various PQC candidates for two primitives:

- **key agreement** (which includes key exchange, public key encryption and key encapsulation mechanisms, or KEMs)
- **digital signatures**

After this evaluation phase, a minimum of one algorithm for each of these primitives would be selected, which would be "capable of protecting sensitive government information well into the future, including after the advent of quantum computers." (NIST)

Note: US federal standards have an impact far beyond the United States. FIPS, the official standards released by NIST, influence industry standards, global cybersecurity practices, and international trade, and they have become the benchmark for best practice, interoperability and compliance around the world. For example, current NIST standards include the AES symmetric encryption algorithm and the SHA family of hash functions.

The standardization project would become the focus of international collaboration. As a consequence of the NIST competition, there have been many breakthroughs in cryptology and research over the last decade, and the project significantly increased the maturity of the field.

By November 2017, NIST had received 69 valid submissions for potential PQC algorithms, and began the process. Proposals were held up to rigorous scrutiny by the community, and rejected if unable to maintain the high level of security and performance required.

The second round of NIST proposals was conducted through 2020-2021, and this time the evaluation resulted in just 15 finalists and alternatives.

In 2022, after three rounds of candidates, NIST proposed the following algorithms for standardization.

- **ML-KEM** (Kyber) Module-Lattice-Based Key-Encapsulation Mechanism Standard
- **ML-DSA** (Dilithium) Module-Lattice-Based Digital Signature Standard
- **SLH-DSA** (SPHINCS+) Stateless Hash-Based Digital Signature Standard
- **FN-DS**A (FALCON) Fast Nominative Digital Signature Algorithm

These algorithms represent the best of both hash-based and lattice-based encryption techniques and, over the course of the last two years, have been subjected to rigorous scrutiny.

Finally, in the summer of 2024, NIST have progressed these Round 3 candidates, and as of August, have published the first tranche of standardized post-quantum algorithms.

The new NIST standards

The selected NIST standards, FIPS 203, FIPS 204, and FIPS 205, are the result of submissions that have shown the highest level of security provable with an acceptable performance.

Algorithm	Standard	AKA	Description/usage
Module-Lattice-Based Key-Encapsulation Mechanism Standard	FIPS 203 ML-KEM	CRYSTALS-Kyber	Key Exchange
Module-Lattice-Based Digital Signature Standard	FIPS 204 ML-DSA	CRYSTALS-Dilithium	Digital Signatures
Stateless Hash-Based Digital Signature Standard	FIPS 205 SLH-DSA	SPHINCS+	Hash-based Signatures

It is these algorithms that have now been finalized, and published as the post-quantum cryptography standards.

In addition, the fourth digital signature algorithm is expected to follow in due course.

- **FN-DSA** (FALCON) Fast Nominative Digital Signature Algorithm

These algorithms have been chosen for their robustness and usefulness in a variety of situations, and are a collection of both lattice-based and hash-based post-quantum secure techniques that cover key agreement and digital signatures. While hash-based schemes have been around for a long time, lattice-based cryptography is a relatively new but important field.

A quick introduction to Lattices

The technology behind lattice-based schemes is based on the idea of creating hard mathematical problems that arise from lattices. As with classical PKC, these problems must be easy to apply, but extremely difficult to undo.

A lattice is a regular grid of points in space that's formed by vectors. For example, the vectors (0,1) and (1,0) form a regular square grid that can be repeated to form a simple lattice. While this is perhaps the simplest lattice of all (fig 1), combining more complex vectors produces much more complicated lattices - especially when those vectors are combined in multiple dimensions.

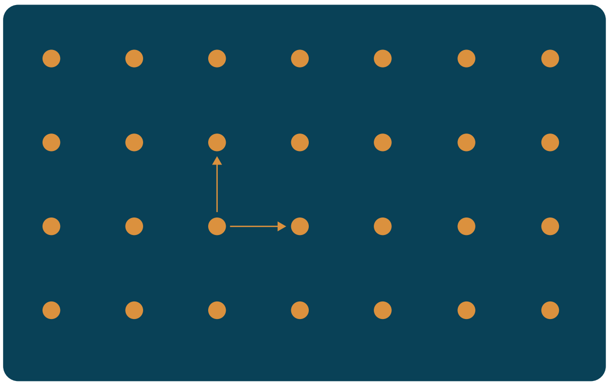


Figure 1. A simple lattice formed by the vectors (0,1) and (1,0).

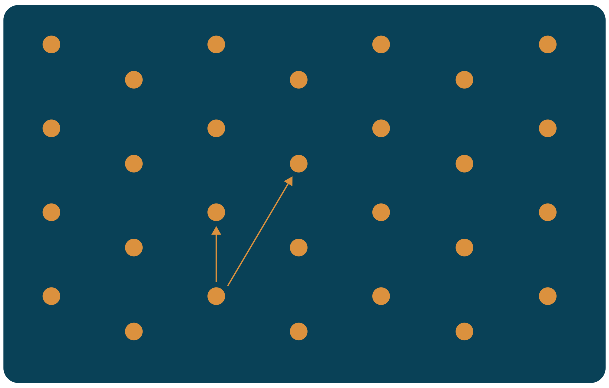


Fig 2. Lattices can be much more complex, and can also have more than two dimensions based on any number of basis vectors.

FIPS 203 ML-KEM - Post-quantum key exchange

As with classical cryptography, FIPS 203 ML-KEM relies on the use of public and private keys. A sender uses the recipient's public key to create a secure ciphertext containing a shared secret. The recipient then uses their private key to open the package and retrieve the message.

With ML-KEM, you could think of the recipient's public key as a point on a lattice that's known. Meanwhile, the private key could be the secret path or vector that's used to find that point.

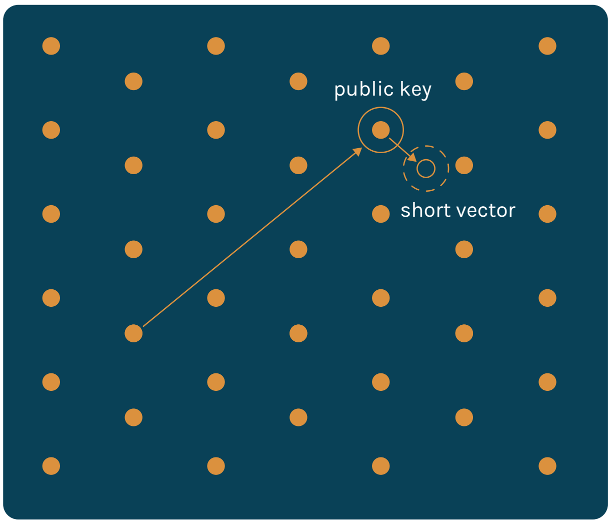


Fig 3. Lattice-based mathematical problems are difficult to solve, but adding a noise vector leverages the so-called 'Learning With Errors assumption', making the problem even harder.

The sender uses the public key to disguise a secret, using the mathematical properties of the lattice. This can be done by adding a short 'noise' vector close to the public point, but one that's indistinguishable from random lattice points nearby. Without knowing the private key (the real path from the starting point), figuring out the starting point is extremely difficult, even for a quantum computer using mathematical techniques.

FIPS 204 ML-DSA - Digital signatures

Similarly, FIPS 204 ML-DSA (Dilithium) is an algorithm used for creating digital signatures. The signer uses their private key to sign a message, while anyone can use the public key to assess the authenticity of the signature.

Forging a signature without knowing the private key essentially requires finding a short solution to a specific linear system. While solving a linear system is easy in general, constraining the solution to be short makes it difficult - exponentially so when increasing the dimensions.

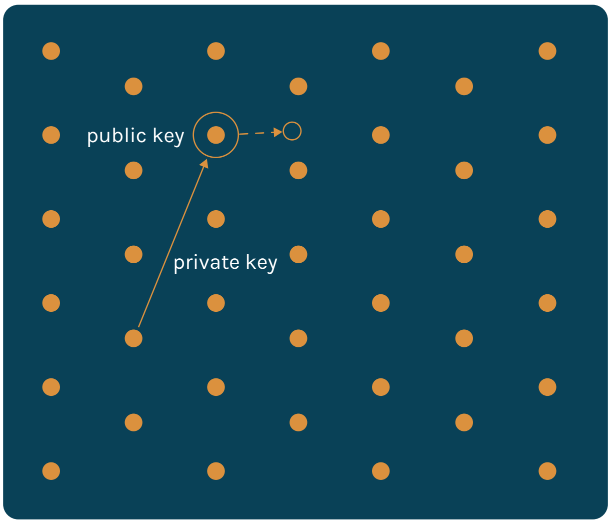


Fig 4. As with ML-KEM, the 'Learning With Errors' problem is used in ML-DSA for a short vector, in combination with hash functions, to make the lattice problem more difficult to solve, particularly in multiple dimensions.

FN-DSA - Digital signatures

FN-DSA (FALCON) uses advanced lattice mathematics to create secure digital signatures. Similarly to ML-DSA, forging a signature requires finding a short solution to a linear system. The signing procedure uses the private key to solve this linear system, and leverages a technique called Gaussian sampling in order to avoid leaking information about the private key in the process.

The scheme is designed to be quick, using fast verification, making it suitable for high-speed applications. FN-DSA also produces small signatures, making it efficient in terms of storage and transmission.

What about hash-based signature schemes (HBSS)?

Hash-based schemes use hash functions to create quantum-safe digital signatures. Typically, these schemes involve a large number of one-time signatures that are aggregated in a data structure as a single public key. The security of hash-based signatures is much better understood than that of lattice-based techniques, although the signature size can be large compared to other signature schemes. They can be viewed as a more conservative option, in cases where the cost can be afforded.

LMS and XMSS

LMS and XMSS are cryptographic signature schemes that are based on the complexity of hash functions and on the structure of binary trees - data structures which are used to generate public and private keys. These schemes are also stateful, which means they keep track of the keys used for signing, to ensure each key is used only once.

Both LMS and XMSS are considered post-quantum secure, and are suited to environments where long-term security is crucial - for example, software updates, secure boot in devices with a long shelf-life, and digital certificates.

Note: These are not part of the latest announcement, as they have previously been formalized in NIST SP 800-208.

FIPS 205 SLH-DSA

FIPS 205 SLH-DSA (SPHINCS+) is a hash-based signature scheme (HBSS) now standardized by NIST as FIPS 205. It relies on the hardness of the reliable, quantum-resistant hash functions, SHA-2 and SHA-3. SLH-DSA leverages this to generate digital signatures, applying them through data structures to then manage the keys that are output. A data structure (such as a Merkle tree) manages and optimizes the output values, allowing SLH-DSA to handle arbitrary length messages.

SLH-DSA is considered robust, as it relies on well-understood hash-functions, and can be tweaked and adjusted for different security and performance requirements. As opposed to LMS/XMSS, SLH-DSA has larger signatures, but is also stateless rather than stateful. This means that the scheme does not need to manage the state of keys used for signing, and in effect, this makes security simpler and easier.

Are there further PQC standards to come?

What happened to the NIST Round 4 candidates?

In 2022, NIST also selected other candidates for potential standardization. These algorithms were selected to diversify the mathematical assumptions used, and add a wider, more robust range to the lattice-based algorithms.

These schemes are based on error-correcting codes, such as:

- **BIKE** (Bit-flipping Key Encapsulation)
- **HQC** (Hamming Quasi-Cyclic)
- **Classic** McEliece

Being based on error-correcting codes, these schemes would not be affected in the (unlikely) event that new attacks on lattice cryptography are found. The public key and/or ciphertext sizes are larger than those of ML-KEM, which makes them less generally applicable - Classic McEliece especially, has extremely large public keys (261kB). McEliece actually dates back to the 1970s, and is considered a very secure and conservative option.

Additionally, the remaining scheme was based on supersingular isogenies, a mathematical technique based on the complexities of elliptic curves:

- **SIKE** (Supersingular isogeny key encapsulation)

Unfortunately, in the summer of 2022, a practical attack was discovered which catastrophically broke SIKE. Meanwhile, BIKE, HQC, and Classic McEliece remain as candidates to potentially complement the NIST standardized algorithms.

You can find further information on the NIST status report here:
https://csrc.nist.gov/pubs/ir/8413/upd1/final

Additional call for digital signature schemes

NIST also issued an additional request for digital signature proposals. Primarily, the interest is in general-purpose signature schemes that are not lattice-based (or outperform existing schemes which are) to help widen the range of algorithms considered. There's a growing interest in signature schemes that have short signatures and fast verification. Evidently, the need is for signature verification to be highly performant, such as would be needed for systems processing real-time communication, or high-frequency trading.

40 candidates were deemed to be complete and proper, according to the specifications [1], and now include code-based, isogeny, multivariate and some lattice that might outperform the likes of Dilithium and SPHINCS+, plus others. You can find much more information about post-quantum signatures here[2].

[1] https://www.nist.gov/news-events/news/2023/07/nist-announces-additional-digital-signature-candidates-pqc-standardization

[2] https://pqshield.github.io/nist-sigs-zoo/

PQC moves mainstream. What happens next?

There's little doubt that the NIST announcement is significant - not just for the world of post-quantum research and development, but for every cryptographic component in the world's technology supply chain.

Adoption of the new standards is likely to be both fast and widespread, reiterated by guidance from security bodies such as the NSA, with equivalent European requirements from Germany's BSI, France's ANSSI, NCSC in the UK, and others. This quantum shift towards compliance is likely to continue, with both regulation and legislation as part of the framework. In fact, the US Federal Government has already reinforced the strategy for PQC migration outlined in the Quantum Computing Preparedness Act, by focusing agencies on the transition of critical systems to the new schemes.

Note: For those agencies, the NIST announcement also triggers a 90-day deadline to propose a timeline for the removal of quantum-vulnerable cryptography. Memo NSM-10 (May 2022) also allows for the procurement of commercially available quantum-resistant solutions, at the point of NIST publication.

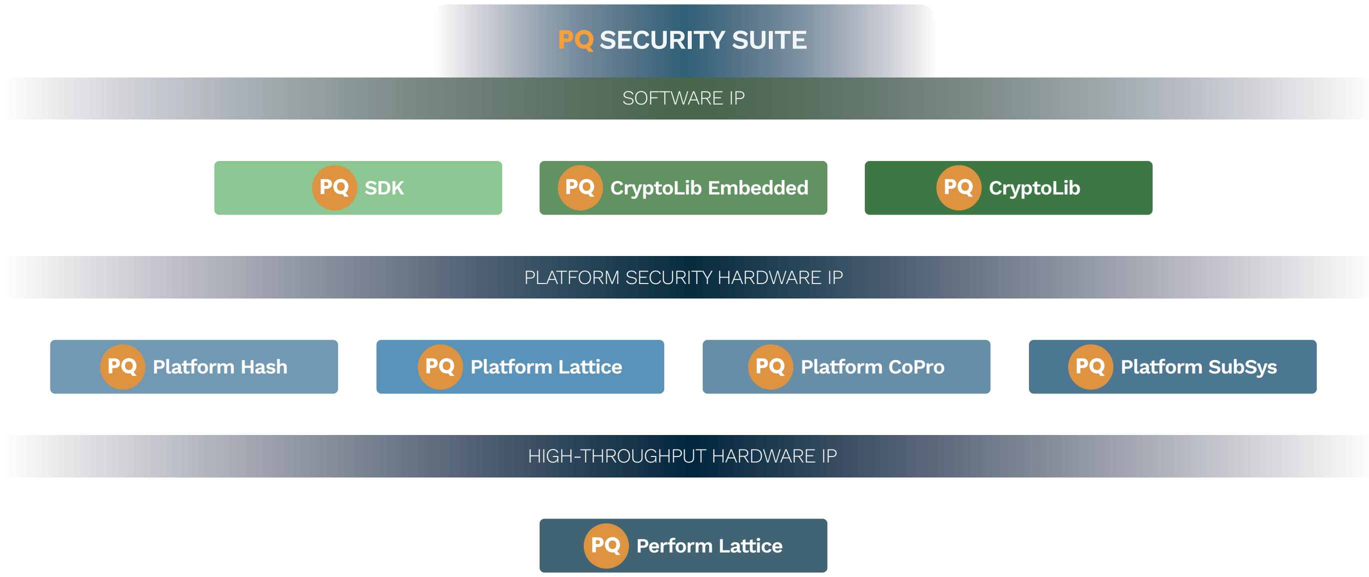
Industry standards bodies will certainly follow, including ISO, governing the expected post-quantum certification in manufacturing and design, plus specific requirements in automotive, telecoms, defense, and many other sectors.

Meanwhile, NIST continues the journey to widen the standards, particularly with ideas that are not necessarily restricted to lattice-based schemes, as mentioned above. It will be fascinating to see what new technologies emerge through the ongoing process, as well as the inevitable compliance of organizations around the world. With the threat of harvest-now-decrypt-later attacks, the effort is more crucial than ever, and NIST's announcement is almost certainly a historic inflection point in the takeup of PQC around the world. There is no doubt: we are in the quantum age.

PQShield - at the forefront

PQShield was founded in 2018, with the aim of developing quantum-safe technology, and our team of experts have been co-authors of each of the NIST PQC standards. We've focused our expertise into building a world-class security suite of configurable, flexible PQC products that use these algorithms - both in hardware and software IP.

What's more, we've spent a lot of time innovating solutions that are designed to be fast and secure implementations of these algorithms. We believe our configurable suite of security solutions achieves this, matching the requirements of international standards bodies as well as giving exceptional performance in the field.



PQ SECURITY SUITE

SOFTWARE IP

PQ SDK

PQ CryptoLib Embedded

PQ CryptoLib

PLATFORM SECURITY HARDWARE IP

PQ Platform Hash

PQ Platform Lattice

PQ Platform CoPro

PQ Platform SubSys

HIGH-THROUGHPUT HARDWARE IP

PQ Perform Lattice

It's our goal to help update the legacy components of the world's technology supply chain, and our belief that we can protect organizations from the threat of quantum computing, and beyond.

PQ SHIELD

Ready to learn more?

Get in touch: contact@pqshield.com | www.pqshield.com

PQShield Ltd
Oxford
Prama House
267 Banbury Road
Oxford
OX2 7HT

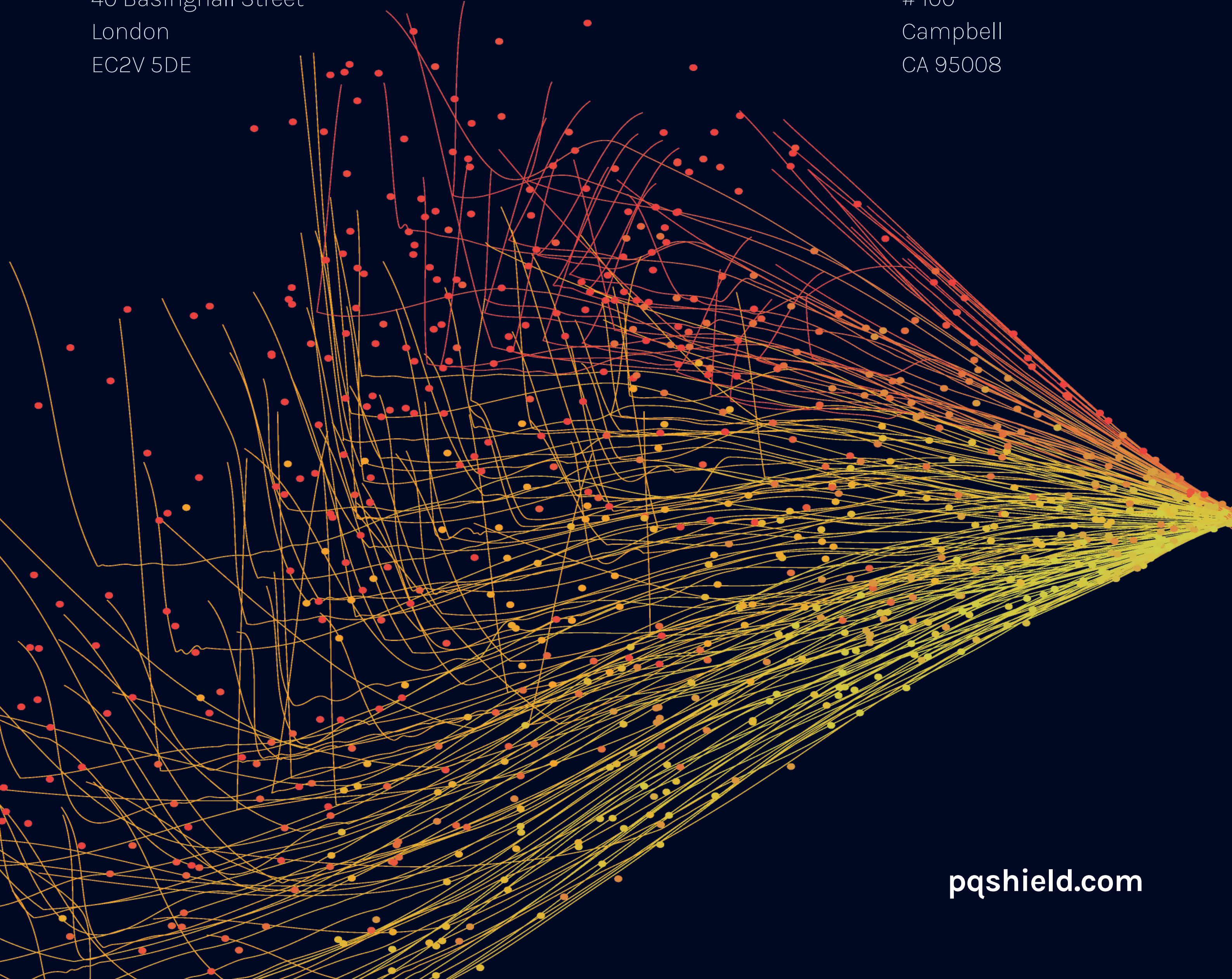
London
City Tower
40 Basinghall Street
London
EC2V 5DE

PQShield SAS
Paris
8 Rue des Pirogues de
Bercy
Paris
75012

PQShield B.V.
Amsterdam
Keizersgracht 62
1015CS
Amsterdam

PQShield Inc.
New York
228 East 45th Street
Suite 9E
New York
NY 10017

California
900 E Hamilton Ave
# 100
Campbell
CA 95008



pqshield.com