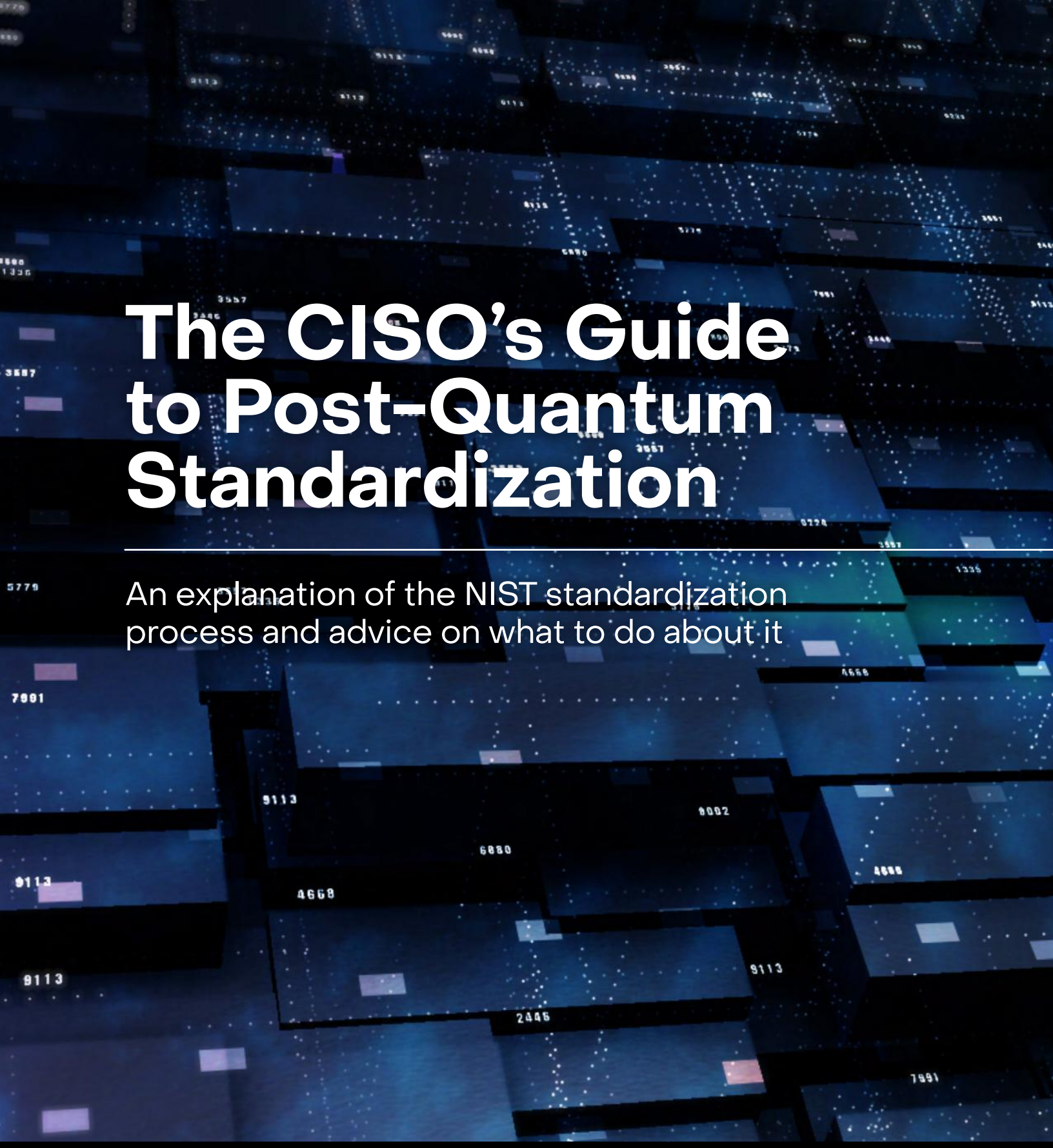


The CISO's Guide to Post-Quantum Standardization

An explanation of the NIST standardization process and advice on what to do about it

QUANTUM ORIGIN

QUANTINUUM

HAVE YOU HEARD ABOUT Y2Q?

What's so special about Sunday, April 14, 2030?

The Quantum-safe Security Working Group of the Cloud Security Alliance (CSA) chose that date to represent "Y2Q," also known as "Q-Day" – the moment secure IT infrastructure becomes vulnerable to the threat of a fault-tolerant quantum computer running Shor's algorithm. This algorithm, discovered in 1994 by American mathematician Peter Shor, will break many of the cryptographic algorithms we rely upon today, including RSA, elliptic curve cryptography, and Diffie-Hellman key exchange.

Although the date is arbitrary, the principle is important. At some future date, common encryption standards will become vulnerable to the threat of quantum computers. The CSA's insight is also important. Until we agree on a deadline, it is easy to ignore the threat.

With a deadline identified, a worldwide effort to prevent Y2Q from threatening encryption is under way. One of the organizations leading that effort is the National Institute of Standards and Technology (NIST). This booklet outlines everything a CISO needs to know about that effort and what it means for their organization's cybersecurity strategy—now and in the future.

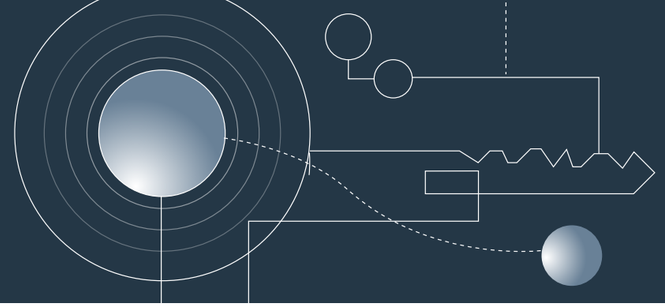
CONTENTS

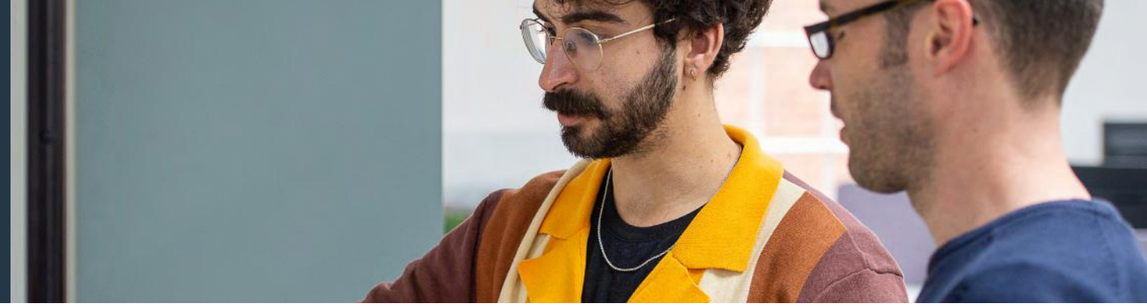
The National Institute of Standards and Technology (NIST) is currently defining which cryptographic algorithms are going to save us from certain doom. In this guide is everything a CISO needs to know about this topic, including:

- The nature of the threat
- An overview of the algorithms and their properties
- What happens next during the NIST process
- What you should be doing next

QUANTINUUM

QUANTUM ORIGIN





Why We Need Post-Quantum Algorithms

Many of the encryption systems we use today are based on a special type of mathematical problem. These problems are easy to solve in one direction, but intractable to solve in the other direction, unless you know some secret data — which we call the secret key.

As an example, RSA is a popular algorithm for encrypting internet data and for digitally signing transactions. RSA relies on a math problem that involves multiplying very large numbers, which is trivial for a traditional computer to compute. However, the reverse process is effectively impossible. If someone gives you the final result and asks you to calculate which two numbers were multiplied together to produce it, the calculations would take thousands of years on the most powerful classical computers existing today.

A new type of computer is emerging which will change this dynamic. Quantum computers are based on the surprising behavior of quantum mechanics, which is quite unlike anything we experience in the world around us. As quantum computers mature over time, they will be able to solve problems we cannot conceive of approaching using today's classical computers.

The challenge of breaking large numbers into their component parts (or factors) is something quantum computers will be able to achieve in as little as 10 years' time. This means, an attacker with a powerful quantum computer could read data encrypted by an RSA public key or forge transactions signed by an RSA private key. This completely breaks the bedrock of current cybersecurity systems.

Worse, a category of attack known as "hack now, decrypt later" may already be under way. Data is continuously being transmitted around the world using quantum-vulnerable algorithms. Attackers who record this information can retrospectively decrypt it in the future using quantum computers. For any organization that shares data with a long sensitivity lifespan — such as government defense agencies and contractors, healthcare providers and financial institutions — this is a real concern.

To defend against these threats, a race has been under way for six years to find new encryption systems — known as "post-quantum" algorithms — for which there are no known quantum attacks. The selection process has been managed and whittled down by NIST from more than 60 potential candidate algorithms to a small group for standardization.

The Post-Quantum Algorithms

In this section, we will explore how these new post-quantum algorithms compare to the systems we use today.

Post-quantum algorithms cannot be used for both encryption[1] and data signing. Instead, they are used for only one task or the other. This means we will be replacing a single algorithm, such as RSA, with two separate algorithms.

Each post-quantum algorithm also has three different security levels defined (SL1, SL3 and SL5). These levels are very similar to key sizes in today's algorithms. Much like 4096-bit RSA keys are stronger than 1024-bit RSA keys, SL5 is stronger than SL3 and SL1. However, that increased security comes at a cost. SL5 keys are typically larger to store and result in slower computations.

Let's walk through the candidate algorithms in detail to see how they compare.

Encryption Algorithms

Classic McEliece

Classic McEliece is one of the oldest and most studied algorithms in the standardization process. The cryptographic properties of this algorithm have been studied for decades, giving a high degree of confidence it will remain resistant to quantum attacks in the future.

The downside of Classic McEliece, and perhaps the reason there might be some surprise if it is selected, is that it has very large keys that are very slow to generate. As you will see in the summary table below, public keys for Classic McEliece range from 256KB to a whopping 1.3MB, which is orders of magnitude larger than today's keys.

[1] Strictly speaking, the post-quantum algorithms are key encapsulation mechanisms (or KEMs), and can't be used for arbitrary data encryption. KEMs use a public key to generate some new secret shared data, as well as a ciphertext which can be decrypted to the same secret data by the corresponding private key.

Although this sounds more exotic than encryption, in practice this is exactly how most asymmetric cryptography is used today: asymmetric operations are much more expensive than AES, and in general they are only used just enough to establish a shared AES key.

Fitting this algorithm into existing standards, like Transport Layer Security (TLS), will be challenging. Along with the large and slow-to-generate keys, the actual cryptographic operations are among the slowest of the finalists.

With that said, key generation speeds are still better than large RSA keys, and the encoding scheme allows for very short ciphertexts, using only 120–240 bytes to establish a standard Advanced Encryption Standard (AES) 256 key; smaller than 2048-bit RSA.

Classic McEliece is based on a mathematical problem family known as error-correcting codes. The encryption operation involves transforming data to introduce a specific number of errors. The decryption operation removes those errors but is only practically possible if you have access to the private key.

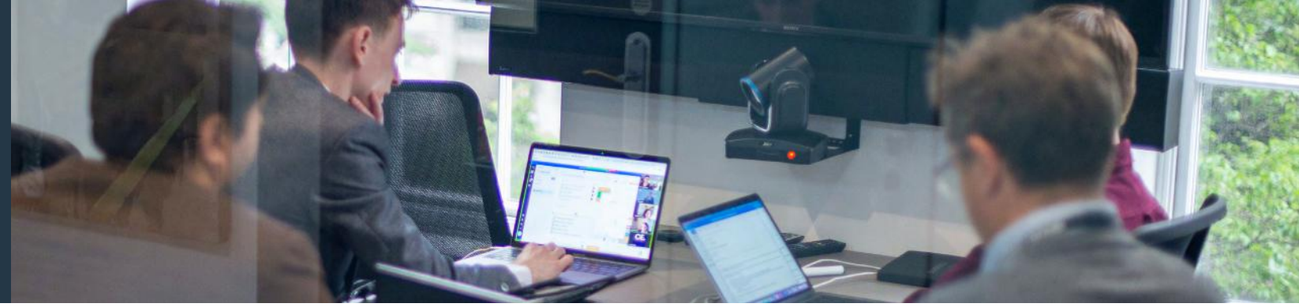
CRYSTALS-KYBER

The KYBER algorithm is "lattice-based," meaning its difficulty relies on a class of mathematical problems around finding the shortest vectors between points in a high-dimensional lattice. This type of problem is believed to be quantum-resistant, and many of the candidate algorithms are lattice-based variations of this.

For technical reasons, when implementing KYBER it is relatively difficult to avoid side-channels that leak key data, especially in hardware implementations. There may be further adjustments to the algorithm to mitigate this.

KYBER has reasonable key sizes, although still much larger than current elliptic curve keys. KYBER secret keys are between 1.6 KB and 3.1KB, with public keys around half that size. This means they should easily fit within most existing cryptographic protocols outside of constrained IoT environments. Ciphertext length for a standard 32-byte AES-256 key ranges from 768 bytes to 1.5KB.

Compared to the other candidates, KYBER has a speed advantage. It is by far the fastest candidate for generating keys and decapsulation, both of which are several times faster than the next leading candidate, NTRU.



NTRU
NTRU is another lattice-based algorithm based on an underlying problem that has been studied for many years. In fact, the NTRU algorithm was originally patented, but the patents have since expired.

The sizes of NTRU keys are larger than we are used to with existing algorithms but should pose no major problems for cryptographic protocols outside of constrained IoT environments. Secret keys range from 935 bytes to 2.3KB, and public keys are slightly smaller.

One downside of NTRU is the length of the ciphertexts it produces. Securely sending a standard 256-bit AES key requires up to 1.8KB at the highest security level, which is more than three times as large as RSA-4096.

NTRU is one of the fastest candidates for encapsulation and decapsulation operations, although key generation is relatively slow compared to the other finalists. Nevertheless, the key generation is still many orders of magnitude faster than RSA.

SABER
SABER is another lattice-based key encapsulation mechanism based on a problem called “learning with rounding” that is probably as hard as well-known lattice problems.

As with KYBER, it is difficult to avoid side-channels during implementation of this algorithm. We anticipate there may be further changes to the algorithm to mitigate this over time.

SABER offers reasonable key sizes, with private keys between about 1.5KB and 3KB, and public keys less than half that. Ciphertext sizes for a standard 256-bit AES key range from 736 bytes to 1.4KB.

Unfortunately, SABER is one of the slowest of the finalists at each security level, beating only McEliece.

Signature Algorithms
Digital signature algorithms are used to sign transactions, proving the identity of the sender and the fact that the data is unchanged.

CRYSTALS-DILITHIUM
Dilithium is a lattice-based signature scheme, based directly on the hardness of particular lattice problems.

Dilithium has large key sizes, with secret keys ranging from 2.5–4.8KB and public keys about half the size. The signature size is similarly large, between 2.4KB and 4.6KB. While this is still easily achievable on the modern Internet, it will be a challenge in constrained environments that require short messages, such as low-bandwidth IoT devices.

One of Dilithium’s significant advantages is its speed — it is by far the fastest finalist for all three operations (key generation, signing, and verification) by an order of magnitude or more, and even faster than the Elliptic Curve Digital Signature Algorithm (ECDSA) over most curves.

Falcon
Falcon is a lattice-based signature scheme built off a similar problem to the NTRU KEM candidate. Unusually, Falcon only has two variants, one for Level 1 and Level 5.

Falcon has the smallest key sizes of the signature finalists, with secret keys of 1.2KB or 2.3KB and public keys of 897 bytes or 1.7KB respectively. Its signatures are also relatively small amongst the finalists, at 690 bytes or 1.3KB, about a quarter the size of Dilithium’s signatures.

Although Dilithium is much faster, Falcon still remains relatively performant; on most hardware it can still perform as fast as ECDSA, so it is easy to see how NIST decided the smaller signature size was worth the tradeoff.

Rainbow
Rainbow is a signature scheme based on multivariate polynomials, whose hardness relies on the difficulty of solving large systems of equations. The public key is the entire system of equations, while the private key encodes ways of transforming the equations so that it is easy to compute solutions of a particular form. A signature is then a solution to this system of equations that produces the starting message.

This approach results in different key and signature sizes than the other finalists. The resulting signature size is very small (between just 66 and 212 bytes depending on the security level) at the cost of massive public keys. The original uncompressed Rainbow public keys range from 161KB up to 1.9MB, with private keys just slightly smaller. This uncompressed scheme is around the middle of the pack for the speed of signing and verifying messages.

In Round 2, two additional key encodings were introduced, one which compresses the public key with a clever encoding, and another which also compresses the private key—storing only the original seed value used to generate the keys. These variants result in slightly smaller public keys (60–536KB) and the latter in an extremely small private key size of only 64 bytes. However, using these compressed keys requires extra computation to recover the 'real' key values, making these variants substantially slower.

Rainbow was in the news for the wrong reason in February 2022 following the publication of a paper entitled "Breaking Rainbow Takes a Weekend on a Laptop."[2] As the name suggests, the paper demonstrated an effective attack on the Rainbow algorithm, which resulted in the lowest security level (SL1) being broken.

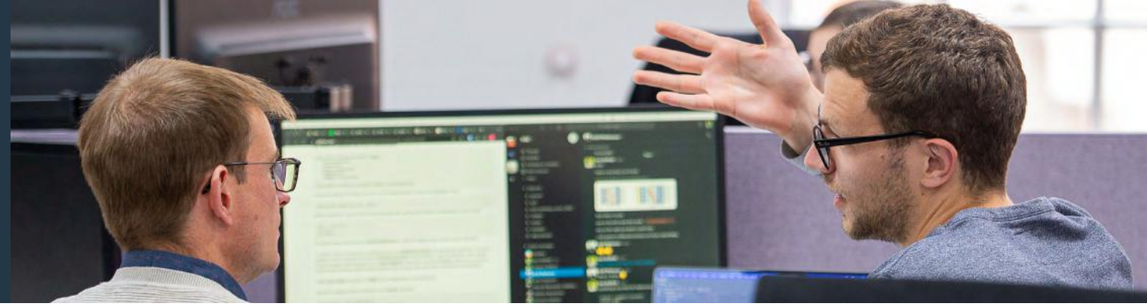
Because of this attack, it is unlikely Rainbow will be selected as a finalist. Although the attack could be thwarted by increasing all of the security parameters, this serves only to make the algorithm less attractive to use, due to larger key sizes and poorer performance.

[2] https://eprint.iacr.org/2022/214

Summary of Algorithms

The table below summarizes the core properties of the candidate algorithms. The output size, for KEMs, is the size of an encrypted 256-bit AES key.

Algorithm	Type	Family	Public Key Size	Ciphertext / Signature Size
Classic McEliece	KEM	Error correcting codes	256Kb - 1.3Mb	0.1Kb - 0.2Kb
CRYSTALS-KYBER	KEM	Lattice-based	1.6Kb - 3.1Mb	0.8Kb - 1.5Kb
NTRU	KEM	Lattice-based	0.9Kb - 2.3Kb	0.7Kb - 1.8Kb
SABER	KEM	Lattice-based	1.5Kb - 3Kb	0.7Kb - 1.4Kb
CRYSTALS-DILITHIUM	Signature	Lattice-based	2.5Kb - 4.8Mb	2.4Kb - 4.6Kb
Falcon	Signature	Lattice-based	1.2Kb - 2.3Kb	0.7Kb - 1.3Kb
Rainbow	Signature	Multivariate	60Kb - 1.9Mb	0.07Kb - 0.2Kb



Next Steps in the NIST Standardization Process

Announcing the winning algorithms will not be the final stage in the NIST post-quantum standardization process. Far from it, in fact. Several parallel activities will continue, including those listed below.

Formal Standardization

Once the winning algorithms are chosen, they will enter a standardization phase where the official technical descriptions of how they work will be ratified. This is a lengthy process that won't be completed until 2024.

During the standardization phase, academics will continue to evaluate the algorithms and agree on the correct parameters for each security level (SL1, SL3 and SL5) as well as the instructions for how to correctly implement the algorithms. The net result will be a document, most likely a Federal Information Processing Standards (FIPS) publication, describing the algorithms in great detail. To see an example of what this may look like, you can review the output from a previous selection process that gave us the AES algorithm.[3]

Round 4 Analysis

Alongside the standardization, academics will also be reviewing additional candidate algorithms in a fourth round of analysis.

NIST has been clear they want a multitude of algorithms to eventually be standardized. Many of the candidate algorithms are based on similar mathematical problems. This could mean that if someone figures out how to break one or more of those problems using a classical or quantum computer, our entire ecosystem will collapse. Ideally, NIST will identify a range of algorithms, over time, that depend on differing mathematical problems. This avoids placing all our eggs into one crypto basket, so to speak.

[3] *https://www.nist.gov/publications/advanced-encryption-standard-aes*

Call for Additional Signature Algorithms

In addition to the Round 4 analysis, NIST has also requested a fresh look at signature algorithms. The existing pool of candidate algorithms do not show a wide enough variety of mathematical problems, leading to the same concerns mentioned above. One devastating attack could break many of our future systems.

Once NIST receives submissions for signature algorithms, they will be subjected to the same multi-year screening process that has been applied to the existing candidates.

What CISOs Should Do Now

As CISO (or CIO), you are likely bombarded with information around quantum computing, and it can be difficult to know what to do next. In this section, we'll cover the main actions you should be thinking about regarding the transition to post-quantum algorithms.

The Roadmap to Quantum Safety

The first thing to recognize is that migrating your business to a fully post-quantum position is a complex process that will take many years.

Although these post-quantum algorithms will not be ready for widespread production use until the standardization process finishes in 2024, there is considerable work required to prepare for these changes.

The key next steps for preparation are:

1. Identifying data assets
2. Identifying use of cryptography
3. Prioritizing systems for migration
4. Speaking to vendors
5. Testing algorithms for home-grown software
6. Considering use of hybrid mode
7. Optimizing for crypto agility

1. Identifying Data Assets

Switching to post-quantum algorithms cannot happen all at once. Even small businesses have far too many interlocking systems to expect to flip a switch at midnight and begin tomorrow as a post-quantum organization. As a result, prioritization is critical.

Before you can prioritize, you need to understand exactly what data you have, and how vulnerable it is to attack. Data that is particularly sensitive, and vulnerable to the "hack-now, decrypt-later" attacks, should be prioritized above less sensitive data that isn't transmitted freely.

For some organizations, this is a very challenging endeavor that they've never accomplished before. Now is an opportune time to build inventory data and keep it up to date.

2. Identifying Use of Cryptography

As well as identifying which data is important, CISOs should catalogue where quantum-vulnerable algorithms are currently being used. For a variety of reasons, not all systems will be affected equally. Symmetric encryption, such as AES, is far less affected by the quantum threat, requiring only a doubling of key sizes to remain secure. By contrast, RSA will be broken completely. CISOs need a very clear picture of the vulnerabilities present in each of their systems.

Many organizations simply don't have this information at hand, particularly if they develop a lot of in-house software and don't centralize their cryptographic decisions.

3. Prioritizing Systems for Migration

Once a clear view of sensitive data and existing cryptographic protections are established, it's time to prioritize your migration. This will require a good old-fashioned risk management conversation, where you will use the collected data to identify the largest vulnerabilities to your organization.

By far, the biggest concern should be the "hack now, decrypt later" threat, since this is a type of attack that may already have begun. This requires attention to encryption use cases more than digital signatures. Closing that stable door, before too many horses have bolted, should bubble to the top of the priority list. Beyond this, the list will be driven by your own business imperatives, and your determination of what could be most damaging to your organization.

4. Speaking to Vendors

It's likely your IT infrastructure is a combination of home-grown software and third-party systems. Typically, for all but the largest of organizations, the amount of third-party software will dwarf the home-grown systems.

Now is the perfect time to be asking your vendors about their plans for adopting post-quantum algorithms. A good vendor should have a clear roadmap already in place and be testing the candidate algorithms in preparation for 2024. Some may even allow you to access builds of their software that already support the candidate algorithms, albeit in pre-standardization form. (See the later section on hybrid modes to learn more about this.)

If you find a vendor who cannot answer this clearly, this might be a time to evaluate whether that vendor has a future with your organization. If nothing else, you should complain loudly that a lack of a plan is unacceptable and set a clear date by which you expect to have a more detailed conversation. The same applies to contractors serving government organizations and meeting agency timelines and requirements.

5. Testing Algorithms for Home-Grown Software

If your company develops its own software, now is the time to begin experimenting with the candidate algorithms to understand the impact they will have on performance and behavior.

The post-quantum algorithms have different properties than the algorithms we use today. The only way to know how they will affect your systems is to implement them and experiment. A good place to start is with the Open Quantum Safe project, which provides many different implementations of post-quantum algorithms designed for experimentation.

6. Considering Use of Hybrid Mode

For companies concerned about the "hack now, decrypt later" attacks, it may be possible to get the benefits of post-quantum security sooner through the use of hybrid modes of operation.

A hybrid mode of operation combines a traditional quantum-vulnerable algorithm, such as RSA, with a post-quantum algorithm. This approach can be used in protocols such as TLS or Secure Shell (SSH) to strengthen security. To break into a hybrid mode system, an attacker would need to break the traditional algorithm as well as the post-quantum algorithm. This means that using hybrid mode is no less secure than existing methods, and may bring the benefit of being quantum-secure as well.

The major downside of hybrid mode approaches is that they are not yet standardized, although this is under way through standards bodies globally. Until standardization is completed, they can only be deployed in closed-loop environments in which both the sender and receiver agree on a non-standard approach to cryptography. An example of this might be a virtual private network connection between two company offices. Since the company controls the software at the receiving and sending end, it can deploy a bespoke solution without worrying about compatibility with the wider world.

It's unclear whether hybrid modes will have a long-term future in post-quantum cryptography. In its post-quantum FAQs[4], NIST acknowledges some applications may desire the added security of hybrid mechanisms, even if it comes at the cost of performance. But for now, they represent an option for experimenting cautiously with non-standardized algorithms in some settings.

7. Optimizing for Crypto Agility

Crypto agility is about how easy it is to transition from one algorithm (or choice of parameters) to another. Companies that prioritize long-term thinking are already looking at this. Ensuring crypto agility has two obvious benefits.

First, if a problem is found with one of the post-quantum candidates, or it turns out that a different option is better for a particular environment, then swapping them out should be relatively easy. It is inevitable that the most popular choice of post-quantum algorithm implemented worldwide will not be the best choice for every use case, as is reflected in NIST's decision to provide options.

Second, the continued use of deprecated cryptography is one of the main cryptographic security issues with deployed systems. For example, the cryptographic hash function SHA-1 has not been considered cryptographically secure since 2005. However, despite the fact that the SHA-2 family of hash functions has been recommended since 2002, it took NIST until 2015 before recommending that federal agencies stop using SHA-1 in digital signatures. It is due to be removed from OCSP and CRL signing in 2022. But there are other places where SHA-1 is still in use today. The reason for delays is simply because SHA-1 is so ingrained that transitioning away from it is very difficult.

There is always the possibility that vulnerabilities will be discovered in the cryptographic algorithms we rely upon today. It is therefore worth using the occasion of transitioning to post-quantum to also address crypto agility. This will lead to more secure systems.

[4] *https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs*

The Positive Side of Quantum

It is worth remembering that while quantum computing poses a threat to cybersecurity, it also offers new techniques for strengthening existing systems.

Quantum computers are already being used today to generate stronger cryptographic keys. This is thanks to the unpredictable nature of quantum mechanics, which is an ideal ingredient for making existing cybersecurity systems stronger. Unlike the quantum threat, which is several years away, this technology is already in production. These keys are designed to work with the NIST-approved post-quantum algorithms to create the “lock and key” of quantum-safe encryption.

We also expect quantum technology to eventually help us move keys securely around the planet, through a process known as quantum key distribution, or QKD. This approach relies on the laws of physics to reduce the risk that an attacker can intercept encryption keys as they are shared between communicating parties.

Over time, we expect more technologies to emerge on the positive side of the quantum cybersecurity debate. And in the future, once this migration to post-quantum algorithms is behind us, we’ll view quantum as a gift to cybersecurity, not a threat.

To learn more about the positive aspects of quantum cybersecurity, please visit quantinuum.com.

Summary

NIST continues to make progress with its post-quantum algorithm standardization. This is an important step in the path to a future where cryptographic systems are safe from attack from quantum computers.

It’s important for CISOs to understand the impact this will have on their organizations and to familiarize themselves with the new algorithms and their properties. Although final standardization is expected to take between 18–24 months, CISOs must start preparing for the immense complexity of migrating every computer system in their domain to new algorithms.

By following our simple step-by-step guide, CISOs can be in a better position to move swiftly when the standardization process is complete.

QUANTUM ORIGIN

QUANTINUUM

QUANTUM ORIGIN

QUANTINUUM