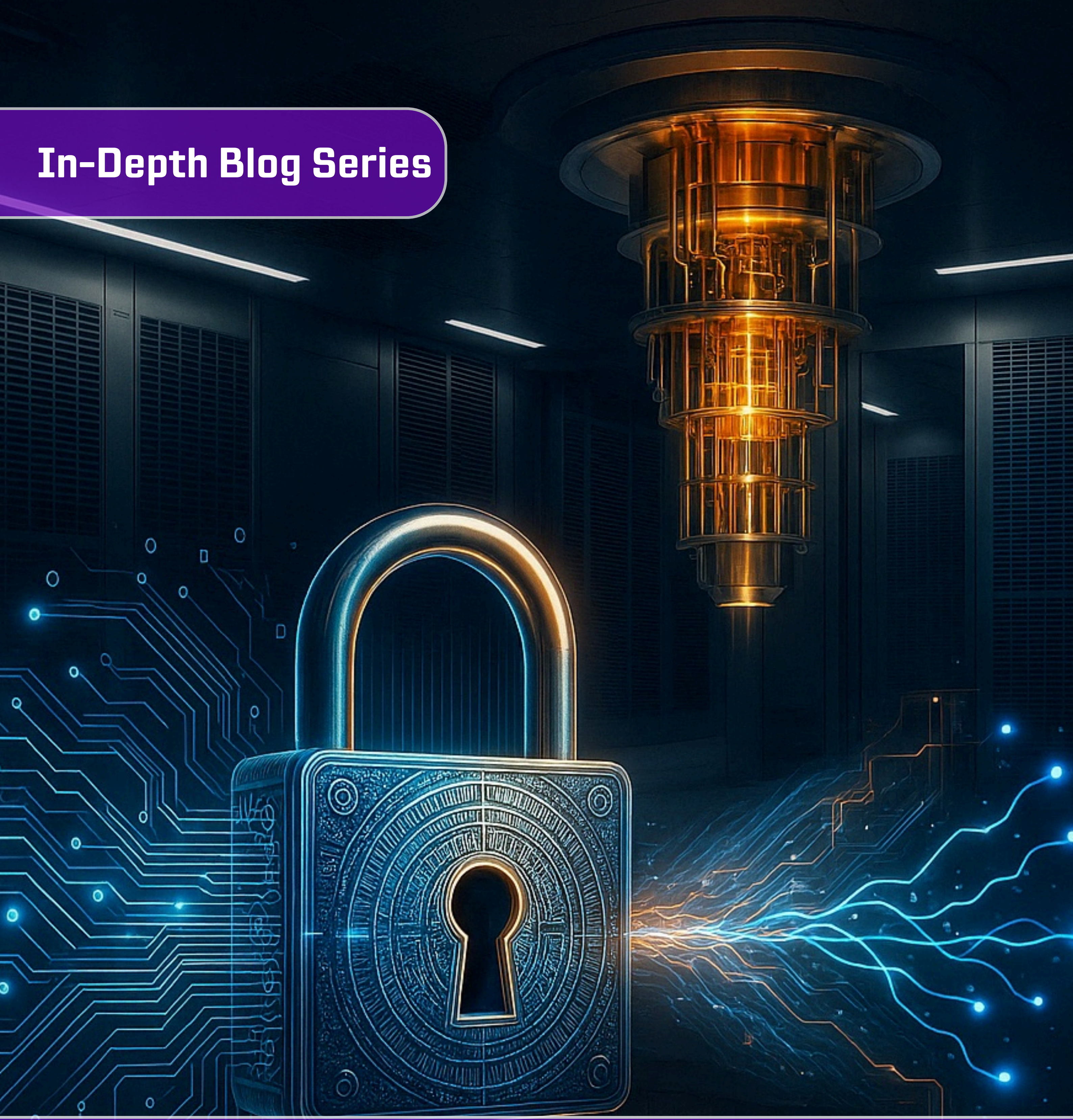
In-Depth Blog Series



Post-Quantum Encryption

Now the Cat's Out of the Box

FLOW

Now the cat's out of the ~~bag~~ box: Post-quantum Encryption.

Scientists have been pondering quantum mechanics for a long time, with Schrödinger's famous thought experiment on quantum superposition dating back to 1935.

This fundamental principle of quantum mechanics states that quantum systems can exist in multiple states simultaneously. According to the principle of quantum superposition, a quantum system can exist in a linear combination of its possible states until observed or measured.

In classic computing technology, the familiar binary bit, characterised as 0 or 1, can only be in one of these two states. Quantum computers utilise quantum bits, commonly referred to as qubits.

Through this phenomenon of coherent superposition, qubits can exist in multiple states simultaneously. Qubits can hold more information, utilising superdense coding to communicate a larger number of classical bits of information by transmitting a smaller number of qubits. This allows quantum computers to process vast amounts of information.

One of the main challenges in developing quantum computing is the fragile nature of qubits. They can be disrupted by various factors, including microscopic defects in hardware, heat, vibration, electromagnetic interference and even cosmic rays. All of which can cause them to decohere and diphase, causing calculation errors.

Quantum Progress: Google and Microsoft Lead the Charge

Google recently announced their Willow chip, which significantly advances error reduction, addressing this key challenge that has been pursued for 30 years.

> "We're optimistic that within five years we'll see real-world applications that are possible on quantum computers"
>
> **Hartmut Neven (Google Quantum AI)**

Quantum computing represents a significant leap forward, bringing many benefits, including revolutionising healthcare and medicine, optimising renewable energy, and advancing AI.

There are many conflicting estimates for the delivery of useful quantum computing. Chetan Nayak, a technical fellow of quantum hardware at Microsoft, while announcing their new Majorana 1chip, was quoted as saying,

"Many people have said that quantum computing that is to say useful quantum computers are decades away. I think that this brings us into years rather than decades."

On the other hand, more conservative estimates, like that of Nvidia CEO Jensen Huang, think that "very useful" quantum computing will come in 20 years.

Quantum vs Encryption: A Looming Threat

If useful quantum computing is still a while away, why should we worry about the security risks now?

Gartner predicted that "by 2029, advances in quantum computing will make asymmetric cryptography unsafe and by 2034 fully breakable."

While the benefits of quantum computing are clear, it also poses some serious security challenges. Encryption forms a key part of our online security today. Relying on complex algorithms to encrypt data that classical computers find challenging to break.

However, quantum computers could crack these encryptions with relative ease, creating a need for quantum-proof security measures.

> **"A conventional computer needs 300 trillion years to break RSA-2048 encryption, while a 4,099-qubit quantum computer would need only 10 seconds to crack the same RSA key."**
>
> **Forbes**

Harvest now, decrypt later (HNDL) is a surveillance strategy that relies on the acquisition and long-term storage of currently unreadable encrypted data, with the intention of utilising future decryption breakthroughs.

Due to the nature of HNDL attacks, the targets are rarely transactional data or payment card information, as these lose value quickly due to expiration or obsolescence.

The key targets are data that retains value over more extended periods of time, such as sensitive business information, research data and intellectual property.

Consequently, the top targets for HNDL are government bodies, healthcare organisations, and commercial organisations with long research and development cycles.

However, this doesn't mean other organisations are immune to this threat. With recent strides in the development of quantum computers, it is possible that attackers could decrypt sooner, which could bring more potential targets into scope.

Policy Momentum: U.S. Federal Roadmap

The threat of HNDL attacks has caused concerns about the need to deploy post-quantum cryptography, leading the U.S. federal government to propose a roadmap for migrating towards quantum-cryptography-resistant algorithms in 2022.

A Deloitte poll of over 400 organisations considering quantum computing benefits found that 50.2% believe they're at risk for harvest-now, decrypt-later attacks.

Post-Quantum VPNs: Today's Defences

Encryption is used in many aspects of IT to secure data at rest and in transit. In this blog, we will explore how to secure VPNs ready for the post-quantum world.

RFC8784 – Quantum-safe IPSEC

The Internet Key Exchange Protocol Version 2 (IKEv2) is one example of a cryptosystem that could be broken by quantum computers. RFC8784 was developed to address this problem until quantum-secure key exchange algorithms become available.

RFC8784, introduced in 2020, describes a method of adding an additional secret shared between the initiator and the responder.

This secret is an addition to the authentication method already provided within IKEv2. This additional secret is used to generate the key material, providing quantum resistance to the IPsec Security Associations (SAs) and IKE SAs.

This approach was inspired by IKEv1, which is considered a much weaker protocol, which utilised shared secrets to generate the SKEYID, which drives the encryption keys, whereas IKEv2 reduced the use of shared secrets to authenticate the peer.

If the pre-shared key has sufficient entropy and the Pseudorandom Function (PRF), encryption, and authentication transforms are quantum secure, the resulting system is believed to be quantum safe. This method is widely adopted by many vendors, including Juniper, Cisco, Palo Alto, and Fortinet.

NIST SP 800-227 - Post-Quantum Cryptography (PQC) / Quantum-Safe Cryptography (QSC) Standardisation

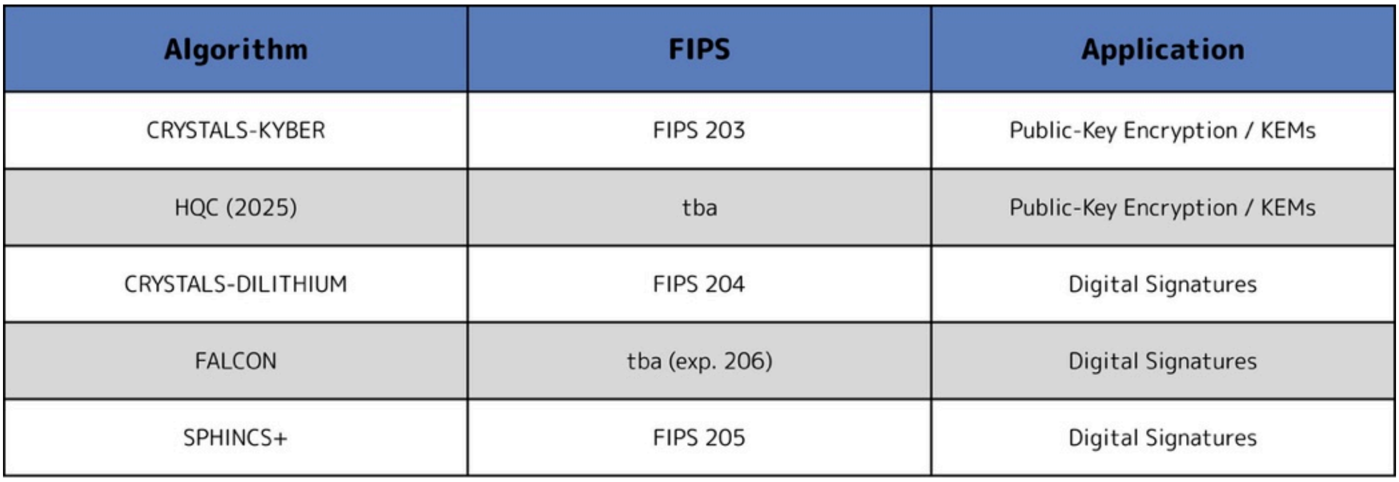
In 2016, NIST initiated the selection and standardisation of quantum-resistant algorithms to counter potential threats from quantum computers.

The intention is to select several 'good choice' algorithms rather than 'pick a winner'. This effort resulted in the initial public draft of NIST SP 800-227 in January 2025.

The first round of algorithms saw 69 submissions accepted as "complete and proper" in December 2017. Since then, there have been several selection rounds, resulting in the current list of selected algorithms and the associated FIPS standards.

Each algorithm has been categorised into two types: Public-Key Encryption/Key Encapsulation Mechanism (KEM) and Digital Signatures.

Current selected algorithms



Algorithm	FIPS	Application
CRYSTALS-KYBER	FIPS 203	Public-Key Encryption / KEMs
HQC (2025)	tba	Public-Key Encryption / KEMs
CRYSTALS-DILITHIUM	FIPS 204	Digital Signatures
FALCON	tba (exp. 206)	Digital Signatures
SPHINCS+	FIPS 205	Digital Signatures

List updated 27th March 2025

The most recent addition to the selected algorithms was HQC on the 11th of March 2025. This work is ongoing, with a tentative sixth Post-Quantum Cryptography PQC standardisation conference scheduled for September 2025.

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a mechanism for producing and distributing encryption keys that relies on quantum mechanics. The resulting keys can be used with any chosen encryption algorithm.

QKD protocols do not provide authentication. Therefore, they are vulnerable to physical man-in-the-middle attacks in which an adversary can agree to individual shared secret keys with two parties who believe they are communicating with each other.

For this reason, QKD protocols must be deployed alongside cryptographic mechanisms that ensure authentication. These cryptographic mechanisms must also be secure against the quantum threat.

The process of measuring a quantum system generally disturbs the system (as demonstrated by Schrödinger's cat). Therefore, a third party trying to eavesdrop on the key must measure it in some way, which would introduce detectable anomalies. This gives QKD the unique property of being able to detect if a third party tried to gain knowledge of the key.

According to Qureca, the quantum key distribution (QKD) market is projected to grow from $6 billion to $13 billion by 2030.

Distributed Symmetric Key Establishment – DSKE

Before we delve deeper into DSKE, it is worth summarising the difference between Symmetric vs. Asymmetric cryptography. Asymmetric encryption uses two keys: a private key and a public key.

It is considered more secure but less efficient than symmetric. There is no need to share the private key, reducing the risk of exposure. Symmetric key encryption uses one key shared between sender and receiver to encrypt and decrypt. This is faster and more efficient for large amounts of data. It does, however, require a secure method to share the key between sender and receiver.

The security of public keys used in asymmetric encryption is dependent on the 'hardness' of the underlying mathematical problems. Shor's algorithm could solve the factoring problem on a sufficiently powerful quantum computer, breaking the security of asymmetric cryptography.

DSKE fully automates the creation and distribution of symmetric keys without relying on the computational complexity of asymmetric encryption.

In a DSKE system, there are two primary components:

Security Hubs and DSKE clients (or simply clients). Systems can include one or multiple Security Hubs. When a new DSKE client joins the system, each Security Hub generates activation data, including high-quality random numbers, called Pre-Shared Random Data (PSRD).

The PSRD is stored on the Security Hub and sent to the client securely. When two clients want to exchange keys with each other, they use the Security Hubs as intermediaries.

The first client sends a key request to each security hub independently, asking for a key with the second client. These key requests are encrypted and authenticated using PSRD.

The Security Hubs compute key instructions using the metadata sent in the request. The key instructions are encrypted and authenticated with the second client using its PSRD. The two clients can now build a secret key that can be used in any symmetric cryptographic algorithm for encryption or authentication. This key is not known by the Security Hubs due to this sharing protocol.

Once a client has joined the DSKE system, it can request keys on demand, including group keys. DSKE has been proved to be theoretically secure information, meaning Quantum or classical computer attacks cannot be used to break the system; they are computationally unbreakable.

Key benefits of DSKE:

- Mathematically unbreakable: DSKE does not rely on computational hardness assumptions, making it resistant to both classical and quantum attacks.
- Lightweight and efficient: DSKE is computationally efficient and does not require the large key sizes associated with PQC.
- No special hardware required: Unlike QKD, DSKE can operate over existing network infrastructure, reducing deployment costs and complexity.

On the 8th of August 2024 Juniper announced a strategic investment in Quantum Bridge Technologies, an industry leader in Distributed Symmetric Key Exchange (DSKE). The two companies will collaborate through Juniper Beyond Labs' pathfinding projects.

"Our comprehensive understanding of the intricate quantum security landscape has enabled us to forge strategic relationships, garner recognition, and build a strong reputation in this rapidly evolving field.

We are thrilled to partner with Juniper Networks and further enhance our ability to help secure vulnerabilities in network infrastructures against quantum computing threats."

Mattia Montagna
CEO, Quantum Bridge Technologies

The combination of DSKE technology, Juniper's quantum-safe VPNs, and Crypto Agility solutions enhances Juniper's AI-Native Networking Platform, helping customers better protect their high-value data from harvest now, decrypt later attacks, and safeguard against future quantum computer-aided attacks.

"Our collaborative efforts with Quantum Bridge have demonstrated the ability to translate theoretical advancements into practical implementations, positioning them as a frontrunner in securing digital infrastructures against quantum attacks.

With this investment, we are helping to safeguard our customers' sensitive data against new risks and enhance the user experience in an unprecedented threat era."

Raj Yavatkar
CTO, Juniper Networks

Closing thoughts

We will undoubtedly hear more about making our networks secure against Quantum-based threats in the near future.

As we have explored, solutions are available today to protect ourselves, alongside evolving new solutions and research to continue innovating new solutions. While the impact of quantum computing may seem still beyond the horizon, by planning now, organisations can ensure their data will be protected in the upcoming post-quantum world.

On the 20th of March 2025, the National Cyber Security Centre (NCSC) released guidance on the key milestones for PQC migration. In this guidance, the suggested timeline for actions is outlined as follows:

Your Post-Quantum Migration Timeline

BY 2028

- **Define your migration goals.**
- **Carry out a whole discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)**
- **Build an initial plan for migration.**

BY 2031

- **Carry out your early, highest-priority PQC migration activities**
- **Refine your plan so that you have a thorough roadmap for completing migration.**

BY 2035

- **Complete migration to PQC of all your systems, services and products.**

What can organisations do today?

- Perform an inventory of assets and their current cryptographic protections. Start preparing to migrate to technology that provides quantum-safe solutions.
- Evaluate prospective vendors' quantum-safe features as part of any current procurement processes, ensuring you future-proof upcoming investments.
- Consider the options carefully to ensure you select a solution that meets your future needs.
- Avoiding early adoption of non-standard QSC is not recommended. Keep an eye on selected algorithms (NIST SP 800-227).
- Continue to track developments in quantum computing and quantum-safe solutions.

By taking proactive steps today, organisations can ensure readiness regardless of when Q-Day arrives.

Stay ahead of Q-Day.

Flow supports organisations in preparing for the post-quantum era with expert insight, strategic delivery, and future-ready partnerships.

Click here to get in touch with our team or call us on **+44 (0) 1442 927 996**
and explore how we can help with your plans.

Secure Tomorrow, Today

Quantum computing is reshaping what’s possible, demanding a new class of resilience in your IT strategy.

At Flow, we don’t just prepare you for change; we help you stay ahead of it.

From post-quantum encryption to future-proof infrastructure, our expert-led approach ensures your organisation is ready for the challenges of a quantum-powered world.

Let's Shape the Future Together

Partner with Flow to build secure, scalable solutions that stand the test of time.

Reach out today to start your journey with Flow.

info@flowtransform.com | +44 (0) 1442 927 996 | flowtransform.com