Post-quantum Cryptography: Protecting Critical Data and Enhancing Cyber Resilience

Michael Fasulo

Commvault, Englishtown, New Jersey, United States
E-mail: commvault@touchdownpr.com

Received 24 November 2025; Accepted 24 November 2025

Abstract

Quantum computing represents a significant threat to the asymmetric cryptographic algorithms currently used to protect the traditional data security infrastructure today's enterprises depend upon. With Gartner predicting that by 2029 advances in quantum computing will render applications, data and networks protected by asymmetric cryptography unsafe, organisations must begin preparations to transition to post-quantum cryptography (PQC). Organisations that fail to prepare for quantum today risk potentially exposing their sensitive data on a massive scale, as threat actors are already collecting encrypted enterprise data in anticipation of future quantum decryption capabilities. The migration to PQC involves updating risk registers and enabling the crypto agility that supports the rapid implementation of new algorithms and ensures organisations can adapt fast to new regulatory standards.

Keywords: Asymmetric cryptography, quantum computing, post-quantum cryptography (PQC), cyber resilience, crypto-agility, NIST standards.

Quantum Information Technologies Journal, Vol. 1_1, 43–48.
doi: 10.13052/qitj2795-0492.113

1 Introduction

While it is not quite mainstream yet, the world is on the brink of a new quantum computing era. Recent advances, such as more stable qubits and improved error correction, mean that the revolutionary potential of quantum computing is fast becoming a tangible reality. Capable of harnessing the power of quantum mechanics to solve substantial, complex problems faster than traditional computers, the risk that quantum computing poses to the current encryption methods used to protect today's digital assets is significant.

Concerned that cybercriminals and malicious actors will harness the power of quantum computing to 'crack' the asymmetric (public-key cryptography) algorithms, such as RSA and ECC (elliptic curve cryptography), that are widely used to secure digital networks, communications and transactions, government agencies around the globe are now urging organisations to transition to quantum-resistant encryption methods that will bolster cyber resilience.

2 Understanding the Risks

While the date when cryptographically relevant quantum computers will become more commonplace remains uncertain, Gartner predicts that by 2029 [1] advances in quantum computing will make most conventional asymmetric cryptography unsafe to use. However, cybercriminals are already adopting a 'harvest now, decrypt later' mindset and stealing encrypted data in anticipation of decrypting it in the near future.

For organisations that retain sensitive data – biometrics, financial information, intellectual property (IP), medical records or personally identifiable information (PII) – for the long term, this represents a significant and growing risk. In addition to which, mission-critical authentication systems, blockchain applications and secure communications will also be at risk of compromise.

As quantum computing capabilities accelerate, policymakers are starting to update cybersecurity regulatory requirements to include post-quantum encryption. Enterprises will need to ensure their cryptographic practices are compliant with these evolving regulatory frameworks and standards.

3 Preparing for a Quantum Safe Future: Post-quantum Cryptography

The National Institute of Standards and Technology (NIST) has been coordinating the global effort to select potential post-quantum cryptography (PQC)

algorithms that will deliver long-term digital security for governments, enterprises and multinational corporations. Based on mathematical problems that are difficult for both traditional and quantum computers to solve, these PQC algorithms are designed to advance the protection of encrypted data against future quantum threats.

Following an eight-year cycle of submission, research and analysis, in August 2024, NIST published its finalised first three PQC standards: FIPS 203 (CRYSTALS-Kyber), FIPS 204 (CRYSTALS-Dilithium) and FIPS 205 (SPHINCS+) [2]. In March 2025, NIST further enhanced its PQC framework, selecting the Hamming quasi-cyclic (HQC) algorithm [3] as a backup encryption method for the existing module-lattice-based key-encapsulation mechanism (ML-KEM) algorithms recommended by FIPS 203. Unlike ML-KEM, which relies on structured lattices, HQC's unique mathematical foundation offers a robust alternative that can help combat the potential threats posed by future quantum computers.

Regulators, governments and standards defining organisations (SDOs) around the world are now issuing mandates relating to PQC adoption. Alongside replacing legacy encryption with PQC, enterprises will be required to demonstrate cryptographic agility – the ability to quickly change algorithms in response to evolving cryptographic and quantum threats. This is essential for organisations that want to maintain cyber resilience and stay quantum ready.

In the UK, the National Cyber Security Centre's (NCSC) guidance recommends organisations should aim to complete their PQC migration of all systems, services and products by 2035 at the latest [4]. Meanwhile, the European Union (EU) has recommended that all member states should transition to PQC by 2030 [5].

4 Transitioning to PQC: Building a Post-quantum, Crypto-agile Strategy

Protecting critical data and infrastructure from current and future quantum risks represents a mission-critical priority for today's enterprise. However, while most organisations are actively working on cyber resilience strategies, the risk that quantum computing represents is often viewed as a low-priority issue and is not widely considered. To maintain cyber resilience and protect future data integrity, organisations should plan their PQC journey as soon as possible. To streamline the migration process, the following key considerations will help define an effective migration strategy.

4.1 Undertake a Cryptography Inventory

Not all data is equally important, and not all data needs to be encrypted in the same way. It is therefore important to identify where cryptography should be used in the digital heritage. This should include the most sensitive data, applications, networks, identity systems and third-party connections.

As a first step, organisations should undertake a detailed inventory of their data and all cryptographic assets within their infrastructure. Utilising AI tools will help deliver a granular and high-fidelity set of signals on the organisation's data-sensitive posture – uncovering all data silos and instances of shadow IT, including AI applications.

4.2 Assess Risk

Given the cost of post-quantum cryptography, it makes sense to prioritise protecting the most sensitive data rather than trying to protect everything. Having evaluated data in terms of its sensitivity and longevity, information that needs to stay confidential for over five years should receive immediate attention. For less sensitive data, standard encryption methods should suffice for the short term.

4.3 Implement Crypto Agility

The ability to switch between different cryptographic algorithms in response to new threats will be essential for ensuring operational resilience and maintaining compliance with evolving regulatory requirements in the post-quantum era. In addition to having a complete inventory of all cryptographic assets across all environments, organisations will need to develop frameworks that make it easy to replace cryptographic algorithms without the need for an extensive system redesign and invest in employee training to support this capability.

4.4 Prepare a Prioritised Migration Strategy

Organisations should plan to start migrating their most sensitive systems and data, prioritising those that protect intellectual property or personally identifiable information. Starting early and utilising this phased approach will help strengthen their overall cyber resilience posture before PQC becomes an operational necessity.

4.5 Supplier Engagement

Organisations should proactively assess third-party dependencies and engage with suppliers to understand their PQC migration plans, ensuring that the efforts of all supply chain stakeholders are aligned.

5 Conclusions

Changing cryptography in complex IT environments is not something that can be done overnight. Historical precedent shows that major cryptographic transitions typically take 5–10 years to complete.

To future-proof their security posture and maintain regulatory compliance, organisations should commence with proactive preparations that will enable them to navigate the multi-year post-quantum transition in a smooth and timely manner. The 'harvest now, decrypt later' strategy being used by cybercriminals today means that industries handling long-term confidential information – such as healthcare, finance, government and manufacturing – will need to take immediate action to mitigate quantum threats and protect sensitive data and systems.

References

[1] Gartner, "Gartner Identifies the Top 10 Strategic Technology Trends for 2025", Oct. 21, 2024. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2024-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2025.

[2] National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards", Aug. 13, 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. [Accessed Oct. 27, 2025].

[3] National Institute of Standards and Technology, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption", Mar. 11, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption. [Accessed Oct. 27, 2025].

[4] National Cyber Security Centre, "Timelines for migration to post-quantum cryptography", Mar.20, 2025. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines. [Accessed Oct. 27, 2025].
[5] European Union, "EU reinforces its cybersecurity with post-quantum cryptography", Jul. 23, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography. [Accessed Oct. 27, 2025].

Biography

Michael Fasulo is Senior Director of Portfolio Marketing at Commvault. He specialises in connecting technology with real customer needs to ensure Commvault's solutions are both relevant and impactful. With over two decades of experience spanning hyperscale cloud, cybersecurity, and emerging technologies like post-quantum cryptography, Fasulo helps organisations to navigate the evolving challenge of achieving cyber resilience in a rapidly changing digital world.