VIEW POINT

# DE-MYSTIFYING QUANTUM COMPUTING – IS IT A DOUBLE-EDGED SWORD?

Infosys®
Navigate your next

Quantum computers are super-powered computers that use the principles of quantum mechanics to speed up calculations — it has the potential to solve problems of exponential scale quickly. Unlike classical computers, which are underpinned by bits that can have only one state at a time, i.e., either 0s or 1s, quantum bits (qubits) can exist in multiple states simultaneously. This property of qubits, known as superposition, allows quantum computers to process massive amounts of information in parallel, thereby solving complex problems at incredible speed. In addition to superposition, qubits also possess another property, entanglement, that allows qubits to remain intertwined, creating correlations between qubits such that measuring one affects the state of another.

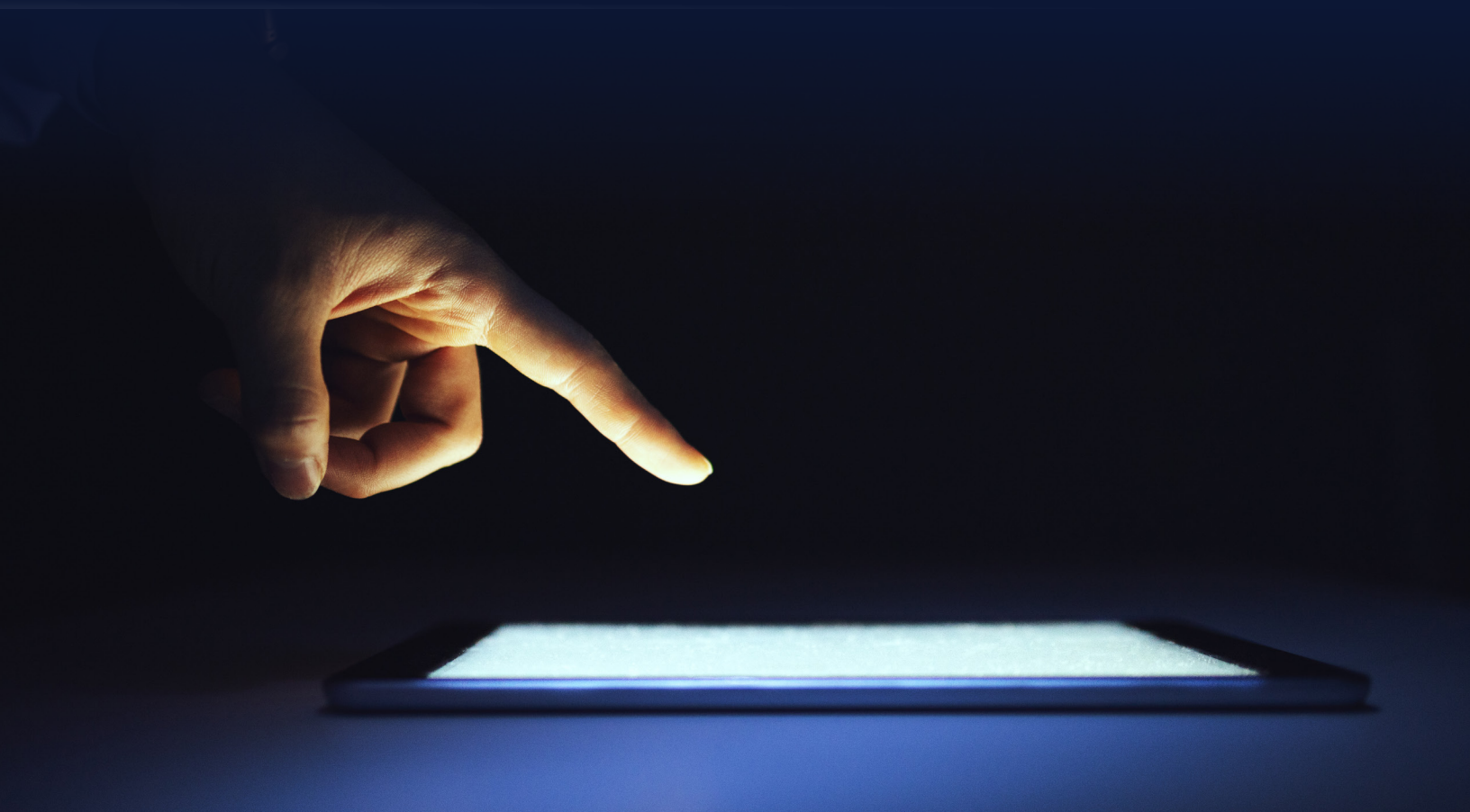
These properties of qubits are profound and can tackle computationally intensive tasks beyond classical computers' reach, fueling breakthroughs in medicine, materials science, financial modeling, and cryptography. In finance, it could enable faster, more complex Monte Carlo simulations, such as trading, price optimization strategies, and fraud detection, to name a few. In life sciences, it could potentially accelerate the drug discovery process.

One might then ask what's stopping quantum computing from reaching its potential. One of the current limitations of quantum bits is that they can hold their quantum states for only tiny fractions of a second. As the number of qubits increases, these results in errors being magnified, thereby resulting in the compounding of "noise," i.e., errors compound. To address this anomaly, information is encoded across more than one qubit so that the system as a whole retains enough information to carry out the required calculation. By employing this technique, qubits can hold the state for a few milliseconds, which is not sufficient. Google recently launched a new chip, Willow, that can hold the state for 100 milliseconds. Google claims that it takes five minutes to solve a problem that would currently take the world's fastest supercomputers 1025 years to complete.

As outlined above, while quantum computing can accelerate positive breakthroughs across industries, it could also break widely used encryption algorithms such as RSA and ECC (Elliptic Curve Cryptography), which underpin the security of transactions and communications. "Q-Day," or quantum day, is when large-scale quantum computers can break the encryption codes protecting much of today's payments and financial data. This looming threat necessitates the development and adoption of post-quantum encryption techniques. Post-quantum encryption is designed to withstand the prowess of quantum computers.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has finalized its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer. These finalized standards include instructions for incorporating them into products and encryption systems. The U.S. government estimates a 10-year migration cost exceeding $7 billion for federal systems alone.

Apple announced in February 2024 that it is upgrading its encryption system to fend off potential quantum computing attacks, while in September 2024, the encrypted messaging app Signal boosted its own encryption by adding support for post-quantum cryptography.

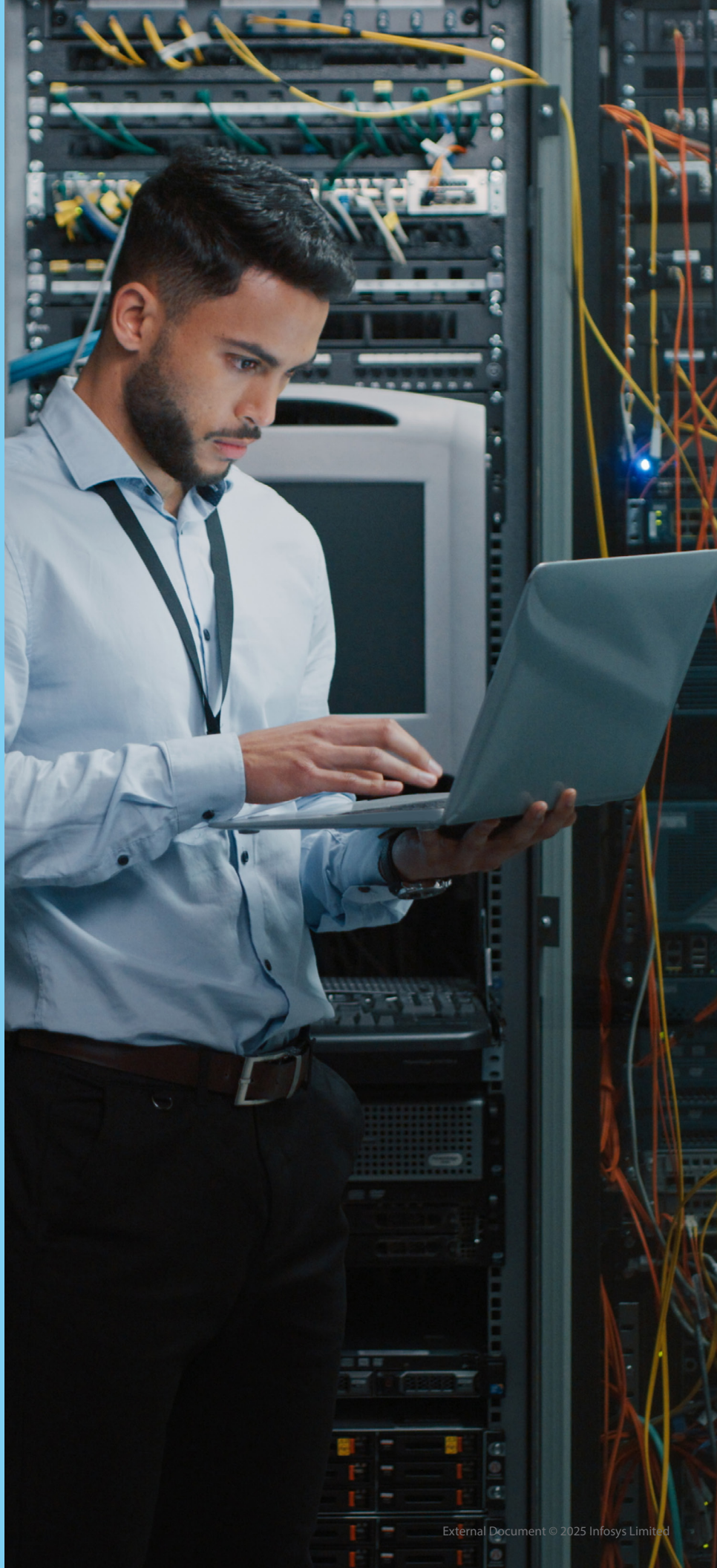


## How can financial organizations prepare themselves for the next Y2K, i.e., post-quantum cryptography?

**Quantum Computing Impact on Cryptography used in the Cards Industry**

Quantum computers are projected to solve asymmetric key algorithms such as RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC) soon. Symmetric encryption is less mathematical than asymmetric encryption, as it uses the same key to encrypt and decrypt data. Because of this, symmetric encryption is not at risk from quantum computing. Asymmetric encryption like RSA relies on finding the prime factors of a large number. RSA is reliable today because even with the best supercomputers, finding the prime factors through brute force is prohibitively expensive. However, QC poses a risk to RSA encryption due to its potential to find the prime factors through superposition. When this happens, RSA systems of the world will be at grave risk, and thus internet communication would come to a grinding halt.

Some parts of PIN/Card transaction processing use 3DES or AES, and both are symmetric keys. EMV cards use RSA signatures and keys - SDA (Static Data Authentication), DDA (Dynamic Data Authentication), or CDA (Combined Data Authentication). This is to ensure fake cards cannot be produced. With quantum computing, this safety feature may no longer be available. EMV Transaction Cryptogram: EMV Card uses a card-unique 3DES key for ARQC generation and ARPC validation. EMV cards use a card-unique 3DES key to generate a dynamic card verification value (DCVV). CVV1/CVV2 validation uses 3DES keys. CAVV in 3D Secure (Card Not Present Transaction processing) is based on 3DES keys. For example, Visa uses RSA-based Message Level Encryption (MLE) for REST API communication with banks.



## EMVCo initiatives focused on security risks arising out of Quantum Computing

In September 2024, EMVCo publicized its Position Statement - Quantum Computing and EMV Chip Cryptography. The Position Statement outlines the EMVCo Security Working Group (SWG) position regarding the threat posed by quantum computers to the cryptography that is intrinsic to the security of EMV and in particular, C-8 contactless. Key highlights from the Position Statement are mentioned below:

The true landscape is more nuanced from a timeline perspective and separates distinctly between asymmetric algorithms (such as RSA and ECC) and symmetric algorithms (such as AES).

SWG supports AES-128 to be the entry-level symmetric algorithm resistant to classical and quantum attacks and being resource efficient is suitable for current and future use. The SWG believes that there is no need to recommend consideration of AES-256 for quantum resistance; however, it is allowed for contingency purposes.

Breaking a Payment System or Issuer key would allow the production of fake cards used for fraudulent offline payments. However, breaking an individual card key would only allow the cloning of that card, and this would be uneconomic for a fraudster.

From a C-8 contactless privacy perspective, an eavesdropper wanting to track an individual across transactions would need to break the ephemeral keys for every transaction.

The SWG is monitoring the following milestones:

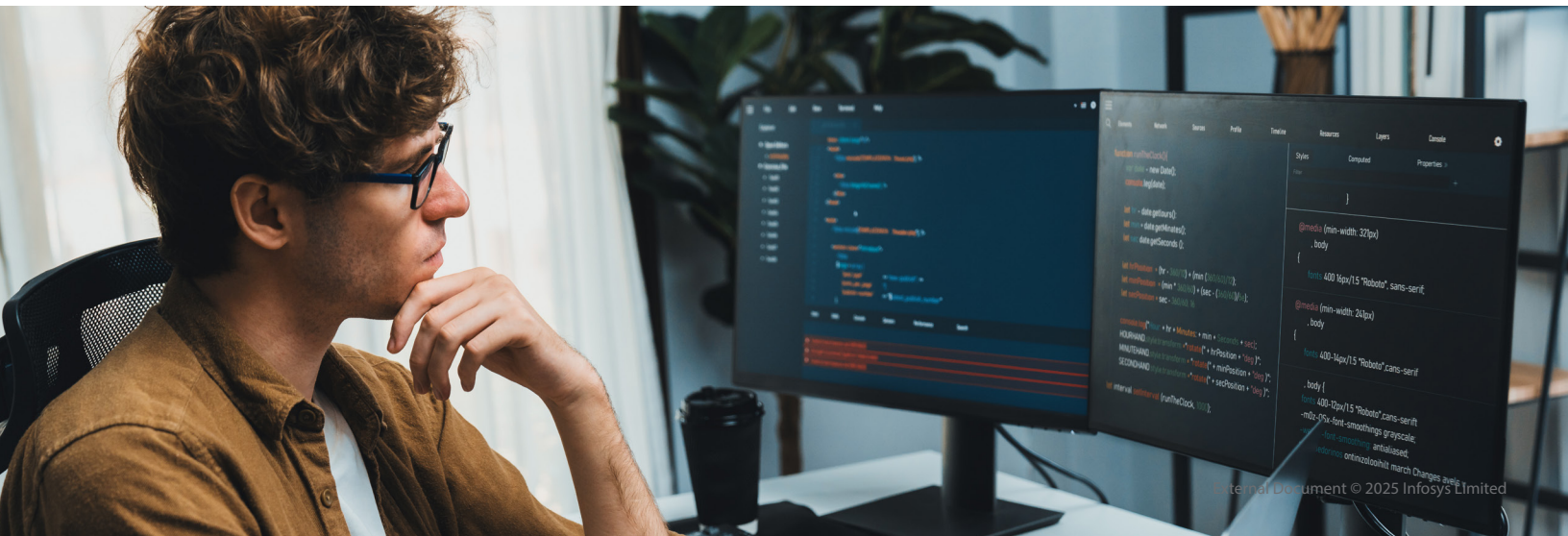
- First fault-tolerant logical qubit
- 1,000 entangled physical qubits
- Multiple entangled fault-tolerant logical qubits
- Identical qubit behavior

## PCI DSS 4.0 (mandatory starting 31st March 2025) focuses on Post Quantum Cryptography (PQC). PCI DSS 4.0 has a defined approach for cryptographic cipher suites and protocols requirements (12.3.3):

- Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:


- PCI DSS 4.0 considers cryptography management and crypto agility best practices for responding quickly to future developments in cryptographic protocol vulnerabilities.

The global financial system relies heavily on established cryptographic methods, and migrating to post-quantum solutions will require substantial investment in the technology and talent necessary to modernize core infrastructures. Financial institutions are caught in a 'hard-and-rock' situation as to whether to take a proactive approach or a wait-and-watch approach for the technology to advance to a state wherein the organization is comfortable making the necessary investment to upgrade the current encryption to post-quantum encryption. While sensible it may sound, we believe that it is a risky approach. Infosys thereby recommends a pragmatic approach of laying the foundation for a full-blown migration so when the technology is matured to a production-ready state, they are fully prepared to take the plunge.



To that end, Infosys proposes a 2-phased approach to help organizations prepare themselves for the Q-Day:

1. Planning through a wave-cluster approach
2. Migration leveraging Agentic AI framework

## 1. Planning through a Wave-Cluster Approach

The wave-cluster approach is a strategic methodology proposed by Infosys to migrate services/applications to post-quantum cryptography in a structured, phased manner. The primary objective of this method is to develop an inventory of critical assets while maintaining high levels of accuracy and predictability. This approach will break down the inventory into smaller, manageable units of work, referred to as clusters, and organize these clusters into waves.

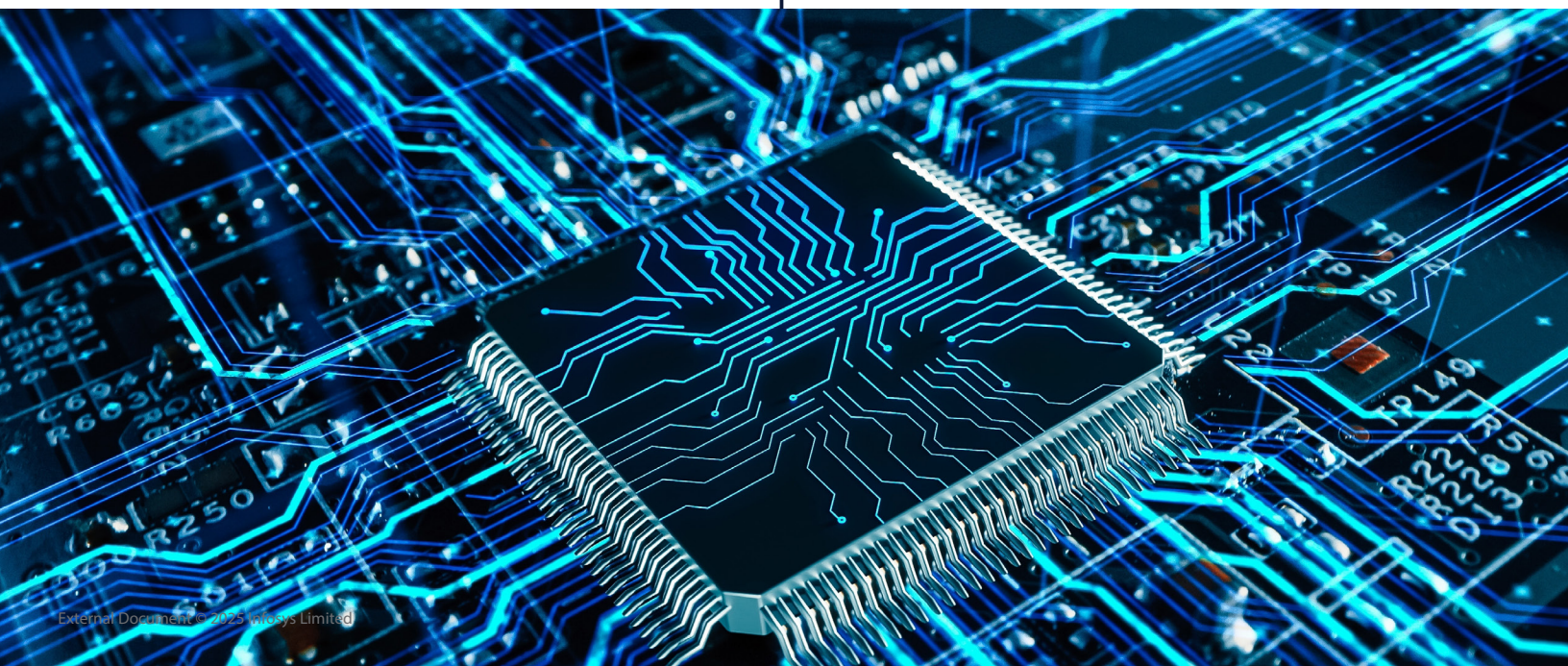
Waves and clusters will be organized based on interdependencies and commonalities between applications, components, devices, and services. This organization will ensure that each wave is manageable and that learnings from each wave can be applied to subsequent waves, thereby improving efficiency and effectiveness. In this phase, Infosys will collect data to form an optimal migration plan, considering factors such as size, complexity, criticality, region, interdependencies, support footprints, and key staff. By leveraging staggered scheduling, the approach allows for continuous improvement and adaptation, ensuring that any issues encountered in earlier waves can be addressed in subsequent ones. This methodical and phased approach will ensure that migrations are smooth, and risks are minimized.

## 2. Migration to post-quantum cryptography leveraging language model (LM) Agentic AI solution

Infosys recommends creating a cybersecurity-tuned Language Model (LM) to detect vulnerable code and generate quantum-safe code. As part of this approach, the cybersecurity fine-tuned LM will scan the code base of the selected applications, services, and components identified as part of the wave-cluster approach. LM will detect references to algorithms like RSA and ECC and generate QC vulnerability index which is a measure of the extent to which quantum computer can break the encryption.

Code with higher vulnerability index will undergo remediation to post quantum cryptography leveraging Agentic AI solution. Agentic AI solution will identify the best implementation to quantum safe algorithm. It will generate the code to implement quantum safe algorithm and replace the vulnerable code with quantum safe code.

To summarize, threat posed by quantum computer is imminent and financial organizations must take proactive step to protect themselves from this threat. Our recommended phased wise approach will help in quantifying the impact of post quantum algorithm and will help in accelerating the migration to post quantum algorithm leveraging LM and Agentic AI solution. By taking these steps, financial organizations can ensure the resilience of their infrastructure in the quantum era.



## Reference URLs


https://www.emvco.com/resources/security-position-statement-quantum-computing-and-emv-chip-cryptography-2/

https://www.encryptionconsulting.com/preparing-for-tomorrow-exploring-pci-dss-4-0s-role-in-quantum-safe-cryptography-transition/

Federal Register :: Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard

Blog - iMessage with PQ3: The new state of the art in quantum-secure messaging at scale - Apple Security Research


## About the Authors

### Dharmendra Choudhari (DC)

**Sr. Business Development Manager – Financial Services**

DC is a payments/financial services professional with a deep payments domain and a breadth and depth of supporting technical knowledge. He comes with 20+ years of IT experience in Sales, Business Development, Account Management, Client Relationship management. His role involves articulating business value that Infosys can bring by introducing more efficient processes, making better use of existing assets and deploying proven Infosys platforms and solutions to accelerate their transformation journey. He also leads Infosys's global Payments COE.

### Vittal Setty

**Product Line Manager, Infosys Center for Emerging Technologies**

Vittal leads the Quantum Computer Center of Excellence. As part of his mission to prepare for the oncoming Quantum Computing Revolution, he has created multiple living labs showcases to demonstrate the application of QC in different industry verticals, published thought leadership articles in MIT Tech Review, conducted client workshops, and fostered partnerships with startups and hyperscalers.

### Manickavasagam S

**Principal Consultant - Financial Services Domain Consulting Group - Payment Practice**

Manickavasagam is an experienced professional in Cards & Payments and played multiple roles - Business & IT Consulting, Platform Management, Product Management, Product Owner (Agile), IT Delivery Management, Program Management.

### Rahul Ameta

**Head of Cards & Payments Practice - Financial Services Domain Consulting Group**

Rahul Ameta is an Industry Leader in the Cards & Payments, with 25 years of IT experience in the domain. He has established himself as a trusted advisor and strategist, working closely with a diverse range of stakeholders including banks, processors, networks, and industry product and platform providers across the globe. His extensive knowledge and expertise have enabled him to play a pivotal role in defining and executing strategies that drive innovation and efficiency within the industry.

For more information, contact askus@infosys.com

Infosys®
Navigate your next