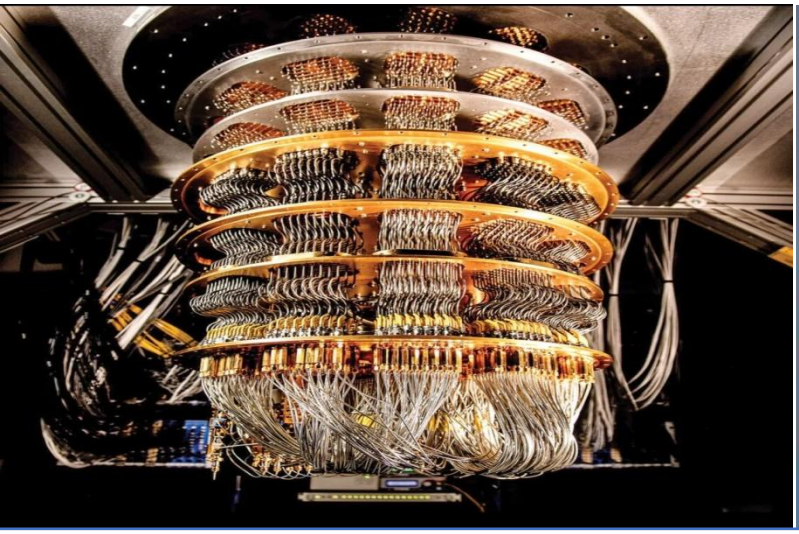
सत्यमेव जयते

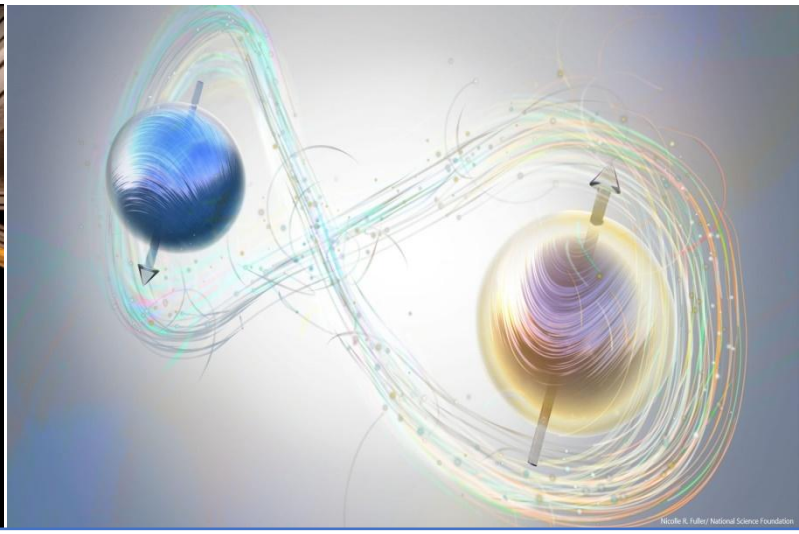
TECHNICAL REPORT

Migration to

POST QUANTUM CRYPTOGRAPHY

TEC 910018:2025





ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE

DEPARTMENT OF TELECOMMUNICATIONS

MINISTRY OF COMMUNICATIONS

GOVERNMENT OF INDIA

RELEASE 1.0 **JANUARY 2025**

Important Notice

Individual copies of the present document can be downloaded from **http://www.tec.gov.in**
Users of the present document should be aware that the document may be subject to revision or change of status.

Any comment/suggestions may please be sent to: ddgqt.tec-dot@gov.in

Disclaimer

The information contained in the report is compiled based on the contributions received from the member of the committee formed for this purpose. The report is based on the consensus built upon the contributions of the member deliberated on the subject in the multiple rounds of meeting.

डॉ. नीरज मित्तल, भा.प्र.से.
सचिव
DR. NEERAJ MITTAL, IAS
Secretary

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
Government of India
Ministry of Communications
Department of Telecommunications

MESSAGE

I am delighted that Telecommunication Engineering Centre (TEC), in collaboration with the subject matter expert from the Academia, Industry and Start-ups, has prepared technical report on ***Migration to Post Quantum Cryptography.*** This report will be useful for critical sectors like defence, financial services, healthcare, telecommunications, information technology, energy sector, etc.

The purpose of the report is to sensitize the organizations for identification of their critical digital infrastructures including data and applications which will be affected due to sudden deployment of cryptographically relevant quantum computers in the network anywhere across the globe. This report will also create sufficient executive awareness to pave way for proactive investments needed in the organizations to be prepared to respond adequately to the quantum threat.

The present day cryptographic standards used for purposes like encryption and digital signatures will be broken by cryptographically relevant quantum computers and put the entire digital infrastructure at risk. Therefore, there is an immediate and urgent need for organizations to prepare for dealing with the quantum threat by identifying their critical digital infrastructure including data and applications beforehand and be ready for a smooth transition to quantum safe cryptography

I appreciate the efforts of Telecommunication Engineering Centre in bringing out the report.

New Delhi
Dated: 26th March, 2025

(Dr. Neeraj Mittal)

कमरा नं. 210, संचार भवन, 20, अशोक रोड़, नई दिल्ली-110001 / Room No. 210, Sanchar Bhawan, 20, Ashoka Road, New Delhi - 110001
Ph. : +91-11-23719898, Fax : +91-11-23711514, E-mail : secy-telecom@gov.in

तृप्ति सक्सेना,
TRIPTI SAXENA
वरिष्ठ उप महानिदेशक एवं प्रमुख
Sr. Deputy Director General & Head

सत्यमेव जयते

भारत सरकार
दूरसंचार विभाग
दूरसंचार अभियांत्रिकी केंद्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली 110001
Govt. of India
Department of Telecommunications
Telecom Engineering Centre
Khurshid Lal Bhawan, Janpath, New Delhi-110001

Foreword

TEC has played a crucial role in the development of telecom ecosystem of India as the technical arm of Department of Telecommunications. TEC is committed to develop standards for the telecommunication sector in India, to ensure development of world class telecom network and smooth interconnection of individual networks.

TEC provides technical support to DOT and other government departments by formulating technical standards for telecom equipment, networks, systems and services to be deployed in Indian Telecom Network. TEC actively participates in the meetings of standards development organizations, viz., ITU, ETSI, APT, WRC, etc. These standards are made after wide stakeholder consultations. During formulation of above mentioned documents, 'Test Schedule Test Procedure' (TSTP) is also prepared to carry out testing and certification of the equipment.

To disseminate information and awareness about the latest developments in Telecom and IT domain, TEC regularly organise Webinars and release Study Papers. In this endeavour, Quantum technology division under TEC, DoT has prepared a technical report on migration to post quantum cryptography with active participation and contribution of subject matter experts from Academia, Industry and start-ups.

The report will be very useful to the enterprises and Government organisations in preparation of the migration strategy before deployment of quantum computers having high computing capacity in the network.

I wish all the best to the officers involved in releasing the report on the important subject.

Saxena

(Ms. Tripti Saxena)

ISO 9001:2015

दूरभाषा/Tel.:+91-11-23320252
ई-मेल/E-mail: srddg.tec@gov.in वेबसाइट/Website : www.tec.gov.in

List of Contributors

A. Approving Authority

Name	Designation	Organization
Ms. Tripti Saxena	Sr DDG & Head	TEC, DoT

B. Authors Committee

S.No.	Name	Organization
1.	Sh. Kamal Kr Agarwal, DDG (QT)	TEC, DoT
2.	Dr. Goutam Paul	ISI Kolkata
3.	Dr. Swagata Mandal	Jalpaiguri Government Engineering College
4.	Dr. Sucheta Chakrabarti	Former Scientist-G, SAG, DRDO
5.	Dr. Angshuman Karmakar	IIT Kanpur
6.	Sh. Vinayaka Pandit	IBM
7.	Sh. Bhupendra Singh	CAIR, DRDO
8.	Sh. B. Srinivas Goud	NCIIPC
9.	Dr. Shravani Shahapure	M/s Deloitte
10.	Sh. Rakesh Singh Rawat	C-DoT
11.	Dr. Roopika Chaudhary	DIT & CS, DRDO
12.	Dr. Mahavir Jhawar	Ashoka University
13.	Sh. Venkata Rama Raju Chelle, Director (QT)	TEC, DoT
14.	Sh. Rakesh Goyal, ADG	TEC

C. Editorial Team

Sl. No	Name	Organization
1.	Ms. Poonam Kumari, ADET (QT)	TEC
2.	Sh. Aryan Joshi, RA (QT)	TEC
3.	Sh. Adil Shaharyar, RA (QT)	TEC

Table of Contents

EXECUTIVE SUMMARY

This technical report is intended for the government organizations, industry and enterprises that are using digital infrastructure in their day-to-day operations to respond adequately to the emerging threat of cryptographically relevant quantum computers. The purpose of the report is to sensitize the organizations to identify their critical digital infrastructures including data and applications which will be affected due to sudden deployment of cryptographically relevant quantum computers in the network anywhere across the globe, and create sufficient executive awareness so as to pave way for proactive investments needed in those organizations to be prepared to respond adequately to the quantum threat The present day cryptographic standards used for purposes like encryption and digital signatures like RSA, ECDSA, ECDH, will be broken by cryptographically relevant quantum computers and put the entire digital infrastructure at risk. Therefore, there is an immediate and urgent need for organizations to prepare for dealing with the quantum threat by identifying their critical digital infrastructure including data and applications beforehand and be ready for a smooth transition to quantum safe cryptography. TEC acknowledge the contributions of academia, industry and startups in the preparation of the report.

Chapter – 1

1.1 Introduction

"*Quantum technology will permeate and impact every key sector of the economy and take us into a period likely to be referred to as the post-quantum era. This collectively creates an economic impact and a distinctive economic ecosystem, which we refer to as the quantum economy*, "by Dr. Arunima Sarkar, Thematic Lead for Quantum Technology at the World Economic Forum.

As per the Quantum economy blueprint released in January 2024 by the World Economic Forum, there is a $40 billion investment in quantum technology across the globe. According to McKinsey, quantum technology could be worth trillions of dollars within the next decade, with chemicals, the life sciences, finance, and mobility first in line to realize its benefits.

Quantum technology is based on the principles of quantum mechanics. Quantum computers, which are under development based on the principles of quantum mechanics, have the potential to provide exponential speed up for certain special classes of search and optimization problems. This is realised by exploiting the properties of superposition and entanglement of quantum bits used in quantum information processing. It is used in solving complex mathematical problems, the discovery of drugs, the study of subatomic particles, etc. Quantum sensors used to collect various data are better than the existing sensors.

Quantum communications ensure secure end-to-end communication quantum key distribution which is the only technique known to provide proof of network intrusion. On the other side, the advancement in the number and fault-tolerances of the qubits poses a threat to the existing cryptography, which may break the encryptions used in financial transactions or communication of critical information over the network by leveraging well known quantum algorithms by Shor and Grover. In the last two decades, new class of cryptographic algorithms have been developed, variously termed as quantum safe cryptography (QSC) and post-quantum cryptography (PQC) that are believed to be safe even in the presence of powerful quantum computers.

1.2 Threats to present cryptography system

Quantum computers while offering transformative benefits, also poses significant threat to the widely used in existing cryptographic standards like RSA, ECDSA, and ECDH by efficiently solving mathematical problems like integer factorization and discrete logarithms using the famous algorithms by Shor and Grover.

The impact of the quantum threat will lead to

a) **Data Breaches:** Sensitive health records, financial data, and cat memes—could be breached.
b) **Document Integrity:** Digital signatures, contracts, and even your grandma's secret cookie recipe—tampered with.
c) **Cryptocurrency**: Bit coin, Ethereum, and their crypto pals—exposed like a magician revealing tricks.

1.3 Post Quantum Cryptography

This evolving landscape necessitates a paradigm shift in the cryptographic practices, with a focus on development and migrating to Post-Quantum Cryptography (PQC) algorithms specifically designed to withstand the computational power of quantum computers. These algorithms rely on mathematical problems, such as lattice-based, hash-based, and multivariate polynomial cryptography, which remain resistant to both classical and quantum attacks.

1.4 Standardisation of PQC algorithms

The development and standardization of Post-Quantum Cryptographic algorithms has been led by National Institute of Standards and Technology (NIST) - a process that started in 2016 with roughly 80 entries and eventually resulted in the publishing of three standard algorithms through four rounds of progressive elimination. In August 2024, NIST finalized First 3 Post-Quantum Cryptographic (PQC) Standards as below:

a) **FIPS 203 (CRYSTALS-Kyber)**, a lattice-based cryptographic algorithm designed as quantum-secure key exchange algorithm to replace existing quantum-vulnerable key exchange algorithms such as RSA, ECC etc.
b) **FIPS 204 (CRYSTALS-Dilithium)**, a lattice-based cryptographic algorithm designed to protect the digital signatures we use when signing documents remotely
c) **FIPS 205 (SPHINCS+)**, a stateless hash-based algorithm designed for digital signatures.

Type	Algorithms	Family	Derived from	Standard
Key Encapsulation Mechanism	Module-Lattice-Based Key-Encapsulation Mechanism Standard	Lattice	CRYSTALS-KYBER	FIPS 203
Digital Signature	Module-Lattice-Based Digital Signature Standard	Lattice	CRYSTALS-Dilithium	FIPS 204
	Stateless Hash-Based Digital Signature Standard	Stateless, hash-based	SPHINCS+	FIPS 205

In the Indian context, a natural question that arises is whether we should have an independent standardisation effort. This question is particularly important because of the time, effort, and cost involved in conducting such an exercise. The Kerckhoffs's principle in cryptography states that the security of a cryptosystem should arise from the secrecy of the keys used rather the secrecy of the algorithm. As the NIST exercise conducted an elaborate, multi-round assessment of the strength of the algorithms against both quantum and classical adversaries, we should adopt the standardized algorithms in the interest of avoiding duplication of efforts. However, the local

organizations should be provided with guidance on the process that they or their technology vendors should use to ensure that generation of the keys and randomness used in the algorithms are not compromised.

1.5 Migrating to Post-Quantum Cryptography

The most immediate threat to the presently secure data is “Harvest Now, Decrypt Later” attacks which intercept and store encrypted data now and recover the key to decrypt by using the strength of quantum computer, when it would be developed in future. This attack demonstrates the vulnerability of the systems which store confidential information for long periods of time, such as banking data or medical records. To mitigate the threat of these attacks based on quantum computers, we need to migrate to PQC inevitably. Compared to Quantum Key Distribution (QKD), PQC is a much less costly and yet effective solution for converting the existing Public Key Infrastructure (PKI) to post-quantum PKI.

Chapter – 2

Quantum threats and Impact

2.1 Introduction to quantum threats

This chapter outlines the immediate threats posed by quantum computers, the consequences of delays in transitioning to PQC, and the importance of developing a cryptographic inventory to assess and categorize cryptographic artefacts present in the digital infrastructure of organizations. By evaluating the quantum threat timeline and organizational readiness, businesses can mitigate risks and ensure data security in a post-quantum world. Early action is essential to protect against data breaches, compliance issues, and reputational damage.

2.2 Immediate Threat

It is important to note that much of the external traffic of any organization, even if it is secured through current encryption standards, is vulnerable for attacks by quantum adversaries. Specifically, the concept of a “harvest now, decrypt later” attack presents an immediate threat. Even though quantum computers have not yet reached the capability to break current cryptographic algorithms, adversaries could be gathering encrypted data now with the intention of decrypting it when quantum capabilities mature. This implies that data encrypted today could become vulnerable in the future, irrespective of when quantum computers become operational.

The organizations continue to depend for a longer period on classical cryptographic systems, the larger the volume of potentially vulnerable data that adversaries could harvest. This creates a cumulative risk where each day of delay increases the amount of data that might eventually be compromised. Furthermore, once data is harvested, an organization loses control over it. Even if a transition to PQC occurs later, any previously harvested data remains at risk of future decryption. In essence, any delay in migrating to post-quantum cryptography is inherently risky.

2.3 Type of attacks

2.3.1 Man-in-the-Middle Attacks

Man-in-the-middle (MITM) attacks involve intercepting and altering communications between two parties without their knowledge. With quantum computing, an attacker can break RSA encryption and decrypt the intercepted messages in real-time. This allows the attacker to impersonate the legitimate parties and modify the communication.

2.3.2 Individual Attacks

Hackers can target high net worth companies and individuals by compromising the bank's RSA encryption using quantum computing. Once the encryption is broken, the attacker can access sensitive information such as account details, transaction history, and personal data.eg brute force attack may be initiated by the group of the people, nation etc. structural attack; exploiting the weakness of the cryptographic algorithms.

2.3.3 Threat to Digital Signatures

Digital signatures are used extensively in financial transactions to authenticate the identity of the signatory and ensure the integrity of the transaction data. Quantum computers could potentially break the RSA encryption underpinning these digital signatures, leading to several risks:

2.3.3.1 Forgery

Attackers could forge digital signatures, making it appear as authorized transactions were conducted.

2.3.3.2 Unauthorized Transactions

Malicious actors could approve unauthorized transactions, leading to financial losses for individuals and institutions.

2.3.3.3 Data Integrity

The integrity of transaction data could be compromised, making it difficult to trust the validity of financial records.

2.4 Impact: Potential Damage from Quantum Attacks

The threat from Cryptographically Relevant Quantum Computer (CRQC) can lead to:

2.4.1 Damage to Reputation and Trust

Internal breaches have the potential to undermine customer confidence in the bank's internal security measures. For instance, if it were to be disclosed that a significant bank's encryption system had been breached, enabling unauthorized individuals to access or modify transactions, and customers may hastily decide to withdraw their funds or terminate their accounts.

2.4.2 Monetary Damage to Banks

The bank could incur costs due to the breach, including investigation, remediation, and potential fines. Example: A coordinated attack exploiting compromised RSA could lead to millions or even billions in fraudulent transfers of money before detection.

2.4.3 Monetary Damage to Customers

Customers could be victims of fraud, leading to financial losses.

2.5 Assessing the Delay

Assessing the delay in migrating to PQC involves assessing both the timing of quantum threats and the organization’s readiness to adopt post-quantum solutions. The evaluation process can be approached as follows:

a) **Assessing the Quantum Threat Timeline:** Continuous monitoring is essential, focusing on the following aspects:

i. Progress in quantum computing research, especially advancements in the development of Cryptographically Relevant Quantum Computers (CRQC) capable of breaking current cryptographic algorithms.

ii. Progress on minimizing the number of qubits and quantum logic gates required by quantum algorithms for important problems like integer factorization and discrete log.

iii. Expert forecasts on when quantum computers might become a credible threat to classical cryptography. These estimates can range from 5 to 120 years, but the inherent uncertainty necessitates on-going vigilance. To illustrate, consider a bank that has not yet begun its PQC migration. By evaluating the progress of quantum computing research, the organization can gain insights into the potential risks of delay.

b) **Evaluating Organizational Readiness:** While the quantum threat timeline provides a window of opportunity, an organization's resources and readiness might not align with this duration. Key factors to assess include:

c) **Migration Roadmap:** Review the organization's plan for adopting PQC algorithms, including timelines for system upgrades, testing new algorithms, and personnel training.

d) **Resource Allocation:** Consider the resources (financial, technical, and human) dedicated to the migration effort. Delays can arise if the organization lacks sufficient resources or if there are competing priorities.

e) **Interdependencies:** Identify dependencies on third-party vendors or systems that also need to transition to PQC, as these could cause delays in your migration efforts.

2.6 Risk of Delay: Impact Analysis

Evaluating the potential consequences of a delayed migration is crucial, particularly if quantum threats materialize before the complete migration. This scenario presents risks of data exposure, compliance issues, and reputational damage. The impact could be significant, depending on the cryptographic landscape within the organization. It is therefore essential to assess the organization's understanding of where and how classical cryptography is used across its systems and to identify which systems are most at risk. This involves allocating resources to develop a comprehensive cryptographic inventory. A cryptographic inventory is a strategic cyber security asset that enables an organization to enforce a secure cryptographic policy across its IT infrastructure, respond quickly to security issues, and efficiently carry out strategic transformations, such as deploying PQC. A cryptographic inventory typically includes a list of algorithms and keys used in applications and infrastructure. The details will depend on the inventory's specific goals. For example, if the goal is to prepare for PQC migration, the inventory should distinguish between cryptographic algorithms that are vulnerable to quantum attacks and those that are not. The inventory must also list the applications and protocols that utilize these algorithms. In an organization, cryptography can be broadly categorized into application

cryptography and infrastructure cryptography, helping to distinguish between different layers and purposes of cryptographic implementations.

2.6.1 Application Cryptography

Application cryptography focuses on securing specific applications or software within the organization. It involves the implementation of cryptographic functions directly within the applications that users interact with. Examples include:

a) Encrypting data stored in databases or files by the application, ensuring that sensitive data is protected from unauthorized access.
b) Using Message Authentication Codes or digital signatures within applications to ensure data integrity and authenticate the sender.
c) Implementing SSL/TLS within web applications to secure
d) HTTP communications, protecting data in transit
e) Employing cryptographic methods like password hashing, multi-factor authentication, and token-based authentication within user-facing applications.

Common usage scenarios include web and mobile applications that require user authentication and secure transactions, secure email and messaging applications where end-to-end encryption is necessary and financial applications where data integrity and non-repudiation are critical.

2.6.2 Infrastructure Cryptography

Infrastructure cryptography secures the broader IT infrastructure within the organization, including networks, hardware, and system-level processes that form the backbone of the IT environment. Examples include:

a) VPNs (Virtual Private Networks): Encrypting traffic over the network to secure remote access to the organization’s internal resources.
b) Disk Encryption: Implementing full-disk encryption on servers and workstations to protect data from physical theft or unauthorized access.
c) Secure Network Protocols: Utilizing protocols like IPSec, SSH, or SSL/TLS at the network level to protect data in transit across internal or external networks.
d) Public Key Infrastructure (PKI): Managing digital certificates and keys that are used for various cryptographic functions across the infrastructure, such as secure email, code signing, and VPN access.
e) Hardware Security Modules (HSMs): Using dedicated hardware devices to generate, store, and manage cryptographic keys securely.

Chapter-3

PREPARATION OF THE MIGRATION PLAN

3.0 INTRODUCTION

In this chapter, we explore the importance and need to migrate to PQC (a solution of Quantum safe cryptography). Here we describe the migration plan to PQC for the organizations at the earliest to prevent from quantum threats and vulnerabilities of long time valuable non-PQC encrypted sensitive data.

3.1 When and how to migrate?

As of now, quantum computers with sufficient qubits to break RSA-2048 do not yet exist. The largest quantum computers available today have hundreds of qubits, but these are mostly noisy intermediate-scale quantum (NISQ) devices, which are not yet capable of running error-corrected algorithms like Shor's at the scale needed for RSA-2048. To implement Shor's algorithm, it is estimated that the number of **logical qubits** needed to break RSA-2048 vary, with the most optimistic estimate being about 6000 logical qubits. It is extremely difficult to predict future technological developments of quantum computers so that RSA-2048 will be compromised. Some leading experts estimate that there is a likelihood of 50% or more that RSA-2048 will be broken by a quantum computer in 5 to 10 years' time. The migration time frame has to be estimated by the individual organization based on Mosca-theorem also known as Mosca Model. It explained as follows by considering the parameters given below:

a) How long do one need encryption to be secure? (X years i.e. Security shelf life)
b) How long will it take to migrate a large-scale quantum-safe solution into current infrastructure? (Y years i.e. Migration time)
c) How long will it take to develop a large-scale quantum computer or any other significant development? (Z years i.e. Collapse time)

Now if X + Y > Z then organization will be at risk to compromise the secure data.

Migration to PQC involves the following steps:

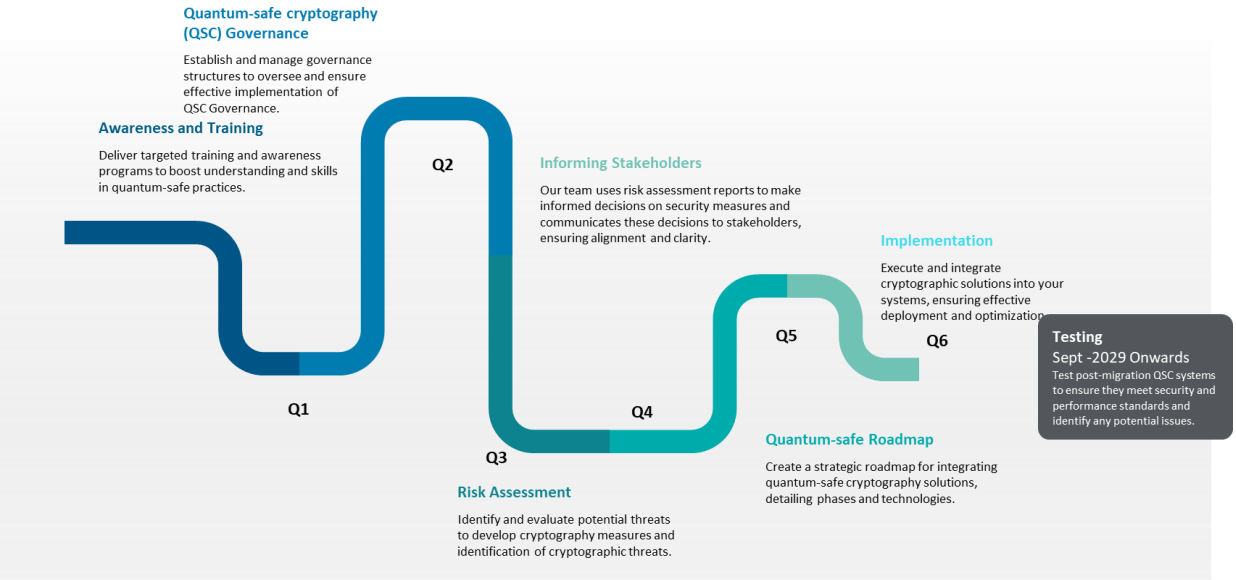


Fig.1

The above diagram illustrates the roadmap for migration to PQC.

a) **Awareness and training:** Many organisations are unaware of the threat from Quantum. The lack of a cryptographic skill set aggravates this problem. Awareness and training are crucial steps in the migration roadmap. It is necessary to give an understanding to key stakeholders of the organisation about the Quantum threat, timeline and cost involved in the migration.

b) **Quantum safe cryptography governance:** As Quantum is in the developing stage, monitoring developments around weak cryptographic algorithms, new cryptographic standards, updating cryptographic policies based on the organisation's requirements, and continuous monitoring of the progress of migration are essential to keeping the organisation safe. The Quantum safe cryptography governance team will help achieve all the cryptography governance tasks.

c) **Risk Assessment:** Before migrating to Quantum-Safe cryptography, it is essential to understand the current cryptographic posture of an organisation. Creating the cryptography inventory will give the visibility to develop the migration roadmap

d) **Quantum Safe migration road map:** Once the organisation has visibility on cryptography, the next step is to develop the migration roadmap. It will cover the short-term, mid-term, and long-term plans along with budget requirements.

e) **Implementation:** The implementation phase is crucial for successful migration. When choosing a product, it is necessary to understand the product's need for the organisation, crypto-agility level, testing, and benchmarking certificate. Rushed migration can create more vulnerability in the existing digital ecosystem of organisations, which will bring catastrophe.

f) **Testing:** As new PQC algorithms are operationally heavy, they may impact the organisation's key operations. It is essential to continuously test new products or updated products and monitor their performances.

3.2 Migration issues and evaluation

There are eight critical factors that must be considered in the migration issues and evaluation.

a. **Bandwidth:** The public keys of CRYSTALS-Kyber (6,000 bit) and CRYSTALS-Dilithium (10,000 bit) are several times larger than the ones of RSA and Diffie-Hellman (2,048 bit). Other proposed post-quantum algorithms even require hundreds of thousands of public-key bits more. Even for private keys, similar size enhancement would happen to resist quantum search. As a consequence, data traffic and latency increase. To avoid the impact on network performance, one must ensure one's network can handle the additional load. This might require upgrading your network infrastructure, optimizing data flow, and possibly increasing bandwidth capacity.

b. **Storage:** As PQC algorithms come with larger key sizes, PQC certificates will require more storage space. One may need additional storage for maintaining hybrid and traditional cryptographic systems during the transition. One needs to evaluate existing storage solutions and plan for expansions to accommodate the increased data volume. It is to be ensured that data backup and recovery systems can manage the larger volumes efficiently.

c. **Protocols:** Existing communication protocols, such as TLS, SSH, S/MIME, and IPsec, must be updated to support PQC algorithms. This includes configuring the existing protocols to use PQC algorithms for key exchange and signature mechanisms. One needs to do a comprehensive review of the existing protocols, conduct rigorous testing, and plan for any changes to the underlying infrastructure to ensure secure communication.

d. **Application Software Upgrades:** Existing software may require extensive modifications to ensure compatibility with PQC libraries and protocols. This process can be complex and time-consuming. Start by building a comprehensive inventory of existing cryptography and associated applications and software. Identify mission-critical assets that need to be migrated on priority. Thoroughly test and validate PQC algorithms in these entities to prevent service disruptions and ensure security.

e. **Hardware Upgrades**: Post -quantum cryptography can impose greater demands on processing power, necessitating hardware upgrades. One may have to invest in new servers and processors that can handle the increased computational load and specialized hardware accelerators to optimize performance. Additionally, one may have to update or replace hardware security modules (HSMs) that currently support classical cryptographic algorithms with models supporting post-quantum algorithms.

f. **Third-Party Applications and Services:** If an organization relies on third-party vendor technology, applications, and services, such as email and VPNs, they must ensure that they support post-quantum cryptography. They should engage with their vendors to understand their PQC integration roadmap and timelines. They should work with them to get new products/applications delivered with PQC built-in and legacy ones upgraded with PQC.

This collaboration is essential to address the performance impact and interoperability issues that may arise during or after PQC migration.

g. **Standards and Guidelines:** Compliance with emerging PQC-related RFCs, Standards and guidelines will be a crucial step in the transition process. One will need to integrate and maintain up-to-date PQC libraries and random number generators (RNG), as per emerging standards from bodies such as the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI). Adhering to these standards ensures interoperability and security across different systems and platforms.

h. **Regulatory Compliance:** Re Regulatory bodies will likely update compliance requirements to include post-quantum cryptographic standards. One needs to ensure that the cryptographic practices align with new regulations and standards related to PQC. This involves updating compliance policies, conducting regular audits, and maintaining documentation to demonstrate adherence to post-quantum security standards.

3.3 Cryptographic primitives Quantum-Secure Transition Framework

Here's a table that lists some well-known standard cryptographic algorithms, used for public key encryption, symmetric key encryption, hash functions, MACs, and signature schemes.

Type	Functionality	Recommended
Symmetric	Block Cipher	AES-256
Symmetric	Stream Cipher	ChaCha20 with 256-bit key
Asymmetric	Public-Key Encryption/KEMs	FIPS-203 (CRYSTALS-KYBER)
Asymmetric	Digital Signatures	FIPS-204 (CRYSTALS-Dilithium)
Hash Functions	Hashing	At least SHA-3-256 or SHA-256
Message Authentication Code (MAC)	Block Cipher Construction	Cipher-based MAC (CMAC)-AES-256
Message Authentication Code (MAC)	Hash Constructions	Hash-based MAC (HMAC) with at least SHA-256 or SHA-3-256
Message Authentication Code (MAC)	Universal Hashing	Poly1305-AES, ChaCha20-Poly

3.4 Trust management during migration _Hybrid Solution approach

During the migration process to quantum safe PKI before finalization of standard PQC profile and tested widely after implementation of PQC algorithms, the users need to be assured the security strength against all possible threats scenarios. In this direction Hybrid solution (combination of classical asymmetric key and PQC algorithms) is one of the best solutions.

A hybrid solution is a solution where multiple algorithms, classical and quantum-safe are used in parallel. When migrating, there are two reasons for combining classical algorithms with quantum safe ones:

a. **Assurance of cryptographic strength:** The new, supposedly quantum-safe algorithms have received much less analysis by the cryptographic community than the classical ones, simply because they are newer. Therefore, the assurance that they are indeed safe algorithms is lower, and will remain so until after more years of analysis. As long as the quantum computer has not yet arrived, the classical algorithms can function as fall-back solutions in case flaws are discovered in the new algorithms. The resulting solution will at least have the strength of the classical algorithms.

b. **Backward compatibility:** Communication parties that have already migrated to quantum-safe algorithms can use that solution; the ones that have not, can use the classical algorithms. This needs to be done in cases where a 'big bang' introduction of quantum-safe crypto is not possible. An example is a Public Key Infrastructure where some parties take longer to implement new crypto than others. Also, the replacement of all client applications that use PKI will not be possible in a single go.

When using a hybrid solution, care must be taken to do this in a correct way. This is described in two examples below, for key establishment solutions and for signatures.

For key establishment:
For key establishment of a session key, a possible solution is as follows. The two communicating parties carry out both a classical key establishment protocol and a quantum-safe one. If more assurance is desired, multiple different quantum-safe algorithms can also be used. Then the session key is derived by both parties from the determined keys by applying a Key Derivation Function (KDF) on them, for example a cryptographic hash functions, as shown in Figure 2 below.

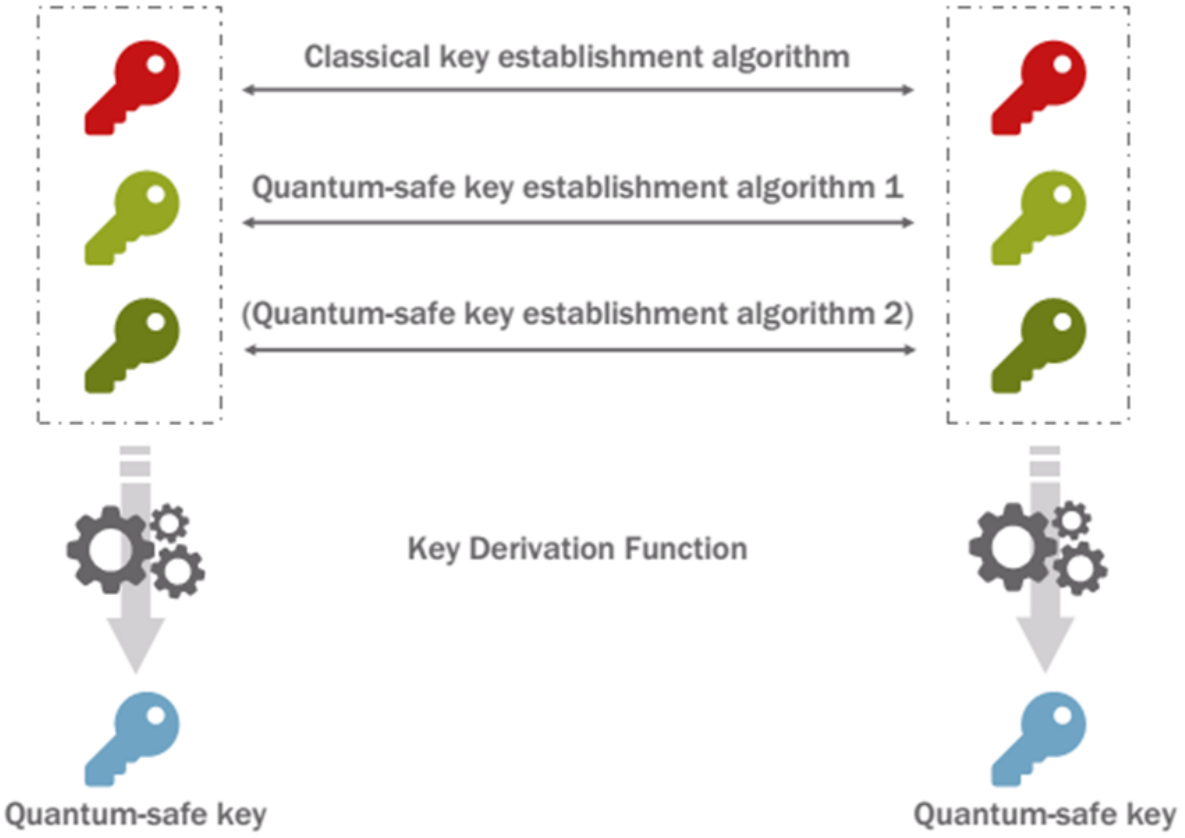


Figure 2: Hybrid encryption for key establishment

Even though part of the input of the KDF is generated using a classical algorithm, the resulting key is quantum-safe. This key therefore provides post-quantum security, yet it at least provides the strength of the classical algorithm, if the quantum-safe algorithms later prove to be insecure. The key thus has at least the strength of the strongest algorithm of the three.
The classical algorithm can also provide backwards compatibility; all parties that have not yet migrated can carry out the key establishment using only the classical cryptography. Note that care must be taken to avoid downgrade attacks, attacks in which a man-in-the-middle manipulates the messages to force the receiver to use the weaker security of a classical algorithm, while both sender and receiver are actually able to use quantum-safe cryptography.

For signatures:

For signatures, important properties of the hybrid solution are that they must be both unforgeable and non-separable. The first property means that an attacker must not be able to generate signatures without knowledge of both private keys, the one for the classical algorithm and the one for the quantum-safe algorithm. The second property means that it must not be possible for an attacker to separate the classical signature from the quantum-safe one, and pretend to the receiver that the signer only used classical cryptography; this is a downgrade attack.

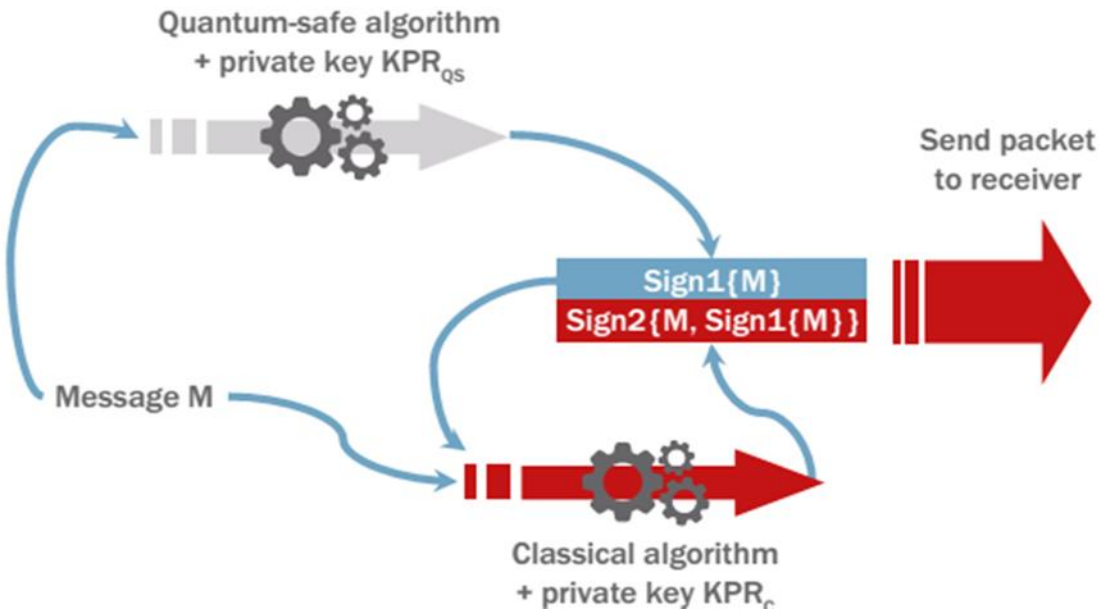


Fig 3: Hybrid signature scheme

In Fig 3, a scheme is presented in which the two mentioned properties of unforgeability and non-separability can be achieved.

The message M is signed with a quantum-safe algorithm; this is signature Sign1 in the figure 3. Then this signature Sign1 together with (again) the hash value of the message M is signed with a classical algorithm; the result is signature Sign2.

The signatures on message M can both be checked with:

1. The public key of PQC algorithm corresponding to the private key of PQC algorithm KPRQS used for signing with the quantum-safe algorithm (signature Sign1, blue part), and
2. The public key of classical asymmetric key algorithm corresponding to the private key KPRc used for signing with the classical algorithm (signature Sign2, red part).

The signature Sign2 provides backwards compatibility; all parties that have not yet migrated can check the signature Sign2 using classical cryptography. Note that this part also provides the non-separability, as by the structure it can be recognized that, besides the message M, a signature Sign1 is also involved, the quantum-safe one. An attacker will thus not succeed in making the verifier believe (in a downgrade attack) that only classical cryptography was used. The signature Sign1 provides post-quantum security. Yet signature Sign2 provides the strength of the classical algorithm, if the quantum-safe algorithm later proves to be insecure. This mechanism thus has at least the strength of the strongest algorithm of the two.

Till the CRQC matured enough to break the classical public key algorithms, during the migration process hybrid solution really provides the trust to the user.

3.5 Isolation approaches during migration

Not all systems will be updated at the same time. As a part of a migration strategy sub-systems should be isolated as far as possible to discrete security domains. Security domains that need to be interconnected may then be interconnected by Quantum Safe pathways, such as quantum-safe VPN. A quantum-safe VPN is a network security measure that uses Post Quantum Cryptography (PQC) to enhance encryption levels. PQC uses unique algorithms to encode data, which makes it more difficult for quantum computers to break encryption. A quantum-safe VPN can create an encrypted tunnel between the sender and receiver. Thus, it will safeguard the data.
In some scenarios, physical separation/isolation might be desired or required to prevent unauthorized access to critical information in a post-quantum world. If possible, keep most critical data from being eavesdropped on. This means off the network, and especially Wi-Fi networks, in particular if those Wi-Fi networks are contactable remotely from public areas. Remember, most existing Wi-Fi networks are not quantum resistant without additional remediation.

3.6 Access to non-QSC protected resources after migration

It may not be economically feasible to migrate all encrypted assets to a QSS. Non-QSC assets should be physically moved to explicitly identified quarantine zones where they can be managed risk free.
If any form of PKI and associated PKCs has been used to maintain any non-migrated assets then a reasonable facsimile of the PKI will be maintained in the quarantined zone. There is a strong likelihood that certificates and associated public keys used in protecting such assets will expire whilst in the quarantine zone. In that scenario, appropriate processes should be put in place to allow the cryptographic operations to continue even if normal protocols and policies fail.

3.7 Migration to quantum-safe cryptographic protocols

A non-exhaustive list of much-used protocols and programs containing asymmetric cryptography is the following: TLS, SSL, HTTPS, IPsec, IKE, X.509 certificates, SSH, S/MIME, PGP/GPG, DNSSEC, ZRTP, DSS, PCIDSS, signatures of apps and Federated Authorization must be updated to support PQC algorithms. This includes configuring the existing protocols to use PQC algorithms for key exchange and signature mechanisms. One needs to do a comprehensive review of the existing protocols, conduct rigorous testing, and plan for any changes to the underlying infrastructure to ensure secure communication. Regarding TLS, RFC 8784 [IETF-IKEv2-mixing] describes the mixing of pre-shared keys into IKEv2. Furthermore, IETF draft [IETF-TLS-hybrid] has been proposed to standardize the methods of hybrid key exchange used in TLS 1.3. Similarly, an IETF draft [IETF-IKEv2- hybrid] describes the use of hybrid key exchange methods in IKEv2, as used to establish shared keys in IPSec VPNs.

Chapter-4

IMPLEMENTATION OF PQC MIGRATION PLAN

4.1 Implementation of PQC migration

4.1.1 Recommended Quantum-Readiness Best Practices and technologies

a) To understand the risks that quantum computing advancements will pose to their - Information Management (IM), Information Technology (IT) and Operational Technology (OT) systems and data; and
b) To plan how to manage the risks to their quantum-vulnerable systems by transitioning those systems and important data assets to introduce support for standardized quantum-resistant cryptography
c) Recommended actions that can be started now include the following steps:
    i. Educating your peers and your teams on the emerging quantum threat and the new technologies for quantum-safety including hybrid cryptography and cryptographic agility.
    ii. Evaluating the sensitivity of your organization's information assets and determining their lifespans to identify information that may be at risk (e.g., as part of on-going risk assessment processes).
    iii. Inventorying the IM, IT and OT systems in your organization that use cryptography, and then implementing new policies and procedures in your change management activities to maintain this inventory on an on-going basis.
    iv. Asking the vendors of your cryptographic products if they support cryptographic agility, as well as when and how they will implement standardized and validated quantum-safe cryptography.
    v. Talking to your business partners and other third-party suppliers about their current PQC posture and timelines for quantum-safety.
    vi. Budgeting for potentially significant software and hardware updates, as the timeframe for necessary replacement approaches.
    vii. Updating your IM, IT, and OT life-cycle management plans to explicitly describe how and when your organization will implement post-quantum cryptographic algorithms to protect your most important data and systems when validated cryptographic modules become available.

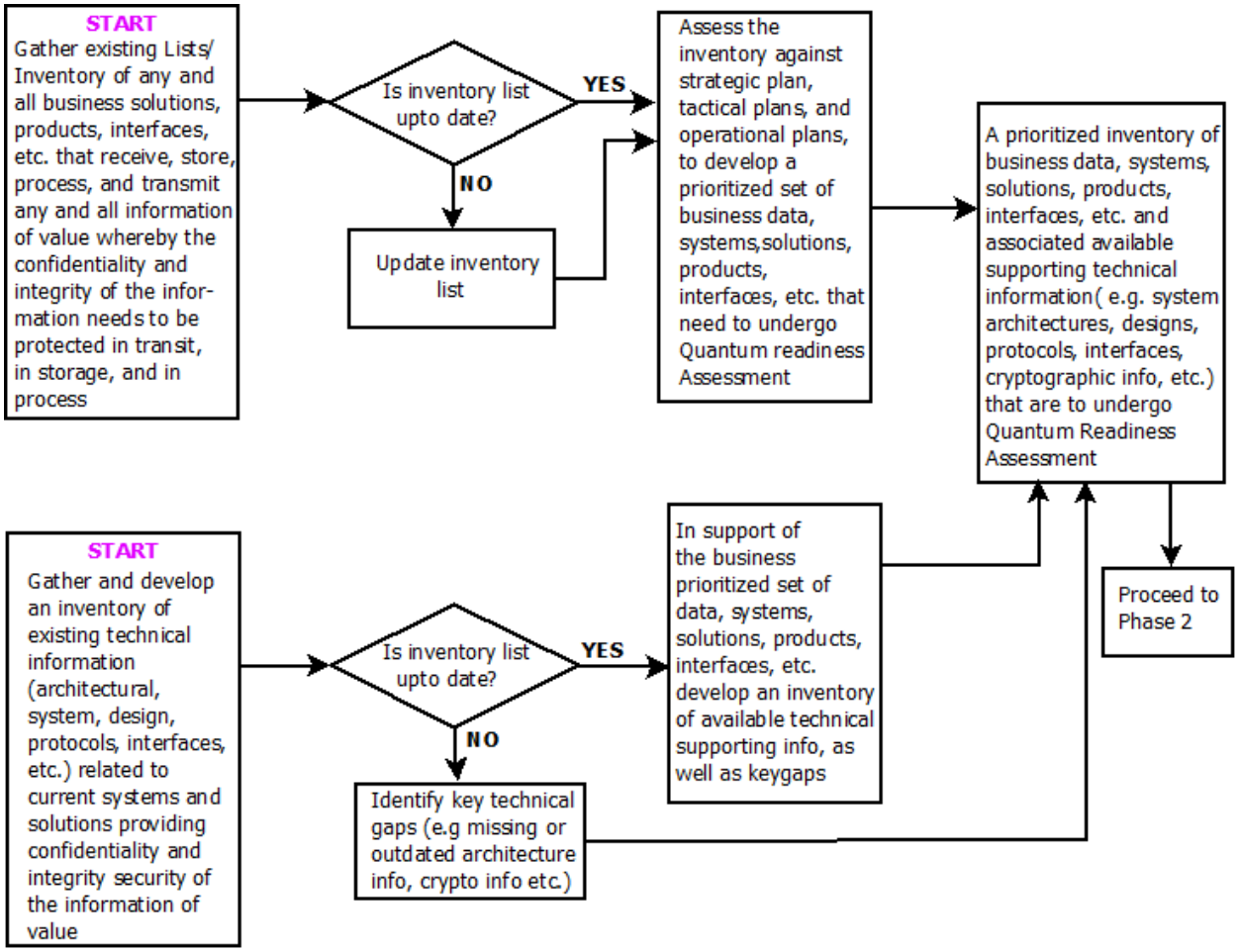
4.1.2 Quantum-readiness program elements

With respect to organizing these recommended actions into a Quantum-Readiness program, a multi-year and multi-phase timeline is recommended, as described below:

a. Preparation: Develop an understanding of the threats that quantum computing will pose to the f ICT infrastructure of the organisation in the coming years.
b. Constitute a team to investigate the scope of the effort that will be needed for your organization to start using standardized and new "quantum-resistant" cryptography in the

coming years, and to identify which of your IM, IT and/or OT systems may need be remediated first.

c. Review the progress of #b and decide when to advance to Phase 1 (Discovery)
d. Discovery: The goal is to discover where and how cryptographic products, algorithms and protocols are used by your organization to protect the confidentiality and integrity of your organization's important data and digital systems.
e. The information collected during this phase will be needed to assess your organization's quantum risks in the next phase
f. Appoint and empower someone to plan and execute a detailed discovery of where and how public-key cryptography is used in the organization.
g. Investigate whether using automated tools would facilitate the crypto discovery. Organizations should balance their security needs with their needs for usability and availability when considering such automated tools.
h. Build an inventory of where and how the organization uses public-key cryptography to protect its most important data and IM, IT and OT systems. Also identify any legacy cryptographic systems being used.
i. Identify the important factors in which public-key cryptography affects the operation and security of organisation's systems and applications (e.g., key sizes, latency and throughput limits, current key establishment protocols, how each cryptographic process is invoked, dependencies).
j. Analyse the findings from #h and #i to develop a prioritized list of the organization's most important quantum-vulnerable systems that must be protected.



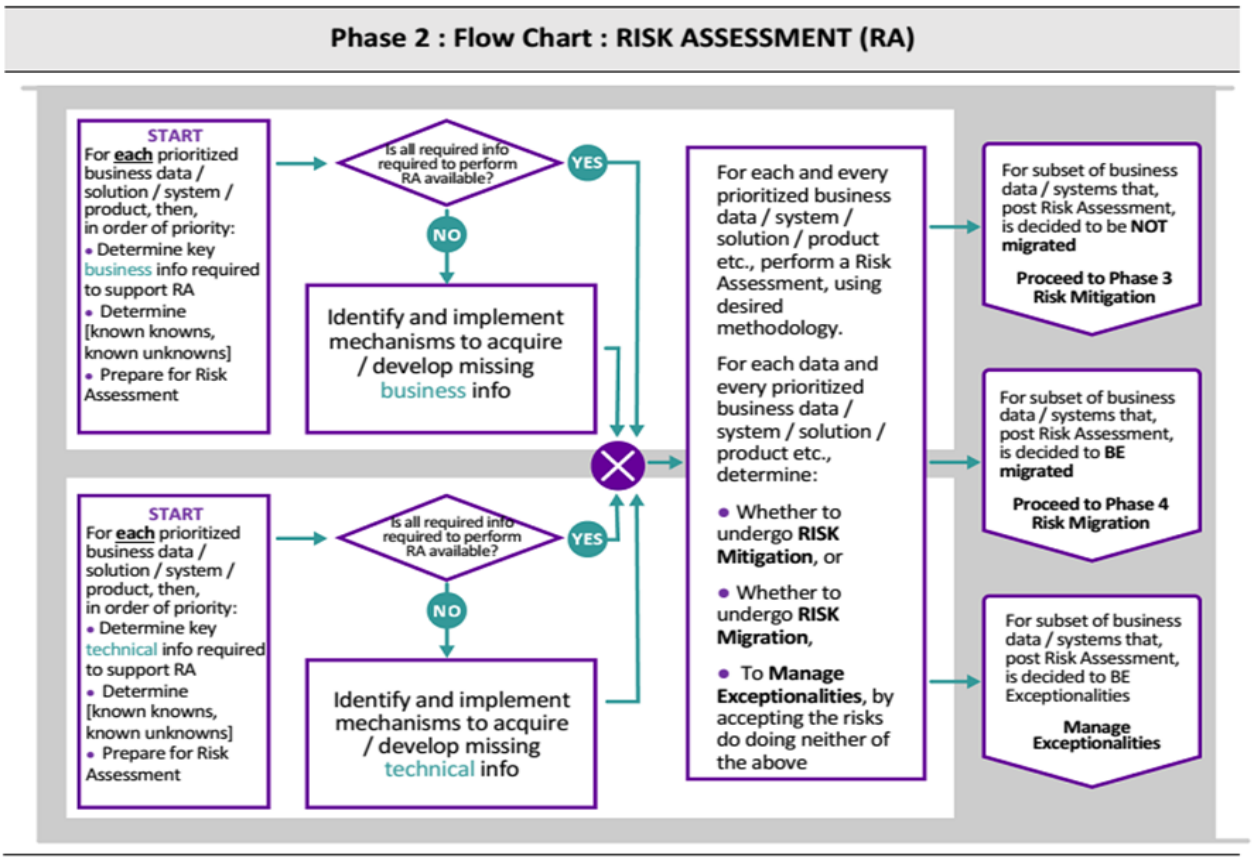
Phase 1 : Flow Chart : DISCOVERY

4.1.3 Risk Assessment

a. Evaluating the sensitivity of an organization's information and determining its lifespan to identify the information that may be at risk (e.g. as part of on-going risk assessment processes).
b. Educating the teams on the threats that quantum computing will pose to the organisation's existing uses of cryptography.
c. Asking the IM, IT and OT vendors and suppliers about their plans and timetables to implement quantum-resistant cryptography and crypto-agility, to understand any new hardware or software that will be needed.
d. Reviewing the organisation's IT lifecycle management plans and budgeting for potentially significant software and hardware updates.
e. Start the Quantum Risk Assessment by reviewing the quantum risk equation, and the inventory of information discovered in Phase 1. That information is needed to determine the following variables for each of the digital systems that handle or store the organization's most sensitive information: shelf-life time, migration time.
f. Decide how the currently anticipated quantum threat timeline affects the organization's risk posture.

g. Evaluate the sensitivity of the organization's information and determine its lifespan (i.e., the shelf-life time that your most important data must be protected) to identify information that may be at risk.
h. Review the technology lifecycle management plans for each of the quantum-vulnerable systems identified in Phase 1 and ask IM, IT and OT vendors if their product development roadmaps include supporting crypto-agility and/or quantum-resistant cryptography in future updates. If yes, ask when those capabilities will be available.
i. Using the information from the previous step, estimate the migration time (measured in years) that the organization will need to migrate each of the systems that handle the longest shelf-life data.
j. Prioritize the systems that will need the most urgent attention, by listing all of the systems that handle important data for which:

   Migration Time + Shelf-life Time > Threat Timeline



4.1.4 Validation

The implementation of the PQC algorithms shall be validated in the test environment before implementation.

a) **Use of Tools and Technology:** It is important to use state of the art tools and technologies available for implementing the above steps in an automated, repeatable, and scalable manner. Some of the keep tools that have been developed by technology pioneers in the field are as follows:
   i. **Scanners:** There are three types of scanners that are important for an organization. They are scanners for source code, binaries, and IT infrastructure deployments. Typically, scanners for source code and binaries detect the use of different cryptographic algorithms and protocols in software. They are needed by independent software vendors to assess potential quantum vulnerabilities in the software that they deliver to clients. Scanners for cryptographic artefacts like certificates and keys that are stored in the infrastructure to be used during communication are required by the IT Operations teams to understand their cryptographic posture.
   ii. **Cryptographic Bill of Material**: Tools that represent the information discovered by the different scanners in the form of a standardized bill of cryptographic materials (i.e. the crypto inventory) so that they can be shared with technology vendors and partners.
   iii. **Threat Assessment Tools** – Tools that analyse the different components of a crypto inventory from the perceptiveness of weakness of algorithms, keys, and dependencies to present a picture of the threats faced by an organization.

b) **Change Management:** It is important to recognize that the entire process of PQC Readiness and Migration is that of a large scale change management involving an organization, its technology vendors, and business partners. Therefore, it is as important to have people with significant experience and expertise in change management as it is to have the people with the right technical skills.

4.2 Implementation roadmap (crypto-agility and PQC implementation)

4.2.1 Crypto-agility

Crypto-agility, or cryptographic agility, is a data encryption practice used by organizations to ensure a rapid response to a cryptographic threat. The idea is to adapt to an alternative cryptographic standard quickly without making any major changes to infrastructure.

Typically, crypto-agility is used when the encryption algorithm of a system is discovered to be vulnerable. Other use cases include when an algorithm breaks suddenly or when there's a security compromise. If one of these cases arises, an organization needs to be able to switch to using a different encryption method quickly to minimize damage. This process includes switching out cryptographic algorithms, security keys, certificates and other crypto technologies.

4.2.2 Importance of crypto-agility

Cryptographic techniques don't stay secure forever. For example, increasing computing power also leads to the increased ability for hostile programs to successfully break previously secure

cryptographic functions. Before this happens, previous cryptographic systems -- such as public key encryption, key exchange and digital signatures -- must be switched over to new encryption systems to stay secure. Crypto-agility is also a relatively sustainable practice, meaning this process won't become a liability. One of the main strengths of quantum computing is its power to crack classic crypto systems. As a result, quantum computing is beginning to pose a threat to modern cryptography. Just having one enterprise encryption strategy isn't viable if an organization wants to ensure secure connections. Being able to switch over to a different cryptography system is imperative. Quantum cryptography systems and quantum key distribution (QKD) are able to aid against some of the major issues facing modern cryptography. However, QKD only focuses on secure key distribution.

4.2.3 How to achieve crypto-agility

To set up and achieve crypto-agility, an organization must do the following:

a. **Define policies**: Ensure that everyone in the organization knows what is needed to secure their systems and who is responsible for what.

b. **Determine group responsibility**: Each group is responsible for having and maintaining an inventory of their assets. This allows each team to react quickly to any threats.

c. **Central organization**: This will most likely be a security group that will help develop an inventory and provide any necessary tools. Each team will then need to make sure they can use each tool. On the hardware side, crypto-agility is achieved by adopting new frameworks for incident response and application development. In addition, a layer of software is required for cryptographic application programming interfaces (APIs) and secure update mechanisms.

4.2.4 Crypto-agility best practices

Best practices surrounding crypto-agility include the need for the following:

a. Develop a method for tracking ownership.
b. Automate as many areas as possible, such as management and replacement tracking.
c. Inventory all crypto assets.
d. Have good visibility and a good understanding of who owns what.
e. Ensure crypto technology uses the latest cryptography techniques and algorithms.
f. Use high bit sizes for hash algorithms.
g. Identify vulnerabilities.

4.2.5 How to improve crypto-agility

To improve crypto-agility practices, organizations can do the following:

a. Ensure visibility, meaning an organization should have a full understanding of where and how cryptography is used throughout their infrastructure.

b. Ensure the correct teams or groups retain ownership of their assigned crypto assets.
c. Ensure any used hardware vendors are quick to release updates or security patches or else an organization might need to switch their cryptography methods more often.

Ensure the ability to test new cryptographic algorithms.

4.3 OEM/Vendor Alignment for PQC requirement

Bringing an OEM (Original Equipment Manufacturer) or vendor in line with an organization's requirements for implementing post quantum cryptography requires a structured approach to ensure that both parties understand the need for security and have a clear plan for future-proofing against quantum computing threats. Here's a step-by-step approach to align the OEM/vendor with post quantum cryptography needs of an organisation:

4.3.1 Educate and Raise Awareness

a) Internal Education: Ensure that your internal team is well-informed about quantum computing and post quantum cryptography. This includes understanding the risks posed by the quantum computers to current encryption methods and the timeline for quantum computers becoming practical brought out in above paragraphs.
b) Vendor Education: Educate the vendor/OEM about the importance of the post quantum cryptography for your organization's long term security. Share industry reports, future projections, and case studies that highlight the potential risks and the need for future-proofing.

4.3.2 Conduct a Risk Assessment

a) Risk Analysis: Perform a risk assessment to identify which parts of your organization's infrastructure are most vulnerable to quantum threats (e.g., data at rest, data in transit, etc.).
b) Vendor-Specific Risks: Assess whether the vendor's products are currently using cryptographic algorithms that may be vulnerable to quantum attacks. For example, check if they use RSA, DSA, or ECC.

c) Identify Critical Systems: Prioritize which systems or products are critical and need immediate attention. This will guide your communication with vendors and the speed at which you need them to act.

4.3.3 Define Post Quantum Requirements

a) Specific Standards: Set clear, specific requirements for post quantum cryptography. You may need to align with industry standards and recommendations from bodies like NIST (National Institute of Standards and Technology/ Standards from India/IETF etc.)
b) Hybrid Approaches: Consider specifying hybrid cryptographic systems in the short term, where existing algorithms (e.g., RSA) are used alongside post algorithms (e.g., lattice-based cryptography or hash-based signatures) during the migration stage for failsafe implementation of PQC.

c) **Key Management:** Ensure that your key management systems are ready to support post-quantum cryptographic standards, which might require more complex processes due to longer key sizes.

4.3.4 Evaluate the Vendor's Roadmap

a) **Vendor's Commitment:** Request that the vendor provides a roadmap for integrating post quantum cryptographic algorithms into their products. This should include timelines, plans for transitioning from vulnerable algorithms, and any security audits or certifications.
b) **Compliance with Standards:** Ensure that the vendor commits to adopting relevant standards from NIST and other recognized bodies once they are finalized.
c) **Integration Plans:** Understand how the vendor plans to integrate post quantum algorithms into existing systems without causing disruption to the service or performance.

4.3.5 Negotiate and Set Milestones

a) **Contractual Clauses:** If applicable, add clauses to the contract or service level agreements (SLAs) that require the vendor to implement quantum-safe cryptography within a specific timeframe. This might include phased deadlines for upgrading cryptographic algorithms or implementing hybrid solutions.
b) **Timelines:** Establish clear timelines for implementation, testing, and integration. Ensure that vendors know what your expectations are for achieving quantum-safe cryptography and when they should be fully compliant.
c) **Monitoring and Enforcement:** Set up mechanisms for monitoring the vendor's progress toward these milestones. This can include regular meetings, reports, or audits to ensure compliance.

4.3.6 Request Proof of Concept (PoC) or Pilots

a) **Testing in a Controlled Environment:** Ask the vendor to provide a Proof of Concept (PoC) or a pilot program to test the quantum-safe cryptographic solutions. This allows you to evaluate how well their systems integrate with your existing infrastructure, assess performance impacts, and ensure that security requirements are met.
b) **Validate Post-Quantum Algorithms:** Test the implementation of post-quantum algorithms and check for potential issues with backward compatibility, performance, and interoperability and validate the algorithms by an authorised body /agency.

4.3.7. Collaboration with Industry Bodies

a) **Participate in Standards Development:** Collaborate with bodies such as Meity/ Academia who are actively involved in the development of Post Quantum standards.
b) **Vendor Certifications:** Encourage the vendor to pursue certifications or assessments from trusted third parties to validate that their quantum-safe implementations are secure and adhere to standards.

4.3.8. Mitigate Short-Term Risks with Hybrid Solutions

a) **Use Dual Solutions:** As a stopgap, you can implement hybrid encryption that combines classical cryptography with quantum-resistant algorithms as explained in

above section. This approach ensures that even if quantum computers are not yet fully operational, your systems are protected from potential future threats.

4.3.9. Plan for On-going Collaboration and Updates

a) **Regular Updates:** Ensure the vendor provides regular updates on the progress of adopting quantum-safe cryptography and inform you of any changes in the status of standards or their product offerings.
b) **Agility in the Face of Advancements:** As quantum computing advances, stay agile and adaptable. Encourage your vendors to be proactive in adjusting their solutions as new algorithms and standards emerge.

4.3.10. Test and Validate the Implementation

a) **Security Audits:** Once the vendor has implemented quantum-safe solutions, conduct thorough security audits to verify that the solutions are secure, effective, and future-proof.
b) **Penetration Testing:** Perform penetration testing or vulnerability assessments to ensure that quantum-safe algorithms are resilient to known threats and potential quantum attacks.

By taking these steps, organisation may effectively align OEM or vendor with organization's requirements for implementing quantum-safe cryptography, ensuring Digital assets of an organisation remain secure in the quantum era.

Abbreviations

Abbreviation	Expansion
API	Application Programming Interface
CRQC	Cryptographically Relevant Quantum Computer
D-H	Diffie-Hellman
ECDH	Elliptic-curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
HSMs	Hardware Security Modules
IM	Information Management
IT	Information Technology
KDF	Key Derivation Function
MITM	Man-in-the-middle
NISQ	Noisy Intermediate-Scale Quantum
OT	Operational Technology
PKI	Public Key Infrastructure
PoC	Proof of Concept
QKD	Quantum Key Distribution
QSC	Quantum Safe cryptography
QSS	Quantum Safe Security
RSA	Rivest-Shamir-Adleman
RNG	Random Number Generator
VNF	Virtualized Network Function
VPNs	Virtual Private Networks

Annexure-I

USE CASES OF PQC IMPLEMENTATION

Telecom Sector

- To secure OSS (operation support system) and BSS (Business support system) applications
- Protection of Data in Transit
- Integrity of Virtualized Network Function: to prevent tampering and unauthorized access of network element.

Cloud Infrastructure

- To secure data at rest and data in transit
- Securing integration of APIs

BFSI Sector

- Protection of customer information viz. – profile, user ID, passwords, OTP, transaction history, etc.

Health Sector

- Medical history of patients

Power Sector

- SCADA Systems

Infrastructure

- Railway Infrastructure
- Aircraft Boings