RBIH WHITEPAPER

Securing the Indian Banking Sector in the Age of Quantum Computing

Migrating to Post Quantum Cryptography

CONTENTS

Glossary of Terms 05

Executive Summary 06

Emerging Risks of Quantum Computing 07

Need for Migration 09

Standardisation Process 11

Approach to Migration 12

Conclusion 15

Appendix 18

A**ppendix A:** Post Quantum Cryptography Algorithms

Professor's Preface

The emergence of quantum computing poses a risk to widely used public-key cryptosystems, like RSA and Elliptic Curve Cryptography (ECC). To address this, post-quantum cryptography has been developed as a secure alternative. Post-quantum cryptography, specifically lattice-based cryptographic techniques, offers a promising defence against emerging quantum risks. Lattice-based cryptography (LBC) is designed to be resistant to both classical and quantum attacks, providing a new level of security that is required to protect the banking sector. Advanced cryptographic methods rely on the hardness of lattice problems, which ensure the continued protection of information even in the advent of quantum computing.

LBC offers a promising approach to safeguarding sensitive information against quantum attacks. By leveraging the complexity of lattice problems, which are believed to be resistant to quantum attacks, LBC provides a new layer of defence for the banking industry. The aim of this whitepaper is to make the principles and applications of LBC accessible to a wider audience, including banking professionals, cybersecurity experts, as well as policymakers.

This preface highlights the importance of transitioning to post-quantum lattice-based cryptographic systems within the banking industry. As we delve deeper into the specifics of these technologies, it is clear that their implementation is not merely an option, but a necessity to maintain the trust along with security that underpins the global financial system. In summary, this whitepaper aims to introduce post-quantum cryptography to a broader audience, and it is designed to be accessible without requiring advanced mathematical knowledge.

Dr. Ashok Kumar Das

Professor, Center for Security, Theory and Algorithmic Research, IIIT Hyderabad

CEO's Preface

In an era where the evolution of technology continually reshapes our financial ecosystems, the risks posed by quantum computing to classical cryptographic systems are a challenge we must proactively address. The Reserve Bank Innovation Hub (RBIH) is committed to tackling these emerging risks and fortifying the security and integrity of the Indian banking and financial sector.

This white paper, 'Securing the Indian Banking Sector in the Age of Quantum Computing', embodies our commitment to staying ahead of technological advancements. As quantum computers grow more sophisticated, the foundations of our digital security face risks from the capabilities of quantum computing.

We advocate for a comprehensive transition from vulnerable classical cryptographic methods to resilient post-quantum cryptographic (PQC) algorithms explicitly designed to withstand the computational power of quantum machines. This proactive approach will ensure the continued security of the financial system.

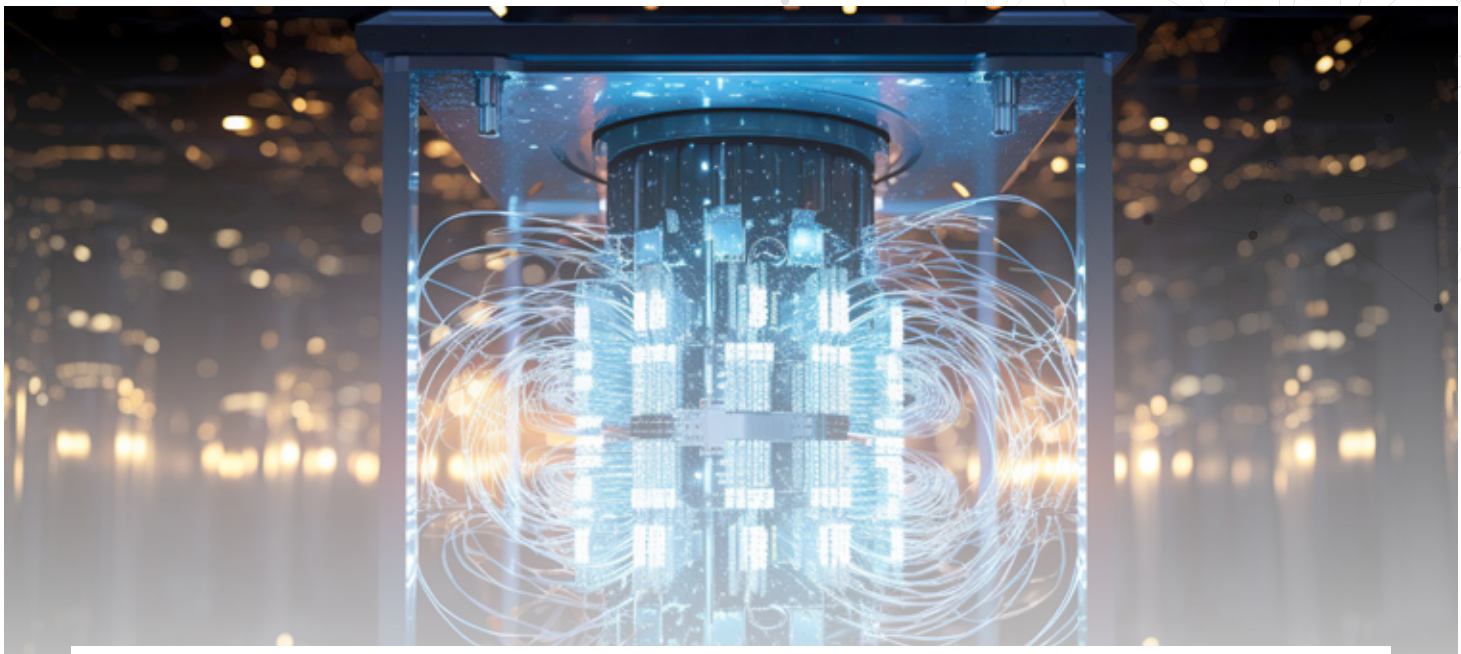
This white paper delves into the intricacies of quantum risks, the need for migration to PQC, and the strategic steps necessary for a seamless transition. Implementing these strategies can safeguard India's banking and financial sector from potential disruptions, thereby maintaining the trust of our stakeholders.

The journey towards quantum resilience is complex and necessitates a collaborative effort. We call upon all stakeholders—financial institutions, regulatory bodies, technology providers, and the research community—to join us in this endeavour. I invite you to engage with the insights presented in this white paper. Let us work together to ensure that our financial systems are not only secure today but also resilient to the challenges of tomorrow.

Rajesh Bansal
Chief Executive Officer
Reserve Bank Innovation Hub

Glossary of Terms

Term	Description
AES	Advanced Encryption Standard
BIS	Bank for International Settlements
BYOK	Bring Your Own Key
CARAF	Crypto Agility Risk Assessment Framework
CBC	Code Based Cryptography
CRYSTALS	Cryptographic Suite for Algebraic Lattices
CSR	Certificate Signing Request
CVP	Closest Vector Problem
DH	Diffe Hellman
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffe Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
HBC	Hash Based Cryptography
HNDL	Harvest Now Decrypt Later
HSM	Hardware Security Module
IBC	Isogeny Based Cryptography
IDS	Intrusion Detection System
IFP	Integer Factorization Problem
IPS	Intrusion Prevention System
IT	Information Technology
KEM	Key Encapsulation Mechanism
LBC	Lattice Based Cryptography
LWE	Learning with Errors
MC	Multivariate Cryptography
NIST	National Institute of Standards and Technology
NTRU	N-th Degree Truncated Polynomial Ring Units
PQC	Post Quantum Cryptography
PCI DSS	Payment Card Industry Data Security Standard
PRNG	Pseudo-Random Number Generators
QKD	Quantum Key Distribution
RSA	Rivest Shamir Adleman
SSL	Secure Socket Layer
SIEM	Security Information and Event Management
SVP	Shortest Vector Problem
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TLS	Transport Later Security
VM	Virtual Machine



Executive Summary

The security of India's banking sector, like its global counterparts, relies on a foundation of robust cryptography. This invisible shield protects financial data and transactions, ensuring trust in the system. Public-key-based classical cryptographic algorithms that rely on the inherent difficulty of solving complex mathematical problems like integer factorisation and finding discrete algorithms form the backbone of this security architecture. The advent of quantum computing has introduced an element of risk to existing cryptography.
Unlike traditional computers that operate on bits (0s and 1s), quantum computers harness the principles of quantum mechanics to perform calculations fundamentally differently. This allows them to tackle the mathematical problems underpinning classical cryptography, potentially making systems vulnerable to quantum attacks.

To mitigate this potential scenario, the Reserve Bank Innovation Hub recommends that Indian banks embark on a proactive transition to post-quantum cryptography (PQC) algorithms specifically designed to resist attacks from quantum computers. Globally, extensive research is underway to identify and standardise these new algorithms. By adopting PQC solutions, Indian banks can ensure the continued security of their systems.

This whitepaper delves deeper into this subject and provides a comprehensive overview of the vulnerabilities within classical cryptography and the potential measures Indian banks can take. It explores the proposed PQC solutions and outlines a migration strategy to ensure a smooth transition. By understanding the evolving landscape and taking proactive steps towards adopting quantum-resistant cryptography, Indian banks can ensure the continued security of the sector.

Disclaimer: The views and recommendations expressed in this report are those of the authors and do not represent the views of the Reserve Bank of India.

Emerging Risks of Quantum Computing

A quantum computer is a machine that uses the principles of quantum mechanics, such as superposition and entanglement, to solve problems that are impossible for classical computers. They have qubits instead of bits (as seen in classical computers) that can execute multiple processes at a single point in time, solving problems in polynomial time unlike classical computers, which solve problems in exponential time.

Superposition is the ability of a system's memory to be in multiple states at the same time until it is measured. Entanglement allows quantum computers to manipulate many qubits in a single operation, instead of manipulating each qubit individually.

Currently, quantum computers are in their early stages and are very sensitive to noise and errors. Hence, Noisy Intermediate Quantum Computers – the first generation of quantum computers being built are small and have limited capabilities.

The next generation, fault-tolerant quantum computers, can correct errors and will be much more reliable, promising to revolutionise all fields and industries that currently utilise computers.

The day when quantum computers' capabilities surpass that of classical computers called "Q-Day" is fast approaching which could potentially break encryption algorithms that protect the privacy and integrity of online financial transactions[1].

> **Grover's search algorithm is a quantum algorithm for the search problem that takes the square root of the time taken to solve problems that classical computer can solve.**

For an encrypted channel of communication between two entities over a public channel like the Internet, Transport Layer Security (TLS)/Secure Socket Layer (SSL) protocol is utilised for encrypting data and secure communication among web browsers and servers.

The two building blocks needed to enable this encrypted communication are as follows

Asymmetric cryptographic (or public-key based) algorithms – RSA (Rivest, Shamir, Adleman: Inventors of the algorithm) and Elliptic Curve Cryptography (ECC) algorithms, rely on a mathematical problem (factoring a very large number that is a product of two very large prime numbers, and discrete logarithm problem, respectively) that cannot be broken by classical computers. The widely used key (an alpha-numeric string used to encrypt and decrypt data) size is 2048 (in bits) for RSA, hence the variant is called RSA-2048. Similarly, 256 bits used for ECC is called ECC-256.

Symmetric cryptographic algorithms – Advanced Encryption Standard (AES), uses simpler mathematical operations, such as byte substitution, rows shift, mixing columns, add round key, and key expansion that perform encryption functions very fast and can't be broken by classical computers. Standardised variants for AES include key sizes of the length 128, 192, and 256 Symmetric cryptosystems depending on the difficulty of searching through many possible secret values. Advanced Encryption Standard (AES) is one such cryptographic algorithm where exhaustive key search is the greatest threat.

For a secure communication channel to be established between two or more parties over the internet, both symmetric and asymmetric algorithms are essential. Compromising with either one can be detrimental to a secure connection.

To reduce the effectiveness of symmetric cryptographic algorithms, a search algorithm that runs on a quantum computation model called Grover's search algorithm is used for the search problem that takes the square root of the time taken to solve problems that classical computers can solve.

Quantum computers, using Grover's algorithm, can find the encryption key used with AES much quicker than a classical computer.

Grover's algorithm reduces the effectiveness of symmetric encryption standard AES-256 to roughly that of AES-128 which is still strong enough but reduces AES-128 to the equivalent of "AES-64" which can be broken with classical computers. This is why AES-256 is generally regarded as Quantum-Safe, but AES-128 is not. Experts advise upgrading AES-128 encryption to AES-256.

Another quantum algorithm called Shor's algorithm demonstrates that quantum computers can effectively break existing mathematical problems utilised in existing asymmetric algorithms, potentially compromising the security of sensitive financial data.

Using Grover's algorithm, quantum computers can significantly reduce the effectiveness of symmetric algorithms like AES. But with Shor's algorithm, a quantum computer can effectively break asymmetric algorithms like RSA and Elliptic Curve.

Quantum computers outperform classical computers in three general cases of problems: 1) search, 2) hidden subgroups, and 3) quantum simulation. The most familiar example of solving hidden subgroup problems is factoring (which happens to be utilised in the RSA algorithm) as well as computing discrete logarithms (used in elliptic curve problems). Classical computers can take over 1024 years to potentially break the algorithm, which can be broken in a matter of hours by quantum computers using Shor's algorithm.

Table 1 shows various algorithms from symmetric and asymmetric algorithms including the one-way cryptographic hash algorithm with their pre-quantum security level and post-quantum security level, and the quantum algorithms used to attack the classical algorithms.

From this table, asymmetric algorithms, like (1) RSA, (2) Diffie-Hellman (DH), Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC)-based algorithms such as Elliptic Curve Diffie-Hellman Key Exchange Algorithm (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA), can be broken using the Shor's algorithm[2]

Table 1. Overview of Effects of Quantum Computing on Cryptographic Algorithms

Algorithm	Application	Pre-quantum security level	Post-quantum security level	Algorithm used for attack
AES-128	Symmetric enc.	128	64	Grover
AES-256	Symmetric enc.	256	128	Grover
Salsa20	Symmetric enc.	256	128	Grover
GMAC	MAC	128	128	-
Poly1305	MAC	128	128	-
SHA-256	Hashing	256	128	Grover
SHA3-256	Hashing	256	128	Grover
RSA-3072	Asymmetric enc. / signatures	128	Broken	Shor
DH-3072 / DSA-3072	Asymmetric enc. / signatures	128	Broken	Shor
ECDH-256 / ECDSA-256	Key exchange / signatures	128	Broken	Shor

Need for Migration

Among the current standard security practices followed in the financial sector, it was found that TLS v1.2 and above is mandatory for all applications to ensure secure communication, according to consultations with a large private sector bank. It was also found that ECDH and ECDSA are preferred cryptographic algorithms for key exchange and digital signature.

> **Threat actors can perform "Harvest Now, Decrypt Later" attacks where attackers can intercept encrypted communications or store encrypted data today and wait for quantum computers to become powerful enough to decrypt them later.**

Key exchange involves parties securely establishing a shared secret key using asymmetric cryptography, enabling subsequent symmetric encryption of data to be secured for efficient communication. Digital signatures ensure data integrity and authenticity. A sender creates a digital signature by encrypting a message hash with their private key. The recipient verifies it using the sender's public key, confirming the message's origin and unaltered content.

A potential scenario is that quantum computing can break encryption mechanisms in banking institutions. Most banks enforce several security measures to protect their customers' information, like SSL and TLS protocols. This is because classical computers cannot easily break these encryption methods. However, given the advancement in quantum computing, quantum computers can break these encryption methods, which can potentially expose sensitive customer information.

Threat actors can perform "Harvest Now, Decrypt Later" attacks where attackers can intercept encrypted communications or store encrypted data today and wait for quantum computers to become powerful enough to decrypt them later. Such attacks pose risks to the integrity and confidentiality of sensitive financial data and banking infrastructure.

Breaking the algorithm can also mean that attackers can break the digital signing algorithm to intercept data sent over, modify as per requirements and forge signatures to impersonate the sender, thus compromising the authenticity of the sender's digitally signed files.

Mitigating these emerging risks calls for transitioning to post-quantum cryptography (PQC) algorithms. PQC algorithms are designed to be resistant to quantum attacks and offer a secure foundation for future cryptographic applications. The design is said to be resistant by utilising different mathematical structures and problems that are believed to be difficult for even the most powerful quantum computers to solve. PQC algorithms are designed to withstand quantum attacks by leveraging mathematical problems that remain computationally hard for quantum computers.

The benefits of transitioning to PQC Algorithms can be as follows.

Enhanced Security: PQC algorithms offer robust protection against quantum attacks, ensuring the confidentiality and integrity of sensitive financial data.

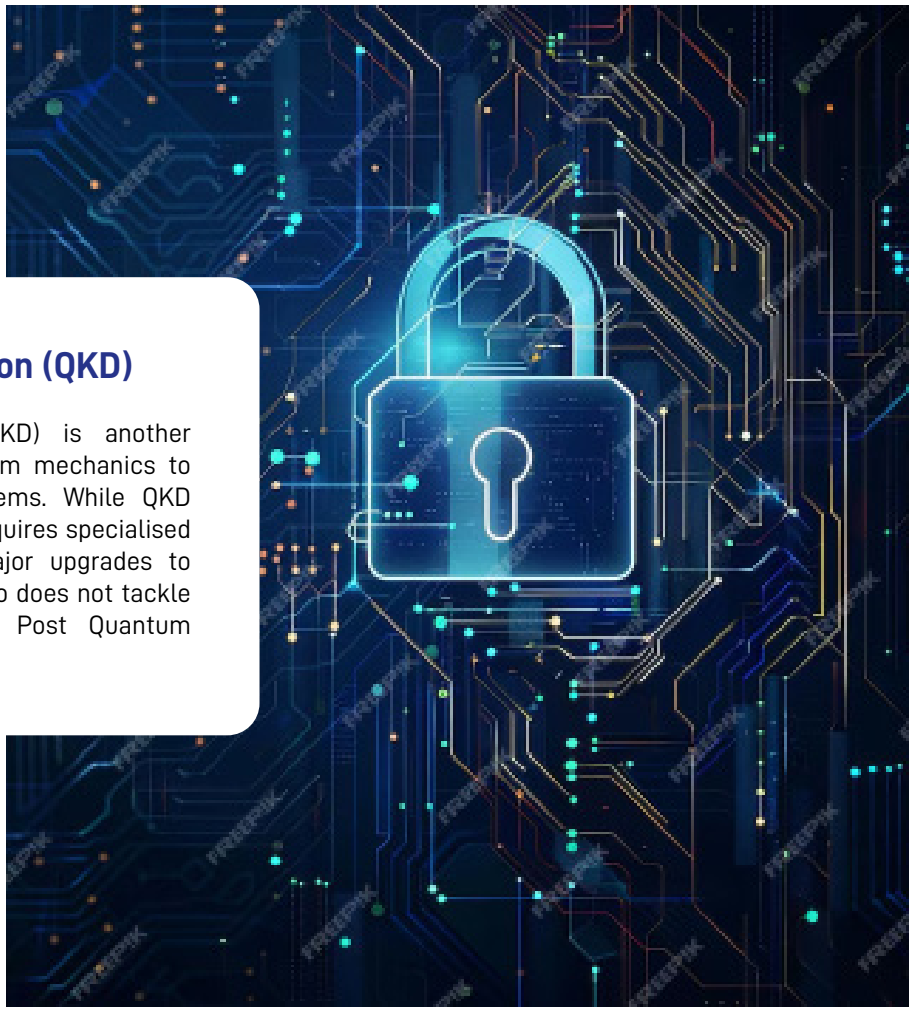
Future-Proof Infrastructure: By adopting PQC early, Indian banks can ensure their infrastructure remains secure against evolving threats posed by quantum computing

Compliance and Confidence: Implementing PQC algorithms can help banks comply with regulatory requirements and build customer trust in their security practices.

Migration to PQC is required to ensure the security of communication and data transmission. This involves transitioning from traditional cryptographic methods to post-quantum cryptographic algorithms (see Appendix A) that are resistant to quantum attacks.

Quantum Key Distribution (QKD)

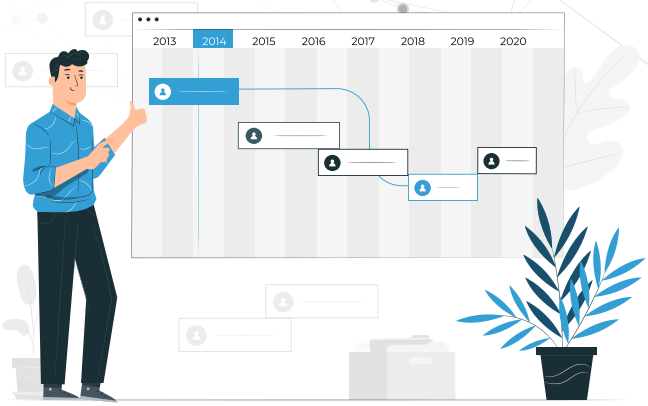
Quantum Key Distribution (QKD) is another technology that utilises quantum mechanics to create quantum-resistant systems. While QKD offers quantum resistance, it requires specialised hardware that would need major upgrades to global IT infrastructure. QKD also does not tackle the authentication issue like Post Quantum Cryptographic solutions would.



Standardisation Process

When an existing cryptographic algorithm needs to be phased out, the National Institute of Standards and Technology (NIST) initiates a standardisation process. This ensures that organisations worldwide can integrate the new algorithm into their infrastructure, maintaining confidentiality, functionality, and competency. The process aims to build public confidence, ensure interoperability, and shortlist the most efficient algorithm without compromising the quality of encryption.

Starting in 2016, NIST has conducted four rounds of the PQC shortlisting process. In round one, 69 algorithms were submitted. These were evaluated on security, performance, and implementation aspects. 26 algorithms progressed to round two, where they underwent further scrutiny, including cryptanalysis, which is the study of encrypted messages to break them without knowing the key, and side-channel attacks, which exploit physical information leaked during cryptographic operations, like power consumption or timing, to extract secret keys. Round three involved a focused analysis of seven finalists, ultimately selecting four algorithms for standardization[3].



Key Encapsulation Mechanisms (KEM)

1. **CRYSTALS Kyber (Lattice-based encryption algorithm)**

Digital Signature Algorithms (DSA)

1. **CRYSTALS-Dilithium (Lattice-based)**
2. **Falcon (Lattice-based)**
3. **SPHINCS+ (Hash based)**

Existing algorithms like RSA and ECC offer both Key Encapsulation Mechanisms (KEMs – the process of transmitting session symmetric key using asymmetric cryptography) and Digital Signature functionalities. However, selecting separate algorithms allows for optimisation based on each specific function and distinct security requirements can be addressed with different mathematical statements.

Selected algorithms include – CRYSTALS Kyber for KEM and CRYSTALS Dilithium, Falcon and SPHINCS+ for Digital Signature Algorithms. Different types of algorithms utilised are elaborated in academic terms in the appendix.

KEMs prioritise speed in generating a random key and encapsulating it for secure transmission. This is crucial for applications requiring frequent key updates, hence requiring fast key generation and encapsulation, while DSAs prioritise the efficiency of signature generation and verification to ensure swift authentication of documents or messages without compromising security. Additionally, using separate algorithms provides diversification and reduces the risk of a single vulnerability affecting both key exchange and digital signatures. This enhances overall system security and resilience against potential cryptographic failure attacks.

The other three algorithms of the seven finalists are further being evaluated and sent forth into round four with algorithm candidates like BIKE, Classic McEliece and HQC for KEMs[4]. A separate call for additional digital signatures is ongoing.

Approach to Migration

While NIST PQC algorithms represent a crucial step towards quantum-resistant cryptography, concerns remain regarding their real-world readiness. Some factors that cause concern include performance overhead, complex implementations, and lingering vulnerabilities like slashing attacks, where specific inputs cause decryption failures. These factors suggest extensive testing, optimisation, and potential algorithm revisions before widespread production deployment to ensure robust security in the quantum age. "Project Leap" – an initiative by the Bank for International

Being cognizant of results

Settlements (BIS)[5] in collaboration with the Bank of France and Deutsche Bundesbank tested and implemented PQC algorithms for transmitting payment messages through a configured Virtual Private Network (VPN) and observed an average of 22 to 37 milliseconds of delay with PQC algorithms compared to existing algorithms utilised in TLS libraries. This delay is almost negligible for the end user while waiting for their webpage to load.

> **"Different implementations will result in distinct performance outcomes. Thus, organizations will need to invest in custom benchmarks that capture the constraints of their assets as well as the respective operational environment.**

Ensuring compatibility between different PQC algorithms and existing cryptographic systems is crucial. The most recommended implementation is by using PQC in hybrid mode – using CRYSTALS Kyber Algorithm in combination with established "pre-quantum" security like ECDSA in a transitional approach, providing layered security so that even if one component is compromised the other still provides protection.

Current versions of AES, and post-quantum cryptographic algorithms like CRYSTALS-Kyber (for general encryption) and CRYSTALS-Dilithium (for digital signatures) are shortlisted by NIST where with specific key lengths (parameter sets) of the encryption algorithms are aimed at respective security levels. The cryptographers who developed PQC algorithms suggest Kyber-512/ Dilithium2 to be rough equivalent to AES-128, Kyber-768/ Dilithium3 aims at security roughly equivalent to AES-192, and Kyber-1024/ Dilithium5 aims at security roughly equivalent to AES-256.

Choosing the best possible alternative with operational constraints and type of asset resources is imperative for an appropriate replacement. For example, the key sizes of Dilithium are not so different from RSA (or Diffe-Hellman) which is at least 1024 bit. Simultaneously, the signature for RSA is in the same order of magnitude as the key. The signatures for Dilithium are also similar in size to their key, compared to other types of algorithms shortlisted – hash-based or multivariate.

Thus, if the asset currently uses RSA, Dilithium may be an appropriate replacement. An organisational transition roadmap will need to ensure that the asset can switch algorithms, e.g. through a software update.

What to expect during implementation?

The implementation process can be time-consuming with continuous performance assessments and optimisation strategies and a high possibility of it being a financially expensive endeavour, requiring cryptanalysis.

However, the organisational roadmap may not have to plan for hardware upgrades as the signature sizes, as well as the key sizes, are like that used for RSA currently. This is more cost-effective than implementing PQC solutions that may require additional investments in banking infrastructure depending on support for PQC algorithms provided by third-party vendor solutions.

Is Training necessary for enterprise employees?

Within this context, training regarding quantum-safe solutions is not necessary for resources that do not fall under the IT security domain. However, security teams would mostly manage digital certificates of the machines generated by PQC algorithms. Lifecycle management – the processes associated with onboarding and offboarding users, assigning and managing access rights, and monitoring and tracking access activity can be automated to stop certification outages and increase authentication efficiency.

Assessing the cryptographic footprint by creating an inventory of all deployed cryptographic security protocols and ensuring continuous risk assessments for minimising the attack surface for quantum threats is essential for the security team to transition critical infrastructure and applications in a phased manner. A forward-thinking strategy is essential for governance and the preparation of migration plans and playbooks is necessary for common implementation reference.

Migration Strategy

The PQC migration process necessitates careful planning and coordination to ensure that the migration is carried out correctly without disrupting the services provided by the existing systems and applications.

IT inventory Classification: Enterprises need to be classified based on the assets' security level. NIST recommends that organisations classify their information assets based on their value and sensitivity to ensure that appropriate security controls are in place to protect them. Information assets - be it hardware or software like applications or operating systems are considered a critical component of enterprises' overall security systems, and their protection is a key priority since most organisations rely on at least some sensitive information to operate.

Cataloguing and Updating Information Assets: Cataloguing assets can be done under different levels of security classification: (1) Unclassified, (2) Protected, (3) Secret and (4) Top Secret. Respective labels on these should specifically assist in prioritising critical data assets.

A cryptographic inventory should be catalogued to encompass all cryptographic objects utilised across an organisation's applications, infrastructure, and networks, including those relevant to static and transit data.

Determine Dependencies: Special provisions for assets that have third-party dependencies should be noted. Also, each asset (enterprise or third party) should be classified to support availability for migrating to the PQC algorithms

After the inventory is built with the cryptographic assets identified, dependencies should be determined by:

1. Understanding the security levels implemented at specific points.
2. Data classified concerning data states – data at rest, data in transit (or in motion), and data in use.
3. To secure data at rest – improving the effectiveness of AES or evaluating the risk posed by the deployed key length can be ascertained.
4. To secure data in motion – replacing RSA and ECDH with PQC algorithms would be the way to move ahead.
5. Cryptographic protocols and algorithms.
6. Cryptographic keys.
7. Processes including software, libraries, workflows combining other processes, and business processes.
8. Assets that process data – Machines, VMs and containers.

Deploy PQC Solutions: With the information of the entire organisation mapped and understood, respective new solutions that provide post-quantum solutions should be deployed. A risk assessment before, during and after should be done continuously to ensure no attack surface is exposed for threat actors to exploit.

Attack Surface Management: Risk management from quantum attacks can be effectively assessed using the 5D Crypto Agility Risk Assessment Framework (CARAF)[6] to analyse and evaluate the risk that results from the lack of crypto agility.4 The framework specifies how:

1. Risk can be estimated with the timeline of quantum computer development, the shelf life of IT assets, and the implementation of PQC solutions.
2. Cost is estimated for enterprise and third-party solutions, with and without PQC support.
3. Action for appropriate security mitigation depending on asset type.

If possible, cryptanalysis experts can be brought in to attempt to break the encryption to validate the encryption functionality of the implemented solution.

Reviewing the entire process concerning confidential information being sent over the internet and maintenance of machine identities (digital certificates) should be performed to validate the performance of the new solution with appropriate documentation for auditing purposes.

Conclusion

This white paper highlights a potential scenario detailing the vulnerability of existing cryptographic algorithms to quantum computing.

Quantum attacks on current encryption methods could undermine consumer trust and expose sensitive financial data. To mitigate such risks, this white paper offers post-quantum cryptography (PQC) algorithms as a potential solution

A concerted effort from industry experts, technology providers, and regulatory bodies can strengthen the entire Indian banking sector.

By leveraging the expertise of technology companies and research institutions, adopting a phased approach, and prioritising critical infrastructure, Indian banks can stay protected from quantum attacks.

The advent of quantum computing presents both challenges and opportunities. By taking decisive action now, Indian banks can safeguard their digital assets, uphold consumer trust, and lead the way in securing the future of banking.

Acknowledgements

Authors
Pruthvi Raj Bhat
Prithwi Bagchi
Dr. Ashok Kumar Das

Contributors
Preethi Ignatius
Iti Panwar

Design
Mohammed Azhar

References

1. Herman, Arthur. "Q-Day Is Coming Sooner Than We Think." Forbes. June 7, 2021. https://www.forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/?sh=56d35f3f5d51.

2. Rothenberger, Benjamin, and Raphael Reischuk. "Quantum Computing and Cybersecurity: Why It's Time to Prepare Now?" Zuehlke. July 12, 2023. https://www.zuehlke.com/en/insights/quantum-computing-and-cybersecurity-why-its-time-to-prepare-now.

3. NIST, Computer Security Resource Center. "Post Quantum Cryptography – Selected Algorithms 2022." Created January 3, 2017. Last updated July 8, 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

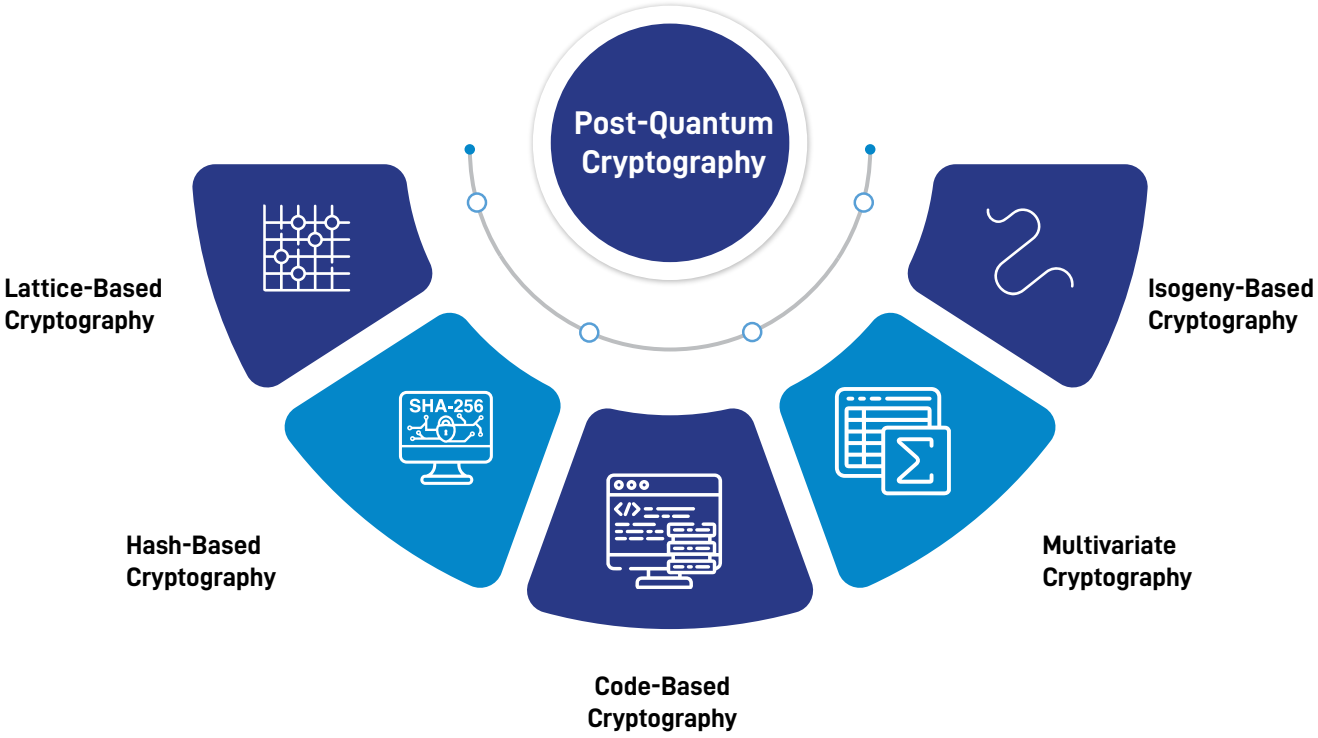
4. NIST, Computer Security Resource Center. "Post Quantum Cryptography – Round 4 Submissions." Created January 3, 2017. Last updated July 19, 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions.

5. BIS Innovation Hub. "Project Leap: Quantum-proofing the Financial System." June 5, 2023. https://www.bis.org/publ/othp67.htm.

6. Ma, Chujiao, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg. "CARAF: Crypto Agility Risk Assessment Framework." Journal of Cybersecurity 7, no. 1 (2021). https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827.

Appendix A:
Post Quantum Cryptography Algorithms

To maintain the security and privacy of digital communications and data in a world where powerful quantum computers exist, it is necessary to provide post-compromise security against Harvest Now, Decrypt Later quantum brute force attacks. Figure 1 shows various types of Post Quantum Algorithms that are shortlisted for use cases which are: 1) Lattice-Based Cryptography (LBC), 2) Hash-Based Cryptography (HBC), 3) Code-Based Cryptography (CBC), 4) Multivariate Cryptography (MC), and 5) Isogeny-Based Cryptography (IBC).



Lattice-Based Cryptography (LBC):

Lattice-based cryptographic constructions hold great promise for post-quantum cryptography, as they enjoy strong security proofs based on worst-case hardness, relatively efficient implementations, as well as great simplicity. In addition, lattice-based cryptography is believed to be secure against quantum computers. Lattice-based cryptographic constructions are based on the presumed hardness of lattice problems, some of them are given below.

- **Shortest Vector Problem (SVP):** The challenge is to find the shortest non-zero vector in a lattice.
- **Closest Vector Problem (CVP)**: This involves simplifying the closest lattice point to a given target point. Like SVP, CVP is also considered hard to solve, especially in high
- **Shortest Independent Vector Problem (SIVP)**: It involves finding a non-zero lattice vector of minimum Euclidean norm that is linearly independent of a given set of lattice vectors.
- **Bounded Distance Decoding (BDD)**: The Bounded Distance Decoding problem is a variation of the Closest Vector Problem, in which it is guaranteed that the target is the close proximity to the lattice concerning the minimum distance of the lattice. BDD offers security benefits, and resilience against quantum attacks because it is impossible to solve the BDD problem in polynomial time.
- **Learning With Errors (LWE):** The LWE problem involves solving linear equations that are perturbed by some

small error. The security of LWE is based on the presumed hardness of finding the solution to these equations given a set of noisy samples. LWE has become a cornerstone for a wide range of cryptographic applications, including encryption, key exchange, and fully homomorphic encryption.

- **Ring Learning With Errors (Ring-LWE)**: A variant of LWE that operates in the setting of polynomial rings.
- **Short Integer Solutions (SIS):** The Short Integer Solution (SIS) problem is a fundamental problem in lattice-based cryptography. It involves finding short nonzero integer vectors that are orthogonal to given vectors within a certain modulus. It is an average case lattice-problem, commonly used in lattice-based signature applications.
- **Ring-Short Integer Solutions (R-SIS):** The Ring-Short Integer Solution (Ring-SIS) problem is a variant of the Short Integer Solution (SIS) problem, that is defined in the context of ideal lattices over a ring. Ring-SIS are important for the development and analysis of lattice-based cryptographic schemes based on ideal lattices.
- **NTRU:** A lattice-based public key cryptosystem distinct from LWE-based constructions, NTRU (N-th degree Truncated polynomial Ring Units) operates directly on polynomials and is renowned for its efficiency. Although it does not rely on the LWE problem, the security of NTRU is considered to be quantum-resistant due to its dependence on the difficulty of specific lattice problems.

Hash-Based Cryptography (HBC):

Hash-Based Cryptography (HBC) denotes a cryptographic methodology that utilizes the characteristics of cryptographic hash functions. These functions are mathematical algorithms designed to process an input (or 'message') and yield a fixed-size byte sequence, typically known as a digest, which seems random. The resulting hash is distinct for each unique input, under ideal conditions, making it computationally impractical to produce identical hash outputs from different inputs. This attribute is referred to as collision resistance.

HBC gains particular relevance in the realm of quantum computing. Contrary to con-ventional cryptographic algorithms, which quantum computers could potentially com-promise, hash-based cryptography is deemed qquantum-resistant. In essence, it is con-sidered secure against adversaries equipped with quantum computing capabilities.

Key applications of hash-based cryptography encompass:

- **Digital Signatures:** Leveraging hash functions to authenticate the integrity and origin of digital documents.
- **Message Authentication Codes (MACs)**: Employing hash functions in tandem with a secret key to verify message integrity and authenticity.
- **Password Hashing:** Utilising hash functions for the secure storage of passwords by saving the hash digest instead of the actual password.
- **Random Number Generation**: Applying hash functions to generate pseudo-random numbers or sequences, crucial in numerous cryptographic operations.
- **Commitment Schemes:** Using hash functions to enable one party to commit to a specif-ic value while concealing it from others, with the option to disclose the committed val-ue later.

Given its resistance to quantum attacks, hash- based cryptography stands as a significant focus of ongoing research and development, especially with the advancement of quantum computing. Agencies like the National Institute of Standards and Technology (NIST) are actively engaged in the standardisation of post-quantum cryptographic protocols, including those based on hash functions, to safeguard digital communications in the emerging quantum era.

Code-Based Cryptography (CBC):

Code-based cryptography (CBC) refers to any cryptographic system that derives its security from challenging problems found in algebraic coding theory. The central problem in this area is the decoding of a random linear code, a task proven to be NP-complete in 1978 by Berlekamp, McEliece, and Van Tilborg. In that same year, McEliece introduced the inaugural code-based cryptosystem, which involves selecting a code that possesses an inherent algebraic structure facilitating efficient decoding, and then camouflaging this code as a random linear code. A message is encrypted as a corrupted code word. Possessing the secret code enables the recovery of the original message, whereas an adversary is confronted with the daunting task of decoding a random linear code.

Multivariate Cryptography (MC):

The Multivariate Public-Key Cryptosystem (MPKC) or Multivariate Cryptography (MC) stands as a leading candidate in the field of post-quantum cryptography. In MPKC, a system of multivariate polynomials constitutes the public key. The security of MPKC hinges on the difficulty of solving a system of random quadratic multivariate polynomials, a task that is NP-hard. Distinct from the number-theoretic problems underpinning traditional cryptographic schemes, the multivariate-quadratic (MQ) problem is believed to be resilient to quantum attacks. As of now, there is no quantum algorithm known to solve the MQ problem in polynomial time.

Of all the different types of algorithms, lattice-based algorithms provide most security and efficiency together when compared to other types of algorithms, which makes it very popular among cryptographers community.

Of the others, code-based could realistically compete with lattice-based, which is why most of the algorithms in Round 4 selection are code-based. Hence, some of the code-based are considered realistic alternatives to Kyber KEM.

Hash-based algorithms although very secure, can be just used for digital signatures. Additional it requires very large signatures.

Other different PQC algorithm types are not popular and different candidate algorithms under these type are shown to be broken.

Isogeny-Based Cryptography (IBC):

Isogeny-Based Cryptography (IBC) is a relatively new field that emerged in the 2000s. It originates from Elliptic Curve Cryptography (ECC), an earlier branch of public-key cryptography that began in the 1980s. Miller and Koblitz's proposal to incorporate el-liptic curves into the Diffie-Hellman key exchange protocol marked ECC's introduction to the realm of cryptography.

Isogeny-based encryption represents a category of quantum-resistant encryption techniques, distinguished by two primary characteristics. It employs the shortest keys and relies on highly sophisticated mathematics. While most post-quantum encryption methods necessitate significantly longer keys often two or three orders of magnitude greater to uphold existing security standards, isogeny-based encryption maintains an edge by utilising the shortest keys among all proposed post-quantum encryption methods, with key sizes comparable to those currently in use.

About RBIH

The Reserve Bank Innovation Hub (RBIH) is a wholly-owned subsidiary of the Reserve Bank of India, dedicated to leveraging technology and innovation to enable frictionless finance for a billion Indians. The RBIH works towards this mission through its four pathways: RBIH Build - developing in-house solutions when market solutions do not exist, RBIH Design - designing customer-centric processes and products, RBIH Incubate - nurturing fintech startups and the innovation ecosystem, and RBIH Insights - conducting in-depth research and analysis to shape financial innovation. By building bridges between various stakeholders in the financial ecosystem, RBIH fosters an environment of collaborative innovation to drive financial inclusion.

About IIIT-HYDERABAD

International Institute of Information Technology, Hyderabad (IIITH) is an autonomous university, founded as a not-for-profit public private partnership (N-PPP) in 1998, and is the first IIIT in India under this model. Over the years, the institute has evolved strong research programs in various areas, with an emphasis on technology and applied research for industry and society. The institute facilitates interdisciplinary research and a seamless flow of knowledge. In this initiative, IIIT - Hyderabad provides the technical expertise on cutting-edge niche technologies like quantum technology to RBIH and help Indian Banking sector to secure themselves in the next age of internet security.

Head Office

Reserve Bank Innovation Hub,
Keonics, 27th Main Road, 1st Sector, HSR Layout,
Bengaluru, Karnataka – 560102

For more information, please contact us at communications@rbihub.in
To learn more about our other projects, visit us at https://rbihub.in

Follow RBIH on Linkedin, X, and Instagram.

Reserve Bank Innovation Hub (RBIH)

@rbinnovationhub

@rbinnovationhub

RBIH