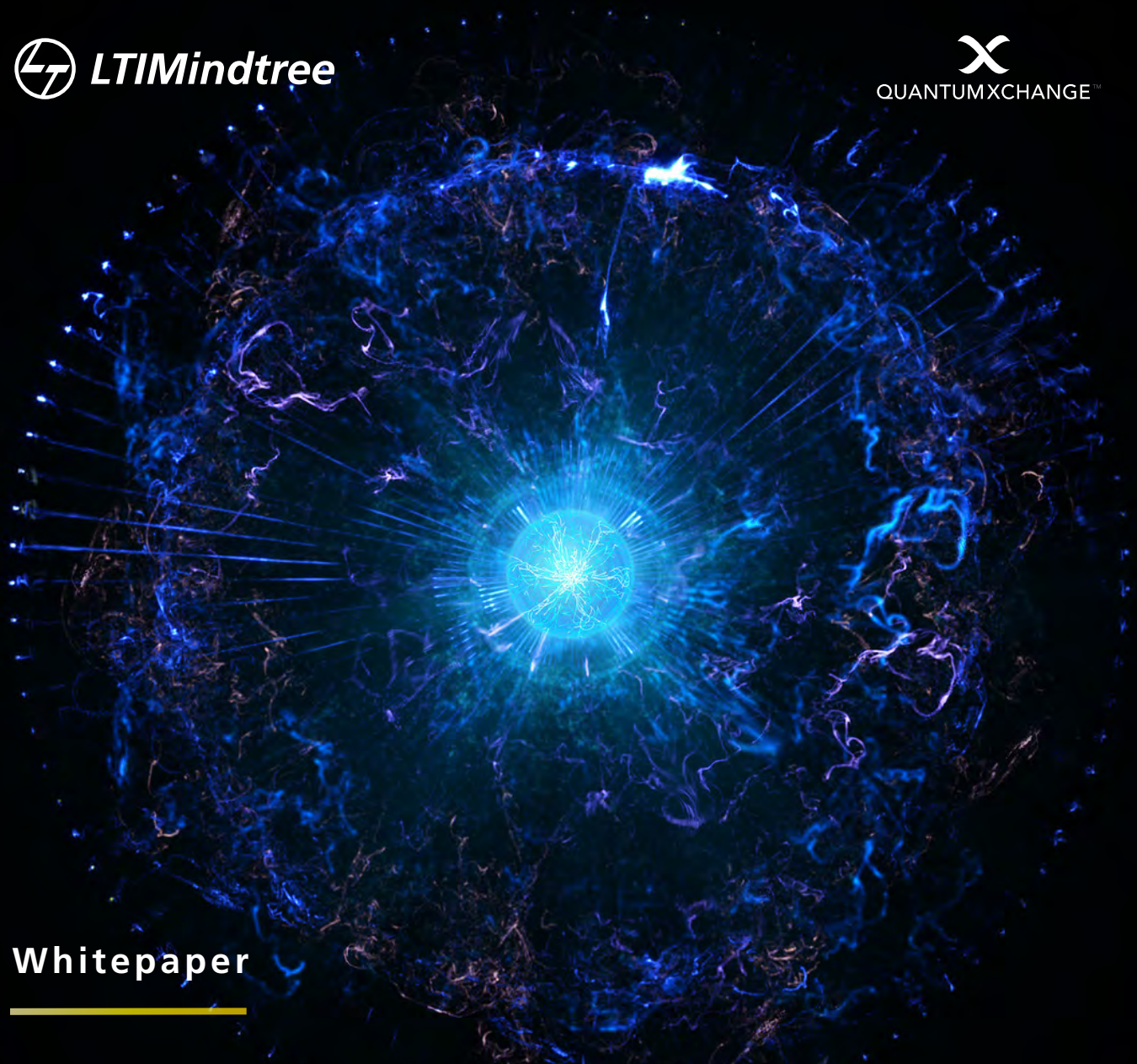
LTIMindtree

QUANTUMXCHANGE™



Whitepaper

Post-Quantum Cryptography: Securing SD-WANs

Table of Contents

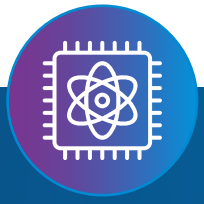
01 Executive summary

Quantum computing is progressing rapidly towards developing a cryptographically relevant quantum computer that can break the current cryptographic systems employing public key cryptography. This whitepaper introduces the quantum threat, its implications, and the vulnerabilities of the current cryptographic methods. Post-Quantum Cryptography (PQC) algorithms are being designed to be quantum resistant. This whitepaper also throws light on NIST efforts to standardize these algorithms and the global response to adopt these, especially in the critical sectors such as banking and financial regulations.

Given the prevalence of Software Defined Wide Area Networks (SD-WANs) in key sectors such as banking and insurance, it is important to migrate them to adopt PQC. We discuss strategic and migration steps for integrating PQC into organization's complex SD-WAN ecosystem. In partnership with Quantum Xchange, this whitepaper provides a practical roadmap for securing SD-WANs against quantum threats, ensuring robust long-term security and operational resilience.

02 Q-day and the challenge posed by quantum threat

Q-day refers to a future event when quantum computers become powerful enough to break the cryptographic algorithms that currently protect our digital communica tions and data. This includes the encryption that secures websites, emails, financial transactions, and virtually any data transmitted over the internet today as well as within enterprises. This **quantum threat** is a major concern for governments, businesses, and individuals alike, as it would allow a quantum computer to decipher encrypted information that was intended to be secure, potentially leading to unprec edented levels of data exposure and cyber threats.



What is the quantum threat?

Asymmetric key cryptography is primarily used to exchange keys and to authenticate using digital signatures. This cryptographic method is based on a simple forward problem (e.g., RSA algorithm multiplies two large prime numbers to get a sufficiently large semi-prime number) and a computationally complex backward problem (e.g., factorizing the semi-prime number into its prime factors in RSA) that would take so long they are practically unbreakable with current supercomputers.

However, a sufficiently powerful quantum computer, referred to as a Cryptographically Relevant Quantum Computer (CRQC), can employ Shor's algorithm[i] to solve the backward problems within minutes, thus, posing a significant security threat.

2.1 Implications of Q-day

Q-day, when it arrives, will immensely affect today's systems, the internet, and applications. Key implications include:

- **Breakdown of digital security:** The most immediate consequence of Q-day is the potential breakdown of digital security. Quantum computers, with their advanced computational powers, could decrypt data that was presumed secure against classical computing attacks, exposing sensitive personal and national security information.
- **Financial systems risk:** The global financial system depends on cryptography for secure transactions; the quantum threat could destabilize these systems and threaten economic stability.
- **Data harvesting risk:** There's a risk that encrypted data is being collected now to be decrypted using a CRQC later, posing privacy and security threats. This is widely referred to as the Harvest Now, Decrypt Later (HNDL) attack.
- **Urgency in research and development:** The looming Q-day accelerates research and development for quantum-resistant cryptographic methods to protect against quantum attacks. Developing and implementing PQC is crucial to secure digital communications against quantum threats.

According to a McKinsey and Company report[ii], the public and financial sectors are highly vulnerable to HNDL attacks because of the critical, long-lasting data they handle and their extensive infrastructural lifecycles. These sectors are extremely important to the functioning of countries and societies and must be safeguarded against any attack. Thus, the banking and financial sectors must become aware of the quantum threats and solutions to safeguard against these attacks.

2.2 Vulnerabilities of current cryptographic methods

Symmetric encryption methods like AES and hash functions like SHA3 are considered quantum-resistant, if sufficiently large key sizes are used, reducing the impact of Grover's algorithm[iii]. However, most asymmetric key cryptography, such as RSA, Diffie-Hellman (DH), and Elliptic Curve Cyptography (ECC), remains vulnerable to quantum threats.These algorithms are crucial for key exchanges and digital signatures in everyday applications such as banking, web browsing, emails, VPNs, and SSH, posing risks to the confidentiality, integrity, and authenticity triad of digital security. These algorithms and their strengh against a CRQC, known as quantum strength, are listed in Table 1.

This article focuses on SD-WANs and site-to-site VPNs used in large enterprises, like banking and insurance, which rely on protocols like Internet Protocol Security (IPSec). IPSec uses public key algorithms to create secure tunnels for data exchange, making it susceptible to quantum attacks (Figure 1).

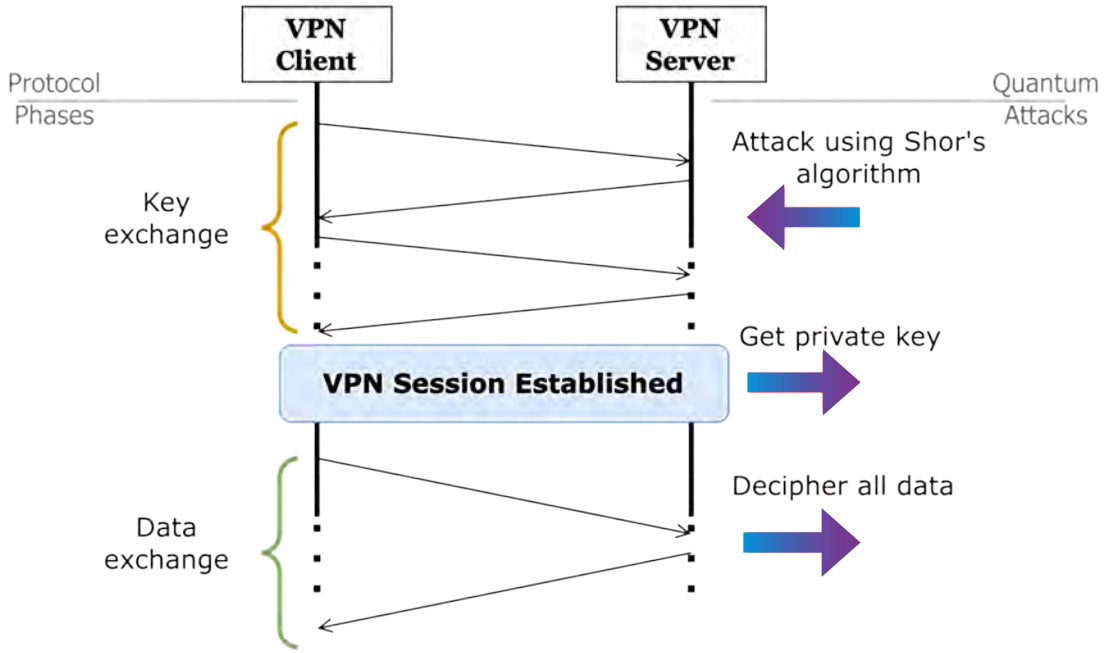
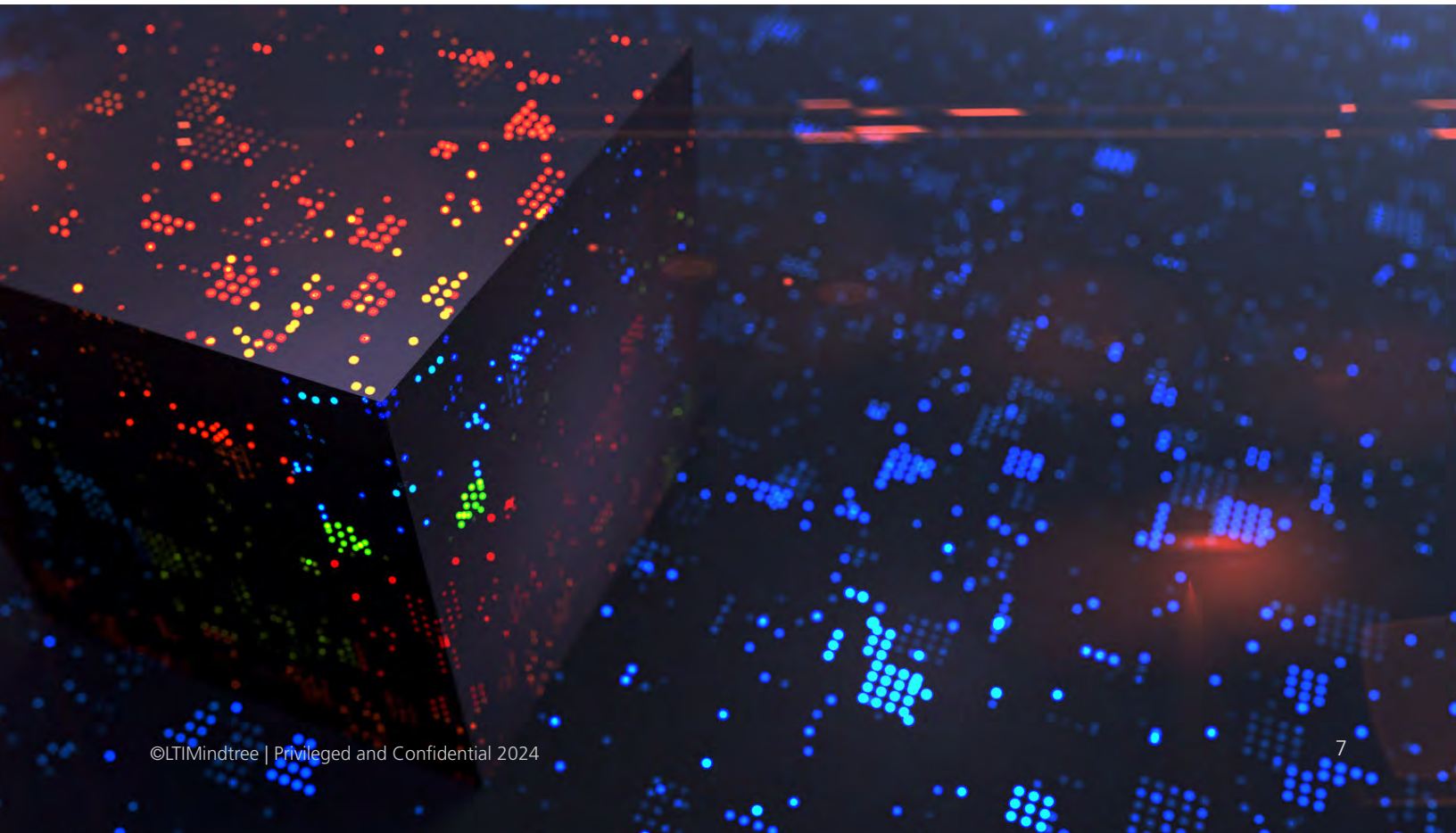


Figure 1: Quantum attack in VPNs

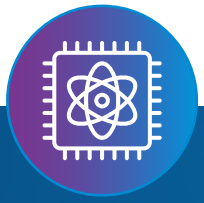
Algorithm	Crypto type	Purpose	Quantum strength (bits)	Recommendation
AES-128	Symmetric	Encryption	64	Larger key size needed
AES-256	Symmetric	Encryption	128	Larger key size needed
SHA-2 (384)	Hashing	Hash functions	128	Larger key size needed
SHA-3 (384)	Hashing	Hash functions	128	Larger key size needed
RSA-2048	Asymmetric	Key exchange, signatures	0	Employ PQC algorithms
RSA-3072	Asymmetric	Key exchange, signatures	0	Employ PQC algorithms
ECC-384	Asymmetric	Key exchange, signatures	0	Employ PQC algorithms
DH-2048	Asymmetric	Key exchange, signatures	0	Employ PQC algorithms

Table 1: Classical algorithms and their quantum strength



03 NIST standards and developments across the globe

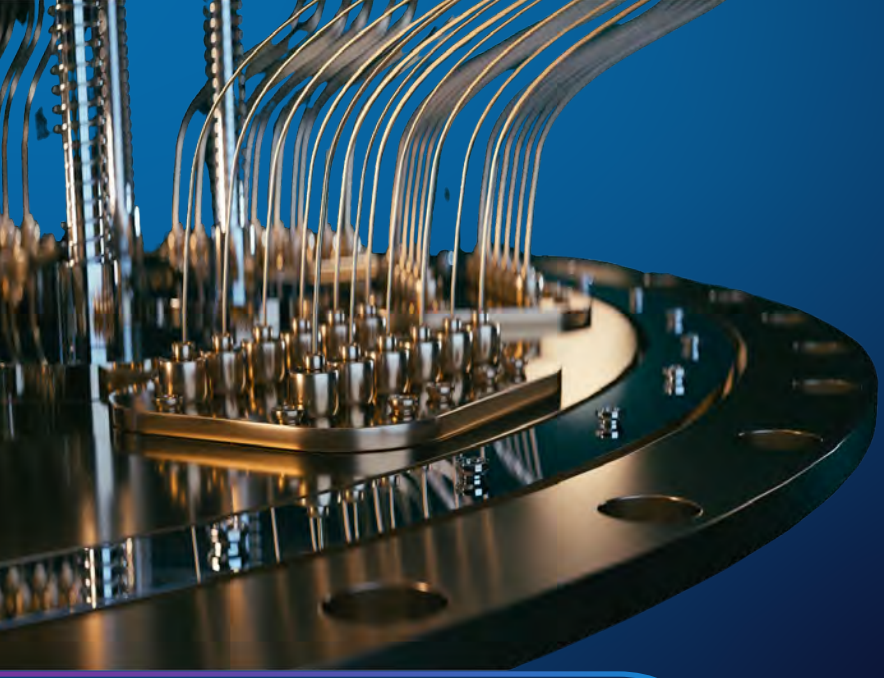
The National Institute of Standards and Technology (NIST) of the United States plays a crucial role in developing and recommending cryptographic standards for federal use and more broadly, for public use to ensure secure and trustworthy communications. With the emergence of quantum computing as a potential threat to current cryptographic standards, NIST has standardized three Post-Quantum Cryptography (PQC) algorithms.



How does PQC work?

PQC algorithms, designed to replace the vulnerable public key algorithms, are integrable into existing protocols to protect applications and infrastructure from quantum threats. PQC algorithms are based on the same philosophy as the current public key algorithms–the forward problem is simple, i.e., computing the keys is simple, but the reverse problem, decoding the keys, is extremely hard even for a CRQC.

The PQC algorithms can be implemented on current classical computers, laptops, and embedded devices and have no dependency on the availability of quantum computers.



Here is a high-level overview of the process NIST follows for PQC standardization:

In 2016, NIST began the process of selecting and standardizing quantum-resistant public-key cryptographic algorithms to counter the potential threats posed by quantum computers.

This process, involving extensive evaluation and competition, culminated in August 2024 with the finalization of three key standards, with a fourth algorithm expected to be standardized later in the year.

Figure 2: NIST standardization timeline, Key Takeaways from the Second PKI Consortium Post-Quantum Cryptography Conference, Hashed Out, Casey Crane, Nov 13, 2023: https://www.thesslstore.com/blog/

The standardized algorithms are described below-

1. **Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)** originally known as **CRYSTALS-Kyber algorithm,** has been standardized as Federal Information Processing Standard **(FIPS) 203.** This key encapsulation mechanism is designed for general encryption. It is praised for its efficiency in key establishment and the relatively small size of the encryption keys, which facilitates easy exchange between parties.
2. **Module-Lattice-Based Digital Signature Algorithm (ML-DSA)** originally known as CRYSTALS-Dilithium algorithm is now recognized as **FIPS 204.** This digital signature algorithm is known for its small key sizes and rapid signature generation. It provides robust security while maintaining performance, making it a top choice for digital signatures.
3. **Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)** originally known as **SPHINCS+.** This algorithm, standardized as **FIPS 205**, is a signature scheme based on hash functions. It offers stateless verification and is designed to withstand quantum attacks, providing a high level of security in various applications.

Although not yet finalized, another algorithm is expected to be standardized later in 2024.

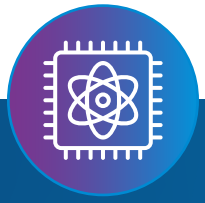
FFT over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), originally known as FALCON, is another digital signature mechanism that is designed for high performance and strong security. It leverages lattice-based cryptography, offering resistance against both conventional and quantum threats.

The standardization of PQC algorithms by NIST offers several benefits:

- **Security with confidence:** Standardized PQC algorithms ensure resistance against known and emerging quantum threats, increasing user confidence.
- **Works everywhere:** Standardized algorithms will enable interoperability and compatibility across different systems and applications.
- **Smooth transition to a quantum-resistant future:** Early adoption of PQC algorithms allows for a gradual migration to quantum-safe cryptography before large-scale quantum computers become a reality.

3.1 Global response and developments in quantum-resistant cryptography

The global efforts to develop standardized PQC algorithms have received significant participation from multiple organizations and countries, all aiming to mitigate the quantum threat. Many nations are aligning with NIST's outcomes and are establishing their guidelines for adoption and migration.



Banking sector efforts towards quantum-resistant cryptography

This collective effort highlights a worldwide commitment to fortifying digital infrastructure in the quantum era. The banking and insurance sectors are particularly active in raising awareness and developing guidelines for PQC migration, as shown in the table below.

Organization	Country	Efforts
Financial Industry Regulatory Authority (FINRA)	USA	Recommends institutions to closely follow NIST to prepare for migration to quantum-resistant algorithms[iv]
Financial Services Information Sharing and Analysis Center (FS-ISAC)	Global	Created a working group and documented the risks, challenges, and a wireframe to migrate towards PQC[v]
European Banking Authority (EBA) together with European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA)	EU	Released a draft of Digital Operational Resilience Act (DORA), which is already adopted in the EU, that recommends using quantum-resistant cryptography[vi]

Table 2: Banking sector efforts towards quantum-resistant cryptography

04 How to migrate to the post-quantum world?

Migrating to a quantum-resistant digital infrastructure is intricate and requires careful strategic planning to ensure no disruptions to businesses. Among several handbooks for migration, NIST, National Cybersecurity Center of Excellence (NCCoE) and Financial Services Information Sharing and Analysis Center (FS-ISAC) provide detailed guidelines. Based on their recommendations, the essential steps for migration are explained in the following subsections.

4.1 Assess your current maturity levels

Assessing your organization's current maturity levels of cryptographic assets and practices is the first step in the migration process. This step starts with identifying all the cryptographic assets in the organization. This is followed by assessing the risks of these assets for the quantum threats. The outcome of this step will be identifying the critical and sensitive assets that need to be secured.

Various methods can be used to identify the inventory, including questionnaires and automated tools. Passive network scanning and analysis tools, such as Quantum Xchange's Cipher Insights[vii], are extremely useful in identifying all the end points that generate traffic that does not comply with organization policies and is vulnerable to quantum threats.

Understanding the quantum security risk (Mosca's risk model)

To assess the quantum threat to your organization, consider three key factors:

- **Data shelf life (X):** Determine how long your data needs to be protected. This varies from short-term for temporary codes to long-term for sensitive data regulated by laws or specific needs.
- **Migration time (Y):** Evaluate the time needed to switch to a new, secure encryption method. This can be a quick change if your assets are highly crypto agile, but typically takes years to update and/or upgrade.
- **CRQC Arrival time (Z):** Estimate when CRQCs will be available.
- **Mosca's Theorem:** Using these parameters, check if X + Y > Z, then your data and infrastructure are no longer safe.

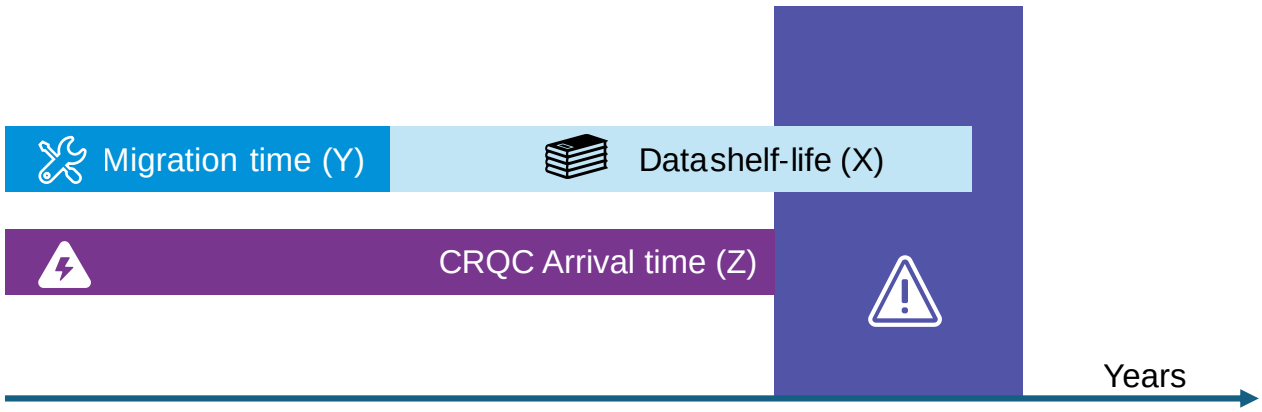


Figure 3: Depiction of Mosca's theorem, Future State Technical Paper, FS-ISAC, 2023 : https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf

4.2 Play, emulate, and test in a sandbox

After inventorying the cryptographic assets, the next step is selecting technology options for upgrading the encryption levels to PQC. It's crucial to choose solutions that support crypto-agility to facilitate future transitions to updated cryptographic standards easily.

It is also important to emulate deployment scenarios in a small-scale sandbox. This allows the stakeholders, like network architects, application architects, and information security teams, to play and test the solution for various aspects ranging from integration points to interoperability with current systems and performance impact on user experiences. Furthermore, this testing phase helps identify and address potential challenges that may occur during full-scale deployment.

4.3 A customized plan to suit your organizational needs

Typically, organizations can be categorized into one of the following:

Advanced crypto-agility

Organizations at the highest maturity level have implemented crypto-agility allowing them to switch between algorithms easily. They must continue to monitor PQC developments and ensure compatibility with new standards.

Early adopters of hybrid systems

Some organizations have started integrating hybrid systems that combine classical and quantum-resistant algorithms, placing them at an intermediate level of readiness for the quantum transition.

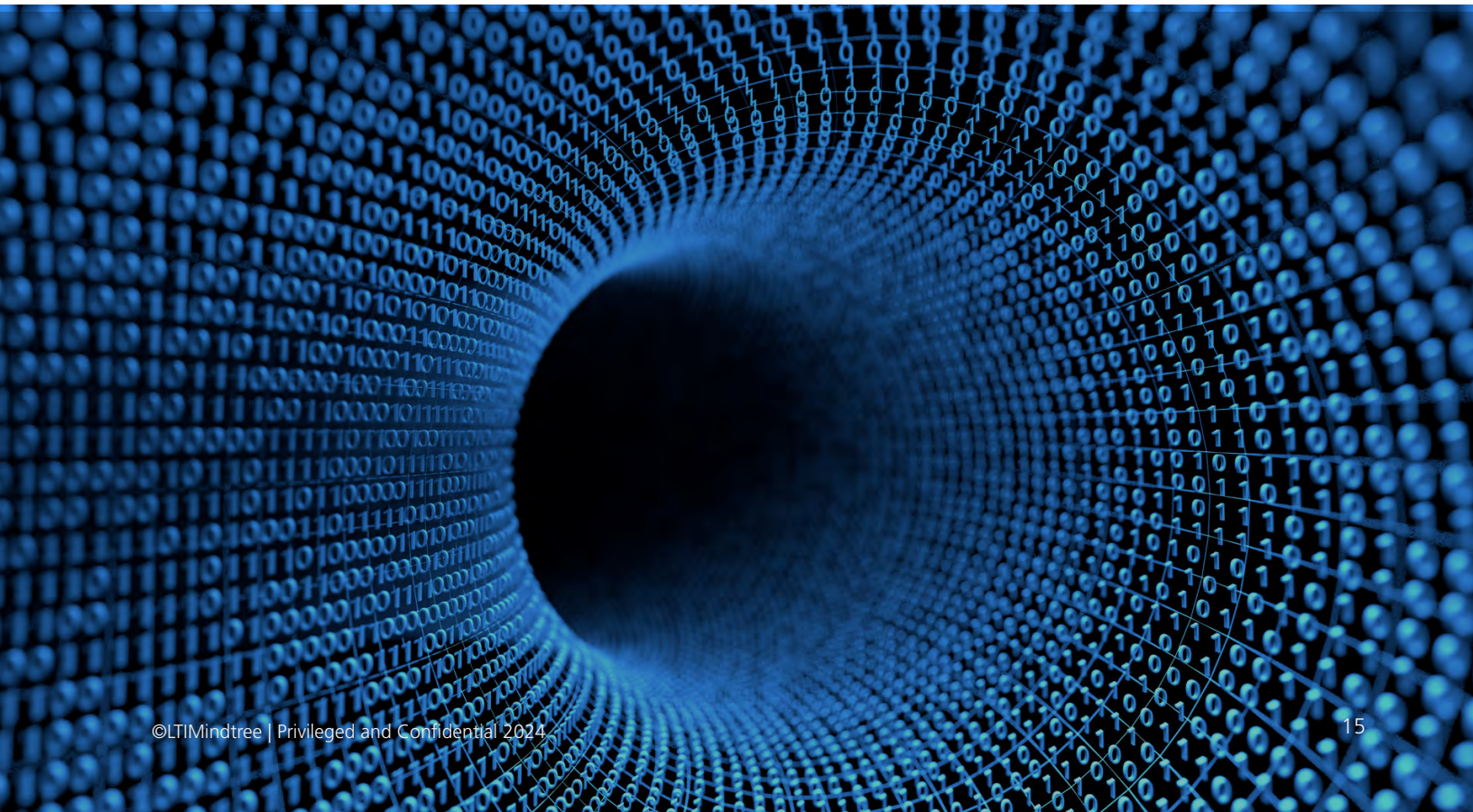
Fully classical cryptography

Organizations solely using classical cryptography are at the beginning of the maturity spectrum. They need a comprehensive plan to transition their critical systems to PQC.

A tailormade plan should be developed for the organization based on its category, security posture, quantum threat risk, PQC strategy, and minimizing any downtimes, among others. Typically, a phased approach is the most adopted one due to its pragmatism.

4.4 Deploy at scale

The chosen solution should be deployed as planned. While small-scale proof-of-concept may resolve many issues, large-scale deployment can reveal new challenges, e.g., performance impacts due to unexpected traffic surges. Thus, thorough testing is essential after every phase of the scaled implementation.



05 Considerations for selecting a PQC solution

When selecting a PQC solution, several critical factors must be considered to ensure the solution is appropriate, integrable, crypto agile, robust, and efficient:

Crypto-agility

It refers to the ability of an organization, system or equipment to switch between cryptographic algorithms easily without significant overhauls to the infrastructure. This is crucial for:

- **Futureproofing:** As quantum computing advances, the ability to integrate newer and more secure algorithms is crucial to adopt without major disruptions.
- **Threat response:** In the face of newly discovered vulnerabilities or attacks, the ability to swiftly change cryptographic algorithms is vital for maintaining security.
- **Flexibility:** Different applications may require different cryptographic strengths or algorithms. A crypto-agile system can cater to this diversity efficiently.

Separate control from data

In cryptographic systems, having a separate control channel for managing cryptographic operations like key management, algorithm selection, and policy enforcement from the data channel is important for several reasons.

- **Security:** Reduces the risk of a single point of failure. If the control mechanism is compromised, the encrypted data remains secure, and vice versa.
- **Scalability:** Allows updates in control mechanisms (like policies or algorithms) without altering the data, facilitating easier scaling.
- **Flexibility:** Enables finer control over cryptographic operations and assists in compliance without affecting data management.

Performance integrity

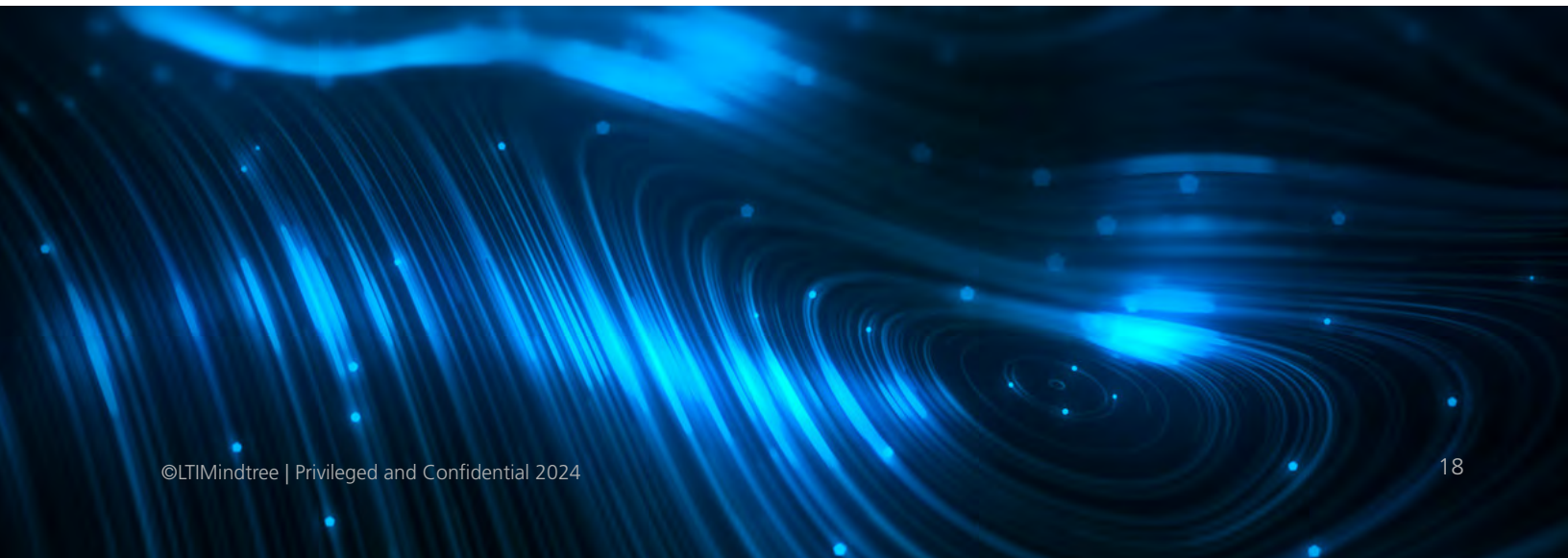
Ensuring PQC solutions do not drastically compromise on performance. Quantum-resistant algorithms are often more computationally intensive than their classical counterparts, which can impact system efficiency. Considerations include:

- **Processing speed:** Encryption and decryption processes should not significantly slow down system operations or user interactions.
- **Resource utilization:** PQC solutions should be resource-efficient, suitable even for devices with limited capabilities.
- **Scalability:** The PQC solution should handle increasing demands without excessive resource consumption or degradation of performance.

06 Our solution

In partnership with Quantum Xchange, we offer a streamlined, scalable, and robust PQC solution tailored for enterprise SD-WANs and site-to-site VPN networks. This solution not only provides crypto-agility but also introduces crypto diversification, enhancing security through features like continuous key rotation and intelligent multi-path key routing. This is achieved via a fault-tolerant, load-balanced mesh network, where each data link employs varied cryptographic methods — different PQCs, Quantum Key Distribution (QKD) if needed, or a combination. Such diversity and complexity in cryptographic approaches substantially mitigate risks, even if specific links or algorithms are compromised. Keys are generated using a FIPS-certified method incorporating multiple randomness sources, including Quantum Random Number Generators (QRNG), ensuring top-level security.

The solution consists of Phio TX, either in the form of physical rack mountable boxes or as a VM image, and a Phio TX cloud, called the hive. Together, they facilitate secure key exchanges, replacing traditional methods with more secure out-of-band key delivery via the hive. This setup enables post-quantum secure connections across VPNs/SD-WANs in data centers and offices, as demonstrated in a typical deployment scenario, as shown in Figure 3.



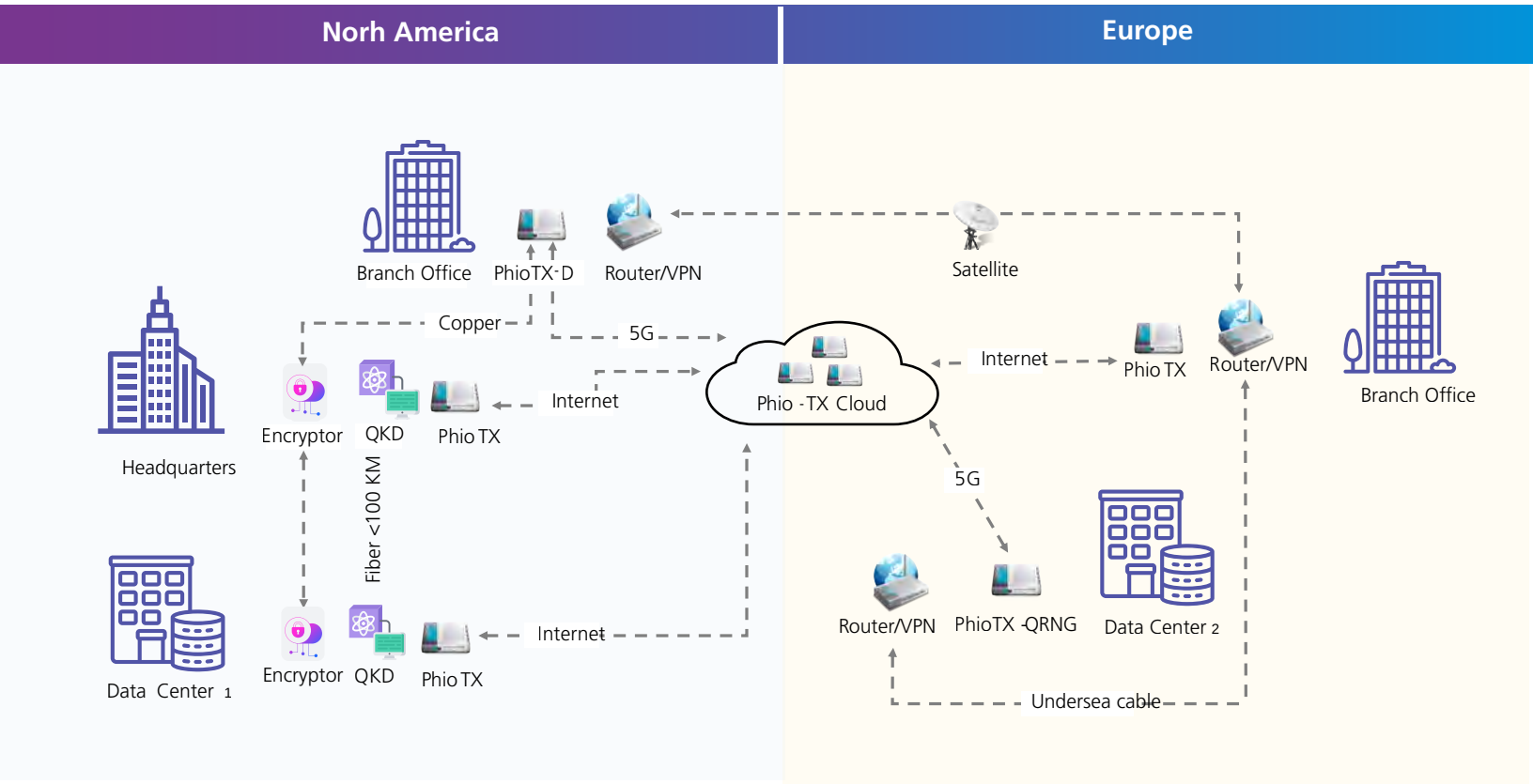


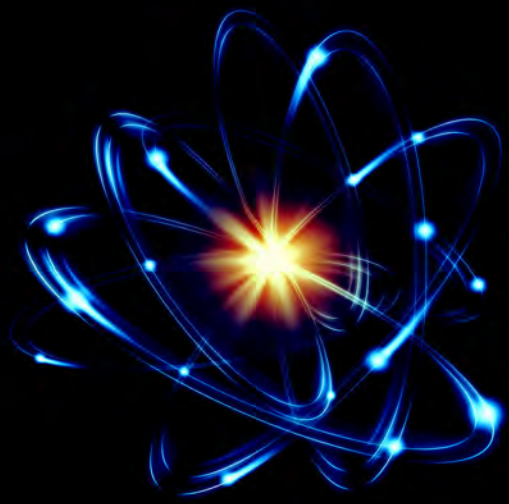
Figure 5. A typical Phio TX and the hive deployment scenario

Features

- FIPS 140-2/3 certified out-of-band key delivery: The out-of-band key delivery using the hive is scalable, robust to single point failures, and supports various deployment configurations (on-prem or on cloud).
- High security and unpredictable keys: Utilizing a FIPS-certified methodology with QRNG and multiple randomness sources for enhanced cyber protection.
- Crypto diverse and quantum-safe: Phio TX and the hive allow customization of each link with user-selected NIST-finalized PQC algorithms.
- Easy integration: Phio TX's ETSI-compliant interfaces facilitate simple integration into an existing system.

6.1 Our offerings

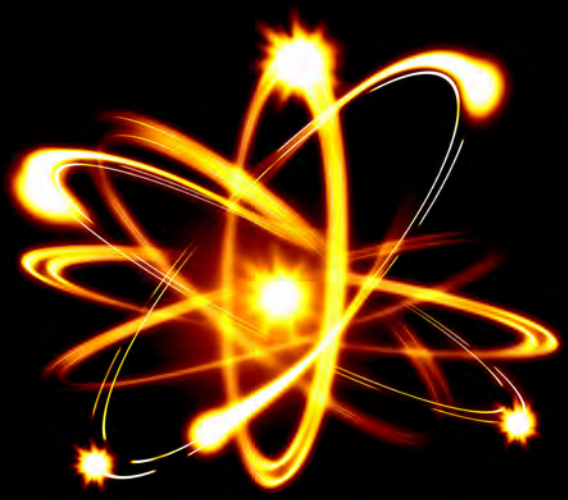
LTIMindtree, together with Quantum Xchange, offers end-to-end PQC migration offerings–from inventorying your cryptographic assets to deploying and maintaining the Quantum-Safe VPNs. For futher details about our latest offerings, visit *www.ltimindtree.com/quantum/.*



Quantum-Safeguard Discovery and Assessment (QSDA):

This service is tailored to help organizations tackle the challenges of quantum computing. We conduct a comprehensive evaluation to identify vulnerabilities to quantum threats within your cryptography defenses, focusing on both new projects and legacy systems.

By deeply assessing your current IT landscape, including networks, applications, and encryption methods, we identify the best opportunities for integrating quantum-safe technologies.



Quantum-safe Proof-of-Concept (PoC):

Before migrating all the infrastructure to PQC, it is important to understand the possibilities, integration points, and implications of integrating new infrastructure into your existing systems and networks. This service is designed to recreate the scenarios of a full-scale environment in a sandbox to understand and test the migration solutions.

We focus on the learning derived from the tests–the integration, security, and performance issues and solutions–and take them along when scaling up. Our clients can leverage our Quantum-Safe VPN testbed in London[ix], thereby enabling a faster PoC testing and evaluation process.

Quantum-safe VPN:

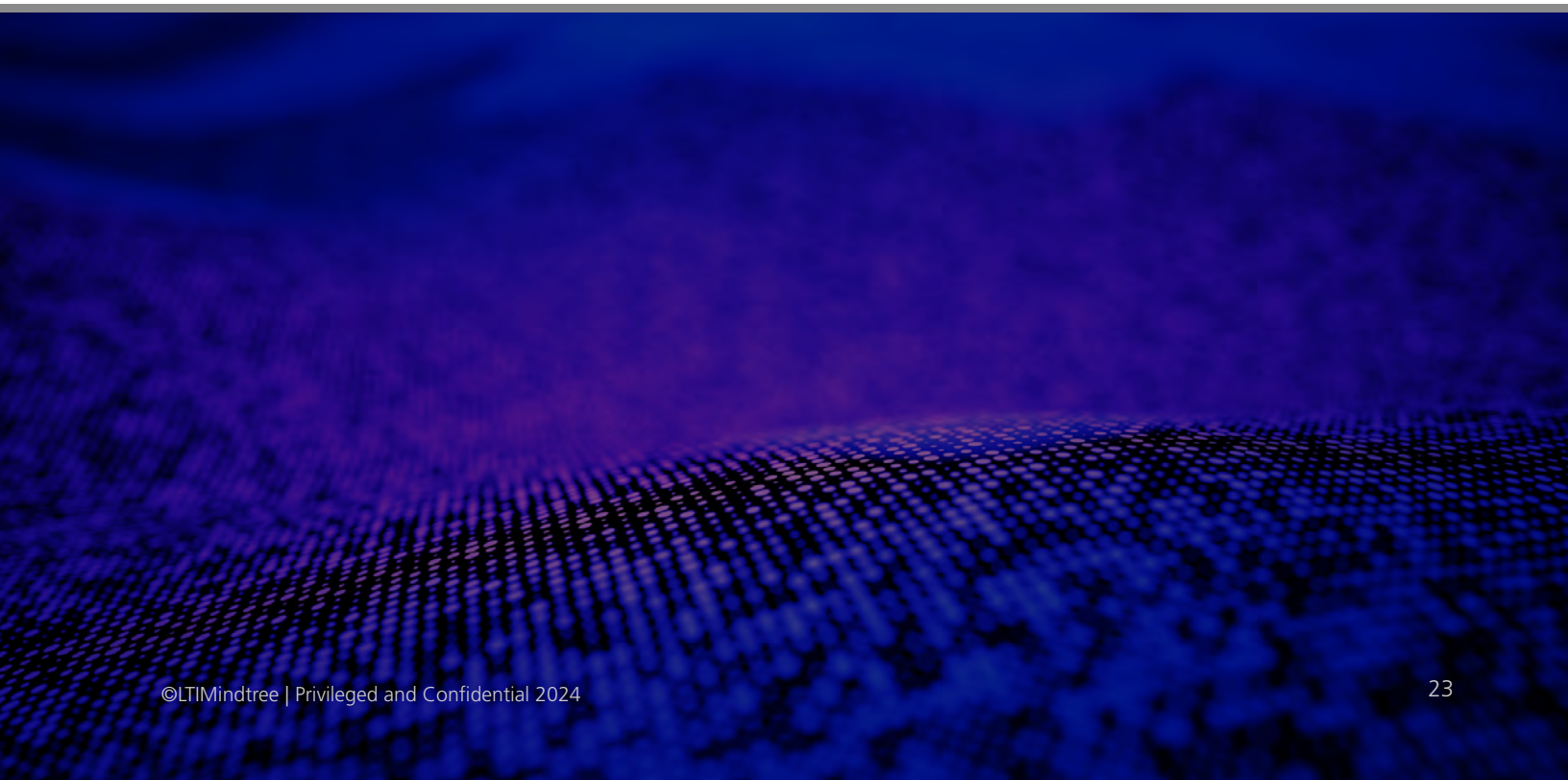
We assist in every step of the migration to PQC. Accordingly, this service focuses on planning, deploying, integrating, and testing Quantum Xchange's Phio TX and hive at scale to make your infrastructure quantum safe.

LTIMindtree will help create a strategy for migration tailormade for your organization based on your organization's priorities and other parameters. Based on the inputs and learnings from the QSDA and PoC stages, a plan for a smooth transition will be carefully crafted. The optimization factors would be quick integration and deployment with minimal downtime and disruptions to users. The integration and deployment will then follow based on the deployment model chosen (on-prem or on cloud) hive. Rigorous testing and performance tuning will be done to ensure smooth operation in the long run.

07 Conclusion

Quantum computing introduces significant vulnerabilities in traditional cryptographic defences, as most IT security systems depend on public-key cryptography which is susceptible to quantum attacks. The threat includes potential HNDL attacks where data and public keys are stored to be decrypted by quantum computers in the future. As advised by NIST's Matthew Scholl, "It's no time to panic, it's time to plan wisely."

LTIMindtree, in partnership with Quantum Xchange, offers a comprehensive suite of quantum-safe security solutions to help organizations migrate to PQC. This includes identifying cryptographic assets and network vulnerabilities and securing them with a PQC-enabled VPN. Our solution features the enterprise-ready, FIPS-certified Phio TX and hive, ensuring a robust network communication infrastructure that is protected against future quantum threats with a quantum-in-depth strategy and advanced key delivery architecture.



08 References

i. Algorithms for quantum computation: discrete logarithms and factoring, P. W. Shor, Proceedings 35th annual symposium on foundations of computer science, pp. 124–134, 1994: https://search.worldcat.org/title/filter-bubble-what-the-internet-is-hiding-from-you/oclc/682892628

ii. When—and how—to prepare for post-quantum cryptography, Lennart Baumgärtner, Benjamin Klein, Niko Mohr, Anika Pflanzer, and Henning Soller, McKinsey & Company, 4 May 2022: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

iii. A fast quantum mechanical algorithm for database search, L. K. Grover, in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219: hhttps://dl.acm.org/doi/10.1145/237814.237866

iv. Section IV: Regulatory Considerations for Quantum Computing, FINRA.org: https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing/regulatory-considerations

v. Preparing for a Post-Quantum World by Managing Cryptographic Risk, FS-ISAC. Post-Quantum Cryptography Report: https://www.fsisac.com/knowledge/pqc

vi. ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification, European Banking Authority, 17 January 2024: https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party

vii. Cyber Risk Discovery & Cryptographic Inventory, CipherInsights | Quantum Xchange: https://quantumxc.com/cipherinsights/

viii. Enterprise Cryptographic Management, Quantum Xchange : https://quantumxc.com/

ix. LTIMindtree Launches and Tests Quantum-Safe VPN Link in London in Collaboration with Quantum Xchange & Fortinet Business Wire, Business Wire, 23 November 2023: https://www.businesswire.com/news/home/20231122868313/en/LTIMindtree-Launches-and-Tests-Quantum-Safe-VPN-Link-in-London-in-Collaboration-with-Quantum-Xchange-Fortinet

09 Authors

Dr.ir. Vijay S. Rao,

Research Leader, LTIMindtree

Vijay is responsible for incubating and building capabilities in new technologies, exploring technologies and establishing partnerships, and providing thought leadership. He is currently working on post-quantum cryptography solutions.

Vijay is a seasoned IoT solutions architect and software engineer with a strong track record in technology project leadership and product development. He holds a Ph.D. in Computer Science and an M.Sc. in Telecommunications from Delft University of Technology. His academic excellence is reflected in multiple best-paper awards at prestigious conferences, numerous high-quality publications, three patents, and contributions to two IEEE standards.

Dr. Nayana Das,

Research Engineer, LTIMindtree

Nayana specializes in quantum communication and post-quantum cryptography. With over eight years of experience in cryptography and information security, she has made significant contributions to the field.

Nayana earned her Ph.D. in Computer Science from the Indian Statistical Institute, specializing in quantum cryptography. Prior to that, she completed her M.Sc. in Pure Mathematics at Calcutta University, building a strong foundation for her research. Throughout her career, Nayana has published more than 10 research papers in prestigious journals and has applied for several patents. Her work continues to push the boundaries of secure communication technology in the quantum era.

Fabien Adouani,

Vice President of Business Development, Quantum Xchange

With a robust background in the Information Technology industry spanning over two decades, Fabien's expertise lies in driving digital transformation and enhancing cybersecurity frameworks. Throughout his career, Fabien has held senior leadership roles, focusing on quantum encryption and cybersecurity solutions.

Fabien's strategic vision has consistently propelled technological advancements and fortified security measures across various enterprises. Fabien's academic credentials include a Master of Advanced Studies in marketing from LRG University and an MBA from the Glion Institute of Higher Education in Switzerland.

Mehul Gandhi,

Senior Director of Cybersecurity, LTIMindtree

With over 25 years in IT, Mehul Gandhi is a seasoned expert in cybersecurity consulting, cyber defense, and cloud security.

As Senior Director, he has led significant cybersecurity transformations, aligning IT strategies with business objectives for enhanced digital security. Currently, he aids clients in proactive threat management, blockchain security, and quantum-safe initiatives.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 81,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit https://www.ltimindtree.com/.