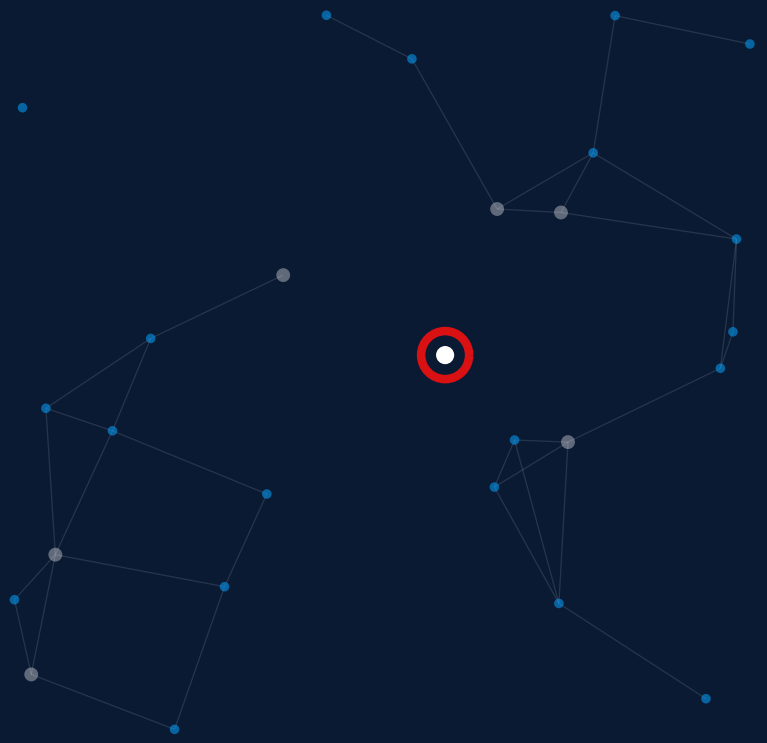
KRYNTHNODE



Cybersecurity and digital risk | Report

Post-quantum cryptography

A migration roadmap for Indian enterprises

Published 1 September 2026
Krynthnode Research and Advisory LLP | krynthnode.com

Research that shows its working.

Executive summary

Much of today's secure communication relies on public-key algorithms such as RSA and elliptic-curve cryptography. A sufficiently capable quantum computer could break them. Nobody can say with certainty when such a machine will exist, but the risk is already present for data that must remain confidential for many years, because encrypted traffic captured today could be decrypted later.

In August 2024, the US National Institute of Standards and Technology published its first post-quantum cryptography standards. Governments and major technology providers have since begun setting migration timelines. This report explains what has changed and sets out a practical, staged roadmap for Indian enterprises, beginning with the work that is valuable regardless of how quickly quantum computing advances.

Key findings	Confidence
The first post-quantum standards are final: FIPS 203 (ML-KEM) for key establishment, and FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) for digital signatures.	High confidence
Harvest-now, decrypt-later attacks make migration urgent for data with long confidentiality requirements, even though the timing of cryptographically relevant quantum computers is uncertain.	Moderate confidence
A cryptographic inventory is the essential first step, and most organisations do not have one.	High confidence
Much of the migration will arrive through vendor updates, so vendor roadmaps and contract terms matter as much as internal engineering.	Moderate confidence

Each finding is graded in the Krynthnode confidence ledger. See the methodology at the end of this report.

What we recommend

1. Build an inventory of where public-key cryptography is used, including in vendor products and connected devices.
2. Classify data by how long it must remain confidential, and prioritise systems that protect long-lived data.
3. Ask critical vendors for their post-quantum roadmaps, and add crypto-agility requirements to new contracts.
4. Pilot hybrid key exchange in a contained environment to learn about performance and compatibility.
5. Assign an executive owner and review progress annually as standards and timelines evolve.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

The quantum threat, in plain terms

Public-key cryptography protects key exchange and digital signatures in protocols such as TLS, VPNs, code signing and secure email. Its security rests on mathematical problems that are hard for classical computers, such as factoring large numbers. Shor's algorithm, run on a large, error-corrected quantum computer, could solve these problems efficiently.

Symmetric encryption such as AES is far less affected; using sufficiently long keys, such as AES-256, is generally considered adequate. The urgent work is replacing the public-key algorithms used for key establishment and signatures.

The new standards

Standard	Algorithm	Purpose
FIPS 203	ML-KEM (from CRYSTALS-Kyber)	Key encapsulation, used to establish shared keys
FIPS 204	ML-DSA (from CRYSTALS-Dilithium)	Digital signatures, the primary general-purpose choice
FIPS 205	SLH-DSA (from SPHINCS+)	Hash-based digital signatures, a conservative alternative

NIST has also selected HQC as an additional key encapsulation algorithm, based on different mathematics, as a backup to ML-KEM, and is developing a further signature standard based on FALCON. In its draft transition guidance, NIST IR 8547, it proposed deprecating widely used quantum-vulnerable algorithms from 2030 and disallowing them from 2035. Organisations should track the final guidance, as well as timelines set by their own regulators and customers.

Why start now

Three reasons make early preparation sensible even though the arrival of cryptographically relevant quantum computers is uncertain. First, harvest-now, decrypt-later attacks put today's long-lived secrets at risk. Second, large organisations take many years to replace cryptography, which is embedded in applications, devices, hardware security modules and supplier products. Third, the first step, understanding where cryptography is used, improves security and resilience regardless of the quantum timeline.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

A staged migration roadmap

Stage	What to do	Outcome
1. Inventory	Discover where public-key cryptography is used: protocols, libraries, certificates, devices, vendor products.	A cryptographic bill of materials
2. Prioritise	Rank systems by the confidentiality lifetime of their data and their exposure.	A risk-ranked migration list
3. Prepare	Build crypto-agility; engage vendors; update procurement requirements.	Systems and contracts ready to change algorithms
4. Pilot	Test hybrid key exchange, combining classical and post-quantum algorithms, in contained environments.	Evidence on performance and compatibility
5. Migrate	Roll out in priority order, starting with externally facing and long-lived-data systems.	Reduced quantum exposure, tracked by metrics

Crypto-agility: the lasting benefit

Crypto-agility means designing systems so that cryptographic algorithms can be replaced without rebuilding the applications that use them. It depends on centralised cryptographic libraries and services, well-managed certificates and keys, and configuration rather than hard-coding. Organisations that invest in crypto-agility will find this migration, and future ones, far less disruptive.

Questions for your vendors

- Which of your products use public-key cryptography, and for what purposes?
- What is your roadmap and timeline for supporting ML-KEM and ML-DSA?
- Will post-quantum support be delivered as a software update, or does it require new hardware?
- How will you support hybrid modes during the transition?
- What performance impact should we expect?

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Methodology and the confidence ledger

This report draws on NIST's published standards and transition guidance, and on guidance from national security agencies, applied to the context of Indian enterprises. Timelines in draft guidance may change; confirm current positions before making commitments.

Grade	What it means	How to use it
High confidence	Consistent across several independent sources and established practice.	Suitable for committing budget.
Moderate confidence	Supported, with some gaps or variation between contexts.	Suitable for a pilot with a review date.
Emerging evidence	Limited or recent evidence.	Worth monitoring before acting.

References

1. National Institute of Standards and Technology. FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.
2. National Institute of Standards and Technology. FIPS 204, Module-Lattice-Based Digital Signature Standard. August 2024.
3. National Institute of Standards and Technology. FIPS 205, Stateless Hash-Based Digital Signature Standard. August 2024.
4. National Institute of Standards and Technology. NIST IR 8547 (initial public draft), Transition to Post-Quantum Cryptography Standards. November 2024.
5. National Institute of Standards and Technology. Selection of HQC for standardisation. March 2025.
6. US National Security Agency. Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). September 2022.

About Krynthnode

Krynthnode Research and Advisory LLP is an independent technology and cybersecurity research and advisory firm. We help leaders make decisions they can defend: every finding we publish carries its evidence, its sources and an honest rating of how sure we are. We do not sell technology, take referral fees or accept payment for ratings.

To discuss this research with the analyst team, visit krynthnode.com/contact or email hello@krynthnode.com.

This publication reflects the views of Krynthnode analysts based on the sources available at the time of writing. It is provided for information and is not legal, regulatory, financial or investment advice. Mention of any organisation, product or standard is not an endorsement. Trademarks belong to their respective owners. No part of this publication may be reproduced or redistributed without written permission, except for short quotations with attribution.