

Post-Quantum Cryptography for Secure Governance: Challenges and Opportunities for India

Deveshree Dhobe

Computer Science & Engineering
Government College of Engineering, Nagpur
Nagpur, India

Swarnima Potdar

Computer Science & Engineering
Government College of Engineering, Nagpur
Nagpur, India

Abstract—India’s digital governance infrastructure, spanning Aadhaar, UPI, DigiLocker, and critical sectors such as defence, finance, and telecommunications, is built upon classical public-key cryptography (RSA, ECC). The emergence of fault-tolerant quantum computers threatens to dismantle these foundations through Shor’s algorithm, which solves integer factorisation and discrete logarithm problems in polynomial time, while Grover’s algorithm reduces symmetric key security. The “harvest now, decrypt later” strategy magnifies the urgency, as adversaries can store encrypted data today for future decryption. This paper provides a comprehensive analysis of the post-quantum cryptography (PQC) migration imperative for India. We examine the quantum threat landscape, review candidate PQC families (lattice-, code-, multivariate-, hash-, and isogeny-based) and the newly standardised NIST algorithms, and detail the technical, regulatory, and economic challenges of large-scale PQC adoption in India’s heterogeneous e-governance ecosystem. A phased implementation roadmap aligned with the National Quantum Mission (2026 to 2035) is presented, prioritising critical sectors (defence, banking, telecom, Aadhaar/UPI). The paper further highlights strategic opportunities for indigenous capability building, global certification leadership, and the reinforcement of digital sovereignty. By synthesising official reports, international standards, and sector-specific requirements, this work offers actionable guidance for transitioning India’s governance to a quantum-resilient future.

The paper further proposes the Quantum Governance Readiness and Infrastructure Decision Framework (Q-GRID), an India-specific, measurable decision framework that integrates quantum exposure, data longevity, systemic criticality, dependency, migration complexity, and regulatory urgency into a composite Quantum Risk Index to prioritise migration actions.

Index Terms—Quantum threat, post-quantum cryptography, Shor’s algorithm, cryptographic agility, India cybersecurity, National Quantum Mission, Aadhaar, UPI, Q-GRID framework.

I. INTRODUCTION

India has undergone one of the world’s most rapid digital transformations. Its governance infrastructure is anchored by platforms such as Aadhaar (the biometric-based digital identity system serving over 1.3 billion residents), the Unified Payments Interface (UPI) processing more than 10 billion transactions per month, DigiLocker, and a wide array of e-government portals. These systems depend on public-key cryptography to establish trust, authenticate users, and protect sensitive data. Every UPI transaction, every Aadhaar authentication, and every government cloud service is secured by digital certificates and signatures rooted in RSA and elliptic curve cryptography (ECC) [1]. The economic and social reliance on this cryptographic trust is immense; a

systemic failure would disrupt financial stability, erode citizen confidence, and compromise national security.

Classical public-key algorithms derive their security from the computational hardness of integer factorisation (RSA) and discrete logarithm problems (Diffie-Hellman, ECC). These problems, however, are rendered tractable by a sufficiently large, fault-tolerant quantum computer running Shor’s algorithm [2], [3]. Unlike the gradual evolution of classical threats, the quantum threat is both catastrophic and retroactive: adversaries can harvest encrypted traffic now and store it for decryption once cryptographically relevant quantum computers (CRQCs) become available, a strategy known as “harvest now, decrypt later” (HNDL) [4], [5]. Data with long confidentiality horizons, including defence communications, financial transaction logs, healthcare records, and land registries, is particularly vulnerable.

The quantum computing timeline is accelerating. Advances in qubit quality, error correction, and algorithmic optimisations have led analysts to shorten the expected arrival of a CRQC to within the next decade [6]. Consequently, the security of sensitive data that must remain confidential beyond 5 to 10 years is already at risk. India’s leadership has recognised this imperative. Under the National Quantum Mission (NQM), a high-level Task Force convened by the Department of Science and Technology (DST) released a comprehensive roadmap for a quantum-safe ecosystem in February 2026 [7]. The document mandates that critical information infrastructure (CII) begin formal PQC adoption by 2027, with full enterprise-wide compliance by 2033. The policy message is unequivocal: quantum risk is no longer hypothetical but a fundamental challenge to digital sovereignty.

Post-quantum cryptography (PQC) refers to classical cryptographic algorithms that are believed to be resistant to quantum attacks. Unlike quantum key distribution (QKD), which requires specialised hardware, PQC can be deployed as a software upgrade on existing infrastructure, making it a scalable solution for the vast majority of India’s e-governance systems. The United States National Institute of Standards and Technology (NIST) finalised its first three PQC standards in 2024: ML-KEM (FIPS 203) for key encapsulation, ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures [8]. These standards, based on lattice and

hashbased constructions, now form the international baseline for migration.

TABLE I

QUANTUM RESOURCE ESTIMATES FOR SHOR'S ALGORITHM [3]

Classical Security	RSA/DH Key	ECC Key	Logical Qubits (RSA/DH / ECC)
112 bits	2048 bits	224 bits	4098 / 2042
128 bits	3072 bits	256 bits	6146 / 2330
192 bits	7680 bits	384 bits	15362 / 3484

This paper provides a unified, in-depth examination of the challenges and opportunities associated with migrating India's digital governance to PQC. It synthesises technical, policy, and strategic perspectives drawn from official reports, international standards, and academic literature. Section II details the quantum threat landscape. Section III surveys PQC algorithm families and the new NIST standards. Section IV analyses the technical implementation challenges unique to India's e-governance ecosystem. Section V discusses the evolving policy and regulatory framework. Section VI presents a phased implementation roadmap. Section VII examines sector-wise priorities. Section VIII explores economic and strategic opportunities. Section IX addresses capacity building and coordination. Section X concludes with actionable recommendations.

II. QUANTUM THREAT LANDSCAPE

A. Quantum Computing Fundamentals

Quantum computing harnesses three fundamental quantum mechanical phenomena: superposition, entanglement, and the quantum Fourier transform (QFT). A qubit, unlike a classical bit, can exist in a superposition of $|0\rangle$ and $|1\rangle$ states: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ [9]. This property, combined with entanglement, namely non-classical correlations that link the states of multiple qubits, enables a quantum computer with n qubits to process a superposition of all 2^n possible computational basis states simultaneously. While superposition provides massive parallelism, it is the QFT that extracts structured global information from that superposition, enabling exponential speed-ups for specific problems.

B. Shor's Algorithm and Asymmetric Cryptanalysis

Shor's algorithm (1994) exploits the QFT to solve the integer factorisation and discrete logarithm problems in polynomial time. For RSA, the algorithm reduces factoring an integer N to the efficient quantum determination of the multiplicative order r of a random element a modulo N [2]. For an n -bit modulus, Shor's algorithm requires approximately $2n$ logical qubits for RSA/DH and about $10n$ logical qubits for ECC, due to the need to embed elliptic curve points. Table I provides comparative resource estimates.

Fig. 1 provides a compact visual summary of the broader quantum-computing and post-quantum-security landscape discussed in this paper.

Despite ECC requiring more qubits per key-bit, its smaller absolute key size means that for a given classical security level, the total number of logical qubits required to break ECC is often lower than that needed for RSA. For example,



Fig. 1. Quantum computing and post-quantum security landscape.

breaking ECDSA-256 (~ 2330 logical qubits) is computationally less demanding than breaking RSA-3072 (~ 6146 logical qubits). Modern metrics like "megaqubit-days" further refine these comparisons: under a physical error rate of 10^{-3} , RSA-2048 costs 1.17 megaqubit-days while ECDSA-256 costs 7.43 megaqubit-days [3]. These figures underscore that all widely deployed public-key systems will become insecure when CRQCs materialise.

C. Grover's Algorithm and Symmetric Cryptography

Grover's algorithm (1996) provides a quadratic speed-up for unstructured search. Its impact on symmetric cryptography is less severe: a 256-bit AES key effectively offers 128-bit security against a quantum adversary, which is still considered secure. Countermeasures such as doubling key lengths (e.g., AES-256 to provide post-quantum resilience) are straightforward. Hash functions must similarly increase output lengths to maintain collision resistance. Thus, symmetric primitives require parameter adjustments but not a complete algorithmic overhaul, unlike asymmetric schemes which demand fundamentally new mathematical foundations.

D. The "Harvest Now, Decrypt Later" (HNDL) Threat

The HNDL strategy exacerbates the quantum threat timeline. Adversaries, whether state-sponsored or cybercriminal, can intercept and archive encrypted communications today, betting that future quantum computers will enable decryption. This means that even if CRQCs remain a decade away, data that must remain secret for 15 to 20 years is effectively compromised today. For India, this encompasses defence secrets, diplomatic cables, critical infrastructure designs, financial records governed by long retention rules, biometric databases, and the entire Aadhaar transaction history. The DST Task Force explicitly warns that "quantum computing technologies... could break many of the cryptographic algorithms currently used to secure digital communications, banking systems, government networks and critical infrastructure," threatening data security far into the future [7]. The HNDL threat transforms post-quantum migration from a future research problem into an immediate national security priority.

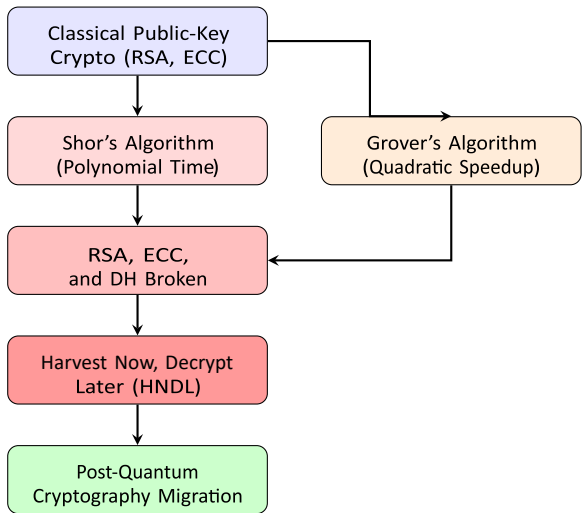


Fig. 2. Quantum threat flow: Shor’s and Grover’s algorithms weaken classical cryptography, enable the HNDL threat, and necessitate migration to PQC.

Fig. 2 summarises how quantum algorithms undermine classical cryptography and intensify the HNDL risk, thereby making migration to PQC unavoidable.

III. POST-QUANTUM CRYPTOGRAPHY: ALGORITHMS AND STANDARDS

A. Families of Post-Quantum Algorithms

PQC candidates are built on mathematical problems believed to be hard for both classical and quantum computers. Five main families exist:

- 1) Lattice-based cryptography: Relies on the hardness of problems such as Learning With Errors (LWE) and its ring/module variants. Examples include CRYSTALSkyber (key encapsulation) and CRYSTALS-Dilithium (signatures). Lattice schemes offer moderate key and ciphertext sizes and efficient operations, making them the most mature and favoured category.
- 2) Code-based cryptography: Based on the difficulty of decoding random linear codes. The most prominent candidate is Classic McEliece, which boasts exceptional security pedigree but has public keys exceeding 100 kB, limiting its use to long-term confidentiality scenarios.
- 3) Multivariate cryptography: Uses the difficulty of solving systems of multivariate polynomial equations over finite fields. Some signature schemes (e.g., Rainbow) have been broken in recent years, tempering enthusiasm.
- 4) Hash-based signatures: Construct digital signatures solely from cryptographic hash functions. Stateless schemes like SPHINCS+ (standardised as SLH-DSA) offer strong security guarantees but produce relatively large signatures (~40 kB).
- 5) Isogeny-based cryptography: Leverages the hardness of finding isogenies between supersingular elliptic curves. SIKE, the leading isogeny scheme, was broken

in 2022, although research continues on more robust parameters.

TABLE II CLASSICAL VS. POST-QUANTUM CRYPTOGRAPHY		
Aspect	Classical (RSA/ECC)	Post-Quantum (Kyber, Dilithium)
Foundation Problem	Integer factorisation, discrete log	Lattice problems (LWE), code decoding, hash
Quantum Attack	Broken by Shor (RSA/ECC); Grover reduces symmetric strength	No known polynomial-time attacks
Key Sizes	RSA-2048 (~2 kB); ECC256 (~64 B)	Kyber-768 (~1 kB); McEliece (>100 kB); SPHINCS+ (~40 kB)
Performance	Well-optimised, fast	Generally slower (2 to 10 times overhead) and heavier memory footprint
Maturity	Decades of deployment	NIST standards finalised 2024; implementations maturing
Trust Model	Widely trusted, mature PKI	Requires cryptoagile architectures and extensive validation

B. NIST PQC Standards (2024)

After a multi-year evaluation process, NIST standardised three algorithms in August 2024 [8]:

- FIPS 203 (ML-KEM): A Module-Lattice-based Key Encapsulation Mechanism derived from CRYSTALSkyber. Recommended parameter set ML-KEM-768 provides 128-bit post-quantum security, with ciphertexts of ~ 1088 bytes (approximately 30 to 40 times larger than ECDH).
- FIPS 204 (ML-DSA): A Module-Lattice-based Digital Signature Algorithm, previously CRYSTALS-Dilithium. Signatures for ML-DSA-65 are ~ 3309 bytes, roughly 50× larger than ECDSA P-256 signatures.
- FIPS 205 (SLH-DSA): A Stateless Hash-Based Signature Scheme based on SPHINCS+. Signature sizes are larger (approximately 17 to 40 kB) but it offers conservative security independent of lattice assumptions.

Additionally, NIST has selected a fourth key-encapsulation algorithm (based on isogenies) for future standardisation as a backup, and is evaluating additional signature schemes to provide diversity.

Table II compares classical and post-quantum cryptographic characteristics.

India's official policy, reflected in the DST roadmap, explicitly adopts NIST PQC standards as the baseline while allowing for the evaluation of indigenous variants provided they meet interoperability and security criteria [7], [10].

IV. TECHNICAL IMPLEMENTATION CHALLENGES IN INDIA'S E-GOVERNANCE

Migrating India's vast and diverse digital infrastructure to PQC presents unprecedented technical hurdles. These challenges span computation, storage, bandwidth, interoperability, and human capital.

A. Computation and Bandwidth Overhead

PQC algorithms require significantly greater computational resources and produce larger ciphertexts, keys, and signatures than classical cryptography. ML-KEM-768 ciphertexts are approximately 30 to 40 times larger than ECDH; MLDSA signatures are roughly 50× larger than ECDSA. These increases directly affect:

- Resource-constrained devices: Aadhaar biometric readers, point-of-sale terminals, IoT sensors, and low-cost smartphones will face CPU, memory, and battery strain. For instance, an Aadhaar authentication device that currently completes a transaction in under one second could experience noticeable latency with PQC operations.
- Bandwidth-limited environments: Rural areas with 2G/3G or limited 4G connectivity will see slower data transmissions due to larger message sizes. The increased bandwidth consumption could raise costs for users and strain mobile network capacity.
- Backend infrastructure: High-frequency systems like UPI switches and telecom handshake protocols will accumulate additional processing delays. Early benchmarks indicate PQC encryption/signing is 2 to 10 times slower than optimised ECC.

Mitigation strategies include hardware acceleration (ASICs/FPGAs), edge-processing, and careful selection of parameter sets balancing security, speed, and size.

B. Legacy System Integration and Interoperability

India's e-governance stacks (UIDAI Aadhaar platform, NPCI UPI switches, state-level e-district portals) were built around RSA/ECC PKI and conventional TLS implementations. Many components, including Hardware Security Modules (HSMs), operating system kernels, and embedded cryptographic libraries, are not designed for PQC. Identifying every cryptographic instance in decades-old core banking systems or telecom infrastructure has been described as "archaeological-level work" [11]. Furthermore, UPI interconnects over 400 banks; a single non-upgraded participant creates a vulnerability for the entire ecosystem.

Transitioning requires a "dual-stack" approach, where systems simultaneously support classical and PQC algorithms during a lengthy coexistence period. Hybrid key exchange (e.g., combining ECDH with ML-KEM) provides resilience if one scheme is broken, but adds protocol complexity, larger handshake messages, and increased

latency. Ensuring crossvendor and cross-border interoperability is critical; TLS libraries must offer standardised PQC cipher suites, and national testing facilities must validate conformance.

C. Performance Demands of Real-Time, High-Volume Systems

UPI's success is built on near-instantaneous fund transfers. Introducing PQC must not degrade this experience. The NPCI will need to mandate PQC readiness milestones, likely beginning with hybrid TLS on inter-bank links before moving to customer-facing mobile applications. Aadhaar, which processes billions of authentication requests monthly across hundreds of government services, requires a phased rollout: enrolling stations first, then authentication agencies, then backend data vaults, ensuring biometric data remains protected throughout.

D. Testing, Validation, and Vendor Dependence

PQC algorithms are newer and less battle-tested than classical ones. India must establish robust testing laboratories, certification frameworks, and algorithm evaluation mechanisms. The DST roadmap proposes a tiered certification system with four assurance levels (Level 1 basic conformance to Level 4 sovereign-grade) and a three-tier national laboratory network [7]. Building this domestic capacity from scratch is a major undertaking that will require upgrading existing facilities and training personnel.

India's telecommunications sector relies heavily on international equipment vendors. Ensuring these vendors provide PQC-ready 5G/4G network elements, with India-specific testing under local conditions, requires contractual mandates and close coordination. Vendor dependency extends to enterprise software, cloud services, and mobile operating systems; procurement rules must mandate Cryptographic Bills of Materials (CBOMs) to enforce transparency.

E. Crypto-Agility as a Foundational Principle

Crypto-agility, the architectural capacity to replace cryptographic algorithms without major system redesign, is both a necessity and a challenge. Legacy systems with hard-coded ciphers must be refactored to support modular, algorithmagnostic interfaces. This is a complex and costly software engineering effort but is essential to future-proof against potential breaks in PQC schemes (e.g., advances in lattice cryptanalysis) and to facilitate adoption of future standards. The DST Task Force enshrines crypto-agility as a mandatory principle for all new deployments [7].

F. Workforce and Skill Gaps

There is an acute shortage of professionals versed in PQC mathematics, quantum-safe system design, and migration planning. Many organisations lack even basic awareness of the quantum threat. Building a quantum-ready workforce through university curricula, professional certification programs (e.g., NASSCOM-backed courses), and specialised

training for government IT staff is a foundational requirement for successful migration.

V. POLICY AND REGULATORY FRAMEWORK FOR INDIA

India's response is coordinated through a multi-agency framework underpinned by the National Quantum Mission (NQM), which was launched in 2023 with a budget of approximately INR 6000 crore (~USD 720 million) for quantum technology R&D through 2031 [12]. Key policy instruments include:

A. DST Task Force Report (February 2026)

The Task Force on "Implementation of Quantum Safe Ecosystem in India" delivered a landmark report providing the first comprehensive PQC policy document [7]. Its core recommendations include:

- **Timelines:** CII sectors (defence, power, telecom, space, core government) must achieve foundational readiness by 2027 and full PQC adoption by 2029. All enterprises are to complete migration by 2033.
- **Crypto-agility:** All new systems must be designed to be algorithm-agnostic; procurement rules must forbid classical-only cryptographic deployments.
- **Tiered certification:** A four-level assurance model (Level 1 to Level 4) for PQC products.
- **Integration with data protection:** PQC readiness is tied to compliance under the Digital Personal Data Protection (DPDP) Act, 2023.

B. CERT-In and Sectoral Guidance

India's Computer Emergency Response Team (CERT-In), in collaboration with industry, published a whitepaper "Transitioning to Quantum Cyber Readiness" in mid-2025 [13]. It advises financial institutions, healthcare providers, and government bodies to conduct cryptographic inventories, test PQC implementations, and adjust cyber-resilience policies. The whitepaper forms the regulatory backbone for sectoral compliance, with expectations that future cyber-security rules will mandate PQC migration progress reporting.

C. Bureau of Indian Standards and International Alignment

The Bureau of Indian Standards (BIS), in concert with the Telecommunication Engineering Centre (TEC) and MeitY, is developing draft PQC standards aligned with NIST FIPS 203 to FIPS 205 and ISO/IEC frameworks. India participates in international forums to ensure interoperability and avoid vendor lock-in. The policy emphasis is on adopting global standards as a baseline while nurturing indigenous competency to develop local variants and testing capabilities.

D. Integration with Data Protection and Critical Infrastructure Laws

The DPDP Act (2023) mandates "appropriate technical and organisational measures" to safeguard personal data. While PQC is not explicitly named, the certification framework explicitly requires testing laboratories to comply with the DPDP Act, creating a direct link between data protection compliance and validated quantum-safe cryptography. For

CII sectors, upcoming cybersecurity regulations are expected to mandate PQC adoption within the stipulated deadlines, with penalties for non-compliance.

Challenges in the policy framework include the ambitiousness of the 2027 CII deadline, lack of detailed guidance on the hybrid PQC-QKD approach, and insufficient domestic testing capacity. Analysts recommend adopting cooperative public private partnership models similar to NIST's and providing more pragmatic, phased guidance for smaller enterprises [10].

VI. IMPLEMENTATION ROADMAP AND MIGRATION STRATEGY (2026 TO 2035)

Based on the DST roadmap and international best practices, a phased migration strategy is proposed. The roadmap recognises that CII sectors must move on an accelerated timeline, while other enterprises follow a more graduated path.

A. Phase 1: Preparation and Foundation (2026 to 2027)

- Conduct national cryptographic inventories and asset audits across all government and CII systems.
- Establish cross-functional quantum risk management teams.
- Set up national PQC testing and certification infrastructure (tiered labs operational by December 2026).
- Launch proof-of-concept pilots in high-risk domains: military communications, RBI payment networks, telecom core links.
- Mandate crypto-agile procurement and CBOM submissions from vendors starting FY 2027 to 2028.
- Integrate PQC awareness into academia and professional training programs.

B. Phase 2: High-Priority Migration (2028 to 2030)

- Begin full-scale deployment of PQC (or hybrid) in CII systems: government internet backbones, banking payment switches, telecom interconnection networks, defence networks.
- Enforce "no new classical-only" policy for all new system deployments in CII and large enterprises.
- Upgrade core cryptographic infrastructure: PKI hierarchies, HSMs, key management systems to PQC-ready versions.
- Decommission classical-only crypto where feasible and isolate legacy systems within controlled enclaves.
- Refine and stress-test migration plans; conduct regular interoperability testing.

C. Phase 3: Complete Adoption (2031 to 2033)

- Transition all remaining CII and enterprise systems to PQC-only trust chains and digital signatures by 2033 (CII fully completed by 2029).
- Retire legacy PKI and ensure long-term support for PQC keys.
- Extend migration to consumer-facing services, mobile applications, and low-security systems (phased updates to avoid disruption).

- Implement continuous algorithm update mechanisms; monitor cryptanalysis of deployed PQC schemes.

TABLE III

SECTOR-WISE PQC MIGRATION DEADLINES

Sector	Foundation	Full PQC	Key Actions
Defence & Security	2027	2029	Pilot PQC comms; QKD on strategic links; isolate legacy networks
Banking & Finance	2027	2030 (hybrid)	Inventory UPI/NEFT crypto; upgrade HSMs; test PQ TLS on payment switches
Telecom & Internet	2027	2030 to 2031	Secure 5G backhaul with PQC; issue quantum-safe certificates; roadmap for devices
E-Governance (Aadhaar)	2028	2032	Pilot PQC in GovPKI; upgrade data centres; re-encrypt biometric vaults
Utilities (Power)	2026	2032 to 2033	Identify SCADA PKI; plan PQC in smart metering
Healthcare, Education	2026	2033+	Crypto audit of medical records; adopt PQ VPNs for research networks
SMEs & General Enterprise	2026	Gradual 2035	Use PQ libraries; incorporate PQC criteria in BIS standards

D. Phase 4: Consolidation and Maintenance (2034 to 2035)

- Achieve full entrenchment of PQC standards across all sectors of the economy.
- Incorporate second-round NIST backup algorithms (isogeny-based, additional signatures) as needed.
- Maintain crypto-agility as a permanent operational capability.
- Conduct long-term monitoring of quantum developments and evolve policies accordingly.

Table III summarises target timelines by sector.

This dual-track timeline aligns with the DST’s “middle path” strategy, which combines software-based PQC for broad applications with hardware-based QKD for high-assurance, strategic links. The hybrid approach, using classical+PQC during transition, provides backward compatibility, a real-world testing environment, and insurance against algorithmic breaks. However, it introduces performance overhead and protocol engineering complexity that must be carefully managed.

Fig. 3 illustrates this dual-track quantum-safe strategy, while Fig. 4 presents the phased national roadmap and accelerated deadlines for critical sectors.

VII. SECTOR-WISE IMPACT AND PRIORITIES

Sectoral priorities are driven by risk exposure, data sensitivity, and systemic interconnectedness.

A. Defence and National Security

Defence communications, intelligence networks, and command-and-control systems carry long-lived national secrets. The DST roadmap designates defence as CII with the most accelerated deadline. Pilots integrating QKD with PQC

on strategic links (e.g., embassy communications, satellite ground stations) are already underway. Isolating legacy India’s Quantum-Safe Strategy

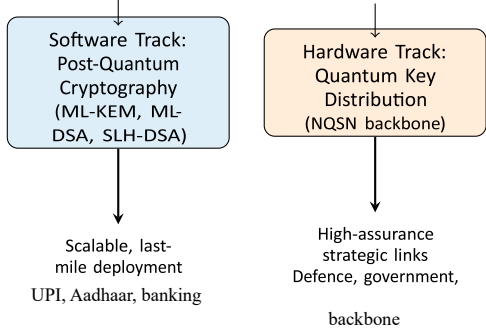


Fig. 3. Dual-track approach: PQC supports broad, scalable deployment, while QKD secures high-assurance strategic links in India’s quantum-safe roadmap [7].

networks and deploying PQC-secured radios are immediate priorities.

B. Banking, Financial Services, and Insurance (BFSI)

The financial sector holds highly sensitive transaction data and is subject to long retention mandates. UPI, RTGS, and NEFT systems rely heavily on PKI; a quantum break could enable transaction forgery and systemic financial chaos. The Reserve Bank of India (RBI) is expected to issue PQC guidelines in 2026. Banks must complete cryptographic inventories of core banking platforms, ATMs, and card payment systems, pilot hybrid TLS on inter-bank links, and upgrade HSMs to support PQC algorithms. Given the complexity of legacy mainframe environments, public sector banks may require the longest lead times; early initiation is critical.

C. Telecommunications

Telecom backbone networks, including 5G core and international gateways, form critical national infrastructure. The DST mandates full PQC for telecom CII by 2029. Operators must plan PQC integration into 5G-authentication (5G-AKA), IPsec tunnels, and SDN controllers. The concurrent 5G rollout presents an opportunity to embed PQC from the outset rather than retrofitting later. Vendor contracts must include PQC support timelines and India-specific conformance testing.

D. E-Governance and Digital Public Infrastructure

Aadhaar and UPI are unique to India and represent the pillars of digital trust. Aadhaar’s PKI underpins identity authentication for over 600 government services; compromise would shatter the trust framework for welfare delivery, KYC, and digital signatures. UPI’s instant payment rails link the entire economy. Migration must be choreographed with extreme care: phased rollouts starting with backend infrastructure, then authentication agencies, and finally consumerfacing endpoints. Aadhaar’s central biometric vault must be re-encrypted with PQC keys to counter HNDL retroactive decryption. UIDAI and NPCI have

not yet announced detailed schedules, but the DST roadmap implies PQC readiness by 2032 for e-governance.

scale provides credible real-world credentials. As a relatively neutral technology partner, India could offer certification

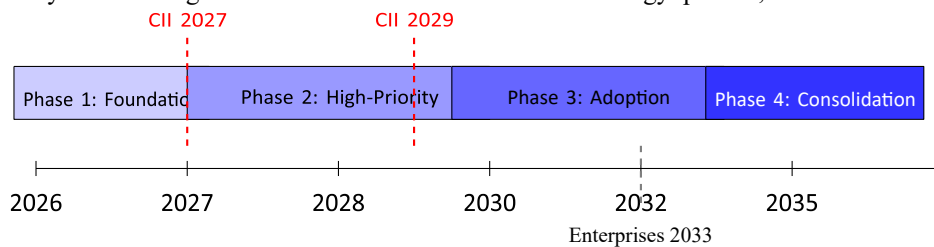


Fig. 4. India's phased PQC migration roadmap from 2026 to 2035, highlighting accelerated deadlines for critical information infrastructure and enterprise-wide adoption.

E. Utilities and Critical Infrastructure

Power grids and water management systems use SCADA/PLC components with embedded cryptography. A quantum attack could disrupt grid control, causing cascading blackouts. Utilities are directed to complete inventory by 2026 and achieve PQC by 2032 to 2033. Upgrading deeply embedded industrial control systems presents a distinct challenge, often requiring hardware replacement rather than software patches.

F. Healthcare and Education

Medical records, research data, and biometric health IDs must be protected under privacy laws. While these sectors are lower priority, planning should begin immediately to audit cryptographic dependencies and prepare for PQC-enabled VPN, TLS, and data-at-rest encryption by 2033+.

VIII. ECONOMIC AND STRATEGIC OPPORTUNITIES

The PQC transition is not merely a cost centre but a catalyst for innovation, industrial growth, and strategic autonomy.

A. Market Potential and Indigenous Innovation

India's quantum technology market is projected to grow from USD 98.4 million in 2025 to USD 465.8 million by 2032, at a CAGR of 24.9% [14]. The BFSI sector alone commands 30% of this demand, driven by the urgent need for quantum-resistant encryption. The NQM provides grants of up to INR 30 crore to selected quantum startups, spurring a dynamic ecosystem of over 57 quantum-focused companies (QpiAI, QNu Labs, BosonQ Psi, etc.). Major IT services firms (Infosys, Wipro, TCS) are establishing dedicated PQC practices. This confluence of funding, talent, and demand positions India to develop Indigenous PQC libraries, hardware accelerators, and complete quantum-safe solutions.

B. Global Certification Leadership

The proposed National PQC Testing and Certification Program, with tiered laboratories, addresses a global gap: independent verification of quantum-safe claims. India's ability to validate both PQC algorithms and QKD products end-to-end is rare. Its experience deploying a 500+ km QKD network and managing brownfield migration at population

C. Digital Sovereignty and Supply Chain Security

The quantum transition aligns with the "AtmaNirbhar Bharat" (Self-Reliant India) vision. Developing domestic PQC and QKD capabilities reduces reliance on foreign cryptographic modules and foreign-controlled certification. Mandating CBOMs and integrating PQC readiness into procurement rules strengthen supply chain visibility and enforce vendor accountability. Control over cryptographic standards for critical national infrastructure ensures that national security remains under sovereign jurisdiction.

D. Export of Expertise and Solutions

India's experience with large-scale digital public infrastructure (Aadhaar, UPI) and its unique challenges (multilingual, low-connectivity, low-cost devices) generates exportable expertise in PQC integration. Indian companies can offer quantum-safe consulting, agile migration tools, and certified security products to other emerging economies facing similar constraints. Capacity-building programs, once established domestically, can be extended internationally, creating long-term strategic partnerships.

IX. CAPACITY BUILDING AND CROSS-SECTORAL COORDINATION

A. Human Resource Development

The acute shortage of PQC-skilled professionals is a binding constraint. To address this, India has launched large-scale educational initiatives. A notable example is the "Quantum Computing: Quantum Algorithms and Qiskit" course organised by the Andhra Pradesh State Council of Higher Education and NPTEL, enrolling 55,000 university students [15]. Industry-led academies, such as QNu Academy, offer hands-on training with commercial QKD systems and QRNGs. However, these efforts must be scaled dramatically. PQC concepts must be integrated into undergraduate and postgraduate cybersecurity, computer science, and electronics curricula. Professional certification programs through NASSCOM, DSCI, and sectoral skill councils are needed to upskill the existing workforce in government, banking, and telecom.

B. Institutional Coordination

The migration involves a dense web of stakeholders: central ministries (MeitY, DST, MoD, DoT), regulators (RBI,

TRAI, SEBI), standardisation bodies (BIS, TEC), certifying agencies (CERT-In), state governments, public sector enterprises, private vendors, and academia. The NQM Task Force provides the apex coordination body, but operational coordination requires dedicated programme management offices within each sector. For example, NPCI must orchestrate UPI migration across 400+ banks, while UIDAI must coordinate Aadhaar authentication agencies. Public-private partnership models, similar to NIST's cooperative agreements with technology partners, can accelerate knowledge transfer and ensure vendor accountability.

C. Managing Dependencies and Long-Term Agility

Sustaining the migration over a decade requires treating PQC as a continuous risk-management process. Board-level oversight, dedicated budgets, and regulatory reporting will embed quantum risk into corporate governance. Crypto-agility must be institutionalised as a permanent requirement, not a one-time fix. National testing facilities (TEC, CERT-In) will play an enduring role in validating algorithmic updates and responding to future cryptanalytic breakthroughs. Regular national readiness exercises, akin to cyber-security drills, can maintain focus and identify gaps.

Although national and international bodies have established post-quantum standards, migration roadmaps, cryptographic inventory practices, and risk-based guidance, a practical challenge remains for country-scale heterogeneous ecosystems: determining which individual systems should receive migration resources first when multiple systems simultaneously exhibit quantum vulnerability. India requires a prioritisation mechanism that considers not only cryptographic exposure, but also the longevity of protected data, systemic criticality, interdependencies, migration complexity, and regulatory urgency. This motivates the Q-GRID framework proposed in this work.

X. PROPOSED QUANTUM GOVERNANCE READINESS AND INFRASTRUCTURE DECISION FRAMEWORK

The existing post-quantum migration approaches provide standards, implementation guidance, cryptographic inventory practices, and high-level migration milestones. However, India's heterogeneous digital infrastructure requires an additional decision layer capable of determining which systems should receive migration priority based on their quantum exposure, societal importance, data lifetime, dependencies, and practical migration constraints. This requirement is particularly relevant because India's digital infrastructure spans highly interconnected systems such as UPI, Aadhaar, telecommunications, defence networks, financial infrastructure, and government services.

To address this requirement, this paper proposes the **Quantum Governance Readiness and Infrastructure Decision Framework (Q-GRID)**. Q-GRID is intended as an India-specific risk-based prioritisation framework that

converts multiple dimensions of quantum risk and migration difficulty into a composite score. Rather than replacing existing national standards or regulatory roadmaps, Q-GRID is designed to complement them by providing an analytical mechanism for prioritising systems and determining appropriate migration actions.

A. Q-GRID Assessment Dimensions

Q-GRID evaluates each digital system using six dimensions:

1) Quantum Exposure (QE)

Quantum Exposure measures the vulnerability of the cryptographic mechanisms currently protecting a system. Systems relying on quantum-vulnerable public-key algorithms such as RSA, Diffie-Hellman, and elliptic-curve cryptography receive higher exposure scores. Symmetric cryptography and hash functions are evaluated according to their effective post-quantum security and parameter strength. A system using RSA-2048 for key exchange and ECDSA-256 for signatures would receive a higher QE score than one already employing AES-256 with extended hash outputs.

2) Data Longevity (DL)

Data Longevity represents the period for which protected information must remain confidential or trustworthy. Systems containing information with long confidentiality horizons receive higher scores. Defence information, biometric identity data, strategic communications, financial records, and sensitive government archives are examples where long-term confidentiality increases exposure to the "harvest now, decrypt later" threat. Aadhaar's biometric vault, with its decades-long retention requirements, exemplifies a system with maximum DL value.

3) Systemic Criticality (SC)

Systemic Criticality measures the consequences of compromise or prolonged disruption. Critical national infrastructure, defence systems, payment systems, identity infrastructure, and telecommunications are assigned higher criticality than systems whose compromise would have limited societal or economic consequences. UPI, which processes over 10 billion transactions monthly and underpins India's digital economy, would receive a maximum SC score.

4) Systemic Dependency (SD)

Systemic Dependency measures the number and importance of other services that rely on the system. Highly interconnected platforms create a larger potential blast radius because compromise of one cryptographic trust anchor may propagate across dependent organisations and services. This factor is particularly relevant to India's digital public infrastructure—Aadhaar's PKI underpins authentication for over 600 government services, creating extensive dependency chains.

5) Migration Complexity (MC)

Migration Complexity measures the technical and operational difficulty of replacing existing cryptographic mechanisms. Factors include legacy infrastructure, hardware dependencies, HSM compatibility, embedded devices, bandwidth constraints, vendor dependencies, certificate hierarchies, interoperability requirements, and the availability of PQC-ready implementations. Core banking systems running on decades-old mainframes represent high MC, while cloud-native applications may migrate more readily.

6) Regulatory Urgency (RU)

Regulatory Urgency represents the time pressure created by national policy, sector-specific requirements, security obligations, and expected migration milestones. Systems belonging to Critical Information Infrastructure or other strategically important sectors receive higher urgency scores when their migration deadlines are closer. The DST roadmap's 2027 deadline for CII foundational readiness elevates RU for defence, telecom, and power systems.

B. Quantum Risk Index Calculation

Each dimension is assigned a score from 0 to 10. A weighted composite score is then calculated:

$$QRI = \frac{w_{QE} \cdot QE + w_{DL} \cdot DL + w_{SC} \cdot SC + w_{SD} \cdot SD + w_{MC} \cdot MC + w_{RU} \cdot RU}{w_{QE} + w_{DL} + w_{SC} + w_{SD} + w_{MC} + w_{RU}} \times 10$$

where **QRI** represents the Quantum Risk Index and each w_i represents the relative importance assigned to the corresponding dimension.

The weighting scheme can subsequently be determined through expert elicitation, Analytic Hierarchy Process (AHP), or empirical validation using sector-specific data. The initial framework does not assume that all dimensions have equal importance; rather, it allows weights to be adapted according to the risk profile of the sector. For instance, defence systems might weight DL and SC more heavily, while consumer-facing services might prioritise MC and RU.

For initial assessment, QRI may be interpreted using four priority categories:

TABLE IV: Q-GRID PRIORITY CATEGORIES AND RECOMMENDED ACTIONS

QRI Range	Priority	Recommended Action
0–39	Low	Monitor, maintain inventory, ensure crypto-agile procurement
40–59	Moderate	Complete cryptographic discovery and migration planning
60–79	High	Begin PQC pilots and prioritised

		migration
80–100	Critical	Accelerated migration, hybrid deployment, continuous assurance

These thresholds are proposed operational categories and should be validated through future empirical studies.

C. Q-GRID Migration Decision Layer

The principal objective of Q-GRID is not merely to produce a numerical score. The score is mapped to an actionable migration pathway.

Low- and moderate-risk systems can initially focus on cryptographic discovery, vendor assessment, crypto-agile architecture, and PQC-ready procurement. High-risk systems should proceed to PQC pilots, hybrid cryptographic deployment, interoperability testing, and infrastructure upgrades. Critical systems may require accelerated PQC migration, re-encryption of long-lived information, upgraded HSM and PKI infrastructure, and, where justified by the threat model and infrastructure feasibility, integration with quantum key distribution for high-assurance links.

This produces the following decision sequence:

Cryptographic Inventory → Q-GRID Assessment → Quantum Risk Score → Migration Priority → PQC/Hybrid/QKD Selection → Validation → Continuous Monitoring

The approach complements India's existing national strategy, which calls for discovery, risk assessment, prioritisation, PQC pilots, cryptographic bills of materials, migration of high-priority systems, and long-term crypto-agility.

D. Quantum-Safe Passport

To operationalise Q-GRID, this paper further proposes a **Quantum-Safe Passport** for critical digital systems. The passport acts as a continuously updated quantum-readiness record containing:

- System and sector identification
- Cryptographic algorithms and key sizes
- Cryptographic dependencies and certificates
- Q-GRID risk score
- HNDL exposure assessment
- Data confidentiality lifetime
- Migration stage
- PQC algorithms deployed
- Hybrid cryptographic mechanisms
- Vendor and supply-chain dependencies
- Cryptographic Bill of Materials (CBOM)
- Certification and testing status
- Next planned migration milestone

A Quantum-Safe Passport would allow regulators, system owners, auditors, and procurement authorities to obtain a common view of the quantum-readiness status of critical infrastructure. This transparency mechanism supports compliance verification, enables cross-sector coordination, and facilitates evidence-based resource allocation.

E. Illustrative Application to Indian Digital Infrastructure

The framework can be applied to representative Indian systems such as defence networks, Aadhaar, UPI, telecommunications, power infrastructure, healthcare, and education. Table V presents an illustrative scoring for selected systems.

TABLE V: ILLUSTRATIVE Q-GRID SCORES FOR KEY INDIAN SYSTEMS

<i>System</i>	<i>E</i>	<i>Q</i>	<i>L</i>	<i>D</i>	<i>C</i>	<i>S</i>	<i>D</i>	<i>C</i>	<i>M</i>	<i>U</i>	<i>R</i>	<i>QRI</i>
<i>Defence Networks</i>	9		10		10		8		8		9	90
<i>Aadhaar PKI</i>	9		10		10		10		9		8	93
<i>UPI</i>	9		8		10		10		7		9	88
<i>Infrastructure Telecom</i>	8		7		9		9		8		9	83
<i>Core Power</i>	8		6		9		8		9		8	80
<i>SCADA</i>	7		9		6		5		6		5	63
<i>Healthcare Records</i>	6		4		4		3		5		4	43
<i>Education Networks</i>												

Note: Scores are illustrative and intended to demonstrate framework application. Actual assessments require detailed system analysis.

For example, Aadhaar and UPI would be expected to receive high scores because of their systemic criticality, large-scale dependency, sensitivity of protected information, and extensive cryptographic infrastructure. Defence systems would similarly receive high scores because of the long confidentiality lifetime and national-security consequences of compromise.

The resulting prioritisation should not be interpreted as a substitute for detailed security assessments. Instead, it provides a structured mechanism for deciding where detailed technical assessments and migration resources should be concentrated first.

F. Expected Benefits

Q-GRID provides four principal benefits.

First, it converts a broad national migration problem into a measurable prioritisation problem. Second, it integrates technical, operational, economic, and regulatory considerations instead of evaluating cryptographic vulnerability in isolation. Third, the framework can consume information from cryptographic inventories and CBOMs and therefore connect discovery directly to migration decisions.

Finally, the framework supports continuous reassessment, allowing priorities to change as cryptographic standards, quantum capabilities, regulations, vulnerabilities, and organisational dependencies evolve.

The proposed framework is therefore intended as a decision-support layer between national quantum-security policy and system-level implementation. Future work should validate the weighting model using expert assessments, real cryptographic inventories, sector-specific datasets, and performance measurements of PQC and hybrid implementations.

XI. CONCLUSION

Quantum computing poses an existential threat to the cryptographic foundations of India’s digital governance and economy. The “harvest now, decrypt later” threat eliminates any justification for delay: migration planning is an immediate national security imperative. Post-quantum cryptography, underpinned by NIST-standardised lattice and hash-based algorithms, provides a viable and scalable path to quantum resilience. However, the transition is arguably the most complex cryptographic migration in history, given India’s scale and diversity.

This paper has outlined a comprehensive framework to navigate that transition. The core recommendations are:

- Start now: Initiate cryptographic inventories, risk assessments, and pilot deployments in CII sectors immediately.
- Embed crypto-agility: Design all new systems to be algorithm-agnostic to accommodate future PQC evolution and potential breaks.
- Adopt a phased, dual-track strategy: Combine PQC for broad deployment with QKD for strategic links; use hybrid schemes during the transitional decade.
- Prioritise critical sectors: Defence, finance, telecom, and Aadhaar/UPI must meet accelerated deadlines (2027 to 2030) to safeguard national security and economic stability.
- Build domestic capacity: Invest in indigenous R&D, testing infrastructure, and a quantum-ready workforce to reduce foreign dependency and capture economic opportunities.
- Strengthen regulatory frameworks: Enforce mandates through updated cyber-security and data protection rules, with clear compliance deadlines and procurement requirements.

The proposed Q-GRID framework extends this strategy by introducing a structured decision layer for migration prioritisation. By combining quantum exposure, data longevity, systemic criticality, dependency, migration complexity, and regulatory urgency into a composite Quantum Risk Index, Q-GRID can help organisations identify which systems require immediate attention and which can follow a graduated migration path. The accompanying Quantum-Safe Passport provides a mechanism for maintaining evidence of cryptographic inventory, migration progress, certification, and continuing

crypto-agility. Future validation of the framework using expert-derived weights, real-world cryptographic inventories, and sector-specific performance data will determine its effectiveness and refine its applicability across India's digital public infrastructure.

The journey to quantum resilience will be lengthy and resource-intensive, but it also presents India with a unique opportunity to become a global leader in quantum-safe technologies. By leveraging its National Quantum Mission, aligning with international standards, and drawing on its proven strength in delivering digital public infrastructure at scale, India can secure its governance systems for the quantum age and, in doing so, reinforce its digital sovereignty and strategic autonomy.

ACKNOWLEDGMENT

The authors acknowledge the valuable insights drawn from reports by the National Quantum Mission Task Force, CERTIn, NIST, and the research community. The authors acknowledge the assistance of OpenAI's ChatGPT in structuring text and refining the presentation of the proposed framework's language.

REFERENCES

- [1] P. Shah, "Quantum readiness and cryptographic agility: Securing India's digital future," *ETCISO (Economic Times)*, Sep. 19, 2025.
- [2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484 to 1509, 1997.
- [3] M. Mosca and V. Gheorghiu, "A quantum-ready workforce," *Nature Phys.*, vol. 18, pp. 127 to 129, 2022. (Resource estimates extrapolated from Kudelski Security analyses.)
- [4] National Cyber Security Centre (NCSC-UK), "Timelines for migration to post-quantum cryptography," 2022.
- [5] Australian Signals Directorate (ASD), *Information Security Manual*, 2025.
- [6] The Quantum Insider, "Q-Day just got closer: Three papers in three months are rewriting the quantum threat timeline," Mar. 2026.
- [7] Department of Science & Technology (DST), India, "Implementation of Quantum Safe Ecosystem in India: Report of the Task Force," Feb. 2026. [Online]. Available: [https://dst.gov.in/sites/default/files/Report TaskForce PQMigration 4Feb26%20%28v1%29.pdf](https://dst.gov.in/sites/default/files/Report%20TaskForce%20PQMigration%204Feb26%20%28v1%29.pdf)
- [8] G. Alagic *et al.*, "NIST releases first 3 finalized post-quantum encryption standards," NIST, Aug. 29, 2024.
- [9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. Cambridge University Press, 2010.
- [10] Observer Research Foundation, "India's post-quantum cryptography migration roadmap," 2026.
- [11] S. J. Podder, "Post-quantum cryptography: India's migration strategy," *Medium*, 2026.
- [12] Government of India, *National Quantum Mission (NQM)*, 2023.
- [13] CERT-In & SISA, "Transitioning to quantum cyber readiness," Whitepaper, Jul. 2025.
- [14] P&S Market Research, "India quantum computing market size, and growth report, 2032," 2025.
- [15] The Quantum Insider, "55,000 Indian university students into a quantum computing course," Jan. 2026.
- [16] PQShield, "India publishes national roadmap for quantum resilience," Feb. 2026.
- [17] ISO/IEC TR 3088, "Quantum cryptography and quantum-safe cryptography," 2025.
- [18] Bureau of Indian Standards, *Draft PQC standards*, 2025.