Post-Quantum Cryptography Challenges in Securing India's GST Digital Infrastructure

Arman Rasool Faridi
Department of Computer Science
Aligarh, India
arman.faridi@gmail.com

Madiha Khan
Department of Computer Science
Aligarh, India
uzaidkhan8005@gmail.com

Faraz Masood
Department of Computer Science
Aligarh, India
ffarazs@gmail.com

***Abstract*— Quantum computing threatens the public-key cryptography that underpins government digital infrastructure, including secure web services, digital signatures, identity systems, and encrypted inter-agency communications. Post-quantum cryptography (PQC) provides quantum-resistant public-key primitives that can be deployed on conventional hardware, making it the most practical path for near-term national readiness. This paper analyzes implementation challenges and transition strategies for adopting PQC in Indian government platforms (e.g., Digital India services, e-governance portals, and large-scale identity and taxation ecosystems). We emphasize the operational reality of migration: while algorithm standardization is progressing, government systems must manage legacy constraints, performance overheads, protocol and certificate interoperability, and new implementation risks such as side-channel leakage. From a policy and governance perspective, key obstacles include limited crypto-agility, uneven organizational readiness, skill shortages, and coordination across agencies and vendors. We propose a phased, risk-based roadmap centered on cryptographic inventory, crypto-agile architecture, hybrid deployment (classical + PQC) to preserve backward compatibility, and sector-specific prioritization of long-lived confidentiality requirements. The paper concludes with actionable recommendations for procurement, certification, workforce development, and inter-agency governance to help India transition to quantum-safe digital infrastructure aligned with national resilience and Viksit Bharat @2047 goals.**

Keywords—post-quantum cryptography, government digital infrastructure, crypto-agility, PKI migration, India, cybersecurity transition

I. Introduction

Government digital infrastructure is based on the use of cryptographic primitives that provide confidentiality, integrity, and authentication for online services and citizen records and communications. Yet, the development of large-scale quantum computers endangers the severely deployed public key schemes like RSA and elliptic curve cryptography (ECC), allowing attackers to decrypt traffic and sign fraudulently when they have sufficient quantum capability [4], [7]. In practice, the threat of this is already happening today: adversaries can capture encrypted data today and decrypt it in the future, which is especially concerning long-lived government data, including identity attributes, legal archives and strategic communications [7].

Post-quantum cryptography (PQC) aims to replace vulnerable public-key primitives with algorithms that are believed to resist both classical and quantum attacks, usually by appealing to difficult problems in lattices, codes or hash functions [8]. Compared with methods that necessitate dedicated quantum hardware, PQC is attractive since it can be deployed mostly through software and firmware updates, which supports widespread deployment across heterogeneous government platforms [6]. Nevertheless, PQC migration is not at all a straightforward algorithmic switch; public key algorithms are everywhere in PKI, secure protocols, secure identity systems and secure procurement or certification pipelines. As such, PQC readiness is a socio-technical programme that includes systems engineering, risk management and public policy considerations [5].

This paper focuses on the government digital infrastructure of India and presents (i) a brief overview of the PQC and its importance for public systems, (ii) the key implementation challenges that need to be solved, and (iii) some pragmatic transition strategies that focus on phased implementation and cryptographic agility.

II. India's Government Digital Infrastructure and Quantum Risk

The digital governance ecosystem in India includes large scale identity and authentication systems, digital payment systems, taxation platforms, citizen services portals and sectoral systems in the areas of health, education and welfare among others. The implementation of these services requires the use, in practice, of certificates issued by PKIs, the use of TLS to ensure secure transport and the use of digital signatures to ensure non-repudiation and simplify document workflows. Even without any specific reference to specific implementations, it is clear that the general dependency is on public-key cryptography, including certificate chains, key exchange protocols, and signature verification mechanisms.

Quantum-safety considerations are unevenly distributed across assets. Certain workloads require confidentiality for small amounts of time - like regular service sessions - but others require protection of information for multi-decadal horizons - e.g. biometric templates, national-scale registries, legal archives, strategic planning documents. Consequently, the migration trajectory should be prioritized based on the data's

lifetime and threat models, with urgent action on systems which are safeguarding long lived secrets [3], [7].

An India-specific factor is the further complication of this landscape: the large number of devices and variable connectivity condition. Government platforms don't just expand in the form of centralized data centres but kiosks, field devices, point of service terminals and IoT like deployments. The overhead that post quantum cryptography adds - larger key sizes, more complex signatures, and extra computational requirements - must therefore be tested in a real-world setting rather than a contrived laboratory setting [9].

III. Implementation Challenges in Government Systems

A. Integration *of legacy and interoperability*

Legacy software is often used, limited devices are available, and certification is often sluggish at government platforms. Post-quantum cryptography (PQC) also brings on bigger key sizes and unique identifier of codes that can violate older protocol assumptions or certificate profiles. Migration should therefore be systematic in dealing with interoperability among applications, cryptographic libraries, network protocols and PKI tooling. Partial deployment may trigger service failures or unintentional security misconfigurations without coordinated updates [5].

B. Operation overhead and performance.

PQC handshakes can expand payloads and increase computation costs, which have an effect on latency and throughput. Empirical experimental results of PQC in TLS protocols indicate that overhead depends on the algorithm selected, and it can be significant to resource-constrained clients or large-scale servers [9]. The government services have the obligation to test PQC under the real life conditions such as during peak load, limited networking conditions among others before full deployment.

C. Implementation security (side channel and engineering risk).

The risk of immature implementation is increased by the introduction of new algorithms. Particularly lattice-based schemes require careful constant-time encoding and strong protection against timing, cache and power-analysis leakage. Considering that government systems have advanced the adversaries, the migration plans should include proven libraries, scrupulous review of secure-coding, and testing regimes that are compatible with certification [8].

D. Organizational preparedness and governance.

PQC migration involves various parties: cybersecurity management, PKI providers, application owners, procurement departments, and vendors. The study on quantum-safe migrations in government agencies highlights barriers in the form of less awareness, shortage of specialists, unclear distribution of responsibility, and insufficient cryptographic agility in the existing systems [1], [5]. Such challenges are further enhanced in federated settings whereby services are spread out across ministries as well as state-level services.

IV. Transition Strategies for India: A Practical Roadmap

A. National cryptographic inventory and classification

The inventory of the locations of public-key cryptography application (in certificates, key-exchange protocols, code signing, document signatures, and device authentication) is the first deliverable. Assets are to be divided by confidentiality, life cycle, and importance. A risk-based migration timeline created through such a taxonomy would allow prioritising those systems whose exploitation would have a long-term national impact [2], [7].

B. Develop crypto-agility into procurement and odernization

Crypto-agility should be considered as an architecture requirement: the systems should support a variety of algorithms, support the ability to use revised cryptographic libraries, prefer configuration-driven choices over hard wired primitives. The Procurement policies and vendor agreements must force Post-Quantum Cryptography (PQC) preparedness and map out upgrade courses of devices in the field. Moreover, crypto-agility will act as a safety valve in the future in case vulnerabilities arise [5].

C. Use progressive and hybrid implementation.

A realistic approach is to use phased migration with hybrid cryptography, i.e. using classical and PQC primitives in an intermediate phase. The deployment of hybrids reduces the risk of an early dependency on one new primitive, as well as maintaining backward compatibility to clients who cannot upgrade immediately. It enables also controlled pilots in a few selected services, which can be scaled later when the reliability and performance have been confirmed [6], [9].

D. PKI and signing pipelines prioritisation.

The government trust chains (root and intermediate Certificate Authorities) and signing processes (software updates, firmware, and signatures of official documents) should take precedence because, once compromised, the process spreads throughout the services. The step to transition can start with making PQC-capable certificate profiles and implementing PQC signatures on high-value artifacts (e.g., code signing). At the same time, trust-anchor updating plans are supposed to include cross-certification and gradual distribution that is carefully controlled.

E. Workforce development and inter-agency coordination.

Migration requires qualified cryptographic engineers, security auditors and PKI operators. One way of dealing with India would be through specific training programmes of government IT staff, collaborations with universities and standards organizations, and a central coordinating body which issues implementation guidelines, testing baselines, and sectoral schedules. This level of governance is crucial to avoid the checkered adoption and to maintain interoperability throughout the ministries and state systems [5].

Error! Reference source not found. illustrates the relationship between core implementation challenges (left), strategic transition mechanisms tailored to India (center), and the target outcome of secure, quantum-resistant government

systems (right). Iterative pilot testing and continuous coordination ensure adaptive, risk-managed migration.

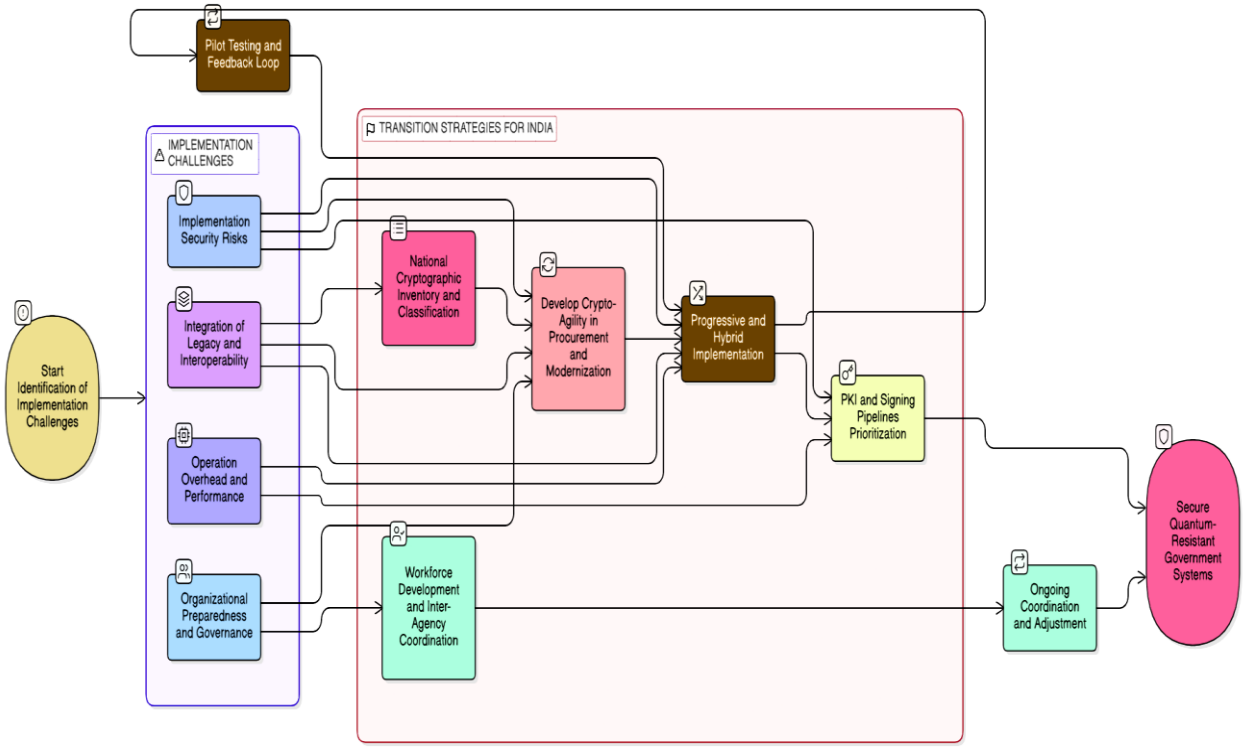

Fig. 1. Implementation challenges and phased transition strategies for adopting post-quantum cryptography (PQC) in Indian government digital infrastructure.

V. Transition Strategies for India: Implementation Program Design

Previous section mentioned an effective roadmap. This part extends it into an implementation program which can be operationalized by government agencies to a heterogeneous platform and vendors. The main focus is on minimizing quantum exposure and maintaining services steady, auditable and interoperable. Before literature on quantum-safe transitions in the public sector, existing research focuses less on how to pick an algorithm on a single algorithm and more on the coordination, phased implementation, and the long-term engineering capacity [5].

A. 2047-aligned transition milestones.

Milestone based planning is proposed in a Viksit Bharat framing of 2047. Short-term goals are cryptographic inventory, crypto-agile refactoring of key services and PQC pilots in controlled settings. The milestones in mid-term involve deployment of hybrid across high-value inter-agency connections and PQC-enabled software supply chain signing. The long-term targets are PQC-by-default PKI and extensive abandonment of legacy public-key schemes wherever possible. This gradual procedure balances the urgency with continuity of service and gradually decreases quantum related exposure.

B. Workforce growth and systematic testing.

Migration needs cryptographic engineering skills which are not readily available at the moment. One practical approach is to develop joint testbeds and reference implementations, which can be reused by ministries and states, and to provide specific training to PKI operators, developers and auditors. Co-exists can decrease fragmentation: interoperability events and shared conformance tests may expose problems early, preventing incompatible agency deployments. The long-term resilience is also supported by this investment, as the process of PQC adoption will engage lots of cycles of upgrades as the standards and implementations will evolve [6].

C. Procurement, vendor preparation, and lifecycle management.

Government acquisition may hasten PQC preparedness when the contracts describe quantifiable demands: supported sets of algorithms, update procedures, limits of cryptographic modules, and a recorded migration course. Vendor due diligence must contain feature claims, but must also contain evidence of testing and maintenance plans. Since most of the existing public services are based on third-party stacks (identity middleware, network appliances, HSMs, mobile SDKs), procurement policies ought to mandate that such stacks be kept up-to-date and the cryptographic dependencies disclosed.

D. Side channel and engineering error protection.

Unless a constant time discipline is enforced, PQC algorithms, especially lattice-based schemes, can be susceptible to timing, cache and power analysis attacks. The engineering teams are expected to use libraries of explicit, proven libraries, impose secure coding and code review policies, and add side-channel testing to acceptance tests. One of the most important

challenges mentioned in the recent PQC analyses is the implementation security aspect, in particular when implemented on the national scale with adversaries that are capable and persistent [8].

E. Modernization in PKI and signing pipeline.

Government trust infrastructure is a migration point with high leverage as access to most of the services is through certificates and signatures. PQC has effects on certificate sizes, load on signature verification and compatibility with other existing libraries. One practical way to do this is to initially facilitate PQC-sensitive certificate issuance in controlled internal settings (e.g., test roots and intermediates), then introduce PQC signatures to high-value artifacts, e.g., firmware and software updates, and finally lay the groundwork to large-scale trust anchor distribution. This sequencing minimises systemic risk and enables engineering personnel to resolve interoperability concerns prior to cutovers facing citizens.

F. Hybrid deployment patterns and cutover criteria.

A classical + PQC is a risk-management tool in the transitory phase: it guards against unknown vulnerabilities in a new primitive and supports the continuity of legacy clients unable to upgrade in the near future. But hybrid modes have the potential to grow message size and computation cost. Empirical data on PQC in TLS suggests that the overhead is determined by the selected scheme and deployment context, which supports the importance of staged pilots and measurement-based rollouts [9]. An example cutover rule that can be implemented is to scale up PQC-enabled endpoints once latency, error, and resource usage benchmarks have been met during peak traffic.

G. Crypto-agility by design, not as an afterthought.

Hard-coded algorithms in applications, embedded devices and identity systems are a significant reason why cryptographic transitions are slow. Crypto-agility means that cryptographic decisions must be relocated to configuration, policy, or negotiated protocol, and the behavior on failure must have been thoroughly tested. As an illustration, the services should accommodate various cipher suites and signature algorithms, and have the capability to change certificates and keys without service interruption. This is in accordance with the socio-technical perspective that the public systems should not treat cryptography as one-time implementation decision, but rather a dependency that needs to be updated over time [5].

H. Program governance and ownership.

The digital services in India are provided by the ministries, state organizations and the partners of the public sector. A PQC program must thus have a definite owner (or steering group) that has the power to stipulate baselines and timelines. This body should operationally publish a profile of the government to PQC deployment (e.g. approved algorithm families, acceptable hybrid modes, certificate profile guidance, minimum implementation requirements) and keep a public change-log of cryptographic policies. Governance should also establish accountability: who signs crypto parameter changes, who signs PKI trust anchors and who signs deployments before go-live.

VI. Conclusion

The shift to post-quantum cryptographic system is a strategic need to maintain trust in the digital infrastructure in operation in government. The essential issue that India faces lies not in the mere choice of quantum-resistant algorithms but in the management of the process of a multi-year transition that has to negotiate the presence of heterogeneous platforms, underlying legacy constraints, and complex governance structures. A practical approach must emphasis on systematic cryptographic inventories, the implementation of crypto-agility principles, staged or hybrid implementation, PKI and signing pipeline prioritization and the coordinated deployment of capacity. All these measures reduce quantum exposure, do not disrupt the continuity of services, and avoid interoperability. Through timely action, India can enhance the country level cyber resilience and place its digital governance ecosystem in a proper location to ensure long-term security in line with the Viksit Bharat @2047 vision.

References

[1] S. Ali, S. A. Wadho, K. R. Talpur, B. A. Talpur, K. S. S. Alshudukhi, M. Humayun, S. R. Talpur, M. A. Al Mamun, M. T. Naseem, A. Abro, D. B. Talpur, and A. Shah, "Next-generation quantum security: The impact of quantum computing on cybersecurity—Threats, mitigations, and solutions," Computers and Electrical Engineering, vol. 128, 2025, doi: 10.1016/j.compeleceng.2025.110649.

[2] V. S. Barletta, D. Caivano, A. Pal, M. Scalera, and M. A. Serrano Martin, "Enabling quantum privacy and security by design: Imperatives for contemporary state-of-the-art in quantum software engineering," Journal of Software: Evolution and Process, vol. 37, no. 2, 2025, doi: 10.1002/smr.70005.

[3] M. El Bizri, A. M. el-Hajj, L. Sliman, and A. M. Haidar, "Institutional approaches to post-quantum cryptography: A comparative analysis of migration frameworks," IEEE Access, 2026, doi: 10.1109/ACCESS.2025.3650465.

[4] M. Khawar, S. Khalid, M. U. Rehman, A. B. Usman, W. Al Malwi, and F. A. Asiri, "Shaping the future of cybersecurity: The convergence of AI, quantum computing, and ethical frameworks for a secure digital era," Computer Science Review, vol. 60, 2026, doi: 10.1016/j.cosrev.2025.100882.

[5] I. Kong, M. Janssen, and N. Bharosa, "Challenges in the transition towards a quantum-safe government," pp. 282–292, 2022, doi: 10.1145/3543434.3543644.

[6] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang, and N. Xiong, "Post-quantum security: Opportunities and challenges," Sensors, vol. 23, no. 21, 2023, doi: 10.3390/s23218744.

[7] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018, doi: 10.1109/MSP.2018.3761723.

[8] B. Rawal and P. Curry, "Challenges and opportunities on the horizon of post-quantum cryptography," APL Quantum, vol. 1, 2024, doi: 10.1063/5.0198344.

[9] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH," 2020, doi: 10.1145/3386367.3431305.