ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

DAILY CURRENT AFFAIRS

National Quantum Mission — India Achieves 1,000-km Secure QKD Network

10 April 2026 · SCIENCE & TECH

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

National Quantum Mission — India Achieves 1,000-km Secure QKD Network

10 April 2026 · 5 min read · 1 tag

On this Page

WHY IN NEWS

India's National Quantum Mission (NQM) demonstrated a 1,000-km secure quantum communication network using Quantum Key Distribution (QKD) technology — one of the longest such deployments globally — developed by Bengaluru-based startup QNu Labs with support from NQM.

India's achievement of a 1,000-km QKD network represents a pivotal milestone in the country's ambition to build quantum-safe digital infrastructure. In an era where advances in quantum computing threaten to break conventional RSA and ECC encryption within years, quantum communication offers a theoretically unbreakable alternative rooted in the laws of physics rather than mathematical complexity.

WHAT IS QUANTUM KEY DISTRIBUTION (QKD)?

Quantum Key Distribution is a method of transmitting cryptographic keys using individual photons — the smallest discrete packets of light. The security guarantee of QKD rests on a fundamental principle of quantum mechanics: **measuring a quantum state inevitably disturbs it**. If an eavesdropper attempts to intercept a photon stream, the quantum state of the photons changes, and the disturbance is immediately detectable by the sender and receiver.

This is fundamentally different from classical encryption, where an eavesdropper can copy an encrypted message and attempt to crack it later (a "harvest now, decrypt later" attack — a growing concern as quantum computers approach practical cryptanalytic capability).

How QKD Works — Step by Step

1. **Photon transmission:** The sender (Alice) transmits photons in random quantum states representing binary bits (0 or 1) through an optical fibre or free-space link.
2. **Measurement:** The receiver (Bob) measures each photon using randomly selected bases.
3. **Sifting:** Alice and Bob publicly compare which bases they used (not the actual values) — only matching-base measurements are kept.
4. **Error checking:** A small sample is compared to detect eavesdropping — if error rate exceeds a threshold, the session is aborted.
5. **Privacy amplification:** The final key is distilled into a shorter, provably secure key — used to encrypt actual data via classical channels.

The resulting key is information-theoretically secure — unbreakable regardless of computing power, because any interception leaves a detectable trace.

INDIA'S NATIONAL QUANTUM MISSION — STRUCTURE AND SCOPE

PARAMETER	DETAILS
Approved	April 2023 (Union Cabinet)
Total outlay	₹6,003.65 crore over 8 years
Duration	2023–24 to 2030–31
Nodal ministry	Ministry of Science and Technology (DST)
Lead agency	Quantum Mission Secretariat, under Principal Scientific Adviser
Thematic Hubs (T-Hubs)	4 — IISc Bengaluru, IIT Bombay, IIT Madras, IIT Delhi

Four Technology Pillars of NQM

1. Quantum Computing

- Target: 50-qubit computers (3 years) → 1,000+ qubit computers (8 years)
- Application: Drug discovery, climate modelling, financial optimisation, materials science

2. Quantum Communication

- Target: 2,000-km national QKD backbone + secure satellite QKD by 2031
- **Current milestone: 1,000-km QKD network — April 2026**
- Developer: QNu Labs (Bengaluru) — India's leading quantum security startup

3. Quantum Sensing and Metrology

- Applications: Gravimeters, magnetometers, atomic clocks, medical imaging (MRI beyond classical limits)
- Military use: Quantum sensors for submarine detection, navigation without GPS

4. Quantum Materials

- Target: Develop new materials for qubits, superconductors, and topological insulators

QNU LABS — INDIA'S QUANTUM SECURITY PIONEER

QNu Labs, founded in 2016 and headquartered in Bengaluru, is India's first quantum cryptography company. It develops QKD systems, Quantum Random Number Generators (QRNGs), and post-quantum cryptography (PQC) solutions. The 1,000-km network demonstration used QNu's **Armos QKD** system, tested over deployed telecom fibre — making it operationally relevant rather than a laboratory prototype.

The company has received funding and support under the NQM framework and has earlier deployed pilot QKD links in Hyderabad and Thiruvananthapuram.

UPSC RELEVANCE

GS3: Science & Technology — Quantum Technology

Why Quantum Communication Matters for India:

- **Defence:** Quantum-encrypted military communications cannot be intercepted by adversaries
- **Banking:** Quantum-safe financial networks protect against future cryptanalytic attacks
- **Governance:** Sensitive government data (voter rolls, Aadhaar, tax records) protected agai harvest-now-decrypt-later attacks

- **Strategic autonomy:** Indigenous QKD development reduces dependence on foreign encryption hardware (which could have backdoors)

Global Context

COUNTRY	QKD STATUS
China	World leader — 12,000-km QKD backbone (Beijing-Shanghai + satellite link) since 2017
EU	EuroQCI initiative — quantum communication infrastructure across EU by 2027
USA	NIST finalised post-quantum cryptography standards (2024) — parallel track
Japan	Tokyo QKD metropolitan network operational since 2015
India	**1,000-km QKD milestone (2026); 2,000-km target by 2031**

China's lead is significant — its Micius satellite demonstrated intercontinental QKD (China-Austria, 7,600 km) in 2017. India's NQM explicitly aims for quantum satellite communication as part of its 8-year roadmap.

Quantum vs Post-Quantum Cryptography — Key Distinction

APPROACH	MECHANISM	BASIS
Quantum Key Distribution (QKD)	Uses quantum physics to distribute keys	Physics laws (quantum mechanics)
Post-Quantum Cryptography (PQC)	Classical algorithms resistant to quantum attacks	Mathematical hardness (lattice problems, hash functions)

India is pursuing both tracks — NQM for QKD infrastructure, and DST has a separate initiative on PQC standardisation aligned with NIST's 2024 PQC standards.

📌 FACTS CORNER — KNOWLEDGEPEDIA

NATIONAL QUANTUM MISSION:

Approved: April 2023 | Cabinet outlay: ₹6,003.65 crore | Duration: 8 years (to 2031)

Nodal: DST (Ministry of Science & Technology)

4 Thematic Hubs: IISc Bengaluru, IIT Bombay, IIT Madras, IIT Delhi

4 Pillars: Quantum Computing, Quantum Communication, Quantum Sensing, Quantum Materials

QKD MILESTONE:

Network: 1,000 km (April 2026) | Developer: QNu Labs, Bengaluru

Technology: Quantum Key Distribution over deployed optical fibre

Target: 2,000-km national backbone + quantum satellite by 2031

GLOBAL LEADERS:

China: 12,000-km QKD network + Micius satellite (intercontinental QKD since 2017)

EU: EuroQCI initiative | USA: NIST PQC standards (2024)

Micius satellite: China's quantum satellite; demonstrated 7,600-km China-Austria QKD (2017)

SECURITY PRINCIPLE:

QKD security basis: Laws of quantum mechanics (any eavesdropping = detectable disturbance)

Classical encryption security basis: Mathematical hardness (factoring large primes)

"Harvest now, decrypt later": Adversaries store encrypted data today; decrypt when quantum computers mature

← PREVIOUS ARTICLE
Current Affairs Today — April 10, 2026

NEXT ARTICLE →
Assembly Elections 2026 — Voting Concludes in Assam, Kerala,...

RELATED EDITORIALS

INDIAN EXPRESS

CBSE's AI Curriculum — Lofty Goals, Little Clarity

10 Apr

THE HINDU

In the Running — Artemis II and the Future of Human Deep-Space Exploration

3 Apr

INDIAN EXPRESS

Digital Sovereignty Begins at the Hardware Layer — India's CCTV Mandate and What Comes Next

1 Apr

DOWN TO EARTH

Rethinking E20 — India's Ethanol Mandate, Climate Trade-offs, and the Food-Fuel Tension

1 Apr

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/daily/2026/04/10/national-quantum-mission-qkd-1000km/