PLUTUS
IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –13-May 2025

QUANTUM KEY DISTRIBUTION: A BREAKTHROUGH IN INDIA'S CYBERSECURITY INFRASTRUCTURE

WHY IN THE NEWS?

In a significant development towards enhancing India's capabilities in quantum-secure communication, the Centre for Development of Telematics (C-DOT) has signed a Memorandum of Understanding (MoU) with Synergy Quantum India Private Limited, a deep-tech company specializing in quantum technologies. This collaboration aims to develop Drone-based Quantum Key Distribution (QKD) systems using the decoy-based BB84 protocol with polarization encoding, at Technology Readiness Level 6 or above. The initiative supports the goals of the Atmanirbhar Bharat mission by fostering indigenous R&D in emerging technologies. The partnership will also facilitate co-development of research proposals, academic dissemination, and organization of expert talks and symposia to promote innovation in quantum communication.

WHAT IS QUANTUM KEY DISTRIBUTION TECHNOLOGY(QKDT)?

Quantum Key Distribution Technology (QKDT) is a cutting-edge method of secure communication that uses the principles of quantum mechanics to exchange encryption keys between two parties. The primary goal of QKDT is to ensure that encryption keys can be shared in a way that is provably secure—meaning that any attempt by an unauthorized party to intercept or tamper with the key can be detected immediately.

Key Features of QKDT:

1. Based on Quantum Physics: Unlike traditional encryption, which relies on complex mathematical algorithms, QKDT uses the fundamental laws of quantum mechanics—such as superposition, entanglement, and the no-cloning theorem.

2. Security Guarantee: If an eavesdropper tries to intercept the quantum key, the quantum state of the particles will be disturbed, alerting the communicating parties to the intrusion.

3. Use of Photons: The technology typically uses individual photons (light particles) transmitted over optical fiber cables to encode key information (called qubits).

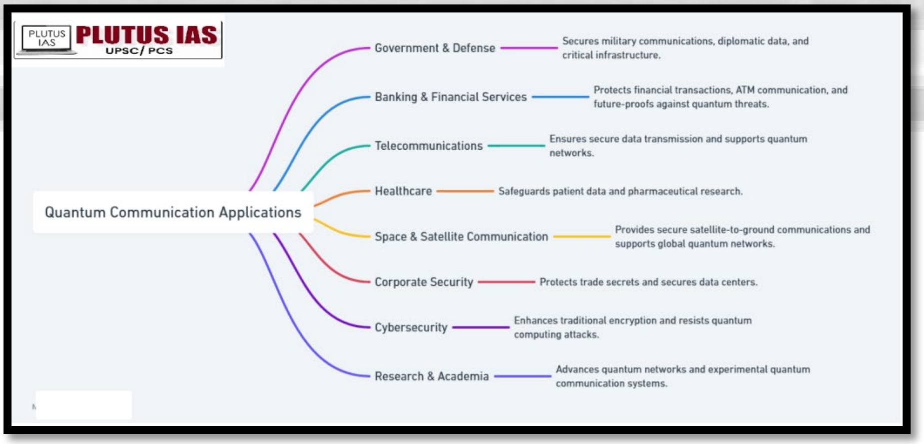
4. Unbreakable Encryption: Because of quantum laws, QKDT cannot be cracked even by quantum computers, making it a key tool in future-proof cybersecurity.

5. Example Protocols: Popular QKDT protocols include BB84, E91, and Decoy State Protocols

QKDT VS TRADITIONAL KDT

Feature	Quantum Key Distribution Technology (QKDT)	Traditional Key Distribution (KDT)
Underlying Principle	Based on quantum mechanics (e.g., superposition, entanglement)	Based on mathematical algorithms and computational hardness
Security Basis	Physics-based – any eavesdropping disturbs the quantum system	Algorithm-based – depends on difficulty of solving problems
Eavesdropping Detection	Yes – intrusion alters quantum states and is detectable	No direct detection – intrusion can go unnoticed
Vulnerability to Quantum Computers	Not vulnerable – inherently resistant to quantum attacks	Vulnerable – quantum computers can break current algorithms
Key Transmission Medium	Photons over optical fibers or free-space channels	Classical communication channels like the internet
Example Protocols	BB84, E91, Decoy State Protocols	RSA, Diffie-Hellman, ECC (Elliptic Curve Cryptography)
Implementation Complexity	High – requires specialized hardware like single-photon detectors	Moderate – compatible with existing digital infrastructure
Key Distribution Range	Limited – typically up to 100–300 km over fiber (without repeaters)	Practically unlimited – via internet and global networks
Maturity and Adoption	Emerging – research and pilot projects ongoing	Mature – widely adopted in global systems
Use Cases	Ultra-secure communication (e.g., defense, banking, government)	General encryption across internet services and data exchange

QKDT APPLICATIONS



Quantum Communication Applications

Government & Defense – Secures military communications, diplomatic data, and critical infrastructure.

Banking & Financial Services – Protects financial transactions, ATM communication, and future-proofs against quantum threats.

Telecommunications – Ensures secure data transmission and supports quantum networks.

Healthcare – Safeguards patient data and pharmaceutical research.

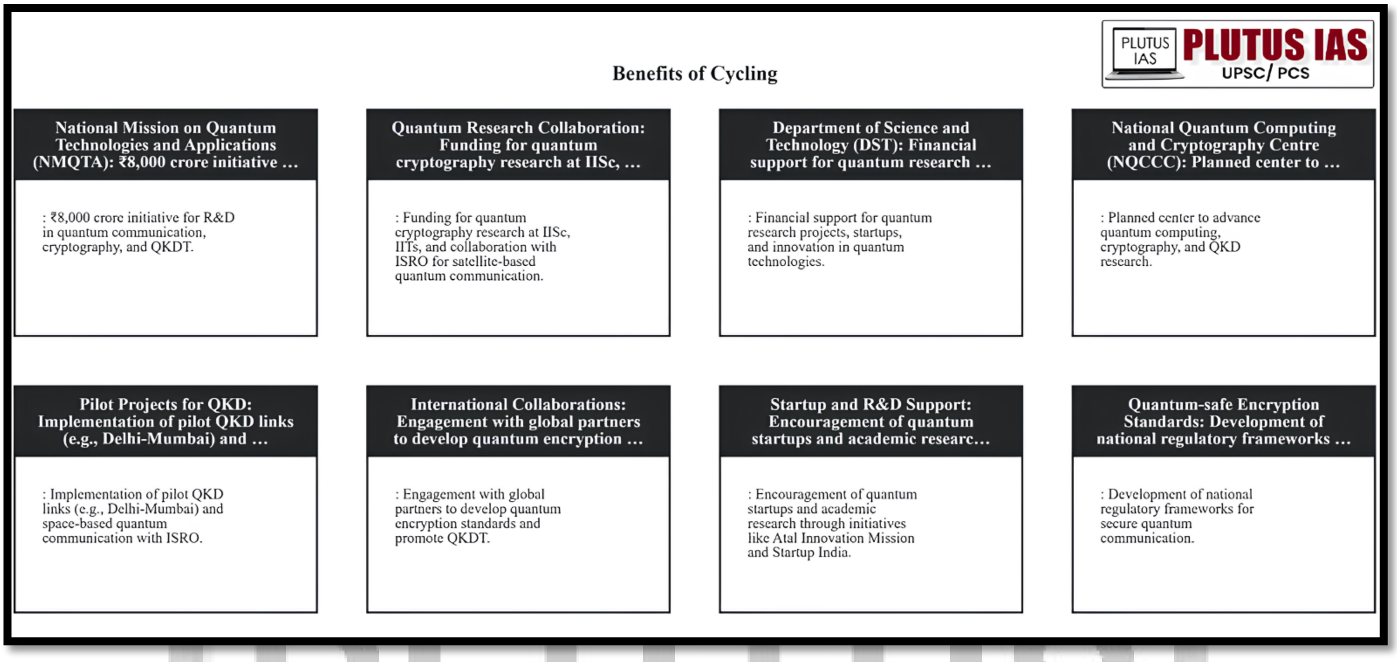
Space & Satellite Communication – Provides secure satellite-to-ground communications and supports global quantum networks.

Corporate Security – Protects trade secrets and secures data centers.

Cybersecurity – Enhances traditional encryption and resists quantum computing attacks.

Research & Academia – Advances quantum networks and experimental quantum communication systems.

WHAT ARE GOVT.INITIATIVES TO PROMOTE QKDT IN INDIA



Benefits of Cycling

National Mission on Quantum Technologies and Applications (NMQTA): ₹8,000 crore initiative …

: ₹8,000 crore initiative for R&D in quantum communication, cryptography, and QKDT.

Quantum Research Collaboration: Funding for quantum cryptography research at IISc, …

: Funding for quantum cryptography research at IISc, IITs, and collaboration with ISRO for satellite-based quantum communication.

Department of Science and Technology (DST): Financial support for quantum research …

: Financial support for quantum research projects, startups, and innovation in quantum technologies.

National Quantum Computing and Cryptography Centre (NQCCC): Planned center to …

: Planned center to advance quantum computing, cryptography, and QKD research.

Pilot Projects for QKD: Implementation of pilot QKD links (e.g., Delhi-Mumbai) and …

: Implementation of pilot QKD links (e.g., Delhi-Mumbai) and space-based quantum communication with ISRO.

International Collaborations: Engagement with global partners to develop quantum encryption …

: Engagement with global partners to develop quantum encryption standards and promote QKDT.

Startup and R&D Support: Encouragement of quantum startups and academic researc…

: Encouragement of quantum startups and academic research through initiatives like Atal Innovation Mission and Startup India.

Quantum-safe Encryption Standards: Development of national regulatory frameworks …

: Development of national regulatory frameworks for secure quantum communication.

CHALLENGES IN QKDT APPLICATION

1. Infrastructure Limitations: Quantum key distribution requires advanced infrastructure, such as high-quality fiber optic cables and photon detectors, which can be expensive and complex to implement.

2. Distance Limitations: The range of QKD is typically limited to around 100-200 km due to photon loss in transmission. Longer distances require specialized techniques, such as satellite-based communication.

3. Photon Loss and Noise: Transmission of photons through fibers or air is prone to loss, noise, and environmental interference, which can degrade the quality and security of the key exchange.

4. Scalability Issues: Scaling QKD systems for widespread use, particularly for large networks, is a significant challenge, especially due to the technical complexity and high cost.

5. Integration with Existing Infrastructure: Integrating QKDT with existing cryptographic systems and networks poses compatibility and security challenges.

6. High Cost: The cost of QKD equipment, such as photon detectors and quantum communication devices, remains high, limiting the widespread adoption.

7. Security Vulnerabilities: While QKDT offers theoretical security, real-world implementations may still be vulnerable to attacks like photon number splitting or imperfections in quantum hardware.

8. Regulatory and Standardization Issues: The lack of universal standards and regulatory frameworks for QKD can hinder its integration into commercial systems and widespread adoption.

WAY FORWARD

1. Enhanced Research and Development: Continued investment in R&D is crucial to overcoming the technical barriers, such as photon loss, noise, and scalability.

2. Infrastructure Development: Governments and private sectors should focus on developing and upgrading the necessary infrastructure for QKDT, including the installation of high-quality optical fibers, photon detectors, and quantum-safe hardware.

3. Cost Reduction: As the technology matures, economies of scale should help reduce the cost of key components such as photon detectors and quantum communication devices.

4. Standardization: International standardization bodies must work on defining and establishing universal standards for QKDT to ensure compatibility, scalability, and security across global platforms.

5. Integration with Existing Cryptographic Systems: Researchers and industry players need to develop hybrid systems that combine classical and quantum key distribution to ensure smooth integration with existing infrastructure and protocols.

6. Policy and Regulatory Framework: Governments should create clear regulatory guidelines and policies around the usage of QKDT to encourage innovation while safeguarding national security and privacy concerns.

7. Public-Private Partnerships: Collaboration between government agencies, research institutions, and private companies can expedite the development and deployment of QKDT, especially in areas like defense, banking, and communication sectors.

8. Awareness and Training: Building a skilled workforce through specialized training programs in quantum technologies will be essential for the smooth adoption of QKDT in various industries.

CONCLUSION

Quantum Key Distribution Technology (QKDT) offers a revolutionary approach to secure communication by leveraging quantum mechanics, ensuring encryption keys cannot be intercepted without detection. Unlike traditional cryptography, QKDT's security relies on quantum principles, making it resistant to quantum computer threats. However, challenges like high infrastructure costs, limited range, and scalability issues remain. The Indian government is fostering QKDT development through initiatives like the C-DOT and Synergy Quantum India partnership, aiming to promote indigenous research. For broader adoption, continued advancements in R&D, infrastructure, standardization, and clear regulatory policies are necessary. As these hurdles are overcome, QKDT could significantly enhance cybersecurity across critical sectors such as defense and banking.

PRELIMS QUESTIONS

Q. Which of the following are key features of QKDT?

1. It uses classical algorithms to encrypt messages.
2. The security of QKDT is based on quantum mechanics principles.
3. QKDT guarantees unbreakable encryption even against quantum computers.
4. It relies on fiber optics or free-space channels for key distribution.

Select the correct answer using the code below:

a) 1, 2 and 3
b) 2 and 3, 4
c) 1, 3 and 4
d) 2 and 3

Answer: B

MAINS QUESTIONS

Q. Quantum Key Distribution Technology (QKDT) is often considered a breakthrough in cybersecurity. Discuss its potential applications, government initiatives in India to promote it, and the challenges that may hinder its widespread adoption.

(250 words, 15 marks)

PLUTUS IAS
UPSC / PCS

MORNING BATCH

ONLINE BATCH AVAILABLE AT CHANDIGARH

STATE PCS

ENGLISH MEDIUM

Starting From 06th & 19th MAY 2025

08:00AM– 12:00PM

PLUTUS IAS WHATSAPP CHANNEL
Know More

2nd Floor, Apsara Arcade, Karol Bagh Metro Station
Gate No. – 6, New Delhi 110005

OUR CENTERS Delhi I Chandigarh I Shimla I Bilaspur

+91-8448440231 info@plutusias.com www.plutusias.com