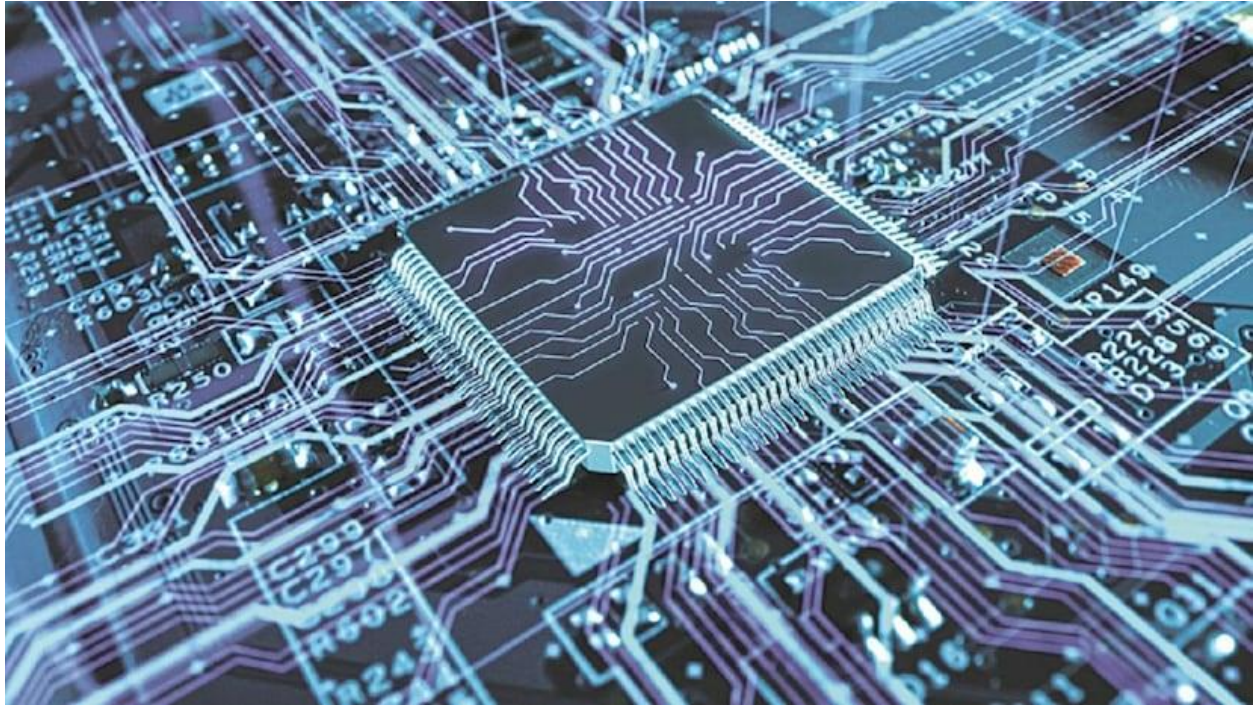


THE RISE OF QUANTUM TECHNOLOGY & INDIA- SCIENCE & TECH - PAPER III



In recent years, **quantum technology** has emerged as one of the most transformative forces poised to revolutionize industries, economies, and national security. As the world faces increasing digital threats and the limitations of current technologies, quantum technology offers groundbreaking solutions. However, the path to fully embracing this technology is complex and filled with challenges, especially for countries like India, which are making strides but still lack a clear road map for widespread adoption.

This article aims to provide an understanding of **quantum technology**, the two key forms driving its development—**Post-Quantum Cryptography (PQC)** and **Quantum Key Distribution (QKD)**—and its significance for the future. Additionally, it will highlight India's progress in the field, the challenges it faces, government measures to promote the technology, the **National Quantum Mission**, and the urgency with which India must act to stay competitive in the global race for quantum supremacy.

What is Quantum Technology?

At its core, **quantum technology** leverages the principles of quantum mechanics, a branch of physics that studies the behavior of matter and energy at extremely small scales, such as atoms and subatomic particles. Quantum mechanics operates differently from classical physics, allowing for new and unexpected behaviors that can be harnessed for technological advancements.

Quantum technology has several branches, including quantum computing, quantum sensing, quantum communication, and quantum cryptography. The most immediate applications of quantum technology involve securing communication networks and enhancing computational power in ways that were previously unimaginable. This has led to an intense global race, as quantum technology has the potential to disrupt everything from cybersecurity to healthcare, finance, and national defense.

Two Key Quantum Technologies: PQC and QKD

In the realm of cybersecurity, two particular forms of quantum technology stand out:

1. **Post-Quantum Cryptography (PQC):**

- PQC involves developing cryptographic algorithms that are resistant to quantum computer-based attacks. Quantum computers, which are exponentially more powerful than traditional computers, have the potential to break many of the encryption standards used today. This could pose a serious threat to the security of digital communication, financial systems, and sensitive government data.
- PQC aims to create new algorithms that can withstand quantum attacks, ensuring that data remains secure even in a world where quantum computers are operational. The **United States** has been at the forefront of developing PQC standards, with the **National Institute of Standards and Technology (NIST)** playing a key role in setting these standards.

2. **Quantum Key Distribution (QKD):**

- Unlike PQC, which focuses on making existing cryptographic techniques quantum-resistant, QKD uses the principles of quantum mechanics to securely distribute encryption keys. QKD ensures that any attempt to intercept or tamper with the keys during transmission is immediately detectable, making communication far more secure than classical methods.
- **China** and **Russia** are investing heavily in QKD, and in recent years, China has made significant strides, establishing a 2,000-kilometer QKD-secured optical fiber network between Beijing and Shanghai and achieving QKD over satellite links.

The Significance of Quantum Technology for the Future

Quantum technology has the potential to fundamentally change the digital landscape. As industries increasingly rely on data, communication, and complex computations, quantum technology promises to make these processes faster, more efficient, and more secure. The implications for cybersecurity are particularly significant, as quantum computers could one day break the encryption methods that protect everything from financial transactions to government communications.

In addition to cybersecurity, quantum technology can transform fields such as:

- **Medicine**, by allowing faster drug discovery and personalized treatments.
- **Finance**, through enhanced risk analysis and fraud detection.
- **Climate science**, by enabling more accurate environmental models.

Moreover, quantum communication and computing could open up entirely new areas of innovation that we cannot yet fully anticipate. This is why nations around the world, including the **United States**, **China**, **Russia**, and **India**, are investing heavily in quantum research and development.

India's Progress in Quantum Technology

India has made significant strides in quantum technology over the past few years, with notable advancements in both PQC and QKD. **Indian startups** have developed PQC solutions that are compatible with NIST standards, positioning the country as a potential leader in quantum-resistant cryptography.

In the field of QKD, India achieved a major milestone in 2019 by securing a 130-kilometer quantum communication link in a single hop. By 2023, an Indian startup under the **Innovations for Defence Excellence (iDEX)** program developed a 200-kilometer single-hop QKD solution, showcasing the country's growing capabilities in this cutting-edge field.

In addition to private-sector innovation, the Indian government has been actively promoting quantum research. In **April 2023**, the government approved the **Rs 6,000 crore National Quantum Mission**, which focuses on four key areas: **quantum computing, quantum communication, quantum sensing, and quantum materials.**

Challenges Facing Quantum Technology Adoption in India

Despite these advancements, India faces several challenges in adopting quantum technology on a larger scale:

1. **Lack of clear policy and road map:** While India has made progress in research and development, there is no well-defined road map for the widespread adoption of quantum technologies. Without a clear strategy, India risks falling behind in the global race for quantum supremacy.
2. **Slow certification and adoption processes:** A major hurdle is the slow pace at which new quantum technologies are certified and adopted. For example, it took over two years for a startup's QKD solution to receive certification, which is too long given the fast-evolving nature of the technology.
3. **Absence of mandatory standards:** India needs established standards to ensure **interoperability** and **quality** across different quantum technologies. Without these standards, adoption will remain fragmented and slow.

4. **Limited infrastructure for testing and deployment:** The infrastructure required to test and deploy quantum technologies, particularly QKD, is still lacking in many parts of the country.

Government Measures to Promote Quantum Technology

The Indian government has taken important steps to promote quantum technology, most notably through the **National Quantum Mission**. This mission aims to develop India's quantum capabilities in both the research and practical application of quantum technologies.

In addition to funding research, the government has also focused on fostering innovation through initiatives like **iDEX**, which supports defense-related startups in developing cutting-edge technologies. However, the government needs to go beyond research and development to implement a robust policy framework that accelerates the adoption of quantum technologies across industries.

National Quantum Mission

The **National Quantum Mission** is India's most significant effort to date in promoting quantum technology. With a budget of **Rs 6,000 crore**, the mission focuses on key areas like **quantum computing, communication, sensing, and materials**. The goal is to not only make India a leader in quantum research but also to ensure the practical deployment of these technologies in critical sectors like **defense, cybersecurity, and telecommunications**.

However, the success of this mission will depend on how effectively it is implemented. As with previous large-scale initiatives like **Aadhaar** and **UPI**, a well-monitored implementation strategy will be key to ensuring widespread adoption.

Urgent Need for a Clear Road Map

Despite the progress made, there is an urgent need for India to develop a clear policy framework and road map for the adoption of quantum technologies. Without such a framework, India risks

losing its competitive edge in the global race for quantum dominance. The government must act quickly to:

- Establish **mandatory standards** for quality and interoperability.
- **Accelerate the certification** and deployment processes for new quantum technologies.
- Use **government procurement** to drive market adoption, ensuring that India's critical digital infrastructure is quantum-safe.
- Develop a clear timeline for the widespread implementation of quantum technologies, possibly setting a deadline as early as **2026**.

Conclusion

Quantum technology has the potential to reshape the future of industries and national security, and countries like India must act swiftly to stay competitive. While India has made commendable progress in research and development, the challenges of slow certification, lack of a clear policy, and limited infrastructure must be addressed. The **National Quantum Mission** provides a strong foundation, but it is imperative that the government adopts a robust implementation strategy to ensure the widespread adoption of quantum technology. The global race for quantum supremacy is accelerating, and India must ensure it is not left behind.

Main Practice Questions

Discuss the significance of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) in the context of future cybersecurity. How are countries like India, the United States, China, and Russia approaching these technologies? What are the key challenges faced by India in adopting quantum technology, and what measures has the Indian government taken to address them?

Answer Guidelines:

- **Introduction to PQC and QKD:**

- Briefly explain **Post-Quantum Cryptography (PQC)** and how it aims to secure data against quantum computer attacks.
- Define **Quantum Key Distribution (QKD)** and its use of quantum mechanics to secure key exchanges, making it highly resistant to interception.
- **Global Approaches:**
 - Discuss how the **United States** is prioritizing PQC, with initiatives led by **NIST** to establish PQC standards.
 - Mention that **China** and **Russia** are investing heavily in **QKD**, achieving significant milestones, such as China's **QKD-secured optical fiber network** and the QKD satellite link between Moscow and Urumqi.
 - Explain India's dual approach, with developments in both **PQC and QKD** and the growing contributions of **Indian startups**.
- **Challenges for India:**
 - Highlight the challenges India faces, such as the **lack of a clear policy framework, slow certification processes, and the absence of mandatory standards** for interoperability and quality.
- **Government Measures:**
 - Discuss the Indian government's efforts, including the launch of the **National Quantum Mission**, with a focus on quantum computing, communication, and sensing.
 - Mention the importance of government support through initiatives like **iDEX** to foster innovation in defense and quantum technology.
- **Conclusion:**
 - Summarize the urgency for India to implement a more robust strategy to stay competitive in the quantum race.