QUANTUM KEY DISTRIBUTION – SCIENCE & TECHNOLOGY

NEWS: India has **successfully demonstrated a free-space quantum secure communication using quantum entanglement** over 1 km recently via an optical link.

WHAT'S IN THE NEWS?

About the Experiment

- The experiment was conducted by researchers at the **DRDO-Industry-Academia Centre of Excellence (DIA-CoE), IIT Delhi**, demonstrating India's growing capability in quantum technologies.
- It was part of a sanctioned project titled **'Design and development of photonic technologies for free space QKD'**, funded by the **Directorate of Futuristic Technology Management (DFTM), DRDO**.
- The primary objective was to **demonstrate quantum secure communication** using **quantum entanglement over free space**, a technique with far-reaching applications in national security and future networks.

Key Features of the Experiment

- A **free-space optical quantum communication link** was successfully established over a **distance of more than 1 km** within the IIT Delhi campus.
- The experiment achieved a **secure key rate of approximately 240 bits per second**, considered significant for a free-space trial.
- The **Quantum Bit Error Rate (QBER)** was recorded at **less than 7%**, indicating high signal integrity with minimal noise or potential interference.
- **QBER** serves as an indicator of possible **eavesdropping or environmental noise**, where a lower QBER implies a **more secure quantum channel**.

Applications and Significance

a) Cybersecurity

- The technology supports **real-time applications in quantum cybersecurity**, especially **Quantum Key Distribution (QKD)** over long distances.
- Future applications include **quantum-safe data encryption**, particularly vital for protecting **financial, healthcare, and strategic data infrastructures**.

b) Quantum Networks and Internet

- The experiment paves the way for **future quantum internet development**, involving **entanglement-based networks** that link various quantum devices and systems securely.
- It contributes to **building India's quantum communication ecosystem**, aligning with the goals of **National Mission on Quantum Technologies and Applications (NM-QTA)**.

c) National Security

- QKD can be deployed in **defence and intelligence sectors** to establish **tamper-proof communication channels**, minimizing the risk of data breaches in sensitive areas.
- It is applicable in **government communications, financial systems**, and **military command-and-control networks**.

About Quantum Key Distribution (QKD)

a) Definition and Principle

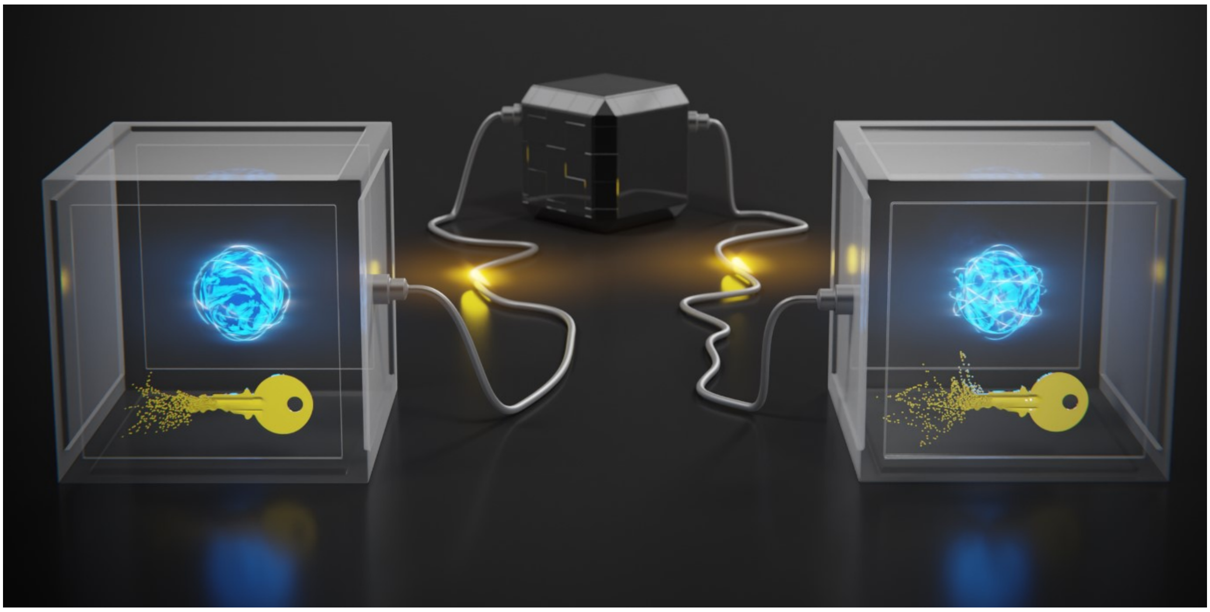
- **Quantum Key Distribution (QKD)** is a method that enables **two parties to securely exchange encryption keys** using principles of quantum mechanics.
- Unlike classical encryption, the **security of QKD is not based on mathematical complexity**, but on **physical laws** that make any interception detectable.

b) How QKD Works

- QKD transmits **quantum bits (qubits)**—often individual photons—**through fiber-optic cables or free space**.
- Each photon carries information in a **random quantum state**, forming a stream of **1s and 0s** (the encryption key).
- **Any interception attempt** (e.g., by an eavesdropper) **disturbs the quantum state**, alerting the parties to a security breach.

c) Origin of Concept

- The concept stems from the early 1970s work of **Stephen Wiesner**, who proposed "quantum conjugate coding".
- It was refined by **Artur Ekert in 1991**, who introduced the use of **quantum entanglement** for secure key sharing.



Types of QKD Protocols

a) Prepare-and-Measure Protocols

- One party **prepares quantum states** (e.g., polarized photons) and sends them to the other for measurement.
- **Example**: The **BB84 protocol**, where different photon polarizations are used to encode data and establish a shared secret key after a sifting process.

b) Entanglement-Based Protocols

- Both parties share **entangled photons**, where measurement on one instantly defines the state of the other.
- **Security is guaranteed** as any interference alters the correlation, allowing detection of eavesdropping.

Significance of QKD Technology

- **Quantum-safe encryption**: QKD is resistant to attacks from **quantum computers**, which threaten to break classical encryption.
- **Eavesdropping detection**: The nature of quantum measurement ensures that **any attempt to spy is immediately noticed**.
- **Unconditional security**: Unlike classical cryptography, QKD is not based on assumptions of computing power but on **inviolable laws of quantum physics**.
- **Future-proofing**: As computational capabilities evolve, QKD offers a **long-term solution** for protecting sensitive communication.

Limitations and Challenges of QKD

a) Authentication Gap

- QKD **does not provide source authentication**; parties still need a classical mechanism to ensure the identities of the sender and receiver.

b) Distance and Signal Loss

- Over long distances, **photon signals attenuate**, especially in fiber-based or free-space channels, **limiting the practical range** of QKD without repeaters.

c) Cost and Hardware Dependency

- QKD systems require **specialized hardware** such as **single-photon detectors and quantum random number generators**.
- These components are **expensive and sensitive**, increasing deployment costs and making large-scale adoption challenging.

d) Infrastructure Barriers

- QKD often needs **dedicated infrastructure**, such as **dark optical fibers**, which may not be compatible with existing communication systems.

e) Practical Security Flaws

- In practice, **hardware imperfections** (e.g., detector flaws) can introduce **security vulnerabilities**, despite the theoretical robustness of QKD.

f) Denial-of-Service (DoS) Risk

- An attacker could deliberately **disrupt transmission** (without reading the data), effectively **denying access to secure communication** by inducing high QBER.

Examples of India’s Advancements in QKD

- In **2022**, DRDO demonstrated **India’s first intercity quantum communication link** between **Vindhyachal and Prayagraj**, using **underground dark fiber**.

- In **2024**, a DRDO-supported team successfully achieved **entanglement-based quantum key distribution over a 100 km optical fiber spool**, showcasing India's **telecom-grade QKD potential**.

Source: https://www.opindia.com/2025/06/drdo-iit-delhi-successfully-demonstrate-quantum-entanglement-based-free-space-secure-communication/