Quantum Satellite

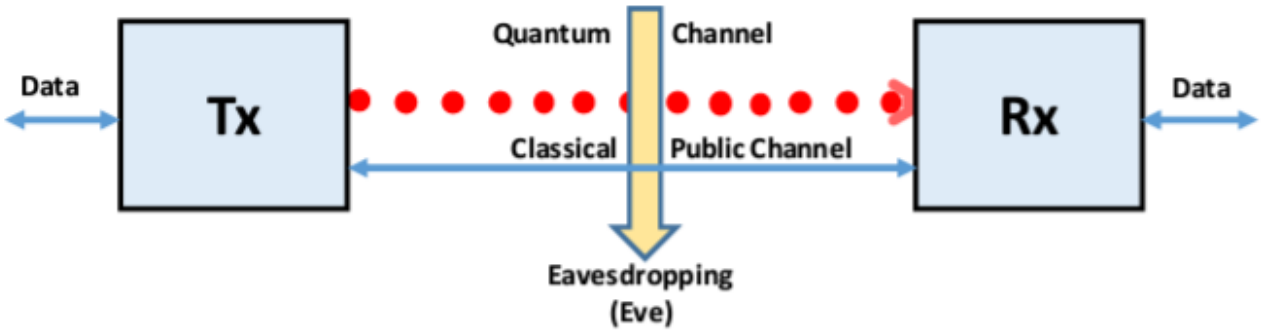
Why in News?

Recently, the chairperson of the National Quantum Computing Mission said India plans to launch a quantum satellite in "2-3 years for quantum communications".

What is Quantum satellite?

To know about National Quantum Mission, click here.

- **Quantum communication** – It relies on individual photons and quantum principles to carry quantum information.



Quantum Channel	Classical public channel
Secure key generation & distribution	Encrypted Communication

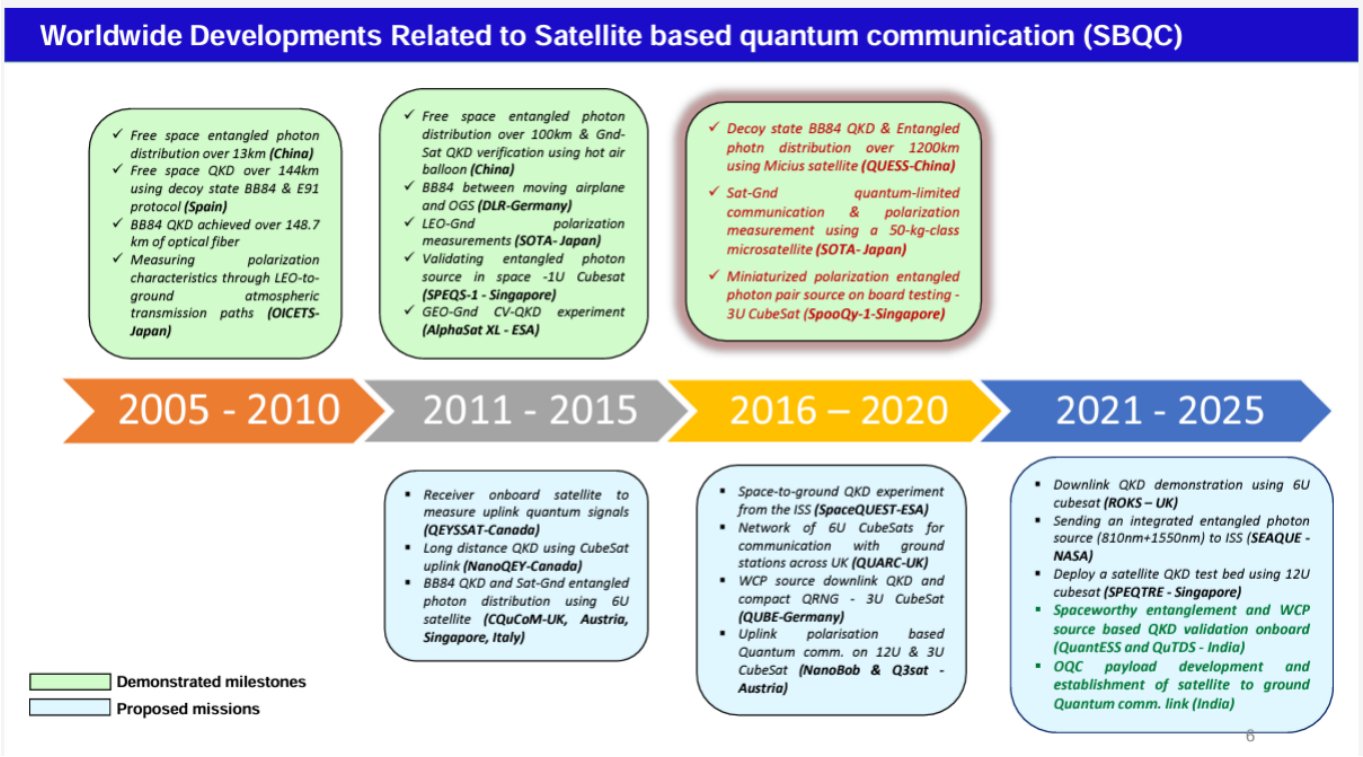
- **Quantum satellite** - These are communication satellites that uses quantum physics to secure its signals.
- **Quantum cryptography** - It uses quantum key distribution(QKD) to secure messages.
- **Quantum Key Distribution (QKD)** – QKD involves sending encrypted data as classical bits over networks, while the keys to decrypt the information are encoded and transmitted in a quantum state using qubits.
- QKD enables two parties to produce a shared random secret key (encryption key) known only to them.
- **Quantum measurement** — It is the act of measuring the properties of a quantum system, like a photon (the subatomic particle of light).
- According to the rules of quantum physics, a quantum measurement changes the state

of the system.

- **Methods of quantum encryption**
  - Encoding the key in a stream of photons (in two states, one representing 0 and the other 1) and any act of measuring them changes the state of the photons.
  - **Quantum entanglement** - when two photons are entangled, any change to one particle will instantaneously change the other.
- **Applications of quantum communication**
  - Satellite based Quantum Key Distribution (QKD) over larger distances
  - Protecting sensitive client information in Banking/ Finance Industry
  - Protecting customer credit card information
  - Government and defence industry
  - Protecting high value/sensitive data in remote data centres
  - NavIC based RS-Key distribution

What are worldwide developments related to quantum communication?

- China & Japan have successfully demonstrated Quantum Communication experiments from satellite to ground.
- **China** - It currently operates the world's largest QKD network with three quantum satellites and four ground stations.
- **Europe** - European Space Agency (ESA) is developing a technology demonstration satellite known as Eagle-1.
- **Germany** - Qube satellite was launched in August 2023 to test QKD capabilities.



- **India's progress:**
  - Single photon based inter-building free space quantum communication link was established over a distance of ~300m of atmospheric channel.
  - 2-way quantum secured client-to-client live video conferencing demonstration has been demonstrated.

- NavIC enabled synchronization mechanism has been implemented.
- BB84 protocol-based quantum key distribution(QKD) protocol was created.

What are the limitations of QKD?

- **Lack of source verification** - QKD does not provide a means to authenticate the QKD transmission source.
- **Upgradation difficulty** - Since QKD is hardware-based, QKD networks can't be upgraded or patched easily.
- **High cost** - QKD increases infrastructure costs that eliminate many use cases from consideration.
- **Limited security** - The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physic but rather the more limited security that can be achieved by hardware and engineering designs.
- **Denial-of-service attack** - Since eavesdroppers can cause a transmission to stop, they can deny the use of a transmission by its intended users (a.k.a. a).
- **Restrictions on quantum physics** - non-quantum information can be amplified before being transmitted across large distances whereas the no-cloning theorem prohibits the amplification of quantum information.
- **Capacity limitation** - Even the best optical fibers/ terrestrial free space can carry these photons only up to few hundreds of kilometres before light absorption makes the process impossible.

Post-quantum cryptography refers to cryptographic techniques that resist attacks from both quantum and classical devices using more advanced classical encryption.

Reference

The Hindu | Quantum Satellite