# Quantum States in Key Distribution

Unlike the traditional encoding of messages in 0s and 1s, quantum states encode messages in units of *Qubits* which are a binary and can also be a superposition of both the units. E.g. Spin of electron (-1/2 or +1/2), polarisation of light (left-polarised or right-polarised).

# Drawbacks and Advantages associated:

Associated drawbacks:

1. A received unknown quantum state cannot be reliably identified.
2. Attempts to read the message results in only partial information and is always accompanied by corruption of the state and part of the sent message is necessarily irretrievably destroyed.

Advantages:

1. Attempted eavesdropping can be will leave a mark, and in theory, be detected by a public discussion between sender and receiver.

# QKD using BB84 protocol

The message is encrypted using traditional means and distributed over a public channel, while the key is generated and distributed over a quantum channel.

Step 1: Node 1 (Sender) generates two uniform binary strings **x** = x1 x2 …xm and **y** = y1 y2 … ym, and then prepares the qubit states (quantum encoding), which are then sent to Node 2 (Receiver) over a quantum channel.

Step 2: Receiver (Node 2) receives these qubits which may not be the same (due to noise or eavesdropping). Receiver then choose a random **y’** = y’1 y’2 … y’m.and measures his **x’** = x’1 x’2 … x’m where x’i = xi if y’I = yi.

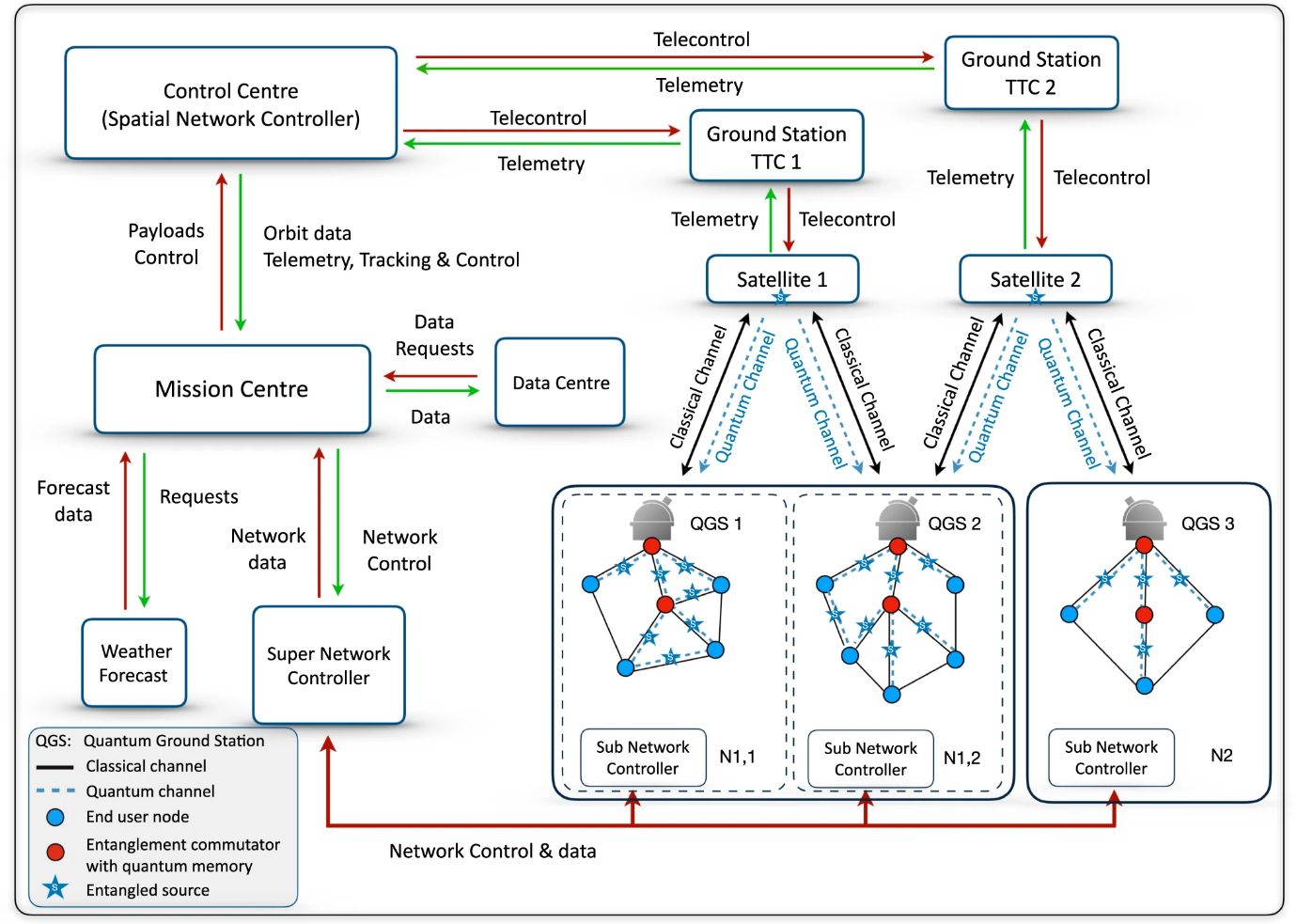
Step 3: Sender and Receiver publicly share their bases (**y** and **y’**). They discard all the bits, xi s and x’i correspondingly, where the bases do not match. The strings that remain (**~x** and **~x’**) are a choice of key to be used if there was not corruption.

Step 4: Sender and Receiver calculate the *bit error rate* (BER) by sharing a sample of **~x** and **~x’**  with each other, and assume that BER of this sample is the same as BER of the remaining string. This information can be used to correct the remaining errors in the string to a reasonably high accuracy at the expense of sacrificing a further portion of the string.

# Quantum Networks

1. Quantum signals are intrinsically weak as they depend on photons (light), not electricity and therefore cannot be amplified.
2. Furthermore, the signal-sending and receiving ends must be in line-of-sight reasonably.
3. Quantum signals loss is exponential in fiber with distance, but follow square-law in space; thus, providing promise when discussing networking between satellites.
4. Free-space links provided by satellites are affected by atmospheric phenomenon.
5. Quantum repeaters are an active area of research and will not mature in the near future.
6. The coverage of the satellite-based quantum networks is dependent on the orbit of the satellite, with higher orbiting ones giving a greater coverage.
7. In a general sense, rather than actually communication using quantum networks, the keys can be generated and exchanged using quantum networks, and the communication using traditional channels.
8. The below diagram provides a framework of a quantum network, wherein the quantum channel between Satellite and QGS is used for the key operation, while classical channel is used for communication.
9. Special hardware is required in the sending and receiving nodes, i.e., quantum processors (QPUs).
10. The communication occurs using optical networks (photon-based), through fiber, or free-space (as in atmosphere and space; relevant for satellites).

# Functional diagram of an integrated quantum information network with Space segment:



# Associated links and papers:

1. de Forges de Parny, L., Alibart, O., Debaud, J. *et al.* Satellite-based quantum information networks: use cases, architecture, and roadmap. *Commun Phys* **6**, 12 (2023). <https://doi.org/10.1038/s42005-022-01123-7>
2. Article: <https://physics.aps.org/articles/v15/172>
3. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, Yin J, Shen Q, Cao Y, Li ZP, Li FZ, Chen XW, Sun LH, Jia JJ, Wu JC. Satellite-to-ground quantum key distribution. Nature. 2017 Sep 7.

<https://doi.org/10.1038/nature23655>

The above paper itself requires subscription, but its preprint can be accessed at:

[https://arxiv.org/pdf/1707.00542](https://arxiv.org/pdf/1707.00542%20)