Quantum Communication

OPTI646 (FALL'23)

SUBMITTED BY SIDDHARTH VATS

Why?

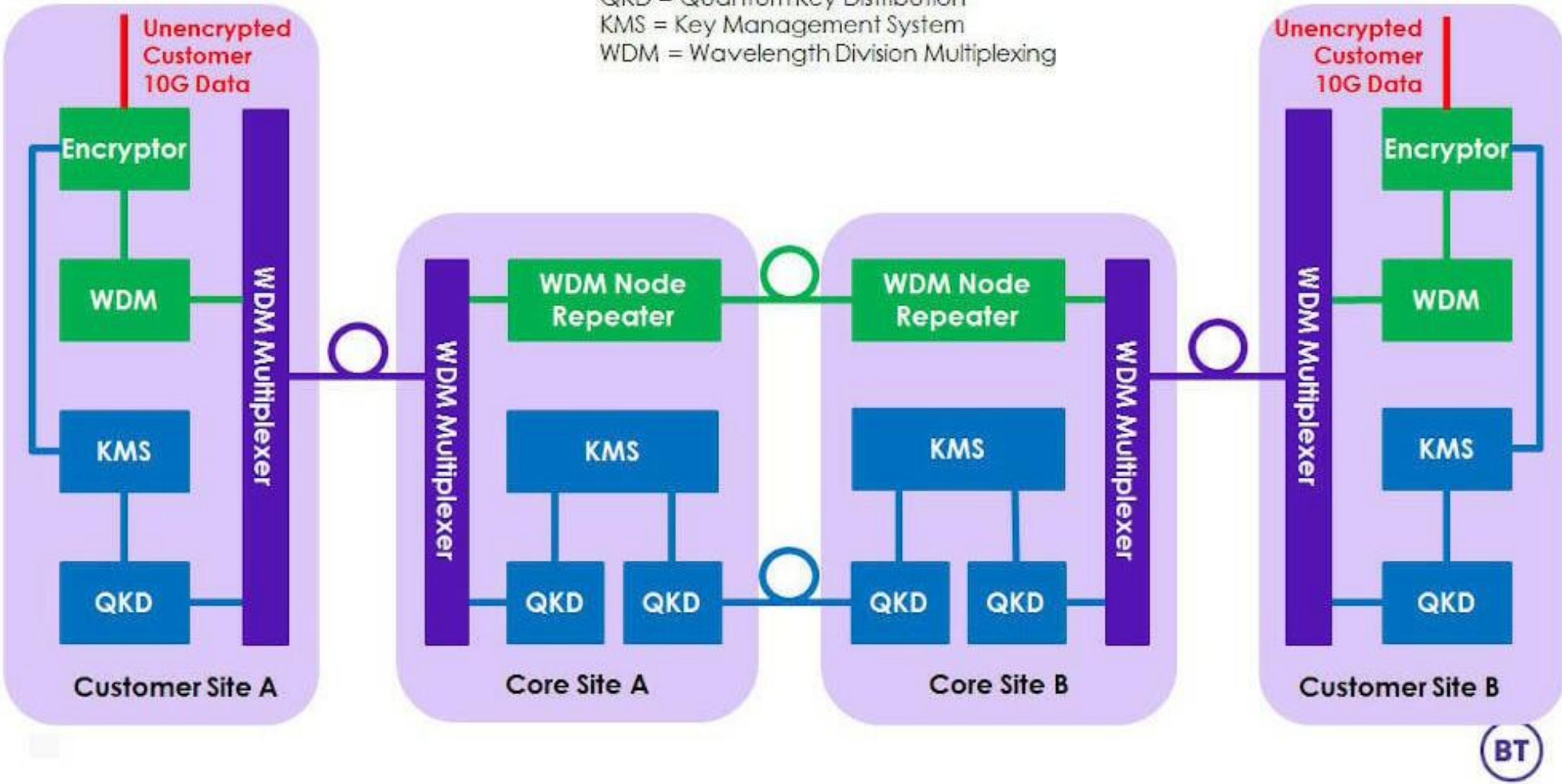
- Quantum information through a quantum channel
  - Exchange of quantum information (information processing)
- Classical information through a quantum channel
  - Quantum key distribution
    - (Quantum) random number generator – Aspect experiment #3
    - Creation of (classical) bit key
    - Encoding onto quantum states
    - Quantum communication
    - decoding

Testbed 1: London **MAN**

- Toshiba (technology) and British Telecom (infrastructure)
- First commercially available QKD as a service
- Store now-crack later: loss of confidence in convention data security
- Quantum and classical channel
- Short distance links: no repeaters
- Decoy states

Design Details

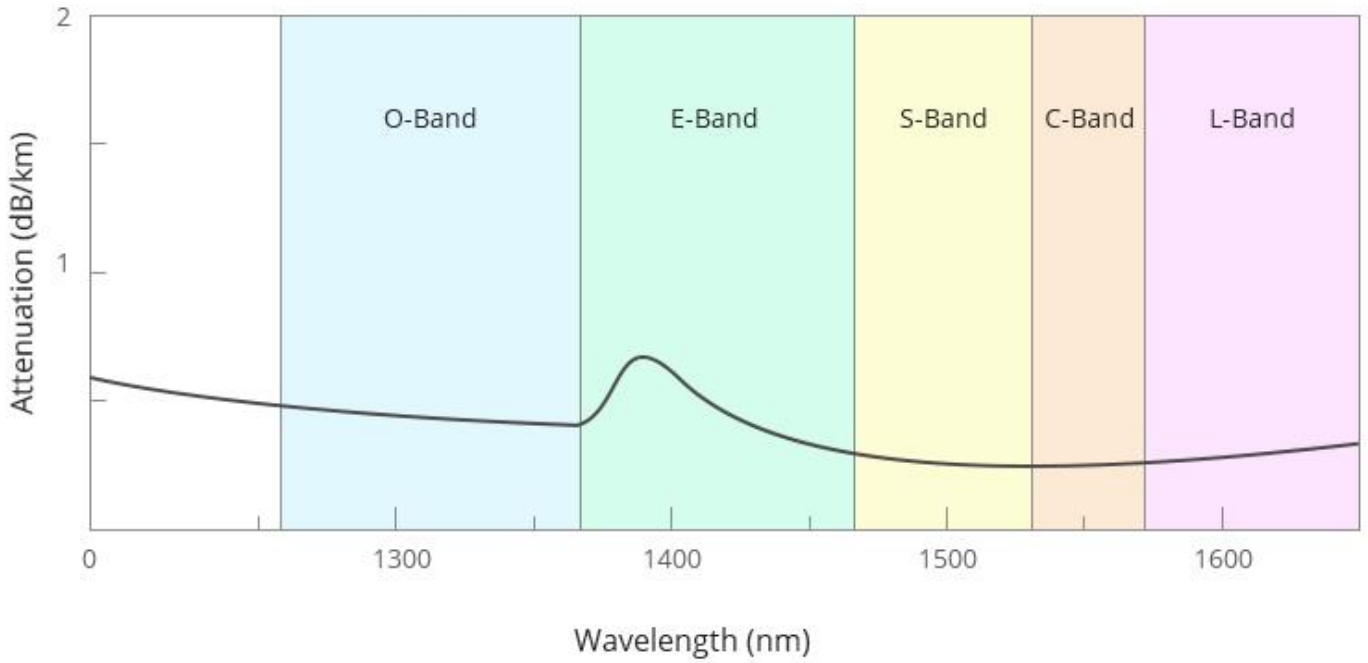
QKD = Quantum Key Distribution
KMS = Key Management System
WDM = Wavelength Division Multiplexing



BT

Coexistence with telecom

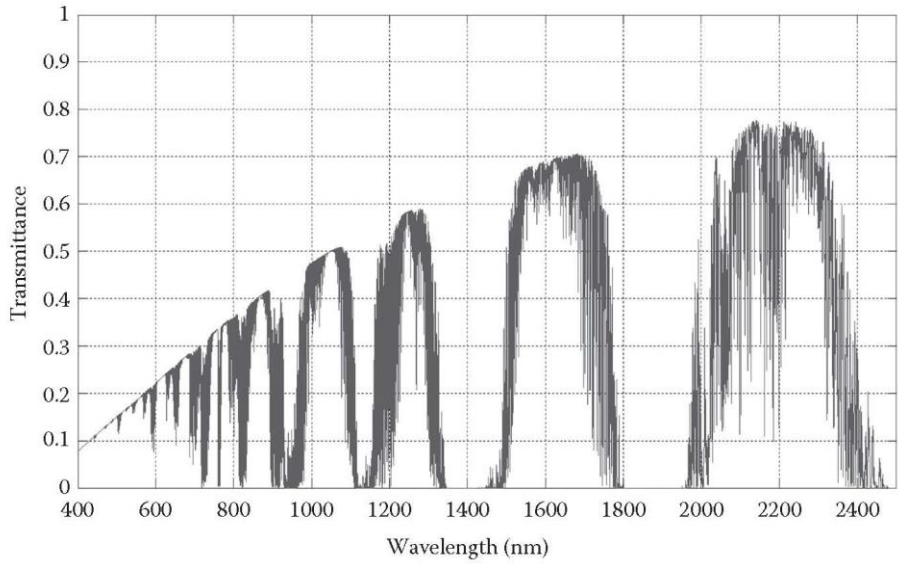
- Inherently incompatible with classical amplifiers
  - {reason}
- Absorption: transmit multiphoton pulses instead of single photon
  - PNS
    - Decoy states
- Scattering (Raman and Rayleigh)
  - Reduce power of classical signal
  - isolate quantum signal > 200nm (O and C band)
  - Time slotting (compatible with PON)
  - Separate fibre/ core
  - Hollow core fibre

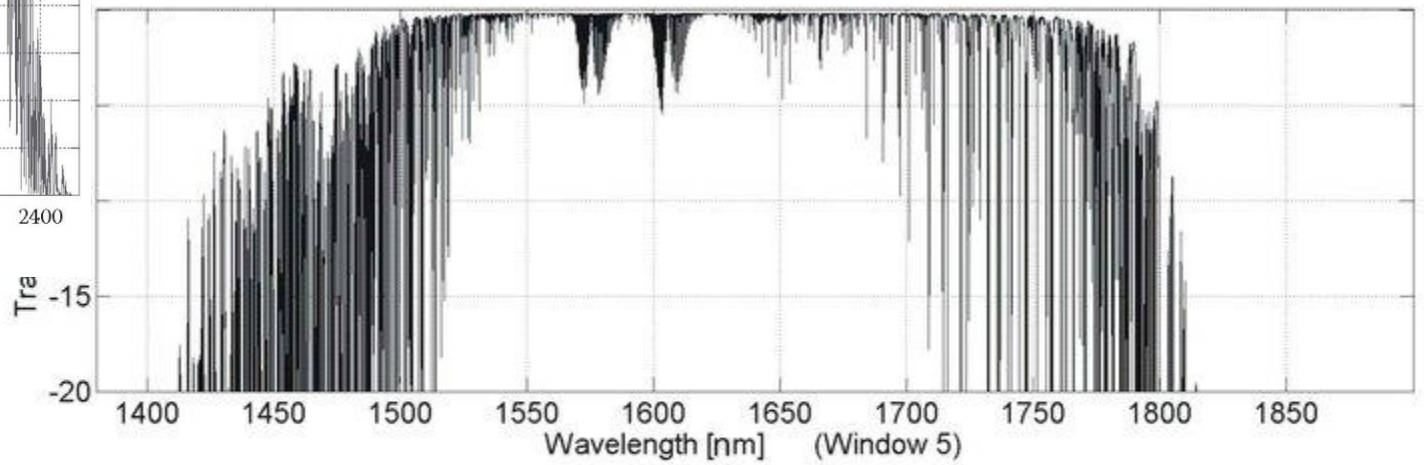


Testbed 2: Great China Network

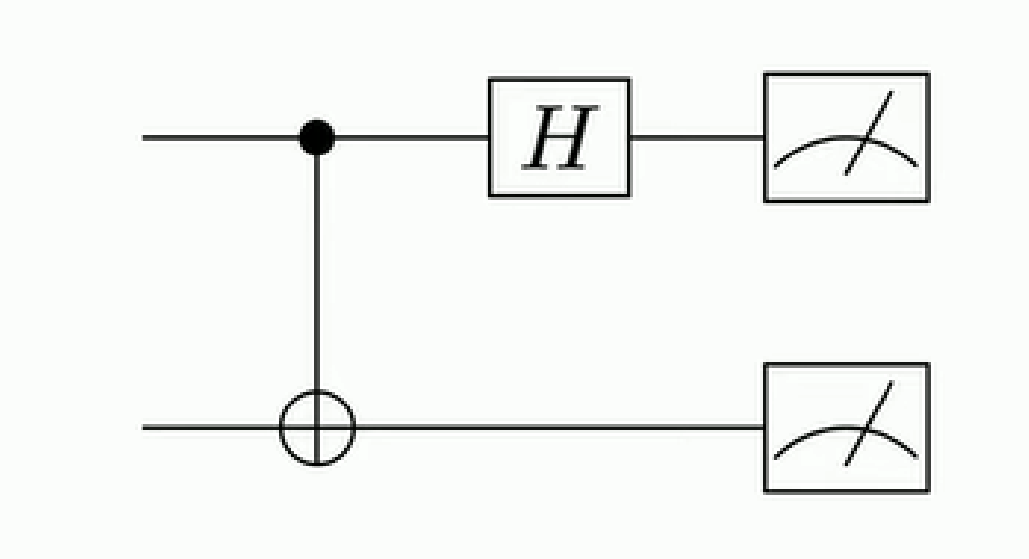
- 4 QMAN connected through optical and satellite communication links through a 4600km long network
- Micius: satellite communication
- Layered quantum network architecture
- Key management system
- Trusted node

Atmospheric Transmission





Bell State Measurement



Measurement outcome	Bell state
00	$\|\Phi^+\rangle$
01	$\|\Psi^+\rangle$
10	$\|\Phi^-\rangle$
11	$\|\Psi^-\rangle$

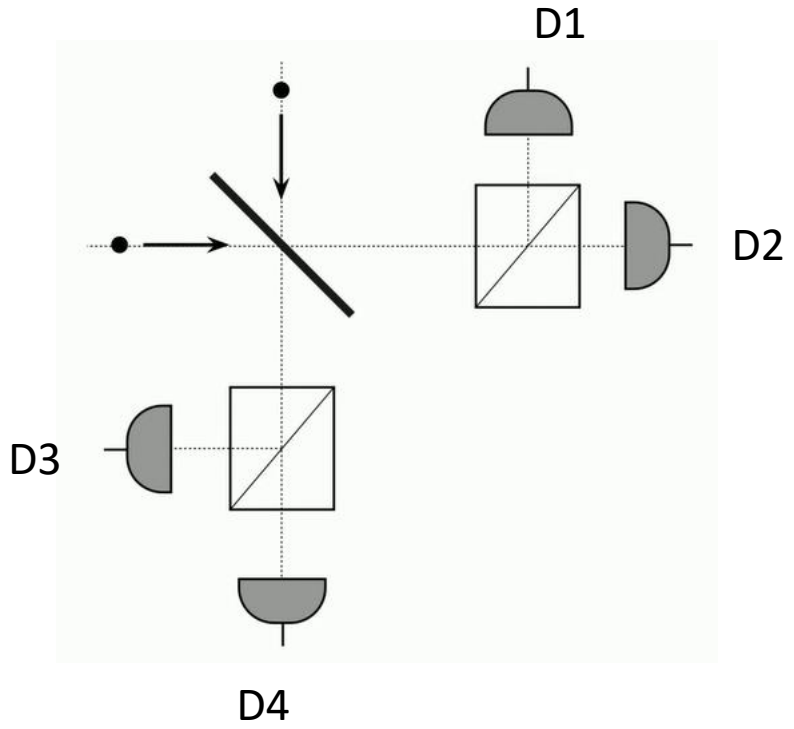
Bell State Measurement

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

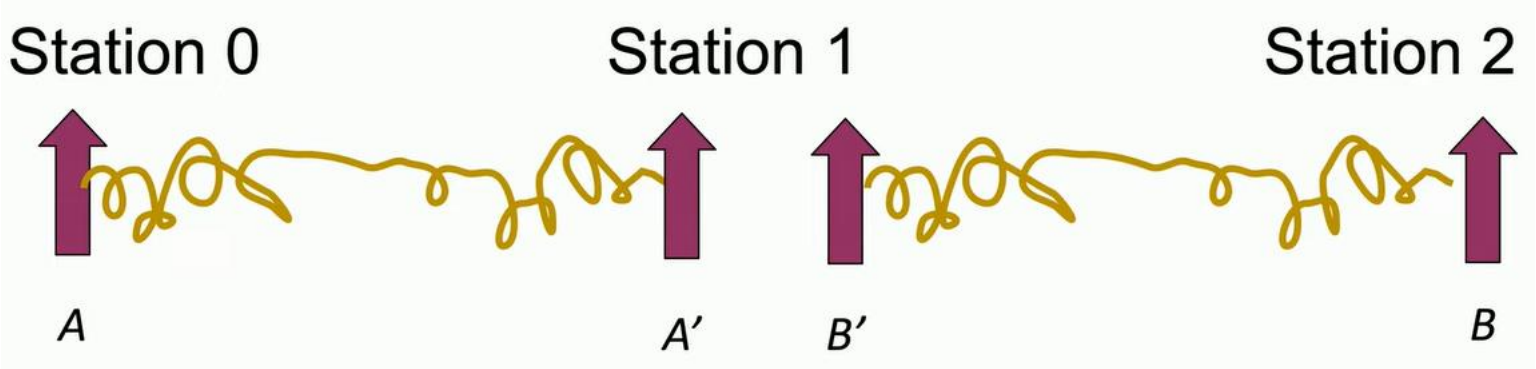
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



Repeaters

- Quantum to classical to quantum conversion (trusted node)
- OR
- Quantum entanglement swapping (quantum repeater)
  - Quantum Memory: time & fidelity
- OR
- Error correction (quantum repeater)

Entanglement Swapping



Entanglement Swapping

$$|00\rangle = \left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right)/\sqrt{2}$$
$$|01\rangle = \left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle\right)/\sqrt{2}$$
$$|10\rangle = \left(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle\right)/\sqrt{2}$$
$$|11\rangle = \left(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle\right)/\sqrt{2}$$

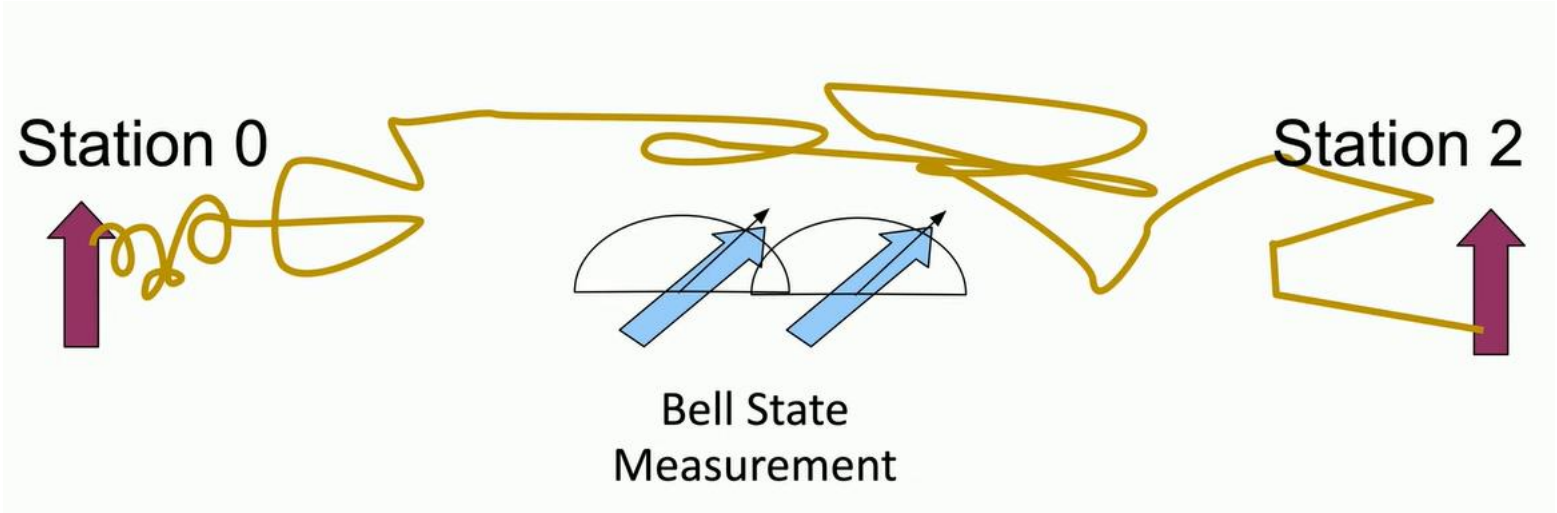
Entanglement Swapping

$$
\begin{aligned}
|\psi\rangle &= \left|\Phi^{+}\right\rangle_{AA'} |\Phi+\rangle_{B'B} \\
&= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) \\
&= \frac{1}{2\sqrt{2}}\left(|0\rangle\left(\left|\Phi^{+}\right\rangle + \left|\Phi^{-}\right\rangle\right)|0\rangle\right. \\
&+ \qquad |0\rangle\left(\left|\Psi^{+}\right\rangle + \left|\Psi^{-}\right\rangle\right)|1\rangle \\
&+ \qquad |1\rangle\left(\left|\Psi^{+}\right\rangle - \left|\Psi^{-}\right\rangle\right)|0\rangle \\
&+ \qquad \left.|1\rangle\left(\left|\Phi^{+}\right\rangle - \left|\Phi^{-}\right\rangle\right)|1\rangle\right)
\end{aligned}
$$

Entanglement Swapping

$$
\begin{aligned}
|\psi\rangle_{A'B'AB} = \frac{1}{2\sqrt{2}} (& \left|\Phi^{+}\right\rangle (|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) \\
& + \left|\Psi^{+}\right\rangle (|0\rangle\,|1\rangle + |1\rangle\,|0\rangle) \\
& + \left|\Psi^{-}\right\rangle (|0\rangle\,|1\rangle - |1\rangle\,|0\rangle) \\
& + \left|\Phi^{-}\right\rangle (|0\rangle\,|0\rangle - |1\rangle\,|1\rangle))
\end{aligned}
$$

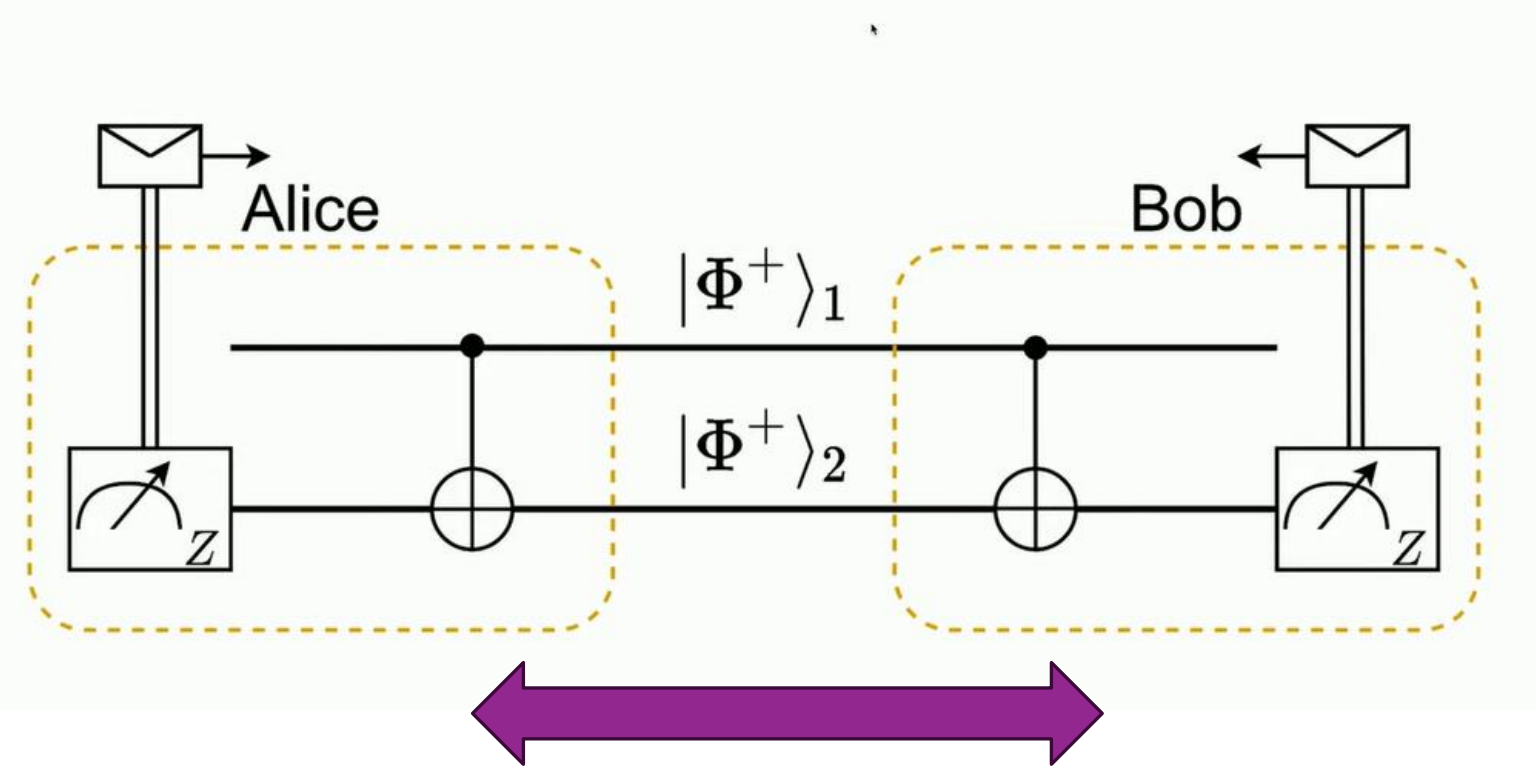
Entanglement Swapping



Purification

$$
\begin{aligned}
\left|\Phi^{+}\right\rangle_1 \left|\Phi^{+}\right\rangle_2 &= (|00\rangle + |11\rangle)(|00\rangle + |11\rangle) \\
&= |00\rangle\,|00\rangle + |00\rangle\,|11\rangle + |11\rangle\,|00\rangle + |11\rangle\,|11\rangle \\
&\xrightarrow{\mathrm{CNOT}_A} |00\rangle\,|00\rangle + |00\rangle\,|11\rangle + |11\rangle\,|10\rangle + |11\rangle\,|01\rangle \\
&\xrightarrow{\mathrm{CNOT}_B} |00\rangle\,|00\rangle + |00\rangle\,|11\rangle + |11\rangle\,|00\rangle + |11\rangle\,|11\rangle \\
&= \left|\Phi^{+}\right\rangle_1 \left|\Phi^{+}\right\rangle_2
\end{aligned}
$$

Purification



Purification

Pair 1	Pair 2	Prob.	Meas. Result	Agree?	Action	Result
$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	F^2	00 or 11	Y	Keep	$\|\Phi^+\rangle$
$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	$F(1-F)$	01 or 10	N	Discard	—
$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	$F(1-F)$	01 or 10	N	Discard	—
$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$(1-F)^2$	00 or 11	Y	Keep	$\|\Psi^+\rangle$

Succeeds w/ probability $F^2 + (1-F)^2$

Output fidelity is $$F' = \frac{F^2}{F^2 + (1-F)^2}$$

$$F' > F \text{ when } F > 0.5$$

Entanglement swapping

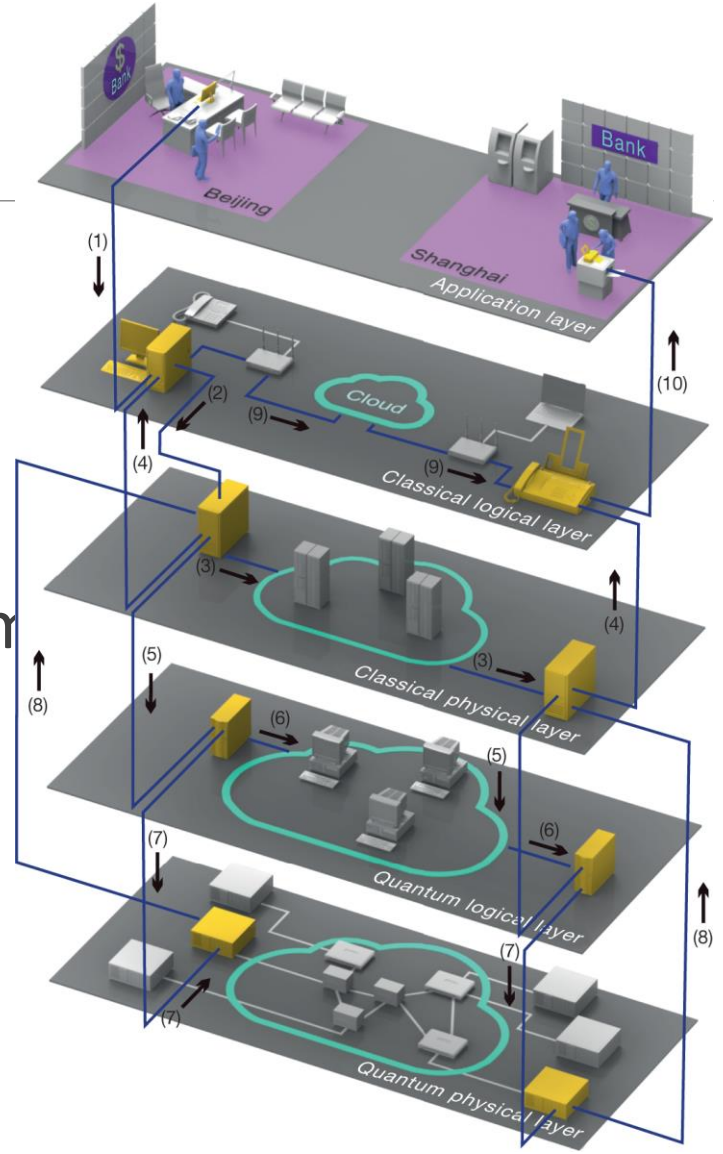
- Requirement of quantum memory: long storage and high fidelity
- scheduling

Quantum Network Architecture

- 5 layered QKD
  - Application: quantum protocol
  - Transport: end-to-end entanglement
  - Network: entanglement over a route
  - Link: entanglement over individual links
  - Physical: generation of physically entangled pairs

Quantum KMS

- User request for key
- Request forwarded to KMS
- Key generation request to quanum server
- Request forwarded to quantum control system
- Finding the best route for key generation
- Key generation
- encryption



Testbed 3: South Korea

- ID Quantique (technology) and SK Telecom (infrastructure)
- 48 sites connected over a 2000km network for QSN
- Quantum safe as a service
- SDN
- BB84

Testbed 4: Spain

- Huawei (technology), Telefonica (infrastructure)
- Continuous variable
- SDN

Continuous Variable

- Quadrature
- Measurement
- Telecom compatible
- Deterministic (guaranteed signal)

Discrete Variable

- Signal generation (attenuate laser or quantum dot)
- Decoy state: send multiple pulses with multiple photons, if there's an eve, a detection will change the statistics at Bob
- detection (photon counter: APD)
  - Single/ Dual rail qubit
  - Polarization: horizontal/ vertical
  - Time-bin: early/ late
- Established (some what), benifited by photonic integrated circuits
- Telecom incompatible
- Not deterministic (photon generation not guaranteed)
- Key rate: 50,000 256 keys/sec i.e. multiple users can be connected

Bibliography

- Chen, YA., Zhang, Q., Chen, TY. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8
- Martin, V., Brito, J.P., Escribano, C. *et al.* Quantum technologies in the telecommunications industry. *EPJ Quantum Technol.* **8**, 19 (2021).
- Hlér Kristjánsson, Robert Gardner and Giulio Chiribella. Quantum Communications Report for Ofcom
- Report of the DOE Quantum Internet Blueprint Workshop, Feb (2020)
- Overview of Quantum Communications, Q-leap Edu Quant Communications
- BT and Toshiba to build world's first commercial quantum-secured metro network across London. Newsroom, British Telecom Oct (2021)
- IDQ and SK Broadband complete phase one of nation-wide Korean QKD Network. IDQuantuque.com
- Telefónica, Huawei and UPM perform a groundbreaking field trial applying quantum cryptography on commercial optical networks to provide secure communication services. Newsroom, Telefonics