FIRST INTERNATIONAL
QUANTUM COMMUNICATION CONCLAVE
Organized by TEC, C-DOT and TSDSI
in technical collaboration with
IEEE Communications Society
Delhi Chapter

Building a Quantum Network

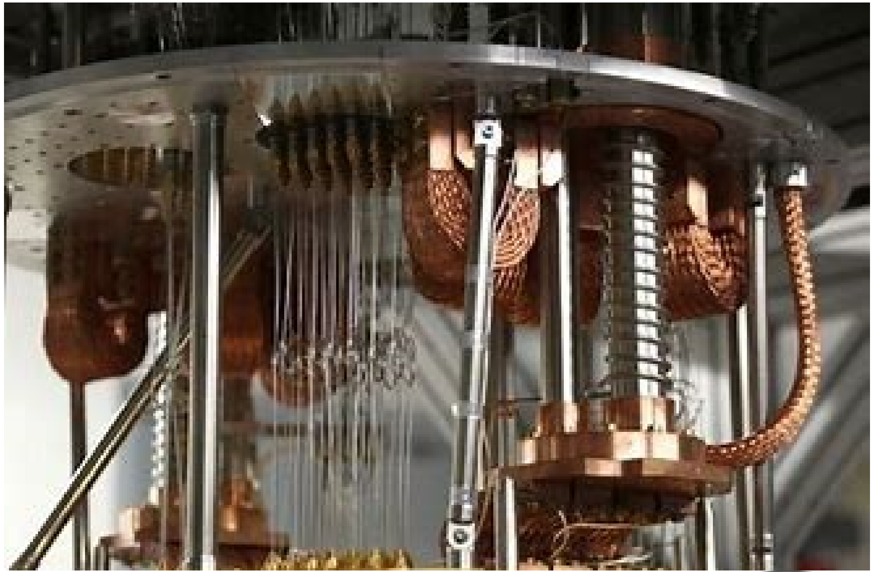
Suma Varughese

OS & Director General (MED & CoS), DRDO

Revolution Eras

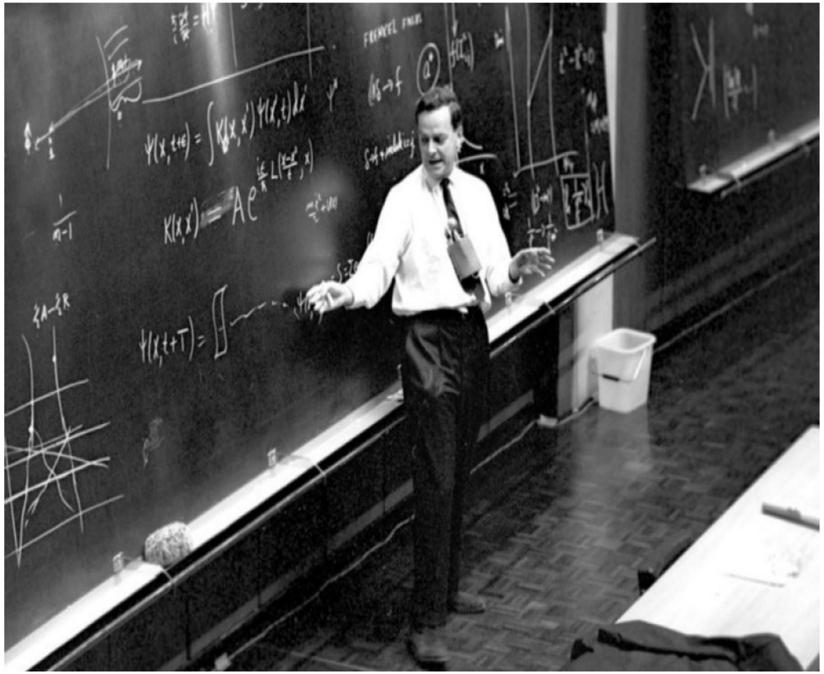
19th: Machine Age

20th: Information Age



21st: Quantum Age

The connection to Quantum Computing

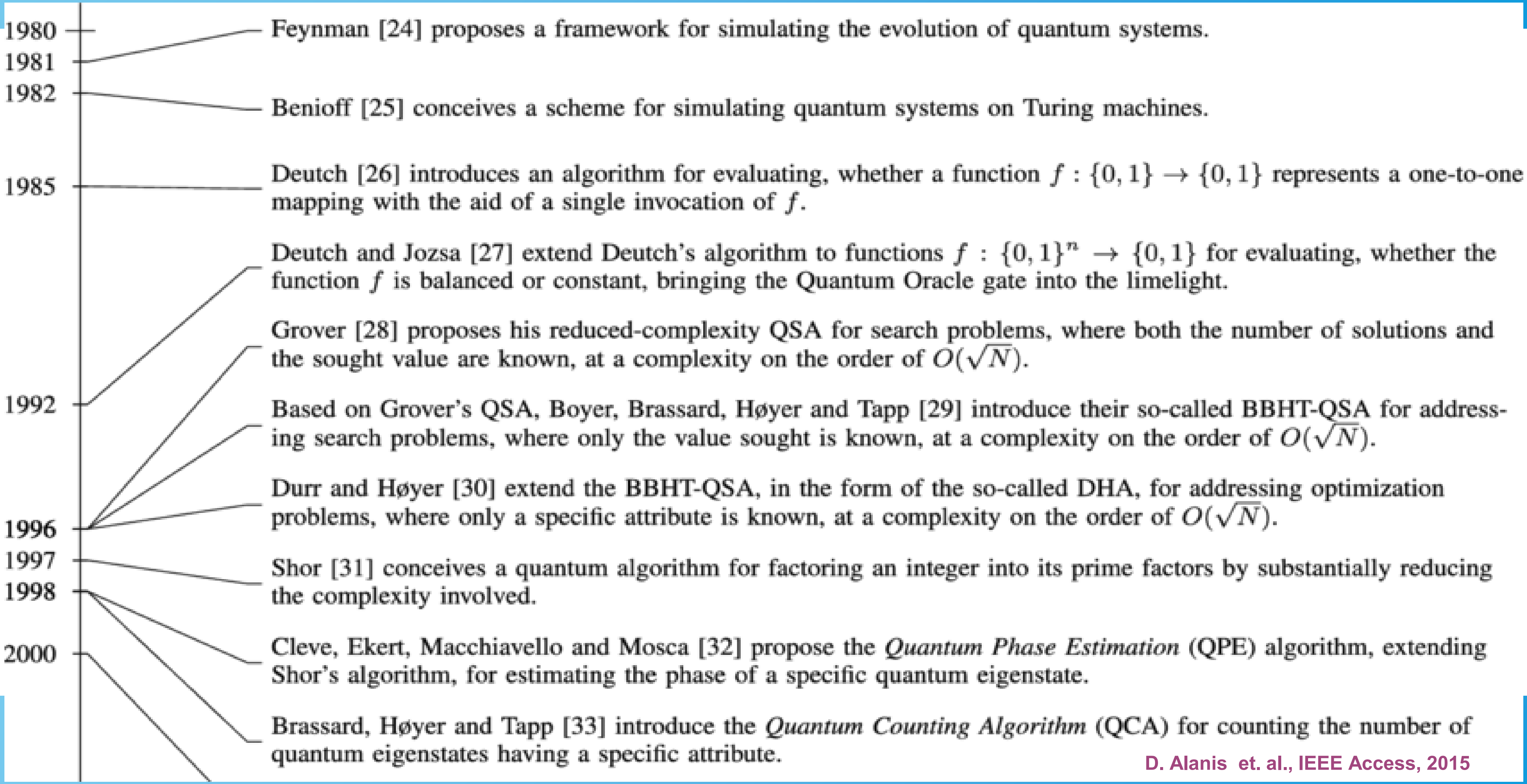


Feynman in 1982 proposed using quantum mechanical phenomena to perform calculations that would be impractical or impossible using classical computers.

This idea was later developed into the field of quantum computing.

Feynman's ideas and work continue to influence the field of quantum computing, and he is often considered one of the founders of the entire field.

Timeline of quantum computing milestones



Feynman [24] proposes a framework for simulating the evolution of quantum systems.

Benioff [25] conceives a scheme for simulating quantum systems on Turing machines.

Deutch [26] introduces an algorithm for evaluating, whether a function $f : \{0,1\} \rightarrow \{0,1\}$ represents a one-to-one mapping with the aid of a single invocation of f.

Deutch and Jozsa [27] extend Deutch's algorithm to functions $f : \{0,1\}^n \rightarrow \{0,1\}$ for evaluating, whether the function f is balanced or constant, bringing the Quantum Oracle gate into the limelight.

Grover [28] proposes his reduced-complexity QSA for search problems, where both the number of solutions and the sought value are known, at a complexity on the order of $O(\sqrt{N})$.

Based on Grover's QSA, Boyer, Brassard, Høyer and Tapp [29] introduce their so-called BBHT-QSA for addressing search problems, where only the value sought is known, at a complexity on the order of $O(\sqrt{N})$.

Durr and Høyer [30] extend the BBHT-QSA, in the form of the so-called DHA, for addressing optimization problems, where only a specific attribute is known, at a complexity on the order of $O(\sqrt{N})$.

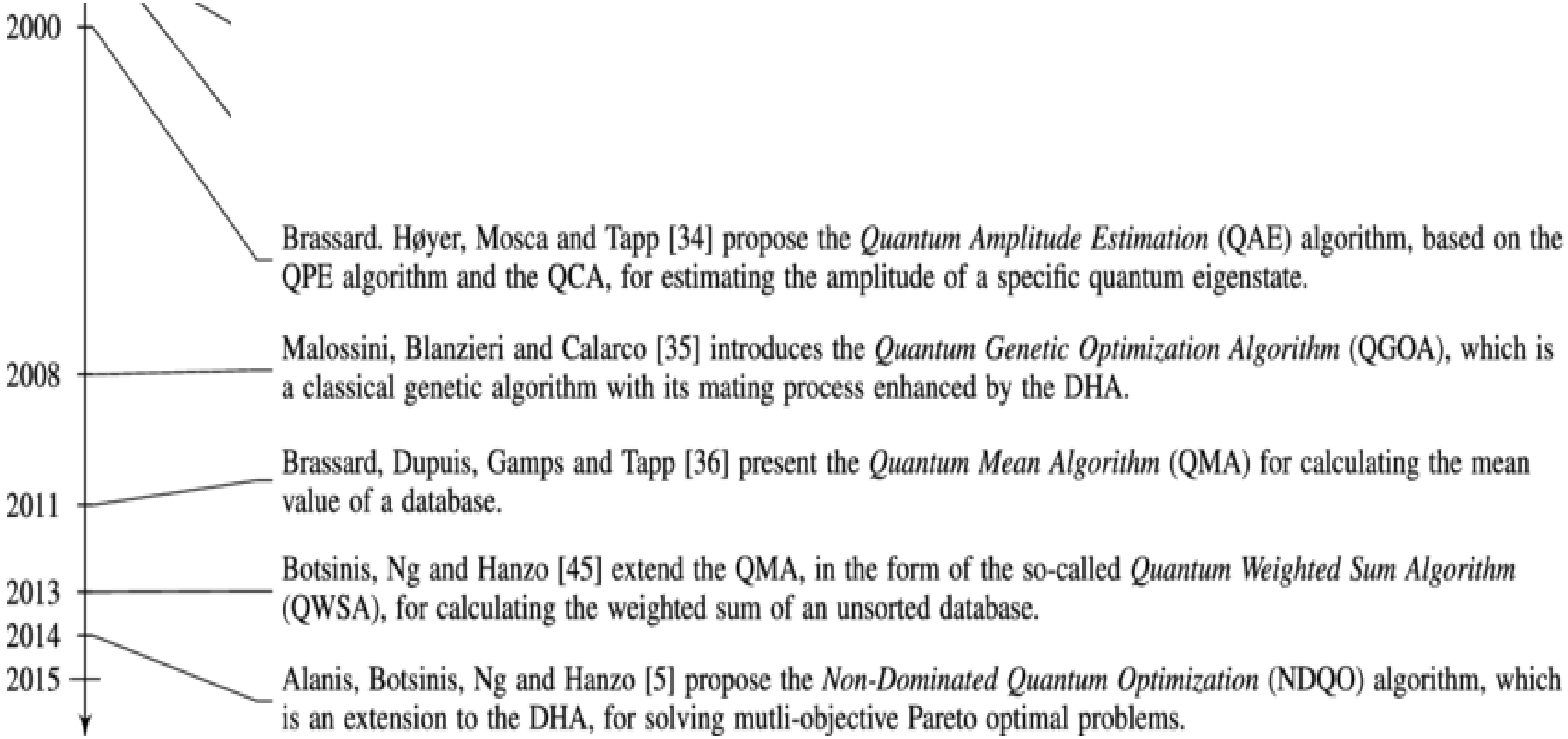
Shor [31] conceives a quantum algorithm for factoring an integer into its prime factors by substantially reducing the complexity involved.

Cleve, Ekert, Macchiavello and Mosca [32] propose the *Quantum Phase Estimation* (QPE) algorithm, extending Shor's algorithm, for estimating the phase of a specific quantum eigenstate.

Brassard, Høyer and Tapp [33] introduce the *Quantum Counting Algorithm* (QCA) for counting the number of quantum eigenstates having a specific attribute.

D. Alanis et. al., IEEE Access, 2015

Timeline of quantum computing milestones



Brassard. Høyer, Mosca and Tapp [34] propose the *Quantum Amplitude Estimation* (QAE) algorithm, based on the QPE algorithm and the QCA, for estimating the amplitude of a specific quantum eigenstate.

Malossini, Blanzieri and Calarco [35] introduces the *Quantum Genetic Optimization Algorithm* (QGOA), which is a classical genetic algorithm with its mating process enhanced by the DHA.

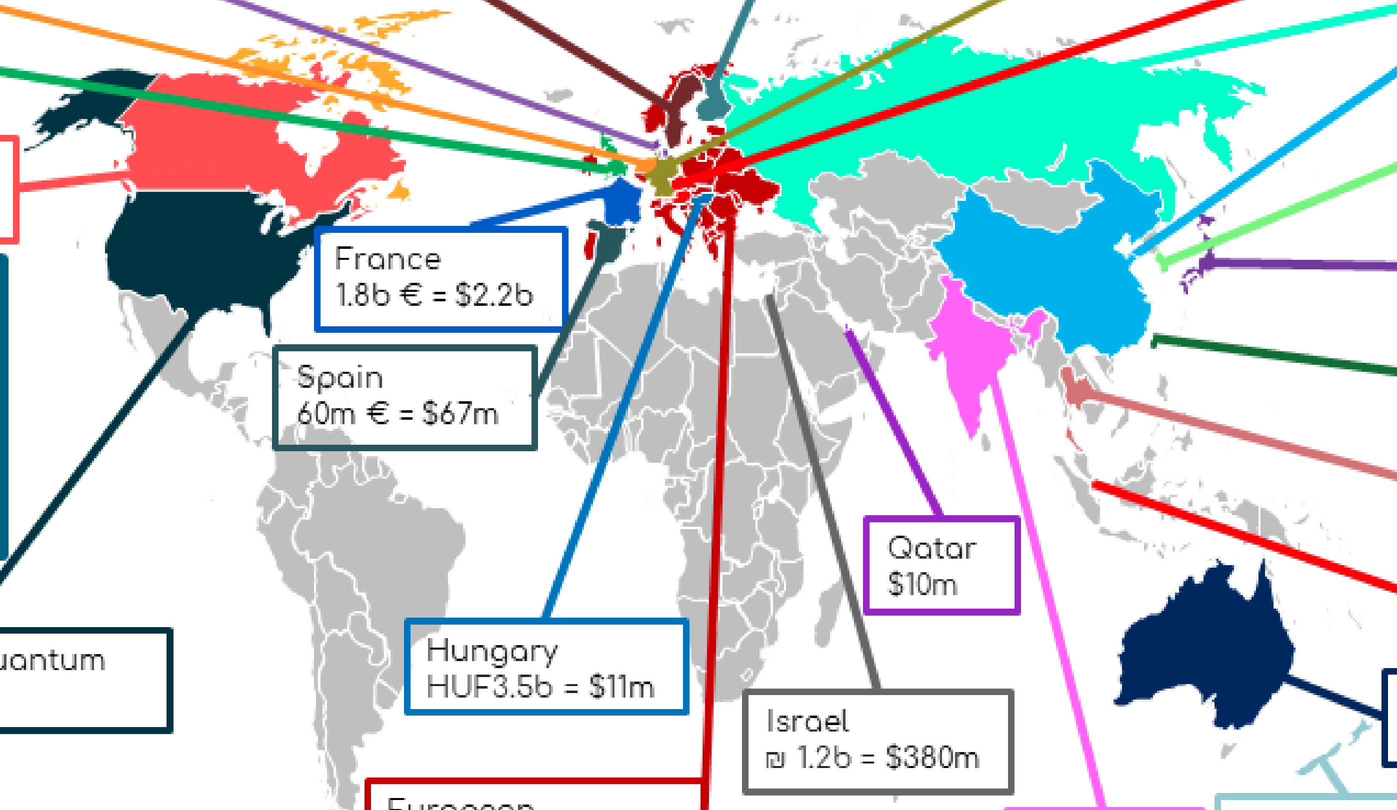
Brassard, Dupuis, Gamps and Tapp [36] present the *Quantum Mean Algorithm* (QMA) for calculating the mean value of a database.

Botsinis, Ng and Hanzo [45] extend the QMA, in the form of the so-called *Quantum Weighted Sum Algorithm* (QWSA), for calculating the weighted sum of an unsorted database.

Alanis, Botsinis, Ng and Hanzo [5] propose the *Non-Dominated Quantum Optimization* (NDQO) algorithm, which is an extension to the DHA, for solving mutli-objective Pareto optimal problems.

D. Alanis et. al., IEEE Access, 2015

Worldwide Quantum Efforts



Netherlands
765m € = $904m

Denmark
DKK230 = $34m

Sweden
SEK1.6b = $160m

Finland
24m € = $27m

Germany
2.6b € = $3.1b

Austria
107m € = $127m

Russia
₽50b = $663m

United Kingdom
£1b = $1.3b

China
$15b

Canada
CA$1.37b = $1.1b

South Korea
₩44.5b = $40m

France
1.8b € = $2.2b

Japan
¥80b = $700m

Global effort 2022 $30b (estimate)

Spain
60m € = $67m

Taiwan
NT$8b = $282m

Thailand
฿200m = $6m

Qatar
$10m

Singapore
S$150m = $109m

US National Quantum Initiative $1.2b

Hungary
HUF3.5b = $11m

Australia
AU$130m = $98.5m

Israel
₪ 1.2b = $380m

European Quantum Flagship
1b € = $1.1b

India
₹73b = $1b

New Zealand
$36.75m

Quantum Warfare utilizing various Quantum Technology Systems

Quantum Race

- Europe launched a $1 billion quantum computing research project, Quantum Flagship, in 2016, and its member states have started building a quantum communications infrastructure that will be operational by 2027.

- In like vein, China's 14th Five Year Plan (2021-2025) prioritizes the development of quantum computing and communications by 2030.
- In all, between 2019 and 2021 China invested as much as $11 billion.
- Europe had spent $5 billion, the U.S. $3 billion, and the U.K. around $1.8 billion between to become tomorrow's quantum superpowers.

- Fortune

Quantum Communication

- Today, sensitive data is typically encrypted and then sent across fibre-optic cables and other channels together with the digital "keys" needed to decode the information.

- The data and the keys are sent as classical bits—a stream of electrical or optical pulses representing 1s and 0s. And that makes them vulnerable.

- Smart hackers can read and copy bits in transit without leaving a trace.

Quantum Communication

- Quantum communication takes advantage of the laws of quantum physics to protect data

- These laws allow particles—typically photons of light for transmitting data along optical cables—to take on a state of superposition, which means they can represent multiple combinations of 1 and 0 simultaneously.

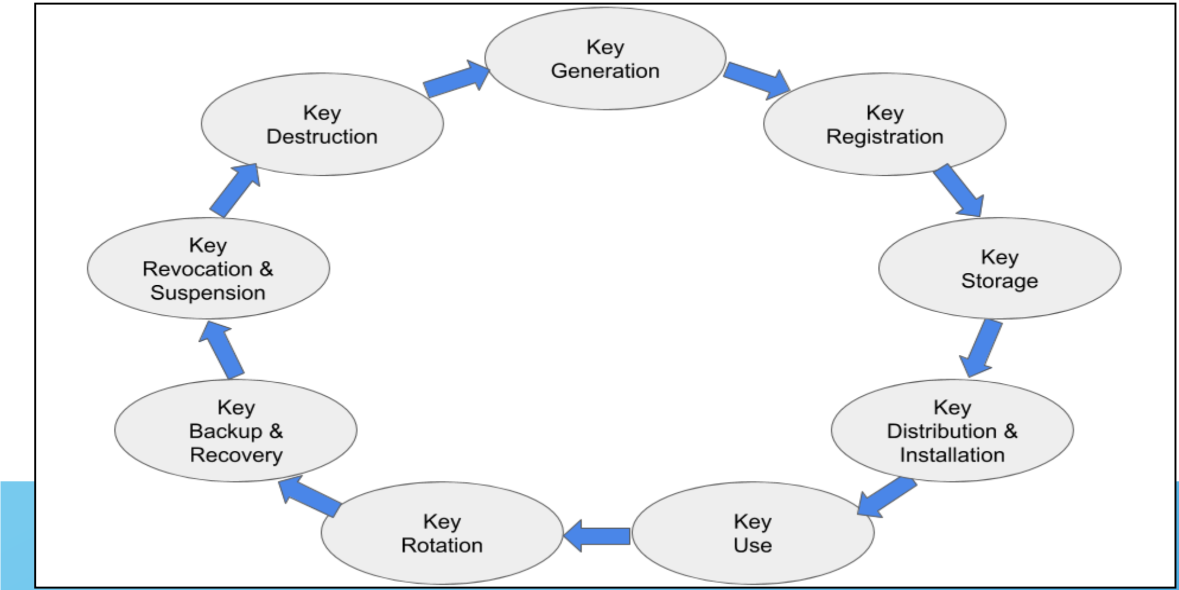
- The beauty of qubits from a cybersecurity perspective is that if a hacker tries to observe them in transit, their super-fragile quantum state "collapses" to either 1 or 0.

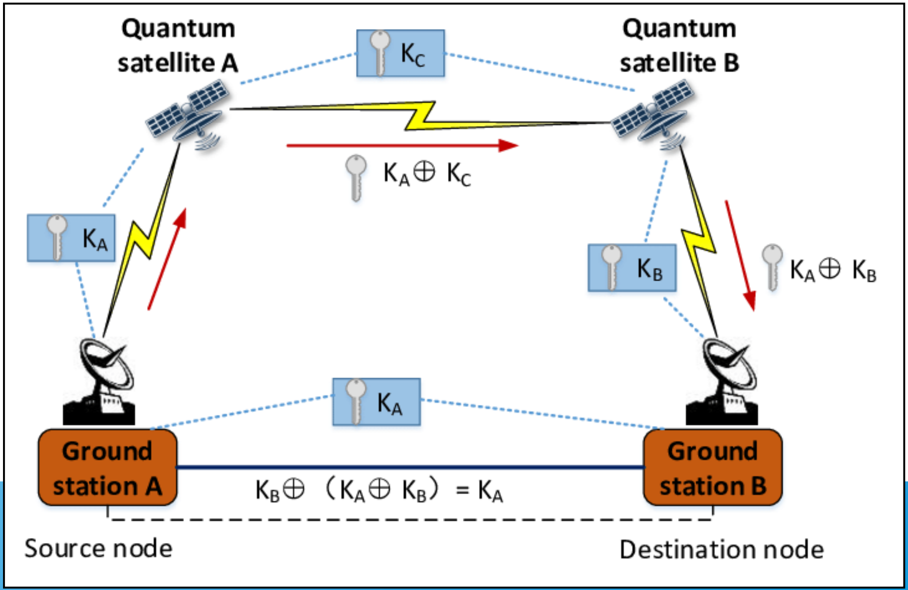
- This means a hacker can't tamper with the qubits without leaving behind a telltale sign of the activity.

Quantum Key Distribution (QKD)

Usage scenarios

- Tactical key distribution for encryption during conflicts or wars
- Key sharing between ground stations and satellites for encryption
- Key sharing between satellites for encryption and mutual authentication

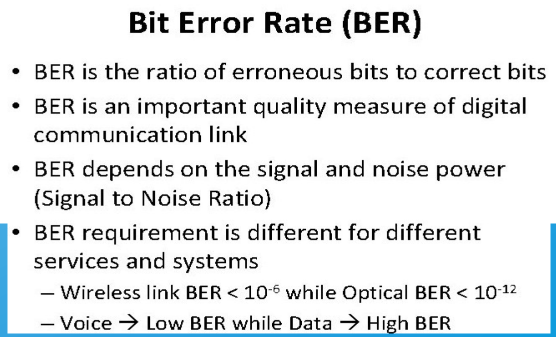




Quantum Key Distribution (QKD)

Working assumptions

a) Any attempt at snooping of photon streams would introduce errors, due to non-clonability.
b) Errors are estimated from a correlation of states of photons reaching the detector with those at the time of leaving the source.
c) Errors could be due to snooping attempts or channel noise, but both are treated as due to snooping.
d) Quantum Bit Error Rate (QBER) or Surviving Decoy Rate (Visibility) are used to decide on accepting or discarding a key-sharing round.
e) Concept of privacy amplification based on QBER estimates is sufficient to cover for the leakage of key information due to snooping.



Bit Error Rate (BER)

- BER is the ratio of erroneous bits to correct bits
- BER is an important quality measure of digital communication link
- BER depends on the signal and noise power (Signal to Noise Ratio)
- BER requirement is different for different services and systems
  – Wireless link BER < 10^{-6} while Optical BER < 10^{-12}
  – Voice → Low BER while Data → High BER

Components of Quantum Network

- ✓ Source: Single Photon Source
- ✓ Detection: Single Photon Detector
- ✓ Quantum Memory
- ✓ Quantum Interface

There parameters directly limit the performance of quantum communication system

Quantum Networks

a) Photonic qubits are preferred thanks to their resilience

b) Networks for quantum computations

- ❖ The case is similar to that of classical parallel computation
- ❖ Qubits need to be transported for short distances
- ❖ Custom quantum channels are required
- ❖ Optical switches need to preserve coherence
- ❖ Quantum teleportation could be an option too

c) Networks for quantum communications

- ❖ Main application is Quantum Key Distribution (QKD)
  - For key sharing for secure communications
- ❖ Qubits need to be transported over long distances (> 1000s of Kms)
- ❖ Existing telecom fibre infrastructure to be used as an option

Typical Architecture and Components of QKD

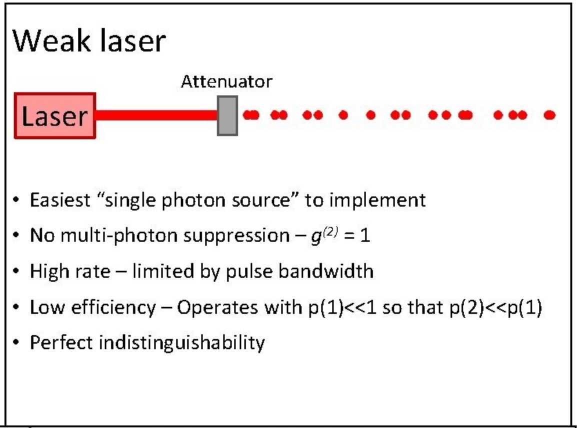
Sources

a) Coherent weak pulses

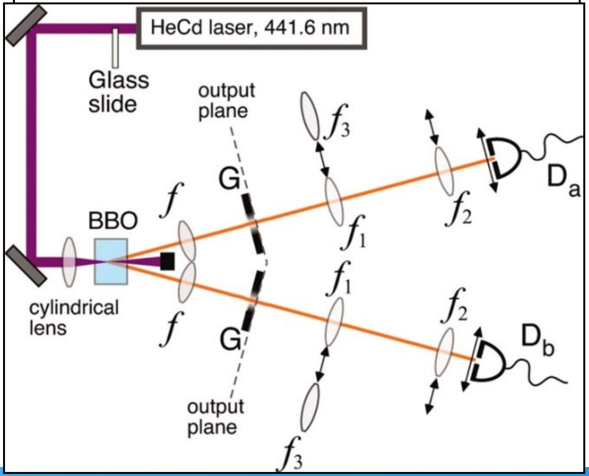
- Pulses are forged out of continuous laser beams; no. of photons per pulse follow the Poisson distribution with a mean, λ, of 0.2
- Low λ is chosen to minimise multi-photon pulses; True RNG required at source

b) Entangled pairs of photons

- Created from a stream of photons passing through a non-linear crystal; the process is called spontaneous parametric down conversion (SPDC)
- Of each pair one photon travels to the sender and the other one to the receiver
- The entangled pair creates true random key string at the time of measurements at the end points


Weak laser

- Easiest "single photon source" to implement
- No multi-photon suppression – $g^{(2)} = 1$
- High rate – limited by pulse bandwidth
- Low efficiency – Operates with p(1)<<1 so that p(2)<<p(1)
- Perfect indistinguishability



Typical Architecture and Components of QKD

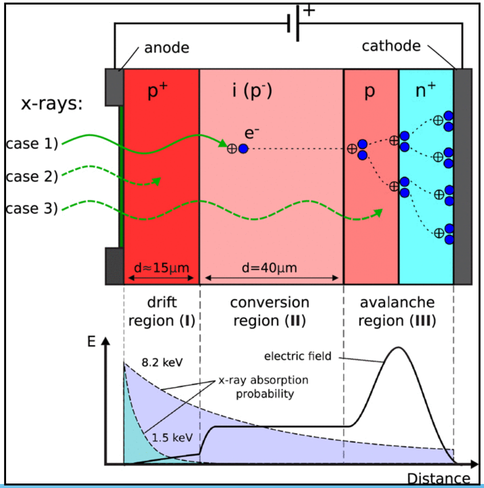
Detectors

a) Avalanche Photo Diodes (APDs) are the inexpensive option, but with low efficiency of around 10 %;

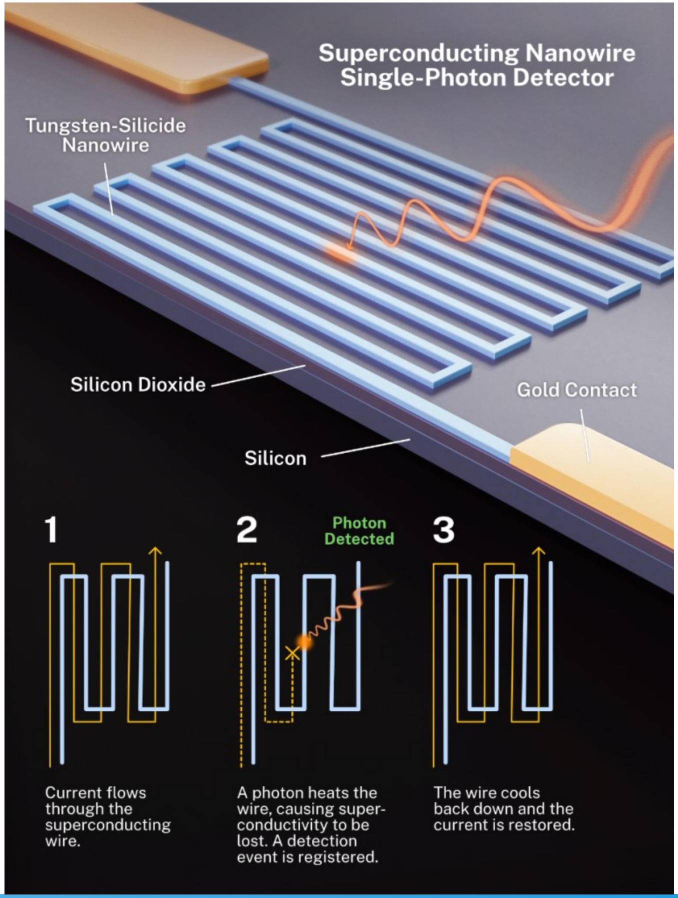
b) Superconducting Nanowire Single Photon Detectors (SNSPD) are the latest option with around 90 % efficiency

Stray photons and dark counts have to be minimized

APD



SNSPD



1 Current flows through the superconducting wire.

2 A photon heats the wire, causing super-conductivity to be lost. A detection event is registered.

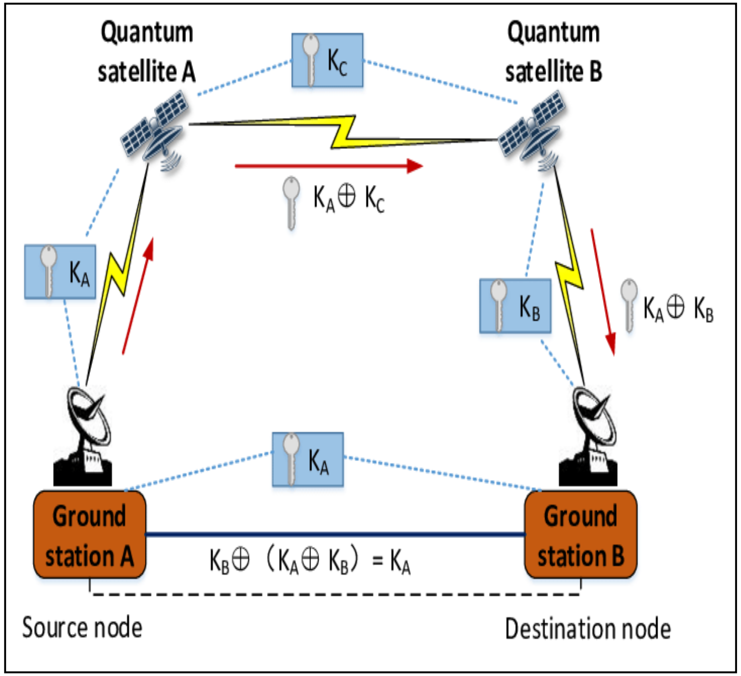
3 The wire cools back down and the current is restored.

Quantum Networks

Networks for quantum communications

Technologies for quantum communications

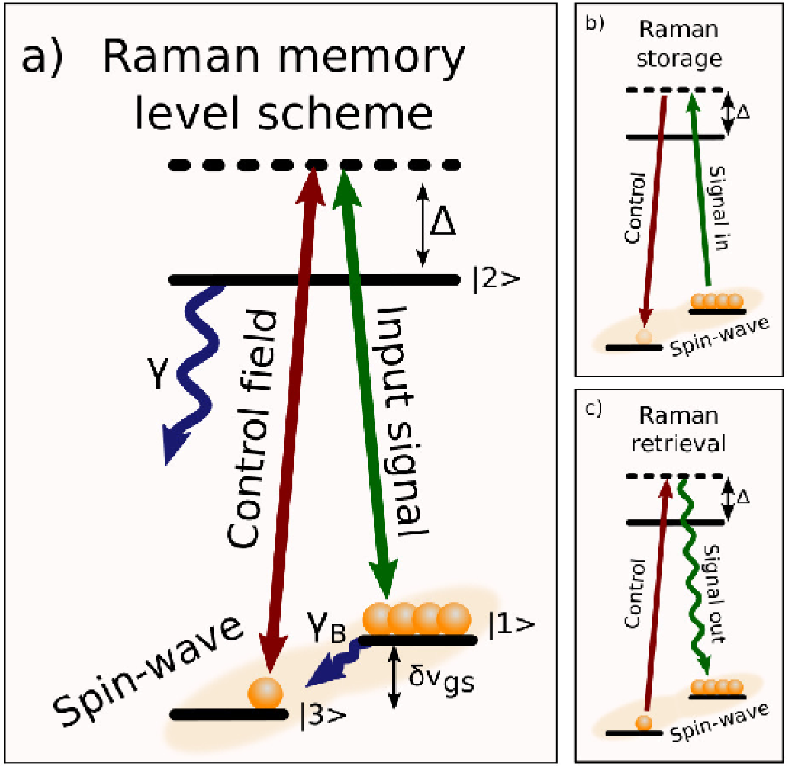
- Over fibre the range is limited to about 100-150 Kms
- Options to extend the range over fibre
  - Dark fibre (a limited and costly option)
  - Trusted repeaters using satellites (See figure on the right)
  - Quantum repeaters – require quantum memory
- Free space transport is another option
  - Line of Sight – for limited range
  - Via satellites – for long range
- Inter-satellite secure communications



Quantum Memories and Repeaters

Quantum memory options

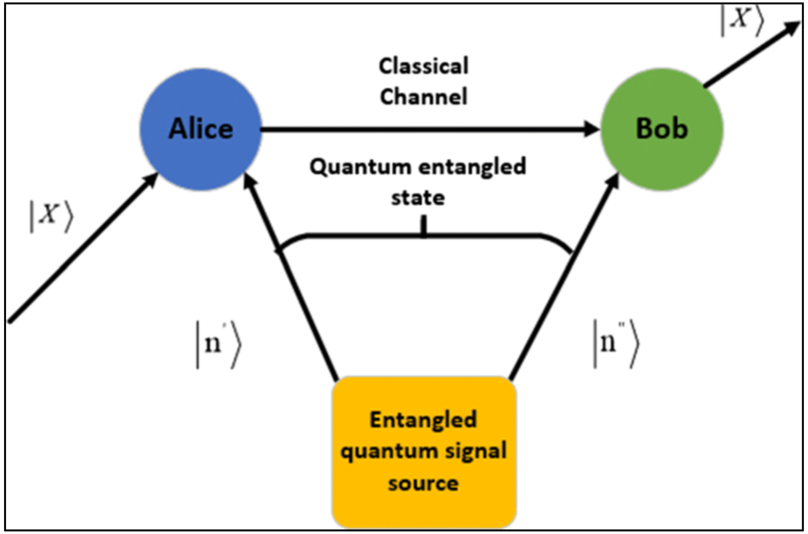
1) The concept – Transfer or absorption, and release later (See figure on the right)
    - Into solids (Ion-doped, NV centres)
    - Atomic gases (of Rubidium)
2) Performance criteria
    - Efficiency (Absorption cross-section)
    - Storage time (ms to s)
    - Fidelity (Coherence and alignment)
    - Speed of operation or bandwidth
3) Very exploratory stage



Quantum Memories and Repeaters

Quantum repeaters

1) Makes use of entangled photon pairs in one of the four Bell states: {|00> + |11>, |00> - |11>, |01> + |10>, |01> - |10>}
2) Needs quantum memory for short term storage at receiving end
3) Quantum teleportation to effect the transfer of |X> from Alice to Bob (See figure on the right)
4) Teleportation process: Alice combines |X> and |n′> and makes a Bell basis measurement. The outcome would be one of the four Bell states. This is communicated to BoB in two bits using a classical channel. Bob recovers |X> from |n″> and the two bits.
5) Highly exploratory stage



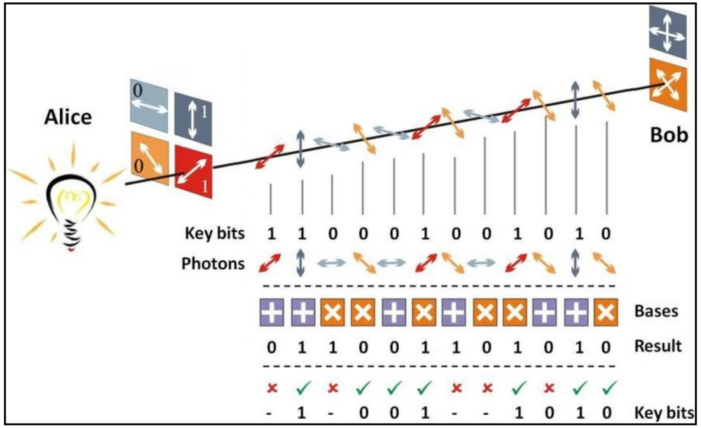
Two Top-level Protocols for QKD

Prepare-and-Measure method

a) Originally proposed by Bennet and Brassard in 1984; hence called the BB84

b) Uses a source of single photons that can be polarized to represent 0s and 1s; Mostly uses photons of 1550 nm wavelength

c) Now a number of variants have been proposed, both for fibre and free space QKD applications



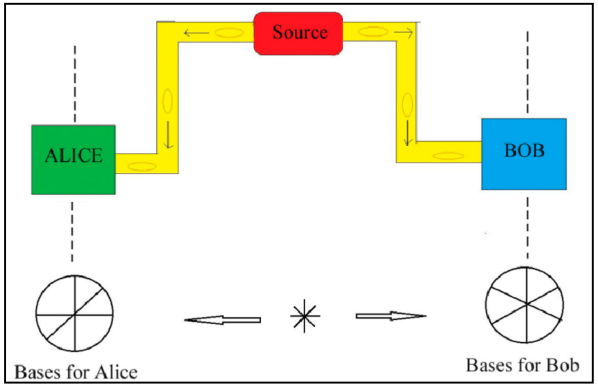
Key bits	1	1	0	0	0	1	0	0	1	0	1	0
Photons	↗	↕	↔	↘	↔	↗	↘	↔	↗	↘	↕	↘
Bases	+	+	×	×	+	×	+	×	×	+	+	×
Result	0	1	1	0	0	1	1	0	1	0	1	0
	×	✓	×	✓	✓	✓	×	×	✓	×	✓	✓
Key bits	-	1	-	0	0	1	-	-	1	0	1	0

Entanglement-based method

a) Originally proposed by A. Ekert in 1991; hence known as E91

b) Now a number of variants have been proposed, both for fibre and free space QKD applications

c) Does not need a True Random Number Generator (RNG) at source; hence source independent



Typical Architecture and Components of QKD

Electronics

a) Field Programmable Gate Arrays as computing core; Time stamping and synchronization devices to the accuracy of Pico seconds

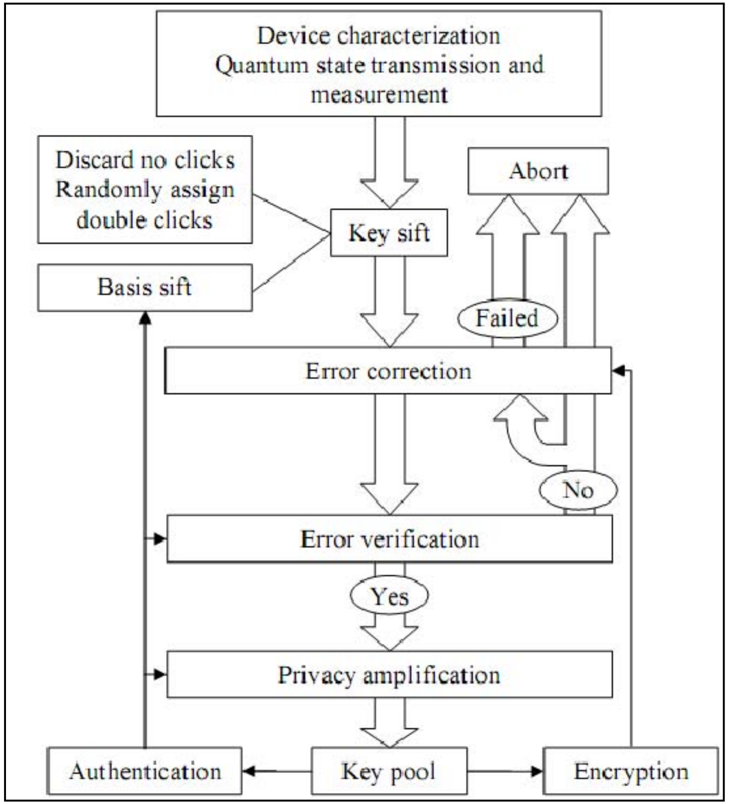
Key establishment software

a) Time synchronisation between the source and detector devices

b) Time correlation between detected photons and their release from the source, and raw key, R, extraction

c) Calculation QBER / Visibility and assessment of leakage; Establishment of pure key as K = fR, where the fraction f accounts for leakage and error correction

d) Privacy amplification for neutralising leakage; uses a reducing hash function



Challenges ahead of Quantum Networks

✓ Compatible co-existence

- ❖ The entanglement procedure is inherently probabilistic, due to the odds of losing a photon before it reaches the detectors.

- ❖ Processes leading to photon losses must therefore be minimised to increase the chances of success.

- ❖ To scale up the network, for example where the nodes are in different cities, light emitted by the NV centres must be compatible with existing telecom infrastructure.

- ❖ Quantum frequency conversion modules can be used to convert the emitted light into the telecom band.

Challenges ahead of Quantum Networks

✓ Timing is everything

- ❖Synchronisation is a crucial aspect of successful entanglement.

- ❖Timing requirements for emitted photons are very strict – the time difference between NV centres needs to be less than one nanosecond.

- ❖Maintaining synchronisation between nodes in a lab environment is challenging and over deployed fibre connections is even more complicated.

- ❖ Many technical solutions are needed to bring a large-scale quantum network, i.e., a quantum internet closer to reality, addressing both synchronisation and compatibility issues.

Challenges ahead of Quantum Networks

✓ Bridging the distance

- ❖ Another curve in the road comes from the fact that fundamentally single photons entangled with NV centres cannot be amplified. This limits the realisable entanglement rate – a lost photon cannot be recovered, instead, the process of generating entangled photons needs to be restarted. As the distance between the nodes increases, losing photons becomes more likely.

- ❖ To enable the transmission of qubits over long distances, work on developing quantum repeaters is needed. The main concept of a quantum repeater is to break up the long entanglement distance into smaller segments. Demonstrating the quantum repeater principle is a crucial milestone for paving the way to large-scale quantum networks.

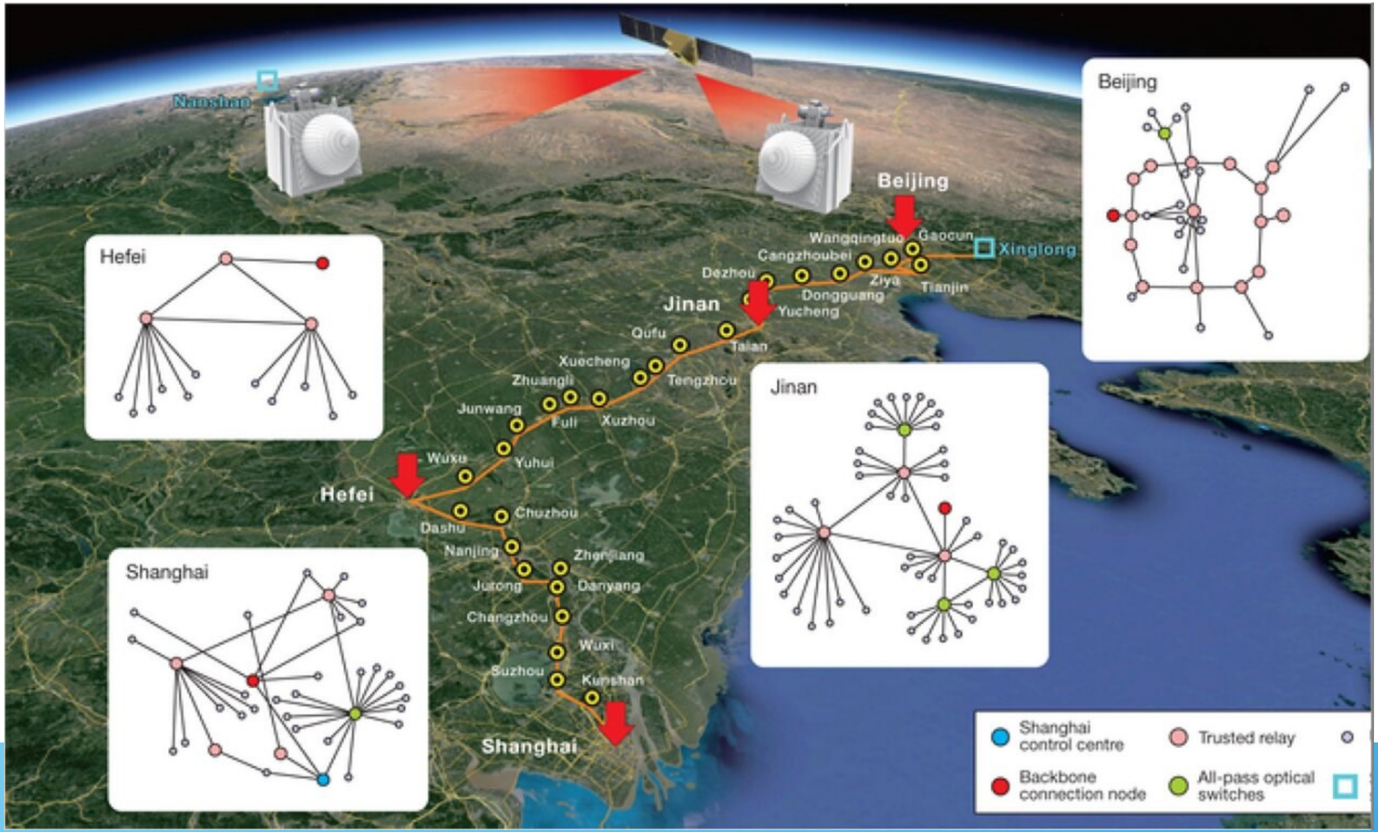
Quantum Enabler

Production & employment of high-performance quantum technologies are enabled by

Enabling Technology	Utility
Foundries	synthesize quantum systems from source materials
High-performance electronic, optical, mechanical & thermal Systems	control & isolation systems
Nano/micro-fabrication facilities	manufacture devices that integrate the control systems with the quantum systems
High-performance software stacks	to operate & apply quantum hardware
Benchmarking, testing & simulation facilities	to accelerate development & support user adoption
Quantum-ready workforce	specialist skills & experience

First integrated quantum communication network

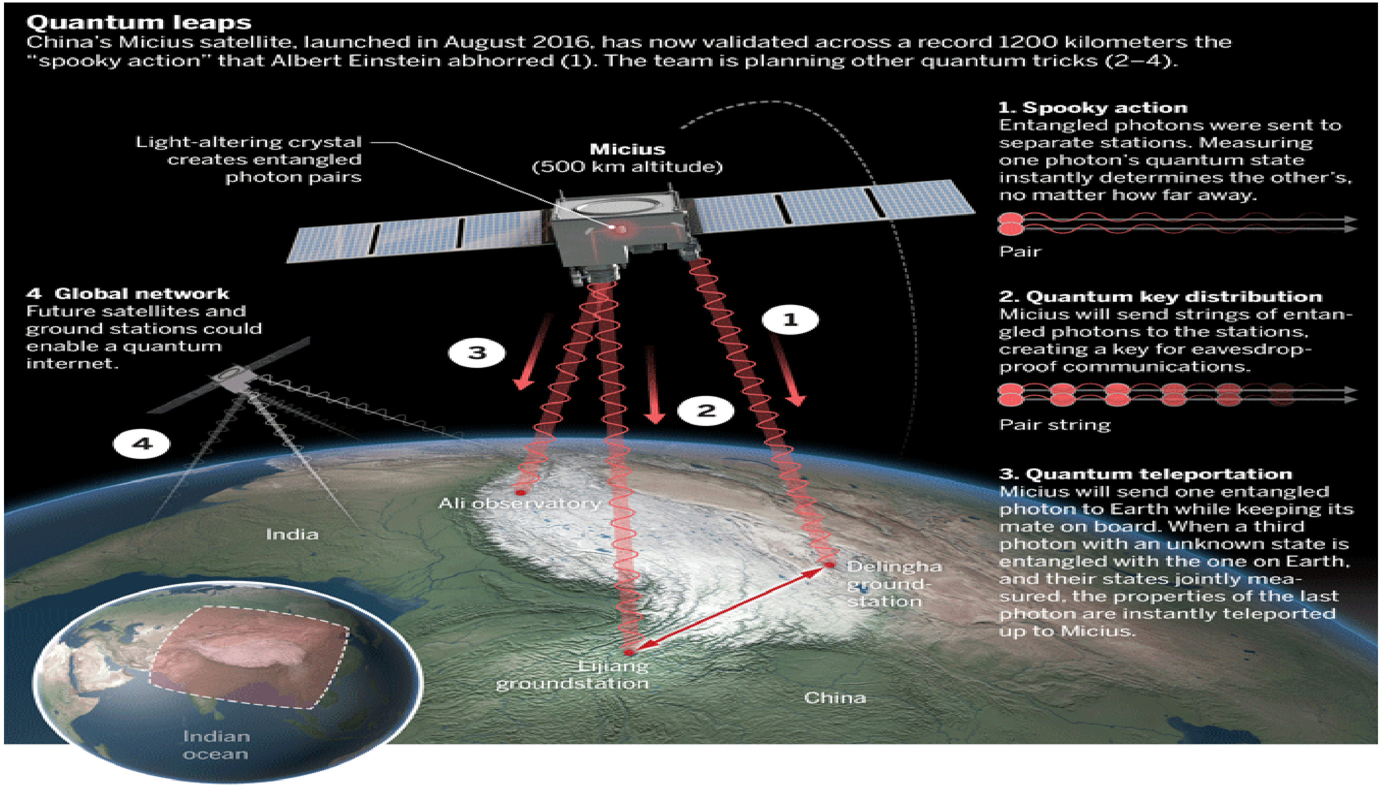
In September 2017, China inaugurated the first long-distance quantum communication landline in the world, connecting the capital city of China with the coastal city of Shanghai.



Over 700 optical fibers on the ground with two ground-to-satellite links to achieve quantum key distribution over a total distance of 4,600 kilometers for users across the country.

University of Science and Technology of China, Jan 2021

Pairs of entangled photons generated on board the Micius satellite are split up and then distributed by two bidirectional downlinks to two ground observatories in Delingha and Nanshan in China, which are separated by 756 miles (1,200 km).



Quantum leaps

China's Micius satellite, launched in August 2016, has now validated across a record 1200 kilometers the "spooky action" that Albert Einstein abhorred (1). The team is planning other quantum tricks (2–4).

Light-altering crystal creates entangled photon pairs

1. Spooky action
Entangled photons were sent to separate stations. Measuring one photon's quantum state instantly determines the other's, no matter how far away.

2. Quantum key distribution
Micius will send strings of entangled photons to the stations, creating a key for eavesdrop-proof communications.

3. Quantum teleportation
Micius will send one entangled photon to Earth while keeping its mate on board. When a third photon with an unknown state is entangled with the one on Earth, and their states jointly measured, the properties of the last photon are instantly teleported up to Micius.

4 Global network
Future satellites and ground stations could enable a quantum internet.

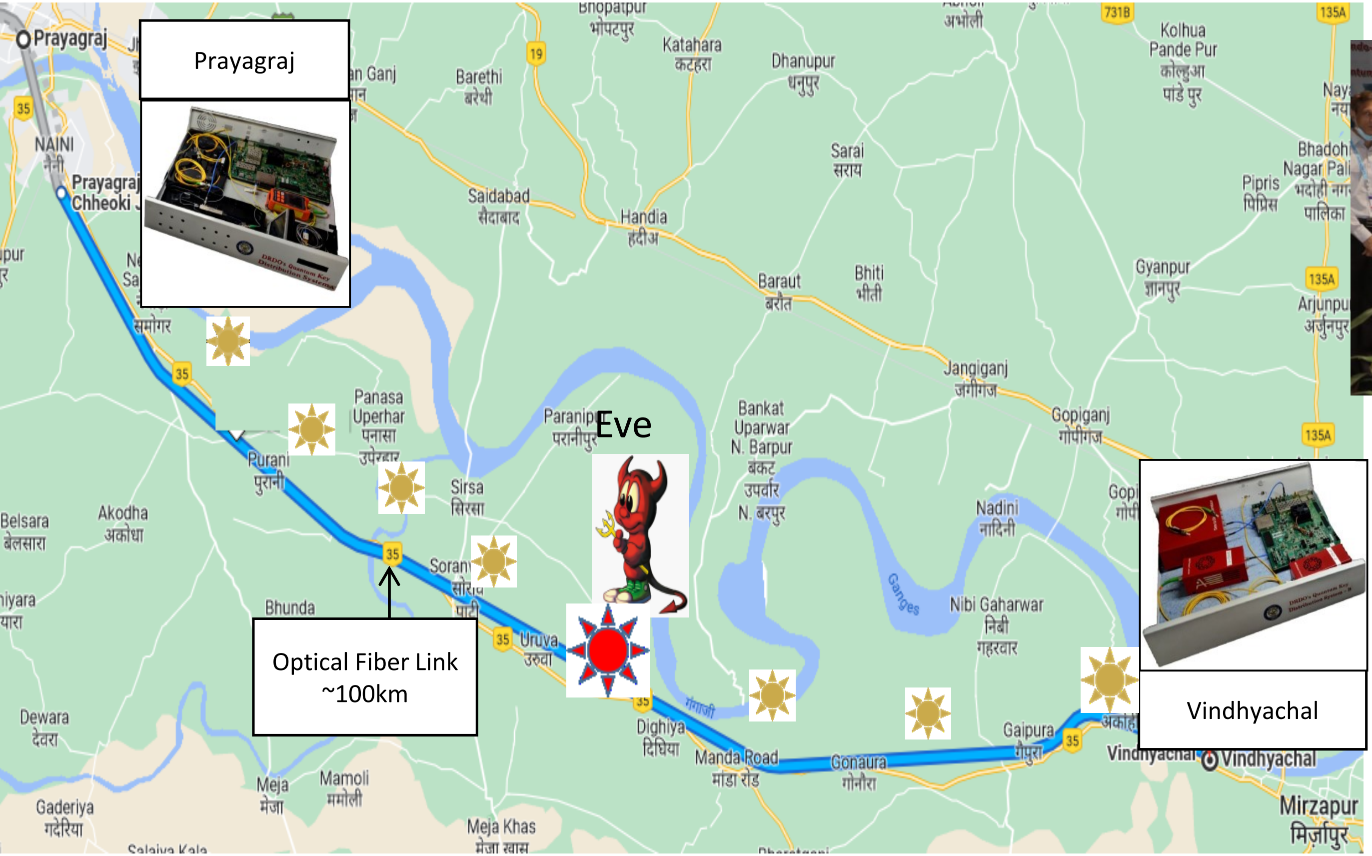
- ➢ The distance was increased from 62 miles (100 km) to 756 miles (1,200 km).
- ➢ That way, two remote points on Earth with greatly reduced channel loss because most of the photons' propagation path is in empty space with negligible loss and decoherence.

DRDO: Quantum Random Number Generator (QRNG)

- Applications: Classical & Quantum Cryptography, Encryption, Numerical methods, Simulations
- Achievements:
  i. In-house Prototype-I Development

  ii. ToT of Prototype-I to Industry

DRDO & IITD: Fiber-based QKD


Prayagraj

Eve

Optical Fiber Link
~100km

Vindhyachal

Field Testing *(Feb.'22)*

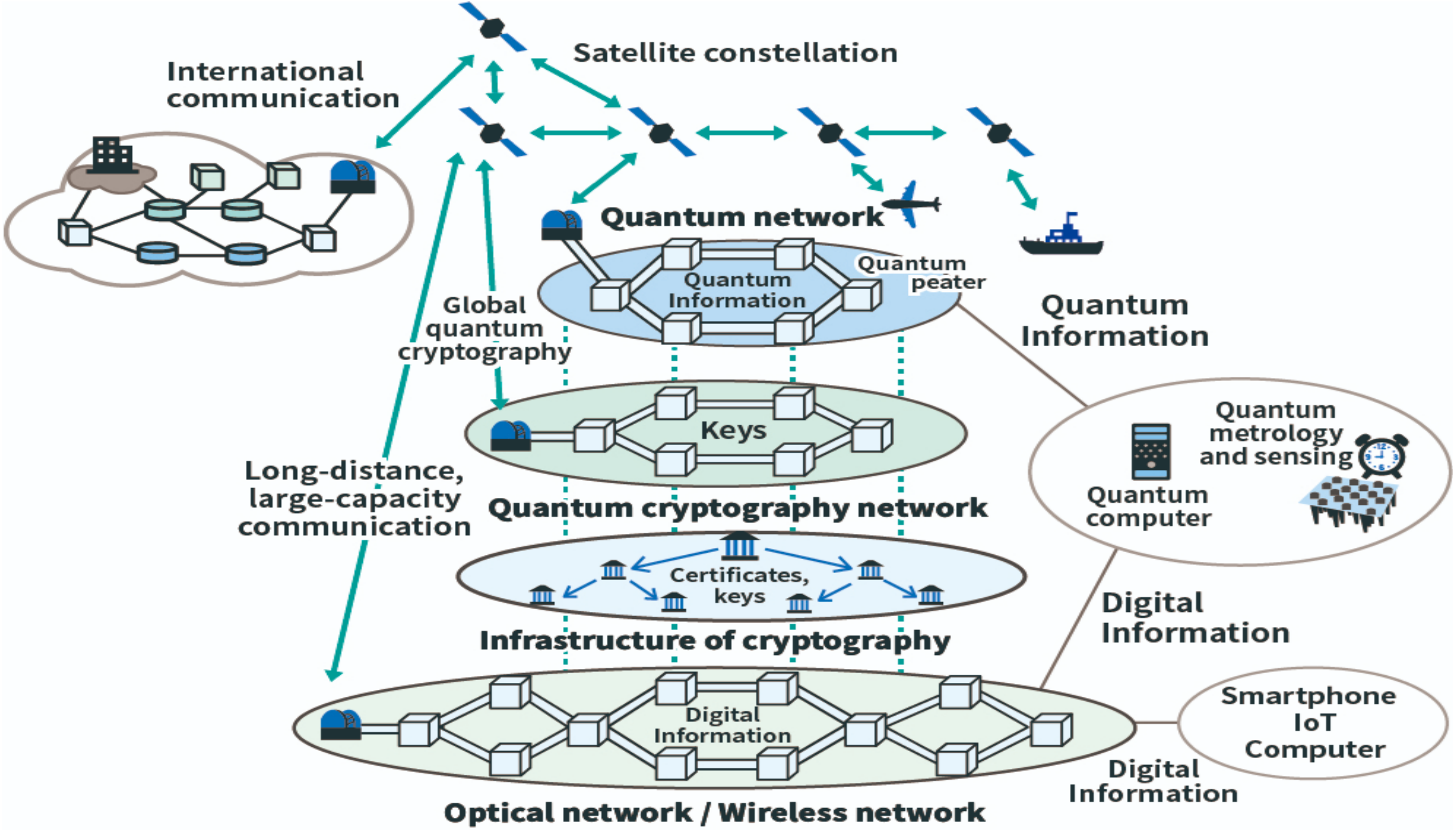
Prayagraj - Vindhyachal: Uttar Pradesh

Distance: ~100 Km, 26 dB loss

QBER: 6% , Secure Key rate: ~5 Kbps

https://pib.gov.in/PressReleasePage.aspx?PRID=1800648

Quantum Communication



Quantum Technology Utilization Impact Classification

Classification	Benefits & Utilization of Quantum Technology
Must have	to be implemented to protect against future quantum attacks (e.g. post-quantum cryptography)
Effectiveness	increase the effectiveness of the current technology and methods (e.g. quantum optimizations, quantum machine learning or artificial intelligence)
Precision	increase the precision of the current measurement technology (e.g. quantum magnetometry, quantum gravimetry, quantum inertial navigation, timing)
New capabilities	offers new capabilities that were beyond the scope of the present technology (e.g. quantum radar, quantum simulation for chemistry, quantum cryptoanalysis, quantum key distribution)

Short term: 0 – 5 years
Mid term: 6 – 10 years
Long term: 10 – 20 years

Thankyou