21º WRNP
Workshop RNP

Quantum Internet: Challenges and opportunities

Antônio J. G. Abelém[1], Gayane Vardoyan[2], and Don Towsley[2]

1-Universidade Federal do Pará - UFPA

2-University of Massachusetts - UMass, Amherst

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Outline

Introduction and Overview

Quantum Information and Quantum Computing

Quantum Communication and Quantum Networks

Current Scenario and Challenges

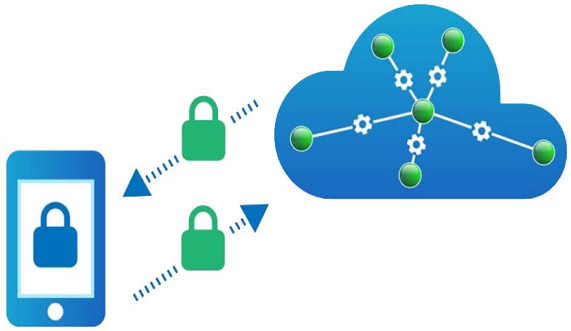
Concluding Remarks

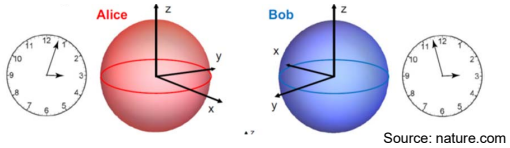
Introduction

- The main motivation for a **quantum Internet** is to enable applications that are out of reach for the classical Internet.
  - Enhance Internet technology by quantum communication between any two points;
  - May operate in parallel to the classical internet
    - connecting quantum processors in order to achieve capabilities that are probably impossible by using only classical means.

Applications (why Quantum Networks?)

- The best-known application of a quantum Internet is **Quantum Key Distribution** (**QKD**);
- Other applications include:
  - **Secure communication**:
    - Secure access to remote quantum computers (in the cloud)
  - **Distributed quantum computing**
    - Quantum computing clusters;
  - Tasks that require **coordination**:
    - clock synchronization, leader election, achieving consensus about data, to help two online bridge players coordinate their actions.
  - **Scientific applications**
    - such as combining light from distant telescopes to improve observations.



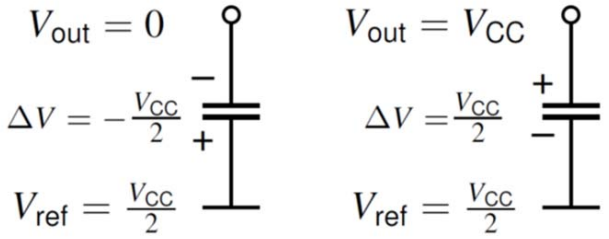


Source: nature.com

Quantum Information and Quantum Computing

- Quantum bit: qubit
  - Classical bit has only two values: 0,1
    - physically represented by two state device

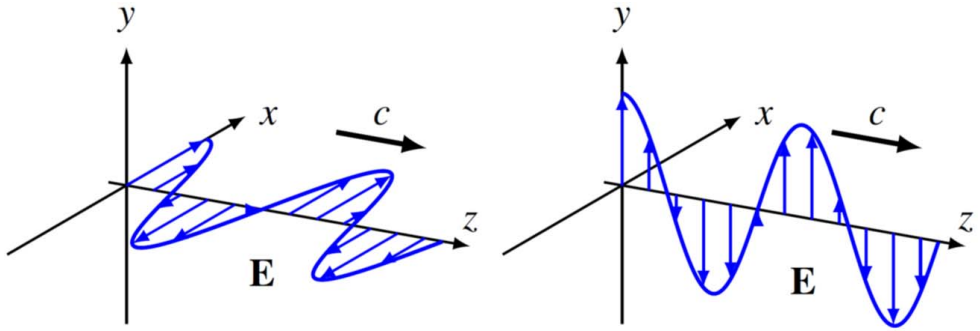
OFF ON



LOW HIGH

Quantum Information and Quantum Computing

- Quantum bits: qubits
  - The analogue of the classical bit is the quantum bit, or qubit for short.
  - Like a classical bit, a qubit has a state,



Horizontally polarized Vertically polarized

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

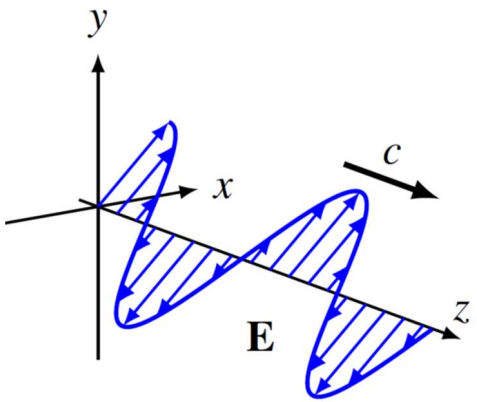
  - But...

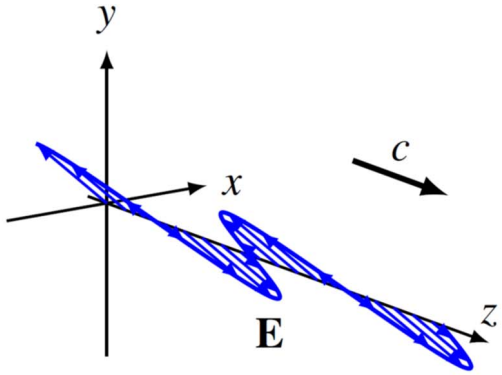
Quantum Information and Quantum Computing

- Quantum bits: superposition states
  - …unlike a classical bit, a qubit may be in a weighted superposition of the two states
  - Allowing certain functions to be evaluated for both input values at the same time.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$\alpha^2 + \beta^2 = 1$$





$$|+\rangle = \tfrac{1}{\sqrt{2}}(|x\rangle + |y\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \qquad |-\rangle = \tfrac{1}{\sqrt{2}}(|x\rangle - |y\rangle) = \tfrac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

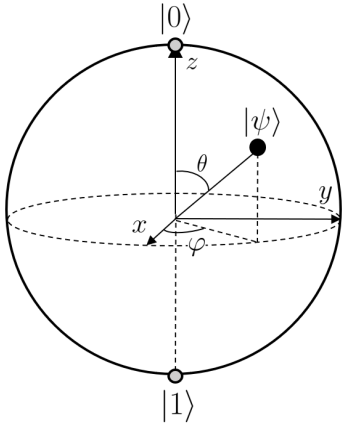
Quantum Information and Quantum Computing

- Quantum bits: superposition states
  - classical bit is like a coin

  - qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$ …
    - until it is observed.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$\alpha^2 + \beta^2 = 1$$



Bloch sphere

Quantum Information and Quantum Computing

Multiple qubits: Two qubits

- Four Basis states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

- A pair of qubits can also be in superpositions of these four states:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \qquad \sum \alpha_{ij}^2 = 1$$

Quantum Information and Quantum Computing

Multiple qubits: Two qubits

- Bell state or Einstein-Podolsky-Rosen (EPR) pair:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Bell pairs have the property that the qubits are correlated or **entangled**
  - Basis of quantum computing
  - Key ingredient in quantum teleportation and quantum networking.

Quantum Information and Quantum Computing

Multiple qubits: Two qubits

- Quantum entanglement

is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated.

Quantum Information and Quantum Computing

Multiple qubits: Two qubits

- There are other, larger multi-party entangled states that are useful for a variety of tasks:
  - Greenberger-Horne-Zeilinger (GHZ) state

$$\frac{|000\ldots\rangle + |111\ldots\rangle}{\sqrt{2}}$$

Other Bell States:

$$(|00\rangle - |11\rangle)/\sqrt{2}$$

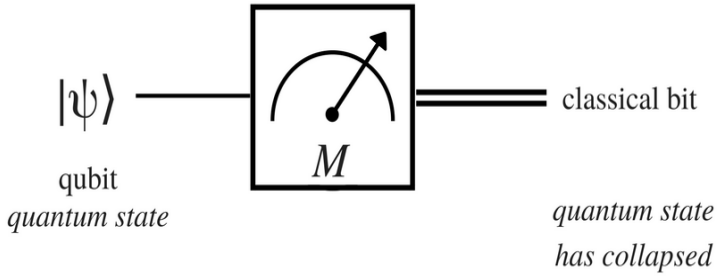
$$(|01\rangle + |10\rangle)/\sqrt{2}$$

$$(|01\rangle - |10\rangle)/\sqrt{2}$$

Quantum Information and Quantum Computing

Measurement

- In quantum physics, measurement is the testing or manipulation of a physical system in order to yield a numerical result.
    - The predictions that quantum physics makes are in general probabilistic.
- When a qubit is measured, it only ever gives ’0’ or ’1’ as the measurement result – probabilistically.

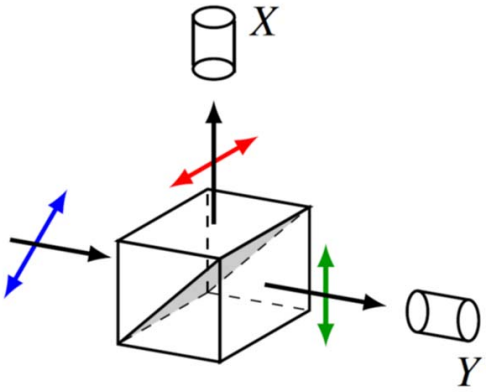


Quantum Information and Quantum Computing

Measurement

- Single photon:
  - either X or Y goes off, not both

$$|\phi\rangle = \alpha\,|x\rangle + \beta\,|y\rangle$$



- Repeat many times:

$$P(x) = \alpha^2, \quad P(y) = \beta^2$$

$$\alpha^2 + \beta^2 = 1$$

Quantum Information and Quantum Computing

Measurement example:

- Consider Bell state (EPR pair):

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- measuring first qubit yields 0 or 1
  - if 1, measuring second qubit yields 1
  - if 0, measuring second qubit yields 0

Quantum Information and Quantum Computing

Imperfect quantum systems:

- The state of a quantum system is exceedingly fragile.
  - Errors result in continuous degradation of our knowledge about the state of the quantum system.
  - Monitoring the system becomes extremely important.
    - As well as the management of error.

Quantum Communication and Quantum Networks

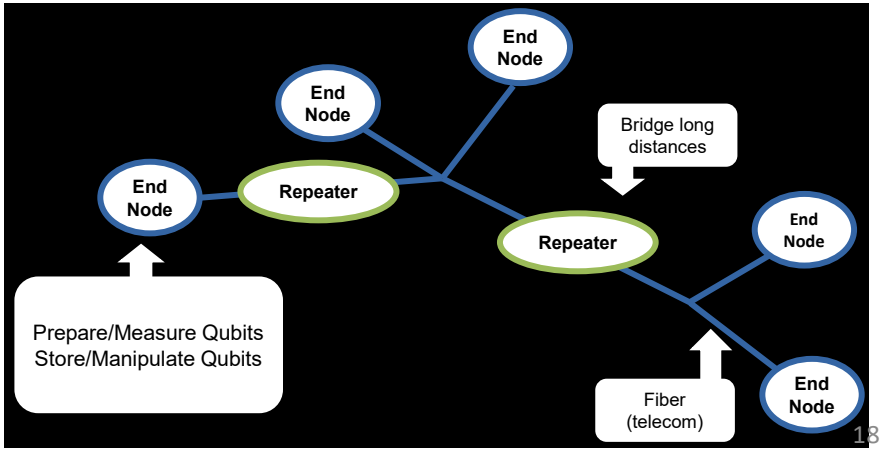
Quantum communication

- Consists of either the exchange of quantum information or the sharing of entangled quantum state between two or more parties.

Quantum Communication and Quantum Networks

Essential components

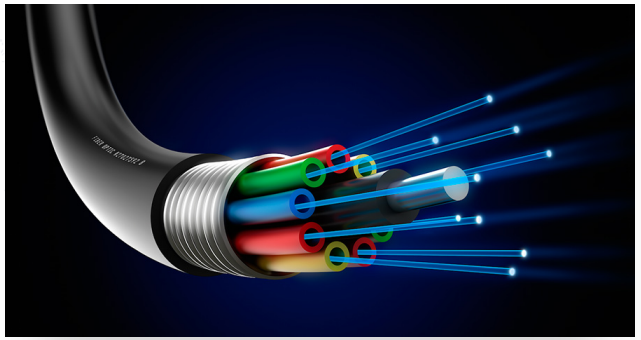
- To transport qubits from one node to another, we need:
  - Quantum communication channels
  - Quantum repeaters (2 connections) or routers or switches (>3 connections)
  - End Nodes

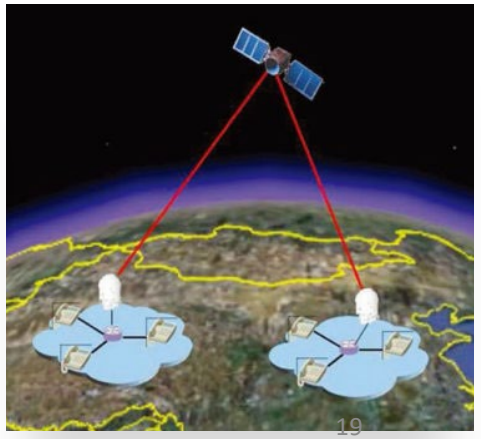


Quantum Communication and Quantum Networks

Quantum channels

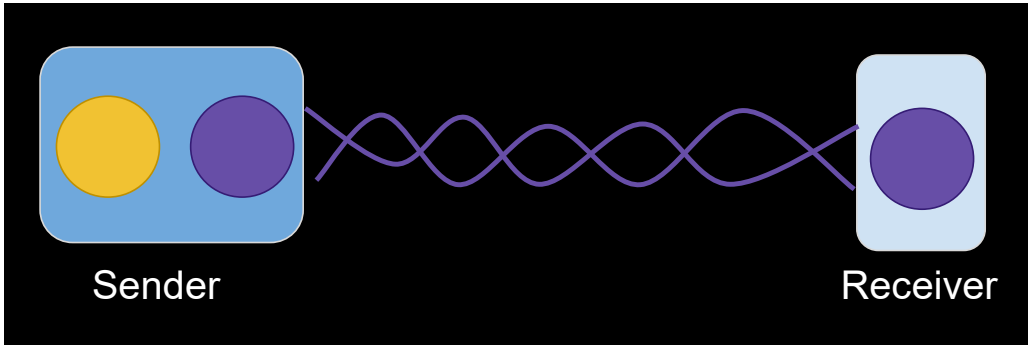
- For the purpose of quantum communication channels, can be used:
  - Standard telecom fibers
  - Free space.





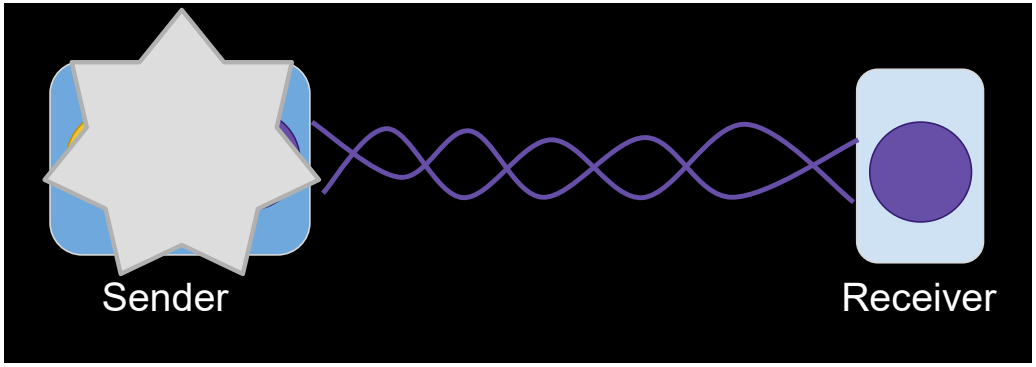
Quantum Communication and Quantum Networks

Sending Qubits via Entanglement:



Quantum Communication and Quantum Networks

Sending Qubits via Entanglement:



Quantum Communication and Quantum Networks

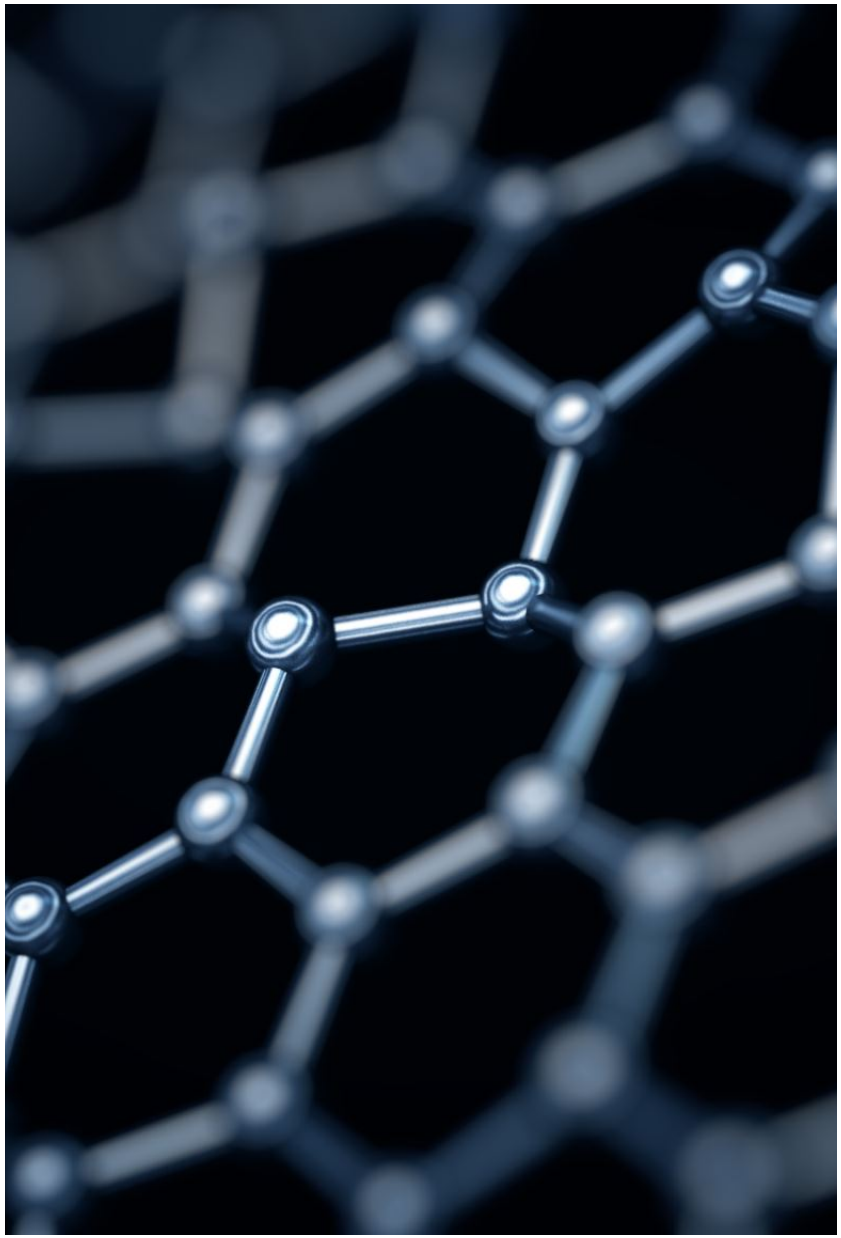
Sending Qubits via Entanglement:

- Consumes the entanglement
- Requires 2 bits of forward communication to the receiver.

Quantum Communication and Quantum Networks

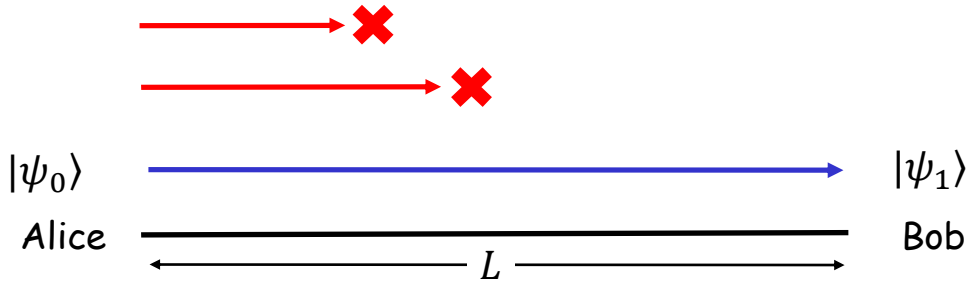
Teleportation

is the process by which quantum information can be transmitted from one location to another, with the help of classical communication and previously shared quantum entanglement between two parties.



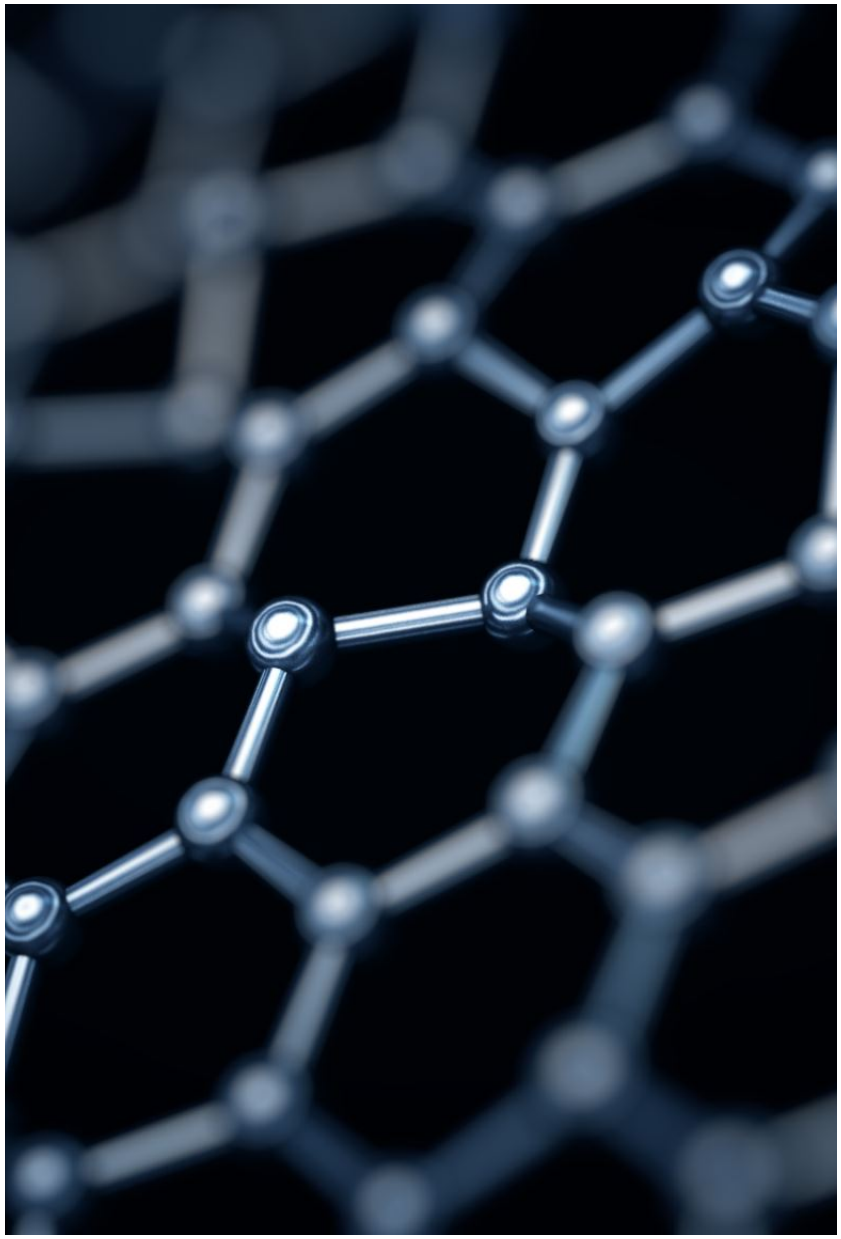
Quantum Communication and Quantum Networks

Quantum repeaters:



$P_{succ} = e^{-\alpha L}$ in fiber

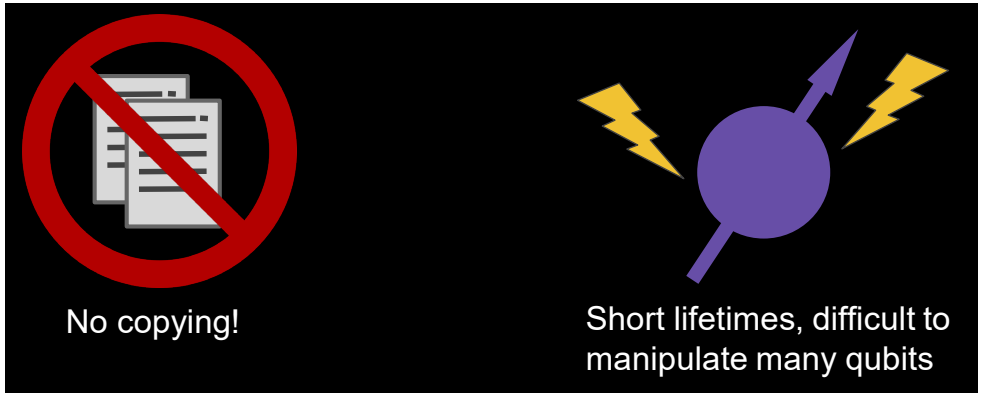
P_{succ} decays exponentially fast in distance



Quantum Communication and Quantum Networks

Quantum repeaters:

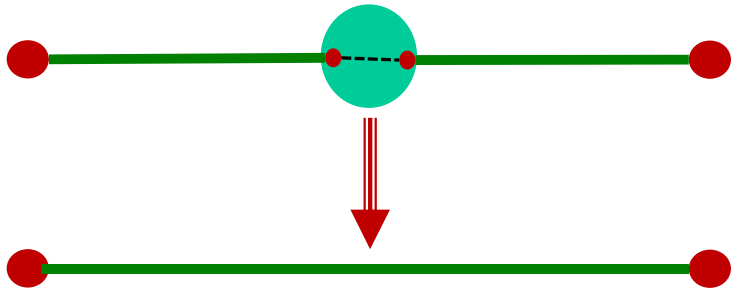
- How to send qubits over long distances?
  - Amplifiers cannot be used since qubits cannot be copied - known as the no-cloning theorem.



Quantum Communication and Quantum Networks

Quantum repeaters:

- How to send qubits for long distances?
  - generate link Bell states (entanglements)
  - Timing coordination: qubits arriving at the same time at the mid point
  - Or storage: wait until both qubits arrived
  - propagate entanglements
    - Original entanglement is consumed
  - Classical communication
    - from the mid point to the end points



Quantum Communication and Quantum Networks

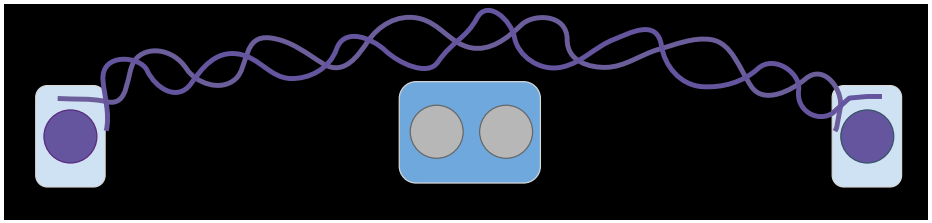
Quantum repeaters:

- In essence, a quantum repeater protocol executes three operations:
  - Entanglement distribution;
  - Entanglement purification;
  - Entanglement swapping.

End-to-end entanglements

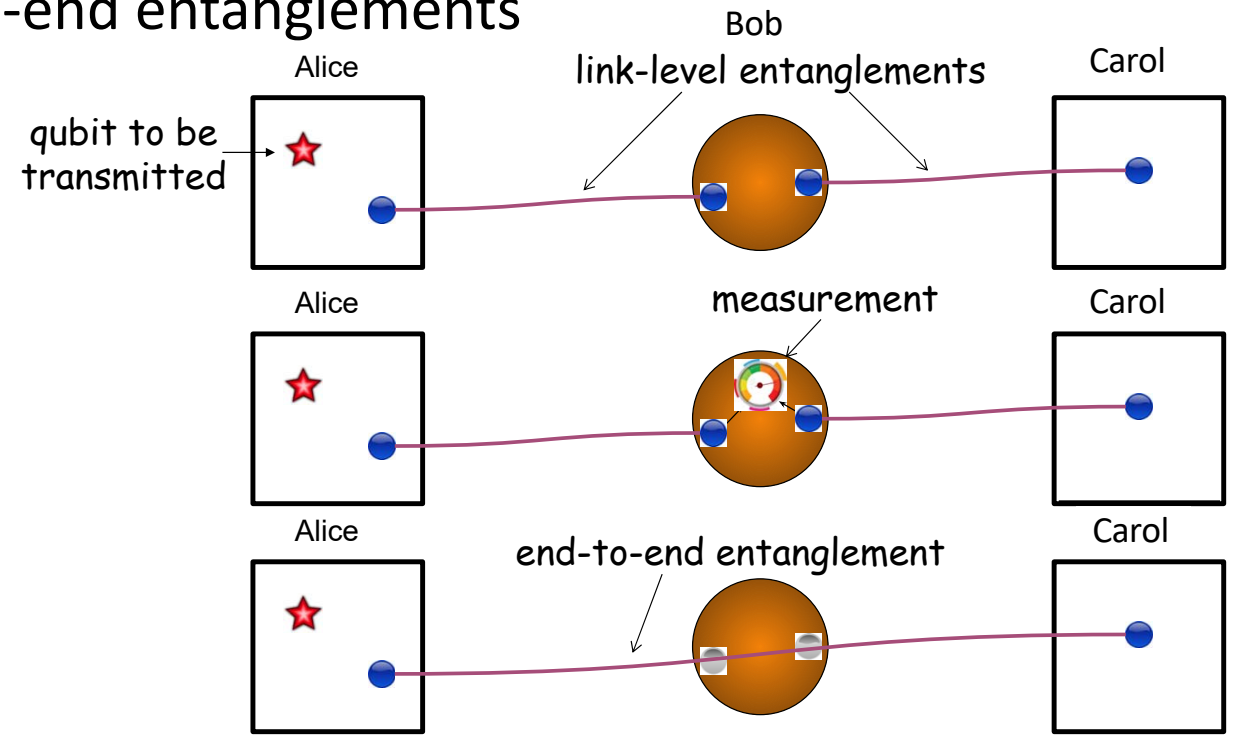
+

Teleportation



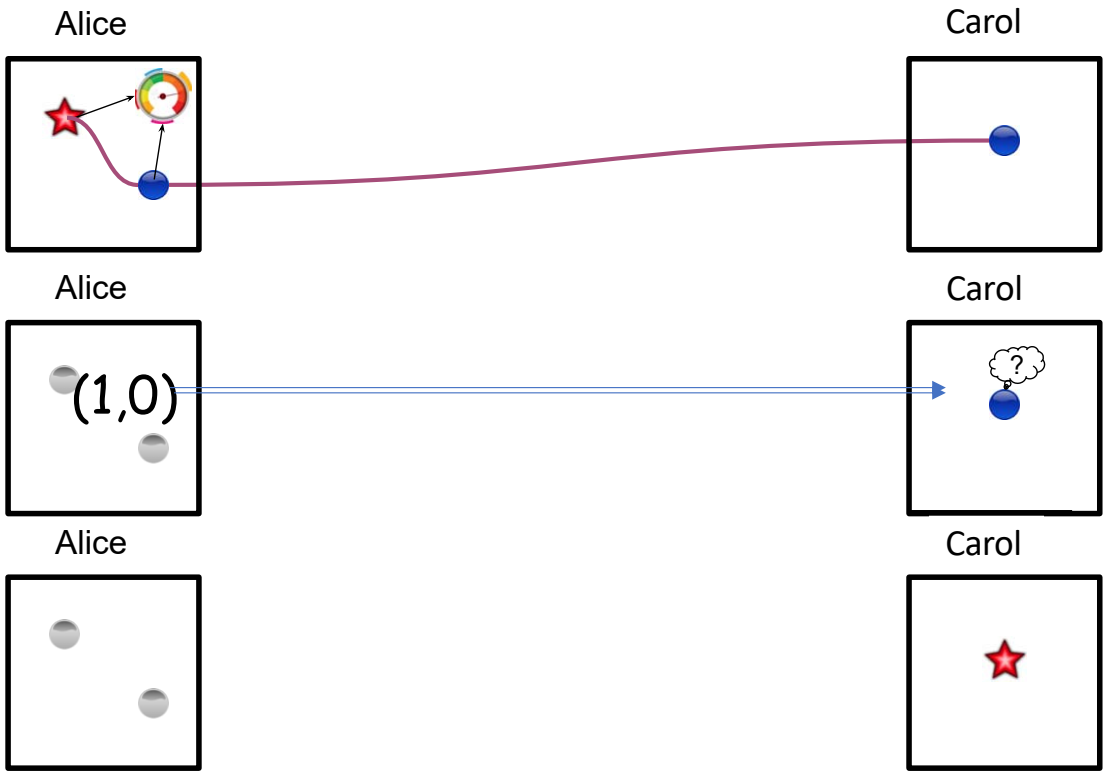
Quantum Communication and Quantum Networks

End-to-end entanglements

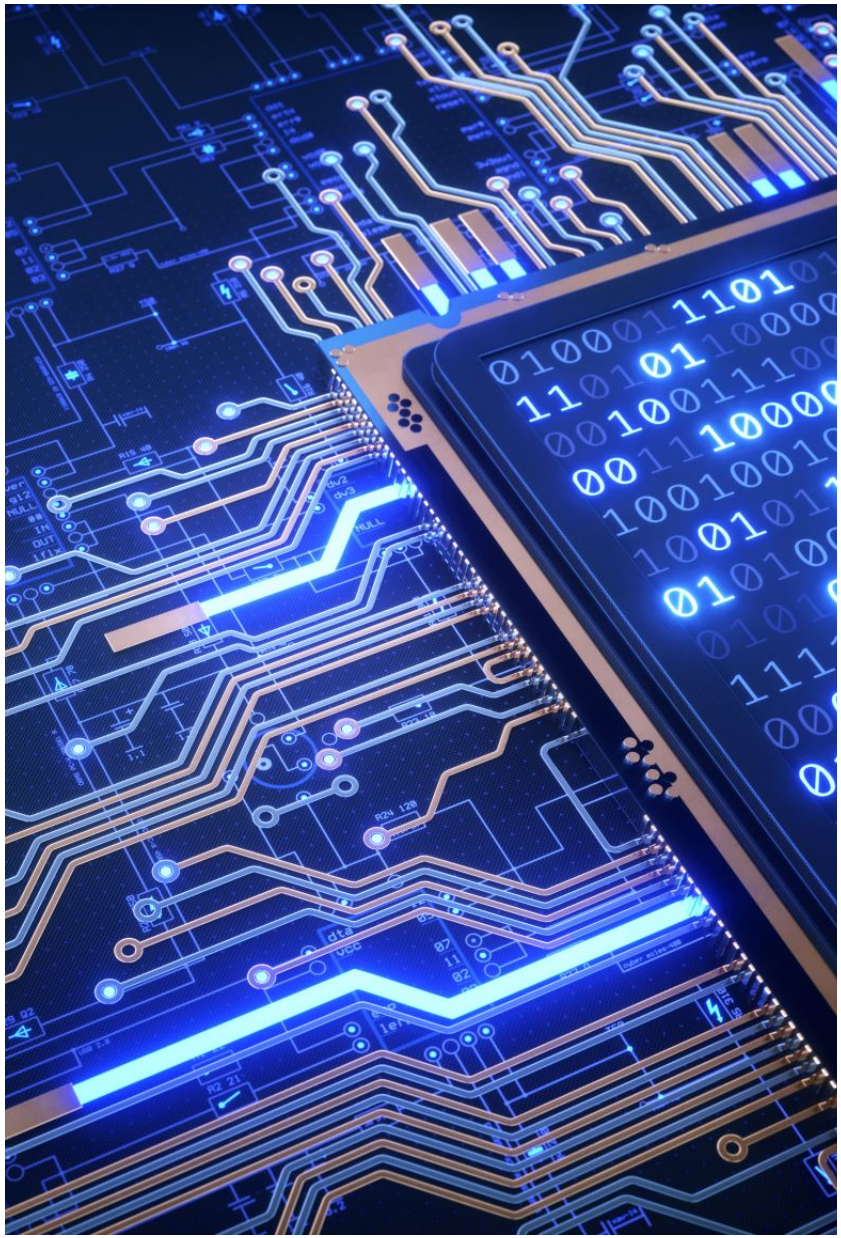


Quantum Communication and Quantum Networks

Teleportation



- Consumes the entanglement
- Requires 2 bits of forward communication to the receiver



Quantum Communication and Quantum Networks

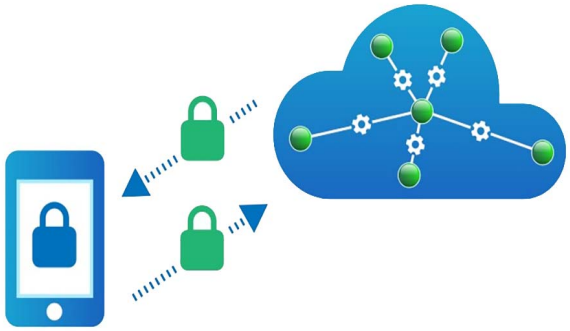
End nodes

- the quantum processors connected to the quantum Internet.
- These may range from extremely simple nodes that can only prepare and measure single qubits to large-scale quantum computers.
- End nodes may themselves act as quantum repeaters, although this is not a requirement.
- All nodes can communicate classically—for example, over the classical internet—in order to exchange control information.

Quantum Communication and Quantum Networks

Quantum Key Distribution (QKD)

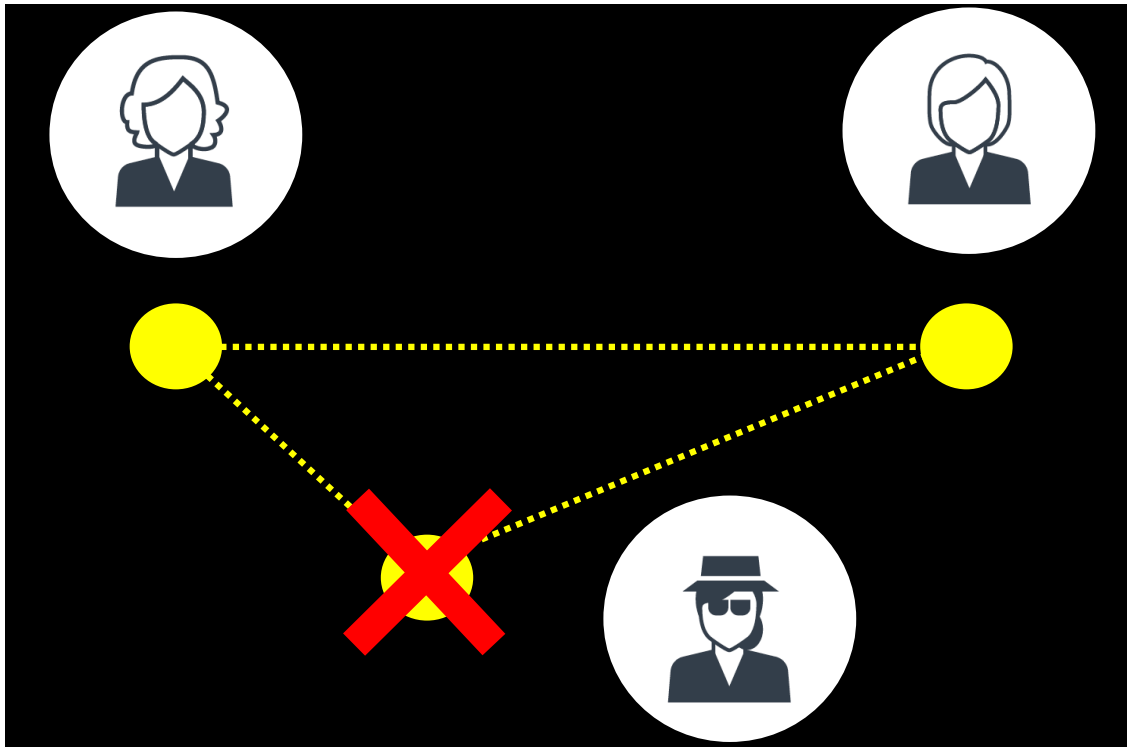
- The most practical, commercially attractive use of quantum networks in the near term.
- The main objective in QKD is generates shared, secret random numbers between two distant parties.
  - Uses quantum mechanics to detect the presence or absence of an eavesdropper.



Quantum Communication and Quantum Networks

Quantum Key Distribution (QKD)

- An important and unique property of QKD is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key;
- This results from a fundamental property of quantum mechanics:
  - the process of measuring a quantum system, in general, disturbs the system.
- The first QKD protocol was proposed in 1984 and since then, more protocols have been proposed:
  - BB84, developed by Charles Bennett and Gilles Brassard;
  - E91, proposed by Artur Ekert.



Quantum Communication and Quantum Networks

QKD Implementations

- Well beyond the experimental phase;
- Commercial products are available, and metropolitan-area testbed networks exist in:
  - Boston, Vienna, Geneva, Barcelona, Durban, Tokyo, several sites in China and elsewhere throughout the world.
- QKD has also been integrated into:
  - custom encryption suítes;
  - Internet standard IPsec suíte;
  - And has been proposed for use with the TLS protocol.

Quantum Networks and Quantum Internet

Characteristics

- Enable to transmit quantum bits;
- Qubits can be entangled with each other enabling stronger correlation and coordination
- Qubits cannot be copied/amplified;
- Quantum network protocols do not require large quantum computer
- Errors in quantum internet protocols can often be dealt with by using classical error correction

Challenges

- Transmit qubits over long distances
- Achieve more useful quantum applications and
- define technology required to realize them.

Quantum Networks and Quantum Internet

The basic structure of a quantum network and more generally a quantum Internet is analogous to a classical network.

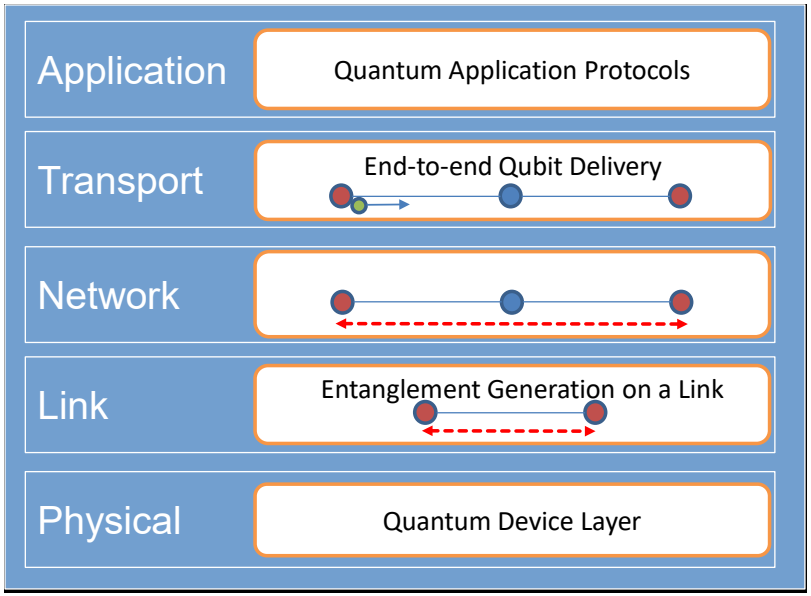
Quantum channels, quantum repeaters (quantum routers/switches) and end nodes.

Layering is a natural means of dividing functionality

the associated modularity allows us to replace individual functions more or less independently.

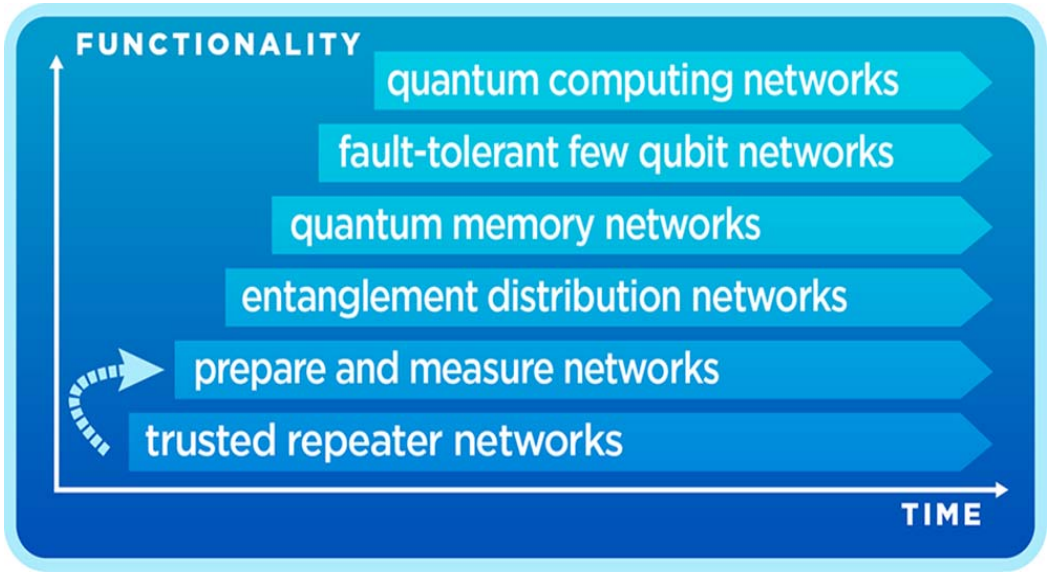
Quantum Networks and Quantum Internet

- Some preliminary functional allocation of a quantum network stack has been proposed:
  - Stages of development toward a full-blown quantum Internet, proposed by Stephanie Wehner et al.;
  - Quantum Recursive Network Architecture (QRNA), proposed by Van Meter et al.;



Evolution Phases

- **Short term:** one may optimize both repeaters and end nodes relatively independently:
  - simple end nodes
  - powerful repeaters
- **Near-term:** quantum internet may be optimized for shorter distances:
  - for example, pan-European
  - powerful end nodes
- **Long term:** a full-blown worldwide quantum internet.
  - quantum repeaters need to be able to support the functionality of each stage.

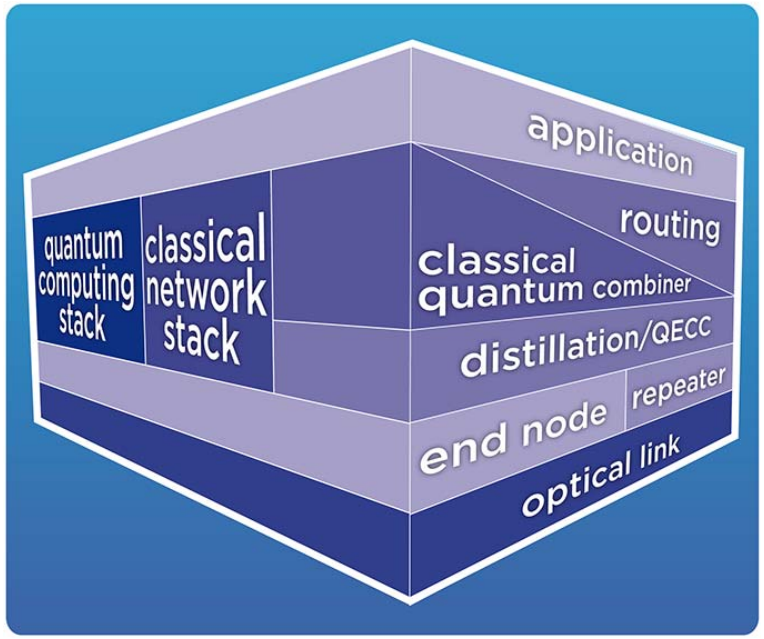


*Funcionality driven stages of Quantum Internet according Stephanie Wehner et al. [S. Wehner and Hanson 2018].

Quantum Network Stack

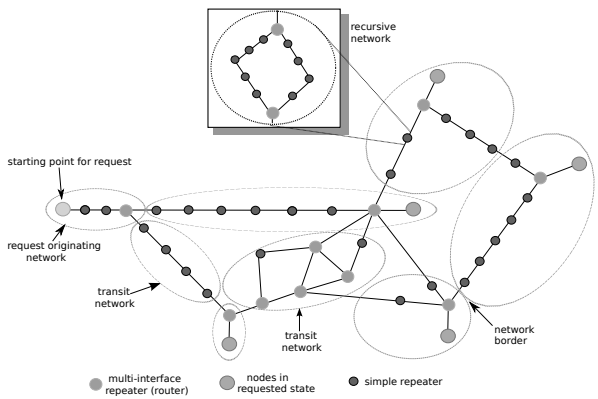
Important to:

- Enable widespread use and application development:
- No such network stack presently exists for a quantum internet:
  - Only some basic elements have been noted.
- Examples of why a new stack is required:
  - Mapping between classical control information (header) and the underlying qubits
  - The use of error detection at the link layer of the classical network stack does not easily translate to a realistic quantum network.

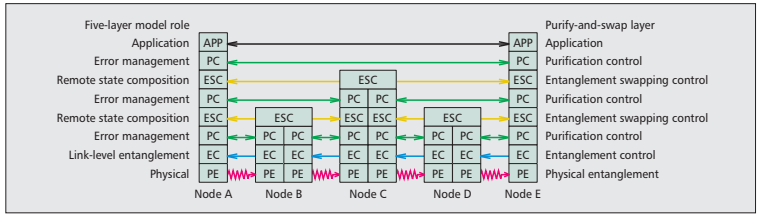


Quantum Recursive Network Architecture (QRNA)

- QRNA's organizing principle is recursion;
- The most radical difference from classical networks arises from the need to extend message semantics:
  - Messages in QRNA will carry requests more explicitly:
    - please build this state for me, and dispose of it like so once it is built.



* 2011, Van Meter, Touch e Horsman



*Proposed by Van Meter, Touch and Horsman

Where are we now?

State of the art

- Quantum Cryptography (QKD): Key Distribution
  - Non Device Independent
  - Metropolitan-area testbed networks

Status:

- Commercial at short (~100km) distances
  (idQuantique, Huawei, Toshiba, Mitsubishi, ...)
- Lab ~300kms
- Entanglement over a distance of ~ 1400km via satellite

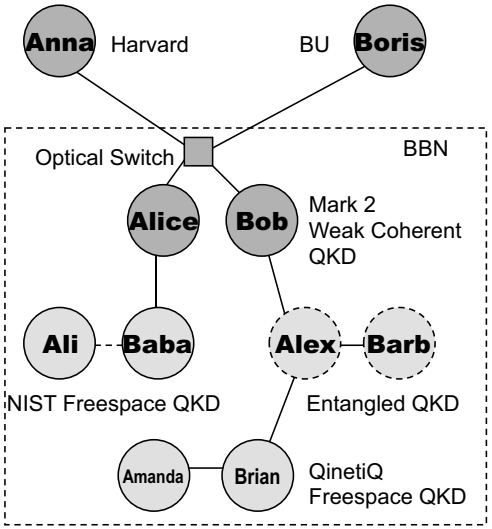
Grand Challenges:

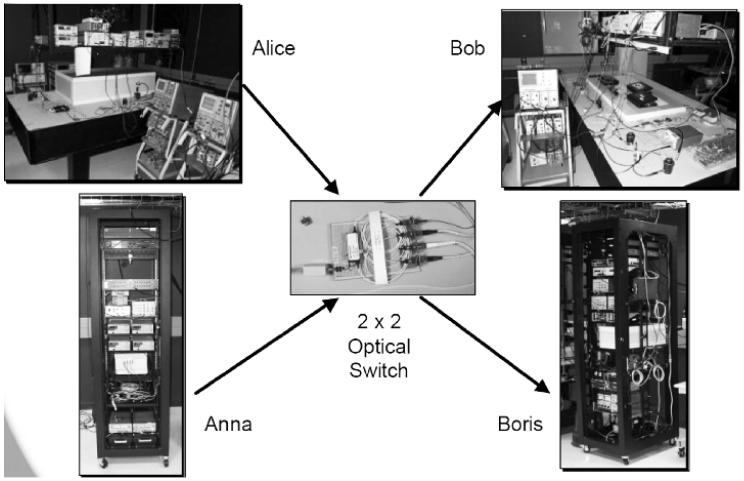
- Distance – want to communicate over long distances
- Functionality – want to do more than QKD

Metropolitan-area testbed networks

Boston-area network

- the world's first deployed QKD network
  - supported by DARPA
- 10 nodes running several different QKD implementations
  - "A" nodes contain the transmitters and "B" nodes contain the receivers .
  - some nodes are multiple hops away.
- BBN developed a quantum key relay protocol to allow those nodes to share secret Keys.





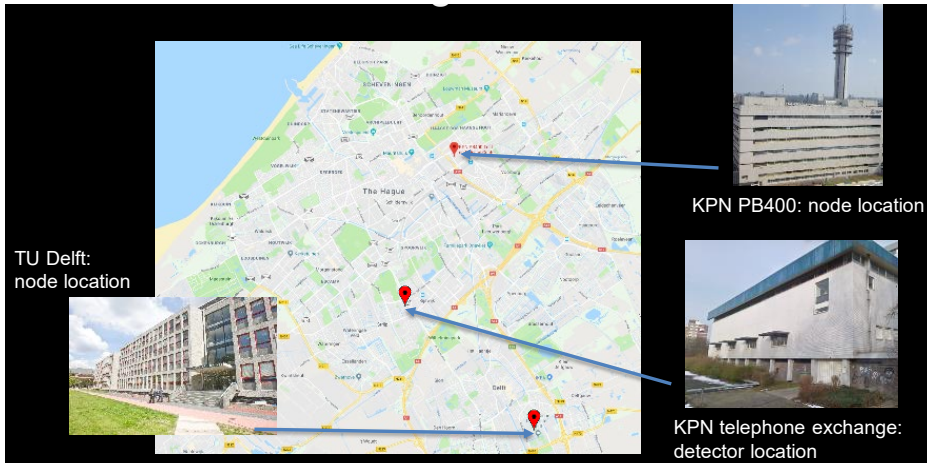
Metropolitan-area testbed networks

Delft – Den Haag

- Make 2 processor nodes that are prepared for future upgrades
- Make use of existing telecom (dark) fibers
- Generation of entanglement between the 2 nodes

Possible Network Expansion

- World's first network connecting quantum computers
- Direct QKD links between neighbouring nodes to authenticate control traffic
- World's first quantum network stack demonstration



Research Challenges

Some networking challenges:

- Link layer
  - No-broadcasting theorem: impossibility of transmitting quantum information to more than a single destination;
- Routing
  - novel quantum routing metrics;
  - Static vs opportunistic routing;
- Network layer
  - new entangled pairs need to be created and distributed between the source and the destination for each additional qubits need to be teleported;
  - Fast and reactive control plane for generating entanglement

Research Challenges

More networking challenges:

- Modeling and performance analysis
- Stateless vs stateful control
- Data, control plane design
  - SDN
  - Quantum data plane
  - programmable quantum switches
- Measurement, management
- Security
- Understanding application requirements

Research Challenges

The main challenges in scaling networks to Internet-scale and beyond are:

- Heterogeneity
  - especially of deployed technologies and local conditions;
- sheer scale
  - affecting routing and naming in particular;
- dealing with out-of-date information
  - e.g. routing or congestion;
- meeting the needs of participating organizations
  - such as privacy, policies and autonomous management;
- and misbehaving nodes on the network
  - deliberate or accidental.

Quantum initiatives

China:

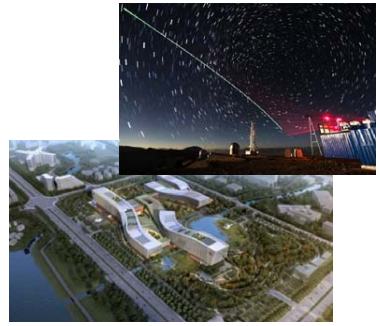
- China's Quantum Experiments at Space Scale (Micius)
- National Laboratory for Quantum Information Science (Hefei)
- 76 billion Yuan

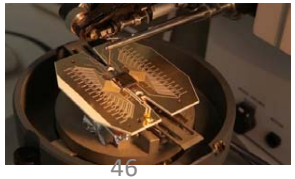
Europe:

- Quantum Technology Flagship
- one billion euros
  2017-2027

USA:

- National Quantum Initiative Act
- 1.25 billion dolllars
  2019-2029
- National Science Foundation
  - Research Center for Quantum Networks





Simulators

- To explore quantum networking:
  - NetSquid: Network Simulator for Quantum Information using Discrete events.
  - http://www.netsquid.org
- To explore quantum applications:
  - Application level simulator - SimulaQron Download
  - http://www.simulaqron.org

QuTech

21º WRNP

Workshop RNP

Thanks! Questions?

RNP ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL