NOKIA Bell Labs

Quantum Internet

Review of the Quantum Internet Research Group (QIRG @ IRTF)

- Ludovic Noirie
- 09-09-2020

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

1. Quantum Internet Research Group @ IRTF
Internet Engineering Task Force (IETF)

IETF = Internet Engineering Task Force

- https://www.ietf.org/
- The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.
- 7 "Areas" with many working groups (WGs) in each (changing with time…):
  - Applications and Real-Time Area (25 WGs): **HTTP**, **IMAP**, **RTP**, …
  - General Area (2 WGs): management of the IETF processes…
  - Internet Area (17 WGs): **IP**, **NTP**, …
  - Operations and Management Area (14 WGs): **DNS**, **NETCONF**, **YANG**, …
  - Routing Area (24 WGs): **BGP**, **PCE**, **MPLS**, **MANET**, **OLSR**, **LISP**, …
  - Security Area (23 WGs): **IPsec**, …
  - Transport Area (10 WGs): **TCP**, **UDP**, **QUIC**…
- Production of "Internet Drafts" that may become "Requests For Comments" (**RFCs**)

1. Quantum Internet Research Group @ IRTF

Internet Research Task Force (IRTF)

IRTF: R = Research part of IETF…

- List of research groups: https://datatracker.ietf.org/rg/
  - Today 14 research groups

- They produce Internet drafts and Request For Comments (RFCs) like IETF
  - Network Management Research Group (NMRG): 4 RFCs
    - Autonomic Networking: Definitions and Design Goals: https://datatracker.ietf.org/doc/rfc7575/
  - Information-Centric Networking (ICNRG): 7 RFCs
  - Internet Congestion Control (ICCRG): 2 RFCs
  - Thing-to-Thing (T2TRG): 1 RFC
  - Measurement and Analysis for Protocols (MAPRG): 0 document…
  - …

1. Quantum Internet Research Group @ IRTF

Quantum Internet Research Group (QIRG @ IRTF)

- Web site: https://datatracker.ietf.org/rg/qirg/about/

- History:
  - 2018/01: Idea of a RG at IRTF launched
  - 2018/11: QIRG approved as a proposed IRTF Research Group
  - 2020/03: QIRG approved as a full IRTF Research Group

- Charter: https://datatracker.ietf.org/doc/charter-irtf-qirg/

- Documents: https://datatracker.ietf.org/rg/qirg/documents/
  - Architectural Principles for a Quantum Internet (v04: 2020-07-12) **[QI-archi]**
    - https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/
  - Applications and Use Cases for the Quantum Internet (v01: 2020-07-10) **[QI-app]**
    - https://datatracker.ietf.org/doc/draft-wang-qirg-quantum-internet-use-cases/

1. Quantum Internet Research Group @ IRTF

QIRG charter 1/2

- **The Quantum Internet will bring new communication and remote computation capabilities such as quantum secure communication, distributed quantum computing, and quantum-enhanced physical sensor systems. A key focus area for quantum networks will be cryptographic functions such as quantum key distribution or quantum byzantine agreement.**

- Overall the goal of the QIRG is to address the question of how to design and build quantum networks. Some of the problems that need to be addressed include:
  - Routing: high fidelity threshold vs. low coherence time…
  - Resource allocation: coherence time, quantum memory
  - Connection establishment: entangled states delivery
  - Interoperability: heterogeneous hardware (ion traps, atomic ensembles, nitrogen vacancy centers…)
  - Security: vulnerability of quantum repeaters?
  - API design: API for entangled states vs. fidelity and low coherence time of quantum memories

- Some other problems that can be tackled by the QIRG:
  - Applications for a Quantum Internet
  - Multi-party states and multi-party transfers such as network coding

1. Quantum Internet Research Group @ IRTF

QIRG charter 2/2

- Concrete work items that QIRG may produce include:
  - **An architectural framework delineating network node roles and definitions, to build a common vocabulary and serve as the first step toward a quantum network architecture.**
  - Wehner, Elkhouss and Hanson have created a roadmap of technical capability milestones for quantum networks. Mapping these milestones to concrete use cases will help to determine the order and timing of classical protocols that will be needed. For example, consider prepare-and-measure networks; what data rates, fidelities are needed to e.g. make a useful position verification service, and how would you incorporate that into a complete information system?
  - Finally, QIRG will serve as a coordination point with other standards organizations that are working on standardization of quantum networks.

- Process
  - QIRG will hold 2-3 meetings per year, online or in person, in accordance with current best practice.

- Membership Policy: Open

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

2. Why quantum networks at IRTF [QI-archi, §1]

Introduction to “Architectural Principles for a Quantum Internet” 1/2

First definition of quantum networks

- **Quantum networks are distributed systems of quantum devices** that utilize fundamental quantum mechanical phenomena such as superposition, entanglement, and quantum measurement to achieve capabilities beyond what is possible with classical networks.
- **Quantum devices**: from simple photonics devices to large-scale quantum computers of the future.

Quantum networks vs. classical networks?

- **A quantum network is not meant to replace classical networks**, but rather form an overall hybrid classical quantum network supporting new capabilities which are otherwise impossible to realize.
- For new applications such as secure communications, distributed quantum computation, or quantum-enhanced measurement networks.
- Most well-known (and existing!) application of quantum communication: **quantum key distribution** (QKD) for secure communications, already deployed at short (<100km) distances.

2. Why quantum networks at IRTF [QI-archi, §1]

Introduction to "Architectural Principles for a Quantum Internet" 2/2

Current situation

- Physical realization of quantum devices
- Connection of such quantum devices, but lot of effort to improve seed and error tolerance

Work to do for quantum networks

- How to run these networks?
- Management of the classical equivalent of sending, receiving, buffers, connection synchronization, common interfaces, …
- Robust protocols for managing quantum state transmission

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

3. Quantum information [QI-archi, §2]
Qubit

Ludovic Noirie: I used here the relational interpretation of quantum mechanics [C. Rovelli, 1996] https://arxiv.org/abs/quant-ph/9609002

Qubit without talking about Hilbert spaces… (relational interpretation of quantum mechanics)

1. Interaction = observation = information acquisition on an observed system by an observer system
2. State = knowledge an observer system has on an observed system (comes from **1**)
3. An observer can always get new information on a system, replacing the old one (information renewal)

- 1 qubit represents 1 bit of information, either “0” or “1”, after a given measurement (**2**)
  - The choice of “0” and “1” is a convention…
- Let’s consider an initial state “0” after a first measurement with a given measurement “basis”
- Different measurement “bases” are possible on one qubit (**3**):
  - Same measurement basis = no renewal of information (0 bit) ⇒ 100% “0”, 0% “1”
  - “Maximal-complementary” measurement basis = full renewal of information (1 bit) ⇒ 50% “0”, 50% “1”
    ⇒ Intrinsic random generator!
  - Any measurement basis = partial renewal of information ($-p\log_2 p - (1-p)\log_2(1-p)$ bit) ⇒ p = (100-X)% “0”, (X)% “1”

⇒ 1 qubit is modeled by rays in a Hilbert space of dimension 2…

3. Quantum information [QI-archi, §2]
Multiple qubits

Ludovic Noirie: I used here the relational interpretation of quantum mechanics [C. Rovelli, 1996] https://arxiv.org/abs/quant-ph/9609002

Multiple qubits without Hilbert spaces… (relational interpretation of quantum mechanics)

1. Interaction = observation = information acquisition on an observed system by an observer system
2. State = knowledge an observer system has on an observed system (comes from **1**)
3. An observer can always get new information on a system, replacing the old one (information renewal)

- N qubits represent N bits of information (**2**)
- N non-interacting qubits = N independent qubits = "separable" state
- N interacting qubits = N correlated qubits (information correlation) = "entangled" state
- Information correlation comes from interactions between the N qubits (**1**):
  - The N qubit gets information from each other that is not known by the rest of the universe (**3**)

    ⇒ This corresponds to the Schrödinger equation in quantum mechanics for isolated systems
  - Information on individual qubits is (partially or fully) lost by the external observer (rest of the universe) (**3**), which has correlation information instead

⇒ N qubits are modeled by rays in the tensor-product Hilbert space of dimension 2^N…

Ludovic Noirie: I used here the relational interpretation of quantum mechanics [C. Rovelli, 1996]

3. Quantum information [QI-archi, §2]

(Maximally) Entangled states (also known as Bell pairs of qubits for $N = 2$)

The “magic” of an entangled pair of qubits (relational interpretation of quantum mechanics)

- 2 qubits represent 2 bits of information (**2**).
- The (maximal) entanglement between 2 qubits comes from a previous interaction between them (**1**): they exchanged 1 bit of information each other (**1**), which is not known by the rest of the universe (**2**)
- The rest of the universe lost the information on the individual qubits (**3**)
- It only knows the states are correlated (**3**) and that a choice of a common measurement basis for the 2 qubits will give the same measured values (1 bit of information left)
- When an observer observes one of the qubits, it gets 1 bit of new information (50% “0”, 50% “1”) for any choice of a measurement basis (**1** & **3**). “New information” really means information creation!
- Because the observer had already 1 bit of correlated information, it also knows the state of the other qubits before measurement on it (by him/her/itself or another observer system) (**2**)
- If the measurement bases on the two qubits coincide (and only if!), then because of this correlated information, with 100% probability the measured values coincide (both “0” or both “1” in the common basis)

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

4. What quantum networks are [QI-archi, §3]
Entanglement as the fundamental resource

Usages of quantum networks?

- Essentially: **transmission of qubits in quantum links and quantum processing in quantum nodes**
- Quantum teleportation helps: maximally-entangled pairs can be used to quantum-teleport qubits

Quantum network = distributed system to create maximally-entangled pairs of qubits between any pair of nodes

1. Creation of maximally-entangled pairs of qubits in each quantum node
2. Short-range direct transmission of one qubit of each entangled pairs to neighbor quantum nodes
3. Quantum-teleportation to transmit hop-by-hop entanglement to any pair of distant quantum nodes
4. Use of classical communication to transmit classical control bits for quantum-teleportation
5. The applications at the end points will consume the entangled pair of qubits:
   - Either directly for Quantum Key Distribution protocol for example
   - Either using quantum teleportation to quantum-teleport qubits from one quantum processor to another one

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

5. Achieving quantum connectivity [QI-archi, §4]

Challenges and limitations of direct transmission

Challenges

- The measurement problem (theoretical barrier ⇒ one must do with it…)
  - A measurement “destroys” the qubit state (wave function collapse principle)
- No-cloning theorem (theoretical impossibility ⇒ one must do with it…)
  - Quantum qubits cannot be duplicated, no amplification…
- Fidelity of qubits (technological issue ⇒ progress expected in future but will it be enough?)
  - Fidelity of a qubit = probability to measure the expected state for this qubit (equivalent to an error rate)
  - Each application has a threshold: the fidelity of used qubits must be above this threshold to work properly

Direct transmission

- Because of no-cloning theorem, direct transmission is limited to short distances
  - Fiber: losses ~0.2 dB/km (exponential with distance…) at best wavelengths ⇒ 99% losses for 100 km

5. Achieving quantum connectivity [QI-archi, §4]
Bell pairs and teleportation

Bell pairs

- Bell pairs of qubits are maximally entangled pairs of qubits (see in §3)

Quantum teleportation

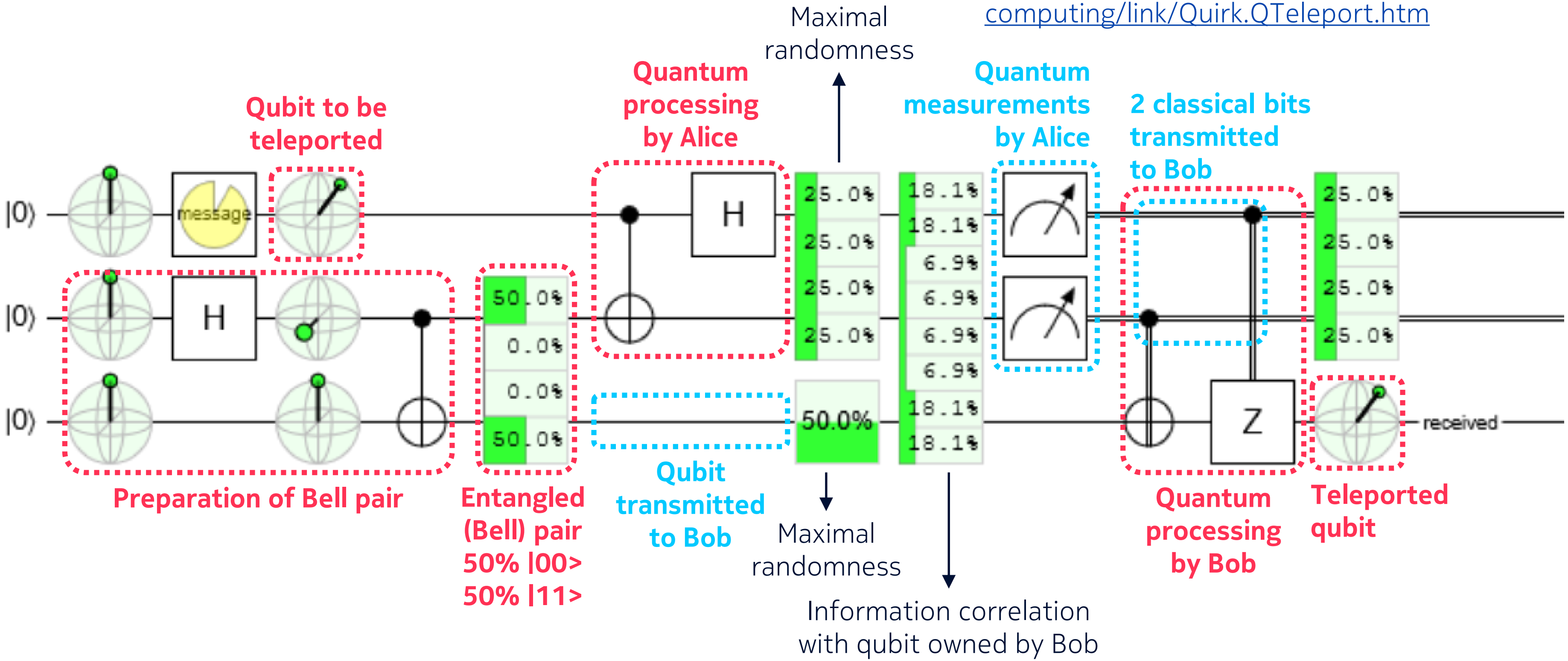
1. A Bell pair shared by node A and B will be consumed to teleport any qubit X from a node A to a node B
2. Node A processes the initial qubit X and the qubit of the Bell pair it owns (quantum processing: C-NOT + Hadamard gates) then measure them: these two qubits are destroyed to produce 2 classical bits
   - Note: these two classical bits are not enough to reconstruct the initial qubits X, one needs to use the other qubit of the shared Bell pair…
3. A classical channel transmits those 2 bits of information from A to B
4. Node B used these two classical bits to transfer the initial state of the initial qubit X to the other qubit of the Bell pair it owns (quantum processing: C-NOT & C-Z gates).

See http://ludovic-noirie.fr/sciences/quantum-computing/link/Quirk.QTeleport.htm

5. Achieving quantum connectivity [QI-archi, §4]

Teleportation quantum processing

See http://ludovic-noirie.fr/sciences/quantum-computing/link/Quirk.QTeleport.htm



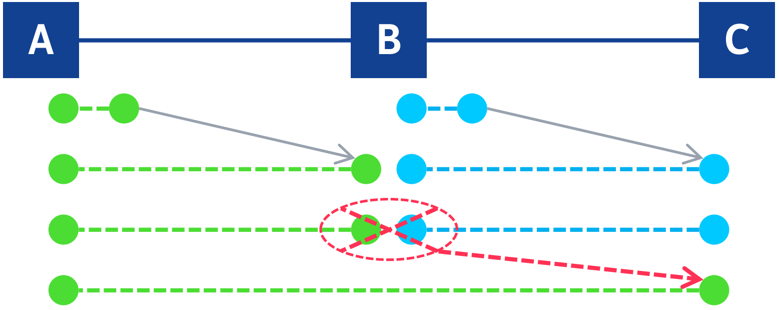
5. Achieving quantum connectivity [QI-archi, §4]
Life-cycle of entanglement

- Elementary link generation
  - Creation of a Bell pair locally
  - Transmission of one (or the two) qubit(s) of the Bell pair to one (or two) neighbor node(s)
  - 3 schemes: at mid-point / at source / at both ends
  - There exist some mechanisms to ensure these processes are successful
- Entanglement swapping
  - Use of quantum teleportation to transfer the entanglement hop-by-hop to distance nodes (see next slide)
- Distillation/purification of the Bell pair
  - Link generation and entanglement swapping are noisy process, which degrades the fidelity of the Bell pair of qubits
  - Distillation/purification is a process to create a Bell pair with higher fidelity from 2 ore more Bell pairs with lower fidelity (a bit like error correction)
- Delivery of the Bell pair to the application at the two end-nodes

5. Achieving quantum connectivity [QI-archi, §4]

Quantum teleportation vs. direct transmission

Quantum teleportation for entanglement swapping



- Step 1: Bell pair creation in A and B
- Step 2: Shared Bell pairs A/B and B/C ("at source" scheme)
- Step 3: Quantum teleportation
  - B teleports the qubits from A to C through the blue Bell pair

Quantum teleportation vs. direct transmission ?

- Hypotheses:
  - Each node produce 100 Bell pairs in a given period of time
  - Link loss: 90% (50 km fiber @ 0.2 dB/km)
  - Quantum teleportation loss: 50% (value chosen "arbitrary" here…)
- Efficiency for direct link between A and C: on average 1 usable Bell pair between A and C
- Efficiency with quantum teleportation: on average 5 usable Bell pairs between A and C

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

6. Architecture of a quantum internet [QI-archi, §5-7]

New challenges vs. classical networks

1. Bell pairs are not equivalent to payload carrying packets
   - No header “physically” attached to qubits ⇒ Need for out-of-band classical control channel

2. Store-and-forward vs. store-and-swap
   - Not directed store-and-forward with hop-by-hop transmission
   - But qubit storing and entanglement swapping (entanglement spreading, order of operations is not important…)

3. An entangled pair is only useful if the locations of both qubits are known
   - The communication entity (entangled pair of qubits) is spatially distributed!
   - Pairs of entangled qubits must be correctly identified
   - Coordination is required between end points

4. Generating entanglement requires temporary state
   - Because of the need for out-of-band classical control channel
   - This process cannot be stateless, it requires memory in nodes

6. Architecture of a quantum internet [QI-archi, §5-7]

Abstract model of a quantum network

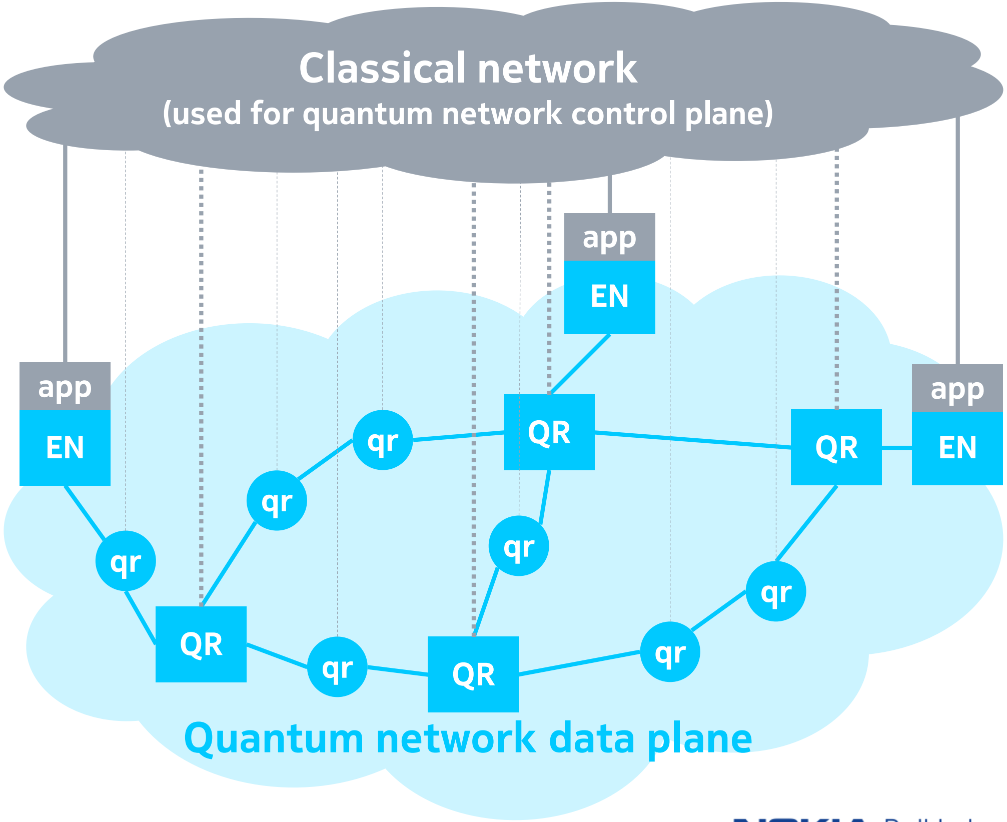
Network Elements

- Quantum Repeaters (qr, degree = 2)
  - – “Automated quantum node”
- Quantum Routers (QR, degree ≥ 2)
- End Nodes (EN)
- Non-Quantum Nodes (classical network)

Links

- Quantum Links
- Classical Links

User application (app) consuming the entangled pairs of qubits


Classical network
(used for quantum network control plane)
app
EN
app
EN
app
EN
QR
QR
QR
QR
qr
qr
qr
qr
qr
qr
qr
qr
Quantum network data plane

6. Architecture of a quantum internet [QI-archi, §5-7]

Current physical constraints

- Memory lifetimes
  - Decoherence = noise due to interactions with the environment.
  - The highest achievable values currently are on the order of seconds.
- Rates
  - Currently, the highest achievable rates of success between nodes capable of storing the resulting qubits are of the order of 10 Hz.
  - Combined with short memory lifetimes this leads to very tight timing windows to build up network-wide connectivity.
- Communication qubits
  - A given node may generate entanglement over the links one at a time…
- Homogeneity
  - Currently all hardware implementations are homogeneous.
  - Coupling different technologies may help overcome the weaknesses of the different implementations, but this may take a long time to be realized with high reliability and thus is not a near-term goal.

6. Architecture of a quantum internet [QI-archi, §5-7]

Goals of a quantum internet (architecture)

1. Support distributed quantum applications
2. Support tomorrow’s distributed quantum applications
3. Support hardware heterogeneity
4. Ensure security at the network level
5. Make them easy to manage and monitor
6. Ensure availability and resilience

6. Architecture of a quantum internet [QI-archi, §5-7]

Principles of a quantum internet

1. Entanglement (Bell pairs) is (are) the fundamental service (building blocks)
   - **The key service that a quantum network provides is the distribution of entanglement between the nodes in a network.**
2. Bell pairs are indistinguishable
   - Separation between bell pair creation in the network and bell pair usage by the applications.
3. Fidelity is part of the service
   - Fidelity ≈ Error rate for quantum networks…
4. Time is part of the service
   - The problem of decoherence ⇒ Limited time of quantum memory
5. Be flexible with regards to capabilities and limitations
   - Be able to function under the physical constraints imposed by the current generation hardware.
   - Be able to run the network over any hardware that may come along in the future.

6. Architecture of a quantum internet [QI-archi, §5-7]

Comparison with classical networks

Creating end-to-end Bell pairs between remote end-points is a stateful distributed task that requires a lot of a-priori coordination. Therefore, a **connection-oriented** approach seems the most natural for quantum networks.

MPLS-like?

- Quantum Virtual Circuit for end-to-end bell pair creation
- Multicast connections possible (N ≥ 2 end-points)
- Required QoS: number of Bell pairs per second and required fidelity
- Routing: optimal path
- Traffic Engineering, Call Admission Control…
- Forwarding rules
- Physical separation of data plane and control plane: GMPLS-like? (see control of WDM networks)

6. Architecture of a quantum internet [QI-archi, §5-7]

Security considerations

Intrinsic security from quantum physics

- Entangled qubits do not carry individual information but only correlation information
- Individual information is created after individual observation/measurement of the qubits!
- Measurement by an eavesdropper Eve can be detected by Alice and Bob:
  1. Alice and Bob can make measurements with random bases on some of the qubit pairs they share (randomly chosen by Alice or Bob, after reception of them)
  2. When their choices of random bases coincide (50% of the cases), they compare their results
  3. If they find some differences in the results, this means that Eve made some measurements on at least one of the qubits (if p is the proportion of intercepted qubits then p/4 is the proportion of different results)

Insecure quantum internet?

- It is still possible to attack the control protocols and violate the authenticity, confidentiality, and integrity of communication.
- The mechanism described above allow the detection of an intrusion if the end points are sure about the identity of each other and if the end points are secured

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

7. Applications and Use Cases for the Quantum Internet [QI-app]

Classification by application usage

1. Quantum Cryptography Applications to ensure secure communications
   - Secure communication setup, see Quantum Key Distribution (QKD).
   - Fast Byzantine negotiation: quantum network based method for fast agreement in Byzantine negotiations.
2. Quantum Sensor Applications to support distributed sensors or Internet of Things (IoT) devices
   - Network clock synchronization: world wide set of atomic clocks connected by the Quantum Internet to achieve an ultra precise clock signal.
3. Quantum Computing Applications to support remote quantum computing facilities
   - Distributed quantum computing: collection of remote small capacity quantum computers (i.e., each supporting a few qubits) that are connected and working together in a coordinated fashion so as to simulate a virtual large capacity quantum computer.
   - Secure quantum computing with privacy preservation: private, or blind, quantum computation, which provides a way for a client to delegate a computation task to one or more remote quantum computers without disclosing the source data to be computed over.

7. Applications and Use Cases for the Quantum Internet [QI-app]

Selected quantum internet use cases: QKD (BB4 & variants)

Secure Communication Setup: Quantum Key Distribution (QKD)

- QKD can securely establish a secret key between two quantum nodes, without physically transmitting it through the network and thus achieving the required security.
- QKD is the most mature feature of the quantum information technology, and has been commercially deployed in small-scale and short-distance deployments.
- More QKD use cases have been described in ETSI GS QKD 002

QKD process using entangled pairs of qubits (BB84):

1. Alice (*source quantum node*) transforms the secret key to qubits. Basically, for each classical bit in the secret key, Alice randomly selects one quantum computational basis and uses it to generate a qubit for the classical bit.
2. Alice sends (or teleports) one qubit of each pair to Bob (*destination quantum node*) via quantum channel.
3. Bob receives qubits and measures them based on its random quantum basis.
4. Bob informs the source node of its random quantum basis.
5. Alice informs the destination node which random quantum basis is correct.
6. Alice & Bob discard measurements using different quantum basis and store all remaining bits as the secret key.

7. Applications and Use Cases for the Quantum Internet [QI-app]

Selected quantum internet use cases: distributed quantum computing

Distributed Quantum Computing

- Noisy Intermediate-Scale Quantum (NISQ) computers distributed in different locations are available for sharing
- In order to gain higher computation power before fully fledged quantum computers become available, NISQ computers can be connected via classic and quantum channels.
- Scientists can leverage these connected NISQ computer to solve highly complex scientific computation problems such as analysis of chemical interactions for medical drug development

- Quantum teleportation can be used to teleport quantum bits from one location to another one

7. Applications and Use Cases for the Quantum Internet [QI-app]

Selected quantum internet use cases: secure quantum computing

Secure Quantum Computing with Privacy Preservation

- A client node with source data delegates the computation of the source data to a remote computation node.
- Furthermore, the client node does not want to disclose any source data to the remote computation node and thus preserve the source data privacy.
- There is no assumption or guarantee that the remote computation node is a trusted entity from the source data privacy perspective.

- There are some quantum ways to delegate calculation on qubits without discarding information on the source data.

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

8. Conclusion
Quantum internet

Principle of quantum internet

- **Quantum internet = distributed system to create fully entangled pairs of qubits between any pair of nodes in the network**
- Pair of end nodes consume the qubits of shared pairs for:
  - Quantum Key Distribution (QKD) for secure communication (most advanced 2nd generation quantum technology)
  - Quantum teleportation of qubits for (futuristic) distributed quantum processing

Technological status

- Too many technological barriers today: quantum memories with long time storage, high fidelity quantum devices, quantum transfer between different technologies…
- Some people have doubts about the utility of such a quantum internet
- My personal point of view: Quantum internet will be useful for long-distance QKD (short-distance QKD is already commercially available)

Outline

1. Quantum Internet Research Group @ IRTF
2. Why quantum networks at IRTF [QI-archi, §1]
3. Quantum information [QI-archi, §2]
4. What quantum networks are [QI-archi, §3]
5. Achieving quantum connectivity [QI-archi, §4]
6. Architecture of a quantum internet [QI-archi, §5-7]
7. Applications and Use Cases for the Quantum Internet [QI-app]
8. Conclusion

Appendices

Annexes
Outline

1. Qubits and Bell pairs (A3)
   - Quantum formalism with Hilbert spaces
2. No-cloning theorem (A5)
   - Demonstration using the quantum formalism
3. Quantum teleportation (A5)
   - Demonstration using the quantum formalism
4. Quantum-proof security (A6)
   - Demonstration using the quantum formalism

Qubits and Bell pairs

A3. Quantum Information
Qubits

Qubit = ray in a Hilbert space of dimension 2

- Vector representation of quantum state: $|\varphi\rangle \in \mathbb{C}^2$
  - Choice of the norm: normalized vectors, i.e., $\langle\varphi|\varphi\rangle$=1
  - Choice of the phase: free parameter, i.e., $|\varphi\rangle \cong e^{i\theta}\,|\varphi\rangle$ (same state represented by different vectors)
- Measurement basis = any $(|\varphi\rangle, |\psi\rangle) \in \mathbb{C}^2 \times \mathbb{C}^2$ such as $\langle\varphi|\varphi\rangle$=1, $\langle\psi|\psi\rangle$=1 and $\langle\varphi|\psi\rangle$=0
  - Identity decomposition: $I = |\varphi\rangle\langle\varphi| + |\psi\rangle\langle\psi|$
  - For all $|\chi\rangle \in \mathbb{C}^2$, $|\chi\rangle = |\varphi\rangle\langle\varphi||\chi\rangle + |\psi\rangle\langle\psi||\chi\rangle = \langle\varphi|\chi\rangle|\varphi\rangle + \langle\psi|\chi\rangle|\psi\rangle$
  - Probability of measuring $|\varphi\rangle$ (resp. $|\psi\rangle$) = $|\langle\varphi|\chi\rangle|^2$ (resp. $|\langle\psi|\chi\rangle|^2$)
- The natural basis is noted $(|0\rangle, |1\rangle)$
- Any maximally-complementary basis of the natural basis is $(|\varphi\rangle, |\psi\rangle)$ with
  - $|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\alpha}|1\rangle\right)$
  - $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i\alpha}|1\rangle\right)$

A3. Quantum Information

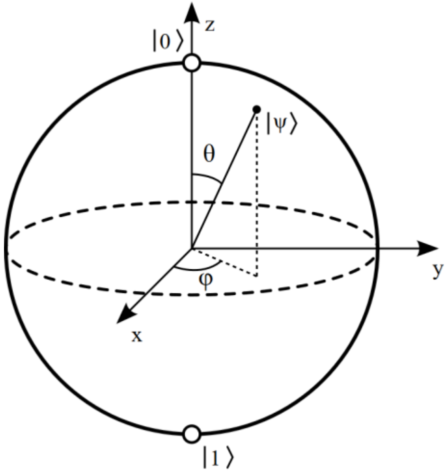
Qubits – Bloch sphere

Bloch sphere representation of qubits (equivalent to 1/2-spin particles)

- https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/blochsphere/blochsphere.html

$$|\psi\rangle = \left(e^{i\eta}\cdot\right)\begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)e^{i\varphi}\end{bmatrix} = \left(e^{i\eta}\cdot\right)\left(\cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\varphi}\,|1\rangle\right) \text{ with } \theta \in [0,\pi] \text{ and } \varphi \in [0,2\pi[.$$

- 3 mutually-maximally-complementary bases in the Bloch sphere:



Z-axis: $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$

Y-axis: $|i\rangle = |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|-i\rangle = |\leftarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$

X-axis: $|+\rangle = |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = |\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

A3. Quantum Information

Multiple qubits

Multiple (N) Qubits = ray in an Hilbert space of dimension 2^N

- State representation $|\varphi\rangle \in \mathbb{C}^{2^N}$
- Natural basis $\left|b_{N-1} \dots b_1 b_0\right\rangle = \left|b_{N-1}\right\rangle \otimes \cdots \otimes \left|b_1\right\rangle \otimes \left|b_0\right\rangle$ with $(b_i)_{0 \le i \le N-1} \in \{0,1\}^N$
- Separable state:$|\varphi\rangle = \left|\varphi_{N-1}\right\rangle \otimes \cdots \otimes \left|\varphi_1\right\rangle \otimes \left|\varphi_0\right\rangle$ with $\left(\left|\varphi_i\right\rangle\right)_{0 \le i \le N-1} \in (\mathbb{C}^2)^N$
- Entangled state: any other state… $(\mathbb{C}^2)^N \subset \mathbb{C}^{2^N}$, $(\mathbb{C}^2)^N \neq \mathbb{C}^{2^N}$, $\mathbb{C}^{2^N} = Vect\left((\mathbb{C}^2)^N\right)$
  - States = Rays: $N \times (2-1) = N$ vs. $2^N - 1$ complex numbers

A3. Quantum Information

Maximally entangled pairs of qubits (Bell pairs)

Pair ($N = 2$) of qubits = ray in a Hilbert space of dimension $2^2 = 4$

- Maximally-entangled state example: $|BP\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$
- Bell pairs = basis of $\mathbb{C}^{2^2}$:

$$\left(\tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle),\ \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle),\ \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle),\ \tfrac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)\right)$$

- Property (just calculation to get it…):

$$|BP\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}}(|i\rangle \otimes |-i\rangle + |-i\rangle \otimes |i\rangle)$$

- Another property: $\forall |\chi\rangle \in \mathbb{C}^2, |\langle\chi| \otimes \langle\chi|BP\rangle|^2 = \frac{1}{2}$
- If $|\chi\rangle = e^{i\beta}\big(\cos\theta\, e^{i\alpha}|0\rangle + \sin\theta\, e^{-i\alpha}|1\rangle\big)$, we note $|\chi'\rangle = e^{i\beta}\big(\sin\theta\, e^{i\alpha}|0\rangle - \cos\theta\, e^{-i\alpha}|1\rangle\big)$ to get a basis, $\frac{1}{\sqrt{2}}(|\chi\rangle \otimes |\chi\rangle + |\chi'\rangle \otimes |\chi'\rangle) = \frac{e^{i2\beta}}{\sqrt{2}}\big(e^{i\alpha}|0\rangle \otimes e^{i\alpha}|0\rangle + e^{-i\alpha}|1\rangle \otimes e^{-i\alpha}|1\rangle\big) = \frac{1}{\sqrt{2}}(|0'\rangle \otimes |0'\rangle + |1'\rangle \otimes |1'\rangle)$ with $|0'\rangle = e^{i(\alpha+\beta)}|0\rangle$ and $|1'\rangle = e^{i(-\alpha+\beta)}|1\rangle$ (change of phases…)

No-cloning theorem

A5. Achieving quantum connectivity

No-cloning theorem 1/2

Problem modeling

- The total Hilbert space is $H = H_{Preparation} \otimes H_A = H_{Garbage} \otimes H_A \otimes H_C$ where $H_A = \mathbb{C}^2$ models the qubit that Alice wants to clone, $H_C = \mathbb{C}^2$ models the clone of this qubit, $H_{Preparation}$ models the system that will be used for the cloning operation and $H_{Garbage}$ models this system after the cloning operation.
- The unknown qubit to be cloned is $|\varphi_A\rangle = a|0\rangle + b|1\rangle \in H_A$ with $(a, b) \in \mathbb{C}^2$ and $|a|^2 + |b|^2 = 1$
  - Known qubits can be easily cloned: any qubit can be produced…
- The initial state in $H_{Preparation}$ is $|\varphi_P\rangle \in H_{Preparation}$
- The input state is thus $|\psi_{in}\rangle = |\varphi_P\rangle \otimes |\varphi_A\rangle = a|\varphi_P\rangle \otimes |0\rangle + b|\varphi_P\rangle \otimes |1\rangle$
- If cloning is possible, the output state after cloning processing should be $|\psi_{out}\rangle = |\varphi_G(a, b)\rangle \otimes |\varphi_A\rangle \otimes |\varphi_A\rangle$

$$= a^2|\varphi_G(a, b)\rangle \otimes |0\rangle \otimes |0\rangle + ab|\varphi_G(a, b)\rangle \otimes (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) + b^2|\varphi_G(a, b)\rangle \otimes |1\rangle \otimes |1\rangle$$

A5. Achieving quantum connectivity

No-cloning theorem 2/2

Impossibility of cloning

- Case $a = 1$ and $b = 0$:
  $\left|\psi_{in}\right\rangle = \left|\varphi_P\right\rangle \otimes \left|\varphi_A\right\rangle = \left|\varphi_P\right\rangle \otimes |0\rangle$
  $$\left|\psi_{out}\right\rangle = |\varphi_G(1,0)\rangle \otimes |0\rangle \otimes |0\rangle$$
- Case $a = 0$ and $b = 1$:
  $\left|\psi_{in}\right\rangle = \left|\varphi_P\right\rangle \otimes \left|\varphi_A\right\rangle = \left|\varphi_P\right\rangle \otimes |0\rangle$
  $$\left|\psi_{out}\right\rangle = |\varphi_G(0,1)\rangle \otimes |1\rangle \otimes |1\rangle$$
- Superposition principle (the evolution operator is linear) for any $(a, b) \in \mathbb{C}^2$ with $a \neq 0$ and $b \neq 0$:
  $\left|\psi_{in}\right\rangle = \left|\varphi_P\right\rangle \otimes \left|\varphi_A\right\rangle = a\left|\varphi_P\right\rangle \otimes |0\rangle + b\left|\varphi_P\right\rangle \otimes |1\rangle$ implies
  $$\left|\psi_{out}\right\rangle = a|\varphi_G(1,0)\rangle \otimes |0\rangle \otimes |0\rangle + b|\varphi_G(0,1)\rangle \otimes |1\rangle \otimes |1\rangle$$
  $$\neq a^2|\varphi_G(a,b)\rangle \otimes |0\rangle \otimes |0\rangle + \underset{ab \neq 0}{ab}|\varphi_G(a,b)\rangle \otimes (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) + b^2|\varphi_G(a,b)\rangle \otimes |1\rangle \otimes |1\rangle$$

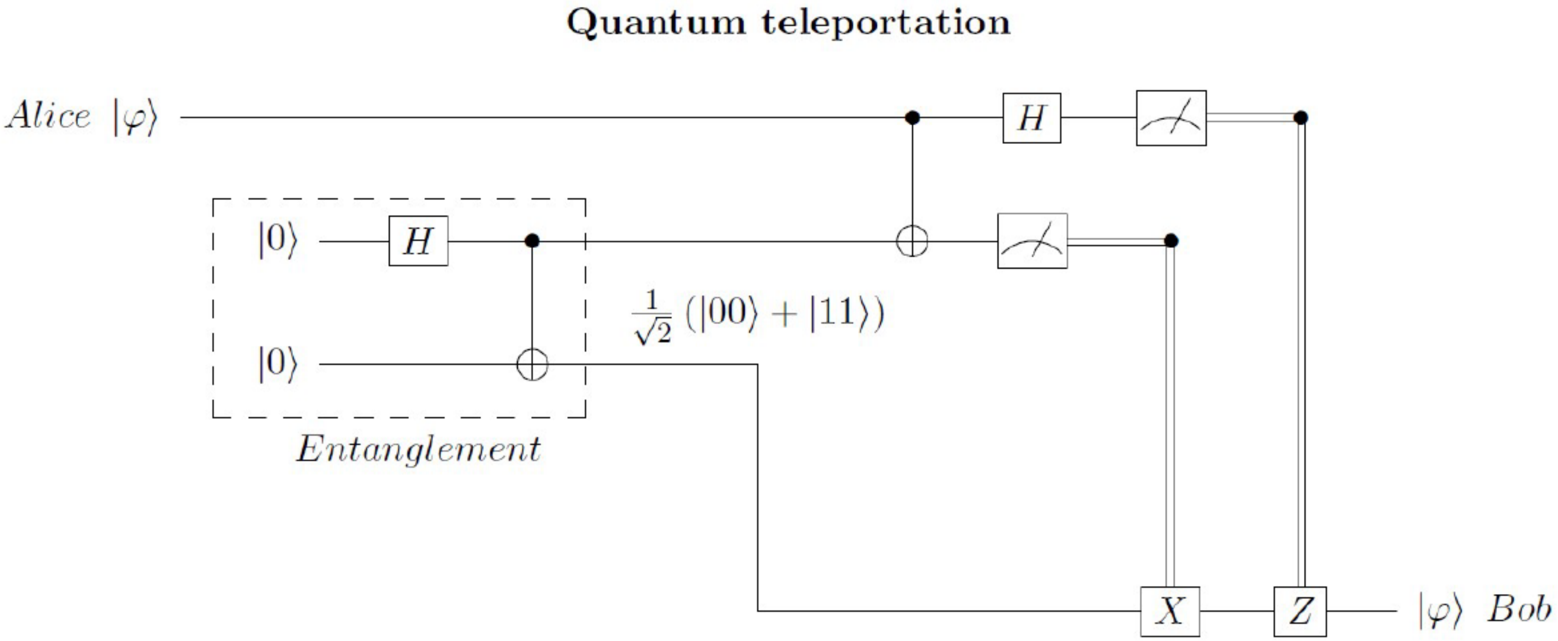
$\Rightarrow$ **Thus cloning of unknown qubit is impossible.**

Quantum teleportation

A5. Achieving quantum connectivity

Teleportation

Diagram of quantum teleportation on 1 qubit



A5. Achieving quantum connectivity

Teleportation processing

Problem modeling

- The total Hilbert space is $H = H_I \otimes H_A \otimes H_B$ where $H_I = \mathbb{C}^2$ models the “Input” qubit that Alice wants to teleport to Bob, and $H_A = \mathbb{C}^2$ and $H_B = \mathbb{C}^2$ model the entangled qubits owned by Alice and Bob.
- The unknown qubit to be teleported is $|\varphi_I\rangle = a|0\rangle + b|1\rangle$ with $(a, b) \in \mathbb{C}^2$ and $|a|^2 + |b|^2 = 1$
- The initial state in $H_A \otimes H_B$ is the Bell pair $\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$
- The input state is $|\psi_{in}\rangle = |\varphi_I\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$,

  i.e., $|\psi_{in}\rangle = \frac{a}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{a}{\sqrt{2}}|0\rangle \otimes |1\rangle \otimes |1\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |1\rangle \otimes |1\rangle$

A5. Achieving quantum connectivity

Teleportation processing 2/5

Quantum processing by Alice

- The initial state is $|\psi_{in}\rangle = \frac{a}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{a}{\sqrt{2}}|0\rangle \otimes |1\rangle \otimes |1\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |1\rangle \otimes |1\rangle$
- C-NOT gate on $H_I \otimes H_A : OP_{A,1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \otimes Id_B$, which gives

$$\left|\psi_{A,1}\right\rangle = OP_{A,1}|\psi_{in}\rangle = \frac{a}{\sqrt{2}}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |1\rangle \otimes |0\rangle + \frac{a}{\sqrt{2}}|0\rangle \otimes |1\rangle \otimes |1\rangle + \frac{b}{\sqrt{2}}|1\rangle \otimes |0\rangle \otimes |1\rangle$$

- Hadamard gate on $H_I : OP_{A,2} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes Id_A \otimes Id_B$, which gives

$$\left|\psi_{A,2}\right\rangle = OP_{A,2}\left|\psi_{A,1}\right\rangle = \frac{a}{2}|0\rangle \otimes |0\rangle \otimes |0\rangle + \frac{a}{2}|1\rangle \otimes |0\rangle \otimes |0\rangle + \frac{b}{2}|0\rangle \otimes |1\rangle \otimes |0\rangle - \frac{b}{2}|1\rangle \otimes |1\rangle \otimes |0\rangle$$
$$+ \frac{a}{2}|0\rangle \otimes |1\rangle \otimes |1\rangle + \frac{a}{2}|1\rangle \otimes |1\rangle \otimes |1\rangle + \frac{b}{2}|0\rangle \otimes |0\rangle \otimes |1\rangle - \frac{b}{2}|1\rangle \otimes |0\rangle \otimes |1\rangle, \text{ i.e.,}$$

$$\left|\psi_{A,2}\right\rangle = \frac{1}{2}|0\rangle \otimes |0\rangle \otimes (a|0\rangle + b|1\rangle) + \frac{1}{2}|0\rangle \otimes |1\rangle \otimes (b|0\rangle + a|1\rangle)$$
$$+ \frac{1}{2}|1\rangle \otimes |0\rangle \otimes (a|0\rangle - b|1\rangle) + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes (-b|0\rangle + a|1\rangle)$$

A5. Achieving quantum connectivity
Teleportation processing

3/5

Measurements by Alice

- $\left|\psi_{A,2}\right\rangle = \frac{1}{2}|0\rangle \otimes |0\rangle \otimes (a|0\rangle + b|1\rangle) + \frac{1}{2}|0\rangle \otimes |1\rangle \otimes (b|0\rangle + a|1\rangle)$
  $+ \frac{1}{2}|1\rangle \otimes |0\rangle \otimes (a|0\rangle - b|1\rangle) + \frac{1}{2}|1\rangle \otimes |1\rangle \otimes (-b|0\rangle + a|1\rangle)$
- Measurements of qubits I and A: 4 possibilities with 25% probability each
  - $\left|\psi_{A,3}\,(0,0)\right\rangle = |0\rangle \otimes |0\rangle \otimes (a|0\rangle + b|1\rangle)$
  - $\left|\psi_{A,3}\,(0,1)\right\rangle = |0\rangle \otimes |1\rangle \otimes (b|0\rangle + a|1\rangle)$
  - $\left|\psi_{A,3}\,(1,0)\right\rangle = |1\rangle \otimes |0\rangle \otimes (a|0\rangle - b|1\rangle)$
  - $\left|\psi_{A,3}\,(1,1)\right\rangle = |1\rangle \otimes |1\rangle \otimes (-b|0\rangle + a|1\rangle)$
  - i.e., $\left|\psi_{A,3}\,(x,y)\right\rangle = |x\rangle \otimes |y\rangle \otimes |\varphi(x,y)\rangle$
- Alice sends to Bob the measured bits $|x\rangle \otimes |y\rangle$

A5. Achieving quantum connectivity

Teleportation processing

4/5

Quantum processing by Bob

- $\left|\psi_{A,3}\,(x,y)\right\rangle = |x\rangle \otimes |y\rangle \otimes |\varphi(x,y)\rangle \in H_I \otimes H_A \otimes H_B$ with $|\varphi(0{,}0)\rangle = a|0\rangle + b|1\rangle$, $|\varphi(0{,}1)\rangle = b|0\rangle + a|1\rangle$, $|\varphi(1{,}0)\rangle = a|0\rangle - b|1\rangle$ and $|\varphi(1{,}1)\rangle = -b|0\rangle + a|1\rangle$
- C-NOT gate on $H_A \otimes H_B : OP_{B,1/A\otimes B} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, which gives
  - $\left|\psi_{B,1}\,(0{,}0)\right\rangle = OP_{B,1/A\otimes B}\left|\psi_{A,3}\,(0{,}0)\right\rangle = |0\rangle \otimes |0\rangle \otimes (a|0\rangle + b|1\rangle)$
  - $\left|\psi_{B,1}\,(0{,}1)\right\rangle = OP_{B,1/A\otimes B}\left|\psi_{A,3}\,(0{,}1)\right\rangle = |0\rangle \otimes |1\rangle \otimes (a|0\rangle + b|1\rangle)$
  - $\left|\psi_{B,1}\,(1{,}0)\right\rangle = OP_{B,1/A\otimes B}\left|\psi_{A,3}\,(1{,}0)\right\rangle = |1\rangle \otimes |0\rangle \otimes (a|0\rangle - b|1\rangle)$
  - $\left|\psi_{B,1}\,(1{,}1)\right\rangle = OP_{B,1/A\otimes B}\left|\psi_{A,3}\,(1{,}1)\right\rangle = |1\rangle \otimes |1\rangle \otimes (a|0\rangle - b|1\rangle)$

A5. Achieving quantum connectivity

Teleportation processing

Quantum processing by Bob

- $\left|\psi_{B,1}(x,y)\right\rangle = |x\rangle \otimes |y\rangle \otimes |\varphi'(x,y)\rangle \in H_I \otimes H_A \otimes H_B$ with $|\varphi'(0,0)\rangle = |\varphi'(0,1)\rangle = a|0\rangle + b|1\rangle$ and $|\varphi'(1,0)\rangle = |\varphi'(1,1)\rangle = a|0\rangle - b|1\rangle$
- C-Z gate on $H_I \otimes H_B : OP_{B,2/I\otimes B} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$, which gives
  - $\left|\psi_{B,2}(0,y)\right\rangle = OP_{B,2/I\otimes B}\left|\psi_{B,1}(0,y)\right\rangle = |0\rangle \otimes |y\rangle \otimes (a|0\rangle + b|1\rangle)$
  - $\left|\psi_{B,2}(1,y)\right\rangle = OP_{B,2/I\otimes B}\left|\psi_{B,1}(1,y)\right\rangle = |1\rangle \otimes |y\rangle \otimes (a|0\rangle + b|1\rangle)$
- Finally we obtain $\left|\psi_{Out}\right\rangle = \left|\psi_{B,2}(x,y)\right\rangle = |x\rangle \otimes |y\rangle \otimes (a|0\rangle + b|1\rangle) = |x\rangle \otimes |y\rangle \otimes \left|\varphi_I\right\rangle$
- The qubit $\left|\varphi_I\right\rangle$ has been teleported from Alice to Bob.

Quantum-proof security

A6. Architecture of a quantum internet [QI-archi, §5-7]

Intrinsic (quantum-proof) security of entangled pairs 1/3

Problem to solve

- Alice and Bob share a Bell pair that they will consume to share 1 bit of information
- Eve has access to this Bell pair before Alice and Bob consume it
  - Full power: Eve can process the Bell pair as she wants, but then needs to give a Bell pair to Alice and Bob.
  - In some case Eve may have access to only one of the qubit, but this case is only a subcase of the "full power" one where Eve let unchanged one of the qubit of the Bell pair
- Is there a process that Eve can use to get the information Alice and Bob will produce by consuming it, without being detected by Alice and Bob?

Problem modeling

- The total Hilbert space is $H = H_A \otimes H_B \otimes H_E$ where $H_A = \mathbb{C}^2$ and $H_B = \mathbb{C}^2$ model the qubits that Alice and Bob will receive, and H_E models the physical system (Eve's apparatus) that Eve uses to try to eavesdrop the results of measurements that Alice and Bob will perform.
  - Note: Everything is quantum physics, classical physics is just an approximation !!!

A6. Architecture of a quantum internet [QI-archi, §5-7]

Intrinsic (quantum-proof) security of entangled pairs 2/3

Demonstration of the (statistical) impossibility of eavesdropping without being detected

- Eve must deliver two qubits to Alice and Bob (one for each) that mimics a Bell pair.
- In the natural basis, the generic form of any output state will be:
  $$|\Psi\rangle = a|0\rangle \otimes |0\rangle \otimes \left|\chi_{00}\right\rangle + b|0\rangle \otimes |1\rangle \otimes \left|\chi_{01}\right\rangle + c|1\rangle \otimes |0\rangle \otimes \left|\chi_{10}\right\rangle + d|1\rangle \otimes |1\rangle \otimes \left|\chi_{11}\right\rangle$$
  with $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$
- If both Alice and Bob choose the measurement basis $(|0\rangle, |1\rangle)$, they cannot measure $|0\rangle \otimes |1\rangle$ nor $|1\rangle \otimes |0\rangle$, which implies $b = c = 0$ to avoid a non-null probability of eavesdropping detection.
- With $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, i.e., $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$, we have $|\Psi\rangle = a|0\rangle \otimes |0\rangle \otimes \left|\chi_{00}\right\rangle + d|1\rangle \otimes |1\rangle \otimes \left|\chi_{11}\right\rangle$
  $$= \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle) \otimes \frac{a\left|\chi_{00}\right\rangle + d\left|\chi_{11}\right\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}(|+\rangle \otimes |-\rangle + |-\rangle \otimes |+\rangle) \otimes \frac{a\left|\chi_{00}\right\rangle - d\left|\chi_{11}\right\rangle}{\sqrt{2}}$$
- If both Alice and Bob choose another measurement basis $(|+\rangle, |-\rangle)$, maximally complementary to the basis $(|0\rangle, |1\rangle)$, they cannot measure $|+\rangle \otimes |-\rangle$ nor $|-\rangle \otimes |+\rangle$, which implies $a\left|\chi_{00}\right\rangle = d\left|\chi_{11}\right\rangle$ to avoid a non-null probability of eavesdropping detection.

A6. Architecture of a quantum internet [QI-archi, §5-7]

Intrinsic (quantum-proof) security of entangled pairs 3/3

No possible eavesdropping without being detected

- Finally, $|\Psi\rangle = |BP\rangle \otimes |\chi_E\rangle$ with $|BP\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle)$ being the Bell pair delivered to Alice and Bob, and $|\chi_E\rangle = a\sqrt{2}|\chi_{00}\rangle = d\sqrt{2}|\chi_{11}\rangle$ being the final state of Eve's apparatus.
- Relatively to the tensor product decomposition $H = H_{AB} \otimes H_E$ where $H_{AB} = H_A \otimes H_B$, the final quantum state $|\Psi\rangle = |BP\rangle \otimes |\chi_E\rangle$ is a separable state, i.e., there is no information correlation between $|BP\rangle$ and $|\chi_E\rangle$.
- In other words, any measurement on $|\chi_E\rangle$ cannot bring any information about the outcomes of measurements on $|BP\rangle$.
- This means that if Eve wishes to be undetectable by Alice and Bob with 100% probability, she cannot get any information about Alice and Bob measurements on the Bell pair $|BP\rangle$.
  - Provided that Eve do not know in advance the choice of measurement basis by Alice and Bob (implicit hypothesis in the demonstration), which is true if Alice and Bob use quantum random bit generator after receiving the Bell pair…
  - And provided that quantum mechanics cannot be contradicted…

NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback"). Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.