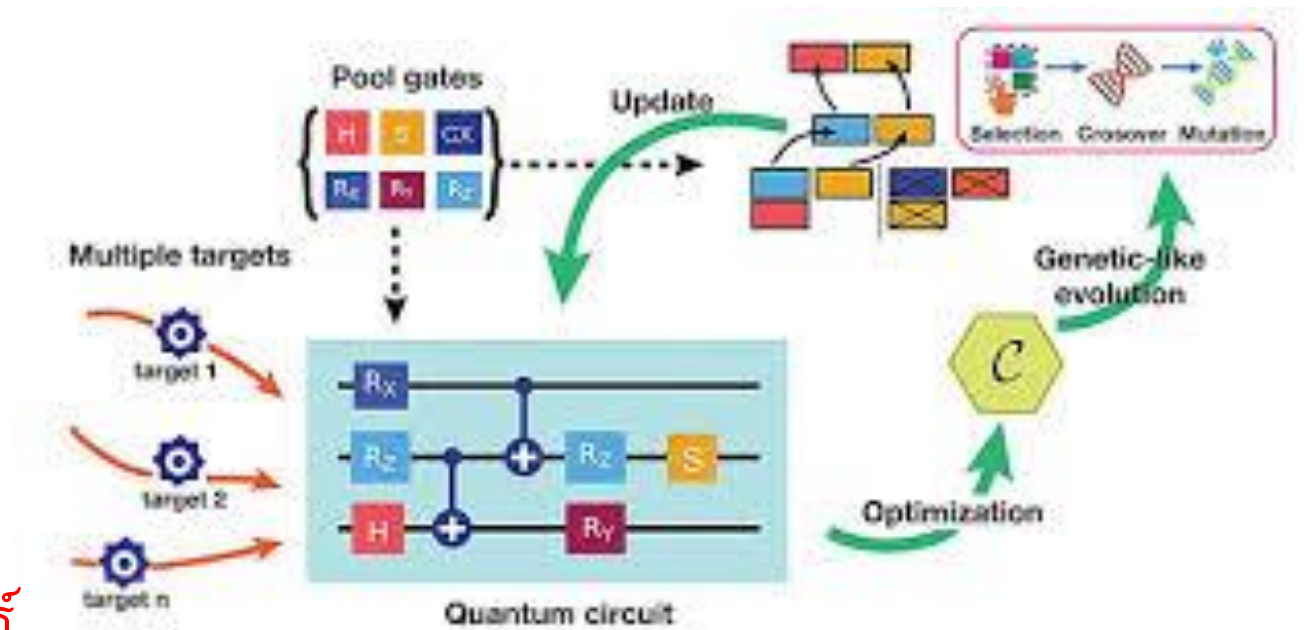


บทที่ 8 SUMMARY & NEXT STEPS

ผู้ช่วยศาสตราจารย์จุฑาภูมิ จันทรมานี

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสวนดุสิต



Pre-Session Quiz

- 1) What are some use-cases for quantum networks?
- 2) What are some of the special properties of quantum bits (Qubits)?
- 3) What makes a quantum computer so fast?
- 4) What is Y2Q? And when do most experts expect it?
- 5) Can you transmit information faster than light with quantum teleporting?
- 6) Will quantum networks replace classical networks?
- 7) What is Cisco researching and developing in Quantum?

Post Session Quiz / Summary

1) What are some use-cases for quantum networks?

Quantum Cryptography

- Quantum networks can be used to securely exchange cryptographic keys, as these are mathematically proven to detect and prevent eavesdropping
- The most well-known method of this application is *Quantum Key Distribution (QKD)*



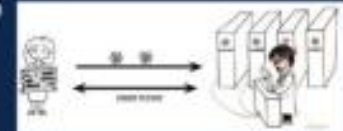
Distributed Quantum Computing

- Interconnecting geographically-dispersed quantum computers to realize benefits such as:
 - Increased Processing Power
 - Distributed Quantum Computing
 - Specialized Quantum Modules
 - Fault Tolerance
 - Hybrid Quantum-Classical Systems
 - Etc.



Blind Quantum Computing

- A privacy-preserving method in which a client can delegate a computation task to remote quantum computer(s) without disclosing the source data or algorithms
- The results of the computations would likewise be private



Network Clock Synchronization

- A world-wide set of high-precision clocks connected by quantum networks could achieve ultra precise clock signals
- Current accuracy: ± 30 ns
- Quantum accuracy: ± 1 ps



Distributed Sensing

- Signals from distributed sensors can be combined via quantum networks to obtain higher-accuracy measurements than currently possible with classical network interconnections
- E.g. Telescope Array
 - Classical precision: $\pm 1/\sqrt{N}$
 - Quantum precision: $\pm 1/N$



Quantum Money

- The main security requirement of money is unforgeability
- A quantum money scheme aims to fulfill by this requirement by exploiting the no-cloning property of the unknown quantum states

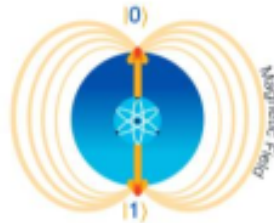


Post Session Quiz / Summary

2) What are some of the special properties of quantum bits (Qubits)?

Quantum Special Property: Superposition

- As long a Qubit is unobserved (i.e. unmeasured) it is in a "Superposition" of probabilities for 0 and 1
- The instant a Qubit is measured, the superposition will collapse into one of the two discrete states



CISCO Live!

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Quantum Special Property: Entanglement

- Entanglement is a physical relationship between Qubits where they react to a change in the other(s) state instantaneously regardless of how far they are apart
- Multiple qubits can become entangled with each other
 - The current record is 54
- If an entangled Qbit is measured, then entanglement collapses



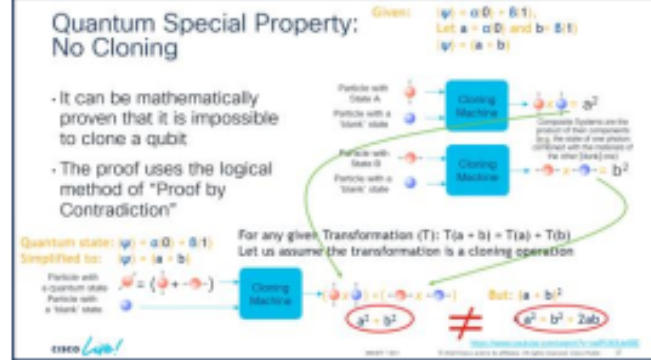
<https://www.research.com/s/54-qubit-entangled-network-of-qubits-entangled-in-a-quantum-computer>

CISCO Live!

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Quantum Special Property: No Cloning

- It can be mathematically proven that it is impossible to clone a qubit
- The proof uses the logical method of "Proof by Contradiction"



CISCO Live!

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Post Session Quiz / Summary

3) What makes a quantum computer so fast?

Quantum Parallelism

QUBIT #1
Holds & operates on values of 0 and 1 simultaneously

QUBIT #1 **QUBIT #2**
Holds & operates on values of 00, 01, 10, 11 simultaneously

QUBIT #1 **QUBIT #2** **QUBIT #3**
Holds & operates on values of 000, 001, 010, 011, 100, 101, 110, 111 simultaneously

Interference Manipulation

Another benefit that can be realized by quantum computing comes from manipulating interference

Interference may be

- constructive or
- destructive

Quantum algorithms (like Grover's and Shor's) endeavor to arrange qubits so that:

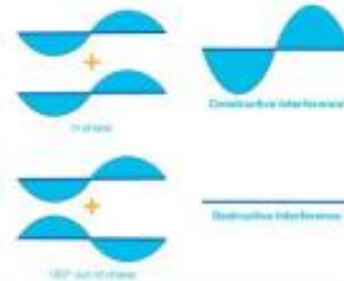
- wanted answers generate constructive interference
- undesired answers generate destructive interference

Remember: Probability = Amplitude²

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

Sum of the squares of the amplitudes must equal 1

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



Post Session Quiz / Summary

4) What is Y2Q? And when do most experts expect it?

Y2Q, CRQC and SNDL

- Years to Quantum (Y2Q) refers to the unknown number of years before there is any Cryptographically Relevant Quantum Computers (CRQC)
- A CRQC can compute prime factorizations and discrete logarithms in polynomial time by Shor's algorithm, thereby rendering public key algorithms all but obsolete
- However, an adversary can capture network traffic today in the hopes of decrypting it later with a CRQC; this is a Store Now, Decrypt Later (SNDL) type of attack, and means that sensitive data is vulnerable right now to future quantum threats
- Sometimes this method is also referred to as Harvest Now Decrypt Later (HNDL)

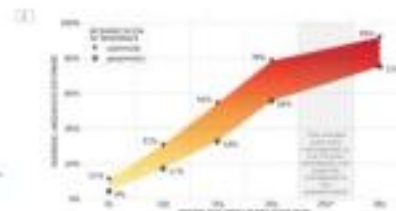


CSA Logo

© 2020 Cloud Security Alliance. All rights reserved.

How Many Y2Q?

- Cloud Security Alliance:
 - April 14, 2030
- Global Risk Inst:
 - ~50% within 15 years
- White House / NIST
 - "in the not-too-distant future"



Source: Cloud Security Alliance, "Quantum Computing Threats to Cybersecurity", April 2020

CSA Logo

CSA Logo

© 2020 Cloud Security Alliance. All rights reserved.

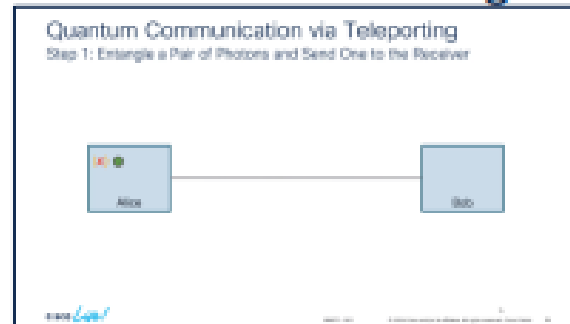
Post Session Quiz / Summary

5) Can you transmit information faster than light with quantum teleporting?

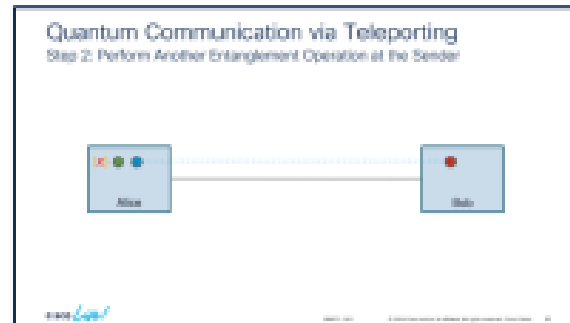
Key Takeaway:

Quantum teleportation does NOT enable faster than light communication

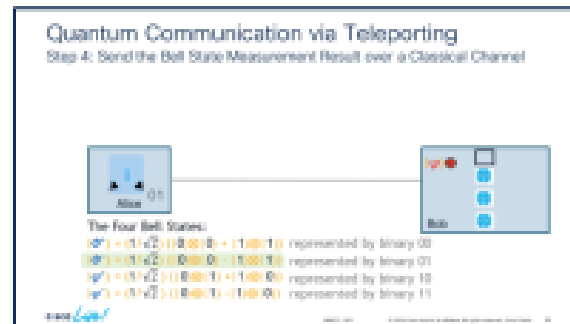
In fact, **for every bit** of information sent via **quantum** teleportation, **at least 3 additional bits** of data must be sent over **classical** channels



Equivalent to sending (at least) one bit over a classical channel



Teleporting one of 4 random states does occur faster than light, but (strictly speaking) this not an information transfer on its own merit, since we cannot correctly interpret what has been sent without additional data



(At least) Two more bits of data are sent over a classic channel

Post Session Quiz / Summary

6) Will quantum networks replace classical networks?

Key Takeaway:

Quantum teleportation does NOT enable faster than light communication

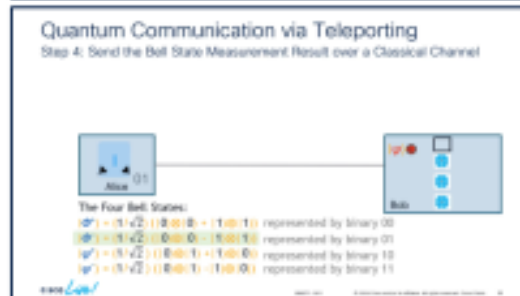
In fact, **for every bit** of information sent via **quantum** teleportation, **at least 3 additional bits of data must be sent over classical channels**



Equivalent to sending (at least) one bit over a **classical channel**



Teleporting one of 4 random states does occur faster than light, but (strictly speaking) this not an information transfer on its own merit, since we cannot correctly interpret what has been sent without additional data



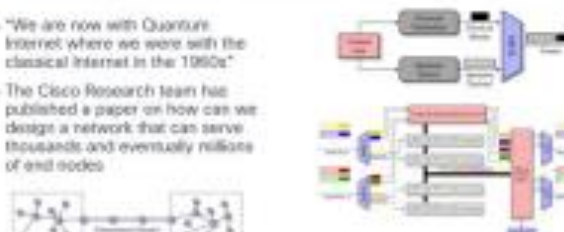
(At least) Two more bits of data are sent over a **classic channel**

Post Session Quiz / Summary

7) What is Cisco researching and developing in Quantum?

Modelling a Unified Classical & Quantum Internet

- "We are now with Quantum Internet where we were with the classical Internet in the 1990s"
- The Cisco Research team has published a paper on how can we design a network that can serve thousands and eventually millions of end nodes



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Planning Quantum Networks Over Existing Fiber Networks

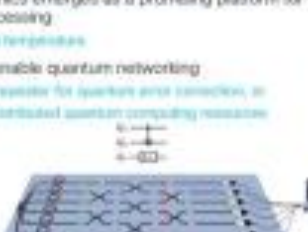
- In another paper, the Cisco Research team developed a framework to guide the first steps of planning a quantum network using the existing optical network infrastructure
- This framework was formulated as an optimization problem
- Specifically an integer Linear Programming (ILP) problem



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Photonic Quantum Processors

- Quantum photonics emerges as a promising platform for scalable quantum information processing
- possibility of room temperature
- These directly enable quantum networking
- Be working as a repeater for quantum entanglement, or
- as a server for distributed quantum computing resources



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Quantum Network Design Kit (QDNK) Simulator



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Quantum Research Lab

- Cisco announced the opening of a Quantum Research Lab in March 2023 in Santa Monica, CA



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

(One-Way) Quantum Repeaters

- Quantum Repeaters leverage Quantum Error Correction, where encoded quantum information is transmitted in the form of multi-photon states
- Only information is decoded at the end-nodes
- Intermediate repeater stations check the incoming state for errors and prepare a fresh encoded qubit as the output to be sent to the next repeater
- This does NOT violate the No-Cloning Theorem, as quantum repeaters perform a multi-qubit measurement that does not disturb the quantum information in the encoded state, but rather, retrieves indirect information about a potential error



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

