What is Cisco Doing in Quantum?

An Introduction to Quantum Mechanics, Computing, and Networking

Tim Szigeti
Distinguished Engineer

Session ID: BRKETI-1401

Cisco Webex App

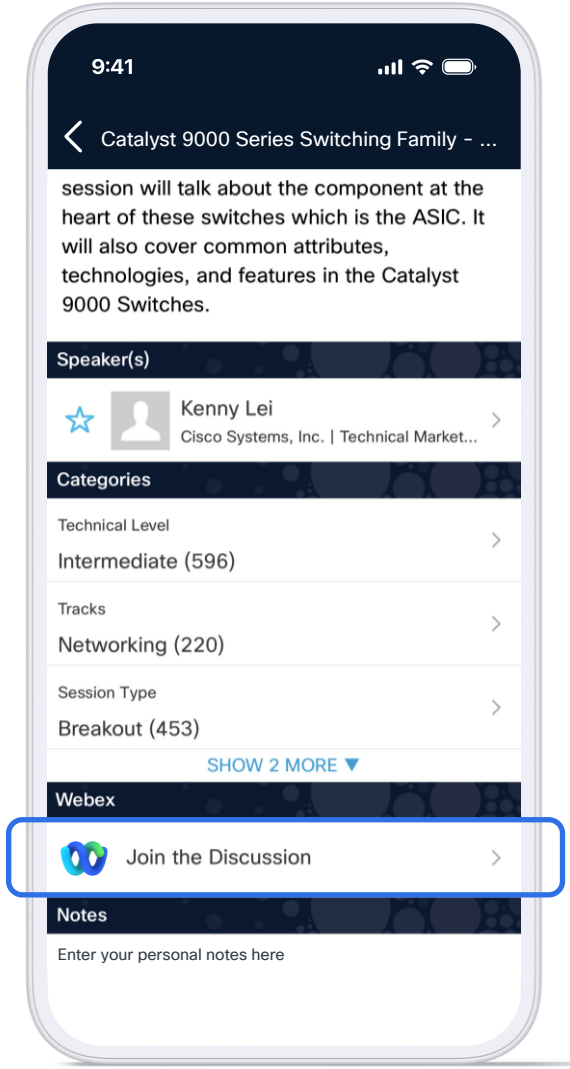
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKETI-1401**

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco’s Mission for Quantum Networking

Our goal is to provide high-rate, high-fidelity entanglement distribution over a scalable, multi-tenant, multi-user architecture.

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Why build quantum networks

02 Intro to quantum mechanics

03 Intro to quantum computing

04 Implications of quantum computing on cybersecurity

05 Intro to quantum networking

06 What is Cisco doing in quantum?

07 Summary / Post-session quiz

© 2025 Cisco and/or its affiliates. All rights reserved.

Pre-Session Quiz

1) Why build quantum networks?
2) What are some of the special properties of quantum bits (qubits)?
3) What makes a quantum computer so fast?
4) Does quantum compute threaten RSA and AES?
5) What is Y2Q? And when do most experts expect it?
6) What are three requirements for quantum safety?
7) When do Australian networks need to be quantum safe?
8) Can you transmit information faster than light with quantum teleporting?
9) Will quantum networks replace classical networks?
10) What is Cisco researching and developing in quantum?

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build 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)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Distributed Quantum Computing

Interconnecting quantum computers to collectively empower:

- Simulations:
  - Chemical/Molecular Engineering
  - Weather forecasting
  - Financial Modelling
  - Etc.
- Optimizations
- AI/ML
- Cryptography (i.e. decryption)

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Network Clock Synchronization

A world-wide set of high-precision clocks connected by quantum networks could achieve ultra precise clock signals

Current accuracy: 10 ns to 500 ps

Quantum accuracy: ≤1ps

https://ieeexplore.ieee.org/document/9756507

© 2025 Cisco and/or its affiliates. All rights reserved.

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. Deep Space Telescope Array

- Classical precision: $\pm\ 1/\sqrt{N}$
- Quantum precision: $\pm\ 1/N$

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Money

The main security requirement of money is unforgeability

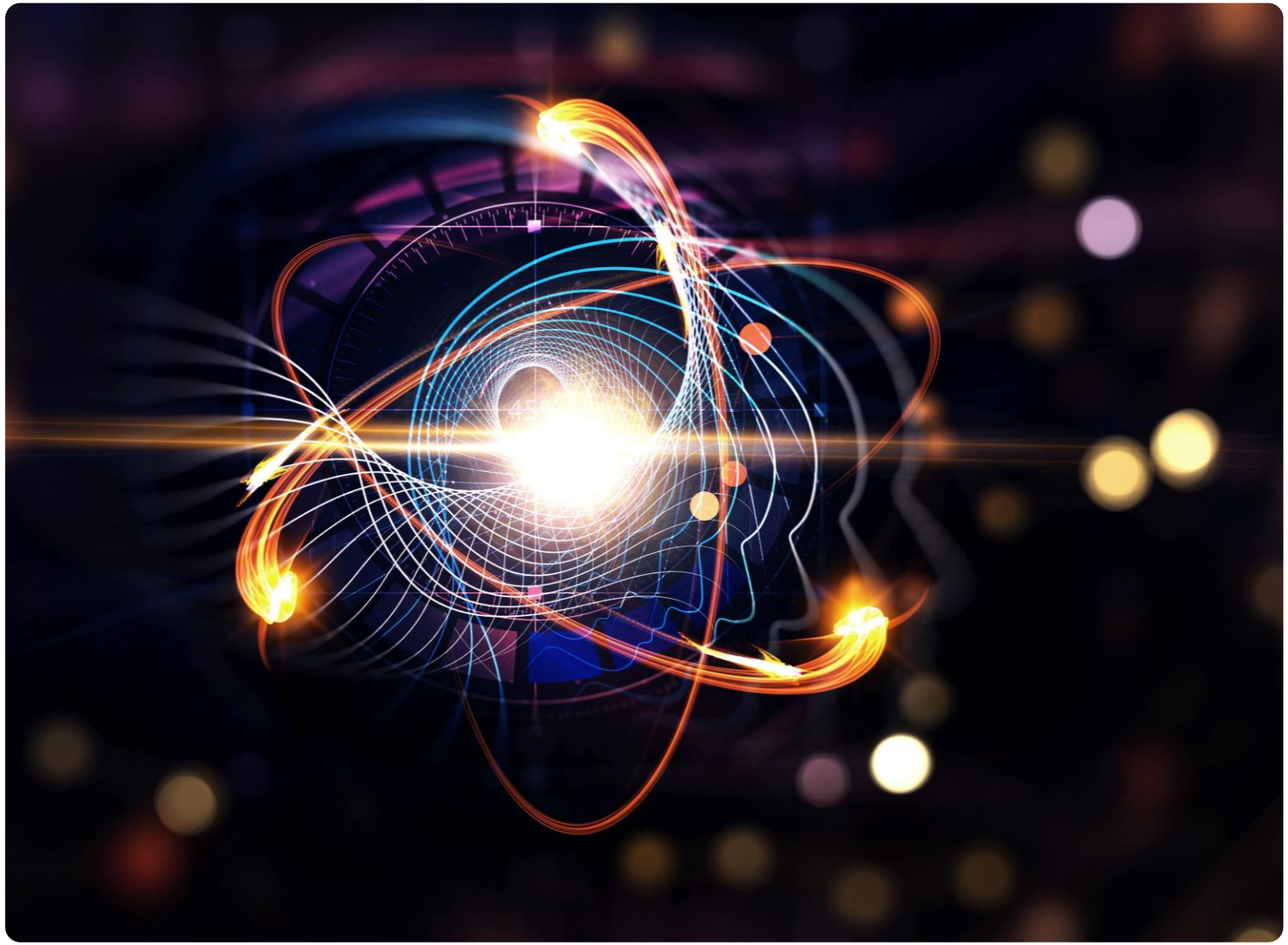
A quantum money scheme aims to fulfill by this requirement by exploiting the no-cloning property of unknown quantum states

© 2025 Cisco and/or its affiliates. All rights reserved.

An Introduction to Quantum Mechanics

CISCO Live !

What is Quantum Mechanics?



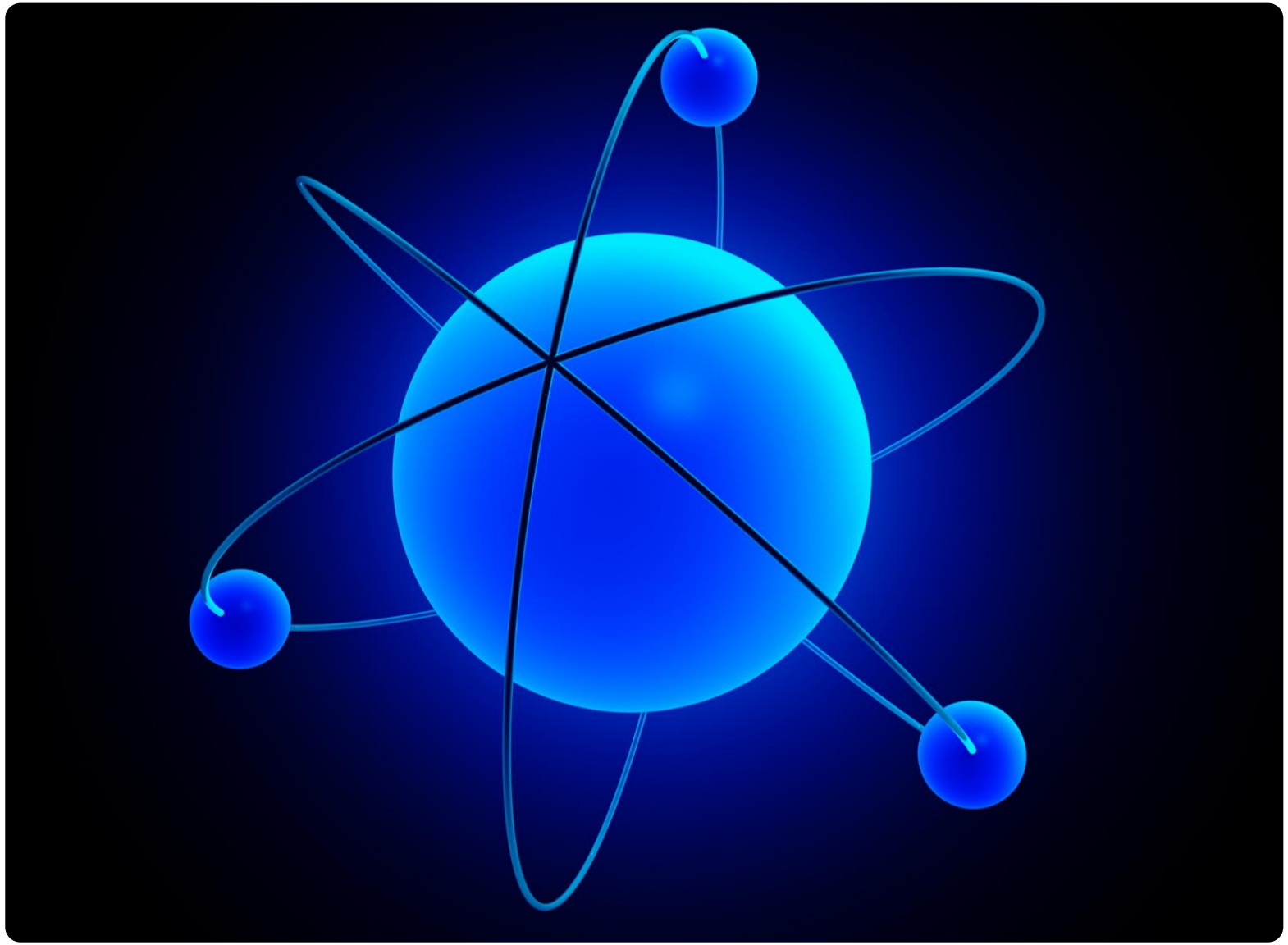
Quantum mechanics is the field of physics that explains how subatomic objects simultaneously have the characteristics of both:

- Particles—tiny pieces of matter, and
- Waves—variations that transfer energy

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Bits (Qubits)



Any quantum particle that can be measured and expressed as being in one of two discrete states

- 0 or 1

These can include:

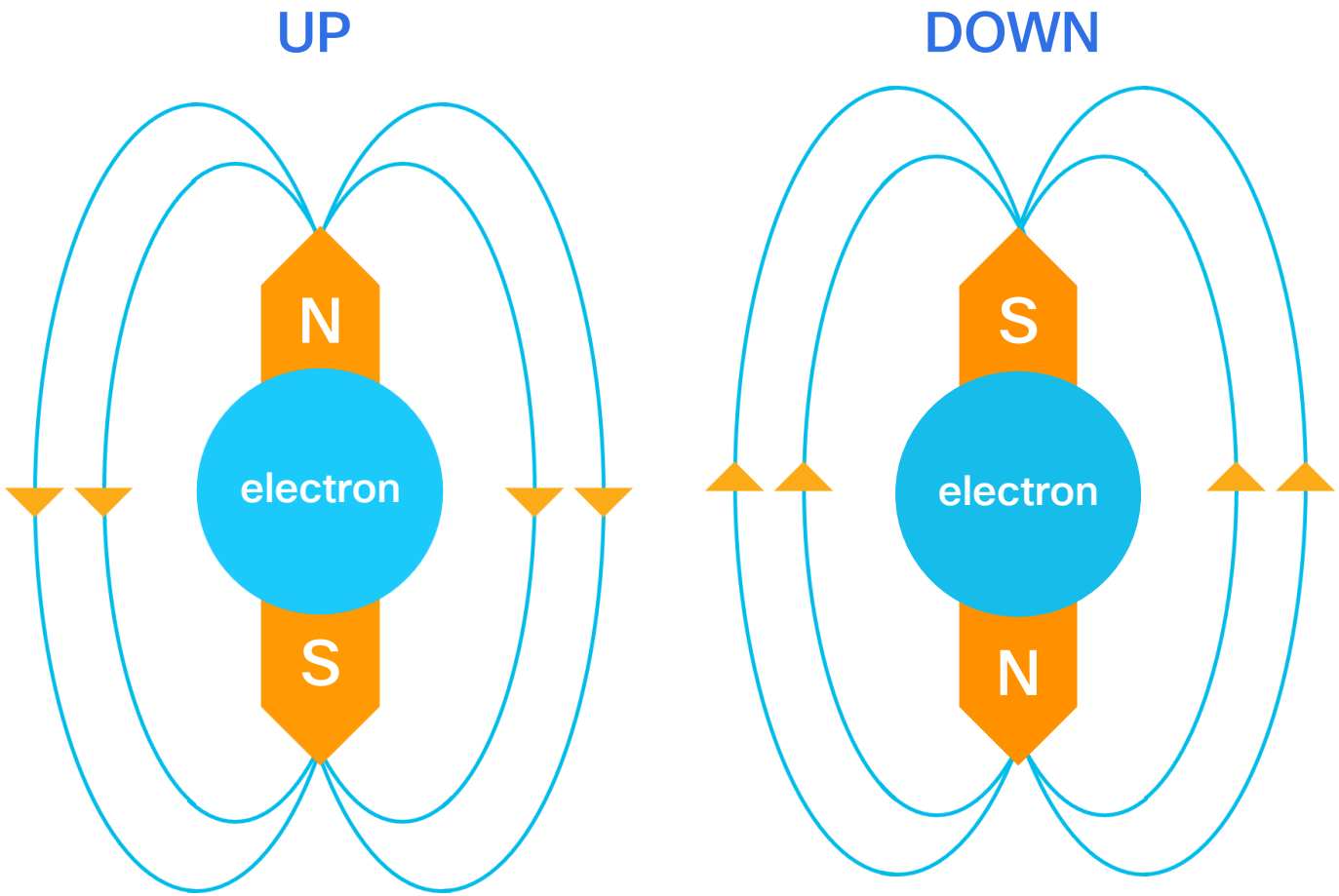
- electrons
- photons
- ions
- etc.

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Qubit Example: Electron Spin

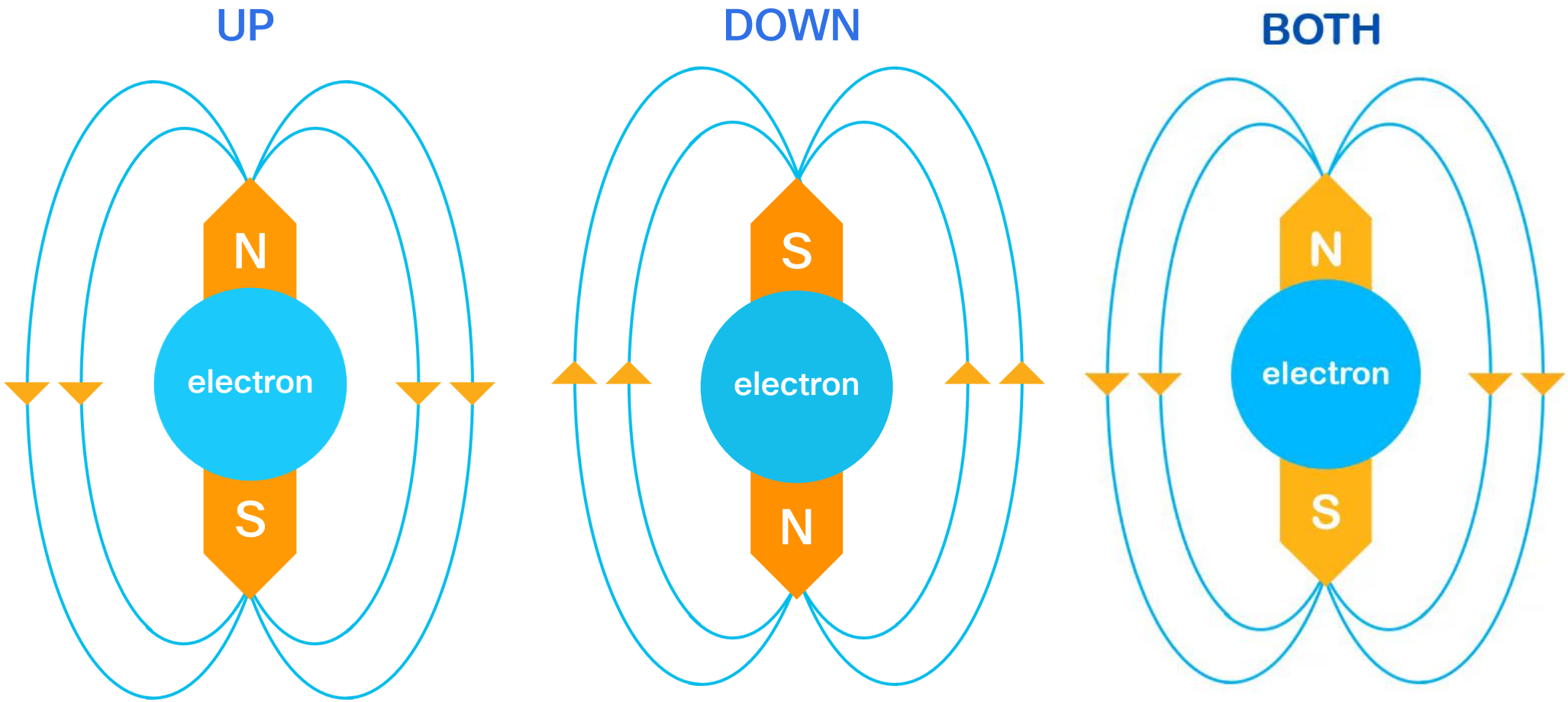
- The spin of an electron can be used as a qubit
- For example:
  - An upwards spin could be used represent a 0
  - A downward spin could be used to represent 1



© 2025 Cisco and/or its affiliates. All rights reserved.

Angular Momentum

- Electron spin a function of an innate property called Angular Momentum
- And the spin isn't just up or down, but can be anywhere in between, along any axis (X, Y, or Z)



© 2025 Cisco and/or its affiliates. All rights reserved.

General Quantum State Formula

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

© 2025 Cisco and/or its affiliates. All rights reserved.

General Quantum State Formula

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

Quantum State
represented by Psi

(Psi is the 23rd letter of the Greek alphabet)

Alpha Ket 0
Alpha represents the amplitude of state 0

(Alpha is the first letter of the Greek alphabet)

Beta Ket 1
Beta represents the amplitude of state 1

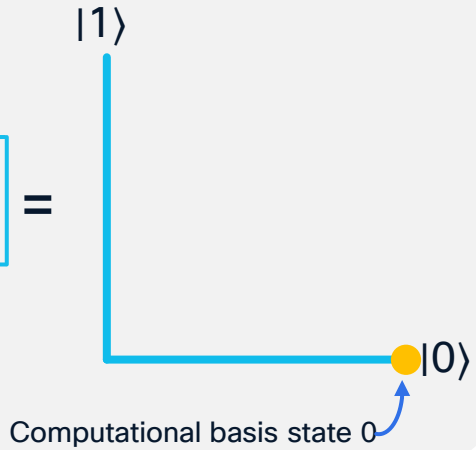
(Beta is the second letter of the Greek alphabet)

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum State and Vectors

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

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



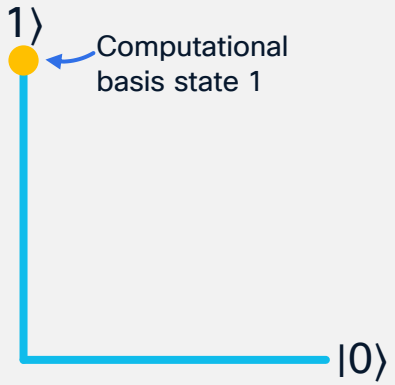
$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ Vector 0

X-Axis Coordinate

Y-Axis Coordinate

$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ Vector 1

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



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum State and Vectors

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

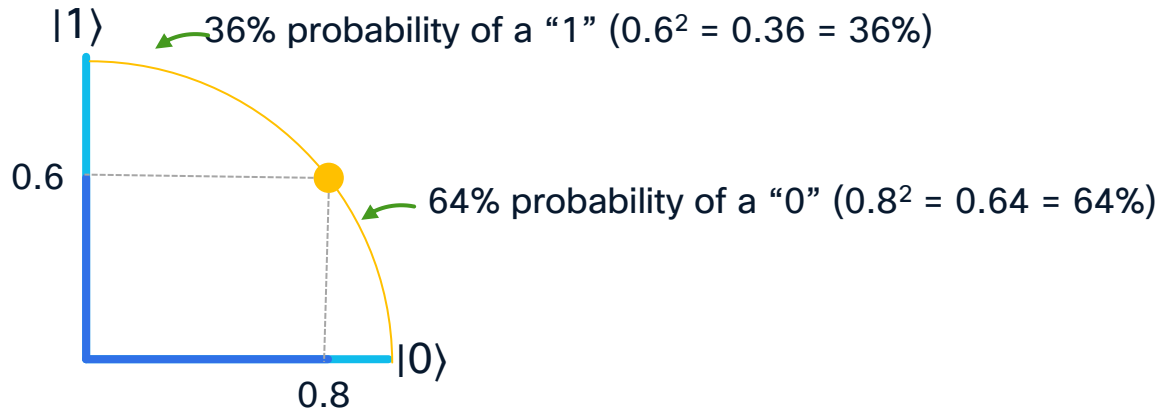
X-Axis Coordinate

Y-Axis Coordinate

$$|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle = \begin{bmatrix} 0.8 \\ 0.6 \end{bmatrix}$$

The square of the amplitude is the probability, and the sum of the probabilities must equal 1

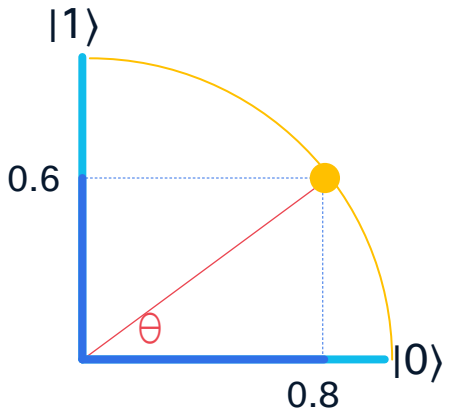
$$\alpha^2 + \beta^2 = 1$$



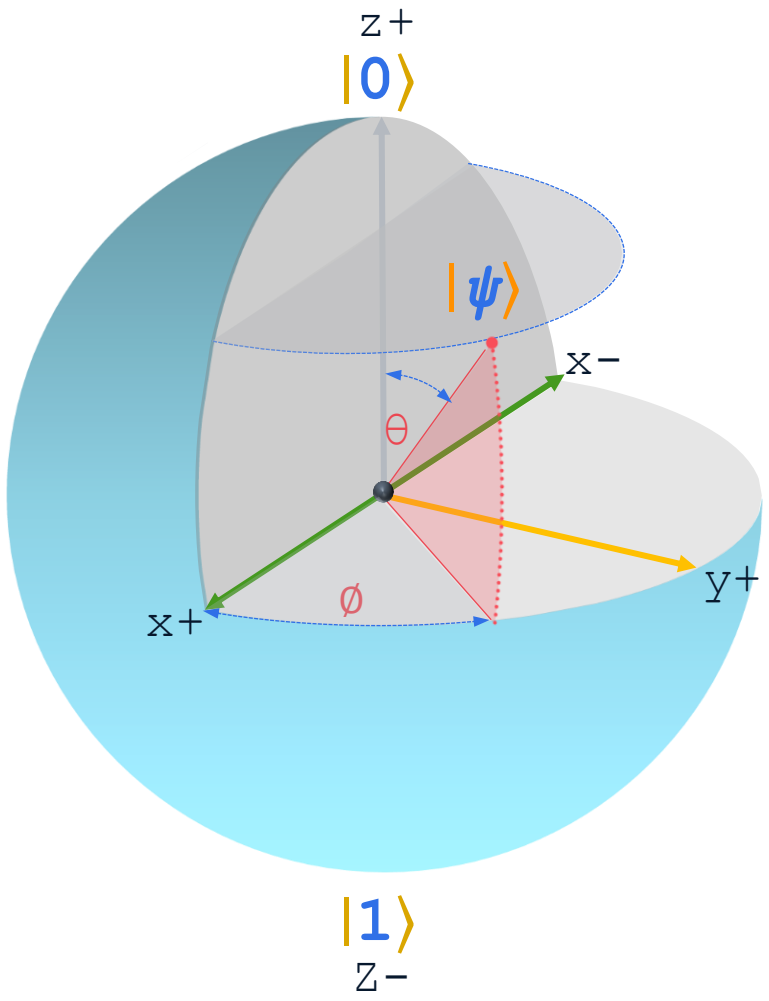
© 2025 Cisco and/or its affiliates. All rights reserved.

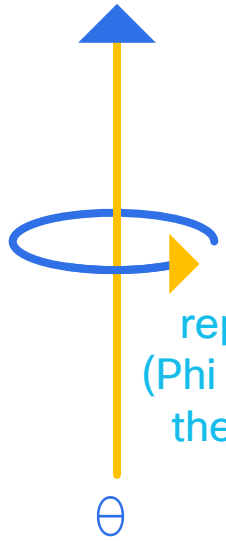
cisco

The Bloch Sphere: A 3D Qubit Representation



$$|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle$$





Ø Phase

represented by Phi
(Phi is the 21st letter of the Greek alphabet)

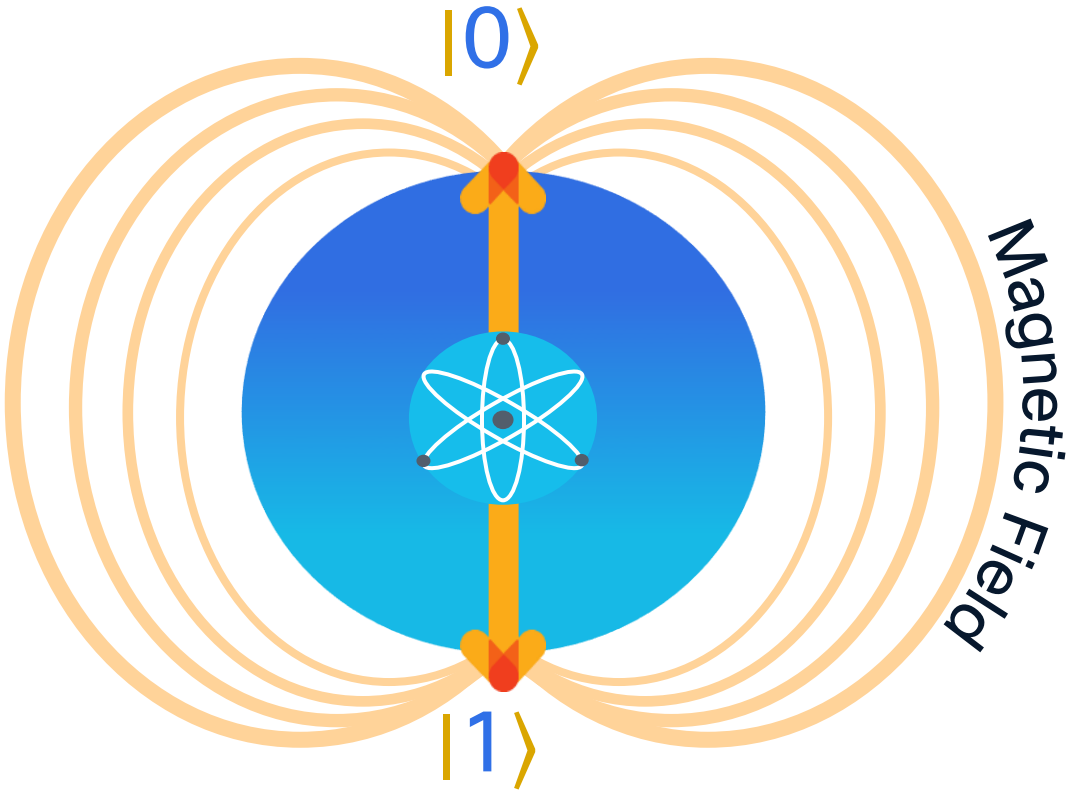
Amplitude

represented by Theta
(Theta is the 8th letter of the Greek alphabet)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Special Property: Superposition



As long a qubit is unobserved (i.e. unmeasured) it remains in a “superposition” of probabilities for 0 and 1

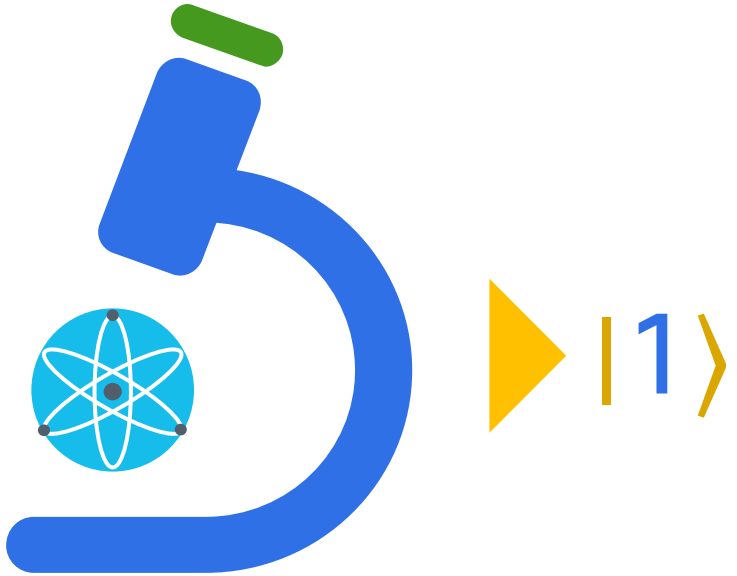
The instant a qubit is measured, the superposition will collapse into one of the two discrete states

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Special Property: Superposition

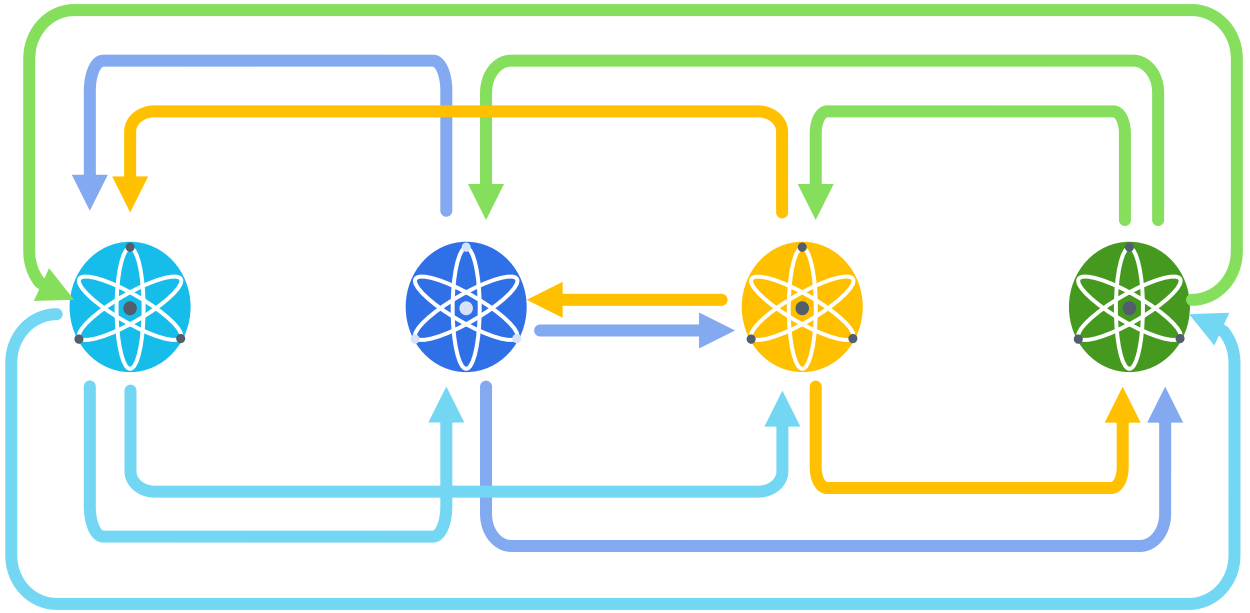
As long a qubit is unobserved (i.e. unmeasured) it remains in a “superposition” of probabilities for 0 and 1

The instant a qubit is measured, the superposition will collapse into one of the two discrete states



© 2025 Cisco and/or its affiliates. All rights reserved.

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 apart

Multiple qubits can become entangled with each other

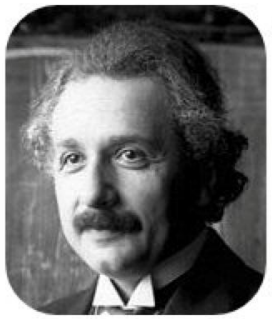
Current world records is 51 (physical) qubits

https://www.newscientist.com/article/2382022-record-breaking-number-of-qubits-entangled-in-a-quantum-computer/
https://www.livescience.com/technology/computing/new-quantum-computing-milestone-smashes-entanglement-world-record

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Special Property: Entanglement

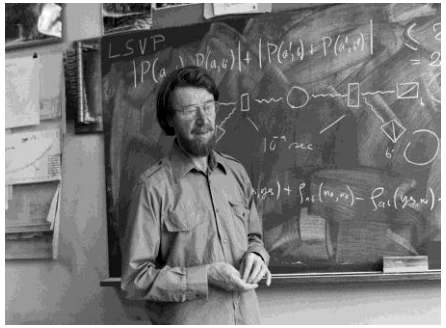
An Introduction to Quantum Mechanics



A. Einstein

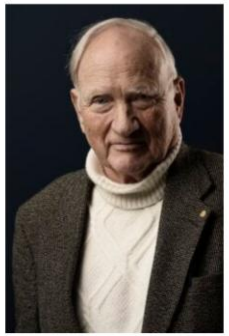
B. Podolsky

N. Rosen



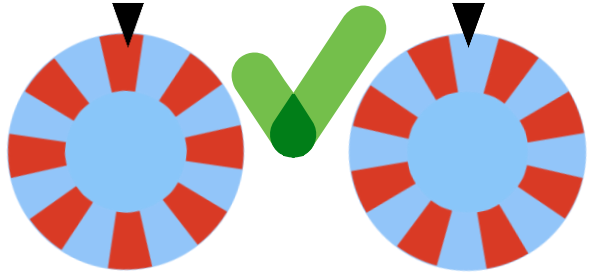
John Bell

Alain Aspect



John Clauser

Anton Zeilinger



2022 Nobel Prize in Physics

"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science“

https://www.nobelprize.org/prizes/physics/2022/summary/

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Special Property: Entanglement

If an entangled qubit is measured, then entanglement is broken

The discrete state of the entangled qubit will depend on the entanglement operation that was performed

The important point is that as one entangled qubit changes state, its counterpart(s) will instantaneously reflect that change

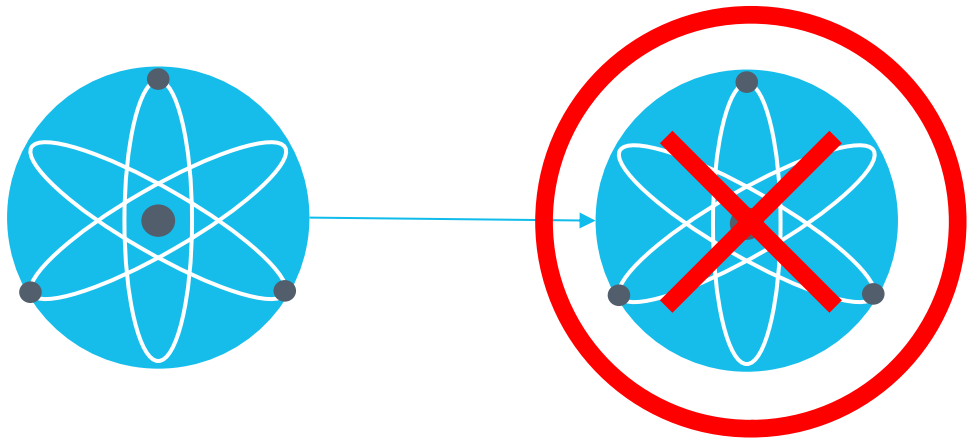
© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Special Property: No Cloning

It can be mathematically proven that it is impossible to clone a qubit

The mathematical proof uses the logical method of “Proof by Contradiction”

A descriptive proof is that a qubit cannot be measured without collapsing, but you cannot copy something without reading/measuring it first



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

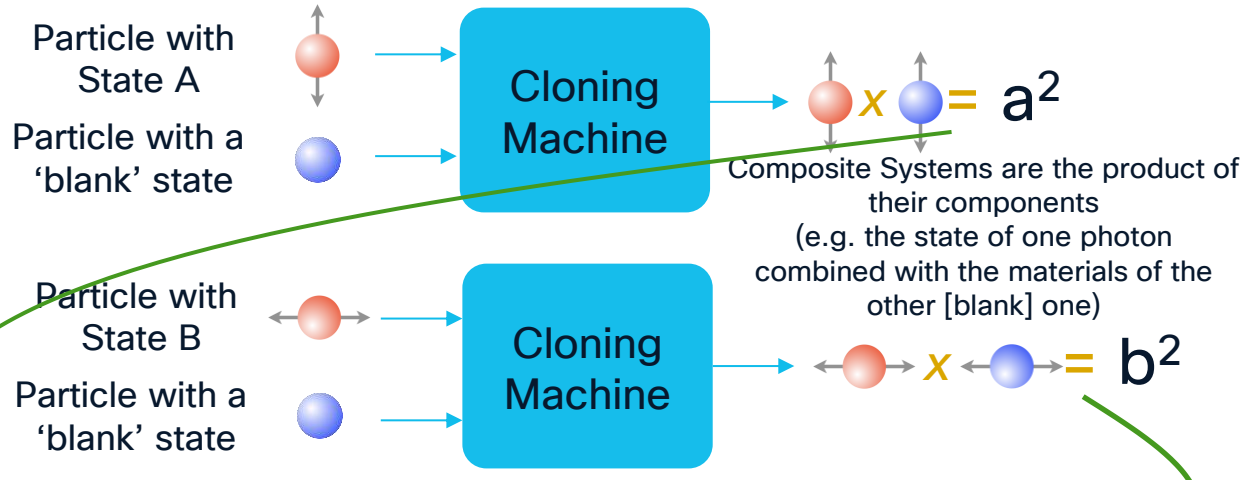
Quantum Special Property: No Cloning

Given: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
Let $a = \alpha|0\rangle$ and $b = \beta|1\rangle$
$|\psi\rangle = (a + b)$

Reference Slide

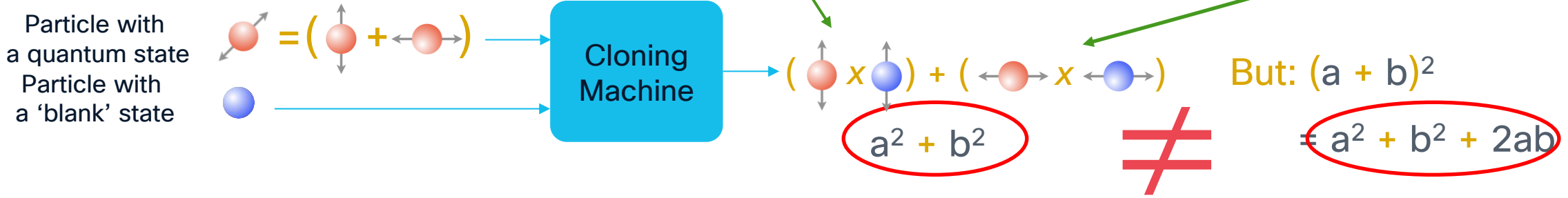
It can be mathematically proven that it is impossible to clone a qubit

The proof is made via a “Proof by Contradiction”



Quantum state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Simplified to: $|\psi\rangle = (a + b)$

For any given Transformation (T): T(a + b) = T(a) + T(b)
Let us assume the transformation is a cloning operation



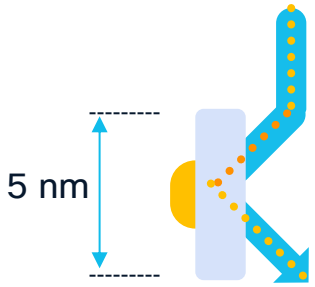
© 2025 Cisco and/or its affiliates. All rights reserved.

https://www.youtube.com/watch?v=owPC60Ue0BE

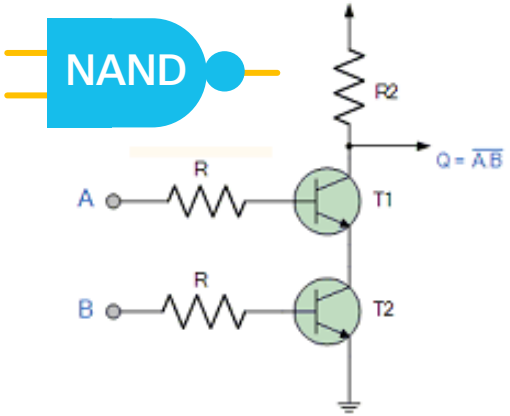
An Introduction to Quantum Computing

CISCO Live !

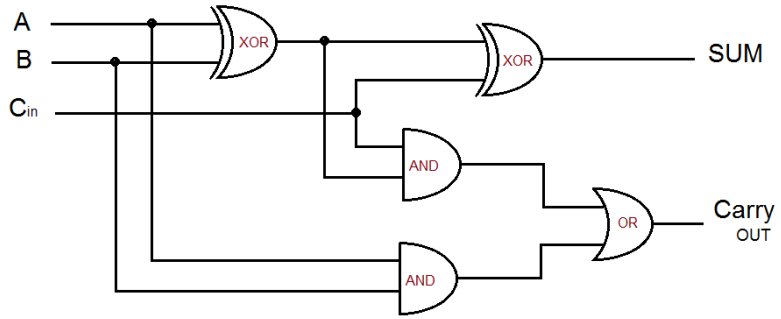
Digital Circuits Quick Recap



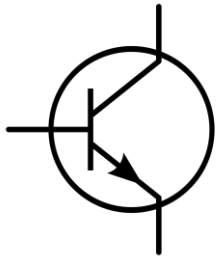
Transistors

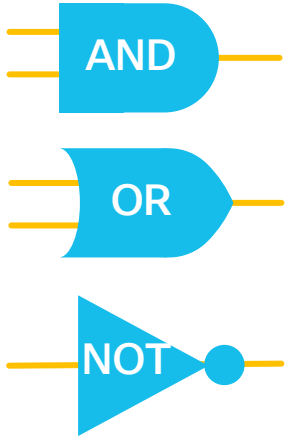


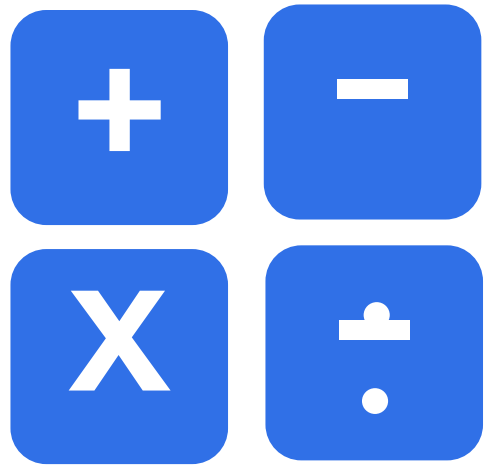
Logic Gates



Circuits







© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

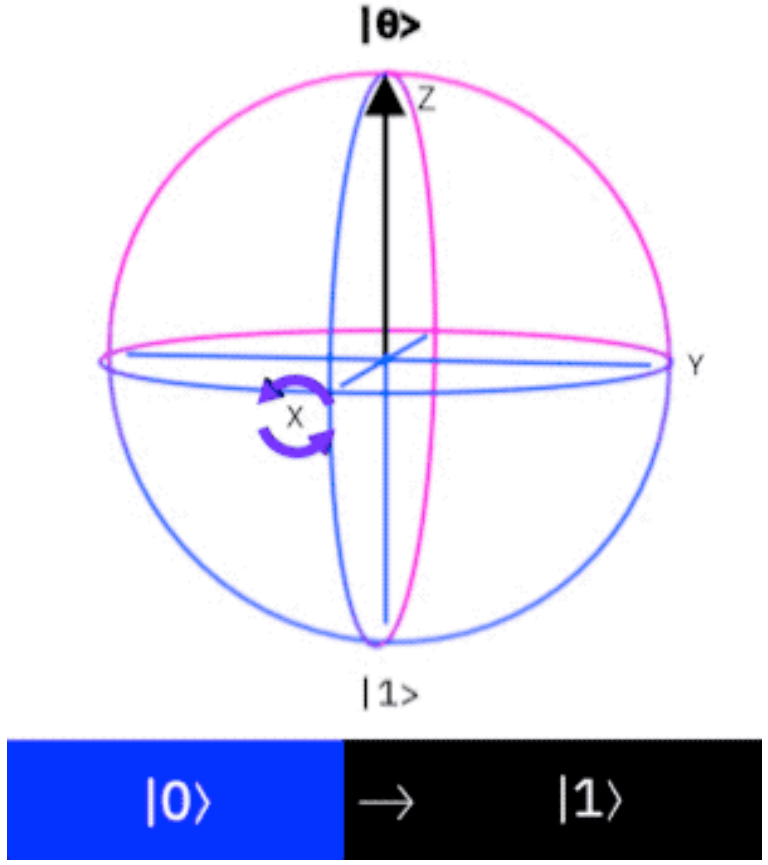
Quantum Gate Operation

Quantum Gates manipulate the Amplitude θ and/or the Phase Φ of the state vector

Quantum gates:

- take a superposition as an input
- rotate their possibilities, and
- produce another superposition as an output

Unlike most digital gates, quantum gates always have the same number of outputs as inputs

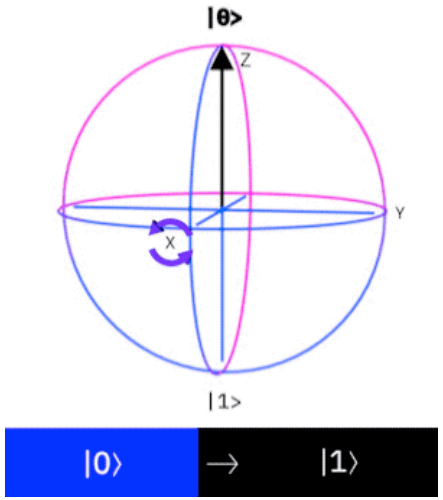


© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Universal Gate Set

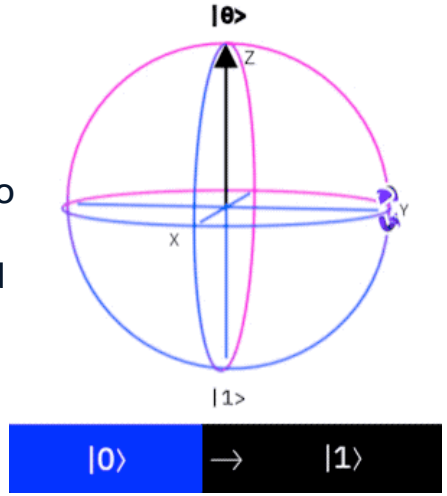
X

Pauli-X Gate is a NOT operation; it will turn a spin-up state to a spin-down state, and vice versa.



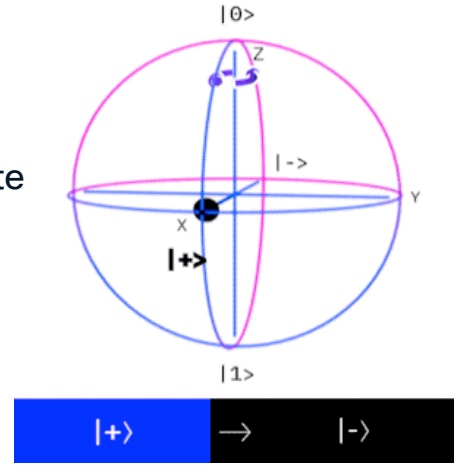
Y

Pauli-Y Gate is also a NOT operation, but rotates around the Y-axis; it is similar to the X-gate, but different in phase.



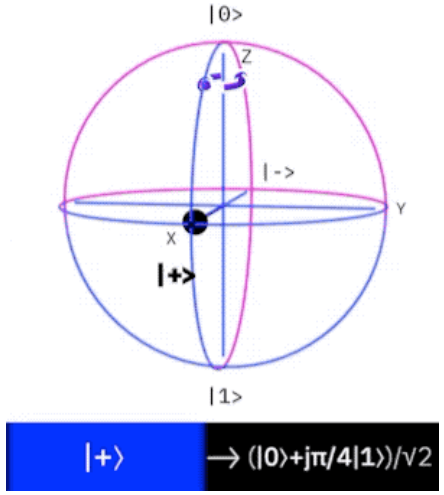
Z

Pauli-Z Gate rotates around the Z-axis.



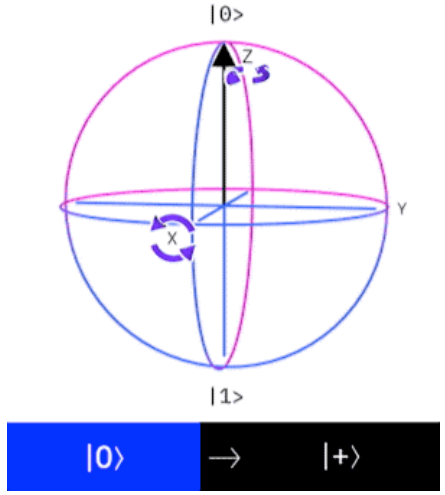
T

T gate rotates a qubit Π/4 around the Z-axis.



H

Hadamard Gate sets the qubit into a superposition state of a 50/50 chance that it will end up as |0> or |1>.



CNOT

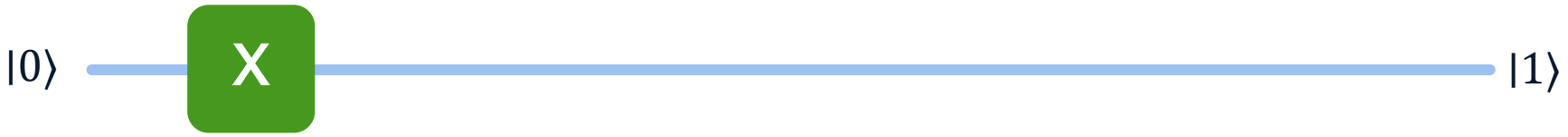
The Controlled- NOT gate acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is |1>, otherwise it leaves it unchanged.

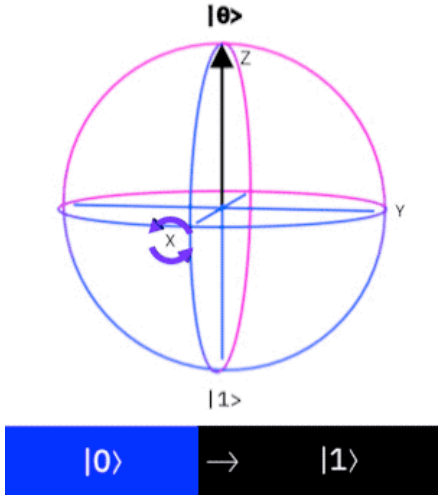
© 2025 Cisco and/or its affiliates. All rights reserved.

Source: quantum.ibm.com

Quantum NOT Gate (Pauli-X Gate)

Rotates π Radians (180^0) Around the X-Axis





MATRIX

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

NOT Gate

VECTOR

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Basis State

$|0\rangle$

Row x Column

$$0 \times 1 + 1 \times 0 = 0$$

$$1 \times 1 + 0 \times 0 = 1$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Basis State

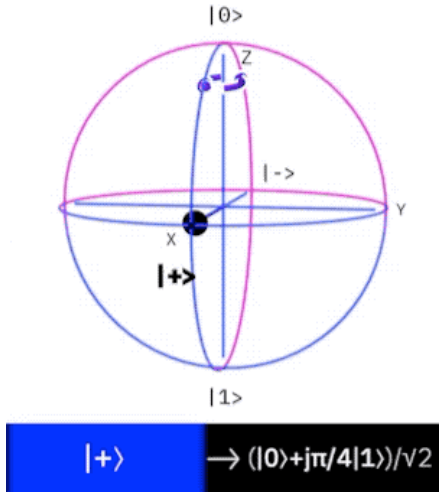
$|1\rangle$

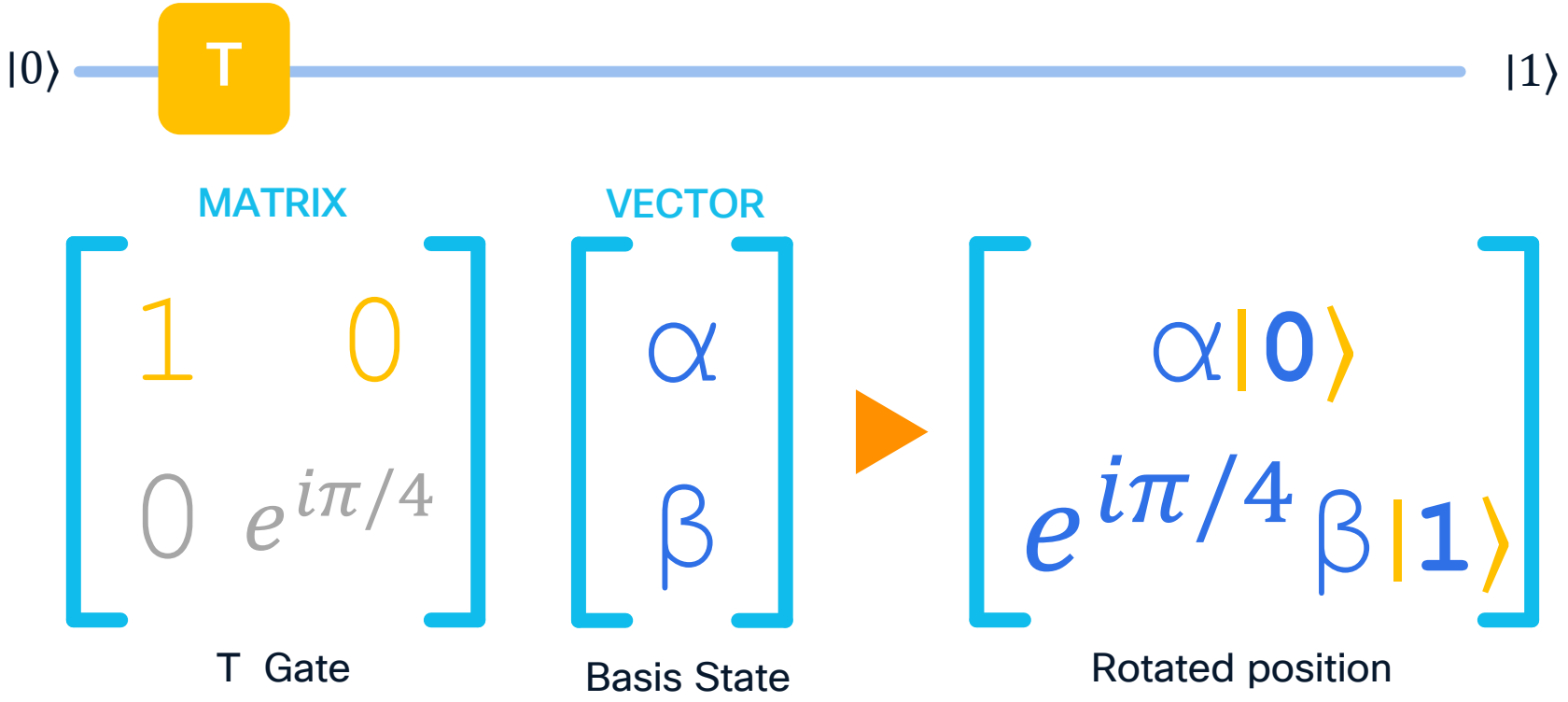
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

T Gate

Rotates $\pi/4$ Radians (45^0) Around the Z-Axis

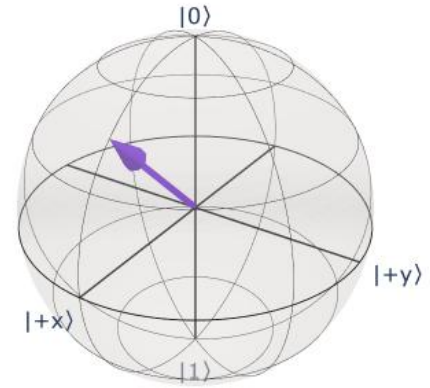


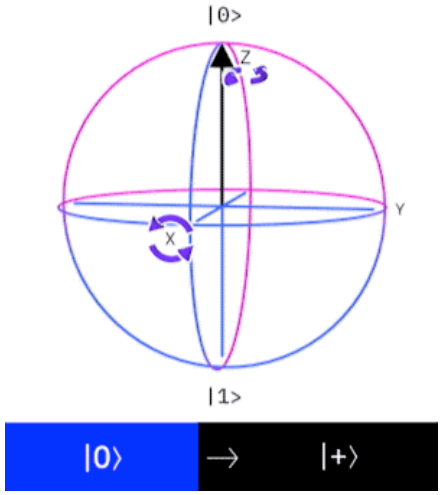


© 2025 Cisco and/or its affiliates. All rights reserved.

Hadamard Gate

Rotates π Radians (180^0) around an X-Y Diagonal Axis (to Set Itself to a 50/50 State)





H

MATRIX

VECTOR

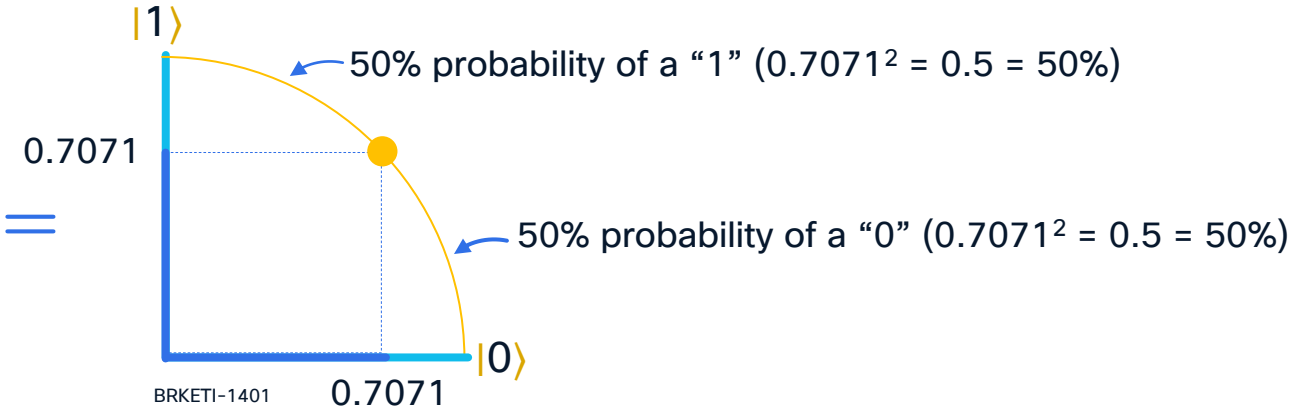
$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} \blacktriangleright \begin{bmatrix}\frac{1}{\sqrt{2}}|0\rangle\\ \frac{1}{\sqrt{2}}|1\rangle\end{bmatrix}$$

Hadamard Gate | Basis State $|0\rangle$ | Uniform Super Position

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\psi\rangle = 0.7071|0\rangle + 0.7071|1\rangle =$$

The square of the amplitude is the probability, and the sum of the probabilities equals 1

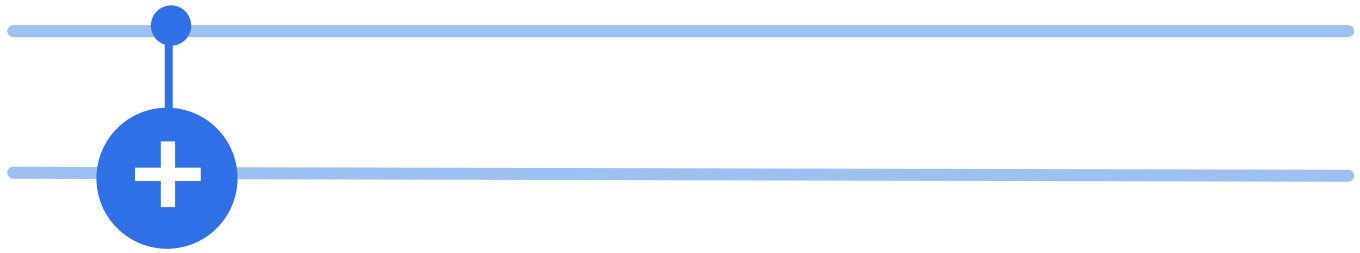


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Two-Qubit Quantum Gate: Controlled NOT (CNOT) Gate

Part 1: Digital Gate Analogy



XOR Truth Table

Input A	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	0

Input A	Input B	A	Output
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Whenever A = 0, the output is B

Whenever A = 1, the output is NOT B

Therefore, A **CONTROLS** the NOT function for B

© 2025 Cisco and/or its affiliates. All rights reserved.

Two-Qubit Quantum Gate: Controlled NOT (CNOT) Gate

Part 2: CNOT Gate Matrix and Truth Table

MATRIX

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Controlled NOT Gate

CNOT Truth Table

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

In this example, q_1 **CONTROLS** the NOT function for q_0

Note: the CNOT gate operation entangles the qubits.

The state of control qubit will determine the state of the target qubit.

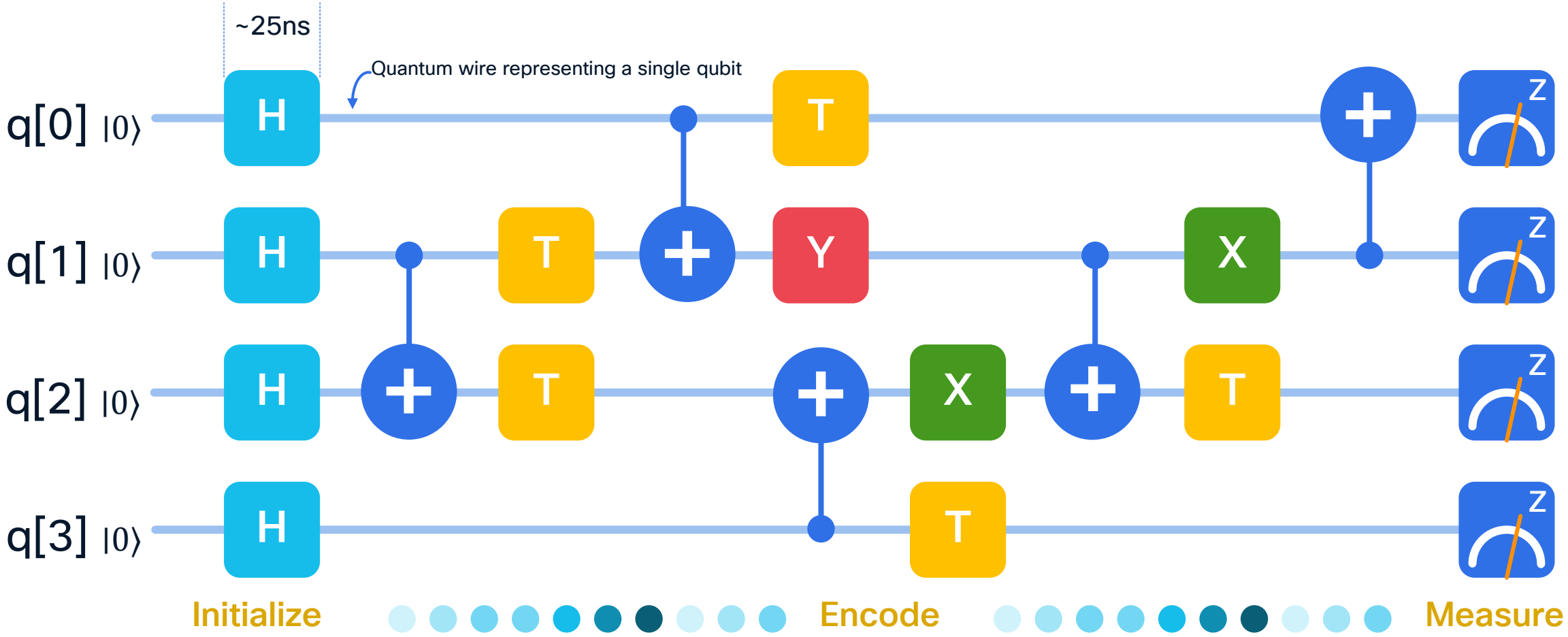
From this point forward, their fates are intertwined (i.e. entangled).

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Circuits

Include Both Quantum Operators + Classical Computing

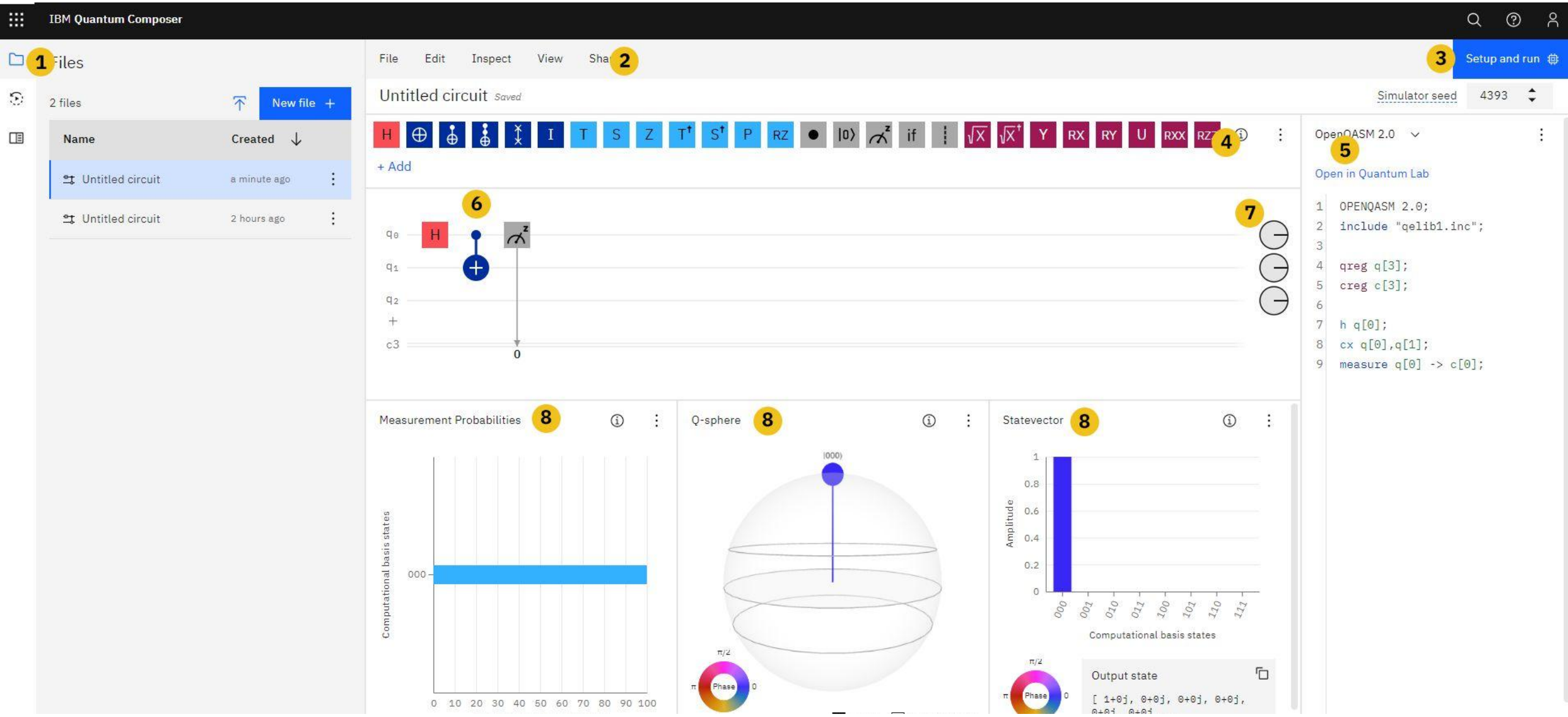


The number of output qubits always matches the number of input qubits

Measuring is a Classical Computing operation

© 2025 Cisco and/or its affiliates. All rights reserved.

IBM Quantum Composer



© 2025 Cisco and/or its affiliates. All rights reserved.

https://learning.quantum.ibm.com/tutorial/explore-gates-and-circuits-with-the-quantum-composer

Quantum Parallelism

Number of Qubits

Number of States

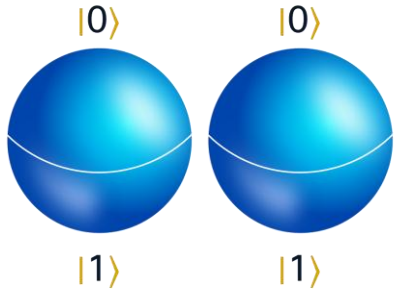
Probability

Base States and Initial Probabilities

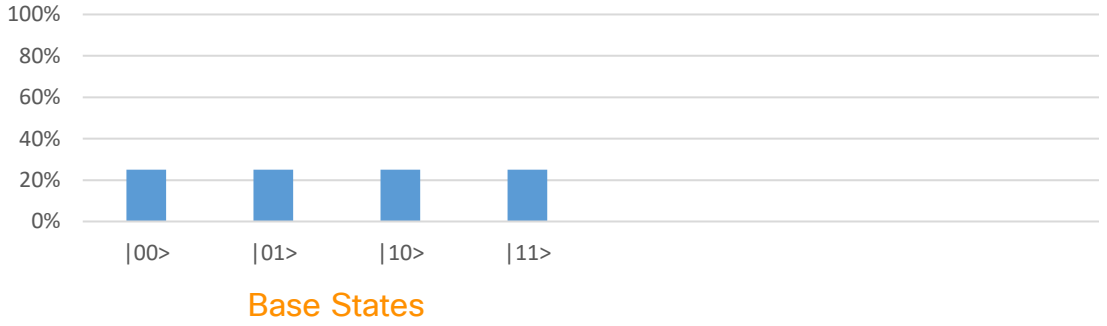
1

$2^1 = 2$

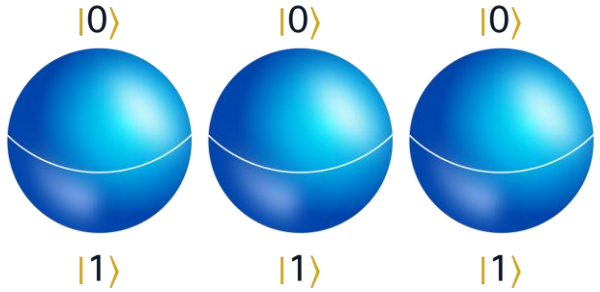
2



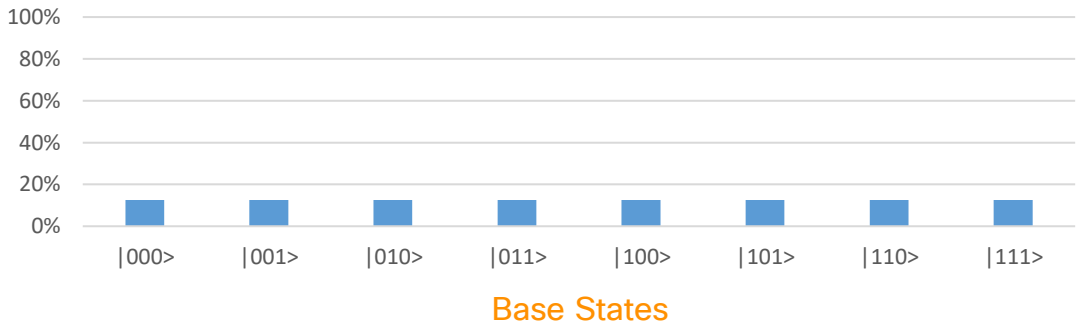
$2^2 = 4$



3



$2^3 = 8$



© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Interference Manipulation

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

Interference may be

- constructive or
- destructive

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

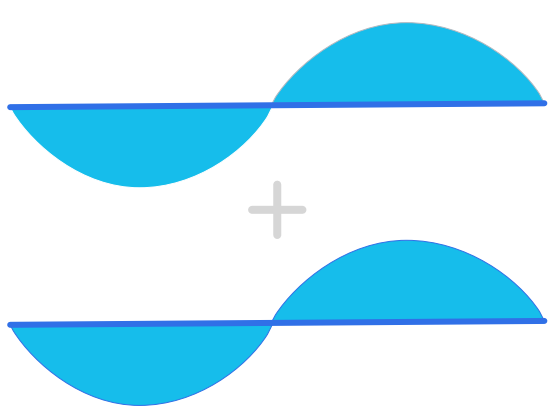
- ***correct*** answers generate ***constructive interference***
- ***incorrect*** answers generate ***destructive interference***

Remember: Probability = Amplitude^2

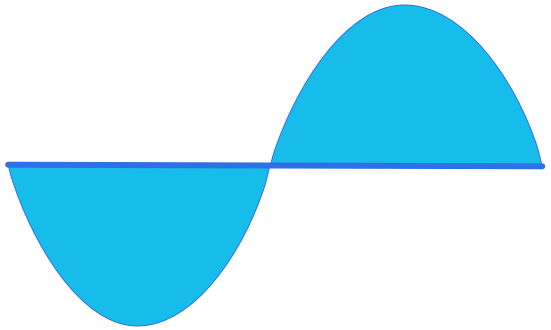
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Sums of the squares of probabilities must equal 1

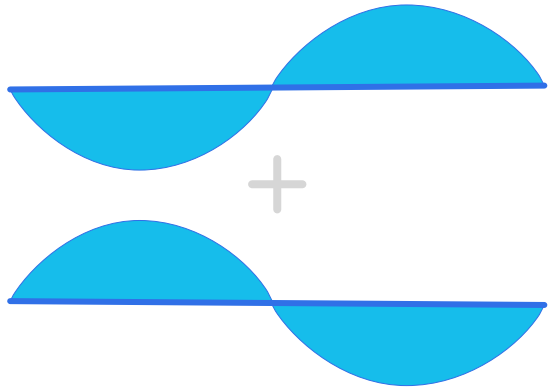
$$\alpha^2 + \beta^2 = 1$$



In phase



Constructive Interference



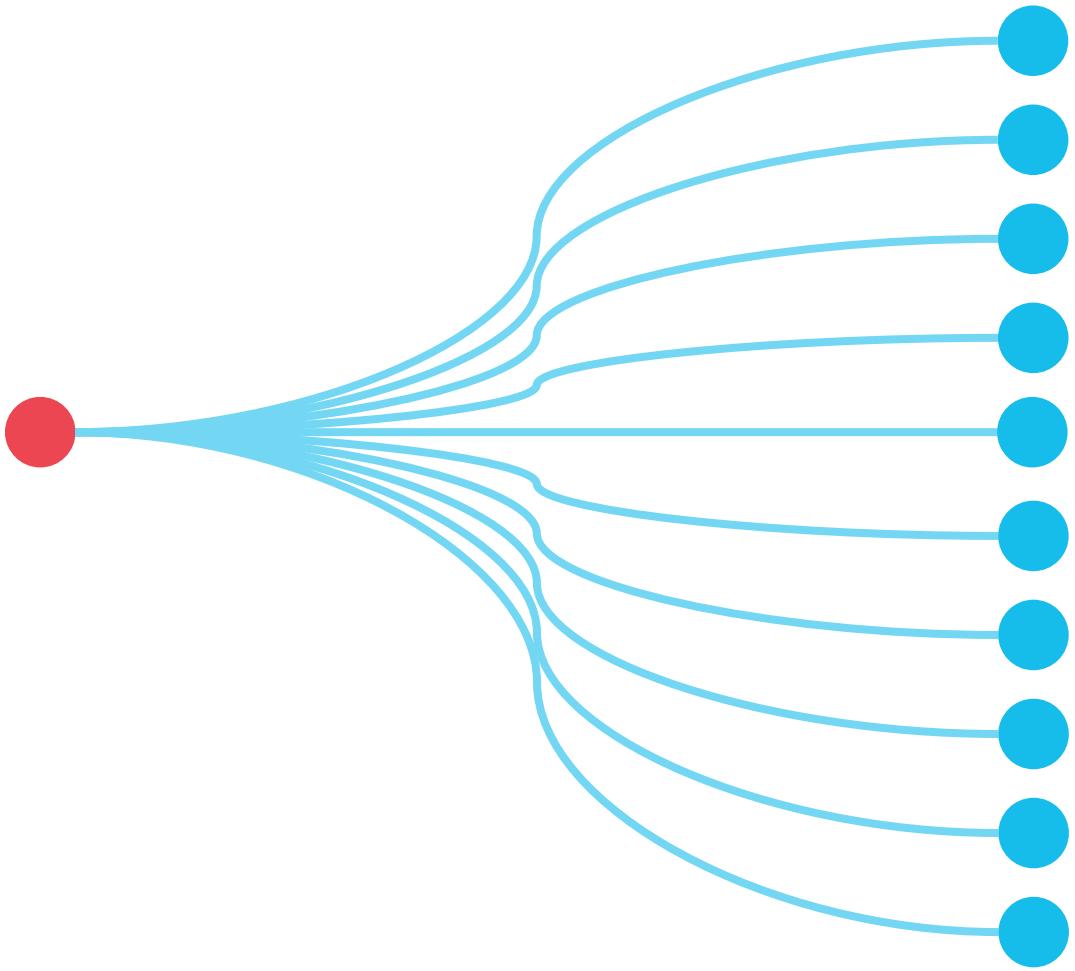
180° out of phase

Destructive Interference

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

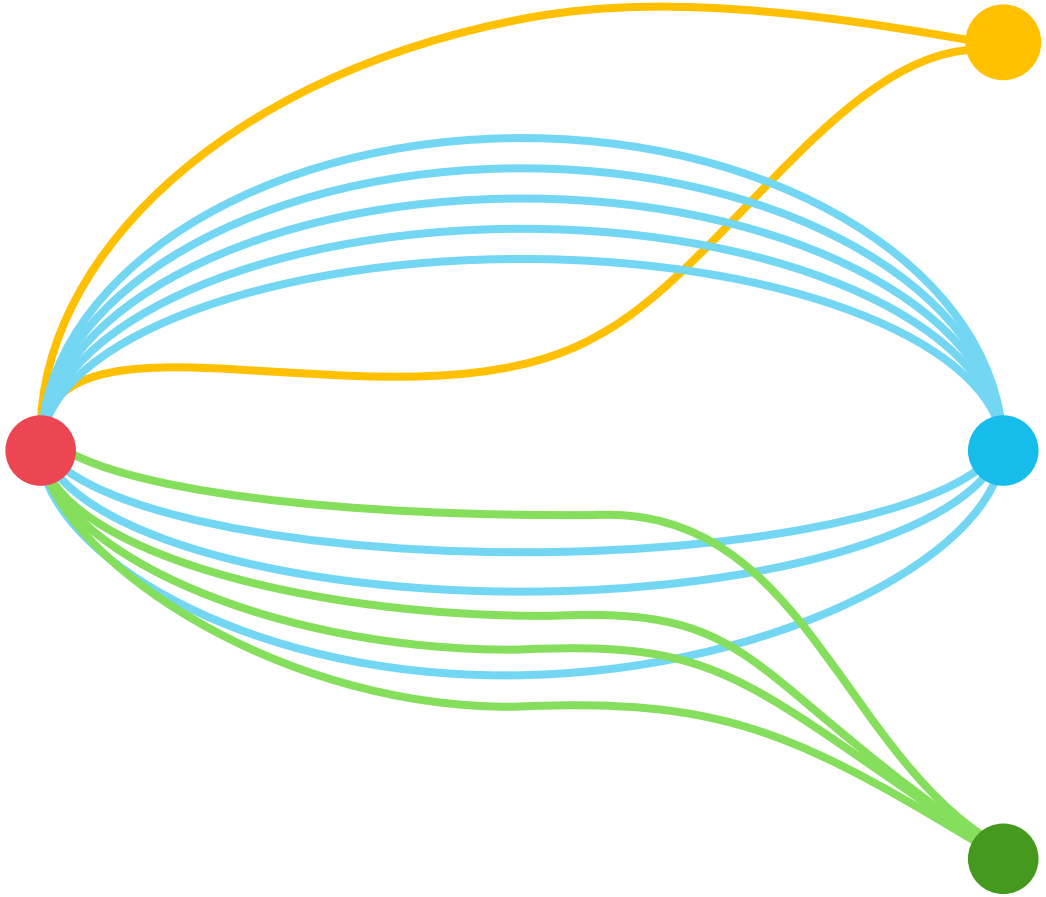
Classical Computing Problem Solving



A classic computer needs to sequentially iterate through a problem until the correct result is found

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Computing Problem Solving



Quantum computing can provide a single or small number of answers with the highest probability of being correct, which narrows down the search for the correct solution

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Speed-Up

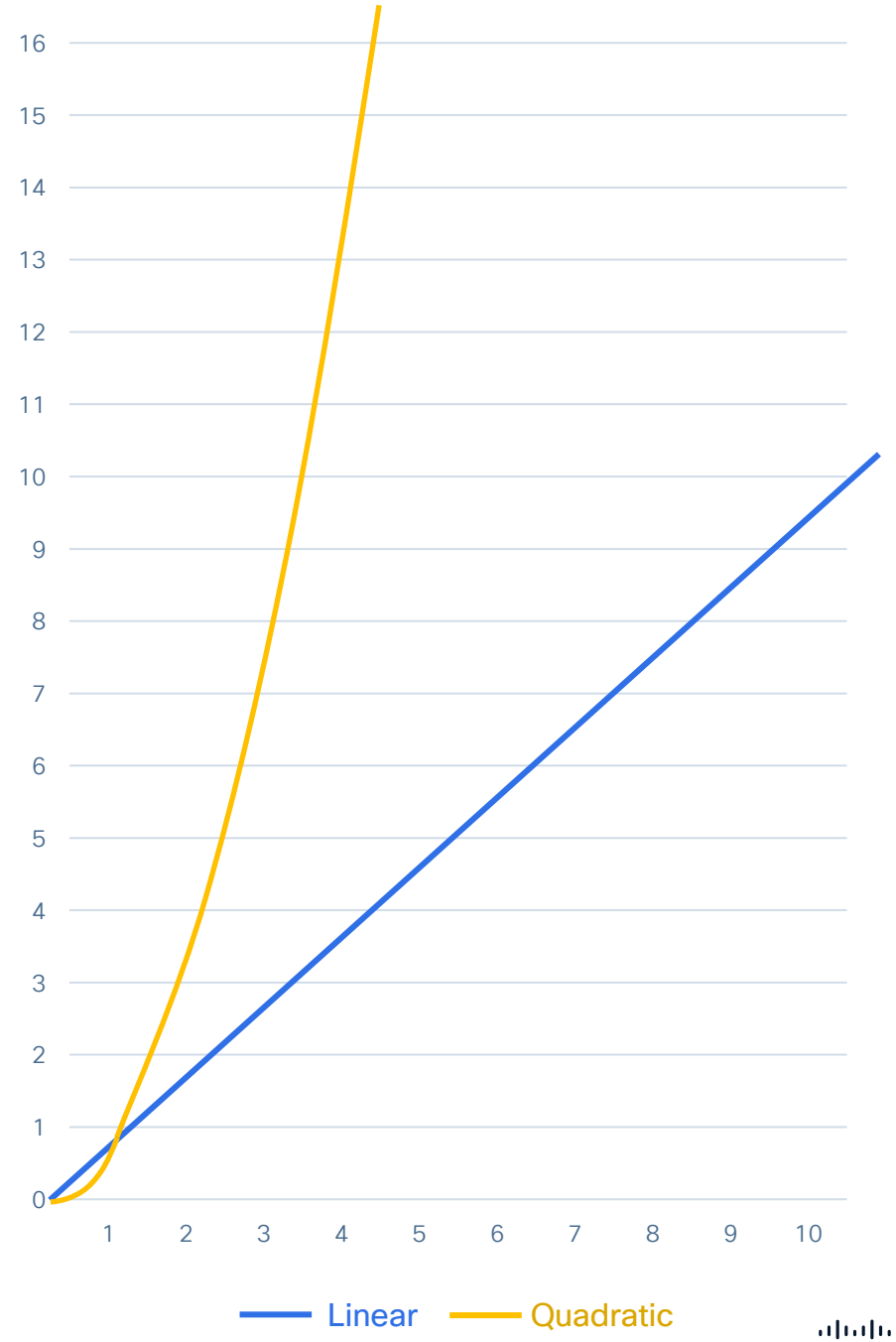
Well-designed quantum circuits can perform operations maximize quantum advantages and can thus exhibit significant speed-ups, as compared to their digital counterparts

Speed-ups may be:

- **Linear**
- **Quadratic**

Linear
$y=x$

Quadratic
$y=x^2$



© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Speed-Up

Well-designed quantum circuits can perform operations maximize quantum advantages and can thus exhibit significant speed-ups, as compared to their digital counterparts

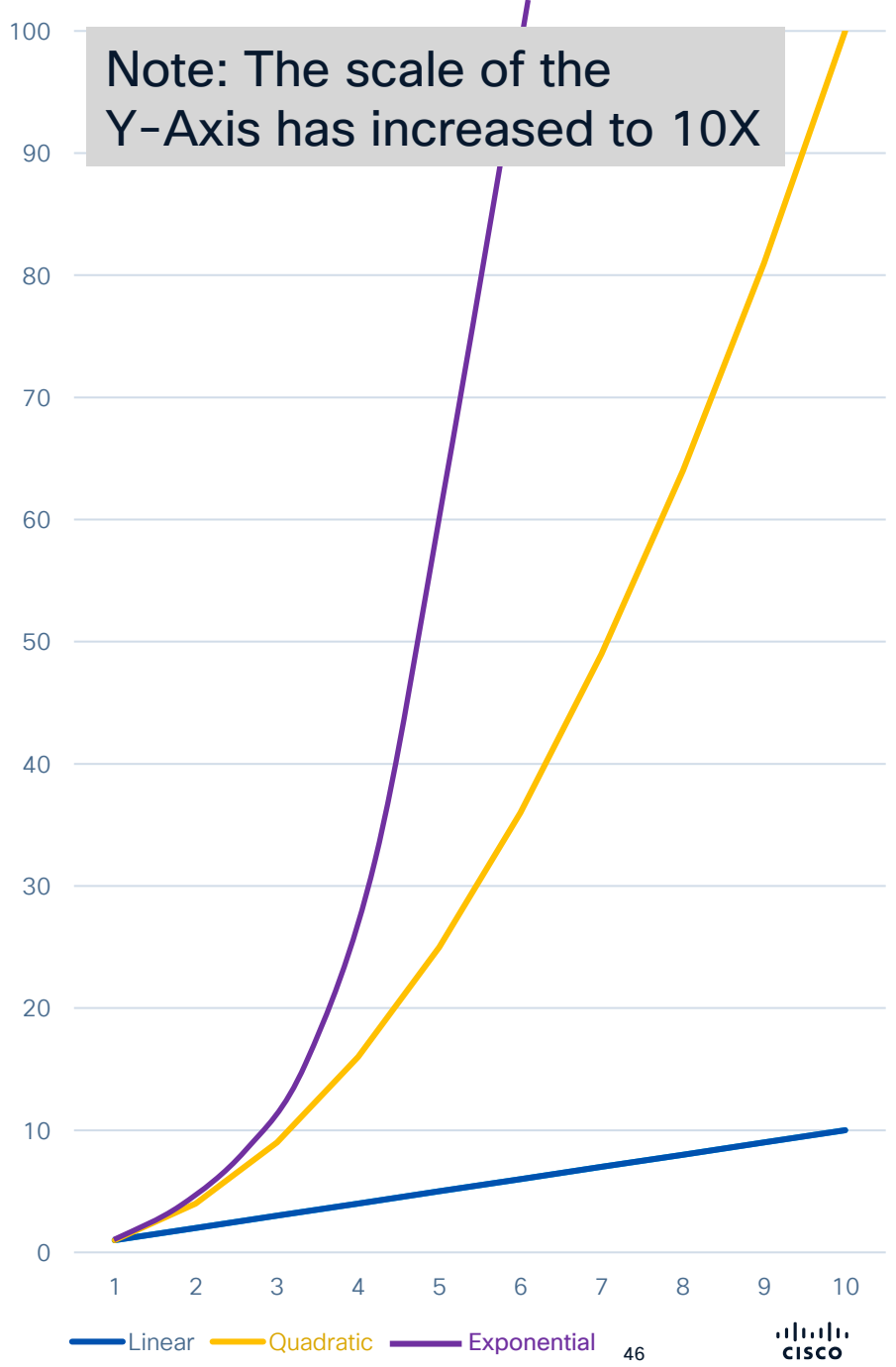
Speed-ups may be:

- **Linear**
- **Quadratic**
- **Exponential**

Linear
$y=x$

Quadratic
$y=x^2$

Exponential
$y=2^x$



© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Speed-Up

Well-designed quantum circuits can perform operations maximize quantum advantages and can thus exhibit significant speed-ups, as compared to their digital counterparts

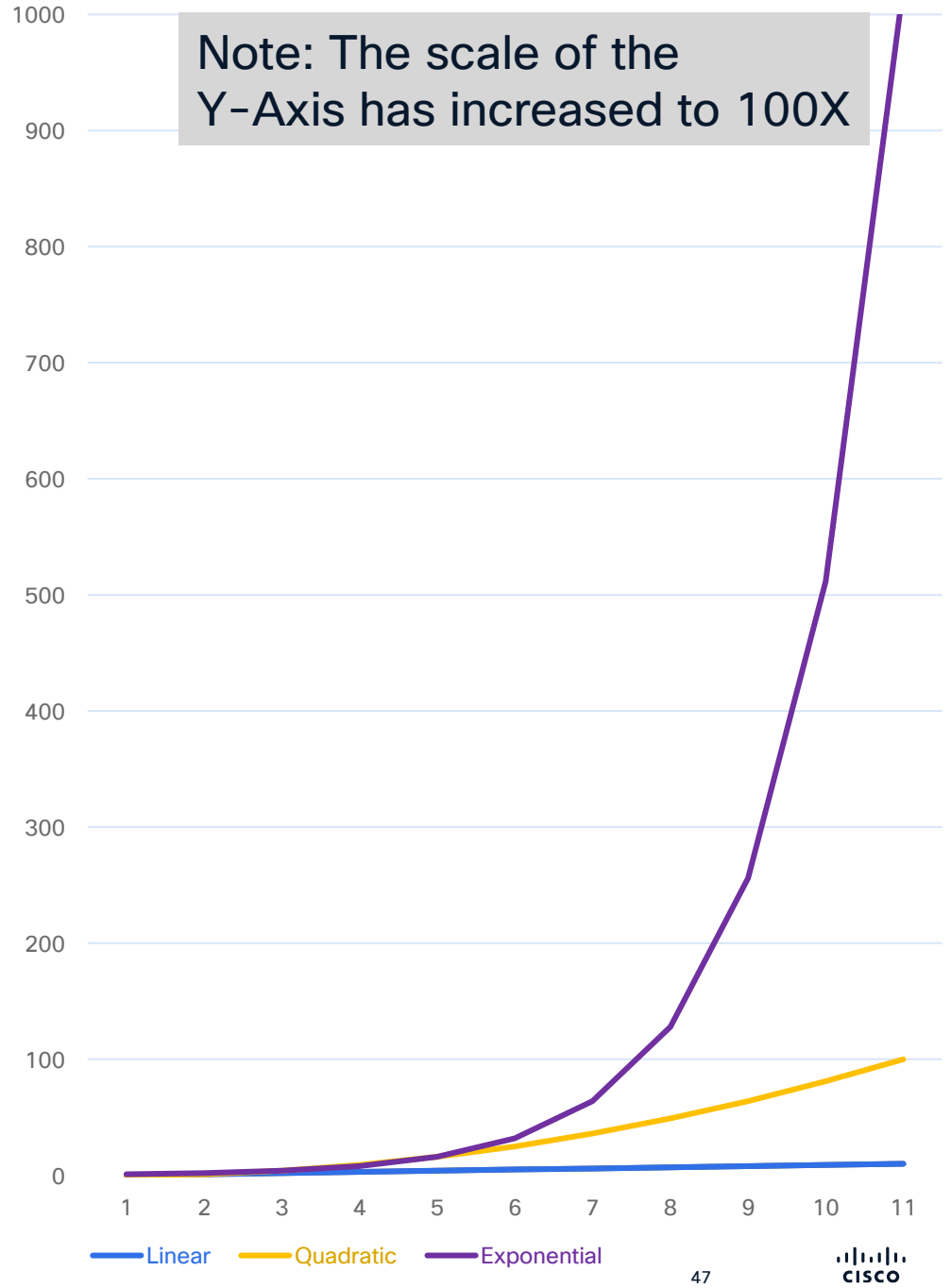
Speed-ups may be:

- **Linear**
- **Quadratic**
- **Exponential**

Linear
$y=x$

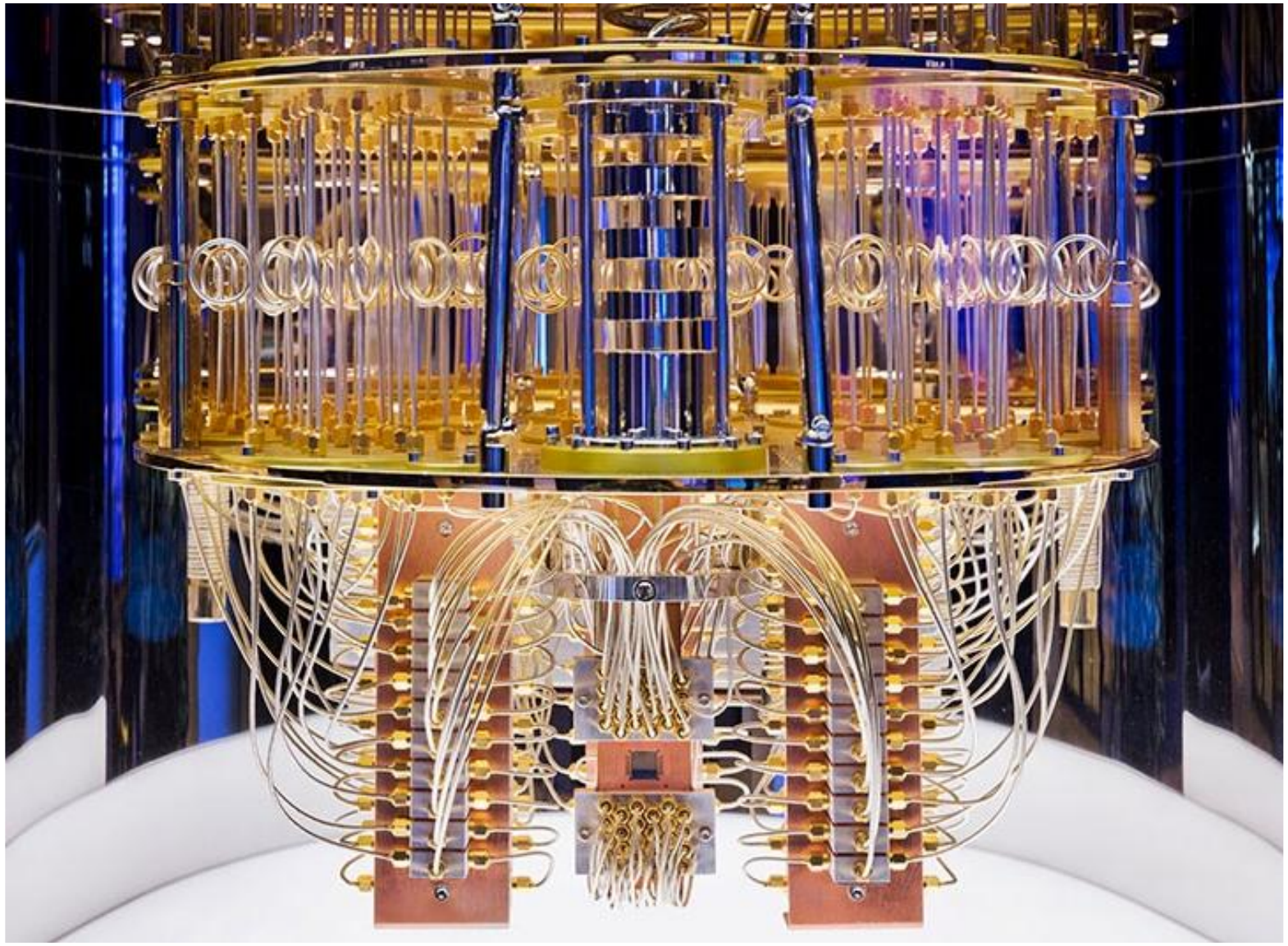
Quadratic
$y=x^2$

Exponential
$y=2^x$



© 2025 Cisco and/or its affiliates. All rights reserved.

How Much Faster is a Quantum Computer?



In 2021, the world's largest quantum computer had 127 qubits

This machine was 158M times faster than its classic counterpart

Example Task Execution Times:

- Classic Computer: 2,500 years
- Quantum Computer: 1 minute

$2^{127} = 1.7 \times 10^{38}$ values

170,000,000,000,000,000,000,000,000,000,000,000

© 2025 Cisco and/or its affiliates. All rights reserved.

How Much Faster is a Quantum Computer?

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16$

...

$2^{10} = 1{,}024$

...

$2^{20} = 1{,}048{,}576$

...

$2^{127} = 1.7 \times 10^{38}$ (IBM Eagle)

...

$2^{275} = 10^{82}$ Number of Atoms in the Universe

...

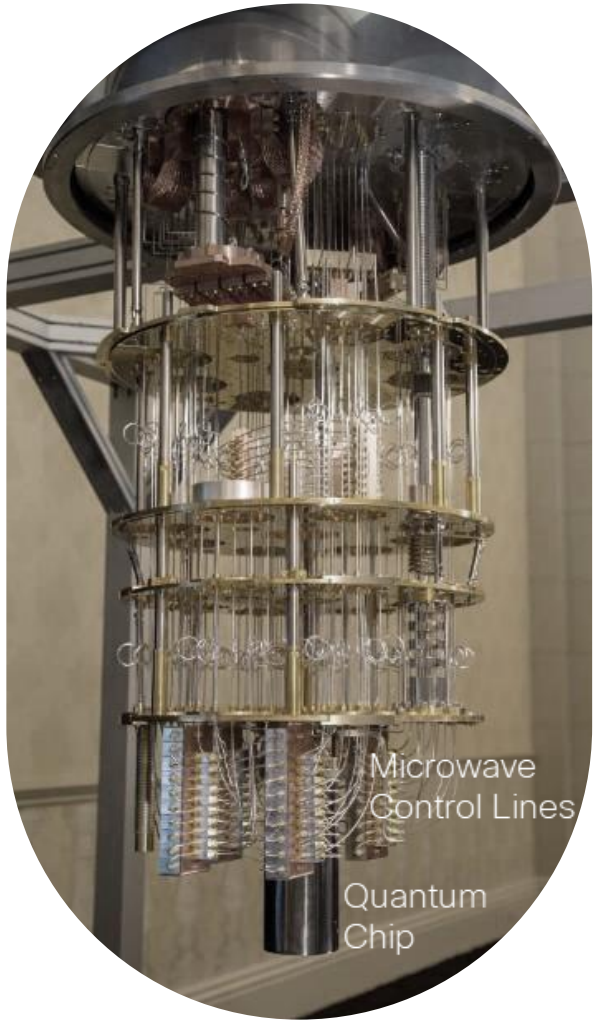
$2^{1121} = 10^{337}$ (IBM Condor)

© 2025 Cisco and/or its affiliates. All rights reserved.

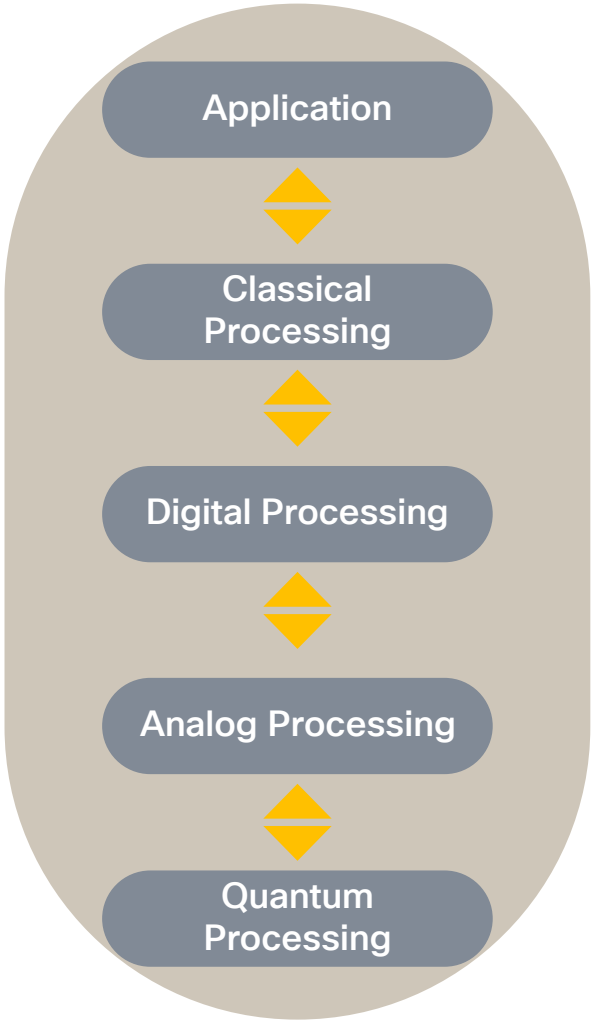
What Do Quantum Computers Look Like?

External (IBM)

External (IBM)



Internal (IBM)



Functions

https://newsroom.ibm.com/media-quantum-innovation

© 2025 Cisco and/or its affiliates. All rights reserved.

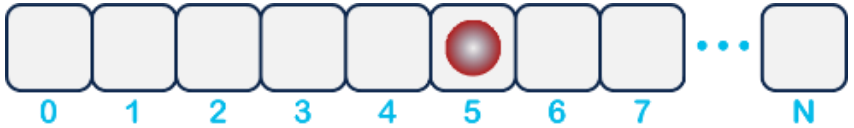
cisco

Implications of Quantum Computing on Cybersecurity

Security-Concerning Quantum Algorithms

Grover's Algorithm

- searches an unstructured database (or an unordered list) for a specific result
- Exhibits **quadratic** speed-up vs. digital (classical compute)
- theoretically threatens **symmetric** key algorithms, such as the Advanced Encryption Standard (AES)

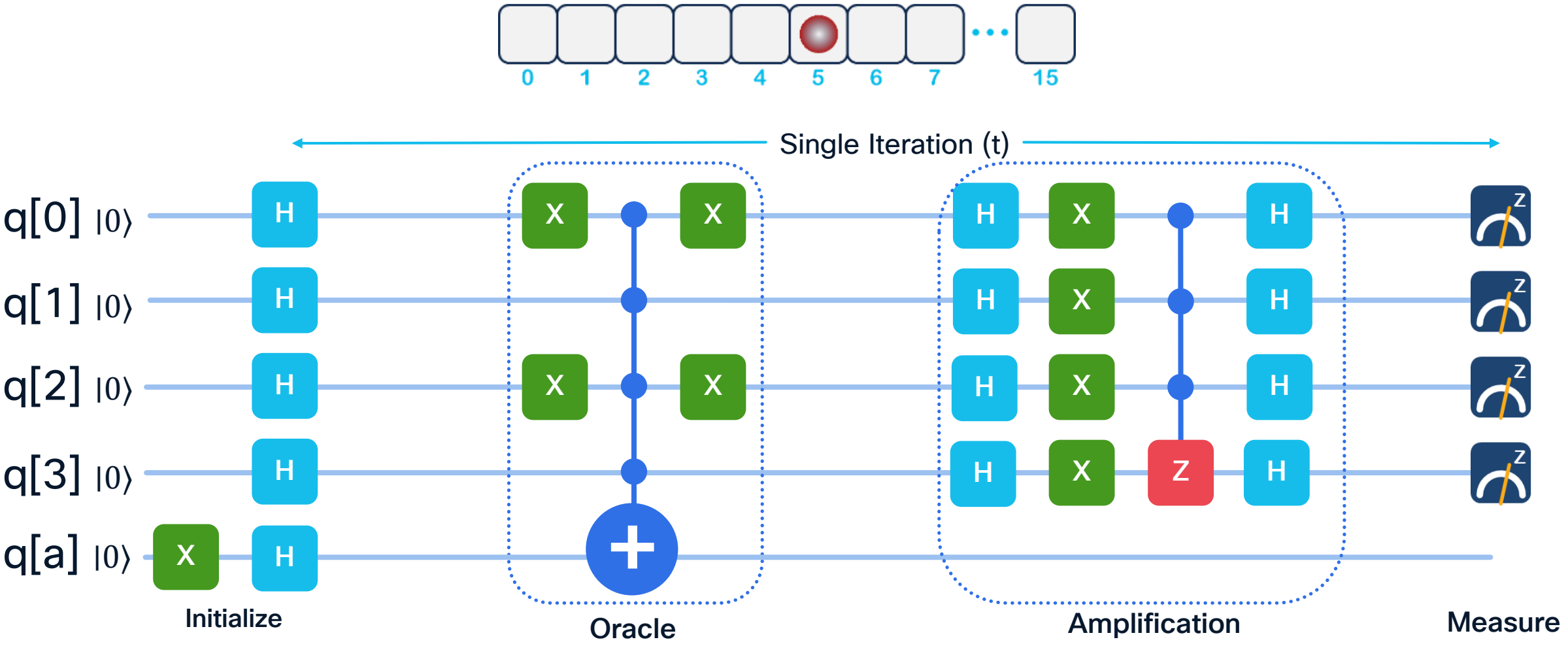


Shor's Algorithm:

- factorizes large numbers
- Exhibits **exponential** speed up over digital
- theoretically threatens the security of asymmetric key algorithms, such as the classical Public Key Infrastructure (PKI) including:
  - Diffie-Hellman (DH)
  - Elliptic Curve Cryptography (ECC), and
  - Elliptic Curve Diffie Hellman (ECDH)

© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm Quantum Circuit

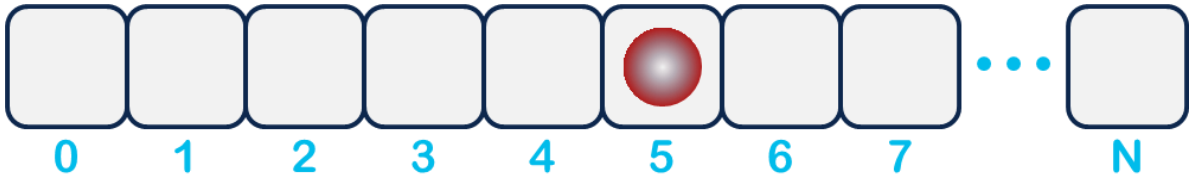


https://www.techscience.com/jqc/v3n4/46224/pdf

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Grover's Algorithm: Classic vs. Quantum



Classic Search

$f("red\ ball") \rightarrow$ "Position 5"

Worst Case: $N\ searches$

Quantum Search

$f("Pos\ 2?") \rightarrow$ "False"

$\vdots$

$f("Pos\ 5?") \rightarrow$ "True"

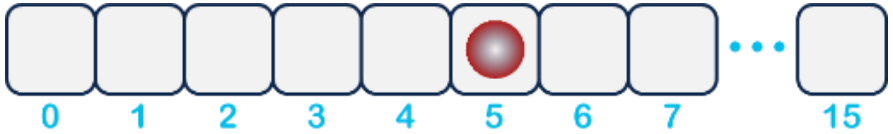
Worst Case: $\sqrt{N}\ searches$

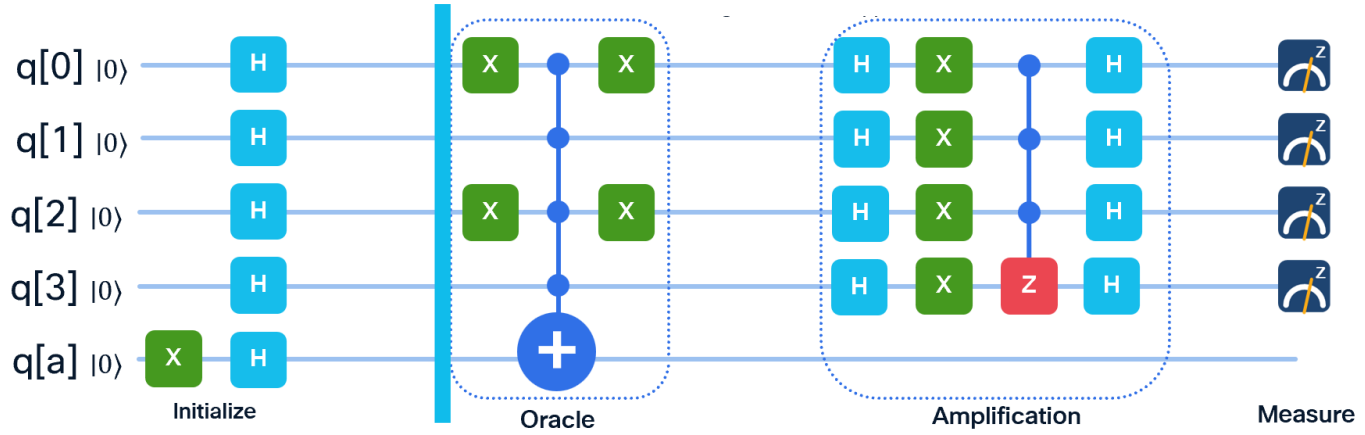
- Grover's Algorithm uses amplitude amplification to return the correct result with high probability
- As such, with quantum parallelism and interference management, Grover's Algorithm becomes **quadratically** faster than it's corresponding classical algorithm

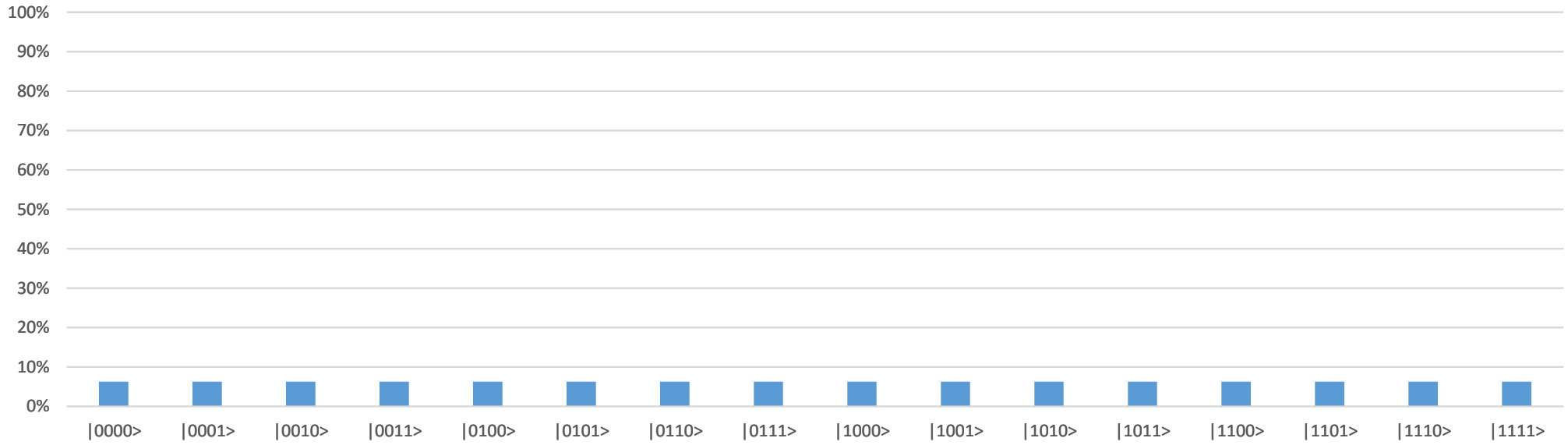
© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm

Initial Probability Distribution

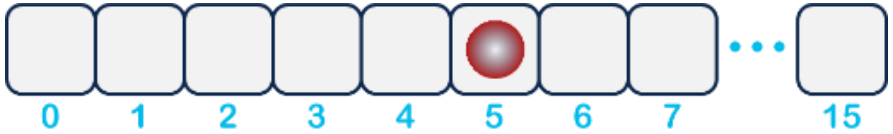




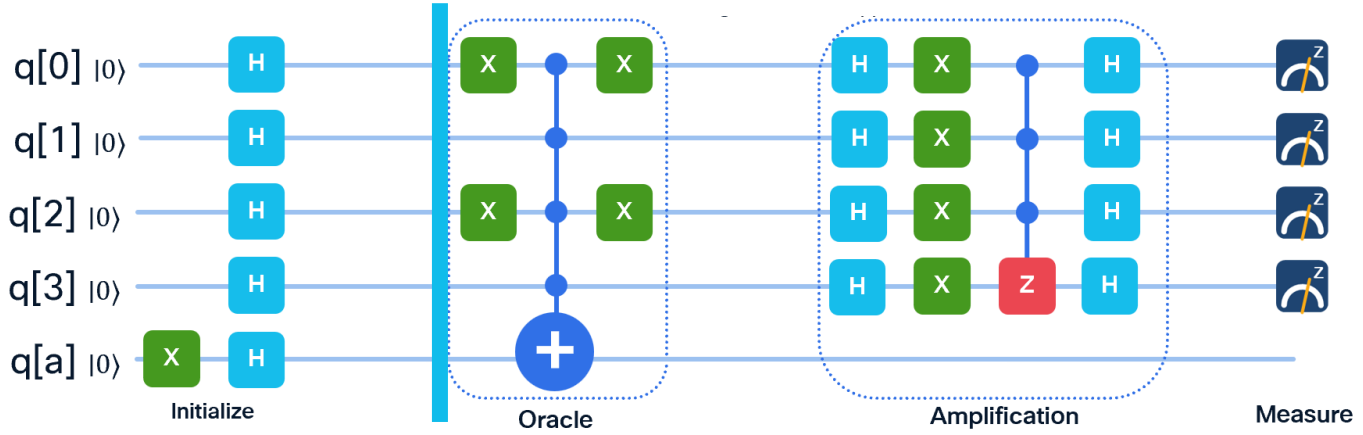


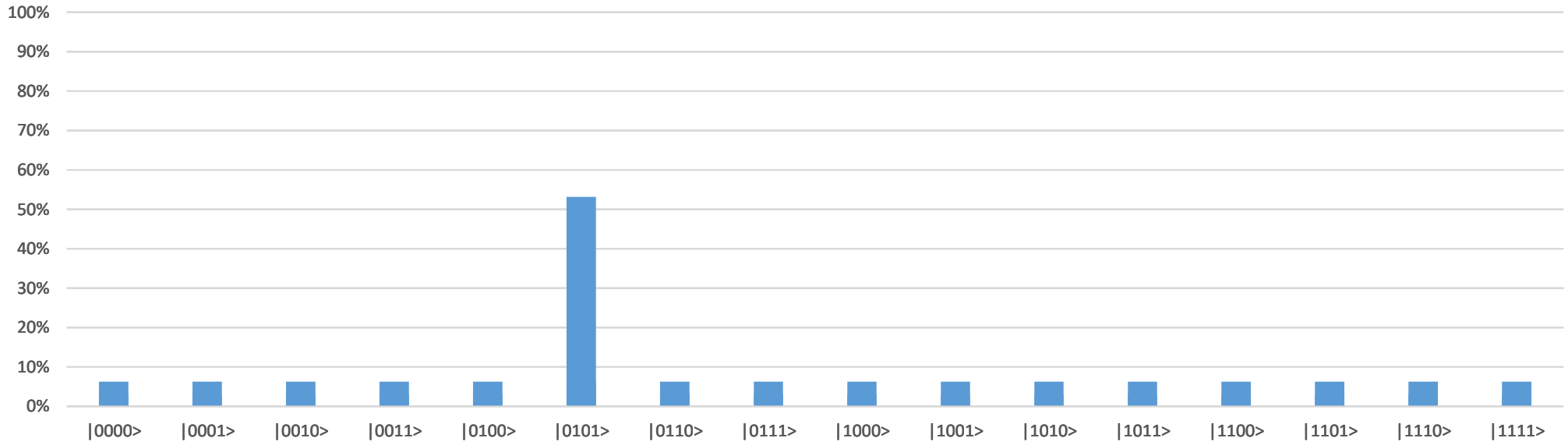
© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm



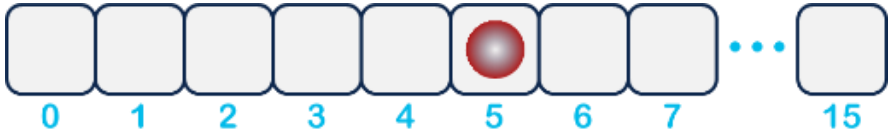
Probability Distribution after Round 1



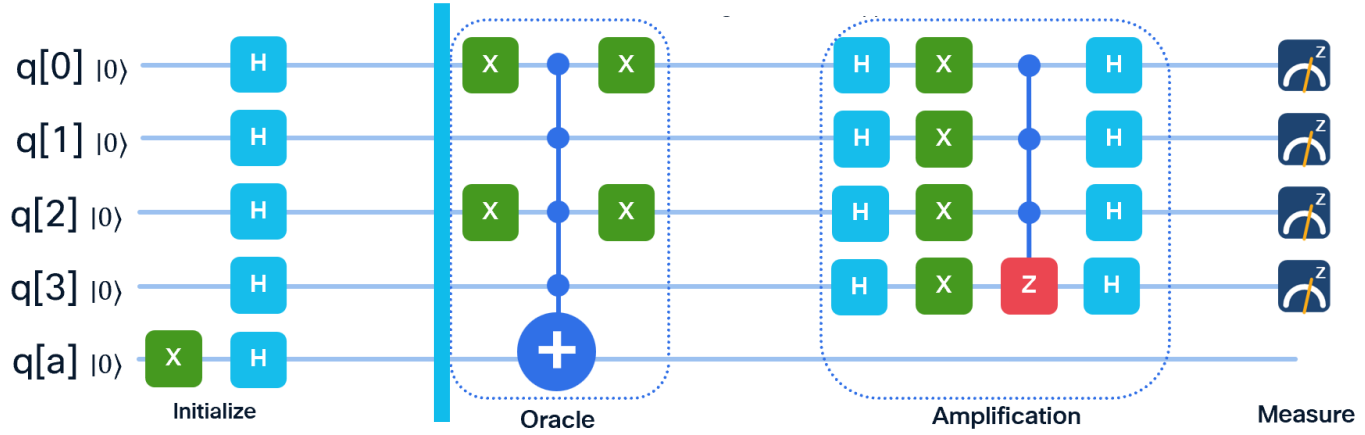


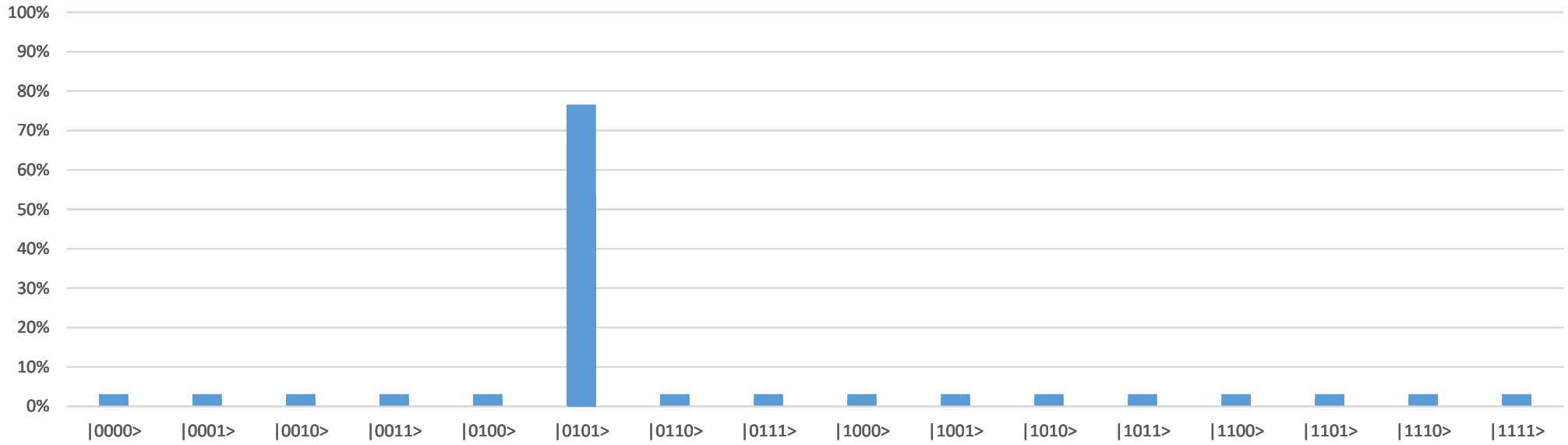
© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm



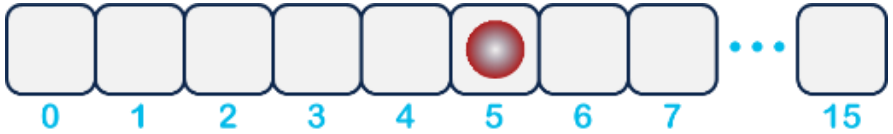
Probability Distribution after Round 2



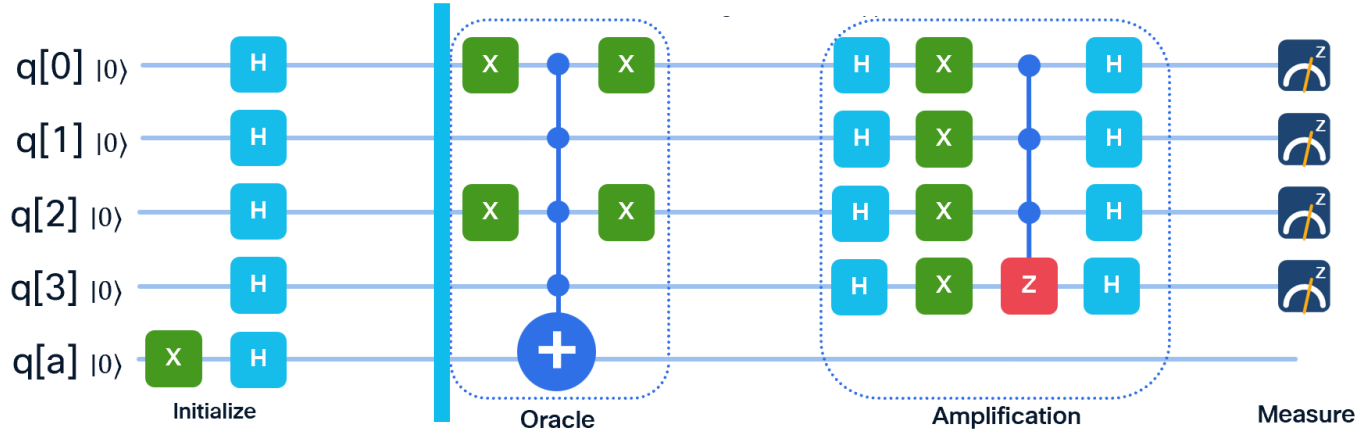


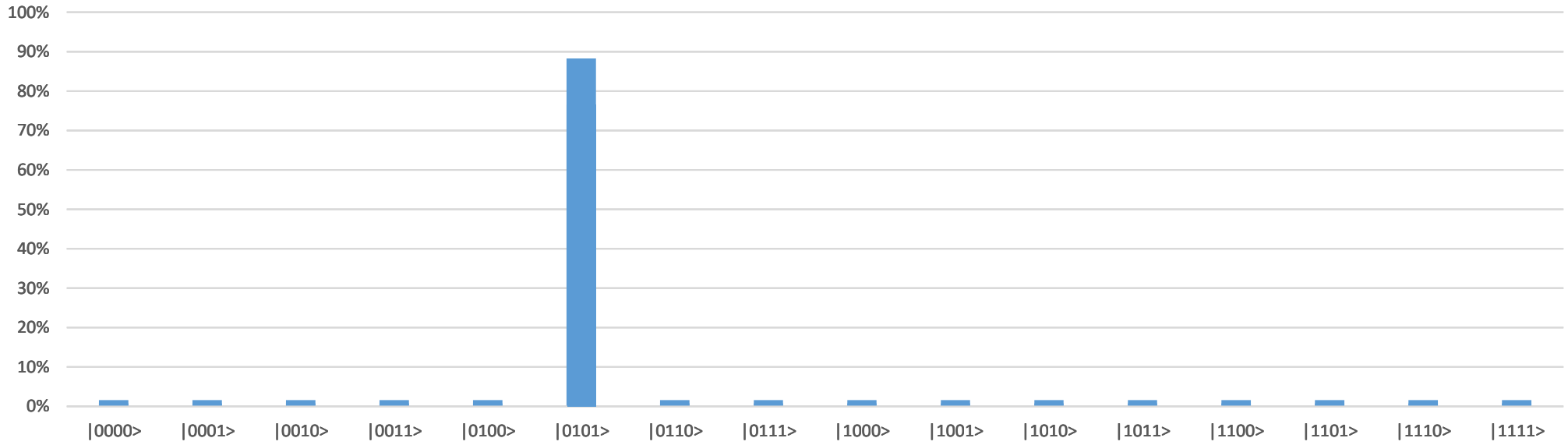
© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm



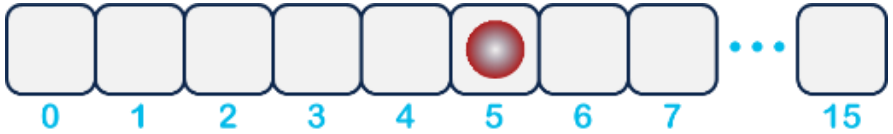
Probability Distribution after Round 3



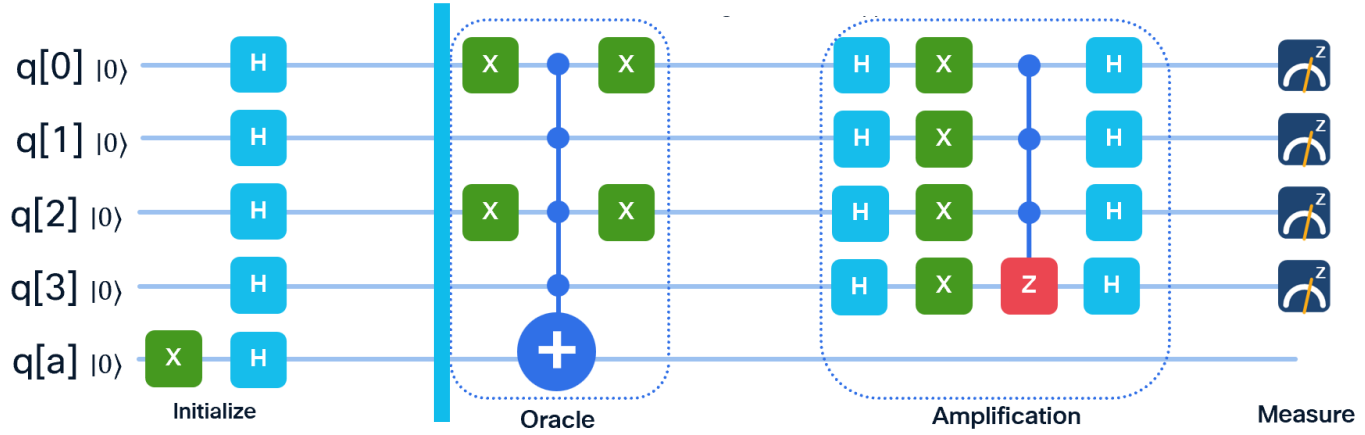


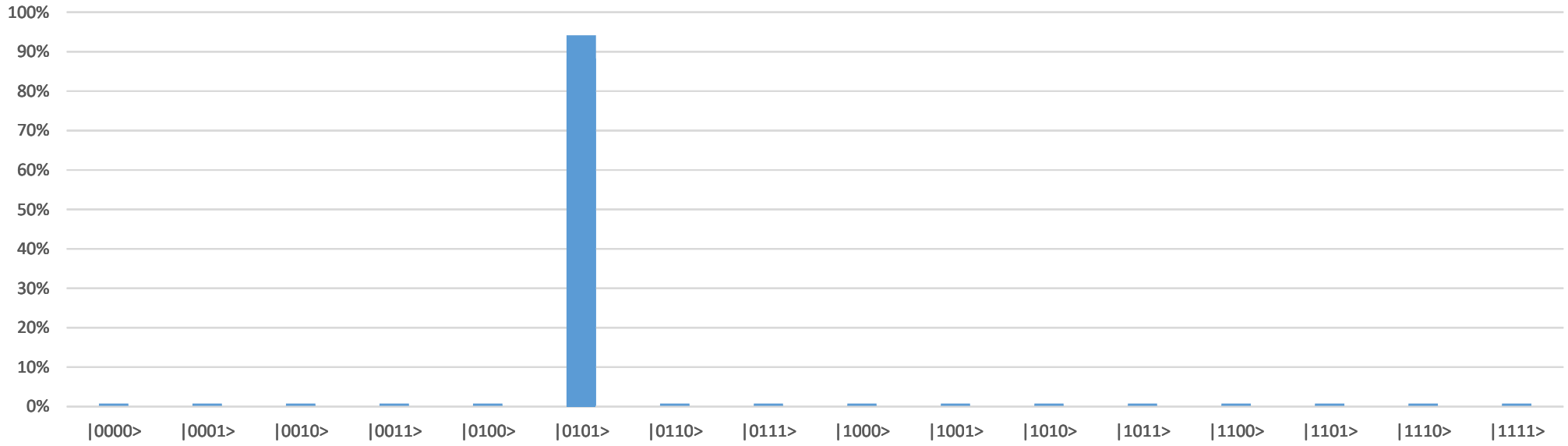
© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Algorithm



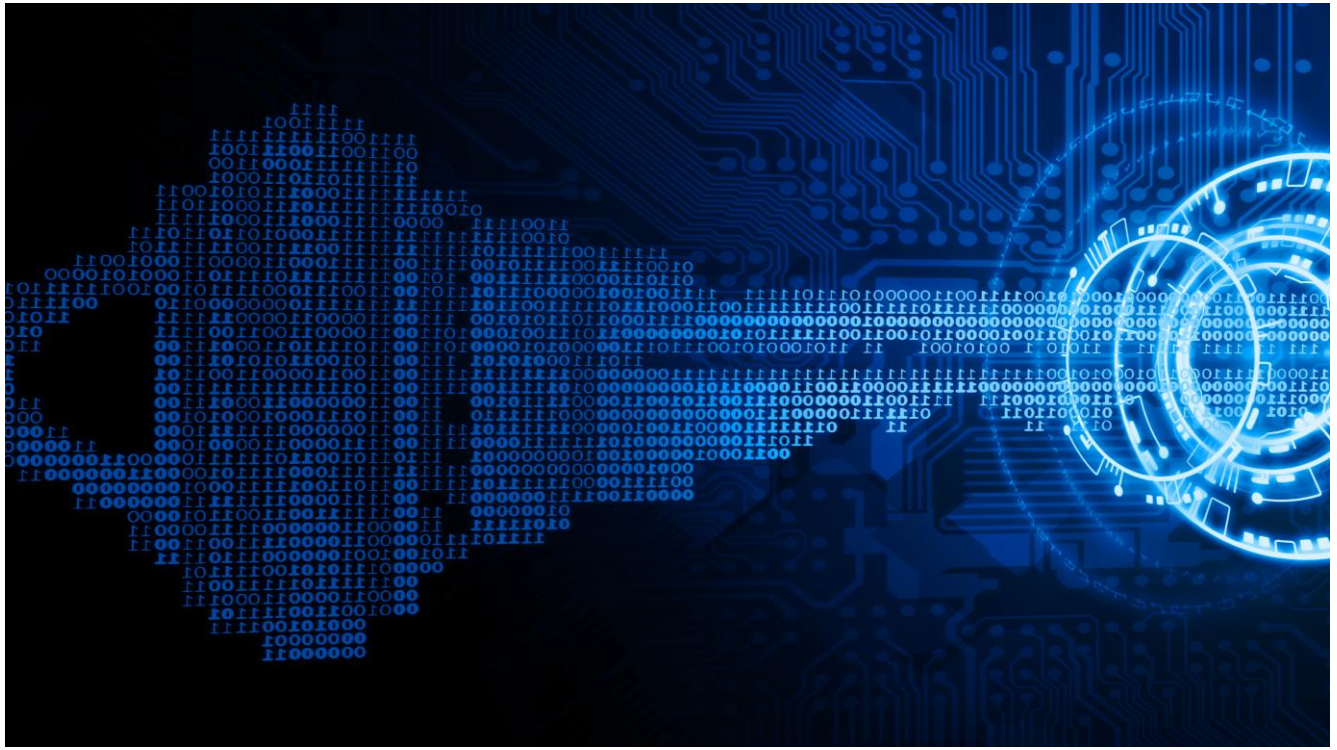
Probability Distribution after Round 4





© 2025 Cisco and/or its affiliates. All rights reserved.

How many Qubits Are Required to Break RSA and AES?



Experts estimate that:

RSA-2048 requires a quantum computer with 1,600 logically-corrected qubits to be broken

AES-256 requires a quantum computer with 6,681 logically-corrected qubits to be broken

https://arxiv.org/pdf/2505.15917
https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

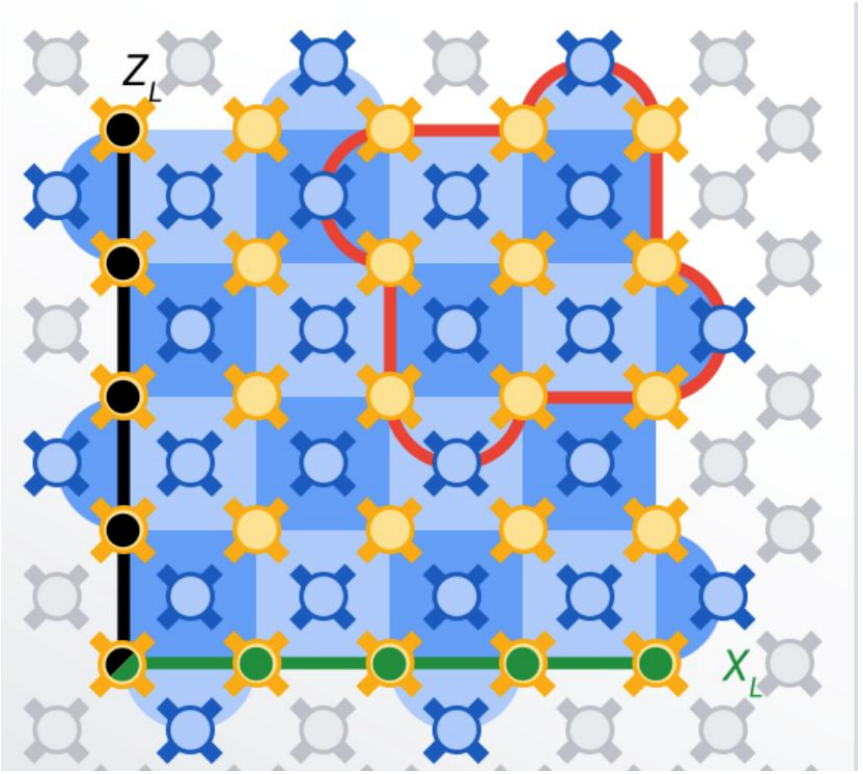
© 2025 Cisco and/or its affiliates. All rights reserved.

How Many Physical Qubits are Required to Produce a Logically-Corrected Qubit?

Qubits are notoriously fragile and extremely sensitive to the environment and can easily lose coherence (state)

The logical state of a qubit can be spread over many physical qubits to achieve Quantum Error Correction (QEC)

- In March 2023, Google realized a logical qubit (LQ) with just 49 physical qubits (PQ)
- In December 2023, Harvard scientists achieved the same result with just 48 qubits
- In February 2024, IBM achieved 12 logical qubits with 288 physical qubits (24 PQ/LQ)
- In April 2024, Microsoft and Quantinuum achieved 4 logical qubits with 30 physical qubits (7.5 PQ/LQ)



https://blog.google/inside-google/message-ceo/our-progress-toward-quantum-error-correction/
https://thequantumrecord.com/quantum-computing/breakthrough-in-quantum-error-correction/
https://pmc.ncbi.nlm.nih.gov/articles/PMC10972743/
https://spectrum.ieee.org/microsoft-quantum-computer-quantinuum

© 2025 Cisco and/or its affiliates. All rights reserved.

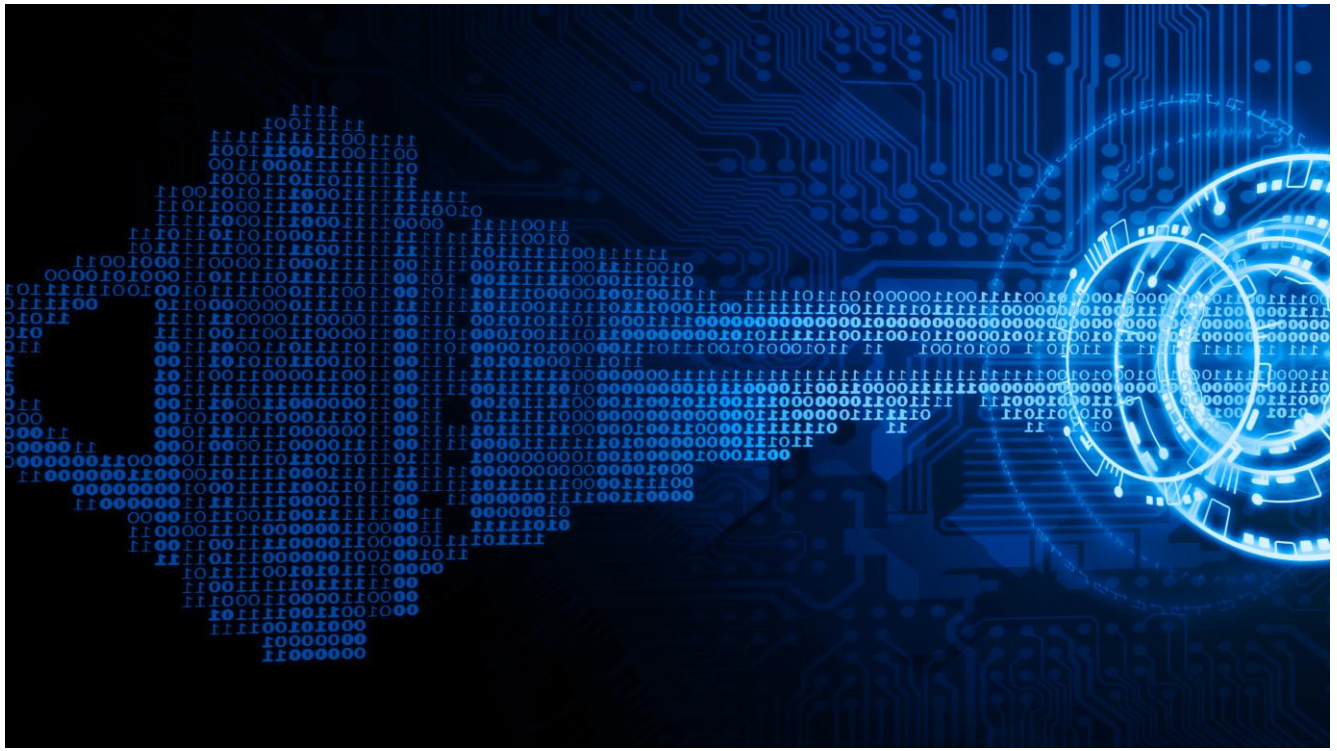
So, Really… How Many Qubits Are Required to Break AES?

Let’s assume 561 physical qubits for one logically-corrected qubit (per Gidney-2025)

AES-256 requires a quantum computer with 6,681 logically-corrected qubits to be broken

(6681 * ~561) = 3,748,041

But there’s more to consider…



https://arxiv.org/pdf/2505.15917
https://pqcrypto2016.jp/data/Langenberg-Grover-AES.pdf

© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Achilles Heel: Quadratic Speed-Up

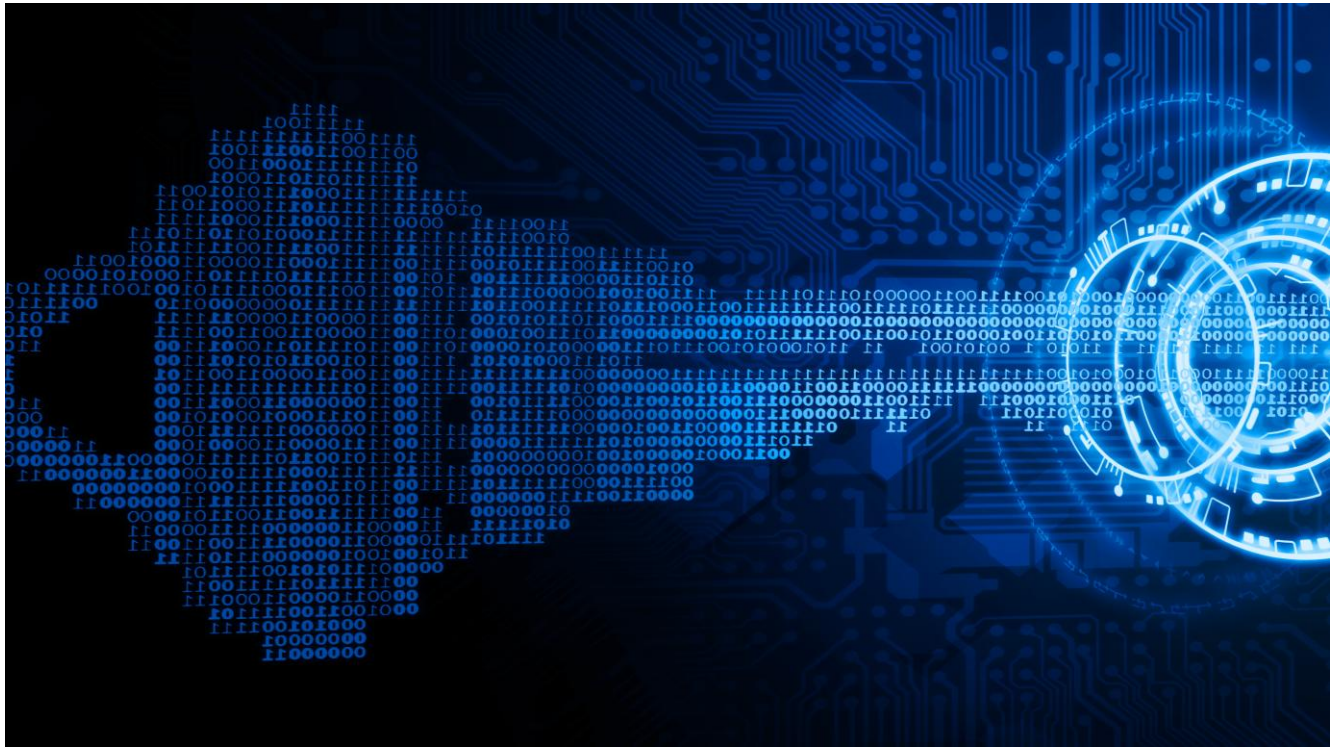
- Grover's algorithm only offers **quadratic** speed up, and does NOT parallelize well
- It is acknowledged that if an attacker had a quantum computer that can issue circa 2^{128} successive evaluations, then they could find the key with high probability
- However, in this attack model, even a 160-bit key (which would require circa 2^{80} successive evaluations), would be secure for all practical purposes
  - For example, even if we assume that the quantum computer could evaluate the encryption function in the absurdly fast time of 1 picosecond, the total of 2^{80} successive evaluations would require over 30,000 years to complete
- Any realistic security policy is not concerned with an attack that takes that long to perform

https://eprint.iacr.org/2017/811.pdf

Key Takeaway:
As such, AES-256 is considered quantum resistant, *provided* the key exchange is also secure (i.e. not via PKI)

© 2025 Cisco and/or its affiliates. All rights reserved.

But What About RSA? How many Qubits are required to Break RSA?



Experts estimate that:

RSA-2048 requires a quantum computer with 1,600 *logically-corrected* qubits to be broken

And that these could be expressed via 897,864 *physical* qubits

Key Takeaway: RSA is very much under threat by quantum computing!!!

https://arxiv.org/pdf/2505.15917

- Shor's algorithm exhibits ***exponential*** quantum speed-up, as compared to classical computing systems, and
- Quantum computers are *increasing* in size, while
- Quantum Error Correction circuits are *decreasing* in size

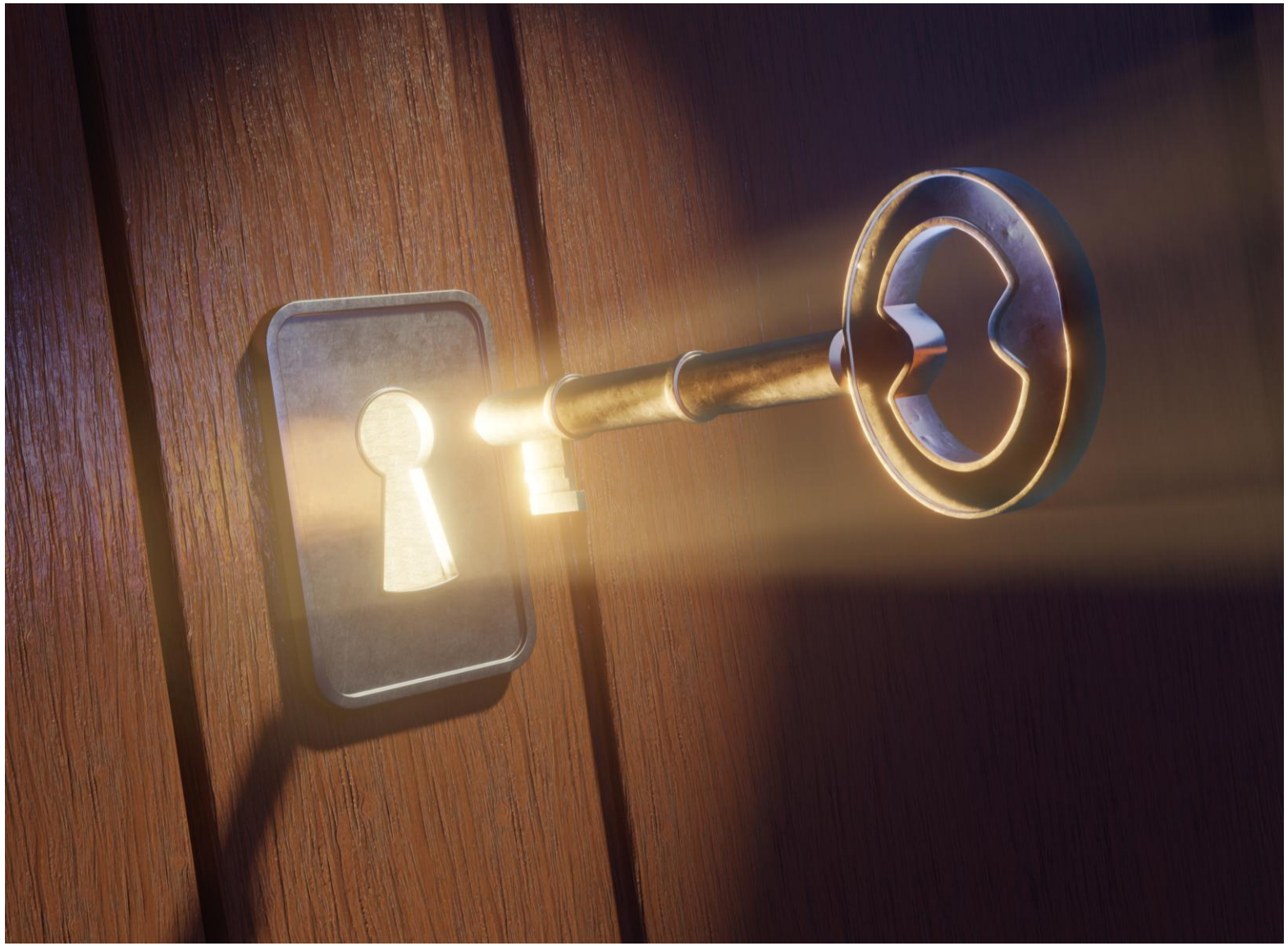
© 2025 Cisco and/or its affiliates. All rights reserved.

Y2Q, CRQC and SNDL

Years to Quantum (Y2Q) refers to the unknown number of years until Cryptographically Relevant Quantum Computers (CRQC) become available

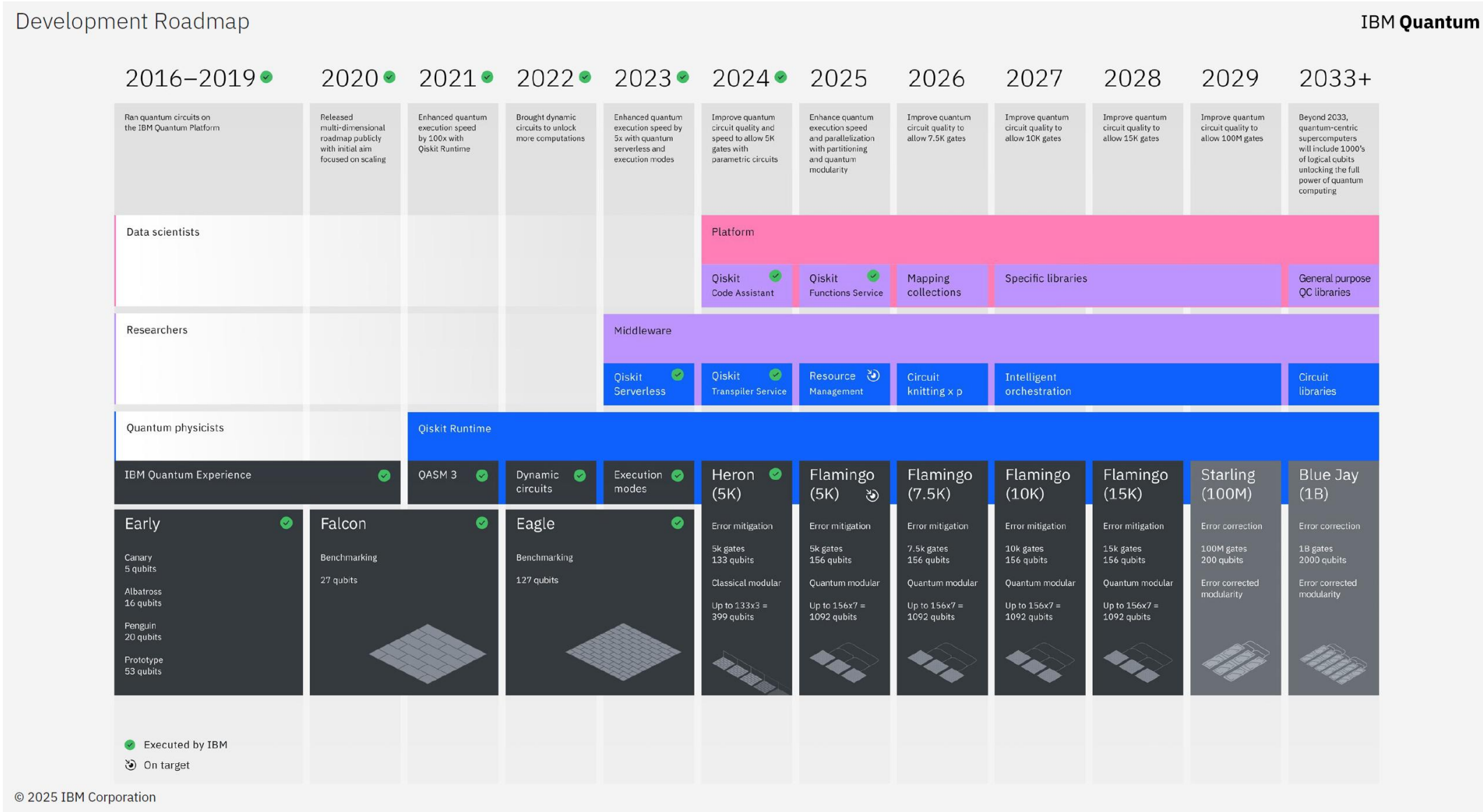
A CRQC can compute prime factorizations in polynomial time, thereby rendering public key algorithms all but obsolete

However, an adversary can capture network traffic today in the hopes of decrypting it later with a CRQC; this is called a Store Now, Decrypt Later (SNDL) or Harvest Now Decrypt Later (HNDL) type of attack



© 2025 Cisco and/or its affiliates. All rights reserved.

How Far Off Is That?



https://www.ibm.com/quantum/assets/IBM_Quantum_Developmen_&_Innovation_Roadmap_Explainer_2024-Update.pdf

How Many Y2Q?

Cloud Security Alliance:

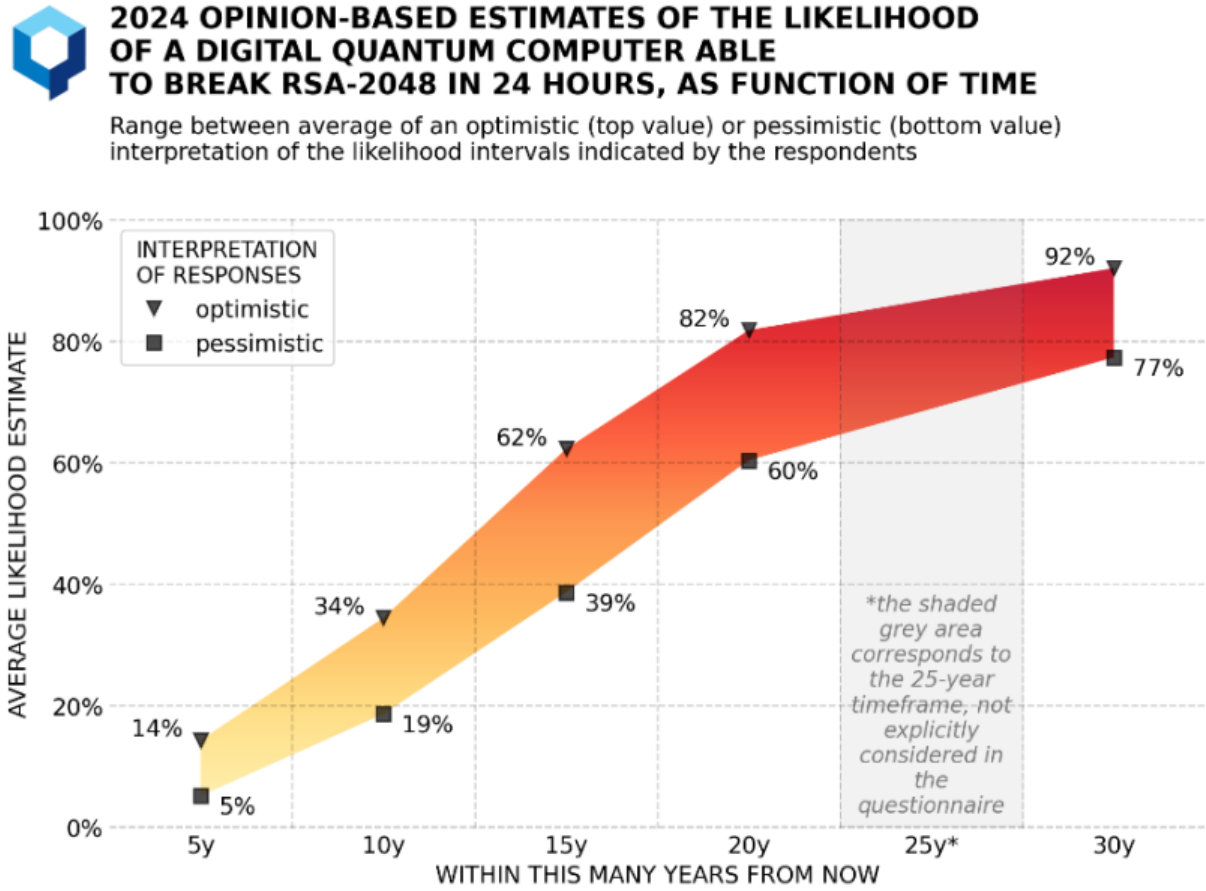
- April 14, 2030

Global Risk Institute:

- ~50% of experts predict 15 years

White House / NIST

- “in the not-too-distant future”



https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum/
https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

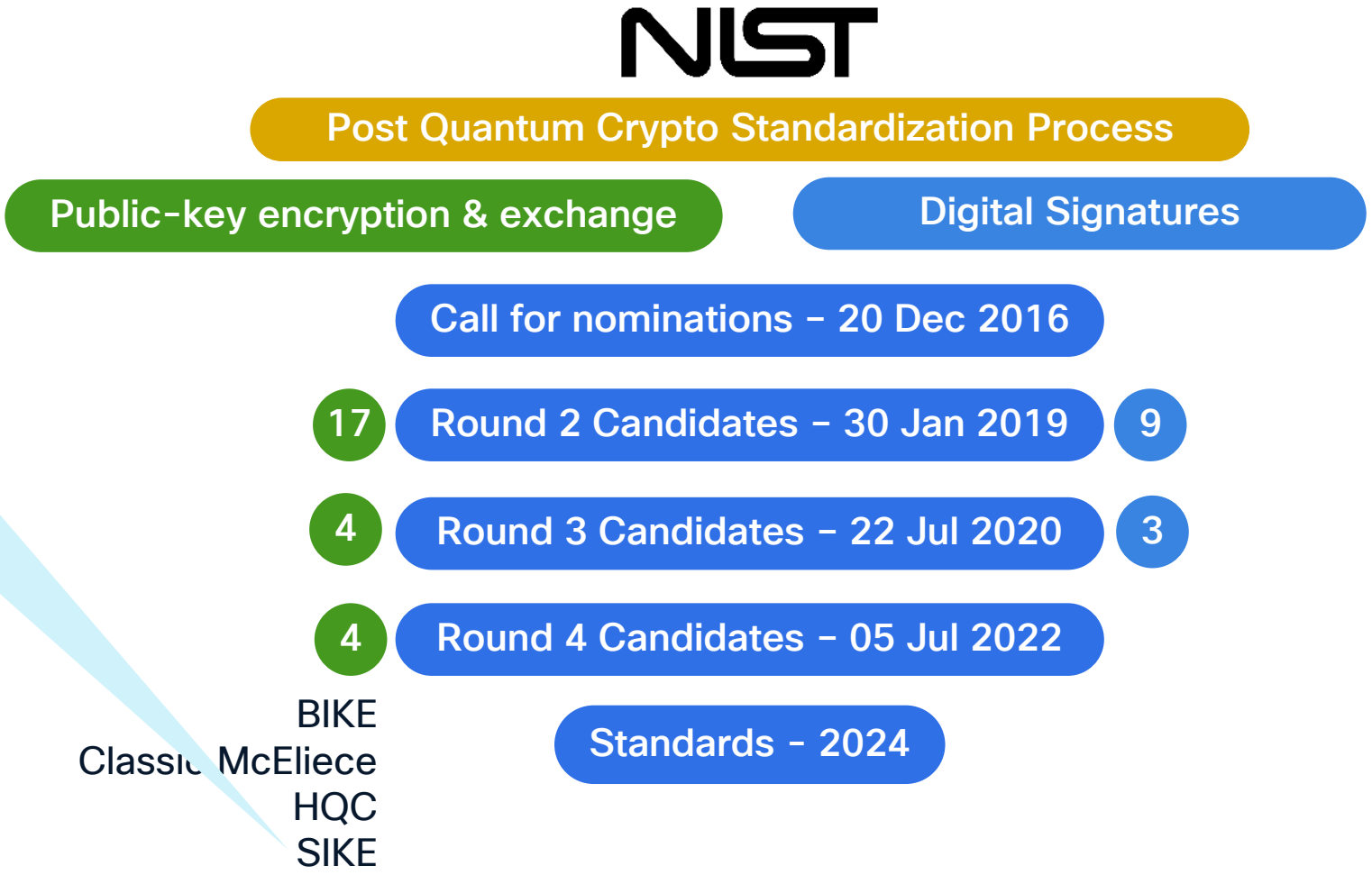
© 2025 Cisco and/or its affiliates. All rights reserved.

Post Quantum Cryptography (PQC) Overview

In August 2022, SIKE was cracked on a single core laptop in just one hour

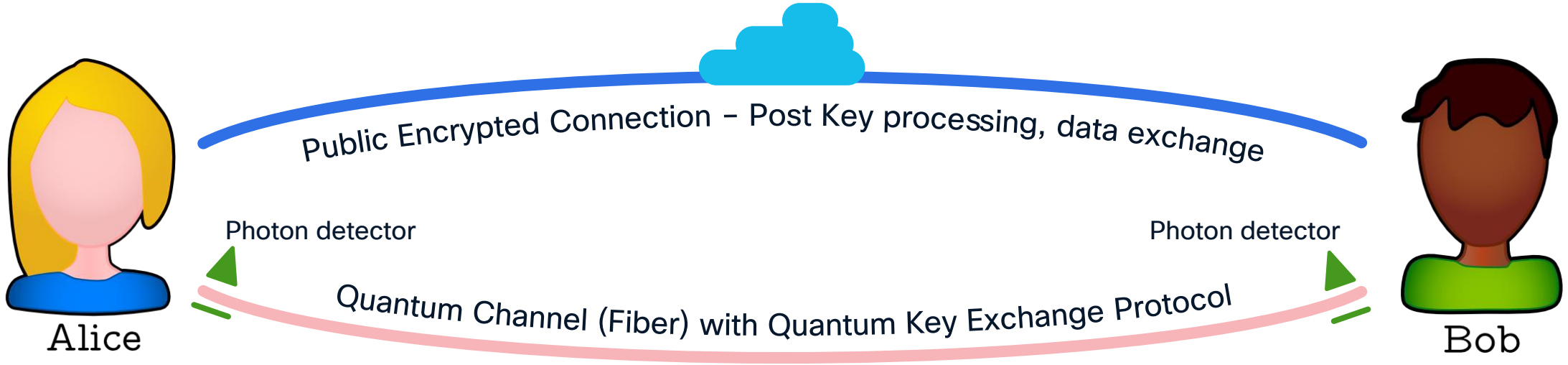
Post Quantum Cryptography (PQC) is the study of cryptographic algorithms that are designed run on a classical computer but are resistant to attack from quantum computers

National Institute of Standards and Technology (NIST) is leading the standardization efforts for PQC



https://csrc.nist.gov/projects/post-quantum-cryptography

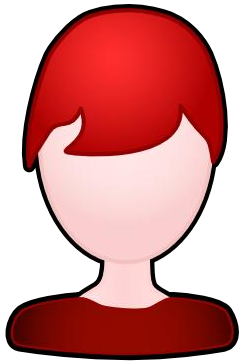
Quantum Key Distribution (QKD)



QKD has already been achieved over distances of 1000 km

QKD requires a direct connection because current optical switches would destroy the quantum effect.

A superior solution would be a Quantum Internet



QKE protocols like BB84, BBM92 & E91 measure received quantum states

An eavesdropper will be unable to read information encoded in a quantum state and any attempt at eavesdropping will be immediately detected by the sender and receiver

https://phys.org/news/2023-06-scientists-km-quantum-key.html

© 2025 Cisco and/or its affiliates. All rights reserved.

Three Requirements to be Quantum-Safe

- Management Plane
- Control Plane
- Data Plane

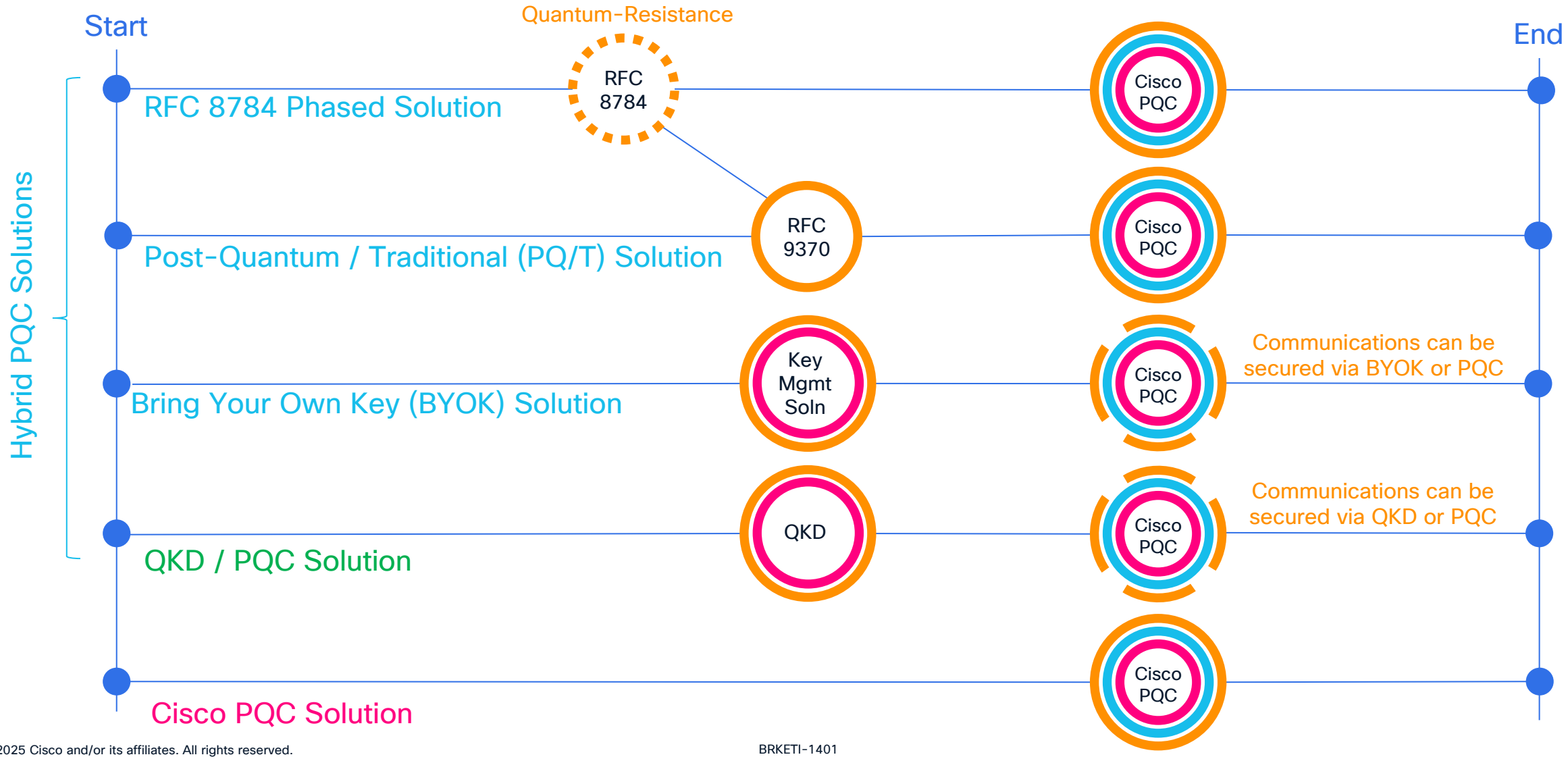
- Secure Firmware
- Secure Software
- Secure Runtime
- Secure Identity

The capabilities needed to replace and adapt to continually evolving cryptographic algorithms while preserving security and ongoing operations

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum-Safe Journey Maps



© 2025 Cisco and/or its affiliates. All rights reserved.

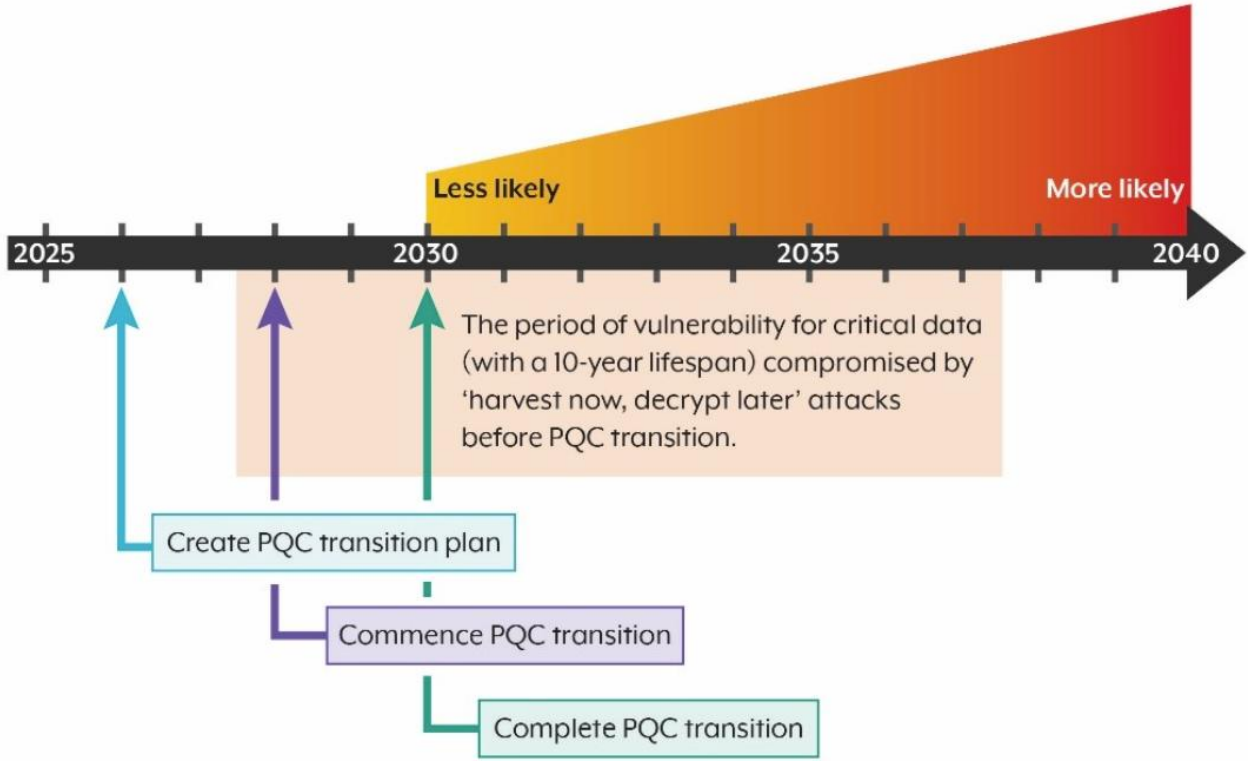
The Urgency of the Threat

In direct response to the quantum threat, governments are mandating application and infrastructure upgrades within the next few years

For example, this Australian Signal's Directorate has issued the following recommendations and timelines:

- By the end of 2026: Organizations are expected to have a refined plan for their PQC transition
- By the end of 2028: Organizations should commence their transition to PQC
- By the end of 2030: Organizations are advised to have completed their PQC transition

The private sector is moving even faster

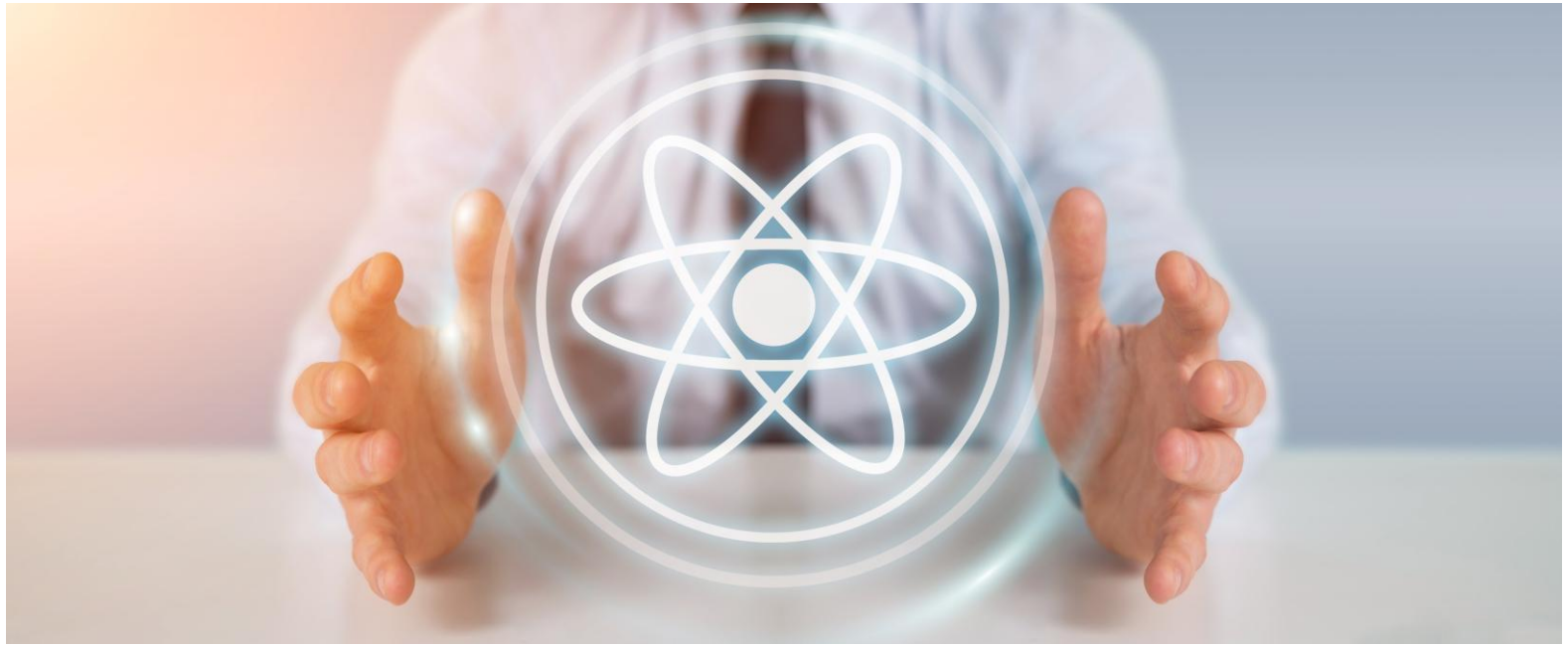


https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Quantum-Ready Services

Mission: Empower our customers to proactively protect their organizations from emerging quantum threats, while enabling them to harness the massive transformative potential of quantum technologies to drive innovation and business growth.



© 2025 Cisco and/or its affiliates. All rights reserved.

An Introduction to Quantum Networking

Photonic Qubits

Photons can represent qubits, as well as electrons

Photons are more conducive to quantum networking than electrons (electrons are more conducive to computing)

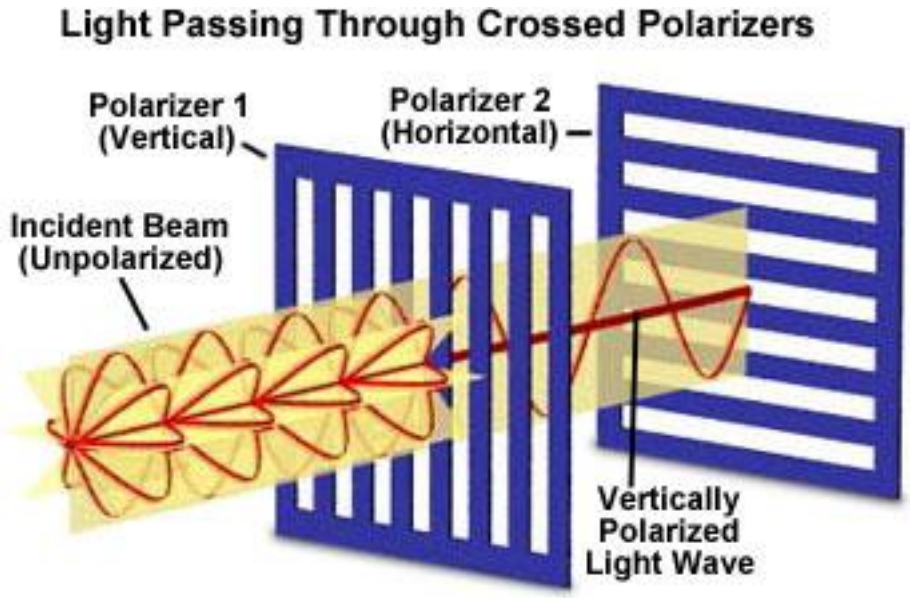
The logical states of 0 or 1 are not determined by the spin of photons, but rather by their polarization

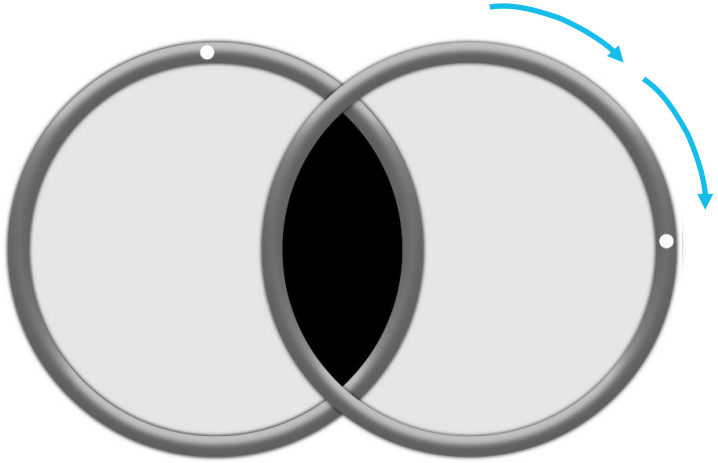
Horizontal Polarization $|1\rangle$

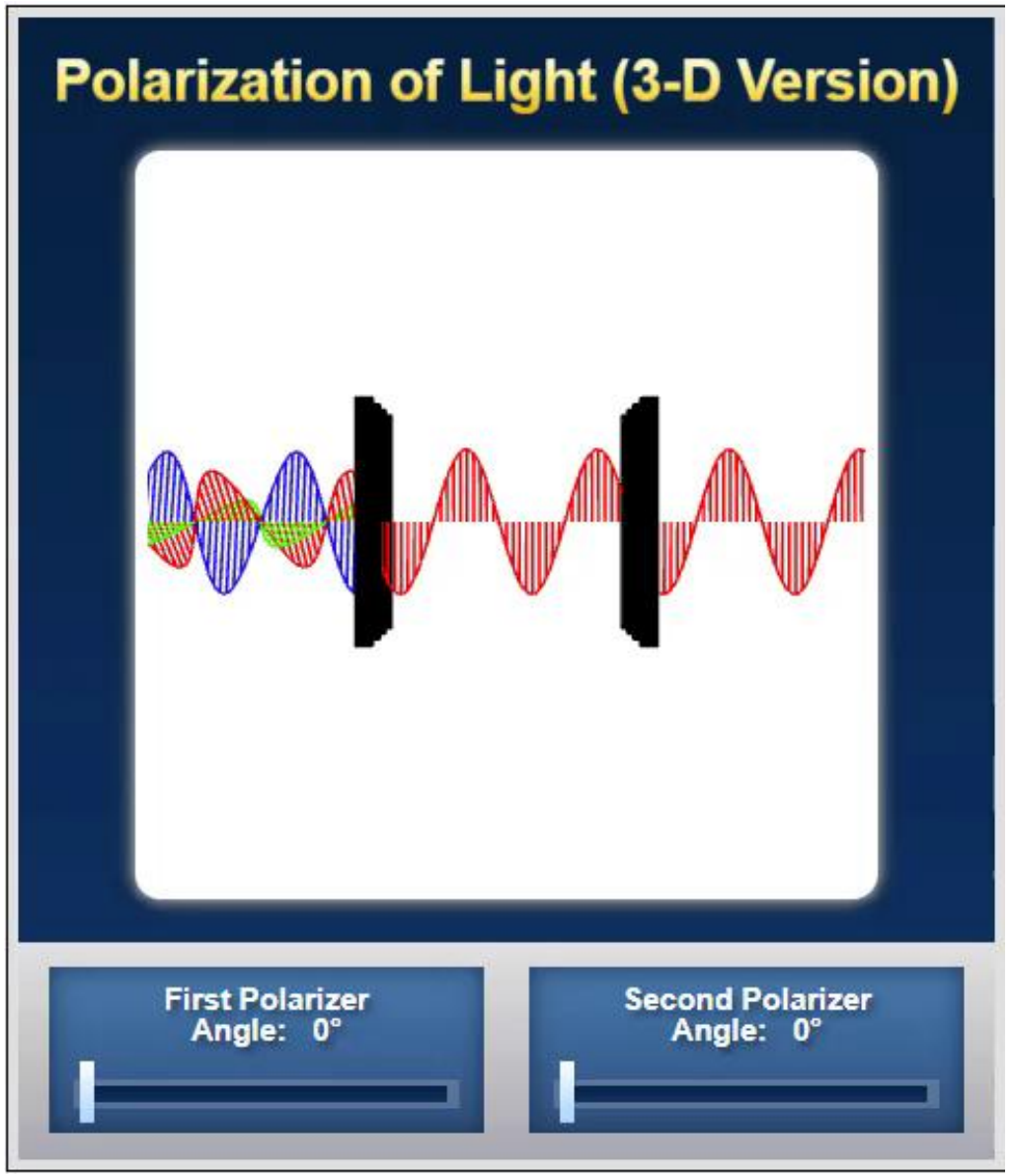
Vertical Polarization $|0\rangle$

© 2025 Cisco and/or its affiliates. All rights reserved.

Polarization Quick Recap



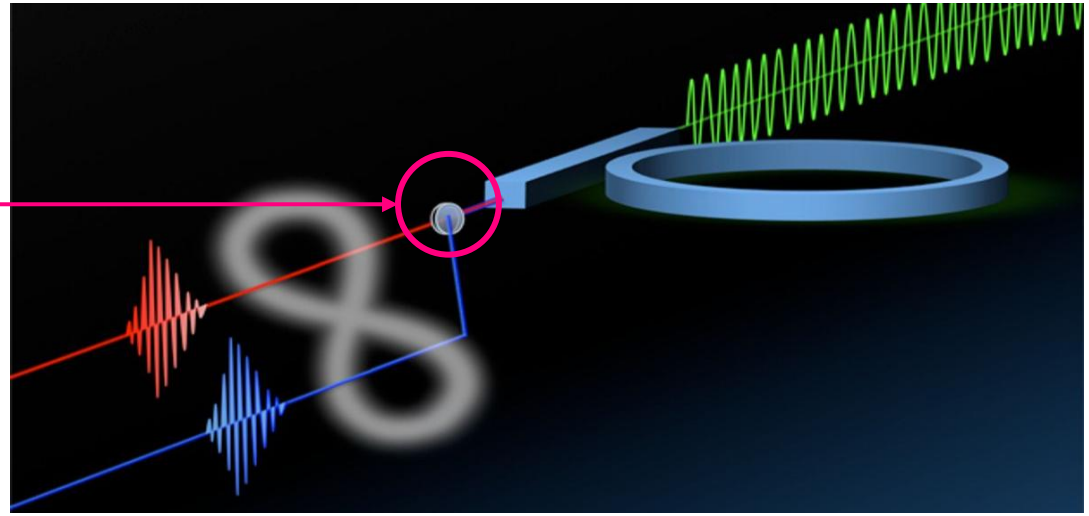


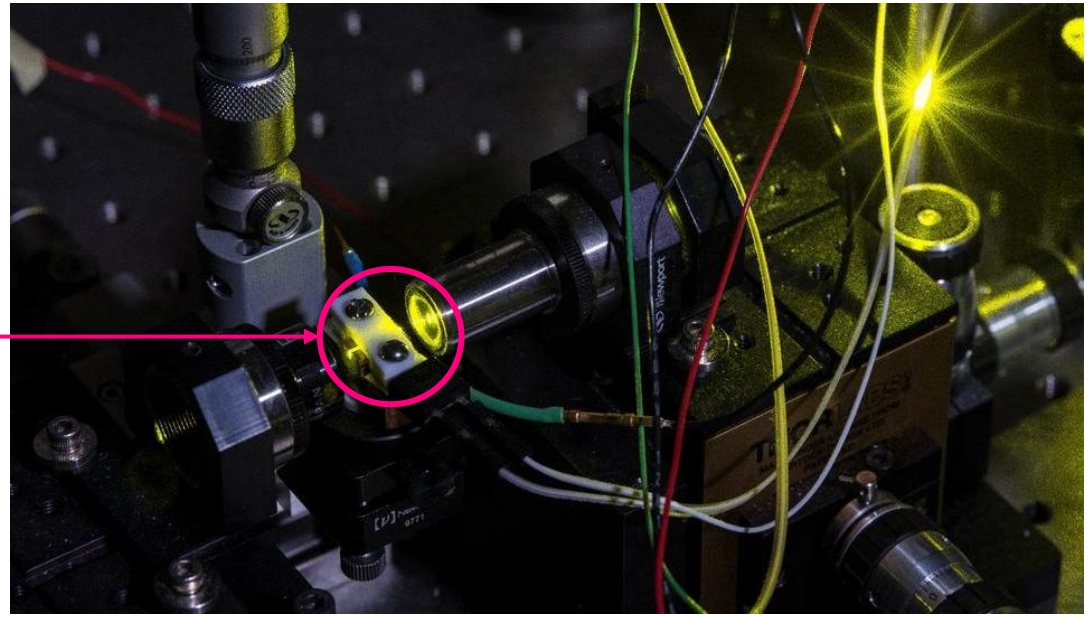


https://www.olympus-lifescience.com/en/microscope-resource/primer/lightandcolor/polarization/
https://www.olympus-lifescience.com/en/microscope-resource/primer/java/polarizedlight/3dpolarized/

© 2025 Cisco and/or its affiliates. All rights reserved.

How Are Photons Entangled?





The most common approach to generate entangled photons is via Spontaneous Parametric Down-Conversion (SPDC) in nonlinear crystals

SPDC is an instant optical process that converts one photon of higher energy into a pair of photons of lower energy

https://www.nature.com/articles/s41377-021-00537-2
https://spectrum.ieee.org/entanglement-on-a-chip
https://www.nist.gov/image/non-linear-crystal

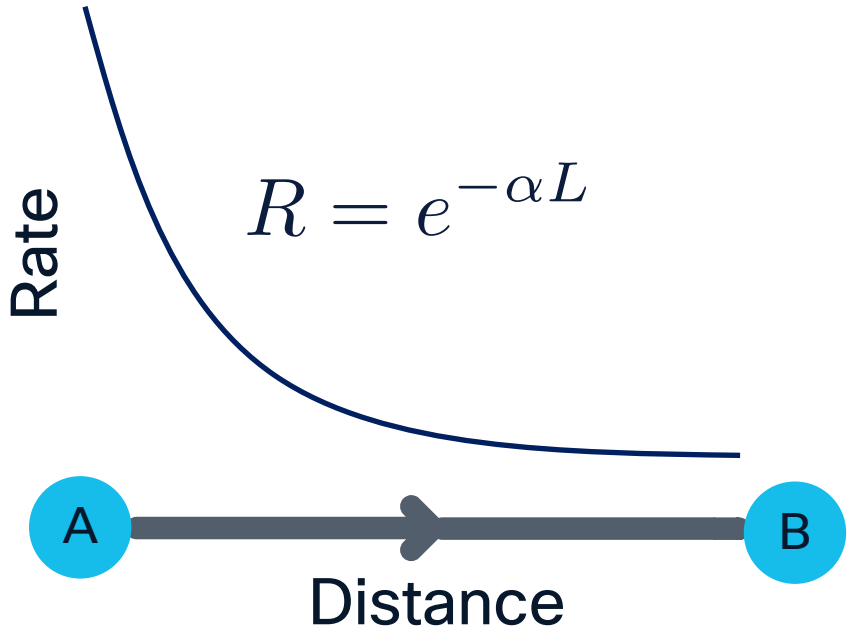
Classical Optical Communication

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Communication via Transporting

© 2025 Cisco and/or its affiliates. All rights reserved.

Primary Challenge to Quantum Transport



Rate decays exponentially with distance

Can we amplify the signal?

No, because of the No Cloning Theorem

© 2025 Cisco and/or its affiliates. All rights reserved.

(Two-Way) Quantum Communication via Teleporting

Initial State

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Communication via Teleporting

Step 1: Entangle a Pair of Photons and Send One to the Receiver

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Communication via Teleporting

Step 2: Perform Another Entanglement Operation at the Sender

Note: This step results in a teleportation of the ***combination*** of the states of qubits Q and A to qubit B

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Communication via Teleporting

Step 3: Perform a Bell State Measurement at the Sender

Note: The Bell State Measurement simultaneously:
- breaks the three-way entanglement,
- collapses the superposition of qubit A, and
- produces a result of 1 of 4 Bell States

Note: ⊗ is a mathematical notation for a tensor product; that is, a product of two quantum states, $|\psi\rangle$ and $|\Phi\rangle$

The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00

$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01

$|\psi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10

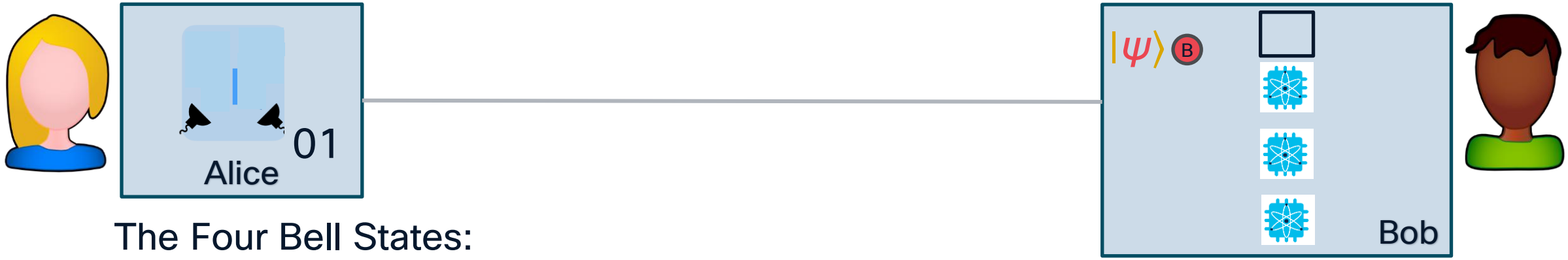
$|\psi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Communication via Teleporting

Step 4: Send the Bell State Measurement Result over a Classical Channel



The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00

$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01

$|\psi^+\rangle = (1/\sqrt{2}\,)\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10

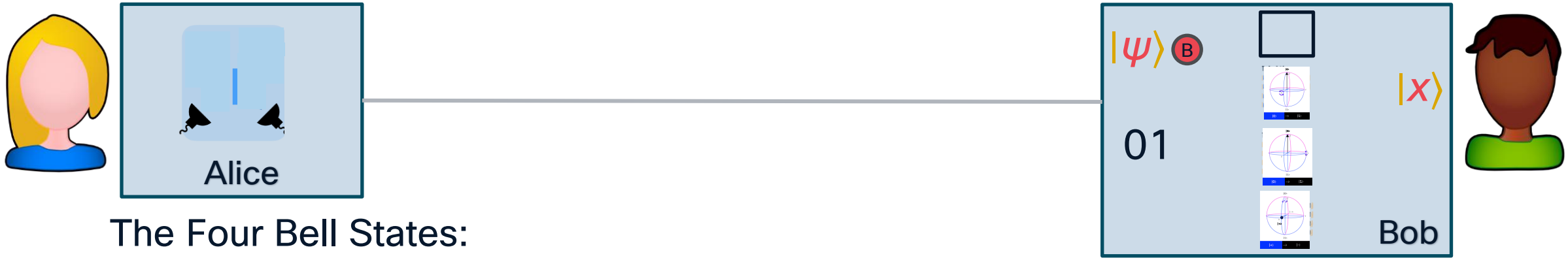
$|\psi^-\rangle = (1/\sqrt{2}\,)\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Communication via Teleporting

Step 5: Perform a Correction Operation on the Received Qubit (if necessary)



The Four Bell States:

$|\Phi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle)$ represented by binary 00 → nothing to correct

$|\Phi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|0\rangle - |1\rangle\otimes|1\rangle)$ represented by binary 01 → rotate around x-axis

$|\psi^+\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle + |1\rangle\otimes|0\rangle)$ represented by binary 10 → rotate around y-axis

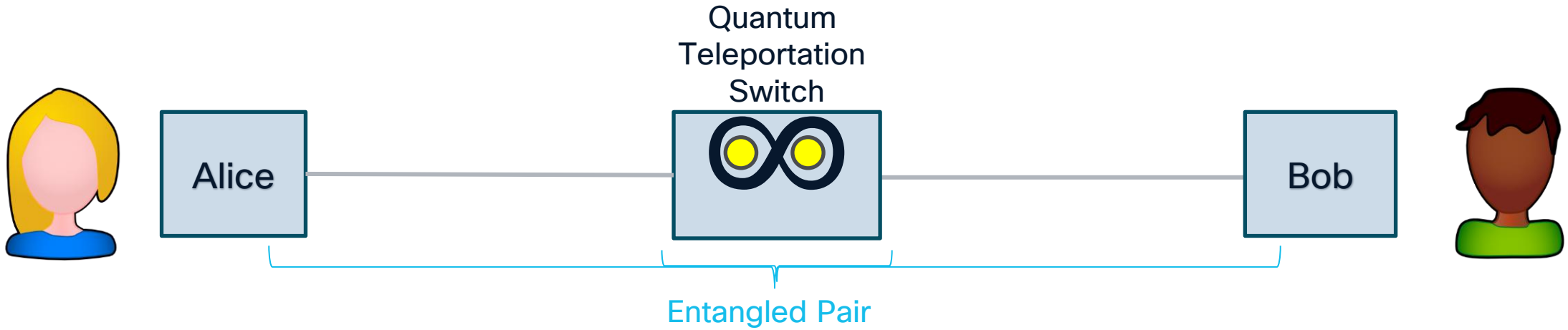
$|\psi^-\rangle = (1/\sqrt{2})\,(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ represented by binary 11 → rotate around z-axis

© 2025 Cisco and/or its affiliates. All rights reserved.

Refer to Bloch Sphere diagram for x,y and z axis

Quantum Teleporting Switch

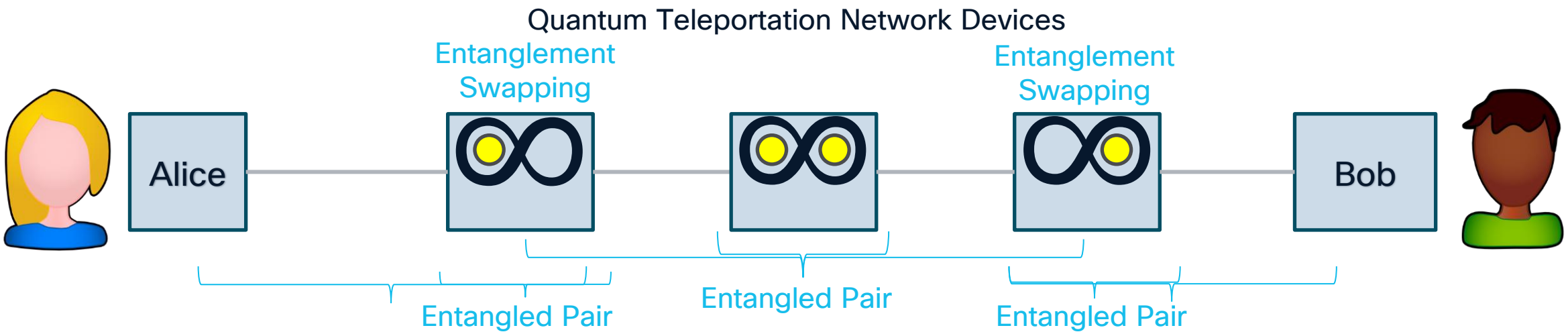
Providing Entanglement in the Network vs. the Endpoint



© 2025 Cisco and/or its affiliates. All rights reserved.

Extending Quantum Teleporting

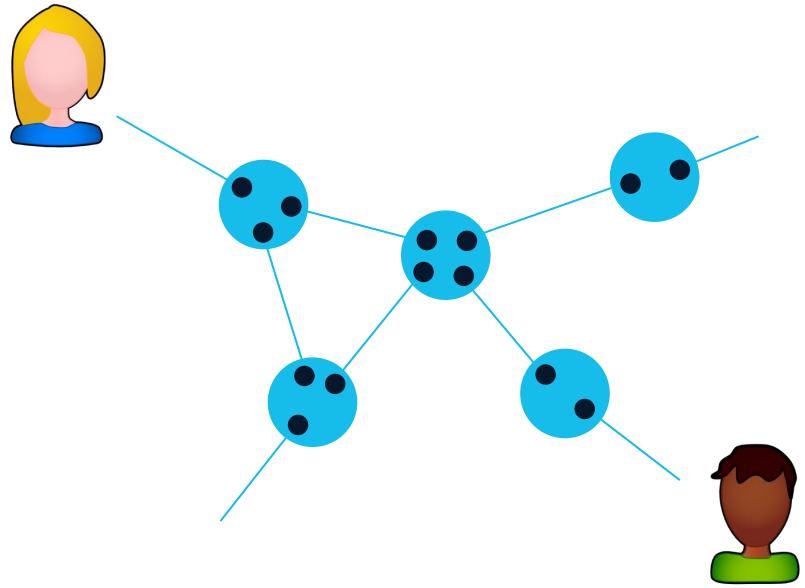
Introducing Entanglement Swapping



© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Routers & Protocols

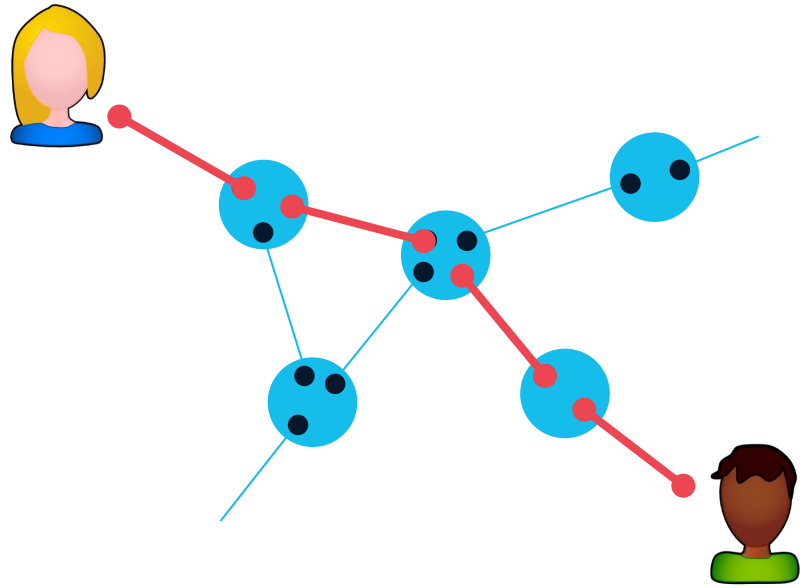
Two-Way Entanglement Distribution Network Example



© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



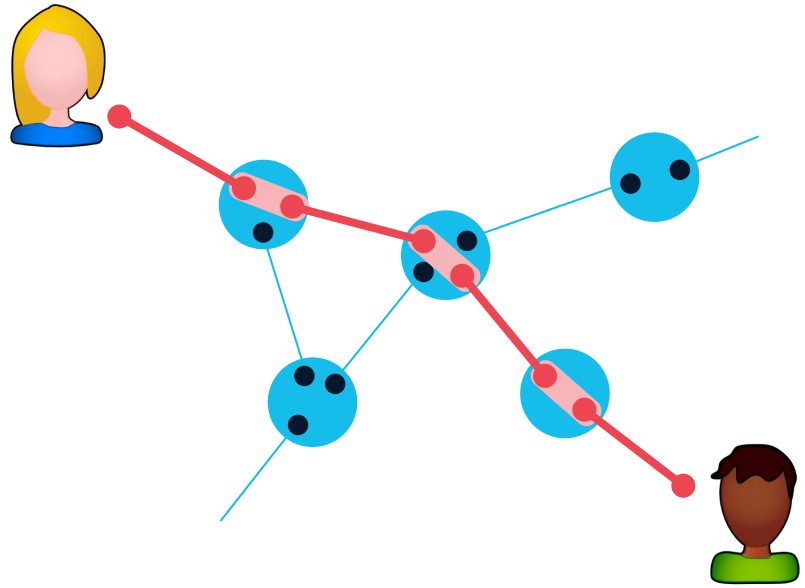
Elementary Link Entanglements

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



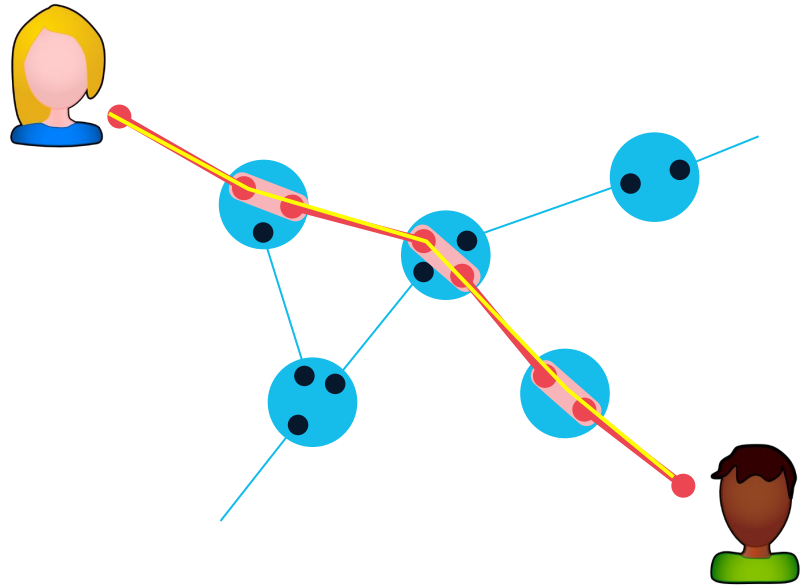
Entanglement Swapping

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



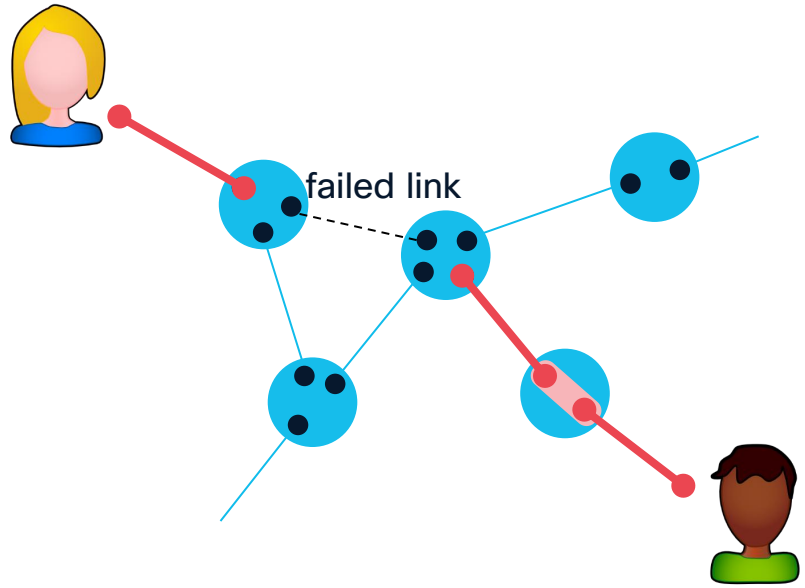
End-to-End Entanglement

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



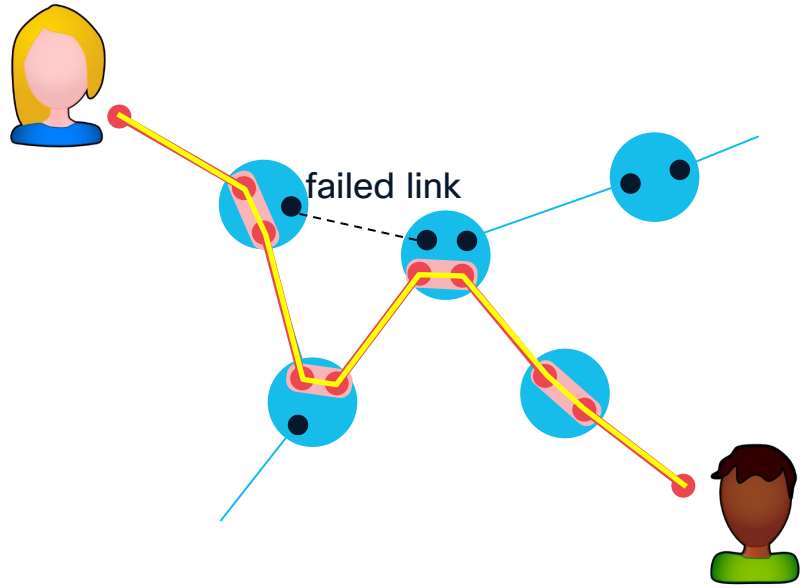
Network Failure Event

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum Routers & Protocols

Two-Way Entanglement Distribution Network Example



Reestablishing End-to-End Entanglement

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

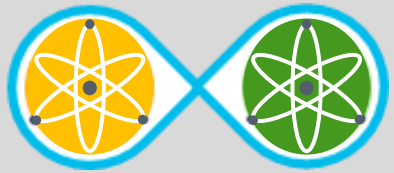
What is Cisco doing in Quantum?

Key Engineering Challenges in Quantum Computing & Networking

Developing Larger Quantum Computers
Current Record: 1121 qubits

Achieving Longer Quantum Coherence
Current Record: 784 ms

Requiring Fewer Qubits for Error Correction
Current Record: 7.5 PQ/LQ

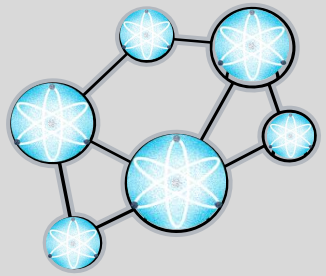


Extending Entanglement
Current Record: 248 km

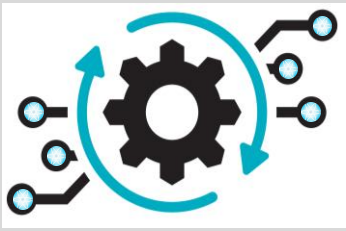
Raising Operating Temperatures

Achieving Longer Quantum Memory

Improving Quantum Transmission Fidelity



Planning & Modelling Quantum Networks



Developing Quantum Network Protocols

Lowering Costs

Cisco's Primary areas of focus

© 2025 Cisco and/or its affiliates. All rights reserved.

Steps to Building a Quantum Internet

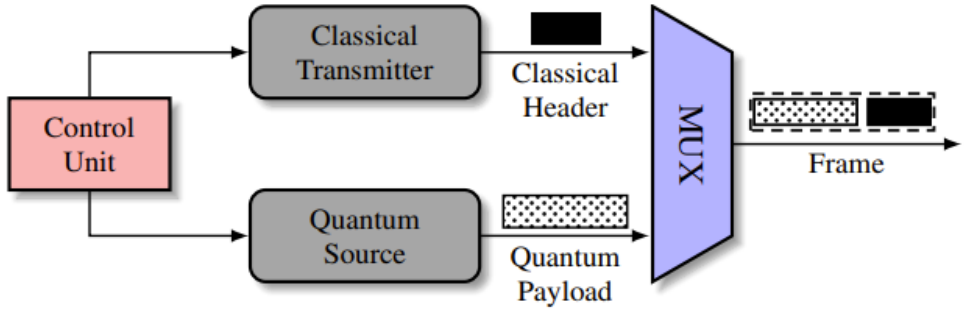
1) Research & Mathematical Modelling
2) Quantum Simulation & Emulation
3) Hardware & Software Development

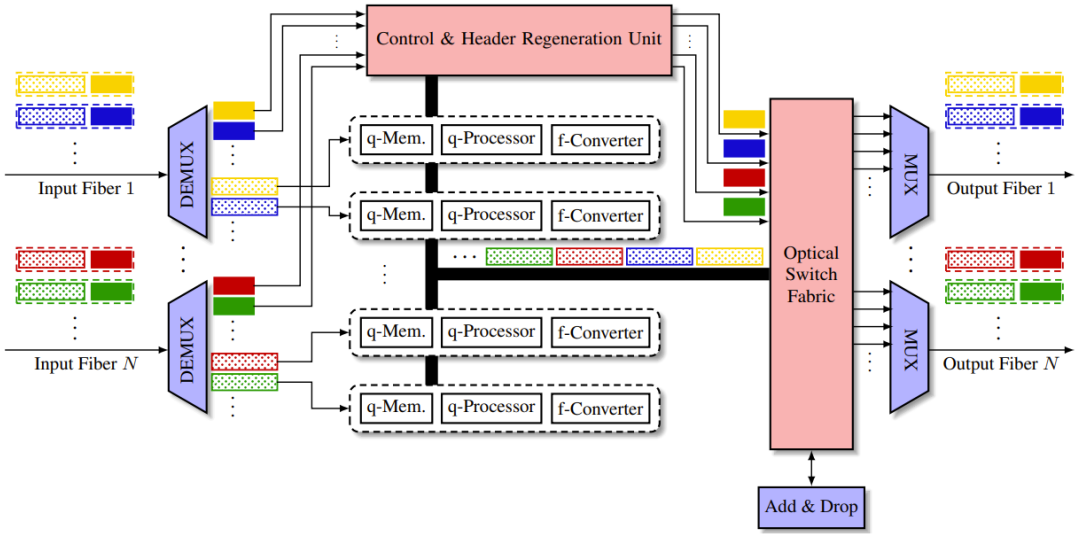
© 2025 Cisco and/or its affiliates. All rights reserved.

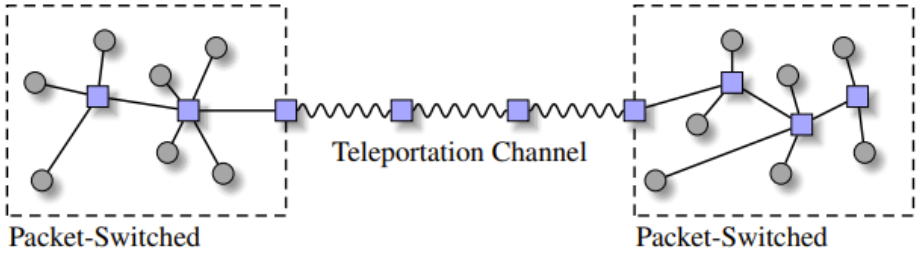
Modelling a Unified Classical & Quantum Internet

"We are now with Quantum Internet where we were with the classical Internet in the 1960s"

The Cisco Research team has published several research papers on how can we design a network that can serve thousands and eventually millions of end nodes







https://outshift.cisco.com/blog/making-a-quantum-ready-internet
https://arxiv.org/abs/2205.07507

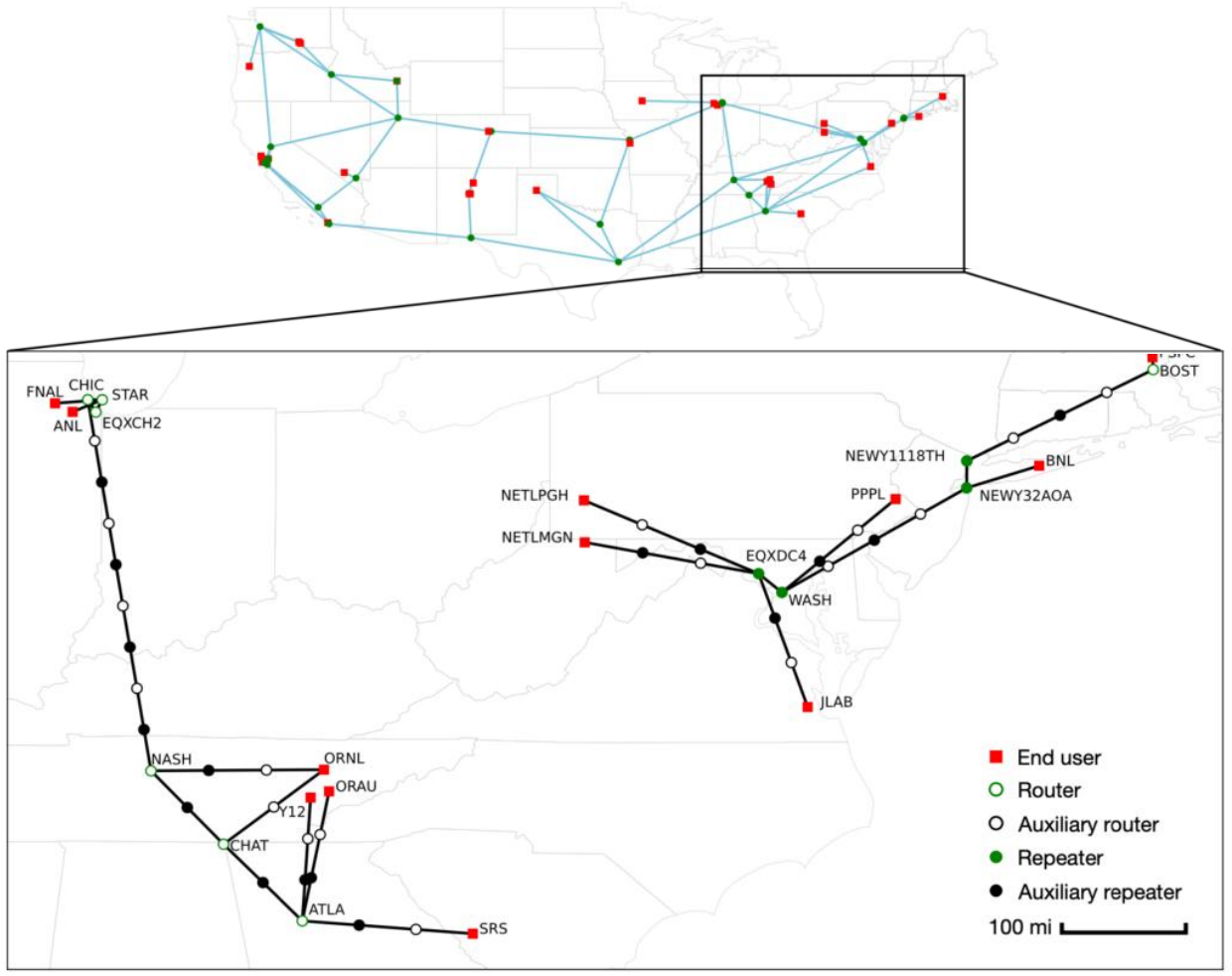
© 2025 Cisco and/or its affiliates. All rights reserved.

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

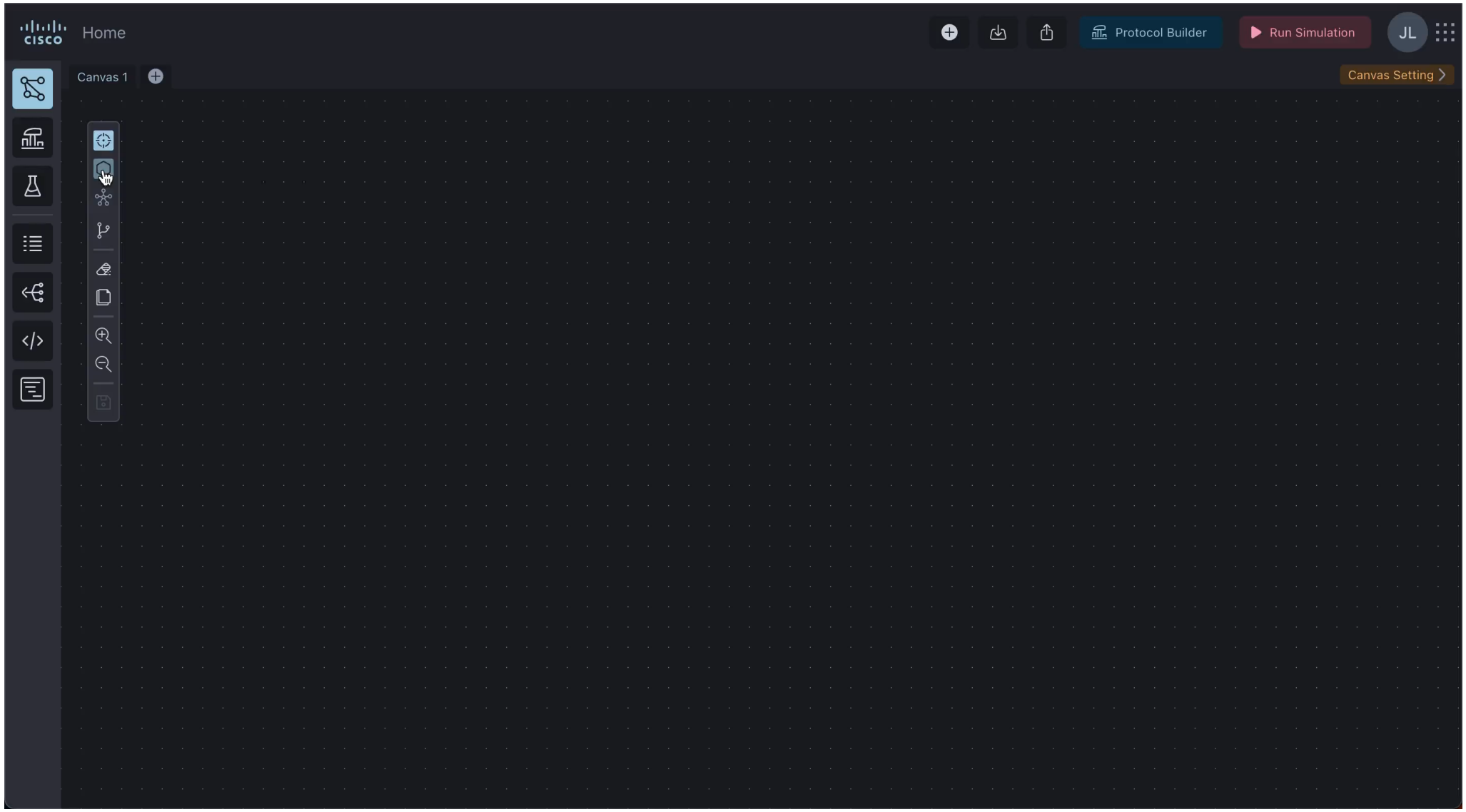
- Specifically, as an Integer Linear Programming (ILP) problem



https://outshift.cisco.com/blog/first-steps-to-quantum-network-planning
https://arxiv.org/abs/2308.16264

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Network Digital Twin



Simulation

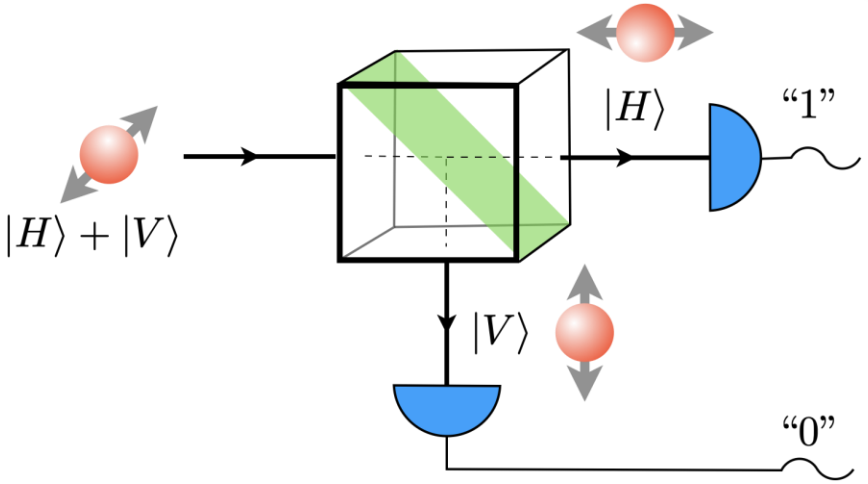
https://research.cisco.com/research-projects/qnet-lab

© 2025 Cisco and/or its affiliates. All rights reserved.

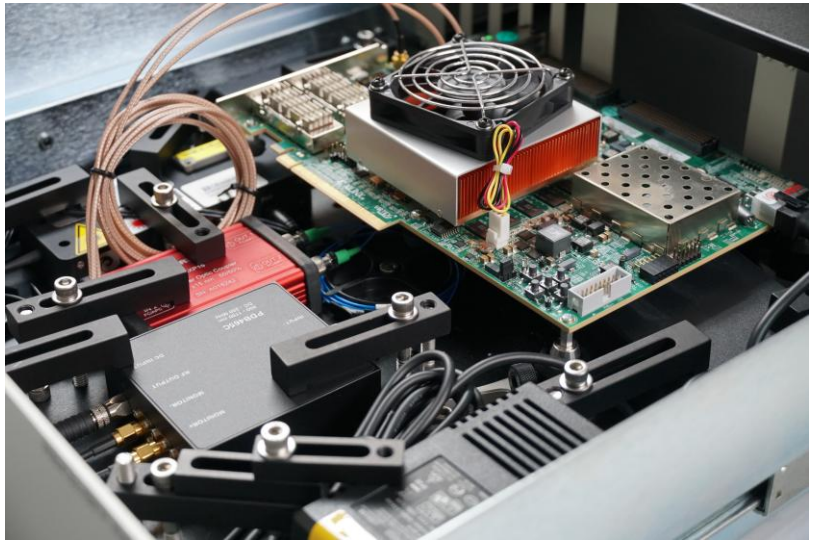
Quantum Random Number Generator (QRNG)

Hardware Development

- Random Number Generation (RNG) is an essential function for cryptography
- Current classical random number generators are not truly random, but rather **pseudo-random**
  - **As these perform mathematical functions on an initial seed value**
- Quantum states are **mathematically guaranteed** be truly random
- Cisco has developed a hardware Quantum Random Number Generator (QRNG)
  - **This hardware is also accessible via the Quantum Network Design Kit (QNDK)**



Random bit string 00111010101111010100110101010110...



© 2025 Cisco and/or its affiliates. All rights reserved.

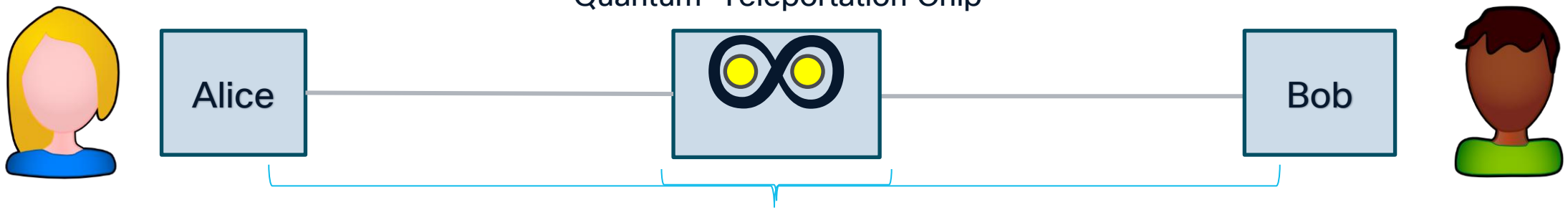
cisco

Quantum Network Entanglement Chip

Hardware Development

Enabling Quantum Teleportation between Quantum Endpoints

Quantum Teleportation Chip



Key Features:

- Miniaturized Photonic Integrated Chip (PIC) that **operates at room temperature**
- **Integrates with existing fiber optic infrastructure** by operating at standard telecom wavelengths
- **Delivers high-performance** by producing 1 million high-fidelity entanglement pairs per output channel, with a rate of up to 200 million entanglement pairs per second
- Consumes less than 1mW of power for **energy efficiency**

https://blogs.cisco.com/news/quantum-networking-how-cisco-is-accelerating-practical-quantum-computing

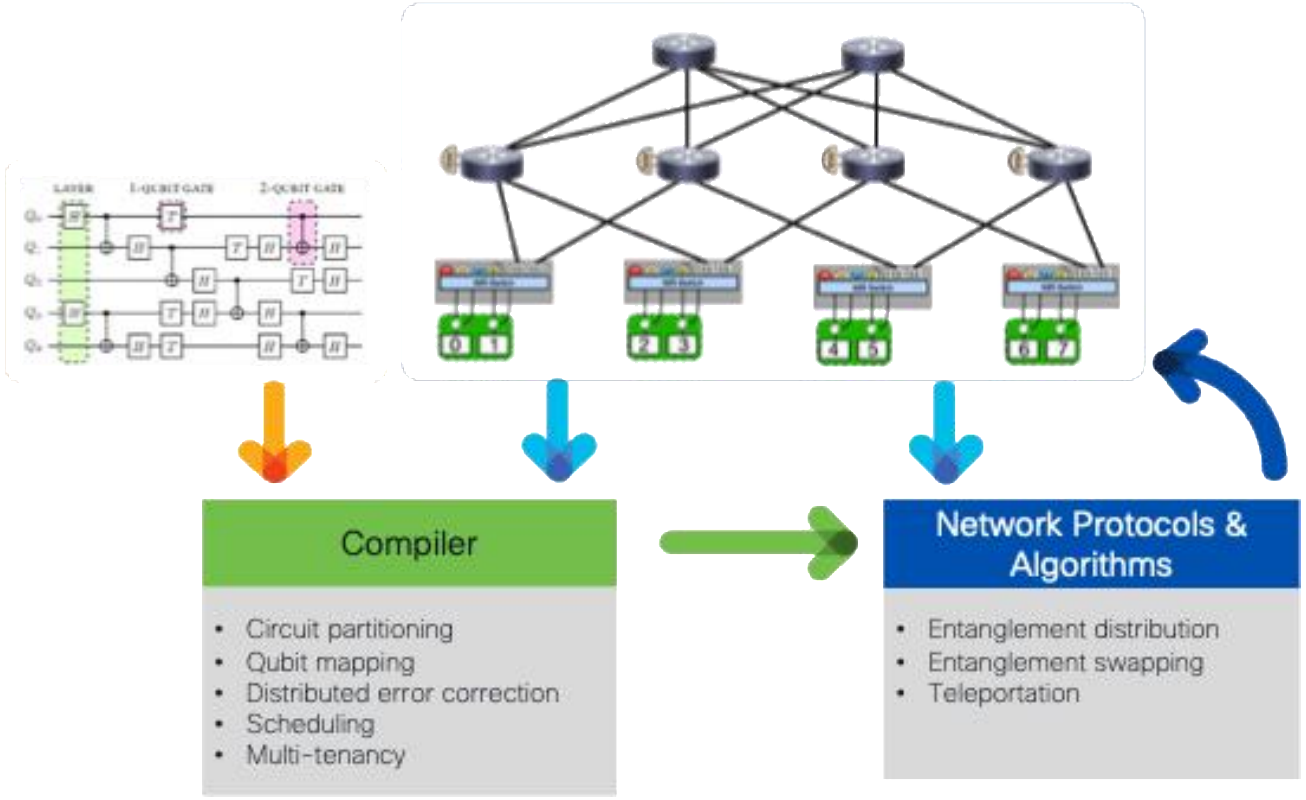
© 2025 Cisco and/or its affiliates. All rights reserved.

Network-Aware Quantum-Compiler

Developing the World's First Quantum Compiler

Hardware/Software Co-Design

- We believe the most practical path to scalable quantum computing lies in distributed quantum computing, housed within a Quantum Data Center (QDC)
- Building a QDC requires a fundamental shift in how we design, manage, and operate quantum systems
- A key component of this vision is a distributed quantum computing compiler that explicitly understands and leverages network connectivity and inter-processor communication
- This industry-first compiler supports:
  - distributed quantum error correction
  - network-aware circuit partitioning
  - qubit mapping
  - advanced scheduling
  - multi-tenancy for QDCs

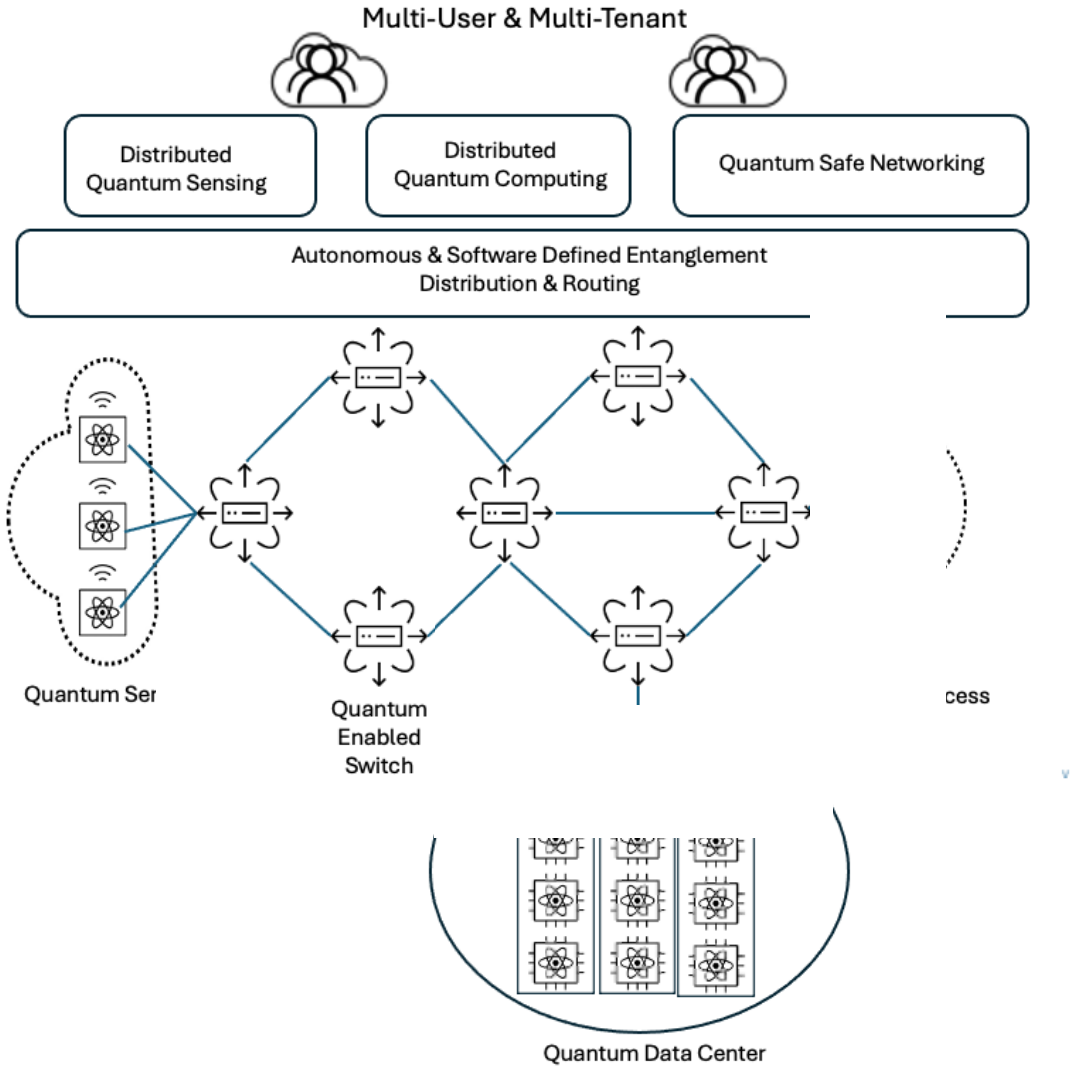


https://outshift.cisco.com/blog/network-aware-quantum-compiler

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

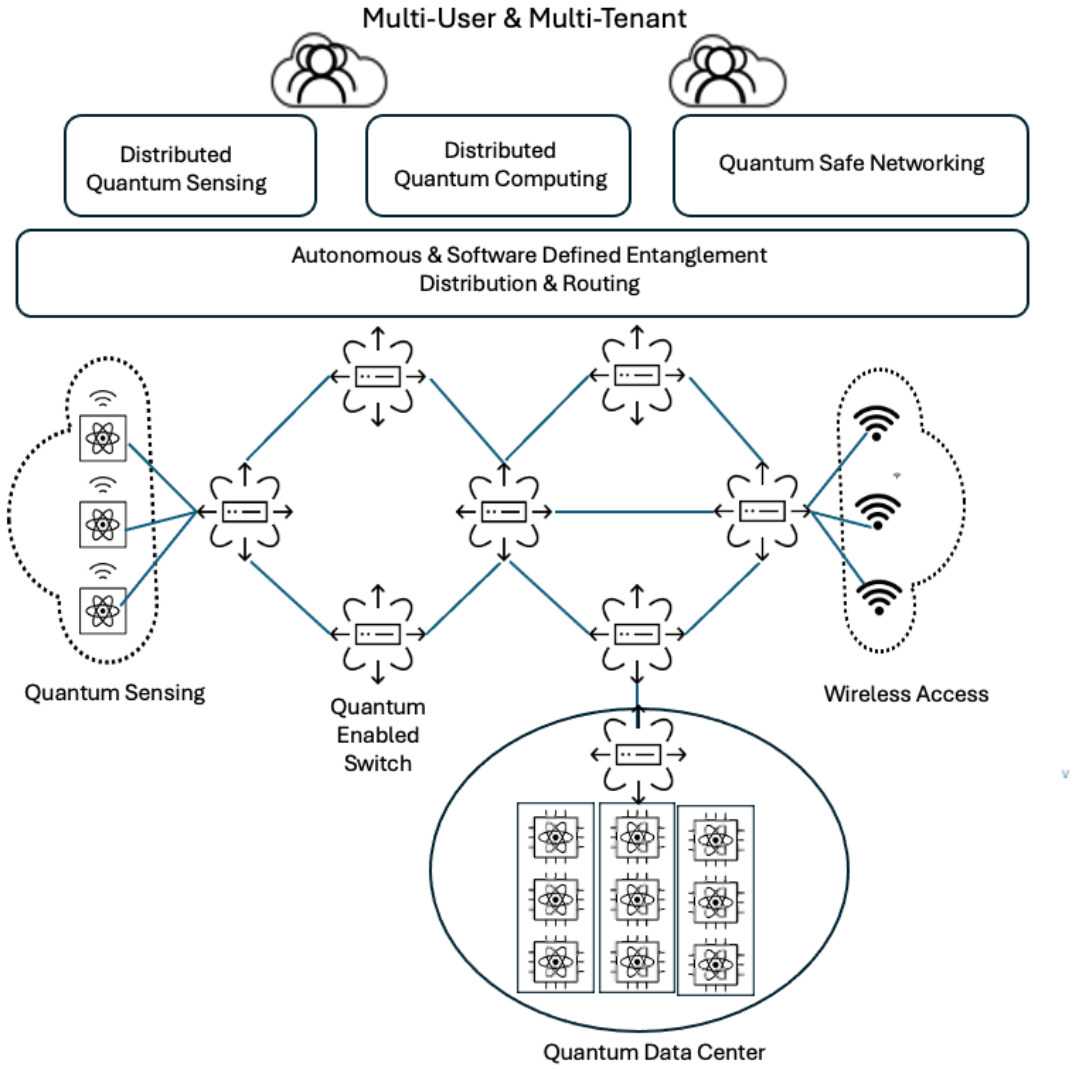
What are We Working on Now?



https://research.cisco.com/quantum-research

© 2025 Cisco and/or its affiliates. All rights reserved.

What are We Working on Now?



https://research.cisco.com/quantum-research

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Summary

Post-Session Quiz

1) Why build quantum networks?
2) What are some of the special properties of quantum bits (qubits)?
3) What makes a quantum computer so fast?
4) Does quantum compute threaten RSA and AES?
5) What is Y2Q? And when do most experts expect it?
6) What are three requirements for quantum safety?
7) When do Australian networks need to be quantum safe?
8) Can you transmit information faster than light with quantum teleporting?
9) Will quantum networks replace classical networks?
10) What is Cisco researching and developing in quantum?

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Post Session Quiz / Summary

1) Why build quantum networks?

Why Build 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)***

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build Quantum Networks?

Distributed Quantum Computing

Interconnecting quantum computers to collectively empower:

- Simulations:
  - Chemical/Molecular Engineering
  - Weather forecasting
  - Financial Modelling
  - Etc.
- Optimization Logistics
- AI/ML
- Cryptography (i.e. Decryption)

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build Quantum Networks?

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build Quantum Networks?

Network Clock Synchronization

A world-wide set of high-precision clocks connected by quantum networks could achieve ultra precise clock signals

Current accuracy: 10 ns to 500 ps

Quantum accuracy: ≤1ps

https://www.gps.gov/systems/gps/performance/accuracy/
https://ieeexplore.ieee.org/document/8856607

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build Quantum Networks?

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. Deep Space Telescope Array

Classical precision: $\pm 1/\sqrt{N}$

Quantum precision: $\pm 1/N$

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Build Quantum Networks?

Quantum Money

The main security requirement of money is unforgeability

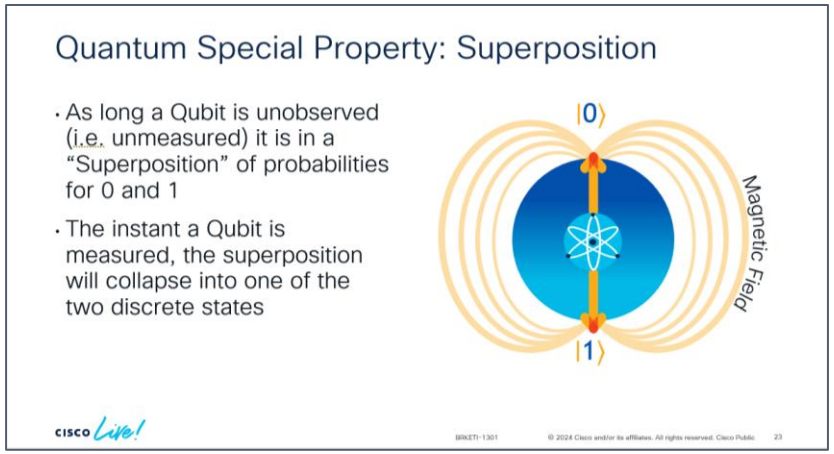
A quantum money scheme aims to fulfill by this requirement by exploiting the no-cloning property of unknown quantum states

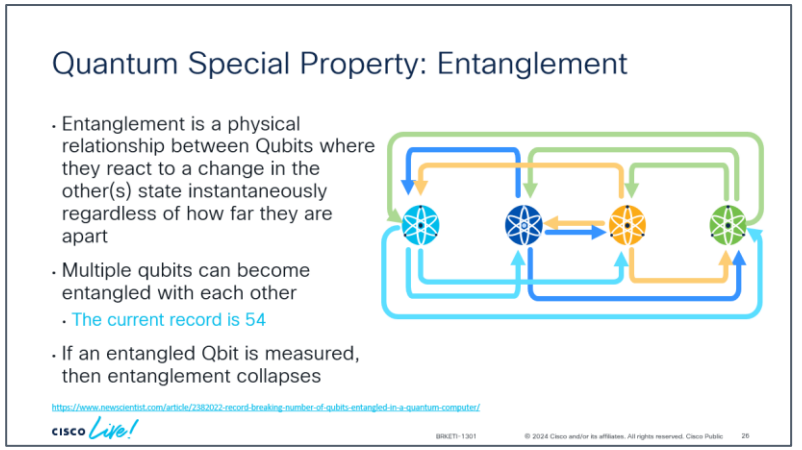
© 2025 Cisco and/or its affiliates. All rights reserved.

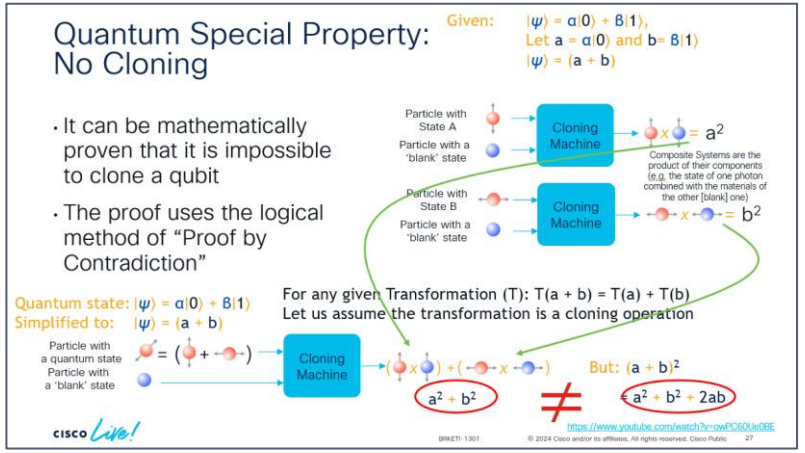
© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

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





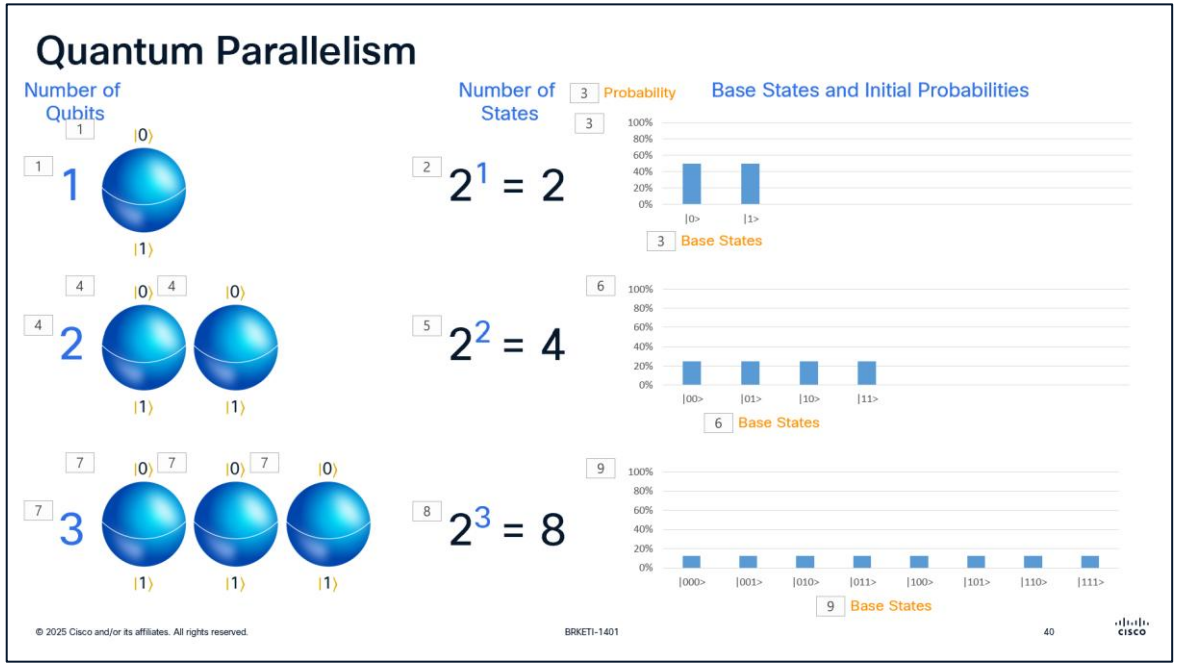


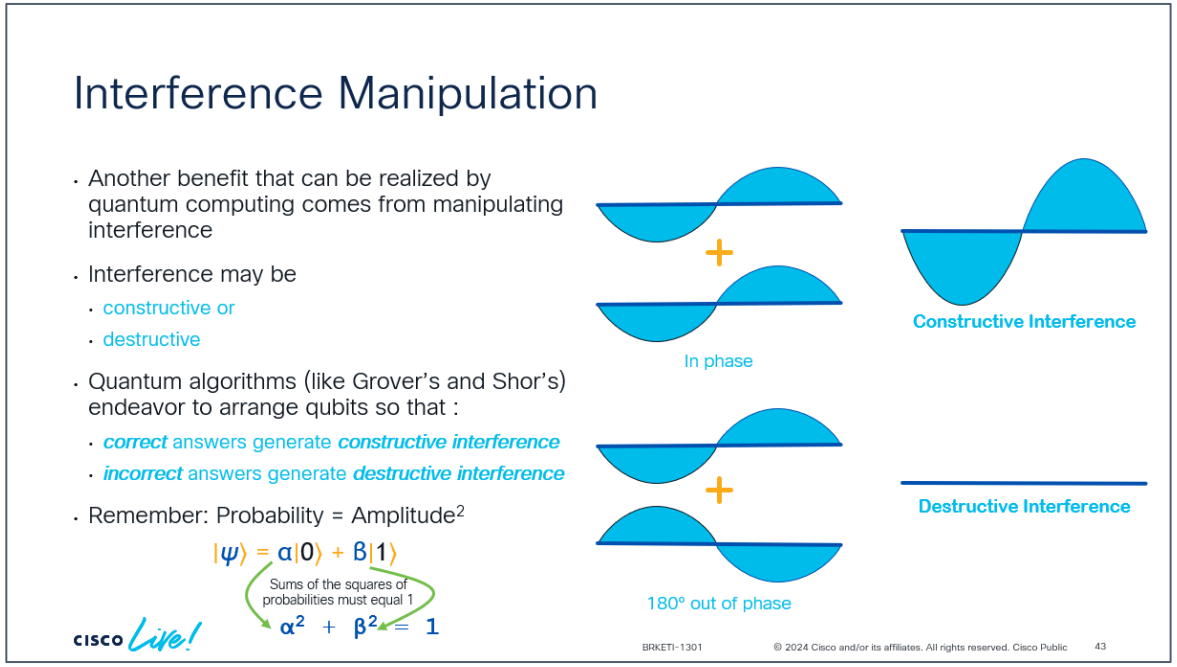
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Post Session Quiz / Summary

3) What makes a quantum computer so fast?





Post Session Quiz / Summary

4) Does quantum compute threaten RSA and AES?

The Implications of Quantum Computing on Cybersecurity

But What About RSA? How many Qubits are required to Break RSA?

Experts estimate that:

RSA-2048 requires a quantum computer with 1,600 *logically-corrected* qubits to be broken

And that these could be expressed via 897,864 *physical* qubits

Key Takeaway: RSA is very much under threat by quantum computing!!!

https://arxiv.org/pdf/2505.15917

- Shor's algorithm exhibits ***exponential*** quantum speed-up, as compared to classical computing systems, and
- Quantum computers are *increasing* in size, while
- Quantum Error Correction circuits are *decreasing* in size

© 2025 Cisco and/or its affiliates. All rights reserved.

Grover's Achilles Heel: Quadratic Speed-Up

- Grover's algorithm only offers quadratic speed up, and does NOT parallelize well

https://eprint.iacr.org/2017/811.pd

- While it is acknowledged that if an attacker had a quantum computer that can issue circa 2^{128} successive evaluations then they could find the key with high probability
- However, in this attack model, even a 160-bit key (which would require circa 2^{80} successive evaluations), would be secure for all practical purposes
  - For example, even if we assume that the quantum computer could evaluate the encryption function in the absurdly fast time of 1 picosecond, the total of 2^{80} successive evaluations would require over 30,000 years to complete
- Any realistic security policy is not concerned with an attack that takes that long to perform

Key Takeaway:
As such, AES-256 is considered quantum resistant, *provided* the key exchange is also secure (i.e. not via PKI)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

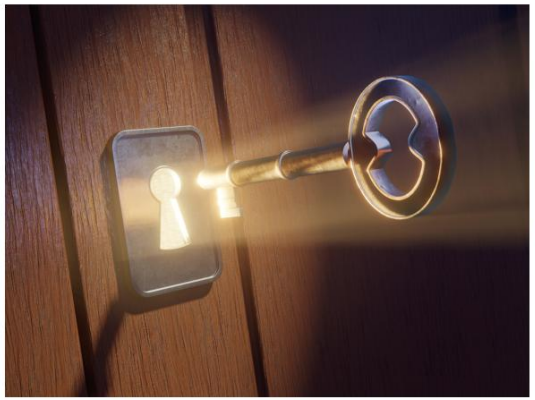
© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

5) 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 are **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)



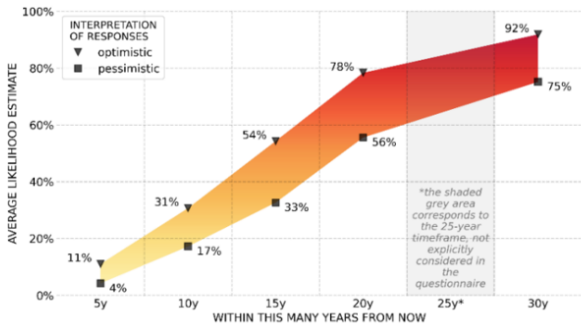
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Many Y2Q?

1 1 2 2 3 3

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

2



https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum/
https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

6) What are three key requirements to become quantum-safe?

- Management Plane
- Control Plane
- Data Plane

- Secure Firmware
- Secure Software
- Secure Runtime
- Secure Identity

The capabilities needed to replace and adapt to continually evolving cryptographic algorithms while preserving security and ongoing operations

© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

7) When do Australian networks need to be quantum-safe?

How to Become Quantum-Safe

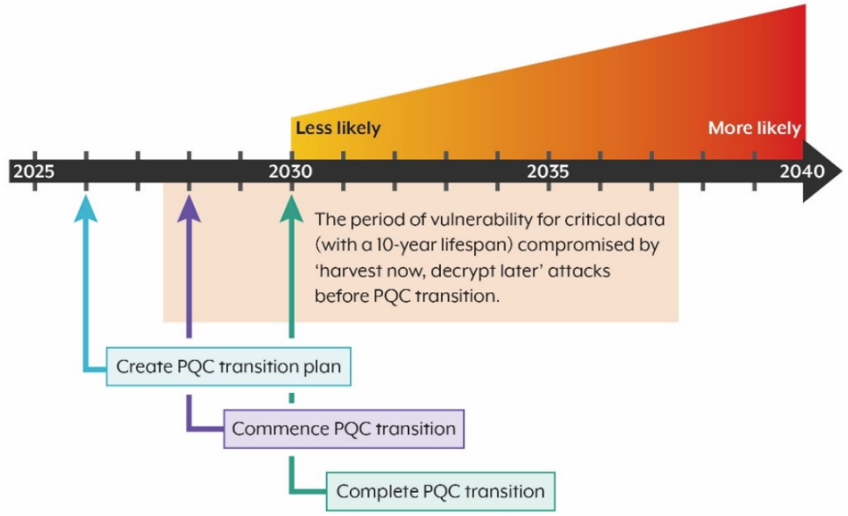
The Urgency of the Threat

In direct response to the quantum threat, governments are mandating application and infrastructure upgrades within the next few years

For example, this Australian Signal's Directorate has issued the following recommendations and timelines:

- By the end of 2026: Organizations are expected to have a refined plan for their PQC transition
- By the end of 2028: Organizations should commence their transition to PQC
- By the end of 2030: Organizations are advised to have completed their PQC transition

The private sector is moving even faster



https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

© 2025 Cisco and/or its affiliates. All rights reserved.

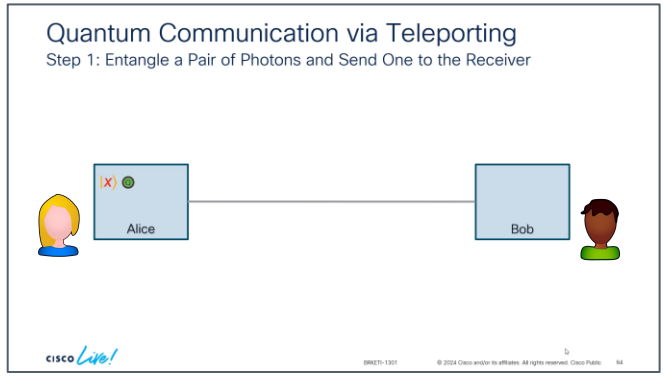
49

Post Session Quiz / Summary

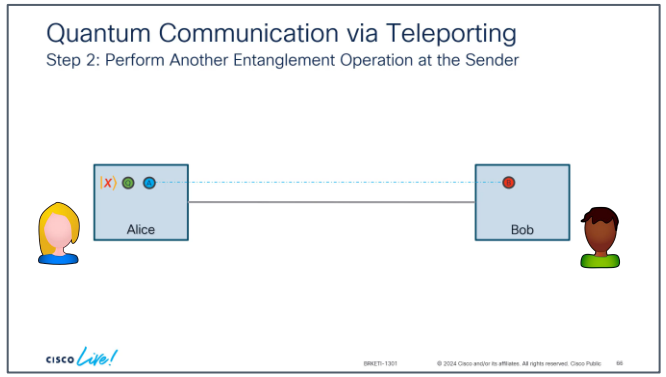
8) Can you transmit information faster than light with quantum teleporting?

Key Takeaway:

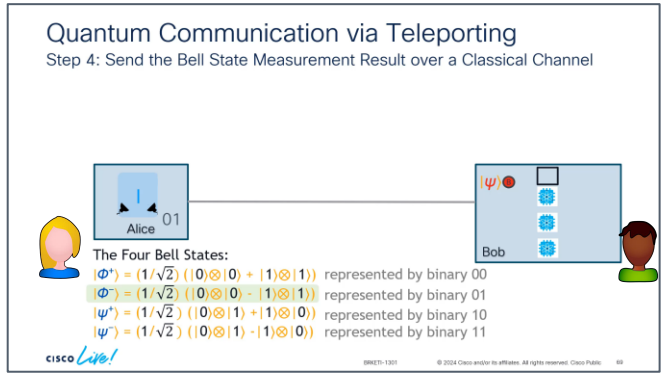
Quantum teleportation does **NOT** enable faster than light communication



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

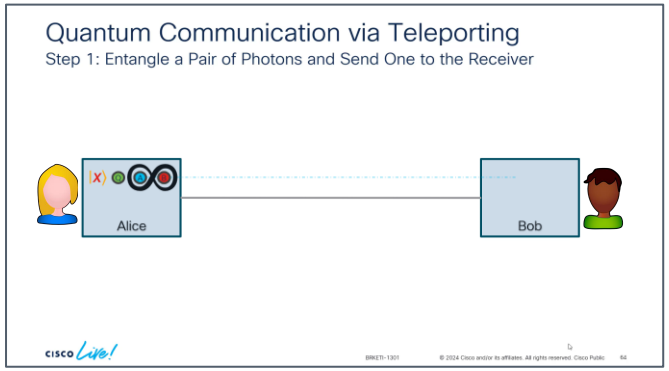


(At least) Two more bits of data are sent over a classic channel

© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

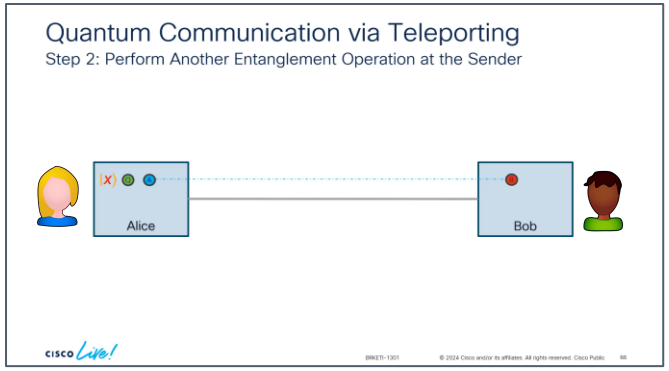
9) Will quantum networks replace classical networks?



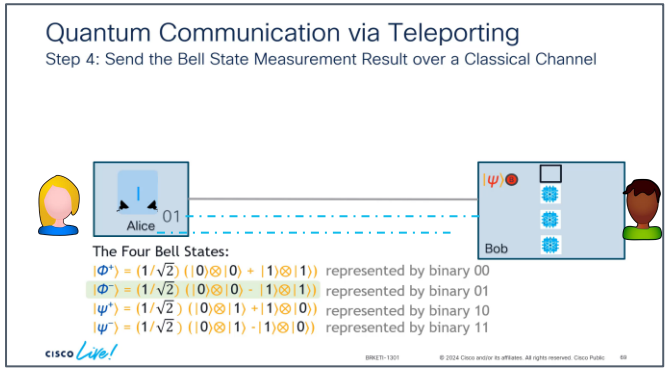
Equivalent to sending (at least) **one bit over a classical channel**

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**



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

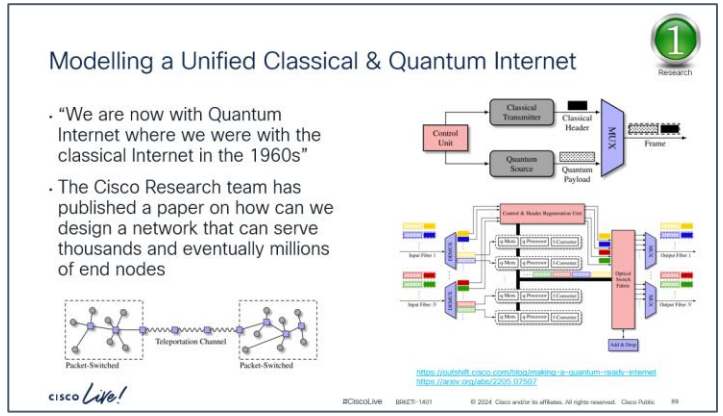


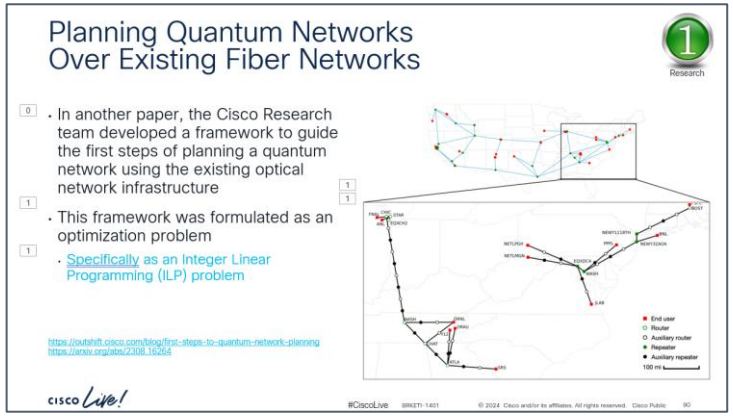
(At least) **Two more bits** of data **are sent over a classic channel**

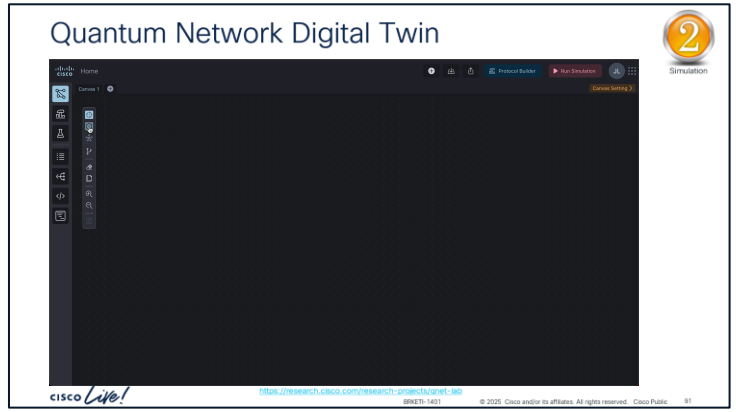
© 2025 Cisco and/or its affiliates. All rights reserved.

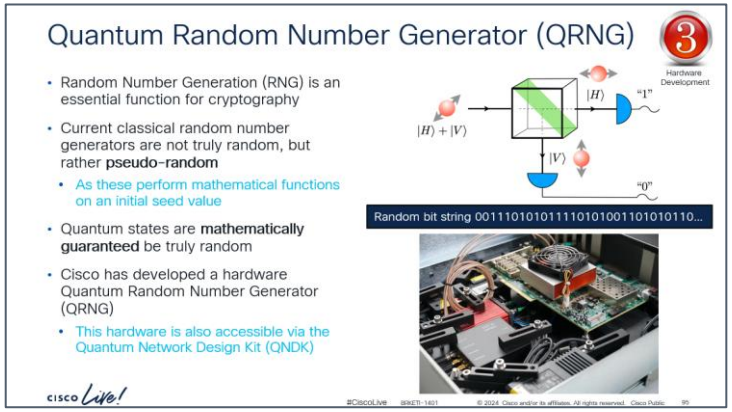
Post Session Quiz / Summary

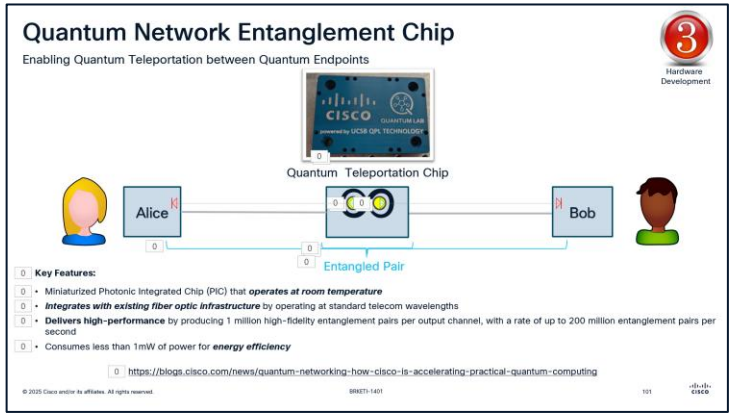
10) What is Cisco researching and developing in quantum?

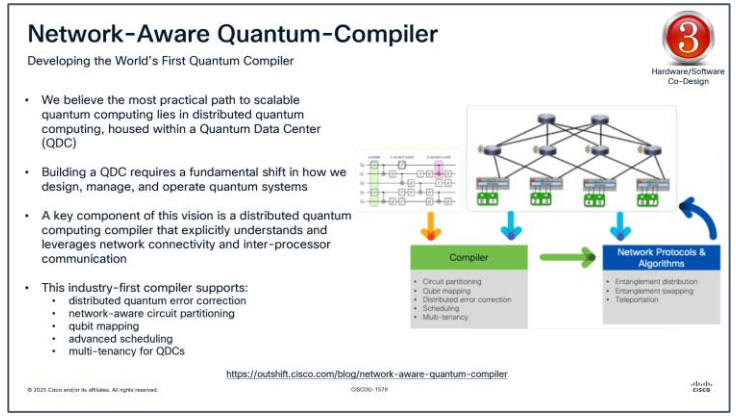








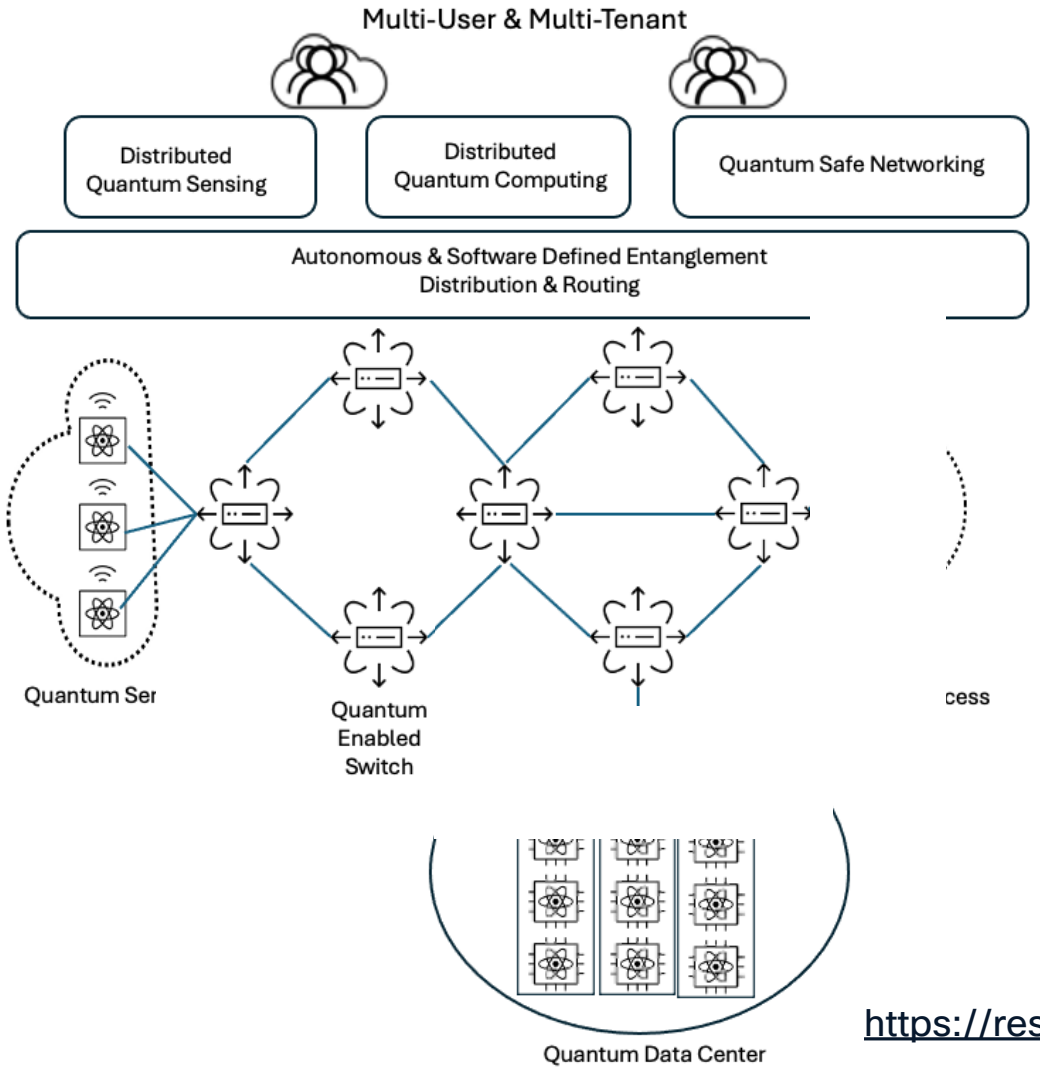




© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

10) What is Cisco researching and developing in quantum?

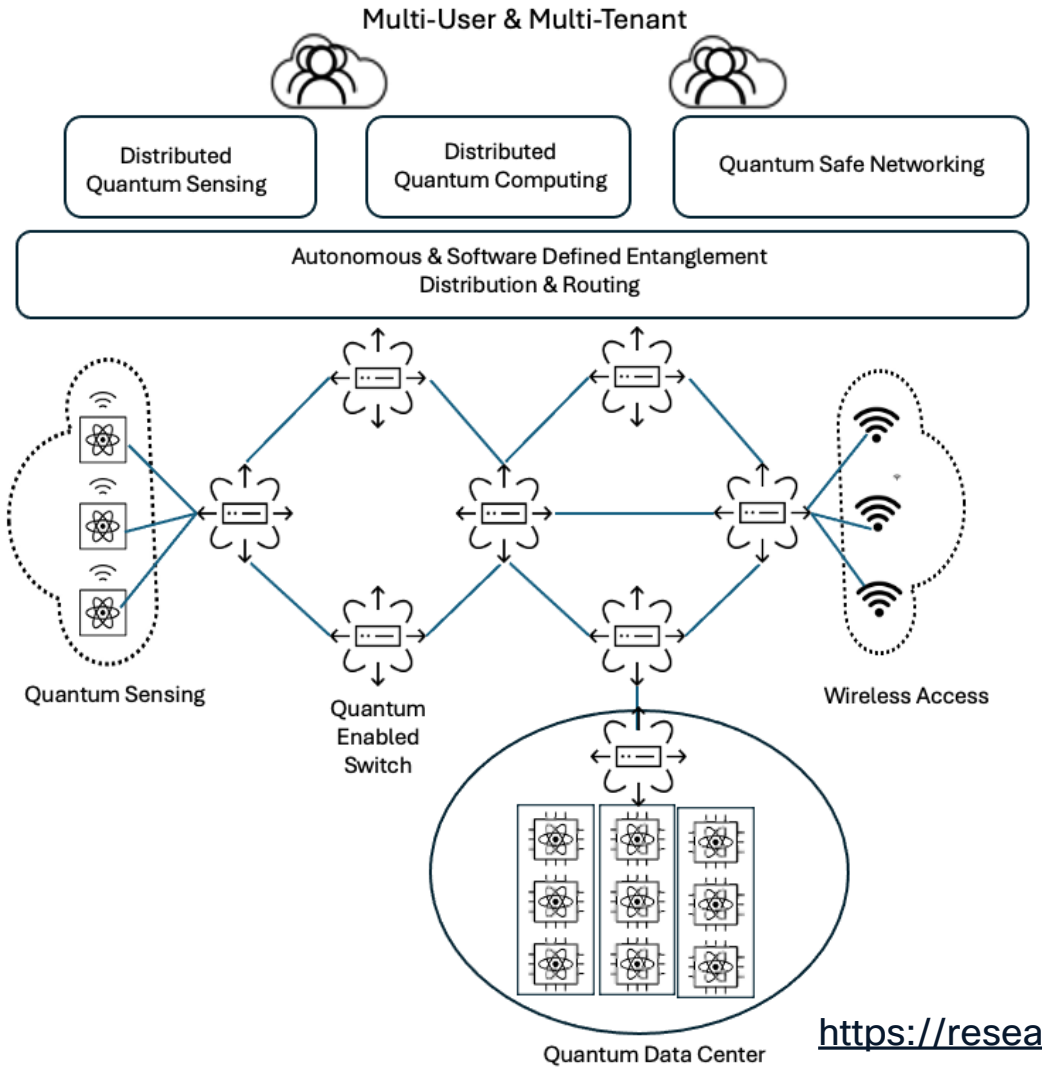


https://research.cisco.com/quantum-research

© 2025 Cisco and/or its affiliates. All rights reserved.

Post Session Quiz / Summary

10) What is Cisco researching and developing in quantum?



https://research.cisco.com/quantum-research

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

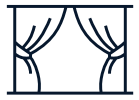
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: szigeti@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !

CISCO