

Quantum Computing for Cybersecurity and Artificial Intelligence

Mohammad **Saidur** Rahman

Assistant Professor

Dept. of Computer Science

University of Texas at El Paso

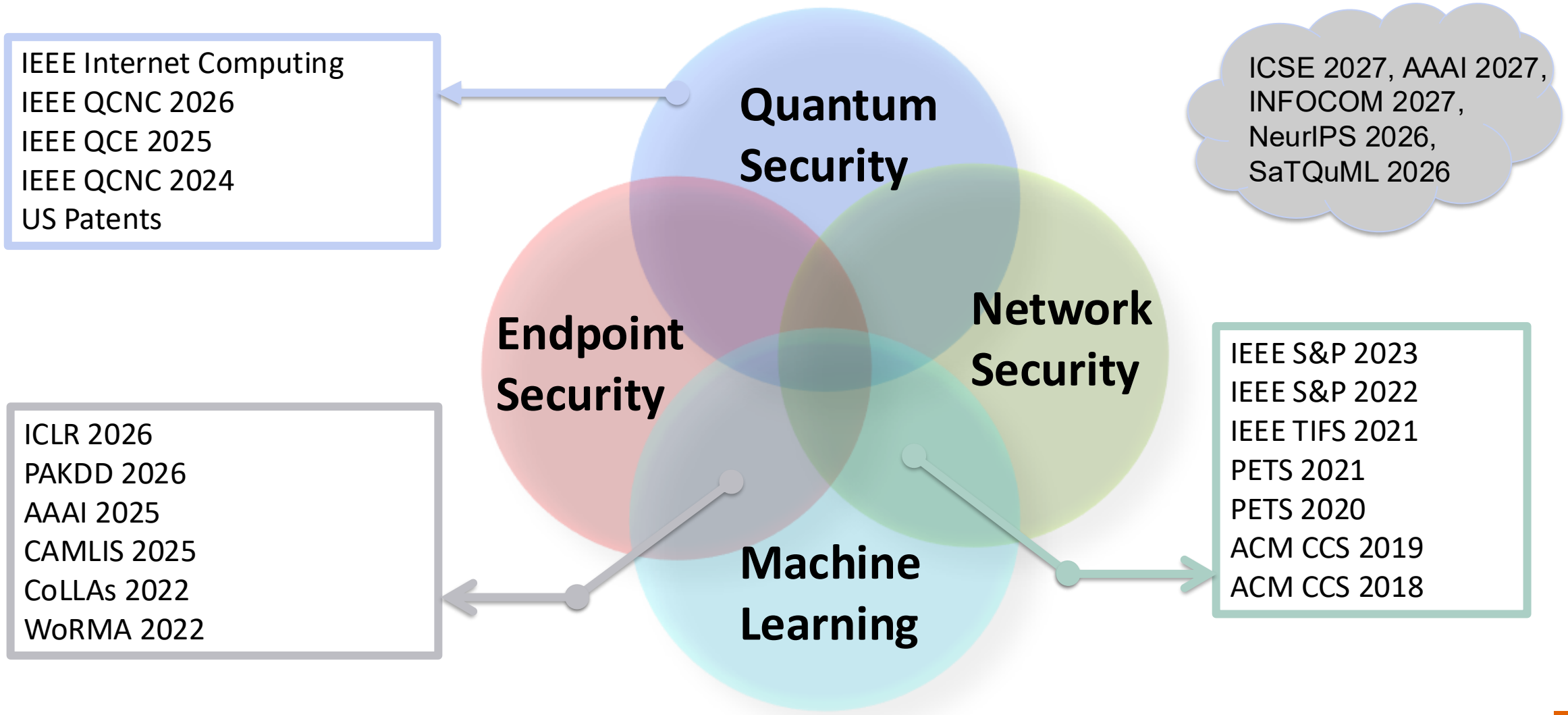
https://www.rahmanmsaidur.com

Great Minds in STEM (GMiS) 2026

Albuquerque, New Mexico | September 17, 2026

My Research

Intelligent and Quantum Secure Advanced Cyber Defense Research (IQSeC) Lab



What are we going to talk about?

- Quantum Computing (QC) / Information Science
  - Qubit
  - Superposition
  - Entanglement
  - Quantum Circuits
- Toy RSA (QC to break RSA)
- Quantum Machine Learning
  - Variational Quantum Circuit

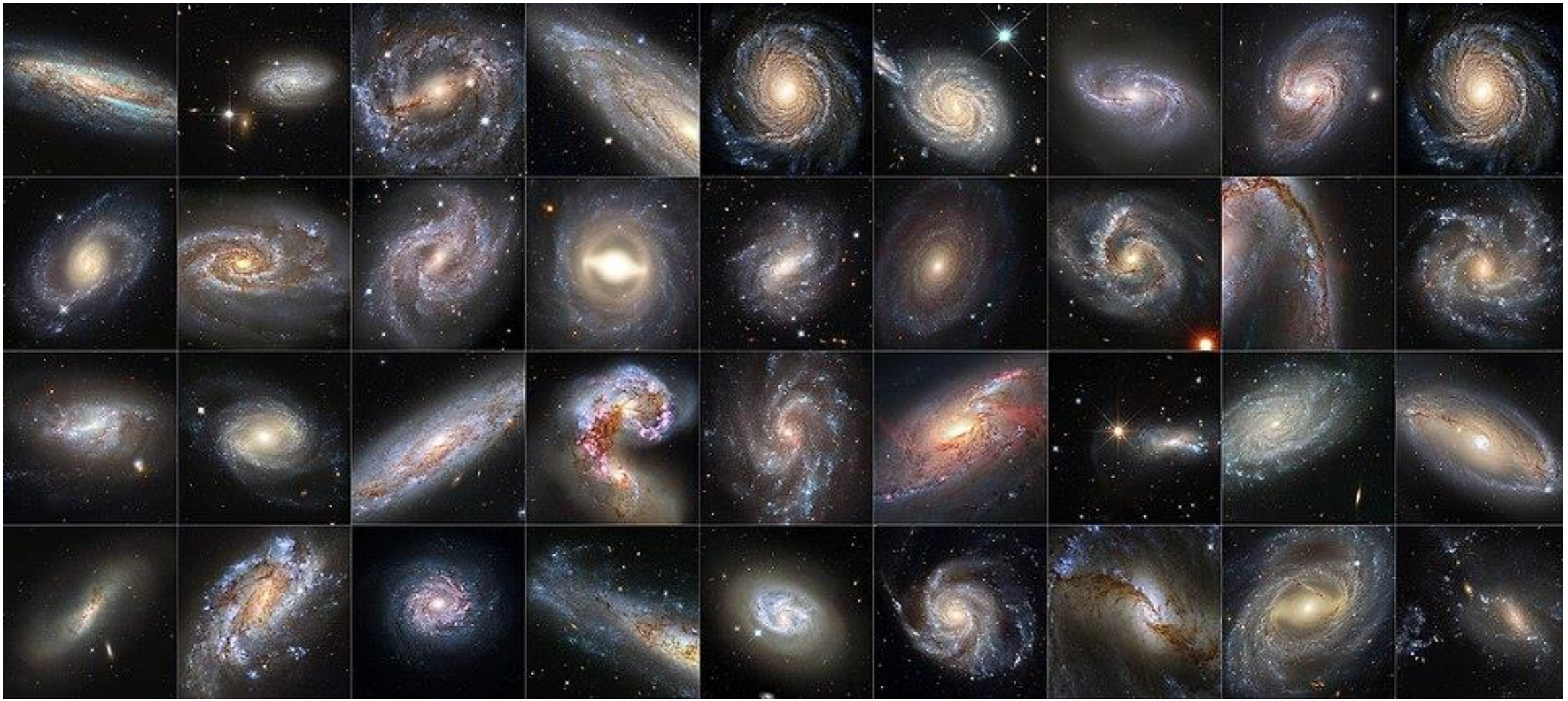


The Pale Blue Dot is a photograph of Earth taken Feb. 14, 1990, by NASA’s Voyager 1 at a distance of 3.7 billion miles (6 billion kilometers) from the Sun.

The image inspired the title of scientist Carl Sagan's book, "Pale Blue Dot: A Vision of the Human Future in Space," in which he wrote:

"Look again at that dot. That's here. That's home. That's us."

Galaxies : 2 trillion



1. THE BIG PICTURE – FROM UNIVERSE TO APPLE



Universe

↓



Milky Way Galaxy

↓



Solar System

↓



Earth

↓



Ecosystem (forest)

↓



Apple Tree (organism)

↓

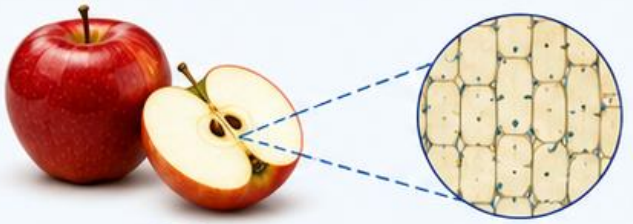


Apple (the fruit)

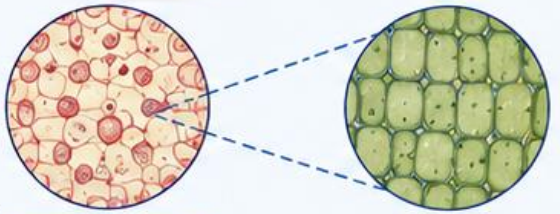


2. ZOOMING IN – FROM APPLE TO ATOMS

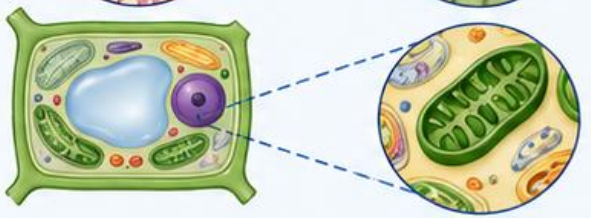
Apple



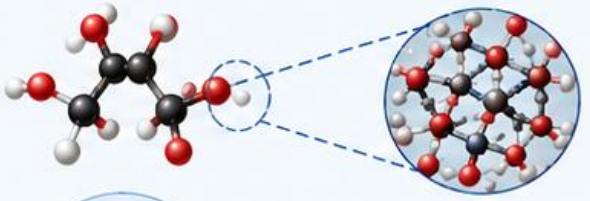
Plant tissues (flesh)



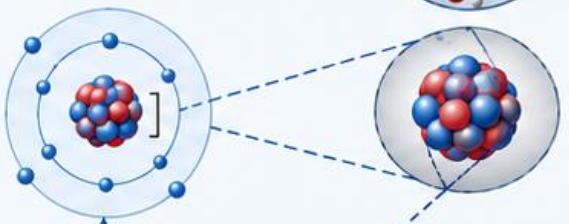
Plant cell



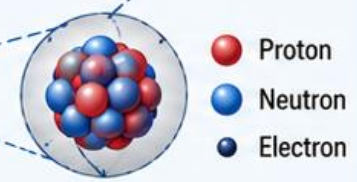
Molecules (e.g., sugar)



Atom (e.g., carbon)

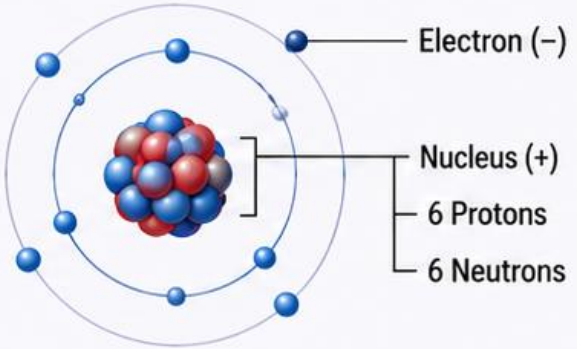


Subatomic particles

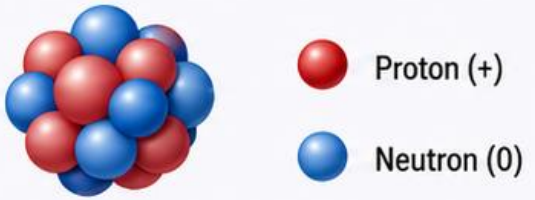


3. THE SMALLEST BUILDING BLOCKS

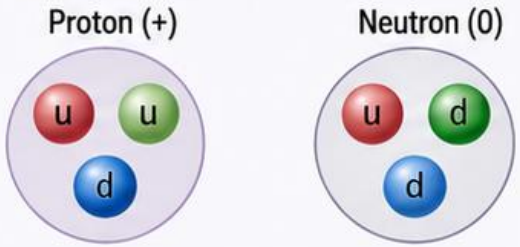
Atom (e.g., Carbon)



Nucleus



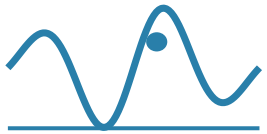
Proton and Neutron (Quarks)



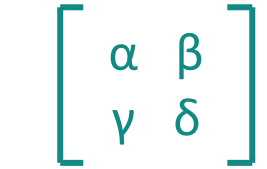
u = up quark d = down quark

∿∿ = gluons (force particles) holding quarks together

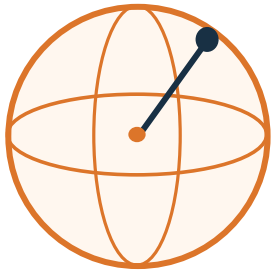
Quantum is interdisciplinary



Physics

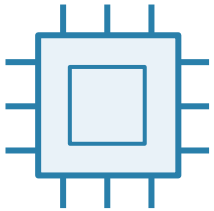


Mathematics

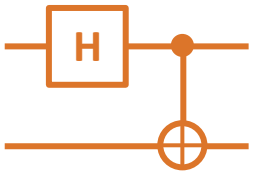


Quantum

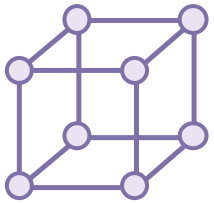
Information Science



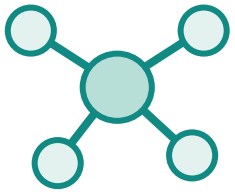
Electrical Engineering



Computer Science

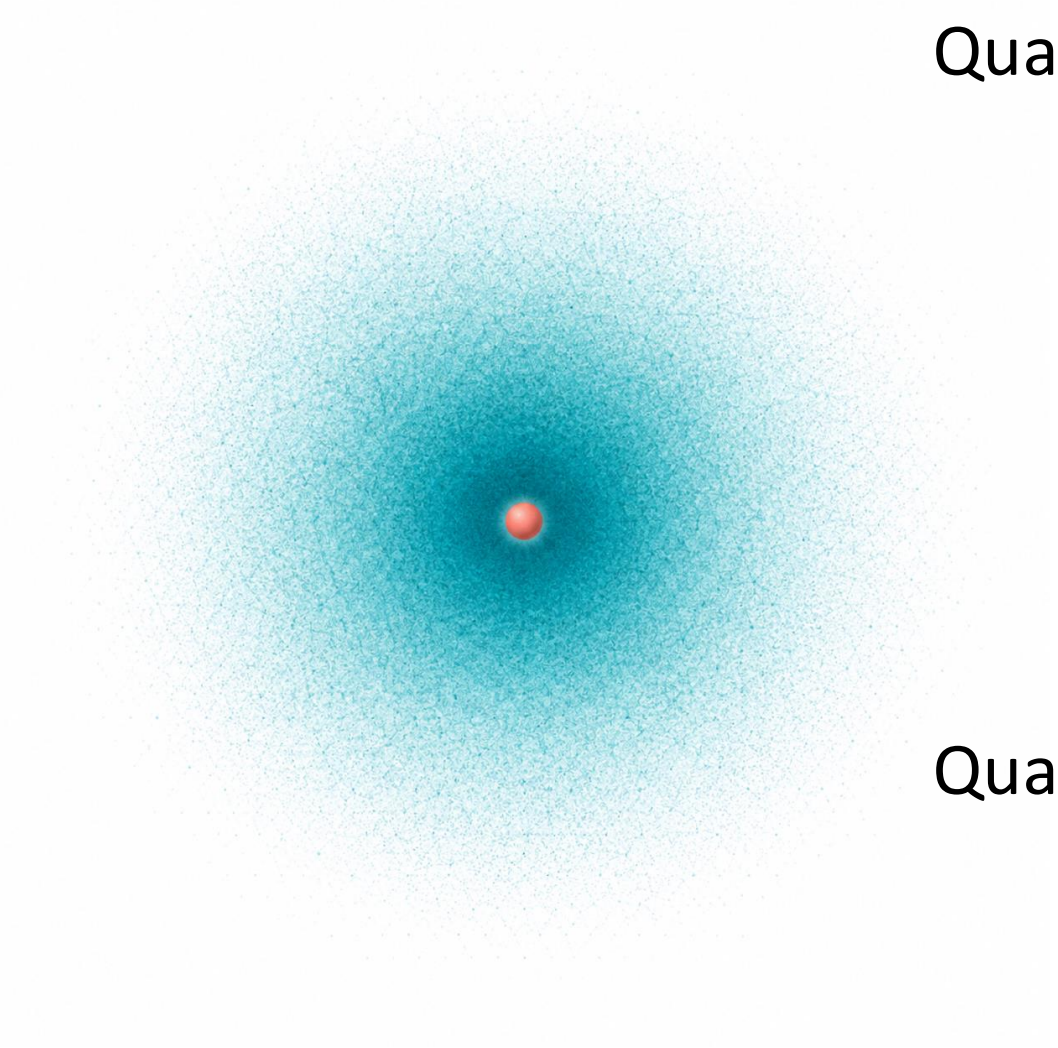


Materials Science



Chemistry

What does “*Quantum*” mean?



Quantum Mechanics

- Describes how objects behave at microscopic scales
- Its effects can differ from everyday observations
- An atom as an example

Quantum Computing

- *Uses quantum phenomena to perform computation*

Quantum Mechanics

- Rules of Probability in Nature
  - Complex numbers
    - Amplitude

$$z = a + bi$$

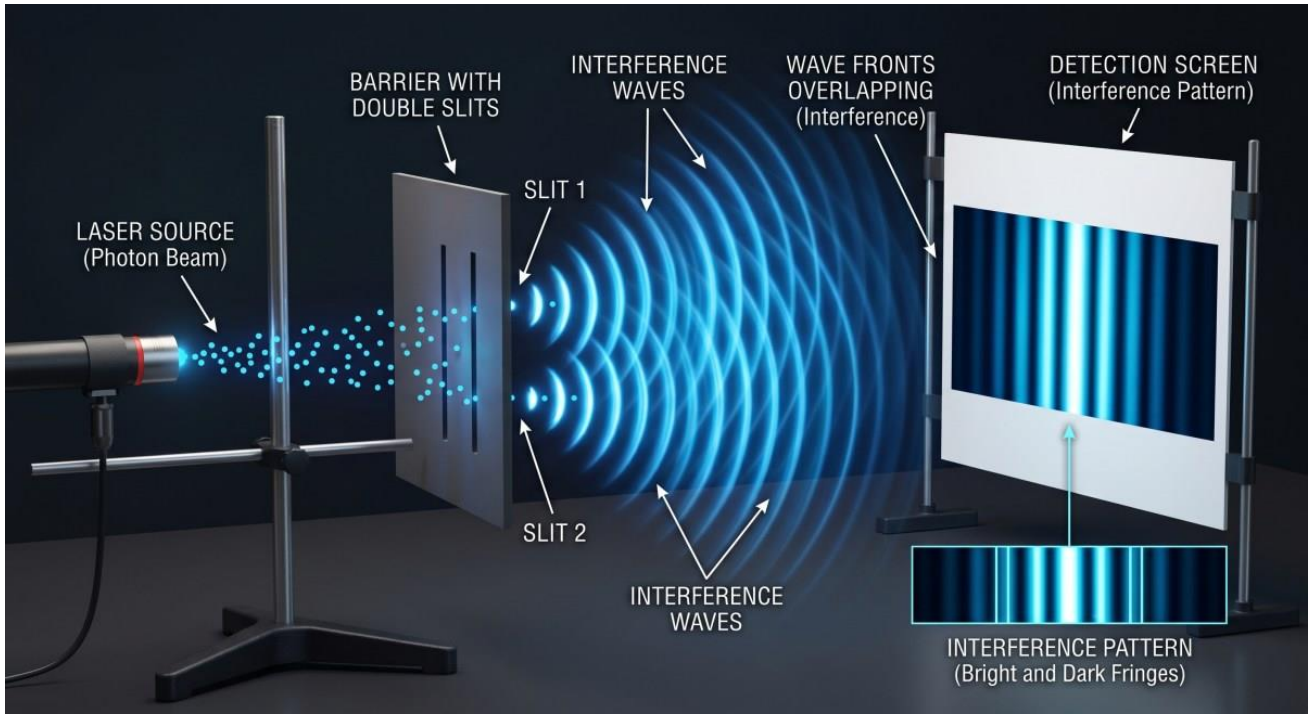
Here, a and b are real numbers;

i is imaginary number;

$$i = \sqrt{-1};\ i^2 = -1$$

Double slit experiment

"Probability theory with minus signs"



Interference: amplitudes combine

Aligned contributions reinforce



½ + ½ = 1

Opposite contributions cancel



0

½ − ½ = 0

Arrows show signed amplitudes for the same outcome.

Coherent alternatives can interfere. Negative amplitude ≠ negative probability.

Interference changes what we observe

OUTCOME 0

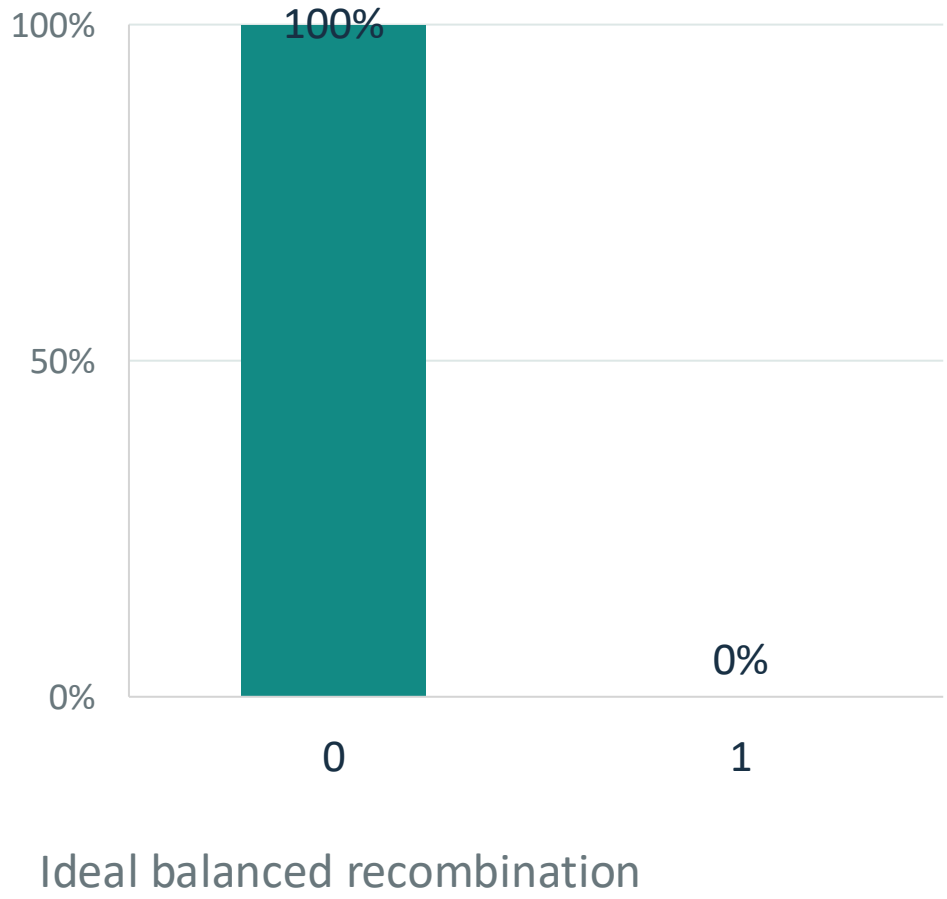
$\frac{1}{2} + \frac{1}{2} = 1$

Probability: $|1|^2 = 100\%$

OUTCOME 1

$\frac{1}{2} - \frac{1}{2} = 0$

Probability: $|0|^2 = 0\%$

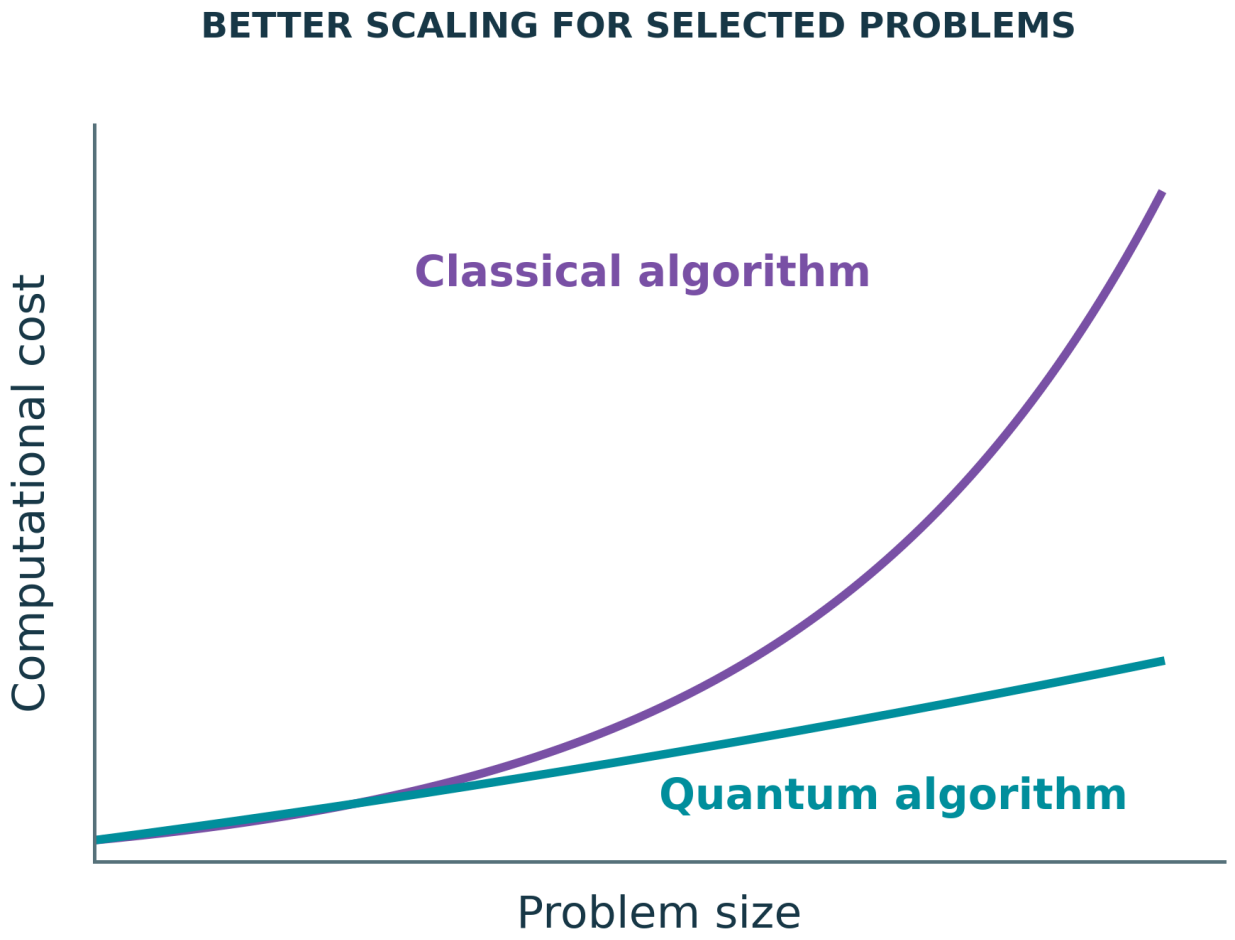


Ideal balanced recombination

Add amplitudes first. Then square the magnitude to get probability.

Why do we need “*Quantum*”?

Some problems are too hard for a classical computer to solve.



Conceptual illustration; curves are not measured data.

From bit to qubit

CLASSICAL BIT

0 or **1**

One stored value

Smallest unit of
ordinary digital information



move to quantum states

QUANTUM BIT · QUBIT

$|0\rangle$ or $|1\rangle$

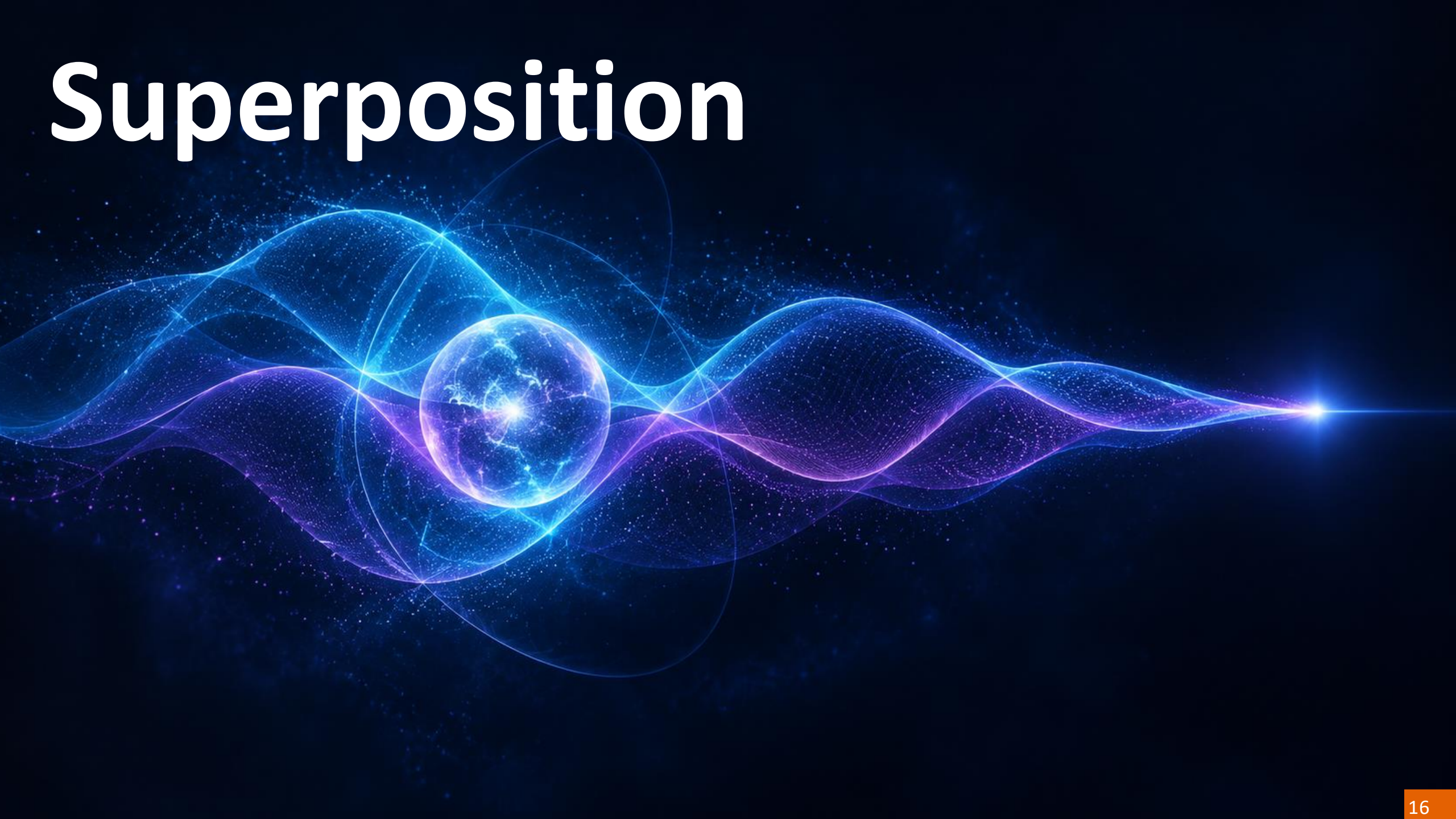
ket zero ket one

Two reference states

Called the computational
basis states

MEASUREMENT IN THIS BASIS records an ordinary classical result: **0 or 1**

Superposition



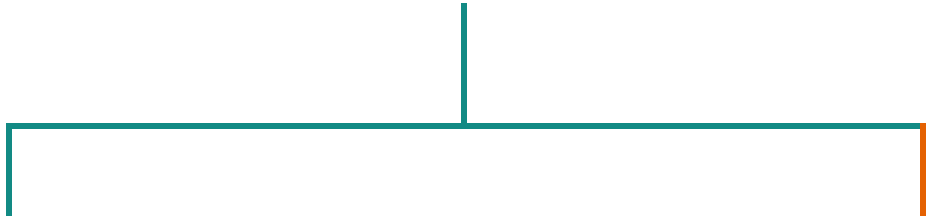
Superposition: one state with two components

ONE QUBIT STATE

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

Read: “ket psi”

two basis components in one state



ZERO COMPONENT

$\alpha|0\rangle$

α = amplitude

ONE COMPONENT

$\beta|1\rangle$

β = amplitude

α and β carry size and phase information.

Together: one coherent quantum state

Superposition is one quantum state. A measurement will still record one result.

From amplitudes to probabilities

Equal superposition

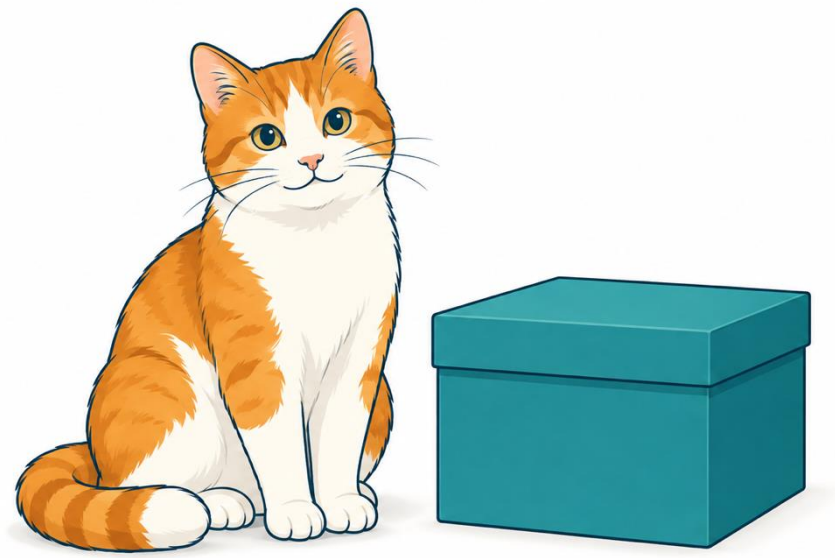
$$|\psi\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$$

OUTCOME	AMPLITUDE		SQUARE THE MAGNITUDE		PROBABILITY
0	$1 / \sqrt{2}$	→	$\lvert 1 / \sqrt{2} \rvert^2$	→	**1 / 2 = 50%**
1	$1 / \sqrt{2}$	→	$\lvert 1 / \sqrt{2} \rvert^2$	→	**1 / 2 = 50%**

Normalization $2 \times (1 / \sqrt{2})^2 = 1$ **Total probability = 100%**

The √2 keeps the total probability equal to 1. Other amplitudes give other probabilities.

Superposition revisited: Schrödinger's cat



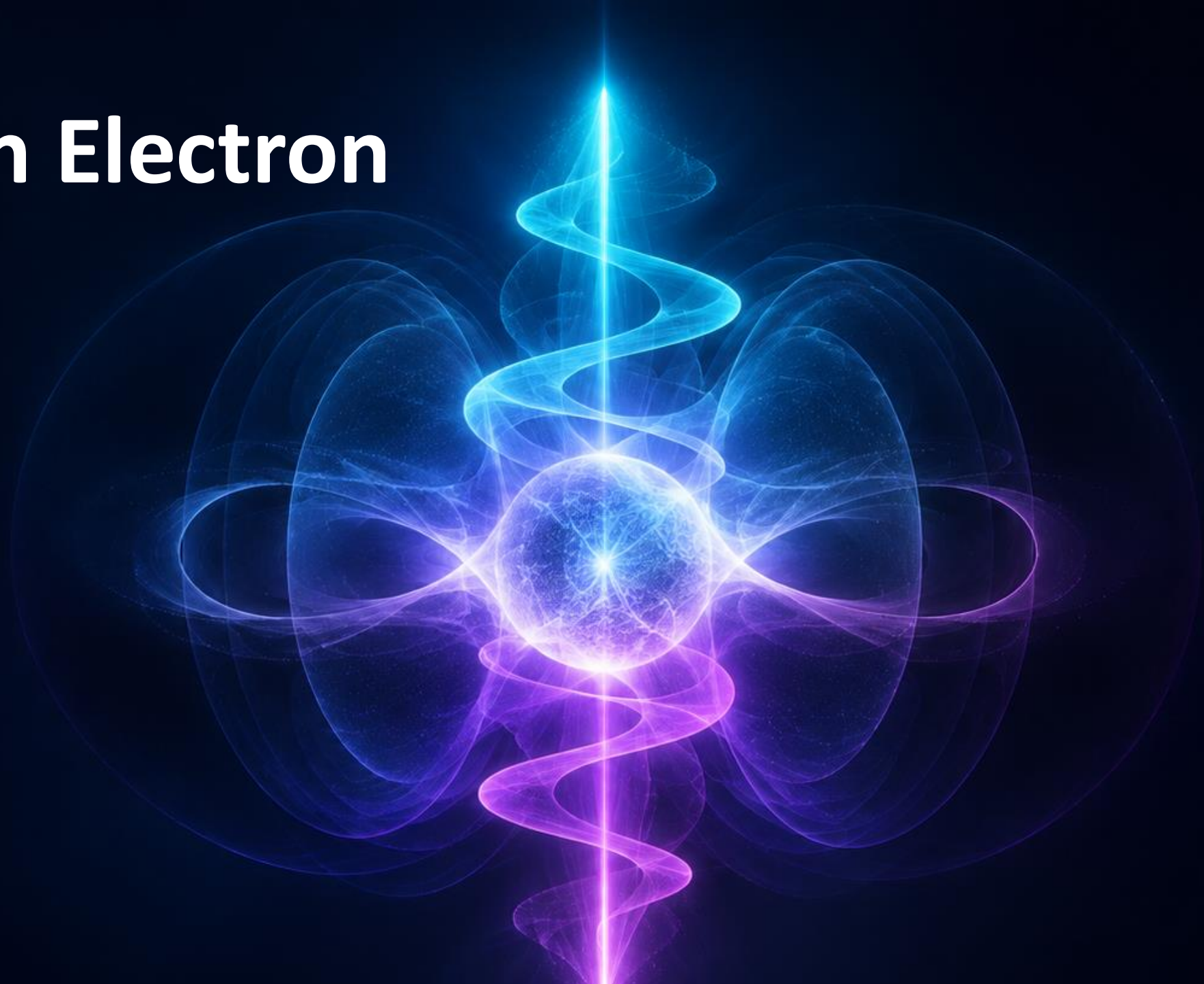
A microscopic event is linked to a macroscopic outcome.

No decay ↔ alive
Decay ↔ dead

Superposition is more than "we have not looked yet."

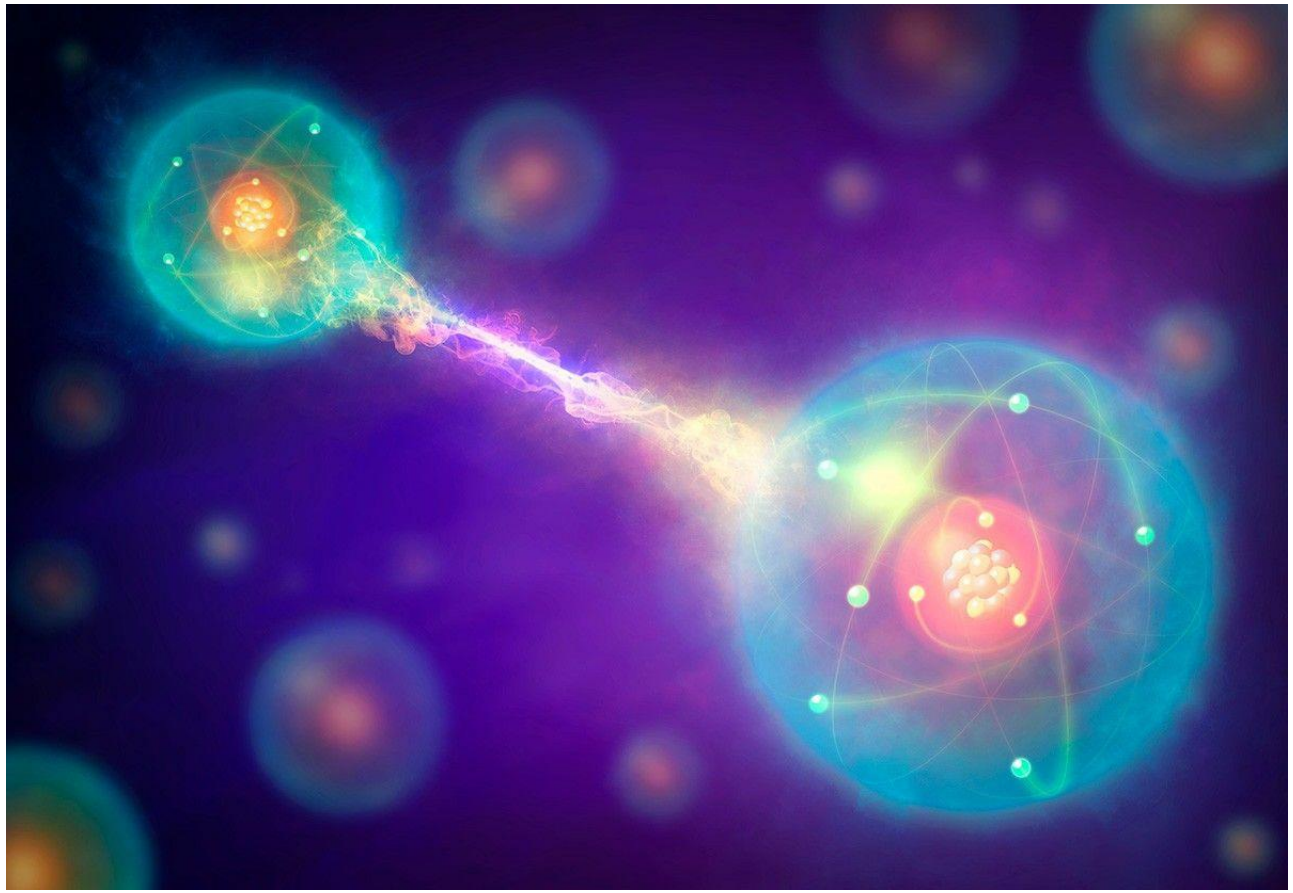
Thought experiment: environmental interactions suppress observable coherence.

Spin of an Electron



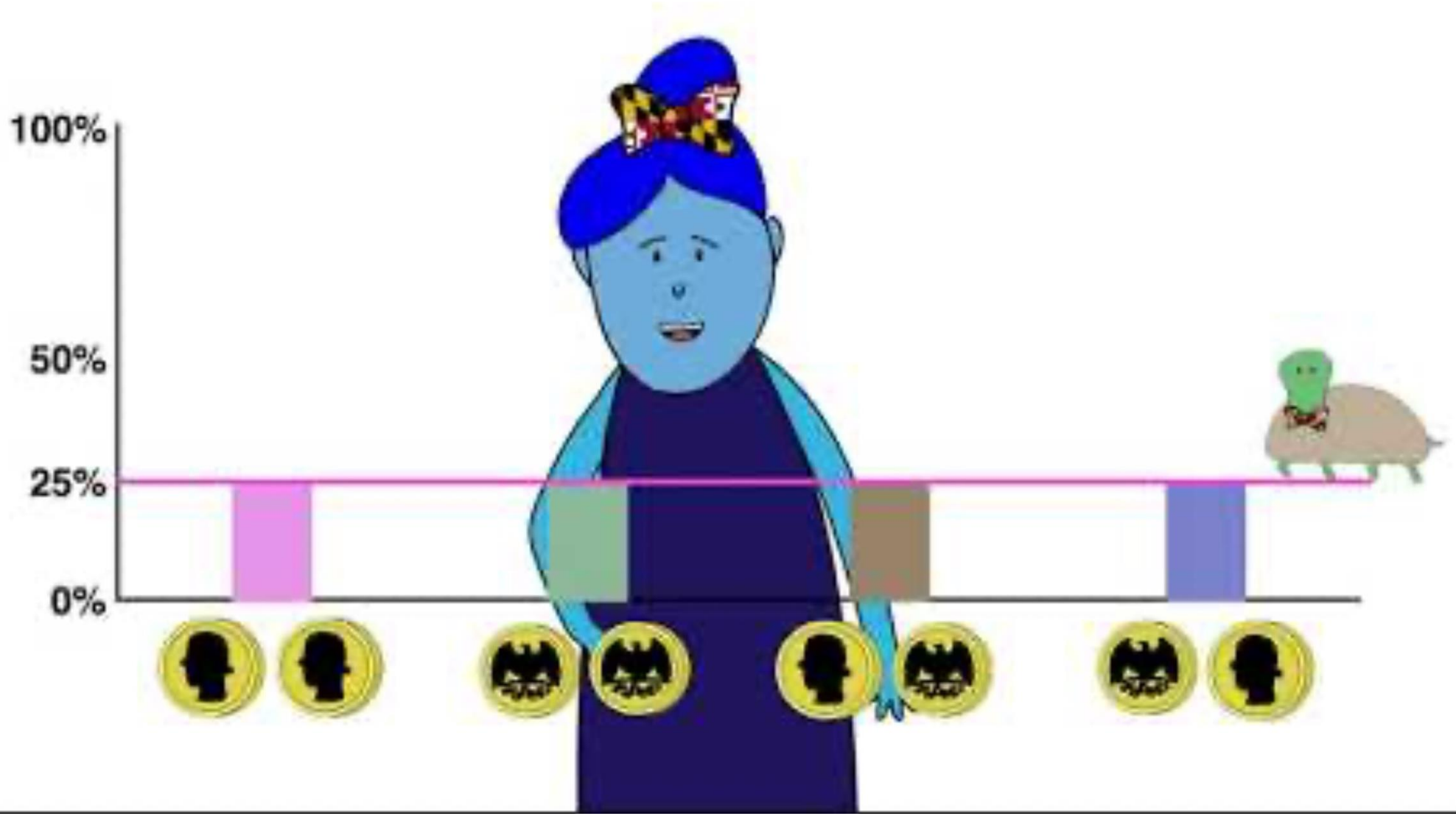
Quantum Entanglement "Spooky Science"

- **1935:** Albert Einstein and colleagues first pointed out the “spooky” action of quantum entanglement.
- Einstein’s theory of special relativity
  - “nothing can travel faster than the speed of light”
- **Entanglement**
  - Enables instantaneous measurement of the quantum state of one particle by measuring that of its entangled partner somewhere else in the universe
  - Which means
    - information would have to be delivered faster than lightspeed.



1964: John Stewart Bell experimentally validated entanglement

Quantum Entanglement "Spooky Science"



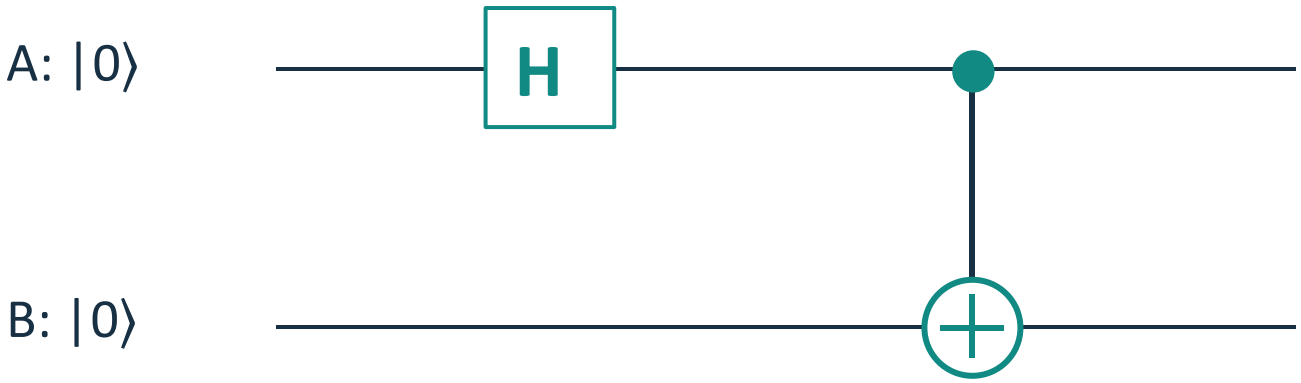
Credit: The Quantum Atlas

Entanglement and Bell pairs

PREPARE

CREATE A BELL PAIR

JOINT STATE



$$|\Phi^+\rangle = (|00\rangle + |11\rangle) / \sqrt{2}$$

“phi plus” Bell state

A Bell pair is two qubits prepared in a Bell state.

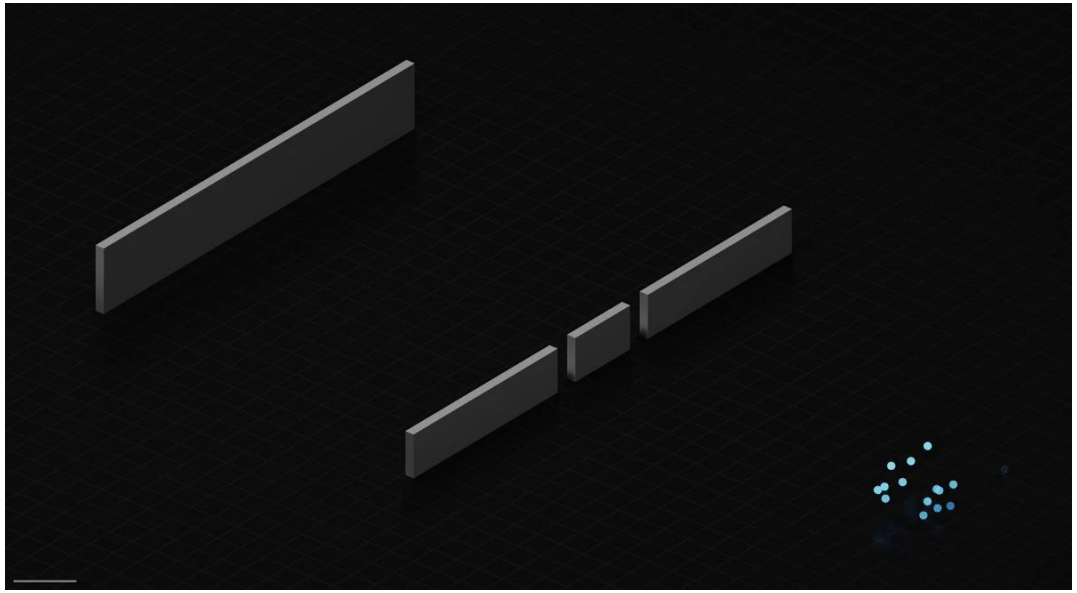
The joint state cannot be split into independent pure states for A and B.

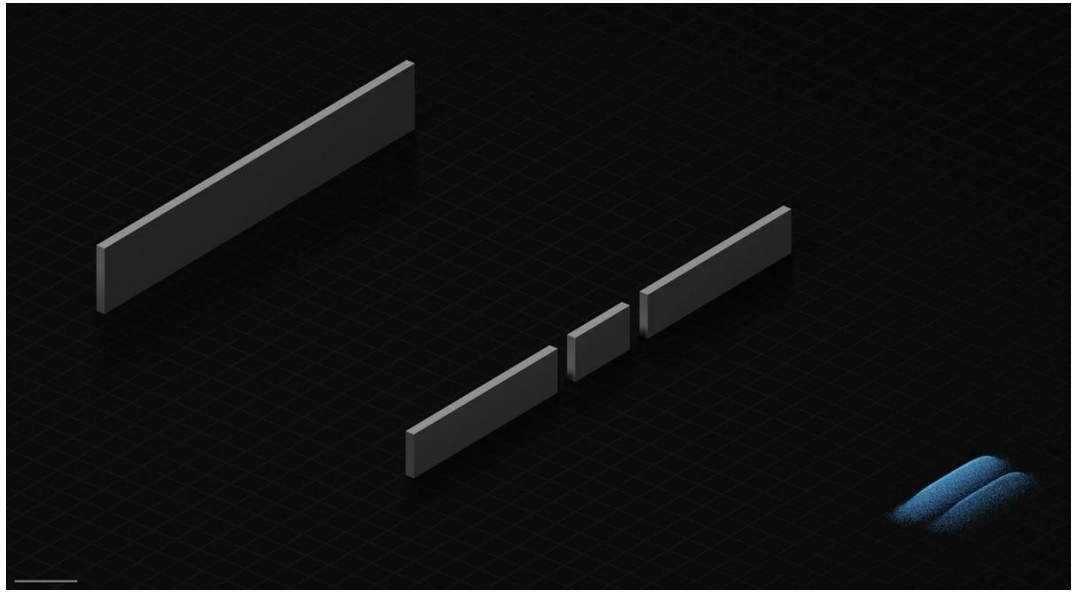
MEASURE BOTH IN THE 0/1 BASIS

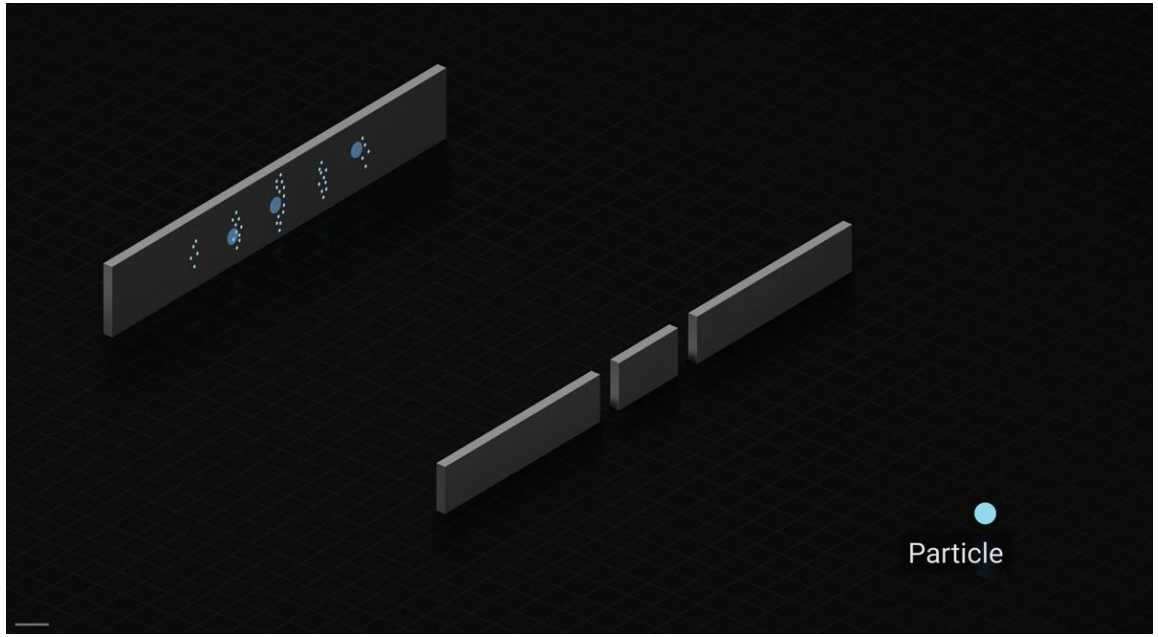


Bell pair = a specific entangled two-qubit state. Each result is random; the pair agrees.

Measurement

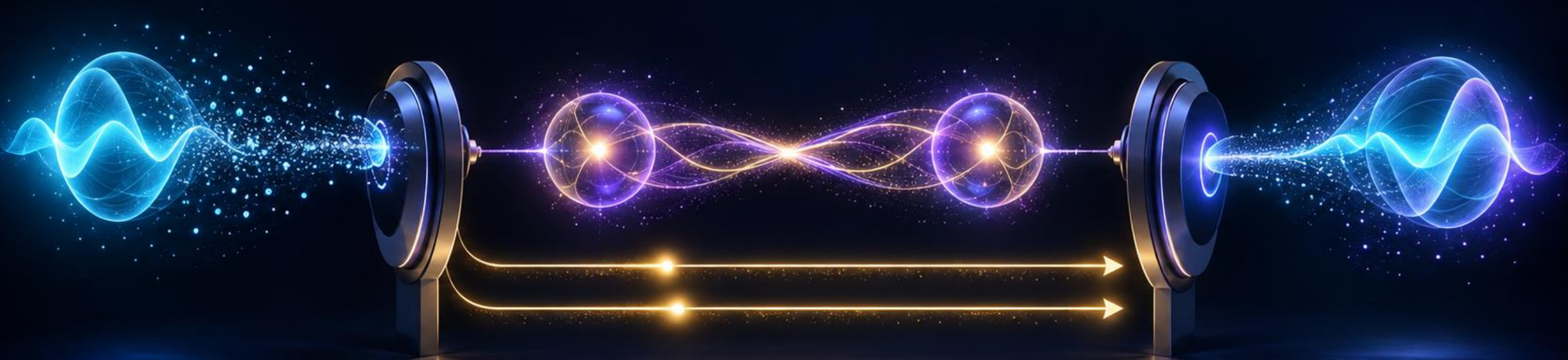






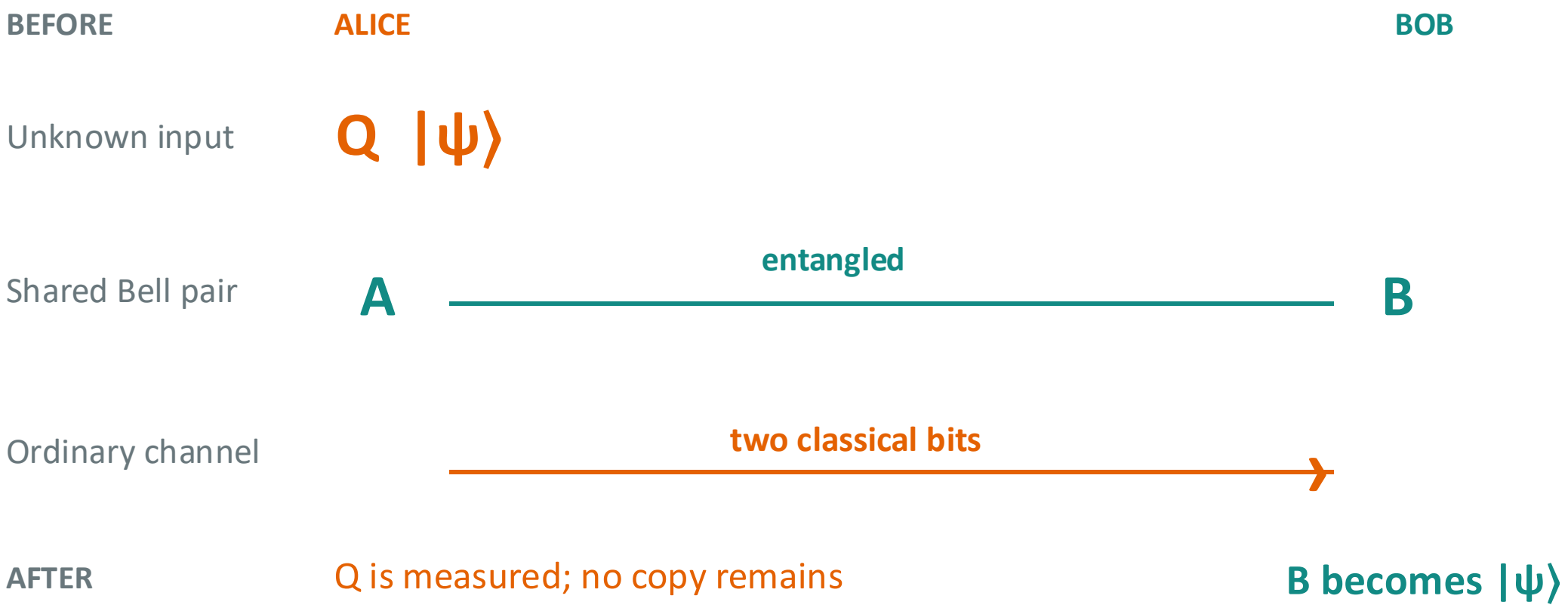
Credit: https://quantumatlas.umd.edu/entry/superposition/

Quantum Teleportation



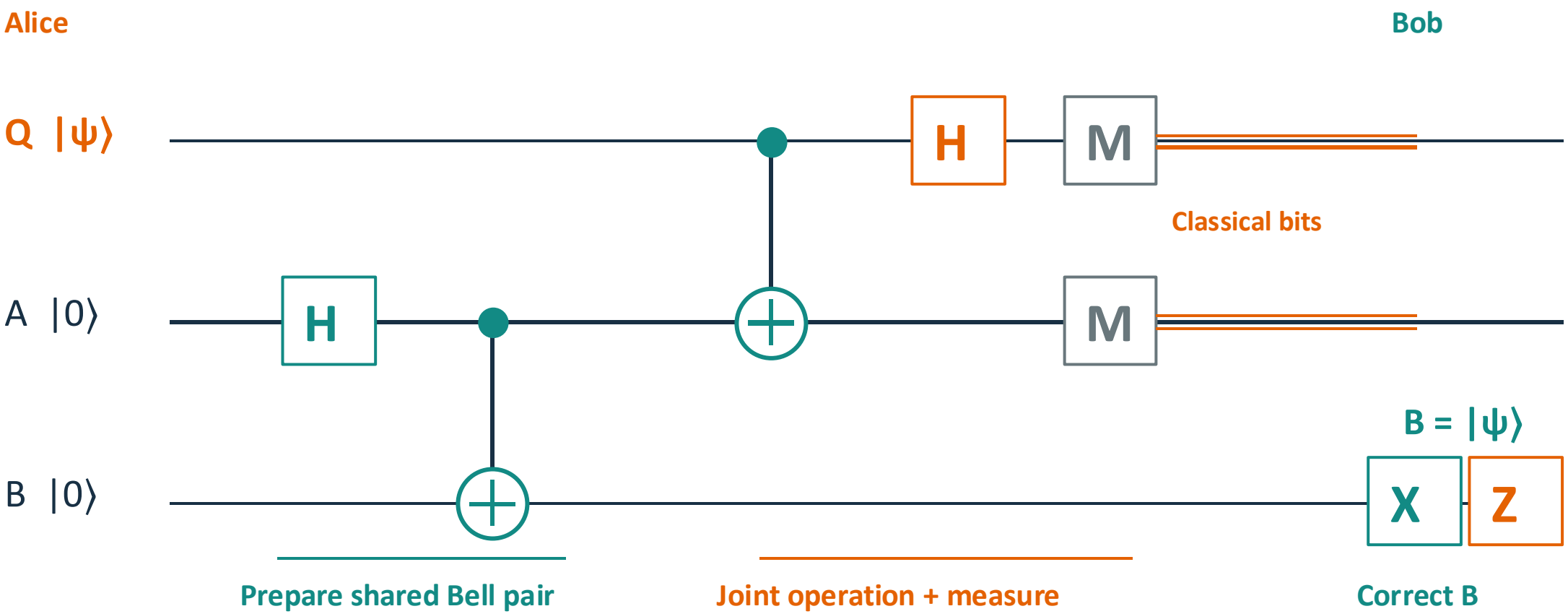
Teleportation transfers a quantum state

Quantum teleportation transfers an unknown qubit state to a distant qubit.



Matter does not travel through the diagram. Bob must receive the classical bits.

Quantum teleportation protocol



Entanglement + two classical bits + conditional correction reproduce |ψ⟩ on B.

Quantum gates change quantum states

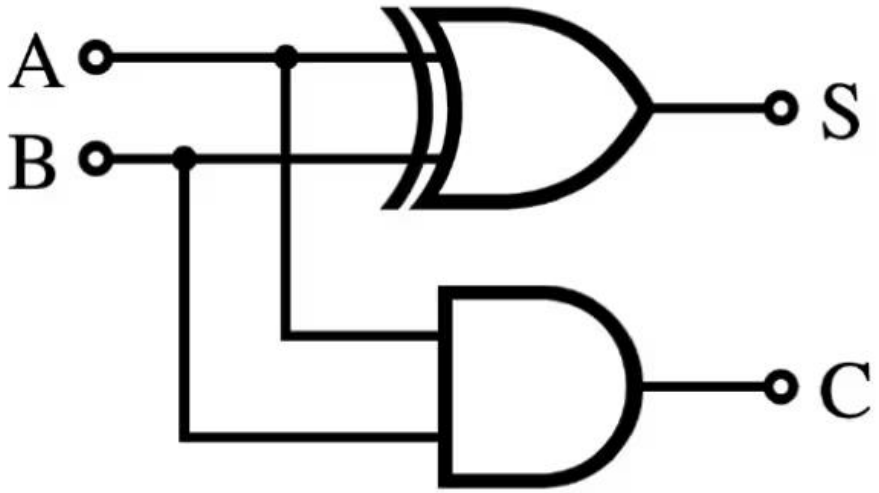


Ideal gates are unitary:

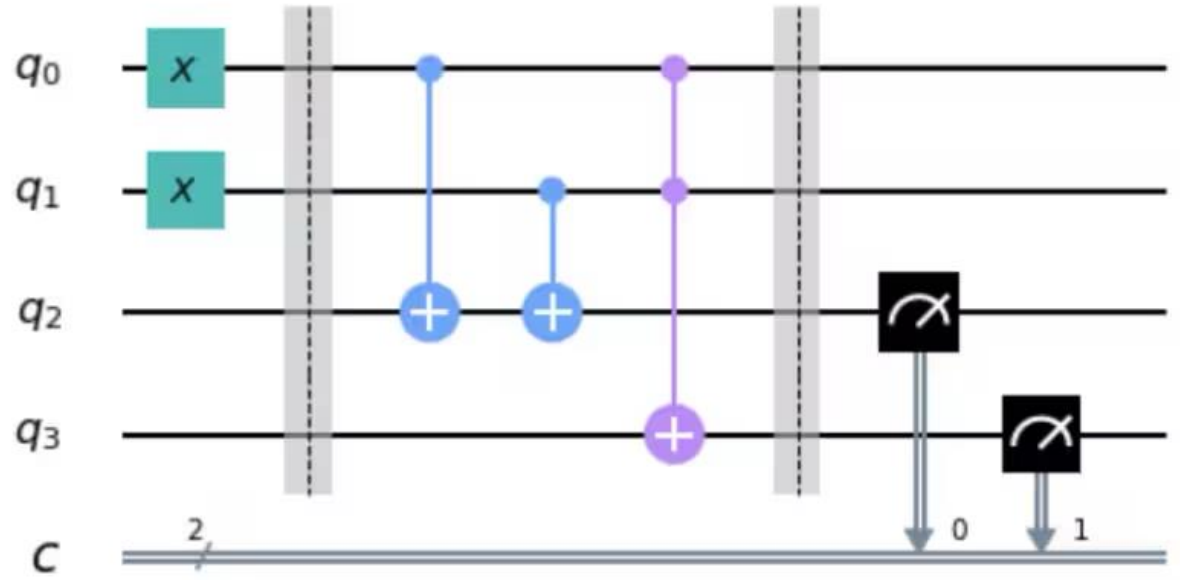
- Preserve total probability
- Have an inverse operation

Measurement is a separate operation; it is not generally reversible.

Quantum Circuits and Gates



Classical



Quantum

Credit: IBM Quantum Cloud

X gate (Pauli X): exchange zero and one

$X|0\rangle = |1\rangle$ $X|1\rangle = |0\rangle$



$\alpha|0\rangle + \beta|1\rangle \rightarrow \beta|0\rangle + \alpha|1\rangle$

X swaps amplitudes. Applying X twice returns the original state.

Hadamard gate: split and recombine

$$H|0\rangle = |+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$$

Measure now: 50% zero, 50% one

Apply H again before measuring:



H can create a superposition—and recombine it through interference.

Z gate: change the relative phase

$|+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$

Z

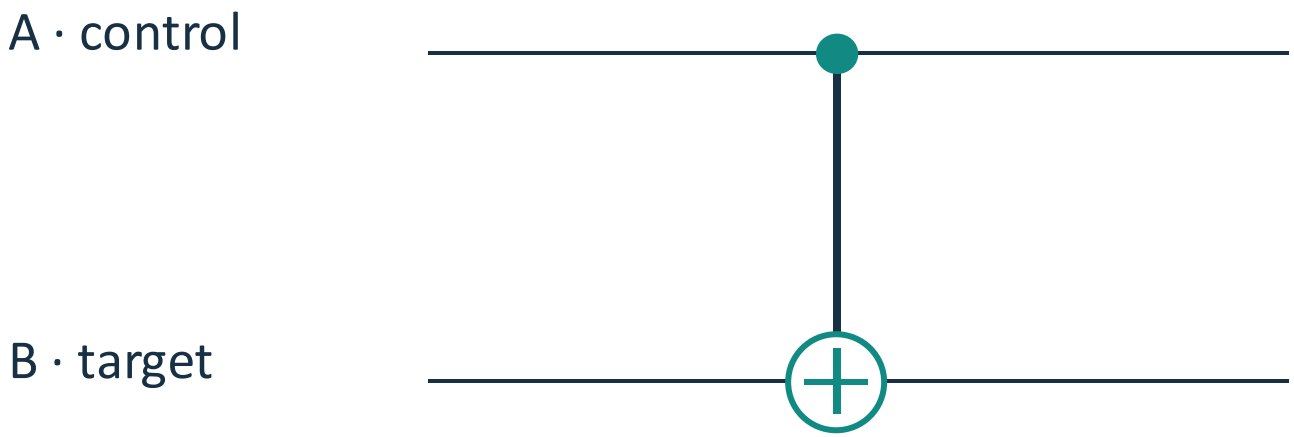
↓

$|-\rangle = (|0\rangle - |1\rangle) / \sqrt{2}$

Same 50/50 probabilities in the zero/one basis.

A later H reveals the difference: $|+\rangle \rightarrow |0\rangle$ and $|-\rangle \rightarrow |1\rangle$.

Controlled-NOT (CX/CNOT): connect two qubits



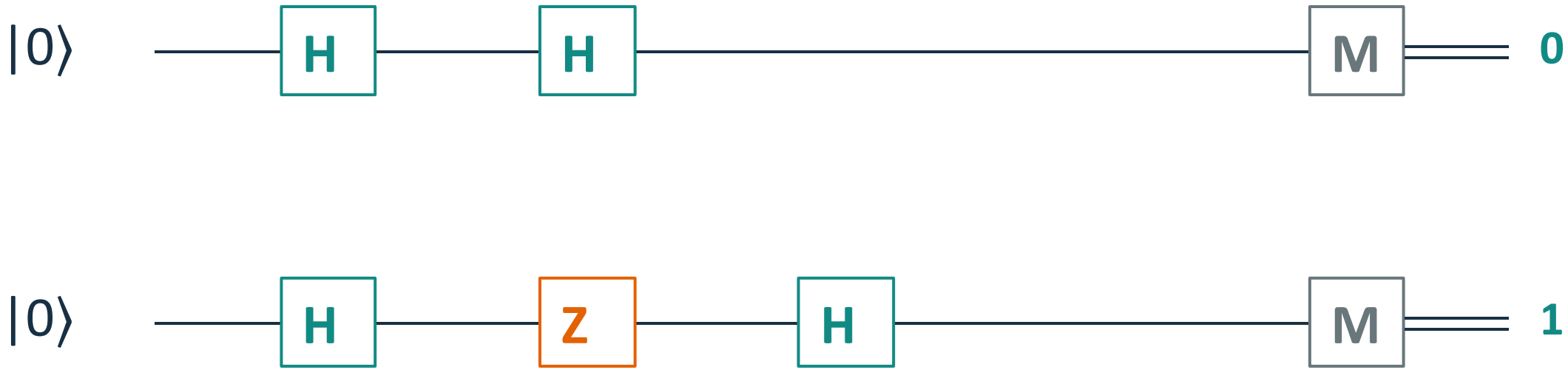
INPUT → OUTPUT
00 → 00
01 → 01
10 → 11
11 → 10

Control 1: flip the target.
Control 0: leave it alone.

A is written first: |AB⟩. CNOT can entangle suitable superposition inputs.

Quantum circuits: read from left to right

Wire = qubit Box = gate M = measurement



Ideal results: changing a relative phase changes the interference pattern.

Break for 10 Mins

Demonstration
RSA

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

Why classical factoring becomes difficult

The task is to recover two secret primes from their public product.

RSA-2048

IBM's example number N

2519590847…

…2120720357

Number abbreviated for display

$N = p \times q$

Find p and q

Classical factoring

Millions of years

IBM's estimate for a powerful classical computer

Shor's quantum algorithm

Hours

Requires a sufficiently large, reliable quantum computer

Broad estimates, not measured RSA-2048 runtimes. Our demo factors 15.

Source: IBM, Anne Dames, Post Quantum Cryptography Smorgasbord, PDF p. 10 (2026).

Shor's Algorithm: Factoring Becomes Period Finding

In 1994, Peter Shor introduced a quantum algorithm for efficient integer factorization.

RSA starts with two large prime numbers

Multiplication is easy

Choose primes P and Q, then publish their product N.

$$N = P \times Q$$

Factoring is the hard step

Given only N, recover P and Q.

Shor's key idea

Find a hidden period r, then use it to recover the factors.

Toy example in the next slides: factor N = 21 using a = 11.

Finding the Period for N = 21 and a = 11

Choose a = 11 and evaluate $f_{11,21}(x) = 11^x \bmod 21$.

Input	Remainder	Why
x = 0	$11^0 \bmod 21 = 1$	$11^0 = 0 \times 21 + 1$
x = 1	$11^1 \bmod 21 = 11$	$11^1 = 0 \times 21 + 11$
x = 2	$11^2 \bmod 21 = 16$	$11^2 = 5 \times 21 + 16$
x = 3	$11^3 \bmod 21 = 8$	$11^3 = 63 \times 21 + 8$
x = 4	$11^4 \bmod 21 = 4$	$11^4 = 697 \times 21 + 4$
x = 5	$11^5 \bmod 21 = 2$	$11^5 = 7669 \times 21 + 2$
x = 6	$11^6 \bmod 21 = 1$	$11^6 = 84360 \times 21 + 1$

The output returns to 1 after six steps: $f_{11,21}(6) = f_{11,21}(0)$. Therefore, r = 6.

Why the Period Helps Us Factor N

Definition of a period

$$f_{a,n}(x + r) = f_{a,n}(x)$$

Set x = 0

$$f_{a,n}(0 + r) = f_{a,n}(0)$$

Since 0 + r = r

$$f_{a,n}(r) = f_{a,n}(0)$$

Thus

$$a^r \bmod N = 1$$

After one full period, the function returns to its starting value.

Factor the resulting expression

$$a^r - 1 \bmod N = 0$$

$$(a^{r/2} - 1)(a^{r/2} + 1) \bmod N = 0$$

This uses $(u - 1)(u + 1) = u^2 - 1$, with $u = a^{r/2}$.

If r is even and $a^{r/2} + 1 \bmod N \neq 0$:

$$P = \gcd(a^{r/2} + 1, N) \quad Q = \gcd(a^{r/2} - 1, N)$$

Recovering the Factors of 21

We found r = 6, which is even. Now check the second condition.

$$a^{r/2} + 1 \bmod N = 11^{6/2} + 1 \bmod 21 = 1332 \bmod 21 = 9 \neq 0$$

Both conditions hold, so calculate the two greatest common divisors.

$$\gcd(11^{6/2} + 1, 21)$$
$$= \gcd(1332, 21) = 3$$

$$\gcd(11^{6/2} - 1, 21)$$
$$= \gcd(1330, 21) = 7$$

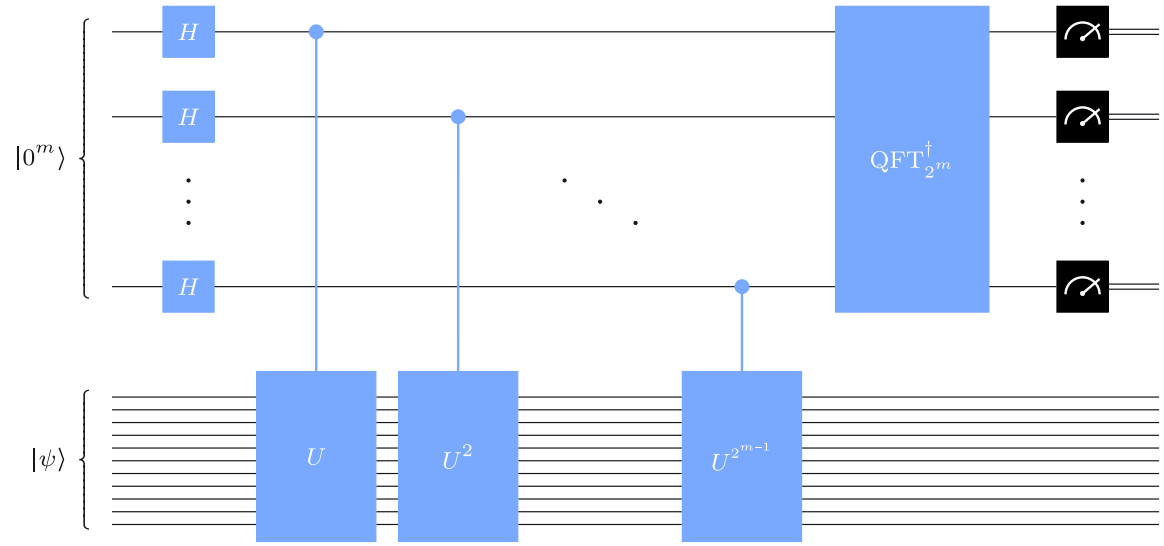
Therefore, 21 = 3 × 7.

Quantum Phase Estimation

- Quantum procedure that measures a hidden phase produced by a quantum operation.

$|u>$ is special for an operation *U*

$$U\ |u> = e^{2\pi i\theta}\ |u>$$



- *U* is a quantum operation
- |u> is an eigenstate of *U*
- Applying *U* preserves the state but adds a phase
- *θ is the unknown phase we want to estimate*
- *$e^{2\pi i\theta}$ represents a rotation around the complex unit circle*
- *QPE cannot be measured directly. QPE converts it into ordinary bits*

Why we need quantum phase estimation

THE DEMO PROBLEM

Shor's algorithm needs a repeating pattern.

For the tutorial example, the pattern comes from:

$2^x \bmod 15$

1	→ 2	→ 4	→ 8	→ 1
x=0	x=1	x=2	x=3	x=4

THE QUANTUM TRICK

QPE helps the quantum circuit detect hidden phase fractions.

Those fractions contain information about the repeat length, called the order.

Here, the repeat length is r = 4.

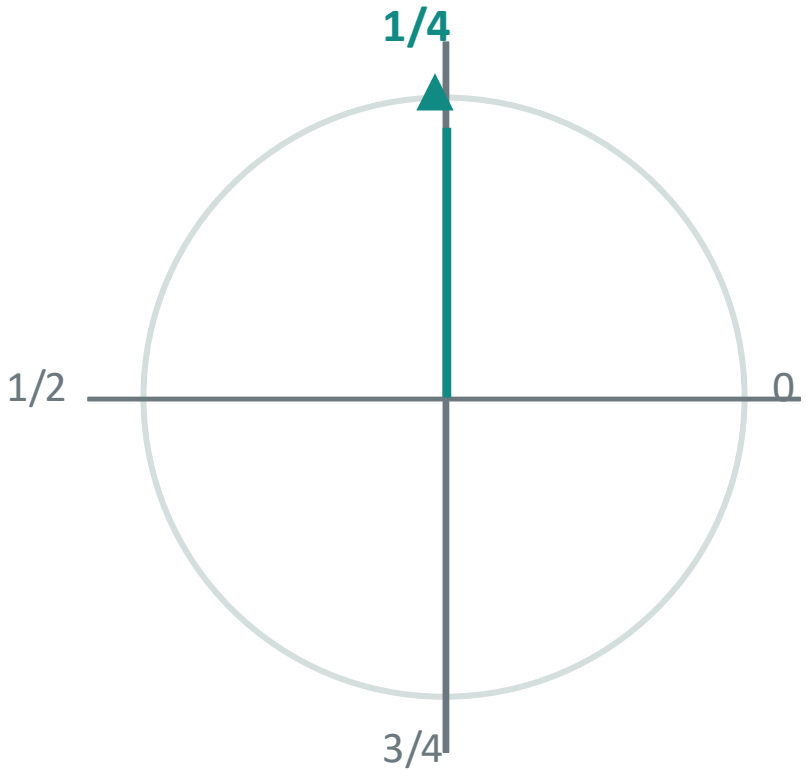
QPE turns hidden phase information into bits that help reveal the repeating period.

A phase as a rotation

BEGINNER PICTURE

A phase is like an angle attached to a quantum state.

A full turn represents 1. A half turn represents 1/2. A quarter turn represents 1/4.



e^(2πiθ)

means a rotation by θ turns

QPE estimates how far around the complex circle the state has rotated.

The special input state

EIGENSTATE IDEA

QPE assumes the input state is special for the operation U.

This special state is called an eigenstate.

- U acts on the state.
- The state keeps the same identity.
- Only the phase changes.



$$U|u\rangle = \text{phase} \times |u\rangle$$

An eigenstate gives QPE a stable object whose phase can be estimated.

The QPE equation

THE PROMISE

$$U|u\rangle = e^{(2\pi i\theta)}|u\rangle$$

U	quantum operation
$\|u\rangle$	eigenstate of U
θ	unknown phase
$e^{(2\pi i\theta)}$	rotation on the complex circle

WHAT QPE RETURNS

The phase cannot be measured directly.

QPE converts it into ordinary bits.

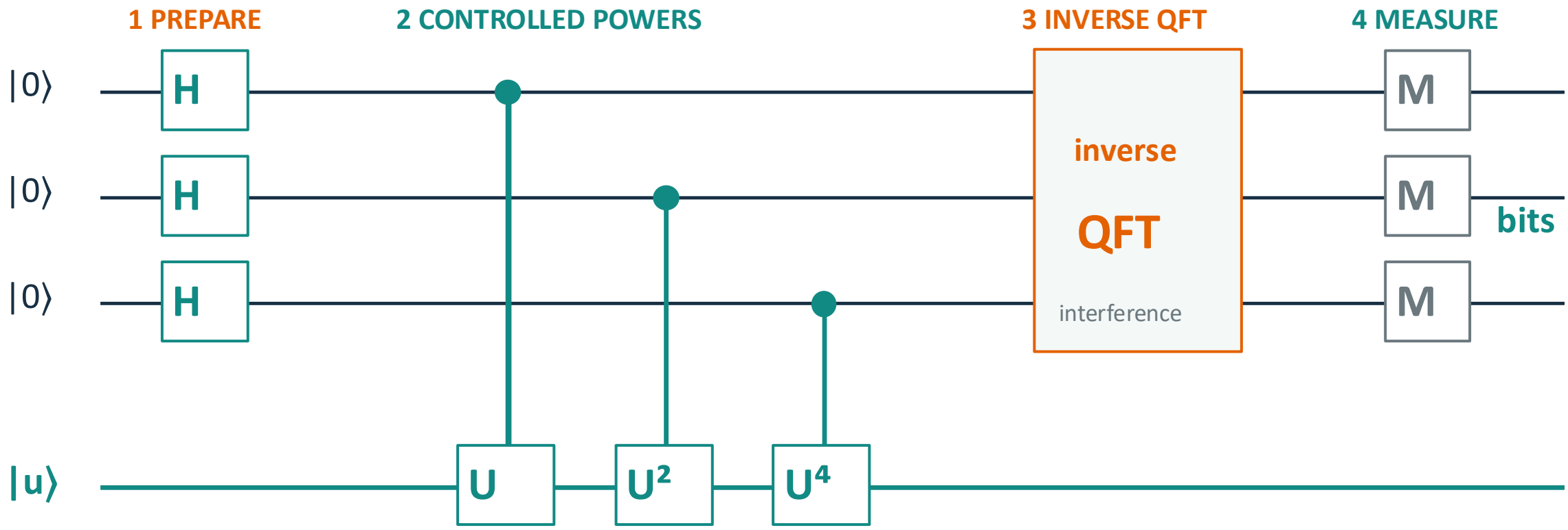
With m control qubits:

$$\theta \approx y / 2^m$$

y is the measured integer.

The equation says U preserves the eigenstate and adds a measurable phase target.

The four steps of QPE



Controlled powers: U, U^2, U^4, U^8, …

QPE uses phase kickback and inverse QFT to make θ visible as bits.

The inverse QFT turns phase information into a readable bit pattern.

Worked example: θ = 1/4

IDEAL EIGHT-BIT CASE

Use m = 8 control qubits.

That gives $2^8 = 256$ possible measured integers.

hidden phase	$\theta = 1/4$
measured integer	$y = \theta \times 2^8 = 64$
eight-bit output	01000000_2
phase estimate	$64 / 256 = 1/4$

01000000_2

→

64

→

1/4

The circuit returns bits. Classical arithmetic converts the bits into a phase estimate.

QPE inside Shor’s order finding

ORDER

The order is the repeat length.

For 2^x mod 15:

1, 2, 4, 8, 1, …

r = 4

PHASE FRACTIONS

QPE estimates phases related to:

k / r

For r = 4, possible phases are:

0, 1/4, 2/4, 3/4

A measured 1/4 has denominator 4, so the classical step proposes r = 4.

QPE does not directly output the order. It outputs phase information that helps recover it.

“Quantum phase estimation converts an invisible phase rotation into measurable binary digits.”

In Shor’s algorithm, those digits reveal information about the repeating period.

Takeaway

Phase → bits → fraction → candidate order → classical check

Use this as the transition from QPE back to the Shor’s algorithm demo.

IBM Quantum Cloud

https://quantum.cloud.ibm.com/



Thank You!

https://www.rahmanmsaidur.com

msrahman3@utep.edu

Break 5 mins

Demonstration
Quantum Machine Learning