CADT
IDT វិទ្យាស្ថានបច្ចេកវិទ្យាឌីជីថល
Institute of Digital Technology

# Quantum Computing

## From Theory to Practical

Gen 10 SE Y4 2026-2027

Lecturer: **Ms. HENG Sovanmonynuth**

Software Engineering (SE), Faculty of Digital Engineering, Department of Computer Science

Cambodia Academy of Digital Technology (CADT)

Email: sovanmonynuth.heng@cadt.edu.kh

Mobile: (+855) 95 479 272

# Course Outline

Chapter 1: Introduction to Quantum Computing

**Chapter 2: Basic of Quantum Mechanics**

Chapter 3: Quantum Algorithms

Chapter 4: Quantum Fourier Transform

Chapter 5: Quantum Errors & Noises

Chapter 6: Quantum Machine Learning

Chapter 7: Quantum Chemistry

Chapter 8: Quantum Cryptography

**Final Presentation**

# Chapter 2: Basic of Quantum Mechanics

- Quantum State & Operations
  - Single Qubit Gates
  - Multi Qubit Gates
  - Measurement
- Quantum Core Phenomena
  - Superpositions
  - Entanglement
  - Interference
  - No Cloning Theorem
  - Randomness
- Quantum Protocols
  - Teleportation
  - Superdense Coding

# Quantum State

- A **quantum state** holds **all information** about a system.
- Represented as: **$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,**
  where α and β are complex amplitudes and **$|\alpha|^2 + |\beta|^2 = 1$**
- Visualized on the **Bloch sphere**

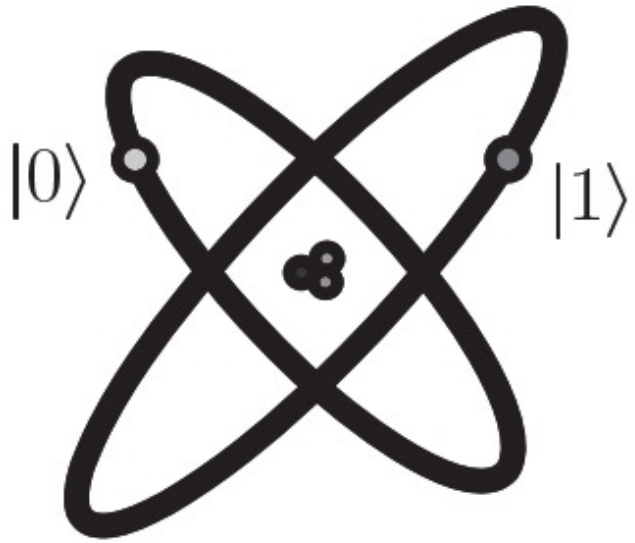



Figure 1.2. Qubit represented by two electronic levels in an atom.

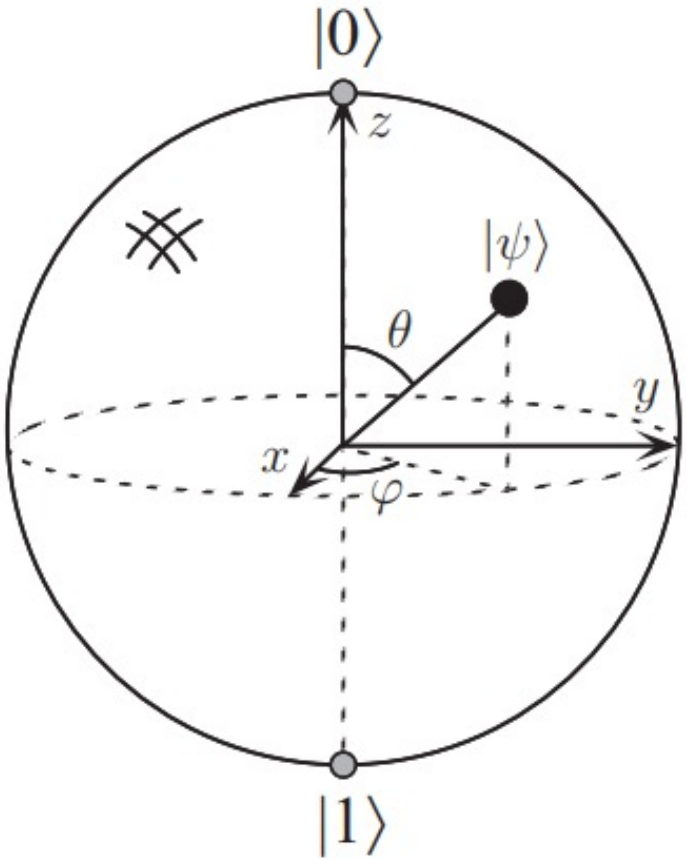



Figure 1.3. Bloch sphere representation of a qubit.

# Quantum State

- **Single Qubit Gates**

| Gate | Symbol | Matrix |
|---|---|---|
| Identity | $I$ | $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ |
| Hadamard | $H$ | $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |
| Pauli-X (NOT) | $X$ | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| Pauli-Y | $Y$ | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| Pauli-Z | $Z$ | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| Phase (S) | $S$ or $\sqrt{Z}$ | $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |

| Gate | Symbol | Matrix |
|---|---|---|
| Conjugate Phase | $S^\dagger$ | $\begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$ |
| T gate (π/8) | $T$ | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ |
| T dagger | $T^\dagger$ | $\begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix}$ |
| Square-root of X | $\sqrt{X}$ or $S_x$ | $\frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$ |
| Square-root of X (adjoint) | $\sqrt{X}^\dagger$ | $\frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix}$ |
| Rotation-X | $R_X(\theta)$ | $\begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$ |

# Quantum State

- **Single Qubit Gates**

| Gate | Symbol | Matrix |
|---|---|---|
| Rotation-Y | $R_Y(\theta)$ | $\begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$ |
| Rotation-Z | $R_Z(\theta)$ | $\begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$ |
| Phase (parameterized) | $P(\lambda)$ | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix}$ *(equals $R_Z(\lambda)$ up to a global phase)* |
| General 1-qubit | $U(\theta, \phi, \lambda)$ | $\begin{bmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\phi+\lambda)}\cos\frac{\theta}{2} \end{bmatrix}$ |

# Quantum State

- **Two-qubit Gates**
- Combine qubits using tensor product
- Common 2-qubit gates: **CNOT**, **CZ**, **SWAP**
- Enable **entanglement** & conditional operations

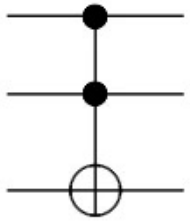
- **Demo:** Apply H + CNOT → create Bell pair

| Gate | Symbol | Matrix |
|---|---|---|
| CNOT | $CX$ | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ |
| Controlled-Z | $CZ$ | $\mathrm{diag}(1, 1, 1, -1)$ |
| Controlled-Y | $CY$ | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix}$ |
| Controlled-Phase | $CP(\phi)$ | $\mathrm{diag}(1, 1, 1, e^{i\phi})$ |
| SWAP | $SWAP$ | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |
| iSWAP | $iSWAP$ | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |
| Sqrt-SWAP | $\sqrt{SWAP}$ | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |

# Quantum Operation

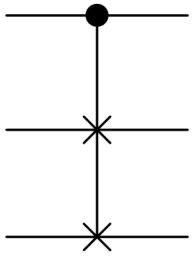
- **Three-qubit Gates**

| Gate | Symbol | Action (on basis) |
|---|---|---|
| **Toffoli** | (CCX) | Flips target if **both** controls are (true) |
| **Fredkin** | (CSWAP) | Swaps the two targets if control is (true) |



$$\text{CCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Toffoli Gate

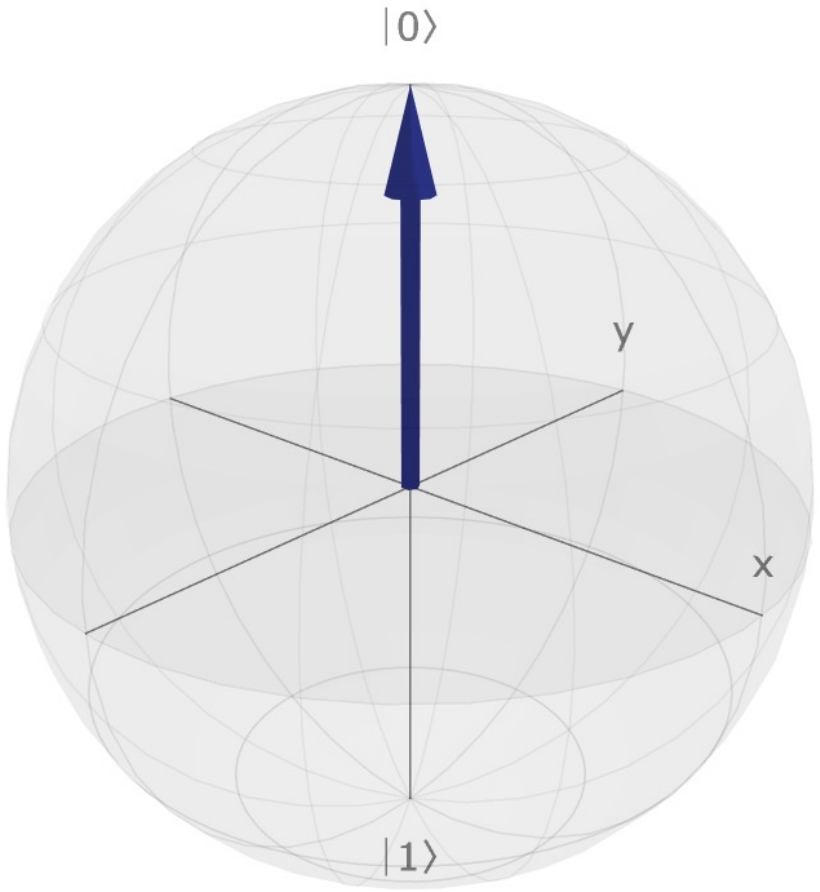


$$\text{Fredkin} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Fredkin Gate

# Quantum State

- Visualized the gate on the **Bloch sphere**
  - Bloch Sphere Simulator
  - Bloch Sphere Simulator
  - Bloch Sphere Simulator



# Quantum Operation

- **Single-Qubit Gates**

| Name | Symbol | # Qubits | Definition | Native? |
|---|---|---|---|---|
| Identity | I | 1 | $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | Yes |
| Pauli-X |  | 1 | $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | Yes |
| Pauli-Y | Y | 1 | $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ | Yes |
| Pauli-Z | Z | 1 | $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | Yes |
| Sqrt-X | $\sqrt{\text{X}}$ | 1 | $\sqrt{-iX} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$ | Yes |
| Sqrt-Y | $\sqrt{\text{Y}}$ | 1 | $\sqrt{-iY} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ | Yes |
| Sqrt-Z (Phase) | $\sqrt{\text{Z}}$ | 1 | $S = \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ | Yes |
| $\pi/8$ (T) | T | 1 | $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ | Yes |
| Hadamard | H | 1 | $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ | No |

# Quantum Operation

- **Multi-Qubit Gates**

| Name | Symbol | # Qubits | Definition | Native? |
|---|---|---|---|---|
| Controlled-NOT (CNOT) |  | 2 | $\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ | No |
| Swap |  | 2 | $\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ | No |
| Toffoli (CCNOT) |  | 3 | $\mathrm{Toff} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$ | No |

**Step III:**
**Translation to QASM code**

Gates

H | I | Y | Z | T | √X | √Y | √Z

Quantum circuit

Manual submit

q[0] H
q[1]
q[2] H T
q[3] Y Z
√Y √X T T

Correspondence

+ −

**Step I:**
**Set number of qubits**

T

**Step II:**
**Drag & drop gates**

QASM code

```
1  OPENQASM 3;
2  include 'stdgates.inc';
3
4  bit[4] c;
5  qubit[4] q;
6
7  h q[2];
8  t q[2];
9  h q[0];
10 cx q[0], q[1];
11 swap q[1], q[2];
12 y q[3];
13 z q[3];
14 ccx q[1], q[2], q[3];
15 t q[3];
16 rx(pi/2) q[2];
17 cx q[2], q[3];
18 ry(pi/2) q[1];
```

**Step IV:**
**Transfer algorithm to server**

University of Stuttgart
Germany

NVIDIA CUDA

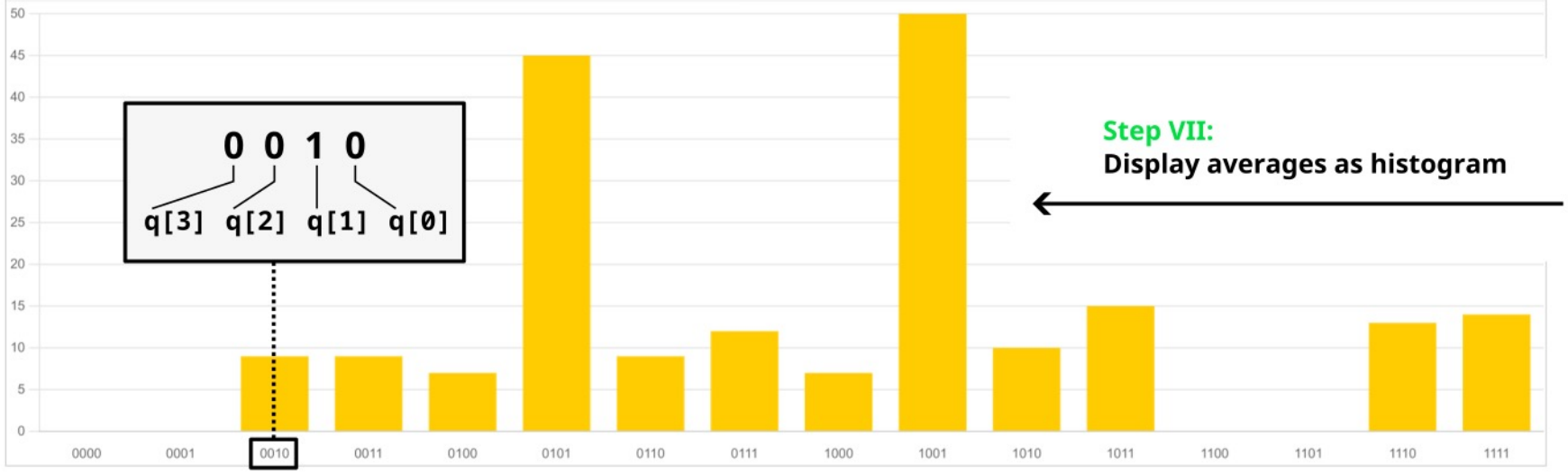


**Step V:**
**Perform simulations (200 shots)**
**& accumulate outcomes**

**Step VI:**
**Transfer results back to client**

**Step VII:**
**Display averages as histogram**

Histogram



# Quantum Core Phenomena

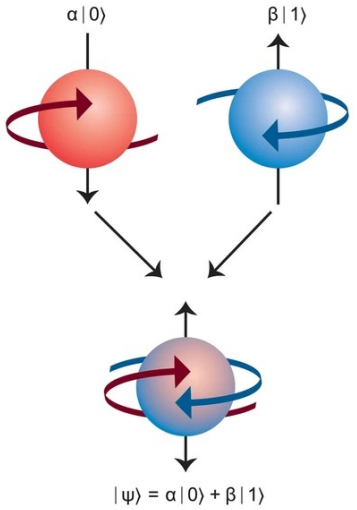
**Superposition**

- **Quantum Mechanics**

  In quantum theory, any isolated system can exist as a linear combination of basis states. For a single qubit:

  $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ where } |\alpha|^2 + |\beta|^2 = 1$$

  This means the qubit simultaneously occupies both $|0\rangle$ and $|1\rangle$ until measured.




- **Mathematical Foundation**

  Superposition arises from the Hilbert space linearity:
  if $|a\rangle$ and $|b\rangle$ are valid states, then $c_1 \mid a\rangle + c_2 \mid b\rangle$ is also a valid state.

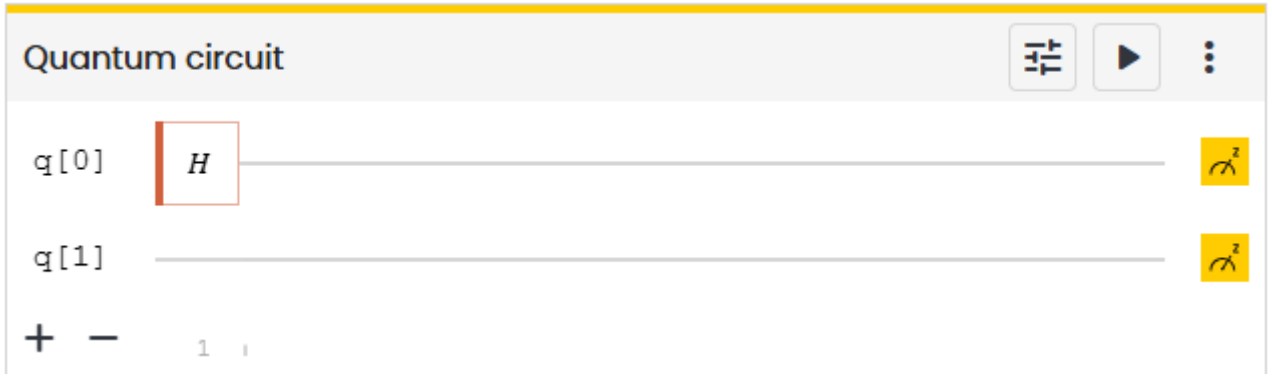
- **Quantum Physics**

  A photon polarized at 45° is in a superposition of horizontal and vertical states.
  A superconducting qubit in IBM Q devices uses two energy levels of a Josephson junction to form this superposed state.

# Quantum Core Phenomena

**Superposition**

- **Algorithmic Role**
  - **Hadamard transform** creates superposition of $2^n$ states → key to quantum parallelism.
  - Used in **Grover's search** and **Shor's algorithm** to explore multiple paths simultaneously before interference filters correct answers.



# Quantum Core Phenomena

**Entanglement**

- **Quantum Mechanics Definition**

  A multi-qubit system is entangled if its total wavefunction cannot be written as a product of individual states:$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$

- **Example**

  The Bell state or EPR Pair: $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, cannot be factored — measurement on one qubit instantaneously determines the other's state.

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \xrightarrow{\text{Measurement}} |\Psi_3\rangle = \begin{cases} |00\rangle & \text{with } p_0 = 0.5 \\ |01\rangle & \text{with } p_1 = 0 \\ |10\rangle & \text{with } p_2 = 0 \\ |11\rangle & \text{with } p_3 = 0.5 \end{cases}$$

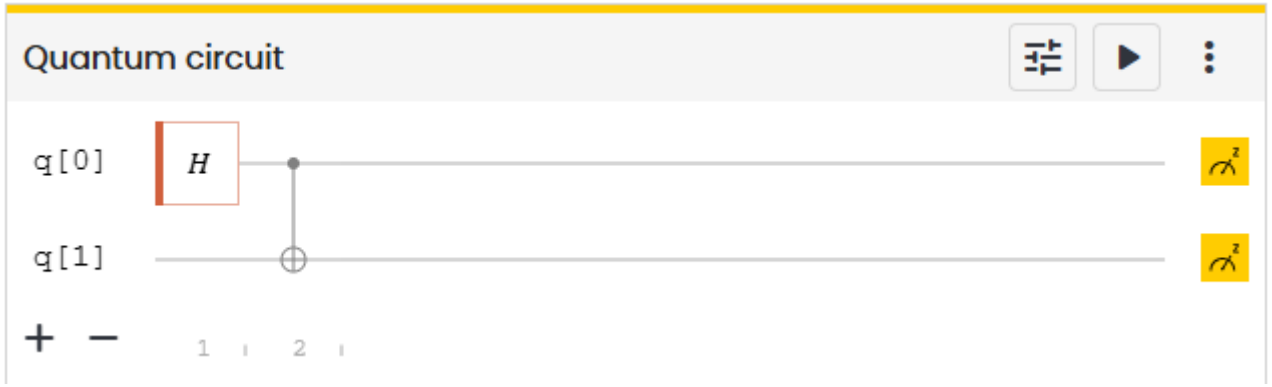
# Quantum Core Phenomena

**Entanglement**

- **Quantum Physics**

  Entanglement arises from interaction Hamiltonians (e.g., spin-spin coupling, photon pair generation through spontaneous parametric down-conversion).

- **Algorithmic Role**
  - **Entanglement** of **Bell State** Circuit
  - Enables **quantum teleportation**, **superdense coding**, **quantum key distribution (QKD)**.



# Quantum Core Phenomena

**Interference**

- **Quantum Mechanics**

  Quantum states carry ***complex probability amplitudes***. When two paths combine, amplitudes add; probabilities depend on the **square modulus**:

  $$P = |\psi_1 + \psi_2|^2$$

  Phase differences produce **constructive** or **destructive** *interference*.

- **Mathematical Form**

  If two paths lead to $|1\rangle$: $A_{total} = A_1 + A_2, P_1 = |A_{total}|^2$

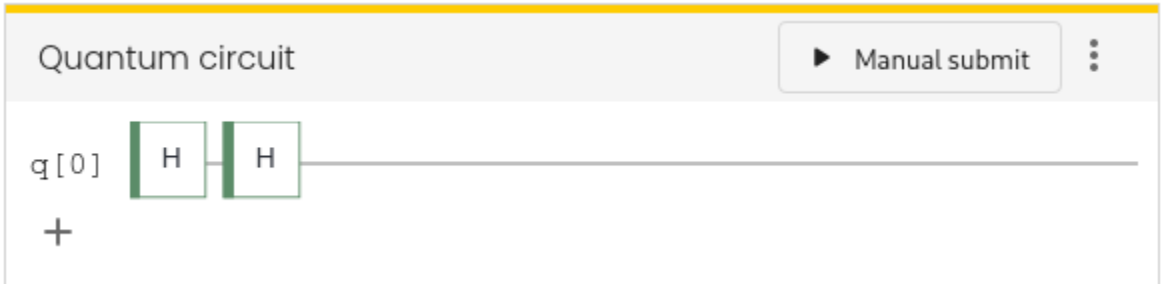
  A relative phase of π leads to **cancellation** (**destructive interference**).

# Quantum Core Phenomena

**Interference**

- **Example**

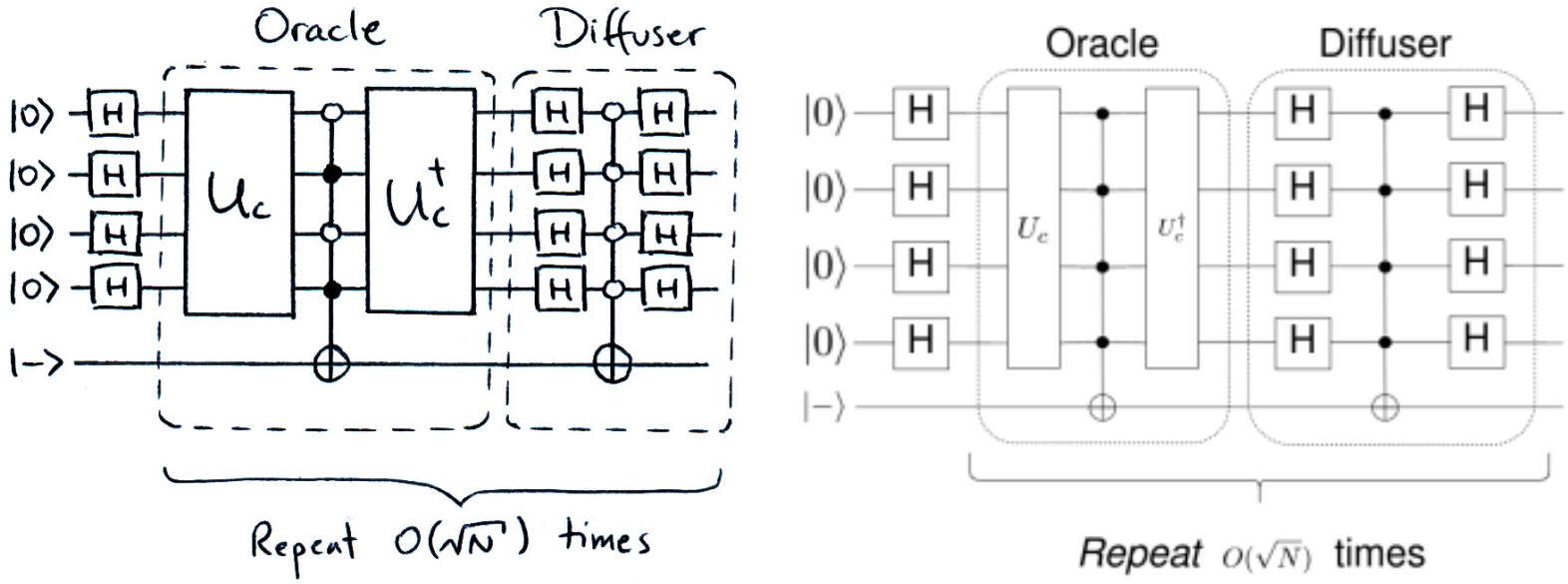
  Double-slit experiment — electrons or photons interfere with themselves, producing fringes determined by relative phase.



# Quantum Core Phenomena

**Interference**

- **Algorithmic Role**
- **Quantum Fourier Transform (QFT)** uses interference to isolate frequency components.
- **Grover's algorithm** amplifies correct answers via *constructive interference* of solution states.




Grover's Algorithm

# Quantum Core Phenomena

**No Cloning Theorem**

- **Quantum Mechanics Definition**

  There is **no unitary operator** $U$ for all possible |ψ⟩, like

  $$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

  You *can't make a perfect photocopy* of an *unknown quantum state* (a qubit), violating linearity of Schrödinger's equation.

- **Physical Meaning**

  Quantum processes are *strictly linear*; perfect copying would need a *nonlinear trick*—so nature forbids it. Quantum information cannot be copied perfectly — *measurement disturbs the state*.

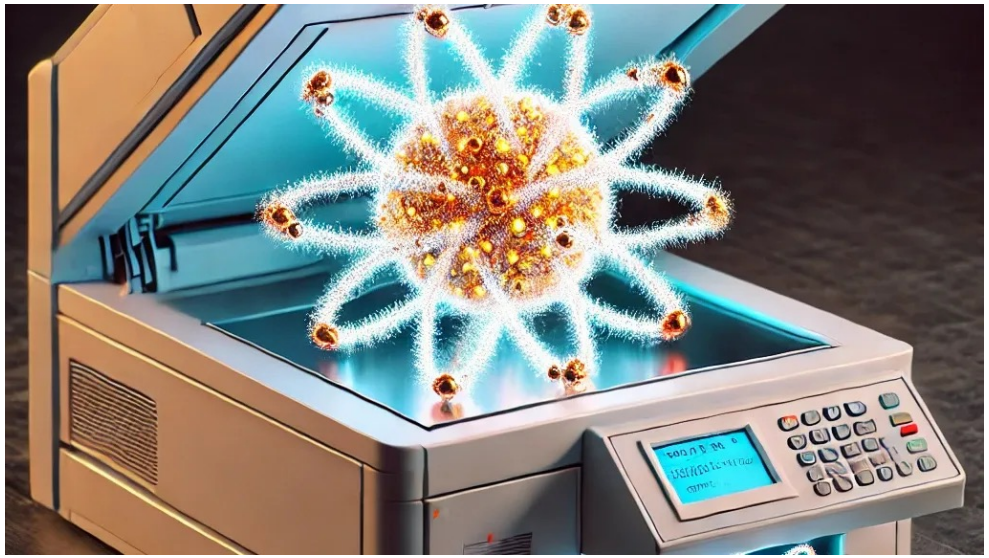
  **Example:** In quantum communication, an eavesdropper cannot duplicate qubits from a QKD channel; any attempt introduces detectable errors.

# Quantum Core Phenomena

**No Cloning Theorem**

- **E.g. of Plain-English Copying**
  - Classical info (text, photos) can be copied because reading it doesn't change it.
  - Quantum info is like a super-delicate paint that changes if you touch it. To learn the state well enough to copy it, you have to measure it, and that measurement disturbs or destroys the very details you needed to copy.





# Quantum Core Phenomena

**Randomness**

- **Quantum Mechanics Definition**

  Measurement outcomes are probabilistic:

  $$P(0) = |\alpha|^2, P(1) = |\beta|^2$$

  The Born rule connects amplitude to observable probability.

- **Physical Example**

  Measuring the polarization of a photon prepared at 45° yields random H/V outcomes—fundamentally unpredictable, not due to hidden variables.

- **Algorithmic / Practical Use**
  - **Quantum Random Number Generators (QRNGs)**: measure superposed states to get unbiased randomness.
  - Used in **Monte Carlo simulations**, **cryptographic key generation**, and **blockchain security**.

# Quantum Protocols

**Teleportation**

- **What it does**

  Move a qubit's **state** from Alice to Bob **without** sending the particle itself.

- **What you need**

  A shared pair of entangled qubits (one with Alice, one with Bob).

  A normal internet/phone line to send **2 classical bits**.

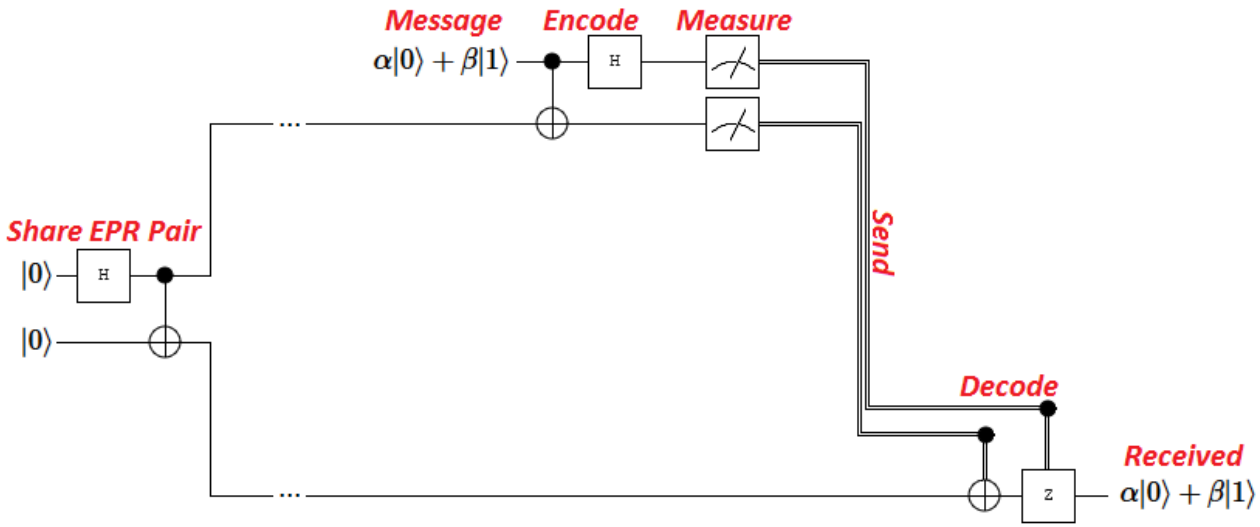
- **How it works**

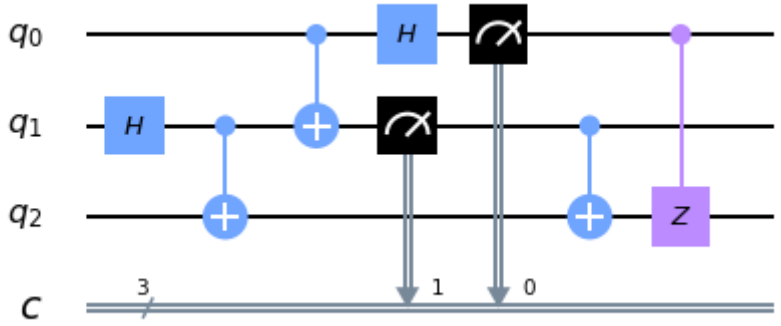
  It helps to solve the *no cloning theorem*.

# Quantum Protocols

**Teleportation**

- **Key points**
  - **No faster-than-light:** The 2 classical bits limit the speed.
  - **No copying:** Alice's original state is gone; it's **moved**, not duplicated.
  - **Why useful:** It's the basic "send-a-qubit-state" tool for **quantum networks** and **distributed quantum computing**.



# Quantum Protocols

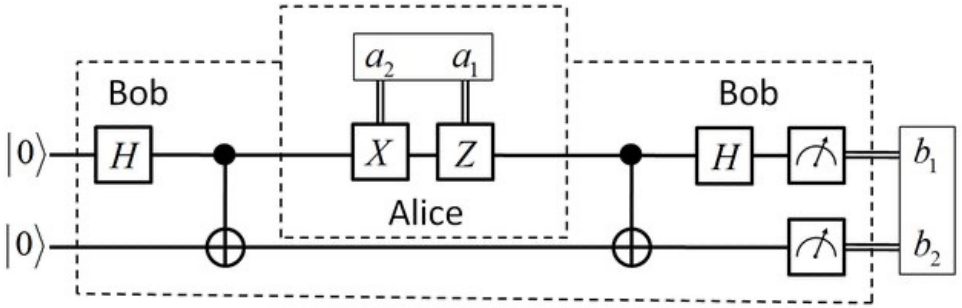
**Superdense Coding**

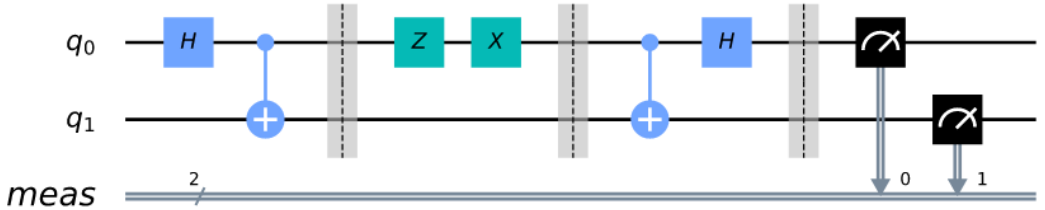
- **What it does**
  - Let Alice send **2 classical bits** of information to Bob by transmitting **only 1 qubit**
- **What you need**
  - A shared pair of **entangled qubits** (pre-shared).
  - A quantum link for Alice to **send her one qubit** to Bob.
- **How it works**
  - **Quantum Teleportation as the communication channel** to transfer information
  - **Superdense coding** to the classical information

# Quantum Protocols

**Superdense Coding**

- **Key points (remember)**
  - **The "extra capacity" comes from entanglement** shared beforehand.
  - Without that pre-shared entanglement, **1 qubit could not reliably carry 2 classical bits**.
  - **Why useful:** It shows how entanglement can **boost channel capacity** in quantum networks.



# Quantum Protocols

**Teleportation VS Superdense Coding**

| Feature | Teleportation | Superdense Coding |
|---|---|---|
| **Goal** | Send a **quantum state** | Send **two classical bits** |
| **What's sent now** | **2 classical bits** | **1 qubit** |
| **Requires** | Pre-shared entanglement | Pre-shared entanglement |
| **What arrives** | Exact qubit state | Two classical bits |
| **Why it's cool** | Move a qubit state safely | Double the info per qubit sent |

# Quantum Core Phenomena & Protocols

| Concept | Quantum Definition | Example | Algorithm / Protocol Use |
|---|---|---|---|
| **Superposition** | Linear combination of basis states | Hadamard state | H Gate |
| **Entanglement** | Non-separable multi-qubit state | EPR pairs | Teleportation, QKD, VQE |
| **Interference** | Phase-dependent amplitude addition | Double-slit, phase gates | Grover, QFT |
| **No-Cloning** | No unitary can duplicate unknown state | QKD eavesdrop test | Ensures info security |
| **Randomness** | Measurement obeys Born rule | QRNG | Cryptography, randomness |
| **Teleportation** | State transfer via entanglement + 2 bits | Teleportation | Quantum networks |
| **Superdense Coding** | Send 2 classical bits via 1 qubit | Bell-pair communication | Quantum internet links |

# Lab Experiment

Simulate **Bell State** using the **The Quantum Land**

- Explain why the Histogram show that way
- Then insert one more H gate to the circuit then explain the Histogram


Thank you!