Quantum Computing

- Lecture 1 (April 23, 2025)

- Today:
  - Admin.
  - Overview of this module

Contact Information

- Course coordinator: Prof. Jiaxin Pan
- Lecturer & TA: **Runzhi Zeng**
- Email:
  - jiaxin.pan@uni-kassel.de
  - runzhi.zeng@uni-kassel.de

- Office hours
  - Office: Room 2628
  - 2 pm – 2:30 pm, Wednesday
  - (Please send an email in advance)

- All information is available on:
  - https://runzhizeng.github.io/QC-s25/

Time

- Summer semester 2025: 23.04.2025 – 24.07.2025

- 14 Weeks: Wednesday and Thursday every week

- Lecture dates:
  - April: 23, 24, 30
  - May: ~~01~~(Labor Day), 7, 8, ~~14-15~~ (Travel), 21, 22, 28-~~29~~ (Ascension)
  - June: 4, 5, 11, 12, 18, ~~19~~(Corpus Christi), 25, 26.
  - July: 2, 3, 9, 10, 16,17, 23, 24.

Format

- Wednesday 12:00 – 13:30:
  - Two lectures (~40min each) + 10min break

- Thursday 10:00 – 12:00:
  - One lecture (~45min)
  - **Exercise and Q&A (~45min-1h)**
  - Explanation of selected exercise questions (~15min-30min)
    - I may ask you to present your solutions

- This module involves a large amounts of calculations
  - Please bring your **pen and paper (especially on Thursday!)**
  - You can also bring your laptop/iPad to check the lecture notes at any time

Resources

- Lecture notes: Will be updated at https://runzhizeng.github.io/QC-s25
- Calculation Manuscripts: Would be updated at the Moodle.

- Textbooks:
  - ***Quantum Computation and Quantum Information*** by Michael Nielsen and Isaac Chuang
  - *Linear Algebra and Learning from Data* by Gilbert Strang
  - *An Introduction to Quantum Computing* by Phillip Kaye, Raymond Laflamme, and Michele Mosca.
  - *Quantum Computing: A Gentle Introduction* by Eleanor Rieffel and Wolfgang Polak
  - ...

Resources

- Resources of other QC courses:

  (Parts of this module are based on these external course materials)

  - Quantum Computation and Information (Videos) by Prof. Ryan O'Donnell (Carnegie Mellon University)
  - Quantum Cryptography by Prof. Qipeng Liu (UC San Diego)
  - Quantum Cryptography by Prof. Mark Zhandry (Princeton University)
  - Introduction to Quantum Computing by Prof. Dakshita Khurana and Prof. Makrand Sinha (University of Illinois)
  - Introduction to Quantum Computing by Prof. Henry Yuen (Columbia University)
  - Lecture Notes of Quantum Information Science by Prof. Scott Aaronson (UT Austin)

- Miscellaneous:
  - Qubit Zoo: “Zoo” of interesting qubits and quantum gates
  - Quantum Programming (Simulated): Q# and Qiskit

Homework and Exam

- Homework: Some problem sets (notice time: 1~2 weeks).

- Exam type (Oral or written?): To be decided
- When? To be decided

What is Quantum Computing?

- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases
  - -> Quantization, introduced/explained by Planck, Einstein, ...
  - -> Quantum theory, formalized by Schrödinger, Heisenberg, Dirac...

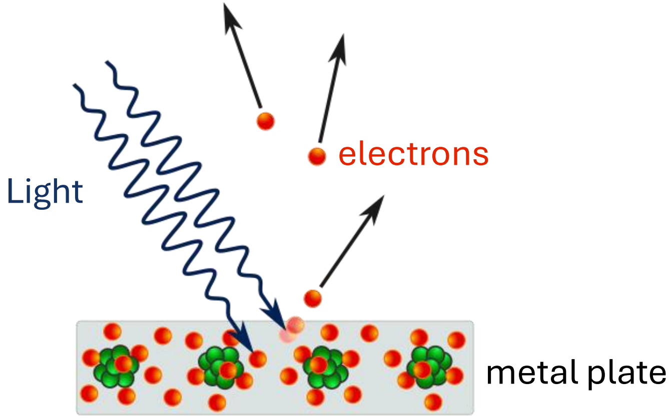
Quantum Mechanics

- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases

    Classical physics:
    "Light is **continuous wave** (with energy)
    $\Longrightarrow$ Shine light on the plate for a long time
    $\Longrightarrow$ Electrons should be emitted eventually"

Example: Photoelectric effect



(Source: Wikipedia)

Quantum Mechanics

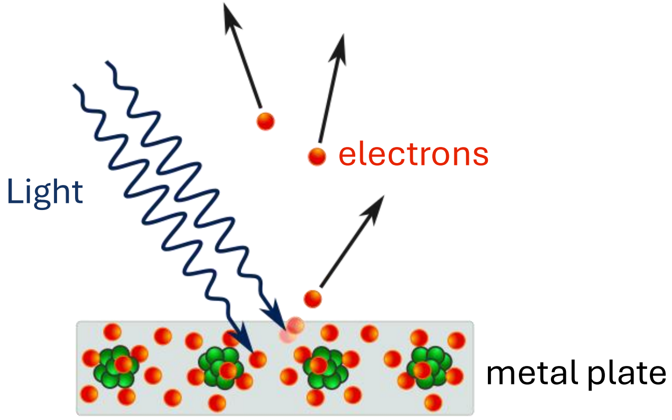
- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases

Classical physics:
"Light is **continuous wave** (with energy)
⟹ Shine light on the plate for a long time
⟹ Electrons should be emitted eventually"

Double slit experiment:
Light is a wave,
or at least it behaves like a wave
https://en.wikipedia.org/wiki/Double-slit_experiment

Example: Photoelectric effect



(Source: Wikipedia)

Quantum Mechanics

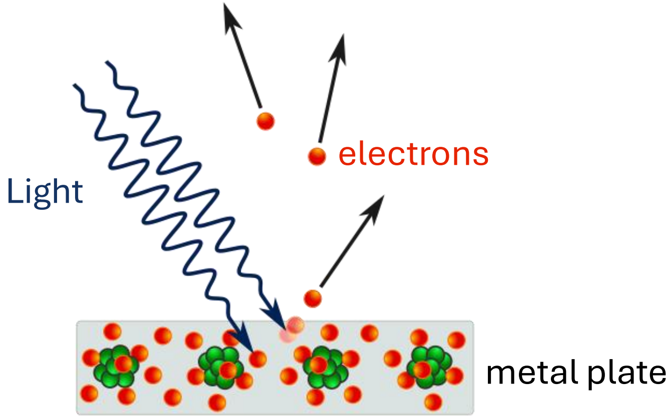
- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases

Classical physics:
"Light is **continuous wave** (with energy)
$\Rightarrow$ Shine light on the plate for a long time
$\Rightarrow$ Electrons should be emitted eventually"

Reality (Experiments):
1. There is a *threshold frequency.*
   (Electrons are emitted **only if** the light's frequency is high enough)
2. The emission of electrons is "immediately", regardless of light's intensity

Example: Photoelectric effect

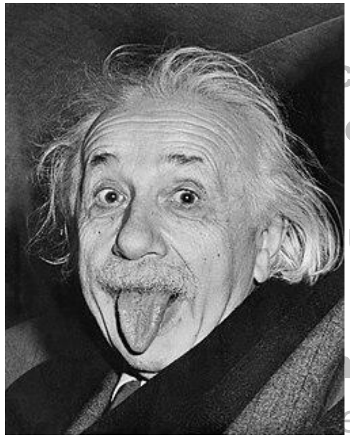


(Source: Wikipedia)

Quantum Mechanics

- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases



(Source: Wikipedia)

cs:

ous wave (with energy)

the plate for a long time

uld be emitted eventually"

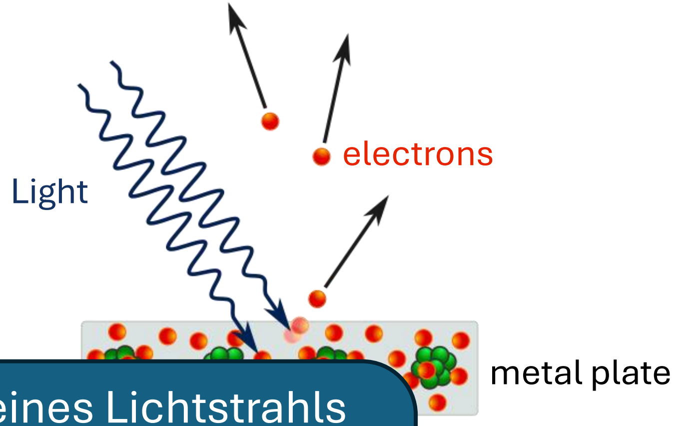
ents):

eshold fre

(Electrons are emitte

2. The emission of electro

Example: Photoelectric effect



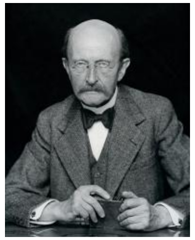
Wenn sich nämlich bei der Ausbreitung eines Lichtstrahls die Energie nicht kontinuierlich im ganzen Raum verteilt, sondern aus einzelnen, **im Raum lokalisierten Quanten besteht**, dann erklärt das diemerkwürdigen Eigenschaften der Photoelektrizität...

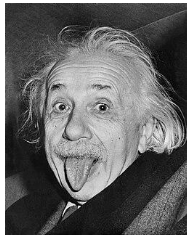
Quantum Mechanics

- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases
  - -> Quantization, introduced/explained by Planck, Einstein, ...

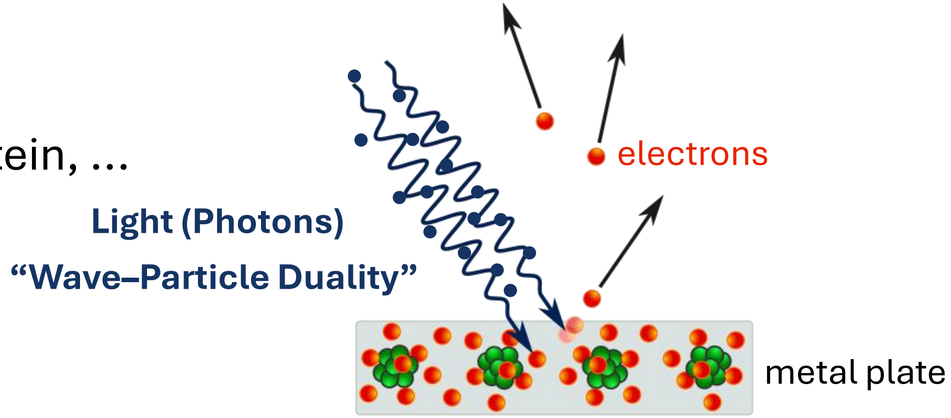
Example: $E = h \cdot v$
E: Energy of the photon
h: Planck's constant
v: Frequency of the photon





(Source: Wikipedia)

Example: Photoelectric effect

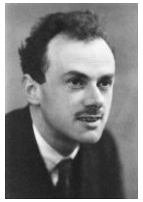


(Source: Wikipedia)

Quantum Mechanics

- Computation based on **quantum mechanics**, rather than classical physics

- **Quantum mechanics:**
  - Classical physics does not work in some cases
  - -> Quantization, introduced/explained by Planck, Einstein, …
  - -> Quantum theory, formalized by Schrödinger, Heisenberg, **Dirac**, …



$$U|\psi\rangle\langle\phi||\psi\rangle = \langle\phi|\psi\rangle U|\psi\rangle$$

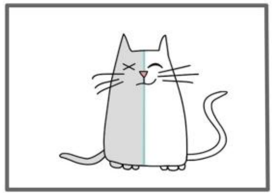
(Dirac's notation)

(Source: Wikipedia)

$$i\hbar\frac{d}{dt}|\Psi(t)\rangle = \hat{H}(\Psi(t))$$

(Schrödinger equation)

(Source: Wikipedia)



Schrödinger's Cat

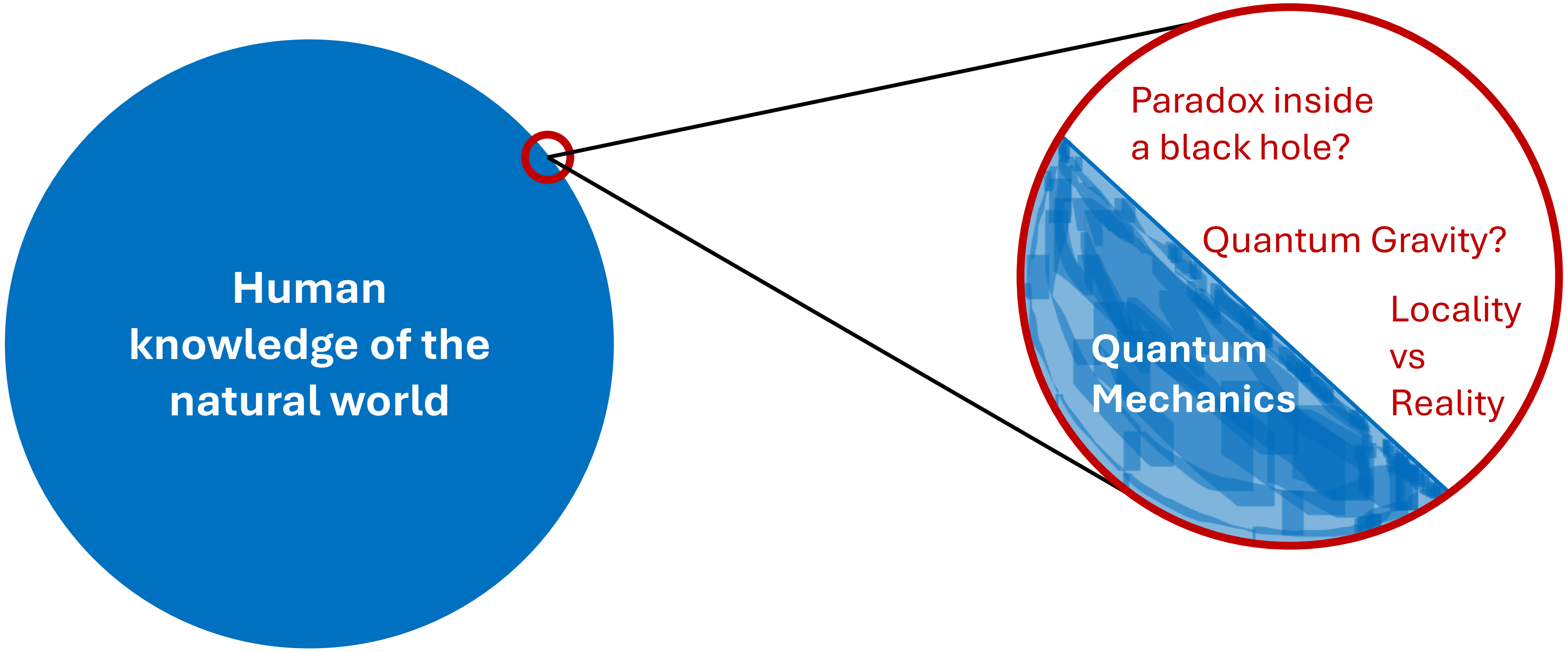
(picture from Medium)

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

(Heisenberg Uncertainty Principle)

(Source: Wikipedia)

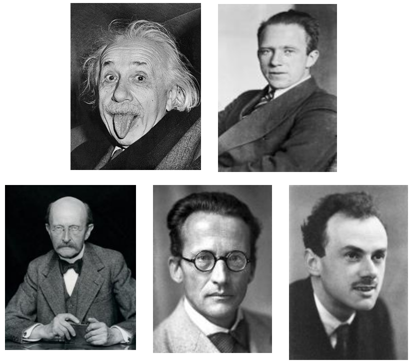
Quantum Mechanics



Quantum Computing

- Computation based on **quantum mechanics**, rather than classical physics

Quantum Mechanics



...

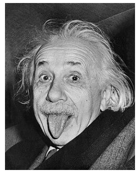
Information Theory
+ Quantum Mechanics
= Quantum Computing

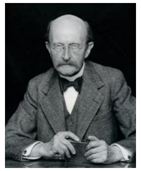
(Source of pictures: Wikipedia)

Quantum Computing

- Computation based on **quantum mechanics**, rather than classical physics

Quantum Mechanics



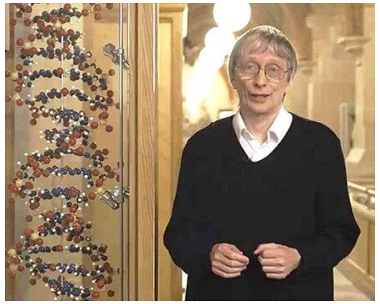


…

Information Theory
+ Quantum Mechanics
= Quantum Computing

Richard Feynman

- Simulating quantum systems with classical computers is *inefficient*
- **Quantum Systems/Computers are required**



David Deutsch

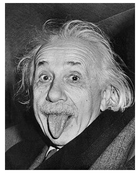
- Deutsch's algorithm, Deutsch-Jozsa algorithm
- **Quantum Turing Machine**

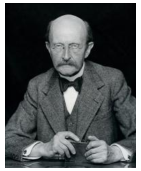
(Source of pictures: Wikipedia)

Quantum Computing

- Computation based on **quantum mechanics**, rather than classical physics

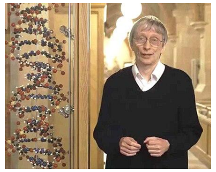
Quantum Mechanics

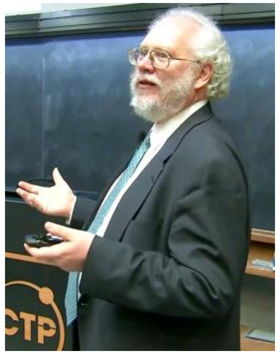




…

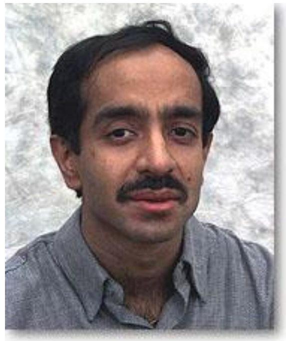
Information Theory
+ Quantum Mechanics
= Quantum Computing



Peter Williston Shor

- **Breakthrough: Shor's algorithm**
- **Break most of existing public-key cryptosystems**
- … which motivates "post-quantum cryptography"



Lov K. Grover

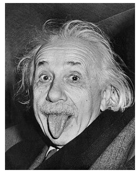
- **Grover search: A Quantum search algorithm**
- Significant impacts on information theory, computation complexity, cryptography, …

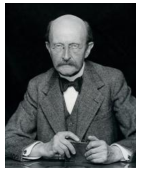
(Source of pictures: Wikipedia)

Quantum Computing

- Computation based on **quantum mechanics**, rather than classical physics

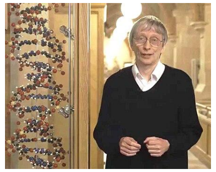
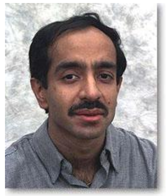
Quantum Mechanics





…

Information Theory + Quantum Mechanics = Quantum Computing


…

Advances in quantum computing

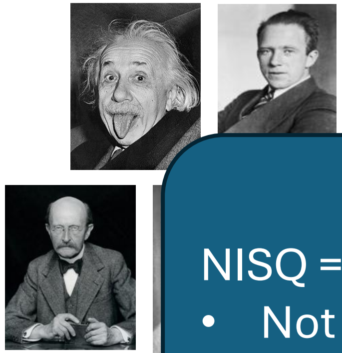
Google IBM Microsoft D:Wave intel®

(Source of pictures: Wikipedia)

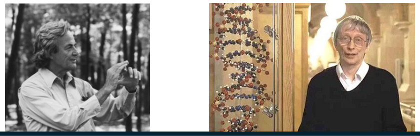
Quantum Computing

- Computation based on **quantum mechanics**, rather than classical physics

Quantum Mechanics



Information Theory + Quantum Mechanics = Quantum Computing



Advances in quantum computing

We are now in the NISQ era!

NISQ = Noisy Intermediate-Scale Quantum

- Not yet powerful enough to run Shor’s or Grover’s algorithms at scale
- But quantum hardware is **scaling up!**
- **Quantum error correction** is still needed for fault-tolerant computing

(Source of pictures: Wikipedia)

Quantum Computer vs Classical Computer

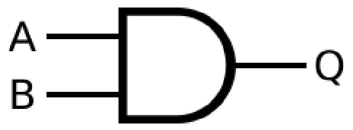
(Classical World)

(Quantum World)

Quantum Computer vs Classical Computer

Classical bit(s): **00101**
01011
10110

- **0** = Low voltage (e.g., 0V)
- **1** = High voltage (e.g., 3.3V – 5V)



Logic gate

(Classical World)

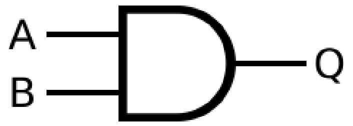
(Quantum World)

(Source of pictures: Wikipedia)

Quantum Computer vs Classical Computer

Classical bit(s): **00101**
01011
10110

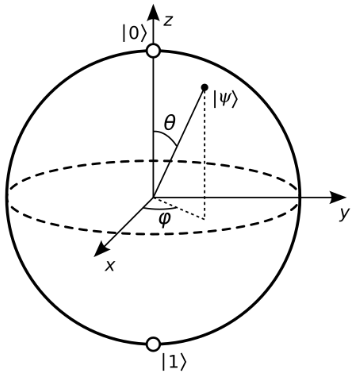
- **0** = Low voltage (e.g., 0V)
- **1** = High voltage (e.g., 3.3V – 5V)



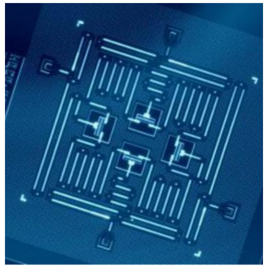
Logo gate

(Classical World)

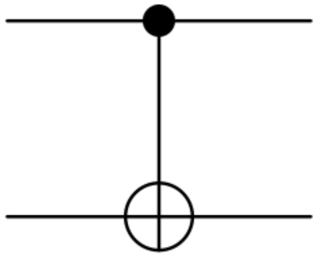
(Quantum World)



Single quantum bit **(qubit)** represented by Bloch sphere
Superposition of 0 and 1!



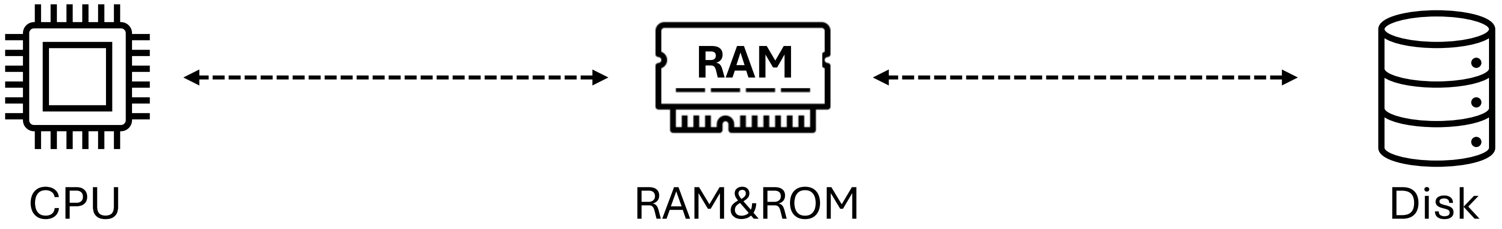
superconducting qubits (IBM)



Quantum logic gate

(Source of pictures: Wikipedia)

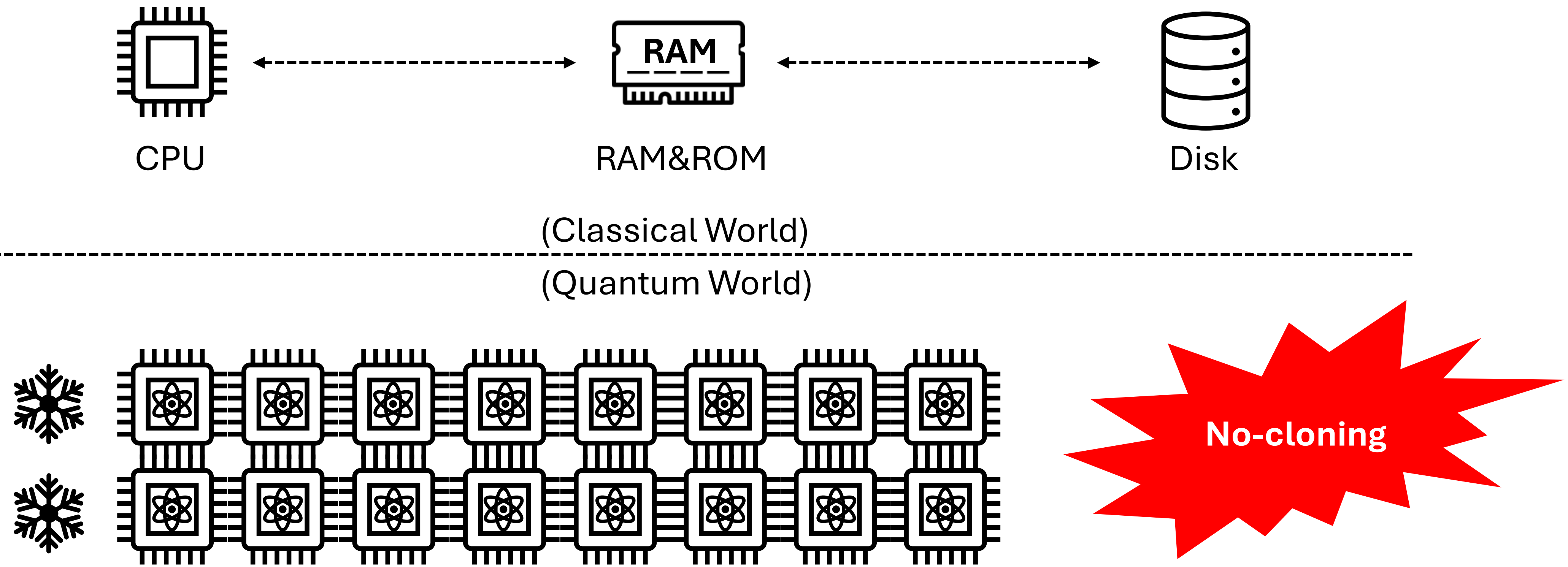
Quantum Computer vs Classical Computer



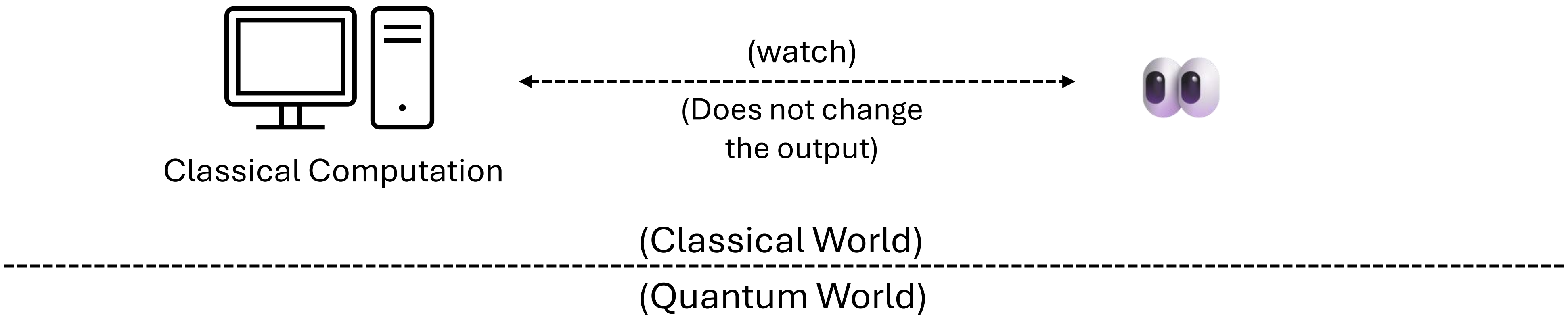
(Classical World)

(Quantum World)

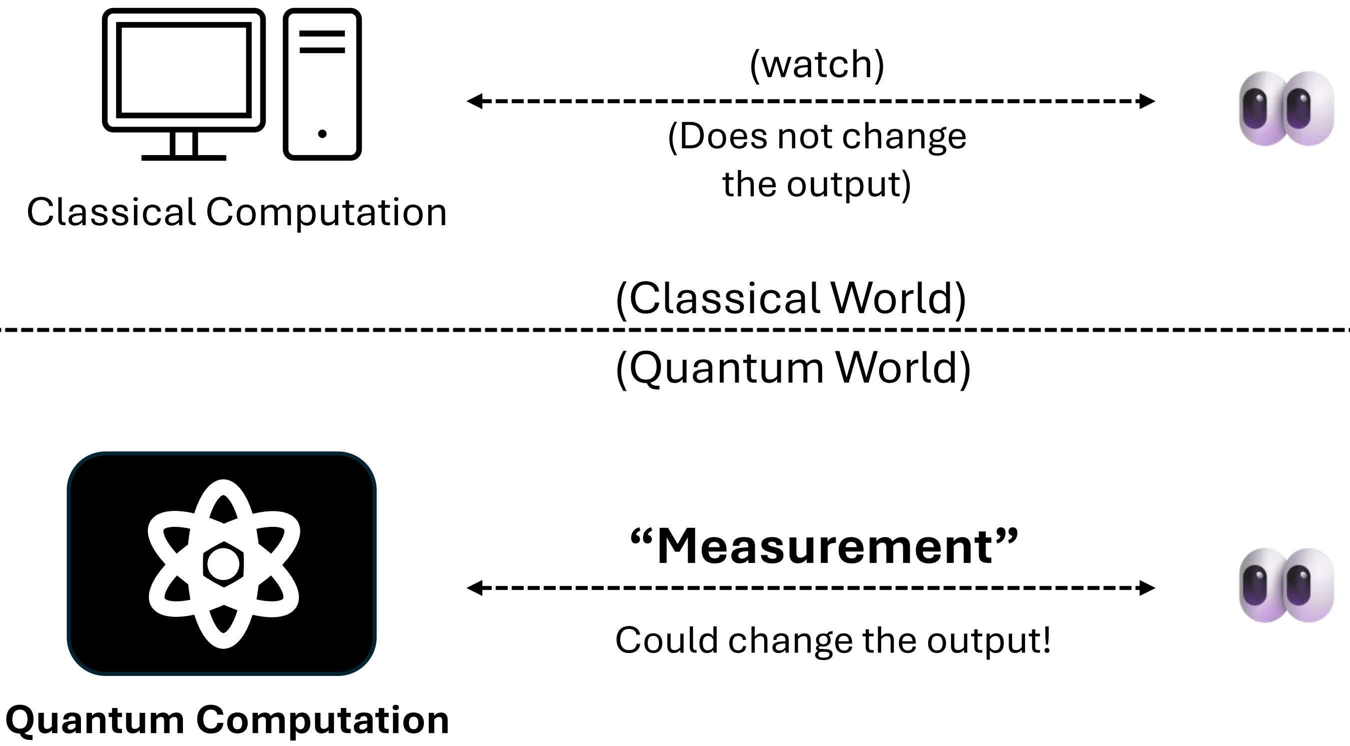
Quantum Computer vs Classical Computer



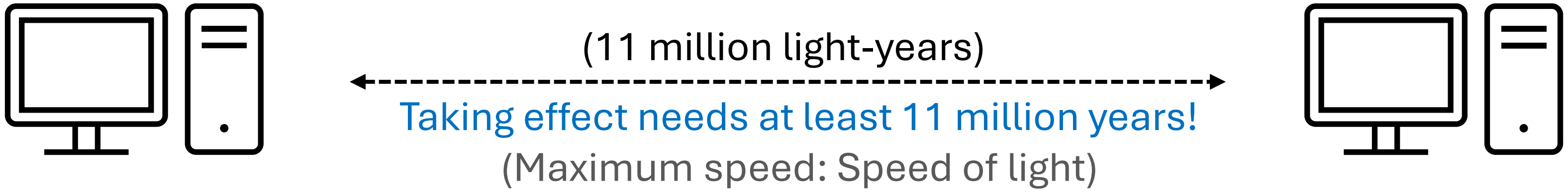
Quantum Computer vs Classical Computer



Quantum Computer vs Classical Computer



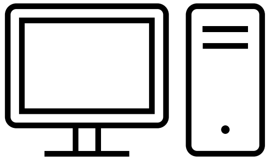
Quantum Computer vs Classical Computer



(Classical World)

(Quantum World)

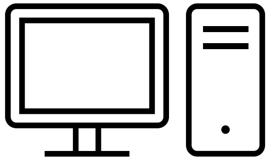
Quantum Computer vs Classical Computer



(11 million light-years)

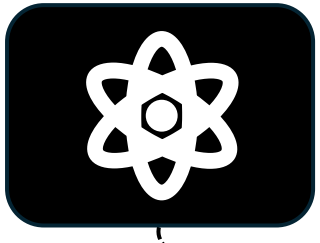
Taking effect needs at least 11 million years!

(Maximum speed: Speed of light)



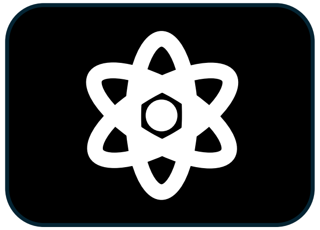
(Classical World)

(Quantum World)



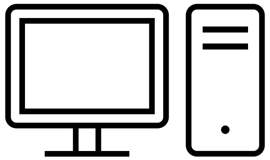
(11 million light-years)

Could “take effect” **immediately**
if they have prior **entanglement**



Entanglement

Quantum Computer vs Classical Computer

$N = pq$ $(\approx 2^{1024})$ $\longrightarrow$  $\xrightarrow{?}$ p, q

$p \neq q$ are big primes

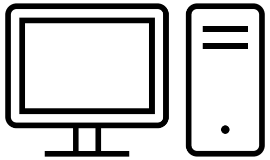
Unknown!

(Classical World)

(Quantum World)

Quantum Computer vs Classical Computer

$\boldsymbol{N = pq}$
$(\approx 2^{1024})$
$\boldsymbol{p \neq q}$ are big primes



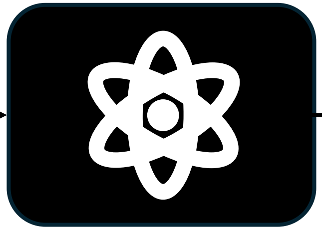
Unknown!

$\boldsymbol{p, q}$

(Classical World)

(Quantum World)

$\boldsymbol{N = pq}$
$(\approx 2^{1024})$
$\boldsymbol{p \neq q}$ are big primes



$\boldsymbol{p, q}$

Using Shor's algorithm

(Though no existing quantum computer can run this yet.)

Quantum Computer vs Classical Computer

- What makes Quantum Computing powerful?
  - Quantum **Superposition – Qubits**
  - **Unitary quantum gates** instead of logic gates
  - Quantum **Entanglement**
  - Quantum **Measurement**
  - **Quantum algorithms** utilizing quantum properties…

Impact on Computational Complexity

- **Exponential speedups for some specific problems**
  - Factoring, discrete logarithm, or more generally, hidden (finite abelian) subgroup problem
- **Polynomial speedups for generic search problems**
  - Grover search
  - Improve some lower bounds

Impact on Computational Complexity

- **Exponential speedups for some specific problems**
  - Factoring, discrete logarithm, or more generally, hidden (finite abelian) subgroup problem

- **Polynomial speedups for generic search problems**
  - Grover search
  - Improve some lower bounds

- **Quantum Computers $\neq$ More "Computable"**
  - They **cannot solve uncomputable** problems (e.g., the halting problem)

- **Quantum Computers $\neq$ Always more efficient**
  - No known advantage in many problems (e.g., Traveling Salesman Problem)

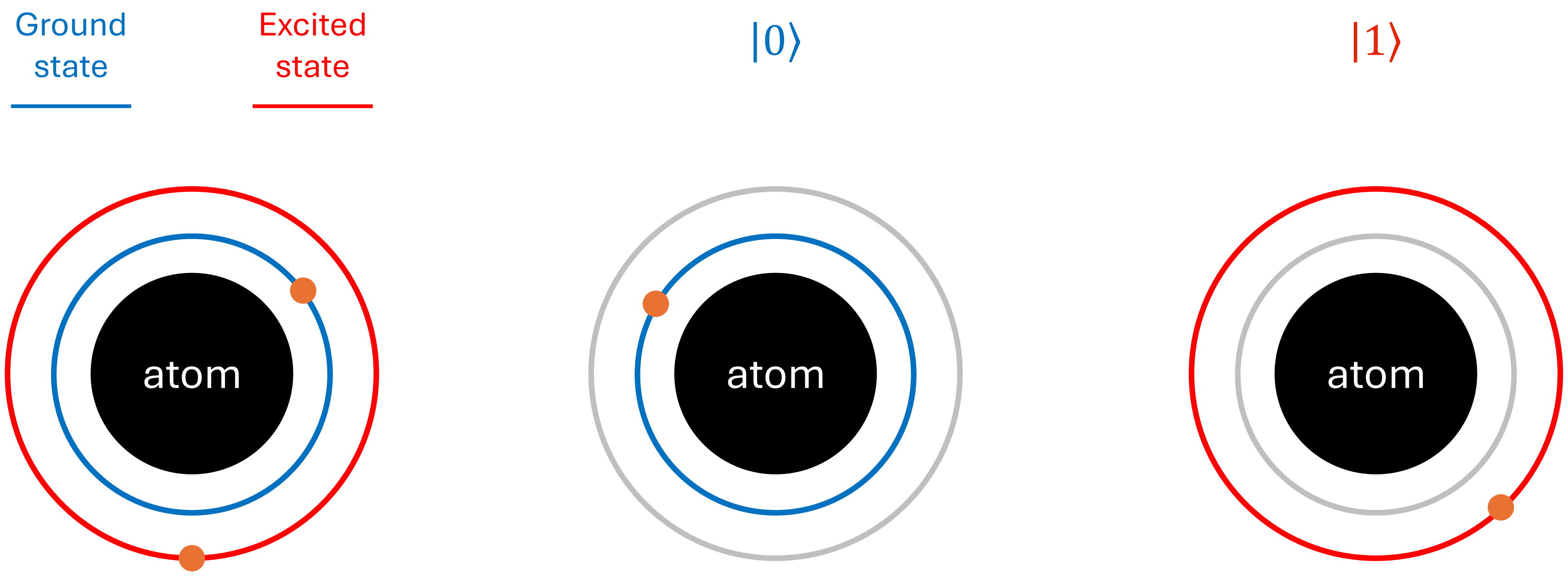
Overall Goals

- Main topics:
  - **Quantum mechanics** and its **linear algebra formulation**
  - **Entanglement and Measurement**
  - **Quantum Algorithms:**
    - Described by **quantum gates/circuits, unitaries**
    - Quantum “parallelism” – **evaluation on superposition**
    - Applications of quantum algorithms – QKD, QFT, search, …
  - **Quantum Information**
  - Quantum Programming (TBD)?

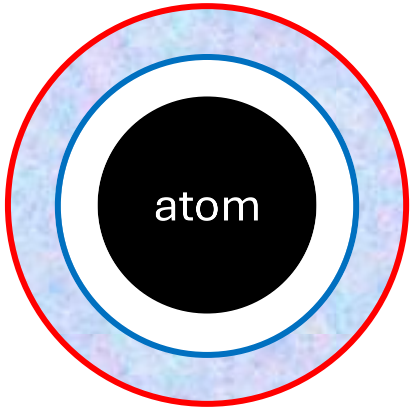
Overall Goals

- After completing this module, you should be able to:
  - **Explain** the fundamental principles of quantum computing (QC) and basic quantum mechanics.
  - **Use** the relevant linear algebra (including qubit representations and quantum gates) to formalize quantum computing notions and perform **basic calculations**.
  - **Describe and apply** quantum algorithms such as the Quantum Fourier Transform and Grover's search algorithm.
  - **Design** some simple quantum circuits/algorithms based on the algorithms you learned
  - **Read and understand** introductory research papers on quantum computing and cryptography.

Qubit and Superposition



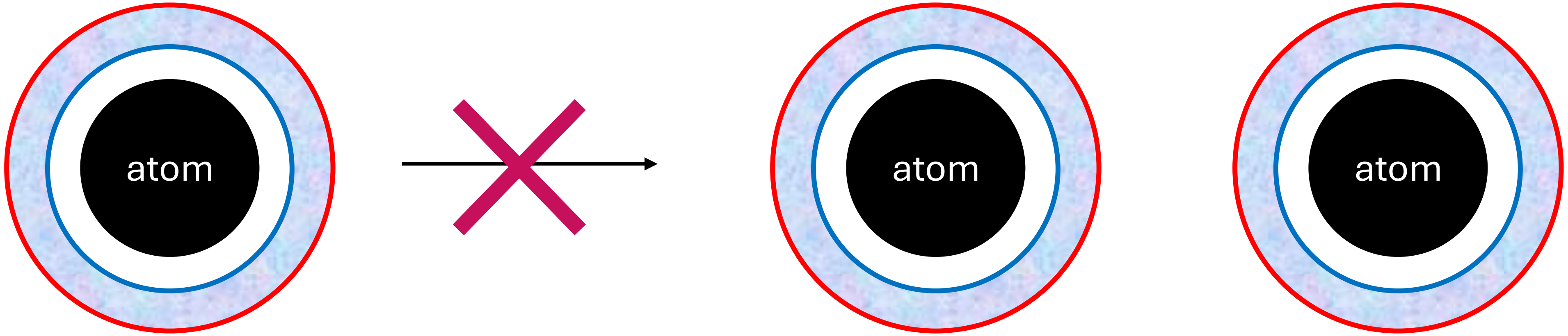
Qubit and Superposition



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

We do not know where ● is...
Or, ● is in “superposition”...

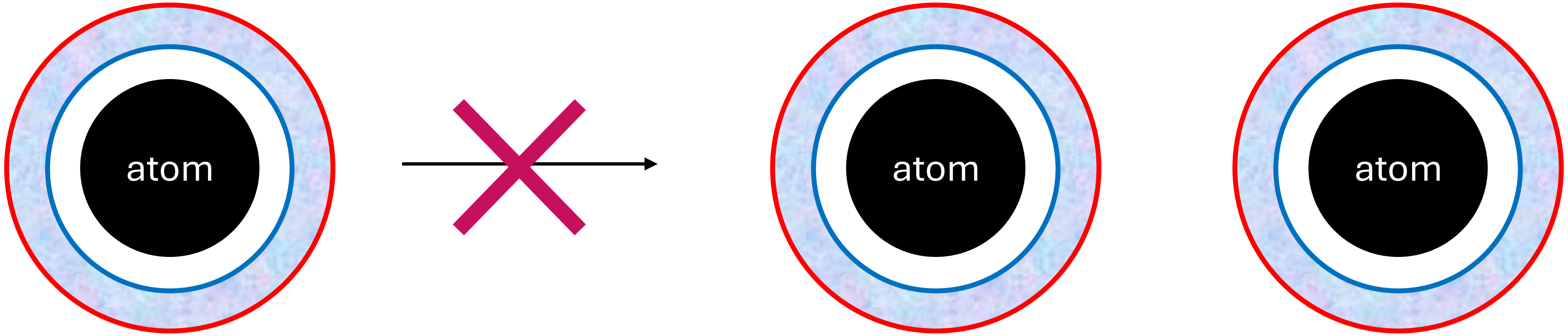
Qubit and Superposition



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

No-cloning

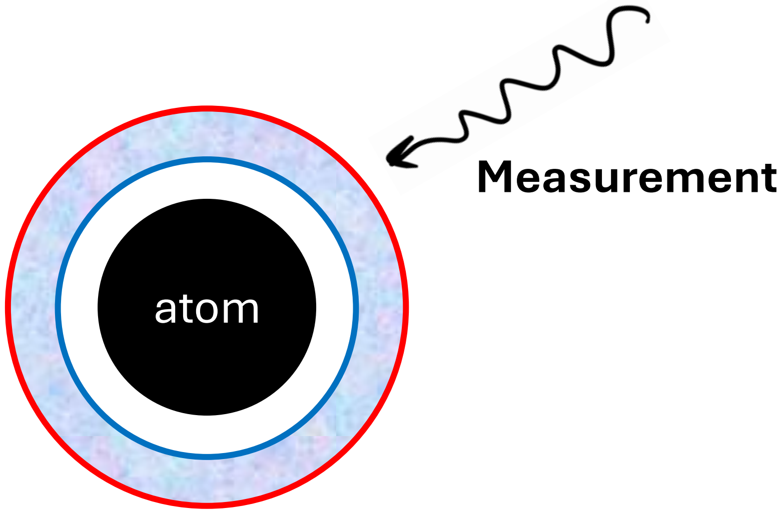
Qubit and Superposition



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

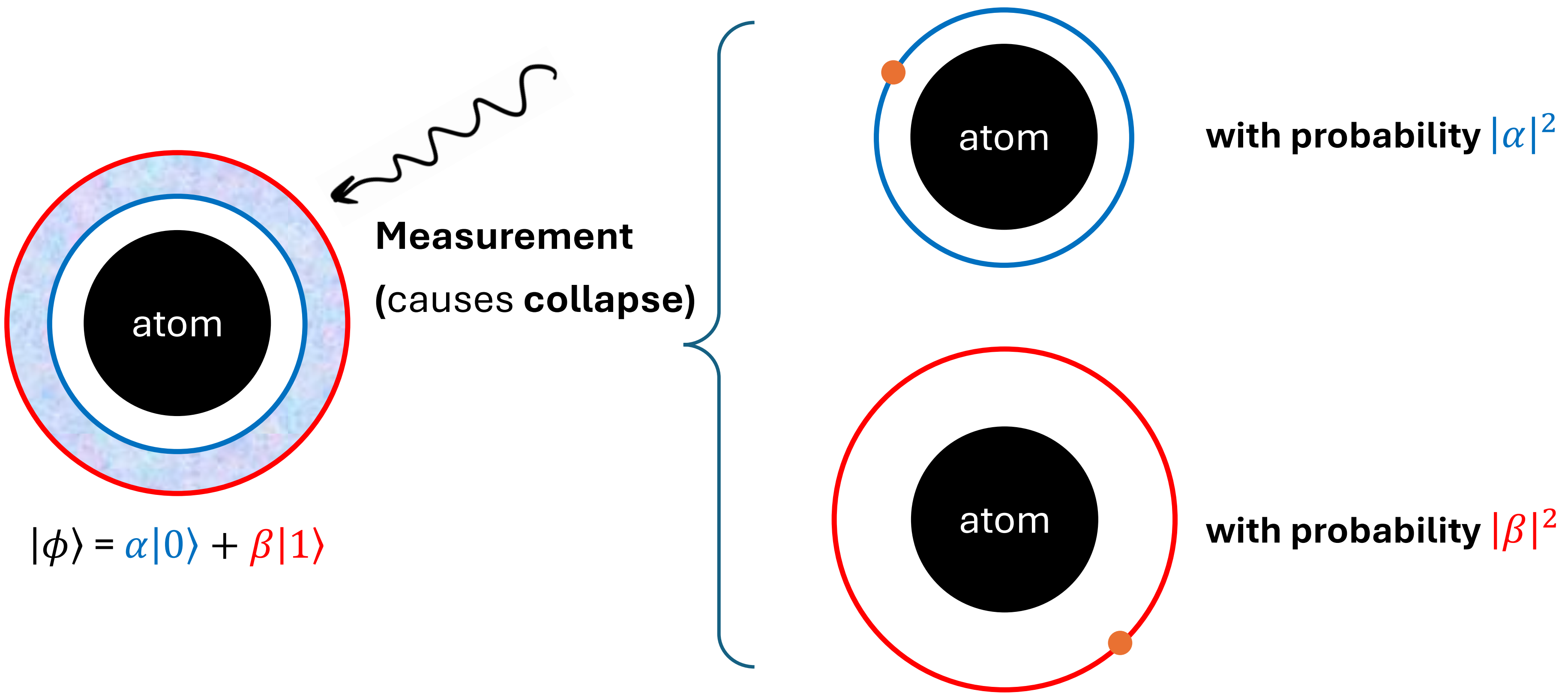
No-cloning → Quantum key distribution, quantum money, ...

Measurement

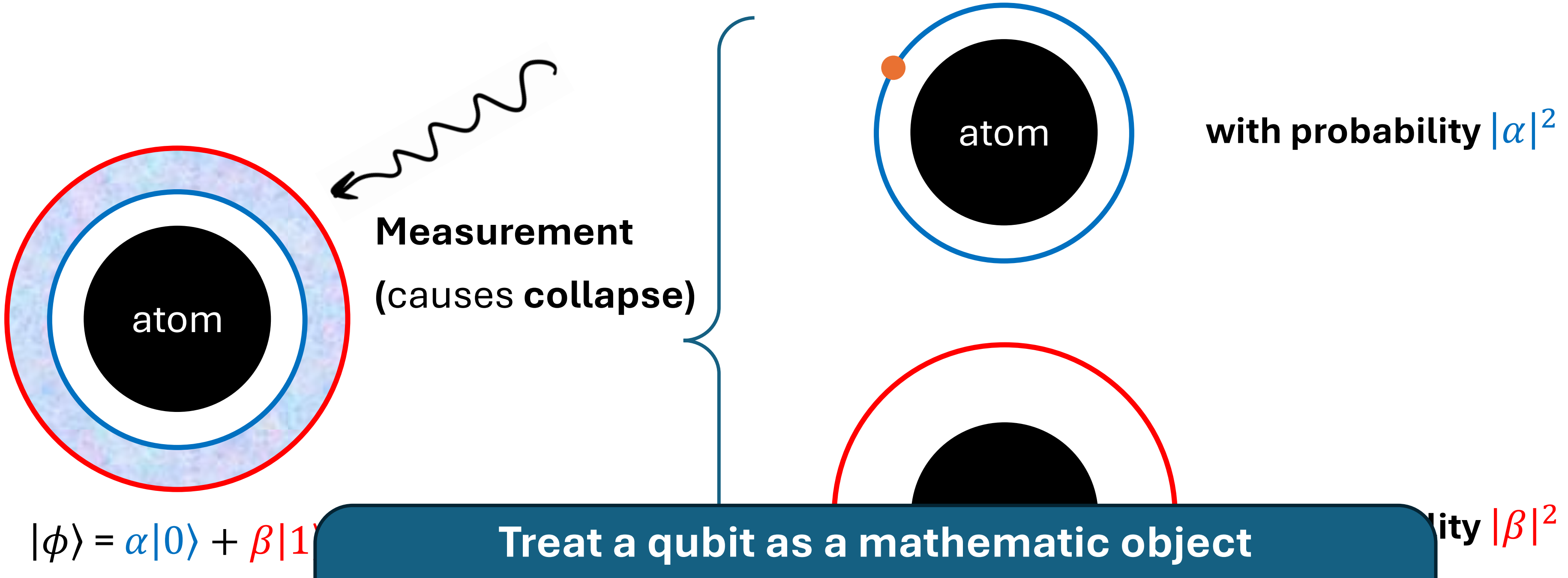


$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Measurement

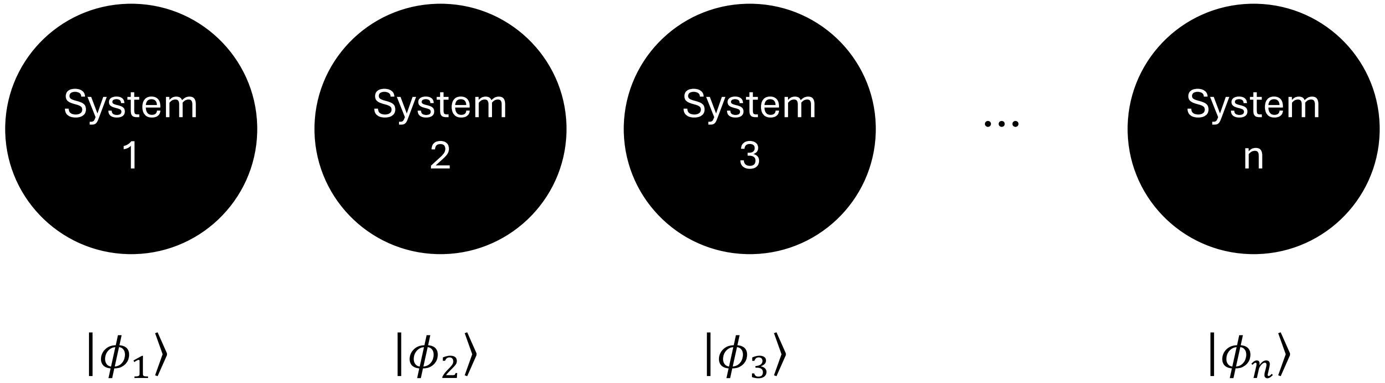


Measurement

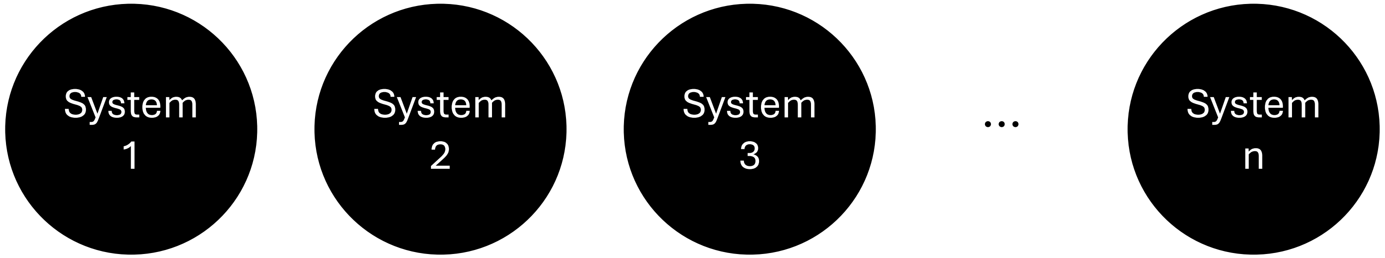


Treat a qubit as a mathematic object
(regardless of its physical meaning)
so we can focus on quantum computing
without diving into physics, philosophy, …

Multiple Qubits



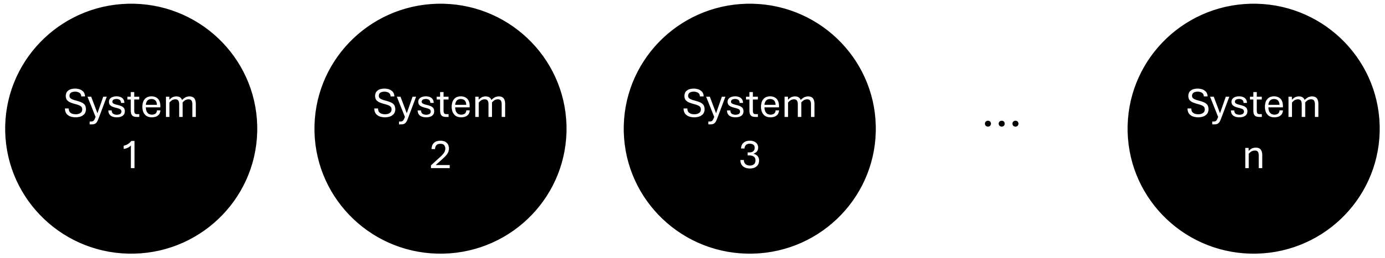
Multiple Qubits



$|\phi_1\rangle$ $|\phi_2\rangle$ $|\phi_3\rangle$ $|\phi_n\rangle$

The state of the composite system: $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle \otimes \cdots \otimes |\phi_n\rangle$, $\otimes$: Tensor product

Multiple Qubits



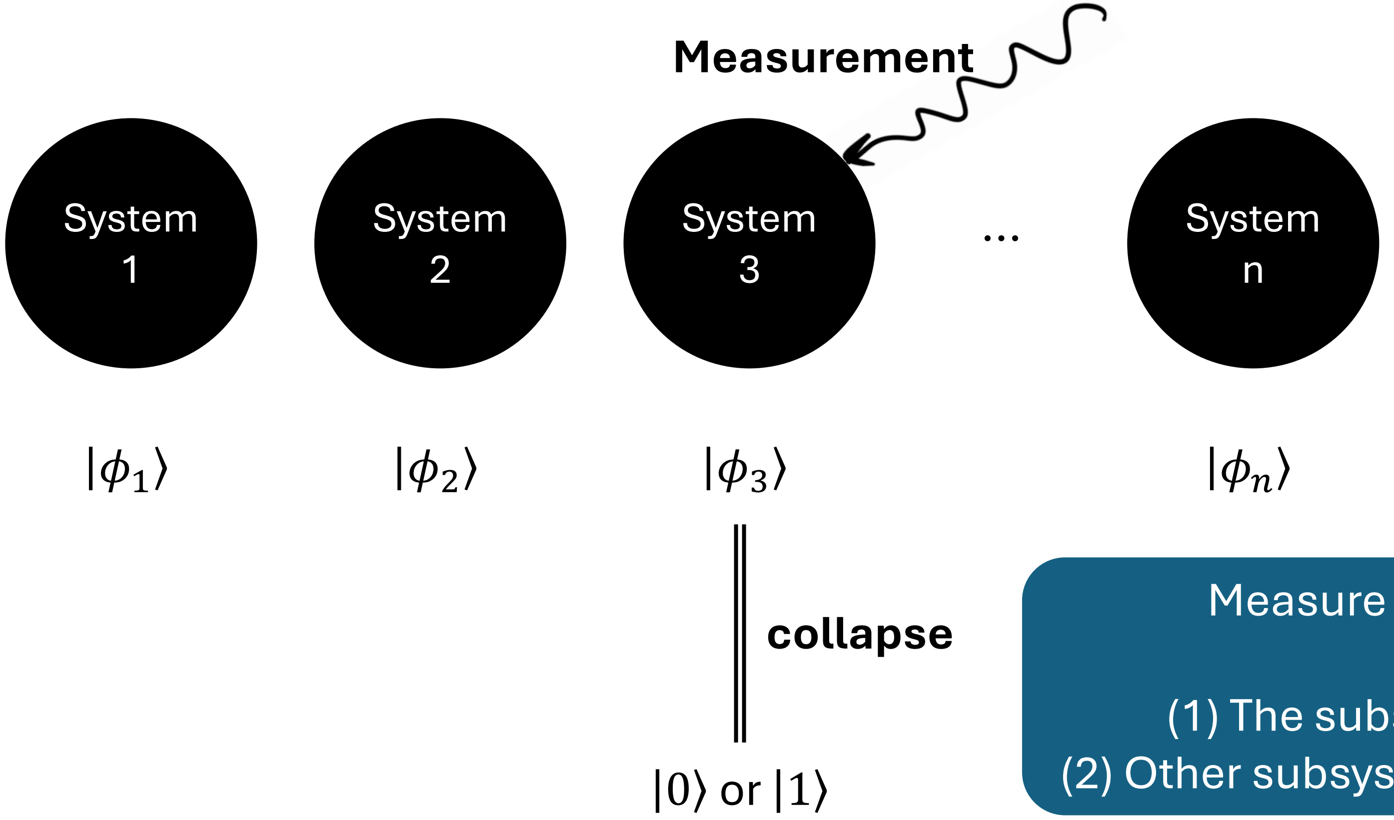
$|\phi_1\rangle$ $|\phi_2\rangle$ $|\phi_3\rangle$ $|\phi_n\rangle$

The state of the composite system: $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle \otimes \cdots \otimes |\phi_n\rangle$, $\otimes$: Tensor product

Examples: $|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |1\rangle = |0111\rangle,\ \ |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle = |10101\rangle$

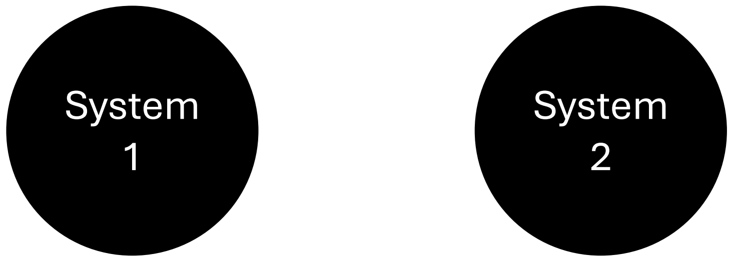
$|0\rangle \otimes |1\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) \otimes |1\rangle$, $|0\rangle \otimes |1\rangle \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |1\rangle$

Multiple Qubits



Measure one subsystem
=>
(1) The subsystem collapses
(2) Other subsystems remain the same

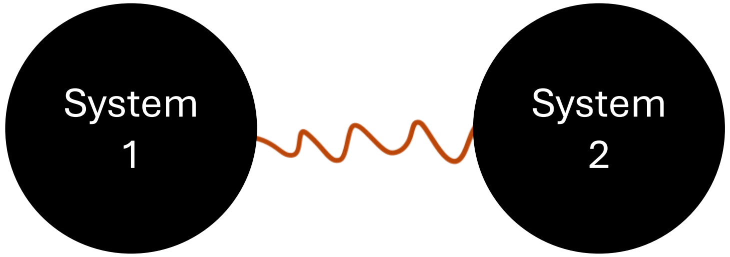
Entanglement



$|\phi_1\rangle$ $\quad\quad$ $|\phi_2\rangle$

$$|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$$

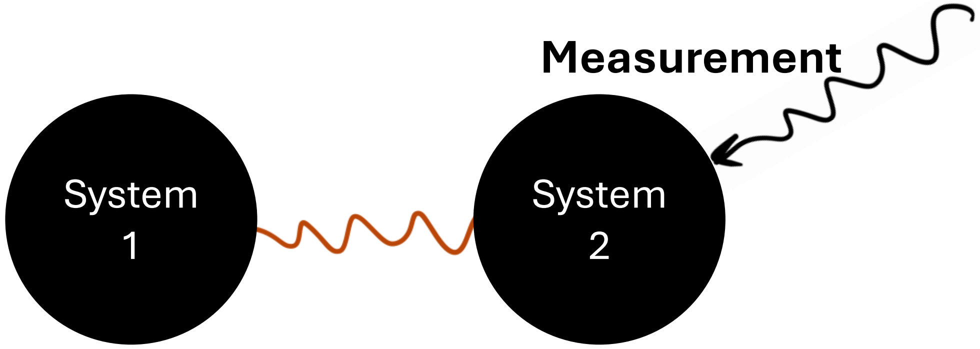
Entanglement



$$|\boldsymbol{\psi}\rangle$$

$$\cancel{|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle}$$

Entanglement



$|\psi\rangle$

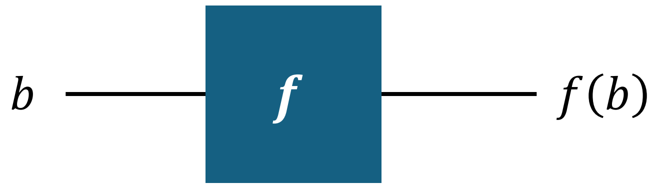
collapse

some basic state

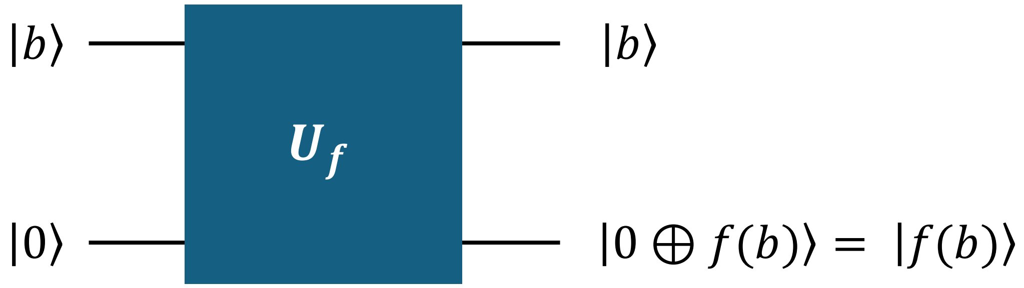
Measure one subsystem
=>
The whole system collapses

Unitaries and Superposition Evaluation

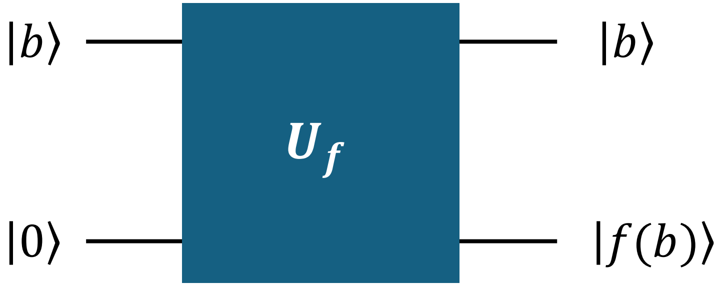
Let $f:\{0,1\} \to \{0,1\}$ be a classical bit function:



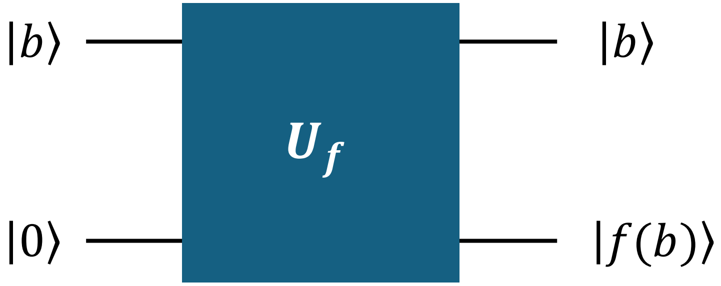
The "quantum version" of f:

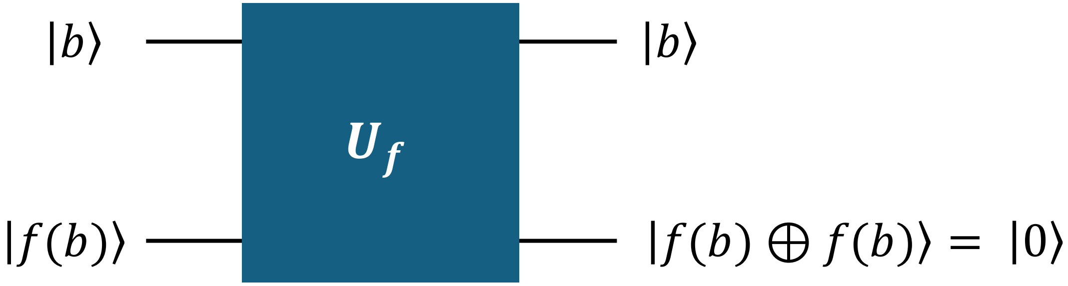


Unitaries and Superposition Evaluation



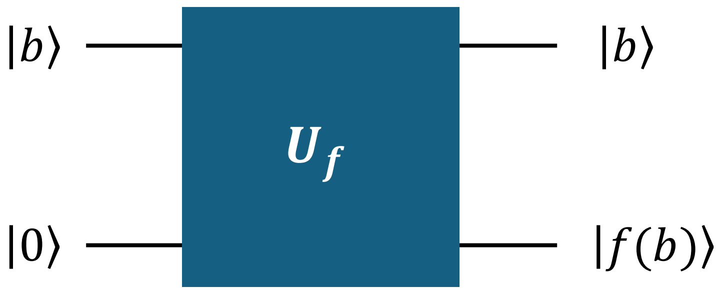
Unitaries and Superposition Evaluation

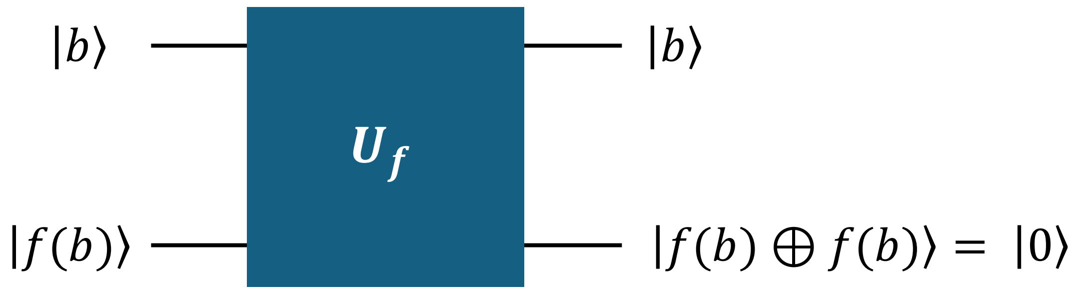


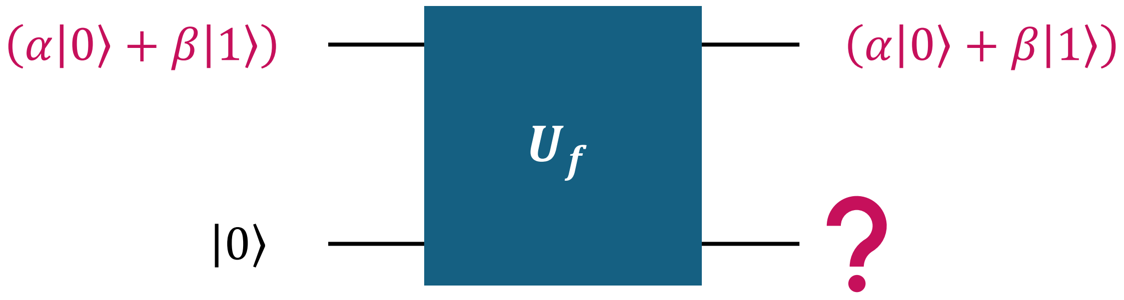


Reversible Computation

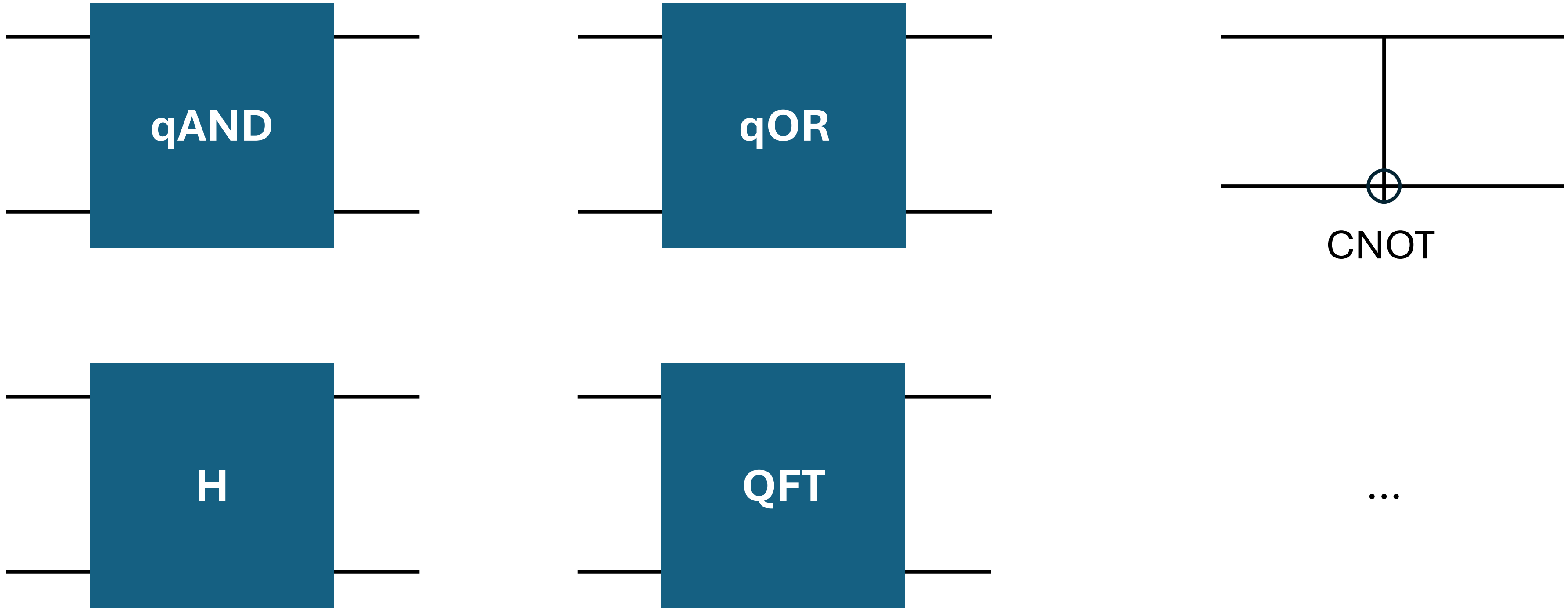
Unitaries and Superposition Evaluation



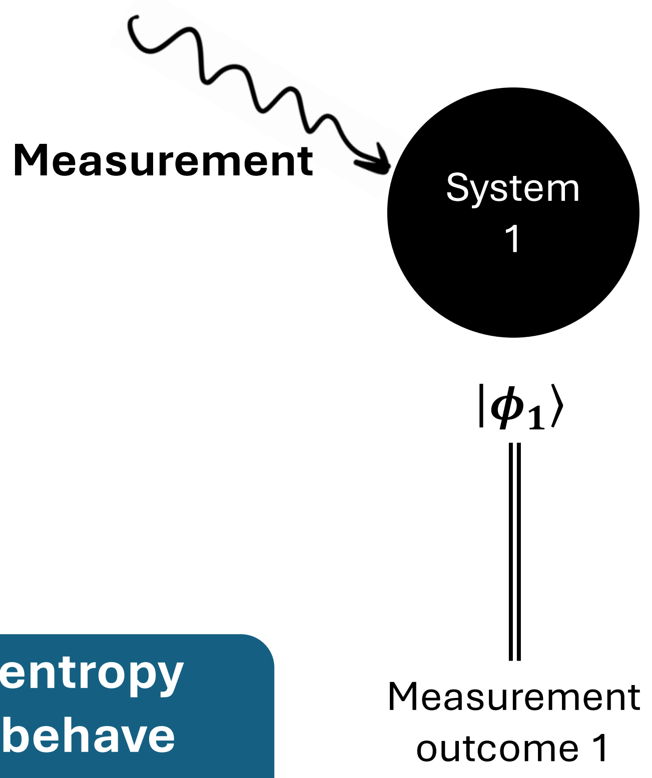




Quantum Gates and Algorithms



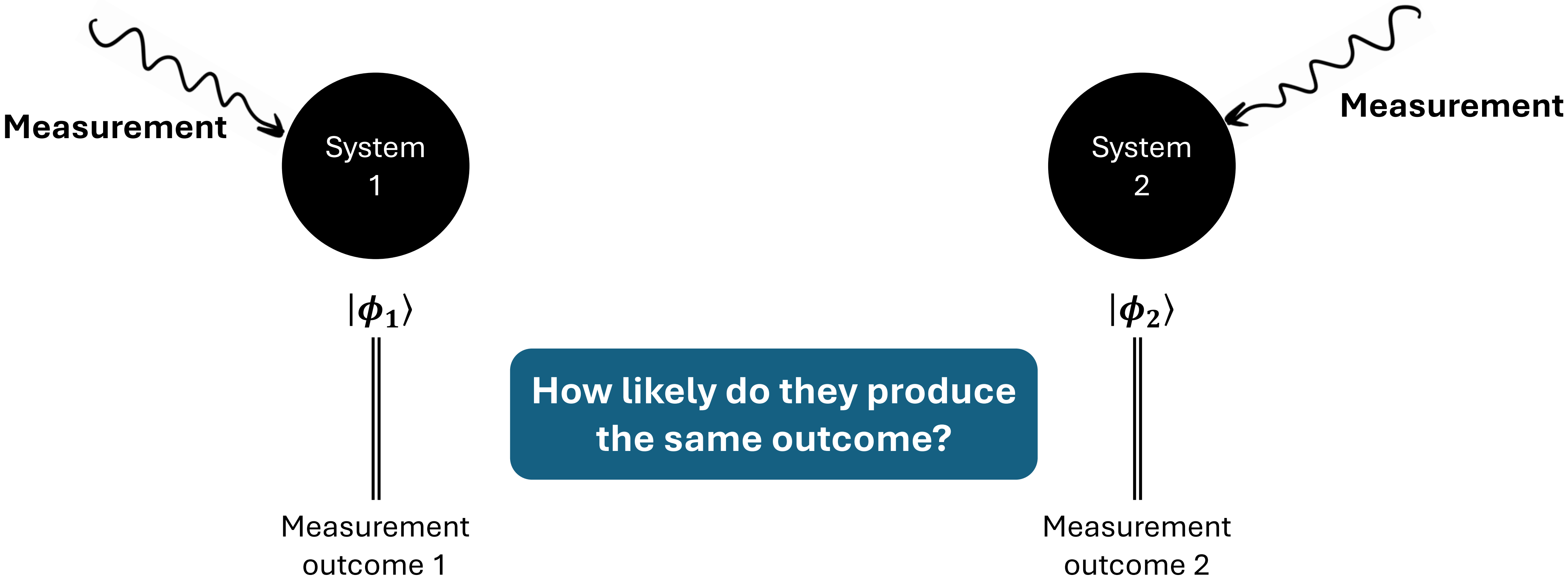
Quantum Information – Entropy and Randomness



How does the entropy of the system behave after measurement?

How much "randomness" does it provide?

Quantum Information - Distinguishability



Thursday’s Topic

- Quantum state, qubit, and their linear algebra formulation

- Bring your **pen** and **paper**