An Engineering Perspective on the Quantum Optical Communications and Sensing

Dr. Kwang-Cheng Chen, IEEE Fellow
Professor of Electrical Engineering
University of South Florida
Email: kwangcheng@usf.edu

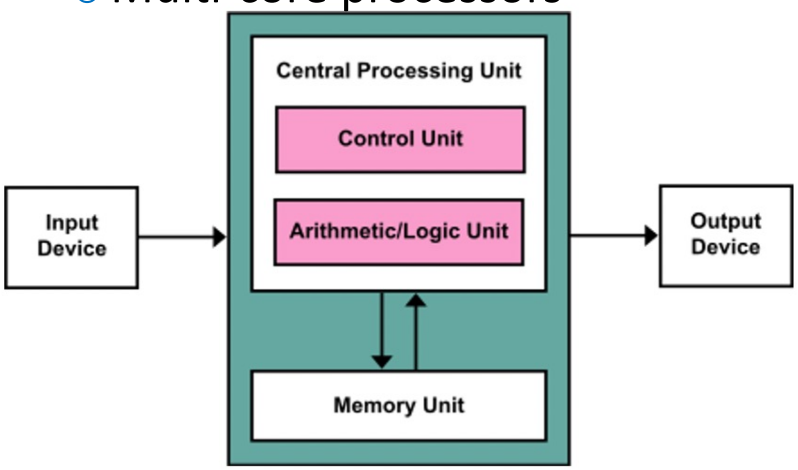
Quantum Supremacy

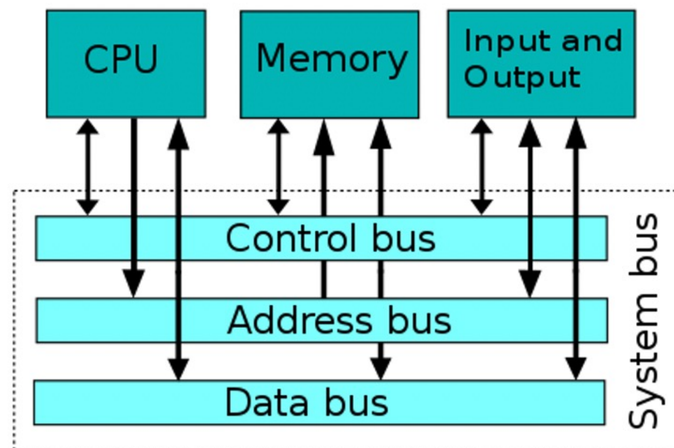
Extreme parallelism due to quantum mechanics' tensor product in Hilbert space

Absolute security due to quantum no-cloning theorem

Classic Computer Architecture: Von Neumann Machine

- Reduced Instruction Set Computer (RISC)
  - ARM (and also MIPS) processors
    - Apple M1 and series A processors
  - Multi-core processors
- INTEL x86
  - Microarchitecture for multi-core processors





Quantum computers take a different way

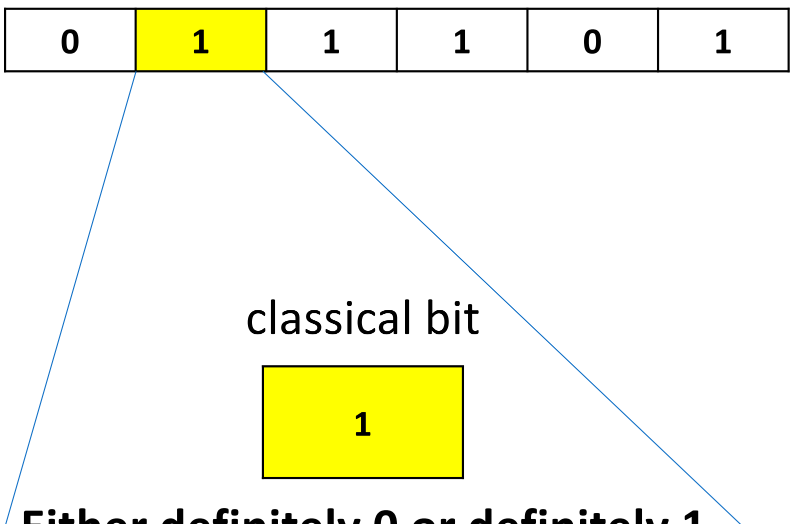
- *It's not a Turing machine, but a machine of a different kind.* Richard P. Feynman, 1981

- Quantum physics grow exponentially

$O(2^{3N})$	
number of particles	number of computer operations
1	8
2	64
3	512
10	1,073,741,824
100	10^{90}
1,000	10^{903}
1,000,000	$10^{903,090}$
10^{23} (approaching realistic)	$10^{100,000,000,000,000,000,000,000}$

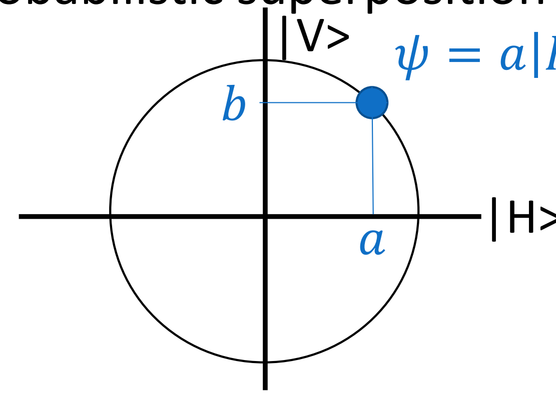
Classic Computer vs. Quantum Computer

- Classic computers are deterministic



Either definitely 0 or definitely 1

- Quantum computers take advantage of quantum states, in probabilistic superposition



$$\psi = a|H> \ +b|V>$$

  - A qubit is not definitely ↑ or ↓ but a *superposition,* while *a* and *b* are complex
  - Measurement gives
    - probability of |H> (0) is $|a|^2$
    - probability of |V> (1) is $|b|^2$

Quantum Supremacy in Mathematical Concept

- Classic world in vector space
  - Direct sum of matrices, $\boldsymbol{A}, \boldsymbol{B}$

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

  - Dimension of direct sum is the sum of dimensions, $m + n$
- Hilbert space, complete infinite-dimension inner-product space

- Quantum world in Hilbert space
  - Outer product of matrices, dimension mn

$$A \otimes B = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}.$$

Quantum supremacy in computing and communications

- Highly Parallel
  - 64-bit classic computer, one instruction per cycle
    - NP-hard problems, such as traveling salesman problem
  - 64-qubit quantum computer
    - Explore $2^{64} \approx 1.84 \times 10^{19}$ quantum states
    - Translate NP-hard problems into the complexity of $O(n)$ or $O(1)$
    - For example, modern public key cryptography is not longer secure based on the quantum algorithm
    - Post-quantum cryptography
- Extreme Security
  - A quantum state can NOT be measured, cloned nor copied, without destroying the information ➔ perfect security

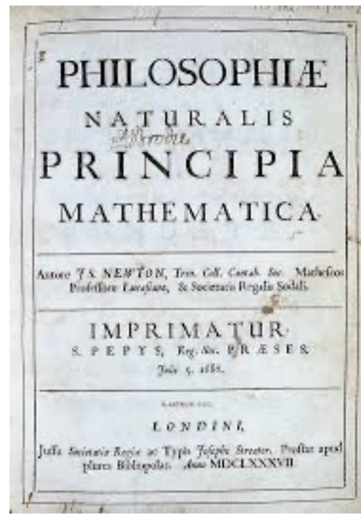
A short tour of Nobel Prizes in Physics

From Classic Physics to Quantum Mechanics

From macroscopic world to microscopic world, while many phenomenon in quantum world violate our intuition (everything is based on mathematical derivations and measurements)

Classic Physics

- Everything in modern physics must start from classic physics, primarily thank Sir Newton during the pandemics.
  - Mechanics
    - $F = ma$
  - Optics
  - Calculus
- Maxwell equations
  - Electromagnetics
    - Concept of fields
    - Birth of EE
- Thermodynamics

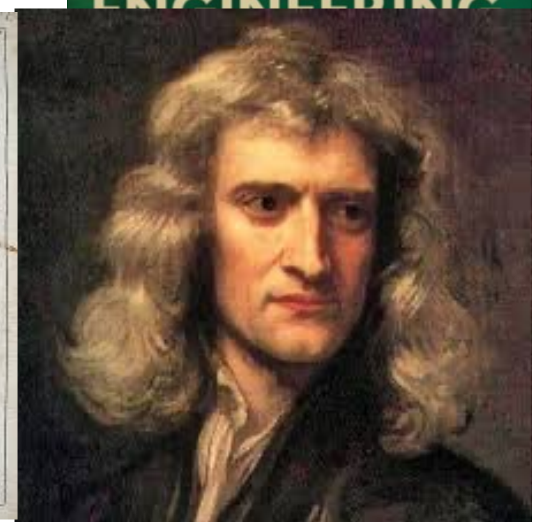


PHILOSOPHIÆ
NATURALIS
PRINCIPIA
MATHEMATICA.

Autore JS. NEWTON, Trin. Coll. Cantab. Soc. Matheseos Professore Lucasiano, & Societatis Regalis Sodali.

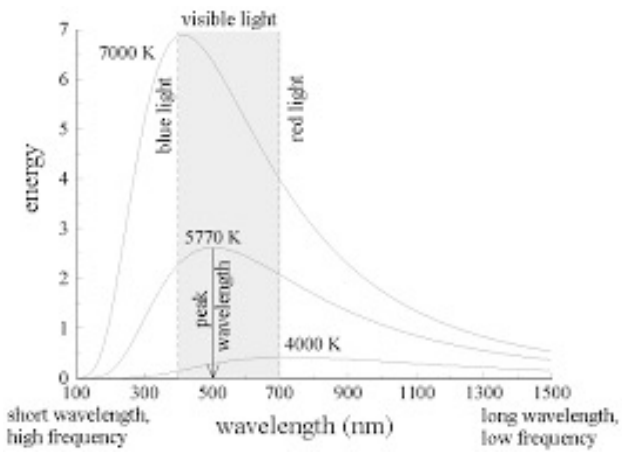
IMPRIMATUR.
S. PEPYS, Reg. Soc. PRÆSES.
Julii 5. 1686.

LONDINI,
Jussu Societatis Regiæ ac Typis Josephi Streater. Prostat apud plures Bibliopolas. Anno MDCLXXXVII.



Three Dilemmas of Classical Physics

- Blackbody radiation

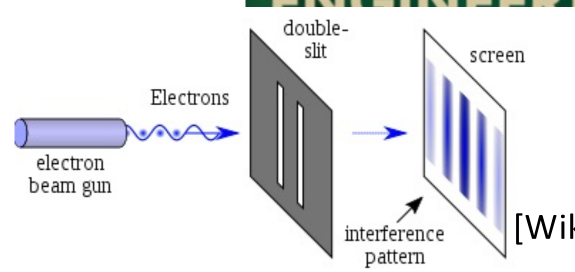


https://physics.weber.edu/carroll/honors/failures.htm

- Max Planck proposed quantum,
  - a clump of energy $E = hf$
    - or, the energy equals to its multiple

- Photoelectronic effect
  - When light shines on the surface of a metallic substance, electrons in the metal absorb the energy of the light and they can escape from the metal's surface. (Einstein's Nobel Prize)
    - classical physicists expected that when using very dim light, it would take some time for enough light energy to build up to eject an electron from a metallic surface.
    - Experiments show that if light of a certain frequency can eject electrons from a metal, it makes no difference for the strength the light. There is never a time delay.
- Hydrogen atom
  - Niels Bohr

Modern Physics



[Wikipedia]

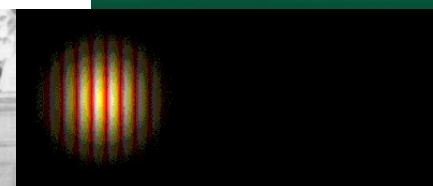
$$-\frac{\hbar^2}{2m}\nabla^2\psi + V\psi = E\psi$$

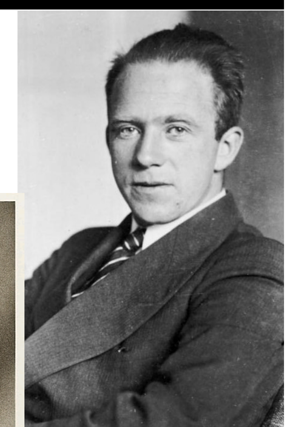
- Photon and its wave-particle duality
- Uncertainty principle
- Schroedinger equation
  - ψ represents a probability distribution.
- Schroedinger's cat
  - Copenhagen interpretation of quantum superstition
  - Einstein, Podolsky, Rosen (EPR paradox, incompleteness of quantum mechanics)
- Bell's Theorem
  - to resolve the incompleteness of quantum mechanics, locality, by Bell's inequality
  - The Bell states are a form of entangled and normalized basis vectors in Hilbert space.
- Quantum entanglement

ENGINEERING
UNIVERSITY OF SOUTH FLORIDA

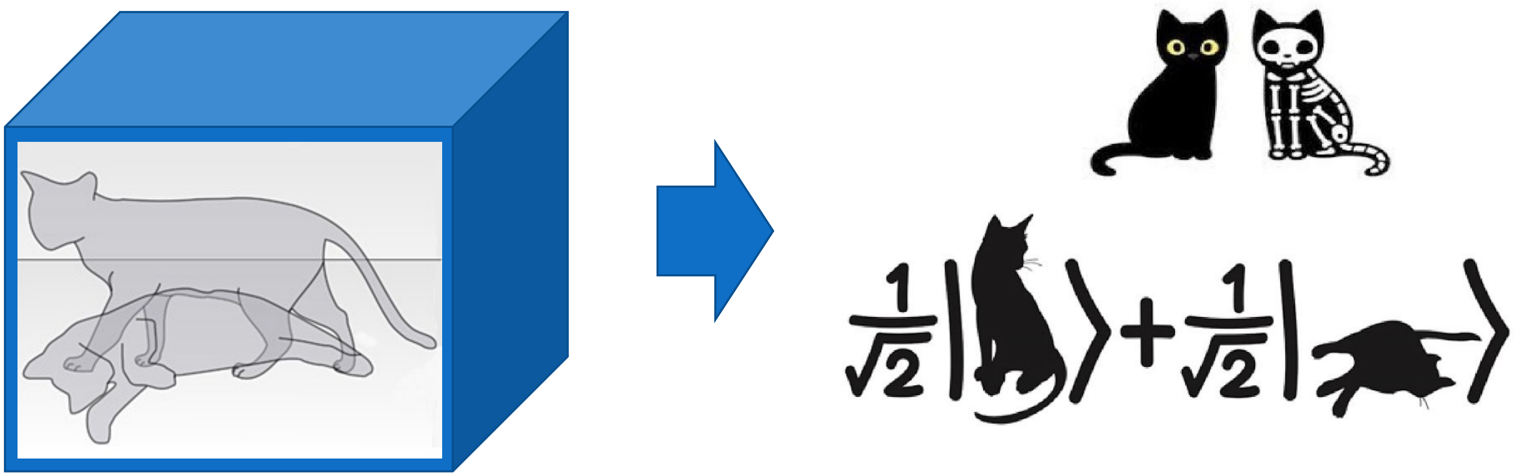
Early Milestones of Quantum Mechanics

- Louis de Broglie
  - PhD Dissertation in 1924 (32 years old) introduced the theory of electron waves
  - Matter and wave-particle duality
  - $mc^2 = hv$
- Werner Heisenberg
  - Uncertainty principle
  - $\sigma_x \sigma_p \geq \hbar/2$
- Erwin Schrodinger
  - Wave mechanics





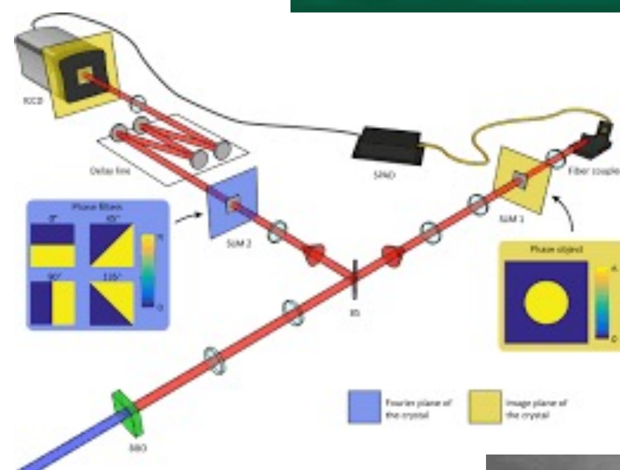
Schröedinger's Cat

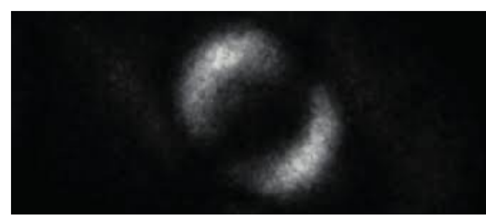


A philosophy question leads to a science leap.
Einstein: God does not play a dice!

Quantum Entanglement

- Quantum entanglement occurs when a pair of a group of particles is generated, and the quantum states of these particles can not be described independently even when they are separated in long distance.
    - Particles A and B are entangled. The measurement for the quantum state of particle A can be highly correlated with measurement for particle B, even they are separated by a large distance, e.g. 300,000 km. (spooky in Einstein's word)
        - Does it imply communication in no time? Mental communication?
    - It totally violates what we understood in classic physics.
    - The incompleteness of quantum mechanics raised by EPR paper was resolved by John Bell in 1964.



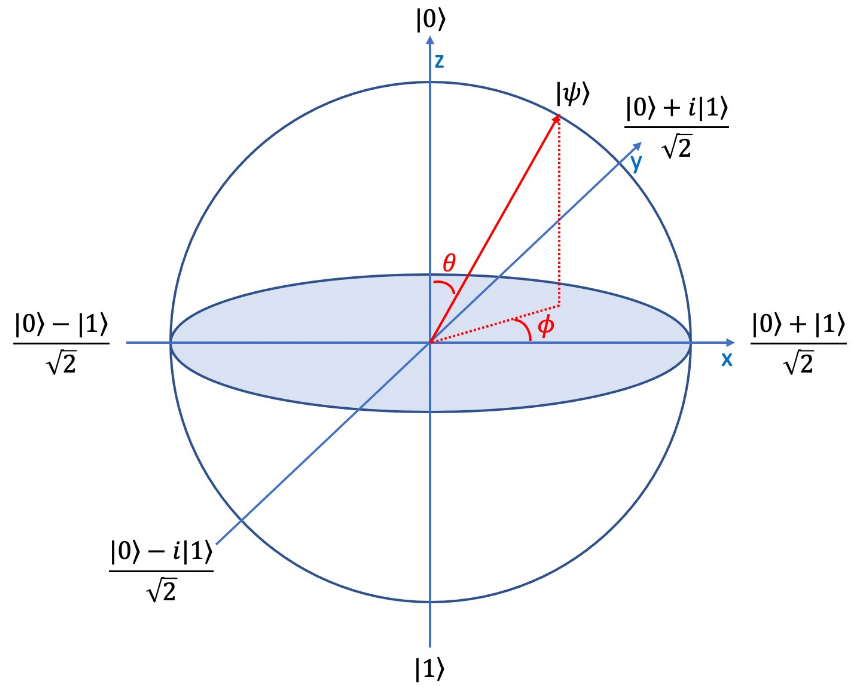


From Quantum Physics to Quantum Computing and Communications

A minimum theoretical approach

A Binary Quantum System

- Denote ψ as the state of a quantum system with binary bases
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
- Born's rule: the sum of squares of the amplitudes of all possible states in the superposition is equal to 1
$$|\alpha|^2 + |\beta|^2 = 1$$
- Two optical polarization modes are widely considered to form the quantum states due to the precision in implementation
$$|\rightarrow\rangle\,, |\uparrow\rangle$$
- A unitary quantum state can be any point on the Bloch sphere, fundamentally different from the classic systems.



Bloch Sphere

Qubit and Logic Operations

- We can define a qubit in the 2-D complex Hilbert space using the computational basis $\{|0\rangle, |1\rangle\}$

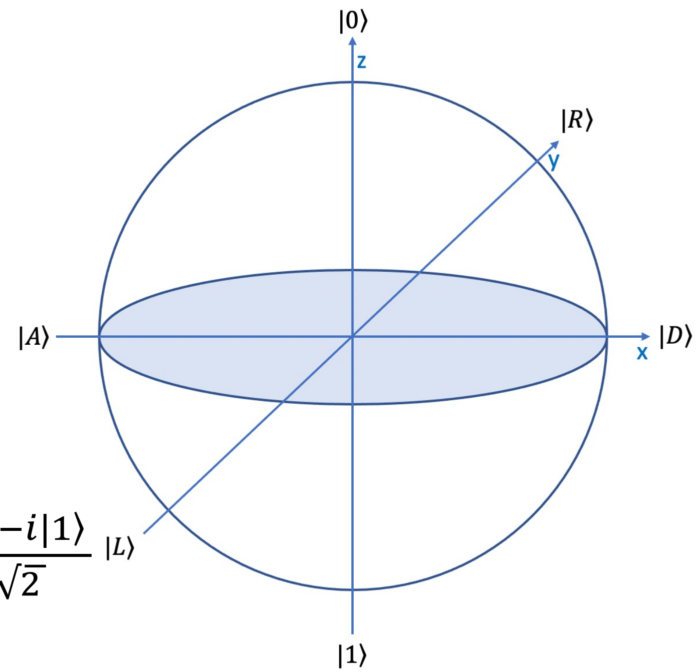
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Pauli Matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- The eigenstates of Pauli X and Y are

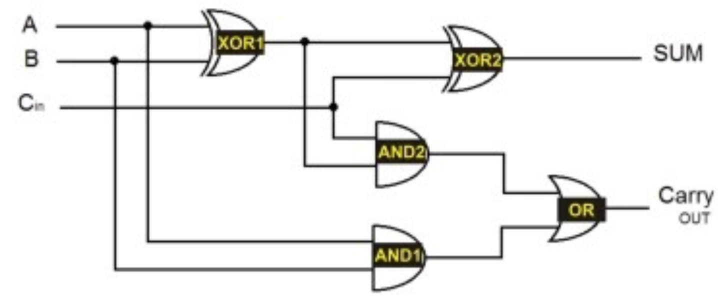
$$|D\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \; |A\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; |L\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \; |R\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

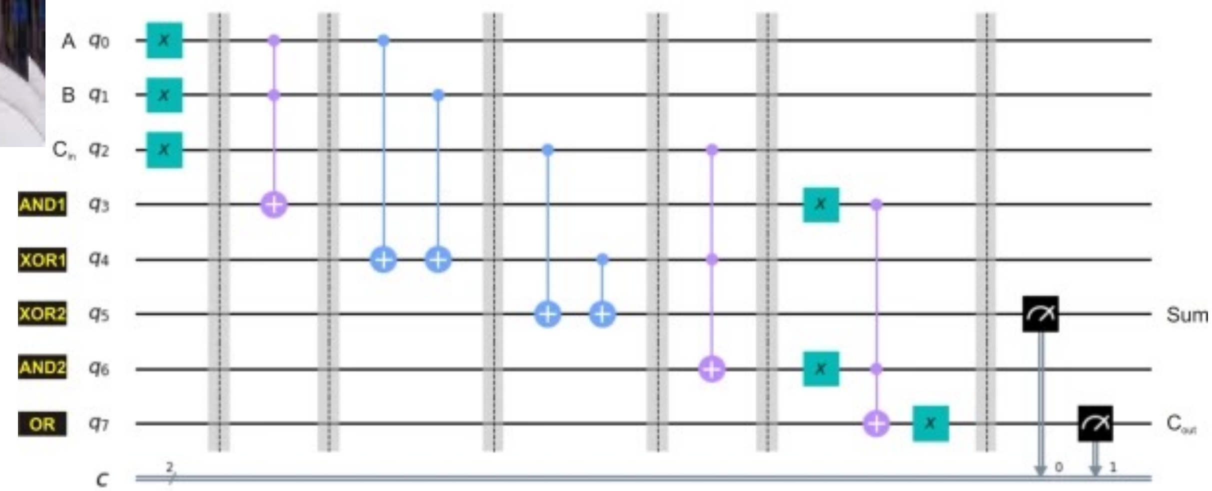


- Quantum logic gates can be therefore defined to develop quantum computing and information processing circuits.

Adder by Quantum Logic Gates

IBM's Quantum Computer
by superconducting devices





Quantum Entanglement (I)

Now, let us look further into the difference between a classic system and a quantum system. If a blue ball and a red ball forms a classic system and these two balls are distant, the possession of the red ball has absolutely has no affect on the blue ball, and *vice versa*.

On the other hand, in a quantum system of two photons A, B, we have

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|{\rightarrow_A}\rangle\,|{\uparrow_B}\rangle + |{\uparrow_A}\rangle\,|{\rightarrow_B}\rangle) \qquad (*)$$

Let these two photons be separated in a long distance such that they can not interact each other. Suppose the photon A with Alice and the photon B with Bob. If Alice measures her photon in state $|{\rightarrow_A}\rangle$, then Bob's photon is definitely in state $|{\uparrow_B}\rangle$, *vice versa*. However, if Alice decides to measure her photon in the basis $\{|{\nearrow}\rangle, |{\nwarrow}\rangle\}$ by passing the photon through a polarizer oriented at 45° with respect to the horizontal. Recall

$$|{\uparrow}\rangle = \frac{1}{\sqrt{2}}(|{\nearrow}\rangle + |{\nwarrow}\rangle)$$

$$|{\rightarrow}\rangle = \frac{1}{\sqrt{2}}(|{\nearrow}\rangle - |{\nwarrow}\rangle)$$

Quantum Entanglement (II)

The two-photon state becomes

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[|\nearrow\rangle_A(|\uparrow\rangle_B + |\rightarrow\rangle_B) + |\nwarrow\rangle_A(|\rightarrow\rangle_B - |\uparrow\rangle_B)\right]$$

Consequently, the measurement outcome of Alice's photon in the state $|\nearrow_A\rangle$ is

$$\langle \nearrow_A|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_B\rangle + |\rightarrow_B\rangle) = |\nearrow_B\rangle$$

On the other hand, if Alice's photon is measured in the state $|\nwarrow_A\rangle$,

$$\langle \nwarrow_A|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_B\rangle - |\rightarrow_B\rangle) = -|\nwarrow_B\rangle$$

Therefore, the quantum state of Bob's photon depends on what Alice decides to do, while there is no way for Alice's photon and Bob's photon to interact with each other. Similarly, the state of Alice's photon is influenced by what Bob does to his photon. That is, these two photons are *entangled* even if they are too far apart to interact, due to the fact that these two photons are initially created in a *non-separable* quantum state as **(*)**

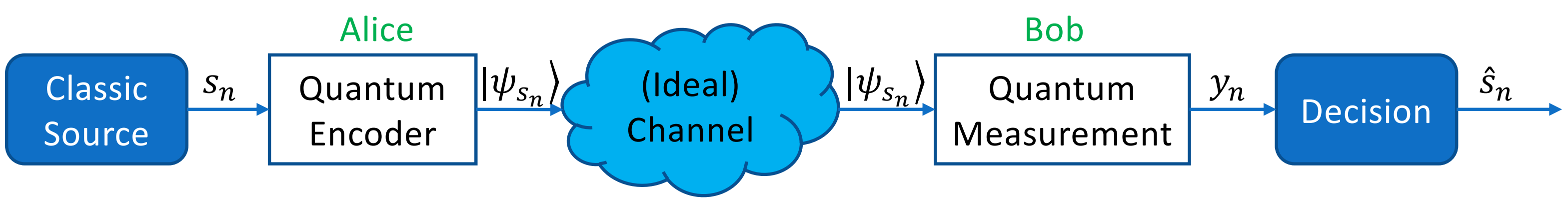
Remark: The state of AB system is *separable* if $|\psi_{AB}\rangle = |\psi_A\rangle\,|\psi_B\rangle$.

No-Cloning Theorem

- In a quantum entangled system, it is NOT possible to copy an arbitrary qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
  - First being articulated by James Park in proving the impossibility of a simple perfect non-disturbing measurement scheme in 1970, which was re-discovered by Wootters and Zurek, and by Diek in 1982
  - Any copying procedure must introduce some form of noise in the qubits.
  - It leads to perfectly secure key distribution in cryptography.
    - The no-cloning theorem prevents using the classical error correction techniques on quantum states (e.g. impossible to back up). However, Shor and Steane independently devised the first quantum error correcting codes in 1995.
    - The no-cloning theorem is implied by the **no-communication theorem**, which indicates that the quantum entanglement cannot be used to transmit the classical information nor bits.
    - The entanglement-assisted teleportation allows a quantum state to be destroyed in one location and an exact copy to be recreated in another location.
- Effective interception of quantum communication is not known yet.
  - Impossibility to extract information without destroying it ➔ Quantum Key Distribution

Quantum Communications

- Quantum-classic communications
  - Primary difference from traditional communication theory: To determine the best projection operators for the receiver, while the objective is to minimize the average cost of all possible detection operators
    - C.W. Helstrom, “Quantum Detection and Estimation Theory”, *Journal of Statistical Physics*, 1969
    - K. Kato, M. Osaki, M. Sasaki, and O. Hirota, “Quantum detection and mutual information for QAM and PSK signals,” *IEEE Trans. Commun.*, vol. 47, pp. 248–254, Feb. 1999.
  - Quantum states, or sometimes entanglement-assisted
  - Quantum (inspired) signal processing and quantum information theory
- Entanglement-based quantum communications
  - Entanglement by optical/photonic information processing to advance future optical wireless communications and networks



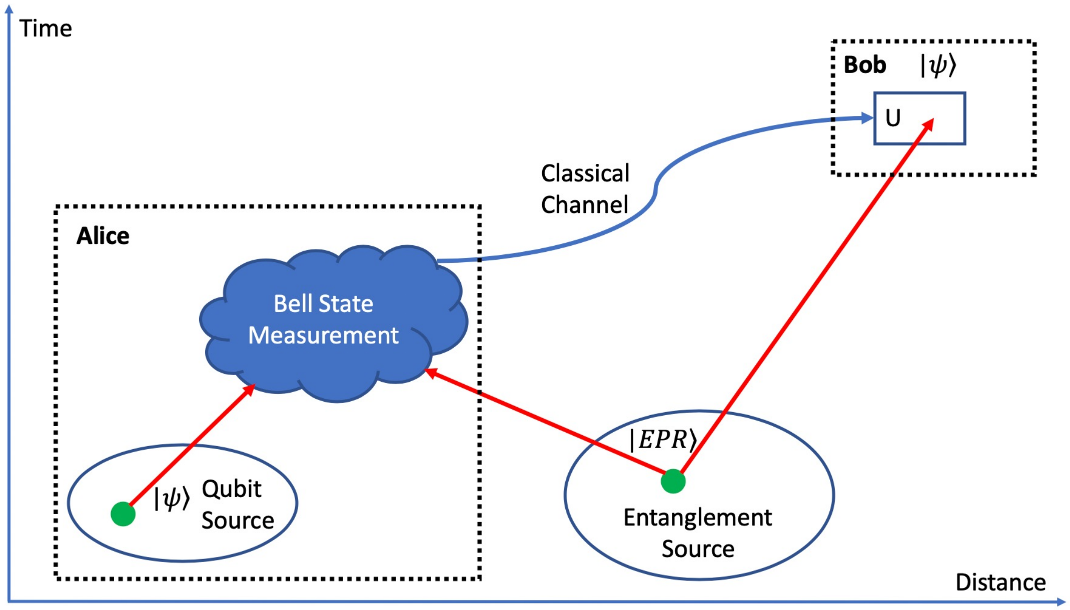
Quantum-classic digital transmission system

Quantum Teleportation

- A quantum state is transferred from one system to another in the following steps, which facilitates point-to-point communication.
  - There exists the distribution of entanglement, typically photons pairs being sent through the optical fibers. Then, the quantum teleportation channel is then established, while the optical fibers are not needed any more.
  - Alice performs the Bell-state measurement (BSM) between her photon from the entangled pair and the qubit photon that carries the quantum state to be teleported, while the BSM obviously provides no information about the teleported quantum state but something regarding the relationship between two photons (i.e. two quantum systems). Such a relationship can be viewed as the manifestation of the entanglement, while the entanglement mathematically lies in the eigenvectors of the BSM operator.
  - Alice informs Bob about the results of her BSM, and Bob performs a result-dependent unitary operation (quantum logic gates) on his quantum system.

Teleportation in the movie (Star Trek)

Illustration of Quantum Teleportation

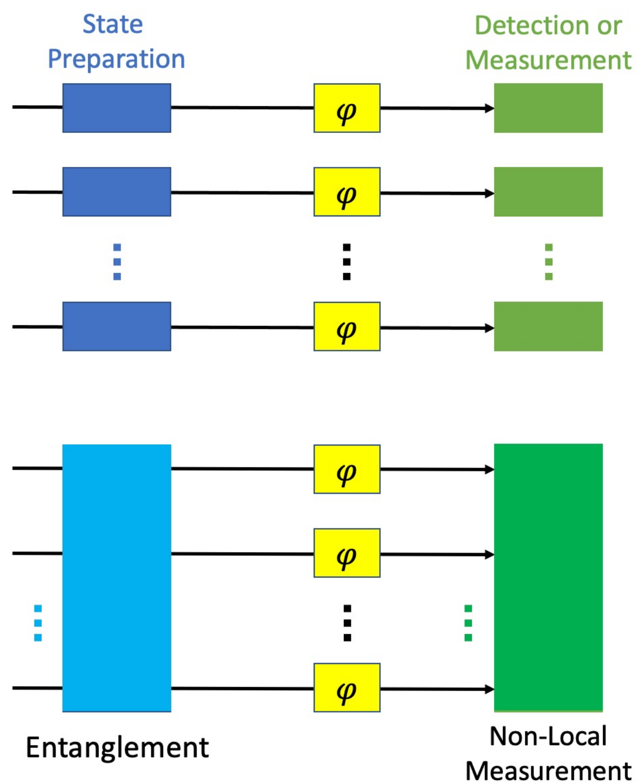


Alice perform a Bell-state measurement (BSM), a joint measurement on the unknown qubit $|\psi\rangle$ and one photon from the entangled state |EPR⟩. This measurement does not reveal the state of the qubit, but is sent to Bob who performs a result-dependent operation U to complete the quantum teleportation.

The speed of communication is still not greater than the speed of light.

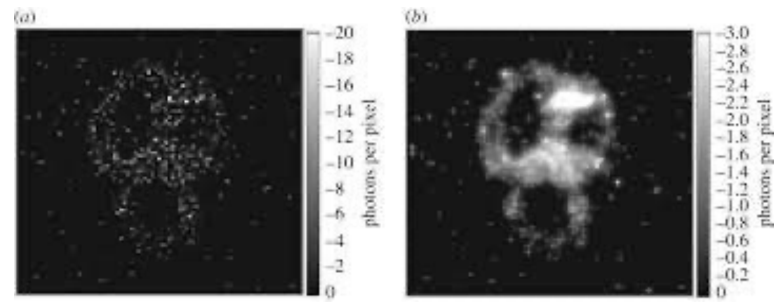
Quantum Metrology

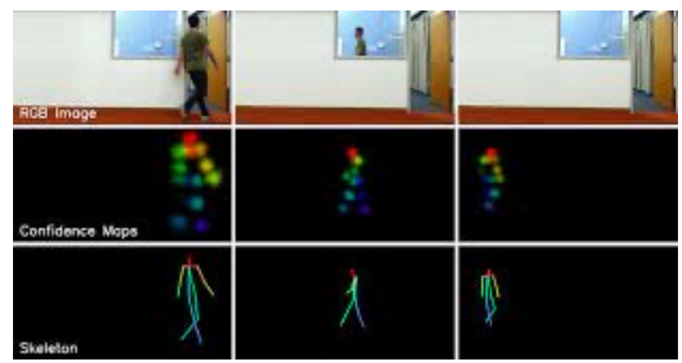
- 20 years ago, researchers at MIT noted that quantum mechanics, particularly quantum entanglement, can greatly enhance the precision of (quantum) measurements ➔ quantum metrology
  - Statistically speaking, n independent classic measurements gives the gain $\sqrt{n}$, but the gain of n for quantum measurements
  - Sophisticated techniques in quantum photonics and interferometers
  - Wide-range applications: timing, frequency, positioning, quantum imaging (such as ghost imaging and see-through-wall), quantum sensing, quantum navigation, quantum networking, and quantum distributed computing
  - Quantum Imaging, Sensing, Navigation, and Radar



Applications of Quantum Metrology and Sensing

- Quantum imaging and ghost imaging
  - Entangled photons
  - Highly correlated beams
- Quantum positioning & navigation
- Quantum remote sensing
  - See-through-the-wall technology
- Quantum radar





Quantum information technology is expected to change the landscape of industry in 10 years

It needs excellent knowledge regarding

- **Physics**
- **Mathematics**
- **Engineering**

Thank you!
Questions?