Lecture 1:
Part B - Introduction to Quantum Physics

QURIOS
THE QUANTUM TECHNOLOGIES ACADEMY

Bra-Ket Notation

Bra-ket notation, also called Dirac notation, is a way of writing and working with quantum states in quantum mechanics. A **ket**, written as $|\psi\rangle$, represents a quantum system, while a **bra**, written as $\langle\phi|$, is a mathematical tool used to describe how quantum states interact.
The expression $\langle\phi|\psi\rangle$ gives a number that represents how similar two quantum states are, and combinations like $|\psi\rangle\langle\phi|$ help describe quantum operations. This notation makes it easier to express and calculate quantum behavior, especially in quantum computing and communication.

Superposition

Superposition is a fundamental concept in quantum mechanics that describes how a quantum system can exist in multiple states at the same time. Unlike classical objects, which are in one definite state, a quantum system can be in a combination of states until it is measured.
For example, if a quantum particle can be in state $|0\rangle$ or state $|1\rangle$, it can also exist in a superposition of both, written as

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

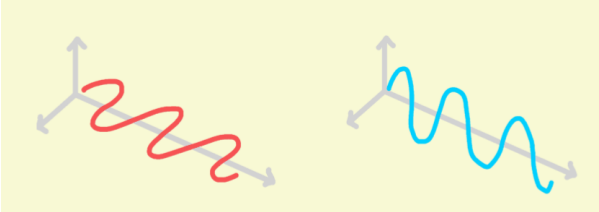
,where $|\psi\rangle$ is the quantum state, and α and β are complex numbers called **probability amplitudes**. The probabilities of observing the states $|0\rangle$ or $|1\rangle$ are $|\alpha|^2$ and $|\beta|^2$, respectively. This notation is foundational for describing quantum phenomena and their inherent randomness.

Bit vs. Qubit

- **Bit**: A classical bit exists in a deterministic state, either 0 or 1.
- **Qubit**: A qubit can exist in a **superposition** of 0 and 1, where the weight of each state is defined by the probability amplitudes. Upon measurement, the superposition collapses into a definite state.

Polarization of Photons

Photon polarization is a physical realization of qubits and a key mechanism in quantum communication. The polarization of a photon refers to the plane in which its electric field oscillates, which can be controlled and measured to encode quantum information:



Polarization of light representing qubits in different bases.

- **Polarization Measurement**: A photon's polarization, initially in superposition, collapses into a definite state when measured.
- **Measurement Bases**: Common bases include horizontal $|H\rangle$ and vertical $|V\rangle$, or diagonal $|+\rangle$ and anti-diagonal $|-\rangle$.

These bases are **mutually unbiased**, meaning that measuring in one basis provides no information about measurements in the other.

Entanglement

Quantum entanglement is a phenomenon where two or more particles become correlated in such a way that the measurement of one particle's state instantaneously determines the state of the other, regardless of the distance between them. This **correlated randomness** arises from entanglement, meaning that while the outcomes appear random individually, they are perfectly correlated when compared. Mathematically, an entangled state of two qubits can be represented as a **Bell state**, such as:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

or

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

These states describe two qubits that, when measured in the same basis, always yield correlated

results. Entanglement is central to quantum communication, enabling technologies like **quantum teleportation** and **quantum key distribution (QKD)**. For example, entangled photons can be used to distribute secure keys between distant parties, with the **non-local correlations** ensuring privacy and security.

No-Cloning Theorem

The **no-cloning theorem** states that it is impossible to create an identical copy of an unknown quantum state. The reason for this is, copying a state requires measurements, and any measurement influences the state of the observed quantum object. This principle is critical for quantum security. Mathematically:

$$U(|\psi\rangle \otimes |e\rangle) \neq |\psi\rangle \otimes |\psi\rangle$$

The **tensor product** ($\otimes$) is a way to combine two quantum states into a single, larger state that describes the whole system. If one qubit is in state $|\psi\rangle$ and another is in state $|\phi\rangle$, their combined state is written as:

$$|\psi\rangle \otimes |\phi\rangle.$$

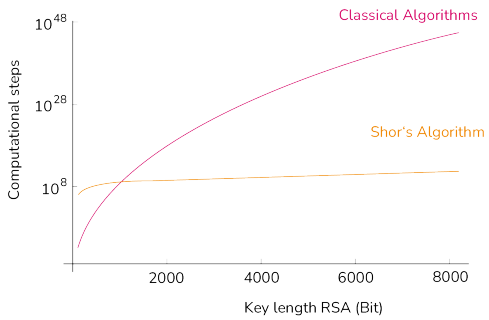
This new state accounts for all possible combinations of the original states.
The inability to clone quantum states underpins the security of **Quantum Key Distribution (QKD)** by preventing eavesdroppers from copying information without detection.

Quantum Algorithms

Quantum algorithms exploit the unique properties of quantum mechanics, such as superposition and entanglement, to solve problems faster than classical algorithms.

- **Grover's Algorithm**: Provides a **quadratic speedup** for unstructured search problems, reducing time complexity from $O(N)$ to $O(\sqrt{N})$.

- **Shor's Algorithm**: Efficiently factors large integers, potentially breaking current asymmetric cryptographic systems like RSA. Shor's algorithm runs in polynomial time, making it exponentially faster than classical algorithms.



Comparison of Shor's algorithm vs. classical algorithm.

Significance in Cryptography

Quantum mechanics enables secure communication protocols, such as **Quantum Key Distribution (QKD)**. Two principles make QKD robust:

- **Randomness**: Quantum measurements produce truly random outcomes, essential for generating secure cryptographic keys.

- **No-Cloning Theorem**: Prevents eavesdroppers from intercepting and duplicating quantum information without detection.

Foreshadowing: Store-Now-Decrypt-Later

Adversaries may store encrypted data now and decrypt it later once quantum computers become available. This threat underscores the urgency of transitioning to **QKD**. Preparing for these challenges requires proactive migration to quantum-safe methods within the next 3–7 years.

Practical Example: Quantum Randomness

A photon in a superposition of polarization states collapses into a definite state (e.g., $|H\rangle$ or $|V\rangle$ and $|+\rangle$ or $|-\rangle$) upon measurement. This unpredictable outcome forms the basis of **Quantum Random Number Generators (QRNGs)**.

QRNGs are critical for secure cryptographic protocols, ensuring truly random keys that cannot be replicated.