**What is Quantum Communication?**

**1. What is Quantum Communication?**

Quantum communication is the transfer of information using the principles of **quantum mechanics** rather than classical physics.  
Instead of sending classical bits (0s and 1s), it often uses **quantum states** (qubits) carried by photons (particles of light).

**2. Key Quantum Principles Behind It**

* **Superposition**  
  A qubit can exist in a combination of |0⟩ and |1⟩ at the same time.  
  This allows quantum communication systems to encode more complex information.
* **Entanglement**  
  Two or more qubits can be entangled, meaning their states are linked.  
  Measuring one immediately determines the other, even if they’re far apart.  
  → This enables *instantaneous correlations* useful in communication and security.
* **No-Cloning Theorem**  
  You cannot copy an unknown quantum state.  
  → This makes quantum communication secure, since eavesdropping is detectable.
* **Measurement Collapse**  
  When you measure a quantum state, it collapses to |0⟩ or |1⟩.  
  → This property is used in security (detecting intruders).

**3. How Quantum Communication Works**

* **Carriers of Information:** Usually photons transmitted through optical fibers or free space.
* **Encoding Information:**  
  Example: Polarization of photons (horizontal = 0, vertical = 1).
* **Transmission:** Sent over quantum channels (fiber optics, satellite-to-ground links).
* **Detection:** Special quantum detectors measure and decode the states.

**4. Main Applications**

* **Quantum Key Distribution (QKD):**  
  Securely sharing encryption keys using quantum states (e.g., BB84 protocol).  
  If an eavesdropper tries to intercept, the disturbance reveals their presence.
* **Quantum Networks:**  
  Building a “Quantum Internet” where quantum information (qubits) can be sent between distant quantum computers.
* **Quantum Teleportation:**  
  Transfer of quantum state information using entanglement and classical communication.  
  (Note: Not physical teleportation, only quantum state transfer.)

**5. Advantages**

Ultra-secure communication (cannot be hacked without detection).  
Enables future **quantum internet**.  
Can link quantum computers globally.

**6. Challenges**

Photon loss in optical fibers (long distances).  
Decoherence (quantum states easily disturbed by environment).  
Need for **quantum repeaters** (devices to extend distance).  
Current systems are expensive and complex.

**The Major Results**

 **QKD (BB84, Ekert protocols):** Practical secure communication.

 **Teleportation:** Trade-off between entanglement and classical communication.

 **Superdense Coding:** Doubles classical capacity per qubit with entanglement.

 **Entanglement Distillation:** Makes reliable long-distance quantum communication possible.

 **Quantum Channel Theory:** Shows surprising new limits and capacities beyond classical communication.

# Quantum Key Distribution (QKD) Basics

* **Goal:** Allow two parties (traditionally called **Alice** and **Bob**) to create a shared secret key.
* **Guarantee:** Any eavesdropper (**Eve**) trying to intercept introduces errors that Alice & Bob can detect.
* **Reason it works:**
  + Quantum states cannot be measured without disturbance (**measurement collapse**).
  + Unknown quantum states cannot be copied (**no-cloning theorem**).

# How QKD Works (Step-by-Step with BB84 Example)

The **BB84 protocol** (Bennett & Brassard, 1984) is the first and most famous QKD scheme.

### 1. Photon Preparation

* Alice prepares photons polarized in one of **two bases**:
  + **Rectilinear basis (+):** |0⟩ = horizontal, |1⟩ = vertical
  + **Diagonal basis (×):** |+⟩ = 45°, |−⟩ = 135°

### 2. Transmission

* Alice sends a random sequence of photons (random basis, random bit).

### 3. Measurement

* Bob measures each incoming photon in a **random basis** (either + or ×).

### 4. Sifting

* Alice and Bob publicly announce which basis they used (not the result).
* They keep only the cases where their bases matched → this becomes the **raw key**.

### 5. Error Checking

* They publicly compare a subset of bits.
* If the error rate is low → Eve was not present.
* If error rate is high → discard communication.

### 6. Privacy Amplification

* Apply error correction + privacy amplification techniques to ensure a secure final key.

**A simplified example of BB84 QKD step by step**

**Goal**

Alice and Bob want to establish a shared **secret key** using quantum states.

We’ll walk through **6 photons (bits)** as an example.

1. **Alice Prepares & Sends Photons**

* Alice wants to send a random string of bits (0s and 1s).
* She chooses **two things for each bit**:
  1. **Bit value (0 or 1)**
  2. **Encoding basis**:
     + **Rectilinear (+ basis):**
       - 0 = Horizontal polarization (→)
       - 1 = Vertical polarization (↑)
     + **Diagonal (× basis):**
       - 0 = 45° polarization (↗)
       - 1 = 135° polarization (↖)

|  |  |  |  |
| --- | --- | --- | --- |
| **Step** | **Alice’s Basis** | **Alice’s Bit** | **Photon Sent** |
| 1 | + | 0 | Horizontal |
| 2 | × | 1 | 135° |
| 3 | + | 1 | Vertical |
| 4 | × | 0 | 45° |
| 5 | + | 0 | Horizontal |
| 6 | × | 1 | 135° |

**Physical implementation:**  
Alice uses a **photon source** (laser attenuated to single photons) + **polarizers** to prepare each photon in the correct polarization.

# 2. Transmission to Bob

* Alice sends the sequence of photons over a **quantum channel**:
  + Optical fiber
  + Free-space link (satellite → ground)

The photons **carry the quantum states** across the channel.

**3. Bob Chooses Random Measurement Bases**

* Bob doesn’t know Alice’s basis, so for each photon he chooses randomly between:
  + **Rectilinear (+ basis)**
  + **Diagonal (× basis)**
* If Bob’s basis = Alice’s basis → **he gets the correct bit**.
* If Bob’s basis ≠ Alice’s basis → **his result is random (50% chance)**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Alice’s Basis** | **Alice’s Bit** | **Bob’s Basis** | **Bob’s Result** |
| 1 | + | 0 | 0⟩ | + |
| 2 | × | 1 | −⟩ | + |
| 3 | + | 1 | 1⟩ | × |
| 4 | × | 0 | +⟩ | × |
| 5 | + | 0 | 0⟩ | + |
| 6 | × | 1 | −⟩ | × |

**Physical implementation:**  
Bob uses a **beam splitter** that randomly directs photons into one of two polarizers (one for +, one for ×), followed by **single-photon detectors**.

**4. Sifting Process (Public Discussion)**

* After transmission, Alice & Bob communicate over a **classical channel** (like the internet).
* They announce **which basis** they used for each photon (not the bit values!).
* They keep only the cases where they **used the same basis**.  
  → This is called **sifting**.

Example:

* Alice: (+, ×, +, ×, +, ×)
* Bob: (+, +, ×, ×, +, ×)
* Keep positions 1, 4, 5, 6.

|  |  |  |  |
| --- | --- | --- | --- |
| **Step** | **Alice’s Basis** | **Bob’s Basis** | **Keep?** |
| 1 | + | + | ✔ |
| 2 | × | + | ✘ |
| 3 | + | × | ✘ |
| 4 | × | × | ✔ |
| 5 | + | + | ✔ |
| 6 | × | × | ✔ |

**5. Raw Key**

From those matching basis cases:

* Step 1 → 0
* Step 4 → 0
* Step 5 → 0
* Step 6 → 1

Raw Key = **0011** (if Bob measured correctly in step 6).

**6. Error Checking**

* To check for eavesdroppers (Eve), Alice & Bob publicly compare a **random subset of their results**.
* If Eve tried to measure, she introduces errors (because of measurement disturbance + no-cloning).
* If the error rate is **below threshold (~11%)**, they proceed. Otherwise, they discard and restart.

Alice and Bob randomly reveal a **subset** of their raw key.

* If too many mismatches appear → Eve (the eavesdropper) is present.
* If matches are good → they keep the rest as a **secure key**.

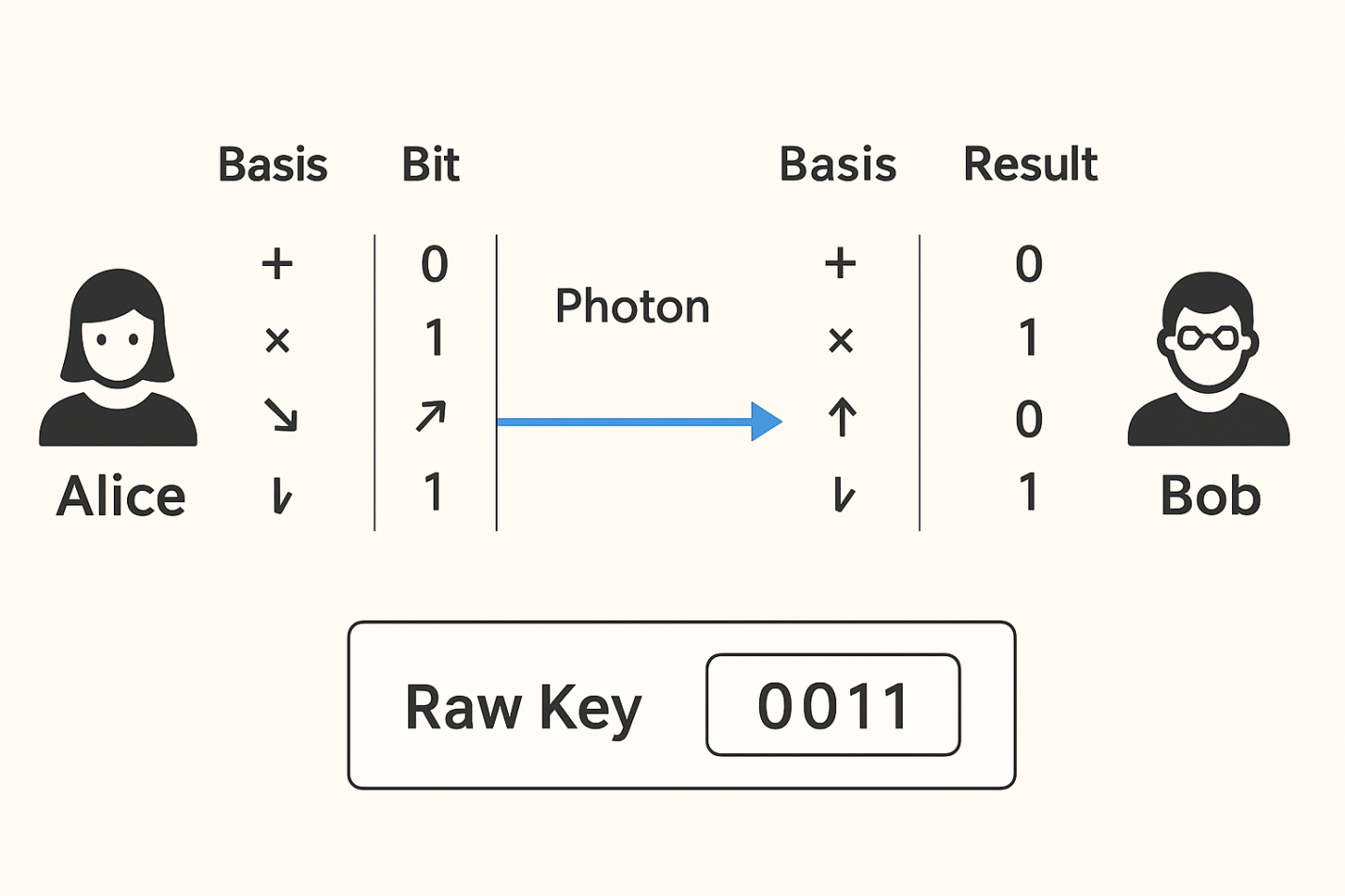
# 7. Post-Processing

Even without Eve, there may be **channel noise**. To fix this:

1. **Error Correction**
   * Alice & Bob apply classical error-correcting codes to make sure they have **identical keys**.
2. **Privacy Amplification**
   * They shorten the key using hash functions to remove any partial knowledge Eve might have.

**8. Final Key**

After error correction & privacy amplification, they get a **shorter but perfectly secure key**, which they can now use for encryption (e.g., a **one-time pad**)



**Summary of Example:**

* Alice sends 6 photons → Bob measures.
* They keep only 4 cases with same basis.
* Their shared raw key = **0011**.
* After error checking & privacy amplification → Final secure key.

# What is Entanglement?

* Two (or more) particles are **entangled** when their quantum states are correlated in such a way that measuring one **instantly determines** the state of the other, no matter how far apart they are.
* Example: For an entangled pair (EPR pair):

∣Φ+⟩=1/2(∣00⟩+∣11⟩)

If Alice measures her qubit as 0, Bob’s qubit is instantly 0. If Alice measures 1, Bob’s is 1.

# Role of Entanglement in Communication

Entanglement enables communication tasks such as:

### 1. ****Quantum Teleportation****

* Entanglement allows Alice to send the **state of a qubit** to Bob without physically transmitting the particle.
* Requirements:
  + Alice and Bob share an entangled pair.
  + Alice performs a joint measurement on her entangled qubit + the qubit she wants to send.
  + She sends **2 classical bits** to Bob.
  + Bob applies the right operation to recover the original state.

**Result:** 1 entangled pair + 2 classical bits → transfer of 1 qubit state.

**Example:**  
Alice wants to send an unknown qubit ∣ψ⟩|\psi\rangle∣ψ⟩ to Bob.

* They share ∣Φ+⟩|\Phi^+\rangle∣Φ+⟩.
* Alice measures her qubits and tells Bob her result (classical 2 bits).
* Bob applies a correction (Pauli operation).
* Bob now has ∣ψ⟩|\psi\rangle∣ψ⟩, even though Alice no longer does.

### 2. ****Superdense Coding****

* Entanglement allows Alice to send **2 classical bits of information by sending only 1 qubit**.
* Process:
  + Alice and Bob share ∣Φ+⟩|\Phi^+\rangle∣Φ+⟩.
  + Alice applies one of four operations (I, X, Z, or XZ) on her qubit → changes the joint state into one of four Bell states.
  + She sends her qubit to Bob.
  + Bob performs a Bell-state measurement → learns which operation Alice did → recovers 2 classical bits.

**Result:** 1 qubit + entanglement = 2 classical bits.

**Example:**

* Alice wants to send "10" (two classical bits).
* She applies Pauli-X (flip) on her half of the entangled qubit.
* Sends it to Bob.
* Bob measures → sees which Bell state they share → learns "10".

### 3. ****Quantum Key Distribution (E91 Protocol)****

* Uses entangled pairs to generate secure keys.
* Alice and Bob measure entangled photons in random bases.
* Correlations follow **quantum mechanics**, not classical.
* An eavesdropper cannot copy the entanglement, and interference introduces errors that Alice & Bob detect using **Bell’s inequality tests**.

# Summary

* **Teleportation:** Send a qubit state using entanglement + classical bits.
* **Superdense Coding:** Double classical capacity using entanglement.
* **QKD (E91):** Generate secure keys via entanglement correlations.

# What is the Quantum Internet?

The **Quantum Internet** is a future network that allows devices to **send, receive, and process quantum information (qubits)** across long distances — just like today’s internet does with classical bits.

It’s not meant to replace the classical internet, but to **complement it**, enabling tasks that are impossible with classical networks.

# Core Idea

* In the classical internet: Information = **0s and 1s**.
* In the quantum internet: Information = **quantum states (superposition & entanglement)**.
* Quantum Internet will use **entanglement** as the main “link” between nodes, instead of just electromagnetic signals.

# Key Building Blocks

1. **Qubits as Information Units**
   * Sent using photons through fiber optics or satellites.
2. **Entanglement Distribution**
   * Distant parties (say Alice in India and Bob in the USA) share entangled qubits.
   * Even across continents, changes in measurement on one qubit affect correlations with the other.
3. **Quantum Repeaters**
   * Like classical repeaters, but they use **entanglement swapping** and **purification** to extend distance.
   * Overcome photon losses in fibers.
4. **Quantum Memories**
   * Store entangled states for later use.

# Examples of Quantum Internet Applications

### 1. ****Quantum Key Distribution (QKD) on a Global Scale****

* Alice and Bob can share a **secret encryption key** across the world.
* Example: A bank in **New York** and a branch in **Tokyo** could exchange secure keys via quantum satellites → impossible to hack.

### 2. ****Distributed Quantum Computing****

* Multiple small quantum computers could link together over a quantum internet → forming a much more **powerful virtual quantum computer**.
* Example: Two 50-qubit computers in different labs connect and behave like one 100-qubit computer.

### 3. ****Quantum Teleportation of Information****

* Using entanglement + classical channels, the **quantum state** of a particle can be transmitted across the network.
* Example: A quantum sensor in **Paris** can “teleport” its measured state instantly to a lab in **Tokyo**.

### 4. ****Ultra-Precise Synchronization****

* Entangled photons can synchronize atomic clocks across the globe with **unprecedented precision**.
* Example: GPS systems could become **1000× more accurate**, useful for navigation and scientific research.

# Real-World Progress

* **China’s Micius satellite (2017):** Sent entangled photons between two cities 1200 km apart.
* **US DOE Quantum Internet Blueprint (2020):** Plans for a national quantum internet.
* **EU Quantum Communication Infrastructure (EuroQCI):** Aims to build a secure quantum network across Europe.
* **Toshiba & BT UK trials (2022):** QKD links over metropolitan fiber networks.

# Simple Analogy

Think of the **classical internet** like sending **copies of a document**. The **quantum internet** is like sharing a **single magical notebook** that both you and your friend have — whatever happens in one instantly affects the other.

# What is Secure Global Networking?

It means creating a worldwide communication system where **sensitive information** (banking, defense, healthcare, government, research data, etc.) is **100% secure**, not just “computationally hard to hack.”

* **Today’s internet security:**
  + Relies on cryptographic algorithms (RSA, ECC).
  + Security depends on the difficulty of solving math problems (like factoring).
  + A powerful **quantum computer** could break these algorithms in the future.
* **Secure networking with quantum communication (QKD):**
  + Security comes from **laws of physics**, not math problems.
  + If anyone tries to eavesdrop, the communication is disturbed and detected.

# How International Banking Network Works with Quantum Security

### 1. ****Entanglement or QKD Distribution**** Organizations in different countries generate **shared secret keys** with absolute security.

* Satellites (like China’s Micius) or undersea fiber optics distribute **entangled photon pairs** or **QKD signals** between global banking hubs.
* Example links:
  + London ↔ New York
  + Singapore ↔ Tokyo
  + Zurich ↔ Frankfurt

### 2. ****Secure Key Generation****

* Using **BB84 protocol** or **entanglement-based QKD (E91)**, each bank generates a **shared secret key** with its partner.
* If hackers (Eve) try to eavesdrop → errors appear → transmission aborted.
  + 3. **One-Time Pad (OTP) Encryption** These keys can encrypt classical communication (emails, bank transactions, video calls).
* Once a key is shared, the bank uses it to encrypt transaction data with OTP.
* OTP + QKD = **provably unbreakable encryption**.

**3. Integration with Classical Networks:** Classical internet carries the bulk data, but encryption keys are provided by the **quantum network**.

# Example: International Banking Network

Imagine **Bank A (London)** and **Bank B (Singapore)** want to exchange **financial transaction data** securely.

### Today’s Method

* They use RSA/ECC encryption over classical internet.
* Vulnerable to future quantum computers (Shor’s algorithm).
* Hackers could record encrypted data now and **decrypt later** when quantum computers are available.

### With Quantum Secure Networking

1. Satellites (like China’s **Micius**) distribute **entangled photon pairs** between London and Singapore.
2. Using **QKD (BB84 or E91 protocol)**, the two banks establish a **shared secret key**.
3. Banks use that key for **one-time pad encryption** on transaction data.
4. If hackers try to intercept → disturbance is detected → session aborted.

Result: Transactions remain **secure forever**, even against future quantum computers.

# Other Real-World Applications

* **Defense & Government:** Secure communication between military bases or embassies worldwide.
* **Healthcare:** Transferring sensitive patient/genomic data securely across continents.
* **Research:** Sharing experimental results in high-security fields (e.g., nuclear, AI, or pharmaceutical research).
* **Finance:** Global stock exchanges and interbank transfers safe from cyberattacks.

# Simple Analogy

Think of today’s internet like a **safe with a complex lock** — a stronger thief (quantum computer) could eventually open it.

Quantum secure networking is like a **safe that destroys its contents if someone tampers with it** — so only the true owners can ever use it.

**In short:** Secure Global Networking with the quantum internet = **absolutely unhackable worldwide communication**, powered by **entanglement + QKD**, protecting data for governments, banks, hospitals, and individuals.

# Benefits for International Banking

**Future-proof security** → safe even against quantum computers.  
**No risk of “store now, decrypt later” attacks** (where hackers record data today to break later).  
**Tamper detection** → banks know instantly if someone tries to spy.  
**Trustless Security** → security is based on physics, not on computational hardness.

# Real-World Progress

* **Swiss Bank network**: Using QKD systems from **ID Quantique** for secure communication.
* **China (Micius satellite)**: Demonstrated QKD between Beijing and Vienna → potential model for **international finance QKD networks**.
* **Toshiba & BT UK trials (2022)**: QKD deployed over live metro banking fiber networks in London.
* **European Union EuroQCI Project**: Aiming to connect **European central banks and governments** via quantum-secure channels.