5.4 QUANTUM SECURITY CONCEPTS

I can provide the complete notes here, including diagrams and examination-oriented explanations. The downloadable Word document could not be generated in the previous attempt.

1. Introduction to Quantum Security

Quantum Security refers to the application of quantum mechanics principles to protect information, communication networks and digital systems from security threats.

Traditional cryptography mainly depends on mathematical problems that are difficult for classical computers to solve. Quantum security uses quantum principles such as superposition, entanglement and measurement disturbance to improve communication security.

Main objectives:

1. Confidentiality – Protect information from unauthorized access.
2. Integrity – Ensure that information is not modified.
3. Authentication – Verify the identity of communicating parties.
4. Secure Key Distribution – Exchange secret encryption keys securely.

Importance of Quantum Security

Quantum computers have the potential to break certain cryptographic algorithms currently used for securing digital information.

For example:

- RSA encryption relies on the difficulty of integer factorization.
- ECC relies on the difficulty of solving discrete logarithm problems.
- Shor's algorithm can efficiently solve these problems on a sufficiently powerful fault-tolerant quantum computer.
- Grover's algorithm can speed up searching through possible keys, reducing the security margin of symmetric encryption.

Therefore, quantum security techniques are being developed to protect future communication systems.

Fundamental Principles of Quantum Security

1 Qubit

A qubit (Quantum Bit) is the basic unit of quantum information.

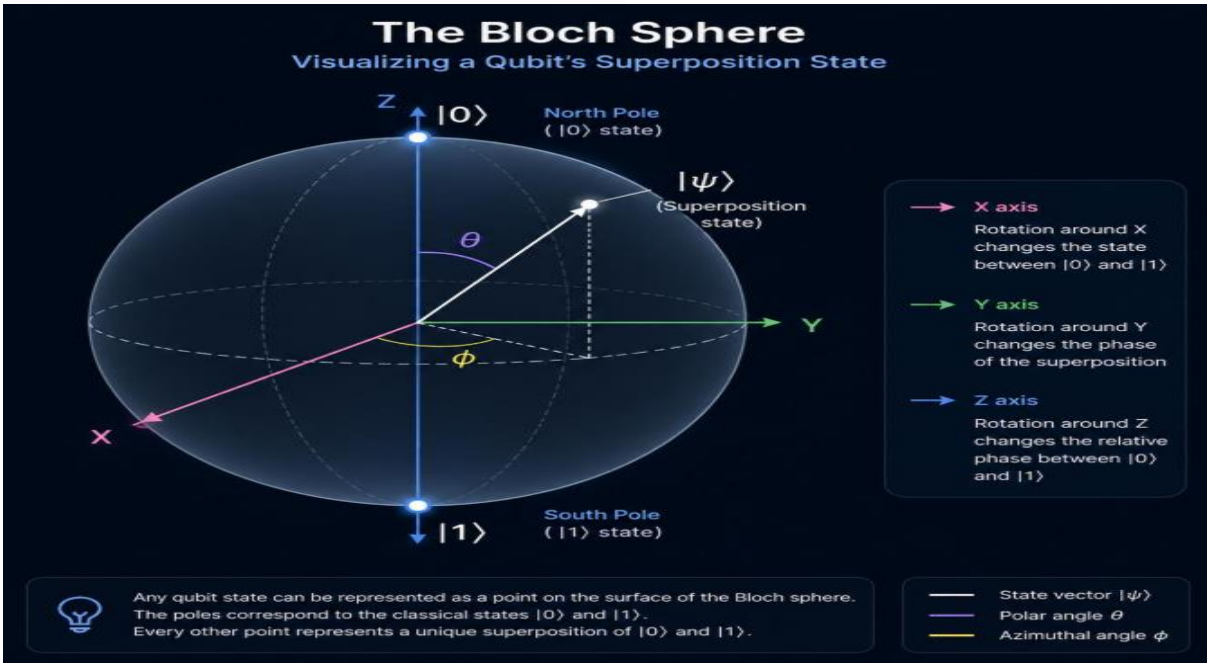
Unlike a classical bit, which can represent either 0 or 1, a qubit can exist in a superposition of both states.

Mathematical representation:

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

Where:

- $|0\rangle$ represents quantum state 0.
- $|1\rangle$ represents quantum state 1.
- α, β are probability amplitudes.
- $|\alpha|^2 + |\beta|^2 = 1$.



2

Quantum Superposition

Superposition is the ability of a quantum system to exist in a combination of multiple possible states before measurement.

For example, a qubit can be represented as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

When measured in the computational basis, the result is 0 or 1 with equal probability.

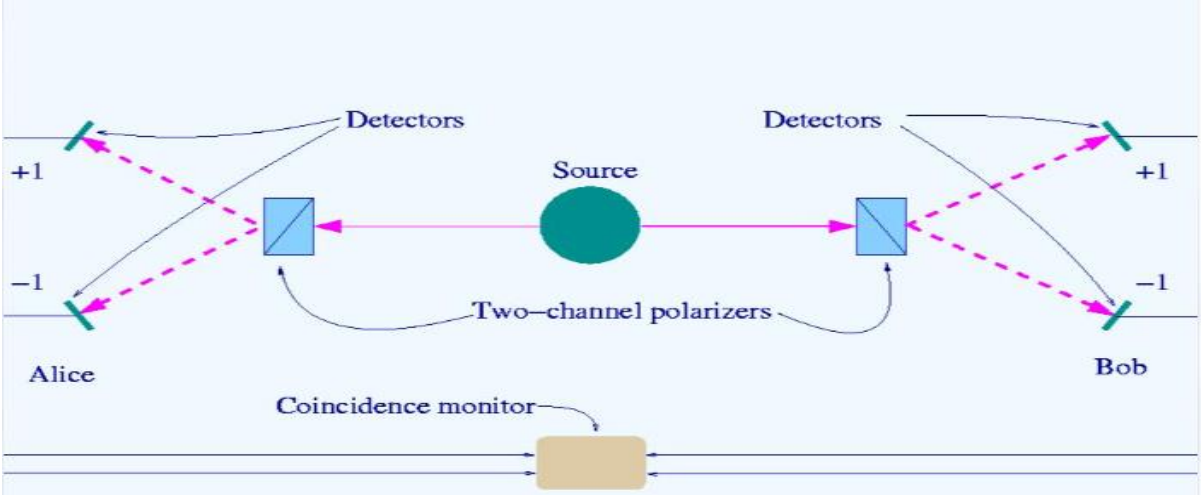
Importance: Superposition is a fundamental principle used in quantum computing and quantum information processing.

3 Quantum Entanglement

Quantum entanglement is a phenomenon in which two or more quantum particles become strongly correlated, even when separated by large distances.

Example:

If two photons are entangled, measuring one photon provides information about the correlated measurement outcome of the other.



Applications:

- Quantum Key Distribution.
- Quantum communication.
- Quantum teleportation.
- Quantum networking.

4 Measurement Disturbance

In quantum mechanics, measuring an unknown quantum state in an incompatible basis generally changes the state.

An eavesdropper attempting to observe quantum communication may introduce errors that can be detected by the communicating parties.

Importance: This principle is used in Quantum Key Distribution to detect possible interception.

5 No-Cloning Theorem

The No-Cloning Theorem states that an unknown arbitrary quantum state cannot be copied perfectly.

For example, an attacker cannot create an exact duplicate of an unknown qubit without knowing its state.

Importance:

- Prevents perfect copying of unknown quantum information.
- Helps protect quantum communication.
- Supports the security principles of QKD.

Quantum Key Distribution (QKD)

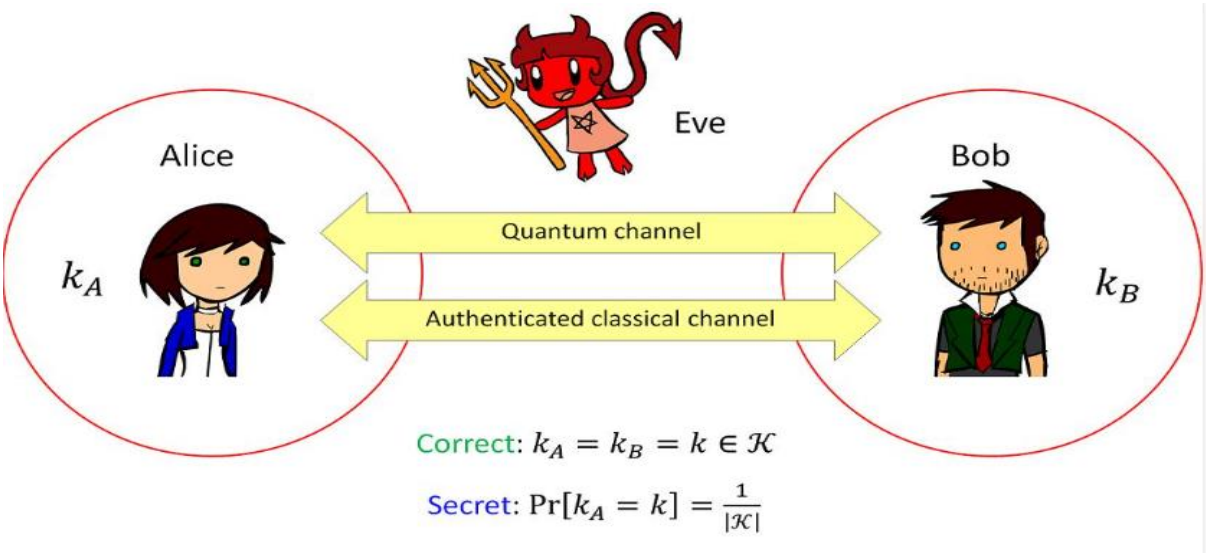
Quantum Key Distribution is a secure communication technique used to generate and share secret encryption keys between two communicating parties.

The communicating parties are commonly called:

- Alice: Sender.
- Bob: Receiver.
- Eve: Eavesdropper or attacker.

QKD uses quantum particles, commonly photons, to establish secret keys.

QKD Working Diagram



Steps Involved in QKD

1. Alice generates random binary bits.
2. Alice encodes the bits into quantum states.
3. The quantum states are transmitted to Bob through a quantum channel.
4. Bob measures the received quantum states using randomly selected measurement bases.

5. Alice and Bob compare their measurement bases through an authenticated classical channel.
6. They retain matching-basis results. This is called key sifting.
7. They compare a sample of their results to estimate the error rate.
8. Error correction and privacy amplification are performed to obtain a shared secret key.

Advantages of QKD:

- Helps detect eavesdropping.
- Uses quantum mechanical principles.
- Provides secure key establishment.
- Supports highly secure communication systems.

BB84 Protocol

BB84 is the first widely known Quantum Key Distribution protocol, introduced by Charles Bennett and Gilles Brassard in 1984.

It is a prepare-and-measure protocol that uses two different polarization bases.

Two Types of Polarization Bases

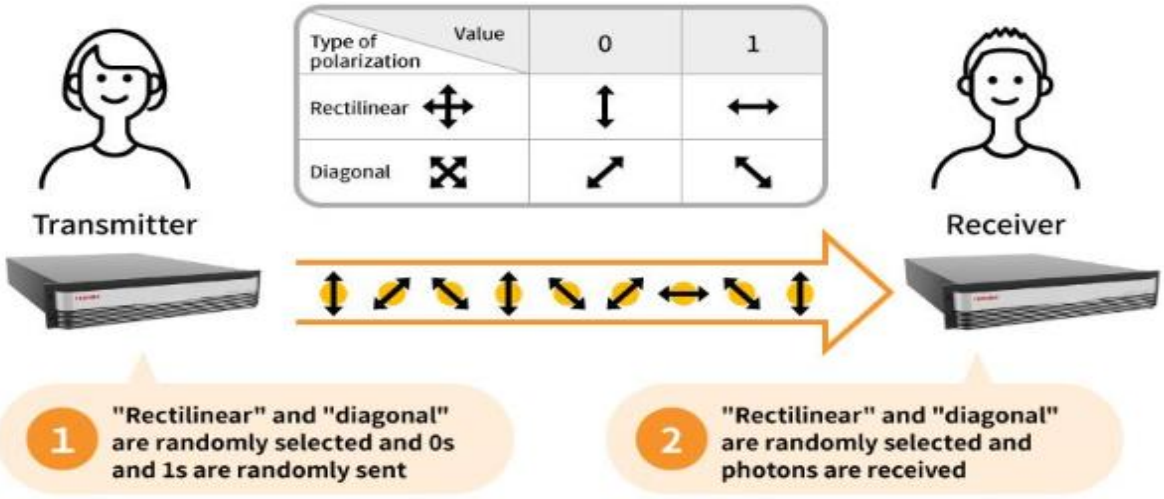
1. Rectilinear Basis (+)

- Horizontal polarization (H) = 0
- Vertical polarization (V) = 1

2. Diagonal Basis (×)

- Diagonal polarization (D) = 0
- Anti-diagonal polarization (A) = 1

Principles of the BB84 protocol (encoding using polarization)



Working of BB84 Protocol

1. Alice randomly generates binary bits.
2. Alice randomly selects rectilinear or diagonal bases.
3. Alice encodes the bits into photon polarization states.
4. Bob receives the photons and randomly selects measurement bases.
5. Alice and Bob publicly compare their bases.
6. They keep the bits measured using matching bases.
7. They check a sample of the remaining bits for errors.
8. If the error rate is acceptable, they process the remaining bits into a secret key.

Important Point: If Eve intercepts and measures the photons using incorrect bases, she may introduce detectable errors.

E91 Protocol

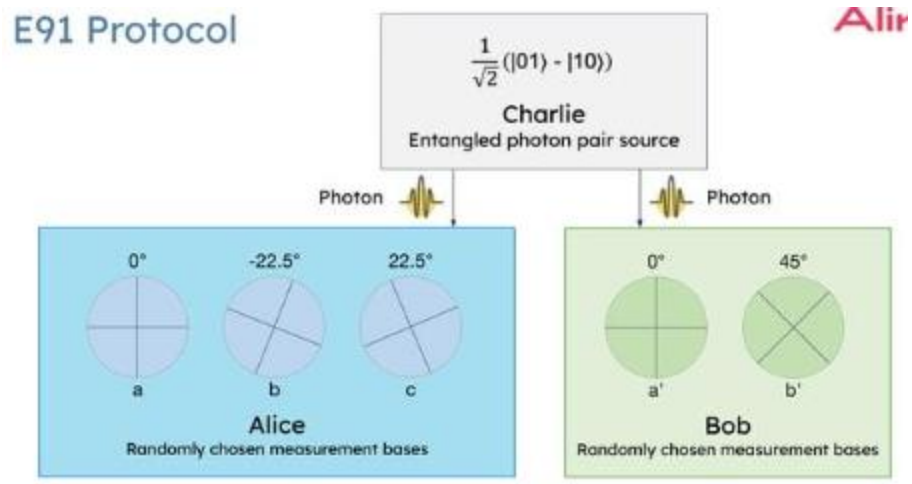
E91 is an entanglement-based Quantum Key Distribution protocol proposed by Artur Ekert in 1991.

Unlike BB84, E91 uses entangled photon pairs to establish a secret key.

Working Principle

1. An entangled photon source generates pairs of entangled photons.
2. One photon is sent to Alice.
3. The other photon is sent to Bob.
4. Alice and Bob independently measure their photons using selected measurement settings.
5. They compare measurement settings and analyse the correlations.
6. Bell inequality tests can be used to assess the security of the observed correlations.

7. They use suitable measurement outcomes to generate a secret key.



Difference Between BB84 and E91

Feature	BB84	E91
Inventor	Bennett and Brassard	Artur Ekert
Year	1984	1991
Technique	Prepare-and-measure	Entanglement-based
Quantum states	Polarized photons	Entangled photons
Security principle	Measurement disturbance and quantum-state properties	Quantum correlations and Bell inequality testing

Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers.

Unlike quantum cryptography, PQC does not require quantum hardware. It works on conventional computers.

Main objectives:

- Protect encrypted information against future quantum attacks.
- Replace vulnerable public-key cryptographic algorithms.
- Secure digital signatures and key exchange.
- Improve long-term information security.

Applications:

- Secure websites.

- Online banking.
- Digital signatures.
- Government communication.
- Cloud computing.



Quantum Cryptography vs Post-Quantum Cryptography

Quantum Cryptography	Post-Quantum Cryptography
Uses principles of quantum mechanics.	Uses quantum-resistant mathematical algorithms.
May require specialized quantum devices.	Runs on conventional computers.
QKD is a major application.	Includes key encapsulation and digital signatures.
Uses quantum states for key distribution.	Uses mathematical problems believed to resist quantum attacks.

Advantages of Quantum Security

1. Provides methods for detecting certain eavesdropping attempts.
2. Uses fundamental principles of quantum physics.
3. Supports secure key distribution.
4. Helps prepare communication systems for future quantum technologies.
5. Supports secure communication in critical applications.

Limitations of Quantum Security

1. Quantum communication equipment can be expensive.
2. Quantum channels are affected by noise and signal loss.
3. QKD has practical distance and key-generation limitations.

4. Special infrastructure may be required.
5. Real-world hardware implementation may introduce security vulnerabilities.
6. QKD requires an authenticated classical communication channel.

Applications of Quantum Security

1. **Banking and Finance** : Protects sensitive financial information and supports secure key establishment.

2. **Telecommunication**: Supports secure communication between network infrastructure and data centres.

3. **Government and Defence**: Helps protect confidential information and sensitive communication links.

4. **Cloud Computing**: Supports the development of future quantum-resistant security infrastructure.

Quantum Security is an important emerging technology that uses quantum mechanical principles to improve information security. Concepts such as superposition, entanglement, measurement disturbance and the No-Cloning Theorem form the foundation of quantum communication security. Protocols such as BB84 and E91 provide methods for Quantum Key Distribution, while Post-Quantum Cryptography helps protect conventional communication systems against future quantum-computer attacks.