**VYADH COLLOIDS PVT LTD**

# Working Mechanisms of Quantum Key Distribution (QKD)

Prepared by: Vyadh Colloids Pvt Ltd

August 21, 2025

## 1. INTRODUCTION

Quantum Key Distribution (QKD) is a secure communication technology that leverages quantum mechanics to enable two parties to generate and share cryptographic keys with provable security. Unlike classical encryption methods that rely on computational complexity, QKD ensures security based on the laws of physics, making it resistant to attacks from both classical and quantum computers.

### 2. CORE PRINCIPLES OF QKD

QKD is built upon two fundamental principles of quantum physics:

**Superposition:**

A quantum particle (e.g., a photon) can exist in multiple states simultaneously until it is measured.

**No-Cloning Theorem:**

It is impossible to make a perfect copy of an unknown quantum state. This prevents an eavesdropper (Eve) from intercepting and reproducing the key undetected.

**Measurement Disturbance:**

Any measurement of a quantum system disturbs it. If an eavesdropper attempts interception, the disturbance will introduce detectable errors in the key exchange.

## 3. GENERAL QKD WORKING MECHANISM

The standard QKD process involves four stages:

### 3.1. Quantum Transmission (Raw Key Exchange)

Alice (sender) transmits qubits (e.g., polarized photons) to Bob (receiver) through a quantum channel (fiber optic cable, free-space optical link, or satellite).

Qubits are encoded in non-orthogonal quantum states (e.g., horizontal/vertical polarization, diagonal polarization).

### 3.2. Sifting (Basis Reconciliation)

- Bob measures the qubits using randomly chosen bases.
- Alice and Bob communicate (over a classical channel) which measurement bases they used.
- They discard mismatched bases, leaving the sifted key.

### 3.3. Error Estimation & Reconciliation

- Alice and Bob compare portions of their sifted key to estimate the Quantum Bit Error Rate (QBER).
- If QBER is below a security threshold (≈11% for BB84), the transmission is considered secure.
- Error correction protocols (e.g., Cascade, LDPC codes) are applied to align keys.

### 3.4. Privacy Amplification

- To mitigate potential partial information leakage to an eavesdropper, Alice and Bob apply hash functions or privacy amplification techniques.
- This produces a shorter, final secret key that is provably secure.

## 4. QKD PROTOCOLS

Several QKD protocols define how qubits are encoded, transmitted, and measured:

- BB84 Protocol (1984, Bennett & Brassard): First and most widely used protocol, based on polarization states of photons.
- E91 Protocol (1991, Ekert): Uses entangled photon pairs and Bell's theorem for security.
- Decoy State Protocols: Prevent photon-number-splitting (PNS) attacks in practical implementations.
- Continuous-Variable QKD (CV-QKD): Encodes key information in quadratures of light instead of discrete photons, compatible with telecom infrastructure.

## 5. SYSTEM ARCHITECTURE OF QKD

A QKD system typically consists of:
**Quantum Channel:** Optical fiber, free-space optics, or satellite-based communication.
**Classical Channel:** A standard communication channel (e.g., Internet) for public discussion of measurement bases and error correction.
**Quantum Source:** Single-photon source or weak coherent laser.
**Quantum Detectors:** Single-photon detectors or homodyne detectors (for CV-QKD).

**Post-Processing Unit:** Hardware/software implementing sifting, error correction, and privacy amplification.

## 6. SECURITY OF QKD

QKD offers information-theoretic security because:

- Any eavesdropping attempt introduces errors detectable by QBER.
- Security proofs exist against classical and quantum adversaries.
- However, practical challenges include side-channel attacks, detector vulnerabilities, and photon loss over long distances.

## 7. APPLICATIONS OF QKD

**Government & Military:** Ultra-secure communication links.
**Financial Institutions:** Protection of high-value transactions.
**Healthcare & Research:** Secure sharing of medical/genomic data.
**Telecom & Cloud Providers:** Integration into next-generation secure networks.

## 8. LIMITATIONS & CHALLENGES

**Distance Limitation:** Fiber-based QKD limited to ~300 km (without repeaters).
**High Cost:** Specialized hardware like single-photon detectors.
**Integration Complexity:** Requires hybrid architectures with classical cryptography.

## 9. FUTURE DIRECTIONS

**Quantum Repeaters:** To extend secure QKD over thousands of kilometers.
**Satellite-Based QKD:** Demonstrated by China’s Micius satellite, enabling global QKD.
**Integration with Post-Quantum Cryptography (PQC):** Hybrid models for practical deployment

## 10. CONCLUSION

QKD represents a paradigm shift in secure communication, moving from computational security to physical security. By harnessing quantum principles, it provides a path toward unconditionally secure key distribution, making it a cornerstone technology for future quantum communication networks.