QUANTU M KEY DISTRIBUTION (QKD)

Abstract—Private-key ciphers such as the One Time Pad are the only cryptographic systems with mathematically proven security, even against an adversary using a quantum computer. However, the One Time Pad is rarely used in practice due to the difficulty of secretly generating and distributing the long, random keys it requires. Quantum key distribution algorithms exploit the physical properties of quantum bits to provide a method for two parties to establish a shared key with guaranteed security. This paper will examine two of the most common protocols for quantum key distribution and provide a basic simulation and analysis of each.

Methodology

BB84 Protocol

- Key Generation: Alice uses a truly random generator to create raw keys encoded into photon states using two bases:
- X-Basis: Vertical (|0⟩) & Horizontal (|1⟩) polarization.
- Z-Basis: Diagonal (|+⟩) & Antidiagonal (|−⟩) polarization.
- Photon Transmission: Encoded photons are sent to Bob through a quantum channel.
- Bob's Measurement: Bob measures photons using a random basis (X or Z) and communicates his choices.
- Key Sifting: Alice and Bob compare bases, retaining only matching results to form the "sifted key."
- Eavesdropping Detection: Subsets of the sifted keys are shared to calculate Quantum Bit Error Rate (QBER), detecting potential interference.

B92 Protocol

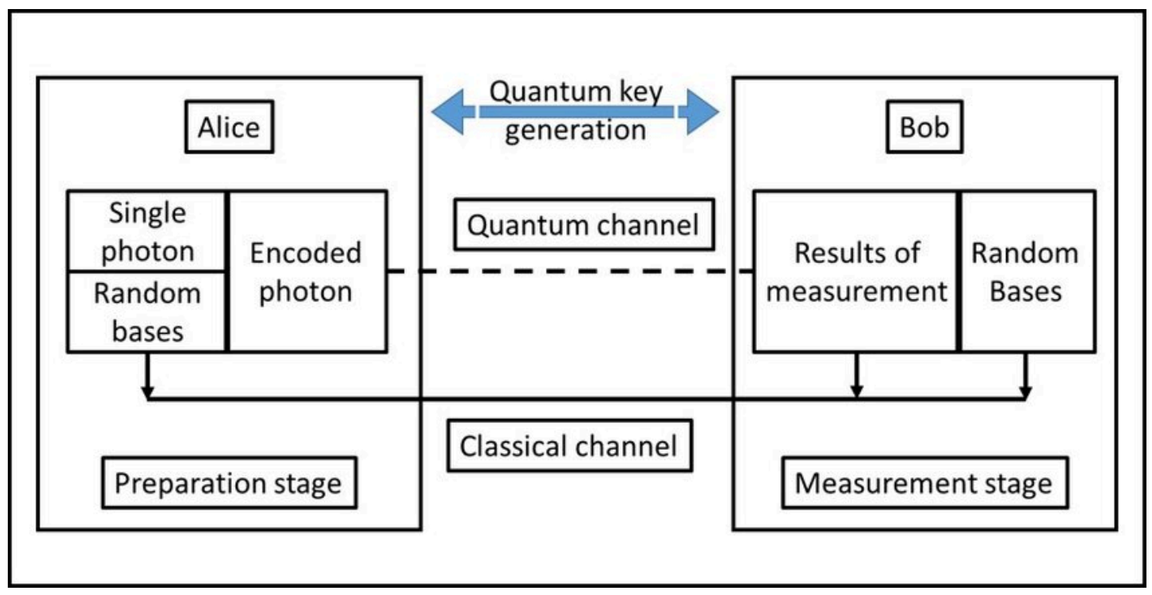
- Key Generation: Alice encodes her raw key using only two non-orthogonal states:
- “0” as Vertical (|↑⟩) and “1” as Diagonal (|−⟩).
- Photon Transmission: Encoded photons are transmitted to Bob.
- Bob’s Measurement: Photons are tested using polarization filters aligned to detect the expected state.
- Key Generation: Bob announces conclusive measurements. Alice derives the shared key based on her encoding.
- Eavesdropping Detection: Actual qubit loss rates are compared to expected values to detect channel manipulation.

Simulation

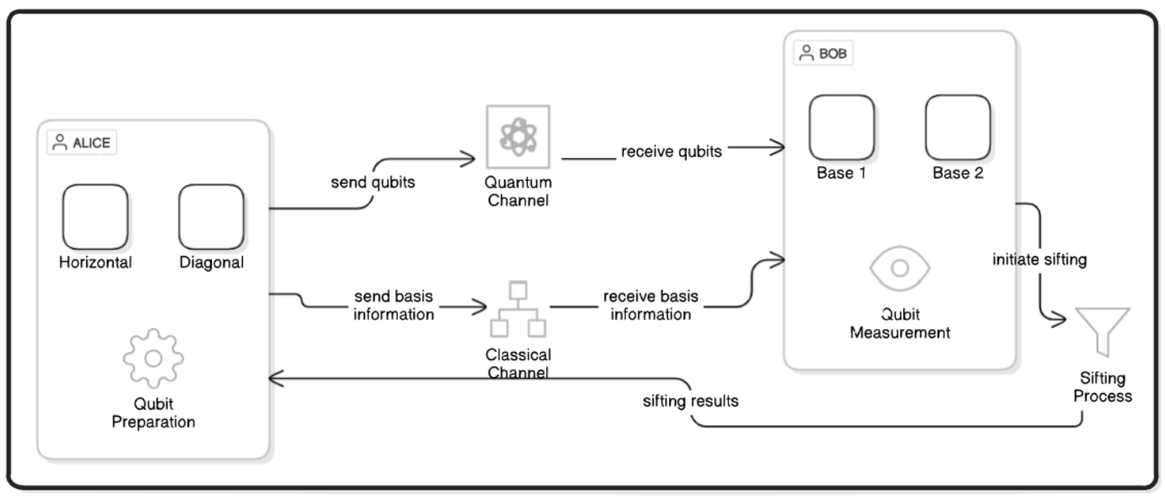
- Implementation: Simulated the BB84 and B92 protocols using Python-based quantum libraries (e.g., Qiskit).
- Eavesdropping Scenarios: Introduced interception-resend attacks to measure their impact on key security.
- Metrics Evaluated:
  - Quantum Bit Error Rate (QBER): Evaluated error rates due to eavesdropping and channel noise.
  - Key Efficiency: Measured the retention rate of sifted keys for secure communication.

Architecture

BB84 Protocol



B92 Protocol



Results

Aspect	BB84 Protocol	B92 Protocol
Without Eavesdropping	- Matching secret keys generated after discarding mismatched bases. - Secure and reliable key exchange.	- Uses two quantum states, simplifying implementation. - High photon loss (75% discarded), reducing efficiency.
With Eavesdropping	- Eve’s interference causes detectable key mismatches. - Errors highlight eavesdropping during verification if error rate is tolerable.	- Eve can exploit discarded photons or manipulate channel loss rates. - Vulnerable to subtle attacks, less secure.

Group Members::

Ahmed Mustafa (21K-4502)

Laiba Nadeem (21K-3398)

Maha Fatima (21K-3180)