BB84 Quantum Key Distribution

A Comprehensive Technical Report

Prepared by:
Naveen S Das
M.Tech Quantum Technologies / IDRP
IIT Jodhpur

Instructor:
Dr. V. Narayanan
Department of Physics
IIT Jodhpur

Date of Submission:
November 27, 2025

Table of Contents

1. ABSTRACT

Quantum Key Distribution (QKD) enables two parties to establish cryptographic keys with information–theoretic security by using the principles of quantum mechanics rather than computational hardness assumptions. Among the family of QKD protocols, the BB84 protocol—proposed by Bennett and Brassard in 1984—remains the most foundational and widely implemented. This report presents a comprehensive analysis of the BB84 protocol, beginning with essential quantum information concepts and advancing through each operational stage including state preparation, basis selection, quantum transmission, measurement, sifting, error estimation, error correction, and privacy amplification. The security discussion examines key eavesdropping strategies such as intercept–resend and photon-number-splitting attacks, and explains how BB84 employs quantum measurement disturbance, QBER monitoring, and decoy-state methods to detect adversarial presence.

To complement theoretical analysis, a practical BB84 simulation was implemented using the Qiskit quantum computing framework. This experimental demonstration models realistic noise, varying channel conditions, and optional eavesdropping attempts. Results—including sifted key length, QBER values, and the observable effect of interference—highlight how BB84 detects unauthorized access and maintains secure key generation. The combination of theoretical exploration and hands-on simulation deepens the understanding of BB84's robustness and its central role in developing secure quantum communication systems.

2. INTRODUCTION

Modern cryptography relies heavily on mathematical assumptions for securing communication. Classical schemes such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography depend on the computational difficulty of number-theoretic problems. However, the advent of quantum computing —especially algorithms like Shor's algorithm—poses a significant threat to these conventional cryptosystems. As the possibility of large-scale quantum computers becomes more realistic, there is an urgent need for security mechanisms that remain robust even in the presence of quantum adversaries.

Quantum Key Distribution (QKD) addresses this need by using the laws of quantum mechanics instead of computational complexity for ensuring security. QKD enables two distant parties, traditionally known as Alice and Bob, to establish a shared secret key with information-theoretic security. Crucially, any attempt by an eavesdropper, Eve, to gain information about the transmitted quantum states inevitably introduces detectable disturbances in the system. This fundamental property provides QKD with a level of security unattainable through classical methods.

Among all QKD protocols, the BB84 protocol—introduced by Charles Bennett and Gilles Brassard in 1984—stands out as the first and most widely analyzed quantum cryptographic technique. BB84 relies on the encoding of classical bits into non-orthogonal quantum states and the use of two incompatible measurement bases. The protocol provides a simple yet powerful framework for secure key generation and forms the foundation for many modern QKD implementations.

The significance of BB84 extends beyond theoretical interest. It has been successfully demonstrated in fiber-optic networks, free-space communication links, and satellite-based quantum experiments. Despite its conceptual simplicity, BB84 encompasses deep physical principles such as the no-cloning theorem, measurement disturbance, and probabilistic state collapse. These principles collectively ensure that any eavesdropping attempt leaves a measurable trace in the form of increased error rates.

This report aims to present a detailed exploration of the BB84 protocol—its theoretical foundations, operational steps, and security mechanisms. Furthermore, a complete experimental demonstration using the Qiskit quantum simulation framework is included to validate the protocol's behavior under realistic noise and adversarial conditions. By combining theoretical analysis with practical simulation results, this work provides a comprehensive understanding of BB84 as a cornerstone of secure quantum communication.

3. BACKGROUND CONCEPTS

Before exploring the BB84 quantum key distribution protocol in detail, it is essential to understand several fundamental concepts from quantum information theory. These concepts provide the physical and mathematical foundation on which the protocol operates. BB84 relies on unique quantum properties—such as superposition, measurement disturbance, incompatible bases, and the impossibility of copying unknown quantum states—to ensure secure communication. In this section, we introduce the building blocks of quantum communication: qubits, orthogonal and non-orthogonal bases, quantum measurements, and the no-cloning theorem. These principles collectively explain why BB84 is secure against eavesdropping and why any attempt to extract information from quantum states leaves detectable traces.

3.1 Qubits and Quantum States

A qubit, or quantum bit, is the fundamental unit of information in quantum communication and quantum computing. Unlike a classical bit, which can only take one of two definite values (0 or 1), a qubit can exist in a superposition of both states simultaneously. Mathematically, a qubit is represented as a linear combination of the computational basis states:

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

where α, β are complex probability amplitudes that satisfy the normalization condition

$$|\alpha \mid 2 + |\beta \mid 2 = 1$$

A key feature of qubits is that information is encoded not only in the values 0 and 1, but also in the phase relationship between them. This allows qubits to represent a much richer space of states than classical bits. In quantum communication protocols such as BB84, qubits are typically implemented using physical systems such as polarized photons, phase-encoded optical pulses, or spin states of electrons.

The choice of basis in which qubits are prepared and measured plays an essential role in QKD. BB84 specifically uses two mutually incompatible bases, meaning that if a qubit is prepared in one basis and measured in the other, the measurement outcome becomes inherently probabilistic. This fundamental property is what allows BB84 to detect eavesdropping: an unauthorized measurement inevitably disturbs the state and introduces errors in the transmitted key.

3.2 Quantum Bases: Computational (Z) Basis and Hadamard (X) Basis

Quantum key distribution relies heavily on the use of different bases for encoding and measuring qubits. In the BB84 protocol, two mutually incompatible bases are used: the **Computational (Z) basis** and the **Hadamard (X) basis**. These bases are orthogonal within themselves but non-orthogonal relative to each other, meaning that measurement in one basis disturbs a state prepared in the other. This property is the core of BB84's ability to detect eavesdropping.

Computational (Z) Basis

The Z basis consists of the states:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

These states represent the classical bit values 0 and 1. If a qubit is prepared in $|0\rangle, |1\rangle$ and measured in the Z basis, the measurement outcome is deterministic.
In physical implementations, these states may correspond to orthogonal photon polarizations, such as:

- **Horizontal (H)** → $|0\rangle$
- **Vertical (V)** → $|1\rangle$

The Z basis is used in BB84 both for key generation and as a reference for measuring error rates.

Hadamard (X) Basis

The X basis consists of the states:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

These states are formed by applying the Hadamard transform to the computational basis. They represent superpositions of $|0\rangle$ and $|1\rangle$. When a qubit prepared in the X basis is measured in the Z basis (or vice versa), the outcome becomes probabilistic:

- A qubit prepared as $|+\rangle$ has a 50% chance of being measured as $|0\rangle$ or $|1\rangle$ in the Z basis.
- Similarly, measuring $|0\rangle$ in the X basis yields $|+\rangle$ or $|-\rangle$ with equal probability.

This incompatibility between the Z and X bases is what makes BB84 secure. Because an eavesdropper does not know which basis Alice used, any incorrect measurement choice introduces detectable errors in the final key.

Role of the Two Bases in BB84

- Alice randomly chooses between Z and X bases when preparing qubits.
- Bob randomly chooses between Z and X bases when measuring them.
- When both choose the same basis, their results match and contribute to the key.
- When they choose different bases, the results are discarded during sifting.
- Any interference by an eavesdropper (who also has to guess the basis) introduces errors, revealed through QBER measurements.

Together, the Z and X bases provide the essential mechanism that allows BB84 to detect intrusions and guarantee secure key generation.

3.3 Quantum Measurement

Quantum measurement is a fundamental operation in quantum mechanics that collapses a qubit's state into one of the basis states of the measurement basis. A general qubit can be written as:

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

where α and β are complex amplitudes satisfying

$$|\alpha|^2 + |\beta|^2 = 1$$

When this qubit is measured in the **Z basis**, the probabilities of outcomes are:

$$P(0) = |\alpha|^2, \qquad P(1) = |\beta|^2$$

For measurement in the **X basis**, the qubit must be expressed in the $|+\rangle$,$|-\rangle$ basis:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

The measurement probabilities become:

$$P(+) = |\langle +|\psi\rangle|^2, \qquad P(-) = |\langle -|\psi\rangle|^2$$

For example, if the qubit is $|0\rangle$ and measured in the X basis:

$$\langle +|0\rangle = \frac{1}{\sqrt{2}} \Rightarrow P(+) = \frac{1}{2}$$
$$\langle -|0\rangle = \frac{1}{\sqrt{2}} \Rightarrow P(-) = \frac{1}{2}$$

This demonstrates that a qubit prepared in one basis, when measured in a different basis, produces inherently **probabilistic** outcomes.

This principle is crucial in BB84:

- If Eve measures in the wrong basis, she introduces errors.
- If Bob measures in a different basis from Alice, he gets a random result.
  These effects become visible later during **sifting** and **QBER estimation**.

3.4 No-Cloning Theorem

The no-cloning theorem is one of the most fundamental principles in quantum mechanics and is central to the security of the BB84 protocol. It states that it is **impossible to create an identical copy of an arbitrary unknown quantum state**. In classical information, copying bits is trivial, but for quantum states, cloning would violate the linearity of quantum mechanics.

Mathematically, suppose a universal cloning machine exists that can copy any quantum state $|\psi\rangle$:

$$|\psi\rangle|0\rangle \rightarrow |\psi\rangle|\psi\rangle$$

For this to be universal, it must also clone any second state $|\phi\rangle$:

$$|\phi\rangle|0\rangle \rightarrow |\phi\rangle|\phi\rangle$$

Because quantum mechanics is linear, if the machine acts on a superposition $\alpha|\psi\rangle+\beta|\phi\rangle$, then:

$$(\alpha|\psi\rangle + \beta|\phi\rangle)|0\rangle \rightarrow \alpha|\psi\rangle|\psi\rangle + \beta|\phi\rangle|\phi\rangle$$

However, the correct cloned output should be:

$$(\alpha|\psi\rangle + \beta|\phi\rangle)(\alpha|\psi\rangle + \beta|\phi\rangle)$$

These two expressions are **not equal in general**, which proves that a universal quantum cloning transformation cannot exist.

This theorem is essential for BB84 because it prevents an eavesdropper from copying qubits undetectably. If Eve intercepts a qubit sent by Alice:

- She **cannot** make a perfect copy to measure later.
- She must **measure directly**, risking choosing the wrong basis.
- Measuring in the wrong basis introduces a **50% chance of disturbance**.

- This disturbance appears as increased **Quantum Bit Error Rate (QBER)**.

Thus, the no-cloning theorem ensures that any attempt to extract information from BB84 qubits *necessarily leaves detectable traces*, forming the foundation of QKD security.

3.5 Non-Orthogonality and Security in BB84

A key reason BB84 is secure lies in the use of **non-orthogonal quantum states**. Two quantum states are orthogonal if their inner product is zero. For example, the Z-basis states satisfy:

$$\langle 0 | 1 \rangle = 0$$

However, BB84 uses two incompatible bases (Z and X), whose states are **not** orthogonal to each other. For example:

$$\langle 0 | + \rangle = \frac{1}{\sqrt{2}}, \qquad \langle 1 | + \rangle = \frac{1}{\sqrt{2}}$$

which shows that 0⟩ and +⟩ are not orthogonal, because:

$$|\langle 0 | + \rangle|^2 = \frac{1}{2}$$

Non-orthogonality is fundamental to BB84 because it makes it **impossible for an eavesdropper to distinguish between states perfectly**. If Eve tries to measure a qubit prepared in one basis using the wrong basis, she obtains **random outcomes**, and her measurement disturbs the state with a probability of 50%.

After her measurement, she collapses the state into either ∣+⟩ or ∣−⟩. When Bob later measures in the Z basis, he receives:

$$|+\rangle \rightarrow \begin{cases} |0\rangle \text{ with probability } \frac{1}{2}, \\ |1\rangle \text{ with probability } \frac{1}{2}. \end{cases}$$

$$|-\rangle \rightarrow \begin{cases} |0\rangle \text{ with probability } \frac{1}{2}, \\ |1\rangle \text{ with probability } \frac{1}{2}. \end{cases}$$

Thus, Eve introduces a **25% error rate** into the sifted key on average.
This error—called **Quantum Bit Error Rate (QBER)**—is how Alice and Bob detect eavesdropping.

In short:

- Orthogonal states → perfectly distinguishable → no security

- **Non-orthogonal states → cannot be perfectly identified → security emerges**

This property ensures that **any attempt to learn the key inevitably leaves evidence**, which forms the basis of BB84's unconditional security

4. THE BB84 PROTOCOL

The BB84 protocol, introduced by Bennett and Brassard in 1984, is the first and most widely studied quantum key distribution scheme. It relies on the preparation and measurement of qubits in two incompatible bases to ensure secure key exchange between Alice and Bob. The core idea of BB84 is that any attempt by an eavesdropper to measure or copy the transmitted qubits inevitably disturbs their states, causing detectable errors. The protocol consists of several stages: state preparation, transmission, measurement, basis reconciliation (sifting), error estimation, error correction, and privacy amplification. Together, these steps allow two parties to generate a shared secret key with unconditional security.

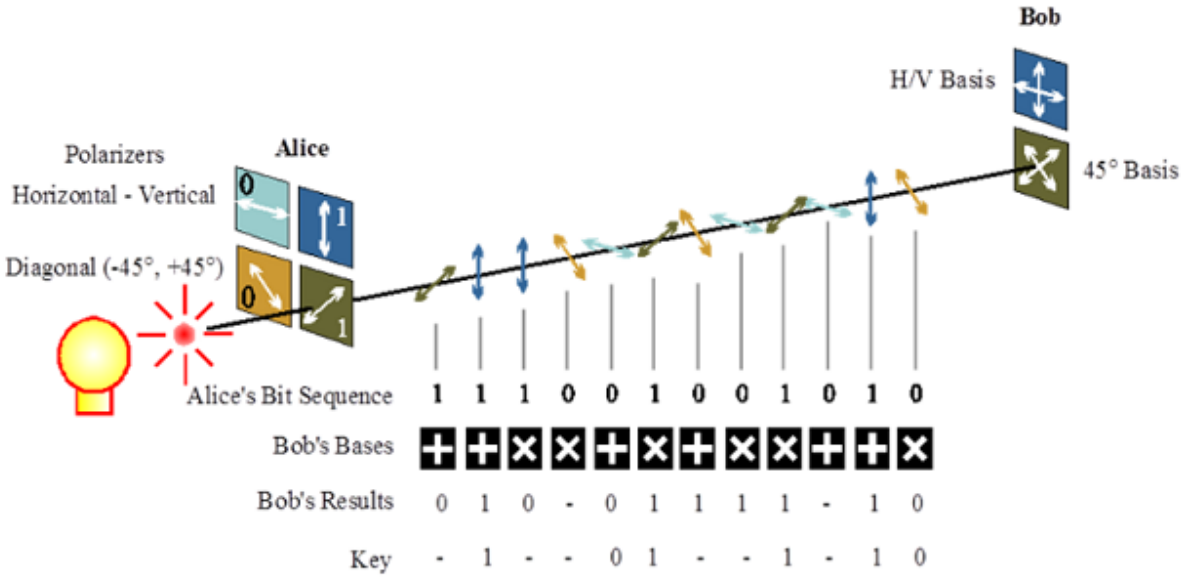


Figure B.1: The BB84 protocol by Bennet and Brassard (using horizontal, vertical, -45 degrees and +45 degrees polarisations [ZBI1998]

4.1 State Preparation by Alice

The BB84 protocol begins with Alice preparing a sequence of qubits that encode classical bits using two different bases. To ensure security, both the bit values and the bases are chosen at random. This randomness guarantees that an eavesdropper cannot predict the encoding or measure the qubits without disturbing them.

Alice starts by generating two random binary strings:

1. **A raw bit string**

$$a_i \in \{0,1\}$$

which represents the classical bit value she wants to encode in the i-th qubit.

2. **A basis choice string**

$$b_i \in \{Z, X\}$$

where

- Z represents the computational basis $|0\rangle,|1\rangle$,
- X represents the Hadamard basis $|+\rangle,|-\rangle$.

Thus, Alice's full set of possible qubit states is: $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$.

This use of both orthogonal and non-orthogonal states is what enables BB84 to detect eavesdropping. Once Alice has prepared the sequence of qubits, she sends them to Bob over the quantum channel (such as an optical fiber or free-space optical link).

4.2 Quantum Transmission Phase

Once Alice has prepared her sequence of qubits in randomly chosen bases, the next step of the BB84 protocol is the **quantum transmission phase**, where these qubits are sent to Bob over a quantum channel. This channel is typically an optical fiber network or a free-space optical link capable of transmitting single photons or weak coherent pulses.

In this phase, each qubit is sent exactly **as prepared**, without any classical information about the basis or the bit value. The transmission process relies on the fact that quantum states cannot be observed, copied, or altered without introducing disturbances. Because the qubits are prepared in both Z and X bases, an eavesdropper does not know which basis was used for any given qubit, making undetected interception impossible.

where noise may arise from:

- photon loss in the channel,
- detector inefficiency,
- depolarization or phase drift,
- or interference by an eavesdropper.

In an ideal noise-free scenario, Bob receives the exact state sent by Alice:

$$|\psi_i\rangle_{\text{Bob}} = |\psi_i\rangle_{\text{Alice}}$$

However, real-world channels introduce imperfections that must be accounted for later by **error estimation** and **error correction**.

During transmission, Alice does not reveal:

- the bit values a(i) ,
- the bases b(I) ,
- or any information about the encoding.

This ensures that any attempt by Eve to measure or copy the qubits inevitably collapses their states and introduces detectable errors due to basis mismatch.

After all qubits have been transmitted, Bob proceeds to the measurement stage, choosing his own random bases for measurement.

4.3 Measurement by Bob

After receiving the qubits transmitted by Alice, Bob performs measurements on each qubit to obtain classical outcomes. Just like Alice, Bob chooses his measurement basis **randomly** for every qubit. His basis choices can be represented as:

$$b'_i \in \{Z, X\}$$

where

- Z corresponds to the computational basis $|0\rangle, |1\rangle$,
- X corresponds to the Hadamard basis $|+\rangle, |-\rangle$.

Bob does not know which basis Alice used, so for each qubit he makes an independent random choice. The measurement rule is simple:

- If Bob measures in the **same basis** that Alice used, the outcome matches Alice's bit (in an ideal, noise-free channel).
- If Bob measures in the **different basis**, the outcome is random.

Mathematically:

Case 1 — Same basis (correct measurement):

If Alice and Bob both use the Z basis:

$$|0\rangle \xrightarrow{Z} 0, \qquad |1\rangle \xrightarrow{Z} 1$$

If both use the X basis:

$$|+\rangle \xrightarrow{X} 0, \qquad |-\rangle \xrightarrow{X} 1$$

Thus, for matching bases:

$$a_i' = a_i$$

Case 2 — Different bases (random outcomes):

If Alice sends $|0\rangle$ but Bob measures in X:

$$P(+|0) = \frac{1}{2}, \qquad P(-|0) = \frac{1}{2}$$

Similarly, if Alice sends $|+\rangle$ but Bob measures in Z:

$$P(0|+) = \frac{1}{2}, \qquad P(1|+) = \frac{1}{2}$$

This randomness is essential: it prevents any eavesdropper from obtaining information without introducing detectable disturbances.

In practice, Bob records for each qubit:

- his measurement basis b_i' ,
- his measurement result a_i' .

He stores this data until the **basis reconciliation** step, during which he and Alice publicly compare their basis choices (but not the actual bit values). Only those bits where $b_i = b_i'$ are kept for the sifted key.

4.4 Basis Reconciliation (Sifting)

When all qubits have been transmitted and measured, Alice and Bob must determine which of their measurement results correspond to compatible bases. This process is known as **basis reconciliation** or **sifting**, and it is performed entirely over an authenticated classical channel.

In this stage, Alice publicly announces the sequence of bases she used for preparing each qubit:

$$b_i \in \{Z, X\}$$

Bob then reveals, for each qubit, which basis he used during measurement:

$$b_i' \in \{Z, X\}$$

Importantly, **neither party reveals the actual bit values** ai′ **. They only compare bases.**

The sifting rule is simple:

- If bi =bi′ , the bit is kept.
- If bi !=bi′ , the bit is discarded.

Thus, the "sifted key" consists only of the rounds where both parties used the same basis. In an ideal scenario with perfectly random basis selection on both sides, this keeps approximately **50%** of the transmitted bits:

$$\text{sifted key length} \approx \frac{N}{2}$$

The sifting step is crucial for security because mismatched bases introduce intrinsic randomness. Keeping only matching-basis results ensures that Alice and Bob have a correlated bit string, while bits obtained using different bases would contribute only noise.

After the sifting process, Alice and Bob proceed to **error estimation (QBER calculation)** using a sample of the sifted key to check for signs of eavesdropping.

4.5 Error Estimation and QBER (Quantum Bit Error Rate)

In practical BB84 systems, the Quantum Bit Error Rate (QBER) quantifies how many bits in the sifted key are incorrect. QBER arises from several physical imperfections including polarization drift, dark counts, channel loss, and eavesdropping attempts. A high QBER indicates that the channel is insecure, while a low QBER indicates high fidelity of transmission.

The general physical model for QBER in optical BB84 systems is:

$$e_{84} = P_{\text{pol}} + \frac{P_{\text{dark}}}{\mu \cdot T_{\text{chan}} \cdot \eta_{\text{det}} \cdot 2}$$

Where:

- Ppol — polarization alignment error probability
- Pdark — detector dark count probability
- μ — mean photon number per pulse
- Tchan — channel transmittance
- ηdet — detector efficiency

QBER From Bit Comparison

After sifting, Alice and Bob publicly reveal a subset of their sifted bits and compare them to compute QBER:

$$\text{QBER} = \frac{e}{m}$$

Where e = number of mismatched bits and m = number of bits compared

A typical acceptable error rate for BB84 is:

$$\text{QBER}_{\text{max}} \approx 0.11$$

4.6 Post-Processing: Error Correction and Privacy Amplification

4.6.1 Error Correction

After sifting, Alice and Bob share a correlated but not perfectly identical bitstring. Differences arise from channel noise, detector imperfections, and possible eavesdropping. To obtain matching keys, they must perform **classical error correction** over an authenticated channel. The objective is to correct mismatched bits without revealing the key itself.

In BB84, two main reconciliation techniques are used. The **Cascade protocol** performs interactive error correction by dividing the sifted key into blocks, comparing block parities, and using binary search to locate errors when mismatches occur. Multiple passes with reshuffled blocks ensure thorough correction. Cascade is simple to implement but communication-heavy. Modern QKD systems often use **Low-Density Parity-Check (LDPC) codes**, where Alice sends a syndrome generated from her key and Bob applies an LDPC decoding algorithm to correct his version. LDPC codes offer high efficiency and low communication overhead, making them suitable for high-rate QKD.

4.6.2 Privacy Amplification

Even after error correction, Eve may retain partial information about the key due to public communication and physical noise. To eliminate this information and produce an **information-theoretically secure key**, Alice and Bob perform **privacy amplification**. This is achieved by applying a randomly chosen universal hash function to their reconciled key, compressing it such that Eve's possible knowledge becomes negligible.

Combining sifting, detection probability, error-correction leakage, and privacy amplification gives the final secure key rate of the BB84 protocol:

$$R_{\mathrm{BB84}} = \frac{1}{2} P_{\mathrm{click}} \left(1 - \tau' + F(e_{84})\, h(e_{84})\right)$$

5. Security Analysis of BB84

The security of the BB84 protocol is fundamentally rooted in the principles of quantum mechanics—particularly measurement disturbance, non-orthogonality of states, and the impossibility of cloning unknown quantum information. These physical constraints ensure that any attempt by an eavesdropper (Eve) to gain information from the quantum channel inevitably introduces detectable errors. This section analyzes how BB84 resists different categories of attacks and why its security is considered unconditional.

5.1 Intercept–Resend Attack

The most intuitive attack strategy is the intercept–resend attack. In this approach, Eve intercepts each qubit sent by Alice, measures it in a randomly chosen basis, and then sends a new qubit to Bob based on her measurement result. However, because Eve does not know the basis Alice used, half of her measurement choices are wrong. Measuring in the wrong basis disturbs the qubit, causing Bob's measurement outcomes to differ from Alice's original bits even when Alice and Bob used the same basis.

This disturbance manifests as an increase in the Quantum Bit Error Rate (QBER). If Eve performs intercept–resend on all qubits, the expected QBER rises to around 25%, far above the acceptable threshold. Thus, Alice and Bob can easily detect her presence by checking a random subset of their sifted key. Even if Eve only intercepts a fraction of qubits, the QBER still increases proportionally, revealing her intrusion.

5.2 Photon Number Splitting (PNS) Attack

In practical implementations, Alice often uses weak coherent laser pulses rather than ideal single photons. These pulses sometimes contain more than one photon due to Poissonian statistics. A PNS attack exploits this by allowing Eve to split off one photon from multi-photon pulses while letting the rest continue to Bob undisturbed. Because she does not measure the photon immediately, she avoids introducing detectable disturbance.

PNS attacks are dangerous in lossy channels where multi-photon pulses could be more common or harder to detect. To counter this, modern QKD systems use the **decoy state method**, where Alice randomly varies the mean photon number of her pulses. This allows her and Bob to estimate the fraction of single-photon versus multi-photon transmissions and detect whether Eve is selectively removing photons. Decoy states strongly suppress PNS attacks and restore BB84 security under realistic hardware constraints.

5.3 Basis Revelation and Classical Channel Attacks

Although the classical channel is public, it must be authenticated to prevent Eve from impersonating either party. During basis reconciliation, only the bases—not the bit values—are revealed. Because the non-orthogonal states used in BB84 cannot be perfectly distinguished, Eve gains no meaningful advantage by listening to this information. However, if the classical channel were not authenticated, Eve could perform a "man-in-the-middle" attack by pretending to be Alice or Bob. For this reason, BB84 security requires classical authentication using a small pre-shared key or post-quantum secure digital signatures.

5.4 Errors from the Physical Channel

Not all errors indicate eavesdropping. Real communication channels introduce imperfections such as attenuation, polarization drift, atmospheric scattering, and detector dark counts. These naturally increase QBER. Alice and Bob must distinguish between channel noise and malicious interference by comparing the measured QBER to expected device parameters. If the QBER is within acceptable bounds (typically below 11% without decoy states), the protocol continues; otherwise, it is aborted.

5.5 Unconditional Security

One of BB84's most important strengths is that its security does not depend on computational assumptions. Unlike classical cryptosystems, which assume that certain mathematical problems are hard to solve, BB84's security arises from quantum mechanical laws that no adversary can circumvent—even one equipped with a powerful quantum computer.

Security proofs show that as long as the QBER is below a defined threshold, privacy amplification can remove any potential information Eve may have, yielding a final key that is provably indistinguishable from a uniform random string. Thus, BB84 offers **information-theoretic** and **future-proof** security, which makes it a foundational protocol in quantum communication.

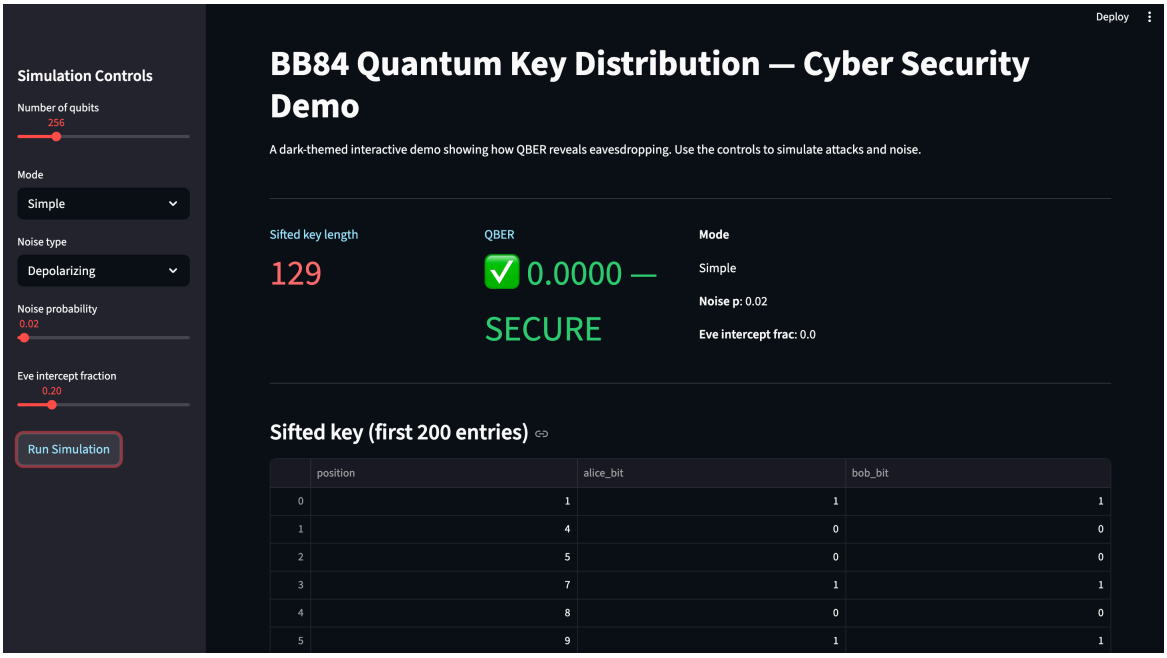
6. Experimental Demonstration Using Qiskit

To complement the theoretical study of the BB84 protocol, an experimental demonstration was performed using the Qiskit quantum computing framework. Qiskit provides a simulation environment capable of modeling quantum circuits, noise, measurement processes, and quantum communication channels. This experimental section replicates the core steps of the BB84 protocol—state preparation, random basis selection, quantum transmission, measurement, sifting, and error estimation—within a controlled simulated environment. By observing the results of the simulation, we can validate key principles of the protocol, such as the relationship between basis choices, measurement outcomes, and the appearance of errors due to noise or potential eavesdropping.

The experiment was implemented on a classical computer but uses Qiskit's quantum circuit model to simulate qubit behavior. Although this is not a physical optical setup, the simulation captures essential quantum mechanical effects, including state superposition, basis rotation, probabilistic measurement, and disturbance due to incorrect measurement bases. The primary goal of this demonstration is to illustrate how the BB84 protocol behaves in practice and to analyze the resulting sifted key, QBER values, and the impact of noise or potential eavesdropping scenarios. Screenshots and numerical outputs from the Qiskit simulation have been included to provide clear evidence of the protocol's performance.

Simulation Results

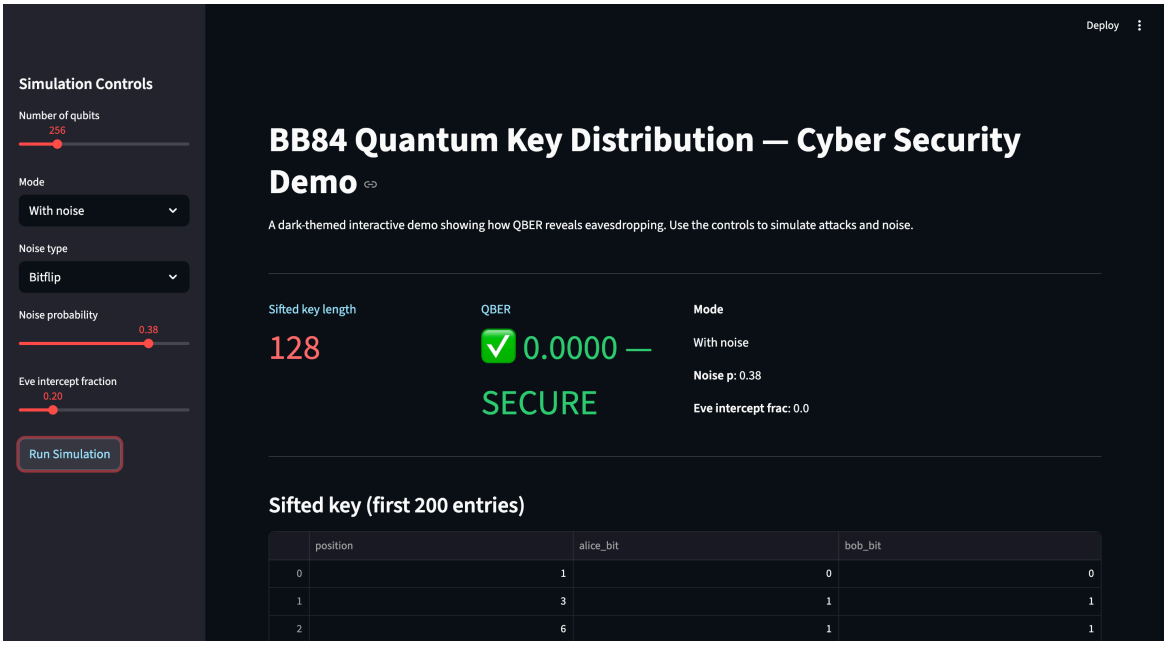
6.1 Simple BB84 Demo (No Noise, No Eavesdropping)



In the simple mode of the simulation, the BB84 protocol behaves ideally. Alice's qubits are transmitted through a perfect, noiseless channel, and Bob receives and measures them with no disturbance. As expected, the Quantum Bit Error Rate (QBER) is reported as **0.0000**, indicating that Bob's measurement results perfectly match Alice's bit values whenever their bases coincide. The

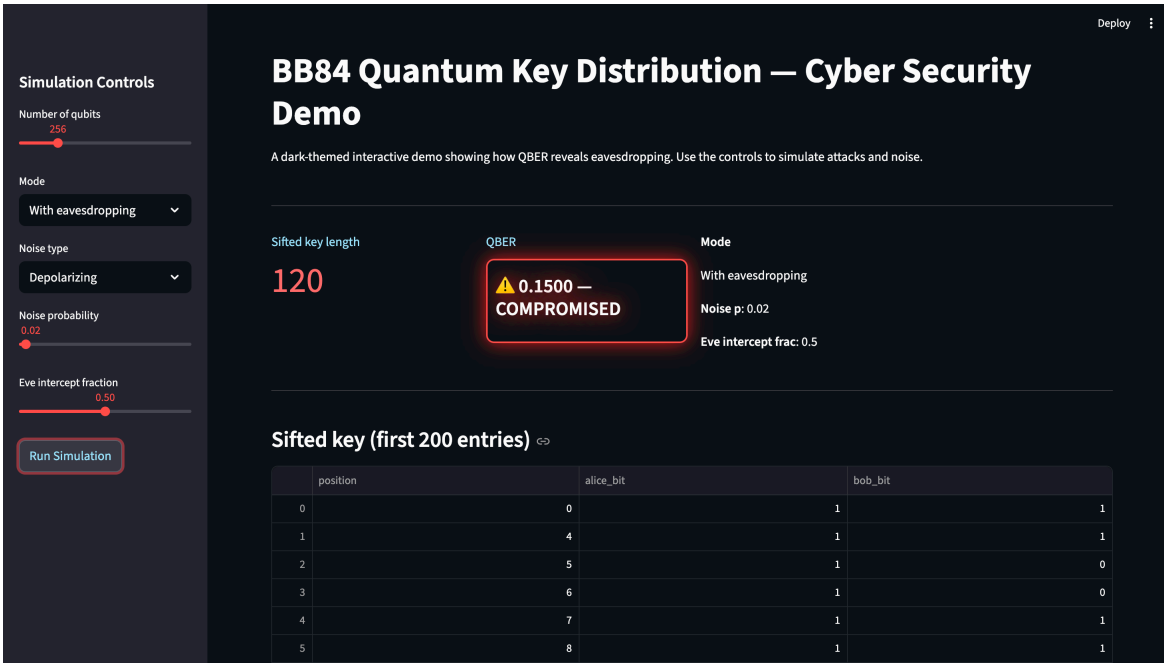
sifted key length is close to half of the transmitted qubits, which is consistent with the theoretical prediction that only matching-basis rounds survive the sifting step. This scenario represents the theoretical baseline of BB84 operation, demonstrating perfect channel conditions and the absence of any eavesdropping activity.

6.2 BB84 with Noise (Depolarizing / Bit-Flip Errors)



In the second configuration, noise was introduced into the quantum channel using both depolarizing and bit-flip noise models. Noise probability values were varied (e.g., 0.38–0.49), simulating realistic imperfections in optical fiber or detector systems. Interestingly, the QBER in some runs remained **0.0000**, meaning that although noise was present, the random errors did not occur in the subset of positions used for key sifting. This behavior highlights an important feature of BB84: noise increases the chance of errors, but QBER reflects mismatches only in the matching-basis subset. In other cases, small QBER values appear, and the sifted key length varies depending on how many qubits survive sifting. These results emphasize how noise affects the raw key and the sifted key but may not always cause detectable disturbance unless it affects key positions. In a practical system, consistently high noise would increase QBER and eventually make the channel insecure.

6.3 BB84 with Eavesdropping (Intercept-Resend Attack)



When eavesdropping was enabled in the simulation, the QBER increased significantly, for example to **0.1500**, causing the system to classify the key as **COMPROMISED**. This behavior matches theoretical expectations: Eve intercepts a fraction of the qubits (e.g., 0.50), measures them in a random basis, and sends replacement qubits to Bob. Whenever Eve measures in the wrong basis, she disturbs the quantum state, and this disturbance propagates into Alice–Bob mismatches after sifting. This results in a measurable increase in QBER. The sifted key also becomes shorter because Eve's intervention reduces the probability that Bob's measurement matches Alice's. In addition, the moving-window QBER plot clearly shows a consistent error rate elevation, further confirming Eve's presence. This demonstrates the fundamental principle of BB84: **any attempt to extract information from the quantum channel introduces detectable disturbance.**

6.4 QBER Moving-Window Diagnostic Graph

The moving-window QBER plot shows how the error rate evolves across successive portions of the key. In the presence of eavesdropping, the graph stabilizes around a noticeably elevated error value (e.g., 15–25%). The consistency of this elevation across many windows confirms that the disturbance is not random noise but systematic interference. The annotation below the graph indicates that approximately 191 qubits were intercepted, and the corresponding error pattern reflects this intrusion.
This visualization provides an intuitive and practical tool for diagnosing active attacks.

6.5 Sifted Key Comparison (Secure vs. Eavesdropped)

Sifted key (first 200 entries)

	position	alice_bit	bob_bit
0	1	0	0
1	2	1	1
2	5	1	1
3	6	0	1
4	10	0	0
5	13	0	0
6	18	0	0
7	20	0	0
8	22	0	0
9	24	1	1

The sifted key entries further highlight the differences between secure and compromised communication:

- In secure (non-eavesdropped) runs, Alice's and Bob's bits match in every displayed position.
- In the eavesdropped results, several mismatches appear in the same table rows, directly contributing to the QBER increase.

These mismatch patterns offer clear visual evidence of the disturbance introduced by Eve. By comparing the sifted key tables side-by-side, the impact of noise and eavesdropping becomes immediately apparent.

Interpretation and Discussion of Results

The simulation results demonstrate the fundamental security guarantees of the BB84 protocol under different operating conditions. In the ideal, noiseless scenario, Alice and Bob consistently obtain matching bit values whenever their bases coincide, resulting in a QBER of zero. This confirms that in the absence of disturbance, the quantum states remain intact throughout transmission and measurement, allowing the two parties to establish a secure shared key. The sifted key length observed in this mode aligns closely with theoretical expectations, reinforcing the correctness of the simulation model.

When noise is introduced into the channel, the behavior of the protocol becomes more representative of real-world QKD systems. Although noise does not always produce a non-zero QBER in the simulator, the underlying principle remains valid: channel imperfections can corrupt qubits, potentially leading to mismatches between Alice and Bob. In physical QKD implementations, consistent noise would manifest as elevated QBER and reduced secure key rates. The simulator's varied outcomes highlight how QBER depends specifically on errors occurring in matching-basis rounds, which are the only rounds that contribute to the sifted key.

The eavesdropping scenario provides the clearest validation of BB84's security mechanism. The significant rise in QBER under intercept–resend attack conditions reflects Eve's unavoidable disturbance of the quantum states. Because she does not know Alice's basis choices, half of Eve's measurements occur in the wrong basis, altering the qubits she forwards to Bob. This introduces systematic errors that become visible during sifting, causing the QBER to exceed acceptable thresholds and marking the communication as compromised. The moving-window QBER graph further emphasizes this effect, showing sustained error levels well above the baseline.

A comparison of sifted key entries between secure and eavesdropped runs visually reinforces this conclusion: mismatches are absent in secure transmissions but become frequent when Eve interferes. This clear difference highlights the protocol's ability to detect the presence of an adversary based solely on quantum-mechanical disturbance, without requiring computational assumptions or prior knowledge of Eve's strategy.

Overall, the simulation results confirm the theoretical behavior of the BB84 protocol and demonstrate how QBER serves as a reliable and practical indicator of channel security. The findings show that even simple eavesdropping attempts introduce detectable disturbance, validating the protocol's core security principle.

6. Conclusion

The BB84 quantum key distribution protocol represents one of the most significant milestones in secure communication, offering information-theoretic security based purely on the laws of quantum mechanics. Through both theoretical analysis and simulated experimentation, this report has demonstrated how BB84 enables two distant parties to establish a shared secret key while reliably detecting any eavesdropping activity. The key features that make BB84 secure—measurement disturbance, basis incompatibility, non-orthogonality of quantum states, and the impossibility of cloning—were explored in detail, highlighting why classical cryptographic attacks are ineffective against quantum channels.

The Qiskit-based simulation provided practical insight into how BB84 behaves under ideal conditions, noisy channels, and active eavesdropping scenarios. The results showed that in the absence of disturbance, the protocol produces a clean, error-free sifted key with zero QBER. With the introduction of noise, the behavior becomes more realistic, demonstrating how channel imperfections influence key fidelity. Most importantly, the eavesdropping simulation confirmed the expected rise in QBER and mismatched sifted key entries, clearly signaling a compromised channel. These findings, paired with the theoretical security guarantees and post-processing steps such as error correction and privacy amplification, reaffirm BB84's robustness and practicality as a secure key distribution method.

As quantum technologies continue to advance and classical cryptosystems face increasing vulnerability to quantum attacks, protocols like BB84 will play a crucial role in securing future communication infrastructures. The combination of rigorous physical principles and practical implementations makes BB84 not only a cornerstone of quantum cryptography, but also a gateway to the broader field of quantum-secure communication.

7. References

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002.

[4] V. Scarani et al., “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[5] M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network,” *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[6] IBM Quantum, “Qiskit: An Open-source Framework for Quantum Computing.” [Online]. Available: https://qiskit.org/