Report QKD

Ismaele Lorenzon - 2195505

December 2025

1 Introduction

1.1 Quantum Key Distribution

Quantum Key Distribution (QKD) is a cryptographic paradigm that leverages the fundamental laws of quantum mechanics to enable the secure exchange of a secret key between communicating parties. Its defining feature is the ability to detect any attempt at eavesdropping: a third-party interception inevitably disturbs the quantum states used for communication, revealing the presence of an attacker. Once a secure key has been established, it can be used in conjunction with standard symmetric encryption schemes for practical data protection.

The principal advantage of QKD lies in its unconditional, or information-theoretic, security. Classical key distribution techniques rely on computational hardness assumptions, such as the difficulty of integer factorization in RSA or the discrete logarithm problem in elliptic-curve cryptography. These assumptions are threatened by advances in computing power—most notably quantum computing—since algorithms like Shor's could efficiently break widely used public-key cryptosystems.

Demand for unconditionally secure communication has therefore grown significantly, especially in sectors such as finance, defense, and critical infrastructure. Although implementing large-scale quantum networks remains an ongoing challenge, QKD has already demonstrated practical feasibility and represents one of the earliest and most mature applications in the broader field of quantum communications.

1.2 The BB84 Protocol

The BB84 protocol was the first fully developed and experimentally feasible Quantum Key Distribution scheme, and remains one of the simplest and most widely deployed. It belongs to the class of Prepare-and-Measure (P&M) protocols, meaning that the sender prepares quantum states in non-commuting bases and the receiver performs measurements that exploit their incompatibility. In our implementation, polarization is used as the degree of freedom, although other encodings such as time-bin or phase are equally valid.

To establish a secret key, Alice and Bob communicate over two distinct channels: a quantum channel for transmitting the quantum states and anauthenticated classical channel for public discussion. Alice prepares single-photon states randomly in either the rectilinear (Z) basis, composed of the horizontal and vertical polarization states $\{|H\rangle, |V\rangle\}$, or in the diagonal (X) basis, composed of $\{|D\rangle, |A\rangle\}$. She sends these states to Bob, who independently and randomly selects a basis in which to measure each photon. After the quantum transmission, Alice publicly discloses her basis choices, and Bob discards all measurement outcomes obtained with mismatched bases. This post-processing step is known as sifting.

Security arises from the fact that any attempt by an eavesdropper (Eve) to intercept and measure the photons inevitably introduces detectable errors due to the no-cloning theorem and the disturbance caused by measurements in incompatible bases. An increase in the measured Quantum Bit Error Rate (QBER) therefore signals a potential intrusion.

Decoy-state techniques are frequently employed in practical implementations. Since weak coherent pulses are often used instead of true single-photon sources, multi-photon emissions can occur and enable photon-number-splitting (PNS) attacks, in which Eve splits off and measures one photon while forwarding the remaining one to Bob without introducing errors. By randomly varying the intensity of the pulses, Alice and Bob can statistically detect such attacks by monitoring variations in channel loss and detection rates across decoy and signal states.

2 Measurements

We analyze 3 different sets of measurements

- *statesRCV.txt* which contains the states received by Bob, encoded in bytes
- *states.txt* which contains the states sent by Alice, encoded in bytes
- *decoy.txt* which encodes the decoy setting, either low or high, again encoded in bytes

The encoding which is used associates each state $|H\rangle, |V\rangle, |D\rangle, |A\rangle$ as a number in each of the bytes and therefore in its binary representation as follows

$$\begin{aligned} 00 = 0 &\mapsto |H\rangle \\ 01 = 1 &\mapsto |V\rangle \\ 10 = 2 &\mapsto |D\rangle \\ 11 = 3 &\mapsto |A\rangle \end{aligned}$$

and in the case of the decoy states

$$\begin{aligned} 00 = 0 &\mapsto \text{null} \\ 01 = 1 &\mapsto \text{low} \\ 10 = 2 &\mapsto \text{high} \end{aligned}$$

although no null decoy state was encountered in the analysis of the file.
The total number of recorded events or qubits sent and received is 13776000: from this events an analysis of the protocol is possible. In the following report, we will indicate with capital letters the basis of Alice or Bob (A or B) and with lowercase letters the states (a and b).

2.1 Base Selection Probabilities

The probabilities of selection for each of the bases of Alice has been found to be

$$P[A = Z] = 0.9089 \qquad P[A = X] = 0.0911$$

which signals a strong bias toward the Z basis in state preparation. This is used to make the sifting phase more efficient: being biased allows to agree with Bob on more bases and therefore discard less qubits, and the Z basis is usually the one of choice because in standard setups it allows for better QBER.
This sifting advantage is nonetheless lost in Bob's basis choice as

$$P[B = Z] = 0.5153 \qquad P[B = X] = 0.4847$$

which signals a somewhat unbiased choice, which helps in identifying possible Eve interceptions.
The base agreement rate and so the ratio of qubits remaining after the sifting phase is 0.5079, which is consistent with the probability analysis seen before.

2.2 Conditional Probability Analysis

We can analyze the data to obtain the conditional probabilities that Bob measures each of the states if Alice sends one in particular, more formally seen in Table 1.

Table 1: Conditional probabilities $P(B \mid A)$.

	$\lvert H\rangle_A$	$\lvert V\rangle_A$	$\lvert D\rangle_A$
$\lvert H\rangle_B$	0.4953	0.0209	0.2044
$\lvert V\rangle_B$	0.0075	0.5011	0.3360
$\lvert D\rangle_B$	0.1792	0.1999	0.4496
$\lvert A\rangle_B$	0.3180	0.2781	0.0100
$\sum_B P(B\|A)$	1.0000	1.0000	1.0000

2.3 QBER Analysis

In order to evaluate the quality of the QKD system at hand, we examine the measured error rates. In particular

$$P[a \neq b | a = |H\rangle] = 0.5047$$
$$P[a \neq b | a = |V\rangle] = 0.4989$$
$$P[a \neq b | a = |D\rangle] = 0.5504$$

This error rates are driven mainly by different choice in basis by the two parties, although a trend can be seen in which the X basis is subject to higher error rates, which justifies the bias in error preparation seen before.
Although these can be seen, in some way, as QBER measurements, they are not in the strict or standard sense, which would define the QBERs in terms of $P[a \neq b | A = B] = \frac{P[a \neq b \wedge A = B]}{P[A = B]}$. In this case we have

$$P[a \neq b | A = B = Z] = 0.0275$$
$$P[a \neq b | A = B = X] = 0.0217$$

in the assumption that when preparing a state in the Z basis

$$P[a = |H\rangle \, | A = Z] = P[a = |V\rangle \, | A = Z] = \frac{1}{2}$$

and for the X basis

$$P[a = |D\rangle \, | A = X] = 1$$

which can be easily seen as the state $|A\rangle$ is never prepared by Alice.
This are very good QBER statistics for a real-world QKD system, which quantify the high quality of our setup.

2.4 Decoy States

The decoy state, encoded as seen before, has a probability of being in the low and high state respectively

$$P[\text{decoy} = \text{low}] = 0.1155 \qquad P[\text{decoy} = \text{high}] = 0.8845$$

which shows a strong bias toward high-mean-photon-number coherent states, which favors higher key rates.

3 QBER Analysis with Eve

The presence of Eve which performs an intercept-resend attack disrupts the quantum states sent by Alice and is therefore quantifiable through a QBER analysis. In the assumption that Eve's base measurements are perfectly aligned with Bob's, Eve's basis choice is unbiased and the channel doesn't introduce any errors or decoherence, we examine the resulting QBERs in the two bases.

3.1 Z-basis

In the Z-basis case we know from previous measurements that the QBER experienced by Bob and therefore in this case by Eve is 0.0275. In the case that Eve's performs a measurement in the right (Z) basis we have that the resulting QBER in the Z basis is still 0.0275 for Bob as Eve doesn't introduce any additional errors, and thus her interception goes undetected. If Eve measures in the wrong basis (X) she will project the state either in $|D\rangle$ or $|A\rangle$, which both can be measured by Alice in Z with $\frac{1}{2}$ probability of error. As Eve performs a balanced base choice the resulting QBER will be

$$\text{QBER}(Z) = \frac{1}{2} \cdot 0.0275 + \frac{1}{2} \cdot \frac{1}{2} = 0.2638$$

3.2 X-basis

Turning ourselves to the X-basis case in an analogous way, the QBER experienced by Bob in the case Eve luckily chooses the correct measurement basis is 0.0217, while in the case she chooses the wrong basis the QBER will be again $\frac{1}{2}$, from which

$$\text{QBER}(X) = \frac{1}{2} \cdot 0.0217 + \frac{1}{2} \cdot \frac{1}{2} = 0.2609$$

In both cases Bob sees a considerable increment in QBER and will discard the current key, deeming it lost to Eve, to retry establishing a secure key with Alice.

4 Conclusions

Our analysis of preparation and detection events has highlighted the quality of the QKD setup object of this experiment. The system exhibits very low intrinsic error rates in both the Z and X bases, with measured QBERs of 2.75% and 2.17% respectively during normal operation. These values reflect a high degree of stability in state preparation, transmission, and detection, demonstrating that the experimental platform is suitable for secure key distribution in practical applications.

The conditional probability structure further confirms the expected quantum behaviour, with strong correlations along matched measurement bases and significantly reduced correlations otherwise. Additionally, the use of decoy states was verified and shown to be compatible with the expected emission statistics, ensuring robustness against photon-number-splitting attacks.

Under an intercept-resend attack by Eve, we have shown that the measured QBER would increase to approximately 25%, a dramatic deviation from baseline performance. This result reflects the inherent ability of the BB84 protocol to detect eavesdropping attempts thanks to the disturbance introduced by measurements in non-matching bases. Therefore, any active intrusion would be identified during the key verification phase, allowing Alice and Bob to discard the compromised key material and maintain security.

In conclusion, the protocol behaves as theoretically expected across all tested performance indicators, confirming both the correct functioning of the hardware and the resilience of quantum key distribution to adversarial interference. With the implementation of classical post-processing steps such as error correction and privacy amplification, the system would be able to generate a secret key with information-theoretic security, illustrating the practical viability of QKD technologies in real-world secure communication scenarios.