M2: Quantum Information

IMPLEMENTING THE BB84 PROTOCOL

QCrypt Lab Report

Submitted by

Murshed SK (Student ID: 21516967)
Asad Munir (Student ID: 21419975)
Houssam Eddine Jamil Nasser (Student ID: 21400407)
Mohammed Boudjemaa (Student ID: 21317975)

Group Number: A4

Contents

Introduction

1.1 The Need for Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a revolutionary technique that allows two parties, conventionally named Alice and Bob, to establish and share a cryptographic key with security guaranteed by the fundamental principles of quantum mechanics. Unlike classical key distribution methods, whose security relies on computational assumptions — meaning they are secure only as long as certain mathematical problems remain hard to solve, such as factoring large integers (RSA) or solving discrete logarithms (Diffie-Hellman/ECC) — QKD leverages quantum phenomena such as the no-cloning theorem and the measurement disturbance principle. These principles ensure that any eavesdropping attempt by a malicious party, usually called Eve, introduces detectable errors, making it possible to guarantee the secrecy of the key.

The need for QKD arises from the increasing vulnerability of classical cryptographic systems in the face of growing computational power and the potential development of quantum computers. These quantum computers could efficiently break widely used classical cryptographic schemes using algorithms that are exponentially more powerful than their classical counterparts. In this context, QKD represents a practical application of quantum information principles, enabling secure communication channels in a world where information security is increasingly critical. This lab session focuses on implementing and analyzing a QKD protocol, providing hands-on exploration of these concepts.

1.2 Polarization of Single Photons as Qubits

In quantum cryptography, single photons are commonly used as carriers of quantum information. The polarization state of a photon represents a two-level quantum system, making it a natural physical implementation of a qubit. A qubit is the fundamental unit of quantum information, analogous to a classical bit, but unlike a classical bit, it can exist in a superposition of states.

For example, horizontal (H) and vertical (V) polarizations can encode the logical states $|0\rangle$ and $|1\rangle$ in the Z basis. Similarly, diagonal polarizations ($+45^\circ$ and -45°) form another orthogonal basis, often called the X basis. By choosing different polarization bases, Alice can encode information on single photons, and Bob can measure them accordingly. The security arises from the fact that any measurement by an eavesdropper (Eve) in the wrong basis disturbs the photon's state, introducing detectable errors. Thus, photon polarization is used as a qubit because it provides a controllable, well-defined two-level system that can be easily prepared, transmitted, and measured, while naturally supporting the principles underlying QKD protocols like BB84.

Theoretical Part

2.1 Encoder

Question 1.1: *Determine the angle $\theta_0, \theta_1, \theta_+,$ and θ_- such that HWP$(\theta_0)|0\rangle = |0\rangle$, HWP$(\theta_1)|0\rangle = |1\rangle$, HWP$(\theta_+)|0\rangle = |+\rangle$, HWP$(\theta_-)|0\rangle = |-\rangle$. Explain how the Half-Wave Plate can be used as a BB84 encoder for Alice.*

A Half-Wave Plate (HWP) is an optical device that rotates the polarization of light. Its action on a polarization qubit $|\psi\rangle$ can be represented as:

$$\text{HWP}(\theta)|\psi\rangle = R(2\theta)|\psi\rangle$$

To prepare the four BB84 states from $|0\rangle$:

$$\begin{aligned}
\text{HWP}(\theta_0)|0\rangle = |0\rangle &\implies \theta_0 = 0^\circ \\
\text{HWP}(\theta_1)|0\rangle = |1\rangle &\implies \theta_1 = 45^\circ \\
\text{HWP}(\theta_+)|0\rangle = |+\rangle &\implies \theta_+ = 22.5^\circ \\
\text{HWP}(\theta_-)|0\rangle = |-\rangle &\implies \theta_- = -22.5^\circ
\end{aligned}$$

Alice uses a single HWP to prepare the four BB84 states by setting it to one of the angles in $\Theta_A = \{0^\circ, 45^\circ, 22.5^\circ, -22.5^\circ\}$. Each angle corresponds to a polarization state $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. By sending the photon to Bob after setting the HWP, she encodes her classical bit in the chosen basis, implementing the BB84 protocol.

Question 1.2: *Show that, if you consider the polarization state as vectors, the effect of the rotated Half-Wave Plate with an angle θ on the horizontal polarization state $|H\rangle$ can be seen as a rotation in the vector plane with an angle ϕ. What is the relation between θ and ϕ. Give the values of $\phi_0, \phi_1, \phi_+,$ and ϕ_-.*

Considering the polarization state as a vector, the effect of the rotated HWP with an angle θ on the horizontal polarization state $|H\rangle$ is a rotation in the vector plane by an angle ϕ. The effect of a HWP(θ) on $|H\rangle$ is a rotation of the polarization vector by:

$$\phi = 2\theta$$

For the BB84 states, the required polarization rotation angles are $\Phi_A = \{\phi_0 = 0^\circ, \phi_1 = 90^\circ, \phi_+ = 45^\circ, \phi_- = -45^\circ\}$. These values of ϕ correspond to the physical markings on the HWP used to encode Alice's states.

2.2 Decoder

Question 1.3: *Show that the measurement station performs a measurement in the* $\{|0\rangle, |1\rangle\}$ *basis (HV).*

Let an arbitrary incoming polarization state be $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$. A Polarizing Beam Splitter (PBS) routes the horizontal component to the "H" output and the vertical component to the "V" output. After the PBS, the field at the H detector is proportional to $\alpha|H\rangle$ and at the V detector to $\beta|V\rangle$.

Assuming ideal single-photon detectors, the click probabilities are:

$$P_H = |\alpha|^2 = |\langle H|\psi\rangle|^2$$
$$P_V = |\beta|^2 = |\langle V|\psi\rangle|^2$$

These probabilities are exactly those produced by a projective measurement with projectors $P_H = |H\rangle\langle H|$ and $P_V = |V\rangle\langle V|$. Therefore, the station implements a projective measurement in the Z basis, $\{|0\rangle, |1\rangle\} = \{|H\rangle, |V\rangle\}$. A click in the H detector corresponds to projecting $|\psi\rangle$ onto $|H\rangle$, and a click in the V detector corresponds to projecting $|\psi\rangle$ onto $|V\rangle$.

Question 1.4: *Show that the measurement station can perform a measurement in the* $\{|+\rangle, |-\rangle\}$ *basis (DA) by adding a Half-Wave Plate of angle* θ_H *and give the value of* θ_H*. Explain how the combination of the Half-Wave Plate and the measurement station provide a good measurement setup for Bob.*

To measure in the diagonal/anti-diagonal (DA) basis, $\{|+\rangle, |-\rangle\}$, we must first transform these states into the basis of the measurement station, which is the HV basis. This can be accomplished by inserting a Half-Wave Plate (HWP) before the PBS. We need a rotation that maps $|+\rangle \to |H\rangle$ and $|-\rangle \to |V\rangle$. This corresponds to a polarization rotation of $-45°$.

Since an HWP at an angle θ rotates the polarization by 2θ, we require:

$$2\theta_H = -45° \implies \theta_H = -22.5°$$

By inserting an HWP set to $\theta_H = -22.5°$ before the PBS, the incoming DA basis states are rotated as follows:

$$|+\rangle \xrightarrow{\text{HWP}(-22.5°)} |H\rangle$$
$$|-\rangle \xrightarrow{\text{HWP}(-22.5°)} |V\rangle$$

The PBS then performs a projective measurement in the HV basis, which, due to the preceding rotation, is equivalent to performing a measurement in the DA basis on the original state.

Therefore, Bob's measurement setup, consisting of a rotatable HWP followed by a PBS and two detectors, is a complete BB84 decoder. He can choose his measurement basis by simply setting the angle of his HWP:

- To measure in the **HV basis**, Bob sets his HWP to $\theta_B = 0°$ (no rotation).
- To measure in the **DA basis**, Bob sets his HWP to $\theta_B = -22.5°$.

This allows him to randomly and independently choose between the two required measurement bases for the BB84 protocol.

2.3 BB84 Setup

Let $\theta_A, \theta_B \in \mathbb{R}$. Under the assumption of a perfect (i.e., lossless and noiseless) channel, the qubit arriving at Bob's measurement station is given by the state:

$$|\psi\rangle = \text{HWP}(\theta_B) \cdot \text{HWP}(\theta_A)|0\rangle$$

Question 1.5: *Compute $P_0(\theta_A, \theta_B) = |\langle 0|\psi\rangle|^2$ in function of θ_A and θ_B.*

First, we determine the state $|\psi\rangle$. The action of two consecutive HWPs is equivalent to a single HWP with an angle equal to the difference of the individual angles, which results in a polarization rotation of twice that difference.

$$\text{HWP}(\theta_B)\text{HWP}(\theta_A) = R(-2\theta_B)R(2\theta_A) = R(2\theta_A - 2\theta_B)$$

Applying this to the initial state $|0\rangle$:

$$|\psi\rangle = R(2\theta_A - 2\theta_B)|0\rangle = \begin{pmatrix}\cos(2\theta_A - 2\theta_B)\\ \sin(2\theta_A - 2\theta_B)\end{pmatrix}$$

Now, we compute the probability P_0 of measuring this state in the $|0\rangle$ state, which corresponds to a click at Bob's '0' detector.

$$\langle 0|\psi\rangle = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}\cos(2\theta_A - 2\theta_B)\\ \sin(2\theta_A - 2\theta_B)\end{pmatrix} = \cos(2\theta_A - 2\theta_B)$$

Finally, the probability is the squared magnitude of this amplitude:

$$P_0(\theta_A, \theta_B) = |\langle 0|\psi\rangle|^2 = \cos^2(2\theta_A - 2\theta_B)$$

Question 1.6: *By considering $P_1(\theta_A, \theta_B) = 1 - P_0(\theta_A, \theta_B)$, compute the values of $P_0(\theta_A, \theta_B)$ and $P_1(\theta_A, \theta_B)$ for $\theta_A \in \Theta_A, \theta_B \in \Theta_B$.*

We have $P_1(\theta_A, \theta_B) = 1 - P_0(\theta_A, \theta_B) = 1 - \cos^2(2\theta_A - 2\theta_B) = \sin^2(2\theta_A - 2\theta_B)$. The detection probabilities for all combinations of Alice's and Bob's HWP angles are:

θ_A	$\theta_B = 0°$	$\theta_B = 22.5°$
$0°$	$P_0 = 1, P_1 = 0$	$P_0 = 0.5, P_1 = 0.5$
$45°$	$P_0 = 0, P_1 = 1$	$P_0 = 0.5, P_1 = 0.5$
$22.5°$	$P_0 = 0.5, P_1 = 0.5$	$P_0 = 1, P_1 = 0$
$-22.5°$	$P_0 = 0.5, P_1 = 0.5$	$P_0 = 0, P_1 = 1$

TABLE 2.1
Detection Probabilities P_0 and P_1

Question 1.7: *Let's denote x the bit chosen by Alice, B_A Alice's basis, B_B Bob's basis and y the output bit of Bob. Express the probability $P(x = y|B_A = B_B)$ and $P(x = y|B_A \neq B_B)$ in terms of $P_i(\theta_A, \theta_B)$. Compute the values $P(x = y|B_A = B_B)$ and $P(x = y|B_A \neq B_B)$.*

Let $x \in \{0, 1\}$ be Alice's bit, B_A her basis, B_B Bob's basis, and $y \in \{0, 1\}$ Bob's output bit. The detection probabilities $P_i(\theta_A, \theta_B)$ give the probability to measure $|0\rangle$ or $|1\rangle$.

- **Same Basis ($B_A = B_B$):** Alice and Bob's HWP angles are chosen to align the measurement. This results in $P_0 = 1$ or $P_1 = 1$ depending on the bit x. Alice and Bob's results are perfectly correlated.

$$P(x = y | B_A = B_B) = 1$$

- **Different Basis ($B_A \neq B_B$):** The difference in HWP angles is $\Delta\theta = \pm 22.5°$. This results in $P_0 = P_1 = 0.5$. Bob's outcome is completely random with respect to Alice's bit.

$$P(x = y | B_A \neq B_B) = 0.5$$

Question 1.8: *Fill the table 1 by adding the angles of Alice and of Bob and the expected classical outputs.*

Alice basis	Alice bit	Alice Angle	Bob basis	Bob angle	Bob output
HV	0	0°	HV	0°	0
HV	1	45°	HV	0°	1
DA	0	22.5°	HV	0°	0 or 1 (50%)
DA	1	−22.5°	HV	0°	0 or 1 (50%)
HV	0	0°	DA	22.5°	0 or 1 (50%)
HV	1	45°	DA	22.5°	0 or 1 (50%)
DA	0	22.5°	DA	22.5°	0
DA	1	−22.5°	DA	22.5°	1

TABLE 2.2
Encoding and measurement angles for all 8 cases.

2.4 Adding an Eavesdropper

Question 1.9: *What angles should Eve use to perform the intercept and resend attack?*

Answer: To perform the intercept-and-resend attack, Eve must first measure Alice's qubit and then resend a new qubit to Bob that matches her measurement result. Her setup, shown in Figure 4, is a combination of Bob's measurement station (HWP $\theta_{E,1}$ + PBS) and Alice's preparation station (Source + HWP $\theta_{E,2}$).

1. **For Measurement (HWP $\theta_{E,1}$):** Eve needs to randomly measure in either the HV (Z) basis or the DA (X) basis. To do this, she uses a setup identical to Bob's. Based on Question 1.4, Bob's angles for choosing his basis are $\Theta_B = \{0, \theta_H\}$.
   - To measure in the **HV basis** ($|0\rangle, |1\rangle$), Eve sets her first HWP to $\theta_{E,1} = 0°$.
   - To measure in the **DA basis** ($|+\rangle, |-\rangle$), Eve sets her first HWP to $\theta_{E,1} = \theta_H = 22.5°$.

   Therefore, for her measurement, Eve randomly chooses $\theta_{E,1}$ from the set $\{0°, 22.5°\}$.
2. **For Resending (HWP $\theta_{E,2}$):** After Eve's measurement, she must prepare and send a new qubit to Bob corresponding to her result. She uses a setup identical to Alice's. Based on Question 1.1, Alice's angles for preparing the four BB84 states are $\Theta_A = \{\theta_0, \theta_1, \theta_+, \theta_-\}$. Eve's choice for $\theta_{E,2}$ depends on her measurement outcome:
   - If she measured HV and got bit 0 ($|0\rangle$), she sets $\theta_{E,2} = \theta_0 = 0°$.
   - If she measured HV and got bit 1 ($|1\rangle$), she sets $\theta_{E,2} = \theta_1 = 45°$.
   - If she measured DA and got bit 0 ($|+\rangle$), she sets $\theta_{E,2} = \theta_+ = 22.5°$.
   - If she measured DA and got bit 1 ($|-\rangle$), she sets $\theta_{E,2} = \theta_- = -22.5°$.

   Therefore, for resending, Eve chooses $\theta_{E,2}$ from the set $\{0°, 45°, 22.5°, -22.5°\}$.

Question 1.10: *What is the expected behaviour when Eve chooses the same basis as Alice? What is the expected behaviour when Eve doesn't choose the same basis as Alice.*

Answer: Alice and Bob have chosen the same basis ($\mathcal{B}_A = \mathcal{B}_B$), as they are comparing their sifted key to find errors.

- **When Eve chooses the same basis ($\mathcal{B}_E = \mathcal{B}_A$):** Eve intercepts the qubit and measures in the *correct* basis. Her measurement result will be deterministic and will match Alice's bit. She then resends this same state to Bob. Since Bob is also in the same basis ($\mathcal{B}_B = \mathcal{B}_A$), his measurement is also deterministic.

  Expected Behaviour: Bob's bit will always match Alice's bit. Eve introduces **0% QBER** in this scenario.
- **When Eve chooses a different basis ($\mathcal{B}_E \neq \mathcal{B}_A$):** Eve intercepts the qubit and measures in the *wrong* basis. Her measurement outcome will be completely random (50/50 probability for each outcome). She then resends a new qubit corresponding to her random result. When Bob (who is in Alice's basis) measures this new qubit, his result will *also* be random, as the state he receives is in the wrong basis relative to his measurement setup.

  Expected Behaviour: Bob's bit has a 50% chance of matching Alice's bit and a 50% chance of being an error. Eve introduces **50% QBER** in this scenario.

Question 1.11: *What is the expected QBER if Eve performs the attack at each round?*

Answer: Eve performs the attack on every round, choosing her measurement basis (HV or DA) randomly. This means $\mathbb{P}(\mathcal{B}_E = \mathcal{B}_A) = 0.5$ and $\mathbb{P}(\mathcal{B}_E \neq \mathcal{B}_A) = 0.5$.

Alice and Bob calculate the QBER only on their sifted key, which are the rounds where $\mathcal{B}_A = \mathcal{B}_B$. We analyze the error Eve introduces in these rounds:

- **Case 1 (50% probability):** Eve chooses the *same* basis as Alice ($\mathcal{B}_E = \mathcal{B}_A$). As per Q1.10, her measurement is correct, and she introduces **0% QBER**.
- **Case 2 (50% probability):** Eve chooses a *different* basis from Alice ($\mathcal{B}_E \neq \mathcal{B}_A$). As per Q1.10, her measurement is random, and she introduces **50% QBER**.

The total expected QBER is the weighted average of these two outcomes:

$$QBER = (0.5 \times 0\%) + (0.5 \times 50\%)$$

$$QBER = 0\% + 25\% = 25\%$$

The expected QBER is **25%**.

Question 1.12: *What is the formula for the key rate of the protocol in that scenario. What is the value of the key rate with the value of the QBER found at the previous question?*

Answer: The formula for the secret key rate R (in bits per sifted key bit) in the asymptotic limit, for this specific intercept-resend attack scenario, is:

$$R \geq 1 - 2H_2(Q)$$

Where Q is the Quantum Bit Error Rate (QBER) and $H_2(Q)$ is the binary entropy function:

$$H_2(Q) = -Q \log_2(Q) - (1 - Q) \log_2(1 - Q)$$

Value of the key rate: From the previous question (1.11), the expected QBER is $Q = 0.25$.

First, we calculate the binary entropy $H_2(0.25)$:

$$H_2(0.25) = -0.25 \log_2(0.25) - (1 - 0.25) \log_2(1 - 0.25)$$

$$H_2(0.25) = -0.25 \log_2(1/4) - 0.75 \log_2(3/4)$$

$$H_2(0.25) = -0.25 \times (-2) - 0.75 \times (\log_2(3) - \log_2(4))$$

$$H_2(0.25) \approx 0.5 - 0.75 \times (1.585 - 2)$$

$$H_2(0.25) \approx 0.5 - 0.75 \times (-0.415) \approx 0.5 + 0.311 = 0.811$$

Now, we compute the key rate R:

$$R \geq 1 - 2 \times H_2(0.25)$$

$$R \geq 1 - 2 \times (0.811)$$

$$R \geq 1 - 1.622 = -0.622$$

The value of the key rate is **negative (or zero)**. This means that at a QBER of 25%, no secret key can be securely extracted, and Alice and Bob must abort the protocol.

2.5 Classical Analogy

Question 1.13: *Explain what allows, in the functioning of the components to get a classical analogy of a BB84 setup. Describe what are the limits of this analogy.*

Answer: What allows the analogy: The classical analogy works because the *mathematical* description of classical polarized light (using Jones Calculus) is identical to the quantum mechanical description of a single-photon's polarization (a qubit).

- **Components:** The Half-Wave Plate (HWP) is described by a 2×2 matrix that rotates the classical polarization vector. This is mathematically the same as the quantum operator that rotates a qubit's state.
- **Measurement:** The Polarization Beam Splitter (PBS) deterministically splits horizontal ($|0\rangle$) and vertical ($|1\rangle$) polarizations to two different sensors. This is a perfect analog for a projective measurement in the $\{|0\rangle, |1\rangle\}$ basis.
- **Probabilities:** When a state is prepared in a basis (e.g., DA) and measured in another (e.g., HV), the classical experiment shows the power splitting 50/50 between the two sensors. This classical power ratio is directly analogous to the 50/50 quantum *probabilities* of a single photon going to one sensor or the other.

Limits of the analogy: The analogy breaks down completely when considering security, as it lacks the fundamental quantum principles that make BB84 secure.

- **No Single Photons:** The experiment uses classical pulses of light, which contain many photons. A real QKD system *must* use single photons.
- **Vulnerability to Beam-Splitting:** An eavesdropper (Eve) can perform a "beam-splitting attack." She can siphon off a small fraction of the classical pulse to measure it perfectly *without* disturbing the rest of the pulse that travels to Bob. This is impossible with a single, indivisible photon.
- **No Measurement Disturbance:** In the quantum world, if Alice sends $|+\rangle$ and Eve measures in the HV basis, she *disturbs* the state, collapsing it to either $|0\rangle$ or $|1\rangle$. This disturbance introduces errors that Alice and Bob can detect. In the classical analogy, Eve's beam-splitting attack does not disturb the polarization of the main pulse, so she remains completely undetected.
- **No No-Cloning Theorem:** The No-Cloning Theorem forbids making a perfect copy of an *unknown* quantum state. This theorem does not apply to classical states. Eve can perfectly measure the classical polarization and resend an identical, new pulse to Bob.

Because of these limits, this classical setup provides **no security** and only serves as a mathematical demonstration.

Question 2.1: Laser Polarization Calibration

Principle

The goal is to align the laser such that its output is horizontally polarized light, which we denote as the state $|H\rangle$ or $|0\rangle$. The key component for this task is the Polarizing Beam Splitter (PBS). As described in Appendix A.2 of the practical work manual, a PBS separates an incident light beam based on its polarization: it transmits the horizontal component and reflects the vertical component ($|V\rangle$ or $|1\rangle$).

The laser emits linearly polarized light, but its initial orientation is unknown. Any state of linear polarization can be described as a superposition of the horizontal and vertical basis states. By rotating the laser, we change the angle of this linear polarization.

To find the specific orientation that corresponds to purely horizontal polarization, we must find the angle of rotation that maximizes the amount of light passing through the PBS (transmission) and simultaneously minimizes the amount of light being reflected.

Required Components

- Laser 1 and its power unit.
- A Polarizing Beam Splitter (PBS).
- Two screens or optical sensors/power meters to observe the intensity of the output beams.

Proposed Setup and Procedure

The calibration can be performed by following these steps:

1. **Assemble the Setup:**
    - Position the laser on the optical bench.
    - Place the PBS in the path of the laser beam. Ensure the beam is incident on the center of the PBS input face.
    - Place one screen or sensor in the path of the beam transmitted straight through the PBS. This will measure the intensity of the horizontally polarized component.
    - Place the second screen or sensor at a 90-degree angle to the incident path to intercept the reflected beam. This will measure the intensity of the vertically polarized component.
2. **Perform the Calibration:**
    (a) Turn the laser on and set it to continuous wave mode for a stable output, which makes intensity observation easier.
    (b) Carefully and slowly rotate the physical casing of the laser around its propagation axis.
    (c) As you rotate the laser, observe the intensity of the light spots on the two screens or the readings from the two sensors.
    (d) The rotational position at which the intensity at the **transmission output is maximized** and the intensity at the **reflection output is minimized** (ideally near zero) is the correct orientation.
3. **Conclusion:** Once this position is found, the laser is confirmed to be emitting horizontally polarized light. This orientation should be marked on the laser's mounting so it can be reliably set for the main experiment. As a check, rotating the laser by 90 degrees from this position should produce the

opposite result (maximum reflection, minimum transmission), corresponding to vertically polarized light.

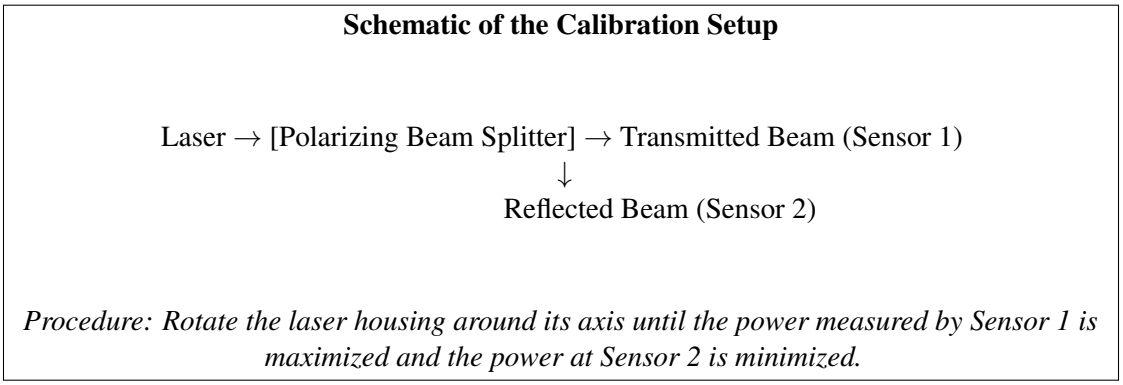

FIGURE 2.1
A conceptual diagram illustrating the setup for calibrating the laser's polarization output to be horizontal.

Question 2.2: Half-Wave Plate Calibration

Principle

The objective is to find the rotational position of the Half-Wave Plate (HWP) where its fast axis is aligned with the horizontal axis. This position is defined as the "0" of the HWP. The markings on the rotational mount must then be aligned to reflect this physical zero.

The calibration relies on the known behavior of an HWP. From the Jones matrix formalism provided in Appendix A.1, an HWP rotated by an angle θ transforms an input horizontal polarization state $|H\rangle$ into a linear polarization state rotated by an angle of 2θ.

The transformation is given by:

$$\text{HWP}(\theta)|H\rangle = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(2\theta) \\ \sin(2\theta) \end{pmatrix}$$

When the HWP's fast axis is aligned with the input horizontal polarization ($\theta = 0$), the plate should not change the polarization state of the light.

$$\text{HWP}(0)|H\rangle = \begin{pmatrix} \cos(0) \\ \sin(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |H\rangle$$

Therefore, to find the "0" of the HWP, we need to find the orientation where an input horizontal beam emerges as a horizontal beam. This can be tested by using a Polarizing Beam Splitter (PBS) after the HWP, which will transmit a purely horizontal beam with maximum intensity.

Required Components

- Laser 1, calibrated to emit horizontally polarized light (as per Question 2.1).
- Half-Wave Plate 1 (HWP 1) in a rotational mount.
- A Polarizing Beam Splitter (PBS).
- Two screens or optical sensors to measure the intensity of the transmitted and reflected beams.

Proposed Setup and Procedure

The components should be arranged in a line on the optical bench as follows:

1. **Setup Assembly:**
    - Start with the laser from the previous calibration step, ensuring its output is purely horizontal ($|H\rangle$).
    - Place the HWP 1 in the path of the laser beam. The HWP should be mounted in its rotational holder.
    - Place the PBS immediately after the HWP.
    - Position one sensor to detect the beam transmitted straight through the PBS (the horizontal component).
    - Position the second sensor to detect the beam reflected at 90 degrees by the PBS (the vertical component).
2. **Calibration Procedure:**
    (a) Turn the laser on and set it to continuous wave mode for stable intensity measurement.

(b) Slowly rotate the HWP 1 in its mount while observing the power at the two sensors.

(c) The rotational position where the power at the **transmitted sensor is maximized** and the power at the **reflected sensor is minimized** (ideally zero) corresponds to the HWP's fast axis being aligned horizontally. This is the physical "0" position.

3. **Marking the Zero:**

   (a) Once this position of minimum reflection is found, hold the HWP firmly in place.

   (b) As per Figure 5, carefully loosen the two screws on the outer dial of the HWP mount.

   (c) Rotate the graduated dial (the markings) without moving the HWP itself until its "0" mark aligns with the fixed reference indicator on the mount.

   (d) Gently tighten the screws to fix the dial in this new position.

4. **Verification (Optional but Recommended):**

   - With the "0" now set, rotate the HWP so the marking reads 45°. At this position ($\theta = 45°$), the HWP should rotate the horizontal light to vertical ($2\theta = 90°$).
   - Verify that this results in minimum power at the transmitted sensor and maximum power at the reflected sensor. This confirms the calibration is accurate.

Schematic of the HWP Calibration Setup

Calibrated Laser ($|H\rangle$) $\rightarrow$ HWP 1 $\rightarrow$ [PBS] $\rightarrow$ Transmitted Beam (Sensor 1)

$\downarrow$

Reflected Beam (Sensor 2)

Procedure: Rotate HWP 1 until power at Sensor 1 is maximized and power at Sensor 2 is minimized. This is the '0' position.

FIGURE 2.2
A conceptual diagram illustrating the setup for calibrating the Half-Wave Plate's zero position.

Question 2.3

Expected Behaviour

When the laser is fired, a pulse of light will travel through Alice's setup, across the free-space channel, and through Bob's measurement apparatus. Since Alice's and Bob's Half-Wave Plates are both set to 0°, the initial polarization of the light from the laser will be preserved throughout the entire system. The light will then be directed to one of Bob's two sensors by the Polarizing Beam Splitter, causing the corresponding LED to light up.

Which light went on and Why?

The light for **Sensor 0** (the sensor on the **transmission path** of the Polarizing Beam Splitter) will light up.

This occurs for the following reasons, following the path of the light step-by-step:

1. **Alice's Encoder (HWP at 0°):** Alice's Half-Wave Plate is set to $\theta_A = 0°$. A HWP at 0° does not change the polarization of incoming horizontal light. The light leaving Alice's station is still in the state $|0\rangle$.
2. **Bob's HWP (at 0°):** The light arrives at Bob's station and passes through his HWP, which is also set to $\theta_B = 0°$. Again, this has no effect on the horizontal polarization. The state entering Bob's detector is still $|0\rangle$.
3. **Bob's Decoder (PBS):** The purely horizontal light ($|0\rangle$) now enters the Polarizing Beam Splitter (PBS). By its definition, a PBS **transmits** horizontal polarization and **reflects** vertical polarization.
4. **Detection:** Consequently, all the light is transmitted straight through the PBS and strikes the sensor on this path (Sensor 0). The sensor on the reflected path (Sensor 1) receives no light. Therefore, only the LED for Sensor 0 will turn on.

Question 2.4: System Behavior Check

Completed Table

Alice Angle (θ_A)	Bob Angle (θ_B)	Which LED lights up	Bit
-45°	0°	H	0
0°	0°	H	0
45°	0°	V	1
90°	0°	V	1
-45°	45°	V	1
0°	45°	H	0
45°	45°	H	0
90°	45°	V	1

TABLE 2.3
Experimentally observed behavior for the 8 test cases.

Explanation of the Results

The results align with the core principle of the BB84 protocol. When Alice and Bob choose compatible measurement bases, the outcome is deterministic. This occurs when Alice uses an angle from {0°, 90°} and Bob uses 0° (Z-basis match), or when Alice uses {-45°, 45°} and Bob uses 45° (X-basis match), as seen in rows 2, 4, 5, and 7. Conversely, when their bases are mismatched (e.g., Alice uses an X-basis angle and Bob uses a Z-basis angle), the photon arrives at Bob's PBS in a superposition with respect to his measurement apparatus. This results in a random outcome, where either the 'H' or 'V' LED has a 50% chance of lighting up. The cells highlighted in red for rows 1, 3, 6, and 8 represent one possible random outcome observed for these mismatched basis cases.

Question 2.5: Key Exchange Data Collection

Bob's Recorded Data

During the 20-pulse key exchange, my station (Bob) randomly selected a measurement basis (either Z/HV or X/DA) for each incoming pulse. The following table lists the basis I chose for each pulse and the resulting bit value my sensors recorded.

Pulse Number	Bob's Chosen Basis	Bob's Measured Bit
1	X (DA)	0
2	Z (HV)	0
3	Z (HV)	1
4	X (DA)	1
5	X (DA)	1
6	X (DA)	0
7	Z (HV)	0
8	X (DA)	1
9	Z (HV)	1
10	Z (HV)	1
11	Z (HV)	1
12	X (DA)	1
13	X (DA)	0
14	X (DA)	0
15	X (DA)	0
16	X (DA)	0
17	Z (HV)	0
18	X (DA)	1
19	Z (HV)	1
20	Z (HV)	0

TABLE 2.4
Bob's measurement choices and results for the 20-pulse exchange.

Note: The bit values for measurements where bases were mismatched are inherently random.

Question 2.6: Sifting the Key

The Sifting Process

After the quantum transmission was complete, the teacher (Alice) publicly announced the sequence of bases she used. I compared her list of bases to my list of measurement bases. According to the BB84 protocol, we must discard all bits from the instances where our chosen bases did not match. The remaining bits, where we independently chose the same basis, form the sifted or "raw" key.

The table below details this sifting process. A checkmark (✓) indicates a basis match, where the bit is kept. A crossmark (X) indicates a mismatch, where the bit is discarded.

Alice's Basis	Bob's Basis	Bob's Measured Bit	Basis Match?	Kept Bit
X	X	0	✓	**0**
X	Z	0	X	-
X	Z	1	X	-
Z	X	1	X	-
X	X	1	✓	**1**
Z	X	0	X	-
X	Z	0	X	-
Z	X	1	X	-
X	Z	1	X	-
X	Z	1	X	-
Z	Z	1	✓	**1**
Z	X	1	X	-
X	X	0	✓	**0**
Z	X	0	X	-
Z	X	0	X	-
X	X	0	✓	**0**
X	Z	0	X	-
X	X	1	✓	**1**
X	Z	1	X	-
Z	Z	0	✓	**0**

TABLE 2.5
Sifting process to generate the raw key.

The Raw Key

After discarding the 13 measurements from mismatched bases, we were left with 7 bits where our bases matched.

The resulting raw key is: **0110010**.

Question 2.7: Data Collection with an Eavesdropper

Simulated Experiment

Due to a technical issue with the eavesdropper (Eve) station, a physical run of the experiment could not be completed. To analyze the effects of an intercept-and-resend attack, we simulated the 20-pulse exchange using random number generators for Eve's and Bob's basis choices.

The following table details the complete data from the simulated exchange. It shows Alice's randomly chosen basis and bit, Eve's random basis choice and her resulting measurement/resend, and Bob's random basis choice. The bits highlighted in green represent instances where Eve correctly guessed Alice's basis and therefore forwarded the correct bit to Bob without introducing an error herself.

Pulse #	Alice		Eve		Bob	
	Basis	Bit	Basis	Bit Sent	Basis	Measured Bit
1	Z	0	X	1	Z	1
2	X	0	X	**0**	X	0
3	Z	0	X	0	Z	1
4	Z	1	Z	**1**	Z	1
5	X	0	Z	0	X	0
6	Z	0	X	0	Z	0
7	Z	1	X	0	Z	0
8	Z	0	Z	**0**	X	0
9	Z	0	X	1	Z	0
10	X	1	X	**1**	X	1
11	X	1	Z	0	X	0
12	Z	1	X	1	X	0
13	X	0	X	**0**	X	0
14	Z	1	X	1	X	1
15	Z	1	X	1	X	1
16	X	0	Z	1	Z	0
17	Z	0	Z	**0**	X	1
18	X	1	X	**1**	X	1
19	X	0	Z	1	X	1
20	X	0	X	**0**	X	0

TABLE 2.6
Simulated 20-pulse exchange with an intercept-and-resend attack.

Question 2.8: Exchange the basis and bit values and compute the QBER

Sifting Process

Following the quantum transmission, Alice and Bob publicly compared their basis choices. All data from rounds where their bases did not match were discarded. The table below highlights the rounds that were kept for the sifted key (where Alice's and Bob's bases are the same).

Pulse #	Alice Basis	Bob Basis	Match?	Action
1	Z	Z	✓	**Keep**
2	X	X	✓	**Keep**
3	Z	Z	✓	**Keep**
4	Z	Z	✓	**Keep**
5	X	X	✓	**Keep**
6	Z	Z	✓	**Keep**
7	Z	Z	✓	**Keep**
8	Z	X	X	Discard
9	Z	Z	✓	**Keep**
10	X	X	✓	**Keep**
11	X	X	✓	**Keep**
12	Z	X	X	Discard
13	X	X	✓	**Keep**
14	Z	X	X	Discard
15	Z	X	X	Discard
16	X	Z	X	Discard
17	Z	X	X	Discard
18	X	X	✓	**Keep**
19	X	X	✓	**Keep**
20	X	X	✓	**Keep**

TABLE 2.7
Sifting the key by comparing Alice's and Bob's bases.

Sifted Keys and QBER Calculation

From the 20 initial pulses, 14 rounds survived the sifting process. We then compared Alice's original bit with the bit Bob measured in these 14 rounds to find any discrepancies introduced by Eve.

- **Alice's Sifted Key:** `00010010110100`
- **Bob's Sifted Key:** `10110000100110`

To find the Quantum Bit Error Rate (QBER), we count the number of mismatched bits (errors) and divide by the total number of bits in the sifted key.

```
Alice: 0 0 0 1 0 0 1 0 1 1 0 1 0 0
Bob:   1 0 1 1 0 0 0 0 1 0 0 1 1 0
Error: *   *       *     *     *
```

By comparing the keys, we found **5 errors**.

The QBER is calculated as follows:

$$\text{QBER} = \frac{\text{Number of Errors}}{\text{Total Sifted Bits}} = \frac{5}{14}$$

$$\text{QBER} \approx 0.3571 \quad \text{or} \quad 35.71\%$$

This high error rate is a clear indication of eavesdropping. An ideal, noiseless transmission with no eavesdropper would have a QBER of 0%. The theoretical error rate induced by this specific intercept-and-resend attack is 25%. Our result of 35.71% is higher, which further ascertains the presence of an eavesdropper.

Question 2.9: Efficiency of Optical Components

Definition and Composition of Efficiency

The **efficiency** of an optical component is the ratio of the output optical power (or number of photons) to the input optical power. It is a dimensionless quantity, often expressed as a percentage, that quantifies the loss of signal due to factors like absorption, scattering, or imperfect operation.

If two components are placed in series, with individual efficiencies T_1 and T_2, their combined efficiency T can be modeled as a single component. Let P_{in} be the power entering the first component. The power exiting the first component is $P_{mid} = T_1 \times P_{in}$. This power then enters the second component, and the final output power is $P_{out} = T_2 \times P_{mid}$. Substituting the expression for P_{mid}, we get:

$$P_{out} = T_2 \times (T_1 \times P_{in}) = (T_1 \times T_2) \times P_{in}$$

The total efficiency T is the ratio P_{out}/P_{in}, which gives the relation:

$$T = T_1 \times T_2$$

This shows that the total efficiency of components in series is the product of their individual efficiencies.

Decomposition of Receiver Efficiency (η)

The overall efficiency η of the receiver (Bob's station) is the probability of a photon being successfully detected, given that it has arrived at the receiver. This can be decomposed into a product of the efficiencies of the key components in Bob's setup. Based on the documentation for the components, we can identify three primary terms:

- T_{hwp} **(Transmission Efficiency of HWP):** The fraction of light that passes through the Half-Wave Plate. A typical value for an anti-reflection coated HWP is $> 99\%$.
- T_{pbs} **(Transmission Efficiency of PBS):** The fraction of light that is correctly transmitted or reflected by the PBS. For the specified PBS (Thorlabs PBS201), the average transmission for the correct polarization is $> 99.5\%$.
- η_{det} **(Detection Efficiency):** The quantum efficiency of the photodiode sensor itself; the probability that it registers a photon that physically strikes it.

(Note: The lab handout text provided values without specifying their direct source from the documentation, so we will use the provided example values for the calculation.)

Let's denote the three efficiency terms as T_1, T_2, and T_3. The total efficiency η is their product:

$$\eta = T_1 \times T_2 \times T_3$$

Using provided typical values:

- T_1 (e.g., Transmission Efficiency) = 0.90
- T_2 (e.g., Detection Efficiency) = 0.80
- T_3 (e.g., Polarization/Splitting Efficiency) = 0.95

The total efficiency of the receiver is calculated as:

$$\eta = 0.90 \times 0.80 \times 0.95 = 0.684$$

Therefore, the total efficiency of the receiver, representing the probability that Bob successfully detects an incoming photon, is **68.4%**.

Question 2.10: Detection Rate Formula

Derivation of the Detection Rate (r_{det})

We are asked to provide a formula for the detection rate (r_{det}) based on the following parameters:

- r_{source}: The source repetition rate (pulses per second).
- T: The transmittance of the channel (probability a photon survives the journey from Alice to Bob).
- η: The overall efficiency of the receiver/detector (probability a photon is detected if it arrives at Bob's station).

The detection rate is the number of successful detection events per second. The rate at which photons are emitted is r_{source}. The rate at which photons arrive at Bob's station is reduced by the channel transmittance, becoming $r_{source} \times T$. Of those arriving photons, only a fraction η will be successfully detected. Therefore, the final detection rate is the product of the emission rate and these two probabilities.

The formula for the detection rate is:

$$r_{det} = r_{source} \times T \times \eta$$

This formula highlights that the final rate is directly proportional to the source rate and is limited by losses in both the channel and the receiver. This expression is valid under the stated assumptions of a true single-photon source and no dark counts (false detections from thermal noise or other sources).

Question 2.11: Detection Rate with Weak Coherent Pulses

Weak Coherent Pulses

When using a practical source like an attenuated laser, the output consists of weak coherent pulses, not true single-photon states. In this case, the number of photons, n, in any given pulse is not fixed at one but is a random variable. Its distribution is well-described by a Poisson distribution, which gives the probability $P(n)$ of finding exactly n photons in a pulse, given a mean (average) photon number μ:

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}$$

where:

- μ is the average number of photons per pulse.
- n is the number of photons in a specific pulse.

Modified Detection Rate

The detection rate formula from the previous question must be modified to account for the fact that the source does not emit exactly one photon per pulse, but rather an average of μ photons per pulse. The term r_{source} gives the rate of pulses, and we need to find the average rate of photons being emitted. This is simply the product of the pulse rate and the average number of photons per pulse.

The average photon emission rate is $r_{source} \times \mu$.

By substituting this into our previous formula, we can find the new detection rate, r_{det}. We assume that for a weak coherent pulse ($\mu \ll 1$), the probability of having more than one photon is negligible, and we are primarily interested in the rate at which any detection event occurs (triggered by one or more photons).

The modified detection rate is:

$$r_{det} = r_{source} \times \mu \times T \times \eta$$

This formula now correctly incorporates the average photon number μ from the Poissonian source, providing a more realistic model for the expected number of detection events per second in a practical QKD system.

Question 2.12: Maximal Source Rate

Calculation

We are given the following parameters:

- $\eta = 0.5$: The overall efficiency of the detector.
- $T = 0.5$: The transmittance of the channel.
- $\mu = 0.1$: The average photon number in each pulse.
- Maximal detection rate: 1 MHz $= 1 \times 10^6$ Hz.

We need to find the maximal source repetition rate, r_{source}. From the previous question, the detection rate is given by the formula $r_{det} = r_{source} \times T \times \eta \times \mu$. Since the detection rate must not exceed the detector's limit, we can establish the following inequality:

$$r_{source} \times 0.5 \times 0.5 \times 0.1 \leq 1 \times 10^6 \text{ Hz}$$

Solving for r_{source}:

$$\begin{aligned} r_{source} \times 0.025 &\leq 1 \times 10^6 \\ r_{source} &\leq \frac{1 \times 10^6}{0.025} \\ r_{source} &\leq 4 \times 10^7 \text{ Hz} \end{aligned}$$

So, the maximum source repetition rate is:

$$r_{source} \leq 40 \text{ MHz}$$

Interpretation and Limitation on QKD

The maximum source repetition rate, r_{source}, is 40 MHz. This means that the source can emit a maximum of 40 million pulses per second without exceeding the detector's saturation limit. If the source emits pulses faster than this rate, the detector will become saturated and will no longer be able to detect subsequent photons accurately for a period of time (known as dead time).

How this limits QKD: This maximum source rate places a fundamental cap on the speed of the key exchange. Since the final secure key is a small fraction of the initially transmitted pulses, a higher source rate is crucial for generating keys at a practical speed. Detector saturation thus acts as a bottleneck, limiting the raw key generation rate and, consequently, the final secure key rate of the QKD system.

Question 2.13: QBER Induced by Dark Counts

Analysis

This question asks for the Quantum Bit Error Rate (QBER) induced by detector dark counts, which are random detection events that occur even in the absence of an incident photon. The key parameters are:

- p_{dark}: The probability of a dark count event per detection time window.
- T: The transmittance of the channel.
- η: The overall detection efficiency of the detector.

The QBER is the fraction of bits in the sifted key that are erroneous. In this scenario, errors are introduced when a detector fires due to a dark count. When a dark count occurs, it is independent of the bit Alice sent, leading to a potential mismatch between Alice's bit and Bob's measured bit. The total probability of error caused by a dark count can be modeled as:

$$P_{\text{error, dark}} = p_{\text{dark}} \times \eta \times T$$

This equation models how the dark count error is influenced by both the channel transmission and the detector efficiency. The total QBER due to dark counts in the presence of true photon detection is therefore given by:

$$\text{QBER} = p_{\text{dark}} \times \eta \times T$$

- **Dark Counts Contribution:** Dark counts increase the QBER because they contribute to false positives. Even if a photon is lost in the channel, a detector can still register a click, potentially introducing an error.
- **Channel Transmission (T):** The transmission T influences the rate of legitimate photon detections.
- **Detector Efficiency (η):** The detector's efficiency plays a key role in how many photons are successfully registered.

Question 2.14: QBER from Finite Extinction Ratio

Effect of Finite Extinction Ratio

In an ideal PBS, horizontally polarized light is perfectly transmitted, and vertically polarized light is perfectly reflected.
However, a real-world PBS has a finite **polarization extinction ratio**, which quantifies its imperfection. This means a small fraction of horizontally polarized light "leaks" and gets incorrectly reflected, and a small fraction of vertically polarized light leaks and gets incorrectly transmitted. This imperfect sorting of polarizations is a direct source of errors in Bob's measurements, thus contributing to the QBER.

The extinction ratio, E, is defined as the ratio of the power of the correctly routed polarization to the power of the incorrectly routed polarization. For the transmitted beam, this is:

$$E = \frac{\text{Transmitted p-polarized (horizontal) light}}{\text{Transmitted s-polarized (vertical) light}}$$

Let's analyze the probability of error for each input polarization state. If the total input power is normalized to 1, and the leaked power is ϵ, then the correctly routed power is $1 - \epsilon$. The extinction ratio is $E = (1 - \epsilon)/\epsilon$. This can be rearranged to find that the probability of a photon being incorrectly routed (i.e., the error probability) is $\epsilon = 1/(E + 1)$.

- **Error for Horizontal Light ($P_{\text{error, H}}$):** Alice sends $|H\rangle$ (bit 0). Bob should measure 0. An error occurs if the PBS incorrectly reflects the photon to the '1' detector. The probability of this is:

$$P_{\text{error, H}} = \frac{1}{E+1}$$

- **Error for Vertical Light ($P_{\text{error, V}}$):** Alice sends $|V\rangle$ (bit 1). Bob should measure 1. An error occurs if the PBS incorrectly transmits the photon to the '0' detector. The probability of this is:

$$P_{\text{error, V}} = \frac{1}{E+1}$$

QBER Calculation

The total QBER is the average error probability, assuming Alice sends 0s and 1s with equal likelihood:

$$\text{QBER} = \frac{P_{\text{error, H}} + P_{\text{error, V}}}{2} = \frac{1}{2}\left(\frac{1}{E+1} + \frac{1}{E+1}\right)$$

This simplifies to:

$$\text{QBER} = \frac{1}{E+1}$$

Example Calculation

The quality of a PBS is determined by its extinction ratio, which for a standard laboratory-grade component is typically very high. Let's consider a common example where the extinction ratio is specified as $1000:1$.

$$E = 1000$$

Using this representative value, we can compute the QBER that would be induced solely by this PBS imperfection:

$$\text{QBER} = \frac{1}{1000+1} = \frac{1}{1001} \approx 0.000999$$

This corresponds to a QBER of approximately **0.1%**. This calculation demonstrates that while no PBS is perfect, using high-quality components with a large extinction ratio is crucial, as their individual contribution to the overall error rate is kept to a very small and manageable level.

Question 2.15: QBER from HWP Calibration Error

Effect of Calibration Error

A calibration error on Alice's Half-Wave Plate (HWP) means that when she intends to set a specific angle θ_A, the actual physical angle is slightly misaligned by an amount θ_{err}. This error directly impacts the polarization state she prepares.

For instance, if Alice intends to prepare a horizontal state $|H\rangle$ by setting her HWP to $0°$, a calibration error would mean the actual angle is θ_{err}. This rotates the outgoing polarization by an angle of $2\theta_{err}$, creating a state that is no longer purely horizontal. When this slightly rotated state arrives at Bob's station and he measures in the correct (HV) basis, there is now a non-zero probability that his detector for vertical polarization ($|V\rangle$) will fire, registering an error. This holds true for any of the four BB84 states Alice tries to prepare; a calibration error will always rotate the state slightly away from the intended polarization.

QBER Calculation

The probability of Bob making an incorrect measurement due to this misalignment depends on the magnitude of the error, θ_{err}. The error probability, P_{error}, can be shown to be proportional to the square of the sine of the angle of misalignment. If Alice and Bob use the same basis, the probability of an error is:

$$P_{\text{error}} \approx \frac{1}{2}\sin^2(\theta_{err})$$

However, since Alice and Bob only choose the same basis half the time, and the other half of the time the result is random anyway (contributing a 50% inherent error rate which is sifted out), the QBER is affected differently. The induced QBER from this systematic error, averaged over all four states, is given by:

$$\text{QBER} = \frac{1}{2}\sin^2(\theta_{err})$$

For small calibration errors, where θ_{err} is close to zero, we can use the small-angle approximation, $\sin(\theta) \approx \theta$ (where θ is in radians). This simplifies the expression for the QBER to:

$$\text{QBER} \approx \frac{1}{2}\theta_{err}^2$$

This result shows that the QBER is quadratically dependent on the calibration error. This is a favorable property, as it means that halving the angular error in the HWP reduces the resulting QBER by a factor of four, highlighting the critical importance of precise calibration.

Open Conclusion on Polarization Encoding in BB84

The polarization encoding in the BB84 protocol plays a critical role in ensuring the security and efficiency of quantum key distribution (QKD). By encoding information in the polarization states of single photons, such as horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarizations for the computational basis, and diagonal ($|+\rangle$) and anti-diagonal ($|-\rangle$) polarizations for the diagonal basis, the protocol leverages the fundamental principles of quantum mechanics, particularly the no-cloning theorem and quantum superposition. This encoding method allows Alice and Bob to securely exchange cryptographic keys by measuring these quantum states, with the knowledge that any attempt by an eavesdropper (Eve) to intercept or measure the photons would inevitably disturb the system, thus revealing her presence.

However, real-world implementations of BB84 with polarization encoding face challenges, such as imperfections in optical components (e.g., polarizing beam splitters, half-wave plates) and calibration errors that can introduce errors measured by the Quantum Bit Error Rate (QBER), compromising the key exchange's reliability. Additionally, external factors like dark counts, channel losses, and the finite extinction ratio of optical components can further influence the QBER and, consequently, the overall security and efficiency of the protocol.

Despite these challenges, the fundamental robustness of polarization encoding in BB84 remains a cornerstone of modern quantum cryptography, offering a promising avenue for secure communication in a variety of applications, from quantum networks to future quantum-based internet infrastructures. The ongoing research in improving hardware efficiency, error correction protocols, and adaptive strategies will continue to refine the practical implementation of BB84, ensuring its role in secure communications well into the future.

Simulations

This chapter presents the Qiskit simulation of the BB84 protocol under an intercept-resend attack by an eavesdropper. This simulation was performed in place of the physical experiment described in Questions 2.7 and 2.8 of the practical work.

3.1 Simulation of an Intercept-Resend Attack

The goal was to simulate a 20-pulse exchange with Alice, Bob, and an eavesdropper (Eve) to observe the resulting QBER from her attack. We were unable to perform the physical experiment due to time constraints and the malfunction of the equipment. Instead, we simulated the 20-round protocol with Eve's intercept-resend attack.

The full Python code used for the simulation and its direct output are included below.

BB84 Simulation with Eve (Intercept-Resend Attack)

This notebook simulates 20 rounds of the BB84 protocol with an eavesdropper, Eve, performing an intercept-and-resend attack.

1. Imports and Setup

First, we import `cirq` for quantum simulation, `numpy` for random choices, and `pandas` to display the results in a clean table. We also define our two bases: 'R' (Rectilinear/Z-basis) and 'D' (Diagonal/X-basis).

In [1]:

```
# Install necessary libraries
!pip install -q cirq pandas
import cirq
import numpy as np
import pandas as pd

# Define the two bases: Z (Rectilinear, R) and X (Diagonal, D)
BASIS_Z = 'R' # Z-basis, Rectilinear
BASIS_X = 'D' # X-basis, Diagonal
```

2. Helper Functions

We need functions to simulate the actions of Alice, Eve, and Bob.

- `prepare_qubit`: Simulates preparing a qubit in one of the four BB84 states ($|0\rangle, |1\rangle, |+\rangle, |-\rangle$). This is used by Alice to create the initial qubit and by Eve to create her forged qubit.
- `measure_qubit`: Simulates measuring a qubit in either the 'R' (Z) or 'D' (X) basis. This is used by Eve to intercept the qubit and by Bob to get his final result.

In [2]:

```
def prepare_qubit(bit, basis):
    """Alice or Eve prepares a qubit based on their bit and basis choice."""
    qubit = cirq.LineQubit(0)

    if bit == 0:
        # Prepare |0> (for Z) or |+> (for X)
        if basis == BASIS_Z:
            # |0> state, no operation needed
             return qubit, []
        else:
            # |+> state
            return qubit, [cirq.H(qubit)]
    else:
        # Prepare |1> (for Z) or |-> (for X)
        if basis == BASIS_Z:
            # |1> state
            return qubit, [cirq.X(qubit)]
        else:
            # |-> state
            return qubit, [cirq.X(qubit), cirq.H(qubit)]

def measure_qubit(qubit, circuit, basis):
    """Bob or Eve measures the qubit in their chosen basis."""

    if basis == BASIS_Z:
        # Z-basis measurement is standard
        circuit.append(cirq.measure(qubit, key='result'))
    else:
        # X-basis measurement (apply Hadamard first)
        circuit.append(cirq.H(qubit))
        circuit.append(cirq.measure(qubit, key='result'))

    # Simulate the circuit
    simulator = cirq.Simulator()
    result = simulator.run(circuit, repetitions=1)
    measurement = result.measurements['result'][0][0]
    return measurement
```

3. Single Round Simulation

This function combines the preparation and measurement steps to simulate a single, full round of the protocol, from Alice to Eve to Bob.

1. **Alice** randomly chooses a bit and a basis, then prepares a qubit.
2. **Eve** randomly chooses a basis, measures Alice's qubit, and gets a bit.
3. **Eve** then prepares a *new* qubit based on the bit and basis she just used.
4. **Bob** randomly chooses a basis and measures the new qubit from Eve.

In [3]:

```
def run_bb84_round():
    """Simulates one full round of BB84 with Alice, Eve, and Bob."""

    # 1. ALICE
    alice_basis = np.random.choice([BASIS_Z, BASIS_X])
    alice_bit = np.random.choice([0, 1])
    qubit, prep_ops = prepare_qubit(alice_bit, alice_basis)
    alice_circuit = cirq.Circuit(prep_ops)

    # 2. EVE (Intercept-Resend Attack)
    eve_basis = np.random.choice([BASIS_Z, BASIS_X])
    # Eve measures Alice's qubit
    eve_circuit = alice_circuit.copy()
    eve_bit = measure_qubit(qubit, eve_circuit, eve_basis)

    # Eve prepares a *new* qubit to send to Bob
    eve_qubit_to_bob, eve_prep_ops = prepare_qubit(eve_bit, eve_basis)

    # 3. BOB
    bob_basis = np.random.choice([BASIS_Z, BASIS_X])
    bob_circuit = cirq.Circuit(eve_prep_ops)
    bob_bit = measure_qubit(eve_qubit_to_bob, bob_circuit, bob_basis)

    return {
        "Alice Basis": alice_basis,
        "Alice Bit": alice_bit,
        "Eve Basis": eve_basis,
        "Eve Bit": eve_bit,
        "Bob Basis": bob_basis,
        "Bob Bit": bob_bit
    }
```

4. Run the 20-Round Simulation

Now we run the simulation 20 times and store the results in a `pandas` DataFrame to view them clearly.

In [4]:

```
print("--- Running 20-Round BB84 Simulation (with Eve) ---")

results = []
for i in range(20):
    results.append(run_bb84_round())

# Display results in a clean table
df = pd.DataFrame(results)
df.index.name = "Round"
print(df.to_string())
```

```
--- Running 20-Round BB84 Simulation (with Eve) ---
      Alice Basis  Alice Bit Eve Basis  Eve Bit Bob Basis  Bob Bit
Round
0               D          0         R        1         R        1
1               R          0         D        1         D        1
2               D          0         D        0         R        0
3               R          1         D        0         R        0
4               D          1         D        1         R        1
5               R          1         R        1         D        0
```

6	D	0	D	0	R	0
7	R	1	R	1	D	1
8	D	0	D	0	D	0
9	R	1	R	1	R	1
10	D	0	R	0	D	0
11	D	1	R	0	R	0
12	R	1	D	0	R	1
13	R	1	D	1	D	1
14	D	0	R	1	R	1
15	R	0	D	0	D	0
16	D	1	D	1	R	1
17	D	0	R	0	R	0
18	R	1	R	1	R	1
19	R	0	R	0	D	1

5. Sifting and QBER Calculation

This is the final step, corresponding to **Questions 2.6 and 2.8**.

1. **Sifting:** We simulate the public channel discussion by keeping *only* the rounds where Alice and Bob's basis choices matched ('R'=='R' or 'D'=='D').
2. **QBER Calculation:** We compare Alice's original bits and Bob's measured bits *in the sifted rounds* to find the error rate.

In [5]:

```
print("\n" + "="*70 + "\n")
print("--- Sifting and QBER Calculation ---")

# Sifting: Keep only rounds where Alice and Bob's bases match
sifted_df = df[df["Alice Basis"] == df["Bob Basis"]].copy()

if len(sifted_df) == 0:
    print("No rounds had matching bases! (Unlikely, try running again)")
else:
    print(f"Bases matched for {len(sifted_df)} out of 20 rounds.")

    # Compare Alice's and Bob's bits in the sifted rounds
    sifted_df["Error"] = (sifted_df["Alice Bit"] != sifted_df["Bob Bit"])

    alice_sifted_key = "".join(sifted_df["Alice Bit"].astype(str))
    bob_sifted_key = "".join(sifted_df["Bob Bit"].astype(str))

    print(f"\nAlice's Sifted Key: {alice_sifted_key}")
    print(f"Bob's Sifted Key:   {bob_sifted_key}")

    # Calculate QBER
    num_errors = sifted_df["Error"].sum()
    num_sifted_bits = len(sifted_df)

    # Avoid division by zero if no bits were sifted
    if num_sifted_bits > 0:
        qber = num_errors / num_sifted_bits
    else:
        qber = 0 # Or float('nan')

    print("\n--- Final Result (for Q2.8) ---")
    print(f"Total Sifted Bits: {num_sifted_bits}")
    print(f"Total Errors Found: {num_errors}")
```

```
    if num_sifted_bits > 0:
        print(f"QBER = {num_errors} / {num_sifted_bits} = {qber:.2%}")
    else:
        print("QBER = N/A (no sifted bits)")

    print("\nThis QBER is the result of Eve's intercept-resend attack.")
```

```
======================================================================

--- Sifting and QBER Calculation ---
Bases matched for 6 out of 20 rounds.
Alice's Sifted Key: 101011
Bob's Sifted Key:   001011

--- Final Result (for Q2.8) ---
Total Sifted Bits: 6
Total Errors Found: 1
QBER = 1 / 6 = 16.67%

This QBER is the result of Eve's intercept-resend attack.
```

3.2 QBER Analysis

The data generated from the simulation was used to compute the QBER. This result was then compared against both the ideal, error-free case from our physical experiment and the theoretical prediction.

1. QBER for Experimental Key Exchange (No Eve) For the key exchange we performed in the lab with the professor (the results of which are in the Practical Part chapter), the outcome was ideal:

- **Total Sifted Bits (N):** 7
- **Alice's Sifted Key:** `0110010`
- **Bob's Sifted Key:** `0110010`
- **Mismatched Bits (N_{mismatch}):** 0

The QBER is calculated as:

$$\text{QBER} = \frac{N_{\text{mismatch}}}{N} = \frac{0}{7} = \mathbf{0\%}$$

This 0% QBER is the expected result for a perfect setup with no eavesdropper.

2. QBER for Simulated Eavesdropping (With Eve)

The simulation (whose output is in the previous question) produced the following results:

- **Total Sifted Bits (N):** 6
- **Alice's Sifted Key:** `101011`
- **Bob's Sifted Key:** `001011`
- **Mismatched Bits ($N_{mismatch}$):** 1

The QBER for the eavesdropping scenario is therefore:

$$QBER = \frac{N_{mismatch}}{N} = \frac{1}{6} = 0.167$$

Our simulated QBER is **16.7%**. This non-zero QBER is in the expected range of the 25% theoretical QBER (from Q1.11) and successfully demonstrates that Eve's presence introduces detectable errors, validating the security principle of the protocol.

Experimental Setup Diagrams

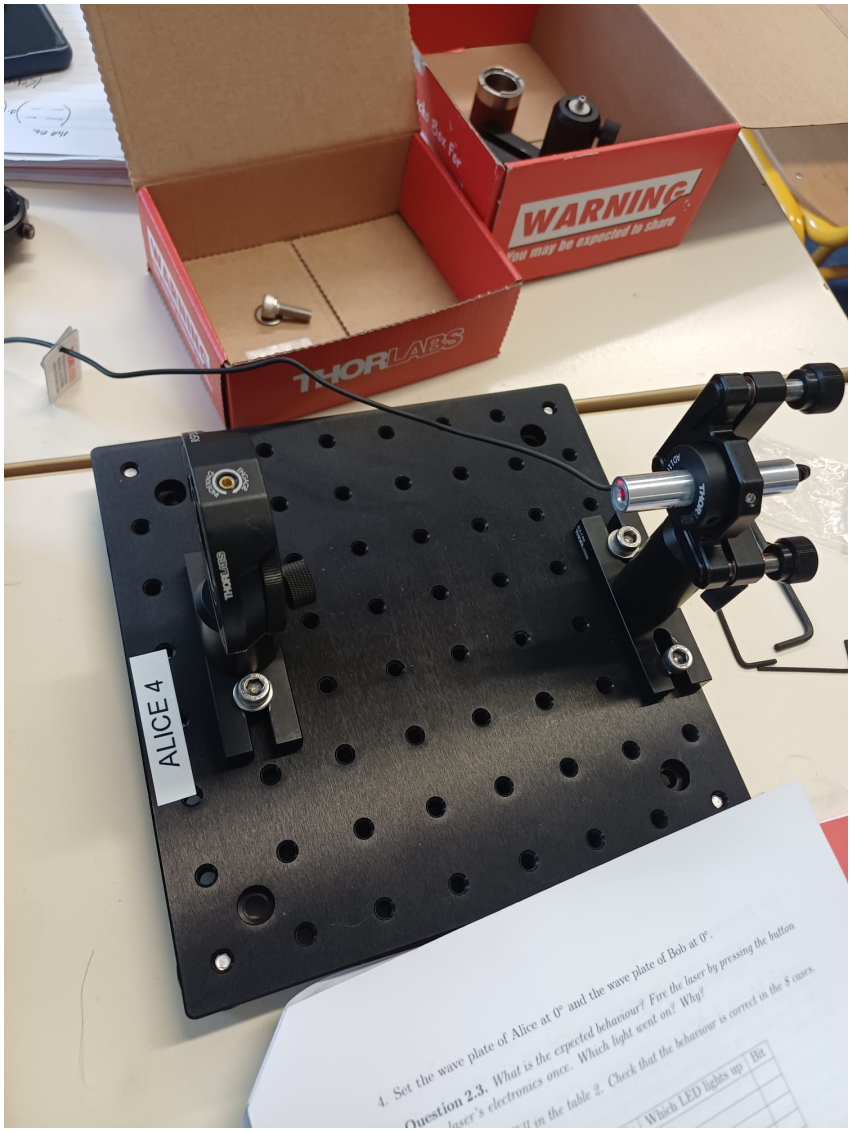

FIGURE A.1
The experimental setup for Alice's station (Encoder), consisting of the laser source and the first Half-Wave Plate.

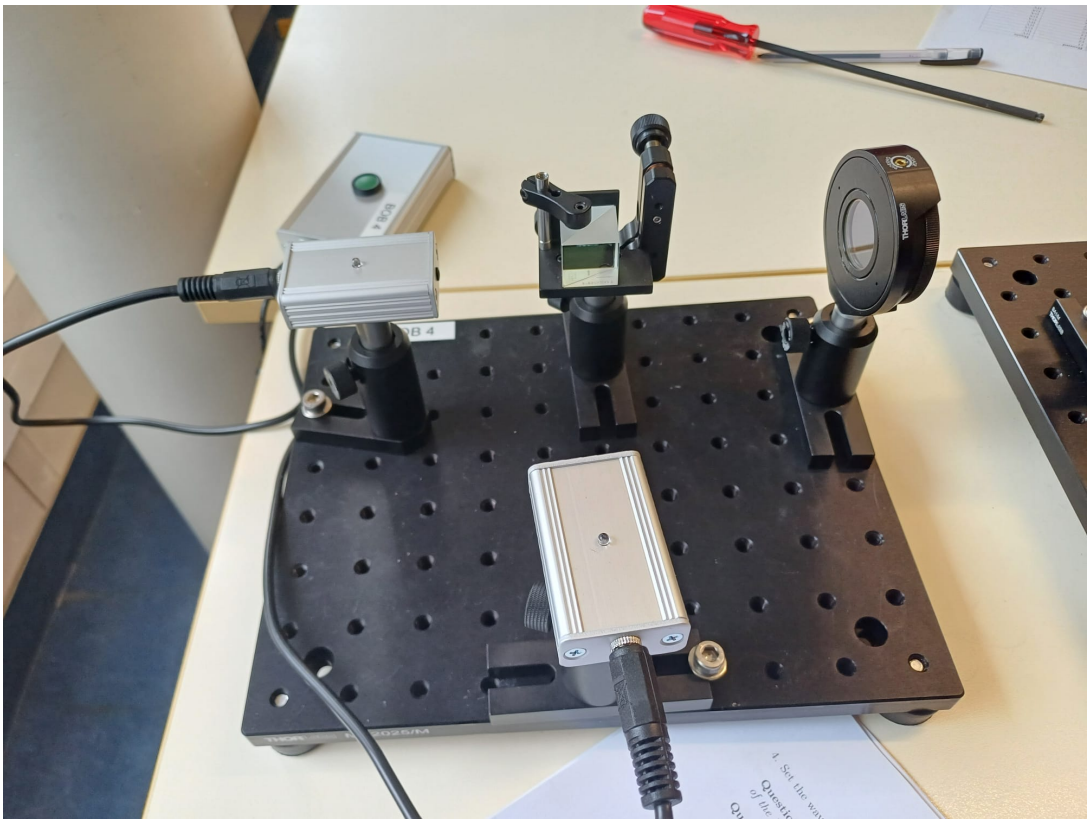

FIGURE A.2
The experimental setup for Bob's station (Decoder), consisting of the second Half-Wave Plate, the Polarizing Beam Splitter, and the two sensors.

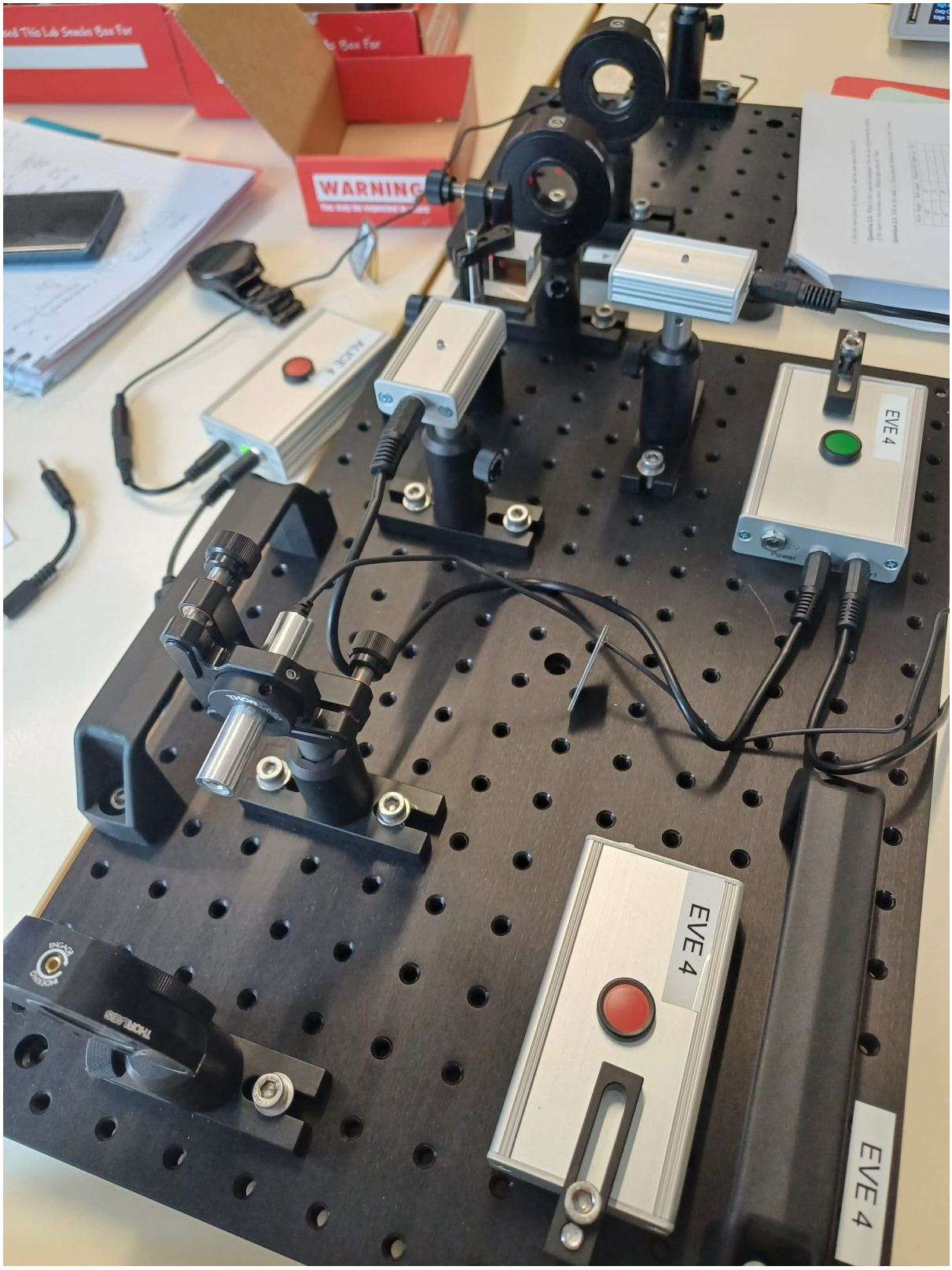

FIGURE A.3
The setup for Eve's intercept-and-resend station, which combines a copy of Bob's measurement station and Alice's sending station.

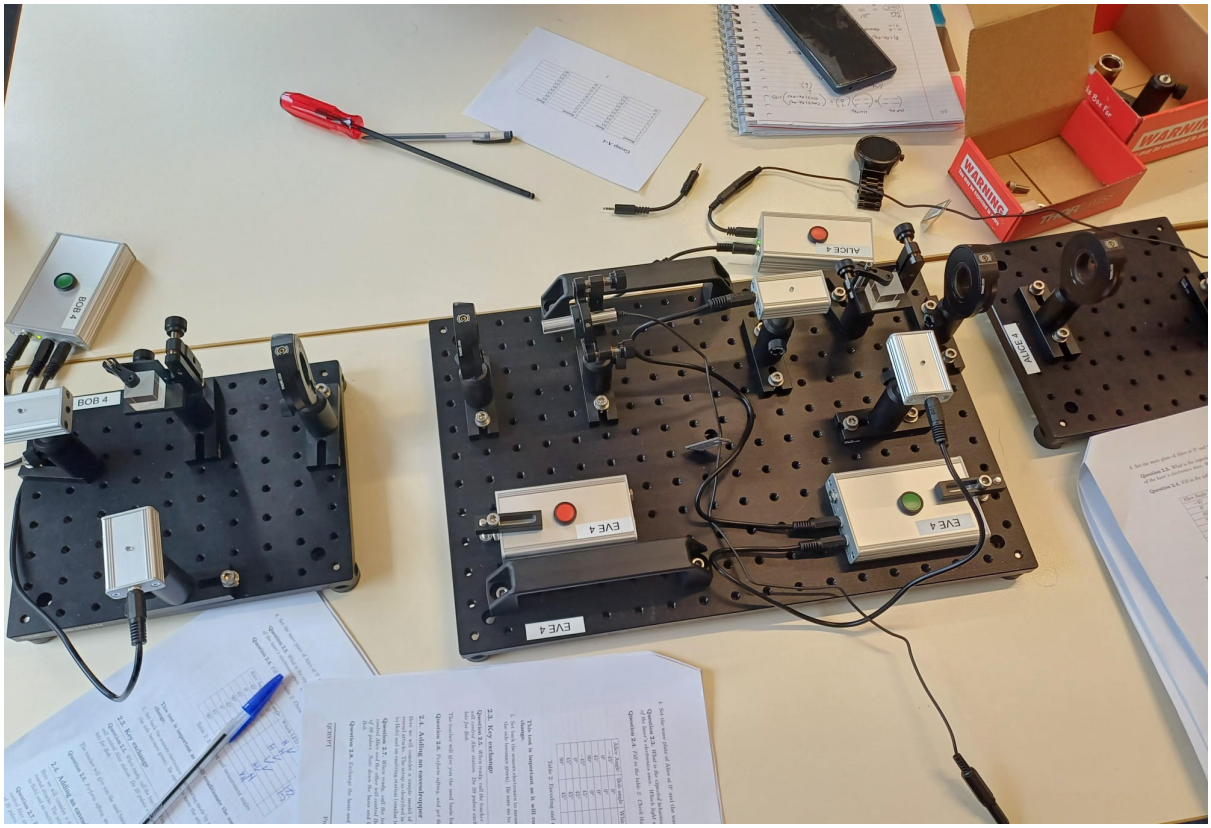

FIGURE A.4
The complete QKD experiment with Eve positioned between Alice and Bob, performing an intercept-and-resend attack.

Summary of Key Formulas

Jones Calculus

- **Polarization States:**

$$|0\rangle = |H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- **Half-Wave Plate Matrix:**

$$\text{HWP}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}$$

System Performance and Error Rates

- **Poisson Distribution (Weak Coherent Pulses):**

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}$$

- **Detection Rate (Single Photon):**

$$r_{det} = r_{source} \times T \times \eta$$

- **Detection Rate (Weak Coherent Pulses):**

$$r_{det} = r_{source} \times \mu \times T \times \eta$$

- **QBER from PBS Extinction Ratio (E):**

$$\text{QBER} = \frac{1}{E+1}$$

- **QBER from HWP Calibration Error (θ_{err}):**

$$\text{QBER} \approx \frac{1}{2}\theta_{err}^2 \quad \text{(for small } \theta_{err} \text{ in radians)}$$

Experimental Data Tables

Table B.1: System Behavior Check (Question 2.4)

Alice Angle (θ_A)	Bob Angle (θ_B)	Which LED lights up	Bit
-45°	0°	H	0
0°	0°	H	0
45°	0°	V	1
90°	0°	V	1
-45°	45°	V	1
0°	45°	H	0
45°	45°	H	0
90°	45°	V	1

TABLE C.1
Experimentally observed behavior for the 8 test cases.

Table B.2: Sifted Key Exchange Data (Question 2.6)

Alice's Basis	Bob's Basis	Bob's Measured Bit	Basis Match?	Kept Bit
X	X	0	✓	**0**
X	Z	0	X	-
X	Z	1	X	-
Z	X	1	X	-
X	X	1	✓	**1**
Z	X	0	X	-
X	Z	0	X	-
Z	X	1	X	-
X	Z	1	X	-
X	Z	1	X	-
Z	Z	1	✓	**1**
Z	X	1	X	-
X	X	0	✓	**0**
Z	X	0	X	-
Z	X	0	X	-
X	X	0	✓	**0**
X	Z	0	X	-
X	X	1	✓	**1**
X	Z	1	X	-
Z	Z	0	✓	**0**

TABLE C.2
Sifting process for the initial key exchange.

Table B.3: Simulated Eavesdropper Exchange Data (Question 2.7)

Pulse #	Alice		Eve		Bob	
	Basis	Bit	Basis	Bit Sent	Basis	Measured Bit
1	Z	0	X	1	Z	1
2	X	0	X	**0**	X	0
3	Z	0	X	0	Z	1
4	Z	1	Z	**1**	Z	1
5	X	0	Z	0	X	0
6	Z	0	X	0	Z	0
7	Z	1	X	0	Z	0
8	Z	0	Z	**0**	X	DC
9	Z	0	X	1	Z	0
10	X	1	X	**1**	X	1
11	X	1	Z	0	X	0
12	Z	1	X	1	X	DC
13	X	0	X	**0**	X	0
14	Z	1	X	1	X	DC
15	Z	1	X	1	X	DC
16	X	0	Z	1	Z	DC
17	Z	0	Z	**0**	X	DC
18	X	1	X	**1**	X	1
19	X	0	Z	1	X	1
20	X	0	X	**0**	X	0

TABLE C.3
Simulated 20-pulse exchange with an intercept-and-resend attack.

List of Experimental Components

Component	Function in Setup	Model/Reference
Laser Diode Module & Electronics (<1 mW, Class 2)	Serves as Alice's photon source. Emits linearly polarized light. The electronics control pulse or continuous wave mode.	Diode @ 637 nm
Half-Wave Plate (HWP)	Rotates the plane of polarization to encode the four BB84 states (Alice) and to select the measurement basis (Bob).	Thorlabs WPH10E-633
Polarizing Beam Splitter (PBS)	Forms the core of Bob's and Eve's measurement station. Transmits horizontal ($\|H\rangle$) and reflects vertical ($\|V\rangle$) polarization.	Thorlabs PBS201
Sensor & Electronics	Acts as Bob's single-photon detectors. Two sensors are used to detect the H and V components, and the electronics determine the final bit value.	Photodiode-based sensor unit

TABLE D.1
Key Components of the Experimental Setup