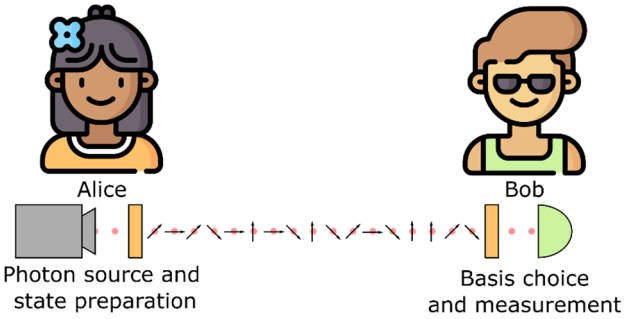
Lab manual

Quantum Cryptography



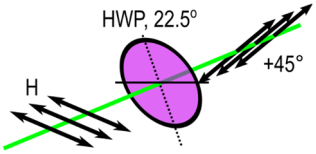
BUILD-YOUR-OWN QKD

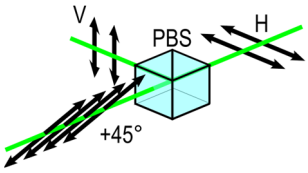
In this activity, you'll divide into two teams (representing Alice and Bob) and build your own QKD setup using lasers and polarization optics. Once it is set up, you can use to go through the BB84 protocol and securely transmit a hidden message.

Remember that the point of QKD is to generate the shared random key, **not** to the send the message. Once we finish the QKD protocol, Alice and Bob are left with a shared random key that they can use to send a message whenever they wish.

In a traditional QKD setup, Alice must have a way to prepare individual photon qubits in arbitrary polarization states, and Bob must be able to measure the light in multiple polarization bases. In this setup, Alice will use a polarized **laser** as a source of light. The laser emits horizontally polarized light, which can be rotated using a **half-wave plate (HWP)**. The HWP is a birefringent material that rotates polarization depending on its angle, as in the matrices below:

Angle	θ	$\theta = 0°$	$\theta = 22.5°$	$\theta = 45°$
Matrix	$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Gate		**Z**	**H**	**X**





To measure the polarization state, Bob will need something that distinguishes between the "0" and "1" states. To do this, we use a **polarizing beam splitter (PBS)**, which transmits horizontally polarized light and reflects vertically polarized light. By placing **detectors** to measure whether light that was transmitted or reflected, we can determine what state the photon was in in the 0/1 basis. By combining a HWP and PBS, we can effectively measure in other bases as well.

BUILD-YOUR-OWN QKD

Assemble your components and build a quantum key distribution experiment! Determine which components Alice will need and which components Bob will need. All components are **magnetic** and can be organized on the provided whiteboards. Trace the laser's path using a paper card, and use the provided polarizer to test as needed.

To read the data out, you will need to connect to the QKD software, controlled by an Arduino. Connect the red wires on the polarizer detector to the red wires in the Arduino, and the black wires to the black wires. Once it is connected, hit "PLAY" on the software. If you find the program is responding too strongly to light from the room, hit "RESET BACKGROUND" to calibrate for this.

When you're ready, **test** your system to ensure that it is aligned as expected. If Alice and Bob set their state/measurement to different settings, Bob's measured results should follow the table to the right.

Alice HWP Setting	**Bob HWP Setting**	
	H/V	**+/−**
H	0	RANDOM
+	RANDOM	0
V	1	RANDOM
−	RANDOM	1

This experiment uses a Class II Laser Product. Be aware of the laser beam at all times, do not leave it on unattended, and keep it below eye level at all times.

QUANTUM EXCHANGE

Recall the steps of the quantum exchange in BB84:

Quantum exchange

1. Alice chooses at random the bit value to send to Bob.
2. Alice chooses at random the basis she'll prepare the photon state corresponding to that bit.
3. Alice prepares the photon in that specific state and sends it to Bob.
4. Before receiving the photon, Bob chooses at random which basis he'll measure the photon in.
5. Bob measures the photon in his chosen basis.
6. Bob records the bit corresponding to the photon state he just measured.
7. Repeat steps 1-6 as many times as needed.

CLASSICAL PROCESSING

In order to extract a useful secure key from the quantum exchange, we must go through two classical post-processing steps. The first part of post-processing is **Basis Reconciliation**.

Post-processing: Basis reconciliation

8. For each bit, Alice tells Bob the basis she used **without revealing the actual bit value**.
9. Bob tells Alice to keep the bit if he measured in the same basis. If he measured in a different basis, Bob discards the bit and tells Alice to do the same.

Discussion Questions

1. When Alice sends a photon in the "+" state and Bob measures in the H/V basis, a random detector clicks. Can you relate this to the quantum measurement and superposition rules?

2. Alice and Bob used the H/V and +/– basis in this implementation of BB84. What other choices could they have made?

3. What percentage of the bits you tried to send were kept after announcing the bases? If Alice sends Bob 1000 qubits, how many would they expect to keep in the sifted key (on average)?

4. Why does revealing the basis not reveal any information about the key?

5. Alice and Bob had to choose their bases randomly and independently. Why would QKD be less secure if they publicly chose their bases together?

6. Why do the bits revealed in the error estimation step have to be removed from the key?

7. In real-life QKD systems, Alice needs a source of single photons instead of laser light. What kind of attack can Eve try with a laser beam that they can't with a single photon? Consider what happens to each at a 50/50 beam splitter.?

EXPERIMENT CHECKLIST

MATERIALS

- ☐ Alice
  - ☐ Laser
  - ☐ Pulse switch
  - ☐ Battery (6V or 4 AAs)
  - ☐ Half-wave plate (HWP)
  - ☐ Wire connections / Gator Clips (3)
  - ☐ Coins or Four-sided die
  - ☐ Worksheet / Paper
- ☐ Bob
  - ☐ Detector module
  - ☐ Arduino
  - ☐ Half-wave plate
  - ☐ Wire connectors / Gator clips (4)
  - ☐ PC
  - ☐ Coin
  - ☐ Worksheet / Paper

EXPERIMENTAL SETUP

- ☐ Alice: Connect the battery to the Pulse Switch and Laser
- ☐ Bob: Connect the Arduino to the Detectors and the PC
- ☐ Bob: Run the program and hit "RESET BACKGROUND" to account for room light
- ☐ Work together to align the laser into the detectors
- ☐ Test with known states and measurements to ensure the system is properly aligned

QUANTUM EXCHANGE

- ☐ Set up paper / spreadsheet to track results and decide on a number of qubits to send
- ☐ For each qubit:
  - ☐ Alice: Randomly choose a basis (H/V or +/−) and a bit value (0 or 1)
  - ☐ Bob: Randomly choose a measurement basis (H/V or +/−)
  - ☐ Prepare wave plates in the proper orientation, without showing the other
  - ☐ Alice: Press the pulse switch **once**
  - ☐ Bob: Write down the bit value recorded

CLASSICAL PROCESSING

- ☐ **Basis reconciliation**: Announce the basis for each qubit sent/measured, and only keep those where Alice and Bob used the same basis. The remainder is the **sifted key**
- ☐ **Error estimation**: Randomly reveal a small fraction of the bits in the key and check that they agree.
  - ☐ If they agree, discard any bits revealed and keep the rest as the **secret key**
  - ☐ If any disagree, discard the whole key and check for eavesdroppers or bugs

SENDING A MESSAGE

- ☐ Alice: Encode a message using the key and send the **cipher** to Bob
- ☐ Bob: Use the key to decrypt the cipher and reveal the **message**

WHAT ABOUT EVE?

- ☐ Introduce the Eve module and investigate the probability of introducing an error

QKD Worksheet (Alice)

	Quantum Exchange		Post-processing	
	Raw key			
	Basis HV or ±	**Bit** 0 or 1	Basis Match?	Check for Error?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

	Quantum Exchange		Post-processing	
	Raw key			
	Basis HV or ±	**Bit** 0 or 1	Basis Match?	Check for Error?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

Sifted Key																										
Secret Key																										
Message																										
Cipher																										

QKD Worksheet (Bob)

	Quantum Exchange		Post-processing	
	Raw key			
	Basis HV or ±	**Bit** 0 or 1	Basis Match?	Check for Error?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

	Quantum Exchange		Post-processing	
	Raw key			
	Basis HV or ±	**Bit** 0 or 1	Basis Match?	Check for Error?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

Sifted Key																										
Secret Key																										
Cipher																										
Message																										

APPENDIX: EXPERIMENTAL DEBUGGING

Not able to make the experiment work? Here are a few potential problems and steps to solve them.

I can't detect any light!

- Is the program running properly?
  - Make sure to hit "PLAY" when starting the program, or it won't start logging data. If you hit "STOP", you can adjust settings, but will need to hit the arrow in the menu bar to run the program again.
  - Check the tab **Debug: QKD Processing**. You should see the graph continuously collecting data if the program is running properly. If it is blank or frozen, restart and try the below steps.
  - Ensure the proper USB port is selected to communicate with the Arduino. You may need to hit "Refresh" if you unplugged and plugged back in the Arduino to the computer.
- Is the laser the problem?
  - Hold your hand in front of the laser. When you push the button, you should see a quick flash of green. If not, check the power connections and/or change the batteries.
  - Hold down the button. Does the laser light pass through the centre of the detector box opening?
  - You can adjust the height with the screw at the back of the laser mount if it needs to be tilted.

I'm detecting too much light!

- Is the Arduino connected properly?
  - If the gator clips aren't making proper contact, you have an open circuit, and the Arduino will detect a rapidly fluctuating voltage. Make sure the gator clips are connected well to both the bare wires from the detector box and the Arduino.
- Is the room light too bright or changing too much?
  - Try to avoid setting up the demo in bright areas. Roll down window curtains and turn off excess lights if possible. At minimum, don't point the detector box opening at a light source like a window.
  - Make sure the lid to the detector box is on tight and not letting light in.
  - With the experiment aligned and the laser off, hit the "RESET BACKGROUND" button. Ensure that the light level does not change after resetting the background, or else reset the background again.

I'm detecting the wrong states!

- Are the polarizers properly aligned?
  - Use an extra polarizer slide to check if the laser light is blocked or transmitted for the expected states. For example, if you set Alice to send a horizontal pulse of light, is the laser absorbed by a vertical polarizer?
  - Open the detector box lid and check where the laser light goes for different settings. You should see all the laser light end up a the "0" or "1" detector when Alice and Bob agree on the basis, and split approximately 50/50 when they disagree on the basis.
- Is it a software problem?
  - Reset the background again, as too high of a background can cause results to seem random.

APPENDIX: ENCRYPTING A MESSAGE WITH FIVE-BIT CODES

Want to use your key to send a message? Any encoding that takes letters and symbols to binary digits will work, but for the lengths of keys generated here, we recommend the **Baudot code** (ITA1), which encodes the entire alphabet into a five-bit string as in the blue table to the right.

The Baudot code was used as a standard for telecommunications throughout much of the 1900s and was optimized for special typing devices used then. However, this is not the only possible way to write the alphabet in binary. **ASCII** is the most common encoding used today, requiring seven bits per symbol. All English letters start with the bits "10", followed by the five-bit string in the red table on the right.

When Alice and Bob have confirmed their private key, they can use it to encrypt a message. For example, say Alice and Bob share the key "01101", and Alice wants to encrypt the letter "Q" in Baudot code ("10111"). Alice can do so by adding the bits of the key to the bits of the letter, as:

"Q"	1	0	1	1	1
+					
Key	0	1	1	0	1
=					
Cipher	1	1	0	1	0

Alice then sends the cipher to Bob, who decrypts it as:

Cipher	1	1	0	1	0
+					
Key	0	1	1	0	1
=					
"Q"	1	0	1	1	1

Anyone without the private key cannot decrypt the cipher.

Baudot Code					
A	1	0	0	0	0
B	0	0	1	1	0
C	1	0	1	1	0
D	1	1	1	1	0
E	0	1	0	0	0
F	0	1	1	1	0
G	0	1	0	1	0
H	1	1	0	1	0
I	0	1	1	0	0
J	1	0	0	1	0
K	1	0	0	1	1
L	1	1	0	1	1
M	0	1	0	1	1
N	0	1	1	1	1
O	1	1	1	0	0
P	1	1	1	1	1
Q	1	0	1	1	1
R	0	0	1	1	1
S	0	0	1	0	1
T	1	0	1	0	1
U	1	0	1	0	0
V	1	1	1	0	1
W	0	1	1	0	1
X	0	1	0	0	1
Y	0	0	1	0	0
Z	1	1	0	0	1

ASCII – Last Five Bits					
A	0	0	0	0	1
B	0	0	0	1	0
C	0	0	0	1	1
D	0	0	1	0	0
E	0	0	1	0	1
F	0	0	1	1	0
G	0	0	1	1	1
H	0	1	0	0	0
I	0	1	0	0	1
J	0	1	0	1	0
K	0	1	0	1	1
L	0	1	1	0	0
M	0	1	1	0	1
N	0	1	1	1	0
O	0	1	1	1	1
P	1	0	0	0	0
Q	1	0	0	0	1
R	1	0	0	1	0
S	1	0	0	1	1
T	1	0	1	0	0
U	1	0	1	0	1
V	1	0	1	1	0
W	1	0	1	1	1
X	1	1	0	0	0
Y	1	1	0	0	1
Z	1	1	0	1	0

Two examples of five-bit codes. Either can be used to send a message, but both Alice and Bob must agree on which one is being used!

APPENDIX: HALF-WAVE PLATE DETAILS

We gave a very brief description of a half-wave plate in the **Materials** section, which is sufficient to use it in this experiment. However, you may be wondering: just how does birefringence rotate the polarization of light?

The half-wave plate introduces a **phase** between two polarization components. For example, the half-wave plate at 0° introduces a phase shift of 180° (π) between the horizontal and vertical components. This occurs because the index of refraction is slightly higher for vertical light than horizontal, meaning that it travels slower through the material and picks up a small delay (equal to one-half of the wave period) relative to the horizontal component.

Recall from trigonometry that a sine wave delayed by half a period is equal to the negative of the same sine wave ($\sin(x+\pi) = -\sin x$). The delay effectively places a negative sign in front of the vertical component.

The +45° diagonal state is a superposition of H and V components, given as:

$$\nearrow = \frac{1}{\sqrt{2}} \rightarrow + \frac{1}{\sqrt{2}} \uparrow$$

If we apply a half-wave plate, the vertical component gets a negative sign instead, flipping the vector and changing the state to the -45° state, ↘. The half-wave plate switches the +45° and -45° states when it's at 0°.

By rotating the HWP to 45°, it applies a π phase between the +45° and -45° polarization states instead of the horizontal/vertical states. This leaves the diagonal states alone, but switches horizontal to vertical and vertical to horizontal instead, since we can write the horizontal and vertical states as superpositions of 45° as:

$$\rightarrow = \frac{1}{\sqrt{2}} \nearrow + \frac{1}{\sqrt{2}} \searrow \;,\; \uparrow = \frac{1}{\sqrt{2}} \nearrow - \frac{1}{\sqrt{2}} \searrow$$

By rotating the half-wave plate to different angles, we can use the birefringence to change polarization states in many ways, including switching between the H/V and +/– basis when at 22.5°.

If you are comfortable with column vectors and matrices, we can model the H, V, +, and – states as:

$\boldsymbol{H} = \rightarrow = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix}$	$\boldsymbol{V} = \uparrow = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \end{pmatrix}$	$+ = \nearrow = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}} \begin{pmatrix} \mathbf{1} \\ \mathbf{1} \end{pmatrix}$	$- = \searrow = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}} \begin{pmatrix} \mathbf{1} \\ \mathbf{-1} \end{pmatrix}$

The half-wave plate performs the following operations at certain angles, which correspond to common gates in quantum computing known as the Pauli-Z, the Pauli-X, and the Hadamard (H).

Angle	$\boldsymbol{\theta}$	$\boldsymbol{\theta = 0°}$	$\boldsymbol{\theta = 22.5°}$	$\boldsymbol{\theta = 45°}$
Matrix	$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Quantum Gate		Z	H	X