James Amidei
Quantum Computing Technologies
Quantum Encryption Lab - Individual Report

Timeline

September 9th - Day 1
I was absent. Matt and Aidan began assembly and calibration of Bob

September 13th - Day 2
Matt, Aidan, and I assembled and calibrated Alice.

September 16th - Day 3
Matt, Aidan, and I generated bases for both Alice and Bob and transmitted a signal in order to get a shared secret key.

September 18th - Day 4
Lecture day. Aidan and Matt were absent. I began to set up Eve but was unable to continue due to a lack of outlets for the three extra power supplies.

September 20th - Day 5
Aidan and Matt were absent. I joined Group B (i.e. Jessica and David) as a temporary member.
I helped calibrate and set a basis for Eve. I then operated Eve as we transmitted a signal to establish a secret key between Alice and Bob. David and Jessica then attempted to send a message using this key and found that 7 bits were mismatched, showing that an “eavesdropper” was present.

1. For this question, you will need to know about the properties of a polarizing beamsplitter. Please refer to figure 1 and its reference. In addition, you can assume that the laser is perfectly linearly polarized (which is not true but it's close enough and it simplifies these questions!). When setting up the laser, you rotate it until the reflected laser dot has minimum brightness. **Draw the polarization vector of the laser after you've performed this procedure.**

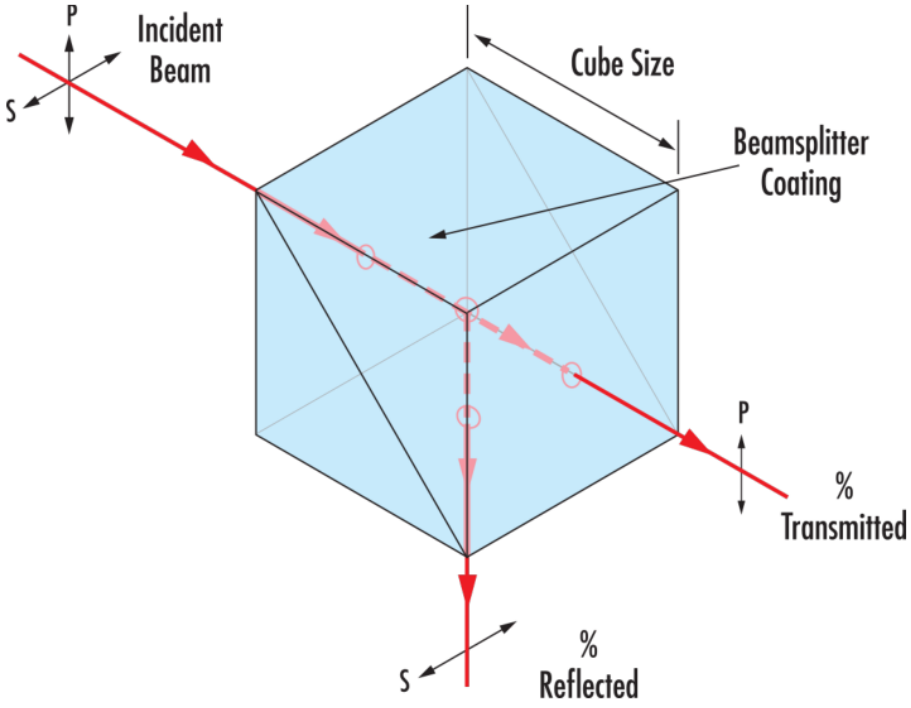
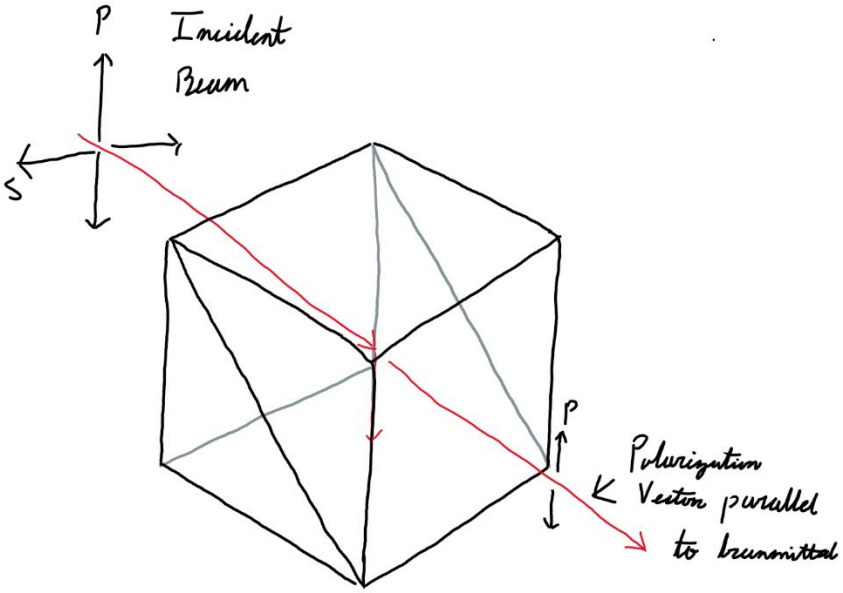


Figure 1 A polarizing beamsplitter. From https://www.edmundoptics.com/knowledge-center/application-notes/optics/what-are-beamsplitters/.



2. When setting up the half-wavelength plates, you rotate the plate until the light reflected through the beamsplitter is minimized and then set the angle marker to zero. This procedure sets the "fast axis" of the waveplate to zero degrees. Explain why. I recommend first watching this video: Half Waveplates - TDTR Short Course. For full credit, I'm looking for a clear explanation that uses images along with at least one other explanation method (text or math).

The lens of a half-wavelength plate is made of a birefringent material, which essentially means that there are two different indices of refraction which correspond to the different polarization directions of linearly polarized light. Due to this, the polarization component which travels in the direction associated with the higher index of refraction travels through the lens materials slower, resulting in a phase shift between the two polarization components. As the name half-wavelength plate may suggest, this phase shift is by half a wavelength, or 180-degrees. Since the phase shifted component travels slower than the other, we call the components the "slow" and "fast" components respectively. This is useful because we can then use these two components to form a complete basis of orthonormal vectors which can be used to describe any electromagnetic wave which travels through the half wave plate. When we take a wave which has passed through the wave plate and put it through a beam splitter, these two components are visually separated. In our case, the slow component is reflected whereas the fast component is transmitted. When we then turn the wave plate in the rotary mount, like we used in our experimental setup, so that the reflected component is minimized (or eliminated if we're assuming a perfect system) and that the only light which exiting the beamsplitter is being transmitted, we are effectively aligning the entire beam with the fast component. We can then set this position as 0-degrees on the angle marker, thus setting the axis for the fast component. Due to the orthogonality of the two components, when we then turn the wave plate so that it's at the 90-degree angle mark, this will alternatively align the entire wave with only the slow axis, so that the entire beam is reflected. To say all this more simply, when we turn the half-wavelength plate so that the reflected light is minimized, we are determining at which position the wave plate needs to be so that the entire incident beam is polarized in the fast polarization direction. By setting this at 0-degrees, we are then setting a basis with the fast component at 0-degrees and the slow component at 90-degrees, which allows us to decompose incident electromagnetic waves into these two components.

To describe this in another way, we can describe some arbitrary polarization unit vector like so:

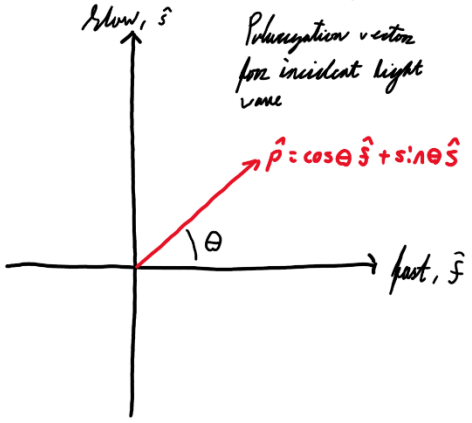


Figure 1.

By introducing this basis with the wave plate, we are able to describe a given light wave's polarization vector in terms of an orthonormal basis, which can be used to describe a linearly

polarized beam of light as a superposition of these two basis elements and to isolate the different polarization directions as needed.

3. The video linked above says that when your polarization vector hits a half-wavelength plate an angle theta relative to the fast axis, the polarization vector is rotated by 2*theta.
    a. Explain why. For full credit, I'm looking for a clear explanation that uses images along with at least one other explanation method (text or math).
    b. Is that clockwise, or counter-clockwise? Does it matter?

a)

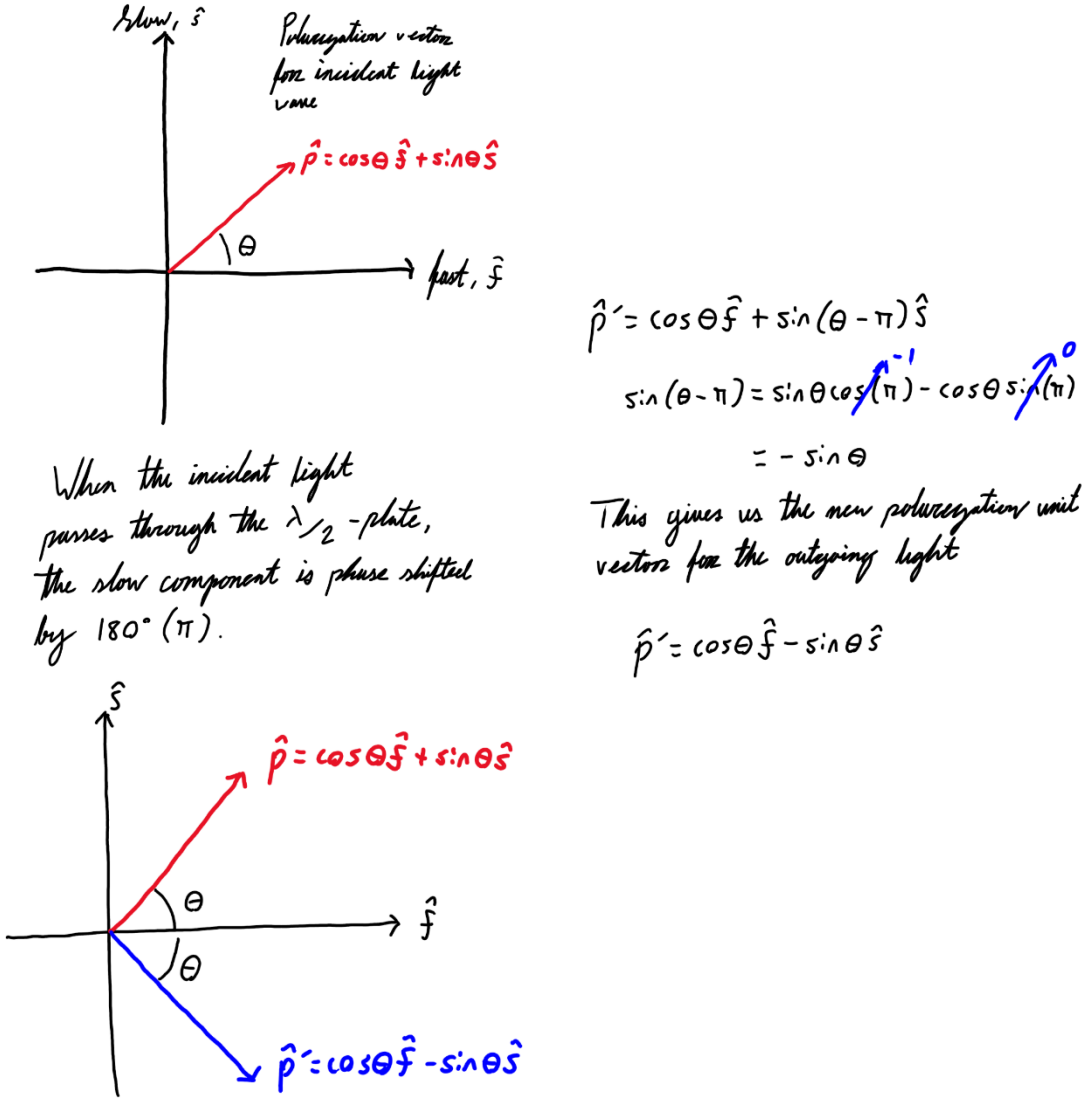


Figure 2(a), (b), (c)

We can see in figure 2(a), 2(b), and 2(c) that the slow component's phase shift by 180-degrees effectively results in its sign flipping, and the original polarization vector being mirrored across the fast axis. Since the fast component does not change, and since the angle θ is defined as the angle of the polarization vector from the fast axis, when we flip the slow component about the fast axis to form the new polarization vector, it's new angle from the fast axis is -θ. To find the difference

between these two vectors, we simply find the absolute value of the difference between the final and initial angles, which gives us $|-\theta - \theta| = 2\theta$.

If we didn't want to find this by using the definition of a phase shift like in fig. 2(b), we can simply look at the plot of the initial polarization vector, identify its projection onto the slow axis, and rotate it 180-degree so that it's flipped over the fast axis. This is why we can conceptualize the 180-degree phase shift as flipping the slow component's direction. The two new components (the flipped slow and the unchanged fast) can be recombined to create the final polarization vector. Since the magnitude of neither vector has been changed, and the sign of the fast component has also not been changed, the magnitude of the angle between the fast component and the new polarization vector will be unchanged. When we plot the initial and final polarization vectors with their respective angles from the fast axis, we can clearly see that the total distance between them will be 2θ.

b) From what I've gathered the direction of rotation depends on the orientation of the fast axis relative to the polarization vector. Essentially, you want to chose the angle orientation so that you stay in quadrants 1 or 4 (or between 90 and -90 degrees). In practice, this shouldn't matter, since you will turn the polarization vector by the same amount whether you go clockwise or counterclockwise. Calculations are simpler if you follow the convention of staying in between 9 and -90 degrees.

4. To test your setup, you checked each of the configurations in the table below. Draw the polarization of the light after it goes through the half-waveplate set to the angle in the table after Alice and then after Bob. In each case, explain why the detection result is what you'd expect from splitting the beam through a polarizing beamsplitter.

Alice	Bob	Which LED lights up	Bit
-45 degrees	0 degrees	Both	Random
0 degrees	0 degrees	Transmitted	0
45 degrees	0 degrees	Both	Random
90 degrees	0 degrees	Reflected	1
-45 degrees	45 degrees	Transmitted	0
0 degrees	45 degrees	Both	Random
45 degrees	45 degrees	Reflected	1
90 degrees	45 degrees	Both	Random

5. When transmitting from Alice to Bob without Eve, having the basis agree always meant that the bit sent also agreed. Explain why this is the case for bits 2 and 4 from the table below by explaining the polarization state of the beam and the effect of the polarizing beamsplitter on that polarization.

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

Figure 2 Without Eve, when the basis is the same for Alice and Bob the bit is always the same.

6. Explain how the BB84 encryption protocol works in the absence of Eve. Please be clear about what information is publicly exchanged and what information remains private. For full credit, you need to explain
    a. How the one-time pad (also called the "key") is generated
        i. How does it remain private to both Bob and Alice?
        ii. Why is it the same for both Bob and Alice?
    b. How data is encrypted and sent
    c. How data is received and decrypted
    d. What keeps the message private?

a) Alice generates a random sequence of bits (either 0 or 1), each with a corresponding basis (either + or x). She then sends the sequence of bits to Bob who measures the sequence through his own randomly generated basis. Wherever Alice and Bob's bases match, the same bit value will be transmitted. The basis information can be publicly exchanged without sharing information about the specific bits and used to develop a shared key which can be used to encrypt and decrypt information. Essentially, you know that wherever the bases match, the bit was successfully transmitted, and thus the specific bit information is superfluous when establishing a key. This is secure because quantum states cannot be copied without being disturbed (i.e. the no-cloning theorem). This is essentially a recapitulation of the idea that measuring a quantum state changes it.
b) Data is encrypted using the shared key that was generated by sending a random string of bits and by sharing the basis information to establish where the bases matched. In order to actually encrypt the data, the message sender will pick a string of bits which correspond to some information or message they want to send. This string will then have the key "added" to it using binary addition, returning an encrypted form of the information/message. This encrypted information/message is then transmitted to Bob from Alice in the same manner as before.
c) Once Bob has received the encrypted message, he will take the bits from the locations in the total sting where they know the bases match then decrypt the message by "adding" the shared key again via binary addition. This will return the original binary string that corresponds to the message that Alice wanted to send.
d) Because the key is randomly generated, the encrypted message will remain secure so long as the key is not shared. Additionally, due to the fact that quantum mechanical properties are used in transmission of the message, the measurement of the message at any point between Alice and Bob will result in mismatched bases in the key. This allows for Alice and Bob to identify if an eavesdropper is present by publicly comparing their keys to see if there are any mismatches.

7. Now consider the case with "Eve," the eavesdropper. Explain how transmission 5, where Alice and Bob have the same basis but different bits, happens (given what Eve does to the signal).

Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
Bit	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

Bob

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
Bit	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

Eve

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basis	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
Bit	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

Figure 3 The presence of Eve introduces errors in the one-time key.

In the case of 5, since Eve is present, she introduces the error we see by measuring the signal transmitted by Alice. Since Eve does not know which basis Alice has chosen (since Alice's basis was chosen randomly) Eve has a 50% chance of choosing the incorrect basis. When Eve measures the signal from Alice in the correct basis, the quantum state is undisturbed, and Eve is able to transmit the corresponding bit with no changes. When Eve measures Alice's signal in the incorrect basis, the quantum state is disturbed and the information contained in the original state is destroyed. In this case, Eve will have a 50% chance of detecting the incorrect bit, which will then result in it transmitting a signal to Bob in the incorrect basis. Similarly, since Eve and Bob's bases mismatched, this results in a 50% chance of Bob measuring the incorrect bit through his own basis. So, even though Alice and Bob share the same basis, Eve having chosen the incorrect basis results in a chance of Bob measuring a different bit than the one that was transmitted by Alice.

So, for 5, where Alice is trying to send bit 1 in the + basis (which corresponds to Alice's wave plate being set to the 90-degrees mark) we can see that Eve has chosen the incorrect basis, as she is reading the signal from Alice in the x basis. This means that Eve's measurement will disturb the state of Alice's signal, resulting a 50% chance of either a 0 or 1 being measured. Since Eve measured a 1, this means that her transmitting wave plate is set to the 45-degree mark before passing the signal along to Bob. Since Bob is in the + basis, a signal from the x basis will have a 50% chance of being measured as either a 0 or 1. As we can see in this case, a 0 was measured, when the correct bit would have been a 1.

8. The consequence of question 7 is that Alice and Bob have different one-time keys. Explain how they can use a publicly-available test transmission to detect the difference in keys.

After going through the transmission process in number 7, Alice and Bob can publicly exchange their bases

From 7, we can see that when Alice and Bob exchange bit information Alice will have the key ‘0110010001’ and Bob will have ‘0100000000’.