James Amidei

Quantum Computing Technologies

Lab #2, Quantum Cryptography - 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.

A diagram of a polarizing beam

Description automatically generated

A drawing of a cube with lines and arrows

Description automatically generated

A close up of text

Description automatically generated

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:

A graph of a function

Description automatically generated with medium confidenceFigure 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.

A close-up of a white background

Description automatically generated

a)

A white paper with text and a red line

Description automatically generatedA math equations and formulas on a white paper

Description automatically generatedA diagram of a mathematical equation

Description automatically generatedFigure 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 |-θ - θ| = 2θ.

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.

A screenshot of a computer

Description automatically generated

(continued on next page)

A close-up of a white board

Description automatically generated

(4 continued)

A whiteboard with math equations and numbers

Description automatically generated

(4 continued)

A math equations and formulas written on a white surface

Description automatically generated

(4 continued)

A math equations and formulas

Description automatically generated with medium confidence

(4 continued)

A white board with math equations

Description automatically generated

(4 continued)

A math equations on a white background

Description automatically generated

(4 continued)

A math equations and formulas

Description automatically generated with medium confidence

(4 continued)

A math equations and formulas on a white background

Description automatically generated

A close-up of a mathematical equation

Description automatically generated

(4 continued)

A math equations and formulas

Description automatically generated with medium confidence

(4 continued)

A graph of mathematical equations

Description automatically generated

(4 continued)

A math equations and formulas

Description automatically generated with medium confidence

(4 continued)

A math equations and formulas

Description automatically generated with medium confidence

A table of maths with red circles

Description automatically generated

(continued on next page)

A whiteboard with math equations and numbers

Description automatically generated

(5 continued)

A math formula and a circle

Description automatically generated with medium confidence

When we say that Alice is set at the -45-degree mark, we mean that Alice's wave plate's fast-axis is at some angle -45/2 = -22.5 -degrees from the 0-axis. This means for an incident beam whose polarization vector is aligned with the 0-axis, the polarization vector will be rotated 2\*-22.5-degrees =  -45-degrees from its original polarization and align with the -45-degree axis. Similarly, when we say that Bob is set at the 45-degree mark, we mean that  Bob's wave plate's fast axis is at 45/2 = 22.5-degrees above the 0-axis.

When a beam whose polarization axis was initially aligned with the 0 axis passes through Alice's waveplate and becomes aligned with the -45-degrees axis then passes through Bob's wave plate, it will have a +22.5-degree difference from the 0 axis, which has a -45-degree difference with the polarization vector after passing through Alice's wave plate. This means that the polarization vector will have a difference of 22.5 - (-45) = 67.5-degrees from Bob's wave plate's fast axis. This means that the polarization vector will be rotated 2\*67.5 = 135-degrees from its initial -45-degree axis so that it aligns with the -0 axis. Since it is now aligned with one of the eigenvectors in the, it will pass purely in the direction of that eigenvector. Since the 0 axis corresponds to the transmitted direction, this means 100% of the light will be transmitted.

(5 continued)

A math equations and formulas on a white background

Description automatically generated

In a similar vein as above, when Alice is at 45-degree, its fast axis is oriented at 22.5-degree up from the 0 axis. This means when our initial beam passes through Alice, its polarization vector is rotated by 2\*22.5=45-degrees counterclockwise so that it aligns with the 45-degree axis. When this new beam passes through Bob, which is also oriented at 45-degrees with its fast axis at 22.5-degrees up from the 0 axis, it is rotated by twice the difference between its polarization vector and the fast axis. This means that it is rotated by 2\*22.5=45-degrees counterclockwise from the 45-degree axis, making it align with the 90-degree axis. Since 90-degrees corresponds to the reflection eigenvector in the beamsplitter, this means 100% of the light is reflected.

A white background with black text

Description automatically generated

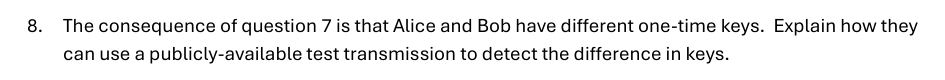
1. Alice generates a random sequence of bits (either 0 or 1), each with a corresponding basis (either + or x). She then sends the sequence of bits to Bob who measures the sequence through his own randomly generated basis. Wherever Alice and Bob’s bases match, the same bit value will be transmitted. The 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.
2. 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.
3. 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.
4. 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.

A screenshot of a math test

Description automatically generated

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.



After going through the transmission process in number 7, Alice and Bob can publicly exchange their bases without exchanging their bit information. This allows them to determine what should be a shared secret key which can be used to encrypt and decrypt messages. In order to test their keys, so as to determine if an eavesdropper was present or not, they can follow the procedure in 7 by sending a test message. For example, let’s say they chose to send the word ‘HI’ and converted it into binary using the table below.

A table of numbers and binary addition table

Description automatically generated

‘HI’ would be written in binary as 00111 01000. This message would then be encrypted by Alice using her key, which can be read off from 7 as 0110010001. Alice would add her key to the binary string using the binary addition rules on the table above to get

0011101000

+ 0110010001

0101111001

This encrypted message would then be transmitted to Bob, who would receive it and then attempt to decrypt it by adding his key to the encrypted message, getting

0101111001

+ 0100000000

0001111001

Converting this back into letters, this gives us D=00011 and Z=11001, which makes ‘DZ’. Since Bob is unable to decrypt the message, this suggests that the two keys were off. Because of this, Alice and Bob can conclude that there must have been an eavesdropper, and thus discard their keys.