QUANTUM CRYPTOGRAPHY WRITEUP

TEAM REPORT

1. Please describe your setup and testing of "Alice" and "Bob," the sender and receiver. Do not include "Eve," the eavesdropper.
    a. Include the table of test cases
    b. and your sheets for generating the key and sending a message.
    c. Describe your procedure for doing both. You don't need to tell me how you set up every single bit you sent; one example is enough.
2. Please describe how you added "Eve," the eavesdropper.
    a. Include the table of test cases
    b. and your sheets for generating the key and sending a message.
    c. Describe your procedure for doing both. You don't need to tell me how you set up every single bit you sent; one example is enough.

INDIVIDUAL REPORT – ALL STUDENTS

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.**

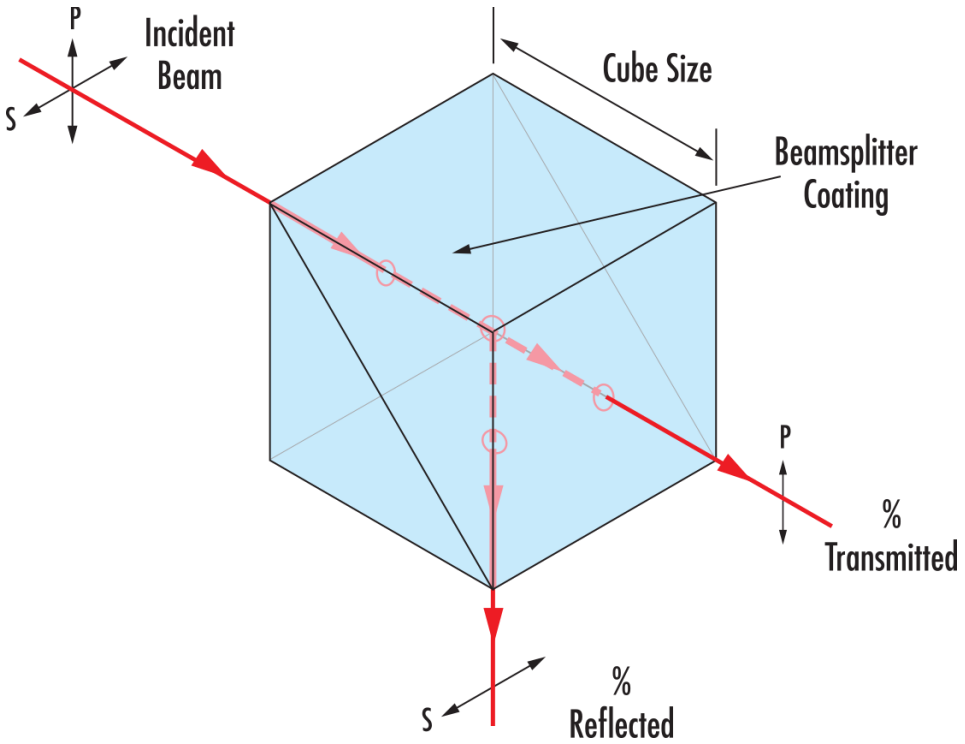

Figure 1 A polarizing beamsplitter. From https://www.edmundoptics.com/knowledge-center/application-notes/optics/what-are-beamsplitters/.

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).
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?
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?
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.

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.

QUESTIONS FOR GRADUATE STUDENTS

1. Explain the expected error rate in the test transmission when an eavesdropper is present.
2. What was the error rate in your test transmission?
3. Read the article "Quantum Internet Protocol Stack: a Comprehensive Survey". Discuss how the current internet protocol stack does not work for the quantum internet, and how the new quantum internet protocol stack differs from the traditional approach.
4. What are some of the practical difficulties in implementing the BB84 protocol? The article, "Modified BB84 quantum key distribution protocol robust to source imperfections" has some useful citations regarding implementation in the introduction. For full credit, please identify two difficulties and explain them in plain language.