Quantum Crpytography

Matthew Crane, Aidan Garcia St. George, James Amidei

Dr. Martin Huber, Dr. Amy Roberts

University of Colorado at Denver
PHYS 4680/ELEC 5680: Quantum Computing Technology
Fall 2024

Part A:

This section of the experiment was primarily focused on assembly and calibration of the laser electronics, sensor electronics and optical components required for this exercise. The laser electronics included a power supply and linearly polarized laser, while the sensor electronics consisted of two sensors and a sensor power supply. The optical components consisted of (2) beam-splitter cubes, (2) beam stops, (4) half-wavelength plates, and (1) alignment tool. It is important to note that all optical components must be handled with extreme care to prevent unwanted contamination. Once general assembly had been completed, the calibration of the devices shortly followed.

To calibrate the laser, the screw that clamps the laser to the adapter ring was loosened which allowed for the laser to be rotated. The intensity of the laser decreased and increased during rotation, and the laser orientation with minimal intensity was selected to complete the experiment. With the laser properly orientated, the half-wavelength plates were calibrated. The half-wavelength plates were calibrated by placing an individual half-wavelength plate between the laser and beam-splitter and rotating the $\lambda/2$-plate such that minimal reflection from the beam-splitter was observed. With the $\lambda/2$-plate oriented such that minimal reflection was observed, the $\lambda/2$-plate was set to 0° and this process was repeated for each plate.

With all electronics and optical components properly calibrated, the sender (Alice), and the receiver (Bob) were constructed. Alice consisted simply of the laser and (1) $\lambda/2$-plate and is depicted in fig. (1) below.

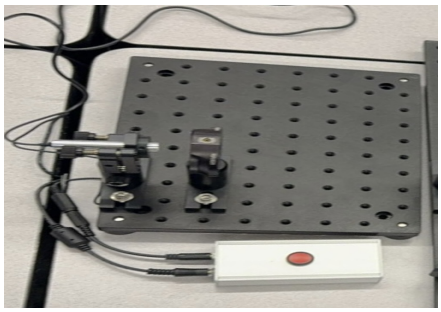


Figure 1: Alice (sender) Configuration

The receiver (Bob) configuration was slightly more involved than Alice. Bob consisted of a $\lambda/2$-plate, beam-splitter cube, and two sensors. The three possible sensor activation cases included reflected, transmitted, or both and are depicted in fig. (2) below (respectively).

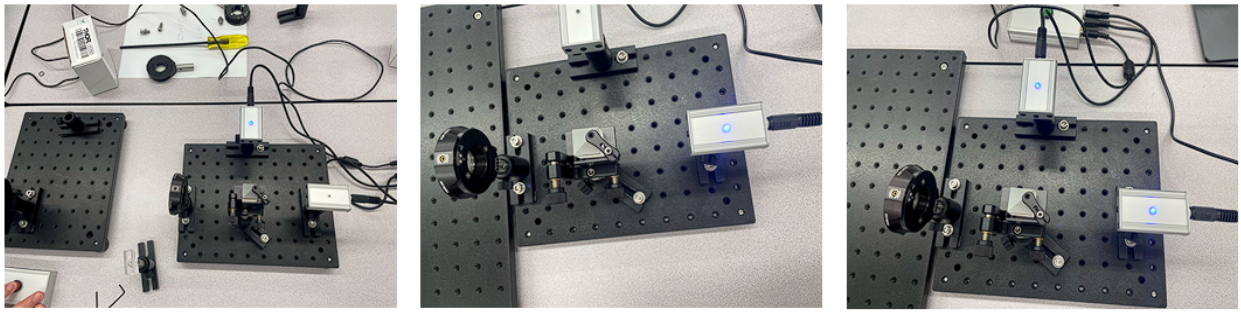


Figure 2: Bob (Receiver) Configuration

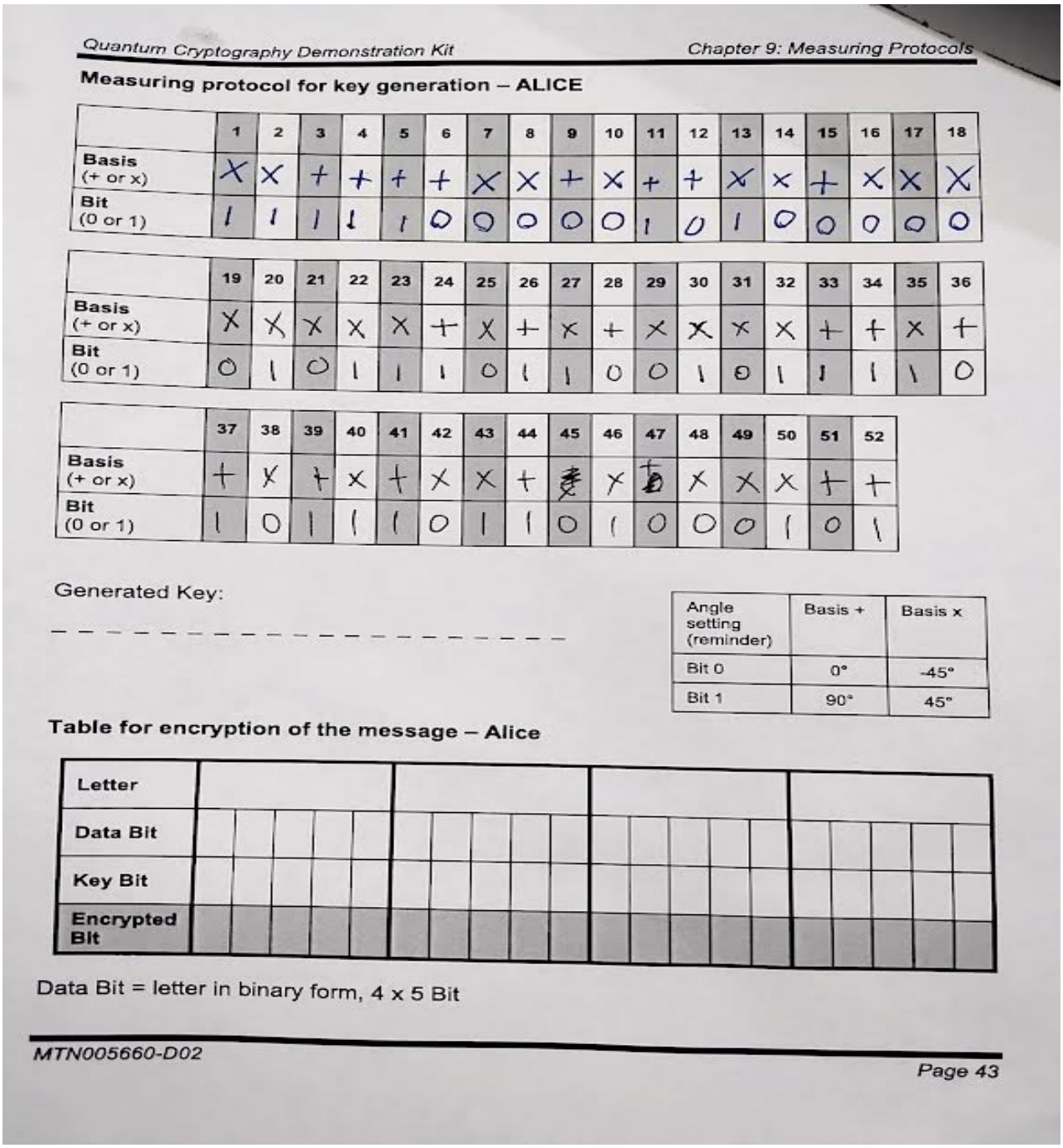
With Alice and Bob constructed, further calibration was required via the completion of test cases. With the sensor box in measuring mode, all possible orientations of the $\lambda/2$-plates were tested. The possible orientations, as well as which LED on Alice is expected to signal, are given below in fig. (3).

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

Figure 3: Test Cases

Initially, some test cases were failed and slight alignment changes were made throughout the process. Once final alignment had taken place, all test cases were passed and we proceeded with the experiment.

In order to test the transmission of a signal from Alice to Bob, bases were chosen for both by performing a series of coin flips with heads corresponding to the + (0° - 90°) basis and tails to the x (−45° - 45°) basis. Additionally, a bit series for Alice was chosen with this same method. The tables for these can be seen in fig. (4) and fig. (5) below.



Quantum Cryptography Demonstration Kit *Chapter 9: Measuring Protocols*

Measuring protocol for key generation – ALICE

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

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis (+ or x)	X	X	X	X	X	+	X	+	X	+	X	X	X	X	+	+	X	+
Bit (0 or 1)	0	1	0	1	1	1	0	1	1	0	0	1	0	1	1	1	1	0

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Basis (+ or x)	+	X	+	X	+	X	X	+	X	X	+	X	X	X	+	+
Bit (0 or 1)	1	0	1	1	1	0	1	1	0	1	0	0	0	1	0	1

Generated Key:

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Angle setting (reminder)	Basis +	Basis x
Bit 0	0°	-45°
Bit 1	90°	45°

Table for encryption of the message – Alice

Letter																		
Data Bit																		
Key Bit																		
Encrypted Bit																		

Data Bit = letter in binary form, 4 x 5 Bit

MTN005660-D02 *Page 43*

Figure 4: Test Key for Alice

With both bases established, the random string of bits was transmitted from Alice to Bob, where it was processed through Bob's own basis. The results of Bob's intake of Alice's message was recorded, and the bases of Alice and Bob were compared. Anywhere that the bases matched was selected and used to form a shared secret key for transmitting further messages. This can be seen in fig. (5), where the circles columns form the shared secret key.

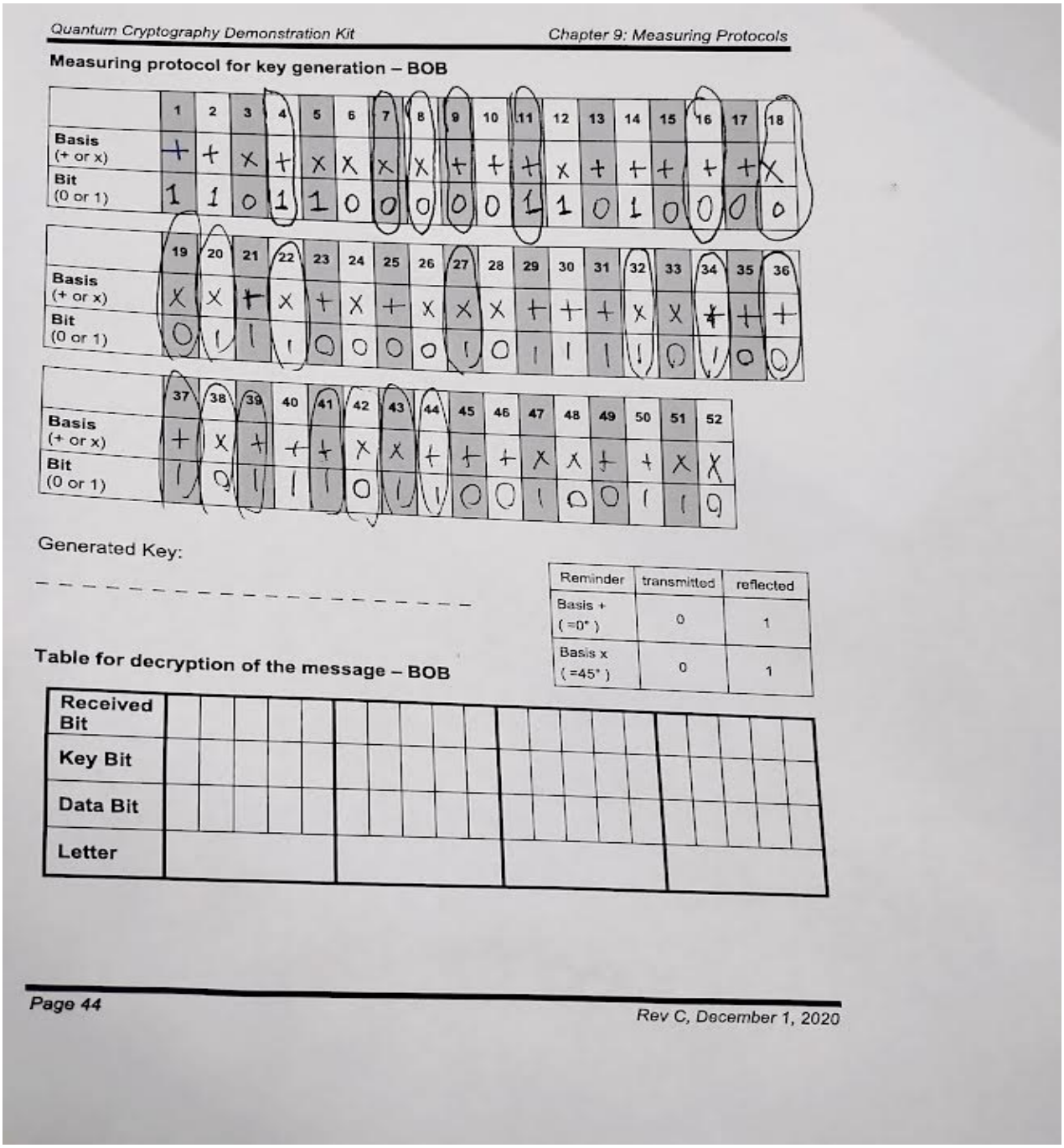


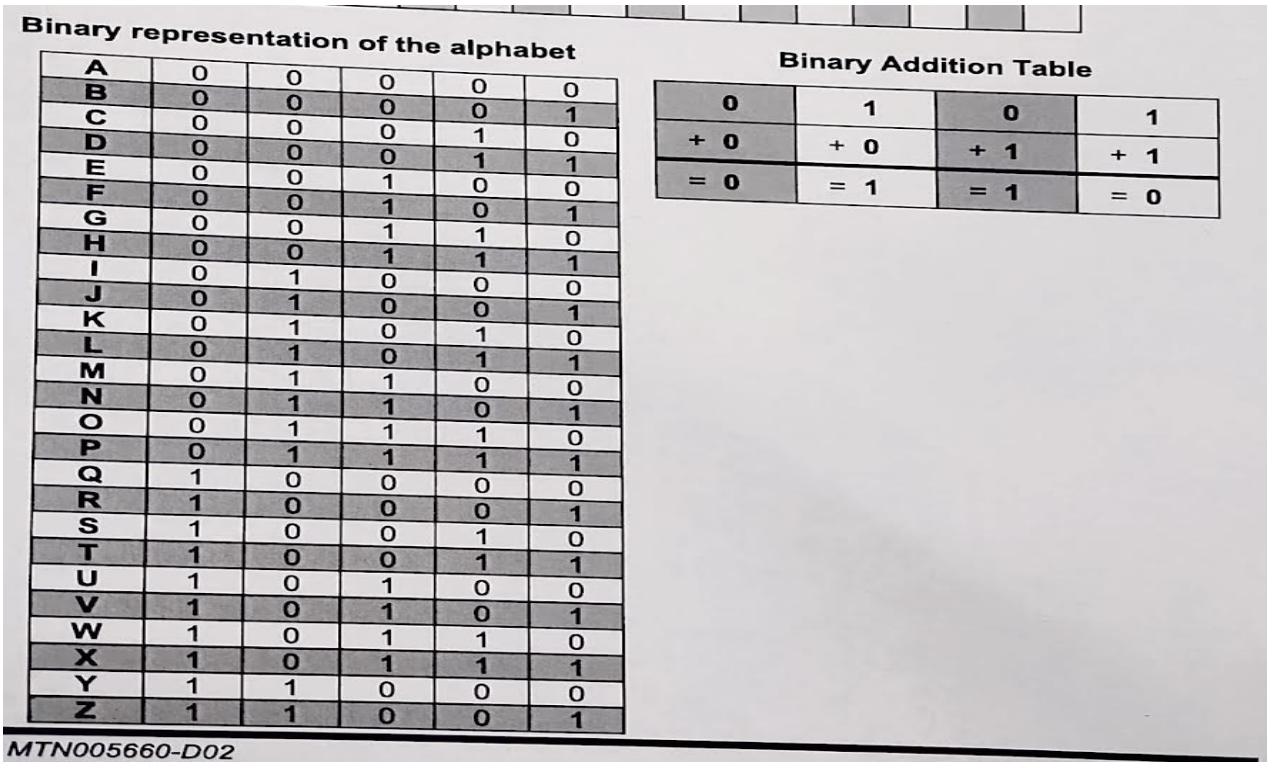
Figure 5: Test Key for Bob

It is worth noting that fig. (5) above contains several error. First, column 16 was circled when column 15 should have been circled instead. Second, column 48 should have been circled, meaning that a total of 22 bits were successfully transmitted, rather than the 21 seen above. This is likely because the comparison was done hastily towards the end of lab. A corrected version of the table can be seen on the following page in Table (1).

	Alice Basis	**Alice Bit**	**Bob Basis**	**Bob Bit**	**Match/No Match**
1	x	1	+	1	No Match
2	x	1	+	1	No Match
3	+	1	x	0	No Match
4	+	1	+	1	Match
5	+	1	x	1	No Match
6	+	0	x	0	No Match
7	x	0	x	0	Match
8	x	0	x	0	Match
9	+	0	+	0	Match
10	x	0	+	0	No Match
11	+	1	+	1	Match
12	+	0	x	1	No Match
13	x	1	+	0	No Match
14	x	0	+	1	No Match
15	+	0	+	0	Match
16	x	0	+	0	No Match
17	x	0	+	0	No Match
18	x	0	x	0	Match
19	x	0	x	0	Match
20	x	1	x	1	Match
21	x	0	+	1	No Match
22	x	1	x	1	Match
23	x	1	+	0	No Match
24	+	1	x	0	No Match
25	x	0	+	0	No Match
26	+	1	x	0	No Match
27	x	1	x	1	Match
28	+	0	x	0	No Match
29	x	0	+	1	No Match
30	x	1	+	1	No Match
31	x	0	+	1	No Match
32	x	1	x	1	Match
33	+	1	x	0	No Match
34	+	1	+	1	Match
35	x	1	+	0	No Match
36	+	0	+	0	Match
37	+	1	+	1	Match
38	x	0	x	0	Match
39	+	1	+	1	Match
40	x	1	+	1	No Match
41	+	1	+	1	Match
42	x	0	x	0	Match
43	x	1	x	1	Match
44	+	1	+	1	Match
45	x	0	+	0	No Match
46	x	1	+	0	No Match
47	+	0	x	1	No Match
48	x	0	x	0	Match
49	x	0	+	0	No Match
50	x	1	+	1	No Match
51	+	0	x	1	No Match
52	+	1	x	0	No Match

Table 1: Corrected table for comparison of Alice and Bob's bases and bit values.

From Table 1, the shared secret key can be read off as 1000100011111010110110. Since the next step would be to transmit a four letter word using the base-5 English-alphabet to binary table in fig. (6), only the first 20 bits are needed, resulting in the adjusted shared secret key 10001000111110101101.



Binary representation of the alphabet

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

Binary Addition Table

0	1	0	1
+ 0	+ 0	+ 1	+ 1
= 0	= 1	= 1	= 0

MTN005660-D02

Figure 6: Binary representation of the alphabet.

Using fig. (6), a binary string can be constructed to form a word which can be encrypted and then transmitted. For example, the word 'JINX' would be represented as 01001 01000 01101 10111. The binary string representation of 'JINX' would be encrypted using the key through binary addition, as seen on fig. (6). Doing this returns

	0	1	0	0	1	0	1	0	0	0	0	1	1	0	1	1	0	1	1	1	(Message)
+	1	0	0	0	1	0	0	0	1	1	1	1	1	1	0	1	0	1	1	0	1	(Key)
	1	1	0	0	0	0	1	0	1	1	1	0	0	0	0	1	1	0	1	0	(Encrypted Message)

This encrypted message would then transmitted from Alice to Bob, which will receive the transmitted bits where ever the bases match. Once Bob has received the encrypted message, the key would then be "added" again in order to "decrypt" the original message.

	1	1	0	0	0	0	1	0	1	1	1	0	0	0	0	1	1	0	1	0	(Encrypted Message)
+	1	0	0	0	1	0	0	0	1	1	1	1	1	1	0	1	0	1	1	0	1	(Key)
	0	1	0	0	1	0	1	0	0	0	0	1	1	0	1	1	0	1	1	1	(Message)

After this, the original message can be transliterated back into the English-alphabet via the table in fig. (6).

Part B:

After Alice and Bob were setup, Eve (the "eavesdropper") was added. Eve had two components: an intake component and a transmitting component. The intake component was very similar to Bob, being composed of a $\lambda/2$-plate in series with a beam-splitting cube, followed by two sensors, situated so that they were 90-degrees from each other in the breadboard's plane. The $\lambda/2$-plate was configured to either 0° or 45°, corresponding to either the + or x basis respectively, which was determined by performing 52 coin flips; similar to the way the bases were determined for Alice and Bob. The transmitting component was made up of a laser beam in series with a $\lambda/2$-plate, configured in an initially undefined basis.

Eve's calibration followed a similar procedure to the one described in Part A. First, the intake component was assembled and bolted to the breadboard so that it was directly between Alice and Bob so that Alice's laser would go directly through Eve's intake $\lambda/2$-plate. Once in place, Alice's laser was placed in calibration mode so that it formed a continuous beam. This was sent through the $\lambda/2$-plate, into the beam-splitter, and aligned with the entrances of both of Eve's sensors. Once this step was completed, the sensors were placed in adjustment mode, and the series of test cases from fig. (7) were checked. After this step was completed, Eve's transmitting component was assembled and calibrated by placing a laser in a mount, placing a $\lambda/2$-plate in front of it on the same breadboard, and positioning it so that the light from the laser fed directly into Bob. Once this was done, the $\lambda/2$-plate was rotated such that minimal reflection from Bob's beam-splitter was observed. After this, the $\lambda/2$-plate was set to 0° and the test cases from fig (7) were checked and adjustments were made as needed.

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

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

Figure 7: Calibration test cases for laser beam transmitting into sensors. This is the same protocol which was followed in Part A.

It is worth noting that Eve's setup and calibration process was split over two days due to a lack of outlets for three additional power supplies needed for the two sensors in the intake component and the laser in the transmitting component.

Part C:

With Eve in place and calibrated, the experiment would start with Alice transmitting a signal, which would then be intercepted by Eve's intake component. The signal from Alice would travel through the intake component's $\lambda/2$-plate, through the beam-splitting cube, and then light up one of the two sensors. Depending on which sensor measured Alice's signal, the basis for the

transmitting component's $\lambda/2$-plate was then set; if Alice's signal was observed to be transmitted through the intake component, this would correspond to the + basis, and if reflected, the x basis. With the transmitting $\lambda/2$-plate's basis was set, the laser was used to pass a signal along to Bob, which would then be recorded and read with respect to Bob's established basis.

Unfortunately, this part of the experiment was left unfinished due to unavoidable absences in the group. In order to complete the lab, collaboration with Group A (i.e. David and Jessica's group) was done on the final day of lab.

James joined Group A as a temporary member and aided in setup and operation of Eve. First, the calibration of each component was tested by running through the test cases in fig. (7). Eve's sensors were found to be misaligned and adjustments had to be made. Each member set the basis for the component they were going to operate; David was set to operate Alice and Jessica was set to operate Bob. This was done by flipping a coin 52 times, with heads corresponding to the + basis and tails to the x basis. After the bases were set, bits were sent from Alice to Eve, where Eve's transmission basis would be set and a message would be sent from Eve to Bob. This process had to be restarted once due to operator error of Eve, but this was caught fairly early and the process was easily corrected. This produced the following basis for Eve in fig. (8)

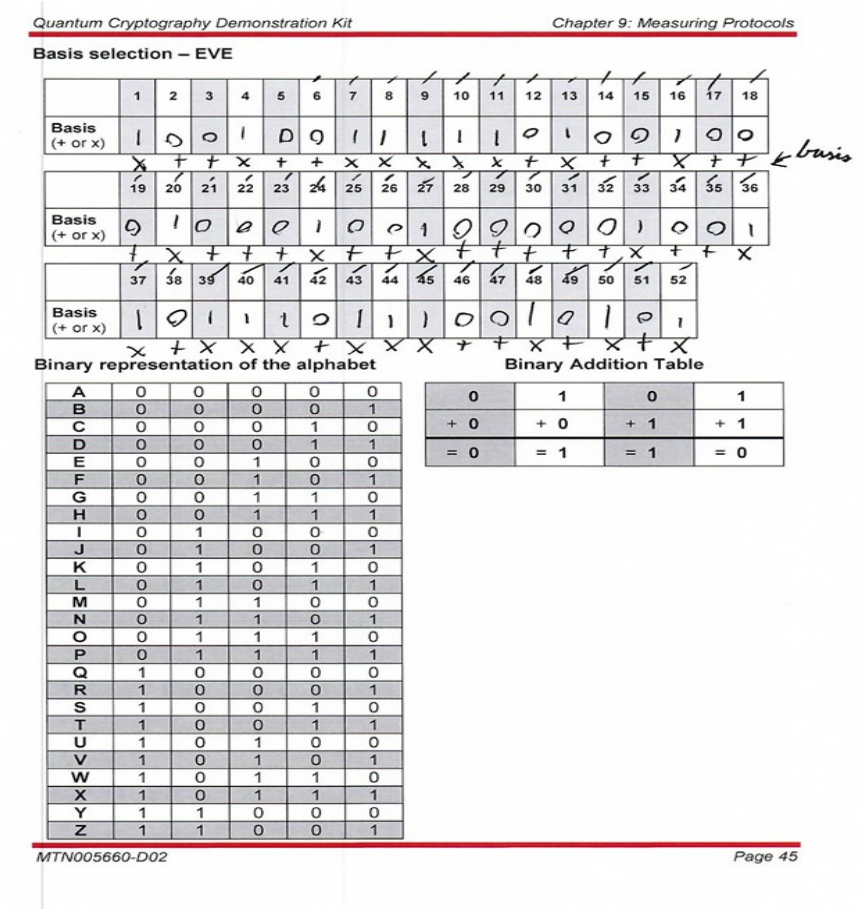
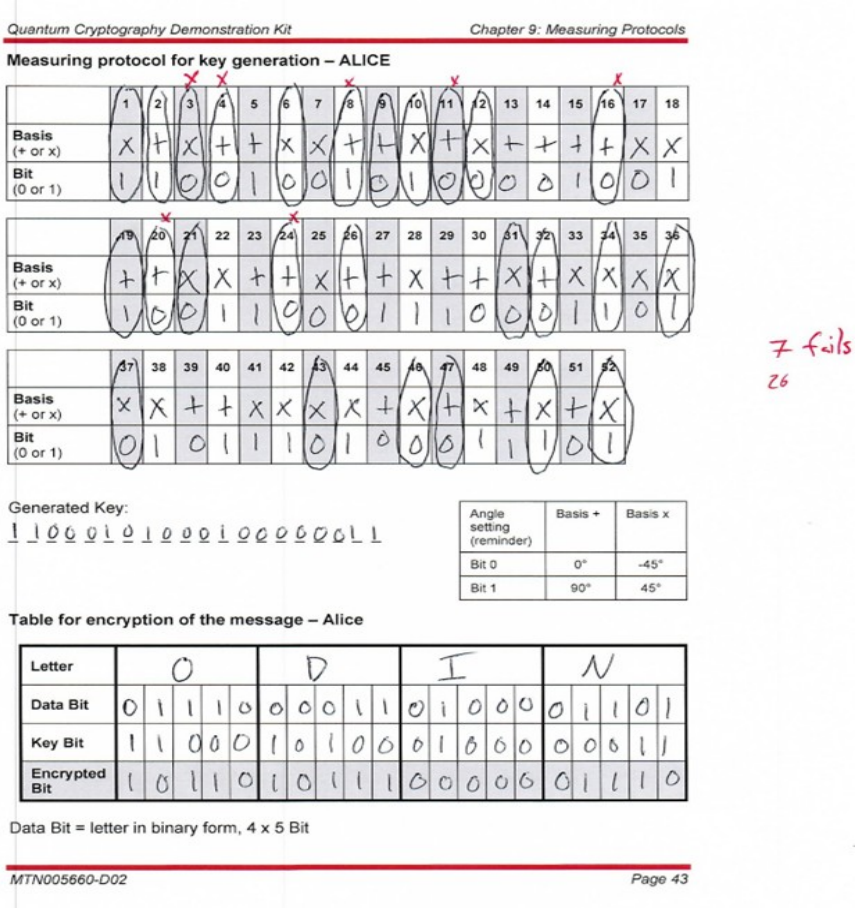


Figure 8: Eve's basis and message from Group A.

Once all the bits were transmitted, David and Jessica publicly compared bases without comparing bits. This allowed them to determine what should be the shared secret basis. Group A then decided to send a message without Eve in order to test this new key. In a previous test, they had decided to send the four letter word "ODIN'. To try and see how the introduction of

Eve changed the message, 'ODIN' was chosen again so that the two tests could be compared. In binary 'ODIN' is written as 01110 00011 01000 01101, from fig. (6). Alice's key was found to be 11000101000100000011. This can also be seen in fig. (9).



Quantum Cryptography Demonstration Kit *Chapter 9: Measuring Protocols*

Measuring protocol for key generation – ALICE

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

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Basis (+ or x)	+	+	x	x	+	+	x	+	+	x	+	+	x	+	x	x	x	x
Bit (0 or 1)	1	0	0	1	1	0	0	0	1	1	1	0	0	0	1	1	0	1

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Basis (+ or x)	x	x	+	+	x	x	x	x	+	x	+	x	+	x	+	x
Bit (0 or 1)	0	1	0	1	1	1	0	1	0	0	0	1	1	1	0	1

7 fails
26

Generated Key:
1 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0 1 1

Angle setting (reminder)	Basis +	Basis x
Bit 0	0°	-45°
Bit 1	90°	45°

Table for encryption of the message – Alice

Letter	O					D					I					N				
Data Bit	0	1	1	1	0	0	0	0	1	1	0	1	0	0	0	0	1	1	0	1
Key Bit	1	1	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	1	1
Encrypted Bit	1	0	1	1	0	1	0	1	1	1	0	0	0	0	0	0	1	1	1	0

Data Bit = letter in binary form, 4 x 5 Bit

MTN005660-D02 *Page 43*

Figure 9: Message, basis, key, and encrypted message for Alice from Group A.

This encrypted message was transmitted from Alice directly to Bob. The results of this measurement through Bob's basis were as follows, in fig. (10).

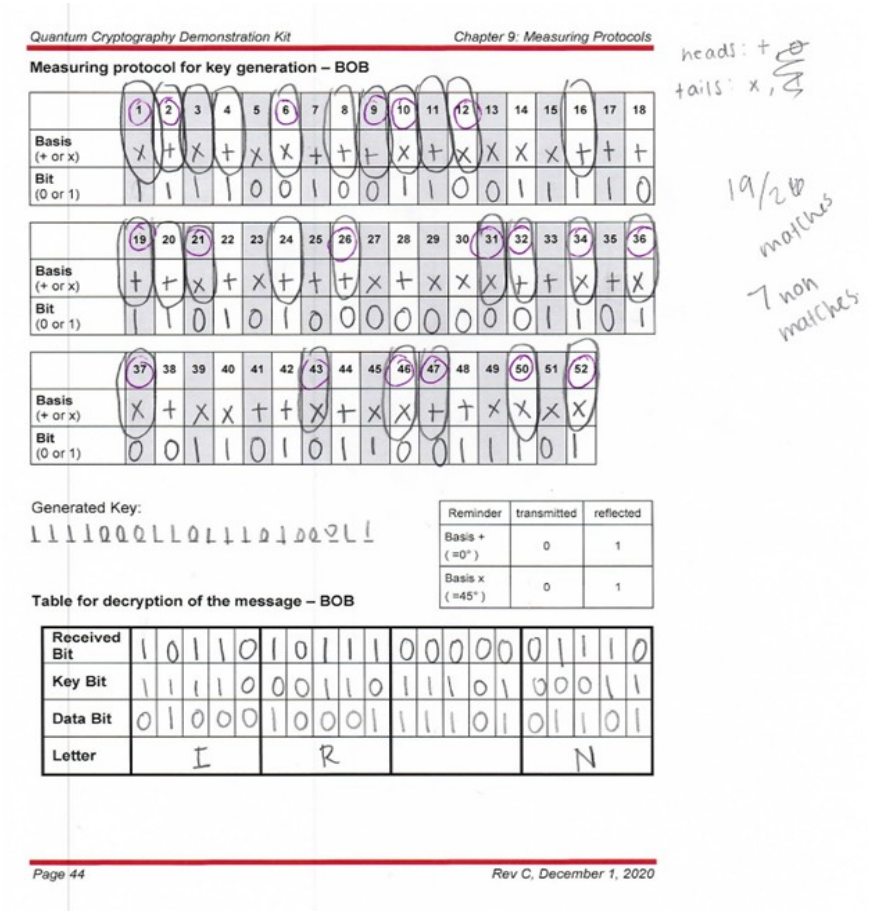


Figure 10: Encrypted message after being sent through Eve.

As we can see from fig. (10), transmission of the word 'ODIN' failed. Instead, the word 'IR?N' was transmitted, where '?' indicates an invalid letter value. This is due to the fact that the base-5 alphabet representation has $2^5 = 32$ possible values while there are only 26 letters in the English-alphabet. From figs. (9) and (10), there were 7 cases where bits were mismatched in Bob's key. This error in the key seems to be substantial enough to conclude that there was an "eavesdropper" present during the key transmission process.

References

[1] Thorlabs. (n.d.). Quantum Cryptography Demonstration Kit. Thorlabs, Inc. - Your Source for Fiber Optics, Laser Diodes, Optical Instrumentation and Polarization Measurement & Control, September 30, 2024