CIS 492/593 Hands-On Lab 4 Quantum Key Distribution Fall 2023

In this hands-on lab, you will study and practice two Quantum Key Distribution methods:

- the BB84 protocol (see textbook page 53)
- the Ekert protocol (see textbook page 87)

Login to a workstation and open a terminal (either middle click the terminal icon on the left side bar or press CTRL-ALT-T). In the terminal window, type

```
cd QC
jupyter notebook
```

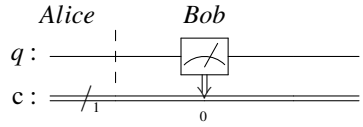
Inside the browser, click "New" and choose "Python 3 (ipykernel)". For each experiment, you need to put the experiment number as a comment (e.g. `# Experiment 1`) in the top of the code.

Experiment 1: Alice's Encoding and Bob's Measurement using the same basis

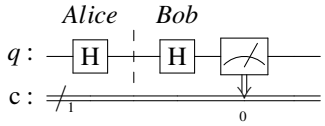
- In the cell, type

  ```
  %load ~cis492s/pub/BB84Test.py
  ```

  and click "Run" to load a simple program. In this program, Alice prepares and sends a qubit with value 0 in the vertical direction to Bob. Bob measures the qubit in the same direction. The procedure is like the diagram below.



  Note that the barrier used here is only an indication of work separation between Alice and Bob. Click "Run" to get and record the result.
- Click the cell done in the previous step. Click the "Edit" button and select "Copy Cells". Click "Edit" again and choose "Paste Cells Below".
  Assume that Alice encodes the qubit in the horizontal direction instead of the vertical direction. That is, she applies the H-gate on the qubit. Also assume that Bob measures the qubit in the horizontal direction. Modify the code just like the figure below:



  Click "Run" to get and record the result. What is your conclusion about the result if Alice and Bob use the same basis?

Experiment 2: BB84 emulation (without Eve's eavesdropping)

- In a new and empty cell, type

  ```
  %load ~cis492s/pub/BB84.py
  ```

  and click "Run" to load the Qiskit program which emulates the BB84 protocol into the cell. Study the code.

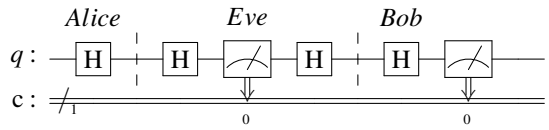
- Click "Run" to get the outputs. Record the outputs (i.e. "Alice bits", "Alice bases". "Bob bases", and "Bob results") in your report. Mark the bit positions where Alice and Bob use the same bases and then extract the corresponding bits from "Alice bits" and "Bob results" into two bit sequences.
- Alice and Bob will select half of the same-basis bits and compare them over an unencrypted line. For simplicity, we just choose the first half of the sequence as the sample bits. Add the code at the end of the cell:

```
sample_size = len(alice_bits_samebasis) // 2
alice_sample = alice_bits_samebasis[0:sample_size]
bob_sample = bob_bits_samebasis[0:sample_size]

print("sample size:", sample_size)
print("alice_sample = ", alice_sample)
print("  bob_sample = " , bob_sample)

print(bob_sample == alice_sample)
```

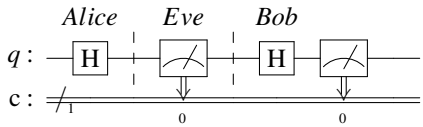
  Click "Run" to execute the code. What is the size of the sampling bits? Note that if the result is True, Alice and Bob can use the other half of the bit sequence as the key.
- Modify the code to change the value of the variable `n` from 4 to 1000. Click "Run" to execute the code to make sure that the program works for a larger size of bit sequence.

Experiment 3: Alice's Encoding and Bob's Measurement using the same basis (with Eve's eavesdropping)

- Click the cell done in Experiment 1 which contains the code based on the horizontal direction. Click the "Edit" button and select "Copy Cells". Click "Edit" again and choose "Paste Cells Below".
- Assume that Eve intercepts the qubit on the way from Alice to Bob and she luckily uses the same basis (i.e. the horizontal direction) to measure the qubit. She then prepares and sends Bob a qubit based on the horizontal basis. To emulate Eve's interception, add four lines of code (including a barrier call at the end) before Bob's action, like the diagram below.



  Click "Run" to get the result. Is there any difference as compared with the result in Experiment 1 (the horizontal direction)? Can Eve's eavesdropping be detected if Alice, Eve, and Bob use the same basis?
- Now assume that Eve guesses the wrong basis to measure the qubit. Click the cell done above. click the "Edit" button and select "Copy Cells". Click "Edit" again and choose "Paste Cells Below". Modify the code so Eve will use the vertical direction to measure and encode the qubit before sending to Bob, like the figure below:



Click "Run" to get and explain the result.

Experiment 4: BB84 emulation (with Eve's eavesdropping)

- Click the cell which contains the code done in Experiment 2. Click the "Edit" button and select "Copy Cells". Click "Edit" again and choose "Paste Cells Below".
- In this experiment, you are asked to add some code between Step 2 and Step 3 to emulate the actions of Eve. That is, she firstly generates a random choice of basis for each bit. Next, she measures each qubit based on the generated random choice of basis. Finally, she encodes the message again based on the generated random choice of basis and then sends the message to Bob. Click "Run" to execute your code and get the result.
- In addition to getting the result False at the end of the previous step, we are also interested in getting the percentage of the sample bits in which Alice and Bob disagree. Add a few lines of code at the end to get the percentage and verify it with the textbook (page 55, lines 23–26).
  Hint: Use a counter and a loop to compare each Alice's sample bit with Bob's sample bit. Increment the counter if they disagree. Output the ratio of the counter over the size of the sample bits.

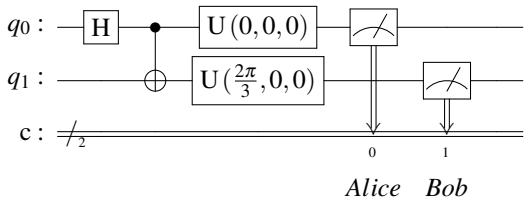
Experiment 5: Ekert – Measuring two entangled bits with different bases

Based on the textbook description about the Ekert91 protocol, Alice and Bob receive a stream of qubits. For each entangled pair of qubits, Alice receives one and randomly chooses a direction to measure her qubit, while Bob gets the other and also randomly selects a direction to measure it. There are three directions Alice and Bob can use: 0°,120°, or 240°. If they choose the same direction, they will get the same result (i.e. both get 0 or both get 1). However, if they use different directions, they may not get the same result. In this experiment, we are interested in getting the probability that they will AGREE the result, and the probability that they will DISAGREE the result, under the condition that thy will use different directions to measure.

- Note that these three directions 0°,120°, and 240° can be implemented by a Qiskit U-gate via passing the first parameter with a value 0, $2 * pi/3$, $4 * pi/3$, respectively. The fourth parameter is the index of the qubit where the the U-gate will be applied.
  In a new cell, type

  ```
  %load ~cis492s/pub/EkertTest.py
  ```

  and click "Run" to load a simple program. In this program, Alice always measures her qubit in the direction 0°, while Bob always uses the direction 120° to measure. Below is the circuit diagram:



- Study the program. Click "Run" to execute the code. Calculate the probability they AGREE (i.e. combining the percentages of '00' and '11') and the probability they DISAGREE (i.e. adding the percentages of '10' and '01') .
- Repeat previous step with Alice using 0° and Bob using 240°. Calculate the two probabilities.
  Repeat previous step with Alice using 120° and Bob using 240°. Calculate the two probabilities.
  Repeat previous step with Alice using 120° and Bob using 0°. Calculate the two probabilities.
  Repeat previous step with Alice using 240° and Bob using 0°. Calculate the two probabilities.
  Repeat previous step with Alice using 240° and Bob using 120°. Calculate the two probabilities.

Experiment 6: Ekert emulation (without Eve's eavesdropping)

- In a new cell, type
  ```
  %load ~cis492s/pub/Ekert.py
  ```
  and click "Run" to load the program which emulates the Ekert protocol.
- Study the program. Add a line of code at the end of the program to print the probability that Alice and Bob AGREE the result when they use different bases.
- Click "Run" to execute the code. Verify your result with the equation on Textbook page 81, line 5.

Experiment 7: Ekert emulation (with Eve's eavesdropping)

- Click the cell which contains the code done in Experiment 6. Click the "Edit" button and select "Copy Cells". Click "Edit" again and choose "Paste Cells Below".
- To emulate Eve's eavesdropping, add one line of code
  ```
  message[q].measure(1,1)
  ```
  before Alice measures her entangled qubit in the function `measure_message()`.
- Click "Run" to execute the code. Compare the probability that Alice and Bob AGREE when they use different bases with the corresponding probability in Experiment 6. Verify your result with the description on Textbook page 87, lines 14–16.
- Is the probability that Alice and Bob AGREE the result when they use the same basis still 1 as in the Experiment 6?

Click "File" and choose "Save as". Type "lab4" in the entry box and click "Save" to save your work today into the file `lab4.ipynb`.

To turn in your file, use CTRL-ALT-T to open a terminal and type

```
ssh grail
```

and type your password to login to the server grail. Then, type

```
cd QC
turnin -c cis492s -p lab4 lab4.ipynb
```

to electronically submit your file `lab4.ipynb`.

Shutdown the jupyter notebook and logout the workstation.

Hand in your lab report before your leave.