Bob 2 (Eve) - Mission 1: Establishing Classical Communication

Qcamp 2019, Experimental Session 22/05/2019

80 minutes of gameplay [70/200 points]

As a group of physicists who naturally have curious minds, you read a seminal 1984 paper by Bennett and Brasard about quantum cryptography. After talking with your friends and colleagues, you are pretty convinced that this scheme will work nicely, but with a little catch: you have a limited funding and you can't buy single photon detectors.

Then, one day, your friend has a genius and evil idea. Your friend is also a good friend with the people from the communication companies Alice and Bob. By using the quantum physics mumbo jumbo, your friend will convince those companies to invest in the new quantum technologies. The evil plan is that, you already know that their communications will not be secure, and you will eavesdrop into their channel.

You also notice that the new security company Charlie (Alice 2) is also developing some IR technologies, similar to the one used by Alice and Bob. You have a plan to also talk to them about this eavesdropping thingy. Your vision is to convince Alice and Bob of the need to use single photon detectors, and hope that by doing this "evil" mission, they will be convinced and buy you the single photon detectors you needed all along. **The aim of this mission is to understand this particular BB84 QKD implementation, which will be used with Alice and Bob later, and also looking (possibly) for some methods to eavesdrop into the channel.**

This mission is divided into smaller tasks, which consists of compulsory and optional tasks. The compulsory tasks are marked with either [Checkpoint], [Final Task], or [Secret Task] flags, while the unmarked tasks are sort of optional. It is thus a priority to complete all the flagged tasks before the optional tasks, as one will not be able to revisit these tasks after the deadline. The compulsory tasks are very important for the upcoming missions. It is also highly advisable to split the tasks among your teammates.

You team is *very lucky* to be assigned such an **important role**.

Good luck for the mission.

Have a lot of fun!

[10 points] BREAK the ice, STOMP the ground, LIFT the air

> ***This is sort of compulsory, but only to get the group going :P***

Objectives:

1. Choose a team captain,
2. Write down a short company manifesto, and
3. Take a team photo.

Point allocation scheme:

- [Full] points upon completion of the objectives.

Step by step walkthrough:

1. A good team is a team whose members knows each other pretty well.
2. A good team is also a team which can split the tasks in an efficient manner. Actually sooner or later, your team might be split into 2 (or even 3) subteams. So, plan well ahead.

[30 points] [Checkpoint] Align the polarisation

> ***No! Marty! We've already agreed that having information about the future can be extremely dangerous. Even if your intentions are good, it can backfire drastically!***
> ***- Dr. Emmit Brown***

Objective: You are going to emulate what the signal sender (Alice) and the signal receiver (Bob) will be doing, so you might also want to split the team into the `sender / Alice` and the `receiver / Bob`. You will need to understand this process pretty well as it will be useful in the later parts (mostly for hacking). Particularly, in this mission, you need to:

1. Align the polarisation between Alice (the sender) and Bob (the receiver),

   Alice's H polarisation might be oriented differently from Bob's H polarisation (imagine their heads are tilted), so alignment is required.

2. Obtain the intensity matrix, with signal degradation less than 0.255, and

   Degradation indicates how different Alice's H,D,V,A's are from Bob's.

3. Be prepared to undergo some short Q&A sessions with the facilitator to test your understanding.

Very important notes: Read the safety precautions in Section 1.3.1 of the technical documents. This is *extremely important*, as you will get tested about this at the end of the session (no joking, confirm plus chop!).

Point allocation scheme:

- [Full] points upon completion of the objectives
- [80%] of total points upon completion of the objectives, but with the signal degradation higher than 0.25.
- [10%] of total points reduction for each unsatisfactory Q&A session. This reduction is capped at [30%] of total points.

Step by step walkthrough:

1. Start the Arduino app and upload the Arduino program `ArduinoQuantum.ino` to the correct device.
2. Run the polarisation alignment `GUI` programs (in the folder `Alignment GUI`): For Alice, `runSender.py` and for Bob, `runReceiver.py`. You might want to refer to `Section 3.4.3` for more information regarding the GUI. The goal of this exercise is to align Alice and Bob polarisation axis with respect to each other, i.e. if Alice sends `H` polarised light, and Bob measures in `H` polarisation basis, the measurement result should give maximal intensity. *You need to close the GUI (or at least stop the device) before moving on to other tasks.*
3. Set the correct device address in `devloc_quantum.txt`. Run the calibration program `send_calibrate.py` (for Alice) and `recv_calibrate.py` (for Bob). This program measures the `Intensity Matrix` between different polarisation states of Alice and Bob. Make sure that the signal degradation is lower than 0.25 (or repeat the previous step if not), and note down the mean value of the intensity.
4. Be prepared for the Q&A sessions. You might wish to start asking your facilitator questions when you encounter something that you don't really understand. This Q&A sessions will be in effect from now until the conclusion of Mission 2.

[10 points] Polarisation basis handout

> ***Give me six hours to chop down a tree and I will spend the first four sharpening the axe.***
> ***- Abraham Lincoln***

Objective: Complete the `Polarisation Basis` handout. No cheating or copying with Charlie allowed [insert stern warning].

Point allocation scheme:

- Based on the number of correct responses in the handout.

Note: Only do this when there is a free time or there is a member in your group who happens to be free.

[20 points] [Final Task] Establishing secure key

> ***There is an interesting similarity between probabilistic encryption and quantum cryptography: both rely on the notion of reduction. However, whereas the former reduces the unproved computational complexity of some outstanding problems of number theory to the difficulty of breaking the schemes, the latter relies on the most fundamental beliefs of quantum physics.***
> ***- Dave Barry***

Objectives:

1. Successfully construct a secure key derived from 16 bit polarisations choices and bases made by Alice and Bob, and keysifted via a public channel.
2. Try to construct 2 to 4 secure keys with those methods, but with Alice "not communicating" with Bob nor looking at his paper or computer (vice versa). The only communication allowed is the `public channel` paper that is passed back and forth between them.

Point allocation scheme:

- [Full] points by completing all the objectives **within 60 minutes** from the start of Mission 2 (leaving 10 more minutes to wrap up other tasks), or if fails,
- [80%] of total points by completing all the objectives within the time limit, or if fails,
- [10%] of total points reduction for each failed attempt in constructing the secure key.

Step by step walkthrough:

1. Alice runs `send_key.py` and Bob runs `recv_key.py`. Note that Bob needs to run his program first. After running the programs, Alice will obtain the unsifted key (16 bits) and basis choices (16 bits), while Bob will obtain the measurement result (16 bits) and basis choices (16 bits). For Bob, remember to set the value in `threshold.txt` to be the mean of the intensity matrix.
2. Alice and Bob fills in the keysift form according to the procedures. Supposedly, they are only allowed to pass the `public channel` paper back and forth. However, in the trials Alice and Bob can work together and help each other. They might also benefit with the program `keysift_hint.py`.
3. Alice and Bob attempt the second objectives, i.e. without any other communication channel except the `public channel` paper.