What actually happened here?

Qcamp 2019, Experimental Session 20/06/2019

1 Deception

> Half of you knew this from the start...
> Some of you probably knew it deep in your heart...
> Is this some sort of a joke? Am I being hacked?

The answer is no, this is not a joke and yes, half of the you are actively hacking the other half.

We have learned previously that Quantum Key Distribution (QKD) promises unconditional security. This is true only if all the assumptions are met. In the QKD workshop, there was one crucial assumption that we neglected, even though we followed the protocol to the letter, and this allows the eavesdroppers to hack into the system and obtain the secret message.

1.1 The Crux of The Attack

The security of BB84 relies on the fact that a single quantum bit (qubit) cannot be copied. When multiple qubits of the same state are distributed, security is compromised since a fraction of the qubits can be intercepted and measured by an adversary. To illustrate this concept, we use macroscopic laser beams instead of single photons, creating a security loophole.

2 Summary of The Session

2.1 Alice and Bob

Mission 1 focuses on establishing the classical communication channel using IR sender and receiver circuits. Mission 2 focuses on establishing the quantum channel using polarised ~~single~~ photons. Mission 3 focuses on combining both the classical and quantum channels to send the ~~secret~~ message.

2.2 Eves

There are actually 2 teams: Eve-Classical (a.k.a. Alice 2) and Eve-Quantum (a.k.a. Bob 2).

Eve-Classical focuses on making the equipment to listen to the classical channel between Alice and Bob. In mission 1, they establish two way classical communication channel between themselves (just like how Alice and Bob did it). In mission 2, they start listening to the conversation of Alice and Bob. In mission 3, they collaborate with Eve-Quantum to crack the ~~secret~~ message.

Eve-Quantum focuses on analysing the polarisation of the photons from the beam splitter. In mission 1, they establish the quantum channel between themselves (just like how Alice and Bob did it). In mission 2, they start to analyse a fraction of photons from Alice. In mission 3, they collaborate with Eve-Classical to crack the ~~secret~~ message.

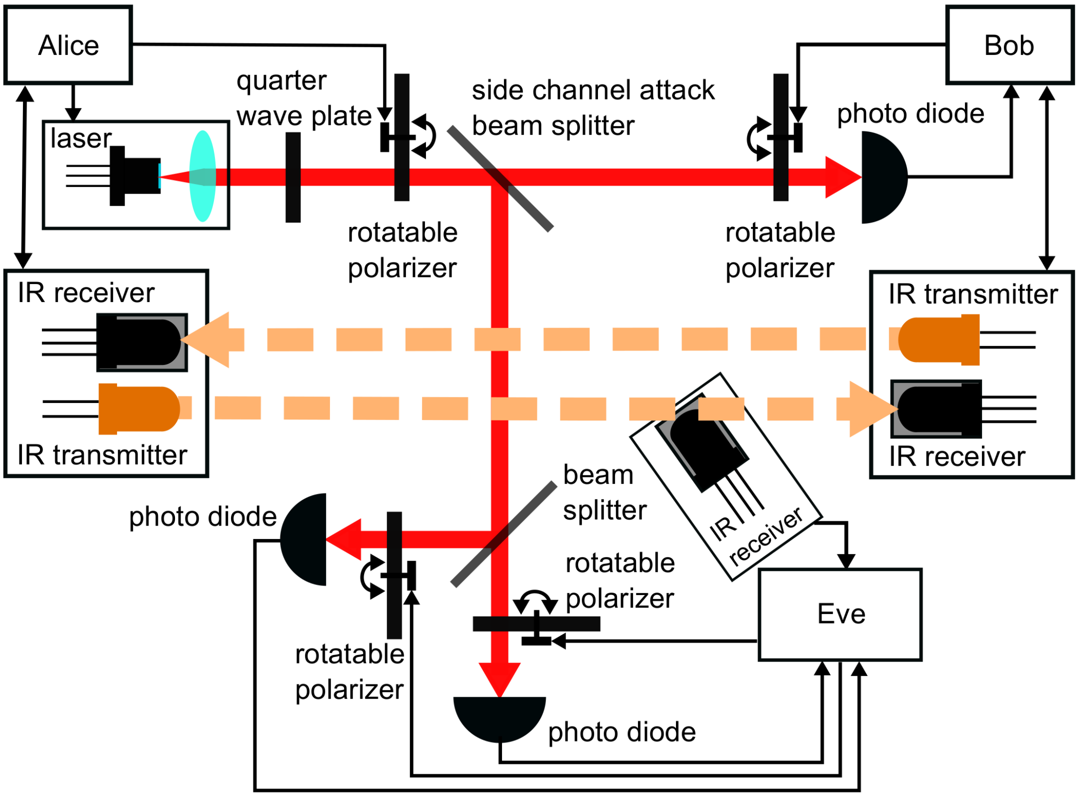

Figure 1: ***BB84 setup:*** Alice encodes a string of bits using different polarization choices set by her polarizer (quantum channel). A quarter-wave plate transforms the linearly polarized light from the laser diode into circular polarization such that the output from Alice's polarizer has equal intensity for all linear polarization choices. Using infrared transceivers (classical channel), Alice and Bob communicate the matching polarization choices and the encrypted secret message. ***Side-channel attack:*** Using a beam splitter on the quantum channel, she intercepts and measures some of Alice's photons in two different bases simultaneously. As Eve's bases choice are *a priori* not aligned to Alice and Bob's, she may not be able to distinguish between polarization states optimally. However, by measuring in more than one bases choice simultaneously, she improves her ability to identify distinct polarization states even in the presence of laser intensity noise. Eve also intercepts the matching polarization choices and the encrypted secret message from the classical channel.

3 Frequently Asked Questions

3.1 Regarding the workshop

I want to understand the setup more. How do I find the reference material?

To keep with the spirit of open source, we put up all the codes, missions, handouts, and technical documents on GitHub. You can access the link at https://github.com/HelpMeFinishPhD/Qcamp2019. For a more complete technical description, you might want to look at the file "Technical_Documents.pdf". It contains the raw, almost unedited ramblings of all the nitty gritty details of the setup. Please do not share the link with your junior friends, particularly those who want to join the camp the next year. Don't spoil them the fun!

I spent a lot of time doing the handout. How do I check my answer?

We will upload our solutions to the GitHub. You can also find other handouts (each group gets different set of handouts). If there is any discrepancy, you can email us (find it at GitHub).

I want to run some parts of the workshop in my home/school. Can I ask for your help?

If you want to do this in your home, you can always email us to discuss about the technicalities of the setup. Make sure that you also understand the safety precautions, particularly regarding the lasers and the electrical components. You might want to brush up on the Arduino/python skills.

If you want to do this in your school, this is beyond the scope of the FAQ. Please contact us directly.

What are the concepts needed to run this? How do I learn them?

For the theoretical aspects, you would probably have learnt enough from the camp. For the experiment itself, you would need to have basic understanding of electronics, programming and optics. To get started, there are tons of Coursera, YouTube, Udemy, and whatnot online courses that you can take. You just need to have a curious mind and a burning passion (brought to you by NUS Physics).

Is it possible to buy this kit directly from you?

This is beyond the scope of the FAQ. Please contact us directly.

What happens to all those points? Do we get prizes?

The points are just red herrings. We hope that you enjoyed the session, and at the same time, learn a bit about building electronics, get some experience in running an experiment, and understand a bit more about some (quantum) physics along the way.

Why is there no lecture notes?

We want to bring back the popularity of Writing Your Own Notes™.

3.2 Regarding the classical channel

Why do we use infrared?

In principle we can use the whole electromagnetic spectrum. However, infrared is nice because we can't see it with our naked eye, but we can still see it with the infrared card or cheap phone cameras.

Why do we use transistor?

Transistor is just like a switch. If you turn it on (via the base), the current will flow on the other two terminals (emitter and collector). The IR LED might require quite a lot of current, so we probably can't power it directly using the Arduino digital output pin.

Can we send some IR light and disrupt the IR detector?

Yes, if they happen to have similar wavelength and modulation frequency.

Why does the data transfer happen so slow?

It depends on how fast you can pulse the IR signals and detect the pulses. Moreover, the computer also needs some time to talk to the Arduino and so on. In principle, we can optimise this, but we are lazy.

I noticed that during the session, the projector suddenly turns on/off. What happened?

Wow you noticed! Team Charlie was trying to hack the projector, so perhaps you can ask them?

I noticed that the message comes in chunks of 4 characters. Why?

The messages are encoded with the NEC protocol which has a capacity of 32 bits (4 bytes) per packet. We send these packets one after another until the entire message is sent.

3.3 Regarding the quantum channel

Why don't we use single photons?

We have a limited budget for the workshop. Right now, single photon sources and detectors are not generally available and pretty expensive ($\sim$20k SGD at least). There are also technicalities and problems associated with operating single photon sources. If you are interested, you can contact our industry colleagues at https://s-fifteen.com/collections/all.

Also, one can hack this setup. We guess in that way, it is more fun?

Why are motors turning so slowly?

The motor operates in steps (look up "stepper motor"). The ones that we use are pretty cheap, so there is a maximum limit on the stepping speed.

Why is there a quarter wave plate in the setup?

This is to "randomise" the polarisation of the laser before going through a polariser, such that the different polarisation states have similar intensity level.

What are the other alternatives to the quarter wave plate?

That is an excellent idea! We can replace the quarter wave plate and the polarizer with a half wave plate. However, we think that polarisers are easier to understand than the half wave plates.

How does the calibration work?

The calibration aligns the polarisation axis between Alice and Bob. For more information, look up the "Polarisation Basis" handout and page 13-15 in the technical document.

How do you generate the random numbers?

We are using the "Entropy" library which utilised timing uncertainty as a source of randomness. For more information, refer to Section 1.1 in the "Randomness" handout.

Are there any entanglement, interference, or superposition in this setup?

It depends on how you see it. You don't need any of those to explain the main idea of this particular protocol, unlike say, the E91 protocol where entanglement is the key.

3.4 Regarding both channels

How did you automate the key generation procedure?

We use the IR channel to communicate the basis choices, and repeat the process a few times (4-5 times) until we obtain 32 bits of the sifted key.

Why only 32 bits?

This is because the key generation process is so slow (refer to the "Our Setup, Bandwidth" handout). If the key is shorter, then it might be too trivial to hack: you can attempt the challenges in the "The Last Handout" handout. If the key is longer, then most of the time will be spent playing with phones.

How can you encrypt the whole message with only 32 bits?

We cheat a bit here. We first expand the key with a pseudo random number generator (PRNG), i.e. the 32 bit key serves as the seed to run the PRNG. We match the output size of the PRNG to the size of the message and perform the XOR operation for encryption/decryption.

Why do you use PRNG? I thought they are not random enough.

The PRNG is only used to expand the key size. The "randomness" is still determined by the "variability" of the seed, i.e. how many possible combinations of the seed inputs, which is 32 bits. It is also useful to think of this as a blackbox: for every unique 32 bit key that you use, you get a unique encrypted message.

Why does the experiment have a lot of problems and bugs?

Life is never easy. We also wanted to let you all have a taste of experimentalists' life so we did not eliminate all the bugs.

3.5 Regarding the hack

What actually happens here?

You can talk directly to the hackers. But, in short, one team is listening to Alice's message via IR receiver, and another team is analysing the polarisation of Alice's photons.

How do you analyse the polarisation?

From the beamsplitter in between Alice and Bob, we split the light further into two parts, send it through different polarisers (the polarisation axis can be anything, as long as they are sufficiently different, see below), and measure the light intensity afterwards.

Why two polarisers?

Refer to Figure 2. With two different polarisation projections, Alice's photons fall into one of the 4 clusters, making it easier to identify. If we only use 1 projection, the signal is too noisy for us to identify the clusters properly. Try to project those clusters onto photodiode 1, and see that cluster B merges with C, and cluster A merges with D. Note again that those two polarisation axis has to be different, if not then the clusters will only fall on a straight line.

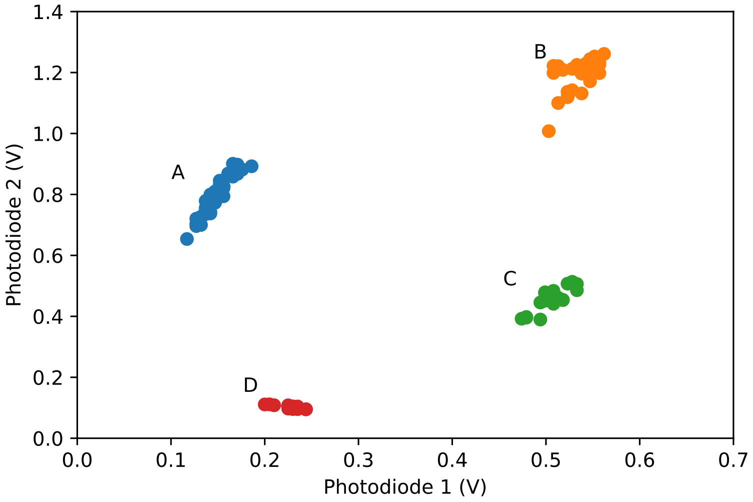

Figure 2: Alice's photons makes four distinct clusters onto two different polarisation projections. Eve still needs to determine which states those are, and luckily there are only 6 possible combinations of the final key.

How does Eve determine which cluster is which polarisation?

There is a bit of trial and error here. There should be around 6 possible different answers. However, when you perform the decryption, only one answer would make sense.

I am not a physicist. How can I trust any QKD device if this stupid hack can happen?

That is a good point! You should not trust anyone based on a blind faith alone. That is why physicist came up with another QKD scheme that is device-independent secure. For more information, stay tune for the lecture on Friday morning about Quantum Hacking.