WACQT Lab course - Linköping

Quantum Key Distribution

Daniel Spegel-Lexne, Joakim Argillander, Guilherme B. Xavier and Alvaro Alarcón,

Quantum communications have revolutionized the field of cryptography, providing the possibility of achieving levels of security never imagined before their appearance. Based on the properties of quantum mechanics, this type of communication has managed to justify its actions in the principles of nature and the universe itself to carry out data protection. This marks a fundamental difference from previous encryption technologies that were based on mathematical constructions or complex algorithms.

One of the protocols used to make effective use of quantum key distribution is the BB84 protocol. Traditionally, single photons are used so that Alice and Bob can en/decode information in one of the photon's degrees of freedom. To do this, Alice and Bob have two bases to en/decode. For a long time, the preferred degree of freedom to encode information was polarization. The bases used to encrypt were rectangular (with the possibility of choosing horizontal or vertical polarization) and diagonal (containing the polarization at +45 or -45). Alice will transmit the encoded state over a channel to Bob. Bob will choose to measure the photon sent out by Alice independently and will decide to use either the rectangular basis or the diagonal basis. If the basis to be measured matches Alice's, Bob will have a 100% chance of successfully decoding Alice's prepared state; otherwise, Bob only has a 50% chance of doing so.

We will define $|H\rangle$ and $|V\rangle$ as horizontal and vertical polarization states respectively. On the other hand, $|45\rangle$ and $|-45\rangle$ represent diagonal and antidiagonal polarizations. In order to perform a projective measurement, we use an optical component called a polarization beam splitter (PBS). A PBS has two inputs (we will only use one for our example) and two outputs. Single-photons will be transmitted (output 1) or reflected (output 2) depending on their initial polarization.

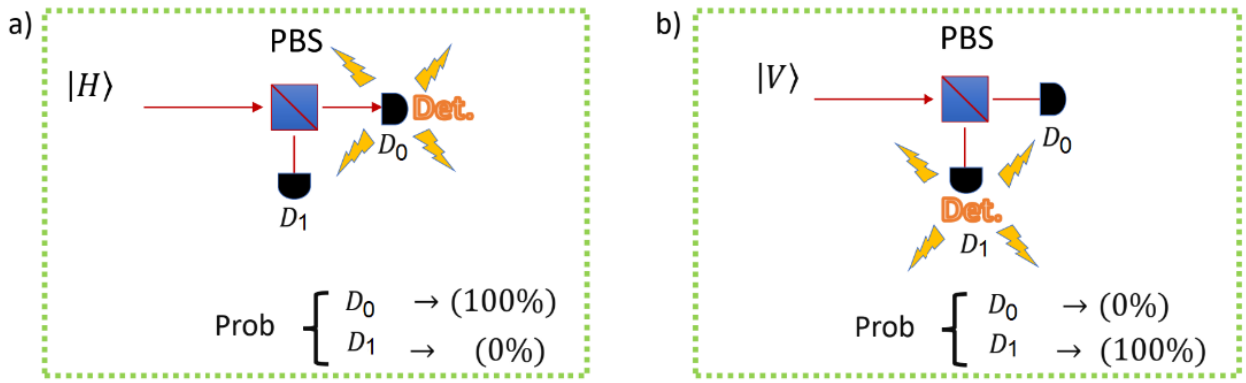

Figure 1: Diagram of a PBS and its operation for different input polarizations.

There is another optical component called half-wave plate (HWP) that allows the rotation of a state of polarization. By applying a rotation of π/2, one can transform from { $|H\rangle$, $|V\rangle$ } to { $|45\rangle$, $|-45\rangle$ } and vice versa. When a photon passes through a PBS, a deterministic or random measurement can be obtained, depending on the input polarization.
In a realistic system, the presence of a spy should always be assumed. We will assume that Eve can always infiltrate the channel and obtain the key.
For this reason, QKD is a great alternative to mitigate these types of problems because the key that Alice and Bob will share is determined by trust in three laws of quantum nature: Inherently random behavior of quantum objects, the quantum measurement process (quantum collapse) and the non-cloning theorem.

In the BB84 protocol using polarized single-photons we usually employ a HWP and a PBS to encrypt and decrypt information. Alice and Bob record the measurement values and the choice of bases during the process. Alice and Bob will exchange the bases they used as public information though a classic channel, but not the bit values (values obtained after measurements). This aspect is important, because this protocol has been designed even when some of the information might be visible to Eve. Once there is mutual knowledge about the choice of the bases, Alice and Bob will discard those measures where their basis choice did not coincide. Theoretically, due to the existence of two measurement bases, and that the measurement process is independent and random, the string will be reduced by approximately half. It is very important to note that once a single-photon has been measured, Alice and Bob now have classical information (bit). After the sifting process, they both have a key. Alice and Bob will randomly choose a small part of this key and share it through a public channel. Then, both compare a random subset of values of their bits. In the ideal case, Alice and Bob will not see any difference in their bits. In a practical scenario, the polarization can fluctuate when a photon is injected into an optical fiber due to birefringence. Therefore, there will be a small threshold of errors that can be characterized in advance.

If the BB84 protocol is running and there is a sudden increase in the number of errors (QBER: quantum bit error rate), there is a possibility that Eve is listening to the channel. The reason lies on the measurement process: If Eve intercepts the information Alice sends, Eve must irrevocably measure the photon. Eve will only have 50 % of chance of sending the same prepared state to Bob. Once Bob reads the photon sent by Eve, the chances of hitting the state of Alice are even lower. After Alice and Bob exchange their bases, they will see that the QBER will have increased. Upon realizing this situation, Alice and Bob can assume Eve's presence and wait until the channel is secured again. Just by taking one action, Eve is part of the complete system, and her action will be revealed.

1) Instruments and equipment presentation

In this lab we will experimentally simulate the behavior of a quantum system to perform a QKD session. It is very important to understand some significant differences of this system with respect to a real implementation of QKD, for example, we will use a light source that sends either pulsed or continuous light, but we are not sending single photons. Despite that, we can understand that the generation of a pulse in Alice and the detection of it in Bob simulates a creation and detection of a single-photon. We will also assume that Eve has the same technology as Alice and Bob. However, one would assume that Eve will always have more technology and resources if she wishes to intercept messages. It is at this point where QKD becomes very relevant when it comes to positioning itself as one of the best alternatives when it comes to providing security, since its performance depends on the principles of nature and not on technological capabilities or mathematical constructs. With that said, we can now move on to the components needed to carry out our lab activity.

2) Implementing an optic setup.

In this first activity, we will move to an experimental implementation from scratch. The main idea of this laboratory is to understand that behind a QKD system there are various experimental complexities that, in one way or another, will condition the feasibility and limitations of our scheme.
The lab activity ends when you can set up the experimental setup that simulates Alice and Bob, do preliminary tests and a short interrogation from the lab assistant.

2.1) Light Source: A key element for Alice

Calibrating Alice will be a critical step in later steps, so we must be careful to properly generate the polarized states.
Once every component on Alice is identified, you will see that there is a red button that activates the continuous laser and the pulsed laser. ***Experimentally test how to go from pulsed mode to continuous mode.*** Once this step is clear, using the continuous laser, try rotating the half wave plate in different directions. With the help of a solid surface, observe the generated spot and define if there are significant changes in the beam. ***This activity is finished once you can say for sure whether Alice's output changes when the half-wave plate is rotated, and you can justify your response.*** We attach a schematic diagram of Alice:

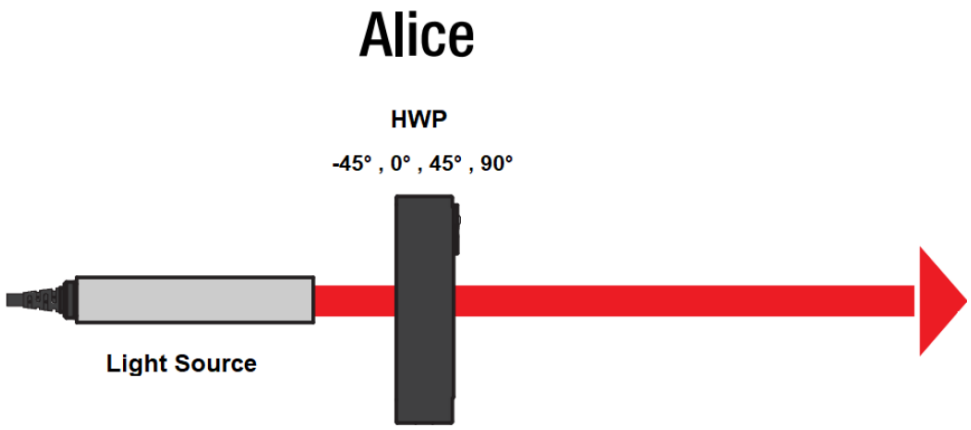

Figure 2: Alice

2.2) First alignment: Alice and Bob

Now it's time for Alice to prepare some messages to Bob. To do this, we will activate the continuous laser again and we will observe that this light hits on the two photodetectors installed in Bob. We must physically move the platform until we get the best possible alignment. This will help reduce system losses. Below is an explanatory schematic for Bob.

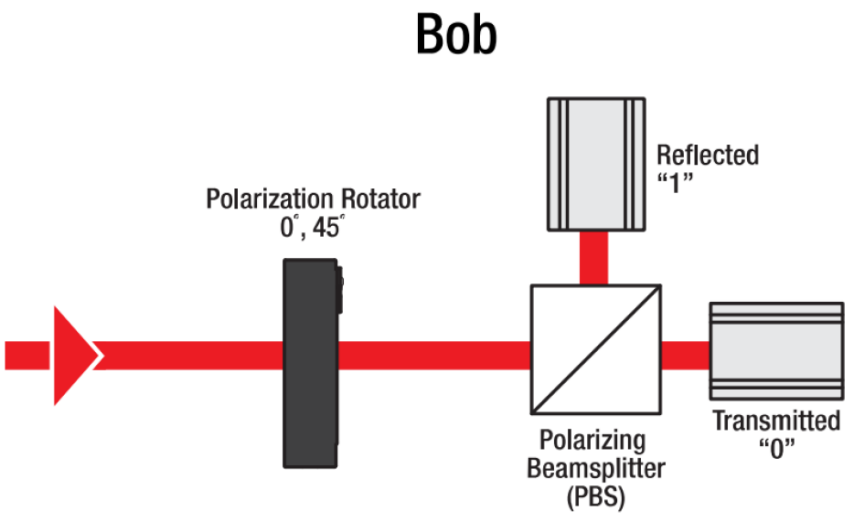

Figure 2: Bob

Once we have proper alignment, place a solid blocker just before the light strikes the photodetectors. ***Move the half wave plate on Alice and observe the behavior of the light beam. Is there a difference when moving the plate?***
If we set the HWP on Alice's side to 0°, and the HWP on Bob's side also to 0°, then we can ensure that the light hitting the PBS located on Bob will be horizontally polarized. We can test this assumption by observing that light has a higher intensity when it is transmitted through the PBS than when it is reflected. In fact, the reflected light must be minimal.
We will now set the HWP at Alice to 90° and keep the HWP on Bob at 0°. Now the incident light must be vertically polarized. The situation that we must observe is the opposite of the previous one, that is, the reflected light must be much more intense than the transmitted one.
Finally we will set the HWP on Alice to 45° and keep the HWP at Bob at 0°. The incident light must be diagonally polarized. The situation that we must observe that the intensity of the reflected and transmitted light is equal.
Now we can move on to the last stage of alignment. For this we will change the laser from continuous to pulsed mode. Now instead of having continuous polarized light we will have polarized pulses coming out of Alice and going to Bob. We will call these pulses "states" from now on. To prepare her states, Alice can choose to encode a pulse of light using 4 polarization states (two bases). To do this, simply select the appropriate angle by adjusting the HWP of Alice's output. Instead, Bob, to configure the measurement base, must resort to adjusting the HWP at its input, which allows selecting the rotation values 0 ° and 45 °, and the PBS before the detectors. In this way, to obtain a deterministic or random result in the detection, we must consider the basis that Alice chose and the measurement basis that Bob chose.
When a pulse is detected on the photodetectors, an LED will activate indicating a successful reading.
One way to align the system is to prepare all the possible states that Alice could encode and project them onto the two bases that Bob can select. Alice must prepare the two rectangular states and the two diagonal states. For this activity, we must check that the light source is working in pulsed mode. Bob will read those states by either measuring with the rectangular base or the diagonal base. When the result is deterministic, that is, with 100% probability of correctly measuring the state generated by Alice, otherwise the measurement result will be random (50% chance of correctly decoding the state encoded by Alice).
In order to align the system, you can fill in the following table. **For this activity Bob must be in "test mode" and Alice must have her light source in "pulsed mode".** (bit "0" is when a pulse of light hits the "0 detector" located in the path of the PBS transmitted light. On the other

hand, a "1" bit will be recorded when a light pulse hits the detector located in the reflected light path of the PBS. "Random" is when both detectors have been hit with light with equal intensity):

Alice (angle HWP)	Bob (Angle HWP)	Bit (0, 1, or random)
-45°	0°	
0°	0°	
45°	0°	
90°	0°	

Alice (angle HWP)	Bob (Angle HWP)	Bit (0, 1, or random)
-45°	45°	
0°	45°	
45°	45°	
90°	45°	

2) QKD without Eve

The time has come to generate our first QKD session. For that we will generate a 40-bit string. Alice's and Bob's half-wave plates are secret, so each entity can generate and detect states independently. One person will be in charge of generating the states in Alice and another will freely decide with which bases to measure in Bob. Each participant must fill in a table with the base that she chose to decrypt/encrypt and the state that she prepared/measured. The bases will not be revealed until the end of the session, that is, after Bob has measured 40 bits of information.

The tables below must be filled out by each group. For this activity Bob must be in "measure mode" and Alice must have her light source in "pulsed mode". (Note that for the rectangular basis, we will use the symbol "+" and for the diagonal basis we will use "x". In addition, we will write a bit "0" or "1" when light is detected at detector 1 or detector 0 respectively.

Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Basis (+ or x)																				
Bit (0 or 1)																				

Alice	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Basis (+ or x)																				
Bit (0 or 1)																				

Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Basis (+ or x)																				
Bit (0 or 1)																				

Bob	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Basis (+ or x)																				
Bit (0 or 1)																				

Once the measurement of the 40 states is finished, Alice and Bob will make public the bases on which they measured. After that, they will discard those measurements where Alice and Bob chose different bases to work with. The remaining values will be the key that both entities will use to encrypt information. Finally, agree between Alice and Bob on some random bits to check that the measurements were correct (50% of the final key is a good number for our activity)

- What is the final length of the key?

- How many errors are there in the final key?

3) Quantum Key Distribution: Eve is in the system

Now we will see how Eve's action is in this communications system. We will place Eve between Alice and Bob. Eve will try to intercept the communication using the following strategy: She will intercept Alice's message using a detection system with the same hardware as Bob's. She will record the base on which she measured and proceed to resend the measured information. Eve in her output also has another system like Alice's, therefore, if she measures a state at detector 0, then she should adjust her HWP to maximize the chances that Bob measures the same. We will also assume that Alice and Bob are initially unaware of Eve's existence. When Alice and Bob end the session, and as in the previous exercise, they will share the key through a public channel. That will be the perfect time for Eve to crack the key and make our system totally vulnerable. Could it be that the principles of nature can help us?

Let's refill the previous tables, only now we will also consider Eve. After finishing the session, discard again those bases where Alice and Bob used different bases (Of course, Eve will also have this information). Note what happened to the error rate. Discuss with the person in charge of supervising the laboratory the results obtained.

Alice	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Basis (+ or x)																				
Bit (0 or 1)																				

Alice	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Basis (+ or x)																				
Bit (0 or 1)																				

Eve	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Basis (+ or x)																				
Bit (0 or 1)																				

Eve	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Basis (+ or x)																				
Bit (0 or 1)																				

Bob	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Basis (+ or x)																				
Bit (0 or 1)																				

Bob	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Basis (+ or x)																				
Bit (0 or 1)																				