Practical session

Implementing the BB84 protocol

QCRYPT

Duration: 4 hours

Introduction

Goal of this practical work

The goal of this practical sessions is three-fold:

- deepen the understanding of the BB84 protocol from a theoretical point of view;
- deepen the understanding of the polarization-encoding for BB84;
- implement an analogical setup using classical light and free space optics.

The practical session is separated into two parts: the theoretical part (duration 2 hours) starting on page 3 and the practical part (duration 2 hours), starting on page 6. The order of the two parts does not matter. One group will start with the theoretical work and the other with the practical work.

Laser safety

This practical session involves working with lasers. Improper use of lasers can lead to eye and skin injuries.

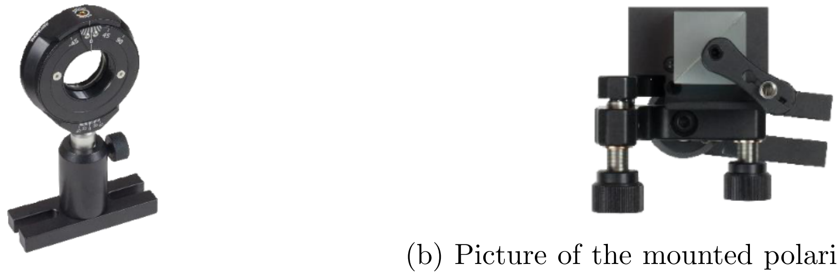
The lasers used in this practical session are of class 2 meaning that they fulfill the following conditions: the emitted light is in the visible domain ($400 - 700$ nm) which in our case the wavelength is 635 nm and the emitted power is less than 1 mW (in our case, around 0.9 mW).

The lasers of class 2 are considered low risk lasers, as one will be protected by the blink reflex. It should however noted that direct stare into the laser beam has to be avoided at all time. There are no risk of skin burns with class 2 lasers.

Report any eye inconvenience to the teacher in case they appear.

Working with optical components

Optical components are fragile and expensive. Hence, they require extra care during manipulation. The Half-Wave plates and the Polarizing Beam Splitters are particularly fragile.



(a) Picture of the mounted Half-Wave Plate

(b) Picture of the mounted polarization Beam Splitter

Figure 1: Half-Wave Plate and polarization Beam Splitter

> ☞ You should avoid providing shocks to the optical components. **You should also avoid touching the optical part with bare hands, as dust and greasy residues can change the properties of the optics. If you accidentally do so, please contact the teacher**.

If you have to move the bare optical component, please ask the teacher first.

Grading of this practical session

This practical session will account for 20% of your final grade. The grade of this practical session will be partly determined by your experimental work during the session but mostly the lab report that will submit after, according to the following (given as an indication):

- 14 points out of 40 on the answers of the theoretical part;
- 14 points out of 40 on the answers of the practical part;
- 6 points out of 40 on the overall report;
- 6 points out of 40 on the overall performance during the practical session.

Instructions for the lab report

A lab report **per group** should be handed in before

November, 16th 23h59 (Paris Time).

The file has to be deposited on Moodle in the according section. Any student from the group can hand in the report. Once the report has been submitted by one student of the group, it will be considered to be submitted by the whole group. After submission, the report can be modified up to the deadline. If the report is handed in after the deadline, penalties will be applied.

The report should contain the following information:

- First and last name of each member of the group;
- Student number of each member of the group;
- Group number for the practical session.

and the following content:

- Start with a general introduction of QKD, why it is needed and introduce the general context;
- Explain how and why the polarization of single photons can be used as qubit;
- Answer question by question the theoretical part;
- Answer question by question the practical part;
- Open conclusion on polarization encoding BB84.

The format of the report is free as long as you upload it as a single pdf file.

PART 1

Theoretical part (2h)

Components are described in Appendix A.

1.1. Encoder

Question 1.1. *Determine the angle* θ_0*,* θ_1*,* θ_+ *and* θ_- *such that* $\mathrm{HWP}(\theta_0)\,|0\rangle = |0\rangle$, $\mathrm{HWP}(\theta_1)\,|0\rangle = |1\rangle$, $\mathrm{HWP}(\theta_+)\,|0\rangle = |+\rangle$, $\mathrm{HWP}(\theta_-)\,|0\rangle = |-\rangle$. *Explain how the Half-Wave Plate can be used as a BB84 encoder for Alice.*

We denote $\Theta_A = \{\theta_0, \theta_1, \theta_+, \theta_-\}$.

Question 1.2. *Show that, if you consider the polarization state as vectors, the effect of the rotated Half-Wave Plate with an angle* θ *on the horizontal polarization state* $|H\rangle$ *can be seen as a rotation in the vector plane with an angle* ϕ*. What is the relation between* θ *and* ϕ*. Give the values of* ϕ_0, ϕ_1, ϕ_+ *and* ϕ_-*.*

We denote $\Phi_A = \{\phi_0, \phi_1, \phi_+, \phi_-\}$ and these values will actually be marked physically on the optical elements.

1.2. Decoder

We now consider the measurement station as shown below:

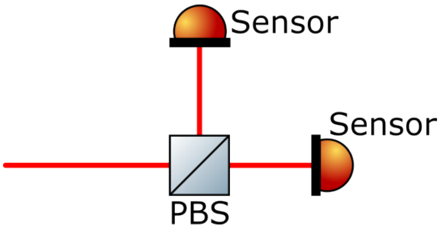


Figure 2: Proposal for a measurement station

Question 1.3. *Show that the measurement station performs a measurement in the* $\{|0\rangle, |1\rangle\}$ *basis (HV).*

Question 1.4. *Show that the measurement station can perform a measurement in the* $\{|+\rangle, |-\rangle\}$ *basis (DA) by adding a Half-Wave Plate of angle* θ_H *and give the value of* θ_H*. Explain how the combination of the Half-Wave Plate and the measurement station provide a good measurement setup for Bob.*

We denote $\Theta_B = \{0, \theta_H\}$. Similar to previously, the polarization angle ϕ_H can also be related to θ_H and we denote $\Phi_B = \{0, \Phi_H\}$ the set of actual markings on the Half-Wave Plates.

1.3. BB84 setup

Let $\theta_A, \theta_B \in \mathbb{R}$. Under the assumption of a perfect (*i.e.* lossless and noiseless) channel, the qubit before the measurement station is given by

$$|\psi\rangle = \mathrm{HWP}(\theta_B) \cdot \mathbb{1} \cdot \mathrm{HWP}(\theta_A) |0\rangle \tag{1}$$

Question 1.5. *Compute* $\mathbb{P}_0(\theta_A, \theta_B) = |\langle 0|\psi\rangle|^2$ *in function of* θ_A *and* θ_B*.*

Question 1.6. *By considering* $\mathbb{P}_1(\theta_A, \theta_B) = 1 - \mathbb{P}_0(\theta_A, \theta_B)$*, compute the values of* $\mathbb{P}_0(\theta_A, \theta_B)$ *and* $\mathbb{P}_1(\theta_A, \theta_B)$ *for* $\theta_A \in \Theta_A$*,* $\theta_B \in \Theta_B$*.*

Question 1.7. *Let's denote* x *the bit chosen by Alice,* $\mathcal{B}_A$ *Alice's basis,* $\mathcal{B}_B$ *Bob's basis and* y *the output bit of Bob. Express the probability* $\mathbb{P}(x = y|\mathcal{B}_A = \mathcal{B}_B)$ *and* $\mathbb{P}(x = y|\mathcal{B}_A \neq \mathcal{B}_B)$ *in terms of* $\mathbb{P}_i(\theta_A, \theta_B)$*. Compute the values* $\mathbb{P}(x = y|\mathcal{B}_A = \mathcal{B}_B)$ *and* $\mathbb{P}(x = y|\mathcal{B}_A \neq \mathcal{B}_B)$*.*

We now consider the setup shown below

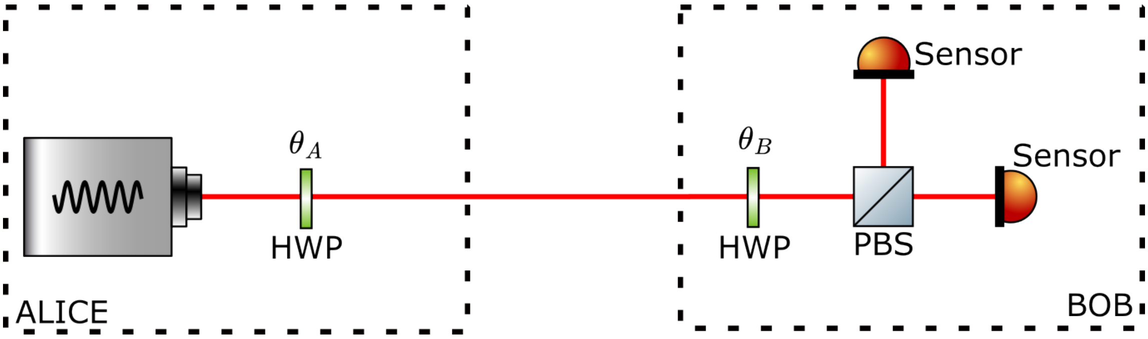


Figure 3: Proposed setup for the BB84 experiment

Question 1.8. *Fill the table 1 by adding the angles of Alice and of Bob and the expected classical outputs.*

Alice basis	Alice bit	Alice Angle	Bob basis	Bob angle	Bob output
HV	0		HV		
HV	1		HV		
DA	0		HV		
DA	1		HV		
HV	0		DA		
HV	1		DA		
DA	0		DA		
DA	1		DA		

Table 1: Encoding and measurement angles

1.4. Adding an eavesdropper

In this section, we analyse how an eavesdropper can be added to the setup, for an intercept-and-resend attack where Eve measures randomly in either the X or Z basis. The proposed scheme for the eavesdropper is below:

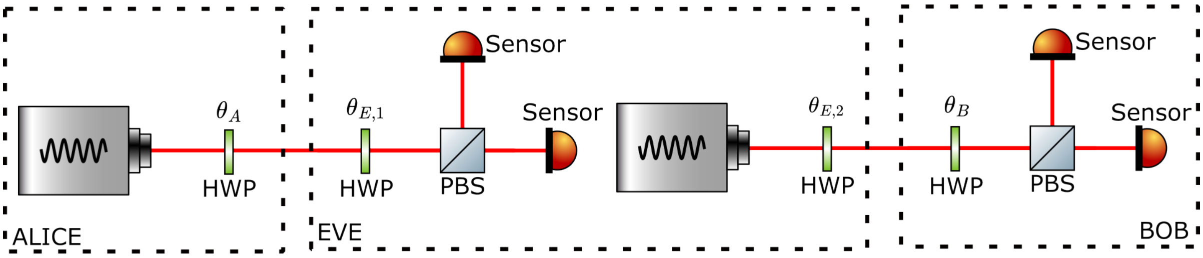


Figure 4: Proposed setup with an eavesdropper

Question 1.9. *What angles should Eve use to perform the intercept and resend attack?*

Suppose that Alice and Bob choose the same basis

Question 1.10. *What is the expected behaviour when Eve chooses the same basis as Alice? What is the expected behaviour when Eve doesn't choose the same basis as Alice.*

Question 1.11. *What is the expected QBER if Eve performs the attack at each round?*

Question 1.12. *What is the formula for the key rate of the protocol in that scenario. What is the value of the key rate with the value of the QBER found at the previous question ?*

1.5. Classical analogy

Instead of using qubits in this practical work, we will perform a classical analog experiment. The light emitted by the source will be classical pulse of linearly polarised light. The detectors are classical power meters. The functioning of the components is described in appendix A.

Question 1.13. *Explain what allows, in the functioning of the components to get a classical analogy of a BB84 setup. Describe what are the limits of this analogy.*

PART 2

Practical part (2h)

At some point during this practical work, you have to choose randomly bits and basis. To do so, you should use a random generator and not generate them “from your head”.

2.1. Preparation

The laser emits a linearly polarised light but the actual orientation is not known. However by physically rotating the laser, we change the orientation of the polarization.

Question 2.1. *Propose a setup using the laser and a polarization beam splitter to find the position of the laser such that the laser emits a horizontally polarised light. Do this calibration with the laser 1 (the other laser is already calibrated).*

The action of the Half-Wave plate is defined through a rotation angle. This rotation angle is relative to the Half-Wave plate fast axis, which is not marked. In practice, one has to find this relative 0 with an experiment, and then move the markings on the mount so that the 0 of the wave plate is the same as the 0 of the markings.

Question 2.2. *Propose a setup using the laser, the half-wave plate and a polarizing beam splitter to find the 0 of the Half-Wave plate. Do this calibration with the Half-Wave Plate 1 (the 3 other Half-Wave plates are already calibrated).*

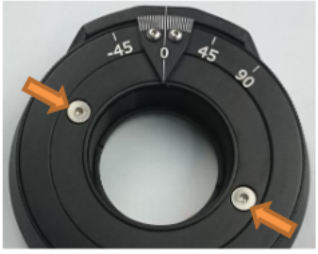


Figure 5: When the 0 is found, loosen the two screws and move the markings so the 0 of the markings aligns with the 0 of the Half-Wave Plate

2.2. Setup

1. Place Alice and Bob breadboards parallel at a distance of approximately 60cm, and realize the setup as indicated in figure 3. The two sensors should be connected to the same sensor unit. The laser should be connected to its laser unit. Both units should be powered on using the power adapters.
2. Set Alice’s laser in continuous mode (press button of the laser’s electronics for 2 seconds).
3. Set Bob’s sensors to adjustment mode (press button). The LED on the side should be **yellow** when in adjustement mode.

4. Set the wave plate of Alice at 0° and the wave plate of Bob at 0°.

   Question 2.3. *What is the expected behaviour? Fire the laser by pressing the button of the laser's electronics once. Which light went on? Why?*

   Question 2.4. *Fill in the table 2. Check that the behaviour is correct in the 8 cases.*

Alice Angle	Bob angle	Which LED lights up	Bit
−45°	0°		
0°	0°		
45°	0°		
90°	0°		
−45°	45°		
0°	45°		
45°	45°		
90°	45°		

Table 2: Encoding and measurement angles

   This test is important as it will conditionate the success of the key exchange.

5. Set back the sensors electronics to measuring mode by pressing the button (LED on the side becomes green). Be sure no to move the setup to avoid any disalignement.

2.3. Key exchange

Question 2.5. *When ready, call the teacher. You will control Bob station, and the teacher will control Alice station. Do 20 pulses exchanges. Note down the basis and the recorded bits for Bob.*

The teacher will give you the used basis for the experiment.

Question 2.6. *Perform sifting, and get the raw key.*

2.4. Adding an eavesdropper

Here we will consider a simple model of an eavesdropper, that performs intercept-and-resend attacks. The setup as described in figure 4 composed of a detection station (similar to Bob) and an emitting station (similar to Alice) is already built. Get it from the teacher.

Question 2.7. *When ready, call the teacher. Separate in two groups. One group will control Alice and the other will control Bob. The teacher will control Eve. Do an exchange of 20 pulses. Note down the basis and bits for Alice, and the basis and recorded bits for Bob.*

Question 2.8. *Exchange the basis and bit values and compute the QBER.*

2.5. Practical QKD

Now that you have seen how a practical system can work, here a few questions to consider for practical implementations of QKD.

Question 2.9. *Give the definition of the efficiency of an optical component. Show that a component of efficiency T_1 followed by a component of efficiency T_2 can be modeled, in terms of efficiency, as a single component of efficiency T and give the relation between T, T_1 and T_2. Show that the efficiency η of the receiver of Fig. 3 (i.e the probability of detecting a photon) can decomposed as a product of 3 terms. Using the documentation, provide values for two of these terms.*

Question 2.10. *Denoting r_{source} the source repetition rate (i.e. the number of emission per second), T the transmittance of the channel, η the overall efficiency of the detector, and supposing a true single photon in each emitted pulse, give the value of the detection rate (i.e. the number of detection events per second), under the assumption of no dark count.*

Question 2.11. *What does the detection rate of the previous question becomes when the pulse is not true single photon, but weak coherent pulses whose photon number distribution follow a Poissonian distribution of average μ.*

Question 2.12. *Assuming $\eta = T = 0.5$, $\mu = 0.1$, and a maximal detection rate of 1 MHz imposed by the detector (above which the detector saturates), give the maximal source rate r_{source}. How this limit QKD ?*

Question 2.13. *What is the QBER induced by a dark count p_{dark} assuming that double click events are assigned to a random value and assuming that true single photons are sent through the channel of transmittance T and that the detector has overall efficiency η?*

Question 2.14. *The PBS has a finite polarization extinction ratio, meaning that part of horizontally polarized light gets reflected and part of vertically polarized light gets transmitted. What is the QBER induced by such behavior (all of the other QBER sources being removed)? Find the value of the parameter in the documentation, and compute the associated QBER.*

Question 2.15. *Consider a calibration error θ_{err} on the Half-Wave plate of Alice. Assuming no other source of error, what is the QBER induced by this error?*

APPENDIX A

Components

A.1. Half Wave Plate

A Half-Wave plate is a particular example of a wave plate (also called retarder). Wave plates are passive optical devices that alter the state of polarization of the light going through it.

A Half-Wave plate adds a π phase between the two components of the electromagnetic field, which, in practice, is used to shift a linear polarization into another linear polarization.

polarization states can be represented using Jones calculus, representing the polarization in a 2 dimensional complex vector. The horizontal, vertical, diagonal and anti-diagonal polarizations are defined by

$$\begin{aligned} |0\rangle = |H\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle = |V\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ |+\rangle = |D\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ |-\rangle = |A\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned} \tag{2}$$

The effect of the Half-Wave plate rotated by an angle θ is represented by the matrix

$$\mathrm{HWP}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \tag{3}$$

such that the output polarization state is the matrix times the input polarization state.

The rotation angle θ is defined relatively to the plate fast axis, which has to be found experimentally as we will see in the practical part.

The available Half-Wave Plates are from Thorlabs (WPH10E-633) and designed for 633 nm. More information can be found at `https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=7054`.

A.2. polarization Beam Splitter

A beam splitter (BS) is a passive optical element that reflects part of the light and transmits the other part of the light. For instance in a 50:50 beam splitter, 50% of the light is reflected and 50% of the light is transmitted.

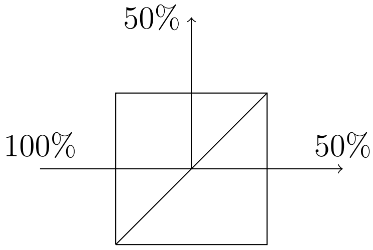


Figure 6: Schema of a 50:50 beam splitter

A polarization beam splitter (PBS) works in a similar way, but instead of splitting the power, the PBS interacts differently on the two polarizations such that the horizontal polarization is transmitted and the vertical polarization is reflected.

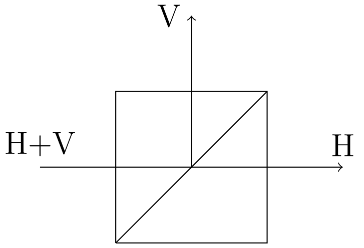


Figure 7: Schema of a polarization beam splitter

The available polarization beam splitters are broadband polarization beam splitters from Thorlabs (reference PBS201). More information can be found at `https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=739`.

A.3. Laser and laser electronics

The lasers are diode modules emitting at around 637 nm with a power slightly below 0.9 mW. The test sheets of both lasers can be requested to the teacher.

The laser is controlled and powered by the laser electronics module. In practice this module enables you to switch between the two modes of the laser:

- Pulse mode: in this mode, the laser will emit a pulse each time the button is pressed. This mode is useful for operating the experiment.
- Continuous wave mode: in this mode the laser is continuously outputting power. This mode is useful for alignment.

To switch from pulse mode to continuous wave mode, hold the red button down for **2 seconds**.

To switch from continuous wave mode to pulse mode, press the red button once.

The laser electronics unit has a green LED on the side indicating that the laser is ready to be used.

A.4. Sensor and sensor electronics

The sensors are regular photodiodes, and each sensor has a blue LED on top. The measurement station will use two sensors that will be connected to the sensors electronics.

The sensors electronics have two modes: measuring mode and adjustment mode. The behaviour of the two modes is described in the following table:

	Most light on sensor 1	Most light on sensor 2	Equal light on both sensors
Measurement mode	Sensor 1 lights up	Sensor 2 lights up	Sensor 1 **OR** 2 randomly lights up
Adjustment mode	Sensor 1 lights up	Sensor 2 lights up	Sensor 1 **AND** 2 light up

Table 3: Difference between measurement and adjustment mode.

It is possible to go from one mode to the other by pressing the green button once. The light on the side is **green** for measurement mode and **yellow** for adjustment mode.

(a) Laser electronics

(b) Sensors electronics

Figure 8: Laser and sensors electronics