

the BIG BELL TEST

Educational Material

www.thebigbelltest.org

@TheBellsters

ICFO^R

The Institute
of Photonic
Sciences

A member of **BIST** Barcelona Institute of
Science and Technology



Generalitat
de Catalunya



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Fundació Privada
CELLEX

Fundació Privada
MIR-PUIG

Fundació
Catalunya
La Pedrera



EXCELENCIA
SEVERO
OCHOA
2016 - 2019



AXA
Research Fund
Through Research, Protection

 **ICREA**



Index

Topic 1 **The BIG Bell Test videogame at the classroom: Randomness and Statistics**

Topic 2 **Quantum Physics: First Concepts**

Topic 3 **The Problem of Sharing Secure Keys**

Topic 4 **Secure Communications through Quantum Physics**

Topic 5 **Polarization and Superposition**

Additional Material

Printed material

General Dossier: <https://cloud.icfo.es/owncloud/index.php/s/hDZRUnNryTQZcJb>

Audiovisual material

Instructions for the videogame: <https://vimeo.com/user57186692>

Promotional video: <https://vimeo.com/184480786>

The BIG Bell Test videogame in the classroom

Basic concepts of statistics: media, statistical distribution, dispersion measures.

Basic Excel functions: filters and graphics.

(Optional introductory material: Randomness and probability)

Randomness is a fundamental element in quantum physics.

In this unit we recommend the excellent material created by Joan Jareño on randomness and probability, in a blog post specifically dedicated to Big Bell Test, which can be found here (it includes English translation button):

<http://calaix2.blogspot.com.es/2016/10/latzar-te-patrons.html>

Activity: Statistics with the BIG Test Bell in the classroom (minimum time: 20 minutes)

The **BIG Bell Test** videogame is the portal to contribute to the experiments of November 30.

You can play at any time, but only on November 30 you will be contributing to the experiment in real time.

On November 30, your students can contribute as many times as they want, from **smartphones**, tablets or computers. No registration is required, but we recommend you to register, for the reasons below.

You can contribute to both of the platform versions: the Quick Bell Test or the BIG Bell Quest, both in www.thebigbelltest.org/contribute.

The BIG Bell Quest is the gamified version, and it allows us to create the classroom activity explained here.

1. Go to www.thebigbelltest.org/quest
2. Register (you may choose to enter as a guest, but then you will lose the data of each mission, plus, you will not have an identifiable user name). **It is not necessary, but recommended, to enter your e-mail.** You can use it to recover a forgotten password. Also, we will use it to send you information about your contribution on November 30.
3. **Create an Event.** In your user profile, locate the "Event" box and choose a meaningful name for it. Your name, or your class followed by the name of your school, for example.
4. Tell your students to register in the game. Give them the name of the event **only when they're at the classroom** with you and you are ready to carry out the activity. Remember they can play using computers, tablets, or smartphones.

Introducing The BIG Bell Test in the classroom

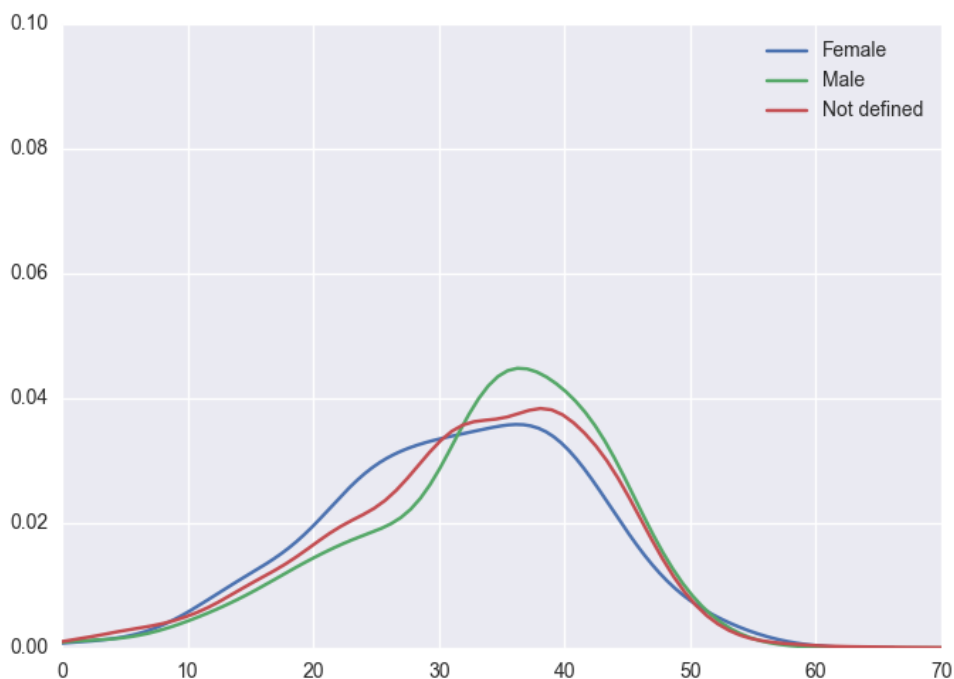
5. Once all the students are registered and enrolled in the event, **it's time to start the game**. They can either play for some minutes, or complete one or two missions. That depends on the time you want to spend on this part.

6. To see the results, go to www.thebigbelltest.org/radarevent Enter the name of your event on the box. You will see the ranking.

7. You can **download the ranking as an Excel file**, and get a plot of the distribution to discuss with your students. How is it shaped? Is it a gaussian? Does it have several peaks? Is it a scattered distribution? You can use it to work on the concepts of **average** and several **dispersion** measures. Does the shape change when you play several times?

8. The students can download the file too, and work on them trying to search for interesting correlations. Is there a difference between the **unpredictability** scores of girls and boys? Do these differences keep through other classes of the school? Do people playing an instrument have higher scores? Do people tend to improve when they play several times? Ask your students to think about other interesting questions.

This is what we got when we plotted female vs male contributions in a recent Bellster competition. Do you obtain something similar?



Quantum Physics

In these series of activities, your students will learn that:

1. in quantum physics, things do not behave as we are **used to observe**.
2. the scientific community has devoted a lot of efforts to the **interpretation** of the surprising predictions of quantum physics
3. the paradoxes of quantum physics can be used for the creation of **new technologies** with capabilities beyond the limits of classical technologies.
4. **their generation will have an unprecedented** understanding of quantum physics, and for sure **they** will be an active part of a society that will have to take on the new quantum paradigm.
5. what is the **BIG Bell Test**, what the experiments are about, and why is important that we contribute.

TOPIC 2: FIRST CONCEPTS

Activity 1 (Homework for home + classroom discussions)

One possible way of starting with this topic is to have students do the following homework assignment: Go to the internet, search for the word "quantum" and see the type of results they get, and ask them to find an **post**, a specific one that calls their attention.

The assignment is to have them come back the next day to school and explain to the class what they have found and why they chose that specific **post**. It must be brief. They are not asked to understand what they have read, but explain why it has surprised them, or what they have not understood.

It might be that some may speak about the strange properties of quantum physics, others on applications such as quantum computers, or cryptography, and others even more bizarre things like quantum meditation, quantum healing, and similar pseudoscience issues.

This first assignment will allow us to:

- Introduce quantum physics as a scientific theory that explains the laws that the smaller objects, such as atoms, electrons, photons, etc., **obey**, which has an extraordinary explanatory and predictive power but, on the other hand, it is extremely counterintuitive and impossible to reconcile with our way of understanding the world.
- Despite being **counterintuitive**, the properties of quantum particles help create and generate new technologies with capabilities that conventional technologies aren't capable of reaching (extremely fast computers, information transactions 100% secure ...)
- Raise awareness that because quantum physics is so difficult and hard to include it in our usual way of understanding the world and, therefore, defies our common sense, many people take this opportunity to

Introducing The BIG Bell Test in the classroom

make up all sorts of "weird connections" as quantum consciousness, quantum splitting, and even quantum healing. It is important that society begins to understand quantum physics, what it means and what it implies, to avoid falling into these kind of deceptions and confusions. Even more, it may be possible that society might have much to say about the new quantum technologies.

Examples of sites on "quantum mysteries":

- <http://www.quantumworldvision.com/scio/> whatever "Scientific Consciousness" may mean, there is no scientific research group that has been able to demonstrate that consciousness is related to quantum physics.
- <http://www.quantumenergywellness.com/> the term "quantum energy" makes no sense at all, and is not used by the scientific community.
- <http://medicinacuantica.cl/> This source makes use of the very good videos made by Dr. Quantum to explain the connections between medicine and quantum physics.

You can then make a summarized list of all the quantum technologies that are now being developed or are currently in use (throughout the literature we have selected some). In the units that we have elaborated, we will delve into one of these technologies, quantum cryptography, which will help us set the grounds to explain the more fundamental quantum properties of quantum physics.

TOPIC 3: THE PROBLEM OF SHARING SECURE KEYS

(Activities aimed at explaining the concept of cryptography)

Modular arithmetic

Use of alphabets

Let's start with a simple game. We will send secret messages between ourselves.

(In case you are interested, in this link <http://crypto.interactive-maths.com/downloadable-resources.html> you may find more classical cryptography activities)

This game is played in pairs. If there are an odd number of students in the classroom, it is possible to have a group with three members.

Each student has to take a seven-letter word, and you have to encrypt it with the Caesar cipher, that is, replacing each letter of the word with a letter "K" positions (the number K is the key and the member of each team **must** decide which one he/she would like to use) to the right of it in the alphabet.

- Depending on how you want to do it, the key is shared or not. That is, when it is time to decipher the message, the student that is trying to decipher the code can act as normal receptor (knows the number that K represents) or can act as a spy (he has to try many possible K's to find the right one).

Introducing The BIG Bell Test in the classroom

- And depending on the academic level of students, they can use the Cesar wheel <https://inventwithpython.com/cipherwheel/> (very easy), or write the alphabet themselves and count positions, or replace each letter by a number and do **sum modulo 27**.

- What does adding modulo 27 mean? We can give a good explanation with the following example. A good example is the hours that we have in a day. If we want to know what time it is say 30 hours from now, we will have to add modulo 24, because there are only 24 hours in a day.

When a student has been able to encrypt the message, he will pass it to his partner, who, in turn, must pass him his encrypted message. Now they will have to decipher each other's message. If any of the students is able to decipher the message before the other, than he or she can continue to encrypt another word. With this, we prevent students from trying to encrypt words in an easy way (small Ks) or in a hard way (large Ks), because they will not want to spend a lot of time encrypting words and have their companions pass them many encrypted words to decipher.

The student who is capable of deciphering all the words on his/her table wins.

We encourage the teacher to **build in advance a collection of words** and give a few to each student. Even more, to make it easier, some letters of the word can be left with out encryption and stating that these do not have to be encrypted.

Now let's see what happens if the receiver does not know the encryption key, or has lost or forgotten it.

Can he decipher the message? Or **similarly**, could a spy decipher a message without the key?

The teacher can do an exercise on the chalkboard for all the students. The strategy of the spy or the message receiver that does not have the key is to begin testing with $K = 1$, $K = 2$, $K = 3$, ...

To encourage the students to find the answer, the teacher can write on the chalkboard an easy word to decipher without telling the students, for example Alabama with $K = 2$, which would be CNCDCOC. Now, when they are capable of finding one letter (say the A), they have many clues to decipher the rest of the word. If they also have a clue, say for example that it is the name of a **state of the United States**, they have another possible advantage in deciphering the word. Therefore, if the spy is given a context for the word that helps him/her decipher the word, his/her task is much easier.

Now, how can we make it more difficult for the spy? One way to make it very difficult (and indeed impossible to decipher!) is to give each letter a different value of K, instead of having the same K, the same displacement, for all letters.

Let's do a test to decipher one word with a different K for each letter. The students will find it impossible and will see why in no time. This method is called the Vernam encryption.

And now, we can observe:

- The encryption key is not a number, but a sequence of numbers (one for each letter)
- The key is as long as the message!

Introducing The BIG Bell Test in the classroom

- Since each number corresponds to a letter of the alphabet, the encryption key can also be a sequence of letters.
- The alphabet has 27 letters, but it is a bit tedious to do sums **modulo 27**. What if we change to an alphabet with only two letters? What if the "letters" are 0 and 1?

Activity:

- The teacher writes a "message" with zeros and ones (can be a totally invented thing, it can be a word in ASCII code, if you want to explain what it is, but make sure it is something not very long).
- Then the teacher asks each student to invent an encryption key. Each student should invent a random key, with the format that he/she wants.
- Now, the students should add **modulo 2** the key they have invented **to** the message. They now have an encrypted message.
- Once again, adding **modulo 2** is jumping to 0 once you get past the 1. Operations would be as follows: $0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$; $1 + 1 = 0$
- Two students go to the chalkboard. Each one writes his fully encrypted message in a different way. The teacher asks them to add the encryption key to their encrypted message. Both (if they do it well) must obtain the original message.

- An in-depth optional homework assignment:

- What if I test all possible combinations to decipher a message?

As we did in the first part of the assignment, we can test $K = 1$, $K = 2$, until we obtain the message (If we do this, we will obtain all possible messages of that length!)

- What if I use the same key twice in two different messages?

(If we do that, messages can be the key to each other. Therefore this method is called the one time pad)

Conclusions:

- The encryption key is a sequence of zeros and ones that has the same length as the message.
- It is important to state that it should be a random sequence, i.e., which has no meaning, so that a spy cannot relate it to anything.
- The sender and receiver of the message must be sure to have the same encryption key, the same sequence, to encrypt and decipher the message. That is, they must share the key.

Introducing The BIG Bell Test in the classroom

- The sender and receiver of the message must share the key without the spy stealing it!!
- If the sender and receiver of the message share a truly random sequence (the spy has no way of inferring it) and if indeed the spy cannot obtain it using any obscure method (that is intercepting the message without transmitter and receiver becoming aware of this), then this method is 100% secure.

Once we understand that if we are capable of having the sender and receiver of an encrypted message share an encryption key, which means we will have secure communications, we can now continue to Topic 4. It explains how Quantum physics is capable of obtaining secure communications. Any other method is prone to error and the spy can always hack the system if he/she **has** a super computer, is very smart and has the resources to spy through all the possible channels.

TOPIC 4: SECURE COMMUNICATIONS THROUGH QUANTUM PHYSICS

Heisenberg's uncertainty principle

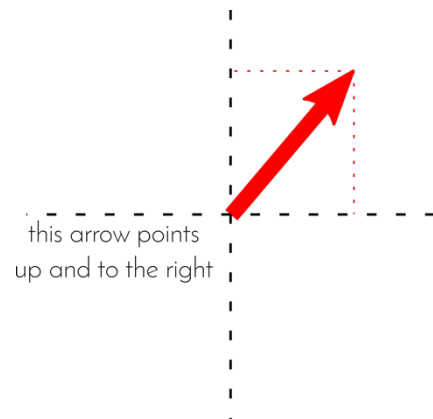
Collapsed state

Randomness

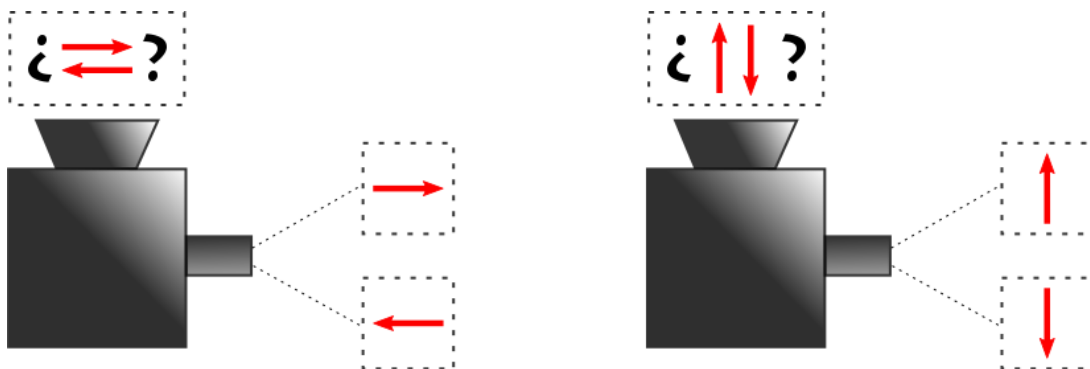
If we want to understand how quantum particles allow us to share this key in a super secure way, we need to understand what is so special about the quantum world if compared to the classical one.

We cannot define all the properties of a quantum object (atom, electron, photon) at the same time.

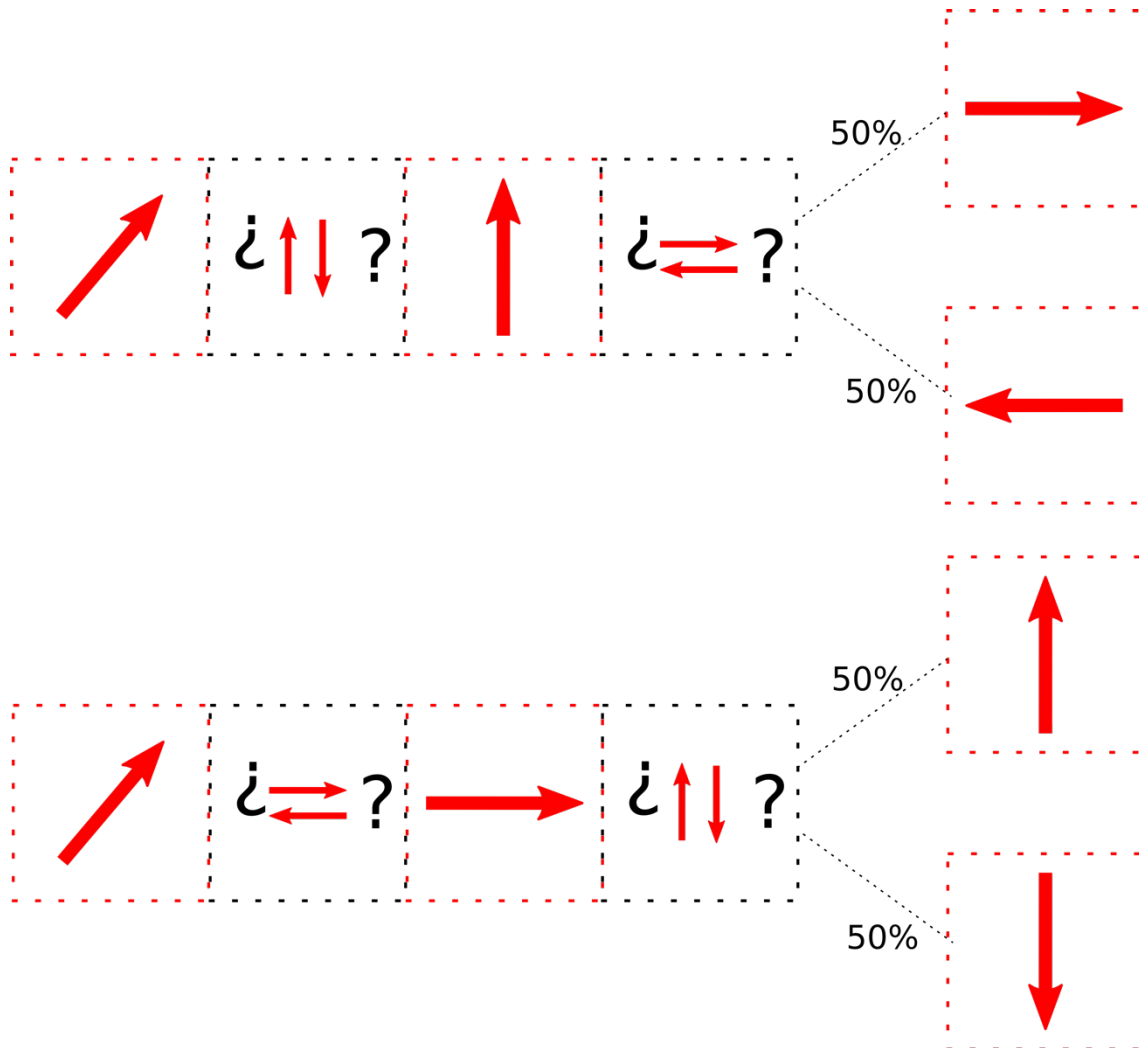
Let's draw an arrow, for example. If you look at this arrow, you can see if it points to the top or to the bottom of the drawing; you can also say if it points to the right or to the left. (You can also say many more things about the arrow that make it different from any other arrow). If a classmate wants to know what does the arrow look like, she can ask you questions like "Does it point up or down?" and then "Does it point to the right or to the left?" and you can answer her consecutively, as if you were playing Guess who? with arrows.



Nevertheless, if we imagine that the arrow with which you are playing is a quantum particle, we face a problem when we ask the second question. We can learn if the arrow points up or down, but then we can't know if it points to the right or to the left. Conversely, we can learn if it points to the right or to the left, but then we can't say anymore if it points up or down. This comes from **Heisenberg's uncertainty principle**, that states that there are incompatible questions, so that we cannot know simultaneously the answers to all of them with good precision. It is as if the arrow were inside a black box impossible to open: we can just inspect that with a device that allows us to ask just one question at a time.



And how does quantum physics prevents us from learning the answer to two incompatible questions? When the particle answers, its state collapses to the answer that it gave. If the particle answers “up” or “down”, it becomes vertical, pointing up or down respectively, so that we have no clue about whether it was pointing right or left before. Note that this implies that the order of the questions can change the final answer, as in the following picture, unlike the game of *Guess Who?* we mentioned before. In the instant when the arrow answers “up”, then it forgets whether it was also pointing right or left and it stays pointing only upwards.



Then what happens if now somebody comes and asks whether it points to the right or to the left? Here it comes another surprise: if a particle is in a definite state in the direction up/down (let's say up, for example) and we ask whether it points right/left, then the particle, forced to answer in these terms, will answer “right” 50% of the times and “left” 50% of the times. This means that **a quantum system is a source of genuine randomness.**

NOTE We can describe the orientation of the arrow, that represents the state of the quantum particle, with the categories either up/down or right/left. Not both at the same time. We can describe the same state in these two bases. We'll stop here for now. We're not going to talk about superposition (we talk about this in the next topic). A state can be up or down or any superposition of these two possibilities.

These properties of quantum physics (incompatible questions, randomness and collapse due to measurement) may seem a disadvantage when you want to describe completely a particle, but we can use them in our favor to **guarantee at 100% the security of cryptography**. We'll explain you how.

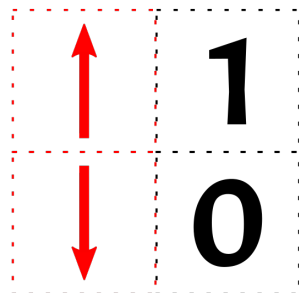
We have already seen in the previous topic that one of the best ways to send secure messages is to share a secret key, a list of randomly chosen zeros and ones (one-time pad key), between the emitter (Alice) and the receiver (Bob).

Now we'll see how Alice and Bob can obtain this list of 0s and 1s from the properties of a quantum particle (we'll use again the quantum arrow in a black box we described above as an example). Alice prepares an arrow for each black box and then sends them to Bob, who asks a question to each box.

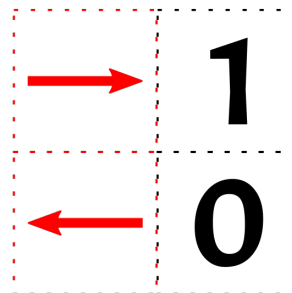
Step 1: Logic behind the code

Alice and Bob agree to associate 0 or 1 to each of the two possible answers to any of the two basic questions.

up/down basis

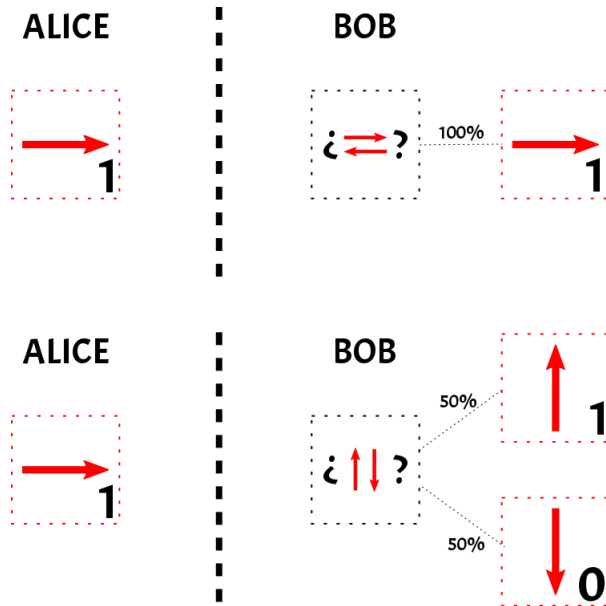


right/left basis

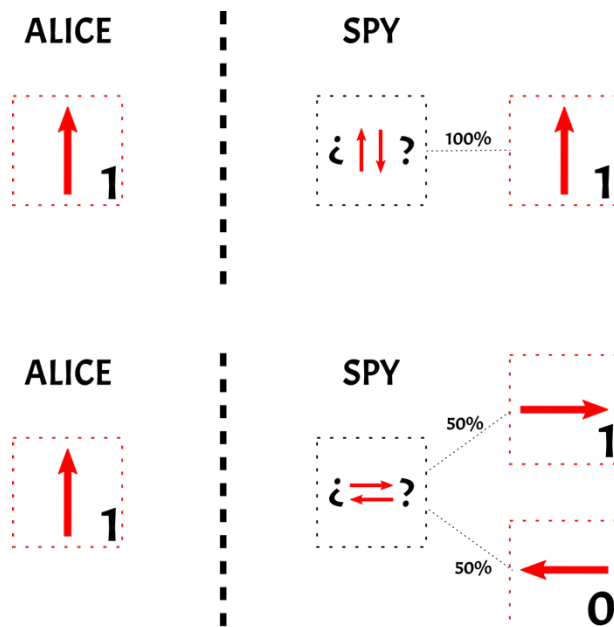


Step 2: Sharing a particle

Alice prepares her first arrow so that it corresponds to a 1 in the right/left basis, for example, and sends it to Bob. **Here's the important point:** Bob does not know which question has to ask the box. Since he does not know it, he can obtain a 0 sometimes!



This may seem a disadvantage, but it is what makes the key secure, because no spy can get the key. For example, if Alice sends her 1 in the up/down basis, and the spy measures it in the right/left basis, she will obtain right (1) 50% of the times and left (0) 50% of the times. If the spy needs the content of ALL the boxes, she needs to be very lucky to guess all of them!



(By the way, choosing what questions to ask the particles is exactly what you (the Bellsters) are going to do on November 30!!!)

Step 3: share the key

We'll describe the so-called BB84 protocol.

Imagine that the message contains 2000 characters. Then we need a key that is a sequence of 2000 random zeros and ones.

Alice chooses at random how to prepare her particles and sends Bob let's say 5000 particles, that – as we said before – are like numbered boxes. 1, 2, 3, ..., 5000.

Bob receives the boxes and observes them, choosing randomly which question he asks (up/down or left/right).

As we saw in step 2, they don't always match. How do they check when their answers match?

Alice calls Bob by phone (it doesn't have to be a secure line!) and they choose some box at random: let's say no. 37, 135, 250, 500, 700, 1234, 3021...

- 1) Alice tells Bob how she prepared the arrows for each of these randomly chosen boxes, in particular
 - a. In which base she prepared the arrow for each box
 - b. Which digit (0 or 1) she put in each box
- 2) Bob selects the boxes for which he and Alice used the same basis and checks if the digit he observes matches what Alice tells him.
- 3) If all the digits match, we can tell that there is no spy. If they don't match, there must be some spy out there who measured the arrows and made them collapse in another basis. (Remember that if there is a spy in the middle, the result of each box changes with a 25% probability) If they infer that there is a spy, they abort the communication. If there is no spy, then they build the key. Alice simply tells Bob which basis she chose for each particle; Bob checks for which boxes their basis choices match and tells her. Alice and Bob communicate their bases publicly, but only them can know the key that is composed by the 0s and 1s associated to the boxes!

And your students may ask:

- 1) How does the information contained in the quantum particles change?
- 2) Quantum physics says that in certain conditions things are not defined before observing them (for example if the arrows points up, it's not defined if it points right or left) and when we observe them, they decide at random which result they show us (the arrow decides randomly if it points right or left after the observation). Isn't it weird? Was it easy to accept this fact in the scientific community?

TOPIC 5: POLARIZATION AND SUPERPOSITION

Polarization

Classical and quantum superposition

Vector addition

ADDITIONAL ACTIVITY: Interference

Classical or Quantum?

The activities that we propose can be found in some websites and are examples of quantum physics experiments that one can do at home. It is actually very difficult to observe quantum properties with homemade materials, because quantum properties of small particles are very delicate and it is very complicated to observe them outside the strict conditions that can be found in a laboratory.

In fact, the **experiments** proposed here can be easily explained with **classical optics** (polarization and interference), which is taught in secondary school. However, it is interesting to consider these experiments from the quantum perspective, as it can lead to surprising conclusions when one does the thought experiment to reflect on how the effects that can be seen in these experiments can be reproduced when we consider that light is composed by individual quantum particles, **photons**.

Furthermore, we must not see this as somewhat distant from the work that physicists do! The thought experiment is a tool that scientists have used for centuries to solve **complicated** questions that were difficult to test experimentally with the technology that was available at that time: famous examples are Galilean's ship, Maxwell's demon, the twin paradox or Schrödinger's cat.

Activity 1. Polarization

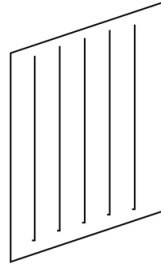
Material: 3 linear polarizers

STEP 1. ONE POLARIZER

The **polarization** of the light is described as a **vector**. The polarizer acts as a filter and projects the polarization of the incident light on the axis of the polarizer.

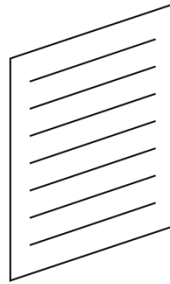
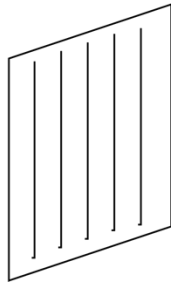


the light from the sun
or from a light bulb
is not polarised

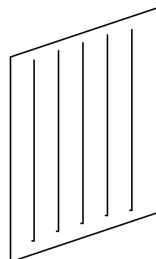
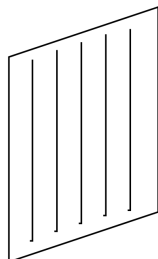
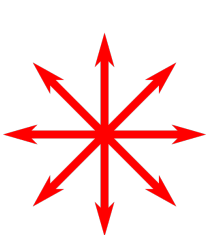


the polariser transmits
only the component
parallel to its axis

STEP 2. TWO POLARIZERS



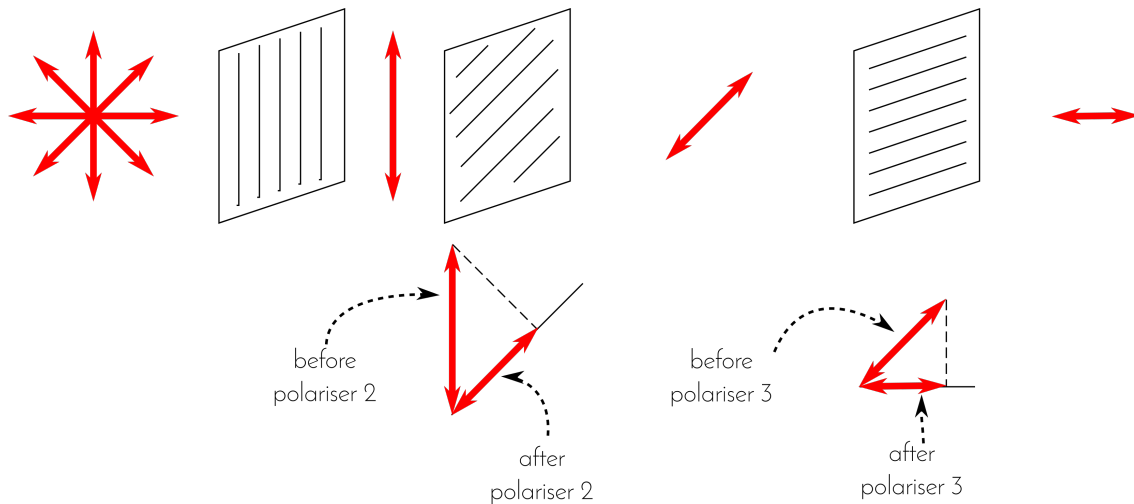
no light passes through
because the light
before the polariser
has no horizontal
component



all light passes through
because the light
polarisation before of
the last polariser
is parallel to its axis

STEP 3: THREE POLARIZERS

Using the two **crossed polarizers** at a 90° angle from step 2, add a third polarizer at an angle of 45° with the horizontal in the middle. What happens?



Light passes through the set of polarizers even though polarizer 1 and 3 are **crossed**!

We can understand this thanks to the properties of vectors: **each polarizer transmits the component parallel to its axis**

THOUGHT EXPERIMENT

Would this also work if we depict light as composed of individual particles called photons?

We could say that each **photon** has its own polarization: for example, non-polarized light contains many photons, each with a different polarization, so that, in average, the light polarization is zero.

However, the more photons polarized in one direction, the longer the vector corresponding to this direction will be, and the resulting light will be polarized.

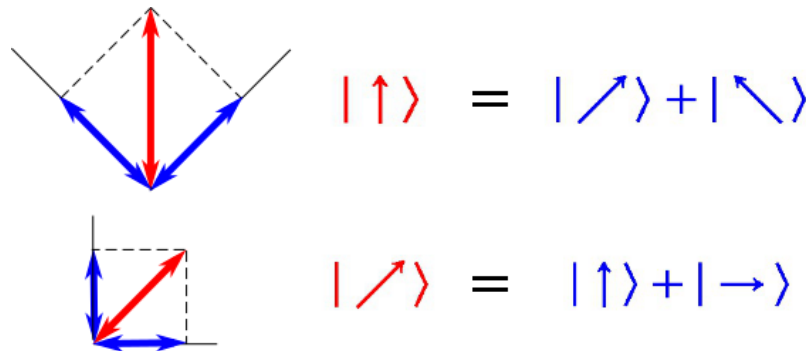
We know that photons do not interact with each other, so that we should get the same result no matter if we send many photons at a time (as in our experiment) or if we just send one at a time.

But how can this result **be** the same if we just send one photon at a time? Our intuition tells us that if the photon can cross the first polarizer, it should not be able to cross the second one, because its polarization is not parallel to the one of the second polarizer.

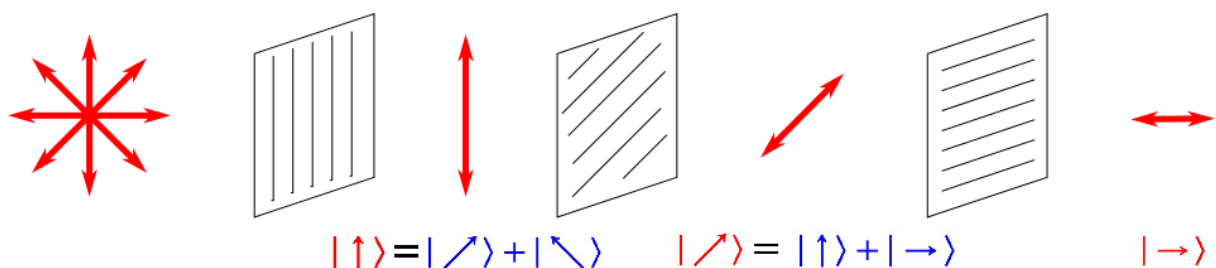
Introducing The BIG Bell Test in the classroom

To explain the experiment of the three polarizers from the quantum point of view, we have then to remember that polarization behaves as a vector. However, because a photon can only have one polarization, we will have to assume that all the possible states (in this case the polarization) of the photon (and generally of the quantum particles) are added as if they were vectors. This is called the **principle of superposition**.

For example, a vertical photon is the superposition of a photon with a polarization at $+45^\circ$ and one at -45° , as shown in the figure below. Similarly, the photon at 45° is the resulting superposition of a vertical photon and a horizontal photon.



In the quantum case, the polarizer has the effect of taking the photon off superposition and make it “collapse” into one of the two states, specifically, into the one that is parallel to the axis of the polarizer.



Note: in topic 4 we also use an arrow to explain the properties of quantum physics, but we describe it differently from polarization. In topic 4, the possible states of the arrow involve the directionality of the arrow (up, down, to the right, to the left), while here we only consider the situation of the arrow (vertical, horizontal, $+45^\circ$, -45°).

To learn more: http://www.informationphilosopher.com/solutions/experiments/dirac_3-polarizers/

Extra Activity: Interference

We can use polarizers to destroy and recreate interference patterns like in the experiment described here:

<https://www.scientificamerican.com/slideshow/a-do-it-yourself-quantum-eraser/>

You can find all necessary materials to do this experiment here:

<https://www.scientificamerican.com/article/a-do-it-yourself-quantum-2007-05/>

If we do the thought experiment of using a single photon for this experiment, we obtain the so called **quantum eraser**.

BIBLIOGRAPHY

About recent quantum cryptography applications

Review in New Scientist

Article in Nature Photonics

2007 Swiss elections

An interactive timeline of cryptography (done by ICFO to CosmoCaixa's exhibit Top Science)

About Einstein and his dilemmas with quantum physics

Is the moon really there?

A great introduction to quantum phenomena

Quantum Physics: A first encounter, by Valerio Scarani

A quantum manifesto - A new era of technology

