REPUBLIQUE DU
CAMEROUN
Paix-Travail-Patrie
* * * * *
UNIVERSITE DE YAOUNDE 1
* * * * *
CENTRE DE RECHERCHE ET
DE FORMATION
DOCTORALE EN SCIENCES
TECHNOLOGIQUES
* * * * *
UNITE DE RECHERCHE ET
DE FORMATION
DOCTORALE PHYSIQUE ET
APPLICATIONS
* * * * *
BP :812 YAOUNDE
* * * * *
Email :bertrand.tsemo@facsciences-uy1.cm

REPUBLIC Of CAMEROON
Peace-Work-Fatherland
* * * * *
UNIVERSITY OF YAOUNDE 1
* * * * *
POSTGRADUATE SCHOOL
OF SCIENCE,TECHNOLOGY
AND GEOSCIENCE
* * * * *
RESEARCH AND
POSTGRADUATE TRAINING
UNIT FOR PHYSICS AND
APPLICATIONS
* * * * *
P.O. BOX :812 YAOUNDE
* * * * *
Email :bertrand.tsemo@facsciences-uy1.cm

Laboratory of atomic, molecular and biophysics

Simulation "Quantum key distribution(BB84 protocol) using polarized photons"

TPE6-PHY4268,Simulation of Quantum Key Distribution

Realized by :
M.Tsemo Peniel Bertrand

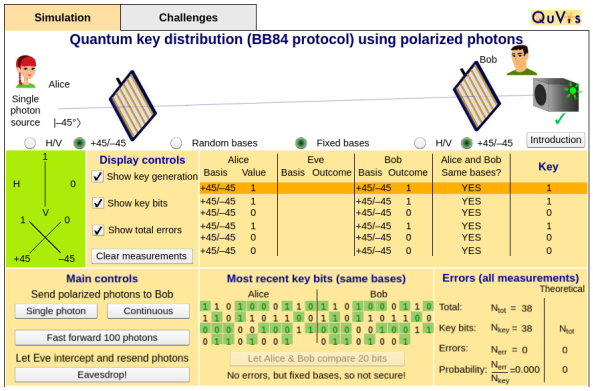
Under the leadership of :
Pr.Serge Guy Nana Engo

Année académique
2019/2020

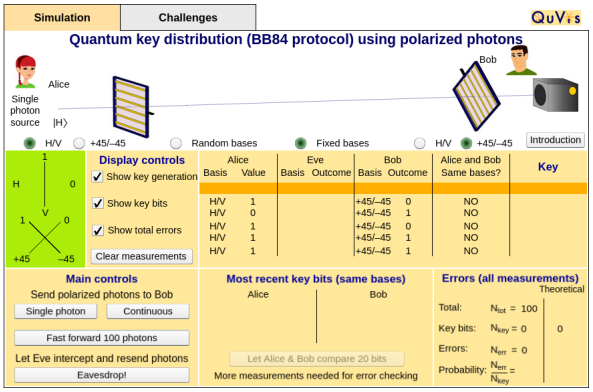
Introduction

Our society is more and more based on communications. Sometimes when we are communicating, we wish to share a secret message with our interlocutor or we want to be sure that nobody intercepted our message we sent. We want our message to be completely secure. There comes yet the problem of sharing a message between two partners with a complete security.In what follows, we will simulate a quantum communication protocol named Quantum Key Distribution, precily the BB84 protocol using polarized photons.

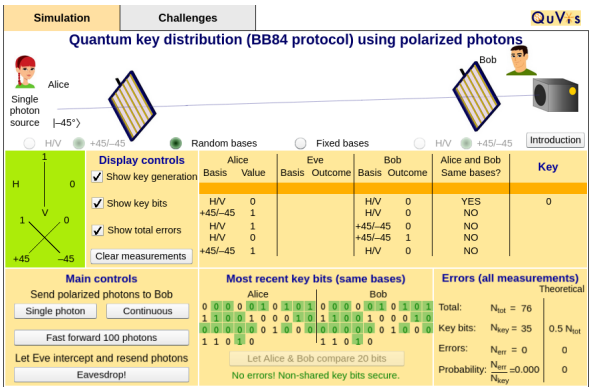
1 We set-uped our simulation with different situations as it follows :



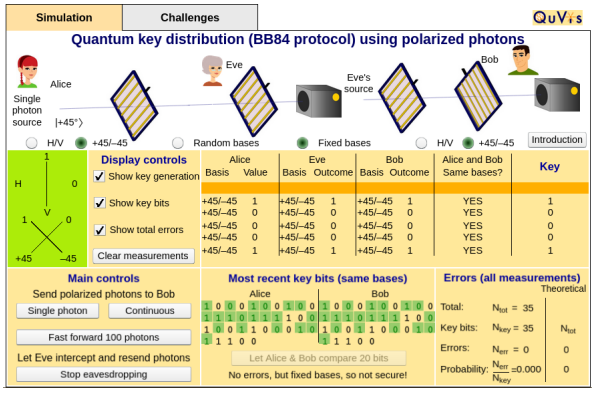
(a) *Fixed same bases used and no eavesdropper*



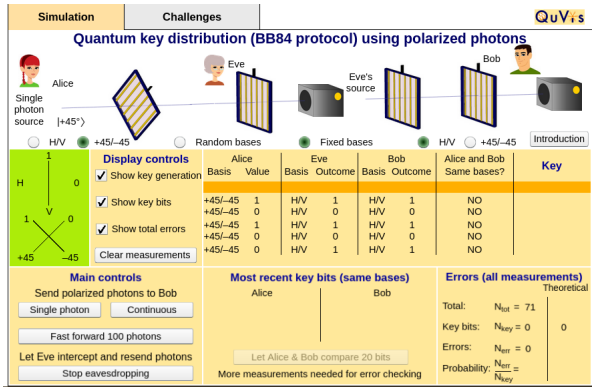
(b) *Fixed different bases used and no eavesdopper*



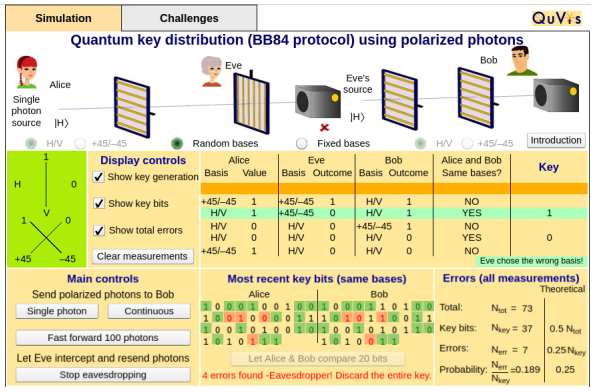
(c) *Random bases used and no eavesdropper*



(d) *Fixed same bases used with an eavesdopper*



(e) *Fixed different bases used with an eavesdopper*



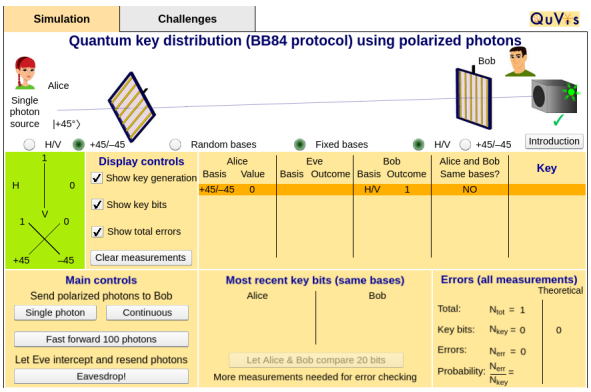
(f) *Random bases used with an eavesdropper*

2 a) Generally, if Alice sends a photon state with a basis different from Bob's basis, this one will detect a photon or not due to his polarizer's orientation. Indeed, by choosing a basis different from Alice, Bob detects a photon or not with 50% of probability.For example, if Alice sends a single photon with the polarisation $+45$, this is to say she sends a photon in the state $|+45\rangle$, this photon is randomly determined in the H/V basis.the state $|+45\rangle$ is in a supersposed

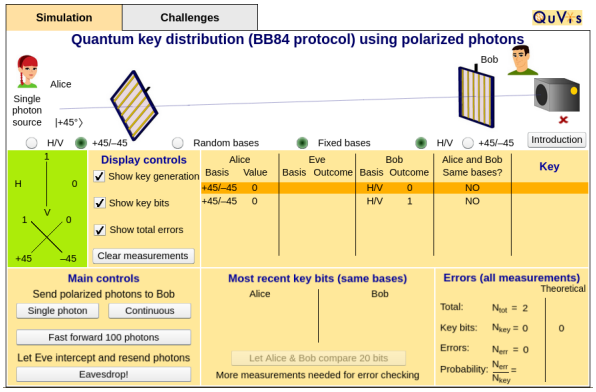
state in the H/V basis that we can write like it follows :

$$|+45\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

So, if for example Bob orients his polarizer in the V axis, this is to say he choosed the H/V basis,the photon $|+45\rangle$ sent by Alice will be projected in the $|H\rangle$ or$|V\rangle$ state each 50% of cases. Thus, Bob will detect a photon with the probability $\frac{1}{2}$ and will not detect it with the probability $\frac{1}{2}$. Why is it like that ?
It is like that because after Bob measurement, the photon sent by Alice take one of $|H\rangle$ and $|V\rangle$ states. If the state took by Alice's photon is $|H\rangle$, Bob's detector will not detect it because his polarizer is oriented along the V axis. But if Alice's photon is projected in the $|V\rangle$ state, his detector will detect it. Bob thus have the two situations with equal probabilities $\frac{1}{2}$.



(a) *Bob detect the photon sent by Alice*



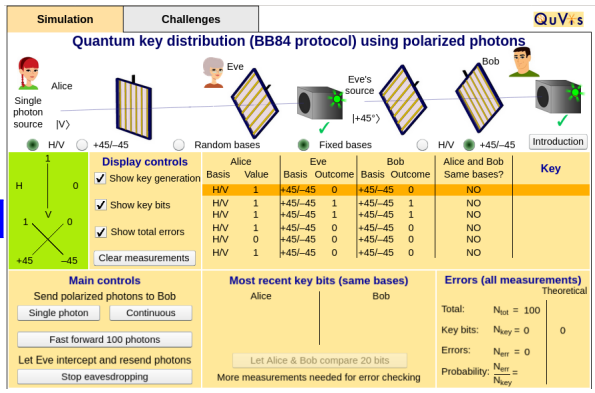
(b) *Bob don't detect the photon sent by Alice*

b) The table below is completed with this principle : **If Bob orients his polarizer along an axis and detect a photon, he understands that Alice sent a single-photon in one of the other basis's states, or in the state of the orientation he choosed ; But if he d'ont detect a photon, he understands that Alice sent a single-photon only in one of the other basis states** .
We thus have the table :

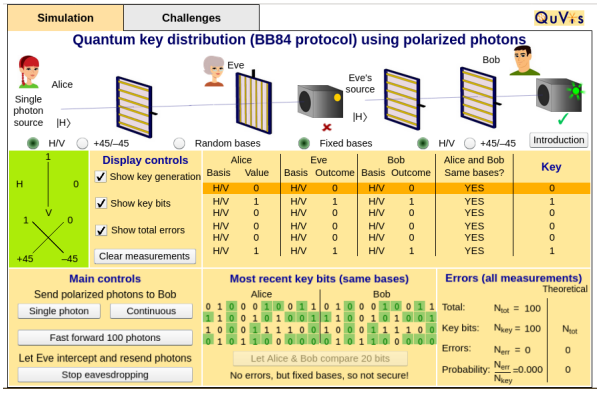
Bob's polarizer	Bob detect a photon ?	What Bob can infer about the polarization state sent by Alice without knowing her basis
V	yes	Alice sent the polarization state $\|+45\rangle$ or $\|-45\rangle$ or $\|V\rangle$
V	no	Alice sent the polarization state $\|+45\rangle$ or $\|-45\rangle$
-45	yes	Alice sent the polarization state $\|V\rangle$ or $\|H\rangle$ or $\|-45\rangle$
-45	no	Alice sent the polarization state $\|H\rangle$ or $\|V\rangle$

c) In the key generation pannel, a key bit is generated when Alice and Bob choose the same basis. A key bit value is determined by the bit value of the orientation of Bob's polarizer if he detects a photon, by the opposite bit value of the orientation of Bob's polarizer if he don't detect any photon.

3



(a) *Alice and Bob choose different bases*



(b) *Alice and Bob choose same bases*

In this simulation, there is an eavesdropper Eve which by chance, chooses the same basis than Bob. In this case, we have two situations that can happen :

Alice and Bob choose different basis : No secret key can be generated. Indeed , to generate a key, Alice and Bob only consider their bits coming from same base used.

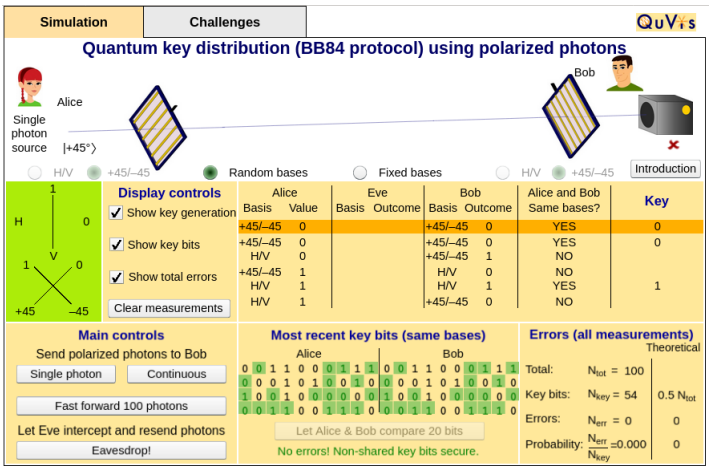
Alice and Bob choose the same basis : : As Eve chooses the same basis than Bob, no error occurs on the quantum channel.Eve intercepts the single-photon sent by Alice and resends it to Bob, this one measures the photon and obtains the same than by Alice. Because of Eve used the same basis than Bob, Alice and Bob establish a key but all is happening like there were no eavesdropper. For this reason, **no secure key is generated ! ! ! !**

a) If Eve's polarizer in front of her detector was set to V :

- ☞ **Eve don't detect any single-photon :** If Eve don't detect a photon, it means that during her measurement, the photon was projected in the $|H\rangle$ state. So she will resend the state $|H\rangle$ to Bob.
- ☞ **Eve detect a single-photon :** It means that after her measurement, her photon is in the $|V\rangle$ state. Then she will resend the state $|V\rangle$ to Bob.

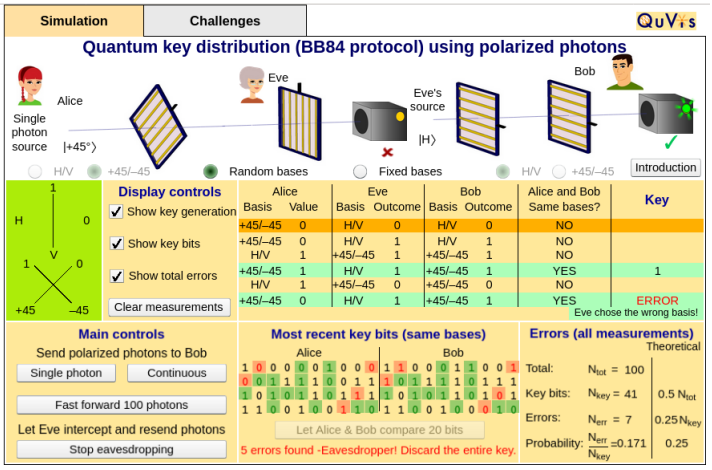
b) Any errors occurs in Alice and Bob maesurements.
Yes the secure key is using only a single-basis.

4



There is no eavesdopper and random bases are used

The half of Alice's photons lead to a key bit. This fraction comes about by the fact that in half of cases, Alice and Bob choose different basis.



Eve is eavesdopping and random bases are used

5

a) When Eve intercepts particules, she act exactly like Bob. Let say that she do what Bob should do before him.She chooses to measure in either H/V or $+45/-45$ basis, then she resends a new polarized photon to Bob according to the result of her measure.

b) *How does an error occurs* ? Let take the example that follows : Alice sends a photon polarized in the state $|+45\rangle$, this means that she choosed the $+45/-45$ basis. Assume Bob chooses the same basis as Alice, this is to say he chooses the $+45/-45$ basis to measure the polarization of the single-photon comming. When the eavesdropper Eve intervenes, there are two situations that can happen, one with no error, another with error :

   ∴ Assume Eve chooses the same basis as Alice, she will obtain the same state as the one sent by Alice (because of the right basis she choosed) and resend it to Bob, this one will then measure it and also obtain the same state as Alice. In this case, all is happening like there where no eavesdopper on the quantum line, **no error when Alice and Bob compare some bits**.

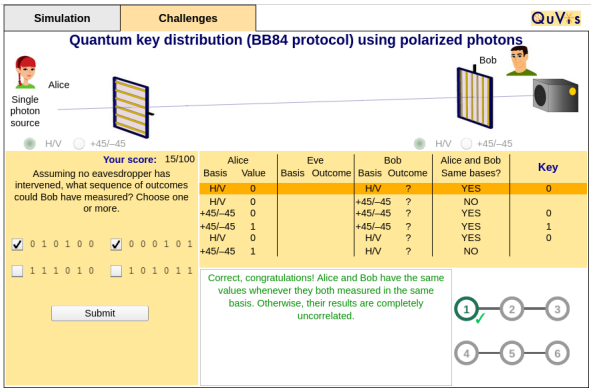
   ∴ But if Eve chooses the basis H/V , she resends a single-photon in one of the states $|H\rangle$ and $|V\rangle$ to Bob. Bob, who shoosed the same basis as Alice, by measuring the photon sent by Eve will obtain the state $|+45\rangle$ only in 50% of cases.We understand that once Bob obtains the state $|-45\rangle$, he has a bit different from Alice. We then conclude that **there is an error on the quantum line**.
   When an error occurs, we can say that Eve's basis is different from Alice and Bob basis.

c) No, not eveytime. Indeed, the error is due to the fact that the basis choosed by Eve makes Bob's result be randomed.When Bob measures the photon resent by Eve, we have an error only when he obtains a state different from the one Alice sent ; But Bob can by chance (*for Eve*) obtain the same result as Alice and no error will occur.

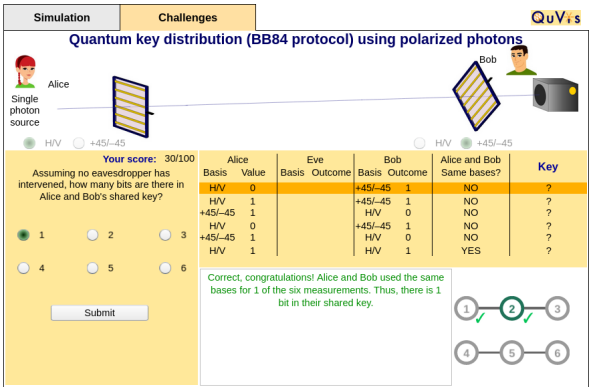
d) 25% of the key bits lead to an error. This fraction comes about the fact that when Eve intercepts Alice's photon, she can imitate Bob only in 50% of cases.

e) To determine if Eve has not compromised their key, they can compute the error rate on the quantum line.

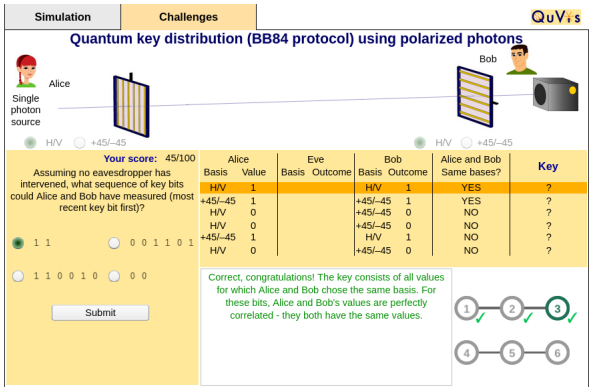
6 Below we have the six challenges of our simulation :



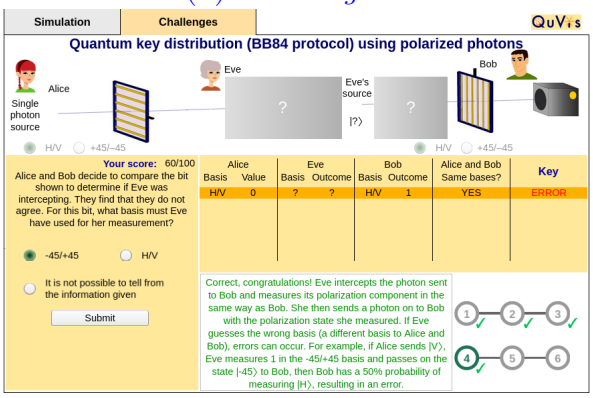
(a) *challenge 1*



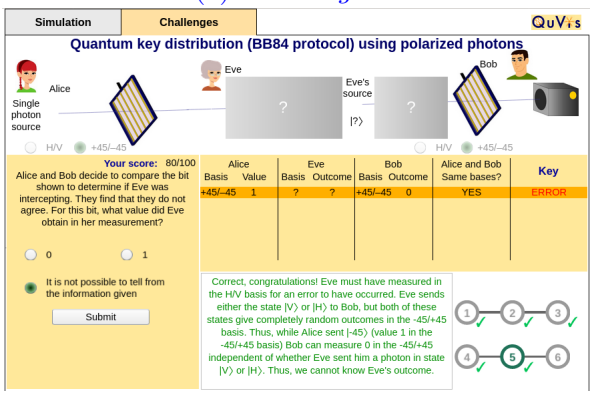
(b) *challenge 2*



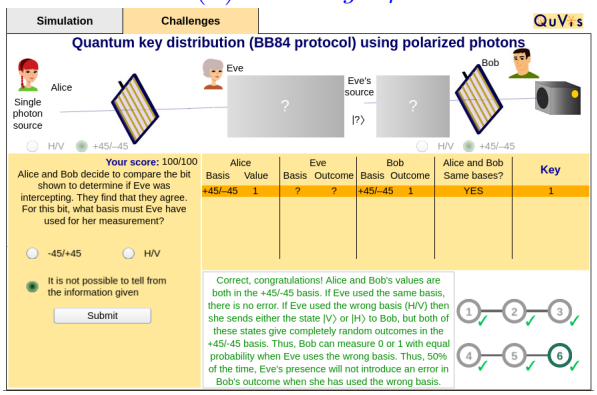
(c) *challenge 3*



(d) *challenge 4*



(e) *challenge 5*



(f) *challenge 6*

The challenge I found most difficult was the challenge number 6, because of his relevance and because I lost it at my first try. In the challenge, they say that Alice and Bob are trying to compare the bit 1 they both obtained choosing the same H/V basis in order to know if Eve is intercepting. Afer measuring, they find that they agree. The question is : **For this bit, what basis must Eve have used for her measurement ?**

We first failed because we considered that if Alice and Bob don't find any error, it means that Eve by chance used necessarily the same basis as them. But this is not completely correct because Eve can use the basis $-45/+45$ (different from Alice and Bob), this don't avoid that Bob by chance (for Eve) measure the same bit than Alice (bit 1 in H/V basis). Thus if Alice and Bob agree to the bit 1 they both obtain , **it is not possible to conclude from the information given**

Conclusion

To conclude, in what is above, we have simulated the BB84 protocol exploiting different situations.The first situation was that Eve was eavesdropping and fixed basis where used. We saw that when fixed bases are used, either no key bit is generated (Alice and Bob choose different bases) or the key bits generated are not secure (because of fixed bases). Then we saw the situation where there was no eavesdropper and random bases where used and we extracted that no error occurs and there is non-chared bits secure. Finally we was the situation where Eve was eavesdropping and random bases where used and we extracted in this situation that when Alice and Bob note that the error rate is high, they discard the entire key and restart. Let ask ourselves how can we sumlate the same protocol without using polarized photons.