Quantum Safe Key Distribution

Dr. Suchetana Chatterjee

July 17, 2015

Scene I

(Mr. Wilson, the project manager is seated on a chair working with his files. Alice, one of his employee, enters.)
Alice: Good morning, Mr. Wilson.

Wilson: Hi, Alice. How are you doing today?

Alice: I'm doing fine, thank you very much.

Wilson: Alice, I have something very important to talk to you about. We need to deliver Bob some very important information about a very confidential pass key. But we need to be absolutely sure that no one is eavesdroppin. Since Bob and you will be talking over the telephone, we need to make sure that no one is intercepting the call. Okay?

Alice: I do understand what you want to achieve, sir. But I do not understand how we can achieve it.

Wilson: Ah that's nothing to worry about. My very good friend Dr. Griffiths will help you about it. I shall refer you to him.

Alice: Thank you, Mr. Wilson! [Leaves]

Scene II

(Prof. Griffiths is working on his table when Alice enters.) **Alice:** Hello, Prof. Griffiths.

Prof: Hello Alice! Wilson told me you'd be paying a visit. I hear you need to understand the quantum safe key distribution, right?
Alice: Yes, sir.
Prof: Please sit down, Alice. We need to begin from the very beginning!

(Prof. takes a piece of chalk and walks to the blackboard.)

Prof. Well, Alice, how are information stored and transferred today? What kind of technology is used? 'Digital' or 'analog'?
Alice: Digital, professor.

Prof.: Great! So everything is stored in bits in a digital system. Tell me what is a bit?

1. What is the correct answer according to you?

   I. Measuring device.

   II. Something that can exist in two states.

   III. 1 and 0.

   IV. Powers of 10.

   The answer is **II** because bit means anything that exists in two distinct states. BIT is binary (which means two) digit.

2. Which among the following can be a bit?

   a) Negative and positive numbers, and zero.

   b) The plates of a capacitor above and below a certain charge.

   c) Head or tail.

d) The result of tossing two coins simultaneously.

I. a.
II. All of the above.
III. b and c.
IV. b only.

It is number **III**, because negative, positive and zero are three possible states, and if you toss two coins simultaneously, the outcome has three possible values out of head-head, head-tail and tail-tail, if you do not distinguish between the coins.

Prof.: But bits are not necessarily classical. There can be quantum mechanical bits called Qu-Bits.

3. Which of the following can be a QuBit?

a) Spin states of an electron.
b) Energy states of the hydrogen atom.
c) Energy eigenstates of the harmonic oscillator.
d) Polarization states of a photon.

I. a and b.
II. b and c.
III. d only.
IV. a and d.

The correct answer is **IV**. The electron is a spin half particle, so its z component is $+\frac{1}{2}$ and $-\frac{1}{2}$. The photon is a spin 1 particle, so it can have three states ± 1 and 0. But, the particle being relativistic, it is not allowed to have the zero state (which is a prediction of quantum field theory). So it also has two states. Therefore, 'a' and 'd' can be QuBits.

Alice: But why do we care about quantum mechanics at all?
Prof.: Well, Alice. Classically we can not by any means transfer a key safely over a public channel. You can not know if someone is eavesdropping. Quantum mechanics, on the other hand, saves us there. But to understand the how, we need to review some concepts of quantum mechanics first.
Alice: Sounds great!
Prof.: Tell me, if I have a two state system in quantum mechanics, then,

4. What is the dimensionality of the associated vector space?

   I. 1-dimensional.

   II. Infinite dimensional.

   III. 2-dimensional.

   IV. None of the above.

The answer is **III**. The vector space is 2-dimensional.

Prof.: One other important concept in quantum mechanics is linear independence and linearly independent vectors. We need to know about them.

5. We call two vectors $|a\rangle$ and $|b\rangle$ linearly independent when:

   I. $\alpha |a\rangle + \beta |b\rangle = 0$, where α and β are any two numbers.

   II. $\alpha |a\rangle + \beta |b\rangle = 0$, where α and β are both simultaneously equal to 0.

   III. $\alpha |a\rangle + \beta |b\rangle = k$, where k is an arbitrary constant.

   IV. $\alpha |a\rangle - \beta |b\rangle = 0$.

The answer is **II** because if $\alpha |a\rangle + \beta |b\rangle = 0$, for non zero α and β, then $|a\rangle = -\frac{\beta}{\alpha} |b\rangle = \gamma |b\rangle$. So, it would be possible to represent $|a\rangle$ in terms of $|b\rangle$. Then

they would be linearly dependent, and co-linear vectors. The only combination for which the combination can be zero for linearly independent vectors is where both α and β are zero.

6. For a 2-dimensional vector space how many linearly independent vectors do you need to represent any state in that vector space?

   I. 2 vectors.

   II. At least 2 vectors.

   III. At most 2 vectors.

   IV. Infinite number of vectors.

   The answer is **II**, because you can represent a two dimensional vector as the linear combination of ANY two linearly independent vectors in that vector space. The two linearly independent vectors are called *basis vectors*. Choosing a basis is like choosing a co-ordinate system.

7. Now, if we take the vertical and horizontal polarization states of the photon as basis vectors in our 2-dimensional vector space then how would you represent a normalized $+45^\circ$ polarization? [$|S\rangle_{45^\circ}$ represents $+45^\circ$ polarization, $|V\rangle$ is vertical and $|H\rangle$ is horizontal polarization. We shall follow this notation throughout.]

   I. $|S\rangle_{45^\circ} = |V\rangle + |H\rangle$.

   II. $|S\rangle_{45^\circ} = |V\rangle - |H\rangle$.

   III. $|S\rangle_{45^\circ} = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle)$.

   IV. $|S\rangle_{45^\circ} = \frac{1}{2}(|V\rangle + |H\rangle)$.

   When we talk about normalized states we mean that $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$, such that $\alpha^2 + \beta^2 = 1$. Only **IV** satisfies this criterion. When you express a state in terms of the basis vectors, the coefficient depends on the angle between the vector and the basis vectors.

If θ and θ' are the corresponding angles then the coefficients will be $\cos\theta$ and $\cos\theta'$. Hence,

$$\begin{aligned} |s\rangle_{45^\circ} &= \cos\theta\,|H\rangle + \cos\theta'\,|V\rangle \\ &= \cos\theta\,|H\rangle + \cos\left(\frac{\pi}{2} - \theta\right)|V\rangle \\ &= \cos\theta\,|H\rangle + \sin\theta\,|V\rangle \end{aligned}$$

8. Express -45° polarization in the basis of $|V\rangle$ and $|H\rangle$.
[Hint: Draw a diagram.]

Ans. It will be $\frac{1}{\sqrt{2}}|H\rangle - \frac{1}{\sqrt{2}}|V\rangle$, because $\theta = -45^\circ$, $\cos(-45^\circ) = \frac{1}{\sqrt{2}}$, $\sin(-45^\circ) = -\frac{1}{\sqrt{2}}$.
The choice of basis is not unique. We can choose any 2 vectors as long as they are not co-linear, as our basis vectors.

9. Which of the following can be a basis for the polarization states of a photon?

I. Vertical and horizontal polarization.
II. 30° and -60°.
III. 45° and and -45°.
IV. Horizontal and -45°.
V. All of the above.
VI. Everything except **IV**.

Ans. The answer is **V** because any of them can be treated as basis vectors. However **IV** is not an orthogonal basis. They have component along each other.

So it is not a convenient basis to choose. It is always a good idea to choose an orthogonal basis.

Alice: What is exactly an orthogonal basis? **Prof.:** Well, rigorously two vectors are said to be orthogonal when the scalar product of $\langle a|\ b\rangle = 0$, which means the vectors do not have components along each other. Meaning, you can not write one of these two vectors with the help of the other in any manner whatsoever.

10. Which of the following is an orthogonal basis?

a) Horizontal and vertical.

b) $-45°$ and $+45°$.

c) $30°$ and $60°$.

d) $-60°$ and $30°$.

I. All of the above.

II. a, b and c.

III. a and b.

IV. a, b and d.

Ans. The correct answer is **IV** because c is the one where the vectors are not perpendicular to each other.

11. In a 2-dimensional vector space, how many orthogonal basis can you have?

I. 1.

II. Infinite.

III. $2 \times 2 + 1 = 5$.

IV. 2.

Ans. The answer is infinite. You can have infinite combinations of orthogonal vectors in a 2-dimensional vector space. The result is the same regardless of dimensions.

Prof.: Then next question is which one should we choose? Well, we will choose the one that is most convenient for our measurement. For example, if we are using vertical and horizontal polarizers to measure the polarization states of a photon it would be best to choose $|V\rangle$ and $|H\rangle$ as our basis, $|S\rangle = \alpha\,|V\rangle + \beta\,|H\rangle$.

12. If you are using $\pm 45^\circ$ polarizers to measure polarization which of the ones should you use as your basis?

    I. $|S\rangle_{45^\circ}$ and $|S\rangle_{-45^\circ}$.

    II. Vertical and horizontal.

    III. $|S\rangle_{100^\circ}$ and $|S\rangle_{190^\circ}$.

    IV. None of the above.

Ans. Since you are measuring with $\pm 45^\circ$ polarizer your state will always collapse to a state where the polarization of the photon after measurement is either $+45^\circ$ or orthogonal to it -45°. So it would bb best to choose your basis as $|S\rangle_{45^\circ}$ and $|S\rangle_{-45^\circ}$. So the correct answer is **I**. Remember that no matter what the state of the photon was initially it will either collapse to $+45^\circ$, or -45°, once you do the measurement. This is called the "collapse hypothesis".
Prof.: Let's think about an experiment now.

13. Suppose you are measuring polarization with $|H\rangle$ and $|V\rangle$. Write down $|S\rangle_{45^\circ}$ in the appropriate basis.

Ans. The basis will be $|H\rangle$ and $|V\rangle$, and $|S\rangle_{+45^\circ} = \frac{1}{\sqrt{2}}\,|H\rangle + \frac{1}{\sqrt{2}}\,|V\rangle$.

14. Now write any state $|S\rangle$ in the basis of $|H\rangle$ and $|V\rangle$.
Ans. $|S\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$.

15. According to the 'collapse hypothesis' fot **14** the state will collapse to either $|H\rangle$ or $|V\rangle$. So what is the probability that you measure horizontal polarization?

I. 1.

II. α.

III. α^2.

IV. $\alpha\beta$.

Ans. The probability for measuring horizontal polarization would be α^2. This comes from the fact that,

$$\begin{aligned} |S\rangle &= \alpha\,|H\rangle + \beta\,|V\rangle\,, \\ \Rightarrow \langle H|\ S\rangle &= \alpha\,\langle H|\ H\rangle + \beta\,\langle H|\ V\rangle\,, \\ &= \alpha. \end{aligned}$$

Thus, the determined coefficient is α, and the probability is thus α^2.

16. Can you find the probabilty for measuring vertical polarization?
Ans. Using the same steps, $|S\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$ yields the coefficient $|V|\ S\rangle = \beta$, hence the probability turns out to be β^2.

17. For $|S\rangle_{45^\circ}$, what is the chance that you measure horizontal polarization?

I. 100%.

II. 50%.

III. 25%.

IV. None of the above.

Ans. The correct answer is **II** because from **Q 13** we see that,

$$|S\rangle_{45^\circ} = \frac{1}{\sqrt{2}}\,|H\rangle + \frac{1}{\sqrt{2}}\,|V\rangle\,.$$

Therefore, the probability for obtaining horizontal polrization is just $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$, which is $\frac{1}{2} \times 100\% = 50\%$.

Prof.: It is interesting to see the difference between the classical "Mallus' Law" with this. Here we are considering only one photon, and unless we do a measurement we are not sure if the photon has passed through a certain polarizer, whereas for "Mallus' Law", there was only a beam of photons and there was no uncertainty. The average intensity was given by $I_0 \cos^2\theta$, where θ is the angle between the polarizing axis of the polarizer and the polarization vector of the electromagnetic wave. The uncertainty thus translates into the so called "expectation value".
Alice: I undertand.

18. If a photon is polarized at 60°, find the probability of observing it with a 45° polarizer.

    I. 50%.

    II. 96.59%.

    III. 93.30%.

    IV. 100%.

Ans. The correct answer is **III** because,

$$|S\rangle_{60^\circ} = \cos 15^\circ \, |S\rangle_{45^\circ} + \cos 105^\circ \, |S\rangle_{-45^\circ} \, ,$$

and hence the probability is $\cos^2 15^\circ = 93.30\%$.
Alice: Professor, aftr doing a measurement on a particle, can we restore it to the original state?
Prof.: No, Alice. Once you do a measurement, the state can never never be restored to the original state. That is all because, you have no idea what the original state was! The moment you made the measurement, you disturbed the system, and all information prior to that measurement about the system is lost.
Alice: Is that not amazing, now!
Prof.: Okay, that's enough of quantum mechanics we did. Now let us move on to "safe key distribution". Do you have some idea now, about how to do this?
Alice: Why! I will send vertical and horizontal polarized photons over to Bob labelling them as 1, and 0, and we will be connected over the phone. Every time Bob says he got a photon, we shall both note that!
Prof.: Excellent! But let's think it over a bit, now.

19. Everytime Alice sends a photon to Bob and Bob measures it. What can Bob infer about the state of the photon?

    I. He is 50% sure when he gets a click.

    II. He is 50% sure when he doesn't get anything.

    III. He is 100% sure in every case.

    IV. He is 100% sure only when he gets a click.

Ans. The answer is **III**. Let's say, Alice sends a vertical photon. If Bob measures it with a horizontal polarizer, he does not get a photon, hence he knows immediately that the original photon was a vertical. Again, if Bob measures it with a vertical polarizer, he gets a photon, and he knows that the photon was vertical, and it is all because they are using orthogonal systems for signal transmission.

20. Answer the following:

Bob uses	Bob observes	Bob infers
$\|V\rangle$	Nothing	
$\|V\rangle$	Photon	
$\|H\rangle$	Nothing	
$\|H\rangle$	Photon	

Ans. The completed table is:

Bob uses	Bob observes	Bob infers
$\|V\rangle$	Nothing	$\|H\rangle$
$\|V\rangle$	Photon	$\|V\rangle$
$\|H\rangle$	Nothing	$\|V\rangle$
$\|H\rangle$	Photon	$\|H\rangle$

Alice: Now let Eve (the culprit) eavesdrops over your conversation. Now, by intercepting each photon sent by you, she can certainly know which photon you have sent? And then she can just relay the same photon over to Bob, so that none of you can ever anticipate that you are being watched.

Alice: Oh my goodness! Then what can I do to prevent this?
Prof.: Wait. We shall need to use two non-orthogonal basis if we have to know if someone is eavesdropping.
Alice: Now how is that?
Prof.: Okay, then read this up!

[Hands over a copy of Bennett (1991) Phys. Rev. Vol. 68 No. 21]

Alice sends photons of $+45^\circ$ polarization and horizontal (0°) polarization. Bob measures them with -45° and vertical (90°). Every time Bob gets a photon, he notifies Alice, and they decide to call $+45^\circ$ bit 1 and 0° as bit 0.

21. Alice transmits $+45^\circ$ and Bob measures it with -45° polarizer. What does Bob observe?

    I. Photons are always blocked.

    II. 50% photons are blocked.

    III. Photons always pass.

    IV. 75% photons are blocked.

Ans. The answer is **I**, because $+45^\circ$ and -45° are mutually orthogonal.

22. Alice transmits $+45^\circ$ polarization. Bob measures it with a 90° filter. What does Bob observe?

    I. Photons are always blocked.

    II. 50% photons are blocked.

    III. Photons always pass.

    IV. 75% photons are blocked.

Ans. The correct answer is II.

$$|S\rangle_{45^\circ} = \frac{1}{\sqrt{2}}|V\rangle + \frac{1}{\sqrt{2}}|H\rangle\,.$$

For measurement with vertical polarizer, the probability that Bob will see photon passing is $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} \equiv 50\%$. So the rest 50% will be blocked.

23. Alice transmits 0° and Bob uses -45° filter. What would Bob observe?

    I. Photons always pass.
    II. Photons are always blocked.
    III. 75% photons are blocked.
    IV. 50% photons pass.

Ans.

$$|H\rangle = \frac{1}{\sqrt{2}} |S\rangle_{45^\circ} + \frac{1}{\sqrt{2}} |S\rangle_{-45^\circ} .$$

The probability that Bob sees them is $\frac{1}{2} \equiv 50\%$ and so the correct answer is **IV**.

24. Alice transmits 0° and Bob measures with 90°, what will Bob observe?

    I. Photons always pass.
    II. Photons pass 75% of the time.
    III. Photons never pass.
    IV. Photons pass only 50%.

Ans. The answer is **III** because 0° and 90° are orthogonal to each other.

25. Based on the answers in **Q 21** and **Q 24**, complete the following table:

Alice Transmits	Bob Measures	Bob Observes
$+45^\circ \equiv 1$	-45°	
	90°	
$0^\circ \equiv 0$	-45°	
	90°	

Ans. The answer is:

Alice Transmits	Bob Measures	Bob Observes
$+45^\circ \equiv 1$	-45°	Photons blocked.
	90°	50% times blocked.
		50% times passed.
$0^\circ \equiv 0$	-45°	50% times passed.
		50% times blocked.
	90°	Photons blocked.

26. For which of the observations is Bob 100% sure of what was originally sent?

    I. In all cases.

    II. In none of the cases.

    III. Only when he does not obtain a photon.

    IV. Only when he gets a photon.

    Ans. The answer is **IV**, since when he gets a photon with a 90° polarizer, he is sure that has come only from a 45° photon. But, when he does not obtain a photon, it can be either 45° (25% chance) photon or −45° photon (50% chance), and there is no way of telling them apart!

    Alice: Aha! So Eve will have the same problem!
    Prof.: Exactly. When she will be unsure, she will have to make a guess about the photon, and relay that over to Bob, hoping she will be right.
    Alice: But she just can't be right all the time!
    Prof.: That's right. Now tell me, what is the probability that she gets it right?

27. Look at the previous table and infer the fraction of time Eve is sure what Alice has sent:

    I. 30% of the time.

    II. 25% of the time.

    III. 50% of the time.

    IV. 75% of the time.

    Ans. The table shows that $\frac{1}{4}$ or 25% of the time Eve will exactly know what Alice has sent. So, the answer is **II**.

28. Complete the following table ($90° \equiv V$ and $0° \equiv H$, $-45° \equiv \bar{S}$ and $45° \equiv S$):

Person		
Alice	Bit Value	1 0 1 0 1 0
	Polarization	S H S H S H
Bob	Polarization	$\bar{S}$ $\bar{S}$ V V V $\bar{S}$
	Result	
Transmitted Key:		

Ans. The answer is:

Person		
Alice	Bit Value	1 0 1 0 1 0
	Polarization	S H S H S H
Bob	Polarization	$\bar{S}$ $\bar{S}$ V V V $\bar{S}$
	Result	
Transmitted Key:		

Prof.: So you see, Alice? No matter how careful Eve is, she will introduce a minimum 25% error in the key transfer, and you will have a key distribution as safe as it can be! You only have to query certain bits which Bob receives (let's say every 10th bit), after the whole key is transferred.
Alice: If someone is eavesdropping, then there will be some discrepancy in the result! How elegant!
Prof.: Yes, it is. So, after the cross check if there is some discrepancy, just discard the key and try some other time!
Alice: Thank you so very much, Prof. Griffiths!
Prof.: I wish you all the best, Alice.

Scene III

[Mr. Wilson's room: Alice enters.]

Alice: Hello, Mr. Wilson! I finally got it!
Mr. Wilson: That is great! Here is a reference: *Bethune and Risk (2000), IEEE Journal 36(3) 340-7* of how it is implemented.
Alice: Thanks, Mr. Wilson! I will look over it and get back to you.

29. Alice and Bob decides that instead of using $+45°$ and $0°$, she will transmit $60°$ and $0°$ polarized photons. Bob will keep his polarizers at $-30°$ and $90°$, with $60° \equiv 1$ and $0° \equiv 0$.

a) When Alice transmits $60°$ and Bob uses $-30°$, what would Bob observe? Explain your answer.

I. Photons are always blocked.
II. 50% of the time the photons are blocked.
III. Photons always pass.
IV. 75% of the time the photons are blocked.

b) When Alice transmits $+60°$ and Bob measures it with $90°$ polarizer, what does Bob observe? Explain your choice.

I. Photons are always blocked.
II. 50% of the time the photons are blocked.
III. Photons always pass.
IV. 75% of the time the photons are blocked.

c) When Alice transmits $0°$ and Bob uses $-30°$ polarizer, what does Bob observe? Explain your choice.

I. Photons are always blocked.
II. 50% of the time the photons are blocked.
III. Photons always pass.
IV. 75% of the time the photons are blocked.

d) When Alice transmits $0°$ and Bob uses $90°$ polarizer, what does Bob observe? Explain your choice.

I. Photons are always blocked.
II. 50% of the time the photons are blocked.
III. Photons always pass.
IV. 75% of the time the photons are blocked.

Based on the answers from **29 a** to **d**, complete the following table:

Alice Transmits	Bob Measures	Bob Observes
$+60° \equiv 1$	$-30°$	
	$90°$	
$0° \equiv 0$	$-30°$	
	$90°$	