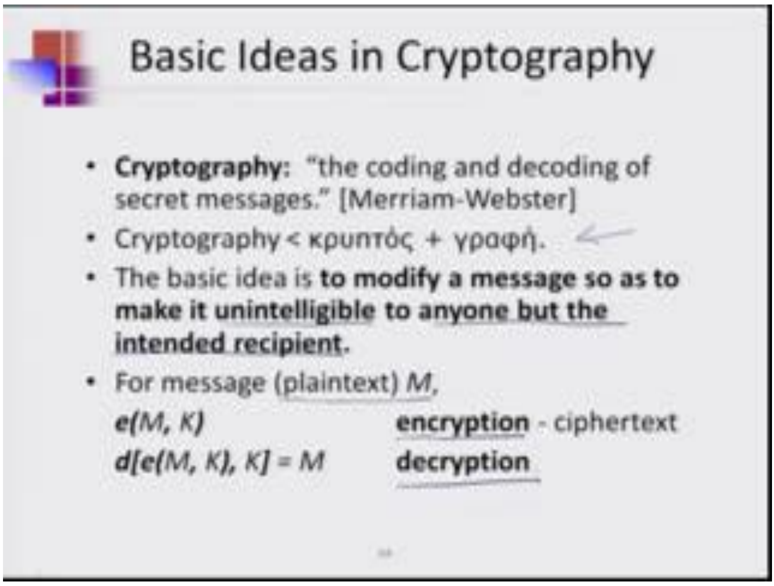
Implementation Aspects of Quantum Computing
Prof. Debabrata Goswami
Department of Chemistry
Indian Institute of Technology, Kanpur

Lecture – 06
Quantum Teleportation and Cryptography

So based on what we did in the last class. We will now get in to the concept of Cryptography and in terms of cryptography the definition or the description is given from various dictionaries.

(Refer Slide Time: 00:23)



Basic Ideas in Cryptography

- **Cryptography:** "the coding and decoding of secret messages." [Merriam-Webster]
- Cryptography < κρυπτός + γραφή.
- The basic idea is **to modify a message so as to make it unintelligible to anyone but the intended recipient.**
- For message (plaintext) *M*,

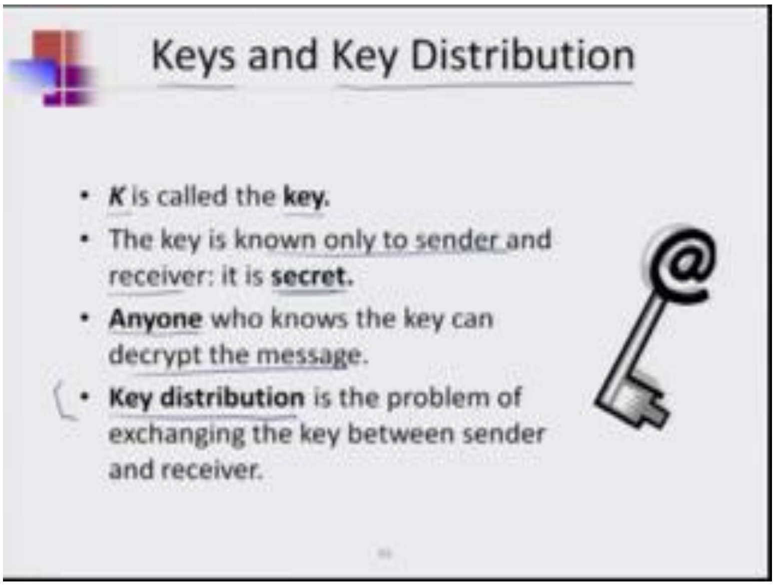
e*(M, K)*	**encryption** - ciphertext
d[e*(M, K), K]* = *M*	**decryption**

.

For example, Merriam-Webster dictionary; cryptography means the coding and decoding of secrete messages - nobody else can read for example, cryptography you write in a way that you cannot understand that sought of like the dictionary definition and we can represent it as a way in which we are not able to understand what is being sent or discussed about unless it is looked at in a proper way. So, cryptography can be coded in such a way that nobody else except the way other people can look at it.

So, the basic idea is to modify a message, so as to make it unintelligible to anyone but the intended recipient that is the main idea. For example, you have a plaintext message M which are going to be encrypted in such a way that unless it is decrypted you cannot understand what the message is. So, that is the basic idea behind cryptography.

(Refer Slide Time: 01:36)



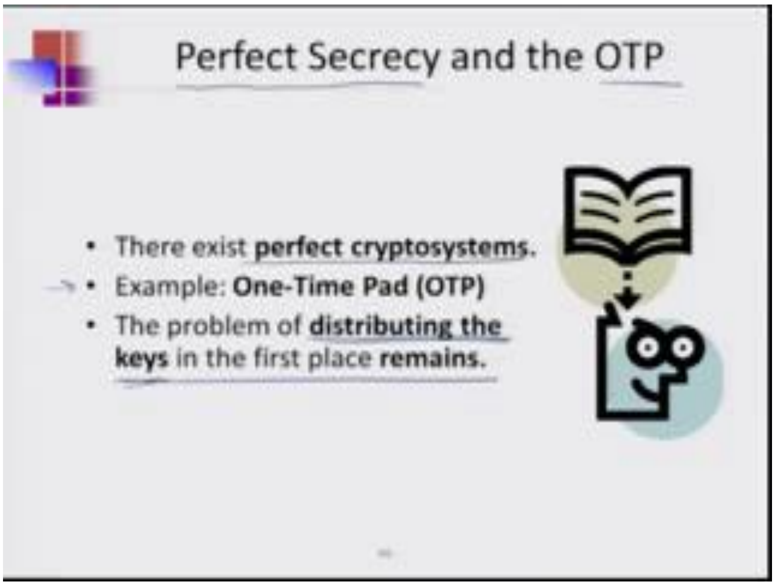
Keys and Key Distribution

- *K* is called the **key.**
- The key is known only to sender and receiver: it is **secret.**
- **Anyone** who knows the key can decrypt the message.
- **Key distribution** is the problem of exchanging the key between sender and receiver.

So, in this process the idea is to have a way to do this process. So, you need some keys and once you have the keys which can be distributed only those who have the keys will be able to understand the message. So, the principle is this K for example, is the key the key is known only to the sender and the receiver and that is how it is a secret.

Anyone who knows the key can decrypt the message. So, the first problem in this field is therefore, the idea of key distribution, because you want to actually distribute the key in a way so that is only for the intended receiver and no one else that is the main idea behind this.

(Refer Slide Time: 02:33)

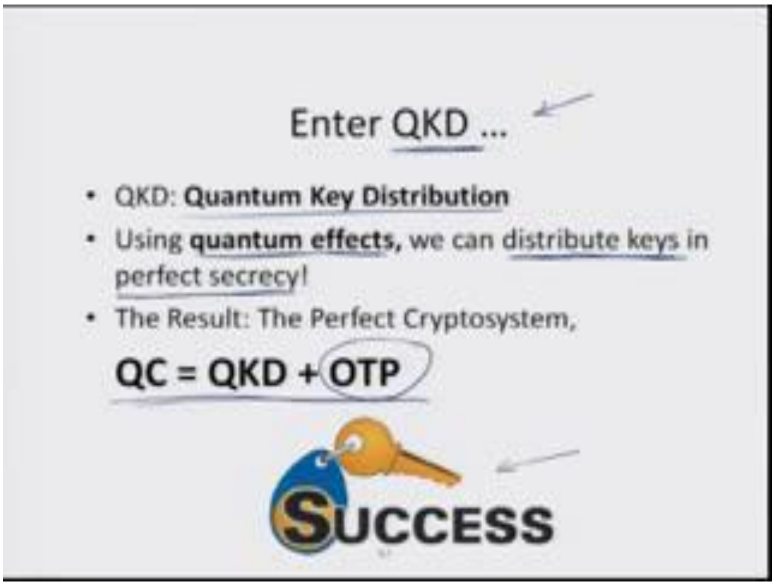


Perfect Secrecy and the OTP

- There exist **perfect cryptosystems**.
- Example: **One-Time Pad (OTP)**
- The problem of **distributing the keys** in the first place **remains.**

Perfect secrecy is roughly provided when the key that you are going to use is only going to be for once or in other words it is called the one time pad. So, this is known as the perfect cryptosystem because whatever you are using for example, this is the case which is a onetime pad only, if anything happens more than once it will not be same. The problem of distributing the keys in the first place however will still remain, because no matter what you do this one time pad also has to be provided appropriately to the right person, so the distribution of key remains as one of the most important parameter in this.

(Refer Slide Time: 03:23)



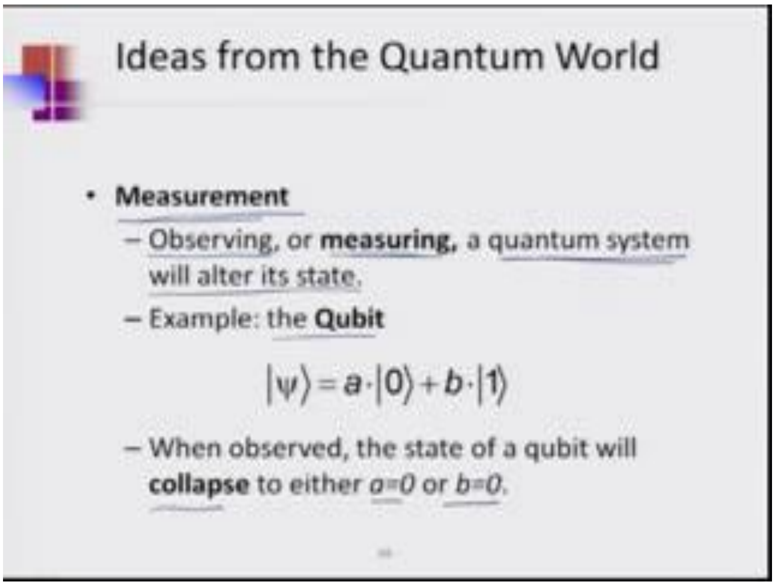
Enter QKD ...

- QKD: **Quantum Key Distribution**
- Using **quantum effects,** we can distribute keys in perfect secrecy!
- The Result: The Perfect Cryptosystem,

QC = QKD + OTP

So, we use quantum key distribution as one of the best ways of doing key distribution because, the quantum key distribution process is done in such a way that the distribution of the keys will be in perfect secrecy. So, the perfect cryptosystem essentially requires therefore, a quantum computing which can utilize the quantum key distribution and one time pad. Once you have that then you have a perfect success in terms of secrecy. So, that is the reason why quantum key distribution and that has become very powerful.

(Refer Slide Time: 04:07)



Ideas from the Quantum World

- **Measurement**
  - Observing, or **measuring,** a quantum system will alter its state.
  - Example: the **Qubit**

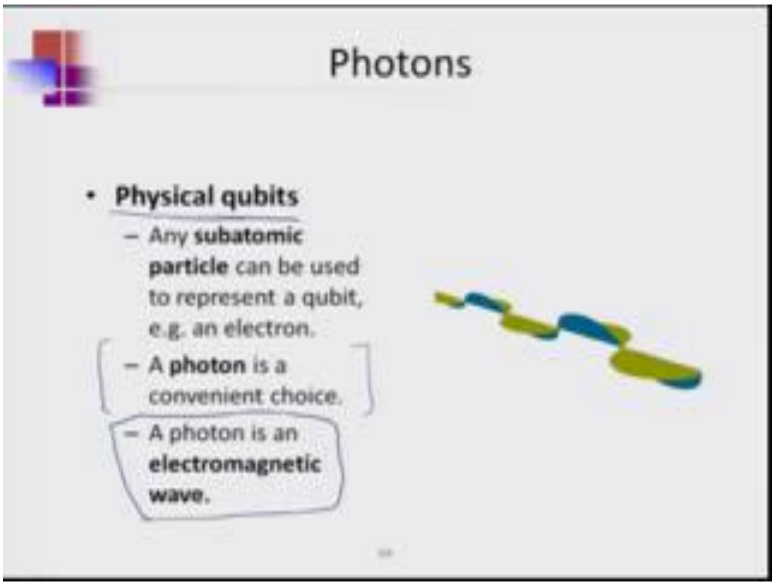
$$|\psi\rangle = a\cdot|0\rangle + b\cdot|1\rangle$$

  - When observed, the state of a qubit will **collapse** to either $a=0$ or $b=0$.

So, what is the key idea from the quantum world? First is the measurement part which we have read, the idea observing or measurement which you have done in a quantum way will alter its states which means that whenever we use a quantum way of doing our measurement then it is only one time use.

So, that is our principle of getting our one time pad in some sense. So, in this regard the qubit when it is observed the state of the qubit will collapse to either one of the two states, but unless it is measured it will be either in one of the two combination states.

(Refer Slide Time: 04:58)



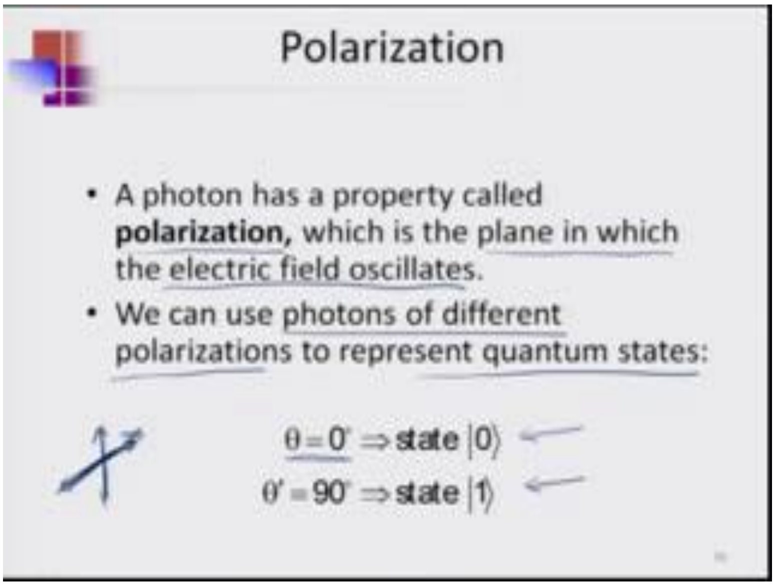
Photons

- **Physical qubits**
  - Any **subatomic particle** can be used to represent a qubit, e.g. an electron.
  - A **photon** is a convenient choice.
  - A photon is an **electromagnetic wave.**

One example which is very popular in this case is the case of photons, why? Because photons are quantum objects which can be transmitted very easily across, so these are the physical qubits where any subatomic particle can be used typically physical units can be any subatomic particle which can be use to represent a qubit. For quantum key distribution a photon is a convenient choice because, it can be transmitted very easily that is the basic idea.

The other kind of qubit that we have been encountered subatomic particles they are generally localized in somewhere, in the sense that whatever is happening in one area that you are looking at the subatomic particles interact and do things in a certain way, but transmission which is a key part in this quantum key distribution that would be preferred if you use a photon, and that is why photon is a convenient choice for quantum key distribution. Photons can be represented as electromagnetic waves where the quantum phenomena, is the part which will be utilized when we do our key distribution.

(Refer Slide Time: 06:25)



Polarization

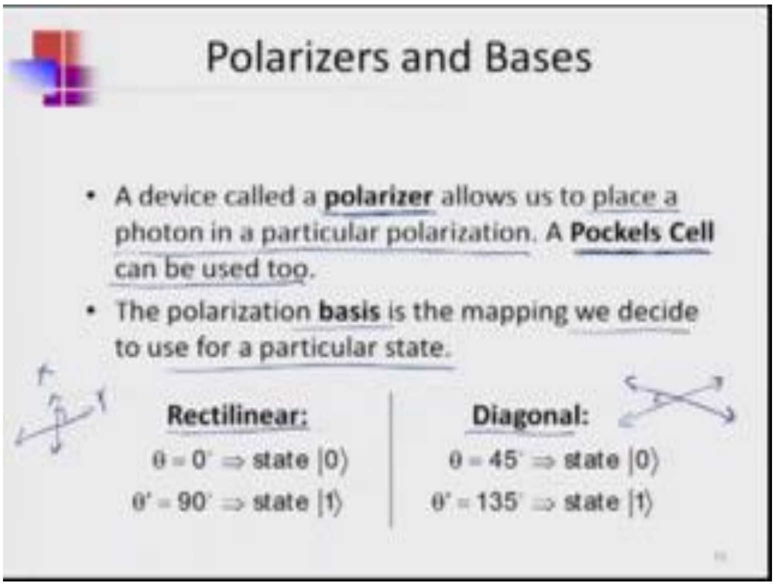
- A photon has a property called **polarization,** which is the plane in which the electric field oscillates.
- We can use photons of different polarizations to represent quantum states:

$\theta = 0^\circ \Rightarrow$ state $|0\rangle$

$\theta' = 90^\circ \Rightarrow$ state $|1\rangle$

Say photon has a property called polarization which is the plane in which the electric field is oscillating, right. So, we can use photons of different polarization to represents quantum sates. So, a photon with say having an angle or an oscillation in a certain way which we call as our 0 degree we can label at as state 0 and something which is 90 degrees to that state we can represent it as 1. So, for example, if this is my 0 then 90 degrees to it is my state 1.

(Refer Slide Time: 07:28)



Polarizers and Bases

- A device called a **polarizer** allows us to place a photon in a particular polarization. A **Pockels Cell** can be used too.
- The polarization **basis** is the mapping we decide to use for a particular state.

Rectilinear:

$\theta = 0^\circ \Rightarrow$ state $|0\rangle$

$\theta' = 90^\circ \Rightarrow$ state $|1\rangle$

Diagonal:

$\theta = 45^\circ \Rightarrow$ state $|0\rangle$

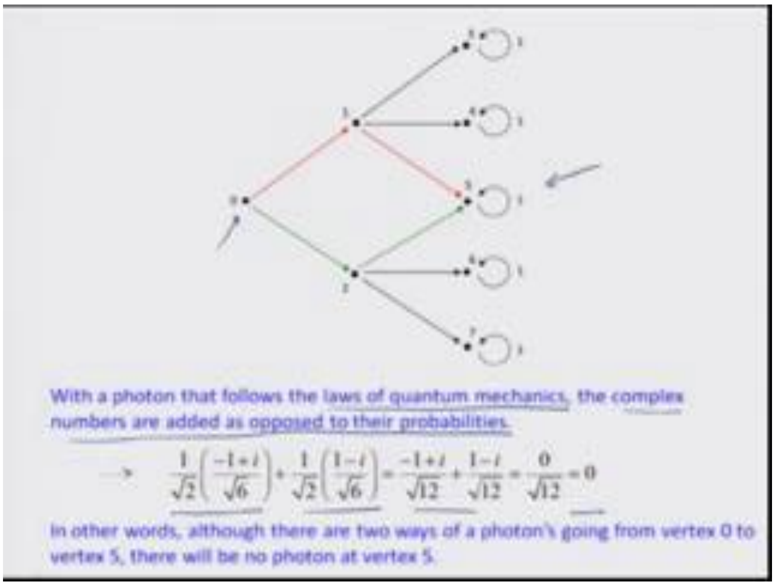
$\theta' = 135^\circ \Rightarrow$ state $|1\rangle$

So, that is the idea behind this definition and we can use this principle that it can oscillate in one way versus the other way as one of the approaches to deciding our quantum state. So, once we use polarization as our basis of qubit or a quantum state we need a device called a polarizer that will allow us to place a photon in a particular polarization, and there are things call pockels cells which are going to allow only certain polarizations to go through and it can be changed to the other kind based on applied field or voltages that is the idea where pockels cell is a material crystal which lets the light of a certain polarization to pass through under certain condition.

If you change the voltage across the pockels cell then the polarization property of the light going through it can be changed. So, that is a very nice way of changing the polarization states that are going through a medium. So, this is our manipulated in some sense. It could be a static manipulator like a polarizer which just sits there and does its job and the other could be a dynamic one which is like a pockels cell which depending on the voltage applied will change the way the polarization is going to be on the other side. So, the polarization basis is the mapping we decide to use for a particular state.

So, the simplest one that we are used to are the 0 and 90 case which is our rectilinear access geometric for example, x and y and the way we decide x y kind of thing; that is our rectilinear such that the angle across is going to be 90 degrees. The other option is to have a rotated case which will be like a diagonal such that the once again the angles are going to be 90 degrees, but they are with respect to a given fame can be rotated by 45 degrees. So, it could be their diagonal case or rectilinear case.

(Refer Slide Time: 09:56)



With a photon that follows the laws of quantum mechanics, the complex numbers are added as opposed to their probabilities.

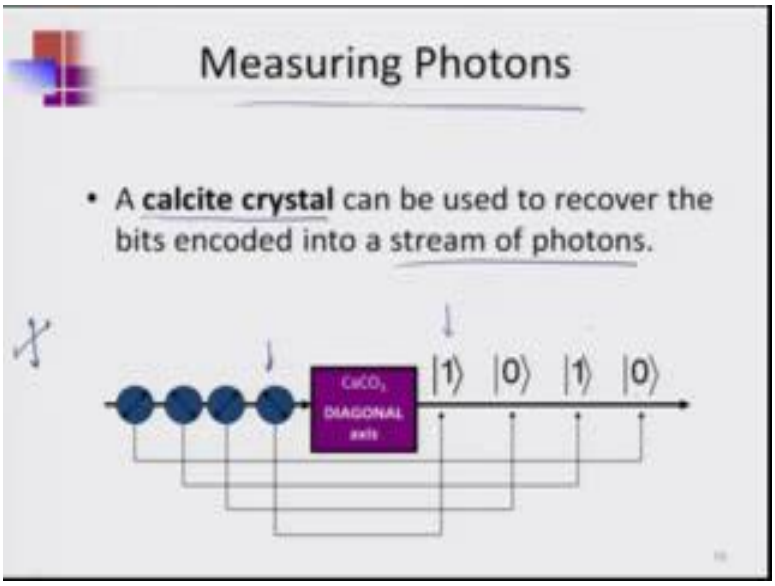
$$\rightarrow \quad \frac{1}{\sqrt{2}}\left(\frac{-1+i}{\sqrt{6}}\right)+\frac{1}{\sqrt{2}}\left(\frac{1-i}{\sqrt{6}}\right)=\frac{-1+i}{\sqrt{12}}+\frac{1-i}{\sqrt{12}}=\frac{0}{\sqrt{12}}=0$$

In other words, although there are two ways of a photon's going from vertex 0 to vertex 5, there will be no photon at vertex 5.

Since the photons are going to follow the laws of quantum mechanics the complex numbers are added as opposed to their probabilities; that is one of the things which we have been learning as a part of quantum mechanics. So, when the additions are happening in the quantum world the complex numbers come in to the picture, but when we are observing it, it is that probability that we are observing. So, here is an example as a result of this - we start at say 0.0 and you can go to different places under different conditions, but the design of the property if you are going to use this particular approach or propagation will be such that there will be no photon at say 0.5, right.

So, this is sort of known as annihilation operator that we are used to in quantum mechanics. That the phases are oppositely set such that the resultant can cancel each other, right. This can only happen because we are looking at their amplitudes and not their probability because the probabilities will not cancel out ever, they will have no signs associated with it, but these will have. So, that is the idea.

(Refer Slide Time: 11:33)



Measuring Photons

- A calcite crystal can be used to recover the bits encoded into a stream of photons.

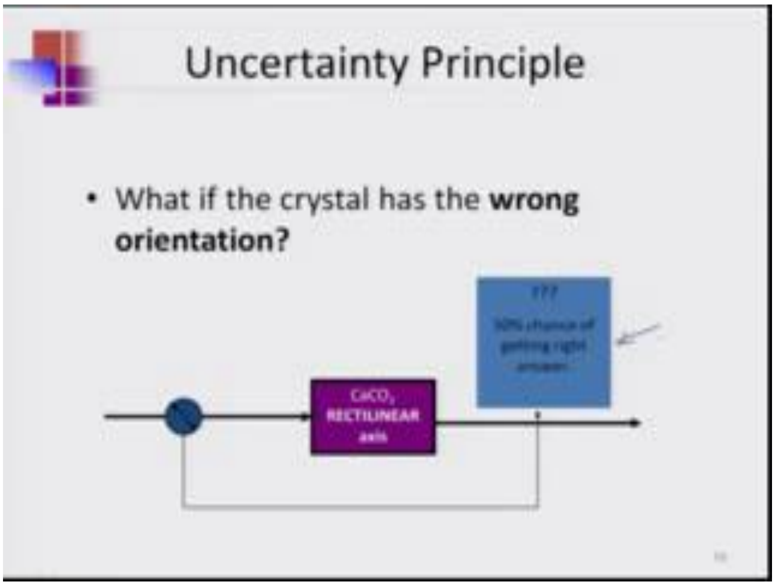
So, that was just an example now, in a realistic case what are you going to do. In order to measure photons and their polarizations one of the most important physical object is a calcite crystal. This can be used to recover the bits enclosed in a stream of photons. So, this is a non-centrosymmetric crystal, this is not a very uniform, optically it is not a 100 percent uniform crystal it has a non-centrosymmetric geometry and as a result of that when light passes through it, it interacts along the diagonal access and is able to allow one versus the other kind of the polarization coming through that is the main principle out here and in some sense therefore it is a polarizer.

So, what will happen? So, we can therefore correlate how they going to go across and be present as we go along this calcite crystal. So, if all the 4 possibilities of a diagonal polarization exist then as they go through it they will switch in to the cases that will considered into. For example, this diagonal axis of the calcite crystal will rotate 45 degrees to the incident polarization that we have.

So, therefore, this particular one will come out in a direction which we have defined as 1. We define 0 and 1, one coming out of the plane and one in the plane oscillating that is have it was. So, this is a two dimension representation of the actual thing. So, this one 45 degrees will give rise to 1, whereas the other one because it is going to rotate only in one direction and the other one will end up producing a 0. Similarly the other one which is again at 90 degrees to it will end up producing 1 and so on and so forth. So, you can get a series of different 0s and 1s in the plane that I am measuring because I am going to always rotate as a result of the calcite crystal by 45 degrees to a given angle that is the design.

So, you can actually set of the problem by aligning the crystal with respect to they applied polarization to start with, so that once you define one polarization as 0 then as soon as you rotate the other one the correspondence keeps on happening that is the idea.

(Refer Slide Time: 14:48)

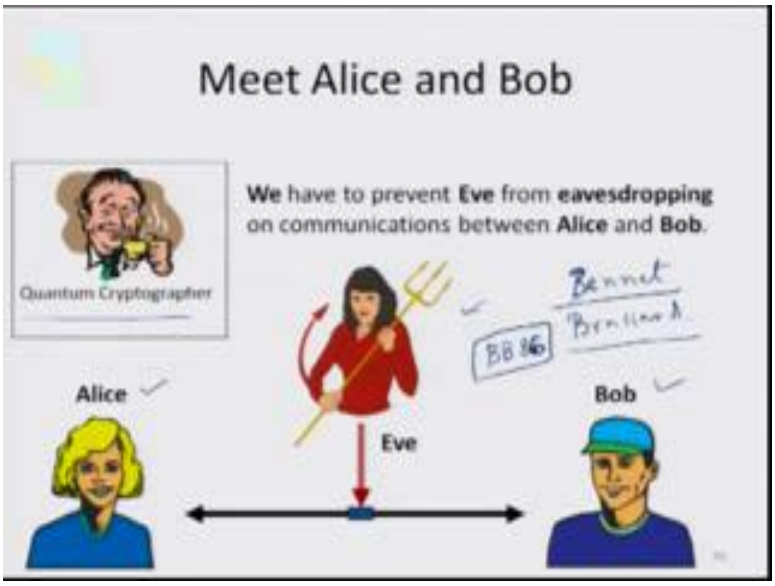


Uncertainty Principle

- What if the crystal has the **wrong orientation?**

Now, if instead of the case that I just mentioned to you where we are able to do the process the way we have done it. If we have wrong orientation what will happen that is the question - then there is a 50 percent chance of getting the right answer, because 50 percent of time you will get the right answer and 50 percent of time you will not get the right answer because there is always 50-50 probability of getting one way versus the other because there only two possibilities in this kind of case. We are either 0 or 1, so if you get it wrong it will be 50 percent wrong, if you get it right it will be 50 percent right.

(Refer Slide Time: 15:33).

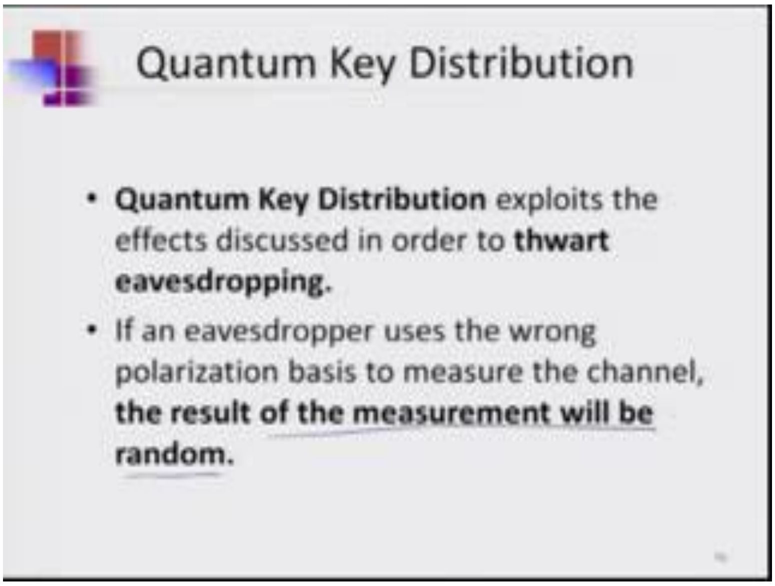


Meet Alice and Bob

We have to prevent **Eve** from **eavesdropping** on communications between **Alice** and **Bob**.

So, in this design the way it was we discussed it last time also - when we are going to send information across it is like having Alice and Bob trying to send the information across and there is a eavesdropper who is going to come in, to try to see if the information can be stolen that is the basic idea. So, what is the job of the quantum cryptographer? He or she has to prevent Eve from eavesdropping on communication between Alice and Bob that is idea. So, this is the famous problem which is first proposed and described well in quantum information theory by Bennett, Charles Bennett and later on he is associate Brassard we will have the names again later on; added to the levels of cryptography that can be done and so there are codes which go by their names. So, there are these two names. So, these are basically BB and they used certain number of parameters to do their things. So, there is this famous code called BB 86 coding. So, it is Bennett and Brassards thing it is 1986 when they did it and that is how (Refer Time: 17:11) BB 86, but we go ahead and see how it is going.

(Refer Slide Time: 17:14)

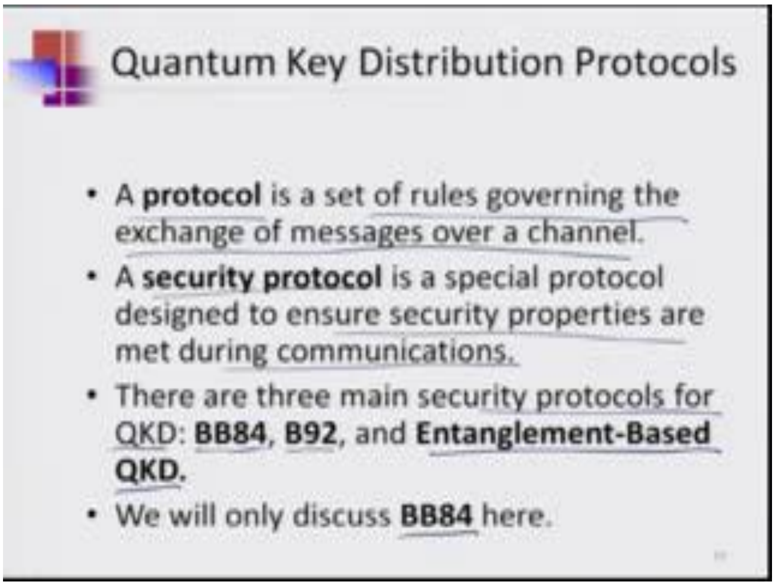


Quantum Key Distribution

- **Quantum Key Distribution** exploits the effects discussed in order to **thwart eavesdropping.**
- If an eavesdropper uses the wrong polarization basis to measure the channel, **the result of the measurement will be random.**

So, what are these steps? It requires as we mentioned quantum key distribution which exploits their effects discussed in order to thwart the eavesdropper. If an eavesdropper uses the wrong polarization basis to measure the channel, the result of the measurement will be random, 50-50 means random.

(Refer Slide Time: 17:40)



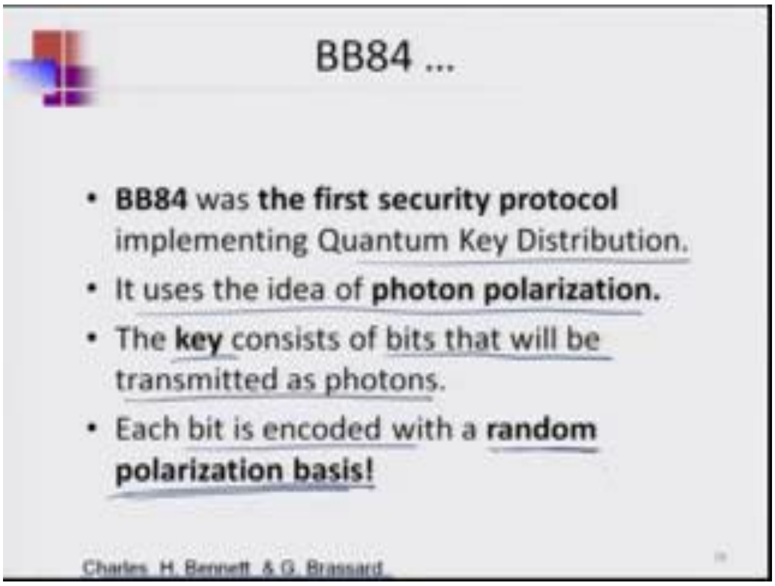
Quantum Key Distribution Protocols

- A **protocol** is a set of rules governing the exchange of messages over a channel.
- A **security protocol** is a special protocol designed to ensure security properties are met during communications.
- There are three main security protocols for QKD: **BB84**, **B92**, and **Entanglement-Based QKD.**
- We will only discuss **BB84** here.

The protocols are important parameters here, a protocol is a set of rules governing the exchange of messages over a channel unless you set it up you will have difficulty in getting to know how information transfer we will happen. So, a security protocol is a special protocol designed to ensure security properties are met during the communications.

There are three main - it was not 86, it is BB84. There are three main security protocols for QKD BB84, B92 and Entanglement-Based QKD. So, we will only discuss BB84 here. So, that is the reason I introduced you earlier I am sorry this was 84, so this correct it here.

(Refer Slide Time: 18:45)



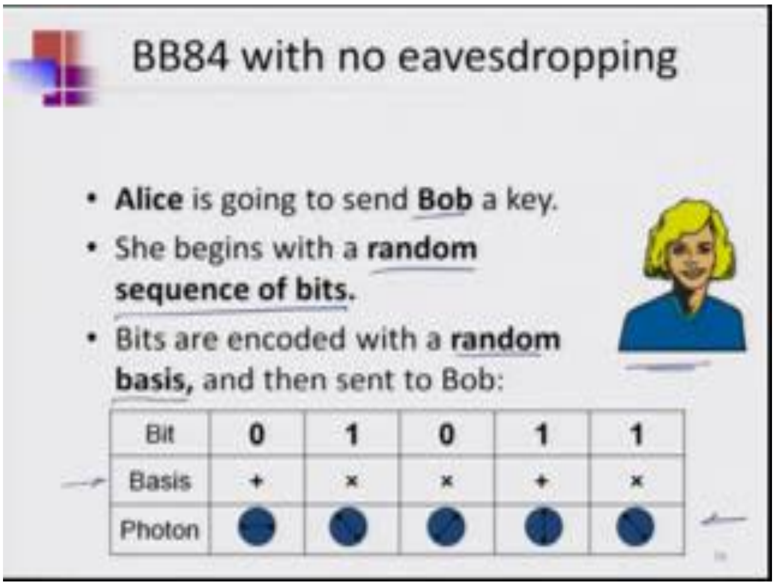
BB84 ...

- **BB84** was **the first security protocol** implementing Quantum Key Distribution.
- It uses the idea of **photon polarization.**
- The **key** consists of bits that will be transmitted as photons.
- Each bit is encoded with a **random polarization basis!**

Charles H. Bennett & G. Brassard

So, BB84 was the first security protocol implementing quantum key distribution this uses the idea. So, as I mention this Charles H Bennett and G Brassard. It uses the idea of photon polarization the key consists of bits that will be transmitted as photons. Each bit is encoded with the random polarization basis, now that is the main important thing - the random polarization basis, will come to it in a minute.

(Refer Slide Time: 19:20)



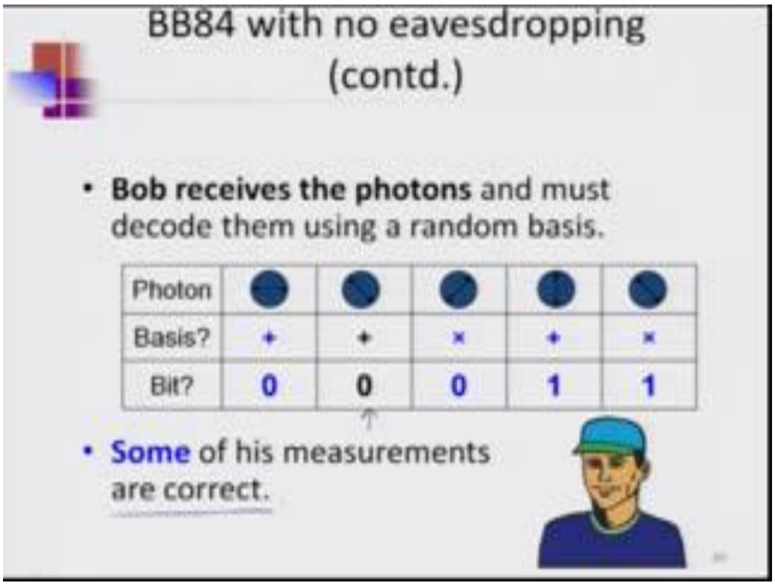
BB84 with no eavesdropping

- **Alice** is going to send **Bob** a key.
- She begins with a **random sequence of bits.**
- Bits are encoded with a **random basis,** and then sent to Bob:

Bit	0	1	0	1	1
Basis	+	×	×	+	×
Photon	⊖	⦸	⊘	⦶	⦸

So, when there is no is eavesdropping how is it going to work? So, the sender Alice is going to send Bob the key, she begins with a random sequence of bits, bits are encoded with a random basis and then sent to Bob. So, the basis can be something like plus cross cross plus cross. So, cross is 0 plus is 1 let us say. Now accordingly you will get your coding done in a certain way for the photons and you get this kind of a resultant.

(Refer Slide Time: 20:14)



BB84 with no eavesdropping (contd.)

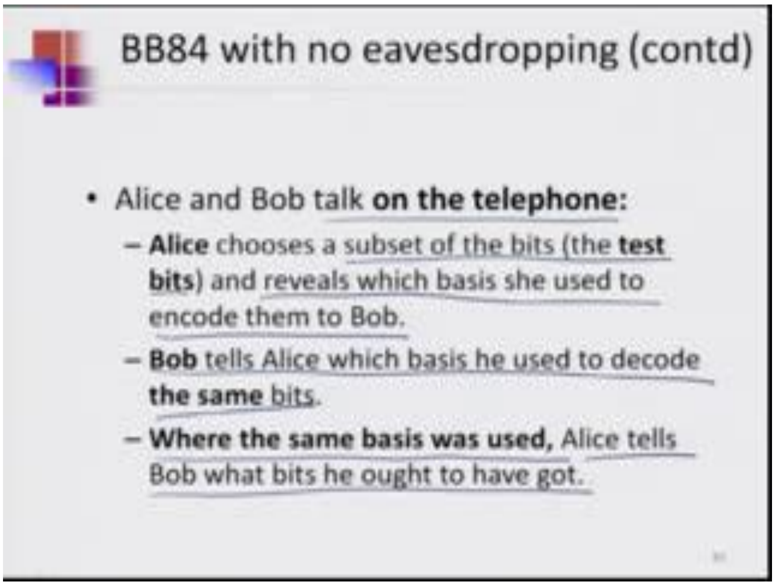
- **Bob receives the photons** and must decode them using a random basis.

Photon	⊖	⦸	⊘	⦶	⦸
Basis?	+	+	×	+	×
Bit?	0	0	0	1	1

- **Some** of his measurements are correct.

Now when Bob receive the photons and must decode them using a random basis some of his measurements are only going to be correct, why? Because there is a possibility of getting them correctly and he uses a basis in which let us say one of his basis does not match up with what was used by Alice and so instead of getting the right numbers there was a place where the right number did not come through. So, some are corrects some are not.

(Refer Slide Time: 20:51)

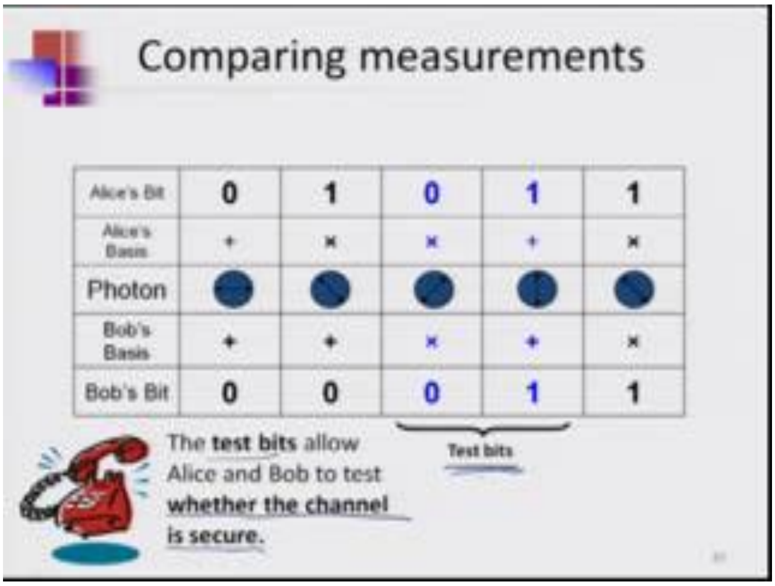


BB84 with no eavesdropping (contd)

- Alice and Bob talk **on the telephone:**
  - **Alice** chooses a subset of the bits (the **test bits**) and reveals which basis she used to encode them to Bob.
  - **Bob** tells Alice which basis he used to decode **the same** bits.
  - **Where the same basis was used,** Alice tells Bob what bits he ought to have got.

So, then what happens? Alice and Bob talk on the telephone because; there is no eavesdropper so you do not need to worry about this. Alice chooses a set a subset of the bits, the test bits and reveals which basis she used to encode them to Bob. So, this is basically hand shaking this is the beginning part you are testing it out. So, Bob tells Alice which basis he used to decode the same bits, where the same bits basis was used Alice tells Bob what bits he ought to have got. So, this is like they are checking their results on whatever they have done and trying to find out what went true what was going on.

(Refer Slide Time: 21:43)



Comparing measurements

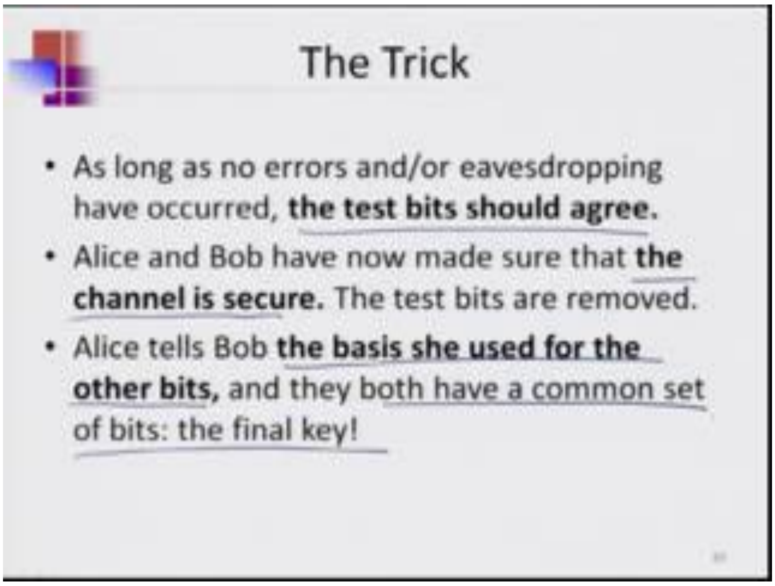
Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon	↔	↘	↗	↕	↘
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits

The **test bits** allow Alice and Bob to test **whether the channel is secure.**

So, when they do the comparing of the measurements they find that two of the basis of all the set that was used where correct where matching, so they call that as test bits. So, once this test bits is established then Alice and Bob can actually exchange information where the test bits are included to be able to test if the channel is secure. Because if somebody tampers with this message the parts which are not in the test bit it does not matter because, that is not going to actually affect anything. But once you keep on sending the information somewhere along the line the test bit will also be having an effect, so if that happens then they know that the channel is corrupted otherwise it is secure.

(Refer Slide Time: 22:50)



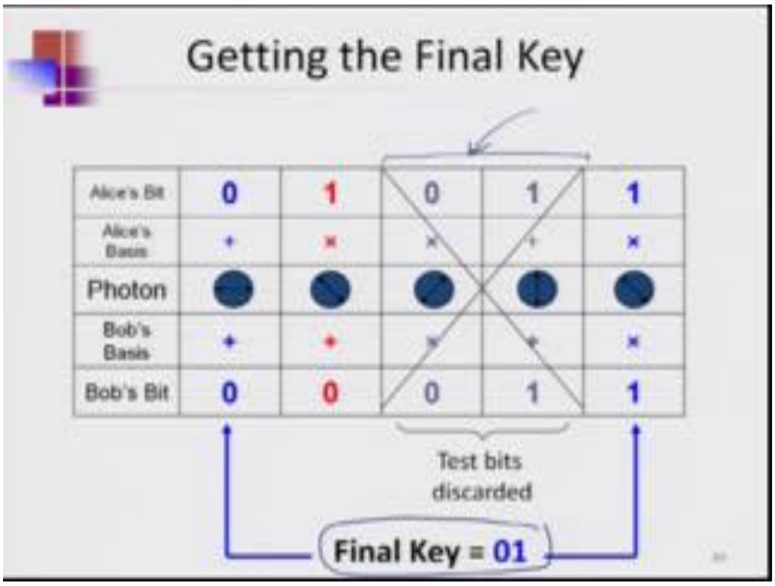
The Trick

- As long as no errors and/or eavesdropping have occurred, **the test bits should agree.**
- Alice and Bob have now made sure that **the channel is secure.** The test bits are removed.
- Alice tells Bob **the basis she used for the other bits,** and they both have a common set of bits: the final key!

So, where is trick? As long as no errors and no eavesdropping have occurred, the test bits should agree every time. Alice and Bob have now made sure that the channel is secure the test bits are removed, Alice tells Bob the basis she used for the other bits and they both have a common set of bits: the final key!

Now, you can actually imagine this iterative process going on for a very long time such that you can actually send across a 256 bit key, imagine what will happen, how long it will take to do all of this, but that is one possibilities. There you can do it step by step to see what happens.

(Refer Slide Time: 23:35)



Getting the Final Key

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon	●	●	●	●	●
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

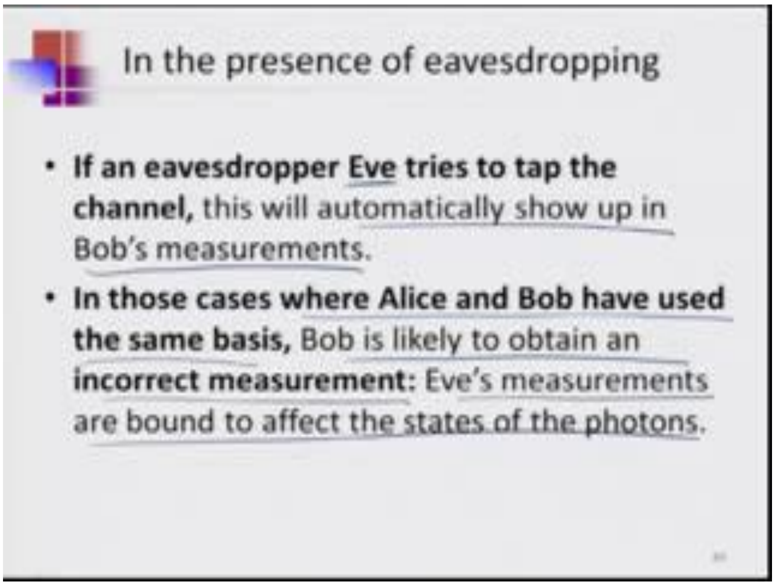
Test bits discarded

Final Key = 01

So, for example, here with this particular set how do you get the final key? What you have to do is you have got this region where the test bits where there you discard them and what you find then is that there were these two which still matched, in spite of the fact that they were not using them as their test bits still they match. So, they considered that as a final key.

So, even if somebody is actually sitting they are trying to figure out what is the security channel they will end up getting this which is the discussion bits the test bits as the security channel is that is what they are been discussing. So, in other words you know the phone conversation is classical for example. So, somebody manages to hear the phone conversation, so they will focus on getting this as the answer right, because that is the discussion point they had the test bits. But they really do not use the test bits, they discarded and then look for the once where the thing worked and that they considered as their final key.

(Refer Slide Time: 25:06)



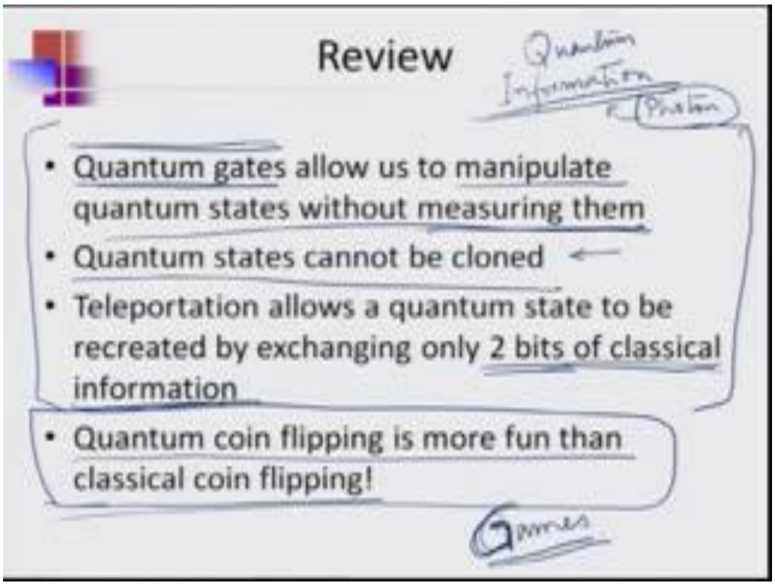
In the presence of eavesdropping

- **If an eavesdropper Eve tries to tap the channel,** this will automatically show up in Bob's measurements.
- **In those cases where Alice and Bob have used the same basis,** Bob is likely to obtain an **incorrect measurement:** Eve's measurements are bound to affect the states of the photons.

Now, this is without having any eavesdropper with assumption that you know when everything happened ideally there was nobody who was listening, so they went through the exercise as if there was going to be something happening, but nothing was there and s they were able to get their answer very easily. Had it been that there was eavesdropping what would have happened? So, see eve if there is an eavesdropper and he is trying to tap the channel this will automatically show up on Bob's measurement. In those cases where Alice and Bob have used the same basis Bob is likely to obtain an incorrect measurement eve's measurements are bound to affect the states of the photons and that is the beauty of quantum part here. Had it been classical, this was not going to be reflected.

Because in a classical system you can always take a little bit out and nothing happens, but in a quantum system that is what you have learnt all this time. Any kind of a (Refer Time: 26:21) or a change or as you call it measurement which is interaction is going to affect whatever is left and that is the reason the places where they were having the correct match is now going to have an incorrectness and that is how they will immediately know that there was an eavesdropping.

(Refer Slide Time: 26:47)



Review

Quantum Information

Photon

- Quantum gates allow us to manipulate quantum states without measuring them
- Quantum states cannot be cloned
- Teleportation allows a quantum state to be recreated by exchanging only 2 bits of classical information
- Quantum coin flipping is more fun than classical coin flipping!

Games

So, the advantage therefore is the quantum gates allow us to manipulate quantum states without measuring them as the first thing which is very important, because that is the basic principle behind quantum gates. So, this is actually I do not know if I mentioned it before, but this is something which will have to be always focusing on; that the reason for having quantum gates is that we will be able to manipulate the quantum states without measuring them.

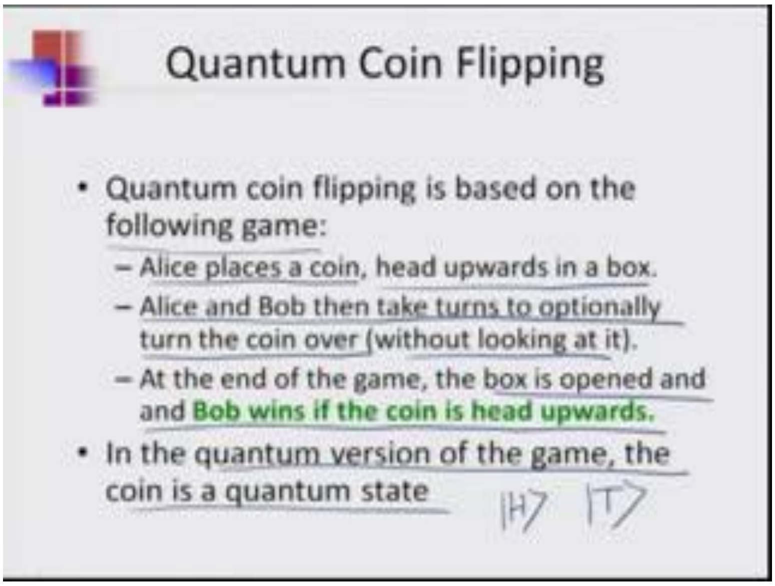
So, the definition of a quantum gate is right there and that is why they are sometimes very difficult to come up with. Quantum sates cannot be cloned, now that again one of the things which you know as this is a property of quantum mechanics. Teleportation allows quantum states to be recreated by exchanging only 2 bits of classical information. Now this is the part which is very important. So, at the end of the day what happen was, they only exchanged 2 bits, which was their test bit to be able to know what was going on with the entire information transfer process. They did not use anything else.

Quantum coin flipping is more fun than the classical coin (Refer Time: 28:03). There are many other aspects of quantum information processing and one of them is also quantum coin flipping because that has much more probability then doing a classical coin flipping and that is how it can be more fun than the classical coin flipping, but I do not know whether I will be doing that next or out let me see; we are doing that next.

So, before I go there let me actually just do a quick review on what was the main process here in terms of quantum information processing. So, this part of the presentation or the classes that we have done has focused more on the quantum information processing. You have to understand one very important part of quantum computing per say that this quantum computing heavily realize, if realize heavily on quantum information. So, you cannot have quantum computing or anything to do close to it unless you have quantum information process in done in the right way. So, information processing or quantum information processing is some very important place where photons or light plays a very important role because they are the once which can be transmitted across much more easily than anything else any other quantum or qubit that you can think of, photons are the best in terms of transferring and therefore, quantum information will almost always have photons as a part of its study.

So, this is one thing which we have done, so basically studied this. Now to make things a little bit more friendly let us say, we will be looking at the quantum coin flipping kind of a situation. There is this entire area which is known as quantum games and its definitely lot more interesting to do a quantum game versus the regularly game because, it is a matter of chance right and you know that matter of chance is much much better off with the quantum system then with the classical systems. So, that is why it is the more much more interesting case. So, what do we mean by quantum coin flipping?

(Refer Slide Time: 31:05)



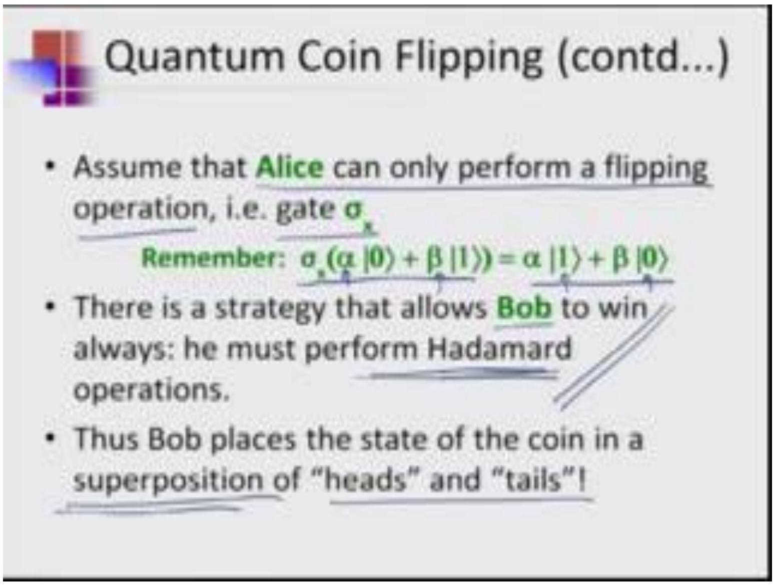
Quantum Coin Flipping

- Quantum coin flipping is based on the following game:
  - Alice places a coin, head upwards in a box.
  - Alice and Bob then take turns to optionally turn the coin over (without looking at it).
  - At the end of the game, the box is opened and and Bob wins if the coin is head upwards.
- In the quantum version of the game, the coin is a quantum state $|H\rangle$ $|T\rangle$

So, the quantum coin flipping principles is based on the following game. So, again this Alice and Bob kind of an idea - Alice places a coin head upwards in a box, Alice and Bob then take turns to optionally turn the coin over without looking at it that the key part.

If you look at it then it has becomes classical information you cannot do that, at the end of the game the box is opened and Bob wins if the coin is head upwards otherwise Alice wins. In the quantum version of the game the coin is a quantum state. So, when we say heads or tails these are classical, but if I say H state and T state then it is a quantum system.

(Refer Slide Time: 31:59)



Quantum Coin Flipping (contd...)

- Assume that Alice can only perform a flipping operation, i.e. gate σ_x

  Remember: $\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$
- There is a strategy that allows Bob to win always: he must perform Hadamard operations.
- Thus Bob places the state of the coin in a superposition of "heads" and "tails"!

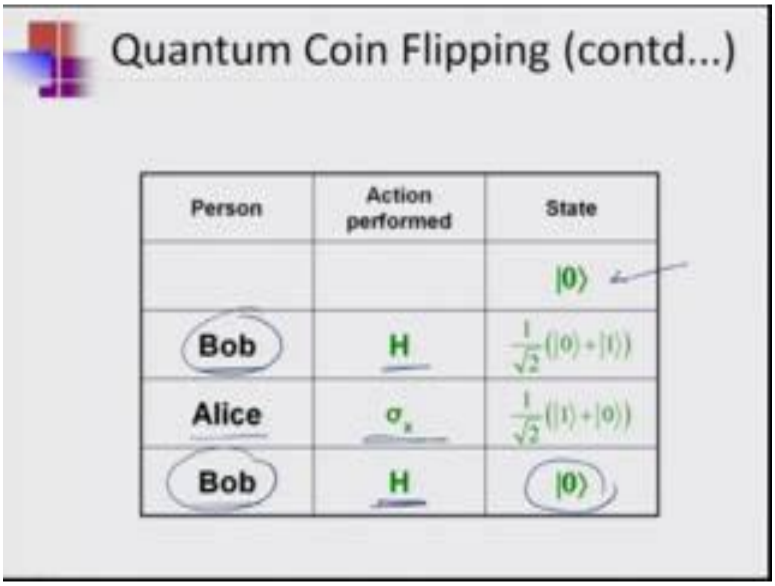
Now for those of who might be thinking that why this is so exciting because this is this is related to your security in terms of tailor machines banking, so will come to that.

So, quantum coin flipping, in this case let us formalize it in a slightly more regress fraction let us say that Alice can only perform a flipping operation that is a gate which is sigma x. We know that the sigma x just does a flip. So, what does sigma x do? It takes the super positions and puts them in the opposite order. So, the alpha becomes associated with one and the beta becomes associated with 0 (Refer Time: 32:58). There is a strategy that allows Bob to win always he must perform Hadamard operation. So, now, that is the very important principles, this means that if you do it in this fashion there is a strategy which can be used by Bob which will make him always win if he does that.

So, thus Bob places the strategy of the coins in a superposition of heads and tails because in order to get to the Hadamard operations you need to have a superposition of the two states. So, I think we have gone through cases where we have discussed before that there were some gates, some processes, some discussions of quantum principles which allowed us to make super positions states, they are actually very very important. There are some resent works that we have also done in terms of research where we have actually shown that creating superposition states are possible say in optical qubit and things and they are very very important because that is one of the principles of Hadamard gates.

And Hadamard gates or Hadamard operations not just appearing in only these cases they appear in almost everywhere, you will also find that they appearing robust algorithm and there often there in even in parts of doing this (Refer Time: 34:26) sorry the shors algorithm. So, let us see what we do here.

(Refer Slide Time: 34:31)



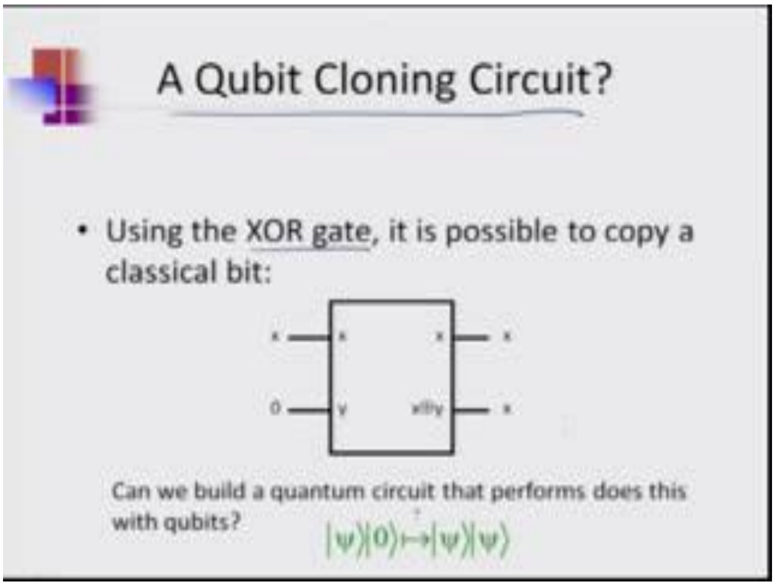
Quantum Coin Flipping (contd...)

Person	Action performed	State
		$\|0\rangle$
Bob	H	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$
Alice	σ_x	$\frac{1}{\sqrt{2}}(\|1\rangle+\|0\rangle)$
Bob	H	$\|0\rangle$

So, here in this coin flip experiments what you have to do is you have the Bob who is going to do his Hadamard operations on the original state, Alice is going to do a flip and once again Bob does a Hadamard to find out what the original state was.

So, that is what Alice just say that if Bob keeps on doing Hadamard he finally, always wins because the flip character will be always seen correctly by Bob every time he does a flip, so that is one part. The next very important thing which I mentioned which is again a difficult one is the cloning right.

(Refer Slide Time: 35:14)



A Qubit Cloning Circuit?

- Using the XOR gate, it is possible to copy a classical bit:

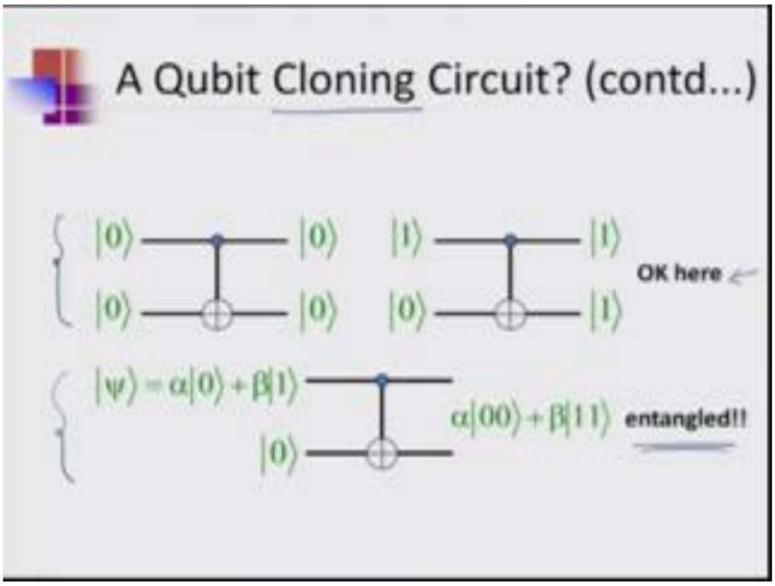
Can we build a quantum circuit that performs does this with qubits? $|\psi\rangle|0\rangle \overset{?}{\mapsto} |\psi\rangle|\psi\rangle$

Because these are the things which we have to be looking at over and over again because, these are the places which are otherwise very difficult to do in a quantum system. So, the idea of a quantum or a qubit cloning circuit is very important. So, why are we doing all this we are doing it because these are essential steps towards providing a full quantum teleportation circuit. So, will find it out later that all these different steps that we are doing see for example, the quantum coin flipping that we just did is one of the steps that is always necessary when we are finally, going to do our quantum teleportation process. So, this is one phase.

The other important thing we need to do in this connection is to actually have a cloning. So, how do you cloning? We have perhaps visited it once before, but let us do it once more in this context because we would need it.

So, a qubit cloning circuit is something which we need, which we know that it is very difficult to get otherwise, because in quantum mechanics you cannot clone anything, but we know for example, in classical case you can always do that. For instance by using a reversible XOR gate it is possible to copy a classical bit. By using the same analogy because it is a reversible case in case of classical we should be able to do the same in the classical. So, here we are looking at it. Can we build a quantum circuit that performs with this kind of a situation with qubits, is it possible?

(Refer Slide Time: 37:10)

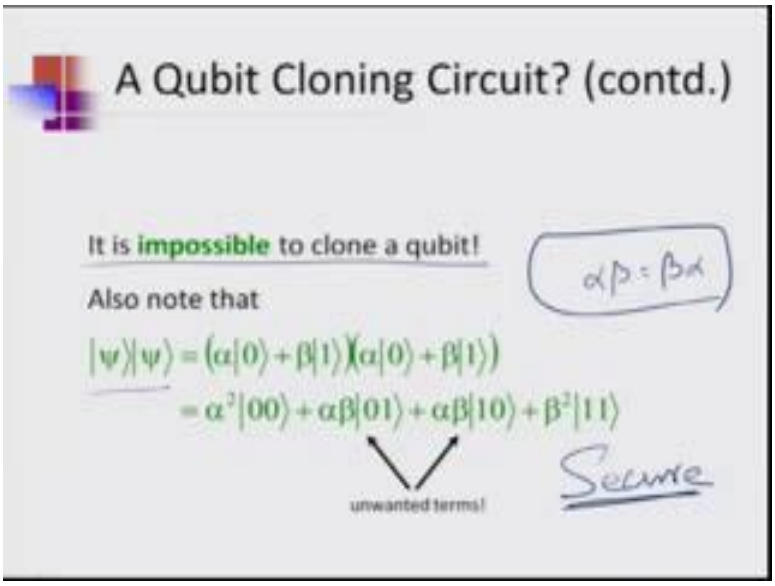


A Qubit Cloning Circuit? (contd...)

$|0\rangle$ $|0\rangle$ → $|0\rangle$ $|0\rangle$
$|1\rangle$ $|0\rangle$ → $|1\rangle$ $|1\rangle$
OK here
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$|0\rangle$
$\alpha|00\rangle + \beta|11\rangle$
entangled!!

So, what is the idea? A qubit cloning circuit would therefore, be meaning that will have to do something which will be utilizing one principle or the other. So, if you take pure states then it is possible to do such things right; however, if you have states which is super position states this it is not that simple, what you will have is you will end up producing and entangled states. So, in order to actually clone all the time it is not possible to just say that - OK, I will just use the same principles that have been used in a reversible classical system, it is not true. So, the reason I wanted to make this point clear here is that many a times you may think that if I take a perfect reversible classical computer I should be able to do this same now, take it and just map it in to my quantum computer, map it in to the quantum world and I get a quantum computer, it is not going to happen, it is not that way.

(Refer Slide Time: 38:31)



A Qubit Cloning Circuit? (contd.)

It is impossible to clone a qubit!

$\boxed{\alpha\beta = \beta\alpha}$

Also note that

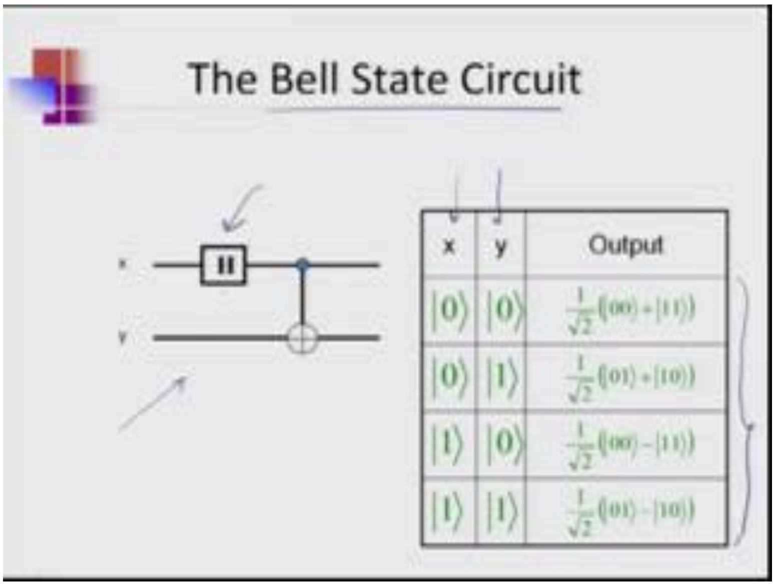
$$|\psi\rangle|\psi\rangle = (\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle)$$
$$= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

unwanted terms!

Secure

So, a direct mapping is not the idea between classical and quantum something more is necessary the idea is correct, it somewhere there but it is not exact. So, we have to do something more, what is it. So, in this case for example, first statement is it is impossible to clone in qubit that we know there is nothing new about it, but there is a way to do this in a slightly different way, but we should note that when we take any two states which has superposition states we will be getting terms which we just discussed which where entangle that is because, in quantum systems alpha beta is not equal to beta alpha that is typically the case, you cannot just; because most of the time they are also complex numbers and so complex numbers are not going to be often looking like this. So, in that case you have to do something more than that and Hadamard Gates again become very important.

(Refer Slide Time: 39:17)



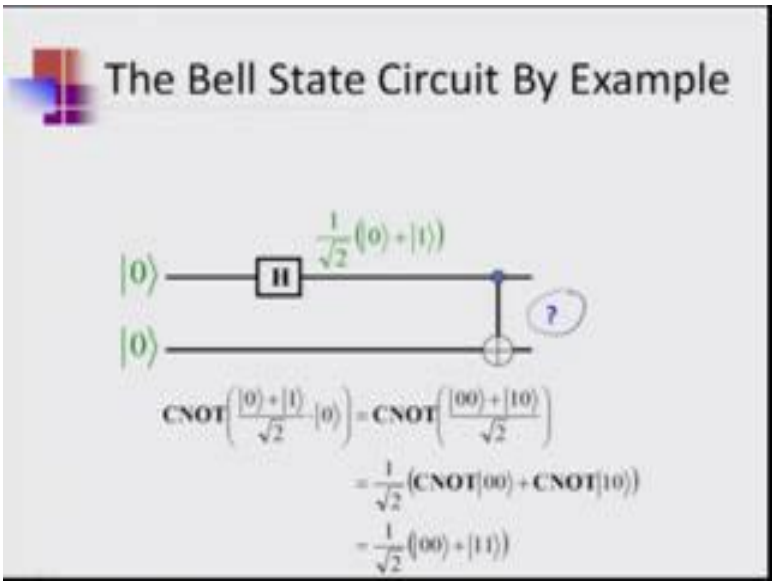
The Bell State Circuit

x	y	Output
$\|0\rangle$	$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$
$\|0\rangle$	$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle+\|10\rangle)$
$\|1\rangle$	$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$
$\|1\rangle$	$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)$

So, in this connection let us actually look at the bell state circuit now we have encountered bell state before hand, where we have taken states and put them together and we found out that these bell states cannot be separated back down to the individual states, so that was the basic idea. So, we have just seen in similar condition here we ended up producing entangle states.

So, if you take this kind of a circuit what you will end of producing depending on how you have your inputs states. The output will essentially form the entire bell state situation. So, just a simple Hadamard along with the CNOT gate will end up producing the bell states that you need. So, this is the bell states circuit. So, here is an example how it goes.

(Refer Slide Time: 40:24)

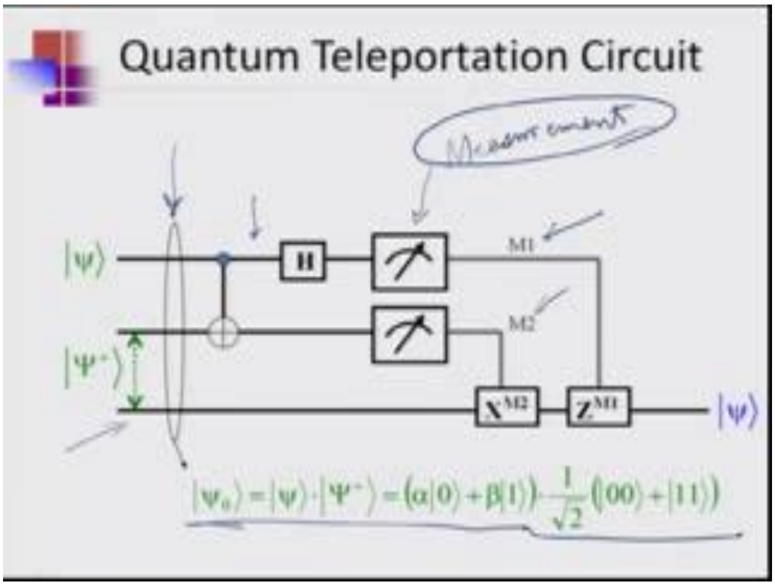


The Bell State Circuit By Example

$$\mathbf{CNOT}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle\right)=\mathbf{CNOT}\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right)$$
$$=\frac{1}{\sqrt{2}}(\mathbf{CNOT}|00\rangle+\mathbf{CNOT}|10\rangle)$$
$$=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

So, you start with the same state one of them goes to a Hadamard, so it becomes reposition states. It is going to the CNOT producing the bell state here. So, this is my bell state then.

(Refer Slide Time: 40:47)

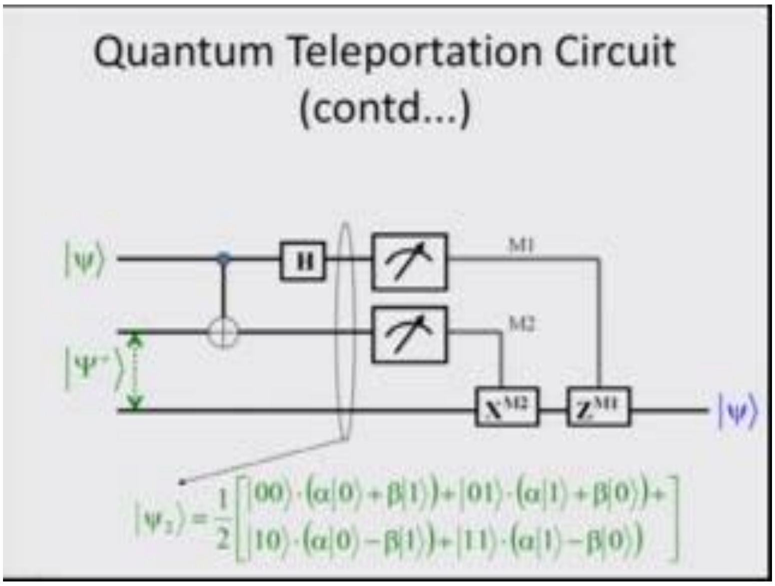


Quantum Teleportation Circuit

$$|\psi_0\rangle=|\psi\rangle\cdot|\Psi^{+}\rangle=(\alpha|0\rangle+\beta|1\rangle)\cdot\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

In order to get to your quantum teleportation circuit all of this that we discussed as of now are necessary, why? By the way I should mention that this symbol represents measurement. Whenever we have a symbol we sort of shows a meter of some sort it means we are looking at a measurement point. So, what is it that we have doing now we are actually having one state say for example, the particular (Refer Time: 41:25) function is been put through a control not with control bits which are of certain kind which is going to go through this system where one of the cases can be a measurement case. But the other case we are not measuring, if you measure in the other case then we in trouble we are only measuring one part of it. So, these are my measurements M1 and M2 and if you remember we always say that we will be using two qubits on the classical channel which is the case where we allowed the measurement to happen, but the other one which was my quantum case remained as it is. It just got some kind of a mixture or it got sort of impacted by these other states to finally give rise to state that is of use.

(Refer Slide Time: 42:25)



Quantum Teleportation Circuit (contd...)

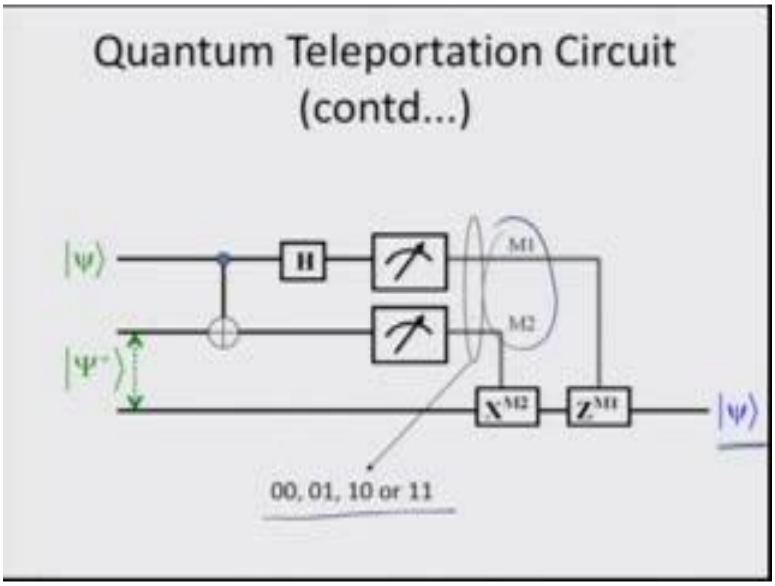
$$|\psi_2\rangle = \frac{1}{2}\begin{bmatrix} |00\rangle\cdot(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\cdot(\alpha|1\rangle+\beta|0\rangle)+ \\ |10\rangle\cdot(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\cdot(\alpha|1\rangle-\beta|0\rangle) \end{bmatrix}$$

So, we look at it in a slightly more difference way, so at each point how does it look? So, here as we entered, so this is another way of. So, whenever we write down circuits at every point when we look at it we kind of put a circle and then we represent what we are seeing right there. So, my psi naught is a resultant of the interaction which is happening at this point of my circuit right. So, this is how I have look at it, this is how it looks.

Now what happens when I go this point? So, this is how the second point would look like. One of them go through the CNOT, the other one is already is as we had seen before. So, this part now is going to go through a CNOT on the one part. So, this part is going to go through a CNOT, this part we have already computed. So, when we apply that we get this. So, this is how it looks like here. Now at next one will be having a

Hadamard on one of them and so when I apply the Hadamard after this point then this is my resultant and then you will be measuring.

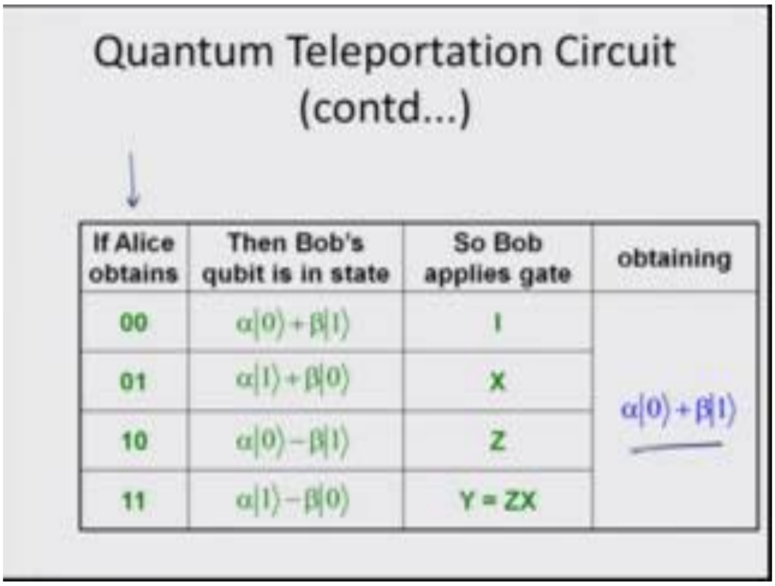
(Refer Slide Time: 43:41)



Quantum Teleportation Circuit (contd...)

And you will be measuring these which are basically the bell states, between two qubits. Actually these are basically the two qubits different possibilities of the two qubits being measured.

(Refer Slide Time: 43:58)

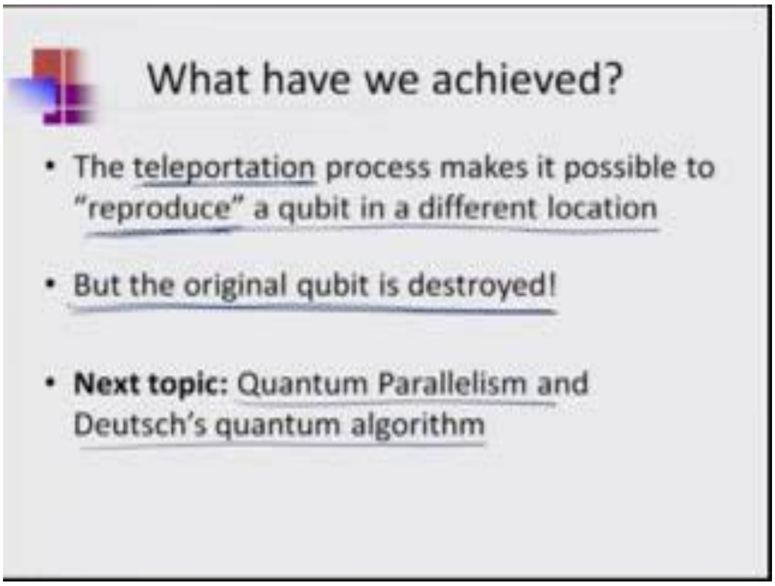


Quantum Teleportation Circuit (contd...)

If Alice obtains	Then Bob's qubit is in state	So Bob applies gate	obtaining
00	$\alpha\|0\rangle+\beta\|1\rangle$	I	$\alpha\|0\rangle+\beta\|1\rangle$
01	$\alpha\|1\rangle+\beta\|0\rangle$	X	
10	$\alpha\|0\rangle-\beta\|1\rangle$	Z	
11	$\alpha\|1\rangle-\beta\|0\rangle$	Y = ZX	

Now that measurement is essentially what Alice has done (Refer Time: 44:06). So, that measurement is essentially what Alice is done (Refer Time: 44:12) because she prepared her condition there. This is how she prepared this the states; she measured before sending it out. And see she got these conditions and as a result of that when it is going to be looked at by Bob then Bob's qubit states will be one of the kinds and when Bob applies any of these states then he will be getting this particular state generated which is the psi states refine and re-function.

(Refer Slide Time: 44:50)



What have we achieved?

- The teleportation process makes it possible to "reproduce" a qubit in a different location
- But the original qubit is destroyed!
- **Next topic:** Quantum Parallelism and Deutsch's quantum algorithm

So, what have we achieved as a result of all this? The teleportation process makes it possible to reproduce a qubit in a different location let us look back. So, the qubit started off here which was my psi function which was this original state. Then, see that was my psi, psi was superposition of 0 and 1 with alpha and beta, then I went through this circuit and I looked at every possibility right there and when the final measurement was done by Alice correspondingly what Bob got as a result of applying these gates is the same state which Alice had.

So, what is the result the teleportation process makes it possible to reproduce, he started off by saying you cannot clone the quantum state right, that was the basic idea. But we ended up managing to do that by using this teleportation process and that is why it is teleportation; it is not cloning but teleportation, this is not at the same location. And the original qubits are destroyed, because once Alice has done this the measurements are done those qubits are no longer there. So, that is the reason why we have to make this statement with the original quibits are destroyed.

The next topic is on quantum parallelism and Deutsch’s quantum algorithm which will do it in the next class, but before going there I think what we did today is extremely important. So, I am going to do once more revise this once more because, now we have seen the whole thing. So, we should be able to understand it little bit better when we were doing it by steps. So, let me actually go back on this a little bit to make sure that we understand because, we did the steps without originally understanding why we wanted to do those steps.

Now, that you have seen how this is all happen we are going to do this once more in a little bit fast manner, but just see. So, essentially there was a lot of background which we have already done to just show you that they have analogs in other information processing. So, the quantum coin flipping was for example, an analog. So, you can use this in terms of some games and other things, but this was a step in the process of quantum teleportation please remember that. So, it was not like we were trying to play games and anything here. It is true that there is a huge area quantum game theory it is there in our (Refer Time: 48:06), it is very interesting and you can even think in term of quantum casinos and discuss about those things.

We can have a discussion on all of that, but the basic original problem was that you have eavesdropper and you are wanting to have a secured channel between two individuals were going to transmit information and if it is a quantum information what we claimed was that it will be 100 percent secure, how is that going to happen. So, in this regard we went through all the steps which showed how this is possible. And we used photons in this case preferentially, because photons are much better in terms of transmission of information in quantum sense. So, use photons and photons are very convenient two states polarization of one kind process the other kind, we use that and we made a parallel with the classical 2 bit system and we use that as an information bit to exchange.

And in this we also explored the possibilities of something like a quantum coin flip and we found out that we could use that principle to understand how Alice can make the measurement or can set up the problem which can be always recovered by Bob with 100 percent outcome which is very important had it been not that way then this entire exercise would have stop right there we did not want to do it that way, we want to do it that way.

So, we found out how the coin flip in principles are. Once we understood that we put it through in a circuit fashion and we ask the question as to whether it is possible to clone which definitely is not possible because, we know that in a classical system which possible, but in quantum system is not. But in some sense we realize that this teleportation business might have something to do with this in that connection and we started asking the question where we landed up with the idea that in very simple cases it is possible that you can use simple control NOT gates to get to the principle that you are able to perhaps get back the same system, but that is true only if you use pure states or single states to start with.

But if they are starting with combination state 0 and 1 being combined in some percentage order which is how a typical quantum state is then you always end up getting entangle states, we will not be able to get the individual states in the right order as we have started and so the principle of cloning that it cannot be done in reality survive which is required for a quantum system and that is the security by the way, right. So, we basically proof the fact of the principle and it was important because that makes it secure. So, that is our secure, it is very important, right. So, then once we went there then we started to ask or re-explode the idea that we have already talked about before is the idea of the bell state which we know we have discussed in terms of entanglements earlier. The two states system always bell entangled that what you get, they are highly entangle system.

And since we are using polarization it is always going to be two states. So, we did that and we found out that this always works out because all you need to do is for the two states he just add an Hadamard you always produce bell states. Once you have gotten to that point then you got one part of the circuit taken care and once you did this then you are able to get your final answer such that you can always produce a pair connected properly in this way, this is the bell pair again that you are generating.

So, then we are ready for our full quantum teleportation circuit where the criticality is we have a measurement part associated because Alice actually makes the measurement and based on this measurements they are able to compare and understand what is going on. So, you go through in a circuit like this. So, you also learn this is very important, whenever we write down a quantum circuit like this there are points and each point we can write out how they are going to go by in this process and then at every point when we do that. For example, we looked at the first point then we went to the next point then we went to the next point. So, at every point of applying a gate we looked at what we were left with or what we were generating and we were able to go through these and finally, get to the point where the measurement was made by Alice and correspondingly whatever (Refer Time: 53:17) applied on his side as a gate that is what we applied and once we did that we were able to get back the state that Alice said started with. Whatever Alice measured is not the state which Alice started with please remember that, that is very important she ended up making something which was possible to be applied a certain way of gates to get the original state that was done by Bob.

Finally, as a result of this entire process we were able to do a teleportation where we reproduce the qubit at the different location and we maintain quantum mechanical principles in the right way because the original state was destroyed. With this let us end here; we will take up the next topic in the next class.

Thank you.