

NPTEL

**NATIONAL PROGRAMME ON
TECHNOLOGY ENHANCED LEARNING**

IIT BOMBAY

**CDEEPIIT
IIT BOMBAY**

**Quantum Information and
Computing**

**Prof. D.K. Ghosh
Department of Physics IIT Bombay**

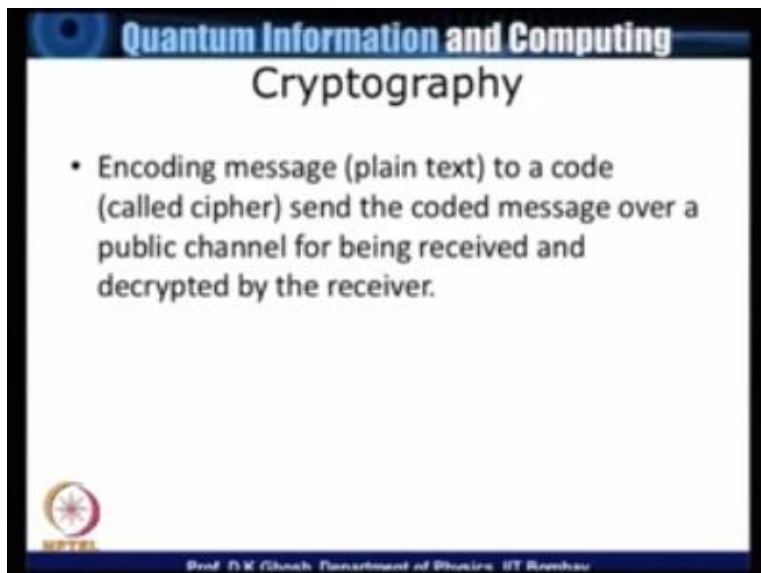
Modul No.08

Lecture No.43

Quantum Cryptography -I


In the last two lectures I had talked about the subject of Cryptography and let me sort of quickly review what we said, we said that.

(Refer Slide Time: 00:30)



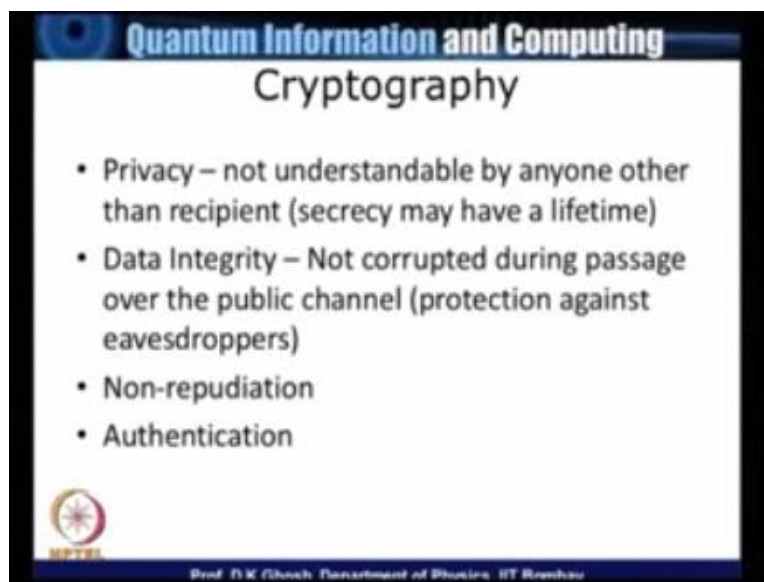
Quantum Information and Computing
Cryptography

- Encoding message (plain text) to a code (called cipher) send the coded message over a public channel for being received and decrypted by the receiver.

 Prof. D.K. Ghosh, Department of Physics, IIT Bombay

Encoding a message which we call as a plain text to a code to be called as cipher and send such a coded message over a public channel such as fiber optic channel or whatever you have or being received and decrypted by received. Now that is the whole cryptosystem that we are talking about from encoding a normal plain text then sending it and it is being received in the coded form and then finally this coded message being decrypted to the original form in which the message was send is known as cryptography.

(Refer Slide Time: 01:09)



As we mentioned last time but we would like to recorrect it there are 4 pillar stones are corner stoners of cryptography number one is there is a need for privacy and the code should not be understandable by anyone other than the intended recipient there are should be integrity of data that is the data should not be corrupted during passage over public channel and this should also imply that you protect your channel against either analysis or non analysis eavesdropper who might be trying to tap that channel.

The third and the fourth are non reputation that is a sender and a receiver should not be in a position who later on claim that they had either not sent it or not received it and finally the, there

must be some method by which this sender is authenticated the identity of the sender as well as that of the receiver or authenticated we talked about RSA algorithm and we said RSA algorithm depends up on.

(Refer Slide Time: 02:20)

Quantum Information and Computing

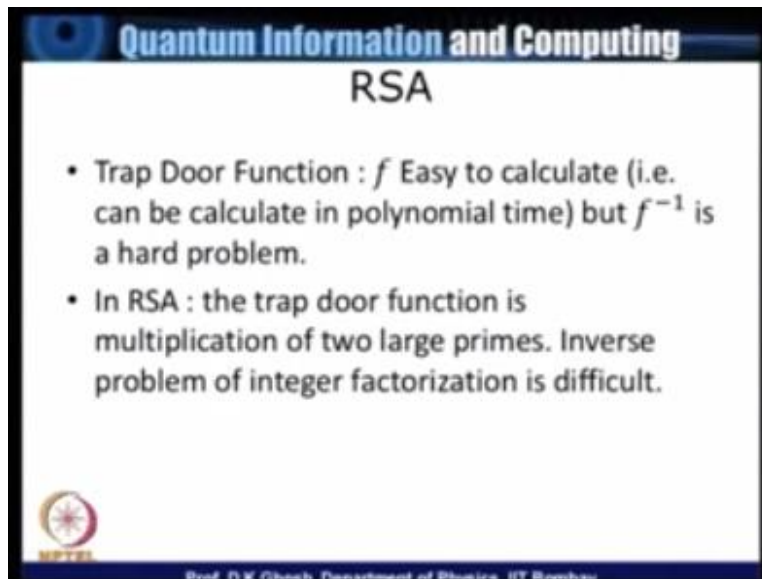
RSA

- $C_i = P_i \oplus K_i$
- $P_i = C_i \oplus K_i$
- RSA Cryptosystem (1977) Rivest, Shamir and Adleman used a public key encryption for encoding and sending data over internet. It enables one to establish the identity of sender and receiver.

Prof. D.K. Ghosh, Department of Physics, IIT Bombay

What we said the trap door function and which sort of tells you that there is a public key encryption for coding and sending data over the internet and this also enables the sender.


(Refer Slide Time: 02:33)



Quantum Information and Computing

RSA

- Trap Door Function : f Easy to calculate (i.e. can be calculate in polynomial time) but f^{-1} is a hard problem.
- In RSA : the trap door function is multiplication of two large primes. Inverse problem of integer factorization is difficult.


Prof. P. V. Choudhary, Department of Physics, IIT Bombay

To establish identity the whole idea behind the trap door function was the function f is easy to calculate in our case it was just multiplication of two large integers but the inverse problem of factorization is known to be a hard problem and that is the basis of the RSA algorithm.

(Refer Slide Time: 02:55)

Quantum Information and Computing
Stephen Wiesner (1960)

- Use polarized light to store information
- Use four bases, vertical/horizontal and diagonal (45°/135°)
- Each currency note contains 20 light traps, tiny devices that capture and store single photon. 4^{20} - a trillion possibilities
- Each bill is identified with a traditional number and a database containing polarization state.

Prof. D.K. Ghosh, Department of Physics, IIT Bombay

With this we will now try to see what differences if any will be made if we have to introduce quantum ideas into the science applicable. The entire subject started with a person with a graduate student known as Stephen Wiesner who in 1960 in his graduate theses had suggested some very interesting idea and I would call it as quantum money. The idea is this that we use polarize light or single photon to sorting function and this is done by having four different bases and the bases meaning it could be vertical horizontal along the x axis y axis let us say or it could be diagonal bases making an angle of 45 degree to the positive x axis or 135 degree with the positive x axis.

Now suppose in each currency note we embedded 20 light traps these are light traps are tiny devices which capture and stores single photon. Now 20 devices would mean basically a huge possibilities they because each of the photons could be coded in one of the 4 options that I gave you and so therefore if we have 20 it is 4^{20} which is a trillion of possibilities so therefore what do you do so each bill.

(Refer Slide Time: 04:40)



Picture we will see how it works so in addition to the usual numbering schemes that you have that particular currency note as number the denomination and things like that in each of these we have 20 light traps the number could be varied and in each of the twenty light traps I have a single photon which is encoded in one of these 24 bases, so obviously we have plenty possibilities are there I said 4^{20} different possibilities.

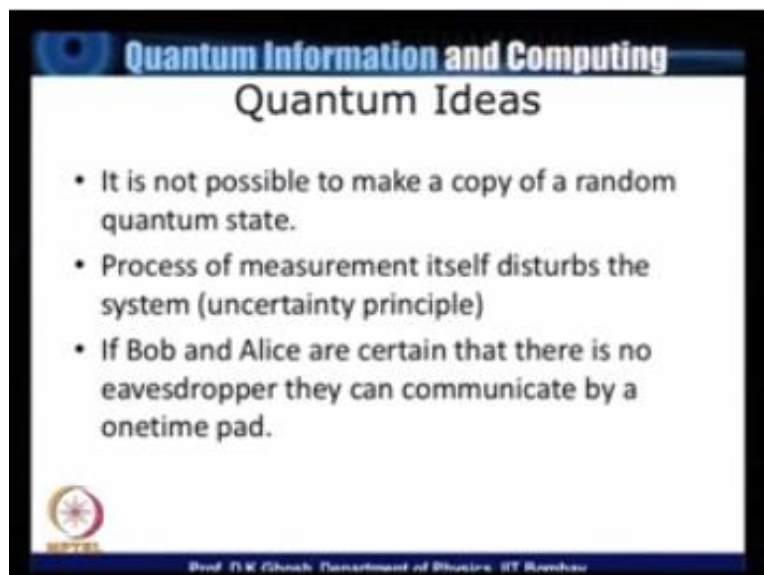
So there is no need for the code on one of the currency notes to be identical to that on another currency note. So therefore the identification of the currency note and the bases which is used to store this 20 photons is kept in a database. That in case a doubt arises then what one could always check against the database whether the a particular currency note that has been brought in is genuine or not.

Of course, we realize that this is a very expensive provision and we will obviously not work in reality just to check let us say the authenticity of a may be 1000 rupee note we will have to spend a lot, lot more. But that was not the point.

The point is this brought in the possibility of using quantum mechanics for verification purpose the using quantum mechanics to code something confidentially. So that today where you see you go to a shop people try to hold a currency note against either ultra violet light or try to identify various symbols that might have been put in to see in the nucleus, you will be simply able to check it against your database and find out whether the currency note is genuine or not.

A duplication is out of question because the process are producing is so expensive that even for the meant which makes it, it will become expensive. So therefore an individual enterprise trying to duplicate it is out of question. So therefore this is what it was but this provided us with an idea and this idea is based on the following.

(Refer Slide Time: 07:22)



That it is not possible to make a copy of a random quantum state, we have talked about this no cloning theorem in detail, we have said that given a arbitrary quantum state one cannot get an exact copy of this state, second thing is this that when you make a measurement that itself will disturb the system and that we have pointed out is because of uncertainty principle. Now suppose that I have two people Alice and Bob who are trying to communicate something among themselves.

(Refer Slide Time: 08:02)

Quantum Information and Computing

Quantum Ideas

- It is not possible to make a copy of a random quantum state.
- Process of measurement itself disturbs the system (uncertainty principle)
- If Bob and Alice are certain that there is no eavesdropper they can communicate by a onetime pad.

Prof. T.K. Ghosh, Department of Physics, IIT Bombay

And if that can mention that there is no eavesdropper which is certified by the fact that any eavesdropper would have disturbed a system by the process of measurement, then they can communicate through what you discussed as a onetime pad, remember the Vernam Cipher or the onetime pad was a string of bits which for which the identical copies are there with Alice and Bob and this pad is to be used once and once only.

So let us look at the various types of protocols chosen as, we start with what is known as a BB 84 protocol which the nomenclature has because of two people who suggested Bennette and Rosalt and 84 is because of.

(Refer Slide Time: 08:58)

Quantum Information and Computing

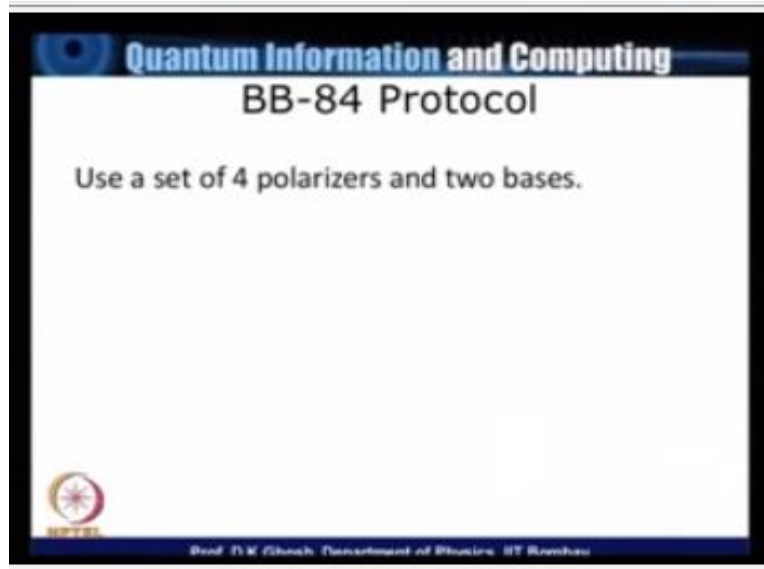
Quantum Ideas

- It is not possible to make a copy of a random quantum state.
- Process of measurement itself disturbs the system (uncertainty principle)
- If Bob and Alice are certain that there is no eavesdropper they can communicate by a onetime pad.

Prof. D.K. Ghosh, Department of Physics, IIT Bombay

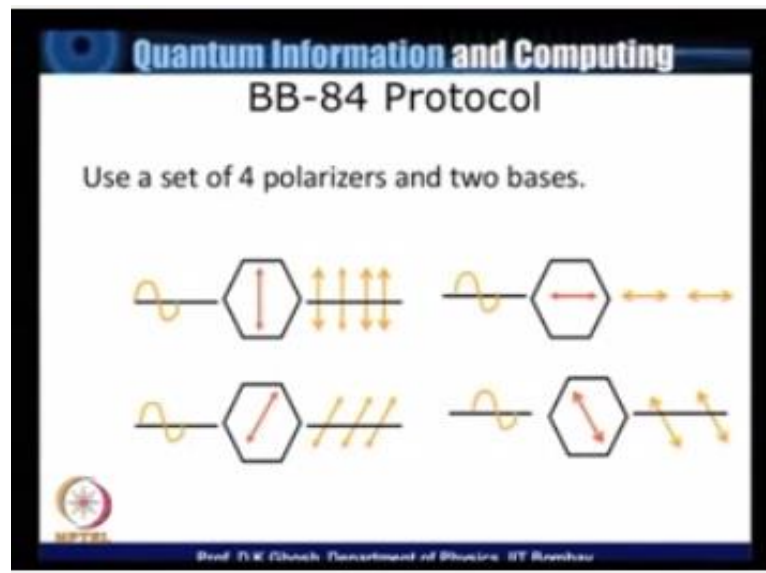
1994 in which this all been.

(Refer Slide Time: 09:01)



Now what the, this thing does is, they use a set of 4 polarizer's and they use two bases, so Alice has a set of two polarizer's, Bob has a set of two polarizer and each one of them they have decided among themselves that in order to encode a bit if Alice is sending to Bob in case of Alice, Alice will encode it in one of these two bases that says 1. And likewise when Bob receives the bit he will decode it using the same two bases. So let us look at what is.

(Refer Slide Time: 09:48)



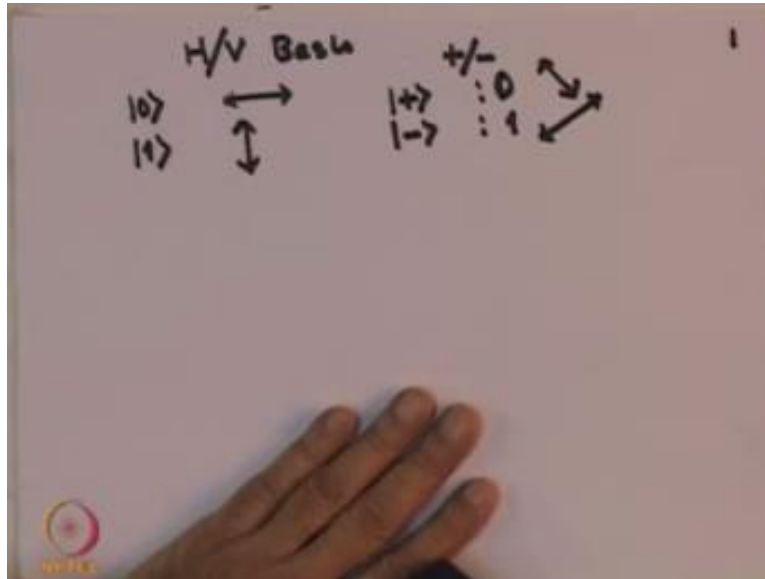
Means it is, so this for example is one of the situations, so this is a vertical bases in which the a photon is being sent and if that is the pass axis on the polarizer then the photons which come out of it they have polarizations which are vertical as indicated. Now this one along with another bases which you call as the horizontal basis in which case the pass axis is horizontal and the photon that is coming out will have polarization which in the horizontal, so that is basis number 2.

The number 3 basis in this that I have a diagonal basis in which the pass axis is that 45° to the positive x axis and a photon that is coming out of it is also, you know polarized in the direction has been shown and finally the one which is perpendicular to this is the one where the pass axis makes 135° with the positive x axis. So these are the four basis which Alice uses to encoded bit and these will also be the basis in which Bob will be decoding it and let see how it works.

Now basically Alice has two pairs of this, horizontal vertical basis and the diagonal basis which is one at 45° the other one at 135° , so what Alice does is she decides randomly which could be done for example by tossing of a coin, so she tosses a coin if she gets a head she decides to use

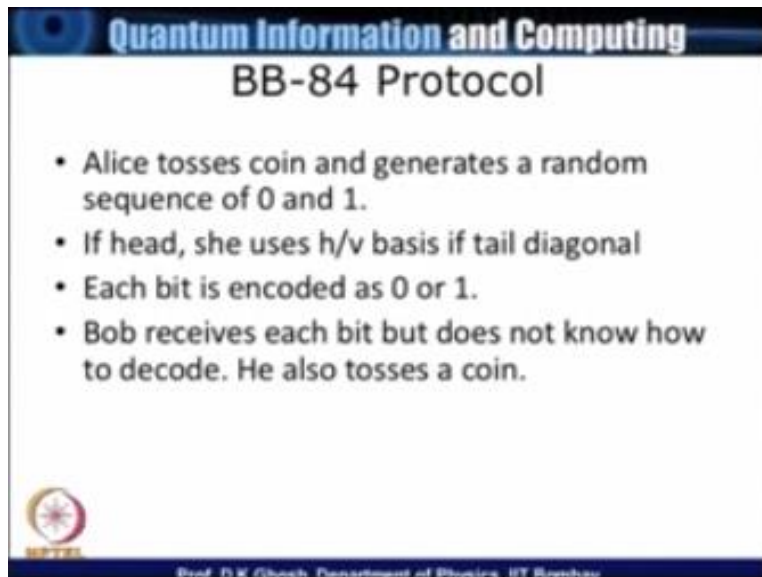
the horizontal vertical basis for encoding the photon. So supposing she has decided to use this basis then she might use for instance the bit 0.

(Refer Slide Time: 12:08)




The qubit 0 maybe encoded as a horizontal 1 and qubit 1 maybe encoded as a vertical 1, and this is provided she is using what we have call as the horizontal vertical basis. Similarly if she gets a tail for her coin toss she will be using what we call as a diagonal basis which using our usual notation let us call it a +/- basis and in this case she encodes a + to indicate 0 the bit 0 and encodes a - to indicate bit 1, so this is a photon polarize like this and this is a photon which is polarize like this. So this is what happens now Bob receives this.

(Refer Slide Time: 13:03)



Quantum Information and Computing
BB-84 Protocol

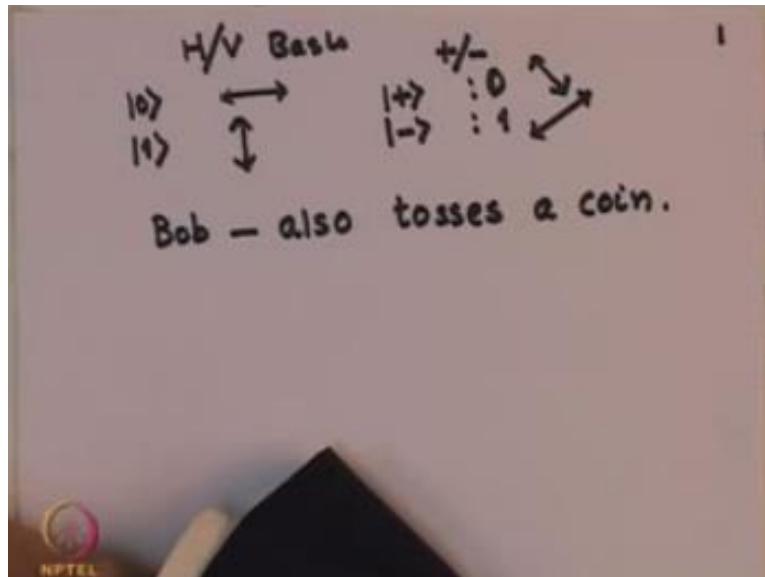
- Alice tosses coin and generates a random sequence of 0 and 1.
- If head, she uses h/v basis if tail diagonal
- Each bit is encoded as 0 or 1.
- Bob receives each bit but does not know how to decode. He also tosses a coin.


Prof. D.K. Ghosh, Department of Physics, IIT Bombay

But Bob has a problem because if Bob knew exactly what basis, Alice use for encoding a bit then of course Bob would use the same basis and then he would in a position to decode it easily. But that is a problem, because if these are publicly known then have eavesdropper let us say she will also be in a position to use that basis and interrupt it on the way. And so for example, if Alice is using a horizontal vertical basis and Eve also knows it.

So Eve also aligns her polarizer accordingly and when a bit comes she gets the information and let that BC bit passes to pass to Bob. So even though Bob has got exactly what Alice has sent but so has Eve, so this is not a desirable in the interest of secrecy of the problem. Because in any public channel cryptosystem we must always take care of the possibility that the, there was somebody who wanted to get this information on the way. Now so what do they do, what they do is the following Bob also decides to do a random job.

(Refer Slide Time: 14:38)



So Bob will also tosses a coin and let say if he gets a head he will also use a head horizontal vertical basis and if gets a tail he will use a diagonal basis.

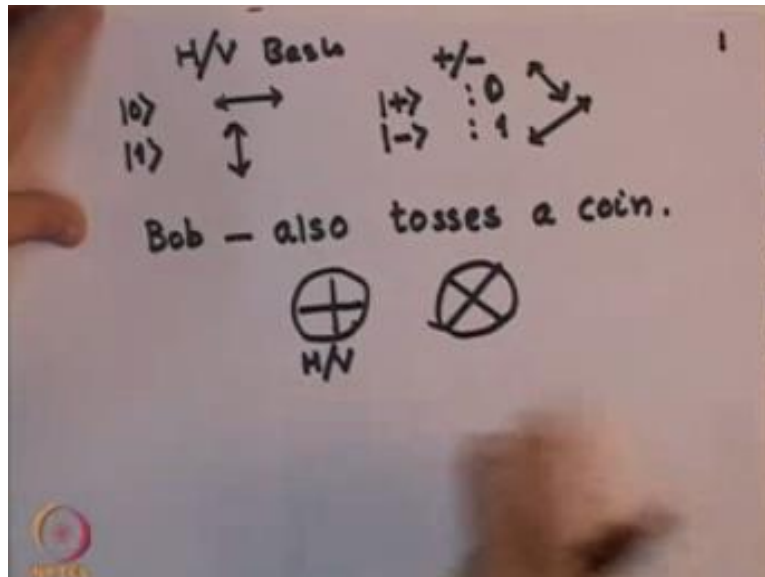
(Refer Slide Time: 14:58)

The slide is titled "Quantum Information and Computing" and "BB-84 (contd.)". It features a bullet point labeled "ALICE :". Below this, there are two rows of boxes and circles. The top row, labeled "BIT TX", contains eight boxes with the bits 1, 0, 0, 1, 1, 0, 0, and 1. The bottom row, labeled "Basis", contains eight circles. The first and sixth circles are red with a white cross, while the others are green. A small logo is in the bottom left, and a footer at the bottom reads "Prof. P.K. Ghosh, Department of Physics, IIT Bombay".

BIT TX	1	0	0	1	1	0	0	1
Basis	Red with cross	Green	Green	Red with cross	Green	Red with cross	Red with cross	Green

Now what does it actually need, now suppose Alice has done this, so this is shown in the slide but let me also illustrated here so that we know what we are talking about I will indicate, I will indicate.

(Refer Slide Time: 15:18)












A horizontal vertical basis like this and so this is my horizontal vertical basis and this is my diagonal basis, so the picture that I have shown you is the following.

(Refer Slide Time: 15:32)

Quantum Information and Computing
BB-84 (contd.)

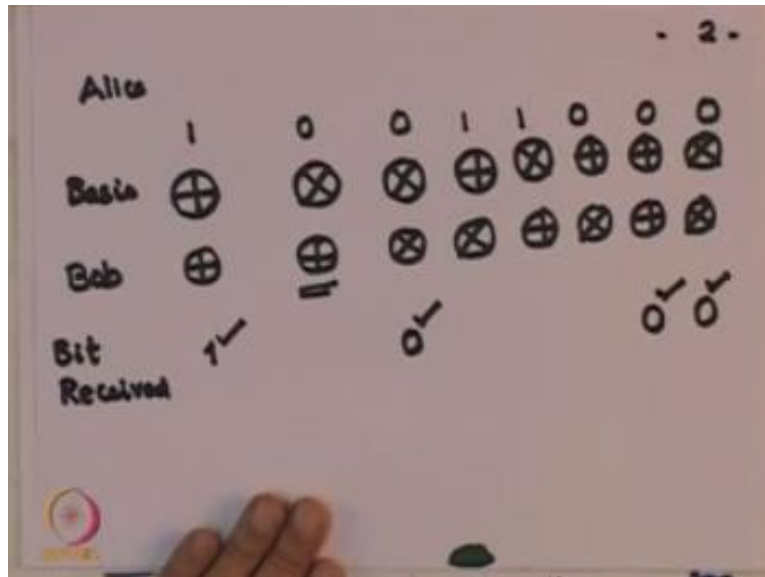
• ALICE :

BIT TX	1	0	0	1	1	0	0	1
Basis								


Prof. D.V. Cheuk, Department of Physics, IIT Bombay

So what you are saying is this, that suppose Alice wants to send.

(Refer Slide Time: 15:46)

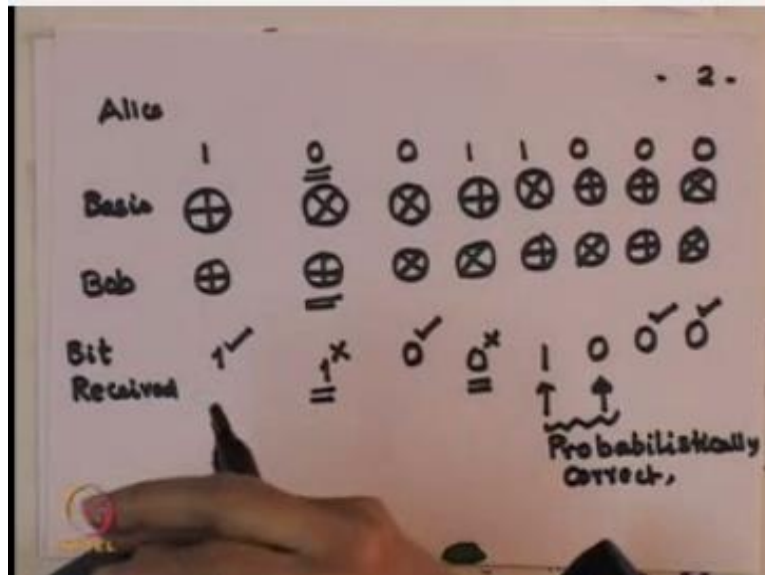


The following bits so 10011000 suppose if she wants to sent this and she does tosses a coin let us suppose she gets this, that, this is only for illustration purpose. So these are the Alice's basis, now when Bob receives this Bob also needs to decide which basis he use, so oblivious of what Alice have used Bob tosses a coin and let us suppose Bob do not gets this + horizontal vertical, horizontal vertical, diagonal, diagonal, horizontal vertical, diagonal, horizontal vertical, and diagonal.

Now let us look at what can happen they notice the bit received now this is an example where both of them had use the same basis so therefore if Alice sent one Bob will also receive it. We will come back to these where they do not agree, but here again there is an agreement so therefore Bob will receive 0 the next agreement is here so Bob will receive 0. So let me let me put tick marks over this to show that and in basis to show that in these cases Bob's and Alice's basis were random. Now what happens here now if you look at here you find they have used different basis, now when they use different basics Bob, Alice could have sent anything, but Bob has an equal probability of measuring either a 0 or 1.

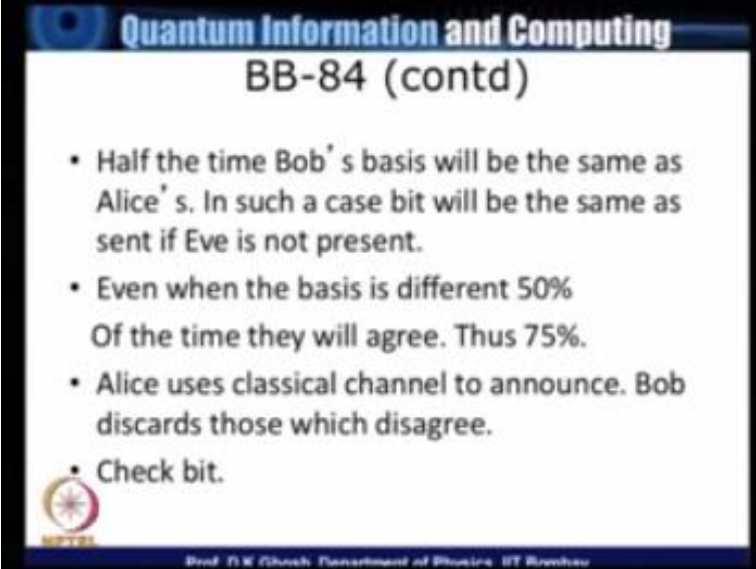
And the reason is supposing Alice have used horizontal vertical basis to encode let us say 0, but then 0 in equivalent to $0 + + - / \sqrt{2}$ in the diagonal basis. And so when Bob makes a measurement he has equal probability of measuring + which is the corresponds to bit 0 and - which corresponds to bit 1.

(Refer Slide Time: 18:53)



So in these cases this is problem is and let me just give you some idea supposing this is 1 this is 0, this let say this is 1 and this is 0. Now if you compare what is happening is this here there is a 0, but we have 1 so let me cross it out. Again here I have a 1 and a 0 so once again let me cross it. But you notice here in these cases this case and this case even though the two basis did not agree the bit sent by Alice is the same bit that was received by Bob purely probabilistically. So these two are probabilistically correct. So let us look at what is that happening.

(Refer Slide Time: 20:09)



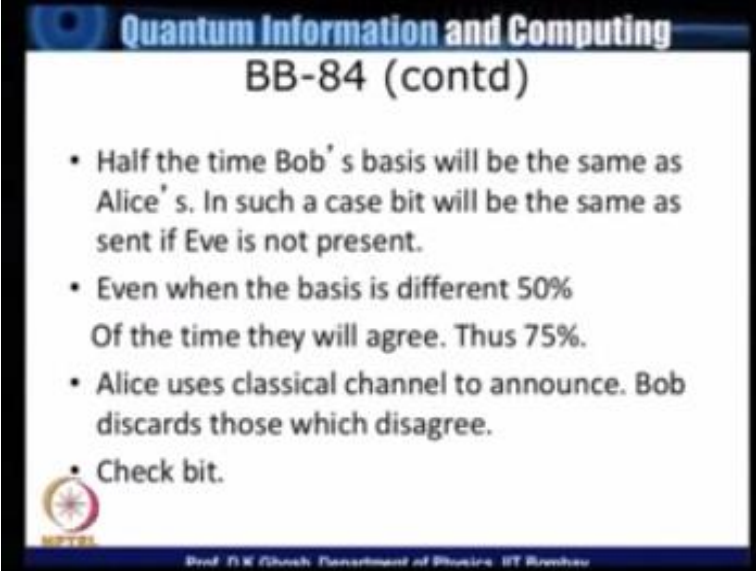
Quantum Information and Computing
BB-84 (contd)

- Half the time Bob's basis will be the same as Alice's. In such a case bit will be the same as sent if Eve is not present.
- Even when the basis is different 50% Of the time they will agree. Thus 75%.
- Alice uses classical channel to announce. Bob discards those which disagree.
- Check bit.

Prof. P.K. Ghosh, Department of Physics, IIT Bombay

So assuming there are large and large number of bits that has been sent and since Alice is doing a random experiment of tossing a coin suppose half the time Alice uses horizontal vertical basis and another half of the time.

(Refer Slide Time: 20:29)



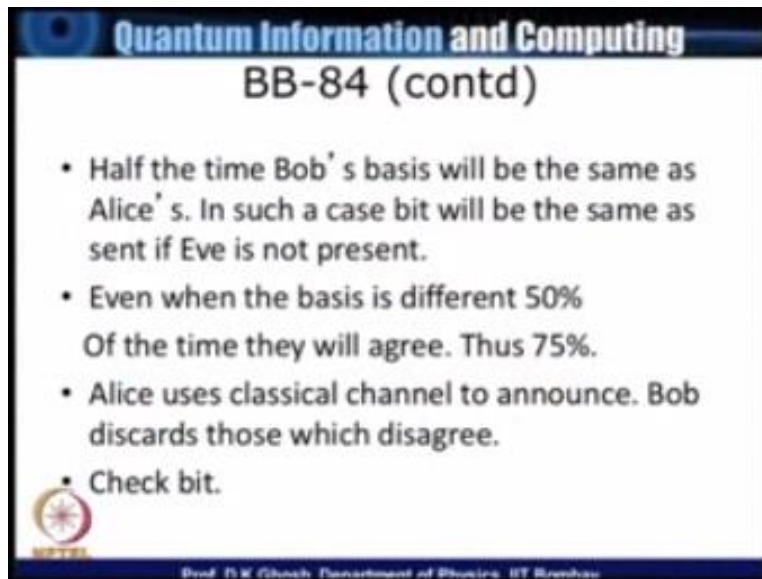
Quantum Information and Computing
BB-84 (contd)

- Half the time Bob's basis will be the same as Alice's. In such a case bit will be the same as sent if Eve is not present.
- Even when the basis is different 50% Of the time they will agree. Thus 75%.
- Alice uses classical channel to announce. Bob discards those which disagree.
- Check bit.

Prof. P.K. Ghosh, Department of Physics, IIT Bombay

The she uses the diagonal basis. Now we assume that there is no eavesdropper. So firstly when Bob use basis is the same as that of Alice now that to happen 50% time now 50% of the time the basis in which Bob measure happens to be the same as that of Alice the bits Alice received will be the same as that Bob, the bits Alice sent will be the same as those which Bob received and hence the bit will be identify so that is 50%. So we are left with another 50% where Bob's and Alice's basis do not agree, but we have seen that probabilistically there is a possibility that even in half of those cases daily. In other words the agreement between the bits and for Alice and those received by Bob will be as much as 75%.

(Refer Slide Time: 21:40)



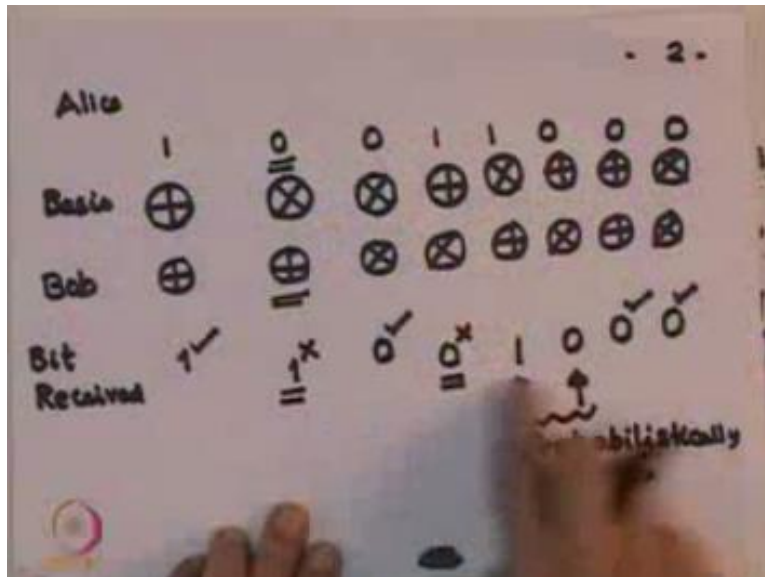
Quantum Information and Computing
BB-84 (contd)

- Half the time Bob's basis will be the same as Alice's. In such a case bit will be the same as sent if Eve is not present.
- Even when the basis is different 50% Of the time they will agree. Thus 75%.
- Alice uses classical channel to announce. Bob discards those which disagree.
- Check bit.

Prof. T. K. Ghatak, Department of Physics, IIT Bombay

The point is that though they would agree 75 % of the time only for 50 % of the time they have used the same percent. Now what Alice does is to she uses a classical channel and she will not announce what bit she use but what she will announce is that what are basis she used in sequence to above. For example, in the example that I gave you.

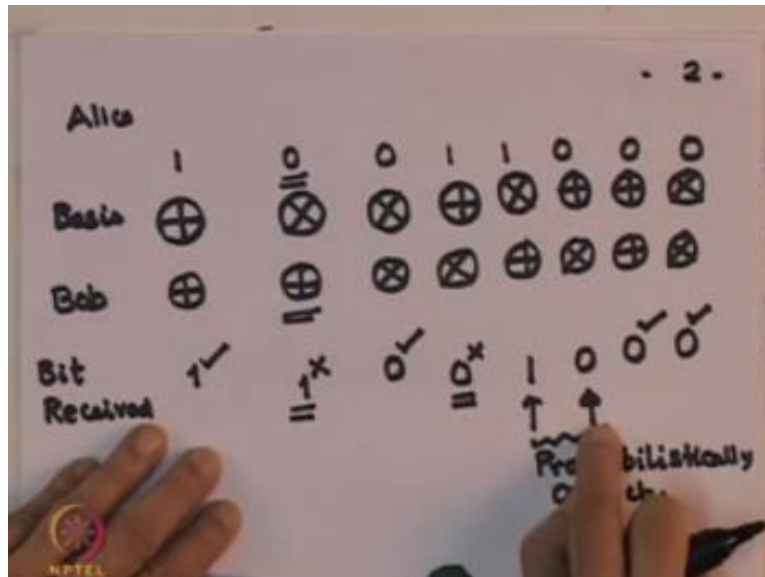
(Refer Slide Time: 22:18)



After the transmission is over Alice will make an announcement over a public channel such as a telephone or whatever she will simply say horizontal vertical, diagonal, diagonal, horizontal vertical, diagonal, horizontal vertical, horizontal vertical, diagonal, this is all the information she makes to the public she does not quite say what are the big such as that. Now when Bob receives this he takes the following access he removes all those where Alice's bits and Alice's basis and his basis of measurement did not agree.

What it implies he going to throw away half of those cases where there was a probabilistic agreement between the bits that Alice said and the bits that Bob received.

(Refer Slide Time: 23:23)




These two he will throw away in spite of the fact that had he kept them they would have been in same, but this is done in order to achieve a certain amount of uniformity, because Bob has no idea which bits would have agreed random. Now once Bob have shown this away you have essentially 50% of the bits which Alice sent and Bob has an identical copy of those bits.

(Refer Slide Time: 24:06)

Quantum Information and Computing

No Cloning Theorem

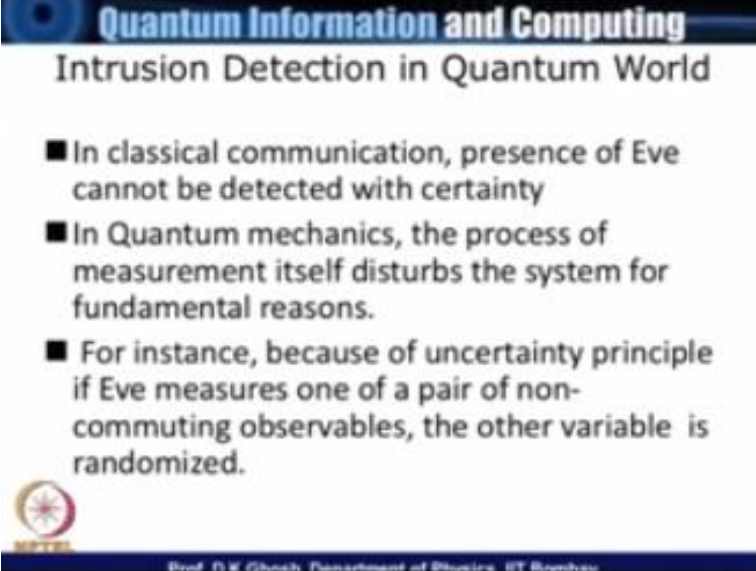
- A copying device can only clone orthogonal states. Since an arbitrary superposition of states is not orthogonal, cloning of a quantum state is not possible.



Prof. P. K. Shukla, Department of Physics, IIT Bombay

So now what we need to do is this that this is fine assuming that Bob and Alice they are not being intervened by a third party whom will call of the eve who is trying to get information from the public channel. Now what makes this problem little more challenging analysis, let us suppose there is eve what can we have do. Now eve has the possible of tapping what Alice sent keep that and make an identical copy of it and send it to Bob. Now this is private by the no cloning theorem.


(Refer Slide Time: 25:01)



Quantum Information and Computing

Intrusion Detection in Quantum World

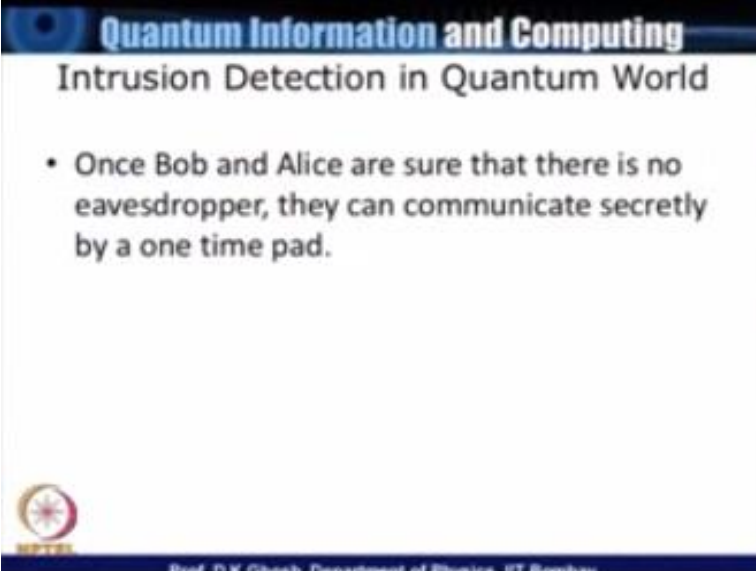
- In classical communication, presence of Eve cannot be detected with certainty
- In Quantum mechanics, the process of measurement itself disturbs the system for fundamental reasons.
- For instance, because of uncertainty principle if Eve measures one of a pair of non-commuting observables, the other variable is randomized.



Prof. T. K. Choudhury, Department of Physics, IIT Bombay

So what will be done is the following that we would some or be alerted that there is somebody in the system who has made a process of measurement. Now let us see what happens when such a thing happens. So let us now introduce.


(Refer Slide Time: 25:26)



Quantum Information and Computing

Intrusion Detection in Quantum World

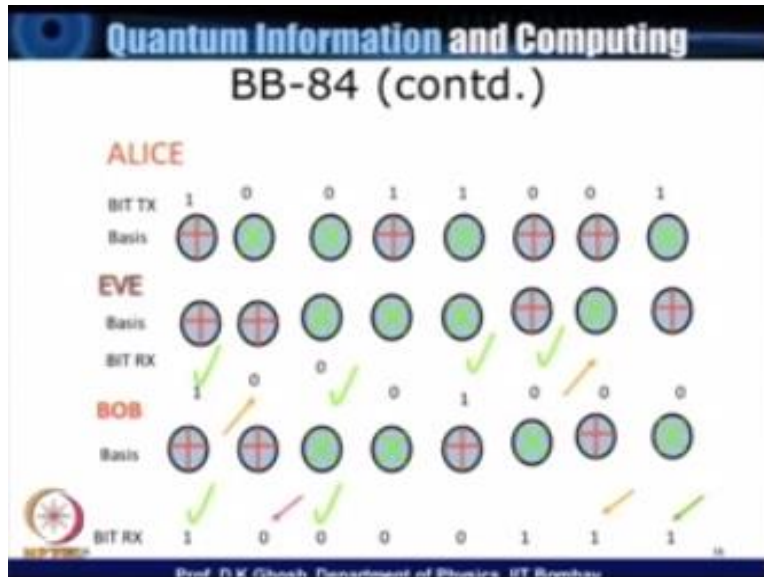
- Once Bob and Alice are sure that there is no eavesdropper, they can communicate secretly by a one time pad.



Prof. T.K. Ghosh, Department of Physics, IIT Bombay

Into our system that presence of, see is there are no aim which Bob and Alice can a certain by certain process then they can communicate assuming that the bits of spins which they have agreed, agreement on that becomes their similar port.

(Refer Slide Time: 25:41)



Now at this stage we have reproduce the same diagram in the presence of the eve but now there is the difference there are situations what now leave not knowing what to do also use as a coin toss, because she knows Alice and Bob are using either horizontal vertical basis or a diagonal basis. And based on that she makes a measurement and let us passes the bit to Bob. Now what will happen how will this affect our Bob's reading up the whole thing is what we will take up in the next lecture.

**NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING
(NPTEL)**

**NPTEL
Principal Investigator
IIT Bombay**

Prof. R.K. Shevgaonkar

Head CDEEP

Prof. V.M. Gadre

Producer

Arun kalwankar

**Online Editor
& Digital Video Editor**

Tushar Deshpande

**Digital Video Cameraman
& Graphic Designer**

Amin B Shaikh

Jr. Technical Assistant

Vijay Kedare

Teaching Assistants

Pratik Sathe
Bhargav Sri Venkatesh M.

Sr. Web Designer

Bharati Sakpal

Research Assistant

Riya Surange

Sr. Web Designer

Bharati M. Sarang

Web Designer

Nisha Thakur

Project Attendant

Ravi Paswan
Vinayak Raut

**NATIONAL PROGRAMME ON TECHNOLOGY
ENHANCED LEARNING**

(NPTEL)

Copyright NPTEL CDEEP IIT Bombay