

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.44

Quantum Cryptography- II

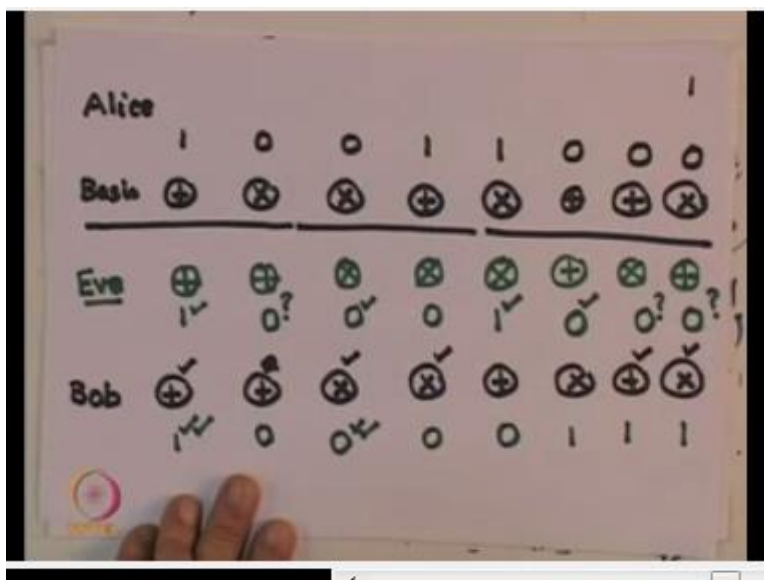
In the last lecture we had introduced what we called as the BB84 protocol for a communication to be set up between Alice and Bob and what we had said was the following that both Alice and Bob have decide to have a protocol in which the coding and decoding of polarize light will happen by using a pair of basis for both encoding and for decoding one of them we called as the horizontal vertical bases and the other one we called the diagonal or what we have been calling as the plus, minus basis.

Now based on that we had said that randomly a particular basis is selected by Alice to encode a particular bit, and as the result when Bob receives it assuming that there are no eavesdropper in the channel whenever there are basis agree because Bob would also measure it randomly. Whatever bits Alice send would be also received by Bob in addition in the remaining case of 50% of the cases where their basis of sending and receiving do not agree they would also probabilistically agree for 50% of the time.

So as a result in cases where there are no eavesdropper the bits sent by Alice would agree with bits received by Bob total 75% of the time however at that stage Alice makes an announcement

of what basis she used in sending the sequence. Now on hearing that over a public channel Bob will remove all those bits where their basis do not agree this would also result in half of those where their basis did not agree, but they received Bob received the same bits as Alice sent to be also discussed. So in other words insisted of agreement being full 75% the agreement that they were right at is a perfect 50% remember the 75% was only a probabilistic estimate so coming back to the picture that I gave you we had shown.

(Refer Slide Time: 03:01)



That when Alice is using these basis this was there in the slide but when Alice is using these basis and Bob is using this, these were the bits that are sent by Alice and let us suppose these are the bases that we use by Bob we simply identified those where their basis agreed these would be discard in any case. Now let us see what happens if there is an intruded in the channel. So I now put in the presence of a eve which I will put in between because she will have to interrupt the process of sending briefly and then measure it herself not knowing what basis was used by either Alice and Bob, eve also decides to do a random basis.

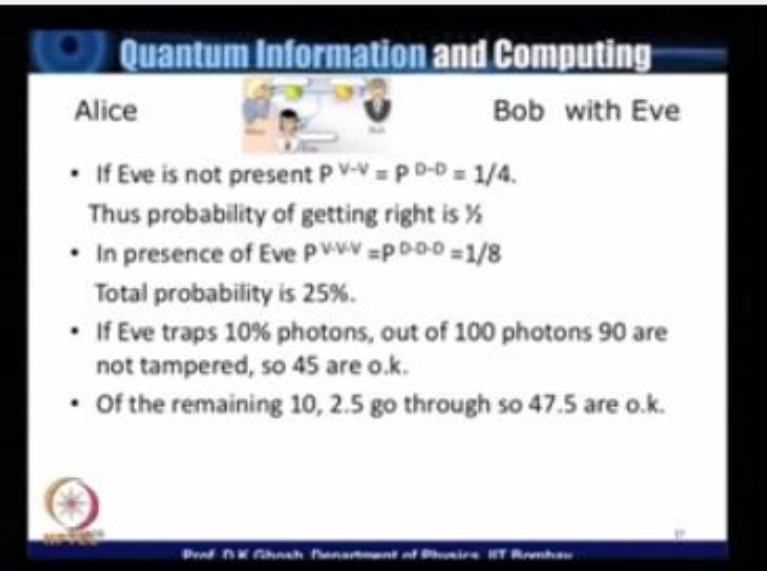
So she will do toss a coin and also send a sequence but on the other hand let us assume that her basis are these plus horizontal vertical, horizontal vertical is just a random sequence which you

can work out now let us look at what happens here now at this stage before the bit reaches Bob if Alice send eves basis agree then the bit received by eve would be the same as that sent by Alice and so therefore this bit will agree and here this bit will also agree this bit will agree this will agree and these we have non element play even though they do not have agreement one would expect that 50% of the time there would still be an agreement between Alice and Eve and let us say that Eve measured 0 here again a 0 there and let us suppose these where Eves measurement.


So you notice these are the case where there are agreements in spite of the fact that their basis did not agree now let us look at what is happening. Now Bob would receive something now Bob receive what Bob would receive would depend upon whether all the three bases are the same now in cases the three bases of the same Bob would receive exactly what Alice sent. So therefore let me write down here 1 let me put a double tick on it to show that everything has agreed there, this is another case like that, well we do not have any other case. So therefore these two element Bob will receive random things here so let me write down what those things are let us say 0, 0, 0, 0 so 1, 1, 1.

Now look at what is happened here, the situation is a following that out of these cases that we have $1/4^{\text{th}}$ of the cases Bob's basis, Eves basis and Alice's basis agree.

(Refer Slide Time: 07:08)



Quantum Information and Computing

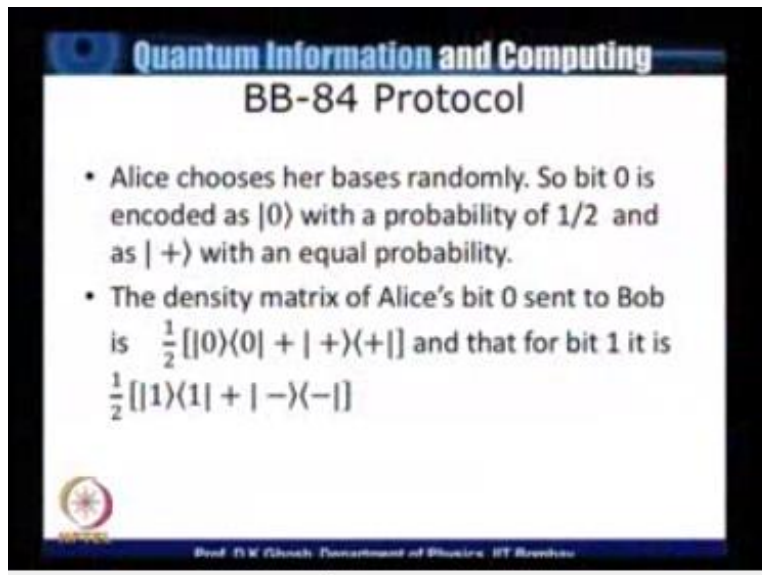
Alice  Bob with Eve

- If Eve is not present $P^{V-V} = P^{D-D} = 1/4$.
Thus probability of getting right is $1/2$
- In presence of Eve $P^{V-V} = P^{D-D} = 1/8$
Total probability is 25%.
- If Eve traps 10% photons, out of 100 photons 90 are not tampered, so 45 are o.k.
- Of the remaining 10, 2.5 go through so 47.5 are o.k.

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

Now previously in the absence of Eve only 50% from the cases the Alice's and Bob's results would match perfectly another 25% was probabilistically which we would throw out in either case. So what happens here is this that the probability now drops to 25% where Alice, Bob and Eve they are basis agree then only whatever Alice sent Bob would receive. There would not be cases of 25% where even though Alice and Bob's bases do not agree, Bob will not receive those because of the interrupt. Now how does one take care of this, so what happens in that case is this.


(Refer Slide Time: 08:13)



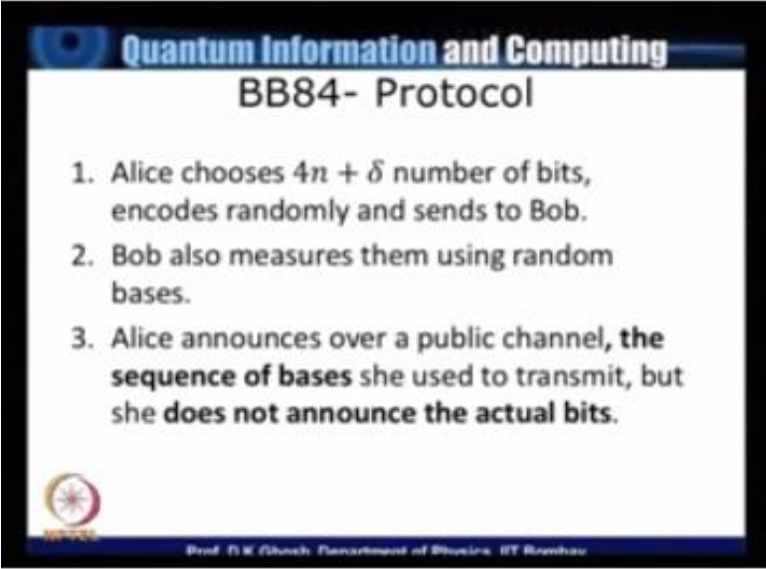
Quantum Information and Computing

BB-84 Protocol

- Alice chooses her bases randomly. So bit 0 is encoded as $|0\rangle$ with a probability of $1/2$ and as $|+\rangle$ with an equal probability.
- The density matrix of Alice's bit 0 sent to Bob is $\frac{1}{2} [|0\rangle\langle 0| + |+\rangle\langle +|]$ and that for bit 1 it is $\frac{1}{2} [|1\rangle\langle 1| + |-\rangle\langle -|]$


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

(Refer Slide Time: 08:14)



Quantum Information and Computing

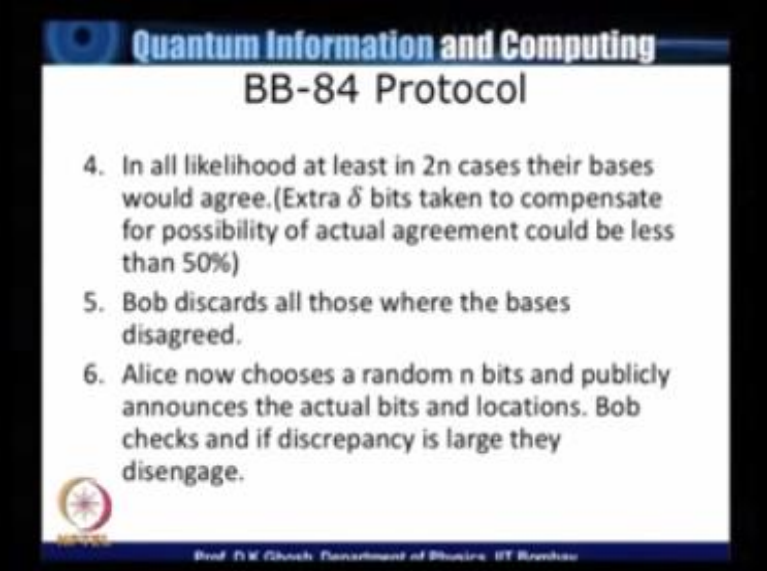
BB84- Protocol

1. Alice chooses $4n + \delta$ number of bits, encodes randomly and sends to Bob.
2. Bob also measures them using random bases.
3. Alice announces over a public channel, **the sequence of bases** she used to transmit, but she **does not announce the actual bits**.

Prof. D.K. Ghosh, Department of Business IT, Ranchi

That the protocol works like this, to start with Alice will choose let us say $4n + \delta$ number of bits, and encode them randomly at the left side using a toss and then send them to Bob, now Bob also will measure them using another set of random base then as we have said Alice would announce over a public channel the sequence of bases she used to transmit but remember she never announced what bits she actually transmit. Now so what will now happen is this.

(Refer Slide Time: 08:57)



The slide is titled "Quantum Information and Computing" and "BB-84 Protocol". It contains three numbered steps:

4. In all likelihood at least in $2n$ cases their bases would agree. (Extra δ bits taken to compensate for possibility of actual agreement could be less than 50%)
5. Bob discards all those where the bases disagreed.
6. Alice now chooses a random n bits and publicly announces the actual bits and locations. Bob checks and if discrepancy is large they disengage.

At the bottom of the slide, there is a small logo on the left and the text "Prof. D.K. Ghosh, Department of Physics, IIT Bombay" on the right.

That the, we have taken $4n + \delta$ so at least in $2n$ cases their bases would agree because we had said that the probability that they have you the same bases is 50% but 50% does not mean out of 4 and you actually agree into n cases, so we have taken some extra bits to make sure that the agreement is at least $2n$ case and we have send the Bob we discard all those where the bases used by Alice was not the same as the bases used by him.

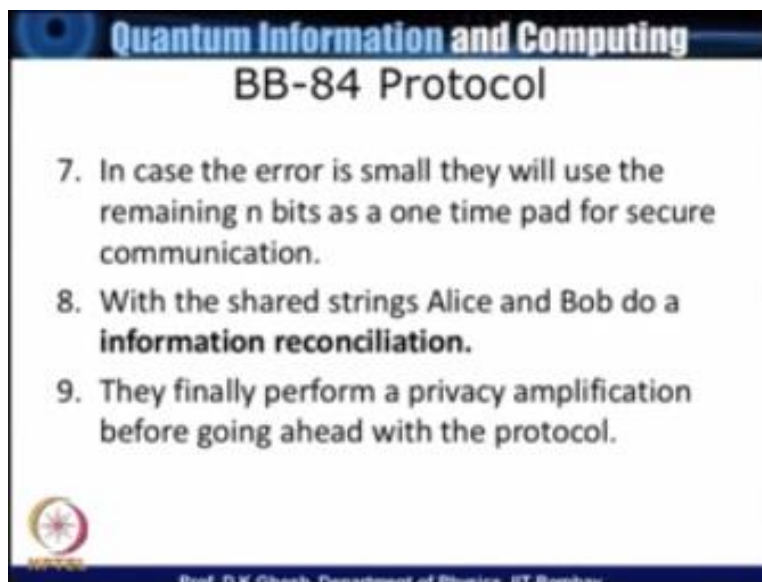
Now what happens is that Alice and Bob have a set of bits the number is $2n$ and in ideal case where there is no Eve the bits at the Alice and the bit receiver Bob must agree. So at this stage what Alice does is this, she picks up a random sequence of n bits I do not have remember I was starting with $4n + \delta$ we now have at least $2n$ out of that Alice chooses a random sequence of n bits and this time over a public channel she actually makes the announcement that in sequence number 5 I send 0 in 7th position I sent 1 or whatever you have.

Now this is public so we still have n of them which are still configuration out of $4n + \delta$ now Bob makes a comparison now of what Alice is send and what he received. Now remember we are talking about situation where the bases used by Alice and the Bob are identity. So therefore ideally they should get the same bits but on comparison if Bob finds that the agreement is not

within acceptable error of a logic channel then they know that something is going wrong in all likelihood there is an eavesdropper in the channel who is disturbing the system.

And if the disturbance is intolerable then they will simply have not done the protocol and who do it for an opportune time assuming that Eve could not be listening to the whole process forever and Eve has been done. Now once they are sure that there is an agreement between the bits which have been publically announced within tolerable error then they can use it the n bits which have not been announced as a onetime pad. Okay, that says but on the other hand there are other information to be take care of.

(Refer Slide Time: 12:14)



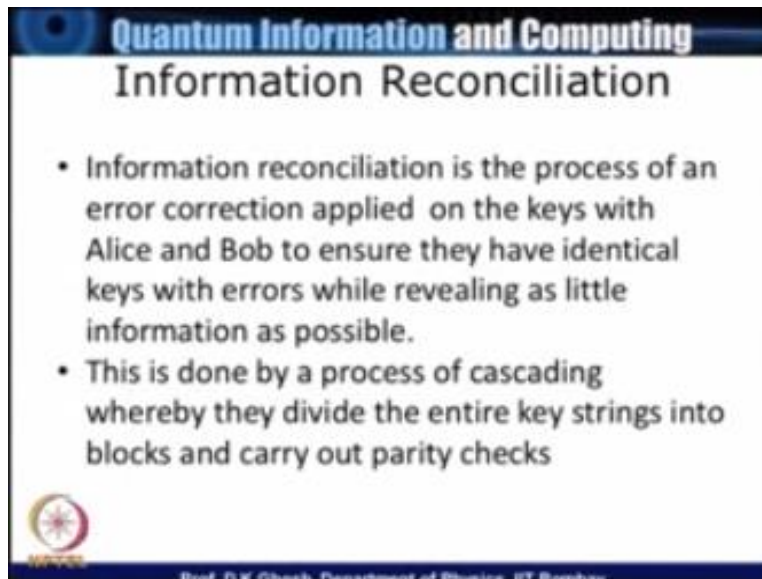
The slide is titled "Quantum Information and Computing" and "BB-84 Protocol". It contains three numbered steps:

7. In case the error is small they will use the remaining n bits as a one time pad for secure communication.
8. With the shared strings Alice and Bob do a **information reconciliation**.
9. They finally perform a privacy amplification before going ahead with the protocol.

At the bottom left, there is a logo for IIT Bombay. At the bottom center, it says "Prof. D.K. Ghosh, Department of Physics, IIT Bombay".


At that stage, what they will do will be two different processor they will follow up their agreement of the secret N bits with what you will call as the information reconciliation, and finally they would do what is call they privacy amplification before going ahead with the protocol. Now let me explain what these two things mean.

(Refer Slide Time: 12:41)



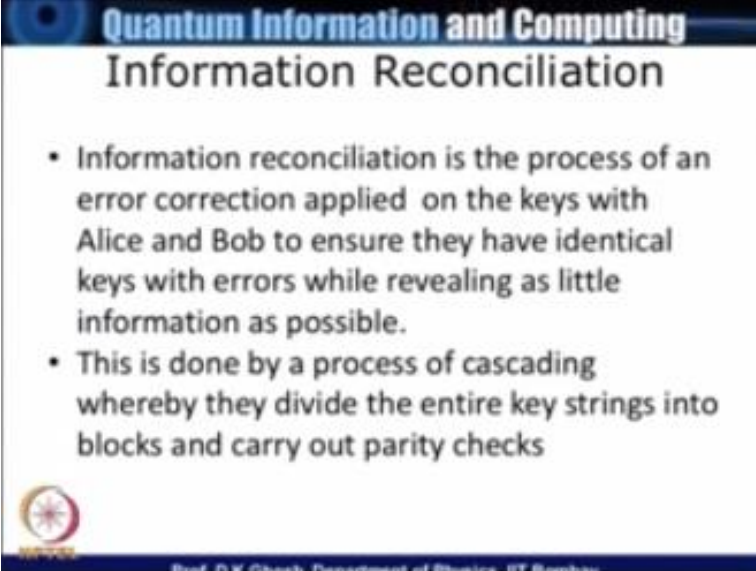
Quantum Information and Computing
Information Reconciliation

- Information reconciliation is the process of an error correction applied on the keys with Alice and Bob to ensure they have identical keys with errors while revealing as little information as possible.
- This is done by a process of cascading whereby they divide the entire key strings into blocks and carry out parity checks


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


I will not go into the details but let us look at that, information reconciliation is actually a process of error correction applied on the keys with Alice and Bob to ensure that they have identical keys, okay. Now when you do that they will be required or of necessity they will be revealing there is little more information. However, this extra information reveal to Eve can be shown not to matter much.

(Refer Slide Time: 13:16)



Quantum Information and Computing
Information Reconciliation

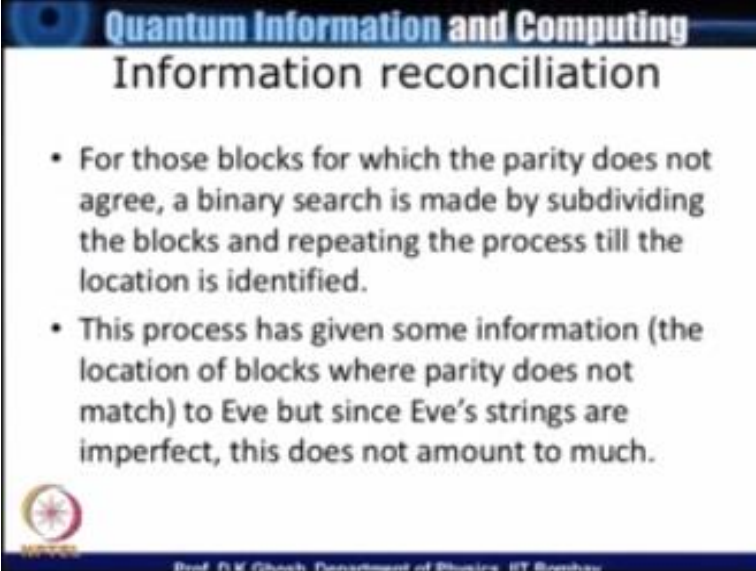
- Information reconciliation is the process of an error correction applied on the keys with Alice and Bob to ensure they have identical keys with errors while revealing as little information as possible.
- This is done by a process of cascading whereby they divide the entire key strings into blocks and carry out parity checks


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

Now what do they do, see they do it by a process call cascading, so they are the setup N strings which ideally should agree completely so they divide this entire key strings into blocks which they have agreed what should be the size of bits nodes. And then they do a parity check on each block, what is the parity check they simply add up modulo 2 the bits that is they are in a given block and announce that these are the parities, now remember we are not talking about announcing the actual bits you are simply saying supposing there are 1000 bits there you have added them you are saying this should be a 0.

Now Bobs parity check must agree with parity announce by Alice, if they had identical sequence, now assuming that the error possibility is smaller of course this is still possible that parities agree but there are still errors there but once you have done that, okay you take those blocks for which.


(Refer Slide Time: 14:31)



Quantum Information and Computing

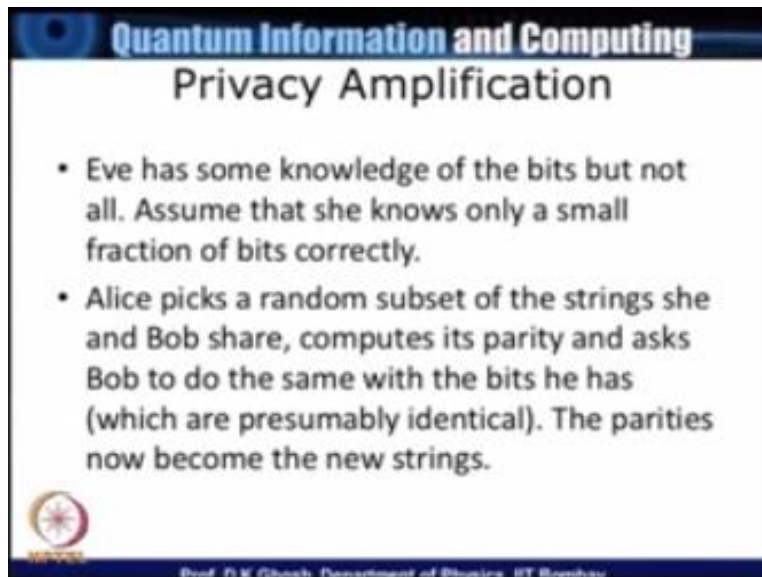
Information reconciliation

- For those blocks for which the parity does not agree, a binary search is made by subdividing the blocks and repeating the process till the location is identified.
- This process has given some information (the location of blocks where parity does not match) to Eve but since Eve's strings are imperfect, this does not amount to much.

 Prof. F. M. Church, Department of Physics, IIT Bombay


There are errors identify, now either you can abandon them or what you can do is you can sub divide them. Now once you sub divide the blocks into some blocks and carry on the parity check then discard those blocks where you know that definitely there are errors and they are small enough to throw it away. So in the process as we have said they have given some information to Eve but on the other hand it does not actually amount to much.

(Refer Slide Time: 15:02)



Quantum Information and Computing
Privacy Amplification

- Eve has some knowledge of the bits but not all. Assume that she knows only a small fraction of bits correctly.
- Alice picks a random subset of the strings she and Bob share, computes its parity and asks Bob to do the same with the bits he has (which are presumably identical). The parities now become the new strings.

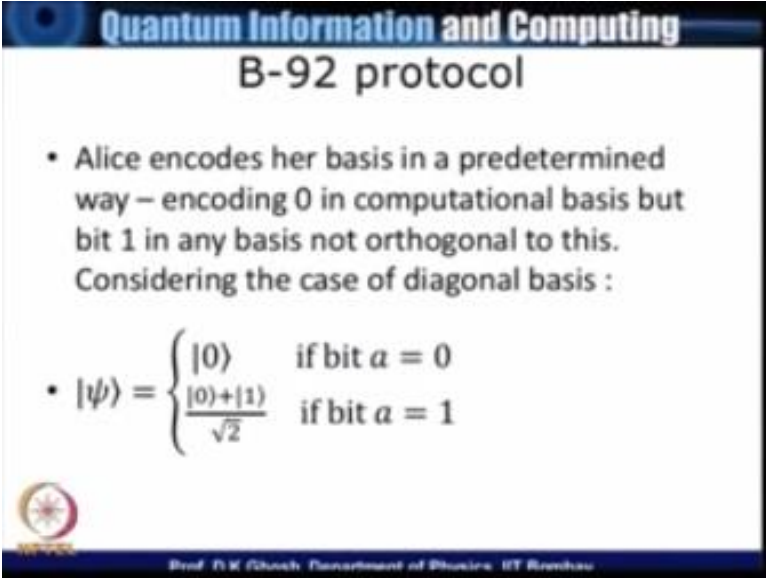
 Prof. P. K. Ghosh, Department of Physics, IIT Bombay

And after this there is in result thing up privacy amplification, now this is the idea behind the privacy amplification in this, so what Alice now that the reconciliation is there ideally we have a set of strings between Alice and Bob which are identical. Now Alice randomly picks some a subset of the strings she says as with Bob. Now what they do is, they now do a parity check on these or calculate the parity of these blocks which now they know are the same, because there is no error, error some being eliminated.

Now the parity they calculate in the various blocks, now they become their secret key instead of the string that was already sent this is the principle of privacy amplification. So this is roughly what BB84 protocol says. However it turns out that BB84 protocol is not all that security process in spite of all that we have said, because our assumptions has been that Eve uses randomly the same set of basis as Alice said Bob use for doing her measurement when she interrupts it can be shown that there are basis in which Eve can make a measurement which will make a much bigger difference to this whole process and she can get a huge amount of information.

By using such basis we will not have time to discuss it, but we will do those in one of the assignments that we will give along with this course. Having discussed BB84 protocol we focus our attention on alternative protocols internet, one of them is known as a B92 protocol.


(Refer Slide Time: 17:26)



Quantum Information and Computing
B-92 protocol

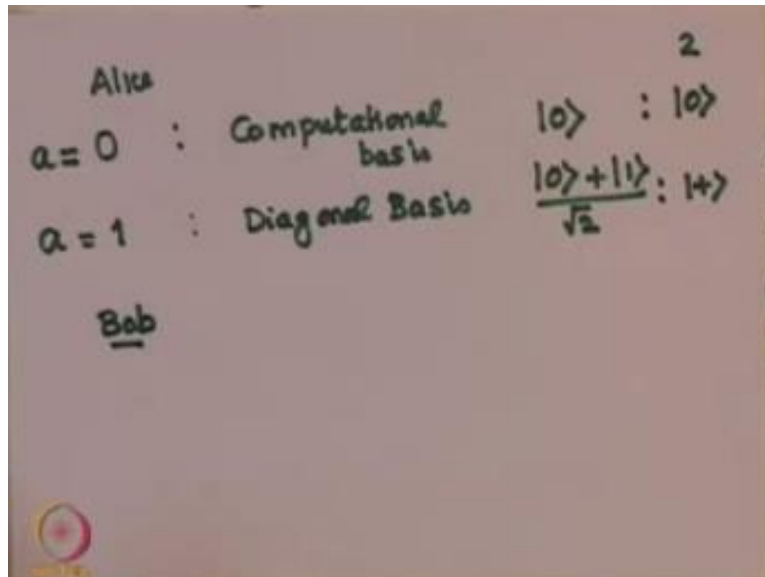
- Alice encodes her basis in a predetermined way – encoding 0 in computational basis but bit 1 in any basis not orthogonal to this. Considering the case of diagonal basis :

$$\bullet |\psi\rangle = \begin{cases} |0\rangle & \text{if bit } a = 0 \\ \frac{|0\rangle + |1\rangle}{\sqrt{2}} & \text{if bit } a = 1 \end{cases}$$


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

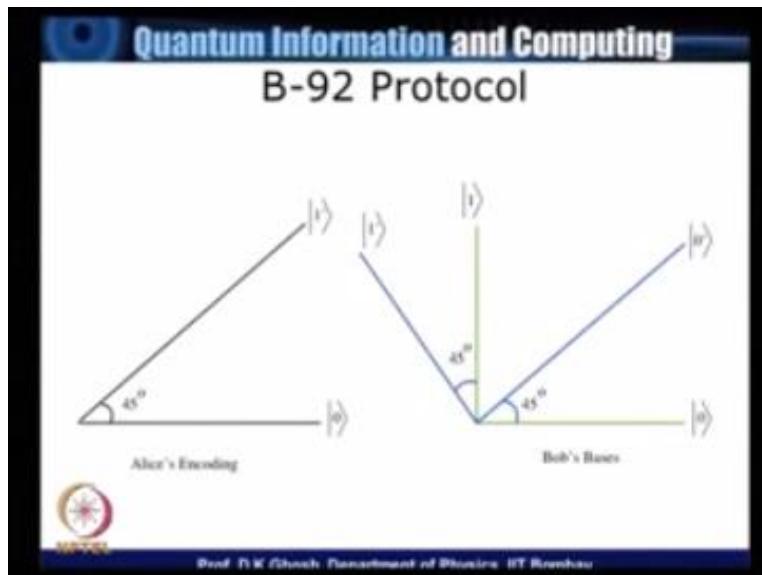
And the B92 protocol works like this, in this case Alice encodes her bits in a predetermined manner. Remember, in BB84 protocol she have encoded them by basis which she decided on the basis of a random coin toss, but she does not do that. What she does is supposing she wants to encode.

(Refer Slide Time: 17:54)



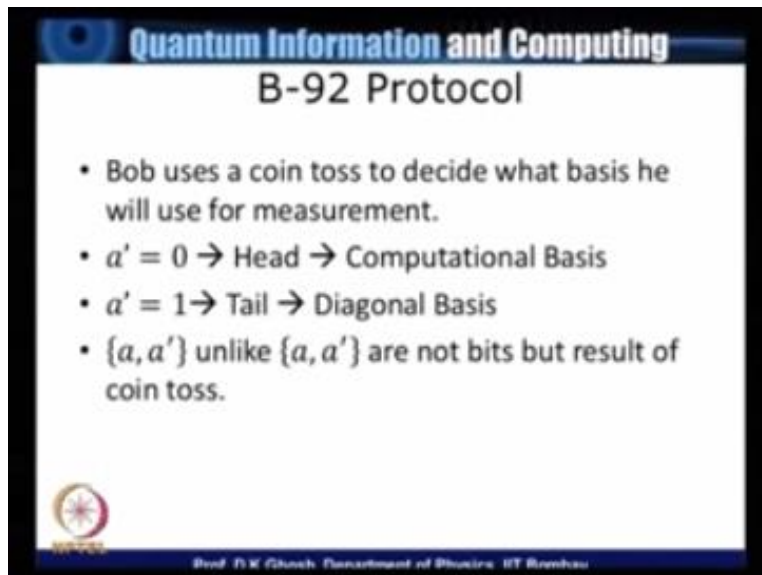
Bit 0 she will use a computational basis and encode this bit 0 as the state 0 so this is I will call it a, $a = 0$ Alice is bit now if see once to encode a bit one see when not use the vertical basis this all horizontal as was used in this previous but see when you the diagonal basis and code it as $0 + 1/\sqrt{2}$ namely as $=$ and this is the bit so these are to this now what Bob have is the following this is shown in this picture.

(Refer Slide Time: 19:01)




They look at the slide the left hand side picture shows the encoding that Alice now Bob have a set of basis for basis which you have written on 0 1 0 time now look at this flips so the Bob 0 is parallel to Alice but you notice one thing that Bob has the other basis there is 0 prime there which Bob has used which is parallel to Alice of 1 it is encoded as ϕ and perpendicular to this picture are the other two basis.

(Refer Slide Time: 19:54)



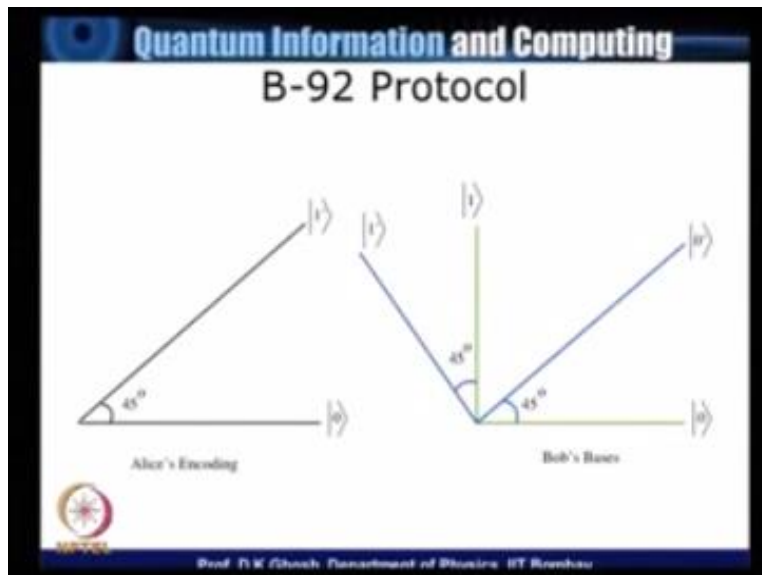
Quantum Information and Computing
B-92 Protocol

- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.


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

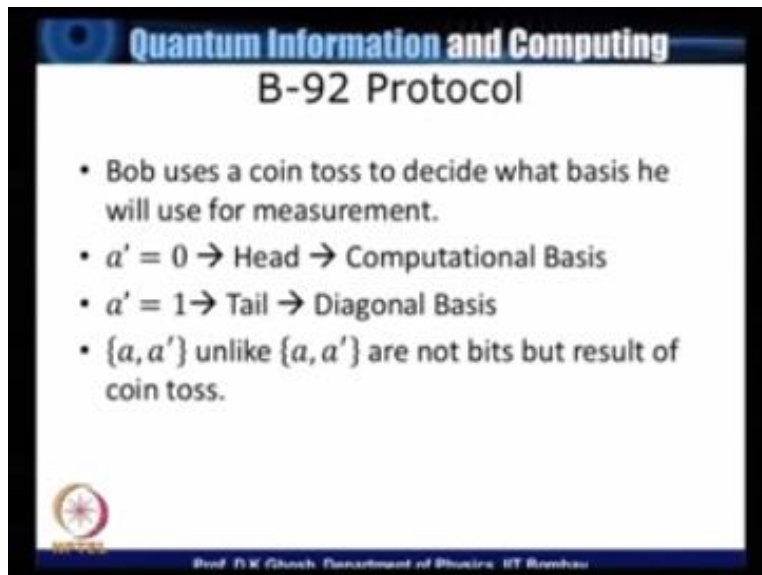
So what that does is Bob uses as a coin and decide quick basis he will use for measurement now remember.

(Refer Slide Time: 20:04)



In this picture $|0\rangle$ is the computation for Bob and $|0\rangle$ prime $|1\rangle$ prime is a diagonal basis arc Bob so based on a quantum Bob will use either a horizontal vertical basis or a diagonal now let us look at what happen if Alice.


(Refer Slide Time: 20:32)



Quantum Information and Computing

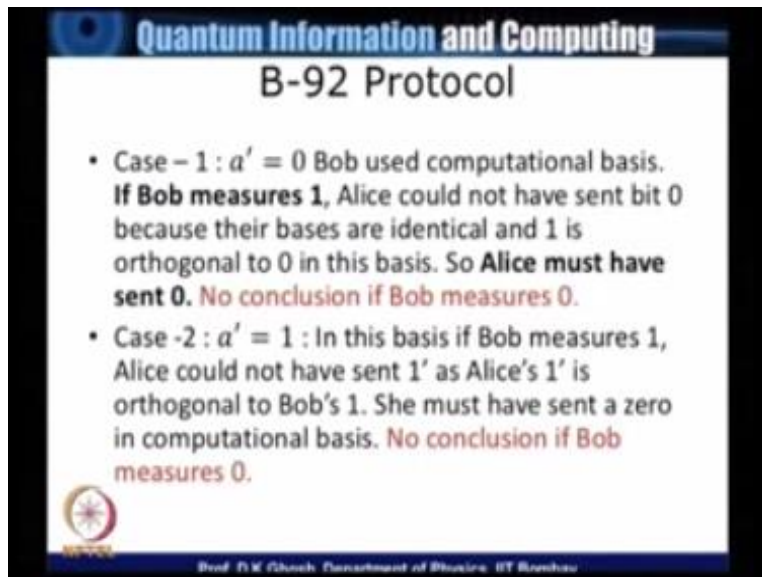
B-92 Protocol

- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.



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

(Refer Slide Time: 20:36)



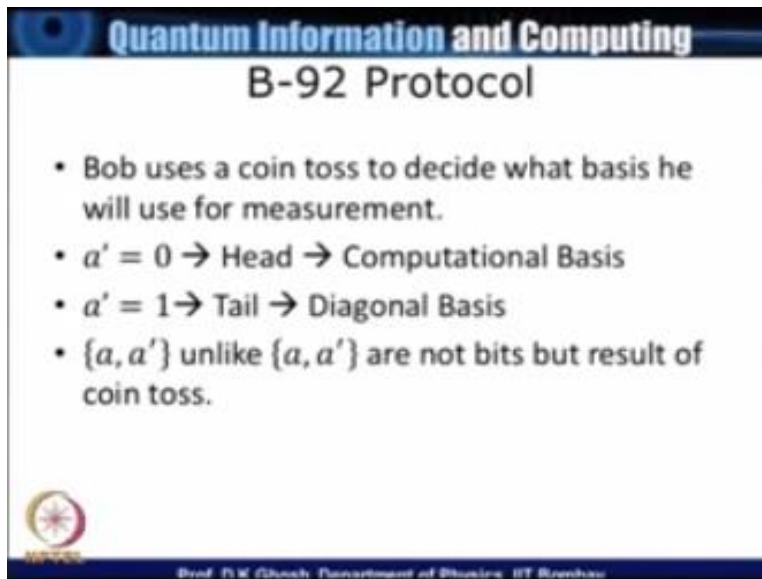
Quantum Information and Computing
B-92 Protocol

- Case - 1 : $\alpha' = 0$ Bob used computational basis. **If Bob measures 1**, Alice could not have sent bit 0 because their bases are identical and 1 is orthogonal to 0 in this basis. So **Alice must have sent 0**. **No conclusion if Bob measures 0**.
- Case -2 : $\alpha' = 1$: In this basis if Bob measures 1, Alice could not have sent 1' as Alice's 1' is orthogonal to Bob's 1. She must have sent a zero in computational basis. **No conclusion if Bob measures 0**.

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

Now look at the first page suppose Bob is computational basis okay now Bob in the computational basis would we there either 0 so let us look at the picture again.


(Refer Slide Time: 20:53)



Quantum Information and Computing

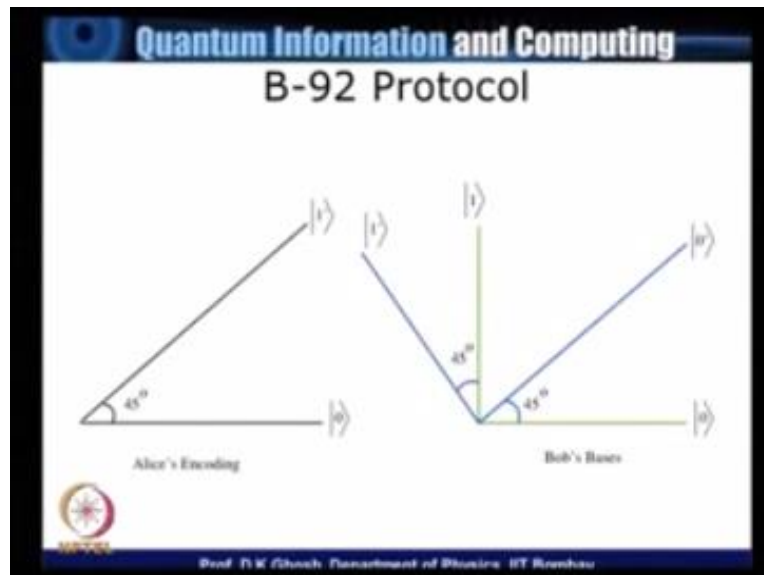
B-92 Protocol

- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.



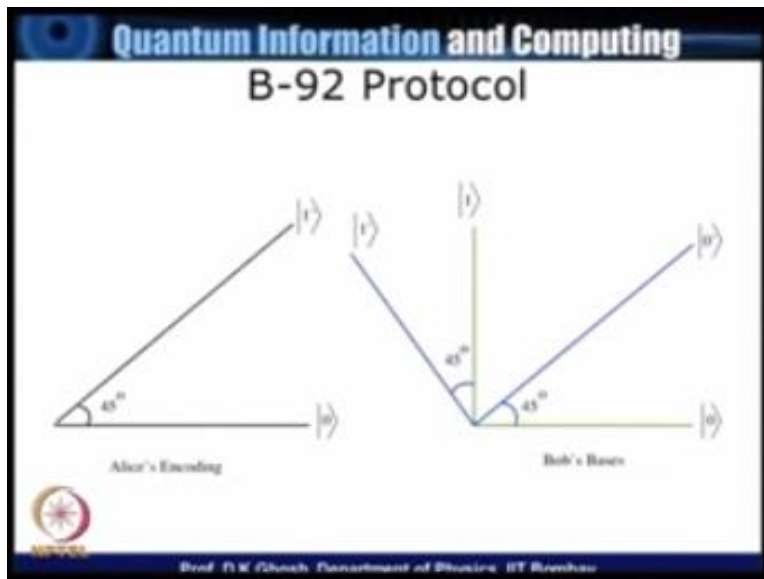
Prof. P. K. Ghosh, Department of Physics, IIT Bombay

(Refer Slide Time: 20:53)

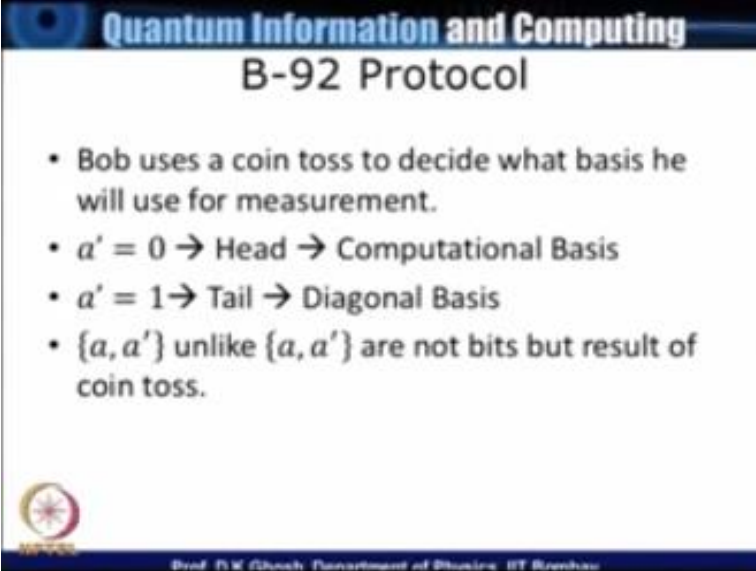


Now if in the computational basis which is 0 and 1 suppose Bob measures 1 now notice in that case Alice could not have used or Alice could not have some because in this particular case Alice's basis and bob basis where highlight and say the bit 0 is perpendicular to the bit 1 in this space when the bob measured one Alice could not have sent the so we must have sent she must have sent.

(Refer Slide Time: 21:38)




(Refer Slide Time: 21:39)



Quantum Information and Computing
B-92 Protocol

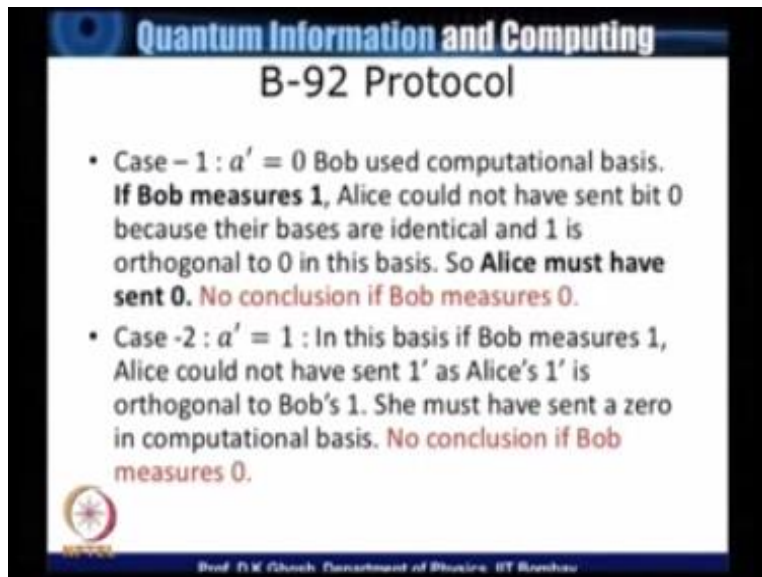
- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.



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

In the case second case.

(Refer Slide Time: 21:40)



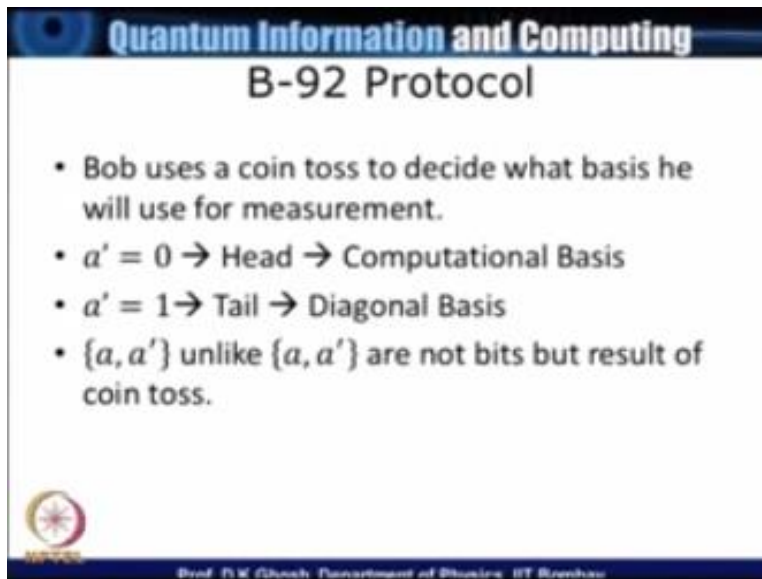
Quantum Information and Computing
B-92 Protocol

- Case - 1 : $\alpha' = 0$ Bob used computational basis. **If Bob measures 1**, Alice could not have sent bit 0 because their bases are identical and 1 is orthogonal to 0 in this basis. So **Alice must have sent 0**. **No conclusion if Bob measures 0**.
- Case -2 : $\alpha' = 1$: In this basis if Bob measures 1, Alice could not have sent 1' as Alice's 1' is orthogonal to Bob's 1. She must have sent a zero in computational basis. **No conclusion if Bob measures 0**.

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

Suppose the basis that Bob has chosen is diagonal and bob measures 1 again now gain if you look at the picture.


(Refer Slide Time: 21:54)



Quantum Information and Computing

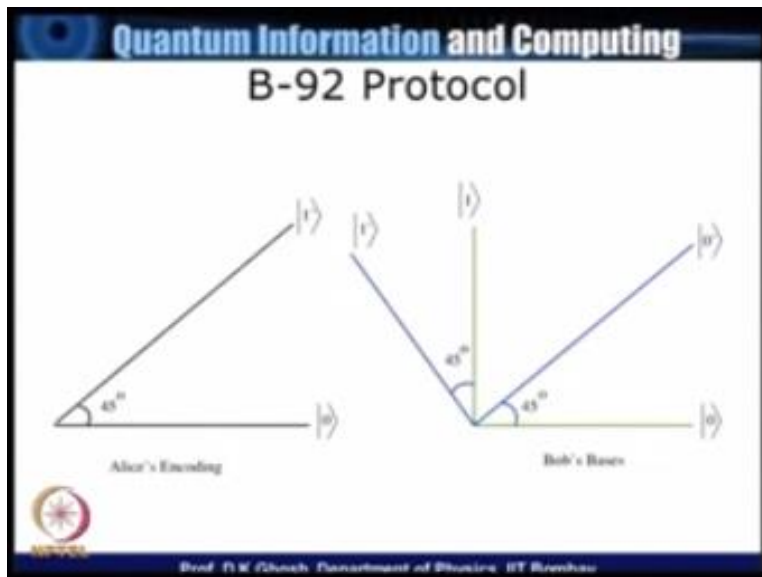
B-92 Protocol

- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.



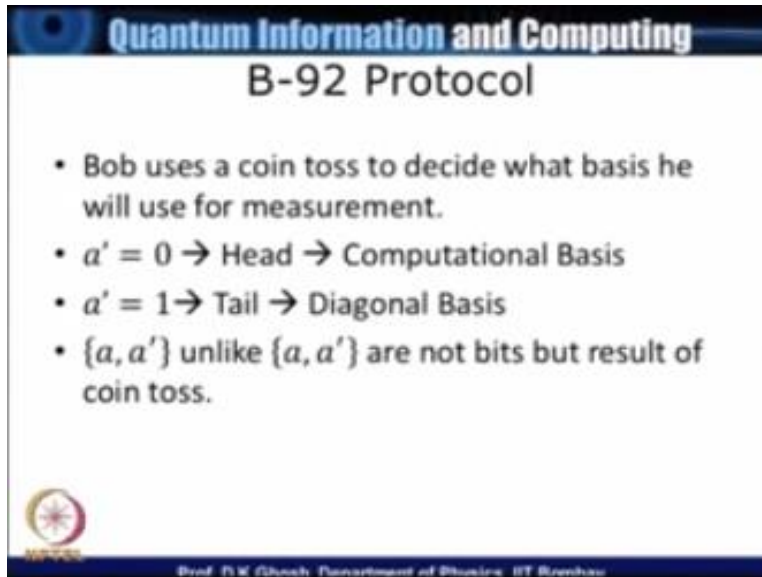
Prof. P. K. Ghosh, Department of Physics, IIT Bombay

(Refer Slide Time: 21:55)



In the diagonal basis which is shown by blue line in this picture supposing bob measures 1 a bob measures 1 Alice could not have sent 1 because the this is perpendicular to that the one point here is perpendicular to the one point that so therefore Alice must have opposite.


(Refer Slide Time: 22:23)



Quantum Information and Computing

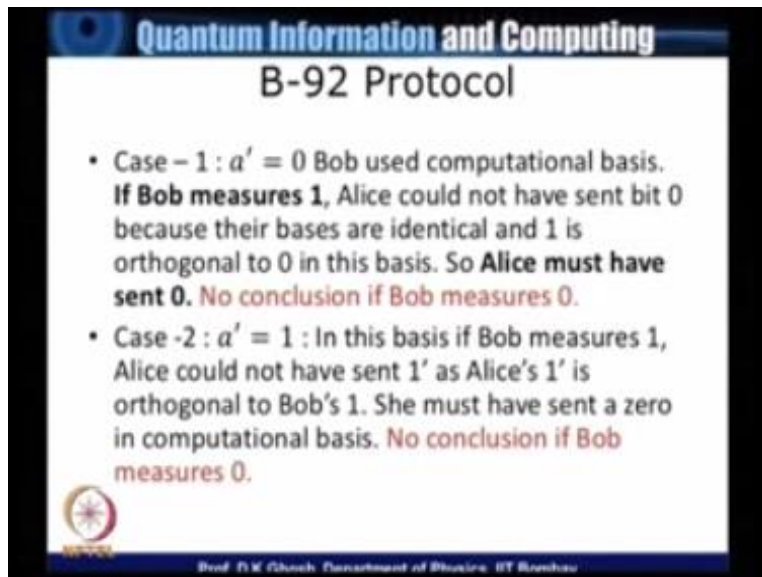
B-92 Protocol

- Bob uses a coin toss to decide what basis he will use for measurement.
- $a' = 0 \rightarrow$ Head \rightarrow Computational Basis
- $a' = 1 \rightarrow$ Tail \rightarrow Diagonal Basis
- $\{a, a'\}$ unlike $\{a, a'\}$ are not bits but result of coin toss.



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

(Refer Slide Time: 22:26)



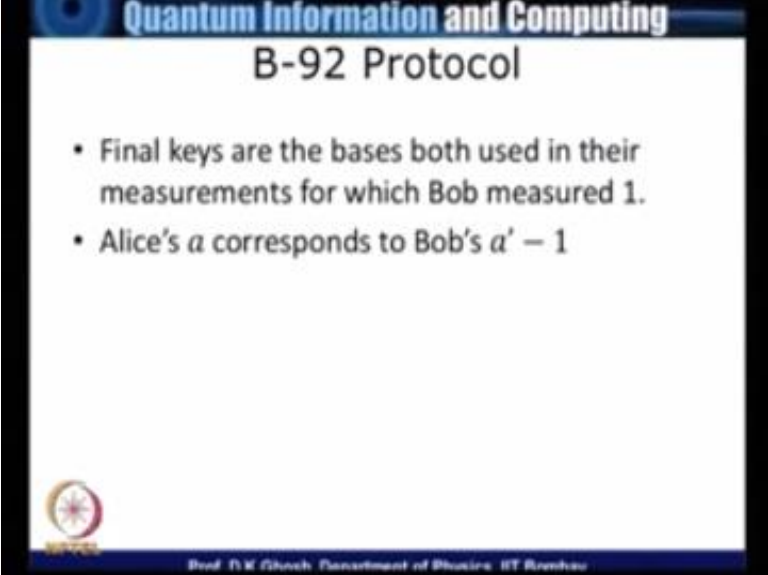
Quantum Information and Computing
B-92 Protocol

- Case - 1 : $\alpha' = 0$ Bob used computational basis. **If Bob measures 1**, Alice could not have sent bit 0 because their bases are identical and 1 is orthogonal to 0 in this basis. So **Alice must have sent 0**. **No conclusion if Bob measures 0**.
- Case -2 : $\alpha' = 1$: In this basis if Bob measures 1, Alice could not have sent 1' as Alice's 1' is orthogonal to Bob's 1. She must have sent a zero in computational basis. **No conclusion if Bob measures 0**.

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

So therefore now notice in either case if bob measures 0 or well in that case is if bob measures 0 no computational basis so what happens now is that we have definite conclusion if bob measures one now when bob measures one.

(Refer Slide Time: 22:48)



The slide is titled "Quantum Information and Computing" in a blue header bar. Below the header, the title "B-92 Protocol" is centered. The main content consists of two bullet points. In the bottom left corner, there is a small circular logo. In the bottom right corner, there is a small text credit: "Prof. D.K. Ghosh, Department of Physics, IIT Bombay".

Quantum Information and Computing

B-92 Protocol

- Final keys are the bases both used in their measurements for which Bob measured 1.
- Alice's a corresponds to Bob's $a' - 1$

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

Measures one then decide the final keys will be the basis which bob in their measure or which bob measured one towards the original bits are not the keys Alice's a corresponds to bob with and that becomes basis so that is the content of we are going to talk about on more protocol and that is what is known as Eckert protocol.

(Refer Slide Time: 22:25)

Quantum Information and Computing

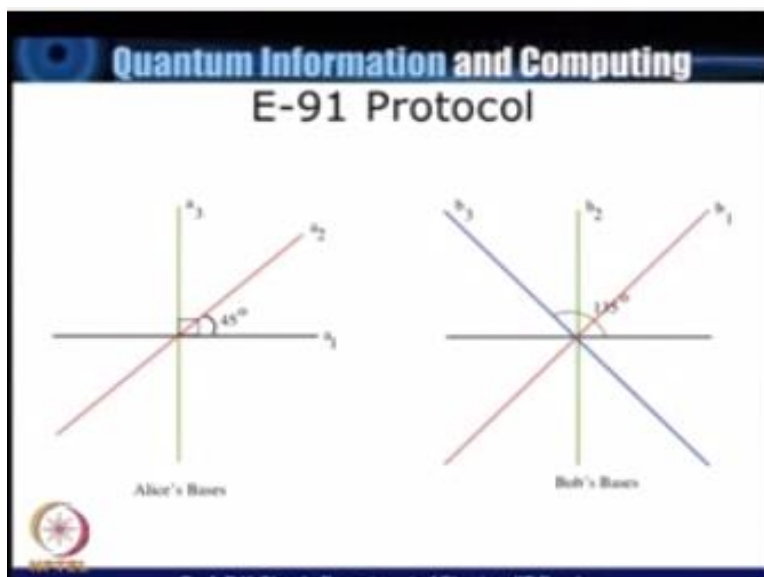
Eckert Protocol (E-91) using EPR Pair

- In this protocol Charlie prepares an EPR pair and sends one qubit each to Alice and Bob.
- $|\psi\rangle = \frac{|0A\rangle|1B\rangle - |1A\rangle|0B\rangle}{\sqrt{2}}$
- $|0\rangle$ and $|1\rangle$ correspond to spin up and spin down states of a spin 1/2 particle.
- Alice and Bob use three coplanar axes to measure the spin of the particle coming towards them.

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

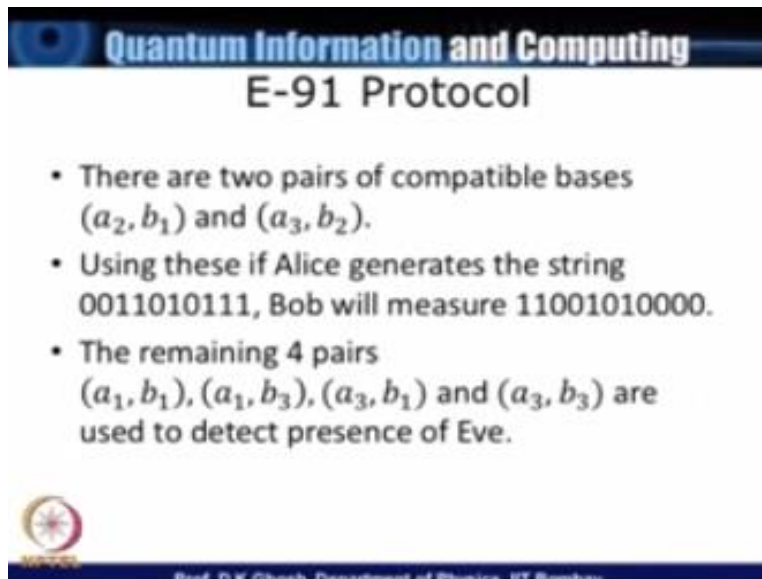
The Eckert protocol uses an EPR pair. The EPR pair will be used to detect the present category in the in this case Alice does not prepare a bit but instance if the third person Charlie prepares the bit and see he prepares it as an EPR pairs and having prepared it for example as $01 - 10$ he said to I qubit the first qubit to Alice which is marked in the state with an A and the second qubit to B we have discussed this state in detail in many of our lecture, so here our 0 as we know corresponds to spin up and one corresponds to spin down of a spin of particle. Now what will happen is here Alice and Bob will use three coplanar in our axes to measure the spin up the particle. Now let us look at what happens.

(Refer Slide Time: 24:41)




So these are the coplanar axes that we have I have indicated this axes by A_1 A_2 and A_3 , and B_1 B_2 and B_3 , now let us look at.

(Refer Slide Time: 24:55)



Quantum Information and Computing
E-91 Protocol

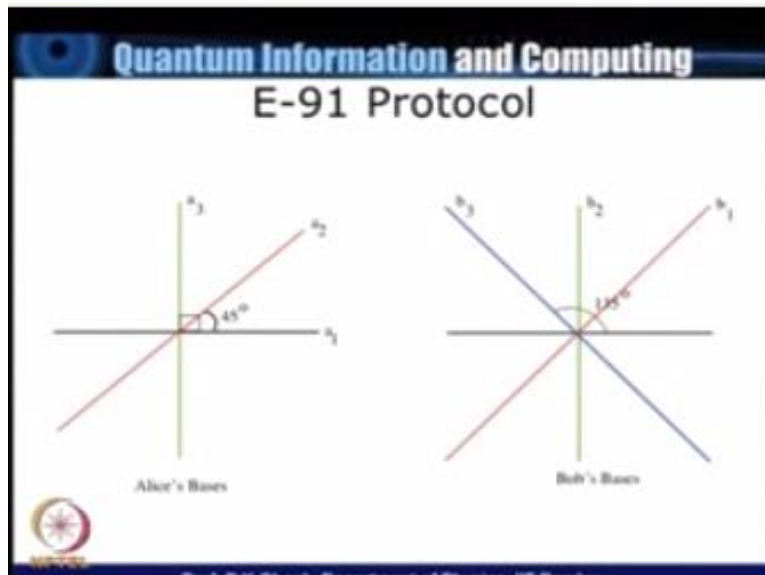
- There are two pairs of compatible bases (a_2, b_1) and (a_3, b_2) .
- Using these if Alice generates the string 0011010111, Bob will measure 11001010000.
- The remaining 4 pairs (a_1, b_1) , (a_1, b_3) , (a_3, b_1) and (a_3, b_3) are used to detect presence of Eve.



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

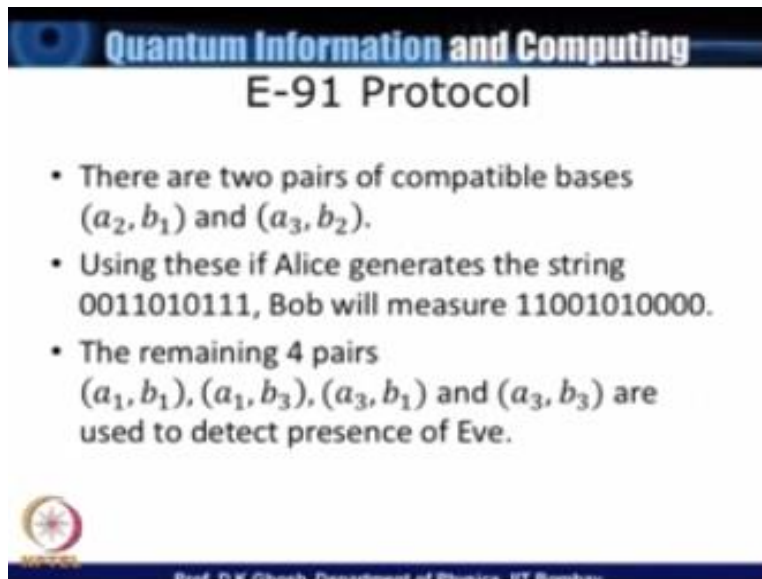
What is acting on here now notice in this case.

(Refer Slide Time: 24:59)




There are two compatible axes so what I am done is A_2 there and B_1 there the second one is B_2A_3 in one and B_2 in them.

(Refer Slide Time: 25:14)



Quantum Information and Computing
E-91 Protocol

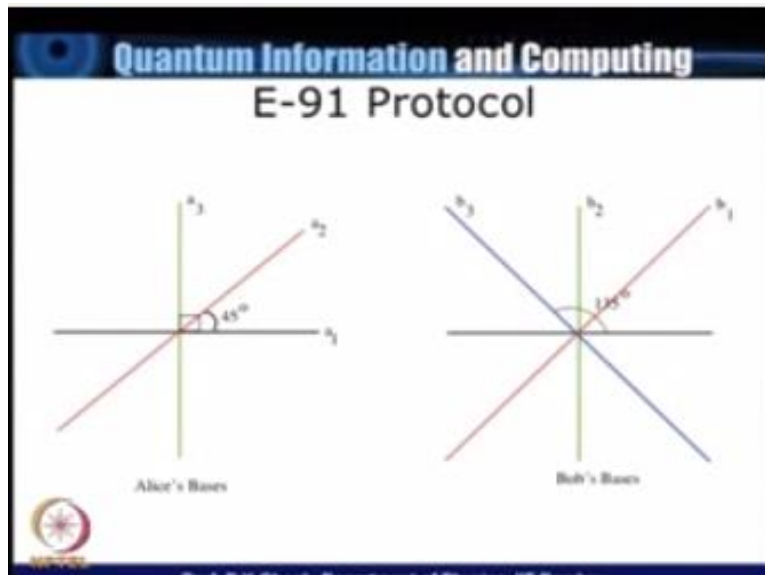
- There are two pairs of compatible bases (a_2, b_1) and (a_3, b_2) .
- Using these if Alice generates the string 0011010111, Bob will measure 11001010000.
- The remaining 4 pairs (a_1, b_1) , (a_1, b_3) , (a_3, b_1) and (a_3, b_3) are used to detect presence of Eve.



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

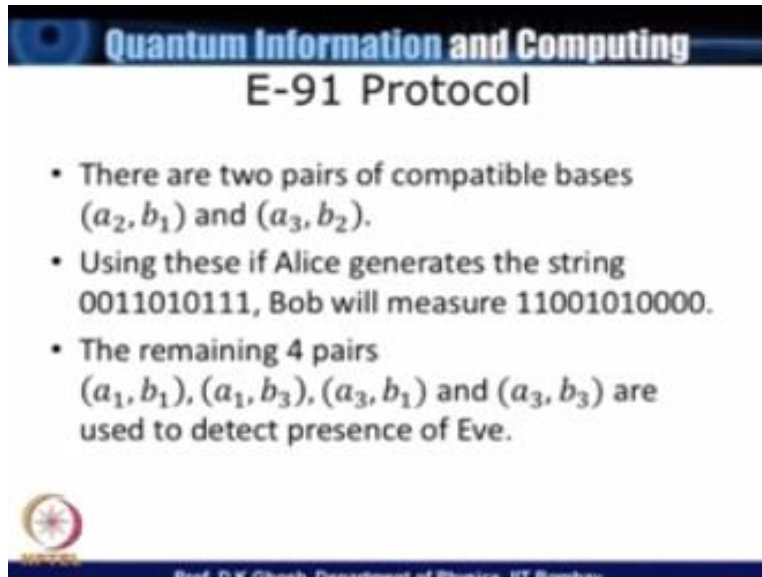
So these are compatible basis in the sense that suppose Alice generates using one of these basis 0011010111 the Bob will measure the complementary string and you can see why.

(Refer Slide Time: 25:34)




See supposing or Alice use.

(Refer Slide Time: 25:42)



Quantum Information and Computing
E-91 Protocol

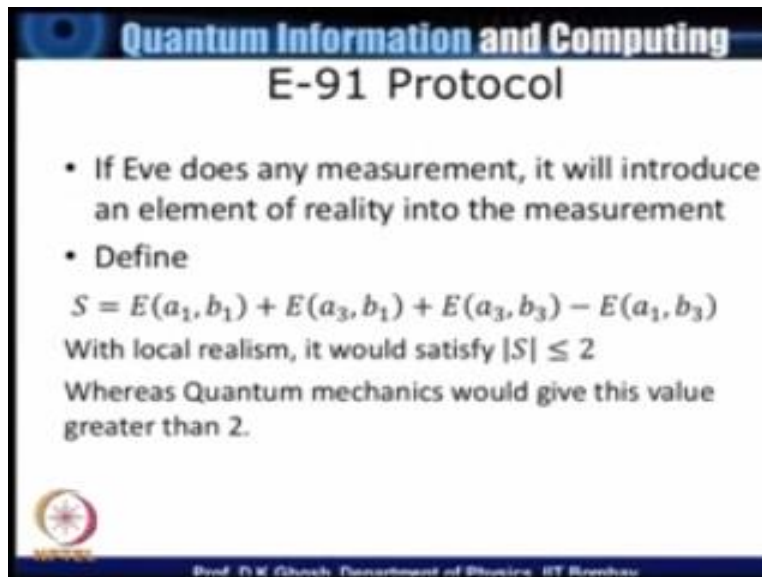
- There are two pairs of compatible bases (a_2, b_1) and (a_3, b_2) .
- Using these if Alice generates the string 0011010111, Bob will measure 11001010000.
- The remaining 4 pairs (a_1, b_1) , (a_1, b_3) , (a_3, b_1) and (a_3, b_3) are used to detect presence of Eve.



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


Where talking about a pair let us say A_2B_1 .

(Refer Slide Time: 25:44)



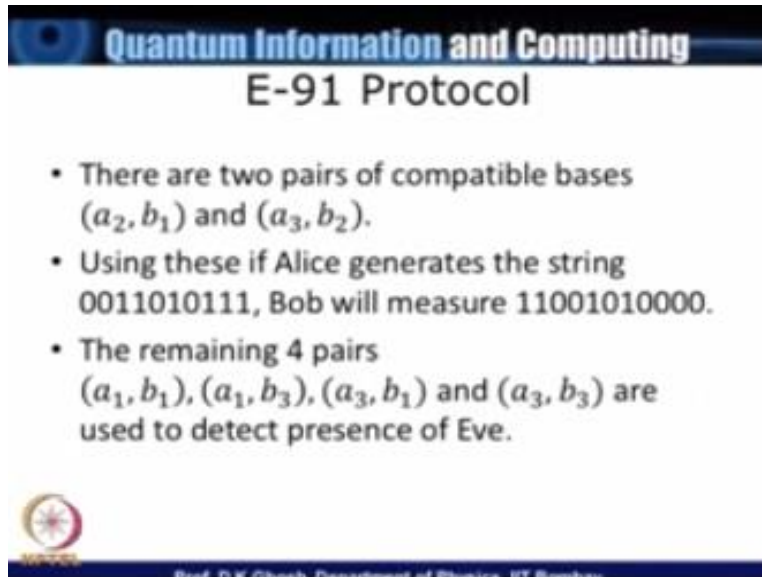
Quantum Information and Computing
E-91 Protocol

- If Eve does any measurement, it will introduce an element of reality into the measurement
- Define
$$S = E(a_1, b_1) + E(a_3, b_1) + E(a_3, b_3) - E(a_1, b_3)$$
With local realism, it would satisfy $|S| \leq 2$ Whereas Quantum mechanics would give this value greater than 2.




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

(Refer Slide Time: 25:45)



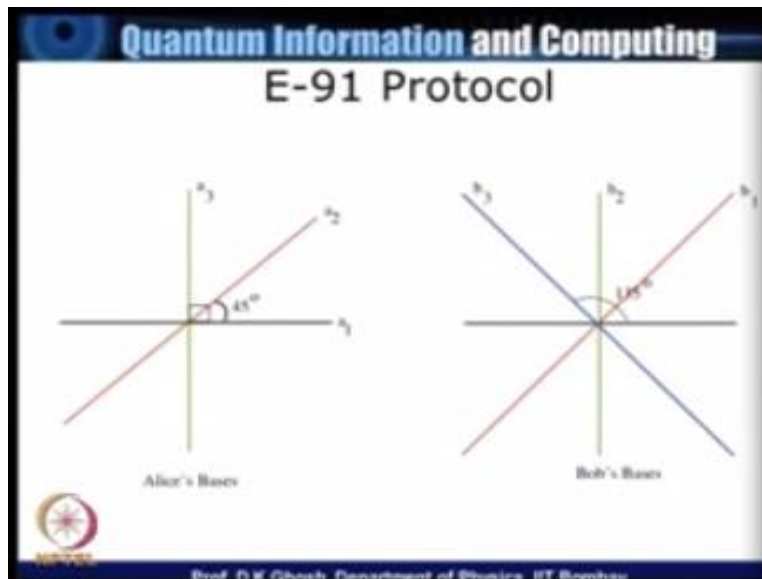
Quantum Information and Computing
E-91 Protocol

- There are two pairs of compatible bases (a_2, b_1) and (a_3, b_2) .
- Using these if Alice generates the string 0011010111, Bob will measure 11001010000.
- The remaining 4 pairs (a_1, b_1) , (a_1, b_3) , (a_3, b_1) and (a_3, b_3) are used to detect presence of Eve.



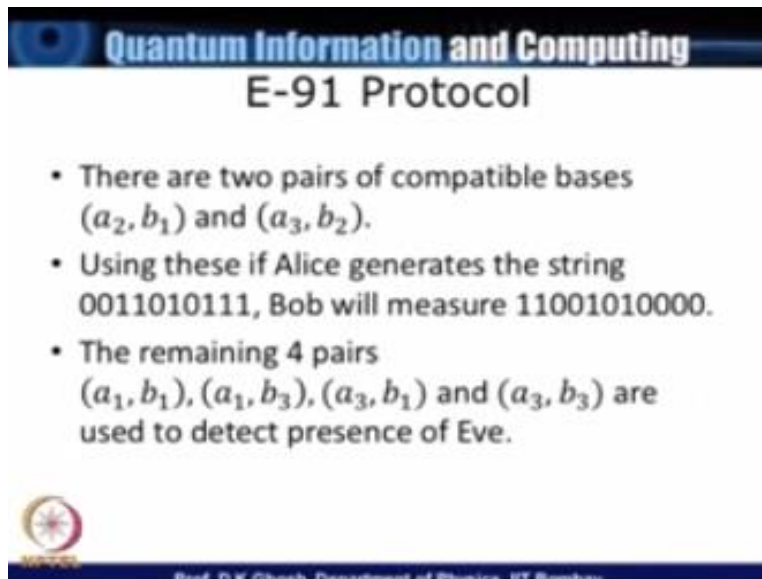
Prof. D.K. Ghosh, Department of Physics, IIT Bombay

(Refer Slide Time: 25:45)




So look at A_2 which is shown there and B_1 is shown there okay so in this case what happens was this that whatever Alice sends.

(Refer Slide Time: 26:00)



Quantum Information and Computing
E-91 Protocol

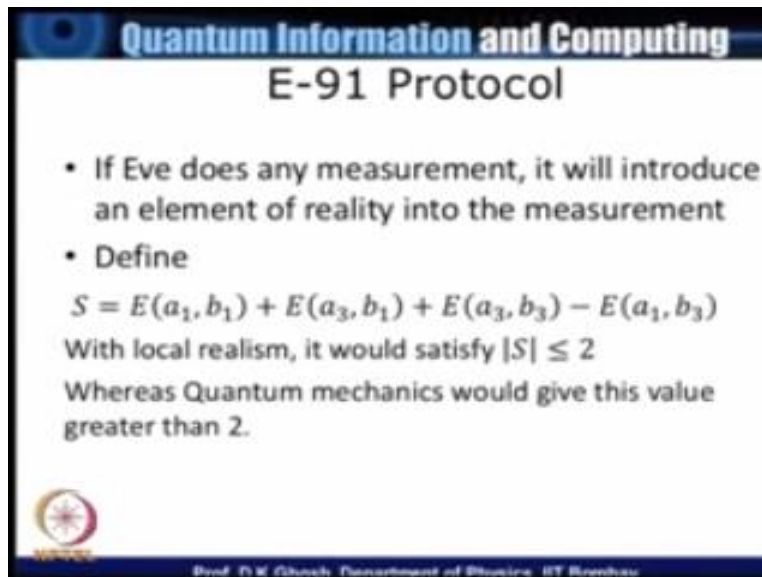
- There are two pairs of compatible bases (a_2, b_1) and (a_3, b_2) .
- Using these if Alice generates the string 0011010111, Bob will measure 11001010000.
- The remaining 4 pairs (a_1, b_1) , (a_1, b_3) , (a_3, b_1) and (a_3, b_3) are used to detect presence of Eve.



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

Bob will measure the complementary basis now that is still leaves us with four pair $a_1 b_1 a_1 b_3 a_3 b_1$ and $a_3 b_3$ now these four are going to be use to detect the present of Eve, how does it do it recall our.

(Refer Slide Time: 26:25)



Quantum Information and Computing
E-91 Protocol

- If Eve does any measurement, it will introduce an element of reality into the measurement
- Define
$$S = E(a_1, b_1) + E(a_3, b_1) + E(a_3, b_3) - E(a_1, b_3)$$
With local realism, it would satisfy $|S| \leq 2$ Whereas Quantum mechanics would give this value greater than 2.

Prof. Dr. W. (Dr.) Choudhury, Department of Physics, IIT Bombay

EPR Bell inequalities so suppose Eve does not interfere then of course whatever we have said is true but suppose there is then interference by Eve and Eve acts in other, what she actually does is to introduce an element of reality into the measurement. We define a quantity S as I shown here in the slide where e stands for expectation value that each one has the same as using those axes.

We have seen that if you had a local realism these expectation values the module of supply would satisfied what we call that is as the $C_h S_h C_h S_h = 2$ and it should have been less and equal to 2, on the other hand because we are talking about quantum states the in the absence of an element of reality we have seen that this quantity for the state that have be given so that been 2 times $\sqrt{2}$.

So in other words these basis where there is no agreement Alice or Bob they will use for determining if there is and Eve in the system by simply calculating these acceptance value and find out whether C_h as an equality is satisfied on it, if it is satisfied then it means that there is an leave in the session. Now with week we come to the conclusion of the subject of it, conclusive

of our discussion of the subject of the program we have discuss in detail that BB84 protocol for it is simplicity.

We are not talked about various attacks that Eve can make who make some of this arguments untenable that is because the trip we have to by itself a fairly integrate subject. We have seen B92 protocol which is another variant of the same process much simpler but it turns out to be much more row bus then BIBBI85 protocol, and we have also seen a method of determine if there is an hips dropper in the system by using our ideal of EPR pares. That would give us an idea of what quantum cryptography gives all about.

**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

