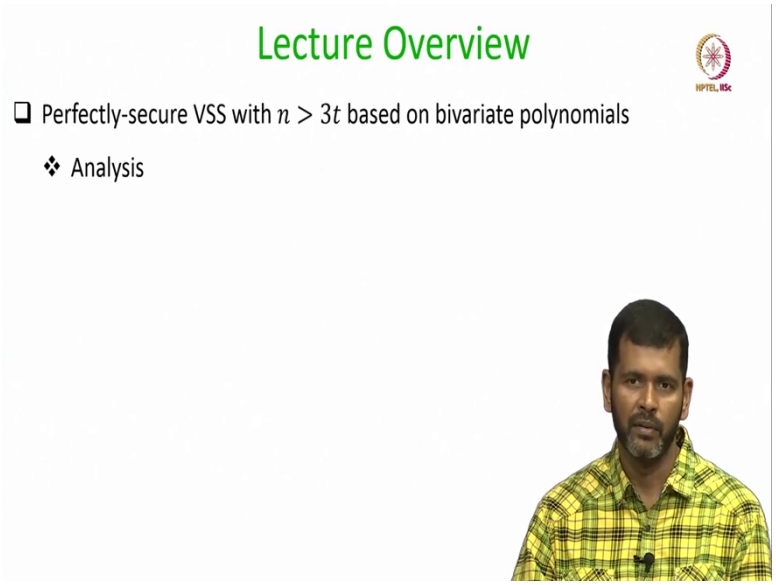
Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 40
Perfectly-Secure VSS with n Greater than 3t Part III

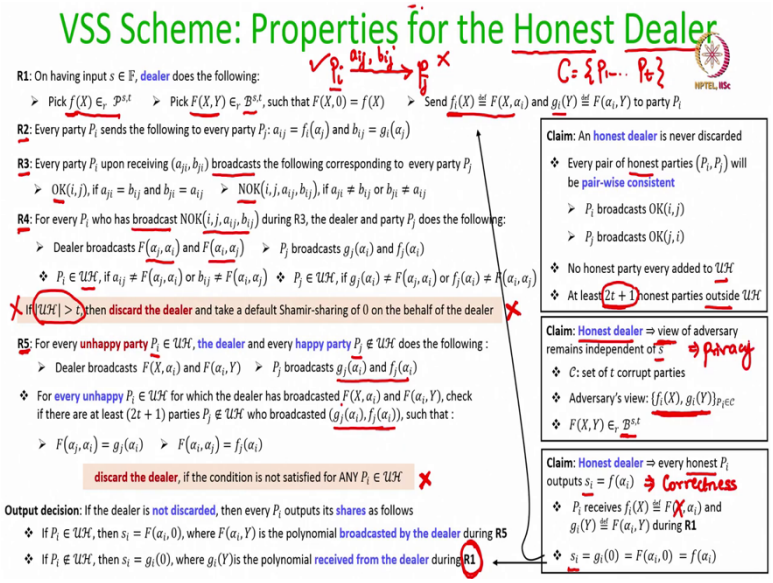
Hello everyone, welcome to this lecture.

(Refer Slide Time: 00:24)



So, in this lecture we will continue our discussion regarding the Perfectly-Secure VSS based on bivariate polynomials which we had designed in the last lecture and we will do a rigorous analysis of the protocol ok.

(Refer Slide Time: 00:39)



So, let me quickly go through the protocol steps once again. So, it is a 5 round protocol wherein the first round dealer picks a random bivariate polynomial of degree t whose constant term is the secret s. And, then it distributes the row and column polynomials to the respective parties. And, then in the rest of the protocol the parties interact and publicly verify whether the dealer has distributed consistent row and column polynomials lying on a single t degree bivariate polynomial.

So, during round 2, the parties start the pair wise consistency check between their row and column polynomials. And, the results of the pair wise consistency check are made public during the round 3 ok. So, the first and the second round everything happens over the point to point channels, no public communication happens. And, the public communication starts happening from the third round onwards.

Namely, during the third round, the results of the pair wise consistency check are made public between every pair of parties either in the form of OK messages or NOK messages. Now, for every dispute between party P i and P j which has been made public through the NOK message, the complainee, complainant and the dealer make public their respective version of the disputed points during the round four.

So, this again requires broadcast channel. Well, the complainee's version of the disputed points would have been already available through the NOK messages during round 3. The

complainant’s version and the dealer's version will be available during round 4; based on that the parties publicly decide the set of happy and unhappy parties.

And, now if there are more than t unhappy parties, then we can show that the dealer is corrupt. And, that is why it is safe to discard the dealer and terminate the sharing base protocol with some default Shamir sharing of 0, where the shares of all the honest parties will be set to 0.

But, if the number of unhappy parties is up to t, then we have this fifth round where the dealer has to ensure that even the potentially honest parties in the unhappy set, they receive their right row and column polynomials. And, this is done by asking the dealer to make public their row and column polynomials. But, to ensure that even a potentially corrupt dealer makes public the right row and column polynomials; we also ask the happy parties to make public their version of the common points on these row and column polynomials.

And, then we check whether the dealer's polynomials are pair wise consistent with at least 2 t + 1 points which are made public by the happy parties. If this condition is not satisfied, then again we can show that the dealer is corrupt. So, it is safe to discard the dealer and terminate the sharing phase protocol with some default sharing of 0. Otherwise, the parties proceed to output their shares depending upon whether they are part of the happy set or unhappy set.

If a party is a part of the unhappy set, then it takes the column polynomial which dealer has made public during round 5 and take the constant term of that polynomial as its share. Whereas, if the party is present in the happy set, then it sticks to the column polynomial which it has received during the round 1 of the protocol and output the constant term of that polynomial as it share. So, that is a 5 round protocol.

Now, we are going to prove the correctness, privacy and a strong commitment property here. So, let us first prove a bunch of properties for the case of honest dealer. So, we first claim that an honest dealer is never discarded in this protocol ok. If the dealer is honest and it follows the protocol instructions whatever steps have been assigned for the dealer, if it follows those steps honestly then it will never be discarded.

So, for this we observe that if the dealer is honest then every pair of honest parties P i and P j will be pair wise consistent. And, as a result the honest party P i will make public an OK message for P j and P j also will make public an OK message for P i. As a result, there will be

no dispute between any pair of honest P i and P j; that means, if at all there is a dispute between Pi and Pj, then it is either because P i is corrupt or P j is corrupt.

At least one of them is corrupt, assuming that the dealer is honest; that means, when the dealer will resolve the complaints during round 4 ok. Then, if the complainee is honest ok, if the complainee is honest then the dealers point, dealer's version of the disputed points will match the complainees version of the disputed points. And, the complainee and the honest complainee will not make it to the unhappy set. It will always be in the happy set.

So, no honest party will make it to the unhappy set. So, if at all there is any unhappy party, it is bound to be a corrupt party. And, how many corrupt parties we can have in the system? We can have up to t corrupt parties and as a result of this the set of unhappy parties can take the size at most t ok. So that means, for the case of an honest dealer this step, this sanity check will not pass; because there could be up to t corrupt parties in the unhappy set.

There cannot be any honest party in the unhappy set, only the corrupt parties will make it to the unhappy set. And, since there could be up to t corrupt parties, this condition will never be satisfied for the case of honest dealer. However, that is not the only sanity check. We also have another sanity check. Now, let us see whether this check passes for the honest dealer.

So, it is easy to see that this check also will not pass if the dealer is honest, because if the dealer is honest there will be at least 2 t plus 1 honest parties who will be happy, who will be outside the unhappy set. This is because all the honest parties will be outside the unhappy set; that means they are happy. That means, the polynomials which are made public by the dealer during the round 5 correspond only to corrupt parties.

So, for every such polynomial there will be $2t + 1$ honest parties outside the unhappy set whose corresponding points will also lie on the dealers polynomials, whatever polynomials dealer is making public; because dealer will be making public their polynomials correctly ok. So that means, this second sanity check will also fail if the dealer is honest and as a result an honest dealer is never discarded in the protocol.

Now, let us prove another property for the honest dealer. So, we claim here that if the dealer is honest, then the view of the adversary remains independent of the dealer's secret. So, view here means whatever information, whatever messages are seen by the adversary; that means,

whatever it has sent, whatever it has received, including its own internal randomness and whatever values it has received from the dealer and so on ok.

That means, whatever that adversary or the corrupt parties has seen throughout the protocol that is the view of the adversary. So, the claim here is that the view of the adversary is independent of the dealer secret. So, let C denotes the set of corrupt parties. For simplicity, we can assume that the set C includes the first t corrupt parties, but again this is just a simplifying assumption. It will not be always the case.

So, what exactly will be the view of the adversary throughout the protocol? The view of the adversary throughout the protocol will consist of only the row and column polynomials corresponding to those t corrupt parties, let us see why? During the first round, the t corrupt parties will receive the row and column polynomials from the dealer itself directly. So, that is included in adversary's view.

Now, during round 2, imagine party P j is corrupt and party P i is honest. Now, from P i, P j would be receiving two common points a i j, b i j. But, these points are already included in adversary's point because these points also lie also lie on P j's row and column polynomials. So that means, whatever information P j is receiving from every honest P i as part of the pairwise consistency check during the second round, that is not a new information.

That is already included in adversary's view that can be already derived from adversary's view. So that means, no new information, no new content can be added to adversary's view during round 2. Now, let us see anything new gets added to adversary's few during round 3. So, during round 3 what happens? So, every party either makes public an NOK message or NOK message, that does not tell anything about honest parties polynomials.

That means, that does not help to add anything regarding honest parties' polynomials to the adversary's view. Now, let us see if anything new gets added to adversary's view during the round 4. And, the answer is no, because even though during round 4 dealer is making public some points and complainants are making some points public, those points are already known to the adversary.

More precisely, if there is a conflict between Pi and Pj at least one of them is corrupt, because we are considering the case when the dealer is honest. And, if the dealer is honest, there would not be any conflict between any pair of honest parties.

So, if at all there is a conflict between Pi and Pj; that means, one of them is corrupt and; that means, whatever points dealer and the complainants are making public that is already known to the adversary, which can be derived from the row and column polynomials of the corrupt parties. So, this is not a new information. And, again during round 5 whatever polynomials whatever points are made public, they can be again derived from the view of the adversary itself.

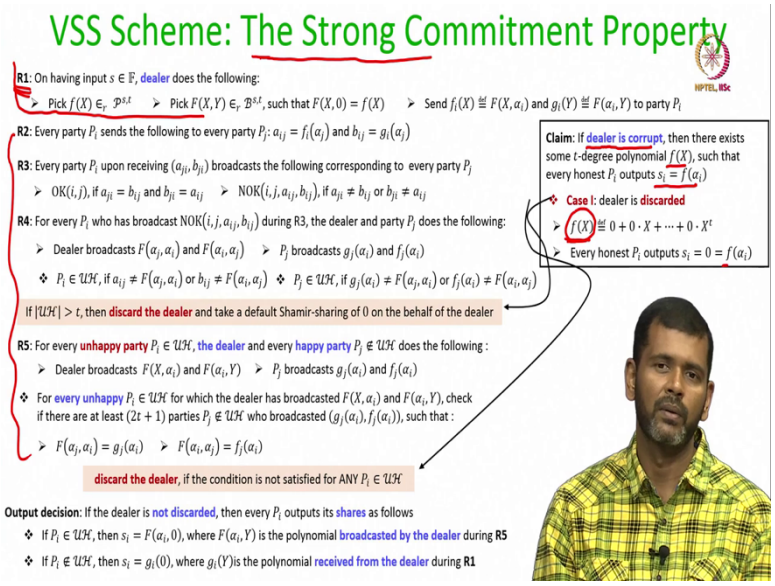
Namely, these t row and column polynomials so, that is why we can safely conclude that the view of the adversary throughout the protocol consists of at most t row and column polynomials lying on a random t degree bivariate polynomial ok. Now, we can invoke the privacy lemma which we had proved in the context of bivariate polynomials.

And, conclude that given up to t row and column polynomials derived from a random t degree bivariate polynomial, the probability distribution of those t row and column polynomials will be independent of the constant term of the bivariate polynomial and that proves this claim.

The third claim is that if the dealer is honest, then every honest party P i outputs the share s i which is the value of the Shamir sharing polynomial f(X) which the dealer has picked during round 1, at X equal to alpha i. And, this directly proves the correctness property for the VSS scheme right. So, let us see why this claim is true. So, every honest P i would have received a row and column polynomial lying on the bivariate polynomial F(X, Y) from the dealer. And, as we have shown that if the dealer is honest, every honest party will belong to the happy set. They will never be a part of the unhappy set. And, as a result every honest party will output the constant term of the column polynomial received from the dealer during round 1.

So, the share of every honest party will be this value and because of the way dealer has picked the polynomials based on its Shamir sharing polynomial and the way that Shamir sharing polynomial has been embedded in the bivariate polynomial, it is easy to see that the share si is same as the value of the Shamir sharing polynomial evaluated at X equal to alpha i. So, this automatically implies the correctness of the VSS scheme and the previous claim basically implies the privacy of the VSS scheme.

(Refer Slide Time: 15:12)



Now, let us prove the strong commitment property which was missing in the simple VSS scheme where we had just this round 1, assuming an honest dealer ok. So, recall that we started with the simpler VSS scheme which had only this round 1 and where we assume that the dealer is honest. And, for that scheme we had proved that the correctness and the privacy properties are achieved, but we also realized that the strong commitment is not achieved.

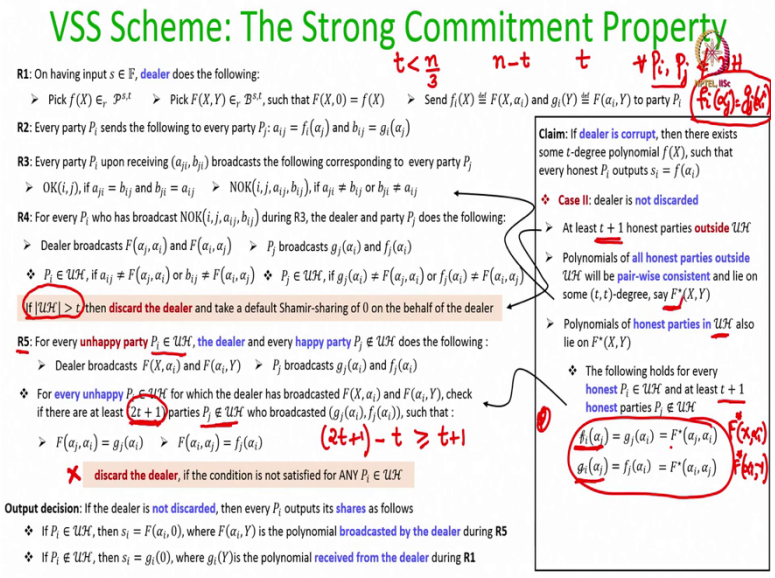
So, to achieve the strong commitment, we have now added these 4 rounds where the parties publicly verify whether the dealer has distributed consistent row and column polynomials. And, now we want to prove that because of these additional rounds where the parties are publicly verifying their respective polynomials, disputes are raised, complaints are made, complaints are resolved. Based on all these things, we will now want to show that strong commitment property is achieved, for which we have to consider a potentially corrupt dealer.

So, we want to show here that if the dealer is corrupt, then at the end of the sharing phase there exist some t degree Shamir sharing polynomial f(X) such that every honest party Pi outputs a share, which is the value of based Shamir sharing polynomial at X equal to alpha i, that is what we want to show.

If we show this property, then what we are showing is that this VSS scheme ensures that whatever an honest dealer is supposed to do, even a potentially corrupt dealer is also doing the same ok. It cannot deviate. So, there are two possible cases here for proving this claim, depending upon whether the dealer gets discarded or not in the protocol.

So, if the dealer gets discarded in the protocol, then the claim is trivial because in this case every party takes a default Shamir sharing of 0. That means, in that case we can consider the Shamir sharing polynomial to be a t degree polynomial where all the coefficients including the constant term is 0.

(Refer Slide Time: 17:47)



And, where the share of every honest party is the value 0 which is nothing but the value of this default Shamir sharing polynomial at X equal to alpha i. That means, in that case our Shamir shearing polynomial will be this t degree polynomial, where all the coefficients including the constant term is 0. Whereas, the second case for proving this claim is when the dealer is not discarded which is the trickier case.

Now, if the dealer is not discarded; that means, definitely this sanity check fails; that means, there could be up to t unhappy parties, not more than t unhappy parties. And remember, we are working in the setting where t < n/3 and there are at least n - t honest parties and up to t corrupt parties. So, if there are at most t parties in the unhappy set, then it also implies that there are at least 2t + 1 parties outside the unhappy set.

And, among those 2t + 1 parties outside the unhappy set, at least t + 1 will be honest right. Now, what we can say about the row and column polynomials of those honest parties outside the unhappy set? We can say that they are pairwise consistent. There is absolutely no dispute between the row and column polynomials of those honest parties. Namely, for every honest P

i and P j who does not belongs to the unhappy set, we can simply say that fi(X) evaluated at alpha j is same as gj(Y) evaluated at alpha i.

Because, if this condition would not have been satisfied, then there would have been a dispute between Pi and Pj and, then based on what dealer makes public during the round 4 either P i will end up in the unhappy set or P j ends up in the unhappy set. But, at the first place we are assuming that neither P i nor P j are in the unhappy set.

So, if P i and P j are outside the unhappy set; that means, there was absolutely no dispute between their row and column polynomials with respect to the supposedly common points; that means, this condition is satisfied and, as we are arguing that there are such at least t plus 1 or more number of such honest parties who are outside the unhappy set.

And since their row and column polynomials are pair wise consistent; we can now trigger the pair wise consistency lemma. And, conclude that their row and column polynomials lie on a single t degree bivariate polynomial. Let us call that bivariate polynomial as $F^{\star}(X, y)$ ok.

Now, we next claim that even the honest parties who are in the unhappy set their polynomials finally, also lie on this t degree bivariate polynomial $F^{\star}(X, y)$; let us see why. So, for every potential honest party who is present in this unhappy set, their final polynomials are the polynomials which dealer makes public during round 5. We want to argue that all those polynomials also lie on $F^{\star}(X, y)$.

Now, since the dealer is not discarded; that means, this second sanity check which the parties have verified which parties have checked at the end of round 5 passes ok. That means, whatever polynomials dealer has made public for P i during round 5, they are consistent with at least 2 t + 1 points, which are made public by the parties outside the unhappy set.

Now, among those parties P j outside the unhappy set, how many are guaranteed to be honest? At least t + 1, because the pair wise consistency check should hold with respect to 2t + 1 parties, up to t of them may be corrupt. So, at least t + 1 honest parties P j are there outside the unhappy set for which this condition would have been satisfied.

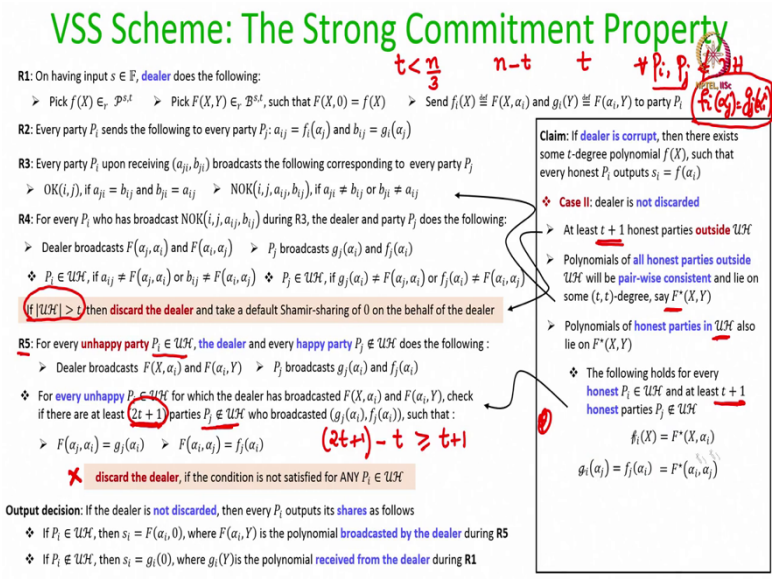
So, let us denote the polynomials which have been made public by the dealer by this small f i and small g i. So, these are the polynomials which have been made public by the dealer ok, corresponding to the party P i. And, the party P j who are honest and who are outside the

unhappy set, they would have made public these points. Now, these points which have been made public by P j, they are nothing but they are the points on the bivariate polynomial $F^{\star}(X, y)$.

Namely, the points lying on their column and row polynomials respectively and, how many such honest parties P j's outside the unhappy set are there for which this condition holds? At least t + 1, because the condition is true for 2t + 1 parties, up to t corrupt parties who are outside the unhappy set they may unnecessarily broadcast some points which are pairwise consistent with the dealer's version of the polynomials.

We ignore those points, even if we ignore those points we are guaranteed to have at least t plus 1 honest parties P j outside the unhappy set whose points match or whose points are pair wise consistent with the polynomials which dealer has made public.

(Refer Slide Time: 24:05)

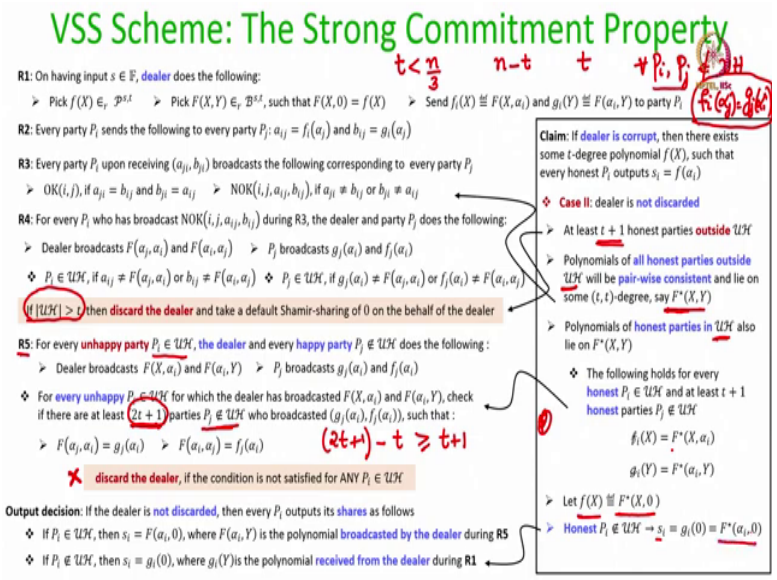


That automatically implies that whatever polynomial dealer has made public for these unhappy parties P i also lie on the $F^{\star}$ polynomial, because of this condition. And, the fact that there are t + 1 such P j's for which this condition holds. So, we cannot have two different t degree polynomials having t + 1 or more number of common points.

So, if at all this condition is satisfied; that means, we have dealers polynomial f i of x, dealers polynomial g i of y and we have this polynomials F star of X of alpha Y right. So, these points are nothing but points on F star of X of alpha i and F star of alpha i Y. So, basically we

are showing here that whatever polynomials dealer has made public, they are same as the supposedly ith row and ith column polynomial lying on this bivariate polynomial F star of X, Y ok.

(Refer Slide Time: 25:17)



So, what we have shown till now? So, we have shown we started with the fact that the polynomials of all honest parties outside the unhappy set they lie on some t degree bivariate polynomial $F^{\star}(X,Y)$. And, now we have shown that because of the sanity check which the parties are applying at the end of round 5, even a potentially corrupt dealer is forced to make public polynomials of the behalf of honest unhappy parties which also lie on the same $F^{\star}(X,Y)$ bivariate polynomial.

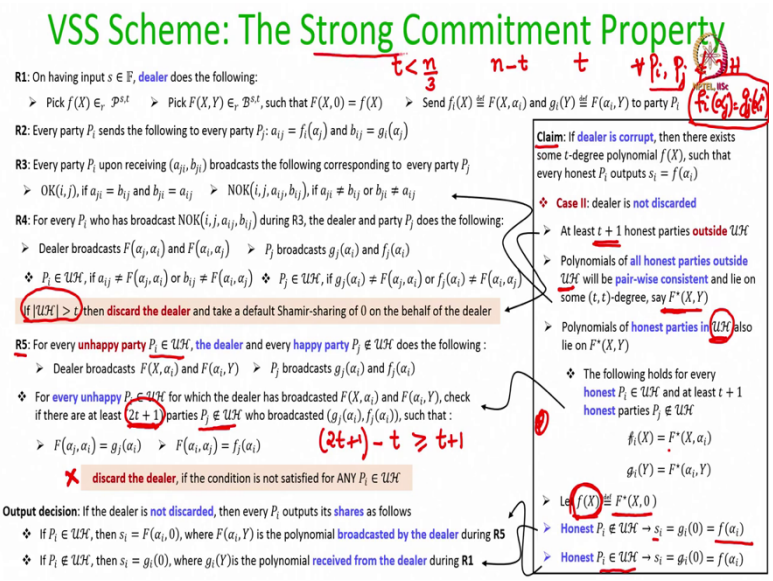
Now, let us take this polynomial $F^{\star}(X,0)$ and we call that polynomial as f(X). What was the claim statement? The claim statement was that there exists some t degree Shamir sharing polynomial such that the shares which are output by every honest party lie on that Shamir sharing polynomial. We define that Shamir sharing polynomial for the corrupt dealer to be the bivariate polynomial $F^{\star}(X,Y)$ evaluated at Y equal to 0.

So, it is guaranteed to be a t degree polynomial. This is because $F^{\star}(X,Y)$ is guaranteed to be a t degree bivariate polynomial. Now, what exactly are the shares of the honest parties? Well, it depends upon whether the honest party P i is in the unhappy set or whether it is outside the

unhappy set. If it is outside the unhappy set, then it will stick to its column polynomial and output the constant term of that column polynomial as it share.

But, we have already argued that such column polynomials $g_i(Y)$ are nothing but $F^{\star}(\alpha_i, Y)$ because we have already argued that all the column polynomials and row polynomials of the honest parties lie on $F^{\star}(X, Y)$. This automatically implies that the share s i of every P i not belonging to the unhappy set is nothing but this value.

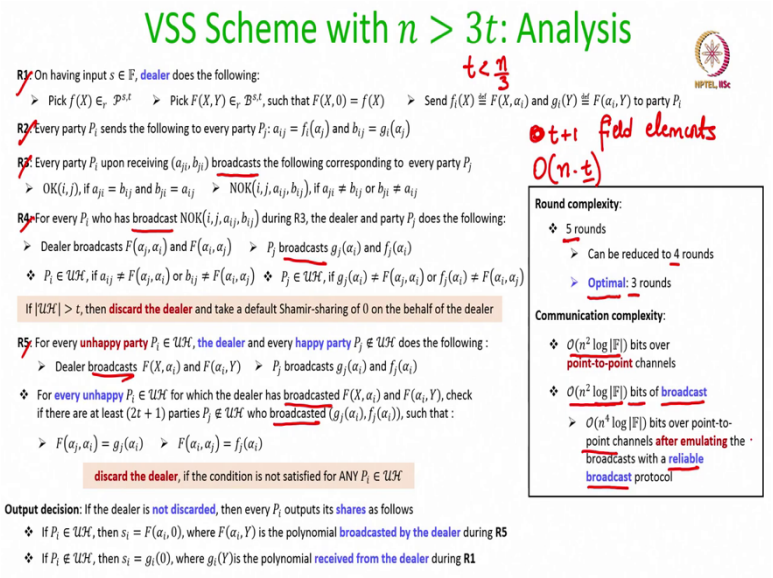
(Refer Slide Time: 27:33)



And this value is nothing but the value of our defined Shamir sharing polynomial at X equal to alpha i. Whereas, consider those honest parties P i who are unhappy, for them we have to take the dealer's version of the column polynomial made public during round 5. But, fortunately for those column polynomials also, we know that they lie on $F^{\star}(X, Y)$ as well.

So, whatever argument we have run for the honest P i outside unhappy set, we can run for the honest P i's in the unhappy set. And, we can conclude that their shares are also the evaluation of this defined Shamir sharing polynomial at X equal to alpha i. So, that concludes the proof of this claim and that also concludes the proof of this strong commitment property.

(Refer Slide Time: 28:28)



Now, let us do the complexity analysis of this VSS scheme. How many rounds are there in the protocol? We have 5 rounds here in the protocol. The first two rounds involve only communication over the pair wise channels. But, in the round 3 we have the broadcast channel invoked, round 4 also broadcast channel invoked, round 5 also broadcast channel invoked.

An interesting question is can we reduce the number of rounds? Why we are interested to reduce the number of rounds? Because, every time the parties need to interact, they have to send messages. So, if the parties are geographically very isolated, then we will prefer a protocol where the number of interactions among the parties is less.

So, in the next lecture, we will see a very cute technique to reduce the number of rounds from 5 to 4. And, one can show that the optimal number of rounds for any perfectly secure VSS scheme in the sharing phase is 3 rounds. We will not be going through the 3 round protocol because, that is quite challenging. We will see in the next lecture, a 4 round version of this current VSS scheme.

Let us do the communication complexity analysis, how much communication is done by the honest parties here. So, over the point to point channels $n^2 \log log |F|$ number of bits are communicated, because dealer has to communicate the row and column polynomials to every party single party. And, then between every pair of parties P i and P j, two values are

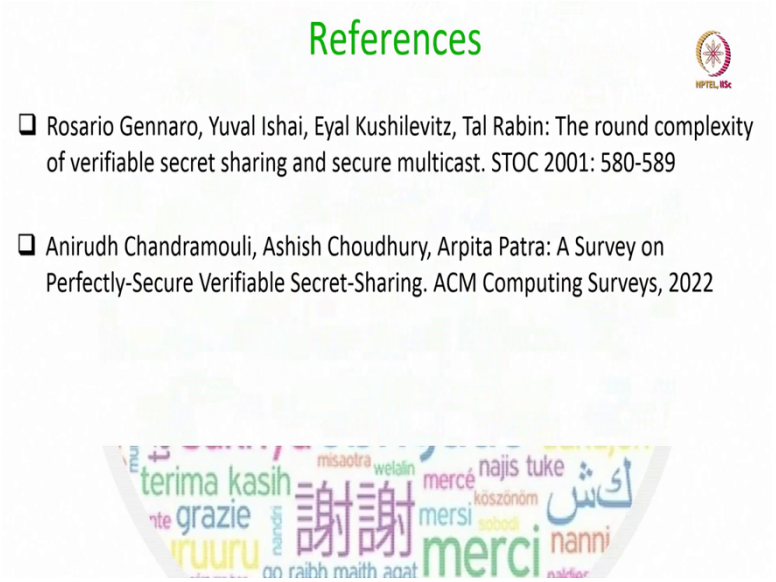
communicated over the point to point channels as part of the pair wise consistency check. So, that involves the communication over the point to point channel.

Over the broadcast channel, also we have a communication of $n^2 \log log |F|$ number of bits. This is because there could be up to t parties in the unhappy set for and for every unhappy party dealer makes public the row and column polynomials. So, the row polynomial will be a t degree polynomial. So, it will be represented by t + 1 field elements, because those will be the coefficients of the polynomial. So, t + 1 field elements.

So, altogether order of O(nt) field elements may be broadcasted by the dealer. And, since we are working with the condition t < n/3; so, asymptotically t is always O(n). So, $O(n^2)$ field elements are broadcasted and each field element can be represented by $\log log |F|$ bits. So, in terms of bits that is the amount of communication done over the broadcast channel. Recall, that to emulate one single broadcast, we can run an instance of the reliable broadcast protocol.

So, after emulating all the broadcasts in this protocol through an efficient polynomial time reliable broadcast protocol, say the phase king protocol. We get that the total communication complexity of the protocol is $n^4 \log log |F|$ bits, that is the communication over the point to point channels after emulating all the broadcast in the protocol.

(Refer Slide Time: 32:02)



So, with that I end this lecture. Now, we have perfectly secure VSS scheme with n greater than 3 t, where we can achieve the correctness and the privacy property for an honest dealer. And, also we can achieve the strong commitment property against a potentially corrupt dealer. So, these are the references used for today's lecture.

Thank you.