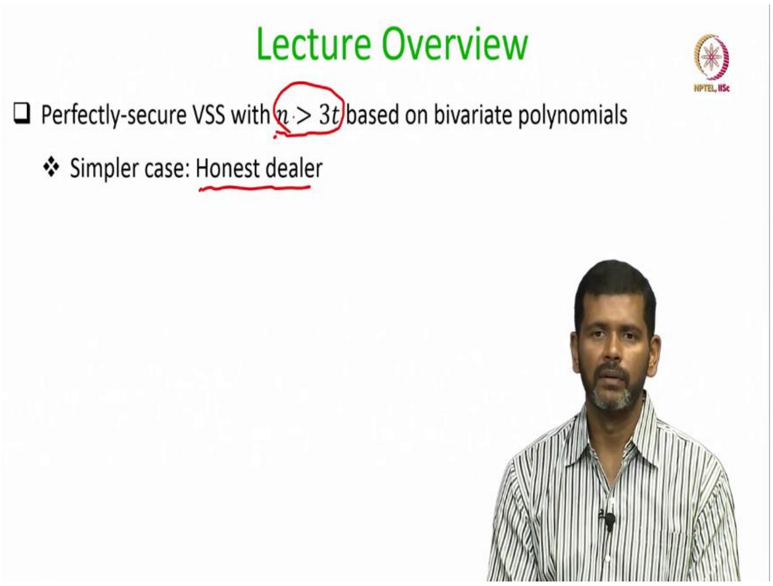
Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bangalore

Lecture - 38
Perfectly-Secure VSS with $n > 3t$: Part I

Hello everyone welcome to this lecture.

(Refer Slide Time: 00:23)



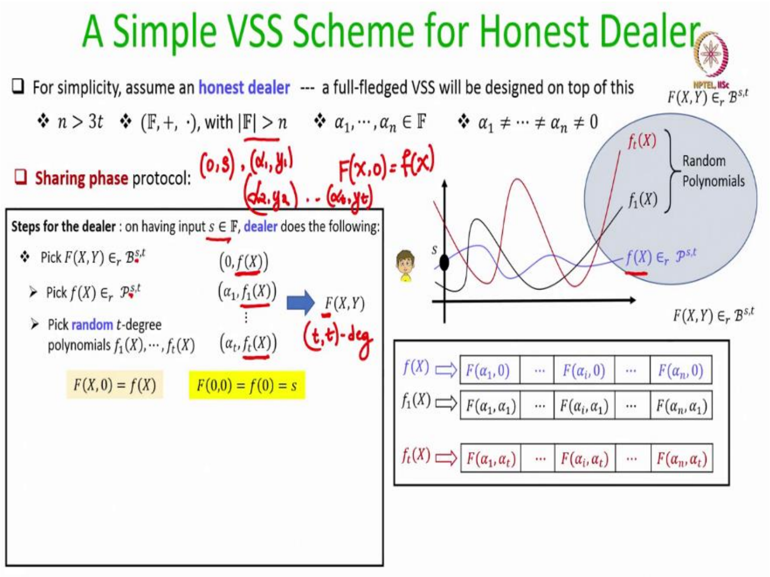
Lecture Overview

- ❑ Perfectly-secure VSS with $n > 3t$ based on bivariate polynomials
  - ❖ Simpler case: Honest dealer

So, now we have discussed a lot about the bivariate polynomials over a finite field. Using all those properties we will now start discussing about how we design a perfectly secure verifiable secret sharing. So, we will kick start with a simple setting, namely we will assume for the moment that our dealer is honest.

Later, we will design a full-fledged VSS on the top of this simple protocol, where the protocol will also take care of a potentially corrupt dealer. Our setting here will be $n > 3t$, which is a necessary condition for any perfectly secure verifiable secret sharing.

(Refer Slide Time: 01:12)



A Simple VSS Scheme for Honest Dealer

□ For simplicity, assume an **honest dealer** --- a full-fledged VSS will be designed on top of this

❖ $n > 3t$ ❖ $(\mathbb{F}, +, \cdot)$, with $|\mathbb{F}| > n$ ❖ $\alpha_1, \cdots, \alpha_n \in \mathbb{F}$ ❖ $\alpha_1 \neq \cdots \neq \alpha_n \neq 0$

□ **Sharing phase** protocol: $(0,s), (\alpha_1, y_1)$ $(\alpha_2, y_2) \ldots (\alpha_t, y_t)$ $F(x,0) = f(x)$

Steps for the dealer : on having input $s \in \mathbb{F}$, **dealer** does the following:

- ❖ Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - ➢ Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - ➢ Pick **random** t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$

$(\alpha_1, f_1(X))$

$\vdots$

$(\alpha_t, f_t(X))$

$\Rightarrow F(X,Y)$

(t,t)-deg

$F(X,0) = f(X)$ $F(0,0) = f(0) = s$

s
$f_t(X)$
$f_1(X)$
Random Polynomials
$f(X) \in_r \mathcal{P}^{s,t}$
$F(X,Y) \in_r \mathcal{B}^{s,t}$
$F(X,Y) \in_r \mathcal{B}^{s,t}$

$f(X) \Rightarrow$	$F(\alpha_1, 0)$	$\cdots$	$F(\alpha_i, 0)$	$\cdots$	$F(\alpha_n, 0)$
$f_1(X) \Rightarrow$	$F(\alpha_1, \alpha_1)$	$\cdots$	$F(\alpha_i, \alpha_1)$	$\cdots$	$F(\alpha_n, \alpha_1)$
$f_t(X) \Rightarrow$	$F(\alpha_1, \alpha_t)$	$\cdots$	$F(\alpha_i, \alpha_t)$	$\cdots$	$F(\alpha_n, \alpha_t)$

So, as I said we assume here an honest dealer and a full-fledged VSS will be designed on the top of this. We will be working with the condition $n > 3t$, we will have a finite field whose cardinality is greater than n, there will be n distinct non-zero evaluation points from the field which will be used in the VSS protocol. Now, what is the sharing phase protocol? So, since we are assuming the honest dealer, an honest dealer can do the following.

If it has an input s which it wants to secret share, and s is an element of field. What the dealer can do is, it can pick a random t-degree bivariate polynomial $F(X,Y)$ whose constant term is s. For doing that what it can do is the following, well there are several ways to pick this random t-degree bivariate polynomial. It can pick all the remaining coefficients of the bivariate polynomial, randomly accept a constant term that is one way of picking the random bivariate polynomial $F(X,Y)$.

Or it can do the following. It can first pick a random t-degree univariate polynomial in X, whose constant term is s, the secret which it wants to secret share, as it would have done in Shamir secret sharing scheme. And then it picks t more random t-degree univariate X polynomials. They are now random t degree, X univariate polynomials their constant term could be anything there is absolutely no restriction on this remaining t numbers of X univariate polynomials.

The restriction was only on the $f(X)$, polynomial its constant term is supposed to be the secret of the dealer, all other constants all other coefficients could be random. Now, it can use the Lagrange's interpolation for the bivariate polynomials, and it can interpolate a t-

degree bivariate polynomial passing through the univariate polynomials $\big(0, f(X)\big), (\alpha_1, f_1(X)), (\alpha_2, f_2(X)), \ldots, (\alpha_t, f_t(X))$, namely it can interpolate a t-degree bivariate polynomial, whose first row polynomial will be $f_1(X)$, second row polynomial will be $f_2(X)$ and the tth row polynomial will be $f_t(X)$ and when evaluated at $Y = 0$ would have given this $f(X)$ polynomial. Well, it is easy to see that this $F(X, Y)$ is a (t, t)-degree bivariate polynomial. It can be also proved that this bivariate polynomial is a randomly chosen bivariate polynomial, whose constant term is s.

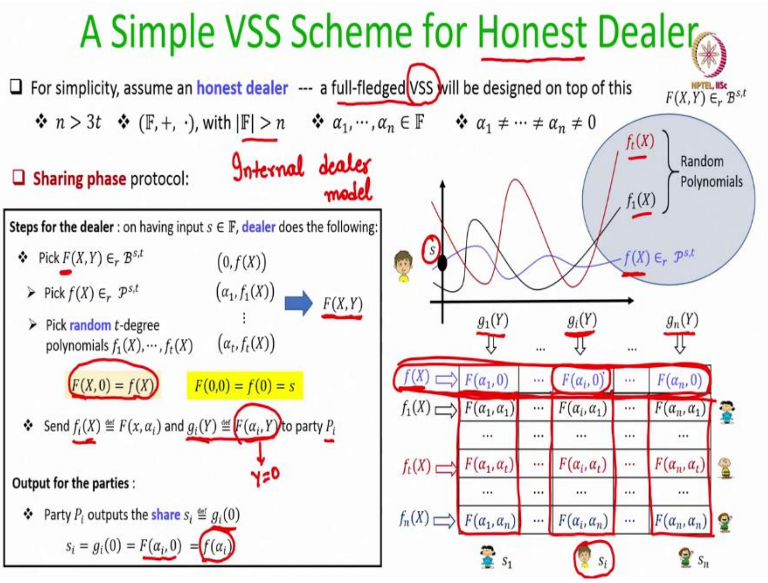
Well its constant term is s that is obvious, because $F(X, 0)$ will be $f(X)$ and; that means, $F(0,0)$ will be same as $f(0)$ and $f(0)$ is s because that is the way the dealer has chosen the polynomial. So, that is another way of picking this random bivariate polynomial. Why it is random? It can be proved very easily. So, if you want to compare it with Shamir secret sharing protocol, in the Shamir secret sharing protocol there are two ways to pick that random t-degree Shamir sharing polynomial.

Either pick the coefficients randomly except the constant term or fix the point $(0, s)$ on that polynomial and the remaining points select randomly. And then interpolate a univariate Shamir sharing polynomial, that also will lead to a random t-degree polynomial whose constant term would have been s right. So, there are two ways to pick a random t-degree univariate polynomial. Either pick the coefficients randomly or pick the points randomly. The same thing we are doing even for the case of now bivariate polynomials.

The dealer is supposed to pick a random t-degree bivariate polynomial, except that its constant term should be the secret of the dealer. Either it can do that by picking the coefficients randomly or by picking the univariate polynomials lying on that bivariate polynomial randomly, except the polynomial at $Y = 0$. That polynomial is also random except that its constant term is the secret of the dealer.

So, pictorially this is what dealer has done. Now, it is easy to see that this sharing protocol is a random randomized protocol, because if the dealer wants to share the same secret s multiple times, then it will be picking random bivariate polynomials on every occasion. It will not be picking the same bivariate polynomial every time. Now, this is the way dealer will pick its sharing polynomials, then how the shares are computed?

(Refer Slide Time: 06:53)



A Simple VSS Scheme for Honest Dealer

❑ For simplicity, assume an honest dealer --- a full-fledged VSS will be designed on top of this

❖ $n > 3t$ ❖ $(\mathbb{F}, +, \cdot)$, with $|\mathbb{F}| > n$ ❖ $\alpha_1, \cdots, \alpha_n \in \mathbb{F}$ ❖ $\alpha_1 \neq \cdots \neq \alpha_n \neq 0$

❑ Sharing phase protocol: Internal dealer model

Steps for the dealer : on having input $s \in \mathbb{F}$, dealer does the following:

- ❖ Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - ➢ Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - ➢ Pick random t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$, $(\alpha_1, f_1(X))$, ⋮, $(\alpha_t, f_t(X))$ ➡ $F(X,Y)$

$F(X,0) = f(X)$ $F(0,0) = f(0) = s$

- ❖ Send $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

$\downarrow$ Y=0

Output for the parties :

- ❖ Party P_i outputs the share $s_i \overset{\text{def}}{=} g_i(0)$

$s_i = g_i(0) = F(\alpha_i, 0) = f(\alpha_i)$

NPTEL, IISc
$F(X,Y) \in_r \mathcal{B}^{s,t}$
$f_t(X)$
$f_1(X)$
Random Polynomials
$f(X) \in_r \mathcal{P}^{s,t}$
s

	$g_1(Y)$ ⇩	…	$g_i(Y)$ ⇩	…	$g_n(Y)$ ⇩	
$f(X)$ ⇨	$F(\alpha_1, 0)$	…	$F(\alpha_i, 0)$	…	$F(\alpha_n, 0)$	
$f_1(X)$ ⇨	$F(\alpha_1, \alpha_1)$	…	$F(\alpha_i, \alpha_1)$	…	$F(\alpha_n, \alpha_1)$	
	…	…	…	…	…	
$f_t(X)$ ⇨	$F(\alpha_1, \alpha_t)$	…	$F(\alpha_i, \alpha_t)$	…	$F(\alpha_n, \alpha_t)$	
	…	…	…	…	…	
$f_n(X)$ ⇨	$F(\alpha_1, \alpha_n)$	…	$F(\alpha_i, \alpha_n)$	…	$F(\alpha_n, \alpha_n)$	
	s_1		s_i		s_n	

To the ith party, the share that is given is nothing but the ith row and ith column polynomial, on this bivariate polynomial. And we are following an internal dealer model here. So, dealer also will keep one share for itself depending upon what is the index of the dealer. Say for instance if the dealer is the ith party then it will keep the ith row and ith column polynomial with itself.

The first row and the first column polynomial will be given to the first party as the share and the nth row and the nth column will be given as the share to the nth party that is the sharing phase protocol. Now, what will be the act output of the party? The output for each party will be the ith column polynomial, which it has obtained from the dealer evaluated at 0.

That is the share, but apart from the share the dealer has given lot of other information to the respective parties. For this for the case of honest dealer, that auxiliary information may not be necessary, but as I said that later, we will design a full-fledged VSS to design to deal even with a potentially corrupt dealer on top of the simple protocol.

So, for the moment you bear with me do not worry that why such a lot of; why so much additional information is given to every party P_i, why cannot it be simply given the value $g_i(0)$ as its share. Well, if the dealer is guaranteed to be honest in the system, then we could have done that as well, but as I am saying again and again it is not necessary that in a VSS scheme the dealer is given to be honest.

We have to ensure that even a potentially corrupt dealer is following the protocol that is why we are distributing this auxiliary information. So, even though every party P_i is getting the ith row and the ith column polynomial and when I say ith row and the ith column polynomial, you can interpret that it is given the coefficients of those polynomials.

And if it is given the coefficients of those polynomial, well it can inter it can evaluate that polynomial at $\alpha_1, \alpha_2, \ldots, \alpha_n$ and get the ith row and the ith column polynomial. Or the dealer itself could have directly given the ith whole, ith row and the whole ith column of this matrix as the contribution or whatever the information party P_i is supposed to get.

Based on that information party P_i can compute $g_i(Y)$ and then evaluate it at $Y = 0$ and that would be considered as the share for the ith party. So, the first party pictorially you can interpret here as the following. So, the first party here will be getting this full highlighted column and these points are nothing but the points on g 1 of Y, then when it evaluated at $Y = 0$, then that will be the share of the first party and like that the ith party it will have this highlighted column.

The values along this highlighted column, these points are nothing but the point on $g_i(Y)$ and if it evaluates at $Y = 0$, it will get its share and in the same way the nth party it will get this highlighted column from the dealer. These are nothing but the points on this column polynomial $g_n(Y)$ and when evaluated at $Y = 0$ will give the share s_n.

Now, let us see what exactly this share s_i as computed by the ith party. So, s_i is the value of the ith column polynomial at $Y = 0$. Now, what is the ith column polynomial? The ith column polynomial is nothing but this particular Y polynomial. So, this polynomial evaluated at $Y = 0$ is nothing but the value $F(\alpha_i, 0)$ which is nothing but $f(\alpha_i)$, because that is the way dealer has picked his polynomial $F(X, Y)$ and $f(X)$.

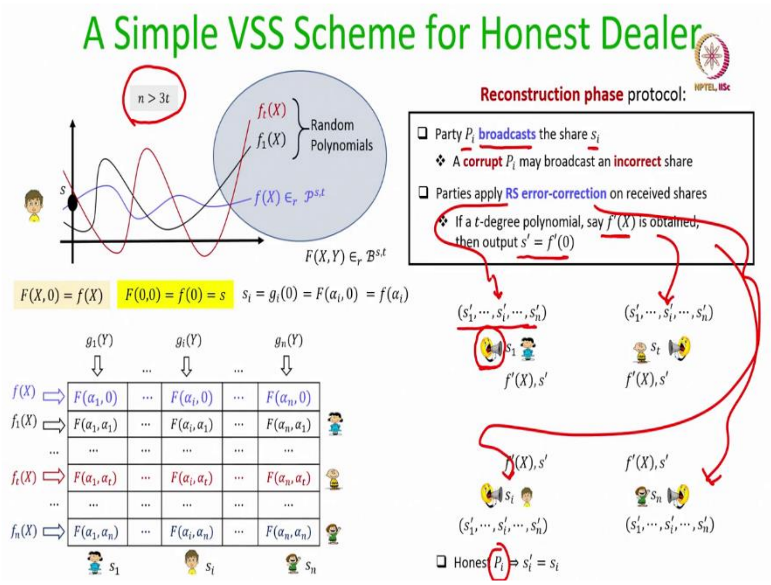
So; that means, even though the value $f(\alpha_i)$ is not explicitly given by the dealer to the ith party, it is implicitly available or it is implicitly given in the form of this polynomial $g_i(Y)$. As soon as $g_i(Y)$ polynomial is given to the ith party, the ith party can evaluate that polynomial at $Y = 0$ and that value is nothing but this value in blue color. And that value is nothing but this $f(X)$ polynomial evaluated at α_i.

So, in a sense what party P_i has done is it has computed its share as it would have got from the dealer in Shamir secret sharing protocol. In the Shamir secret sharing protocol, dealer would have chosen $f(X)$ and it would have directly given $f(\alpha_i)$ as the share to the ith party. The first party would have directly received $f(\alpha_1)$ as the share from the dealer, the second party would have directly received $f(\alpha_2)$ as the share and so on.

But now, they are not directly given $f(\alpha_1)$, $f(\alpha_2)$ respectively, but rather $g_1(Y), g_2(Y), \ldots, g_n(Y)$ which implicitly have those shares as they would have been computed in an instance of Shamir secret sharing protocol. So, what you can imagine here is that what dealer has done is, dealer is running an instance of Shamir secret sharing protocol internally implicitly.

And it is embedding a lot of information on top of that. It is wrapping a lot of information on top of that Shamir sharing polynomial. So, that Shamir sharing polynomial $f(X)$, which is the blue coloured polynomial here is embedded in a bivariate polynomial and the parties are now getting the row and column polynomials of that bivariate polynomial and implicitly in those column polynomials the Shamir shares are embedded.

(Refer Slide Time: 14:09)



A Simple VSS Scheme for Honest Dealer

$n > 3t$
$f_t(X)$
$f_1(X)$
Random Polynomials
s
$f(X) \in_r \mathcal{P}^{s,t}$
$F(X,Y) \in_r \mathcal{B}^{s,t}$
NPTEL, IISc

$F(X,0) = f(X)$ $F(0,0) = f(0) = s$ $s_i = g_i(0) = F(\alpha_i, 0) = f(\alpha_i)$

	$g_1(Y)$	⋯	$g_i(Y)$	⋯	$g_n(Y)$
$f(X)$	$F(\alpha_1, 0)$	⋯	$F(\alpha_i, 0)$	⋯	$F(\alpha_n, 0)$
$f_1(X)$	$F(\alpha_1, \alpha_1)$	⋯	$F(\alpha_i, \alpha_1)$	⋯	$F(\alpha_n, \alpha_1)$
⋯	⋯	⋯	⋯	⋯	⋯
$f_t(X)$	$F(\alpha_1, \alpha_t)$	⋯	$F(\alpha_i, \alpha_t)$	⋯	$F(\alpha_n, \alpha_t)$
⋯	⋯	⋯	⋯	⋯	⋯
$f_n(X)$	$F(\alpha_1, \alpha_n)$	⋯	$F(\alpha_i, \alpha_n)$	⋯	$F(\alpha_n, \alpha_n)$
	s_1		s_i		s_n

Reconstruction phase protocol:

- ❑ Party P_i **broadcasts** the share s_i
  - ❖ A **corrupt** P_i may broadcast an **incorrect** share
- ❑ Parties apply **RS error-correction** on received shares
  - ❖ If a t-degree polynomial, say $f'(X)$ is obtained, then output $s' = f'(0)$

$(s'_1, \cdots, s'_i, \cdots, s'_n)$
s_1
$f'(X), s'$
$(s'_1, \cdots, s'_i, \cdots, s'_n)$
s_t
$f'(X), s'$
$f'(X), s'$
s_i
$(s'_1, \cdots, s'_i, \cdots, s'_n)$
$f'(X), s'$
s_n
$(s'_1, \cdots, s'_i, \cdots, s'_n)$

❑ Honest $P_i \Rightarrow s'_i = s_i$

So, this is the sharing, this is the sharing phase protocol. Now, what will be the reconstruction phase protocol? Well, every party P_i can make public its share s_i and when I say broadcast well, it is not a reliable broadcast it is not invoking an instance of reliable broadcast, but rather sending the share over the point-to-point channel to every other party. So, the party P_i will send its share to every other party.

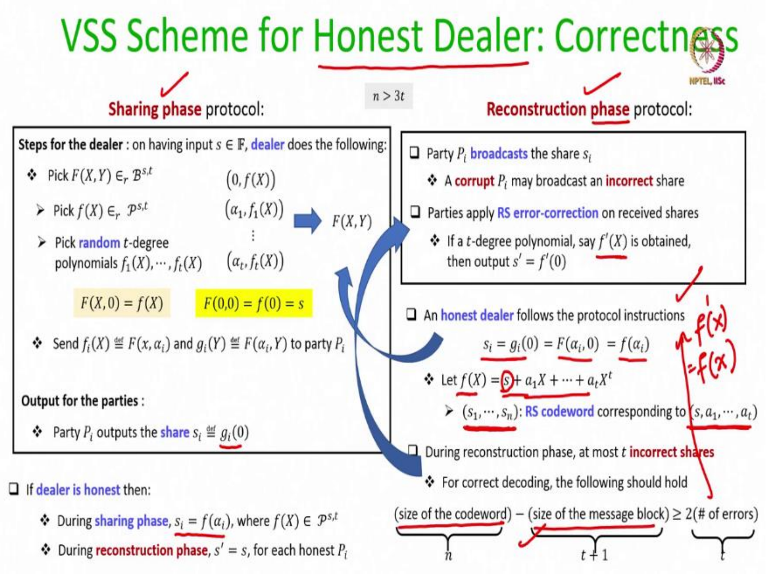
Even though I am using this notation or this picture of reliable broadcast that need not be the case, well the parties can use instances of reliable broadcast as well to make public their shares, but that is not necessary since we are working with the setting of $n > 3t$. Later on, we will see that it is sufficient even if the parties send their shares over the point to point channels directly to everyone.

So, the honest party, if P_1 is honest say for instance it will send its share s_1 identically to everyone, but if P_1 is corrupt it may send different versions of s_1 to different honest parties that is fine. So, we denote the vector of shares received by all the parties as $s'_1, s'_2 \ldots, s'_i, \ldots, s'_n$ and so on. And what we know here is that if the party P_i is honest and whatever he has broadcasted, whatever share he has broadcasted is the correct share.

So, up to t shares among these n shares could be incorrect. And the parties will not be knowing the exact identity of the t corrupt parties. So, to reconstruct the dealer secret, what the party can do is the following. It can apply Reed-Solomon error correction on the received shares. So, for instance P_1, will apply the Reed-Solomon error correction.

P_2 also, will apply Reed-Solomon error correction, P_i also will do the same every party will be doing locally the Reed-Solomon error correction. And after Reed-Solomon error correction, if a t-degree polynomial is obtained say $f'(X)$, then take the constant term of that $f'(X)$ polynomial as the output. That is the reconstructed secret, whether that secret reconstructed secret is correct or incorrect we will argue soon.

(Refer Slide Time: 16:42)



VSS Scheme for Honest Dealer: Correctness

$n > 3t$

Sharing phase protocol:

Steps for the dealer : on having input $s \in \mathbb{F}$, dealer does the following:

- ❖ Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - ➢ Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - ➢ Pick random t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$

$(\alpha_1, f_1(X))$

$\vdots$

$(\alpha_t, f_t(X))$

$F(X,Y)$

$F(X,0) = f(X)$ $F(0,0) = f(0) = s$

- ❖ Send $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

Output for the parties :

- ❖ Party P_i outputs the share $s_i \overset{\text{def}}{=} g_i(0)$

Reconstruction phase protocol:

- ❑ Party P_i broadcasts the share s_i
  - ❖ A corrupt P_i may broadcast an incorrect share
- ❑ Parties apply RS error-correction on received shares
  - ❖ If a t-degree polynomial, say $f'(X)$ is obtained, then output $s' = f'(0)$

- ❑ If dealer is honest then:
  - ❖ During sharing phase, $s_i = f(\alpha_i)$, where $f(X) \in \mathcal{P}^{s,t}$
  - ❖ During reconstruction phase, $s' = s$, for each honest P_i

- ❑ An honest dealer follows the protocol instructions

$$s_i = g_i(0) = F(\alpha_i, 0) = f(\alpha_i)$$

  - ❖ Let $f(X) = \boxed{s} + a_1X + \cdots + a_tX^t$
    - ➢ $(s_1, \cdots, s_n)$: RS codeword corresponding to $(s, a_1, \cdots, a_t)$

$f'(x)$

$= f(x)$

- ❑ During reconstruction phase, at most t incorrect shares
  - ❖ For correct decoding, the following should hold

$$\underbrace{\text{(size of the codeword)}}_{n} - \underbrace{\text{(size of the message block)}}_{t+1} \geq \underbrace{2\text{(\# of errors)}}_{t}$$

So, that is the VSS scheme and since it is a VSS scheme, it will have two protocols, one protocol for the sharing phase, one protocol for the reconstruction phase. So, the sharing phase protocol is based on distributing the row and column polynomials on a random t-degree bivariate polynomial and the reconstruction protocol is based on making the respective shares public followed by applying the Reed-Solomon error correction.

Now, let us prove the properties of this VSS scheme, whether it achieves the required properties or not and since we are assuming an honest dealer, for simplicity we must prove two properties, correctness and privacy. So, let us first put the correctness and just to recap what exactly is the correctness property the correctness property of the VSS demands that if the dealer is honest then the shares of all the honest parties lie on some t-degree polynomial, chosen by the dealer and that is exactly is happening here.

Because if the dealer is honest, which we are assuming to be true then during the sharing phase every party P every honest party P_i outputs the share s_i and s_i is nothing but $g_i(0)$ which we have already shown is nothing but $f(\alpha_i)$. So, there is some t-degree polynomial picked by the dealer and the share of all the honest parties indeed constitute a distinct point on that t-degree polynomial.

And during the reconstruction phase the value reconstructed by the honest parties we want to show is the same as the dealer secret. So, since we are assuming that the dealer is honest it honestly follows the protocol instructions which ensure that during the sharing phase the share of the ith party is $g_i(0)$ which, as we have argued earlier, is nothing but the point $F(\alpha_i, 0)$.

And the point $F(\alpha_i, 0)$ is nothing but $f(\alpha_i)$ because of the way the honest dealer has chosen its polynomial. Now, imagine the t-degree $f(X)$ polynomial is this polynomial, its coefficients are $s, a_1, a_2, \ldots, a_t$. Why s? Because its constant term is supposed to be s remaining all other coefficients are random coefficients. Now, we want to show that at the time of reconstruction when the reconstruction phase protocol is executed the reconstructed protocol $f'(X)$ is same as $f(X)$.

Because if we show that the reconstructed polynomial $f'(X)$ is same as $f(X)$ polynomial then that also shows that the reconstructed output s' is same as s. So, if $f(X)$ polynomial has these coefficients, then what when what can we say about the vector of shares s_1 to s_n

held by the parties P_1 to P_n? Where the now; well or the entire vector is not held by P_1 to P_n the ith component is held by the ith party.

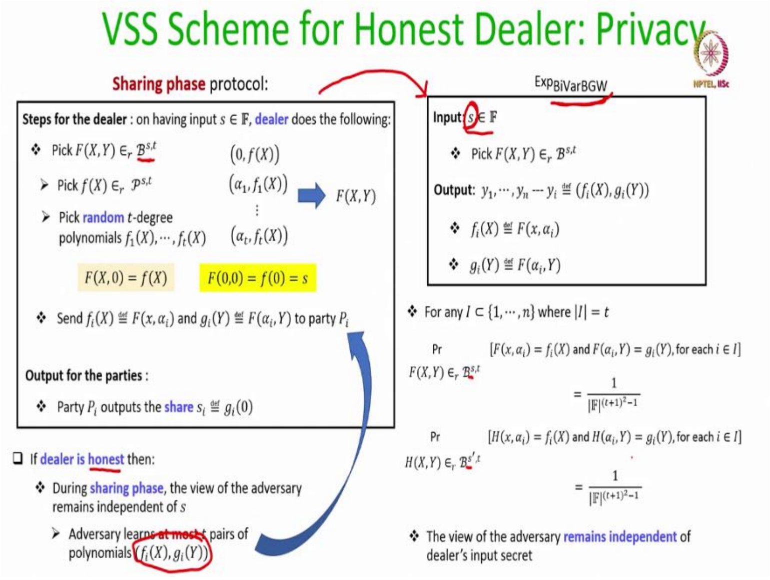
Well, the collectively this vector of shares s_1 to s_n corresponds to a Reed-Solomon code word for a message block consisting of the elements $s, a_1, \dots, a_t$. And this follows from one of our earlier discussions we had regarding the similarity between Shamir secret sharing and Reed-Solomon encoding algorithm. Now, what happens during the reconstruction phase?

During the reconstruction phase there could be at most t corrupt parties who may produce incorrect shares and we do not know what exactly the identity is, what exactly are the identity of the corrupt parties. Now, if at all we want that the reconstructed polynomial $f'(X)$ is same as the sharing polynomial $f(X)$, this relationship should hold which comes from the bound that we have in coding theory.

Namely the size of the Reed-Solomon code word minus the size of the message block should be at least 2 times the number of errors that we want to correct. Now, what is the size of the code word here? Namely, how many shares will be made public at the time of reconstruction? n number of shares and those shares basically correspond to a Reed-Solomon code word ideally, corresponding to a message consisting of $t + 1$ elements.

And how many errors might be there among those n shares which are made public at the time of reconstruction? At most t shares. So, if this relationship holds, namely $n - t + 1 \geq 2t$, then it will be guaranteed that $f'(X)$ is same as $f(X)$. Now, since we are working with the condition $n > 3t$, it automatically implies that this condition holds, and which further implies that $f'(X)$ is same as $f(X)$. So, that shows that the correctness property holds.

(Refer Slide Time: 22:08)



VSS Scheme for Honest Dealer: Privacy

NPTEL, IISc

Sharing phase protocol:

Steps for the dealer : on having input $s \in \mathbb{F}$, dealer does the following:

- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - Pick random t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$
$(\alpha_1, f_1(X))$
$\vdots$
$(\alpha_t, f_t(X))$
$\Rightarrow F(X,Y)$

$F(X,0) = f(X)$ $F(0,0) = f(0) = s$

- Send $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

Output for the parties :

- Party P_i outputs the share $s_i \overset{\text{def}}{=} g_i(0)$

□ If dealer is honest then:

- During sharing phase, the view of the adversary remains independent of s
  - Adversary learns ~~at most t~~ pairs of polynomials $(f_i(X), g_i(Y))$

$\mathsf{Exp}_{\mathsf{BiVarBGW}}$

Input: $s \in \mathbb{F}$

- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$

Output: $y_1, \cdots, y_n$ --- $y_i \overset{\text{def}}{=} (f_i(X), g_i(Y))$

- $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$
- $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$

- For any $I \subset \{1, \cdots, n\}$ where $|I| = t$

$$\Pr_{F(X,Y) \in_r \mathcal{B}^{s,t}} [F(x,\alpha_i) = f_i(X) \text{ and } F(\alpha_i, Y) = g_i(Y), \text{for each } i \in I] = \frac{1}{|\mathbb{F}|^{(t+1)^2-1}}$$

$$\Pr_{H(X,Y) \in_r \mathcal{B}^{s',t}} [H(x,\alpha_i) = f_i(X) \text{ and } H(\alpha_i, Y) = g_i(Y), \text{for each } i \in I] = \frac{1}{|\mathbb{F}|^{(t+1)^2-1}}$$

- The view of the adversary remains independent of dealer's input secret

Now, let us prove the privacy property. And what we want to show regarding the privacy here? The privacy property of the VSS scheme demands that if the dealer is honest, then during the sharing phase the view of the adversary corrupting up to t parties excluding the dealer. Why excluding the dealer? Because we are arguing privacy only for the case when dealer is honest if dealer is corrupt well in that case the secret s and the entire distribution of information is known to the adversary.

So, if at all dealer is honest, we want to argue that during the sharing phase the view of the adversary should remain independent of the dealer's secret. And why only till sharing phase? Because anyhow during the reconstruction phase the secret s will be publicly reconstructed. Now, is it guaranteed in this protocol that now information about the secret s is learned during the sharing phase? So, how much information adversary learns in this sharing phase protocol? Well, it learns at most t pairs of row and column polynomials, on the dealer's bivariate polynomial.

And what is the dealer's bivariate polynomial? Dealer's bivariate polynomial is a random t-degree bivariate polynomial with its secret being the constant term. Now, let us relate this sharing phase protocol with the BGW experiment based on bivariate polynomials which we had discussed in the last lecture. What was happening in that experiment? In that experiment also there was a secret, which was the input and to generate the output a random t-degree polynomial was chosen and the ith output consists of the ith row and the ith column polynomial on that bivariate polynomial.

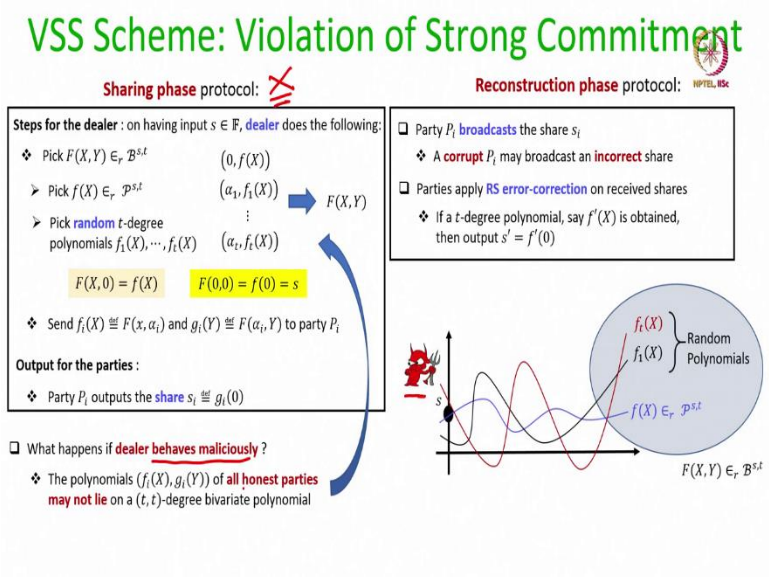
And in the context of this experiment, we had argued in the last lecture that the probability distribution of any t pairs of output row and column polynomials is independent of the input of this experiment. That means, if someone gets to see t row and column polynomials from this experiment, then from the viewpoint of that observer it could be the case that the experiment has been run with input s, with the same probability with which the input would have been run with input s'.

It cannot that observer cannot distinguish apart whether the t pairs of row and column polynomials which had has seen corresponds to input s or correspond to input s'in the experiment. And that is why the view of that observer will remain independent of the input of the experiment. Now, what exactly is happening in this sharing phase protocol?

In this sharing phase protocol, we are precisely running this BGW bivariate based experiment. What exactly is dealer doing? Dealer is basically running this experiment only. And what the adversary would have seen in the sharing phase protocol? Whatever an observer would have seen in this experiment namely t pairs of row and column polynomials.

And we have already argued that any subset of t row and column polynomials from this experiment does not reveal anything about the input of the experiment, we run the same argument here and conclude that during the sharing phase if there is an adversary with computationally unbounded resources, even in that case its probability distribution will remain independent of dealer’s secret.

(Refer Slide Time: 25:55)



VSS Scheme: Violation of Strong Commitment

Sharing phase protocol:

Steps for the dealer : on having input $s \in \mathbb{F}$, **dealer** does the following:

- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - Pick **random** t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$

$(\alpha_1, f_1(X))$

$\vdots$

$(\alpha_t, f_t(X))$

$\Rightarrow F(X,Y)$

$F(X,0) = f(X)$ $\quad$ $F(0,0) = f(0) = s$

- Send $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

Output for the parties :

- Party P_i outputs the **share** $s_i \overset{\text{def}}{=} g_i(0)$

Reconstruction phase protocol:

□ Party P_i **broadcasts** the share s_i

- A **corrupt** P_i may broadcast an **incorrect** share

□ Parties apply **RS error-correction** on received shares

- If a t-degree polynomial, say $f'(X)$ is obtained, then output $s' = f'(0)$

□ What happens if **dealer behaves maliciously** ?

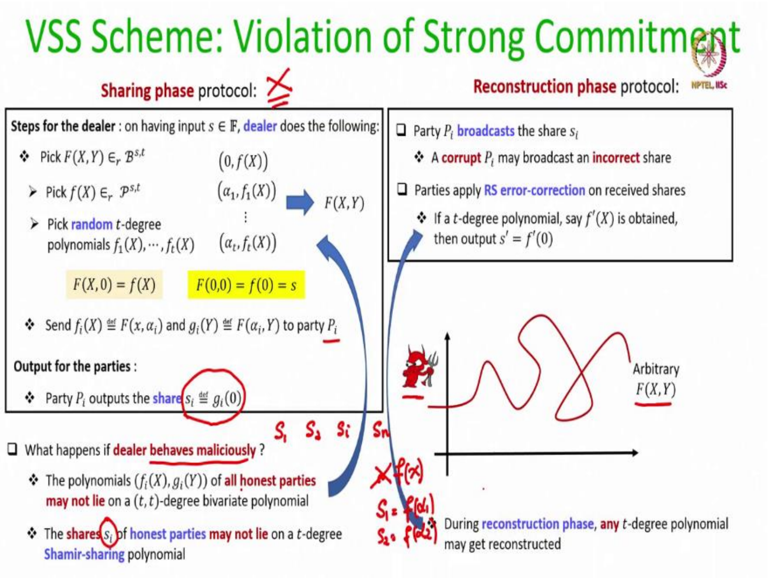
- The polynomials $(f_i(X), g_i(Y))$ of **all honest parties may not lie** on a (t,t)-degree bivariate polynomial

NPTEL, IISc
s
$f_t(X)$
$f_1(X)$
Random Polynomials
$f(X) \in_r \mathcal{P}^{s,t}$
$F(X,Y) \in_r \mathcal{B}^{s,t}$

So, well it looks like that we have got a VSS scheme, but the answer is no. We made a strong assumption that in that we in the VSS scheme this simple VSS scheme the dealer is honest. What if dealer gets corrupt during the execution of the protocol? What if he behaves maliciously? So, if the dealer gets corrupt and remember that parties will have no idea whether during the execution of the protocol dealer is behaving maliciously or not. If the dealer behaves maliciously then it may not follow this protocol instruction. What exactly is his protocol instruction?

He is supposed to pick a t-degree bivariate polynomial with the secret being the constant term and distribute univariate polynomials on those bivariate polynomials to all the parties, but it may not do that. In which case what may happen is that the row and column polynomials of the honest parties may not be consistent, may not be consistent in the sense that may not lie on a t-degree bivariate polynomials.

(Refer Slide Time: 27:03)



VSS Scheme: Violation of Strong Commitment

Sharing phase protocol:

Steps for the dealer : on having input $s \in \mathbb{F}$, dealer does the following:

- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$
  - Pick $f(X) \in_r \mathcal{P}^{s,t}$
  - Pick random t-degree polynomials $f_1(X), \cdots, f_t(X)$

$(0, f(X))$
$(\alpha_1, f_1(X))$
$\vdots$
$(\alpha_t, f_t(X))$ $\Rightarrow$ $F(X,Y)$

$F(X,0) = f(X)$ $\quad$ $F(0,0) = f(0) = s$

- Send $f_i(X) \overset{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \overset{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

Output for the parties :

- Party P_i outputs the share $s_i \overset{\text{def}}{=} g_i(0)$

Reconstruction phase protocol:

□ Party P_i broadcasts the share s_i

- A corrupt P_i may broadcast an incorrect share

□ Parties apply RS error-correction on received shares

- If a t-degree polynomial, say $f'(X)$ is obtained, then output $s' = f'(0)$

□ What happens if dealer behaves maliciously ?

- The polynomials $(f_i(X), g_i(Y))$ of all honest parties may not lie on a (t,t)-degree bivariate polynomial
- The shares s_i of honest parties may not lie on a t-degree Shamir-sharing polynomial

- During reconstruction phase, any t-degree polynomial may get reconstructed

So, what the corrupt dealer can do is it can just pick an arbitrary bivariate polynomial, which may not have the degree t in X and Y and distribute junk row and column polynomials to every honest party, in which case what can happen is that the share s_i which every honest party P_i is outputting in the protocol may not lie on a t-degree Shamir sharing polynomial.

Namely, the honest party P_i will think that ok, I got my polynomial $g_i(Y)$, I will just output the constant term of that polynomial fine. So, P_1 is doing that, P_2 is doing that, P_i is doing that, P_n is doing that fine, If the dealer is corrupt, then what I am claiming is that it is, there is no single t-degree $f(X)$ polynomial, there is no such $f(X)$ polynomial such that s_1 is $f(\alpha_1)$, s_2 is $f(\alpha_2)$ and so on.

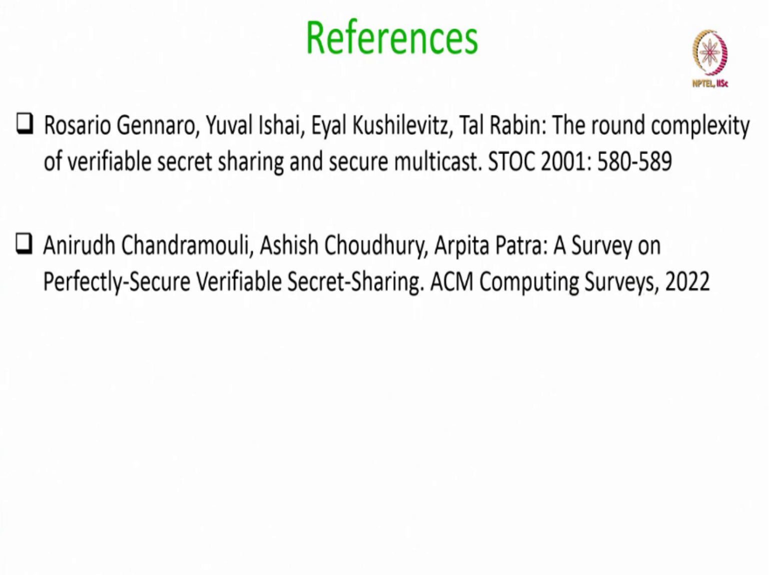
No, that is not happening if the dealer is behaving maliciously. And if this happens; that means, if the shares of the honest parties do not lie on a unique t-degree polynomial, then at the time of reconstruction even the error correction may fail. Parties will think that their shares lie on a t-degree polynomial. So, even if the corrupt parties produced incorrect shares, it is fine, we can error correct them.

But at the first place the shares of the honest parties themself do not lie on a unique t-degree polynomial, how can they think of error correcting other points? So, any polynomial can be reconstructed, it could be any $f'(X)$ and hence it could be any s' which gets reconstructed right. So, that is why even though the correctness and the privacy properties are achieved through this sharing and reconstruction phase protocols, if the dealer gets corrupt then the strong commitment property of the VSS is violated.

And strong commitment demands that even if the dealer is corrupt, the shares of all the honest parties should lie on a t-degree univariate polynomial, t-degree Shamir sharing univariate polynomial. That means, even a potentially corrupt dealer should have followed the protocol, that is why it is called verifiable secret sharing. That means, the secret sharing has been done in such a way that it is verifiable.

The parties can verify that whether a potentially corrupt dealer has followed the protocol instructions correctly or not. But right now, this secret, this pair of protocols is not a verifiable secret sharing, it is just a secret sharing scheme it will work only if the dealer is honest. If a dealer is allowed to be potentially corrupt, then the strong commitment property is violated.

(Refer Slide Time: 29:57)



References

- ❑ Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, Tal Rabin: The round complexity of verifiable secret sharing and secure multicast. STOC 2001: 580-589
- ❑ Anirudh Chandramouli, Ashish Choudhury, Arpita Patra: A Survey on Perfectly-Secure Verifiable Secret-Sharing. ACM Computing Surveys, 2022

So, now in our follow up lectures, we will build upon this simple pair of sharing and reconstruction protocol and then we will develop it into a full-fledged VSS protocol, where even the strong commitment property is satisfied. So, these are the references used for today’s lecture.

Thank you.