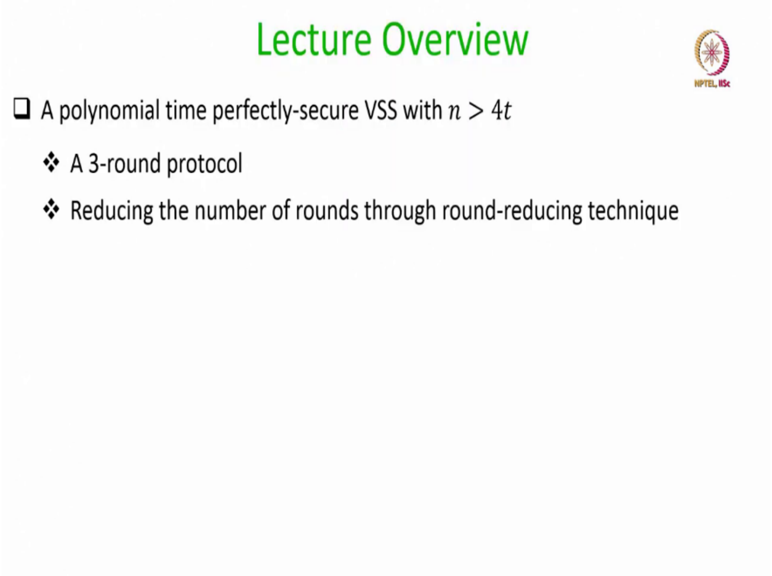
Secure Computation: Part II
Prof. Ashish Choudury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 43
Perfectly-Secure VSS with n > 4t: Part II

(Refer Slide Time: 00:27)

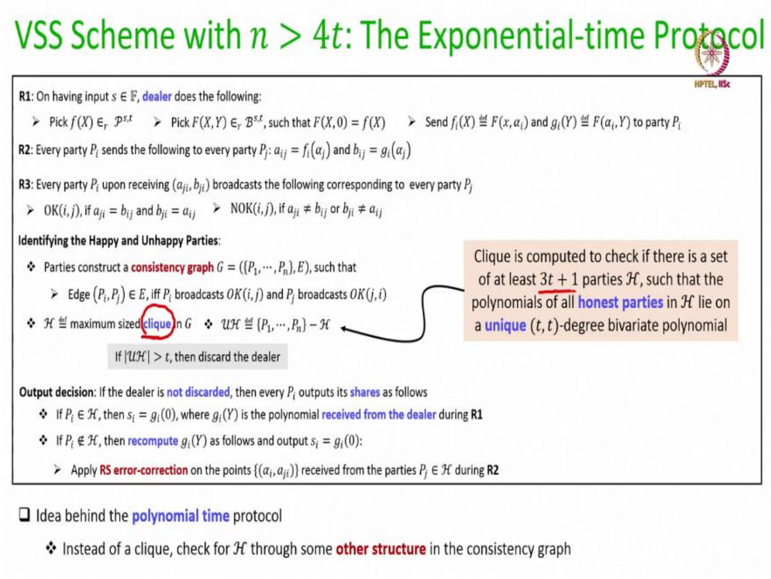


Lecture Overview

- ❑ A polynomial time perfectly-secure VSS with $n > 4t$
  - ❖ A 3-round protocol
  - ❖ Reducing the number of rounds through round-reducing technique

Hello everyone, welcome to this lecture. So, in this lecture, we will continue our discussion with perfectly secure VSS with $n > 4t$ which we had discussed in the last lecture. And we will present a polynomial time protocol.

(Refer Slide Time: 00:46)



VSS Scheme with $n > 4t$: The Exponential-time Protocol

NPTEL, IISc

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- Send $f_i(X) \stackrel{\text{def}}{=} F(x,\alpha_i)$ and $g_i(Y) \stackrel{\text{def}}{=} F(\alpha_i,Y)$ to party P_i

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- OK(i,j), if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- NOK(i,j), if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- $\mathcal{H} \stackrel{\text{def}}{=}$ maximum sized clique in G
- $\mathcal{UH} \stackrel{\text{def}}{=} \{P_1, \cdots, P_n\} - \mathcal{H}$

If $|\mathcal{UH}| > t$, then discard the dealer

Clique is computed to check if there is a set of at least $3t + 1$ parties $\mathcal{H}$, such that the polynomials of all honest parties in $\mathcal{H}$ lie on a unique (t,t)-degree bivariate polynomial

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

❑ Idea behind the polynomial time protocol

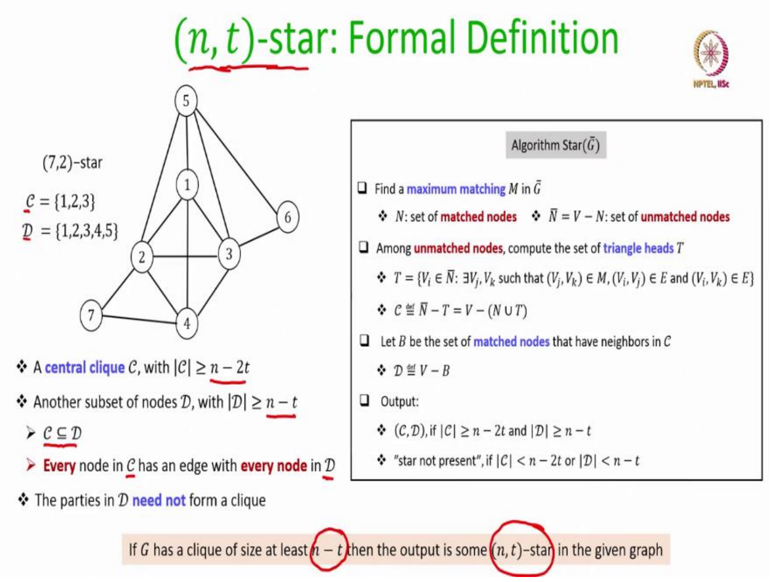
- Instead of a clique, check for $\mathcal{H}$ through some other structure in the consistency graph

So, I do not know whether you have noticed it or not that the protocol that we had discussed in the previous lecture was an exponential time protocol. Why it is an exponential time protocol? Because the set of happy parties is said to be the parties or the nodes representing the parties in the maximum size clique in the graph.

And finding the maximum size clique or basically checking whether there exists a clique of size at least $n - t$ we do not know whether we have a polynomial time algorithm for that problem or not. We have only had an exponential time protocol. So, even though we have a nice protocol, its running time is exponential. We would like to make the running time of the protocol polynomial time and we can do that.

And the idea behind this polynomial time protocol will be to define the set of happy parties based on some other structure in the consistency graph rather than the maximum size clique.

(Refer Slide Time: 01:45)



(n,t)-star: Formal Definition

NPTEL, IISc
5
1
6
2
3
7
4

(7,2)-star

$\mathcal{C} = \{1,2,3\}$

$\mathcal{D} = \{1,2,3,4,5\}$

- ❖ A central clique $\mathcal{C}$, with $|\mathcal{C}| \geq n - 2t$
- ❖ Another subset of nodes $\mathcal{D}$, with $|\mathcal{D}| \geq n - t$
  - ➢ $\mathcal{C} \subseteq \mathcal{D}$
  - ➢ **Every** node in $\mathcal{C}$ has an edge with **every node** in $\mathcal{D}$
- ❖ The parties in $\mathcal{D}$ **need not** form a clique

Algorithm Star($\bar{G}$)

- ❑ Find a **maximum matching** M in $\bar{G}$
  - ❖ N: set of **matched nodes** ❖ $\bar{N} = V - N$: set of **unmatched nodes**
- ❑ Among **unmatched nodes**, compute the set of **triangle heads** T
  - ❖ $T = \{V_i \in \bar{N}: \exists V_j, V_k$ such that $(V_j, V_k) \in M, (V_i, V_j) \in E$ and $(V_i, V_k) \in E\}$
  - ❖ $\mathcal{C} \overset{\text{def}}{=} \bar{N} - T = V - (N \cup T)$
- ❑ Let B be the set of **matched nodes** that have neighbors in $\mathcal{C}$
  - ❖ $\mathcal{D} \overset{\text{def}}{=} V - B$
- ❑ Output:
  - ❖ $(\mathcal{C}, \mathcal{D})$, if $|\mathcal{C}| \geq n - 2t$ and $|\mathcal{D}| \geq n - t$
  - ❖ "star not present", if $|\mathcal{C}| < n - 2t$ or $|\mathcal{D}| < n - t$

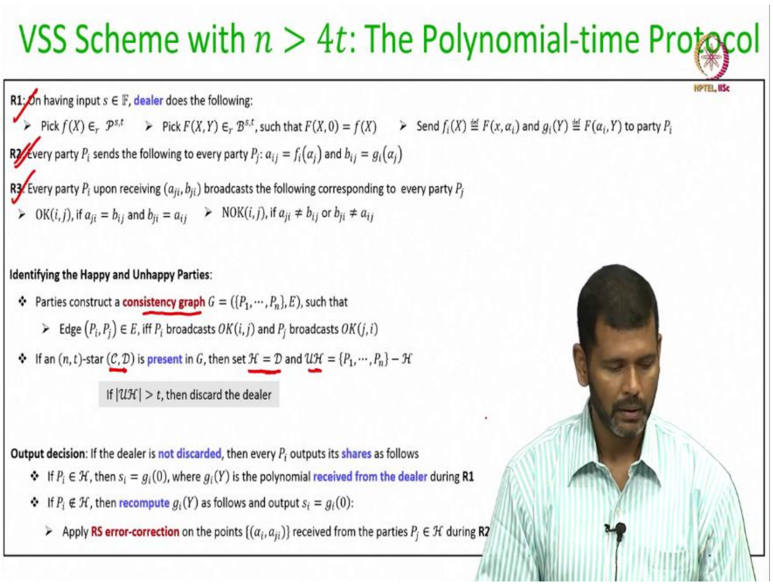
If G has a clique of size at least $n - t$ then the output is some (n,t)-star in the given graph

And, if and what we are going to do is that alternate structure in the consistency graph will be the (n, t)-star which we had used earlier in some other context. So, let me quickly recall the definition of (n, t)-star. So, if you are given a graph with n nodes, then an (n, t)-star basically consist of two subsets $\mathcal{C}$ and $\mathcal{D}$, where the size of $\mathcal{C}$ is at least $n - 2t$; that means, there should be at least $n - 2t$ nodes in the $\mathcal{C}$ set. There should be at least $n - t$ nodes in the $\mathcal{D}$ set and $\mathcal{C}$ set should be a subset of $\mathcal{D}$ set.

And there should be an edge between every node in $\mathcal{C}$ and every node in $\mathcal{D}$. However, that does not mean that the nodes in $\mathcal{D}$ constitute a clique; however, the nodes in $\mathcal{C}$ constitute a clique. And we have also seen an algorithm which can helps which can help us to find an (n, t)-star in the graph and that algorithm has the property that if it is guaranteed that my graph has a clique of at least $n - t$.

Then the algorithm will definitely output an (n, t)-star. Well, it can output an (n, t)-star even if the graph does not have a clique, but what we are guaranteed is that if the graph has a clique of size at least $n - t$ then the output of the algorithm will always be some (n, t)-star.

(Refer Slide Time: 03:21)



VSS Scheme with $n > 4t$: The Polynomial-time Protocol

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- Send $f_i(X) \stackrel{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \stackrel{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- OK(i,j), if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- NOK(i,j), if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If an (n,t)-star $(\mathcal{C}, \mathcal{D})$ is present in G, then set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If $|\mathcal{UH}| > t$, then discard the dealer

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

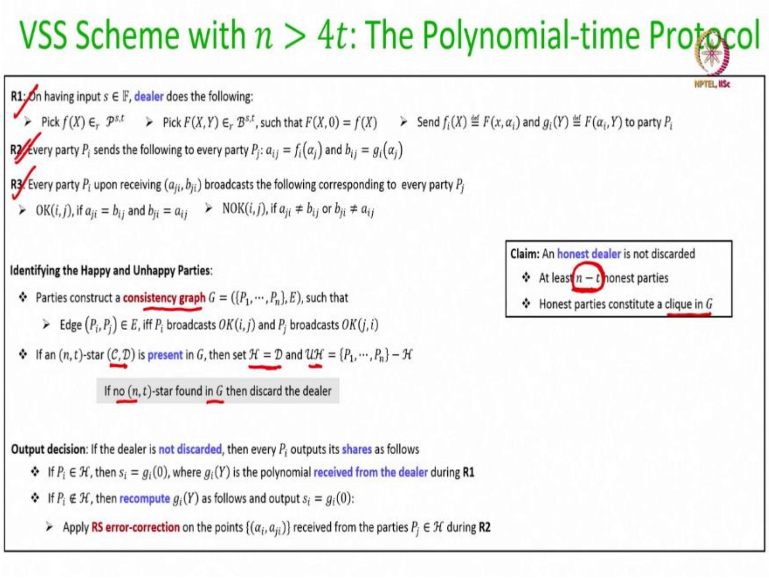
Now, let us see that how we can find the set of happy parties based on (n, t)-star in the consistency graph. So, the protocol steps remain same. During round 1 the dealer will distribute the row and column polynomials; in round 2 the parties exchange the common points. Again, I am exchange explaining the protocol without applying the round reducing technique, but at the end we can see that by applying the round reducing technique the resultant polynomial time protocol can be reduced to two rounds.

So, during the second round, the parties exchange the common points on their respective row and column polynomials over the private channels. And during the third round, they make the result public based on the publicly available results of the pair wise consistency tests, the parties construct the consistency graph.

And now we do not define the set of happy parties to be the parties representing the maximum sized clique. We do not do that, but rather what we do is we check whether some (n, t)-star is present in the graph or not. And how can we check? We use the previous algorithm the algorithm which we have for finding the (n, t)-star in the graph. We use that algorithm and check whether there exist some (n, t)-star in the graph.

And if that algorithm outputs an (n, t)-star namely a $\mathcal{C}$ component and $\mathcal{D}$ component, then the happy parties are said to be the parties representing the nodes in the $\mathcal{D}$ component of the star; and the unhappy parties will be the remaining parties.

(Refer Slide Time: 05:08)



VSS Scheme with $n > 4t$: The Polynomial-time Protocol

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- 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

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- $\mathrm{OK}(i,j)$, if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- $\mathrm{NOK}(i,j)$, if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If an (n,t)-star $(\mathcal{C}, \mathcal{D})$ is present in G, then set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Claim: An honest dealer is not discarded

- At least $n - t$ honest parties
- Honest parties constitute a clique in G

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

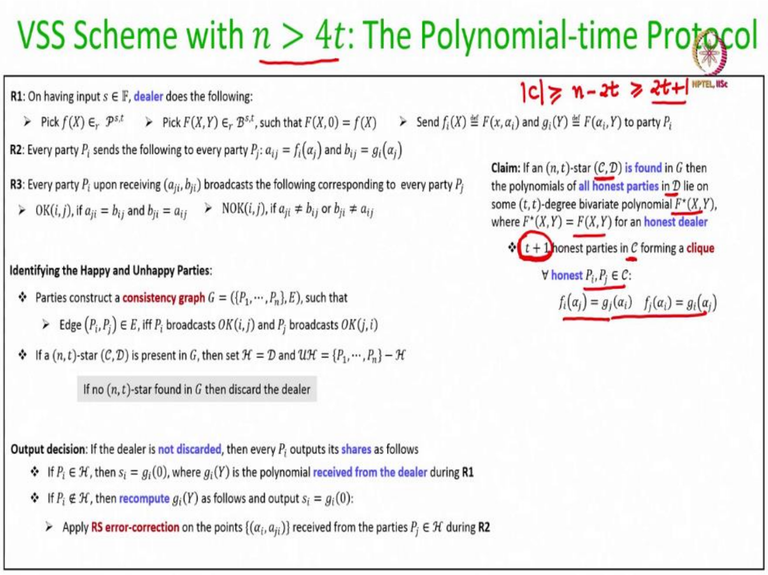
- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

And the sanity check will be now that if the star algorithm fails to identify any star in the graph, then we can safely conclude that the dealer is corrupt. So, it is safe to discard the dealer. Now, let us see the properties of this modified protocol the first claim is that if the dealer is honest, it will never get discarded. And the proof is very simple if the dealer is honest then there will be at least $n - t$ honest parties in the system.

And since the dealer is honest it will distribute pair wise consistent polynomials to all the honest parties. In fact, it is distributing pair wise consistent polynomials to all the parties. And this honest parties when they perform the payer wise consistency check they will come to know that the pair wise consistency checks are positive as a result every pair of honest parties P_i, P_j will broadcast an OK message; that means, they will constitute a clique in the consistency graph and the size of the clique will be at least $n - t$.

And now we can use the property of the star finding algorithm which guarantees that if there is a clique of size at least $n - t$, then the output will be some (n, t)-star. And since for an honest dealer a clique is guaranteed in the consistency graph, it implies that an (n, t)-star is also guaranteed. As a result, the sanity check will fail and hence an honest dealer will never get discarded.

(Refer Slide Time: 06:41)



VSS Scheme with $n > 4t$: The Polynomial-time Protocol

$|C| \geq n-2t \geq 2t+1$

NPTEL, IISc

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- 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

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- $\mathrm{OK}(i,j)$, if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- $\mathrm{NOK}(i,j)$, if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If a (n,t)-star $(\mathcal{C}, \mathcal{D})$ is present in G, then set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Claim: If an (n,t)-star $(\mathcal{C}, \mathcal{D})$ is found in G then the polynomials of all honest parties in $\mathcal{D}$ lie on some (t,t)-degree bivariate polynomial $F^\star(X,Y)$, where $F^\star(X,Y) = F(X,Y)$ for an honest dealer

- $\boxed{t+1}$ honest parties in $\mathcal{C}$ forming a clique

$\forall$ honest $P_i, P_j \in \mathcal{C}$:

$\underline{f_i(\alpha_j) = g_j(\alpha_i)}$ $\underline{f_j(\alpha_i) = g_i(\alpha_j)}$

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

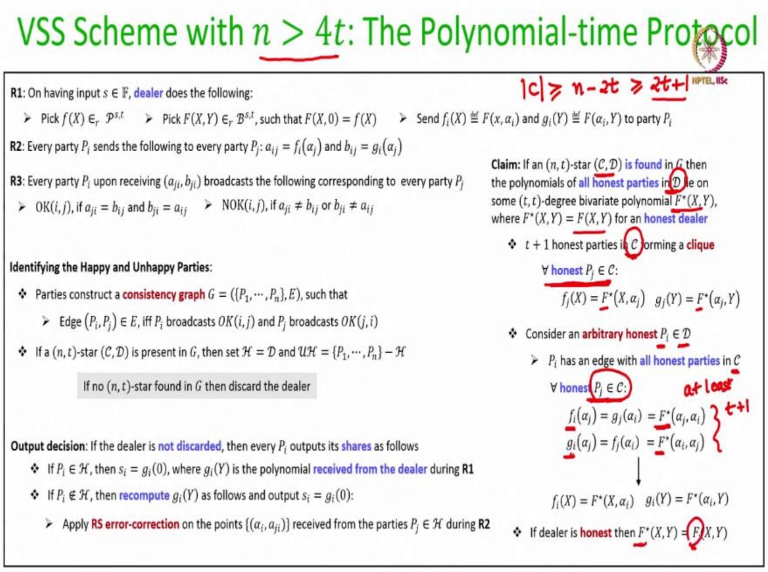
Now, the second property which we can claim with respect to this modified protocol is the following. Suppose the dealer is not discarded; that means, some star is obtained then the polynomials of all the honest parties in the $\mathcal{D}$ component of the star they together lie on a unique t degree bivariate polynomial $F^\star$, where this $F^\star$ bivariate polynomial is the F bivariate polynomial selected by the honest dealer.

Now, why this claim is correct? So, since a star is obtained, what will be the cardinality of the $\mathcal{C}$ component of the star? The cardinality of the $\mathcal{C}$ component of the star will be at least $n - 2t$ and $n - 2t$ means at least $2t + 1$, because we are working with the condition $n > 4t$; that means, there are at least $2t + 1$ parties in the $\mathcal{C}$ component of the star. Among those $2t + 1$ parties up to t could be corrupt; that means, there are at least $t + 1$ honest parties in the $\mathcal{C}$ component of the star.

And remember the $\mathcal{C}$ component of the star constitutes a clique; that means, there are at least $t + 1$ honest parties in the $\mathcal{C}$ which constitutes which constitute a clique; that means, they have broadcasted an OK message for each other; that means, what we can conclude is the following. There are at least $t + 1$ honest parties in $\mathcal{C}$ and for every pair of honest parties P_i, P_j in the $\mathcal{C}$ component of the star, their respective polynomials are pair wise consistent.

Because that is why they have broadcasted OK message for each other and that is why they are part of the clique. And now, we can apply the pair wise consistency lemma because now we have at least $t+1$ pairs of row and column polynomials guaranteed in the system which are pair wise consistent.

(Refer Slide Time: 08:58)



VSS Scheme with $n > 4t$: The Polynomial-time Protocol

$|C| \geq n-2t \geq 2t+1$

NPTEL, IISc

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- Send $f_i(X) \overset{\text{def}}{\equiv} F(x,\alpha_i)$ and $g_i(Y) \overset{\text{def}}{\equiv} F(\alpha_i,Y)$ to party P_i

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- $\mathrm{OK}(i,j)$, if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- $\mathrm{NOK}(i,j)$, if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If a (n,t)-star $(\mathcal{C},\mathcal{D})$ is present in G, then set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

Claim: If an (n,t)-star $(\mathcal{C},\mathcal{D})$ is found in G then the polynomials of all honest parties in $\mathcal{D}$ lie on some (t,t)-degree bivariate polynomial $F^{\star}(X,Y)$, where $F^{\star}(X,Y) = F(X,Y)$ for an honest dealer

- $t+1$ honest parties in $\mathcal{C}$ forming a clique

  $\forall$ honest $P_j \in \mathcal{C}$:

  $f_j(X) = F^{\star}(X,\alpha_j) \quad g_j(Y) = F^{\star}(\alpha_j,Y)$

- Consider an arbitrary honest $P_i \in \mathcal{D}$
  - P_i has an edge with all honest parties in $\mathcal{C}$

  $\forall$ honest $P_j \in \mathcal{C}$: at least

  $$\left.\begin{array}{l} f_i(\alpha_j) = g_j(\alpha_i) = F^{\star}(\alpha_j,\alpha_i) \\ g_i(\alpha_j) = f_j(\alpha_i) = F^{\star}(\alpha_i,\alpha_j) \end{array}\right\} t+1$$

  $$\downarrow$$

  $f_i(X) = F^{\star}(X,\alpha_i) \quad g_i(Y) = F^{\star}(\alpha_i,Y)$

- If dealer is honest then $F^{\star}(X,Y) = F(X,Y)$

And as a result, we can conclude that the row and column polynomials of all the honest parties in the $\mathcal{C}$ component of the star together lie on this t degree bivariate polynomial $F^{\star}$. But that is not the claim the claim statement is that the column polynomial of all the honest parties in the $\mathcal{D}$ component lie on $F^{\star}$. So, what we have proved till now what we have concluded till now? That if we take the honest parties in the $\mathcal{C}$ component their polynomials are lying on $F^{\star}$, but there might be some parties who are part of $\mathcal{D}$, but not part of $\mathcal{C}$.

So, now let us prove the actual claim. So, consider any arbitrary honest party who is a part of the $\mathcal{D}$ component of the star. Now what is the property of the star? The property of the star is that the node representing this party P_i, it has an edge with all the parties representing the $\mathcal{C}$ component of the star name. And, when I say all the parties representing the $\mathcal{C}$ component of the star; that means, both the honest parties in $\mathcal{C}$ as well as the corrupt parties in $\mathcal{C}$.

Forget about the corrupt parties in $\mathcal{C}$, what we know is that definitely this honest party P_i who is part of the $\mathcal{D}$ component of the star it has an edge with all the honest parties in the

$\mathcal{C}$ component of the star because, P_i would have said broadcasted an OK message for P_j and P_j would have broadcasted an OK message for P_i.

So, it has an edge with all the honest parties P_j in $\mathcal{C}$; that means, if I take every honest P_j in the $\mathcal{C}$ component of the star, the polynomial the column polynomial of P_j. So, the column polynomial of P_i and the row polynomial of P_i, they are pair wise consistent with the row and column polynomials of the honest parties P_j in the $\mathcal{C}$ component of the star.

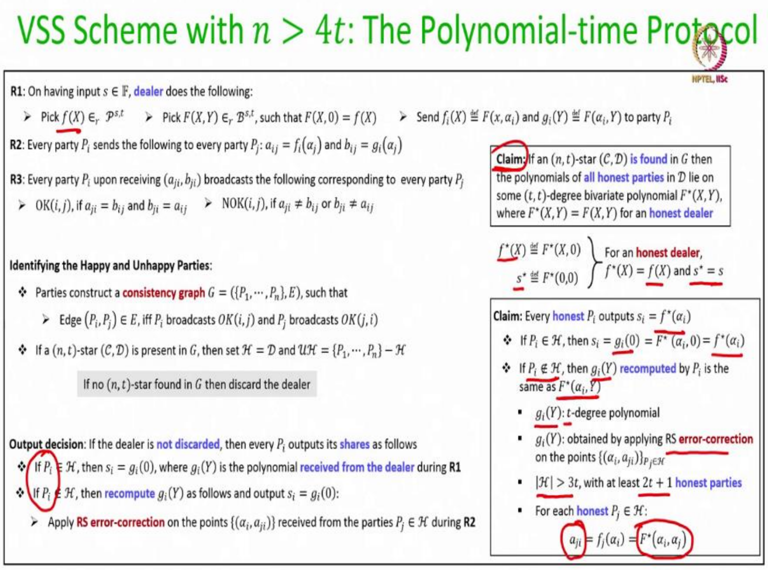
But the polynomials of the honest parties in the $\mathcal{C}$ component of the star they lie on $F^\star(X, Y)$ because of that we get these equalities. We get these two equalities and how many such equalities are there at least $t + 1$, because we have at least $t + 1$ honest parties guaranteed in the $\mathcal{C}$ component of the star.

So that means, what we have shown here is the following we have the row and column polynomial of the party P_i. For the row and column polynomial of P_i, there are $t + 1$ points which also lie on the supposedly ith row and the ith column polynomial of $F^\star$ bivariate polynomial.

And we know that two different t degree polynomials cannot have $t + 1$ or more number of common points, that automatically shows that the row and column polynomials of the party P_i which it has received from the dealer they are nothing but the supposedly ith row and ith column polynomial lying on this $F^\star$ bivariate polynomial which is defined by the honest parties in the $\mathcal{C}$ component of the $F^\star$.

And it is also easy to see that if the dealer is not on if the deal sorry if the dealer is honest and this defined polynomial $F^\star$ is nothing but the polynomial $F(X, Y)$ which has been selected by the dealer because all the row and column polynomials which dealer which an honest dealer distributes are with respect to this bivariate polynomial $F(X, Y)$.

(Refer Slide Time: 12:58)



VSS Scheme with $n > 4t$: The Polynomial-time Protocol

NPTEL, IISc

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- 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

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every party P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every party P_j

- $\mathrm{OK}(i,j)$, if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- $\mathrm{NOK}(i,j)$, if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$, such that
  - Edge $(P_i, P_j) \in E$, iff P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If a (n,t)-star $(\mathcal{C},\mathcal{D})$ is present in G, then set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

Claim: If an (n,t)-star $(\mathcal{C},\mathcal{D})$ is found in G then the polynomials of all honest parties in $\mathcal{D}$ lie on some (t,t)-degree bivariate polynomial $F^\star(X,Y)$, where $F^\star(X,Y) = F(X,Y)$ for an honest dealer

$$\left.\begin{aligned} f^\star(X) &\overset{\text{def}}{=} F^\star(X,0) \\ s^\star &\overset{\text{def}}{=} F^\star(0,0) \end{aligned}\right\} \begin{array}{l}\text{For an honest dealer,} \\ f^\star(X) = f(X) \text{ and } s^\star = s\end{array}$$

Claim: Every honest P_i outputs $s_i = f^\star(\alpha_i)$

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0) = F^\star(\alpha_i, 0) = f^\star(\alpha_i)$
- If $P_i \notin \mathcal{H}$, then $g_i(Y)$ recomputed by P_i is the same as $F^\star(\alpha_i, Y)$
  - $g_i(Y)$: t-degree polynomial
  - $g_i(Y)$: obtained by applying RS error-correction on the points $\{(\alpha_i, a_{ji})\}_{P_j \in \mathcal{H}}$
  - $|\mathcal{H}| > 3t$, with at least $2t+1$ honest parties
  - For each honest $P_j \in \mathcal{H}$:

$$a_{ji} = f_j(\alpha_i) = F^\star(\alpha_i, \alpha_j)$$

So, that is the main claim which we have proved and now we can prove the correctness and the strong commitment property very easily for the modified protocol. So, let us call the bivariate polynomial $F^\star$ evaluated at $Y = 0$, to be the $f^\star$ polynomial. It is a going to be a t degree univariate polynomial in X. We consider it to be a Shamir sharing polynomial. And let us focus on the constant term of this defined $F^\star$ polynomial for an honest dealer.

Because of this claim statement we automatically get that this defined Shamir sharing polynomial is the $f(X)$ polynomial picked by the honest dealer. And the defined secret $s^\star$ is nothing but the dealer secret. Now, what we are claiming is here is the following. Every honest party in the protocol outputs the ith point on this defined Shamir sharing polynomial.

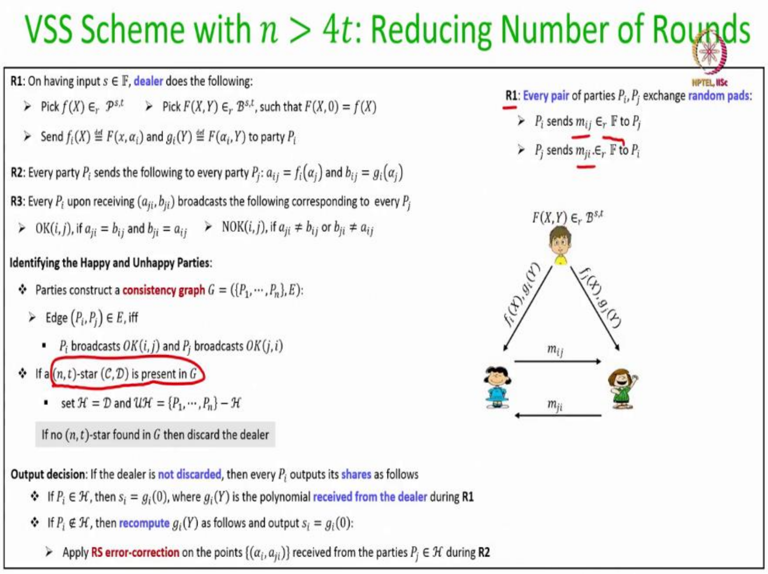
And again, it depends upon whether the party P_i that arbitrary honest party P_i is part of the happy set or not if it is a part of the happy set then basically its share is nothing but the constant term of its column polynomial which it has received from the dealer. And we have already proved in the previous claim that the constant term of its column polynomial is nothing but the value of the $f^\star$ polynomial at $X = \alpha_i$.

Whereas there is a possibility that the arbitrary honest party P_i is not a part of the happy set, in which case it recomputes its column polynomial. And again, we can show that the recomputed polynomial is same as the ith column polynomial of $F^\star$ bivariate polynomial.

This is because the recomputed polynomial is obtained by applying the Reed-Solomon error correction process. Its degree is t and the cardinality of the happy set of parties is at least $3t + 1$ with $2t + 1$ among them being honest parties. And now we can use the fact that the a_{ji} values which are used by the party P_i on which the Reed-Solomon error correction is applied.

They basically constitute points on this defined bivariate polynomial $F^{\star}$. So, because of the Reed-Solomon error correction property because of the properties of the Reed-Solomon error correction the recomputed polynomial $g_i(Y)$ is guaranteed to be the ith column polynomial of the defined bivariate polynomial $F^{\star}$.

(Refer Slide Time: 16:00)



VSS Scheme with $n > 4t$: Reducing Number of Rounds

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- Send $f_i(X) \stackrel{\text{def}}{=} F(x, \alpha_i)$ and $g_i(Y) \stackrel{\text{def}}{=} F(\alpha_i, Y)$ to party P_i

R2: Every party P_i sends the following to every party P_j: $a_{ij} = f_i(\alpha_j)$ and $b_{ij} = g_i(\alpha_j)$

R3: Every P_i upon receiving (a_{ji}, b_{ji}) broadcasts the following corresponding to every P_j

- $\mathrm{OK}(i,j)$, if $a_{ji} = b_{ij}$ and $b_{ji} = a_{ij}$
- $\mathrm{NOK}(i,j)$, if $a_{ji} \neq b_{ij}$ or $b_{ji} \neq a_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$:
  - Edge $(P_i, P_j) \in E$, iff
    - P_i broadcasts $OK(i,j)$ and P_j broadcasts $OK(j,i)$
- If a (n,t)-star $(\mathcal{C}, \mathcal{D})$ is present in G
  - set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}$ received from the parties $P_j \in \mathcal{H}$ during **R2**

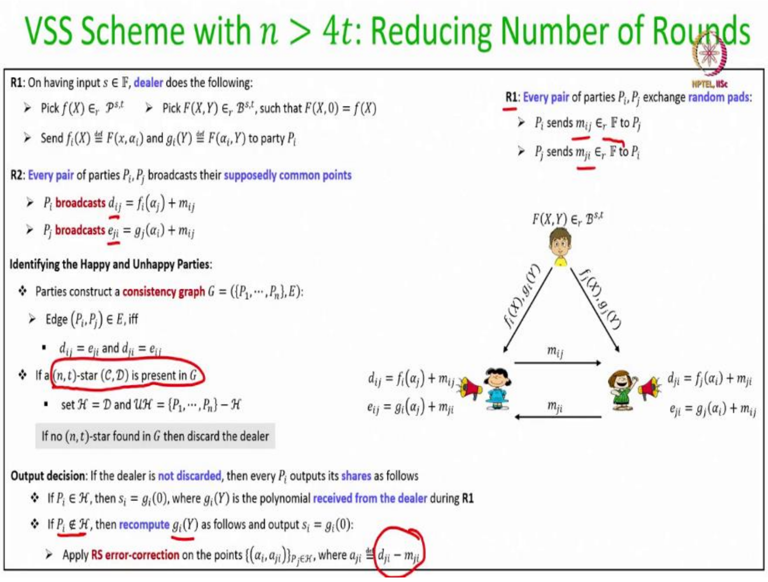
R1: Every pair of parties P_i, P_j exchange random pads:

- P_i sends $m_{ij} \in_r \mathbb{F}$ to P_j
- P_j sends $m_{ji} \in_r \mathbb{F}$ to P_i

Now, that is the way we can make the protocol a polynomial time protocol just by changing the structure in the consistency graph based on which the parties identify the set of happy parties. Now, this is the three round protocol to make it a two-round protocol, we can apply our usual round reducing technique.

Namely, during the first round apart from the distribution of the row and column polynomials by the dealer, every pair of parties can pre exchange random OTP pads. And then during the second round the pair wise consistency check happens publicly in through OTP encryptions.

(Refer Slide Time: 16:37)



VSS Scheme with $n > 4t$: Reducing Number of Rounds

NPTEL, IISc

R1: On having input $s \in \mathbb{F}$, dealer does the following:

- Pick $f(X) \in_r \mathcal{P}^{s,t}$
- Pick $F(X,Y) \in_r \mathcal{B}^{s,t}$, such that $F(X,0) = f(X)$
- 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

R1: Every pair of parties P_i, P_j exchange random pads:

- P_i sends $m_{ij} \in_r \mathbb{F}$ to P_j
- P_j sends $m_{ji} \in_r \mathbb{F}$ to P_i

R2: Every pair of parties P_i, P_j broadcasts their supposedly common points

- P_i broadcasts $d_{ij} = f_i(\alpha_j) + m_{ij}$
- P_j broadcasts $e_{ji} = g_j(\alpha_i) + m_{ij}$

Identifying the Happy and Unhappy Parties:

- Parties construct a consistency graph $G = (\{P_1, \cdots, P_n\}, E)$:
  - Edge $(P_i, P_j) \in E$, iff
    - $d_{ij} = e_{ji}$ and $d_{ji} = e_{ij}$
- If a (n,t)-star $(\mathcal{C}, \mathcal{D})$ is present in G
  - set $\mathcal{H} = \mathcal{D}$ and $\mathcal{UH} = \{P_1, \cdots, P_n\} - \mathcal{H}$

If no (n,t)-star found in G then discard the dealer

Output decision: If the dealer is not discarded, then every P_i outputs its shares as follows

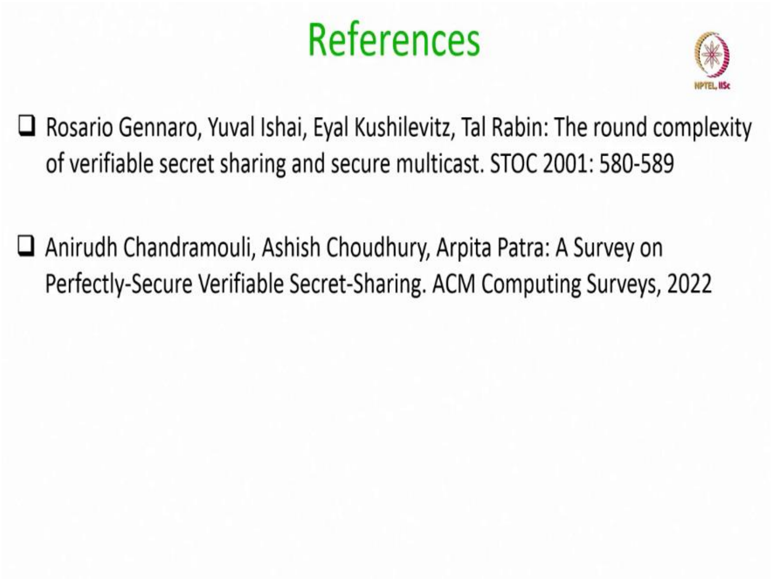
- If $P_i \in \mathcal{H}$, then $s_i = g_i(0)$, where $g_i(Y)$ is the polynomial received from the dealer during **R1**
- If $P_i \notin \mathcal{H}$, then recompute $g_i(Y)$ as follows and output $s_i = g_i(0)$:
  - Apply RS error-correction on the points $\{(\alpha_i, a_{ji})\}_{P_j \in \mathcal{H}}$, where $a_{ji} \overset{\text{def}}{=} d_{ji} - m_{ji}$

$F(X,Y) \in_r \mathcal{B}^{s,t}$
$f_i(X), g_i(Y)$
$f_j(X), g_j(Y)$
m_{ij}
m_{ji}
$d_{ij} = f_i(\alpha_j) + m_{ij}$
$e_{ij} = g_i(\alpha_j) + m_{ji}$
$d_{ji} = f_j(\alpha_i) + m_{ji}$
$e_{ji} = g_j(\alpha_i) + m_{ij}$

And then if there is a mismatch in the OTP encryptions, the edge between the corresponding parties is not added in the consistency graph otherwise the edge is added then we check whether a star is present. If the star is not present and we discard the dealer, otherwise we continue the protocol and every party P_i who is not part of the happy set it needs the a_{ji} value to apply the Reed-Solomon error correction process for recomputing its column polynomial.

The a_{ji} values are obtained by unmasking the pads from the publicly available OTP encryptions and the rest of the steps and analysis remains the same.

(Refer Slide Time: 17:34)



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, this is the final two round polynomial time VSS scheme with $n > 4t$ which is taken from this paper. And again, for other perfectly secure VSS scheme you are referred to this survey paper.

Thank you.