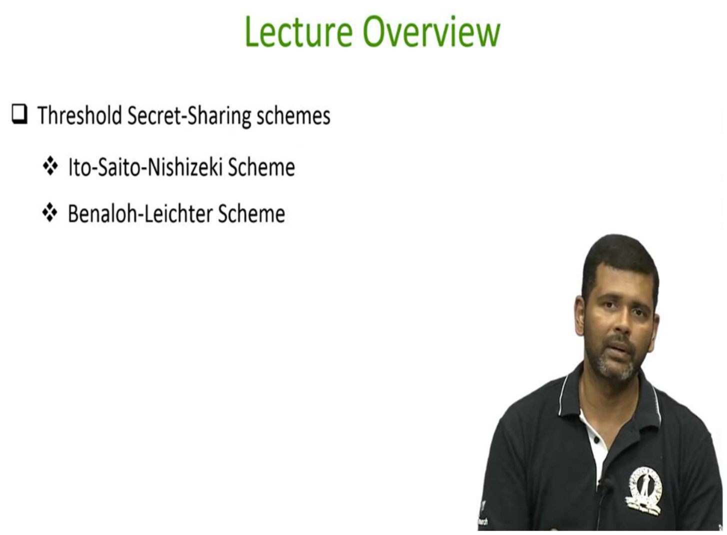
Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 1
Lecture - 9
Inefficient Threshold Secret Sharing

(Refer Slide Time: 00:32)

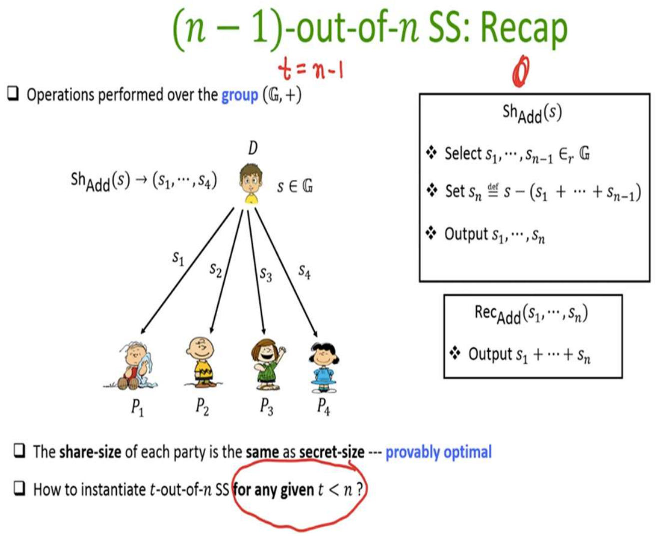


Lecture Overview

- ❑ Threshold Secret-Sharing schemes
  - ❖ Ito-Saito-Nishizeki Scheme
  - ❖ Benaloh-Leichter Scheme

Hello everyone. Welcome to this lecture. So, the plan for this lecture is as follows: We will see some constructions of threshold secret-sharing, which are very popular, but they are inefficient. And this will be the motivation for our next lecture, where our goal will be to design efficient threshold secret-sharing schemes.

(Refer Slide Time: 00:52)



$(n-1)$-out-of-n SS: Recap

t = n-1

❑ Operations performed over the **group** $(\mathbb{G}, +)$

D
$\mathsf{Sh}_{\mathsf{Add}}(s) \rightarrow (s_1, \cdots, s_4)$
$s \in \mathbb{G}$
s_1
s_2
s_3
s_4
P_1
P_2
P_3
P_4
0

$\mathsf{Sh}_{\mathsf{Add}}(s)$

- ❖ Select $s_1, \cdots, s_{n-1} \in_r \mathbb{G}$
- ❖ Set $s_n \overset{\text{def}}{=} s - (s_1 + \cdots + s_{n-1})$
- ❖ Output $s_1, \cdots, s_n$

$\mathsf{Rec}_{\mathsf{Add}}(s_1, \cdots, s_n)$

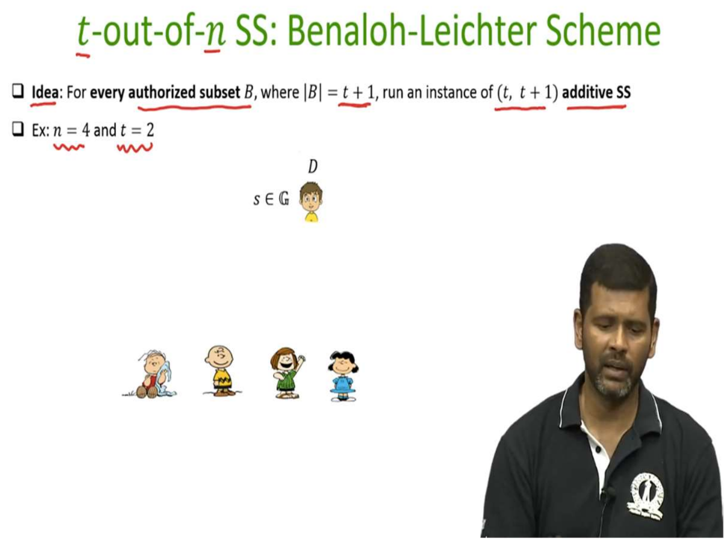
- ❖ Output $s_1 + \cdots + s_n$

❑ The **share-size** of each party is the **same** as **secret-size** --- **provably optimal**

❑ How to instantiate t-out-of-n SS **for any given** $t < n$?

So, just a quick recap. We had seen the construction of additive secret-sharing, namely, $n - 1$ out of n secret-sharing, where the threshold was $t = n - 1$. And in the last lecture, we asked ourselves that, how can we design a secret-sharing scheme for any given t which is strictly less than n, which is not necessarily $n - 1$.

(Refer Slide Time: 01:24)



t-out-of-n SS: Benaloh-Leichter Scheme

- ❑ Idea: For every authorized subset B, where $|B| = t + 1$, run an instance of $(t,\ t + 1)$ additive SS
- ❑ Ex: $n = 4$ and $t = 2$

So, let us first see a scheme by Benaloh et al. which is a very elegant construction. And what is the underlying idea here? The underlying idea is that, since we want to design a t out of n secret-sharing scheme; and remember, t out of n secret-sharing scheme means, your access structure consists of subsets of size $t + 1$ or more. That means, your minimal authorised subsets are of cardinality $t + 1$.

That means, if any subset of $t + 1$ shareholders make their shares available, the reconstruction algorithm should give you back the secret. Whereas, unauthorised subsets are of cardinality t or less. So, the idea here is the following: You take any authorised subset B of cardinality $t + 1$, and for that specific subset B, you run an instance of additive secret-sharing, assuming the threshold to be t and n to be $t + 1$.

That means, you ignore the parties outside the set B and just focus on the subset B. And let the dealer run an instance of additive secret-sharing, assuming that it is only the parties in B with whom he wants to share the secret; he do not want to share the secret among the parties outside the B. Now, you might be asking that, what about the parties outside the B? If they come with their shares, you are not giving him any shares?

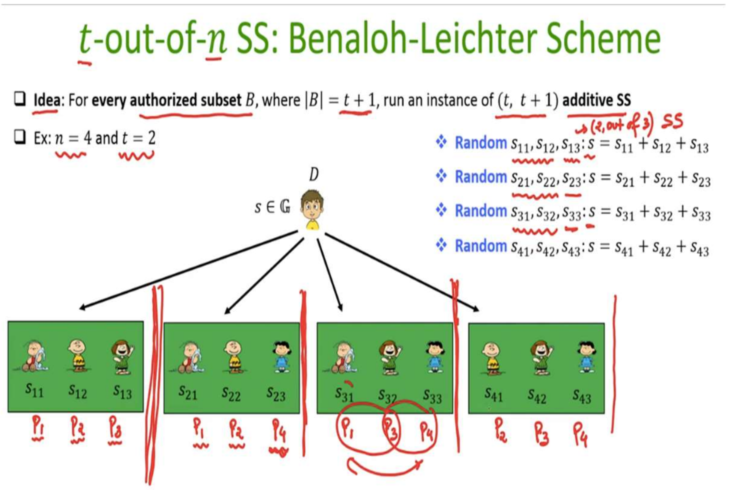
Well, they will be part of another candidate subset B of size $t + 1$. And for that candidate B, an independent instance of additive secret-sharing will be run. So, the idea is, dealer does not know in advance that which authorised subset will be coming to reconstruct the secret. It could be either the authorised subset B_1 or the authorised subset B_2 or the authorised subset B_3. It could be any of the possible authorised subset whose cardinality is $t + 1$.

For each of them is basically giving them enough number of shares, so that, if they come together, they should get back the dealer's secret. That is the underlying idea. So, let me demonstrate this scheme assuming a concrete value of n and t. So, we take the case where there are 4 parties. And again, all the computations here will be performed over a group with respect to n plus operation.

And I am taking the case where $n = 4$ and $t = 2$. That means, now you can see here, I cannot run my earlier additive secret-sharing, because the earlier additive secret-sharing demands the threshold t to be 3. But here, it is given to me that, I have to design a scheme in such a way that, if any 3 shareholders or more than 3 shareholders make their shares available, the secret should be reconstructed back.

But 2 shareholders or less than 2 shareholders, the probability distribution of their shares should be independent of the underlying secret. That is what is my goal. So, what dealer is going to do here is the following: He has the parties, shareholders 1, 2, 3 and 4.

(Refer Slide Time: 05:10)



t-out-of-n SS: Benaloh-Leichter Scheme

❑ **Idea**: For **every authorized subset** B, where $|B| = t + 1$, run an instance of $(t,\ t+1)$ **additive SS**

❑ Ex: $n = 4$ and $t = 2$

(2, out of 3) SS

❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$

❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$

❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$

❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

D
$s \in \mathbb{G}$
s_{11} s_{12} s_{13}
P_1 P_2 P_3
s_{21} s_{22} s_{23}
P_1 P_2 P_4
s_{31} s_{32} s_{33}
P_1 P_3 P_4
s_{41} s_{42} s_{43}
P_2 P_3 P_4

He imagines in his mind various possible authorised subsets. So, remember, $t = 2$. So, the minimal cardinality of any authorised subset will be $t + 1$, 3. So, these are the possible authorised subsets from the viewpoint of the dealer. That means, it could be the case that P_1, P_2, P_3 wants to learn the secret. If that is the case, they should be allowed to learn the dealer's secret.

Or it could be the case that it is P_1, P_2, P_4. Or it could be the case that it is P_1, P_3, P_4. Or it could be the case that it is P_2, P_3, P_4. Of course, entire collection of parties, that also constitutes an authorised subset, but that is not a minimal authorised subset. We are basically focusing on the minimal authorised subsets. Any superset of them is also trivially an authorised subset.

So, now, what dealer does is, he thinks in his mind that, okay, I want to do a secret-sharing only considering party 1, 2 and 3 as the possible shareholders, that is all. He do not bring the fourth shareholder into the picture. And it runs an instance of 2 out of 3 secret-sharing. So, this is an instance of 2 out of 3 secret-sharing, which is an instance of additive secret-sharing. And for that, what dealer has to do?

Dealer has to choose the first 2 shares uniformly at random. And then, it has to compute the third share such that all the 3 shares sum up to the secret s. And then, the first share which I am calling s_{11}, which will be communicated to the first shareholder, to the party number 1. The second piece will be given to party number 2. The third piece will be given to party number 3.

Independently, it runs another instance of 2 out of 3 secret-sharing, assuming that it wants to share the secret only among 1, 2, and 4. That means, it is now not bringing the party number 3 into the picture. And he is assuming that he wants to share the secret only among 1, 2 and 4 in such a way that, only when 1, 2 and 4 come together, they should get back the dealer's secret.

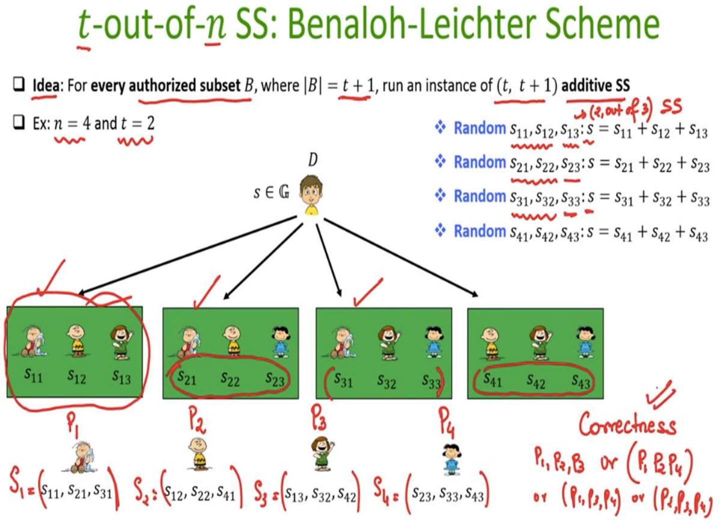
But if either 1 or 2, or if either 2 or 4, or if either 1 or 4 come together, they should fail to get the secret. How can dealer do that? Again, just run an independent instance of 2 out of 3 additive secret-sharing. Namely, pick the first 2 pieces uniformly at random and set the third piece to be such that summation of the 3 pieces should be the dealer's secret. And now, give the piece number s_{21} to the first shareholder in this group.

Give the piece s_{22} to the second shareholder in the group. And give the third piece now to the third shareholder in the group, but now, the third shareholder is not party number P_3. It is actually party number 4. Independently, dealer runs another instance of 2 out of 3 secret-sharing, assuming that it wants to share the secret only among 1, 3 and 4, in such a way that only when all the 3 parties, P_1, P_3, P_4 come together, the secret should be reconstructed back.

But if it is only 1 or 3, or if it is only 3 or 4, or if it is only 1 or 4, they should fail to get back the secret. How dealer can do that? Well, he has to pick the first 2 pieces independently, uniformly at random. And set the third piece in such a way that the summation of the 3 pieces should be the dealer's secret. And now give the corresponding pieces to the respective parties in this short group.

And now, run another instance of 2 out of 3 secret-sharing for the same secret. Remember, dealer's secret in all these independent instances of 2 out of 3 secret-sharing is the same. It is the same secret s. The secret is not getting changed. So, it runs an instance of 2 out of 3 secret-sharing for this last group and distribute the corresponding share only within this restricted group. Now, what will be the overall share for party 1, 2, 3 and 4? Because now, party 1, 2, 3 and 4 are present in several groups here.

(Refer Slide Time: 10:22)



t-out-of-n SS: Benaloh-Leichter Scheme

- ❑ **Idea**: For **every authorized subset** B, where $|B| = t + 1$, run an instance of $(t,\ t+1)$ **additive SS**
- ❑ Ex: $n = 4$ and $t = 2$

→ (2, out of 3) SS

- ❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$
- ❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$
- ❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$
- ❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

D
$s \in \mathbb{G}$
s_{11} s_{12} s_{13}
s_{21} s_{22} s_{23}
s_{31} s_{32} s_{33}
s_{41} s_{42} s_{43}
P_1
P_2
P_3
P_4

$S_1 = (s_{11}, s_{21}, s_{31})$ $S_2 : (s_{12}, s_{22}, s_{41})$ $S_3 = (s_{13}, s_{32}, s_{42})$ $S_4 = (s_{23}, s_{33}, s_{43})$

Correctness ✓✓

P_1, P_2, P_3 or (P_1, P_2, P_4) or (P_1, P_3, P_4) or (P_2, P_3, P_4)

The overall share for party P_1, which I denote by this capital S_1, will be now this whole collection of 3 pieces. Why this whole collection of 3 pieces? Because P_1 is given some piece of information with respect to this possible authorised collection, this possible authorised collection and this possible authorised collection. In the same way, the shares of all the pieces which are given to party P_2 by the dealer, that will be constituted as the overall share for party number P_2.

In the same way, whatever pieces party P_3 has got from the dealer, based on which candidate authorised subsets P_3 is part of, the collection of all those pieces actually constitutes the overall share for P_3. And in the same way, if I consider P_4, all the pieces that P_4 got as part of various candidate authorised subsets, constitute the overall share for the party number P_4.

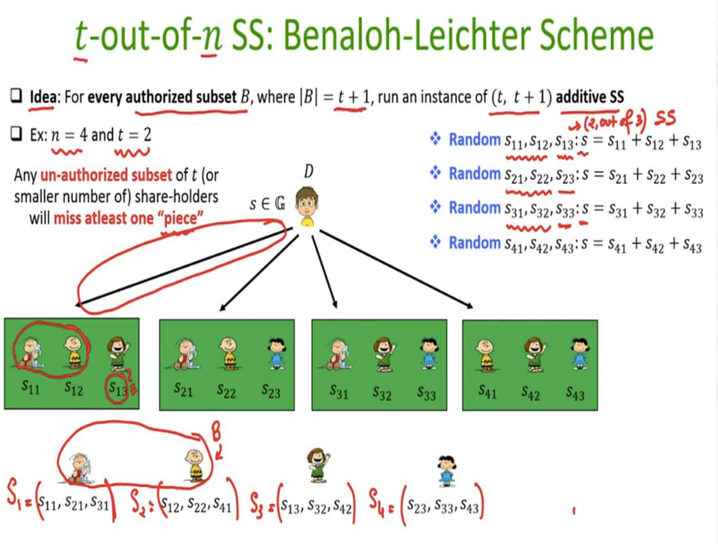
Now, let us try to argue the correctness property and privacy property; whether this mechanism achieves the correctness property or not. So, what is the correctness property? We want to ensure that, if any subset of 3 parties come together, then can they learn the dealer's secret? 3 or more number of parties; of course, if 3 can learn, any superset of that can also learn.

So, imagine if P_1, P_2, P_3, if they come together, will they learn the dealer's secret? Well, if P_1, P_2, P_3 come together, that means, we are now talking about this authorised subset. And indeed, the shares s_{11}, s_{12}, s_{13} have the property that, if they are added, it gives you back the secret. Or, it could be the case that 1, 2 and 4, they want to learn the secret. Can they learn? Yes.

The pieces s_{21}, s_{22}, s_{23} are such that, if they are added together, it gives you back the secret. Or, if 1, 3 and 4, they want to learn, can they learn? Yes. The pieces s_{31}, s_{32}, s_{33}, they are such that, if they are added together, they gives you back the secret. Or, if 2, 3, 4, they want to learn, can they learn? Yes, the pieces s_{41}, s_{42}, s_{43}, they are such that, when added, it gives you back the dealer's secret.

So, the correctness property is satisfied. Now, what about the privacy property? Does it satisfy the privacy requirement? Can I argue that, if I take any subset of 2 parties, then the probability distribution of the information that those 2 parties receive from the dealer is independent of the secret s?

(Refer Slide Time: 13:47)



t-out-of-n SS: Benaloh-Leichter Scheme

- ❑ **Idea**: For **every authorized subset** B, where $|B| = t + 1$, run an instance of $(t,\ t + 1)$ **additive SS**
- ❑ Ex: $n = 4$ and $t = 2$

Any **un-authorized subset** of t (or smaller number of) share-holders will **miss atleast one "piece"**

- ❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$ → (2, out of 3) SS
- ❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$
- ❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$
- ❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

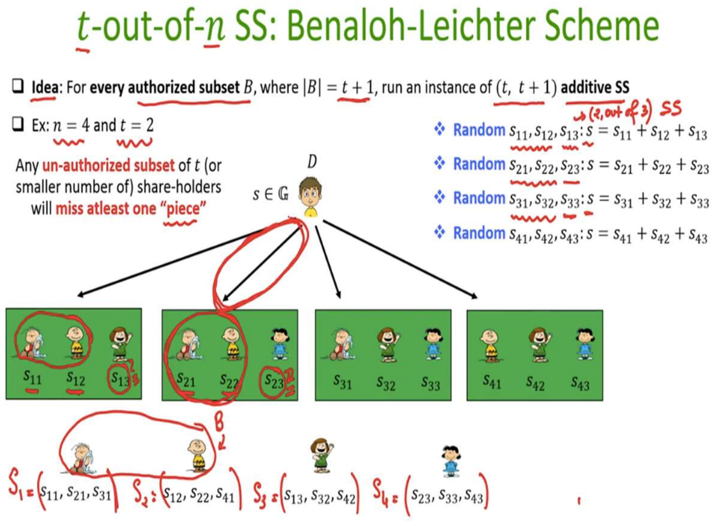
$S_1 = (s_{11}, s_{21}, s_{31})$ $S_2 = (s_{12}, s_{22}, s_{41})$ $S_3 = (s_{13}, s_{32}, s_{42})$ $S_4 = (s_{23}, s_{33}, s_{43})$

My claim is that you take any unauthorised subset of t or a small number of shareholders, they will miss at least 1 value to get back the secret. And that missing value could be any value, and hence it could be any secret which dealer has actually shared with those 2 parties. So, for instance, imagine that I talk about an unauthorised collection consisting of the first party and the second party.

What are the pieces that they have got? They have got $s_{11}, s_{21}, s_{31}, s_{12}, s_{22}, s_{41}$. You might be saying, argue thinking that, okay, that is lot of information to get back secret. No. If 1 and 2, if I think it from the viewpoint of the first instance of the dealer's additive secret-sharing, then 1 and 2, they are present in this instance, where they are actually treated as part of the whole bunch of shareholders.

They will have s_{11} and s_{12}, but they do not know what is the s_{13} that this third party got. Since s_{13} is kind of not known to P_1 and P_2, that means, based on this instance of secret-sharing which dealer has executed, P_1 and P_2 cannot infer anything about the secret s.

(Refer Slide Time: 15:25)



t-out-of-n SS: Benaloh-Leichter Scheme

❑ **Idea**: For **every authorized subset** B, where $|B| = t+1$, run an instance of $(t,\ t+1)$ **additive SS** (2, out of 3) SS

❑ Ex: $n = 4$ and $t = 2$

Any **un-authorized subset** of t (or smaller number of) share-holders will **miss atleast one "piece"**

❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$

❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$

❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$

❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

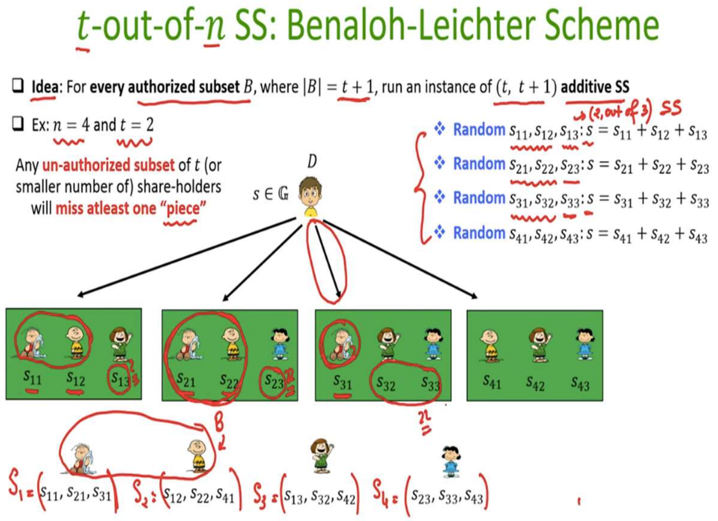
D
$s \in \mathbb{G}$
s_{11} s_{12} s_{13}
s_{21} s_{22} s_{23}
s_{31} s_{32} s_{33}
s_{41} s_{42} s_{43}
B

$S_1 = (s_{11}, s_{21}, s_{31})$ $S_2 = (s_{12}, s_{22}, s_{41})$ $S_3 = (s_{13}, s_{32}, s_{42})$ $S_4 = (s_{23}, s_{33}, s_{43})$

Now, 1 and 2 are also member of this instance of the secret-sharing, where they learn s_{21} and s_{22}. And remember, s_{21} and s_{11}, they have no relationship, they are picked independently, I stress, they are picked independently. Similarly, s_{12} and s_{22}, they have no relationship among them, they are picked independently. Now, as part of this second secret-sharing instance, can I say that s_{21} and s_{22} helps the 2 parties to learn anything about the secret?

No, because this third piece s_{23} is missing for them, and it could be any group element from the group. And hence it could be; that means, s_{21} and s_{22} could be the shares corresponding to every candidate s from the group. So, that means, this instance is also useless for P_1 and P_2. Now, what about the third instance?

(Refer Slide Time: 16:31)



t-out-of-n SS: Benaloh-Leichter Scheme

❑ **Idea**: For **every authorized subset** B, where $|B| = t+1$, run an instance of $(t,\ t+1)$ **additive SS** (2, out of 3) SS

❑ Ex: $n = 4$ and $t = 2$

Any **un-authorized subset** of t (or smaller number of) share-holders will **miss atleast one "piece"**

❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$

❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$

❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$

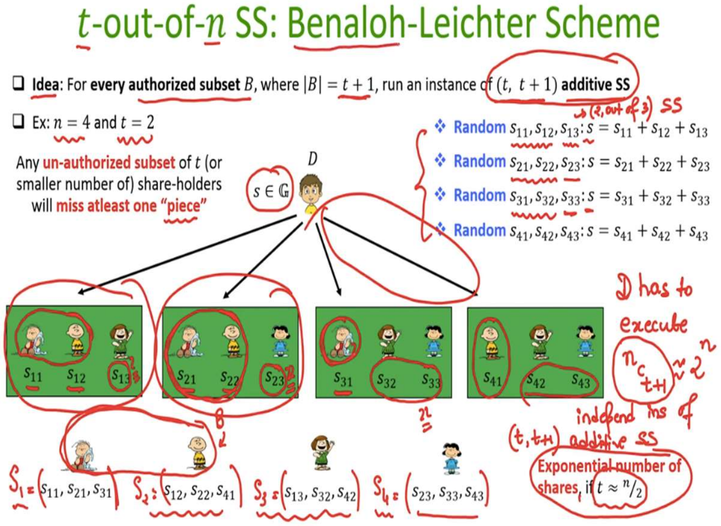
❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

$S_1 = (s_{11}, s_{21}, s_{31})$ $S_2 = (s_{12}, s_{22}, s_{41})$ $S_3 = (s_{13}, s_{32}, s_{42})$ $S_4 = (s_{23}, s_{33}, s_{43})$

D
$s \in \mathbb{G}$
s_{11} s_{12} s_{13}
s_{21} s_{22} s_{23}
s_{31} s_{32} s_{33}
s_{41} s_{42} s_{43}
B

In the third instance, P_2 is missing; it is only P_1 who is from the set B. And now, remember s_{31} has got nothing to do with $s_{11}, s_{12}, s_{21}, s_{22}$. He is getting it completely independent. Because all these 4 instances, they are picked, they are executed independently of each other. Now, there are 2 pieces which P_1 is lacking here. And hence, it cannot learn anything from this third instance as well. Now, let us consider the fourth instance.

(Refer Slide Time: 17:12)



t-out-of-n SS: Benaloh-Leichter Scheme

- ❑ Idea: For every authorized subset B, where $|B| = t+1$, run an instance of $(t,\ t+1)$ additive SS
- ❑ Ex: $n = 4$ and $t = 2$

Any un-authorized subset of t (or smaller number of) share-holders will miss atleast one "piece"

- ❖ Random s_{11}, s_{12}, s_{13}: $s = s_{11} + s_{12} + s_{13}$
- ❖ Random s_{21}, s_{22}, s_{23}: $s = s_{21} + s_{22} + s_{23}$
- ❖ Random s_{31}, s_{32}, s_{33}: $s = s_{31} + s_{32} + s_{33}$
- ❖ Random s_{41}, s_{42}, s_{43}: $s = s_{41} + s_{42} + s_{43}$

Exponential number of shares, if $t \approx n/2$

D
$s \in \mathbb{G}$
$\to$ (2, out of 3) SS
s_{11} s_{12} s_{13}
s_{21} s_{22} s_{23}
s_{31} s_{32} s_{33}
s_{41} s_{42} s_{43}
B
$S_1 = (s_{11}, s_{21}, s_{31})$
$S_2 : (s_{12}, s_{22}, s_{41})$
$S_3 = (s_{13}, s_{32}, s_{42})$
$S_4 = (s_{23}, s_{33}, s_{43})$
D has to execute
$^nC_{t+1} \approx 2^n$
independ ins of
$(t, t+1)$ additive SS

In the fourth instance, from the set B, unauthorised collection, it is only the party number P_2 who is present. But there are 2 pieces in that instance, which is missing for him. And hence, it could be any candidate s for which he has seen the s_{41}. That means, even though it might look like that now the parties in B are getting too much of information because members of B are present in multiple possible executions of the additive secret-sharing instances executed by the dealer, we have cleverly executed the independent instances in such a way that, for each instance, the parties in subset B will be missing at least 1 piece of information.

And even though they know that, okay, all these invocations are with respect to the same secret s, they cannot pinpoint what is that secret s. It could be any element from the group space, from the group. And that is why this constitutes a valid t out of n secret-sharing scheme. What is the problem with this secret-sharing scheme? Well, the correctness and privacy is satisfied.

But what is the share size? The share size for party 1 is actually 3 group elements. The share size for party 2 is 3 group elements. The share size for party 3 is 3 group elements. The share size for party 4 is 3 group elements. This is unlike your $n - 1$ out of n secret-sharing, additive secret-sharing, where the share size was just 1 group element; share was just 1 group element its size was the same as the secret.

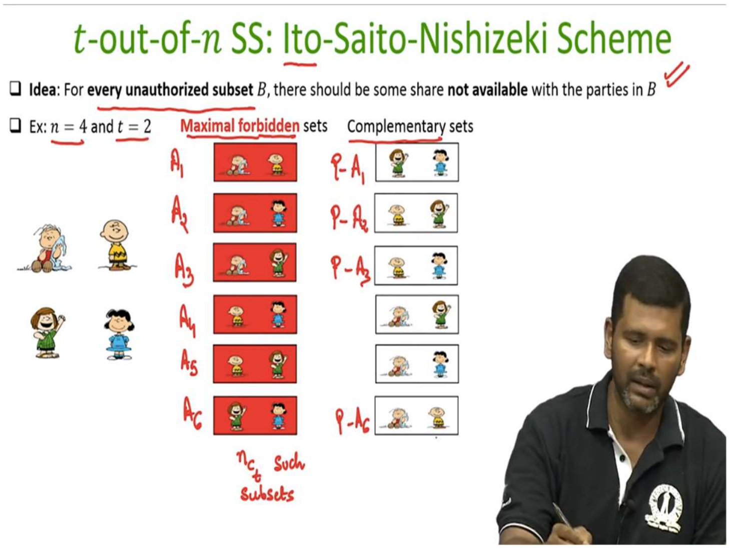
But now, the secret is just 1 element of the group, but the share size for each shareholder is 3 times the size of the secret. Now, in general, if my threshold $t = n/2$. So, in this case, it was $n/2$, but I am talking now about an arbitrary n and arbitrary t, where t is roughly $n/2$. Then, how many instances of additive secret-sharing D has to execute? So, D then has to execute n choose $t + 1$ independent instances of $t, t + 1$ additive SS.

Why these many? Because, these many candidate authorised subsets could be there, minimal sized authorised subsets could be there for the dealer. And for each such possible candidate authorised subset, it has to run an independent instance of additive secret-sharing. But what is this quantity, n choose $t + 1$? It is exponentially large if I set my t to be $n/2$. That means, the share size for each party will be exponentially large.

Because, each party could be now present in exponentially many candidate authorised subset; and with respect to each candidate authorised subset, it will be receiving an independent share as part of the additive secret-sharing which dealer would have executed for that candidate authorised subset. And that is why, even though this is a valid secret-sharing scheme, it becomes impractical if my value of n and t increases, and if my threshold t is roughly half the number of parties.

This is unlike your strict $n - 1$ out of n additive secret-sharing, because, there it does not matter how large is your n, each party will just receive a single group element as its overall share. But that is not happening in the scheme by Benaloh et al.

(Refer Slide Time: 21:23)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

- ❑ **Idea**: For **every unauthorized subset** B, there should be some share **not available** with the parties in B
- ❑ Ex: $n = 4$ and $t = 2$ **Maximal forbidden** sets Complementary sets

Now, let us see another interesting t out of n secret-sharing scheme by Ito et al. And this also might look similar to the construction of Benaloh et al., but it is slightly different. What is the idea in this scheme? The idea in this scheme is now, we will ensure that for every unauthorised subset, there should be some piece, some share which is not available with the parties in that unauthorised subset.

If we ensure this, then it does not matter what exactly is that unauthorised subset, whether it is the first subset of t shareholders or whether it is the last subset of t shareholders. If I ensure that my sharing algorithm has this property, then the privacy property will be achieved. Let me demonstrate it with an example. I take my $n = 4$ and $t = 2$. So, I want a sharing mechanisms so that any subset of 3 or more shareholders have enough information to get back the secret, but any subset of 2 or less number of shareholders do not have sufficient information to get back the secret.

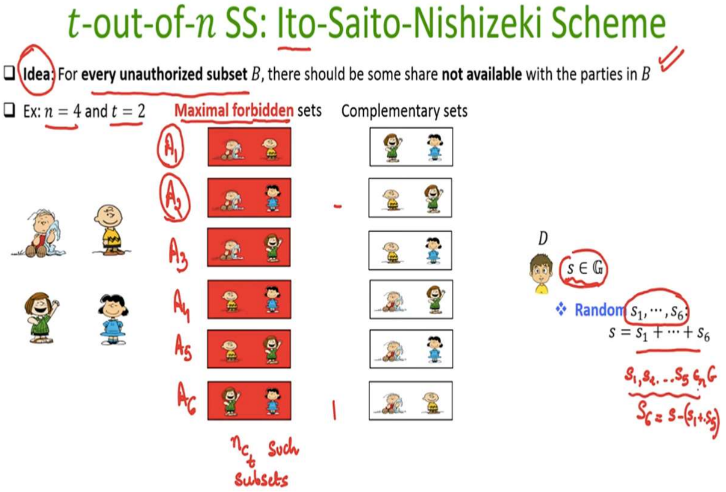
So, what we do is, we focus here on the maximal sized unauthorised subset. So, since $t = 2$, I am talking about the largest possible unauthorised subsets which can be there. So, I am talking about the case where my unauthorised subsets are of cardinality 2. Because, any subset of these forbidden sets are also trivially forbidden sets. So, I am basically trying to consider of the worst case scenario.

I am trying to consider about the largest pool, largest possible sized unauthorised subsets. So, that is why maximal forbidden subsets. By maximal, I mean here that any subset of these forbidden subsets are also forbidden subsets, they are not allowed to get back the secret. So, I have listed down all possible forbidden sets here. Let us call them as $A_1, A_2, A_3, A_4, A_5, A_6$. So, how many such maximal forbidden sets you can have?

You can have n choose t such subsets. Now, I focus on the complimentary sets. And when I say complimentary, I mean complement with respect to the set of n parties, not with respect to the power set. That is important here. So, by complementary I mean here; so, this set is basically the difference of the set of n parties and A_1. Second complimentary set is $P - A_2, P - A_3$ and so on.

And it is not necessary that complimentary set is an authorised set. It may or may not be, it depends. So, for instance, in this specific case, what is happening is that each complimentary set is also of size 2, and each set of size 2 is a potential forbidden set. So, in this specific case, since the compliment is take with respect to just the set of parties and not with respect to the power set of the set of shareholders, I cannot say that the complimentary sets are always authorised sets.

(Refer Slide Time: 25:18)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

Maximal forbidden sets

Complementary sets

D

$s \in \mathbb{G}$

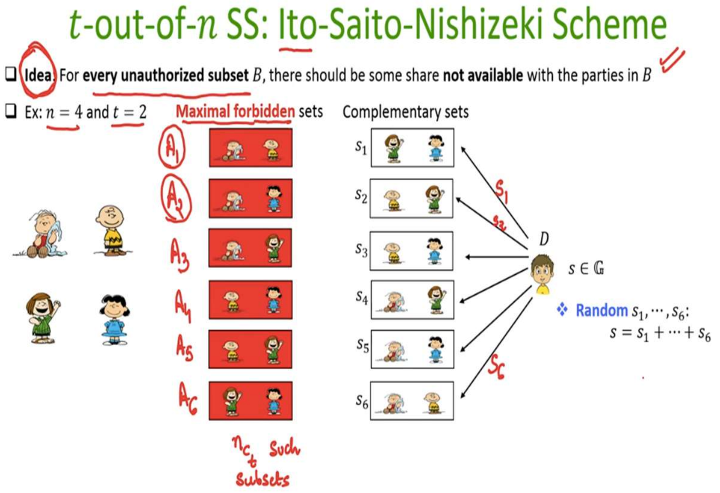
❖ Random $s_1, \cdots, s_6$: $s = s_1 + \cdots + s_6$

So, what is the idea that we want to follow here? We want to ensure that dealer should have shared its secret in such a way that, if the parties in A_1 try to get back the secret, there is something which is missing for them. Or, if the parties in A_2 is trying to reconstruct, there should be something which is missing for it, and so on. How the dealer can do that? So, dealer has a group element which it wants to share.

It now creates an instance of additive secret-sharing in the following way. So, how many forbidden subsets are here? There are 6 possible forbidden subsets. So, it randomly picks 6 group elements s_1 to s_6, subject to the condition that their sum is its secret s. So, how he can pick the random s_1 to s_6? Well, he can first pick s_1, s_2 up to s_5, uniformly at random from the group.

And then, it can set the sixth piece to be the difference of s and the first, summation of first 5 pieces. That means, for the same secret s, the shares s_1 to s_6 could be any 6 pieces from the group, because he is picking the first 5 pieces uniformly at random. That means, every time dealer wants to share the secret, the shares s_1 to s_6 will be different, with different probability. Now, how he should distribute this s_1 to s_6? Remember, we have to ensure that this idea is followed.

(Refer Slide Time: 27:04)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

- ❑ **Idea** For **every unauthorized subset** B, there should be some share **not available** with the parties in B
- ❑ Ex: $n = 4$ and $t = 2$

Maximal forbidden sets

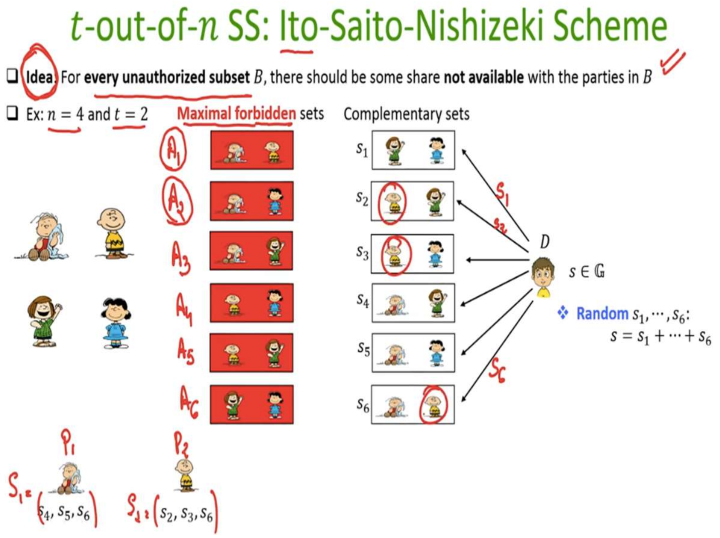
Complementary sets

❖ Random $s_1, \cdots, s_6$:
$s = s_1 + \cdots + s_6$

He gives s_1 only to the parties in $P - A_1$. That means, to the complimentary set with respect to A_1. And remember, when I say give, I mean, I am assuming here that there is a private channel between dealer and every shareholder. So, this s_1 piece is given to this party number 3 over the private channel, and party number 4 over the private channel. The piece s_2 is given to the complimentary set with respect to A_2.

And like that, the piece s_6 is given to the complimentary set of parties with respect to A_6. That is a simple secret-sharing mechanism. Now, we have to argue whether the correctness and the privacy properties are achieved.

(Refer Slide Time: 27:52)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

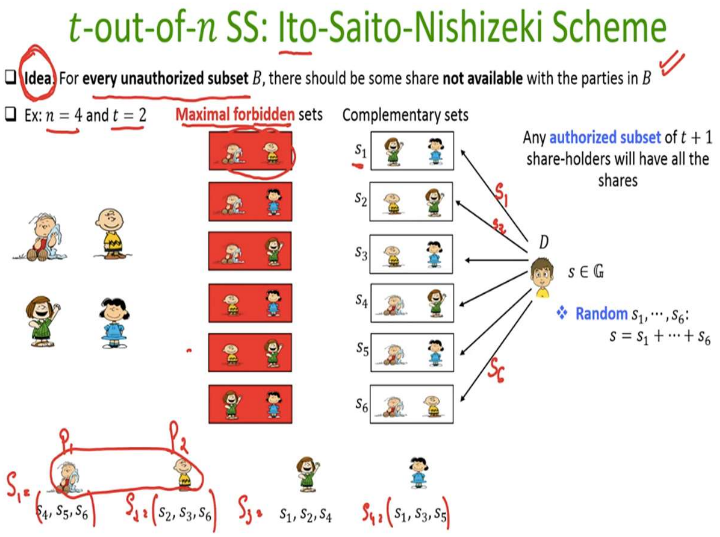
Maximal forbidden sets

Complementary sets

❖ Random $s_1, \cdots, s_6$: $s = s_1 + \cdots + s_6$

Before going into that, what will be the overall shares for the individual parties? So, now, what will be the overall share for party number P 1? Because party number 1 now is going to receive multiple piece of information from the dealer, so, he is going to receive s_4, s_5 and s_6. So, that will be its overall shares. What will be the shares of party number 2? He is part of this complimentary set, this complimentary set and this complimentary set.

(Refer Slide Time: 28:30)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

Maximal forbidden sets

Complementary sets

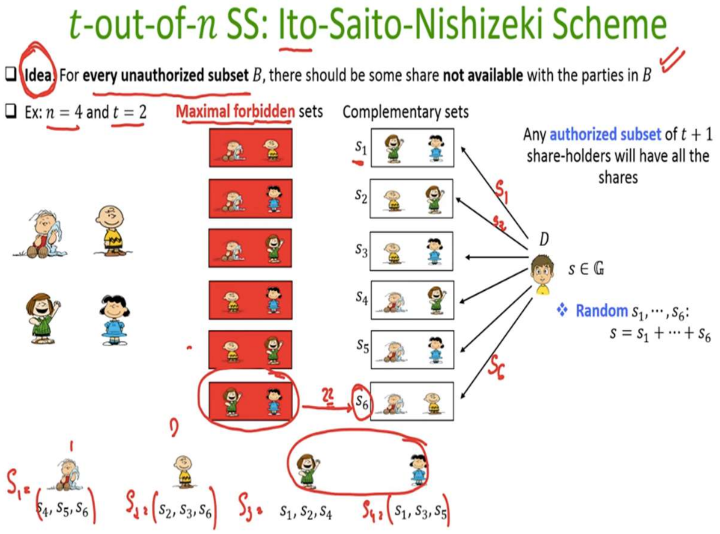
Any authorized subset of $t + 1$ share-holders will have all the shares

❖ Random $s_1, \cdots, s_6$: $s = s_1 + \cdots + s_6$

In the same way, this will be the overall shares of P_3, and this will be the overall shares of P_4. Now, here the privacy property is very easy to argue, and the correctness is slightly subtle to argue, compared to the previous scheme. In the previous scheme, correctness was easy to argue and privacy was subtle. Why the privacy is easy to argue here? So, imagine, it is the party 1 and 2 who tries to learn the secret, because they together constitute an unauthorised collection.

Will they be able to learn the secret? No. Because this idea is followed for them. Because, if I consider this unauthorised collection, consisting of P_1 and P_2, there is some piece of information namely s_1, which is not given to the parties P_1 and P_2. And since s_1 could have been any value from the group, that means, it is any candidate element from the group which dealer could have shared.

(Refer Slide Time: 29:53)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

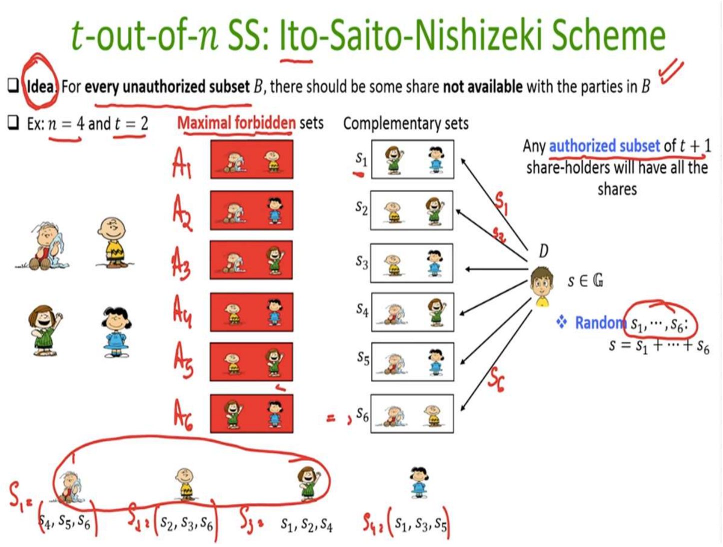
❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

In the same way, let us consider whether 3 and 4 will be able to learn anything. If, because, now you might be saying that, okay, 3 and 4 have too much of information; they have $s_1, s_2, s_4, s_1, s_3, s_5$. Will they learn anything about the secret? So, the point here is, this parties 3 and 4 constitute this candidate forbidden set. And with respect to this candidate forbidden set, there is some missing information namely s_6, which is not available with both P_3 as well as P_4.

And s_6 could have been any value from the group. And hence, it could have been any value from the secret space which dealer could have shared. So, that is why, you can focus on any unauthorised collection of 2 number of shareholders; with respect to them, there is at least 1 s_i which is missing for them.

(Refer Slide Time: 30:47)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

Maximal forbidden sets

Complementary sets

Any authorized subset of $t + 1$ share-holders will have all the shares

D

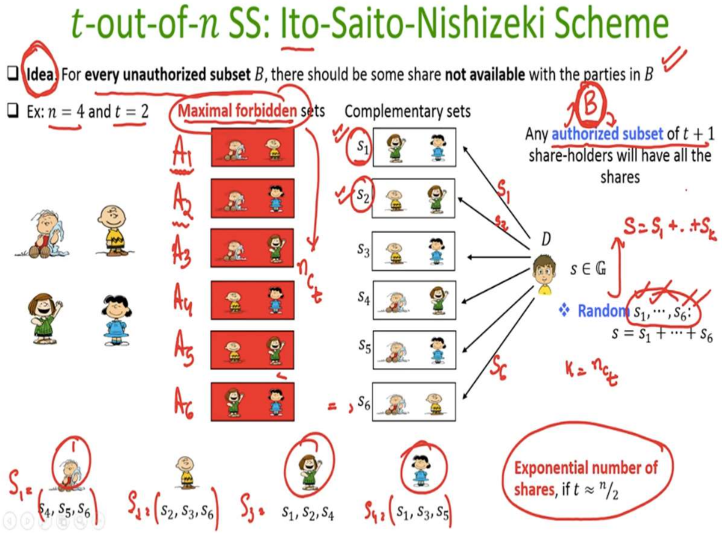
$s \in \mathbb{G}$

❖ Random $s_1, \cdots, s_6$: $s = s_1 + \cdots + s_6$

And hence, it could be any candidate secret from the group which dealer could have shared. That means, if A_1 is trying to learn, they will fail to find out s_1. If A_2 is trying to learn, they will fail to find out s_2 and so on. On the other hand, the claim here is that, you take any authorised subset of $t + 1$ or more number of shareholders, they always have all the 6 pieces to get back the secret.

So, for instance, if I consider 1, 2 and 3, will they have all the pieces? Yes, they have $s_1, s_2, s_3, s_4, s_5, s_6$, all within themselves, as a group, because they constitute an authorised subset. And hence, they can add them and get back the secret.

(Refer Slide Time: 31:45)



t-out-of-n SS: Ito-Saito-Nishizeki Scheme

❑ Idea: For **every unauthorized subset** B, there should be some share **not available** with the parties in B

❑ Ex: $n = 4$ and $t = 2$

Maximal forbidden sets

Complementary sets

Any authorized subset of $t + 1$ share-holders will have all the shares

D

$s \in \mathbb{G}$

❖ Random $s_1, \cdots, s_6$: $s = s_1 + \cdots + s_6$

Exponential number of shares, if $t \approx n/2$

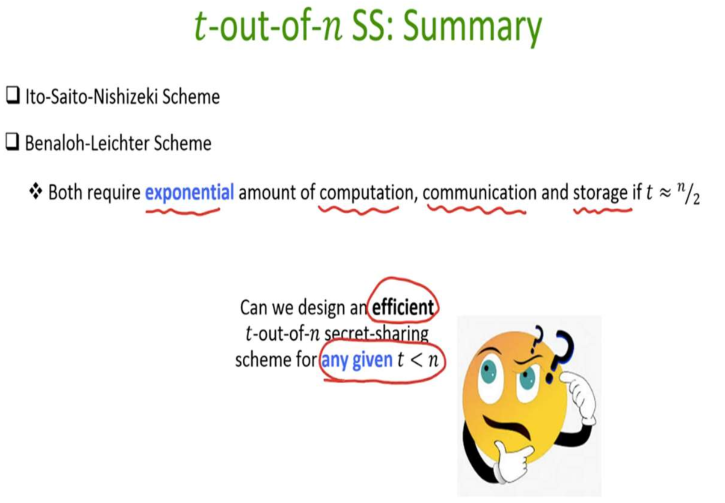
Or, if I focus on, say, 1, 3 and 4, together they constitute an authorised group. And indeed they have all the 6 pieces, and they will be able to get back the secret. How can we argue this for a general n and t, based on the construction? Well, you take any authorised collection B. Can I say that there is at least 1 party in B who will have s_1? Yes, the answer is yes, because there will be at least 1 party in the B who is not a member of A_1.

That is why B is an authorised collection. B is definitely not a proper subset of A_1, because a proper subset of A_1 is also a forbidden set. So, B definitely consists of at least 1 party who is not in A_1. And that 1 party will have s_1. In the same way, can I say that the party in B who is an authorised set will have s_2? Yes. My claim is, there will be at least 1 party in the authorised set B who is not a member of A_2.

And since it is not a member of A_2, it will have the piece s_2. And I can run the same argument. I can say that, you take any A_i; with respect to that A_i, there will be at least 1 party who is not in A_i but present in B, and that party will have the missing piece s_i. And that is why the parties in B will have all the pieces s_1, s_2, whatever is the number of s pieces. And hence, they can get back the secret.

So, this is again a very interesting construction of t out of n secret-sharing. But again, the problem here is that it requires exponential number of shares. Why? Because the number of forbidden sets will be n choose t. And that is why, if K is equal to n choose t, basically dealer has to distribute or compute K random pieces of shares for its secret s, and hence, it has to distribute. And that requires exponential amount of computation and communication.

(Refer Slide Time: 34:16)



t-out-of-n SS: Summary

❑ Ito-Saito-Nishizeki Scheme

❑ Benaloh-Leichter Scheme

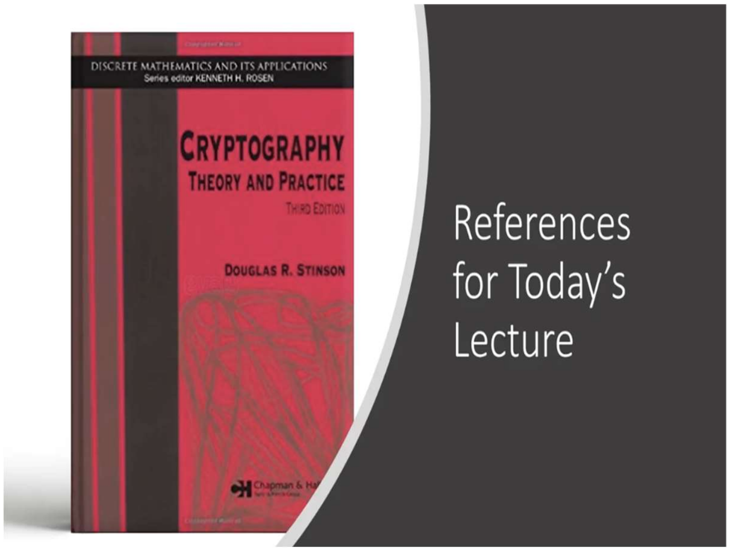
❖ Both require exponential amount of computation, communication and storage if $t \approx n/2$

Can we design an efficient t-out-of-n secret-sharing scheme for any given $t < n$

So, this is the summary of t out of n secret-sharing. We have seen 2 constructions, might look similar, but based on different ideas. And the downside is that both of them require exponential amount of computation, communication and storage. Why computation? Because dealer has to compute so many number of shares. Why communication exponential? Because, those many number of shares it has to communicate to the respective shareholders.

And why exponential amount of storage? Because each party has to store whatever information it is getting from the dealer. So, all these 3 resources will become exponentially large. So, now the next challenging interesting question is, can we design an efficient; by efficient, I mean polynomial time constructions, polynomial time solutions. Can I design efficient t out of n secret-sharing scheme for any given t < n. And that will be the focus of next lecture. Thank you.

(Refer Slide Time: 35:15)



References for Today's Lecture