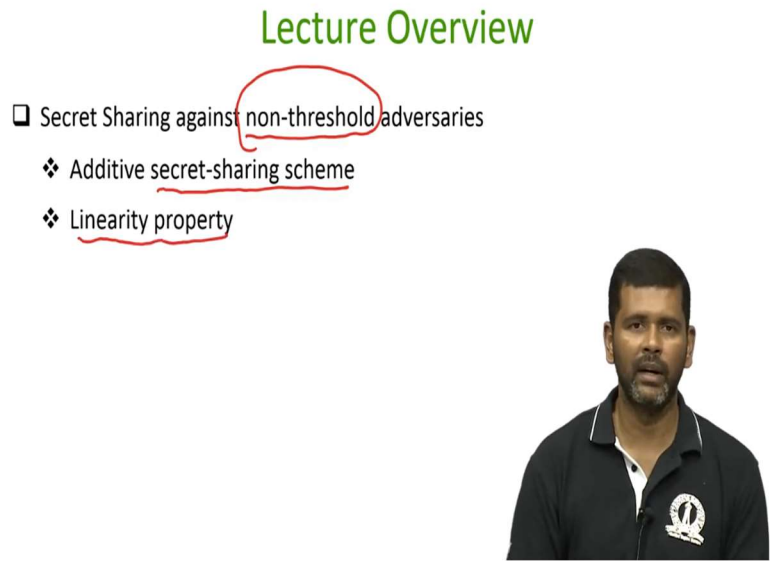
Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 3
Lecture - 14
General Secret Sharing

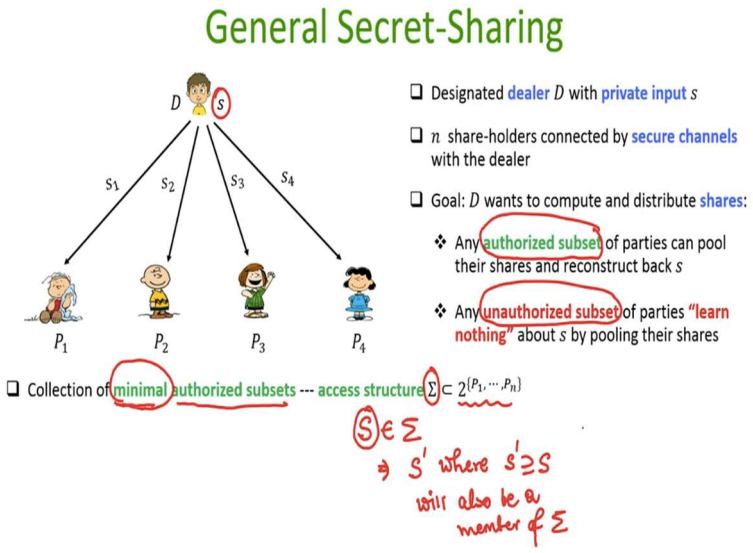
(Refer Slide Time: 00:35)



Hello everyone. Welcome to this lecture. So, in this lecture, we will see general secret-sharing schemes. Namely, we will see secret-sharing schemes against non-threshold adversaries. And by non-threshold adversaries I mean, where the cardinality of forbidden sets in my adversary structure need not be upper bounded by some specific threshold, unlike your threshold secret-sharing scheme.

So, we will see additive secret-sharing scheme adopted for the case of non-threshold adversaries. And it will be the case that the resultant secret-sharing scheme satisfies the linearity property.

(Refer Slide Time: 01:16)



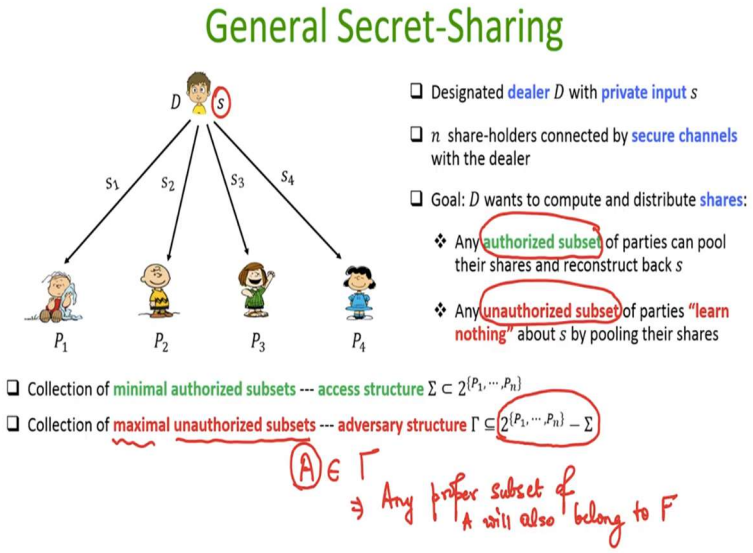
So, let us recall the problem of general secret-sharing. So, in the problem of general secret-sharing, you have a designated dealer with some private input and dealer is connected with individual shareholders by a secure channel. And there is some value s which dealer wants to share among these n shareholders; namely, it wants to compute shares of the values and distribute to the respective shareholders in such a way that the privacy under correctness properties are satisfied.

Correctness means, if we have any authorised subset of parties who are coming together, and if they pool their shares together, they should be able to get back the secret s; but if there is any unauthorised subset of parties who tries to learn the secret s, they should fail to do that, even if they have unbounded computing power. So, this collection of authorised subset of parties and unauthorised subset of parties will be given to us.

So, if we consider the set of all minimal authorised subsets, that is called as the access structure. So, it will be a proper subset of your power set of n shareholders. So, it will be collection of various subsets, and the collection is actually a collection of minimal subsets; because, if you have any authorised subset s belonging to Sigma, then it will be the case that any superset s prime where s prime is a superset of s, will also be a member of Sigma.

That is why, we focus only on the minimal sized authorised subsets, and the collection of such minimal sized authorised subsets will be present in Sigma. It will be the case that any superset of those subsets also are implicitly elements of Sigma; we will not be writing them down explicitly.

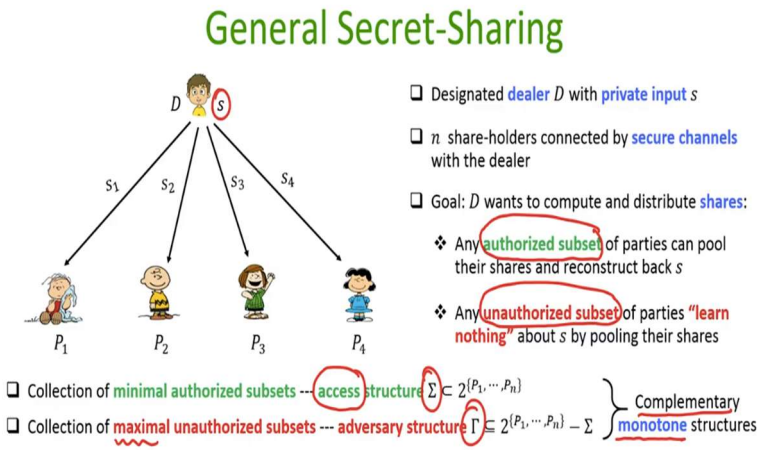
(Refer Slide Time: 03:41)



And in the same way, if I take the compliment of the access structure with respect to the power set, that will give us the adversary structure namely the collection of all maximal unauthorised subsets. And maximal in the sense that, if A is an element of Gamma, that means, if A is an unauthorised subset, then any proper subset of A will also belong to Gamma.

That means, if the parties in A, they alone cannot reconstruct back the secret s. Then, even if you remove any party further from the set A, they should also fail to get back the secret. That is what is the interpretation of saying maximal unauthorised subsets.

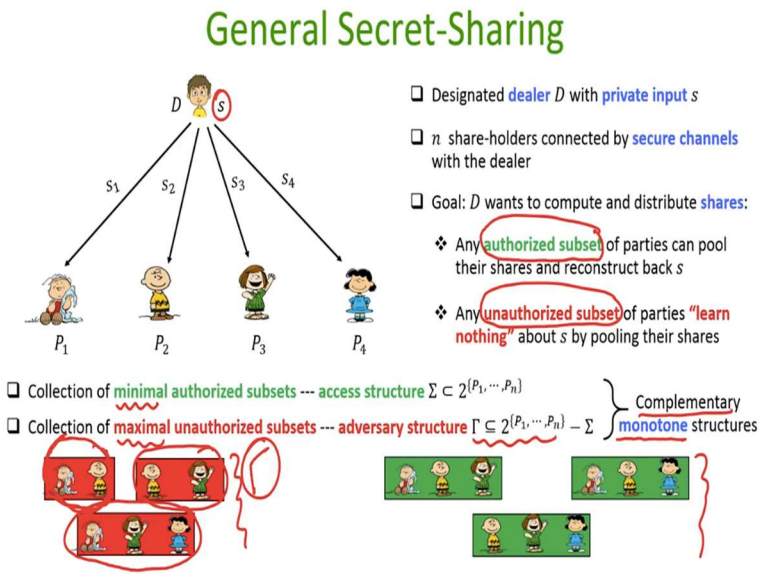
(Refer Slide Time: 04:54)



So, that is why, these two collection, this adversary access structure, and this adversary structure, they are complimentary in nature and they are often called as monotone structures.

Monotone in the sense, for the access structure, any superset of minimal authorised subset is also an authorised subset. But with respect to adversary structure, any proper subset of a maximal unauthorised subset is also an unauthorised subset. That is why it is called monotone structures.

(Refer Slide Time: 05:35)



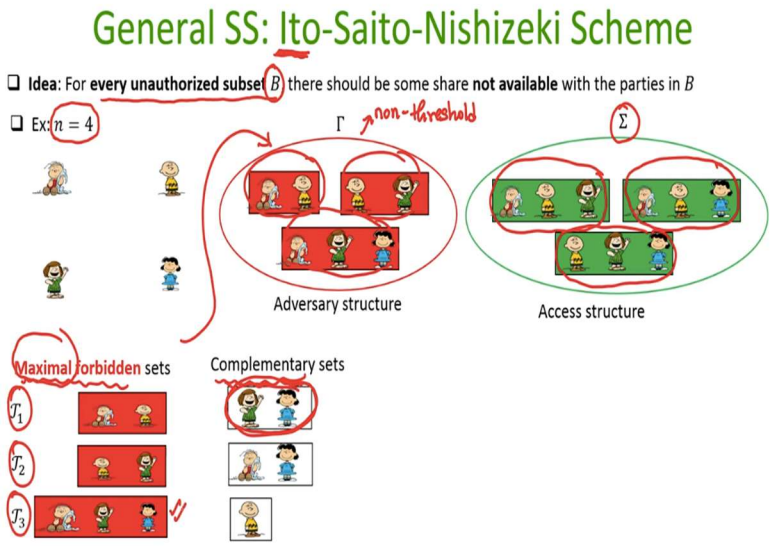
So, here is an example. So, it could be the case that this is my collection Gamma given to me, all in red. That means, party 1 and 2, they alone cannot reconstruct back the secret. That means, my secret should be distributed in such a way that P_1 and P_2 alone cannot reconstruct back the secret; or P_2 and P_3 alone, they should not be able to reconstruct back the secret; or P_1, P_3, P_4 alone, they should not be able to reconstruct back the secret.

So, they are the maximal unauthorised subsets given to me. This also means that; so, if I take the first subset here, this automatically means that P_1 alone or P_2 alone also should fail to get back the secret. But I am not writing down them explicitly, because they are proper subsets. I am focusing on the largest possible subsets who are unauthorised; that is what I mean by maximal unauthorised subset.

And now, if I take the complement of this all subsets which are explicitly here or implicitly here with respect to the power set, I will get the corresponding access structure, namely the minimal authorised subsets. So, this means that, 1, 2 and 3, if they come together, then fine, they should be able to get back the secret; or if 1, 2 or 4, they come together, they should be able to get back the secret; or if 2, 3, 4 come together, they should be able to get back the secret. This also means that if 1, 2, 3, 4 also come together, they should get back the secret.

But I am not writing down it explicitly as an authorised set, because I am focusing on the smallest possible subsets which are authorised. So, let us see the secret-sharing scheme for a non-threshold adversary. By adversary, here I mean collection of unauthorised subsets. Our goal is to design a secret-sharing scheme where an adversary; and by adversary I mean an adversary who can control any subset from the adversary structure; should fail to get back the secret s. That means, from its viewpoint, the probability distribution of the shares that it is seeing is independent of the underlying secret.

(Refer Slide Time: 08:06)



So, we had already seen the secret-sharing scheme due to Ito et al. for the threshold adversary structure, where the cardinality of each unauthorised subset was t. But now, we want to generalise it for any arbitrary adversary structure, where the cardinality of individual subsets in the adversary structure is not upper bounded by a threshold t. So, if you see this example, in my adversary structure, I had sets, I had subsets whose cardinality was 2 and I have also subsets whose cardinality is 3.

So, that is why, this is not an example of a threshold adversary structure. So, my goal is now to design a secret-sharing scheme for such an arbitrary non-threshold adversary structure. So, the idea here remains the same. We want to distribute the secret or we want to split the secret in such a way that, for every potential unauthorised subset B, there should be some piece or some share missing for that unauthorised subset.

And since that missing piece will be random from the viewpoint of the parties in B, it could be the case that any value from the secret space has been shared by the dealer. So, again, to

demonstrate the scheme, I take a specific example. So, imagine this is the adversary structure given to you, and this is a non-threshold adversary structure, because different unauthorised subsets are of different cardinality; you have subsets of cardinality 2, and you have one subset whose cardinality is 3.

So, my goal is to design a secret-sharing scheme where, if these 2 parties alone try to learn, they should fail; if these 2 parties alone try to learn, they should fail; or if these 3 parties alone try to learn, they should fail. And the corresponding access structure is this. That means, the sharing should also have the property that if these 3 parties come together, they should be able to get back the secret; or if these 3 parties come together, they should be able to get back the secret; or if these 3 parties come together, they should be able to get back the secret.

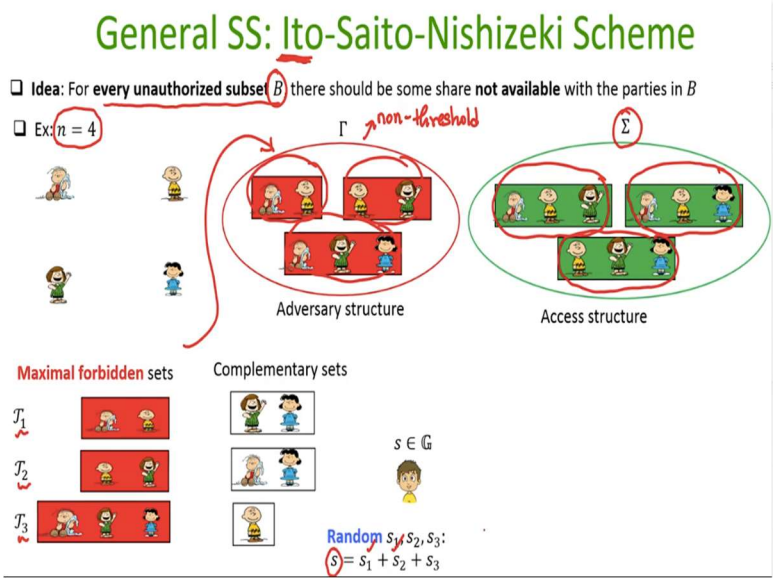
So, let us simply generalise the threshold secret-sharing scheme that we had seen by Ito et al. when we discussed the threshold secret-sharing, for the case of non-threshold adversary. The idea will remain the same. We will list down the various subsets from my adversary structure, namely, the various maximal forbidden sets which are given to me as per the adversary structure. So, we are given 3 potential unauthorised subsets.

Remember, implicitly, any proper subset of these subsets are also unauthorised. But we will not be focusing them explicitly, we will be focusing only on the maximal forbidden sets. That is important here. I am not again considering a red box where only P_1 is present, or a red box where P_2 is present. They are implicitly present in my adversary structure Gamma, but I am not going to consider them.

I am going to consider only on the largest possible forbidden subsets which are given to me; and I am given 3 such subsets; call them as this fancy T_1, fancy T_2, fancy T_3. And now, I take the complimentary sets of this forbidden sets, complimentary with respect to the set of n parties, not with respect to the power set. Remember, the axis structure is computed as the complement of the adversary structure; but as part of the secret-sharing algorithm, these complimentary sets are basically just the complimentary sets with respect to the set of n parties.
That means, if P_1, P_2 is a forbidden set, the complement set will be P_3 and P_4. If 2 and 3 is a forbidden set, then the complement set is 1, 4, and so on. And remember, it is not the case that these subsets in the collection of the complement sets, they are member of the access structure;

no. So, for instance, these 2 parties, they also constitute a potential forbidden set, because a bigger subset of these 2 parties is already listed as tau 3 here. So, do not get the impression that these complimentary sets constitute authorised subsets. I have just taken the compliment with respect to the set of parties.

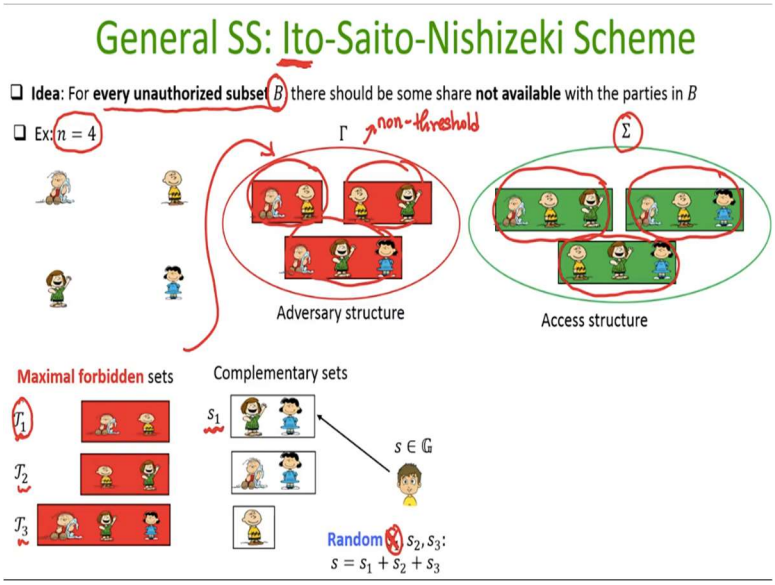
(Refer Slide Time: 13:15)



Now, to share the secret s, what dealer will do is the following: It will check how many potential unauthorised subsets are given in the adversary structure. In this case, there are 3 potential unauthorised subsets. So, it has to now compute 3 random shares for the secret s, which sum up to the secret s. And how it can do that? It can randomly pick s_1, it can randomly pick s_2, and it can set s_3 to be the difference of s and summation of s_1 and s_2.

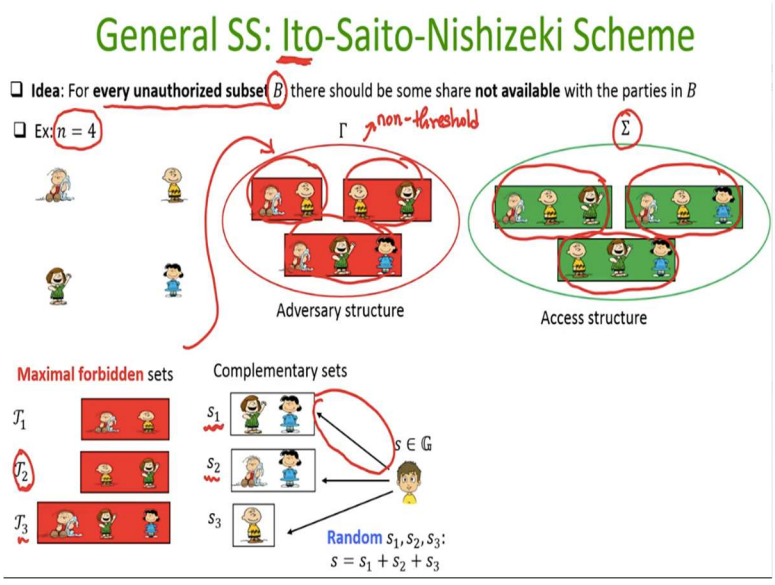
If there would have been more sets in my adversary structure, then dealer needs those many additional pieces as well. Now, how he should distribute s_1, s_2, s_3? Which group of parties should get s_1? which group of parties should get s_2? and so on.

(Refer Slide Time: 14:15)



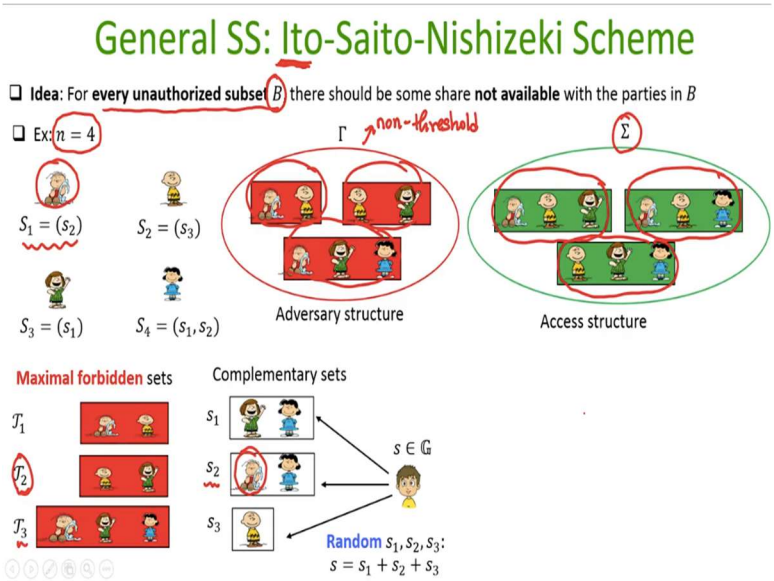
So, it gives the first piece s_1 to the complement of τ_1. And the idea is that, if the subset τ_1 tries to get back the secret s, they should fail to do that, because the piece s_1 is not available with them. And in the absence of s_1, the parties in $\tau_1$will fail to learn what is the secret s. That is idea.

(Refer Slide Time: 14:47)



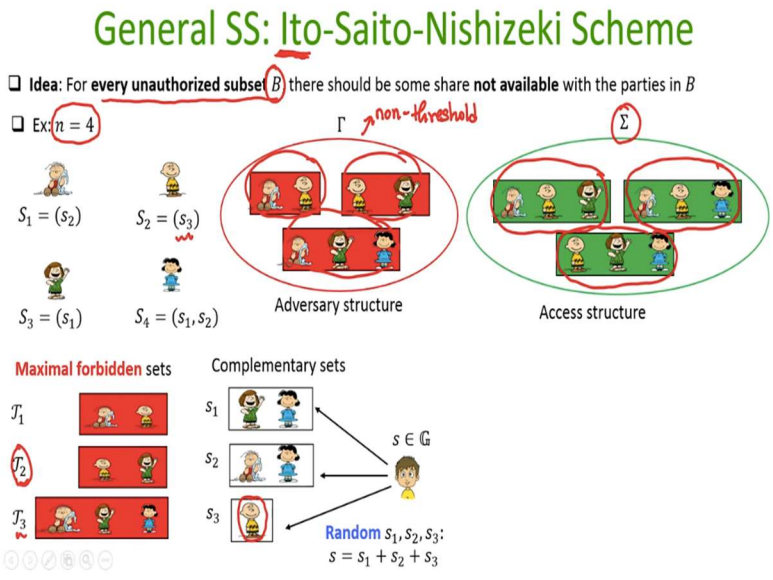
Similarly, the piece $s_2$will be given to the complement of τ_2, namely, to these 2 parties. And the idea is that if the parties in τ_2 now tries to learn the secret, they will fail to do that, because the piece s_2 is missing for them. And in the same way, the piece s_3 is given to the party, all the parties who are in the complement of τ_3. And when I say it is given by this arrow, I mean to say that; remember, between dealer and every shareholder, there is a secure channel; so, whatever pieces are supposed to be given to respective parties, they are communicated over the secure channel available between the dealer and the corresponding shareholder.

(Refer Slide Time: 15:29)



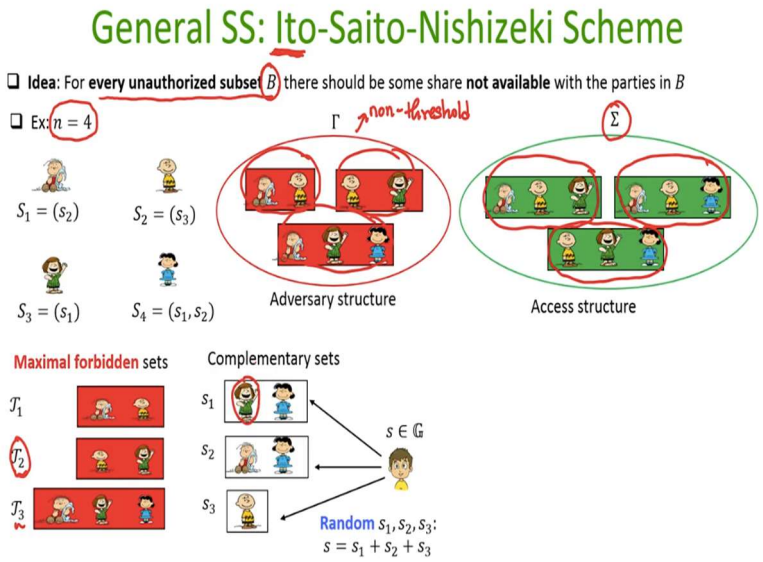
So, now, what will be the overall share for the individual party? The overall share in this secret-sharing scheme for the individual party will depend upon the number of complimentary sets where each individual party is present. So, if I consider this first party P_1, it is present only in this second complimentary set. And as part of that, it is getting the piece s_2. So, that will be the overall share of this party P_1.

(Refer Slide Time: 16:02)



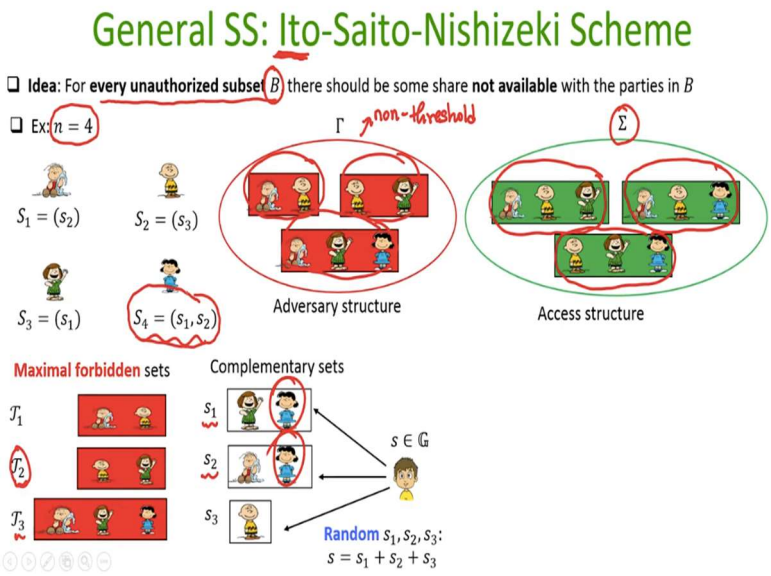
In the same way, if I consider the second party, the second party is present only in the third complimentary set, and as part of that, it is getting the information s_3.

(Refer Slide Time: 16:15)



If I consider the third party P_3, it is present only in this complimentary set and getting s_1. So, that will be its overall share.

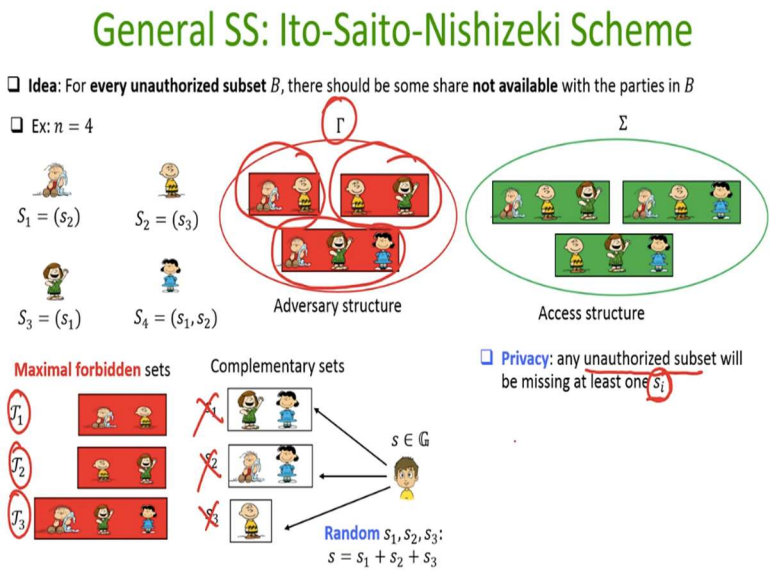
(Refer Slide Time: 16:21)



And if I consider the fourth party; now, you see, the fourth party is member of 2 complimentary sets. As part of 1 complimentary set, it is getting s_1; as part of another complimentary set, it is getting s_2. So, the overall share for this fourth party will be the concatenation or the collection s_1, s_2; both will be considered as the share of s_4. So, now, you can see here, unlike your Shamir secret-sharing where each party gets the same number of share, namely, 1 field element; here, different parties may get different number of shares, depending upon how many complimentary sets they belong to; it may not be symmetric.

So, now, let us try to argue here that whether this scheme satisfies the privacy property and whether this scheme satisfies the correctness property.

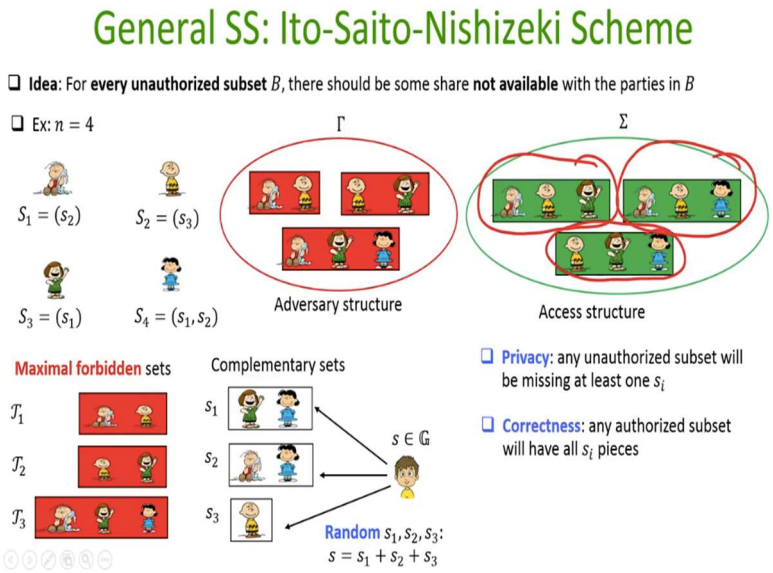
(Refer Slide Time: 17:15)



The privacy is very easy to argue, because, that I have already demonstrated when I was explaining you how the shares are communicated to the respective complimentary sets. My claim here is that, you take any unauthorised subset from this adversary structure; for that unauthorised subset, there will be at least 1 piece s_i as such which is missing. Say, if I consider for instance γ_i, s_1 is missing; if I consider γ_2 as a potential unauthorised subset, s_2 is missing; if I consider γ_3, then s_3 is missing.

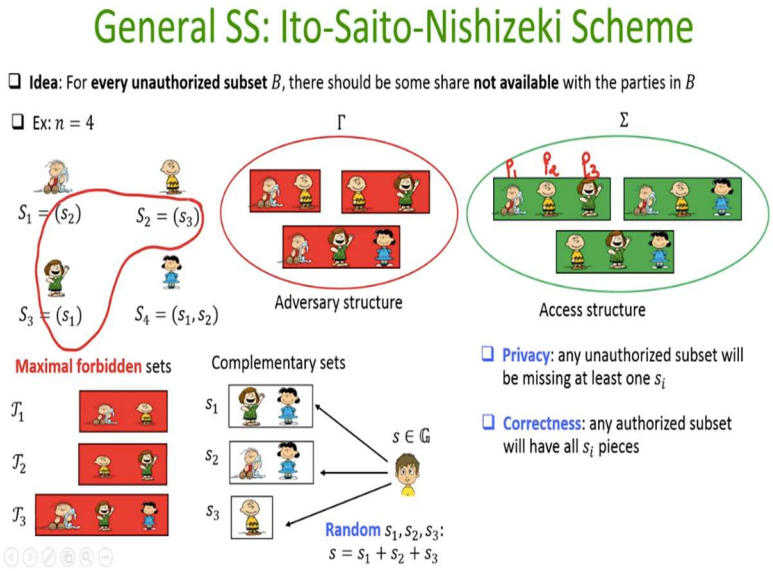
And you cannot have more than 1 unauthorised subset trying to learn the secret. That is not allowed. Remember, when I say non-threshold adversary structure, then it can control only 1 potential unauthorised subset from the adversary structure. So, if it controls the first unauthorised subset, it will fail to learn; or if it controls the second unauthorised subset τ_2, it will fail; or if it controls the parties in the third unauthorised subset, s_3 will be missing. So, it will fail to learn the secret. So, privacy is very easy to argue here. Now, comes the correctness property.

(Refer Slide Time: 18:41)



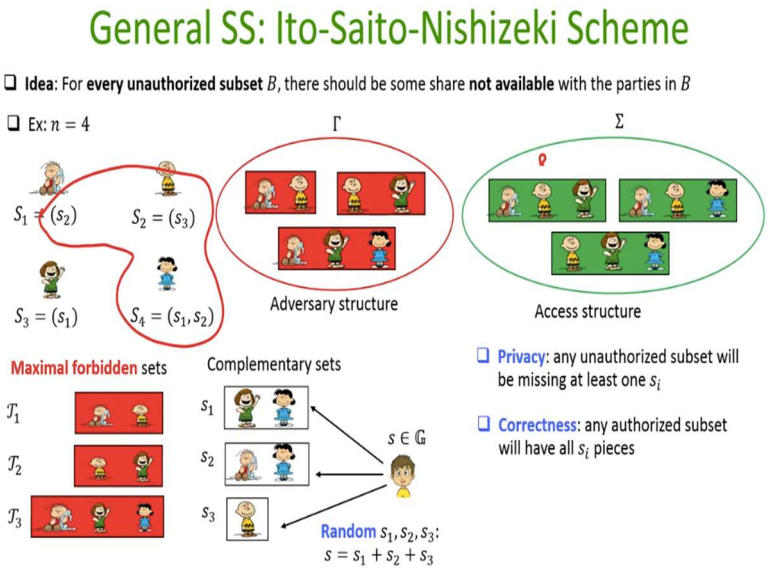
Can I say that if any collection of these green parties try to learn the secret, they will have enough information to get back? Yes.

(Refer Slide Time: 18:54)



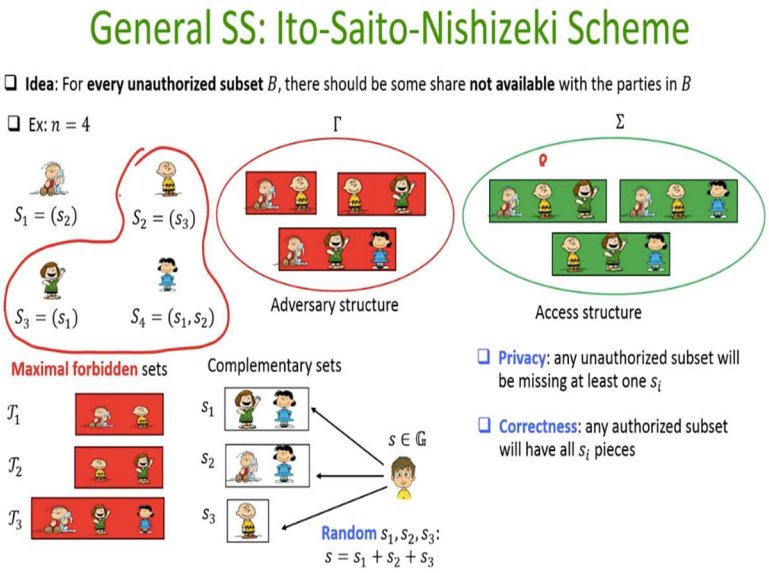
So, let us consider the case when P_1, P_2 and P_3 tries to learn the secret. So, P_1, P_2, P_3, collectively they have s_1, s_2, s_3. And then, they can sum them up and get back the secret. Or, let us see whether P_1, P_2, P_4, collectively they can learn.

(Refer Slide Time: 19:15)



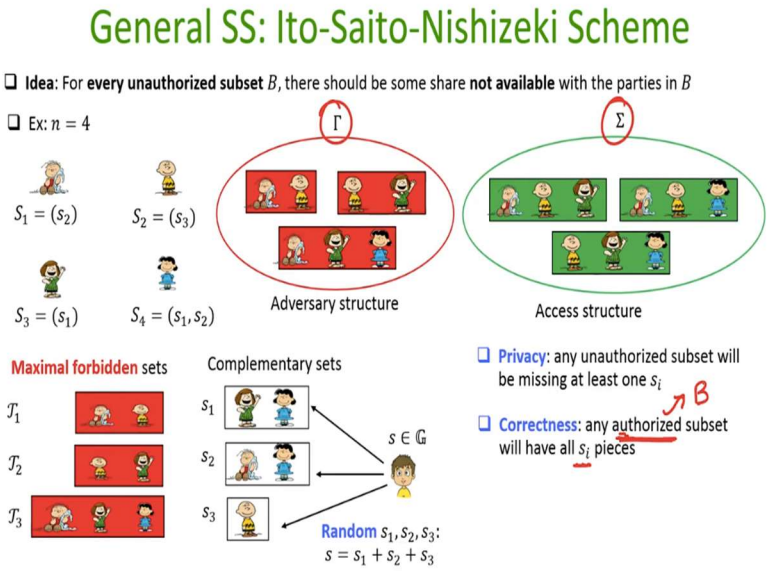
So, yes, P_1, P_2, P_4, collectively they can learn; because, if they come together, they have s_1, s_2, s_3.

(Refer Slide Time: 19:29)



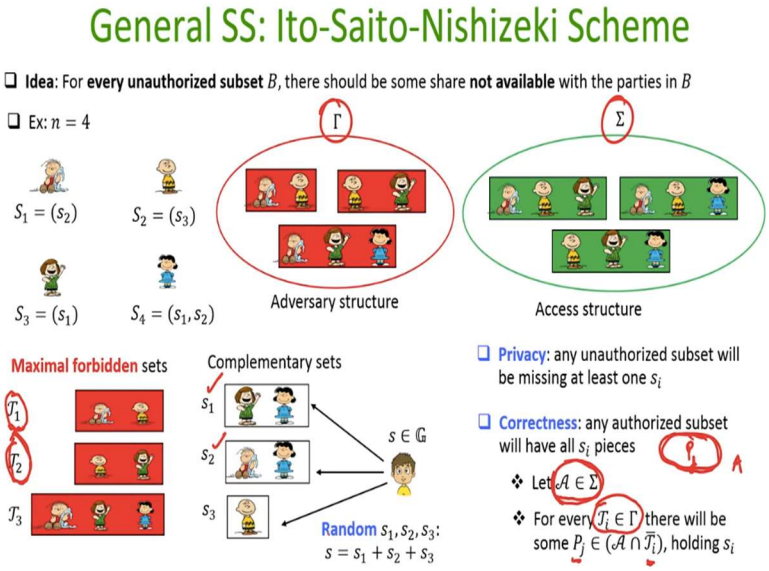
Or if 2, 3, 4 comes together, then also, collectively they have s_1, s_2, s_3, and hence they can learn. Well, in this specific example, correctness is there; but we have to now argue that, okay, when we run this secret-sharing algorithm with respect to a general Gamma and a general Sigma, the correctness will be satisfied.

(Refer Slide Time: 19:47)



The claim here is the following: If you take any green subset, call that green subset as B. It could be either first green subset or second green subset or third green subset or any potential green subset from your access structure. My claim is, it will have all the s_i pieces. Namely, if the secret s would have been divided into, say k number of pieces, then any authorised subset B will have all those k s_i pieces. It will have k_1; that collectively, it will have s_1, s_2, s_3, s_4, s_i, s_k, everything. And if they have all the s_i pieces, they can add them together and get back the secret s. Now, why this claim is true?

(Refer Slide Time: 20:44)



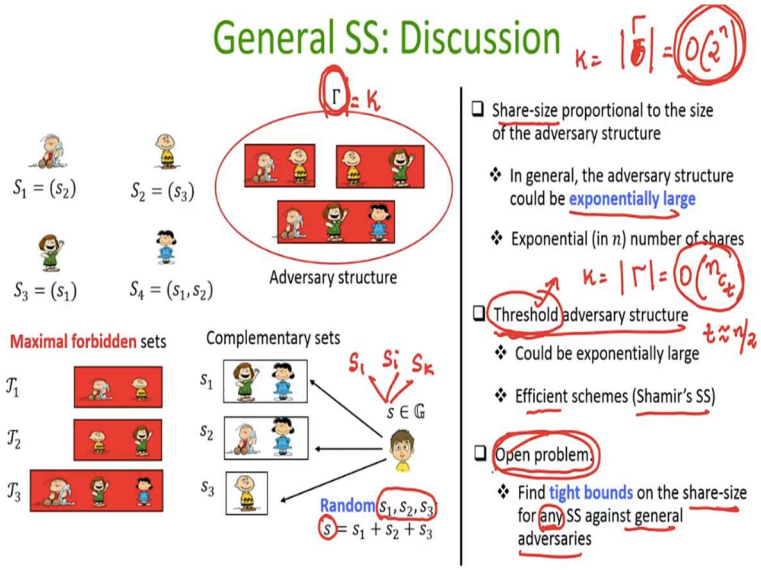
So, I have used the notation A here, for the authorised subset. So, consider an arbitrary authorised subset A, belonging to the access structure. Now, definitely, A will not be a subset of any of the forbidden sets; because, if A is a subset of a forbidden set, then how at the first

place it is belonging to the access structure? Because, access structure consists of the complimentary parties with respect to the adversary structure.

So, no subset of these red coloured subsets will be present in my Sigma. So, that means, if at all I am considering a subset A, a green subset of parties; and now, if I compare it with τ_1, there will be at least 1 party in A, who is not a member of τ_1. And that party who is not a member of τ_1, but a member of A, will have the piece s_1. In the same way, if I consider τ_2 and the same subset A, this subset A will have definitely 1 party who is not a member of τ_2; and dealer would have given the piece s_2 to that party.

In general, you take any bad subset T_i from your adversary structure, there will be at least 1 party in your set A, call it P_j, who will not be a member of τ_j. And that party P_j would have been given the peace s_j, by the dealer; because, that is how dealer would have distributed the pieces. That means, if I take all the parties in this authorised subset A, collectively they will have s_1, s_2, s_i, s_k, all the pieces of s; and hence, they can add them together and get back the secret s. That is the simple idea here.

(Refer Slide Time: 22:54)



So, that is our secret-sharing scheme now, against the general adversary structure. And if you see here that the share size is proportional to the size of the adversary structure; because, the secret s is divided into a number of pieces which is same as the cardinality of your adversary structure. So, if they are, if there are k number of subsets in the adversary structure, then basically, dealer has to now divide his secret s into k pieces.

But in general, the size of your adversary structure could be exponentially large. In this specific example, it is only collection of 3 potentially bad sets, but in general, if I consider a general n, then my adversary structure could be as large as order of 2^n. There could be exponentially many number of subsets in my adversary structure. And that means, my k will be exponentially large.

And hence, exponentially many number of s_i pieces have to be computed by the dealer and distributed. And this is unlike your threshold adversary structure, which also could be exponentially large. For the case of threshold adversary structure, my k which is the cardinality of adversary structure, is basically order of n choose t; because, there could be n_{C_t} number of subsets of size t, and each potential subset of size t is a potential bad subset.

And if I say t is, if I consider the case where t is roughly n/2, then this quantity n_{C_t} becomes exponentially large. But, even though my threshold adversary structure is a special case of general adversary structure, and my threshold adversary structure could be exponentially large, we have seen that, even for an exponentially large adversary structure with respect to the threshold case, we have efficient secret-sharing scheme, namely the Shamir secret-sharing scheme, where dealer need not have to distribute exponentially many number of shares; to each party, it just has to give 1 share.

But Shamir secret-sharing scheme works for a specific threshold which is given to you, and you cannot run Shamir secret-sharing scheme for a general adversary structure; because, for a general adversary structure, the cardinality of individual subsets could be anything. So, now, a big open problem in the domain of secret-sharing is the following: Can we find tight bounds on the share size needed for any secret-sharing scheme against any given general adversary structure?

I stress, for any secret-sharing scheme. For the scheme by Ito et al., we know that, okay, we may require exponentially many number of shares. But open problem here is the following: Can one design a secret-sharing scheme with respect to any given general adversary structure, where we end up distributing only polynomial many number of shares? Or, if we cannot do that, then prove that what is the minimum number of shares that any secret-sharing algorithm

has to compute and distribute for tolerating that given general adversary structure. That is a big open problem in the domain of secret-sharing. With that, I end this lecture. Thank you.