


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

Lecture - 06
EIG Protocol for Perfectly - Secure Byzantine Agreement: Analysis Part II

Hello everyone. Welcome to this lecture; in this lecture we will complete the proof of the consistency property for the EIG protocol.

(Refer Slide Time: 00:31)

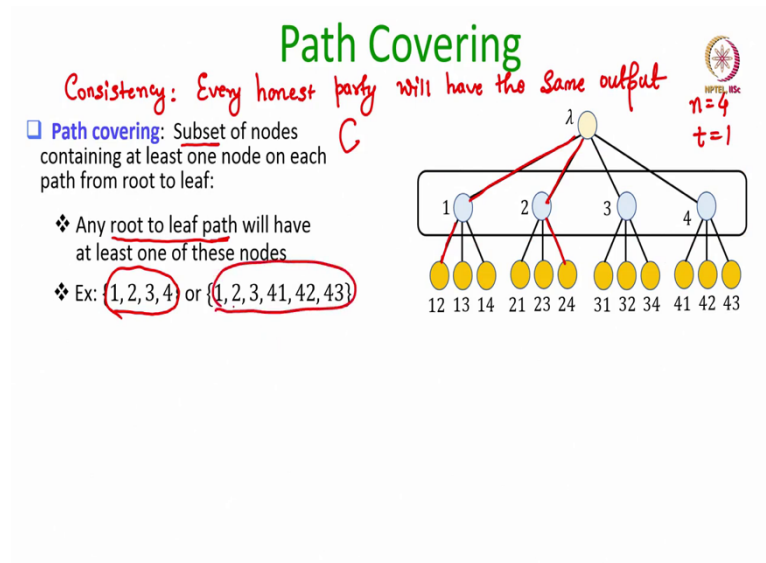
Lecture Outline



- ❑ Analysis of the EIG protocol
 - ❖ Proof of the consistency property

In the last lecture we have proved validity and the liveness property.

(Refer Slide Time: 00:37)



So, to prove the consistency property. And what is the consistency property? The consistency property is that every honest party will have the same output, irrespective of what messages the bad parties or the corrupt parties communicate during the protocol. And to prove this, we will use this notion of path covering in the EIG tree.

What is a path covering? It is a subset of nodes any subset of nodes, there is no restriction on its cardinality, any subset of nodes such that it is guaranteed that if you go from root to leaf via any path in the EIG tree you will hit at least one of the nodes in the subset, ok. So, call the subsets to be say C , the subset of node C will be called path covering if at least one node from this subset C occurs along any path from the root to the leaf in the EIG tree.

So, let me demonstrate it. So, one path covering in this EIG tree where n is equal to 4 and t is equal to 1, could be the subset 1, 2, 3, 4, that is one candidate path covering. Because you see you go from the root to any leaf node, you will hit one of the nodes in this rectangle. Any path from the root to leaf, either you will encounter 1, or you will encounter 2, or you will encounter 3, or you will encounter 4. Another candidate path covering is this collection of nodes ok.

(Refer Slide Time: 02:55)

Path Covering

Consistency: Every honest party will have the same output

Path covering: Subset of nodes containing at least one node on each path from root to leaf:

- Any root to leaf path will have at least one of these nodes
- Ex: $\{1, 2, 3, 4\}$ or $\{1, 2, 3, 41, 42, 43\}$

Common node: One for which all honest parties have the same newval.

- If label ends in an honest party's index, **Lemma 1** implies it's common.
- Might be others too.

In the EIG protocol, does there exist a set of common nodes which constitutes a path covering?

Handwritten notes:

- $n=4$
- $t=1$
- $x = (i_1 i_2 \dots i_k)$ and if p_k is honest \Rightarrow newval(x) will be the same in every honest party's copy of EIG tree

Of course, the entire tree can be considered as a path covering, that is a trivial path covering, ok. Because if you take all the nodes in the tree, then definitely any path from the root to leaf will encounter, will have at least one of the nodes from the collection. So, that is the definition of path covering. The next property that we will use or the next concept that we will use is that of common nodes.

So, we will call a node, a common node in the EIG tree if the new value, which is assigned to that node is same across all the honest parties copy of the EIG tree. That means all the honest parties assigned the same new value to that node, if that is the case then the new node will be called as a common node, otherwise it will not be considered as a common node.

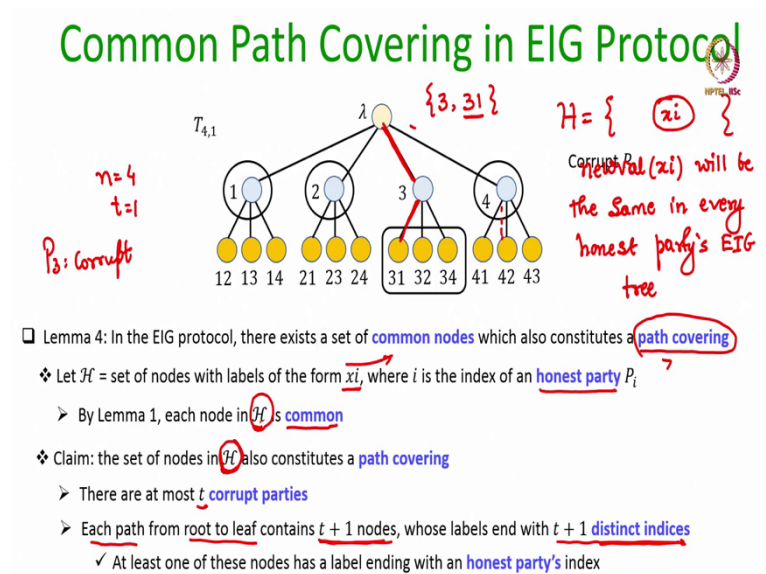
And from the previous lecture, if we focus on lemma 1; then lemma 1 says that if I take any node whose label ends with an index of an honest party then it is a common node. That means, if x is of the form i_1, i_2, \dots, i_k and if p_k is honest, then we have shown in the last lecture that newval of x will be the same in every honest parties copy of EIG tree right.

Of course, there could be other nodes whose label may not end with an index of an honest party; they could be common as well depending upon how the corrupt parties behave during the protocol execution. For them, for those nodes the newval could be common or the newval may not be common. So, we cannot say that they are common nodes, but what we can say is

that if there is a node whose label ends with an index of an honest party, definitely it is a common node.

Now, we want to answer this question to prove the consistency property. In the EIG protocol does there exist a set of common nodes, which also constitutes a path covering ok. That means a collection of nodes C which is not only common, but which also constitutes a path covering.

(Refer Slide Time: 06:04)



And interestingly the answer is yes, and that is lemma number 4 which states that in the EIG protocol there always exist at least 1 set of nodes which is common and which also constitutes a path covering.

What is that subset of nodes? That subset of nodes is the set of nodes whose label ends with an index of an honest party. That means, it is the collection of all nodes of the label of the form x followed by i , where x is some string, it could be an empty string followed by i , where i corresponds to the index of an honest party. Lemma number 4 basically states that that the collection of node H is common; that means, it has the same newval across all the honest parties EIG trees and it also constitutes a path covering as well.

So, let us prove both these properties. The first property namely the set of nodes in H is common, comes from lemma number 1, if I take any node from the set H . So, H is a collection of many nodes, suppose I take an arbitrary node from H , which is of the form x

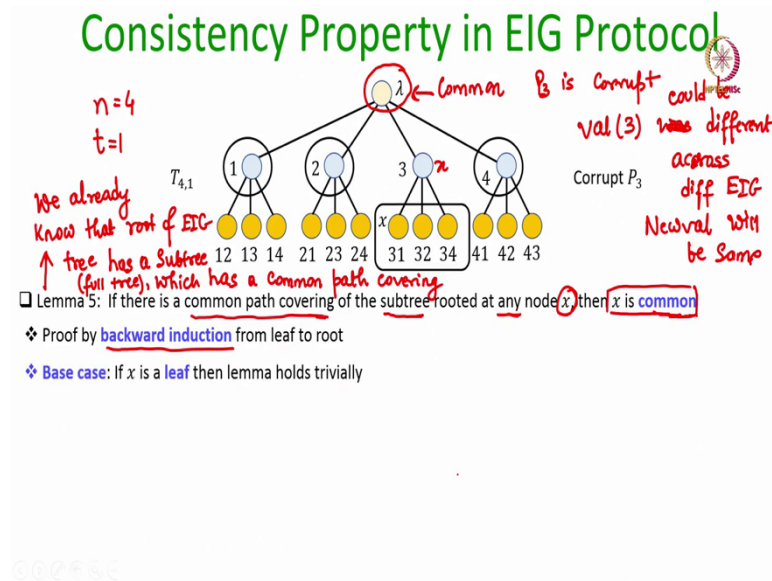
followed by i , then we have shown in lemma 1 that newval of x_i will be same, will be the same in every honest parties EIG tree ok.

So, the subset of nodes H is definitely common. Now, what we are going to claim here is that the set of nodes in H also constitutes a path covering; that means, if I consider any path from the root to the leaf, say the path where I go to the node to 2 and then go to the node 2 4 or if I consider the path where I go from root to 4 and then from 4 to 2. The claim is in any of these paths, at least one node from the set H will occur.

And the proof simply follows from the fact that there are at most t corrupt parties and what we know is that each path from the root to leaf will have $t + 1$ nodes, because there are $t + 1$ layers. And each node has a label ending with the index of a distinct party. The end index will never get repeated right; that means, if I consider any path say, I take this example where n is equal to 4 and t is equal to 1 and say I take this path, ok. So, what are the nodes which we are encountering in the path? We are first encountering 3 and then the node 3 1 and imagine P_3 is corrupt. Now, since P_3 is corrupt it is not a part of this set H , but the node 3 1 is a part of the set fancy H and that is why we have encountered a node from the set H along this path, right.

So, basically the proof for this claim is that, since there will be $t + 1$ distinct nodes in any path from the root to leaf and among those $t + 1$ nodes, there are $t + 1$ distinct parties, which occur as the last index. Among those $t + 1$ last index parties, t could correspond to corrupt parties. But at least 1 index will be there corresponding to an honest party right, and that is why we will encounter at least 1 node from this set fancy H , when we go from root to leaf ok.

(Refer Slide Time: 11:08)



So, now we have shown that in EIG tree, the set of nodes whose label ends with the index of an honest party constitutes a common path covering. Now, based on this notion of common path covering we are going to claim the following, that if in the EIG tree at if I focus on any sub tree, need not be the full EIG tree, but any sub tree rooted at the node x . And suppose that sub tree is guaranteed to have a common path covering, then the root x is also common, ok.

So, for instance if I take this example here when n is equal to 4 and t is equal to 1 ok. So, what I am claiming is that if I take a common path covering of the sub tree say rooted at this is my x suppose, this is my candidate x and I take the case where P_3 is corrupt.

What I am claiming here is that the newval of x will be same across all honest parties tree, even though P_3 is corrupt, even though the val of 3 was different across different EIG trees, newval will be same. Or in general case, if I take any subtree rooted at the node x and if it is guaranteed to have a common path covering then x is common, that is the statement which we want to prove.

Now, before going into the proof of this lemma, what is the consequence of this lemma? How it ensures that the consistency property is satisfied? We already know that the root of EIG tree has a subtree, namely the full tree, which has a common path covering. We have already proved that, namely if we take the set of nodes fancy H that constitutes a common path covering for the entire tree. And hence for the tree rooted at the main root of the EIG tree and if this lemma 5 is true then, that shows that the root node of the EIG tree will be common

across all the EIG trees. That means it will have the same new value across all the EIG trees, even if it has some of the children's ending with the index of a corrupt party.

So, it is basically lemma 5 which helps us to conclude the consistency property. Now, let us prove the lemma number 5 and again we will use backward induction because this lemma number 5 is for any node x . So, x could be a node at layer 1 or it could be a node at layer 2 or it could be a node at layer $t + 1$.

The lemma statement is true for any x . So, since we want to show that it is true for any x , we want to show that it is true irrespective of the length of the label x and that is why we are going to use an induction on the length of the label x .

So, we start with the base case, when x corresponds to a leaf node namely, it has the largest label in terms of size. So, assume that the hypothesis of the lemma is true for this x , namely there is a common path covering of the subtree rooted at this leaf x then the lemma trivially holds.

Because, if there is a common subtree at this rooted at this x ; then what is the subtree rooted at this x ? It is the node x only; that means, x itself is a part of that common path covering. And if x itself is a part of that common path covering, then because of the definition of common node the new value of x is same, it is common across all the honest parties EIG tree.

(Refer Slide Time: 16:53)

Consistency Property in EIG Protocol

Lemma 5: If there is a common path covering of the subtree rooted at any node x , then x is common.

Proof by backward induction from leaf to root

- Base case:** If x is a leaf then lemma holds trivially.
- Inductive hypothesis:** Let statement be true for all level- $(k+1)$ nodes x .
- Inductive step:** let x be a level- k node.
 - Case I:** x is a part of the common path covering of the subtree --- from definition, node x is common.
 - Case II:** x is not part of the common path covering of the subtree rooted at x .
 - Each child of x is a rooted subtree with some common path covering.
 - By inductive hypothesis, each child of x is common.

Handwritten Notes:

- λ is common. P_3 is corrupt could be $val(3)$ was different across diff EIG. Newval will be same.
- Corrupt P_3 .
- x is common.
- newval(x) will be the same across all EIG tree.
- x is common, as newval(x) is computed deterministically based on newval of its children.

So now, we want to prove the statement for any x different from the leaf node. So, assume that the inductive hypothesis is true; that means, the statement is true for all the nodes x , whose labels are of size $k + 1$. And now I want to prove the inductive step where I consider a node x occurring at layer x , whose label has length k ok.

So, take this as the candidate x for instance and imagine that there is a common path covering of the subtree rooted at x . Imagine that that is the case. Now, there could be two possibilities. The first possibility is that the node with label x itself is a part of the common path covering. See when I say that there is a common path covering for the subtree rooted at x , then x the node with label x may or may not be a part of that common path covering ok.

So, one case could be x is a part of that common path covering. So, if x is a part of that common path covering; that means, the newval of x is common. That means, it is same across all the honest parties. The tree that comes from the definition and that proves the lemma for this category of x .

But consider the case when I consider a different x ok, where even though it is guaranteed that there is a common path covering of the subtree rooted at x , see if I take this sub tree highlighted within this red box and its root is x corresponding to the index of a corrupt party.

So, definitely it is not a part of the common path covering, but this entire subtree has a common path covering. Because if I take the collection of nodes $3_1, 3_2, 3_4$ it constitutes a common path covering for the highlighted subtree ok. So, if the root x is not a part of the common path covering, then in order that the sub tree rooted at x has a common path covering, it should be the case that each child of x is a rooted sub tree with some common path covering.

So, what I am stating here is that, in general if you have an x here the root is x and say it has children's and it is guaranteed that there is a common path covering of the subtree rooted at x that is guaranteed. That means, there is a collection of nodes C so that when you go from x to any leaf node, you encounter at least one path in the subset C , but x is not a part of C .

If x is not a part of C and it is guaranteed that if you have a common path covering for the tree rooted at x , then that is possible only when each of the children of x has a rooted subtree with a common path covering. Because if that is not the case; that means, suppose the first child of x , and if I focus on the subtree rooted at that first child it does not

have a common path covering. There is no subset of nodes or there is at least one path from this root to say one of the leaves, which does not have any path which does not have any node from the subset C . Then that basically means that I have a path in the bigger tree rooted at x , where if I traverse along that path, I do not encounter any node from the set C ok.

So, in order that there is a path covering or there exist such a subset C so that each path from the root x to the leaf of the subtree rooted at x encounters at least one node from the set C , it should be the case that each of the children has rooted subtree with a common path covering. Now, the children of x , their labels are of size $k + 1$ ok.

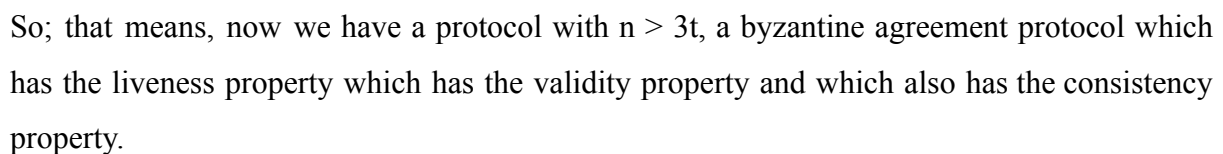
And as per our inductive hypothesis, we are assuming that the lemma statement, the implication that x is common is true for all the nodes, which occur at layer $k + 1$. That means each child of x is actually common. That means, it has the same newval across all the honest parties EIG tree.

That automatically implies that x also will end up to be common; that means, the newval of x will be the same across all EIG trees because if each child of x is actually common; that means, each child of x has the same newval across all the EIG trees. Then newval of x is computed deterministically based on the majority rule. And since it is computed deterministically based on the majority rule; that means, each honest party is going to assign the same newval to the x in its respective copy of the EIG tree.

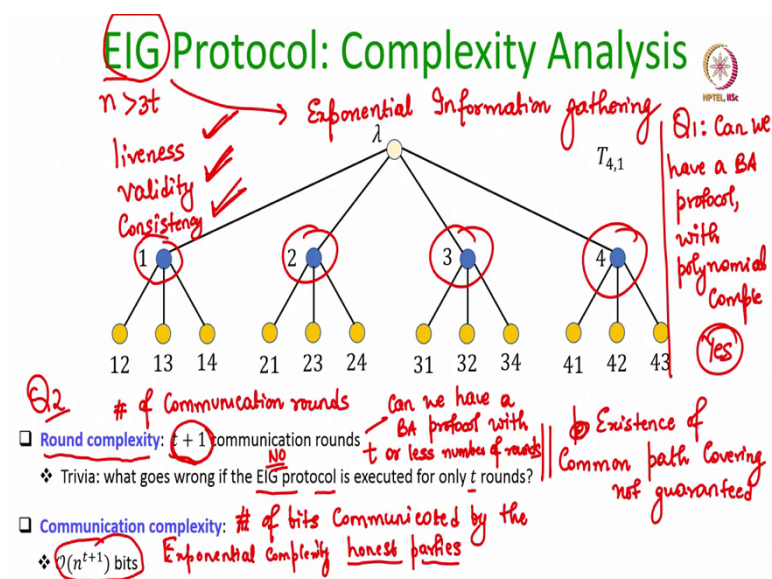
So, again if I focus on this example, where if party P_3 is corrupt then val_3 could be different ok, I have already written that. val_3 could be different across different EIG trees, but newval of 3 will turn out to be the same. And if newval of 3 turn out to be the same in all the copies of the EIG tree and anyhow all the remaining nodes whose label ends with the index of an honest party, they are anyhow common.

Since the newval of the root is computed deterministically based on the majority rule right. Every honest party will have the same newval computed for its root node and that is what ensures that every honest party ends up with a common output and that shows that the consistency property is satisfied in the EIG protocol ok.

(Refer Slide Time: 25:03)



Now, let us do the complexity analysis. How many communication rounds are required that is called as the round complexity, the number of communication rounds. So, there are $t + 1$ communication rounds in the protocol that is why the round complexity is $t + 1$. And you



might be wondering what goes wrong if in the EIG protocol the parties exchange messages only for t rounds.

Why they need to compute or why they need to construct the EIG tree, till $t + 1$ layers. What if they stop the tree at t layers and exchange messages for only t rounds by exchanging the values of the nodes at t layers; what goes wrong? So, basically the existence of common path covering is then not guaranteed, because now the paths from root to leaf will have only t nodes and they will have labels ending with t distinct parties. And in the worst case all of them could correspond to corrupt parties. So, the existence of common path covering is no longer guaranteed if we execute the protocol for less than $t + 1$ communication rounds ok. So, communication wise, what is the communication complexity? So, communication complexity means the number of bits communicated by the honest parties, we do not count how much communication is done by the corrupt parties, because corrupt parties can deviate from the protocol and it may keep on sending arbitrary messages, even if they are not supposed to.

So, for instance during round 1 every party is supposed to send only the value values of the nodes at layer 1 in its local copy of the EIG tree, but it may keep on sending extra messages on top of that, if the party is corrupt. We cannot prevent corrupt parties from doing that.

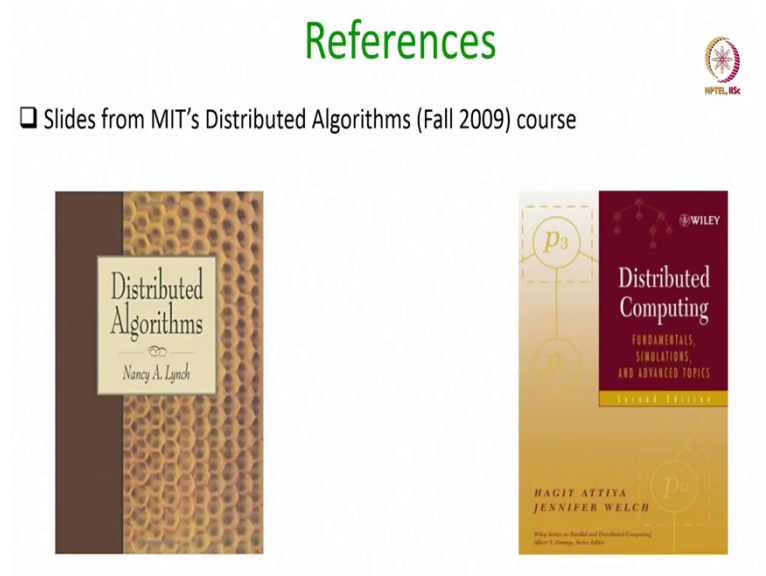
But we would not count such communication as part of the communication complexity. So, communication complexity is the measure of the number of bits communicated by the honest parties in the system during the protocol. And it turns out that a communication complexity is n^{t+1} , because there are $t + 1$ layers. And in each round every party basically communicates the value of all the nodes in its current layer to everyone else. And this is an exponential quantity and that is why the name EIG protocol, because it gathers information exponentially in exponential amount, it is exponential information gathering protocol, ok.

So, we now have the next set of interesting questions. Question number 1: can we have a BA protocol with polynomial complexity? And the answer is yes, of course EIG protocol is not the answer, we have some other protocols which we will discuss in subsequent lectures.

Question number 2: can we have a BA protocol with t or less number of rounds with liveness, validity and consistency property being achieved, without any error against computationally unbounded adversaries? And the answer is, no. Interestingly the answer is no.

We cannot reduce the number of rounds, we can prove generically that you take any perfectly secure byzantine agreement protocol, it necessarily have to allow t plus 1 rounds of communication. Otherwise at least 1 of these three properties will be achieved with some error ok.

(Refer Slide Time: 31:33)



So, we will see such kind of protocols later on. So, these are the references used for today's lecture and with that I concluded this lecture.

Thank you.