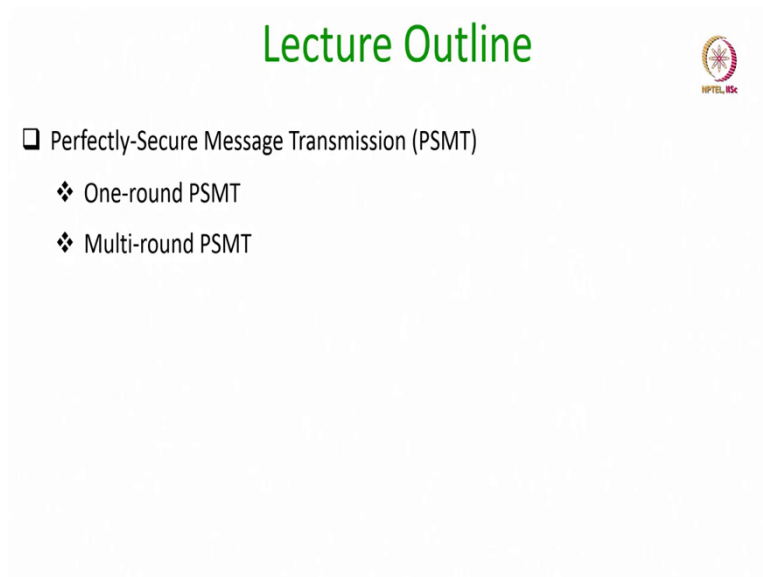


Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 20
Perfectly-Secure Message Transmission

(Refer Slide Time: 00:24)

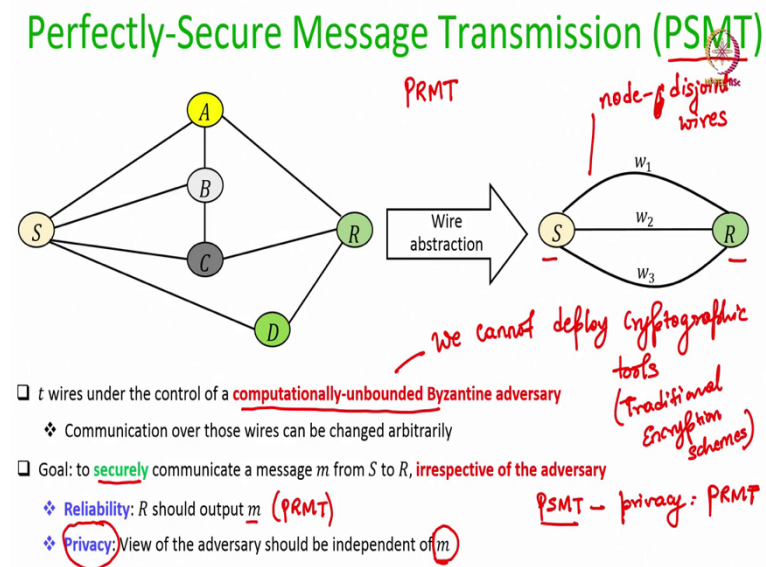


The slide is titled "Lecture Outline" in green text. In the top right corner, there is a small circular logo with a star and the text "IITM RSC" below it. The main content is a list of topics:

- ❑ Perfectly-Secure Message Transmission (PSMT)
 - ❖ One-round PSMT
 - ❖ Multi-round PSMT

Hello everyone welcome to this lecture. So, in this lecture we will introduce the problem of Perfectly-Secure Message Transmission or PSMT. And we will discuss two variants of this problem namely the one-round PSMT problem and multi-round PSMT problem.

(Refer Slide Time: 00:38)



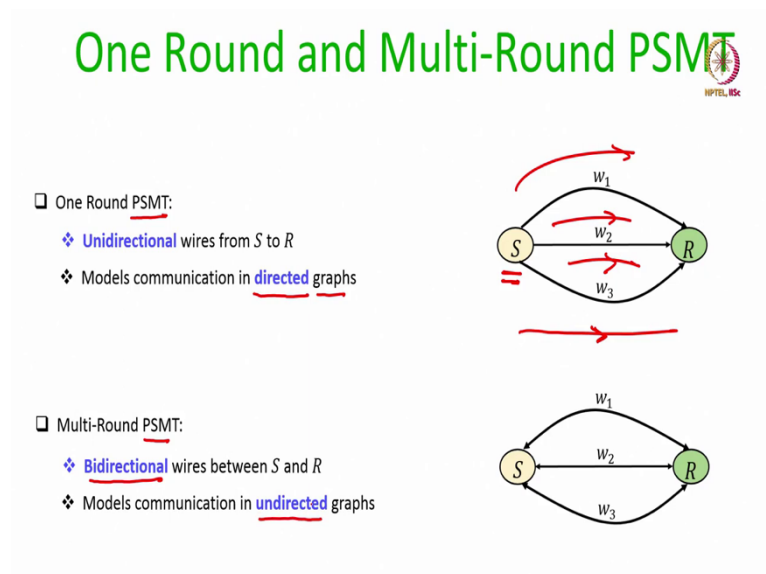
So, this PSMT problem, perfectly-secure message transmission problem is a variation of the PRMT problem which we had discussed in the earlier lecture. So, in that problem we had abstracted an underlying network as a collection of node-disjoint wires between two parties a sender and a receiver and up to t wires could be under the control of a computationally unbounded byzantine adversary where the communication over those wires can be arbitrarily changed.

And now in the new problem PSMT we have two goals to achieve. We want to securely communicate a message from the sender to the receiver irrespective of the way the corrupt channels or the channels which are under the control of the adversary behave. The two goals are the following: the receiver should be able to obtain the sender's message correctly without any error. So, that is the same as PRMT, but in the PRMT problem, in the PRMT protocol, it is fine if the adversary learns the message. And in fact, if you recall the protocol the naive PRMT protocol where the sender simply sends its message over all the n channels, the adversary also will be knowing the sender's message. There the goal was not privacy, there the goal was only reliability. But now in the PSMT problem, we also have another goal namely privacy. Namely in the protocol whatever information the adversary sees over the t channels, t wires, that should be independent of the senders message ok.

So, PSMT minus privacy is the same as PRMT; that means if you just want reliable communication, but you are fine to compromise privacy then you can use PRMT protocols,

but if you also want privacy on top of reliability then you have to go for PSMT protocol. And since we are assuming here a computationally unbounded adversary we cannot deploy cryptographic tools here ok. Because when I say cryptographic tools, I mean traditional encryption schemes. And the security of all these encryption schemes, the traditional encryption schemes, holds under the assumption that the adversary is computationally bounded ok.

(Refer Slide Time: 03:50)



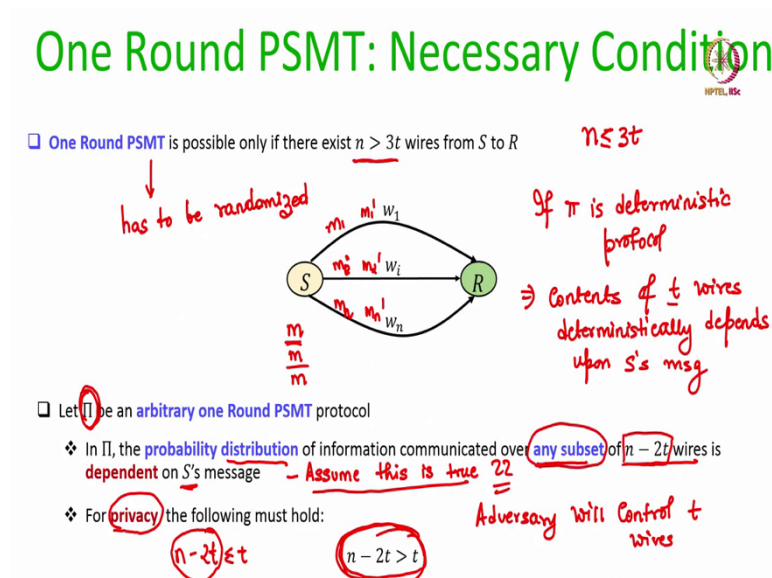
Now there are two variants of the PSMT problem. One-round PSMT problem: when I say I have a one-round PSMT protocol, by that I mean that my protocol will now operate in a scenario where the wires are unidirectional from sender to receiver. That means, only the sender can communicate to the receiver over those channels and backward communication is not possible, this models communications in directed graphs ok.

Say for instance sender is a base station and it has only the capability to broadcast or send some communication to the receiving parties. But the other way around communication may not be possible. So, such scenarios are modelled by this unidirectional wire model and in such models, we can only design a one-round PSMT protocol. Why one round? Because the protocol will be a single-shot protocol where only there will be one round of communication from the sender to the receiver over the wires and the protocol terminates.

Whereas when we talk about multi-round PSMT protocol then we assume that the communication channels between the sender and the receiver are bidirectional. That means,

the sender can send some information to the receiver and then the receiver can send feedback and then again in the next round sender can communicate and then again in the next round receiver can send feedback and so on. That means interaction in both directions is possible. And this models communications in undirected graphs where there is no direction associated with the underlying links. That means interaction in both directions is possible. And this models communications in undirected graphs where there is no direction associated with the underlying links.

(Refer Slide Time: 05:43)



So, now let us first focus on one-round PSMT and we can prove a very simple necessary condition for the existence of one-round PSMT protocols. So, we can show that one round PSMT protocol is possible to design only if there exists at least $3t$ plus 1 unidirectional wires from the sender to receiver. If there are t $3t$ or less than $3t$ number of wires from sender to receiver then one round PSMT protocol can never be possible, ok and proof will be through a contradiction.

So, what basically we will show is the following. Imagine you have some abstract one round PSMT protocol, let us denote it by Π . We do not know what exactly are the operations done in the protocol Π , we only know that Π allows a sender to compute some messages which it can communicate over the n wires and even if up to t wires change the contents of the communications, ok, even if the contents over the t wires get changed, the receiver will somehow be able to recover back the message by applying the protocol Π by executing the

steps of the protocol Π assigned to the receiver, that is what we assume. Now what we are going to show is the following. We will argue that in protocol, the probability distribution of the messages over any subset of $n - 2t$ wires has to depend on the sender's message.

Now what does that mean? First of all any PSMT protocol has to be randomized. And what does that mean? That means, even if sender wants to send the same message m multiple times say Monday it wants to send a message m , Tuesday again it wants to send a message m , Wednesday again it wants to send a message m . Then the protocol π_i should be randomized in the sense that first time it wants to send a message m , the contents over the wires could be say m_1, m_2, m_i, m_n .

The second time it wants to send the message, the content could be m_1 prime, m_2 prime, m_n prime. That means, every time sender runs the protocol π_i , the values which sender sends over the wires, they will be different with high probability. It will not be the same set of values which it will be sending over different wires, every time it has to send the same message, its not going to be a deterministic protocol. Why that is the case?

Because if the protocol π_i is a deterministic protocol, then it implies that contents over t wires deterministically depends upon senders message, but that will simply violate the privacy property. Because now if adversary controls some set of t wires and if again and again it sees the same contents being communicated over those t wires then it can sense that sender is sending the same message, sender's input is the same message which it is trying to communicate to the receiver and that itself is a violation of the privacy.

When I say privacy, remember the definition of privacy is that even if adversary controls any subset of t wires, whatever information it learns, its distribution should be completely independent of the sender's message. That means, even the fact that sender's message is repeated should not be revealed to the adversary and that is possible only when your protocol π_i is a randomized protocol.

That means, if we view the set of information which will be communicated over different set of wires by considering all possible executions of the protocol π_i over all possible inputs. Then that constitutes a probability distribution because different values will be obtained with different probabilities. So, now what we are going to claim here is that in the protocol π_i the distribution of information which is communicated over any subset of n minus $2t$ wires, if we take the probability distribution of only that subset of wires, that has to depend on senders

message, it cannot be independent of sender's message. If we take the probability distribution of only that subset of wires that has to depend on sender's message, it cannot be independent of sender's message.

Now assume this statement is true for the moment, assume this is true, we will soon prove this assumption is true. Then in order that the privacy property is satisfied in the protocol π , the condition $n - 2t$ greater than t should hold. Because, adversary will control t wires and if $n - 2t$ is less than or equal to t and anyhow we are assuming that the probability distribution over the subset of $n - 2t$ wires is dependent on sender's message. Then basically by observing what is happening over those $n - 2t$ wires adversary will be able to completely figure out what is sender's message and that goes against the privacy requirement.

That means, assuming that the distribution over the subset of $n - 2t$ wires is dependent on sender's message, if at all the protocol π satisfies the privacy property, this condition has to be ensured. That means whatever adversary observes, that has to be strictly less than the contents which depends upon the sender's message that is basically the idea.

Now how do we prove that in the protocol π whatever information is communicated over any subset, I stress any subset of $n - 2t$ wires, is dependent of the sender's message? Well we will prove it through a contradiction.

(Refer Slide Time: 13:12)

One Round PSMT: Necessary Condition

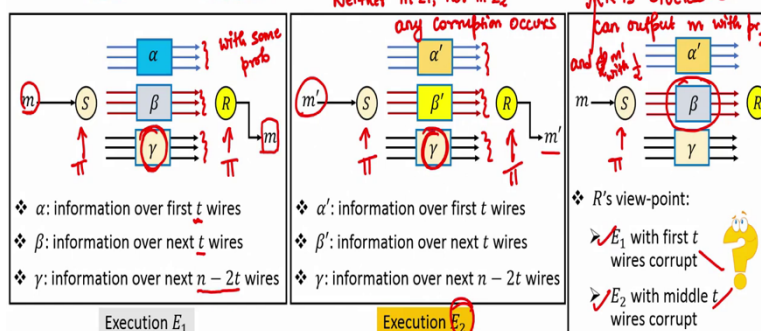
Let π be an arbitrary one Round PSMT protocol

$$n - 2t > t \Rightarrow n > 3t$$



In π , the probability distribution of information communicated over any subset of $n - 2t$ wires is dependent on S 's message

Proof by contradiction: let the probability distribution of information communicated over any subset of $n - 2t$ wires be independent of S 's message



So, imagine that this is not the case; that means in the protocol π_i the probability distribution of the information which is communicated over any subset of $n - 2t$ wires is independent of sender's message. That means, it does not matter whether sender's message is x or y the contents over some subset of $n - 2t$ wires will be the same with same probability ok .

So, consider this execution for the protocol π_i , execution E_1 , where the sender's input was some message m , it runs the protocol π_i . It computes the triplet of information α , β and γ ok . And the content α is communicated over the first t wires, the content β is communicated over the next t wires and the content γ is communicated over the $n - 2t$ wires ok .

So, total there are n wires ok and α denotes whatever total content is communicated over the first t wires ok . I am not showing the contents wire wise, but over the full subset of t wires, that is denoted by α . Whatever communication happens over the next t wires that is denoted by β and whatever communication happens over the last $n - 2t$ wires that is denoted by γ that is the case in the execution E_1 .

α will occur with some probability ok , β is occurring with some probability, γ is occurring with some probability and since it is a one round protocol there is no mechanism for the receiver to send back any feedback. Receiver whatever α , β , γ it receives it will be running the protocol π_i and since the protocol π_i is a PSMT protocol it should satisfy the reliability property; that means, it should be able to recover back the message m .

Now consider another execution E_2 for the same protocol π_i , where now the sender's message is m' . And now suppose when it runs the protocol π_i with its input m' the contents over the first t wires turn out to be α' with some probability. The contents over the next t wires turn out to be β' with some probability and the contents over the last $n - 2t$ wires turn out to be γ only. Now you might be wondering that since the sender's message is m' , how can γ occur both during the execution of π_i for m , as well as m' ? Well that is what we are assuming here when we are assuming a contradiction to our claim. We assumed that the probability distribution of information communicated over any subset of $n - 2t$ wires is independent of sender's message

That means, it does not matter whether the sender's message is m or whether the sender's message is m' , with whatever probability a candidate γ occurs over this $n - 2t$ wires

$2t$ wires during the execution $E1$, with the same probability γ will occur as a candidate for the information communicated over the last n minus $2t$ wires in the execution $E2$ right.

Now, even in this execution $E2$ if receiver receives α prime β prime and γ and if it runs the protocol π it should be able to recover back m prime ok. I stress neither in $E1$ nor in $E2$ any corruption occurs; that means, α β and γ go as it is, the byzantine corrupt wires do not do any harm over the channels, receiver receives α β and γ applies π and recovers m .

And in execution $E2$ again the adversary cause causes no harm, it simply listens over the the channels which it is controlling. The receiver receives α prime β prime and γ , applies the protocol π and recovers π .

Now consider another execution $E3$ of π where sender has again an input m , it runs the protocol π and again it turns out that the contents for the first t wires turn out to be α . The contents for the next t wires turn out to be β and the contents for the last n minus $2t$ wires turn out to be γ , ok, it can occur with some non-zero probability. But now the byzantine adversary controls the first t wires and it changes the contents from α to α prime and delivers it to the receiver.

Now what will be the receivers viewpoint? Receivers viewpoint is that it is receiving the triplet of information α prime β and γ . And it is now totally confused whether it is seeing an execution $E1$ where the first t wires would have sent α ; that means, they are supposed to deliver α , but the adversary has changed them to α prime. Or whether it is execution $E2$ where the sender has sent β prime over the next t wires and an adversary sitting over those t wires has changed it to β . From the viewpoint of the receiver is completely clueless whether it is scenario 1 or whether this is scenario 2 because it does not know what was sender's input, and it does not know which wires are under the control of the adversary.

So, with equal probability receiver should have output m as well as m prime right. So, the receiver is clueless it can output m with probability half and m prime with probability half. But that goes against the reliability condition, the reliability condition demands that irrespective of what the adversary does over the t channels, receiver should be able to recover back the sender's message.

But if this scenario happens then the receiver cannot do anything. It can only say, I think I am in execution E1 and it's only the first t wires who have done the corruption and changed it to alpha prime. But it could also be the case that actually sender's input was m prime and the sender has actually done the execution E2 and beta prime has been changed to beta, that could also be the case.

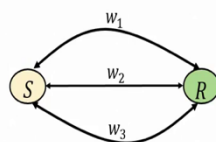
So, if the receiver's action is always to output m , then consider another execution where the sender's input was m prime and the middle t wires change their contents from beta prime to beta, in that case receiver will be still outputting m instead of m prime and that goes against the reliability condition.

And that shows that whatever contradictory statement we assumed here is incorrect and that shows that the probability distribution over any subset of n minus $2t$ wires in any one-round PSMT protocol has to depend on the sender's message. And as a result of that, the condition n minus $2t$ strictly greater than t should hold implying that n greater than $3t$ ok.

(Refer Slide Time: 22:08)

Multi-Round PSMT: Necessary Condition

Multi-Round PSMT is possible only if there exist $n > 2t$ wires between S and R



Let Π be an arbitrary Multi-Round PSMT protocol

In Π , the probability distribution of information communicated over any subset of $n - t$ wires is dependent on S 's message

Else, adversary can block communication over t wires and R will fail to recover the message

For privacy the following must hold:

$$n - t > t$$

$$n - t = t$$

Now, let me quickly go through the necessary condition for multi-round PSMT protocol. And we can easily prove that in any multi-round PSMT protocol, the condition n greater than $2t$ should hold. This we can argue by showing that if we take any arbitrary multi-round PSMT protocol, then the probability distribution over the information communicated over any set of n minus t wires has to depend on sender's message.

If this is not correct; that means, the information communicated over any subset of n minus t wires does not determine the sender's message, and does not depend on the sender's message. Then the adversary can simply do the following. It can simply block the communication over the t wires throughout the protocol. And now the receiver will be receiving only a truncated communication over n minus t wires and if the truncated communication is independent of the sender's message, how in the first place receiver will be able to recover the message?

It will simply fail to recover the message if that truncated communication over the n minus t clean wires fails to determine sender's message unambiguously; that means this statement is true. But if this statement is true then for privacy, we require the condition n minus t should be to be strictly greater than t .

Because if this is not correct, if n minus t is equal to t ; that means, the information over n minus t wires is sufficient to determine sender's message. And if t is equal to n minus t then the adversary can also eavesdrop that much amount of information and it can completely find out what was sender's message which goes against the privacy requirement ok.

(Refer Slide Time: 24:17)

References

- ❑ D. Dolev, C. Dwork, O. Waarts and M. Yung: Perfectly Secure Message Transmission. JACM 40(1): 17-47, 1993
- ❑ Ashish Choudhury: Protocols for Reliable and Secure Message Transmission. IACR Cryptology ePrint Archive: 281 (2010)

Interaction not allowed $n > 3t$

Interaction allowed $n > 2t$

} tradeoff b/w # of corrupt wires and # of rounds

So, we have seen today the necessary condition for one round PSMT protocol, it is n greater than $3t$. We have also seen the necessary condition for multi-round PSMT protocol it is n greater than $2t$. And you can see there is a tradeoff between the number of faults, number of corrupt wires and number of rounds.

Namely if you allow interaction between sender and receiver, namely if the channels are bidirectional, ok, interaction is allowed, then you can design a protocol even if up to 49 percent of the channels are corrupt. But if the interaction is not allowed, namely only the sender can communicate to the receiver, then you can design a protocol if only up to 33 percent of the channels are corrupt.

So, depending upon whether interaction is allowed or not, the percentage of corrupt channels which you can tolerate in the protocol varies.

So, these are the references where you can find more about perfectly secure message transmission problem, the underlying necessary condition. The problem was introduced in the seminal work by D. Dolev, Dwork, O. Waarts and Yung in 1993. And my entire PhD thesis was explicitly on this problem of PRMT and PSMT. So, you can get more details and this thesis is publicly available.

Thank you.