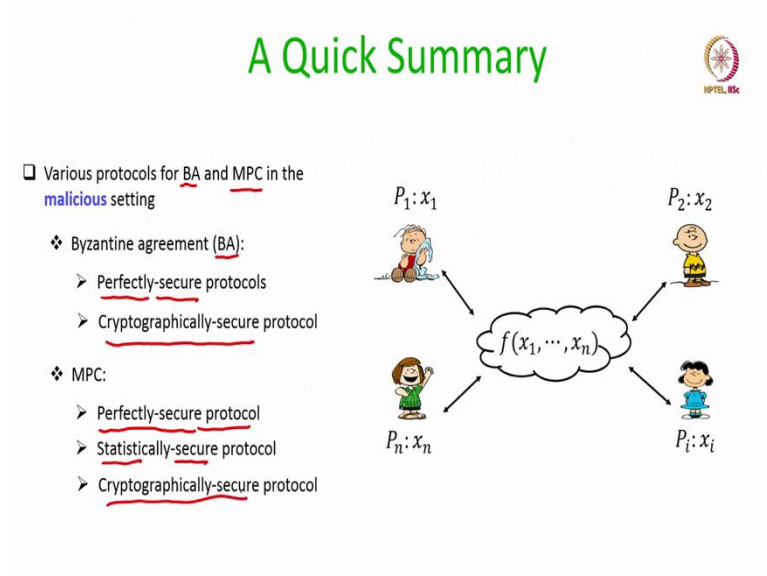


Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 62
Goodbye and Farewell

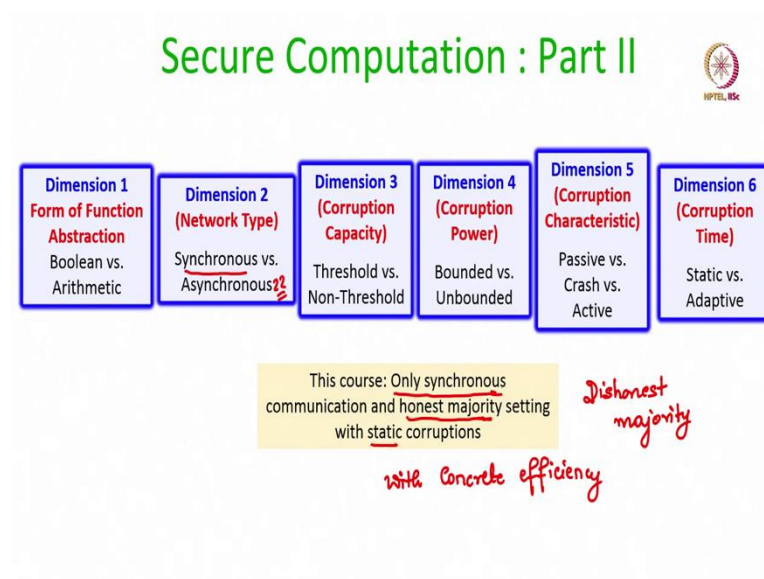
(Refer Slide Time: 00:25)



Hello everyone. So, this is the concluding lecture. So, we are done with the course. Here is a quick summary of what we discussed in this course. We had seen various protocols, various classical protocols for Byzantine agreement and some of the seminal MPC protocols in the malicious setting.

For the case of Byzantine agreement, we had seen perfectly secure protocols which are secure against computationally unbounded adversaries, as well as cryptographically secure protocol secure against polynomial time adversaries. For MPC we rigorously discussed the perfectly secure protocols and we briefly discussed statistically secure and cryptographically secure protocols.

(Refer Slide Time: 01:19)



So, just to recall, there are various dimensions in which we can study the MPC problem starting with how do we abstract the function, what is the type of underlying communication network, how do we model the adversary etcetera. And in this course our focus was only on synchronous setting and honest majority with static corruptions.

So, there are plenty of other settings which are not yet discussed in this course like what about asynchronous network and what if we have dishonest majority and what about protocols with concrete efficiency for a small number of parties and so on.

So, of course, it is not possible to discuss each and everything in a single course due to time constraints, but I hope that through this course the participants are exposed to some of the basics and foundation stuff regarding maliciously secure MPC.

(Refer Slide Time: 02:46)

Acknowledgements



(Prof. Kamala Krithivasan)



(Prof. C. Pandu Rangan)



(Prof. S. A. Choudum)

To my beloved gurus of IIT Madras, who built my foundations of Theoretical Computer Science





As usual I would like to tribute this course, I would like to dedicate this course to my beloved gurus, who have built my foundations in theoretical computer science starting with Professor Kamala Krithivasan, my MS advisor and my beloved sir Professor Pandu Rangan my PhD advisor and Professor Choudum who offered the wonderful course on graph theory at IIT Madras.

(Refer Slide Time: 03:18)

Concluding Remarks


Picture copyright@Arpita Patra



And it was wonderful teaching this course. As I said I hope that the participants would be able to understand some of the basic stuff in this course.

(Refer Slide Time: 03:34)

Some Advertisement



- ❑ Looking for **full-time**, motivated MS (and PhD) research scholars, who want to work in cryptography
- ❖ Motivated candidates should apply in response to the advertisements (twice a year), published at IIITB's website

<https://www.iiitb.ac.in>

- ❖ Please do not write to me for research-assistant, internship, project positions, etc.

Some advertisement. I am always looking for full time research scholars who would like to work in the area of cryptography. They can apply in response to the advertisements which are published at IIIT Bangalore's website. Please do not write to me for research assistant or internship or project positions, I do not offer any such positions. With that I end this course.

Thank you.