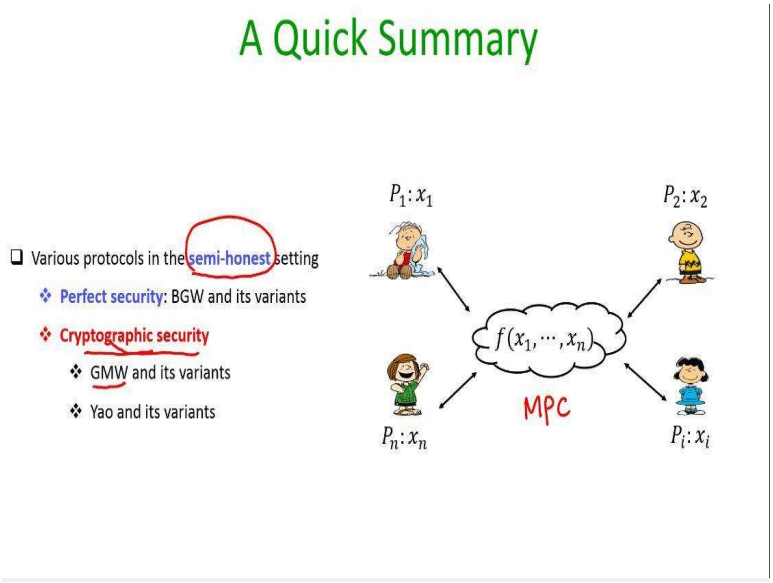
Secure Computation: Part I
Prof. Ashish Choudhury
International Institute of Information Technology, Bengaluru

Lecture - 59
Goodbye and Farewell

(Refer Slide Time: 00:31)

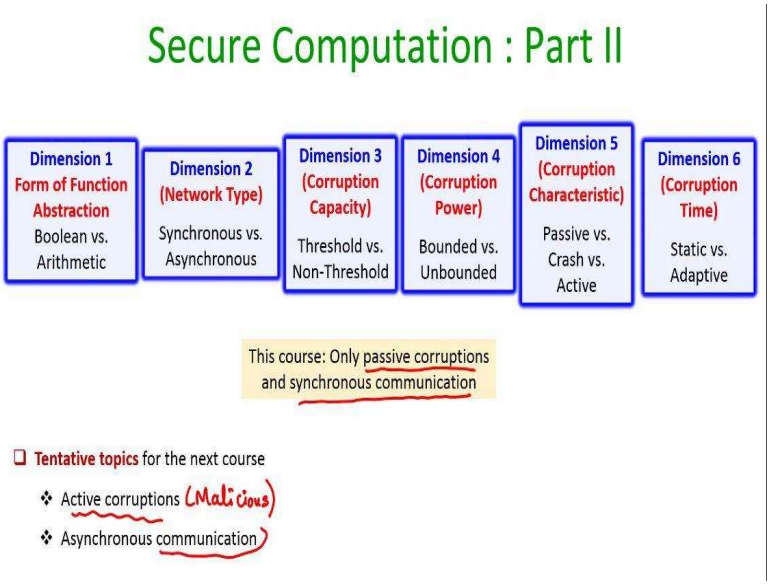


Hello everyone. So, we are done with the course. Let me quickly summarize what we have covered in this course, we have studied the problem of secure multi party computation, where we have a set of mutually distrusting parties with private inputs. And they would like to collaborate to perform some joint computation on their data by keeping their data as private as possible. We had seen several real world motivation examples to study this problem.

And in this course, we have considered only a semi honest adversary and synchronous communication setting. We saw different types of protocols which provides your different security guarantees and which provides different trade off. We started with perfect security and discuss the secret sharing based BGW protocol and its variants. And we also discussed cryptographically secure protocols.

Under that category we have protocols with non-constant number of rounds namely the GMW protocol and its variants and we have the constant round protocol due to Yao. So, we discussed both these protocols and they are variants various optimizations.

(Refer Slide Time: 01:52)



So, recall there are various dimensions in which we can study the MPC problem depending upon the form of function abstraction, network type, corruption capacity, adversarial capacity and so on. And in this course, we have considered a very simplistic setting namely of namely that of passive corruption, where the corrupt parties are the parties under the control of the adversary honesty follows the protocol instruction.

And synchronous communication, setting where they are a strict time upper bound on the message delays. So, in part 2 of the course, which hopefully I will offer some time, very soon, the tentative topics will be to cover more powerful adversarial model namely active corruptions or malicious corruptions, where the bad parties or the corrupt parties may not follow the protocol instructions, they can deviate in any arbitrary fashion.

And also consider a synchronous communication setting where there will be no upper bound on the message delays. These are the tentative topics for the next course.

(Refer Slide Time: 03:14)

I would like to dedicate this course to my beloved guru's teachers of IIT Madras who built my foundations for theoretical computer science. Namely Professor Kamala Krithivasan, my PhD supervisor, Professor Pandu Rangan, and Professor Choudum.

(Refer Slide Time: 03:35)

And that is all from my site. I hope you really enjoyed the course aim and objective of the course to introduce the participants to the basics and formal details of this wonderful and very, very important area of research called secure multi party computation. And I hope that together, we are able to achieve those goals.

(Refer Slide Time: 04:02)

Some advertisement from my site, I am looking always for full time, MS and PhD research scholars who want to work in cryptography if you want to apply then go to the website of IIITB. We have admissions twice a year. So, if you are interested, go through the advertisement and apply. And please do not write to me for research assistant or internship or project positions. With that, I end this lecture and of course thank you.