# SECURE COMPUTATION: PART II

**PROF. ASHISH CHOUDHURY**
Department of Computer Science
IIIT Bangalore

**PRE-REQUISITES :** It is expected that the participant has done a basic course on Cryptography (such as the Foundations of Cryptography course available on NPTEL), a basic course on Discrete Mathematics (several courses on Discrete Mathematics are available on NPTEL) and the course titled Secure Computation: Part I (available on NPTEL).

## COURSE OUTLINE :

Secure multi-party computation (MPC) is one of the most fundamental problems in cryptography as well as distributed computing. In a nutshell, a MPC protocol allows a set of mutually distrusting parties with private inputs, to perform any joint computation on their data, by keeping their respective data as private as possible. Secure MPC abstracts several real-world problems, for example privacy-preserving data mining, privacy-preserving ML, secure e-auctions, private matchmaking, secure set-intersection, secure e-voting, secure signal-processing, secure bioinformatics, secure biometrics, secure outsourcing, to name a few. Since the domain of secure computation is enormously vast, it is impossible to discuss every relevant topic in just a single course. Hence the plan is to cover the topics in two parts. The first part titled Secure Computation: Part I has been already offered. In that course, we covered a simpler form of adversarial setting, namely semi-honest adversary (passive adversary), where the corrupt parties are supposed to follow protocol instructions. However, real-life attackers may not be so benign and can cause the compromised parties to behave in any arbitrary fashion. Such corruptions are better modelled by active/malicious (Byzantine) adversaries, which will be the focus of this course.

## ABOUT INSTRUCTOR :

Prof. Ashish Choudhury is currently an Associate Professor at IIIT Bangalore. He did his MS and PhD in Computer science from IIT Madras, followed by postdoc at ISI Kolkata and University of Bristol. His research work is focused on the foundation of cryptographic protocols for real-world problems. His current projects aim to design efficient protocols in the asynchronous network model which can be realized in practice. In general, he is interested in secure distributed computing and all areas of theoretical computer science.

## COURSE PLAN :

**Week 1:** Broadcast and Byzantine Agreement: definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds
**Week 2:** Broadcast and Byzantine Agreement: definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds (contd.)
**Week 3:** Broadcast and Byzantine Agreement: definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds (contd.)
**Week 4:** Broadcast and Byzantine Agreement: definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds (contd.)
**Week 5:** Reed-Solomon codes, perfectly secure message transmission protocols
**Week 6:** Verifiable Secret-Sharing (VSS): definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds
**Week 7:** Verifiable Secret-Sharing (VSS): definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds (contd.)
**Week 8:** Verifiable Secret-Sharing (VSS): definition, various protocols (deterministic, randomized, perfectly secure, cryptographically secure, statistically secure), various lower bounds (contd.)
**Week 9:** Classic protocols for actively-secure MPC: BenOr-Goldwasser-Wigderson (BGW), Rabin-BenOr (RB), detailed analysis
**Week 10:** Classic protocols for actively-secure MPC: BenOr-Goldwasser-Wigderson (BGW), Rabin-BenOr (RB), detailed analysis (contd.)
**Week 11:** State-of-the-art actively-secure protocols, player-elimination, actively-secure MPC for small number of parties and applications
**Week 12:** State-of-the-art actively-secure protocols, player-elimination, actively-secure MPC for small number of parties and applications (contd.)