NPTEL Video Course - Computer Science and Engineering - NOC:Secure Computation - Part II

Subject Co-ordinator - Prof. Ashish Choudhury

Co-ordinating Institute - IISc - Bangalore

Sub-Titles - Available / Unavailable | MP3 Audio Lectures - Available / Unavailable

Lecture 1 - What is Secure Multi-Party Computation (MPC)?
Lecture 2 - Reliable Broadcast and Byzantine Agreement
Lecture 3 - EIG Protocol for Perfectly-Secure Byzantine Agreement
Lecture 4 - EIG Protocol for Perfectly-Secure Byzantine Agreement: Illustration
Lecture 5 - EIG Protocol for Perfectly-Secure Byzantine Agreement: Analysis - Part I
Lecture 6 - EIG Protocol for Perfectly-Secure Byzantine Agreement: Analysis - Part II
Lecture 7 - Efficient Protocols for Perfectly-Secure Byzantine Agreement - Part I
Lecture 8 - Efficient Protocols for Perfectly-Secure Byzantine Agreement - Part II
Lecture 9 - Domain Extension for Perfectly-Secure Byzantine Agreement
Lecture 10 - Cryptographically/Statistically-Secure Reliable Broadcast
Lecture 11 - Dolev-Strong Reliable Broadcast Protocol: Analysis
Lecture 12 - Randomized Protocol for Byzantine Agreement - Part I
Lecture 13 - Randomized Protocol for Byzantine Agreement - Part II
Lecture 14 - Randomized Protocol for Byzantine Agreement - Part III
Lecture 15 - Lower Bound for Number of Parties for Byzantine Agreement - Part I
Lecture 16 - Lower Bound for Number of Parties for Byzantine Agreement - Part II
Lecture 17 - Lower Bound for Number of Parties for Byzantine Agreement - Part III
Lecture 18 - Recap of Basic Concepts from Abstract Algebra
Lecture 19 - Reed-Solomon Error-Correcting Codes
Lecture 20 - Perfectly-Secure Message Transmission
Lecture 21 - Properties of Polynomials Over a Field - I
Lecture 22 - Properties of Polynomials Over a Field - II
Lecture 23 - One Round PSMT Protocol
Lecture 24 - Multi-Round PSMT Protocol - I
Lecture 25 - Multi-Round PSMT Protocol - II
Lecture 26 - Domain Extension for Perfectly-Secure Broadcast Based on RS Error-Correcting Codes - I
Lecture 27 - Domain Extension for Perfectly-Secure Broadcast Based on RS Error-Correcting Codes - II
Lecture 28 - Domain Extension for Perfectly-Secure Broadcast Based on RS Error-Correcting Codes - III
Lecture 29 - (n,t) - Star Structure

Lecture 30 - Domain Extension for Perfectly-Secure Broadcast Based on RS Error-Correcting Codes - IV
Lecture 31 - The BGW MPC Protocol for Passive Corruptions: Recap
Lecture 32 - The BGW MPC Protocol for Byzantine Corruptions: Challenges
Lecture 33 - Perfectly-Secure VSS: Necessary Condition
Lecture 34 - Bivariate Polynomials Over Finite Fields - I
Lecture 35 - Bivariate Polynomials Over Finite Fields - II
Lecture 36 - Bivariate Polynomials Over Finite Fields - III
Lecture 37 - Bivariate Polynomials Over Finite Fields - IV
Lecture 38 - Perfectly-Secure VSS with n greater than 3t - Part I
Lecture 39 - Perfectly-Secure VSS with n greater than 3t - Part II
Lecture 40 - Perfectly-Secure VSS with n greater than 3t - Part III
Lecture 41 - Perfectly-Secure VSS with n greater than 3t - A Round-Reducing Technique
Lecture 42 - Perfectly-Secure VSS with n greater than 4t - Part I
Lecture 43 - Perfectly-Secure VSS with n greater than 4t - Part II
Lecture 44 - The BGW MPC Protocol for Linear Functions
Lecture 45 - The BGW MPC Protocol for Linear Functions: Security Analysis
Lecture 46 - The BGW MPC Protocol: The Case of Non-Linear Gates
Lecture 47 - The Degree-Reduction Problem
Lecture 48 - Generating Random Multiplication-Triples - I
Lecture 49 - Generating Random Multiplication-Triples - II
Lecture 50 - Generating Random Multiplication-Triples - III
Lecture 51 - Perfectly-Secure Protocol for Verifying Multiplicative Relationship
Lecture 52 - Perfectly-Secure Verifiable Triple-Sharing Protocol
Lecture 53 - Perfectly-Secure Triple-Extraction Protocol
Lecture 54 - Towards Secure MPC with an Honest Majority
Lecture 55 - ICP from Information-Theoretic MAC - I
Lecture 56 - ICP from Information-Theoretic MAC - II
Lecture 57 - Ingredients for Statistically-Secure MPC
Lecture 58 - Statistically-Secure VSS
Lecture 59 - Cyclic Groups and Discrete Logarithm
Lecture 60 - Pedersen Commitment Scheme
Lecture 61 - Cryptographically-secure VSS and MPC
Lecture 62 - Goodbye and Farewell