

NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

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

Subject Co-ordinator - Prof. Ashish Choudhury

Co-ordinating Institute - IIITB

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

- Lecture 1 - What is Secure MPC
- Lecture 2 - Real-World Examples of Secure MPC
- Lecture 3 - Various Dimensions to Study Secure MPC
- Lecture 4 - Recap of Basic Concepts from Abstract Algebra
- Lecture 5 - Recap of Basic Concepts from Abstract Algebra (Continued...)
- Lecture 6 - Recap of Basic Concepts from Cryptography
- Lecture 7 - Secret sharing
- Lecture 8 - Additive Secret Sharing
- Lecture 9 - Inefficient Threshold Secret Sharing
- Lecture 10 - Polynomials Over Fields
- Lecture 11 - Shamir Secret-Sharing
- Lecture 12 - Linear secret-sharing
- Lecture 13 - Linear Secret Sharing (Continued...)
- Lecture 14 - General Secret Sharing
- Lecture 15 - Perfectly-Secure Message Transmission
- Lecture 16 - A Toy MPC Protocol
- Lecture 17 - A Toy MPC Protocol (Continued...)
- Lecture 18 - A Toy MPC Protocol (Continued...)
- Lecture 19 - The BGW MPC Protocol
- Lecture 20 - The BGW MPC Protocol for Linear Functions
- Lecture 21 - The BGW MPC Protocol for Linear Functions: Security Analysis
- Lecture 22 - The BGW MPC Protocol: The Case of Non-Linear Gates
- Lecture 23 - The Degree-Reduction Problem
- Lecture 24 - The Gennaro-Rabin-Rabin (GRR) Degree-Reduction Method
- Lecture 25 - Analysis of the GRR, Degree-Reduction Method
- Lecture 26 - Shared Circuit-Evaluation via GRR Degree-Reduction Method
- Lecture 27 - Shared Circuit-Evaluation in the Pre-processing Model
- Lecture 28 - Optimality of Corruption Bound for Perfectly-Secure MPC
- Lecture 29 - Perfectly-Secure MPC Tolerating General (Non-Threshold) Adversaries

Get DIGIMAT For High-Speed Video Streaming of NPTEL and Educational Video Courses in LAN

<http://www.digimat.in>

NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

- Lecture 30 - Perfectly-Secure MPC Tolerating General (Non-Threshold) Adversaries with $Q^{(2)}$ Condition
- Lecture 31 - Perfectly-Secure MPC for Small Number of Parties
- Lecture 32 - Perfectly-Secure 3PC (Continued...)
- Lecture 33 - More Efficient Perfectly-Secure 3PC
- Lecture 34 - More Efficient Perfectly-Secure 3PC (Continued...)
- Lecture 35 - Towards Cryptographically-Secure MPC
- Lecture 36 - GMW MPC protocol
- Lecture 37 - Oblivious Transfer (OT)
- Lecture 38 - RSA Assumption and RSA Hard-Core Predicate
- Lecture 39 - Bit OT Based on RSA Assumption and Hard-Core Predicate
- Lecture 40 - Discrete Logarithm and DDH Assumption
- Lecture 41 - OT Based on the DDH Assumption
- Lecture 42 - Pre-Processing Phase for the GMW Protocol
- Lecture 43 - Pre-Processing Phase for the GMW Protocol: The n-Party Case
- Lecture 44 - Pre-Processing Phase for the GMW Protocol (Continued...)
- Lecture 45 - Pre-Processing of OT
- Lecture 46 - OT Extension
- Lecture 47 - Analysis of IKNP OT Extension
- Lecture 48 - Yao's Protocol for Secure 2PC
- Lecture 49 - Yao's Garbling Scheme
- Lecture 50 - Yao's Protocol for Secure 2PC
- Lecture 51 - Optimizations for Yao's Garbling
- Lecture 52 - Interpreting Yao's Secure 2PC Protocol as a Secret-Sharing Based Protocol
- Lecture 53 - Mixed Protocols for Secure 2PC
- Lecture 54 - The Arithmetic, Boolean and Yao Sharing for Secure 2PC
- Lecture 55 - The ABY Conversions
- Lecture 56 - The ABY Conversions (Continued...)
- Lecture 57 - The ABY Conversions (Continued...)
- Lecture 58 - ABY Computations : Example
- Lecture 59 - Goodbye and Farewell