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 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 - Yaoâ s Protocol for Secure 2PC
Lecture 49 - Yaoâ s Garbling Scheme
Lecture 50 - Yaoâ s Protocol for Secure 2PC
Lecture 51 - Optimizations for Yaoâ s Garbling
Lecture 52 - Interpreting Yaoâ 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