SECURE COMPUTATION: PART I

PROF. ASHISH CHOUDHURY
Department of Computer Science
IIIT Bangalore

PRE-REQUISITES : The participant should have done a basic course on Cryptography (such as the Foundations of Cryptography course available on NPTEL) and a basic course on Discrete Mathematics

INTENDED AUDIENCE : The course is intended for any student from the computer science and Mathematics discipline

COURSE OUTLINE :
This course will discuss about how using various cryptographic primitives, one can do computation on distributed and sensitive data, also known as secure multi-party computation (MPC), which arguably is one of the most fundamental problems in cryptography as well as distributed computing.The need for distributed computation on private data arises in several real-world applications that require computations involving sensitive data from two or more mutually distrusting entities. Consider the following example, which is one of the latest applications of secure computation: The Earth is orbited by thousands of man-made satellites and several thousands of orbital debris. The growing number of satellites and space debris orbiting the planet increases the danger of collisions. And this is not a hypothetical scenario, as several such “high-profile” collisions have been reported in the recent past. Given the expensive cost of satellites, the host countries would like to avoid collision. A collision can only be predicted if the detailed orbit information of the individual satellites is known. However, such information can be highly sensitive and in fact, it can even be a national secret. So, what is needed here is a way to determine whether two satellites are about to clash with each other based on the detailed locations of the satellites, but without the need of disclosing the locations of the satellites to other host countries.Secure MPC models the above and several such applications that make simultaneous demands for the privacy and usability of sensitive data. Other examples include secure e-voting, secure e-auction, secure signal-processing, secure bioinformatics, secure biometrics, secure machine-learning, secure outsourcing, privacy-preserving data mining, to name a few.

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**:** Secure Computation: motivation and real-world examples, various dimensions, recalling relevant topics from abstract algebra (groups, rings, fields) and cryptography

Week 2**:** Secret sharing (motivation, definition and applications), Shamir secret-sharing, additive secret-sharing, replicated secret-sharing

Week 3**:** Linear secret-sharing, monotone span programs (MSP), secure message transmission (SMT)

Week 4**:** BenOr-Goldwasser-Wigderson (BGW) protocol: security proof and detailed analysis

Week 5**:** Degree-Reduction problem and various solutions, efficient protocols for evaluating multiplication gates

Week 6**:** Oblivious transfer (OT), OT protocols, OT extension

Week 7**:** Goldreich-Micali-Wigderson (GMW) protocol: security proof and detailed analysis

Week 8**:** Construction of OT protocols from various cryptographic assumptions, GMW protocol in the pre-processing model

Week 9**:** OT extension, Yao’s protocol for secure 2-party computation

Week 10**:** Various optimizations of Yao’s 2PC protocol

Week 11**:** Mixed-world MPC protocols: The case of 2 PC

Week 12**:** Mixed-world 2PC protocols in the ABY framework