Proposal for a Course

Indian Institute of Technology Kanpur

Course Title: Secure Computation

Course No: CS670A

Credits: 3-0-0-0- [9]

Prerequisite: CS201, CS202, and CS203 or equivalent. CS 641 or equivalent would be useful, but not necessary. CS670 would be useful, but not necessary. The instructor will try making the course as self-contained as possible. Main prerequisite is mathematical maturity.

Who can take the course: Ph.D., Masters, 3rd and 4th year UG Students

Proposer: Adithya Vadapalli,

Departments that may be interested: CSE, Mathematics and Statistics

Course Rationale: The early pioneers of the Internet envisioned it would be *the great equalizer* and lead to the complete democratization of the online world—nearly four decades since the reality has diverged considerably from their grand vision. Rather than the bastion of freedom and free speech, which the early visionaries envisioned, the Internet has become a dangerous place. Data theft leading to identity theft has become commonplace. Despite these challenges, it is undeniable that the Internet has revolutionized our lives by making day-to-day tasks easier and connecting people worldwide — however, the risks associated with the Internet loom large. Secure Computation is a promising technique that allows users to keep their data private without sacrificing the Internet's benefits.

Interestingly, the origins of Secure Computation were during the exact times when the Internet was in its nascent stages. The early researchers of Secure Computation studied it mainly as a theoretical endeavor. However, nearly four decades after its inception, Secure Computation is more than just a problem of theoretical importance; it can solve practical privacy problems many of which arise due to the expansion of the Internet.

Course Objectives: On completion of this course, a student should be able to: (i) articulate the definition of Secure Multiparty Computation (ii) articulate different MPC constructions, prove their security and correctness; (iii) articulate the definitions of Oblivious Random Access; (iv) articulate the construction of different types of Oblivious RAM protocols; (v) build cryptographically secure systems using Secure Computation.

Course Content:

Module	**Topic**	**No. of 1 hour Lectures**
Introduction	Cryptography Refresher Big Picture of Secure Computation	**3**
Basics of MPC	Writing Proofs of Security Simulation Proofs Read and Ideal World Paradigm Security in the semi-honest and malicious model	**6**
Basic MPC Techniques	Garbled Circuits GMW, BGW, BMR Protocol Server Aided MPC Oblivious Transfer Oblivious Shuffling Oblivious Sorting	**9**
Advanced MPC Techniques	ABY family of protocols Mixed Protocols DPF-based MPC	**9**
Oblivious Random Access Memory (ORAM)	Hierarchical ORAMs Tree-based ORAMs ORAMs for Multiparty Computation Revisiting Square Root ORAM Distributed ORAMs	**9**
Applications	Private Recommendation Systems Computing Private Statistics	**4**
Total Lecture hours		**40 hours**

Text:

There is no one textbook for such a course. Research Papers will be the main sources of study material.

Some useful textbooks are:

- Modern Cryptography by Katz and Lindell
- Pragmatic MPC by Evans, Koselnikov, and Rosulek
- Efficient Secure Two-Party Protocols: Techniques and Constructions (Information Security and Cryptography) by Carmit Hazay and Yehuda Lindell
- Secure Multi-Party Compuation Against Passive Adversaries by Ashish Choudhury and Arpita Patra

There will be other resources put on the web by the instructor.

- Lecture notes, assignments, supplemental readings, and other resources will be provided via the course website
- The course will consist of 3 hours of lectures per week, projects and homework, and possibly a course project.

Proposer: Adithya Vadapalli

Dated: March 18, 2024

DPGC Convener:

Chairman SPGC:

DOAA: