Fall 2024: Special Topics in Cryptography

Instructor: Aarushi Goel
When: M 11:30 – 2:20 PM
Where: LWSN B134

Course Description

Zero-knowledge proofs are cryptographic protocols that enable a prover to convince a verifier of the truth of an NP statement without disclosing the secret witness. These protocols play a crucial role in the design of larger cryptographic systems. Since the foundational work of Goldreich, Micali, and Wigderson, which established their feasibility for all NP languages, significant efforts have been devoted towards improving their practical efficiency. The goal of this course is to study state-of-the-art techniques for designing efficient zero-knowledge proofs, understand their practical implications and trade-offs. We will also explore their applications in different domains.

Prerequisites

Students should have a basic understanding of the theory of cryptography. Students must have taken a course on "Discrete Mathematics" and at least one course on cryptography. Please feel free to consult with the instructor for eligibility confirmation.

Learning Objectives

By the end of this course, students should:

1. Understand advanced techniques for designing efficient zero-knowledge proofs.
2. Analyze trade-offs between different techniques.
3. Evaluate applications of these techniques in blockchains, machine learning, and other domains .

Course Format

This seminar-style course will include lectures, paper discussions, short quizzes, and a course project. Lectures will introduce key concepts, while paper discussions will delve into state-of-the-art techniques. Each paper will be presented by designated student(s). Additionally, students will be expected to collaborate on a group project, which may involve a literature survey or original research addressing open problems in the field.

Assessment

Quiz: 10% of the grade
Participation: 10% of the grade
Presentation: 40% of the grade
Project: 40% of the grade

Reading Material

Course readings include research papers. We will also use Oded Goldreich's "Foundations of Cryptography" as reference.