CS 282B/MATH 209B: Cryptographic Protocols Prof. Rafail Ostrovsky

CRYPTOGRAPHIC PROTOCOLS

First lecture: Monday, January 3^{rd}, 2pm – 3:50PM

When/Where: first 2 weeks are on ZOOM:

`https://ucla.zoom.us/j/91098169206`.

Subsequently in 2760 Boelter Hall.

Office: 475 Engineering VI
Office hours: are on ZOOM: `https://ucla.zoom.us/j/99075052301`
each Wednesday 4:15pm-5pm or by appointment.

Description: This is a second graduate course on the mathematical theory of cryptography — concentrating on advanced cryptographic protocol design and analysis. Topics will include: secure two-party and multi-party computation; non-malleable noninteractive zero-knowledge proofs; zero-knowledge arguments; concurrent and non-black-box zero-knowledge; IP=PSPACE, stronger notions of security for public-key encryption; dealing with dynamic adversary; non-malleability and composability of secure protocols; Private Information Retrieval; software protection; hardware-based security notions; threshold cryptography; identity-based cryptography; Oblivious RAMs and Garbled RAMs.
Objectives: This course is meant to engage students in current topics of research in theoretical cryptography.
Prerequisites: 282A/209A or permission of instructor.
Textbooks: None. The course material will consists mostly of papers, and in part my 2010 lecture notes.
Grading Policy: take-home project 50% and its in-class presentation 50%.