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

CRYPTO PROTOCOLS

First lecture: Monday, January 9th, 12noon-1:50PM

When/where: M,W 12am-1:50pm at 4413 Boelter Hall
Office: 3732D Boelter Hall;
Office hours: Monday 2-3pm 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; software protection; software obfuscation; 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 (mathematical maturity and 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%.