

CRYPTOGRAPHIC PROTOCOLS

First lecture: Monday, January 6th, 12noon-1:50PM

When/Where: M,W 12am-1:50pm, Royce Hall 154;

Office: 475 Engineering VI

Office hours: Monday 2:10-3pm 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; 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%.