CS 282A/MATH 209A: Foundations of Cryptography Prof. Rafail Ostrovsky

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 30th, 2024 **CRYPTO**

When: M,W 4pm-5:50 pm
Where: Royce Hall 156
Email: rafail@cs.ucla.edu
Office: 475 Engineering VI;
Office hours: Monday 6:15-7 pm or by appointment (starting on 10/21/2024)

Description: This is a graduate course that introduces students to the theory of cryptography, stressing rigorous definitions and proofs of security. Topics include notions of hardness, one-way functions, hard-core bits, pseudo-random generators, pseudo-random functions and permutations, public-key and private-key encryption, verifiable random functions, secret-sharing and function secret-sharing, message authentication, digital signatures, interactive proofs, zero-knowledge proofs and its variants, collision-resistant hash functions, commitment protocols, key-agreement, Oblivious Transfer, Private Information Retrieval, Oblivious RAMs and multiparty secure computation (Yao, GMW, BGW, Garbled RAM).

Objectives: This course is meant to introduce students to up-to-date research in cryptography, including modern cryptographic definitions and proofs of security.

Prerequisites: Mathematical maturity and knowledge of undergraduate algorithms.

Textbooks: None. The course material will consists of on-line materials for recent topics, and my 2010 lecture notes, see:
https://web.cs.ucla.edu/∼rafail/PUBLIC/OstrovskyDraftLecNotes2010.pdf

Scribe: Each student registered for class must scribe notes for at least one lecture. Please use my 2010 lecture notes (see above) as a starting point for your scribe. (OK to copy from my notes verbatim, but expand portions that you think are unclearor have typos). The scribe(s) for a given lecture will jointly prepare a LaTeX document understandable for students who did not attend the class. Please prepare scribe notes on Overleaf and share your Overleaf document with rafail.ostrovsky@gmail.com. Scribes are due four days after the lecture at 8 pm (either Friday or Sunday). LaTeX These links are also available on my UCLA web page and can also be found here:
https://web.cs.ucla.edu/∼rafail/preamble.tex https://web.cs.ucla.edu/∼rafail/Template.tex

Grading Policy: Grading: Midterm 40%; Final 50%; Scribe 10%. All exams will be closed book/notes/electronics.