CSCI 2590 — Advanced Cryptography

Anna Lysyanskaya
Spring Semester, 2019

Course Description

This is a seminar course on advanced topics in cryptography. The focus of this semester is zero-knowledge proofs and arguments. Starting from definitions of zero-knowledge, the discussion will proceed to different zero-knowledge protocols. Their applications in various settings such as identification protocols, secure computation and cryptocurrencies will be covered. Finally, more recent works on zero-knowledge succinct non-interactive arguments [zk-SNARGs and SNARKs] will be discussed.

The main component of the class is reading, presenting papers and class discussion. All assigned papers are required readings. Students will present at least twice in the semester. When not presenting, students are expected to read the papers, prepare and ask questions and participate in class discussion

Instructor	Email	Office
Prof. Anna Lysyanskaya	anna@cs.brown.edu	CIT 501

Course TA	Email	Office
Apoorvaa Deshpande	acdeshpa@cs.brown.edu	CIT 421

Course Credit	
Presenting Papers	40%
Class Participation	20%
Problem Sets	40%

Prerequisite CSCI 1510 or permission of the instructor.

Problem Sets There will be 2-3 problem sets during the semester. Collaboration on problem sets is allowed as long as all collaborators are acknowledged.

There will also be a paper due at the end of the semester in which students will list what they think are important open problems in the field, and also give preliminary approaches to solving them.

Information Sources The CSCI 2590 webpage (http://www.cs.brown.edu/courses/csci2590/) will be a primary source of information for this course. Check the website regularly for syllabus and assigned papers. Website will contain electronic versions of problem sets.

Sign up for presenting papers will be through shared spreadsheet (https://bit.ly/2W3j6HM). For the first presentation, sign up before February 4.