CS 4501: Cryptography

Instructor: Mohammad Mahmoody

Credit Units: 3

Time and Location: Mondays and Wednesdays 2pm-3:15pm, Over Zoom

Instructor: Mohammad Mahmoody (Rice 511 – but only meets virtually!) mohammad@cs.virginia.edu

Office Hours: (The URL is the same as class's URL.)
Mohammad: Fridays 10:30-11:30am.
TA (Abtin) Tuesday 1-2pm and Thurs: 3:30-4:30.

Objectives: The goal of this course is to develop skills that allow formally arguing about security. This involves knowing how to define security in various settings and how to use the right theoretical tools (also known as cryptographic "primitives") to design the right solutions (also called "protocols") for various tasks. As a result, "proofs" of security would be a big part of this course. The course will have two parts. In the first part we go over the basic goals of privacy and security as well as main theoretical tools in cryptography for reaching these goals. The second part of the course will be focused on reading classical as well as recent research papers in selected topics, examples include: consensus/block-chain protocols, oblivious RAM/computation, structured encryption, etc. At the end, we explore connections between cryptographic notions of security and privacy with machine learning. Below is a tentative list of topics that we would like to cover in this class.

Topics:

- Part I:
  - Information theoretic vs. computational security.
  - Pseudorandomness generators and functions, and hash functions.
  - Private-key encryption using pseudorandomness.
  - Private-key authentication (aka message authentication codes).
  - Public key encryption (and tools from number theory).

  - Public key authentication (aka digital signatures).

- Part II:
  - Zero-knowledge proofs and interactive protocols.
  - Secure multi party computation.
  - Differential privacy and machine learning.
  - Proofs of work and block-chain protocols.
  - Structured encryption

Textbooks: There will be no single text-book for the class. The content of the first half of the course will largely be based on the following book.

> Introduction to Modern Cryptography: Principles and Protocols, *by Jonathan Katz and Yehuda Lindell.*

However, there are quite a few other great books that we will also benefit from. (I will post for each session which related chapters of the books could be used.) Examples include:

- Foundations of Cryptography, by Oded Goldreich.
- A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup.
- Secure Multi-party computation and secret sharing by Cramer, Damgard, and Nielsen.
- The Joy of Cryptography by Mike Rosulek.

Other Resources. We will also have a Piazza page for off-class discussions. There you can ask any questions you have about the material and other students as well as myself will provide their thoughts on that.

Prerequisites: C or higher in CS2102 (Discrete Math) + CS3102 (Theory of computation). However, I am willing to make exceptions if someone believes they are comfortable with mathematical proofs. In that case, please email me, and I will approve the enrollment.

Grading: There will be a take-home final exam, and about five assignments throughout the course, one of which will be a take-home midterm. The grades will be almost evenly distributed among all these tasks, with some more weights given to the mid-term and the final exams.

You can miss 20% of the classes (it means 5 out of 26 classes) but not more. Interaction during the class is highly recommended.

Honor Policy: All assignments are subject to the UVa's honor policy. Collaboration is allowed, or even encouraged, for assignments, but not for the mid-term and final take home exams. However, you have to write the assignments (and the take home exam) completely on your own, and state the collaborators on the submissions.