CS 4501-6501: Special Topics in Cryptography

Instructor: Mohammad Mahmoody

Credit Units: 3

Time and Location: Fridays 2pm-4:30pm, Thornton Hall D115

Instructor: Mohammad Mahmoody (Rice 511) mohammad@cs.virginia.edu

Office Hours: Wed 12:30-1:30pm 511 Rice Hall.

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: block-chain protocols, oblivious computation, structured (searchable encryption) encryption, etc. 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.
  - Public key encryption (and number theory).
  - Public key authentication.
- Part II:
  - Zero-knowledge proofs and interactive protocols.
  - Secure multi party computation.

  - Database (differential) privacy.
  - Proofs of work
  - Block-chain consensus protocols.
  - Searchable 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 in which you can find the videos of the class (shortly after the class) as well as my handwritten notes during the class, and the scribed notes. Piazza will also serve as a place for discussions after the class. 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: Pre-req for undergrads: C or higher in CS2102 (Discrete Math) + CS3102 (Theory of computation). Algorithms (CS4102) also helps, but not mandatory if you are willing to learn the concepts needed for this class. If you have taken CS4102 but not CS3102, it is also accepted.

Grading: There will be a take-home final exam, and some assignments throughout the course, and a project (groups of 2 or 3). Each group will also scribe two sessions of the class. The grades will be almost evenly distributed among all these tasks. The project will be presented by the whole group at some point during the second half of the class, i.e., after the Spring break where the class will be more of the form of a seminar. The project will be around reading and presenting an interesting topic related to the content of the course. You are encouraged to talk to me about your proposals as soon as possible.

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