COMS E6261: Advanced Cryptography

Class time: Thursdays 4:10PM-6:00PM
Class location: MUDD 627
Instructor: Allison Lewko
Office hours: Tuesdays 12:00PM - 2:00PM in CSB 519
Instructor email: alewko@cs.columbia.edu

Additional Course Information This class features different topics every time it is taught, and can be repeated for credit. The main pre-requisite is a general level of mathematical sophistication, particularly in linear algebra and probability theory. Prior exposure to cryptography (e.g. by taking 4261 introduction to cryptography) is helpful.

1 Outline of Topics to be Covered

Note: Subject to change

1. Background on cryptographic primitives, security definitions, mathematical tools
2. Expanding public key functionality
   Identity-based encryption
   Attribute-based encryption
3. Simulation-based security definitions, secure multi-party computation, zero knowledge
4. Functional encryption
5. Applications and Barriers (some sample topics below, time permitting)
   Obfuscation - possibilities and impossibilities
   Connections between cryptography and differential privacy, distributed computing
   Black-box separations

2 Grading

There will be 3 homework assignments throughout the semester. Students are allowed to work together on the homework assignments but must write up their solutions individually. The course grade will be based on:

- 25% first homework assignment
- 25% second homework assignment

- 25% third homework assignment
- 25% final project

The details of the final project will be discussed in class a few weeks into the semester.

3 Reference Materials

Books: Note: these can be helpful but are not required.

1. *Introduction to Modern Cryptography* by Katz and Lindell
2. *Foundations of Cryptography* by Goldreich, Volumes I and II.

How to Access Relevant Papers Much of the material in lectures can be supplemented by research papers which are typically available on the crypto eprint archive, http://eprint.iacr.org/. Relevant references/citations will be mentioned in class.