Instructor: Adam O'Neill
adamo@cs.umass.edu

CS-690J: Advanced Cryptography

Course Description: This is a graduate-level course in advanced cryptographic primitives and protocols, with an eye toward their far-reaching applications in secure messaging, surveillance prevention, cloud computing, and privacy-preserving machine learning, among others. Topics may include: functional encryption, homomorphic encryption, multiparty computation, identification protocols, zero-knowledge proofs, authenticated key exchange, key ratcheting. Specific topics and schedule to be determined by student preferences. This course is a natural "second course" in cryptography, but we will review core concepts in the beginning to make it accessible to motivated students who have not studied cryptography before.

The schedule and topics are subject to change according to the instructor or students' preferences.

NB: Cryptography is only one part of a much broader field of information security. In particular, we will not consider implementation issues in depth, nor will we cover topics such as viruses, worms, buffer overflow and denial of service attacks, access control, intrusion detection, etc. Students interested in these topics are advised to take computer and network security courses.

Time and Place. TuTh 4:00–5:15, CSB 140. See the class website for office hours and other logistical information.

Requirements: (1) 3-4 homeworks (70%) and (2) A course project (30%). The homeworks will not require any programming. The project can be either theory or implementation-based. Example projects will be discussed in class. New this semester, *the project must be research based*. You must agree with me on a research problem to work on. If you do not make any progress on it, describe what you tried and why it didn't work. The project should follow a conference-paper-like format.

Grading: Approximate grading is as follows: 80-100: A, 65%-80%: B, 40%-65%: C, <40%: F.

Textbook: The course textbook is *A Graduate Course in Applied Cryptography* by Dan Boneh and Victor Shoup at `http://toc.cryptobook.us/`. We will also use additional resources as posted on the class website.

Prerequisites: Graduate standing or consent of instructor. Knowledge of basic cryptography (as taught in CS-690C in Fall 2019) is helpful but not required. Most importantly, students should have *mathematical maturity*, being comfortable reading and writing mathematical proofs.

Academic Honesty: Since the integrity of the academic enterprise of any institution of higher education requires honesty in scholarship and research, academic honesty is required of all students at the University of Massachusetts Amherst. Academic dishonesty is prohibited in all programs of

the University. Academic dishonesty includes but is not limited to: cheating, fabrication, plagiarism, and facilitating dishonesty. Appropriate sanctions may be imposed on any student who has committed an act of academic dishonesty. Instructors should take reasonable steps to address academic misconduct. Any person who has reason to believe that a student has committed academic dishonesty should bring such information to the attention of the appropriate course instructor as soon as possible. Instances of academic dishonesty not related to a specific course should be brought to the attention of the appropriate department Head or Chair. Since students are expected to be familiar with this policy and the commonly accepted standards of academic integrity, ignorance of such standards is not normally sufficient evidence of lack of intent. See more information at `http://www.umass.edu/dean_students/codeofconduct/acadhonesty`.

For problem sets, you are encouraged to work with others, but when you actually write your solutions you must do so by yourself as if you are taking an exam. You must also explicitly list all collaborators with whom you worked and any references or online material you used.

Accommodation Statement: The University of Massachusetts Amherst is committed to providing an equal educational opportunity for all students. If you have a documented physical, psychological, or learning disability on file with Disability Services (DS), you may be eligible for reasonable academic accommodations to help you succeed in this course. If you have a documented disability that requires an accommodation, please notify me within the first two weeks of the semester so that we may make appropriate arrangements.