CAS CS 548: Advanced Cryptography

Spring 2006

Official Description

Continuation of CS 538. Advanced techniques to preserve confidentiality and authenticity against active attacks. Zero-knowledge proofs; Fiat-Shamir signature schemes; non-malleable public-key encryption; authenticated symmetric encryption; secure multiparty protocols for tasks ranging from Byzantine agreement to mental poker to threshold cryptography.

Prerequisites

CAS CS 538 or permission of instructor. I expect you to be comfortable with CS 538 material (see websites of past CS 538 incarnations from Gene Itkis in Fall 2005 or myself in Fall 2004). If you haven't taken CS 538, please talk to me in the first week of class.

Instructor

Leonid Reyzin, `reyzin@cs.bu.edu`, (617-35)3-3283, MCS (111 Cummington St) room 287
Office hours: Tuesday 3:30-5:00 and Wednesday 1:30–3:00

I encourage you to come to my office hours. If you need to talk to me but can't make the office hours, please send me email. I check it a few times on a weekday and at least once on a weekend.

Lectures and Notes

The lecture is in MCS (111 Cummington St) room B29, Tuesdays and Thursdays 12:30 pm–2:00 pm

I expect you to come to lecture and I encourage you to participate. This class is small enough that we can keep it interactive. There is no textbook for the class. Lectures and original research papers will be your primary sources of information.

Other Communication

The class has a home page: `http://www.cs.bu.edu/~reyzin/teaching/s06cs548/index.html`. On occasion, I will send out email to the class list. Please sign up for the list by typing csmail -a cs548 on csa or csb as soon as possible.

Homework and Academic Conduct

There will be roughly 4 problem sets, assigned in class. **I encourage you to discuss course material, including problem sets, with other students in the class, subject to the following rules:**

1. You must write up your solutions completely on your own, without looking at other people's write-ups.
2. In your solution to each problem, you must write the names of those with whom you discussed it.
3. You may not consult solution manuals or other people's solutions from similar courses.

I expect you to follow these rules as well as the academic conduct code of CAS/GRS. If you have any questions or are not sure what is appropriate, consult me *before* taking steps that you are afraid may violate the rules. If you violate the academic conduct code, you will be reported to the Academic Conduct Committee and fail the course.

Late assignments will not ordinarily be accepted. If an assignment is due at the beginning of class, I expect you to hand it in at the *beginning* of class. If, for some compelling reason, you cannot hand in an assignment on time, please contact me as far in advance as possible.

Grading

There will be no exams in this class. Homework will count for 50% of your final grade, the final project for 40%, and class participation for 10%. I reserve the right to deviate from this formula in unusual cases.

If you are unsure of your performance in the class, please come and talk to me. Remember that the last day to drop a class without a 'W' is Friday, February 17. The last day to drop a class with a 'W' is Friday, March 17. After that, you must receive a real grade for the course. It is your responsibility to talk to me before these dates if you may need to drop the course to avoid receiving a low grade. I am powerless to change these university-wide rules about drop dates.

Topics and Schedule

Given that this is a small class, I will try to choose topics in cooperation with the students; we will concentrate on recent research results, although not exclusively. The following list should be viewed as a first draft, with items to be added and removed:

- Security notions for encryption
- Combining encryption and signatures; signcryption, universal padding schemes.
- Achieving chosen-ciphertext security in the public-key setting
- Combining symmetric and asymmetric techniques
- Bilinear pairings in cryptography
- Identity-based encryption and chosen-ciphertext security
- Forward-secure cryptography
- Beyond forward security: way of dealing with key leakage
- Error-correction techniques in cryptography
- Verifiable secrete sharing and multi-party computation