This sheet summarizes information for the course CSC 2419 S ("Topics in Cryptography: Secure Computation") during the Spring session of 2013 on the St. George campus at the University of Toronto. By the end of the first week of classes, you should have read and become familiar with the contents of this information sheet.

Course Website

`http://www.cs.utoronto.ca/~vinodv/COURSES/CSC2419-S13/`

The course website will be available at the start of the first week of classes and it will always contain the most up-to-date information possible regarding the course. *You are responsible for all announcements posted on the course web site*, so please check the `Schedule` and `Announcements` sections of the page frequently (at least once a week).

Instructor and Lectures Info

Instructor	**Office**	**Email**	**Office Hours**
Vinod Vaikuntanathan	*SF2301B*	`vinodv@cs.toronto.edu`	T 5-6pm in my office.

Please include [**CSC2414**] in *all* email communication about course-related matters.

Lecture: *Time:* T 3-5 *Place:* Bahen Center BA 4010

Textbook

There is no *required* textbook for this course. Instead, we will use material from the references given in the course web-page.

Outline

This is an advanced graduate course. We will focus on understanding the fundamental cryptographic problem of secure multi-party computation: how can n mutually distrusting users each with their private inputs collaborate to compute a joint function of their inputs? In the course of understanding this question, we will see the exciting cryptographic concepts of zero knowledge, oblivious transfer, secret sharing, homomorphic encryption, and (time permitting) various advanced notions such as functional encryption and differential privacy. The set of topics covered in the course is expected to include foundational material as well as questions at the forefront of current research. Students will be expected to read papers and eventually present a paper of their choice in class.

Prerequisites: CSC 2426 (Foundations of Cryptography) or an equivalent course is highly recommended although it can be compensated with mathematical maturity, knowledge of complexity theory and a willingness to learn.

Grading Scheme

The workload for this course will be "moderate". Grades will be based on one assignment, scribing notes for 1-2 lectures, and presentation / writeup based on a recent research paper from the crypto literature. We will use the following grading scheme.

Item	Weight
Assignments	20%
Lecture Scribing	20%
Paper presentation	60%

Class attendance is mandatory, and you are encouraged to ask many questions in class!

Assignment Submission

Assignments:

- All assignments are due *no later than 11:59pm* on their due date.

Scribe notes:

- All scribe notes are due the Thursday after the week of the lecture at 11:59pm (approximately 10 days).

All assignments and scribe notes should be e-mailed to the instructor. Include "[CSC2414]" in the subject of the e-mail. The submissions should be in pdf. You can find the appropriate Latex style files in the course website.

The primary considerations in grading the scribe notes will be accuracy and clarity. The notes should contain a clear exposition of the material taught in the class. A rule of thumb is: *the lecture notes should be better than the lectures, not worse!* If you have questions about the material, feel free to schedule an appointment with the instructor.

Lateness Policy

You have a quota of *120 "late hours"* for the course (including the problem sets and scribe notes) which you can use at your discretion.

Collaboration Policy

You are free to discuss the problem sets with others. However, the actual writeup of your assignments must be done in isolation from others (and without copying from notes or other sources!). In addition, you must acknowledge your sources and the discussions in your submission.

Please read the `Guidelines for Avoiding Plagiarism` page for full details of the course policies and the Faculty's rules. If you are having trouble with the course, come speak to me!

Courtesy: François Pitt and Mark Braverman.