CSE 5854: Modern Cryptography: Protocols

Spring 2018

January 16, 2018

1 Administrative

Description This course is the second of a two course sequence on the foundations of cryptography. It builds heavily on the material in CSE 5852 which introduced private and public key encryption, signatures, and authentication codes. This course will focus on more advanced cryptographic primitives with two fundamental changes:

1. We will consider tasks beyond just secret and authentication communication. This includes allowing multiple distrusting parties to jointly compute a secret value (known as multi-party computation).
2. We will consider adversaries that actively participate in the protocol and may have some of the secret information of the protocol.

We will continue to use security reductions to hardness problems. In addition, this class will include discussion of interactive proofs and more problems in complexity theory. We will stress the importance of definitions in this class.

Contact Benjamin Fuller, benjamin.fuller@uconn.edu, 6-2122, ITE (Information Technologies Engineering) room 243.

Office hours (changes will be posted on HuskyCT): 2-3pm Tuesdays and 10-11am Thursdays. I encourage attending office hours. If you cannot make office hours, please ask technical questions on HuskyCT and email me for personal questions.

Meeting and Notes Class meetings are in ITE 125.

The class will follow a cadence designed to encourage discussion and limit lecture. The cadence will be as follows:

1. Students will be given a short technical reading assignment before each class. Most of the time this reading will be lecture notes prepared by the instructor. Occasionally, important technical papers will be assigned as reading over a sequence of classes.
2. Short three question quizzes will be administered at the start of class. (15 min.)
3. The class will critical discuss important points from the reading. (20 min.)
4. The instructor will present dive into a critical part of the reading (30 min.)
5. The instructor will introduce the next class's reading (10 min.)

Textbook The instructor will provide notes as required reading before each class. A detailed exposition for much of the material can be found in Foundations of Cryptography by Oded Goldreich. This text is dense and serves better as a reference. It is incredibly detailed and discusses important technical details that often omitted in other texts (and our reading assignments). Please don't try and read it as a novel!

Communication The assigned readings, problem sets, and solutions will be posted on the course web site at `https://benjamin-fuller.uconn.edu/teaching/modern-cryptography-primitives-and-protocols/`. Announcements, discussion, homework submission will be done on HuskyCT. Please ensure you receive emails from HuskyCT so you get announcements. In addition, I encourage students to post and answer questions about class material and problem sets. I will also answer questions but I encourage students to try and jointly answer questions. **Do not directly ask or answer homework problems.**

Personal questions should be directly to my email or handled in person during office hours. I will not answer emails from Friday 6pm to Monday 9am.

Grading, assignments and exams There will be four problem sets throughout the semester. The class will be graded as follows:

- 30% homework assignments.
- 30% final exam.
- 20% in class quizzes.
- 20% team project.

Assignment These assignments are due via HuskyCT and should be submitted in LaTeX. LaTeX has a significant learning curve, contact the instructor if you have not used it before.

All students have four late days to be used however they wish throughout the semester. Each assignment should be marked with the number of late days used. Students who exceed this number of late days will receive 20% off the assignment for each additional day the assignment is late. Assignments will be graded no more than one week after they are due. Solutions will be based on student responses and will include the student's name if they desire.

Final Exam There will be a final exam to be scheduled by the registrar. The final exam is the only individual evaluation. In order to pass the class you must score about 50% on the final exam.

Quizzes A three question quiz will be given to students once a week. Each response will be graded as sufficient or incomplete. The quiz grade will be the median of the student's grade on each quiz.

Team Project There will be a team project where teams of up to four will try to understand and contribute to an area of cryptography. These teams can be formed by students, the topic must be approved by the instructor no later than March 15. The output of this project will be two artifacts, a 20 minute presentation to be done the last week of class and a written report that will be weighted equally. The written report will be due on the last day of class on April 26. The expected rigor on this portion of the class will depend on whether the student is an undergraduate or graduate student.

Grades will be assigned according to the scale in Table 1.

Number Grade	Assigned Grade	Grade Points
90+	A	4.0
86-89	A-	3.7
82-85	B+	3.3
79-81	B	3.0
76-78	B-	2.7
73-75	C+	2.3
69-72	C	2.0
66-68	C-	1.7
65-67	D+	1.3
62-64	D	1.0
59-61	D-	.7
0-58 (Or at most 50 on final exam)	F	0

Table 1: Grading Scale

As necessary the instructor reserves the right to decrease the minimum value for any assigned grade.

The last day to drop a class without a ‘W’ or convert to Pass/Fail is January 29. The last day to drop a class with a ‘W’ March 26. Please come talk to me before that date if you have concerns about your performance.

Collaboration Thoughtful discussion will help you answer the problem sets. At the same time, we need to measure individual performance and contribution. In an effort to balance these two needs, abide by the following conditions:

- You may collaborate with up to three other students. Each student you collaborate with should be named on the homework assignment.
- You must first consider each problem on your own and generate ideas on how to solve the problem.
- You may discuss problems and solution ideas jointly. The goal of collaboration is to understand the high level ideas of how to solve the problem. Do not go further than this.
- You must write solutions completely on your own. If an issue arises during writing the solutions you may speak to your collaborators. Do not bring your write-up; you need to be able to describe the problem without referring to the solutions.
- The quizzes final exam will be an individual effort. As noted above, students cannot pass the class without scoring at least 50% on the final exam.

- Do not use other resources (outside of your textbooks and collaborators) to attempt to find the problem or the solution. This includes using the Internet to search for parts of the problem.

2 Course contents

This course will focus on modern, reduction-based cryptography. We will focus on rigorous definitions and relations between cryptographic objects. Concrete mathematical examples of cryptography concepts will be presented but will not be the focus of the class. The class will cover:

1. Commitments
2. Interactive Proof Systems
3. Zero-knowledge proof systems
4. Witness Indistinguishable proof systems
5. Non-interactive proof systems
6. Two-party computation using Garbled circuits
7. Oblivious Transfer
8. Extending Garbled circuits to malicious security
9. Extending Garbled Circuits to many parties
10. Secret Sharing
11. Information-theoretic multi-party computation
12. Extending to malicious security
13. Fully homomorphic encryption

Special care will be taken to understand security goals and constructing formal definitions to codify this intuition. We will show constructions from other cryptographic objects and directly from mathematical objects. We will generate formal mathematical proofs that an object satisfies our definition.

Course Objections By the end of this course, you will be able to:

- Be skilled in writing reduction based proofs of security.
- Understand how to effectively carry out complex cryptographic tasks.
- Be able to craft formal definitions for any security goal.

Tentative Class Schedule Table 2 contains a tentative plan for the topics week by week. We'll adjust the schedule as needed.

Class	Topics
1	Course Overview, Defining interactive cryptographic goals.
2	Constructing commitments (hiding vs. binding)
3	Review of P, NP, what is an interactive proof?
4	Interactive proof for graph nonisomorphism, amplifying soundness/correctness
5	How much knowledge is conveyed by a proof? Defining zero-knowledge
6	A zero knowledge proof system for graph isomormophism. Zero knowledge for NP.
7	Sequential/parallel repetition
8	Witness indistinguishability and applications
9	Non-interactive proof systems
10	Constructing non-interactive proof systems
11	Defining Oblivious Transfer, constructions
12	Malicious security oblivious transfer
13	Defining two party secure computation
14	Yao's construction
15	Yao w/ malicious security
16	Defining multi party secure computation
17	A passively secure multi party protocol, defining secret sharing
18	A generic transform to malicious security
19	Polynomial secret sharing, information-theoretic multi party computation
20	Extending to malicious security, verifiable secret sharing
21	Homomorphic encryption, El Gamal, RSA
22	What is a lattice?
23	Encrypting using lattices, basic homomorphism
24	Bootstrapping and fully homomorphic encryption
25	Project Presentations
26	Project Presentations

Table 2: Tentative class schedule. The last two classes are left empty as a buffer and to tailor to student interest.

3 Policies

Academic Honesty This course expects all students to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. If you have questions about academic integrity or intellectual property, you should consult with your instructor. Additionally, consult UConn's guidelines for academic integrity.

The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, talk to me!

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include: not reporting collaborators, jointly writing solutions, copying or plagiarizing solutions from other sources, and cheating on the exam.

Student Conduct Code Students are expected to conduct themselves in accordance with UConn's Student Conduct Code.

Copyright My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expression. Students may take notes. In addition, we will ask you to release your created notes. In addition, students will be consulted before using their solutions either with or without their name.

Students with Disabilities The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. Students who require accommodations should contact the Center for Students with Disabilities, Wilbur Cross Building Room 204, (860) 486-2020, or `http://csd.uconn.edu/`.

Final Exam Policy In accordance with UConn policy, students are required to be available for their final exam and/or complete any assessment during the time stated. If you have a conflict with this time you must obtain official permission to schedule a make-up exam with the Office of Student Support and Advocacy (OSSA). If permission is granted, OSSA will notify the instructor. Please note that vacations, previously purchased tickets or reservations, graduations, social events, misreading the assessment schedule, and oversleeping are not viable reasons for rescheduling a final.