Privacy Enhancing Technologies

Bulletin Description

(Comp 790 Description) Permission of the instructor. This course has variable content and may be taken multiple times for credit.

General Course Info

Term: Spring 2022  
Department: COMP  
Course Number: 590/790  
Section Number: 171

Time: MW, 2:30 – 3:45pm  
Location: FB009  
Website: http://www.cs.unc.edu/~saba/pets_class

Instructor Info

Name: Saba Eskandarian  
Office: Brooks 346  
Email: saba@cs.unc.edu  
Web: http://www.cs.unc.edu/~saba  
Office Hours: See course website

Textbooks and Resources

We will primarily use email for course announcements and answering questions. If you have any questions, comments, or suggestions regarding the course organization and policies, please feel free to reach out.

Assignments and grading will be handled via Gradescope. See the class website for a link.

Course Description

This class covers a combination of fundamental tools and recent developments in privacy-enhancing technologies. The first half of the course will cover cryptographic tools that can be used to build privacy-preserving systems, and the second half will cover various privacy-enhancing technologies, including both research contributions and deployed systems. Along the way we will discuss how to think about the technology we create and its impact on society.
Class meetings will consist of a mix of lectures and discussions, with discussion participation being an important component. Students will also complete a semester-long project on a relevant topic of their choosing.

Outline of topics:
1. Topics in private computation (4.5 weeks)
2. Digital money (1.5 weeks)
3. Miscellaneous topics (2.5 weeks)
4. Privacy, anonymity, and surveillance (4.5 weeks)
5. Wrap-up and project presentations (1.5 weeks)

Target Audience

This course is intended for advanced undergraduate students and graduate students who have some background in cryptography and are interested in cryptography research or the development of privacy enhancing technologies.

Prerequisites

The prerequisite for this course is COMP 590/790: Introduction to Cryptography or similar background. Exceptions can be made, so please reach out if you are interested and want to discuss your background.

Other helpful courses to have taken include COMP 435 or 535 (Computer Security), COMP 455 (Models of Language and Computation), or COMP 550 (Algorithms and Analysis), but these are not required.

Goals and Key Learning Objectives

By the end of this course, students should:
• Be familiar with a broad range of advanced topics in applied cryptography
• Be able to read and understand academic papers that use cryptography
• Be prepared to think about and develop technologies that make useful improvements to users’ privacy

Course Requirements

Class meetings will consist of a mix of lectures and discussions. There will additionally be a semester-long course project. Requirements for each appear below.
Lectures: Participation in the form of attendance and asking questions is expected. Most of the first half of the class will be lectures.

Discussions: Some class meetings will consist primarily of discussing assigned readings. Everyone is expected to do the reading, submit a response on Gradescope before class, and participate in the discussion. Most of the second half of the class will be discussions.

*Do not underestimate the amount of time required to properly read and process a research paper. It can take several hours.*

Project: The project will last all semester and will be on a cryptography or privacy-related topic of students’ choice. The project will be completed in groups of up to 3 people and can consist of, e.g., original research, implementations of new cryptographic or privacy-preserving systems, new implementations of systems from existing research works, etc. Feel free to discuss potential project ideas with me in the first few weeks of class. You may use research projects you are already conducting as the class project if your research is connected to cryptography or security.

Project deliverables will consist of an initial proposal, two updates, a presentation, and a final report. The proposal and updates will be 1-2 pages long in a format of your choosing. The final report will be a 5-10 page workshop-style paper properly typeset in Latex, and the presentation will be a 10-15 min description and summary of your project for the class near the end of the semester.

Key Dates

- Project proposal due: Feb 2
- Project update 1 due: March 2
- Project update 2 due: April 4
- Project Presentations: April 20, 25
- Final project report due: April 27

Grading Criteria

- Project: 50%
  - Proposal: 5%
  - Update 1: 5%
  - Update 2: 5%
  - Final presentation: 15%
  - Final report: 20%
- Readings & Responses: 30%
• Participation: 20%

Course Policies

All project-related assignments are due at 11:59pm on the listed day and must be submitted via Gradescope.

Reading responses are due at 11:59pm the night before the lecture for which the readings are assigned. You may skip 3 days of readings with no penalty.

Honor Code

You must write your own reading responses, but you are welcome (and encouraged) to discuss the readings with others or consult other online sources.

Project work must be your own, but you may use research projects you are already conducting as the class project if your research is connected to cryptography or security.

I expect all students to follow the guidelines of the UNC honor code. In particular, students are expected to refrain from “lying, cheating, or stealing” in the academic context. You can read more about the honor code at honor.unc.edu. Please see me if you are unsure about what may or may not violate the honor code in this class.

Course Schedule

See course website for schedule of topics

Attendance and Participation

Class will be held in person. Participation in class discussions are an important part of the course. That said, students who are not feeling well should not come to class and will not be penalized. You can skip 3 class meetings with no penalty. Please get in touch if you need to miss additional days.

Mask Use

This semester, while we are in the midst of a global pandemic, all enrolled students are required to wear a mask covering your mouth and nose at all times in our classroom. This requirement is to protect our educational community — your classmates and me — as we learn together. If you choose not to wear a mask, or wear it improperly, I will ask you to leave immediately, and I will submit a report to the Office of Student Conduct. At that point you will be disenrolled from this course for the protection of our
educational community. Students who have an authorized accommodation from Accessibility Resources and Service have an exception. For additional information, see Carolina Together.

Grade Appeal Process

If you feel you have been awarded an incorrect grade, please discuss with me. If we cannot resolve the issue, you may talk to our departmental director of undergraduate studies or appeal the grade through a formal university process based on arithmetic/clerical error, arbitrariness, discrimination, harassment, or personal malice. To learn more, go to the Academic Advising Program website.

Accessibility Resources and Services

The University of North Carolina at Chapel Hill facilitates the implementation of reasonable accommodations, including resources and services, for students with disabilities, chronic medical conditions, a temporary disability or pregnancy complications resulting in barriers to fully accessing University courses, programs and activities.

Accommodations are determined through the Office of Accessibility Resources and Service (ARS) for individuals with documented qualifying disabilities in accordance with applicable state and federal laws. See the ARS Website for contact information: https://ars.unc.edu or email ars@unc.edu.

Counseling and Psychological Services

CAPS is strongly committed to addressing the mental health needs of a diverse student body through timely access to consultation and connection to clinically appropriate services, whether for short or long-term needs. Go to their website: https://caps.unc.edu/ or visit their facilities on the third floor of the Campus Health Services building for a walk-in evaluation to learn more.

Title IX Resources

Any student who is impacted by discrimination, harassment, interpersonal (relationship) violence, sexual violence, sexual exploitation, or stalking is encouraged to seek resources on campus or in the community. Reports can be made online to the EOC at https://eoc.unc.edu/report-an-incident/. Please contact the University’s Title IX Coordinator (Elizabeth Hall, interim – titleixcoordinator@unc.edu), Report and Response Coordinators in the Equal Opportunity and Compliance Office (reportandresponse@unc.edu), Counseling and Psychological Services (confidential), or the Gender Violence
Services Coordinators (gvsc@unc.edu; confidential) to discuss your specific needs. Additional resources are available at safe.unc.edu.

**Policy on Non-Discrimination**

The University is committed to providing an inclusive and welcoming environment for all members of our community and to ensuring that educational and employment decisions are based on individuals’ abilities and qualifications. Consistent with this principle and applicable laws, the University’s [Policy Statement on Non-Discrimination](https://eoc.unc.edu/report-an-incident/) offers access to its educational programs and activities as well as employment terms and conditions without respect to race, color, gender, national origin, age, religion, creed, genetic information, disability, veteran’s status, sexual orientation, gender identity or gender expression. Such a policy ensures that only relevant factors are considered and that equitable and consistent standards of conduct and performance are applied.

If you are experiencing harassment or discrimination, you can seek assistance and file a report through the Report and Response Coordinators (see contact info at [safe.unc.edu](http://safe.unc.edu)) or the [Equal Opportunity and Compliance Office](http://eoc.unc.edu/report-an-incident/), or online to the EOC at [https://eoc.unc.edu/report-an-incident/](https://eoc.unc.edu/report-an-incident/).

**Diversity Statement**

I value the perspectives of individuals from all backgrounds reflecting the diversity of our students. I strive to make this classroom an inclusive space for all students. Please let me know if there is anything I can do to improve, I appreciate suggestions.

**Syllabus Changes**

I reserve the right to make changes to the syllabus, including project due dates and test dates. These changes will be announced as early as possible.