CS 4803/8803: Programmable Cryptography

Course Information

Latest offering: Fall 2026

Credit Hours: 3

Instructor: Alex Ozdemir

Course Description

This course will introduce recent tools for programmable cryptography, such as zero-knowledge proofs, multi-party computation, fully homomorphic encryption, private information retrieval, differential privacy, and trusted execution environments. These tools take as input a computation, and execute it securely and privately over some data, for different definitions of secure and private. We will learn what these different tools can do, learn how they work internally, learn how to prove security for some of them, and also write some code to use and implement them.

Topics

We plan to learn about these topics:

1. indistinguishability (PRGs)
2. hybrid arguments (Blum-Micali)
3. coin flipping (commitments, Dlog, Pedersen, ROM)
4. IP
5. ZK (physical demo, definition, impossibility)
6. ZK for NP via Hamiltonian cycle (slowly)
7. sigma protocols: knowledge soundness, Schnorr
8. ZK for circuit SAT (sigma combinators)
9. Fiat-Shamir (ROM analysis)
10. succinctness (PCP, Kilian-Micali)
11. polynomial commitments (pairings, KZG)
12. polynomial IOPs (fibonacci)
13. Plonk
14. sumcheck (+GKR)
15. garbled circuits (passive MPC, Bellare-Micali OT)
16. arithmetic MPC (Beaver), malicious security idea
17. DP
18. PIR
19. LWE, Regev
20. FHE (GSW, via eigen-'encryption')
21. TEEs

Required Materials

No textbooks are required.

Grading Policy

The grade cutoffs will be approximately: A > 90%; B > 80%; C > 70%; D > 60%. The instructor reserves the right to adjust these upwards or downwards depending on how hard the assignments and exams end up being.

Graded Components

There will be written assignments, programming assignments, and two exams.

Policies

Attendance
Attendence is encouraged. Lectures will not be recorded and there is no textbook. Notes will be released, but following them without attending has been difficult for past students of this course.

Academic Integrity
Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. Review Georgia Tech's Honor Code and the student Code of Conduct.

Any student suspected of cheating or plagiarism on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Student-Faculty Expectations
At Georgia Tech, we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. The Student-Faculty Expectations articulates some basic expectations that you can have of me and that I have of you. Additional information for research-related work is given in The Expectations of Advisors and Advisees. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Accommodations for Students with Disabilities
If you are a student with learning needs that require special accommodation, contact the Office of Disability Services (404-894-2563) as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Prerequisites
Undergraduate students must have taken CS 3510 (algorithms).

There are no prerequisites for graduate students, but prior experience proving things about programs is recommended. Prior exposure to cryptography (e.g., encryption and signatures) is helpful but not required.

Collaboration
You can discuss and work on all assignments with others. However, you must write up your solutions on your own. Your write-up should also acknowledge your collaborators. For example "I worked on this problem with Alice and Bob."

Generative AI
You can use Generative AI for research and generally learning. You **may not** use it to research specific problems, generate solutions, or revise them.

Extensions
You have three late days to be used in integral amounts. If personal circumstances arise which require a longer extension, contact the instructor.

Acknowledgement
We appreciate the many instructors for Stanford's Advanced Cryptography—David, Henry, Sam, Dima, Florian, Saba, Riad, Neil, Wilson, Lior, Aditi, and Trisha—upon which this course is based.