Course Information

Course: CSCI 3907 / 6907 – Advanced Cryptography
Semester: Spring, 2022
Meeting time: Wednesdays, 12:45 – 3:15
Location: 350 James Monroe Hall
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/advanced_crypto/s22/

Instructor

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office: SEH 4570 and Zoom
Office hours: TBD

Course description

This course will introduce students to the topic of secure multi-party computation (MPC). MPC allows parties to perform joint computation on their private inputs without disclosing those inputs to each other or using a trusted party. The course will cover the definitions and classical constructions of MPC, and then will introduce students to modern research in this topic.

As part of this course, students will learn how to read, understand, and evaluate recent research papers on MPC, and will be expected to present and lead discussion of these papers in class. Additionally, there will be a half-semester long research project that will give students hands-on experience with MPC application development using an existing MPC library.

Course prerequisites

The main prerequisites for this course is mathematical maturity. Students should be able to follow rigorous mathematical concepts and proofs. Some background in algorithms and cryptography is recommended, but is not required. In particular, the intro cryptography course (CS 4331/6331) is NOT required.

Suggested prerequisites to cover this material include:

For CSCI 3907:
CSCI 2312, CSCI 3212, CSCI 3313, MATH 2971

For CSCI 6907:
CSCI 6212

Learning outcomes

As a result of completing this course, students will be able to:

1. Read, understand, and analyze modern crypto research papers in MPC
2. Understand several different MPC protocols and their security
3. Identify open questions based on recent crypto literature
4. Implement simple MPC-based applications using existing libraries

Average expected effort

In addition to 2.5 hours / week of lecture, students are expected to spend approximately 7-10 hours per week on homework, reading papers, and the research project.

Textbooks

None

Grading

The grades for this course will be determined as follows:

Participation in class discussions	20%
Homework	20%
Paper presentation	30%
Research project	30%

In the first half of the semester, there will be several homework assignments that will contribute 20% to the grade. Then, we will shift to reading and discussing recent research papers with each student responsible for leading a presentation on a paper of their choice. These presentations and responses to others' presentations will count for 30% of the grade. Additionally, there will be a half-semester long research project that will count for 30% of the grade. Finally, participation in all lectures and discussion will contribute 20%.

Homework policy

Homework will be assigned during the first half of the course. Homework is due before class (by 12:45PM) on the due date. They must be submitted via Blackboard (https://blackboard.gwu.edu/) by this time to receive credit. Homework can be typed using your favorite tool (I am happy to help anybody interested in learning LaTex) or handwritten and scanned. But, make sure that what you submit is legible as it is what will be graded. No late homework will be accepted!

Students are welcome to work together on homework, however each student must write up and submit their own solutions. If you work on the homework with someone else, you MUST acknowledge them on your submitted homework. The solutions you submit MUST be your own. Make sure to write-up your own answers and that you understand them, copying and pasting solutions is not acceptable. Submitted homework violating these guidelines will be considered in breach of the academic integrity code and will be prosecuted accordingly.

Laptop policy

I ask that students not use laptops or other electronic devices in class (except when presenting). I will make sure to lecture at a pace that allows for hand-written notes. If you need to use an electronic device for taking notes, please come talk to me.

Research Project

A major part of this course will be a research project where students will be expected to implement and experiment with an MPC applications. Specifically, students will design and develop an MPC application

of their choice and then present their findings to the class. The goal of the project is to give students hands-on experience with MPC development.

Lecture schedule

The following is a tentative agenda for the course:

Lecture	Topic(s):
Jan. 12	Introductions, MPC definitions and applications, MPC from multiplication triples
Jan. 19	Proving security of MPC (real-ideal paradigm), malicious security
Jan. 26	Shamir secret-sharing, Efficient MPC for honest majority
Feb. 2	Computationally-secure MPC, SPDZ protocol
Feb. 9	Garbled circuits and optimizations
Feb. 16	Homomorphic encryption
Feb. 23 – Apr. 6	Student paper presentations and paper discussions
Apr. 13	Oblivious RAM and RAM-based secure computation
Apr. 20	Student project presentations

University Policies

Use of Electronic Course Materials and Class Recordings

Students are encouraged to use electronic course materials, including recorded class sessions, for private personal use in connection with their academic program of study. Electronic course materials and recorded class sessions should not be shared or used for non-course related purposes unless express permission has been granted by the instructor. Students who impermissibly share any electronic course materials are subject to discipline under the Student Code of Conduct. Please contact the instructor if you have questions regarding what constitutes permissible or impermissible use of electronic course materials and/or recorded class sessions. Please contact Disability Support Services at disabilitysupport.gwu.edu if you have questions or need assistance in accessing electronic course materials.

University policy on observance of religious holidays

Students must notify faculty during the first week of the semester in which they are enrolled in the course, or as early as possible, but no later than three weeks prior to the absence, of their intention to be absent from class on their day(s) of religious observance. If the holiday falls within the first three weeks of class, the student must inform faculty in the first week of the semester. For details and policy, see "Religious Holidays" at provost.gwu.edu/policies-procedures-and-guidelines.

Academic Integrity Code

Academic Integrity is an integral part of the educational process, and GW takes these matters very seriously. Violations of academic integrity occur when students fail to cite research sources properly,

engage in unauthorized collaboration, falsify data, and in other ways outlined in the Code of Academic Integrity. Students accused of academic integrity violations should contact the Office of Academic Integrity to learn more about their rights and options in the process. Outcomes can range from failure of assignment to expulsion from the University, including a transcript notation. The Office of Academic Integrity maintains a permanent record of the violation.

More information is available from the Office of Academic Integrity at studentconduct.gwu.edu/academic-integrity. The University's "Guide of Academic Integrity in Online Learning Environments" is available at studentconduct.gwu.edu/guide-academic-integrity-online-learning-environments. Contact information: rights@gwu.edu or 202-994-6757.

Academic support

Writing Center

GW's Writing Center cultivates confident writers in the University community by facilitating collaborative, critical, and inclusive conversations at all stages of the writing process. Working alongside peer mentors, writers develop strategies to write independently in academic and public settings. Appointments can be booked online at gwu.mywconline.

Academic Commons

Academic Commons provides tutoring and other academic support resources to students in many courses. Students can schedule virtual one-on-one appointments or attend virtual drop-in sessions. Students may schedule an appointment, review the tutoring schedule, access other academic support resources, or obtain assistance at academiccommons.gwu.edu.

Support for students outside the classroom

Disability Support Services (DSS) 202-994-8250

Any student who may need an accommodation based on the potential impact of a disability should contact Disability Support Services at disabilitysupport.gwu.edu to establish eligibility and to coordinate reasonable accommodations.

Counseling and Psychological Services 202-994-5300

GW's Colonial Health Center offers counseling and psychological services, supporting mental health and personal development by collaborating directly with students to overcome challenges and difficulties that may interfere with academic, emotional, and personal success. healthcenter.gwu.edu/counseling-and-psychological-services.

Safety and Security

- In an emergency: call GWPD 202-994-6111 or 911
- For situation-specific actions: review the Emergency Response Handbook at: safety.gwu.edu/emergency-response-handbook
- In an active violence situation: Get Out, Hide Out, or Take Out. See go.gwu.edu/shooterpret
- Stay informed: safety.gwu.edu/stay-informed