Course Information

Course: CSCI 3907-83 / 6907-83 – Advanced Cryptography
Semester: Spring, 2021
Meeting time: Wednesdays, 12:45 – 3:15
Location: Zoom (info will be provided via Blackboard)
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/advanced_crypto/s21/

Instructor

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office: Zoom
Office hours: By appointment

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 recent research papers on MPC, and be expected to present and lead discussion about the papers they read. Additionally, there will be a half-semester long research project that will require students to use an existing MPC framework to implement and experiment with an MPC application.

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

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 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	20%
Research project	40%

Technology for online instruction

This will be an entirely online class for the Spring 2021 semester. The material will be accessible as follows:

Lectures

All lectures will be held at 12:45 PM on Wednesdays over Zoom. The lectures will be recorded and made available after the class.

Discussion Boards:

Slack will be used for asynchronous discussions and questions about the course material. Students will be expected to participate in discussion every week.

Homework:

All homework will be posted, collected, and graded via Blackboard.

Office Hours:

Office hours will be held via Zoom.

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 if you have questions or need assistance in accessing electronic course materials.

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.

University policy on observance of religious holidays

In accordance with University policy, students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance. For details and policy, see "Religious Holidays" at provost.gwu.edu/policies-procedures-and-guidelines

Support for students outside the classroom

Virtual academic support

A full range of academic support is offered virtually in fall 2020. See coronavirus.gwu.edu/top-faqs for updates.

Tutoring and course review sessions are offered through Academic Commons in an online format. See academiccommons.gwu.edu/tutoring

Writing and research consultations are available online. See academiccommons.gwu.edu/writing-research-help

Coaching, offered through the Office of Student Success, is available in a virtual format. See studentsuccess.gwu.edu/academic-program-support

Academic Commons offers several short videos addressing different virtual learning strategies for the unique circumstances of the fall 2020 semester. See academiccommons.gwu.edu/study-skills. They also offer a variety of live virtual workshops to equip students with the tools they need to succeed in a virtual environment. See tinyurl.com/gw-virtual-learning

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. See 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.

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 to establish eligibility and to coordinate reasonable accommodations. disabilitysupport.gwu.edu

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