Course Information

Course: CSCI 3907-83 / 6907-81 – Advanced Cryptography
Semester: Spring, 2020
Meeting time: Wednesdays, 12:45 – 3:15
Location: 1957 E St. 211
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/advanced_crypto/s20/

Instructor

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office: SEH 4570
Phone: (202)-994-1057
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 applications using existing libraries

Average expected effort

In addition to 2.5 hours / week of lecture, students are expected to spend approximately 10-15 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%

University Policies

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: students.gwu.edu/accommodations-religious-holidays.

Academic integrity code

Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and the fabrication of information. For details and complete code, see: studentconduct.gwu.edu/code-academic-integrity

Support for students outside the classroom

Disability Support Services (DSS)

Any student who may need an accommodation based on the potential impact of a disability should contact the Disability Support Services office at 202-994-8250 in the Rome Hall, Suite 102, to establish eligibility and to coordinate reasonable accommodations. For additional information see: disabilitysupport.gwu.edu/

Mental Health Services 202-994-5300

The University's Mental Health Services offers 24/7 assistance and referral to address students' personal, social, career, and study skills problems. Services for students include: crisis and emergency mental health consultations confidential assessment, counseling services (individual and small group), and referrals. For additional information see: counselingcenter.gwu.edu/

Safety and security

In the case of an emergency, if at all possible, the class should shelter in place. If the building that the class is in is affected, follow the evacuation procedures for the building. After evacuation, seek shelter at a predetermined rendezvous location.