Disclaimer
This syllabus is to be used as a guideline only. The information provided is a summary of topics to be covered in the class.
Information contained in this document such as assignments, grading scales, due dates, office hours, required books and materials may be from a previous semester and are subject to change. Please refer to your instructor for the most recent version of the syllabus.

CSE 598 - Secure Computation for Machine Learning

Spring 2021

1 Contact Information

Instructor: Ni Trieu Email: nitrieu@asu.edu

Office: 130B, Biodesign Building B

Office Hours: Tuesday & Thursday 5:45 PM - 6:30 PM

Zoom Link: `https://asu.zoom.us/j/3345775326`

2 Course Schedule

Lectures: Tuesday & Thursday 4:30 PM - 5:45 PM, Tempe - CDN 68

Zoom Link: `https://asu.zoom.us/j/3345775326`

I will deliver the lectures through the Zoom link above. The course slides or lecture notes will be available on Canvas.

3 Course Description

Many machine learning (ML) algorithms require large-scale data. When the data is sensitive and comes from different sources, it is highly desirable to maintain the privacy of each database while allowing computation of a function (e.g. training a model) on the joint database.

Cryptography is more than just hiding information (i.e., encryption). Using cryptography, it is possible to perform a wide range of computations on secret data that cannot be seen. For example, two hospitals may wish to train various models (e.g. classification) on their joint medical database without revealing any information except the output.

The idea of computing on private data is called secure multi-party computation (MPC). In this course, we will focus mainly on some of the new exciting techniques in MPC with a specific focus on operations used in popular machine learning algorithms.

3.1 Enrollment Requirement

No prior background in cryptography is required as my intention is to make the course accessible to students who have not taken cryptography before. However, mathematical maturity is assumed. Basic ML knowledge and proficiency in computer programming are necessary to be successful in this course.

3.2 Course Objectives

The objectives of this course are:

- To gain foundational knowledge of cryptography and secure computation
- To understand and experiment with privacy preserving ML
- To enable application of cryptographic tools in other areas, and spurring interdisciplinary research.

3.3 Tentative Course Itinerary

This course will introduce the fundamentals of secure computation for machine learning. In total, we will have 15 weeks (30 lecture times) before the final week. Topics to be covered and the approximate time on each topic are given below (in the given order):

1. Introduction (2 lectures):
   - Overview of modern cryptography and topics to be discussed in the class
   - Overview of secure computation and secure machine learning
2. Basics of cryptography(3 lectures):
   - Security definition, Encryption/decryption scheme
   - Block cipher, Pseudo-random functions
   - Secret sharing scheme
3. Secure computation (10 lectures):
   - Oblivious transfer (OT)
   - Secure addition, multiplication
   - Student papers presentation (2 lectures)
   - Secure 2-party computation: Garbled circuit (3 lectures)
   - Introduction to secure multi-party computation
   - Student papers presentation (2 lectures)
4. Secure computation using homomorphic encryption (2 lectures)
5. Privacy-preserving machine learning (7 lectures)
   - Overview
   - Clustering
   - Linear/logistic regression/Neural network
   - Advanced lecture given by Peter Rindal, Research Scientist at Visa Research
   - Student papers presentation (3 lectures)
6. Other practical problems (2 lectures): Private matching, private database query
7. Final project presentations (4 lectures)

3.4 Textbook

1. A Pragmatic Introduction to Secure Multi-Party Computation; David Evans, Vladimir Kolesnikov, Mike Rosulek; `https://securecomputation.org/`
2. Introduction to Modern Cryptography (2nd edition); Jonathan Katz and Yehuda Lindell; `http://www.cs.umd.edu/~jkatz/imc.html`
3. A library for secure machine learning: `https://crypten.ai/`

3.5 Assignment

Homework (30%): Expect 4-5 homework assignments. Most of the homework assignments involve simple programming. For example, writing code for secure aggregation (e.g. 10 parties, each of which has a number and wants to compute a sum of all numbers without revealing anything except the final output). **Note that if you need more time to prepare for your paper presentation, you are allowed to skip the homework right before the presentation.**

Paper reading and presentation (20%): Students will present papers related to lectures.

Final project and presentation (50%): A group of students will choose a machine learning problem (e.g. K-mean clustering) and implement its privacy-preserving version based on secure computation techniques learned through the lectures and homework assignments. Most secure computation components are supported by `https://github.com/facebookresearch/CrypTen`.

Late submission of homework/project will not be accepted.

3.6 Grade Policies

A+	A	A-	B+	B	B-	C+	C-	D	E
$\geq 95\%$	$\geq 90\%$	$\geq 85\%$	$\geq 80\%$	$\geq 75\%$	$\geq 70\%$	$\geq 65\%$	$\geq 60\%$	$\geq 50\%$	$0 - 49\%$

4 Other Policies

4.1 Policy regarding expected classroom behavior

Until further notification, per ASU policy, faculty, staff, students, and visitors, are required to wear face coverings in classrooms, labs, offices, and community spaces.

As this course is delivered online and office hours are held online, the above policy is not relevant unless when/if any in-person meeting is necessary.

However, please note the following policy regarding any Zoom meeting (including the lectures, office hours, and any other ad-hoc meetings) you participate in this class:

- You must use the same (real) name as in your MyASU account. If you use any other name to join a meeting, we will NOT allow that name to earn any attendance credit for you, and the instructor/TA may remove from a meeting anyone who's screen name is not on the official roster.
- You are encouraged to turn on your camera during any meeting (lectures, office hours, etc.). You must turn on your camera upon the instructor/TA's request in any meeting, so that the instructor/TA may see you and your real surroundings (not a virtual background).

Email: Often questions regarding a lecture topic or an assignment may be common for many, and thus it will be most beneficial to ask such questions on the Discussions forum on the Canvas, to avoid repetition. Accordingly, emails should be reserved for solving mostly non-technical matters like grade appeal, reporting excused absence, etc. When you have to send an email, please include in the subject line the prefix CSE 598: (For example, the subject line of your email may read CSE 598: Potential grading error for HW1). A good rule of thumb: if your question cannot be answered in a short paragraph, then it is not appropriate for email.

4.2 Academic Integrity

Students in this class must adhere to ASU's academic integrity policy, which can be found at `https://provost.asu.edu/academic-integrity/policy`. Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. In addition, all engineering students are expected to adhere to both the ASU Academic Integrity Honor Code and the Fulton Schools of Engineering Honor Code. All academic integrity violations will be reported to the Fulton Schools of Engineering Academic Integrity Office (AIO). The AIO maintains record of all violations and has access to academic integrity violations committed in all other ASU college/schools.

4.3 Copyright

All course content and materials, including lectures (Zoom recorded lectures included), are copyrighted materials and students may not share outside the class, upload to online websites not approved by the instructor, sell, or distribute course content or notes taken during the conduct of the course (see ACD 304–06, "Commercial Note Taking Services" and ABOR Policy 5-308 F.14 for more information).

You must refrain from uploading to any course shell, discussion board, or website used by the course instructor or other course forum, material that is not the student's original work, unless the students first comply with all applicable copyright laws; faculty members reserve the right to delete materials on the grounds of suspected copyright infringement.

4.4 Disability Accommodations

Suitable accommodations will be made for students having disabilities. Students needing accommodations must register with the ASU Disabilities Resource Center and provide documentation of that registration to the instructor. Students should communicate the need for an accommodation in sufficient time for it to be properly arranged. See ACD 304-08 Classroom and Testing Accommodations for Students with Disabilities.

4.5 Harassment and Sexual Discrimination

Arizona State University is committed to providing an environment free of discrimination, harassment, or retaliation for the entire university community, including all students, faculty members, staff employees, and guests. ASU expressly prohibits discrimination, harassment, and retaliation by employees, students, contractors, or agents of the university based on any protected status: race, color, religion, sex, national origin, age, disability, veteran status, sexual orientation, gender identity, and genetic information. Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at `https://sexualviolenceprevention.asu.edu/faqs`. Mandated sexual harassment reporter: As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, `https://eoss.asu.edu/counseling`, is available if you wish discuss any concerns confidentially and privately.

4.6 Title IX Language

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at `https://sexualviolenceprevention.asu.edu/faqs`.

As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, `https://eoss.asu.edu/`counseling is available if you wish to discuss any concerns confidentially and privately. ASU online students may access 360 Life Services, `https://goto.asuonline.asu.edu/success/online-resources.html`.

5 Additional Notes

Syllabus changes: Any information in this syllabus (other than grading and absence policies) may be subject to change with reasonable advance notice.
Absent Instructor: If the instructor could not make it to a lecture 15 minutes after its start time and also did not make an advance notice about the absence, you are excused from the lecture (no exam/quiz/test/attendance-taking/importance course content can be given in this lecture, even if the instructor arrives later).