CS 519.003, ECE 599.003: Special Topics in Cryptography
Practical Two-Party Secure Computation

In this course, we will study techniques for practical secure computation. We'll mostly focus on the
special case of two-party secure computation (2PC), specifically those techniques that employ
garbled circuits. Towards the end, we will also discuss other techniques & paradigms as well.

Vital Statistics

Instructor: Dr. Mike Rosulek <rosulekm@eecs.oregonstate.edu>
Meets: MWF 2 @ KEC 1005
Office hours: By appointment @ KEC 3063
Website: https://web.engr.oregonstate.edu/~rosulekm/2pc/

Phase I: Building Blocks

Course structure:

- We will develop the foundations needed to discuss & understand 2PC literature. Students
  will read relevant materials to prepare for in-class lecture/discussion. Lectures will not be a
  substitute for reading the material! Students are expected to come to class having finished
  the relevant readings.

- Lectures will be at a somewhat high level, so there will be occasional homework exercises to
  reinforce the material and fill in some of the low-level details.

- We will collectively develop an annotated bibliography (in the form of an online wiki) for the
  material covered in class. During this part of the class, students will contribute to the wiki by
  writing glossary entries for main concepts.

Topics:

1. Definitions for secure computation: adversary models, simulation paradigm
2. Garbling against passive adversaries: garbled circuit technique, garbling scheme abstracton,
   oblivious transfer
3. Cut-and-choose approach for security against malicious adversaries: understanding the prob-
   lems of input consistency, output authenticity, and selective failure attacks.

Phase II: Exploration

Course structure:

- This part of the course will be highly driven by the students. We will survey a large number
  of papers related to the course topic.
• For each lecture, a group of students will be assigned responsibility for reading and understanding the relevant paper(s). The group as a whole will develop a short annotated bibliography entry for these papers.

• One member of the primary group will present the materials during the lecture (similar to a conference presentation). Every student must present at least one lecture. Presenters must schedule a meeting with me with a prepared draft presentation, at least 1 week before the lecture.

• All other students will provide formal feedback on the presentations as well as the material itself.

Topics:

1. Optimizations at the level of garbled gates: point-and-permute, free XOR, fleXOR, garbled row-reduction, gate-level ciphers

2. Circuit constructions & optimizations: Wire-label tricks, universal circuits

3. Efficiently extending oblivious transfer

4. Improvements to the core cut-and-choose mechanism

5. Covert security and 1-bit leakage as alternatives to malicious security

6. Other paradigms: gate-level cut and choose, GMW protocol, multi-party setting

Miscellaneous

There will be no class on the following days: Friday Feb 21, Monday Feb 24, Wednesday Feb 26.

Other Policies

Cheating: Academic dishonesty (including plagiarism and cheating) will not be tolerated. Consult the university’s student conduct code for more details. I will follow the guidelines given there, and seek out the maximum allowable penalty for violations that occur in this course.

Accommodation of Disabilities: Accommodations are collaborative efforts between students, faculty, and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at 737-4098.