This sheet summarizes information for the course CS 858 F ("(Very Hot) Topics in Computing on Encrypted Data") during the Fall session of 2016 at the University of Waterloo.

Course Website

`TBA,`
`https://piazza.com/uwaterloo.ca/fall2016/cs858/home`

The course website will be available at the start of the first week of classes and it will always contain the most up-to-date information possible regarding the course. *You are responsible for all announcements posted on the course web site and piazza course webpage.*

Instructor

Instructor	**Office**	**Email**
Sergey Gorbunov	DC 3528	`sgorbunov@uwaterloo.ca`

Course Information

A course about encryption-in-use. We will study techniques, cryptographic algorithms, and methods that enable encryption-in-use and allow applications to run over encrypted data. Topics will include multi-party computation protocols, homomorphic, functional, searchable and attribute-based encryption schemes, as well as secure hardware technologies. We will study mathematics behind these algorithms, crypto, performance impacts and integration challenges.

Grading

Item	Worth
Class and Forum Participation	20%
Paper Presentations	20%
Project	60%

Classes

Lecture: Fridays 11am-1.50pm. DC 2585

This seminar will primarily consist of reading, presenting research papers, and discussions. There will be two papers assigned to each class period, selected from the course topics. All students are to have read both of the papers before the class. Each week a student responsible for a paper, must initiate a discussion on piazza web-page a week before. The discussion should include a short paper summary, and a starting list of questions to discuss. Each student must add at least 1-2 questions/discussion topics on the paper 1 day before the class. All students must read the questions/discussion topics and think about them before coming to the class.

Each paper will be presented to the class by one student, in a 50-minute presentation. The presentation will be mixed with questions. The student presenting the paper will then lead the class in a discussion of the paper (using questions and discussion topics from piazza), taking 75 minutes for the presentation and discussion in total for each paper.

Course Outline

This outline is subject to change during the course.

- Week 1: Multi-party computation (MPC) protocols
- Week 2: Fully-homomorphic encryption
- Week 3: Searchable encryption
- Week 4: Order-preserving encryption
- Week 5: In-class project discussions
- Week 6: Systems and applications based on the advanced crypto algorithms
- Week 7: Systems and applications of MPC
- Week 8: Attribute-based and functional encryption
- Week 9: Secure hardware technologies
- Week 10: In-class project discussions
- Week 11: In-class project presentations
- Week 12: In-class project presentations

Academic Integrity

Note that students are not generally permitted to submit the same work for credit in multiple classes. For example, if a student has reviewed or presented one of the papers in another seminar class, he or she should avoid reviewing or presenting it again for this class.

The general university policy:

- Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. Check the Office of Academic Integrity's website (https://uwaterloo.ca/academic-integrity/) for more information.
- All members of the UW community are expected to hold to the highest standard of academic integrity in their studies, teaching, and research. This site explains why academic integrity is important and how students can avoid academic misconduct. It also identifies resources available on campus for students and faculty to help achieve academic integrity in - and out - of the classroom.
- Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70 - Student Petitions and Grievances, Section 4 (https://uwaterloo.ca/secretariat-general-counsel/policies-procedures-guidelines/policy-70). When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.

- Discipline: A student is expected to know what constitutes academic integrity, to avoid committing academic offenses, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offense, or who needs help in learning how to avoid offenses (e.g., plagiarism, cheating) or about ”rules” for group work/collaboration should seek guidance from the course professor, academic advisor, or the Undergraduate Associate Dean. For information on categories of offenses and types of penalties, students should refer to Policy 71 - Student Discipline (https://uwaterloo.ca/secretariat-general-counsel/policies-procedures-guidelines/policy-71). For typical penalties, check Guidelines for the Assessment of Penalties (https://uwaterloo.ca/secretariat-general-counsel/policies-procedures-guidelines/guidelines/guidelines-assessment-penalties).

- Avoiding Academic Offenses Most students are unaware of the line between acceptable and unacceptable academic behaviour, especially when discussing assignments with classmates and using the work of other students. For information on commonly misunderstood academic offenses and how to avoid them, students should refer to the Faculty of Mathematics Cheating and Student Academic Discipline Policy (https://uwaterloo.ca/math/current-undergraduates/regulations-and-procedures/cheating-and-student-academic-discipline-guidelines).

- Appeals: A decision made or a penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72 - Student Appeals (https://uwaterloo.ca/secretariat-general-counsel/policies-procedures-guidelines/policy-72).

Note for Students with Disabilities

AccessAbility Services (https://uwaterloo.ca/disability-services/), located in Needles Hall, Room 1401, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with AccessAbility at the beginning of each academic term.