# Syllabus Fall 2017

## CS848: Topics in Encryption in Databases, Machine Learning and Distributed Systems

- Instructor: Florian Kerschbaum
- Office: DC3524
- Office Hours: by appointment
- Email: florian.kerschbaum@uwaterloo.ca

## Course Website

`https://cs.uwaterloo.ca/~fkerschb/cs848/`

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. We will also heavily use Piazza

`https://piazza.com/uwaterloo.ca/fall2017/cs848/home`

You are responsible for all announcements posted on the course web site and piazza course webpage.

## Grading

- Class and Forum Participation 25%
- Paper Presentation 25%
- Project 50%

## Course Information

This course is about how to operate computer programs, such as databases, machine learning algorithms and distributed systems on encrypted data. We will study the properties of cryptographic algorithms and protocols and how they can be used in these systems. This is not only an exercise in cryptography, but also needs to consider the systems aspects in order to balance performance, security and functionality. The goal is to study practical systems that run over encrypted data and leak as little information as possible.

Cryptographic techniques will include multi-party computation protocols, homomorphic, functional, searchable and property-preserving encryption schemes. We will also look at inferences from the result of the computation and consider techniques such as differential privacy. The systems we study include database management systems, machine learning algorithms and blockchains.

Prerequisites: Students should be familiar with basic crypto (public/secret key encryption, hash functions, etc.). No additional “advanced” math or crypto knowledge is required to take the course. The instructor will give an introduction to the cryptographic techniques used in the read assignments in the first two lectures. Students should also be familiar with undergrad CS topics such as database systems, data mining, neural networks, etc.

The course is currently listed in the database area. It may be possible to count it as an algorithms course under some conditions, if desired.

## Classes

- Lectures: T 3:00pm - 5:20pm, DC2568

This seminar will primarily consist of reading, presenting research papers, and discussions. There will be three papers assigned to each lecture period, selected from the course topics. All students have to read all 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 (3 in total) on the papers 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 25-minute presentation. The student presenting the paper must send the instructor the presentation slides one week before the lecture. 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 45 minutes for the presentation and discussion in total for each paper.

## Course Outline

This outline is subject to change during the course.

- Week 1: Introduction to Secure Multi-Party Computation (instructor taught)
- Week 2: Introduction to Homomorphic, Searchable, Property-Preserving Encryption (instructor taught)
- Week 3: Databases Encryption Using Property-Preserving Encryption
- Week 4: Searchable Encryption
- Week 5: Attacks on Property-Preserving Encryption, Sear
- Week 6: Attacks on Searchable Encryption
- Week 7: Attacks on Machine Learning
- Week 8: Machine Learning on Encrypted Data
- Week 9: Privacy on the Blockchain
- Week 10: Student project presentations
- Week 11: Student project presentations
- Week 12: Student 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 Faculty and 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 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. 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. For typical penalties, check Guidelines for the Assessment of 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.

- 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.

## Note for Students with Disabilities

AccessAbility Services, located in Needles Hall, Room 1132, 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.