COSC 531: Data Privacy

Course Description: This is a graduate-level course in cryptographic techniques for maintaining privacy in the era of massive data. While the course will treat practical techniques, it will be a theory course focusing on rigorous security definitions and proofs of security for such techniques rather than on specific systems and implementation details. The main objective of the course will be to acquaint students with remarkable recent advancements in such cryptographic techniques and provide a bridge to incorporating such techniques into their work.

A main focus of the course will be on techniques for searching on encrypted data; that is, how can we index and search on encrypted data without giving the parties able to perform these operations the ability to decrypt? A secondary focus will be on the basics of secure multiparty computation; that is, how can parties with sensitive datasets compute joint functions of their datasets without revealing them to each other?

Time and Place. TTh 2:00-3:15pm, St. Mary's 326.

Requirements: (1) 3-5 homeworks (60%) and (2) A course project (40%). The homeworks will not require any programming. The project can be either theory or implementation-based. Example course projects are: (1) Read a recent research paper related to a topic covered in the class and write a comprehensive, readable summary and your opinion of it; (2) Work on a research problem related to the course material and your own research, and write a paper following a conference-paper-like format that describes your findings; (3) Implement a protocol covered in the course and do a comprehensive performance evaluation of your implementation. Projects can be done in groups of up to three students; however, the more students involved, the more substantial the project is expected to be. Each group is responsible for clearing their project with me and scheduling progress meetings make sure they are on track.

Textbook: There is no required textbook. We will use a combination of lecture notes for courses at other universities, lecture notes written by the instructor, and recent research papers.

Prerequisites: Graduate standing or consent of instructor. Most importantly, students should have mathematical maturity, being comfortable reading and writing mathematical proofs.

Academic Honesty: Academic honesty is taken very seriously. For problem sets, you are encouraged to work with others, but when you actually write your solutions you must do so by yourself as if you are taking an exam. You must also explicitly list all collaborators with whom you worked and any references or online material you used. Most importantly, never turn in something that you don’t understand! I reserve the right to ask you to explain to me something you turned in, and if you cannot do so in a way that demonstrates your understanding, you will not receive credit and may be reported to the University.