COSC732: Advanced Cryptography

Course Description: This is a graduate-level course in advanced cryptography. The goal of the class will be to provide a bridge to research. We will read and discuss some recent influential papers. Topics will be based on student interest but may include: program obfuscation, functional encryption, instantiating random oracles.

Time and Place: MW 5:00-6:15pm, Reiss 284.

Requirements: There will be a few assigned homeworks that are more open-ended than traditional assignments and may have research potential. Students are also expected to read the assigned papers and participate in class discussions. The majority of the grade will be based on class participation. Students may also work on a course project which integrates cryptography with their own research. Those doing a project will not be required to hand in the homework.

Textbook: There is no required textbook. Lectures will mostly be based on research papers which will be assigned ahead of time.

Prerequisites: A basic knowledge of cryptography including block ciphers, symmetric encryption schemes, message authentication codes, public-key encryption schemes, digital signatures, and their security. Good references for this material include lecture notes by Bellare and Rogaway (http://cseweb.ucsd.edu/~mihir/cse207/classnotes.html) and a textbook by Katz and Lindell (http://www.cs.umd.edu/~jkatz/imc.html).

Academic Honesty: Students are expected to behave according to Georgetown’s Honor System. When handing in homework please explicitly list all collaborators with whom you worked and any references or online material you used, separately for each problem. Failure to acknowledge such sources of information is considered plagiarism.