CMSC 33251: Topics in Computer Security: Theoretical Symmetric Cryptography

Lectures: Tuesdays and Thursdays, 12:30-1:50pm in Ryerson 277 (Annex)

Instructor: David Cash, davidcash@uchicago.edu

Prerequisites: Some familiarity with modern theoretical cryptography. Alternatively, a good grounding in probability, algorithms, and complexity may be sufficient for students willing to learn the crypto background topics on their own.

Course description: This course will cover the usage of idealized primitives and information theory in (mostly) symmetric cryptography. Topics will be selected (and added to) the following list:

- The random oracle (RO) and ideal cipher (IC) models.
- Analysis techniques for encryption, MACs, and hash functions.
- Time-space trade-offs, including rainbow tables and attacks on other primitives. Lower bounds for such trade-offs.
- The generic group model, including algorithms and lower bounds.
- The bounded-retrieval model (aka “big-key crypto”).
- Garbled circuits and secure two-party computation.

The course can be taken pass-fail or for a letter grade, but does not count for an elective. For pass-fail, the requirement is that you read the papers, attend the lectures, and follow the topics. For a letter grade, you need to complete a project related to the course topics, and present a lecture on a topic related to your project. You should notify me that you are taking the course for a letter grade by week 3; At that time you should have a proposed topic area and discuss it with me.

Before each lecture, a relevant resource (usually a paper) will be posted. You are expected to attempt reading it before lecture, and come with questions.

Projects: Projects may be completed alone or in pairs. There are two options for projects:

1. Survey option. Read between 3-5 papers on a topic, and write a clean survey of the area that places the prior results in a common framework. This requires some substantial thought and assimilation of results (e.g. giving unifying definitions or proofs).

2. Research option. Working with me, identify a direction in which to find an open problem and attempt to solve it. Write up your progress at the end of the quarter.
In both cases, your write-up is due during finals week.

**Student presentations:** Students doing a project will present half of a lecture to the class. Dates will be chosen after week 3. The actual presentations will take place weeks 5-10, depending on when everyone is ready. If you are doing a project as a pair, then you will each present your own half-lecture.

Before your presentation, you will meet with me to plan the topics you’ll present and discuss your plan for the half-lecture.