CMSC 33251: Topics in Computer Security: Theoretical Symmetric Cryptography

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

Instructor: David Cash, `davidcash@uchicago.edu`

Webpage: `https://people.cs.uchicago.edu/~davidcash/33251-symmetric/index.html`

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. Meetings will focusing on a few results with a discussion leader. A tentative list of papers and schedule is posted on the course webpage. Before each meeting, a relevant resource (usually a paper) will be posted. You are expected to attempt reading it before lecture, and come with questions.

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 meetings, and lead discussion at least once. For a letter grade, you need to complete a project related to the course topics in addition to the pass-fail requirements. **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.**

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.

Leading meetings: I will lead meetings for about the first two weeks, and rotate in occasionally thereafter. Dates for rotating the lead for meetings will be chosen during week 2.