600.641 Special Topics in Theoretical Cryptography March 26, 2007

Handout 6: Problem Set 3

Instructor: Susan Hohenberger

Current Research Talks

Each student will present a current research paper of their choice from ASIACRYPT, CRYPTO, EUROCRYPT, or TCC from 2002 or later.[1] Talks will be 20 minutes each with 5 minutes afterwards for questions. Students *may* be briefly interrupted during their main presentation for quick clarifying questions. A grade will be assigned worth 26% of your final grade (the rest is 34% for PS1 and PS2, 30% for scribing, and 10% participation).

A Powerpoint (or equivalent) presentation is recommended. If you do not have a laptop or you would like to use transparencies, please make arrangements with Susan a week in advance.

The purpose of this assignment is three-fold. First, the purpose is to evaluate your ability to read, understand, explore, and critique current cryptography research. To this end, your presentation should be clear, interesting, and comprehensive. Twenty minutes is not a lot of time, but an organized speaker should be able to clearly explain and motivate the problem at hand, describe the solution using an appropriate mix of intuition and details, talk about extensions, touch on the related (and perhaps subsequent) work, and communicate the main strengths and weaknesses of the paper. It is highly recommended that you practice your talk before giving it to make sure it fits in 20 minutes.

Second, the purpose is to allow you to practice the *necessary* research skill of being able to confidently and clearly communicate technical ideas to your peers. To this end, the entire class will be given slips of paper for each talk on which they should record advice for the speaker. (This may range from "The intuition provided was not much beyond the abstract of the paper. I would have liked to see more details." to "There was so much math on slide 10 that I couldn't identify the big ideas." to "You said 'ummm' more than 30 times." to "I really liked the motivation and applications you mentioned.")

Third, have fun! Cryptography is an exciting research area. We will hear about 12+ recent results over the course of two weeks. This is a great opportunity for gathering new ideas and deciding which topics most interest you.

Collaboration Policy: As always, you are encouraged to discuss ideas with your classmates. However, each student *must* create their own presentation and should understand the material in depth on their own.

[1] Before you decide to change topics from those indicated in Problem Set 2, please check with me.