CO 685 Project Descriptions

Student evaluations in CO 685 will be based in part on a final project. The project involves a typed report on a topic of your choice, due on **Tuesday, December 22, 2009**. The report should, at a minimum, present the topic material in a way that substantially improves upon every other presentation available in the literature.

Please choose a topic which is of interest to you. Otherwise, it will be very hard for you to do well on the project. You may choose a topic from the list below, or you may choose your own topic. In either case, **I must approve your topic** before you can receive credit for your project.

Two students may not share the same topic. *All such conflicts will be resolved on a first-come-first-served basis.*

Sample topics

- Polynomial time primality testing (AKS etc.)
- Special purpose factoring hardware (TWIRL etc.)
- Relationships between security notions
- Elliptic curve primality proving
- Number field sieve
- Point counting on elliptic curves
- XTR and point compression
- Group signatures
- Blind signatures
- Undeniable signatures
- Electronic voting
- Electronic cash
- Homomorphic encryption
- Private information retrieval
- Password authenticated key exchange
- Implementations of cryptographic pairings
- Hyperelliptic curve cryptography

. . . or a topic of your choice.

Evaluation criteria

Projects will be evaluated according to the following criteria, each weighted equally. The intent is to simulate as closely as possible the peer review process at an academic conference.

Technical merit: This category includes correctness of your proofs, significance of the results, originality (if applicable), and clarity of your technical explanations.

Suitability: Within your choice of topic, you will be evaluated on the choice of which subtopics you include, and which ones you exclude. Your aim should be to provide a balanced treatment that is as comprehensive as possible without sacrificing focus.

Presentation: Factors that affect your presentation score include organization of your paper, paragraph and sentence structure, grammar and spelling, and overall readability.

Some of these areas overlap with others, and (just as with a real conference) you may find that your scores in one category are correlated with scores in the others.