Institut for Matematik og Datalogi
Syddansk Universitet

April 18, 2011
JFB

Cryptology – F11 – Week 10

Lecture, April 14

We finished with undeniable signatures from the notes (the denial protocol) and began on zero-knowledge (from the notes by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage). We covered definitions and the proof of quadratic residuosity.

No lecture, April 18

Lecture, April 28

We will continue with on zero-knowledge (from the notes by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage).

Lecture, May 4

We will continue with zero-knowledge, from the notes and slides, and begin on chapter 9 in the textbook.