Institut for Matematik og Datalogi
Syddansk Universitet

November 29, 2019
JFB

Cryptology – 2019 – Lecture 18

Announcement

I have moved the remaining lectures on Thursdays to Mondays and Tuesdays in December.

Lecture, November 25

We began on protocols and zero-knowledge from the slides, covering up through the Rubik's Cube example. Interactive proof systems are defined in section 21.1 of the textbook and zero-knowledge in section 21.2. Bit commitment from chapter 20 were also discussed.

Lecture, December 2

We will finish protocols from the slides.

Lecture, December 9

We will continue with chapter 21, concentrating on sections 21.3 and 21.4. We will also go over some problems from the second assignment.

Problem session December 10

We will finish those problems not finished on December 3 and any problems from the second assignment which are not finished.