Institut for Matematik og Datalogi
Syddansk Universitet

December 10, 2019
JFB

Cryptology – 2019 – Lecture 20

Announcements

1. Information about the exam and the required task for being allowed to take the exam are now available on the course homepage. Do not forget the required task.

2. The only remaining class time will be 8-10 on Monday, December 16.

Lecture, December 9

We looked at zero-knowledge proofs for graph isomorphism and graph nonisomorphism. The graph isomorphism result is in section 21.1. The graph nonisomorphism result is just another example similar to the quadratic nonresiduosity. (Special soundness is defined in section 21.3.)

Problem session December 10

We went over Assignment 2 and a problem from the 16th lecture note about proving in zero-knowledge that two strings committed to were different.

Lecture, December 16

We will talk about the exam. I will also present an electronic voting system from seciton 21.4. There may be a small slice of cake.