Institut for Matematik og Datalogi
Syddansk Universitet

May 12, 2008
JFB

Cryptology – F08 – Week 14

Lecture, May 7

We finished chapter 9 in the textbook and began on chapter 10.

Lecture, May 13

We will cover sections 10.1, 10.2, and 10.5.4 of chapter 10, section 11.2 of chapter 11, and section 13.1 of chapter 13.

Lecture, May 15

We will cover quantum cryptography from Charles H. Bennett, Franois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography", J. of Cryptology 5, 1992. This can be found through a link on the course's homepage.

Lecture May 21

We will introduce quantum computation and Shor's factoring algorithm from de Wolf's survey, which can be found through a link on the course's homepage.

Problem sessions May 20 and 22.

1. Continue with any unfinished problems from last week.
2. Let x, y be two bit strings of length n. Suppose $x \neq y$. Choose a random subset S of the n indices and let $x' = \sum_{s \in S} x_s \pmod 2$ and $y' = \sum_{s \in S} y_s \pmod 2$. Prove that the probability that $x' \neq y'$ is exactly $1/2$.

3. Explain why removing the last bit from a set removes any information given by the parity of that set.

4. Suppose, as in the fourth assignment, that there are bit commitments to n bits, all of which are zero. Design a zero-knowledge protocol to prove this, using the following outline for one round of the protocol: The Prover creates a new bit commitment Z which is also a commitment to zero. The Verifier specifies a random subset to check that the parity of the bits committed to is zero. The Verifier also sends a single bit challenge. The Prover responds by opening Z or by opening Z divided by the product of all the bit commitments in the set specified earlier.

   Prove that this is zero-knowledge. Prove completeness. What is the probability of a Verified accepting even though the Prover is cheating?

5. Come with questions about the exam.