Institut for Matematik og Datalogi
Syddansk Universitet

May 28, 2013
JFB

Cryptology – F13 – Week 14

Lecture, May 23

We discussed a few more topics in quantum cryptography, including bit commitment, and continued with quantum computation from we will begin on quantum computing from R. de Wolf's survey on Quantum computation and Shor's factoring algorithm, which can be accessed through the course's homepage.

Lecture, May 30

We will cover up through section 13.2.1 in chapter 13. I will lecture on a small depth-16 for the AES S-box.

Problem session May 31

1. Do problem 13.2 in the textbook.

2. Consider the Hadamard transform on two bits:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

   What is the result of applying it to the basis vectors? How about applying H^2?

3. Compute the continued fraction expansion of 126/55.