

## Cryptology – F13 – Week 13

### Lecture, May 16

We finished section 13.1 of chapter 13 in the textbook and covered quantum cryptography from Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography", J. of Cryptology 5, 1992. This can be found on-line through SDU's library (under the archived volumes of that journal).

### Lecture, May 23

We will discuss a few more topics in quantum cryptography and continue 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 finish quantum computing. We may also cover up through section 13.2.1 in chapter 13 and up through Theorem 10.4 in section 10.4 in the textbook.

### Problem session May 31

1. Do problem 13.2 in the textbook.
2. Consider the Hadamard transform on two bits:

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

What is the result of applying it to the basis vectors?

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