Institut for Matematik og Datalogi — May 23, 2011
Syddansk Universitet — JFB

Cryptology – F11 – Week 15

Instruktorater

Hjælp dine medstuderende, dygtiggør dig selv og få penge for det. Søg i dag!
Der er ofte gode muligheder for at få et instruktorat, selvom man ikke er langt henne i studiet. Se nærmere information på

`http://www.jobs.sdu.dk/vis_stilling.php?id=6562&lang=da`

Hvis du allerede er ansat som instruktor i foråret 2011, leverer du ansøgning om tildeling af timer ind på IMADAs sekretariat (se opslaget vedr. bilag mm.)
Hvis du har sprgsmål, så henvend dig gerne på IMADA.

ANSØGNINGSFRIST: **27. maj 2010 kl. 12:00**.

Lecture, May 19, from 11:15 to 12

We finished 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). Then 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 25

We will cover 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.. 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 26

1. 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.

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

We will do a course review. Come with questions.