T-79.4001 Seminar on Theoretical Computer Science (3 cr) V

Spring 2008 -- Protecting Information

http://www.tcs.hut.fi/Studies/T-79.4001/

Seminar

- Wednesdays 12-14, hall TB353
- Language: English
- Text book: Susan Loepp and William K. Wootters

  http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=9780521534765

  Protecting Information: From Classical Error Correction to Quantum Cryptography

  (Cambridge University Press, 2006).

  One copy of the book will be available for short-term loan and another for reading-room use in the DCSE library.

Passing the course

- Seminar presentation plus archivable slides 3 cr.

- In addition, feedback must be provided for the speakers of at least three sessions using the respective electronic forms.
- Forms will be available via the seminar schedule.
- Feedback forms for presentations in a given week must be completed by the beginning of the session on the following week.

Overview

- Protecting information against noise and eavesdropping
- Error correcting codes and cryptography
- Applications of Quantum Mechanics to achieve these goals
  - Quantum cryptography
- Quantum computing
  - Schor's algorithm for factoring large integers

Schedule

23 Jan: Opening, overview, handing out assigments

30 Jan:

- Enigma *Vehkamäki*
- Number theory for Schor's algorithm *Fagerholm*

6 Feb:

- Photon polarization *Putkinen*
- General quantum variables and composite systems *Häkkinen*

20 Feb:

- Measuring a subsystem and other incomplete measurements *Malinen*
- Bennett-Brassard QKD protocol *Lindfors*

27 Feb:

- No-cloning theorem *Lahola*
- Quantum teleportation *Kettunen*

Schedule

5 Mar:

- Error-correcting codes introduction, Hamming distance *Sevalnev*
- The Hat Problem *Peltola*

9 Apr:

- Linear codes, generator matrices, dual codes *Korpela*
- Syndrome decoding and error correcting for QKD *Päivärinta*

23 Apr:

- Privacy amplification *Nevalainen*
- Quantum gates *Pieviläinen*

30 Apr:

- The Deutsch algorithm *Savola*