Wahlpflichtfach (3+1 SWS) im WS2011

Prof. Dr. Thomas Canzler
canzler@informatik.haw-hamburg.de

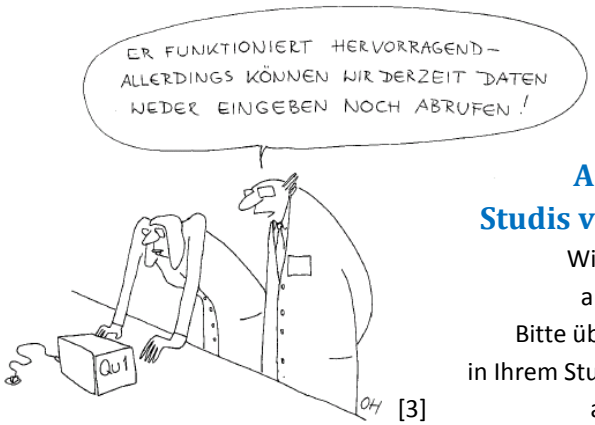
Quantenrechner

Die Kryptoknacker? ...

und

Quantenkryptographie

... Perfekte Verschlüsselung? ...



[3]

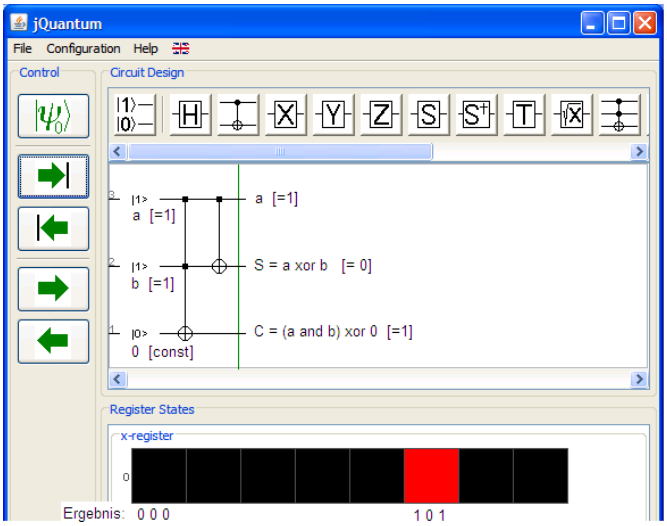
Auch für Studis von IuE!
Wird als WP anerkannt.
Bitte über STISYS in Ihrem Studiengang anmelden und eMail an mich.
Termin: freitags

... „Was die Quantenmechanik mit der einen Hand nimmt, gibt sie mit der anderen"

Quantenrechner (QR) arbeiten hochgradig parallel und können daher bestimmte Probleme sehr effektiv lösen – z.B. die Primfaktorzerlegung, mit der heute übliche Verschlüsselungsverfahren ‚geknackt' werden könnten. Ihre Realisierung steckt allerdings noch sehr in den Anfängen. Die Theorie hingegen ist inzwischen gut bekannt, und es gibt schon eine sehr große Zahl von Simulatoren [4,5], mit denen man Quantenalgorithmen entwickeln kann.
Die *Quantenkryptographie* (QK) erlaubt – zumindest im Prinzip – eine sichere Verschlüsselung. Hier gibt es bereits kommerzielle Produkte.

Voraussetzungen

- Eine Vorstellung davon, was Vektoren sind
- Ansonsten: keine weiteren Voraussetzungen
- Alle weiteren Begriffe werden in der Vorlesung entwickelt



Simulation eines reversiblen Quanten-Halbaddierers [4]

Literatur

[1] Dagmar Bruß: Quanteninformation; Fischer: Frankfurt 2003. Eine allgemeinverständliche Einführung.
[2] Matthias Hohmeister: Quantum Computing verstehen; Vieweg: Wiesbaden 2005.
Guter ‚Rundumschlag' über das ganze Gebiet, mit Anhängen: Geschichte, Übungen, math. Grundlagen
[3] Spektrum der Wissenschaft 11'2008, S 56

Lernziele

- Grundlagen der Quantenrechner (und deren Unterschiede zu konventionellen Rechnern) verstehen
- Einen Quantenalgorithmus verstehen und simulieren (evtl. sogar den zur Primfaktorzerlegung)
- Quantenkryptographie verstehen

Inhalt

- Grundlagen, u.a.:
  - Superposition [warum arbeiten QR so effektiv parallel?]
  - No-Cloning-Theorem [Schutz gegen Abhören]
  - Verschränkung [Teleportation / "Beamen"]
  - Quantengatter [warum **müssen** sie reversibel sein?]
- Quantenrechner, u.a.:
  - Realisierung
  - Simulation [4,5]
  - Quantenalgorithmen
  - Quantenprogrammiersprachen
- Quantenkryptographie, u.a.:
  - Verschlüsselungsverfahren
  - Schlüsselerzeugung

Links

[4] http://jquantum.sourceforge.net/jQuantumApplet.html [4.5.2010] // Java-Applet und ausführbares Programm für Entwurf und Simulation von Quantenschaltungen, mit ladbaren Beispielen
[5] http://www.quantiki.org/wiki/index.php/List_of_QC_simulators [4.5.2010]