Graz University of Technology

Institut für Theoretische Physik – Computational Physics

. .
Institut für Theoretische Physik
– Computational Physics
TU Graz
Petersgasse 16
A-8010 Graz (Austria)

DVR: 008 1833 UID: ATU 574 77 929

Vortragsankündigung

Im Rahmen des Projektpraktikums
Theoretische Physik - Computational Physics

findet am **Mi. den 8. Okt 2008 um 17:15 im Hörsaal P3**
der Vortrag von **Manuel Grill** über

„Quantencomputer- Vorteil demonstriert am RSA-Verfahren, Kryptoanalyse mit Shor 94“

statt.

Abstract:

- Zuerst wird bei dieser Präsentation eine kleine Einführung in die (1.) Grundlagen der Kryptographie (’public-key’-Kryptographie),
- (2.) Grundlagen des Quantencomputers (grundlegende Gates, Fouriertransformation, Quantenparalleslismus,’Schnelligkeit’) gegeben. Danach wird der
- (3.) Shor-Algorithmus genauer betrachtet, und es werden immer wieder (4.) Überlegungen zur Effizienz dieses Algorithmus angestellt.
- Abschließend „betreiben“ wir Kryptoanalyse und sehen uns 2 konkrete Beispiele an:
- (5.) Demonstrationsbeipsiel mit kleinen Zahlen
- (6.) Demonstrationsbeispiel mit größeren Zahlen