



sie nach Cambridge zu ihrem Neffen Otto Frisch, wo sie ihren Lebensabend verbrachte.

Am 27. Oktober 1968 starb die fast 90jährige, die ihr Leben der friedlichen Nutzung der Atomenergie verschrieben hatte. Auf ihrem Grab-

stein steht: "A physicist who never lost her humanity".

(ga)

Quelle: Ulla Fölsing: Nobel-Frauen, Naturwissenschaftlerinnen im Porträt. München: Beck, 1991.

Dieses Buch und viele andere sind (wegen der Umstrukturierung erst) ab dem Sommersemester jeweils Dienstag von 13 bis 15 Uhr bei Sabine Höfert, Frauenreferatsbibliothek, ÖH-Technik, auszuleihen.

Gastprofessor

## Maguire - Ein Gastprofessor aus America

**Als Techniker sollte man - nach dem neuen Gesetz - Lehrveranstaltungen besuchen, die in Englisch gehalten werden. Das Angebot solcher Vorlesungen an der TU ist leider gering. Umso erfreulicher ist es, wenn man die Chance hat, eine Vorlesung bei einem amerikanischen Professor besuchen zu können.**

Im kommenden Sommersemester wird Prof. Gerald Quentin Maguire als Gastprofessor nach Graz kommen. Er überzeugt durch eine umfangreiche Liste von wissenschaftlichen Arbeiten, diversen Veröffentlichungen und ein paar Bücher.

### Im Sommersemester will er folgende LV anbieten:

- \* Computer Networks  
The course will examine computer networks with an emphasis on the levels above the

physical and link levels. Several different protocol families will be examined - with an emphasis on TCP/IP and ISO OSI. This course will also explore the effects of the merge of computing and communications.

- \* A graduate seminar to focus on routing (in LAN and WAN) communications which will include:
  - (1) what happens when processing rather than bandwidth is the limiting factor in network
  - (2) routing for mobile computing and communication devices
  - (3) will routing replace switching

(pm)

Informationen bei: Institut 505, Angewandte Informationsverarbeitung und Kommunikationstechnologie, Klooswiesgasse 32/1, Prof. R. Posch

Bei der Übertragung, Speicherung und Abfrage von Daten treten immer häufiger Forderungen nach Informations- und Kommunikationssicherheit in den Vordergrund. Neben Vertraulichkeit und Integrität der Daten muß dabei zumeist auch gewährleistet werden, daß Ursprung und Empfänger der Daten authentisch sind.

Ausgehend vom diskreten Logarithmusproblem und dem darauf aufbauenden Signaturverfahren von ElGamal werden Modifikationen sowie die daraus abgeleitete Generalisierung dargestellt. Desweiteren wird gezeigt, wie sich solche Signaturverfahren in Protokollen zur Authentifikation von Benutzern und zur Vereinbarung authentischer Schlüssel einsetzen lassen. Hierbei ist insbesondere die Einrichtung von Zertifizierungsinstanzen von Bedeutung. Als weitere Anwendungen werden die Realisierung eines (einfach zu beweisenden) Zero-Knowledge-Protokolls so wie die elektronische Version eines Münzwurfs (Coin-Flipping-Protokoll) betrachtet. Dabei zeigt sich, daß das diskrete Logarithmusproblem, als nahezu universelles Hilfsmittel eingesetzt werden kann.

Dies ist eine kurze Beschreibung der Lehrveranstaltung, die der Gastprofessor Dr. Patrick Horster im SS94 hier in Graz halten wird.

(pm)

