ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

FAKULTÄT FÜR ANGEWANDTE WISSENSCHAFTEN

Fakultäts - Kolloquium

Zeit: Mittwoch, 26.06.1996, 17.00 Uhr c.t.
Ort: Raum 02-017, Geb. 52, Am Flughafen 17

Interaktive Beweise, Zero-Knowledge und kryptographische Anwendungen

Prof. Dr. Uwe Schöning

Universität Ulm

Abstract

Der Vorgang des Beweisens kann in einer interaktiven Weise zwischen zwei Parteien, dem Beweiser und dem Verifizierer, stattfinden. Durch das Verwenden von Zufallszahlen wird es möglich gemacht, daß derartige interaktive Beweise kürzer sein können als konventionelle. Ferner ist es möglich, daß der Verifizierer vollständig von der Tatsache überzeugt wird, daß der Beweiser den Beweis (das kann zum Beispiel ein Passwort sein) kennt, ohne daß aus der Kommunikation zwischen Beweiser und Verifizierer auf den Beweis rückgeschlossen werden kann. Solche *interaktiven Zero-Knowledge Beweise* spielen eine wichtige Rolle in verschiedenen kryptographischen Anwendungen.

Gastgeber: Prof. Dr. Thomas Ottmann

Alle Interessenten sind recht herzlich eingeladen.

Organisation : Prof. Dr. B. Becker / H. Hengster
Weitere Informationen im WWW unter http://www.informatik.uni-freiburg.de:/~hengster/kolloquium oder von H. Hengster (Tel: 0761/203-8148; Email: hengster@informatik.uni-freiburg.de).