Johann Wolfgang Goethe-Universität Frankfurt am Main
Fachbereich Informatik und Mathematik

Prof. Dr. Detlef Krömker

Einladung zum Vortrag

am

Donnerstag, den 01.02.07 um 14.00 Uhr
im Seminarraum 612 (Robert-Mayer-Str. 10)

hält

Herr Dr. Küsters
ETH Zürich

einen Vortrag mit dem Titel:

Modularer Entwurf und Analyse kryptographischer Protokolle

Zusammenfassung:

Kryptographische Protokolle bilden die Basis sicherer Kommunikation und Geschäftsprozesse. Der Entwurf kryptographischer Protokolle ist allerdings äußerst komplex und fehleranfällig, da diese Protokolle ihre Sicherheitsziele auch dann erreichen müssen, wenn Kommunikationspartner unehrlich sind, d.h., vom Protokoll abweichen, oder Angreifer das Kommunikationsnetzwerk kontrollieren. Mathematisch präzise Definitionen von Sicherheitsanforderungen, der modulare Entwurf sowie die systematische Analyse kryptographischer Protokolle sind deshalb unverzichtbar.

Im Vortrag werde ich diese zentralen Probleme im Bereich der Kryptographischen Protokolle näher erläutern und einen Überblick über meine Beiträge dazu geben, welche an der Schnittstelle zwischen Logik und formalen Methoden auf der einen sowie Kryptographie auf der anderen Seite liegen.