



Universität Karlsruhe (TH)
Fakultät für Informatik
*Institut für Algorithmen und
Kognitive Systeme*
Dipl.-Inform. Jens-Matthias Bohli
Dr. Jörn Müller-Quade
Dipl.-Inform. Stefan Röhrich
Dipl.-Inform. Dominique Unruh

Am Fasanengarten 5
Postfach 69 80
D-76128 Karlsruhe
Telefax: +49 721 608 55022

Seminar im Wintersemester 2005/2006

Komplexität und Kryptographie

Die Notwendigkeit von Sicherheitsbeweisen für kryptographische Protokolle wird in letzter Zeit mehr und mehr erkannt. Im Lichte dieser Entwicklung wollen wir in diesem Seminar erarbeiten, wie in solchen Beweisen die Sicherheit eines Protokolls auf komplexitätstheoretische Annahmen zurückgeführt wird.

Untersuchte Themenkomplexe sind unter anderem:

- Sicherheitsmodelle
- Komplexitätsannahmen
- Reduktionsbeweise

Voraussetzungen

Das Seminar richtet sich an Studenten der Informatik, Mathematik, Physik und verwandter Fächer im Hauptstudium.

Über die im Vordiplom angebotenen Mathematikvorlesungen hinaus sind keine Vorkenntnisse nötig. Eine gewisse Vertrautheit mit Algebra und Wahrscheinlichkeitstheorie ist sehr empfehlenswert. Grundlegende kryptographische Kenntnisse, z. B. aus den Vorlesungen Public-Key-Kryptographie und Signale, Codes, Chiffren II sind hilfreich.

Anmeldung: per E-Mail oder persönlich

Vorbesprechung: **Mittwoch, 2. November 2005**, um 13¹⁵ Uhr im Seminarraum 252.

Fragen bitte richten an:

Jens-Matthias Bohli (Zi. 259, 608-6310), Jörn Müller-Quade (Zi. 238, 608-4327), Stefan Röhrich (Zi. 230, 608-4025), Dominique Unruh (Zi. 238, 608-6287) im Informatik-Neubau.

E-Mail: {bohli, muellerq, sr, unruh}@ira.uka.de

WWW: <http://iaks-www.ira.uka.de/home/roehrich/lehre/ws200506/seminar-komplexitaet/>