Praktikum / Diplomarbeit
in
- Kryptographie -

Thema: Es gibt unterschiedliche Themenstellungen mit Bezug zur aktuellen Forschung in der Kryptographie. Insbesondere geht es um Stromchiffren, Hashfunktionen oder SAT Solver. Stromchiffren werden überall dort benötigt, wo große Mengen an Daten online (also schnell) verschlüsselt werden sollen. Bekannte Anwendungen die Stromchiffren verwenden sind: GSM, Bluetooth, UMTS RFID sowie Streaming-Video und Audio Anwendungen. Die Stromchiffren in GSM und Bluetooth sind mitlerweile gebrochen und die Anwendungen gelten somit als unsicher. Deswegen findet aktuell viel Forschung auf diesem Gebiet statt, mit dem Ziel neue sichere Stromchiffren zu entwickeln (ähnliches gilt für Hashfunktionen). Die Theorie in diesem Gebiet ist noch wenig fortgeschritten, somit beruht die Sicherheit im wesentliche darauf dass Angriffe auf diese Chiffren bislang erfolglos waren. Solche Angriffe sind u.A. mittels SAT Solvern möglich.

Ablauf: Im **Sommer Semester 2008** bieten wir Diplomarbeiten oder individual Praktika auf diesem Gebiet an. Der Beginn ist auch bereits in der vorlesungsfreien Zeit möglich.

Voraussetzungen: Das Angebot richtet sich an Studenten der Informatik oder Mathematik. Wichtig sind grundlegende Kenntnisse in Mathematik/Wahrscheinlichkeitsrechnung und in theoretischer Informatik. Weniger wichtig sind Vorkenntnisse in Kryptographie.

Anspruch: Durch die Arbeit erfährt man einiges über aktuelle kryptographische System und den Stand der Forschung. Weiter bekommt man einen Eindruck wie wissenschftliches Arbeiten in der theoretischen Informatik stattfindet. Das Ziel der jeweiligen Themenstellung wird immer sein, einen Beitrag zur aktuellen Forschung zu leisten, was aber natürlich nicht notwendig erreicht werden muss.

Betreuung: Die Arbeiten werden betreut durch Dipl.-Inf. Tobias Eibach und Prof. Schöning. Bei Interesse bitte mit T. Eibach Kontakt aufnehmen: tobias.eibach@uni-ulm.de oder O27 Zimmer 532.