Prof.Dr.C.P.Schnorr

BLOCKSEMINAR „Kryptographie und Komplexität".

Raum 612, Robert-Mayer-Str. 10

Freitag, 19. Juni

14:15	A. Maurer:	Verbesserte Analyse des SVP Algorithmus von Kannan
16:00	P. Sacher:	Das Closest Vektor Problem

Freitag, 26. Juni

14:15	M. Bachmann und M. Leinweber:	Interaktive Beweissysteme, Teil I
16:00		Interaktive Beweissysteme, Teil II

Freitag, 3. Juli

14:15	V. Michalski:	Beweisbar schnelle Faktorisierung ganzer Zahlen nach B. Vallee
16:00	H. Jamal:	Das Public-Key Kryptosystem von Paillier

Weitere Vorträge werden nach Abschluss ihrer Vorbereitung ergänzt.