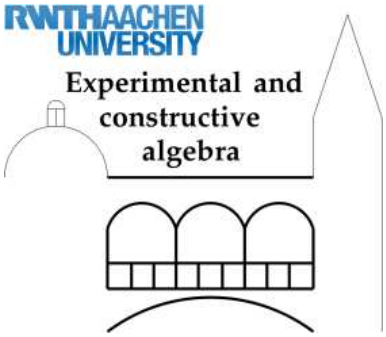
Graduiertenkolleg

Experimentelle und konstruktive Algebra



Kolloquiumsvortrag

Freitag, 18. Oktober 2013, 10:15 Uhr, Hörsaal Fo 7

Martin Kreuzer (Universität Passau):
Gröbner-Basen in der Kryptographie

Post-Quantum Kryptogrphie, ein Teilgebiet der algebraischen Kryptographie, beschäftigt sich mit der Konstruktion und der Sicherheitsanalyse von Kryptosystemen, die nicht auf zahlentheoretischen Problemen wie der Primfaktorzerlegung oder dem diskreten Logarithmus beruhen. Gröbner-Basen sind eine der wichtigsten Grundlagen der Computeralgebra. Für die Kryptographie kann man sie auf zweierlei Arten nutzbar machen: zur Konstruktion neuer Post-Quantum Kryptosysteme, deren Sicherheit auf der Schwierigkeit der Berechnung von Gröbner-Basen beruht, und für algebraische Angriffe, die Kryptosysteme mit Hilfe von polynomialen Gleichungssystemen modellieren und dann versuchen, diese mit Gröbner-Basen zu lösen.

Wir laden alle Interessierten herzlich ein.

Im Anschluss an den Vortrag gibt es Kaffee und Tee in der Bibliothek des Lehrstuhl D für Mathematik.