Berechnungsprobleme quadratischer Formen: Komplexität und Kryptographie

Dr. Rupert Hartung
Johann Wolfgang Goethe Universität Frankfurt

21.04.2008

Wir betrachten das folgende Berechnungsproblem: Gegeben zwei äquivalente quadratische Formen f und g, finde eine Matrix $T \in \mathrm{GL}_n \mathbb{Z}$, so dass $f(Tx) = g(x)$.

Für dieses Problem scheinen noch keine nichtrivialen Algorithmen zu existieren; mehr noch, das Problem scheint inhärent schwer zu sein, so dass gar keine effizienten Algorithmen existieren können.

Auf diesem Problem lassen sich neuartige kryptographische Schemata begründen. Für deren Sicherheit ist es zentral, dass dieses Problem tatsächlich nicht effizient lösbar ist.

Im Vortrag werden nun verschiedene Komplexitätsresultate zum genannten Problem und Varianten vorgestellt; insbesondere wird gezeigt: T zu finden ist mindestens so schwer, wie det f zu faktorisieren; wenn die Determinante von det f gegeben ist, dann ist es bereits in Dimension $n = 3$ NP-schwer, das kleinste T (in geeignetem Sinne) zu finden. Außerdem verliert das Problem nicht an Schwierigkeit, wenn wir die Dimension von f durch 4 beschränken.

Diese Resultate sind besonders überraschend im Vergleich mit der Kryptographie, die auf definiten Formen beruht, und versprechen deutlich kleinere Schlüssellängen und damit besonders effiziente Anwendungen.