Verbesserte Schranken für SVP-Approximation und SVP-Berechnung

Von großer Bedeutung in der Kryptographie ist das *Shortest Vector Problem* (SVP). Es besteht darin, zu gegebener Gitterbasis einen kürzesten nicht-trivialen Gittervektor zu finden. Durch Basis-Reduktionsalgorithmen kann dieser bis auf einen Faktor α approximiert werden. Es wird gezeigt, dass sich die bisherigen Schranken für α unter schwachen Annahmen im Exponenten halbieren lassen. Die verbesserten Schranken lassen sich für alle gängigen Reduktionsverfahren beweisen.
Ferner werden bessere Laufzeitschranken für SVP-Aufzählungsalgorithmen gegeben, die die bisherige Schranken um einen exponentiellen Faktor verbessern.