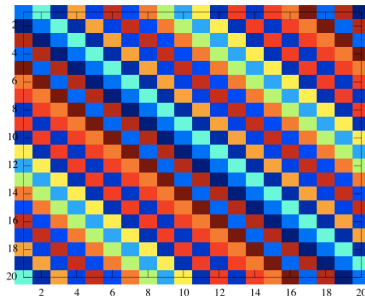


Sieving for Shortest Vectors in Ideal Lattices (work in progress)

Michael Schneider, TU Darmstadt
mischnei@cdc.informatik.tu-darmstadt.de

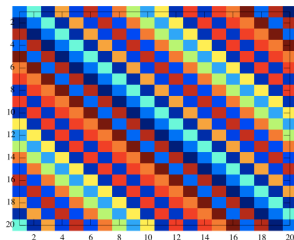


TECHNISCHE
UNIVERSITÄT
DARMSTADT

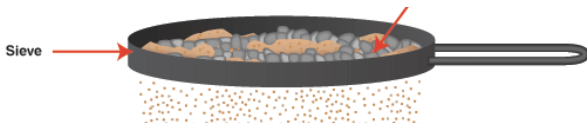


Africacrypt 2010 - Rump Session

- ▶ Lattices of special form
- ▶ Used preferably for lattice crypto
- ▶ Supposed to be as hard as regular lattices



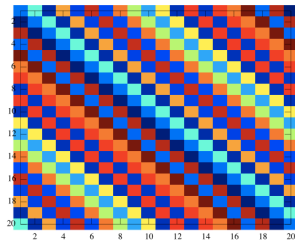
- ▶ SVP solver
- ▶ Probabilistic
- ▶ Exponential space



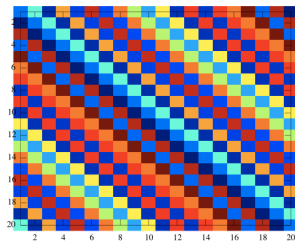
- ▶ Original version: AKS Sieve [AKS01]
- ▶ AKS Sieve without perturbations [NV08]
- ▶ List Sieve [MV10]
- ▶ Gauss Sieve [MV10]
- ▶ Ideal Sieve [this work]

Use

Use

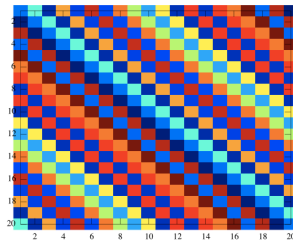


Use

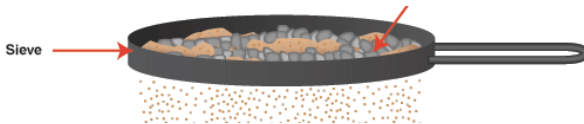


to speed up

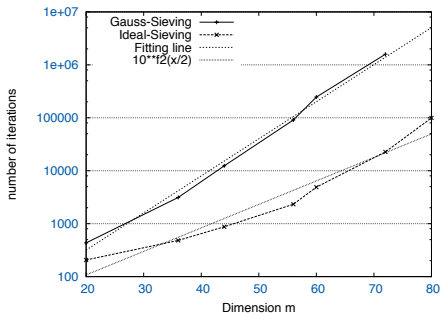
Use



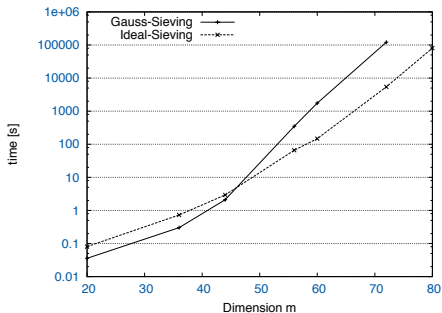
to speed up



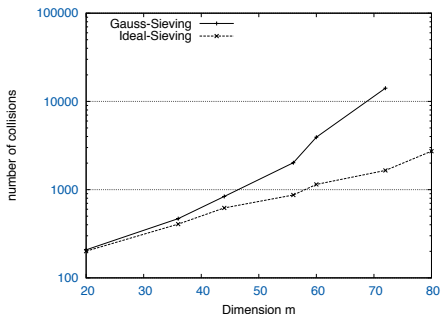
Number of Iterations



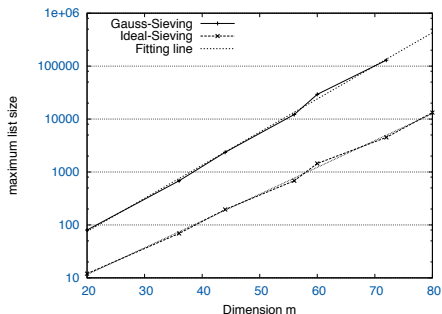
Measured Runtime



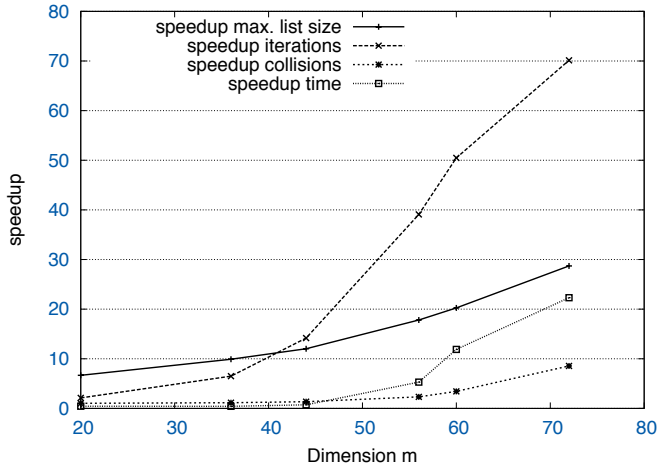
Number of Collisions



Maximum List Size



Experimental Results - Speedups





Miklos Ajtai, Ravi Kumar, and D. Sivakumar.

A sieve algorithm for the shortest lattice vector problem.
In *STOC 2001*, pages 601–610. ACM, 2001.



Daniele Micciancio and Panagiotis Voulgaris.

Faster exponential time algorithms for the shortest vector problem.
In *SODA 2010*, pages 1468–1480, 2010.



Phong Q. Nguyen and Thomas Vidick.

Sieve algorithms for the shortest vector problem are practical.
J. of Mathematical Cryptology, 2(2), 2008.