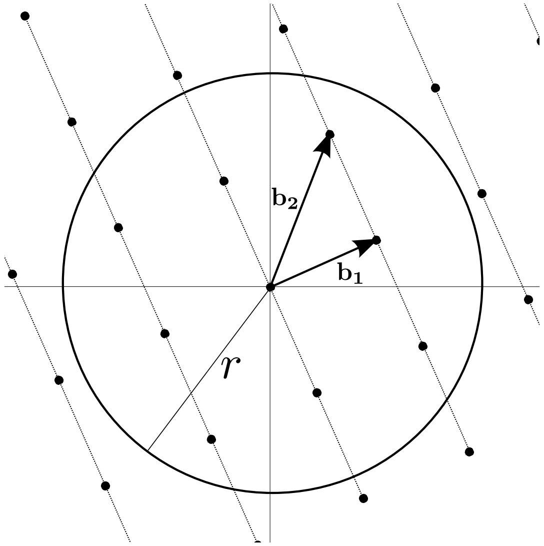
Fast Lattice Point Enumeration with Minimal Overhead

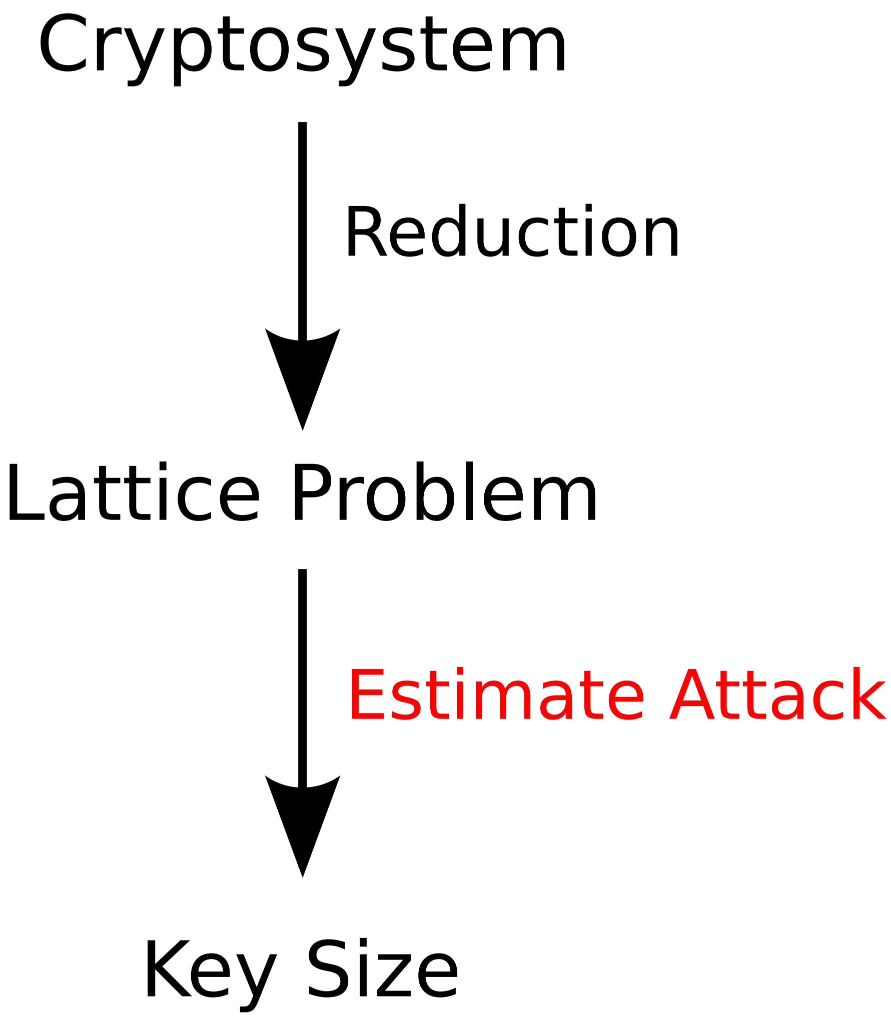


Daniele Micciancio Michael Walter

UCSD

http://eprint.iacr.org/2014/569

Shortest Vector Problem



Cryptosystem

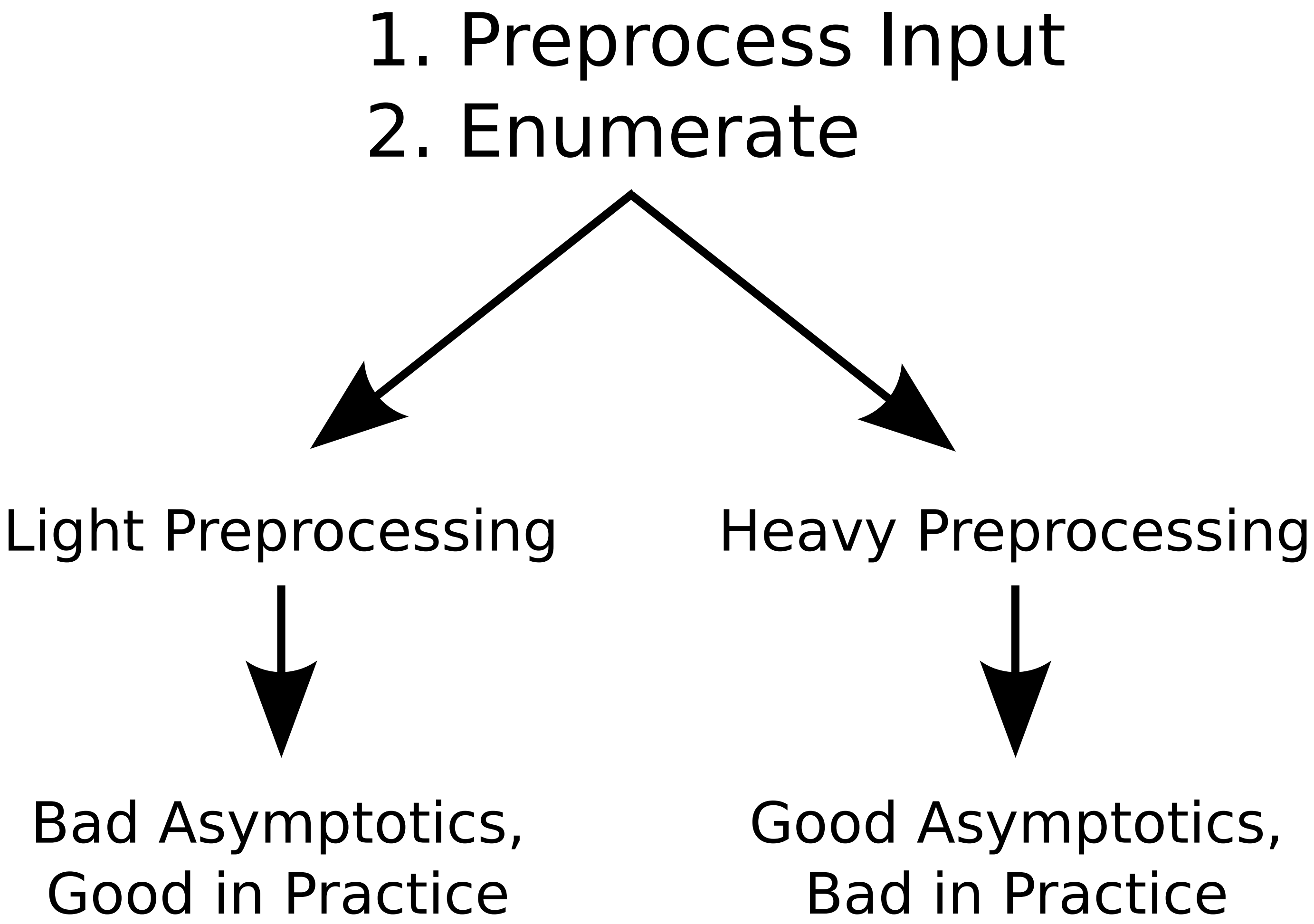
Reduction

Lattice Problem

Estimate Attack

Key Size

Enumeration Algorithms



1. Preprocess Input
2. Enumerate

Light Preprocessing

Heavy Preprocessing

Bad Asymptotics,
Good in Practice

Good Asymptotics,
Bad in Practice

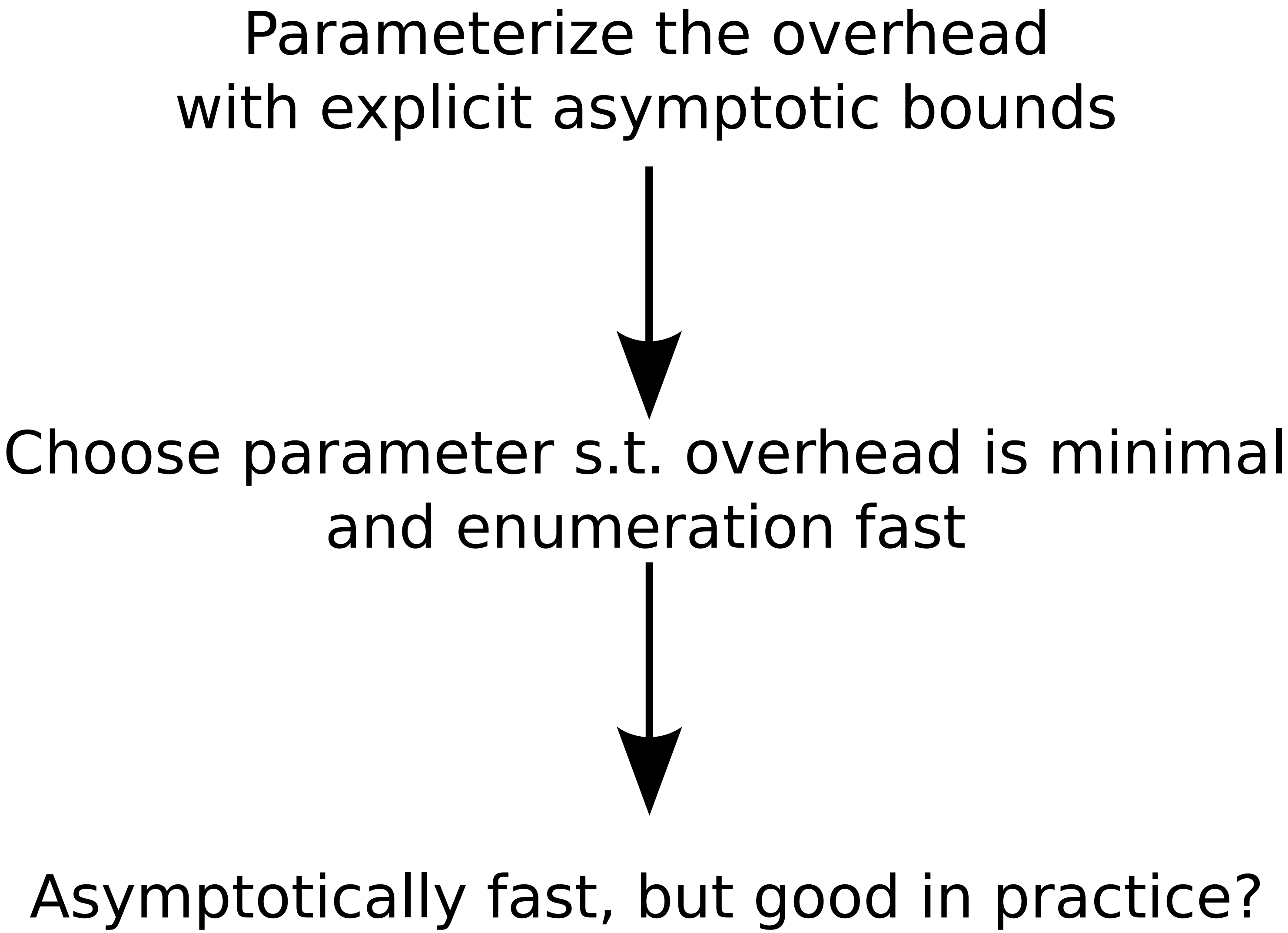
Can we have it all?

Why do we care?

1. Obtain faster algorithms in practice

2. Estimation of key sizes more meaningful

Our Contribution



Parameterize the overhead
with explicit asymptotic bounds

Choose parameter s.t. overhead is minimal
and enumeration fast

Asymptotically fast, but good in practice?

Experimental Results

Experimental Data

+ Model derived from Theoretical Analysis
+ Extrapolation

= Expect to outperform any other algorithm
in practically tractable dimensions

http://eprint.iacr.org/2014/569