Public Key Encryption from the Worst-Case Shortest Vector Problem

Chris Peikert

SRI International

CRYPTO 2008 Rump Session

Lattice-Based Cryptography

What's To Like

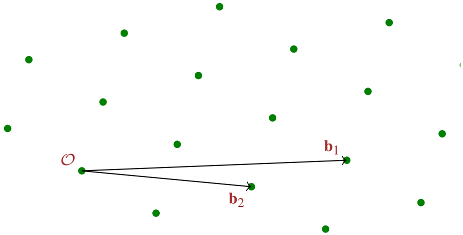
- Simple & efficient: linear ops, small integers
- Resist subexp & quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96,...]

Lattice-Based Cryptography

What's To Like

- Simple & efficient: linear ops, small integers
- Resist subexp & quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96,...]

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$

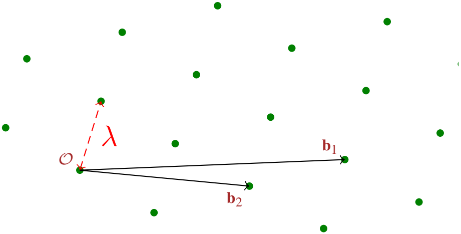


Lattice-Based Cryptography

What's To Like

- Simple & efficient: linear ops, small integers
- Resist subexp & quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96,...]

$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Shortest Vector Problem (GapSVP$_\gamma$)

- Given $\mathbf{B}$, is: $\lambda \leq 1$ or $\lambda > \gamma$?

Constructions and Assumptions

“Computational” Apps	
✔ CRHF	[Ajt96,PR06,LM06]
✔ ID schemes	[MV03,Lyu08]
✔ Signatures	[LM08,GPV08]

“Decisional” Apps	
✔ PKE	[AD97,Reg03,Reg05]
✔ CCA	[PW08]
✔ OT	[PVW08]
✔ IBE	[GPV08]

Constructions and Assumptions

“Computational” Apps

✔ CRHF	[Ajt96,PR06,LM06]
✔ ID schemes	[MV03,Lyu08]
✔ Signatures	[LM08,GPV08]

Assumption

☞ GapSVP$_\gamma$ etc. hard

“Decisional” Apps

✔ PKE	[AD97,Reg03,Reg05]
✔ CCA	[PW08]
✔ OT	[PVW08]
✔ IBE	[GPV08]

Assumptions

☞ ‘unique’-SVP$_\gamma$ hard

☞ GapSVP$_\gamma$ *quantumly* hard

Constructions and Assumptions

“Computational” Apps

✔ CRHF	[Ajt96,PR06,LM06]
✔ ID schemes	[MV03,Lyu08]
✔ Signatures	[LM08,GPV08]

Assumption

☞ GapSVP$_\gamma$ etc. hard

“Decisional” Apps

✔ PKE	[AD97,Reg03,Reg05]
✔ CCA	[PW08]
✔ OT	[PVW08]
✔ IBE	[GPV08]

Assumptions

☞ ‘unique’-SVP$_\gamma$ hard

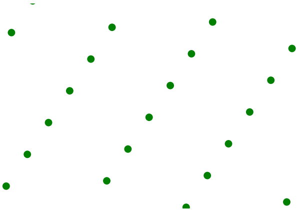
☞ GapSVP$_\gamma$ *quantumly* hard

NOW: GapSVP$_\gamma$ hard

Prior Cryptosystems [AD97,Reg03,Reg05]

Main Reduction

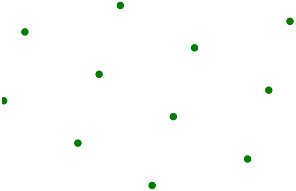
(small λ)



$\Downarrow$

Known “lumpy” dist

(large λ)



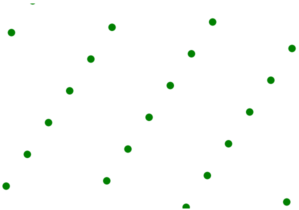
$\Downarrow$

Uniform dist

Prior Cryptosystems [AD97,Reg03,Reg05]

Main Reduction

(small λ)



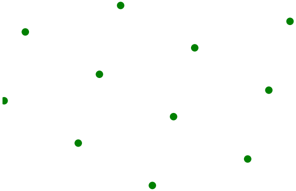
$\Downarrow$

Known “lumpy” dist

$\Downarrow$

Normal public key

(large λ)



$\Downarrow$

Uniform dist

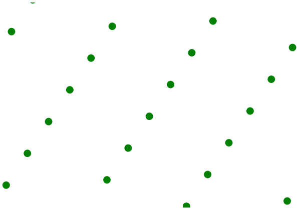
$\Downarrow$

Statistically-secure pk

Prior Cryptosystems [AD97,Reg03,Reg05]

Main Reduction

(small λ)



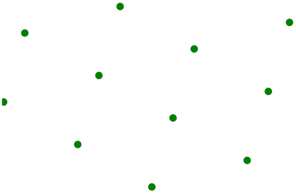
$\Downarrow$

Known “lumpy” dist

$\Downarrow$

Normal public key

(large λ)



$\Downarrow$

Uniform dist

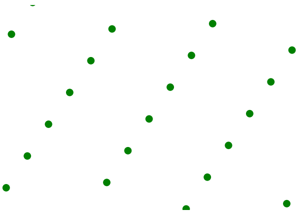
$\Downarrow$

Statistically-secure pk

BOTH dists “fully specified” – need structured input.

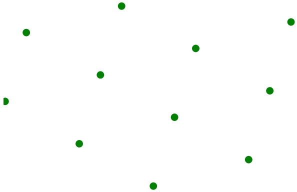
Our Cryptosystem

Main Reduction



⇓

Unknown “lumpy” dist

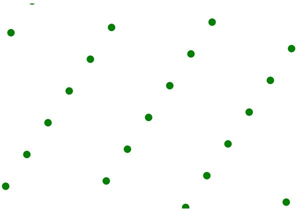


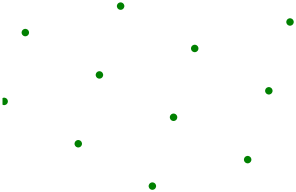
⇓

Uniform dist

Our Cryptosystem

Main Reduction





$\Downarrow$

Unknown “lumpy” dist

$\Downarrow$

$\mathcal{L}$ with small λ

$\Downarrow$

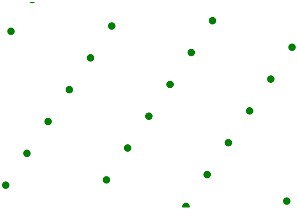
Uniform dist

$\Downarrow$

“Uniform” $\mathcal{L}$, **large** λ

Our Cryptosystem

Main Reduction



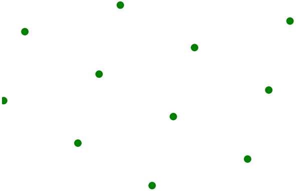
$\Downarrow$

Unknown “lumpy” dist

$\Downarrow$

$\mathcal{L}$ with small λ

Statistically-secure pk



$\Downarrow$

Uniform dist

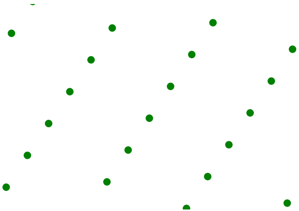
$\Downarrow$

“Uniform” $\mathcal{L}$, **large** λ

Normal public key

Our Cryptosystem

Main Reduction



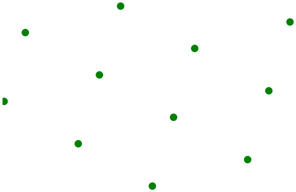
$\Downarrow$

Unknown "lumpy" dist

$\Downarrow$

$\mathcal{L}$ with small λ

Statistically-secure pk



$\Downarrow$

Uniform dist

$\Downarrow$

"Uniform" $\mathcal{L}$, **large** λ

Normal public key

sk = "good" basis for $\mathcal{L}$

Miscellaneous

- Efficiency comparable to [AD97,Reg03] – potentially improvable
- 'Dequantize' [Reg05] ?

  Efficiency and apps: PKE, CCA, OT, IBE, . . .