Nearest Planes in Practice

Christian Bischof [1], Johannes Buchmann[1], **Özgür Dagdelen**[1], Robert Fitzpatrick[2], Florian Göpfert[1], and Artur Mariano[1]

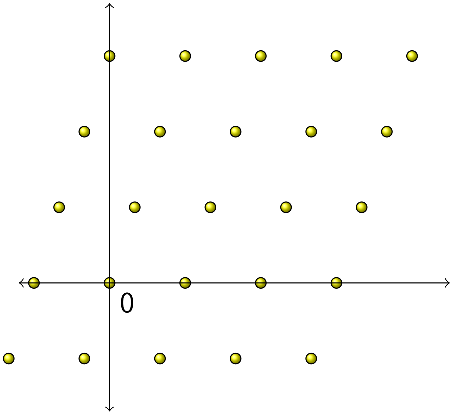
[1]Technische Universität Darmstadt

[2]Academia Sinica, Taipei

October 17th, 2014

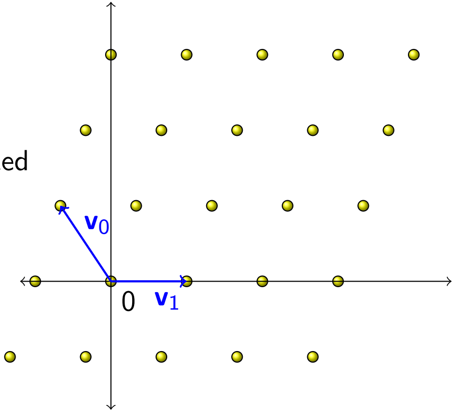
Lattices

- A lattice is a discrete additive subgroup of $\mathbb{R}^m$



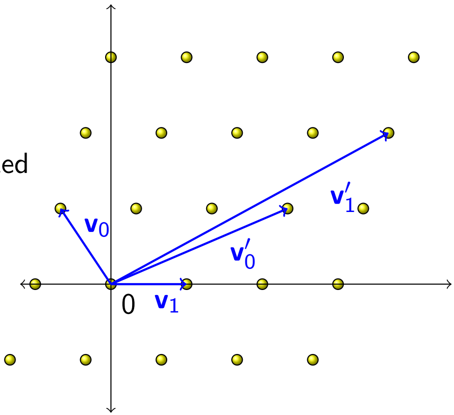
Lattices

- A lattice is a discrete additive subgroup of $\mathbb{R}^m$
- A lattice can always be represented by a basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ via $\mathbb{L} = \left\{ \sum_{i=1}^{n} \alpha_i \mathbf{v}_i \mid \alpha_i \in \mathbb{Z} \right\}$



Lattices

- A lattice is a discrete additive subgroup of $\mathbb{R}^m$
- A lattice can always be represented by a basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ via $\mathbb{L} = \left\{ \sum_{i=1}^{n} \alpha_i \mathbf{v}_i \mid \alpha_i \in \mathbb{Z} \right\}$
- The basis is not unique



Learning With Errors

- Easy problem: solving a linear equation (Gauß)

$$\mathbf{A} \cdot \mathbf{s} = \mathbf{b} \mod q$$

  - Given **A** and **b**, find **s**

Learning With Errors

- Easy problem: solving a linear equation (Gauß)

$$\mathbf{A} \cdot \mathbf{s} = \mathbf{b} \mod q$$

  - Given **A** and **b**, find **s**

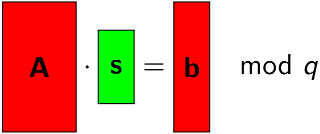
- Hard problem: solving a linear equation with noise (Regev)

$$\mathbf{A} \cdot \mathbf{s} + \mathbf{e} = \mathbf{b} \mod q$$

  - Given **A** and **b**, find **s** and / or **e**

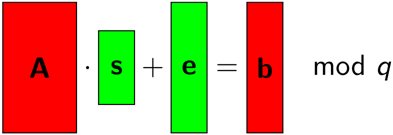
Learning With Errors

- Easy problem: solving a linear equation (Gauß)



  - Given **A** and **b**, is there an **s** satisfying $\mathbf{A}\mathbf{s} = \mathbf{b}$?

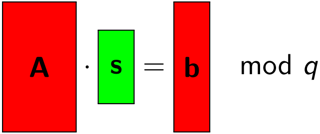
- Hard problem: solving a linear equation with noise (Regev)



  - Given **A** and **b**, is there an **s** satisfying $\mathbf{A}\mathbf{s} \approx \mathbf{b}$

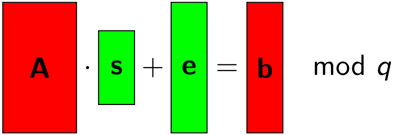
Learning With Errors

- Easy problem: solving a linear equation (Gauß)



  - Given **A** and **b**, is there an **s** satisfying **As** = **b**?

- Hard problem: solving a linear equation with noise (Regev)



  - Given **A** and **b**, is there an **s** satisfying **As** ≈ **b**

- Creating instance: **A** uniformly random in $\mathbb{Z}_q^{m \times n}$, **s**, **e** small

LWE and Lattices

LWE

Lattice

$$\mathbf{As} + \mathbf{e} = \mathbf{b} \mod q$$

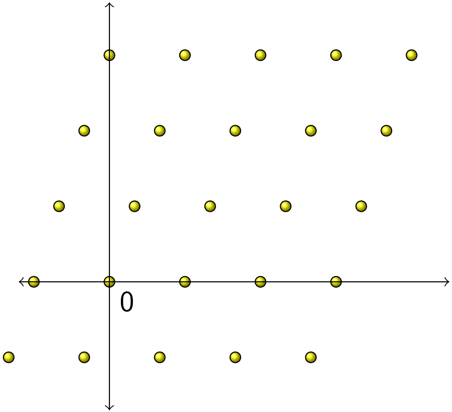
$$\mathbb{L} = \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{Ax} = \mathbf{v} \mod q \right\}$$

LWE and Lattices

LWE

$$\mathbf{As} + \mathbf{e} = \mathbf{b} \mod q$$

Lattice



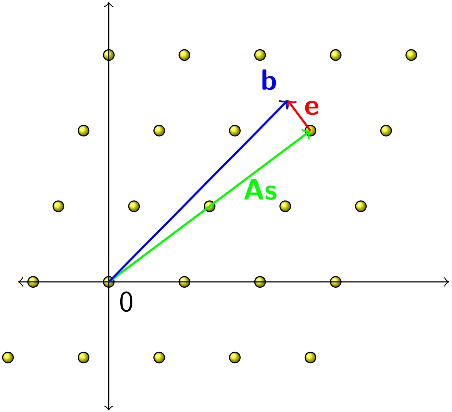
$$\mathbb{L} = \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{Ax} = \mathbf{v} \mod q \right\}$$

LWE and Lattices

LWE

$$\mathbf{As} + \mathbf{e} = \mathbf{b} \mod q$$

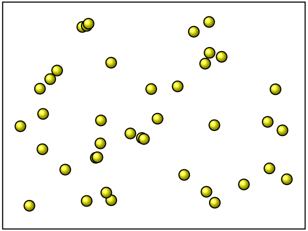
Lattice



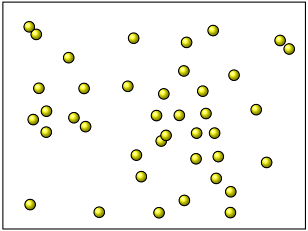
$$\mathbb{L} = \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{Ax} = \mathbf{v} \mod q \right\}$$

Average case Hardness

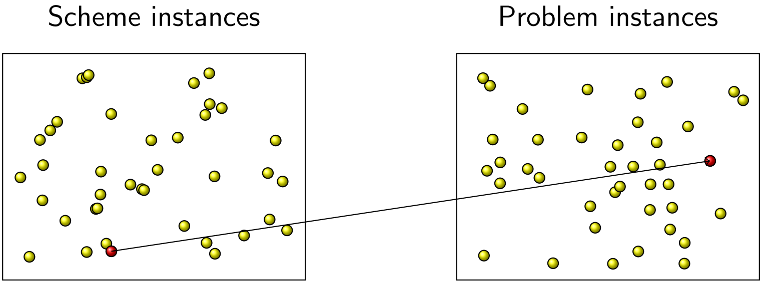
Scheme instances



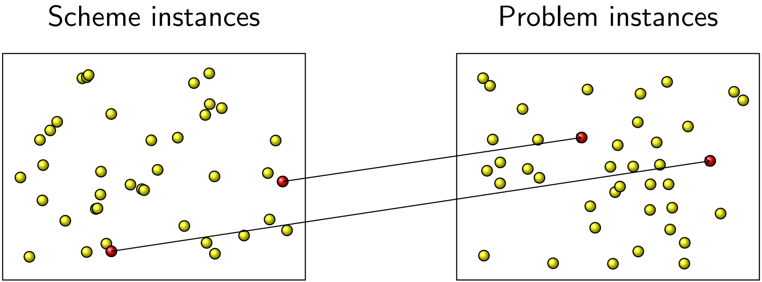
Problem instances



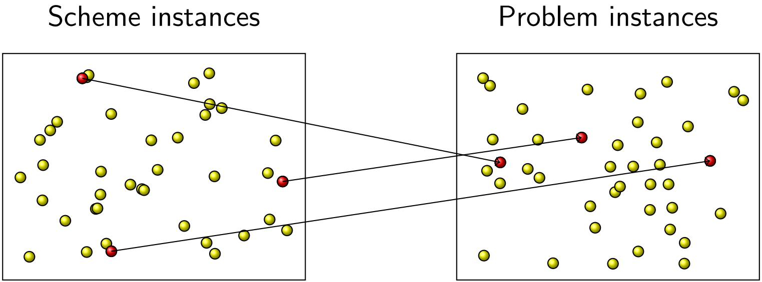
Average case Hardness



Average case Hardness

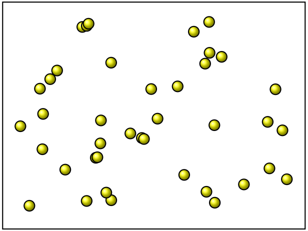


Average case Hardness

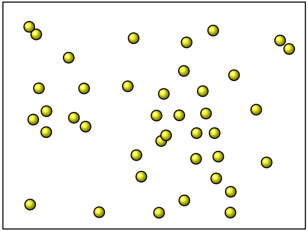


Worst case Hardness

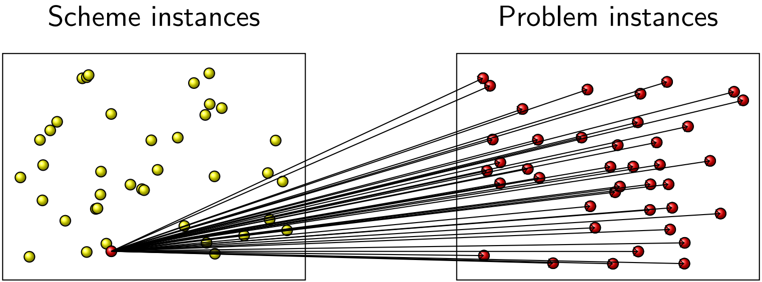
Scheme instances



Problem instances

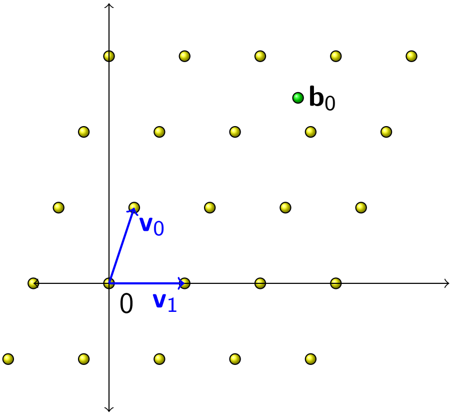


Worst case Hardness



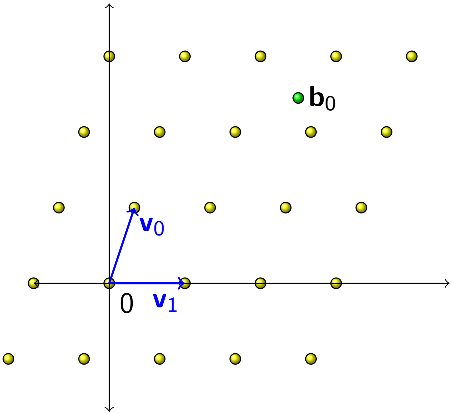
Nearest Plane

if $k < 0$ **then**
    return $\mathbf{0} \in \mathbb{Z}^m$
end if
Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$
Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$
return $\alpha \mathbf{v}_k + \text{NearestPlane}(\mathbf{t}')$



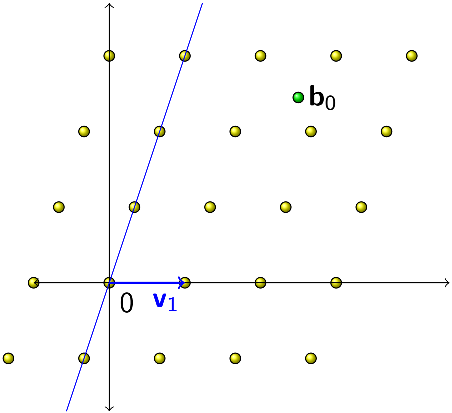
Nearest Plane

if $k < 0$ **then**
    return $\mathbf{0} \in \mathbb{Z}^m$
end if
Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\mathrm{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$
Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\mathrm{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$
return $\alpha \mathbf{v}_k + \mathrm{NearestPlane}(\mathbf{t}')$



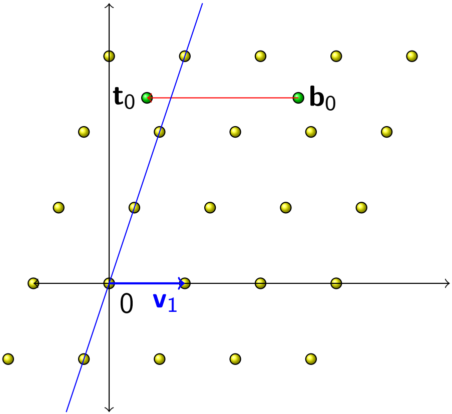
Nearest Plane

```
if k < 0 then
    return 0 ∈ Z^m
end if
Set t to be the orthogonal projection of b on span(v_0, ..., v_k)
Set t' = t − αv_k, (α ∈ Z) such that t' is as close as possible to span(v_0, ..., v_{k−1})
return αv_k + NearestPlane(t')
```



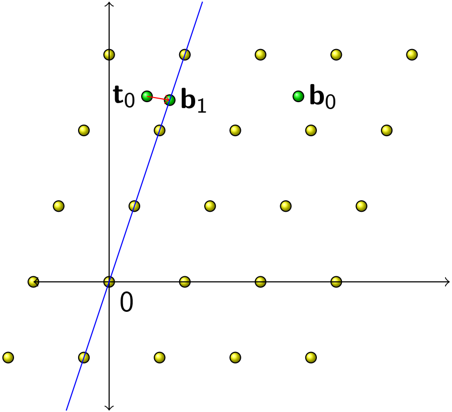
Nearest Plane

1: **if** $k < 0$ **then**
2: return $\mathbf{0} \in \mathbb{Z}^m$
3: **end if**
4: Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\mathrm{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$
5: Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\mathrm{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$
6: return $\alpha \mathbf{v}_k + \mathrm{NearestPlane}(\mathbf{t}')$



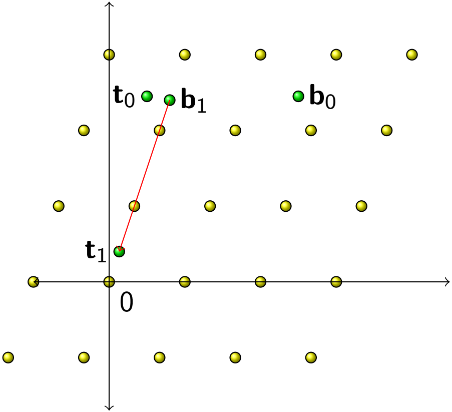
Nearest Plane

if $k < 0$ **then**
    return $\mathbf{0} \in \mathbb{Z}^m$
end if
Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$
Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$
return $\alpha \mathbf{v}_k + \text{NearestPlane}(\mathbf{t}')$



Nearest Plane

if $k < 0$ **then**
    return $\mathbf{0} \in \mathbb{Z}^m$
end if
Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$
Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$
return $\alpha \mathbf{v}_k + \text{NearestPlane}(\mathbf{t}')$



Nearest Plane

1: **if** $k < 0$ **then**

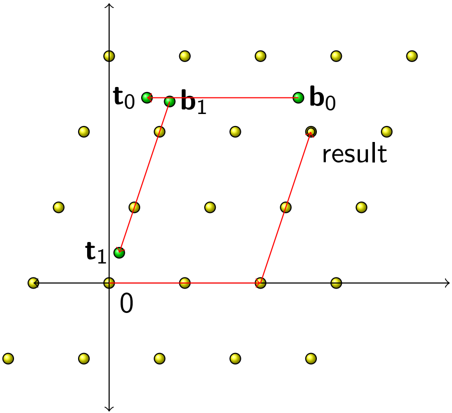
2: return $\mathbf{0} \in \mathbb{Z}^m$

3: **end if**

4: Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$

5: Set $\mathbf{t}' = \mathbf{t} - \alpha \mathbf{v}_k$, $(\alpha \in \mathbb{Z})$ such that $\mathbf{t}'$ is as close as possible to $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$

6: return $\alpha \mathbf{v}_k + \text{NearestPlane}(\mathbf{t}')$



Nearest Planes: Pseudocode

if $k < 0$ **then**

  return $\mathbf{0} \in \mathbb{Z}^m$

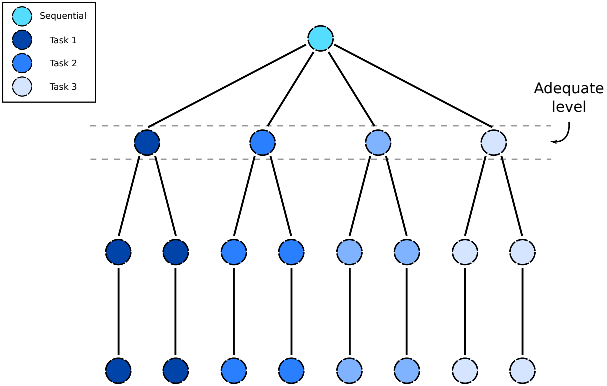
end if

Set $\mathbf{t}$ to be the orthogonal projection of $\mathbf{b}$ on $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_k)$

Set $\mathbf{t}'_i = \mathbf{t} - \alpha_i \mathbf{v}_k$, where $\alpha_i \in \mathbb{Z}$ are chosen such that $\mathbf{t}'_i$ are distinct vectors as close as possible to $\text{span}(\mathbf{v}_0, \ldots, \mathbf{v}_{k-1})$

return $\bigcup \left\{ \alpha_i \mathbf{v}_k + \text{Nearest Planes}(\mathbf{t}'_i) \right\}$

Nearest Planes: Parallelization



Result

Enumerations	2^{12}		2^{15}		2^{18}	
Threads	R	S	R	S	R	S
1	7.04	1.00	56.03	1.00	446.93	1.00
2	3.61	1.95	28.54	1.96	227.43	1.97
4	1.87	3.77	14.88	3.77	117.18	3.81
8	1.01	6.99	8.04	6.97	63.81	7.00
16	0.66	10.71	5.36	10.45	42.01	10.64

Table: Runtime in seconds (R) and speed-up (S) for parallel Nearest Planes

Conclusion

"This 2^{16} factor is somewhat arbitrary, but seems to be a reasonable estimate on the number of NearestPlanes enumerations that can be performed per second, especially with parallelism."

— Lindner and Peikert, 2011

Our Result

It is probably possible to perform more than 2^{16} operations using less than 1000 cores. New security estimations for LWE should take this into considerations.

Questions?