Fundamentals of Lattice-Based Cryptography

Chris Peikert
University of Michigan

2nd Crypto Innovation School
Shanghai, China
13 December 2019

Talk Outline

1. Lattices and hard problems
2. The SIS and LWE problems; basic applications
3. Using rings for efficiency

Today's Cryptography (e.g., RSA, Diffie-Hellman)

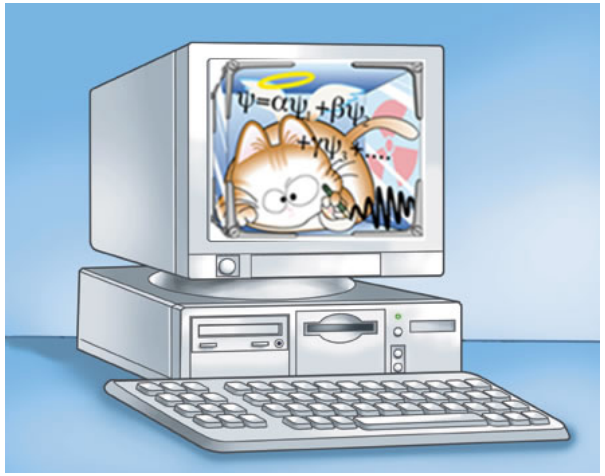
- Conjectured-hard problems: factor $N = P \cdot Q$, compute discrete logs

Today's Cryptography (e.g., RSA, Diffie-Hellman)

- Conjectured-hard problems: factor $N = P \cdot Q$, compute discrete logs
- Shor's quantum algorithm:

```
N =
21305750140972822779
67336009072353225107
58864221620325802176
55802658737520126407
22059995071405557278
96702785456335134354 7
```

$\longrightarrow$



$\longrightarrow$

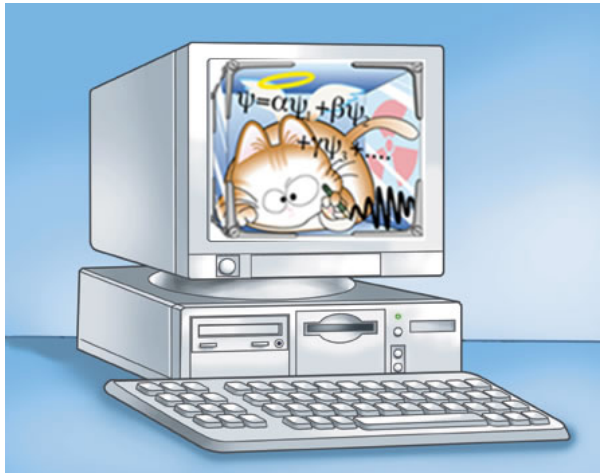
```
P =
16062216870909044065
12585584569433331615
82765877559703299166 3

Q =
13264514053200565459
67263583507984286802
75620138376808956766 9
```

Today's Cryptography (e.g., RSA, Diffie-Hellman)

- Conjectured-hard problems: factor $N = P \cdot Q$, compute discrete logs
- Shor's quantum algorithm:

```
N =
21305750140972822779
67336009072353225107
58864221620325802176
55802658737520126407
22059995071405557278
96702785456335134354 7
```

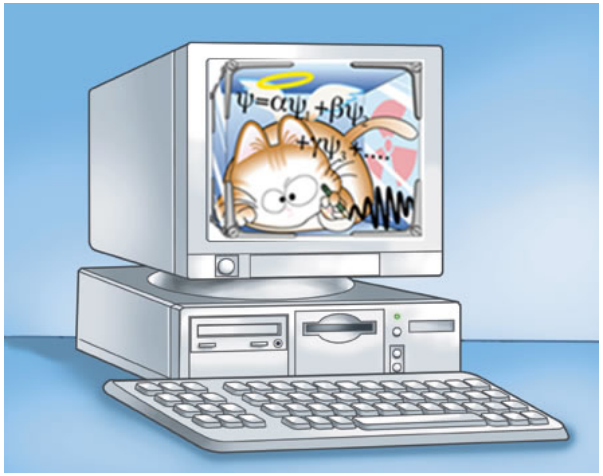
$\longrightarrow$



$\longrightarrow$

```
P =
16062216870909044065
12585584569433331615
82765877559703299166 3

Q =
13264514053200565459
67263583507984286802
75620138376808956766 9
```

$$g, y = g^X \in G \longrightarrow$$



$$\longrightarrow X$$

Lattice-Based Cryptography

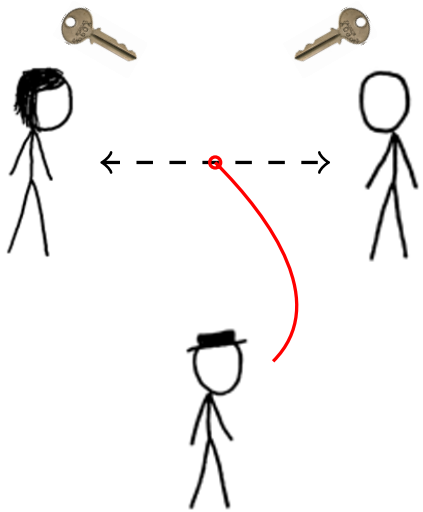
$y = g^x \bmod p$

$N = p \cdot q$

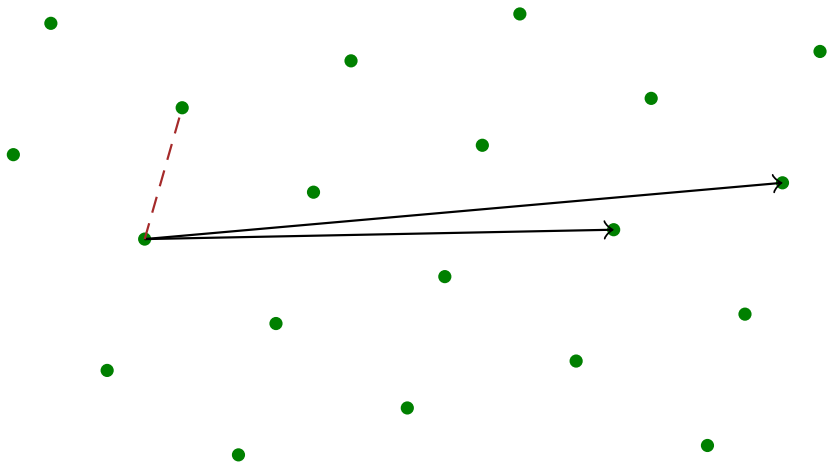
$m^e \bmod N$

$e(g^a, g^b)$

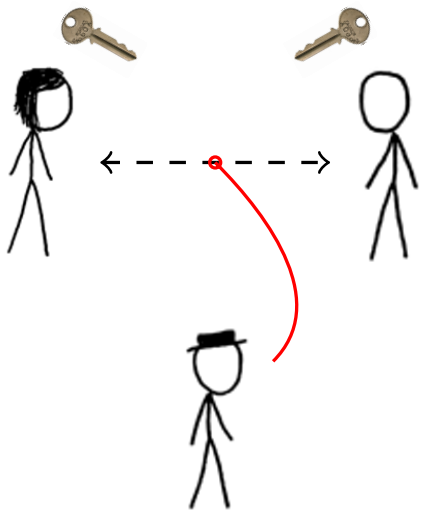
$\Longrightarrow$



Lattice-Based Cryptography

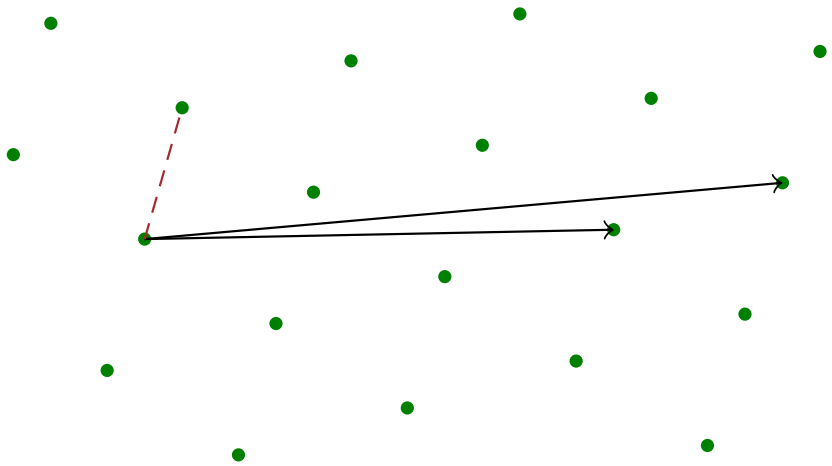


$\Longrightarrow$

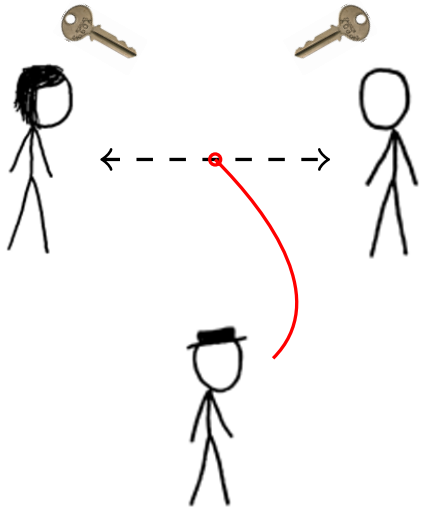


(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

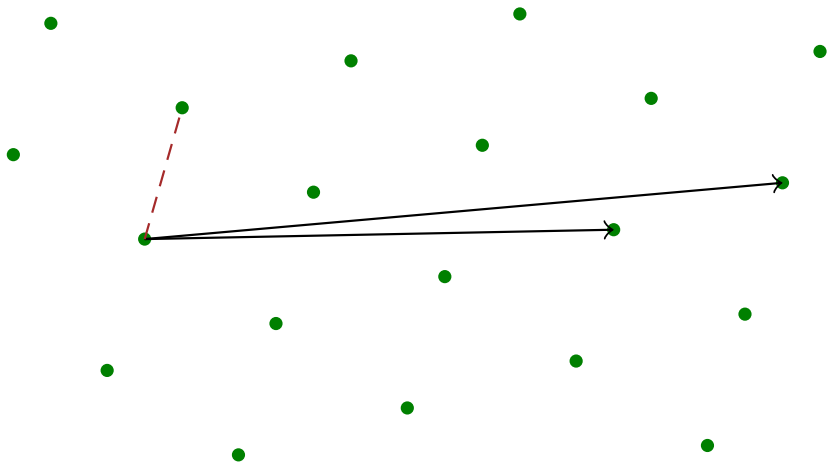


Advantages

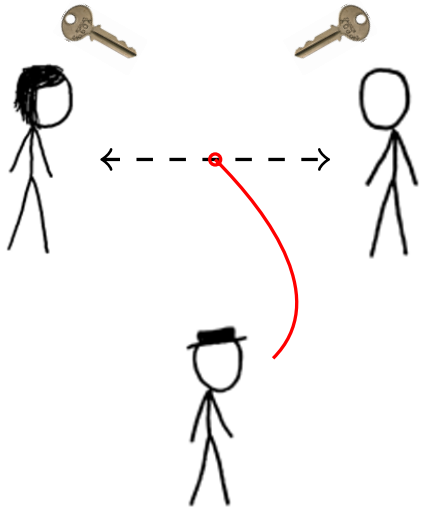
- Appears resistant to quantum attacks

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

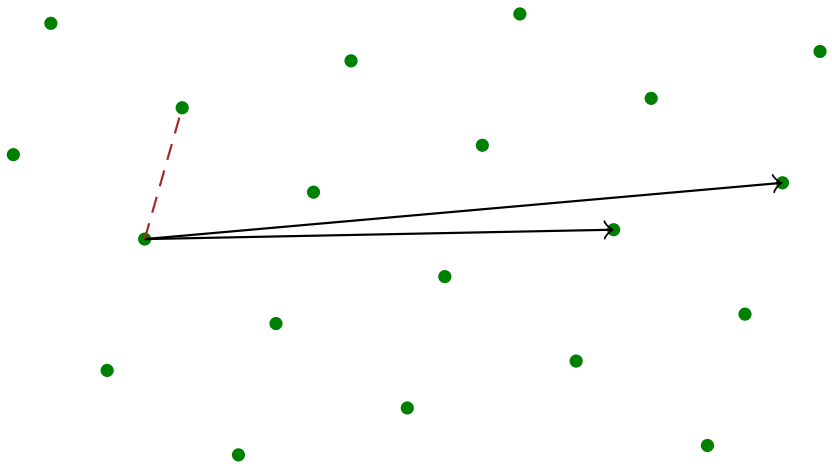


Advantages

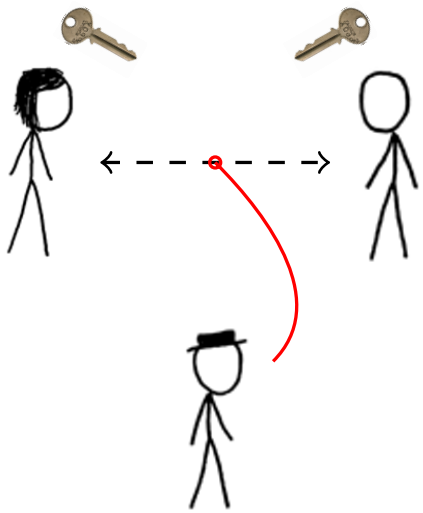
- Appears resistant to quantum attacks
- Simple description and implementation

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

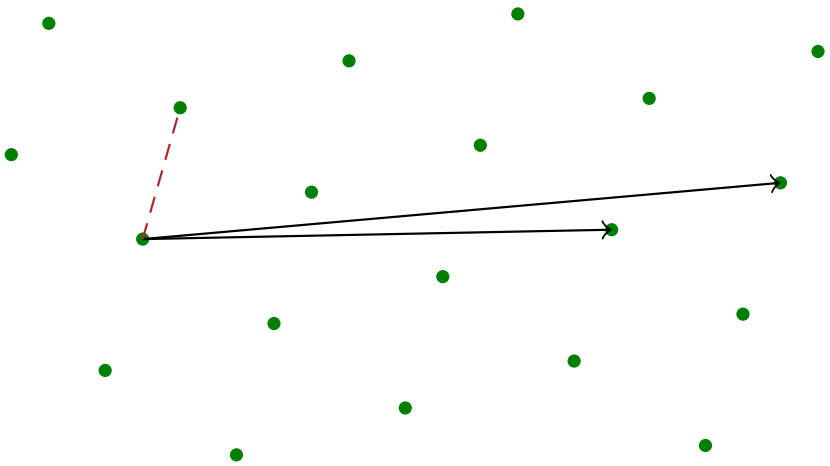


Advantages

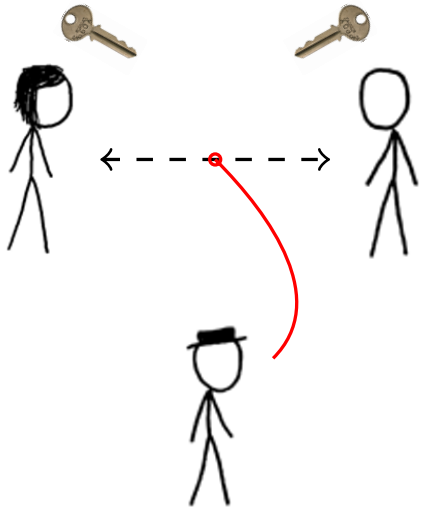
- Appears resistant to quantum attacks
- Simple description and implementation
- Efficient: linear, highly parallelizable

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$



Advantages

- Appears resistant to quantum attacks
- Simple description and implementation
- Efficient: linear, highly parallelizable
- Security from worst-case assumptions [Ajtai96,...]

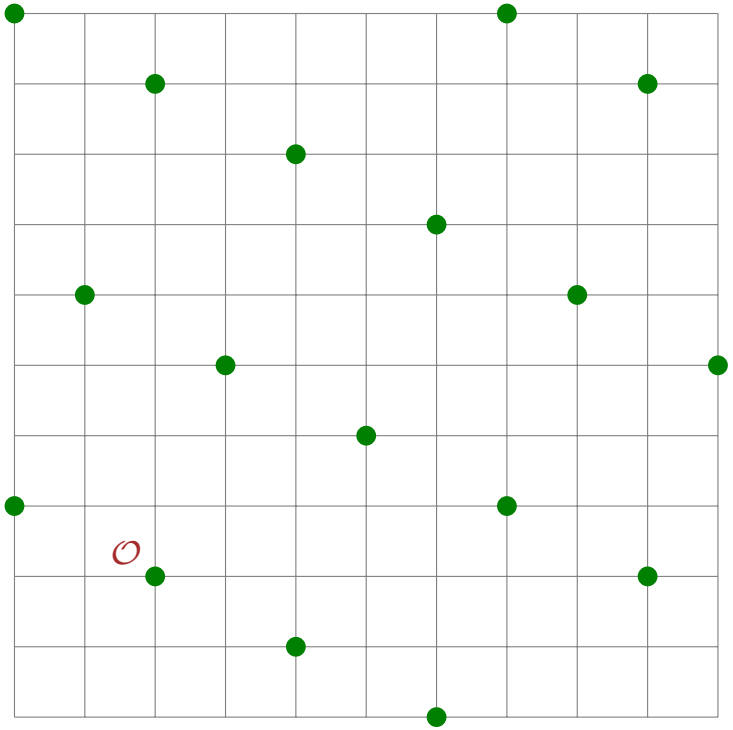
(Images courtesy xkcd.org)

Part 1:

Lattices and Hard Problems

Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")

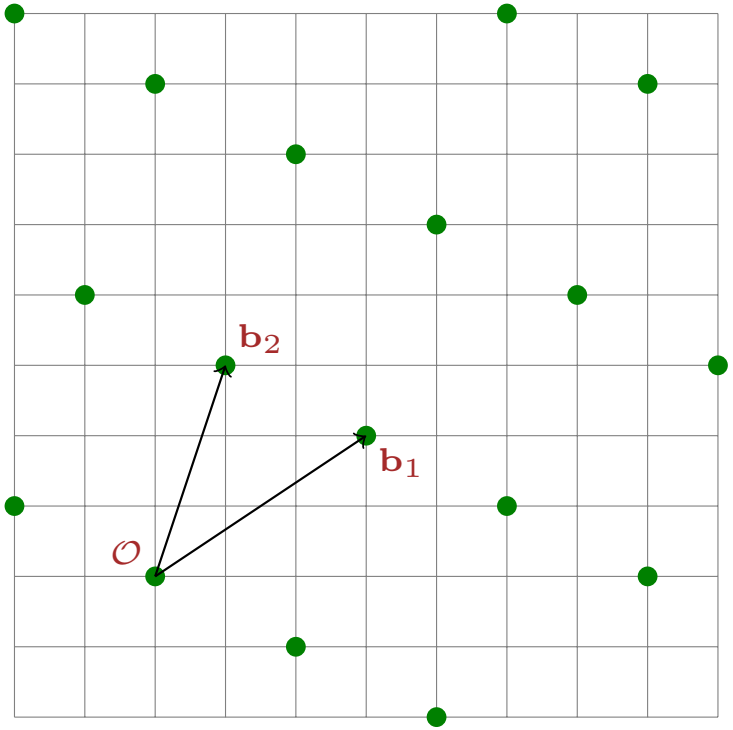


Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")
- Has a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ of linearly independent vectors:

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

Today, $k = m$ always: "full rank."

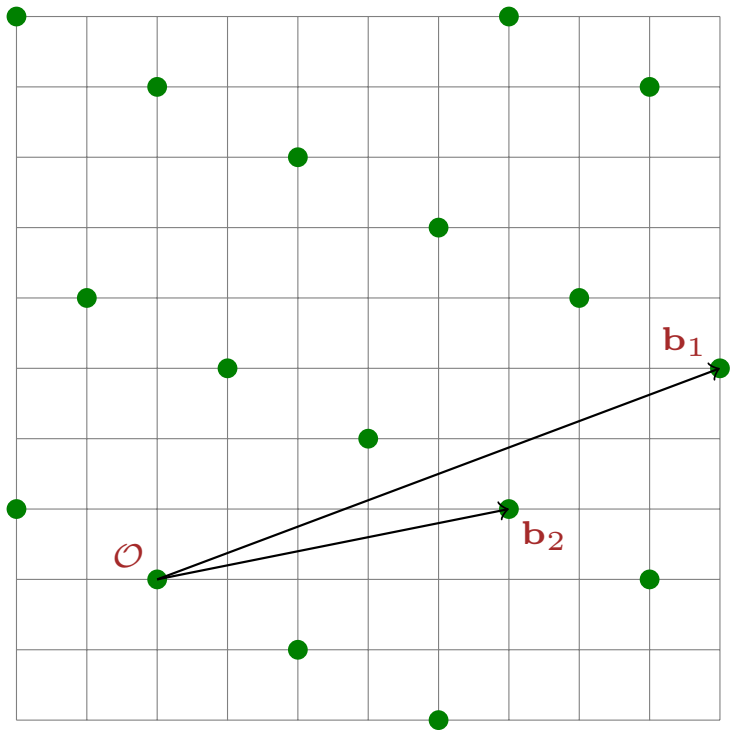


Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")
- Has a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ of linearly independent vectors:

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

Today, $k = m$ always: "full rank."



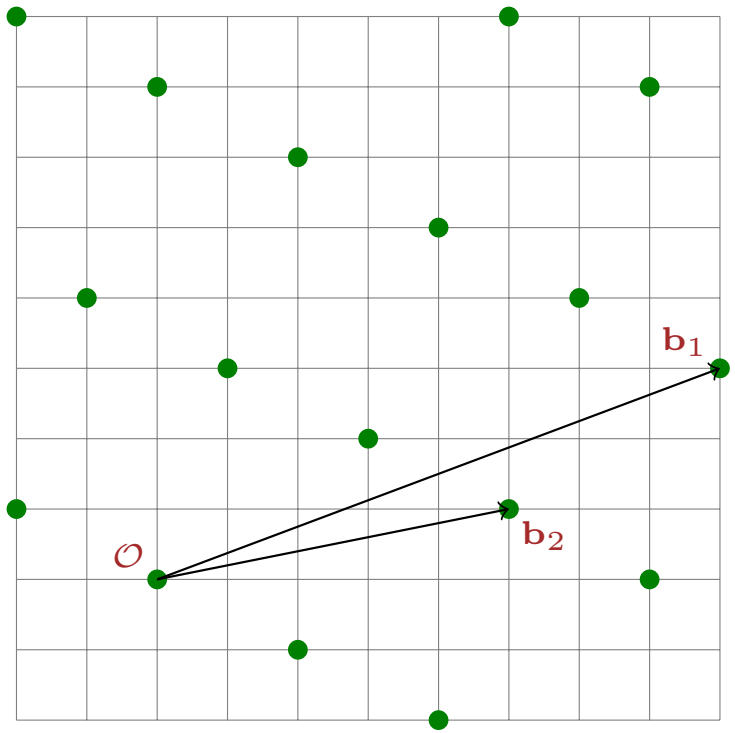
Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")
- Has a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ of linearly independent vectors:

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

Today, $k = m$ always: "full rank."

(Other representations as well...)



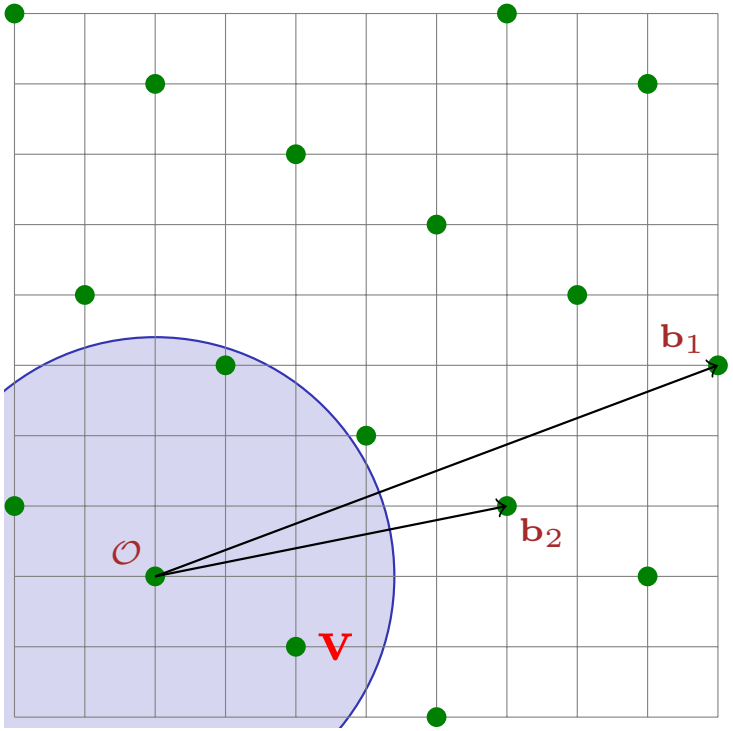
Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")
- Has a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ of linearly independent vectors:

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

Today, $k = m$ always: "full rank."

(Other representations as well...)



Conjectured Hard Problems

- Find 'relatively short' (nonzero) lattice vector(s): SVP_γ, SIVP_γ

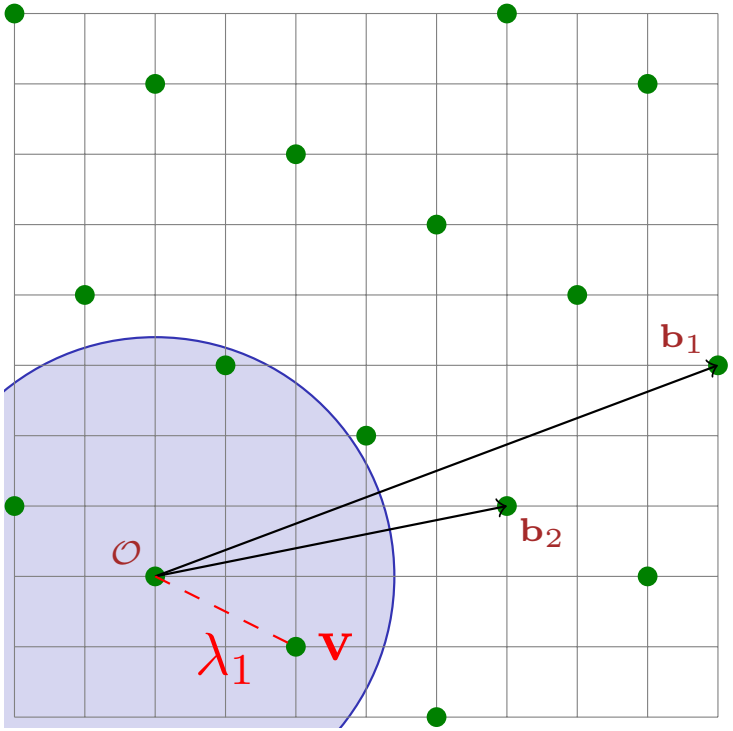
Lattices

- An (integer) lattice is a subgroup $\mathcal{L} \subseteq \mathbb{Z}^m$. (Looks like a periodic "grid.")
- Has a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ of linearly independent vectors:

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

Today, $k = m$ always: "full rank."

(Other representations as well...)



Conjectured Hard Problems

- Find 'relatively short' (nonzero) lattice vector(s): SVP_γ, SIVP_γ
- Estimate geometric quantities of the lattice: minimum distance λ_1, successive minima λ_i, covering radius μ, ...

Complexity (for the Worst Case)

GapSVP$_\gamma$

- Given (a basis of) an m-dim lattice $\mathcal{L}$ and some $d > 0$, distinguish

$$\lambda_1(\mathcal{L}) \leq d \quad \text{FROM} \quad \lambda_1(\mathcal{L}) > \gamma(m) \cdot d$$

Complexity (for the Worst Case)

GapSVP$_\gamma$

- Given (a basis of) an m-dim lattice $\mathcal{L}$ and some $d > 0$, distinguish

$$\lambda_1(\mathcal{L}) \leq d \quad \text{FROM} \quad \lambda_1(\mathcal{L}) > \gamma(m) \cdot d$$

- Becomes easier for larger $\gamma(m)$:

Complexity (for the Worst Case)

GapSVP$_\gamma$

- Given (a basis of) an m-dim lattice $\mathcal{L}$ and some $d > 0$, distinguish

$$\lambda_1(\mathcal{L}) \leq d \quad \text{FROM} \quad \lambda_1(\mathcal{L}) > \gamma(m) \cdot d$$

- Becomes easier for larger $\gamma(m)$:

$\gamma =$	$2^{(\log m)^{1-\epsilon}}$	$\sqrt{m}$	$\gtrsim m$	$2^{\sim m}$
	NP-hard*	$\in$ coNP	crypto	$\in$ P
	[Ajt98,...]	[GG98,AR05]	[Ajt96,...]	[LLL82,Sch87]

Complexity (for the Worst Case)

GapSVP$_\gamma$

- Given (a basis of) an m-dim lattice $\mathcal{L}$ and some $d > 0$, distinguish

$$\lambda_1(\mathcal{L}) \leq d \quad \text{FROM} \quad \lambda_1(\mathcal{L}) > \gamma(m) \cdot d$$

- Becomes easier for larger $\gamma(m)$:

$\gamma =$	$2^{(\log m)^{1-\epsilon}}$	$\sqrt{m}$	$\gtrsim m$	$2^{\sim m}$
	NP-hard*	$\in$ coNP	crypto	$\in$ P
	[Ajt98,...]	[GG98,AR05]	[Ajt96,...]	[LLL82,Sch87]

- For $\gamma = \text{poly}(m)$, fastest algorithm: 2^m time & space [AKS01,MV10,...]

Complexity (for the Worst Case)

GapSVP$_\gamma$

- Given (a basis of) an m-dim lattice $\mathcal{L}$ and some $d > 0$, distinguish

$$\lambda_1(\mathcal{L}) \leq d \quad \text{FROM} \quad \lambda_1(\mathcal{L}) > \gamma(m) \cdot d$$

- Becomes easier for larger $\gamma(m)$:

$\gamma =$	$2^{(\log m)^{1-\epsilon}}$	$\sqrt{m}$	$\gtrsim m$	$2^{\sim m}$
	NP-hard*	$\in$ coNP	crypto	$\in$ P
	[Ajt98,...]	[GG98,AR05]	[Ajt96,...]	[LLL82,Sch87]

- For $\gamma = \text{poly}(m)$, fastest algorithm: 2^m time & space [AKS01,MV10,...]
- Similar status for other problems like SIVP$_\gamma$, ...

Part 2:

SIS/LWE and Basic Applications

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \quad \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} \quad \cdots \quad \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \quad \in \mathbb{Z}_q^n$$

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.
- **SIS**: given many uniform $\mathbf{a}_i$, find nontrivial $z_1, \ldots, z_m \in \{0, \pm 1\}$ s.t.

$$z_1 \cdot \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + z_2 \cdot \begin{pmatrix} | \\ \mathbf{a}_2 \\ | \end{pmatrix} + \cdots + z_m \cdot \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ 0 \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.
- <u>**SIS**</u>: given many uniform $\mathbf{a}_i$, find 'short' nonzero $\mathbf{z}$ s.t.

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.
- <u>**SIS**</u>: given many uniform $\mathbf{a}_i$, find 'short' nonzero $\mathbf{z}$ s.t.

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Collision-Resistant Hash Function

- Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ for any $m > n \lg q$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.
- <u>**SIS**</u>: given many uniform $\mathbf{a}_i$, find 'short' nonzero $\mathbf{z}$ s.t.

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Collision-Resistant Hash Function

- Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ for any $m > n \lg q$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

A Hard Problem: Short Integer Solution [Ajtai'96]

- Fix a dimension n and modulus q (e.g., $q \approx n^2$).
  Let $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q.
- **SIS**: given many uniform $\mathbf{a}_i$, find 'short' nonzero $\mathbf{z}$ s.t.

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

Collision-Resistant Hash Function

- Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ for any $m > n \lg q$ as

$$f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}.$$

- Collision $\mathbf{x}, \mathbf{x}' \in \{0,1\}^m$ where $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}'$ ...

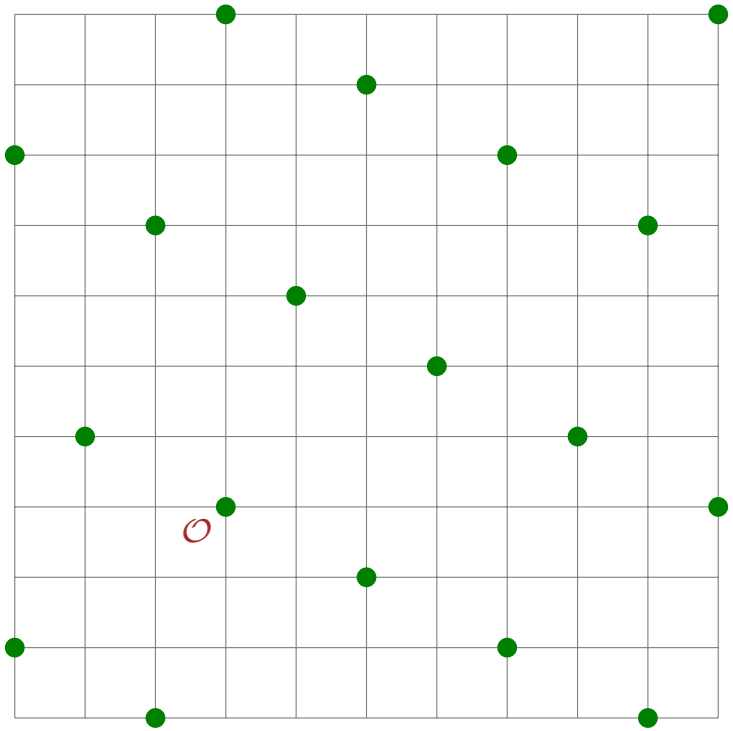
  ...yields a short (nonzero) solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

Cool! (but what does this have to do with lattices?)

Cool!

- Matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$:

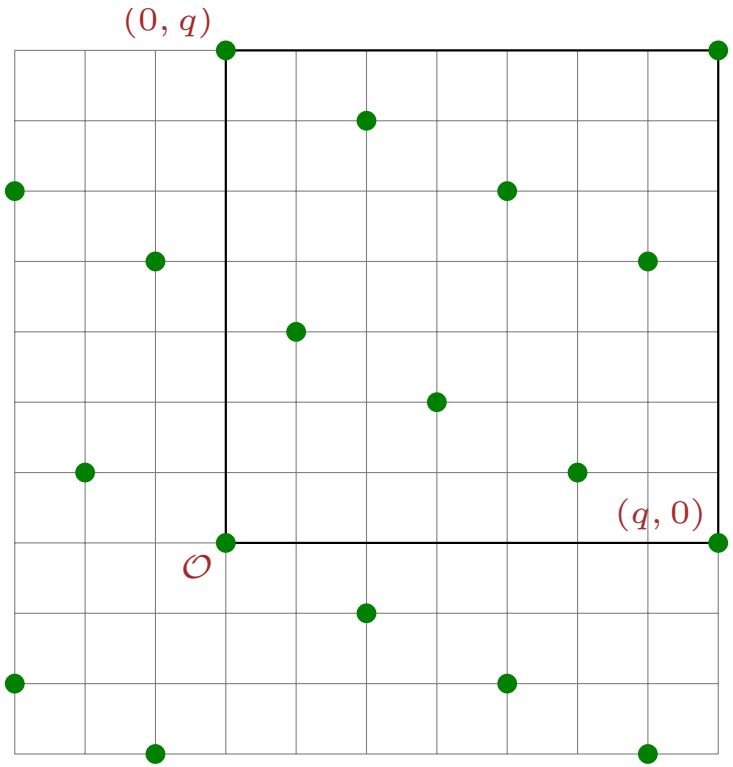
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$



Cool!

- Matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$:

$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$

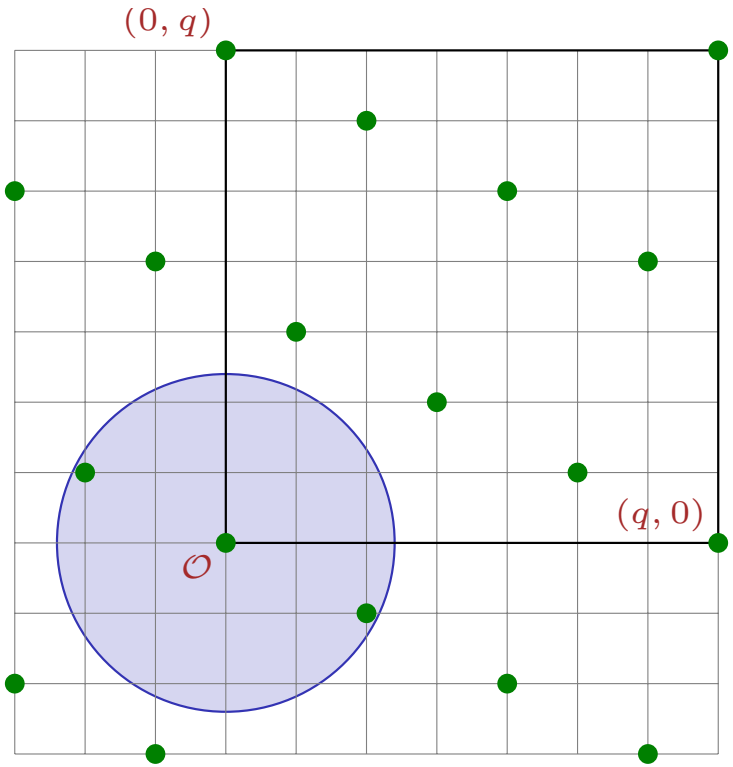


Cool!

- Matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$:

$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$

- 'Short' solutions $\mathbf{z}$ lie in 

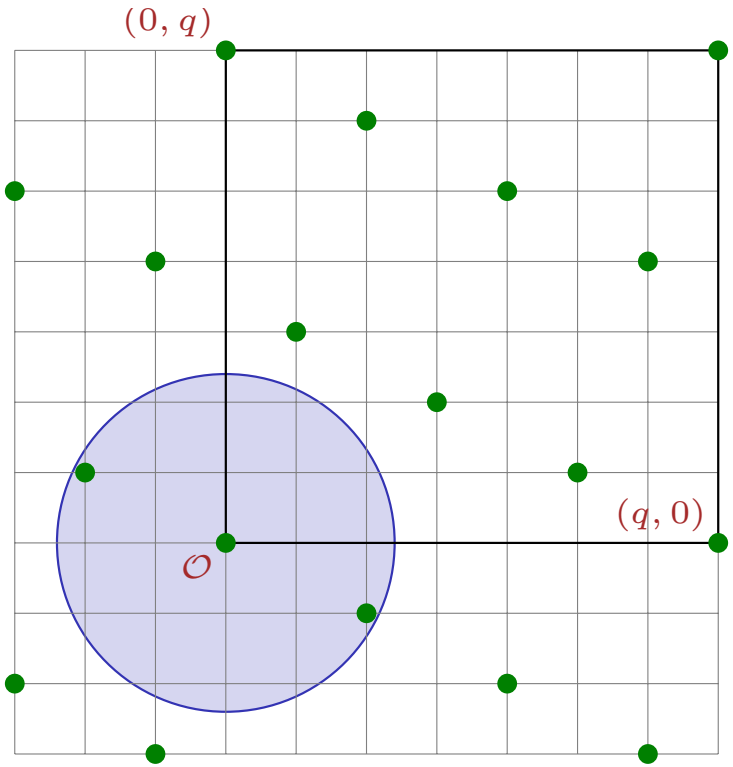


Cool!

- Matrix $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$:

$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$

- 'Short' solutions $\mathbf{z}$ lie in 



Worst-Case/Average-Case Connection [Ajtai96,...]

Finding 'short' ($\|\mathbf{z}\| \leq \beta \ll q$) nonzero $\mathbf{z} \in \mathcal{L}^{\perp}(\mathbf{A})$

(for uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$)

$$\Downarrow$$

solving GapSVP$_{\beta\sqrt{n}}$ and SIVP$_{\beta\sqrt{n}}$ on any n-dim lattice

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

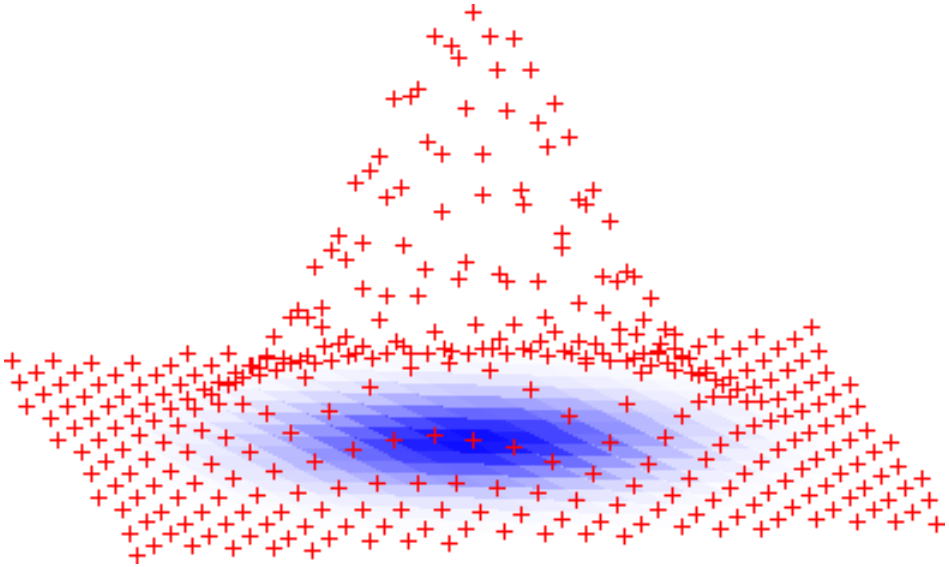
- Generate uniform $vk = \mathbf{A}$ with 'trapdoor' $sk = \mathbf{T}$. [Ajtai'99,...,MP'12]

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

- Generate uniform $vk = \mathbf{A}$ with 'trapdoor' $sk = \mathbf{T}$. [Ajtai'99,...,MP'12]
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{x} = H(\mu) \in \mathbb{Z}_q^n$.

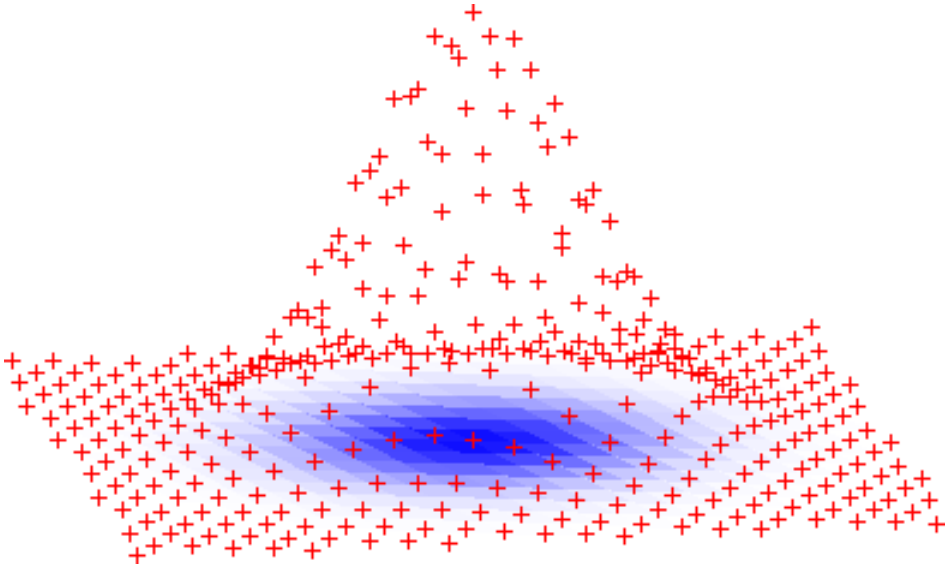
Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

- Generate uniform $vk = \mathbf{A}$ with 'trapdoor' $sk = \mathbf{T}$. [Ajtai'99,...,MP'12]
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{x} = H(\mu) \in \mathbb{Z}_q^n$. Draw $\mathbf{x}$ from a (Gaussian) distribution, which reveals nothing about $\mathbf{T}$:



Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

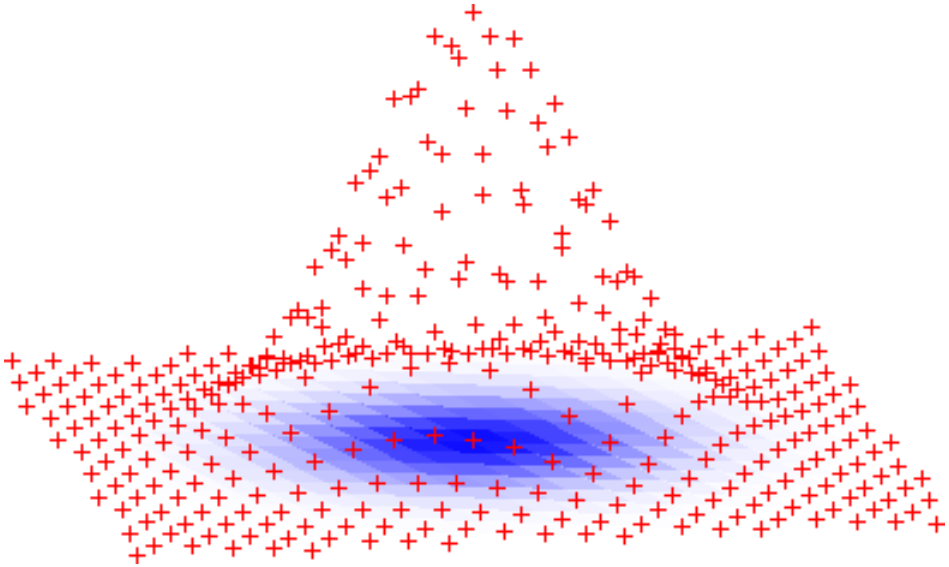
- Generate uniform $vk = \mathbf{A}$ with 'trapdoor' $sk = \mathbf{T}$. [Ajtai'99,...,MP'12]
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{x} = H(\mu) \in \mathbb{Z}_q^n$. Draw $\mathbf{x}$ from a (Gaussian) distribution, which reveals nothing about $\mathbf{T}$:



- Verify$(\mathbf{A}, \mu, \mathbf{x})$: check that $\mathbf{A}\mathbf{x} = H(\mu)$ and $\mathbf{x}$ is sufficiently short.

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

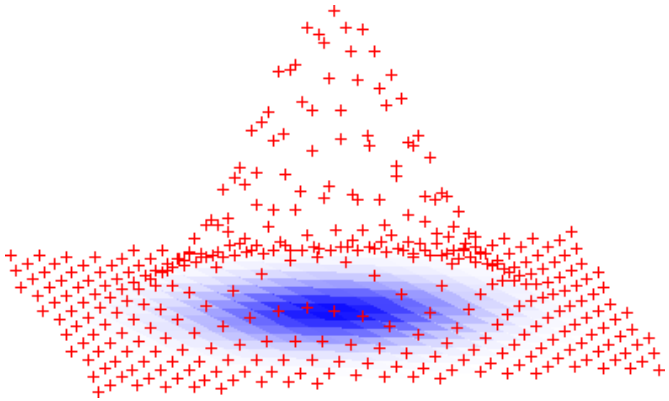
- Generate uniform $vk = \mathbf{A}$ with 'trapdoor' $sk = \mathbf{T}$. [Ajtai'99,...,MP'12]
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{x} = H(\mu) \in \mathbb{Z}_q^n$. Draw $\mathbf{x}$ from a (Gaussian) distribution, which reveals nothing about $\mathbf{T}$:



- Verify$(\mathbf{A}, \mu, \mathbf{x})$: check that $\mathbf{A}\mathbf{x} = H(\mu)$ and $\mathbf{x}$ is sufficiently short.
- <u>Security</u>: forging a signature for a new message μ^* requires finding a short $\mathbf{x}^*$ s.t. $\mathbf{A}\mathbf{x}^* = H(\mu^*)$. This is SIS!

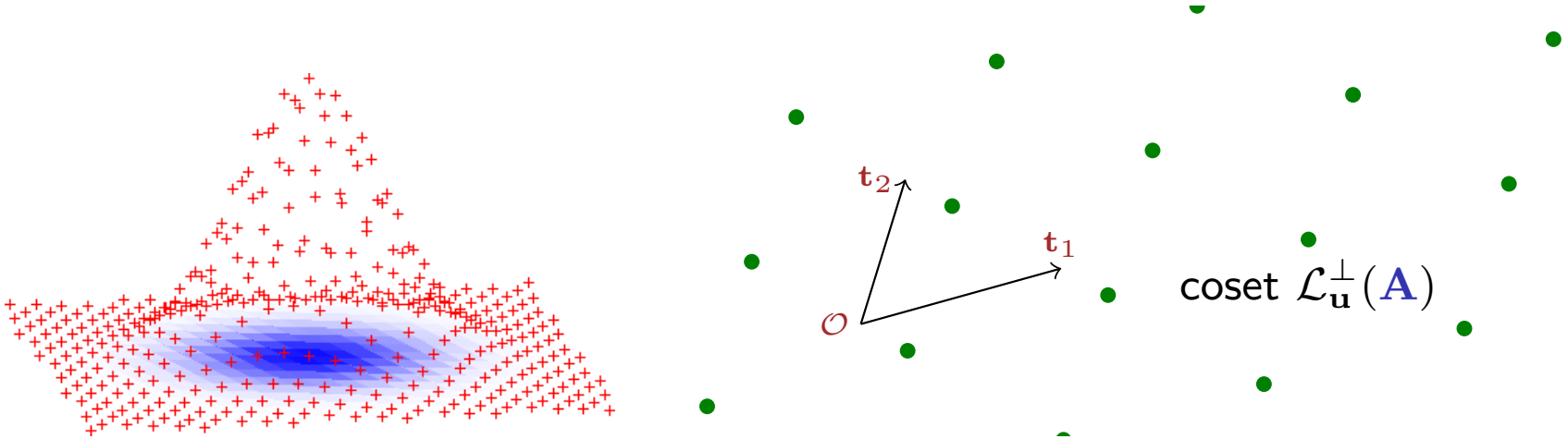
Gaussian Sampling over a (Shifted) Lattice

- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!



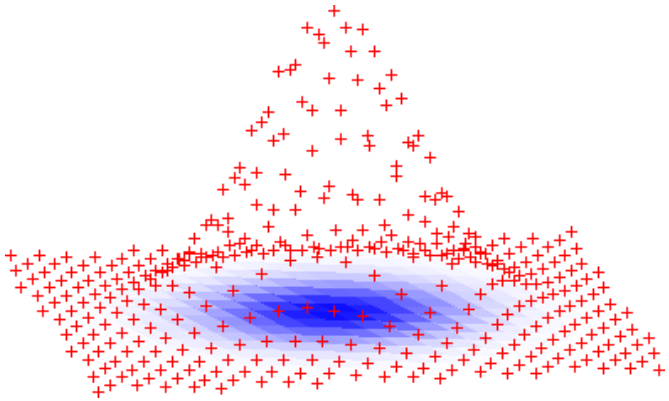
Gaussian Sampling over a (Shifted) Lattice

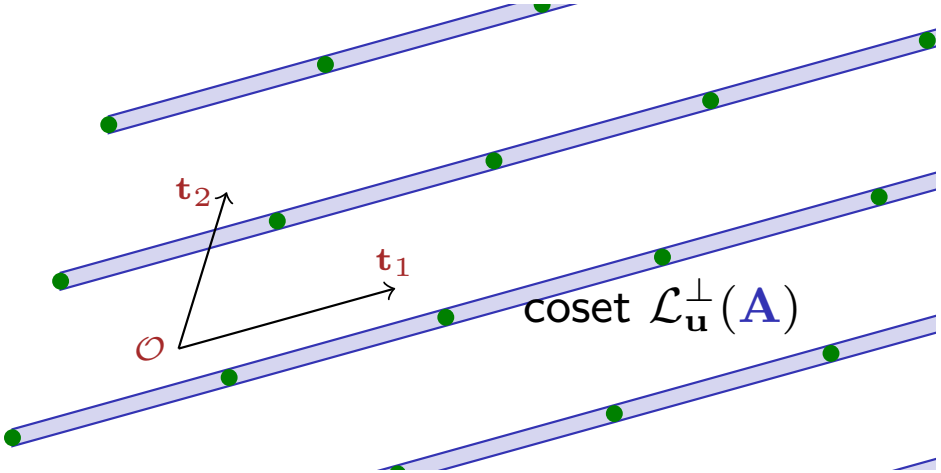
- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!
- "Nearest-plane" algorithm with randomized rounding [Klein'00,GPV'08]



Gaussian Sampling over a (Shifted) Lattice

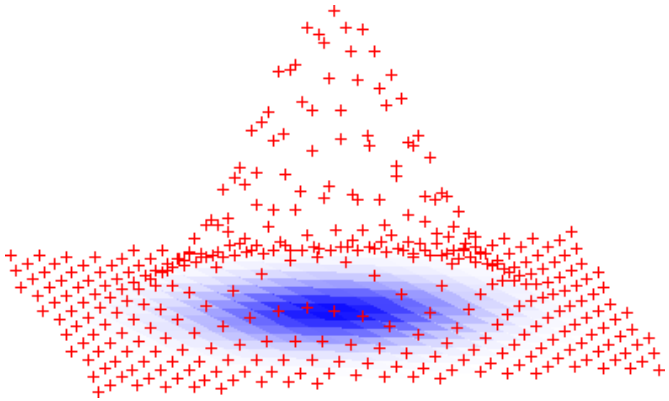
- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!
- "Nearest-plane" algorithm with randomized rounding [Klein'00,GPV'08]

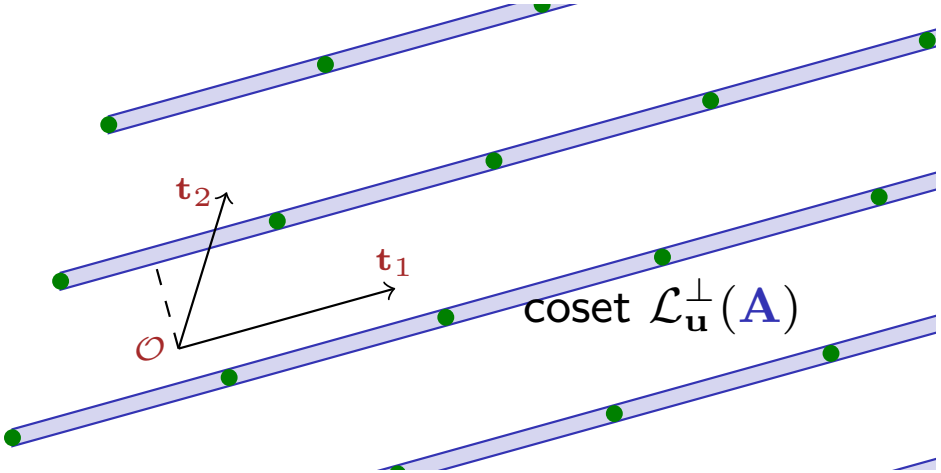




Gaussian Sampling over a (Shifted) Lattice

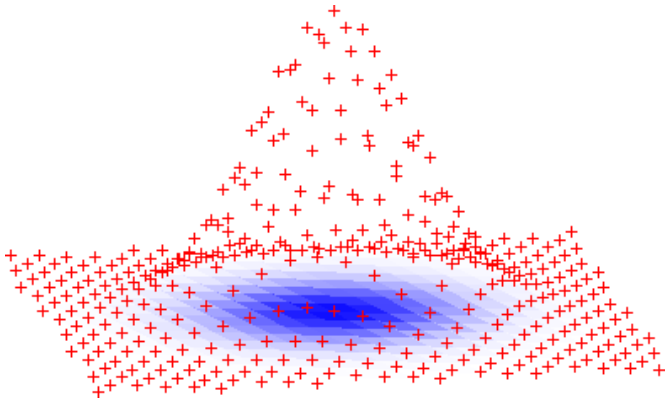
- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!
- "Nearest-plane" algorithm with randomized rounding [Klein'00,GPV'08]

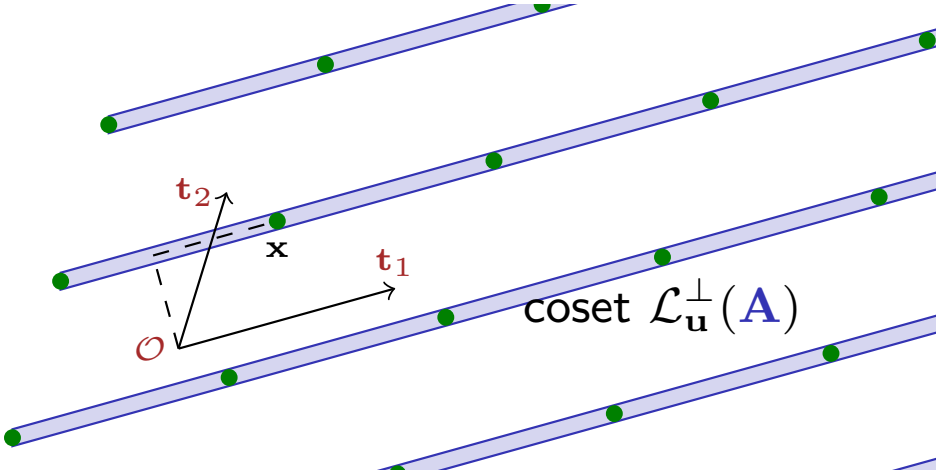




Gaussian Sampling over a (Shifted) Lattice

- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!
- "Nearest-plane" algorithm with randomized rounding [Klein'00,GPV'08]

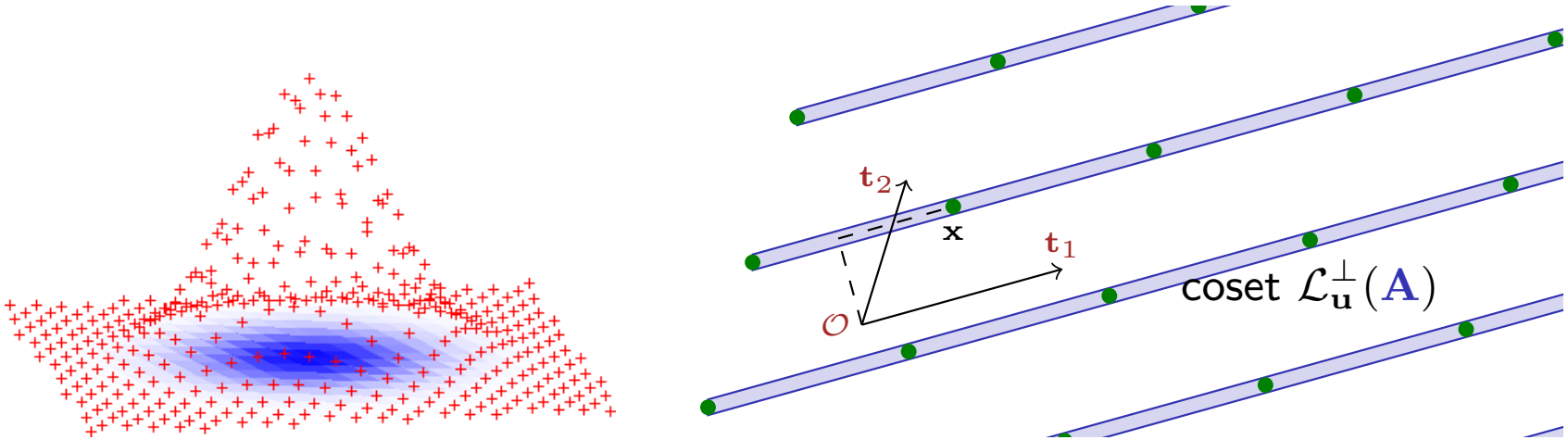




Gaussian Sampling over a (Shifted) Lattice

- Sample $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$ given any 'short' basis $\mathbf{T}$: $\max\|\mathbf{t}_i\| \leq$ std dev
  - ⋆ Output distribution leaks no information about secret basis $\mathbf{T}$!

- "Nearest-plane" algorithm with randomized rounding [Klein'00,GPV'08]



- Proof idea: $D_{\mathcal{L}_{\mathbf{u}}^{\perp}}(\text{plane})$ depends (essentially) only on $\mathrm{dist}(\mathcal{O}, \text{plane})$; not affected by shift within plane. So rounding with that probability produces that distribution.

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ

Another Hard Problem: Learning With Errors [Regev'05]

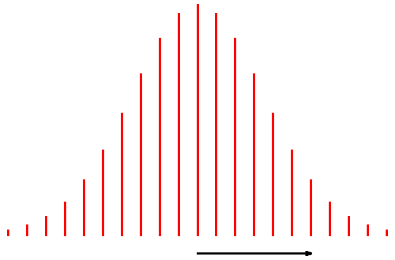
- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{aligned} \mathbf{a}_1 \leftarrow \mathbb{Z}_q^n \quad &, \quad b_1 \approx \langle \mathbf{s}\ ,\ \mathbf{a}_1 \rangle \bmod q \\ \mathbf{a}_2 \leftarrow \mathbb{Z}_q^n \quad &, \quad b_2 \approx \langle \mathbf{s}\ ,\ \mathbf{a}_2 \rangle \bmod q \\ &\vdots \end{aligned}$$

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\mathbf{a}_1 \leftarrow \mathbb{Z}_q^n \quad , \quad b_1 = \langle \mathbf{s} \, , \, \mathbf{a}_1 \rangle + e_1 \in \mathbb{Z}_q$$
$$\mathbf{a}_2 \leftarrow \mathbb{Z}_q^n \quad , \quad b_2 = \langle \mathbf{s} \, , \, \mathbf{a}_2 \rangle + e_2 \in \mathbb{Z}_q$$
$$\vdots$$

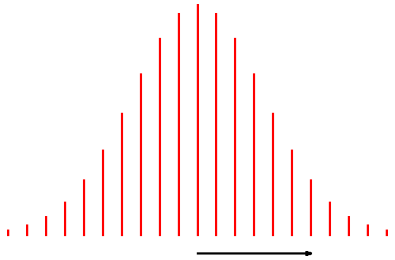


$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad \begin{pmatrix} \cdots & \mathbf{b}^t & \cdots \end{pmatrix} \approx \mathbf{s}^t \mathbf{A}$$

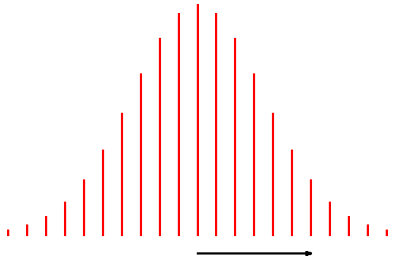


$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad \begin{pmatrix} \cdots & \mathbf{b}^t & \cdots \end{pmatrix} \approx \mathbf{s}^t \mathbf{A}$$



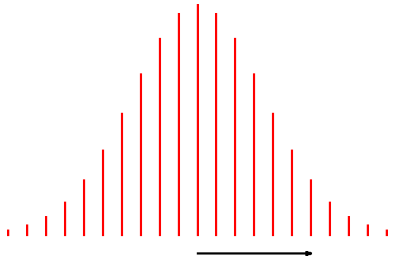
$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

- **Decision:** distinguish $(\mathbf{A}\ ,\ \mathbf{b})$ from <u>uniform</u> $(\mathbf{A}\ ,\ \mathbf{b})$

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad \begin{pmatrix} \cdots & \mathbf{b}^t & \cdots \end{pmatrix} \approx \mathbf{s}^t \mathbf{A}$$



$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

- **Decision:** distinguish $(\mathbf{A}\ ,\ \mathbf{b})$ from <u>uniform</u> $(\mathbf{A}\ ,\ \mathbf{b})$

LWE is Hard

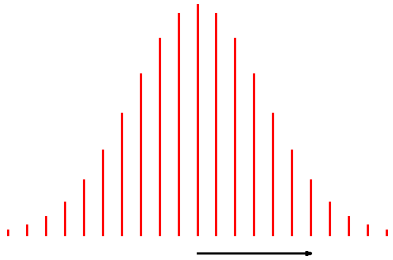
(n/α)-approx *worst case* GapSVP, SIVP $\leq$ search-LWE $\leq$ decision-LWE $\leq$ crypto

(quantum [R'05]) [BFKL'93,R'05,...]

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad \begin{pmatrix} \cdots & \mathbf{b}^t & \cdots \end{pmatrix} \approx \mathbf{s}^t \mathbf{A}$$



$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

- **Decision:** distinguish $(\mathbf{A}\ ,\ \mathbf{b})$ from <u>uniform</u> $(\mathbf{A}\ ,\ \mathbf{b})$

LWE is Hard

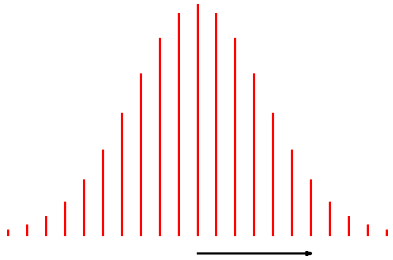
(n/α)-approx *worst case* GapSVP, SIVP $\underset{\text{(quantum [R'05])}}{\leq}$ search-LWE $\underset{\text{[BFKL'93,R'05,...]}}{\leq}$ decision-LWE $\leq$ crypto

- Also fully *classical* reductions, for worse params [Peikert'09,BLPRS'13]

Another Hard Problem: Learning With Errors [Regev'05]

- Parameters: dimension n, modulus $q = \text{poly}(n)$, error distribution χ
- **Search:** find <u>secret</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad \begin{pmatrix} \cdots & \mathbf{b}^t & \cdots \end{pmatrix} \approx \mathbf{s}^t \mathbf{A}$$



$\sqrt{n} \leq$ std dev $\ll q$, 'rate' α

- **Decision:** distinguish $(\mathbf{A}\ ,\ \mathbf{b})$ from <u>uniform</u> $(\mathbf{A}\ ,\ \mathbf{b})$

LWE is Hard

(n/α)-approx *worst case* GapSVP, SIVP $\underset{\text{(quantum [R'05])}}{\leq}$ search-LWE $\underset{\text{[BFKL'93,R'05,...]}}{\leq}$ decision-LWE $\leq$ crypto

- Also fully *classical* reductions, for worse params [Peikert'09,BLPRS'13]
- Also a direct worst-case $\leq$ decision-LWE (quantum) reduction [PRS'17]

LWE is Versatile

What kinds of crypto can we construct from LWE?

LWE is Versatile

What kinds of crypto can we construct from LWE?

- ✔ Key Exchange/Public Key Encryption
- ✔ Oblivious Transfer
- ✔ Actively Secure Encryption (w/o random oracles)
- ✔ (Constrained) PRFs

LWE is Versatile

What kinds of crypto can we construct from LWE?

- ✔ Key Exchange/Public Key Encryption
- ✔ Oblivious Transfer
- ✔ Actively Secure Encryption (w/o random oracles)
- ✔ (Constrained) PRFs

- - - - - - - - -

- ✔✔ Identity-Based Encryption (w/ RO)
- ✔✔ Hierarchical ID-Based Encryption (w/o RO)
- ✔✔ NIZK for NP (w/o RO)

LWE is Versatile

What kinds of crypto can we construct from LWE?

- ✔ Key Exchange/Public Key Encryption
- ✔ Oblivious Transfer
- ✔ Actively Secure Encryption (w/o random oracles)
- ✔ (Constrained) PRFs

- - - - - - - - -

- ✔✔ Identity-Based Encryption (w/ RO)
- ✔✔ Hierarchical ID-Based Encryption (w/o RO)
- ✔✔ NIZK for NP (w/o RO)

- - - - - - - - -

- !!! Fully Homomorphic Encryption
- !!! Attribute-Based/Predicate Encryption for arbitrary policies

and much, much more...

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

$$\xleftarrow{\mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

(ciphertext 'preamble')

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

$$\xleftarrow{\mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

(ciphertext 'preamble')

$$\xleftarrow{b' = \mathbf{s}^t\, \mathbf{u} + e' + \text{bit} \cdot \frac{q}{2}}$$

('payload')

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

$$\xleftarrow{\mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

(ciphertext 'preamble')

$$b' - \mathbf{b}^t \mathbf{x} \approx \text{bit} \cdot \frac{q}{2}$$

$$\xleftarrow{b' = \mathbf{s}^t \mathbf{u} + e' + \text{bit} \cdot \frac{q}{2}}$$

('payload')

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

$$\xleftarrow{\mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

(ciphertext 'preamble')

$$b' - \mathbf{b}^t \mathbf{x} \approx \text{bit} \cdot \frac{q}{2}$$

$$\xleftarrow{b' = \mathbf{s}^t \mathbf{u} + e' + \text{bit} \cdot \frac{q}{2}}$$

('payload')

$(\mathbf{A}, \mathbf{u}), (\mathbf{b}, b')$

Public-Key Cryptosystem from LWE [Regev'05,GPV'08]

short $\mathbf{x}$

$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$

$\mathbf{s} \leftarrow \mathbb{Z}_q^n$

$$\xrightarrow{\mathbf{u} = \mathbf{A}\mathbf{x}}$$

(public key, uniform when $m > n \log q$)

$$\xleftarrow{\mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

(ciphertext 'preamble')

$$b' - \mathbf{b}^t \mathbf{x} \approx \text{bit} \cdot \frac{q}{2}$$

$$\xleftarrow{b' = \mathbf{s}^t \mathbf{u} + e' + \text{bit} \cdot \frac{q}{2}}$$

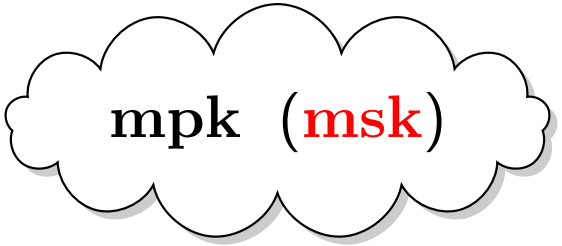
('payload')

$(\mathbf{A}, \mathbf{u}), (\mathbf{b}, b')$

by LWE

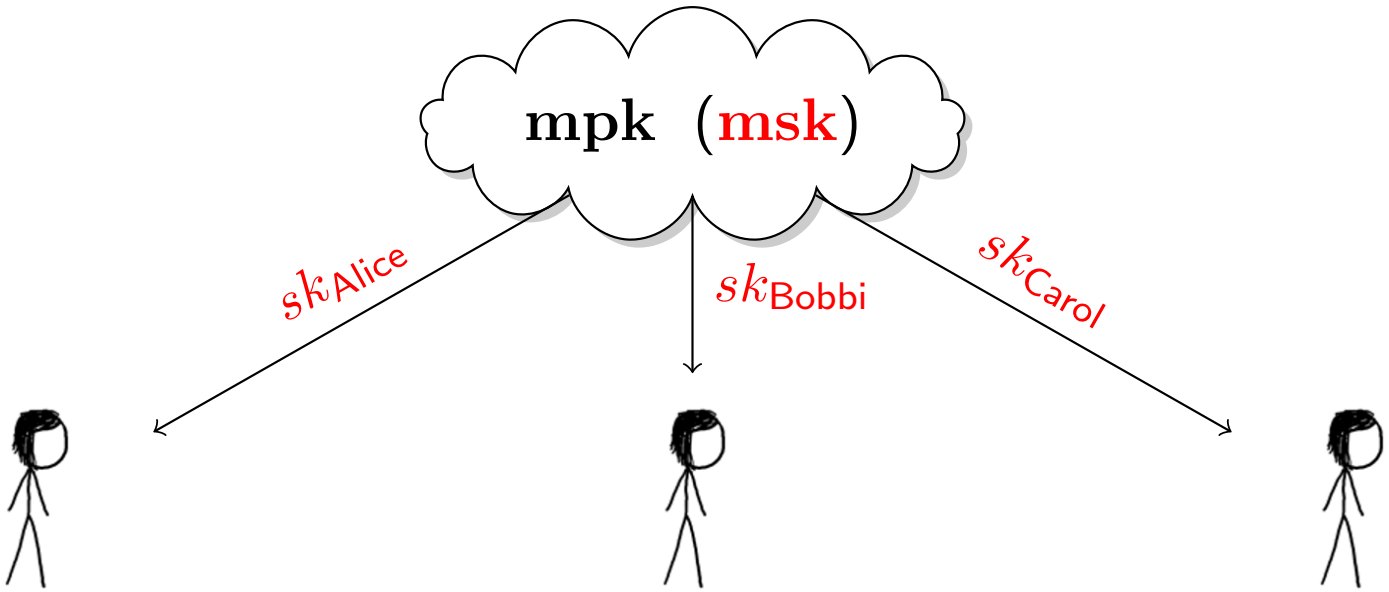
Identity-Based Encryption

- Proposed by [Shamir'84]: could this exist?



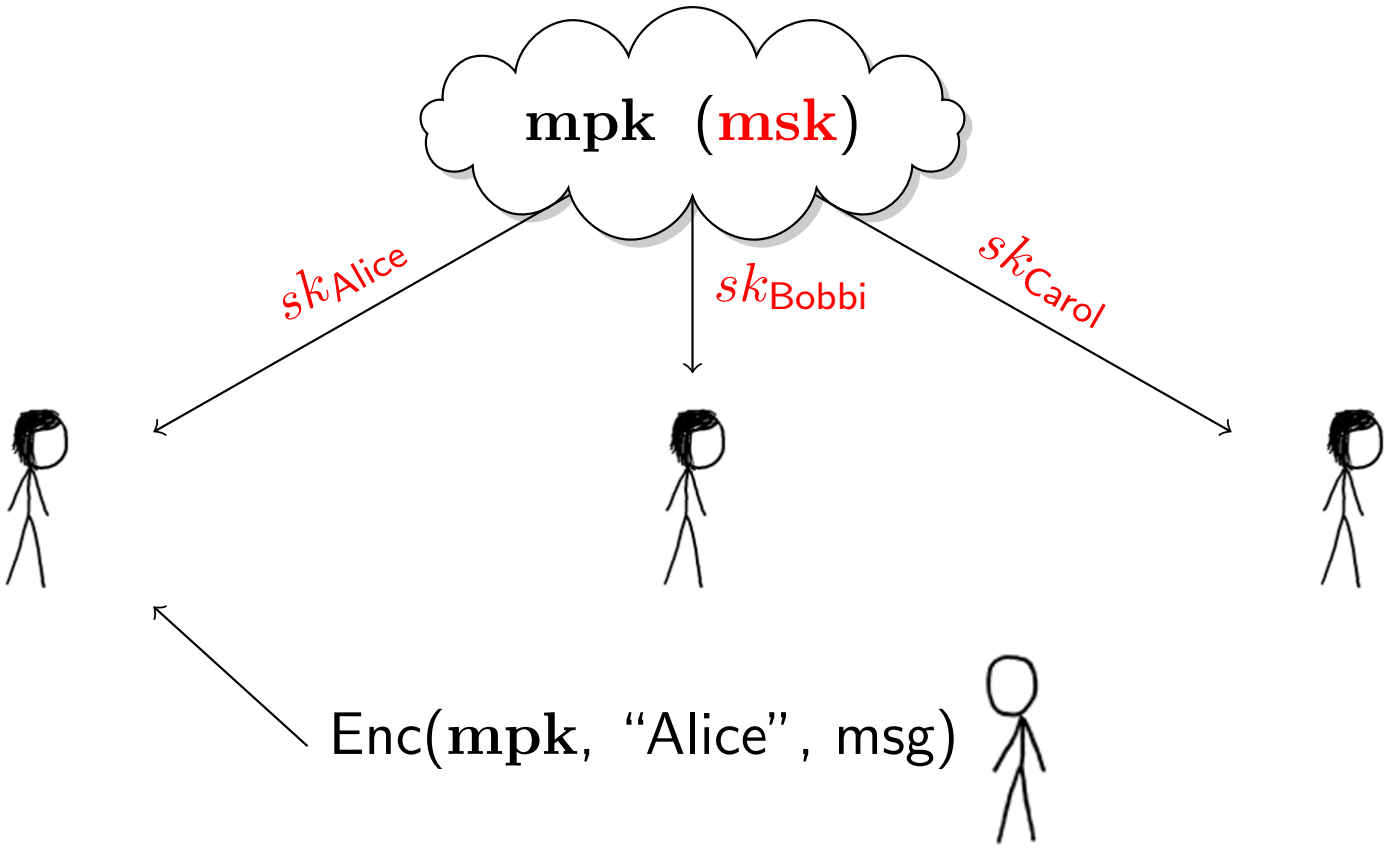
Identity-Based Encryption

- Proposed by [Shamir'84]: could this exist?



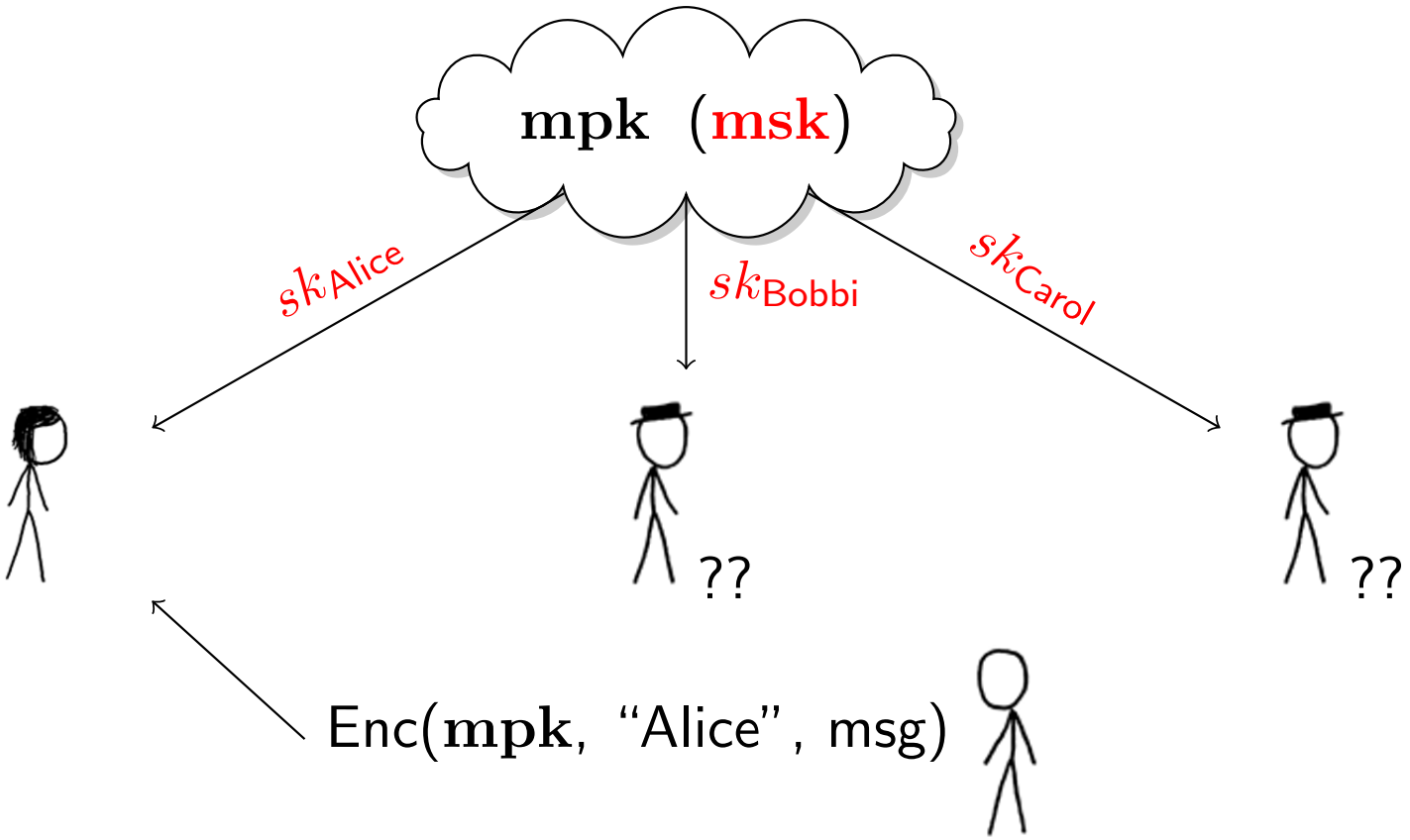
Identity-Based Encryption

- Proposed by [Shamir'84]: could this exist?



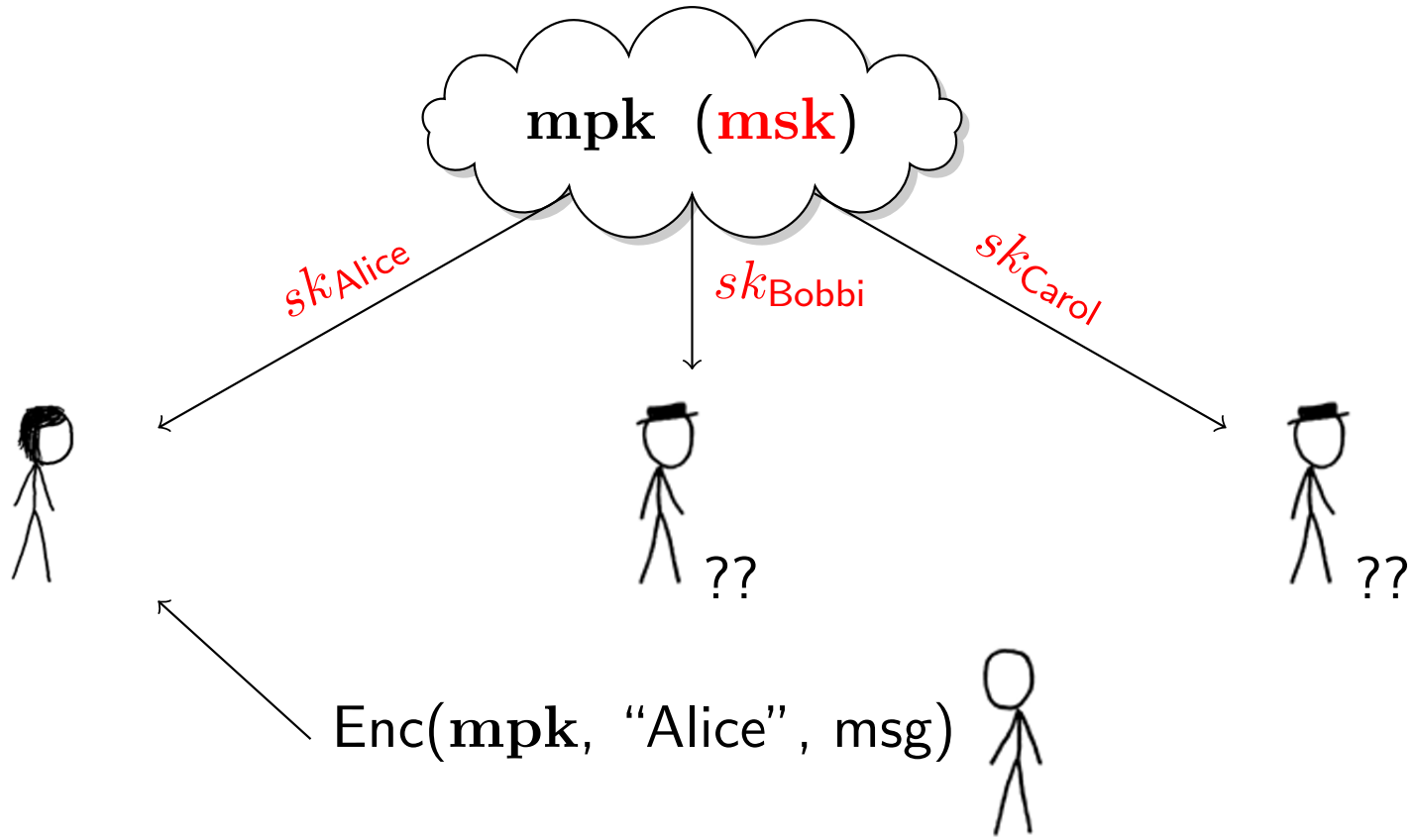
Identity-Based Encryption

- Proposed by [Shamir'84]: could this exist?



Identity-Based Encryption

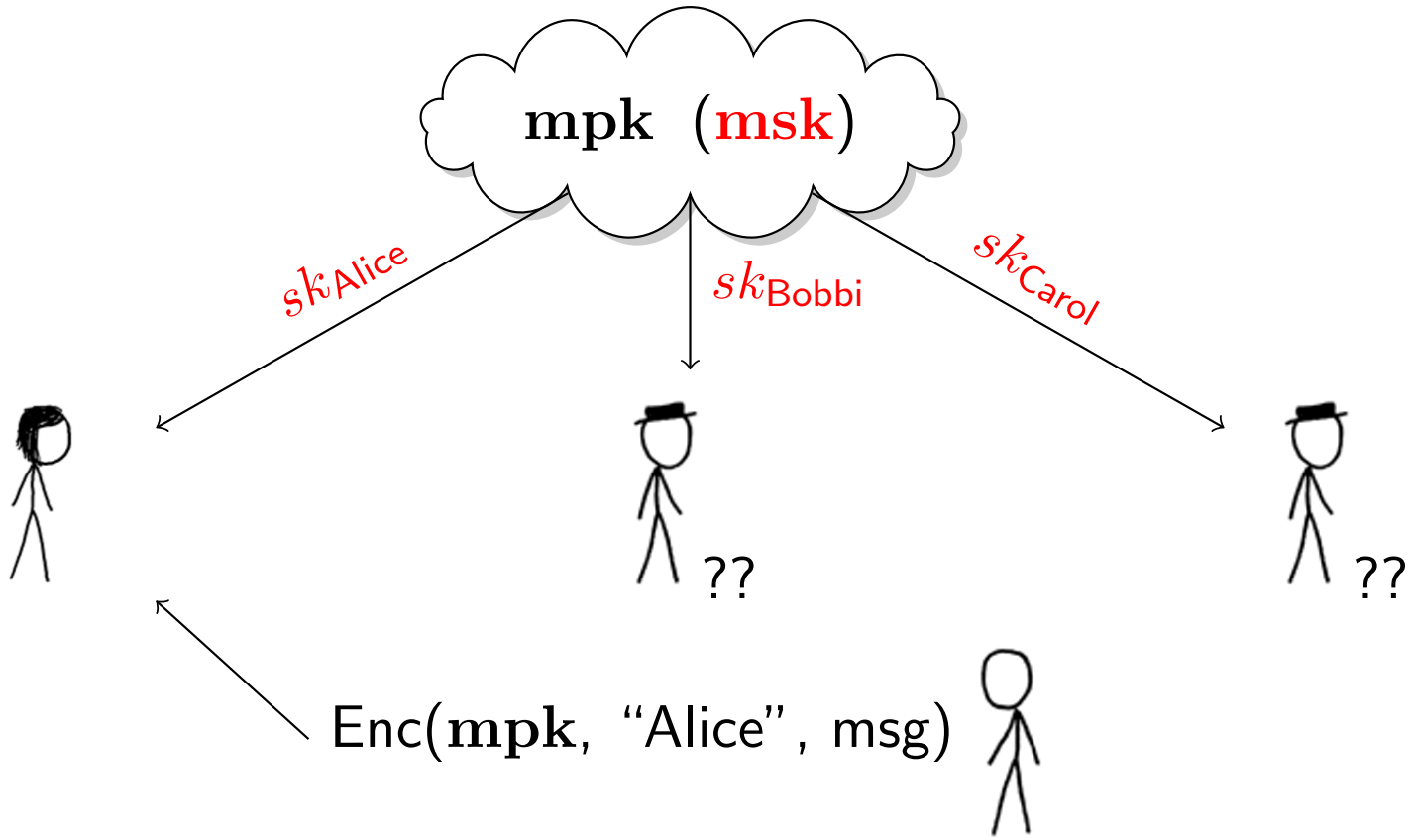
- Proposed by [Shamir'84]: could this exist?



1. [BonehFranklin'01,...]: first IBE, based on pairings

Identity-Based Encryption

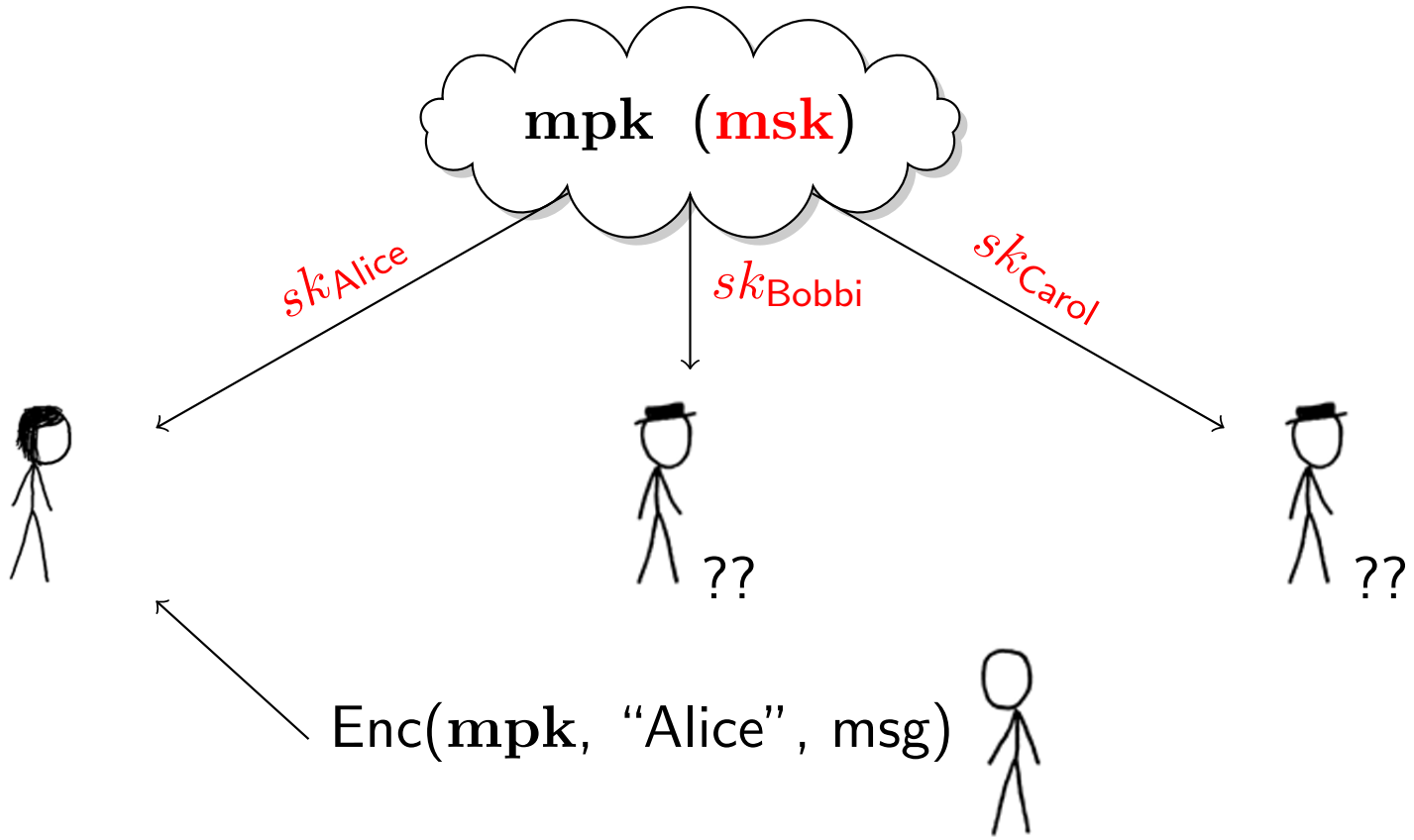
- Proposed by [Shamir'84]: could this exist?



1. [BonehFranklin'01,...]: first IBE, based on pairings
2. [Cocks'01,BGH'07]: based on quadratic residuosity mod $N = pq$

Identity-Based Encryption

- Proposed by [Shamir'84]: could this exist?



1. [BonehFranklin'01,...]: first IBE, based on pairings
2. [Cocks'01,BGH'07]: based on quadratic residuosity mod $N = pq$
3. [GPV'08]: based on lattices!

IBE from LWE

Gaussian $\mathbf{x}$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{u}$

$$mpk = \mathbf{A}$$
$$msk = \text{trapdoor } \mathbf{T}$$

$$\mathbf{u} = H(\text{“Alice”})$$

(‘identity’ public key)

$$\mathbf{b} = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$

(ciphertext preamble)

$$b' = \mathbf{s}^t \mathbf{u} + e' + \text{bit} \cdot \tfrac{q}{2}$$

(‘payload’)

$$b' - \mathbf{b}^t \mathbf{x} \approx \text{bit} \cdot \tfrac{q}{2}$$

Part 3:

Rings for Better Efficiency

SIS/LWE are (Sort Of) Efficient

$$\left(\cdots \mathbf{a}_i \cdots\right) \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + e_i \;=\; b_i \in \mathbb{Z}_q$$

- Getting one pseudorandom scalar $b_i \in \mathbb{Z}_q$ requires an n-dim inner product (mod q)

SIS/LWE are (Sort Of) Efficient

$$(\cdots \mathbf{a}_i \cdots) \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + e_i \;=\; b_i \in \mathbb{Z}_q$$

- Getting one pseudorandom scalar $b_i \in \mathbb{Z}_q$ requires an n-dim inner product (mod q)
- Can amortize each $\mathbf{a}_i$ over many secrets $\mathbf{s}_j$, but still $\tilde{O}(n)$ work per scalar output.

SIS/LWE are (Sort Of) Efficient

$$(\cdots \mathbf{a}_i \cdots) \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + e_i \;=\; b_i \in \mathbb{Z}_q$$

- Getting one pseudorandom scalar $b_i \in \mathbb{Z}_q$ requires an n-dim inner product (mod q)
- Can amortize each $\mathbf{a}_i$ over many secrets $\mathbf{s}_j$, but still $\tilde{O}(n)$ work per scalar output.

- Cryptosystems have rather large keys:

$$pk = \underbrace{\begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix}}_{n} \quad , \quad \left.\begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix}\right\} \Omega(n)$$

SIS/LWE are (Sort Of) Efficient

$$(\cdots \mathbf{a}_i \cdots) \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + e_i \;=\; b_i \in \mathbb{Z}_q$$

- Getting one pseudorandom scalar $b_i \in \mathbb{Z}_q$ requires an n-dim inner product (mod q)
- Can amortize each $\mathbf{a}_i$ over many secrets $\mathbf{s}_j$, but still $\tilde{O}(n)$ work per scalar output.

- Cryptosystems have rather large keys:

$$pk = \underbrace{\begin{pmatrix} \vdots \\ \mathbf{A}^t \\ \vdots \end{pmatrix}}_{n} \quad , \quad \left.\begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix}\right\} \Omega(n)$$

- Inherently $\geq n^2$ time to encrypt & decrypt a message.

Wishful Thinking...

$$\begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ \mathbf{e}_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \mathbf{b}_i \\ \vdots \end{pmatrix} \in \mathbb{Z}_q^n$$

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $n \times n$ blocks by n-dimensional vectors.

Wishful Thinking...

$$\begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ \mathbf{e}_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \mathbf{b}_i \\ \vdots \end{pmatrix} \in \mathbb{Z}_q^n$$

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $n \times n$ blocks by n-dimensional vectors.

Question

- How to define the product '$\star$' so that $(\mathbf{a}_i, \mathbf{b}_i)$ is pseudorandom?

Wishful Thinking...

$$\begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ \mathbf{e}_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \mathbf{b}_i \\ \vdots \end{pmatrix} \in \mathbb{Z}_q^n$$

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $n \times n$ blocks by n-dimensional vectors.

Question

- How to define the product '$\star$' so that $(\mathbf{a}_i, \mathbf{b}_i)$ is pseudorandom?
- Careful! With small error, coordinate-wise multiplication is insecure!

Wishful Thinking...

$$\begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ \mathbf{e}_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \mathbf{b}_i \\ \vdots \end{pmatrix} \in \mathbb{Z}_q^n$$

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $n \times n$ blocks by n-dimensional vectors.

Question

- How to define the product '$\star$' so that $(\mathbf{a}_i, \mathbf{b}_i)$ is pseudorandom?
- Careful! With small error, coordinate-wise multiplication is insecure!

Answer

- '$\star$' = multiplication in a polynomial ring: e.g., $\mathbb{Z}_q[X]/(X^n + 1)$.

  Fast and practical with FFT: $n \log n$ operations mod q.

Wishful Thinking...

$$\begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix} \star \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + \begin{pmatrix} \vdots \\ \mathbf{e}_i \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \mathbf{b}_i \\ \vdots \end{pmatrix} \in \mathbb{Z}_q^n$$

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $n \times n$ blocks by n-dimensional vectors.

Question

- How to define the product '$\star$' so that $(\mathbf{a}_i, \mathbf{b}_i)$ is pseudorandom?
- Careful! With small error, coordinate-wise multiplication is insecure!

Answer

- '$\star$' = multiplication in a polynomial ring: e.g., $\mathbb{Z}_q[X]/(X^n + 1)$.

  Fast and practical with FFT: $n \log n$ operations mod q.
- Same ring structures used in NTRU cryptosystem [HPS'98],

  compact one-way / CR hash functions [Mic'02,PR'06,LM'06,...]

LWE Over Rings, Over Simplified

- Let $\boxed{R = \mathbb{Z}[X]/(X^n + 1)}$ for n a power of two, and $\boxed{R_q = R/qR}$

LWE Over Rings, Over Simplified

- Let $\boxed{R = \mathbb{Z}[X]/(X^n + 1)}$ for n a power of two, and $\boxed{R_q = R/qR}$
  - ⋆ Elements of R_q are deg $< n$ polynomials with mod-q coefficients
  - ⋆ Operations in R_q are very efficient using FFT-like algorithms

LWE Over Rings, Over Simplified

- Let $\boxed{R = \mathbb{Z}[X]/(X^n + 1)}$ for n a power of two, and $\boxed{R_q = R/qR}$
  - ⋆ Elements of R_q are deg $< n$ polynomials with mod-q coefficients
  - ⋆ Operations in R_q are very efficient using FFT-like algorithms
- **Search**: <u>find</u> secret ring element $s \in R_q$, given:

$$
\begin{aligned}
a_1 &\leftarrow R_q \quad , \quad b_1 = s \cdot a_1 + e_1 \in R_q \\
a_2 &\leftarrow R_q \quad , \quad b_2 = s \cdot a_2 + e_2 \in R_q \\
a_3 &\leftarrow R_q \quad , \quad b_3 = s \cdot a_3 + e_3 \in R_q \\
&\vdots
\end{aligned}
\qquad (e_i \in R \text{ are 'small'})
$$

LWE Over Rings, Over Simplified

- Let $\boxed{R = \mathbb{Z}[X]/(X^n + 1)}$ for n a power of two, and $\boxed{R_q = R/qR}$
  - ⋆ Elements of R_q are deg $< n$ polynomials with mod-q coefficients
  - ⋆ Operations in R_q are very efficient using FFT-like algorithms
- **Search**: <u>find</u> secret ring element $s \in R_q$, given:

$$
\begin{array}{lcl}
a_1 \leftarrow R_q & , & b_1 = s \cdot a_1 + e_1 \in R_q \\
a_2 \leftarrow R_q & , & b_2 = s \cdot a_2 + e_2 \in R_q \\
a_3 \leftarrow R_q & , & b_3 = s \cdot a_3 + e_3 \in R_q \\
 & \vdots &
\end{array}
\qquad (e_i \in R \text{ are 'small'})
$$

- **Decision**: <u>distinguish</u> $(a_i\ ,\ b_i)$ from uniform $(a_i\ ,\ b_i) \in R_q \times R_q$

Hardness of Ring-LWE

Initial Reductions [LyubashevskyPeikertRegev'10]

worst-case approx-SVP on *ideal* lattices in R $\leq$ search R-LWE $\leq$ decision R-LWE

(quantum, any $R = \mathcal{O}_K$)

(classical, any cyclotomic R)

Hardness of Ring-LWE

Initial Reductions [LyubashevskyPeikertRegev'10]

worst-case approx-SVP on *ideal* lattices in R $\underset{\text{(quantum, any } R = \mathcal{O}_K)}{\leq}$ search R-LWE $\underset{\text{(classical, any cyclotomic } R)}{\leq}$ decision R-LWE

Newer Reduction [PeikertRegevStephens-Davidowitz'17]

worst-case approx-SVP on *ideal* lattices in R $\underset{\text{(quantum, any } R = \mathcal{O}_K)}{\leq}$ decision R-LWE

Hardness of Ring-LWE

Initial Reductions [LyubashevskyPeikertRegev'10]

worst-case approx-SVP on *ideal* lattices in R $\leq$ search R-LWE $\leq$ decision R-LWE

(quantum, any $R = \mathcal{O}_K$) (classical, any cyclotomic R)

Newer Reduction [PeikertRegevStephens-Davidowitz'17]

worst-case approx-SVP on *ideal* lattices in R $\leq$ decision R-LWE

(quantum, any $R = \mathcal{O}_K$)

Constructions

decision R-LWE $\leq$ much crypto

Final Thoughts

- Lattices are a very attractive foundation for post-quantum crypto, for both 'basic' and 'advanced' objects.

  See remaining talks for much more.

Final Thoughts

- Lattices are a very attractive foundation for post-quantum crypto, for both 'basic' and 'advanced' objects.

  See remaining talks for much more.

- Cryptanalysis/concrete security estimates are subtle and ongoing, but maturing.

  See Phong Nguyen's talks tomorrow for coverage of this topic.

Final Thoughts

- Lattices are a very attractive foundation for post-quantum crypto, for both 'basic' and 'advanced' objects.

  See remaining talks for much more.

- Cryptanalysis/concrete security estimates are subtle and ongoing, but maturing.

  See Phong Nguyen's talks tomorrow for coverage of this topic.

Thanks!