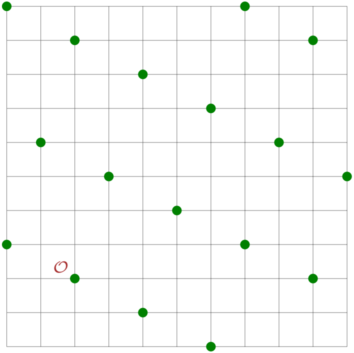
Lattice-Based Cryptography: Short Integer Solution (SIS) and Learning With Errors (LWE)

Chris Peikert
Georgia Institute of Technology

crypt@b-it 2013

Recall: Lattices

- Full-rank additive subgroup in $\mathbb{Z}^m$.

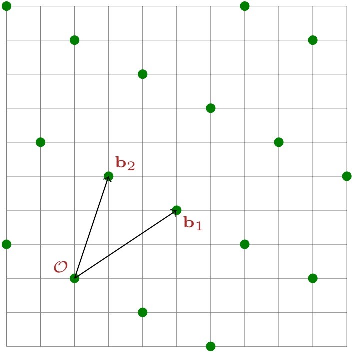


Recall: Lattices

- Full-rank additive subgroup in $\mathbb{Z}^m$.

- Basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$:

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

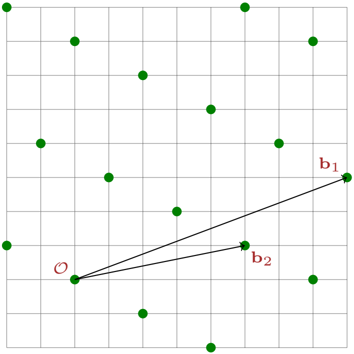


Recall: Lattices

- Full-rank additive subgroup in $\mathbb{Z}^m$.

- Basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$:

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



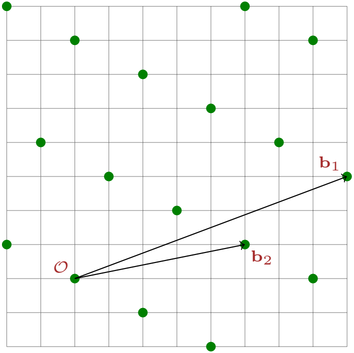
Recall: Lattices

- Full-rank additive subgroup in $\mathbb{Z}^m$.

- Basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$:

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

(Other representations too . . .)



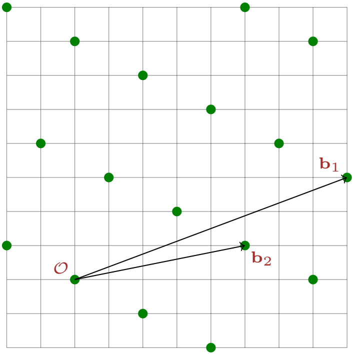
Recall: Lattices

- Full-rank additive subgroup in $\mathbb{Z}^m$.

- Basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$:

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

(Other representations too . . .)



Hard Problems

- Find/detect short nonzero lattice vector(s): SVP, GapSVP, SIVP
- Decode under small amount of error: BDD

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)

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

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)
- Goal: find nontrivial small $z_1, \ldots, z_m \in \mathbb{Z}$ such that:

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

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)
- Goal: find nontrivial short $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)
- Goal: find nontrivial short $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

One-Way & Collision-Resistant Hash Function

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

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

A Hard Problem: Short Integer Solution

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)
- Goal: find nontrivial short $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

One-Way & Collision-Resistant Hash Function

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

- $\mathbb{Z}_q^n = n$-dimensional vectors modulo q (e.g., $q \approx n^3$)
- Goal: find nontrivial short $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

One-Way & Collision-Resistant Hash Function

- Set $m > n \lg q$. Define $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$ 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 solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$, of norm $\|\mathbf{z}\| \leq \sqrt{m}$.

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

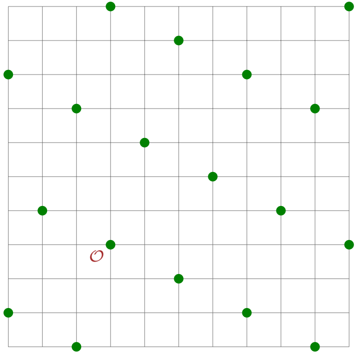
Cool! (but what does this have to do with lattices?)

- Parity-check matrix

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

defines the 'q-ary' integer lattice

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



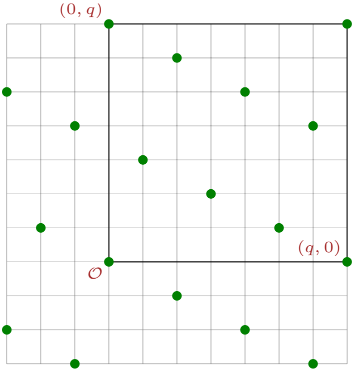
Cool! (but what does this have to do with lattices?)

- Parity-check matrix

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

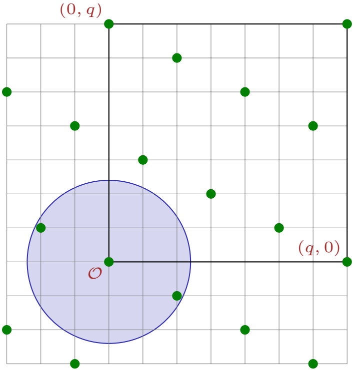
defines the 'q-ary' integer lattice

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



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

- Parity-check matrix
$$\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$$
defines the 'q-ary' integer lattice
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0}\}.$$
- SIS is SVP on random lattices $\mathcal{L}^{\perp}(\mathbf{A})$!



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

- Parity-check matrix

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

  defines the 'q-ary' integer lattice

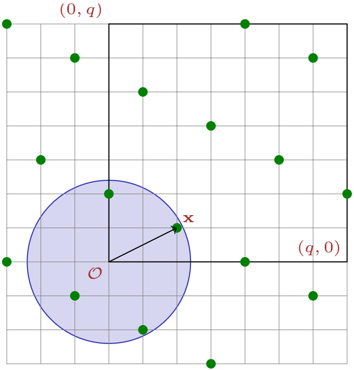
  $$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0}\}.$$

- SIS is SVP on random lattices $\mathcal{L}^{\perp}(\mathbf{A})$!

- Syndrome $\mathbf{u} \in \mathbb{Z}_q^n$ defines coset

  $$\mathcal{L}_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{x} : \mathbf{A}\mathbf{x} = \mathbf{u}\},$$

  $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ reduces $\mathbf{x}$ modulo $\mathcal{L}^{\perp}(\mathbf{A})$.



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

- Parity-check matrix

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

  defines the 'q-ary' integer lattice

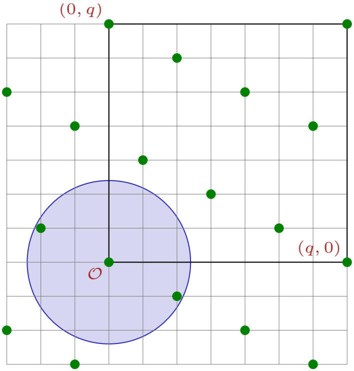
  $$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{A}\mathbf{z} = \mathbf{0}\}.$$

- SIS is SVP on random lattices $\mathcal{L}^{\perp}(\mathbf{A})$!

- Syndrome $\mathbf{u} \in \mathbb{Z}_q^n$ defines coset

  $$\mathcal{L}_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{x} : \mathbf{A}\mathbf{x} = \mathbf{u}\},$$

  $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ reduces $\mathbf{x}$ modulo $\mathcal{L}^{\perp}(\mathbf{A})$.



Worst-Case/Average-Case Connection [Ajtai'96,...]

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

A "Key" Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):

A “Key” Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.

A “Key” Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.
  2. Let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}]$ and $\mathbf{x} = \left[\begin{smallmatrix} \bar{\mathbf{x}} \\ 1 \end{smallmatrix}\right]$. (We just reduced $-\bar{\mathbf{x}}$ modulo $\mathcal{L}^{\perp}(\bar{\mathbf{A}})$.)

A "Key" Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.
  2. Let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}]$ and $\mathbf{x} = \left[\begin{smallmatrix} \bar{\mathbf{x}} \\ 1 \end{smallmatrix} \right]$. (We just reduced $-\bar{\mathbf{x}}$ modulo $\mathcal{L}^{\perp}(\bar{\mathbf{A}})$.)
- For *many* short solutions, let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{X}}]$ and $\mathbf{X} = \left[\begin{smallmatrix} \bar{\mathbf{X}} \\ \mathbf{I} \end{smallmatrix} \right]$.

A "Key" Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.
  2. Let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}]$ and $\mathbf{x} = \left[\begin{smallmatrix} \bar{\mathbf{x}} \\ 1 \end{smallmatrix}\right]$. (We just reduced $-\bar{\mathbf{x}}$ modulo $\mathcal{L}^{\perp}(\bar{\mathbf{A}})$.)
- For *many* short solutions, let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{X}}]$ and $\mathbf{X} = \left[\begin{smallmatrix} \bar{\mathbf{X}} \\ \mathbf{I} \end{smallmatrix}\right]$.
- Nothing special about $\{0,1\}^{\bar{m}}$: enough entropy suffices (essentially).

A "Key" Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.
  2. Let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}]$ and $\mathbf{x} = \left[\begin{smallmatrix} \bar{\mathbf{x}} \\ 1 \end{smallmatrix}\right]$. (We just reduced $-\bar{\mathbf{x}}$ modulo $\mathcal{L}^{\perp}(\bar{\mathbf{A}})$.)
- For *many* short solutions, let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{X}}]$ and $\mathbf{X} = \left[\begin{smallmatrix} \bar{\mathbf{X}} \\ \mathbf{I} \end{smallmatrix}\right]$.
- Nothing special about $\{0,1\}^{\bar{m}}$: enough entropy suffices (essentially).

'Leftover Hash' Lemma

- Over choice of $\bar{\mathbf{A}}$ and $\bar{\mathbf{x}}$, matrix $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}] \stackrel{s}{\approx}$ uniform.
- Proof: family $\left\{ f_{\bar{\mathbf{A}}} : \{0,1\}^{\bar{m}} \to \mathbb{Z}_q^n \right\}$ is pairwise independent; $\bar{\mathbf{x}}$ has sufficient (min-)entropy.

A "Key" Trick

- Generate uniform $\mathbf{A}$ with a short solution $\mathbf{x}$ (s.t. $\mathbf{A}\mathbf{x} = \mathbf{0}$):
  1. Choose $\bar{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n \times \bar{m}}$ and $\bar{\mathbf{x}} \leftarrow \{0,1\}^{\bar{m}}$ for (say) $\bar{m} \geq 2n \lg q$.
  2. Let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}]$ and $\mathbf{x} = \left[\begin{smallmatrix} \bar{\mathbf{x}} \\ 1 \end{smallmatrix}\right]$. (We just reduced $-\bar{\mathbf{x}}$ modulo $\mathcal{L}^{\perp}(\bar{\mathbf{A}})$.)
- For *many* short solutions, let $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{X}}]$ and $\mathbf{X} = \left[\begin{smallmatrix} \bar{\mathbf{X}} \\ \mathbf{I} \end{smallmatrix}\right]$.
- Nothing special about $\{0,1\}^{\bar{m}}$: enough entropy suffices (essentially).

'Leftover Hash' Lemma

- Over choice of $\bar{\mathbf{A}}$ and $\bar{\mathbf{x}}$, matrix $\mathbf{A} = [\bar{\mathbf{A}} \mid -\bar{\mathbf{A}}\bar{\mathbf{x}}] \stackrel{s}{\approx}$ uniform.
- Proof: family $\left\{ f_{\bar{\mathbf{A}}} : \{0,1\}^{\bar{m}} \to \mathbb{Z}_q^n \right\}$ is pairwise independent; $\bar{\mathbf{x}}$ has sufficient (min-)entropy.

Dirty Little Secret

- This trick — reducing a short vector modulo a lattice — is the only one-way function used in all of lattice crypto!

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

- As before, dimension n and modulus $q \geq 2$

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

- As before, dimension n and modulus $q \geq 2$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

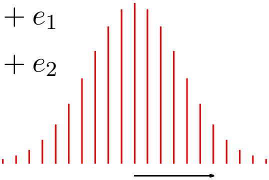
$$\mathbf{a}_1 \leftarrow \mathbb{Z}_q^n \ , \ b_1 = \langle \mathbf{s} \ , \ \mathbf{a}_1 \rangle + e_1$$
$$\mathbf{a}_2 \leftarrow \mathbb{Z}_q^n \ , \ b_2 = \langle \mathbf{s} \ , \ \mathbf{a}_2 \rangle + e_2$$
$$\vdots$$

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

- As before, dimension n and modulus $q \geq 2$, error rate $\alpha \ll 1$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

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

Errors $e_i \leftarrow \chi =$ Gaussian over $\mathbb{Z}$, width αq.



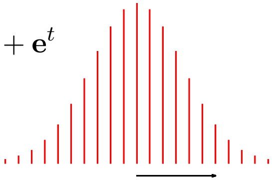
$\alpha q > \sqrt{n}$

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

- As before, dimension n and modulus $q \geq 2$, error rate $\alpha \ll 1$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

$$\mathbf{A} = \begin{pmatrix} | & & | \\ \mathbf{a}_1 & \cdots & \mathbf{a}_m \\ | & & | \end{pmatrix}, \quad \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$

Errors $e_i \leftarrow \chi =$ Gaussian over $\mathbb{Z}$, width αq.



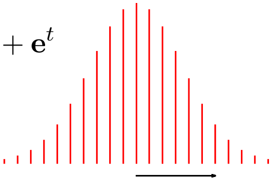
$\alpha q > \sqrt{n}$

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

- As before, dimension n and modulus $q \geq 2$, error rate $\alpha \ll 1$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

$$\mathbf{A} = \begin{pmatrix} | & & | \\ \mathbf{a}_1 & \cdots & \mathbf{a}_m \\ | & & | \end{pmatrix}, \quad \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$

Errors $e_i \leftarrow \chi =$ Gaussian over $\mathbb{Z}$, width αq.



$\alpha q > \sqrt{n}$

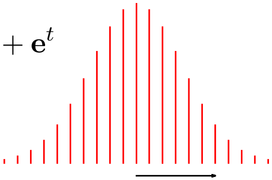
- **Decision:** distinguish $(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ from uniform $(\mathbf{A}, \mathbf{b}^t)$.

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

- As before, dimension n and modulus $q \geq 2$, error rate $\alpha \ll 1$
- **Search:** <u>find</u> $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

$$\mathbf{A} = \begin{pmatrix} | & & | \\ \mathbf{a}_1 & \cdots & \mathbf{a}_m \\ | & & | \end{pmatrix}, \quad \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$

Errors $e_i \leftarrow \chi =$ Gaussian over $\mathbb{Z}$, width αq.



$\alpha q > \sqrt{n}$

- **Decision:** <u>distinguish</u> $(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ from uniform $(\mathbf{A}, \mathbf{b}^t)$.
- Foundation for a huge amount of crypto

[R'05,PW'08,GPV'08,PVW'08,CDMW'08,AGV'09,ACPS'09,CHKP'10,ABB'10a,ABB'10b,GKV'10,BV'11,BGV'12,. . .]

LWE as a Lattice Problem

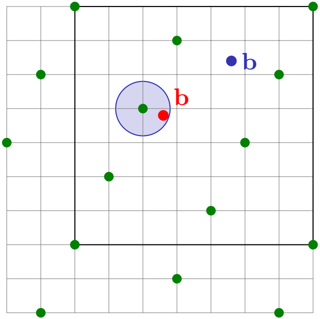
$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \in \mathbb{Z}_q^{n \times m} \quad , \quad \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t \quad \text{vs.} \quad \mathbf{b} \leftarrow \mathbb{Z}_q^m$$

- Lattice interpretation:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$$

Finding $\mathbf{s}, \mathbf{e}$: BDD on $\mathcal{L}(\mathbf{A})$!

Distinguishing $\mathbf{b}$ vs. $\mathbf{b}$: decision-BDD.



LWE as a Lattice Problem

$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \in \mathbb{Z}_q^{n\times m} \quad , \quad \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t \quad \text{vs.} \quad \mathbf{b} \leftarrow \mathbb{Z}_q^m$$

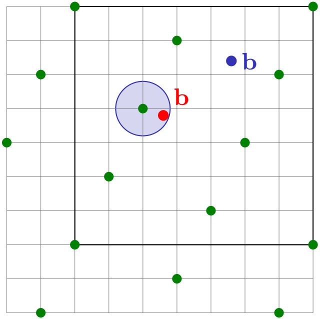
- Lattice interpretation:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$$

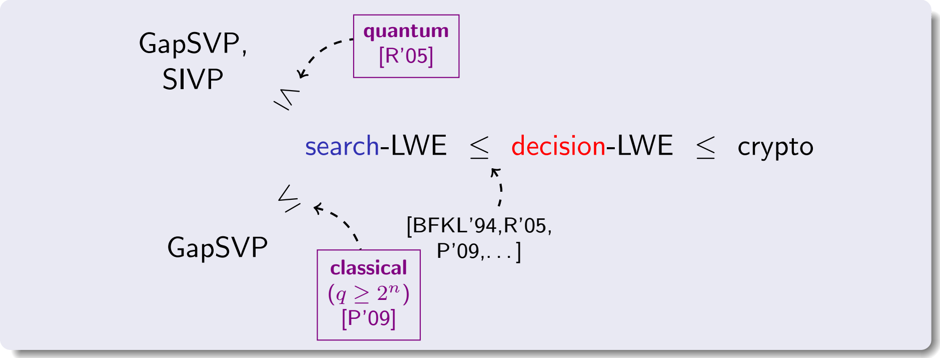
  Finding $\mathbf{s}, \mathbf{e}$: BDD on $\mathcal{L}(\mathbf{A})$!

  Distinguishing $\mathbf{b}$ vs. $\mathbf{b}$: decision-BDD.

- Also enjoys worst-case hardness [R'05,P'09]
  . . . but results are more subtle.



Overview of LWE Hardness



- Dim-modulus tradeoff [BLPRS'13]: e.g., $n, q = 2^n$ for $n^2, q = \text{poly}(n)$.
- Why error $\alpha q > \sqrt{n}$?
  - ⋆ Required by worst-case hardness proofs
  - ⋆ There's an $\exp((\alpha q)^2)$-time attack! [AG'11]

SIS versus LWE

SIS	LWE
$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$	$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

SIS versus LWE

SIS	LWE
$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$	$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Computational' (search) problem *a la* factoring, CDH

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH

- Many valid solutions $\mathbf{z}$

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{A}\mathbf{z} = \mathbf{0}$, then $\mathbf{b}^t\,\mathbf{z} = \mathbf{e}^t\,\mathbf{z}$ is small, but $\mathbf{b}^t\,\mathbf{z}$ is 'well-spread'

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$

SIS versus LWE

SIS

$\mathbf{Az} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{Az} = \mathbf{0}$, then $\mathbf{b}^t \mathbf{z} = \mathbf{e}^t \mathbf{z}$ is small, but $\mathbf{b}^t \mathbf{z}$ is 'well-spread'

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- SIS $\leq$ LWE quantumly [R'05]

SIS versus LWE

SIS

$\mathbf{Az} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{Az} = \mathbf{0}$, then $\mathbf{b}^t \mathbf{z} = \mathbf{e}^t \mathbf{z}$ is small, but $\mathbf{b}^t \mathbf{z}$ is 'well-spread'
- Applications: OWF / CRHF, signatures, ID schemes

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- SIS $\leq$ LWE quantumly [R'05]

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{A}\mathbf{z} = \mathbf{0}$, then $\mathbf{b}^t\mathbf{z} = \mathbf{e}^t\mathbf{z}$ is small, but $\mathbf{b}^t\mathbf{z}$ is 'well-spread'
- Applications: OWF / CRHF, signatures, ID schemes

'minicrypt'

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- SIS $\leq$ LWE quantumly [R'05]

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{A}\mathbf{z} = \mathbf{0}$, then $\mathbf{b}^t\mathbf{z} = \mathbf{e}^t\mathbf{z}$ is small, but $\mathbf{b}^t\mathbf{z}$ is 'well-spread'
- Applications: OWF / CRHF, signatures, ID schemes

'minicrypt'

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- SIS $\leq$ LWE quantumly [R'05]
- Applications: PKE, OT, ID-based encryption, FHE, ...

SIS versus LWE

SIS

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- LWE $\leq$ SIS: if $\mathbf{A}\mathbf{z} = \mathbf{0}$, then $\mathbf{b}^t \mathbf{z} = \mathbf{e}^t \mathbf{z}$ is small, but $\mathbf{b}^t \mathbf{z}$ is 'well-spread'
- Applications: OWF / CRHF, signatures, ID schemes

'minicrypt'

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- SIS $\leq$ LWE quantumly [R'05]
- Applications: PKE, OT, ID-based encryption, FHE, ...

'CRYPTOMANIA'

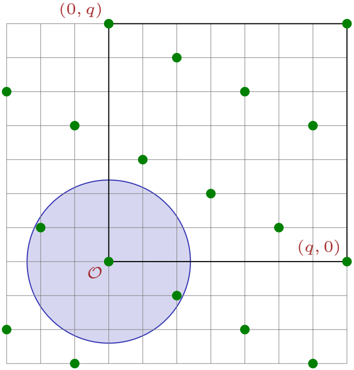
SIS versus LWE

<u>SIS</u>

$\mathbf{A}\mathbf{z} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$

Average-case SVP:

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

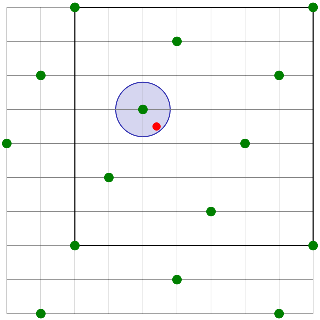


<u>LWE</u>

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

Average-case BDD:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$$



Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$:

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$:   test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

   If $\mathbf{s}' \neq \mathbf{s}$, then $b - \langle \mathbf{s}', \mathbf{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \mathbf{a} \rangle + e$ is 'well-spread' in $\mathbb{Z}_q$.

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

   If $\mathbf{s}' \neq \mathbf{s}$, then $b - \langle \mathbf{s}', \mathbf{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \mathbf{a} \rangle + e$ is 'well-spread' in $\mathbb{Z}_q$.

2. Shift the secret by any $\mathbf{t} \in \mathbb{Z}_q^n$:

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

   If $\mathbf{s}' \neq \mathbf{s}$, then $b - \langle \mathbf{s}', \mathbf{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \mathbf{a} \rangle + e$ is 'well-spread' in $\mathbb{Z}_q$.

2. Shift the secret by any $\mathbf{t} \in \mathbb{Z}_q^n$: given $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$, output

$$\mathbf{a} \, , \; b' = b + \langle \mathbf{t}, \mathbf{a} \rangle$$
$$= \langle \mathbf{s} + \mathbf{t}, \mathbf{a} \rangle + e.$$

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

   If $\mathbf{s}' \neq \mathbf{s}$, then $b - \langle \mathbf{s}', \mathbf{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \mathbf{a} \rangle + e$ is 'well-spread' in $\mathbb{Z}_q$.

2. Shift the secret by any $\mathbf{t} \in \mathbb{Z}_q^n$: given $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$, output

$$\mathbf{a}\ ,\ b' = b + \langle \mathbf{t}, \mathbf{a} \rangle$$
$$= \langle \mathbf{s} + \mathbf{t}, \mathbf{a} \rangle + e.$$

   Random $\mathbf{t}$'s (with fresh samples) $\Rightarrow$ random self-reduction.

   Lets us amplify success probabilities (both search & decision):

   non-negl on uniform $\mathbf{s} \leftarrow \mathbb{Z}_q^n \quad \Longrightarrow \quad \approx 1$ on <u>any</u> $\mathbf{s} \in \mathbb{Z}_q^n$

Warm-Up: Simple Properties of LWE

1. Check a candidate solution $\mathbf{s}' \in \mathbb{Z}_q^n$: test if all $b - \langle \mathbf{s}', \mathbf{a} \rangle$ small.

   If $\mathbf{s}' \neq \mathbf{s}$, then $b - \langle \mathbf{s}', \mathbf{a} \rangle = \langle \mathbf{s} - \mathbf{s}', \mathbf{a} \rangle + e$ is 'well-spread' in $\mathbb{Z}_q$.

2. Shift the secret by any $\mathbf{t} \in \mathbb{Z}_q^n$: given $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$, output

$$\begin{aligned} \mathbf{a} \ , \ b' &= b + \langle \mathbf{t}, \mathbf{a} \rangle \\ &= \langle \mathbf{s} + \mathbf{t}, \mathbf{a} \rangle + e. \end{aligned}$$

   Random $\mathbf{t}$'s (with fresh samples) $\Rightarrow$ random self-reduction.

   Lets us amplify success probabilities (both search & decision):

   non-negl on uniform $\mathbf{s} \leftarrow \mathbb{Z}_q^n \quad \Longrightarrow \quad \approx 1$ on <u>any</u> $\mathbf{s} \in \mathbb{Z}_q^n$

3. Multiple secrets: $(\mathbf{a}, b_1 \approx \langle \mathbf{s}_1, \mathbf{a} \rangle, \ldots, b_t \approx \langle \mathbf{s}_t, \mathbf{a} \rangle)$ vs. $(\mathbf{a}, b_1, \ldots, b_t)$.

   Simple hybrid argument, since $\mathbf{a}$'s are *public*.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

The test: for each $(\mathbf{a}, b)$, choose fresh $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs

$$(\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0), \, b).$$

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

The test: for each $(\mathbf{a}, b)$, choose fresh $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs

$$(\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0)\,,\, b).$$

- Notice: $b = \langle \mathbf{s}, \mathbf{a}' \rangle + s_1 \cdot r + e$.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

<u>The test</u>: for each $(\mathbf{a}, b)$, choose fresh $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs

$$(\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0)\,,\, b).$$

- Notice: $b = \langle \mathbf{s}, \mathbf{a}' \rangle + s_1 \cdot r + e$.
  - ⋆ If $s_1 = 0$, then $b = \langle \mathbf{s}, \mathbf{a}' \rangle + e \Rightarrow \mathcal{D}$ accepts.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

The test: for each $(\mathbf{a}, b)$, choose fresh $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs

$$(\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0)\,,\ b).$$

- Notice: $b = \langle \mathbf{s}, \mathbf{a}' \rangle + s_1 \cdot r + e$.
  - ⋆ If $s_1 = 0$, then $b = \langle \mathbf{s}, \mathbf{a}' \rangle + e \Rightarrow \mathcal{D}$ accepts.
  - ⋆ If $s_1 \neq 0$ and $\boxed{q \text{ prime}}$ then $b = \text{uniform} \Rightarrow \mathcal{D}$ rejects.

Search/Decision Equivalence [BFKL'94,R'05]

- Suppose $\mathcal{D}$ solves decision-LWE: it perfectly* distinguishes between pairs $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ and $(\mathbf{a}, b)$.

  We want to solve search-LWE: given pairs $(\mathbf{a}, b)$, find $\mathbf{s}$.

- If $\boxed{q = \text{poly}(n)}$, to find $s_1 \in \mathbb{Z}_q$ it suffices to test whether $s_1 \stackrel{?}{=} 0$, because we can shift s_1 by $0, 1, \ldots, q-1$. Same for $s_2, s_3, \ldots, s_n$.

<u>The test</u>: for each $(\mathbf{a}, b)$, choose fresh $r \leftarrow \mathbb{Z}_q$. Invoke $\mathcal{D}$ on pairs

$$(\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0)\,,\ b).$$

- Notice: $b = \langle \mathbf{s}, \mathbf{a}' \rangle + s_1 \cdot r + e$.
  - ⋆ If $s_1 = 0$, then $b = \langle \mathbf{s}, \mathbf{a}' \rangle + e \Rightarrow \mathcal{D}$ accepts.
  - ⋆ If $s_1 \neq 0$ and $\boxed{q \text{ prime}}$ then $b = \text{uniform} \Rightarrow \mathcal{D}$ rejects.

- (Don't actually need $\boxed{\text{prime } q = \text{poly}(n)}$.) [P'09,ACPS'09,MM'11,MP'12,BGV'12]

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

(This is called the "Hermite normal form" of LWE.)

Decision-LWE with ‘Short’ Secret

Theorem [M’01,ACPS’09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

(This is called the “Hermite normal form” of LWE.)

- Intuition: finding $\mathbf{e} \Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

(This is called the "Hermite normal form" of LWE.)

- Intuition: finding $\mathbf{e} \Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Transformation from secret $\mathbf{s} \in \mathbb{Z}_q^n$ to secret $\bar{\mathbf{e}} \leftarrow \chi^n$:

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

(This is called the "Hermite normal form" of LWE.)

- Intuition: finding $\mathbf{e} \Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Transformation from secret $\mathbf{s} \in \mathbb{Z}_q^n$ to secret $\bar{\mathbf{e}} \leftarrow \chi^n$:

1. Draw samples to get $(\bar{\mathbf{A}}, \bar{\mathbf{b}}^t = \mathbf{s}^t \bar{\mathbf{A}} + \bar{\mathbf{e}}^t)$ for square, invertible $\bar{\mathbf{A}}$.

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

  (This is called the "Hermite normal form" of LWE.)

- Intuition: finding $\mathbf{e} \Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Transformation from secret $\mathbf{s} \in \mathbb{Z}_q^n$ to secret $\bar{\mathbf{e}} \leftarrow \chi^n$:

1. Draw samples to get $(\bar{\mathbf{A}}, \bar{\mathbf{b}}^t = \mathbf{s}^t \bar{\mathbf{A}} + \bar{\mathbf{e}}^t)$ for square, invertible $\bar{\mathbf{A}}$.
2. Transform each additional sample $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ to

$$\mathbf{a}' = -\bar{\mathbf{A}}^{-1}\mathbf{a} \quad , \quad b' = b + \langle \bar{\mathbf{b}}, \mathbf{a}' \rangle$$

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

(This is called the "Hermite normal form" of LWE.)

- Intuition: finding $\mathbf{e}$ $\Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Transformation from secret $\mathbf{s} \in \mathbb{Z}_q^n$ to secret $\bar{\mathbf{e}} \leftarrow \chi^n$:

1. Draw samples to get $(\bar{\mathbf{A}}, \bar{\mathbf{b}}^t = \mathbf{s}^t \bar{\mathbf{A}} + \bar{\mathbf{e}}^t)$ for square, invertible $\bar{\mathbf{A}}$.
2. Transform each additional sample $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ to

$$\mathbf{a}' = -\bar{\mathbf{A}}^{-1}\mathbf{a} \quad , \quad b' = b + \langle \bar{\mathbf{b}}, \mathbf{a}' \rangle = \langle \bar{\mathbf{e}}, \mathbf{a}' \rangle + e.$$

Decision-LWE with 'Short' Secret

Theorem [M'01,ACPS'09]

- LWE is no easier if the secret is drawn from the error distribution χ^n.

  (This is called the "Hermite normal form" of LWE.)

- Intuition: finding $\mathbf{e} \Leftrightarrow$ finding $\mathbf{s}$: take $\mathbf{b}^t - \mathbf{e}^t = \mathbf{s}^t \mathbf{A}$, solve for $\mathbf{s}$.

Transformation from secret $\mathbf{s} \in \mathbb{Z}_q^n$ to secret $\bar{\mathbf{e}} \leftarrow \chi^n$:

1. Draw samples to get $(\bar{\mathbf{A}}, \bar{\mathbf{b}}^t = \mathbf{s}^t \bar{\mathbf{A}} + \bar{\mathbf{e}}^t)$ for square, invertible $\bar{\mathbf{A}}$.
2. Transform each additional sample $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e)$ to

$$\mathbf{a}' = -\bar{\mathbf{A}}^{-1} \mathbf{a} \quad , \quad b' = b + \langle \bar{\mathbf{b}}, \mathbf{a}' \rangle$$
$$= \langle \bar{\mathbf{e}}, \mathbf{a}' \rangle + e.$$

- This maps $(\mathbf{a}, b)$ to $(\mathbf{a}', b')$, so it applies to decision-LWE too.

Public-Key Cryptosystem using LWE [Regev'05]

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

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

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

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

(public key)

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

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

(ciphertext 'preamble')

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

← $\mathbf{u} = \mathbf{A}\mathbf{x}$

(ciphertext 'preamble')

← $u' = \mathbf{b}^t \mathbf{x} + \text{bit} \cdot \frac{q}{2}$

('payload')

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

$\mathbf{u} = \mathbf{A}\mathbf{x}$ ←

(ciphertext 'preamble')

$u' = \mathbf{b}^t \mathbf{x} + \text{bit} \cdot \frac{q}{2}$ ←

('payload')

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

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

$\mathbf{u} = \mathbf{A}\mathbf{x}$ ←

(ciphertext 'preamble')

$u' = \mathbf{b}^t \mathbf{x} + \text{bit} \cdot \frac{q}{2}$ ←

('payload')

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

$(\mathbf{A}, \mathbf{b}^t), (\mathbf{u}, u')$

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

$\mathbf{u} = \mathbf{A}\mathbf{x}$ ←

(ciphertext 'preamble')

$u' = \mathbf{b}^t \mathbf{x} + \text{bit} \cdot \frac{q}{2}$ ←

('payload')

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

$(\mathbf{A}, \mathbf{b}^t), (\mathbf{u}, u')$ by LWE

(Images courtesy xkcd.org)

Public-Key Cryptosystem using LWE [Regev'05]

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

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

$\mathbf{x} \leftarrow \{0,1\}^m$

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

(public key)

$\mathbf{u} = \mathbf{A}\mathbf{x}$ ←

(ciphertext 'preamble')

$u' = \mathbf{b}^t \mathbf{x} + \text{bit} \cdot \frac{q}{2}$ ←

('payload')

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

- - - - - - - - - - - - - - - - -

$(\mathbf{A}, \mathbf{b}^t), (\mathbf{u}, u')$
by LWE and
by LHL when
$m \geq n \log q$

(Images courtesy xkcd.org)

"Dual" Cryptosystem [GPV'08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

“Dual” Cryptosystem [GPV'08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

$\mathbf{u} = \mathbf{A}\mathbf{x}$ →

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

“Dual” Cryptosystem [GPV’08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

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

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

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

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

(ciphertext ‘preamble’)

“Dual” Cryptosystem [GPV’08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

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

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

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

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

(ciphertext ‘preamble’)

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

(‘payload’)

"Dual" Cryptosystem [GPV'08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

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

$\mathbf{u} = \mathbf{A}\mathbf{x}$ →

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

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

(ciphertext 'preamble')

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

('payload')

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

“Dual” Cryptosystem [GPV’08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

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

$\mathbf{u} = \mathbf{A}\mathbf{x}$ →

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

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

(ciphertext ‘preamble’)

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

(‘payload’)

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

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

"Dual" Cryptosystem [GPV'08]

$\mathbf{x} \leftarrow \{0,1\}^m$

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

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

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

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

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

(ciphertext 'preamble')

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

('payload')

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

- - - - - - - - - - - - - - - - -

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

by LWE

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

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

(public key)

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

$$\longleftarrow \mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$$

(ciphertext 'preamble')

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

$\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$ $\longleftarrow$

(ciphertext 'preamble')

$b' = \mathbf{u}^t \mathbf{r} + x' + \text{bit} \cdot \frac{q}{2}$ $\longleftarrow$

('payload')

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

$\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$ $\longleftarrow$

(ciphertext 'preamble')

$b' = \mathbf{u}^t \, \mathbf{r} + x' + \mathsf{bit} \cdot \frac{q}{2}$ $\longleftarrow$

('payload')

$b' - \mathbf{s}^t \, \mathbf{b} \approx \mathsf{bit} \cdot \frac{q}{2}$

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

← $\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$

(ciphertext 'preamble')

← $b' = \mathbf{u}^t \mathbf{r} + x' + \text{bit} \cdot \frac{q}{2}$

('payload')

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

- - - - - - - - - - - - - - - - -

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

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

$\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$ $\longleftarrow$

(ciphertext 'preamble')

$b' = \mathbf{u}^t \mathbf{r} + x' + \text{bit} \cdot \frac{q}{2}$ $\longleftarrow$

('payload')

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

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

Most Efficient Cryptosystem [A'03,LPS'10,LP'11]

$\mathbf{s} \leftarrow \chi^n$

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

$\mathbf{r} \leftarrow \chi^n$

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

(public key)

← $\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$

(ciphertext 'preamble')

← $b' = \mathbf{u}^t \mathbf{r} + x' + \text{bit} \cdot \frac{q}{2}$

('payload')

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

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

by LWE (HNF)

by LWE (HNF)

Wrapping Up

- Now you know all the basic techniques for working with SIS and LWE.
- We've covered a lot: do the exercises to reinforce your understanding!
- Tomorrow: more advanced applications, using "strong trapdoors."