Session #5: Learning With Errors

Chris Peikert
Georgia Institute of Technology

Winter School on Lattice-Based Cryptography and Applications
Bar-Ilan University, Israel
19 Feb 2012 – 22 Feb 2012

Last Time...

- SIS: find "small" nontrivial $z_1, \ldots, z_m \in \mathbb{Z}$ such that:

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

Last Time...

- SIS: find "small" nontrivial $z_1, \ldots, z_m \in \mathbb{Z}$ such that:

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

Last Time...

- SIS: find "short" nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

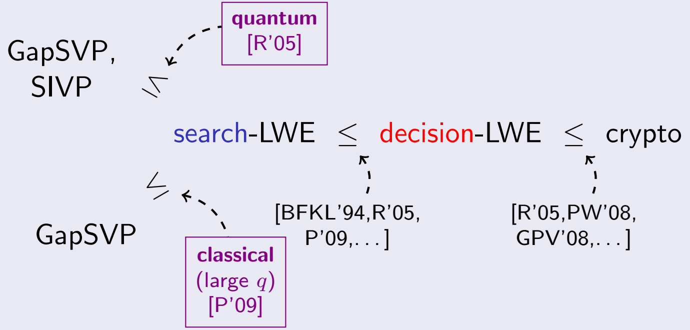
Last Time...

- SIS: find "short" nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

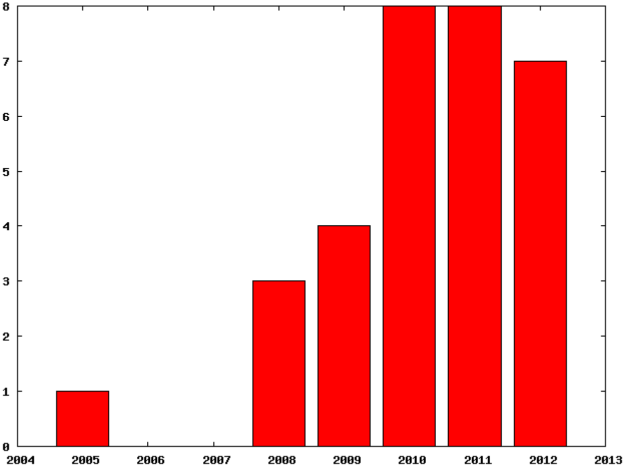
- This talk: a complementary problem, Learning With Errors

Overview of LWE Hardness



History of LWE

Crypto papers with “something new” regarding LWE:



Learning With Errors [Regev'05]

- Dimension n (security param), modulus $q \geq 2$

Learning With Errors [Regev'05]

- Dimension n (security param), modulus $q \geq 2$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

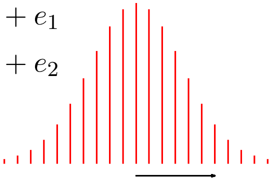
$$\mathbf{a}_1 \leftarrow \mathbb{Z}_q^n \ , \ b_1 = \langle \mathbf{s} \ , \ \mathbf{a}_1 \rangle + e_1$$
$$\mathbf{a}_2 \leftarrow \mathbb{Z}_q^n \ , \ b_2 = \langle \mathbf{s} \ , \ \mathbf{a}_2 \rangle + e_2$$
$$\vdots$$

Learning With Errors [Regev'05]

- Dimension n (security param), 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 $\mathbb{Z}$, param αq



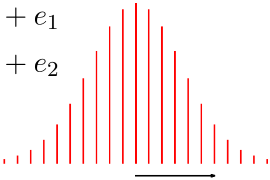
$\alpha \cdot q > \sqrt{n}$

Learning With Errors [Regev'05]

- Dimension n (security param), 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 $\mathbb{Z}$, param αq



$\alpha \cdot q > \sqrt{n}$

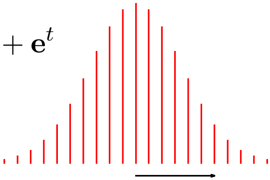
- **Decision:** distinguish $(\mathbf{a}_i, b_i)$ from uniform $(\mathbf{a}_i, b_i)$ pairs

Learning With Errors [Regev'05]

- Dimension n (security param), 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 $\mathbb{Z}$, param αq



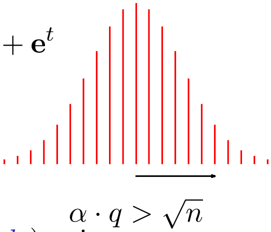
$\alpha \cdot q > \sqrt{n}$

- **Decision:** distinguish $(\mathbf{a}_i, b_i)$ from uniform $(\mathbf{a}_i, b_i)$ pairs

Learning With Errors [Regev'05]

- Dimension n (security param), 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 $\mathbb{Z}$, param αq

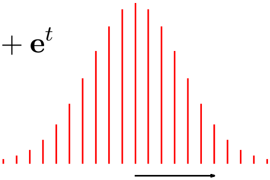
- **Decision:** distinguish $(\mathbf{a}_i, b_i)$ from uniform $(\mathbf{a}_i, b_i)$ pairs

Generalizes LPN ($q = 2$, Bernoulli noise) [AL'88,BFKL'94,...]

Learning With Errors [Regev'05]

- Dimension n (security param), modulus $q \geq 2$, 'error rate' $\alpha \ll 1$
- **Search:** find $\mathbf{s} \in \mathbb{Z}_q^n$ given 'noisy random inner products'

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



$\alpha \cdot q > \sqrt{n}$

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

- **Decision:** distinguish $(\mathbf{a}_i, b_i)$ from uniform $(\mathbf{a}_i, b_i)$ pairs

  Generalizes LPN ($q = 2$, Bernoulli noise) [AL'88,BFKL'94,...]

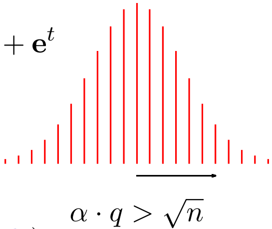
- Why error $\alpha q > \sqrt{n}$?
  - ⋆ Required by worst-case hardness proofs [R'05,P'09]

Learning With Errors [Regev'05]

- Dimension n (security param), 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 $\mathbb{Z}$, param αq



- **Decision:** distinguish $(\mathbf{a}_i, b_i)$ from uniform $(\mathbf{a}_i, b_i)$ pairs

  Generalizes LPN ($q = 2$, Bernoulli noise) [AL'88,BFKL'94,...]

- Why error $\alpha q > \sqrt{n}$?
  - ⋆ Required by worst-case hardness proofs [R'05,P'09]
  - ⋆ There's an $\exp((\alpha q)^2)$-time attack! [AG'11]

SIS versus LWE

SIS

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

LWE

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

SIS versus LWE

SIS

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

LWE

$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ 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	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	'Decisional' problem *a la* QR, DCR, DDH
Many valid solutions $\mathbf{z}$	Unique solution $\mathbf{s}$ (w/short $\mathbf{e}$)

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 $\mathbf{s}$ (w/short $\mathbf{e}$)

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 $\mathbf{s}$ (w/short $\mathbf{e}$)
- SIS $\overset{??}{\leq}$ LWE (stay till Wed...)

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

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 $\mathbf{s}$ (w/short $\mathbf{e}$)
- SIS $\overset{??}{\leq}$ LWE (stay till Wed...)

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 $\mathbf{s}$ (w/short $\mathbf{e}$)
- SIS $\overset{??}{\leq}$ LWE (stay till Wed...)

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 $\mathbf{s}$ (w/short $\mathbf{e}$)
- SIS $\overset{??}{\leq}$ LWE (stay till Wed...)
- 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

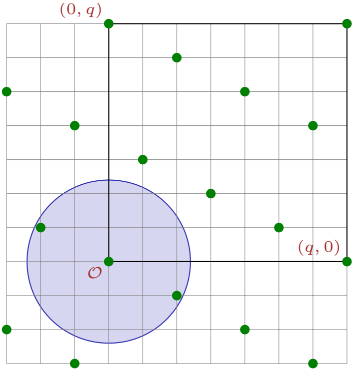
$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

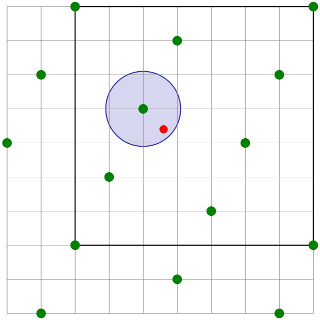
- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}$ (w/short $\mathbf{e}$)
- SIS $\overset{??}{\leq}$ LWE (stay till Wed...)
- Applications: PKE, OT, ID-based encryption, FHE

'CRYPTOMANIA'

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. $(\mathbf{A}, \mathbf{b}^t)$
Average-case SVP:	Average-case BDD:
$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$	$\mathcal{L}(\mathbf{A}) = \{\mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$





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

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

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 any $\mathbf{s} \in \mathbb{Z}_q^n$

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

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

   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> $\mathbf{s} \in \mathbb{Z}_q^n$

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 $s_2, s_3, \ldots, s_n$.

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

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.

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 $s_2, s_3, \ldots, s_n$.

<ins>The test</ins>: 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 = $ 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 $s_2, s_3, \ldots, s_n$.

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 $b =$ uniform $\Rightarrow \mathcal{D}$ rejects.

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

Decision-LWE with 'Short' Secrets

Theorem ([M'01,ACPS'09])

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

Decision-LWE with 'Short' Secrets

Theorem ([M'01,ACPS'09])

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

(This is the 'Hermite normal form' of LWE.)

Decision-LWE with 'Short' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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

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

Decision-LWE with 'Short' Secrets

Theorem ([M'01,ACPS'09])

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

(This is 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

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

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

Public-Key Cryptosystem [R'05]

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

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

(Images courtesy xkcd.org)

Public-Key Cryptosystem [R'05]

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

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

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

(public key)

(Images courtesy xkcd.org)

Public-Key Cryptosystem [R'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 [R'05]

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

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

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

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

(public key)

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

(ciphertext 'preamble')

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

('payload')

(Images courtesy xkcd.org)

Public-Key Cryptosystem [R'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)

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

(ciphertext 'preamble')

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

('payload')

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

(Images courtesy xkcd.org)

Public-Key Cryptosystem [R'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 [R'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 [R'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 $m \geq n \log q$)

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

(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]

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

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

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

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

(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’)

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

'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]

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

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

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

$\mathbf{u} = \mathbf{A}\mathbf{x}$ →

(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’)

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

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

by LWE

Primal vs. Dual Systems

Primal | Dual

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$
- c'text $(\mathbf{u} = \mathbf{A}\mathbf{x}, u' \approx \mathbf{s}^t\,\mathbf{u})$ is a fresh LWE sample, with many possible Enc coins $\mathbf{x}$

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$
- c'text $(\mathbf{u} = \mathbf{A}\mathbf{x}, u' \approx \mathbf{s}^t\,\mathbf{u})$ is a fresh LWE sample, with many possible Enc coins $\mathbf{x}$

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$
- c'text $(\mathbf{b}, b') \approx \mathbf{s}^t(\mathbf{A}, \mathbf{u})$ is many LWE RHS's, with unique Enc coins $\mathbf{s}, \mathbf{e}$

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$
- c'text $(\mathbf{u} = \mathbf{A}\mathbf{x}, u' \approx \mathbf{s}^t\,\mathbf{u})$ is a fresh LWE sample, with many possible Enc coins $\mathbf{x}$
- security: encrypting to 'malformed' $pk = (\mathbf{A}, \mathbf{b}^t)$ induces uniform ciphertext

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$
- c'text $(\mathbf{b}, b') \approx \mathbf{s}^t(\mathbf{A}, \mathbf{u})$ is many LWE RHS's, with unique Enc coins $\mathbf{s}, \mathbf{e}$

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$
- c'text $(\mathbf{u} = \mathbf{A}\mathbf{x}, u' \approx \mathbf{s}^t\,\mathbf{u})$ is a fresh LWE sample, with many possible Enc coins $\mathbf{x}$
- security: encrypting to 'malformed' $pk = (\mathbf{A}, \mathbf{b}^t)$ induces uniform ciphertext

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$
- c'text $(\mathbf{b}, b') \approx \mathbf{s}^t(\mathbf{A}, \mathbf{u})$ is many LWE RHS's, with unique Enc coins $\mathbf{s}, \mathbf{e}$
- security: switch ciphertext to uniform using LWE

Primal vs. Dual Systems

Primal

- $pk = (\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ is pseudorandom with unique $sk = \mathbf{s}$
- c'text $(\mathbf{u} = \mathbf{A}\mathbf{x}, u' \approx \mathbf{s}^t\,\mathbf{u})$ is a fresh LWE sample, with many possible Enc coins $\mathbf{x}$
- security: encrypting to 'malformed' $pk = (\mathbf{A}, \mathbf{b}^t)$ induces uniform ciphertext

Dual

- $pk = (\mathbf{A}, \mathbf{u} = \mathbf{A}\mathbf{x})$ is statistically random with many possible $sk = \mathbf{x}$
- c'text $(\mathbf{b}, b') \approx \mathbf{s}^t(\mathbf{A}, \mathbf{u})$ is many LWE RHS's, with unique Enc coins $\mathbf{s}, \mathbf{e}$
- security: switch ciphertext to uniform using LWE

(shared) $\mathbf{A}$ size: $n \times (n \log q)$ elements of $\mathbb{Z}_q$

(user) pk & ct size: $n \log q$ & n elements, or vice-versa

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]

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

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

$$\xrightarrow[\text{(public key)}]{\mathbf{u}^t = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t}$$

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)

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

(ciphertext 'preamble')

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

('payload')

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

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

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

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

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

(public key)

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

(ciphertext 'preamble')

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

('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')

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

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

('payload')

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

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

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

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

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

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

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

(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)

by LWE (HNF)

When We Come Back. . .

- A different kind of LWE application: Efficient pseudorandom functions

When We Come Back...

- A different kind of LWE application: Efficient pseudorandom functions

Selected bibliography for this talk:

R'05 O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," STOC'05 / JACM'09.

GPV'08 C. Gentry, C. Peikert, V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," STOC'08.

ACPS'09 B. Applebaum, D. Cash, C. Peikert, A. Sahai, "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems," CRYPTO'09.

LPS'10 V. Lyubashevsky, A. Palacio, G. Segev, "Public-Key Cryptographic Primitives Provably as Secure as Subset Sum," TCC'10.

LP'11 R. Lindner, C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption," CT-RSA'11.