Lattices:
. . . to Cryptography

Chris Peikert
Georgia Institute of Technology

Visions of Cryptography
10 December 2013

Agenda

1. The ~~two~~ one main lattice-based OWF
2. Two simple tricks that yield all* of lattice cryptography
3. Lots of applications

A Hard Problem: Short Integer Solution

- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

A Hard Problem: Short Integer Solution

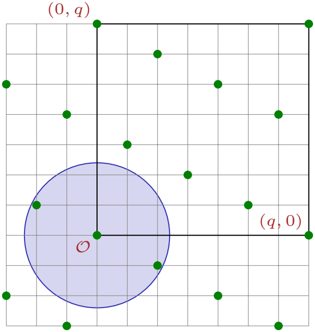
- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

- Just SVP on random 'q-ary' lattice

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



A Hard Problem: Short Integer Solution

- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

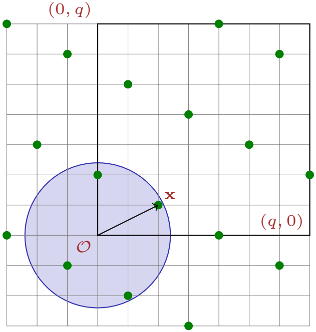
$$\underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix}}_{m} \begin{pmatrix} \\ \mathbf{z} \\ \\ \end{pmatrix} = \mathbf{0} \in \mathbb{Z}_q^n$$

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

- Just SVP on random 'q-ary' lattice

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

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



A Hard Problem: Short Integer Solution

- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

Worst-Case/Average-Case Connection [Ajtai'96,...,MR'04,GPV'08,MP'13]

Finding solution $\mathbf{z}$ with $\|\mathbf{z}\| \leq \beta \ll q$

(for uniformly random $\mathbf{A}$)

$\Downarrow$

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

A Hard Problem: Short Integer Solution

- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

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

- Goal: given uniform $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find short nonzero $\mathbf{z} \in \mathbb{Z}^m$ such that:

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

(When $m \geq n \log q$, short solutions are guaranteed to exist.)

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 $\|\mathbf{z}\| \leq \sqrt{m}$.

Another (?) Hard (?) Problem: Learning With Errors

- Wlog, $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n \times (m+n)}$.

  For $m \geq n \log q$, function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ is regular ($\Rightarrow$ many preimages).

Another (?) Hard (?) Problem: Learning With Errors

- Wlog, $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n\times(m+n)}$.

  For $m \geq n \log q$, function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ is regular ($\Rightarrow$ many preimages).

- What about $m \ll n \log q$? E.g., $m = n$? $m = 100$?

  Map $\mathbf{x} \mapsto \mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}_1 + \mathbf{x}_2$ is highly injective (whp).

Another (?) Hard (?) Problem: Learning With Errors

- Wlog, $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n \times (m+n)}$.

  For $m \geq n \log q$, function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ is regular ($\Rightarrow$ many preimages).

- What about $m \ll n \log q$? E.g., $m = n$? $m = 100$?

  Map $\mathbf{x} \mapsto \mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}_1 + \mathbf{x}_2$ is highly injective (whp).

  Is it one-way? Pseudorandom?

Another (?) Hard (?) Problem: Learning With Errors

- Wlog, $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n\times(m+n)}$.

  For $m \geq n \log q$, function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ is regular ($\Rightarrow$ many preimages).

- What about $m \ll n \log q$? E.g., $m = n$? $m = 100$?

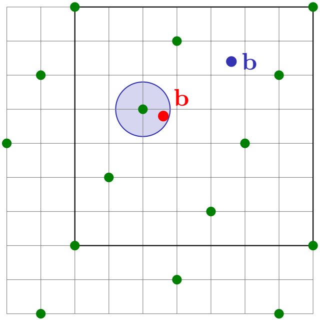
  Map $\mathbf{x} \mapsto \mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}_1 + \mathbf{x}_2$ is highly injective (whp).

  Is it one-way? Pseudorandom?

- Lattice interpretation: BDD on

$$\mathcal{L}(\bar{\mathbf{A}}) = \{\mathbf{v} \equiv \bar{\mathbf{A}}\mathbf{x}_1 \bmod q\}.$$

- Search $\Leftrightarrow$ decision: $\mathbf{A}\mathbf{x}$ is pseudorandom.



Another (?) Hard (?) Problem: Learning With Errors

- Wlog, $\mathbf{A} = [\bar{\mathbf{A}} \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n \times (m+n)}$.

  For $m \geq n \log q$, function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ is regular ($\Rightarrow$ many preimages).

- What about $m \ll n \log q$? E.g., $m = n$? $m = 100$?

  Map $\mathbf{x} \mapsto \mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{x}_1 + \mathbf{x}_2$ is highly injective (whp).

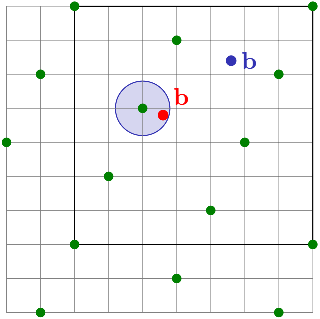
  Is it one-way? Pseudorandom?

- Lattice interpretation: BDD on

$$\mathcal{L}(\bar{\mathbf{A}}) = \{\mathbf{v} \equiv \bar{\mathbf{A}}\mathbf{x}_1 \bmod q\}.$$

- Search $\Leftrightarrow$ decision: $\mathbf{A}\mathbf{x}$ is pseudorandom.

- As hard as worst case problems on m-dim lattices [Regev'05,P'09].



The two amazingly simple tricks behind all of lattice cryptography...

Trick #1: Generate Random Instance with Solution(s)

- Generate (pseudo)random $\mathbf{A}'$ with a short solution:

Trick #1: Generate Random Instance with Solution(s)

- Generate (pseudo)random $\mathbf{A}'$ with a short solution:
  1. Choose $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and short $\mathbf{x}$.

Trick #1: Generate Random Instance with Solution(s)

- Generate (pseudo)random $\mathbf{A}'$ with a short solution:

  1. Choose $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and short $\mathbf{x}$.

  2. Let $\mathbf{u} = -[\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x}$ and $\mathbf{A}' = [\mathbf{u} \mid \mathbf{A}]$.

     Then $[\mathbf{A}' \mid \mathbf{I}_n] \begin{bmatrix} 1 \\ \mathbf{x} \end{bmatrix} = \mathbf{u} + [\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x} = \mathbf{0}$.

Trick #1: Generate Random Instance with Solution(s)

- Generate (pseudo)random $\mathbf{A}'$ with a short solution:

  1. Choose $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and short $\mathbf{x}$.

  2. Let $\mathbf{u} = -[\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x}$ and $\mathbf{A}' = [\mathbf{u} \mid \mathbf{A}]$.

  Then $[\mathbf{A}' \mid \mathbf{I}_n] \begin{bmatrix} 1 \\ \mathbf{x} \end{bmatrix} = \mathbf{u} + [\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x} = \mathbf{0}$.

- For *many* solutions, let $\mathbf{U} = -[\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{X}$ and $\mathbf{A}' = [\mathbf{U} \mid \mathbf{A}]$.

  Then $[\mathbf{A}' \mid \mathbf{I}_n] \cdot \left[\begin{smallmatrix} \mathbf{I}_k \\ \mathbf{X} \end{smallmatrix} \right] = \mathbf{0}$.

Trick #1: Generate Random Instance with Solution(s)

- Generate (pseudo)random $\mathbf{A}'$ with a short solution:

  1. Choose $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and short $\mathbf{x}$.

  2. Let $\mathbf{u} = -[\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x}$ and $\mathbf{A}' = [\mathbf{u} \mid \mathbf{A}]$.

  Then $[\mathbf{A}' \mid \mathbf{I}_n] \begin{bmatrix} 1 \\ \mathbf{x} \end{bmatrix} = \mathbf{u} + [\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{x} = \mathbf{0}$.

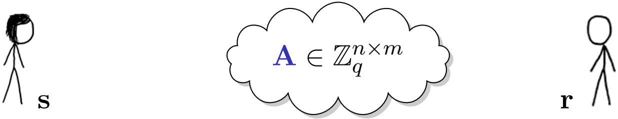
- For *many* solutions, let $\mathbf{U} = -[\mathbf{A} \mid \mathbf{I}_n] \cdot \mathbf{X}$ and $\mathbf{A}' = [\mathbf{U} \mid \mathbf{A}]$.

  Then $[\mathbf{A}' \mid \mathbf{I}_n] \cdot \left[\begin{smallmatrix} \mathbf{I}_k \\ \mathbf{X} \end{smallmatrix} \right] = \mathbf{0}$.

- Of course, we can also multiply on the left:

  Let $\mathbf{u}^t = \mathbf{x}^t \left[\begin{smallmatrix} \mathbf{A} \\ \mathbf{I}_m \end{smallmatrix} \right]$ and $\mathbf{A}' = \left[\begin{smallmatrix} \mathbf{u}^t \\ \mathbf{A} \end{smallmatrix} \right]$.

Key Agreement/Encryption



Key Agreement/Encryption

$\mathbf{s}$

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

$\mathbf{r}$

$$\mathbf{u} = \begin{bmatrix} \mathbf{A} & \mathbf{I}_n \end{bmatrix} \mathbf{r}$$

$\longleftarrow$

$$\mathbf{v}^t = \mathbf{s}^t \begin{bmatrix} \mathbf{A} \\ \mathbf{I}_m \end{bmatrix}$$

$\longrightarrow$

Key Agreement/Encryption

$\mathbf{s}$

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

$\mathbf{r}$

$$\mathbf{u} = \begin{bmatrix} \mathbf{A} & \mathbf{I}_n \end{bmatrix} \mathbf{r}$$

$\longleftarrow$

$$\mathbf{v}^t = \mathbf{s}^t \begin{bmatrix} \mathbf{A} \\ \mathbf{I}_m \end{bmatrix}$$

$\longrightarrow$

$$k_a = \mathbf{s}_1^t \cdot \mathbf{u} + \mathsf{err} \approx \mathbf{s}_1^t \mathbf{A} \mathbf{r}_1$$

$$k_b = \mathbf{v}^t \cdot \mathbf{r}_1 + \mathsf{err} \approx \mathbf{s}_1^t \mathbf{A} \mathbf{r}_1$$

Key Agreement/Encryption

$\mathbf{s}$

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

$\mathbf{r}$

$\mathbf{u} = [\, \mathbf{A} \;\; \mathbf{I}_n \,]\mathbf{r}$ ←

$\mathbf{v}^t = \mathbf{s}^t \begin{bmatrix} \mathbf{A} \\ \mathbf{I}_m \end{bmatrix}$ →

$k_a = \mathbf{s}_1^t \cdot \mathbf{u} + \text{err}$

$\approx \mathbf{s}_1^t \mathbf{A} \mathbf{r}_1$

$k_b = \mathbf{v}^t \cdot \mathbf{r}_1 + \text{err}$

$\approx \mathbf{s}_1^t \mathbf{A} \mathbf{r}_1$

$(\mathbf{A}, \mathbf{u}, \mathbf{v}, k_a)$

Key Agreement/Encryption

$\mathbf{s}$

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

$\mathbf{u}$

$\longleftarrow$

$\mathbf{v}^t = \mathbf{s}^t \begin{bmatrix} \mathbf{A} \\ \mathbf{I}_m \end{bmatrix}$

$\longrightarrow$

$k_a = \mathbf{s}_1^t \cdot \mathbf{u} + \mathsf{err}$

$(\mathbf{A}, \mathbf{u}, \mathbf{v}, k_a)$

Key Agreement/Encryption

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

$\mathbf{u}$

$\longleftarrow$

$\mathbf{v}^t$

$\longrightarrow$

$(\mathbf{A}, \mathbf{u}, \mathbf{v}, k_a)$

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert SIS: given $\mathbf{u} \in \mathbb{Z}_q^n$, can compute $\mathbf{x} \in \{0,1\}^{nk}$ s.t. $\mathbf{G}\mathbf{x} = \mathbf{u}$.

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert SIS: given $\mathbf{u} \in \mathbb{Z}_q^n$, can compute $\mathbf{x} \in \{0,1\}^{nk}$ s.t. $\mathbf{G}\mathbf{x} = \mathbf{u}$.

  More generally, can sample a Gaussian $\mathbf{x} \leftarrow \mathbf{G}^{-1}(\mathbf{u})$.

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert SIS: given $\mathbf{u} \in \mathbb{Z}_q^n$, can compute $\mathbf{x} \in \{0,1\}^{nk}$ s.t. $\mathbf{G}\mathbf{x} = \mathbf{u}$.

  More generally, can sample a Gaussian $\mathbf{x} \leftarrow \mathbf{G}^{-1}(\mathbf{u})$.

  Can generate $(\mathbf{x}, \mathbf{u})$ in two equivalent ways:

$$\text{Gauss} \rightarrow \mathbf{x} \xrightarrow{\ \mathbf{G}\ } \mathbf{u} \quad \equiv \quad \mathbf{x} \xleftarrow{\ \mathbf{G}^{-1}\ } \mathbf{u} \leftarrow \mathbb{Z}_q^n$$

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert LWE: given $\mathbf{v} = \mathbf{x}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{I} \end{smallmatrix} \right] \approx [x_1\ 2x_1\ \cdots\ 2^{k-1}x_1\ \cdots]$, find $\mathbf{x}$.

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert LWE: given $\mathbf{v} = \mathbf{x}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{I} \end{smallmatrix} \right] \approx [x_1\ 2x_1\ \cdots\ 2^{k-1}x_1\ \cdots]$, find $\mathbf{x}$.

  Say $q = 2^k$. Can recover bits of x_1 with errors, then x_2, etc.

Trick #2: Inverting an Easy Function

- A special parity-check matrix: let $\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1} \geq \frac{q}{2}]$ and

$$\mathbf{G} = \begin{bmatrix} \cdots \mathbf{g}^t \cdots & & & \\ & \cdots \mathbf{g}^t \cdots & & \\ & & \ddots & \\ & & & \cdots \mathbf{g}^t \cdots \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}.$$

- Invert LWE: given $\mathbf{v} = \mathbf{x}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{I} \end{smallmatrix} \right] \approx [x_1\ 2x_1\ \cdots\ 2^{k-1}x_1\ \cdots]$, find $\mathbf{x}$.

  Say $q = 2^k$. Can recover bits of x_1 with errors, then x_2, etc.

  (Something similar works for any q.)

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{A}\mathbf{R}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{A}\mathbf{R}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

- Invert LWE: given $\mathbf{v}^t = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{A}' \\ \mathbf{I} \end{smallmatrix} \right]$, recover $\mathbf{s}$ from

$$\mathbf{v}^t \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{s}^t \begin{bmatrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{I} \end{bmatrix} \approx \mathbf{s}_1^t \mathbf{G}.$$

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{A}\mathbf{R}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

- Invert LWE: given $\mathbf{v}^t = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{A}' \\ \mathbf{I} \end{smallmatrix} \right]$, recover $\mathbf{s}$ from

$$\mathbf{v}^t \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \approx \mathbf{s}_1^t \mathbf{G}.$$

- Invert SIS: given target $\mathbf{u}$, output $\mathbf{x} = \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u})$. Then

$$\mathbf{A}'\mathbf{x} = \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{u}) = \mathbf{u}.$$

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{AR}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

- Invert LWE: given $\mathbf{v}^t = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{A}' \\ \mathbf{I} \end{smallmatrix} \right]$, recover $\mathbf{s}$ from

$$\mathbf{v}^t \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \approx \mathbf{s}_1^t \mathbf{G}.$$

- Invert SIS: given target $\mathbf{u}$, output $\mathbf{x} = \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u})$. Then

$$\mathbf{A}'\mathbf{x} = \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{u}) = \mathbf{u}.$$

Problem: $\mathbf{x}$ is 'skewed,' leaks trapdoor $\mathbf{R}$!

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{A}\mathbf{R}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

- Invert LWE: given $\mathbf{v}^t = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{A}' \\ \mathbf{I} \end{smallmatrix} \right]$, recover $\mathbf{s}$ from

$$\mathbf{v}^t \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{s}^t \begin{bmatrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{I} \end{bmatrix} \approx \mathbf{s}_1^t \mathbf{G}.$$

- Invert SIS: given target $\mathbf{u}$, output $\mathbf{x} = \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u})$. Then

$$\mathbf{A}'\mathbf{x} = \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{u}) = \mathbf{u}.$$

Problem: $\mathbf{x}$ is 'skewed,' leaks trapdoor $\mathbf{R}$!

Solution: output $\mathbf{x} = \mathbf{p} + \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u} - \mathbf{A}'\mathbf{p})$ for 'perturbation' $\mathbf{p}$.

Put $\mathbf{G}$ in Public Key $\Rightarrow$ TDF, Signatures, IBE [GPV'08,MP'12]

- Let $\mathbf{A}' = [\mathbf{A} \mid \mathbf{G} - \mathbf{A}\mathbf{R}]$, so $\mathbf{A}' \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{G}$. Trapdoor $= \mathbf{R}$.

- Invert LWE: given $\mathbf{v}^t = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{A}' \\ \mathbf{I} \end{smallmatrix} \right]$, recover $\mathbf{s}$ from

$$\mathbf{v}^t \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] = \mathbf{s}^t \left[\begin{smallmatrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \approx \mathbf{s}_1^t \mathbf{G}.$$

- Invert SIS: given target $\mathbf{u}$, output $\mathbf{x} = \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u})$. Then

$$\mathbf{A}'\mathbf{x} = \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{u}) = \mathbf{u}.$$

Problem: $\mathbf{x}$ is 'skewed,' leaks trapdoor $\mathbf{R}$!

Solution: output $\mathbf{x} = \mathbf{p} + \left[\begin{smallmatrix} \mathbf{R} \\ \mathbf{I} \end{smallmatrix} \right] \cdot \mathbf{G}^{-1}(\mathbf{u} - \mathbf{A}'\mathbf{p})$ for 'perturbation' $\mathbf{p}$.

$$\text{Gauss} \to \mathbf{x} \xrightarrow{\mathbf{A}'} \mathbf{u} \quad \equiv \quad \mathbf{x} \xleftarrow{\mathbf{A}'^{-1}} \mathbf{u} \leftarrow \mathbb{Z}_q^n$$

Put $\mathbf{G}$ in Evaluation Key $\Rightarrow$ FHE [BV'11]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, ciphertext $\mathbf{c} \in \mathbb{Z}_q^n$ is s.t. $\mathbf{s}^t \cdot \mathbf{c} \approx \frac{q+1}{2} \cdot \mu$.

Put $\mathbf{G}$ in Evaluation Key $\Rightarrow$ FHE [BV'11]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, ciphertext $\mathbf{c} \in \mathbb{Z}_q^n$ is s.t. $\mathbf{s}^t \cdot \mathbf{c} \approx \frac{q+1}{2} \cdot \mu$.
- Homomorphic mult:

$$(\mathbf{s} \otimes \mathbf{s})^t \cdot \underbrace{(2\mathbf{c}_1 \otimes \mathbf{c}_2)}_{\mathbf{c}_\times} \approx \frac{q+1}{2} \cdot \mu_1 \mu_2.$$

Problem: $\mathbf{c}_\times$ has dimension n^2!

Put $\mathbf{G}$ in Evaluation Key $\Rightarrow$ FHE [BV'11]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, ciphertext $\mathbf{c} \in \mathbb{Z}_q^n$ is s.t. $\mathbf{s}^t \cdot \mathbf{c} \approx \frac{q+1}{2} \cdot \mu$.
- Homomorphic mult:

$$(\mathbf{s} \otimes \mathbf{s})^t \cdot \underbrace{(2\mathbf{c}_1 \otimes \mathbf{c}_2)}_{\mathbf{c}_\times} \approx \frac{q+1}{2} \cdot \mu_1 \mu_2.$$

  Problem: $\mathbf{c}_\times$ has dimension n^2!

- "Compress" $\mathbf{c}_\times$ by "recrypting:"
  1. Rewrite decryption expression as $(\mathbf{s} \otimes \mathbf{s})^t \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{c}_\times)$.

Put $\mathbf{G}$ in Evaluation Key $\Rightarrow$ FHE [BV'11]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, ciphertext $\mathbf{c} \in \mathbb{Z}_q^n$ is s.t. $\mathbf{s}^t \cdot \mathbf{c} \approx \frac{q+1}{2} \cdot \mu$.
- Homomorphic mult:

$$(\mathbf{s} \otimes \mathbf{s})^t \cdot \underbrace{(2\mathbf{c}_1 \otimes \mathbf{c}_2)}_{\mathbf{c}_\times} \approx \frac{q+1}{2} \cdot \mu_1 \mu_2.$$

Problem: $\mathbf{c}_\times$ has dimension n^2!

- "Compress" $\mathbf{c}_\times$ by "recrypting:"
  1. Rewrite decryption expression as $(\mathbf{s} \otimes \mathbf{s})^t \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{c}_\times)$.
  2. Hide $(\mathbf{s} \otimes \mathbf{s})^t \mathbf{G}$ in an evaluation key $\mathbf{K}$ (having n rows):

$$\mathbf{s}^t \cdot \mathbf{K} \approx (\mathbf{s} \otimes \mathbf{s})^t \mathbf{G}.$$

Put $\mathbf{G}$ in Evaluation Key $\Rightarrow$ FHE [BV'11]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, ciphertext $\mathbf{c} \in \mathbb{Z}_q^n$ is s.t. $\mathbf{s}^t \cdot \mathbf{c} \approx \frac{q+1}{2} \cdot \mu$.
- Homomorphic mult:

$$(\mathbf{s} \otimes \mathbf{s})^t \cdot \underbrace{(2\mathbf{c}_1 \otimes \mathbf{c}_2)}_{\mathbf{c}_\times} \approx \frac{q+1}{2} \cdot \mu_1 \mu_2.$$

Problem: $\mathbf{c}_\times$ has dimension n^2!

- "Compress" $\mathbf{c}_\times$ by "recrypting:"
  1. Rewrite decryption expression as $(\mathbf{s} \otimes \mathbf{s})^t \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{c}_\times)$.
  2. Hide $(\mathbf{s} \otimes \mathbf{s})^t \mathbf{G}$ in an evaluation key $\mathbf{K}$ (having n rows):

$$\mathbf{s}^t \cdot \mathbf{K} \approx (\mathbf{s} \otimes \mathbf{s})^t \mathbf{G}.$$

  3. Then

$$\mathbf{s}^t \cdot \underbrace{\mathbf{K} \cdot \mathbf{G}^{-1}(\mathbf{c}_\times)}_{\mathbf{c}'} \approx (\mathbf{s} \otimes \mathbf{s})^t \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{c}_\times) \approx \mu_1 \mu_2 \cdot \frac{q+1}{2}.$$

Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t \mathbf{A} \approx \mathbf{0}$.

Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t \mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0, 1\}$ as $\mathbf{C} = \mathbf{AR} + \mu \mathbf{G}$. Decryption relation is

$$\mathbf{s}^t \mathbf{C} \approx \mu \cdot \mathbf{s}^t \mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

$$\begin{aligned} \mathbf{s}^t \mathbf{C}_\times &= \mathbf{s}^t \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1 \cdot \mathbf{s}^t \mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1 \mu_2 \cdot \mathbf{s}^t \mathbf{G} \end{aligned}$$

Put $\mathbf{G}$ in Ciphertext $\Rightarrow$ FHE [GSW'13]

- Secret key $\mathbf{s} \in \mathbb{Z}^n$, public key $\mathbf{A}$ satisfies $\mathbf{s}^t\mathbf{A} \approx \mathbf{0}$.
- Encrypt $\mu \in \{0,1\}$ as $\mathbf{C} = \mathbf{A}\mathbf{R} + \mu\mathbf{G}$. Decryption relation is

$$\mathbf{s}^t\mathbf{C} \approx \mu \cdot \mathbf{s}^t\mathbf{G}.$$

- Homomorphic mult: $\mathbf{C}_\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

$$\begin{aligned} \mathbf{s}^t\mathbf{C}_\times &= \mathbf{s}^t\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1 \cdot \mathbf{s}^t\mathbf{G} \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &\approx \mu_1\mu_2 \cdot \mathbf{s}^t\mathbf{G} \end{aligned}$$

Error in $\mathbf{C}_\times$ is $\mathbf{e}_1^t \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + \mu_1 \cdot \mathbf{e}_2^t$.

Asymmetry allows homom mult with additive noise growth. [BV'13]

Concluding Thoughts

- Many more applications:

  PRFs [BPR'12,BLMR'13], ABE [GVW'13,GGHSW'13], Obf & FE [GGHRSW'13], . . .

Concluding Thoughts

- Many more applications:

  PRFs [BPR'12,BLMR'13], ABE [GVW'13,GGHSW'13], Obf & FE [GGHRSW'13], . . .

- Amazing amount of magic from such a small bag of tricks!
  A true case of making strength out of 'weakness.'

Concluding Thoughts

- Many more applications:

  PRFs [BPR'12,BLMR'13], ABE [GVW'13,GGHSW'13], Obf & FE [GGHRSW'13], . . .

- Amazing amount of magic from such a small bag of tricks!
  A true case of making strength out of 'weakness.'

Thanks!