Lattice-Based Cryptography

Chris Peikert
University of Michigan

QCrypt 2016

Agenda

1. Foundations: lattice problems, SIS/LWE and their applications

2. Ring-Based Crypto: NTRU, Ring-SIS/LWE and ideal lattices

3. Practical Implementations: BLISS, NewHope, Frodo, HElib, $\Lambda \circ \lambda$, ...

4. Along the Way: open questions, research directions

Foundations

Lattice-Based Cryptography

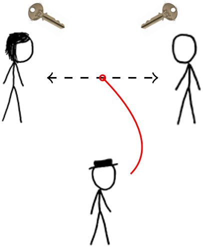
$y = g^x \bmod p$

$N = p \cdot q$

$m^e \bmod N$

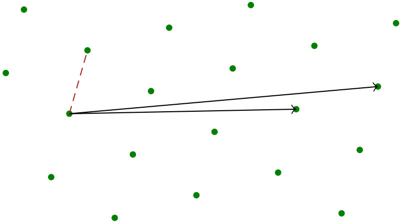
$e(g^a, g^b)$

$\Longrightarrow$

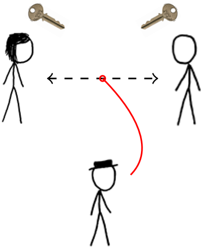


(Images courtesy xkcd.org)

Lattice-Based Cryptography

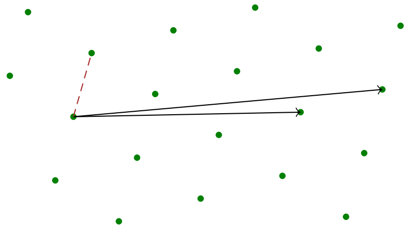


$\Longrightarrow$

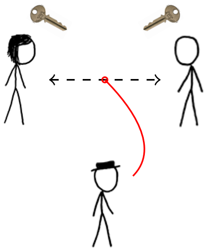


(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

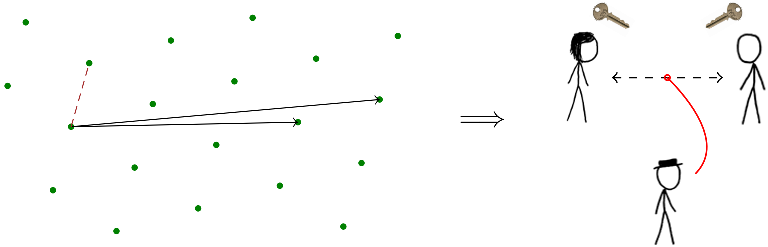


Why?

- Efficient: linear, embarrassingly parallel operations

(Images courtesy xkcd.org)

Lattice-Based Cryptography

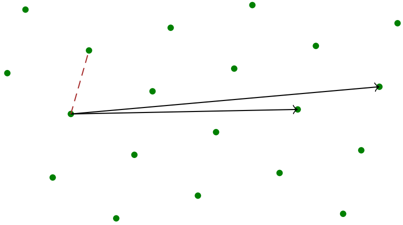


Why?

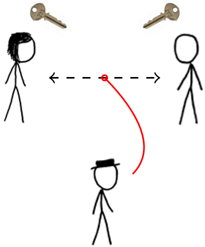
- Efficient: linear, embarrassingly parallel operations
- Resists quantum attacks (so far)

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

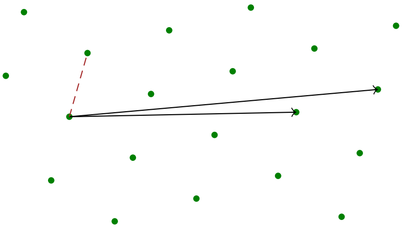


Why?

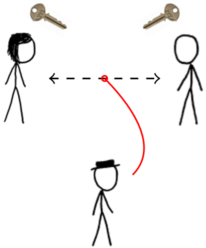
- Efficient: linear, embarrassingly parallel operations
- Resists quantum attacks (so far)
- Security from mild worst-case assumptions

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$



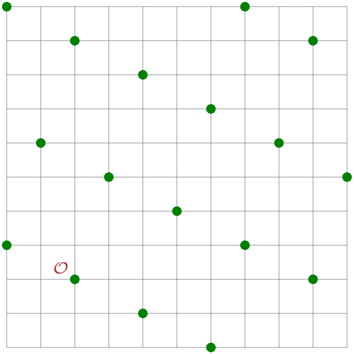
Why?

- Efficient: linear, embarrassingly parallel operations
- Resists quantum attacks (so far)
- Security from mild worst-case assumptions
- Solutions to ‘holy grail’ problems in crypto: FHE and related

(Images courtesy xkcd.org)

What's a Lattice?

- A periodic 'grid' in $\mathbb{Z}^m$. (Formally: full-rank additive subgroup.)

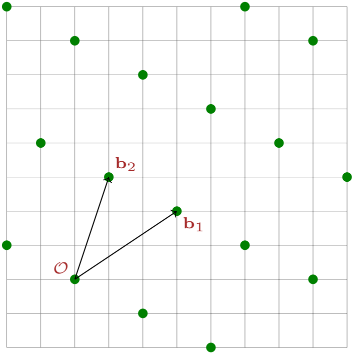


What's a Lattice?

- A periodic 'grid' in $\mathbb{Z}^m$. (Formally: full-rank additive subgroup.)

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

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

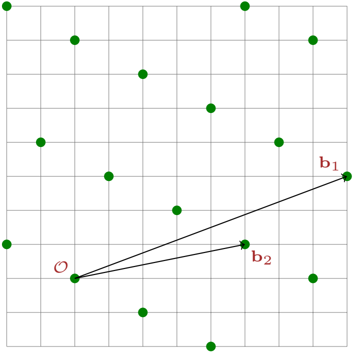


What's a Lattice?

- A periodic 'grid' in $\mathbb{Z}^m$. (Formally: full-rank additive subgroup.)

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

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



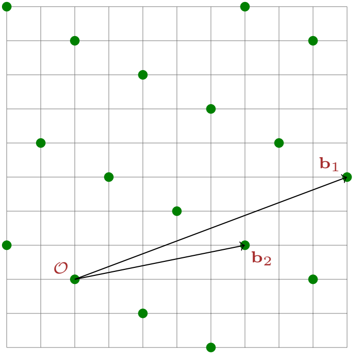
What's a Lattice?

- A periodic 'grid' in $\mathbb{Z}^m$. (Formally: full-rank additive subgroup.)

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

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

(Other representations too . . .)



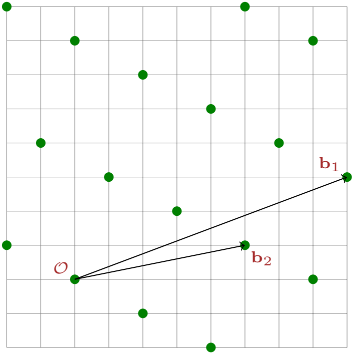
What's a Lattice?

- A periodic 'grid' in $\mathbb{Z}^m$. (Formally: full-rank additive subgroup.)

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

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

(Other representations too ...)



Hard Lattice Problems

- Find/detect 'short' nonzero lattice vectors: (Gap)SVP$_\gamma$, SIVP$_\gamma$
- For $\gamma = \text{poly}(m)$, solving appears to require $2^{\Omega(m)}$ time (and space).

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

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q

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

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q

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

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

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q
- Goal: find nontrivial $z_1, \ldots, z_m \in \{0, \pm 1\}$ 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 [Ajtai'96]

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

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

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

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

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

Collision-Resistant Hash Function

- Set $m > n \log_2 q$. Define 'shrinking' $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$

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

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

- $\mathbb{Z}_q^n = n$-dimensional integer vectors modulo q
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

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

Collision-Resistant Hash Function

- Set $m > n \log_2 q$. Define 'shrinking' $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$

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

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

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

- $\mathbb{Z}_q^n$ = n-dimensional integer vectors modulo q
- Goal: find nontrivial $\mathbf{z} \in \{0, \pm 1\}^m$ such that:

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

Collision-Resistant Hash Function

- Set $m > n \log_2 q$. Define 'shrinking' $f_{\mathbf{A}} \colon \{0,1\}^m \to \mathbb{Z}_q^n$

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

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

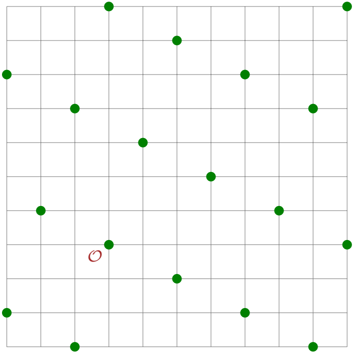
...yields solution $\mathbf{z} = \mathbf{x} - \mathbf{x}' \in \{0, \pm 1\}^m$.

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

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

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ defines a 'q-ary' lattice:

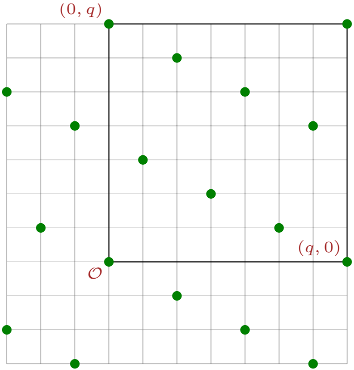
$$\mathcal{L}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m \ : \ \mathbf{A}\mathbf{z} = \mathbf{0}\}$$



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

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ defines a 'q-ary' lattice:

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

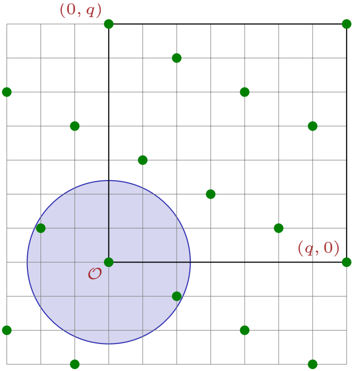


Cool! (But what does this have to do with lattices?)

- $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ defines a 'q-ary' lattice:

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

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

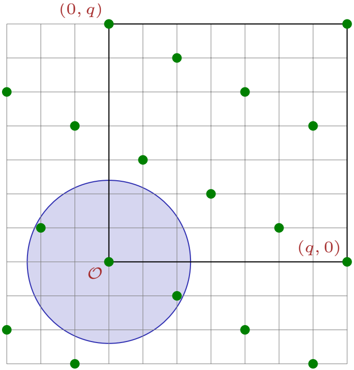


Cool! (But what does this have to do with lattices?)

- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ defines a 'q-ary' lattice:

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

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



Worst-Case to Average-Case Reduction [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 $\mathsf{GapSVP}_{\beta\sqrt{n}}, \mathsf{SIVP}_{\beta\sqrt{n}}$ on any n-dim lattice

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

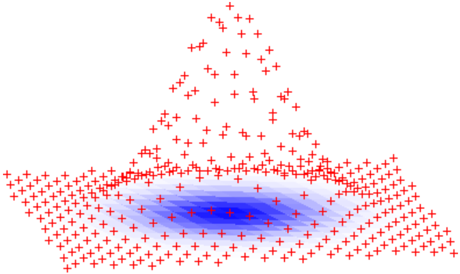
- Generate uniform $vk = \mathbf{A}$ with secret 'trapdoor' $sk = \mathbf{T}$.

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

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

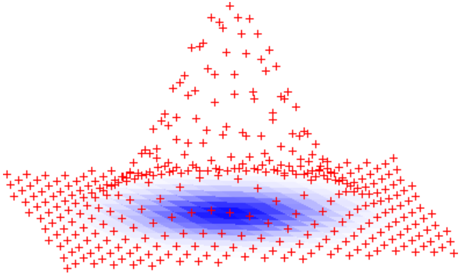
Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

- Generate uniform $vk = \mathbf{A}$ with secret 'trapdoor' $sk = \mathbf{T}$.
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = H(\mu) \in \mathbb{Z}_q^n$.
  Draw $\mathbf{z}$ from a distribution that reveals nothing about secret key:



Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

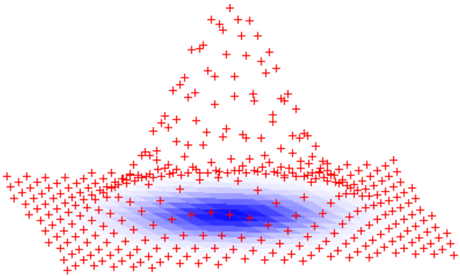
- Generate uniform $vk = \mathbf{A}$ with secret 'trapdoor' $sk = \mathbf{T}$.
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = H(\mu) \in \mathbb{Z}_q^n$.
  Draw $\mathbf{z}$ from a distribution that reveals nothing about secret key:



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

Application: Digital Signatures [GentryPeikertVaikuntanathan'08]

- Generate uniform $vk = \mathbf{A}$ with secret 'trapdoor' $sk = \mathbf{T}$.
- Sign$(\mathbf{T}, \mu)$: use $\mathbf{T}$ to sample a short $\mathbf{z} \in \mathbb{Z}^m$ s.t. $\mathbf{A}\mathbf{z} = H(\mu) \in \mathbb{Z}_q^n$.
  Draw $\mathbf{z}$ from a distribution that reveals nothing about secret key:



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

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

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

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

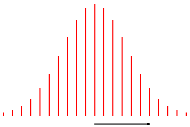
- Parameters: dimension n, modulus $q = \mathrm{poly}(n)$, error distribution
- **Search:** find secret $\mathbf{s} \in \mathbb{Z}_q^n$ given many 'noisy inner products'

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

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

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

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

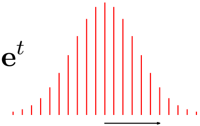


$\sqrt{n} \leq$ error $\ll q$, 'rate' α

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

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

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

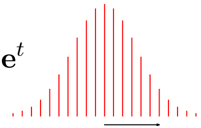


$\sqrt{n} \leq \text{error} \ll q$, 'rate' α

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

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

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



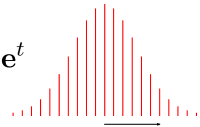
$\sqrt{n} \le$ error $\ll q$, 'rate' α

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

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

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

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \\ & & \end{pmatrix} \quad , \quad (\cdots \quad \mathbf{b}^t \quad \cdots) = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$



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

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

LWE is Hard

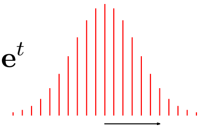
(n/α)-approx *worst case* lattice problems $\leq$ search-LWE $\leq$ decision-LWE $\leq$ crypto

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

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

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

$$\begin{pmatrix} \cdots & \mathbf{A} & \cdots \end{pmatrix} \quad , \quad (\cdots \quad \mathbf{b}^t \quad \cdots) = \mathbf{s}^t \mathbf{A} + \mathbf{e}^t$$



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

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

LWE is Hard

(n/α)-approx *worst case* lattice problems $\leq$ search-LWE $\leq$ decision-LWE $\leq$ crypto

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

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

LWE is Versatile

What kinds of crypto can we do with LWE?

LWE is Versatile

What kinds of crypto can we do with LWE?

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

LWE is Versatile

What kinds of crypto can we do with LWE?

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

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

LWE is Versatile

What kinds of crypto can we do with LWE?

✔ Key Exchange, Public Key Encryption

✔ Oblivious Transfer

✔ Actively Secure Encryption (w/o random oracles)

✔ Block Ciphers, PRFs

- - - - - - - - -

✔✔ Identity-Based Encryption (w/ RO)

✔✔ Hierarchical ID-Based Encryption (w/o RO)

- - - - - - - - -

!!! Fully Homomorphic Encryption

!!! Attribute-Based Encryption for arbitrary policies

and much, much more. . .

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\xrightarrow{\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n}$$

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\xrightarrow{\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n}$$

$$\xleftarrow{\mathbf{v} \approx \mathbf{A} \cdot \mathbf{s} \in \mathbb{Z}_q^n}$$

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\xrightarrow{\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n}$$

$$\xleftarrow{\mathbf{v} \approx \mathbf{A} \cdot \mathbf{s} \in \mathbb{Z}_q^n}$$

$\mathbf{r}^t \cdot \mathbf{v} \approx \mathbf{r}^t\mathbf{A}\mathbf{s}$

$k \approx \mathbf{u}^t \cdot \mathbf{s} \approx \mathbf{r}^t\mathbf{A}\mathbf{s}$

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\xrightarrow{\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n}$$

$$\xleftarrow{\mathbf{v} \approx \mathbf{A} \cdot \mathbf{s} \in \mathbb{Z}_q^n}$$

$\mathbf{r}^t \cdot \mathbf{v} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

$k \approx \mathbf{u}^t \cdot \mathbf{s} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

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

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n \longrightarrow$$

$$\mathbf{v} \approx \mathbf{A} \cdot \mathbf{s} \in \mathbb{Z}_q^n \longleftarrow$$

$\mathbf{r}^t \cdot \mathbf{v} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

$k \approx \mathbf{u}^t \cdot \mathbf{s} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

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

by decision-LWE

Key Exchange from LWE [Regev'05,LP'11]

$\mathbf{r} \leftarrow \mathbb{Z}^n$ (error)

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

$\mathbf{s} \leftarrow \mathbb{Z}^n$ (error)

$$\mathbf{u}^t \approx \mathbf{r}^t \cdot \mathbf{A} \in \mathbb{Z}_q^n \quad \longrightarrow$$

$$\longleftarrow \quad \mathbf{v} \approx \mathbf{A} \cdot \mathbf{s} \in \mathbb{Z}_q^n$$

$\mathbf{r}^t \cdot \mathbf{v} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

$k \approx \mathbf{u}^t \cdot \mathbf{s} \approx \mathbf{r}^t \mathbf{A} \mathbf{s}$

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

by decision-LWE

Efficiency from Rings

SIS/LWE are (Sort Of) Efficient

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

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

SIS/LWE are (Sort Of) Efficient

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

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

SIS/LWE are (Sort Of) Efficient

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

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

- Cryptosystems have rather large keys:

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

SIS/LWE are (Sort Of) Efficient

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

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

- Cryptosystems have rather large keys:

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

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

Wishful Thinking. . .

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

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $\mathbb{Z}_q^{n \times n}$-chunks by $\mathbb{Z}_q^n$.

Wishful Thinking...

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

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $\mathbb{Z}_q^{n\times n}$-chunks by $\mathbb{Z}_q^n$.

Question

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

Wishful Thinking...

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

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $\mathbb{Z}_q^{n \times n}$-chunks by $\mathbb{Z}_q^n$.

Question

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

Wishful Thinking...

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

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $\mathbb{Z}_q^{n \times n}$-chunks by $\mathbb{Z}_q^n$.

Question

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

Answer

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

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

Wishful Thinking...

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

- Get n pseudorandom scalars from just one (cheap) product operation?
- Replace $\mathbb{Z}_q^{n \times n}$-chunks by $\mathbb{Z}_q^n$.

Question

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

Answer

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

  Fast and practical with FFT: $n \log n$ operations mod q.
- Same ring structures used in NTRU cryptosystem [HPS'98], compact one-way / CR hash functions [Mic'02,PR'06,LM'06,...]

LWE Over Rings, Over Simplified

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

LWE Over Rings, Over Simplified

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

LWE Over Rings, Over Simplified

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

$$\begin{array}{lcl} a_1 \leftarrow R_q & , & b_1 = s \cdot a_1 + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = s \cdot a_2 + e_2 \in R_q \\ a_3 \leftarrow R_q & , & b_3 = s \cdot a_3 + e_3 \in R_q \\ & \vdots & \end{array}$$

($e_i \in R$ are 'small')

LWE Over Rings, Over Simplified

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

- **Search**: <u>find</u> secret ring element $s(X) \in R_q$, given:

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

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

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

(classical, any cyclotomic R)

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

(classical, any cyclotomic R)

1. If you can find s given $(a_i\ ,\ b_i)$, then you can find approximately shortest vectors in *any* ideal lattice in R (using a quantum algorithm).

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

1. If you can find s given $(a_i\ ,\ b_i)$, then you can find approximately shortest vectors in *any* ideal lattice in R (using a quantum algorithm).
2. If you can distinguish $(a_i\ ,\ b_i)$ from $(a_i\ ,\ b_i)$, then you can find s.

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

1. If you can find s given (a_i, b_i), then you can find approximately shortest vectors in *any* ideal lattice in R (using a quantum algorithm).
2. If you can distinguish (a_i, b_i) from (a_i, b_i), then you can find s.

- Then:

decision R-LWE $\leq$ lots of crypto

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

(classical, any cyclotomic R)

1. If you can find s given (a_i, b_i), then you can find approximately shortest vectors in *any* ideal lattice in R (using a quantum algorithm).
2. If you can distinguish (a_i, b_i) from (a_i, b_i), then you can find s.

- Then:

decision R-LWE $\leq$ lots of crypto

★ If you can break the crypto, then you can distinguish (a_i, b_i) from (a_i, b_i)...

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{R}^n$. How?

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{R}^n$. How?

1. Obvious answer: 'coefficient embedding'

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in R \quad \mapsto \quad (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{R}^n$. How?

1. Obvious answer: 'coefficient embedding'

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in R \quad \mapsto \quad (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

$+$ is coordinate-wise, but analyzing $\cdot$ is cumbersome.

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{C}^n$. How?

1. Obvious answer: 'coefficient embedding'

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in R \quad \mapsto \quad (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

   $+$ is coordinate-wise, but analyzing $\cdot$ is cumbersome.

2. Minkowski: 'canonical embedding.' Let $\omega = \exp(\pi i/n) \in \mathbb{C}$, so roots of $X^n + 1$ are $\omega^1, \omega^3, \ldots, \omega^{2n-1}$. Embed:

$$a(X) \in R \quad \mapsto \quad (a(\omega^1)\,,\, a(\omega^3)\,, \ldots,\, a(\omega^{2n-1})) \in \mathbb{C}^n$$

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{C}^n$. How?

1. Obvious answer: 'coefficient embedding'

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in R \quad \mapsto \quad (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

   $+$ is coordinate-wise, but analyzing $\cdot$ is cumbersome.

2. Minkowski: 'canonical embedding.' Let $\omega = \exp(\pi i/n) \in \mathbb{C}$, so roots of $X^n + 1$ are $\omega^1, \omega^3, \ldots, \omega^{2n-1}$. Embed:

$$a(X) \in R \quad \mapsto \quad (a(\omega^1)\,,\, a(\omega^3)\,, \ldots,\, a(\omega^{2n-1})) \in \mathbb{C}^n$$

   Both $+$ and $\cdot$ are coordinate-wise.

Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^n + 1)$ for power-of-two n. (Or $R = \mathcal{O}_K$.)
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

To get ideal lattices, embed R and its ideals into $\mathbb{R}^n$. How?

1. Obvious answer: 'coefficient embedding'

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in R \quad \mapsto \quad (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

$+$ is coordinate-wise, but analyzing $\cdot$ is cumbersome.

2. Minkowski: 'canonical embedding.' Let $\omega = \exp(\pi i/n) \in \mathbb{C}$, so roots of $X^n + 1$ are $\omega^1, \omega^3, \ldots, \omega^{2n-1}$. Embed:

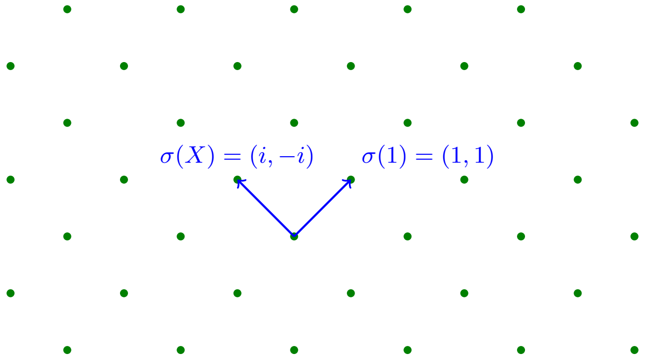
$$a(X) \in R \quad \mapsto \quad (a(\omega^1)\,,\, a(\omega^3)\,, \ldots,\, a(\omega^{2n-1})) \in \mathbb{C}^n$$

Both $+$ and $\cdot$ are coordinate-wise.

Error distribution is Gaussian in canonical embedding.

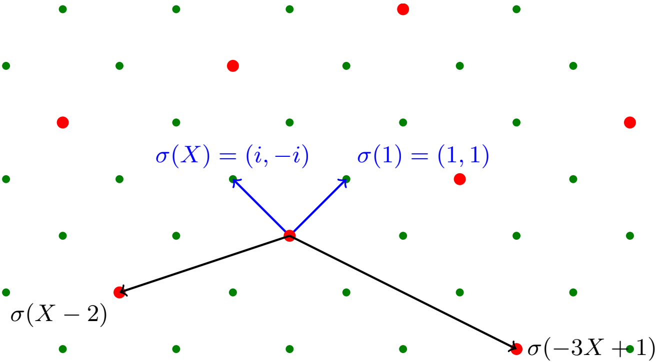
Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^2+1)$. Embeddings map $X \mapsto \pm i$.



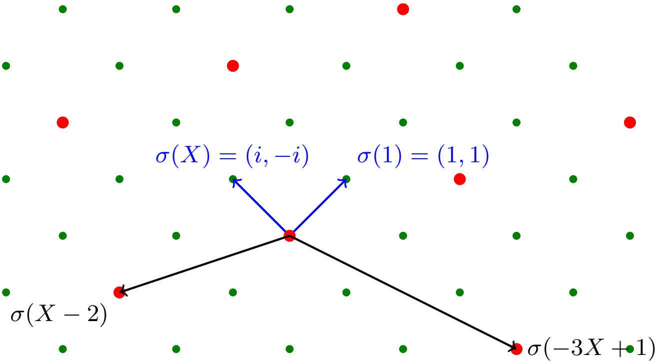
Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^2 + 1)$. Embeddings map $X \mapsto \pm i$.
- $\mathcal{I} = \langle X - 2, -3X + 1 \rangle$ is an ideal in R.



Ideal Lattices

- Say $R = \mathbb{Z}[X]/(X^2+1)$. Embeddings map $X \mapsto \pm i$.
- $\mathcal{I} = \langle X-2, -3X+1 \rangle$ is an ideal in R.



(Approximate) Shortest Vector Problem

- Given (an arbitrary basis of) an arbitrary ideal $\mathcal{I} \subseteq R$, find a nearly shortest nonzero $a \in \mathcal{I}$.

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   Can we solve R-LWE using an oracle for approx-R-SVP?

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   Can we solve R-LWE using an oracle for approx-R-SVP?

   R-LWE samples (a_i, b_i) don't readily translate to ideals in R.

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   Can we solve R-LWE using an oracle for approx-R-SVP?

   R-LWE samples (a_i, b_i) don't readily translate to ideals in R.

2. How hard/easy is poly(n)-R-SVP? (In cyclotomics etc.)

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   Can we solve R-LWE using an oracle for approx-R-SVP?

   R-LWE samples (a_i, b_i) don't readily translate to ideals in R.

2. How hard/easy is poly(n)-R-SVP? (In cyclotomics etc.)

   * Despite much ring structure (e.g., subfields, Galois), no significant improvement versus general n-dim lattices is known.

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   <u>Can we solve R-LWE using an oracle for approx-R-SVP?</u>

   R-LWE samples (a_i, b_i) don't readily translate to ideals in R.

2. <u>How hard/easy is poly(n)-R-SVP? (In cyclotomics etc.)</u>

   * Despite much ring structure (e.g., subfields, Galois), no significant improvement versus general n-dim lattices is known.
   * But $2^{O(\sqrt{n \log n})}$-SVP is quantum poly-time solvable in prime-power cyclotomics, and maybe other rings [CDPR'16,BS'16,K'16,CDW'16]

Complexity of Ideal Lattices

1. We know approx-R-SVP $\leq$ R-LWE (quantumly). Other direction?

   Can we solve R-LWE using an oracle for approx-R-SVP?

   R-LWE samples (a_i, b_i) don't readily translate to ideals in R.

2. How hard/easy is poly(n)-R-SVP? (In cyclotomics etc.)

   - ⋆ Despite much ring structure (e.g., subfields, Galois), no significant improvement versus general n-dim lattices is known.

   - ⋆ But $2^{O(\sqrt{n \log n})}$-SVP is quantum poly-time solvable in prime-power cyclotomics, and maybe other rings [CDPR'16,BS'16,K'16,CDW'16]

   - ⋆ There is a $2^{\Omega(\sqrt{n}/\log n)}$ barrier for the main technique. Can it be circumvented?

Implementations

Key Exchange

- NewHope [ADPS'15]: Ring-LWE key exchange *a la* [LPR'10,P'14], with many optimizations and conjectured ≥ 200-bit quantum security.

Key Exchange

- NewHope [ADPS'15]: Ring-LWE key exchange *a la* [LPR'10,P'14], with many optimizations and conjectured ≥ 200-bit quantum security.

  Comparable to or even faster than state-of-the-art ECDH w/ 128-bit (non-quantum) security.

Key Exchange

- NewHope [ADPS'15]: Ring-LWE key exchange *a la* [LPR'10,P'14], with many optimizations and conjectured ≥ 200-bit quantum security.

  Comparable to or even faster than state-of-the-art ECDH w/ 128-bit (non-quantum) security.

  Google has experimentally deployed NewHope+ECDH in Chrome canary and its own web servers.

Key Exchange

- NewHope [ADPS'15]: Ring-LWE key exchange *a la* [LPR'10,P'14], with many optimizations and conjectured ≥ 200-bit quantum security.

  Comparable to or even faster than state-of-the-art ECDH w/ 128-bit (non-quantum) security.

  Google has experimentally deployed NewHope+ECDH in Chrome canary and its own web servers.

- Frodo [BCDMNNRS'16]: removes the ring! Plain-LWE key exchange, with many tricks and optimizations. Conjectured ≥ 128-bit quantum security.

Key Exchange

- NewHope [ADPS'15]: Ring-LWE key exchange *a la* [LPR'10,P'14], with many optimizations and conjectured ≥ 200-bit quantum security.

  Comparable to or even faster than state-of-the-art ECDH w/ 128-bit (non-quantum) security.

  Google has experimentally deployed NewHope+ECDH in Chrome canary and its own web servers.

- Frodo [BCDMNNRS'16]: removes the ring! Plain-LWE key exchange, with many tricks and optimizations. Conjectured ≥ 128-bit quantum security.

  About 10x slower than NewHope, but only ≈2x slower than ECDH.

Digital Signatures

- Most implementations follow design from [Lyubashevsky'09/'12,...].

Digital Signatures

- Most implementations follow design from [Lyubashevsky'09/'12,...].
- BLISS [DDLL'13]: optimized implementation in this framework.

Digital Signatures

- Most implementations follow design from [Lyubashevsky'09/'12,...].
- BLISS [DDLL'13]: optimized implementation in this framework.
- Compelling efficiency:

System	Sig (Kb)	PK (Kb)	KSign/sec	KVer/sec
RSA-4096	4.0	4.0	0.1	7.5
ECDSA-256	0.5	0.25	9.5	2.5
BLISS	5.6	7.0	8.0	33

(Conjectured ≥ 128 bits of security, `openssl` implementations.)

Other Implementations

- HElib [HaleviShoup]: an 'assembly language' for fully homomorphic encryption (FHE).

Other Implementations

- HElib [HaleviShoup]: an ‘assembly language’ for fully homomorphic encryption (FHE).

  Implements many advanced FHE features, holds most speed records

Other Implementations

- HElib [HaleviShoup]: an 'assembly language' for fully homomorphic encryption (FHE).

  Implements many advanced FHE features, holds most speed records

- $\Lambda \circ \lambda$ (L O L) [CrockettPeikert'16]: a general-purpose, high-level framework aimed at advanced lattice cryptosystems.

Other Implementations

- HElib [HaleviShoup]: an 'assembly language' for fully homomorphic encryption (FHE).

  Implements many advanced FHE features, holds most speed records

- $\Lambda\circ\lambda$ (L O L) [CrockettPeikert'16]: a general-purpose, high-level framework aimed at advanced lattice cryptosystems.

  Focuses on modularity, safety, and consistency with best theory.

Conclusions

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

Conclusions

- Lattices are a very attractive foundation for ‘post-quantum’ crypto, both ‘basic’ and ‘advanced.’
- Cryptanalysis/security estimates for concrete parameters is subtle and ongoing, but maturing.

Conclusions

- Lattices are a very attractive foundation for 'post-quantum' crypto, both 'basic' and 'advanced.'
- Cryptanalysis/security estimates for concrete parameters is subtle and ongoing, but maturing.
- A big success story for rigorous theory and practical engineering alike!

Conclusions

- Lattices are a very attractive foundation for 'post-quantum' crypto, both 'basic' and 'advanced.'
- Cryptanalysis/security estimates for concrete parameters is subtle and ongoing, but maturing.
- A big success story for rigorous theory and practical engineering alike!

Thanks!