Lattice-Based Cryptography: Ring-Based Primitives and Open Problems

Chris Peikert
Georgia Institute of Technology

crypt@b-it 2013

SIS [Ajtai'96,...] and LWE [Regev'05]

<u>SIS</u>

find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$

<u>LWE</u>

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

SIS [Ajtai'96,...] and LWE [Regev'05]

SIS	LWE
find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$	$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$

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

SIS [Ajtai'96,...] and LWE [Regev'05]

SIS

find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$

- '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 [Ajtai'96,...] and LWE [Regev'05]

SIS

find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$

- '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 [Ajtai'96,...] and LWE [Regev'05]

SIS	LWE
find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{Az} = \mathbf{0}$	$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ 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 $\mathbf{s}, \mathbf{e}$

SIS [Ajtai'96,. . .] and LWE [Regev'05]

SIS

find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- Applications: OWF / CRHF, signatures, ID schemes

'minicrypt'

LWE

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

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

SIS [Ajtai'96,...] and LWE [Regev'05]

SIS

find short $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{A}\mathbf{z} = \mathbf{0}$

- 'Computational' (search) problem *a la* factoring, CDH
- Many valid solutions $\mathbf{z}$
- Applications: OWF / CRHF, signatures, ID schemes

'minicrypt'

LWE

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

- 'Decisional' problem *a la* QR, DCR, DDH
- Unique solution $\mathbf{s}, \mathbf{e}$
- Applications: PKE, OT, ID-based encryption, FHE, ...

'CRYPTOMANIA'

SIS/LWE are Efficient (. . . sort of)

$$\begin{pmatrix} — & \mathbf{s}^t & — \end{pmatrix} \begin{pmatrix} | \\ \mathbf{a} \\ | \end{pmatrix} + e = b \in \mathbb{Z}_q$$

- Each pseudorandom scalar b requires an n-dim inner product

SIS/LWE are Efficient (. . . sort of)

$$\begin{pmatrix} \text{—} & \mathbf{s}^t & \text{—} \end{pmatrix} \begin{pmatrix} | \\ \mathbf{a} \\ | \end{pmatrix} + e \; = \; b \in \mathbb{Z}_q$$

- Each pseudorandom scalar b requires an n-dim inner product
- Can amortize each $\mathbf{a}$ over many secrets $\mathbf{s}_i$, but still $\tilde{O}(n)$ work per scalar b.

SIS/LWE are Efficient (...sort of)

$$\begin{pmatrix} — & \mathbf{s}^t & — \end{pmatrix} \begin{pmatrix} | \\ \mathbf{a} \\ | \end{pmatrix} + e \; = \; b \in \mathbb{Z}_q$$

- Each pseudorandom scalar b requires an n-dim inner product
- Can amortize each $\mathbf{a}$ over many secrets $\mathbf{s}_i$, but still $\tilde{O}(n)$ work per scalar b.

- Crypto functions have rather large key sizes: $\Omega(n^2)$ bits

$$pk = \underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \\ & & \end{pmatrix}}_{m \approx n \log q}$$

SIS/LWE are Efficient (. . . sort of)

$$\left(\text{---}\ \mathbf{s}^t\ \text{---}\right)\begin{pmatrix} | \\ \mathbf{a} \\ | \end{pmatrix} + e \;=\; b \in \mathbb{Z}_q$$

- Each pseudorandom scalar b requires an n-dim inner product
- Can amortize each $\mathbf{a}$ over many secrets $\mathbf{s}_i$, but still $\tilde{O}(n)$ work per scalar b.

- Crypto functions have rather large key sizes: $\Omega(n^2)$ bits

$$pk = \underbrace{\begin{pmatrix} \cdots & \mathbf{A} & \cdots \\ & & \end{pmatrix}}_{m \approx n \log q}$$

- Can fix $\mathbf{A}$ for all users, but still $\tilde{\Omega}(n^2)$ time to evaluate functions.

Wishful Thinking. . .

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

$$\begin{pmatrix} | \\ \mathbf{s} \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + \begin{pmatrix} | \\ \mathbf{e} \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{b} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

- SIS: n-dimensional $\mathbf{x}_i$, and $m \approx \log q$

Wishful Thinking...

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

$$\begin{pmatrix} | \\ \mathbf{s} \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + \begin{pmatrix} | \\ \mathbf{e} \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{b} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

- SIS: n-dimensional $\mathbf{x}_i$, and $m \approx \log q$
- LWE: each $\star$ operation yields n pseudorandom scalars

Wishful Thinking...

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

$$\begin{pmatrix} | \\ \mathbf{s} \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + \begin{pmatrix} | \\ \mathbf{e} \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{b} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

- SIS: n-dimensional $\mathbf{x}_i$, and $m \approx \log q$
- LWE: each $\star$ operation yields n pseudorandom scalars

Key Question

- How to define '$\star$' so SIS and LWE are fast and secure?

Wishful Thinking…

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

$$\begin{pmatrix} | \\ \mathbf{s} \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + \begin{pmatrix} | \\ \mathbf{e} \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{b} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

- SIS: n-dimensional $\mathbf{x}_i$, and $m \approx \log q$
- LWE: each $\star$ operation yields n pseudorandom scalars

Key Question

- How to define '$\star$' so SIS and LWE are fast and secure?
- Careful: coordinate-wise multiplication is not secure!

Wishful Thinking...

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

$$\begin{pmatrix} | \\ \mathbf{s} \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} + \begin{pmatrix} | \\ \mathbf{e} \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{b} \\ | \end{pmatrix} \in \mathbb{Z}_q^n$$

- SIS: n-dimensional $\mathbf{x}_i$, and $m \approx \log q$
- LWE: each $\star$ operation yields n pseudorandom scalars

Key Question

- How to define '$\star$' so SIS and LWE are fast and secure?
- Careful: coordinate-wise multiplication is not secure!
- Answer: multiplication in a suitable polynomial ring.

A First Attempt

- Define $R := \mathbb{Z}[X]/(X^n - 1)$ and $R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$, as in NTRU [HPS'98]

A First Attempt

- Define $R := \mathbb{Z}[X]/(X^n - 1)$ and $R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$, as in NTRU [HPS'98]
- Multiplication $\star$ in R (or R_q) is "cyclic convolution:"

$$a(X) \cdot b(X) \leftrightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_2 \\ & \cdots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}}_{\mathsf{rot}(\mathbf{a})} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

A First Attempt

- Define $R := \mathbb{Z}[X]/(X^n - 1)$ and $R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$, as in NTRU [HPS'98]
- Multiplication $\star$ in R (or R_q) is "cyclic convolution:"

$$a(X) \cdot b(X) \leftrightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_2 \\ & \cdots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}}_{\mathsf{rot}(\mathbf{a})} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

There are sub-quadratic algorithms for computing $\star$ (later).

A First Attempt

- Define $R := \mathbb{Z}[X]/(X^n - 1)$ and $R_q := R/qR = \mathbb{Z}_q[X]/(X^n - 1)$, as in NTRU [HPS'98]
- Multiplication $\star$ in R (or R_q) is "cyclic convolution:"

$$a(X) \cdot b(X) \leftrightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_2 \\ & \cdots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}}_{\mathsf{rot}(\mathbf{a})} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

  There are sub-quadratic algorithms for computing $\star$ (later).

- For 'short' $\mathbf{x}_i \in R$, is this ring-SIS function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

- [PR'06,LM'06]: the function is not collision resistant!

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

- [PR'06,LM'06]: the function is not collision resistant!
  - With prob $1/q$, we have $a(1) = a_0 + a_1 + \cdots + a_{n-1} = 0 \in \mathbb{Z}_q$.

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

- [PR'06,LM'06]: the function is not collision resistant!
  - With prob $1/q$, we have $a(1) = a_0 + a_1 + \cdots + a_{n-1} = 0 \in \mathbb{Z}_q$.
  - Then for $\mathbf{x} = \mathbf{1}$, we have $\mathbf{a} \star \mathbf{x} = \mathrm{rot}(\mathbf{a}) \cdot \mathbf{x} = \mathbf{0} \in R_q$.

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

- [PR'06,LM'06]: the function is not collision resistant!
  - With prob $1/q$, we have $a(1) = a_0 + a_1 + \cdots + a_{n-1} = 0 \in \mathbb{Z}_q$.
  - Then for $\mathbf{x} = \mathbf{1}$, we have $\mathbf{a} \star \mathbf{x} = \text{rot}(\mathbf{a}) \cdot \mathbf{x} = \mathbf{0} \in R_q$.
  - Algebraically,
    $(X-1)|a(X) \Rightarrow a(X)(1 + X + \cdots + X^{n-1}) = 0 \bmod (X^n - 1)$.

A First Attempt, Continued

- For 'short' $\mathbf{x}_i \in R$, is this 'ring-SIS' function one-way? Coll. resistant?

$$\begin{pmatrix} | \\ \mathbf{a}_1 \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_1 \\ | \end{pmatrix} + \cdots + \begin{pmatrix} | \\ \mathbf{a}_m \\ | \end{pmatrix} \star \begin{pmatrix} | \\ \mathbf{x}_m \\ | \end{pmatrix} = \begin{pmatrix} | \\ \mathbf{u} \\ | \end{pmatrix} \in R_q$$

- [Micciancio'02]: the function is one-way, if SVP_γ on ideal lattices in $R = \mathbb{Z}[X]/(X^n - 1)$ is hard in the worst case.

- [PR'06,LM'06]: the function is not collision resistant!
  - ⋆ With prob $1/q$, we have $a(1) = a_0 + a_1 + \cdots + a_{n-1} = 0 \in \mathbb{Z}_q$.
  - ⋆ Then for $\mathbf{x} = \mathbf{1}$, we have $\mathbf{a} \star \mathbf{x} = \text{rot}(\mathbf{a}) \cdot \mathbf{x} = \mathbf{0} \in R_q$.
  - ⋆ Algebraically, $(X-1) | a(X) \Rightarrow a(X)(1 + X + \cdots + X^{n-1}) = 0 \bmod (X^n - 1)$.

- Main problem: $R = \mathbb{Z}[X]/(X^n - 1)$ is not an integral domain, because $X^n - 1$ is reducible.

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.
  ($X^n + 1$ is irreducible over $\mathbb{Z}$, but "splits completely" over $\mathbb{Z}_q$.)

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.

  ($X^n + 1$ is irreducible over $\mathbb{Z}$, but "splits completely" over $\mathbb{Z}_q$.)

- Multiplication $\star$ in R (or R_q) is "anti-cyclic convolution"

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ & \dots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.

  ($X^n + 1$ is irreducible over $\mathbb{Z}$, but "splits completely" over $\mathbb{Z}_q$.)

- Multiplication $\star$ in R (or R_q) is "anti-cyclic convolution"

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ & \dots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

- Multiplication in $O(n \log n)$ time: use "FFT" over $\mathbb{Z}_q$

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.
  ($X^n + 1$ is irreducible over $\mathbb{Z}$, but "splits completely" over $\mathbb{Z}_q$.)
- Multiplication $\star$ in R (or R_q) is "anti-cyclic convolution"

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ & \dots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

- Multiplication in $O(n \log n)$ time: use "FFT" over $\mathbb{Z}_q$

Theorem [PR'06,LM'06]

- The ring-SIS function is collision resistant,
  if SVP_γ on ideal lattices in R is hard in the worst case.

A Better Construction

- $R := \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/qR$, for $n = 2^k$ and $q = 1 \bmod 2n$.

  ($X^n + 1$ is irreducible over $\mathbb{Z}$, but "splits completely" over $\mathbb{Z}_q$.)

- Multiplication $\star$ in R (or R_q) is "anti-cyclic convolution"

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \star \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ & \dots & & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$$

- Multiplication in $O(n \log n)$ time: use "FFT" over $\mathbb{Z}_q$

Theorem [LPR'10]

- Ring-LWE is pseudorandom if SVP_γ on ideal lattices in R is quantumly hard in the worst case.

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

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

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

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

  'Expansion factor' ϕ can bound $\|a \star b\| \leq \phi \cdot \|a\| \cdot \|b\|$, but is often loose, and doesn't help with distributions.

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

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

  'Expansion factor' ϕ can bound $\|a \star b\| \leq \phi \cdot \|a\| \cdot \|b\|$, but is often loose, and doesn't help with distributions.

- [Minkowski'1800s,...]: 'canonical embedding' σ. Let $\omega = \exp(\pi i/n)$:

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

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

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

  'Expansion factor' ϕ can bound $\|a \star b\| \leq \phi \cdot \|a\| \cdot \|b\|$, but is often loose, and doesn't help with distributions.

- [Minkowski'1800s,...]: 'canonical embedding' σ. Let $\omega = \exp(\pi i / n)$:

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

  Both $+$ and $\star$ are coordinate-wise! Nice geometric behavior.

A Few Words on Ideal Lattices

- Recall example ring $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$.
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\star$ with R.

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

- 'Coefficient embedding' [HPS'98,M'02,PR'06,LM'06,G'09,...]:

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

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

  'Expansion factor' ϕ can bound $\|a \star b\| \leq \phi \cdot \|a\| \cdot \|b\|$, but is often loose, and doesn't help with distributions.

- [Minkowski'1800s,...]: 'canonical embedding' σ. Let $\omega = \exp(\pi i/n)$:

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

  Both $+$ and $\star$ are coordinate-wise! Nice geometric behavior.

- Lengths, Gaussians, etc. are all defined in terms of σ.

Some of My Favorite Open Problems

1. Classical hardness of LWE, subsuming the quantum reduction of [Regev'05]: $q = \text{poly}(n)$, based on GapSVP and SIVP

Some of My Favorite Open Problems

1. Classical hardness of LWE, subsuming the quantum reduction of [Regev'05]: $q = \mathsf{poly}(n)$, based on GapSVP and SIVP

2. Adaptive security for IBE, with good key sizes (e.g., $O(1)$ $\mathbf{A}$s).

   Adapt [Waters'09] from bilinear setting?

Some of My Favorite Open Problems

1. Classical hardness of LWE, subsuming the quantum reduction of [Regev'05]: $q = \text{poly}(n)$, based on GapSVP and SIVP

2. Adaptive security for IBE, with good key sizes (e.g., $O(1)$ $\mathbf{A}$s).

   Adapt [Waters'09] from bilinear setting?

3. Provable hardness for small parameters for related problems like Learning With Rounding and PRFs [BPR'12]

Some of My Favorite Open Problems

1. Classical hardness of LWE, subsuming the quantum reduction of [Regev'05]: $q = \text{poly}(n)$, based on GapSVP and SIVP

2. Adaptive security for IBE, with good key sizes (e.g., $O(1)$ $\mathbf{A}$s).

   Adapt [Waters'09] from bilinear setting?

3. Provable hardness for small parameters for related problems like Learning With Rounding and PRFs [BPR'12]

4. Multilinear maps [GGH'12] from standard lattice assumptions (LWE)

Some of My Favorite Open Problems

1. Classical hardness of LWE, subsuming the quantum reduction of [Regev'05]: $q = \text{poly}(n)$, based on GapSVP and SIVP

2. Adaptive security for IBE, with good key sizes (e.g., $O(1)$ $\mathbf{A}$s).

   Adapt [Waters'09] from bilinear setting?

3. Provable hardness for small parameters for related problems like Learning With Rounding and PRFs [BPR'12]

4. Multilinear maps [GGH'12] from standard lattice assumptions (LWE)

5. Anything nontrivial about ideal lattices: attacks, hardness, applications, . . .

Parting Thoughts

- You now have a solid foundation in the central concepts and techniques used in lattice-based cryptography.

Parting Thoughts

- You now have a solid foundation in the central concepts and techniques used in lattice-based cryptography.
- The field is vibrant: there are endless unanswered questions, and endless new discoveries to be made.

Parting Thoughts

- You now have a solid foundation in the central concepts and techniques used in lattice-based cryptography.
- The field is vibrant: there are endless unanswered questions, and endless new discoveries to be made.
- Enjoy the cryptography!

Parting Thoughts

- You now have a solid foundation in the central concepts and techniques used in lattice-based cryptography.
- The field is vibrant: there are endless unanswered questions, and endless new discoveries to be made.
- Enjoy the cryptography!

Thanks!