Cryptography from Rings

Chris Peikert

University of Michigan

HEAT Summer School
13 Oct 2015

Agenda

1. Polynomial rings, ideal lattices and Ring-LWE
2. Basic Ring-LWE encryption
3. Fully homomorphic encryption

Selected bibliography:

LPR'10 and '13 V. Lyubashevsky, C. Peikert, O. Regev.
"On Ideal Lattices and Learning with Errors Over Rings," Eurocrypt'10 and JACM'13.
"A Toolkit for Ring-LWE Cryptography," Eurocrypt'13.

BV'11 Z. Brakerski and V. Vaikuntanathan.
"Fully Homomorphic Encryption from Ring-LWE..." CRYPTO'11.

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction, one-way function & public-key encryption (very inefficient)

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction,
one-way function & public-key encryption (very inefficient)

1996 NTRU efficient "ring-based" encryption (heuristic security)

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction, one-way function & public-key encryption (very inefficient)

1996 NTRU efficient "ring-based" encryption (heuristic security)

2002 Micciancio's ring-based one-way function with worst-case hardness from ideal lattices (no encryption)

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction, one-way function & public-key encryption (very inefficient)

1996 NTRU efficient "ring-based" encryption (heuristic security)

2002 Micciancio's ring-based one-way function with worst-case hardness from ideal lattices (no encryption)

2005 Regev's LWE: encryption with worst-case hardness (inefficient)

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction, one-way function & public-key encryption (very inefficient)

1996 NTRU efficient "ring-based" encryption (heuristic security)

2002 Micciancio's ring-based one-way function with worst-case hardness from ideal lattices (no encryption)

2005 Regev's LWE: encryption with worst-case hardness (inefficient)

2008– Countless applications of LWE (still inefficient)

Rings in Lattice Cryptography (A Selective History)

1996-97 Ajtai(-Dwork) worst-case/average-case reduction, one-way function & public-key encryption (very inefficient)

1996 NTRU efficient “ring-based” encryption (heuristic security)

2002 Micciancio’s ring-based one-way function with worst-case hardness from ideal lattices (no encryption)

2005 Regev’s LWE: encryption with worst-case hardness (inefficient)

2008– Countless applications of LWE (still inefficient)

2010 Ring-LWE: very efficient encryption, worst-case hardness ()

Cyclotomic Rings

- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m.
  I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.

Cyclotomic Rings

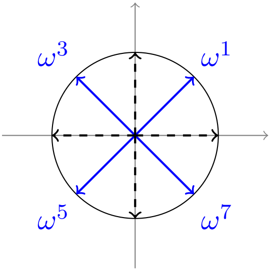
- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m.
  I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.
- Fact: $X^m - 1 = \prod_{d|m} \Phi_d(X)$ for irreducible

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}.$$

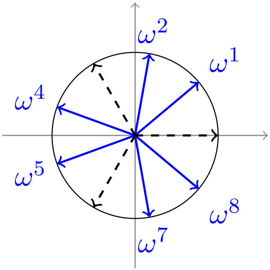
Cyclotomic Rings

- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m. I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.
- Fact: $X^m - 1 = \prod_{d|m} \Phi_d(X)$ for irreducible

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}.$$



$\Phi_8(X) = 1 + X^4$



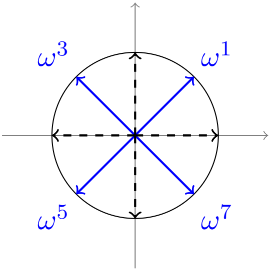
$\Phi_9(X) = 1 + X^3 + X^6$

Cyclotomic Rings

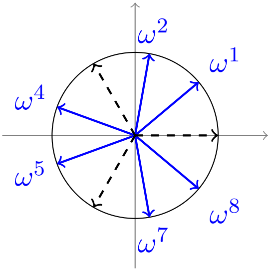
- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m.
  I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.
- Fact: $X^m - 1 = \prod_{d|m} \Phi_d(X)$ for irreducible

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}.$$

  Therefore, $\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/\Phi_m(X)$ via $\zeta \leftrightarrow X$.



$\Phi_8(X) = 1 + X^4$



$\Phi_9(X) = 1 + X^3 + X^6$

Cyclotomic Rings

- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m.
  I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.
- Fact: $X^m - 1 = \prod_{d|m} \Phi_d(X)$ for irreducible

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}.$$

  Therefore, $\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/\Phi_m(X)$ via $\zeta \leftrightarrow X$.
- We have $\deg(R) = \deg(\Phi_m) = n := \varphi(m)$,
  and R has a $\mathbb{Z}$-basis $\{\zeta^0, \zeta^1, \ldots, \zeta^{n-1}\}$: the power basis.
  This corresponds to $\mathbb{Z}[X]/\Phi_m(X)$ representation.

Cyclotomic Rings

- The mth cyclotomic ring is $R = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_m$ has order m.
  I.e., $\zeta^m = 1$ and $\zeta^j \neq 1$ for $1 < j < m$.

- Fact: $X^m - 1 = \prod_{d|m} \Phi_d(X)$ for irreducible

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}.$$

  Therefore, $\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/\Phi_m(X)$ via $\zeta \leftrightarrow X$.

- We have $\deg(R) = \deg(\Phi_m) = n := \varphi(m)$,
  and R has a $\mathbb{Z}$-basis $\{\zeta^0, \zeta^1, \ldots, \zeta^{n-1}\}$: the power basis.
  This corresponds to $\mathbb{Z}[X]/\Phi_m(X)$ representation.

- There are other $\mathbb{Z}$-bases, e.g., $\{\zeta_p^0, \ldots \zeta_p^{k-1}, \zeta_p^{k+1}, \ldots, \zeta_p^{p-1}\}$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."
So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."
So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Reduction to the Prime-Power Case

- Say m has prime-power factorization $m_1 \cdots m_\ell$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."
So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Reduction to the Prime-Power Case

- Say m has prime-power factorization $m_1 \cdots m_\ell$. By $\zeta_{m_i} \leftrightarrow \zeta_m^{m/m_i}$,

$$R = \mathbb{Z}[\zeta_m] \;\cong\; \mathbb{Z}[\zeta_{m_1}, \ldots, \zeta_{m_\ell}].$$

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."
So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Reduction to the Prime-Power Case

- Say m has prime-power factorization $m_1 \cdots m_\ell$. By $\zeta_{m_i} \leftrightarrow \zeta_m^{m/m_i}$,

$$R = \mathbb{Z}[\zeta_m] \;\cong\; \mathbb{Z}[\zeta_{m_1}, \ldots, \zeta_{m_\ell}].$$

- R has powerful $\mathbb{Z}$-basis $\{\zeta_{m_1}^{j_1} \cdots \zeta_{m_\ell}^{j_\ell}\} = \bigotimes \{\zeta_{m_i}^{j_i}\}, \;\; 0 \leq j_i < \varphi(m_i)$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."
So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Reduction to the Prime-Power Case

- Say m has prime-power factorization $m_1 \cdots m_\ell$. By $\zeta_{m_i} \leftrightarrow \zeta_m^{m/m_i}$,
$$R = \mathbb{Z}[\zeta_m] \;\cong\; \mathbb{Z}[\zeta_{m_1}, \ldots, \zeta_{m_\ell}].$$
- R has powerful $\mathbb{Z}$-basis $\{\zeta_{m_1}^{j_1} \cdots \zeta_{m_\ell}^{j_\ell}\} = \bigotimes \{\zeta_{m_i}^{j_i}\}$, $0 \le j_i < \varphi(m_i)$.
In general, powerful basis $\neq$ power basis $\{\zeta_m^j\}$, $0 \le j < \varphi(m)$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$.
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$.

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more "dense."

So it can be cumbersome to work with $\mathbb{Z}[X]/\Phi_m(X)$.

Reduction to the Prime-Power Case

- Say m has prime-power factorization $m_1 \cdots m_\ell$. By $\zeta_{m_i} \leftrightarrow \zeta_m^{m/m_i}$,

$$R = \mathbb{Z}[\zeta_m] \;\cong\; \mathbb{Z}[\zeta_{m_1}, \ldots, \zeta_{m_\ell}].$$

- R has powerful $\mathbb{Z}$-basis $\{\zeta_{m_1}^{j_1} \cdots \zeta_{m_\ell}^{j_\ell}\} = \bigotimes \{\zeta_{m_i}^{j_i}\},\ 0 \le j_i < \varphi(m_i)$.

  In general, powerful basis $\neq$ power basis $\{\zeta_m^j\},\ 0 \le j < \varphi(m)$.

- Bottom line: we can efficiently reduce operations in R to independent operations in prime-power cyclotomics $\mathbb{Z}[\zeta_{m_i}]$.

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use?

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!
- $R = \mathbb{Z}[\zeta_m]$ has $n = \varphi(m)$ ring embeddings into $\mathbb{C}$, given by mapping ζ_m to each primitive mth root of unity:

$$\sigma_i(\zeta_m) = \omega_m^i \in \mathbb{C},\ i \in \mathbb{Z}_m^*.$$

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!
- $R = \mathbb{Z}[\zeta_m]$ has $n = \varphi(m)$ ring embeddings into $\mathbb{C}$, given by mapping ζ_m to each primitive mth root of unity:

$$\sigma_i(\zeta_m) = \omega_m^i \in \mathbb{C}, \ i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* $\sigma \colon R \to \mathbb{C}^n$ is $\sigma(a) = (\sigma_i(a))_{i \in \mathbb{Z}_m^*}$.

  Canonical because it is independent of representation (basis) of R.

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!
- $R = \mathbb{Z}[\zeta_m]$ has $n = \varphi(m)$ ring embeddings into $\mathbb{C}$, given by mapping ζ_m to each primitive mth root of unity:

$$\sigma_i(\zeta_m) = \omega_m^i \in \mathbb{C}, \ i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* $\sigma \colon R \to \mathbb{C}^n$ is $\sigma(a) = (\sigma_i(a))_{i \in \mathbb{Z}_m^*}$.

  Canonical because it is independent of representation (basis) of R.
- Define all geometric quantities using σ: e.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!
- $R = \mathbb{Z}[\zeta_m]$ has $n = \varphi(m)$ ring embeddings into $\mathbb{C}$, given by mapping ζ_m to each primitive mth root of unity:
  $$\sigma_i(\zeta_m) = \omega_m^i \in \mathbb{C}, \; i \in \mathbb{Z}_m^*.$$
- The *canonical embedding* $\sigma \colon R \to \mathbb{C}^n$ is $\sigma(a) = (\sigma_i(a))_{i \in \mathbb{Z}_m^*}$.
  Canonical because it is independent of representation (basis) of R.
- Define all geometric quantities using σ: e.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Nice Properties

✔ Under σ, both $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

Canonical Geometry of R

- Need a geometry and notion of "short" for ring elements.
  Use coefficient vector w.r.t. a $\mathbb{Z}$-basis? Which basis to use? None!
- $R = \mathbb{Z}[\zeta_m]$ has $n = \varphi(m)$ ring embeddings into $\mathbb{C}$, given by mapping ζ_m to each primitive mth root of unity:

$$\sigma_i(\zeta_m) = \omega_m^i \in \mathbb{C}, \; i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* $\sigma \colon R \to \mathbb{C}^n$ is $\sigma(a) = (\sigma_i(a))_{i \in \mathbb{Z}_m^*}$.

  Canonical because it is independent of representation (basis) of R.
- Define all geometric quantities using σ: e.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Nice Properties

✔ Under σ, both $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

This yields the "expansion" bound

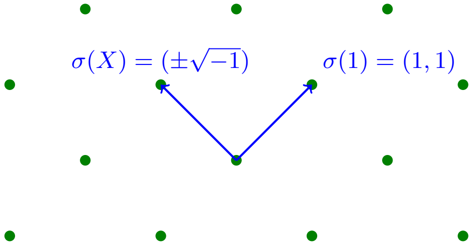
$$\|a \cdot b\|_2 \leq \|a\|_\infty \cdot \|b\|_2 , \quad \text{where } \|a\|_\infty = \max_i |\sigma_i(a)|.$$

Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1 + X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$

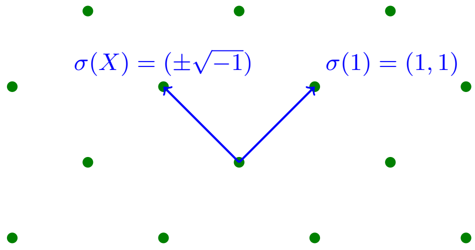
Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$



Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$

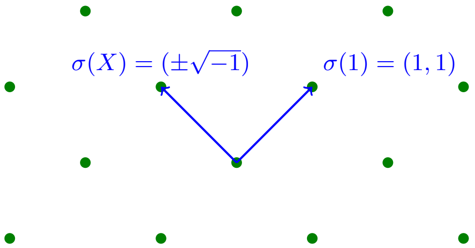


In Any 2^k-th Cyclotomic...

✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.

Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$

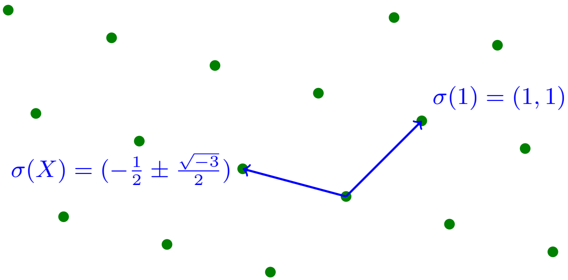


In Any 2^k-th Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- ✔ Power basis $\{1, X, \ldots, X^{n-1}\}$ is orthogonal under embedding σ.
  So power & canonical geometries are equivalent (up to $\sqrt{n}$ scaling).

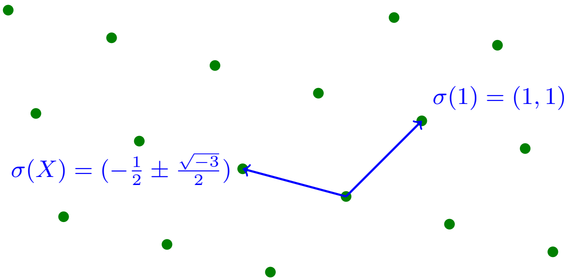
Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$



Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1+X+X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

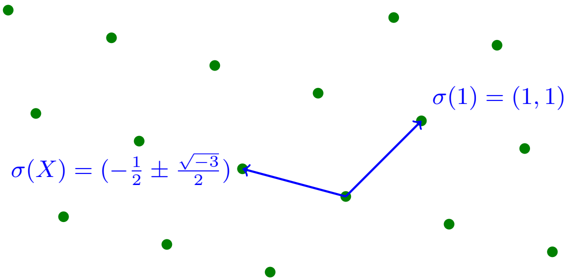


In Any Cyclotomic...

✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

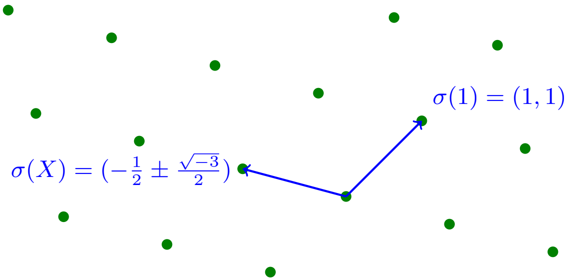


In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1+X+X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

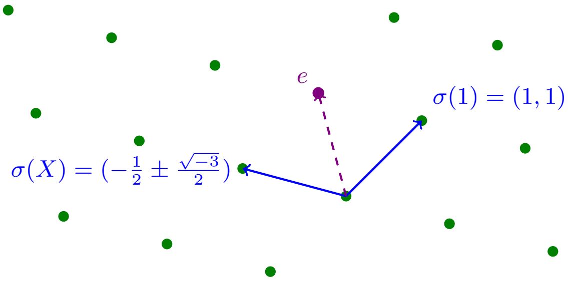


In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).
- In power basis, short elements can have long coeff vectors.

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$



In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).
- In power basis, short elements can have long coeff vectors.

  E.g., $e = 1 + X + \cdots + X^{p-2}$ but $\|e\| = \|1\| = \|X\| = \sqrt{p-1}$.

Ideal Lattices

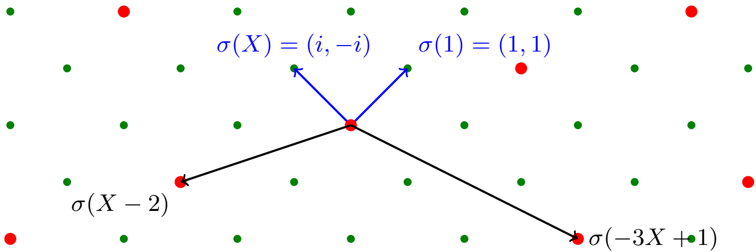
- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.

Ideal Lattices

- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R.
  Every ideal $\mathcal{I}$ embeds as an ideal lattice $\sigma(\mathcal{I})$.

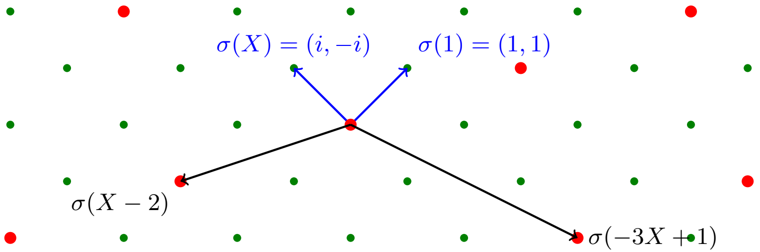
Ideal Lattices

- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R. Every ideal $\mathcal{I}$ embeds as an ideal lattice $\sigma(\mathcal{I})$.
- E.g., $R = \mathbb{Z}[X]/(X^2+1)$. Embeddings send $X \mapsto \pm\sqrt{-1}$. $\mathcal{I} = \langle X-2, -3X+1 \rangle$ is an ideal in R.



Ideal Lattices

- An ideal $\mathcal{I} \subseteq R$ is closed under $+$ and $-$, and under $\cdot$ with R. Every ideal $\mathcal{I}$ embeds as an ideal lattice $\sigma(\mathcal{I})$.
- E.g., $R = \mathbb{Z}[X]/(X^2+1)$. Embeddings send $X \mapsto \pm\sqrt{-1}$. $\mathcal{I} = \langle X-2, -3X+1 \rangle$ is an ideal in R.



(Approximate) Ideal Shortest Vector Problem

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

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.

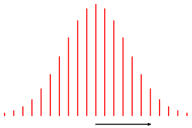
Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.
  (For product $q = q_1 \cdots q_t$ of distinct primes, $R_q \cong R_{q_1} \times \cdots \times R_{q_t}$.)

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.
  (For product $q = q_1 \cdots q_t$ of distinct primes, $R_q \cong R_{q_1} \times \cdots \times R_{q_t}$.)
- **Search**: find secret ring element $s \in R_q$, given:

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

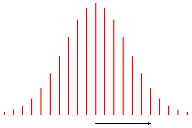


$\sqrt{n} \leq$ error coeffs $\ll q$

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.
  (For product $q = q_1 \cdots q_t$ of distinct primes, $R_q \cong R_{q_1} \times \cdots \times R_{q_t}$.)
- **Search**: find secret ring element $s \in R_q$, given:

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



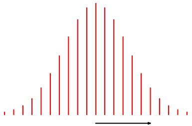
$\sqrt{n} \leq$ error coeffs $\ll q$

Note: (a_i, b_i) are uniformly random subject to: $\boxed{b_i - a_i \cdot s \approx 0}$.

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.
  (For product $q = q_1 \cdots q_t$ of distinct primes, $R_q \cong R_{q_1} \times \cdots \times R_{q_t}$.)
- **Search**: find secret ring element $s \in R_q$, given:

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



$\sqrt{n} \leq$ error coeffs $\ll q$

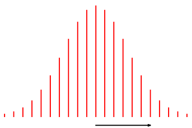
Note: (a_i, b_i) are uniformly random subject to: $\boxed{b_i - a_i \cdot s \approx 0}$.

Errors are subtle! Coeffs of e_i are small in "decoding" $\mathbb{Z}$-basis of R, and not necessarily independent!

Ring-LWE [LyubashevskyPeikertRegev'10]

- Let R be a cyclotomic ring and $R_q = R/qR = \mathbb{Z}_q[\zeta_m]$.
  For prime $q = 1 \pmod{m}$, $\tilde{O}(n)$-time ring ops in R_q via CRT basis.
  (For product $q = q_1 \cdots q_t$ of distinct primes, $R_q \cong R_{q_1} \times \cdots \times R_{q_t}$.)
- **Search**: find secret ring element $s \in R_q$, given:

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



$\sqrt{n} \le$ error coeffs $\ll q$

  Note: (a_i, b_i) are uniformly random subject to: $\boxed{b_i - a_i \cdot s \approx 0}$.
  Errors are subtle! Coeffs of e_i are small in "decoding" $\mathbb{Z}$-basis of R, and not necessarily independent!
- **Decision**: distinguish $(a_i\ ,\ b_i)$ from uniform $(a_i\ ,\ b_i) \in R_q \times R_q$.

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

(classical, any cyclotomic R)

  - ⋆ 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 $\underset{\substack{\text{(quantum,}\\ \text{any } R=\mathcal{O}_K)}}{\leq}$ search Ring-LWE $\underset{\substack{\text{(classical,}\\ \text{any cyclotomic } R)}}{\leq}$ decision Ring-LWE

  - ⋆ If you can distinguish $(a_i\ ,\ b_i)$ from $(a_i\ ,\ b_i)$, then you can find s.
  - ⋆ If you can find s, 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 $\leq$ search Ring-LWE $\leq$ decision Ring-LWE

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

(classical, any cyclotomic R)

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

- Then:

decision Ring-LWE $\leq$ tons of crypto!

Hardness of Ring-LWE [LyubashevskyPeikertRegev'10]

- Two main theorems (reductions):

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

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

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

- Then:

decision Ring-LWE $\leq$ tons of crypto!

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

Ring-LWE Symmetric Cryptosystem [LyubashevskyPeikertRegev'10]

- Secret key: $s \leftarrow R_q$.

Ring-LWE Symmetric Cryptosystem [LyubashevskyPeikertRegev'10]

- Secret key: $s \leftarrow R_q$.
- Encrypt $\mu \in R_2$: choose error $e \in R$ s.t. $e = \mu \bmod 2R$. Output

$$(c_0, c_1) = (a \cdot s + e\,,\, -a).$$

Ring-LWE Symmetric Cryptosystem [LyubashevskyPeikertRegev'10]

- Secret key: $s \leftarrow R_q$.
- Encrypt $\mu \in R_2$: choose error $e \in R$ s.t. $e = \mu \bmod 2R$. Output

$$(c_0, c_1) = (a \cdot s + e\,,\, -a).$$

- Decrypt: 'lift' $c_0 + c_1 \cdot s \in R_q$ to $e \in R$, output $\mu = e \bmod 2R$.

Ring-LWE Symmetric Cryptosystem [LyubashevskyPeikertRegev'10]

- Secret key: $s \leftarrow R_q$.
- Encrypt $\mu \in R_2$: choose error $e \in R$ s.t. $e = \mu \bmod 2R$. Output

$$(c_0, c_1) = (a \cdot s + e\,,\ -a).$$

- Decrypt: 'lift' $c_0 + c_1 \cdot s \in R_q$ to $e \in R$, output $\mu = e \bmod 2R$.

Security

- Ciphertexts are RLWE samples, so can't distinguish them from uniform (c_0, c_1), so message is hidden.

Ring-LWE Symmetric Cryptosystem [LyubashevskyPeikertRegev'10]

- Secret key: $s \leftarrow R_q$.
- Encrypt $\mu \in R_2$: choose error $e \in R$ s.t. $e = \mu \bmod 2R$. Output

$$(c_0, c_1) = (a \cdot s + e\,,\, -a).$$

- Decrypt: 'lift' $c_0 + c_1 \cdot s \in R_q$ to $e \in R$, output $\mu = e \bmod 2R$.

Security

- Ciphertexts are RLWE samples, so can't distinguish them from uniform (c_0, c_1), so message is hidden.

Alternative Interpretation

- Encryption of $\mu \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Fully Homomorphic Encryption [BrakerskiVaikuntanathan'11]

- Need a system where: if c, c' encrypt m, m', then

$$c \boxplus c' \quad \text{encrypts} \quad m + m',$$
$$c \boxdot c' \quad \text{encrypts} \quad m \cdot m'.$$

Symmetric Cryptosystem

- Encryption of $m \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Fully Homomorphic Encryption [BrakerskiVaikuntanathan'11]

- Need a system where: if c, c' encrypt m, m', then

$$c \boxplus c' \quad \text{encrypts} \quad m + m',$$
$$c \boxdot c' \quad \text{encrypts} \quad m \cdot m'.$$

Symmetric Cryptosystem

- Encryption of $m \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Full Homomorphism

- Define $\boxplus, \boxdot$ to be simply $+, \cdot$ in $R_q[S]$:

Fully Homomorphic Encryption [BrakerskiVaikuntanathan'11]

- Need a system where: if c, c' encrypt m, m', then

$$c \boxplus c' \quad \text{encrypts} \quad m + m',$$
$$c \boxdot c' \quad \text{encrypts} \quad m \cdot m'.$$

Symmetric Cryptosystem

- Encryption of $m \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Full Homomorphism

- Define $\boxplus, \boxdot$ to be simply $+, \cdot$ in $R_q[S]$:

$$\begin{aligned} (c + c')(s) = c(s) + c'(s) &= (e + e') \approx 0 \bmod qR \\ (e + e') &= (m + m') \bmod 2R. \end{aligned}$$

Fully Homomorphic Encryption [BrakerskiVaikuntanathan'11]

- Need a system where: if c, c' encrypt m, m', then

$$\begin{aligned} c \boxplus c' &\quad \text{encrypts} \quad m + m', \\ c \boxdot c' &\quad \text{encrypts} \quad m \cdot m'. \end{aligned}$$

Symmetric Cryptosystem

- Encryption of $m \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Full Homomorphism

- Define $\boxplus, \boxdot$ to be simply $+, \cdot$ in $R_q[S]$:

$$\begin{aligned} (c \cdot c')(s) = c(s) \cdot c'(s) &= (e \cdot e') \approx 0 \bmod qR \\ (e \cdot e') &= (m \cdot m') \bmod 2R. \end{aligned}$$

Fully Homomorphic Encryption [BrakerskiVaikuntanathan'11]

- Need a system where: if c, c' encrypt m, m', then

$$c \boxplus c' \quad \text{encrypts} \quad m + m',$$
$$c \boxdot c' \quad \text{encrypts} \quad m \cdot m'.$$

Symmetric Cryptosystem

- Encryption of $m \in R_2$ is a linear polynomial $c(S) = c_0 + c_1 S \in R_q[S]$:
  1. $c(s) = e \approx 0 \bmod qR$, and
  2. $e = m \bmod 2R$.

Full Homomorphism

- Define $\boxplus, \boxdot$ to be simply $+, \cdot$ in $R_q[S]$:

$$\begin{aligned} (c \cdot c')(s) = c(s) \cdot c'(s) &= (e \cdot e') \approx 0 \bmod qR \\ (e \cdot e') &= (m \cdot m') \bmod 2R. \end{aligned}$$

- Error size and polynomial degree (in S) grow with $\boxplus, \boxdot$.
  Use "linearization/key switching" and "modulus reduction" to shrink.