Lattice Cryptography

Jay Daigle

Occidental College

October 31, 2019

Definition

A ring is a set R together with two operations $+$ and $\cdot$, such that

1. *R is an abelian group under the operation $+$, with identity 0;*
2. *Multiplication is commutative, and has identity element 1;*
3. *and we have the distributive law $k(x + y) = kx + ky$.*

Definition

A ring is a set R together with two operations $+$ and $\cdot$, such that

1. *R is an abelian group under the operation $+$, with identity 0;*
2. *Multiplication is commutative, and has identity element 1;*
3. *and we have the distributive law $k(x+y) = kx + ky$.*

Definition

The ring of polynomials with integer coefficients is
$\mathbb{Z}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in \mathbb{Z}, n \in \mathbb{N}\}$.
The ring of polynomials with $\mod m$ *coefficients is*
$\mathbb{Z}/m\mathbb{Z}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in \mathbb{Z}/m\mathbb{Z}, n \in \mathbb{N}\}$.

Ideals

Definition

Let R be a ring and $r_1, \ldots, r_n \in R$. The ideal generated by r_i, written $\langle r_1, \ldots, r_n \rangle$, is the set of all linear combinations of the r_i. That is,

$$\langle r_1, \ldots, r_n \rangle = \{r_1 s_1 + r_2 s_2 + \cdots + r_n s_n : s_i \in R\}.$$

In particular, if $f \in \mathbb{Z}/m\mathbb{Z}[x]$ then $\langle f \rangle = \{f(x)g(x) : g(x) \in \mathbb{Z}/m\mathbb{Z}[x]\}$. If R is a ring and I is an ideal in R, and $r, s \in R$, we say $r = s + I$ or $r = s \mod I$ if $r - s \in I$. We write R/I for the set of equivalence classes of R modulo I. R/I is a ring under the operations inherited from R.

Ideals

Definition

Let R be a ring and $r_1, \ldots, r_n \in R$. The ideal generated by r_i, written $\langle r_1, \ldots, r_n \rangle$, is the set of all linear combinations of the r_i. That is,

$$\langle r_1, \ldots, r_n \rangle = \{r_1 s_1 + r_2 s_2 + \cdots + r_n s_n : s_i \in R\}.$$

In particular, if $f \in \mathbb{Z}/m\mathbb{Z}[x]$ then $\langle f \rangle = \{f(x)g(x) : g(x) \in \mathbb{Z}/m\mathbb{Z}[x]\}$. If R is a ring and I is an ideal in R, and $r, s \in R$, we say $r = s + I$ or $r = s \mod I$ if $r - s \in I$. We write R/I for the set of equivalence classes of R modulo I. R/I is a ring under the operations inherited from R.

Example

Take $R = \mathbb{Z}/m\mathbb{Z}[x]$ and $I = \langle x^n + 1 \rangle$ for some $n = 2^k$.
(This polynomial is the *2nth cyclotomic polynomial* $\Phi_{2n}(x)$.)

Definition

Let $f(x) \in R$ *and write* $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ *where each* $a_i \in \left\{ \frac{-(q-1)}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2} \right\}$. *That is, we choose each coefficient to be as close to zero as possible.*

Definition

Let $f(x) \in R$ *and write* $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ *where each* $a_i \in \left\{ \frac{-(q-1)}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2} \right\}$. *That is, we choose each coefficient to be as close to zero as possible.*

We define the infinity norm of f *to be* $\|f\|_\infty = \max\{|a_i|\}$. *Thus the norm is the magnitude of the largest-magnitude coefficient.*

Ring Learning with Errors

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.
3. Let $s(x)$ be an unknown polynomial with $\|s\|_\infty \leq b$.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.
3. Let $s(x)$ be an unknown polynomial with $\|s\|_\infty \leq b$.
4. Set $b_i(x) = (a_i(x) \cdot s(x)) + e_i(x)$.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.
3. Let $s(x)$ be an unknown polynomial with $\|s\|_\infty \leq b$.
4. Set $b_i(x) = (a_i(x) \cdot s(x)) + e_i(x)$.

The *Ring-LWE Decision Problem*: given list $\{(a_i(x), b_i(x))\}$, determine whether the $b_i(x)$ were generated randomly, or by this process from the $a_i(x)$.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.
3. Let $s(x)$ be an unknown polynomial with $\|s\|_\infty \leq b$.
4. Set $b_i(x) = (a_i(x) \cdot s(x)) + e_i(x)$.

The *Ring-LWE Decision Problem*: given list $\{(a_i(x), b_i(x))\}$, determine whether the $b_i(x)$ were generated randomly, or by this process from the $a_i(x)$.
The *Ring-LWE Search Problem*: given a list of pairs $(a_i(x), b_i(x))$ generated by this process, determine s.

Ring Learning with Errors

1. Let $a_i(x)$ be a set of random known polynomials in R.
2. Let e_i be a set of random unknown polynomials that are small with respect to the bound b.
3. Let $s(x)$ be an unknown polynomial with $\|s\|_\infty \leq b$.
4. Set $b_i(x) = (a_i(x) \cdot s(x)) + e_i(x)$.

The *Ring-LWE Decision Problem*: given list $\{(a_i(x), b_i(x))\}$, determine whether the $b_i(x)$ were generated randomly, or by this process from the $a_i(x)$.
The *Ring-LWE Search Problem*: given a list of pairs $(a_i(x), b_i(x))$ generated by this process, determine s.

Theorem (Lyubashevsky, Peikert, Regev)

The Ring-LWE Search Problem is at least as hard as the worst-case approximate shortest vector problem, even on a quantum computer.


A LONG TIME AGO IN A GALAXY FAR FAR AWAY...
STAR WARS
A NEW HOPE

Rounding and Masking

Rounding and Masking

$$I_0 = \mathbb{Z}/q\mathbb{Z} \cap [0, q/4)$$
$$I_1' = \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2)$$
$$I_0' = \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4)$$
$$I_1 = \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)$$

Rounding and Masking

$$
\begin{aligned}
I_0 &= \mathbb{Z}/q\mathbb{Z} \cap [0, q/4) \\
I_1' &= \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2) \\
I_0' &= \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4) \\
I_1 &= \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)
\end{aligned}
$$

$$
\lfloor v \rceil_2 = \begin{cases} 0 & v \in I_0 \cup I_1 \quad 0 \leq v < q/4 \text{ or } 3q/4 \leq v < 0 \\ 1 & v \in I_0' \cup I_1' \qquad\qquad q/4 \leq v < 3q/4 \end{cases}
$$

Rounding and Masking

$$
\begin{aligned}
I_0 &= \mathbb{Z}/q\mathbb{Z} \cap [0, q/4) \\
I_1' &= \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2) \\
I_0' &= \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4) \\
I_1 &= \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)
\end{aligned}
$$

$$
\lfloor v \rceil_2 = \begin{cases} 0 & v \in I_0 \cup I_1 \quad 0 \leq v < q/4 \text{ or } 3q/4 \leq v < 0 \\ 1 & v \in I_0' \cup I_1' \quad q/4 \leq v < 3q/4 \end{cases}
$$

$$
\langle v \rangle_2 = \begin{cases} 0 & v \in I_0 \cup I_0' \quad 0 \leq v < q/4 \text{ or } q/2 \leq v < 3q/4 \\ 1 & v \in I_1 \cup I_1' \quad q/4 \leq v < q/2 \text{ or } 3q/4 \leq v < q \end{cases}
$$

Rounding and Masking

$$
\begin{aligned}
I_0 &= \mathbb{Z}/q\mathbb{Z} \cap [0, q/4) \\
I_1' &= \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2) \\
I_0' &= \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4) \\
I_1 &= \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)
\end{aligned}
$$

$$
\lfloor v \rceil_2 = \begin{cases} 0 & v \in I_0 \cup I_1 \quad 0 \leq v < q/4 \text{ or } 3q/4 \leq v < 0 \\ 1 & v \in I_0' \cup I_1' \quad q/4 \leq v < 3q/4 \end{cases}
$$

$$
\langle v \rangle_2 = \begin{cases} 0 & v \in I_0 \cup I_0' \quad 0 \leq v < q/4 \text{ or } q/2 \leq v < 3q/4 \\ 1 & v \in I_1 \cup I_1' \quad q/4 \leq v < q/2 \text{ or } 3q/4 \leq v < q \end{cases}
$$

$$
\text{rec}(w, b) = \begin{cases} 0 & w \in I_b + E \mod q \\ 1 & \text{otherwise} \end{cases}
$$

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Ring-LWE Diffie-Hellman

Key Generation:

Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.
3. Shared secret: Bob computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$. This gives n bits.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.
3. Shared secret: Bob computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$. This gives n bits.
4. Bob computes $\langle v \rangle_2 \in \{0,1\}^n$.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.
3. Shared secret: Bob computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$. This gives n bits.
4. Bob computes $\langle v \rangle_2 \in \{0,1\}^n$.
5. Bob transmits the ciphertext $c = (u, \langle v \rangle_2) \in R \times \{0,1\}^n$.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.
3. Shared secret: Bob computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$. This gives n bits.
4. Bob computes $\langle v \rangle_2 \in \{0,1\}^n$.
5. Bob transmits the ciphertext $c = (u, \langle v \rangle_2) \in R \times \{0,1\}^n$.

Decapsulation:

1. Alice computes $w = u \cdot s_1$ using her private s_1.

Ring-LWE Diffie-Hellman

Key Generation:
Parameters $n = 2^k$, q an odd prime with $q \equiv 1 \mod 2n$,
$a \in R = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1\rangle$, and a probability distribution over R.

1. Private key: Alice generates two random elements $s_0, s_1 \in R$.
2. Public key: Alice computes $b = s_1 \cdot a + s_0$.

Encapsulation:

1. Bob generates three random elements $e_0, e_1, e_2 \in R$.
2. Bob computes $u = e_0 \cdot a + e_1, v = e_0 \cdot b + e_2 \in R$.
3. Shared secret: Bob computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$. This gives n bits.
4. Bob computes $\langle v \rangle_2 \in \{0,1\}^n$.
5. Bob transmits the ciphertext $c = (u, \langle v \rangle_2) \in R \times \{0,1\}^n$.

Decapsulation:

1. Alice computes $w = u \cdot s_1$ using her private s_1.
2. Then Alice computes $\mu = \mathrm{rec}(w, v')$.

Rounding and Masking

$$
\begin{aligned}
I_0 &= \mathbb{Z}/q\mathbb{Z} \cap [0, q/4) \\
I_1' &= \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2) \\
I_0' &= \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4) \\
I_1 &= \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)
\end{aligned}
$$

$$
\lfloor v \rceil_2 = \begin{cases} 0 & v \in I_0 \cup I_1 \quad 0 \leq v < q/4 \text{ or } 3q/4 \leq v < 0 \\ 1 & v \in I_0' \cup I_1' \quad q/4 \leq v < 3q/4 \end{cases}
$$

$$
\langle v \rangle_2 = \begin{cases} 0 & v \in I_0 \cup I_0' \quad 0 \leq v < q/4 \text{ or } q/2 \leq v < 3q/4 \\ 1 & v \in I_1 \cup I_1' \quad q/4 \leq v < q/2 \text{ or } 3q/4 \leq v < q \end{cases}
$$

$$
\text{rec}(w, b) = \begin{cases} 0 & w \in I_b + E \mod q \\ 1 & \text{otherwise} \end{cases}
$$