Section 1

Ring LWE
(In)efficiency of LWE

Standard LWE

- Ciphertexts: \((a, b) \in \mathbb{Z}_q^{(n+1) \times \log q}\) store one value (mod \(p\))
- Ciphertext size: \(O(n \log q)\)
- Addition, Scalar multiplication: \(T \approx n \log q\)
- Ciphertext multiplication: \(T \approx n^2 \log^2 q\)

Compact LWE

- Ciphertexts: \((a, b) \in \mathbb{Z}_q^{(2n) \times \log q}\) store \(n\) values (mod \(p\))
- Amortized ciphertext size: \(O(\log q)\)
- Amortized addition, scalar multiplication: \(T \approx \log q\)
- Ciphertext multiplication?
Ring LWE

- Generalize LWE using a ring $R$ instead of $\mathbb{Z}$
- Ring of polynomials $\mathbb{Z}[X]$
- Monic irreducible $p(X)$ of degree $n$
  - e.g., $p(X) = X^n - 1$
- Quotient ring $R = \mathbb{Z}[X]/p(X)$
  - isomorphic to $(\mathbb{Z}^n, +)$
  - convolution product
  - $R_q = R/qR$
- Ring LWE
  - Key: $s(X) \in R$
  - Ciphertexts $(a, b) \in R_q^2$
  - Messages: $m \in R_p$
Ring LWE vs Compact LWE

Both methods:
- Encrypt $n$ values (mod $p$) using $O(n)$ values (mod $q$)
- Efficient (linear time) vector addition and scalar multiplication

Multiplication:
- Compact LWE: tensor multiplication, cost $O(n^2)$
- Ring LWE: polynomial multiplication, cost $O(n \log n)$ using FFT

Applications / Programming model:
- Addition, scalar multiplication: SIMD
- Multiplication: convolution is usually not what you want
- Encode data to perform SIMD multiplication
Data encoding

- **Polynomial representation**
  - \( p(x_1), \ldots, p(x_n) \in \mathbb{Z}_q^n \)
  - \( p(x) = a_0 + a_1x_1 + \ldots a_{n-1}x_{n-1} \equiv \mathbb{Z}_q^n \)
  - Polynomial multiplication: SIMD multiplication of evaluation representations

- **Quasilinear time transformations**:
  - \((y_1, \ldots, y_n) \rightarrow (a_0, \ldots, a_{n-1})\): polynomial interpolation
  - \((a_0, \ldots, a_{n-1}) \rightarrow (y_1, \ldots, y_n)\): polynomial evaluation

- **Other operations**:
  - SIMD: great to run same program on \( n \) data sets
  - Need also to *pack*, *unpack*, *shuffle*, etc. for general computations
Security

- Is Ring LWE secure?
- For what rings?

Short answer:

- Working modulo $p(X) = X^n - 1$ is not a good idea
- Better to work with *cyclotomic* polynomials
- SWIFFT ring: $p(X) = X^n + 1$ where $n = 2^k$

Useful both for

- security, pseudorandomness, search/decision reductions
- efficient implementation using Number Theoretic Transform (NTT)
Implementation and Libraries

Libraries:
- SEAL
- HElib
- PALISADE
- Lattigo
- ...

Interface:
- try to hide math as much as possible
- offer encoding, decoding and SIMD operations
Cyclic lattices

- A lattice is cyclic if it is closed under 
  \[ \text{rot}(v_1, \ldots, v_n) = (v_n, v_1, v_2, \ldots, v_{n-1}) \]

- Equivalently
  - view vectors as coefficients of a polynomial
  - lattice is closed under \[ \text{rot}(v(X)) = X \cdot v(X) \mod (X^n - 1) \]

- Commonly used in coding theory (over finite fields)
  - cyclic codes: linear code, closed under rotation
  - equivalently, set of polynomials in \( \mathbb{F}[X]/(X^n - 1) \), closed under multiplication by \( X \)
Generators

Theorem

Any cyclic code over finite a field $\mathbb{F}$ can be written as

$$C = \{g(X) \cdot f(X) \mod (X^n - 1) | f(X)\}$$

for some $g(X)$

Proof.
Theorem

Any cyclic code over finite a field $\mathbb{F}$ can be written as

$$C = \{g(X) \cdot f(X) \mod (X^n - 1)|f(X)\}$$

for some $g(X)$

Proof.

Question

Is the same true for cyclic lattices?
Cyclic lattices and one-way functions

- NTRU (1998): public key encryption, efficient, no proof
- First provable construction, (M., FOCS 2002): one-way function
  - $R_q = \mathbb{Z}[X]/(q, X^n - 1)$
  - key: $a_1(X), \ldots, a_m(X) \in R_q$
  - input: $v_1(X), \ldots, v_m(X) \in \{0, 1\}^n \subset R_q$
  - output: $w(X) = \sum_i a_i(X) \cdot v_i(X) \in R_q$
  - compression function: $m = 2n \log_2(q)$
- One-way: given $a_1, \ldots, a_m$ and $w$,
  - easy to find $v_1, \ldots, v_m \in R_q$ such that $\sum_i a_i v_i = w \in R_q$
  - hard to find $v_1, \ldots, v_m \in \{0, 1\}^n$
- Intuition: Compact knapsack, circulant matrices
Compact knapsack, circulant matrices

- Polynomials: \( a(X) \in \mathbb{Z}[X]/(X^n - 1) \)
- Equivalently: \( A \in \mathbb{Z}^{n \times n} \) circulant matrix
  - \( a_1 + a_2 \equiv A_1 + A_2 \)
  - \( a_1 \cdot a_2 \equiv A_1 \cdot A_2 \)
- Compact knapsack
Collision resistance?

- Regular knapsack:
  - given random $a_1, \ldots, a_m \in \mathbb{Z}_q$
  - $m = 2 \log_2(q)$
  - collisions exist
  - collisions are hard to find

- Compact knapsack:
  - given random $a_1, \ldots, a_m \in \mathbb{Z}_q[X]/(X^n - 1)$
  - $m = 2n \log_2(q)$
  - collisions exist

Question

Are collisions hard to find?
Collisions in compact knapsacks

- Multiply each “circulant” matrix $a_i$ by the all-one vector
- Find collision in $\mathbb{Z}_q$
- Algebraic description:
  - multiply each $a_i(X)$ by $u(X) = (1 + X + X^2 + ....)$
  - Notice $(X^n - 1) = u(X) \cdot (X - 1)$
  - CRT: $R \equiv (\mathbb{Z}[X]/(X - 1)) \times (\mathbb{Z}[X]/u(X))$
  - Multiplication by $u(X)$ maps $R$ to $\mathbb{Z}[X]/(X - 1) \equiv \mathbb{Z}$
Anti-Cyclic lattices

- A lattice is anticyclic if it is closed under \( \text{rot}(x_1, \ldots, x_n) = (-x_n, x_1, x_2, \ldots, x_{n-1}) \)
- Equivalently: work in \( R = \mathbb{Z}[X]/(X^n + 1) \)
- Questions:
  1. Are compact knapsacks over \( R \) collision resistant?
  2. Does \((X^n + 1)\) have small degree factors?
Anti-Cyclic lattices

- A lattice is anticyclic if it is closed under \( \text{rot}(x_1, \ldots, x_n) = (-x_n, x_1, x_2, \ldots, x_{n-1}) \)

- Equivalently: work in \( R = \mathbb{Z}[X]/(X^n + 1) \)

- Questions:
  1. Are compact knapsacks over \( R \) collision resistant?
  2. Does \( (X^n + 1) \) have small degree factors?

**Theorem**

\( X^n + 1 \text{ is irreducible if and only if } n \text{ is a power of 2} \)
Roots of Unity

- \( \omega_m = \exp(2\pi i / m) \in \mathbb{C} \), primitive \( m \)th root of unity
- Observation: \( X^m - 1 = \prod_{k=0}^{m-1} (X - \omega_m^k) \)

\[
X^m - 1 = \prod_{d \mid m \gcd(k,m) = d} \prod_{d \mid m} \prod_{k \in \mathbb{Z}_m^*} (X - \omega_m^{k/d})
\]

**Definition**

Cyclotomic Polynomial: \( \Phi_m(X) = \prod_{k \in \mathbb{Z}_m^*} (X - \omega_m^k) \in \mathbb{C}[X] \)

- Question: does \( \Phi_m \) have integer coefficients?
Division Theorem

- $(R, +, *, 0, 1)$: any ring
- $R[X]$: polynomials with coefficients in $X$

**Theorem**

For any $a(X) \in R[X]$ and monic $b(X) \in R[X]$, there exists unique $q(X), r(X) \in R[X]$ such that

- $a(X) = q(X) \times b(X) + r(X)$
- $\deg(r(X)) < \deg(b(X))$
**Division Algorithm**

```haskell
divRem :: Poly → Poly → Poly
divRem a b =
    if (deg a < deg b)
      then (0,a)
      else let
        aL = leadingTerm a
        bL = leadingTerm b
        qL = aL / bL
        a' = a - b*qL
        (q',r) = divRem a' b
        q = qL + q'
    in divRem (q, r)
```

- Dividing by \( b(X) \) requires divisions by the leading coefficient of \( b \)
- If \( R \) is a field, we can divide by any non-zero \( b(X) \):
- If \( b(X) \) is monic, division is possible in any ring \( R \)
Polynomial Division: Example

**Question**

Divide $a(X) = 5X^8 + 4X^6 - 5X^3 + 4$ by $b(X) = X^3 - X + 7$
Polynomial Division: Example

**Question**

Divide \(a(X) = 5X^8 + 4X^6 - 5X^3 + 4\) by \(b(X) = X^3 - X + 7\)

**Solution:**

- quotient: \(q(X) = 5X^5 + 9X^3 - 35X^2 + 9X - 103\)
- remainder: \(r(X) = 254X^2 - 166X + 725\)
Remarks about Division Algorithm

- Division Algorithm:
  \[(a(X), b(X) \in R[X]) \mapsto (q(X), r(X) \in R[X])\]
- For any subring \(S \subseteq R\), and \(a(X), b(X) \in S[X]\)
  - Result of dividing \(a(X)\) by \(b(X)\) is in \(S[X]\)
  - Division as polynomials in \(R[X]\) or as polynomials in \(S[X]\) produces the same result
Polynomial GCD

- \( \mathbb{F}[X] \): polynomials with coefficients in a field \( \mathbb{F} \)

- The Greatest Common Divisor (gcd) of \( a(X), b(X) \in \mathbb{F}[X] \) is a polynomial \( g(X) \in \mathbb{F}[X] \) such that
  - \( g(X) \) divides \( a(X) \) and \( b(X) \)
  - any \( d(X) \in \mathbb{F}[X] \) that divides both \( a(X) \) and \( b(X) \) also divides \( g(X) \)

**Theorem**

For any \( a(X), b(X) \in \mathbb{F}[X] \)

\[
gcd(a(X), b(X)) = u(X)a(X) + v(X)b(X)
\]

for some \( u(X), v(X) \in \mathbb{F}[X] \).
Euclid’s Algorithm

- **Input:** \( a(X), b(X) \in \mathbb{F}[X] \)
- **Output:** \( u(X), v(X) \in \mathbb{F}[X] \) such that
  \[
u(X)a(X) + v(X)b(X) = \gcd(a(X), b(X))\]
- **Invariant:** \( \gcd(a(X), b(X)) = \gcd(b(X), a(X) \mod b(X)) \)

\[
euclid :: (\text{Poly}, \text{Poly}) \rightarrow (\text{Poly}, \text{Poly})
\]
\[
euclid \ (a, b) =
\]
\[
\text{if} \ (\deg b \equiv 0)
\]
\[
\text{then} \ (1, 0)
\]
\[
\text{else let} \ (q, r) = \text{divRem} \ b \ a
\]
\[
(u, v) = \text{euclid} \ (b, r)
\]
\[
in \ (-q \ast v , u + v)
\]

- **Base case:** \( 1 \ast a + 0 \ast b = a = \gcd(a, b) \)
- **Induction:** \( (-q \ast v) a + (u + v) b = u b + v (b - q a) = ub + vr \)
Remarks about Euclid Algorithm

```
euclid :: (Poly, Poly) → (Poly, Poly)
euclid (a, b) =
  if (deg b ≡ 0)
    then (1, 0)
  else let (q, r) = divRem b a
         (u, v) = neuclid (b, r)
         in (-q * v, u + v)
```

- Euclid Algorithm works over a field:
  - Even if \( b(X) \) is monic, \( r(X) = b(X) \mod a(X) \) may not be
  - If \( a(X), b(X) \in R[X] \) have coefficients in a domain \( R \subseteq F \),
    then we can compute \( \gcd(a(X), b(X)) \in F[X] \)
Cyclotomic Polynomials

\[ X^m - 1 = \prod_{d \mid m} \Phi_m(X) \]

Theorem

\[ \Phi_m(X) \in \mathbb{Z}[X] \]
Cyclotomic Polynomials

\[ X^m - 1 = \prod_{d|m} \Phi_m(X) \]

**Theorem**

\[ \Phi_m(X) \in \mathbb{Z}[X] \]

**Proof:**

- For \( m = 1 \), \( \Phi_1(X) = (X - 1) \)
- For \( m > 1 \), \( b(X) = \prod_{m > d|m} \Phi_d(X) \) is in \( \mathbb{Z}[X] \) by induction
- Compute \( (q(X), r(X)) = \text{divRem}(X^m - 1, b(X)) \) in \( \mathbb{Z}[X] \)
- \( r(X) = 0 \) because \( b(X) \) divides \( X^m - 1 \)
- \( \Phi_m(X) = q(X) \) is in \( \mathbb{Z}[X] \)
Irreducibility of Cyclotomies

Theorem
\[ \Phi_m(X) \in \mathbb{Z}[X] \text{ is irreducible} \]

Theorem
\[ C_m \equiv \mathbb{Z}[X]/\Phi_m(X) = \mathbb{Z}[\omega_m] \]

- simple proof, helps intuition

Algebraic Number Fields
- finite dimensional extensions of \( \mathbb{Q} \)
- key concepts: field extensions, vector spaces

Algebraic Number Rings
- finite dimensional extensions of \( \mathbb{Z} \), i.e., lattices
- key concepts: ring extensions, modules over a ring
Factoring primes in Cyclotomic rings

- $\Phi_m(X) \in \mathbb{Z}[X]$: $m$th cyclotomic polynomial
- $\Phi_m(X)$ is irreducible in $\mathbb{Z}[X]$
- Let $p$ be a prime, and assume $\gcd(m, p) = 1$
- Question: if $\Phi_m(X)$ irreducible also in $\mathbb{Z}_p[X]$?
- Answer: no, and this is very useful

Question

Question: What’s the factorization of $\Phi_m(X)$ modulo $p$?

Technically, this is the problem of factoring (the ideal generated by) the prime $p$ in the ring of polynomials modulo $\Phi_m(X)$
Factoring primes in Cyclotomic rings

- \( \Phi_m(X) \in \mathbb{Z}[X] \): \( m \)th cyclotomic polynomial
- \( \Phi_m(X) \) is irreducible in \( \mathbb{Z}[X] \)
- Let \( p \) be a prime, and assume \( \gcd(m, p) = 1 \)
- Question: if \( \Phi_m(X) \) irreducible also in \( \mathbb{Z}_p[X] \)?
- Answer: no, and this is very useful

**Question**

*Question: What’s the factorization of \( \Phi_m(X) \) modulo \( p \)?*

Technically, this is the problem of factoring (the ideal generated by) the prime \( p \) in the ring of polynomials modulo \( \Phi_m(X) \)

*“The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers”* (Bill Gates, *The Road Ahead*, p. 265)
Motivation

- \( R = \mathbb{Z}[X]/\Phi_m(X) \)
- \( R_p = R/(pR) \equiv \mathbb{Z}[X]/\langle \Phi_m(X), p \rangle_{\mathbb{Z}[X]} \)
- Equivalently, \( R_p \equiv \mathbb{Z}_p[X]/\Phi_m(X) \)
- The structure of \( R_p \) is equivalently described by
  - the factorization of \((pR)\) in \( R \), or
  - the factorization of \( \Phi_m \) in \( \mathbb{Z}_p[X] \)