Section 9

Ring LWE
(In)efficiency of LWE

Standard LWE

- Ciphertexts: \((a, b) \in \mathbb{Z}_q^{(n+1) \times \log q}\) store one value \(\pmod p\)
- 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 \(\pmod p\)
- 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**
  - \( p(x_1), \ldots, p(x_n) \in \mathbb{Z}_q^n \)
  - \( p(x) = a_0 + a_1 x_1 + \ldots a_{n-1} x^{n-1} \equiv \mathbb{Z}_q^n \)
  - 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
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
Project:

- Use one of the libraries
- Open ended, do anything you want
- Goal: demonstrate you managed to use the library
- Extra points: do something interesting
- Submission: pdf report describing your work + supporting code

Teams:

- You can work in pairs if you like
- Larger teams only if doing something more substantial
- Individual project required to use for master competency
Project Deadlines:

Deadlines:

- Next lecture (Tue, Dec 1): need to know what you are doing (team, library)
- End of finals week (Fri, Dec 18): project submission (canvas, pdf+code)

In the meantime:

- in class, mathematics underlying Ring LWE used by the libraries
- useful to understand/improve the libraries
- not required to use the libraries