A Very Brief Introduction to Lattice-Based Homomorphic Encryption

Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

May 6, 2023

Fully Homomorphic Encryption

Fully Homomorphic Encryption

- μ: message
- pk: public key
- $c = E(\mu, pk)$: ciphertext

Fully Homomorphic Encryption

- μ: message
- pk: public key
- $c = E(\mu, pk)$: ciphertext
- Additive Homomorphism:

$$E(\mu, pk) \oplus E(\widetilde{\mu}, pk) = E(\mu + \widetilde{\mu}, pk)$$

Fully Homomorphic Encryption

- μ: message
- pk: public key
- $c = E(\mu, pk)$: ciphertext
- Additive Homomorphism:

$$E(\mu, pk) \oplus E(\widetilde{\mu}, pk) = E(\mu + \widetilde{\mu}, pk)$$

- Multiplicative Homomorphism:

$$E(\mu, pk) \odot E(\widetilde{\mu}, pk) = E(\mu \cdot \widetilde{\mu}, pk)$$

R-LWE

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$
- $\mathcal{R}_q$ denotes the ring $\mathcal{R}$ reduced modulo q;

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$
- $\mathcal{R}_q$ denotes the ring $\mathcal{R}$ reduced modulo q;
  - i.e., $\mathcal{R}_q = \mathbb{Z}_q[x]/\Phi(x)$

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$
- $\mathcal{R}_q$ denotes the ring $\mathcal{R}$ reduced modulo q;
  - i.e., $\mathcal{R}_q = \mathbb{Z}_q[x]/\Phi(x)$
  - $a \in \mathcal{R}_q$ is a polynomial $a = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$
- $\mathcal{R}_q$ denotes the ring $\mathcal{R}$ reduced modulo q;
  - i.e., $\mathcal{R}_q = \mathbb{Z}_q[x]/\Phi(x)$
  - $a \in \mathcal{R}_q$ is a polynomial $a = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$
  - $a_i \in (-q/2, q/2)$ for $i = 0, 1, \ldots, n-1$

R-LWE

- Consider the ring of polynomials $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$, where $\Phi(x)$ is cyclotomic polynomial of degree n, where n is a power of 2.
  - $\mathcal{R}$ is the set of polynomials of degree less than n with integer coefficients.
    - **Addition:** standard polynomial addition
    - **Multiplication:** standard polynomial multiplication and reduction modulo $\Phi(x) = x^n + 1$
- $\mathcal{R}_q$ denotes the ring $\mathcal{R}$ reduced modulo q;
  - i.e., $\mathcal{R}_q = \mathbb{Z}_q[x]/\Phi(x)$
  - $a \in \mathcal{R}_q$ is a polynomial $a = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$
  - $a_i \in (-q/2, q/2)$ for $i = 0, 1, \ldots, n-1$
  - **Example:** $q = 7,\ F_7 = \{-3, -2, -1, 0, 1, 2, 3\}$

Error Distribution: $D_{\mathcal{R},\sigma}$

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)
- Let B_0 be a bound on normal distribution with $\mu = 0$ and σ

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)
- Let B_0 be a bound on normal distribution with $\mu = 0$ and σ
- We can use error function erf to compute a bound for the samples

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)
- Let B_0 be a bound on normal distribution with $\mu = 0$ and σ
- We can use error function erf to compute a bound for the samples
- For a normal distribution with $\mu = 0$ and σ, erf $\left(\frac{a}{\sigma\sqrt{2}}\right)$ is the probability that a sample lies in $(-a, a)$ for a positive a.

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)
- Let B_0 be a bound on normal distribution with $\mu = 0$ and σ
- We can use error function erf to compute a bound for the samples
- For a normal distribution with $\mu = 0$ and σ, erf $\left(\frac{a}{\sigma\sqrt{2}}\right)$ is the probability that a sample lies in $(-a, a)$ for a positive a.
- Then, erfc $\left(\frac{a}{\sigma\sqrt{2}}\right)$ gives the probability that a sample lies outside of $(-a, a)$.

Error Distribution: $D_{\mathcal{R},\sigma}$

- The operation $a \leftarrow D_{\mathcal{R},\sigma}$ outputs a polynomial in $\mathcal{R}$, whose coefficients are sampled from a normal distribution with 0 mean and standard deviation σ.
  - In other words, it outputs a polynomial with "small" coefficients if σ is small (e.g. $\sigma = 3.5$)
- Let B_0 be a bound on normal distribution with $\mu = 0$ and σ
- We can use error function erf to compute a bound for the samples
- For a normal distribution with $\mu = 0$ and σ, erf $\left(\frac{a}{\sigma\sqrt{2}}\right)$ is the probability that a sample lies in $(-a, a)$ for a positive a.
- Then, erfc $\left(\frac{a}{\sigma\sqrt{2}}\right)$ gives the probability that a sample lies outside of $(-a, a)$.
- Pick a B_0 so that erfc $\left(\frac{B_0}{\sigma\sqrt{2}}\right)$ is negligible.

Hard Problems

Hard Problems

- Two hard problems can be given:

Hard Problems

- Two hard problems can be given:
  - **Ring-LWE Search Problem:** Pick $a, s \in \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$ and set $b \leftarrow as + e \pmod{q}$. The search problem is, given the pair (a, b), to output the value s.

Hard Problems

- Two hard problems can be given:
  - **Ring-LWE Search Problem:** Pick $a, s \in \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$ and set $b \leftarrow as + e \pmod q$. The search problem is, given the pair (a, b), to output the value s.
  - **Ring LWE Decision Problem:** Given (a, b) where $a, b \in \mathcal{R}_q$, determine which of the following two cases holds:

Hard Problems

- Two hard problems can be given:
  - **Ring-LWE Search Problem:** Pick $a, s \in \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$ and set $b \leftarrow as + e \pmod{q}$. The search problem is, given the pair (a, b), to output the value s.
  - **Ring LWE Decision Problem:** Given (a, b) where $a, b \in \mathcal{R}_q$, determine which of the following two cases holds:
    1. b is chosen uniformly at random $(b \leftarrow \mathcal{R}_q)$

- Two hard problems can be given:
  - **Ring-LWE Search Problem:** Pick $a, s \in \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$ and set $b \leftarrow as + e \pmod{q}$. The search problem is, given the pair (a, b), to output the value s.
  - **Ring LWE Decision Problem:** Given (a, b) where $a, b \in \mathcal{R}_q$, determine which of the following two cases holds:
    1. (i) b is chosen uniformly at random $(b \leftarrow \mathcal{R}_q)$
    2. (ii) $b \leftarrow a \cdot s + e$ where $s \leftarrow \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$

- Two hard problems can be given:
  - **Ring-LWE Search Problem:** Pick $a, s \in \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$ and set $b \leftarrow as + e \pmod q$. The search problem is, given the pair (a, b), to output the value s.
  - **Ring LWE Decision Problem:** Given (a, b) where $a, b \in \mathcal{R}_q$, determine which of the following two cases holds:
    1. b is chosen uniformly at random $(b \leftarrow \mathcal{R}_q)$
    2. $b \leftarrow a \cdot s + e$ where $s \leftarrow \mathcal{R}_q$ and $e \leftarrow D_{\mathcal{R},\sigma}$
- R-LWE Problems are still hard even if $s \leftarrow D_{\mathcal{R},\sigma}$

A PKC based on R-LWE - Key Generation

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.
  1. $s, e \leftarrow D_{\mathcal{R},\sigma}$

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.
  i) $s, e \leftarrow D_{\mathcal{R},\sigma}$
  ii) $a \leftarrow \mathcal{R}_q$

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.
    i) $s, e \leftarrow D_{\mathcal{R},\sigma}$
    ii) $a \leftarrow \mathcal{R}_q$
    iii) $b \leftarrow as + pe \pmod q$

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.
  i) $s, e \leftarrow D_{\mathcal{R},\sigma}$
  ii) $a \leftarrow \mathcal{R}_q$
  iii) $b \leftarrow as + pe \pmod{q}$
  iv) pk $\leftarrow (a, b)$

A PKC based on R-LWE - Key Generation

- We pick two prime integers p and q such that $p \ll q$, a ring $\mathcal{R}$, and a normal distribution with standard deviation σ. (e.g., $p = 2$)
- Security depends on the ring dimension n, q and σ.
- $\{p, q, \mathcal{R}, \sigma\}$: public domain parameters.
  - i) $s, e \leftarrow D_{\mathcal{R},\sigma}$
  - ii) $a \leftarrow \mathcal{R}_q$
  - iii) $b \leftarrow as + pe \pmod q$
  - iv) pk $\leftarrow (a, b)$
  - v) sk $\leftarrow s$

A PKC based on R-LWE - Encryption

A PKC based on R-LWE - Encryption

- Let $\mu \in \mathcal{R}_p$ be an arbitrary message

A PKC based on R-LWE - Encryption

- Let $\mu \in \mathcal{R}_p$ be an arbitrary message
  1. $e_0, e_1, e_2 \leftarrow D_{\mathcal{R},\sigma}$

A PKC based on R-LWE - Encryption

- Let $\mu \in \mathcal{R}_p$ be an arbitrary message
  i) $e_0, e_1, e_2 \leftarrow D_{\mathcal{R},\sigma}$
  ii) $c_0 \leftarrow be_0 + pe_1 + \mu$

A PKC based on R-LWE - Encryption

- Let $\mu \in \mathcal{R}_p$ be an arbitrary message
    i) $e_0, e_1, e_2 \leftarrow D_{\mathcal{R},\sigma}$
    ii) $c_0 \leftarrow be_0 + pe_1 + \mu$
    iii) $c_1 \leftarrow ae_0 + pe_2$

A PKC based on R-LWE - Encryption

- Let $\mu \in \mathcal{R}_p$ be an arbitrary message
  1. $e_0, e_1, e_2 \leftarrow D_{\mathcal{R},\sigma}$
  2. $c_0 \leftarrow be_0 + pe_1 + \mu$
  3. $c_1 \leftarrow ae_0 + pe_2$
     - Ciphertext: (c_0, c_1)

A PKC based on R-LWE - Decryption

A PKC based on R-LWE - Decryption

- $\mu \leftarrow (c_0 - c_1 s \pmod q) \pmod p$

A PKC based on R-LWE - Decryption

- $\mu \leftarrow (c_0 - c_1 s \pmod q) \pmod p$
- Decryption is a vector product $\langle (c_0, c_1), (1, -s) \rangle$ where

A PKC based on R-LWE - Decryption

- $\mu \leftarrow (c_0 - c_1 s \pmod q) \pmod p$
- Decryption is a vector product $\langle (c_0, c_1), (1, -s) \rangle$ where
  - secret key: $(1, -s)$

A PKC based on R-LWE - Decryption

- $\mu \leftarrow (c_0 - c_1 s \pmod q) \pmod p$
- Decryption is a vector product $\langle (c_0, c_1), (1, -s) \rangle$ where
  - secret key: $(1, -s)$
  - ciphertext: (c_0, c_1)

Correctness of the decryption operation

Correctness of the decryption operation

$$
\begin{aligned}
\mu &= (c_0 - c_1 s \pmod q) \pmod p \\
&= ((be_0 - pe_1 + \mu) - (ase_0 - pe_2 s) \pmod q) \pmod p \\
&= (p(ee_0 + e_1 - e_2 s) + \mu \pmod q) \pmod p \\
&= (p \cdot \text{“small”} + \mu \pmod q) \pmod p
\end{aligned}
$$

Correctness of the decryption operation

$$
\begin{aligned}
\mu &= (c_0 - c_1 s \pmod q) \pmod p \\
&= ((be_0 - pe_1 + \mu) - (ase_0 - pe_2 s) \pmod q) \pmod p \\
&= (p(ee_0 + e_1 - e_2 s) + \mu \pmod q) \pmod p \\
&= (p \cdot \text{“small”} + \mu \pmod q) \pmod p
\end{aligned}
$$

- $(p \cdot \text{“small”} + \mu \pmod q) \pmod p$ will return μ only if $\|p \cdot \text{“small”} + \mu\|_\infty < \|p \cdot \text{“small”} + p\|_\infty < \frac{q}{2}$.

Correctness Constraint

Correctness Constraint

- For correct decryption, we should have

$$\|p(ee_0 + e_1 - e_2 s) + p\|_\infty < \frac{q}{2},$$

where s, e, e_0, e_1, e_2 are sampled from the same distribution.

Correctness Constraint

- For correct decryption, we should have

$$\|p(ee_0 + e_1 - e_2 s) + p\|_\infty < \frac{q}{2},$$

  where s, e, e_0, e_1, e_2 are sampled from the same distribution.
- Also they are all in $\mathcal{R} = \mathbb{Z}[x]/F(x)$

Correctness Constraint

Correctness Constraint

- $\|p(ee_0 + e_1 - e_2 s + 1)\|_\infty < \frac{q}{2}$

Correctness Constraint

- $\|p(ee_0 + e_1 - e_2 s + 1)\|_\infty < \frac{q}{2}$
- B_0 is an upper bound for coefficients of e, e_0, e_1, e_2 and s where $e, e_0, e_1, e_2, s \in \mathcal{R} = \mathbb{Z}[x]/F(x)$

Correctness Constraint

- $\|p(ee_0 + e_1 - e_2 s + 1)\|_\infty < \frac{q}{2}$
- B_0 is an upper bound for coefficients of e, e_0, e_1, e_2 and s where $e, e_0, e_1, e_2, s \in \mathcal{R} = \mathbb{Z}[x]/F(x)$
- What is the upper bound for the coefficients of ee_0 and $e_2 s$?

Correctness Constraint

- $\|p(ee_0 + e_1 - e_2 s + 1)\|_\infty < \dfrac{q}{2}$
- B_0 is an upper bound for coefficients of e, e_0, e_1, e_2 and s where $e, e_0, e_1, e_2, s \in \mathcal{R} = \mathbb{Z}[x]/F(x)$
- What is the upper bound for the coefficients of ee_0 and $e_2 s$?
- Infinity norm of a polynomial $\|e\|_\infty$ is the maximum of its coefficients.

Correctness Constraint

- $\|p(ee_0 + e_1 - e_2 s + 1)\|_\infty < \frac{q}{2}$
- B_0 is an upper bound for coefficients of e, e_0, e_1, e_2 and s where $e, e_0, e_1, e_2, s \in \mathcal{R} = \mathbb{Z}[x]/F(x)$
- What is the upper bound for the coefficients of ee_0 and $e_2 s$?
- Infinity norm of a polynomial $\|e\|_\infty$ is the maximum of its coefficients.
- $\|e\|_\infty, \|e_0\|_\infty, \|e_1\|_\infty, \|e_2\|_\infty, \|s\|_\infty < B_0$

Correctness Constraint - Example

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ ($m = 8, n = 4$)
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$
  - $c_2 = a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3$

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$
  - $c_2 = a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3$
  - $c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$
  - $c_2 = a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3$
  - $c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$
- Every coefficient in c_i is the sum of four $(n = 4)$ product terms.

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$
  - $c_2 = a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3$
  - $c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$
- Every coefficient in c_i is the sum of four $(n = 4)$ product terms.
- An upper bound for a product term is B_0^2

Correctness Constraint - Example

- $\mathcal{R} = \mathbb{Z}[x]/\Phi_8(x)$ $(m = 8, n = 4)$
- $\Phi_8(x) = x^4 + 1$
- $c(x) = a(x)b(x)$ where $a(x), b(x), c(x) \in \mathcal{R}$
  - $c_0 = a_0b_0 - a_1b_3 - a_2b_2 - a_3b_1$
  - $c_1 = a_0b_1 + a_1b_0 - a_2b_3 - a_3b_2$
  - $c_2 = a_0b_2 + a_1b_1 + a_2b_0 - a_3b_3$
  - $c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$
- Every coefficient in c_i is the sum of four $(n = 4)$ product terms.
- An upper bound for a product term is B_0^2
- An upper bound for a coefficient is then nB_0^2 (a bit loose upper bound)

Correctness Constraint - Cont.

Correctness Constraint - Cont.

- Let $\eta = ee_0 + e_1 - e_2 s$

Correctness Constraint - Cont.

- Let $\eta = ee_0 + e_1 - e_2 s$
- An upper bound for η is, then, $nB_0^2 + B_0 + nB_0^2$

Correctness Constraint - Cont.

- Let $\eta = ee_0 + e_1 - e_2 s$
- An upper bound for η is, then, $nB_0^2 + B_0 + nB_0^2$
- $\|p\eta + \mu\|_\infty < p(nB_0^2 + B_0 + nB_0^2 + 1) < \dfrac{q}{2} \Rightarrow q > 2p(2nB_0^2 + B_0 + 1)$

Correctness Constraint - Cont.

- Let $\eta = ee_0 + e_1 - e_2 s$
- An upper bound for η is, then, $nB_0^2 + B_0 + nB_0^2$
- $\|p\eta + \mu\|_\infty < p(nB_0^2 + B_0 + nB_0^2 + 1) < \frac{q}{2} \Rightarrow q > 2p(2nB_0^2 + B_0 + 1)$
- Let $B = (2nB_0^2 + B_0)$ bound for η then $q > 2p(B + 1)$

Fully Homomorphic Encryption

Fully Homomorphic Encryption

- $\mu \in \mathcal{R}_p$

Fully Homomorphic Encryption

- $\mu \in \mathcal{R}_p$
- $c = E(\mu, pk)$

Fully Homomorphic Encryption

- $\mu \in \mathcal{R}_p$
- $c = E(\mu, pk)$
- $c \in \mathcal{R}_q^2$

Fully Homomorphic Encryption

- $\mu \in \mathcal{R}_p$
- $c = E(\mu, pk)$
- $c \in \mathcal{R}_q^2$
- Additive Homomorphism:

$$E(\mu, pk) \oplus E(\widetilde{\mu}, pk) = E(\mu + \widetilde{\mu}, pk)$$

- $\mu \in \mathcal{R}_p$
- $c = E(\mu, pk)$
- $c \in \mathcal{R}_q^2$
- Additive Homomorphism:

$$E(\mu, pk) \oplus E(\widetilde{\mu}, pk) = E(\mu + \widetilde{\mu}, pk)$$

- Multiplicative Homomorphism:

$$E(\mu, pk) \odot E(\widetilde{\mu}, pk) = E(\mu \cdot \widetilde{\mu}, pk)$$

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Consider two ciphertexts c and $\widetilde{c}$, which encrypts μ and $\widetilde{\mu}$, respectively,

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Consider two ciphertexts c and $\widetilde{c}$, which encrypts μ and $\widetilde{\mu}$, respectively,
    - $c = (c_0, c_1)$

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Consider two ciphertexts c and $\widetilde{c}$, which encrypts μ and $\widetilde{\mu}$, respectively,
    - $c = (c_0, c_1)$
    - $\widetilde{c} = (\widetilde{c_0}, \widetilde{c_1})$

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Consider two ciphertexts c and $\widetilde{c}$, which encrypts μ and $\widetilde{\mu}$, respectively,
    - $c = (c_0, c_1)$
    - $\widetilde{c} = (\widetilde{c_0}, \widetilde{c_1})$
  - Consider also the decryption operation

$$\langle (c_0, c_1), (1, -s) \rangle = (c_0 - sc_1 = \mu + p\eta \pmod q) \pmod p$$

$$\langle (\widetilde{c_0}, \widetilde{c_1}), (1, -s) \rangle = (\widetilde{c_0} - s\widetilde{c_1} = \widetilde{\mu} + p\widetilde{\eta} \pmod q) \pmod p$$

Additive Homomorphism

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Now, apply addition to ciphertexts $c + \widetilde{c}$ and decrypt

$$\begin{aligned}
\langle c + \widetilde{c}, (1, -s) \rangle &= (c_0 + \widetilde{c_0} - sc_1 - s\widetilde{c_1} \pmod q) \pmod p \\
&= (c_0 - sc_1 + \widetilde{c_0} - s\widetilde{c_1} \pmod q) \pmod p \\
&= (\mu + p\eta + \widetilde{\mu} + p\widetilde{\eta} \pmod q) \pmod p \\
&= (\mu + \widetilde{\mu} + p(\eta + \widetilde{\eta}) \pmod q) \pmod p
\end{aligned}$$

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Now, apply addition to ciphertexts $c + \widetilde{c}$ and decrypt

$$\begin{aligned}
\langle c + \widetilde{c}, (1, -s) \rangle &= (c_0 + \widetilde{c_0} - sc_1 - s\widetilde{c_1} \pmod q) \pmod p \\
&= (c_0 - sc_1 + \widetilde{c_0} - s\widetilde{c_1} \pmod q) \pmod p \\
&= (\mu + p\eta + \widetilde{\mu} + p\widetilde{\eta} \pmod q) \pmod p \\
&= (\mu + \widetilde{\mu} + p(\eta + \widetilde{\eta}) \pmod q) \pmod p
\end{aligned}$$

  - So long as $\|p(\eta + \widetilde{\eta}) + (\mu + \widetilde{\mu})\|_\infty < \frac{q}{2}$, the modulo q reduction does not happen $\Rightarrow$ CORRECT decryption

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Now, apply addition to ciphertexts $c + \widetilde{c}$ and decrypt

$$\begin{aligned}
\langle c + \widetilde{c}, (1, -s) \rangle &= (c_0 + \widetilde{c_0} - sc_1 - s\widetilde{c_1} \pmod q) \pmod p \\
&= (c_0 - sc_1 + \widetilde{c_0} - s\widetilde{c_1} \pmod q) \pmod p \\
&= (\mu + p\eta + \widetilde{\mu} + p\widetilde{\eta} \pmod q) \pmod p \\
&= (\mu + \widetilde{\mu} + p(\eta + \widetilde{\eta}) \pmod q) \pmod p
\end{aligned}$$

  - So long as $\|p(\eta + \widetilde{\eta}) + (\mu + \widetilde{\mu})\|_\infty < \frac{q}{2}$, the modulo q reduction does not happen $\Rightarrow$ CORRECT decryption
  - An upper bound for both $p\eta$ and $p\widetilde{\eta}$ is pB

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Now, apply addition to ciphertexts $c + \widetilde{c}$ and decrypt

$$
\begin{aligned}
\langle c + \widetilde{c}, (1, -s) \rangle &= (c_0 + \widetilde{c_0} - sc_1 - s\widetilde{c_1} \pmod{q}) \pmod{p} \\
&= (c_0 - sc_1 + \widetilde{c_0} - s\widetilde{c_1} \pmod{q}) \pmod{p} \\
&= (\mu + p\eta + \widetilde{\mu} + p\widetilde{\eta} \pmod{q}) \pmod{p} \\
&= (\mu + \widetilde{\mu} + p(\eta + \widetilde{\eta}) \pmod{q}) \pmod{p}
\end{aligned}
$$

  - So long as $\|p(\eta + \widetilde{\eta}) + (\mu + \widetilde{\mu})\|_\infty < \frac{q}{2}$, the modulo q reduction does not happen $\Rightarrow$ CORRECT decryption
  - An upper bound for both $p\eta$ and $p\widetilde{\eta}$ is pB
  - Then, an upper bound for $p(\eta + \widetilde{\eta})$ is the $2pB$

Additive Homomorphism

- Our R-LWE-based PKC system is additively homomorphic
  - Now, apply addition to ciphertexts $c + \widetilde{c}$ and decrypt

$$\begin{aligned}
\langle c + \widetilde{c}, (1, -s) \rangle &= (c_0 + \widetilde{c_0} - sc_1 - s\widetilde{c_1} \pmod q) \pmod p \\
&= (c_0 - sc_1 + \widetilde{c_0} - s\widetilde{c_1} \pmod q) \pmod p \\
&= (\mu + p\eta + \widetilde{\mu} + p\widetilde{\eta} \pmod q) \pmod p \\
&= (\mu + \widetilde{\mu} + p(\eta + \widetilde{\eta}) \pmod q) \pmod p
\end{aligned}$$

  - So long as $\|p(\eta + \widetilde{\eta}) + (\mu + \widetilde{\mu})\|_\infty < \frac{q}{2}$, the modulo q reduction does not happen $\Rightarrow$ CORRECT decryption
  - An upper bound for both $p\eta$ and $p\widetilde{\eta}$ is pB
  - Then, an upper bound for $p(\eta + \widetilde{\eta})$ is the $2pB$
  - The noise increases linearly

Homomorphic addition of l ciphertexts

$$\mu^{(1)}, \ldots, \mu^{(l)} \rightarrow c^{(1)}, \ldots, c^{(l)}$$
$$\left\langle c^{(1)} + \ldots + c^{(l)}, (1, -s) \right\rangle = \mu^{(1)} + \ldots + \mu^{(l)} + p(\eta^{(1)} + \ldots + \eta^{(l)})$$

Homomorphic addition of l ciphertexts

$$\mu^{(1)}, \ldots, \mu^{(l)} \rightarrow c^{(1)}, \ldots, c^{(l)}$$
$$\left\langle c^{(1)} + \ldots + c^{(l)}, (1, -s) \right\rangle = \mu^{(1)} + \ldots + \mu^{(l)} + p(\eta^{(1)} + \ldots + \eta^{(l)})$$

- An upper bound for $p(\eta^{(1)} + \ldots + \eta^{(l)})$ is then lpB

Homomorphic addition of l ciphertexts

$\mu^{(1)}, \ldots, \mu^{(l)} \rightarrow c^{(1)}, \ldots, c^{(l)}$

$\left\langle c^{(1)} + \ldots + c^{(l)}, (1, -s) \right\rangle = \mu^{(1)} + \ldots + \mu^{(l)} + p(\eta^{(1)} + \ldots + \eta^{(l)})$

- An upper bound for $p(\eta^{(1)} + \ldots + \eta^{(l)})$ is then lpB
- Eventually, the error term will exceed $\frac{q}{2}$ depending on l and p.

Homomorphic addition of l ciphertexts

$\mu^{(1)}, \ldots, \mu^{(l)} \rightarrow c^{(1)}, \ldots, c^{(l)}$
$\left\langle c^{(1)} + \ldots + c^{(l)}, (1, -s) \right\rangle = \mu^{(1)} + \ldots + \mu^{(l)} + p(\eta^{(1)} + \ldots + \eta^{(l)})$

- An upper bound for $p(\eta^{(1)} + \ldots + \eta^{(l)})$ is then lpB
- Eventually, the error term will exceed $\frac{q}{2}$ depending on l and p.
- This means that we can perform only a limited number of homomorphic additions of ciphertexts, whereby this number is determined mainly by p and q.

Homomorphic addition of l ciphertexts

$$\mu^{(1)}, \ldots, \mu^{(l)} \rightarrow c^{(1)}, \ldots, c^{(l)}$$
$$\left\langle c^{(1)} + \ldots + c^{(l)}, (1, -s) \right\rangle = \mu^{(1)} + \ldots + \mu^{(l)} + p(\eta^{(1)} + \ldots + \eta^{(l)})$$

- An upper bound for $p(\eta^{(1)} + \ldots + \eta^{(l)})$ is then lpB
- Eventually, the error term will exceed $\dfrac{q}{2}$ depending on l and p.
- This means that we can perform only a limited number of homomorphic additions of ciphertexts, whereby this number is determined mainly by p and q.
- This is what is known as SOMEWHAT HOMOMORPHIC ENCRYPTION system (SWHE or SHE)

Multiplicative Homomorphism

Multiplicative Homomorphism

- Our R-LWE-based PKC supports homomorphic multiplication of ciphertexts

Multiplicative Homomorphism

- Our R-LWE-based PKC supports homomorphic multiplication of ciphertexts
  - Suppose two ciphertexts $c = (c_0, c_1)$ and $\widetilde{c} = (\widetilde{c_0}, \widetilde{c_1})$ encrypting μ and $\widetilde{\mu}$, respectively.

Multiplicative Homomorphism

- Our R-LWE-based PKC supports homomorphic multiplication of ciphertexts
  - Suppose two ciphertexts $c = (c_0, c_1)$ and $\widetilde{c} = (\widetilde{c_0}, \widetilde{c_1})$ encrypting μ and $\widetilde{\mu}$, respectively.
  - Define tensor product of c and $\widetilde{c}$ as

$$c \otimes \widetilde{c} = (c_0\widetilde{c_0}, c_0\widetilde{c_1}, c_1\widetilde{c_0}, c_1\widetilde{c_1}) = (d_0, d_1, d_2, d_3)$$

Multiplicative Homomorphism - Decryption for Mutiplication of Ciphertexts

Multiplicative Homomorphism - Decryption for Mutiplication of Ciphertexts

- Now, we have four-dimensional ciphertext, which will decrypt with respect to the "secret key" vector $(1, -s) \otimes (1, -s) = (1, -s, -s, s^2)$ since

Multiplicative Homomorphism - Decryption for Mutiplication of Ciphertexts

- Now, we have four-dimensional ciphertext, which will decrypt with respect to the "secret key" vector $(1, -s) \otimes (1, -s) = (1, -s, -s, s^2)$ since

$$\begin{aligned}
\left\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \right\rangle &= (d_0 - d_1 s - d_2 s + d_3 s^2 \pmod q) \pmod p \\
&= c_0\widetilde{c_0} - c_0\widetilde{c_1}s - c_1\widetilde{c_0}s + c_1\widetilde{c_1}s^2 \\
&= (c_0 - c_1 s)(\widetilde{c_0} - \widetilde{c_1}s)(\mathrm{mod} q) \\
&= (\mu + p\eta)(\widetilde{\mu} + p\widetilde{\eta})(\mathrm{mod} q) \\
&= (\mu\widetilde{\mu} + p(\mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}) \pmod q) \pmod p \\
&= (\mu\widetilde{\mu} + p\eta_f \pmod q) \pmod p
\end{aligned}$$

Multiplicative Homomorphism - Decryption for Mutiplication of Ciphertexts

- Now, we have four-dimensional ciphertext, which will decrypt with respect to the "secret key" vector $(1, -s) \otimes (1, -s) = (1, -s, -s, s^2)$ since

$$
\begin{aligned}
\left\langle c \otimes \tilde{c}, (1, -s, -s, s^2) \right\rangle &= (d_0 - d_1 s - d_2 s + d_3 s^2 \pmod q) \pmod p \\
&= c_0 \tilde{c_0} - c_0 \tilde{c_1} s - c_1 \tilde{c_0} s + c_1 \tilde{c_1} s^2 \\
&= (c_0 - c_1 s)(\tilde{c_0} - \tilde{c_1} s) (\mathrm{mod} q) \\
&= (\mu + p\eta)(\tilde{\mu} + p\tilde{\eta}) (\mathrm{mod} q) \\
&= (\mu\tilde{\mu} + p(\mu\tilde{\eta} + \tilde{\mu}\eta + p\eta\tilde{\eta}) \pmod q) \pmod p \\
&= (\mu\tilde{\mu} + p\eta_f \pmod q) \pmod p
\end{aligned}
$$

- Therefore, $c \otimes \tilde{c}$ is an encryption of $\mu\tilde{\mu}$ under the secret key $(1, -s, -s, s^2)$

Noise Increases Quadratically

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}$

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}$
- For correct decryption $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < \dfrac{q}{2}$

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod q) \pmod p$
- $\eta_f = \mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}$
- For correct decryption $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < \dfrac{q}{2}$
- $\|\mu\|_\infty, \|\widetilde{\mu}\|_\infty < p$, $\|\mu\widetilde{\mu}\|_\infty < p^2$ and $\|\eta\|_\infty, \|\widetilde{\eta}\|_\infty < B$.

Noise Increases Quadratically

- $\langle c \otimes \tilde{c}, (1, -s, -s, s^2) \rangle = (\mu\tilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\tilde{\eta} + \tilde{\mu}\eta + p\eta\tilde{\eta}$
- For correct decryption $\|\mu\tilde{\mu} + p\eta_f\|_\infty < \frac{q}{2}$
- $\|\mu\|_\infty, \|\tilde{\mu}\|_\infty < p$, $\|\mu\tilde{\mu}\|_\infty < p^2$ and $\|\eta\|_\infty, \|\tilde{\eta}\|_\infty < B$.
- $\|\eta_f\|_\infty < pB + pB + pB^2$

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}$
- For correct decryption $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < \dfrac{q}{2}$
- $\|\mu\|_\infty, \|\widetilde{\mu}\|_\infty < p$, $\|\mu\widetilde{\mu}\|_\infty < p^2$ and $\|\eta\|_\infty, \|\widetilde{\eta}\|_\infty < B$.
- $\|\eta_f\|_\infty < pB + pB + pB^2$
- $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < p^2 + p^2(2B + B^2) < \dfrac{q}{2}$

Noise Increases Quadratically

- $\langle c \otimes \tilde{c}, (1, -s, -s, s^2) \rangle = (\mu\tilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\tilde{\eta} + \tilde{\mu}\eta + p\eta\tilde{\eta}$
- For correct decryption $\|\mu\tilde{\mu} + p\eta_f\|_\infty < \frac{q}{2}$
- $\|\mu\|_\infty, \|\tilde{\mu}\|_\infty < p$, $\|\mu\tilde{\mu}\|_\infty < p^2$ and $\|\eta\|_\infty, \|\tilde{\eta}\|_\infty < B$.
- $\|\eta_f\|_\infty < pB + pB + pB^2$
- $\|\mu\tilde{\mu} + p\eta_f\|_\infty < p^2 + p^2(2B + B^2) < \frac{q}{2}$
- $q > 2p^2(B^2 + 2B + 1)$

Noise Increases Quadratically

- $\langle c \otimes \widetilde{c}, (1, -s, -s, s^2) \rangle = (\mu\widetilde{\mu} + p\eta_f \pmod{q}) \pmod{p}$
- $\eta_f = \mu\widetilde{\eta} + \widetilde{\mu}\eta + p\eta\widetilde{\eta}$
- For correct decryption $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < \dfrac{q}{2}$
- $\|\mu\|_\infty, \|\widetilde{\mu}\|_\infty < p$, $\|\mu\widetilde{\mu}\|_\infty < p^2$ and $\|\eta\|_\infty, \|\widetilde{\eta}\|_\infty < B$.
- $\|\eta_f\|_\infty < pB + pB + pB^2$
- $\|\mu\widetilde{\mu} + p\eta_f\|_\infty < p^2 + p^2(2B + B^2) < \dfrac{q}{2}$
- $q > 2p^2(B^2 + 2B + 1)$
- Noise increases quadratically.