Cryptography

Lecture 26

Announcements

- HW9 due today
- “Optional” HW10 up on course webpage due on Wed 5/15.
- Final Review Sheet up on course webpage
- Upcoming:
  - Scholarly paper EC due on 5/13
  - Final Review Sheet solutions and Cheat Sheet will be posted on Canvas by the end of the week

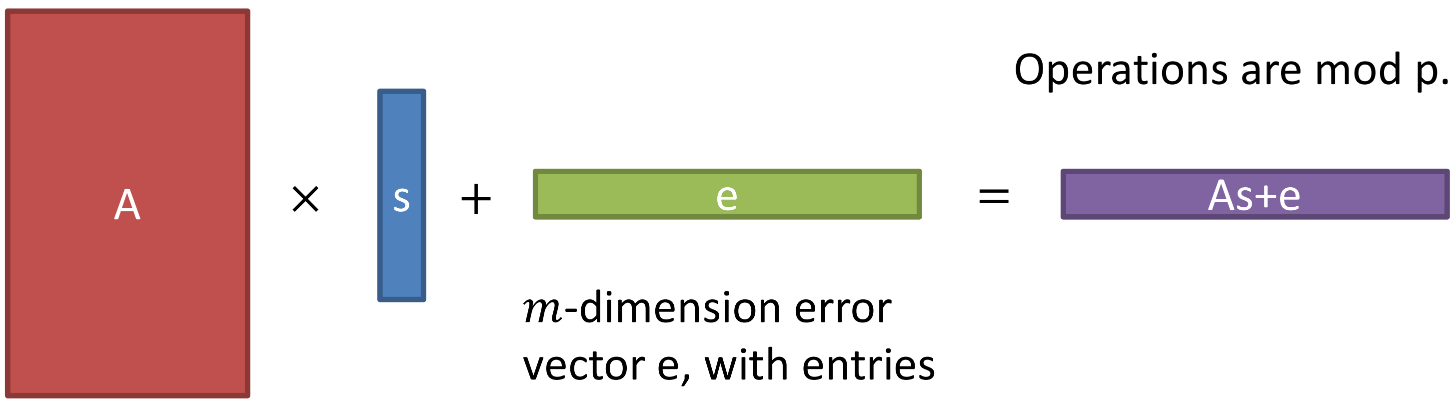
Agenda

- Post-Quantum Crypto
- Last time:
  - Lattices and hard problems, SVP, SIVP, Gap-SVP
  - SIS problem, CRHF from SIS
- This time:
  - LWE problem (search and decision)
  - PKE from LWE
  - The Ring-LWE (RLWE) Setting
  - Key Exchange from RLWE
  - Fully Homomorphic Encryption

The LWE Problem (Search)

Secret n-dimension vector s with entries chosen at random

Operations are mod p.

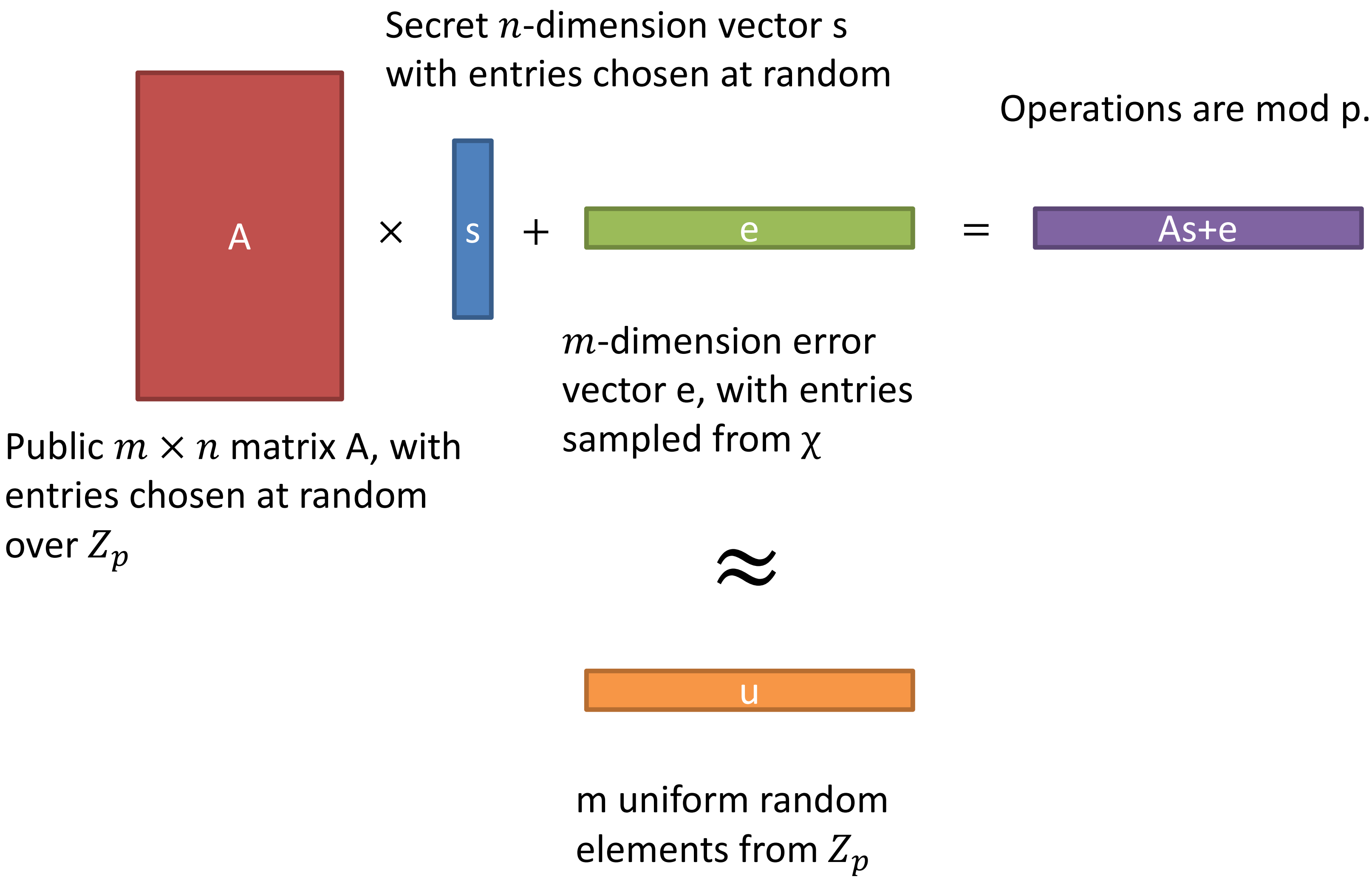


Public $m \times n$ matrix A, with entries chosen at random over Z_p

m-dimension error vector e, with entries sampled from χ. **Distribution χ depends on dimension of A and the modulus.**

Problem: Given, A, As+e, find s.

The LWE Problem Decision



Relation to Lattices

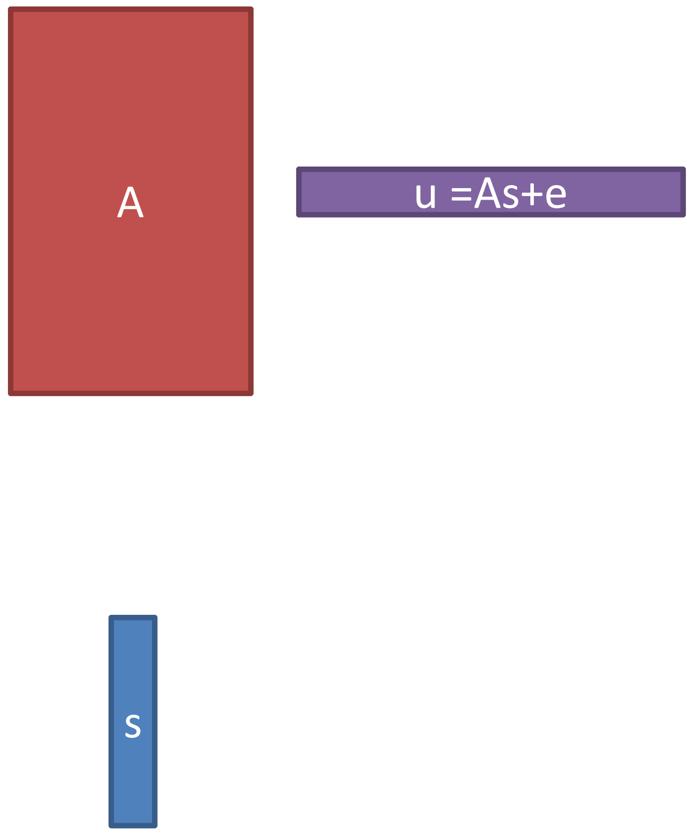
- Worst-Case to Average-Case Reduction: Breaking the cryptosystem on average is as hard as breaking the hardest instance of the underlying lattice problem.
- LWE:
  - Worst-Case to Average-Case Quantum Reduction from SIVP.
  - Worst-Case to Average-Case Classical Reductions from GapSVP.

Lattice-Based Encryption

Regev’s Cryptosystem

Public Key:

Secret Key:



Regev's Cryptosystem

Encryption of $m \in \{0,1\}$

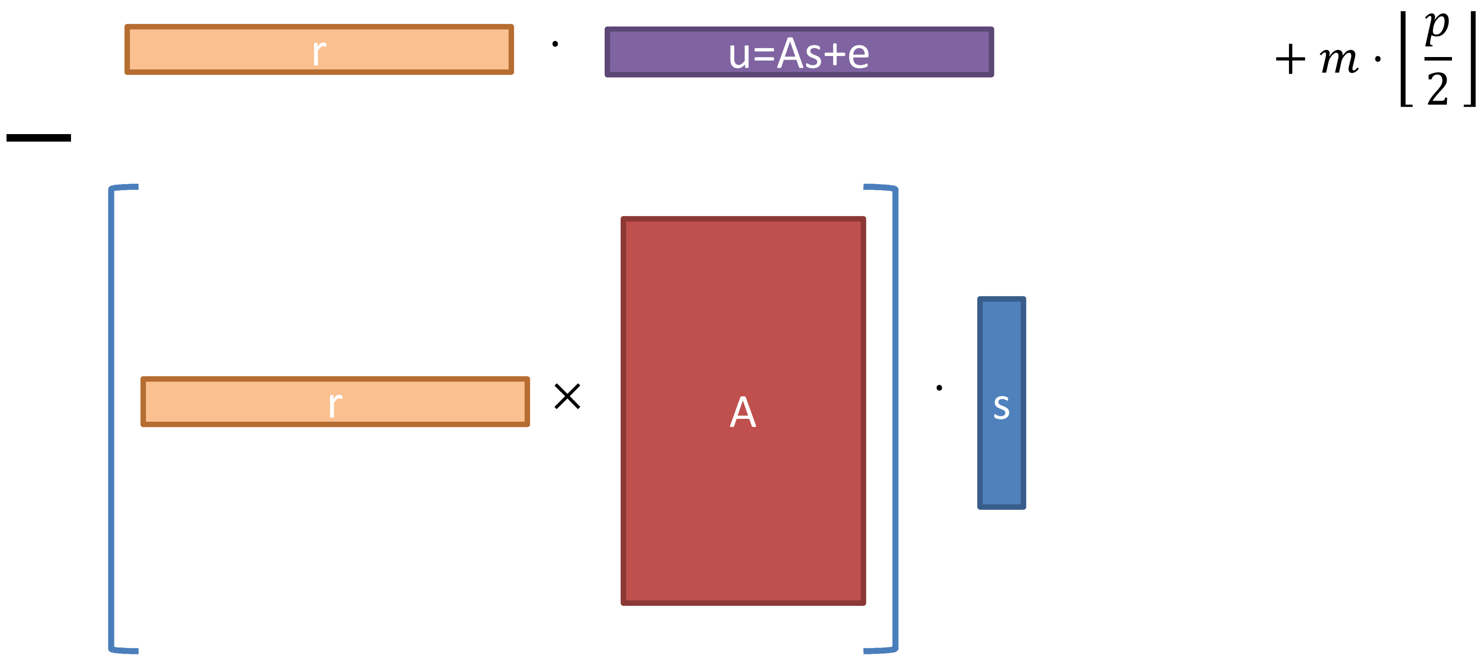
(1) r $\times$ A

r $\in \{0,1\}^m$ chosen at random.

(2) r $\cdot$ u=As + e $+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor$

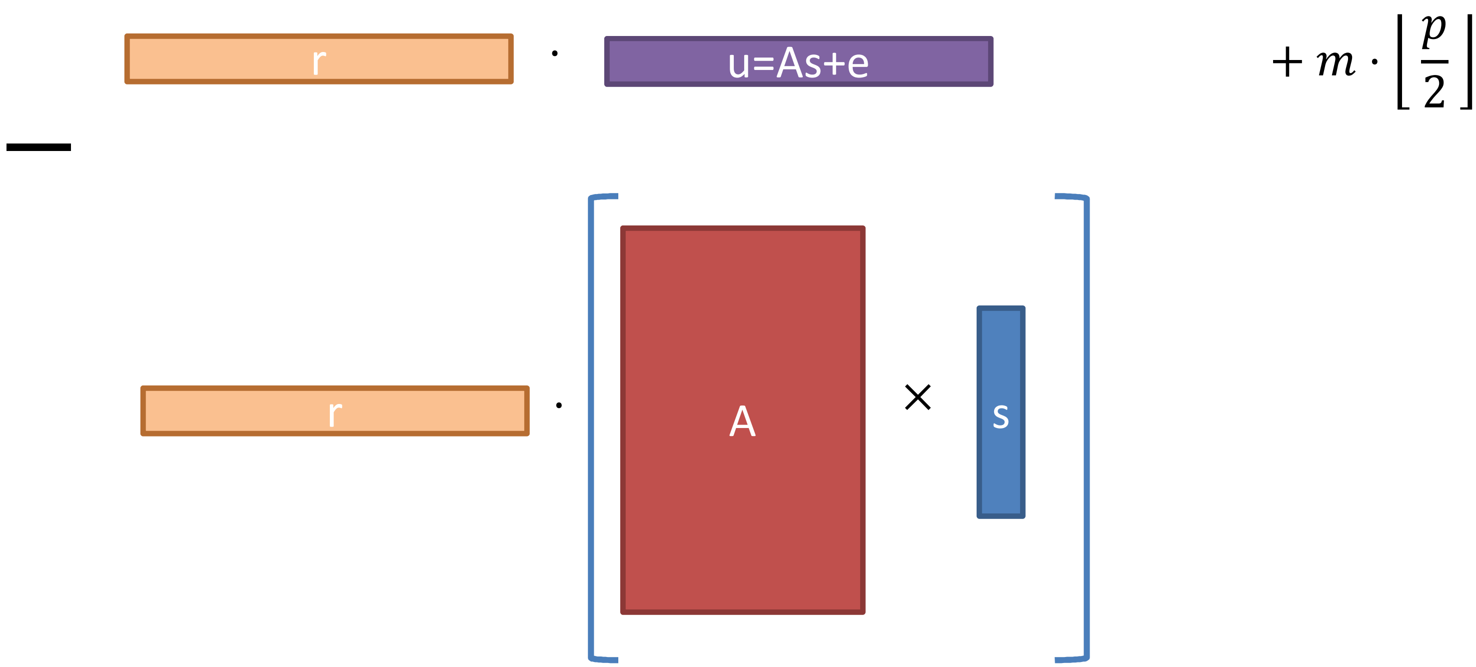
Regev's Cryptosystem

Decryption



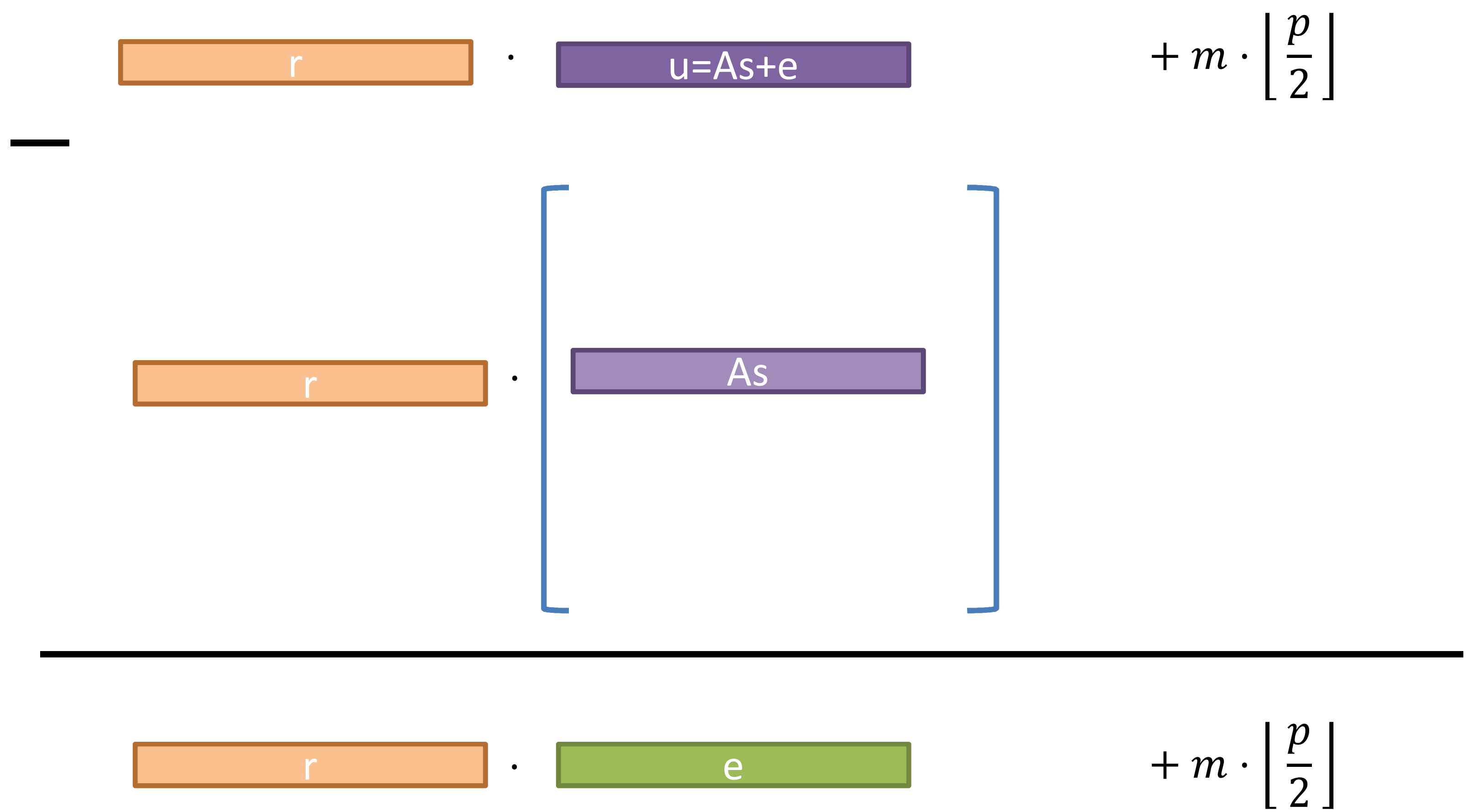
Regev's Cryptosystem

Decryption



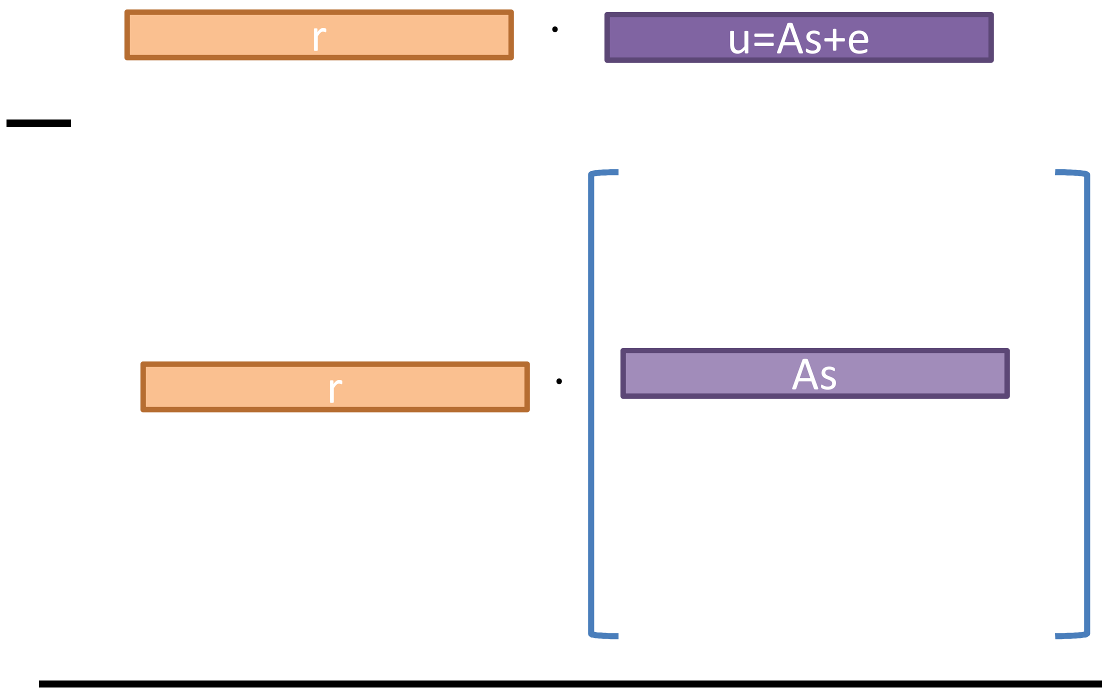
Regev's Cryptosystem

Decryption



Regev's Cryptosystem

Decryption



$$+ m \cdot \left\lfloor \frac{p}{2} \right\rceil$$

$$\approx 0 \qquad + m \cdot \left\lfloor \frac{p}{2} \right\rceil$$

Properties of LWE

- Equivalance of Search/Decision LWE
- Equivalence of LWE with random secret/secret drawn from error distribution

Efficiency

- Efficiency is a main concern in lattice-based cryptosystems.
- In both SIS and LWE-based cryptosystems, the public key consists of a random matrix of size $\mathrm{m} \times \mathrm{n}$ $(m \geq n \log p)$, requiring space $O(n^2 \log^2 p)$.
  - RSA and discrete-log based cryptosystems: public key size is linear in the security parameter.
- To reduce the public key size, consider lattices with structure.

The Ring Setting

- Quotient ring $Z_q[x]/\Phi_m(x)$, where Φ_m is the m-th cyclotomic polynomial of degree $\varphi(m)$
  - e.g.,$\Phi_{2n} = x^n + 1, n = 2, q = 13.$
  - $x^2 = -1 \; mod \; (x^2 + 1)$
  - $12x^3 + 15x^2 + 9x + 25 \to 12x^3 + 2x^2 + 9x + 12 \to x - 2 + 9x + 12 \to (10{,}10).$
- Lattice is defined as an ideal $I \subseteq Z[x]/\Phi_m(x)$.
- Ring-LWE and ring-SIS problems are defined by substituting the matrix A with polynomials from the quotient ring and substituting polynomial multiplication for matrix-vector multiplication.
- The public key is now a polynomial in $Z_q[x]/\Phi_m(x)$, and so can be described using $O(n \log q)$ bits.

NTT Transform

Consider Φ_m, where m is a power of 2. Then degree is equal to n, power of 2, $m = 2n$. $\Phi_{2n} = x^n + 1$

- Consider prime q s.t. $q = 1 \ mod \ 2n$.
- Then we have n $2n$-th primitive roots modulo q
  - Why? Z_q^* is cyclic with order $q - 1$. $2n \mid (q - 1)$.
  - Let g be a generator of Z_q^*. g is a $(q - 1)$-th primitive root.
  - $g^{a \cdot 2n} = g^{q-1}$, since $2n \mid (q - 1)$. g^a is a $2n$-th primitive root. Also $(g^a)^i$, where i is relatively prime to $2n$.
  - Note that $(g^a)^n = -1 \ mod \ q$. Modulo $x^n + 1$ means $x^n = -1$.
  - Let $\gamma_1, \ldots, \gamma_n$ be the n number of $2n$-th primitive roots
- For a polynomial $p(x) \in Z_q[x]/x^n$+1
- For every $\gamma_i, p(\gamma_i) \ mod \ p$ is equal to taking $p(x)$ modulo $x^n + 1$ and modulo q and then evaluating the reduced polynomial at γ_i.

NTT Transform

- For a polynomial $p(x) \in Z_q[x]/x^n$+1
- Evaluate $p(x)$ on all n number of $2n$-th primitive roots. Obtain a vector $p(\gamma_1) \dots p(\gamma_n)$.
- Can now do both addition and multiplication coordinate-wise.

Key Exchange from Ring-LWE

Simple Key Exchange

P_1 $\qquad\qquad$ P_2

s_1 $\qquad$ $(a, u_1 = a \cdot s_1 + e_1)$ $\longrightarrow$ $\qquad$ s_2

$\longleftarrow$ $(a, u_2 = a \cdot s_2 + e_2)$

RECONCILIATION

$u_2 \cdot s_1 \approx a \cdot s_2 \cdot s_1$ $\qquad\qquad$ $u_1 \cdot s_2 \approx a \cdot s_1 \cdot s_2$

Fully Homomorphic Encryption

- Key Generation: Sample $g^{(i)}, u^{(i)}$ from χ
  - Secret Key: $f^{(i)} = 2u^{(i)} + 1$
  - Public Key: $h^{(i)} = 2g^{(i)}\left(f^{(i)}\right)^{-1}$
- Encrypt a bit b:

$$c^{(i)} = h^{(i)}s + 2e + b, \{s, e\} \leftarrow \chi$$

- Decrypt ciphertext $c^{(i)}$: Output

$$b = f^{(i)}c^{(i)} \; mod \; 2$$

- Addition:

$$c_0^{(i)} = h^{(i)}s_0 + 2e_0 + b_0, c_1^{(i)} = h^{(i)}s_1 + 2e_1 + b_1$$

$$c_0^{(i)} + c_1^{(i)} = h^{(i)}(s_0 + s_1) + 2(e_0 + e_1) + (b_0 + b_1)$$

- Multiplication:

$$c_0^{(i)} = h^{(i)}s_0 + 2e_0 + b_0, c_1^{(i)} = h^{(i)}s_1 + 2e_1 + b_1$$

$$c_0^{(i)} \cdot c_1^{(i)}$$
$$= (h^{(i)})^2(s_0 \cdot s_1) + h^{(i)}(2s_0e_1 + 2s_1e_0 + s_0b_1 + s_1b_0) + 4e_0e_1 + 2e_0b_1 + 2e_1b_0$$
$$+ \; (b_0 \cdot b_1)$$

Decrypts correctly under $(f^{(i)})^2$, but noise grows fast

Relinearization

- Idea: Different secret key at each "level" I
- After the i-th multiplication switch from a noisy encryption under sk_i to a fresh encryption under sk_i+1.
- To do this, we encrypt sk_i under sk_i+1 and use homomorphic properties to perform decryption under sk_i inside the sk_i+1 ciphertext

Relinearization

- Helper ciphertexts: Encryptions of sk_i under sk_i+1:
  - $\zeta_\tau^{(i+1)} = h^{(i+1)} s_\tau^{(i+1)} + 2e_\tau^{(i+1)} + 2^\tau \left(f^{(i)}\right)^2$
  - $\left\{s_\tau^{(i+1)}, e_\tau^{(i+1)}\right\} \leftarrow \chi, \tau \in [0, \log q_i]$
- Given ciphertext $c^{(i)}$, let $c_\tau^{(i)}$ denote the polynomial consisting of the τ-th bit of each coefficient
- $\sum_\tau \zeta_\tau^{(i+1)} c_\tau^{(i)} = h^{(i+1)} \tilde{s} + 2\tilde{e} + (f^{(i)})^2 \cdot c^{(i)}$

Decryption of $c^{(i)}$ under $\left(f^{(i)}\right)^2$.