

# 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  $p$ .

$$A \times s + e = As+e$$

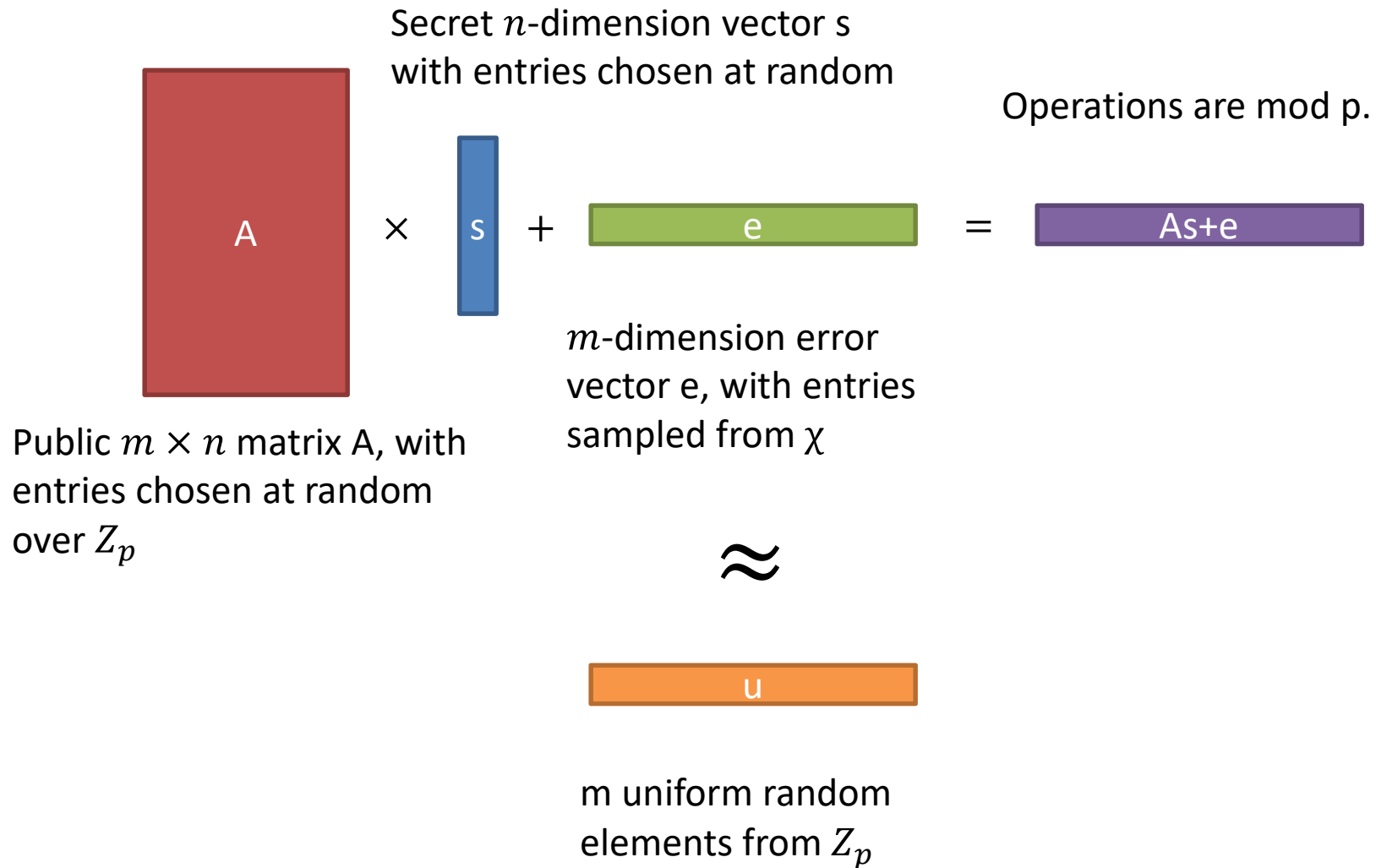
Public  $m \times n$  matrix  $A$ , with  
entries chosen at random  
over  $Z_p$

$m$ -dimension error  
vector  $e$ , with entries  
sampled from  $\chi$ .

**Distribution  $\chi$  depends  
on dimension of  $A$  and  
the modulus.**

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

# The LWE Problem Decision



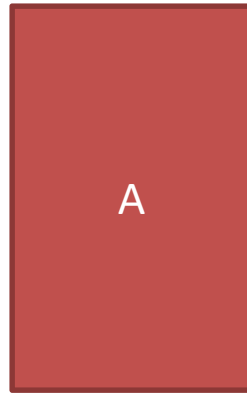
# Relation to Lattices

- 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:



A purple rectangular box with a thin black border, containing the equation  $u = As + e$  in white text.



Secret  
Key:







# Regev's Cryptosystem

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

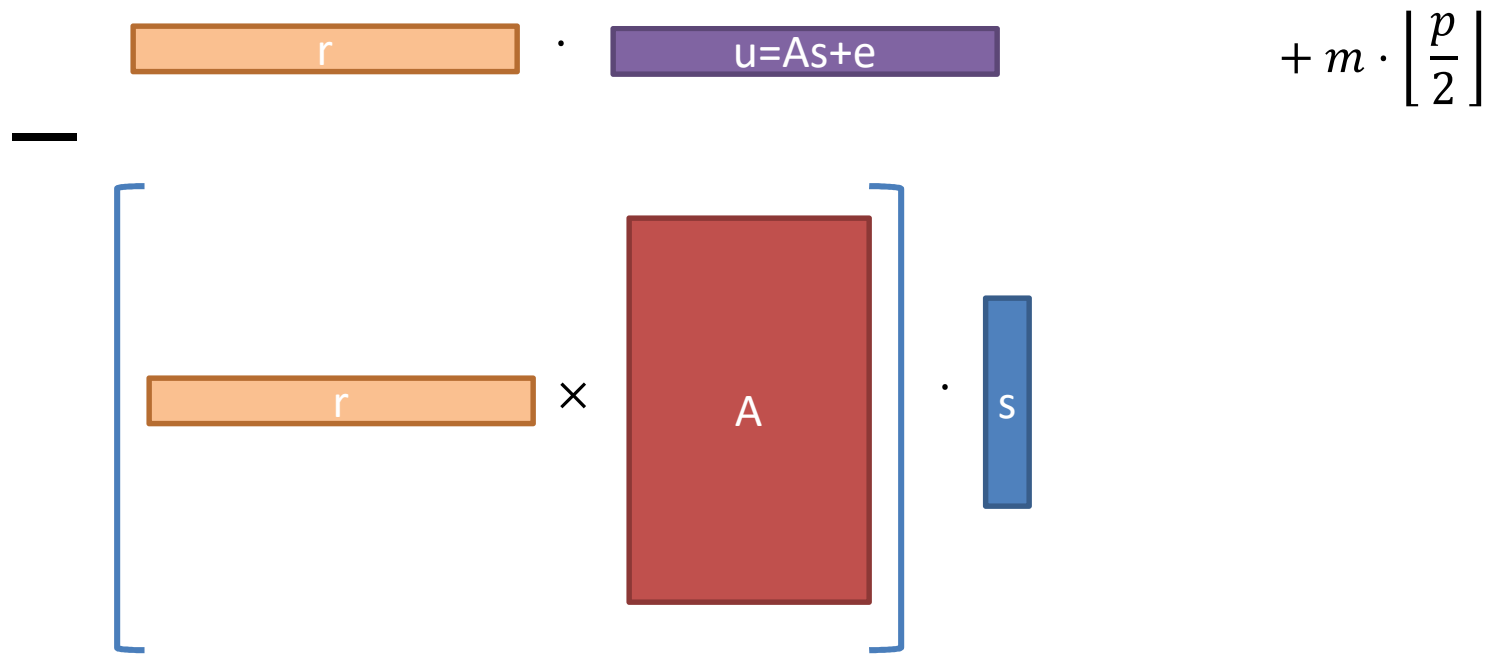
(1)   $\times$  

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

(2)   $\cdot$    $+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor$

# Regev's Cryptosystem

## Decryption

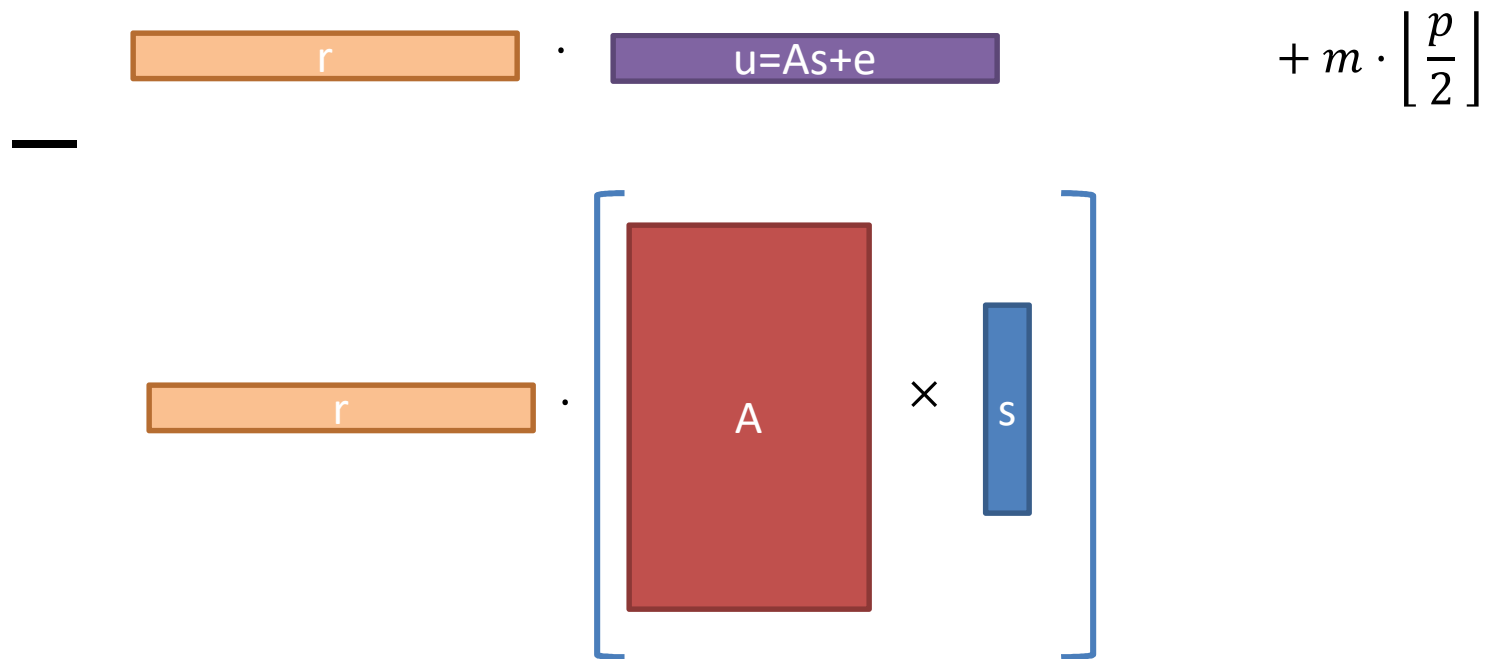


The diagram illustrates the decryption process in Regev's cryptosystem. It features several colored boxes and mathematical symbols:

- An orange box labeled  $r$  is positioned above a purple box labeled  $u=As+e$ . A dot  $\cdot$  is placed between them.
- To the right of the purple box is the expression  $+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor$ .
- A horizontal black line is located below the orange box  $r$ .
- Below the line, a blue bracket groups an orange box labeled  $r$  and a red box labeled  $A$ . A multiplication symbol  $\times$  is placed between them.
- To the right of the red box  $A$  is a dot  $\cdot$  and a blue box labeled  $s$ .

# Regev's Cryptosystem

Decryption

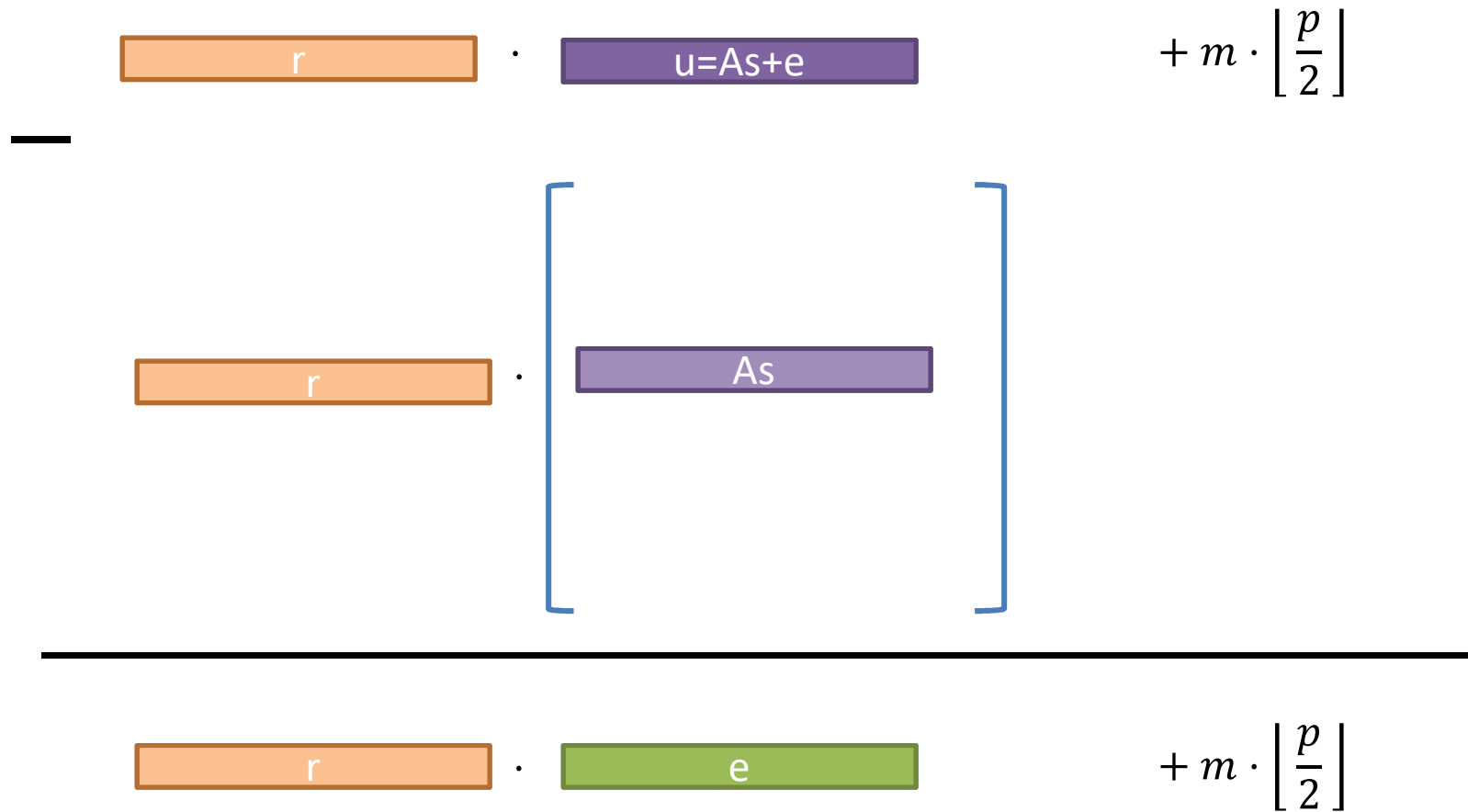


The diagram illustrates the decryption process in Regev's cryptosystem. It features two rows of mathematical components. The top row shows an orange box labeled 'r' followed by a dot and a purple box labeled 'u=As+e'. To the right of this row is the expression '+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor'. The bottom row shows an orange box labeled 'r' followed by a dot and a large blue bracketed area. Inside this bracket is a red box labeled 'A' followed by a multiplication sign and a blue box labeled 's'. A horizontal line is positioned to the left of the bottom row.

$$\underline{\quad} \quad r \cdot u = As + e \quad + m \cdot \left\lfloor \frac{p}{2} \right\rfloor$$
$$r \cdot \left[ A \times s \right]$$

# Regev's Cryptosystem

Decryption



# Regev's Cryptosystem

Decryption

The diagram illustrates the decryption process in Regev's cryptosystem. It features two horizontal rows separated by a thick black line. The top row shows an orange box labeled 'r' followed by a purple box labeled 'u=As+e', with a dot operator between them. To the right of this row is the expression  $+ m \cdot \left\lfloor \frac{p}{2} \right\rfloor$ . The bottom row shows an orange box labeled 'r' followed by a purple box labeled 'As', with a dot operator between them. This row is enclosed in large blue square brackets. Below the bottom row is the expression  $\approx 0$ . A thick black horizontal line is positioned between the two rows. A small black horizontal line is located to the left of the top row.

$$\begin{array}{l} \text{---} \\ \text{r} \cdot \text{u=As+e} \quad + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \\ \\ \text{r} \cdot \text{As} \\ \approx 0 \quad + m \cdot \left\lfloor \frac{p}{2} \right\rfloor \end{array}$$

# Properties of LWE

- Equivalence 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  $m \times n$  ( $m \geq n \log p$ ), 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  $\mathbb{Z}_q[x]/\Phi_m(x)$ , where  $\Phi_m$  is the  $m$ -th cyclotomic polynomial of degree  $\varphi(m)$ 
  - e.g.,  $\Phi_{2n} = x^n + 1, n = 2, q = 13$ .
  - $x^2 = -1 \pmod{x^2 + 1}$
  - $12x^3 + 15x^2 + 9x + 25 \rightarrow 12x^3 + 2x^2 + 9x + 12 \rightarrow x - 2 + 9x + 12 \rightarrow (10, 10)$ .
- Lattice is defined as an ideal  $I \subseteq \mathbb{Z}[x]/\Phi_m(x)$ .
- 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  $\mathbb{Z}_q[x]/\Phi_m(x)$ , and so can be described using  $O(n \log q)$  bits.



# NTT Transform

Consider  $\Phi_m$ , 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.  $q = 1 \pmod{2n}$ .
- 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  $(g^a)^n = -1 \pmod{q}$ . Modulo  $x^n + 1$  means  $x^n = -1$ .
  - Let  $\gamma_1, \dots, \gamma_n$  be the  $n$  number of  $2n$ -th primitive roots
- For a polynomial  $p(x) \in Z_q[x]/x^n+1$
- For every  $\gamma_i$ ,  $p(\gamma_i) \pmod{p}$  is equal to taking  $p(x)$  modulo  $x^n + 1$  and modulo  $q$  and then evaluating the reduced polynomial at  $\gamma_i$ .

# 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

$P_1$

$P_2$

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

$s_1$

$s_2$

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

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

RECONCILIATION

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

# Fully Homomorphic Encryption

- Key Generation: Sample  $g^{(i)}, u^{(i)}$  from  $\chi$ 
  - Secret Key:  $f^{(i)} = 2u^{(i)} + 1$
  - Public Key:  $h^{(i)} = 2g^{(i)}(f^{(i)})^{-1}$

- Encrypt a bit  $b$ :

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

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

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

- 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”  $l$
- 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  $sk_{i+1}$ :

$$- \zeta_\tau^{(i+1)} = h^{(i+1)} s_\tau^{(i+1)} + 2e_\tau^{(i+1)} + 2^\tau (f^{(i)})^2$$

$$- \{s_\tau^{(i+1)}, e_\tau^{(i+1)}\} \leftarrow \chi, \tau \in [0, \log q_i]$$

- Given ciphertext  $c^{(i)}$ , let  $c_\tau^{(i)}$  denote the polynomial consisting of the  $\tau$ -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  $(f^{(i)})^2$ .