Ring-LWE Example

Parameters:

$$n = 4$$
$$p = 101$$
$$k = 20$$

meaning of small: coefficients from $\{1, 0, -1\}$

Key Generation

Private key:

$$s = x^3 + 100$$

Errors for use in public key:

$$e = x^3 + x^2 + 100x$$

Public key:

$$a = 83x^3 + 23x^2 + 51x + 77$$
$$b = as + e = 96x^3 + 97x^2 + 26x + 74$$

Encryption

Message $m \in \{0, 1, 2, 3, 4\}$. Let's say $m = 3$.

Ephemeral key:

$$r = 100x^2 + 100x$$

Errors for use in ciphertext:

$$e_1 = x^2$$
$$e_2 = 100x^2 + x$$

Ciphertext:

$$v = ar + e_1 = 27x^3 + 75x^2 + 6x + 5$$
$$w = br + e_2 + km = 79x^3 + 23x + 51$$

Decryption

Decryption formula:

$$w - vs = x^2 + 3x + 62$$

Rounding to the nearest 20:

$$60 = 3k$$

Therefore the message is 3.