The Ring-LWE Ring

We choose a moderately large prime p and a moderately large dimension n, which should be a power of 2. We define

$$R_p := \mathbb{F}_p[X]/(X^n + 1).$$

This is a ring with p^n elements, namely

$$R_p = \{a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0 : a_i \in \mathbb{F}_p\}.$$

Ring-LWE Encryption

The public set up involves the following:

1. A prime p and dimension n and resulting Ring-LWE ring R_p.
2. A moderately large integer $k \in \mathbb{Z}$.
3. A notion of "small," as applied to elements of R_p. For our purposes, we take this to be the elements

   $$\{a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0 : a_i \in \{0, 1, -1\}\}.$$

   In other words, a polynomial of R_p is small if its coefficients are all 0 or ± 1.

Bob creates a private/public key pair.

1. Bob selects a small random element s of R_p.
2. Bob selects a small random element e_1 of R_p.
3. Bob defines $(a, b = as + e_1) \in R_p \times R_p$.

The element e_1 can be thrown away. Bob keeps s as his secret key and makes (a, b) public as his public key.

Alice encrypts a message.

A message means an integer $0 < m < p/k$. Encryption proceeds as follows:

1. Alice selects a small random $r \in R_p$. This is the *ephemeral key.*
2. Alice selects small random $e_2, e_3 \in R_p$.
3. Alice defines

   $$v = ar + e_2, \quad w = br + e_3 + km.$$

Alice may discard k, e_2 and e_3. The ciphertext is (v, w), which she sends to Bob.

Bob decrypts the message.

Bob does the following to decrypt:

1. Compute $x = w - vs$.

2. Round x to the nearest multiple of k.

3. The result should be an integer; divide it by k, revealing the message m.

Verifying correctness: choosing parameters

To verify that this works, observe that

$$w - vs = km + br + e_3 - ars - se_2 = km + re_1 + e_3 - se_2$$

where $re_1 + e_3 - se_2$ is a 'fairly small' element of R_p. If this is really 'fairly small', then rounding to the nearest multiple of k gives km. Dividing by k reveals m.

To make this 'fairly small' precise, we have a lemma:

Lemma 1. *Suppose that a and b are short elements of R_p. Then ab has coefficients not exceeding $2n$.*

Proof. Suppose $a = \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ and $b = \beta_{n-1}X^{n-1} + \cdots + \beta_0$. The proof is simply the multiplication of polynomials: the coefficient of X^i in ab (before modding out by $X^n + 1$) is given by

$$\sum_{j+k=i} \alpha_j \beta_k.$$

Since $\alpha_i, \beta_i \in \{0, 1, -1\}$, this has magnitude at most $i + 1 \leq n$. The highest power of X before modding out is X^{2n-2}. So when modding out by $X^n + 1$, we combine certain coefficients (those of X^i and X^{i+n}). This can at most double the size of the coefficients. □

Using this lemma, it is possible to bound the absolute value of the coefficients of the quantity $re_1 + e_3 - se_2$ by at most $4n + 1$. So, provided that $k/2 > 4n + 1$, we are guaranteed that the decryption process will work. In fact, it will almost always work even with somewhat looser conditions, since the bound is determined by the worst case scenario, not the average case scenario.

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.