Exercise 10.1

Task

Prove the claim made in the text: assume that the distribution D_e satisfies that $\sum_{i=1}^{m} |e_i| < \frac{q}{4} - 1$ when each e_i is chosen according to D_e. Then the decryption defined for the public key LWE scheme always works correctly.

Solution

Let's remind ourselves that the encryption is:

$$E(w) = (\sum_{i=1}^{m} b_i a_i, \sum_{i=1}^{m} b_i(a_i s + e_i) + \lceil \frac{q}{2} \rceil w)$$

The decryption is defined as:

$$D(u, v) = v - su$$

To prove that decryption works every time we can just expand it and see what we get:

$$v - su = \sum_{i=1}^{m} b_i(a_i s + e_i) + \lceil \frac{q}{2} \rceil w - s \sum_{i=1}^{m} b_i a_i =$$

$$\sum_{i=1}^{m} b_i a_i s + \sum_{i=1}^{m} b_i e_i + \lceil \frac{q}{2} \rceil w - s \sum_{i=1}^{m} b_i a_i s = \sum_{i=1}^{m} b_i e_i + \lceil \frac{q}{2} \rceil w$$

In the worst case all b_i are going to be 1, so $\sum_{i=1}^{m} b_i e_i < \sum_{i=1}^{m} e_i$, but we know that thanks to the distribution D_e we expect this sum to be less than $\frac{q}{4} - 1$.

According to the algorithm definition

$$D(u, v) = \begin{cases} 0 & \text{if } v - su \text{ is closer to } 0 \text{ than to } \frac{q}{2} \\ 1 & \text{otherwise} \end{cases}$$

This makes sense because $v - su$ takes values $w \pm \frac{q}{4}$ as we saw from the above results. Therefore:

- If $w = 0$, $v - su = 0 \pm \frac{q}{4}$, which is indeed closer to 0, than to $\frac{q}{2}$.
- If $w = 1$, $v - su = \frac{q}{2} \pm \frac{q}{4}$, which is indeed closer to $\frac{q}{2}$ than to 0.

This of course works in the negatives as well, because we're working in mod q.

And the $w = 0$ case we have that $0 \equiv q$, so when we say that $v - su$ is closer to 0, it can also be closer to q.

i.e. When $w = 0$, $v - su$ is in the interval $(0, \frac{q}{4}) \cup (\frac{3q}{4}, q)$.

When $w = 1$, $v - su$ is in the interval $(\frac{q}{4}, \frac{3q}{4})$.

The edge points like $\frac{q}{4}$ aren't clear what result they should return, but they are unlikely due to the D_e's distribution.