Cryptology Exercise Week 10

Zijun Yu 202203581

Octobor 2023

Correctness of LWE-based encryption

We have the ciphtertext $(\mathbf{u}, v)$, where

$$u = b_1\mathbf{a_1} + b_2\mathbf{a_2} + ... + b_m\mathbf{a_m}$$

and

$$v = b_1(\mathbf{a_1} \cdot \mathbf{s} + e_1) + b_2(\mathbf{a_2} \cdot \mathbf{s} + e_2) + ... + b_m(\mathbf{a_m} \cdot \mathbf{s} + e_m) + \lceil q/2 \rceil w$$

The decryption is $v - \mathbf{s} \cdot \mathbf{u}$, which is

$$b_1e_1 + b_2e_2 + ... + b_me_m + \lceil q/2 \rceil w$$

Because $\sum_{i=1}^{m} |e_i| < q/4 - 1$, we have

$$|b_1e_1 + b_2e_2 + ... + b_me_m| <= \sum_{i=1}^{m} |e_i| < q/4 - 1$$

So in the case of $w = 0$, the ciphtertext is $b_1e_1 + b_2e_2 + ... + b_me_m$, of which the absolute value is less than $q/4 - 1$, hence it is closer to 0 than to $\lceil q/2 \rceil$, so the decryption is 0. In the case of $w = 1$, the ciphtertext is $\lceil q/2 \rceil - X$ where $|X| < q/4 - 1$, hence it is closer to $\lceil q/2 \rceil$ than to 0, so the decryption is 1.