

Assignment question

1. This question is about the third generation of fully homomorphic encryption scheme GSW. This is a FHE from Learning with Errors which is conceptually simpler, asymptotically faster and attribute based.

Suppose we have a ciphertext C is a $N \times N$ matrix. The secret key v is a N -dimensional vector. We say C encrypts μ when $C \cdot v = \mu \cdot v + e \bmod q$ where e is a small error vector and q is some modulus.

- a. If we use $C \cdot v = \mu \cdot v \bmod q$, it's already homomorphic, why are we still using $C \cdot v = \mu \cdot v + e \bmod q$? Try to explain in two to three sentences.
- b. Given that e is a small error vector, what range should e be in?
- c. Let $C_1 \cdot v = \mu_1 \cdot v + e_1 \bmod q$, and $C_2 \cdot v = \mu_2 \cdot v + e_2 \bmod q$
Calculate the new error of $C_1 + C_2$
Calculate the new error of $C_1 \times C_2$
Will addition or multiplication make the error grow faster?

2. Before moving on to Q3, let's take a short review on Diffie-Hellman Key Exchange. Suppose that Alice and Bob are trying to simulate DHKE. Show your steps on how to calculate the shared key.

$$p = 97, g = 5$$

$$\text{Alice: } a = 9$$

$$\text{Bob: } b = 11$$

3. Take a look at the dhke.py. Here's a message that's encrypted by Alice using DHKE. Use the provided information in the file to decrypt the message. Paste the decrypted message below: