Assignment 1

Questions

q1. (10%) Install and play with the HE package TenSEAL

q2. (25%) Operation exercise with BFV scheme

1. Encrypt the last 3 digits of your SID (or SID mod 1000).
2. Multiply the encrypted number by 914.
3. Store the multiplication result (a cyphertext) and the private key in a pickle object. Please refer to the section submission guideline for formatting.

Notes: Since TenSEAL encrypts an array instead of an integer, we will only check the first element of your encrypted result.

q3. (25%) Operation exercise on given encrypted data

Download your cyphertext a, b, and public key (context) from this folder, then compute `a * (SID % 1000) + b`. Please also store the computed result in the pickle object.

Files will be uploaded before 9/15 12:30. Since there are still students registering, if you can't find your SID, please reach out to the TA.

You can refer to the following code to extract data:

```
import tenseal as ts
import pickle

with open('{YOUR_STUDENT_ID}.pkl', 'rb') as f:
    given = pickle.load(f)

context = ts.context_from(given['context'])
encrypted_a = ts.bfv_vector_from(context, given['encrypted_a'])
encrypted_b = ts.bfv_vector_from(context, given['encrypted_b'])
```

q4. (40%) Noise observation

Multiply a number with another number multiple times and add a number with another number multiple times by the CKKS scheme. Then, observe the noise introduce by the two operations and explain why the noises are different. Write your observation in a short report and submit your report (PDF) to the system. **The font size is 12, and the page limit is 1 page.**

Submission Guideline

Please compress your files named `{SID}_a1.zip` (SID in upper case) to the COOL System, such as `D111111_a1.zip`, with two required files

file 1. `{SID}_a1.pkl`

Please store your outputs of **q2** and **q3** as follows.
Notes: To dump the pickle object, all objects need to be serialized first.

```
result = {
  'q2_context': context.serialize(save_secret_key=True),
  'q2_result': q2_ciphertext.serialize(),
  'q3_result': q3_ciphertext.serialize()
}
```

files 2. `{SID}_a1_report.pdf`

Supplementary Materials

TenSEAL installation: https://github.com/OpenMined/TenSEAL
Package the tutorials:
https://github.com/OpenMined/TenSEAL/blob/main/tutorials/Tutorial%200%20-%20Getting%20Started.ipynb