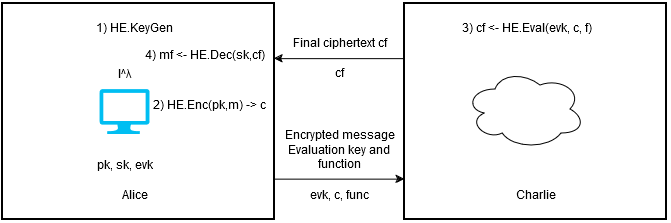
Task – 1



1. Alice generates keys (pk, sk, evk) using λ as security parameter.
2. Message m is encrypted using pk and ciphertext c is created.
3. Ciphertext c is sent to the cloud (Charlie) along with function f and evaluation key.
4. Charlie computes function f on ciphertext c and then encrypts it with eval key.
5. Final ciphertext cf is sent to Alice
6. Alice decrypts it using her private key and gets message back with function f applied on it.

Task – 2

A computer screen with numbers and letters

Description automatically generated

./simple-integers output

A screen shot of a computer

Description automatically generated

./mycode output

A computer screen with blue and white text

Description automatically generated

./mycode with 10 vectors output

Task – 3

A screenshot of a computer

Description automatically generated

./mycode with 10 vectors and some metrics

Key Generation Time: 34 ms

Public Key Size: 14 bytes

Secret Key Size: 14 bytes

Eval Key Size: 1.8 mega bytes

Encryption Time: 209 ms

Evaluation (Addition) Time: 3 ms

Decryption Time: 3 ms

Based on this output we can see that public key and secret key are similar in size, they actually had only a few bits different which I manually checked and thought they are the same.

Running diff

diff public\_key.txt secret\_key.txt

1c1

< 0x625bd82f54f0

\ No newline at end of file

---

> 0x625bd829c1e0

\ No newline at end of file

The eval key is the biggest being 1.8MB in size. The key generation size is 34ms which is quite fast as well. Encryption time is slower around 200ms. Evaluation time is quite small which was unexpected for me. Decryption is fast again 3ms.

Encryption is slow because it involves a lot of complex mathematical computations such as generating noise etc.

Evaluation is fast since its usually a simple function like addition in this case.