

Building a Fully Homomorphic Encryption Scheme in Python

GROUP NAME:
哈利波特



MEMBERS



王振倫	資工三	110550068
施柏江	資工三	110550108
林英碩	資工三	110550117
呂偉祥	資工三	110550115





01

ABSTRACT



Abstract



In this project, we will demonstrate Fully Homomorphic Encryption (FHE) with the BFV algorithm by showcasing addition and multiplication results, explaining the implementations in detail.

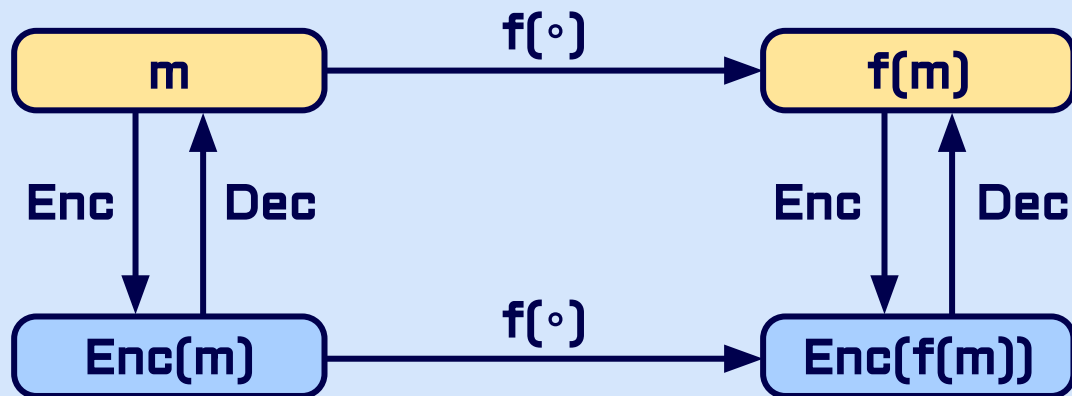
We also apply FHE in three scenarios:

1. Registering grades without publishing them
2. Verifying possession of a secret key with server and client GUI
3. Securely transmitting an image between server and client using agreed base photos



INTRODUCTION 02

Homomorphic Encryption

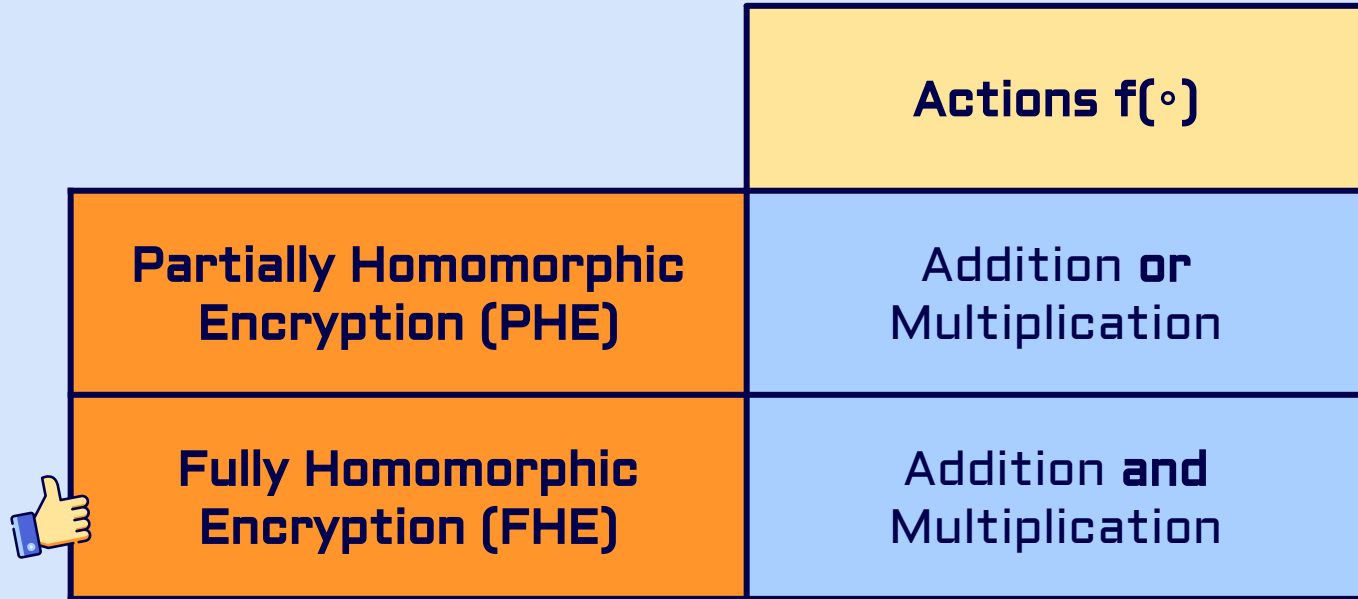


同態加密 (Homomorphic Encryption) 允許對加密後的資料執行計算並獲得加密結果，而不需要解密完才進行計算。


$$Enc(m_1 \circ m_2) = Enc(m_1) \circ Enc(m_2)$$



Fully Homomorphic Encryption (FHE)



The diagram is a table with two columns and three rows. The first column lists encryption types, and the second column lists the actions they support. The first row is a header with a yellow background. The next two rows have orange backgrounds for the first column and light blue for the second column. A thumbs-up icon is next to the 'Fully Homomorphic Encryption (FHE)' row. A large yellow arrow points from the left towards the table, and another points from the table towards the right. A curved orange line with dots is in the top right corner.

	Actions $f(\circ)$
Partially Homomorphic Encryption (PHE)	Addition or Multiplication
 Fully Homomorphic Encryption (FHE)	Addition and Multiplication



03



SYSTEM ARCHITECTURE



System Architecture

$\text{KeyGen}(1^\lambda) \rightarrow \text{sk}, \text{pk}$

密鑰生成算法
生成密鑰 sk & 公鑰 pk

$\text{Enc}(\text{pk}, m) \rightarrow \text{ct}$

利用 pk 對明文 m 進行加密
生成密文 ct

$\text{Eval}(f, \text{ct}_1, \dots, \text{ct}_k) \rightarrow \text{ct}'$

將 k 個密文進行 $f(\circ)$ 的運算
得到加密後的結果 ct'

$\text{Dec}(\text{sk}, \text{ct}') \rightarrow m'$

利用 sk 對運算後的密文 ct' 進行解密
解出 $m' = \text{Eval}(f, m_1, \dots, m_k)$

對密文進行操作等同對明文進行同種操作

BFV Algorithm

BFV 是 FHE 中的一種核心方案, 基於 Ring-Learning With Errors (RLWE) 問題, 其同態性在於多項式環。

$$\text{KeyGen}(1^\lambda) \rightarrow \text{sk}, \text{pk}$$

$\text{sk} = s$ 是係數皆為 $\{-1, 0, 1\}$ 的多項式, $\text{pk} = \{[-as + e]_q, a\}$

其中 a 為 cipher space (q) 中隨機選出的多項式, e 為隨機噪聲多項式

因此接收者無法透過 pk 來推導出 sk , 能夠有效保護隱私

$$\text{Enc}(\text{pk}, m) \rightarrow ct$$

利用 pk 進行加密, 同時生成三個隨機數: e_1, e_2, u

其中 e_1, e_2 為噪聲, u 為類似 sk 的多項式

$$ct = \{[pk_0 u + e_1 + qm / t]_q, [pk_1 u + e_2]_q\}$$

$$\text{Dec}(\text{sk}, ct') \rightarrow m'$$

利用 $\text{sk} = s$ 進行解密, 計算 $ct' = ct_0 + ct_1 s = [qm / t + e_1 + eu + e_2 s]_q$

其中噪聲足夠小能夠忽略

$$\text{因此可得明文 } m' = [(t / q)[ct_0 + ct_1 s]_q]_t$$


$$\text{Eval}(f, ct_1, \dots, ct_k) \rightarrow ct'$$


Addition:


$$ct_1 = \{[pk_0 u_1 + e_1 + qm_1 / t]_q, [pk_1 u_1 + e_2]_q\}$$

$$ct_2 = \{[pk_0 u_2 + e_3 + qm_2 / t]_q, [pk_1 u_2 + e_4]_q\}$$

$$ct' = ct_1 + ct_2$$


$$= \{[pk_0(u_1 + u_2) + (e_1 + e_3) + q(m_1 + m_2) / t]_q, [pk_1(u_1 + u_2) + (e_2 + e_4)]_q\}$$

$$= \{[pk_0 u_3 + e_5 + qm_3 / t]_q, [pk_1 u_3 + e_6]_q\}$$


可見 ct' 的形式與一般的密文 ct_1, ct_2 一樣, 因此解密 ct' 能得到 $m_1 + m_2$


$$\text{Eval}(f, ct_1, \dots, ct_k) \rightarrow ct'$$

Multiplication:


$$ct_1 = [a_0 + a_1s]_q = qm_1 / t + e_1$$

$$ct_2 = [b_0 + b_1s]_q = qm_2 / t + e_2$$

$$ct' = ct_1 \times ct_2 \times (t / q)$$

$$= qm_1m_2 / t + e_1m_2 + e_2m_1 + (t / q)e_1e_2$$

$$= [a_0b_0 + (a_0b_1 + a_1b_0)s + a_1b_1s^2]_q$$

其中 a, b, s 為已知條件，因此解密能夠利用密鑰 s 去做解密，得到 m





EXPERIMENTS



04



Results



實驗流程

1. 將 m_1, m_2 做加密運算
2. 解密運算結果
3. 觀察是否與 m_1, m_2 直接做相同運算後的結果相等
(此算法加法跟乘法都有支援)

```
true m1+m2:
[ 2.  3.  0. -4. -4. -2. -4.  4.]
decrypted ct1+ct2:
[ 2.  3.  0. -4. -4. -2. -4.  4.]
true m1*m2:
[ 4.  4. -2.  4. -1.  0. -2.  4.]
decrypted ct1*ct2:
[ 4.  4. -2.  4. -1.  0. -2.  4.]
true m1*m2*m3*m4
[-4.  2. -3.  1.  0.  4. -2. -2.]
decrypted ct1*ct2*ct3*ct4
[-4.  2. -3.  1.  0.  4. -2. -2.]
true a+b:
5000
decrypted ct1+ct2:
[5000.]
true a*b:
5389461
decrypted ct1*ct2:
[5389461.]
```



Application 1

助教想登記成績，但還不想公布讓所有人看。





Application 2


Server 希望確認 client 是否擁有 secret key,
且 client 不能告訴 server 這個 secret key。





Application 3

Server & client 雙方先說好用兩張照片當作 base,
server 希望安全地傳圖片給 client。





05

CONTRIBUTION



Contribution

- 提供一個保密登記成績的方法
- 提供一個驗證對方身分的方法
- 提供一個安全傳送圖片的方法



References

- Microsoft SEAL
- BFV全同态基本概念概述
- Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme
- BFV全同态密码实现和应用: 图片加密