Final Project: FHE-secured CAPTCHA Solver

蕭凱鴻 B13902046, 蔡兆豐 B13902110

1. 目標

模擬一個場景，使用者的 CAPTCHA 輸入會加密，伺服器對加密輸入與正確答案進行匹配驗證，不需看到明文。挑戰：如何在 FHE 下做字元等值比較。

2. 實作架構

我們全部都使用 python 實作，搭配 zama 官方提供的 concrete API 來達到 FHE 加密。程式分為 4 個檔案：`app2.py`、`client.py`、`server.py`、`service.py`。

啟動 `python app2.py` 以後會聯絡 `server.py`。server 會生成隨機的 6 個字元字串並編譯好用來加密比較兩個字串的 circuit，把 circuit 的計算部份和加密後的正確答案交給 `service.py`。然後 app 會在 `127.0.0.1:5000` 啟動 flask 框架的網頁，顯示 captcha 圖片給使用者。

使用者輸入完以後，會由 `client.py` 加密完把東西傳給 `service.py` 做運算，和正確答案做逐字比較，要每個字元的 FHE 加密都和答案一樣才算成功。比較完成以後會把結果回傳給 client 和 server，就能進到認證成功或失敗的頁面。

3. 一些問題

關於這樣的架構，由於 zama 並沒有在 python 支援編譯器產生的 public key 傳送，要的話只能用 rust 寫。

4. Github

`https://github.com/GrandTiger1729/BDA-FHE.git`