

# 自傳

姓名：許峻豪

學校：國立中正大學資訊工程學系(預計 2024 年畢業)

## 一、畢業專題

題目：使用向量化技術優化與實作雙方安全運算 C/C++函式庫([連結](#))

專題指導教授：陳鵬升教授

### ● 多方安全運算介紹

身處一個資訊發達的年代，從生活中便可以感受到資訊為我們的生或帶來多大的便利，也因此資訊安全也逐漸被重視。多方安全運算讓多個使用者可以在不用交換敏感資料的情況下，用多方的資料來進行加密計算並達到目的。

### ● 研究動機與問題

因為資訊安全重要性的提高，資料本身的隱私也受到很大的重視。多方安全運算可以做為某些問題的解決手段，但此技術尚未成熟，而為了安全性也勢必會影響到程式的執行速度，進而降低了實用性。

我們是使用 ABY Library 來實作多方安全運算，它會幫忙程式在進行運算前，將資料加密，計算後再解密。而我們的專題為 ABY Library 的使用者可以更方便的撰寫多方安全運算的程式。

### ● 專題成果

ABY 版本的 math.h：我們以 C/C++的 math.h 為原型實作出了 MPC\_math.h，讓使用者再撰寫 ABY 的程式時，可以更方便的使用原本 math.h 的功能，不用再自己用 ABY Library 重新寫一個 function，大幅度的加快程式的開發速度。  
提高 ABY Library 效能：透過 ABY Library 提供的範例程式，我們找出這些範例程式中最常出現且最花時間的 function，並且優化該 function 的效能。

## 二、專業能力

C/C++：

實作 aggregation tree([資料結構作業](#))

HTML/CSS：

軟體工程期末專題的前端部分([demo 影片](#))

Python：

利用深度學習來預測餐廳特定日期的客人數([深度學習概論期中考](#))

## 三、特殊經歷

1. 教育部 ITSA 極客挑戰賽初賽通過([證明](#)、[決賽名單](#))
2. 曾在國立中正大學資訊處資源管理組協助管理部分網頁([證明](#))
3. 參加華文哲學百科網頁維護 2022-2023 建置計畫([證明](#))

#### 四、課業表現

GPA：3.4

系排名：58/100

班排名：28/52

學業成績總平均：0.37

作品集：<https://github.com/howcat/introduction>

#### 五、自我介紹

我是許峻豪，現在就讀國立中正大學資訊工程學系四年級。在資工系中，我學會了許多有關本科系的專業能力，我也相信，我學會的技術背景會對我未來在資訊工程研究所的學習以及研究提供堅實的基礎。而在學習及做專題的過程中，透過所學，一步一步地發現問題、尋找資料、解決問題，解決問題的那一刻的成就感是我升大學時選擇資工系的原因之一，很高興直到現在，解決問題的時候，我依然會感到那一絲成就感。

有關於我的畢業專題，多方安全運算的開發確實相當不易，比當初想像的難度更高一些，但我和組員仍在教授的建議下，一步一腳印的逐步完善研究成果。過程中，我們曾將一個原本執行時間需要 200 秒以上的 function，透過不斷的查資料和 debug，努力壓縮到了 50 秒上下。雖然我也知道，可能有更好的解法，可能有人可以壓縮到更短，而執行時間需要 50 秒的 function 以實用性來說其實也不大，但我也不會覺得我是可以一步登天的人，比起最好的結果，我更希望自己至少要做到力所能及的最好。