

國立交通大學
National Chiao Tung University

出國報告（出國類別：☐ A 類、考察訪問
☒ B 類、出國短期研究
☐ C 類國際會議）

2011 年哈佛大學比爾蓋茲榮譽講座教授孔祥重教授實驗室
短期交流

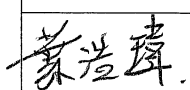
服務機關：電機資訊學士班

姓名職稱：葉浩瑋 學生

前往國家：美國 波士頓, 麻州 哈佛大學

出國期間：2011/08/07~09/18

報告日期：2011/09/30

撰 寫 人	審 核 人	初 閱	複 閱
 葉浩瑋			

備註：出國報告書審核程序如下

- 一、初閱：各學院教師 A、B、C 類及其他行政單位 A 類由單位主管，研究生由指導教授；中心計畫及學群 A、B、C 類由各中心計畫主持人。
- 二、複閱：經費所屬之一級單位；中心計畫及學群 A、B、C 類由頂尖計畫執行長。

一、摘要

本人首次榮獲電資班遴選，前往美國哈佛大學接受孔祥重院士之指導，參與實驗室中計畫 IC Trojan Detection via Compressive Sensing。此次計畫中，成員除了孔院士實驗室之研究團隊外，還包括來自台灣大學博士生蔡一民，負責 Trojan Detection Circuit 之電路功能設計，台灣大學碩士畢業生黃耿彥，負責 Trojan Detection Circuit 之電路硬體設計，及本人葉浩瑋，負責：1. 利用 MATLAB 進行模擬，觀察與了解 Central Limit Theorem。2. 了解 Trojan Detection Circuit 電路之錯誤偵測率，將隨著電路內 gate 的 leakage power 之機率分布曲線標準差增大而增大。3. 比較不同 Sensing matrix 在 Compressive Sensing 中執行效能之差異程度。

本次短期交流計畫出國報告詳如下文所述。

二、目次

● 本文.....	P.4
■ (一) 目的.....	P.4
■ (二) 過程.....	P.4
■ (三) 心得及建議.....	P.10
● 附錄.....	P.11

三、本文

(一) 目的

國立交通大學電機學院與資訊學院電機資訊學士班秉持交大「知新致遠、崇實篤行」的學風，本年度首次推動選送優秀同學赴美國哈佛大學比爾蓋茲榮譽講座教授孔祥重教授實驗室進行短期交流，以期激發雙邊國際合作更優質的研究成果，培育具跨領域整合溝通能力之領袖人才。

(二) 過程

1. 甄選階段：

本人於二月初獲悉系上於本年度首次推動選送優秀同學赴美國哈佛大學比爾蓋茲榮譽講座教授孔祥重教授實驗室進行短期交流，基於希望了解頂尖學府之研究環境，並學習參與國外頂尖實驗室研究計畫之經驗，本人積極參與遴選，並榮幸於四月通過甄選，正式展開此次研究之歷程。

2. 行前準備階段：

在實際參與計畫前，為建立與研究主題 Compressive Sensing 相關之背景知識，承蒙孔院士之提式，先期閱讀文獻資料(請參照附錄[1]-[8])，並自行辦理出國簽證與當地住屋租賃相關事宜。

3. 參與計畫階段：

(1) 了解環境團隊與分工：

地點：美國哈佛大學 Maxwell Dworkin 大樓，孔祥重院士的實驗室

研究人員：

指導教授：孔祥重院士

學生：

原研究團隊：Youngjune L. Gwon, Dario Vlah

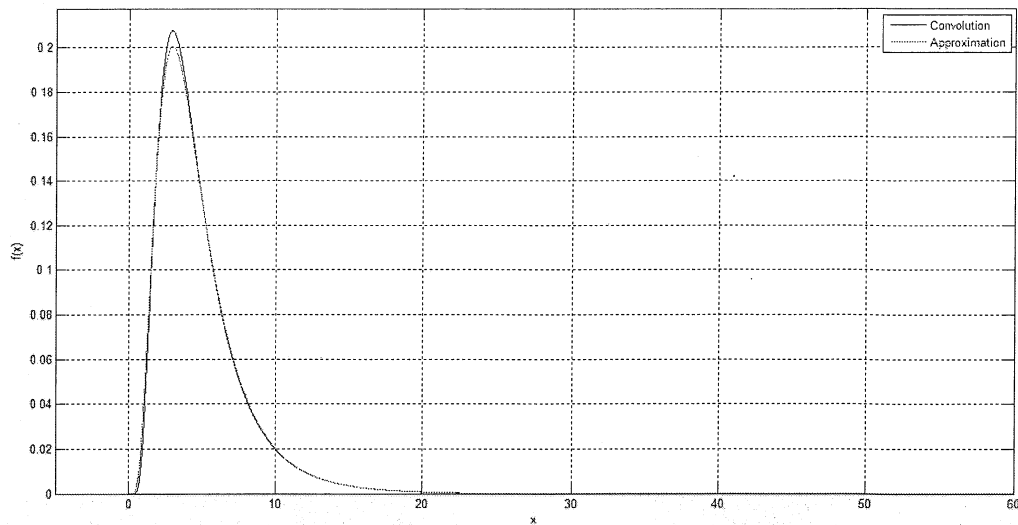
國立台灣大學：蔡一民，黃耿彥

國立交通大學：葉浩瑋

研究主題：IC Trojan Detection via Compressive Sensing

(2) MATLAB 之學習：

本人於 8/10 首次進入實驗室，由一民學長提供模擬軟體 MATLAB，即於 8/10~8/15 了解 MATLAB 之基本操作方法，並於 8/15 第一次定期研究小組會議中提出初次模擬結果如下圖：



我們以 log-normal random variable 來模擬電路中各 gate 的 leakage power。上圖模擬結果顯示兩個 log-normal random variable 相加之後的機率分布，可以以另一個 log-normal random variable 的機率分布來趨近，驗證文獻(請參照附錄[9])中所提及方法之可行性。

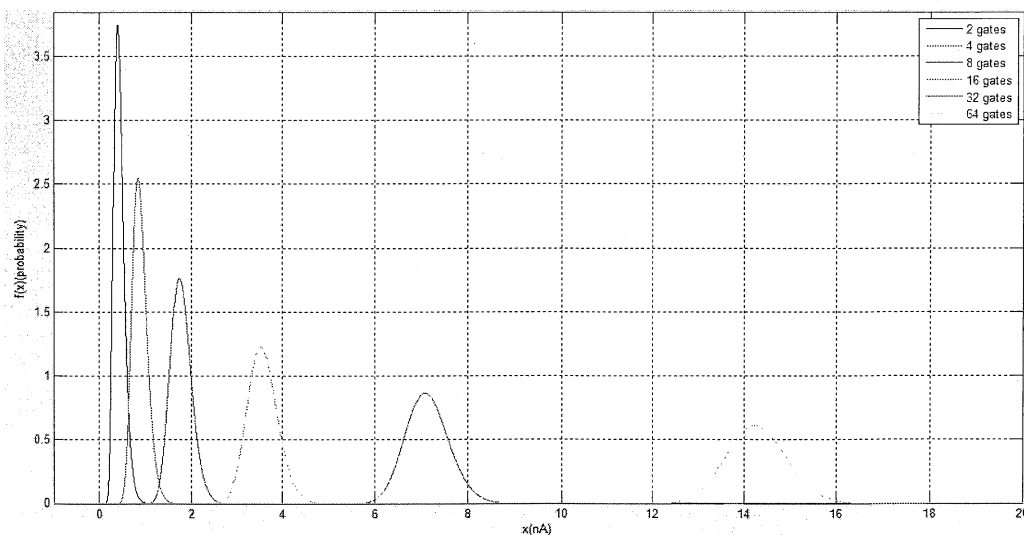
(3)實際參與計畫，配合計畫推動，本人主要完成以下成果：

A. 利用 MATLAB 進行模擬，觀察與了解 Central Limit Theorem：

時間：8/15~8/17

緣由：本人於 8/15 定期研究小組會議中提出初次模擬結果，並在孔院士的指導下，於 8/17 定期研究小組會議中提出 leakage power 機率分布曲線隨 gate 數目增加的改變趨勢圖。

成果：



上圖模擬結果顯示隨著相加之 log-normal random variable 數目增加，總體的機率分布將越來越接近 normal random variable。

學習經驗：由模擬結果觀察相加之 log-normal random variable 逐漸接近 normal random variable 的情形，此即 Central Limit Theorem 中所提及之現象。

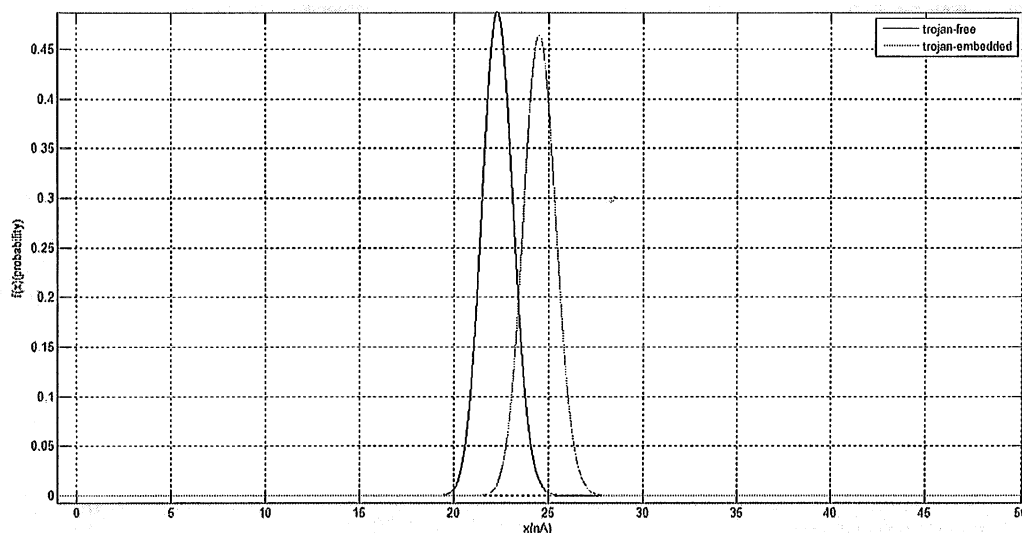
B. 了解 Trojan Detection Circuit 電路之錯誤偵測率，將隨著電路內 gate 的 leakage power 之機率分布曲線之標準差增大而增大：

時間：8/17~8/22

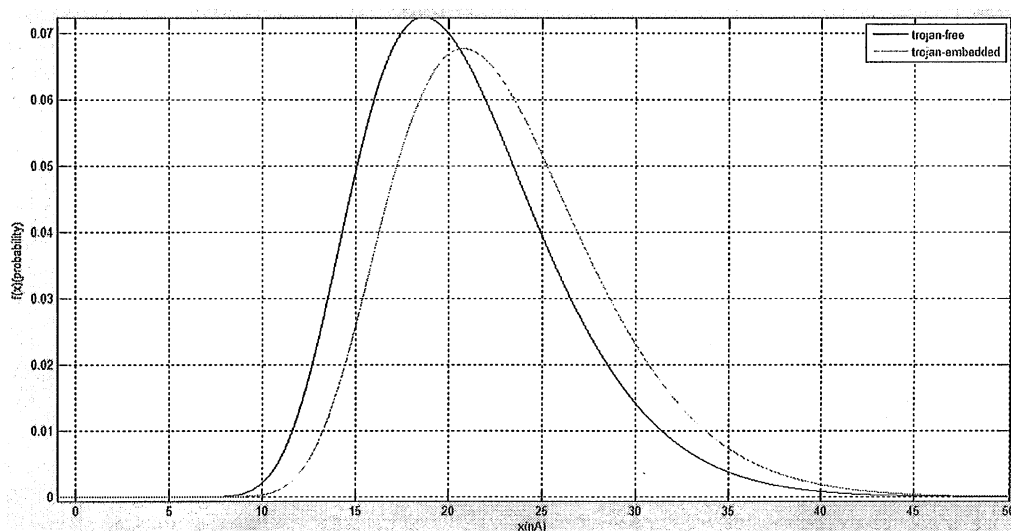
緣由：為了能使我了解 Trojan Detection Circuit 之效能限制，在孔院士的指導下，於 8/22 定期研究小組會議中提出 leakage power 機率分布曲線隨電路內各別 gate 之 leakage power 機率分布曲線標準差增大的改變趨勢圖。

成果：

圖(1)



圖(2)



上圖模擬結果顯示固定被測試電路內之 gate 數目，隨著 gate 的 leakage power 機率分布曲線之標準差增大 (圖(2)之標準差為圖(1)的 10 倍)，無 Trojan 與有 Trojan 的 leakage power 機率分布曲線間的重疊比例增加，這將導致 Trojan Detection Circuit 的偵測效能下降。

學習經驗：了解 Trojan Detection Circuit 的效能將隨著 leakage power 機率分布曲線之標準差增大而下降。

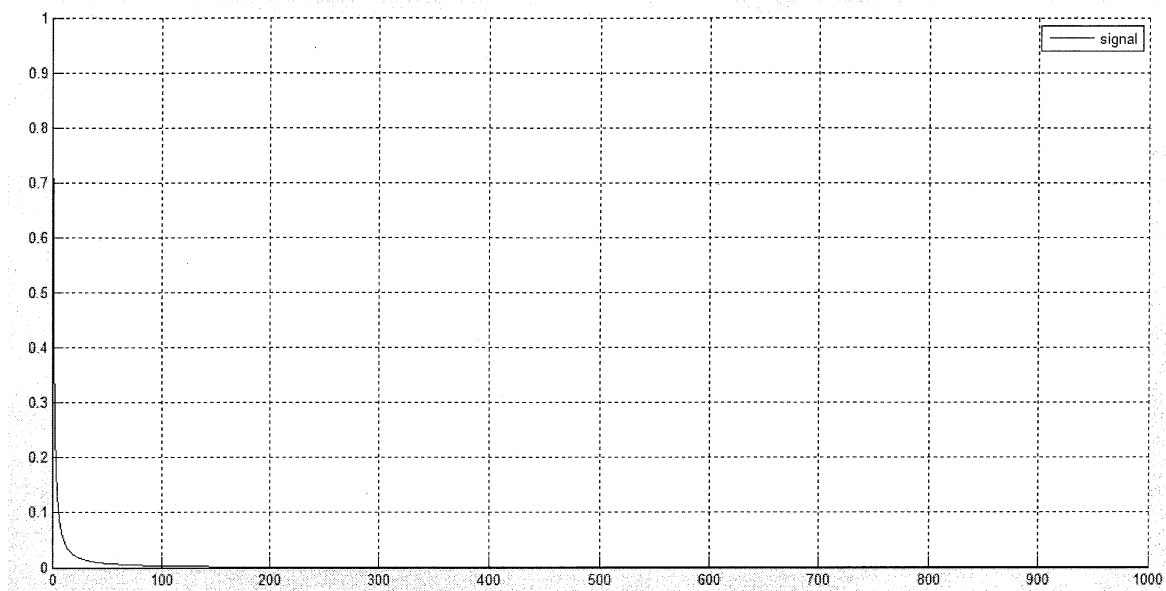
C. 利用 MATLAB 進程式模擬, 比較不同 Sensing matrix 在 Compressive Sensing 中之執行效能之差異程度 :

時間 : 8/22~9/16

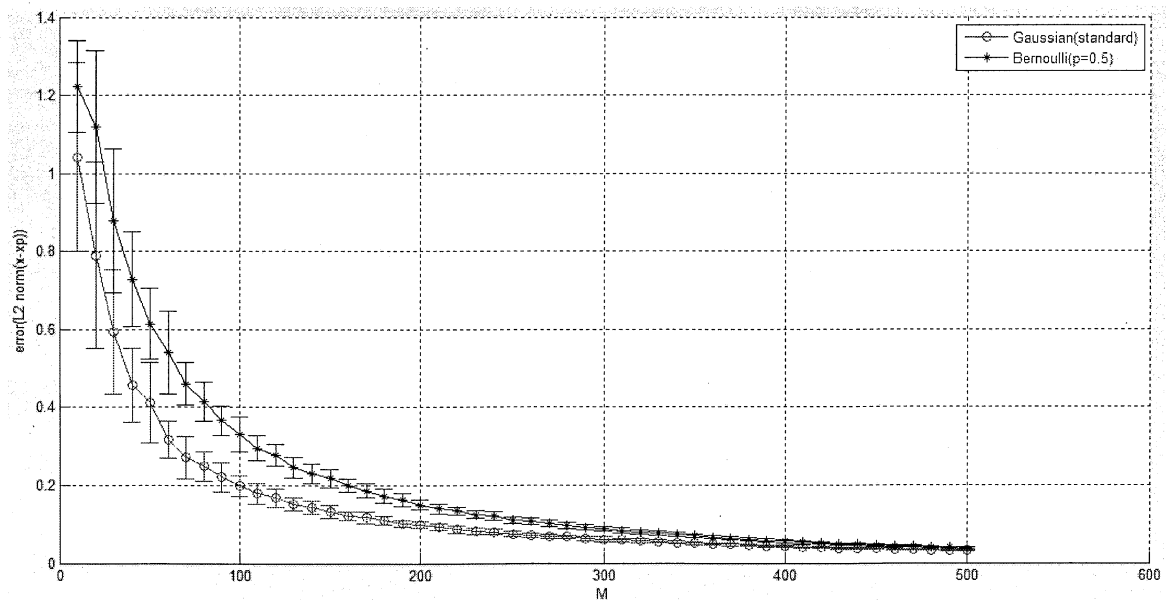
緣由 : 於 8/22 定期研究小組會議中, 孔院士指示擴大學習深度, 利用 Bernoulli matrix 與 Gaussian matrix 作為 Compressive Sensing 的 Sensing matrix, 比較兩者間之效能差異。

成果 :

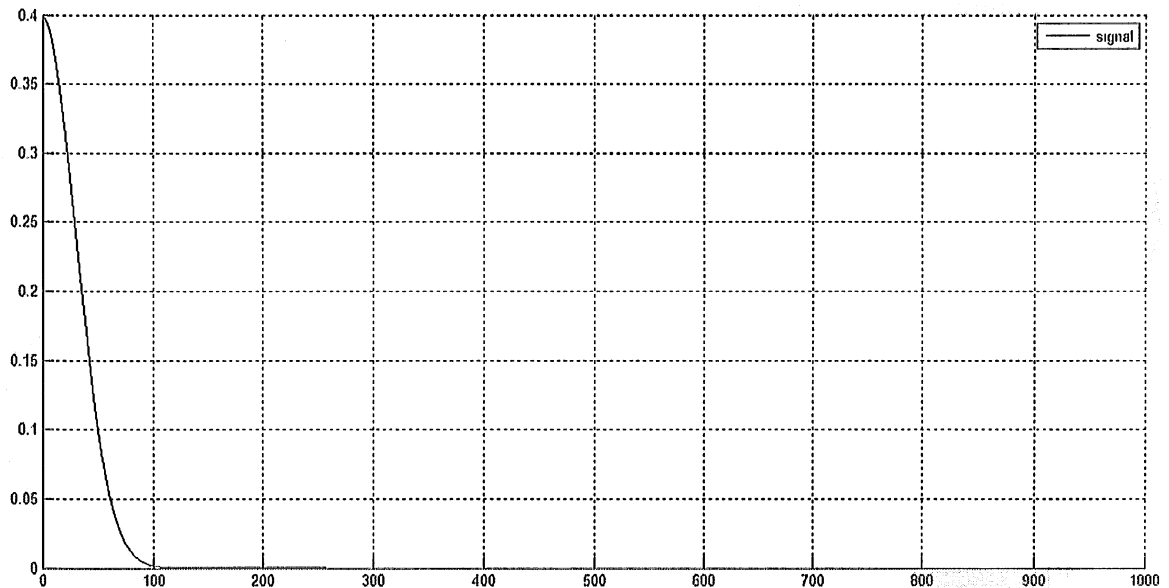
圖(1)



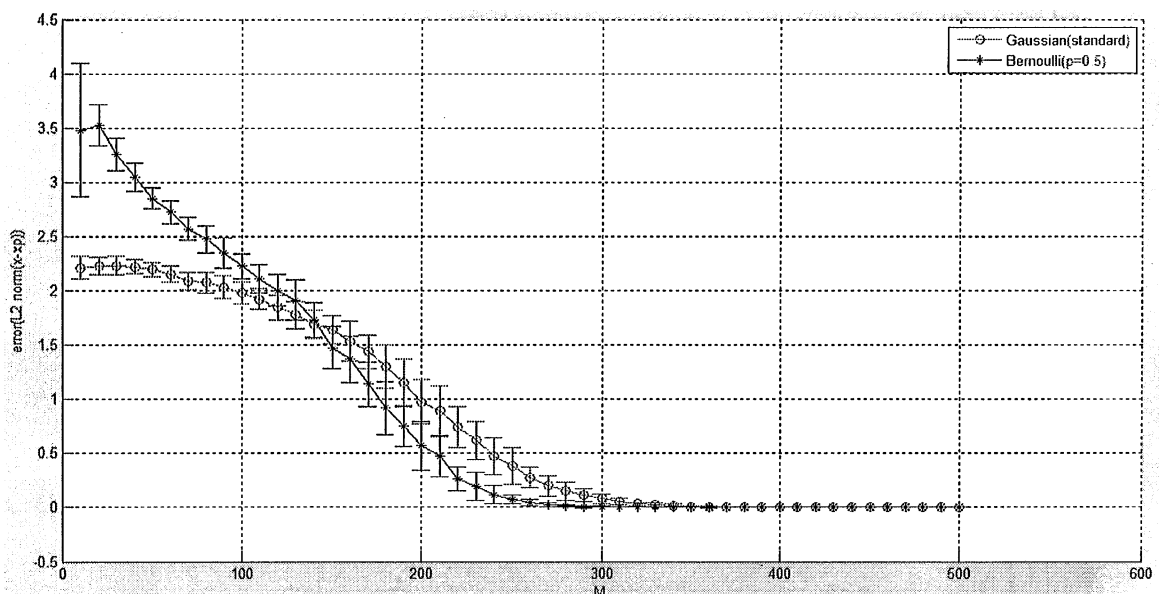
圖(2)



圖(3)



圖(4)



以上四圖模擬結果顯示兩種不同種類的訊號對於 Bernoulli matrix 與 Gaussian matrix 運作效能的影響，我們以還原訊號與原訊號的差距，作為比較效能之依據，差距越大表示效能越差：對第一種訊號(參見圖(1))而言，Gaussian matrix 的效能一直比 Bernoulli matrix 好(參見圖(2))；而對第二種訊號(參見圖(3))而言，Gaussian matrix 的效能一開始比 Bernoulli matrix 好，但隨著所得資訊量增加 (即圖中的 M 上昇)，Bernoulli matrix 的效能開始超越 Gaussian matrix(參見圖(4))。

學習經驗：從模擬成果中可發現，兩者間之效能差異會隨原訊號的特性不同，而有相當大的差別，目前推測原因為原訊號中 tail (非主要訊號部分) 的值的大小以及原訊號與使用之 Sensing matrix 是否為單號 (全為正或全為負)。

4. 觀摩學習：

在本次短期交流中，孔院士也指示我延長一周，由原訂 9/9 改至 9/16 返國，以期能觀摩哈佛大學開學後之上課環境，於 9/1~9/16 旁聽以下課程：

- a. Applied Mathematics 205 - Advanced Scientific Computing: Numerical Methods
- b. Computer Science 143 - Computer Networks
- c. Computer Science 121 - Introduction to Formal Systems and Computation
- d. Computer Science 182 - Intelligent Machines: Reasoning, Actions, and Plans
- e. Computer Science 205 - Computing Foundations for Computational Science

兩周時間的觀摩學習，讓我有以下的體驗與感受：

(a)上課互動良好：

許多同學上課直接提出問題與意見，我覺得這是比較好的學習方式，當場提問可以當場解決問題，以利學習效率，也可以當場確認自己的觀念是否正確，甚至許多時候是學生發現了教授所沒發現的問題，也是一個讓師生腦力激盪的好機會，能激發出更多點子。

(b)對於"作業"的態度

對於課程作業，教授鼓勵同學間討論，但強調必須自己完成，有一位教授甚至要學生把作業是跟誰合作，用了什麼樣的資源副在作業上，十分有趣。

(c)課程搭配專題：

整學期的課程除了授課，多會有加入與實際應用結合的實驗或專題，台灣雖然也有但是並不常見，我覺得將課堂所學與實際應用結合的作業或專題，能整合知識並發揮創意，更再次確認自己了解這堂課的知識到什麼程度，感覺整個課程就變得有趣許多。

(d)講課為輔，自學為重：

而且老師多是假設同學已預習上課的內容，上課多是複習基本的重要觀念，以及與學生腦力激盪，解決閱讀教課書後的問題與激發出新點子。

➤ 總結 - 一種良性的教學循環：

在課堂中，感覺不管是學生還是教授，真的有把"課程"認真地看成一回事，並盡其所能的發揮自己最大的努力與創意，把一堂課"上"好；到 Office Hour 問問題時，看老師仔細為我講述證明與定義的每一個環節，我覺得有一大部分的原因來自老師對於教課的責任心與認真的態度，而且從這點看來，也因為學生都經常使用 Office Hour 與 Section 時間問問題，老師也覺得開這些時間很有意義，所以才會教得如此認真。

（三）心得及建議

1. 申請簽證問題：

在此次短期交流中，我因申請觀光簽證時，AIT 針對是否提供觀光簽證而有內部討論，甚至也在進入美國海關時，遭詢問滯留長達四個小時，造成許多不便。此次短期交流，就性質方面，介於觀光與求學之間，建議未來舉辦類似短期交流計畫時，以申請留學簽證較為妥當。

2. 明確心態的建立：

此次短期交流與在學校上課不同，並非按表操課，建議未來學弟妹在參與交流時，能保持勇於嘗試與探索新事物的心態，除了在實驗室裡參與研究，也可利用時間旁聽學校課程，以及安排深度旅遊，藉此擴大視野。

3. 事前規劃：

此次短期交流除了近 40 天的實際參與，事前也需進行縝密的規畫，建議未來學弟妹在參與交流時，能建立事前規劃的作業習慣。

4. 背景知識重要：

實際參與短期交流前，所需培養的背景知識非常重要，像此次的研究主題，需運用到大量機率與線性代數的觀念，而 MATLAB 軟體更是在自學中才逐漸熟習運用的，建議未來舉辦類似短期交流計畫時，能先與孔院士確認研究主題，以提供申請同學參考，利於事前培養所需背景知識，若運用到尚未學習過的觀念與軟體，也期望學弟妹能主動以自學方式補齊。

5. 語文溝通能力：

除了學校的研究，在國外生活也須處理日常生活上的問題，語文溝通能力也因此的十分重要，未來獲遴選之學弟妹，能注重強化語文溝通能力。

四、附錄

- [1] Youngjune L. Gwon, H. T. Kung, and Dario Vlah, “DISTROY: Detecting Integrated Circuit Trojans with Compressive Measurements”
- [2] H. T. Kung, “Compressive Sensing: A Potentially Revolutionary Technology”
- [3] H. T. Kung, Tsung-Han Lin, Dario Vlah, “Identifying Bad Measurements in Compressive Sensing”
- [4] H. T. Kung, Chit-Kwan Lin and Dario Vlah, “CloudSense: Continuous Fine-Grain Cloud Monitoring With Compressive Sensing”
- [5] Hsieh-Chung Chen and H. T. Kung , “Separation-based Joint Decoding in Compressive Sensing”
- [6] Hsieh-Chung Chen, H. T. Kung, Dario Vlah, Bruce Suter, “Measurement Combining and Progressive Reconstruction in Compressive Sensing”
- [7] Hsieh-Chung Chen, H. T. Kung, Dario Vlah, Daniel Hague, Michael Muccio and Brendon Poland, “Collaborative Compressive Spectrum Sensing in a UAV Environment”
- [8] H.T. Kung and Stephen J. Tarsa, “Partitioned Compressive Sensing with Neighbor-Weighted Decoding”
- [9] Romana Fernandes, Ranga Vemuri, “Accurate Estimation of Vector Dependent Leakage Power in the Presence of Process Variations”