# 出國報告（出國類別：進修）

# 維吉尼亞理工學院暨州立大學
# 碩士進修報告

服務機關：國防大學理工學院
姓名職稱：邱廷鴻上尉
派赴國家：美國
出國期間：**111** 年 **8** 月 **16** 日至 **113** 年 **5** 月 **10** 日
報告日期：**113** 年 **6** 月 **3** 日

# 摘要

於 111 年 8 月 16 日，我受派前往維吉尼亞理工學院暨州立大學電機資訊工程系攻讀碩士學位（Master of Science, Electrical and Computer Engineering）。此次進修的目的是為國防大學理工學院資訊及工程學系培養未來的師資。於 113 年 5 月 8 日完成學業，並於 5 月 10 日返國，5 月 13 日回院報到。在美國維吉尼亞州進修期間，除了專研課業相關知識及技術並拓展視野外，我也利用了課餘時間與各國的同學交流，不僅吸收各國文化，也了解了不同國情下，思維邏輯的差異，期許自己能在未來將這段時間所獲得的知識及世界觀運用在教學方面。

本報告根據「行政院及所屬各機關出國報告宗和處理要點」相關規定撰寫，旨在分享個人進修經驗與見聞，不僅有助於大眾查閱，亦能提供國內大專院校相關行政及教學人員參考。報告內容均屬公開性質，未涉及機敏資料，主要記錄在美進修期間的研究與學習心得。報告分為目的、過程、心得與建議、參考資料等部分，內容包括進修學校及系所介紹、修課及評分制度、個人實驗專案計畫以及心得與建議。

# 目次

# 壹、目的

本次進修奉國防部 111 年 7 月 18 日國人培育字第 1110178581 號令核定，於 111 年 8 月 16 日，我受派前往美國維吉尼亞理工學院暨州立大學電機資訊工程系攻讀碩士學位（Master of Science, Electrical and Computer Engineering）。此次進修的目的是為國防大學理工學院資訊及工程學系培養未來的師資。於 113 年 5 月 8 日完成學業，並於 5 月 10 日返國，5 月 13 日回院報到。在美國維吉尼亞州進修期間，除了專研課業相關知識及技術並拓展視野外，我也利用了課餘時間與各國的同學交流，不僅吸收各國文化，也了解了不同國情下，思維邏輯的差異，期許自己能在未來將這段時間所獲得的知識及世界觀運用在教學方面。

本報告根據「行政院及所屬各機關出國報告宗和處理要點」相關規定撰寫，旨在分享個人進修經驗與見聞，不僅有助於大眾查閱，亦能提供國內大專院校相關行政及教學人員參考。報告內容均屬公開性質，未涉及機敏資料，主要記錄在美進修期間的研究與學習心得。報告分為目的、過程、心得與建議、參考資料等部分，內容包括進修學校及系所介紹、修課及評分制度、個人實驗專案計畫以及心得與建議。貳、過程

## 一、維吉尼亞理工學院暨州立大學介紹

維吉尼亞理工學院暨州立大學（Virginia Polytechnic Institute and State University，簡稱 Virginia Tech 或 VT）位於美國維吉尼亞州黑堡市(blacksburg)，是一所公立研究型大學。其歷史可追溯至 1872 年由維吉尼亞聯邦創立的維吉尼亞農工學院（Virginia Agricultural and Mechanical College），該學院當時是一所軍校。後續，在第七任校長任內將學制改成傳統的四年制學院，且更名為「維吉尼亞農工學院暨理工學院（Virginia Agricultural and Mechanical College and Polytechnic Institute），並於 1944 年縮減為「維吉尼亞理工學院（Virginia Polytechnic Institute, VPI）」，最後於第十三任校長任內正名為「維吉尼亞理工學院暨州立大學（Virginia Polytechnic Institute and State University, VPISU）」，但由於學校內運動盛行，在 20 世紀時接受「維吉尼亞理工（Virginia Tech, VT）」。

維吉尼亞理工大學於 1903 年成立了維吉尼亞理工大學工程學院（Virginia Tech College of Engineering）第一個行政部門身為一間理工大學

工程學院是其中重要的學院之一，其包含了眾多的工程領域，主要科系包括：

1. 航空航太與海洋工程（Aerospace and Ocean Engineering
2. 生物系統工程 Biological Systems Engineering
3. 生物醫學工程與力學 Biomedical Engineering and Mechanics
4. 化學工程 Chemical Engineering
5. 土木與環境工程 Civil and Environmental Engineering
6. 電腦科學 Computer Science
7. 電機資訊工程 Electrical and Computer Engineering
8. 工程教育 Engineering Education
9. 工業與系統工程 Industrial and Systems Engineering
10. 材料科學與工程 Materials Science and Engineering
11. 機械工業 Mechanical Engineering
12. 採礦與礦物工程 Mining and Minerals Engineering
13. 建築學院 Myers-Lawson School of Construction
14. 生物醫學工程與科學 School of Biomedical Engineering & Sciences

這些學系共同構成了維吉尼亞理工大學工程學院的教學和研究核心，提供了廣泛的大學和研究生課程，旨在培養工程領域的未來領袖和創新者。

## 二、電機資訊工程學系（Electrical and Computer Engineering）

電機資訊工程學系（Electrical and Computer Engineering，簡稱 ECE）是維吉尼亞理工大學工程學院中的一個核心學系，為全美國第四大 ECE 學系在控制系統、通訊、電子、電力、計算機等多個領域提供教育及研究機會。該學系學生可選擇針對電機方面（Electrical Engineering，簡稱 EE）選擇課程，包含自動控制、通訊、半導體等，也可以選擇計算機方面（Computer Engineering，簡稱 CPE）的課程，包含硬體設計、編譯器設計、網路安全、密碼學等。

碩士課程介紹

維吉尼亞理工大學的電機資訊工程學系提供全面的碩士課程，旨在培養高級專業人才，並提供相關的業界資源及技術，可讓學生畢業後順利的與社會接軌。維吉尼亞理工大學的電機資訊工程學系每年都有來自美國國家科

學基金會、美國國立衛生研究院、美國國家航空暨太空總署以及波音等公司的資金，提供學校師生研究使用。碩士課程的設計強調理論與實踐的結合，為學生提供深入的專業知識和實際操作經驗。以下是電機資訊工程學系碩士課程的主要內容及特點：

課程分類

電機資訊工程學系中，資訊課程分成四大類別，學校要求學生須於這四大類別中選修至少兩種不同類別的課程，以培養學生多元發展：

1. 計算機系統（Computer Systems）：深入研究計算機系統的結構和設計原理，包含系統安全、記憶體、平行運算、編譯器系統等。
2. 網路（Networking）：研究網路設計與應用，包括網路安全、網路設計及封包格式與內容。
3. 軟體及機器學習（Software & Machine Intelligence）：探討軟體及機器學習的設計與應用，包含軟體安全、軟體設計、機器學習及深度學習的應用。
4. 超大型積體電路及自動化設計（VLSI & Design Automation）：涵蓋半導體設計、自動控制的應用。

實驗室與研究機會

維吉尼亞理工大學電機資訊工程學系提供多樣且特殊的實驗室和研究機會，讓學生能夠參與到前沿科技的研究中。主要研究領域包括：

1. 電腦系統
2. 無線通訊、網路及網路安全
3. 能源與電力系統：探索機器學習算法、深度學習模型及其應用。
4. 積體電路與系統
5. 機器學習及數據科學
6. 電磁與光電學
7. 電力電子
8. 微電子與量子工程
9. 系統軟體
10. 太空技術與工程

學生可以通過參與這些研究項目，獲得寶貴的實踐經驗，並有機會在國際會議和期刊上發表研究成果。

## 三、評分制度

學期成績評定依課程分為兩種評分方式，一種為標準使用 GPA 4.0 制，區分 5 個等第(A：4；B：3；C：2.0； D：1.0 ；F：0.0)，另一種為 P/F 制，即為通過(Pass)/不通過(Fail)。工程學院學生畢業總成績須達 GPA 3.0 以上，並修畢至少 30 學分（含一般課程 18 學分、研討會 3 學分及論文 9 學分，且除畢業學期外，其餘學期需修習必、選修或論文至少達 9 學分）。

## 四、研究成果

我這次論文的題目為:針對 RSA 及 CSIDH 故障注入攻擊。

故障注入攻擊是一種主動式且強大的攻擊手法。攻擊者會利用各式各樣的方式，例如：加熱、電磁脈衝、電壓干擾、雷射光等，造成設備出現短暫的故障，進而產生錯誤的結果。攻擊者可以透過分析所獲得的錯誤結果推導出密碼金鑰，以破解加密內容，並奪取機密資料。

先前有關故障注入攻擊的研究顯示出，該攻擊不但容易，且傷害性極高（攻擊者可以透過少量的攻擊次數就能分析出密碼金鑰），因此我們必須防範相關的攻擊。另外，密碼學遍佈在我們生活中，在現今的社會，許多機密資料都必須依賴密碼學保護，所以密碼學對於資訊安全來說是相當重要的一個領域。如果攻擊者可以透過故障注入攻擊輕鬆的破解密碼，對於使用者來說無疑是一件非常危險的事情。

在論文中，我針對常用的密碼學 RSA 以及現今最常使用的後量子密碼 CSIDH 做故障注入攻擊。我參考了先前針對 RSA 及 CSIDH 故障注入攻擊的論文，將其實作在 Pinata 電路板上。由於先前相關的論文僅止於理論，並且在論文中，作者皆假設攻擊者在執行故障注入時，可以百分之百造成設備產生故障，然而在我的實作過程中發現，實際上當執行故障注入時，環境因素嚴重影響其成功率，在比較過後發現實際上故障注入的成功率低於百分之三十，而破解 CSIDH 的成功率也不高。在論文中，我也實現了先前論文提及的 CSIDH 防禦方式，並測試及比較該防禦方式是否確實有其功能。

# 參、心得及建議

自 111 年 8 月至美國進修，直到 113 年 5 月返國，在疫情趨緩的情形下出國，這是我第一次出國留學。以下區分求學、生活以及心態等三方面論述：

(一)　求學方面

大學畢業之後一直都在理工學院裡面任職，其中包含了排長、副連長等職務，較不需要使用到大學所學專業知識。一直到出國前接任資安中心教育行政官一職後，所經手的行政事務才與資訊有關。剛到美國的第一個學期，所修的課程跟大學時期學的內容有所不同，甚至是完全沒學過的課程，再加上來自不同地方的教授口音都不同，所以第一個學期花了很長一段時間在尋找讀書的方法。再加上跟大學時期不同的是，雖然學分數沒有像大學一樣多，但是每一堂課的課後作業以及實作報告卻是跟大學相差甚遠。每天除了上課之外，剩下的時間就是在寫作業。教授課堂上教的內容只是讓學生們了解準備方向為何，主要還是學生自己要花時間去讀教科書以及尋找課外補充內容。但是第一個學期後半段我就有掌握到讀書的方法，後續壓力就相對小了許多。

(二)　生活方面

維吉尼亞理工大學是在維吉尼亞州黑堡市內，而黑堡市是鄉下地區，生活極度的不方便，不管是採買方面，或是旅遊方面，都需要花很多時間才能到達目的地，例如採買，從租屋處到超市需要搭公車大約 30 到 50 分鐘才能到達，中間還需要轉車。如果要到機場或是火車站都需要搭 1 個多小時的客運才能抵達。

美國各方面的消費都比台灣還要昂貴，例如在鄉下租屋費一個月大約要 800~900 美金，如果到大城市甚至可以到 1000 美金以上。另外，伙食費的部分，在外面吃一餐最便宜的大約 25 美金以上，所以在國外的這段時間我大多都是自己買時才回來料理。

(三)　心態方面

這是我第一次出國這麼長一段時間沒有回家，一開始有些不習慣跟擔心，但大約 1~2 個月之後就適應了在那邊的生活。現在的科技很發達，每個禮拜都可以跟父母親視訊，除了讓他們放心

之外，也可以讓我抒發在外的心情。另外一方面，我也很高興能夠有這個機會到國外念書，除了能夠了解國外文化與台灣文化的差異外，也能夠跟不同國家的學生交流，增進自己的視野。大學時期由於是讀軍校，難免會跟外界社會脫節，趁著這段時間學習到不少美國教育值得學習的方面，希望能夠利用這段時間所得到的經驗，在未來不論是工作上或是教學上帶來一些新的刺激與衝擊，讓學校的教育方面有所成長。

# 肆、參考資料

[1].https://en.wikipedia.org/wiki/Virginia_Tech

[2].https://www.vt.edu/