出國報告（出國類別：學術交流）

參訪廣西大學計算機與電子信息學院

服務機關：國立高雄應用科技大學 資訊工程系
姓名職稱：蕭淳元 助理教授
派赴國家：中國大陸
出國期間：101/08/13 至 101/08/24
報告日期：102/01/17

摘要

本報告是記錄 101 年 8 月參訪廣西大學計算機與電子信息學院的過程。廣西大學位於號稱綠城的廣西省南寧市，擁有寬廣美麗的校園。這次訪問由計算機與電子信息學院副院長覃團發教授邀請，並由該院張學軍教授陪同，訪問的主要目的有兩個：一是與對方的教授與研究人員進行學術討論，以便將來合作發表論文，初步認為可以合作的議題有「雲端架構下的混淆與認證」、「醫院病歷資料的安全傳輸通訊協定」與「視覺密碼學在醫學影像上的應用之探討」等三大方向。訪問的另一個目的是參觀對方的研究設備，特別是雲端伺服器以及圖形運算伺服器，以了解將來合作時，對方能提供哪些軟硬體的支援。

目　　次

壹、目的

隨著兩岸往來日益密切，除了經貿與文化的交流外，學術上的交流更能發揮兩岸往正面發展的積極作用，特別是兩岸合辦的學術研討會以及合作發表的論文。本人擔任中華民國資訊安全學會教育與推廣委員會委員，將協助在臺灣舉辦的 2013 年第二屆海峽兩岸資訊安全研討會 (2012 第一屆在大陸杭州舉辦)。正好於民國 101 年 5 月份收到廣西大學計算機與電子信息學院副院長覃團發教授的邀請，於同年 8 月前往該院參訪，目的是希望促進兩岸學術交流，於上述研討會以及往後的國際期刊合作發表論文。

這次訪問的為期兩週(101/08/13 至 101/08/24)，有兩個主要任務：一是與對方的教授與研究人員進行學術討論，以便將來合作發表論文，初步認為可以合作的議題有「雲端架構下的混淆與認證」、「醫院病歷資料的安全傳輸通訊協定」與「視覺密碼學在醫學影像上的應用之探討」等三大方向。訪問的另一個任務是參觀對方的研究設備，特別是雲端伺服器以及圖形運算伺服器，以了解將來合作時，對方能提供哪些軟硬體的支援。

貳、過程

這次參訪主要由張學軍教授陪同，分為以下兩大部分：

甲、 學術交流

張教授的專長為醫學影像處理，特別是肝臟的超音波影像分析，由於醫學影像牽涉到病人的隱私，光靠醫療從業人員的自我要求有時候是不夠的，因此這些電子病歷的安全儲存與傳輸機制是非常重要的。而本人的專長為密碼學，正在進行關於視覺密碼學的研究:視覺密碼學有別於傳統的密碼學在於解密的過程只需仰賴人類的雙眼，而不需要經過電腦運算，這種技術對於醫學影像的安全性至今未曾有學者探討，主要原因有可能是因為視覺密碼學的圖像解析度欠佳，但是超音波影像的解析度本來就不高(相較於一般相機拍攝的圖像)，因此兩人經過三個下午的討論後敲定的第一個主題就是「視覺密碼學在醫學影像上的應用之探討」，這可以說是一個全新的跨領域組合。

接下來幾個下午的討論，選定第二個主題是「醫院病歷資料的安全傳輸通訊協定」，這個主題是應用傳統的密碼學技術，對醫院與醫院間或醫院與學校間的電子病歷傳輸做加密的動作，這個主題還牽涉到資料庫的專業，很可惜的是這次訪問，這方面專長的博士後研究員黃保華正好不在廣西大學。由張教授得知黃博士的簡歷如下：

「2007 年於華中科技大學獲電腦軟體與理論專業博士學位，2009 年 6 月前在華中科技大學基礎醫學博士後流動站做博士後。長期從事資訊安全方面的研究，在資料庫安全增強方面做了大量工作，成功研發了中國大陸首個通用資料庫加密系統。主持中國大陸國家自然科學基金、中國博士後科學基金專案各 1 項，主持完

成了多個應用於要害部門、關鍵單位、重大工程的資訊系統及其安全工程項目。獲中國大陸國家密碼科技進步二等獎 1 項（第一完成人）、湖北省技術發明二等獎 1 項、廣西科技進步二等獎 1 項；獲國家發明專利授權 2 項（其中 1 項為第一發明人）；在國內外期刊和會議上發表論文 20 餘篇。目前研究興趣主要包括資料庫安全增強理論、智慧移動設備安全、大規模系統聯合免疫、虛擬免疫系統等新興領域。」

希望將來有機會能與黃博士合作與討論。

最後一個主題是本人還在構想中的想法，也就是「雲端架構下的混淆與認證 (obfuscation and verifiability in cloud computing)」。這個議題是從理論出發，探討雲端架構中兩個重要的安全性議題。未來將由新聘的研究員黃汝維博士與我進行這個議題的合作，若能提出合理的數學模型，將可應用在對方近期添購的大型雲端伺服器上。這方面由於對方的人員與設備還未準備完全，因此只能說有初步的共識而已，還未有實質的討論。

乙、 參觀設備

本章節主要介紹廣西大學計算機與電子信息學院的軟硬體設備：占地面積 1000 多平方公尺，實驗室現在擁有曙光 5000A，W5801，A620r-G 等伺服器；Sun E450、E250 超小型電腦、HP 和 IBM p 系列 610 6C1 型高檔伺服器、Sun Ultra60 和 20 圖形工作站、Cisco 高端交換機和路由器、Agilent 頻譜分析儀、Agilent 信號發生器、Agilent33250A 函數/任意波形發生器、HP 8903B 音訊信號分析儀、HP 繪圖器、數位示波器、各類高檔微機、印表機等儀器設備 300 多套。

其中與本人研究(見前段 甲、學術交流)相關的設備有佈局在網路大樓一樓的曙光 5000A 伺服器，曙光天闊 W5801 伺服器，曙光天闊 A620r-G 伺服器的資料，Intel 超毅 4805HS 伺服器。在此附上各伺服器的簡介，詳細資料請參考附件。

i. 「曙光 5000A 簡介：中國魔方超級電腦是中國首台百萬億次超級電腦，產品序列名稱“曙光 5000A”。曙光 5000 採用新型“超並行”體系結構（Hyper Parallel Processing，簡稱 HPP），是中國自主智慧財產權產品，具有高性能、高效率、高密度、高性價比、低功耗以及廣泛適用等特點。曙光 5000 適用於各個領域的大規模科學工程計算、商務計算，還可以作為各種資料中心、雲計算中心的支撐平臺。」

ii. 「曙光天闊 W580I 工作站是曙光精心打造的一款性能卓越，穩定可靠，配置靈活的新一代雙路工作站產品。W580I 具有處理速度快、擴展性強、易管理和低噪音等特點。曙光天闊 W580I 採用 Intel 晶片組設計，使系統可以提供超強的專業顯卡的擴展能力；配合獨具特色的主機殼設計，不僅可以保證系統在高配置下的散熱和穩定行，同時也極大地降低了機器的噪

音，配合轉機架套件，W580I 還可以方便的轉化為 4U 機架式安裝。」

iii. 「曙光天闊 A620r-G 伺服器是曙光公司最新推出的一款支持 AMD 最新 Magny-Cours 處理器的部門級雙路伺服器。該機型最多可以支援記憶體容量 256GB，支援最多達 12 塊熱插拔 SAS/SATA 硬碟，如此強大的擴展性足以支撐關鍵任務的運行，滿足資源密集型應用的需要。先進的管理和存儲技術,具有更好的可擴充性和高可用性。作為曙光天闊系列雙路伺服器的高性價比產品，A620r-G 伺服器非常適用于金融、證券、交通、郵政、電信、能源等對伺服器性能、可擴展性及可靠性要求苛刻的行業資料中心和遠端的企業環境。」

iv. 「超毅 4805HS-Intel Xeon MP（SR4850HW4）－企業級伺服器：Intel 四路至強伺服器 SR4850HW4 採用最新的多路處理伺服器技術，專為需要部署關鍵企業應用系統的客戶而設計，為企業資料庫、CRM、ERP、電子商務、政府機關等關鍵應用提供超強動力。SR4850HW4 整合了目前最先進的電子及機械工程技術，提供比早期四路伺服器更高的性能、更高的可用性、更高的可擴展性、更高的可維護性。」

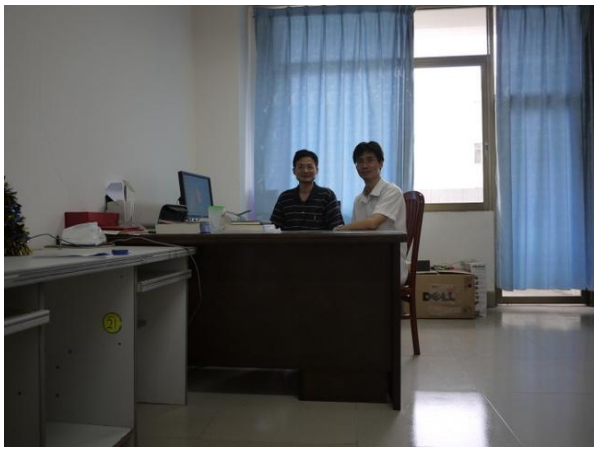
參、心得及建議

本次參訪最大的感想就是中國大陸在高端的硬體設備真的是突飛猛進,尤其是在看了他們的設備後，發現他們很多「國產」的高階伺服器，更覺得他們是由國家在支持，真的有心要跟美國一爭高下，成為世界第一。這點從他們老師與學生用的個人電腦、實驗室桌椅還相當簡陋來看，形成非常強烈的對比；臺灣民間或學術用的普通設備可能比對岸的豪華或是品質高，也就是一般大眾平均起來還是比對岸富有，但是由國家投入發展的尖端科技方面，我們正逐漸地落後，在一些重大工程與建設如高鐵、衛星或是潛艇甚至到武器，我們更可以說是遠遠地落後，真的是值得警惕的地方。個人認為我們應該要有至少一兩項的尖端科技由國家帶領來投入，在某些特定的領域成為世界第一，這樣整體才能保有競爭力。

肆、附錄

<table>
<tr>
<td> 

廣西大學計算機與電子信息學院門口</td>
<td> 

與張學軍教授於門口合照</td>
</tr>
<tr>
<td> 
於張學軍教授辦公室</td>
<td></td>
</tr>
</table>