本期焦點 | 所長的話 2| 名人榜 3| 計畫特寫 4| 卓越講座系列 6| 活動快訊 7| 實驗室報導 8|
計畫特寫 10| 人物焦點 12| 創意發想 14| 活動快訊 16

# iIS 資訊科學簡訊

# Update

Newsletter of the Institute of Information Science, Academia Sinica, Taiwan

2013

# 所長的話

資訊科學研究所於 1977 年開始設立籌備處，歷經五年籌備，於 1982 年 9 月正式成立研究所，是中央研究院數理組十個單位之一。本所的研究重點分為八大方向，包含生物資訊、電腦系統、資料處理與探勘、多媒體技術、語言與知識處理、網路系統與服務、程式語言與形式方法、計算理論與演算法。

本所並於 2003 年配合中研院國際研究生院 (TIGP)，開始招收生物資訊學程博士班，致力延攬及培訓此一新領域之國際人材，八年來已招募 39 名學生，對生物資訊的研究有很大的助益。

所內資深研究人員皆指導或共同指導來自全國各地頂尖大學之碩、博士生，並與這些大學保持緊密的研究關係及合作計劃，與國內外資訊業界亦有極為良好之互動關係。

所長：許聞廉

副所長：高明達
王新民

研究群主持人：
宋定懿教授
生物資訊實驗室
吳真貞教授
電腦系統實驗室
陳孟彰教授
資料處理與探勘實驗室
廖弘源教授
多媒體技術實驗室
許聞廉教授
語言與知識處理實驗室
何建明教授
網路系統與服務實驗室
王柏堯教授
程式語言與形式方法實驗室
徐讚昇教授
計算理論與演算法實驗室

資訊所成立以來，已邁入第二十九年，各種研究發展蒸蒸日上，在國內外屢創佳績，包含了 ACM 最佳論文獎、李國鼎青年研究獎、國科會傑出研究獎、中國電機工程學會優秀青年電機工程師獎、潘文淵文教基金會研究傑出獎、資訊學會資訊榮譽獎章、Linux 黃金企鵝人才貢獻獎，希望對國內外資訊科學研究有所貢獻。值此研究提昇之際，承蒙院長指派重任，能在這資訊研究的時代巨輪中，貢獻棉薄之力，也期望資訊所在台灣軟體科技扮演不可或缺的重責大任。

因此，所刊特別介紹了 MIFARE Classic 智慧卡技術。悠游卡的安全性值得我們詳加檢視，以技術的角度，一一剖析它的設計缺陷，以及實作上的錯誤，同時更要督促有關當局加強檢測這類卡片的安全性，使得以其進行身分確認與小額付費能夠更為安全普及，造福社會大眾。

其次，在網路系統與服務上，我們介紹創新網路、系統和服務，改善無線和耐延遲網路協定；結合社會大眾的計算能力，探討學術研究上的關鍵挑戰；發展災害管理的資通訊技術；和探討提供大規模金融風險管理服務相關的網路計算問題等等，希望讓世界更美好。

另外，就是談談有關人機介面的研究。機器人已在軍事、工業、醫療等專業領域擁有極高的應用，發展機器人相關的系統設計、感測、規畫、控制的基礎理論和整合技術、情感與認知計算，讓人能安全舒適的與機器人進行必要的互動，使機器人能廣泛走入民生用品領域，在食、衣、住、行、育、樂等生活層面上，扮演著積極而不可或缺的任務和角色。

冬天的腳步近了，綿綿細雨中，資訊所籠罩著濃濃的寒意，而本刊秋冬版相信是資訊人交流的園地，資訊所也希望能為社會盡一份微薄的力量，歡迎大家能多多投稿，提供建言，分享您的近況。

# 名人榜

特聘研究員許聞廉兼任本所所長，聘期自 101 年 6 月 18 日起。

穆信成升等為本所副研究員，自 101 年 09 月 14 日生效。

合聘助研究員鍾偉和榮獲 IEEE 通訊學會 2012 WCNC 最佳論文獎。

王柏堯升等為本所研究員，自 101 年 9 月 14 日生效。

楊得年升等為本所副研究員，自 101 年 09 月 14 日生效。

助研究員林靖茹榮獲潘文淵文教基金會 2012 考察研究獎。

特聘研究員廖弘源獲選為 IEEE Fellow。

研究員王新民、合聘助研究員楊奕軒及林彥宇、研究助理王如江及卓奕宏榮獲 ACM Multimedia 2012 Grand Challenge First Prize。

特聘研究員廖弘源與台大徐宏民教授共同指導的學生陳殷盈獲得 ACM Multimedia 2012 Doctoral Symposium Best Paper Award 。

新任助研究員古倫維於 2012 年 8 月 1 日起加入本所研究團隊。

## 卓越講座系列

September **Kenneth Church** Researcher, IBM
Human Language, Data Mining, OCR

October **Ching Y. Suen** Director, CENPARMI at Concordia University in Canada
Computational Linguistics, Computer Analysis and Recognition of Documents

December **Erik Demaine** Professor, Computer Science, Massachusetts Institute of Technology
Theory, Algorithms, Geometric Folding

# 非接觸式智慧卡技術
# 密碼系統需更為安全防密

楊柏因 研究員

MIFARE Classic 是恩智浦半導體(NXP Semiconductors) 所擁有的一種非接觸式智慧卡技術。根據恩智浦半導體的數據，MIFARE Classic 智慧卡晶片在全球的銷售量已經超過了十億，而其讀卡機模組的銷售，也以百萬計算，可說是目前全球市場佔有率最高的非接觸式智慧卡技術。MIFARE Classic 廣泛應用在全球各大城市的公共交通票證系統，包括美國、加拿大、中國、印度、南韓、土耳其、英國、德國、荷蘭、愛爾蘭、瑞典、丹麥、巴西、阿根廷、澳洲等國家，都有使用 MIFARE Classic 的城市公共交通票證系統。台北市的悠游卡所使用的技術，也是 MIFARE Classic。

MIFARE Classic 卡片靠上面的線圈從快速變換的電場經由電磁感應取得少許能量而運作，除了極少的控制線路之外，它基本上是一個記憶卡，它的記憶體被劃分成若干個 sector，每一個 sector 又被劃分成 4 個 block。在 MIFARE Classic 中的一個 block 是 16 bytes。MIFARE Classic 使用專有的 CRYPTO1 密碼系統提供安全存取控制，讀卡機在存取每一個 sector 之前，必須先和卡片進行認證，確保雙方都有共同的密鑰，卡片才會允許讀卡機對其操作。

恩智浦半導體將 CRYPTO1 密碼演算法列為商業機密，試圖保障 MIFARE Classic 的安全性，在今天資訊暢通的時代，自始就注定失敗。早在 2004 年左右，就有傳言指出上海復旦微電子公司已經能夠製造出和恩智浦半導體官方讀卡機相容的卡片，表示 CRYPTO1 的秘密已經開始流出。2006 年開始有謠言說 CRYPTO1 已經被逆向工程所破解，這個謠言在 2007 年底的 Chaos Communication Congress 上面被兩位德裔的工程師 Nohl 和 Pl\”otz 所證實，他們隨後並且把結果發表在 2008 年的 USENIXSecurity Symposium 上面。2008 年另一組在荷蘭 Radboud University Nijmegen 的團隊隨即也試圖發表他們對 MIFARE Classic 的攻擊。恩智浦半導體試圖在荷蘭的法庭上阻止這件事的公開，但是案件隨即被法官以言論自由不可侵犯為由，直接扔出了法庭。

平心而論，MIFARE Classic 是相當成功的一項產品，它的造價低廉，性能穩定，因此能夠在短短的十年內，攻陷許多公共交通票證系統的市場。可惜它在密碼系統的設計和實作上，犯了許多致命的錯誤，以至於作為一個票證系統或是小額付款系統，它連最基本的安全性都無法提供。以下我們就以技術的角度，一一剖析它的設計缺陷，以及實作上的錯誤，說明它為什麼無法提供足夠的安全性。

MIFARE Classic 讀卡機和卡片之間的通信，包括三個階段：防碰撞，認證，和儲存指令。防碰撞遵循 ISO-14443 標準，代表一個 session 的開始，此後讀卡機可以啟動認證機制。驗證成功後，所有後續通信，包括同一 session 內的儲存操作，與對其它 sector 的認證，都使用剛建立起的 session 密鑰加密。

如上所述，MIFARE Classic 使用的稱為 CRYPTO1 的串流式密碼系統。所謂串流式密碼系統，簡單來說就是由秘鑰產生一連串看似隨機的位元，將之和所要加密的明文 XOR 起來。它的安全性在於，如果攻擊者不知道這些隨機位元，那他也無法預測明文，這是 Shannon 所證明安全的 one-time pad 密碼系統的原理。不過，這一類的密碼系統要達到足夠的安全性，必須能夠強力保證，攻擊者必須取得非常多的隨機位元，並且擁有非常強大的計算能力，才能反推出密鑰。這是由於攻擊者往往有許多機會，能夠猜到某些明文的內容，因而能夠獲得對應的隨機位元，藉此反推出密鑰，一般稱為已知明文攻擊。例如，卡片如果經常會以加密的狀態回傳某個控制字元就會

洩露這樣的資訊。

很不幸的，Mifare Classic 的設計過程裡，犯下了相當多的錯誤，我們簡述如下：

CRYPTO1 密碼系統，所使用的金鑰長度太短，只有 48 個位元，以現在電腦的計算能力，可以輕易地以暴力法搜尋，找出對應的密鑰。NXP 的設計失誤另外還有幾個，但這無疑是 MIFARE Classic 最大的失誤。假設可以從側面讀到一筆認證過程，或是使用市面上可以簡單購買到的無線電器材，再利用合理的計算資源就可以破解 － 筆者的研究群利用 16 個市售兩個世代前的 NVIDIA GPU，就能夠輕易地在 14 個小時內，成功地破解出密鑰。這樣的攻擊對剛剛發行的二代悠游卡也適用。

通訊協定中使用奇偶性偵錯碼 (parity check)，但是卻是先算出偵錯碼再加密。更糟糕的，這個偵錯碼的加密與下一個被傳送的位元組的第一個位元使用在密碼串流中相同的位元來加密。在理論上這不好，實際上這也給了攻擊者 1/8 左右的額外資訊。

在常見的第一版 Mifare Classic 卡，生成認證中所需要的一次性隨機數 (random nonce) 的亂數產生器僅有 216 種輸出可能性，而且攻擊者在某種程度內可藉由準確控制　動認證過程的時刻而讓這個這個隨機數重複出現。這大大減小了某些暴力攻擊的過程。

理論上只要認證過程未完成，卡片應該都給出相同回應，以避免洩露額外的資料。很不幸的 Mifare Classic 的原版卻沒有做到這點，所以攻擊者有更多側向管道 (Side Channel) 來獲得所需的資料。

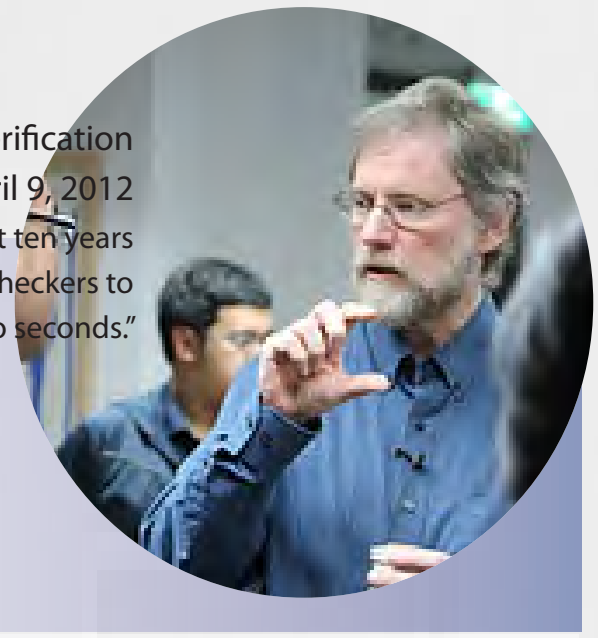
我們面對這末多漏洞，唯一可以感到差可告慰的就是這些攻擊並沒有任何一個會洩露廠商的主金鑰。但是攻擊者只要能側錄卡與讀卡機的交談過程，就能很簡單的經破解 CRYPTO1 密碼系統而獲得並修改所有卡上的能修改的資料，這對使用者來說。就像是 Mifare Classic 卡片如一個掛在公開網路的 USB 碟一樣不設防。雖然剛剛發行不久的二代卡 － Mifare Classic Plus － 修補了後三個缺點，但是金鑰太短的問題沒有解決，而為了相容性起見，大部份的通訊協定不能隨便修改。因此如上所述，蠻力攻擊對剛剛發行的二代悠游卡也適用。

助理在搬破密用的顯示卡。

## 小結

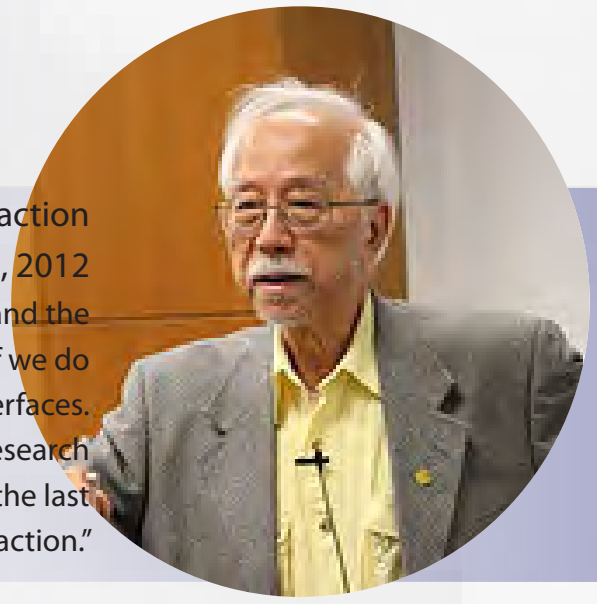
利用悠游卡小額付費的確為現代人忙碌的生活帶來了許多便利，但是作為支付的工具，悠游卡的安全性值得我們詳加檢視。固然悠游卡只是整個小額付費系統的終端，但是如果悠游卡的安全性非常低，使得篡改或複製是非常容易而且低成本，那麼這無意使得使用這項支付工具的成本大為上升。特別是在不改變已發行卡片的限制下，要維持這樣的卡片的使用，使用者或多或少的都會喪失一部份隱私權。我們呼籲大家一起來監督悠游卡業者，以免他們將成本盡數轉嫁於整個社會，同時更要督促他們加強檢測這類卡片的安全性，使得以這樣的卡片進行的身分確認與小額付費能夠更為安全普及，造福社會大眾。

# 卓越講座系列



New Frontiers in Formal Software Verification
Gerald J. Holzmann — April 9, 2012
"Much progress has been made in the last ten years to reduce the time required by model checkers to perform correctness checks from hours to seconds."

Technical Computing: Past, Present, Future
Dan Reed — May 7th, 2012
"This talk will examine the scientific, technical, and social issues around high-performance computing, computational science, research empowerment, and new scientific domains."



Human Computer Intelligent Interaction
Thomas S. Huang — July 3, 2012
"The tremendous computing speed and the enormous storage capacity come to naught if we do not have intelligent human–computer interfaces. In this talk, I shall describe some of the research my students and I have been doing during the last decade on Human–Computer Interaction."

Towards Google-like Search on Spoken Documents with Zero Resources
Kenneth Church — September 17th, 2012
"Many of these systems, especially ASR [automatic speech recognition], are often based on large (expensive) linguistic resources. When we have resources, we should use them. But when we don't, we can still do much of what you can do with bags of words (BOWs), even when many/most/all terms are out-of-vocabulary (OOV)."

Model Checking Cell Biology
David Dill — August 7, 2012
"Perhaps techniques from formal verification could lead to insights about the systems principles that allow biological systems using very low energy (and high noise) components to function dynamic environments. I will explore some past and future research directions in this area, as well as some of the non-computational challenges that arise in this kind of research."

2012-08-27 (Mon) – 2012-09-07 (Fri)

## 2012 Formosan Summer School on Logic, Language, and Computation (FLOLAC '12)

Researchers in Taiwan who are interested in the foundational aspects of computing science have founded a number of research teams and worked together in some joint projects. As in any discipline, a student will have to go through a series of courses to be prepared for further research in this field. Being affiliated to different institutes, however, the researchers often find it difficult to lecture all these courses alone. It is thus desirable to bring together those who share a common interest and give lectures together.
The aim of this summer school is to give a collection of courses that would prepare the students with enough knowledge to carry on research in foundational computing science. The courses on the even years cover advanced topics in programming languages, those on the odd years on model checking and program verification. The theme of this year is "Advanced Programming Languages and Type Systems".
FLOLAC was held in 2007, 2008, 2009, 2010, and 2011.
The summer school consists of 54 hours of lectures and lab/tutor sessions. In addition, there is a 3-hour exam and a 3-hour research seminar. Students who passed the exam will be awarded 3 credits from National Taiwan University.

further information: http://flolac.iis.sinica.edu.tw/flolac12/doku.php?id=en:start

CODATA 23
Taipei 2012

## Open Data and Information for a Changing Planet

2012-10-28 (Sun) – 2012-10-31 (Wed)

Plenary Room in the Humanities building, Academia Sinica

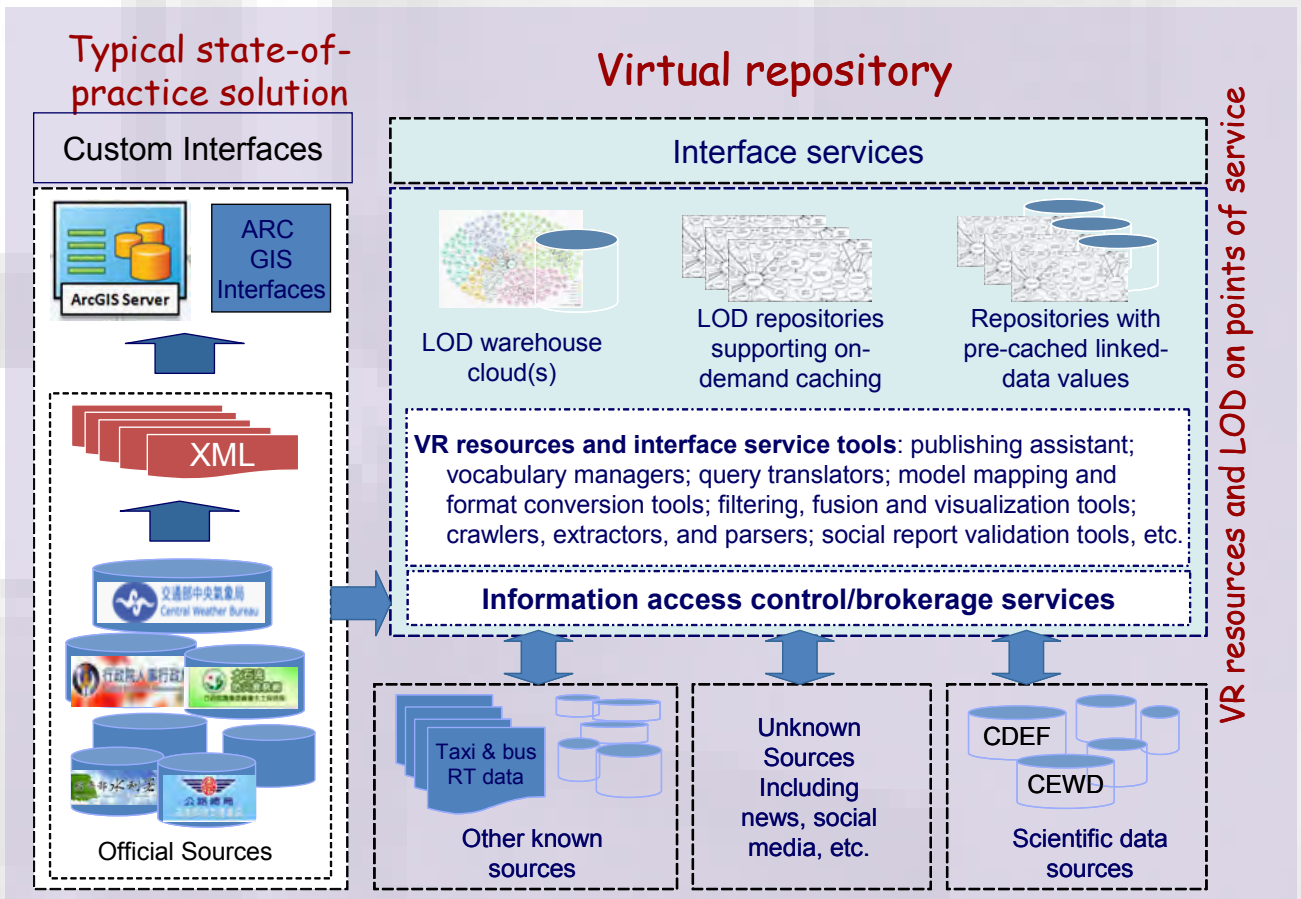
The theme "Open Data and Information for a Changing Planet" encompasses some relevant issues in data-intensive scientific fields. Nurturing an open environment for data and information is crucial for disseminating research results to a wide audience and allowing thorough, collaborative analysis. Also, the theme distinguishes between data and information and by so doing highlights the role data-intensive science plays in transforming raw observations into applicable, intelligible results and discoveries.

## 2012 學術咨詢委員會

年度學術咨詢會於 5 月 16 日開辦為期兩日，圓滿達成任務。此次與會委員，皆為國際學術領域具領導地位之彥碩，會中咨詢委員提出相關建言，對提昇本所之研究，具長足之助益，並在學術研究方向具有決定性的影響力。

# 創新網路、系統和服務，讓世界更美好
## 網路系統與服務實驗室

何建明
陳伶志
陳孟彰
陳昇瑋
陳文村
莊庭瑞
張韻詩




Open ISDM: 開放式災害管理資訊架構。

網路系統與服務實驗室主要研究的方向，包括改善無線和耐延遲網路協定；結合人類計算能力，探討學術研究上的關鍵挑戰；發展災害管理的關鍵資通訊技術；和探討提供大規模金融風險管理服務相關的網路計算問題等。

我們針對網路感測系統中之節能議題與感測資料管理議題進行研究。研發可調變式 GPS 接收器的排程演算法，用於延長行動位置感測之系統的運作時間；研發感知式排程演算法，利用低成本的額外感測器建構環境感知，並據以動態調整高耗能之 GPS 接收器與無線網路的使用；同時提出一種輕量級且零失真的時空資料壓縮方法。設計一系列資料查詢演算法，讓時空感測資料能夠在未經解壓縮的狀況下，直接支援各種時空資料運算。研究成果包含支援玉山國家公園旅客遊憩、追蹤與搜救的任務型感測系統；以及使用智慧型手機，針對大台北地區大眾運輸工具的乘車舒適度感測系統。

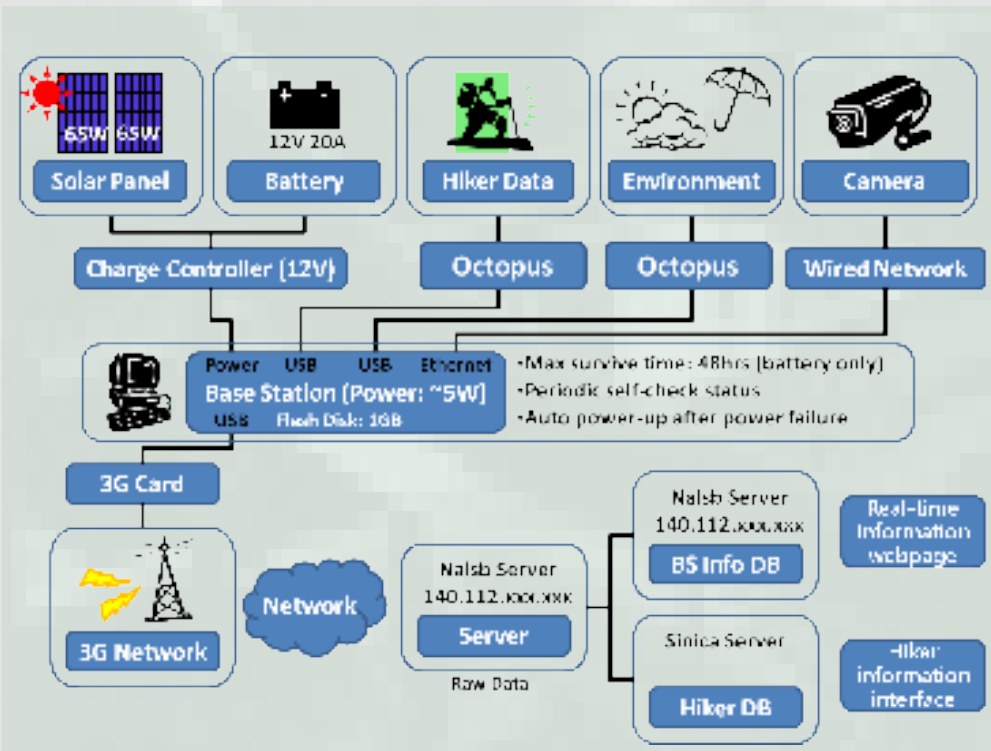
在過去幾年中，我們對於 GWAP (Games with A Purpose) 系統進行了一系列的研究，提升 GWAP 系統的效率及節省人力成本，同時也設計了一種進行人智遊戲的新方法，讓使用的文字更能夠涵蓋欲描述的概念，所收集到的使用者輸入更具有代表性。除此之外，我們也提出了一個能夠偵測作弊行為的方法，

讓研究者能在網路使用者協助下，精確有效率地評估多媒體內容的品質。從各個方面來看，群眾外包都是一個相當有潛力的技術，將電腦與人腦結合共同解題。未來我們也將持續研究及發展群眾外包技術，期能徹底發揮此策略的潛力，解決各領域中重要及懸而未決的問題。

我們與院內及國內外幾所大學合作，研發一個開放式災害管理資訊系統，能支援提供決策與救災資訊所需的各類型服務，主要可接收不同型態與不同來源之訊息（包括智慧型監控系統的感測數據、網路社群、非官方組織的訊息等），經由此一系統過濾與整合後，將產出更完整可靠的救災相關資訊。本實驗室的成員投入的工作包括研發以智慧型網絡實體互連設備與應用做為元件的智慧型災害整備環境；建立在一個預先處理與事後回復之機制上的可靠的應急資訊代理人；在災害發生時各種可用以減少收集、驗證及篩選社群所提供之災害相關資訊所需之人力的方法和工具；及運用不同類型網路接取技術、方式、和網路型態之互補的優點來強化災害發生當時和災後的實體連結。

Quadrant of Euphoria 平台。

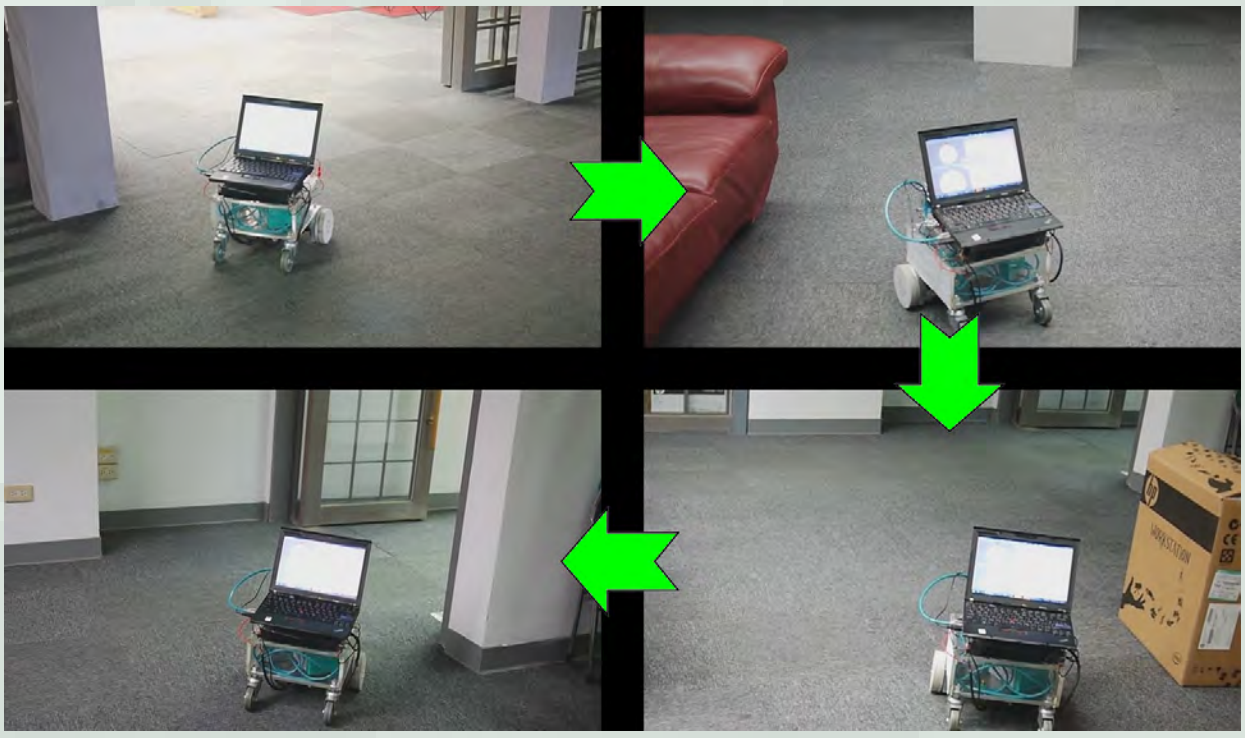
我們也探討大規模風險管理服務相關的網路計算問題。2008 年爆發的世界性信用危機暴露了現今金融體系承受風險的體質相當脆弱。三大信評機構缺乏效率，未能即時揭露公司倒閉事件。例 2001 年安隆宣告破產的五天前，安隆的債券仍維持「可投資」評等；2008 年萊曼兄弟宣告破產當天，也還得 到「可投資」的評等。公司信用的即時評等有相當高的計算複雜度，互補於傳統的經濟與金融理論和實務發展，我們將以雲端計算為基礎，探討佈建大規模即時金融信用風險管理服務的研究主題，發展包括「公司信用的即時評等」、「個人信用的即時評等」、「金融商品評價及風險計量」等計算方法和技術。




玉山國家公園任務型感測系統架構。

# 機器人地圖重建與導航技術

計劃主持人
劉進興副研究員



這套導航系統是一模組化的系統，由不同子系統整合而成。

機器人技術的研發，五十年來愈來愈受到世界各國，尤其是先進國家的重視。得力於 3C 科技以及感測與嵌入式系統技術的逢勃發展，技術的水平及垂直整合，機器人系統的形式及所能達成的功能與任務更加完善及多元。機器人已在軍事、工業、醫療等專業領域擁有極高的應用，發展機器人相關的系統設計、感測、規畫、控制的基礎理論和整合技術、情感與認知計算，讓人能安全舒適的與機器人進行必要的互動，使機器人能廣泛走入民生用品領域，在食、衣、住、行、育、樂等生活層面上，扮演著積極而不可或缺的任務和角色。

## 現階段的研發

目前中研院資訊所的機器人研究，由劉進興博士領導的研究團隊，正進行機器人導航系統的建置與應用。研究的方式在於建造一個配備有雷射測距儀的實驗用輪型導航機器人，這個機器人由兩個前輪馬達驅動，進行水平面方向的運動，雷射測距儀經由一個四連桿機構帶動，可進行簡諧運動。在未知環境的重建技術方面，藉由這個實驗機器人進行資料收集後最佳化地圖比對，研究團隊在中研院資訊所內進行自主二維及三維未知環境的重建實驗。相關連結：

二維地圖重建 -http://www.youtube.com/watch?v=Rpl7tuGHsUA&feature=relmfu

三維地圖重建 -http://www.youtube.com/watch?v=ceBAgnJhack

導航 -http://youtu.be/jGuq4SsEN9Q

在導航技術方面，研究團隊應用邊緣追蹤的導航模式，由感應器的量測資訊中辨認出障礙物的邊緣或牆壁的轉角，並將此邊緣或轉角設為移動的目標。為避免重複路徑與脫離死路狀況，本研究提出標記排斥區域的方式，大量減少記憶空間的需求量。

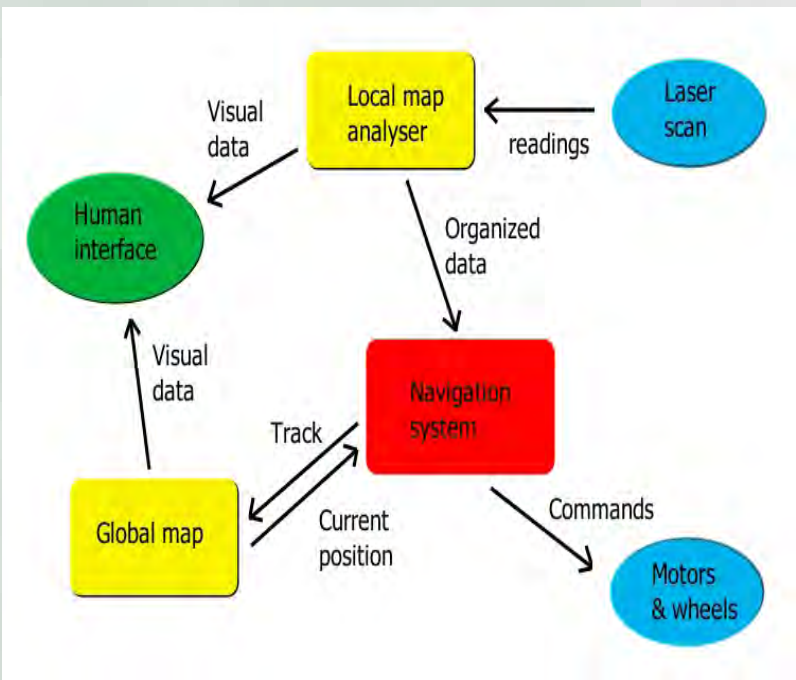
Nao 機器人。

## 未來展望

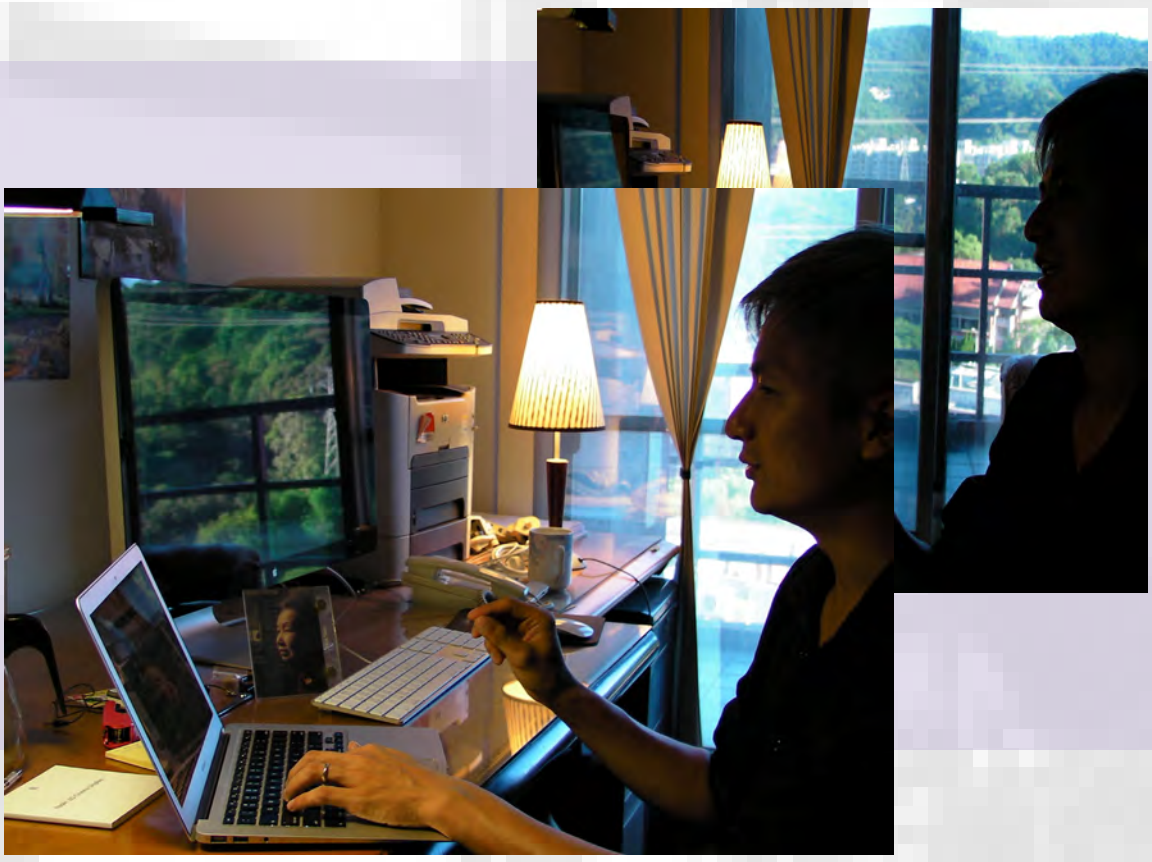
這套導航系統是一模組化的系統，由不同子系統整合而成。搭配不同設計的軟體與感測器（子系統），可進行的任務包括：探索、三維環境重建、保全及巡守的工作，執行的細節包括巡邏、入侵者的追蹤、攔截、訊息通報、甚至包括防衛、救災之任務、或者醫療照護。這些機器人技術也將整合無線感測網路用之於建置居家照護機器人系統的延伸研究。

Sony humanoid Nao 機器人。

各種不同設計的軟體與感測器。



# 數學是簡單化理解事物的美學
## 副研究員穆信成


穆信成副研究員接下傳承火把。

### 您成長背景以及當時引起您學習興趣的動機

在資訊領域中我所感興趣的研究是「程式語言」，當我和圈外人介紹時我會說我在做「電腦科學中比較數學的部分」。但求學過程中我的數學並不特別好，高中時也曾考過零分。

我是一個從小愛玩電腦、學寫程式的小孩。後來才知道，因為當時時代背景政府查禁電玩業，所以電玩機台業者改做蘋果二號電腦仿冒機求生存（幾年後又改作 PC 相容機）。而我家裡買了一台，那年我才十歲。當時，人們對於電視、音響、冷氣機，可以很容易的了解它的功能。但電腦有什麼功能呢？而且還是一台功能很弱的個人電腦？那年代的一般人很難說出個所以然來。和所有小朋友一樣，我先拿那台電腦玩遊戲 --- 那時得把電腦接上錄音機，載入錄在錄音帶裡面的遊戲程式。玩膩了，我讀隨著電腦贈送的書和雜誌，學寫程式。從印簡單的圖形開始，到賽馬之類的簡單小遊戲。因為我只認識英文字母，不會任何單字，便把指令一個字母一個字母硬記下來。我不會把程式存到錄音帶裡頭，每次開機，程式都得重寫。寫著寫著，漸漸覺得這程式的結構在腦裡越來越清晰。我可以把程式寫得越來越短，越來越清楚。多年後回想起來，我會解釋為這是把自己拉到抽象的層次去理解程式的過程。

也許當時我對「程式語言」已經產生初步的興趣。我覺得這是這門學問優美之處，就是把一個問題用適當的抽象方式去理解、用合適的符號寫下來，它的解決方式自然地變得很清晰。這門學問告訴我們的是：抽象的理解是重要的，好的符號是重要的。

當我在國、高中時期常往當時的中華商場跑，並且加入一間後來是黑店的會員，因為他們答應替我拷貝到一套 Lisp 語言的編譯器。我問他們有多少會員？老闆支支唔唔的，後來我才知道我是第一個會員，之後他們生意做得不錯，說我是該店的福星。當時，中華商場是取得軟體的管道，除了學生、玩家，還有外國訪客慕名而來和店家比手畫腳。現在我們會說那是違法的盜版軟體公司，

台灣進入世界貿易體系必須擺脫的不堪過去。我買了厚厚三本手冊，邊查單字邊學怎麼在麥金塔電腦上寫程式。當時這些書得偷偷地看，但再過個幾年，台灣興起一股電腦熱潮，父母爭相把小孩送去學電腦。但我早生了幾年，家人更擔心我太沈迷在電腦上，大學考不好。母親曾拜訪該店的老闆，請他勸勸我。我記得那天他難得地嚴肅，「我自己學歷不高，吃了很多苦，」他說，「功課還是要顧呀！」

**您的研究專長為 Programming Language，這個領域在台灣算是非常冷門。您當初怎麼會想要往這方面發展，如何認識這個領域的呢？有何影響深刻的科學家？**

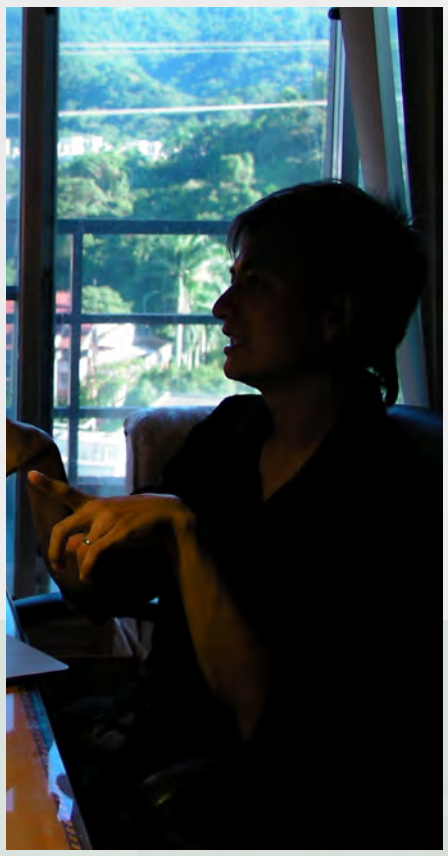
後來我考上資訊系，一次放假回家，發現以前藏在桌下看的「電腦書」，現在成了功課，可以放到桌上看了，一下子竟難以適應起來。資訊系成為大熱門，而我又喜歡上了熱門中的冷門。後來我會成為 Richard Bird 的學生，多少也因為他覺得知音難尋，對「程式推導」這門學問有興趣的人不多。我很任性的悠遊在此學門中，因此成了學歷高的人。人生有時很荒謬，雖然我選擇了冷門的學門，很幸運的我的興趣被歸類到熱門產業的範疇內。我覺得這不很公平的是，一些像我一樣堅持恣意投身其他冷門行業的朋友，他們卻享受不到這麼多資源，但我認為因此更顯出他們的勇氣與另人敬佩其堅持的毅力。

在一次偶然的機會下，我在圖書館時發現一本「函數編程」的入門書。後來經人推薦，讀了 Richard Bird 與 Philip Wadler 的函數編程簡介，發覺「這就是我要的」。但同學之中沒人了解我在說什麼。一天，又是很偶然地看到莊庭瑞老師徵助理的告示，專長需求中赫然見到「函數編程」。我興奮的半跑半跳著回宿舍，迫不及待的想和他聯絡。那年來到資訊所當工讀生，記得莊老師的辦公室還在歐美所。一切都很新鮮愉快，我印象最深刻的卻是他唯一一次責備我的一句話。我在白板前並不是很有把握地比手畫腳解釋一篇論文，他說：「也許你懂了，但你這樣講我不懂唷。」，一語點醒我，原來，能把事情說清楚，才是真正懂了。就和清晰的程式一樣。

雖然我的興趣決定了，但可走的路就窄了。同學大都去當工程師，而我得出國才能往有興趣的方向發展及出路。申請學校前一年，我讀了 Bird 與 Oege de Moor 的「編程的代數」，覺得實在無法想像程式設計能這樣去理解，若能學會這東西的話一定很棒吧。可是，我做得到嗎？我數學沒那麼好，學得來嗎？無論如何我遞出了申請表，並很幸運的被選上成為他的學生。在牛津的那幾年很愉快，那是個可以寵壞我的搖籃，大家的題目不同，但說著彼此可以理解的語言。 原來數學，至少是我們用得上的數學，沒那麼難親近：數學是一門希望盡量用簡單、通用的方式，去理解事理的學問。這點我到大學才體會到，到最近才想通。高中以下的數學教育似乎白費了。 可惜在我畢業時，「程式推導」這門技術已經很少人在玩。

「輪你拿火把了，」他們說。

Richard Bird 是我心目中理想的學者典型。他的演講清晰有力，魅力十足。身為教授，雖然已經屆退休年齡，他仍自己算程式，解決我的技術問題時反應比我還快。許許多多次，我會胡亂湊出個解，而他會皺著眉頭，把我的東西丟掉重作一遍，將一切理得又清楚又漂亮。這是他有的美感。相對於我印象中的亞洲教授層級學者大都已不在第一線親手作研究，我希望自己也能像他一樣。後來我才知道這也是不得不然。Richard 多年來申請到計畫的數量很少。沒有研究生，他只好自己動手。


剪影般的人生。

我的另一個偶像是 Edsgar Dijkstra，他的文章鏗鏘有力，讀來痛快淋漓。他讓你相信，數學需要計算科學的啟發，而形式方法不僅讓軟體開發變得更容易（而不是一般認為的更難），根本是有效軟體開發的「唯一」方法。但人如其

( 文轉第 15 頁 )

# 善用自由、開源軟體便利您的生活

自由、或是開源軟體 (Free or Open Source Software) 對於網路資訊爆炸的現代人來說並不算陌生。自由或開源軟體的好處除了大多數是免費使用、散布之外，最大的優點在於其開放原始碼的特性，每一個懂程式開發的開發者還可以自由地去修改該軟體缺乏或是不完善的功能，使之更加趨近於完美。自由軟體鑄造場（Open Source Software Foundry）的網站： www.openfoundry.org 本身即是一個開源專案，網站上即可下載到程式碼。OpenFoundry 匯集程式開發者會使用到的專案管理功能，以及各種程式開發的教材資源、網站列表等等，定期發布自由軟體電子報，也會舉辦與 Open Source Software 相關的推廣活動。歡迎各界有興趣的朋友一同參與！

## Xmind

心智圖不但可以幫助我們釐清思考，也可以運用在心得記錄、創意發想、書籍草擬、會議記錄 ... 等等。XMind 是一套類似 FreeMind 的開放原始碼的心智圖軟體，可以讓使用者快速地畫出心智圖，而且它比起 FreeMind 更加地色彩繽紛。它也有提供附加專業功能的約期授權商業版本。

## GanttProject

GanttProject 是一套開放源碼的專案管理程式，管理專案的可用資源、時程表、任務、子任務，並可記錄任務的起始日期、持續時間、相依性等功能，並且在排程的同時畫出甘特圖，還可以建立 PERT 圖。檔案可以輸出為 PNG 圖檔，PDF 或是 HTML 格式，另外它也可以匯入 Microsoft Project 檔案。

## OpenVAS

OpenVAS 全名是 Open Vulnerability Assessment System（開放弱點評估系統），為一款整合相關工具的網路安全掃描圖型化套件。核心部分是由伺服器元件，以及一群遠端系統與程式組成的測試弱點外掛。目前版本引入了新的功能及新的架構，將原先只是弱點掃描的形式轉化為弱點管理解決方案。本專案每日皆以 15,500 以上的網路弱點測試來反饋更新組件。

## Blender

Blender 是一套專家級的 3D 繪圖軟體。它除了是自由軟體、免費供人使用之外，功能也相當齊全，可以廣泛地被應用在製作動畫短片、技術視覺特效、商業圖表、或者設計使用者介面等用途。它不僅支持各種多邊形繪圖，也能夠輕鬆地製做出動畫。喜歡 3D 繪圖的玩家們不用花大錢，也可以製作出自己喜愛的動畫、模型。

自由軟體鑄造場（Open Source Software Foundry，OSSF）重點任務爲培植本土自由軟體社群與人才，主要目標爲：

（一）推廣自由軟體概念

（二）集結國內自由軟體社群

（三）促進臺灣人才培育與產業合作

（四）與國際趨勢交流接軌

主網站： http://www.openfoundry.org

聯絡電話： (02) 2788-3799 # 1469, 1477

聯絡信箱： contact@openfoundry.org

Website: http://www.openfoundry.org

Tel: (02) 2788-3799 # 1469, 1477

E-mail: contact@openfoundry.org

## 人物焦點

（文轉自第 **13** 頁）

文，Dijkstra 的優點是他的熱情、執著、與強烈的好惡。這也是他的缺點。一次我與來自他曾任教過的荷蘭學校的學者聊起，「你在台灣教 Dijkstra 的東西嗎？」他很驚訝，「我們那兒沒人在教了。他走之前得罪了所有人。」

### 您研究的目標為何，其中遇到什麼困境，並且期許對人類生活具有何影響？

透過研究，我希望對人類生活有什麼具體影響？這很難答。說穿了，促使我研究的原因是「我還不懂」，這令我很不舒服，我希望懂得更多。小時我經常覺得不懂，後來理解了，一個個程式變清晰了，但不懂的東西更多了，於是這麼一直追著下一個目標，直到今天。好奇心和美感都是人的本能。好奇心使你找不到問題的答案時會翻來覆去睡不著覺，而美感使你能分辨哪個答案是好的，是美的。找到了一個美的答案，會讓你蹦蹦跳跳很興奮，迫不及待想和人說。我常愛說，我的工作本質上是娛樂業，也可以這麼讀解，「研究是應該要帶給人快樂的」。

### 對未來想從事該領域資訊研究的學莘有何建議

說到對未來學子的建議，我最近有一個很深的體會，我們所受的訓練，有時會太沉迷於前人的成就，而覺得一些新的、太「工程」的領域不夠美，沒有深度。但我們所知的「美」的領域，也都是前人將一團亂的東西理出頭緒的結果。我們應做的是投入不美的領域，將其中的美感發掘出來。我認為 Dijkstra 所謂的「美是我們的責任」指的應該就是這個意思。

# 活動快訊

## 自強活動一日樂活

年度自強活動一日遊，於四月十三日前往桃園天空步道，風景優美，媲美於美國大峽谷玻璃天空步道，小烏來角板山、桃園仙谷，有如世外桃園，因此，活動參加人數十分踴躍，創歷年新高，大家無不盡興而歸。

中央研究院資訊科學研究所
115 台北市南港區研究院路二段 128 號
發行人：許聞廉
編輯：王佩琪，曾慧琦
tel.: +886-2-2788-3799
www.iis.sinica.edu.tw