中研院訊

Academia Sinica Newsletter

第 1769 期｜ 2022 年 07 月 14 日發行

本期目錄

當期焦點

學術活動

漫步科研

編輯委員
湯雅雯、林于鈴、吳岱娜
賴俊儒、陳玉潔、吳志航
林千翔、陳禹仲、曾國祥

編輯
陳竹君、黃詩雯、陳昶宏

電話
02-2789-9488

傳真
02-2785-3847

信箱
wknews@gate.sinica.edu.tw

地址
11529 臺北市南港區研究院路二段 128 號

本院電子報為同仁溝通橋樑，隔週四發行，投稿截止時間為前一週星期四下午 5:00，若逢連續假期則提前一天截稿，歡迎同仁踴躍賜稿。

本院第 33 屆院士暨名譽院士選舉結果出爐
公布 19 位新科院士 3 位名譽院士

▲ 左起：施明哲院士、司徒惠康院士、廖俊智院長、林昭庚院士、林麗瓊院士、唐堂院士

本院第 33 屆院士暨名譽院士名單揭曉，由廖俊智院長與院士會議四組召集人於 7 月 7 日會後記者會中共同宣布選舉結果，共選出 19 位新科院士，3 位獲選名譽院士。

針對本屆選舉結果，院士會議發言人伍焜玉院士表示，院士選舉過程審慎嚴謹，經過多天多次詳細討論及審查，並以依法行政及最尊重候選人的方式處理院士國籍議題。

伍院士進一步指出，公布的新科院士當選人皆屬本國國籍；除 19 位已確認國籍者外，另有票數通過當選門檻、但國籍待確認者計 5 位，生命科學組 1 人、工程科學組 2 人、人文及社會科學組 2 人。由於本院非國籍法最終認定單位，將協助當事人釐清，若有需要亦將請主管機關認定之，待確認適法後，才會公告並發給院士當選證書。

本屆新科院士以生命科學組 6 人最多，數理科學組 5 人、工程科學組 5 人、人文及社會科學組 3 人，其中女性院士有 4 人。最年輕的是生命科學組吳慶明（男，51 歲），最年長的是數理科學組陳騮（男，76 歲）。

另也選出 2022 年名譽院士 3 位，頒予美國加州理工學院大衛．莫里斯物理學講座教授史東愛（Edward Carroll Stone）、日本京都大學高等研究院副院長暨特聘教授本庶佑（Tasuku Honjo），以及哈佛大學藝術與科學學院人類學系教授凱博文（Arthur Kleinman）。

史東愛曾於 1984 年獲選美國國家科學院院士；本庶佑曾榮獲 2018 年諾貝爾獎生理醫學獎；凱博文曾榮獲英國皇家人類學會 Wellcome Medal、美國人類學會最高成就 Boas 獎、美國心理分析學會的終生成就獎等。

本院現有院士 264 人，新科院士出爐後，也讓院士陣容增至 283 人。名譽院士原為 13 人，亦增加至 16 人。

第 34 次院士會議主題演講 邀請國際頂尖科研機構院長，分享新世代科學永續新動力

▲本院廖俊智院長與美國國家科學院院長瑪西婭 · 麥克納特進行對談

本院第 34 次院士會議 7 月 4 日正式開幕，首日上午以線上視訊方式，邀請日本理化學研究所（RIKEN）理事長五神真（Gonokami Makoto）以及美國國家科學院（National Academy of Sciences, NAS）院長瑪西婭 · 麥克納特（Marcia K. McNutt）進行主題演講。五神真以「學術界在社會變遷中的角色」（The Role of Academia as a Platform for Social Change）為題，分享科學界如何運用不斷創新的知識，參與實現社會的包容及永續發展。瑪西婭 · 麥克納特以「延續無盡的前沿」（Sustaining the Endless Frontier）為題，分享尖端科學在全球化與現代公民社會的互動性。

RIKEN 和 NAS 都是世界知名的基礎科學研究機構，和臺灣的學術界有深厚的合作。五神真是一位實驗物理學家，在東京大學有數十年的研究與教學經驗，在 2015 年成為東京大學校長，2022 年成為 RIKEN 新任理事長。瑪西婭 · 麥克納特是一位地球物理學家，她於 2009 年至 2013 年擔任美國地質調查局（USGS）主任，領導並參與多起國際地質災害調查，2013 年至 2016 年，她擔任《科學》（*Science*）期刊的主編，2016 年起擔任 NAS 的院長。

歷經全球化與社會變遷，科學在人類生活中持續扮演關鍵角色

兩位主講人都提到，「科學」在人類生活中扮演關鍵角色，當代的科學社群已經走向國際合作及跨領域協力的新時代，必須以更快、更創新的策略整合資源和人才，共同因應氣候變遷、疾病、地緣政治衝突等重大挑戰。

五神真理事長以日本經驗，說明科學對社會生活帶來永續的影響力。包括東京多摩川（Tama River）的水源復育、減碳科技緩解氣候變遷的衝擊、因應新冠疫情快速啟動數位變革、大數據與通信網路輔助氣象與災害防治等經典案例，都是日本學界擴大基礎研究能量，以應用科學的形式在民眾的日常生活中發揮正面助益，達到日本「社會 5.0」的願景。

瑪西婭・麥克納特院長以 1945 年的《Science, the Endless Frontier》報告為基礎，這份開創性的報告是當代美國科學界的發展藍圖，擘劃了科學飛躍性的發展與科技普及。在歷經超過 77 年之後，世界情勢與人類生活劇烈變化，當代的科學社群更講究跨領域的重要性，匯流型的研究計畫越來越普及，跨國、跨學科、跨政府、學術與產業界的合作案例大幅增加，加上政策及科學行銷的推廣，使得科學成果的影響力超越過往的想像。

鼓勵女性、新世代參與，營造跨領域合作的新時代

瑪西婭・麥克納特是NAS首位女性院長，演講後本院安排三位女性研究人員與談。物理研究所林耿慧副研究員，是生物和物理學的跨領域研究專家，她特別呼應了跨領域研究的重要性，除了激盪創新的想法，也能促進研究的競爭與進步。分子生物研究所薛雁冰副研究員，提到「科學傳播」與「科學教育」的重要性，隨著科學普及，溝通變得越來越重要；中國文哲研究所劉瓊云副研究員，從人文學者的角度呼應了自然科學結合人文關懷的重要性。瑪西婭・麥克納特回應，NAS 正在施行一些創新的計畫，鼓勵跨領域競爭、科學傳播以及科普教育，科學社群就像一棵向下扎根、向上發展的樹，要兼顧自然與人文的果實，也要有能力吸引更年輕的養分持續投入。

主持人廖俊智院長提及，「好奇探索」與「解決問題」一直是基礎研究的重要驅動力，本院也致力於打造完善的研究環境和文化，推動科學研究生生不息。瑪西婭・麥克納特也認同創新與應用的需求是科學的起源，許多基礎研究成果就像青黴素的發現，經過創新的應用擴散對全人類生活的福祉。

本次院士會議因為疫情因素改為實體及線上同步，廖俊智院長感謝來自美國及日本的兩位主講人，以及全球各地上線參與的院士，也期待在疫情緩解後，能早日重啟與 RIKEN 和 NAS 兩位院長的實體交流和互訪。

第 34 次院士會議開幕 關注前瞻科研議題 擘劃學術研究方向

本院第 34 次院士會議於 7 月 4 日正式開幕，為期 4 天的議程包括頒發院士證章、討論學術研究重大議題與選出第 33 屆院士暨名譽院士等。此次會議原訂 2020 年舉行，受 COVID-19 疫情影響延至今（2022）年，也是史上首度以實體和視訊方式同步進行。院長廖俊智開幕致詞時，感謝院士不辭旅途辛勞現場參與，以及克服時差視訊與會，有各領域院士們協助，以及政府單位支持，本院得以持續強化國內外學術合作，在關鍵研究領域尋求突破，將基礎研究成果貢獻於人類社會發展。

總統蔡英文致詞感謝本院與院士們為臺灣的學術研究、科技發展貢獻心力，讓國際社會看見臺灣的研究實力，更體會到臺灣對和平、民主與自由的重視。總統表示，此次院士會議在全球疫情影響下順利舉行，意義格外重大，期盼透過院士們共同討論，為國家擘劃願景，一起推動臺灣的進步發展。

廖俊智院長致詞表示，自 4 年前第 33 次院士會議結束以來，本院持續拓展新知識領域，也有許多具開創意義的重要發現。數理科學領域研究人員與全球科學家攜手合作，參與「事件視界望遠鏡（EHT）」計畫，成功拍攝銀河系中心的黑洞影像。生命科學領域研究團隊

發現細胞分裂過程的第 3 種可能性「無合成分裂」，顛覆過去百年來細胞分裂學說，對於未來探究細胞生理機制有革命性影響。人文社會科學領域，近期與美國西雅圖華盛頓大學共同召開第 4 屆「臺灣研究世界大會」，邀請美洲、歐洲、亞洲各領域傑出的臺灣研究專家與會，此大型國際會議為臺灣研究建立起堅實的世界性學術交流平台。

人類社會面臨的問題日趨複雜且迫切，從基礎研究到解決問題的時程大幅縮短。為了積極回應當前挑戰，中研院持續整合院內研究能量，組成跨領域團隊，投入前瞻研究，也提供年輕研究人員發揮空間。此外，設立臺灣量子科技研發基地，引領我國量子科技發展；在人文社科領域推動「未來社會」研究課題等。各項策略與制度皆致力以基礎研究成果，破解問題的關鍵點；創造科學研究的傑出成果時，也善盡科學家的社會關鍵責任。

廖院長指出，本院除致力創造研究成果外，也積極關注世界各地科學社群發起的行動。例如今年發起「烏克蘭學人獎學金計畫」，提供烏克蘭學者及學生來臺延續學習和研究的機會，期許藉由善盡世界公民責任，盡力提升臺灣的國際影響力。

開幕式主題演講，邀請到二位國際重量級科學家，以線上視訊演講，分別是美國國家科學院（National Academy of Sciences, NAS）院長瑪西婭・麥克納特（Marcia K. McNutt）與日本理化學研究所（RIKEN）理事長五神真（Gonokami Makoto）。瑪西婭・麥克納特以「無盡的前沿」（Sustaining the Endless Frontier）為題，分享尖端科學與現代公民生活的互動性。五神真以「社會變遷：學術界的角色與發展策略」（The Role of Academia as a Platform for Social Change）為題，分享科學界如何藉由知識進步，參與實現社會的包容及永續發展。

中研院第 34 次院士會議自 7 月 4 日開始，至 7 月 7 日結束。7 月 4 日舉辦二場主題演講、頒發院士證章給第 26 屆及第 32 屆當選院士，隨後進行院務報告。7 月 5 日專題討論邀請行政院政務委員唐鳳與談。7 月 5 日至 6 日展開院士暨名譽院士選舉閉門分組審查，於 7 月 7 日進行院士選舉。

第 34 次院士會議專題討論
唐鳳與院士對談
以數位連結人，擴散數位素養，創造數位共融

▲ 左為行政院唐鳳政務委員，右為本院廖俊智院長

本院第 34 次院士會議於 7 月 5 日邀請行政院政務委員唐鳳，以「國家數位發展規劃」為主題參與專題討論。這是一場「沒有任何形式、完全開放的討論」，兼有現場發言及網路匿名提問，議題涵蓋數位、科學、人文、性別等，唐政委與院士們共創了一場精彩的思想激盪！

唐政委首先援引《行政院 112 年度施政方針》，說明我國數位政策發展願景「建構數位服務跨域協力典範，增進政府效能與韌性運作；完備數據公益生態制度及應用，拓展個人資料自主運用範疇；促進跨國公民科技與資料民主化的共同發展，落實智慧國家願景。」主持人廖俊智院長進一步提問數位能力與人才培育策略；唐政委則回應道，政策願景落實到中長程的行動策略，是希望最終能讓「數位」大使從數百位、數千位擴散到數千萬位，逐漸加深政府、非政府組織與全民的「數位素養」。

院士提問聚焦數位發展部的籌備現況，以及未來數位政策的走向。唐政委一再強調，數位發展部的籌劃精神是以數位引領發展，數位不是技術，而是深入社會生活的媒介，不應該被量化比較優劣；期許政府能持續藉由數位的資源加速推展社會共同的價值、激發創新，幫助臺灣形成新的「數位典範」。

唐政委特別強調數位共榮必須仰賴人與人之間的溝通、理解與信任。她以高齡近九十歲的阿嬤為例，阿嬤沒有在網路上登記實名制買口罩，但是願意走到超商操作機器再付現金完成交易，是她最好的數位測試員。新的技術工具如果若能保有人文的溫度與信任感的元素，將會跨越年齡與技術障礙，促進世代的數位共融。

這場「沒有任何形式、完全開放的討論」，內容將公開在唐鳳政委的工作紀錄中，歡迎大家一同回顧這場精彩的對話沙龍。

網址：https://youtu.be/mvt8jDs-SVs

本院鄧昌黎院士辭世

本院鄧昌黎院士於今（2022）年 6 月 24 日於美國辭世，享耆壽 97 歲。

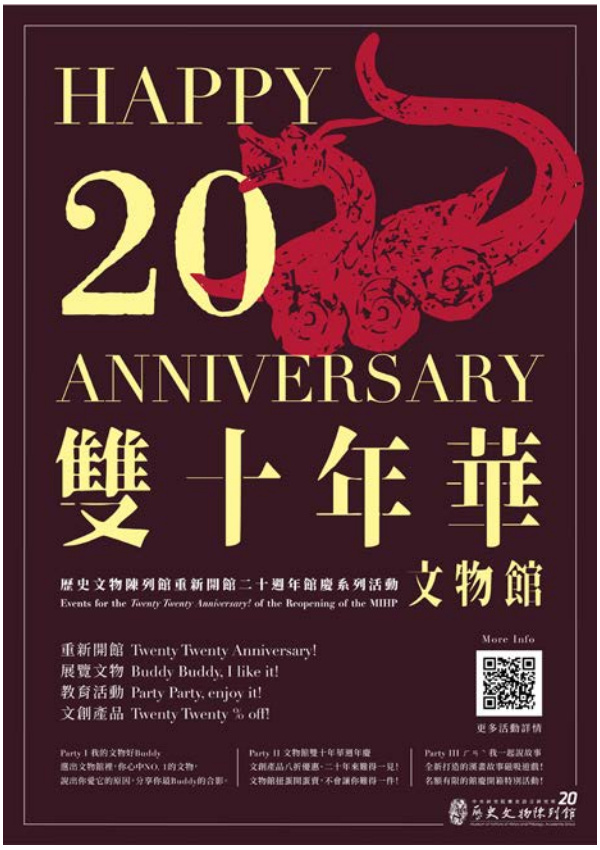
鄧昌黎院士為國際知名物理學家，專長為應用物理學。1951 年取得美國芝加哥大學物理博士後，陸續於美國阿岡國家實驗室及費米加速器實驗室擔任要職，領導粒子加速器大型設施的研發；亦曾於芝加哥大學及威斯康辛大學任教。

鄧院士於 1983 年起參與策劃興建我國國家同步輻射研究中心，為臺灣同步加速器發展奠定重要基礎，影響深遠。2007 年，鄧院士獲美國物理學會（APS）頒發羅伯特 ・ 威爾遜獎（Robert R. Wilson Prize），表彰其於近代粒子加速器研究領域的傑出成就，為全球首位獲此榮譽的華人科學家。鄧院士並於 1966 年當選為本院第 6 屆院士。

活動訊息〉「雙十年華，文物館！」歷史文物陳列館重新開館二十週年館慶系列活動

本院歷史語言研究所歷史文物陳列館自 2002 年重新開館至今已二十年。文物館將於今（2022）年舉辦重新開館二十週年館慶活動，包括精彩絕倫的文物與展覽、趣味互動的教育活動，以及期間限定的文創優惠。邀請大家一同歡慶文物館的雙十年華！系列活動辦理時間詳見活動網站。

活動網址：http://museum.sinica.edu.tw/events/157/



本院物理所新科院士系列講座

【第一場】

時間：7 月 20 日（星期三）14 時至 16 時

地點：物理所 1 樓演講廳

講者：本院錢嘉陵院士（Dept. of Physics & Astronomy, Johns Hopkins University）

講題：Half Quantum Flux and Spin Triplet Superconductors

【第二場】

時間：8 月 18 日（星期四）14 時至 16 時

地點：物理所 1 樓演講廳

講者：本院李定國院士（國立清華大學物理系特聘研究講座教授）

講題：在銅氧高溫超導體中之配對密度波 Pair Density Waves in Cuprate High Temperature Superconductors

【第三場】

時間：8/24（星期三）14 時至 16 時

地點：物理所 1 樓演講廳

講者：本院盧志遠院士（旺宏電子科技總監暨總經理、欣銓科技董事長）

講題 產業應用物理的典範——半導體 IC 技術之峰迴路轉

活動報名網址：

https://forms.gle/VNvLXeiTm6G2nNM28

聯絡人：洪敏玲，(02)2789-6750 / mlhong@gate.sinica.edu.tw

活動報名〉
2022 International Conference on Method Triangulation: Implications for Social Science Research

時間：2022 年 8 月 18 至 19 日（星期四至星期五）

地點：本院人文社會科學研究中心第二會議室

主辦單位：本院人文社會科學研究中心調查研究專題中心

協辦單位：國立政治大學臺灣政經傳播研究中心

籌備委員：張卿卿特聘研究員（本院人社中心調查研究專題中心）、賴至慧副研究員（本院人社中心調查研究專題中心）、林芝璇副教授（國立政治大學傳播學院）

活動網址（含議程及報名資訊）：https://survey.sinica.edu.tw/CSR2022/

報名期間：即日起至 8 月 10 日（8 月 11 日以電子郵件通知報名結果）

聯絡人：邱亦秀小姐，(02)2787-1821，csrevent@gate.sinica.edu.tw

活動簡介：

此研討會主題聚焦於「跨方法研究的應用」，除了 8 篇精彩的論文發表之外， Keynote 邀請到美國密西根大學的 Dr. Frederick G Conrad 主講社群媒體與調查資料的跨界應用。另有 3 場座談會：分別邀請英國愛丁堡大學何俊霆博士、美國華盛頓大學的蕭遠教授，以及美國麻省理工學院的 Dr. Teppei Yamamoto，針對 Digital Footprint Data、Text Mining，以及 Conjoint Experiments 等議題籌組場次，並邀請該領域內頂尖之學者發表研究成果。

備註：

本次研討會將以線上及實體併行（外國學者於線上發表；國內發表人及與會者現場參與），全程將以英語進行發表及討論交流。為保持室內社交距離，報名人數有限，主辦單位保留錄取名單決定權。

「中研院出版品整合平臺」已上線 匯聚全院學術能量

「中央研究院出版品整合平臺」目前已彙整全院數理科學、生命科學、人文及社會科學三大領域共 16 個研究單位，自 1932 年以來逾 3,000 筆書目資訊。歡迎大家透過線上一鍵遨覽，掌握本院研究成果與研究趨勢。

除了「GPI 政府出版品資訊網」、院內各研究單位自行建置的出版品專頁，此前本院並無一個統合性管道，集中呈現全院出版成果。不僅各界無法透過單一平臺快速掌握本院出版概況，院內人士參與國際會議、國際書展或國際交流時，亦缺乏管道簡便地透過數位展示，凸顯本院學術出版特色、各單位長期及近期的研究取向，實屬可惜。

有鑑於此，本院以「線上圖／圖書館」為設計理念，打造此一出版品整合平臺。現階段針對「想了解中研院或中研院出版特色」、「有明確的查找範圍與目標」二種不同目的的使用者，初步設置「從數據看出版」、「書庫總覽」與「書庫檢索」三大功能，讓其能有系統地檢索本院系列出版成果、瀏覽新書資訊，甚至一窺研究單位及學者的研究方向與出版特色。

「書庫總覽」以書架為意象，以顏色為區隔，陳列了不同類型（如期刊、史料、論文集、專書、目錄、手冊等）之出版品，搭配篩選器的數目呈現，本院的出版分布概況一目了然。使用者並可進一步根據出版品類型、出版單位、出版年份，縮小檢索範圍，藉此勾勒出不同範圍下院內出版品的輪廓。點擊單筆出版品，可概覽書名、作者等基本出版資訊，並連結至各研究單位的書目介紹。

在此探索過程中，使用者得以初步了解本院著重的研究方向，以及各單位的發展過程與出版特色。為了更具體呈現之，「從數據看出版」功能特以若干研究單位為例，搭配資訊圖表，透過數據佐證帶出出版特色。例如，臺灣史研究所三分之一的出版品與日記相關，原因在於研究人員自1999 年就組成日記解讀班，定期解讀、校訂及註釋，並將累積成果轉為知識庫，成為反映經濟社會政治史的重要參考素材。

有明確查找目標之使用者，則可透過「書庫檢索」功能進行出版品搜尋。目前此功能提供書名、作者名、出版單位、出版品主題等檢索，日後平臺將介接各研究單位的書籍目錄及摘要，提供更精確且完整的搜尋脈絡與結果。

除了讓使用者如同置身於書架間，瀏覽揀選，尋找自己期待的書籍，本院期能藉由出版品整合平臺，使更多意料之外的知識能量偶遇碰撞。

未來「中央研究院出版品整合平臺」將持續豐富內容與功能，整合院內各式出版需求，化身為掌握學術前沿資訊不可或缺之窗口。

期刊出版〉《中央研究院歷史語言研究所集刊》第九十三本第二分已出版

本院歷史語言研究所編印之《中央研究院歷史語言研究所集刊》第九十三本第二分已出版，本期共收錄 4 篇論文：

1. 黃儒宣，〈左冢棋局及博塞遊戲相關問題探究〉
2. 黃怡君，〈漢代功次升遷制度考〉
3. 郭津嵩，〈僧一行改曆與唐玄宗制禮〉
4. 任小波，〈吐蕃帝國興佛運動與西藏早期中觀傳統——《大乘經纂要義》以及相關文本研究〉

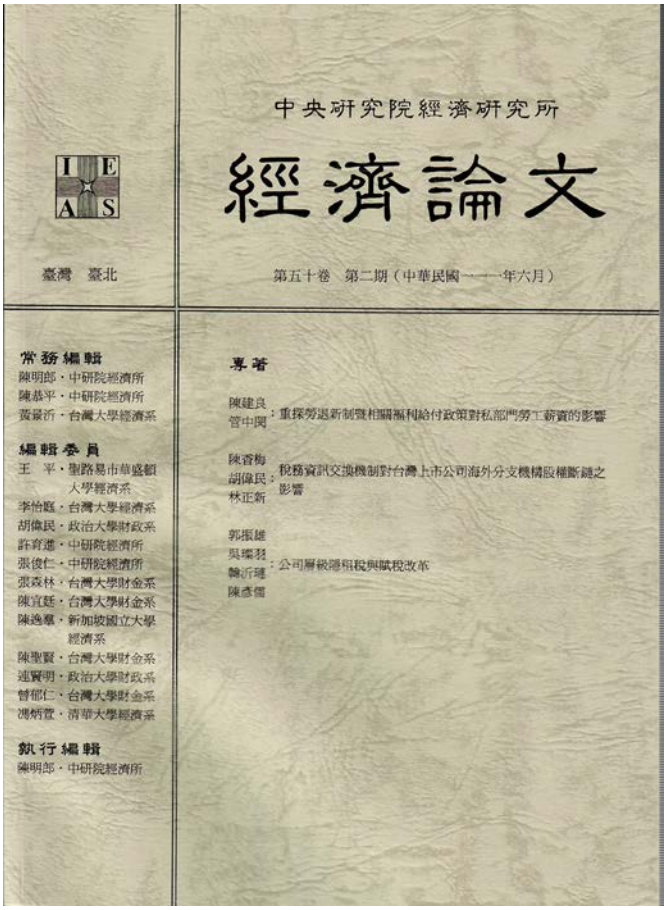
歡迎線上瀏覽：https://www1.ihp.sinica.edu.tw/Publications/Bulletin/1146

期刊出版〉《經濟論文》第 50 卷 第 2 期已出版

本院經濟研究所編印之《經濟論文》第五十卷第二期已出版，本期共收錄三篇論文，作者及文章標題如下：

1. 陳建良、管中閔，〈重探勞退新制暨相關福利給付政策對私部門勞工薪資的影響〉
2. 陳香梅、胡偉民、林正新，〈稅務資訊交換機制對台灣上市公司海外分支機構股權斷鏈之影響〉
3. 郭振雄、吳璨羽、韓沂璉、陳彥儒，〈公司層級隱租稅與賦稅改革〉

《經濟論文》已全文上網，歡迎至本刊網站瀏覽：https://www.econ.sinica.edu.tw/4d49b1b1-d551-4956-84a5-6bbf392d8417/pages/64



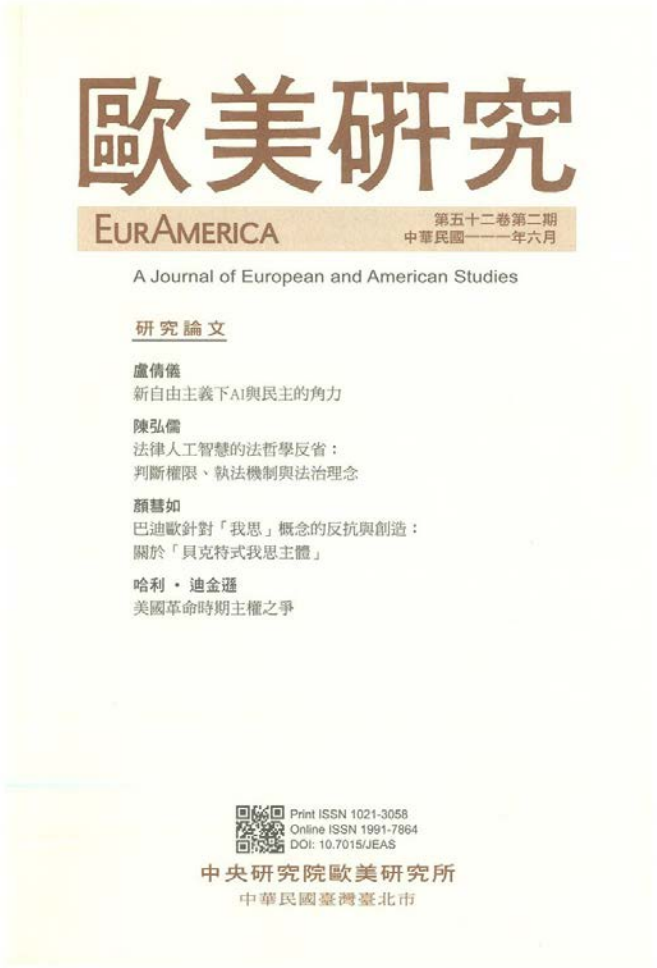
期刊出版〉
《歐美研究》第 52 卷 第 2 期已出刊

本期共收錄 4 篇文章，作者及論文名稱如下：

1. 盧倩儀，〈新自由主義下 AI 與民主的角力〉
2. 陳弘儒，〈法律人工智慧的法哲學反省：判斷權限、執法機制與法治理念〉
3. 顏彗如，〈巴迪歐針對「我思」概念的反抗與創造：關於「貝克特式我思主體」〉
4. 哈利・迪金遜，〈美國革命時期主權之爭〉

可至《歐美研究》期刊官網瀏覽全文：

https://www.ea.sinica.edu.tw/allQuarterly_main.aspx



【專欄】後量子密碼學
Postquantum Cryptography

作者：楊柏因研究員（本院資訊科學研究所）

後量子密碼學 - 以古典電腦抵禦量子破密

每種加密系統的根基，都是一道複雜的數學難題，而現在主流的公鑰加解密系統，包括 RSA 加密演算法 、橢圓曲線密碼系統 (ECC)，背後的數學難題 （大整數的分解因數問題，橢圓曲線上的離散對數問題）複雜得讓古典電腦一籌莫展，卻正好是量子電腦最擅長解決的問題型態。因為這些數學難題的答案，皆可轉化成週期性的結構，理論上，只要找到結構的週期，就可以「較為輕鬆」的破解問題。對於古典電腦來說，當數字相當巨大時，尋找週期仍是十分困難的任務，對於量子電腦卻是小事一樁。在 1994 年 Peter Shor 發明的演算法正好可以尋找週期，也就是能破解目前主流的所有量子密碼系統。相較於常見的對稱式密碼系統如 AES 只需要兩倍長的金鑰就可保證同樣的安全性，基於 RSA 和 ECC 的公鑰密碼系統在夠大的量子電腦出現後便不再安全。因此，量子電腦蓬勃的發展勢必會威脅到生活中的隱私。

後量子密碼學（post-quantum cryptography，PQC）就是一個研究能夠抵禦量子破密的密碼學分支。在 PQC 中的公鑰密碼系統，主要歸類為以下五類：晶格密碼系統、編碼密碼系統、雜湊函數密碼系統、多變量密碼系統和超奇異橢圓曲線同源密碼系統。

後量子密碼學標準化競賽

為了迎接後量子密碼學時代的來臨，美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）自 2016 年起舉辦「後量子密碼學標準化競賽」，徵求新時代的加解密系統與數位簽章系統。在這場競賽取得最終優勝者，將成為新一代的標準化密碼系統。NIST 曾經舉辦過兩場競賽：千禧年前後的先進加密標準 AES 競賽和 2010 年前後的雜湊函數 (SHA-3) 競賽。成為最後獲選的 AES 和 SHA-3 的贏家的密碼系統的投稿人名利雙收。也因此，這次的競賽吸引了來自全世界的團隊參賽一較高下。2016 年，NIST 在當年 4 月於日本福岡舉辦的 PQCrypto（後量子密碼學）會議上宣布開始徵集後量子密碼系統參加競賽。而 2017 年 11 月 30 日截止收件時共有 82 組投稿。經過一番簡單的檢查，同年 12 月 21 日（聖誕假期前夕的週五）公告上網有 69 件合格的稿件。

比賽的故事

民間故事中煉蠱的過程是把毒蟲全部丟進一個水缸，活著爬出來的就是蠱王。其實這個競賽好像也沒有什麼差別。NIST 的人員公告了誰進入第一輪就回家放假過節了。但是密碼學家多數都是阿宅 (不分男女老少都是)。眾所週知，阿宅是不過節的。美國當地時間 12 月 21 日的晚上就有密碼學家破了其他人投的系統。四個月之後的第一次後量子標準化會議在佛羅里達召開時，已經有 ¼ 投稿的密碼系統被徹底擊破或是嚴重受損。

次年 (2019) 的一月 31 日，因為川普關閉聯邦政府而跟著關門關了快一個月的 NIST 重新開門辦公不久就公告了 26 組晉級第二輪的密碼系統。當年八月，NIST 在加州 Santa Barbara 大學舉辦第二次後量子準化會議。翌年 (2020) 的 7 月 23 日，NIST 公告了晉級第三輪的密碼系統。 經過兩輪的篩選，這時已經剩下 15 組人馬，被分為七組決選者 (finalist) 和八組備選者 (alternate)。決選者中，有五個晶格密碼系統、一個編碼密碼系統和一個多變量密碼系統。備選者中還有兩個晶格密碼系統。晶格密碼系統顯然因為其總體性能優越而佔了絕大多數的晉級名額。

中研院本有相當強的密碼學團隊，這次比賽也沒有缺席。通過了第一、二輪的考驗，我們參與了兩組決選者 (數位簽章系統 Rainbow，和加解密系統 Classic McEliece) 和兩組備選者 (數位簽章系統 SPHINCS+，和加解密系統 NTRU PRIME) 。距離成為世界標準，似乎只剩一步之遙。在這過程當中，筆者的 Rainbow 團隊還成功的破解了和 Rainbow 最接近的競爭者，同屬多變量數位簽章系統的 LUOV。

爭議

在 Rainbow 入選第三輪，和跟它同類的系統 GeMSS 也受到致命的攻擊之後，它本來被看好成為標準。但是 LUOV 的發明人之一，一位年輕比利時人 Ward Beullens，站出來復仇了。Beullens 發現了 Rainbow 結構上的一個問題，並主張因此 Rainbow 的安全性不足。筆者代表團隊進行了一系列的分析並得到結論：我們的系統在 Beullens 攻擊下還是有足夠的安全性。然後雙方和 NIST 就到底誰的分析比較精確爭議了數個月之久。但是聰明的 Beullens 此時發出了更凌厲的一擊。基於相同的結構問題他發現了另一個攻擊，並破解了 Rainbow 最小的參數。這個攻擊或許並不是根本性的，或許 Rainbow 可以換個大點的參數仍然安全，但是它已不可能選上了。

與此同時晶格密碼系統也出現學理和法務上的爭議。學理上有人 (D. J. Bernstein) 主張某種攻擊是可以破解 Kyber 和 SABER。但另一派密碼學家對 Bernstein 的結果極力否認。

法務上的爭議是這樣的：決選者中的 Kyber 和 SABER 都有可能的專利覆蓋，有 ¼ 個世紀歷史的老牌 NTRU 系統則是沒有這個問題。有專利覆蓋的系統如果成為標準，就相當於在為特定人牟利了。剛剛提到的那一派人則極力主張專利上沒有問題。

持有專利者在法院獲得了一些勝利之後。Kyber 和 SABER 的命運看來似乎也就決定了。但最後 NIST 決定花錢買下這兩個專利，並選擇 Kyber 為最後的勝利者。由於之前吹哨者 Snowden 事件中已經有人指控過美國國家安全局 (NSA) 能夠指揮 NIST，因此 NIST 究竟有何想法受到一些質疑。

其他的選拔結果

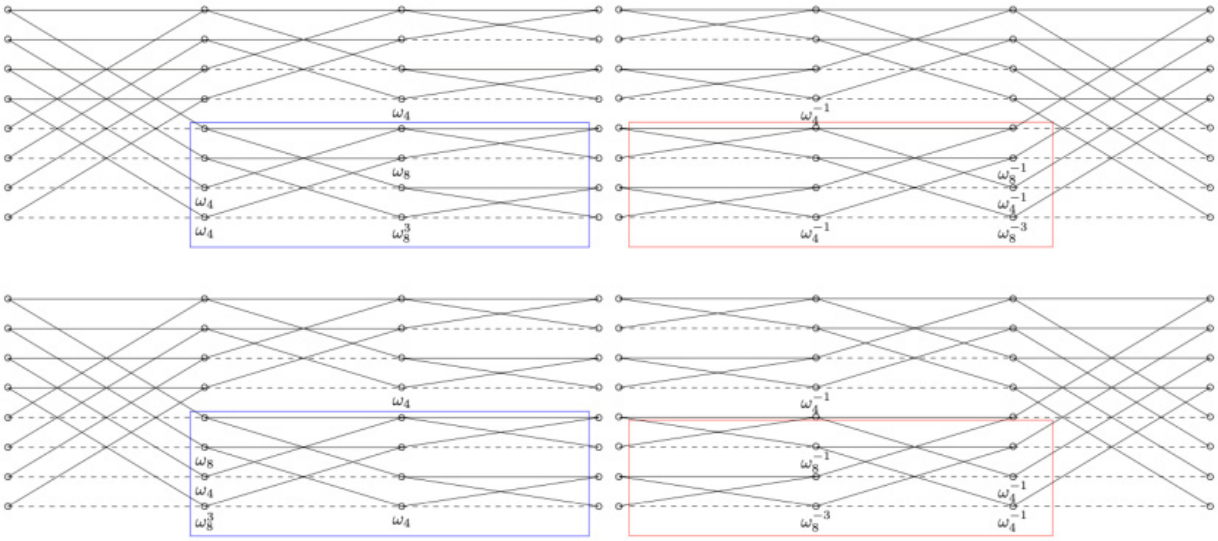
除了 Kyber，加解密的晶格密碼系統均被宣判出局，NIST 宣告兩個晶格體系的數位簽章系統 Dilithium 和 Falcon 都是新的標準 (Dilithium 是屬於和 Kyber 的同一派系支持的，但在很多性能考量上 Falcon 要更好)。另外基於雜湊函數的簽章 SPHINCS+ 也因為它廣被接受的安全性而被選為標準。資訊所的倪儒本老師是 SPHINCS+ 的共同提出者，我們也要恭喜他。

同時 NIST 另外開了一個給數位簽章的選拔，咸認他們心目中的目標是上個世紀發展出來的多變量系統 UOV。中研院團隊也將參與這個系統的投稿。他們也宣告幾個加解密系統 Classic McEliece, BIKE, HQC, 和 SIKE 繼續進行第四輪選拔。

實作和組合語言的重要性

雖然競賽暫時落幕，但是為了這個競賽所做的研究並不會消失。中研院在晶格密碼系統的計算上投注了大量的心血，主要在晶格密碼系統 Dilithium、Kyber、NTRU、NTRU Prime 和 SABER。我們並專注於這些密碼系統中最消耗時間的計算：多項式乘法和其變換。

C 語言是一個通用程式語言。因其精細的記憶體調控能力，資深程式設計師所寫的 C 程式通常被視為優化的實作。然而在密碼學實作



上，C 程式通常只被做為參考實作，而不論及效能和各平台的安全性。密碼學實作中，目標是寫出全世界最快的程式，記憶體配置只是其中一個影響因素。效能良好且安全的實作常常用到平台的特殊指令和組合語言。

在這幾年間，中研院開發出很多的手法來實作晶格密碼學，特別是在快速傅立葉變換 (Fast Fourier Transform, FFT) 和數論轉換 (Number Theoretic Transform 或 NTT, FFT 用在整數環的一種特化) 的實作技巧上堪稱獨步全球。上圖是其中之一，我們開發出來新版的蝴蝶變換 (butterfly) 用來加速晶格密碼學中最重要的 NTT。中研院也是最早提供形式驗證作用於快速晶格密碼學組合語言程式並證明為正確的出處。

將來與願景

不論最後結果這個世界是採用哪個或哪些系統，中研院的密碼學團隊希望提供給全世界快速、安全、正確、廣用的程式庫，同時也對後量子密碼系統的安全性做出更精確的評量。還請大家拭目以待。

首度揭開珊瑚共生菌聚合體神秘的「面紗」

微菌聚合體 (Microbial aggregates) 常出現在許多的動物、植物體內，這些聚合體對寄主多有著重要的共生和寄生等生態功能角色。雖然過去有零星報告曾發現珊瑚蟲體內有微菌聚合體，但是對於這些聚合體的生理、生化、形態、遺傳、生態功能等，學界幾乎是一無所知。本院生物多樣性研究中心湯森林老師團隊與 NanoSIMS 核心設施、應用科學研究中心陳壁彰老師、澳洲 James Cook 大學 Prof. David Bourne 等團隊合作，首度發現珊瑚微菌聚合體扮演珊瑚體內磷鹽循環角色，其研究成果於 2022 年 7 月發表於《科學前進》（*Science Advances*）。

論文網址：https://www.science.org/doi/10.1126/sciadv.abo2431