量子電腦和量子密碼學的趨勢與相關新創的發展方向

TAcc+ 新創分析團隊

量子運算 (Quantum computing) 技術的快速進展，將對現今使用的加密與解密系統帶來衝擊，解鈴還須繫鈴人，先進國家已展開次世代資安技術(「量子密碼學 (Quantum Cryptography)」)的研究與規格制定，後進者勢必要跟上，才能控制風險與掌握商機。

量子可以是光子、電子或離子，透過物理操作產生量子疊加和量子糾纏狀態，在這樣的特性下，單一量子須同時處於 2 種物理狀態，且 2 個量子間須形成聯結，即使不處於同一空間，仍可即時互相影響。科學家將此特性做為量子運算的基本單元，應用在電腦運算上，稱為量子位元（qubit）。量子運算在解特定種類的數學問題上具有強大能力，可輕易破解現今主流的加密演算法，例如質因數分解（RSA）等，將對高度數位化的全球政經環境帶來無可避免的衝擊與風險 — 根據 2019 年美國國家科學院出版社（National Academies Press）出版的《量子計算：進展與前景》一書提到，若要使用經典 Shor 算法有效破解 RSA1024，大概需要 2,300 量子位元；至於使用 Grover 算法破解 AES-GCM 則需 3,000 量子位元。

一、全球量子電腦發展趨勢

現今各先進國家紛紛加快投入量子資訊技術的研發，其中以歐盟、美國、中國、日本與韓國為相關技術專利申請量的領先者。龍頭科技公司如 IBM、Google、Microsoft、Intel、Amazon 等皆已投入多年並取得領先優勢，例如 2020 年 IBM 推出代號為 IBM Quantum Hummingbird 的 65 量子位元量子處理器，2021 年推出 127 量子位元的 IBM Eagle 處理器，已能用於改善傳統電腦無法精確可靠模擬量子電路的問題。2022 年，433 量子位元的 IBM Osprey 處理器問世，相較 Eagle 處理器性能提升十倍，開始能處理現今超級電腦無法解決的問題。2023 年繼續推出 1,121 量子位元的 Condor 量子運算處理器，並設定 2025 年推出 4,000 量子位元以上的處理器。除了不斷推升量子位元數外，業界目前也將重點放在量子的糾錯和容錯率的提升，此部分也會影響運算能力。IBM 也展示 Quantum System 2 模組化系統，能將多個量子處理器緊密連結，擴展量子運算可釋出的潛力規模，並於 2023 年底 IBM 量子高峰會上，推出以此系統為基礎，目前性能最高、錯誤率最低的 Heron 量子處理器。

中國大陸則透過整合產官學研機構能量進行發展，例如阿里巴巴集團 2023 年 11 月將旗下研究機構的量子運算實驗室與相關設備捐贈給浙江大學，百度集團也於 2024 年 1 月跟進捐贈旗下實驗室與設備給政府支持的研究機構。量子電腦主要研製機構中國科學技術大學也持續於 2020 年完成 76 光子的「九章」光量子計算原型機、2021 年研製 113 光子的「九章二號」、2023 年完成 255 光子的「九章三號」光量子計算原型機。

臺灣中央研究院於 2023 年 10 月開發出量子晶片，2024 年 1 月 29 日宣布完成首部自行研製的 5 位元超導全系統量子電腦，藉此建立量子電腦生態系發展平台，聚焦通用量子電腦硬體技術、光量子技術、量子軟體技術與應用開發、週邊關鍵零組件等，未來將朝向與高效能電腦緊密結合，提升整體運算效能。

量子科技的推動需要跨領域整合，相關知識涵蓋物理、化學、數學、資工、電機等，臺灣量子電腦協會理事長 張慶瑞教授 於 2023 年受訪時指出，量子科技的發展會逐步前進，從算力提升與穩定性上取得突破的『量子突破』階段，到能夠在處理現今超級電腦難以解決的特定複雜問題上取得全面性優勢的『量子優勢』階段，再進一步發展到如同現今的網路生態一樣，成為各行、各業、各學科底層環境的『量子生態』階段。張教授估計未來 5 至 6 年會解決部分『量子突破』問題，並逐漸由科研轉變成工程問題，距離實用化的腳步越來越近。自澳洲新南威爾斯大學（UNSW）成立世界第一所量子工程學系以來，歐洲、中國大陸、美國也陸續有大學院校成立相關系所，積極培育量子工程師。此外，美國也已經開始推動將量子科技的運作原理納入學齡前教育，做為常識教育，以利下個世代無縫接軌量子生態環境。

量子電腦雖擁有很快的特定運算速度，目前還有其限制，並不會取代傳統電腦，而是與傳統電腦互補使用。因應量子狀態極不穩定，現今開發的量子電腦都必須在絕對零度（-273℃）環境下運作，目前只適合以雲端作業方式執行特定運算，預計初期會用於藥物、氣象、材料、金融、人工智慧等研究與分析。

二、後量子密碼學發展現況

雖然以量子電腦目前的發展進程看來，短期內對現有密碼系統的衝擊不大，但真正的問題並不在此 — SHA-1 在 2005 年被發現有效攻擊方法後，一直延用到 2017 年才陸續被各大公司停止使用，美國國家標準暨技術研究院

（NIST）已於 2022 年宣布 2030 年後淘汰 SHA-1 加密演算法。如何能夠在指數成長的量子技術與各國網路軍備競賽中，及時制定、標準化及部署足夠抵擋量子衝擊的加密技術，是全世界需要共同面對的課題。

美國國家標準暨技術研究院於 2016 年啟動了後量子密碼學（Post-Quantum Cryptography, PQC）標準化流程，向世界公開徵求演算法，找出最不會被量子運算破解的演算法，替代現今的主流加密演算法，做為量子運算時代來臨時的通用加密演算法，並在 2020 年 7 月宣布了七個第三輪候選演算法，涵蓋在公鑰加密與金鑰建立（PKE/KEMs）與數位簽章兩項目。

在因應量子電腦破密的威脅上有 2 大路線，一是基於密碼學的後量子密碼學（PQC），另一則是基於量子技術的量子密鑰分發（Quantum Key Distribution，QKD）。美國國家安全局(NSA)公開表示，儘管 QKD 理論上無法破解且絕對安全，但目前 QKD 的技術限制，包括需要專用設備，以及需要增加基礎設施成本與內部威脅風險等，因此不建議使用 QKD。而在 PQC 標準化競賽晉級第三輪的 7 個候選團隊與 8 個備選團隊，總共 15 種演算法中，有 7 種屬於晶格演算法，不同於現行的 RSA 與橢圓曲線密碼系統，晶格演算法不是量子電腦擅長的難題，且產生的公私鑰、密文、數位簽章等長度僅為現行密碼系統的 10 倍左右，因此成為顯學。

2022 年 7 月 5 日，歷經三輪 6 年的選拔，美國國家標準暨技術研究院公布第一批入選的 4 款演算法，包括用於公鑰加密與金鑰建立的 CRYSTALS-Kyber 演算法，以及用於數位簽名的 CRYSTALS-Dilithium、FALCON、SPHINCS+ 三種演算法。同時 NIST 也公布公鑰加密與金鑰建立項目進入第四輪的候選演算法名單，設定第二批入選的演算法於 2024 年出爐並正式發布標準。NIST 解釋，為了符合實務上的需要，需要能為各種使用情境提供 2 個以上的演算法，避免單一演算法被找出漏洞，確保安全性。

上一次大規模更換加密演算法是在 2000 年左右，各大企業花了將近 10 年時間導入 AES 演算法，NIST 也呼籲所有組織提早開始準備導入即將發布的新演算法，並提供 6 項建議作法：找出組織中使用公鑰密碼的系統、測試新的密碼標準、制定轉換新加密標準的計畫、建立新的採購政策、組織內部 IT 部門與供應商準備應對方式、對員工進行培訓，相關商機也應運而生。

三、相關新創發展方向

根據顧問機構麥肯錫截至 2022 年的報告，美國、英國、加拿大為最多新創公司投入量子運算領域的國家。近年來，多家量子電腦新創獲得來自創投、政府投資，例如英國量子科技新創 Quantum Motion 於 2023 年最新一輪募資，獲得英國政府與創投公司合計投資 4,200 萬英鎊，加上過往累積募得約 2,400 萬美元，總計已募得約 22.7 億台幣。該公司將加速量子處理器的開發。同年還有法國新創 Pasqal 募得 1 億歐元、以色列新創 Quantum Machines 募得 B 輪 700 億美元、澳洲新創 Quantum Brilliance 募得 1,800 萬美元等。此外，科技大廠也積極從內部培育新創，例如 Google 母公司 Alphabet 於 2022 年將量子運算業務獨立為新創 Sandbox AQ，該公司 2023 年募得 5 億美元。由此可見量子科技領域在創投資本市場的火熱程度。

風險投資者的大量投資意味著看好量子科技的商業化腳步，例如法國量子科技新創 Quobly 成立於 2022 年，公司目標 2030 年前開發出世界第一台百萬量子位元的量子電腦，創辦人 Maud Vinet 指出，AI 模型底層的類神經網路，若以量子位元來運算，理論上可大幅節省用電。超微執行長蘇姿丰評估，生成式 AI 所帶動的運算需求快速成長，十年後運算 1 台超級電腦可能會消耗 1 座核電廠的電，由此可知，量子運算的潛在商機龐大。

臺灣在量子電腦的發展上雖與領先國家有所差距，在 PQC 與 QKD 的研究上則已取得一定成果。如何持續跟上先進國家的腳步，既是挑戰也是機會，國外已有將此技術應用於銀行業的案例，與此技術相關之商業化解決方案市場，也是臺灣資安新創可掌握的商機。在入選 PQC 決賽的團隊中，臺灣共有 4 位專家學者參與，且在此領域已深耕 20 年以上，與國外頂尖專家也長期合作，有望緊跟先進國家的步伐。

TAcc+計畫輔導之臺灣新創團隊中，也有投入 PQC 領域的資安新創「池安量子資安（Chelpis）」，該公司以量子密碼學為核心、零信任架構為基礎，提供企業級 Edge-to-Cloud 資安解決方案及產品，保護和強化 IT/OT 基礎設施和應用程序，開發出的基於認證授權的晶片，可應用於 IoT 端點安全。同時還推出端到端量子安全科技、雲端與端點的數據傳輸安全、後量子密碼技術及零知識證明等解決方案。

儘管目前 QKD 技術最大的瓶頸在如何於現有基礎架構上高速有效地分配光子，相關投入者仍在努力突破，例如加拿大新創公司 Quantropi 是世界上第

一個透過雲端平台與網路實現 QKD 技術，並證明此模式比現有的 QKD 系統快上十萬倍。Quantropi 的聯合創始人兼首席執行官 James Nguyen 表示：「我們的 QiSpace™ 軟件平台在本質上是 100% 演算法的，建立在用線性代數表示的量子力學基礎上，沒有光子意味着沒有光子速度或距離限制」。臺灣科技部從 2018 年開始，將量子技術列為優先補助的項目之一，並於 2019 年成功測試 25 公里室內光纖量子加密通訊和 4 公里的戶外光纖量子加密通訊，相關資安新創可留意技術發展與相關商業化解決方案商機。

為了迎接即將來臨的量子時代，臺灣政府也積極培養相關人才，聚焦「通用量子電腦硬體技術」、「光量子技術」、「量子軟體技術與應用開發」3 大領域，集結跨部會產、學、研團隊，投入資源與輔導，以期建構臺灣量子科技產業鏈。中央研究院院長廖俊智表示，儘管量子科技的門檻很高，臺灣仍必須跟上早期發展階段，透過聚焦、合作與整合等方式，實際了解量子科技發展過程中面臨的技術瓶頸與關鍵點，儘早體認臺灣產業能在那些環節扮演角色，成為量子科技供應鏈的重要參與者。

參考資料：

- "量子電腦為何比傳統電腦強大？量子運算的發展又有哪些挑戰呢？" 泛科學, 2018.
- "【臺灣資安大會直擊】為對抗量子電腦攻擊手法，後量子加密 PQC 演算法有望變成未來全球加密與數位簽章新標準," iThome, 2020.
- "資安關鍵字：網路加密技術｜量子加密通訊】抵抗量子電腦問世的威脅，以光子傳送密碼或金鑰," iThome, 2020.
- "從 4 大關鍵問題搞懂 PQC 與密碼學競賽," iThome, 2020.
- "是否有密碼之盾能夠擋住量子電腦之矛？後量子密碼學的前世今生——匯智安全科技陳君明董事長專訪," 泛科學, 2021.
- "量子電腦問世後的密碼學主力戰場「後量子加密技術」," 科技大觀園, 2021.
- "Google、IBM 都來競爭！英國實驗室突破量子電腦新成就，將比超級電腦更厲害？" 數位時代, 2022.
- "量子國家隊成軍，17 項團隊底定，聚焦未來量子世代臺灣產業鏈,"

iThome, 2022.

- "首批 NIST 認可的 PQC 演算法出爐，美 CISA 建議即刻做好六大準備," iThome, 2022.
- "量子運算能夠協助未來 AI 系統的安全性，讓 AI 演算法運用在更多方面," iKnow 科技產業資訊室, 2023.
- "IBM 聲稱量子電腦大突破，且進入實用階段，兩年後有機會打敗傳統超級電腦," iKnow 科技產業資訊室, 2023.
- "IBM 推出新量子運算晶片和處理器　探索科學新領域," 科技島, 2023.
- "Google 展示量子霸權：僅幾秒完成的任務最強超級電腦要花 47 年," 鉅亨網, 2023.
- "臺灣資安產業開始推動 PQC 遷徙，池安成立量子安全遷移中心," iThome, 2023.
- "中研院研發 5 位元量子電腦 年底推出 / 台灣首次自製量子晶片 將放到雲端提供學術研究單位試用," 自由時報, 2023.
- "矽谷科學家：量子電腦有望實現通用人工智慧," 中央通訊社, 2023.
- "重要趨勢！量子跟你想的不一樣！量子電腦將掀起超級運算大革命！將如何引領科技發展？ft.台灣量子電腦協會理事長 張慶瑞教授！" 曲博科技教室, 2023.
- "新一代 IBM 量子處理器「蒼鷺」Heron 與 IBM Quantum System Two 亮相," IBM, 2023.
- "「量子日」最快明年降臨？量子運算恐顛覆全球軍經安全," 聯合新聞網, 2024.
- "Quantropi 使用現有網絡基礎設施展示量子熵的量子安全分布," 頭條匯, 2024.
- "台灣自製超導量子電腦 成少數完成研發國家," 中央通訊社, 2024.
- "連台積都只看 5 年內技術　一家法國量子新創，給台灣電子業的警示," 天下雜誌, 2024.