前瞻科技與管理　9 卷 1/2 期，1-3 頁（2019 年 11 月）
Journal of Advanced Technology and Management Vol. 9, No. 1/2, pp. 1-3 (November, 2019)
DOI:10.6193/JATM.201911_9(1_2).0001

量子計算與量子通訊

管希聖 *

國立臺灣大學物理學系教授
《前瞻科技與管理》期刊編輯委員

量子電腦與傳統電腦是截然不同的運作原理，量子電腦提供巨大的量子平行性，進而具有解決現今功能強大的超級電腦難以處理或不能解決之問題的潛力，例如：量子計算對於現行的網際網路密碼系統之安全性產生了巨大威脅。因為量子技術的重要性與其可能對社會及產業帶來的巨大衝擊，促使各國政府甚至民間資訊大廠近來大量投入量子資訊及相關量子技術的研發。就在不久前，量子電腦還普遍只被視為是未來可能的技術，但在 IBM, Google, Intel 等科技巨擘努力下，近年來有顯著的進展。例如：2016 年 5 月，IBM 開放配備有超導 5 個量子位元處理器的量子電腦作為量子體驗（Quantum Experience）的服務使用，讓所有有興趣的人士皆可通過 IBM Cloud 雲端登入免費在 IBM 量子處理器上進行實驗或量子計算。2017 年 5 月 IBM 宣布已成功構建並測試了一個具有 16 個量子位元的升級處理器也讓用戶免費使用。在 2017 年 11 月，20 個量子位元的機器問世，IBM 也正式啟動收費的商業運轉模式，讓用戶通過 IBM Cloud 的更準確量子處理器來探索量子計算。IBM 在 2019 年 9 月 18 日宣布，在一個月內，IBM 的商用量子處理器將增長到 14 個系統，其中包含最新的 53 個量子位元處理器的量子電腦，這是迄今為止公開宣稱最大的通用量子電腦系統（Nay, 2019）。另外，據 2019 年 9 月的網路媒體報導，Google 和 National Aeronautics and Space Administration（NASA）合作，使用 53 個量子位元的量子電腦完成一項鑑定一個隨機數產生器是不是真的隨機的運算，總共用 3 分 20 秒，然而全球最強大的超級電腦 Summit 對量子電路的一個實例取樣 100 萬次，則需要花一萬年處理（Murgia and Waters, 2019）。如果該項報導正確，則這是第一次有人證明，量子電腦的性能真的能超過傳統電腦，也就是實現

* 通訊作者：管希聖
電子郵件：goan@phys.ntu.edu.tw

RECAST　Ainosco Press

了「量子霸權」，或量子優勢（Supremacy），是個了不起的成就。而此量子霸權的實現，也揭示了量子電腦強大的原因。由於量子力學中，多量子位元系統的可能狀態數是隨系統的量子位元數 n 成指數增長，也就是 2^n。因此只需 53 個量子位元就可以模擬 $2^{53} \sim 9 \times 10^{15}$ 種狀態，而這個數字的狀態數已經超出了當今超級電腦的運算能力。因此在過去的四年中，量子電腦處理器的量子位元數隨時間增長，由 5 個量子位元、16 個量子位元、20 個量子位元到今年 53 個量子位元的量子電腦處理器的問世運轉（Nay, 2019），以及超越當今傳統計算系統的計算能力展現後（Murgia and Waters, 2019），量子電腦已變成將是在可見的未來就極有可能實現的技術產品。

若未來量子邏輯閘運算錯誤率能顯著改善，且量子位元數能增加到 $10^6 \sim 10^8$ 個，則有希望建構一部能夠實現擁有錯誤更正能力的量子電腦，使量子運算具有容錯計算（Fault-Tolerant Quantum Computation）的能力，提升其穩定的運算效能。到那時量子電腦就能夠從事較為複雜且需要時間較長的計算。例如：量子電腦在數十分鐘或幾小時之內就能破解原本幾萬年才能破解的非對稱性或公鑰（Public Key）編碼方式的密碼。因此如何確保在量子電腦時代來臨時，仍能保有安全秘密的通訊是非常重要的課題。雖然，量子電腦與量子計算對於現行的密碼系統之安全性產生了威脅，但同時，基於量子的特性，量子力學也提供了一套絕對安全的（Unconditionally Secure）量子通訊機制：量子金鑰分發（Quantum Key Distribution, QKD）。另外後量子密碼學（Post-Quantum Cryptography），也稱為量子抗性密碼學（Quantum-Rresistant Cryptography）也被提出，其目標是開發對量子電腦和傳統電腦均安全的密碼系統，並且可以與現有的通信協議和網路進行相互操作。《前瞻科技與管理》期刊在本期所刊登的兩篇與量子技術相關的文章即是探討並深入說明此兩種在量子電腦時代來臨亦能解決安全通訊問題的有前景方法。

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST），於是在 2016 年舉辦一場設計、分析和選擇一套新的公鑰密碼演算法的後量子密碼學競賽，即使構建了量子電腦，這些新演算法也沒有對應的量子演算法可以將他們破解。NIST 自 2016 年 4 月開始接受提案，並於 2017 年 11 月停止接受新演算法進入 NIST 的第一個評估階段，進行審議。NIST 宣布，該競賽於 2019 年 1 月 30 日進入第二輪競賽，最初的 69 項申請中有 26 個演算法通過了所謂的「半決賽」（Computer Security Resource Center, 2019）。NIST 預計下一階段的評估將花費 12 ~ 18 個月，此後可能會進行第三輪評估，然後將採用官方標準演算法。

QKD 研究上，最近也有新的進展。Twin-Field QKD 在 2018 年被提出是目前能夠在沒有量子中繼器（Quantum Repeater）下，超越在標準光纖典型 100 ~ 200 公里的傳輸距離而達到更長距離的最新量子金鑰分發協定提案（Lucamarini, Yuan, Dynes, and Shields, 2018）。最近在 2019 年 9 月發表的兩項 Twin-Field QKD 的獨立實驗展示了打破適用於標準 QKD 之基本的速率—距離限制，證明了 Twin-Field QKD 的實用性，是一種在遠距離上執行量子密碼學的有前景的方法（Liu et al., 2019; Zhong, Hu, Curty, Qian, and Lo, 2019）。

量子計算與量子通訊無疑是本世紀最熱門、最具潛力和前瞻性的研究領域與技術。這些量子技術將非常可能要從根本上改變我們的生活、社會和經濟。相關單位應積極規劃和投入該尖端、新穎量子科技的研發和相關技術人才的培育，做好迎向第二次量子革命以及未來新

的量子科技與量子產業發展的準備。

參考文獻

Computer Security Resource Center, 2019/9/23, "Post-Quantum Cryptography Standardization," *National Institute of Standards and Technology*, https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization (accessed September 23, 2019).

Liu Y., Yu Z.-W., Zhang W., Guan J.-Y., Chen J.-P., Zhang C., Hu X.-L., Li H., Jiang C., Lin J., Chen T.-Y., You L., Wang Z., Wang X.-B., Zhang Q., and Pan J.-W., 2019, "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," *Physical Review Letters*, 123(10), 100505. doi:10.1103/PhysRevLett.123.100505

Lucamarini M., Yuan Z. L., Dynes J. F., and Shields A. J., 2018, "Overcoming the Rate Distance Limit of Quantum Key Distribution without Quantum Repeaters," *Nature*, 557, 400-403. doi:10.1038/s41586-018-0066-6

Murgia M., and Waters R., 2019/9/21, "Google Claims to Have Reached Quantum Supremacy," *Financial Times*, https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17 (accessed September 23, 2019).

Nay C., 2019/9/18, "IBM Opens Quantum Computation Center in New York; Brings World's Largest Fleet of Quantum Computing Systems Online, Unveils New 53-Qubit Quantum System for Broad Use," *IBM News Room*, https://newsroom.ibm.com/2019-09-18-IBM-Opens-Quantum-Computation-Center-in-New-York-Brings-Worlds-Largest-Fleet-of-Quantum-Computing-Systems-Online-Unveils-New-53-Qubit-Quantum-System-for-Broad-Use (accessed September 20, 2019).

Zhong X., Hu J., Curty M., Qian L., and Lo H.-K., 2019, "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution," *Physical Review Letters*, 123(10), 100506. doi:10.1103/PhysRevLett.123.100506