全球量子加密通訊發展現況與趨勢

台灣亞太產業分析專業協進會 99 年認證產業分析師 魏伊伶

根據國際研究機構 MarketAndMarkets 研究顯示，全球量子加密通訊設備與軟體產值將從 2017 年 2.857 億美金以 27%年複合成長率快速擴大為 2022 年的 9.437 億美金，目前量子密鑰產生器、量子密鑰收發設備已有商用化產品。驅動量子加密通訊市場發展的主要因素，包含數位化時代下頻傳的資安攻擊事件、各國持續提高的資安技術投資以及在雲端與物聯網世代下，對於新興資安技術架構的需求也不斷增長。此外，新興無線通訊技術(如 5G)的商用化，預期也將帶動量子加密通訊需求的增加。

一、國際電信營運商積極布局量子加密通訊

韓國電信商 SK Telecom 在 2018 年 2 月耗資 6,500 萬美金買入瑞士量子新創廠商 ID Quantique 超過 50%股權，為 5G 安全通訊解決方案鋪路，同時整合 Nokia 的高安全性光傳輸系統，成功在 SK Telecom 的網路上完成互通測試。

SK Telecom 在 2019 年 4 月正式在首爾及六個都會區開始正式運行 5G 商用化服務，並逐步拓展其 5G 服務到約 85 個城市。著眼於 5G 網路對於穩定與安全的重要性，因此花費 6 年的時間與 ID Quantique 研發出全球最小型的量子隨機變數晶片，也進一步擴大在 ID Quantique 持股來提高其 5G 網路安全性。初步預計將在首爾安山地區佈建其量子加密網路。

除了 SK Telecom 外，歐洲電信營運商 Telefónica 也與華為、馬德里理工大學合作，建構第一個在商用光纖網路上應用的量子加密通訊，在光纖網路整合上也應用了 SDN (Software Defined Networking)技術來協助。尤其量子加密通訊技術必須架構在高品質的光纖網路上才能運作，過去 Telefónica 只成功與馬德里理工大學在單一都會區範圍內完成量子加密通訊的實驗，但這次與華為成功在商用光纖網路上佈建且展示，顯示其商用可行性。

英國電信營運商 British Telecom 也獲得政府投資的 200 萬英鎊建構量子加密試行網路的佈建，採用 Toshiba 的量子加密通訊原型系統進行量子加密通訊的實驗，透過架構在現有的光纖網路上運作，BT 僅成功在其伊普斯維奇實驗室到劍橋大學間建構了一個量子加密網路。並於 2019 年初開始將量子加密技術導入到衛星上，期望透過低軌道衛星從地面接收密鑰後，透過衛星繞行地球的模式攜帶且傳遞密鑰，但整體來看，傳輸距離的限制仍是目前量子加密通訊的技術瓶頸。

整體來看，國際電信營運商目前在 5G 網路的佈局上，開始因應全球對資訊傳輸安全性的需求，陸續佈局與投資量子加密通訊技術，也透過與廠商的合作進行測試驗證，而隨著 5G 網路在全球的陸續商用化，預期也將帶動量子加密通訊的需求興起。

二、新興量子加密通訊廠商

量子加密通訊市場相關解決方案包含了量子密鑰傳輸系統、連續變數密鑰設備與軟體、密鑰分發與管理軟體等，相關廠商除了軟硬體系統供應商、量子加密通訊整合廠商外，也包含量子通訊關鍵元件廠商及量子加密通訊諮詢服務商。

整體來說量子加密通訊產業鏈已初具雛形，主要廠商除瑞士 ID Quantique 外，美國 MagiQ technologies、 Nucrypt、Qubitekk；德國 Infineon Technologies、Qutools；英國 Crypta Labs、 PQ Solutions 與澳洲 QuintenssenceLabs 皆是目前量子通訊設備主要供應商。其中更陸續有新創廠商持續投入

(一) QEYnet-以微衛星為基礎的量子加密通訊網路

QEYnet 是在 2016 年由一群太空工程師與量子通訊專家所共同成立的新創公司，公司主要的目標是建構一個低成本、以微衛星為基礎的全球量子加密通訊網路。主要原理就是期望透過衛星來協助遞送量子密鑰。

以 A 與 B 進行量子加密通訊為例，QEYnet 的解決方案透過衛星經過 A 方時，透過交換光子來產生密鑰 a；而當衛星通過 B 時，也會在利用交換光子的做法來產生密鑰 b。之後再利

用密鑰 b 將密鑰 a 加密後，回傳給 B，而 B 就可計算 A 的密鑰且建立與 A 之間的共有的密鑰。因此整體解決方案主要是先透過衛星傳送密鑰而非所有資料都透過衛星傳送，一旦 A 與 B 兩方產生共有的密鑰後，則會透過現有的網際網路來互傳資訊。

(二) Qubitekk-專注提供物聯網的量子加密通訊技術

Qubitekk 是一家 2012 年創立的加州新創公司，主要提供商用化的工業控制系統互連量子加密技術，目前主要以能源網路的安全解決方案為公司發展主力，包含電網、石油與瓦斯等產業的資訊傳輸等。目前 Qubitekk 也與加州的四家主要能源廠商合作進行量子加密技術測試。

Qubitekk 的解決方案主要是應用產生糾纏的光子來防止資訊被竄改，透過產生糾纏的光子，加密的密鑰與認證碼就可利用現有未經保護的網路進行光子的傳輸，以達到資料安全傳輸的效果。

三、結論-量子加密通訊可望帶動光學元件需求

從產業發展現況來看，量子加密通訊技術的原理主要是透過光子的傳輸來達到資料安全傳輸的效果，使得光源相關元件成為量子加密通訊中的技術布局重點。目前國際廠商在切入量子加密通訊時，仍以軟硬兼備的策略投入技術研發，但從產業發展現況來看，已經可看到有新創廠商透過單獨切入關鍵元件的方式來切入，可見量子加密通訊元件有機會獨立開發，對於我國具備非線性光學、雷射等基礎技術能量的廠商來說，為有機會切入之方向。

以量子加密通訊架構來看，目前量子光學元件可切入的設備主要為量子密鑰產生器(連續變數產生)、量子密鑰收發設備以及量子中繼傳輸設備。其中量子密鑰產生器主要任務為透過連續變數技術產生密鑰，因此需要可處理連續變數的量子加密晶片以及密鑰分發軟體技術。而在量子密鑰收發設備部分，首先光源會涉及雷射光學頭與非線性晶體的開發，而光的衰減則需要倚靠光學調變器或單光子晶片，最後則是在光子的生成到傳輸與接收為能維持穩定，則需要光學低溫恆溫器來提供穩定的環境。最後在量子中繼傳輸設備部分，目前須考量如何延續或強化光子的狀態，因此除了光學低溫恆溫器外，非線性晶體的技術可能也是重點。

量子加密通訊元件因技術門檻高與元件精準度要求高，使得元件價格動輒數十萬元，對於未來量子加密通訊之商用化發展或是整合 5G 網路應用來說都可能成為障礙。尤其是在量子加密通訊設備中，應用雷射等可調式光源、光學調變器、非線性晶體等元件，為深具光學基礎之我國產業可望投入發展方向。然量子設備對元件技術要求高，對過去著重大體積、大面積光學技術之我國廠商來說，要切入量子通訊用的光學元件，重點在小型化、精準化，包含光源的調整如何精準衰減到僅剩個位數的光子，以及光子傳輸過程中的穩定性都將是技術瓶頸。此外量子加密通訊目前從產業需求來看，能否發展出具規模的量產市場仍有變數，建議有意投入高利潤利基市場之光學廠商可優先思考投入之可能。

(本文作者為工研院產科國際所執行產業技術基磐研究與知識服務計畫產業分析師)

原文出處：ITIS 智網 http://www.itis.org.tw/