



量子科技專利趨勢分析——量子通訊與後量子密碼

陳繹安^{*}、廖家興^{**}

壹、前言

貳、量子通訊

一、量子通訊技術概述與分類

二、量子通訊專利趨勢分析

參、後量子密碼

一、後量子密碼技術概述與分類

二、後量子密碼專利趨勢分析

肆、結語

* 作者現為經濟部智慧財產局專利三組專利助理審查官。

** 作者現為經濟部智慧財產局專利二組專利助理審查官。

本文相關論述僅為一般研究探討，不代表任職單位之意見。

摘要

隨著量子電腦近年來的快速發展，其強大的計算能力以及獨特的運算方式使得現今通用的密碼技術不再足以保護通訊安全。面對量子電腦所帶來的威脅，現有的兩種可行解決方案，其一係以量子密鑰分發為主的量子通訊相關技術，另一者為將加密系統改良汰換之後量子密碼學。本文中對此二技術主題進行技術介紹及專利趨勢分析，藉由專利申請趨勢分析了解各別技術主題當前的國際技術發展態勢以及研發重心，作為我國未來在此二通訊重點科技領域研發布局的參考依據。

關鍵字：量子密碼學、量子通訊、量子密鑰分發、後量子密碼學、量子對抗

quantum cryptography、quantum communication、quantum key distribution、post-quantum cryptography、quantum-proof、quantum-safe、quantum-resistant

壹、前言

在現今蓬勃發展的通訊產業中，為了確保傳輸訊息與資料的安全性，加密通訊系統主要以對稱式及非對稱式加密等二種加密方式實現通訊安全。隨著量子電腦近年來的快速發展，其強大的計算能力以及獨特的運算方式使得現今通用的密碼技術不再足以保護通訊安全。具體而言，量子電腦所使用的秀爾演算法（Shor's Algorithm），可有效計算質因數分解、離散對數以及橢圓曲線離散對數等傳統上不具有快速破解方法的困難問題，因此前述這些經典密碼學所廣泛使用的非對稱式金鑰加密演算法，如 RSA（Rivest-Shamir-Adleman）演算法、迪菲－赫爾曼演算法（Diffie-Hellman Algorithm）以及橢圓曲線加密法（Elliptic Curve Encryption）皆已不再安全。

研究顯示，具有 2,330 個量子位元的量子電腦足以破解 128 位元安全等級的橢圓曲線加密法，而具有 4,098 個量子位元的量子電腦亦可以破解 2,048 個位元金鑰長度的 RSA 演算法¹。除了非對稱加密方式遭受到破解的風險外，對稱式加密的安全性亦受到量子電腦的影響。現今常用的對稱式加密演算法 AES（Advanced Encryption Standard）在面對量子電腦時，其安全性等級比量子電腦出現前所認定的安全性降低一個等級²，故在當今通訊應用空前發達的時代，如何在量子電腦快速發展的過程中，持續維持既有通訊的安全性，即成為一個重要的課題。

面對量子電腦的威脅，為了維持現有通訊的安全性，在訊息加密的方式上有兩種可行的解決方法，其一是利用量子力學的基本物理特性達到安全通訊的目的，例如以量子密鑰分發（Quantum Key Distribution）為主的量子通訊（Quantum Communication）相關技術，另一種方式則是開發使量子電腦亦無法有效破解的數學難題作為密碼基礎，此類方法則是後量子密碼學（Post-Quantum Cryptography），後量子密碼學早期亦被稱為量子對抗技術（Quantum Resistant）。

¹ Martin Roetteler et al., Quantum resource estimates for computing elliptic curve discrete logarithms, arXiv:1706.06752 (2017).

² Daniel J. Bernstein, Grover vs. McEliece, PQCrypto 2010: Post-Quantum Cryptography, International Workshop on Post-Quantum Cryptography, page 73-80 (2010).

最早提出以量子通訊作為保障通訊安全之技術係可追溯自 1984 年，Bennett 和 Brassard 兩位物理學家首先提出了利用量子力學來安全傳輸密鑰的方式，其想法是藉由傳輸一次性使用的密鑰，使通訊雙方擁有相同的密鑰，以保障加密通訊的安全性，使得訊息及密鑰在傳輸時處於安全的狀態，該想法亦開啟了量子通訊中量子密鑰分發技術的大門。

後量子密碼學則是屬於整個現代密碼學技術進程中的一部分，其專指於量子電腦尚無法有效破解的密碼系統。歷來密碼系統的研發過程中，數學家會以各式各樣的數學難題作為核心基礎來設計各種不同的加密系統，而在這些加密系統中，若其核心的數學難題在現代以量子電腦來進行破解時仍未有快速有效的破解方法者，即可被歸類於後量子密碼的技術類別。最早的後量子密碼系統為編碼密碼系統，其與現今廣泛利用的 RSA 加密系統均係於 1978 年所研發，該技術領域經歷了約半個世紀的發展，迄今已有 5 種具代表性可對抗量子計算的密碼系統。

在通訊相關的量子科技議題中，目前的量子通訊及後量子密碼學技術均圍繞於如何處理量子計算時代下所產生的訊息傳輸安全問題，本文中以量子科技時代下用以加強通訊安全的新技術為主軸，分別對量子通訊以及後量子密碼學二技術領域進行技術介紹及專利趨勢分析，以期藉由專利申請趨勢，了解此二技術領域的主要技術發展方向及各國技術研發重心。本文中的專利趨勢分析係使用 Derwent Innovation 專利資料庫檢索 2020 年 12 月 31 日前公開的全世界專利資料，以各領域的關鍵字及 IPC 分類號進行檢索後，再以人工方式逐篇閱讀專利摘要，以選出與技術主題相關的案件進行分析，資料總數包含量子通訊技術 3,000 餘件以及後量子密碼學技術 500 餘件（相同的 INPADOC 專利家族計為 1 件³）。本文中的專利分析圖表除了受理專利申請之主要專利局／專利組織的分析圖以外，均以同專利家族的案件計為 1 件進行統計分析，以避免因同一專利跨國申請而造成數據失真，並使研究數據更加貼近於實際發明的數量，而於受理專利申請之主要專利局／專利組織分析中則係統計個別專利局／專利組織實際的申請數進行分析，未排除相同專利家族之重複申請案件。

³ INPADOC (International Patent Documentation) 專利家族為歐洲專利局所創建之專利資料庫，其包含專利資料的法律狀態以及優先權關聯性所形成之資料集合。

貳、量子通訊

一、量子通訊技術概述與分類

在通訊技術的發展歷史中，為了使訊息能夠在傳輸過程中維持其秘密性，通訊雙方可以使用事先約定好且具有秘密性的加解密規則來傳輸訊息密文，以確保在傳輸過程中，不會被不知其加解密規則的任意第三方破譯。然而，在現今的遠距離通訊環境中，如何讓素未謀面的通訊雙方安全的共享一用於加解密之共同密鑰（秘密的加解密規則），一直都是長期存在的重要課題。為了解決上述問題，當前普遍使用的方法是以公眾皆知的數學上困難問題，將該密鑰進行加密後再做單向傳輸（以非對稱式加密系統傳輸共同密鑰），藉此讓通訊雙方建立起安全的共享密鑰。然而，在面對量子計算所使用的演算法時，現今常使用的數學困難問題已不再足以保障其加密時的安全性。

量子通訊的技術係以量子狀態來進行訊號傳輸，與傳統的傳輸訊號技術相比，量子狀態在受到任何觀測時會使該狀態產生資訊缺失或是資訊錯誤，因此通訊雙方可以藉由傳輸者與接收者雙方量子狀態的校對，觀察量子狀態是否在傳輸過程中有第三方介入觀測的痕跡。

量子通訊的技術分類如表 1 及圖 1 所示，此技術分類係參考實際專利資料的技術內容所整理創設。在一階技術中，量子通訊的技術分類包含量子密鑰分發（Quantum Key Distribution, QKD）、量子安全直接通訊（Quantum Secure Direct Communication, QSDC）以及量子通訊網路建設，此外，現有的量子通訊網路建設技術特別著重於量子密鑰分發網路（Quantum Key Distribution Networks, QKDNs）之技術。

量子密鑰分發是現在量子通訊技術領域的主要應用方式，此技術可在通訊雙方間建立具有竊聽偵測能力的通訊管道，其二階技術包含協議設計以及實體元件設計，分別對應於通訊時所使用的通訊規則以及實現此通訊架構所必須的硬體、軟體元件。協議設計的三階技術係以不同的通訊規則和編碼方式作為技術區隔，例如以光偏振方向進行訊號編碼的離散變量（Discrete Variable）協議或以光相位進行編碼的分布式相位（Differential Phase Shift）協議等，這些協議係將其傳輸的

訊號寫入於傳輸光（傳輸介質）的不同性質之上，進而建立出不同的訊號寫入、讀取、校驗等通訊協議（通訊規則）。

量子安全直接通訊是利用量子糾纏（Quantum Entanglement）物理特性，發展出量子遙傳（Quantum Teleportation）的傳輸技術，以進行遠距離訊息傳輸。其與量子密鑰分發同樣都是以量子狀態傳輸訊號，此二技術的主要差異在於量子安全直接通訊所傳輸的資訊為訊息本身，而量子密鑰分發所傳輸的資訊為密鑰，該密鑰僅係作為對後續的訊息加解密處理使用。

表 1 量子通訊技術分類表⁴

一階技術	二階技術	三階技術
量子密鑰分發	協議設計	離散變量
		分布式相位
		連續變量
		量子糾纏應用
	實體元件設計	編碼／調製電路
		密鑰蒸餾（密鑰提取）
		量子隨機產生器
量子安全直接通訊		
量子通訊網路建設	接取連結及管理	
	密鑰管理	
	安全認證	

量子通訊網路建設⁵則是著重於量子通訊網路的建置。在量子通訊的架構底下，如何維持長距離的訊號正確性係為量子通訊技術領域的一大挑戰，而網路建設的技術即係探討如何設立訊號傳輸中繼站（傳輸節點），以支撐龐大的長距離通訊需求。因此，在量子通訊網路建設的技術中，其包括有通訊節點間的接取連結及管理、通訊過程密鑰管理及通訊安全認證這三種二階技術，用以提高長距離傳輸訊號的正確性，在使用者眾多通訊網路環境下實現量子訊號的傳輸。

⁴ 本文之圖表均為自行研究整理繪製而成。

⁵ ITU-T, Overview on networks supporting quantum key distribution, ITU publication, Y.3800(2019.10).

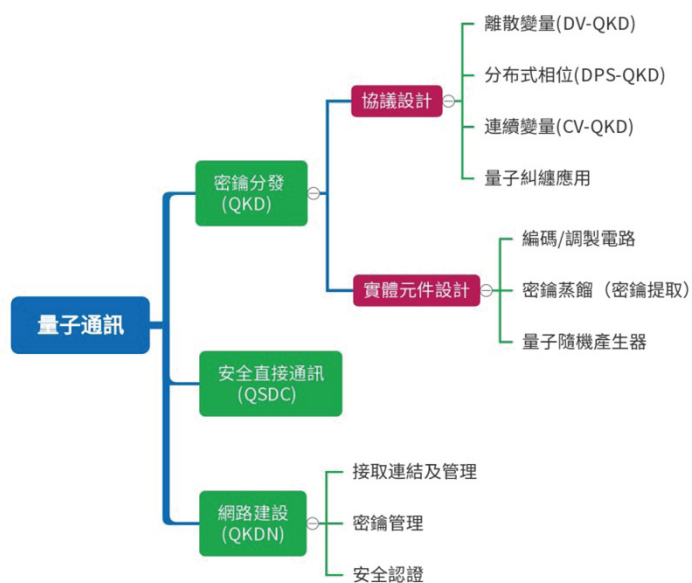


圖 1 量子通訊技術分類樹狀圖

二、量子通訊專利趨勢分析

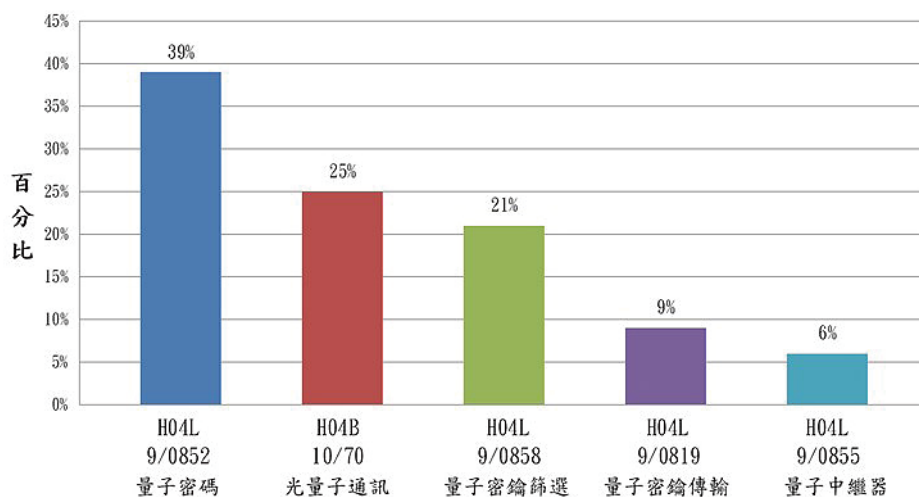


圖 2 量子通訊 CPC 分類號長條圖

量子通訊 CPC 分類號分析結果如圖 2 所示。量子通訊技術 CPC 分類中，占比最高的分類號為 H04L9/0852（量子密碼），占 39%；次高為 H04B10/70（光量子通訊），占 25%；第三高為 H04L9/0858（量子密鑰篩選或編碼的細節），占 21%；第四高為 H04L9/0819（量子密鑰傳輸或分發），占 9%。從 CPC 分類的專利數量比例中可看出，量子通訊技術的研發著重於傳輸過程中，如何利用量子密鑰分發技術確保密鑰分配的安全性、穩定性，俾強化現有通訊過程如何在未來量子技術革新中確保穩定安全的資料傳輸。

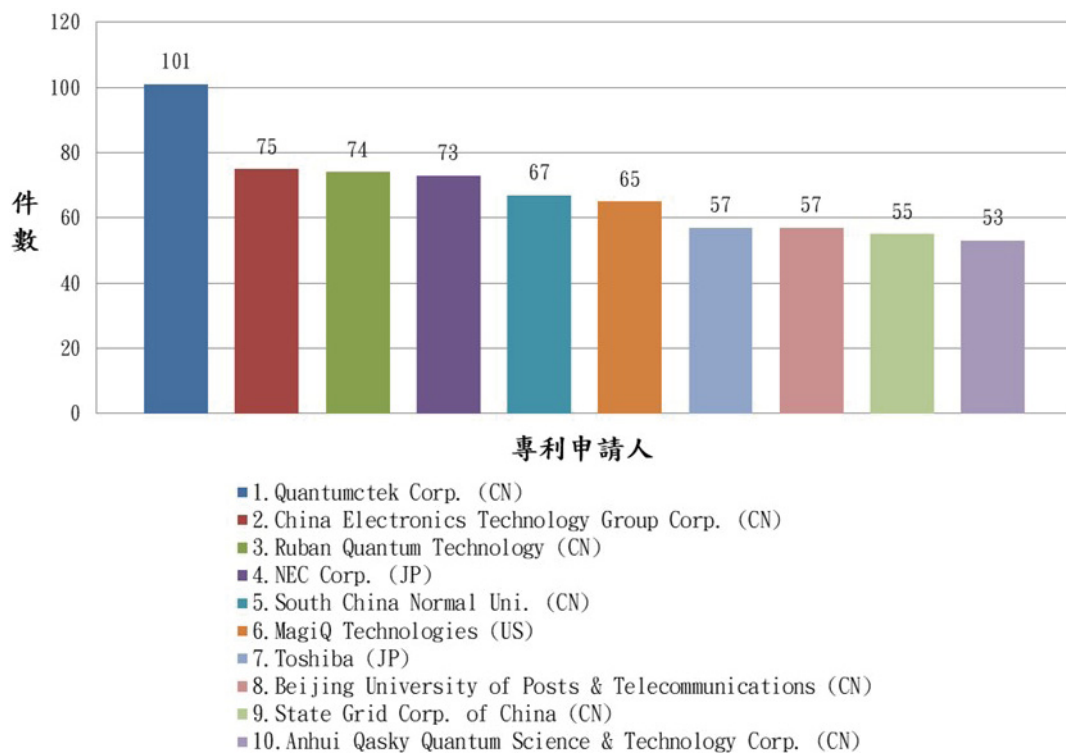


圖 3 量子通訊前十大專利申請人

圖 3 為量子通訊技術的專利申請人分析。在前十大專利申請人中，專利數量最多者為科大國盾量子技術股份有限公司（Quantumctek Corp.）、第二為中國大陸電子科技集團（China Electronics Technology Group Corp.）、第三為如般量子科技股份有限公司（Ruban Quantum Technology），前三大專利申請人均為中國大陸公司；其後依序為日本電氣株式會社（NEC Corp.）、華南師範大學（South

China Normal Uni.)、MAGIQ 技術公司 (MagiQ Technologies)、東芝株式會社 (Toshiba)、北京郵電大學 (Beijing University of Posts & Telecommunications)、國家電網公司 (State Grid Corp. of China)、安徽問天量子科技股份有限公司 (Anhui Qasky Quantum Science & Technology Corp.)。在十大專利申請人中，有 7 位專利申請人為中國大陸公司或學研單位，2 位專利申請人為日本公司，1 位為美國公司，可大致看出中國大陸在此領域的鑽研程度遠遠領先於世界各國，而日本及美國亦有維持一定水準的技術投入。依專利申請人的產學研性質分析，十大專利申請人中除第五及第八位專利申請人為學研單位以外，其餘的 8 位專利申請人均為公司，可見得量子通訊技術具有相當程度的商用價值以及被實踐利用的可能性。

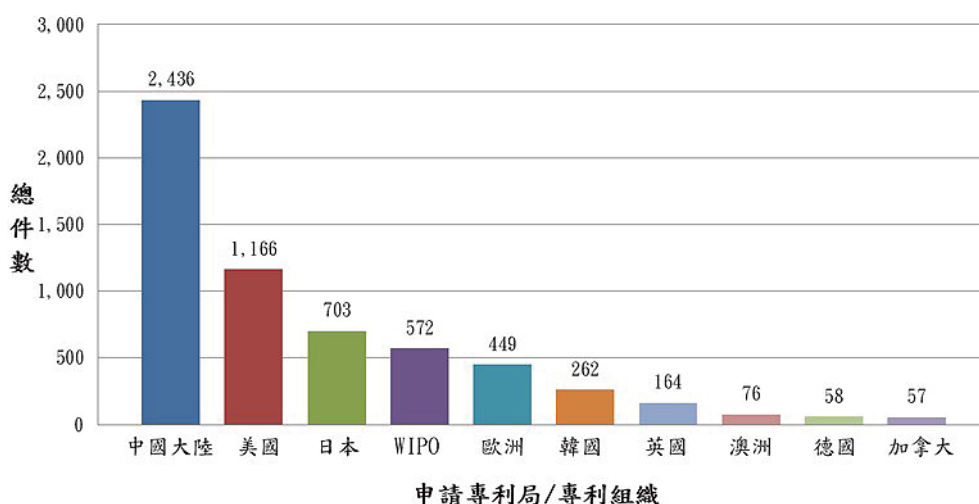


圖 4 受理量子通訊專利申請之前十大專利局／專利組織

圖 4 為受理量子通訊專利申請之前十大專利局／專利組織。在十大申請國家／地區中，最重要的前三個申請國家分別為中國大陸、美國以及日本，其中中國大陸的總申請數量超過其後的美國 2 倍，可見主要的專利申請國家亦集中於中國大陸。排序在第四至第十的國家／地區依序為：世界智慧財產權組織 (WIPO)、歐洲、韓國、英國、澳洲、德國、加拿大。與圖 3 的分析結果做比較，除在專利申請人本國申請外，申請國家／地區的選擇主要涉及到專利布局申請策略，在具有重要市場地位的國家申請專利以搶占商業先機係其首要目標。

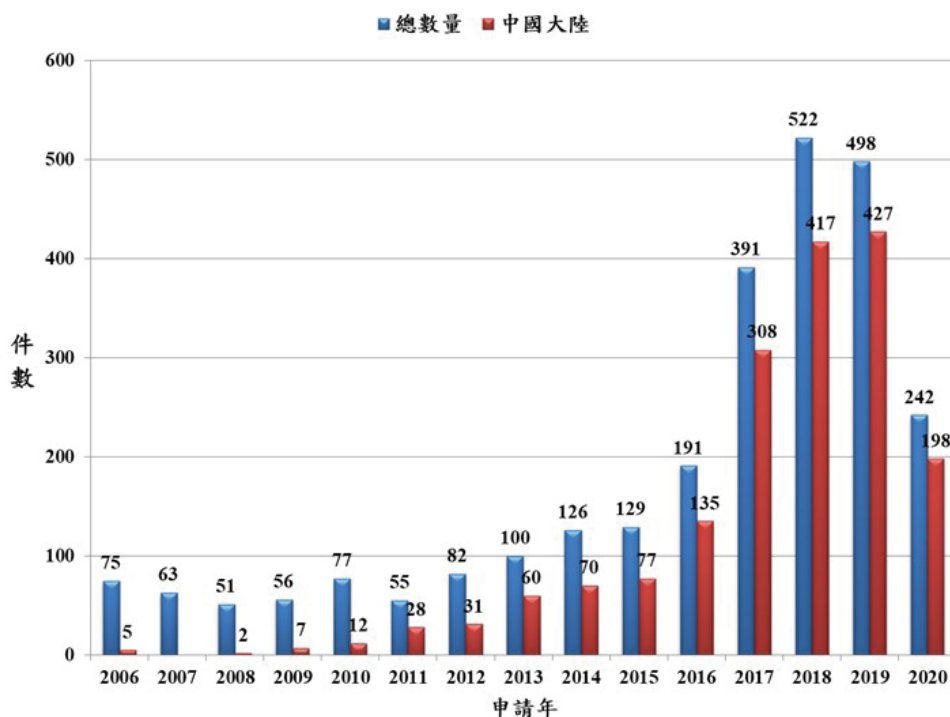
圖 5 量子通訊專利申請趨勢⁶

圖 5 為量子通訊 2006~2020 年的專利申請趨勢。由圖 5 中可知，中國大陸在量子通訊技術領域的起步雖較其他國家晚，但觀察整體專利數量所占比例，可發現中國大陸是近年來該技術領域中專利申請數量呈現跳躍式增長的主要推手，而自 2017 至 2020 年，中國大陸的專利申請數量占總數量的比例更是來到 8 成左右。

中國大陸近年來在政策上高度重視量子通訊的技術發展，其不斷以國家政策及研究計畫等方式組成國家隊，持續擴大投入研發並促進技術產業化。在量子通訊技術發展競賽中，中國大陸有望在未來全球市場中，成為此技術領域中的主導國家，並進一步主導量子通訊技術標準化的流程。中國大陸的技術投入及發展里程碑簡述如下⁷：

⁶ 本報告蒐集 2020 年 12 月 31 日前公開之全世界專利資料，因專利有 18 個月早期公開的規定（自申請日或是最早優先權日起算），致使 2020 年申請之專利數量未完整反應於統計資料中，導致統計數量下降。

⁷ 中國量子通信發展的十個「瞬間」，搜狐新聞網，https://www.sohu.com/a/474984029_348129（最後瀏覽日：2021 年 12 月 7 日）。

- (一) 2008 年誘騙態量子密鑰分發進入實際應用階段⁸。
- (二) 2013 年城市規模的量子通訊網路建成⁹。
- (三) 2013 年啟動世界首條千公里級量子保密通訊幹線——「京滬幹線」技術驗證及應用示範專案，並於 2017 年 9 月底正式開通¹⁰。
- (四) 2016 年量子科學實驗衛星「墨子號」發射升空，2017 年 9 月「墨子號」與正式開通的量子保密通訊「京滬幹線」成功對接，實現了洲際量子保密通訊，全球第一個星地一體化的廣域量子通訊網路初具雛形。2018 年，基於墨子號和「京滬幹線」的成績，中國大陸國家發展和改革委員會啟動了「國家廣域量子保密通訊骨幹網路建設」，列入「新一代資訊基礎設施建設工程」支援專案¹¹。
- (五) 量子通訊國內外標準逐步建立，其中 2019 年，國際電信聯盟 (ITU) 設立「面向網路的量子資訊技術焦點組 (FG-QIT4N)」，這是國際標準組織中第一個量子資訊技術焦點組¹²，由國科量子、國盾量子、中國信通院、三大運營商、華為、中興、中國信科等中國大陸團隊發起設立。
- (六) 2019 年，中國科大團隊及其合作者研製出連續變數量子密鑰分發晶片，大大縮小了量子通訊硬體的體積，為量子通訊技術的普及提供了新思路¹³。
- (七) 2020 年，中國科大團隊利用「墨子號」量子科學實驗衛星在國際上第一次實現千公里級基於糾纏的量子密鑰分發¹⁴。

⁸ Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, 94 Phys. Rev. Lett., 230503 (2005).

⁹ Chen T Y et al., Field test of a practical secure communication network with decoy-state quantum cryptography, 17 Opt Express, 6540–6549 (2009).

¹⁰ 許琦敏，「京滬幹線」構建量子保密通信網絡雛形，中國科學院，https://www.cas.cn/cm/202101/t20210107_4773810.shtml（最後瀏覽日：2022 年 1 月 21 日）。

¹¹ 同註 7。

¹² Telecommunication Standardization Sector, Focus Group on Quantum Information Technology for Networks, International Telecommunication Union, <https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx> (last visited Jan. 21, 2022).

¹³ G. Zhang et al., An integrated silicon photonic chip platform for continuous-variable quantum key distribution, 13 Nature Photonics, 839–842 (2019).

¹⁴ Yu-Ao Chen et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, 589 Nature volume, 214–219 (2021).

圖 6 為量子通訊申請人國籍排名。如前所述，中國大陸的申請人所占專利數量，不僅在總申請量的占比上明顯高於其他各國，在各階技術分類中也全部高居第一位，遙遙領先其他國家。由此可見，中國大陸在量子通訊技術領域的領先優勢係全面性的涵蓋整體技術發展。其他各國的技術投入情形，在各個技術分類中，第二、第三大申請人係以日本、美國為主，二者的專利數量所差無幾；而歐盟和韓國除在連續變量量子密鑰分發（CV-QKD）以及量子通訊網路安全認證等技術分類有較多申請量外，其餘的技術分類中大致係排名第四及第五位。

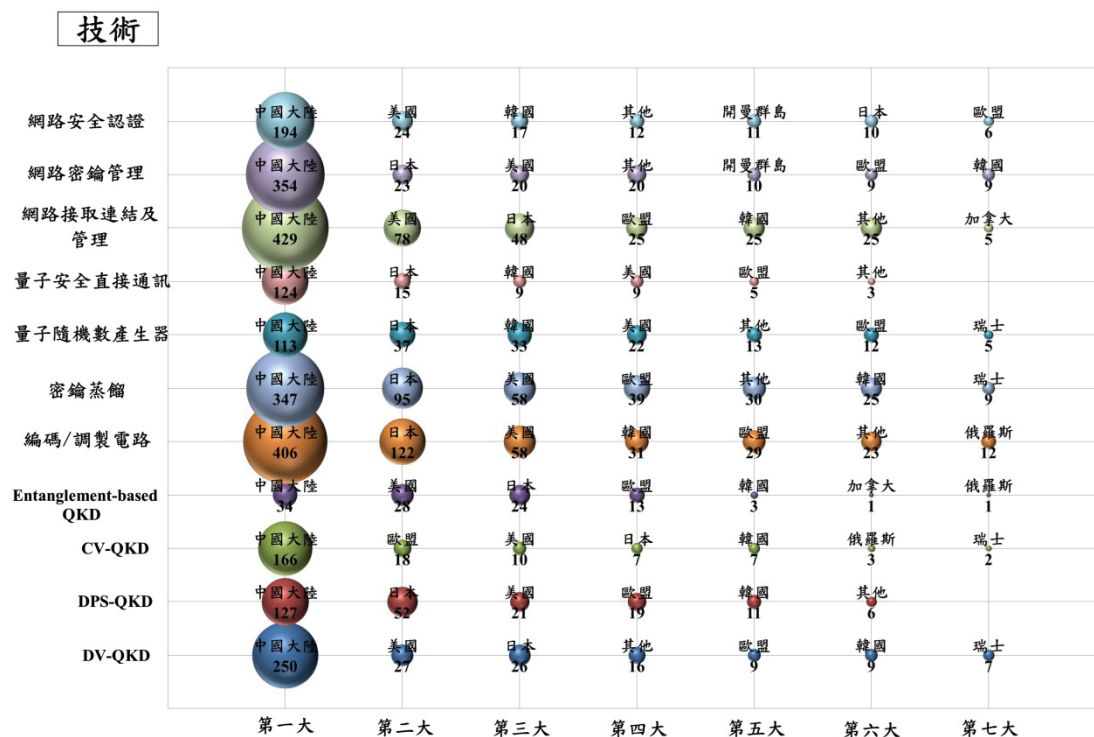


圖 6 量子通訊申請人國籍排名

自 1984 年 Bennett 和 Brassard 提出 BB84 的量子密鑰分發方案以來，關於量子密鑰分發技術的各種理論方案日臻完善，其技術實現日趨成熟，亦使得量子密鑰分發相關的量子通訊技術逐漸走向實際應用。然而儘管理想的量子密鑰分發技術具有絕對的安全性，並可偵測竊聽者，但在實際應用中，裝置元件在工作效能上之固有缺陷仍會對通訊系統的安全性帶來潛在威脅。圖 7 為量子通訊的技術功效矩陣，從圖中可以發現，量子通訊系統功效上的主要發展方向著重於提高保密

性、增加穩定性、提升效能以及降低錯誤率，這顯示了目前的量子通訊技術仍須加強其通訊穩定、安全的基本功能，此技術尚無法支撐現今多樣化、大傳輸量的通訊應用需求。

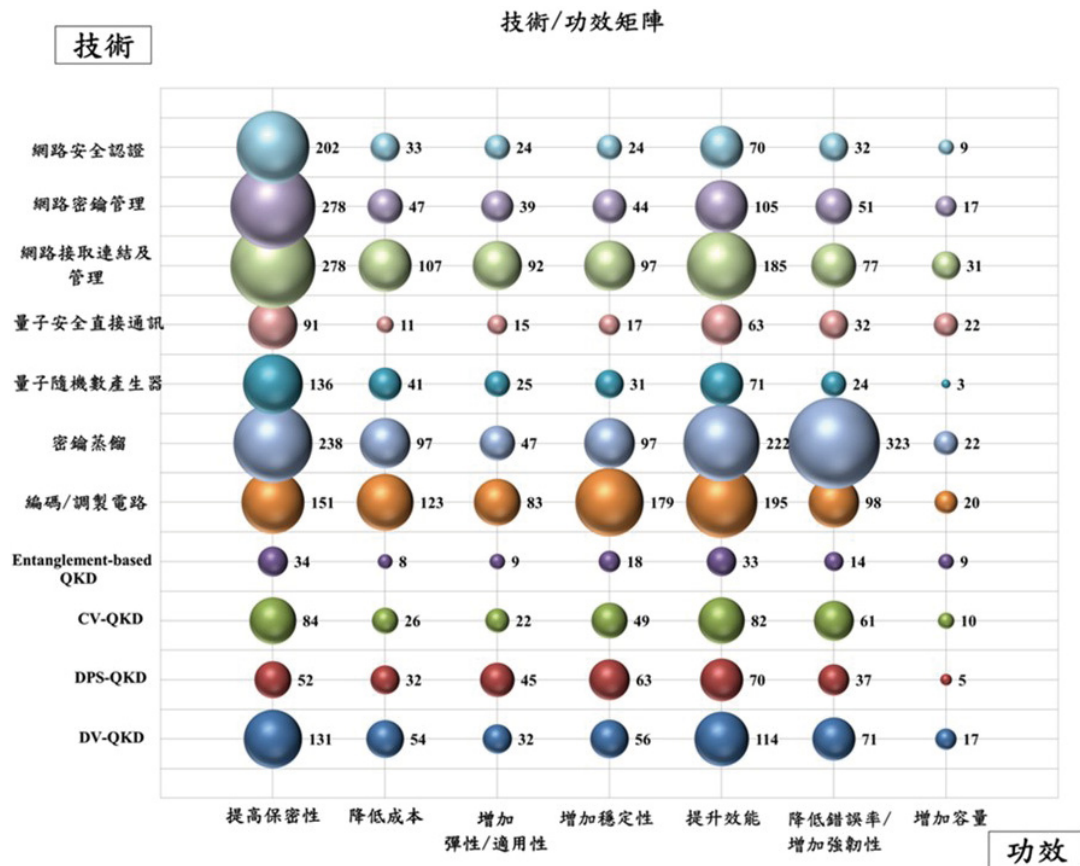


圖 7 量子通訊技術功效矩陣

參、後量子密碼



如前言所述，為因應量子電腦可能破解經典密碼學的威脅，主要有二種應對方法。第一種應對方法量子通訊技術如第貳章中所介紹，雖具有良好對抗量子電腦之效果，然由於其通訊設備需要專用化的設計改良，目前該技術的實際應用仍處於開發階段，尚無法即刻廣泛使用，並完全取代經典密碼學所扮演的角色。第二種應對方法則是開發具有可對抗量子計算能力的新加密技術，藉由研究量子電腦亦無法快速破解的新的數學上困難問題，以其作為核心發展新的加密技術，藉此研究出不會被量子計算輕易破解的加密系統，由於此類加密系統具有對抗量子計算的能力，故這類型的密碼學系統被稱之為後量子密碼系統。

後量子密碼系統並非現今才發展出的密碼系統，其是從密碼學發展歷史中所出現的眾多密碼系統中，挑選具有對抗量子計算潛力的密碼系統後所生成的多個密碼體系。如圖 8 所示，最早出現的後量子密碼系統為發表於 1978 年的編碼密碼系統¹⁵，其與現今廣泛使用的 RSA 密碼系統出現時間相近；而後於 1996~1999

¹⁵ Robert J. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, 42-44 DSN Progress Report, 114-116 (1978).

年間、2011 年間，其餘四個後量子密碼系統的體系逐漸成形，分別為網格密碼系統¹⁶（Lattice-based cryptography，又稱為晶格密碼系統）、多變量密碼系統¹⁷（Multivariate cryptography）、雜湊密碼系統¹⁸（Hash-based cryptography）及超奇異橢圓曲線同源密碼系統¹⁹（Supersingular elliptic curve isogeny cryptography），上述的這五種密碼系統即為當今後量子密碼領域最具代表性的 5 種後量子密碼系統。

隨著量子計算的快速發展，通訊安全受到的威脅日益逼近，通訊領域的專家們早已意識到，終有一日，現有的密碼系統將無法維持所須的通訊安全水準。早在 2006 年 5 月，探討後量子密碼學的第一屆後量子密碼學年度會議 PQCrypto 就已在比利時召開²⁰，顯見密碼學潛藏的危機在量子電腦尚未能夠被實踐的年代就已逐漸受到矚目。近年來，可取代經典密碼學的後量子密碼學體系已漸趨成熟，美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）於 2016 年時開啟「後量子密碼學標準化競賽」，藉由這個競賽，NIST 希望可以選出適合作為新時代標準的後量子密碼加密系統，為未來通訊設備全面性的密碼系統更新打下重要基石。後量子密碼競賽進行至今已進入第三輪的決選選拔階段，在這段過程中參賽的演算法數量由 82 個被篩選至 15 個，在 2020 年所公布的決選名單中，包含了 7 個勝部演算法，以及 8 個備選演算法。經過了漫長的選拔競賽，預計將於近年內，選出最後勝出的後量子密碼演算法，並以其作為基礎開始進行後量子密碼的標準制定²¹。

¹⁶ Miklós Ajtai, Generating Hard Instances of Lattice Problems, Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Special Interest Group on Algorithms & Computation Theory, page 99–108 (1996).

¹⁷ Aviad Kipnis et al., Unbalanced Oil and Vinegar Signature Schemes, Advances in Cryptology — EUROCRYPT '99, International Association for Cryptologic Research, page 206–222 (1999).

¹⁸ Johannes Buchmann et al., XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions, PQCrypto 2011: Post-Quantum Cryptography, International Workshop on Post-Quantum Cryptography, page 117–129 (2011).

¹⁹ Luca De Feo et al., Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, PQCrypto 2011: Post-Quantum Cryptography, International Workshop on Post-Quantum Cryptography, page 19–34 (2011).

²⁰ Daniel J. Bernstein, Conference, Post-quantum cryptography, <https://pqcrypto.org/conferences.html> (last visited Jan. 21, 2022).

²¹ Computer Security Resource Center, Post-Quantum Cryptography Standardization, NIST, <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization> (last visited Jan. 21, 2022).

一、後量子密碼技術概述與分類

在後量子密碼學領域中，進入 NIST 後量子密碼系統競賽決選名單的最後 15 個（7 個勝部、8 個備選）演算法，分別涵蓋了前述的 5 種主要後量子密碼系統。其中，7 個勝部密碼演算法分別為 5 個網格密碼演算法、1 個多變量密碼演算法以及 1 個編碼密碼演算法，而在備選的 8 個演算法中則包含有雜湊密碼以及超奇異橢圓曲線同源密碼的演算法。

前述 5 種主要後量子密碼系統，分別係以不同的數學問題和技巧作為核心所設計，其技術簡介分述如下：

- （一）編碼密碼系統：編碼密碼系統的原理係將錯誤訊息加入至明文訊息中以形成密文，而解密時則藉由所設計的糾錯碼，將該錯誤訊息修正後還原出明文訊息。
- （二）網格密碼系統：網格密碼系統的設計是利用「以多重維度的大向量基底所建構的網格空間中，其距離原點最近的網格點無法輕易求得」之數學問題作為此密碼系統的核心。
- （三）多變量密碼系統：多變量密碼系統係以多變量二階方程式組作為核心困難問題，藉由仿射函數將原始的多變量二階方程式組進行變換隱藏使其多變量方程式組的反函數不易被反向破解。
- （四）雜湊密碼系統：雜湊密碼系統以複數組一次性公鑰為基底，利用雜湊函數建立起與該些一次性公鑰相對應的雜湊樹（Merkle tree），其藉由雜湊函數只能單向計算的特性，串聯起雜湊樹中各個節點間的整體關聯性，使雜湊樹具有驗證個別一次性公鑰是否可信的功能。
- （五）超奇異橢圓曲線同源密碼系統：超奇異橢圓曲線同源密碼系統係經典密碼學中橢圓曲線密碼系統的進階版。橢圓曲線密碼以離散點群集合所組成的橢圓曲線為基礎，利用映射規則建立起無法輕易反向推導的加密系統；而超奇異橢圓曲線則是將橢圓曲線設定為具有特定條件的橢圓曲線，以加強密碼系統的安全性。

除了前述 5 種主流密碼技術外，在專利的技術分布中，另外包含有一類較為特殊的加密技術，係占了較高比例的專利申請數量，於本文中概稱此類技術為「實體密鑰池」。實體密鑰池技術係將所有成員的公共密鑰限制儲存於實體媒介中，而於訊息傳輸時僅傳輸實體媒介中的公鑰存取地址，而未於頻道中傳輸公鑰，由於公鑰並未被傳輸，故第三方無法藉由竊聽的方式獲取公鑰，也就無法利用公鑰推算出私鑰並破譯密文。此技術之安全機制雖非建立在數學難題上，與其他後量子密碼系統之機制大相逕庭，然而此技術架構確實同樣具有對抗量子計算的能力。

本文中專利分析之技術分類，係依據各專利所屬技術類別歸納整理而成，經觀察編碼密碼系統的專利件數相當稀少，不具有代表性，故不列入本文專利分析的技術分類中。因此，本文中後量子密碼學的專利分析技術分類係以網格密碼系統、多變量密碼系統、雜湊密碼系統、實體密鑰池以及超奇異橢圓曲線同源密碼系統等 5 類技術為主，其技術分類樹狀圖如圖 9 所示。



圖 9 後量子密碼技術分類樹狀圖

二、後量子密碼專利趨勢分析

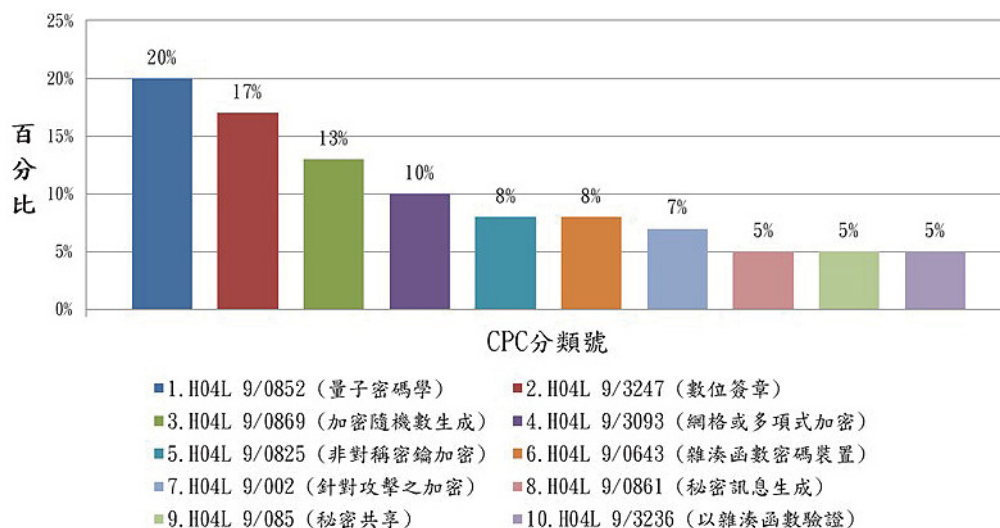


圖 10 後量子密碼 CPC 分類號長條圖

後量子密碼學屬於通訊領域中的訊息加密技術，其主要四階 IPC 分類號為 H04L 9/00。在圖 10 的 CPC 分類中可看出，此技術領域中主要的四階 CPC 分類號亦為 H04L 9/00（訊息的傳輸：用於保密或安全通訊的加密機制或加密裝置），其中，占比最高的分類號為 H04L 9/0852（密鑰分配管理：量子密碼學），占比為 20%；次高的為 H04L 9/3247（用於驗證系統用戶的身分或憑證的裝置：數位簽章），占比為 17%；第三高的為 H04L 9/0869（密鑰分配管理：加密隨機數生成），占比為 13%；第四高的為 H04L 9/3093（公鑰加密系統：網格或多項式加密），占比為 10%。整體而言，後量子密碼學的專利著重於密碼系統的發展，密鑰分配管理（H04L 9/08）以及公鑰加密系統（H04L 9/30）是目前技術發展的重心。

在圖 11 的十大專利申請人中，中國大陸的專利申請人有 7 位、美國 2 位、日本 1 位。專利申請人中專利數最高的為如般量子科技公司（Ruban Quantum Technology）申請了 121 件，其專利數遠大於其他專利申請人，其後依序為索尼公司（SONY Corp.）、英特爾公司（Intel Corp.）、華南理工大學（South China Uni.）、深圳職業技術學院（Shenzhen Polytechnic）、西安理工大學（Xi'an University of

Technology)、廣東技術師範大學(Guangdong Polytechnic Normal Uni.)、西安電子科技大學(Xidian University)、國際商用機器公司(IBM Corp.)、武漢大學(Wuhan University)。其中,前三大專利申請人均為公司,而其餘的專利申請人中有6位中國大陸專利申請人為學研單位,整體而言仍以學研單位為主要專利申請者,可見目前產業界參與投入在後量子密碼領域研發的公司數以及專利數均較少。

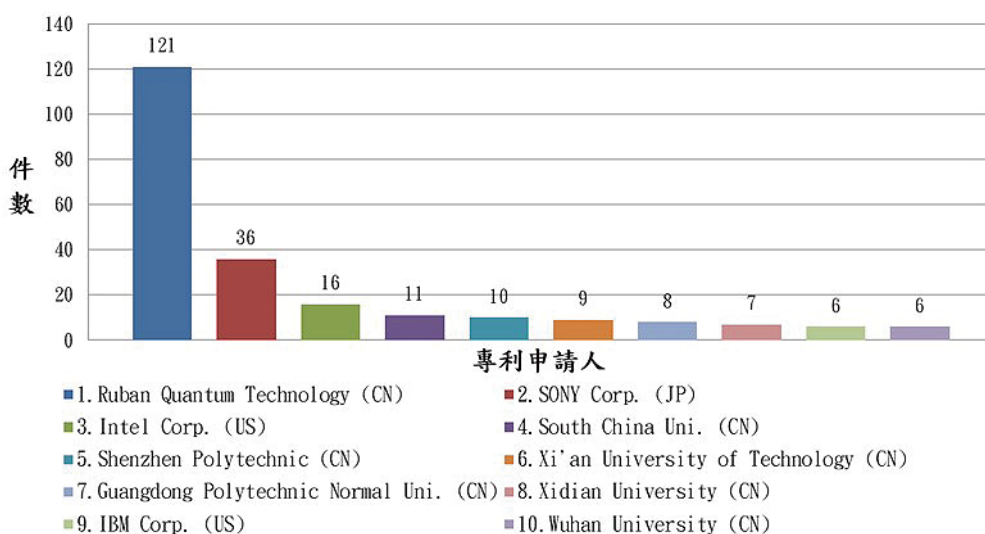


圖 11 後量子密碼前十大專利申請人

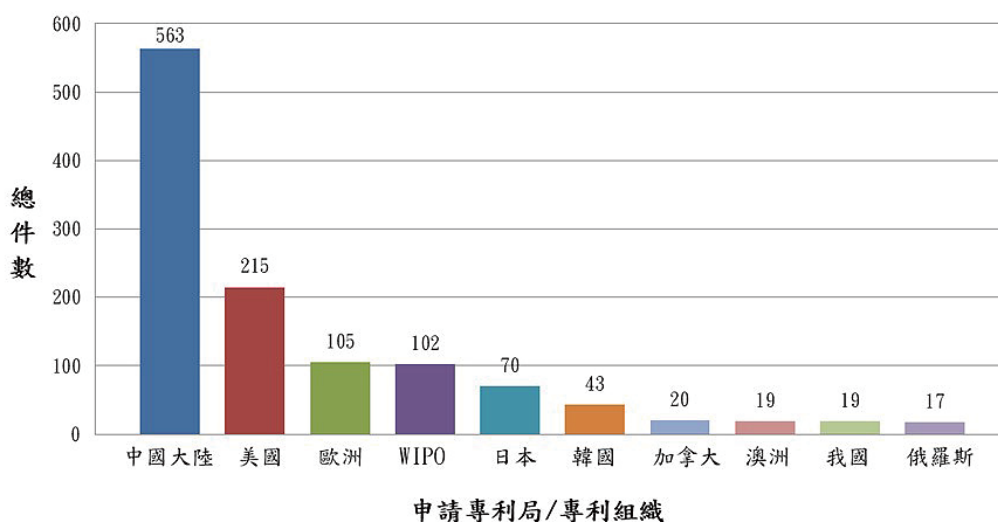


圖 12 受理後量子密碼學專利申請之前十大專利局/專利組織

圖 12 為受理後量子密碼學專利申請之前十大專利局／專利組織，此處的統計以專利申請總件數統計，以使數據可反映真實申請案在各國家／地區的申請數量。後量子密碼學專利申請的數量由中國大陸位居第一，總件數高達 563 件，約占該領域總申請件數的一半，其後為美國（215 件）、歐洲（105 件）、WIPO（102 件）、日本（70 件）、韓國（43 件）、加拿大（20 件）、澳洲（19 件）、我國（19 件）、俄羅斯（17 件）。我國的總申請件數為 19 件排在第 9 位，以我國申請案進行申請人分析後發現，該些我國專利主要由日本的索尼公司申請，此外另有少數我國學研單位零星的專利申請案。

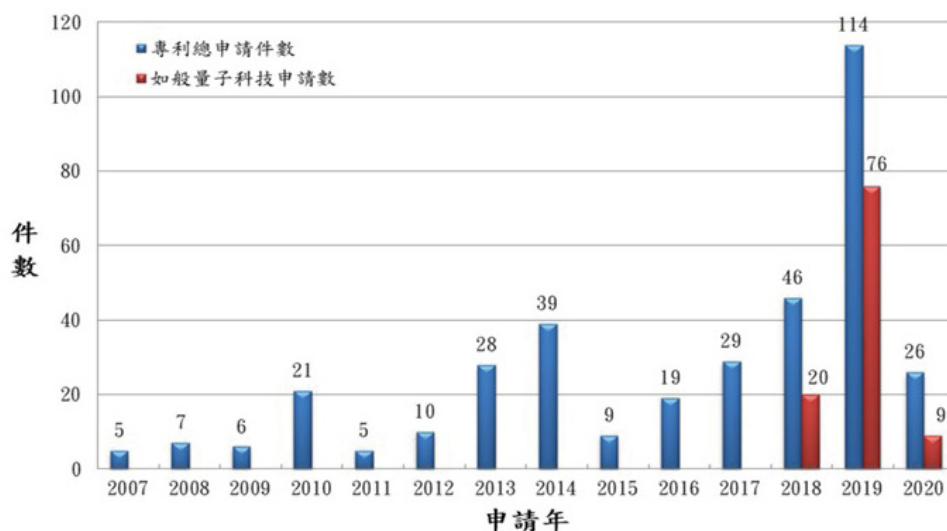


圖 13 後量子密碼專利申請趨勢分析²²

圖 13 為後量子密碼專利申請趨勢分析，圖中藍色為後量子密碼學各技術分類加總的件數統計，紅色為如般量子科技公司的申請件數。從圖中可以看出此領域的專利申請案件數量在 2007~2017 年間無明顯趨勢，而在 2018~2019 年有較高數量的專利申請案，惟若扣除僅在此段期間大量申請的如般量子科技公司專利件數（圖中以紅色標示），可發現在這段期間專利數量仍無太大的波動。

²² 2020 年數量下降之原因同註 5。

綜上而論，依圖 11~12 的申請人／申請地區分析可知，中國大陸在此技術領域的發展，不論是專利申請數量亦或是專利申請人數，均領先於世界各國。就產業面而言，產業界僅有少數幾間公司較集中的申請後量子密碼專利，而十大專利申請人中第四至十位平均持有件數係小於 10 件，顯示出此領域專利持有分散且主要申請人為學研單位居多。以圖 11~13 的專利分析整體來看，後量子密碼學技術的商業化熱潮尚未開始，僅有少數個別公司開始進入此領域進行技術開發，並未成為整體產業的向上發展趨勢。

後量子密碼學的發展進程早在 1980 年代即已開始發展，然而當時量子電腦的發展尚未達到可實作的程度，由於後量子密碼學與 RSA、ECC 等傳統密碼技術相比在使用效能上較為劣勢，故一直以來密碼學領域的應用仍以經典密碼技術為主，後量子密碼學則較偏向於單純的學術研究。近年來，因應量子電腦的快速發展，現有的密碼系統的安全性能已漸漸不敷使用，後量子密碼系統的採用成為一種必然的趨勢。然而，由於密碼系統牽涉的應用範圍非常廣泛，縱使現有密碼系統已有全面更換的必要，若要將現有公鑰加密系統全面汰換仍是一項艱鉅的工程。以 2000 年美國汰換 AES 加密系統為例，當時的各行各業僅將部分加密系統更新就花了近十年的時間。為了降低密碼系統汰換的影響層面及成本，係可考慮設定不同安全等級，漸進式的將密碼系統汰換，即可同時確保高安全等級的資料傳輸安全性並降低系統更替的影響範圍，在通訊安全與成本考量之間取得平衡²³。綜上所述併同圖 11~13 的專利分析結果，可以看出現今的後量子密碼技術在通訊安全領域中，雖由於其發展實施的必要性而受到許多關注，然而在考量加密系統標準尚未成形，以及研發汰換加密系統的成本過高之二前提下，實際投入此領域研究的企業仍然較少，其後續發展熱潮尚有待於標準確立之後，再依實際應用所須進行針對性的開發研究。

圖 14 為後量子密碼學技術分類之申請趨勢圖。各技術類別以總量而言最高者為多變量密碼學，其專利申請件數於 2013 年至 2020 年間保持穩定且相較其餘技術類別更多。實體密鑰池的類別在總數量上僅次於多變量密碼學，可看出於 2018

²³ 姚荏富，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，<https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=f9093947-6062-46d4-858a-3d16824edc95>（最後瀏覽日：2021 年 12 月 7 日）。

至 2020 年間係其集中申請的時點。實際分析專利案件後發現，實體密鑰池的專利數量雖為主要技術之一，然其專利均為中國大陸之如般量子科技公司所申請，且實體密鑰池的技術有別於其他的後量子密碼學演算法，其密碼的安全性係藉由實體的儲存媒體來實現，與一般密碼學技術的設計概念不同，是後量子密碼學中較為特殊的一種技術類別，其技術發展是否將普及化仍有待觀察。網格密碼學的專利數量雖排行第三，然其一直是在學研界中最受關注的後量子密碼學系統，且網格密碼學在實務上已經研發出許多種完整的實施型態，諸如 NTRU、基於 LWE 或 RLWE 等基礎所建立的個別密碼系統皆已受到廣泛的利用開發，相對來說其技術發展程度已較為完整成熟。雜湊密碼學及超奇異橢圓曲線同源密碼學的專利數量較少，其雖持續有零星申請案件分布於 2008~2020 年間，然因此二者為較新穎的後量子密碼系統，使得投入該些技術類別研發的專利數量也較其餘技術類別少，其技術發展趨勢尚待後續觀察。

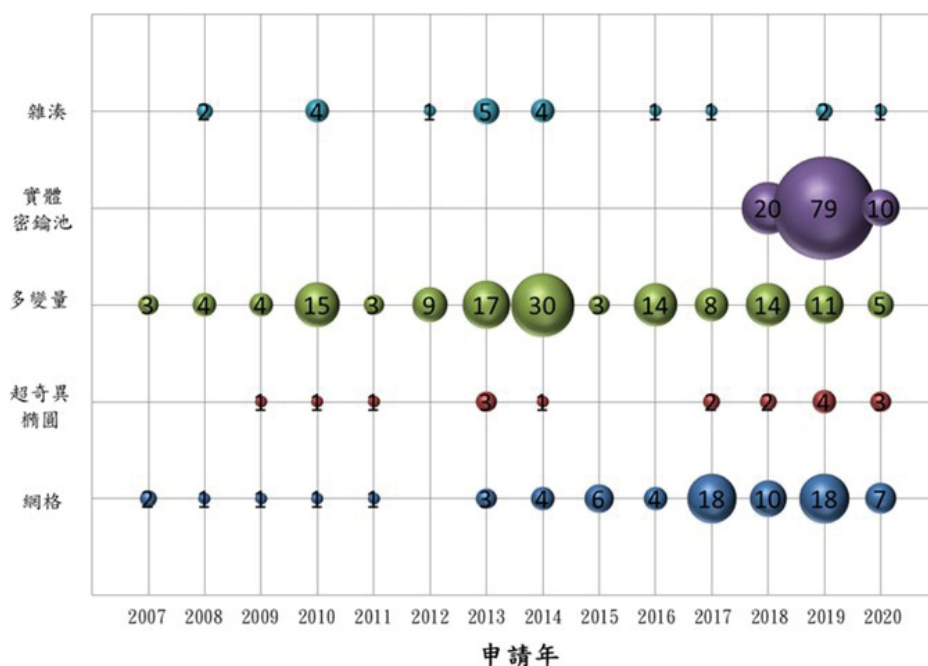


圖 14 後量子密碼學技術分類之申請趨勢圖²⁴

²⁴ 2020 年數量下降之原因同註 5。

圖 15 為後量子密碼學技術分類之申請人國籍分布圖。在申請人國籍分布中可以看出，中國大陸的申請人申請數量於各技術分類均大幅領先其餘各國，這顯示了中國大陸在後量子密碼技術領域的專利布局企圖心高於其餘各國。日本與美國籍的申請人申請數量則所差無幾同居於第二梯隊，兩者的專利數量約各占總數的 13%，二者的差異主要在於關注的技術類別不同，日本主要的專利申請係以多變量密碼學為主，而美國則在多變量密碼學以及雜湊密碼學等二領域均有發展。各技術分類的主要申請人羅列如表 2 所示。

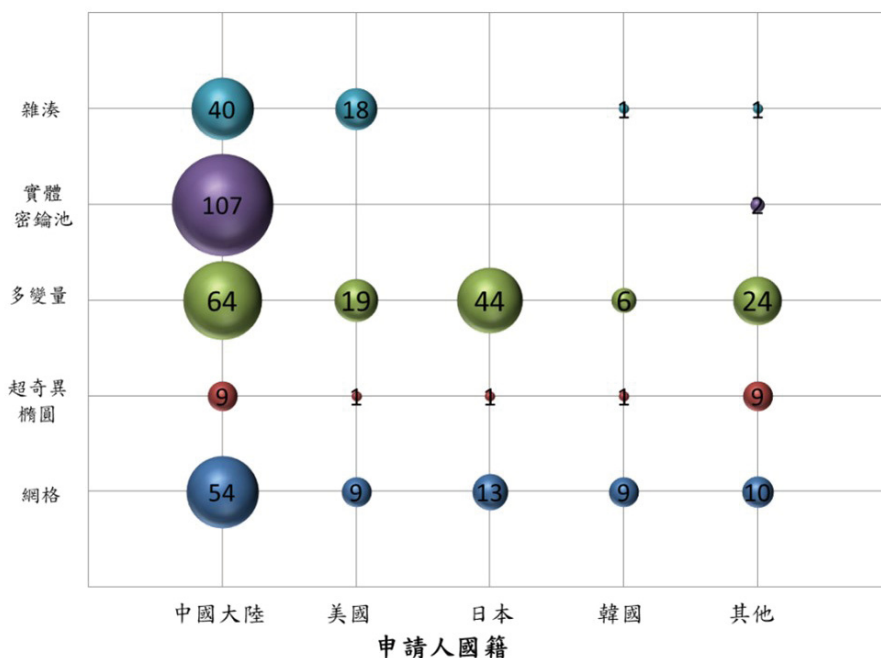


圖 15 後量子密碼學技術分類之申請人國籍分布圖

表 2 後量子密碼學各技術類別主要專利申請人統計

技術類別	專利件數	主要申請人（件數）
網格	95	NTT Docomo（3）、Panasonic（3）、成都電子科技大學（3）、中國科學院（3）
多變量	157	Sony（33）、華南理工大學（10）、西安理工大學（9）、廣東技術師範學院（8）
實體密鑰池	109	如般量子科技有限公司（105）
雜湊	60	Intel（14）

圖 16 為後量子密碼學技術發展矩陣。網格密碼學、超奇異橢圓密碼學及多變量密碼學等三大技術類別的技術發展方向主要集中在加密演算法改良和協議優化，顯見這三個技術類別目前仍著重於密碼系統及協議本身的改良。在實體密鑰池技術類別中，發展方向集中在應用領域及協議優化上，由於實體密鑰池的安全性關鍵技術在於密鑰是承載於實體儲存媒介，因此在通訊的過程中通訊雙方應如何有效地進行訊息交換即成為該技術的主要課題，此外，由於此技術的安全性設計較為單純，因而較多的專利技術係著重於應用面而非加密系統的設計上。雜湊密碼學中的案件數在四種發展方向中較為平均，其在硬體協作上的數量較其他技術類別多，其主要申請人英特爾公司即有針對運算硬體開發專用之加速器，以提升後量子密碼計算時的效能。

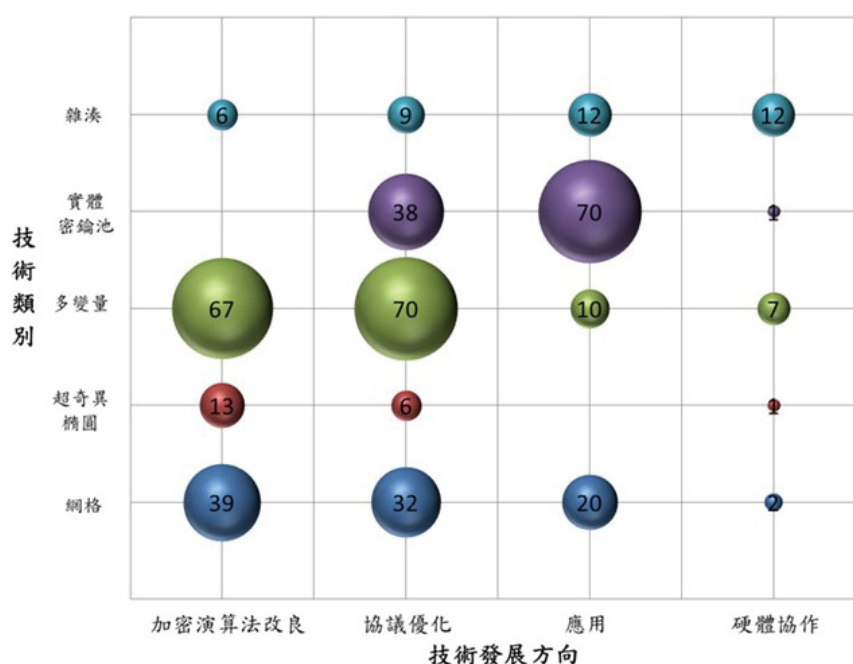


圖 16 後量子密碼學技術發展矩陣

肆、結語

一、趨勢分析結論

在量子通訊的分析中，可以發現中國大陸的專利數量在各技術類別中均處於領先地位，從申請人分析結果可以看出無論是學術界或是產業界均擁有大量專利，依據現今各國在 5G 通訊等尖端通訊技術的發展態勢，可以確定中國大陸在政策面非常重視通訊領域的技術領先地位，並持續在如量子通訊等具有前瞻性的通訊技術投入研發，以保持其在國際上通訊領域的強勢競爭力，在目前量子通訊技術發展的競賽中，中國大陸係具有領導地位，並逐漸成為此領域技術發展走向以及標準制定的主導者。在此技術領域的技術功效分析中可看出，此技術領域主要著重於通訊協議規則的設計以及通訊網路建構這兩大類的技術，主要的功效發展方向著重於提高保密性、增加穩定性、提升效能以及降低錯誤率，呈現出量子通訊目前技術走向係以提升通訊穩定性為主，使此技術逐漸貼近於長距離通訊網路的應用形態。

在後量子密碼學的分析中，可以發現技術主要集中於多變量密碼學以及網格密碼學。多變量密碼學如 Rainbow 加密系統具有數位簽章的體積較小之優勢，因而在數位簽章的應用上頗受青睞；而網格密碼學的優勢則在於其多變成熟的實施型態，實施上較具有彈性，也因此目前已有許多建立於網格問題的不同演算法已被實作出來而受到廣泛討論開發。在技術發展方向上，網格密碼學、超奇異橢圓密碼學及多變量密碼學等三個技術類別之技術發展方向主要集中在加密演算法改良和協議優化，係著重於密碼系統及協議本身的改良；實體密鑰池技術受惠於其設計較為單純，主要發展方向集中在應用領域及協議優化；雜湊密碼學之發展方向則較為平均。在申請人國籍的分布上可以看出，此技術領域之申請人以中國大陸、美國、日本為主，其他國家少有涉獵此技術領域的相關專利。隨著量子電腦的問世，後量子密碼學系統已是通訊安全領域中不可或缺的重要拼圖，然而礙於加密系統標準尚未確立以及密碼系統研發汰換成本過高二因素，目前的專利分析結果中並未觀察到明顯的技術投入上升趨勢。在未來中，加密系統的標準選定以及量子電腦的實用化進程等兩大關鍵因素，將成為後量子密碼系統領域整體發展的重要推動指標。

二、產業發展建議

目前量子通訊技術的發展推動力，主要是用於因應量子計算對現有公鑰加密系統造成的威脅，以解決通訊網路傳輸的安全性問題。我國對於量子通訊的發展起步相較於美、中、日、歐等國晚且專利布局上亦不深，即便我國對於量子通訊技術領域已有一定的投入，例如在 2020 年底，由科技部、經濟部、中研院與教育部共同組成「量子國家隊（Quantum Taiwan）」並提出量子通訊相關專案，且國內技術亦已達成在一般家用光纖網路上實現戶外量子密鑰傳輸，然而整體而言，我國相關產業鏈尚未成形，且具體的產業化方向亦不明朗，整體上的技術乃至產業均未成熟。以國際上量子通訊的技術發展趨勢而言，目前此技術仍然面臨技術成熟度、設備可靠性、資料傳輸安全性等各方面的考驗，這些問題都需要透過產官學研大規模的整合研發量能才有望克服，我國應從設備升級、產業鏈建設、人才培育、核心技術研發和產品商用化等多方面共同推動，進而帶動未來我國量子通訊產業發展，以實現量子通訊網路的全面通用化利用，為我國在國際競爭中占得一席之地。

以後量子密碼的發展而言，由於新密碼系統的建立及汰換需要耗費極高的成本，在密碼標準尚未明朗之前，我國通訊業者尚不宜貿然大量投入特定密碼系統的研發，應有待於密碼標準確立之後，再針對標準進行新系統的建置及開發。此外，美國標準局 NIST 後量子密碼學標準化競賽中的多項候選演算法係有我國學者參與研發，例如決選名單中數位簽章類的勝部演算法 Rainbow 多變量密碼即係由我國中研院團隊所共同研發，顯示我國學者對於後量子密碼系統的技術參與程度很高，我國通訊業者在新密碼系統建置中，係可藉由技術移轉或是合作開發等方式，大幅降低新密碼系統發展普及的技術門檻，以加快技術研發之進程，係為我國在後量子密碼領域中不可或缺的重要優勢。