前瞻科技與管理 9 卷 1/2 期，22-49 頁（2019 年 11 月）
Journal of Advanced Technology and Management Vol. 9, No. 1/2, pp. 22-49 (November, 2019)
DOI:10.6193/JATM.201911_9(1_2).0003

解鎖量子金鑰分發

鍾宏彬 *

國立中央大學光電科學與工程學系博士後研究員

摘 要

本文簡述了量子金鑰分發系統的重大發展歷程，由基本測不準原理與量子糾纏特性之兩種物理定律的介紹出發，配合整列出國際上具有相關技術之公司介紹，分析其發展路程，並簡介了五種常見的量子金鑰通訊協定之應用架構，與探討量子金鑰分發系統未來延伸至廣泛的應用終端，可能遭遇的困難點。於本文第肆章，筆者整理了近年來與合作團隊如何利用光學量子技術，結合積體化光學晶片的概念，提供開發積體量子光源的研究發想，並提出積體量子平臺的概念，冀望未來的量子系統，能高度整合於單一異質材料的晶片中，配合大幅縮小系統尺度的優勢，提高量子應用面的廣度與深度，並於文末探討如何將此積體量子平臺，未來實際應用於普及化的量子金鑰分發系統中。

關鍵詞：量子光源、量子金鑰分發、量子密鑰通訊協定、量子糾纏、積體量子平臺

* 通訊作者：鍾宏彬
電子郵件：xoxo311@hotmail.com
（收件日期：2019 年 7 月 17 日；修正日期：2019 年 8 月 28 日；接受日期：2019 年 9 月 4 日）

Journal of Advanced Technology and Management Vol. 9, No. 1/2, pp. 22-49 (November, 2019)
DOI:10.6193/JATM.201911_9(1_2).0003

Unlocking Quantum Key Distribution

Hung-Pin Chung*

Postdoctoral Fellow, Department of Optics and Photonics, National Central University

Abstract

This paper outlines the major development of quantum key distribution (QKD) systems. Starting from the introduction of two basic laws of fundamental uncertainty principle and quantum entanglement in conjunction with a comprehensive list of international companies with this technology, the author introduced the application framework of five common QKD protocols, analyzed their development paths, and explored the difficulties that various communication protocols may extend to a wide range of application terminals in the future. On the other hand, in the fourth chapter of this paper, the author has compiled the research ideas on how to use optical quantum technology and integrated optical circuits in recent years and provides research and development of integrated quantum light sources. The concept of an integrated quantum platform, the future of quantum systems, can be highly integrated into a single heterogeneous material substrate, in conjunction with a significant reduction in system scale, to increase the breadth and depth of quantum applications; and at the end of the paper, the author explored how to conform this integrated quantum platform into the popular QKD system in the future.

Keywords: quantum light source, quantum key distribution (QKD), QKD protocols, quantum entanglement, integrated quantum platform

* Corresponding Author: Hung-Pin Chung
E-mail: xoxo311@hotmail.com

AECAST Ainosco Press

壹、通訊淺談

隨著自然的演化，不管是發出獨立音節還是特定的肢體動作，或是用古代烽火塔的點對點訊息傳遞，兩個獨立的個體，開始有了交換彼此資訊的機會。人類不同於大多數的動物，我們更進一步的發展出了語言，利用多數共識，賦予聲律、段落、音節，去代表某些公認的意義，讓一定數量的群體有了共同的聲律模式，因而使得訊息更能夠快速傳播，藉由人傳人、族群傳族群、地區傳地區的方式，讓語言散播的區域局限性降低，讓訊息能在地理空間維度下擴散式的分布。另一方面，自從人類發明了文字，讓訊息不再只是瞬態的系統，而是一種可以跨越時間的資訊紀錄，不論是記錄在龜甲上的甲骨文，亦或是記錄在網路世界某個角落的片段資訊，都能稱為某種通訊的紀錄，其差異只在甲骨文的通訊時間維度僅為由古代向現代的單向式傳播，而現今網路病毒般的訊息擴散方式，則同時將空間與時間維度都濃縮在一個又一個的網路伺服器中，等待著全球各地的人，在任何時間的讀取、複寫、調整，與再次散播。

通訊，是一種跨越物種的鏈結方式，人與人溝通、人藉由機器與人溝通，或是更進一步，機器用機器語言跟其他機器溝通。各種不同溝通的方式，藉由不同的媒介，人們可以定義出有意義的訊息，這些訊息已經超越了傳統各種由人類自然發展出的語言文字，人類可以利用數學符號，針對物理現象進行概念闡釋，也能利用人類創造的各種程式語言讓電腦進行計算運作，或是讓機器依照人類設定的工作模式，不間斷的長時間運作。在資訊量超載的本世紀，人類更進一步的利用電腦來處理電腦的資訊，讓系統自行收集資料、分析出有效資訊，更進一步的思考出應對方式，最後自動執行。以上這個模式基本上就是電腦人工智慧（Artificial Intelligence, AI）的概念濃縮版本，這些溝通與通訊，都不再僅止於人類彼此間的訊息交流，而是需要人類、電腦、程式、機器等跨物種的資訊交流，試想：筆者在利用筆記型電腦在瀏覽器搜尋欄輸入：「甲骨文、圖片」資訊的當下，跨越了多少時間與空間！

現代網路發展的進程，其實僅不過四十餘年，網際網路的興起大約在三十多年之前，隨著美國軍方網路技術的釋出，與個人電腦的興起與平民化，據估計，全球資料量由 2013 年的 4.4 ZB（1 ZB 約為 1 TB 的 1,000,000,000 倍），於 2020 年將突破 44 ZB，估計其中三分之二皆由個人所產生（International Data Corporation, 2014）。這些資料包含了你今天去了哪些店、待了幾分幾秒、花了多少時間在網路上、玩了什麼遊戲、網路上買了什麼東西、付了多少信用卡費、銀行存款有多少……等，各種網站的個人帳號、密碼等不計其數含有個人隱私訊息的龐大資料量。或許你不在意昨天去了哪家店，用了多少時間的 Google 地圖導航，但若有一天，你能輕易在 Google 上搜尋到自己銀行的帳號、密碼、交易紀錄和存款金額，甚至是任何一個路人的個人隱私資訊，包含他五年前的某天下午 3 點 21 分去了哪裡，豈不是一件很可怕的事情嗎？

有鑑於此，如何管理如此龐大資訊的安全性，就是一大重要的難題。資訊安全，不僅僅包含說者跟聽者兩方，其中，訊息產生、傳遞、儲存、複製、整合等等的各個階段，都可能有不知名的第三方，將原本的訊息外洩、仿製、假造或是刻意遺失。因此，在訊息處理的各個階段，雖然都有不同程度的加密機制，但從最單純的網路銀行上的隨機鍵盤密碼，就可以發現各種漏洞，雖然螢幕鍵盤的字母順序為隨機產生的，令使用者只能用滑鼠一個字母、一

個字母慢慢點選，雖然其本質立意良善，是為防止駭客直接利用鍵盤固定位置複製個人重要的密碼訊息，但卻忘了慢慢鍵入各字元的當下，若電腦後面有著監視系統，或是一個不良善的人偷偷經過，就很容易因為使用者輸入太慢，而輕易的將密碼記起來，然後破解。正所謂的，防君子卻不防小人。

因此，如何讓使用者能夠快速加密與解密，且在訊息傳輸過程中，又要確保其順暢性與安全性，這技術可以說是一種藝術。如同演武一般，外行者知其然，卻不知其所以然。通訊涵蓋的面向很廣，資訊量龐大且相當複雜，由於量子（Quantum）其物理上的獨特與多元特性，特別適合用來處理如此複雜的系統，現今，各種量子應用都有不同團隊正在整合與開發中，譬如說是量子計算（Quantum Computing）、量子瞬間移動（Quantum Teleportation）、量子通訊（Quantum Communication），甚至是量子電腦（Quantum Computer）與量子網路（Quantum Network）等。本文將聚焦在量子通訊中，一項特別的技術——量子金鑰分發（Quantum Key Distribution, QKD）（Shor and Preskil, 2000）。

由於筆者並不是加解密的專家，本文希望藉由文獻的分析與整理目前已知公開的資訊出發，讓讀者能跟著筆者的思維，逐漸開始在量子技術層面踏步拓樸，並能有較廣面但不過度深入且稍微清楚的應用概念圖樣。因此，本文中並不會深入介紹各自背後的數學模型，而是從量子實際應用的層面出發，筆者將由比較熟悉的物理觀點起步，整理現今當代的量子通訊技術，針對基礎原理、通訊協定邏輯與國內外的發展現況，配合筆者與合作團隊開發中的相關量子技術，進行一系列大綱式的介紹。如同外行者看著演武者耐人尋味的氣勢一躍，配上獅吼般的吶喊聲，我們將隨之起舞，漸漸剖析這位舞著量子通訊大旗演武者的獨門招式。

貳、發展沿革與現狀

通訊，在考慮多於兩個人的情形之下，最簡化可以分成五個人，分別編號A、B、C、D、E，代表發送方（A）、接收方（B）、可信任的中繼者（C）、不可信任的中繼者（D）、竊聽者（E）。假設通訊發生在極小的範圍尺度之下，雖然可以簡化成僅剩下A、B兩人，但別忘了隔牆有耳、上帝之手也無所不在，因此，一個或多個假定的竊聽者E們永遠存在。如果使用了一般的通訊技巧，例如：加密的語言、特殊聲律、長短音（如摩斯密碼）等等，雖然方便快速，但試想，這樣的通訊系統是否處處存在漏洞呢？

傳統上可以利用一組長度較短的密碼，當作金鑰（Key），利用金鑰讓原文上鎖，變成密文，理論上這個加密的密文可以經由不保證安全的通道傳輸，而金鑰只能在秘密通道傳輸，若B收到A的金鑰之後，即可將密文轉回原文，但問題來了，如果金鑰密碼過短，竊聽方E是否容易利用各種計算與估計方式，將金鑰破解，進而將加密的密文破解。因此，有另一個方式為利用跟原文一樣長（甚至更長）的金鑰作為密碼，同步用另一個安全通道將金鑰傳送到B，但問題來了，如要保持A、B兩人的通訊順暢，卻又要使用更長的金鑰，是否又會占用了安全通道大量的使用時間？

另一個現行廣泛應用的方案則為使用非對稱式的公開金鑰加密法（Public-Key Cryptography），常見的非對稱式加密演算法為Rivest-Shamir-Adleman（RSA）加密法（Robinson,

2003），加密系統為利用密碼學偽亂數生成器（Cryptographically Secure Pseudo-Random Number Generator, CSPRNG）由接收端 B 製作出一組公鑰與私鑰，其中公鑰可以藉由各種不安全管道傳至每個訊息發送者（如 A），發送者 A 可以利用公鑰將訊息加密，接收端 B 擁有的私鑰可以將加密訊息打開，但除此之外，用原先加密的公鑰是不能開啟密文的。此方案在實務上被證明有效，能阻絕大量的破壞性攻擊，且已經大量使用在日常生活之中，如網路通訊、電子郵件、影音電話、銀行訊息交換等，但問題又再一次出現，若竊聽者 E，利用管道複製且偷偷擁有了私鑰（例如：使用萬能隨身碟或是網路郵件病毒等直接入侵接收者 B），竊聽者 E 可以任意打開各種由接收者 B 私鑰保護的訊息，在此假定之下，此非對稱式的加密原理基本上已被破解。另一方面，若反璞歸真的使用了對稱式的加密方案，由於金鑰與加密的密文都需要藉由訊息通道進行傳輸，此時如何確保金鑰通道的安全性將是個極重要的問題，若僅考量到對稱式的加密受限於安全通道的實用性與可行性，其資安的風險目前基本上遠高於非對稱式的加密方案，畢竟現今沒有任何所謂真正保障安全的通道吧？

另一方面，在 RSA 加密法的概念下，相較於私鑰被破解的可能性，公鑰的取得更是容易。一般來說，公鑰通常不需要特別經過加密保護，由於密碼還是具有總長度的限制，因此，有心人士所能針對公開網路系統流通的公鑰與密文，通通記錄下來，並利用暴力破解方式，持續針對密文與私鑰進行數值攻擊。在高速電腦快速升級的進度之下，這些被保存的加密資訊，難保再過一陣子就能被破解，並進行密文解密。如同量子電腦建構的當下，未來 RSA 加密法的保證安全年限，可能由數千年，大幅降至數天，甚至數秒鐘。因此，在發展具有超高速運算能力的量子電腦世界潮流中，如何建置一套具有更高度安全的密鑰系統，這是量子技術的實務運用中，發展的契機與挑戰。

經由以上極淺白的通訊加密原理介紹，讀者是否開始頭暈腦脹了呢？接下來我們再升等一級，來談談量子技術目前在通訊所扮演的角色。

量子通訊，一種通過量子物理原理，配合適當的邏輯運作，進而產生量子密鑰的機制，其密鑰本身並不帶有訊息，而密鑰規則可以利用不同的定義方式進行邏輯運作，這些邏輯運作通稱為通訊協定（Protocols），或簡稱協定。

其根據的是量子物理中，主要背後的兩大原理，分別為海森堡測不準原理（Heisenberg Uncertainty Principle）與量子糾纏（Quantum Entanglement）特性。迄今，近代量子物理的發展僅約一世紀，但卻是非常精彩的一百年，比方說：由西元 1900 年，普朗克提出了第一個量子黑體輻射理論開始，經過西元 1905 年愛因斯坦的光電效應理論、西元 1924 年的波粒二象性與物質波理論，到西元 1925 年海森堡提出了完整量子力學理論，竟然僅僅只花了 25 年，如此不可思議的 25 年！筆者有幸出生在量子技術發展滿一世紀的當代，過去很多僅於理論上可以工作的模型，現在都已經是實際存在的技術，例如：量子位元（Qubit）的產生（Wootters, 1998）、量子密碼學（Quantum Cryptography）的實用化（Bennett and Brassard, 2014; Ekert, 1991; Gisin, Ribordy, Tittel, and Zbinden, 2002），或是在公分尺度的積體量子晶片中（Khasminskaya et al., 2016），就可以完成某些特定量子訊息的處理。如上節所述，如果要使用對稱式的加密法，需要一個極安全且不可被竊聽、破解的通道來傳輸金鑰，這樣的通道似乎使用傳統物理的技術之下，相當難以達成或是近乎不可能達成，那讓我們看看量子物理的招數吧。

一、任務目標：製作絕對安全通道，傳輸金鑰

（一）方案一：海森堡測不準原理

測不準原理，或稱為不確定性原理，可以用相當簡單的圖例說明，如圖 1。其中，紅點為理想的粒子位置與動能大小，藍點為可能的粒子位置與動能強度的分布範圍。海森堡在 1927 年基於粒子動能與粒子位置關聯性的探討中，提出了此項原理，原理闡釋了粒子的絕對位置與絕對動能不能同時被確定，當粒子的動能越小，其可能的位置分布範圍越大，反之，若當粒子位置越確定，其動能分布的範圍越大，意即不能同時確定粒子的動能與位置，只能以機率分布描述之，如圖 1 藍點所示。

根據這樣的基本原理，我們可以延伸一個思考：如果單位時間內，這個系統只有一個粒子，假定這個粒子不可以再分割成更小的粒子時，如果在行進方向出現了兩條路，假設這個粒子通過兩條路的機率正好是 50%：50%，此時，這個粒子就在兩個出口產生了一個相等的機率分布，但由於此粒子不能夠再分割了，如果進行量測，在完美的情形之下，每次測量就一定只有某一個出口能探測到一顆粒子，另一個出口一定沒有收到粒子。但在進行測量之前呢？觀察者是否能夠提前知道粒子會從哪一個出口通過？看來是不能，對吧？那我們怎麼製作出這一個不能再分割的粒子呢？最簡單的方式就是取得一顆量子，例如：一顆光子。那如何製作出兩個通道呢？最直覺的方式就是經過平均分光的分光鏡，讓光子走兩條路徑，這兩條路徑具有相等機率的分光比率。除了利用空間上的分光之外，還能利用光子所帶的偏振訊息（偏振，即為光波的電場震動方向），製作出 50%：50% 比率的分布。例如：利用人為控制光子的偏振方向，使之呈現水平（0 度）與垂直（90 度）或是正負對角線（45 度與 135 度）的分布，若兩個情形的機率正好是 50%：50%，則可以利用這個方案，達成產生金鑰的方式，實際達成金鑰分配的方法，則對應到以下情境。

1. 發送者 A 每次隨機產生一個位元（0 或 1），並利用 A 給的隨機偏振選擇器（Basis），水平與垂直（0 度與 90 度，稱為 O-basis）或是正負對角線（45 度與 135 度，稱為 D-basis），假定 A 每次發送一光子，此時，光子如果遇到選擇 O-basis 時，定義水平偏振（以下簡稱為 H）代表 1、垂直偏振（以下簡稱為 V）代表 0，另一方面，若光子遇到選擇 D-basis 時，定義 45 度偏振（以下簡稱為 L）代表 1、135 度偏振（以下簡稱為 R）代表 0。
2. 因此，原先發送者 A 隨機選擇的位元，便利用以上方式，轉成光子偏振狀態，根據兩種位元（0、1）與兩種 Basis（O-basis, D-basis）選擇，光子隨機帶有四種可能的偏振狀態，位元 0 有 50% 機率為偏振 V 與 50% 機率為偏振 R，而位元 1 則有 50% 機率為偏振 H 與 50% 機率為偏振 L，以上關聯性如表 1 所示，然後發送者 A 就將這顆帶有特定偏振訊息的光子發送至接收者 B。
3. 接收者 B 利用他自己隨機挑選的偏振檢查器（水平與垂直 O-basis 或是正負對角線 D-basis），檢查 A 送過來的每一個光子的偏振。利用與 A 相同的定義方式，利用偏振還原位元資訊，並於 B 本地記錄起來，成為 0 或 1 的序列。
4. 接收者 B 將剛剛一連串的偏振檢查器的紀錄（O-basis 或 D-basis 序列），傳輸至發送者 A。

5. 發送者 A 則將接收者 B 傳來偏振檢查器的 Basis 與自己原先設定的偏振選擇器的 Basis 做比對，將相同的 Basis 的量測結果保存下來（0 或 1 序列），並回傳訊息告知接收者 B 有哪一些偏振選擇器 Basis 是錯誤的。
6. 接收者 B 將錯誤的測量結果刪除，將部分正確的結果（部分共享的 0 或 1）於公開頻道上公告，發送給 A 確認並檢查是否有竊聽者 E。
7. 發送者 A 確認 B 回傳的部分正確資訊之後，確定無竊聽者 E 之後，A 與 B 將這些使用過的正確資訊刪除，剩餘未使用的正確訊息（剩餘共享的 0 或 1 的序列），就是最後的共享密鑰（Final Keys）。

以上的通訊協定方案，就是由 Bennett 與 Brassard（1984）所提出的方案，現簡稱為

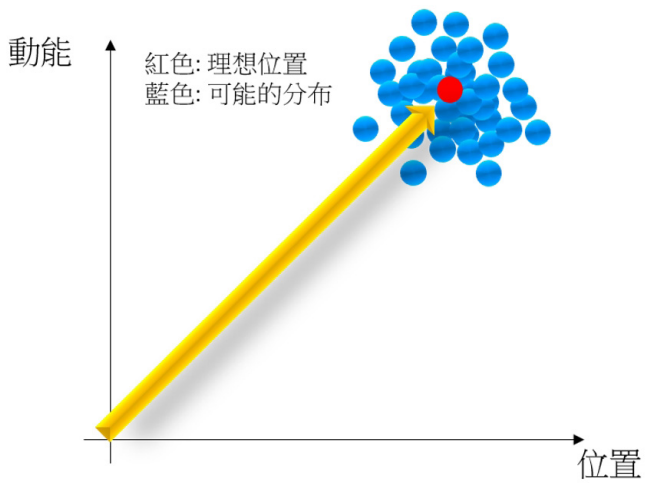

圖 1　測不準原理的示意圖

資料來源：作者自行繪製整理。

BB84，為第一個明確定義的 QKD 方案的實用協定。現今，國際上許多團隊已就 BB84 基本協定模型，藉由加入不同的步驟或是結構，發展出各類型的通訊協定，此 BB84 類型的協定通稱為測不準原理協定，此類型協定有一個特色，就是有明確的發送者 A 與接收者 B，金鑰起始源來自發送者 A，但這個機制或許造成了一些源自系統不完美，導致產生可破解的漏洞，這部分於第參章會再行詳述。

（二）方案二：量子糾纏原理

量子糾纏，一種量子整體性的狀態描述，或借用愛因斯坦當年提及的稱呼：鬼魅般的超距作用（Spooky Action at a Distance）。根據上述的測不準原理，粒子並不同時具有絕對空間位置與絕對動量，而是利用機率來描述其完整性，這樣的概念在 Einstein、Podolsky 與 Rosen（1935）的思想實驗之下，延伸出了一個物理與哲理上弔詭的悖論：Einstein-Podolsky-Rosen（EPR）Paradox，在近一百年前的物理世界裡掀起一陣波瀾，漣漪至今。根據這篇歷

史性的思想實驗文章，一個完備的物理理論須建立在以下數個事實之上，包含：1. 物理理論必須正確無誤、2. 物理理論必須給出完備的描述。其中，第二項須具備完備的描述中，Einstein et al. 的論文提出定域性定律（Locality）與實在論（Reality）都必須在量子力學理論中被嚴格闡釋，根據該理論觀點，定域性指出某件物理事件只能在特定的範圍內有作用，無法利用超過光速的方式影響其他區域，而實在論則認為「觀察」這個動作與物理本身特性無關，意即不論有沒有人在觀察，物理特性都存在，黑就是黑、白就是白，不論是否有人在觀察。將定域性與實在論可合稱為定域實在論，表明了一個簡單的描述關係：微觀粒子具有完整、可量測的物理特性，且其不受到來自遙遠區域之超光速的事件影響。因此，Einstein et al. 的論文想像了一對彼此關聯的雙量子系統，如果檢驗了其中一顆量子的狀態（例如：光量子的偏振狀態），那是否就能確認另一顆量子的狀態呢？這樣的檢驗是否有受兩者之間的距離影響？這樣是否就不符合測不準原理所描述的情形呢？

表 1　偏振對應位元與 Basis 組合關聯性

	Polarization (Bit)	
Basis	0	1
O-basis	V	H
D-basis	R	L

資料來源：作者自行繪製整理。

以上的思想實驗，「量子力學是否不完備？」在當時的確演變成兩派人馬互相爭論不休的主題，直到 Bell（1964）提出了著名的一套可經由實驗驗證的公式：貝爾理論與貝爾不等式（Bell Inequalities）。根據貝爾不等式，觀察者可以利用統計歸納法，檢查疑似具有超距作用系統的關聯性（Correlation）是否存在且能夠利用實驗重複驗證，例如：檢查一對可能有關聯性的光子對（Photon-Pair）的偏振狀態。由於 Einstein et al.（1935）的論文中的定域實在論（簡稱為傳統物理預測，Classical）與量子力學理論（通稱為量子物理預測，Quantum），都能夠預測此光子對關聯性的分布關係，因此，兩個理論流派所爭執不休的量子力學完備性，孰是孰非，終於可以通過實驗進行驗證，見真章的時刻到了。

二、真相只有一個，量子力學的預測符合了最終實驗的結果

根據以上貝爾關聯性測試的實驗驗證結果，不僅關乎兩大流派爭論的真相，更隱含著更重大的一個物理事實：鬼魅般的超距作用是真實存在於物理世界的。這樣的雙粒子超距作用的關聯系統，在爭論熱度最高的 1930 年代，就由薛丁格（Erwin Schrödinger）為了方便與愛因斯坦通信討論，利用德文對這個系統起了個名字，稱之 Verschränkung，而後由薛丁格本人以英文譯之，稱為：量子糾纏（Quantum Entanglement）。

由於糾纏量子對（可稱為 EPR Pair）具有超距作用的關聯性，且具有量子態不可能被完美複製（No-Cloning）（Koashi and Imoto, 1998）的特性，也適合被用來製作共享的量子金鑰，其應用方案與上述的 BB84 通訊過程類似，但主要的差別在於，如果系統使用量子糾纏

架構，並不需要明確界定糾纏量子對一定來自發送方 A，事實上，糾纏量子對可以由可信任的第三方 C 發出，並送至訊息發送方 A 與訊息接收方 B，A 與 B 可以分別針對 A、B 本地量測到的量子態進行關聯性分析，並藉由類似 BB84 通訊協定的交互驗證方式，產生共享金鑰。歷史上，最早由 Ekert（1991）提出了此類利用量子糾纏特性進行金鑰分發的通訊協定，現稱為 E91 通訊協定，隨後 Bennett、Brassard 與 Mermin（1992）提出了新的通訊協定方案，他們延伸 BB84 的概念至利用糾纏量子對作為金鑰，現稱為 BBM92 通訊協定。

本段落筆者整理了目前全球 QKD 系統的發展主流，包含數個具有商業規模的公司與近代科學突破的里程碑。於 1980～1990 年代初期，提出 BB84、BBM92 等協定架構的先驅者，主要來自美國與加拿大，而 E91 協定架構提出者為英國—波蘭學者，2000 年代由日本、澳洲相繼投入相關開發，2005 年之後中國也啟動相關研發團隊，並於 2017 年利用墨子衛星進行數項太空尺度的 QKD 實驗，開始在國際上占有一席領先地位。以下，筆者就近二十年關於 QKD 系統重要的里程碑與相關公司進行粗淺的介紹。

三、近二十年 QKD 系統里程碑

（一）2002 年：Differential Phase Shift（DPS）QKD 通訊協定（日本）（Inoue, Waks, and Yamamoto, 2002）。

（二）2003 年：DARPA Quantum Network 啟用（BB84 通訊協定，美國）（Elliott, 2018）。

（三）2004 年：SARG04 通訊協定（瑞士）（Scarani, Acín, Ribordy, and Gisin, 2004）。

（四）2005 年：誘騙態（Decoy State）QKD 通訊協定（加拿大）（Lo, Ma, and Chen, 2005）。

（五）2009 年：SECOQC QKD Network 啟用（奧地利）（Peev et al., 2009）。

（六）2009 年：Coherent One-Way QKD（COW 通訊協定，瑞士）（Stucki et al., 2009）。

（七）2009 年：300 km Free-Space QKD（Entanglement-Based QKD，西班牙）（Scheidl et al., 2009）

（八）2010 年：Tokyo QKD Network 啟用（日本）（Sasaki et al., 2011）。

（九）2017 年：墨子衛星，1,203 km 量子糾纏與 BB84 通訊協定驗證（Yin et al., 2017）。

（十）2018 年：墨子衛星與地面連線，7,600 km（BB84 通訊協定，中國、奧地利）（Liao et al., 2018）。

四、實際應用方面

1999 年代開始，歐美許多著名的 QKD 公司陸續成立，例如：MagiQ Technologies（美國，1999 年開始發展）、ID Quantique（瑞士，2001 年）、qutools GmbH（德國，2005 年）、QuintessenceLabs（澳洲，2006 年）等。在亞洲方面，日本的 Toshiba Corporation、Nippon Telegraph and Telephone Corporation（日本電信電話公司，簡稱 NTT）、Mitsubishi Group（三菱集團）與 NEC Corporation（日本電氣公司）則分別有提供 QKD 技術方案。其中，2010 年代開始的東京 QKD 系統之布建資訊，請參考 Fujiwara, Waseda, Nojima, Moriai, Ogata, and

Sasaki（2016）之文章。筆者整理世界目前主要的 QKD 系統與相關模組供應商，其公司位置分布如圖 2，並估計各公司開始研發 QKD 系統的年分、可能使用的通訊協定，統整於表 2 中。其中，常見的 QKD 通訊協定可以分類成兩類，利用測不準原理相關協定如：BB84、B92（Bennett, 1992）、Decoy State、SARG04、KMB09（Khan, Murphy, and Beige, 2009）、S13（Serna, 2013）、AK15（Abushgra and Elleithy, 2015）等，而利用糾纏特性之相關協定如：E91、BBM92、COW、DPS 等，這些不同的協定的本質上，大多具有互相關聯性，根據系統架構與使用廣泛度，本文將選出 BB84、BBM92、Decoy State、COW、DPS 這五種常見協定的基本架構，將於第參章進行介紹與分析。

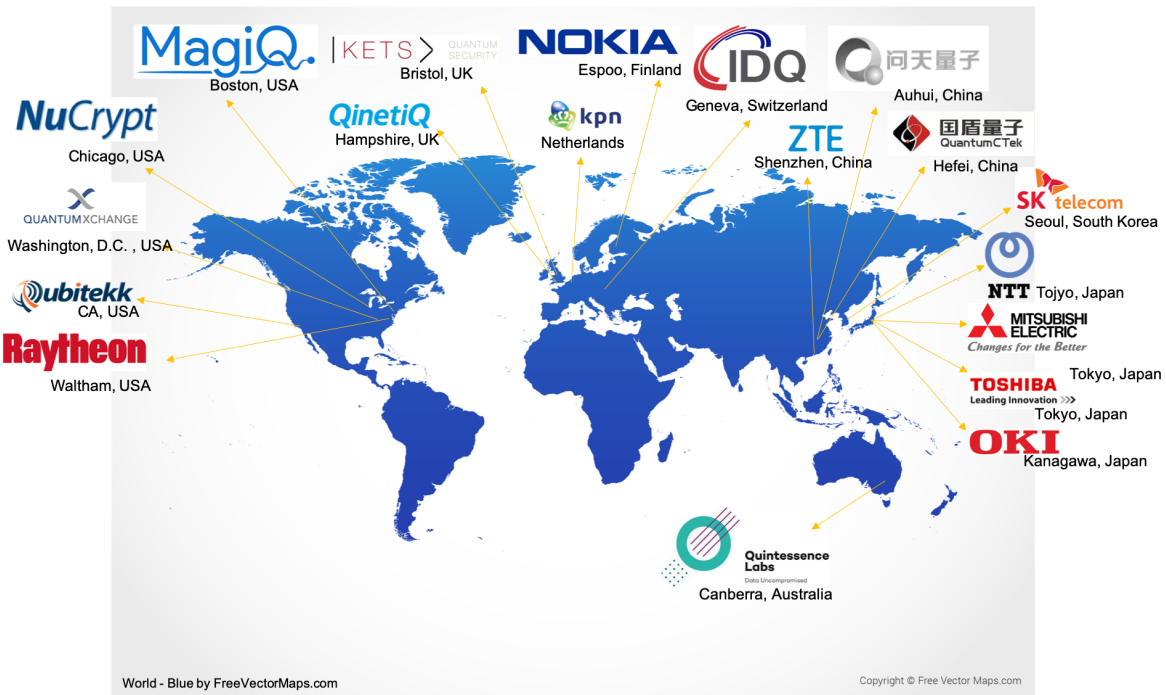

圖 2　國際上現有的 QKD 系統相關公司（2018 年）

資料來源：作者自行繪製整理。

五、臺灣相關研究發展與挑戰

我國於 2000 年初期，由行政院國家科學委員會（簡稱國科會，於 2014 年升格為科技部）工程處啟動了量子資訊科學之先導性的研究計畫開始，並於 2005 ~ 2008 年的國家科學技術發展計畫中，亦將量子研究列為重要的發展項目之一。量子計算領域的部分，則由 2007 年代開始發展迄今，由國科會工程處主導的五大領域，包含量子計算理論、量子電路、量子演算法、量子密碼及量子資訊學等範疇。另一方面，於科技部自然司的物理學門中，從早期就持續支持量子相關領域的研究計畫，於 2018 年啟動的大型計畫中，「量子電腦旗艦計畫」為利用國家層級執行共同跨校推動的旗艦計畫之一。科技部規劃補助五大研究計畫，分別為期五年，每年度預算約在一億元新臺幣等級。其發展主軸為奠基於國內深厚的科技發展實力

表 2 國際上現有供應商的 QKD 相關資訊整理

地區	國家	公司	年分[1]	QKD 系統與相關模組	通訊協定
美洲	United States	MagiQ Technologies	1999	MagiQ QPN	BB84
	United States	Quantum Xchange	2018	Phio	N/A[2]
	United States	Raytheon	2005	N/A	N/A
	United States	Nucrypt	2003	EPS, CPDS, and Polarization Analyzer	N/A
	United States	Qubitekk	2012	Quantum DataLoc™ Key Server	BBM92
大洋洲	Australia	QuintessenceLabs	2006	qOptica	N/A
歐洲	Switzerland	ID Quantique	2001	Clavis3 QKD Platform	COW
	Germany	qutools GmbH	2005	N/A	N/A
	United Kingdom	QinetiQ	2004	N/A	N/A
	United Kingdom	KETS Quantum Security	2016	Quantum Photonics	N/A
	Finland	NOKIA	2016	(Work with SK Telecom and IDQ)	COW (?)[3]
	Netherlands	KPN	2016	(Collaborating with IDQ)	BB84 (?)
亞洲	South Korea	SK Telecom	2016	(Work with NOKIA and IDQ)	COW (?)
	Japan	Oki Electric	2000	N/A	N/A
	Japan	NTT	2000	DPS-QKD	BB84
	Japan	Mitsubishi Electric	2001	(Work with NTT, NEC, and Toshiba)	BBM92, DPS, SARG04
	Japan	Toshiba	2010	Quantum Encryption System	T12, Decoy State BB84
	China	Anhui Qasky	2009	Quantum Key Distribution Terminal	Decoy State BB84
	China	QuantumCtek	2009	QKD-PHA300 Series	Decoy State BB84

註：[1] 利用發表之文獻、新聞、媒體報導等資訊，粗估各公司開始發展 QKD 的年分。[2] N/A 表示查無資訊。[3](?) 標記處為推測該公司可能使用通訊協定的方案。EPS: Entangled Photon Source; CPDS: Correlated Photon Detection System。

資料來源：作者自行繪製整理。

與半導體製程技術，並推動量子運算、量子晶片與量子通訊發展與應用，並強化臺灣與國際領先研究單位的合作鍵結，量子電腦旗艦計畫則包含臺灣大學的矽基量子元件、量子計算與量子通訊、中央大學的矽基量子光電晶片、成功大學的量子運算、元件與科技等。國內目前量子相關重點研究中心如：清華大學的前瞻量子科技研究中心，以及臺灣大學與 IBM 合作的量子電腦中心，成功大學於 2003 年成立量子資訊科學研究中心，臺灣大學則設立了校級跨領域之量子科學與工程研究中心。

由以上可知，臺灣目前在量子科技的發展仍以學研單位為主力，從早期分散的個別研究，於近年方有政策性的鼓勵與較為聚焦的研發方向，除了投入時程是否過晚、資金是否充裕、人才是否齊全足夠、發展藍圖或策略是否正確、產業是否願意投入開發此新興且高端技術、產學研如何鍵結與合作，及跨國合作如何開展等都將面臨相當大的挑戰。臺灣半導體產

業擁有世界公認的頂尖實力，在發展量子電腦的長程總體目標之下，我們可以利用半導體先進製程技術的優勢，配合基礎量子物理的學術研究，與量子實驗技術、量子材料、量子邏輯等技術的開發，在量子電腦產業鏈的全球分工之中，占有重要的一席。科技部在「量子電腦旗艦計畫」，希望由上而下，整合全臺產學研界相關研發能量，合理化挹注資源，達到最大效益與執行效率，但綜觀臺灣現狀，主要發展瓶頸將來自：

（一）總體目標明確，但細部分工不明確，容易導致各大專院校、產業各自攻山頭，沒有統籌分配資源與研發資訊。

（二）量子關鍵技術的重點開發啟程稍晚，國際領先團隊於量子技術方面，往往是政府與產學研界長年的耕耘，利用持續資源挹注與長期政策的配合，延續開發能量與開拓量子應用市場的大環境，如澳洲的量子技術大本營 Center for Ultrahigh Bandwidth Devices for Optical Systems（CUDOS）於 2003 年由澳洲研究理事會（Australian Research Council, ARC）就成立迄今。

（三）量子電腦的發展藍圖尚不明確，由於相關技術涵蓋的面向很廣，可以粗分為量子源、量子處理晶片、量子計算、量子除錯、量子邏輯、量子資訊處理等。需要中央政府進行統籌管理各分項的發展藍圖與合理的資源分配。

（四）量子技術人才的短缺，由於過往臺灣基礎物理的相關人才，除培養不易之外，且缺少合理相對應的工作機會，因國外求職或進修，導致基礎科學人才外流之外，也缺少新血加入，使相關量子技術人才相當短缺，需要由中央政府統籌管理的專案部門，轉請大專院校鼓勵新人專攻量子領域，並招募國內外有志之材加入。

（五）國際分工的舞臺角色定位尚未建立，尋求國際合作與提供自身量子研發能量之關鍵技術的國際交流，可參考國外相關技術的發展模式，利用國際分工，思考全球量子電腦產業鏈的關鍵定位，包含提高技術含量的量子技術、半導體技術加值延伸、深耕大數據與 AI 自動化產業、加強學術與產業鏈結，使臺灣由世界級高科技矽島，逐步轉型成世界級量子電腦關鍵技術供應鏈成員。

參、系統架構與應用限制

延續第貳章的介紹，達成 QKD 的途徑可以分成測不準原理類型與量子糾纏類型，根據不同通訊協定框架，QKD 系統實際量子層面的架構雖大同小異，但還是可以分類出幾種主要的架構類型，本節由常見 QKD 協定的系統設計概念出發，分析不同協定之間的異同與相互對應關係，並針對數種可能的破解方案，進行實際應用場域限制的探討。以下介紹五種常見 QKD 協定設計架構概念。

一、BB84 通訊協定

1984 年被提出的 BB84 通訊協定，主要由發送端 Alice 利用單光子源加上兩種等比率分布機率的路徑，這樣的分光路徑可利用光束分光器（Beam Splitter, BS）達成，配合隨機相

位調制（Phase Modulation, PM）機制，於某一路徑製作出相對於另一個路徑產生相位差，並於接收端 Bob，再利用一組與發送端 Alice 相同架構的分光／合光路徑，製作出不可分辨的兩種路徑（包含 Alice 長徑加上 Bob 短徑，與 Alice 短徑加上 Bob 長徑），如圖 3 所示。理論上，此兩種路經會在時間上同時抵達 Det 1 或是 Det 2，根據 Alice 與 Bob 隨機選擇的 Basis（利用相位調制器隨機選擇），並藉由本文第二章所提及的 BB84 通訊協定原理，可以將 Alice 與 Bob 各自選擇的 Basis 藉由傳統訊息通道進行比對與檢查，達成 QKD 的目的。

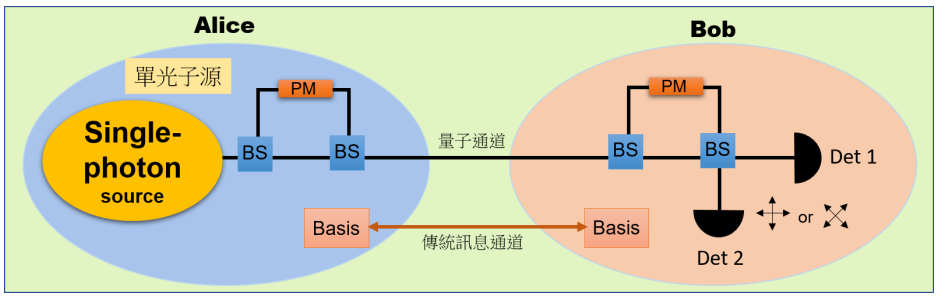

圖 3　BB84 QKD 通訊架構概念

資料來源：作者自行繪製整理。

二、BBM92 通訊協定

1992 年被提出的利用量子糾纏特性達成分發的 BBM92 通訊協定，其概念圖如圖 4 所示，與 BB84 最大的不同在於 BBM92 為利用量子糾纏光子（Entangled Photon-Pair, EPP or EPR pair）對做為 QKD 的光子源。因此，糾纏光子源發送方不見得需要在 Alice 與 Bob 兩

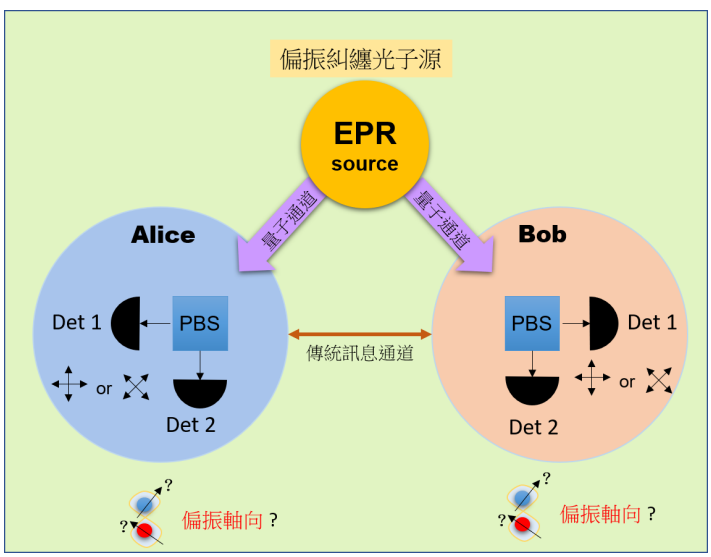

圖 4　糾纏光子態（BBM92）QKD 通訊架構概念

註：PBS: Polarization Beam Splitter。

資料來源：作者自行繪製整理。

方之一，可為中立之第三方地區，並利用等距離的傳送距離，將未知偏振狀態的光子對，同時發送至 Alice 與 Bob 兩地，並由 Alice 與 Bob 兩地分別檢查送來的光子對的時變偏振狀態。由於此種光源並非由衰減雷射所達成之類單光子源，可以有效阻擋或是減低一些外部竊聽者的攻擊伎倆，如第三方竊聽攻擊（Man-in-the-Middle Attack）（Wang, Wang, Li, and Huang, 2009）或是將光子分開而進行竊聽的 Photon Number Splitting（PNS）Attack（Lütkenhaus and Jahma, 2002）、Beam-Splitting Attack（Dušek, Haderka, and Hendrych, 1999）等方式。

三、Decoy State 通訊協定

另一方面，於 2000 年代初期，Decoy State 的 BB84 協定也開始被提出，與 BB84 類似，Decoy State 協定也是由明確的發送端 Alice 利用若脈衝雷射製作出類單光子源，但加上了一組光學強度調制器（Intensity Modulator, IM），如圖 5 所示，此 IM 作用可以做為光的開關，在特定傳輸時間上，可以將主動的光源開啟或是關閉，因此，加上此功能之後，原先 BB84 協定僅有相位調制的功能，而 Decoy State 的 BB84 協定則同時具有了強度與相位的調制功能，能阻擋一些針對光源缺陷進行的特定攻擊。

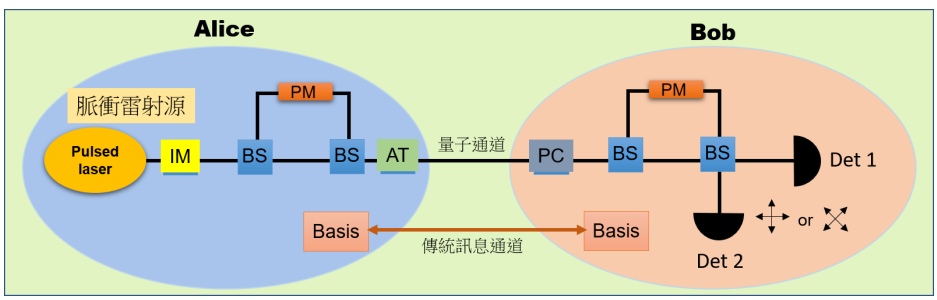

圖 5　Decoy State 的 BB84 QKD 通訊架構概念

註：AT：脈衝強度衰減器（Attenuator）。
資料來源：作者自行繪製整理。

四、COW 通訊協定

於 2005 年代左右，歐洲研發團隊提出了改良式的 BB84 協定，研發團隊將此協定稱為 COW，其基本架構延伸了誘騙態的 BB84 架構，如圖 6 所示，其 Alice 發送端類似誘騙態結構，同時利用 IM 與加上可調式光學強度衰減器（Variable Optical Attenuator, VOA）與 AT，並於 Bob 接收端另用三組光耦合器將收到的單光子進行特定比率的分光，利用三個單光子偵測器（Det B、Det M1、Det M2）進行時間同步的巧合計數量測，由於有一組單光子偵測器（Single-Photon Detector）Det B 持續監測接收端的光子數，COW 協定可以提高以下攻擊的抵抗性，如：PNS Attack、Beam-Splitting Attack、Man-in-the-Middle Attack、Intercept and Resend（IRA）Attack（Curty and Lütkenhaus, 2005）。

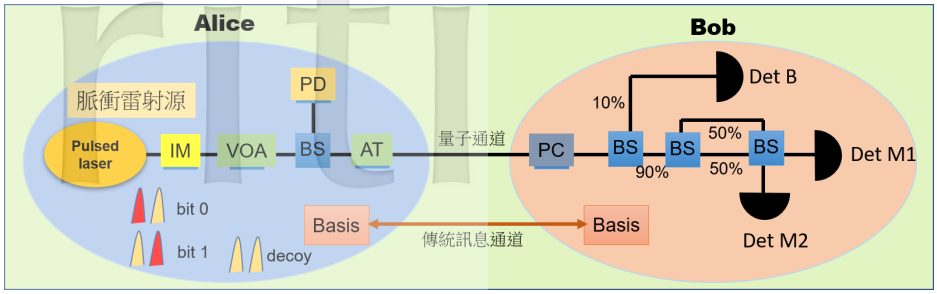

圖 6　同調單向式（COW）QKD 通訊架構概念

資料來源：作者自行繪製整理。

五、DPS-QKD 通訊協定

日本 NTT 研究團隊，於 2000 年代初期，基於改良式的非正交態 B92 協定，研發團隊提出了差分相移式的 QKD 協定（DPS-QKD），如圖 7 所示，與 COW 協定比較下，DPS 結構相對簡單，其主要利用脈衝同調光源 IM、PM 與 AT，即可作為 Alice 發送端的光子源製備，於 Bob 接收端則利用了干涉儀架構，接收並解析非正交態的訊息光。DPS 協定，可以有效阻擋以下攻擊，如 PNS Attack、Beam-Splitting Attack、Man-in-the-Middle Attack、IRA Attack、Denial of Service（DoS）Attack（Hugues-Salas et al., 2018）。

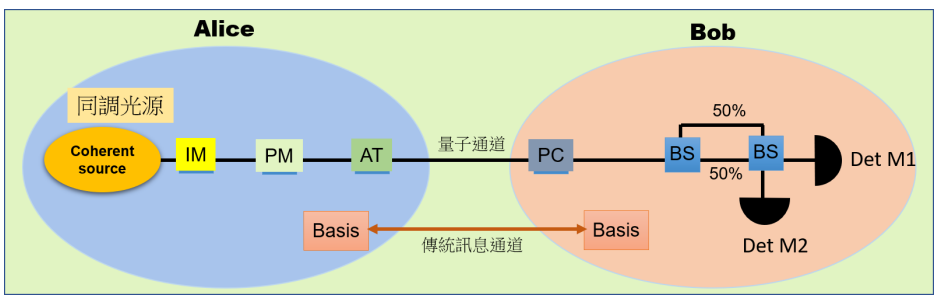

圖 7　差分相移式（DPS）QKD 通訊架構概念

資料來源：作者自行繪製整理。

六、五種協定實作優缺點分析

以上五種協定，於實作面討論的範圍下，BB84 與 BBM92 可以分別代表兩種量子機制形式的協定原理展現架構，適合教學或是前期研究使用，但由於此兩種方案之發展時程較早，也可能有幾種密鑰漏洞的疑慮（Abushgra and Elleithy, 2016）。由於為了補償前述兩種基本形式的系統上，可能因為不完美而導致的漏洞，進階的協定開發者，可以利用 Decoy State 的協定開始下手，並研究其原理與系統缺陷的補償機制。具有實際應用並商用化的 DPS 與 COW 協定系統，則適合於嘗試開發自主控制 QKD 系統的開發者，通過利用已被證明安全性與密鑰率皆可商用化的協定進行雛型研究，再進行自主協定的開發，可以奠基在一

定基礎之上，進行更嚴謹的協定開發研究與量子密鑰分發的應用。關於以上各類型協定，嚴格的量子密鑰分發各協定系統安全性之數值理論分析，請查閱回顧文獻 Renner（2008），應用實務上的安全性分析，請參考 Scarani, Bechmann-Pasquinucci, Cerf, Dušek, Lütkenhaus, and Peev（2009）。以上所提及的五種常見的 QKD 協定，除 BBM92 為利用量子糾纏特性之外，其餘皆須要使用衰減弱脈衝雷射（Attenuated Weak Coherence Laser）光源製作類單光子源，或是直接使用單光子源，但由於產生光學損耗的環境因子非常多，使得如何將 QKD 系統進行有效率且長距離的傳輸，是這個世紀以來許多研發團隊的目標，筆者認為 QKD 系統未來能否普及化的應用瓶頸分述如下。

（一）穩定 QKD 光源取得的難易度

綜觀以上幾種實用化的 QKD 系統，其中光源主要還是來自脈衝雷射配合衰減器，製作出類單光子光源，此類脈衝雷射方式製作的單光子源，由於衰減之後的平均光能量強度在單光子能量強度等級，且需要在長時間工作之下非常穩定，才能持續進行量子密鑰的分配。另一方面，若使用量子糾纏光源，糾纏光子對的生成機制為機率分布，如何穩定持續有一定比率的量子糾纏光子對持續生成，並保持其產生機率，以達成有效率的 QKD，這還是科學與工程學上需要克服的難題，關於以上量子金鑰光源的分析，於下一章節有更詳細的介紹。

（二）系統工作環境的要求嚴苛程度

QKD 系統主要可以分成光源、調制、偵測與解析等四大部分，其中，調制方面，使用傳統強度調制器與相位調制器的技術已相當成熟，但單光子偵測器，大多需要工作在極低溫，以確保偵測器的效率，由於加入了冷卻系統，導致偵測器本身體積大且其對於工作環境的要求相對高，如何將單光子偵測器進行微縮化、並提升其對於工作溫度的容忍度，還是系統工程上須要克服的關鍵之一。

（三）光學損耗的補償能力

QKD 傳輸距離主要受限於光子於傳輸過程中的衰減率，由於為了比擬單光子源，脈衝雷射通常在發射端就已經削弱到極低的平均能量，導致經由光纖或是自由空間傳輸損耗後，其抵達接收端的有效光子能量等級非常低，通常需要長時間的量測積分時間，與配合高效率的單光子偵測器才能讀取訊息。另一方面，使用糾纏光子對的通訊架構，則會面臨到糾纏光子對不可被預先偵測的問題，例如：若糾纏光子對訊號強度過低，而需要重新放大糾纏訊號時，其訊號放大站必須將接收到的糾纏光子對進行偵測，因此導致破壞了原先光子對的糾纏特性，使得通訊機制失效。倘若不經由放大機制，如何提高糾纏光子對抵達接收端的能量水平，又能確保通訊效率之議題，已引起廣泛研究。

（四）密鑰除錯率與傳輸效率的提升

由於密鑰分配過程中，來自環境因素與傳輸介面的損耗，導致了各種機率不明確性的發生，不論是測不準原理或是糾纏方式的通訊協定，在實際應用中，通常可能由於傳輸過程中，受各種偏振相依的元件影響，產生多餘的偏振錯誤訊號，導致後端接收者需要將錯誤的偏振訊息進行校正，再與發送端進行比對，這樣來回比對校正，導致除了犧牲了單位時間內的傳

輸效率，也使得接收到的密鑰正確度受到質疑。因此，密鑰除錯技術的提升，將有助於提高量子密鑰分發的密鑰率，與維持此系統工作時的順暢性。

（五）系統架構的實用程度

本章節提及五種常見架構中，除 BBM92 協定之外，其餘四種都利用弱同調光子源作為光源，加上不同結構的調制架構，並配合兩到三組單光子偵測器作為訊號解析機制。而利用糾纏特性的 BBM92 則需要四組單光子偵測器才能有效的進行量子偏振糾纏的解析，在如此的架構下，系統通常相當複雜且體積龐大（大約公尺等級），如何將整體系統進行模組型的統整，將系統尺度降至數十公分等級，還需要更多在系統面整合的努力。

肆、發展中的方案：積體量子光源平臺

量子光學實驗在近三十年內，獲得重大的進展，除了著名的違反 Bell 不等式實驗與量子糾纏實驗等理論實驗化，QKD 系統由 Bennett 與 Brassard（1984）提出之量子通信原理的概念之後，此系統於 2000 年代已開始商用化，並逐步將量子應用於人類生活的實際場域中。其中量子密碼學的最早發展可以追溯到 Wiesner（1983）開創了量子密碼學，而於 1990 年代，較晚被提出之量子密鑰分發之概念，因具有即時性、高保真的特性，將可能是未來量子糾纏效應於實際應用中的一大應用形式（Horodecki, Horodecki, Horodecki, and Horodecki, 2009）。以光子型態之量子密鑰分發的實驗中，奧地利團隊於 2007 年將糾纏光子對於空間中分離 144 公里，尚能量測到其糾纏效應（Ursin et al., 2007）。此外，利用光纖低損耗之特性，已有來自日本的團隊於 2013 年成功將兩糾纏光子分離 300 公里，依舊能量測到其糾纏特性（Inagaki, Matsuda, Tadanaga, Asobe, and Takesue, 2013）。在各項量子應用的架構中，主要需要考量幾個面向，包含量子源的取得、量子態的保存、量子態的分發、量子態的解析與重建等。在量子光源方面，目前主要常見的量子光源可以粗略分成以下幾種，包含：單光子源（Single-Photon Source, SPS）（Lounis and Orrit, 2005）、先驅型單光子源（Heralded Single Photon Source, HSPS）（Fasel et al., 2004）或是糾纏光子對（Kurtsiefer, Oberparleiter, and Weinfurter, 2001）。其中，單光子源可以利用原子震盪（Kuhn, Hennrich, and Rempe, 2002）與量子阱結構（Pelton et al., 2002）產生，或是利用弱同調光源（Weak Coherence Source, WCS）（Brendel, Gisin, Tittel, and Zbinden, 1999）仿製，而先驅型單光子源則可以利用非線性轉換的原理，由非線性晶體產生；另一方面，在各項量子光源中，糾纏光子對具有的特性特別令人著迷，如同第貳章所提及，在著名的 EPR Paradox 文章中，愛因斯坦等人利用思想實驗討論了量子糾纏中，對於定域性定律、實在性的疑似矛盾觀點，但經過六十多年的理論建立、材料創新，與實驗技術的進步，現今糾纏光子對同樣可以利用非線性晶體製作出，配合使用的機制為自發光參量下轉換過程（Spontaneous Parametric Down-Conversion, SPDC）。由於利用 SPDC，配合特定架構所產生的糾纏光子對，必須符合雙光子（Biphoton）的不可分辨性（Indistinguishability）（Dousse et al., 2010），因此，在設計端至實際場域應用時，皆需要更高的技術門檻與環境控制能力，才能使量子系統產生穩定的糾纏光子對光源。根據不同的非線性轉換模式，一般來說可以分成三種類型（Type）：第一種，經由非

線性轉換 SPDC 過程後，如果泵浦光（Pump）、訊號光（Signal）、閒置光（Idler）皆處於相同偏振的狀態時，稱為 Type-0 SPDC；第二種，如果訊號光與閒置光偏振相同，但與泵浦光偏振呈現正交時，稱為 Type-I SPDC；第三種，若訊號光與閒置光之偏振呈現彼此正交時，稱為 Type-II SPDC，由於 Type-II SPDC 之訊號光與閒置光具有偏振正交的關聯特性，此類 SPDC 之光子對常稱為偏振相關光子對（Polarization-Correlated Photon-Pairs），常見於各項量子偏振糾纏態檢驗的實驗中。對於量子對之不可分辨的特性實驗，常見的方法就是利用 50：50 分光鏡，將平均分光的光子對，利用雙光子干涉法（Two-Photon Interference），檢驗其 HOM 現象（Hong, Ou, and Mandel, 1987），利用分析 HOM 圖，可以估計光子對的不可分辨的機率。另外，在量子偏振糾纏態的檢驗方面，傳統上可以利用量子層析（Quantum State Tomography, QST）的方式（Thew, Nemoto, White, and Munro, 2002）進行，QST 能夠檢驗量子態的純度（Purity）與狀態機率分布係數，其量測方法為利用兩組單光子偵測器與時間數位耦合器（Time-to-Digital Convertor, TDC）針對光子對進行分光與偏振選擇性的巧合計數（Coincidence Counts）量測與統計，再利用機率統計的方式，重建出光源對應的量子態之密度矩陣（Density Matrix）。

針對偏振量子態的檢驗研究，筆者與國立中央大學光電所陳彥宏教授實驗室所設計製作之積體量子偏振糾纏光源晶片，為利用準相位匹配之鈮酸鋰晶體為載體，通過非線性效應產生之光子量子偏振相關的特性，藉由實驗架構的配置，可以建置出單光子態，亦或是偏振相關的量子雙光子光源。由於鈮酸鋰為具有較高之非線性係數、電光係數、酸鹼高抗性、溫度容忍度高等良好的物理與化學特性，且利用鈮酸鋰晶體發展非線性轉換機制已逾五十年，科學界已積累了大量經驗，鈮酸鋰晶體目前已發展以下多種可積體化之元件，包含：積體雷射光源（Lallier et al., 1991）、低損耗波導元件（Bortz and Fejer, 1991）、高速電光相位調制器（Ghione et al., 1999）、高轉換效率非線性元件（Parameswaran, Route, Kurz, Roussev, Fejer, and Fujimura, 2002）、電光波譜濾波器（Huang, Lin, Chen, and Huang, 2007）、高消光比偏振濾波器（Waters and Fritz, 1992）、電光可調定向耦合器（Papuchon et al., 1975）、積體多功能元件（Suchoski, Findakly, and Leonberger, 1988）等。因此，近年來大量文獻開始深入研究鈮酸鋰晶體中光參量下轉換之光子偏振相關效應，其原理為由於 SPDC 過程係由相同泵浦母體光分裂之訊號光與閒置光，於光子量子糾纏實驗上，通過特定的實驗架構下，可發現其訊號光與閒置光具有糾纏特性，配合上述之鈮酸鋰可積體化之特性，積體化的量子光源元件將可能由鈮酸鋰為基板所實現。在此，筆者與團隊開發的量子光源晶片介紹如下。

一、積體量子偏振糾纏光源晶片

本研究結合國立中央大學非線性積體雷射光子（Nonlinear Integrated Laser Photonics, NILP）實驗室之鈮酸鋰波導與極化反轉技術與澳洲國立大學（The Australian National University, ANU）非線性物理中心（Nonlinear Physics Center, NPC）之糾纏光子實驗與分析技術，共同設計出世界第一個同時具有偏振相關光子對產生與頻譜絕熱空間分光之多功能積體化鈦擴散式週期性極化反轉鈮酸鋰波導元件（Multifunctional Integrated Ti-Diffused PPLN Waveguide [MIT-PPLNWG] Devices）。此元件由中央大學光電所 NILP 實驗室製作，並至

ANU 的 NPC 實驗室進行實驗與分析。本晶片除了提供新式積體化空間波譜濾波功能，並結合積體量子光源的產生機制，利用波導式絕熱耦合器（Adiabatic Couplers, AC）的空間濾波特性，將泵浦母體光與訊號光和閒置光於空間中分開，SPDC 轉換後剩餘的泵浦母體光將於中心波導輸出，但訊號光與閒置光分別於兩側波導輸出，由於泵浦母體光主要能量並未進入兩側波導，使由兩側波導輸出光中來自泵浦母體光比例的變少，由於泵浦母體光在量子糾纏關聯性實驗中為雜訊光，減低其比例，則可提升其訊號光與閒置光量子糾纏之關聯性。根據先導實驗結果，我們發現此特殊結構具有高製程誤差容忍度與極寬之高穿透率之波譜寬度（平均穿透率：> 90 ~ 98%、波譜波寬：> 100 ~ 200 nm），相對於低製程容忍度、低穿透波譜寬度之定向耦合器元件，此絕熱耦合波導元件將提供更高之量子態波長與製程容忍度（Chung et al., 2015）。

在晶片設計中，我們將光參量下轉換工作於其簡併點（Degeneracy Point），使泵浦光、訊號光與閒置光波長分別設計為：785 nm、1,570 nm 與 1,570 nm，在實際設計時，必須考慮鈦擴散式波導產生之不同波長下之模態等效折射率，建立一鈦擴散式波導之等效折射率與溫度於不同波長之響應關係，為一重要目標。利用正確的等效折射率來進行設計滿足準相位匹配光參量產生的結構週期，才能有效達成高轉換效率的 SPDC 過程，以增強訊號光對泵浦光源之信噪比（Signal-to-Noise Ratio, SNR），以提高在量子糾纏實驗中的關聯性。在此晶片中，其元件第二段即是用來解決此殘餘泵浦光之干擾，我們能使用特殊設計之絕熱耦合波導結構，利用波導間耦合效率與波長的相依關係，進而使短波長的泵浦光與長波長的訊號光、閒置光於空間中分開，使泵浦光藉由中間波導輸出，而訊號光、閒置光藉由波長空間分光的特性，由兩側波導出口輸出（Chung et al., 2019）。利用此設計，ANU 團隊已利用模擬預期了在經過此波長相依之空間濾波段後，量測量子糾纏效益時來自泵浦光之干擾將大幅減少，其模擬結果指出此結構之泵浦光濾波強度可達 72 dB（Wu, Solntsev, Neshev, and Sukhorukov, 2014）。

在積體量子光源晶片的驗證方面，主要由筆者於 2016 ~ 2017 年間，至 ANU 進行量子偏振糾纏態的實驗驗證，並與 ANU 團隊共同進行超微型 QST 實驗的研究。ANU 團隊提出了利用一種特殊設計的超表面結構（Metasurface, MS），此 MS 可以利用空間偏振相依分光的概念，直接將整個 QST 所需要的數十公分等級的偏振選擇架構，整合於單片奈米尺度的超表面上，配合筆者與陳教授團隊的公分等級的積體量子光源晶片作為光源，整體大幅縮小了傳統 QST 實驗所需要的元件數量與空間，並於 2018 年與合作夥伴 Kai Wang 等人，將以上實驗與分析結果共同列名發表於 *Science* 期刊中（Wang et al., 2018）。

但在那項研究中，我們發現一個困難點，就是我們選用的 Type-II SPDC 量子光源之偏振糾纏純度不如預期，僅 66.82%。根據實驗分析，我們判斷其問題點除了來自於各元件的偏振不確定性之外，由於我們利用的積體量子偏振糾纏光源晶片，其 Type-II SPDC 簡併態附近的訊號頻寬也相當窄（~ 1 nm），且由於為了保持較高的量子純度，我們選用的量子光源強度極低，導致一般市售的光學頻譜分析儀難以針對 Type-II SPDC 簡併態附近的訊號光與閒置光之頻譜重疊性直接量測確認，導致系統有可能會因為溫度不穩定或是泵浦雷射波長不穩定，使得 SPDC 訊號光與閒置光在頻率上的分布錯移，進而產生部分光子對可以分辨（Partially Distinguishable）的結果，使得那些可分辨區域並不滿足量子不可分辨性，導致量

子單光子純度下降，如圖 8 之量子偏振態分布密度矩陣的實際量測結果所示。另一方面，若使用 Type-0 SPDC 的情形下，雖然泵浦光、訊號光、閒置光之偏振皆相同，使得相位匹配條件限制較 type-II SPDC 來的寬鬆，但若需要製作窄頻 SPDC 糾纏光子對之光源，則需要利用頻譜濾波器（Spectrum Filter）進行頻率濾光，因此，相比於 Type-II SPDC 光源，Type-0 SPDC 光源將損失了大量的非正確頻率的光子對，導致實際整體量子效率下降。

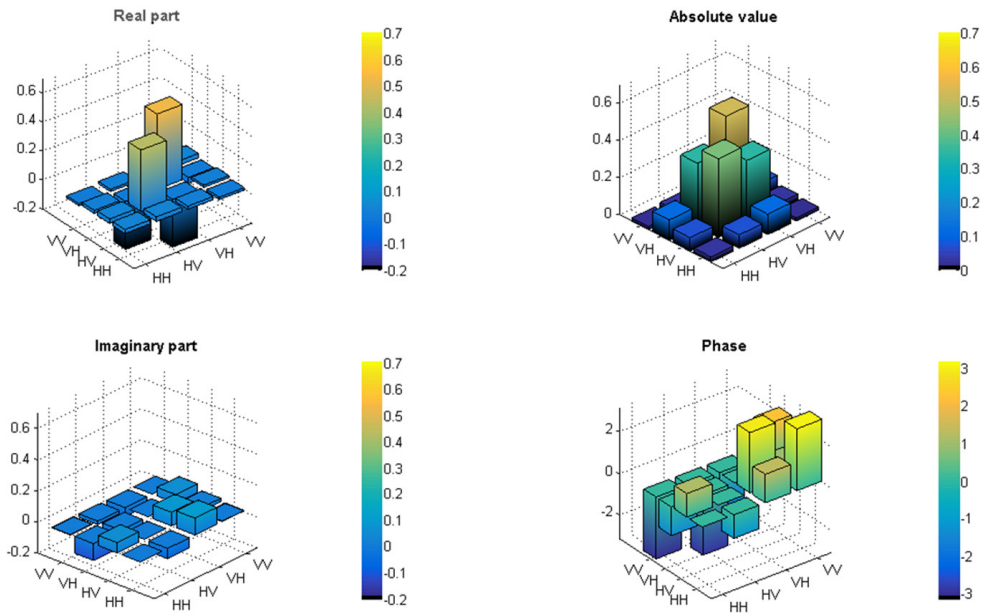

圖 8　利用超表面重建的量子偏振態之密度矩陣

資料來源：作者自行繪製整理。

因此，於本團隊 2019 年的最新研究中，我們將同類型的積體量子光源晶片送至德國 Jena 大學（Friedrich-Schiller-Universität Jena）的 Institute of Applied Physics 中心，特別進行針對窄頻寬、高亮度之 Type-II SPDC 偏振糾纏之光子對進行簡併態頻譜特徵的研究。我們利用可調雷射與配合傳統合頻（Sum-Frequency Generation, SFG）的檢驗方式，根據 SFG-SPDC 類比法（Lenzini et al., 2018），重建近簡併態（Near-Degeneracy）附近的 SPDC 頻譜，整合傳統 SFG 與量子 SPDC 兩種量測結果，我們可以更清楚的一覽 Type-II SPDC 在近簡併態附近的頻譜分布，提高偏振糾纏之光子對不可分辨的機率。根據以上的研究結果，未來利用傳統 SFG 就可以估計 SPDC 頻寬之穩定性，並利用此方式進行同步頻譜監控（Synchronous Spectrum Monitoring），並可通過動態的回饋溫度補償與泵浦雷射波長飄移補償等方式，提高動態長時間的量子糾纏對的穩定純度，若未來能整合光源穩定系統與動態回饋系統，將正交訊號光與閒置光頻譜之重合性能夠動態調整與即時校正，可望提高糾纏態的動態純度。

另一方面，由於利用非線性轉換機制所產生糾纏光子對，其為了避免多光子關聯態（Multi-Photon Correlated States）的現象，一般系統都操作在較低的轉換效率之下，盡可能地將光源

操作在雙光子態（Two-Photon States），因此，SPDC 轉換後，常見剩餘高強度的泵浦光需要被濾除，過去常見的方法是利用在光源後端加上短波長濾波器，將短波長之泵浦光由系統中移除，但通常此類方案需要較大的外部濾波器。筆者與陳彥宏教授的團隊，於 2015 開始，與 ANU 進行了一系列的積體泵浦光濾波晶片元件的研究，我們在積體光路上，利用特殊設計的絕熱耦合結構，將泵浦濾光（Chung et al., 2015）、強度分光（Chung et al., 2017）與偏振分光等機制整合於單一積體光電晶片中（Chung et al., 2019），將過去需要數十公分等級的濾波與偏振分光系統，大幅度整合至 2 ~ 5 公分等級之單一晶片中。以上方案使用之積體量子光源元件，皆具有公釐（mm）至公分（cm）等級的尺度，且所需泵浦雷射光源強度僅約 mW 等級，因此，研究結果皆可直接應用於未來使用偏振糾纏光源作為積體量子通訊光源的平臺，對未來更嚴苛的量子通訊應用場域，提供穩定的量子偏振糾纏光源的方案。

由於積體光路選用之光學波導可以對於標準 1,550-nm 單模光纖或保偏光纖，具有良好的光學耦合特性，其光學耦合損耗大約僅在 0.5 dB/face 等級，對於未來設計與整合積體量子光源元件與積體量子光路（Quantum Integrated Optical Circuits, QIOC）或是積體量子平臺（Integrated Quantum Platform, IQP）、量子系統單晶片（Quantum System-on-a-Chip, QSoC）等願景來說，具有極大的吸引性與特殊競爭力。筆者與團隊所規劃的 IQP 的概念如圖 9 左圖所示，僅分成三個部分，包含泵浦光源、IQP 晶片與單光子偵測系統。其中，IQP 晶片為利用單一或異質材料將數個量子光源需要的功能整合於單一晶片中，其中重要功能包含：泵浦光偏振控制器（Polarization Controller, PC）、量子光源轉換（SPDC）器、泵浦光濾波器（Pump Filter）、訊號光與閒置光分光器（Splitter）、時間延遲補償器（Time-Delay Compensator, TC）、偏振選擇器（Selective-Polarization, SP）、偏振分析器（Polarization Analyzer, PA）、

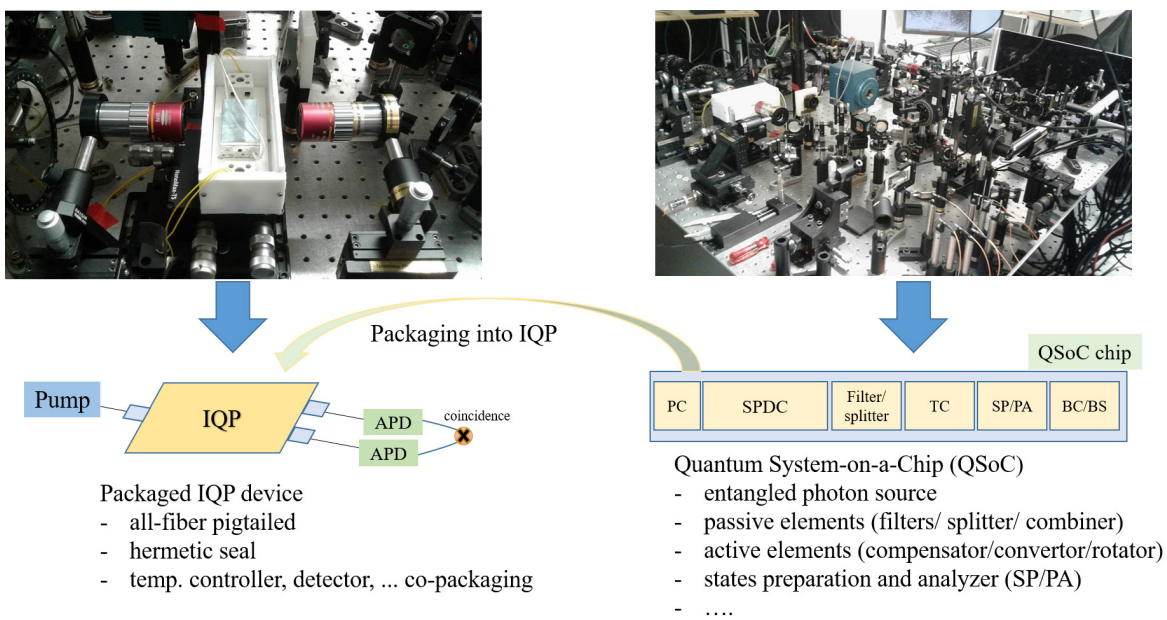

圖 9　IQP 的整合晶片概念

資料來源：作者自行繪製整理。

和光器（Beam Combiner, BC）與 50/50 分光器（BS）。

對於量子偏振糾纏的應用，尤其在通訊應用方面，如 QKD 中 BBM92 等利用糾纏本質的通訊協定，未來若利用積體量子光源晶片與整合型的 IQP，除了能穩定量子光源系統之糾纏光子對的產生機制之外，並可望提高量子傳輸之正確性。根據文獻中指出，利用分光鏡製作出來的量子糾纏狀態，若使用單純的 Bell 不等式原理進行 QKD，無法檢驗密鑰傳輸過程中是否有被竊聽（Caro and Garuccio, 1994; Eberhard, 1993），因此，在實用化量子糾纏特性的通訊協定時，亦可以參考誘導態的分發方式，加上時間序列糾纏光子對（Time-Bin Entangled Photon-Pair）的設計（Honjo et al., 2008），配合於收發兩端的干涉儀的建置，將密鑰可能被竊聽的疑慮降低。

配合實際 QKD 系統所需物理尺度的縮減，將 QKD 系統能運作於更廣泛的應用環境之中，如將微型化的 QKD 系統安裝於移動式通訊裝置或是小型基地站，加上量子中繼器（Quantum Repeater）的實用化，將量子系統由艱深的科學研究領域，逐步拉近至使用者的應用終端，進而提升整體量子通訊系統的實用價值。

伍、結語

本文由回顧了 QKD 的發展歷程，並簡述量子分發系統背後所應用的兩大量子原理，根據不同的應用原理，QKD 系統可基於測不準原理或是量子糾纏特性進行設計建立，文中除回顧現今國際上相關廠商相關資訊之外，並簡介了五種常見的 QKD 所使用的通訊協定架構，如：BB84、BBM92、Decoy State、COW、DPS-QKD 等。於本文第肆章，介紹了筆者與合作團隊發展中的積體量子光源相關技術，並提出 IQP 的概念，此 IQP 將朝著使 QKD 系統進行微型化改良的目標努力，將過去似乎過於笨重而不切實際的移動式量子通訊設備，嘗試將 QKD 系統所需的各種單元，利用分段異質整合的概念，整合並積體於更簡易輕便型的下一代微型化量子通訊系統中。

參考文獻

Abushgra A., and Elleithy K., 2015, “Initiated Decoy States in Quantum Key Distribution Protocol by 3 Ways Channel,” in *Proceedings of the 2015 Long Island Systems, Applications and Technology*, New York, NY: IEEE. doi:10.1109/LISAT.2015.7160178

Abushgra A., and Elleithy K., 2016, “QKDP’s Comparison Based Upon Quantum Cryptography Rules,” in *Proceedings of the 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY: IEEE. doi:10.1109/LISAT.2016.7494101

Bell J. S., 1964, “On the Einstein Podolsky Rosen Paradox,” *Physics Physique Fizika*, 1(3), 195-200. doi:10.1103/PhysicsPhysiqueFizika.1.195

Bennett C. H., 1992, “Quantum Cryptography Using Any Two Nonorthogonal States,” *Physical*

Review Letters, 68(21), 3121-3124. doi:10.1103/PhysRevLett.68.3121

Bennett C. H., and Brassard G., 1984, An Update on Quantum Cryptography, in G. R. Blakley and D. Chaum (Eds.), *Advances in Cryptology*, Heidelberg, Germany: Springer. pp. 475-480. doi:10.1007/3-540-39568-7_39

Bennett C. H., and Brassard G., 2014, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science*, 560, 7-11. doi:10.1016/j.tcs.2014.05.025

Bennett C. H., Brassard G., and Mermin N. D., 1992, "Quantum Cryptography without Bell's Theorem," *Physical Review Letters*, 68(5), 557-559. doi:10.1103/PhysRevLett.68.557

Bortz M. L., and Fejer M. M., 1991, "Annealed Proton-Exchanged $LiNbO_3$ Waveguides," *Optics Letters*, 16(23), 1844-1846. doi:10.1364/OL.16.001844

Brendel J., Gisin N., Tittel W., and Zbinden H., 1999, "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication," *Physical Review Letters*, 82(12), 2594. doi:10.1103/PhysRevLett.82.2594

Caro D. L., and Garuccio A., 1994, "Reliability of Bell-Inequality Measurements Using Polarization Correlations in Parametric-Down-Conversion Photon Sources," *Physical Review A*, 50(4), R2803-R2805. doi:10.1103/physreva.50.r2803

Chung H.-P., Huang K.-H., Wang K., Yang S.-L., Yang S.-Y., Sung C.-I., Solntsev A. S., Sukhorukov A. A., Neshev D. N., and Chen Y.-H., 2017, "Asymmetric Adiabatic Couplers for Fully-Integrated Broadband Quantum-Polarization State Preparation," *Scientific Reports*, 7(1), 16841. doi:10.1038/s41598-017-17094-7

Chung H.-P., Huang K.-H., Yang S.-L., Chang W. K., Wu C. W., Setzpfandt F., Pertsch T., Neshev D. N., and Chen Y. H., 2015, "Adiabatic Light Transfer in Titanium Diffused Lithium Niobate Waveguides," *Optics Express*, 23(24), 30641-30650. doi:10.1364/OE.23.030641

Chung H.-P., Lee C.-H., Huang K.-H., Yang S.-L., Wang K., Solntsev A. S., Sukhorukov A. A., Setzpfandt F., and Chen Y.-H., 2019, "Broadband On-Chip Polarization Mode Splitters in Lithium Niobate Integrated Adiabatic Couplers," *Optics Express*, 27(2), 1632-1645. doi:10.1364/OE.27.001632

Curty M., and Lütkenhaus N., 2005, "Intercept-Resend Attacks in the Bennett-Brassard 1984 Quantum Key Distribution Protocol With Weak Coherent Pulses," *Physical Review A*, 71(6), 062301. doi:10.1103/PhysRevA.71.062301

Dousse A., Suffczyński J., Beveratos A., Krebs O., Lemaître A., Sagnes I., Bloch J., Voisin P., and Senellart P., 2010, "Ultrabright Source of Entangled Photon Pairs," *Nature*, 466(7303), 217-220. doi:10.1038/nature09148

Dušek M., Haderka, O., and Hendrych, M., 1999, "Generalized Beam-Splitting Attack in Quantum Cryptography with Dim Coherent States," *Optics Communications*, 169(1-6), 103-108. doi:10.1016/S0030-4018(99)00419-8

Eberhard P. H., 1993, "Background Level and Counter Efficiencies Required for a Loophole-Free Einstein-Podolsky-Rosen Experiment," *Physical Review A*, 47(2), R747-R750. doi:10.1103/physreva.47.r747

Einstein A., Podolsky B., and Rosen N., 1935, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review*, 47(10), 777-780. doi:10.1103/PhysRev.47.777

Ekert A. K., 1991, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, 67(6), 661-663. doi:10.1103/PhysRevLett.67.661

Elliott C., 2018, The DARPA Quantum Network, in A. V. Sergienko (Ed.), *Quantum Communications and Cryptography*, Boca Raton, FL: CRC Press. pp. 83-102. doi:10.1201/9781315221120

Fasel S., Alibart O., Tanzilli S., Baldi P., Beveratos A., Gisin N., and Zbinden H., 2004, "High-Quality Asynchronous Heralded Single-Photon Source at Telecom Wavelength," *New Journal of Physics*, 6(1), 163. doi:10.1088/1367-2630/6/1/163

Fujiwara M., Waseda A., Nojima R., Moriai S., Ogata W., and Sasaki M., 2016, "Unbreakable Distributed Storage with Quantum Key Distribution Network and Password-Authenticated Secret Sharing," *Scientific Reports*, 6, 28988. doi:10.1038/srep28988

Ghione G., Goano M., Madonna G. L., Omegna G., Pirola M., Bosso S., Frassati D., and Perasso A., 1999, "Microwave Modeling and Characterization of Thick Coplanar Waveguides on Oxide-Coated Lithium Niobate Substrates for Electrooptical Applications," in *Proceedings of the IEEE Transactions on Microwave Theory and Techniques*, 47(12), 2287-2293. doi:10.1109/22.808972

Gisin N., Ribordy G., Tittel W., and Zbinden H., 2002, "Quantum Cryptography," *Reviews of Modern Physics*, 74(1), 145. doi:10.1103/RevModPhys.74.145

Hong C. K., Ou Z. Y., and Mandel L., 1987, "Measurement of Subpicosecond Time Intervals Between Two Photons by Interference," *Physical Review Letters*, 59(18), 2044-2046. doi:10.1103/PhysRevLett.59.2044

Honjo T., Nam S. W., Takesue H., Zhang Q., Kamada H., Nishida Y., Tadanaga O., Asobe M., Baek B., Hadfield R., Miki S., Fujiwara M., Sasaki M., Wang Z., Inoue K., and Yamamoto Y., 2008, "Long-Distance Entanglement-Based Quantum Key Distribution Over Optical Fiber," *Optics Express*, 16(23), 19118-19126. doi:10.1364/OE.16.019118

Horodecki R., Horodecki P., Horodecki M., and Horodecki K., 2009, "Quantum Entanglement," *Reviews of Modern Physics*, 81(2), 865. doi:10.1103/RevModPhys.81.865

Huang C. Y., Lin C. H., Chen Y. H., and Huang Y. C., 2007, "Electro-Optic Ti: PPLN Waveguide as Efficient Optical Wavelength Filter and Polarization Mode Converter," *Optics Express*, 15(5), 2548-2554. doi:10.1364/OE.15.002548

Hugues-Salas E., Ntavou F., Ou Y., Kennard J. E., White C., Gkounis D., Nikolovgenis K., Kanellos

G., Erven C., Lord A., Nejabati R., and Simeonidou D., 2018, "Experimental Demonstration of DDoS Mitigation Over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN)," in *Proceedings of 2018 Optical Fiber Communications (OFC) Conference*, San Diego, CA: IEEE. doi:10.1364/OFC.2018.M2A.6

Inagaki T., Matsuda N., Tadanaga O., Asobe M., and Takesue H., 2013, "Entanglement Distribution Over 300 km of Fiber," *Optics Express*, 21(20), 23241-23249. doi:10.1364/OE.21.023241

Inoue K., Waks E., and Yamamoto Y., 2002, "Differential Phase Shift Quantum Key Distribution," *Physical Review Letters*, 89(3), 037902. doi:10.1103/PhysRevLett.89.037902

International Data Corporation, 2014/4, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," *IDC*, https://www.emc.com/leadership/digital-universe/2014iview/index.htm (accessed August 25, 2019).

Khan M. M., Murphy M., and Beige A., 2009, "High Error-Rate Quantum Key Distribution for Long-Distance Communication," *New Journal of Physics*, 11(6), 063043. doi:10.1088/1367-2630/11/6/063043

Khasminskaya S., Pyatkov F., Słowik K., Ferrari S., Kahl O., Kovalyuk V., Rath P., Vetter A., Hennrich F., Kappes M. M., Gol'tsman G., Korneev A., Rockstuhl C., Krupke R., and Pernice W. H. P., 2016, "Fully Integrated Quantum Photonic Circuit with an Electrically Driven Light Source," *Nature Photonics*, 10(11), 727-732. doi:10.1038/nphoton.2016.178

Koashi M., and Imoto N., 1998, "No-Cloning Theorem of Entangled States," *Physical Review Letters*, 81(19), 4264. doi:10.1103/PhysRevLett.81.4264

Kuhn A., Hennrich M., and Rempe G., 2002, "Deterministic Single-Photon Source for Distributed Quantum Networking," *Physical Review Letters*, 89(6), 067901. doi:10.1103/PhysRevLett.89.067901

Kurtsiefer C., Oberparleiter M., and Weinfurter H., 2001, "High-Efficiency Entangled Photon Pair Collection in Type-II Parametric Fluorescence," *Physical Review A*, 64(2), 023802. doi:10.1103/PhysRevA.64.023802

Lallier E., Pocholle J. P., Papuchon M. R., He Q., de Micheli M. P., Osstrowsky D. B., Grèzes-Besset C., and Pelletier E. P., 1991, "Integrated Nd:MgO:$LiNbO_3$ FM Mode-Locked Wave-Guide Laser," *Electronics Letters*, 27(11), 936-937. doi:10.1049/el:19910585

Lenzini F., Poddubny A. N., Titchener J., Fisher P., Boes A., Kasture S., Haylock B., Villa M., Mitchell A., Solntsev A. S., Sukhorukov A. A., and Lobino M., 2018, "Direct Characterization of a Nonlinear Photonic Circuit's Wave Function with Laser Light," *Light: Science & Applications*, 7(1), 17143. doi:10.1038/lsa.2017.143

Liao S.-K., Cai W.-Q., Handsteiner J., Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M., Deng L., Xi T., Ma L., Hu T., Li L., Liu N.-L., Koidl F., Wang P., Chen Y.-A., Wang X.-B., Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang J.-Y., Zeilinger A., and Pan J.-W., 2018,

"Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters*, 120(3), 030501. doi:10.1103/PhysRevLett.120.030501

Lo H.-K., Ma X., and Chen K., 2005, "Decoy State Quantum Key Distribution," *Physical Review Letters*, 94(23), 230504. doi:10.1103/PhysRevLett.94.230504

Lounis B., and Orrit M., 2005, "Single-Photon Sources," *Reports on Progress in Physics*, 68(5), 1129. doi:10.1088/0034-4885/68/5/R04

Lütkenhaus N., and Jahma M., 2002, "Quantum Key Distribution with Realistic States: Photon-Number Statistics in the Photon-Number Splitting Attack," *New Journal of Physics*, 4(1), 44. doi:10.1088/1367-2630/4/1/344

Papuchon M., Combemale Y., Mathieu X., Ostrowsky D. B., Reiber L., Roy A. M., Sejourne B., and Werner M., 1975, "Electrically Switched Optical Directional Coupler: Cobra," *Applied Physics Letters*, 27(5), 289-291. doi:10.1063/1.88449

Parameswaran K. R., Route R. K., Kurz J. R., Roussev R. V., Fejer M. M., and Fujimura M., 2002, "Highly Efficient Second-Harmonic Generation in Buried Waveguides Formed by Annealed and Reverse Proton Exchange in Periodically Poled Lithium Niobate," *Optics Letters*, 27(3), 179-181. doi:10.1364/OL.27.000179

Peev M., Pacher C., Alléaume R., Barreiro C., Bouda J., Boxleitner W., Debuisschert T., Diamanti E., Dianati M., Dynes J. F., Fasel S., Fossier S., Fürst M., Gautier J.-D., Gay O., Gisin N., Grangier P., Happe A., Hasani Y., Hentschel M., Hübel H., Humer G., Länger T., Legré M., Lieger R., Lodewyck J., Lorünser T., Lütkenhaus N., Marhold A., Matyus T., Maurhart O., Monat L., Nauerth S., Page J.-B., Poppe A., Querasser E., Ribordy G., Robyr S., Salvail L., Sharpe A.W., Shields A. J., Stucki D., Suda M., Tamas C., Themel T., Thew R. T., Thoma Y., Treiber A., Trinkler P., Tualle-Brouri R., Vannel F., Walenta N., Weier H., Weinfurter H., Wimberger I., Yuan Z. L., Zbinden H., and Zeilinger A., 2009, "The SECOQC Quantum Key Distribution Network in Vienna," *New Journal of Physics*, 11(7), 075001. doi:10.1088/1367-2630/11/7/075001

Pelton M., Santori C., Vučković J., Zhang B., Solomon G. S., Plant J., and Yamamoto Y., 2002, "Efficient Source of Single Photons: A Single Quantum Dot in a Micropost Microcavity," *Physical Review Letters*, 89(23), 233602. doi:10.1103/PhysRevLett.89.233602

Renner R., 2008, "Security of Quantum Key Distribution," *International Journal of Quantum Information*, 6(1), 1-127. doi:10.1142/S0219749908003256

Robinson S., 2003, "Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders," *SIAM News*, 36(5), 1-4.

Sasaki M., Fujiwara M., Ishizuka H., Klaus W., Wakui K., Takeoka M., Miki S., Yamashita T., Wang Z., Tanaka A., Yoshino K., Nambu Y., Takahashi S., Tajima A., Tomita A., Domeki T., Hasegawa T., Sakai Y., Kobayashi H., Asai T., Shimizu K., Tokura T., Tsurumaru T., Matsui M., Honjo T., Tamaki K., Takesue H., Tokura Y., Dynes J. F., Dixon A. R., Sharpe A. W., Yuan Z. L.,

Shields A. J., Uchikoga S., Legré M., Robyr S., Trinkler P., Monat L., Page J.-B., Ribordy G., Poppe A., Allacher A., Maurhart O., Länger T., Peev M., and Zeilinger A., 2011, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," *Optics Express*, 19(11), 10387-10409. doi:10.1364/OE.19.010387

Scarani V., Acín A., Ribordy G., and Gisin N., 2004, "Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, 92(5), 057901. doi:10.1103/PhysRevLett.92.057901

Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N., and Peev M., 2009, "The Security of Practical Quantum Key Distribution," *Reviews of Modern Physics*, 81(3), 1301. doi:10.1103/RevModPhys.81.1301

Scheidl T., Ursin R., Fedrizzi A., Ramelow S., Ma X.-S., Herbst T., Prevedel R., Ratschbacher L., Kofler J., Jennewein T., and Zeilinger A., 2009, "Feasibility of 300 km Quantum Key Distribution with Entangled States," *New Journal of Physics*, 11(8), 085002. doi:10.1088/1367-2630/11/8/085002

Serna E. H., 2013/11/12, "Quantum Key Distribution From a Random Seed," *arXiv*, https://arxiv.org/abs/1311.1582 (accessed July 7, 2019).

Shor P. W., and Preskill J., 2000, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, 85(2), 441-444. doi:10.1103/PhysRevLett.85.441

Stucki D., Barreiro C., Fasel S., Gautier J.-D., Gay O., Gisin N., Thew R., Thoma Y., Trinkler P., Vannel F., and Zbinden H., 2009, "Continuous High Speed Coherent One-Way Quantum Key Distribution," *Optics Express*, 17(16), 13326-13334. doi:10.1364/OE.17.013326

Suchoski P. G., Findakly T. K., and Leonberger F. J., 1988, "$LiNbO_3$ Integrated Optical Components for Fiber Optic Gyroscopes," *Integrated Optical Circuit Engineering VI*, 993, 240-245. doi:10.1117/12.960095

Thew R. T., Nemoto K., White A. G., and Munro W. J., 2002, "Qudit Quantum-State Tomography," *Physical Review A*, 66(1), 012303. doi:10.1103/PhysRevA.66.012303

Ursin R., Tiefenbacher F., Schmitt-Manderbach T., Weier H., Scheidl T., Lindenthal M., Blauensteiner B., Jennewein T., Perdigues J., Trojek P., Ömer B., Fürst M., Meyenburg M., Rarity J., Sodnik Z., Barbieri C., Weinfurter H., and Zeilinger A., 2007, "Entanglement-Based Quantum Communication Over 144 km," *Nature Physics*, 3(7), 481-486. doi:10.1038/nphys629

Wang K., Titchener J. G., Kruk S. S., Xu L., Chung H.-P., Parry M., Kravchenko I. I., Chen Y.-H., Solntsev A. S., Kivshar Y. S., Neshev D. N., and Sukhorukov A. A., 2018, "Quantum Metasurface for Multiphoton Interference and State Reconstruction," *Science*, 361(6407), 1104-1108. doi:10.1126/science.aat8196

Wang Y., Wang H., Li Z., and Huang J., 2009, "Man-in-the-Middle Attack on BB84 Protocol and Its Defence," in *Proceedings of 2009 2nd IEEE International Conference on Computer Science*

and Information Technology, Beijing, China: IEEE. doi:10.1109/ICCSIT.2009.5234678

Waters J. P., and Fritz D. J., 1992, "White Light Interferometer for Measuring Polarization Extinction Ratio," *Laser Interferometry IV: Computer-Aided Interferometry*, 1553, 14-22. doi:10.1117/12.135287

Wiesner S., 1983, "Conjugate Coding," *ACM Sigact News*, 15(1), 78-88. doi:10.1145/1008908.1008920

Wootters W. K., 1998, "Entanglement of Formation of an Arbitrary State of Two Qubits," *Physical Review Letters*, 80(10), 2245-2248. doi:10.1103/PhysRevLett.80.2245

Wu C. W., Solntsev A. S., Neshev D. N., and Sukhorukov A. A., 2014, "Photon Pair Generation and Pump Filtering in Nonlinear Adiabatic Waveguiding Structures," *Optics Letters*, 39(4), 953-956. doi:10.1364/OL.39.000953

Yin J., Cao Y., Li Y.-H., Liao S.-K., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li B., Dai H., Li G.-B., Lu Q.-M., Gong Y.-H., Xu Y., Li S.-L., Li F.-Z., Yin Y.-Y., Jiang Z.-Q., Li M., Jia J.-J., Ren G., He D., Zhou Y.-L., Zhang X.-X., Wang N., Chang X., Zhu Z.-C., Liu N.-L., Chen Y.-A., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., and Pan J.-W., 2017, "Satellite-Based Entanglement Distribution Over 1,200 Kilometers," *Science*, 356(6343), 1140-1144. doi:10.1126/science.aan3211