前瞻科技與管理　13 卷 1 期，47-55 頁（2024 年 11 月）
Journal of Advanced Technology and Management Vol. 13, No. 1, pp. 47-55 (November, 2024)
DOI:10.6193/JATM.202411_13(1).0003

量子通訊系統發展趨勢、挑戰及對策

褚志崧 *

國立清華大學物理學系教授

摘 要

量子通訊不僅能提供密鑰的遠端傳送，也能防止密鑰在傳送過程中被竊取，是未來的網路抵抗量子電腦攻擊的利器，其應用涵蓋金融財務、電子商務和個資傳遞。本文介紹量子通訊系統的基本架構、量子通訊的發展現況和未來挑戰。

關鍵詞：量子通訊、量子密鑰分發、資安、量子電腦、光子

* 通訊作者：褚志崧
電子郵件：cschuu@phys.nthu.edu.tw
（收件日期：2024 年 8 月 2 日；修正日期：2024 年 8 月 8 日；接受日期：2024 年 8 月 8 日）

Journal of Advanced Technology and Management Vol. 13, No. 1, pp. 47-55 (November, 2024)
DOI:10.6193/JATM.202411_13(1).0003

Development and Challenges of Quantum Communication

Chih-Sung Chuu*

Professor, Department of Physics, National Tsing Hua University

Abstract

Quantum communication provides a secure way of distributing keys against the eavesdropping or attacks from quantum computers. Its applications range from finance and electronic commerce to the protection of personal information. In this article, we describe the essential elements of quantum communication as well as the current status and challenges of developing quantum communication.

Keywords: quantum communication, quantum key distribution, information security, quantum computer, photon

* Corresponding Author: Chih-Sung Chuu
E-mail: cschuu@phys.nthu.edu.tw

壹、緒論

近年來隨著物聯網的迅速發展，網路的安全性顯得更加重要。理想的網路安全應該有長期的安全性，讓有心人士無法保存竊取來的機密文件，待有方法可解密時，再進行文件的解密。不過，目前的網路通訊安全大多是依賴數學的複雜性，是有條件性的安全，並無法提供長期的保護。如果未來的電腦運算速度大幅提升，我們的網路通訊安全將會面臨極大的挑戰。這種擔心並非杞人憂天，2019 年谷歌（Google）宣布旗下研發的「量子電腦」僅花 200 秒即完成全球最快的超級電腦需要 1 萬年才能處理的數學運算（Arute et al., 2019）。

不過絕對安全的網路通訊也不是天方夜譚，如果加密用的密鑰可以安全的分發到使用者手中，再利用密碼學裡的「一次性密碼本」（Vernam, 1926），將能達成絕對安全的通訊方式，而安全的密鑰分發能以量子通訊的「量子密鑰分發」（Bennett and Brassard, 1984）技術實現。量子密鑰分發於 50 年前在美國貝爾實驗室首次得到驗證後（Bennett, Bessette, Brassard, Salvail, and Smolin, 1992），至今已數度使用於商業應用中。2007 年的瑞士地方選舉（Marks, 2007）、2010 年的足球世界盃（Johnston, 2010），或是中國的部分金融機構（Chen et al., 2021）都曾使用量子密鑰分發保護機密資料的傳遞。近年來美國、中國、英國、奧地利和日本都積極的興建大規模的量子加密通訊網路，例如華盛頓特區與波士頓間 800 公里長的量子通訊網路（Whittaker, 2018），或是上海與北京間 2,000 公里長的量子通訊網路（Chen et al., 2021）。

量子密鑰分發被視為實現長期、無條件性網路通訊安全的基石，它是如何達成絕對安全的密鑰分發呢？在量子密鑰分發中，密鑰位元 0 和 1 隨機的被編碼在「光子」的偏振方向或是「光子」脈衝間的相位差。光或電磁波的能量是不連續的，而光子就是最小的單位，光子的偏振方向即電磁波的電場振動方向。光子在量子密鑰分發中完成編碼後，由「量子通道」（如光纖）在使用者間傳遞。接收端先利用單光子偵測器測量光子的偏振方向或脈衝間的相位差，並與發送端比對編碼和量測的方式或「基底」，剔除因使用不同編碼和量測方式而引起的錯誤位元。其餘的位元因為發送端和接收端隨機的編碼和測量，形成一串隨機的 0 和 1 的序列，成為雙方共享且無法被預知的密鑰。這是因為光子擁有「無法被複製」的量子性質（Wootters and Zurek, 1982），所以它們的狀態在傳遞的過程中無法被窺探，而能防範攜帶的位元資訊被第三方竊取或保存。

貳、量子通訊系統

量子通訊系統在選擇硬體或量子密鑰分發協議時，雖然會因不同的應用場域有所不同，但是運作的機制或流程都是相似的。量子通訊系統由「光源」產生單光子或糾纏光子對後，「編碼器」把隨機的位元轉譯到光子的光學特性上。光子經過編碼後，透過「量子通道」（例如大氣或光纖）傳輸，抵達接收端，再由「解碼器」和「單光子偵測器」進行量測並讀取位元。有了測量結果後，使用者利用公用通道（例如一般網路或電話）交換編碼和測量的基底，並進行錯誤碼更正和隱私放大而產生密鑰。因此，所有的量子密鑰分發系統基本上都可拆解

為五個模組：光源、編碼器、量子通道、解碼器和單光子偵測器。以下我們就以這五個模組說明不同的量子密鑰分發系統之相同和相異處。

一、光源

光源在量子密鑰分發裡負責產生單光子或糾纏光子對，以攜帶密鑰位元。無論是單光子或糾纏光子對，光子皆有無法被複製的量子性質，因此都能讓竊聽者無法準確的測量它們的量子態或攜帶的位元。竊聽者任何形式的測量都會造成位元錯誤率升高，進而被發現。除了以量子糾纏為基礎的協議（如 E91 協議〔Ekert, 1991〕和 BBM92 協議〔Bennett, Brassard, and Mermin, 1992〕），單光子光源是量子通訊必備的光源。可以產生單光子的材料系統有很多種類，例如本研究團隊使用的半導體奈米晶體（Feng et al., 2017）、非線性晶體內的自發性降頻轉換（Spontaneous Parametric Down-Conversion）（Wu et al., 2017; Wu, Liu, Chen, and Chuu, 2019; Yang, Lin, Liljestrand, Su, Canalias, and Chuu, 2016），或是冷原子和熱原子系統裡的自發性四波混頻（Spontaneous Four-Wave Mixing）（Chinnarasu et al., 2020; Hsu et al., 2021）。但若考量在室溫下能運作、波長容易調整、系統架設又可微型化及擴充，則「類單光子式」的衰減雷射脈衝和利用非線性晶體的降頻轉換產生預報型（Heralded）單光子是較佳的選擇。前者使用電光光強調變器將衰減後的連續波雷射進行週期性的光強調變，而為了讓每一個週期內的脈衝相位互不相關（有如真正的單光子脈衝），還需使用電光相位調變器對每個脈衝進行隨機的相位調變。此外，若同一個脈衝內含有多於一個光子，則會增加竊聽者成功竊取位元資訊的機率，而破壞量子密鑰分發的安全性，因此必需再調變每個脈衝的光強，產生誘騙態（Decoy State）（Lo, Ma, and Chen, 2005），唯一例外的是 Differential-Phase-Shift（DPS）協議（Inoue, Waks, and Yamamoto, 2002）。若以非線性晶體產生預報型單光子，常見的非線性晶體有 β 型硼酸鋇（Beta Barium Borate, BBO）、鈮酸鋰（Lithium Niobate, LN）或磷酸鈦氧鉀（KTiOPO4, KTP）等塊材或波導晶片。自發性降頻轉換需要的幫浦光可使用脈衝雷射或連續波雷射，而產生的單光子波長則由幫浦波長和晶體的相位匹配溫度決定。非線性晶體內的自發性降頻轉換也是產生糾纏光子的常見方法，單一塊晶體就可以產生在時間和能量上糾纏的光子對。若需要偏振維度上的糾纏，則可以把晶體放入干涉儀內產生偏振糾纏光子對（Fedrizzi, Herbst, Poppe, Jennewein, and Zeilinger, 2007）。而若要配合量子中繼器（Briegel, Dür, Cirac, and Zoller, 1998）延長量子通訊距離，則可以使用共振式降頻轉換（Ou and Lu, 1999）減少糾纏光子的頻寬並提高量子記憶體的儲存效率。我們所發展的單晶雙共振式降頻轉換（Wu et al., 2017, 2019）即以微型化的晶體構造實現共振式降頻轉換。

二、編碼器

量子密鑰分發裡的編碼器負責將位元 0 和 1 轉譯為單光子或糾纏光子的光學特性，常見的光學特性包含光子的偏振方向（可使用於 BB84 協議〔Bennett and Brassard, 1984〕、E91 協議〔Ekert, 1991〕、BBM92 協議〔Bennett, Brassard, et al., 1992〕或 Measurement-Device-Independent（MDI）協議〔Lo, Curty, and Qi, 2012〕）和光子出現的時間區間及脈衝相位差（可使用於 BB84 協議〔Bennett and Brassard, 1984〕、DPS 協議〔Inoue et al., 2002〕、MDI 協議

〔Lo et al., 2012〕或 Coherent-One-Way（CoW）協議〔Stucki et al., 2009〕）。在 E91 協議（Ekert, 1991）或 BBM92 協議（Bennett, Brassard, et al., 1992）中，偏振編碼的隨機性則已經存在於光子對的偏振糾纏，因此不需要再另外進行操作。然而，光子的偏振方向在光纖中容易受光纖的振動或溫度變化而改變，因此多使用於大氣中的傳遞，或以波片（Wave Plate）搭配電光相位調變器、高速偏振控制器進行偏振的回饋控制。反之，產生光子的時間區間和其相位差在光纖中極為穩定，因此是光纖網路常見的編碼方式，不同的時間區間或脈衝間的相位差可以使用高速電光光強和相位波導調變器（調變頻寬可達 40 GHz）產生。

三、量子通道

量子密鑰分發裡的量子通道負責將光子由發送端傳遞至接收端，或由糾纏光子源傳遞至使用者端，常見的量子通道有大氣（自由空間）或光纖。光子在量子通道內傳輸時會有損耗，在光纖中以光波長 1,550 nm 或 1,300 nm 的損耗最低，在自由空間裡則以 800 nm 或 1,550 nm 附近的光波長吸收較低。因為電磁波在自由空間行進會擴散，光子也不例外，因此長距離的自由空間傳輸需要以望遠鏡收發光，並能使用衛星做為中繼站延伸距離。光纖和自由空間相比，則可以讓光子在不擴散的情況下傳遞，量子密鑰分發系統也可以使用已經布好線的通訊用光纖網路，但需在光纖網路的中繼器或放大器處以一段光纖繞道。不過根據我們的研究經驗，偏振在部分戶外光纖中容易受到光纖的振動或溫度變化而改變，而解碼器的部分元件特性又會和偏振相關，因此可以額外使用單頻雷射光監測在光纖內的偏振變化，回饋給系統內的高速偏振控制器，以穩定光子出光纖後的偏振方向。

四、解碼器

量子密鑰分發裡的解碼器負責把編碼器輸出的偏振方向或不同時間區間的脈衝相位差轉譯回位元 0 和 1。不論是以單光子或糾纏光子對攜帶位元，偏振方向的轉譯都可以使用電光相位調變器或高速偏振控制器隨機選擇欲測量的基底（水平／垂直或 ± 45° 偏振方向）。若選擇的基底是正確的，則偏振分光鏡即可將位元 0 和 1 轉譯為空間上不同的行進方向。不同時間區間的脈衝相位差的轉譯則以臂長差為一個時間區間的 Mach-Zehnder 不等臂干涉儀，讓相鄰時間區間內的光子脈衝可以產生干涉。不同的相位差（0 或 π）會使光子由干涉儀的不同出口出來，因此也可以將相位差轉譯為兩個不同的空間模式。因為 Mach-Zehnder 干涉儀的臂長差的穩定度會影響到干涉的對比度，進而影響讀取位元的準確性，可以使用頻率穩定的雷射在同一個干涉儀內產生干涉條紋，再以壓電材料（Piezoelectric Actuator）即時改變其中一臂的光程，予以穩定。

五、單光子偵測器

量子密鑰分發裡的單光子偵測器負責測量解碼後的量子位元，因此決定了密鑰篩選率和密鑰率的高低。目前市售的單光子偵測器有不同的材質和工作原理，以矽為主的雪崩光電二極體在 600 ~ 800 nm 波段的量子效率約為 60 ~ 70%（例如 Excelitas Technologies SPCM AQRH 系列），以 InGaAs/InP 為主的雪崩光電二極體在 1,300 ~ 1,550 nm 波段的量子效率約

為 25 ~ 30%（例如 ID Quantique ID230 系列），而以超導奈米線為主的單光子偵測器則在 1,550 nm 波段有 80 ~ 90% 的量子效率（例如 Single Quantum Eos 系列）。因為 1,550 nm 在光纖中的損耗最低，因此若要提高光纖系統的密鑰率或通訊距離，則超導奈米線單光子偵測器為最佳的選擇。

參、量子通訊的發展現況

臺灣在量子通訊的發展雖然比其他國家晚起步，但近幾年也陸續達成數個重要的里程碑。作者研究團隊在 2019 年以自製的單光子光源完成臺灣首次的戶外量子密鑰分發。我們為了減低戶外環境變化（如溫度擾動或地面振動）對量子金鑰分發的影響，採用差分移相量子密鑰分發協議（Inoue et al., 2002），將每個通訊波段的光子均勻散布在多個脈衝內，並使用相鄰脈衝的相位差進行位元 0 和 1 的編碼。編碼後的光子脈衝進入數公里長的校園光纖網路繞行，待光子脈衝陸續回到實驗室後，我們再以不等臂干涉儀為主的解碼器便對光子進行位元的分析和讀取，並產生一連串隨機位元組成的密鑰，這些安全的密鑰即可以透過「一次性密碼本」（Vernam, 1926）對通訊資料進行加密。不過，若要在現行的網路裡實現量子通訊，仍有許多困難必須克服，例如：如何讓多個用戶進行量子通訊？如何使資料傳輸速度不受限於量子金鑰產率？如何簡化量子系統的操作？

為了建立網路內多用戶的連線，我們在 2023 年以學術光纖網路在國立清華大學和國立陽明交通大學校園建立臺灣第一座量子通訊網路雛型。我們以星狀方式連結所有用戶至單一機房，各用戶先以量子密鑰分發分別和機房建立共享的密鑰，再由機房公開不同密鑰間的同異性，讓不同用戶在不曝露自己的密鑰下更改自己的密鑰，產生與其他用戶共享的密鑰，因此每個用戶只需和機房建立連線即可與遠端用戶進行量子通訊。而為了簡化量子系統的操作，我們採用誘餌態技術（Lo et al., 2005）並以衰減的雷射脈衝取代單光子光源，而產生的密鑰再提供給進階加密標準（Advanced Encryption Standard, AES）做為初始密鑰進行資料的加密，實現量子加密網路電話。量子密鑰分發和進階加密標準的整合不但能強化現行資料傳輸系統的安全性，也使資料傳輸速率不再受限於量子密鑰分發系統的密鑰率。

2024 年我們進一步與中華電信和國家高速網路與計算中心合作，分別完成長達 10 公里和 70 公里的跨縣市量子通訊。與中華電信的合作中，我們使用的商用光纖由新竹市跨越頭前溪到新竹縣，途中行經數個電信機房。為了簡化用戶端的操作並防止量子駭客攻擊偵測器的可能性，我們將操作上較複雜的解碼器放置於量子網路機房，並將用戶端的編碼器模組化，光源也改以輕便的半導體雷射取代。經過衰減的光子脈衝於新竹縣電信服務中心產生後，每個脈衝以兩種不同的時間延遲分別攜帶密鑰位元 0 和 1。這些脈衝經由中華電信的商用光纜，從新竹縣傳送至位於新竹市的接收端進行分析，每分鐘約可生成 10 ~ 20 萬個位元組成的密鑰。與國家高速網路與計算中心的合作中，我們使用的暗光纖由新竹市至新北市，總損耗高達 19 dB，每秒鐘則可產生接近 100 個位元的密鑰，位元錯誤率約為 0.6%。這些密鑰可以直接使用於一次性密碼本的資料加密，或與進階加密標準並用。

肆、長距離量子通訊

光子在光纖內或光纖接點間傳輸時都會有損耗，若量子通訊距離太長，量子密鑰分發在光纖網路內將無法有效產生密鑰，而光子的量子訊號又無法被複製或放大，因此量子通訊在光纖網路內的通訊距離終將受限於光子在光纖網路的整體損耗。為了實現更長距離的量子通訊，量子通道必須採用自由空間，並且可能需要以衛星做為中繼站。不過，少了光纖維持光子在空間的模式，光子在自由空間行進時將會發散，因此必須借助望遠鏡收發光子。以光纖網路實現長距離量子通訊也並非不可行，我們可以使用量子中繼器（Briegel et al., 1998）延伸在量子通道兩端建立量子糾纏的間距，並改用量子糾纏實現量子密鑰分發，如 E91 協議（Ekert, 1991）和 BBM92 協議（Bennett, Brassard, et al., 1992）。不過，量子中繼器的實現除了需要高效率的糾纏光子光源，也需要量子記憶體（Sangouard, Simon, de Riedmatten, and Gisin, 2011）（儲存量子糾纏）和量子頻率轉換器（提升量子記憶體的儲存效率）。

伍、結論與建議

臺灣的量子通訊網路能以我們發展的量子通訊技術為基本架構，在縣市間以長距離的跨縣市量子通訊連結，在各縣市內則以區域型星狀網路進行多個節點間的量子通訊，未來的應用將涵蓋金融財務、電子商務和個資傳遞。這樣的量子通訊網路若再與量子糾纏光源和量子記憶體結合，將有更豐富的應用，例如提升時鐘同步的精準度和望遠鏡天文觀測的解析度（Gottesman, Jennewein, and Croke, 2012），或建立與遠端量子電腦的安全連線，因此發展高效率的糾纏光子光源、量子頻率轉換器、量子記憶體也是極為重要。

參考文獻

Arute F., Arya K., Babbush R., Bacon D., Bardin J. C., Barends R., Biswas R., Boixo S., Brandao F. G. S. L., Buell D. A., Burkett B., Chen Y., Chen Z., Chiaro B., Collins R., Courtney W., Dunsworth A., Farhi E., Foxen B., Fowler A., et al., 2019, "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, 574, 505-510. doi:10.1038/s41586-019-1666-5

Bennett C. H., Bessette F., Brassard G., Salvail L., and Smolin J., 1992, "Experimental Quantum Cryptography," *Journal of Cryptology*, 5, 3-28. doi:10.1007/BF00191318

Bennett C. H., and Brassard G., 1984, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of International Conference on Computers, Systems and Signal Processing*, Bangalore, India: Steering Committee, 175-179.

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

Briegel H.-J., Dür W., Cirac J. I., and Zoller P., 1998, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," *Physical Review Letters*, 81(26), 5932-5935. doi:10.1103/PhysRevLett.81.5932

Chen Y.-A., Zhang Q., Chen T.-Y., Cai W.-Q., Liao S.-K., Zhang J., Chen K., Yin J., Ren J.-G., Chen Z., Han S.-L., Yu Q., Liang K., Zhou F., Yuan X., Zhao M.-S., Wang T.-Y., Jiang X., Zhang L., Liu W.-Y., et al., 2021, "An Integrated Space-to-Ground Quantum Communication Network Over 4,600 Kilometres," *Nature*, 589, 214-219. doi:10.1038/s41586-020-03093-8

Chinnarasu R., Liu C.-Y., Ding Y.-F., Lee C.-Y., Hsieh T.-H., Yu I. A., and Chuu C.-S., 2020, "Efficient Generation of Subnatural-Linewidth Biphotons by Controlled Quantum Interference," *Physical Review A*, 101(6), 063837. doi:10.1103/PhysRevA.101.063837

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

Fedrizzi A., Herbst T., Poppe A., Jennewein T., and Zeilinger A., 2007, "A Wavelength-Tunable Fiber-Coupled Source of Narrowband Entangled Photons," *Optics Express*, 15(23), 15377-15386. doi:10.1364/OE.15.015377

Feng S.-W., Cheng C.-Y., Wei C.-Y., Yang J.-H., Chen Y.-R., Chuang Y.-W., Fan Y.-H., and Chuu C.-S., 2017, "Purification of Single Photons from Room-Temperature Quantum Dots," *Physical Review Letters*, 119(14), 143601. doi:10.1103/PhysRevLett.119.143601

Gottesman D., Jennewein T., and Croke S., 2012, "Longer-Baseline Telescopes Using Quantum Repeaters," *Physical Review Letters*, 109(7), 070503. doi:10.1103/PhysRevLett.109.070503

Hsu C.-Y., Wang Y.-S., Chen J.-M., Huang F.-C., Ke Y.-T., Huang E. K., Hung W., Chao K.-L., Hsiao S.-S., Chen Y.-H., Chuu C.-S., Chen Y.-C., Chen Y.-F., Yu I. A., 2021, "Generation of Sub-MHz and Spectrally-Bright Biphotons from Hot Atomic Vapors with a Phase Mismatch-Free Scheme," *Optics Express*, 29(3), 4632-4644. doi:10.1364/OE.415473

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

Johnston H., 2010/5/27, "Encryption Kicks Off in the Quantum Stadium," *Physics World*, https://physicsworld.com/a/playing-in-the-quantumstadium/ (accessed August 1, 2024).

Lo H.-K., Curty M., and Qi B., 2012, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, 108(13), 130503. doi:10.1103/PhysRevLett.108.130503

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

Marks P., 2007/10/15, "Quantum Cryptography to Protect Swiss Election," *New Scientist*, https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/ (accessed August 1, 2024).

Ou Z. Y., and Lu Y. J., 1999, "Cavity Enhanced Spontaneous Parametric Down-Conversion for the Prolongation of Correlation Time between Conjugate Photons," *Physical Review Letters*, 83(13), 2556-2559. doi:10.1103/PhysRevLett.83.2556

Sangouard N., Simon C., de Riedmatten H., and Gisin N., 2011, "Quantum Repeaters Based on Atomic Ensembles and Linear Optics," *Review of Modern Physics*, 83(1), 33-80. doi:10.1103/RevModPhys.83.33

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

Vernam G. S., 1926, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," *Transactions of the American Institute of Electrical Engineers*, XLV, 295-301. doi:10.1109/T-AIEE.1926.5061224

Whittaker Z., 2018/10/25, "New Plans Aim to Deploy the First US Quantum Network from Boston to Washington, DC," *Tech Crunch*, https://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-first-u-s-quantum-network-from-boston-to-washington-dc/ (accessed August 1, 2024).

Wootters W. K., and Zurek W. H., 1982, "A Single Quantum Cannot Be Cloned," *Nature*, 299, 802-803. doi:10.1038/299802a0

Wu C.-H., Wu T.-Y., Yeh Y.-C., Liu P.-H., Chang C.-H., Liu C.-K., Cheng T., and Chuu C.-S., 2017, "Bright Single Photons for Light-Matter Interaction," *Physical Review A*, 96(2), 023811. doi:10.1103/PhysRevA.96.023811

Wu C.-H., Liu C.-K., Chen Y.-C., and Chuu C.-S., 2019, "Revival of Quantum Interference by Modulating the Biphotons," *Physical Review Letters*, 123(14), 143601. doi:10.1103/PhysRevLett.123.143601

Yang C.-Y., Lin C., Liljestrand C., Su W.-M., Canalias C., and Chuu C.-S., 2016, "Parametric Down-Conversion with Nonideal and Random Quasi-Phase-Matching," *Scientific Reports*, 6, 26079. doi:10.1038/srep26079