以光複合載訊法增強量子通道中金鑰配送之研究

The Study of the Compound Carrier of Light Scheme in enhancing Quantum Key Distribution Protocol

鍾隆宇*

Long-Yeu Chung*

Tung-Fang Institute of Technology

Associate Professor

chung@mail.tf.edu.tw

黃伯霖

Po-Lin Huang

Kao Yuan University

Assistant Professor

polin@cc.kyu.edu.tw

***: Corresponding Author**

摘要

資訊安全在目前為通訊發展的重要課題之一，基於量子通道通訊中金鑰配送與查竊機制的 BB84 協定發表以來，它獲得相當大的重視。然因 BB84 協定至少是成立於無干擾、無漏失、傳輸與收發角度絕對完美等的假設上，但是事實上即使透過技巧排除竊聽者、傳遞遺漏等效應，雙方的原鑰中仍會有誤碼的存在，而且會隨著傳遞距離的增加而增多，故原鑰糾錯與更正的問題幾成了量子通訊量子金鑰配送協定能否可行的重要關鍵問題。本文研究以量子鑰配送協定設計，結合光學原理，提出「光複合載訊」構想，用以解決待克服的通訊資料確實問題。例如，竊聽干擾、傳輸損耗與雜訊影響的更正處理。研究為考量即時與錯誤更正簡明，本文設計架構由傳輸訊息即能自行糾錯(查竊、檢漏與偵錯)，並能及時補正，在錯誤更正率為 42.86% 性能下，毋須再經由傳統管道確認訊息之正確性再予判斷是否重發。

關鍵字：BB84、竊聽干擾、光複合載訊

Abstract:

The security of information is currently one of the important developments of communication. It had a considerable notice from BB84 which was designed to detect of communication eavesdropping with the private key distribution in the study of quantum cryptography. BB84 was set up in an ideal scheme without interference and transmission lose. But even if so, error codes still exist, and more quantities far transmission distance. Detection and correction for the raw key of error seems a key point to decides whether the private key distribution in the study of quantum cryptography successes or not. In order to solve these series problems of distortion, such as eavesdropping interference, transmission lose and noise effect, it is a feasible way that a new design scheme of compound carrier of light (CCL), which is based on quantum, key distribution (QKD) and combined with optics. In consideration of real-time and convenience, the design scheme of CCL let communication eavesdropping and distortion message can

directly be detected from the transmission carrier, and the distortion message can immediately be corrected. If the system performance rate of error correction is less 42.86%, it is unnecessary to check the precision of message between the transmitter and receiver by way of any traditional channel or re-transmit if the transmission message exist errors.

Key word：BB84, eavesdropping interference, compound carrier of light (**CCL**)

一、前言

過去多年以來，摩爾定律顯示幾乎每隔 18 個月，計算機的速度就加快近一倍，而晶片上的電晶體數目也隨著時間亦呈倍數指數增加。摩爾定律也預測 2025 年以後計算機中記憶體存儲單元將是單原子，在這樣微小的世界裡，將無可避免造成電路元件間的相互擾動問題，系統溫度的急速升高及能量損耗的大量增加，從而使計算機無法正常運作，這是當現有傳統計算機所使用的晶片精密度已經小到了某一極限的時候，電子在電路中的行為將不再服從古典力學的規律，取而代之的將是量子力學。

近年來，量子密碼通訊學的相關研究也引起許多學者專家共鳴與深入討論。基本而言，量子密碼通訊學的安全性主要是依賴於： (1)量子力學效應，諸如測不準定理、Bell 不等式、量子不可複製(Quantum no-cloning)定理等，與(2)量子鑰配送協定(QKD Protocol)，它為古典密碼學中，秘鑰被竊聽後可能會被更強大的計算能力(如：量子電腦)所破解的問題，及以往為古典密碼學所依賴之計算上的複雜度未能成功地，提供了資訊安全保障。像這樣的想法最早是由 S. Wiesner 在 1969 年所提出的[1]，他首先將量子理論應用到密碼學上並提出『Conjugate Coding』觀念，因而開啟了 Quantum cryptography，可惜的是他的理論在當時並沒有獲得共鳴與注意，直在 1984 年 C. H. Bennett 和 G. Brassard 則利用對兩種共軛基的四態光子的收發，首先提出了第一個量子鑰配送(QKD) 的協定－BB84 協定[2]；1989 年，在 IBM 的 Thomas J. Watson 研究中心則實現了第一次 QKD 的實驗[3]。到了 1991 年，A. K. Ekert 提出了利用量子糾纏的 EPR 關聯光子對的 E91 協定[4]。1992 年 C. H. Bennett 更提出只用兩種非正交態的光子就可以進行量子密碼通訊的 B92 協定[5]。量子密碼通訊的三大主流方式，從此基本建立。另基於量子鑰配送 BB84 協定之傳遞光子實驗可區分為三大類：

(1) Free Space experiment[10,11],
(2) Single Photon experiment[12,13,14],
(3) Fiber optic experiment [15,16, 17,18,19,20].

二、緣由與研究目的

雖然量子鑰配送在資料安全上有了成功的進展，然而在技術面上，仍有著發射源、量子通道、接收端、通訊協定等須克服的問題：

1. 發射源

   若量子資訊的載送是利用單光子，那麼首先面對的問題便是高效率的單光子源產生不易。因為脈衝光的光子數服從 Poisson 分佈，需將脈衝光的強度減弱到平均每次只有 0.1 個光子時，單次脈衝光含 2 個以上光子的機率才會降到 0.5%，這便限制了整個傳輸系統

的頻寬與效率。

2. 量子通道

承上，對於單光子的傳送，即使是像光纖那樣擁有損耗低、穩定性佳等特性，已經是目前最能實現長距傳輸的媒介，但依然有著難以避免的損耗率與被干擾率，這限制了量子訊號的傳輸距離。

3. 接收端

而在單光子偵測器方面，現行技術往往需要以極高電壓來放大訊號，並維持極低溫度以減少雜訊，這有著高維護成本、高耗能等缺點。

4. 通訊協定

除了硬體性能外，通訊協定則更是整個量子鑰配送的靈魂，它必須能同時滿足方法可行、資料確實、資訊安全等要求。

量子密碼通訊的三大主流方式已經為可行性提供了方向；但在確實與安全方面，因為在損耗與雜訊的影響下，必然會發生漏失與誤碼，所以通訊協定還須加上資訊糾錯的機制，又因為在理論上往往難以區分非法侵入與環境產生的雜訊誤差，通訊協定又須能做到保密加強與必要的認證校驗。

在上述四項技術面的問題中，又以通訊協定的演進，對於整個量子鑰配送效能的提升，似乎最能發揮其貢獻。例如 H.-K. Lo 等人提出了由 BB84 協定改進的引誘態 (decoy state) QKD 協定[6]，利用強引誘態與弱引誘態的交替出現，來偵知竊聽者是否存在，這便允許資訊載子可以是數量相當的單光子或雙光子，使得脈衝光的強度可達到平均每個脈衝光有 2 個光子或更多，同時提升了發射源的有效頻寬與量子通道的傳輸距離。

另外，資料傳送的誤碼率會隨著傳遞距離的增加而增多，若在通訊協定上所附加的糾錯方法能夠有所提升，也可讓資料在傳送時能容許較高的誤碼率，進而可以傳送得更遠。本文便以 BB84 協定為例，引入「光複合載訊」(Compound carrier of light, CCL)技術，探討量子通訊在誤碼糾錯與更正上的應用。

三、BB84 量子鑰配送協定

本文將提出與探討量子金鑰配送 (Quantum key distribution)的新型架構。早由 S. Wiesner 在 1969 年所提出的『Conjugate Coding』觀念，因而開啟了 Quantum cryptography 的研究，量子金鑰配送的安全性是建立在量子力學的獨特性質上，而非計算上難解的數學問題，其中最重要的就是 1982 年證明的 Quantum No-Cloning Theorem[2,3]。簡略言之，由於量子測量會改變系統原始狀態，我們無法完全複製一個量子狀態。此關鍵性質也引發 Charles H.Bennett 和 Gills Brassard 在 1984 年運用此性質建立 BB84 量子金鑰配送協定[2]，在 BB84 協定中，量子通信實際上是由兩個階段完成的。第一階段在量子通道 (Quantum Channel) 進行量子金鑰的通信。第二階段是在傳統通道 (Classical Channel) 進行金鑰的驗證協商，探測竊聽者是否存在。其設計理念簡單來說就是 (a)**Alice** 隨機地選擇 Basis State 以

z 基底：

$|0\rangle$ 與 $|1\rangle$

或 ***x*** 基底：

$$|0\rangle_x = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |1\rangle_x = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

來傳送資料產生的 0、1 所構成的序列，這些序列將被用來建立金鑰並紀錄選擇的 Basis State 以 Polarized Photon 傳發，(b)

而 **Bob**，此時並不知 **Alice** 選擇哪些 Basis State，亦隨機地以 z 基底或 x 基底來收接訊號，並紀錄選擇的 Basis State，(c)然後雙方透過傳統通道交換各自收與發的基底比較，(d) **Alice、Bob** 最後只保留基底相同的部份下的 bits，這樣子雙方便可以將相同的部份下的 bits 組織成共同擁用的**原鑰(raw key)**，簡單的例子可見於表 1。

而此共同擁用的原鑰(raw key) 將成為判斷是否有竊聽者 **Eve** 存在的依據。根據量子測量理論，『**測量必改變狀態**』，若雙方共同擁用的原鑰(raw key)不同時，就是竊聽者 **Eve** 存在的依據。然而，BB84 協定至少是成立於無干擾、無漏失、傳輸與收發角度絕對完美等的假設上，但是事實上即使透過技巧排除竊聽者、傳遞遺漏等效應，雙方的原鑰中仍會有誤碼的存在，而且會隨著傳遞距離的增加而增多，故原鑰糾錯與更正的問題幾成了量子通訊量子金鑰配送協定能否可行的重要關鍵，以下就此問題的解決，引起本文的動機並嘗試提供可行的技術研究。

四、光複合載訊技術

(一) 光複合載訊方法

本文基於 BB84 協定，提出一嶄新量子通道中金鑰的光複合載訊架構，此方法由原 BB84 設計，增加一新「**光色別**」用於載訊。光色別的設計乃傳輸光子不再是單一波長色光，而是包含兩種不同波長的色光。光複合即取光兩種不同波長與 BB84 光共軛基態複合之意。光複合載訊技術仍以光共軛基態來傳輸訊息(又稱訊息碼)，防止惡意第三者的竊聽；而新增加的光色別載訊(又稱偵錯碼)，則專門設計用為傳輸訊息糾錯、更正，參閱圖 1 之載訊組成示意。

(二) 光色別糾錯更正設計

光色別用為糾錯更正設計原因為：光色別載訊的光波長具有恆定性，不若光共軛基態會受到竊聽與雜訊影響而改變狀態。但光子若在傳輸損耗情況下，原寄望用於糾錯更正功能便無法發揮，故又須設計成：光子漏失亦能達到偵錯更正的需求，此種需求可將光色別載訊糾錯機制設定成交叉聯立方式，即任一共軛基態訊息(傳輸位元)由相鄰兩位的光色別訊息聯立決定，參閱圖 2 示意。

圖 2 所示之箭頭乃光色別載訊對所指鄰位光共軛基態(BB84)訊息提供偵錯，由於任一光色別載訊可提供兩鄰位偵錯，而任一光共軛基態載訊可受到兩鄰位糾錯，故若任一或任兩相鄰光子漏失皆能更正訊息，除非是相鄰三光子一起漏失，才無法補正，但此種情況的損耗應不可能用為通訊傳輸。

(三) 糾錯之判斷準則

糾錯機制建立後須有進一步的「協定」，方能用為執行依據，甚至形成方便的「判斷準則」。光複合載訊用兩種色光構成糾錯機制，此兩種光於收訊端識別後定義為「0」與「1」態，故糾錯協定可定成如下方式：

(1) 「0」態表兩鄰位之光共軛基態位元數值和為偶數(即 0 或 2 數)

(2) 「1」態表兩鄰位之光共軛基態位元數值和為奇數(即僅為 1 數)

根據(1)、(2)的協定，可推演出如下兩則方便的判斷準則：

(A) 凡位元受到兩鄰位光色偵出可能錯誤時，必然為錯誤位元。

(B) 凡位元受到一鄰位光色偵出可能錯誤時，須由隔一位判斷。

或：對生的可能錯誤中，若其一正確時，則另一必然錯誤。

(註：按任一光色可提供兩鄰位偵錯，故所偵出的可能錯誤必是隔一位對生的。)

判斷準則源自於協定，不同的協定會有不同的判斷準則。茲就光複合載訊光色別協定(糾錯機制)用於竊聽干擾與傳輸損耗之偵錯補正，提供如下範例了解。

範例 1

光複合載訊編碼如表 2 所示。

遭竊聽(雜訊)干擾如表 3 所示。

箭頭所指之 BB84 基態位元(訊息碼)為光色別(偵錯碼)偵出可能錯誤之處，很明顯的第 5 與第 8 位元受到兩鄰位偵出可能錯誤，按判斷準則(A)必然錯誤；而由判斷準則(B)可能錯誤的對生之一為錯誤時，其另一必然正確，故其它基態位元皆正確。

Bob 收到的資料位元，經干擾後有可能產生嚴重的後果。例如，原鑰訊息遭干擾，已非原鑰訊息；而非原鑰訊息經干擾，有可能被誤為原鑰訊息。比對本例與表 1 例子，第 5 位元的原鑰訊息已經是錯誤的訊息。由本例之錯誤計有第 5 與第 8 兩位元，若是訊息錯誤率太多，超過一般雜訊量值時，我們可直接判定通訊遭受竊聽干擾，毋須再經由傳統通道印證是否遭竊聽。

範例 2

承範例 1，若是傳輸損耗(漏失)情形發生時，如表 4 所示。

方框□表示光子漏失，導致 BB84 基態位元(含 raw key 訊息)與光色別訊息同時失去，可由鄰位光色別協定補正，本例可看出相鄰兩光子漏失，仍能校正補回。

範例 3

承範例 1、2，若是遭竊聽(雜訊)干擾與傳輸損耗(漏失)情形同時發生時，如表 5 所示

第 8 位元受到兩鄰位偵出可能錯誤，按判斷準則(A)必然錯誤；而由判斷準則(B)可能錯誤的對生之一為錯誤時，其另一必然正確，故其它基態位元皆正確；方框□表示光子漏失，導致 BB84 基態位元(含 raw key 訊息)與光色別訊息同時失去，可由鄰位光色別協定補正。

「光複合載訊」(CCL)技術用於量子通訊，可增強通訊在誤碼糾錯與更正效能，由範例 2、3 的結果，可獲致更正率為 42.86%(=3／7)，即 7 個位元可容許有 3 個位元的漏失(或漏失含誤碼至少為 3 位元)，此與原 BB84 協定無法自動糾錯更正有很大的差別。另就傳輸效能而言，比較「光複合載訊」(CCL)與原 BB84 協定，光複合載訊協定可獲致原傳輸的所有位元，而原 BB84 協定則在傳輸後比對，勢必捨棄掉傳輸的部份資訊。

五、光複合載訊安全討論

以光載訊的通訊目前以光纖為管道，因非以單光子傳輸，現尚無誤碼與漏失顧慮，但其傳輸安全僅限於用密碼方式防止破解，在講求資訊安全的時代，更安全的方式，例如偵查竊聽，必然為將來趨勢，利用單光子量子特性的 BB84 協定提供了查竊的可行性，但單光子傳輸卻可能出現會有誤碼與漏失的顧慮，故有須再對糾錯與補正的問題解決不可，本文引入光複合載訊技術與協定即針對此問題提供克服的

可行方法，使量子通道中金鑰配送的使用能夠無慮，企能有助於量子通訊的發展。

【傳輸設計與色光選用】

1. 傳輸以近紅外光或紅光為宜

(1) 因較高能量的紫色光與綠色光雖光粒子效應顯著，但其損耗太大，約傳輸不出幾公尺，光子即告損耗掉；反觀，近紅外光或紅光之光子其光粒子效應已足夠被鑑別，且其低損耗可用做遠距傳輸。

(2) 就近紅外光區之傳輸低損耗測試，0.83μm 與 1.3μm 波長處出現峰值[7]，此兩峰值處之色光選用值得納入考量。

2. 訊息耗損與中繼站設計考量

(1) 因就傳輸效果玻璃光纖優於塑膠光纖，故傳輸以選用玻璃光纖為宜，以近紅外光之石英碳纖傳輸損耗參考值[7]：1.5μm 約 0.2db／km，故若選用 0.83μm 與 1.3μm 之兩色光於玻璃光纖中傳輸，其損耗應近於前述參考值，考量做為遠距較無顧慮。

(2) 在評估選用前述低損耗兩近紅外光，對普及於市面使用提供可行性，但若為達跨國遠距傳輸，在無法避免傳輸的損耗下，中繼站設置成為設計的考量。

註：國內目前用兩種波長傳，若是較長距離用較長的波長傳，因為損耗較小；若是較短距離用較短波長傳，故慎選低損耗的波長傳輸應該可行。

【收訊機制與訊息識別】

1. 收訊以先識別共軛基態

(1) 收訊應先就光共軛基態識別，再讀取光色。一則因共軛基態易受干擾而改變，若較後識別，當收訊干擾加入後，將導致難以查竊，二則因光色不受收訊影響，可在最後讀取。

(2) 讀取色光一般用光譜儀，光譜儀讀取後之訊息，連同先前識別光訊息皆連接(記錄)到電腦上，故在讀取色別訊息後，每個光子載訊讀取即告完成。

讀取光色別後光傳輸即告結束，並無被竊還能再傳可能性，不像光共軛基態(極化)被竊後，仍能繼續傳輸被接收端接收。

目前通訊已有測試協定，例如，A 端(發射端)發一測試碼給 B 端(接收端)，B 端收到測試碼後判斷訊號正常(無被截取、無斷線、無訊息減弱、無管線不佳等)，將自動回覆一可發訊息指示碼給 A 端，A 端開始發訊，B 端即時收下。

仿此「測試碼(與指示碼)」機制，若竊聽者為竊色別(波長)必致斷線，斷線當然談不上竊聽，稱為破壞，而斷線時發射端無須再傳訊，當然也沒有洩密問題，故不會有竊聽到色別(相當測試碼或調整的測試碼部份)，而能藉部份色別偵出部份極化錯誤得到全部正確訊息之可能。但若竊聽者僅竊極化訊息，因竊聽改變極化狀態，在被光色別(偵錯碼)糾錯偵出竊聽後，隨即停止後續傳輸，竊聽者將僅得部份可能是錯的訊息而已，故光色別的使用亦可防範洩密問題。

目前光纖通訊的載訊普遍使用：有光訊號為 1 碼、無光訊號為 0 碼，故可想而知的是：若是用單光子傳輸藉以查竊，勢必非改變使用不可，原因為若是訊號漏失會被視為 0 碼，將造成誤碼。光複合載訊傳輸設計的 0 碼，已針對此項疑慮設想，用光共軛態、色光別代表傳輸與偵錯協定的 0 碼，基此，單光子的查竊功能日後能否發揮，實有賴於類似光複合載訊變更無

訊號 0 碼的設計。

鑑於愛因斯坦光量子說與戴卜洛伊物質波理論，傳輸訊號的光若選用較低能量(較長波長)會出現光量子性不顯著，此不顯著並非失去了量子性，只是不若較高能量的光顯著而已，即並非無法鑑別。另有以光可能無單一個之說，若使用上能讀出光共軛態(極化態)與鑑別出光色，滿足光量子態符合測不準原理要求，是否為光子之說應無妨，較重要的是在訊息識別時須注意時間序列，讓其載訊碼位，甚至是漏失碼位，能夠明確。

六、結論

量子金鑰分配的安全性是建立在量子力學的獨特性質上，而非計算上難解的數學問題,其中最重要的就是 1982 年證明的 Quantum No-Cloning Theorem[3]。簡略言之，由於量子測量會改變系統原始狀態，我們無法完全複製一個量子狀態。本文基於 BB84 協定針對量子金鑰分配提出與探討一嶄新、有效率的光複合載訊之新架構研究，並給予三個範例，雖僅著眼在防止惡意竊聽與資訊糾錯更正使用，然光複合載訊應該不侷限於此，如將其用於資料傳輸，其傳輸應較已往傳輸更具多元；如用於個別需求的協定使用，其應用也應較已往使用更加寬廣。

七、參考文獻

1. S. Wiesner, "*Conjugate coding*", Sigact News, **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, "*Quantum cryptography: Public key distribution and coin tossing*", in Proc. IEEE International Conference on Computers, Systems and Signal Processing, pp.175-179 (1984).
3. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "*Experimental quantum cryptography*", J. Cryptology **5**, 3 (1992).
4. A. K. Ekert. "*Quantum cryptography based on Bell's theorem*", Phys. Rev. Lett. **67**, pp.661-663 (1991).
5. C. H. Bennett, "*Quantum Cryptography Using Any Two Non-Orthogonal States*", Phys. Rev. Lett. **68**, pp.3121-3123 (1992).
6. H.-K. Lo, X. Ma, and K. Chen, "*Decoy state quantum key distribution*", On-line available at http://arxiv.org/pdf/quant-ph/0411004.
7. 賴耿陽。紅外線工學基礎應用。
8. Hartmut Klauck. "*On Rounds in Quantum Communication*", (GB Amsterdam, the Netherlands) Also:quant-ph/0004100 v5 28 Jun 2001.
9. Peter W. Shor(1) amd John Preskill(2). "*Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*", ((1)AT&T Labs Research NJ; (2)Lauritsen Laboratory of High Energy Physics CA, USA) Also:quant-ph/0003004 v2 12 May 2000.
10. Buttler. W.T. et al "Daylight quantum key distribution over 1.6 km ",Phy.Rev Lett 84,2000,5652-5655.
11. Kurtsiefer C. et al, Nature vol. 419,450(2002).
12. Alexios Beveratos, Rosa Brouri, Thierry Gacoin, Andre Villing,Jean-Philippe Poizat., and Philippe Grangier, "Single Photon Quantum Cryptography",Phys. Rev. Lett. 89,187901(2002).

13.R All’eaume et. al, "Experimental open air quantum key distribution with a single photon source",quant-ph/0402110.

14.Edo Waks, Kyo Inoue, Charles Santori, David Fattal, Jelena Vuckovic, Glenn S.Solomom, Yoshihisa Yamamoto, "Secure communication: Quantum cryptography with a photon turnstile", Nature 420,760(2002).

15. Muller.A，et al Quantum cryptography over 23km in installed under-lake telecom fibre，Europhys.Lett ，30(1996)335-339.Hughes.R.J.，et al. Quantum key distribution over a 48km optical fibre network[J]，J..Mod.Opt，47(2000)533-547.

16.Hideo Kosaka，Akihisa Tomita，Yoshihiro Nambu，Tadamasa Kimura，Kuzuo Nakamura，Single-photom interference experiment over 100 km for puantum system using a balanced gated-mode photon detector，Electron. Lett.，vol.39，No.16，pp.1199-1201(2003).

17.D Stucki1，N Gisin1，O Guinnard，G Ribordy and H Zbinden，New Journal of physics H，4(2002)41.1-41.8(http://www.njp.org/)，Zbinden H，Gisin N，Huttner B，Muller A and Tittel W，Practical aspects of quantum cryptographic key distribution J. Crypto1.13 207-20，(2000)，Ribordy G，Gautier J-D，Gisin N，Guinnard O and Zbinden H，Fast and user-friendly quantum key distribution J .Mod .Opt. 47 517-31，(2000)，

18.Bethune D and Risk W，An auto-compensating. fiber-optic quantum cryptography system based on polarization splitting of light, IEEE J. Quantum Electron. 36 340-7，(2002)

19.Nielsen P M，Schori C，Sorensen J L，Savail L，Damgard I and Polzik E，Experimental quantum key distribution with proven security against realistic attacks J. Mod. Opt. 48 1921-42，(2001)

20.Tadamasa Kimura， Yoshihiro Nambu，Takaaki Hatanaka， Akihisa Tomita，Hideo Kosaka，Kazuo Nakamura，Jpn.J. Appl. Phys. Vol.43 (2004) No.9AB pp. L1217-L1219

表 1　BB84 協定的例子

Alice 送出的資料位元	1	1	0	0	1	0	0	1	0	1
Alice 的發送基底	***x***	***z***	***x***	***x***	***x***	***z***	***x***	***z***	***z***	***x***
所傳輸的量子位元	$\|1\rangle_x$	$\|1\rangle$	$\|0\rangle_x$	$\|0\rangle_x$	$\|1\rangle_x$	$\|0\rangle$	$\|0\rangle_x$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle_x$
Bob 的接收基底	***z***	***x***	***x***	***z***	***x***	***x***	***x***	***z***	***x***	***z***
Bob 收到的資料位元	0	1	0	0	1	1	0	1	1	0
原鑰 (**Raw key**)			**0**		**1**		**0**	**1**		

光複合載訊

原 BB84：　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle_x$　$|\cdot\rangle_x$　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle$　$|\cdot\rangle_x$　傳輸訊息

光 色 別：　1　1　0　0　1　0　0　1　0　1　糾錯更正

圖 1

光複合載訊

原 BB84(訊息碼)　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle_x$　$|\cdot\rangle_x$　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle_x$　$|\cdot\rangle$　$|\cdot\rangle$　$|\cdot\rangle_x$

光色別(偵錯碼)　1　1　0　0　1　0　0　1　0　1

圖 2

表 2 光複合載訊編碼

Alice 送出資料位元		1	0	1	0	0	1	0	0	1	1
光複合載訊編碼	BB84	$\|1\rangle_x$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle_x$	$\|0\rangle$	$\|1\rangle_x$	$\|0\rangle_x$	$\|0\rangle_x$	$\|1\rangle$	$\|1\rangle_x$
	光色別	0	0	0	1	1	0	1	1	1	1

表 3 遭竊聽(雜訊)干擾

糾錯					0		0			
Bob 收到的資料位元	BB84	$\|1\rangle_x$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle_x$	$\|1\rangle$	$\|1\rangle_x$	$\|0\rangle_x$	$\|1\rangle_x$	$\|1\rangle$	$\|1\rangle_x$
	光色別	0	0	0	1	1	0	1	1	1	1

表 4 光複合載訊之色別訊息(偵錯碼)偵漏補正例子

補正					0	0			0		
Bob 收到的資料位元	BB84：	$\|1\rangle_x$	$\|0\rangle$	$\|1\rangle$	□	□	$\|1\rangle_x$	$\|0\rangle_x$	□	$\|1\rangle$	$\|1\rangle_x$
	光色別：	0	0	0	□	□	0	1	□	1	1

表 5 光複合載訊之色別訊息(偵錯碼)糾錯與偵漏補正例子

糾錯與補正					0	0			0		
Bob 收到的資料位元	BB84：	$\|1\rangle_x$	$\|0\rangle$	$\|1\rangle$	□	□	$\|1\rangle_x$	$\|0\rangle_x$	$\|1\rangle_x$	$\|1\rangle$	$\|1\rangle_x$
	光色別：	0	0	0	□	□	0	1	1	1	1