量子加密服務網路構建技術之研究

作者/葉作球、蔡一鳴

提要

由於數位文件發信用公開密鑰加密，文件收信用私鑰解密的 RSA 加解密法等，一般傳統之密碼技術，可被量子電腦所破解。且科學家發現與利用微觀物理之量子(單電子或單光子)瞬時的狀態，無法被複製的特性，可以用特定程序與調變方法，讓甲端連續的發送，帶有不同極化調變角度或波形相位的光量子。這些序列的每一個光量子，經過的路徑衰減等障礙因素，個別的光量子，統計機率性的，有可能或沒有可能到達乙端。乙端用光量子偵測器，量測陸續有到達乙端的光量子的角度或相位，依事先與甲端約定好的特定程序，產生安全的量子密碼鎖鑰，此絕對安全的量子密鑰，用以加解密甲端與乙端之間，傳送數位文件的發信與收信。量子密碼技術無論在軍事或商業用途上，均為相當先進而值得發展的通信技術。本文描述中華電信研究所利用量子密碼通信設備，研究運作原理與實際實驗量測，以現今光網路特性，作為應用的方向思考，期望能帶動風氣，作為資訊安全通信的先河。

關鍵字：量子密碼(Quantum Cryptogram)、測不準原理(Uncertainty Principle)、量子通道(Quantum Channel)、一般通道(Classical Channel)、相位調變器(Phase Modulator)、光耦合器/光分歧器(Coupler)

前言

物質有分子、原子與基本粒子夸克等觀念。能量也有基本的大小觀念，而且可量測(Quantum)，相對於可作用某物質狀態的基本能量，簡稱量子(Quantum)。1900 年，普朗克提出「能量子」概念；1905 年，愛因斯坦提出「光量子」概念；1923 年，德布羅意建立物質波理論；1925～1926 年，海森伯和薛丁格各自獨立建立矩陣力學和波動力學，量子力學從此誕生。基於量子物理之量子計算及量子通信之相關研究，亦於 1980 年代積極展開。當時科學家們探討計算機與物理系統之關係，以及如何有效率地模擬一個量子系統等問題，進而衍生出利用量子特性，就是以光子或電子之量能疊加狀態為平行計算的基礎。在 1994 年，善用量子平行式計算觀念，Shor發表了有效率的整數質因數分解法[1]，此演算法可

[1] Peter W. Shor , Algorithms for quantum computation: discrete logarithms and factoring, Foundations of Computer

以用來破解，目前被廣泛使用的RSA公鑰密碼系統，因而對目前之商用或軍用密碼系統帶來重大之影響。另利用量子特性與極化光子之複製的測不準原理(Uncertainty Principle)，衍生作為絕對不破的密碼通信之方法，稱為量子密碼通信技術。因此，目前國際間許多研究單位均投入量子通信相關之研究，且均有相當之研究成果，其中包括LANL (Los Alamos National Labs) 、NIST (National Institute of Standards and Technology)等國家級實驗室以及如IBM等商業機構，學術單位則包括Caltech、MIT、Stanford、U.C. Berkeley及USC等，亞洲如中國大陸及日本等，亦有相當之研究成果。本文描述中華電信研究所深入研究量子密碼通信設備的操作，探討其實際應用所面臨的情況，逐漸揭開量子密碼通信神秘面紗。

量子物理及量子位元簡介

特殊設計物質作用為量子系統內的量子位元，主要是基於非常奇妙之量子的疊加狀態特性，所產生的一種承載資訊的單位。傳統的資訊工程應用皆以二進制（也就是 0 和 1，這位元的狀態為 0 或 1，不能同時為 0 又為 1 的狀態，為互斥表現）來作為計算與通信的基礎。沿用此一習慣，利用具兩態（Two-State）特徵 ； 例如電子正或反之自旋（Electron Spin）方向或光子偏振（Photon Polarization）角度的量子系統，以二進位數字表示的訊息，即可編碼於這些量子系統的量子態（Quantum States）中。但這些編碼後的量子態，不再是傳統的位元（Bits），而是具有量子特性的量子位元（Quantum Bits；Qubits），也就是這位元的狀態可以機率性地為 0 又為 1，(因為微觀物理，單一個光子或電子，可以同時出現在兩個地方或三個地方....，此現象不可思議而無法解釋，但實驗證實確實如此)，其比例視當時量子系統的狀態而定。例如:甲光子之量子位元用ϕ_1表示，其兩量子位元 l0>狀態與 l1>狀態之比例表示為$|\phi_1>=C_1|0>+C_2|1>$, $|C_1|^2+|C_2|^2=1$。又如乙光子量子位元用ϕ_2 表示，其兩量子位元狀態比例為$|\phi_2>=C_3|0>+C_4|1>$, $|C_3|^2+|C_4|^2=1$。甲光子與乙光子量能疊加作用以⊗(tensor Product)表示，狀態結果用ψ表示，且｜ψ＞的符號表示，是狄拉克（P. Dirac ） 發 明 的 。 其 大 小 為 $|\Psi>=|\phi_1>\otimes|\phi_2>=C_1C_3|00>+C_1C_4|01>+C_2C_3|10>+C_2C_4|11>$。很簡單的，以上運算可看成$\phi_1$與$\phi_2$兩個矩陣的內積運算。請再注意$|00>,|01>,|10>,|11>$，這四個疊加狀態是同時存在，其存在機率比例分別為系數 C_1C_3, C_1C_4, C_2C_3, C_2C_4,。這些量子位元

Science, 1994 Proceedings., 35th Annual Symposium on, 20-22 Nov. 1994 Page(s):124-134.

除了可以存在於某些離散的基底狀態（Basis State），如三位量子位元，$|000>, |111>$外，也可以是像線性代數一樣，以這些基底，疊加出的疊加態（Superposition State），例如 $(1/\sqrt{2})(|000> + |111>)$。這個特性是與邏輯 0 和 1 互斥態最大的不同。

量子態的疊加現象，僅僅在量子系統演化過程未被觀測時才發生，一旦被觀測，疊加狀態就消失，量子系統將會隨機(random)落入某一基底中，例如上例中的$|000>$。觀測其實就是廣義的「看」。「看」這個動作，在微觀能量的世界(所謂量子的世界)裡卻變得有些奇怪了。一般而言，「看」這個動作在巨觀的世界裡，並不會改變被觀察目標本身的狀態，例如:彈珠再怎麼去看它、量它重量或體積大小，彈珠仍然還是彈珠。然而，在剛剛的例子裡，「看」這個動作卻改變了被觀察目標(也就是量子態)的本身。這一點與傳統經驗相違背的理論，雖然困擾著科學家一段時間，不過在下面的章節裡，我們將看到這一點，除了被證實以外，還被使用來做量子密碼技術的基礎。

物理學家經過深入研究，已經知道如何利用量子原理，設計量子邏輯閘（Quantum Gates），控制量子系統的演化，使疊加態能演化出某些機率最高的狀態，計算的「答案」即屬於這些最後狀態之一。 值得注意的是，N 個粒子的量子狀態基底數是以指數的型式來成長。例如，一個 1024 個狀態的系統只需要 10 個電子即可表示其所有狀態($1024=2^{10}$)，尤有甚者，因為所有的量子運算（Quantum operation）皆為線性運算，對這 10 個電子所做的運算皆同時平行地作用於這 1024 個狀態之上。意思就是，所有小於 32X32 的乘法，一步驟就同時完成；例如 17X18、9X8、25X19…..等等。巧妙地利用此一特質，可以使量子電腦在多項式時間內解決一些，目前電腦還需要強大指數能力計算量，才能解決的問題，這給需要大量平行運算的工作，帶來解決的可能性。這種強大的運算能力，是傳統電腦所不能及的。美國國際商業機器公司的科學家在 2000 年建構的五位元 215 赫茲量子處理器。2001 年，他們又建構了七位元的量子電腦。

量子密碼通信協定簡介

本節以一個典型之量子密碼協定(Protocol)--BB84[2]為例，討論以量子位元為基礎之密碼技術。依傳統密碼通信慣例，送端取名為Alice，收端取名為Bob。之前有介紹量子的意義，基於這樣的觀念，現在半導體技術，作出接近單光子的

[2] C.H. Bennett and G. Brassard "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179.

光源串流，運用其依序做 4 個偏振(光波震動方向與光傳播前進方向的角度差)極化方向的隨機調變。BB84 協定包括以下幾個步驟：

一、光子發送與測定

Alice 利用量子通道(量子通道 ;可為自由空間,或光纖)傳送一串隨機調變偏振方向的光子給 Bob，就有到達 Bob 端的光子(有些光子沒有到達 Bob 端)，Bob 依序分別隨機測定它們的偏振方向，其結果暫存起來(不告訴任何人)。並將剛剛使用過的，依序分別隨機測定偏振方向之方法的訊息，利用一般通道(Classical Channel;可用無線或有線公開的通信通道)告知 Alice。此時 Alice 幾乎可以知道 Bob 測定的結果，只有被光通道傳播因素，或是偷聽者干擾的少數位元不知道。

二、光子測定方法確認

Alice 協助 Bob 檢查他哪幾次用對了正確的測定方法。將結果用一般通道傳送給 Bob。

三、有效接收光子確認

Alice 和 Bob 捨棄那些，Bob 用了錯誤方法所測出的位元，留下正確偏振方法量測光子的訊息，這些就是原生的量子金鑰位元。(假定 Alice 傳送 100 個偏振光子給 Bob，有 50 個偏振光子到達 Bob 端， Bob 量測這 50 個偏振光子，正確量測 25 個，這 25 個的量測方法，Bob 告訴 Alice，因有雜訊等因素，Alice 告訴 Bob 有 22 個正確量測，這些 22 個正確量測的內容，就成為 Alice 與 Bob 原生的量子金鑰位元)。

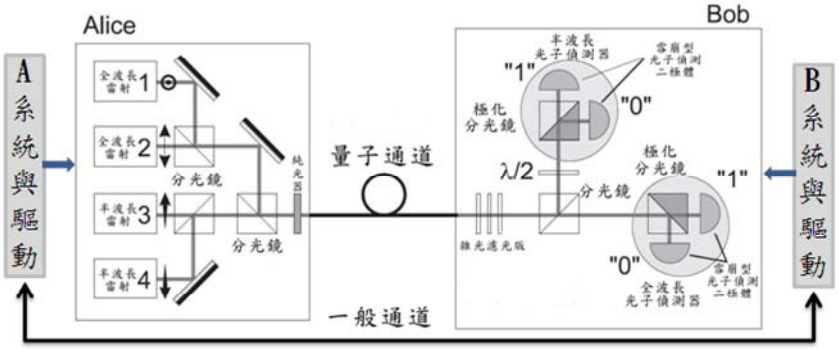
四、光子訊息更正與萃取

Alice 及 Bob 從原生的量子金鑰位元中，利用錯誤更正(Error Correction)理論，檢驗其中一小部分的原生的量子金鑰位元，確認他們的鑰匙是否有錯誤。確認結果正確時，他們就可以使用最後剩下萃取的正確位元做為鑰匙(就是量子金鑰)；若是這一段程序，所得到的量子金鑰，確認結果顯現錯誤時，他們就知道有第三者 Eve 在攔截這些光子，就放棄這些不安全的鑰匙，重新再來一次。值得注意的是此時量子通道傳送的錯誤，也被視為竊聽。

這個通訊協定的原理簡述如下。在二進制的位元中，我們將偏振「0^o」和偏振「45^o」的光子編碼成「0」 ；「90^o」和偏振「135^o」的光子編碼成「1」 。Alice 欲秘密地傳送一個位元字「45^o」給 Bob，但不告訴 Bob 正確的測量方式。設若 Bob 有兩種測量方式的選擇：測量「0^o」或「90^o」；測量「45^o」或「135^o」。若 Bob 以隨機方法，選取測量方式，有一半的機會，會選取到正確的測量方式。也有一半的機會，會選取到錯誤的測量方式。測量之後，Bob 告訴 Alice 其選取之測量方式。如果 Bob 的測量方式不正確，其結果將有一半的機會得到模糊的

0，一半的機會得到模糊的 1。此時，Alice 告訴 Bob 刪除這個位元。反之，如果 Bob 採用了正確的測量方式，Alice 告訴 Bob 保留其測量到的位元。

假設有一個竊聽者 Eve。Alice 及 Bob 如何偵測 Eve 的竊聽呢？為了竊聽，Eve 也採取兩種不同的測量方式。最大的問題在於：Eve 並不知道正確的測量方式，而 Bob 在 BB84 協定運作過程中，透過一般通道，Alice 間接的告訴 Bob，Bob 一連串測定結果中，正確的測定方法。故我們假設 Eve 也隨機採用兩種測量方式。Eve 在做完測量之後，趕快再複製將測量後的字元，傳送給 Bob。我們考慮如下可能：Alice 告知 Bob 採用正確的測量，但 Eve 竊聽時，卻用了不同的測量方式。舉例而言，Alice 欲秘密傳送一個位元字「45^o」給 Bob，Bob 選擇正確的測量方式：測量「45^o」或「135^o」。但 Eve 採用了「0^o」或「90^o」測量錯誤方法。假設 Eve 測量到的是「0^o」，而且因為 Eve 測量用錯方法，根據測不準原理，Eve 將 Alice 原來送出的信號，「45^o」改送出為「90^o」或是「0^o」。使得 Bob 做測量時，有一半的機率得到模糊的「135^o」，一半的機率得到模糊的「45^o」，這樣錯誤的結果；另一方面，若 Eve 也用正確的方式，那麼 Eve 就不會改變 Alice 所傳送之位元字。綜合上述的結果，當 Eve 竊聽且 Bob 用正確的方式測量時，Bob 所測量到的位元字，其中約有四分之一，會與 Alice 所傳送之位元字完全相反。也就是說，Eve 在四分之一的字元上留下了痕跡。最後，Alice 跟 Bob 可做某些的檢查，檢查是否有約四分之一的字元遭到改變。若是如此，Alice 跟 Bob 則可以確定有人在竊聽！



圖一 實現 BB84 之架構舉例

(資料來源：Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel and Hugo Zbinden. “Quantum cryptography”, arXiv:quant-ph/0101098 v2 18 Sep 2001, pp53.)

值得注意的是，上述之協定可以偵測竊聽者的存在與否，但不能阻止竊聽行為。總結而言，在傳統的密碼學中，假設竊聽者有更高的科技能力並有無窮的計算能力，那麼這竊聽者很有可能不被發現。然而量子密碼學告訴我們的是：

除非違反量子物理的定律，否則竊聽者必會留下痕跡。

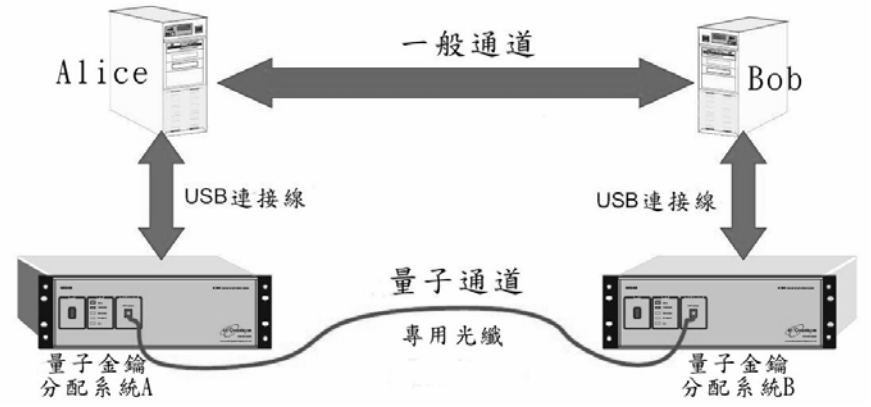
中華電信研究所之量子密碼實驗室

現行量子密碼(Quantum Cryptography)通信設備，是利用測不準原理讓竊聽行為無法遁形，以及竊聽者無法立即複製用來通訊的光子的物理原理，來達成秘密通訊的目的。密文的傳送者與接收者，使用量子密碼通信設備，很容易偵測竊聽行為的存在，而加以防範，作為無條件式安全(Unconditional Secure)的密碼通信方法。

密碼通信最怕的是，使用傳統加密技術做不斷的密文通信，密文通信間使用的密鑰卻經久不變。窺密者可將兩封以上的密文，重複做各種試驗與計算，雖然運算量很大，但使用電腦不斷的運算，總有找出密鑰的一天。一種比較好的加密方法，是使用真亂數作為密鑰，避免密鑰有重複性，使得窺密者雖然測試多封以上的密文，重複做各種數學運算，但皆無法找到各密文中，加密之密鑰種子的關係。量子密碼協定 BB84 所產生的密鑰，便具備這種特性，Alice 使用亂數法發送光量子，Bob 也用亂數法測量光量子，BB84 協定讓亂數對亂數之運作，Alice 與 Bob 得到雙方亂數中，其部分有一致性的亂數，作為密鑰，讓竊聽者無法從自然亂數密鑰中，得到規則性，因而無法破解密鑰。即使有強大計算能力的量子電腦，用來破解量子密碼，也無用武之地。

本段簡述實際量子密碼通信設備，「相位調變」(Phase Modulate)量子密碼通信設備的組成。設備分為主控電腦 Alice 與 Bob，分別用 USB 介面操控量子金鑰送收設備，量子金鑰分配系統 A(Quantum Key Distribution, QKD-A)與量子金鑰分配系統 B(QKD-B)。Alice 與 Bob 用一般通道互通訊息。量子金鑰分配系統 A 與量子金鑰分配系統 B 透過量子通道，在 Alice 與 Bob 控制下，遂行 BB84 協定金鑰的產生。量子金鑰分配系統 B 硬體中有很重要的是一組量子亂數產生器(Quantum Random Number Generator, QRNG)，與相位雪崩型光子偵測器(Avalanche Photor Diode, APD)1 及雪崩型光子偵測器 2 的冷卻溫度。Alice 控制的量子金鑰分配系統 A 有兩組量子亂數產生器。

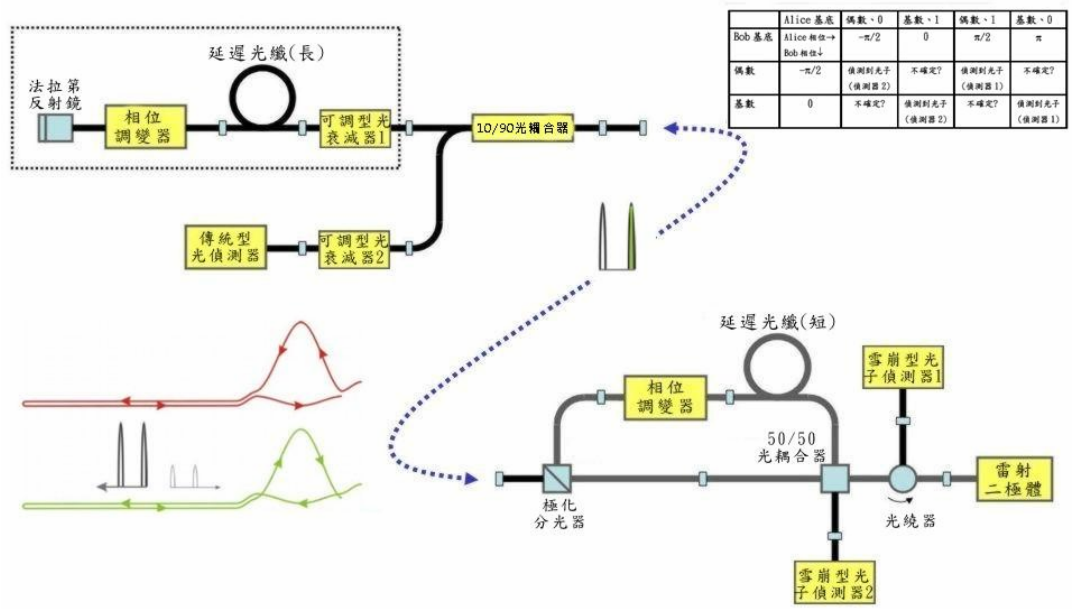
Alice 與 Bob 利用 Linux 終端機視窗，進入 line command 模式。有三種指令，包括(狀態)Status、(設定)Setting、(量子金鑰分配系統操作法則)QKD Algorithms。操作者可以選擇其中指令，分別讓量子金鑰分配系統 A 及量子金鑰分配系統 B 設備動作。但是這些指令有順序關係，要按照光量子通信概念依序執行。。整體架構如下圖二：



圖二 瑞士 id Quantique 公司的設備 Clavis2
(資料來源：id quantique SA, "Quantum Key Distribution System id 3100 Clavis2 User guide" version 1.0, 2008, pp22.)

光子偏振傳播密鑰之方法相當好，惟光子受到量子通道之光纖極化特性，對傳播中的光子偏振影響很大。尤其是長距離(>10 Km)更為明顯。因此現在有量子密碼通信設備廠商，改用相位調變的方法，並且改由 Bob 送出光束，再由 Alice 反射回送並做相位調變與衰減為光子，這樣的送收結構，自動避開光纖極化特性的干擾因素，光子的傳送，能夠保持光子原始調變的相位。其結構有如下頁圖三。中間虛線部分是單模光纖，作為光子傳送用的量子通道，左上角部分是 Alice 控制的量子金鑰分配系統 A，右下角部分是 Bob 控制的量子金鑰分配系統 B。

參考下圖三，其運作過程敘述如後；首先 Bob 的雷射二極體(Laser Diode)發射出一多光子光束脈衝(每秒 5 百萬個)，這光束經過光繞路器(Circulator)，來到 50/50 光耦合器(Coupler)，被分成走上與下兩路徑的光束脈衝，第一路光束脈衝往前傳播，經過極化分光器(Polarization Beam Spliter, PBS)，打進單模光纖繼續前進(回來時將走上面光路)。第二路光束脈衝從上面光路經過光纖延遲線(delay line)與相位調變器(Phase Modulator)，來到極化分光器，被極化分光器做 90 度的極化後，打進單模光纖(回來時將走下面光路)。追隨第一光束脈衝往前傳播，如圖三虛線單模光纖中間部分兩個光束脈衝。另請參考下圖左下角，兩光束傳播路徑示意(去程走下面光路，回程走上面光路。去程走上面光路，回程走下面光路。總結而言，這兩光束走的路徑一樣長。最後會相碰，因此發生干涉現象)。



	Alice 基底	偶數、0	基數、1	偶數、1	基數、0
Bob 基底	Alice 相位→ Bob 相位↓	-π/2	0	π/2	π
偶數	-π/2	偵測到光子(偵測器2)	不確定?	偵測到光子(偵測器1)	不確定?
基數	0	不確定?	偵測到光子(偵測器2)	不確定?	偵測到光子(偵測器1)

圖三 第二代量子密碼設備相位調變的結構圖

(資料來源：id quantique SA, "Quantum Key Distribution System id 3100 Clavis2 User guide" version 1.0, 2008, pp28&32.)

這一前一後兩路光束脈衝來到 Alice，碰到 10/90 光耦合器又分別再被分成上下兩路前進。走下面一路，碰到可調型光衰減器 2(Variable Optical Attenuator, VOA2)，讓光能量不要太強，繼續前進來到傳統型光偵測器(Classical Detector)，經過光電轉換與電子電路的處理，產生出相位調變鐘訊(Phase Modulated Clock)，讓 Alice 使用，Alice 相關運作速率得以與 Bob 的動作同步一致。走上面一路的兩光束脈衝通過可調型光衰減器 1，經過延遲光纖線，這個與下面一路產生時間差，可以讓 Alice 稍後充分使用前述的相位調變鐘訊。繼續經過延遲光纖線以後，經過相位調變器，來到法拉第反射鏡(Faraday mirror)，第一光束脈衝被反射，且被極化 90 度。第二光束脈衝也被反射，但是第二光束脈衝，之前被 Bob 的極化分光器極化 90 度，現在被法拉第反射鏡矯正回 0 度，繼續追隨第一光束脈衝。這被反射的兩光束脈衝又通過相位調變器，這一次的經過，第二光束脈衝會被調變，從 0^o、90^o、180^o、270^o 任意四個相位角度(Alice 有兩組量子亂數產生器，因而可以產生任意四個相位角)，選一做調變。被調變第二光束脈衝與未被調變的第一光束脈衝，這兩光束脈衝又要通過可調型光衰減器 1，且被衰減為單光子(從此開始，測不準原理自動發揮作用)，再打進單模光纖回傳到 Bob(這回程約數公尺，或數十公里，將不怕被竊聽)。

回到 Bob 的這兩路單光子，第一光子含有極化 90 度，碰到極化分光器就會被導到 Bob 的上面光路，通到相位調變器，從 0^o、90^o 任意兩個相位角度選一做

調變(Bob 只有一組量子亂數產生器，因而只可以產生任意兩個相位角)，接著經過延遲光纖線，到達 50/50 光耦合器。而第二光子因為極化角度是 0 度，因此直接通過極化分光器，到達 50/50 光耦合器，而且因為路徑較短趕上第一光子。從 Alice 反射回來的兩光束脈衝，衰減為兩光子脈衝，其行徑示意圖，如上頁圖三左下角所示。

這第一光子含有 Bob 的相位調變，第二光子含有 Alice 的相位調變，其互相干涉的結果如下表所示:

表 一Bob 與 Alice 相位干涉結果圖

	Alice 基底	偶數、0	基數、1	偶數、1	基數、0
Bob 基底	Alice 相位→ Bob 相位↓	$-\pi/2$	0	$\pi/2$	π
偶數	$-\pi/2$	偵測到光子 (偵測器 2)	不確定?	偵測到光子 (偵測器 1)	不確定?
基數	0	不確定?	偵測到光子 (偵測器 2)	不確定?	偵測到光子 (偵測器 1)

(資料來源：William P. Risk and Donald S. Bethune,"quantum cryptography Using Autocompensating Fiber-Optic Interferometers", Optics & Photonics News, July 2002,pp29.)

上表中兩同相位光子脈衝干涉輸出偵測器 2，即上頁圖三 第二代量子密碼設備相位調變的結構圖中，可被 Bob 其中的雪崩型光子偵測器 2 偵測到。反相位干涉輸出偵測器 1，可被雪崩型光子偵測器 1 偵測到。

如果由竊聽的地方來分析，Eve 在光束脈衝去程竊聽是無意義的，因為此時光束脈衝沒有帶訊息，且 Alice 的傳統型光偵測器因為偵測到脈衝振幅劇烈變動，故 Alice 知道 Eve 在作怪而發生告警。另竊聽者 Eve 在光子回程作用是無法達到目的，因為根據量子無法複製定理(No-Cloning Theorem)，帶有未知量子態的光子，無法被複製。

量子通信網路運作基本測試

量子密碼通信技術的實用化已漸趨成熟。前述測試技巧與操作程序熟悉以後。剩下的是要配合現場光纖傳輸的環境因素。因為傳統光通信設備是傳送光束脈衝，與傳送光子的性質有很大的差距。針對這個不同的特性，需要測試額

外的光傳輸因素，讓量子密碼通信可以在傳統光網路運行。

光纖網路的跳接線，在機房中很常見，然而跳接線的光接頭，其斷面的品質，關係接續損失大小，影響光網路的運作。因此選用 10m 跳接線共 3 對，前後連接起來，共長 60m 以及 6 組光接頭作測試。依照前節所述的步驟，逐一操作進行運作，頗為順利與正常。除了在長度時間延遲測試項目，需要更改長度參數外，其餘參照點對點接續之引數進行測試，一一順利完成。本次測試用的光接頭形式，為高品質的 FC/PC。未來將嘗試用較經濟的 LC 與 SC 光接頭來測試，以符合現今輕薄短小的趨勢。

本設備製造公司的實際使用，特別調校長度是 80 公里。按一般單模光纖規格推算，容許損失值是 12db(分貝)。嘗試利用一個 15 分貝光衰減器(Optical Attenuator)，介入量子金鑰分配系統 A 與量子金鑰分配系統 B 連接的量子通道單模光纖中，然後依照前節所述的步驟，逐一操作。最後結果是無法產生金鑰。由此推知，量子金鑰分配系統 A 與量子金鑰分配系統 B 連接的量子通道經過的整體光網路元件損失值，最好不要超過 12 分貝。

再次嘗試利用一個可調光衰減器，介入量子金鑰分配系統 A 與量子金鑰分配系統 B 連接的量子通道單模光纖中，然後依照標準步驟，分別設定衰減值 3 分貝、4 分貝與 5 分貝，進行操作 100 秒，量子金鑰順利分別產生。其結果為 409676bps/100sec、317941bps/100sec、210156bps/100sec。這樣的設定的條件，量子通道時間延遲是一樣。從這項實驗知道，等效長度不相同而時間延遲相同的量子通道，仍然能正常產生量子金鑰。但因為光子路徑損失值不同，代表長度不同的光子路徑，產生的量子金鑰數量就不同。

最後利用兩捲裸光纖，長度分別為 10Km 與 20Km，介入量子金鑰分配系統 A 與量子金鑰分配系統 B 中做實驗。依照標準步驟操作量子密碼設備，此時碰到相當大的困難，因為長度參數需要精確到 1 公尺。長度分別為 10Km 與 20Km 裸光纖，很難猜到其正確長度。此時量子設備有提供估計操作程式，人機一同判斷光纖長度。因為光子運行 10Km 或 20Km，必需用光衰減量的機率思考。經過約 1.5 天不斷的實驗與程式操作，終於得到這兩捲光纖長度為 10.707 Km 與 20.601Km。繼續依程序進行操作運作，量子金鑰順利分別產生。其結果為 18658/80000buffer 與 31043/200000buffer。從這項實驗知量子通道長度，最好先用光時域反射儀(Optical Time Domain Reflector, OTDR)先行量測得到，再做量子密碼通信設備操作，以爭取時效。

未來量子通信網路運作設計思考

一、長距離點對點應用

點對點長距離的網路應用，已經被證實可行。。依據量子理論，光子運行不可能被複製，然而 12 分貝損失極限值，代表接收端 Bob 只能收到十分之一以下個數，Alice 發出的光子，雖然整個系統的軟體運作可以正常，然而其金鑰產生性能有待研究。

超過 80Km 的量子密碼通信網路，可用兩套量子密碼設備中繼方式，一段銜接另一段運作，這種方式成本很高，且管理不易，最主要是要保證機房網路的絕對安全。目前已經有廠商研發量子再生器(Quantum Repeater)，取代中繼方式。要維護光子特性，而又能讓光子繼續前進，或是讓光子通過損失值大的光網路元件，這部分有待進一步研究。

二、光交換光網路應用

在上節基本測試項目中，已經證明量子通道容許六組共 12 個光接頭以上。光纖網路的手動跳接，在機房中很容易做到。用在量子密碼通信的運作也是可行。然而要做到隨意多方向交換，必須依賴光交換器。本研究室現有全光交換器[3]，它的交換單元是用半導體的微機電(MEMS)技術做成，插入損失為 7 分貝。雖然它可以雙向運作，符合量子通道的要求，但是其原為光束通信所設計，中有光分歧器做性能監測，被量子密碼通信設備偵測到，等同有竊聽者，無法作為量子密碼通信網路交換所用。

三、DWDM 光網路應用

使用量子金鑰分配系統 A 與量子金鑰分配系統 B，其所運行收發連接的量子通道單模光纖中，只有用到 1550nm(奈米)的光波段。密式光波多工(Dense Wavelength De-multiplexer/Multiplexer, DWDM)設備的單一通道波寬為 0.8 奈米。現今密式光波多工設備所用光波段，寬達 1450nm~1650nm 的光波段，共有 250 光通道。量子金鑰分配系統 A 與量子金鑰分配系統 B 收發光子仍然無法被載入密式光波多工每一個別通道(Channel)中。但理論上，只要插入損失在容許值內，且中間光子未被轉換成電的形式，量子密碼通信設備可以用光耦合器，與密式光波多工外部式共用光纖。得到資料顯示，密式光波多工設備必須讓出 10 個通道的波寬。因為目前沒有微能量光示波器，量子密碼通信設備與密式光波多工外部式共用光纖的互相影響，無法觀察到其變形。已知的效應，是波長對波長的調變(Cross Phase Modulation, XPM)，這部分有待未來構思研究。

[3] Photonics Cross Connector: diamondwave, http://www.calient.net/products/diamondwavePXC.php.

國際發展現況

由於密碼通信技術本身很敏感，無論在商業、外交與應用最廣泛的軍事上，競爭非常激烈。由於量子電腦可以破解 RSA 加解密，對於接近絕對安全的量子密碼通信，其需求可說是日益重要，簡單的說，就是各國都在默默的發展，也不想太張揚。目前市場上，接近可以商業運轉的產品，僅有兩家。這兩家廠商，分別代表歐美的研發實力。

量子密碼協定--BB84 原來是 IBM 在實驗桌自由空間上成功完成，後來有人改進在遠距空間上的實驗，也得以成功。但在光纖上的實驗，就不是那麼順利。光纖的極化現象，非常不利極化光子的傳播，極化光子在光纖中傳波，其極化訊息，被光纖極化特性所隨機改變，完全無法預測與改善。因此之故，有異曲同工之妙，光子的相位調變技術，就取而代之，成為最近光纖量子密碼通信的主流技術，但其須搭配光子同調干涉，檢測干涉訊息的技巧，產生量子金鑰。

利用量子金鑰將數據資訊加解密，已漸漸成熟。由於改用光子的相位調變技術，使得舊有傳統被動光纖網路，可以裝置光纖量子密碼通信收發終端機，運轉使用，不須重新佈放昂貴的極化維持光纖(PM Fiber)。可說是電信公司一大福音。然而量子金鑰的產生，是點對點的產生。無法立即使用在，階層式整面網路拓樸的電信網路。這個課題就是要想出辦法解決。

歐洲電信聯盟(Europe Telecommunication Standards Institute, ETSI) 的 the Sixth Framework Program 的 SECOQC(SEcure COmmunication Quantum Cryptography)，正在研究訂定規範，有關建立量子密碼通信網路架構。初步構想是用多套量子金鑰分配系統 A 與量子金鑰分配系統 B，組成星狀量子密碼網路。這些構想距離普遍的量子密碼網路，仍然要想出，克服超越 3 個量子密碼網路節點之限制的方法。

結論

本論文中，對相關設備操作原理與應用測試之初步研究，及可能應用的網路形式。有些技術細節仍待進一步擴大使用儀器量測後討論。另日後安排量子通信設備，選擇現場佈建，試用測試後，更深入的探討與規劃。雖然量子密碼技術之理論已有相當豐碩之研究成果，然而其實做技術則尚未商用普及化。擁有建構量子密碼相關設備的能力之單位，皆為國家級實驗室以及知名學術單位或高科技公司。除了上述之研究團體外，亞洲如中國大陸及日本等亦有初步之研究成果，但台灣目前在這方面的研究則顯然落後，值得各單位積極投入。

參考資料

一、 Andrew C. Yao, “Protocols for secure computations,” in Proceedings of IEEEFOCS82, pp. 160-164, Chicago, 1982.

二、 id Quantique SA, “Quantum Cryptography: The key to future-proof confidentiality” , ver. 3.1 June 2008, http://www.idquantique.com/products/files/networksec.pdf .