行政院國家科學委員會專題研究計畫　成果報告

可承受雜訊干擾與竊聽攻擊的量子鑰匙發送協定之設計

計畫類別：個別型計畫
計畫編號：NSC94-2218-E-034-002-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：中國文化大學應用數學系

計畫主持人：林豐澤

計畫參與人員：梁家豪、鄭伊廷、陳怡至

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 95 年 10 月 1 日

可承受雜訊干擾與竊聽攻擊的量子鑰匙發送協定之設計

Designing A Quantum Key Distribution Protocol Under Noise Interference and Eavesdropping Attack

計劃編號：NSC 94-2218-E-034 -002
執行期限：94 年 8 月 1 日 至 95 年 7 月 31 日
主持人：林豐澤　　中國文化大學應用數學系

摘要

量子密碼學是根據量子物理定律而不是傳統的數學技巧，提供的一種絕對安全的通訊管道。根據海森堡測不準原理，任何對粒子的測量都會影響到粒子的狀態。因此量子具有不可複製的特性，通訊不怕被竊聽，通訊雙方不必事先約定好解碼鑰匙，可以解決長久以來惱人的鑰匙發送問題。

然而量子鑰匙的發送會發生傳送錯誤，所造成的錯誤率，一部分固然是竊聽造成的，但有一部分卻是雜訊的干擾所致。雜訊干擾的因素主要是由設備本身所造成，包括有發送者使用的光源設備，接收者使用的偵測設備，以及量子通道等等。雜訊干擾不但會增加量子鑰匙發送的錯誤率，也會造成所謂的消相干現象，造成量子以非么正方式進行變換。本研究計劃我們利用抽樣理論，設計一套錯誤檢測機制來判斷竊聽者是否存在，再使用量子錯誤更正技術來偵測雜訊的干擾程度，自動做量子狀態的錯誤校正，以確保量子鑰匙發送的可靠性。

關鍵詞：量子密碼學、量子鑰匙發送、量子疊加、量子糾纏、EPR 效應、竊聽、雜訊干擾、消相干、量子錯誤更正

Abstract

Quantum cryptography is based on physical fundamental laws but not conventional mathematical algorithms to provide an absolute secrecy communication channel between two parties. Based on Heisenberg Uncertainty Principle, any observation of the particle in the channel will affect its internal state. Therefore, the property of quantum mechanics is that qubits cannot be copied and eavesdropping can be detected in the communication channel. Any two parties do not need to share a secret key before their communication. Thus quantum cryptography could solve the long-term troublesome key distribution problem.

The error rate occurred in quantum key distribution is partly due to eavesdropping and partly because of noise interference. The equipments used in the communication system are the main factor of noise interference caused. These equipments include the emitter used by the sender, the detector used by the receiver, and the quantum channel. Noise interference not only increases the error rate in quantum key distribution, but also produces quantum decoherence that causes non-unitary quantum transformation. In this research project, we use sampling theory to design an error code detection mechanism to detect Eve's eavesdropping or not. And then we use an error correction code as the quantum state automatic correction mechanism to ensure the reliability of quantum key distribution.

Keywords: Quantum cryptography, quantum key distribution, quantum superposition, quantum entanglement, EPR pair, eavesdropping, noise Interference, decoherence, quantum error correction

一、 前言

早期的密碼學主要使用於軍事與外交的通信系統，由於近年來電子商務的熱潮，使得資訊界、商業界、與工業界對於資訊安全的需求與日俱增。因為在開放的網際網路世界裏，所流通的訊息隨時可能被有心人士利用特殊的軟體直接從網路上攔截封包、利用電表或者利用電磁感應器量測訊號而獲悉。廣義而言，透過特定的程序將資訊從一可讀的明文映射成不可讀、但仍不失其原有內容的密文稱做加密，其相反的過程則稱之為解密。近代密碼學所採用的加密方法，通常是使用不同的數學計算公式來改變原始資訊的內容，事實上，所使用改變資訊的方法主要是透過鑰匙的途徑。當傳送者與接收者有相同的單一鑰匙時，這種密碼系統稱為對稱式密碼系統 (symmetric cryptography system)。對稱鑰匙密碼系統，存在著鑰匙發送問題 (key distribution problem)。此即傳送者與接收者在通訊之前，必需要有一條安全的管道能夠先將解碼的鑰匙送交給對方，如此一來產生了一個悖論：既然有一個安全的管道，為何不直接把文件送給對方，卻需要先把文件加密然後再解密？此外，若系統中有 1000 人，為了保證系統的秘密通訊，每一個人必需擁有其他 999 人的不同鑰匙，因此所需要的鑰匙數目大約與系統人數的平方成正比。

到了 1976 年，史丹福大學的 Whitfield Diffie 與 Martin Hellman 以及另一個 Ralph Merkle 同時提出公開鑰匙密碼系統 (public-key cryptography) 的觀念，來解決惱人的鑰匙發送問題。公開鑰匙系統又稱為雙鑰匙密碼系統，是非對稱式密碼系統 (asymmetric cryptography system)。依照這個觀念，上述 1000 人的系統，原來一共需要 499500 把不同鑰匙，現在只需要 2000 把鑰匙 (此即 1000 把公開鑰匙與 1000 把秘密鑰匙)。1978 年，麻省理工學院的 Ron Rivest、Adi Shamir 以及 Leonard Adleman 等三人製作稱為 RSA 的公開鑰匙密碼系統，這是現代密碼學最強的密碼系統。RSA 的安全性是來自於分解質因數的困難度，例如：我們很容易求得 17159 與 10247 的質因數乘積是 175828273，但是卻很難從 175828273 得到 17159 與 10247。當然，如果有朝一日有人發明了一個新的方法可以很快的得到質因數的分解，那麼 RSA 會變的一文不值了。

1994 年，AT&T 貝爾實驗室的 Peter Shor 提出第一個量子演算法，宣稱可以在多項式時間內快速的完成任何大數字的質因數分解，因此被視為是破解 RSA 的殺手途徑。不但如此，Shor 演算法更激盪出量子密碼學 (Quantum Cryptography) 研究的新希望。因為量子密碼學沒有鑰匙發送的問題，量子是不可複製的，所以通訊不怕被竊聽，保證可以抓到竊聽者，因此可以說是絕對安全的密碼系統。關於量子密碼學，這要回溯到 1984 年的 Bennett 與 Brassard，他們兩人將 Wiesner 先前提出的量子貨幣觀念應用到密碼學中，於是建立量子密碼的研究領域。Bennett

與 Brassard 認為量子密碼學可以取代目前的公開鑰匙密碼系統，於是他們提出 BB84 協定。

二、研究目的

Bennett 與 Brassard 期望建立一套無法破解的密碼系統，來取代傳統的密碼學。由於量子鑰匙具有不可複製的特性，任何截獲或測量量子鑰匙的動作都會造成量子狀態的改變，通訊雙方可以知道是否有人竊聽，如此一來截獲者只會得到無意義的資訊。因此透過量子密碼，Alice 與 Bob 可以協議出鑰匙，即使 Eve 攔截到這把鑰匙，也無法正確的詮釋出這把鑰匙的內容。BB84 能夠解決鑰匙發送問題，以量子狀態來傳送，任何截獲或測量量子的動作都會造成量子狀態的改變，如此一來截獲者只會得到無意義的資訊。因此透過量子鑰匙的傳送，Alice 與 Bob 可以協議出一把鑰匙，即使 Eve 截獲這把鑰匙，Alice 與 Bob 可以知道是否已經被竊聽。Bennett 與 Brassard 認為量子密碼技術可以取代目前的公開鑰匙密碼系統，因為量子密碼的特點是：通訊雙方不必事先約定解碼鑰匙，通訊不怕被竊聽，保證可以抓到竊聽者。Bennett 與 Brassard 所提出的量子鑰匙發送協定通稱為 BB84。

然而，BB84 仍然存在著被竊聽者攻擊、雜訊干擾、以及量子的消相干等諸多問題，造成通訊錯誤率的攀升，以致於 Alice 與 Bob 必須拋棄為數可觀的光子，影響鑰匙發送協定的進行。雖然量子是不可複製的，量子密碼不怕被竊聽，但是竊聽者的攻擊技術不斷的提升，逐漸會影響到量子密碼的安全性。本研究計劃的目的是延續先前量子密碼的研究計畫，想針對竊聽者攻擊技術的提升、雜訊的干擾、以及量子的消相干等問題提出解決方法，我們分析竊聽與雜訊干擾所造成的錯誤率，利用抽樣理論設計，一套錯誤檢測機制來判斷竊聽者是否存在，再使用量子錯誤更正技術偵測雜訊的干擾程度，自動做錯誤校正，建立更可靠的協議，以確保量子鑰匙發送的可靠性與安全性。

三、文獻探討

目前量子密碼學的主要研究在於探討量子鑰匙發送協定的製作，我們將目前文獻上的相關資料 [2, 10, 16, 18, 19, 20] 歸納成為三種基本的協定：第一是 Bennett 和 Brassard 的 BB84 協定，第二是 Bennett 的 B92 協定 ，第三是 Ekert 提出的 EPR 協定。BB84 協定分成兩個階段，第一階段在量子通道進行量子鑰匙

的單向傳送，第二階段在經典通道進行雙向的鑰匙協議以及探測竊聽者是否存在，最後雙方協商出鑰匙的內容，完成量子鑰匙發送動作。但是一旦加入雜訊後，第二階段的協議會有問題，此即 Alice 與 Bob 分不出量子錯誤是由雜訊造成的或是由 Eve 竊聽造成的。B92 使用兩個 non-orthogonal states 定義在二度空間 Hilbert space 上，然而 B92 如同 BB84 一樣需要兩個階段，Alice 與 Bob 可根據錯誤率來判斷 Eve 是否在竊聽，但是加入雜訊的干擾後，這個錯誤率也應該會顯著的增加，而且其鑰匙發送的效率只有 BB84 的一半。EPR 協定是使用 Bell's inequality 來建立的 3-state protocol。關於竊聽策略與反制方法，Ekert 等人提出 Eve 可使用不同的竊聽策略而不會增加原來可能發生的量子錯誤率，同樣的考慮雜訊的干擾後，這個錯誤率也應該會顯著的增加 [20]。

其次討論其他相關的研究。Bennet, Mor, and Smolin [3] 提出使用 parity bit 方法來解決部分雜訊干擾問題，但是 parity bit 只能解決單一量子位元的錯誤，所以此法必需確保所切割的資料區塊只有單一錯誤。Lee and Chang [40] 提出一個量子鑰匙交換協定效能的提升，他們認為現有的 BB84 會浪費 50% 的光子，而提出一種稱為基底機率調整的策略，然而竊聽成功的機率將會因基底機率的調整而提高。此外，此法的最大問題在於 Alice 必需將所使用量測方案的機率告訴 Bob，他們假設 Eve 只使用 intercept/resend 的傳統竊聽方式，然而根據我們整理的資料，竊聽攻擊的技術尚有：beam-splitting，entanglement scheme，quantum copying，以及 indirect copying 等等 [8, 32]。Yang and Kuo [31] 提出 BB84 與 BB92 的改進版本，不過他們未針對竊聽技術的提升、通道的雜訊干擾、以及消相干問題提出解決之道。Zeng at el. [33] 提出兩種量子鑰匙交換協定，他們根據兩個以及三個粒子間的量子相關 (quantum correlation) 特性建立 Bell state 以及 GHZ state，透過一個可信賴的資訊仲裁單位來解決量子錯誤問題。

四、研究方法

BB84 協定是分成兩個階段完成的。第一階段在量子通道進行量子鑰匙的單向傳送，第二階段在經典通道進行雙向的鑰匙協議以及探測竊聽者是否存在，最後雙方協商出鑰匙的內容，完成量子鑰匙發送動作。B92 不像 BB84 需要使用兩套正交基底，而是只使用一套非正交基底，例如：使用 40° 與 -40°。因此發送者可定義 $|\theta\rangle$ 與 $|\underline{\theta}\rangle$ 代表 1 與 0，$0 < \theta < 45^\circ$。$|\theta\rangle$ 與 $|\underline{\theta}\rangle$ 是非正交，$|\underline{\theta}\rangle$ 代表 $-\theta$ 的偏振光子。而接收者使用下列兩個不相容的投射運算子來觀測光子：

$$\lambda_1 = 1 - |\theta\rangle\langle\theta| \text{ 以及 } \lambda_2 = 1 - |\underline{\theta}\rangle\langle\underline{\theta}|。$$

經由 λ_1 與 λ_2 兩個投射運算子的觀測，接收者可能正確無誤的偵測到發送者送來的位元，或者得到其他不確定的狀態，這種狀態是廢物。當發送者以相同機率使

用 $|\theta\rangle$ 或 $|\underline{\theta}\rangle$ 隨機傳送 0 與 1，而接收者也以相同機率使用 λ_1 或 λ_2 運算子觀測傳送來的光子時。EPR 協定是 1991 年 Ekert 根據“量子相關”的特性提出的。量子相關就是 EPR 效應，指一對光子不管距離多遠，只要測量其中一個光子的方向，也立即可以知道另一個光子的方向，這對光子被稱為 EPR pair，又被稱為遠距離的幽靈。假設有一個 EPR pair 如下：

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |\frac{\pi}{2}\rangle_2 - |\frac{\pi}{2}\rangle_1 |0\rangle_2),$$

$|\theta\rangle$ 就是先前描述的光子偏振角度，$|0\rangle$ 是水平方向而 $|\frac{\pi}{2}\rangle$ 是垂直方向，而下標 1 與 2 分別代表第 1 與 第 2 光子。狀態 $|\psi\rangle$ 的第 1 位元被觀測是 0 ($|0\rangle$) 的機率是 1/2，被觀測是 1 ($|\frac{\pi}{2}\rangle$) 的機率也是 1/2。不過只要確定第 1 位元是 0 那麼第 2 位元一定是 1，同理第 1 位元是 1 那麼第 2 位元一定是 0，不管這兩位元的距離多遠。EPR 協定是一個三個狀態的協定，Ekert 利用貝爾不等式來偵測是否有人在竊聽。假設三個狀態定義如下：

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle |\frac{\pi}{2}\rangle - |\frac{\pi}{2}\rangle |0\rangle)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\frac{\pi}{6}\rangle |\frac{4\pi}{6}\rangle - |\frac{4\pi}{6}\rangle |\frac{\pi}{6}\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\frac{2\pi}{6}\rangle |\frac{5\pi}{6}\rangle - |\frac{5\pi}{6}\rangle |\frac{2\pi}{6}\rangle)$$

根據這三個狀態送出者可定義出三種非正交的字母表來編碼 0 與 1。例如：使用 $|0\rangle$ 代表 0，$|\frac{\pi}{2}\rangle$ 代表 1，或使用 $|\frac{\pi}{6}\rangle$ 代表 0，$|\frac{4\pi}{6}\rangle$ 代表 1，或使用 $|\frac{2\pi}{6}\rangle$ 代表 0，$|\frac{5\pi}{6}\rangle$ 代表 1。

我們已知 Alice 與 Bob 使用相同或不相同的基底的機率是 1/2 時，可得

$$\frac{1}{2}\times 100\% + \frac{1}{2}\times 50\% = \frac{3}{4} = 75\%$$

代表 Eve 沒有竊聽時，Bob 有 75% 機率可收到 Alice 送來的正確光子，但是有 25% 機率會發生錯誤。可是當 Alice 與 Eve 使用相同或不相同的基底的機率各是 1/2 時，則發生錯誤的機率變成

$$\frac{1}{2}\times 25\% + \frac{1}{2}\times 50\% = \frac{3}{8} = 37.5\% \text{ 。}$$

我們利用隨機抽樣來設計一套錯誤檢測機制來判斷竊聽者是否存在，再使用量子

錯誤更正技術來偵測雜訊的干擾程度，自動做量子狀態的錯誤校正，以確保量子鑰匙發送的可靠性。 隨機抽樣是機率抽樣的簡單型式，母體中的每一個成員都有相同的機率被挑選。一個 $n \geq 30$ 的隨機樣本假設 mean 是 μ，standard deviation 是 σ，則隨機變數 $z = \frac{\bar{x} - \mu}{\sigma / \sqrt{n}}$ 會大致趨近於標準的常態分配，其中 $\bar{x}$ 是樣本的平均值。因此當所抽取的樣本數 $n \geq 30$ 時，即稱之為大樣本，根據中央極限定理，無論母體為何種分配型態，此時樣本統計量的抽樣分配皆會趨近常態分配，因此只要藉著標準常態的分配，即可在給定的信賴水準下求出母體均值的信賴區間。在樣本數 $n \geq 30$ 時，$\hat{P}$ 的抽樣分配為常態分配，其均值為 p，標準差為 $\sqrt{\frac{pq}{n}}$，又根據標準常態的性質在給定的信賴水準 1–α 可求出 $z_{\alpha/2}$，p 的信賴區間是：$\bar{p} - z_{\alpha/2} \times \sqrt{\bar{p}(1-\bar{p})/n}$， $\bar{p} + z_{\alpha/2} \times \sqrt{\bar{p}(1-\bar{p})/n}$，其中 n 是樣本數而 $\bar{p} = x/n$ 是樣本比率。而 $z_{\alpha/2} \times \sqrt{\frac{pq}{n}}$ 是最大誤差。常用的經驗法則是：某組資料的分布若趨近於常態則 (1) 大約有 68% 的資料落在和均數差一個標準差的範圍內，(2) 大約有 95% 的資料落在和均數差二個標準差的範圍內，(3) 大約有 99% 的資料落在和均數差三個標準差的範圍內。

五、 結果與討論

我們以下面五種 cases 來說明所提出抽樣檢查的結果並討論其成效。

Case 1. 假設 Alice 與 Bob 經過雙向的協議後已經初步決定好原始鑰匙，接著兩人隨機抽取 680 位元做為抽樣的樣本規模，發覺其中有 40 位元有錯誤，現在想知道原始鑰匙於 95% 的信賴水準發生錯誤的機率有多少？由於 $\alpha = 0.05$ 經由查表得知 $z_{0.025} = 1.96$。今 $n = 680$ 而樣本的錯誤比率是 $\bar{p} = \frac{x}{n} = \frac{40}{680} = 0.0588$，因此 p 的信賴區間是 $\bar{p} - z_{\alpha/2} \times \sqrt{\bar{p}(1-\bar{p})/n} = 0.0588 - 1.96 \times \sqrt{(0.0588)(1-0.0588)/680}$ $= 0.0411$ 與 $\bar{p} + z_{\alpha/2} \times \sqrt{\bar{p}(1-\bar{p})/n} = 0.0588 + 1.96 \times \sqrt{(0.0588)(1-0.0588)/680} = 0.0765$, 此即 Alice 與 Bob 有 95% 的信心說，原始鑰匙發生的錯誤率是介於 4.11% 以及 7.65% 之間。

Case 2. 假設 Alice 與 Bob 已經隨機抽取 60 位元，公開檢驗後發覺有 9 個位元發生錯誤，現在想知道在 90% 的信心水準，原始鑰匙發生錯誤的比率是多少？由於 $\bar{p} = 9/60 = 0.15$，而 $1 - \alpha = 0.90$ 與 $\alpha/2 = 0.05$，我們可得到 $z_{0.05} = 1.645$。因為

$(\overline{p} - z_{\alpha/2} \times \sqrt{\overline{p}(1-\overline{p})/n}\,, \overline{p} + z_{\alpha/2} \times \sqrt{\overline{p}(1-\overline{p})/n}\,)$ = (0.15 − 1.645$\sqrt{(0.15 \times 0.85)/60}$, 0.15 + $\sqrt{(0.15 \times 0.85)/60}$) = (0.15 – 0.075, 0.15 + 0.075) = (0.075, 0.225)。此即 Alice 與 Bob 有 90% 的信心說，原始鑰匙發生錯誤率是介於 7.5% 以及 22.5% 之間。

根據上述得到的錯誤率區間，Alice 與 Bob 可以解譯發生錯誤的原因。若判斷得到的錯誤率是竊聽造成的，則就根據竊聽處理程序來執行之。反之，若是通訊雜訊造成的錯誤，則可使用錯誤更正碼自動更正之。

假設 Alice 與 Bob 可以找到一個錯誤估計的界限 B，若 N 是母體的大小，而 p 是母體發生錯誤的百分比率。Alice 與 Bob 可以知道需要使用多少個光子 n 來做為樣本，而可估計出發生錯誤的比率，這個計算公式簡介如下：

$$n = \frac{Npq}{(N-1)D + pq}, \text{ where } q = 1 - p \text{ and } D = \frac{B^2}{4} \text{ 。}$$

Case 3. 假設原始光子的數目 (母體) 是 N = 2000，令 B = 0.05，我們可得 $D = \frac{B^2}{4} = \frac{(0.05)^2}{4}$ = 0.000625。因此 $n = \frac{Npq}{(N-1)D + pq} = \frac{2000 \times 0.5 \times 0.5}{1999 \times 0.000625 + 0.5 \times 0.5}$ = $\frac{500}{1.499}$ = 333.56。這代表 Alice 與 Bob 至少應該取 334 個光子做為樣本，才能做出有意義的檢測。若令 B = 0.07，則得 D = 0.001225 與 n = 185.3。這代表至少應該取 186 個光子做為樣本。

計劃成果自評

於本研究計劃中，我們以 BB84 為主軸來探討與分析竊聽或雜訊所造成的量子錯誤情形。當 Eve 沒有竊聽時，Bob 有 75% 機率可收到 Alice 送來的正確光子，有 25% 機率會發生錯誤。而 Eve 竊聽時，Bob 的錯誤率會提升到 37.5%。此外量子鑰匙發送協定存在著雜訊干擾以及量子的消相干等諸多問題，造成通訊錯誤率的攀升超過 37.5%。在這個研究計劃中，我們考慮不同的竊聽技術，完成原始鑰匙錯誤檢測與抽樣之協議，可經由檢測與抽樣兩道程序來判斷是否有人竊聽。此外，我們也考慮瞭量子設備與量子通道的雜訊干擾與量子消相干現象等問題，設計一套量子錯誤碼更正程序，對於發生錯誤的量子位元自動更正之。

參考文獻

1. A. Barenco, “Quantum physics and computers”, arXiv:quant-ph/9612014 v2, Dec, 1996.
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”, pp. 175-179, 1984.
3. C. H. Bennett, T. Mor, and J. A. Smolin, “Parity bit in quantum cryptography”, Physical Review A 54, pp.2675, 1996
4. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, Berlin, 1993.
5. D. Deutsch and A. Ekert, “Quantum Computation”, Physics World, 1998.
6. W. Differ and M. Hellman, “New Directions in Cryptography”, IEEE Trabsactions on Information Theory, vol. 22, issue 6, pp. 644-654, 1976.
7. A. Ekert and R. Jozsa, “Quantum computation and Shor’s factoring algorithm”, Reviews of Modern Physics 68, pp. 733-753, 1996.
8. A. Ekert, “Quantum cryptanalysis – Introduction”, CQC Introduction, 1996.
9. A. Ekert, B. Huttner, M. Palma, and A. Peres, “Eavesdropping on quantum-cryptographical systems”, Physics Review A, vol. 50, no. 2, pp.1047-1056, 1994.
10. A. Ekert, “Quantum cryptography based on Bell’s theorem”, Physical Review Letters, vol. 67, no. 6, 1991, pp. 661-663.
11. C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, “Optimal eavesdropping in quantum cryptography (I) Information bound and optimal strategy”, Physical Review A 56, pp. 1163, 1997.
12. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, arXiv:quant-ph/0101098 v2, Sep, 2001.
13. L. K. Grover, “A fast quantum mechanical algorithm for database search”, Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp.212-219, 1996.
14. T. Hogg and C. Mochon, “Tools for quantum algorithms”, arXiv:quant-ph/9811073 v2, Dec, 1998.
15. M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Crytology, CRYPTO’94, pp.1-11, 1994.
16. D. Mayers, “Unconditional security in quantum cryptography”, arXiv:quant-ph/9802025 v4, Sep, 1998.
17. R. Merkel and H. Hellman, “On the security of multiple encryption”, Communication of the ACM 24, 00. 465-567, 1981.
18. H. K. Lo, Quantum Cryptology, Chapter 4 of Introduction to Quantum Computation and Information, World Scientific Press, 1998.
19. S. J. Lomonaco, Jr., “A quick glance at quantum cryptography”, Cryptologia, Vol. 23, No. 1, pp. 1-41, 1999.
20. S. J. Lomonaco, Jr., “A talk on quantum cryptography or how Alice outwits Eve”, Coding Theory and Cryptography: From Geheimscheimschreiber and Enigma to Quantum Theory, Lecture Notes in Computer Science and Engineering, Springer-Verlag, pp. 144-174, 1999.

21. B. Schneier, Applied Cryptography, second edition, John Wiley & Sons, Inc. 1996.
22. P. W. Shor, “Introduction to quantum algorithms”, arXiv:quant-ph/0005003 v2, July, 2001.
23. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 124-134, 1994.
24. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computation”, SIAM Journal Computing 26, pp. 1484-1509, 1997.
25. P. W. Shor, “Scheme for reducing decoherence in quantum computer memory”, Physical Review A. vol. 55, no. 4, pp. R2493-R2496, 1995.
26. D. Simon, “On the power of quantum computation”, Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 116-123, 1994.
27. A. Steane, “Quantum computation”, arXiv:quant-ph/970822 v2, Sep, 1997.
28. A. Stumpf, “Quantum Cryptography: A brief introduction to quantum key distribution”, 2000.
29. W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall, 2002.
30. S. Wiesner, “Conjugate coding”, Sigact News, vol. 15, no. 1, pp.78-88, 1983.
31. C. N. Yang and C. C. Kuo, “Enhanced quantum key distribution protocols using BB84 and B92”, Proceedings of the 2002 International Computer Symposium”, vol. 2, pp.951-959, 2002.
32. G. Zeng, “A simple attacks strategy of BB84 protocol”, quant-ph/9812064 v1 22 Dec 1998.
33. G. Zeng, Z. Wang, and X. Wang, “Quantum key distribution relied on trusted information center”, quant-ph/0001045 v1 13 Jan 2000.
34. 碼書 (The Code Book)，Simon Singh 著，台灣商務印書館，2000。
35. 費曼的六堂物理課 (Six easy pieces – Essentials of physics explained by its most brilliant teacher)，Richard Feynman 著，天下文化，2001。
36. 愛麗絲漫遊量子奇境 (Alice in Quantum land)，Robert Gilmore 著，天下文化，2002。
37. 賴溪松，韓亮，張真誠，近代密碼學及其應用，松崗電腦圖書公司，1995。
38. 你抓得到我嗎？非 0 非 1 的量子資訊，張為民，科學發展 351 期，國科會，58-61 頁，2002。
39. 量子計算與資訊，黃吉川、謝金源、李明哲，科學發展 363 期，國科會，46-53 頁，2003。
40. 李南逸、張庭魁，量子密鑰交換協定效能提升之研究，電腦學刊第 16 卷第三期， 19-25 頁，2004。