行政院國家科學委員會專題研究計畫　成果報告

量子密碼術 – 量子密碼學與量子密碼分析發展的先導研究

計畫類別：個別型計畫
計畫編號：NSC92-2218-E-034-002-
執行期間：92 年 12 月 01 日至 93 年 10 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：廖雅慧、劉以義、施孟萱、廖虹雅、陳瑩真、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 94 年 1 月 25 日

量子密碼術 – 量子密碼學與量子密碼分析發展的先導研究

計劃編號：NSC 92-2118-E-034-002
執行期限：92 年 12 月 1 日 至 93 年 10 月 31 日
主持人：林豐澤　　中國文化大學應用數學系

摘要

密碼術的歷史其實是幾世紀來編碼者與解碼者之間的競爭史。近幾年來由於研究學者引入量子力學的理論，因而產生一門新的量子密碼術。根據編碼者與解碼者的不同立場，量子密碼術可分為兩種不同的角度來討論。對解碼者而言，量子演算法具有量子疊加與量子糾纏的特性，會擁有量子平行處理的超強能力，因此可輕易的解決困難的大數目的質因數分解問題。所以使用量子電腦會很容易的破解傳統電腦很難破解的 DES 與 RSA 等著名的密碼系統。另一方面對編碼者而言，根據量子的不可複製定理，量子密碼學沒有鑰匙發送的問題，所以是無法破解的系統，可以說是“絕對安全”的密碼系統。量子密碼學就是根據物理基本定律而非傳統的數學演算法則或者計算技巧所提供的一種絕對安全的通訊管道。過去量子計算僅停留在抽象的理論探討，近幾年來，從 Peter Shor 提出第一個量子演算法可快速分解大數目的質因數，以及 Lov Grover 提出快速資料庫搜尋的量子力學演算法後，量子計算已經進入實驗的階段。IBM 以及史丹佛大學的科學家最近宣稱使用實驗用的量子電腦可算出 15 的質因數。此外，科學家又在量子密碼的相關研究中取得一定的進展，能夠在光纖中傳遞量子密碼，這使得量子密碼的相關研究逐漸受到重視。我們對量子密碼術的發展有著濃厚的興趣，希望能夠深入了解量子密碼學的各種問題與發展現況，期許將來能夠長期從事量子密碼學與量子計算的研究。我們打算從現有的 BB84，B92，以及 ERP 等現有的協定開始，研究量子鑰匙的發送、量子密碼的協定、以及公眾決策等諸多問題。此外，也打算研究量子傅立葉轉換與運用連分數技巧來求得週期近似值的量子演算法等相關技術，希望能夠充分應用這些量子計算技術於量子密碼術的發展上。

關鍵詞：量子密碼分析、量子密碼學、量子鑰匙發送、量子疊加、量子糾纏、量子演算法、量子傅立葉轉換

Abstract

The history of cryptology is in fact a contest between code-makers and code-breakers that has been going on for thousands of years. The birth of quantum cryptology is due to the introduction of quantum mechanics theory to classical cryptology by researchers in recent years. Quantum cryptology is divided into two different views based on the roles of code-makers and code-breakers for the purpose of discussion. In code-breakers' view, the quantum algorithms which have the properties of quantum superposition and quantum entanglement will have the superpower of quantum parallelism for solving the difficult large number factoring problem. Thus, quantum computers can easily break the popular encryption schemes such as DES and RSA, which are essentially intractable by classical computers. On the other hand, in code-makers' view, quantum cryptography that based on no cloning theorem has no key distribution problem is an unbreakable cryptographic system and then can be called an absolute secrecy system. Therefore, quantum cryptography, which is based on physical fundamental laws instead of using conventional mathematical algorithms, can provide absolute secrecy communication channel between two users. In the past years, quantum computing was discussed only for abstract theoretical study interest. After Peter Shor proposed the first quantum algorithm as well as Lov Grover proposed the quantum mechanics-based fast database search algorithm, quantum computing was entering into experimental research era. Meanwhile, scientists from both IBM and Stanford University recently claimed that they have found the prime factors of 15 using experimental quantum computers successfully. On the other hand, other scientists claim a major progress in quantum cryptography is also obtained. They transmitted quantum ciphers in optical fibers from one place to other place. Thus, the research of quantum cryptography has started to blossom. We have a great interest in studying quantum cryptology and try to find out what kind of problems occurred when developing quantum cryptography. We have made a long-term schedule for studying quantum cryptography and quantum computing. In our plan, we begin with the study of BB84, B92, and ERP protocols, and then focus on the problems such as quantum key distribution, quantum cryptographic secrecy protocols, and public decision. In addition, the Quantum Fourier Transform and the method of continued fractions used for finding a periodic sequence is our next work. We hope that these quantum-computing techniques can be successfully applied to quantum cryptology.

Keywords: Quantum cryptanalysis, Quantum cryptography, Quantum Key Distribution, Quantum superposition, Quantum entanglement, Quantum algorithm, Quantum Fourier Transform

一、 前言與研究目的

密碼術 (Cryptology) 是指有關研究秘密通訊的一門學問，這包含了如何秘密通訊與如何破解密碼系統兩個研究領域。通常將研究製造密碼的領域稱為密碼學 (Cryptography)，而研究破解密碼的則稱為密碼分析 (Cryptanalysis)。早期的密碼學主要使用於軍事與外交的通信系統，然而近年來由於電子商務的熱潮，急需要使用各種密碼技術，來隱藏雙方（春嬌與志明）的商業通訊訊息或信用資料，以避免被第三者（文聰）獲悉，確保網路資訊的通訊安全。評估一個密碼系統的優劣程度，安全性是最重要的指標，因為再好的密碼系統如果容易被攻擊而破解，則絲毫沒有使用的價值。

密碼學經過了數百年的發展，從單套字母替代法，例如：波雷費密碼 (Playfair)，到後來宣稱無法破解的多套字母替代法，例如：維瓊內爾密碼 (Vigenère)，最後都被輕易的破解了，這也暴露出古典密碼學的重大缺失。1950 年代左右，夏農 (Shannon) 曾証明：”任何密碼系統欲達理論安全，必需要使得鑰匙 (Key) 的長度大於或等於明文的長度”。此即鑰匙只能用一次，稱之為一次活頁 (One-time Pad) 系統。一次活頁雖可達到最高的安全性，但是因為明文的長度很長時，如何產生比明文更長的鑰匙則是一大難題，因此不適用於實際的通訊場合。

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（春嬌）與接收者（志明）都有相同的單一鑰匙時，這種密碼系統稱之為對稱式密碼系統 (Symmetric Cryptography System)。1977 年，IBM 公司發表了資料加密標準 -- DES (Data Encryption Standard)，之後美國國家安全局和美國國家科技標準局也參與了 DES 的後期發展。DES 屬於區塊加密的對稱式密碼系統。它作用於一個 64 位元長的區塊，並且使用 64 位元長的鑰匙，不過其中的 8 位元是做為同位檢查用的，所以實際上只有 56 位元。DES 的混亂手法是不斷的以鑰匙和區塊做為參數，對區塊資料進行排列、轉型、排列、替換、排列、再排列等六個步驟，此六個步驟稱為一輪，整個 DES 的編碼過程一共會進行 16 輪重複的動作。

然而對稱鑰匙密碼系統，存在著鑰匙的發送問題 (Key Distribution Problem)。此即春嬌與志明在通訊之前，必需要有一條安全的管道能夠先把解碼用的鑰匙送交給對方，如此一來產生了一個悖論：既然你有一個安全的管道，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 1,000 人，為了保證系統的秘密通訊，每一個人必需擁有其他 999 人的鑰匙，因此需要不同鑰匙的數目大約與系統人數的平方成比率。

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，是屬於非對稱式密碼系統 (Asymmetric Cryptography System)。這個系統的主要觀念是：(1) 編碼鑰匙 (Encryption key) 和解碼鑰匙 (Decryption Key) 是分開的，編碼鑰匙是公開的而解碼鑰匙是秘密的。(2) 無法由編碼鑰匙推導得到所對應的解碼鑰匙。(3) 也無法由解碼鑰匙推導得到所對應的編碼鑰匙。依照這個觀念，上述 1,000 人的系統，原來一共需要 499,500 把不同鑰匙，現在只需要 2,000 把鑰匙 (此即 1,000 把公開鑰匙與 1,000 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 的做法如下所述：每一個人有一把公開鑰匙 P 做為加密之用，同時每一個人也有一把秘密鑰匙 S 做為解密之用。如何產生公開鑰匙 P 與秘密鑰匙 S 呢？首先令 $P=(n, p)$ 與 $S=(n, s)$。n, p, s 是三個很大數目的隨機質數，至少有 100 位數，先假設此三個質數分別為 a, b, c。令 $s=\max(a, b, c)$，剩下兩個質數令為 x 與 y。取 x 與 y 的乘積令為 n，此即 $n=xy$，取 p 滿足 $ps \bmod (x\text{-}1)(y\text{-}1)=1$。當春嬌欲送出訊息 M 給志明時，先要找出志明的公開鑰匙 P，將明文 M 每次取若干位元進行加密，來產生密文 $C=P(M)=M^P \bmod n$ 而傳送給志明。志明使用他的秘密鑰匙 S 將收到的密文 C 每次取若干位元進行解密，來得到明文 $M=S(C)=C^S \bmod n$。即使密文 C 被文聰截獲到，但是由於文聰不知道秘密鑰匙 S，所以無法破解密文。RSA 的安全性是來自於質因數分解上的困難，這是因為要從一個上百位數的 n 中去分解出質數 p 與 s 是非常困難的，所以秘密鑰匙的 s 值不可能輕易的從公開鑰匙的 p 值推導出來。曾經有一位電腦安全專家 Simson Garfinkel 估計，以一台 100MHz 的 Intel Pentium 機器，大約要 50 年的時間才能分解 130 位數的質因數。當然，如果有朝一日有人發明了一個新的方法可以很快的由 p 求出 s 值，那麼 RSA 也許會變的一文不值了。很不幸的，這個夢魘終於在 1994 年發生了。

1994 年 AT&T 貝爾實驗室的 Peter Shor 提出第一個量子演算法 (Quantum Algorithm) 可快速完成質因數的分解，因而將量子計算帶入一個新境界。量子演算法最大的優點是能將 NP 問題變成 P 問題，縮短原來需要的計算時間。Shor 演算法能夠於多項式時間內分解質因數，因此 Shor 演算法說明了量子計算是破解 RSA 密碼系統的一種新途徑。另一方面，1984 年 Bennett 與 Brassard 將 Wiesner 先前提出的量子貨幣觀念應用於密碼學中，因而產生量子密碼學，他們期望建立一套無法破解的密碼系統。以量子狀態做為鑰匙會具有不可複製的特性，因而可以說是“絕對安全”的密碼系統。任何截獲或測試量子鑰匙的動作都會造成量子狀態的改變，如此一來截獲者只得到無意義的資訊。因此透過量子密碼，春嬌與志明可以協議出鑰匙，即使文聰攔截這把鑰匙，也無法正確的詮釋出這把鑰匙，同

時春嬌與志明也可以知道文聰是否在竊聽。Bennett 與 Brassard 認為量子密碼可以取代目前的公開鑰匙密碼系統。因此量子密碼的特點是：通訊雙方不必事先約定解碼鑰匙，通訊不怕被竊聽，可以保證抓到竊聽者。因此，量子密碼術可分兩個角度來看。對編碼者而言，由於量子狀態是不可複製的，所以量子密碼沒有鑰匙發送的問題，所以是無法破解的系統，可以說是“絕對安全”的密碼系統。另一方面，對解碼者而言，在量子電腦執行的量子演算法，具有量子疊加與量子糾纏的特性，而擁有量子平行處理的超強能力，可以很輕易的解決困難的大數目質因數分解問題，因此很容易破解傳統電腦很難破解的 DES 與 RSA 等著名的密碼系統。

過去量子電腦僅停留在抽象的理論探討階段，例如探討 Bell's inequality，many worlds interpretation 等等。但是近幾年來，Shor 提出第一個量子演算法，接著 Grover 也提出一個快速資料庫搜尋的量子力學演算法，Chau 與 Wilczek 進行量子邏輯元件設計，Schumacher 從事量子編碼及資料傳輸方面的研究，使得量子計算進入實驗的階段。IBM 及史丹佛大學的科學家宣稱使用實驗的量子電腦計算出 15 的質因數。此外，科學家又在量子密碼的相關研究中取得一定的進展，能夠在光纖中傳遞量子密碼。德國慕尼黑大學和英國軍方合作，成功的傳送 23.4 公里的量子密碼。然而日本三菱電機公司的研究人員宣稱他們傳遞量子密碼的距離長度可達到 87 公里，打破了美國洛杉磯國立研究所先前創造的 48 公里的記錄。由於人類社會資訊交換越來越頻繁，對資訊安全的要求也越來越迫切，因此量子密碼術也更顯得重要。科學家希望，將來可以實現 1000 公里距離的量子密碼傳輸時，就可以利用衛星來傳遞資訊，並且建立全球的資訊密碼交換體系。

我們對量子密碼術的發展有著濃厚的興趣，因此於本先導性的研究計劃中，我們以十個月左右的時間，深入了解量子密碼學的現況發展與發掘各種存在的問題，整理出待解決的研究方向，期許能夠長期從事量子密碼學與量子計算的相關研究。

二、 相關研究文獻探討

從理論上來看，傳統數學的計算加密方法都是可以破解的，因為再複雜的數學鑰匙也可以找到規律。隨著計算機的快速發展，例如：Intel Pentium 處理機的速度已達到 2.66GHz，破解數學密碼的困難度也會逐漸降低。我們先從計算機的速度講起。隨著人類對於資訊的需求與日具增，人們必須不斷地推進資訊技術的發展，然而現有資訊處理系統的功能已接近於物理極限。過去 30 多年來，幾乎每隔兩年左右，電腦的速度就加快了一倍，而晶片上的電晶體數目也隨著時間呈指數

增長。摩爾定律顯示，10 多年以後電腦儲存單元將會是單原子，在這樣微小的世界裡，將無可避免的造成電路間的相互干擾，系統溫度的急速升高及能量損耗的大量增加，從而使電腦無法正常運作，這是現有資訊處理系統必須面對的危機。從物理上來看，這是電子在電路中的行為將不再服從經典力學的規律，取而代之的將是量子力學。物理學家相信：當傳統電腦所使用的晶片精密度已經小到了極限的時候，祇有量子力學 (Quantum Mechanics)，才能使電腦的發展再有突破。因此，資訊科學的下一步發展必須借助於量子力學的原理和方法，發展量子計算甚至量子電腦。過去半個世紀來，量子力學對工業技術發展發揮了不可忽視的作用。從半導體技術、各種新材料的發現、到最近奈米技術的產生，無一不是以量子力學為其科學基石。

其次關於量子密碼的重要性。古典物理容許巨觀 (Macroscopic) 的媒體，例如：紙張、磁帶、電波訊號等等，被偷看後不留下任何痕跡。這是因為這些訊號都是使用 “可以觀測”的媒體來記錄訊息。如果我們使用 ”量子媒體” 記錄訊息，那麼事情就不一樣了。雖然量子力學對巨觀或微觀 (Microscopic) 的物體都可適用，但是有些量子效應對微觀系統，例如：原子或者更小的核子、電子等等，會特別的顯著。”偷看” 或者 “竊聽” 對系統說來就是 “測量”。於古典物理，測量不會影響到系統的狀態。但是對於量子系統，“測量” 是系統的一部分，它會造成系統的波函數 “走調” (dechorence)。因此，我們可以設計一個量子通訊管道，任何人 “測量” 量子都會改變系統的狀態，通訊雙方也就知道有人在竊聽了。量子資訊與傳統資訊最大的不同在於：傳統資訊的位元 (bit) 只能處在一個狀態，非 0 即 1，而量子資訊中的量子位元 (qubit) 可以同時處在狀態 |0> 和狀態 |1> 中，這就是量子的狀態疊加 (superposition)。如果 |A> 與 |B> 是兩個互相獨立的量子狀態，它們的任意線性疊加也是某一時刻的一個量子狀態。這會使得每個量子位元的組態比傳統位元多得多，量子位元利用不同的量子疊加狀態來記錄不同的資訊。例如：7 個在疊加狀態的量子位元，等於同時代表 128 種不同的狀態，或代表 128 個數字。當量子電腦執行計算時就猶如同時測試所有 128 個數字，一秒鐘後，這部電腦就會輸出結果，這等於以一個計算的成本而得到 128 個計算一樣。因此，同樣由 2 個狀態組成的物理裝置，量子位元的功能比起傳統位元強得多。應用量子力學於資訊領域，可以大量增加資訊的儲存容量、可以提高運算的速度、以及可以確保資訊的絕對安全。所以，一門新的科學分支— 稱為量子資訊科學也就應運而生，它是結合量子力學與資訊科學，以量子力學的狀態疊加以及量子糾纏 (entanglement) 為基礎，來研究資訊處理的一門新興科學。廣義的說，量子資訊科學包括量子計算 (量子電腦) 和量子資訊 (量子通訊和量子密碼) 兩大領域，近年來量子計算與量子資訊在理論和實驗上都取得重大的突破，證明它們的可行性。2003 年七月初出版的新聞周刊 (Newsweek) 其封面報導是改變世界的十個發明 (Inventions That Will Change the World)，其中的一項發明就是量子密碼。

文章內說明這十種匪夷所思的發明與創造，有的還停留在實驗階段，但是將來的某一個時刻，它會改變我們共同的未來。另外，也是 2003 年七月出版的 PC 雜誌報導有二十種未來熱門的尖端科技 (Future tech: 20 hot technologies to watch)，即將帶給人類更文明與方便生活，其中的一項也是量子密碼。

三、研究方法

這個先期研究計畫以十個月時間深入了解量子密碼以及量子演算法的現況發展，而整理出這些領域的研究重點與待解決問題，我們分成兩部分進行的。第一部分，關於量子密碼學方面。量子密碼學是根植於海森堡測不準原理 (Heisenberg Uncertainty Principle) 和單量子不可複製定理 (No Cloning Theorem)。”海森堡測不準原理” 是量子力學的基本原理，指在同一時刻以相同精度測定量子的位置與動量是不可能的，只能精確測定兩者之一。而 “單量子不可複製定理” 是 “海森堡測不準原理” 的推論，它指在不知道量子狀態的情況下複製單個量子是不可能的，因為要複製單個量子就只能先做測量，而測量必然改變數子的狀態。根據這個基礎，我們從 Bennett 與 Brassard 的 BB84 開始，研究量子鑰匙發送 (Quantum Key Distribution) 的通訊協定。BB84 需要一個雙方可以交換偏極化光子的量子管道，以及一個公開的通訊管道來交換一般的訊息。首先，春嬌送出一串任意在 0° (→)、45° (↙)、90°(↑) 或者 135°(↘) 方向偏極化的光子。志明收到光子時就任意選定是要測量 “正角” 方向或 “斜角” 方向的偏極化，將測量的結果紀錄下來。然後可以公開宣布他選擇用 ”正角” 或 ”斜角”，不過不能公布測量的結果。此時春嬌可以告訴志明他是否選對了測量的方向。春嬌可以把所有志明選錯方向或者沒量到的光子全部丟棄。當然文聰可以測量到量子管道上的光子。春嬌與志明可以在雙方的光子中任選一些來比較，測試文聰是否在竊聽。如果發現文聰在竊聽，他們就把整批光子丟掉重新再來一次。文聰也不知道春嬌送出來的是 “正角” 或者 “斜角” 偏極化的光子，如果他猜對了，根據量子力學，他所作的測量並不會改變光子的狀態；但是如果猜錯了 (他自己絕對不會知道猜錯了)，他的測量會影響到下一次志明的測量結果。於是當春嬌與志明公開比較結果時，就可以發現文聰是否在偷聽了。文聰能否在測量之前先複製一個光子給志明呢？量子力學告訴我們量子狀態無法複製。只要文聰竊聽，都會使得訊號傳遞發生錯誤，因此竊聽者就無法遁形了。如果春嬌與志明比對後發現沒有人竊聽，剩下的光子就已經成功地由春嬌手中傳給志明。最後他們可以把水平或者 45° 偏極化的光子解釋為 “0”，垂直或者 135°偏極化的解釋為 “1”。如此一串 0 與 1 就可以當做一把鑰匙了。事實上，這種做法不太有效率，因為平均情況必須丟棄一半的位元，我們覺得可以加以改進為更有效率的協定。此外，我們也正在研究有雜訊干擾的 BB84 的修正協定。

而 B92 協定是 1992 年由 Bennett 提出的。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°。因此春嬌可定義 $|\theta\rangle$ 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。而志明使用下列兩個不相容的投射運算子 (projection operator) 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，志明可能正確無誤的偵測到春嬌送來的位元，或者得到其他不確定的狀態，這種狀態是廢物 (erasure)。當春嬌以相同機率使用 $|\theta\rangle$ 或 $|\underline{\theta}\rangle$ 隨機傳送 0 與 1，而志明也以相同機率使用 λ_1 或 λ_2 運算子觀測傳送來的光子時，志明正確接收光子的機率是

$$P_1 = \frac{1 - \left\|\langle\theta \mid \bar{\theta}\rangle\right\|^2}{2}$$

而接收到廢物的機率是

$$P_2 = \frac{1 + \left\|\langle\theta \mid \bar{\theta}\rangle\right\|^2}{2}$$

其中 $\left\|\langle\theta \mid \bar{\theta}\rangle\right\| = \cos(2\theta)$，因此志明大約有 50% 以上的機率得到廢物。但是志明若收到正確的光子，則一定會正確的解譯春嬌送的是 0 或 1。B92 如同 BB84 一樣需要兩個階段。

第二部分，關於量子計算方面。我們研究 Shor 提出的兩篇快速質因數分解的量子演算法以及 Grover 提出的快速資料庫搜尋的量子演算法。Shor 証明量子電腦能夠快速的進行大因數的分解，促使量子電腦的研究進入實驗的階段。量子電腦的量子邏輯元件是對應數學上的一個么正變換矩陣 (Unitary matrix)，不僅可將|0>態和|1>態互換外，還可以對|0>態 和|1>態做任意的疊加。此外量子計算會將量子暫存器 (Quantum register) 的量子位元變換為糾纏狀態，量子糾纏會使得量子位元間具有強烈的關聯性，當其中的一個量子位元被測量時，會決定糾纏狀態內所有其它位元狀態的相應變化，這種量子糾纏特性提供了量子大量平行處理的能力。量子大量平行處理是對量子位元的每一疊加分量同時進行么正變換，根據一定的機率疊加計算來得到結果。假設現在有兩個量子暫存器，每一暫存器可儲存 2 個 qubits，我們令第一個暫存器產生量子糾纏 (此即含有所有可能儲存的整數)，因此每一個 qubit 是：$|0> \rightarrow \frac{1}{\sqrt{2}}(|0> + |1>)$ 或 $|1> \rightarrow \frac{1}{\sqrt{2}}(|0> + |1>)$，暫存器的疊加狀態是 $\frac{1}{\sqrt{2}}(|0> + |1>) \otimes \frac{1}{\sqrt{2}}(|0> + |1>) = \frac{1}{2}(|00> + |01> + (|10> + |11>)$。

若我們利用量子平行來計算一個函數 $F_N(x)$ 的週期，其中 x 是疊加狀態的每一個整數。這是因為找出 $N = p_1^{k1} p_2^{k2} \ldots p_m^{km}$ ，(p_i 是質數) 的因數分解問題相當於計算一個函數週期的問題。此即 $F_N(x) = a^x \bmod N$，a 是任意數與 N 互質。當第二個暫存器含有 $F(x)$ 時，經過計算過程後，此兩個暫存器產生量子糾纏：$\sum_x |x>|F(x)$。

當我們對第二個暫存器做測量時，此測量會隨機挑選 $F(x)$ 的一個值，令為 $F(k)$。而經過測量後的第一個暫存器是所有狀態 $|x>$ 的凝聚疊加，$x = k, k+r, k+2r, \ldots$ 滿足 $F(x) = F(k)$，r 是 $F(x)$ 的週期。此即第一個暫存器會經由么正變換將任何 $|k>$ 變成 $|0>$，再將週期從 r 變成 $1/r$ 的倍數，事實上這種動作是量子傅立葉轉換 (Quantum Fourier Transform)，而分數 j/r 可使用連分數 (Continued Fractions) 方法得到近似值，此即當 $r \le \phi(n) < n$，我們希望近似的得到一個 j/r，$r < n$。從這個研究我們了解到量子計算與量子平行處理有那些獨特的特性。

四、 結果與討論

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。首先假設通道沒有其他雜訊的干擾，這兩階段的工作如下所述。

第一階段：單向鑰匙的傳送

春嬌隨意產生一串 bit strings (至少有 100 bits) 準備發送給志明做為雙方通訊的鑰匙。春嬌經由量子通道傳送此鑰匙給志明，每次欲傳送一個 bit (0 或 1) 時，她使用 A_1 或 A_2 的“起偏振板”來編碼產生光子傳送出去，而志明也使用 A_1 或 A_2 的“偏振過濾板”去測量所收到光子的偏振，並解譯出所代表的 bit 是 0 或 1。

第二階段：雙向的鑰匙協議

第二階段有兩個子階段，首先是原始鑰匙的確定，其次是檢查文聰是否在竊聽。第一子階段，志明經由經典通道告訴春嬌他使用了那一種方案來測量光子。春嬌收到訊息後，比較自己發送時所使用的方案，確定有那些光子使用相同的方案，再將比較結果告訴志明。最後，春嬌和志明只保留雙方使用相同方案測量出來的位元，放棄不相同方案的位元，做為他們協議出來的原始鑰匙 (假設此鑰匙的長度為 n bits)。接著進行第二子階段。我們已假設通道沒有其他雜訊的干擾，志明和春嬌從原始鑰匙中隨機抽取 m 位元 (m 遠小於原始鑰匙的長度 n) 來進行驗證，比較此 m 位元是否相同。如果有不一致，則代表文聰在竊聽，已協議的原始鑰匙要作廢，整個過程重新再來。如果完全相同，也不能保證文聰一定沒有竊聽，

因此還需要去計算文聰竊聽的可能機率，不過由於此 m 位元已經曝光所以必需要丟棄，原始鑰匙的長度縮短為 $n-m$。

效率評估：

A. 假設文聰沒有竊聽：

春嬌以隨機方式使用 A1 或 A2 基底傳送光子，志明也是以隨機方式使用 A1 或 A2 基底接收光子。

(1) 若兩人使用相同的基底，則志明可 100% 正確無誤收到春嬌的光子。

(2) 若兩人使用不相同的基底，則志明仍有 50% 可正確收到春嬌的光子。

結論：若兩人使用相同或不相同的基底的機率是 1/2 時，則：

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

在沒有文聰竊聽時，志明有 75% 機率可收到春嬌送來的正確光子，有 25% 機率發生錯誤。

B. 假設文聰有竊聽：

春嬌以隨機方式使用 A1 或 A2 基底傳送光子，文聰以隨機方式使用 A1 或 A2 基底竊聽光子，志明也是以隨機方式使用 A1 或 A2 基底接收光子。

(1) 春嬌與文聰使用相同基底時，此時不影響志明的觀測。換言之，春嬌與志明沒發覺文聰在竊聽，此情況與 (A) 相同，志明有 75% 機率可收到春嬌送來的正確光子，有 25% 機率發生錯誤。

(2) 春嬌與文聰使用不相同基底時，此時會影響到志明的觀測，文聰會有 50% 機率造成錯誤。

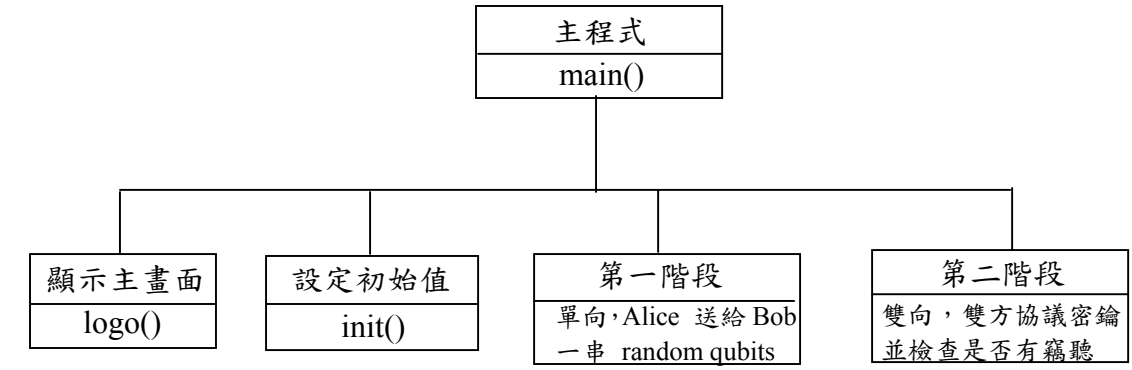
結論：若春嬌與文聰使用相同或不相同的基底的機率是 1/2 時，則發生錯誤的機率是：

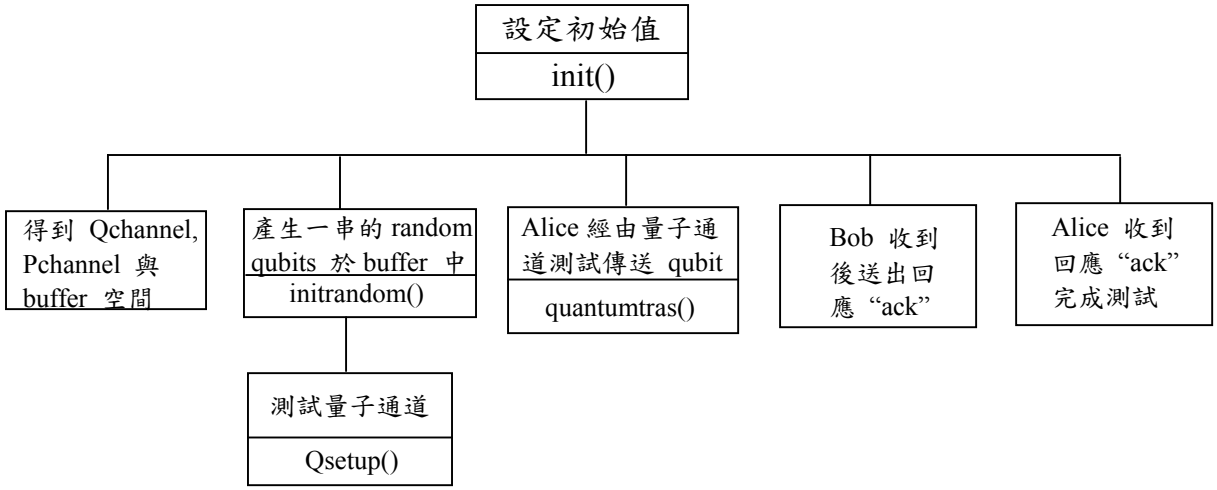
$$\frac{1}{2}\times 25\% + \frac{1}{2}\times 50\% = \frac{3}{8} = 37.5\%$$

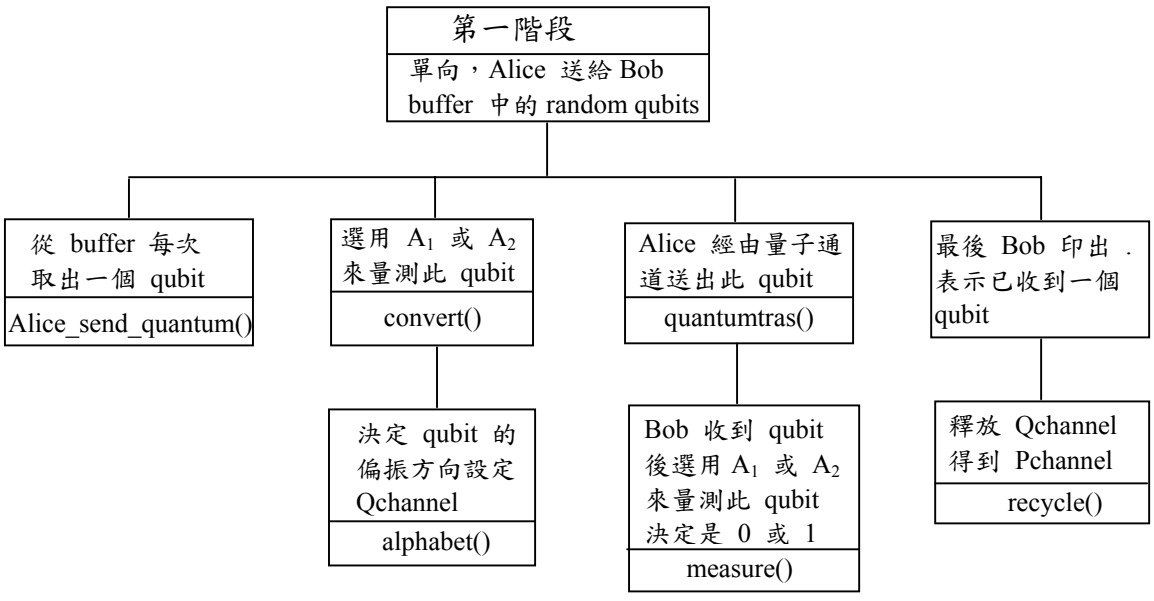
假設文聰以 λ 的機率進行竊聽 $(0 \le \lambda \le 1)$，則上述志明接收發生的錯誤率公式是：$\frac{1}{4}\times(1-\lambda) + (\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{2})\times\lambda = \frac{1}{4}+\frac{\lambda}{8}$。當 $\lambda = 0$，代表文聰沒有竊聽，志明的錯誤率是 25%。當 $\lambda = 1$，代表文聰有竊聽，則志明的錯誤率是 3/8 = 37.5%。由於文聰的竊聽，造成志明的錯誤率提升 50%。

此外，我們也設計了一套模擬程式，可在傳統機器上模擬量子通道執行 BB84 協定，此程式的一部分結構如下所示：

BB84 模擬程式的一部分結構設計圖示







計劃成果自評

於本研究計劃中我們深入了解 BB84, B92 與 EPR 等協定，而以 BB84 為主軸來探討與分析竊聽造成的量子錯誤率情形，進而再探討 BB84 的效率性。當文聰沒有竊聽時，志明有 75% 機率可收到春嬌送來的正確光子，有 25% 機率會發生錯誤。而文聰竊聽時，志明的錯誤率會提升到 37.5%。此外，現有的量子鑰匙發送協定仍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，以致於春嬌與志明必需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。例如：Fuchs et al. 提出一個量子密碼最佳竊聽技術，Zeng 提出一種稱為 “indirect copying” 的竊聽攻擊技術等等。針對竊聽技術的提升，實在有必要增強現有量子鑰匙發送的協議程序。在這個先導研究計劃中我們獲得許多量子密碼學與量子計算的重要知識，我們也撰寫程式實際模擬量子傳送的場景，瞭解量子觀測對偏振方向的影響，奠定了研究量子密碼與量子計算的基礎，下一個研究計劃我們將進行應用量子技術來建立一個量子密碼通訊的系統模式。

這個研究計劃的初步研究成果是：三篇正在撰寫中的論文。它們是：

(1) 量子密碼學通訊協定的理論探討。

(2) 量子密碼學的三種量子鑰匙發送協定的研究與分析。

(3) 量子鑰匙發送協定的量子位元錯誤率分析。

參考文獻

1. A. Barenco, “Quantum physics and computers”, arXiv:quant-ph/9612014 v2, Dec, 1996.
2. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, Berlin, 1993.
3. D. Deutsch and A. Ekert, “Quantum Computation”, Physics World, 1998.
4. A. Ekert and R. Jozsa, “Quantum computation and Shor’s factoring algorithm”, Reviews of Modern Physics 68, pp. 733-753, 1996.
5. A. Ekert, “Quantum cryptanalysis – Introduction”, CQC Introduction, 1996.
6. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, arXiv:quant-ph/0101098 v2, Sep, 2001.
7. 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.
8. T. Hogg and C. Mochon, “Tools for quantum algorithms”, arXiv:quant-ph/9811073 v2, Dec, 1998.
9. M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Crytology, CRYPTO’94, pp.1-11, 1994.
10. D. Mayers, “Unconditional security in quantum cryptography”, arXiv:quant-ph/9802025 v4, Sep, 1998.
11. S. J. Lomonaco, Jr., “A quick glance at quantum cryptography”, Cryptologia, Vol. 23, No. 1, pp. 1-41, 1999.
12. 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.
13. P. W. Shor, “Introduction to quantum algorithms”, arXiv:quant-ph/0005003 v2, July, 2001.
14. 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.
15. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computation”, SIAM Journal Computing 26, pp. 1484-1509, 1997.
16. D. Simon, “On the power of quantum computation”, Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 116-123, 1994.
17. A. Steane, “Quantum computation”, arXiv:quant-ph/970822 v2, Sep, 1997.
18. A. Stumpf, “Quantum Cryptography: A brief introduction to quantum key distribution”, 2000.
19. W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall, 2002.
20. 碼書 (The Code Book)，Simon Singh 著，台灣商務印書館，2000。
21. 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。
22. 愛麗絲漫遊量子奇境 (Alice in Quantum land)，Robert Gilmore 著，天下文化，2002。
23. 物理與生活，丁志良著，高立圖書公司，2003。
24. 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。
25. 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。