Communications of the CCISA
Vol. 28 No. 2 May 2022

量子密碼學簡覽

曾國鈞 [1,*]
[1] 國立臺灣大學
[1]nk32325959@gmail.com

摘要

隨著各國極力發展量子電腦，傳統密碼學將會遭遇量子演算法的威脅，使得各國皆思索並建立下一世代的密碼學，以抵禦量子電腦未來的崛起。本文提供一簡覽，讓讀者可以了解到量子密碼學帶來的革新與應用，並且藉由本文可以了解到一些經典的量子密碼協定，將來可由這些基礎知識進一步自我學習跟探索深奧且有趣的量子密碼學領域。

關鍵詞：量子密碼學、量子金鑰配置、量子安全直接傳輸、量子秘密分享、量子模糊傳輸

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 28 No. 2 May 2022

Quantum Cryptography: A Brief Overview

Kuo-Chun Tseng[1*]
[1]National Taiwan University
[1]nk32325959@gmail.com

Abstract

As countries strive to develop quantum computers, classical cryptography will be threatened by quantum algorithms. Countries are thinking of and building the next generation of cryptography to resist the threats from the quantum computer. This article provides a brief overview of the innovations and applications of quantum cryptography. In addition, the readers can learn some important quantum cryptography protocols, which can be used for further self-study as well as exploring this profound and interesting quantum cryptography in the future.

Keywords: Quantum Cryptography, Quantum Key Distribution, Quantum Secure Direct Communication, Quantum Oblivious Transfer

壹、前言

密碼學發展至今已與我們的日常生活密不可分，不僅在商業、金融這些重要的領域之上，甚至是平常簡單的通訊軟體上，都需要倚賴密碼學的保護。密碼學在發展之初，密碼學家專注於如何解決加解密問題、金鑰配置問題、資料完整性問題而發展出許多密碼學的基石演算法，如公開金鑰加解密演算法 (Rivest Shamir Adleman, RSA) [56]、金鑰交換演算法 (Diffie-Hellman key exchange, D-H key exchange) [23]、進階加密標準 (Advanced Encryption Standard, AES) [53]、安全雜湊演算法 (Secure Hash Algorithm, SHA) [18]等，密碼學家接著藉由這些基石來發展各種重要的安全通訊協定，如簡單郵件傳輸協定 (Simple Mail Transfer Protocol, SMTP)、安全外殼協定 (Secure Shell, SSH)、安全電子交易協定 (Secure Electronic Transaction, SET)、安全通訊端層/傳輸層安全性協定 (Secure Socket Layer/Transport Layer Security, SSL/TLS) 等重要的基礎安全協定，這些安全協定的廣泛應用，才能保障我們生活中資料的安全傳輸。

HTTPS 是一個最廣泛使用的安全協定，所有人在瀏覽網站的時候，皆會使用 HTTPS 協定作為資料安全傳輸的加解密機制，HTTPS 的安全核心為 TLS 協定，TLS 包含了 RSA、D-H、AES 以及 SHA，這其中還需配合公開金鑰基礎建設中的憑證頒發機構 (Certificate Authority, CA) 來確保身分認證機制，以公正第三方來協助通訊雙方驗證彼此身分，避免中間人攻擊 (man-in-the middle attacks)，在雙方身分可以透過公開金鑰演算法及憑證頒發機構確認後，因為加解密速度的關係，每次一區間的傳輸會使用 D-H 金鑰交換協議來重新製造對稱金鑰，並採用 AES 來加解密傳輸的資訊，以達成前向保密 (Forward Secrecy, FS) 的目的，最後以 SHA 雜湊演算法來確保每次資料傳輸的完整性。由以上範例可以了解到這些基石扮演著舉足輕重的地位，一旦其中一個基石出現問題將會波及到所有有使用到這些演算法的上層安全協定。

1994 及 1996 年這兩年間，量子計算領域有重大突破，Shor[62]及 Grover[32]先後發表了兩個重要的量子演算法，這兩個演算法足以撼動傳統密碼學的基石，Shor 的演算法[62]可以破解 RSA 加密演算法，以及所有跟其有共同基礎的公開金鑰演算法，這意味著 TLS、SSH、SET 和 SMTP 這些常見的安全協定未來可能面臨量子電腦的重大威脅。最早在 2001 年時，科學家們在實驗室中成功分解 3*5 的質因數分解[70]，而 13 年過後，在 2014 年時[20]科學家只能分解到 56153 這個半質數，目前慶幸的是量子電腦還沒有能力可以破解目前主流 2048 長度的 RSA 演算法，但也確實讓科學家們開始規劃未來的密碼學。而 Grover 受到 Shor 演算法[62]的啟發，發明了 Grover 演算法[32]，這個演算法可以在有 N 個物件但沒有排序的資料庫以 $O(\sqrt{N})$的複雜度搜尋到資料，比傳統方法 O(N) 還要快，在這之後 Grassl 等人[31]也找到 Grover 搜尋演算法[32]與 AES 之間的關聯性，提出加速解開 AES 的方法，但總歸來說量子演算法對於 AES 只是加速找到金鑰，還沒有到 RSA 這種大量降低時間複雜度的程度，所以人類真正面臨的是量子電腦在公開金鑰演算法上的威脅。

目前有許多量子電腦相關的發展，並且皆取得重要的突破，即便不是真正的量子電腦也展示了強大的運算能力，像是 D-Wave 2X[21]，這個量子電腦計畫是由 D-Wave、Google 以及 NASA 在 2015 年開始進行的，他們採用量子退火法 (Quantum Annealing, QA) [1][38]當作量子運算的平台 (量子退火法是透過量子物理所架構的量子模型來模擬量子穿隧效用的一種演算法)，並利用低溫環境以及特殊的量子核心架構來讓粒子獲得量子效應，如此可以更真實的模擬量子退火法上面的量子模型，透過特殊模型的轉換[26]可以應用至 NP-complete 問題之上，使期能夠更有效率的找到給定問題的最佳解，透過此種方式，在單顆 CPU 上面比較[21]，量子模擬退火的效率可以勝過模擬退火法 (Simulated Annealing, SA) [39] 1000 萬到 10 億倍。目前 D-Wave 也提供 1000 到 2000 位元的量子電腦可供使用，用戶可以透過 C/C++、Python 和 Matlab 來對其進行連線，並傳遞問題及獲得結果。除此之外，IBM 也在 2016 年[37]釋出了 Quantum Experience，這個平台可以讓使用者透過 QASM-language 來撰寫量子程式，並且透過 IBM 的量子電腦來執行，一開始 IBM 釋出 5 量子位元的量子電腦，科學家已經在上面進行過無數的實驗，並發表多個實驗成果，證明其量子電腦的可行性，目前 IBM 釋出 65 位元的量子電腦可供使用，而在 2022 年之後更有計畫陸續開放 127 位元的量子電腦供科學家們使用，甚至是用於商業用途。目前大型企業及國家都想發展屬於自己的量子電腦技術，想要在下個世代依然保持領先，微軟也不例外，微軟希望能夠打造量子運算的雲端平台，讓使用者可以透過 Python 或其他程式語言，就可以讓量子電腦為其服務。我相信在不久的未來，量子電腦可能真正的可以威脅到傳統密碼的基石，這讓我們不得不思索因應之策。

量子電腦能夠如此強大的秘訣，在於其可以進行平行運算，由於量子位元有疊加的特性，N 個量子位元就可以一次表示 2^N 的解，因此量子電腦每對這些量子位元進行一次計算，等於同時評估 2^N 種可能性，這讓一些基於數學難題而保證其安全性的安全協定面臨空前的威脅。但量子電腦也非萬能，因為其演算法的侷限性，即便能夠平行化計算，但若無法控制其振幅來調整看到目標的機率，則沒有辦法能夠正確讀出最後計算的結果。不過不可否認的是，量子電腦在特定問題上能夠讓計算複雜度呈指數的下降，並且也可以有效的加速其他重要問題的效能。

密碼學家也開始重視量子電腦對傳統密碼學帶來的威脅，並且發展出另一分支稱作後量子密碼學 (Post-Quantum Cryptography, PQC)，這個分支是希望能夠用其他傳統已知的加解密演算法來抵禦量子電腦的攻擊，雖然後量子密碼學所採用的基石也都是基於數學難題之上，但這些數學難題已被證明即便有量子電腦也無法順利破解。目前許多國家已經開始成立後量子密碼的研究計畫與機構，像是歐盟的 SAFEcrypto 計畫、日本的 CryptoMathCREST 計畫。不僅如此，美國國家標準暨技術研究院也開始公開徵稿關於後量子密碼的相關演算法，目前被看好的有幾種方法分別為編碼密碼學 (code-based) [50]、網格密碼學 (lattice-based) [35]、雜湊密碼學 (hash-based) [51]等。其中在公開金鑰演算法的領域最被受關注，有四個演算法進到最後一輪的篩選中，分別為 McEliece、CRYSTALS-KYBER、NTRU 和 SABER，其中 McEliece 屬於編碼密碼學，其他三者屬

於網格密碼學。

另一方面密碼學家也嘗試用量子的特性來發展量子密碼學，將其密碼學的安全性建立在物理定律之上，而非傳統的數學難題之上。藉由這一想法，密碼學家們成功用量子特性克服了千古難題的金鑰配置問題，金鑰配置問題是如何在兩個使用者之間秘密的配置相同金鑰的問題，這是長久以來困擾著密碼學家的問題，我們稱其為量子金鑰配置 (Quantum Key Distribution, QKD) [7]，量子金鑰配置提供了我們一個配置無限長度金鑰的方法，稱其為一次性密碼 (One-Time Pad, OTP)，透過一次性密碼可以達到絕對安全的加密目標[42][63]，這是以往難以達成的目標，並且量子金鑰配置可以保證通道一但有竊聽者，可以被參與者發現，及時停止傳輸避免資料外洩。至此之後更多密碼學家投入量子密碼學領域，以量子特性來建立過往傳統密碼學的應用，以及以往難以達到的密碼學目標，甚至是全新的應用，如量子金鑰配置、量子直接通訊 (Quantum Secure Direct Communication, QSDC)、量子秘密分享 (Quantum Secret Sharing, QSS)、量子模糊傳輸 (Quantum Oblivious Transfer, QOT) 等。

1.1 量子金鑰配置

Bennett 和 Brassard 在 1984 年提出了第一個量子金鑰配置協定，簡稱為 BB84[7]，他使用了兩個正交基底以及四個不同的量子態來配置金鑰，因為量子態有不可複製性 (non-cloning) [72]以及不確定性原理 (Uncertainty Principle)，讓量子位元的狀態無法被確切得知，使得監聽者在無法事先得知量子態的情況下，貿然進行測量想竊取量子態都會導致量子態的改變，進而達成偵測監聽者的目的，並且該協定也被證明可以達到絕對安全之目的[42][63]。Bennett 更進一步在 1992 年提出非正交基底的金鑰配置方法，稱為 B92[5]，之後其他研究者也嘗試採用量子糾纏態來配置金鑰[25][16]。Zhang 等人[76]在 2001 年也成功發展出了直接利用量子通道來當作量子金鑰加解密不僅是傳統訊息，更可以加解密傳送量子訊息的協定。Zhou 等人[79]在 2004 年提出第一個量子金鑰協議的協定 (Quantum Key Agreement, QKA)，金鑰協議跟金鑰配置稍微有些不同，協議意味著大家一起創造金鑰，而非單一參與者可以決定金鑰，此概念與 D-H 金鑰交換[23]一樣，但最後結果與量子金鑰配置一樣，故筆者認為可以視為是量子金鑰配置領域的一個分支。之後 Matsumoto[49]在 2007 年提出了第一個多方的量子金鑰配置協定，此後 BB84 和其他的量子金鑰配置協定被廣泛的應用到各個量子的協定與設計之上，如監聽偵測。

此外，在 2016 年量子通訊的距離達到了 404 公里[74]。而義大利的研究團隊[69][22]近來更成功的與 LAGEOS-2 衛星交換了單光子，這個距離超過了 7000 公里。中國也在 2016 年 8 月 16 日成功建立了墨子號量子衛星[73]，該衛星可以製造量子糾纏態的通訊，該通訊距離可達 1120 公里[75]，其進行的量子糾纏態的實驗打破了 144 公里的紀錄[45]，下一步中國希望可以達成洲際的量子金鑰配置目標，這些實驗的成功可以進一步讓量子密碼的普及越來越可行。量子金鑰配置領域是量子密碼學最先發展的領域，故該領域有

許多相關的總覽型論文，讀者若有興趣，可以查閱 Scarani 等人[58]以及 Lo[44]的總覽型論文，本文鎖定在與各位介紹量子密碼主要的分支與經典的協定。

1.2 量子安全直接通訊

量子安全直接通訊允許參與者透過量子資源直接傳輸訊息到其他參與者手上，傳輸中藉由量子資源來達成加密之目的，不過這種方式也被一些密碼學家爭論並非為密碼學，這些持否定意見的學者認為量子安全直接傳輸並沒有加解密的過程，所以並不算是密碼學的一種，但這種意見還有待討論，不可否認的是量子安全直接傳輸確實是擁有量子資源才能夠達成的應用，他透過量子資源來提供訊息的保護，亦或可以看作是訊息的加解密。第一個量子安全直接傳輸是由 Beige 等人[3]在 2002 年三月提出，之後 Boström 和 Felbinger[12]在同年四月提出另一個使用量子糾纏態的量子安全直接傳輸協定，其他研究人員以其傳輸方式命名為乒乓協定。自此之後開啟了量子直接傳輸的相關研究，開拓了不同的資料傳輸模式，像是可以同時雙方直接交換訊息的量子對話 (Quantum Dialogue)[54]，又稱雙向量子安全直接傳輸 (Bidirectional Quantum Secure Direct Communication, BQSDC)；受控的量子安全直接傳輸 (Controlled Quantum Secure Direct Communication, CQSDC)[29]，這種傳輸方式會有一個額外的第三方，須由該第三方同意訊息之傳遞；受控的雙向量子安全直接傳輸 (Controlled Bidirectional Quantum Secure Direct Communication, CBQSDC)[46]，此種協定結合了受控與雙向傳輸的需求；此外還有另一個新的領域稱為 Authencryption[36] (這個字結合了 authentication 與 encryption)，該領域結合了量子金鑰配置與量子安全直接傳輸兩個特點，同時達成資料傳輸以及身分認證的目的。

1.3 量子秘密分享

量子秘密分享的目的為將訊息廣播給除了分享者以外的所有參與者，但是除了分享者的所有參與者必須要共同合作才能夠解開該秘密訊息。Hillery 等人[34]首先提出量子秘密分享的協定，他們以量子糾纏態來分享訊息給所有參與者，並且使其協定成為通用型協定，即可以參與者的人數沒有限制。往後密碼學家們也將目光放在量子訊息的分享上，在量子通訊協定上，訊息的種類分為兩種，一種是傳統或稱古典訊息，是由傳統位元組成，另一種是量子訊息，由量子位元組成，量子訊息可以真正挾帶量子資訊，這種量子態可以真正幫助量子電腦的計算，並且也可以藉由量子位元來傳遞傳統位元，因此量子位元的協定會優於傳統位元的協定。

目前量子秘密分享的分支相對少，只有一個分支為有門檻值的量子秘密分享，在這個目標之下，除了分享者以外的參與者必須要聚集到一個門檻值以上才能夠還原訊息，通常這個門檻值被相信是大於一半的參與者，因為若小於一半人數的參與者，意味著可

以複製量子訊息，這被認為與不可複製性相違背。有門檻的量子秘密分享是一個非常困難的領域，目前有不同的幾種做法，但主要都是借鏡傳統的數學方法來進行，如 Lagrange 內插法[68]、Markham 等人[47]以特殊的圖形狀態拓譜來達成的方法等，目前有門檻的秘密分享領域還尚未有多種不同的做法，雖說與該領域的難度也有密切關係，但也是一個可以繼續嘗試的領域。

1.4 量子模糊傳輸

量子模糊傳輸是一個極為特別的領域，這個傳輸協定的特性是接收者可能會有一定的機率收不到訊息，這樣的奇特傳輸可能在讀者看來非常奇怪，但可以在上面架設許多有用的應用，如安全計算、位元承諾、遠距丟銅板、同時交換秘密、同時合約簽署等，這些協定主要的運作核心就是訊息發送端無法對接收端進行欺騙。在傳統或古典的模糊傳輸領域上有一定的爭議性，許多密碼學家相信沒有百分之百安全的模糊傳輸協定，必須要引入一個公正第三方來進行協助，因此密碼學家也寄托在量子領域上能夠有機會發明不用第三方的量子模糊傳輸協定。但是因為量子模糊傳輸與量子位元承諾有一定的相關性 (密碼學家們也尚在討論中)，而在量子位元承諾有不可行定理[48][43]，這啟發了其他的密碼學家也開始懷疑量子模糊傳輸也不可行，並且也嘗試證明了量子模糊傳輸不可行[41]，但幸運的是有其他的學者利用量子的特性證明了一些不等價性[33]，所以筆者認為在量子領域上面還尚有討論的空間。

貳、相關知識

在更深入探討量子密碼學的領域之前，讀者必須要先建立一些必要的基礎知識，透過這些知識可以更好的了解之後各安全協定的核心概念與想法，如此讀者才能夠一起體會量子世界這純粹思維的美好。我們在這個章節會介紹一些量子符號的基本表示、量子疊加與糾纏的特性、一些量子密碼學基石的定理、以及最後量子相關領域中使用的邏輯閘跟測量方式。

2.1 Bra 及 Ket 符號表示

量子機器使用量子位元 (Quantum Bit, qubit) 當作訊息的載子，任何粒子只要有量子特性的粒子都可以當作量子位元，如光子、電子、原子等，因此不同的量子機器可以依照自身的需求打造，皆有粒子可當其量子位元供其使用。我們使用 Bra 和 Ket 的符號來表示所有的量子狀態。

- Bra 符號：Bra 符號以⟨· |為表示，這當中的·表示基底的向量，例如⟨0|表示一個

二維平面下面的某軸基底如$\langle 0| = (1\ 0)$。

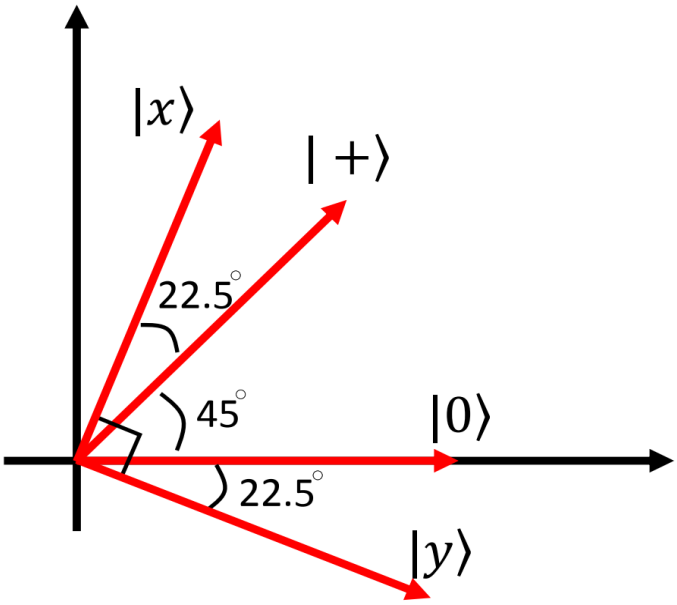
- Ket 符號：Ket 的符號為$|\cdot\rangle$，沿用上面的例子$|0\rangle = \binom{1}{0}$，他是 Bra 符號的共軛轉置，在二維平面上另一軸為$|1\rangle = \binom{0}{1}$，這組基底為二維平面下的一組標準基底，我們通常也使用此基底來表示量子態。

量子位元不局限於位元形式，也可以有更高維的表示，例如三維的量子態稱為 qutrit 表示成$|0\rangle$、$|1\rangle$、$|2\rangle$，更高維度我們稱之為 qudit，這表示了 d 維的狀態。但如同傳統電腦的運作，二進制可以表示所有進制，不同進制之間可以互相轉換，所以量子位元可以適用於所有安全協定，除非有特殊情況才需要採用更高位元的形式表示，本文章內的知識皆以量子位元來進行闡述。

2.2 量子疊加

在傳統電腦上，一個位元只能表示成不是 0 就是 1，而量子位元則可以是同使處於 0 和 1 的情況。若我們先採標準基底$|0\rangle$和$|1\rangle$ (一般稱作 Z 基底)來表示疊加的量子態$\alpha|0\rangle + \beta|1\rangle$，其中會有$|\alpha|^2$當觀測該量子位元時其量子態會塌陷在$|0\rangle$，而有另外$|\beta|^2$會塌陷在$|1\rangle$，這兩個機率的總和必為 1，也意味著$|\alpha|^2 + |\beta|^2 = 1$。一旦當塌陷發生，原本的量子態就會不復存在，截至目前為止沒有人知道這個塌陷的過程[52]，科學家嘗試以不同的論點來闡述這個過程，但仍有許多爭議，愛因斯坦與波爾乃至整個量子力學的爭論也很大原因是從該解釋而來。

另一個常見使用的基底為 X 基底，其基底表示為$|+\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$和$|-\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$，此為二維平面上的另一組基底，所以 X 基底與 Z 基底之間可以互相表示，也可以用不同基底來互相測量，但一旦測量引起狀態塌陷之後，量子的狀態就會被永遠的改變，事實上可以在平面上找到無數組基底，並且這些基底都可以互相表示，也都可以拿來當作量子態的狀態。舉例來說，如果量子位元的初始狀態為$|+\rangle$，而使用 Z 基底來進行測量，則會有$\left|1/\sqrt{2}\right|^2 = 50\%$的機會各塌陷成$|0\rangle$和$|1\rangle$，另一個有趣的現象為初始狀態越接近某一基底內的某一個軸，則塌陷成該軸的機率越高，離另一軸越遠則塌陷成另一軸的機率就越低。舉例來說，如圖一為例，其中有$|0\rangle$和$|+\rangle$兩個狀態的量子態，而我們使用$|x\rangle$和$|y\rangle$當作基底測量，則$|0\rangle$會有$cos^2(22.5^\circ) = 0.85355$的機率為$|y\rangle$，反之有$cos^2(67.5^\circ) = 0.14645 = 1 - 0.85355$。



圖一：疊加及測量範例

2.3 張量積 (Tensor Product)

張量積⊗，或稱克羅內克積 (Kronecker Product)，可以幫助我們表示一個以上的量子位元，張量積會將位元的維度拓展成$dim(|basis\rangle)^n$，此處的 *basis* 可以是任何基底，而n為量子位元的數量。例如：

$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1\begin{pmatrix}1\\0\end{pmatrix} \\ 0\begin{pmatrix}1\\0\end{pmatrix} \end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$，並且簡化成$|00\rangle$，另一個例子假設需要合併兩個處於疊加態的量子位元$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$，此處$\alpha$、$\beta$、$\gamma$及$\delta$為任意實數，並且$|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$，最後的結果為$\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$。

2.4 量子糾纏

愛因斯坦曾說過「鬼魅般的超距作用」來形容糾纏的現象，這個現象由愛因斯坦與其他兩位科學家在 1935 年[24]提出，並且 Schrödinger[59][60]以此現象接續做了許多研究。愛因斯坦他們提出的糾纏態為$1/\sqrt{2}\,(|01\rangle + |10\rangle)_{12}$，其中底標 1 和 2 是量子位元 1 和 2，稱為 EPR 糾纏對，當時被認為是 EPR 悖論。一旦測量了量子位元 1 且該狀態為$|0\rangle$，則我們可以馬上知道量子位元 2 的狀態一定為$|1\rangle$，而不需要去測量量子位元 2，這樣的現象由愛因斯坦看起來像是量子位元 1 和 2 之間存在著鬼魅般的聯絡。愛因斯坦等

人提出這樣的思想實驗舉證依照量子物理而產生此奇異現象是有問題的，在 1964 年 Bell[4]以局域性為主要假設創建了一不等式，稱為貝爾不等式，以此不等式可以驗證EPR現象是否存在，之後 Clauser 等人[19]提出了 CHSH 不等式完善了 Bell 不等式，建立了相關實驗的上限，並且在 1972 年[27]以實驗證明了糾纏的現象真實存在。至此科學界已接受了此一特殊的現象，目前常見的兩位元糾纏的狀態稱為貝爾態為$|\Phi^{\pm}\rangle_{12} = 1/\sqrt{2}\,(|00\rangle \pm |11\rangle)_{12}$、$|\Psi^{\pm}\rangle_{12} = 1/\sqrt{2}\,(|01\rangle \pm |10\rangle)_{12}$，且常見的三位元糾纏態稱為 GHZ 態，其八種狀態如下：

$$|\Psi_{000}\rangle_{123} = 1/\sqrt{2}\,(|000\rangle + |111\rangle)_{123}, |\Psi_{001}\rangle_{123} = 1/\sqrt{2}\,(|001\rangle + |110\rangle)_{123},$$
$$|\Psi_{010}\rangle_{123} = 1/\sqrt{2}\,(|010\rangle + |101\rangle)_{123}, |\Psi_{011}\rangle_{123} = 1/\sqrt{2}\,(|011\rangle + |100\rangle)_{123},$$
$$|\Psi_{100}\rangle_{123} = 1/\sqrt{2}\,(|000\rangle - |111\rangle)_{123}, |\Psi_{101}\rangle_{123} = 1/\sqrt{2}\,(|001\rangle - |110\rangle)_{123},$$
$$|\Psi_{110}\rangle_{123} = 1/\sqrt{2}\,(|010\rangle - |101\rangle)_{123}, |\Psi_{111}\rangle_{123} = 1/\sqrt{2}\,(|011\rangle - |100\rangle)_{123}$$

糾纏態無法隨便將粒子集體表示就產生，必須是要經過一些特定運算才能夠讓粒子糾纏在一起；反過來說，糾纏態無法將個別粒子拆解出來看待。其簡單的證明如：

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$
$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$
$$\neq \alpha\gamma|00\rangle + \beta\delta|11\rangle,$$

因為$\alpha\delta$和$\beta\gamma$無法為 0，所以也意味著無法將糾纏的粒子單獨拆成單一粒子。

讀者可能會納悶，依照糾纏態的特性來看是不是資訊傳輸的速度已超過光速？但我們可以更仔細的看糾纏態$1/\sqrt{2}\,(|01\rangle + |10\rangle)_{12}$，假設我們測量量子位元 1，代表我們有 50%的機會獲得$|0\rangle$以及$|1\rangle$，這意味著我們沒有辦法控制量子位元 2 的狀態，這也代表我們沒有辦法透過糾纏態來瞬間傳遞訊息，實務上必須要以傳統的傳輸方式來當作輔助，才有辦法傳遞訊息，因此使用糾纏態的資訊傳遞速度也沒有超過光速。

2.5 量子不可複製性[72]

若對一量子位元的狀態一無所知，即$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$，則我們無法完美的複製他，若我們希望藉由測量來知道該量子態為何，但因為我們對一開始的α和β未知，所以所有的測量都會毀壞最原始的量子態。簡單的證明如下，假設我們有一個運算$U_{cloning}$可以複製量子位元，則該運算會有以下效果：

$$U_{cloning}(|\phi\rangle|0\rangle) = |\phi\rangle \otimes |\phi\rangle = \alpha\alpha|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta\beta|11\rangle。$$

但因為其運算為線性運算，故該式子可以重寫成：

$$U_{cloning}(|\phi\rangle|0\rangle) = U_{cloning}(\alpha|00\rangle + \beta|10\rangle)$$
$$= U_{cloning}(\alpha|00\rangle) + U_{cloning}(\beta|10\rangle) = \alpha|00\rangle + \beta|11\rangle。$$

比較兩個式子我們可得$\alpha\alpha|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta\beta|11\rangle \neq \alpha|00\rangle + \beta|11\rangle$，因此我們

無法找到$U_{cloning}$。雖然不存在完美的複製運算，但 Bužek 和 Hillery[15]找到了一個運算可以提供$5/6$相近的複製辦法，在這之後還有其他科學家也投入相關研究[30][14][71]。

2.6 量子邏輯閘

量子邏輯閘是量子計算的核心組成要件，就跟傳統電腦的 AND、OR、NOT、NAND 邏輯閘一樣，並且在實際應用的時候還要考慮量子電路合成問題。而所有的量子邏輯閘皆為么正運算 (unitary operation)，么正運算為 one-to-one 且 onto (bijective)，這也意味著量子運算皆為可逆運算即$UU^* = I$，從真值表來看，代表輸入到輸出可以互相推導並且一一對應，且輸入數量與輸出數量必定一致，這樣的特性與傳統邏輯閘有非常大的差異。接下來這章會用兩個子小節來闡述常見的單一量子位元邏輯閘與多重量子位元邏輯閘。

2.6.1 單一量子位元邏輯閘

單一量子位元邏輯閘是作用在單一量子位元上面的邏輯閘，常見的單一量子位元邏輯閘有五個，分別是 I, X, Y, Z 和 H (Hadamard) 如下：

$$I|0\rangle \mapsto |0\rangle,\ I|1\rangle \mapsto |1\rangle,\ X|0\rangle \mapsto |1\rangle,\ X|1\rangle \mapsto |0\rangle,$$
$$Y|0\rangle \mapsto i|1\rangle,\ Y|1\rangle \mapsto -i|0\rangle,\ Z|0\rangle \mapsto |0\rangle,\ Z|1\rangle \mapsto -|1\rangle,$$
$$H|0\rangle \mapsto 1/\sqrt{2}\,(|0\rangle + |1\rangle),\ H|1\rangle \mapsto 1/\sqrt{2}\,(|0\rangle - |1\rangle)。$$

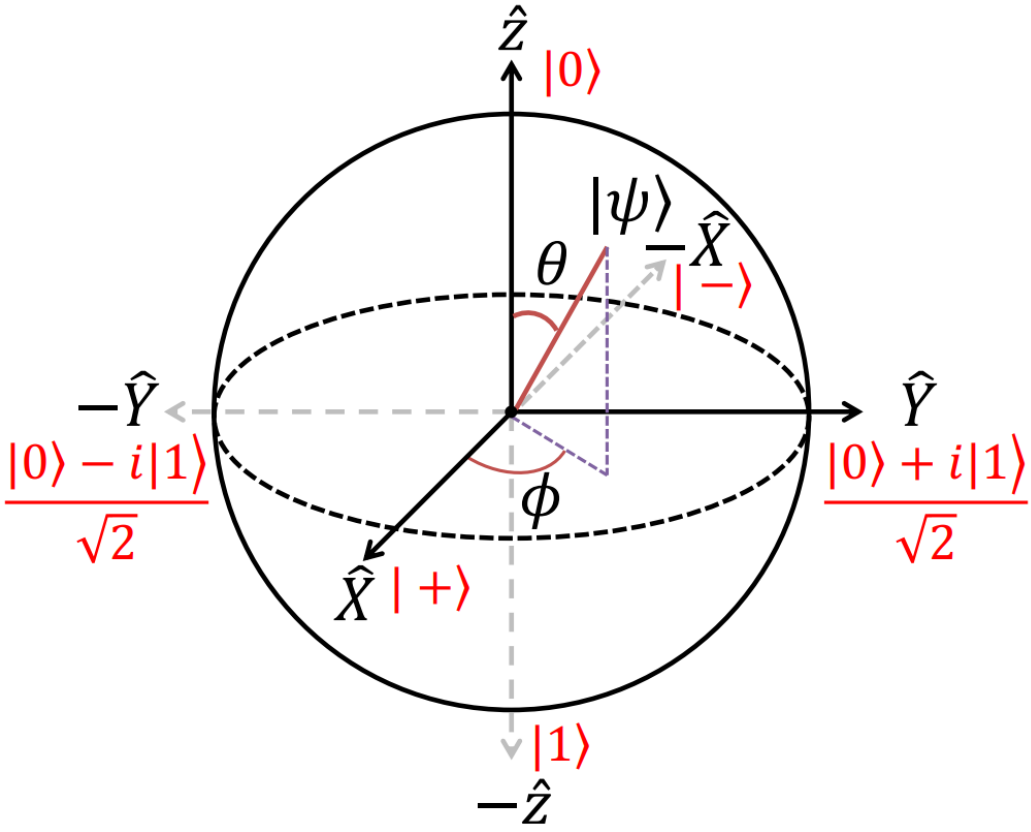
I, X, Y, Z 稱作 Pauli 矩陣，Pauli 矩陣和 Hadamard 矩陣表示如下：

$$I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\ Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}。$$

一般來說，我們在描述量子位元行為時是採用布洛赫球面 (Bloch Sphere) 模型來進行闡述，該模型很好的描繪了單一量子位元的所有行為，所有的量子態都是在該球面上的任意一點，因此么正運算會讓量子態可以順利的轉換成球面上任何一點。而所有運算皆可以被兩個變因所決定，如圖二所示，由於是球模型的關係只要控制θ與ϕ兩個的角度即可任意改變量子態，概念與極座標一樣，這樣讓三維的三個座標變因降成兩個。不同的 I、X、Y、Z 運算被視為以該球模型的不同軸進行旋轉，不同軸如圖二$\hat{Z}$、$\hat{X}$和$\hat{Y}$軸所示。如 I 運算是沿著$\hat{X}$軸選轉0π，X、Y 和 Z 運算是分別沿著$\hat{X}$、$\hat{Y}$和$\hat{Z}$軸旋轉π，而 H 運算則是沿著$\hat{X}$軸轉$\pi/2$。至此我們可以針對不同軸定義出不同的旋轉矩陣如下：

$$R_X(\theta) = \begin{pmatrix} cos\frac{\theta}{2} & -i\,sin\frac{\theta}{2} \\ i\,sin\frac{\theta}{2} & cos\frac{\theta}{2}\end{pmatrix},\ R_Y(\theta) = \begin{pmatrix} cos\frac{\theta}{2} & -sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & cos\frac{\theta}{2}\end{pmatrix},\ R_Z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix}。$$

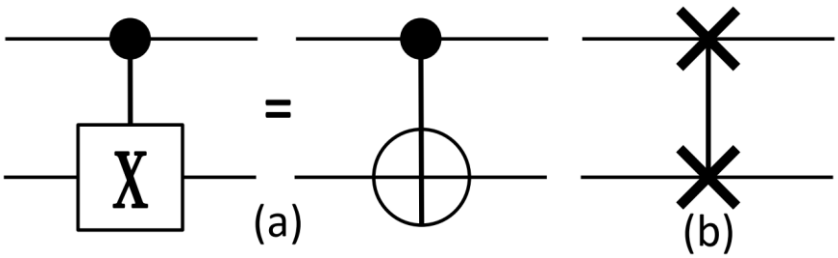
這邊有一個事情要請讀者特別注意，若是布洛赫全球模型的話θ還是原本的角度，但若是布洛赫半球模型的話則是$\theta/2$，也因為各學者一開始討論的模型差異，容易在角度的描述上面會有差異，而這些差異都是源自於該模型的引用差異所致。因為以矩陣形式套論皆是建立在半球模型之上，並且可以用圖一的平面想像所有運算的結果，所以筆者已將上述旋轉矩陣以半球轉換過。



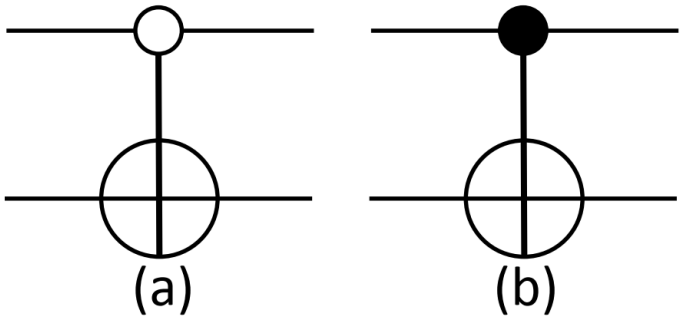
圖二：布洛赫球面量子模型

2.6.2 多重量子位元邏輯閘

多重量子位元邏輯閘可以一次作用在兩個以上(含)的量子位元上面，常見的有控制反閘 (controlled-not, CNOT) 和交換閘 (SWAP)，如圖三的 (a) 和 (b) 所示。在控制反



圖三：CNOT 與 SWAP 邏輯閘



圖四：zero-control 與 one-control

閘的第一個位元為控制位元，而第二個位元為目標位元，一旦控制位元的輸入值符合條件，則目標位元會作動，以控制反閘為例，若控制位元輸入值為$|1\rangle$則目標位元則會進行反閘運算，如目標位元的值為$|0\rangle$則會改變成$|1\rangle$，反之則改變成$|0\rangle$。事實上，控制位元的種類有兩種，一是 one-control (如圖四 (b) 所示) 另一個則是 zero-control (如圖四 (a) 所示)。one-control 是控制位元為$|1\rangle$的時候目標位元作動，而 zero-control 則是控制位元為$|0\rangle$的時候目標位元作動，一般稱呼的控制非閘都是 one-control，若沒有特別強調，則皆是 one-control。另一個常見的邏輯閘為交換閘，一旦交換閘作動，可以將兩個量子位元進行交換，例如$SWAP(|01\rangle_{12}) = |10\rangle_{12}$。另外，控制非閘是最簡單能夠創造糾纏態的邏輯閘，如：

$$CNOT\left(1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes |0\rangle\right) = CNOT\left(1/\sqrt{2}\,(|00\rangle + |10\rangle)\right)$$
$$= 1/\sqrt{2}\,(CNOT(|00\rangle) + CNOT(|10\rangle)) = 1/\sqrt{2}\,(|00\rangle + |11\rangle)。$$

2.7 貝爾測量

一般來說，無法以 Z 或者是 X 基底的測量方式來分辨一對貝爾糾纏態處於哪一個貝爾態之中，例如若目前有一對糾纏態處於$|\Phi^+\rangle_{12} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{12}$之中，若我們使用 Z 基底來進行測量，則只會獲得不是$|00\rangle_{12}$就是$|11\rangle_{12}$，所以我們無法區分其貝爾態，即便我們擁有大量的樣本可以測量並得到 50%的$|00\rangle_{12}$以及$|11\rangle_{12}$，但也無法確定這個樣本裡面是本來就存在著 50%的$|00\rangle_{12}$和$|11\rangle_{12}$，亦或是$|\Phi^{\pm}\rangle_{12} = 1/\sqrt{2}\,(|00\rangle \pm |11\rangle)_{12}$。因此需要而外的基底轉換來確定這些糾纏態特定的貝爾態，事實上只需要一個控制反閘和 Hadamard 閘就可以正確分辨該糾纏態為何種貝爾態，而四種貝爾態分別對應$|00\rangle_{12}$、$|01\rangle_{12}$、$|10\rangle_{12}$和$|11\rangle_{12}$這四個 Z 基底測量的結果。舉例來說如下：

$$|\Phi^+\rangle_{12} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{12}$$
$$\xrightarrow{CNOT_{12}} 1/\sqrt{2}\,(|00\rangle + |10\rangle)_{12} = 1/\sqrt{2}\,(|0\rangle + |1\rangle)_{12} \otimes |0\rangle$$
$$\xrightarrow{H_1} |0\rangle_1 \otimes |0\rangle_2 = |00\rangle_{12}。$$

更進一步來說，若要分辨多個糾纏態的話，也可以透過這種運算來進行如：

$$CNOT_{x_1x_N}, CNOT_{x_1x_{N-1}}, \ldots, CNOT_{x_1x_2}, H_{x_1}$$ ，

此處 N 為需要辨識幾顆量子糾纏態，經過這些運算後，其糾纏狀態會被破壞掉。除此之外，控制反閘也可以重新製造糾纏態，只要將上述運算反向做回去則可以獲得糾纏態。

參、量子密碼學應用與發展

在介紹量子密碼學之前，讀者還要先知道一些基礎知識與性質，如此才比較能了解在真正實作這些協定的時候會碰到哪些實作上的問題。如先前所提到，任何具有量子特性的粒子皆可以做為量子訊息的載體，稱為量子位元，而量子位元可以攜帶傳統訊息與量子訊息。由於量子位元皆非常的微小，以至於很容易與環境產生互動進而被影響其狀態，也稱量子相干性，而粒子的狀態隨著時間消失的過程我們稱之為去相干或消相干，倘若量子態無法很好的被保存，則容易使得量子電腦在運算過程中產生錯誤。因此在討論量子電腦或量子機器的組成，都需要著重在三個面向，分別是計算、容錯與儲存，這意味著一個可用的通訊也通常要考慮這些面向。

目前因為專業分工的關係，通常量子密碼學家在設計協定的時候，都會先假設底層的量子通道的錯誤率是足夠低的，並且所有的量子態也可以被很好的保存到協定結束。但這樣的想法會有點不切實際，所以另一部分科學家則專注在改善不完美的通道，或者是增加量子位元的容錯能力，意即量子錯誤更正碼。Shor[64]在 1995 年使用了 9 個量子位元來保護 1 個量子位元，使其可以克服位元及定相錯誤 (bit and phase flip error)，一般傳統位元只會有位元錯誤，即"0"被判定成"1"，而"1"被判定成"0"，但量子位元還多了一個定相錯誤。我們以一個簡單的例子來講解這兩種錯誤，假設我們要傳遞$|0\rangle$，當位元錯誤發生時，其狀態會被改變成$|1\rangle$；若我們要傳遞$|+\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$，在同樣發生位元錯誤時則結果為$1/\sqrt{2}\,(|1\rangle + |0\rangle)$，我們可以得知這個結果不變；但若$|+\rangle$發生定相錯誤則會使其變成$|-\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$。這種錯誤在傳遞一個狀態未知的量子態時尤其嚴重。同年 Calderbank 和 Shor[17]以及 Steane[67]兩個研究團隊獨立發表了 7 個量子位元的量子錯誤更正碼，我們現在稱之為 Calderbank-Shor-Steane (CSS) 碼。而在 1996 年 Bennett 等人[10]和 Laflamme 等人[40]更進一步發現了 5 個量子位元的錯誤更正碼，並且 5 個量子位元的錯誤更正碼也被認為是最佳碼。

但另一方面，通訊不僅只有兩端的單點通訊問題要被考慮而已，量子態在經過長距離的傳輸也容易讓其消相干 (量子態會隨著時間或者跟環境作用而漸漸改變)，尤其是量子糾纏態更難以被直接傳輸到遠端。因此量子中繼器 (Quantum Repeater) 就顯得格外的重要，但因為量子有不可複製性的限制，想要成功製造量子中繼器也成為一個難題。Bennett 等人首先提出兩個針對糾纏態純化 (Purification) [9]以及精煉 (Concentration) [6]

的方法，如此可以有效的維持其糾纏態的狀態。而 Briegel 等人[13]則提出了量子中繼器的方法，透過不斷的糾纏交換來配置糾纏態到遠端接收者的手上，如此避免了兩點之間的長距離傳輸，可以將糾纏態的傳輸侷限在兩個近距離的點，透過多個子節點則可以達成將糾纏態傳遞到遠方的概念。目前已有許多糾纏態純化[55][65]、精練[77][61]與量子中繼器[57][2]的方法被廣泛的探討，更甚者科學家們還進一步實驗更複雜糾纏態的純化與精煉如 GHZ 態[78]和叢集態 (Cluster State) [66]等。由於這些科學家的努力，現在密碼學家們可以更專注在量子安全協定的設計之上，也更有機會讓這些協定能夠真正的被實作。

接下來這個章節會介紹一些有了量子資源後才能夠真正運作的重要量子通訊協定，分別為量子密集傳輸[11]、量子瞬間傳輸[8]、量子金鑰配置 (BB84) [7]和另一個重要且有趣的量子金鑰配置協定 (B92) [5]。這些協定成為了許多量子安全協定的基石。

3.1 量子密集傳輸[11]

量子密集傳輸 (Quantum Dense Coding) [11]在 1992 年由 Bennett 和 Wiesner 所提出，一開始稱為超密集傳輸，後來改為密集傳輸。這個協定的目的是傳遞一個量子位元，但最後接收方可以讀出兩個傳統位元的訊息，也因為一個量子位元就可以取得兩個傳統位元的訊息，故稱為「密集」傳輸。在這個場景中，一樣有兩個角色，傳送方 Alice 與接收方 Bob，雙方必須在傳輸前先互相配置好糾纏態，如$|\phi\rangle_{12} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{12}$，其中量子位元 1 在 Alice 手上，而量子位元 2 在 Bob 手上 (如圖五(a))，當傳輸開始後，Alice 會透過 *I, X, Y, Z* 四種運算分別代表四種不同的傳統位元訊息"00"、"01"、"11"與"10"，來對量子位元 1 透過欲傳送的訊息來做相對應的運算 (如圖五(b))，之後將量子位元 1 傳輸到 Bob 手上，最後 Bob 對手上的$|\phi\rangle_{12}$進行貝爾測量 (如圖五(c)、(d))，藉由$|\phi\rangle_{12}$由初始態轉換到四個不同的貝爾態的差異，就可以推估出 Alice 做了何種運算，並得知欲傳遞的傳統位元訊息。其整個過程如圖五所示。

在此舉一個簡單的例子，假設 Alice 和 Bob 雙方預先準備的貝爾態為$|\Phi^+\rangle_{12} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{12}$，並且量子位元 1 和 2 分別在 Alice 和 Bob 手上(如圖五(a))，之後 Alice 選擇 *Y* 運算代表欲傳遞的兩個傳統訊息為"11"，此舉會將糾纏態轉變成$|\Psi^-\rangle_{12} = 1/\sqrt{2}\,(|01\rangle - |10\rangle)_{12}$(如圖五(b))，之後 Alice 將量子位元 1 傳給 Bob，並且 Bob 進行貝爾測量(如圖五(c)和(d))，這會導致$|\Psi^-\rangle_{12}$的變化如下：

$$|\Psi^-\rangle_{12} = 1/\sqrt{2}\,(|01\rangle - |10\rangle)_{12} \xrightarrow{CNOT_{12}} 1/\sqrt{2}\,(|01\rangle - |11\rangle)_{12} = 1/\sqrt{2}\,(|0\rangle - |1\rangle)_1 \otimes |1\rangle_2 \xrightarrow{H_1} |1\rangle_1 \otimes |1\rangle_2 = |11\rangle_{12}。$$

最後 Bob 會獲得$|11\rangle_{12}$的測量結果，在這個例子上我調整了四個運算所對應的四個傳統位元訊息，故最後 Z 基底獲得的測量結果即是最後的傳統位元訊息。

3.2 量子瞬間傳輸[8]

量子瞬間傳輸 (Quantum Teleportation) [8]是一個非常有趣的量子資源應用。相信許多人都看過星際迷航 (Star Trek) 裡的一句經典台詞「Beam me up, Scotty」，裡面神奇的瞬間傳輸機器可以把人傳送回母艦，或者是從母艦傳送到其他地方。但這種傳輸方式不免受到許多人的質疑，像是既然可以瞬間傳輸資料到遠方，那其資料傳輸速度有超過光速嗎?或甚至是有些 youtuber 會把量子瞬間傳輸認為是一種複製器，可以瞬間在遠處複製一個一模一樣的物體，並且需要消滅本體，但這種思維概念完全是錯誤的，讀者可以透過前述的不可複製原理就可以知道量子瞬間傳輸不可能是一個複製器。

Bennett 等人[8]在 1993 年提出了瞬間傳輸的方法，可以藉由一對糾纏態的幫忙，瞬間將一個任意的量子態傳送到遠方，但這需要傳輸者 Alice 及接收者 Bob 預先先分享一對糾纏態$|\Phi^+\rangle_{23} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{23}$，其中量子位元 2 在 Alice 手上，而量子位元 3 在 Bob 手上 (如圖六(a))，之後 Alice 將要進行瞬間傳輸的量子態$|\varphi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$與量子位元 2 做貝爾測量 (如圖六(b)和(c))，此時量子位元 1 的量子態就會被瞬間傳輸到遠方的量子位元 2 之上，但是其狀態還不完全正確 (如圖六(d))，需要透過 Alice 和 Bob 的額外訊息傳遞才有辦法使其恢復狀態，其全部過程如圖六所示。由此可知，量子瞬間傳輸的速度並沒有超越光速，因為必須還是要靠 Alice 和 Bob 雙方額外的互相溝通才能夠復原量子態，而所有的溝通方式都侷限於光速，另外量子位元 1 的量子態是直接轉移到量子位元 3 之上，量子位元 1 和 2 則成了四種貝爾態的其中一種，故並無複製一事。

以下我們以一個簡單的例子來進行說明，Alice 和 Bob 預先分享了$|\Phi^+\rangle_{23} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{23}$，並且欲瞬間傳輸的量子位元為$|\varphi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$，Alice 在量子位元 1 和 2 上實施貝爾測量如下：

$$|\varphi\rangle_1 \otimes |\Phi^+\rangle_{23} = (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{23}$$

$$= 1/\sqrt{2}\,(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)_{123}$$

$$\xrightarrow{CNOT_{12}} 1/\sqrt{2}\,(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)_{123}$$

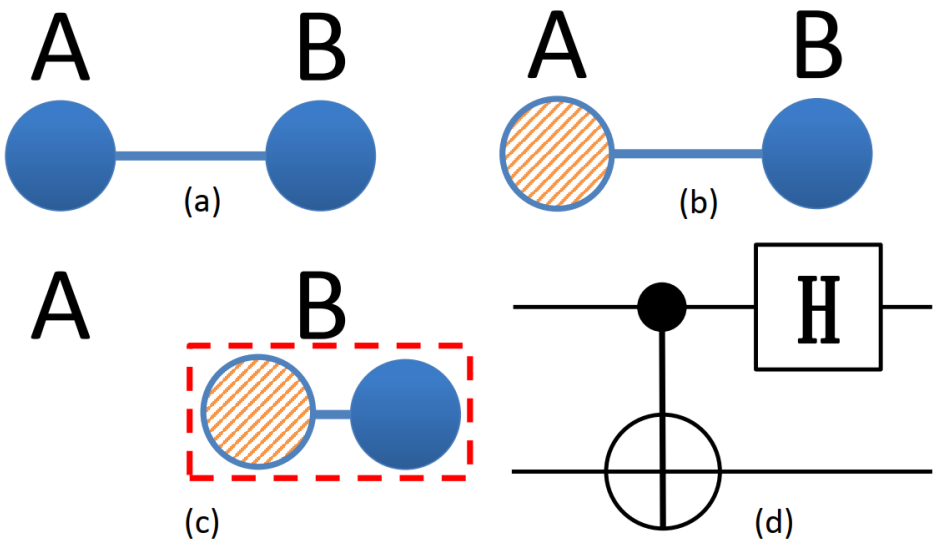
$$\xrightarrow{H_1} 1/\sqrt{2}\begin{pmatrix} \alpha\, 1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes |00\rangle + \alpha\, 1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes |11\rangle \\ +\beta\, 1/\sqrt{2}\,(|0\rangle - |1\rangle) \otimes |10\rangle + \beta 1/\sqrt{2}\,(|0\rangle - |1\rangle) \otimes |01\rangle \end{pmatrix}_{123}$$

$$= 1/2\,(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle)_{123}$$

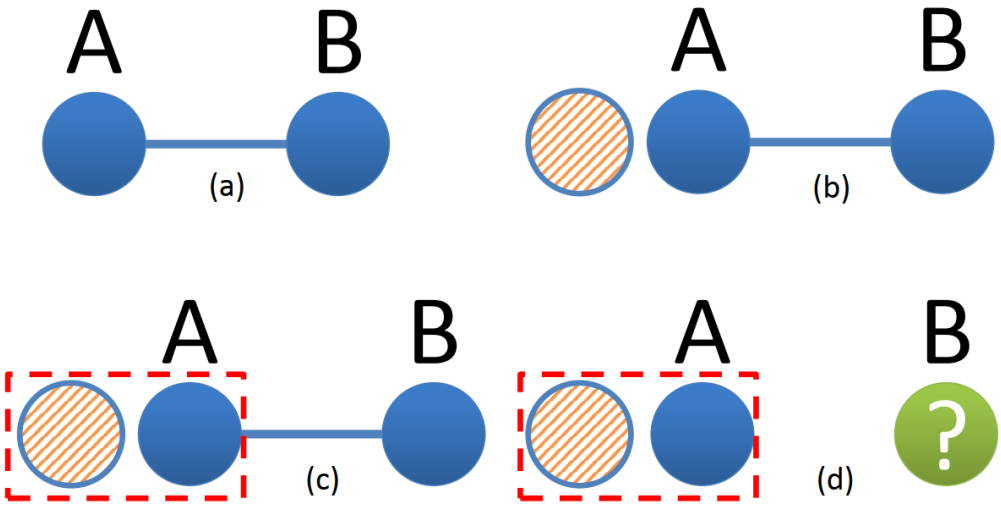
$$= \frac{1}{2}\begin{pmatrix} \alpha|000\rangle + \beta|001\rangle \\ +\alpha|011\rangle + \beta|010\rangle \\ +\alpha|100\rangle - \beta|101\rangle \\ +\alpha|111\rangle - \beta|110\rangle \end{pmatrix}_{123} = \frac{1}{2}\begin{pmatrix} |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) \\ +|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) \\ +|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) \\ +|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle) \end{pmatrix}_{123} \quad 。$$

藉由最後的結果可知若量子位元 1 和 2 測量到$|00\rangle_{12}$、$|01\rangle_{12}$、$|10\rangle_{12}$與$|11\rangle_{12}$，則量子位元 3 必須藉由 I、X、Z 和 Y 來將其狀態恢復成$= (\alpha|0\rangle_3 + \beta|1\rangle_3)$。否則其量子的

狀態有誤會影響到之後的應用與計算。



圖五：量子密集傳輸範例



圖六：量子瞬間傳輸範例

3.3 量子金鑰配置(BB84)[7]

金鑰配置問題是一個困擾密碼學家很久的難題，假設 Alice 和 Bob 因為需要互相通訊所以需要一個加密的通道，也因此雙方需要有一把對稱式金鑰讓雙方能夠進行加解密，所以發送方 Alice 必須要秘密傳遞一把金鑰給 Bob，但問題來了，因為該金鑰非常重要，所以也要透過加密通道來傳輸，但這個加密通道的金鑰又要從哪裡來？這是一個雞生蛋蛋生雞的問題，所以才會困擾密碼學家許久的時間，傳統密碼學直到公開金鑰演算法問

世之後，才真的順利解決這個難題。

但是金鑰配置問題在擁有量子資源之後就可以輕易做到，Bennett 和 Brassard[7]在 1984 年提出第一個量子金鑰配置協定，僅透過 Z 基底的|0⟩和|1⟩及 X 基底的|+⟩和|−⟩四種狀態，就可以做到量子版本的金鑰配置協定，並且這種方法可以任意的產生金鑰，即一次性密碼表 (one-time pad)，這種密碼使用一次即丟，並且隨機產生，所以整個量子金鑰協定也被證明是無條件安全的通訊協定 (Unconditionally Secure) [42][63]。除此之外，該協定也保證可以有效地抓出監聽者，意即只要有 Alice 和 Bob 以外的人想要竊取雙方的通訊，皆會導致初始量子態的改變，並且造成過高的錯誤率，使 Alice 和 Bob 可以知道該通道已被竊聽。

目前 BB84 協定[7]可以輕易直接被實作出來，因為其過程並不需要量子態的保存，所以已有許多軍事及商業版本的機器，其步驟分成 7 個步驟如下：

步驟1：Alice 準備一個二元的字串當作金鑰

步驟2：她對每個位元任意選擇 Z 或 X 基底

步驟3：她依照每個位元的值及基底準備對應的量子態並傳送給 Bob

步驟4：Bob 對每個位元隨機選擇 Z 或 X 基底

步驟5：他依照選擇的基底來測量並獲得測量結果

步驟6：Alice 和 Bob 公布使用的基底，雙方互相比對基底，只留下相同基底的量子態，這意味著將有 50%的位元將被捨棄

步驟7：雙方將其同基底的量子態轉成字串金鑰，|0⟩與|+⟩皆代表 0，反之代表 1，至此雙方成功配置相同金鑰。以表一為例，其雙方最後的金鑰為"1100"。

以上為 BB84 的基本想法範例，只要雙方的基底相同，則 Bob 最後獲得的結果會與 Alice 一開始準備的狀態一致，這也意味著若結果不一致可能存在著監聽者，所以可以從金鑰裡面隨機選一些來當作通道檢測。舉例來說監聽者 Eve 想要獲得 Alice 和 Bob 的量子狀態，所以她在步驟 3 和 4 之間插入雙方的通訊，並且因為她並不清楚 Alice 的基底及狀態，所以她只能隨機使用基底來測量，但因為該測量有可能會改變到初始的量子態，如表二所示 (此處為了要展示其1/4的機率可以抓到監聽者，所以此處的四個金鑰位元全部拿來做檢測，實際的 BB84 協定並不需要拿所有金鑰來做通道檢測)，所以會導致最後的金鑰將會有無法預期的錯誤，例如 Alice 一開始準備的量子態為|0⟩，但 Eve 選錯 X 基底並測量導致狀態改變為|+⟩，而當 Bob 即便選擇正確的 Z 基底則也可能獲得錯誤的結果，因此我們可以推估出需要 Eve 選錯基底，這有 50%的機率，以及 Bob 最後獲得錯誤的結果，這也有 50%的機率，意味著一顆檢測粒子有1/4的機率可以發現竊聽者，因此我們可以得到$1-(3/4)^N$這個檢測成功率的式子，此為可抓到監聽者 Eve 的機率，其中 N 為檢測的粒子，可以依照安全需求性來獲得可接受的檢測成功率。

表一：BB84 範例(不含監聽者)

步驟 1	1	1	0	1	0	0	0	1
步驟 2	X	Z	Z	Z	X	X	Z	X
步驟 3	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$
步驟 4	X	X	X	Z	X	Z	Z	Z
步驟 5	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
步驟 6	V			V	V		V	
步驟 7	1			1	0		0	

表二：BB84 範例(含監聽者)

步驟 1	1	1	0	1	0	0	0	1
步驟 2	X	Z	Z	Z	X	X	Z	X
步驟 3	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$
Eve 基底	X	Z	X	Z	Z	Z	X	X
Eve 結果	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
步驟 4	X	X	X	Z	X	Z	Z	Z
步驟 5	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
步驟 6	V			V	V		V	
步驟 7	1			1	0		1	
通道檢查	pass			pass	pass		fail	

3.4 量子金鑰配置(B92)[5]

在了解 BB84[7]的運作原理之後，應該會很難相信在擁有量子資源之後，居然可以以這麼簡單的方式解決困擾著密碼學家這麼久的問題。這也是筆者一直覺得量子領域有趣的地方，可以天馬行空的想像，並且在腦中進行思想實驗，就跟當年的愛因斯坦一樣，最後用一些數學來驗證思考的結果，這是一個非常有趣的過程。接下來我們來介紹另一個十分有趣的金鑰配置協定 B92[5]，他是由 Bennett 單獨在 1992 所提出，並且只使用任兩個非正交狀態就可以做到，整體來說對設備的要求會較 BB84 簡單，且不用額外比對基底的過程，讓我們見識了另外一種有趣的思維。B92 協定一共包含了 5 步如下：

步驟1：Alice 與 Bob 協調好以量子態$|0_Z\rangle$和$|-_X\rangle$表示傳統位元訊息"0"和"1"，其中底標 Z 和 X 表示基底 (為了方便讀者對照加上這些底標)，Alice 隨機產生金鑰串

步驟2：Alice 依照其金鑰串的每個位元來傳遞特定的量子態給 Bob

步驟3：Bob 隨機用兩個基底對每個位元去接收其量子態

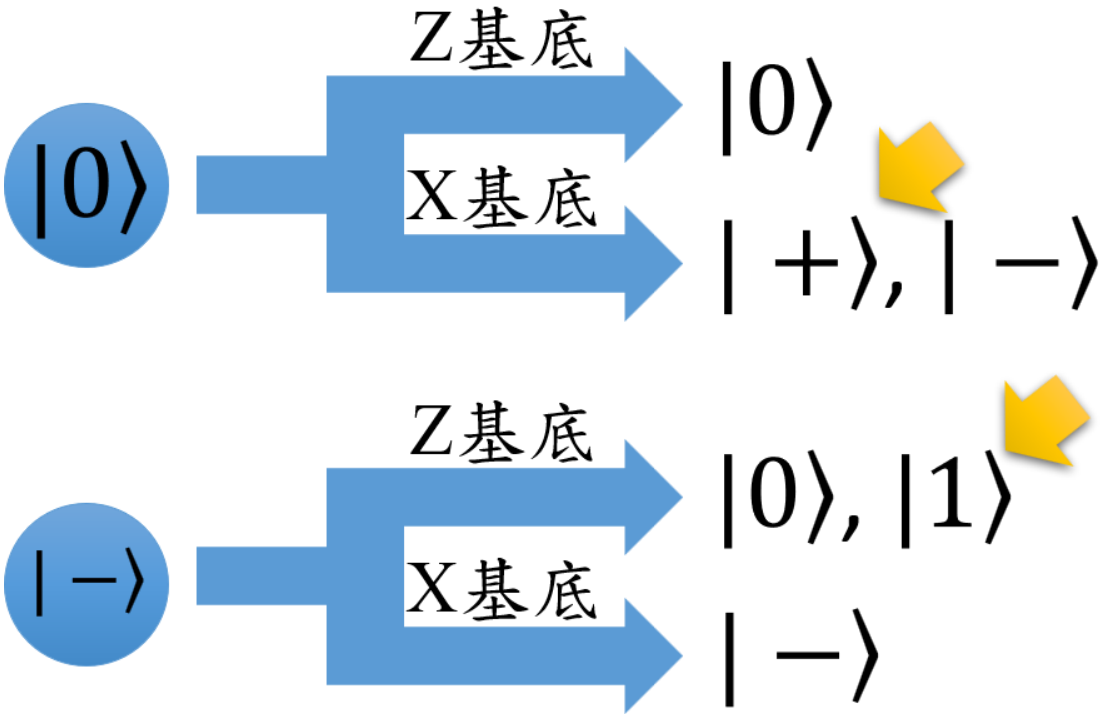
步驟4：Bob 將確定的量子位元測量結果留下

步驟5：Bob 公布他留下哪些位置的量子態，之後雙方就可以用這些位子的位元訊息來

當作金鑰串。所有簡單的範例如表三所示

我們可以整理一下金鑰產生的邏輯，只要 Bob 能確定從 Alice 傳過來的量子態是出自何種初始態，就可以把該位元留下當作金鑰，如圖七範例，若 Bob 測量結果為$|+\rangle$和$|1\rangle$，則他可以確定這一定是他選錯基底才能夠測量到的，並且能夠確定其初始態分別一定是$|0\rangle$和$|-\rangle$。但倘若 Bob 測量到$|0\rangle$和$|-\rangle$這兩種狀態，他無法確定到底 Alice 傳送的初始態為何，因為如果是測量到$|0\rangle$，他有可能是因為 Alice 傳送$|0\rangle$且 Bob 選到一樣的基底才測到，或者是 Alice 傳送$|-\rangle$而 Bob 選錯基底，但剛好測到$|0\rangle$；Bob 測量到$|-\rangle$則與前述是一樣的狀況。所以僅有 Bob 測量到$|+\rangle$和$|1\rangle$才能當作金鑰"0"和"1"留下。在經過表三的簡單範例後，我們可以觀察出 B92 協定會丟棄掉 75%的量子位元，僅有 25%可以當作金鑰來使用，這比 BB84 要丟棄 50%還要來得多，但其他的優點就是對硬體設備的要求相對較低，故更容易實作。

現在我們簡單討論一下，倘若中間若有 Eve 監聽，該如何找出監聽者以及偵測成功率為何。Eve 會使用和 Bob 一樣的方式來進行測量，所以 Eve 也會知道 25%的金鑰，只有剩下 75%她會隨便傳量子態，在這之中她有 50%的機率選到錯誤的基底，最後 Bob 在接收的時候會有 25%的機率獲得他以為正確的金鑰，並由這些金鑰去做通到檢測，因此可以總結一個檢測粒子會有 75%×50%×25%=9.375%的機率抓到 Eve。



圖七：B92 金鑰產生範例

表三：B92 範例

步驟 1	1	1	0	1	0	0	0	1
步驟 2	$\|-_X\rangle$	$\|-_X\rangle$	$\|0_Z\rangle$	$\|-_X\rangle$	$\|0_Z\rangle$	$\|0_Z\rangle$	$\|0_Z\rangle$	$\|-_X\rangle$
步驟 3	X	X	X	Z	X	Z	Z	Z
步驟 4	$\|-_X\rangle$	$\|-_X\rangle$	$\|+_X\rangle$	$\|1_Z\rangle$	$\|-_X\rangle$	$\|0_Z\rangle$	$\|0_Z\rangle$	$\|0_Z\rangle$
步驟 5			V	V				

3.5 量子金鑰通道協定[76]

前面介紹的方法都是使用量子資源產生傳統位元金鑰，並且之後使用其金鑰來加解密。倘若我們都擁有量子資源了，可否直接透過量子資源來幫助我們傳遞資訊呢？意即量子資源就是我們加解密的金鑰。這種思維也很大程度啟發了量子安全直接傳輸這一領域，Zhang 等人[76]在 2001 年提出了此協定，而後 Gao 等人[28]在 2005 年提出了一攻擊方法，並同時也給一有效的改良方法。這個協定十分簡單，Alice 與 Bob 希望透過糾纏態來當作其量子通道，且以 $\vdash |0\rangle$和 $\vdash |1\rangle$來表示"0"和"1"的傳統位元訊息，其中包含了 3 步驟如下：

步驟1：Alice 和 Bob 先配置貝爾態$|\Phi^+\rangle_{AB} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{AB}$，其中量子位元 A 和 B 分別在 Alice 和 Bob 手上

步驟2：在要加密訊息之前，雙方會先用$R_Y(\theta)$在他們手上的糾纏態量子上，之後 Alice 使用$CNOT_{Am}$在他要傳送的量子位元$|\varphi\rangle_m$上，並且將量子位元m傳送給 Bob

步驟3：在 Bob 接收到量子位元 m 之後，他一樣執行$CNOT_{Bm}$就可以解糾纏並且還原$|\varphi\rangle_m$

在此舉一個簡單的例子，假設 Alice 的秘密訊息為$|0\rangle_m$，所以當她執行完$CNOT_{Am}$時，其糾纏態為$1/\sqrt{2}\,(|000\rangle + |111\rangle)_{mAB}$，而最後 Bob 接收到量子位元$m$並且執行$CNOT_{Bm}$時，其量子態為 $1/\sqrt{2}\,(|000\rangle + |110\rangle)_{ABm} = 1/\sqrt{2}\,(|00\rangle + |11\rangle)_{AB} \otimes |0\rangle_m$，從該狀態來看可發現 Bob 成功獲得量子位元$m$。

但即便雙方採用量子通道進行傳輸 (糾纏態)，也是需要進行通道檢測才能確保通道內無監聽者，而這個協定保證了 50%的偵測率，因為該協定是一開始就會配置好糾纏態來當作量子通道，並且之後僅有一個量子位元m在實體通道傳輸，故監聽者 Eve 只能在量子位元m傳輸的時候動手腳，她有可能會趁機偷偷糾纏一顆她的粒子進來，並且想要學 Bob 的方式獲得量子位元m的訊息。舉例來說，一旦 Eve 可以讓整個系統的糾纏狀態變成$|\xi\rangle_{ABE} = 1/\sqrt{2}\,(|000\rangle + |111\rangle)_{ABE}$，其中量子位元 E 在 Eve 手上，則她就可以跟 Bob 一樣取得訊息，因此該協定才會有一個秘密的$R_Y(\theta)$，每當要糾纏量子位元m之前雙方都要運作這個旋轉矩陣進去，這樣可以確保如果 Eve 也在該系統中，會使整個系統出現混亂，進而讓量子位元m的狀態改變來揪出監聽者 Eve。倘若通道內沒有其他監聽者，則 Alice 和 Bob 雙方都實作$R_Y(\theta)$到自己的量子位元上，則會互消抵銷彼此的運算，讓糾纏

態還是保持在$1/\sqrt{2}\,(|00\rangle + |11\rangle)_{AB}$。

舉例來說，倘若整個系統狀態若是$|\xi\rangle_{ABE}$，則雙方使用$R_Y(\theta)$會形成

$$R_Y(\theta)_A \otimes R_Y(\theta)_A \otimes I_E|\xi\rangle_{ABE}$$

$$= \begin{pmatrix} cos^2\frac{\theta}{2}\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) + sin^2\frac{\theta}{2}\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) \\ +sin\frac{\theta}{2}cos\frac{\theta}{2}\frac{1}{\sqrt{2}}(|100\rangle - |011\rangle) + sin\frac{\theta}{2}cos\frac{\theta}{2}\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle) \end{pmatrix}_{ABE}$$

，其中$(|100\rangle - |011\rangle)_{ABE}$和$(|010\rangle - |101\rangle)_{ABE}$會導致糾纏與解糾纏的量子位元$m$發生錯誤進而抓出 Eve，若想要最大化找到 Eve 的機率可以調整其震幅(讓$(|100\rangle - |011\rangle)_{ABE}$和$(|010\rangle - |101\rangle)_{ABE}$出現的機率增大，震幅越大意味著有越高的機率被測量到)，其最大震幅的角度為$sin(\theta/2)cos(\theta/2)$，其$\theta = \pi/2$。但有趣的是，此協定的偵測律超過了 25%，高過 BB84 的偵測率，所以 Gao 等人[28]就是以此來提出攻擊的方法，也論證了必須要降低偵測率才有辦法讓此協定保持安全。

肆、結論

往後量子電腦的發展還是必須面對三個重要的因素：計算、儲存及容錯，每個因素都和傳統的設計方式大相逕庭。由於量子密碼學這個領域十分寬廣且深奧，而筆者才疏學淺，尚無法完整道盡所有的量子密碼學領域，因此本文目的僅先讓讀者們了解量子電腦的威脅為何，以及密碼學家做何因應 (後量子密碼學與量子密碼學) 來抵禦未來的量子電腦；並且也幫助讀者建立基本的量子知識，藉由這些知識應該可以很清楚的了解本文內的所有協定及其概念，筆者最想與各位分享的是這些令人讚嘆的協定那純粹想法的美好；最後針對擁有量子資源才能產生的應用向各位介紹，並且多花一些篇幅在介紹量子金鑰配置協定領域，這些協定向世人展現了量子密碼學有別於傳統密碼學不同的一面。量子密碼學還有其他特殊的應用，也有一些在傳統認為無法做到的協定，而密碼學家嘗試想要透過量子資源來達成，若未來有機會再與各位讀者分享。

參考文獻

[1] B. Apolloni, C. Carvalho, and D. D. Falco, “Quantum stochastic optimization,” *Stochastic Processes and their Applications*, vol. 33, no. 2, pp. 233–244, 1989.

[2] K. Azuma, K. Tamaki, and H.-K. Lo, “All-photonic quantum repeaters,” *Nature Communications*, vol. 6, no. 1, pp. 1–7, 2015.

[3] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *Acta Physica Polonica A*, vol. 101, no. 3, pp. 357–368, 2002.

[4] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964.

[5] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[6] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Physical Review A*, Vol 53, p. 2046, 1996.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, pp. 175–179, 1984.

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, no. 5, p. 722, 1996.

[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[11] C. H. Bennett and S. J. Wiesner, "Communication via one and two particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[12] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, no. 18, 187902, 2002.

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[14] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, "Optimal universal and state-dependent quantum cloning," *Physical Review A*, vol. 57, no. 4, p. 2368, 1998.

[15] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, no. 3, p. 1844, 1996.

[16] A. Cabello, "Quantum key distribution without alternative measurements," *Physical Review A*, vol. 61, no. 5, 052312, 2000.

[17] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical*

Review A, vol. 54, no. 2, pp. 1098–1105, 1996.

[18] F. Chabaud and A. Joux, "Differential collisions in SHA-0" *In Advances in Cryptology-CRYPTO'98*, pp. 56–71, Springer, 1998.

[19] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theory," *Physical Review Letters*, vol. 23, no. 15, pp. 880–884, 1969.

[20] N. S Dattani and N. Bryans, "Quantum factorization of 56153 with only 4 qubits," *arXiv preprint arXiv:1411.6758*, 2014.

[21] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven, "What is the computational value of finite-range tunneling?," *Physical Review X*, vol. 6, no. 3, 031015, 2016.

[22] D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km," *Physical Review A*, vol. 93, no. 1, 010301, 2016.

[23] W. Diffie and M. E Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[24] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review A*, vol. 47, no. 10, pp. 777–780, 1935.

[25] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[26] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, Andrew Lundgren, and Daniel Preda, "A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem," *Science*, vol. 292, no. 5516, pp. 472–475, 2001.

[27] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 28, no. 14, pp. 938–941, 1972.

[28] F. Gao, S. J. Qin, Q. Y. Wen, and F. C. Zhu, "An effective attack on the quantum key distribution protocol based on quantum encryption," *International Conference on Information Security and Cryptology*, pp. 302–312, Springer, 2005.

[29] T. Gao, F.-L. Yan, and Z.-X. Wang, "Controlled quantum teleportation and secure direct communication," *Chinese Physics*, vol. 14, no. 5, pp. 893–897, 2005.

[30] N. Gisin and S. Massar, "Optimal quantum cloning machines," *Physical Review Letters*, vol. 79, no. 11, p. 2153, 1997.

[31] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: Quantum resource estimates," *In International Workshop on Post-Quantum Cryptography*, pp. 29–43, Springer, 2016.

[32] L. K. Grover, "A fast quantum mechanical algorithm for database search," *In Proceedings of the 28 Annual ACM Symposium on Theory of Computing*, pp. 212–219, 1996.

[33] G.-P. He and Z.-D. Wang, "Nonequivalence of two flavors of oblivious transfer at the quantum level," *Physical Review A*, vol. 73, no. 4, 044304, 2006.

[34] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, pp. 1829–1834, 1999.

[35] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," *In International Algorithmic Number Theory Symposium*, pp. 267–288, Springer, 1998.

[36] T. Hwang, Y.-P. Luo, C.-W. Yang, and T.-H. Lin, "Quantum authencryption – one-step authenticated quantum secure direct communications for off-line communicants," *Quantum Information Processing*, vol. 13, no. 4, pp. 925–933, 2014.

[37] IBM, The quantum experience, https://quantum-computing.ibm.com/ (2016/05).

[38] T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model," *Physical Review E*, vol. 58, no. 5, p. 5355, 1998.

[39] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 200, no. 4598, pp. 671–680, 1983.

[40] R. Lafiamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correction code," *Physical Review Letters*, vol. 77, no. 1, pp. 198–201, 1996.

[41] H.-K. Lo, "Insecurity of quantum secure computations," *Physical Review A*, vol. 56, no. 2, p. 1154, 1997.

[42] H.-K. Lo and H.-F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[43] H.-K. Lo and H.-F. Chau, "Is quantum bit commitment really possible?," *Physical Review Letters*, vol. 78, no. 17, p. 3410, 1997.

[44] H.-K. Lo and Y. Zhao, "Quantum cryptography," *arXiv preprint arXiv:0803.2507*, 2008.

[45] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[46] Z.-X. Man and Y.-J. Xia, "Controlled bidirectional quantum direct communication by using a GHZ state," *Chinese Physics Letter*, vol. 23, no. 7, pp. 1680–1682, 2006.

[47] D. Markham and B. C Sanders, "Graph states for quantum secret sharing," *Physical Review A*, vol. 78, no. 4, 042309, 2008.

[48] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Physical*

Review Letters, vol. 78, no. 17, p. 3414, 1997.

[49] R. Matsumoto, "Multiparty quantum-key-distribution protocol without use of entanglement," *Physical Review A*, vol. 76, no. 6, 062316, 2007.

[50] R. J. Mceliece, "A public-key cryptosystem based on algebraic," *Coding Theory*, vol. 4244, pp. 114–116, 1978.

[51] R. C. Merkle, "Protocols for public key cryptosystems," *IEEE symposium on security and privacy*, pp. 122–122. IEEE, 1980.

[52] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2002.

[53] NIST-FIPS Standard, "Announcing the advanced encryption standard," *Federal Information Processing Standards Publication 197*, pp. 1–51, Nov. 2001.

[54] B. A. Nguyen, "Quantum dialogue," *Physics Letters A*, vol. 328, no. 1, pp. 6–10, 2004.

[55] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, "Entanglement purification for quantum communication," *Nature*, vol. 410, no. 6832, pp. 1067–1070, 2001.

[56] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[57] N. Sangouard, C. Simon, H. D. Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[58] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, p. 1301, 2009.

[59] E. Schrödinger, "Discussion of probability relations between separated systems," *In Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, pp. 555–563, Cambridge University Press, Oct. 1935.

[60] E. Schrödinger, "Probability relations between separated systems," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 32, pp. 446–452, Oct. 1936.

[61] Y.-B. Sheng, L. Zhou, S.-M. Zhao, and B.-Y. Zheng, "Efficient single-photon-assisted entanglement concentration for partially entangled photon pairs," *Physical Review A*, vol. 85, no. 1, 012307, 2012.

[62] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *In 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[63] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, 2000.

[64] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical*

Review A, vol. 52, no. 4, pp. 2493–2496, 1995.

[65] C. Simon and J.-W. Pan, "Polarization entanglement purification using spatial entanglement," *Physical Review Letters*, vol. 89, no. 25, 257901, 2002.

[66] T.-T. Song, X. Tan, and T. Wang, "Entanglement concentration for arbitrary four-particle linear cluster states," *Scientific Reports*, vol. 7, no. 1, pp. 1–11, 2017.

[67] A. M. Steane, "Error-correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, pp. 793–797, 1996.

[68] Y. Tokunaga, T. Okamoto, and N. Imoto, "Threshold quantum cryptography," *Physical Review A*, vol. 71, no. 1, 012314, 2005.

[69] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, 040502, 2015.

[70] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[71] R. F. Werner, "Optimal cloning of pure states," *Physical Review A*, vol. 58, no. 3, p. 1827, 1998.

[72] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[73] U. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[74] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M.-J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, 190501, 2016.

[75] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometers," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[76] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Quantum key distribution via quantum

encryption," *Physical Review A*, vol. 64, no. 2, 024302, 2001.

[77] Z. Zhao, J.-W. Pan, and M. S. Zhan, "Practical scheme for entanglement concentration," *Physical Review A*, vol. 64, no. 1, 014301, 2001.

[78] L. Zhou and Y.-B. Sheng, "Purification of logic-qubit entanglement," *Scientific Reports*, vol. 6, no. 1, pp. 1–9, 2016.

[79] N. Zhou, G. Zeng, and J. Xiong, "Quantum key agreement protocol," *Electronics Letters*, vol. 40, no. 18, pp. 1149–1150, 2004.

[作者簡介] Biography

曾國鈞博士畢業於國立暨南國際大學資訊工程學系，專長在量子密碼學、量子計算、啟發式演算法、資訊安全及網路安全。曾任國立暨南國際大學博士後研究員，致力於維護與提升國教署各核心系統之資訊安全。現任國立臺灣大學 IBM 量子電腦中心博士後研究員，致力於量子密碼與量子計算之研究。