使用量子線路模擬量子網際網路核心機制

江振瑞
國立中央大學
資訊工程學系
jrjiang@g.ncu.edu.tw

摘要

本論文使用量子線路模擬量子網際網路最核心的機制，包括量子糾纏、量子遙傳、量子密鑰分發與量子中繼器的糾纏交換機制。透過量子線路的模擬結果，可以觀察量子網際網路核心機制處理量子位元狀態傳輸的過程，並進一步了解量子網際網路最終如何達成不可破解的資料傳輸無條件安全性，以及如何透過連接位於全球各地的量子電腦，進行大規模的分散式量子計算以實現量子霸權。

關鍵詞：量子網際網路, 量子糾纏, 量子遙傳, 量子密鑰分發, 量子中繼器, 量子霸權, 糾纏互換, 無條件安全性

I. 緒論

網際網路(Internet or internet)以 TCP/IP 或其他通信協定為基礎，串聯了全球的人、機與服務，已經是我們生活中不可或缺的一部份。人們不論是上班、上學、購物、旅遊，休閒或是進行娛樂與社交，都離不開使用網際網路。從網際網路的前身 ARPANET 在1969年10月開始運作算起[1]，五十多年來，網際網路持續運作，發展精進與拓廣更大的連線規模。但這也伴隨產生許多網路資訊安全問題，例如，駭客可以輕易透過網際網路發動網路攻擊勒索金錢，竊取機密或隱私資料，盜取銀行帳戶金錢，或冒用信用卡資訊取得不當財物或利益等。

量子電腦(quantum computer)的出現，形成網際網路安全更大的隱憂。量子電腦與現行的電腦運算模式不同。現行的電腦稱為古典電腦(classical computer)，如 IBM Summit 超級電腦，以位元(bit)或古典位元(classical bit)為基礎進行計算；而量子電腦，如 Google Sycamore 以及 IBM Q，則以量子位元(quantum bit, or qubit)為基礎進行計算[2]。因為量子位元可以處於特殊的同時是0狀態又是1狀態的疊加(superposition)狀態接受操作，所以 n 個量子位元可以同時表示2^n個 n 位元的所有狀態接受操作，這與 n 個古典位元一次只能表示1個 n 位元的狀態接受操作不同。因此，量子電腦在執行計算或操作時，具有隨著量子位元數的增加，產出比古典電腦計算速度更快的指數量級加速(exponential speedup)計算能力。

文獻中提出許多可以在量子電腦上執行的量子演算法(quantum algorithm)，可以有效地解決過去難以解決的問題。例如，秀爾(Shor)教授在1994年提出秀爾演算法(Shor's algorithm)[3]，其中部份步驟可以在量子電腦上執行，以多項式時間複雜度(polynomial time-complexity)解決大數因數分解問題，這相較於在古典電腦上執行目前最快的一般數域篩選(general number field sieve, GNFS)演算法具有指數量級的加速，因而得以破解以大數因數分解為基礎的RSA公開密鑰密碼系統。目前的網際網路中有許多使用 RSA 或相關密碼系統維持網路安全的機制，因此網際網路的安全性受到極大的威脅。

因應量子電腦對網際網路的安全威脅，研究學者提出後量子密碼學(post-quantum cryptography, PQC)[4]以及量子密碼學(quantum cryptography)[5]作為因應。後量子密碼學致力於發展在古典電腦上執行，但是與現行密碼系統使用不同原理，而且仍然未被量子演算法破解的密碼系統，例如美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)推薦的基於格(lattice-based)密碼以及基於雜湊(hash-based)密碼系統[6]；而量子密碼學則著墨於使用量子通訊通道傳送量子位元狀態，依賴測不準原理(uncertainty principle)以及不可複製定理(no-cloning theorem)的特性，偵測量子通道是否被竊聽來採取適當處理，進而增進網路資訊安全性。例如BB84通信協定[7]透過在量子通道上傳送隨機但特定的量子狀態，以及選擇隨機的量子狀態測量方式，搭配使用傳統通訊通道來進行量子密鑰分發(quantum key distribution, QKD)[8]，可以達成單次密碼本(one-time pad, OTP)[9]概念中不可破解的資訊理論安全(information-theoretic security)或無條件安全(unconditional security)[10]。

現今的網際網路大量的使用光纖來建立通信通道來傳送位元資料。因為光子可以用來表示量子位元，因此我們恰好可以藉由光纖連線來建立量子通道(quantum channel)以傳送量子位元疊加態，並進一步建構量子網際網路(quantum Internet or quantum internet)。量子通道除了可以使用光纖連線來建立之外，也可以透過與自由空間衛星連線的雷射光鏈路來建立。為了與量子網際網路中的量子通道有所區別，我們將現行網際網路中所建立的通道稱為古典通道(classical channel)。以光通訊為例，古典通道使用光脈衝傳送位元資料，每個脈衝中包含數以億計的光子，用來表示位元1，若某段時間沒有光子脈衝出現，則代表傳送的資訊為位元0。量子通道則使用一個一個的光子來傳送量子位元疊加態，以光子

的垂直偏振(vertical polarization)代表量子位元1，而以光子的水平偏振(horizontal polarization)代表量子位元0。除了水平偏振與垂直偏振之外，當然也可以利用光子其他正交的兩種狀態來代表0與1，例如，45度偏振與-45度偏振。請注意，量子通道傳輸的是任意的量子疊加態，這可以透過以量子糾纏(quantum entanglement)特性為基礎，搭配古典通道的量子遙傳(quantum teleportation)機制來達成。

如前所述，量子網際網路中的量子通道與古典通道不同。古典通道以包含數以億計光子的光脈衝傳送位元資料，因此傳輸距離長而且錯誤率低。但是量子通道使用一個光子的偏振狀態來傳送量子位元疊加態，因此很容易衰減，而造成傳輸距離短且錯誤率高，或是說造成量子位元疊加態的保真度(fidelity)低。為克服量子通道的問題，可以設置一連串的量子中繼器(quantum repeater)[11]來延長量子通道的距離。量子中繼器最早由 Briegel 等人提出[12]，基於測不準原理以及不可複制定理，量子中繼器不能像傳統古典通道中的中繼器一樣，採用複製並重送的方式運作，而是必須採用量子糾纏生成(entanglement generation)、糾纏純化(entanglement purification)、量子記憶體(quantum memory)以及糾纏交換(entanglement swap)等機制來實現量子中繼器。

本論文將介紹量子網際網路的整體架構以及基本知識，並針對量子網際網路中一些關鍵的機制，如量子糾纏、量子遙傳、量子密鑰分發以及量子中繼器糾纏交換等機制加以詳細說明，設計對應的量子線路(quantum circuit)並且在 IBM 量子電腦模擬器及真實的 IBM Q 量子電腦上執行這些量子線路。希望透過量子線路的設計展示與其執行結果的呈現，能夠讓讀者充分了解量子網際網路最核心機制的實際運作情形，以便能夠從事進一步的改良或延伸研究。

本論文的其他節次安排如下，第二節將說明量子網際網路的基本概念及知識。第三節則進一步說明一些量子網際網路的核心機制，並使用量子線路模擬其運作的情形。最後第四節則下結論總結整篇論文。

II. 量子網際網路架構及背景知識

量子網際網路的建構是歐盟量子技術旗艦(quantum technologies flagship)計畫的主要目標之一，希望能夠藉以達到極度安全的傳遞資料，包括古典位元資料以及量子位元狀態。這個計畫在2016年5月發布，在2018年10月啟動，是一個總投資約10億歐元的10年計畫[13]。2020年7月，美國能源部(department of energy, DOE)發布了量子網際網路藍圖[14]，預計在10年內建構一個全國性的量子網際網路，關鍵的研究包括在現有光纖通道上驗證量子通訊協定的安全性，在網路節點間傳送糾纏的量子資訊，構建並整合量子網路設備(如量子中繼器及交換器)，開發繞徑技術以及量子位元在網際網路中傳輸時的糾錯技術等。2017年中國建立京滬幹線，一個通過32個中繼節點，全長約2000公里的量子加密通信幹線。並透過兩個衛星地面站透過雷射鏈路與墨子號(Micius)量子衛星[15]相連，使幹線總距離達到4600公里。另外，更以墨子號量子衛星做為中繼，達成中國與與奧地利間7600公里的量子通道。

根據一篇著名的科學(Science)期刊論文[16]的說明：量子網際網路的願景是與現今的網際網路並存，實現地球上任意兩點之間的量子通信，藉以連接量子處理器，因而達成使用古典方式絕對無法達到的通信與計算能力。綜合以上說明，除了可以傳送量子疊加狀態，藉以加強資料傳輸安全之外，量子網際網路實際上還可以連接許多量子電腦，協助實現分散式量子計算(distributed quantum computing, DQC)。因為現今量子電腦的發展正處有雜訊中等尺度量子(noisy intermediate-scale quantum, NISQ)世代[17]，量子電腦中的量子位元數量還不多，而且還是具有雜訊的(noisy)，需要使用容錯技術透過許多冗餘量子位元來提高一個量子位元的保真度。量子網際網路可以將許多量子電腦連接在一起實現量子位元的糾纏，以進行極大規模的量子計算，確實達成 Google 所宣稱已實現的量子霸權(quantum supremacy)[18]，也就是透過量子電腦完成古典電腦絕對不可能完成或不可能在有限的時間內完成的計算。

量子網際網路使用量子通道與古典通道構成可以涵蓋全球的網路，用以連接量子電腦以及古典電腦，其中量子通道用來傳送量子位元，而古典通道用來傳送古典位元，能夠達成不可破解的完美安全資訊傳輸以及古典電腦無法達到的量子霸權計算能力。圖1顯示量子網際網路的實體架構[19]，其中包含許多網路節點、自由空間衛星以及與衛星連線的地面站。一般使用光纖或衛星與地面站間的雷射鏈路建立量子通道，用以傳送量子位元。因為光子在光通道中的強度隨著傳輸距離呈現指數型衰減，雖然地面站與衛星間可以達到1200公里的傳輸距離，但是地面上的光纖通道大約數十公里就要透過量子中繼器來延長通道的傳輸距離。

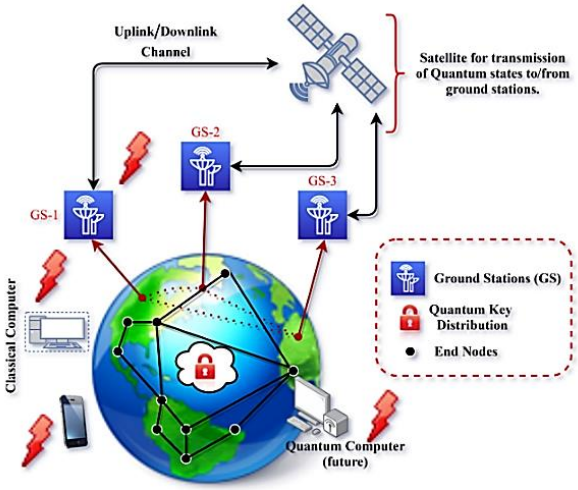

圖1. 量子網際網路實體架構圖[19]

量子通道可以透過量子遙傳機制來傳送任意量子位元疊加態。量子遙傳的第一步是產生具有糾纏態的量子位元對(量子粒子對)，然後將位元對中的位元分送到狀態發送節點與接收節點。有許多方式可以產生糾纏量子粒子對，例如，可以利用量子光學中的自發參量下轉換(spontaneous parametric down-conversion, SPDC)技術，利用雷射光射入特殊非線性雙折射晶體(nonlinear birefringent crystal)產生一對處於糾纏態的光子，如圖2所示。將這個光子對中的一個光子傳送到量子位元狀態發送節點 Alice，而另一個傳送倒量子位元狀態接收節點 Bob，就可以進行量子遙傳動作了。我們將於下節中詳細描述量子遙傳機制。

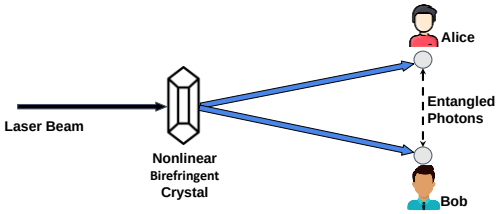

圖2. 量子糾纏對生成示意圖

因為量子遙傳機制可以在量子通道中傳遞量子位元狀態，因此可以再搭配古典通道進行量子密鑰分發(QKD)[8]。根據一次密碼本(OTP)[9]的概念，只要密鑰的長度大於或等於密文的長度，就可以達成不可破解的資訊理論安全或無條件安全的完美安全性質[10]。在下一節，我們將以 BB84通信協定為例，說明如何進行量子密鑰分發達成無條件安全的完美安全性質。

如前所述，量子網際網路必須採用量子中繼器來連接量子通道，以延長量子疊加態的傳送距離。量子中繼器不可以像古典中繼器一樣使用複製-再傳送的方法來進行量子通道的延長，而必須使用糾纏交換的機制來進行。如圖3所示，透過一連串的量子中繼器進行糾纏交換，可以讓距離很遠的量子位元狀態發送節點 Alice 與接收節點 Bob 的量子位元產生糾纏，因而可以進行距離非常遠的量子遙傳動作。

以圖3的場景為例，距離為 D 的 Alice 與 Bob 之間有3個量子中繼器，以4段距離為 D/4的量子通道相連。3個量子中繼器先各自準備兩對處於糾纏態的量子位元: 中繼器1的其中一個量子位元與 Alice 的量子位元糾纏，而另一個量子位元與中繼器2的量子位元糾纏；中繼器2的其中一個量子位元與中繼器1的量子位元糾纏，而另一個量子位元與中繼器3的量子位元糾纏；中繼器3的其中一個量子位元與中繼器2的量子位元糾纏，而另一個量子位元與 Bob 的量子位元糾纏。此時，在中繼器1執行糾纏交換，使得 Alice 的量子位元與中繼器2的左方量子位元產生糾纏；在中繼器3執行糾纏交換，使得 Bob 的量子位元與中繼器2的右方量子位元產生糾纏；最後，在中繼器2進行左方及右方量子位元的糾纏交換，儘管 Alice 與 Bob 原來並沒有直接連線，而其量子位元也沒有任何關聯，但是 Alice 與 Bob 的量子位元還是可以形成量子糾纏。

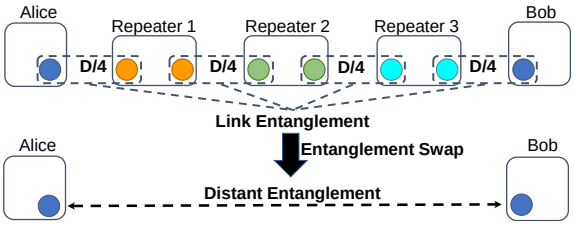

圖3. 量子中繼器使用糾纏交換示意圖

III. 量子網際網路核心機制量子線路

A. 量子糾纏

量子糾纏(quantum entanglement)是量子力學中非常重要的概念，這個名詞由薛定諤提出，並被愛因斯坦稱為“幽靈般的遠距離作用(spooky action at a distance)”。它是相互作用量子實體(或量子粒子)間的物理現象，處於糾纏態的量子實體的屬性已被整合為一個整體屬性。因此，當一個實體的狀態發生變化時，無論糾纏的量子實體距離多遠，其他量子實體的狀態都會立即發生變化。例如，對於兩個具有相反偏振的糾纏光子，如果觀察或測量其中一個光子是坍縮為垂直偏振，那麼另一個光子必定立即坍縮(collapse)為水平偏振。

貝爾態(Bell state)或是 EPR 配對(Einstein-Podolsky-Rosen pair)是兩個量子位元間的量子糾纏狀態。圖4是對應貝爾糾纏態量子位元配對的量子線路，透過一個哈達馬(Hadamard, H)閘以及一個受控非(Controlled-Not, CNOT or Controlled-X, CX)閘構成。圖5是透過 IBM Quantum 服務，以 IBM 量子電腦模擬器執行貝爾糾纏態量子位元配對量子線路結果的直方圖(histogram)。可以看出其中兩個量子位元狀態不是00就是11，而且其出現機率都接近50%，表示兩個位元確實處於糾纏態。實際上這個量子線路對應以狄拉克記號(Dirac notation)記為 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$的量子糾纏狀態。以下以 H 閘以及 CNOT 閘對應的么正矩陣(unitary matrix)，針對量子位元初始狀態$\begin{pmatrix}1\\0\end{pmatrix}$進行計算來驗證這個結果:

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$$

$$\mathrm{CNOT}(\mathrm{H}|0\rangle \otimes |0\rangle) = \mathrm{CNOT}\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ 0\\ 0\\ \frac{1}{\sqrt{2}}\end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle = |\Phi^+\rangle$$

圖6則是透過 IBM Quantum 服務，以真實 IBM 量子電腦(ibm_oslo)執行貝爾糾纏態量子位元配對量子線路結果的直方圖。與圖5類似，量子線路中兩個量子位元不是00就是11的機率都接近50%。但是因為真實量子電腦具有雜訊，其保真度不是100%，因此直方圖中還出現兩個量子位元為01及10的微小機率。

請注意，因為論文篇幅的緣故，我們在以下的內容中均省略么正矩陣計算的驗證以及在 IBM 實際量子電腦的執行結果，而僅呈現量子線路及其在量子電腦模擬器上的執行結果。

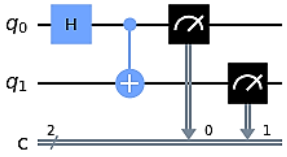

圖4. 量子糾纏貝爾態量子線路

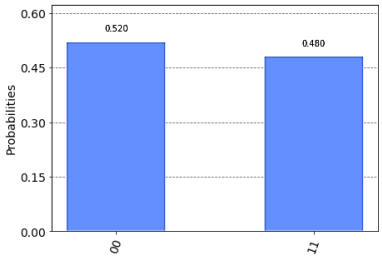

圖5. 量子糾纏貝爾態量子線路量子電腦模擬器執行結果

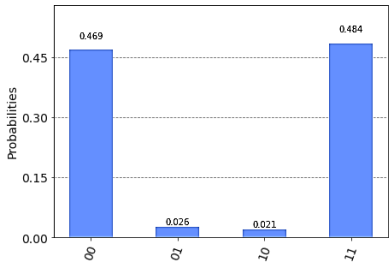

圖6. 量子糾纏貝爾態量子線路真實量子電腦執行結果

B. 量子遙傳

處於貝爾態的糾纏量子位元可以作為量子遙傳(quantum teleportation)的基礎，讓相隔很遠的網路節點 Alice 與 Bob，可以透過古典通訊的方式，在不損壞量子位元量子態的條件下傳遞一個量子位元的量子態。

以下以量子位元狀態 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 說明量子遙傳的實施方式。假設相隔很遠的通訊發送節點 Alice 與通訊接收節點 Bob 各擁有處於貝爾糾纏態 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 之二個量子位元中的一個。令 Alice 擁有的量子位元記為q_a； Bob 擁有的量子位元記為q_b。現在假設 Alice 想要傳送量子位元q_s的狀態給 Bob，則 Alice 可以透過圖7中的量子遙傳量子線路來完成，說明如下:

Alice 首先以 q_s為控制位元，以q_a為目標位元加入受控非(Controlled-Not, CNOT)閘， 然後針對q_s加入哈達馬(Hadamard, H)閘，最後再針對q_s及q_a進行測量，並將測量結果透過古典通訊通道傳送給 Bob。當 Bob 收到測量結果時，可以分為以下 4 個處理狀況來完成量子遙傳：

(狀況1) q_s及q_a的測量結果均為$|0\rangle$，則q_b本身就是q_s的狀態。

(狀況2) q_s的測量結果為$|0\rangle$，而q_a的測量結果為$|1\rangle$，則針對q_b進行 X 閘操作就可以還原q_s的狀態。

(狀況3) q_s的測量結果為$|1\rangle$，而q_a的測量結果為$|0\rangle$，則針對q_b進行 Z 閘操作就可以還原q_s的狀態。

(狀況4) q_s及q_a的測量結果均為$|1\rangle$，則針對q_b先進行 X 閘再進行 Z 閘操作就可以還原q_s的狀態。

請注意，圖7中的量子線路中第一條壁壘(barrier)線之前代表初始狀態，第一條與第二條壁壘線之間代表 Alice 啟動量子遙傳程序的操作，而第二條壁壘線之後則代表 Bob 完成最後量子遙傳的操作。圖7的量子線路在第二條壁壘線之後僅展示出狀況4對應的量子閘操作，其他的狀況可以簡單的由此量子線路延伸推導得出，在此省略。

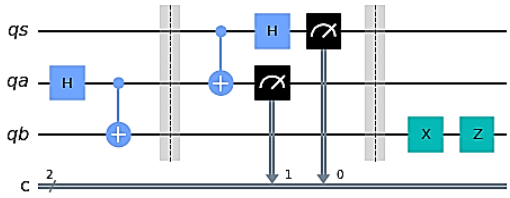

圖7. 對應量子遙傳的量子線路

C. BB84通信協定

BB84通信協定[7]由 Bennett 與 Brassard 在1984年提出，是一種量子密鑰分發(QKD)協定[8]，被認為是第一個量子密碼協定。BB84通信協定可以用來傳送單次密碼本(OTP)[9]的一次性密鑰，只要密鑰的長度大於或等於密文的長度，就可以達到完全不可破解的資訊理論安全或無條件安全或可證明安全(provable security)。密文(ciphertext)完全不洩漏明文(plaintext)的任何訊息，因此即使在攻擊者具有不受任何條件限制能力的情況下，也依然能夠保持密文不可能被破解的完美安全(perfect secrecy)性質[10]。

BB84協定使用量子通道傳送量子態，並同時使用古典通道傳送量子態的測量結果與控制訊息。其作法為使用兩組不同的量子狀態基底，例如，若量子通道以光纖或是量子衛星雷射鏈路實現，則可以使用一組包含垂直偏振與水平偏振的直線(rectilinear)基底，以及一組包含45度偏振與-45度偏振的對角(diagonal)基底。然後讓發送節點與接收節點在每一次傳送量子態與測量量子態時各自隨機選擇一個基底，例如，發送節點可以選擇直線基底透過垂直偏振傳送位元0及透過水平偏振傳送位元1；而接收節點可以選擇對角基底，若測得45度偏振則

代表位元0，反之，若測得-45度偏振則代表位元1。

在 BB84通訊協定中，由於發送節點與接收節點都任意選擇基底，因此大約有50%的機率兩端節點會選到同樣的基底，兩端節點可以正確交換訊息，也就是接收節點與發送節點的量子位元訊息是相同的，這些訊息可於稍後作為單次密鑰之用。另外，即使發送節點與接收節點選擇不同的基底，又大約有50%的機率接收節點與發送節點的訊息是相同。因此，綜合而言，接收節點與發送節點有75%的機率訊息是相同的，我們將於稍後以量子線路的執行結果驗證這一點。

在執行 BB84通信協定時，在量子通道中若出現竊聽者竊聽量子位元，由於量子位元狀態的竊聽必須進行測量，根據測不準原理及不可複製定理，測量之後量子位元的狀態就坍縮為測量的基底狀態了，因此接收者即使採用與發送節點同樣的基底，在竊聽者有50%機率選錯基底的情況下，會再各有50%的機率接收到正確與不正確的量子位元。根據這個現象，發送節點與接收節點可以交換一些量子位元訊息用來偵測是否有竊聽者存在，這將於稍後描述。

圖8為 BB84通信協定對應的量子線路，顯示發送節點 Alice 與接收節點 Bob 採用不同的基底傳輸量子位元0的四種狀況，圖9則顯示量子線路在 IBM 量子電腦模擬器上的執行結果。量子線路中採用以布洛赫球面上+Z 代表0，-Z 代表1的 Z 基底，以及以+X 代表0，-X 代表1的 X 基底。我們可以在量子上透過 H 閘進行基底轉換。實際上，在量子線路中第一條壁壘線之前的狀態代表 Alice 對量子位元0的表示方式，前兩個量子位元 q_0及 q_1 選擇 Z 基底，後兩個量子位元 q_2及 q_3選擇 X 基底。由於 IBM 量子電腦無法改變測量基底，而其預設的測量基底為 Z 基底，因此，我們在量子位元測量前加上 H 閘再進入量子位元 Z 基底測量，就等同是進行 X 基底測量。量子線路中第一條與第二條壁壘線之間顯示 Bob 對測量基底的選擇，量子位元 q_0及 q_2選擇 Z 基底測量，量子位元 q_1及 q_3選擇 X 基底測量。由圖9的結果得知，量子位元 q_0及 q_3都100%正確測量接收為0，而量子位元 q_1及 q_2則有50%的機率正確測量接收為0，因此正確測量接收為0的機率總計為75%。

當 Alice 與 Bob 採用相同的基底表示與測量量子位元時，量子位元可以100%被正確接收。理論上 Alice 與 Bob 只要透過古典的通道確認那些量子位元的表示與測量基底相同，就可以確認哪些量子位元是正確接收的，並利用這些量子位元來傳送一次性密鑰。但是因為通道中可能潛藏著竊聽者 Eve，因此還必須透過這些正確接收量子位元的一部份來偵測通道中是否有任何竊聽者 Eve。完整的 BB84通信協定可以簡化為以下的4個步驟，描述如下:

步驟1. Alice 隨機選擇一組量子位元，針對每個量子位元選擇一個隨機的基底，透過量子通道將量子位元傳送給 Bob。

步驟2. Bob 針對每個量子位元選擇一個隨機的基底測量並接收其狀態，並在接收後透過古典通道公開自己的基底選擇。

步驟3. Alice 對照自己與 Bob 的基底選擇，並透過古典通道公開哪些量子位元的基底選擇是相同的。

步驟4. Bob 隨機選擇一部份(例如1/10)基底選擇相同的量子位元，透過古典通道公開傳送給 Alice 比對。若不存在 Eve，則 Alice 可以成功比對量子位元完全相同，如此，Alice 可以通知 Bob 使用基底選擇相同而且未公開的量子位元作為密鑰之用。但是若存在 Eve，則 Alice 可以比對出許多不同的量子位元，此時可以確定通道遭到竊聽，則 Alice 通知 Bob 通信協定要重新從頭開始執行。

因為 BB84通信協定完全沒有傳輸任何密鑰的內容，因此密鑰的傳輸是完全安全的，再搭配單次密碼本的概念，就可以達到不可破解的完美安全。另外，因為在步驟4中， Bob 公開的每個量子位元有1/4的機率可以偵測出竊聽者的存在，因此若 Bob 公開 N 個量子位元，則可以偵測出竊聽者的機率為1-(3/4)^N，然當 N 越大，則偵測出竊聽者的機率也越大。

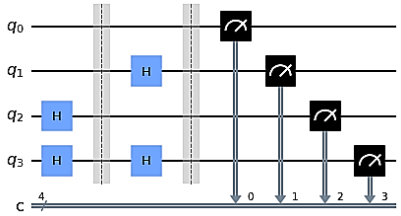

圖8. BB84量子密鑰分發對應的量子線路

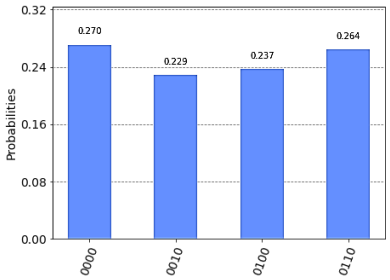

圖9. BB84量子密鑰分發對應的量子線路執行結果

D. 量子中繼器

量子中繼器[11]可以用來延長量子通道的距離。如前所述，一個量子中繼器依賴量子糾纏生成、糾纏純化、量子記憶體以及糾纏交換等機制連實現。以下我們僅針對其中最核心的糾纏交換機制進一步的說明，必且展示其對應的量子線路以及量子線路的執行結果。

假設量子網際網路的兩個節點 Alice 與 Bob 距離太遠，無法在二者之間建立直接相連的量子通道使二者的量子位元形成量子糾纏。但是在 Alice 與 Bob 中間存在節點 Sue，分別可與 Alice 與 Bob 建立直接連接的量子通道。此時可以透過 Sue 進行糾纏交換，建立 Alice 與 Bob 之間的量子糾纏，其做法描述如下:

節點 Sue 先產生兩對處於糾纏態的量子位元，其中一

個量子位元與 Alice 的量子位元糾纏，而另一個量子位元與 Bob 的量子位元糾纏。此時 Sue 再針對本身擁有的兩個量子位元進行量子狀態交換，則會形成兩對量子位元糾纏，分別為 Sue 本身的兩個量子位元產生糾纏，並且 Alice 與 Bob 的量子位元產生糾纏，形成糾纏交換。儘管 Alice 與 Bob 原來並沒有直接的量子通道連線，而且其量子位元也沒有任何關聯，但是 Alice 與 Bob 的量子位元還是可以形成量子糾纏。

圖10及圖11顯示量子糾纏相關的量子線路及量子線路在IBM量子電腦模擬器上的執行結果。可以看出在量子線路中的第一條壁壘線之前，Alice及Bob的量子位元分別與 Sue 的第一個與第二個量子位元產生糾纏。在第二條壁壘線之後，Sue 透過兩個 CNOT 閘、一個 H 閘以及一個受控 Z(controlled Z, CZ)閘完成糾纏交換。量子線路中 Alice 與 Bob 的量子位元之間沒有任何直接的操作，但是卻已經產生糾纏。這可以由圖11中的執行結果中看出，也就是說 Alice 與 Bob 的量子位元不是測量為00，就是測量為11，而且兩種測量結果的出線機率都大約為50%。

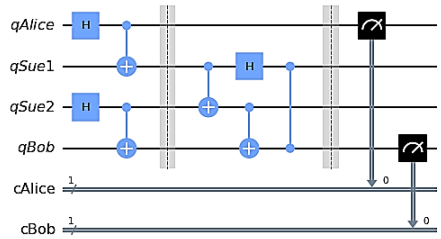

圖10. 糾纏交換量子線路

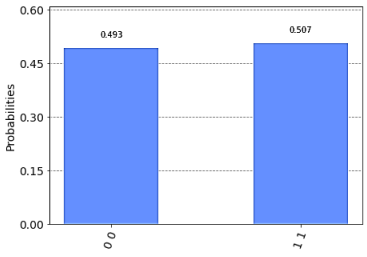

圖11. 糾纏交換量子線路量子電腦模擬器執行結果

IV. 結論

本論文詳細介紹從網際網路到量子網際網路的演進，也說明世界各地量子網際網路的發展現況與展望。本論文並使用量子線路模擬量子網際網路最核心的機制，包括量子糾纏、量子遙傳、量子密鑰分發與量子中繼器的糾纏交換等機制。透過量子線路的模擬結果，可以觀察量子網際網路核心機制處理量子位元狀態傳輸的過程，並進一步了解量子網際網路最終如何達成不可破解的無條件安全資料傳輸。

量子網際網路正在發展之中，面臨許多困難與挑戰，有許多相關的議題需要深入的研究與探討。主要的研究方向包括建構更有效率的量子密鑰分發機制，創立新穎的糾纏生成、糾纏純化、糾纏分配、量子記憶體與糾纏互換機制，選擇不同的中介量子中繼器，形成高效且高品質端對端量子通道連線的量子網際網路繞徑機制，以及連接位於全球各地的量子電腦，進行大規模分散式量子計算的機制等。

參考文獻

[1] B. Stewart, “Internet History – One Page Summary,” The Living Internet, 2000.

[2] 江振瑞, 輕鬆學量子程式設計--從量子位元到量子演算法, 碁峰資訊出版, ISBN: 786263242715, 2022.

[3] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” In Proc. of 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994.

[4] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, “Recent advances in post-quantum cryptography for networks: a survey,” In Proc. of 2022 7th International Conference On Mobile And Secure Services (MobiSecServ), pp. 1-8, 2022.

[5] A. Kumar, and S. Garhwal, “State-of-the-art survey of quantum cryptography,” Archives of Computational Methods in Engineering, 28(5), pp. 3831-3868, 2021.

[6] T. Hasija, K. R. Ramkumar, A Kaur, S. Mittal, and B. Singh, “A survey on NIST selected third round candidates for post quantum cryptography,” In Proc. of 2022 7th International Conference on Communication and Electronics Systems (ICCES), pp. 737-743, 2022.

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

[8] K. K. Choure, A. Saharia, N. Mudgal, M. Tiwari, and G. Singh, “Recent advancement in high speed and secure quantum key distribution: a review,” Optical and Wireless Technologies, pp. 259-267, 2022.

[9] F. Miller, Telegraphic code to insure privacy and secrecy in the transmission of telegrams, CM Cornwell, 1882.

[10] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, 28(4), pp. 656-715, 1949.

[11] P. S. Yan, L. Zhou, W. Zhong, and Y. B. Sheng, “A survey on advances of quantum repeater,” Europhysics Letters, 136(1), 14001, 2021.

[12] 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, 81(26), 5932, 1998.

[13] Quantum Flagship, url: https://golden.com/wiki/Quantum_Flagship-DB8PKDY, last accessed in October 2022.

[14] U.S. Department of Energy, “Launch to the future: quantum internet,” url: https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet, last accessed in October 2022.

[15] S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, and J. W. Pan, “Satellite-to-ground quantum key distribution,” Nature, 549(7670), pp. 43-47, 2017.

[16] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: a vision for the road ahead,” Science, 362(6412), eaam9288, 2018.

[17] J. Preskill, “Quantum computing in the NISQ era and beyond,” Quantum, 2, 79, 2018.

[18] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, ... , and J. M. Martinis, “Quantum supremacy using a programmable superconducting processor,” Nature, 574(7779), pp. 505-510, 2019.

[19] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, “Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions,” IEEE Communications Surveys & Tutorials, 23(4), pp. 2218-2247, 2021.