使用量子線路模擬量子網際網路核心機制

Computer Science and Information Engineering Department
National Central University, Taiwan

Jehn-Ruey Jiang (江振瑞)

Outline

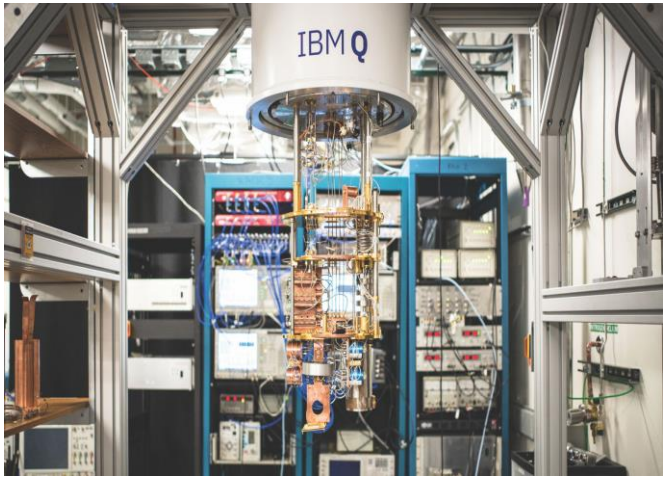
- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

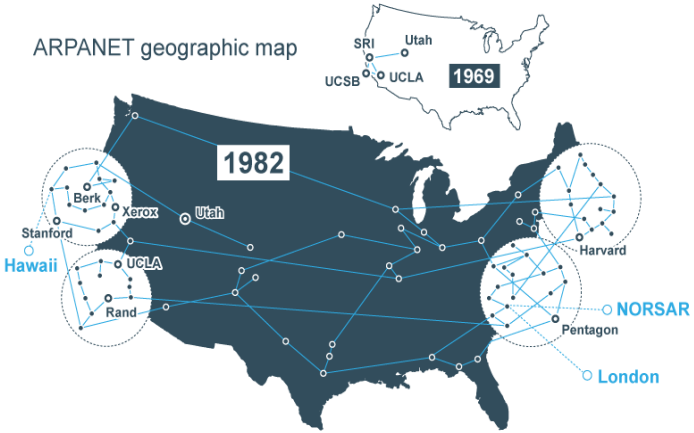
緒論 (1)

- 網際網路(Internet or internet)以 TCP/IP 或其他通訊協定為基礎，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。
- 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。



IBM Q system

Source:https://www.bnl.gov/newsroom/news.php?a=114371

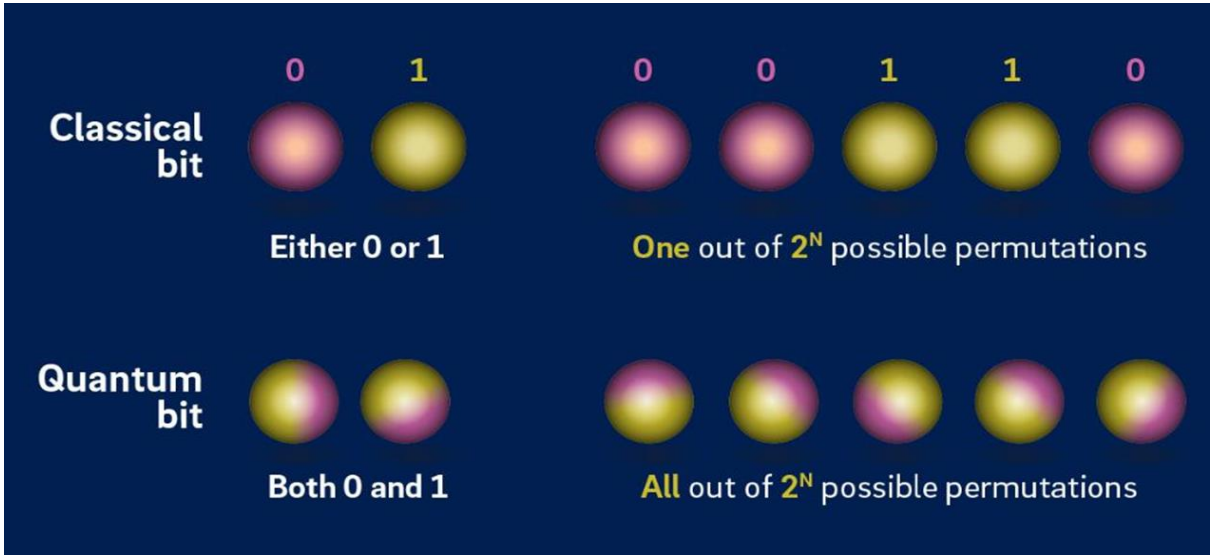


ARPANET 是美國國防部高等研究計畫署 (Advanced Research Projects Agency) 開發的世界上第一個運營的封包交換網路，是全球網際網路的鼻祖。

(source:https://portswigger.net/cms/images/e0/91/1afc66d7078e-article-arpanet-infographic-map.png)

緒論 (2)

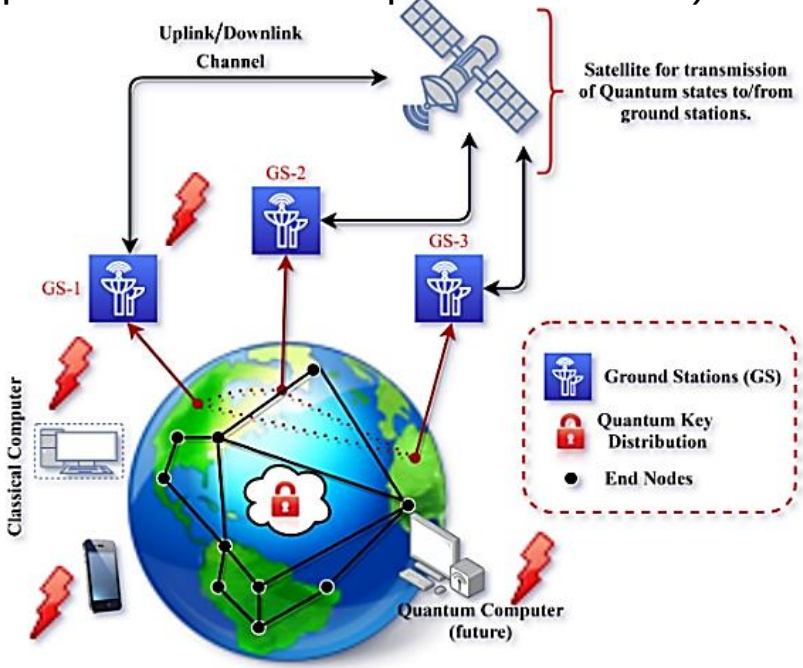
- 因為量子位元可以處於特殊的同時是0狀態又是1狀態的疊加(superposition)狀態接受操作，所以 n 個量子位元可以同時表示 2^n 個 n 位元的所有狀態接受操作，這與 n 個古典位元一次只能表示 1 個 n 位元的狀態接受操作不同。因此，量子電腦在執行計算或操作時，具有隨著量子位元數的增加，產出比古典電腦計算速度更快的指數量級加速(exponential speedup)計算能力，可以解決目前古典電腦無法短期內解決的問題，例如快速破解RSA密碼系統。



Source: https://www.rolandberger.com/en/Insights/Publications/Quantum-technology-is-leaping-into-our-lives.html

緒論 (3)

- 目前網際網路的資訊安全，受到量子電腦計算能力的威脅。而現今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)，解除這個威脅。



量子網際網路實體架構圖

Source: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.

Outline

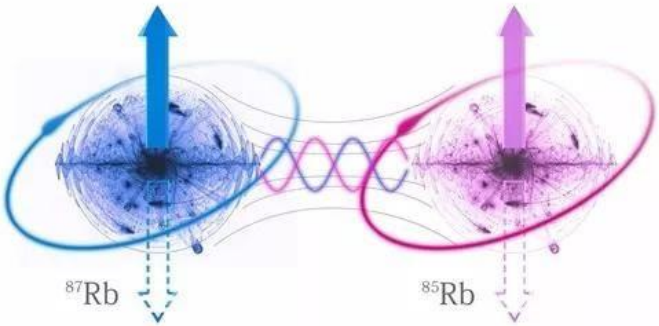
- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

量子糾纏 (1)

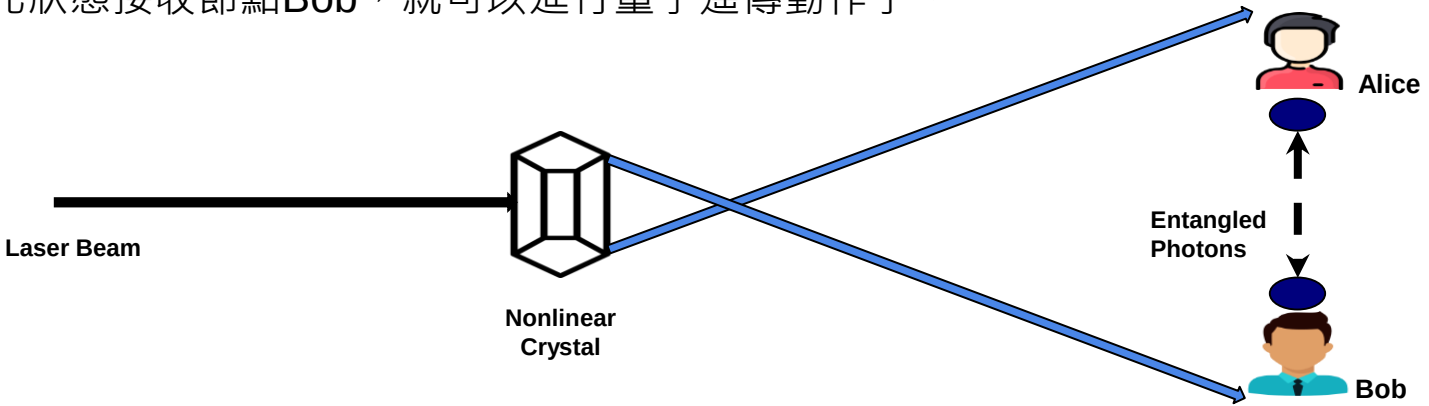
- 量子糾纏(quantum entanglement)是量子力學中非常重要的概念，這個名詞由薛定諤提出，並被愛因斯坦稱為“幽靈般的遠距離作用(spooky action at a distance)”。
- 它是相互作用量子實體(或量子粒子)間的物理現象，處於糾纏態的量子實體的屬性已被整合為一個整體屬性。 因此，當一個實體的狀態發生變化時，無論糾纏的量子實體距離多遠，其他量子實體的狀態都會立即發生變化。 例如，對於兩個具有相反偏振的糾纏光子，如果觀察或測量其中一個光子是坍縮為垂直偏振，那麼另一個光子必定立即坍縮(collapse)為水平偏振。



source:https://www.xuehua.us/a/5eb7e06c86ec4d0bd8de5c0b?lang=zh-hk

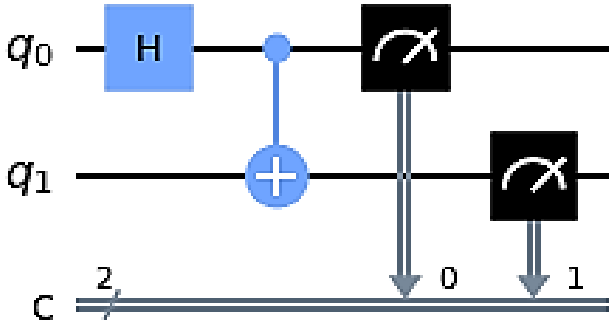
量子糾纏 (2)

- 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(non-linear birefringent crystal)產生一對處於糾纏態的光子，如下圖所示。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。



量子糾纏 (3)

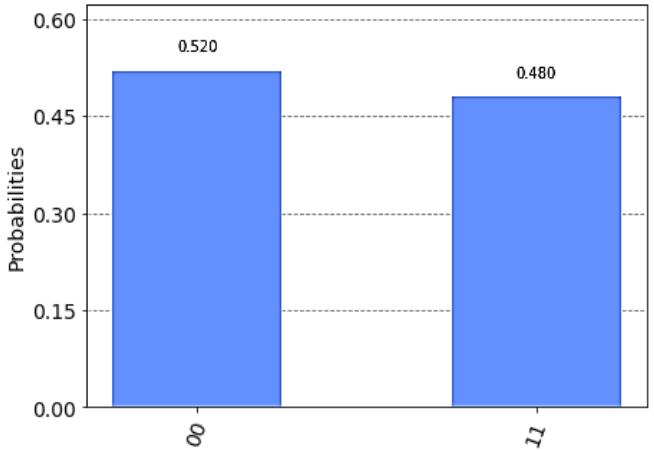
- 貝爾態(Bell state)或是EPR配對(Einstein-Podolsky-Rosen pair)是兩個量子位元間的量子糾纏狀態。下圖是對應貝爾糾纏態量子位元配對的量子線路，透過一個哈達馬(Hadamard, H)閘以及一個受控非(Controlled-Not, CNOT or Controlled-X, CX)閘構成。



量子糾纏貝爾態量子線路

量子糾纏 (4)

- 下圖是透過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$|\Phi^+\rangle=1/\sqrt{2}(|00\rangle+|11\rangle)$的量子糾纏狀態。



量子糾纏貝爾態量子線路量子電腦模擬器執行結果

Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

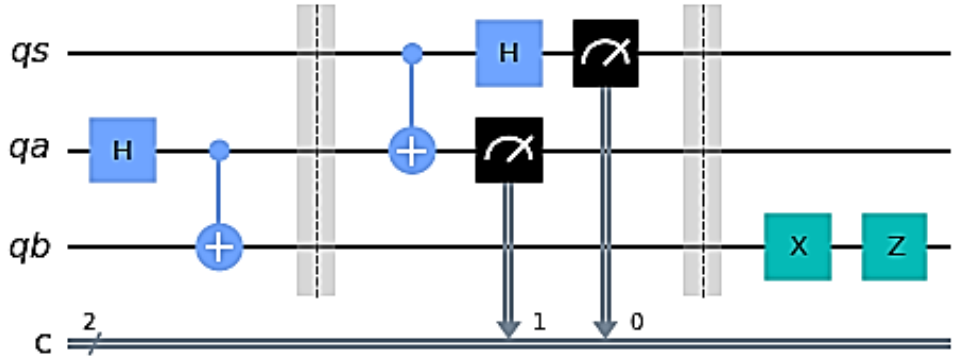
量子遙傳 (1)

- 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 $|\Phi^+\rangle=1/\sqrt{2}(|00\rangle+|11\rangle)$ 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$|\Phi^+\rangle=1/\sqrt{2}(|00\rangle+|11\rangle)$之二個量子位元中的一個。

量子遙傳 (2)

- 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 可以透過下圖中的量子遙傳量子線路來完成，說明如下:



對應量子遙傳的量子線路圖

量子遙傳 (3)

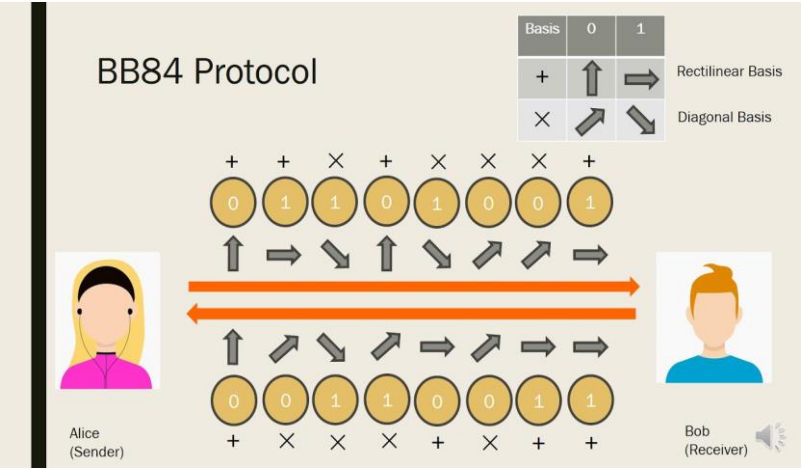
- Alice首先以 q_s為控制位元，以q_a為目標位元加入受控非(Controlled-Not, CNOT)閘，然後針對q_s加入哈達馬(Hadamard, H)閘，最後再針對q_s及q_a進行測量，並將測量結果透過古典通訊通道傳送給 Bob。當 Bob 收到測量結果時，可以分為以下 4 個處理狀況來完成量子遙傳：
  - (狀況1) q_s及q_a的測量結果均為$|0\rangle$，則q_b本身就是q_s的狀態。
  - (狀況2) q_s的測量結果為$|0\rangle$，而q_a的測量結果為$|1\rangle$，則針對q_b進行 X閘操作就可以還原q_s的狀態。
  - (狀況3) 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。

Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

BB84通信協定 (1)

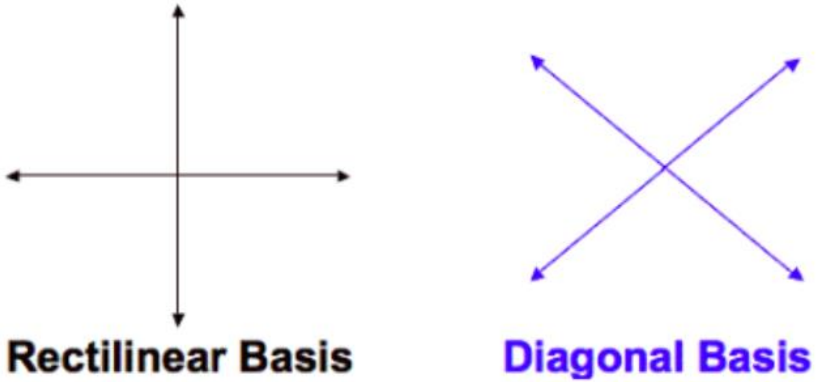
- BB84通信協定由Bennett與Brassard在1984年提出，是一種量子密鑰分發(quantum key distribution, QKD)協定，被認為是第一個量子密碼協定。
- BB84通信協定可以用來傳送單次密碼本(one-time pad, OTP)的一次性密鑰，只要密鑰的長度大於或等於密文的長度，就可以達到完全不可破解的資訊理論安全或無條件安全或可證明安全(provable security)。
- 密文(ciphertext)完全不洩漏明文(plaintext)的任何訊息，因此即使在攻擊者具有不受任何條件限制能力的情況下，也依然能夠保持密文不可能被破解的完美安全(perfect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



Source:https://www.youtube.com/watch?v=44G9UuB2RWI&ab_channel=%EC%B0%BD%ED%95%98%EA%B9%80

BB84通信協定 (2)

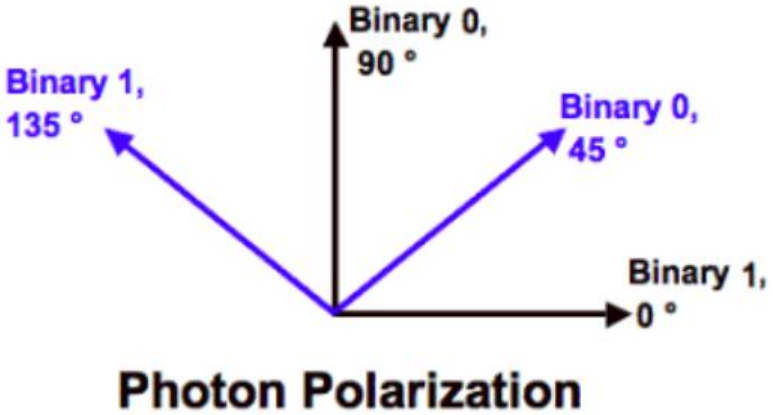
- BB84協定使用量子通道傳送量子態，並同時使用古典通道傳送量子態的測量結果與控制訊息。其作法為使用兩組不同的量子狀態基底，例如，若量子通道以光纖或是量子衛星雷射鏈路實現，則可以使用一組包含垂直偏振與水平偏振的直線(rectilinear)基底，以及一組包含45度偏振與-45度偏振的對角(diagonal)基底。



Source:https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

BB84通信協定 (3)

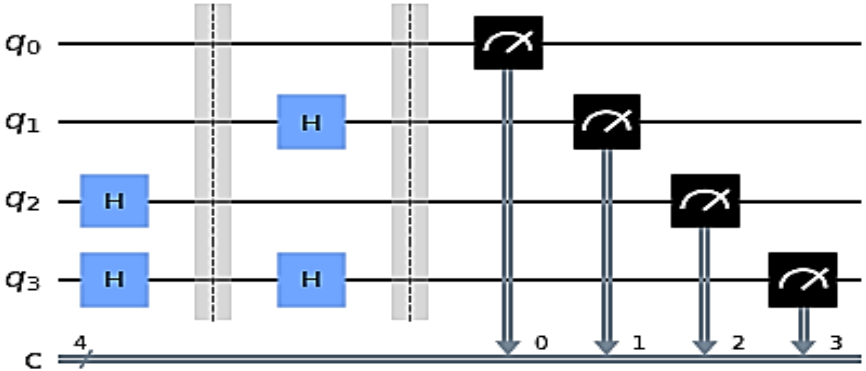
- 然後讓發送節點與接收節點在每一次傳送量子態與測量量子態時各自隨機選擇一個基底，例如，發送節點可以選擇直線基底透過垂直偏振傳送位元0及透過水平偏振傳送位元1；而接收節點可以選擇對角基底，若測得45度偏振則代表位元0，反之，若測得-45度偏振則代表位元1。

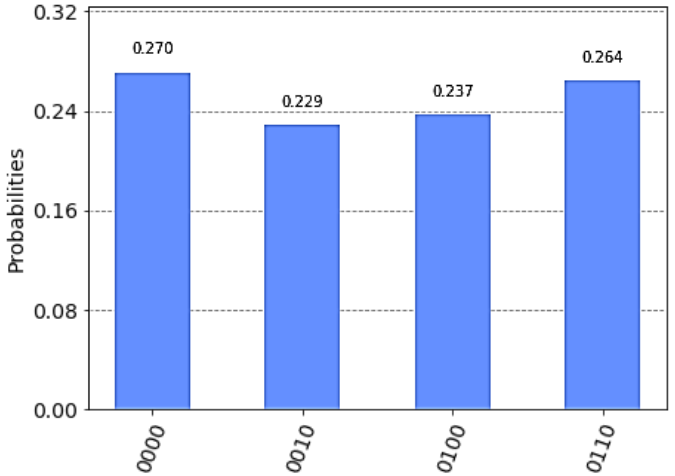


Source:https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

BB84通信協定 (4)

- 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。下圖為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。





BB84通信協定 (5)

- 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。

BB84通信協定 (6)

- 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。

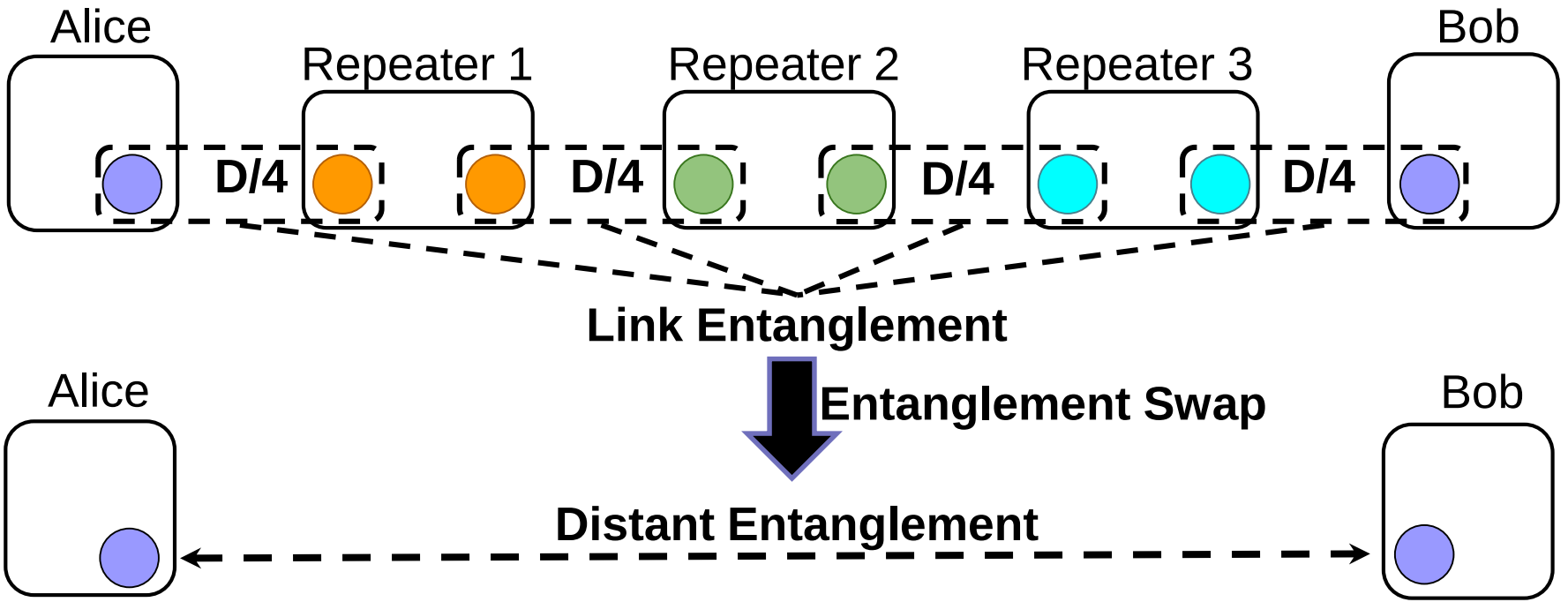
Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

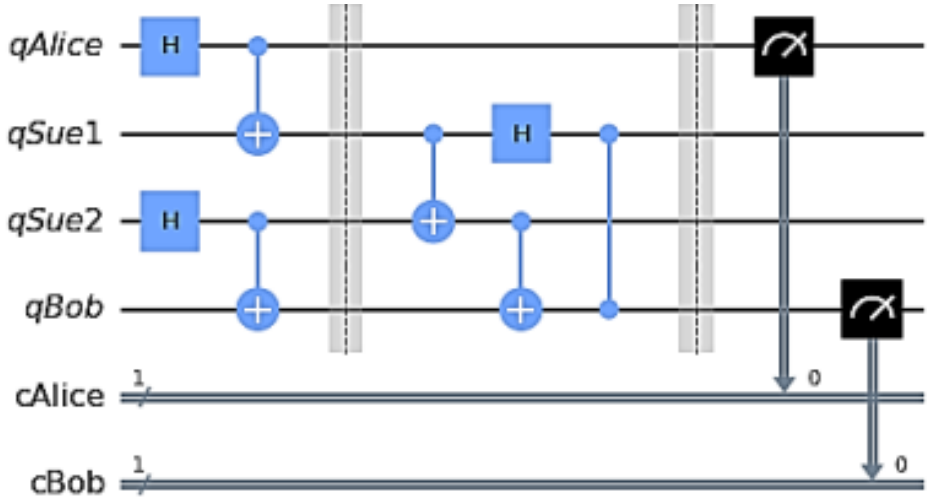
量子中繼器 (1)

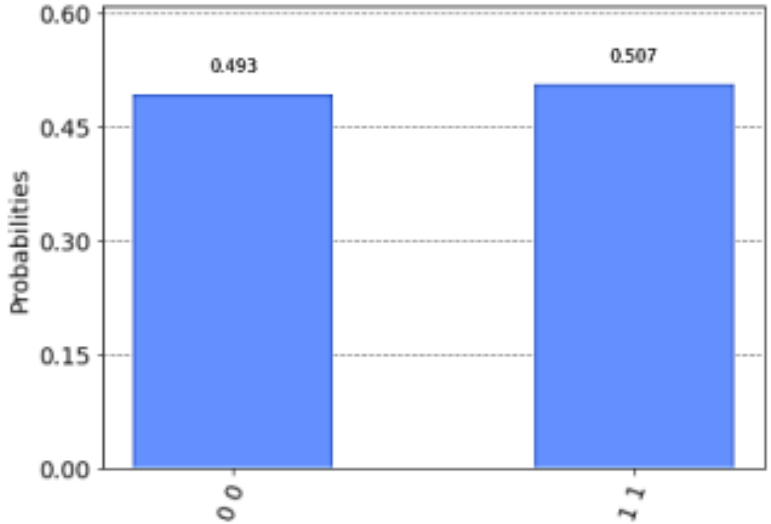
- 量子中繼器可以用來延長量子通道的距離。如前所述，一個量子中繼器依賴量子糾纏生成、糾纏純化、 量子記憶體以及糾纏交換等機制連實現。以下我們僅針對其中最核心的糾纏交換機制進一步的說明，必且展示其對應的量子線路以及量子線路的執行結果。
- 假設量子網際網路的兩個節點 Alice 與 Bob 距離太遠，無法在二者之間建立直接相連的量子通道使二者的 量子位元形成量子糾纏。但是在 Alice 與 Bob 中間存在節點 Sue，分別可與 Alice 與 Bob建立直接連接的量子通 道。此時可以透過 Sue進行糾纏交換，建立 Alice與 Bob 之間的量子糾纏，其做法描述如下頁圖所示:

量子中繼器 (2)


Alice
Repeater 1
Repeater 2
Repeater 3
Bob
D/4
D/4
D/4
D/4
Link Entanglement
Entanglement Swap
Alice
Bob
Distant Entanglement

量子中繼器 (3)





糾纏交換量子線路與其執行結果

Outline

- 緒論
- 量子網際網路架構及背景知識
  - 量子糾纏
  - 量子遙傳
  - BB84通信協定
  - 量子中繼器
- 結論

結論

- 本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，以及如何透過連接位於全球各地的量子電腦，以進行大規模的分散式量子計算實現量子霸權。
- 未來研究方向: 糾纏純化(entanglement purification)、量子記憶體(quantum memory)、量子交換器(quantum switch)、量子網際網路繞徑(quantum Internet routing)技術。

Q&A