中文

成大研發快訊　第十四卷 第九期 - 2010年七月十六日
[http://research.ncku.edu.tw/re/articles/c/20100716/3.html]

新的高效能三方量子金鑰分配協定

石瀚成、李國彰、黃宗立*
國立成功大學資訊工程學系
islab@ismail.csie.ncku.edu.tw

IEEE Journal of Selected Topics in Quantum Electronics, Vol. 15, No. 6, pp. 1602-1606

大部分現存的量子金鑰分配協定(QKDP)皆假設所有的通訊方都配備了量子儀器(QD)，例如：量子位元產生器、量子記憶體或量子量測裝置。然而，在實際的情況中，這些量子儀器是非常昂貴的且可能只有伺服器端有足夠的能力擁有這些儀器設備。雖然學者Phoenix等人首先發現此問題的存在，但是他們提出的方法卻只有13%的量子使用率。本論文提出二種類型的三方量子金鑰分配協定。第一種方法假設伺服器端是誠實的，且允許通訊者只執行基本量子運算達到分享密鑰之目的。此外，考慮到伺服器端的信賴度問題，本論文的第二種方法將不假設伺服器端為可信任的。最後，本論文所提出的三方量子金鑰分配協定，由於使用了量子記憶體之觀念與利用單向雜湊函數之技術檢查竊聽者存在與否，所以比起現存的方法提供了更高效能的量子使用率。

伺服器端為可信任之三方量子金鑰分配協定 **(KHC)**

首先提出的三方量子金鑰分配協定中，發送者Alice將傳送密鑰給接受者Bob，詳細的描述過程如下（如圖一）：

步驟1. 伺服器端產生n個相同極化狀態 ｜0〉的量子位元Q_1，然後將量子位元Q_1透過量子通道傳送給Alice。
步驟2. Alice收到Q_1之後，產生一組亂數序列K且計算檢查碼$h=H(K)$，K代表密鑰、H代表單向雜湊函數。完成後，可得到長度為n位元的序列$K||h$，Alice根據$(K||h)_i$對量子位元執行運算U_i。此外，Alice產生長度為n位元的亂數序列B_1，且根據$(B_1)_j$對量子位元執行運算U_j，方式如下：

- 當$(K||h)_i$的位元是0 (1)，對應的運算U_i是U_0 (U_1)。
- 當$(B_1)_j$的位元是0 (1)，對應的運算U_j是U_0 (U_2)。

Alice執行運算U_i與U_j，將Q_1的極化狀態轉換成Q_2。最後，將量子位元Q_2透過量子通道傳送給Bob。

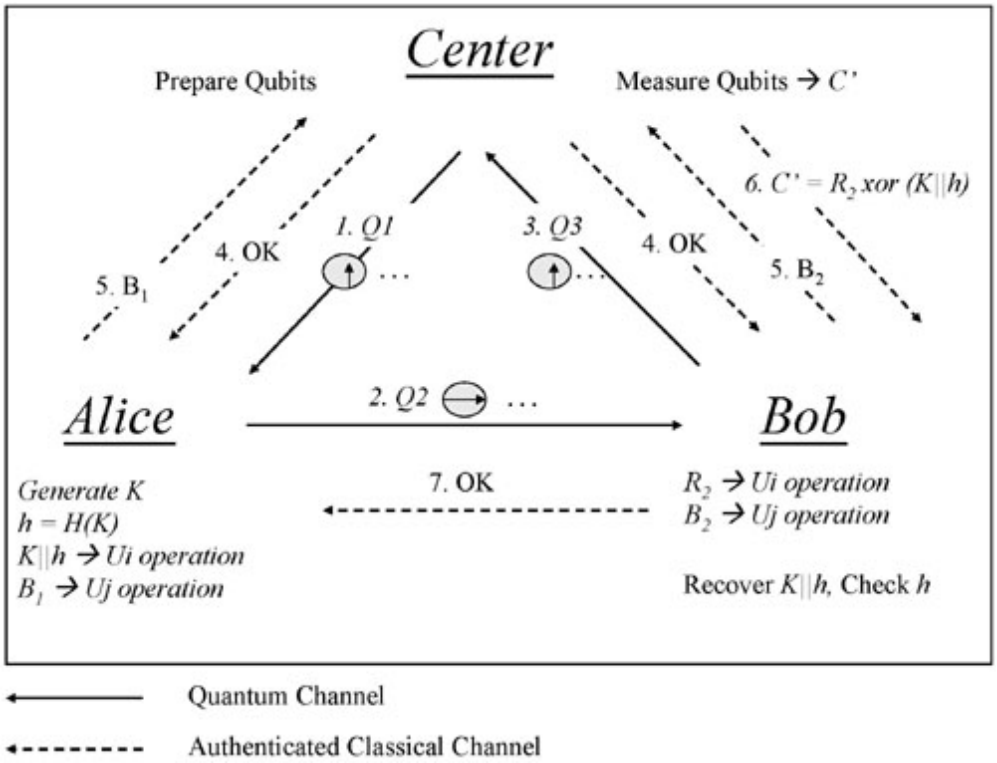
步驟3. Bob收到Q_2之後，產生二組長度為n位元之亂數序列R_2與B_2。接著，分別根據$(R_2)_i$與$(B_2)_j$對量子位元執行運算U_i與U_j，方式如下：

- 當$(R_2)_i$的位元是0 (1)，對應的運算U_i是U_0 (U_1)。
- 當$(B_2)_j$的位元是0 (1)，對應的運算U_j是U_0 (U_2)。

Bob執行運算U_i與U_j，將Q_2的極化狀態轉換成Q_3。最後，將量子位元Q_3透過量子通道傳送給伺服器端。

步驟4. 伺服器端收到Q_3之後，通知Alice與Bob已收到。

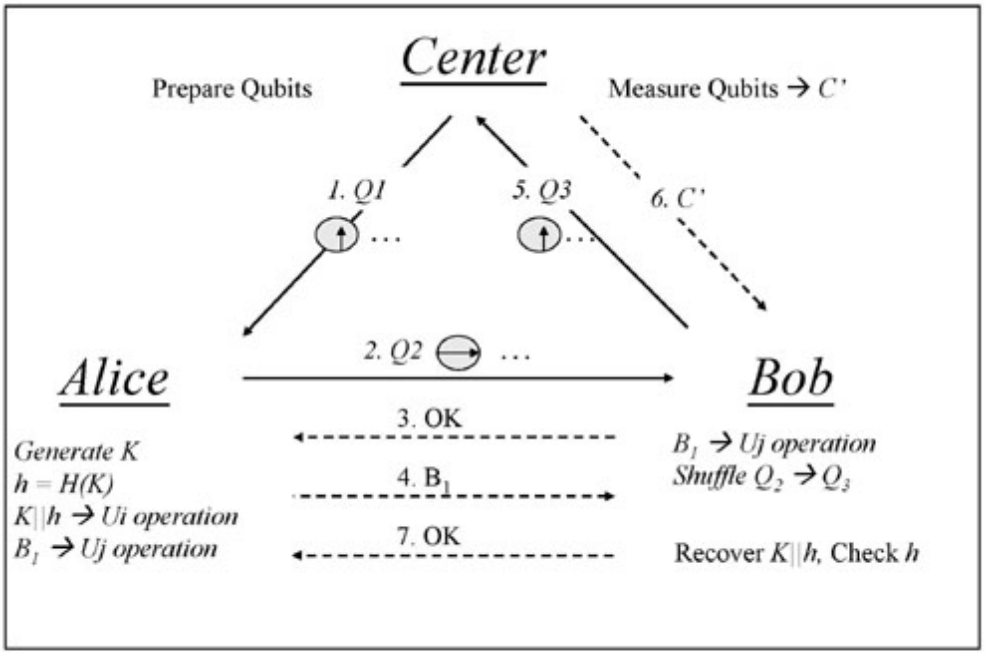
步驟5. Alice與Bob分別傳送B_1與B_2給伺服器端。
步驟6. 伺服器端收到B_1與B_2的資訊後，對量子位元執行對應的U_j運算，可得到原始的極化狀態。接著，伺服器端使用R基底量測量子位元，可獲得量測結果$C'=R_2 \oplus (K||h)$且將C'傳送給Bob。
步驟7. Bob收到C'之後，將重新獲得$(K||h)= R_2 \oplus C'$且驗證$h=H(K)$是否正確。如果$h=H(K)$結果正確，Bob將得到正確的密鑰K且告知Alice “OK”。



圖一、伺服器端為可信任之三方量子金鑰分配協定 (KHC)

允許伺服器端為不可信任之三方量子金鑰分配協定 **(KUC)**

步驟1. 相似KHC的步驟1，伺服器端產生n個相同極化狀態｜0〉的量子位元Q_1，然後將量子位元Q_1透過量子通道傳送給Alice。
步驟2. 相似KHC的步驟2，Alice收到Q_1之後，產生長度為n位元的亂數序列B_1與一組亂數序列K且計算檢查碼$h=H(K)$，可得到長度為n位元的序列$K||h$。此外，Alice分別根據$(K||h)_i$與$(B_1)_j$對量子位元執行運算U_i與U_j。最後，Alice將執行後的量子位元Q_2透過量子通道傳送給Bob。
步驟3. Bob收到Q_2之後，儲存Q_2且告知Alice “OK”。
步驟4. Alice收到Bob的通知後，將序列B_1傳送給Bob。
步驟5. Bob根據$(B_1)_j$執行對應的運算U_j。當$(B_1)_j$是0 (1)，對應的運算U_j為U_0 (U_2)。此外，Bob將量子位元重新排序且透過量子通道將排序後的Q_3傳送給伺服器端。
步驟6. 伺服器端收到Q_3之後，使用R基底量測收到的量子位元，可獲得量測結果$C'=Shuffled_(K||h)$，接著將C'傳送給Bob。
步驟7. Bob將C'重新排回原位，可得到序列$(K||h)$且驗證$h=H(K)$是否正確。如果$h=H(K)$結果正確，Bob將得到正確的密鑰K且告知Alice “OK”。



圖二、允許伺服器端為不可信任之三方量子金鑰分配協定 (KUC)

三方量子金鑰分配協定比較分析表

	學者 Phoenix 等人	KHC	KUC
伺服器端需要量子記憶體	否	是	否
使用者需要量子記憶體	否	否	是
伺服器端需要測量光子	是	是	是
量子通道數目	3	3	3
討論竊聽者方法	隨機選擇部份	雜湊值	雜湊值
分享金鑰長度	n/8	n-|h|	n-|h|
伺服器端必須信任	否	是	否
正規證明方法	否	是	是

本論文提出了二種有效的三方量子金鑰分配協定，其中伺服器端必須擁有所有昂貴的量子儀器與設備，而使用者只需擁有少數的儀器即可。首先提出的三方量子金鑰分配協定(KHC)，使用者只需執行簡單的量子運算即可達到密鑰分享的目的。接著提出的三方量子金鑰分配協定(KUC)，利用重新排序的技巧達到可防止被不信任的伺服器端取代Bob的量子運算之攻擊。然而，Bob必須擁有量子記憶體，才可執行重新排序的技術。所以在伺服器端不可信任的情況下，如何設計不需要使用者擁有量子記憶體也可達到三方量子金鑰分配之協定，在未來是一個重要的議題。