量子密碼學研究領域介紹

黃宗立，楊竣崴，張智閎，羅翊萍，高士閎，黃勝亮，洪志修，余昆霏
國立成功大學資訊工程學系
量子資訊與網路安全實驗室
(Quantum Information and Network Security Laboratory)
E-mail: hwangtl@csie.ncku.edu.tw
http://islab.csie.ncku.edu.tw/

摘要

量子密碼學(Quantum cryptography)是一門結合量子力學與密碼學之研究。不同於以複雜的計算過程或數學難題為基礎的傳統密碼學，量子密碼學利用量子物理特性來達成各種密碼技術。可說是量子電腦時代的密碼技術。由於量子力學深奧而有趣，其應用於資訊安全的保護自然也是潛力無限。本文主旨在於提綱挈領地介紹近幾年在量子密碼學這新興領域的各類研究。

關鍵詞：量子密碼學、量子金鑰分配、量子金鑰協商、隨機量子金鑰分配、量子秘密分享、量子直接通訊、確定式量子通訊、量子對話、可控制式量子通訊、量子私密比較、量子簽章、量子身分認證、量子集體雜訊、量子網路。

壹、前言

資訊技術的成熟與網路科技的快速發展，為人們的生活帶來莫大的便利性，使得我們能夠方便地透過電腦網路進行資料的傳送、存取及交換。然而，伴隨而來的隱憂則是資訊安全的問題考量，例如資料在傳輸過程中，是否遭受洩露或竄改。基於保護資料傳送之安全性，目前則使用密碼技術來達成資料的機密性及認證性。

傳統密碼技術可分為對稱式密碼系統及公開金鑰密碼系統，前者以替換和重排為基礎，後者則是植基於數學上的難題來達到其安全性，例如：因數分解[1, 2]、離散對數[3, 4]等，這些難題以目前電腦的運算速度來進行破解，可能需花上數十億年以上的時間，因此被公認是安全的。迄今公開金鑰密碼系統仍是傳統密碼學的研究主流，並且被廣泛地應用在不同的研究領域，例如金鑰分配、秘密分享、金鑰協商與電子簽章等。但在量子電腦和量子演算法的發展與實現後，使得一些在傳統電腦上被認為難解的數學難題，已被證明可以使用量子電腦在多項式的時間內破解[5-9]。換言之，目前基於數學難題的傳統密碼系統，都可能在量子電腦實現後，變得不安全。

在量子資訊中，量子位元（qubit）是一個組成二維量子系統的基本元素，其中$|0\rangle$代表傳統位元的“0”、$|1\rangle$代表傳統位元的“1”。量子位元與傳統位元有顯著的差異，某一時刻的傳統位元只會處在一種狀態（非 0 即 1），但量子位元卻可同時具有 0 與 1 的狀態，稱為「量子疊加態」，此量子疊加態直到被量測破壞後，才會呈現出 0 或 1 的最終結果。

由於量子疊加態的特性，使得量子具有平行處理之能力，而使得量子計算應用在某些問題上顯著地優於傳統計算，雖然量子位元具有疊加態的特性，可以同時計算所有結果的值。但也由於量子位元量測的特性，使得量子位元經由量測後，將只有一個確定的結果，即疊加態立即消失。因此，雖然量子位元利用疊加態之特性，可較傳統計算更快解決部分難題，但量子計算並非在所有運算上都比傳統計算快速。所以如何利用量子特性設計量子演算法，達到量子計算的強大能力是目前一直持續研究的議題。目前，在量子計算中，最有名的兩個演算法如下：1994 年，學者 Shor 的量子演算法可以在多項式時間內，破解因數分解的問題。1996 年，學者 Grover 的量子搜尋演算法，可以在 N 個無排序的資料中，只需 $O\left(\sqrt{N}\right)$ 次即可找到搜尋的結果。

另一方面，在量子資訊的相關研究迅速發展下，使得利用量子的物理特性來製作的量子電腦在未來很可能被實現。早期，IBM 宣稱發展出具有 7 量子位元的量子電腦，且成功測試學者 Shor 的演算法，但只能執行兩位數的因數分解。2007 年，加拿大的量子計算公司 D-wave 宣稱研發出首部量子電腦，此電腦具有 16 量子位元的計算能力。2013 年，D-wave 研發生產具有 512 量子位元的量子電腦，雖然此設備是否為真正的量子電腦或可以執行所有的量子演算法仍然備受質疑，但南加大的洛克希德馬丁量子電腦研究中心（Lockheed Martin Quantum Computation Center）研究[10]認為 D-wave 所開發的設備已經很接近真正的量子電腦，且所使用的概念和方法有機會被運用開發通用的量子電腦。

若 D-wave 公司發展的量子電腦可執行學者 Shor 的演算法[5-7]或其相關的演算法[8, 9]，則目前植基於數學難題的傳統密碼系統，例如：基於因數分解的難題、離散對數的難題或橢圓曲線的離散對數問題，將在多項式時間內被破解。換言之，為了對抗量子電腦強大的運算能力，如何利用量子特性設計相關的密碼協定，使其不被量子電腦輕易破解，將更成為目前重要的研究發展議題、同時也是未來的研究趨勢。

此外，在傳統密碼學裡，攻擊者亦可能藉由竊聽或監測合法使用者之間的通訊，蒐集與金鑰有關的密文進行分析研究，進而破解金鑰。現今的傳統密碼學技術及網路科技，對於竊聽之類的被動式攻擊行為是無法偵測的，而量子理論的提出，卻能解決在傳統密碼學裡，偵測竊聽者的問題。

基於上述的安全需求，使得量子密碼學的研究受到廣泛的重視。量子資訊科學的研究，起源於 1980 年代，最初是探討計算與物理系統之間的關係，後來進而發展至利用量子物理特性做為計算與通訊媒介的相關研究[11-14]，而量子密碼學則是其中最重要的研究領域之一。量子密碼學主要是利用量子的物理特性來達成量子資訊安全之目的，這些重要的量子物理特性包括：

- **量測不確定性**(uncertainty of measurement)：若使用某個基底(basis)對量子極化產生一量子位元，那麼使用該基底對該量子位元進行量測，便能得到確定的量子資訊。但是，若使用其它基底進行量測，則其量測結果是不確定的。換言之，在此情況下，即保證了量子的不可複製性。

- **不可複製性**(non-cloning)：1982 年，學者 Wootters 與 Zurek[15]提出量子態無法複製的證明，即量子狀態處於未知的情況下，是無法對量子狀態進行完美的複製。

目前而言，大多數的量子密碼研究著重於量子金鑰分配與量子通訊協定相關之應用，例如：量子金鑰協商、隨機量子金鑰分配、量子秘密分享、量子直接通訊、確定式量子通訊、量子對話、可控制式量子通訊等。而根據不同環境，亦有量子私密比較、量子簽章等協定被廣泛的研究。這些量子協定其安全性並不植基於任何數學難題上，而是利用量子物理特性提供在不同環境中的安全需求，除此之外，亦能偵測竊聽者的存在。本文將以上述所列出之量子密碼協定為主軸，分別簡述各個協定在現今量子密碼學之背景及研究現況。

貳、量子金鑰分配 (Quantum Key Distribution)

量子金鑰分配協定為昔知量子安全協定中最廣為發展的領域之一，學者 Bennett 和 Brassard 首先於 1984 年，使用量子物理特性提出第一個量子密碼協定[16]，在此協定中，雙方參與者在不需要事先分享秘密金鑰的情況下，透過量子通道(quantum channel)與傳統通道(classical channel)，讓傳送方可以安全的將一把秘密金鑰分配給接收方，其中，傳統通道被假設為已認證通道，換言之，攻擊者只能竊聽訊息，但是無法修改或是阻斷此通道上所傳送的訊息。此協定為第一個量子金鑰分配協定(quantum key distribution protocol; QKDP)，亦被稱之為“BB84”。而 BB84 協定的安全性主要基於**量測不確定性**與**不可複製性**這兩個量子物理特性。透過這兩個量子物理特性，BB84 中所傳送的秘密金鑰之安全性可以被證明為「無條件安全」(unconditional security)[17-25]，意味著其安全性不需要仰賴任何數學上的計算難題。而後許多相關的量子金鑰分配協定也陸續發表，甚至有學者提出三方的量子金鑰分配協定，即藉由第三方負責產生量子和協助通訊雙方安全的分配一把金鑰。而量子物理的特性陸續被廣泛應用於設計量子金鑰分配協定與討論證明其安全性。

參、量子金鑰協商 (Quantum Key Agreement)

金鑰協商的觀念最早是在 1976 年，由 Diffie 和 Hellman 兩位學者所提出[26]，其演算法的目的是使兩位使用者共同協商出一把共享祕密金鑰 (shared secret key)，以其作為後續通訊之加解密。通訊雙方透過此演算法可以在不安全的通道 (insecure communication channels) 上共同建立一把安全的金鑰，因此金鑰協商這門領域的研究在往後受到密碼界極大的重視，至今亦已累積豐碩的研究成果。不幸地，如同上文所述，這些基於解離散對數或因數分解等數學難題的協定，其安全性將在量子電腦強大的運算能力下備受威脅且不再是堅不可破。

故如何利用量子特殊的物理特性來發展、建立一套安全的金鑰協商協定漸漸成為一項重要的研究議題。現有量子金鑰協商協定的研究中，探討的主要是如何使雙方或多方參與者在一個彼此互相不信任的環境 (mutually-mistrustful environment) 下，利用量子資源以及既定的程序步驟安全且秘密地建立一把共享金鑰，其中這把共享金鑰是由協定中的各個參與者貢獻出自己的子金鑰才得以產生。為了確保所有參與者對於共享金鑰的決定具有相同的影響力，必須極力避免讓任何一方參與者能夠單獨的決定或控制這把共享金鑰。由此可知，“公平性”一直是量子金鑰協商協定中一項非常重要的議題。一個被視為公平公正的量子金鑰協商協定，除了需滿足所有參與者對於共享秘密金鑰擁有同樣的影響力之外，還需具備當任何參與者執行非法之操作以試圖控制共享金鑰時，當下能夠將其偵測出來之能力。若非如此，一但有參與者嘗試去非法地修改共享金鑰，然而卻導致參與者間共享的金鑰不一致而失敗，如此可將失敗之原因歸咎於外部竊聽者之干擾，事實上卻是內部的惡意參與者所造成的。因此，如何避免上述問題並使協定能夠達到真正的公平即成為研究此門領域的一項挑戰。

肆、隨機量子金鑰分配 (Probabilistic Quantum Key Distribution)

在目前傳統密碼學的研究中，我們無法以真正隨機的方式來決定出一把秘密金鑰。真正隨機的意義就好比丟擲一枚硬幣到空中取下，而此硬幣的正、反面是由上帝所決定的。然而，基於量子天生具有的不確定特性，想要設計出一把真正隨機的金鑰就不再是紙上談兵了。

而前述的量子金鑰協商協定中，即適用於雙方互不信任的環境中，但是此協定的設計為參與者事先準備好各自的子金鑰，接著透過量子傳輸的保護，達到所產生的秘密金鑰為所有參與者所共同決定之目的。由於此種設計方法，並沒有利用到量子天生具有的不確定性的優勢。所以，2011 年，學者 Hwang 等人[27]基於量子量測的不確定性，進而發展出新概念的量子金鑰分配協定，稱之為隨機量子金鑰分配協定，其適用於互不信任的雙方可以互相合作，利用量子物理的特性產生一把真正隨機的金鑰，即便是一位元的金鑰值也無法猜測。因此，隨機量子金鑰分配協定在量子密碼學中，屬於新的概念也是新的研究領域。

伍、量子秘密分享 (Quantum Secret Sharing)

秘密分享主要的理念是將一把主密鑰分成多把子密鑰，然後分給多人分別保管這些子密鑰，所以當要重建這把主密鑰時，必須所有參與保管這些子密鑰的人共同合作才能復原這把主密鑰，且缺少一名參與保管的人就無法重建。

與秘密分享相仿，在量子秘密分享的環境中，存在一秘密分享者與多個參與者。在協定完成後，所有參與者必須合作才能解得秘密分享者之私密訊息，缺少任何一位成員

皆無法解得該秘密訊息。1999 年，學者 Hillery 等人[28]提出第一篇量子秘密分享協定後，很多量子秘密分享的相關研究相繼提出。在量子秘密分享協定之研究中，除了探討量子在秘密分享者與參與者之間的傳送方式不同所帶來之影響外，也探討惡意的參與者是否可能在不被發現的情況下，忽略其他參與者就能夠直接竊取秘密分享者之私密訊息，這個問題也成為研究量子秘密分享協定中最重要的一環。

陸、量子訊息通訊 (Quantum Message Communication)

前述之量子金鑰協定或量子秘密分享協定，主要是分配安全的金鑰給予通訊雙方或協定參與者。在量子金鑰分配完成後，若通訊雙方想要溝通訊息，他們可以利用金鑰加密訊息，並以傳統通道傳輸密文。**量子訊息通訊**即為直接使用量子保護私密訊息的通訊協定，其考慮的是在無須事先共享金鑰的環境下就能夠進行私密通訊。由於傳統密碼學無法達到不需加密（即不需共享金鑰）的私密通訊，因此量子訊息通訊為量子密碼學獨有且新穎的研究議題。根據傳輸類型與是否需要額外的傳統訊息來協助雙方完成通訊，量子訊息通訊協定可以分為三類：（1）**量子直接通訊協定**(Quantum Secure Direct Communication)、與（2）**確定式量子通訊協定**(Deterministic Secure Quantum Communication)兩種。另一方面，考慮兩位通訊參與者並非單純的傳送者與接收者關係，而可能是兩方都想要交換訊息，（3）**量子對話協定**(Quantum Dialogue) 則為另一種不同的量子訊息通訊協定。

（1）量子直接通訊協定

量子直接通訊協定中，傳送方將秘密訊息透過量子編碼後，直接傳送給接收方。除了雙方公開討論檢查量子傳輸的安全需要交換一些傳統訊息，接收方可以直接量測接收到的量子，得到傳送方欲傳送的私密訊息。

2002 年，學者 Bostrom 與 Felbinger [29]提出第一篇量子直接通訊協定，由於此協定中量子傳輸為訊息接收方發送給訊息傳送方，再由傳送方送回給接收方，如此一來一回的傳輸方式使得此協定又稱為乒乓協定（ping-pong protocol），雖然已有學者證明乒乓協定是不安全的，但其新穎的傳輸模式卻被廣為應用於量子傳輸協定的設計。有別於乒乓的傳輸模式，2003 年，學者 Deng 等人[30]提出第一篇利用兩階段傳輸的量子直接通訊協定，同時也是第一篇安全的量子直接通訊協定。爾後，如何在符合安全準則下，能夠提升量子利用率，也成為諸多後續研究突破的目標。

（2）確定式量子通訊協定

確定式量子通訊為傳送方將編碼的量子傳送給接收方，確認量子傳輸的安全後，再傳送一組傳統訊息給接收方。接收方需要得到這組資訊才能夠正確地解開通訊之內容。

協定過程中是否有額外傳送傳統訊息，為區分量子直接通訊協定與確定式量子通訊協定之最大差異。

1999 年，學者 Shimizu 與 Imoto [31]提出第一篇確定式量子通訊協定，在接收方收到傳送方所產生的所有量子之後，他必須等到傳送方公布量子的初始狀態，始可推得傳送方的秘密訊息。之後陸續有學者利用量子糾結置換（entanglement swapping）與量子隱傳(quantum teleportation)等量子物理特性相繼提出各種確定式量子通訊協定。

（3）量子對話協定

不同於上述量子直接通訊協定或確定式量子通訊協定，皆為單方向的通訊協定。在量子對話協定中，通訊雙方可以同時交換彼此的秘密訊息。傳送方將秘密訊息透過量子編碼後，直接傳送給接收方。接收方收到訊息後，沒有直接量測量子，而是將自己的秘密訊息也透過量子編碼在相同的量子上。完成編碼後，接收方量測編碼完的量子且公佈量測到的結果給傳送方。如此一來，通訊雙方便能達成同時交換秘密訊息的目的。

2004 年，學者 Nguyen[32]提出第一篇量子對話協定，但在 2008 年，學者 Gao 等人[33]發現學者 Nguyen 的量子對話協定存在資訊洩漏的問題，即竊聽者可以透過分析傳送的資訊得到將近一半的傳輸訊息。爾後，如何解決資訊洩漏的問題，並設計出安全的量子對話協定成為此研究領域中最重要的一環。

有別於量子訊息通訊，另一種量子通訊的理念被提出，亦即**可控制式量子通訊** (Controlled Quantum Communication)。在原本僅有傳送方與接收方的環境下，加入一位或多位控制者 (controller)。接收方必須獲得控制方的允許 (權限，permission)，方可解開傳送方之私密訊息。這樣的協定可利用在電子商務之環境：訊息接收方向傳送方購買文件後，傳送方將資訊傳輸給接收方。但接收方目前還無法打開文件，必須待控制方確認已經付款完成後，再將有助於解開文件的權限資訊傳輸給接收方，接收方才能得到傳送方之文件。本研究領域最主要考量的是訊息接收方是否會採取任何主動攻擊的方式在沒有控制者的允許下就解開訊息。更進一步，在允許控制者可以執行任何主動攻擊以竊取傳送者訊息的前提下，傳送者的私密通訊仍然可以安全執行，則是未來可能的研究方向。

柒、量子私密比較 (Quantum Private Comparison)

在生活中，私密比較是很有趣的議題，可以擴展應用到許多現實層面上，例如拍賣會的喊價與比價、不公開的選舉投票、及身分認證等各種環境。其主要的目的是讓一對互不信任的雙方去比較各自擁有的私密訊息是否相等，但又不願意透漏自己的任何私密資訊給其他人知道。

而最為著名的問題即是由學者 Yao[34]所提出的”Millionaires’problem”的比較，內容為兩個百萬富翁如何在不透漏自己的財富下，讓彼此去比較雙方的財富是否相等。後來

有學者 Lo[35]指出要比較私密訊息的雙方在不藉由第三人協助幫忙下進行公平的比較而不洩漏任何訊息是不可能達成的。之後在私密比較的研究中，加入第三方的協助已成為必要的條件。

在量子私密比較中，如何避免協助幫忙比較的第三方進行內部的攻擊是最廣泛被探討的安全議題，例如：不依照比較步驟流程實施、或是企圖得知任一方的資訊等。為符合實際狀況，我們通常會以"第三方除不能與任一方共謀外，可以實施任何的攻擊" 視為事先的假設。除了比較私密是否相等外，越來越多人開始投入研究如何比較私密的大小，以及如何在多人間從事私密大小之比較。

捌、量子簽章 (Quantum Signature)

數位簽章(digital signature) [26, 36]，其概念模擬在紙上的物理簽名，主要利用非對稱式加解密演算法之技術(如 RSA[36]演算法，其難度基於因數分解之數學難題)，用於鑒別數位信息或身分識別的方法。至今，數位簽章已被廣泛應用在電子商務系統、電子交易…等。然而，在 1994 年，學者 Peter Shor[6]提出了量子因數分解演算法（factorization algorithm），證明了量子電腦可以在多項式時間（polynomial time）裡有效地進行因數分解。這項突破使得數位簽章，甚至是傳統密碼學的技術面臨了強大的挑戰。而**量子簽章**，其設計基於量子的物理特性，達成數位簽章機制之環境與要求，將在未來量子電腦普及的網路中，成為保護資訊不可或缺的重要研究之一。

在現存文獻的量子簽章下，存在一簽章者(Signatory)，利用自己的秘密資訊簽署訊息；存在一驗證者(Verifier)，負責驗證簽章者身分與簽章合法性。由於量子力學的特性，所有的操作(operation)皆為可逆運算，因此現存文獻中大部分量子簽章系統的環境與對稱式數位簽章機制相同，皆存在一個最重要的角色：受信任的第三方─仲裁者(Arbitrator)。仲裁者在協定中必須能夠協助驗證者成功的驗證簽章者的身分與簽章的合法性，也必須具備雙方 (簽章者與驗證者) 一定程度的信任，當糾紛發生時，仲裁者擁有判斷是非的能力以解決紛爭。因此在此環境下之量子簽章又可被稱為**可仲裁式量子簽章**(Arbitrated Quantum Signature, AQS) [37-49]。可仲裁式量子簽章具備以下特性：

1. 不可偽造性(Non-forgeability/ Unforgeability)：只有簽章者能夠產生合法簽章，其他人無法產生也無法偽冒。簽章者產生並送出簽章後其簽章內容不可被任意人(包含簽章者本身)更改。
2. 不可否認性(Non-repudiation/Undeniability)：在完成簽章流程後，簽章者不能否認自己所簽署的簽章，驗證者也不能否認已驗證簽章的事實。
3. 可驗證性(Verifiability)：簽章者所簽署的資訊必須可被仲裁者或驗證者所驗證。

除此之外，基於量子物理特性下所設計各式各樣的簽章應用環境，如：量子盲簽章(blind signature) [50]、量子代理簽章(proxy signature)[51]、量子群簽章(group signature)[52]…等，也陸續被廣泛研究中。

玖、其他相關議題研究

基於前述的各種量子密碼學的主題被廣泛研究之下，也引領出一些現實層面必需得面臨到的議題，主要可分為三大類：(1) **量子身分認證**(Quantum Identity Authentication)[53-55]、(2) **量子集體雜訊**(Quantum Collective Noises)[56-59]、(3) **量子網路**(Quantum Network) [60-63]。

(1) 量子身分認證

在現實生活中，電話的聯絡交談就是身分認證通訊的一個例子，即通訊雙方彼此都知道對方身分為誰的情況下進行通話。所以在量子密碼學中，大部分的協定設計也都是假設在具有身分認證的雙方進行彼此分享私密或通訊，也就是參與者之間的通訊需在認證通道(authenticated channel)下完成。但實際上這條認證通道並不一定隨時存在，故如何在不存在這條認證通道下進行分享私密和通訊之外，還能保證參與者的身分是正確的，此研究領域也廣受許多學者相繼探討。

(2)量子集體雜訊

雖然利用量子的特性發展出了許多可以偵測竊聽者存在的安全性協定，但這些協定都必須假設在通訊的過程中無雜訊干擾的環境下(也就是量子通道為理想的通道)。如果沒有此假設，則在實際的量子通道裡，所面臨的錯誤率就無法分辨是雜訊干擾造成，抑或是竊聽者攻擊所造成的。基於此弱點，攻擊者就可以藉由雜訊來隱蔽其攻擊所造成的錯誤率，讓通訊者在公開討論中誤以為錯誤率是由於通道上的雜訊干擾所造成的。在考慮雜訊干擾方面，由於實際網路環境中，通訊雙方執行量子通訊時必須透過光纖(optical fiber)傳輸。但在傳輸過程中，光纖的雙折射(birefringence)波動將導致集體雜訊(collective noise)產生，其中最主要的集體雜訊有集體相位衰退雜訊(collective-dephasing noise)與集體相位旋轉雜訊(collective-rotation noise)。因此如何在量子通道受到雜訊干擾下還能設計出安全的量子協定也成為近幾年熱門的議題。

(3) 量子網路

關於量子資訊與安全的研究，發展至今已經可以達成許多目標，像是金鑰分配、金鑰協定、秘密傳輸、...等。在大部分的條件下，這些量子資訊協定只需執行的雙方參與者就可以運作，但如果雙方位置距離非常遙遠、或面臨特殊需求時，往往無法以單純的雙方環境來進行通訊。然而，也許雙方之間可能會有多方需求、無法直接通訊、互相不信任，甚至是需要一個控制裁斷者等等的因素，使得協定需要依靠第三方(third party)或是伺服(Server)的輔助來完成，所以就產生量子網路的概念。目前普遍文獻對於量子網路的定義，只要協定裡有加入第三方，使得系統變成環環相扣的多方結構，就可稱之為量子網路。由於其易拓展性與廣闊的應用面，使得量子網路的研究探討將成為未來最新穎、且最具前瞻性的研究議題。

壹拾、結論

2013 年，D-wave 公司研發生產具有 512 量子位元的量子電腦，使得量子電腦不再是遙遠的夢想。然而量子電腦的實現也代表著現今的密碼系統面臨危機，透過量子演算法，現行電腦難以解開的數學難題將被破解，使得安全性基於數學難題的加密系統不再安全。面對量子電腦和量子演算法的挑戰，現行的安全加密系統，尤其是國防、銀行等資訊安全系統需提早防衛，才能保障量子電腦時代下的資訊安全。在量子電腦的時代中，若能掌握量子密碼的相關技術，就得以保障國安、財金資訊傳遞之安全性；而透過量子電腦的運算能力，也可以有效破解現行之加密系統。換句話說，對量子密碼技術掌握的程度，正意味著國家未來資訊安全的程度。

參考文獻

[1] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms in GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory,* vol. 24, pp. 106-110, 1978.

[2] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory,* vol. 36, pp. 553-558, 1990.

[3] O. Ore, "Invitation to Number Theory," *Washington, DC: The Mathematical Association of America,* 1967.

[4] W. Leveque, "Elementary Theory of Number," *New York: Dover,* 1990.

[5] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *35th Annual Symposium on the Foundations of Computer Science*, Los Alamitos, Calif., 1994, pp. 124-134.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Siam Journal on Computing,* vol. 26, pp. 1484-1509, Oct 1997.

[7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review,* vol. 41, pp. 303-332, Jun 1999.

[8] R. Jozsa, "Quantum factoring, discrete logarithms, and the hidden subgroup problem," *Computing in Science & Engineering,* vol. 3, pp. 34-43, Mar-Apr 2001.

[9] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Information & Computation,* vol. 3, pp. 317-344, Jul 2003.

[10] S. Boixo, T. Albash, F. M. Spedalieri, N. Chancellor, and D. A. Lidar, "Experimental signature of programmable quantum annealing," *Nature Communications,* vol. 4, p. 2067, 2013.

[11] G. Brassard and C. Crépeau, "Quantum Bit Commitment and Coin Tossing Protocols," presented at the Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, 1991.

[12] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties," in *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, 1993, pp. 362-371.

[13] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *Cambridge University Press,* 2000.

[14] K. Shimizu and N. Imoto, "Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty. II. Closing EPR-type loopholes," *Physical Review A,* vol. 67, p. 034301, 03/11/ 2003.

[15] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," *Nature,* vol. 299, pp. 802-803, 1982.

[16] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," presented at the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984.

[17] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science,* vol. 283, pp. 2050-2056, Mar 26 1999.

[18] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters,* vol. 85, pp. 441-444, 2000.

[19] H. K. Lo, "A simple proof of the unconditional security of quantum key distribution," *Journal of Physics A-Mathematical and General,* vol. 34, pp. 6957-6967, Sep 7 2001.

[20] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the Acm,* vol. 48, pp. 351-406, May 2001.

[21] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *Journal of Cryptology,* vol. 19, pp. 381-439, Oct 2006.

[22] H. Inamori, N. Lutkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *European Physical Journal D,* vol. 41, pp. 599-627, Mar 2007.

[23] Y. F. Chung, Z. Y. Wu, and T. S. Chen, "Unconditionally secure cryptosystems based on quantum cryptography," *Information Sciences,* vol. 178, pp. 2044-2058, Apr 15 2008.

[24] K. Tamaki and T. Tsurumaru, "Security Proof of Quantum Key Distribution," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences,* vol. E93A, pp. 880-888, May 2010.

[25] H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel," *Physical Review A,* vol. 84, Oct 31 2011.

[26] W. Diffie and M. E. Hellman, "NEW DIRECTIONS IN CRYPTOGRAPHY," *Ieee Transactions on Information Theory,* vol. 22, pp. 644-654, 1976.

[27] T. Hwang, C. W. Tsai, and S. K. Chong, "Probabilistic Quantum Key Distribution," *Quantum Information & Computation,* vol. 11, pp. 615-637, Jul 2011.

[28] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A,* vol. 59, pp. 1829-1834, Mar 1999.

[29] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," *Physical Review Letters,* vol. 89, p. 187902, 2002.

[30] F.-G. Deng, G. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A,* vol. 68, p. 042317, 2003.

[31] K. Shimizu and N. Imoto, "Communication channels secured from eavesdropping via transmission of photonic Bell states," *Physical Review A,* vol. 60, pp. 157-166, Jul 1999.

[32] B. A. Nguyen, "Quantum dialogue," *Physics Letters A,* vol. 328, pp. 6-10, Jul 19 2004.

[33] F. Gao, F. Guo, Q. Wen, and F. Zhu, "Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication," *Science in China Series G: Physics, Mechanics and Astronomy,* vol. 51, pp. 559-566, 2008.

[34] A. C. Yao, A. C. Yao, A. C. Yao, and A. C. Yao, "Protocols for secure computations," in *Foundations of Computer Science, 1982. SFCS '08. 23rd Annual Symposium on*, 1982, pp. 160-164.

[35] H.-K. Lo and H. F. Chau, "Is Quantum Bit Commitment Really Possible?," *Physical Review Letters,* vol. 78, pp. 3410-3413, 04/28/ 1997.

[36] R. L. Rivest, A. Shamir, and L. Adleman, "METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS," *Communications of the Acm,* vol. 21, pp. 120-126, 1978.

[37] S.-K. Chong, Y.-P. Luo, and T. Hwang, "On “Arbitrated quantum signature of classical messages against collective amplitude damping noise”," *Optics Communications,* vol. 284, pp. 893-895, 2/1/ 2011.

[38] M. Curty and N. Lütkenhaus, "Comment on “Arbitrated quantum-signature scheme”," *Physical Review A,* vol. 77, p. 046301, 04/30/ 2008.

[39] T. Hwang, S.-K. Chong, Y.-P. Luo, and T.-X. Wei, "New arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications,* vol. 284, pp. 3144-3148, 6/1/ 2011.

[40] T. Hwang, Y.-P. Luo, and S.-K. Chong, "Comment on “Security analysis and improvements of arbitrated quantum signature schemes”," *Physical Review A,* vol. 85, p. 056301, 05/24/ 2012.

[41] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, "Arbitrated quantum signature scheme with message recovery," *Physics Letters A,* vol. 321, pp. 295-300, 2/16/ 2004.

[42] Q. Li, W. H. Chan, and D.-Y. Long, "Arbitrated quantum signature scheme using Bell states," *Physical Review A,* vol. 79, p. 054307, 05/21/ 2009.

[43] Y.-P. Luo and T. Hwang, "Erratum “New arbitrated quantum signature of classical messages against collective amplitude damping noise” [Optics Communications 284 (2011) 3144]," *Optics Communications,* vol. 303, p. 73, 8/15/ 2013.

[44] Y.-P. Luo and T. Hwang, "Arbitrated quantum signature of classical messages without using authenticated classical channels," *Quantum Information Processing,* pp. 1-8, 2013/08/24 2013.

[45] Y.-G. Yang and Q.-Y. Wen, "Erratum: Arbitrated quantum signature of classical messages against collective amplitude damping noise (Opt. Commun. 283 (2010) 3198–3201)," *Optics Communications,* vol. 283, p. 3830, 10/1/ 2010.

[46] Y.-G. Yang and Q.-Y. Wen, "Arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications,* vol. 283, pp. 3198-3201, 8/15/ 2010.

[47] G. Zeng, "Reply to “Comment on ‘Arbitrated quantum-signature scheme’ ”," *Physical Review A,* vol. 78, p. 016301, 07/28/ 2008.

[48] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Physical Review A,* vol. 65, p. 042312, 04/01/ 2002.

[49] X. Zou and D. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes," *Physical Review A,* vol. 82, p. 042325, 10/21/ 2010.

[50] C. W. Yang, T. Hwang, and Y. P. Luo, "Enhancement on "quantum blind signature based on two-state vector formalism"," *Quantum Information Processing,* vol. 12, pp. 109-117, Jan 2013.

[51] Y. Tian, H. Chen, G. Yan, J. F. Tian, and X. J. Wen, "A proxy blind signature scheme based on quantum entanglement," *Optical and Quantum Electronics,* vol. 45, pp. 1297-1305, Dec 2013.

[52] Z. Kejia, S. Tingting, Z. Huijuan, and Z. Weiwei, "A secure quantum group signature scheme based on Bell states," *Physica Scripta,* vol. 87, pp. 045012 (5 pp.)-045012 (5 pp.), April 2013.

[53] C. W. Yang, T. Hwang, and T. H. Lin, "Modification Attack on QSDC with Authentication and the Improvement," *International Journal of Theoretical Physics,* vol. 52, pp. 2230-2234, Jul 2013.

[54] T. H. Lin, C. Y. Lin, and T. Hwang, "Man-in-the-Middle Attack on "Quantum Dialogue with Authentication Based on Bell States"," *International Journal of Theoretical Physics,* vol. 52, pp. 3199-3203, Sep 2013.

[55] T. H. Lin, C. W. Yang, and T. Hwang, "Attacks and Improvement on "Quantum Direct Communication with Mutual Authentication"," *International Journal of Theoretical Physics,* vol. 53, pp. 597-602, Feb 2014.

[56] C. Yang, C. Tsai, and T. Hwang, "Fault tolerant two-step quantum secure direct communication protocol against collective noises," *Science China Physics, Mechanics and Astronomy,* vol. 54, pp. 496-501, 2011/03/01 2011.

[57] J. Lin and T. Hwang, "Bell state entanglement swappings over collective noises and their applications on quantum cryptography," *Quantum Information Processing,* vol. 12, pp. 1089-1107, 2013/02/01 2013.

[58] C.-W. Yang and T. Hwang, "Quantum dialogue protocols immune to collective noise," *Quantum Information Processing,* vol. 12, pp. 2131-2142, 2013/06/01 2013.

[59] C.-W. Yang and T. Hwang, "Fault tolerant authenticated quantum direct communication immune to collective noises," *Quantum Information Processing,* vol. 12, pp. 3495-3509, 2013/11/01 2013.

[60] D. Leung, J. Oppenheim, and A. Winter, "Quantum Network Communication-The Butterfly and Beyond," *Ieee Transactions on Information Theory,* vol. 56, pp. 3478-3490, Jul 2010.

[61] M. Hayashi, "Prior entanglement between senders enables perfect quantum network coding with modification," *Physical Review A,* vol. 76, Oct 2007.

[62] S. Y. Ma, X. B. Chen, M. X. Luo, X. X. Niu, and Y. X. Yang, "Probabilistic quantum network coding of M-qudit states over the butterfly network," *Optics Communications,* vol. 283, pp. 497-501, Feb 2010.

[63] J. Dong and J. F. Teng, "Quantum key distribution protocol of mesh network structure based on n+1 EPR pairs," *Journal of Systems Engineering and Electronics,* vol. 21, pp. 334-338, Apr 2010.