量子技術於網際網路安全通信的應用

能源與環境研究所財團法人工業技術研究院退休研究員 / 呂錫民

關鍵字：量子金鑰分配、網際網路通信、量子理論安全

摘要

為了使大量敏感數據（例如，電子健康記錄，政府文件），在十年甚至若干世紀之後，仍能保持可存取性，網際網路（Internet）在進行此類數據通信時，需要長期安全通信通道，這又需要可靠的金鑰分配協定（Key Distribution Protocol, KDP）。但是，當前使用的KDP並非為長期安全而設計。它們的安全性不是受到量子計算機的威脅，就是在基本上對計算問題的依賴而受到威脅。量子金鑰分配（Quantum Key Distribution, QKD）協定在信息理論上是安全的（Information-theoretically Secure），因此可針對計算攻擊提供長期安全性。但是，在現實世界中使用仍然存有重大障礙。我們在計算機學家和物理學家的跨領域協助下，針對QKD長期安全網際網路通信的挑戰和策略，實現本研究論文對這些知識的系統化。首先，我們對現今所謂「點對點QKD」技術的性能和安全性進行分析。然後，我們討論在大型多用戶網路中啟用QKD的幾種方法。最後，我們列出若干重要挑戰，如果未來這些挑戰成功克服，則將使基於QKD網際網路的通信，達到長期安全且切實可行的境界。

一、引言

網際網路（Internet）可以說是當今最重要的通信媒介，它使全球任何兩個客戶端都可以立即相互通信。如果有敏感信息（例如病歷或政府文件）即將傳達，則需要建立安全連接，以保護所傳達數據的機密性、完整性和真實性。這樣的安全連接協定將金鑰分配協定（KDP）與通道協定結合在一起，其中一個較為顯著的例子是傳輸層安全性（Transport Layer Security, TLS）協定。首先，啟動金鑰分配協定以建立對竊聽通信的潛在竊聽者未知的公共秘密金鑰。然後，此金鑰在通道協定中用於加密和驗證傳輸的數據。

當今最常用的金鑰分配協定係以Diffie-Hellman金鑰交換協定為基礎，該協定提供

了所謂的計算安全性：該協定的安全性建立在離散對數（discrete logarithms）在大型有限領域中無法被有效計算。但是，量子計算機可以有效地計算出這樣的離散對數，因此，一旦量子計算機未來可用，Diffie-Hellman金鑰交換就變得不安全。近來，基於晶格密碼學（lattice-based cryptography）的替代金鑰分配協定已被提出，其被認為對量子計算機是安全的。但是，它們的安全性仍然取決於計算問題，只要有足夠的計算能力和時間就可以破解。因此，計算安全的金鑰分配協定僅在有限的時間段內實現安全性。一旦解決了計算問題，所有傳輸數據的機密性就會丟失。

計算安全金鑰分配的替代方案是信息理論安全（information-theoretically secure）金鑰分配。信息理論安全協定可以抵抗任何計算攻擊（譬如，來自量子計算的進步或蠻力攻擊），因此可以提供長期的安全性。提供長期機密性的連接需要理論安全金鑰分配和加密信息。然而，這種通道的完整性要求通常只是臨時性的（或者計算性的），也就是說，在傳輸數據時足以保證完整性。儘管在定義、理解和構建計算安全通道方面付出巨大努力，但如何構建信息理論安全的通道，從而實現機密性和完整性的雙重效果，以及重播（replay）和重新排序保護標準安全目標的全面了解目前仍然缺乏。對於信息理論加密，一次性填充加密（one-time pad encryption）是最佳解決方案。對於信息理論安全的金鑰分配，目前存在幾種候選方法。其中，較天真的方法是使用受信任的快遞員分配金鑰，該快遞員以物理交付存儲在硬碟上的已生成金鑰。但是，這種方法存在明顯的成本和延遲問題，因為它需要在全球範圍內移動的硬碟。用於信息理論安全金鑰分配的其他方法包括定義在有界存儲模型（bounded storage model）或雜訊通道模型（noisy channel model）中的協定。

然而，目前尚不清楚如何在實際上應用它們。當前，信息理論安全的金鑰分配最看好的方法是量子金鑰分配（QKD）。QKD的安全性是根據量子物理學定律為基礎，其可行性已在許多現場測試場合中獲得驗證。但是，要使QKD在網際網路通信上達到長期安全的切實可行地步，仍有一些技術上的難題需要解決。尤其是QKD在實際上的性能和安全性仍然是一個問號。此外，大多數QKD技術著重於兩方設置，但是未來還需要做更進一步的技術改良，以便能夠在大規模多用戶網路（例如，網際網路）中使用。

在本立場文件（position paper）中，我們對根據QKD的網際網路通信所需的構建模塊進行分類和比較。具體來說，我們將對現有技術的分析分為兩項步驟。

1. 首先，我們在兩方環境下檢查QKD協定。為此，我們按照功能、信息準備方法和信息載體所用變量的類型對「點對點QKD協定」進行分類。然後，我們從性能和安全性方面比較此類協定。

2. 其次，我們轉向大規模通信網路的問題。為了可擴展性，未來的網路運行不能依賴每兩方之間的專用通信通道。因此，支持根據QKD通信的大型網路需要集線器，即多鏈路節點。當前的集線器技術不支持

QKD。我們將現有的QKD支持方法分為兩類：受信任節點網路和全量子網路。然後比較兩種方法的實用性。

通過以上分析，我們得出實現大規模QKD網路所必須解決的關鍵性挑戰。

本立場文件的目的在於提供計算機科學家和物理學家都可以理解此一主題（即本質上跨領域）的概述。同時，我們另一目標在於，以計算機科學和物理兩面向來解讀該主題時，雙方都可達到類似的詳細程度。因此，我們最終目的在於提供一個易於相互溝通的概述管道，以促進跨學科之間的合作研究與開發。

本文其餘部分的結構如下。我們首先討論兩方QKD技術在性能和安全性面向上的現狀（第貳章）。然後，我們討論在大規模多用戶網路中啟用QKD的幾種方法（第參章）。最後，我們總結經過研究分析之後的發現，並且討論當前的標準化和部署工作，同時列出在網際網路上基於QKD的長期安全通信時，所面臨實際上需要解決的挑戰（第肆章）。

二、兩方之間的 QKD

在本章中，我們將描述點對點QKD技術的最新發展。我們首先解釋量子物理學的相關概念。然後，我們對主要的QKD協定進行分類和總結。接下來，我們比較協定的性能，並討論安全性模型以及對協定上所實施的攻擊。

（一）量子物理學

QKD協定背景係建立在量子物理學中的兩個基本定律之上：1. 量子物件在測量後的典型狀態變化，即波函數崩潰；以及，2. 不可能在不干擾原始粒子狀態的情況下複製量子狀態，即無克隆定理。QKD協定的安全性取決於這樣一個事實，即潛在的竊聽者通過其攻擊過程來揭示自己。竊聽會給交換量子狀態帶來不可避免的錯誤，這些錯誤隨後可以由通信方檢測到。每個QKD協定的核心都在於量子狀態的交換。在現代的光通信系統中，在一定的時間間隔內，典型位元（bits）被編碼成不存在（0）或存在（1）的「經典」雷射脈衝。但是，QKD使用量子位元（qubits），也就是一次能夠攜帶不止一個經典位元信息的量子物件，因此表現出古典物理學無法描述的行為。

基本上，完全不同的物理系統可以作為量子位元：例如，單光子、弱雷射脈衝、福克態（Fock state）和光壓縮態、半自旋量子系統（當作捕獲原子和離子）、或腔耦合里德堡原子（Rydberg atom）。量子信息可以使用不同類型可觀測值（即量子位的物理可測量屬性）來被編碼。也就是說，信息可以使用下列量測物理屬性來編碼，例如極化、相位、單光子的創建時間、或者多光子同調雷射態的正交、相位和幅度。

（二）共同功能

現在，我們將概述隨後討論到的所有QKD協定的共同功能。這些協定包含原始金鑰分配階段和後處理階段。

1. 原始金鑰分配

每個QKD協定運作的第一個步驟，是利用特殊量子通道來傳輸qubit，以便建立原始金鑰。理想地，由於量子位元與傳輸介質的相互作用（例如，玻璃纖維中的極化改變），這種通道不應改變編碼信息。為了成功分配金鑰，失真或扭曲必須保持低階水平，因為量子位元狀態的干擾也可能是由攻擊者所造成。

在原始金鑰分配階段，通信夥伴通過量子通道來交換量子位元。一旦接收到量子位元，接收者就對可觀察到的量子位元進行測量，並根據選取QKD協定的確定過程，從其接收結果中解碼出典型位元。之後，通信夥伴使用典型鑑定管道來諮商他們的測量。此一過程在每個QKD協定都是特定的，最後得出的結果就是原始金鑰。如果他們推斷出攻擊者可能嚴重干擾了量子信息，則必須重新開始金鑰分配程序。

2. 後處理

在原始金鑰分配階段之後，每個通信夥伴都獲得一個單獨原始金鑰。由於實驗的不完美，具備完全相關性的金鑰是不可能的，因此糾錯編碼（例如，低密度同位元檢查、串接（cascade）或極性（polar）等編碼）必須執行。之後，隱私放大程式被應用，以便從糾錯後的原始金鑰生成最終金鑰。在原始金鑰交換或錯誤校正過程中，即使無法完全防範竊聽者看到少量位元，但這仍可確保安全性。最後，將生成的秘密金鑰用作一次性密碼或高級加密標準（Advanced Encryption Standard, AES）加密的金鑰。

如上所述，QKD需要在通信夥伴之間進行身份驗證的經典通道。這樣的認證通道可以使用簡短的共享密碼或典型的安全連接（例如，傳輸線系統（Transmission Line System, TLS）來建立。最近，基於量子物理學定律實現認證通道方法已被提出。我們認為，在QKD協定執行時，只有使用已驗證通道，才能保持QKD協定的安全。

（三）協定家族

實現QKD協定的方式有很多種。為了方便分析，我們以信息製備（製備和測量或基於糾纏）的方式和變量（離散變量、連續變量或分佈式相位參考）的類型對它們進行分類。

1. 按信息製備方法的分類

我們根據量子態製備方法來描述QKD協定的類別。

(1) 製備和測量：在製備和測量（Prepare-and-Measure, PaM）協定（圖1a）中，發送方“Alice”主動製備信息載體，並對其內信息進行編碼，然後將其發送給一個或多個接收者。該類協定的傑出代表作是由Bennett和Brassard所開發的協定（BB84）或延生的協定。

(2) 基於糾纏：在基於糾纏（Entanglement-based, EB）的協定中（圖1b），「源」產生糾纏粒子—多個量子物件，它們可以違反局部現實的相關量子態來描述。根據量子力學糾纏理論：對一個物件的某些可觀察到的測量會立即影響另一個物件的狀態。其後，糾纏粒子狀態被通信對方測量。在此類通信過程中，為了驗證接收到的粒子的糾纏，並進行竊聽檢測，於是施行貝爾測試（Bell test）。如圖1（b）所示，通過粒子之間的非經典相關性，可以確保「愛麗絲」和「鮑

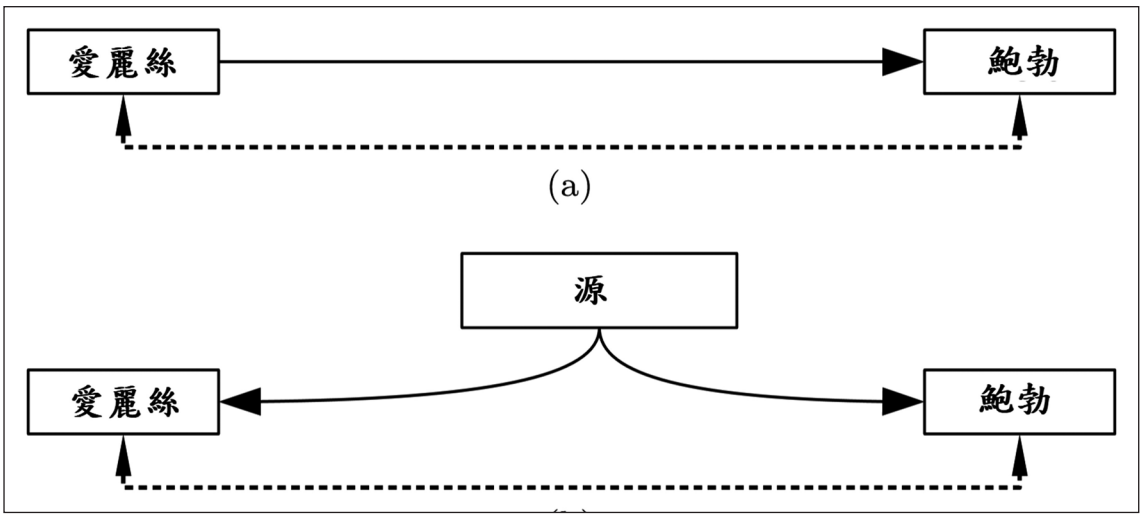

圖 1　（a）製備和測量協定（例如 BB84），（b）基於糾纏的協定（例如 E91）。實線表示量子通道，虛線表示已認證的經典通道。箭頭表示信息流動的方向。

勃」無需直接交換信息即可擁有一個共同秘密。該類協定的傑出代表作是Ekert所開發的E91協定。

2. 按變量種類分類

QKD協定也可以按照信息載體的變量種類來進行分類。

(1) 離散變量（DV）

對於具有離散變量（Discrete Variable, VD）的協定，其中所攜帶可觀察信息值是離散的。最常見的是，單光子或弱雷射脈衝被用來傳輸量子位元。原則上，半自旋粒子（例如電子）也可以使用，但是這種粒子的傳輸有問題。該信息可以在時間、極化、自旋、相位中編碼。源可以PaM系統或基於糾纏系統來實現。DV協定需要昂貴且效率低的單光子源和檢測設備。

(2) 連續變量（CV）

連續變量（Continuous Variable, CV）協定是DV協定的替代方案，該協定使用許多粒子狀態（例如，光的壓縮狀態或相關狀態）來代替量子位元（例如，單光子和弱雷射脈衝）。因此，其中沒有檢測到離散變量（例如，0和1），但是光正交分量的連續光譜被觀察到（例如，通過同差技術（homodyne technique）。CV協定中檢測的量子狀態也不同於DV協定。在此，針對量子通信的標準組件被使用。例如，採用同差或外差檢測方案。這比檢測單光子要快得多，效率也更高。大多數現有的CV協定都可以當作PaM變體或EB變體來實施。

(3) 分佈式相位參考（DPR）

QKD協定的第三系列，稱為分佈式相位參考（Distributed Phase Reference, DPR）協定，其使用離散變量進行信息編碼，但同時也觀察後續脈衝的相關性

來確保安全。其中，位元可以按脈衝對的順序或後續脈衝的相位編碼。兩種方法也可以組合成二維QKD協定，其中幾個位元可以兩個後續脈衝編碼。DPR協定需要與DV協定類似的設備，即單光子源和檢測器。

（四）運行和績效

前述QKD協定可以在自由空間上或玻璃纖維中運行。不同秘密金鑰生成速率和有效距離可以獲得，這理論上取決於通信介質的種類。DV協定典型金鑰在幾十公里距離內的最高速率為幾kbit s^{-1}，而在大約100 km距離內的最高速率為若干bit s^{-1}（參見表1）。CV協定金鑰速率（key rate）與DV協定不相上下，其在幾公里通道和最大150 km有效距離內的數值高達10 kbit s^{-1}。在表1中，我們列出基於光纖的QKD技術的性能指標。對於所有QKD協定，由於量子通道中的雜訊和損耗，金鑰速率隨著通信距離增加而呈指數下降。研究結果顯示，QKD最大可達金鑰速率取決於通道損耗的函數限制，後者是唯一僅有的影響參數。另一方面，在自由空間的QKD系統可以達到更遠的距離，這是因為空氣的衰減係數遠小於光纖。最近，基於衛星的QKD技術已達歷史里程碑。在2017年，通過衛星以DV為基礎的量子金鑰分配已經在1200 km的距離上以1 kbit s^{-1}的金鑰速率進行演練。在2018年，在奧地利格拉茨和中國上海之間，通過衛星的洲際QKD也進行同樣演練。由此，專家發現標準電信衛星能夠實現基於CV的QKD協定。

除了金鑰速率和距離的因素之外，系統與現有通信基礎結構的兼容性也很重要。例如，DV QKD協定需要昂貴的單光子檢測器、單光子或糾纏光子源以及精確的時間測量設備。同時，金鑰分配的典型分配距離和速率僅允許在都會網路區域內使用。單光子源的缺陷使光子數分裂攻擊成為可能（請參閱第2.5節）。

另一類更新的協定是CV協定，由於不需要單光子源或單光子檢測器，因此它可以提供更高的秘密金鑰速率和更低的實現成本，

表 1　點對點 QKD 技術的性能比較

實驗	類型	100 公里處的鍵速	最大距離
Boaron [1]	PaM-DPR	14 kbit s^{-1}	421 km
Yin [2]	EB-DV	2 kbit s^{-1}	404 km
Korzh [3]	PaM-DPR	10 kbit s^{-1}	307 km
Wang [4]	PaM-DPR	20 kbit s^{-1}	260 km
Stucki [5]	PaM-DPR	6 kbit s^{-1}	250 km
Grünenfelder [6]	PaM-DV	50 kbit s^{-1}	200 km
Huang [7]	PaM-CV	500 bit s^{-1}	100 km
Honjo [8]	EB-DV	0.59 bit s^{-1}	100 km
Jouguet [9]	EB-CV	200 bit s^{-1}（80 km）	80 km

表 2　QKD 協定系列的定性比較

	部署	鍵速	距離	成本效益
DV	+	+	+	+
CV	+	++	+	++
DPR	++	++	++	+

並且可以使用光通信的標準組件。最近的一項實驗證實，即使在相對靜止衛星，CV協定也可以應用標準光通信，從而實現更長的通信距離。但是，相對於DV協定（參見第2.5節），CV協定對旁通道攻擊的安全性防護較少。

DPR協定目前在最大金鑰分配距離方面可達到最佳性能（表1）。此外，像DPR協定一樣，多維QKD方案允許在單個qubit中傳輸多於一位元的經典信息。

針對所有協定類型，專家正在研究如何將量子通道和經典通道一體成型到單個玻璃纖維當中。因為，在如此設置下，量子位元與經典通信脈衝可以不同波長同時傳輸，以避免串擾（cross-talk），從而降低QKD部署成本。表2總結不同QKD協定系列的觀察結果。

（五）安全性

如果在協定執行後，通信夥伴「愛麗絲」和「鮑勃」知道一個公用金鑰，並且如果通道上的竊聽者「夏娃」無法獲得有關該金鑰的任何信息，則雙方可以認定該QKD協定是安全的。現在，我們總結有關分析QKD協定安全性的研究，並討論QKD實行時所遭遇的理論和實際攻擊。

1. 理論分析

在分析QKD協定安全性時，我們目標在於證明對抗可能擁有完善技術的強大攻擊者「夏娃」的絕對安全性。例如，夏娃可能能夠在任意持續時間內提取和存儲量子位元，並對它們執行任何量子運算或測量。然而，根據基本量子物理定律，由於非克隆定理，「夏娃」既不能完美地克隆也不能完美地測量系統的狀態並重新發送新粒子而不會留下痕跡。此外，我們通常假定在通信夥伴之間存在需要身份驗證的經典通道或較短的預共享金鑰。這些是保證數據完整性和真實性所必需的，因此「夏娃」不能執行模擬攻擊或更改發送的經典數據。我們強調，身份驗證通道不需要提供任何機密性保證。

如果「夏娃」分別測量每個量子位元，則這將是對QKD系統的個體攻擊。在集體攻擊中，「夏娃」仍然與每個量子位分別互動，但是她可以整體性地測量所有用於互動的輔助系統。如果允許「夏娃」同時攻擊幾個發送量子位元，則該攻擊稱為相關攻擊（coherent attack）。Renner等[10]證明各種QKD協定針對相關攻擊的安全性。

QKD安全保證建立在信息理論（information theory）之上，而非取決於計算難度設定。與當前使用的金鑰分配方法相比，這種基本上差異保證QKD的長期安全性。但是，在QKD安全保證中的理想化假設會導

致不完整的安全性模型。為了獲得有關施行上的實際安全保證，我們需要更多有關硬體和軟體的設定。如下所述，藉由不完善的設備和不安全的軟體進行攻擊是可能的。隨著各種協定的不同，對抗理論攻擊的安全保證也有所不同。儘管某些DV協定已被證明是無條件安全的[11, 12]，但CV和DPR協定的類似證據仍然缺乏。Diamanti，Kogias，Laudenbach等[13-15]概述有關CV協定的安全保證。Moroder等[16]則提供DPR協定的安全分析。

作為範例，我們討論BB84對抗攔截重發（intercept-resend）攻擊的安全性，這是一個體攻擊案例。在此攻擊中，「夏娃」隨機選擇一個基底（basis）並檢測粒子狀態。她有50%的可能性選擇了錯誤的基底。之後，針對檢測量子位元，她製備替換品，並發送給「鮑勃」。這樣，她在「鮑勃」金鑰匙引發25%的QBER（Quantum Bit Error Rate）。但是，Shor和Preskill研究結果證明，如果QBER超過11%，則「愛麗絲」和「鮑勃」將知道金鑰分配已受到損害。在其他策略中，例如，使用不是根據每個量子位元或中間基底的檢測，則對「夏娃」不利，因為她獲得較少金鑰信息。在基於糾纏協定的情況下，在量子位元測量過程中，「夏娃」破壞粒子之間的非經典相關性，造成在金鑰處理過程中Bell測試的失敗。總而言之，針對QKD協定的安全性保證，專家證明如果攻擊者試圖竊聽網路發送的量子狀態，則會暴露自己。與傳統的金鑰分配相比，這就是為什麼QKD會如此強大的原因。

2. 實施時的攻擊

即使是證明為無條件安全的協定，旁通道和不完善設置也可能導致漏洞。因此，實施QKD協定需要擴展到周邊環境的安全性分析。特別需要考量的是，旁通道的脆弱性和設置的不完美，最有可能必須採取的措施是安全性證明。

舉例來說，建立客製化單光子數並不繁瑣。在大多數情況下，脈衝內具有1個以上的光子是很有可能的。因此，如果弱雷射脈衝有多個光子，「夏娃」可用分束器（beam splitter）拾取若干光子，以獲得信息而不被注意。這類攻擊稱為光子數分裂攻擊。作為對策，專家修改協定，例如，添加誘餌狀態（decoy state）到BB84，並開發新協定，例如，SARG04。

利用特洛伊木馬攻擊可以劫持量子通道，因此，有關「愛麗絲」和「鮑勃」設置的信息可被提取，甚至可被操縱。例如，如果「夏娃」實時獲得有關「愛麗絲」選擇基底的信息，那麼她就可以進行成功的攔截-重發攻擊，因為她不再局限於隨機猜測基底。

另一種可能性是「鮑勃」檢測器通過量子通道所產生的明亮照明，使得攻擊者得以控制「鮑勃」的測量結果。Lydersen等[17]描述攻擊者如何成功獲取完整金鑰並且不被注意的細節。

至關重要的是，所有這些攻擊都必須在物理上和實際的金鑰分配過程中進行，這是QKD協定與經典金鑰分配協定的根本上差別，傳統金鑰分配協定的安全性可能會因分配時的未知攻擊而被破壞。

3. 與設備無關的QKD

與設備無關（device-independent）的QKD是一種方法，旨在擺脫對自己設置硬體信任的假設。因此，基本上應該通過類似於

E91協定的量子相關測試（即Bell測試）來評估整個QKD系統的安全性。由於我們很難實現純粹與設備無關的協定，因此專家已經開發了與測量設備無關的QKD協定。

三、大型網路中的 QKD

到目前為止，我們已經討論了QKD技術，該技術使用環境為，在短距離內通過專用量子通道直接連接兩方通信。然而，在大規模通信網路（例如，網際網路）中，任何兩個參與者之間通常不存在專用通信通道。此外，通信夥伴之間的物理距離可能很大，而且通常需要低延遲和高吞吐量功能。在網際網路上，業者通常使用網路集線器（network hub）來解決任何兩方皆能相互連接和通信的問題（圖2）。為此，業者通常使用諸如邊界閘道協定（Border Gateway Protocol, BGP）之類的路由協定。但是，當前集線器的體系結構和協定並不支持QKD，因此，其需要新技術以便在大規模網路中實現QKD。這涉及QKD集線器的體系結構和相應路由協定的開發。另外，QKD體系結構與應用程序層之間介面也需要定義。

在下文中，我們討論實現QKD網路的不同方法，並將它們相互比較。QKD集線器可以使用標準電信技術來實現，例如，波分-或時分-多工傳輸，或有緣光開關（active optical switching）。然而，如第貳章所述，這些方法不能克服QKD中的距離限制。但是，只有中繼器（repeater）可擴展QKD連接的有效範圍。目前有兩種中繼器正在開發：信任中繼器（trusted repeater）和量子中繼器（quantum repeater），它們支持兩種根本不同類型的QKD網路：信任節點網路和全量

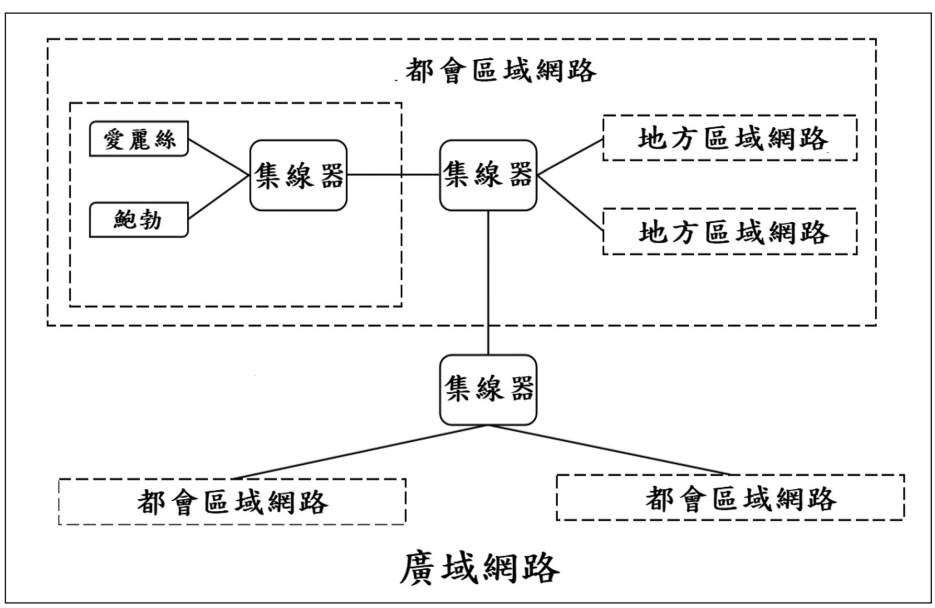

圖 2　通過集線器連接的網際網路的各個網路層

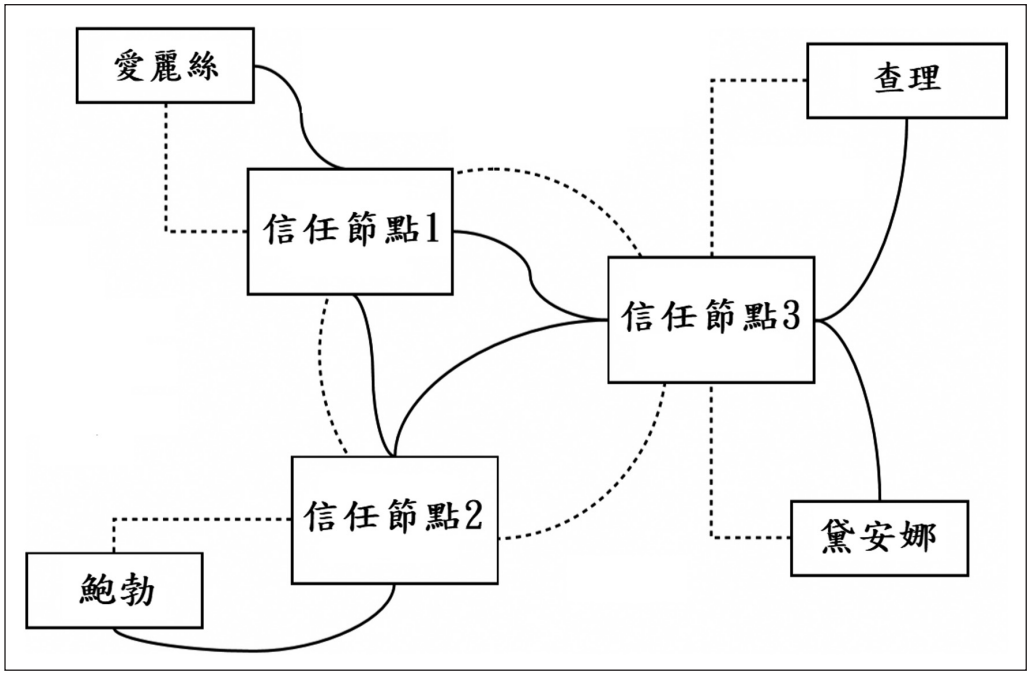

圖 3　與信任節點的 QKD 網路鏈接的方案。實線是量子通道，虛線表示經典通道。

子網路。

（一）信任節點網路

信任節點（trusted node）方法需要一連串的中繼器，該中繼器藉兩方QKD系統相互連接，並且一步接一步，將金鑰彼此中繼。因此，每個中繼器都知道金鑰，所以節點必須是安全且可信賴。這種方法已經研究十年。突出的例子包括SECOQC網路，東京QKD網路。

信任節點網路技術已經跨出研發階段，目前處於商業成功門檻。在中國，一條長2000公里連接北京到濟南、合肥和上海的線路已於2017年完成。電信運營商SK Telecom正在韓國實施基於信任節點的網路，計劃完成日期為2020年。

詳細說明信任節點網路的運作步驟如下。每個通信夥伴「愛麗絲」和「鮑勃」連接到附近的信任節點，該處的多個信任節點也相互連接（圖3）。為了使「愛麗絲」和「鮑勃」之間建立安全連接，業者使用路由和負載平衡協定，穿過信任節點網路層，建立彼此之間的安全路徑。然後，他們與各自的信任節點交換金鑰，不同信任節點還彼此交換金鑰。最後，從通信路徑生成的金鑰材料中，通信夥伴衍生出秘密金鑰。路由建立和金鑰衍生過程可由額外網路層和所謂金鑰管理服務來執行，這些服務獨立執行金鑰生成，並將最終秘密金鑰移交給客戶。

基於信任節點的網路克服了當前QKD技術的典型距離限制，並允許通過網路輕鬆靈活地進行通信路徑路由。假設有足夠多的信任節點，則金鑰可以中繼幾次，並且QKD距離限制僅針對每個金鑰中繼單獨考慮。此外，在一條通信路徑中可以使用不同類型的QKD協定。另外，大量工作已經致力於開發必要的路由協定和應用介面。基於信任節點的集線器的主要缺點在於，它們不提供嚴格的端到端安全性。實際上，量子狀態在每個集線器中都被破壞，並且信任中繼節點無法確保傳輸數據的機密性。但是，既使在某些節點有損壞的情況下，基於信任節點的網路仍然可以確保安全性。

（二）全量子網路

基於量子集線器和中繼器的全量子網路（all-quantum network），可在兩個遙遠的各方之間分配量子信息，從而實現真正端到端的安全性。從「愛麗絲」到「鮑勃」，量子信息載體分配糾纏給通信方。這種沒有任何失真或檢測的通信是透過傳輸光子來實現，例如它們之間的光-電-光轉換。因此，要達成高安全性的目標很難。其中網路協定必須謹慎選擇，因為它必須在整個網路實施，這對金鑰分配性能具有決定性的影響。該網路協定應該對所有已知的攻擊類型和稀疏的旁通道提供最佳安全性，同時也應具有成本效益和可擴展性等諸特徵。

在具有不同拓撲結構和使用不同QKD協定的都會區域網路（metropolitan area network）中，許多實驗已經證明全量子網路的可行性，例如：

- 圓形網路：因為光子僅注入網路中的一個位置，在所有參與者共享同一量子通道的情況下，因此減少雙方之間的有效距離，進而使得應用在大多數現實世界中的設置變得不那麼有趣。

- 具有PaM的星形網路：首先，每個通信者都配有量子狀態源和量子狀態檢測器等設備。然後，通過位於網路中心的量子路由器來實現量子粒子分配，並使用一種滿足量子態無失真要求的標準電信技術，例如，有源光開關或時分多工傳輸。在交換量子位元之後，建立的安全金鑰與兩方傳輸情況相同。然而，網路的可擴展性受到量子路由器可以處理通道數的限制。此外，該系統的成本很高，因為每個新接收者都必須建立源設備和檢測器。

- 帶有EB的星形網路：此方法的工作原理與典型基於兩方糾纏的QKD協定相似，但涉及的通信方數目擴展到兩個以上（圖4）。該方案具有挑戰性的部分是設計一個糾纏對源，即一個量子集線器，它建立與這些技術兼容的量子位元，並包含用於路由的所需硬體。與先前描述的網路設計相比，其中一個好處是每個接收者僅需要一個量子狀態檢測器，而無需量子狀態源。另外，由於源位於中央，所以通信雙方之間的有效距離更高。一些實驗已經證實在電信波長下通過波分多工（wave length division multiplexing）在玻璃纖維中進行糾纏分配的可行性，並且這種量子中心源的第一個實現已經完成。但是，這些設備的性能必須提高，並且需要在更大的現場測試中進行評估。這種量子集線器協定具

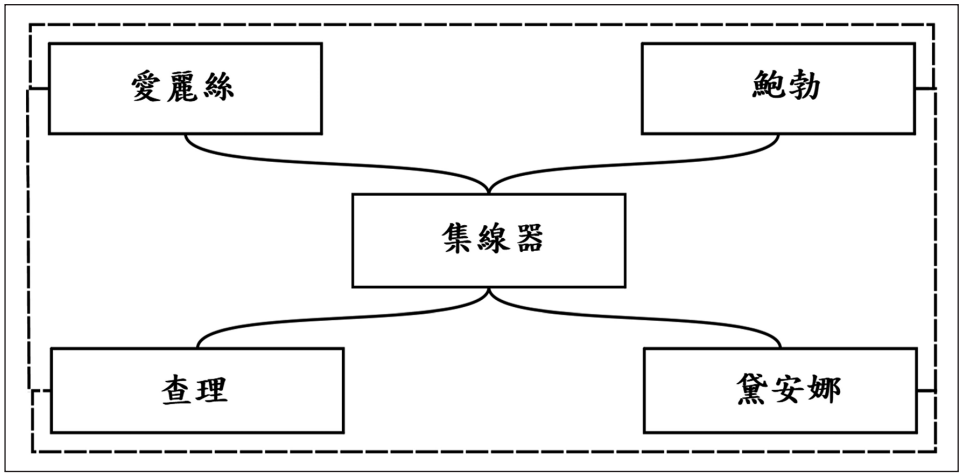

圖 4　星形 QKD 網路的方案。實線是量子通道，虛線是經典通道。

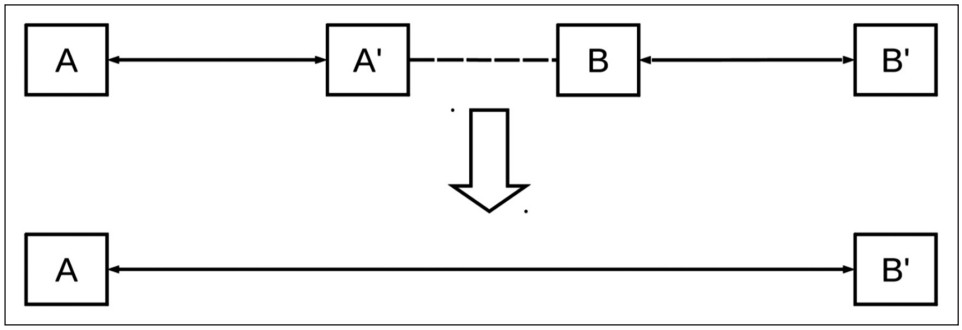

圖 5　量子中繼器的示意圖結構

有與典型上基於糾纏協定相同的優點和缺點。它們允許端到端安全金鑰的交換，但可達到的距離僅有幾十公里，如果沒有諸如量子中繼器之類的附加設備。主動或被動路由的方法也限制了連接接收者的最大數量，從而將這種設備限制在都會區域網路中。

（三）克服距離限制

如上所述，為了克服距離限制，專家已經提出量子中繼器，將糾纏粒子以更長的距離分配，如圖5所示。首先，將所需距離劃分為較短間隔。然後，在每個間隔中，建立糾纏粒子A-A'和B-B'，以標準方式共享糾纏，並將它們分配到間隔末端，其中光子A'和B共同測量，例如使用貝爾測量。該測量的一些經典信息分配給剩餘一對粒子A和B'，使得它們之間的纏結得以建立。此過程稱為糾纏交換。由於時間是此過程的關鍵因素，因此光子必須存儲在量子存儲器（quantum memory），在該存儲器中，量子信息可以保

留一定的時間，並且可以根據需要以高度保真進行檢索。所需時間的最高容量從幾微秒到幾秒不等。因此，存儲時間應要足夠長，才方便與最近節點進行粒子交換、糾纏交換、以及存儲和檢索存儲器中的量子位元。而且，應該提供對存儲在量子存儲器中的每個單一粒子的存取功能。另外，同時存儲多少粒子取決於所使用QKD協定的類型，數目範圍從一千到幾千。當前量子存儲技術允許同時存儲665個光量子狀態，最長存儲時間可達50 μs，而單個光子則最多可存儲幾個小時。為了讓QKD網路獲得更高的吞吐量，這些數量和時間還需要改善。

由於量子態的去相干（decoherence），以及其他量子雜訊，量子中繼器對通信通道引入額外雜訊。因此，量子和經典糾錯算法正在開發，從而開拓更廣的研究領域。如前所述，針對兩方通信系統，金鑰速率存在上限，該上限是通道雜訊的函數。這個基本限制也適用於全量子網路。針對具有量子中繼器鏈的網路，這些限制已在[18-19]研究。因此，中繼器鏈內的錯誤傳播也被考慮進來，這顯示這種網路的可行性。

結合量子集線器和量子中繼器，不僅可以解決距離限制問題，而且可以解決僅支持少量客戶端問題。接收器內的糾纏透過不同集線器交換（見圖6），在任意距離之下，我們可以建立擴展性全量子網路。量子中繼器的整合設置尚未完成，儘管已有不同財團和歐盟支持。

（四）路由

由於邏輯信息流與物理粒子分配的不平行，穿過全量子網路的信息路由非常複雜。在圖6示例中，我們可以使用不同方式來分

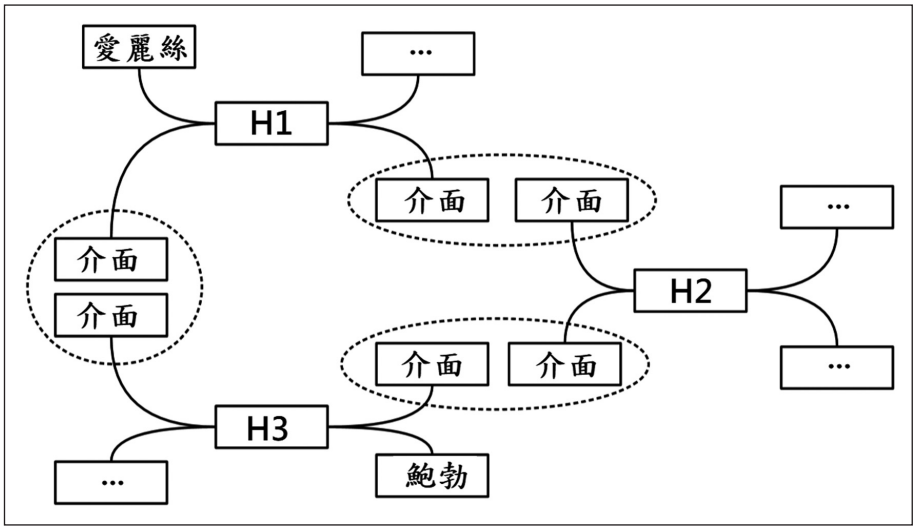

圖 6　全量子網路的示意圖結構。圓圈表示糾纏交換設備與不同集線器之間介面內的量子存儲器結合在一起。經典頻道未顯示。

表 3　信任節點網路和全量子網路之間的比較

	部署狀態	性能	距離靈活性	協定靈活性	成本效益	安全性
信任節點網路	+	+	+	+	+	-
全量子網路	-	-	-	-	-	+

註：在所有面向當中，除了安全性之外，信任節點網路皆優於全量子網路。

配「愛麗絲」和「鮑勃」之間的糾纏粒子。雖然集線器H1和H3之間的直接路徑可以進行一次交換，但是跨越集線器H1、H2和H3的其它路徑應該可以提供更高的傳輸速率，因為那些集線器彼此可能更為靠近。因此，我們需要BGP量子類比，以建立「愛麗絲」和「鮑勃」之間快速的金鑰交換和連接。這需要找到最佳的分配路徑，並且，在最終通信方之間，對量子中心和量子中繼器的分配和時序進行管理。然而，這樣的協定目前尚未開發。

（五）安全性

結合已開發QKD協定與量子中繼器，需要對此類網路進行複雜的安全性分析。在這方面，Rass等[20]開發一個用於量子網路中路由優化的框架，該框架允許找到最安全的網路路由。此外，Lee等[21]最近證實，在多節點網路中存在貝爾不等式，從此實現設備獨立安全性。與兩方系統及經典優化問題一樣，整體性能和安全性也要考慮在內，多節點網路系統的安全性是由量子物件的非局部相關性來確保。但是，最佳拓撲仍然取決於量子中繼器的潛力。

四、結論與展望

最後，我們討論信任節點和全量子網路的當前狀態，然後得出在大規模網路中實現QKD所面臨的開放性挑戰。

（一）現狀討論

在表3中，我們可以找到信任節點網路和全量子網路的比較。接下來，我們將詳細討論比較的標準。

部署狀態：在實際部署中，基於信任節點的網路已不再處於研究階段，而是處於商業成功邊緣。目前，所有關鍵硬體問題已經解決，並且成本優化和關鍵管理層逐漸步入實施階段。因此，未來迫切需要將信任節點最大程度整合到經典網路系統，並建立綜合整體網路的最佳路由。至於有關全量子網路，由於需要客製化設備，因此在未來十到二十年內，不太可能實現迅速的商業化。

性能：基本上，信任節點網路的性能取決於可用的最佳兩方QKD協定。另一方面，全量子網路的性能取決於諸如量子存儲器和量子中繼器之類的附加技術性能，因此，整體性能可能比預期更低，但是，由這些附加技術導致的確切性能損失尚未得到量化。

距離靈活性：信任節點方法主要優點在於，儘管以額外信任設定為代價，但QKD技術固有距離限制可以輕鬆克服。至於全量子

網路，克服距離限制仍是一大挑戰，它需要安裝量子路由器和量子存儲器（第3.2節）。而且，最近實驗結果顯示，即使折衷性方案使用量子中繼器，全量子網路也無法克服某些基本上的速率損失。

協定靈活性：至於協定選擇的靈活性，在信任節點方法中，同一網路中任何供應商的任何類型QKD協定和硬體允許混合使用。但是在全量子網路設計中，整個網路中的各個硬體組件必須彼此相互兼容。

成本效益：成本效益問題與先前討論的比較標準相關。由於構建量子集線器和中繼器需要量身訂製設置元件，因此導致全量子網路的設備昂貴。相反，信任節點網路的協定靈活性可降低成本。

安全性：信任節點網路的主要缺點在於，惟有中繼節點完全受信任時，傳輸數據的機密性才能被保證，因此，如果骨幹網路是由單一公司或政府控制，而它們同時也是該網路的主要用戶，則該方法就足夠安全。另一方面，全量子網路的主要優點在於，它們不需要上述前提條件，經由量子物理學定律和相應QKD設備的正確實施，它的信息傳輸安全性就可保證。

（二）標準化與部署

標準化和部署是QKD技術從研究過渡到實踐的兩項重要因素。在下文中，我們總結在這方面的過去及現在的工作努力。

首先，我們說明正在進行的QKD組件標準化活動。從2010年以來，ETSI（European Telecommunication Standard Institution）在QKD行業規範小組內持續實施激烈運作。特別是，ETSI最近發布一份有關量子密碼學實施安全性白皮書。ETSI規定面向包括：光學組件表徵、應用程序介面和金鑰傳遞API（application programming interface）。最近，ITU-T（國際電信聯盟電信標準化部門（International Telecommunications Union-Telecommunication Standardization Sector））第17研究組也開始進行標準化工作，除了QKD之外，重點項目包括量子隨機數發生器（quantum random number generator）。此外，最近在IETF（Internet Engineering Task Force）上，一個量子網際網路提議的研究小組被提出，但是，該小組的目前工作進度到僅止於早期草案的研議。

各種致力於QKD系統的部署已經實施，而目前也正在進行。在2000年代初期，先進國家和主要研究機構開始研究計畫，以部署原型QKD網路。最近，在東京QKD網路中，基於QKD的長期安全存儲系統的可行性已被證實。在商業領域中，一些公司正在開發和銷售QKD設備。特別是，若干重要電信公司最近開始投資QKD技術，同時也努力部署原型QKD系統。

（三）挑戰與展望

網際網路上的長期安全通信一直是人們企盼的目標，而當前QKD是實現此目標的最有希望候選技術。然而，大規模多用戶網路實現QKD，仍有若干技術挑戰存在。總而言之，我們展望未來列出以下重要挑戰：

- 候選QKD協定需要早日擬定，讓安全網路通信免於理論和實施攻擊。
- QKD協定的數據速率需要進一步提升，以便實現與傳統通信同等的數據速率。
- 安全連接協定（例如TLS）需要重新設計，以支持基於QKD的信息，從理論上來講，這就是安全的金鑰分配。
- 通信專家建議的實現量子中心方法必須實施，並且必須要有實用性證明。
- 量子中繼器的實用性需要在現實世界中加以展示，且它們如何與量子集線器結合必須驗證。至於量子中繼器所需的量子存儲技術，亦即，最大存儲能力和最大可能存儲時間都必須增加。
- 相關於全量子網路，具有高效路由的BGP量子類比必須開發。

除了這些挑戰之外，我們還希望有更多良好機會被創造。由於全量子網路在任何兩個節點之間分配了糾纏（即量子信息），因此除了網際網利通信的金鑰分配功能之外，它們尚可應用在其他項目。量子網際網路聯盟（Quantum Internet Alliance）規劃在2020年以前建立連接量子計算機的多節點全量子網路，因此屆時，有效且安全的聯合計算能力將被整體提升。

參考文獻

1. Boaron, A., et al.: Secure quantum key distribution over 421 km of optical fiber. Phys.Rev. Lett. 121 190502, 2018.
2. Yin, H.L.,et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. 117 190501, 2016.
3. Korzh, B., et al.: Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics 9 (3), 163-168, 2015.
4. Wang, S., et al.: 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Optics letters 37(6), 1008–1010, 2012.
5. Stucki, D.,et al.: Highrate, long-distance quantum key distribution over 250 km of ultralow loss fibres. New Journal of Physics 11(7), 075003, 2009.
6. Grünenfelder, F., Boaron, A., Rusca, D., Martin, A., Zbinden, H.: Simple and high-speed polarization-based QKD. Applied Physics Letters 112(5), 051108, 2018.
7. Huang, D., Huang, P., Lin, D., Zeng, G.: Long-distance continuous-variable quantum key distribution by controlling excess noise. Scientific reports 6, 2016.
8. Honjo, T., et al.: Long-distance entanglement-based quantum key distribution over optical fiber. Opt. Express 16(23), 19118-19126, 2008.
9. Jouguet, P., et al.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photonics 7(5), 378-381, 2013.
10. Renner, R., Gisin, N., Kraus, B.: Information-theoretic security proof for quantum-key-distribution protocols. Physical Review A72(1), 012332, 2005.
11. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distributionoverarbitrarilylongdistances. Science 283(5410), 2050-2056, 1999.
12. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters 85(2), 441, 2000.
13. Diamanti, E., Leverrier, A.: Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy 17(9),6072-609, 2015.
14. Kogias, I., Xiang, Y., He, Q., Adesso, G.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Physical Review A 95(1), 012315, 2017.
15. Laudenbach, F., et al.: Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. arXiv preprint tquant-ph/1703.09278, 2017.
16. Moroder, T., et al.: Security of Distributed-Phase-Reference Quantum Key Distribution. Phys. Rev. Lett. 109 260501, 2012.
17. Lydersen, L., et al.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics 4(10), 686-689, 2010.
18. Azuma, K., Mizutani, A., Lo, H.K.: Fundamental rate-loss trade-off for the quantum internet. Nature Communications 7 13523, 2016.
19. Guha, S., et al.: Rate-loss analysis of an efficient quantum repeater architecture. Phys. Rev. A 92 022357, 2015.
20. Rass, S., Schartner, P.: Security in quantum networks as an optimization problem. In: ARES2009. pp.493-498. IEEE, 2009.
21. Lee, C.M., Hoban, M.J.: Towards device-independent information processing on general quantum networks. Phys. Rev. Lett. 120 020504, 2018.