I676384

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I676384 B**

(45)公告日： 中華民國 108 (2019) 年 11 月 01 日

(21)申請案號：104127894 (22)申請日： 中華民國 104 (2015) 年 08 月 26 日

(51)Int. Cl.： ***H04L9/08 (2006.01)***

(30)優先權：2015/01/08 中國大陸 201510009615.5

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)
香港

(72)發明人：付穎芳 (CN)；劉拴林 (CN)；高亞濱 (CN)；陳秀忠 (CN)

(74)代理人：林志剛

(56)參考文獻：

US 2005/0286723A1 US 2008/0137868A1

US 2012/0177201A1 US 2014/0372761A1

WO 2012/072983A2

趙紅濤,”基于密钥位协商的多路径量子密钥协商技术研究”,中原工學院學報, Dec. 2014.

審查人員：程敦睿

申請專利範圍項數：39 項 圖式數：7 共 57 頁

(54)名稱

基於可信中繼的量子密鑰分發系統、方法及裝置

(57)摘要

本申請公開了一種基於可信中繼的量子密鑰分發系統，一種基於可信中繼的量子密鑰分發方法及裝置。其中，所述系統包括：量子密鑰分發設備、用於中繼密鑰和轉發加密資料的路由設備、以及資料設備；所述每個量子密鑰分發設備與至少一個所述路由設備相連，所述每個量子密鑰分發設備與至少一個所述資料設備相連，所述路由設備彼此連接形成網狀拓撲；其中，所述量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商、並採用預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。採用上述系統，不僅可以有效提高量子密鑰的成碼量，而且可以提高量子密鑰分發網路的安全性。

指定代表圖：

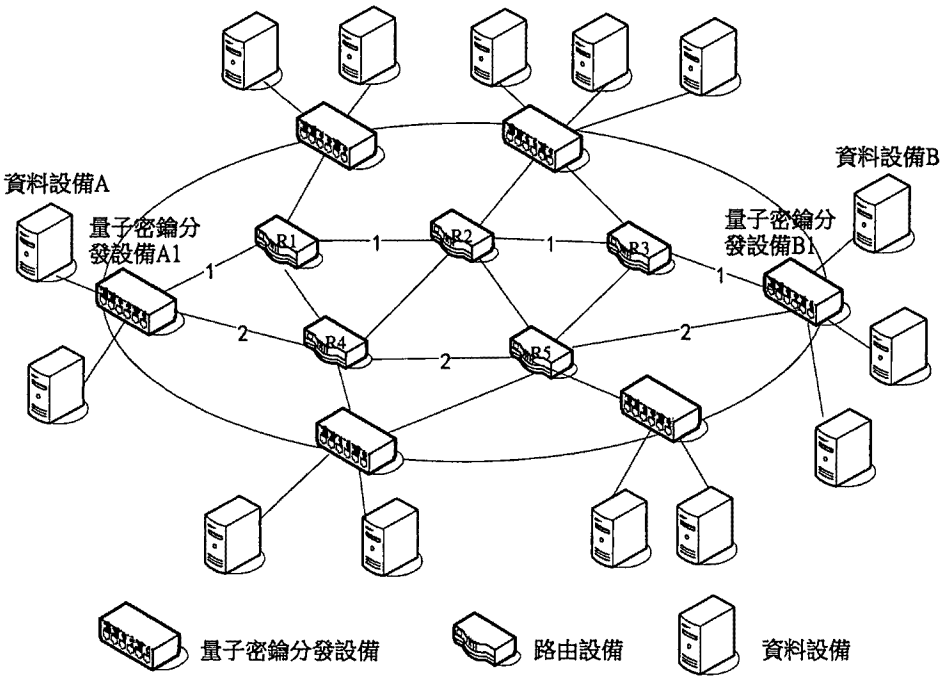
資料設備A
量子密鑰分發設備A1
資料設備B
量子密鑰分發設備B1
R1
R2
R3
R4
R5
1
1
1
1
2
2
量子密鑰分發設備
路由設備
資料設備

圖 2

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

基於可信中繼的量子密鑰分發系統、方法及裝置

【技術領域】

本申請係關於量子密鑰分發領域，具體關於一種基於可信中繼的量子密鑰分發系統。本申請同時提供一種基於可信中繼的量子密鑰分發方法，以及一種基於可信中繼的量子密鑰分發裝置。

【先前技術】

量子密碼作爲量子力學和密碼學的交叉產物，其安全性由量子力學基於原理保證，任何企圖截獲或測量量子密鑰的操作都會改變量子狀態，接收端可以透過量子態的改變判斷通信過程中是否存在竊聽者，從而可以確定是否捨棄此次密鑰，由此給通信帶來無條件安全的保障。目前採用 BB84 等量子密鑰協商協議可以實現端到端的量子密鑰分發(Quantum Key Distribution-QKD)。

隨著端到端量子密鑰分發技術的日益完善，人們開始關注 QKD 網路，一些公司和研究機構已經開始嘗試以不同方式建立 QKD 網路，包括：基於光學器件的 QKD 網路、基於可信中繼的 QKD 網路、以及基於量子中繼的純量子網路。其中基於信任中繼的 QKD 網路，可以同時保

證多用戶和長距離傳輸的要求，理論上甚至可以實現全球性的密鑰分配網路，而且在現有技術條件下，這種網路易於實現，因此可信中繼成爲了實現大規模 QKD 網路架構的有效手段。例如：歐洲建立的 SECOQC 量子保密通信網路、日本建立的東京高速量子網路、以及我國建立的量子政務網都採用了可信中繼的手段。

請參見附圖 1，其爲可信中繼量子密鑰傳輸模型的示意圖，Alice 與 Bob 之間要進行保密通信，兩者之間的密鑰協商路徑共包括了 3 個可信中繼節點。首先發送方 Alice 先和可信中繼節點 1 之間建立密鑰分發鏈路，進行量子密鑰協商，產生一個密鑰 K1；隨後，可信中繼節點 1 和可信中繼節點 2 之間建立密鑰分發鏈路，進行量子密鑰協商，產生一個共享密鑰 K2，且把密鑰 K1 用 K2 加密後傳送給可信中繼節點 2；.....依此類推，最終 Bob 接收到用密鑰 K4 加密的 K1，Bob 利用 K4 對其解密後獲得 K1，Alice 與 Bob 之間就可以使用密鑰 K1 進行保密通信了。

透過上述對密鑰中繼過程的描述可以看出，基於可信中繼的 QKD 網路要求中繼節點必須是安全的，如果任何一個中繼節點被攻破，整個路徑都變得不安全了，資料通信的安全性和穩定性將受到很大影響；而且採用上述密鑰中繼方式，密鑰成碼量(即：密鑰分發量)也比較低，無法滿足使用密鑰量較大的應用場景的需求，例如：雲計算。

【發明內容】

同的伺服器相連；或者，所述每個量子密鑰設備與複數個功能不同的伺服器相連。

可選的，所述系統還包括：具有量子密鑰分發設備的雲使用商網路；所述雲使用商網路的量子密鑰分發設備與所述雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連；

所述雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與所述雲計算資料中心的對端量子密鑰分發設備進行密鑰協商、並採用所述預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

可選的，所述雲使用商網路的量子密鑰分發設備採用兩條或者兩條以上的不同路徑與所述雲計算資料中心的對端量子密鑰分發設備進行密鑰協商包括，在所述任一路徑中採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商。

可選的，所述雲使用商網路的量子密鑰分發設備的數量爲兩個或者兩個以上，其中每個量子密鑰分發設備都與所述雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連。

可選的，所述量子密鑰分發系統分別部署於分散式雲計算網路的多個資料中心，所述資料設備是指各資料中心的伺服器，所述多個資料中心之間通過量子密鑰分發設備相連形成網狀拓撲；

其中，所述量子密鑰分發設備還用於採用兩條或者兩條以上的不同路徑與位於不同資料中心的對端量子密鑰分發設備進行密鑰協商，並採用所述預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

可選的，所述系統還包括：具有量子密鑰分發設備的雲使用商網路，所述雲使用商網路通過其量子密鑰分發設備與兩個或者兩個以上資料中心的量子密鑰分發設備相連；

所述雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與所述資料中心的對端量子密鑰分發設備進行密鑰協商、並採用所述預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

可選的，所述雲使用商網路的量子密鑰分發設備採用兩條或者兩條以上的不同路徑與所述資料中心的對端量子密鑰分發設備進行密鑰協商包括：在所述任一路徑中採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商。

此外，本申請還提供一種基於可信中繼的量子密鑰分發方法，所述方法在上述量子密鑰分發系統中實施，包括：

發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設

徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，所述多路徑協商單元除了包括實現其功能的本體子單元外，還包括路徑驗證子單元，所述路徑驗證子單元用於實現下述功能：所述路徑包含的路由設備以及接收方量子密鑰分發設備，根據接收到的所述路徑資訊，對與其進行密鑰協商的對端設備的身份進行驗證；若通過驗證，與所述對端設備進行密鑰協商並完成本節點的密鑰中繼操作；否則，通知所述發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

可選的，所述多路徑協商單元具體用於，通過所述路由設備的動態選路功能，實現經由兩條或者兩條以上的不同路徑進行所述密鑰協商。

可選的，所述裝置包括：

路徑驗證單元，用於在所述多路徑協商單元執行完畢後，所述發送方或接收方量子密鑰分發設備通過獲取本次密鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的各個設備的身份合法性進行驗證；若檢測到非法設備，則所述發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

可選的，所述裝置還包括：

身份驗證單元，用於在觸發所述多路徑協商單元工作之前，所述發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證；若所述對方設備未通過所

述身份驗證，則結束本方法的執行。

可選的，所述合併判斷單元包括：

安全評估結果獲取子單元，用於所述量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果；

策略判斷子單元，用於所述量子密鑰分發設備根據預先設定的策略及所述安全評估結果，判斷是否需要執行所述合併操作；

選擇協商子單元，用於所述量子密鑰分發設備選取執行密鑰合併操作的具體處理方式，以及通過經典通道，與對端量子密鑰分發設備協商並確認所述密鑰合併的具體處理方式，並觸發所述合併執行單元工作。

可選的，所述裝置還包括：

資料加密傳輸單元，用於所述發送方量子密鑰分發設備使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給所述接收方量子密鑰設備；

資料解密單元，用於所述接收方量子密鑰分發設備採用與所述發送方相同的共享密鑰對接收到的資料進行解密。

與現有技術相比，本申請具有以下優點:

本申請提供的基於可信中繼的量子密鑰分發系統及方法，在路由設備彼此連接形成網狀拓撲的基礎上，在發送方量子密鑰分發設備與接收方量子密鑰分發設備之間多路徑地進行密鑰協商、並採用預先設定的策略確定是否需要對所述多路徑協商得到的共享密鑰進行合併、並執行相應

的合併操作。採用上述技術方案，在網路安全性比較高的應用場景下，由於同時使用多條路徑進行密鑰協商，可以有效提高量子密鑰的分發量；在網路安全性比較低的應用場景下，則可以對經由不同路徑協商的密鑰進行合併生成新的共享密鑰，從而有效抵禦對可信中繼節點的攻擊等安全隱患，提高整個量子密鑰分發網路的安全性。

【圖式簡單說明】

圖 1 是基於可信中繼的量子密鑰傳輸模型的示意圖；

圖 2 是本申請的一種基於可信中繼的量子密鑰分發系統的示意圖；

圖 3 是本實施例提供的雲使用商訪問資料中心的系統架構的示意圖；

圖 4 是本實施例提供的分散式資料中心及雲使用商訪問分散式資料中心的系統架構示意圖；

圖 5 是本申請的一種基於可信中繼的量子密鑰分發方法的實施例的流程圖；

圖 6 是本實施例提供的採用多路徑進行密鑰協商的處理流程圖；

圖 7 是本申請的一種基於可信中繼的量子密鑰分發裝置的實施例的示意圖。

【實施方式】

在下面的描述中闡述了很多具體細節以便於充分理解

本申請。但是本申請能够以很多不同於在此描述的其它方式來實施，本領域技術人員可以在不違背本申請內涵的情況下做類似推廣，因此本申請不受下面公開的具體實施的限制。

在本申請中，提供了一種基於可信中繼的量子密鑰分發系統，一種基於可信中繼的量子密鑰分發方法，以及一種相應的裝置。在下面的實施例中逐一進行詳細說明。

請參考圖 2，其爲本申請的一種基於可信中繼的量子密鑰分發系統的示意圖，所述量子密鑰分發系統包括：量子密鑰分發設備、用於中繼密鑰和轉發加密資料的路由設備、以及用作資料傳輸的源端或目的端的資料設備；所述每個量子密鑰分發設備與至少一個所述路由設備相連，所述每個量子密鑰分發設備與至少一個所述資料設備相連，所述路由設備彼此連接形成網狀拓撲；其中，所述量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商、並採用預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

現有的基於信任中繼的量子密鑰分發網路，一方面只要有任意一個中繼節點被攻破，就無法保證密鑰的安全性，另一方面密鑰分發量也比較低。針對上述問題，本申請的技術方案提供了一種新的密鑰協商方式，在路由設備彼此連接形成網狀拓撲的基礎上，量子密鑰分發設備採用兩條或者兩條以上的不同路徑與對端量子密鑰分發進行密

他指標，例如，通過監控中繼節點的安全性而獲取的指標等；如何根據評估參數或者指標確定是否需要進行合併的策略也可以根據實際應用需要進行調整；具體的合併算法也可以與本例不同。上述這些都是具體實施方式的變更，都不偏離本申請的核心，都在本申請的保護範圍之內。

進一步地，針對量子密鑰協商過程中可能存在的中間人攻擊(中間人採用截獲、重發的方式進行攻擊)，本實施例還提供了一種採用路徑驗證技術的較佳實施方式。具體說，收發雙方的量子密鑰分發設備在協商密鑰之前，由發起量子密鑰協商的量子密鑰分發設備通過經典通道把本次進行密鑰協商的路徑資訊發給該路徑包含的各個路由節點以及接收方量子密鑰分發設備。由於每條路徑都是由一段一段的中繼鏈路組成的，所述路徑資訊包括路徑中每段鏈路的節點資訊，因此也稱爲路徑鏈資訊。

路由設備和接收方量子密鑰分發設備儲存接收到的路徑鏈資訊，並在隨後的量子密鑰協商過程中，根據所述路徑鏈資訊，對與其進行密鑰協商的路由設備或量子密鑰分發設備的身份合法性進行驗證，如果發現與所述路徑鏈資訊不一致，則說明可能存在中間人攻擊，那麼可以放棄本次量子密鑰協商過程，重新選擇其他路徑進行量子密鑰協商。

上面描述的實施方式通常與靜態路由方式配合使用，即，量子密鑰協商過程的發起方在啓動量子密鑰協商過程之前，就可以獲知本次協商的完整路徑資訊，因此可以預

先將路徑資訊發送給該路徑包含的設備。

在具體實施過程中，如果採用動態路由方式，也可以透過在網路內部設置監視節點實現與上述類似的路徑鏈驗證功能。具體說，監視節點透過對密鑰協商過程的監控，可以獲取本協商過程所經路徑中的各個中繼節點的資訊，並透過對該資訊的分析，辨別是否存在異常的中間節點，從而判斷是否存在中間人攻擊，如果存在，則放棄本次密鑰協商過程獲取的共享密鑰。

採用路徑鏈驗證技術，可以對量子密鑰協商過程中各個節點身份的合法性進行驗證，避免中間人攻擊，進一步保證量子密鑰協商過程的安全性。

本實施例提供的技術方案，在前面描述的多路徑進行密鑰協商的基礎上，還進一步採用了分波多工技術(Wavelength Division Multiplex, WDM)實現多量子通道的密鑰協商。所述 WDM 技術，是一種爲了充分利用單模光纖低損耗區巨大的帶寬資源，根據每一個通道光波頻率(或波長)的不同而將光纖的低損耗窗口劃分成若干個通道的技術，用不同的波長傳送各自的資訊，即使在同一根光纖上也不會相互干擾，以達到提高光纖的通信容量。

具體到本實施例，在進行多路徑密鑰協商的任一路徑中，量子密鑰分發設備與作爲中繼節點的路由設備之間，以及所述路由設備之間在進行量子密鑰協商時，可以同時使用不同的光波長協商密鑰，從而提高密鑰的分發量。

類似的，還可以在上述密鑰協商過程中，採用分時多

協商或資料加解密交互的過程中，可以綜合運用分波多工、分時多工以及上述光傳輸技術，以達到多路徑密鑰協商、提高密鑰分發量及資料交互吞吐量的目的。

至此，描述了本實施例提供的基於可信中繼的量子密鑰分發系統，所述系統由於採用了多路徑密鑰協商機制，因此可以取得提高密鑰分發量以及提高密鑰分發安全性的有益效果。

考慮到現有的雲計算環境中，雲骨幹網的各伺服器之間重要資料的交互、雲網路中各個資料中心之間資料的遠程備份及交互、雲使用商訪問雲資源等都對密鑰安全提出了較高的要求。經典網路中的加密方法無法提供可靠的安全性保障，而現有的各種小型量子密鑰分發網路也無法滿足雲密鑰安全分發的需求，包括，量子密鑰分發網路的吞吐量、成碼量；密鑰的傳輸距離；多用戶需求；保證任意用戶可以與雲骨幹網進行通信以及和現有公共網路融合等。

基於上述考慮，可以將本實施例提供的基於可信中繼的量子密鑰分發系統應用到雲網路架構中，從而解決上述問題。下面從雲骨幹網(資料中心)、雲使用商訪問資料中心，以及分散式資料中心三個方面作進一步說明。

(一)雲骨幹網系統架構。

在雲營運商的雲骨幹網中(即：本實施例所述的資料中心)，通常包含各種伺服器集群，比如檔案伺服器集群、Web 伺服器集群、應用伺服器集群、管理伺服器集

群、目錄伺服器集群，每個集群都包含若干台伺服器，這些伺服器之間交互的資料量通常比較大，對密鑰的分發量、整個網路的資料吞吐量的要求都比較高。

將本實施例提供的基於可信中繼的量子密鑰分發系統部署於上述的雲計算資料中心，所述用作資料傳輸的源端或者目的端的資料設備，就是上述的各種伺服器。與每個量子密鑰分發設備相連的複數個伺服器可以是功能相同的伺服器(例如都是檔案伺服器)，也可以是功能彼此不同的伺服器(例如，web 伺服器和管理伺服器等)。本實施例所述的複數個是指兩個或者兩個以上。

由於現有的雲計算資料中心通常是採用三層架構，而本實施例提供的量子密鑰分發系統採用的是基於路由設備的扁平架構，爲了實現現有三層架構與扁平架構之間的平滑過渡，同時也爲了擴展量子密鑰分發設備的有限端口數量，實現更多伺服器的接入，可以在部署了本實施例提供的量子密鑰分發系統的資料中心網路架構中引入光交換機，一個路由設備可以與一個或者一個以上光交換機相連，一個光交換機與一個或者一個以上的量子密鑰分發設備相連。

由於將本實施例提供的量子密鑰分發系統部署於雲計算資料中心，爲了實現資料中心伺服器之間的保密通信，與所述伺服器相連的量子密鑰分發設備採用兩條或者兩條以上的路徑進行密鑰協商，並採用預先設定的策略執行所需的密鑰合併操作。此外，在本實施例前面描述的路徑鏈

驗證、分波多工、分時多工以及其他光傳輸技術等也都可以應用於所述資料中心，以達到提高密鑰分發量、資料交互吞吐量，以及提高密鑰分發過程安全性的目的，從而滿足雲計算資料中心的需求，對於上述內容請參見上文的相關文字，此處不再贅述。

(二)雲使用商訪問資料中心的系統架構。

在(一)中將本實施例提供的量子密鑰分發系統部署於雲計算資料中心的基礎上，爲了滿足雲使用商訪問資料中心的需求，本系統還可以包括：具有量子密鑰分發設備的雲使用商網路；所述雲使用商網路的量子密鑰分發設備與所述雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連。

請參見圖 3，其爲本實施例提供的雲使用商訪問資料中心的系統架構示意圖，在該例子中，包括一個雲計算資料中心、兩個雲使用商網路(甲網路和乙網路)，雲使用商甲網路使用其量子密鑰分發設備、通過接入光纖與雲計算資料中心的三個量子密鑰分發設備相連，雲使用商乙網路使用其量子密鑰分發設備、通過接入光纖與雲計算資料中心的兩個量子密鑰分發設備相連。雲使用商網路中通常還包括內部閘道以及用於訪問雲計算資料中心的多種終端設備，此示意圖中沒有示出。

所述雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與所述雲計算資料中心的對端量子密鑰分發設備進行密鑰協商、並採用所述預先設定的策

略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。通過多路徑協商機制，提高量子密鑰分發過程的安全性以及量子密鑰的分發量。

所述雲使用商網路的量子密鑰分發設備在任一路徑的密鑰協商過程中，也可以採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商，以進一步提高密鑰分發量。

此外，在本實施例前面描述的路徑鍵驗證、以及光塞取多工技術、光交叉互聯技術、光封包交換技術等也都可以應用在雲使用商訪問資料中心的系統架構中，以達到提高密鑰分發量及資料交互吞吐量的目的。

需要說明的是，在具體實施中，根據實際業務的需要，雲使用商網路也可以設置兩個或者兩個以上的量子密鑰分發設備，其中每個量子密鑰分發設備都與所述雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連。

(三)分散式資料中心的系統架構。

雲供應商透過資料中心向雲使用商提供業務服務的同時，通常還使用備份資料中心進行資料備份，或者雲供應商採用雙活資料中心爲雲使用商提供業務服務，另外，隨著雲計算技術的發展，雲供應商僅提供單一的資料中心已經無法滿足雲使用商的需求，因此通常在不同的地域設置多個資料中心。在上述基於多資料中心的分散式架構下，也可以通過部署本實施例提供的量子密鑰分發網路，滿足分散式雲計算對密鑰分發量以及密鑰安全性的要求。

具體說，所述量子密鑰分發系統分別部署於分散式雲計算網路的多個資料中心，所述資料設備是指各資料中心的伺服器，所述多個資料中心之間通過量子密鑰分發設備相連形成網狀拓撲。

請參見圖 4，其爲本實施例提供的分散式資料中心及雲使用商訪問資料中心的系統架構示意圖，在該例子中，包括雲供應商的 4 個雙活資料中心，這 4 個資料中心之間通過量子密鑰分發設備相連形成網狀拓撲。這 4 個資料中心彼此進行資料備份或者資料傳輸時，作爲源端的資料中心的量子密鑰分發設備可以採用兩條或者兩條以上的不同路徑與位於不同資料中心的對端量子密鑰分發設備進行密鑰協商，並採用所述預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。通過多路徑協商機制，提高量子密鑰分發過程的安全性以及量子密鑰的分發量。

進一步地，上述系統還可以包括具有量子密鑰分發設備的雲使用商網路，所述雲使用商網路通過其量子密鑰分發設備與兩個或者兩個以上資料中心的量子密鑰分發設備相連。

在圖 4 所示的例子中，包括 2 個雲使用商網路(甲網路、乙網路)，甲、乙網路使用各自的量子密鑰分發設備、通過接入光纖分別與兩個資料中心的量子密鑰分發設備相連。雲使用商網路中通常還包括內部閘道以及用於訪問雲計算資料中心的多種終端設備，此示意圖中沒有示

出。

所述雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與所述資料中心的對端量子密鑰分發設備進行密鑰協商、並採用所述預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。通過多路徑協商機制，提高量子密鑰分發過程的安全性以及量子密鑰的分發量。

所述雲使用商網路的量子密鑰分發設備在任一路徑的密鑰協商過程中，也可以採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商，以進一步提高密鑰分發量。

此外，在本實施例前面描述的路徑鏈驗證、以及光塞取多工技術、光交叉互聯技術、光封包交換技術等也都可以應用在分散式雲計算資料中心及雲使用商訪問資料中心的系統架構中，以達到提高密鑰分發量及資料交互吞吐量的目的。

在上述實施例中提供了一種基於可信中繼的量子密鑰分發系統，在此基礎上，本申請還提供一種基於可信中繼的量子密鑰分發方法，所述方法在上述量子密鑰分發系統中實施。請參考圖 5，其爲本申請提供的一種基於可信中繼的量子密鑰分發方法的實施例的流程圖，本實施例與第一實施例內容相同的部分不再贅述，下面重點描述不同之處。本申請提供的基於可信中繼的量子密鑰分發方法包括：

步驟 501：發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商。

本技術方案的核心在於，多路徑地進行量子密鑰協商，一方面可以提高量子密鑰的成碼量，另一方面可以抵禦對中繼節點(即：路由設備)的攻擊。爲了進一步提高量子密鑰協商過程的安全性，在本步驟中還提供了收發雙方進行身份驗證、以及對密鑰協商路徑進行驗證的較佳實施方式，下面結合附圖 6 對本步驟作進一步說明。

步驟 501-1：所述發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證。

具體說，發送方量子密鑰分發設備(簡稱 A 設備)首先通過經典通道，向接收方量子密鑰分發設備(簡稱 B 設備)發送密鑰協商請求，請求中至少包含 A 設備的身份資訊(例如，帳戶資訊)。該請求經過若干個路由器設備的轉發到達 B 設備，B 設備驗證所述請求中携帶的 A 設備身份的合法性，如果合法則向 A 設備發送應答，同時可以在應答中携帶 B 設備的身份資訊，同理，A 設備收到所述應答後對 B 設備的身份進行驗證。如果經過上述驗證過程，A 設備和 B 設備都認爲對方設備是合法的，則可以繼續後續的處理，否則本方法結束。

上面給出了收發雙方量子密鑰分發設備通過經典通道進行身份驗證的一種方式，在具體實施過程中，也可以採用其他身份驗證方式，例如，採用數位憑證等方式，只要

能夠確認即將與其進行量子密鑰協商的對端量子密鑰分發設備的身份是否合法即可。

步驟 501-2：所述發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

發送方量子密鑰分發設備根據預先獲取的網路拓撲資訊，選擇兩條或者兩條以上的不同路徑，其中任意兩條路徑所包含的路由設備都不完全相同，也就說，允許不同的路徑之間共用相同的路由設備。所述發送方量子密鑰分發設備在進行路徑選擇時，可以採用負載均衡策略。

步驟 501-3：發送方量子密鑰分發設備通過經典通道，將每條路徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備。

所述路徑資訊中包含了路徑中每個節點的相關資訊，所述發送方量子密鑰分發設備選擇完路徑後，可以通過經典通道將每條路徑的路徑資訊發送給該路徑包含的路由設備及接收方量子密鑰分發設備，供這些設備在中繼量子密鑰的過程中對對方身份進行驗證(參見步驟 501-4 中的說明)。

步驟 501-4：收發雙方的量子密鑰協商設備及路由設備通過所述兩條或者兩條以上的不同路徑進行密鑰協商，並在該過程中進行路徑驗證。

爲了滿足遠距離傳輸的需求，本技術方案採用了信任中繼的方式，因此在每一條路徑中，每兩個相鄰設備可以

通過量子通道的密鑰協商過程獲取共享密鑰，並逐段實現密鑰的中繼轉發，最終使得收發雙方的量子密鑰分發設備獲取相同的共享密鑰。在具體實施中，每兩個相鄰設備之間的共享密鑰，可以採用上述動態協商的方式獲取，也可以採用出廠預置的初始密鑰或雙方預先協商好的共享密鑰，同樣可以實現上述中繼功能。

由於並發進行密鑰協商的多條路徑，通常是採用負載均衡機制選取的，可能共用相同的路由設備，因此路由設備在實現上述中繼功能時，可能只是執行轉發操作，也可能需要通過各種多工手段執行合併操作，或者通過相應的解多工手段執行相應的分拆操作，最終多路徑地完成端到端的量子密鑰協商過程。

進一步地，爲了防止中間人攻擊，本技術方案還採用了路徑驗證技術，每個路由設備以及接收方量子密鑰分發設備，在與相鄰設備進行密鑰協商及執行相應的中繼操作之前，先根據接收到的路徑資訊，對所述相鄰設備的身份進行驗證；若通過驗證，與所述相鄰設備進行密鑰協商並完成本節點的密鑰中繼操作；否則，通知發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

需要說明的是，上面給出的是採用靜態選路方式實現多路徑密鑰協商的實施過程。在具體實施中，也可以通過路由設備基於負載均衡策略進行動態選路，實現經由兩條或者兩條以上的不同路徑進行所述密鑰協商。如果採用動態選路方式，可以在量子密鑰協商過程完成後，進行路徑

驗證，即：發送方或接收方量子密鑰分發設備或者監視節點，通過收集本次密鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的各個設備身份的合法性進行驗證；若檢測到非法設備(說明可能存在中間人攻擊)，則通知發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

此外，爲了最大限度地抵禦對中繼節點的攻擊，本實施例還提供一種較佳實施方式，即：本步驟進行端到端量子密鑰協商採用的路徑是完全不相關的多條路徑，也就說，對任意一個中繼節點的攻擊只可能對一條路徑的安全性產生影響，而不會影響到其他路徑。

步驟 502：所述發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過所述密鑰協商過程獲取的共享密鑰進行合併操作；若是，執行步驟 503。

通過步驟 501 的多路徑協商過程，收發雙方的量子密鑰分發設備通常可以獲取多個共享密鑰(與路徑數目一致)，在本步驟中通過預先設定的策略判斷是否需要執行合併操作。

發送方或者接收方量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果(例如包括誤碼率、丟包率等)；如果任一路徑的所述安全評估結果超出了所述策略中設定的安全範圍，則說明該路徑或中繼節點存在安全隱患，需要針對多路徑獲取的共享密鑰執行相應的合併操作，以保證密鑰的安全性。

在具體實施中，可以採用多種密鑰合併方式，因此作出上述判斷的量子密鑰分發設備可以選取執行密鑰合併操作的具體處理方式，並通過經典通道，與對端量子密鑰分發設備協商並確認所述密鑰合併的具體處理方式，從而使得收發雙方的量子密鑰分發設備能夠在步驟 503 中對共享密鑰進行相同的合併處理，從而雙方最終得到新的共享密鑰。

步驟 503：所述發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

本實施例並不對合併操作所採用的算法，進行具體的限定。關於本步驟的說明，請參見“基於可信中繼的量子密鑰分發系統”實施例中的相關文字，此處不再贅述。

通過上述步驟 501-503 描述的多路徑密鑰協商過程可以看出，在網路安全性比較高的應用場景下，收發雙方的量子密鑰分發設備可以同時協商獲取多個共享密鑰，提高密鑰分發量；在網路安全性比較低的應用場景下，即使其中有某一條或者幾條路徑的中繼節點被攻破，但只要其中有一條路徑是安全的，仍然可以通過對不同路徑密鑰的合併操作生成新的、安全的共享密鑰，從而提高整個量子密鑰分發網路的安全性。

相應的，發送方量子密鑰分發設備可以使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給所述接收方量子密鑰分發設備，接收方量子密鑰分發設備採用與所述發送方相同的共享密鑰對接收到的資料進行

解密。由於密鑰分發量的提高，資料交互吞吐量也能得到相應提高。

進一步地，可以將上述實施例描述的量子密鑰分發方法，應用在雲計算網路中，以滿足雲計算網路對雲密鑰的安全性、成碼量、傳輸距離、以及資料吞吐量等各方面的要求。

(一)將所述方法應用在雲骨幹網路(資料中心)。

爲了實現雲計算資料中心的任意兩台伺服器之間的保密資料傳輸，與所述伺服器分別相連的量子密鑰分發設備可以多路徑地進行密鑰協商，並用最終獲取的共享密鑰對資料進行加解密，從而實現資料的保密傳輸。

(二)將所述方法應用在雲骨幹網路(資料中心)和雲使用商網路組成的系統中。

爲了實現雲使用商網路與雲計算資料中心的任一伺服器之間的保密資料傳輸，雲使用商網路的量子密鑰分發設備和與所述伺服器相連的量子密鑰分發設備，可以多路徑地進行密鑰協商，並用最終獲取的共享密鑰對資料進行加解密，從而實現資料的保密傳輸。

(三)將所述方法應用在由分散式雲計算資料中心和雲使用商網路組成的系統中。

爲了實現位於不同雲計算資料中心的任意兩台伺服器之間的保密資料傳輸(資料備份或者是資料訪問)，與所述伺服器分別相連的量子密鑰分發設備可以多路徑地進行密鑰協商，並用最終獲取的共享密鑰對資料進行加解密，從

而實現資料的保密傳輸。

爲了實現雲使用商網路與分散式雲計算資料中心的任一伺服器之間的保密資料傳輸，雲使用商網路的量子密鑰分發設備和與所述伺服器相連的量子密鑰分發設備，可以多路徑地進行密鑰協商，並用最終獲取的共享密鑰對資料進行加解密，從而實現資料的保密傳輸。

在上述的實施例中，提供了一種基於可信中繼的量子密鑰分發方法，與之相對應的，本申請還提供一種基於可信中繼的量子密鑰分發裝置。請參看圖 7，其爲本申請的一種基於可信中繼的量子密鑰分發裝置的實施例的示意圖。由於裝置實施例基本相似於方法實施例，所以描述得比較簡單，相關之處參見方法實施例的部分說明即可。下述描述的裝置實施例僅僅是示意性的。

本實施例的一種基於可信中繼的量子密鑰分發裝置，包括：多路徑協商單元 701，用於發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商；合併判斷單元 702，用於所述發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過所述密鑰協商過程獲取的共享密鑰進行合併操作；合併執行單元 703，用於當所述合併判斷單元的輸出爲“是”時，所述發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

可選的，所述裝置還包括：

路徑獲取單元，用於在觸發所述多路徑協商單元工作之前，所述發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

可選的，所述裝置還包括：

路徑分發單元，用於在觸發所述多路徑協商單元工作之前，發送方量子密鑰分發設備通過經典通道，將每條路徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，所述多路徑協商單元除了包括實現其功能的本體子單元外，還包括路徑驗證子單元，所述路徑驗證子單元用於實現下述功能：所述路徑包含的路由設備以及接收方量子密鑰分發設備，根據接收到的所述路徑資訊，對與其進行密鑰協商的對端設備的身份進行驗證；若通過驗證，與所述對端設備進行密鑰協商並完成本節點的密鑰中繼操作；否則，通知所述發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

可選的，所述多路徑協商單元具體用於，通過所述路由設備的動態選路功能，實現經由兩條或者兩條以上的不同路徑進行所述密鑰協商。

可選的，所述裝置包括：

路徑驗證單元，用於在所述多路徑協商單元執行完畢後，所述發送方或接收方量子密鑰分發設備通過獲取本次密鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的

各個設備的身份合法性進行驗證；若檢測到非法設備，則所述發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

可選的，所述裝置還包括：

身份驗證單元，用於在觸發所述多路徑協商單元工作之前，所述發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證；若所述對方設備未通過所述身份驗證，則結束本方法的執行。

可選的，所述合併判斷單元包括：

安全評估結果獲取子單元，用於所述量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果；

策略判斷子單元，用於所述量子密鑰分發設備根據預先設定的策略及所述安全評估結果，判斷是否需要執行所述合併操作；

選擇協商子單元，用於所述量子密鑰分發設備選取執行密鑰合併操作的具體處理方式，以及通過經典通道，與對端量子密鑰分發設備協商並確認所述密鑰合併的具體處理方式，並觸發所述合併執行單元工作。

可選的，所述裝置還包括：

資料加密傳輸單元，用於所述發送方量子密鑰分發設備使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給所述接收方量子密鑰分發設備；

資料解密單元，用於所述接收方量子密鑰分發設備採用與所述發送方相同的共享密鑰對接收到的資料進行解

密。

本申請雖然以較佳實施例公開如上，但其並不是用來限定本申請，任何本領域技術人員在不脫離本發明的精神和範圍內，都可以做出可能的變動和修改，因此本申請的保護範圍應當以本申請之申請專利範圍所界定的範圍爲準。

在一個典型的配置中，計算設備包括一個或多個處理器(CPU)、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體(RAM)和/或非揮發性記憶體等形式，如唯讀記憶體(ROM)或快閃記憶體(flash RAM)。記憶體是電腦可讀媒體的示例。

1、電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程序的模組或其他資料。電腦的儲存介質的例子包括，但不限於相變記憶體(PRAM)、靜態隨機存取記憶體(SRAM)、動態隨機存取記憶體(DRAM)、其他類型的隨機存取記憶體(RAM)、唯讀記憶體(ROM)、電可抹除可編程唯讀記憶體(EEPROM)、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體(CD-ROM)、數位多功能光碟(DVD)或其他光學儲存、磁盒式磁帶，磁帶磁片儲存或其他磁性儲存設備或任何其他非傳輸媒體，可用於儲存可以被計算設備訪問的資訊。按照本文中的界定，電腦可讀媒體不包括非暫存電腦可讀媒體

(transitory media)，如調製的資料信號和載波。

2、本領域技術人員應明白，本申請的實施例可提供爲方法、系統或電腦程式產品。因此，本申請可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本申請可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體(包括但不限於磁碟記憶體、CD-ROM、光學記憶體等)上實施的電腦程式產品的形式。

【符號說明】

701：多路徑協商單元

702：合併判斷單元

703：合併執行單元

公告本

I676384

發明摘要

※申請案號：104127894

※申請日：104 年 08 月 26 日　　※IPC 分類：

【發明名稱】(中文/英文)

基於可信中繼的量子密鑰分發系統、方法及裝置

【中文】

本申請公開了一種基於可信中繼的量子密鑰分發系統，一種基於可信中繼的量子密鑰分發方法及裝置。其中，所述系統包括：量子密鑰分發設備、用於中繼密鑰和轉發加密資料的路由設備、以及資料設備；所述每個量子密鑰分發設備與至少一個所述路由設備相連，所述每個量子密鑰分發設備與至少一個所述資料設備相連，所述路由設備彼此連接形成網狀拓撲；其中，所述量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商、並採用預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。採用上述系統，不僅可以有效提高量子密鑰的成碼量，而且可以提高量子密鑰分發網路的安全性。

【英文】

【代表圖】

【本案指定代表圖】：第(２)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

圖式

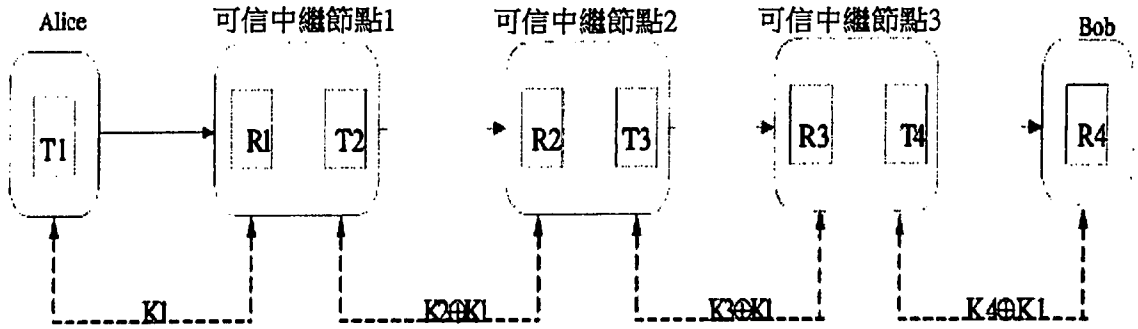
Alice
可信中繼節點1
可信中繼節點2
可信中繼節點3
Bob
T1
R1
T2
R2
T3
R3
T4
R4
K1
K2⊕K1
K3⊕K1
K4⊕K1

圖 1

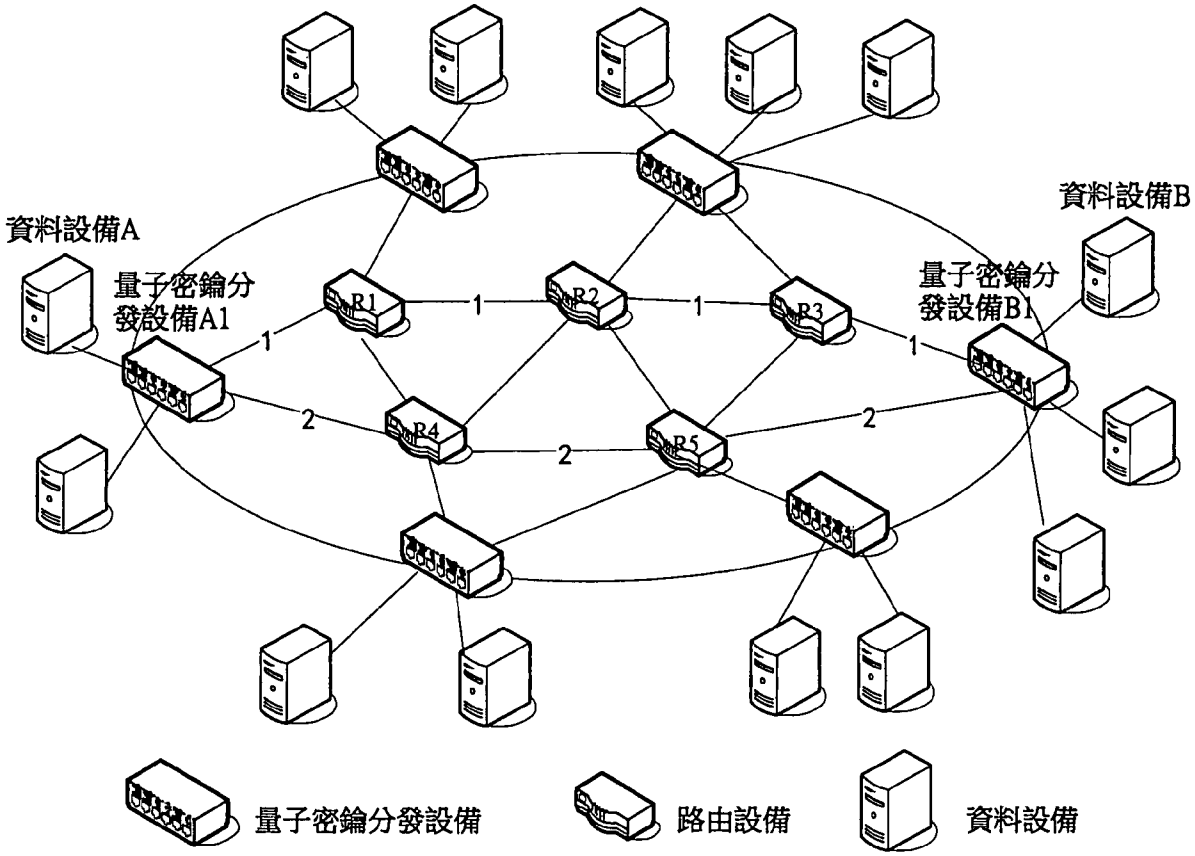
資料設備A
量子密鑰分發設備A1
資料設備B
量子密鑰分發設備B1
R1
R2
R3
R4
R5
1
2
量子密鑰分發設備
路由設備
資料設備

圖 2

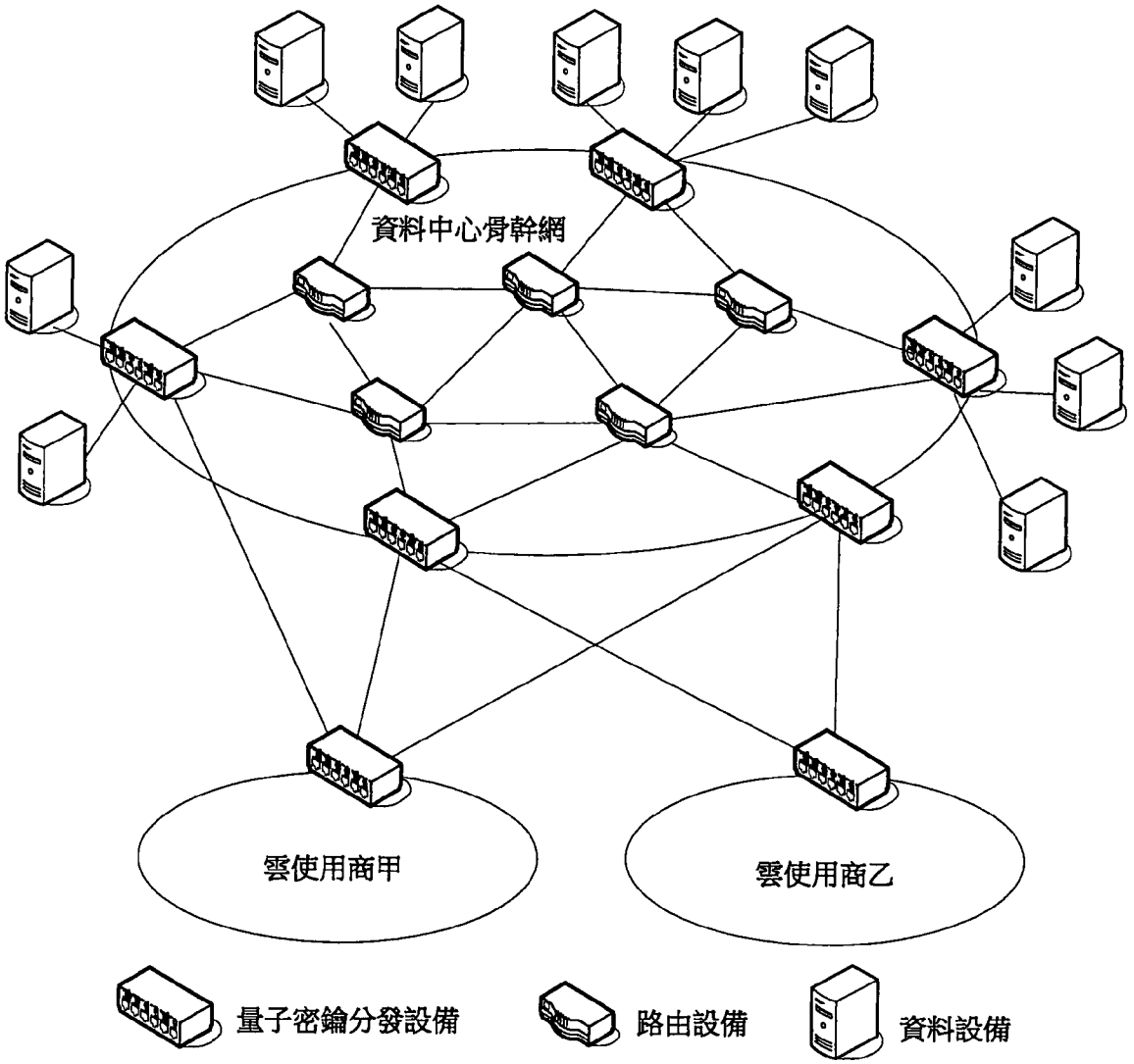

圖 3

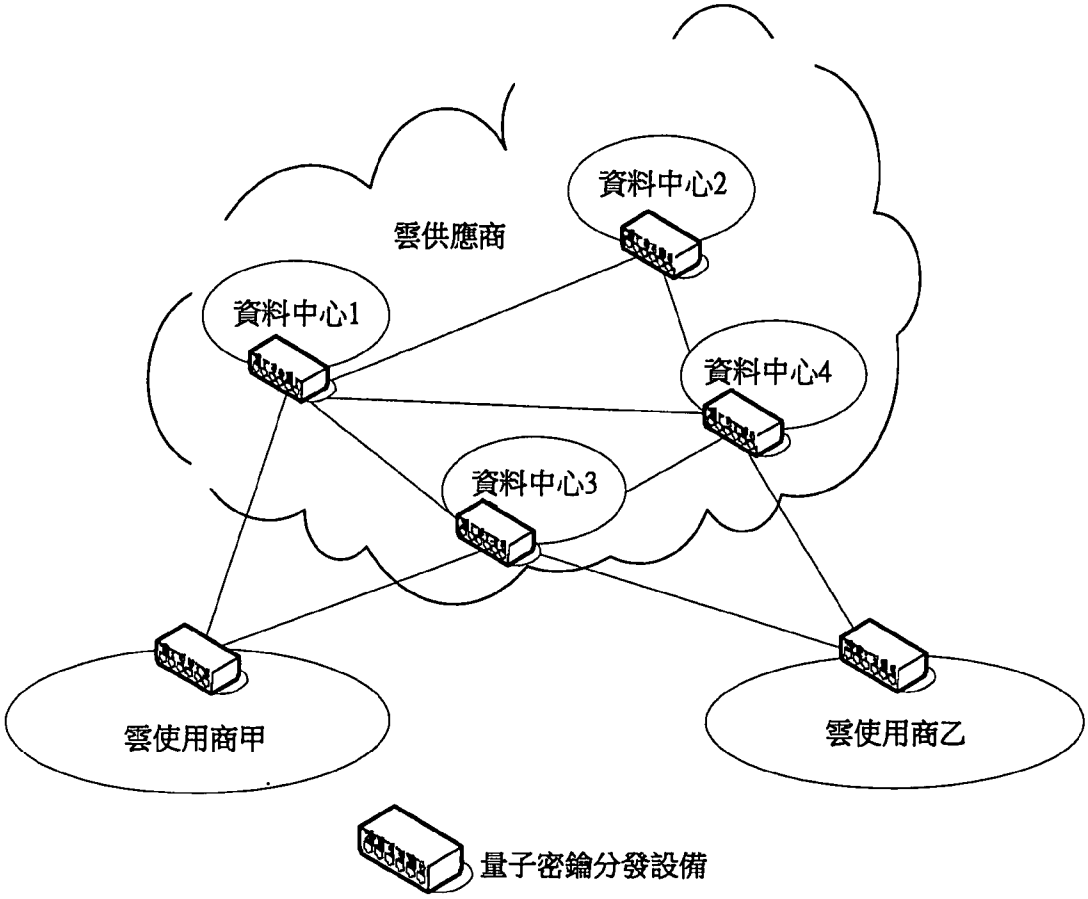
雲供應商
資料中心1
資料中心2
資料中心3
資料中心4
雲使用商甲
雲使用商乙
量子密鑰分發設備

圖 4

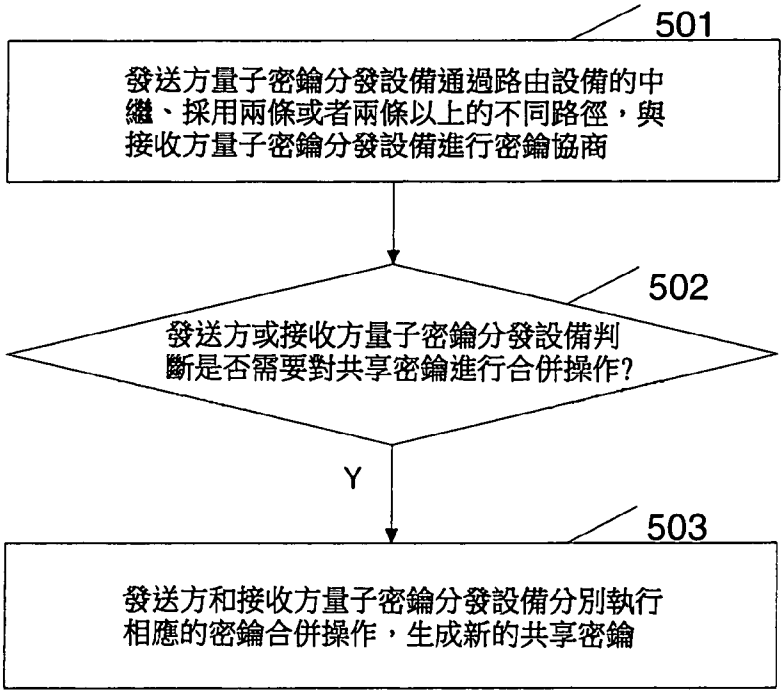
501
發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商
502
發送方或接收方量子密鑰分發設備判斷是否需要對共享密鑰進行合併操作?
Y
503
發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰

圖 5

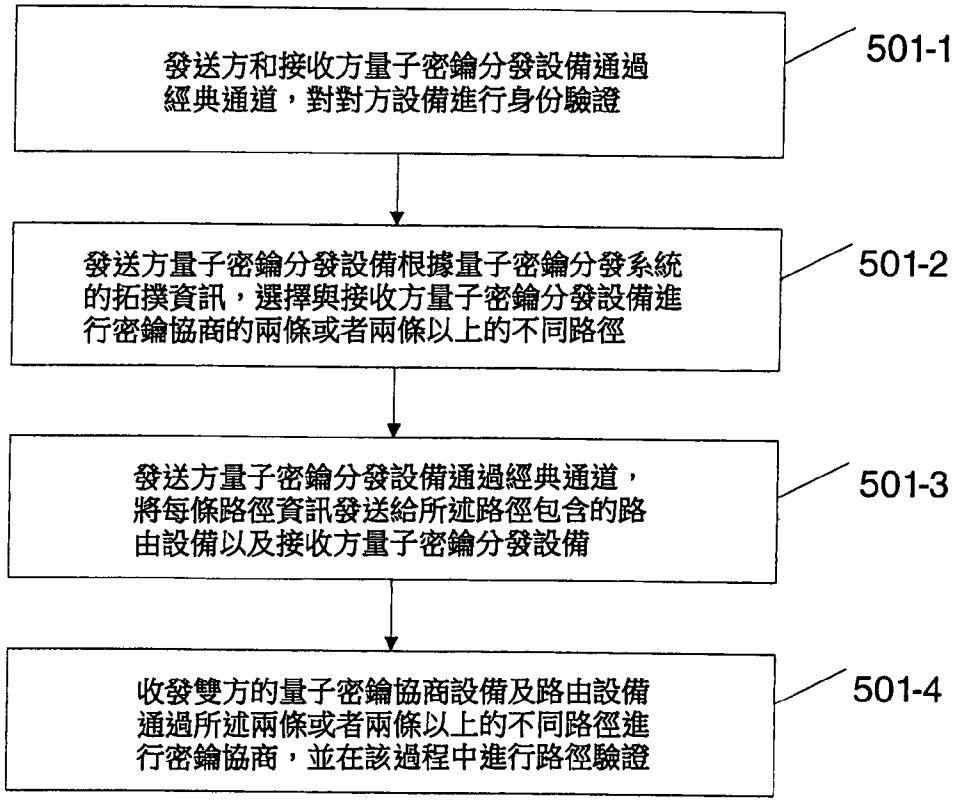
發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證
501-1
發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑
501-2
發送方量子密鑰分發設備通過經典通道，將每條路徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備
501-3
收發雙方的量子密鑰協商設備及路由設備通過所述兩條或者兩條以上的不同路徑進行密鑰協商，並在該過程中進行路徑驗證
501-4

圖 6

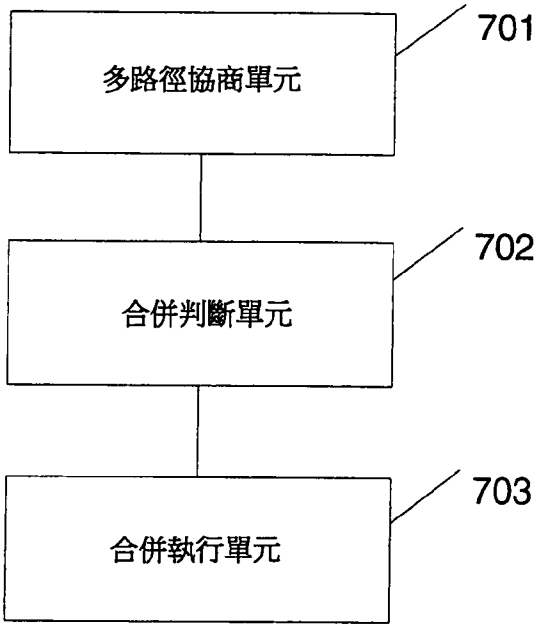
多路徑協商單元
701
合併判斷單元
702
合併執行單元
703

圖 7

本申請提供一種基於可信中繼的量子密鑰分發系統，以解決現有的基於可信中繼的量子密鑰分發網路安全性低、密鑰分發量低的問題。本申請另外提供一種基於可信中繼的量子密鑰分發方法，以及一種基於可信中繼的量子密鑰分發裝置。

本申請提供一種基於可信中繼的量子密鑰分發系統，包括：

量子密鑰分發設備、用於中繼密鑰和轉發加密資料的路由設備、以及用作資料傳輸的源端或目的端的資料設備；所述每個量子密鑰分發設備與至少一個所述路由設備相連，所述每個量子密鑰分發設備與至少一個所述資料設備相連，所述路由設備彼此連接形成網狀拓撲；

其中，所述量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商、並採用預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

可選的，所述量子密鑰分發設備還用於在發起量子密鑰協商之前，將本次量子密鑰協商的路徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，所述路由設備和所述接收方量子密鑰分發設備還用於根據接收到的路徑資訊，對與其進行密鑰協商的路由設備或量子密鑰分發設備的身份進行驗證。

可選的，所述每個量子密鑰分發設備與至少兩個所述路由設備相連。

可選的，所述兩條或者兩條以上的不同路徑是指其中任意兩條路徑都不包含相同的路由設備。

可選的，所述量子密鑰分發設備所採用的兩條或者兩條以上的不同路徑，是根據負載均衡策略選擇的。

可選的，所述量子密鑰分發設備還用於對在所述資料設備之間傳輸的資料進行加解密。

可選的，所述系統還包括：量子閘道設備，所述量子密鑰分發設備通過所述量子閘道設備與所述資料設備相連，所述量子閘道設備用於採用與其相連的量子密鑰分發設備提供的量子密鑰，對在所述資料設備之間傳輸的資料進行加解密。

可選的，所述量子密鑰分發設備採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商包括，在所述任一路徑中採用分波多工技術和/或分時多工技術，實現多量子通道的密鑰協商。

可選的，所述路由設備採用光塞取多工技術、光交叉互聯技術、和/或光封包交換技術，對採用量子密鑰加密後的資料進行轉發。

可選的，所述量子密鑰分發系統部署於雲計算資料中心；

所述資料設備是指雲計算資料中心的伺服器。

可選的，所述系統還包括：光交換機，所述路由設備通過所述光交換機與量子密鑰分發設備相連。

可選的，所述每個量子密鑰分發設備與複數個功能相

備進行密鑰協商；

所述發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過所述密鑰協商過程獲取的共享密鑰進行合併操作；

若是，所述發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

可選的，在進行所述密鑰協商之前，執行下述操作：

所述發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

可選的，所述發送方量子密鑰分發設備在選擇所述兩條或者兩條以上的不同路徑後，執行下述操作：

通過經典通道，將每條路徑資訊發送給所述路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，在所述密鑰協商過程中，所述路徑包含的路由設備以及接收方量子密鑰分發設備執行如下操作：

根據接收到的所述路徑資訊，對與其進行密鑰協商的對端設備的身份進行驗證；

若通過驗證，與所述對端設備進行密鑰協商並完成本節點的密鑰中繼操作；

否則，通知所述發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

可選的，所述採用兩條或者兩條以上的不同路徑進行密鑰協商，採用如下方式實現：

通過所述路由設備的動態選路功能，實現經由兩條或者兩條以上的不同路徑進行所述密鑰協商。

可選的，在完成所述密鑰協商之後，執行下述操作：

所述發送方或接收方量子密鑰分發設備通過獲取本次密鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的各個設備的身份合法性進行驗證；

若檢測到非法設備，則所述發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

可選的，所述兩條或者兩條以上的不同路徑是指其中任意兩條路徑都不包含相同的路由設備。

可選的，所述兩條或者兩條以上的不同路徑，是根據負載均衡策略選擇的。

可選的，在進行所述密鑰協商之前，執行下述操作：

所述發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證；若所述對方設備未通過所述身份驗證，則結束本方法的執行。

可選的，所述發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過所述密鑰協商過程獲取的共享密鑰進行合併操作，包括：

所述量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果；

根據預先設定的策略及所述安全評估結果，判斷是否需要執行所述合併操作；

若是，執行下述操作：

選取執行密鑰合併操作的具體處理方式；

通過經典通道，與對端量子密鑰分發設備協商並確認所述密鑰合併的具體處理方式；

轉到所述發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作的步驟執行。

可選的，所述方法還包括：

所述發送方量子密鑰分發設備使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給所述接收方量子密鑰設備；

所述接收方量子密鑰分發設備採用與所述發送方相同的共享密鑰對接收到的資料進行解密。

可選的，所述方法應用於雲計算資料中心；所述發送方和接收方量子密鑰分發設備是指與進行保密資料傳輸的源端和目的端伺服器分別相連的量子密鑰分發設備。

可選的，所述方法應用於由雲計算資料中心和雲使用商網路組成的系統中；

所述發送方和接收方量子密鑰分發設備是指雲使用商網路的量子密鑰分發設備、以及與雲使用商網路進行保密資料傳輸的伺服器相連的量子密鑰分發設備，所述伺服器位於所述雲計算資料中心內。

可選的，所述方法應用於由分散式雲計算資料中心和雲使用商網路組成的系統中；

所述發送方和接收方量子密鑰分發設備是指與進行保密資料傳輸的源端和目的端伺服器相連的量子密鑰分發設

備，所述源端和目的端伺服器位於不同的雲計算資料中心；或者，

雲使用商網路的量子密鑰分發設備、以及與雲使用商進行保密資料傳輸的伺服器相連的量子密鑰分發設備，所述伺服器位於所述分散式雲計算資料中心內。

相應的，本申請還提供一種基於可信中繼的量子密鑰分發裝置，包括：

多路徑協商單元，用於發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商；

合併判斷單元，用於所述發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過所述密鑰協商過程獲取的共享密鑰進行合併操作；

合併執行單元，用於當所述合併判斷單元的輸出爲“是”時，所述發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

可選的，所述裝置還包括：

路徑獲取單元，用於在觸發所述多路徑協商單元工作之前，所述發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

可選的，所述裝置還包括：

路徑分發單元，用於在觸發所述多路徑協商單元工作之前，發送方量子密鑰分發設備通過經典通道，將每條路

鑰協商。本申請實施例所述的兩條或者兩條以上的不同路徑是指其中任意兩條路徑所包含的路由設備都不完全相同。

在具體實施時，可以採用靜態路由(也稱指定路由)方式選擇進行量子密鑰協商的不同路徑。具體說，量子密鑰分發設備可以通過網路泛洪等機制維護整個網路拓撲資訊，從而可以在發起量子密鑰協商過程之前，採用負載均衡策略，綜合考慮網路拓撲中路由設備的負載狀況和鏈路的占用狀況，選擇相對空閒的路由設備以及鏈路，組成兩條或者多條不同的路徑，每條路徑所涉及的各路由設備按照所述路徑進行密鑰協商與中繼。此外，也可以採用動態路由方式，即，量子密鑰分發設備與路由設備採用逐跳動態選路的方式，根據本地儲存的路由表資訊，基於負載均衡等策略選擇到達對端量子密鑰分發設備的下一跳路由。

在路由設備彼此連接形成網狀拓撲的基礎上，本實施例還提供一種較佳實施方式，每個量子密鑰分發設備與至少兩個路由設備相連，由於路由設備彼此之間採用網狀拓撲相連，因此量子密鑰分發設備進行密鑰協商時可以採用完全不相關的多條路徑，即：其中任意兩條路徑都不包含相同的路由設備，也就是說任意兩條路徑都沒有共用的路由設備。

請參見圖 2，其中資料設備 A 與資料設備 B 之間要進行保密資料傳輸，量子密鑰分發設備 A1 採用路徑 1 和路徑 2 與對端量子密鑰分發設備 B1 進行密鑰協商，其中路

徑 1 包含路由設備 R1、R2、R3，路徑 2 包含路由設備 R4、R5，由於路徑 1 與路徑 2 不包含相同的路由設備，因此是兩條完全不相關路徑。

量子密鑰分發設備採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商。在每一條路徑中，每兩個相鄰設備利用彼此之間的 QKD 鏈路通過密鑰傳輸、資料篩選、資料協調以及隱私放大等階段獲取兩者之間的共享密鑰，並逐段利用所述共享密鑰對發送方量子密鑰分發設備獲取的共享密鑰進行“加密-解密-加密.....解密”的中繼轉發操作，最終接收方量子密鑰分發設備與發送方量子密鑰分發設備獲取相同的共享密鑰。由於採用多路徑協商，因此收發雙方可以獲取多個共享密鑰。例如，在圖 2 所示的例子中，通過兩條路徑的密鑰協商過程，量子密鑰分發設備 A1 和量子密鑰分發設備 B1 獲取了兩個共享密鑰 key1 和 key2。

對於獲取的兩個或者兩個以上的共享密鑰，收發雙方的量子密鑰協商設備可以採用預先設定的策略確定是否需要對所述協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

所述預先設定的策略，包括從安全性角度出發，依據密鑰協商過程中的誤碼率和/或風險機率來確定是否需要執行密鑰合併操作。在通過中繼方式進行密鑰協商的過程中，每兩個相鄰設備在協商過程中，都會對本次密鑰協商的誤碼率進行估算，還可以進一步計算可能存在的各種攻

擊(例如，強光致盲攻擊、光束分離攻擊、死時間攻擊等)的風險機率，並可以將每一條路徑的每一段中繼鏈路的誤碼率估計值和/或風險機率匯總起來，如果某一條路徑的上述資料超出了預先設定的安全範圍，則可以認爲該路徑的密鑰協商過程存在被攻擊的風險，中繼節點(即：本實施例所述的路由設備)也存在被攻破的安全隱患，因此在這種情況下，可以對協商得到的共享密鑰進行合併的方式，從而抵禦中繼節點被攻破帶來的風險，提高量子密鑰分發的安全性。

所述對協商得到的共享密鑰進行合併是指採用預先設定的算法，對通過多路徑協商得到的多個共享密鑰進行處理、生成新密鑰的過程。例如：可以對所述多個共享密鑰執行異或操作，或者先移位再執行異或操作等。具體採用何種合併算法，本實施例不做具體限定。

例如，在圖 2 所示的例子中，量子密鑰分發設備 A1 和 B1 通過路徑 1 協商得到共享密鑰 key1，通過路徑 2 協商得到共享密鑰 key2，通過將路徑 1 中的每一段中繼鏈路的誤碼率估計值和風險機率進行匯總後，計算出了表徵密鑰協商過程安全性的指標值，該指標值超出了預先設定的安全範圍，說明經由路徑 1 的密鑰協商過程可能受到攻擊，各中繼節點的安全性也存在隱患，而路徑 2 的相應指標值沒有超出所述安全範圍，因此量子密鑰分發設備 A1 和 B1 採用預先設定的異或算法對 key1 和 key2 執行合併操作，生成新的密鑰 key3，即：key3=key1 xor key2，並

採用 key3 對資料設備 A 與資料設備 B 之間傳輸的資料進行加解密。

在上述例子中，如果針對路徑 1 和路徑 2 匯總得到的安全指標值，都沒有超出預先設定的安全範圍，也就是說基於路徑 1 和路徑 2 的密鑰協商過程都是安全的，各中繼節點也是安全的，則可以不執行密鑰合併操作，那麼通過本次協商，量子密鑰分發設備 A1 和 B1 得到了兩個共享密鑰，並可以將這兩個密鑰用於資料設備 A 和 B 之間的保密通信。

透過上述分析可以看出，本實施例提供的量子密鑰分發系統，在網路安全性比較高的應用場景下，由於使用多條路徑進行密鑰協商，從而透過提高路由設備以及鏈路利用率，達到提高密鑰分發量的目的；在網路安全性比較低的應用場景下，即使其中有某一條或者幾條路徑的中繼節點被攻破，協商得到的相應密鑰不再安全，但只要其中有一條路徑是安全的(各中繼節點均沒有被攻擊)，仍然可以通過對不同路徑密鑰的合併操作生成新的、安全的共享密鑰，從而可以抵禦部分中繼節點被攻擊的安全隱患，提高整個量子密鑰分發網路的安全性。

需要說明的是，上述給出的是一個具體的例子，在其他實施方式中，可以進行相應的變更或者調整。例如，可以不採用匯總路徑中每條中繼鏈路的誤碼率以及風險機率，而是從中抽取某幾條鏈路進行匯總；也可以不採用誤碼率和/或風險機率作爲安全性的評估參數，而是採用其

工技術，達到多通道傳輸的目的，提高密鑰的分發量。所述分時多工技術是指採用同一物理連接的不同時段來傳輸不同的信號。分波多工和分時多工都屬於比較成熟的現有技術，此處不再贅述。

在本實施例提供的量子密鑰分發系統中，所述量子密鑰分發設備除了具備多路徑密鑰協商功能，還可以用於對在資料設備之間傳輸的資料進行加解密。在圖 2 所示的例子中，量子密鑰分發設備 A1 使用與 B1 協商得到的共享密鑰，對資料設備 A 發送的資料進行加密；加密後的資料通過各路由設備轉發給量子密鑰分發設備 B1，B1 同樣採用與 A1 協商的共享密鑰對接收到的資料進行解密，然後將解密後的資料發送給資料設備 B，從而完成了資料設備 A 與資料設備 B 之間的保密通信。

在其他實施方式中，也可以將對資料進行加解密的功能從量子密鑰分發設備中剝離出來，交由量子閘道完成。也就是說，在上述量子密鑰分發系統中，還可以包括量子閘道設備，量子密鑰分發設備通過量子閘道設備與資料設備相連。所述量子密鑰分發設備負責多路徑地進行密鑰協商，並將協商獲取的量子密鑰提供給與其相連的量子閘道設備，量子閘道設備則採用所述量子密鑰，對在所述資料設備之間傳輸的資料進行加解密。

在具體實施中，可以根據實際需要從上述兩種加解密方式中選擇其中一種。加密後的資料經由路由設備的轉發，最終到達對端的量子密鑰分發設備，並經解密後發送

給本次資料傳輸的目的端資料設備。在路由設備對加密資料進行轉發的過程中，可以採用現有的光塞取多工技術、光交叉互聯技術、光封包交換技術中的一種或者幾種，由於採用多路徑密鑰協商方式，提高了密鑰的分發量，因此加密資料的交互吞吐量也可以得到有效的提高。上述光傳輸技術屬於比較成熟的現有技術，下面對僅對其作簡要說明。

1)光塞取多工(Optical Add/Drop Multiplex, OADM)技術，一種用濾光器或分用器從分波多工傳輸鏈路插入或分出光信號的技術。在 WDM 系統中有選擇地上/下所需速率、格式和協議類型的光波長信號，即：在節點上只分接/插入所需的波長信號，其它波長信號則光學透明地通過這個節點；

2)光分叉互聯技術，用於光纖網路節點的設備，通過對光信號進行交叉連接，能够有效靈活地管理光纖傳輸網路，是實現可靠的網路保護/恢復以及自動配綫和監控的重要手段；

3)光封包交換技術，全光封包交換可分成兩大類：時隙和非時隙。在時隙網路中，封包長度是固定的，並在時隙中傳輸。時隙的長度應大於封包的時限，以便在封包的前後設置保護間隔。在非時隙網路中，封包的大小是可變的，而且在交換之前，不需要排列，非同步的，自由地交換每一個封包。

在具體實施中，所述量子密鑰分發系統，在進行密鑰

第 104127894 號　　民國 108 年 6 月 21 日修正

申請專利範圍

1.一種基於可信中繼的量子密鑰分發系統，其特徵在於，包括：量子密鑰分發設備、用於中繼密鑰和轉發加密資料的路由設備、以及用作資料傳輸的源端或目的端的資料設備；該每個量子密鑰分發設備與至少一個該路由設備相連，該每個量子密鑰分發設備與至少一個該資料設備相連，該路由設備彼此連接形成網狀拓撲；

其中，該量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商、並採用預先設定的策略確定是否需要對該協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

2.根據申請專利範圍第 1 項所述的基於可信中繼的量子密鑰分發系統，其中，該量子密鑰分發設備還用於在發起量子密鑰協商之前，將本次量子密鑰協商的路徑資訊發送給該路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，該路由設備和該接收方量子密鑰分發設備還用於根據接收到的路徑資訊，對與其進行密鑰協商的路由設備或量子密鑰分發設備的身份進行驗證。

3.根據申請專利範圍第 1 項所述的基於可信中繼的量子密鑰分發系統，其中，該每個量子密鑰分發設備與至少兩個該路由設備相連。

4.根據申請專利範圍第 3 項所述的基於可信中繼的量子密鑰分發系統，其中，該兩條或者兩條以上的不同路徑

是指其中任意兩條路徑都不包含相同的路由設備。

5.根據申請專利範圍第 1-4 項任一項所述的基於可信中繼的量子密鑰分發系統，其中，該量子密鑰分發設備所採用的兩條或者兩條以上的不同路徑，是根據負載均衡策略選擇的。

6.根據申請專利範圍第 1-4 項任一項所述的基於可信中繼的量子密鑰分發系統，其中，該量子密鑰分發設備還用於對在該資料設備之間傳輸的資料進行加解密。

7.根據申請專利範圍第 1-4 項任一項所述的基於可信中繼的量子密鑰分發系統，其中，該系統還包括：量子閘道設備，該量子密鑰分發設備通過該量子閘道設備與該資料設備相連，該量子閘道設備用於採用與其相連的量子密鑰分發設備提供的量子密鑰，對在該資料設備之間傳輸的資料進行加解密。

8.根據申請專利範圍第 1-4 項任一所述的基於可信中繼的量子密鑰分發系統，其中，該量子密鑰分發設備採用兩條或者兩條以上的不同路徑與對端量子密鑰分發設備進行密鑰協商包括，在該任一路徑中採用分波多工技術和/或分時多工技術，實現多量子通道的密鑰協商。

9.根據申請專利範圍第 1 項所述的基於可信中繼的量子密鑰分發系統，其中，該路由設備採用光塞取多工技術、光交叉互聯技術、和/或光封包交換技術，對採用量子密鑰加密後的資料進行轉發。

10.根據申請專利範圍第 1 項所述的基於可信中繼的

量子密鑰分發系統，其中，該量子密鑰分發系統部署於雲計算資料中心；

該資料設備是指雲計算資料中心的伺服器。

11.根據申請專利範圍第 10 項所述的基於可信中繼的量子密鑰分發系統，其中，該系統還包括：光交換機，該路由設備通過該光交換機與量子密鑰分發設備相連。

12.根據申請專利範圍第 10 項所述的基於可信中繼的量子密鑰分發系統，其中，該每個量子密鑰分發設備與複數個功能相同的伺服器相連；或者，該每個量子密鑰設備與複數個功能不同的伺服器相連。

13.根據申請專利範圍第 10-12 項任一項所述的基於可信中繼的量子密鑰分發系統，其中，該系統還包括：具有量子密鑰分發設備的雲使用商網路；該雲使用商網路的量子密鑰分發設備與該雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連；

該雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與該雲計算資料中心的對端量子密鑰分發設備進行密鑰協商、並採用該預先設定的策略確定是否需要對該協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

14.根據申請專利範圍第 13 項所述的基於可信中繼的量子密鑰分發系統，其中，該雲使用商網路的量子密鑰分發設備採用兩條或者兩條以上的不同路徑與該雲計算資料中心的對端量子密鑰分發設備進行密鑰協商包括，在該任

一路徑中採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商。

15.根據申請專利範圍第 13 項所述的基於可信中繼的量子密鑰分發系統，其中，該雲使用商網路的量子密鑰分發設備的數量爲兩個或者兩個以上，其中每個量子密鑰分發設備都與該雲計算資料中心的兩個或者兩個以上量子密鑰分發設備相連。

16.根據申請專利範圍第 1 項所述的基於可信中繼的量子密鑰分發系統，其中，該量子密鑰分發系統分別部署於分散式雲計算網路的多個資料中心，該資料設備是指各資料中心的伺服器，該多個資料中心之間通過量子密鑰分發設備相連形成網狀拓撲；

其中，該量子密鑰分發設備還用於採用兩條或者兩條以上的不同路徑與位於不同資料中心的對端量子密鑰分發設備進行密鑰協商，並採用該預先設定的策略確定是否需要對該協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

17.根據申請專利範圍第 16 項所述的基於可信中繼的量子密鑰分發系統，其中，還包括：具有量子密鑰分發設備的雲使用商網路，該雲使用商網路通過其量子密鑰分發設備與兩個或者兩個以上資料中心的量子密鑰分發設備相連；

該雲使用商網路的量子密鑰分發設備用於採用兩條或者兩條以上的不同路徑與該資料中心的對端量子密鑰分發

設備進行密鑰協商、並採用該預先設定的策略確定是否需要對該協商得到的共享密鑰進行合併、並在需要時執行相應的合併操作。

18.根據申請專利範圍第 17 項所述的基於可信中繼的量子密鑰分發系統，其中，該雲使用商網路的量子密鑰分發設備採用兩條或者兩條以上的不同路徑與該資料中心的對端量子密鑰分發設備進行密鑰協商包括：在該任一路徑中採用分波多工技術和/或分時多工技術實現多量子通道的密鑰協商。

19.一種基於可信中繼的量子密鑰分發方法，其特徵在於，該方法在如申請專利範圍第 1 項所述的量子密鑰分發系統中實施，包括：

發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商；

該發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過該密鑰協商過程獲取的共享密鑰進行合併操作；

若是，該發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

20.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，在進行該密鑰協商之前，執行下述操作：

該發送方量子密鑰分發設備根據量子密鑰分發系統的

拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

21.根據申請專利範圍第 20 項所述的基於可信中繼的量子密鑰分發方法，其中，該發送方量子密鑰分發設備在選擇該兩條或者兩條以上的不同路徑後，執行下述操作：

通過經典通道，將每條路徑資訊發送給該路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，在該密鑰協商過程中，該路徑包含的路由設備以及接收方量子密鑰分發設備執行如下操作：

根據接收到的該路徑資訊，對與其進行密鑰協商的對端設備的身份進行驗證；

若通過驗證，與該對端設備進行密鑰協商並完成本節點的密鑰中繼操作；

否則，通知該發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

22.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該採用兩條或者兩條以上的不同路徑進行密鑰協商，採用如下方式實現：

通過該路由設備的動態選路功能，實現經由兩條或者兩條以上的不同路徑進行該密鑰協商。

23.根據申請專利範圍第 22 項所述的基於可信中繼的量子密鑰分發方法，其中，在完成該密鑰協商之後，執行下述操作：

該發送方或接收方量子密鑰分發設備通過獲取本次密

鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的各個設備的身份合法性進行驗證；

若檢測到非法設備，則該發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

24.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該兩條或者兩條以上的不同路徑是指其中任意兩條路徑都不包含相同的路由設備。

25.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該兩條或者兩條以上的不同路徑是根據負載均衡策略選擇的。

26.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，在進行該密鑰協商之前，執行下述操作：

該發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證；若該對方設備未通過該身份驗證，則結束本方法的執行。

27.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過該密鑰協商過程獲取的共享密鑰進行合併操作，包括：

該量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果；

根據預先設定的策略及該安全評估結果，判斷是否需要執行該合併操作；

若是，執行下述操作：

選取執行密鑰合併操作的處理方式；

通過經典通道，與對端量子密鑰分發設備協商並確認該密鑰合併的處理方式；

轉到該發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作的步驟執行。

28.根據申請專利範圍第 19-27 項任一項所述的基於可信中繼的量子密鑰分發方法，其中，還包括：

該發送方量子密鑰分發設備使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給該接收方量子密鑰分發設備；

該接收方量子密鑰分發設備採用與該發送方相同的共享密鑰對接收到的資料進行解密。

29.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該方法應用於雲計算資料中心；該發送方和接收方量子密鑰分發設備是指與進行保密資料傳輸的源端和目的端伺服器分別相連的量子密鑰分發設備。

30.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該方法應用於由雲計算資料中心和雲使用商網路組成的系統中；

該發送方和接收方量子密鑰分發設備是指雲使用商網路的量子密鑰分發設備、以及與雲使用商網路進行保密資料傳輸的伺服器相連的量子密鑰分發設備，該伺服器位於

該雲計算資料中心內。

31.根據申請專利範圍第 19 項所述的基於可信中繼的量子密鑰分發方法，其中，該方法應用於由分散式雲計算資料中心和雲使用商網路組成的系統中；

該發送方和接收方量子密鑰分發設備是指與進行保密資料傳輸的源端和目的端伺服器相連的量子密鑰分發設備，該源端和目的端伺服器位於不同的雲計算資料中心；或者，

雲使用商網路的量子密鑰分發設備、以及與雲使用商進行保密資料傳輸的伺服器相連的量子密鑰分發設備，該伺服器位於該分散式雲計算資料中心內。

32.一種基於可信中繼的量子密鑰分發裝置，其特徵在於，包括：

多路徑協商單元，用於發送方量子密鑰分發設備通過路由設備的中繼、採用兩條或者兩條以上的不同路徑，與接收方量子密鑰分發設備進行密鑰協商；

合併判斷單元，用於該發送方或接收方量子密鑰分發設備根據預先設定的策略，判斷是否需要對通過該密鑰協商過程獲取的共享密鑰進行合併操作；

合併執行單元，用於當該合併判斷單元的輸出爲“是”時，該發送方和接收方量子密鑰分發設備分別執行相應的密鑰合併操作，生成新的共享密鑰。

33.根據申請專利範圍第 32 項所述的基於可信中繼的量子密鑰分發裝置，其中，該裝置還包括：

路徑獲取單元，用於在觸發該多路徑協商單元工作之前，該發送方量子密鑰分發設備根據量子密鑰分發系統的拓撲資訊，選擇與接收方量子密鑰分發設備進行密鑰協商的兩條或者兩條以上的不同路徑。

34.根據申請專利範圍第 33 項所述的基於可信中繼的量子密鑰分發裝置，其中，該裝置還包括：

路徑分發單元，用於在觸發該多路徑協商單元工作之前，發送方量子密鑰分發設備通過經典通道，將每條路徑資訊發送給該路徑包含的路由設備以及接收方量子密鑰分發設備；

相應的，該多路徑協商單元除了包括實現其功能的本體子單元外，還包括路徑驗證子單元，該路徑驗證子單元用於實現下述功能：該路徑包含的路由設備以及接收方量子密鑰分發設備，根據接收到的該路徑資訊，對與其進行密鑰協商的對端設備的身份進行驗證；若通過驗證，與該對端設備進行密鑰協商並完成本節點的密鑰中繼操作；否則，通知該發送方量子密鑰分發設備放棄相應路徑的密鑰協商過程。

35.根據申請專利範圍第 32 項所述的基於可信中繼的量子密鑰分發裝置，其中，該多路徑協商單元用於通過該路由設備的動態選路功能，實現經由兩條或者兩條以上的不同路徑進行該密鑰協商。

36.根據申請專利範圍第 35 項所述的基於可信中繼的量子密鑰分發裝置，其中，該裝置包括：

路徑驗證單元，用於在該多路徑協商單元執行完畢後，該發送方或接收方量子密鑰分發設備通過獲取本次密鑰協商的路徑資訊，對參與每一條路徑密鑰協商過程的各個設備的身份合法性進行驗證；若檢測到非法設備，則該發送方和接收方量子密鑰分發設備放棄經由相應路徑協商獲取的共享密鑰。

37.根據申請專利範圍第 32 項所述的基於可信中繼的量子密鑰分發裝置，其中，該裝置還包括：

身份驗證單元，用於在觸發該多路徑協商單元工作之前，該發送方和接收方量子密鑰分發設備通過經典通道，對對方設備進行身份驗證；若該對方設備未通過該身份驗證，則結束本方法的執行。

38.根據申請專利範圍第 32 項所述的基於可信中繼的量子密鑰分發裝置，其中，該合併判斷單元包括：

安全評估結果獲取子單元，用於該量子密鑰分發設備獲取經由每一條路徑進行密鑰協商的安全評估結果；

策略判斷子單元，用於該量子密鑰分發設備根據預先設定的策略及該安全評估結果，判斷是否需要執行該合併操作；

選擇協商子單元，用於該量子密鑰分發設備選取執行密鑰合併操作的處理方式，以及通過經典通道，與對端量子密鑰分發設備協商並確認該密鑰合併的處理方式，並觸發該合併執行單元工作。

39.根據申請專利範圍第 32-38 項任一項所述的基於可

信中繼的量子密鑰分發裝置，其中，該裝置還包括：

資料加密傳輸單元，用於該發送方量子密鑰分發設備使用最終獲取的共享密鑰對待傳輸資料進行加密，並經由路由設備轉發給該接收方量子密鑰分發設備；

資料解密單元，用於該接收方量子密鑰分發設備採用與該發送方相同的共享密鑰對接收到的資料進行解密。