I709870

(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 I709870 B**

(45)公告日： 中華民國 109 (2020) 年 11 月 11 日

(21)申請案號：105107428　(22)申請日： 中華民國 105 (2016) 年 03 月 10 日

(51)Int. Cl.：　*G06F21/31　(2013.01)*　*H04L9/32　(2006.01)*

H04L9/28　(2006.01)

(30)優先權：2015/08/18　中國大陸　201510509537.5

(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)

(74)代理人：林志剛

(56)參考文獻：

TW	I487308	US	2008/0144833A1
US	2009/0106553A1	US	2011/0170690A1
US	2013/0315395A1		

審查人員：張耕誌

申請專利範圍項數：22 項　圖式數：12　共 64 頁

(54)名稱

用於量子密鑰分發過程的身份認證方法、裝置及系統

(57)摘要

本發明揭示了一種用於量子密鑰分發過程的身份認證方法，同時揭示了另外兩種身份認證方法及相應裝置，以及一種身份認證系統。所述方法包括：發送方按照基矢選擇規則、選擇利用第一預定演算法產生的動態變化的發送方身份認證資訊的製備基，並發送包含密鑰資訊以及發送方身份認證資訊的量子態；接收方遵循所述基矢選擇規則而對發送方身份認證資訊量子態進行測量，若測量結果與採用第一預定演算法而得到的相應資訊不相符，則結束本次量子密鑰分發過程。採用本技術方案，可以實現在量子密鑰分發過程中對量子密鑰分發請求物件的動態身份認證，能夠防禦偽冒攻擊、中間人攻擊和拒絕服務攻擊，提高量子密鑰分發過程的安全性，同時可以避免對量子密鑰資源的浪費。

指定代表圖：

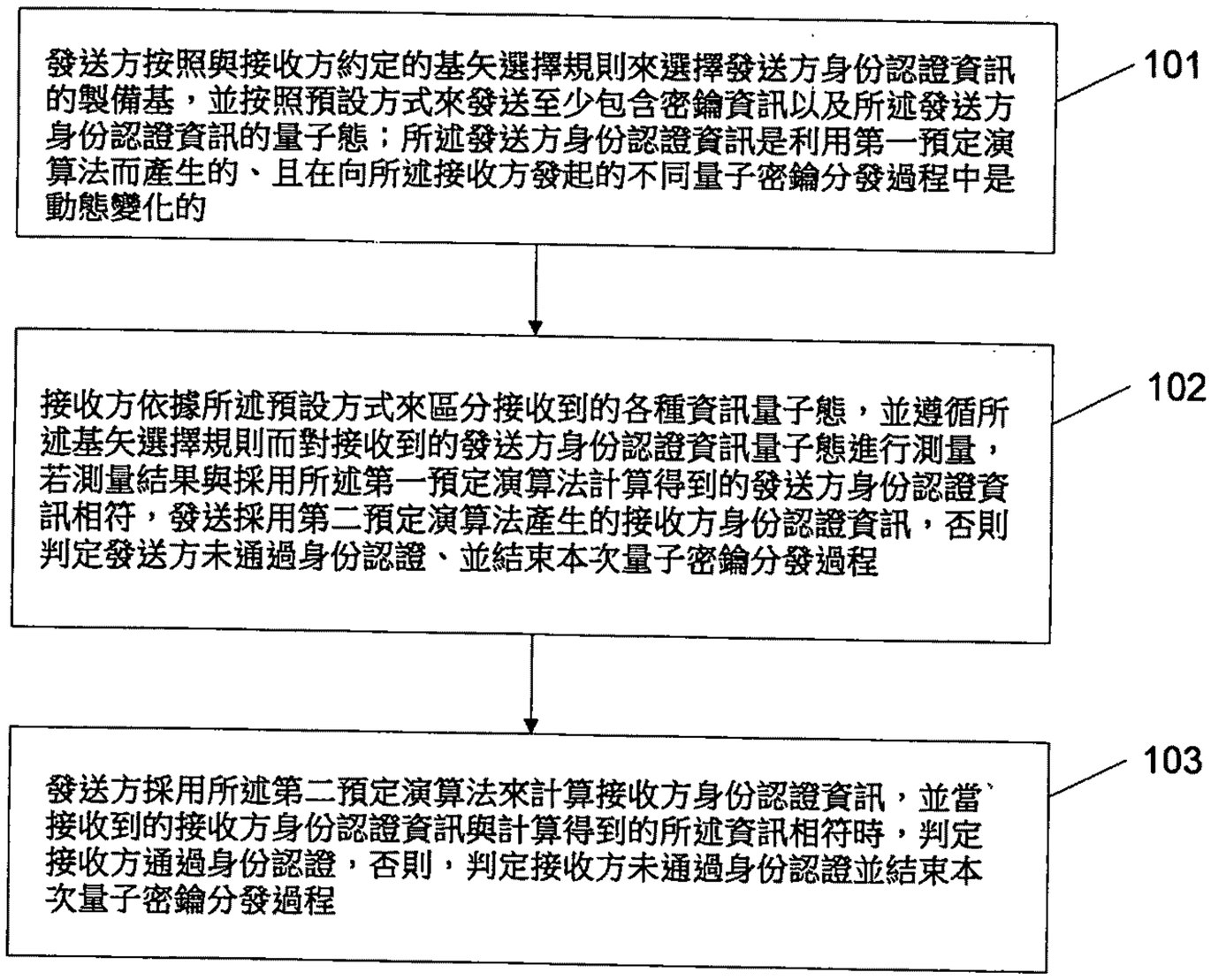
發送方按照與接收方約定的基矢選擇規則來選擇發送方身份認證資訊的製備基，並按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；所述發送方身份認證資訊是利用第一預定演算法而產生的、且在向所述接收方發起的不同量子密鑰分發過程中是動態變化的
101
接收方依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預定演算法計算得到的發送方身份認證資訊相符，發送採用第二預定演算法產生的接收方身份認證資訊，否則判定發送方未通過身份認證、並結束本次量子密鑰分發過程
102
發送方採用所述第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的所述資訊相符時，判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程
103

圖 1

公告本

I709870

發明摘要

※申請案號：105107428

※申請日：105 年 03 月 10 日　　**※IPC 分類：**

【發明名稱】(中文/英文)

用於量子密鑰分發過程的身份認證方法、裝置及系統

【中文】

本發明揭示了一種用於量子密鑰分發過程的身份認證方法，同時揭示了另外兩種身份認證方法及相應裝置，以及一種身份認證系統。所述方法包括：發送方按照基矢選擇規則、選擇利用第一預定演算法產生的動態變化的發送方身份認證資訊的製備基，並發送包含密鑰資訊以及發送方身份認證資訊的量子態；接收方遵循所述基矢選擇規則而對發送方身份認證資訊量子態進行測量，若測量結果與採用第一預定演算法而得到的相應資訊不相符，則結束本次量子密鑰分發過程。採用本技術方案，可以實現在量子密鑰分發過程中對量子密鑰分發請求物件的動態身份認證，能夠防禦偽冒攻擊、中間人攻擊和拒絕服務攻擊，提高量子密鑰分發過程的安全性，同時可以避免對量子密鑰資源的浪費。

【英文】

【代表圖】

【本案指定代表圖】：第(1)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

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)

用於量子密鑰分發過程的身份認證方法、裝置及系統

【技術領域】

本發明係有關身份認證技術，具體有關一種用於量子密鑰分發過程的身份認證方法。本發明同時有關另外兩種用於量子密鑰分發過程的身份認證方法及相應裝置，以及一種用於量子密鑰分發過程的身份認證系統。

【先前技術】

身份認證是確保網路安全的一個重要環節，透過認證可以保障通信雙方的真實性、消息的完整性和來源可靠性，以防止非法方對資訊進行偽造、修改和延遲等攻擊。密碼學中通常利用私鑰密碼機制和公鑰密碼機制來確保通信中身份資訊的安全性、完整性、不可否認性和抵抗身份冒充攻擊。

量子密碼作為量子力學和密碼學的交叉產物，其安全性係由量子力學基本原理來予以確保，而與攻擊者的計算能力和儲存能力無關，被證明具有無條件安全性和對竊聽者的可檢測性。然而，傳統的量子密鑰分配協議卻沒有提供有效的身份認證機制，因此可能在量子密鑰分配過程（也稱分發過程）中受到偽冒攻擊、中間人攻擊或者分散

式拒絕服務（Distributed Denial of Service-DDoS）攻擊。

針對上述問題，現有技術提出了如下兩種解決方案：

（一）M.Dusek 等認為在通信過程中不需要認證全部的經典資訊，僅需要對影響正確判斷量子態錯誤率的經典資訊進行認證，其他的經典資訊不需要認證。因此M.Dusek 提出了結合經典消息認證演算法的量子身份認證協定，其實質就是用經典的認證演算法對儘量少的經典消息進行認證。

（二）採用帶身份認證的 BB84 協定。該協定與原BB84 協定的主要不同點是將隨機發送的量子位元串中某些位元位設定為特定的認證位元，其具體的位置係由認證密鑰來予以決定，通過此認證位元的位元所代表的測量基矢以及光量子的偏振態來實現通信雙方的身份認證，認證位元的量子態資訊不可隨機發送，而應根據特定的規則由雙方共用的認證密鑰來予以決定。收發雙方透過將每次協商獲取的共用量子密鑰中的一部分設定為認證密鑰，從而實現認證密鑰的動態更新。

上述兩種方案由於都採用了身份認證機制，在一定程度上可以加強量子密鑰分發過程的安全性，但是各自都存在有一定的缺陷：

（一）M.Dusek 方案，通信雙方事先共用的認證密鑰數量有限，而且該方案沒有充分利用量子的優越性，依然採用的是經典認證技術，存在有被破解的風險，易遭受偽冒攻擊、中間人攻擊和 DDoS 攻擊。

（二）帶身份認證的 BB84 協定雖然將身份認證資訊以量子態形式來予以發送，提高了密鑰分發的安全性，但是該技術方案需要從每次協商獲取的共用量子密鑰中選取一部分作為認證密鑰，導致這部分量子密鑰無法用於業務資料加密，浪費量子密鑰資源。

【發明內容】

本發明實施例提出的一種用於量子密鑰分發過程的身份認證方法，不僅提供了一種在量子密鑰分發過程中進行動態身份認證的新思路，而且可以有效解決現有量子密鑰分發過程採用的身份認證機制存在的不安全、以及浪費量子密鑰資源的問題。本發明實施例還提供另外兩種用於量子密鑰分發過程的身份認證方法及相應裝置，以及一種用於量子密鑰分發過程的身份認證系統。

本發明提供一種用於量子密鑰分發過程的身份認證方法，所述方法在參與量子密鑰分發過程的收發雙方量子通信設備中實施，包括：

發送方按照與接收方約定的基矢選擇規則選擇發送方身份認證資訊的製備基，並按照預設方式發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態，所述發送方身份認證資訊是利用第一預定演算法產生的；

接收方依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預

定演算法所計算得到的發送方身份認證資訊相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程；

其中，所述利用第一預定演算法產生的發送方身份認證資訊，在向所述接收方發起的不同量子密鑰分發過程中是動態變化的。

可選地，在接收方判定發送方通過身份認證之後，執行下述操作：

接收方利用第二預定演算法來產生接收方身份認證資訊，並發送所述接收方身份認證資訊；

發送方採用所述第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的所述資訊相符時，判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

可選地，接收方在判定發送方通過身份認證之後，還執行下述操作：

隨機選擇測量基對接收到的密鑰資訊量子態進行測量，並透過經典通道公佈所述測量基；

相應地，發送方在判定接收方通過身份認證之後，執行下述操作：

確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

透過經典通道來公佈所述密鑰資訊量子態的正確測量基；

相應地，在上述發送方公佈所述密鑰資訊量子態的正

確測量基的步驟之後，執行下述操作：

接收方篩選原始密鑰；以及，

收發雙方透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

可選地，所述第一預定演算法包括：根據發送方標識資訊以及收發雙方按照預設策略同步變換的參數，計算發送方身份認證資訊；接收方一側的發送方標識資訊是預定的、或者由發送方透過經典通道發送給接收方的。

可選地，在所述發送方按照與接收方約定的基矢選擇規則來選擇發送方身份認證資訊的製備基之前，執行下述操作：

收發雙方在透過經典通道執行的發起請求交互流程中，利用所述按照預設策略同步變換的參數與對端設備相互進行身份驗證，若其中任一設備未通過所述身份驗證，則不啟動量子密鑰分發過程。

可選地，所述第二預定演算法包括：根據接收方標識資訊以及收發雙方按照預設策略同步變換的參數的變體，計算接收方身份認證資訊；發送方一側的接收方標識資訊是預定的、或者由接收方透過經典通道而發送給發送方的。

可選地，所述按照預設策略同步變換的參數的變體，包括：

所述參數本身；或者，

採用預設的數學變換方法來處理所述參數得到的結

果。

可選地，所述收發雙方按照預設策略同步變換的參數包括：收發雙方執行量子密鑰分發過程的次數。

可選地，計算身份認證資訊包括：採用散列函數來計算相應身份認證資訊。

可選地，所述按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態，包括：

按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊的量子態，所述資料資訊包括：所述密鑰資訊和所述發送方身份認證資訊。

可選地，所述預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

可選地，承載作為身份認證資訊首碼的控制資訊量子態的波長、與承載作為密鑰資訊首碼的控制資訊量子態的波長不同。

可選地，所述預設資訊格式包括：作為身份認證資訊首碼的控制資訊與作為密鑰資訊首碼的控制資訊分別採用不同編碼；

所述不同編碼是收發雙方預先設定的、或者透過經典通道而預先協商確定的；收發雙方用來製備或者測量控制資訊量子態的基矢是收發雙方預先設定的、或者透過經典通道而預先協商確定的。

可選地，所述預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密

鑰資訊之間的身份認證資訊的長度是收發雙方預先設定的、或者透過經典通道而預先協商確定的。

此外，本發明還提供一種用於量子密鑰分發過程的身份認證方法，所述方法在參與量子密鑰分發過程的發送方量子通信設備上實施，包括：

利用第一預定演算法來產生發送方身份認證資訊；

按照與參與量子密鑰分發過程的對端設備約定的基矢選擇規則、選擇所述發送方身份認證資訊的製備基；

按照預設方式而向所述對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；

其中，所述利用第一預定演算法來產生的發送方身份認證資訊，在向所述對端設備發起的不同量子密鑰分發過程中是動態變化的。

可選地，在所述按照預設方式而向參與量子密鑰分發過程的對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態之後，執行下述操作：

接收所述對端設備返回的資訊，所述資訊至少包括接收方身份認證資訊；

採用第二預定演算法來計算接收方身份認證資訊；

判斷接收到的接收方身份認證資訊是否與計算得到的所述資訊相符；若相符，則判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

可選地，所述對端設備返回的資訊不僅包括：所述接

收方身份認證資訊，還包括：測量密鑰資訊量子態所採用的測量基；

相應地，在判定接收方通過身份認證之後，執行下述操作：

確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

透過經典通道來公佈所述密鑰資訊量子態的正確測量基；

透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

可選地，所述第一預定演算法包括：根據宿主設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數，計算發送方身份認證資訊。

可選地，所述第二預定演算法包括：根據所述對端設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數的變體，計算接收方身份認證資訊。

可選地，所述與所述對端設備按照預設策略同步變換的參數包括：與所述對端設備執行量子密鑰分發過程的次數。

可選地，計算身份認證資訊包括：採用散列函數計算相應身份認證資訊。

可選地，所述按照預設方式發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態，包括：

按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊的量子態，所述資料資訊包括：所述密鑰

資訊和所述發送方身份認證資訊。

可選地，所述預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

可選地，所述預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是預先設定的、或者與所述對端設備透過經典通道預先協商確定的。

相應地，本發明還提供一種用於量子密鑰分發過程的身份認證裝置，所述裝置係部署在參與量子密鑰分發過程的發送方量子通信設備上，包括：

發送方身份資訊產生單元，用以利用第一預定演算法來產生發送方身份認證資訊，所述發送方身份認證資訊，在向所述接收方發起的不同量子密鑰分發過程中是動態變化的；

製備基選擇單元，用以按照與參與量子密鑰分發過程之對端設備約定的基矢選擇規則、選擇所述發送方身份認證資訊的製備基；

量子態發送單元，用以按照預設方式而向所述對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態。

可選地，所述裝置還包括：

接收方身份資訊接收單元，用以在所述量子態發送單元完成量子態發送操作後，接收所述對端設備返回的資訊，所述資訊至少包括接收方身份認證資訊；

接收方身份資訊計算單元，用以採用第二預定演算法來計算接收方身份認證資訊；

接收方身份驗證單元，用以判斷接收到的接收方身份認證資訊是否與計算得到的所述資訊相符；若相符，則判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

可選地，所述接收方身份資訊接收單元接收的資訊不僅包括：所述接收方身份認證資訊，還包括：所述對端設備測量密鑰資訊量子態所採用的測量基；

相應地，所述裝置包括：

原始密鑰篩選單元，用以當所述接收方身份驗證單元判定接收方通過認證之後，確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

正確測量基公佈單元，用以透過經典通道來公佈所述密鑰資訊量子態的正確測量基；

共用量子密鑰產生單元，用以透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

可選地，所述發送方身份資訊產生單元所採用的第一預定演算法包括：根據宿主設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數，計算發送方身份認證資訊。

可選地，所述接收方身份資訊計算單元所採用的第二預定演算法包括：根據所述對端設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數的變體，計算接

收方身份認證資訊。

可選地，所述發送方身份資訊產生單元和所述接收方身份資訊計算單元進行計算時所採用的所述按照預設策略同步變換的參數包括：與所述對端設備執行量子密鑰分發過程的次數。

可選地，所述發送方身份資訊產生單元或所述接收方身份資訊計算單元具體用於，採用散列函數計算相應身份認證資訊。

可選地，所述量子態發送單元具體用於，按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊的量子態，所述資料資訊包括：所述密鑰資訊和所述發送方身份認證資訊。

可選地，所述量子態發送單元所採用的預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

可選地，所述量子態發送單元所採用的預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是預先設定的、或者與所述對端設備透過經典通道預先協商確定的。

此外，本發明還提供一種用於量子密鑰分發過程的身份認證方法，所述方法在參與量子密鑰分發過程的接收方量子通信設備上實施，包括：

接收參與量子密鑰分發過程之對端設備發送的量子

態，並根據與所述對端設備相同的預設方式來區分接收到的各種資訊量子態；

採用與所述對端設備相同的第一預定演算法來計算發送方身份認證資訊；

按照與所述對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量；

判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

可選地，在判定發送方通過身份認證之後，執行下述操作：

採用與所述對端設備相同的第二預定演算法來產生接收方身份認證資訊；

向所述對端設備發送所述接收方身份認證資訊。

可選地，在判定發送方通過身份認證之後，還執行下述操作：

隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道公佈所述測量基；

接收所述對端設備透過經典通道而發送的所述密鑰資訊量子態的正確測量基；

篩選原始密鑰，並透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

相應地，本發明還提供一種用於量子密鑰分發過程的身份認證裝置，所述裝置係部署在參與量子密鑰分發過程

的接收方量子通信設備上，包括：

量子態接收區分單元，用以接收參與量子密鑰分發過程之對端設備發送的量子態，並根據與所述對端設備相同的預設方式來區分接收到的各種資訊量子態；

發送方身份資訊計算單元，用以採用與所述對端設備相同的第一預定演算法來計算發送方身份認證資訊；

身份資訊量子態測量單元，用以按照與所述對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量；

發送方身份驗證單元，用以判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

可選地，所述裝置還包括：

接收方身份資訊產生單元，用以在所述發送方身份驗證單元判定發送方通過身份認證之後，採用與所述對端設備相同的第二預定演算法來產生接收方身份認證資訊；

接收方身份資訊發送單元，用以向所述對端設備發送所述接收方身份認證資訊。

可選地，所述裝置還包括：

密鑰資訊量子態測量基公佈單元，用以在所述發送方身份驗證單元判定發送方通過身份認證之後，隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道來公佈所述測量基；

正確測量基接收單元，用以接收所述對端設備透過經典通道而發送的所述密鑰資訊量子態的正確測量基；

篩選及共用量子密鑰產生單元，用以篩選原始密鑰，並透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

此外，本發明還提供一種用於量子密鑰分發過程的身份認證系統，包括：根據上述任意一項所述之部署於發送方量子通信設備的身份認證裝置、以及根據上述任意一項所述之部署於接收方量子通信設備的身份認證裝置。

與現有技術相比，本發明具有以下優點：

本發明提供的一種用於量子密鑰分發過程的身份認證方法，發送方按照與接收方約定的基矢選擇規則、選擇利用第一預定演算法產生的發送方身份認證資訊的製備基，並按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；接收方依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預定演算法計算得到的發送方身份認證資訊相符，則判定發送方通過身份認證，否則判定發送方未通過身份認證並結束本次量子密鑰分發過程。上述技術方案，由於發送方採用量子態形式發送之利用第一預定演算法而產生的發送方身份認證資訊、在向所述接收方發起的不同量子密鑰分發過程中是動態變化的，接收方則通過相同的預定演算法而對接收到的身份認證資訊進行驗證，

從而實現在量子密鑰分發過程中對量子密鑰分發請求物件的動態身份認證，既能夠有效防禦對接收方的偽冒攻擊、中間人攻擊和拒絕服務攻擊，提高量子密鑰分發過程的安全性，同時由於採用演算法來動態產生身份認證資訊，可以避免對量子密鑰資源的浪費。

【圖式簡單說明】

圖 1 是本發明提供之一種用於量子密鑰分發過程的身份認證方法的實施例的流程圖；

圖 2 是本發明實施例提供之發送方發送包含身份認證資訊和密鑰資訊的量子態的處理流程圖；

圖 3 是本發明實施例提供之第一種資訊格式的示意圖；

圖 4 是本發明實施例提供之第二種資訊格式的示意圖；

圖 5 是本發明實施例提供之第三種資訊格式的示意圖；

圖 6 是本發明實施例提供之接收方執行身份認證操作的處理流程圖；

圖 7 是本發明提供之另一種用於量子密鑰分發過程的身份認證方法的實施例的流程圖；

圖 8 是本發明提供之一種用於量子密鑰分發過程的身份認證裝置的實施例的示意圖；

圖 9 是本發明提供之第三種用於量子密鑰分發過程的

身份認證方法的實施例的流程圖；

圖 10 是本發明提供之一種用於量子密鑰分發過程的身份認證裝置的實施例的示意圖；

圖 11 是本發明提供之一種用於量子密鑰分發過程的身份認證系統的實施例示意圖；

圖 12 是本發明實施例提供之身份認證系統的交互處理流程示意圖。

【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發明。但是，本發明能夠以很多不同於在此描述的其他方式來實施，本領域技術人員可以在不違背本發明之內涵的情況下做類似地推廣，因此，本發明不受下面所揭示之具體實施的限制。

在本發明中，分別提供了一種用於量子密鑰分發過程的身份認證方法、另外兩種用於量子密鑰分發過程的身份認證方法以及相應裝置、以及一種用於量子密鑰分發過程的身份認證系統，在下面的實施例中逐一進行詳細說明。

請參考圖 1，其為本發明之一種用於量子密鑰分發過程的身份認證方法的實施例的流程圖，所述方法在參與量子密鑰分發過程的收發雙方量子通信設備中予以實施。在詳細描述本實施例的具體步驟之前，先對有關本實施例的收發雙方量子通信設備以及本實施例作簡要說明。

本實施例在量子密鑰分發過程中動態地對參與分發過

程的量子通信設備的身份進行驗證。其中，選取製備基而向對端設備發送量子態的設備，亦即，通常所述的 Alice 一方（也稱為量子密鑰分發過程的發起方或請求方），在本技術方案中稱為發送方量子通信設備，簡稱發送方；選取測量基而對接收到的量子態進行測量的設備，亦即，通常所述的 Bob 一方，在本技術方案中稱為接收方量子通信設備，簡稱接收方。

量子密鑰分發過程包括：發送方發送量子態、接收方測量量子態、收發雙方比對測量基並篩選原始密鑰、估算位元錯誤率、錯誤更正、隱私放大這樣幾個階段，本技術方案在上述過程中實現動態身份認證。在具體實施本技術方案時，發送方在發送包含密鑰資訊和身份認證資訊的量子態後，接收方可以透過測量身份驗證資訊量子態來驗證發送方的身份，從而避免遭受偽冒攻擊、中間人攻擊或者 DDoS 攻擊，在實現上述單向認證功能的基礎上，發送方還可以根據接收方提供的身份認證資訊而對接收方身份進行驗證，避免遭受“釣魚式攻擊”，從而實現更為安全的雙向身份認證功能。

由此可見，雙向認證是本技術方案的較佳實施方式，在下面的實施例將重點描述該方式。需要說明的是，在具體實施本技術方案時，也可以僅執行接收方對發送方的單向身份驗證，同樣可以取得提高安全性、避免浪費量子密鑰資源的有益效果。

此外，在具體實施本技術方案時，可以在完成身份認

證後再繼續後續的測量密鑰資訊量子態、比對測量基等各階段的處理流程；也可以將相互驗證身份的處理過程穿插在各階段中完成。其中，第二種方式可以簡化交互過程，提高執行效率，是較佳實施方式，因此下面的實施例中描述基於上述第二種方式的實施方式。下面對本實施例作詳細說明。

所述用於量子密鑰分發過程的身份認證方法包括如下步驟：

步驟 101、發送方按照與接收方約定的基矢選擇規則來選擇發送方身份認證資訊的製備基，並按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；所述發送方身份認證資訊是利用第一預定演算法而產生的、且在向所述接收方發起的不同量子密鑰分發過程中是動態變化的。

為了避免在不合法的量子通信設備之間啟動量子密鑰分發過程，本實施例提供了一種較佳實施方式：在發送方啟動量子密鑰分發過程之前，收發雙方的量子通信設備先透過經典通道而對對端設備的身份進行驗證，只有雙方設備都通過驗證，才能夠啟動後續的量子密鑰分發過程。

在本技術方案中，發送方透過執行第一預定演算法來產生發送方身份認證資訊，該身份認證資訊對於不同的量子密鑰分發過程來說，是動態變化的。為了實現此一功能，在本實施例中，收發雙方可以各自維護按照預設策略同步變換的參數 n（相關說明請參見後續步驟 101-1 中的

有關文字），收發雙方可以利用所述參數 n 來實現上述基於經典通道的身份驗證過程。

例如，量子密鑰分發過程的請求方，亦即，本發明所述的發送方，可以首先發送量子密鑰協商請求，所述請求中包含由發送方的標識資訊 userid_A（關於標識資訊的說明參見後續步驟 101-1 中的有關文字）和所述參數 n 而計算得到的散列值 hash(userid_A, n)。參與量子密鑰分發過程的對端設備，亦即，本發明所述的接收方接收到上述資訊後，計算本地預定的 userid_A 和本地維護的所述參數 n 的散列值，若與接收到的值一致，則向發送方返回回應資訊，並在其中包含散列值 hash(userid_B, n)，否則結束本次量子密鑰分發過程。同樣的道理，所述發送方也可以採用同樣的方式而對接收方身份進行驗證，若通過驗證，則可以啟動量子密鑰分發過程，否則，不啟動。

上述描述的實施方式中，採取了收發雙方都預定對方標識資訊的方式，在其他實施方式中，收發雙方也可以不預定對方標識資訊，而是採用在上述量子密鑰分發過程的請求交互流程中攜帶標識資訊的方式，例如：發送方發送的資訊包括 hash(userid_A, n)和 userid_A；接收方返回的回應資訊包括 hash(userid_B, n)和 userid_B，透過這種方式收發雙方也可以獲知對方的標識資訊。

若發送方和接收方都通過了上述身份驗證過程，則啟動後續的量子密鑰分發過程，由發送方向接收方發送至少包含身份認證資訊和密鑰資訊的量子態，處理過程包括步

驟 101-1 至 101-3，下面結合附圖 2 作進一步說明。

步驟 101-1、利用第一預定演算法產生發送方身份認證資訊。

在本技術方案中，收發雙方預定相同的用於計算發送方身份認證資訊的演算法，亦即，本發明所述的第一預定演算法，透過該演算法而產生的發送方身份認證資訊，對於向所述接收方發起的不同量子密鑰分發過程來說是動態變化的，也就是說，對於所述接收方來說，其接收到的各請求物件所攜帶的身份認證資訊是動態變化的，接收方可以根據第一預定演算法而對請求物件進行身份驗證，而攻擊者則難以類比該動態變化的身份認證資訊，因此接收方可以有效防禦偽冒攻擊、中間人攻擊或者是 DDoS 攻擊。

在具體實施中，可以根據需要來設計所需的第一預定演算法，只要能夠滿足上述動態變化的要求即可，在本實施例中採用如下所述的第一預定演算法：根據發送方標識資訊 userid_A 以及收發雙方按照預設策略同步變換的參數 n，計算所述發送方身份認證資訊。

所述發送方標識資訊 userid_A，通常是指能夠將所述發送方與其他量子通信設備相區分的標識資訊，例如，可以採用出廠時所帶的設備標識、也可以採用發送方的固定 IP 位址等都是可以的（下文涉及的接收方標識資訊 userid_B 也可以採用同樣的標識方式，不再贅述）。

所述參數 n，則可以是收發雙方按照相同的預設策略同步變換的一個數值，亦即：收發雙方可以推知的變數，

例如：收發雙方可以預定同一個初始數值，然後按照預設週期而定期對各自維護的該數值進行同步變換，也可以在每次啟動量子密鑰分發過程之前觸發一次同步變換。所述同步變換方式則可以採用加、減、乘、除等基本運算或者預設函數來予以實現。由於 n 設定在收發雙方本地，不需雙方協商，且 n 是個動態變化值，因此被洩露或被猜測出來的概率很小，從而確保了身份認證資訊的安全性。

在本實施例中，所述發送方身份認證資訊 Y 可以由以下第一預定演算法所計算得到：Y = f(userid_A, n)，收發雙方採用相同的函數 f，例如可以採用散列函數。其中，發送方可以透過調用本地函數介面等方式而獲知自己的標識資訊 userid_A，而接收方一側的 userid_A 資訊則可以是預定的，也可以由發送方透過經典通道而發送給接收方，例如在啟動量子密鑰分發過程之前的協商請求階段發送該資訊（發送方一側的 userid_B 資訊也可以採用同樣的方式來獲取）。

由此可見，在上述第一預定演算法中，userid_A 是收發雙方可預知的，收發雙方的參數 n 也是可推知的，因此對於收發雙方來說，在某一次量子密鑰分發過程中，採用第一預定演算法而計算得到的發送方身份認證資訊是確定的，發送方在量子態中包含該資訊，接收方則可以利用該資訊而對發送方身份進行驗證。由於標識資訊所具有的區別能力以及 n 值的動態變換，使得接收方可以有效防禦偽冒攻擊、中間人攻擊或者是 DDoS 攻擊。

在上述提供的第一預定演算法的基礎上，本實施例還提供一種較佳實施方式，可以用收發雙方執行量子密鑰分發過程的次數作為所述參數 n 的值，例如，收發雙方將參數 n 的初始值設定為 0，收發雙方第一次啟動量子密鑰分發過程時，雙方將各自維護的 n 值設定為 1，第二次啟動量子密鑰分發過程時則各自將 n 值設定為 2，.....，以此類推，從而實現了收發雙方 n 值的同步變換。在具體實施時，當 n 值累計到某一預設的上限值時，收發雙方可同步清零，重新累計。

採用上述較佳實施方式，對於同一個接收方來說，由於不同的量子密鑰分發請求物件（亦即，本發明所述的發送方）的標識資訊是肯定不同的，因此，各請求物件在量子密鑰分發過程中提供的發送方身份認證資訊不同；而同一個量子密鑰分發請求物件，因為 n 值是根據量子密鑰分發過程的次數而變化的，因此其在不同量子密鑰分發過程中提供的發送方身份認證資訊也是不同的。在這種情況下，接收方可以更為安全地驗證請求方身份資訊，可以更為有效地防禦偽冒攻擊、中間人攻擊或者是 DDoS 攻擊。

在具體實施中，除了可以採用本實施例給出的基於標識資訊和參數 n 的第一預定演算法，也可以採用其他形式的第一預定演算法，例如：可以在收發雙方之間預定相同的亂數、不同的收方雙方預定不同的亂數，並採用所述亂數來代替標識資訊也可以實現本發明的技術方案。

步驟 101-2、按照與接收方約定的基矢選擇規則來選

擇所述發送方身份認證資訊的製備基。

由於收發雙方採用相同的第一預定演算法來計算發送方身份認證資訊，發送方採用量子態來發送該資訊，接收方則用該資訊而對發送方身份進行驗證。因此，收發雙方可以在透過計算而獲知發送方身份認證資訊的基礎上，按照預先約定好的基矢選擇規則來選擇相應的製備基或者測量基。

所述預先約定的基矢選擇規則，可以是收發雙方預先設定的、也可以是在啟動量子密鑰分發過程之前透過經典通道而協商確定的。例如：發送方採用水準偏振和垂直偏振兩種方向的製備基矢，接收方採用線偏振測量基進行測量；或者，發送方採用左旋偏振和右旋偏振兩種方向的製備基矢，接收方採用圓偏振測量基來進行測量；或者，對於位元 0，發送方採用水準偏振方向的製備基矢，接收方採用線偏振測量基，對於位元 1，發送方採用左旋偏振方向的製備基矢，接收方採用圓偏振測量基。

發送方按照預先約定好的基矢選擇規則，為在步驟 101-1 中產生的發送方身份認證資訊對應的位元串，選擇相應的製備基。

步驟 101-3、按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態。

所述預設方式可以是收發雙方預先設定的，發送方按照該方式來發送量子態，接收方則按照該方式來區分各種資訊量子態，例如：發送方可以採用不同波長來發送所述

發送方身份認證資訊和隨機產生的密鑰資訊的量子態，接收方則根據所述不同波長來進行區分。

較佳地，為了提供進一步的安全保障，避免攻擊者進行有針對性的監測，可以採用相同波長來發送所述發送方身份認證資訊和密鑰資訊的量子態（可以統稱為資料資訊的量子態），為了便於接收方進行區分，可以引入控制資訊作為所述發送方身份認證資訊和密鑰資訊的首碼。出於上述考慮，在本實施例中發送方按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊（包括密鑰資訊和發送方身份認證資訊）的量子態，接收方則按照波長特徵以及所述資訊格式來區分接收到的各種資訊量子態。所述不同波長可以是收發雙方預先設定的，也可以是在啟動量子密鑰分發過程之前透過經典通道而協商確定的。

所述資訊格式可以採用多種定義方式，只要接收方能夠正確區分就都是可以的。下面給出幾種具體的例子。

例 1：發送方身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼（以下分別簡稱為：身份認證控制資訊和密鑰控制資訊），且承載兩種控制資訊量子態的波長不同，請參見圖 3 給出的資訊格式示意圖。承載資料資訊（包括發送方身份認證資訊和密鑰資訊）量子態的波長為 λ_1，承載身份認證控制資訊量子態的波長為 λ_2，承載密鑰控制資訊量子態的波長為 λ_3，λ_1、λ_2 及 λ_3 都互不相同。其中，λ_2 和 λ_3 可以是收發雙方預先設定的、也可以是在啟動量子密鑰協商過程之前協商確定的。採用這種方

式，發送方可以隨機選擇兩類控制資訊的量子態，而接收方則可以直接根據波長來區分身份認證控制資訊和密鑰控制資訊。

例 2：發送方身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼，且兩種控制資訊編碼不同，請參見圖 4 給出的資訊格式示意圖。承載資料資訊（包括發送方身份認證資訊和密鑰資訊）量子態的波長為 λ_1，承載身份認證控制資訊量子態的波長、與承載密鑰控制資訊量子態的波長都為 λ_2（不同於 λ_1），但是兩類控制資訊的編碼不同，例如，00000 為身份認證控制資訊的編碼，11111 為密鑰控制資訊的編碼。其中，所述不同編碼是收發雙方預先設定的、或者在啟動量子密鑰分發過程之前透過經典通道而協商確定的；收發雙方用於製備或者測量上述兩種控制資訊量子態的基矢也可以是收發雙方預先設定的、或者是在啟動量子密鑰分發過程之前透過經典通道而協商確定的。

例 3：發送方身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，請參見圖 5 給出的資訊格式示意圖。承載資料資訊（包括發送方身份認證資訊和密鑰資訊）量子態的波長為 λ_1，發送方身份認證資訊和密鑰資訊共用同一個控制資訊首碼，承載控制資訊量子態的波長為 λ_2，λ_2 不同於 λ_1。採用這種方式，由於接收方可以根據波長來區分控制資訊和資料資訊，發送方可以隨機選擇控制資訊量子態，然而位於控制資訊和密鑰資訊之間的發送方身

份認證資訊的長度應該是收發雙方約定好的，這樣接收方才能夠正確區分資料資訊中的發送方身份認證資訊和密鑰資訊，在具體實施時，所述發送方身份認證資訊的長度可以是收發雙方預先設定的，也可以是在啟動量子密鑰分發過程之前透過經典通道而協商確定的。

需要說明的是，上面給出的例子以及相關圖示中，給出的都只是資訊格式的一部分，在具體實施時，每種資訊格式可以多次重複並串接在一起。例如，對於例 3 中給出的資訊格式，可以擴展為：控制資訊|發送方身份認證資訊|密鑰資訊|.....|控制資訊|發送方身份認證資訊|密鑰資訊。

在本實施例提供的上述較佳實施方式中，發送方按照與接收方約定好的波長特徵和資訊格式，發送控制資訊、發送方身份認證資訊以及密鑰資訊的量子態。為了便於理解，下面採用上述例子 3 中的資訊格式舉例說明。

例如，發送方在時間點 t_1、t_2...t_n 發送長度為 n 的二進位位元串的量子態，所述二進位位元串如下所示：

$$x_1, x_2 \cdots x_i, x_{i+1} \cdots x_{i+m}, x_{i+m+1} \cdots x_n$$

該二進位位元串包含三部分，第一部分是控制資訊位元串，第二部分是身份認證資訊位元串，第三部分是密鑰資訊位元串。其中，控制資訊位元串為隨機選擇的二進位位元串，長度為 i；身份認證資訊位元串則是在步驟 101-

1 中利用第一預定演算法而產生的發送方身份認證資訊位元串，其長度 m 可以由發送方和接收方預先透過經典通道而協商確定；密鑰資訊位元串是隨機產生的二進位位元串，其長度為 n-m-i。

發送方在時間點 t_1、t_2、..... t_n 發送上述二進位位元串的編碼量子態

$$(\ |\varphi_{j_1}^{x_1}, |\varphi_{j_2}^{x_2} \cdots |\varphi_{j_i}^{x_i}, |\varphi_{j_i+1}^{x_{i+1}} \cdots |\varphi_{j_i+m}^{x_{i+m}}, |\varphi_{j_i+m+1}^{x_{i+m+1}} \cdots |\varphi_{j_n}^{x_n} \ )$$

給接收方，$j_1, j_2, \cdots j_i, j_{i+1} \cdots j_{i+m}, j_{i+m+1}, \cdots j_n$是發送方採用的製備基序列，其中，$j_1, j_2, \cdots j_i$是控制資訊位元串對應的隨機量子態製備基，波長為 λ_2，是按照收發雙方約定的基矢選擇規則而選取的身份認證資訊位元串的量子態製備基，$j_{i+m+1}, \cdots j_n$是密鑰資訊位元串對應的隨機量子態製備基，身份認證資訊位元串和密鑰資訊位元串的製備基的波長都為 λ_1，λ_1與 λ_2不同。

相應地，接收方可以根據波長來區分控制資訊和資料資訊，根據長度 m 來區分資料資訊中的發送方身份認證資訊和密鑰資訊，並採用測量基序列 $k_{i+1} \cdots k_{i+m}, k_{i+m+1} \cdots k_n$ 而對接收到的資料資訊量子態進行測量，其中，$k_{i+1} \cdots k_{i+m}$ 為發送方身份認證資訊量子態對應的測量基，該測量基是遵循與發送方預先約定的基矢選擇規則所選取的，$k_{i+m+1}, \cdots k_n$為密鑰資訊量子態對應的隨機量子態測量基。

至此，透過步驟 101-1 至 101-3，發送方完成了量子態的發送操作。在該過程中，由於發送方採用第一預定演算法而產生了發送方身份認證資訊，且所述發送方身份認

證資訊在向所述接收方發起的不同量子密鑰分發過程中並不是固定不變的、而是動態變化的，從而為接收方防禦各種可能的偽冒攻擊、中間人攻擊或者 DDOS 攻擊提供了保障。

步驟 102：接收方依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預定演算法計算得到的發送方身份認證資訊相符，發送採用第二預定演算法產生的接收方身份認證資訊，否則判定發送方未通過身份認證、並結束本次量子密鑰分發過程。

在具體實施本技術方案時，接收方透過對接收到的發送方身份認證資訊量子態的測量，驗證發送方的身份，若發送方未通過驗證，則結束本次量子密鑰分發過程，否則可以執行測量密鑰資訊量子態等後續操作。

較佳地，在實現上述單向認證功能的基礎上，接收方還可以將自己的身份資訊提供給發送方供其驗證，透過這種方式，發送方可以避免遭受“釣魚式攻擊”以及其他可能的攻擊，從而實現更為安全的雙向身份認證功能。上述較佳實施方式的具體處理過程包括步驟 102-1 至 102-5，下面結合圖 6 作進一步說明。

步驟 102-1、依據所述預設方式來區分接收到的各種資訊量子態。

在本步驟中，接收方針對從量子通道接收到的各種資

訊量子態，採用與發送方預先約定好的預設方式來區分其中的發送方身份認證資訊以及密鑰資訊等資訊的量子態。在具體實施時，可以根據所述預設方式的不同，採用不同的處理方式，以步驟 101-3 中給出的發送方採用不同波長來發送控制資訊以及資料資訊量子態的較佳實施方式為例，可以先根據不同的波長來區分控制資訊和資料資訊的量子態，並進一步結合預設資訊格式區分身份認證資訊和密鑰資訊的量子態。

例如，發送方和接收方預先約定了如步驟 101-3 中例 1 所述的波長特徵和資訊格式，那麼在本步驟中，接收方如果接收到波長為 λ_2 的量子態，則可獲知為身份認證控制資訊量子態，隨後接收到的波長為 λ_1 的量子態為發送方身份認證資訊量子態，應該遵循雙方約定的基矢選擇規則來選擇測量基進行測量；如果接收到波長為 λ_3 的量子態，則可獲知隨後接收到的波長為 λ_1 的量子態為密鑰資訊量子態，可以採用隨機選取的測量基進行測量。

再例如，發送方和接收方預先約定了如步驟 101-3 中例 2 所述的波長特徵和資訊格式，那麼在本步驟中，接收方如果接收到波長為 λ_2 的量子態，則可獲知為控制資訊量子態，採用與發送方預先約定的（預先設定或者協商確定的）測量基進行測量，透過將測量結果與預先約定的編碼值進行比對，從而獲知接收到的控制資訊類型：身份認證控制資訊、或者密鑰控制資訊，後續接收到波長為 λ_1 的量子態時，則可以採用與所述類型對應的測量基進行測

量。

對於步驟 101 中例 3 所述的波長特徵和資訊格式，以及其他發送方可能採用的波長特徵和資訊格式，接收方也可以採用類似方式來區分各種資訊量子態，此處不再贅述。

步驟 102-2、採用所述第一預定演算法來計算發送方身份認證資訊。

在本技術方案中，收發雙方預定相同的用於計算發送方身份認證資訊的演算法，亦即，本發明所述的第一預定演算法，關於該演算法的說明請參見步驟 101-1 中的描述，此處不再贅述。

由於接收方也預定了相同的演算法，因此對於發送方應該提供的身份認證資訊是可以預期的，在本步驟中接收方採用所述第一預定演算法來計算發送方身份認證資訊，作為對發送方提供身份認證資訊的預期值。

步驟 102-3、遵循所述基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量。

本技術方案中，收發雙方預先約定了基矢選擇規則，關於基矢選擇規則的說明請參見步驟 101-2 中的描述，此處不再贅述。

如果所述基矢選擇規則為接收方設定了固定的測量基，例如線偏振測量基，那麼本步驟就採用所述固定的測量基而對接收到的發送方身份認證資訊量子態進行測量，如果所述基矢選擇規則對不同的位元值設定了不同的測量

基，那麼本步驟就根據步驟 102-2 計算得到的發送方身份認證資訊的每一位元位的值，選擇對應的測量基，並對接收到的發送方身份認證資訊量子態中的相應位元位進行測量。

步驟 102-4、判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，執行步驟 102-5，否則，結束本次量子密鑰分發過程。

經過步驟 102-3 的測量獲取了相應的測量結果，亦即，量子態中攜帶的發送方身份認證資訊，本步驟將測量得到的發送方身份認證資訊與步驟 102-2 中計算得到的發送方身份認證資訊進行比較，從而完成對發送方的身份驗證。

在本實施例中，發送方採用第一預定演算法 Y = f(userid_A, n) 來產生發送方身份認證資訊，接收方也採用相同演算法來計算該資訊的預期值，並將測量得到的發送方身份認證資訊與預期值進行比較；如果兩者相符，說明發送方在產生其身份認證資訊時採用了正確的標識資訊 userid_A、變數 n、以及函數 f，而只有身份合法的量子通信設備才可能獲知上述資訊，從而可以判定發送方通過身份驗證，因此可以繼續執行後續的步驟 102-5；反之，可以判定發送方未通過身份驗證、並結束本次量子密鑰分發過程。

考慮到在量子通道傳輸過程中，可能因為衰減、雜訊干擾等因素，導致個別光子探測不到、或者測量結果與預

期不完全一致，如果在這種情況下，認為發送方未通過身份認證，並結束本次量子密鑰分發過程，那麼會造成量子密鑰分發量的無謂減少。基於上述考慮，同時也兼顧防禦偽冒攻擊、中間人攻擊或者 DDoS 攻擊的需求，可以採取設定閾值的方式，亦即：如果接收方測量得到的發送方身份認證資訊與預期值的差異小於預先設定的閾值，例如，測量得到的發送方身份認證資訊與預期值不相符的位元位的個數小於預先設定的上限值，則接收方可以認為發送方通過身份認證。

步驟 102-5、隨機選擇測量基而對接收到的密鑰資訊量子態進行測量並公佈所述測量基，發送採用第二預定演算法而產生的接收方身份認證資訊。

執行到本步驟，說明發送方已通過接收方的身份認證，因此量子密鑰分發過程可以繼續，接收方可以按照量子密鑰分配協議，隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道來公佈所採用的測量基。在本實施例中，公佈的測量基可以採用接收方維護的變數 n 進行加密後傳輸，發送方接收後也採用其維護的變數 n 進行解密。

為了提供進一步的安全保障，實現雙向身份認證，收發雙方可以預定相同的用於計算接收方身份認證資訊的演算法，亦即，本發明所述的第二預定演算法，接收方利用該演算法來產生自己的身份認證資訊並提供給發送方，發送方則利用該演算法而對接收方身份進行驗證。

在具體實施時，可以根據需要設計所需的第二預定演算法。在本實施例中，為了產生動態的接收方身份認證資訊，在第一預定演算法的基礎上，採用如下所述的第二預定演算法：根據接收方標識資訊 userid_B 以及收發雙方按照預設策略同步變換的參數 n 的變體，計算接收方身份認證資訊。其中，關於參數 n 的說明請參見步驟 101-1 中的相關文字，此處不再贅述。所述按照預設策略同步變換的參數 n 的變體，則可以包括：所述參數 n 本身；或者，採用預設的數學變換方法來處理所述參數得到的結果，例如：n+1。關於如何利用參數 n 來產生變體的規則，可以是收發雙方預先約定好的。

下面給出所述第二預定演算法的一個具體例子：接收方身份認證資訊 Y=hash(userid_B，n+1)，亦即，計算接收方標識資訊與參數 n 的變體資訊拼接而成的字串的散列值，並將該散列值用作為接收方身份認證資訊。

透過上面的描述可以看出，採用上述第二預定演算法而計算得到的接收方身份認證資訊也是動態變化的：對於本實施例中的發送方來說，不同的接收方其標識資訊不同，因此其提供的接收方身份認證資訊不同；而同一個接收方，因為 n 值是動態變化的，因此其提供的接收方身份認證資訊也是動態變化的，進一步地，如果採用收發雙方執行量子密鑰分發過程的次數作為所述參數 n，那麼，同一個接收方在不同量子密鑰分發過程中提供的接收方身份認證資訊也是不同的。上述動態特性，攻擊者是難以模仿

的，因此為發送方透過驗證接收方身份、避免釣魚等攻擊提供了有力保障。

步驟 103、發送方採用所述第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的所述資訊相符時，判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

發送方接收到所述接收方身份認證資訊後，採用第二預定演算法來計算接收方身份認證資訊，並透過將接收的接收方身份認證資訊與計算得到的該資訊進行比對，從而完成對接收方的身份驗證。

仍沿用步驟 102-5 給出的具體例子，發送方採用第二預定演算法來計算接收方身份認證資訊 Y= hash(userid_B，n+1)，其中，userid_B 可以是預定的，也可以是由接收方透過經典通道而預先發送給發送方的。如果接收到的接收方身份認證資訊與計算得到的該資訊一致，說明接收方在產生其身份認證資訊時採用了正確的標識資訊 userid_B、變數 n、以及散列函數，並且知道雙方約定的變體產生規則，而只有身份合法的量子通信設備才可能獲知上述資訊，從而可以判定接收方通過身份認證；反之，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

如果發送方判定接收方通過身份認證，則可以按照量子密鑰分配協定的流程，將接收方公佈的測量基與自己使

用的製備基進行比較，從中選出正確的測量基，根據正確的測量基而篩選出原始密鑰，並透過經典通道向接收方公佈正確的測量基。

隨後接收方根據發送方公佈的正確測量基篩選原始密鑰，收發雙方再進一步透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰，本次量子密鑰分發過程結束。在本實施例中，在位元錯誤率估算、錯誤更正和隱私放大等階段中，收發雙方透過經典通道而協商的資訊可以採用參數 n 的變體，例如 n+1，執行相應的加密或者解密操作。

至此，透過上述步驟 101-步驟 103 可以看出，本實施例描述的技術方案，對現有的量子密鑰分配協議進行了改進，提供了在量子密鑰分發過程中進行動態身份認證的新思路。由於發送方透過量子通道發送利用第一預定演算法產生的、在向所述接收方發起的不同量子密鑰分發過程中動態變化的身份認證資訊，接收方也透過預定的相同演算法而對接收到的身份認證資訊進行驗證，從而實現在量子密鑰分發過程中對量子密鑰分發請求物件的動態身份認證，能夠有效防禦對接收方的偽冒攻擊、中間人攻擊和拒絕服務攻擊；進一步地，在上述單向認證的基礎上，收發雙方利用第二預定演算法而實現了發送方對接收方的動態身份驗證，從而能夠有效防禦對發送方的釣魚攻擊等可能存在的風險。

此外，本技術方案中的發送方身份認證資訊以量子態

形式來予以發送，能夠進一步提高安全性，而且由於採用演算法而動態產生身份認證資訊，可以避免對量子密鑰資源的浪費。

此外，本發明還提供了另一種用於量子密鑰分發過程的身份認證方法，所述方法在參與量子密鑰分發過程的發送方量子通信設備上實施。請參考圖 7，其為本發明的另一種用於量子密鑰分發過程的身份認證方法的實施例的流程圖，本實施例與上述實施例步驟相同的部分不再贅述，下面重點描述不同之處。所述方法包括如下步驟：

步驟 701、利用第一預定演算法來產生發送方身份認證資訊，所述利用第一預定演算法而產生的發送方身份認證資訊，在向接收方發起的不同量子密鑰分發過程中是動態變化的；所述接收方設備是指參與本次量子密鑰分發過程的對端設備。

所述第一預定演算法包括：根據宿主設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數，計算發送方身份認證資訊。所述計算發送方身份認證資訊，可以採用散列函數進行計算。

步驟 702、按照與所述對端設備約定的基矢選擇規則、選擇所述發送方身份認證資訊的製備基。

步驟 703、按照預設方式而向所述對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態。

例如，可以按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊的量子態，所述資料資訊包

括：所述密鑰資訊和所述發送方身份認證資訊。

所述預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼；或者，身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是預先設定的、或者與所述對端設備透過經典通道而預先協商確定的。

執行完畢本步驟的量子態發送操作後，還可以執行下述操作：接收所述對端設備返回的資訊，所述資訊至少包括接收方身份認證資訊；採用第二預定演算法來計算接收方身份認證資訊；判斷接收到的接收方身份認證資訊是否與計算得到的所述資訊相符；若相符，則判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

所述第二預定演算法包括：根據所述對端設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數的變體，計算接收方身份認證資訊。所述與所述對端設備按照預設策略同步變換的參數包括：與所述對端設備執行量子密鑰分發過程的次數。所述計算接收方身份認證資訊可以採用散列函數來進行計算。

所述對端設備返回的資訊可以不僅包括：所述接收方身份認證資訊，還包括：測量密鑰資訊量子態所採用的測量基。在上述判定接收方通過身份認證之後，還可以執行下述操作：確定密鑰資訊量子態的正確測量基，篩選原始密鑰；透過經典通道來公佈所述密鑰資訊量子態的正確測

量基；透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰，從而完成本次量子密鑰分發過程。

在上述的實施例中，提供了另一種用於量子密鑰分發過程的身份認證方法，與之相對應的，本發明還提供一種用於量子密鑰分發過程的身份認證裝置，所述裝置係部署在參與量子密鑰分發過程的發送方量子通信設備上。請參看圖 8，其為本發明之一種用於量子密鑰分發過程的身份認證裝置的實施例示意圖。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。

本實施例之一種用於量子密鑰分發過程的身份認證裝置，包括：發送方身份資訊產生單元 801，用以利用第一預定演算法來產生發送方身份認證資訊，所述發送方身份認證資訊，在向所述接收方發起的不同量子密鑰分發過程中是動態變化的；製備基選擇單元 802，用以按照與參與量子密鑰分發過程之對端設備約定的基矢選擇規則、選擇所述發送方身份認證資訊的製備基；量子態發送單元 803，用以按照預設方式而向所述對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態。

可選地，所述裝置還包括：

接收方身份資訊接收單元，用以在所述量子態發送單元完成量子態發送操作後，接收所述對端設備返回的資

訊，所述資訊至少包括接收方身份認證資訊；

接收方身份資訊計算單元，用以採用第二預定演算法來計算接收方身份認證資訊；

接收方身份驗證單元，用以判斷接收到的接收方身份認證資訊是否與計算得到的所述資訊相符；若相符，則判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

可選地，所述接收方身份資訊接收單元接收的資訊不僅包括：所述接收方身份認證資訊，還包括：所述對端設備測量密鑰資訊量子態所採用的測量基；

相應地，所述裝置包括：

原始密鑰篩選單元，用以當所述接收方身份驗證單元判定接收方通過認證之後，確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

正確測量基公佈單元，用以透過經典通道來公佈所述密鑰資訊量子態的正確測量基；

共用量子密鑰產生單元，用以透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

可選地，所述發送方身份資訊產生單元所採用的第一預定演算法包括：根據宿主設備的標識資訊以及與所述對端設備按照預設策略同步變換的參數，計算發送方身份認證資訊。

可選地，所述接收方身份資訊計算單元所採用的第二預定演算法包括：根據所述對端設備的標識資訊以及與所

述對端設備按照預設策略同步變換的參數的變體，計算接收方身份認證資訊。

可選地，所述發送方身份資訊產生單元和所述接收方身份資訊計算單元進行計算時所採用的所述按照預設策略同步變換的參數包括：與所述對端設備執行量子密鑰分發過程的次數。

可選地，所述發送方身份資訊產生單元或所述接收方身份資訊計算單元具體用於，採用散列函數計算相應身份認證資訊。

可選地，所述量子態發送單元具體用於，按照預設資訊格式、分別採用不同波長發送控制資訊以及資料資訊的量子態，所述資料資訊包括：所述密鑰資訊和所述發送方身份認證資訊。

可選地，所述量子態發送單元所採用的預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

可選地，所述量子態發送單元所採用的預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是預先設定的、或者與所述對端設備透過經典通道而預先協商確定的。

此外，本發明還提供了第三種用於量子密鑰分發過程的身份認證方法，所述方法在參與量子密鑰分發過程的接收方量子通信設備上實施。請參考圖 9，其為本發明的第

三種用於量子密鑰分發過程的身份認證方法的實施例的流程圖，本實施例與上述各實施例步驟相同的部分不再贅述，下面重點描述不同之處。所述方法包括如下步驟：

步驟 901、接收參與量子密鑰分發過程之對端設備發送的量子態，並根據與所述對端設備相同的預設方式來區分接收到的各種資訊量子態。

步驟 902、採用與所述對端設備相同的第一預定演算法來計算發送方身份認證資訊。

步驟 903、按照與所述對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量。

步驟 904、判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

在本步驟判定發送方通過身份認證之後，可以執行下述操作：採用與所述對端設備相同的第二預定演算法來產生接收方身份認證資訊，並向所述對端設備發送所述接收方身份認證資訊。

在本步驟判定發送方通過身份認證之後，還可以執行下述操作：隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道來公佈所述測量基；接收所述對端設備透過經典通道而發送的所述密鑰資訊量子態的正確測量基；篩選原始密鑰，並透過位元錯誤率估算、錯誤

更正和隱私放大過程，獲取最終的共用量子密鑰。

在上述的實施例中，提供了第三種用於量子密鑰分發過程的身份認證方法，與之相對應的，本發明還提供一種用於量子密鑰分發過程的身份認證裝置，所述裝置係部署在參與量子密鑰分發過程的接收方量子通信設備上。請參看圖 10，其為本發明之一種用於量子密鑰分發過程的身份認證裝置的實施例示意圖。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。

本實施例之一種用於量子密鑰分發過程的身份認證裝置，包括：量子態接收區分單元 1001，用以接收參與量子密鑰分發過程的對端設備發送的量子態，並根據與所述對端設備相同的預設方式來區分接收到的各種資訊量子態；發送方身份資訊計算單元 1002，用以採用與所述對端設備相同的第一預定演算法來計算發送方身份認證資訊；身份資訊量子態測量單元 1003，用以按照與所述對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量；發送方身份驗證單元 1004，用以判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

可選地，所述裝置還包括：

接收方身份資訊產生單元，用以在所述發送方身份驗證單元判定發送方通過身份認證之後，採用與所述對端設備相同的第二預定演算法來產生接收方身份認證資訊；

接收方身份資訊發送單元，用以向所述對端設備發送所述接收方身份認證資訊。

可選地，所述裝置還包括：

密鑰資訊量子態測量基公佈單元，用以在所述發送方身份驗證單元判定發送方通過身份認證之後，隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道公佈所述測量基；

正確測量基接收單元，用以接收所述對端設備透過經典通道而發送的所述密鑰資訊量子態的正確測量基；

篩選及共用量子密鑰產生單元，用以篩選原始密鑰，並透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

此外，本發明實施例還提供了一種用於量子密鑰分發過程的身份認證系統，如圖 11 所示，該系統包括：部署於發送方量子通信設備的身份認證裝置 1101，以及部署於接收方量子通信設備的身份認證裝置 1102。

分別部署於收發雙方量子通信設備的身份認證裝置，採用本發明提供的身份認證方法，在量子密鑰分發過程中實現對對端設備身份的動態身份驗證。下面結合圖 12，對所述用於量子密鑰分發過程的身份認證系統的交互處理流程作簡要說明。其中，部署於發送方量子通信設備的身

份認證裝置，簡稱為 A，部署於接收方量子通信設備的身份認證裝置，簡稱為 B，收發雙方都預定了標識資訊 userid_A 和 userid_B 以及第一預定演算法和第二預定演算法，收發雙方各自維護按照預設策略同步變的參數 n。

1）A 向 B 發送密鑰協商請求，請求中攜帶 hash(userid_A, n)；

2）B 驗證 A 身份的合法性，向 A 發送 hash(userid_B, n)；

3）A 驗證 B 身份的合法性；按照與 B 約定的基矢選擇規則，為利用第一預定演算法 f(userid_A,n)而產生的發送方身份認證資訊選擇相應的製備基，並按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；

4）B 依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預定演算法 f(userid_A,n)計算得到的發送方身份認證資訊相符，則發送採用第二預定演算法產生的接收方身份認證資訊 hash(userid_B,n+1)、並在隨機選擇測量基而對接收到的密鑰資訊量子態進行測量後公佈所述測量基，否則判定發送方未通過身份認證並結束本次量子密鑰分發過程；

5）A 採用第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的所述資訊相符時，篩選原始密鑰，並透過經典通道公佈所述密

鑰資訊量子態的正確測量基，否則判定接收方未通過身份認證並結束本次量子密鑰分發過程；

6）B 篩選原始密鑰；A 與 B 方透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

需要說明的是，上述示出的是本系統的一種可能的交互流程，在其他實施方式中可以採用不同的對話模式，在之前提供的各方法實施例中有相關的說明，此處不再贅述。

本發明雖然以較佳實施例揭示如上，但其並不是用來限定本發明，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，因此本發明的保護範圍應當以本發明之申請專利範圍所界定的範圍為準。

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/或非易失性記憶體等形式，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、 程式的模組或其他資料。電腦的儲存媒體的例子包括，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)、電可擦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)、數位影音光碟(DVD) 或其他光學儲存器、磁盒式磁帶，磁帶式磁碟片儲存或其他磁性儲存設備或任何其他非傳輸媒體，可用來儲存可以被計算設備所訪問的資訊。按照本文中的界定，電腦可讀媒體不包括非暫態性電腦可讀媒體(transitory media)，如調變的資料信號和載波。

2、本領域技術人員應明白，本發明的實施例可提供為方法、系統或電腦程式產品。因此，本發明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態樣的實施例的形式。而且，本發明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】

801：發送方身份資訊產生單元

802：製備基選擇單元

803：量子態發送單元

1001：量子態接收區分單元

1002：發送方身份資訊計算單元

1003：身份資訊量子態測量單元

1004：發送方身份驗證單元

1101：部署於發送方量子通信設備的身份認證裝置

1102：部署於接收方量子通信設備的身份認證裝置

申請專利範圍

【請求項 1】一種用於量子密鑰分發過程的身份認證方法，其特徵在於，該方法在參與量子密鑰分發過程的收發雙方量子通信設備中實施，包括：

收發雙方在透過經典通道執行的發起請求交互流程中，利用按照預設策略同步變換的參數與對端設備相互進行身份驗證，若其中任一設備未通過該身份驗證，則不啟動該量子密鑰分發過程；

發送方按照與接收方約定的基矢選擇規則來選擇發送方身份認證資訊的製備基，並按照預設方式來發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態，該發送方身份認證資訊是利用第一預定演算法而產生的，其中，該第一預定演算法包括：根據發送方標識資訊以及該收發雙方按照預設策略同步變換的參數，計算發送方身份認證資訊；以及

接收方依據該預設方式來區分接收到的各種資訊量子態，並遵循該基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用該第一預定演算法所計算得到的發送方身份認證資訊相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程；

其中，該利用第一預定演算法而產生的發送方身份認證資訊，在向該接收方發起的不同量子密鑰分發過程中是動態變化的。

【請求項 2】如請求項 1 所述之用於量子密鑰分發過程的身份認證方法，其中，在接收方判定發送方通過身份認證之後，執行下述操作：

接收方利用第二預定演算法來產生接收方身份認證資訊，並發送該接收方身份認證資訊，其中，該第二預定演算法包括：根據接收方標識資訊以及該收發雙方按照預設策略同步變換的參數的變體，計算接收方身份認證資訊；以及

發送方採用該第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的該資訊相符時，判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

【請求項 3】如請求項 2 所述之用於量子密鑰分發過程的身份認證方法，其中，接收方在判定發送方通過身份認證之後，還執行下述操作：

隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道來公佈該測量基；

相應地，發送方在判定接收方通過身份認證之後，執行下述操作：

確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

透過經典通道來公佈該密鑰資訊量子態的正確測量基；

相應地，在該發送方公佈該密鑰資訊量子態的正確測量基的步驟之後，執行下述操作：

接收方篩選原始密鑰；以及

收發雙方透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

【請求項 4】如請求項 1 所述之用於量子密鑰分發過程的身份認證方法，其中，接收方一側的發送方標識資訊是預定的、或者由發送方透過經典通道而發送給接收方的。

【請求項 5】如請求項 2 所述之用於量子密鑰分發過程的身份認證方法，其中，發送方一側的接收方標識資訊是預定的、或者由接收方透過經典通道而發送給發送方的。

【請求項 6】如請求項 1 或 2 所述之用於量子密鑰分發過程的身份認證方法，其中，該收發雙方按照預設策略同步變換的參數包括：收發雙方執行量子密鑰分發過程的次數。

【請求項 7】如請求項 1 所述之用於量子密鑰分發過程的身份認證方法，其中，該按照預設方式而發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態，包括：

按照預設資訊格式、分別採用不同波長來發送控制資訊以及資料資訊的量子態，該資料資訊包括：該密鑰資訊和該發送方身份認證資訊。

【請求項 8】如請求項 7 所述之用於量子密鑰分發過程的身份認證方法，其中，該預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

【請求項 9】如請求項 7 所述之用於量子密鑰分發過程的身份認證方法，其中，該預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是收發雙方預先設定的、或者透過經典通道而預先協商確定的。

【請求項 10】一種用於量子密鑰分發過程的身份認證方法，其特徵在於，該方法在參與量子密鑰分發過程的發送方量子通信設備上實施，包括：

利用第一預定演算法來產生發送方身份認證資訊，其中，該第一預定演算法包括：根據宿主設備的標識資訊以及與對端設備按照預設策略同步變換的參數，計算發送方身份認證資訊；

按照與參與量子密鑰分發過程之對端設備約定的基矢選擇規則、選擇該發送方身份認證資訊的製備基；以及

按照預設方式而向該對端設備發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態；

其中，該利用第一預定演算法而產生的發送方身份認證資訊，在向該對端設備發起的不同量子密鑰分發過程中是動態變化的。

【請求項 11】如請求項 10 所述之用於量子密鑰分發過程的身份認證方法，其中，在該按照預設方式而向參與量子密鑰分發過程的對端設備發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態之後，執行下述操作：

接收該對端設備返回的資訊，該資訊至少包括接收方

身份認證資訊；

採用第二預定演算法來計算接收方身份認證資訊，其中，該第二預定演算法包括：根據該對端設備的標識資訊以及與該對端設備按照預設策略同步變換的參數的變體，計算接收方身份認證資訊；以及

判斷接收到的接收方身份認證資訊是否與計算得到的該資訊相符；若相符，則判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程。

【請求項 12】如請求項 11 所述之用於量子密鑰分發過程的身份認證方法，其中，該對端設備返回的資訊不僅包括：該接收方身份認證資訊，還包括：測量密鑰資訊量子態所採用的測量基；

相應地，在判定接收方通過身份認證之後，執行下述操作：

確定密鑰資訊量子態的正確測量基，篩選原始密鑰；

透過經典通道來公佈該密鑰資訊量子態的正確測量基；以及

透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

【請求項 13】如請求項 10 或 11 所述之用於量子密鑰分發過程的身份認證方法，其中，該與該對端設備按照預設策略同步變換的參數包括：與該對端設備執行量子密鑰分發過程的次數。

【請求項 14】如請求項 10 所述之用於量子密鑰分發過程的身份認證方法，其中，該按照預設方式來發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態，包括：

按照預設資訊格式、分別採用不同波長發送控制資訊以及資料資訊的量子態，該資料資訊包括：該密鑰資訊和該發送方身份認證資訊。

【請求項 15】如請求項 14 所述之用於量子密鑰分發過程的身份認證方法，其中，該預設資訊格式包括：身份認證資訊和密鑰資訊分別有各自的控制資訊作為首碼。

【請求項 16】如請求項 14 所述之用於量子密鑰分發過程的身份認證方法，其中，該預設資訊格式包括：身份認證資訊和密鑰資訊採用共同的控制資訊作為首碼，位於控制資訊與密鑰資訊之間的身份認證資訊的長度是預先設定的、或者與該對端設備透過經典通道而預先協商確定的。

【請求項 17】一種用於量子密鑰分發過程的身份認證裝置，其特徵在於，該裝置係部署在參與量子密鑰分發過程的發送方量子通信設備上，包括：

發送方身份資訊產生單元，用以利用第一預定演算法而產生發送方身份認證資訊，該發送方身份認證資訊，在向該接收方發起的不同量子密鑰分發過程中是動態變化的，其中，該第一預定演算法包括：根據宿主設備的標識資訊以及與對端設備按照預設策略同步變換的參數，計算

發送方身份認證資訊；

製備基選擇單元，用以按照與參與量子密鑰分發過程之對端設備約定的基矢選擇規則、選擇該發送方身份認證資訊的製備基；以及

量子態發送單元，用以按照預設方式而向該對端設備發送至少包含密鑰資訊以及該發送方身份認證資訊的量子態。

【請求項 18】一種用於量子密鑰分發過程的身份認證方法，其特徵在於，該方法在參與量子密鑰分發過程的接收方量子通信設備上實施，包括：

接收參與量子密鑰分發過程之對端設備發送的量子態，並根據與該對端設備相同的預設方式來區分接收到的各種資訊量子態；

採用與該對端設備相同的第一預定演算法來計算發送方身份認證資訊，其中，該第一預定演算法包括：根據發送方標識資訊以及收發雙方按照預設策略同步變換的參數，計算發送方身份認證資訊；

按照與該對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量；以及

判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

【請求項 19】如請求項 18 所述之用於量子密鑰分發

過程的身份認證方法，其中，在判定發送方通過身份認證之後，執行下述操作：

採用與該對端設備相同的第二預定演算法來產生接收方身份認證資訊，其中，該第二預定演算法包括：根據接收方標識資訊以及收發雙方按照預設策略同步變換的參數的變體，計算接收方身份認證資訊；以及

向該對端設備發送該接收方身份認證資訊。

【請求項 20】如請求項 19 所述之用於量子密鑰分發過程的身份認證方法，其中，在判定發送方通過身份認證之後，還執行下述操作：

隨機選擇測量基而對接收到的密鑰資訊量子態進行測量，並透過經典通道來公佈該測量基；

接收該對端設備透過經典通道而發送的該密鑰資訊量子態的正確測量基；以及

篩選原始密鑰，並透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰。

【請求項 21】一種用於量子密鑰分發過程的身份認證裝置，其特徵在於，該裝置係部署在參與量子密鑰分發過程的接收方量子通信設備上，包括：

量子態接收區分單元，用以接收參與量子密鑰分發過程之對端設備發送的量子態，並根據與該對端設備相同的預設方式來區分接收到的各種資訊量子態；

發送方身份資訊計算單元，用以採用與該對端設備相同的第一預定演算法來計算發送方身份認證資訊，其中，

該第一預定演算法包括：根據發送方標識資訊以及收發雙方按照預設策略同步變換的參數，計算發送方身份認證資訊；

身份資訊量子態測量單元，用以按照與該對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量；以及

發送方身份驗證單元，用以判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程。

【請求項 22】一種用於量子密鑰分發過程的身份認證系統，其特徵在於，包括：如請求項 17 所述之部署於發送方量子通信設備上的身份認證裝置、以及如請求項 21 所述之部署於接收方量子通信設備上的身份認證裝置。

圖式

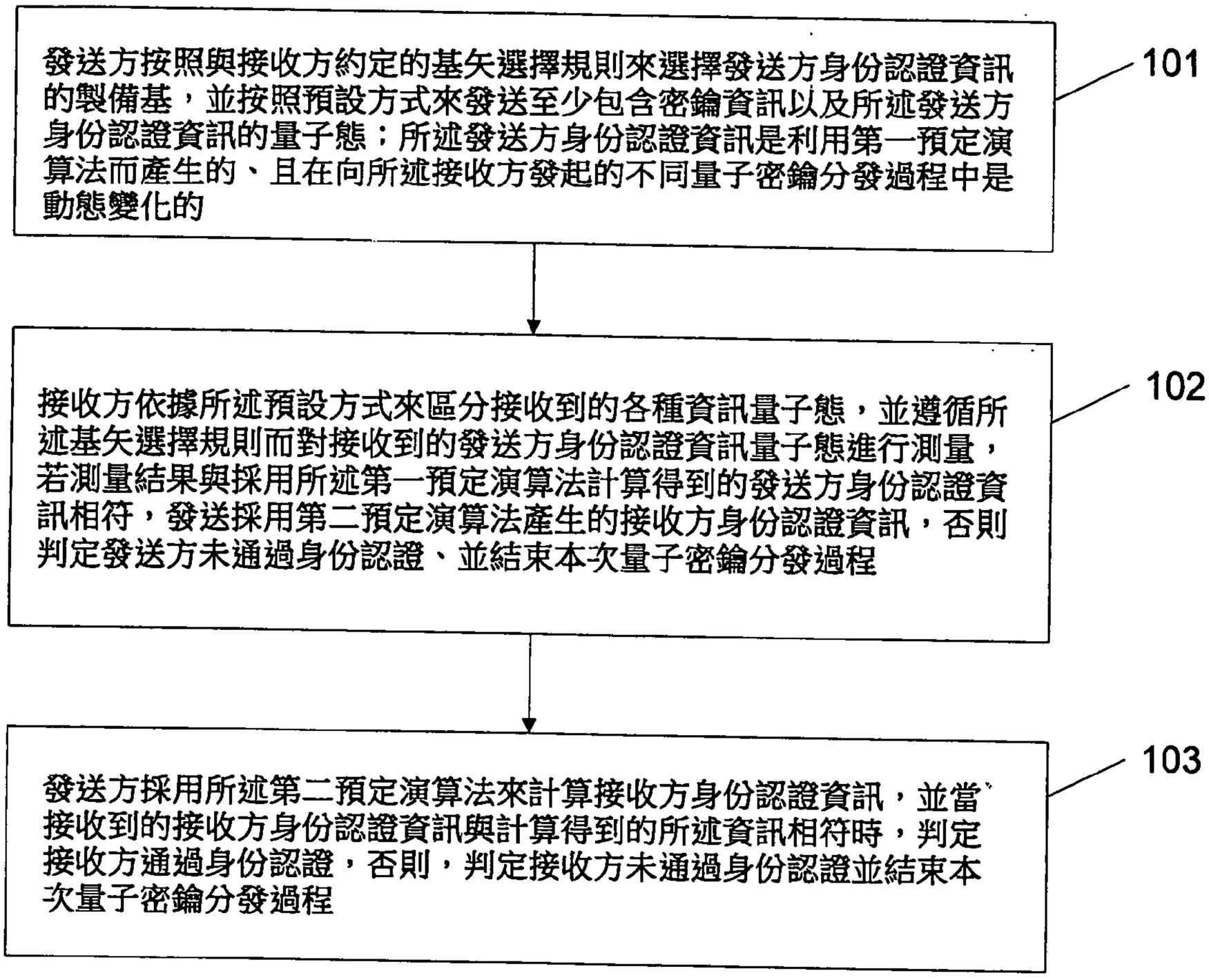
發送方按照與接收方約定的基矢選擇規則來選擇發送方身份認證資訊的製備基，並按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態；所述發送方身份認證資訊是利用第一預定演算法而產生的、且在向所述接收方發起的不同量子密鑰分發過程中是動態變化的
101
接收方依據所述預設方式來區分接收到的各種資訊量子態，並遵循所述基矢選擇規則而對接收到的發送方身份認證資訊量子態進行測量，若測量結果與採用所述第一預定演算法計算得到的發送方身份認證資訊相符，發送採用第二預定演算法產生的接收方身份認證資訊，否則判定發送方未通過身份認證、並結束本次量子密鑰分發過程
102
發送方採用所述第二預定演算法來計算接收方身份認證資訊，並當接收到的接收方身份認證資訊與計算得到的所述資訊相符時，判定接收方通過身份認證，否則，判定接收方未通過身份認證並結束本次量子密鑰分發過程
103

圖 1

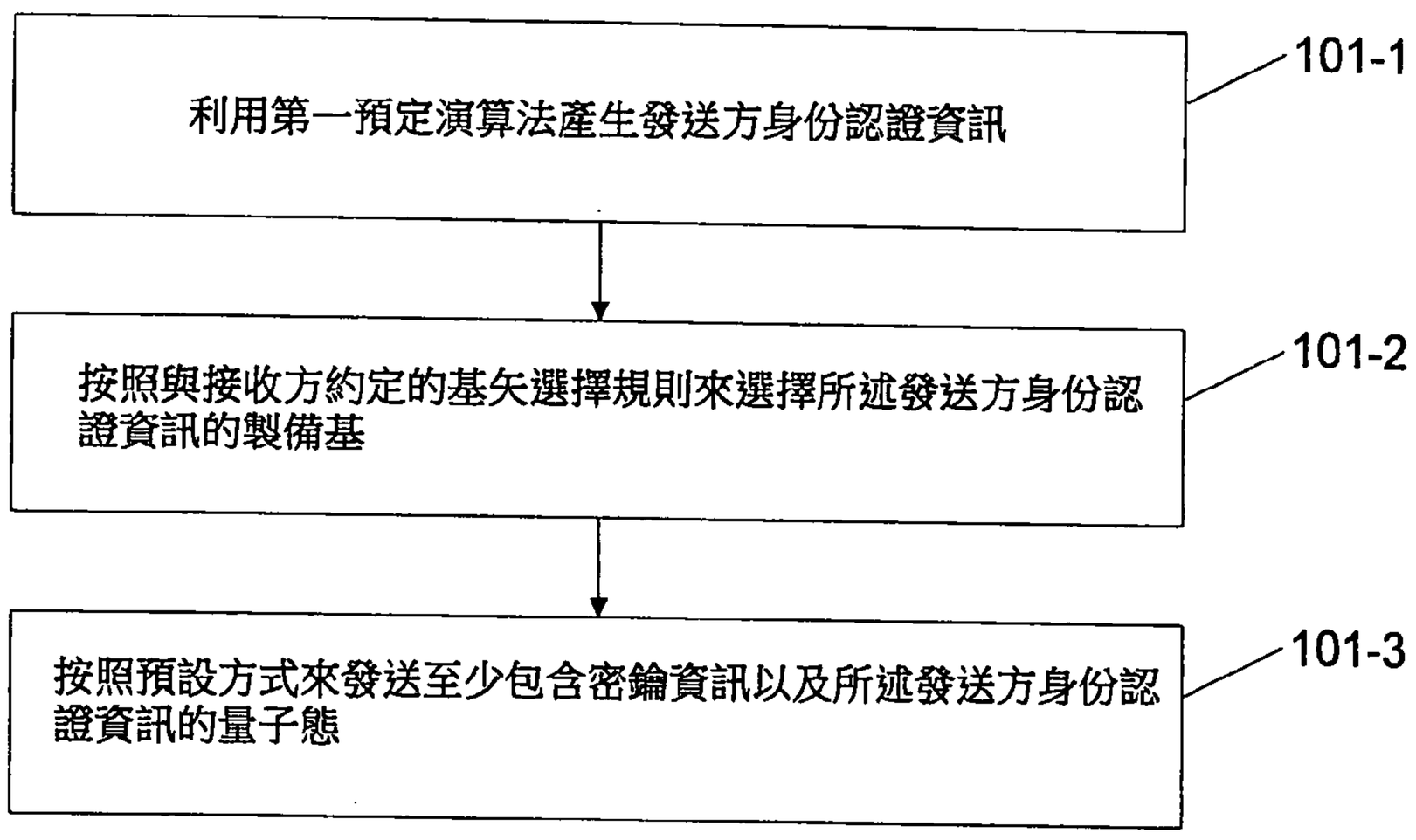
利用第一預定演算法產生發送方身份認證資訊
101-1
按照與接收方約定的基矢選擇規則來選擇所述發送方身份認證資訊的製備基
101-2
按照預設方式來發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態
101-3

圖 2

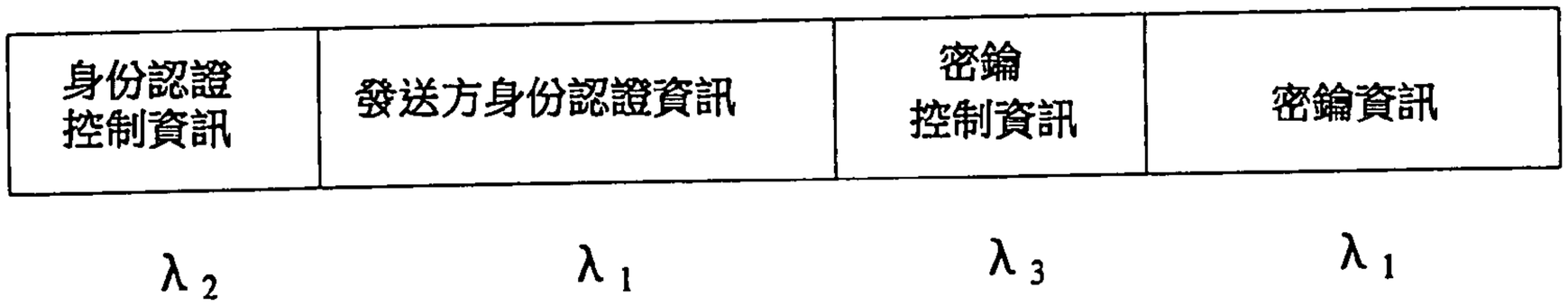
身份認證
控制資訊
發送方身份認證資訊
密鑰
控制資訊
密鑰資訊
λ 2
λ 1
λ 3
λ 1

圖 3

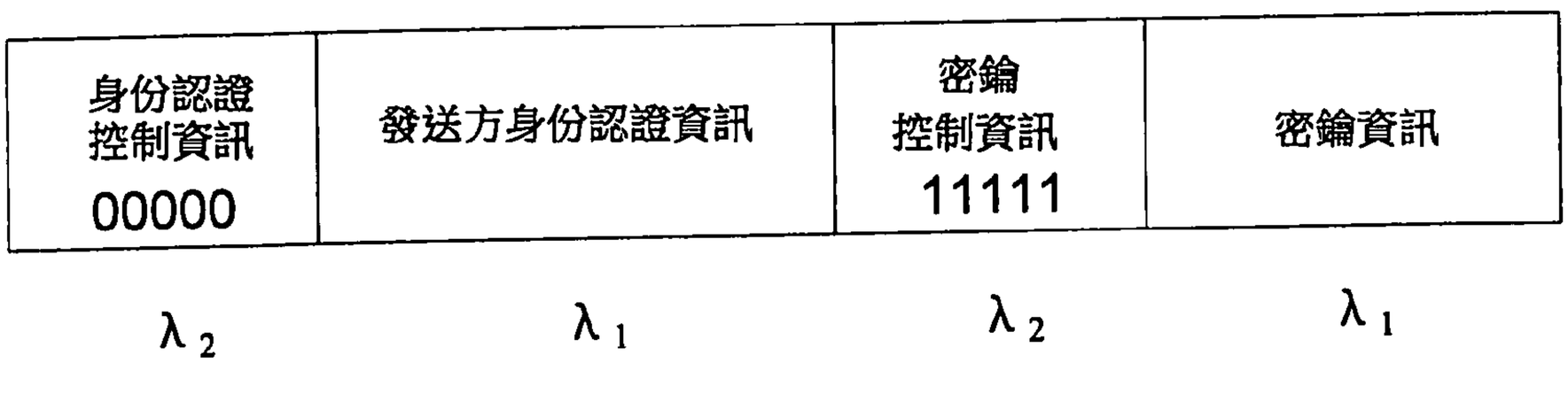
身份認證
控制資訊
00000
發送方身份認證資訊
密鑰
控制資訊
11111
密鑰資訊
λ 2
λ 1
λ 2
λ 1

圖 4

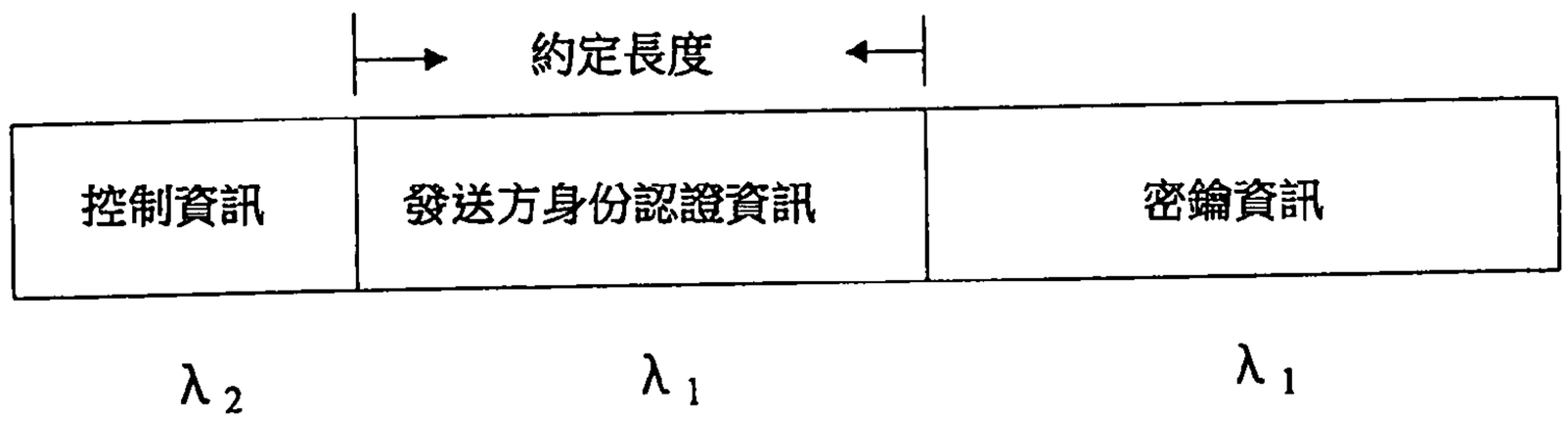
約定長度
控制資訊
發送方身份認證資訊
密鑰資訊
λ 2
λ 1
λ 1

圖 5

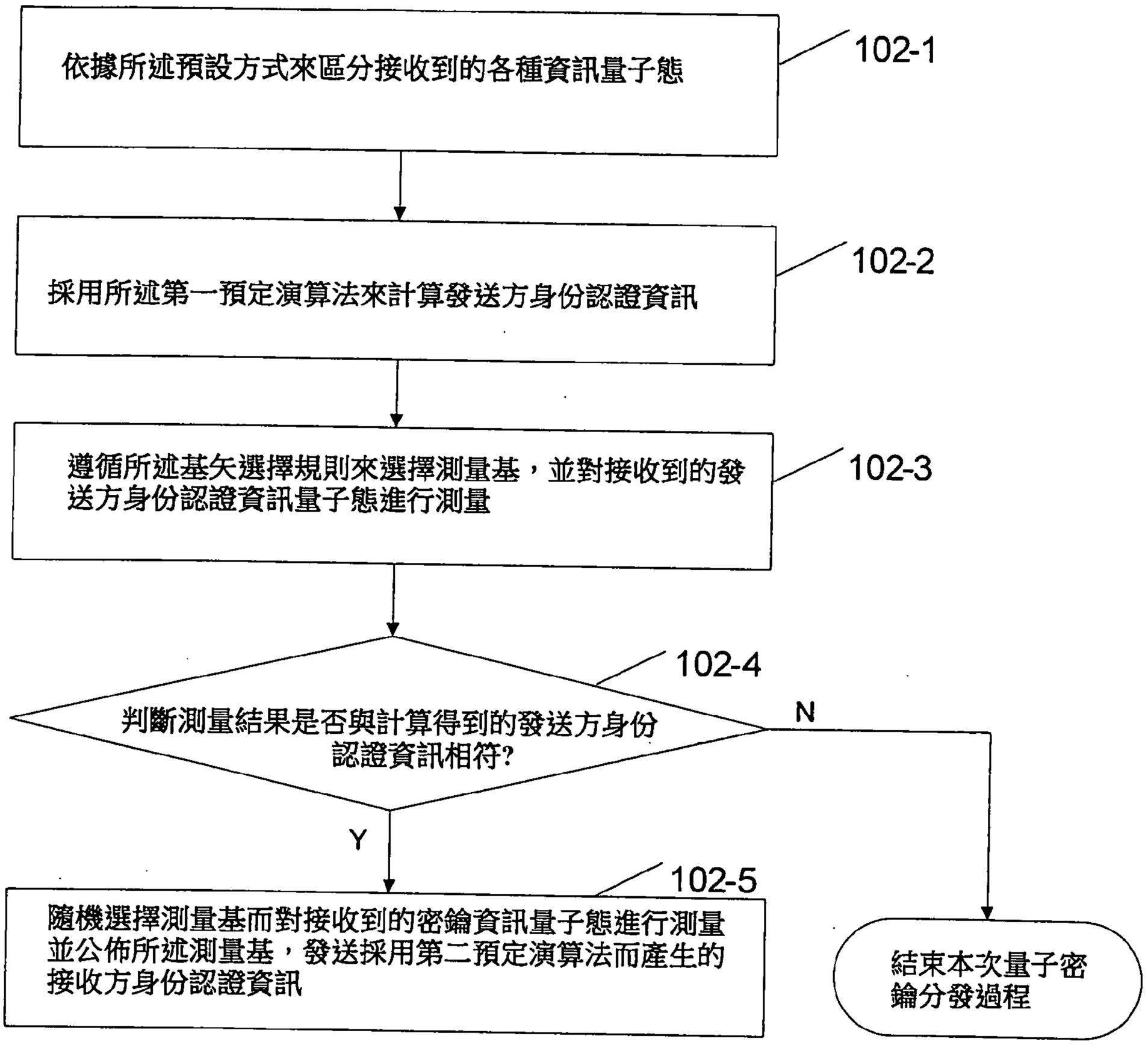
依據所述預設方式來區分接收到的各種資訊量子態
102-1
採用所述第一預定演算法來計算發送方身份認證資訊
102-2
遵循所述基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量
102-3
判斷測量結果是否與計算得到的發送方身份認證資訊相符?
102-4
N
Y
隨機選擇測量基而對接收到的密鑰資訊量子態進行測量並公佈所述測量基，發送採用第二預定演算法而產生的接收方身份認證資訊
102-5
結束本次量子密鑰分發過程

圖 6

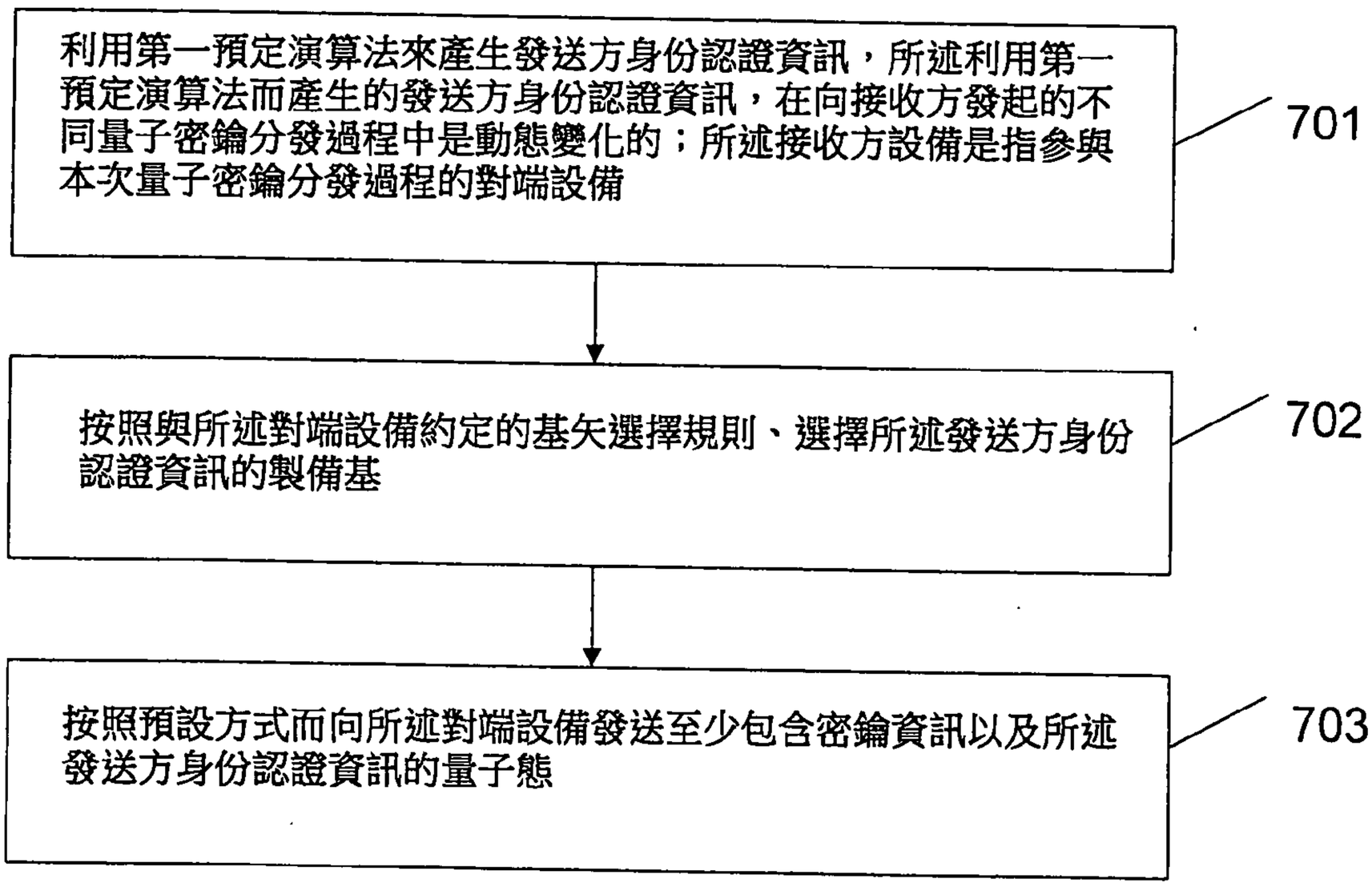
利用第一預定演算法來產生發送方身份認證資訊，所述利用第一預定演算法而產生的發送方身份認證資訊，在向接收方發起的不同量子密鑰分發過程中是動態變化的；所述接收方設備是指參與本次量子密鑰分發過程的對端設備
701
按照與所述對端設備約定的基矢選擇規則、選擇所述發送方身份認證資訊的製備基
702
按照預設方式而向所述對端設備發送至少包含密鑰資訊以及所述發送方身份認證資訊的量子態
703

圖 7

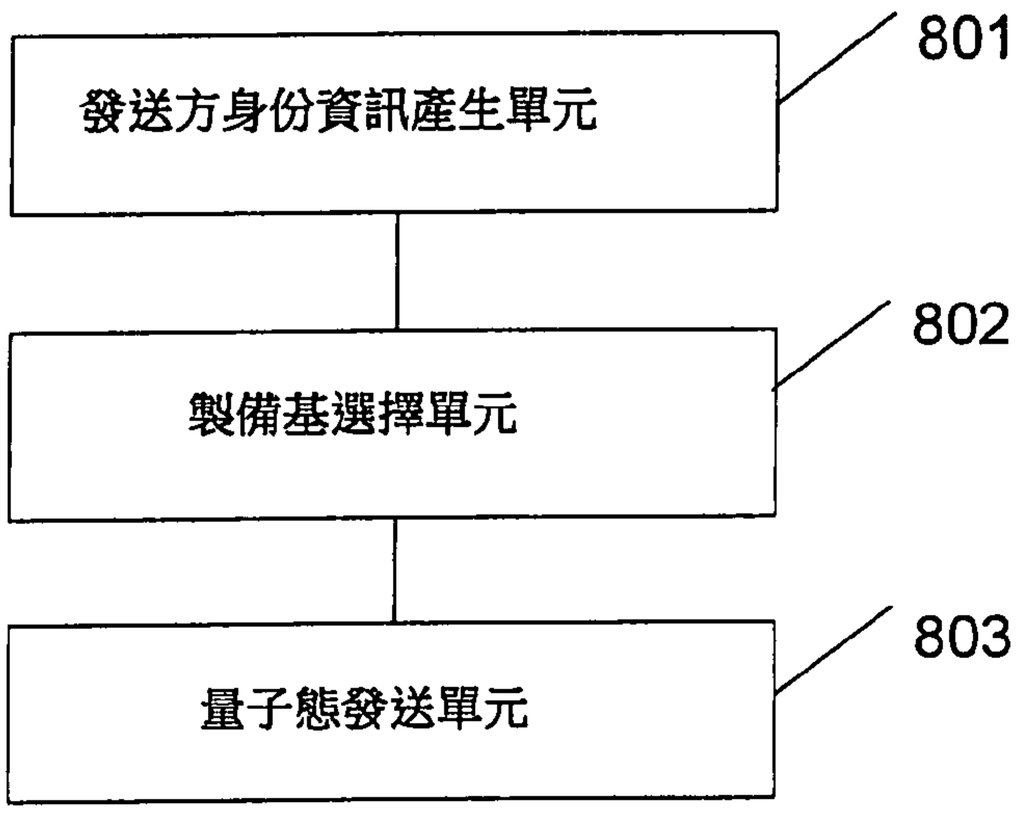
發送方身份資訊產生單元
801
製備基選擇單元
802
量子態發送單元
803

圖 8

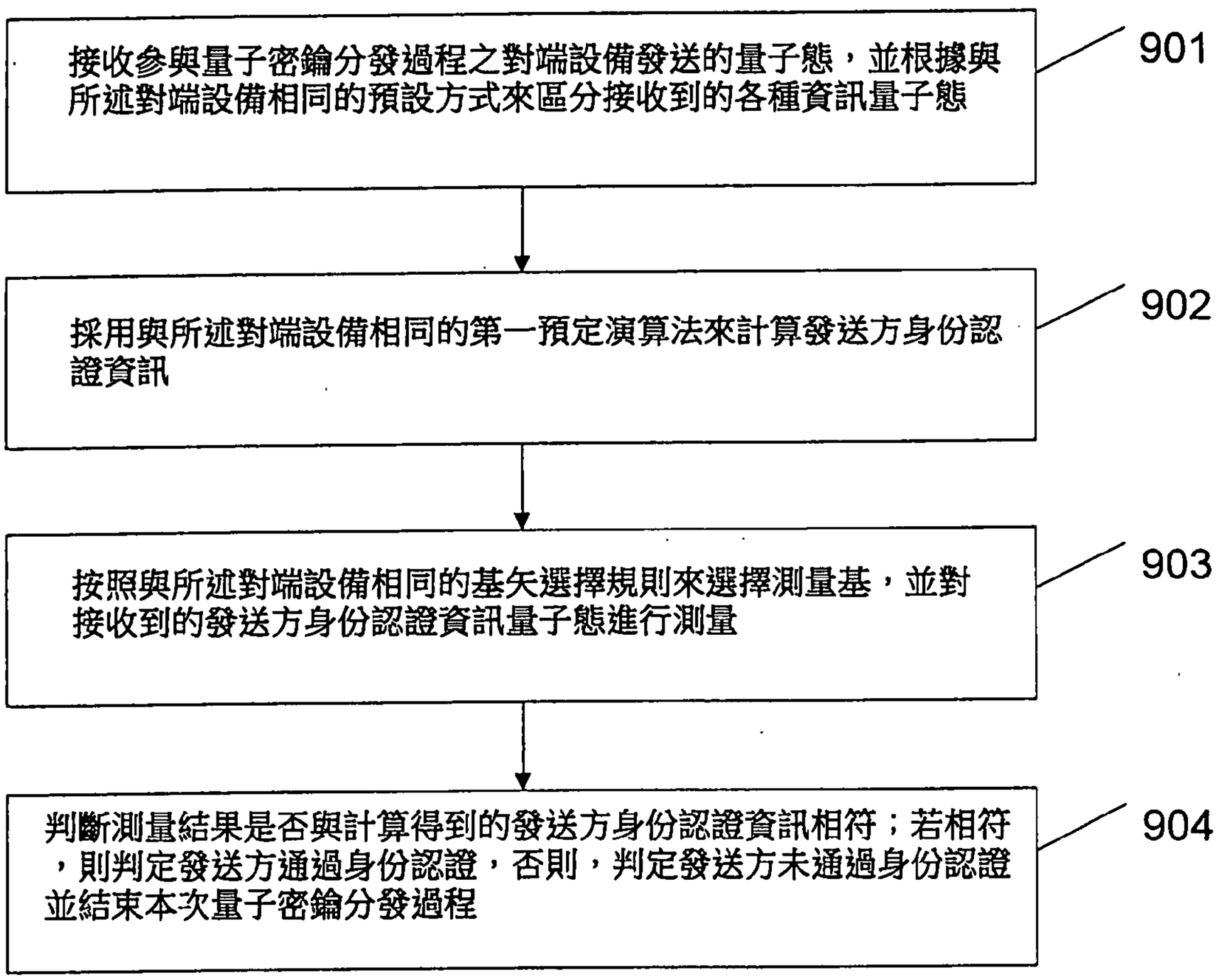
接收參與量子密鑰分發過程之對端設備發送的量子態，並根據與所述對端設備相同的預設方式來區分接收到的各種資訊量子態
901
採用與所述對端設備相同的第一預定演算法來計算發送方身份認證資訊
902
按照與所述對端設備相同的基矢選擇規則來選擇測量基，並對接收到的發送方身份認證資訊量子態進行測量
903
判斷測量結果是否與計算得到的發送方身份認證資訊相符；若相符，則判定發送方通過身份認證，否則，判定發送方未通過身份認證並結束本次量子密鑰分發過程
904

圖 9

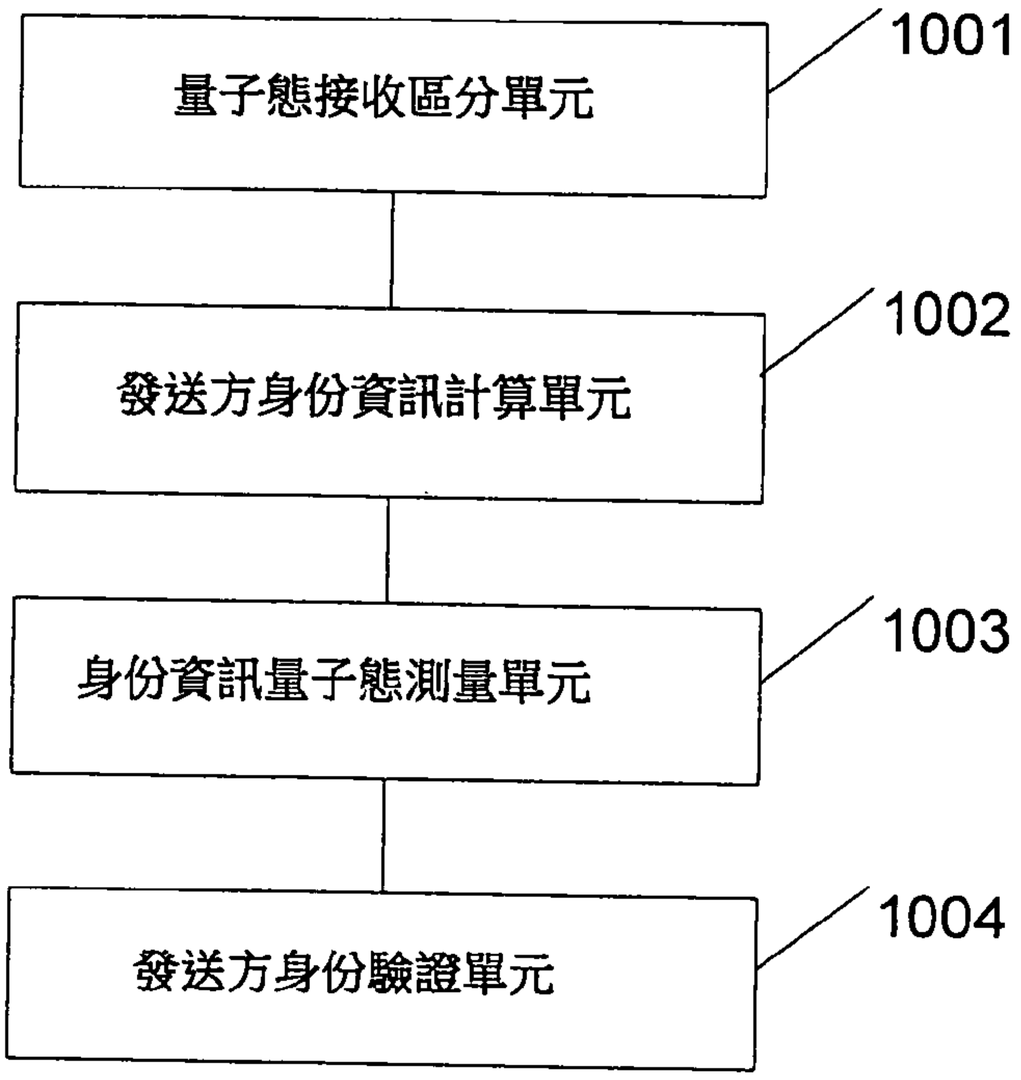
量子態接收區分單元
1001
發送方身份資訊計算單元
1002
身份資訊量子態測量單元
1003
發送方身份驗證單元
1004

圖 10

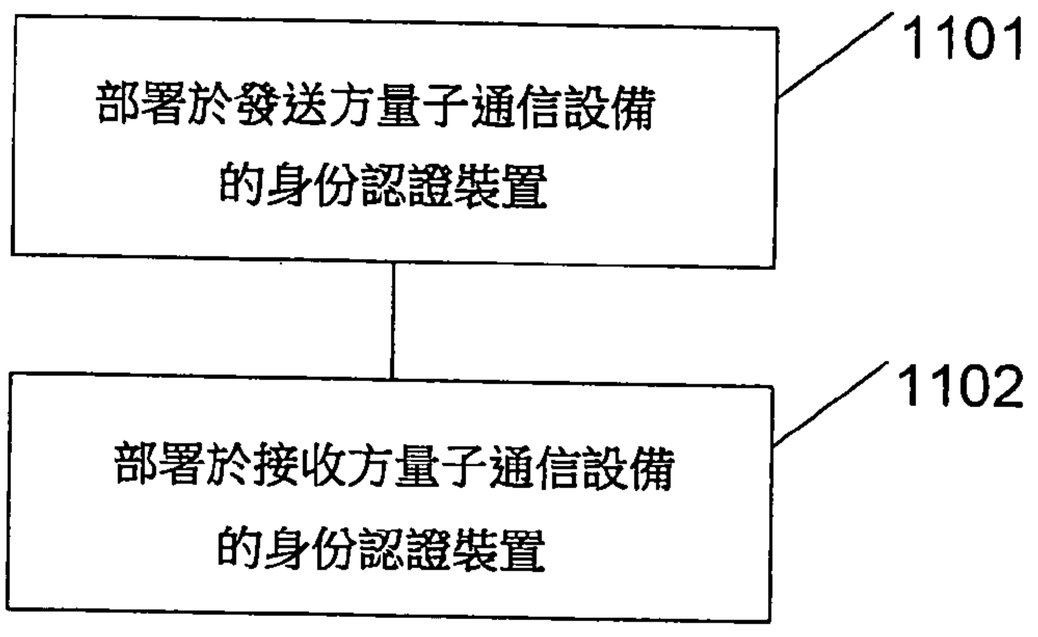
部署於發送方量子通信設備
的身份認證裝置
1101
部署於接收方量子通信設備
的身份認證裝置
1102

圖 11

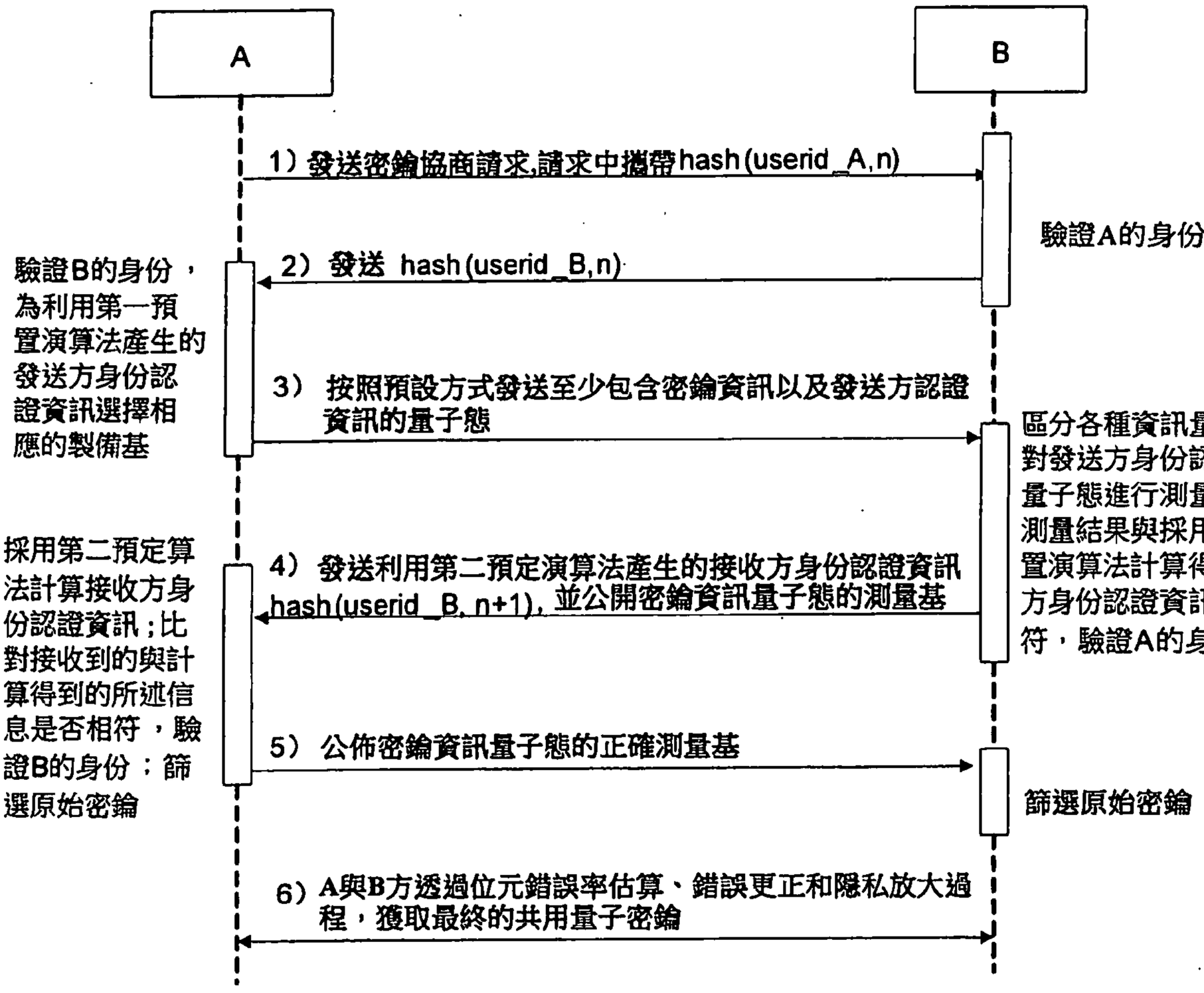
A
B
1）發送密鑰協商請求,請求中攜帶hash(userid_A,n)
驗證A的身份
驗證B的身份，為利用第一預置演算法產生的發送方身份認證資訊選擇相應的製備基
2） 發送 hash(userid_B,n)
3） 按照預設方式發送至少包含密鑰資訊以及發送方認證資訊的量子態
區分各種資訊量子態，對發送方身份認證資訊量子態進行測量，比對測量結果與採用第一預置演算法計算得到的發送方身份認證資訊 是否相符，驗證A的身份
採用第二預定算法計算接收方身份認證資訊；比對接收到的與計算得到的所述信息是否相符，驗證B的身份；篩選原始密鑰
4） 發送利用第二預定演算法產生的接收方身份認證資訊hash(userid_B, n+1)，並公開密鑰資訊量子態的測量基
5） 公佈密鑰資訊量子態的正確測量基
篩選原始密鑰
6）A與B方透過位元錯誤率估算、錯誤更正和隱私放大過程，獲取最終的共用量子密鑰

圖 12