(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201445902 A
(43)公開日： 中華民國 103 (2014) 年 12 月 01 日

(21)申請案號：102118974 (22)申請日： 中華民國 102 (2013) 年 05 月 29 日
(51)Int. Cl.： *H04B10/70 (2013.01)* *H04L9/28 (2006.01)*
H04W12/06 (2009.01)
(71)申請人：國立成功大學 (中華民國) NATIONAL CHENG KUNG UNIVERSITY (TW)
臺南市東區大學路 1 號
(72)發明人：黃宗立 HWANG, TZONELIH (TW) ；羅翊萍 LUO, YI PING (TW) ；楊竣崴 YANG, CHUN WEI (TW) ；林子翰 LIN, TZU HAN (TW)
(74)代理人：陳啟舜
申請實體審查：有 申請專利範圍項數：9 項 圖式數：2 共 23 頁

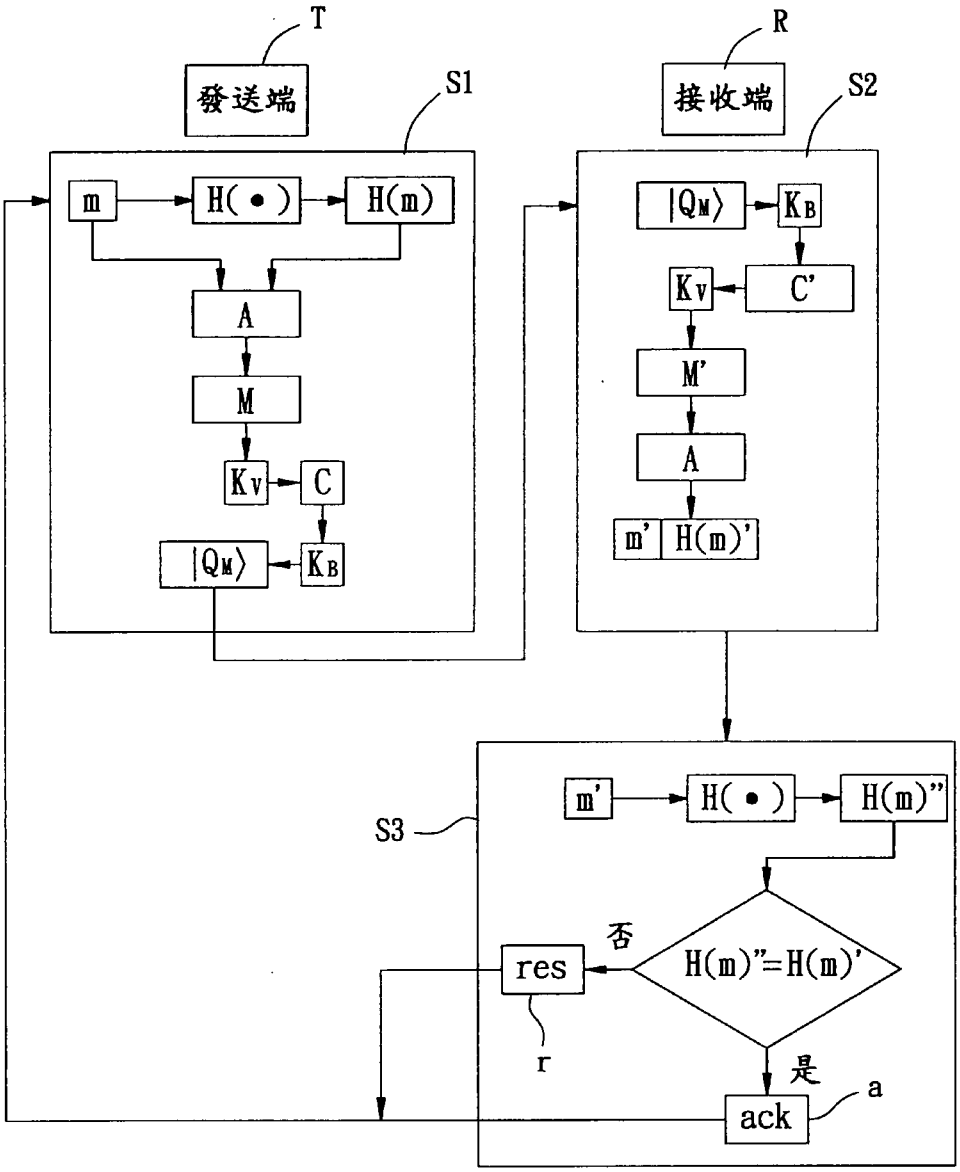
(54)名稱

量子通訊方法

METHOD FOR QUANTUM COMMUNICATION

(57)摘要

本發明揭示一種量子通訊方法，用以解決「通訊資料無法兼具加密及認證功能」問題，包含：由一發送端將一第一明文依據一雜湊函數運算而產生一第一雜湊值，再將該第一明文與該第一雜湊值依據一合併規則編輯成為一第一輯文，再將該第一輯文依據一數值金鑰加密產生一第一密文，再將該第一密文依據一基底金鑰轉換成為一量子，再將該量子傳送至一接收端；及由該接收端依據該基底金鑰量測該量子而獲得一第二密文，再將該第二密文依據該數值金鑰解密取得一第二輯文，再依據該合併規則由該第二輯文中取得一第二明文。藉此，可確實解決上述問題。



A：合併規則
a：回應訊息
C：第一密文
C’ ：第二密文
H(•)：雜湊函數
H(m)：第一雜湊值
H(m)’ ：第二雜湊值
H(m)” ：第三雜湊值
K_B：基底金鑰
K_V：數值金鑰
M：第一輯文
m：第一明文
M’ ：第二輯文
m’ ：第二明文
R：接收端
r：重送訊息
S1：傳送步驟
S2：接收步驟
S3：認證步驟
T：發送端
$|Q_M\rangle$：量子

第 2 圖

201445902

發明摘要

※ 申請案號：102118974

※ 申請日：

※IPC 分類：H04B 10/70 (2013.01)
H04L 9/08 (2006.01)
H04W 12/06 (2009.01)

【發明名稱】(中文/英文)

量子通訊方法 / **Method for Quantum Communication**

【中文】

本發明揭示一種量子通訊方法，用以解決「通訊資料無法兼具加密及認證功能」問題，包含：由一發送端將一第一明文依據一雜湊函數運算而產生一第一雜湊值，再將該第一明文與該第一雜湊值依據一合併規則編輯成爲一第一輯文，再　將該第一輯文依據一數值金鑰加密產生一第一密文，再將該第一密文依據一基底金鑰轉換成爲一量子，再將該量子傳送至一接收端；及由該接收端依據該基底金鑰量測該量子而獲得一第二密文，再將該第二密文依據該數值金鑰解密取得一第二輯文，再依據該合併規則由該第二輯文中取得一第二明文。藉此，可確實解決上述問題。

【英文】

This invention discloses a method for quantum communication to solve the problem of the communication data unable to provide authentication and encryption functions in the same time. The method comprises two steps. The first step performs a first hash value from a first plaintext based on a hash function, and then edits the first plaintext and the first hash value to form a first compiling text base on a merging rule, and then encrypts the first compiling text to form a first ciphertext based on a value key, and then transforms the first ciphertext to a quantum based on a format key, and then

transmits the quantum to a receiver by a transmitter. The second step measures the quantum to obtain a second ciphertext based on the format key, and then decrypts the second ciphertext to obtain a second compiling text based the value key, and then obtains a second plaintext from the second compiling text based on the merging rule by the receiver. Thus, it can actually resolve the said problems.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

A	合併規則	C	第一密文
C’	第二密文	H(・)	雜湊函數
H(m)	第一雜湊值	H(m)’	第二雜湊值
H(m)’’	第三雜湊值	K_B	基底金鑰
K_V	數值金鑰	M	第一輯文
M’	第二輯文	R	接收端
S1	傳送步驟	S2	接收步驟
S3	認證步驟	T	發送端
$\|Q_M\rangle$	量子		
a	回應訊息	r	重送訊息
m	第一明文	m’	第二明文

【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）

量子通訊方法 / **Method for Quantum Communication**

【技術領域】

【0001】 本發明係關於一種通訊方法；特別是關於一種結合通訊與認證功能的量子通訊方法。

【先前技術】

【0002】 隨著資通訊技術（ICT）的進步，人類生活中對於資訊傳輸的依賴程度與日俱增，如：電子郵件或電子交易等，在傳輸過程中採用密碼學更可提升資訊傳遞的安全性和隱密性。在傳統資訊技術中，除了一次性密碼本（one-time pad）或已被證明理論安全之方法外，多數習知加密器皆可基於「計算安全」原則進行運算，以確保資訊安全，然而，由於量子平行運算擁有龐大計算能力，將使得習知加密器面臨密碼被破解的危機，導致原本具有保密性的資訊遭到截獲。因此，世界各國先後投入量子（quantum）資訊研究領域，如：量子通訊系統及方法等，期待能爲資訊傳輸過程提供更有效且安全的保密方法。

【0003】 習知量子通訊系統通常包含「發送端（transmitter，或稱Alice）」及「接收端（receiver，或稱 Bob）」兩部分，其中，該「發送端」含有一計算機及一偏振光光子隨機產生器（optical quantum random number generator），該「接收端」含有另一計算機及數台單光子探測器（single photon detector），該「發送端」與「接收端」之間可通過光纖（或稱通道，channel）相連，以便傳輸資訊。

【0004】 在習知量子通訊方法的運作流程中，當使用者欲經由上述「發送端」傳輸資訊至上述「接收端」時，該「發送端」的偏振光光子產

生器會經由該通道向該「接收端」的單光子探測器發射「脈沖偏振光光子」，之後，該「發送端」與「接收端」的計算機將會經由該通道進行公開討論（public discussion），以及複雜的判斷過程，用以檢查光子是否有被竊聽或修改，例如：產生並傳送相互認可的密碼，當該「發送端」的資訊以此密碼加密後，即可經由通訊網路（如：網際網路等）進行傳輸，並由該「接收端」還原該資訊。

【0005】 惟，在多數習知量子通訊方法的資訊傳輸過程中，通訊雙方的加密及認證過程通常須分開進行（即無法同時達成加密及認證功能），導致資料傳輸次數增加，除會造成「傳輸效率降低」及「通訊負擔提高」等情況之外，且會提高「資訊遭到攻擊、截獲或竄改」等風險。其中，上述「接收端」還可由一「公正第三方（如：驗證伺服器等）」協助認證上述密碼及「發送端」的身分，然縱如此，該「接收端」與「發送端」之間仍需使用傳統通道（classical channel）及量子通道（quantum channel）傳送不同資訊，故亦會面臨上述「傳輸效率降低」、「通訊負擔提高」及「資訊遭受攻擊、截獲或竄改風險提高」等情事；而且，該「公正第三方」須隨時在線上（on-line）待命，倘若該「公正第三方」因故無法提供服務，則上述認證過程將無法正常運作，造成該「接收端」與「發送端」之間無法正常通訊。

【0006】 有鑑於此，上述習知量子通訊方法在使用時，除會造成「無法同時達成加密及認證功能」問題，且會產生「降低傳輸效率」、「提高通訊負擔」及「資訊遭到攻擊、截獲或竄改」等疑慮，在實際使用時更衍生諸多限制與缺點，確有不便之處，亟需進一步改良，以提升其實用性。

【發明內容】

【0007】 本發明之主要目的係提供一種量子通訊方法，可於通訊過程中同時提供加密及認證功能，以提高傳輸效率。

【0008】 本發明之次一目的係提供一種量子通訊方法，可於通訊過程中同時提供加密及認證功能，以降低通訊負擔。

【0009】 本發明量子通訊方法，係藉由一發送端及一接收端相互耦接，使該發送端及該接收端能夠相互通訊，該方法之步驟包含：由上述發送端將一第一明文依據一雜湊函數運算而產生一第一雜湊值，再將該第一明文與該第一雜湊值依據一合併規則編輯成爲一第一輯文，再將該第一輯文依據一數值金鑰加密而產生一第一密文，再將該第一密文依據一基底金鑰轉換成爲一量子，再將該量子傳送至上述接收端；及由上述接收端依據上述基底金鑰量測上述量子而獲得一第二密文，再將該第二密文依據上述數值金鑰解密而取得一第二輯文，再依據該合併規則由該第二輯文中取得一第二明文。

【0010】 較佳地，上述接收端依據上述合併規則由上述第二輯文中取得一第二雜湊值，依據上述第二明文與上述雜湊函數運算而產生一第三雜湊值，判斷該第三雜湊值與該第二雜湊值是否相同，若判斷爲是，該接收端認可該第二明文，若判斷爲否，該接收端放棄該第二明文。

【0011】 較佳地，若上述接收端判斷該第三雜湊值與該第二雜湊值相同，該接收端傳送一回應訊息至上述發送端，否則，該接收端傳送一重送訊息至該發送端。

【0012】 較佳地，上述基底金鑰、上述第一密文及上述量子分別包含 n 個位元，若該基底金鑰之第 i 位元爲 0，上述發送端將該第一密文之第 i 位元以 Z 基底轉換爲該量子之第 i 位元，上述接收端以 Z 基底量測該量子之第 i 位元；若該基底金鑰之第 i 位元爲 1，該發送端將該第一密文之第 i 位元以 X 基底轉換爲該量子之第 i 位元，該接收端以 X 基底量測該量子之第 i 位元；$0 \leq i < n$。

【0013】 較佳地，上述量子之第 i 位元係如下表所示：

Q_i		C_i	
		0	1
B_i	0	$\|0\rangle$	$\|1\rangle$
	1	$\|+\rangle$	$\|-\rangle$

其中，B_i 爲上述基底金鑰之第 i 位元，C_i 爲上述第一密文及上述第二密文之第 i 位元，Q_i 爲該量子之第 i 位元。

【0014】 較佳地，上述第一輯文與上述數值金鑰所包含之位元數相同，上述發送端將該第一輯文與該數值金鑰進行互斥或邏輯運算而產生上述第一密文，上述接收端將上述第二密文與該數值金鑰進行互斥或邏輯運算而產生上述第二輯文。

【0015】 較佳地，上述第一輯文與上述數值金鑰所包含之位元數相同，上述發送端將該第一輯文與該數值金鑰進行加密運算而產生上述第一密文，上述接收端將上述第二密文與該數值金鑰進行解密運算而產生上述第二輯文。

【0016】 較佳地，上述第一明文及上述第一雜湊值依據上述合併規則串連成上述第一輯文，上述第二輯文中包含上述第二明文及上述第二雜湊值，該第二雜湊值依據該合併規則串連該第二明文。

【0017】 較佳地，上述第一雜湊值依據上述合併規則插入上述第一明文中而形成上述第一輯文，上述第二輯文中包含上述第二明文及上述第二雜湊值，該第二雜湊值依據該合併規則插入該第二明文中。

【圖式簡單說明】

【0018】

第 1 圖係本發明量子通訊方法較佳實施例之系統架構圖。

第 2 圖係本發明量子通訊方法較佳實施例之運作流程圖。

【實施方式】

【0019】 爲讓本發明之上述及其他目的、特徵及優點能更明顯易懂，下文特舉本發明之較佳實施例，並配合所附圖式，作詳細說明如下：

【0020】 本發明全文所述之「發送端」(transmitter)，係指量子通訊系統中用以發送資訊的硬體(hardware)，該發送端可包含一計算機及一偏振光光子隨機產生器等，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0021】 本發明全文所述之「接收端」(receiver)，係指量子通訊系統中用以接收資訊的硬體，該發送端可包含一計算機及數台單光子探測器等，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0022】 本發明全文所述之「耦接」(coupling)，係指二裝置(如：發送端與接收端)之間相互連結，例如：藉由實體線路(如：光纖等)相互連接等，用以傳輸可表示量子位元(qubit)的載體(例如：光子等)，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0023】 本發明全文所述之「明文」(plaintext)，係指二通訊裝置(如：發送端與接收端)之間欲流通的訊息，如：文字或影音訊息等，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0024】 本發明全文所述之「密文」(ciphertext)，係指二通訊裝置(如：發送端與接收端)之間欲流通的訊息經過加密過程後的結果，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0025】 本發明全文所述之「輯文」(compiling text)，係指二資料經過一合併(merge)規則所編輯成的另一資料，例如：將 A、B 資料合併爲 C 資料等，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0026】 本發明全文所述之「量測」(measurement)，係指用以得知量子狀態的過程，例如：利用單光子量測(single photon measurement)方

法得知量子狀態等過程，其詳細情形係本發明所屬技術領域中具有通常知識者可以理解。

【0027】 請參閱第 1 圖所示，其係本發明量子通訊方法較佳實施例之系統架構圖。其中，該系統包含一發送端 T 及一接收端 R，該發送端 T 及接收端 R 相互耦接，用以執行一量子通訊作業，使該發送端 T 及接收端 R 能夠相互通訊。其中，該發送端 T 及接收端 R（即通訊雙方）可以共享一基底金鑰 K_B 及一數值金鑰 K_V 等通訊雙方秘密分享之資訊，且通訊雙方可公開約定一合併規則 A 及一雜湊函數 H(•)等資訊，該基底金鑰 K_B 及一數值金鑰 K_V 可供該發送端 T 將一第一明文 m 轉爲一量子（quantum）$|Q_M\rangle$，並供該接收端 R 由該量子 $|Q_M\rangle$ 中取得一第二明文 m'。在此實施例中，該發送端 T 及接收端 R 之間係耦接一通道 N（如：光纖等）作爲實施態樣，該發送端 T 由一計算機電性連接一偏振光光子隨機產生器，該接收端 R 由另一計算機電性連接數台單光子探測器；該二計算機可以執行資料處理（data processing）功能，並共同儲存數組安保資料（即該基底金鑰 K_B、數值金鑰 K_V）及上述合併規則 A 雜湊函數 H(•)等，如此，該二計算機可於每次通訊過程中更換不同安保資料作爲確保資訊安全的依據，例如：依該安保資料之序號等作爲指定順序，惟不以此爲限；該偏振光光子隨機產生器與單光子探測器之間經由該通道 N 相互耦接，該偏振光光子隨機產生器可由該發送端 T 之計算機控制，而將該第一明文 m 轉爲該量子 $|Q_M\rangle$，以便傳送該量子 $|Q_M\rangle$ 至該單光子探測器，並由該接收端 R 之計算機取得該第二明文 m'；其中，前述量子通訊過程中所運用的硬體設備係該技術領域中具有通常知識者可以理解，在此容不贅述。

【0028】 請參閱第 2 圖所示，其係本發明量子通訊方法較佳實施例之運作流程圖。請一併參閱第 1 圖所示，其中，該量子通訊方法較佳實施例主要包含一傳送步驟 S1 及一接收步驟 S2，分別敘述如後。

【0029】 上述傳送步驟 S1 係由上述發送端 T 將上述第一明文 m 依據上述雜湊函數（hash function）H(・)運算而產生一第一雜湊值 H(m)，再將該第一明文 m 與該第一雜湊值 H(m)依據上述合併規則 A 編輯成爲一第一輯文 M，再將該第一輯文 M 依據上述數值金鑰 K_V 加密而產生一第一密文 C，再將該第一密文 C 依據上述基底金鑰 K_B 轉換成爲上述量子$|Q_M\rangle$，再將該量子$|Q_M\rangle$傳送至上述接收端 R。詳言之，該發送端 T 可將該第一明文 m（如：以二進位表示的文字訊息等）利用該雜湊函數 H(・)運算，而產生該第一雜湊值 H(m)，該第一明文 m 與第一雜湊值 H(m)包含至少一位元，該位元數量可爲不同的預設值，該雜湊函數 H(・)之定義可參酌「Damgard, "A design principle for hash functions", Advances in Cryptology: Proceedings of CRYPTO'89, Santa Barbara, California, USA, pp.416-427, 20-24 Aug, 1989」論文，其係本發明所屬技術領域中具有通常知識者可以理解，在此容不贅述。其中，由於該第一明文 m 已依據該雜湊函數 H(・)進行轉換，使該第一明文 m 轉變爲該第一雜湊值 H(m)，因此，該雜湊函數 H(・) 可作爲該接收端 R 認證或取得該第一明文 m 的依據。

【0030】 接著，該發送端 T 可將該第一明文 m 與該第一雜湊值 H(m)依據該合併規則 A 編輯成爲該第一輯文 M，使該第一輯文 M 與數值金鑰 K_V 所包含之位元數相同，例如：若該第一明文 m 爲〝110〞，且該第一雜湊值 H(m)爲〝0〞，則可採用「串連（concatenate，||）」合併規則 A，將該第一明文 m 與該第一雜湊值 H(m)兩者串連形成該第一輯文 M，如：〝110〞串連〝0〞而組成〝1100〞；或者，採用「插入（inserted）」合併規則 A，將該第一雜湊值 H(m)插入該第一明文 m 中形成該第一輯文 M，如：在〝110〞中的位元〝11〞間插入〝0〞而組成〝1010〞等，惟不以此爲限。其中，由於該第一明文 m 與該第一雜湊值 H(m)已依據該合併規則 A 進行轉換，使該第一明文 m 散佈於該第一輯文 M 中，因此，該合併規則 A 可做爲該接

收端 R 認證或取得該第一明文 m 的依據。

【0031】 接著，將該第一輯文 M 依據該數值金鑰 K_V 加密而產生該第一密文 C，例如：採用該第一輯文 M 與數值金鑰 K_V 進行加密運算，如：邏輯運算（如：互斥或，XOR）或 AES、DES、3-DES 加密演算法等，惟不以此爲限，使該第一密文 C、基底金鑰 K_B 及量子 $|Q_M\rangle$ 分別包含 n 個位元，n 爲正整數，例如：若該第一密文 C 的 n 個位元爲〝0101〞，則其第 i(i=0~3) 位元分別爲〝0〞、〝1〞、〝0〞、〝1〞。其中，由於該第一輯文 M 已依據該數值金鑰 K_V 進行加密，使該第一輯文 M 隱藏於該第一密文 C 中，因此，該數值金鑰 K_V 可做爲該接收端 R 解密該第一輯文 M 的依據。

【0032】 接著，該發送端 T 可將該第一密文 C 之第 i 位元依據該基底金鑰 K_B 之第 i 位元進行轉換，而形成能夠表示該第一密文 C 之位元值的不同基底值(如：Z 基底或 X 基底等)，並以該轉換後的基底值作爲該量子 $|Q_M\rangle$ 之第 i 位元。在此實施例中，係以 Z 基底及 X 基底說明該量子 $|Q_M\rangle$ 之第 i 位元的實施態樣，惟不以此爲限，任何可表示該第一密文 C 之位元值的不同基底（basis）皆含括於本發明之揭露範圍，該量子 $|Q_M\rangle$ 之第 i 位元如下列表一所示：

表一、量子位元表

Q_i		C_i	
		0	1
B_i	0	$\|0\rangle$	$\|1\rangle$
	1	$\|+\rangle$	$\|-\rangle$

其中，Q_i 爲該量子 $|Q_M\rangle$ 之第 i 位元，B_i 爲該基底金鑰 K_B 之第 i 位元，C_i 爲密文（如：該第一密文 C）之第 i 位元，倘若 B_i 爲〝0〞，則「Q_i 可採用 Z 基底 $\{|0\rangle,|1\rangle\}$ 表示 C_i 之〝0〞及〝1〞」，亦即，該第一密文 C 之第 i 位元係以 Z 基底轉換爲該量子 $|Q_M\rangle$ 之第 i 位元，使該接收端 R 可採用 Z 基底量測

該量子$|Q_M\rangle$ 之第 i 位元；反之，倘若 B_i 爲〝1〞，則「Q_i 可採用 X 基底$\{|+\rangle,|-\rangle\}$表示 C_i 之〝0〞及〝1〞」，亦即，該第一密文 C 之第 i 位元係以 X 基底轉換爲該量子$|Q_M\rangle$之第 i 位元，使該接收端 R 可採用 X 基底量測該量子$|Q_M\rangle$之第 i 位元，惟不以此爲限。其中，由於該第一密文 C 已依據該基底金鑰 K_B 進行轉換，使該第一密文 C 轉變爲該量子$|Q_M\rangle$，因此，該基底金鑰 K_B 可做爲該接收端 R 解密該第一密文 C 的依據。

【0033】 舉例而言，倘若上述基底金鑰 K_B、數值金鑰 K_V、第一明文 m 及第一雜湊值 H(m)分別爲〝0101〞、〝0011〞、〝110〞及〝0〞，則上述發送端 T 可先串連該第一明文 m 及第一雜湊值 H(m)，而得到上述第一輯文 M 爲〝1100〞，接著，再將該數值金鑰 K_V 與第一輯文 M 進行 XOR 運算，而得到上述第一密文 C 爲〝1111〞，接著，再利用該基底金鑰 K_B 轉換該第一密文 C 之值，而產生上述量子$|Q_M\rangle$爲〝$|1\rangle|-\rangle|1\rangle|-\rangle$〞，之後，該發送端 T 即可將該量子$|Q_M\rangle$經由上述通道 N 傳送至上述接收端 R，並由該接收端 R 進行上述接收步驟 S2。

【0034】 請再參閱第 1 及 2 圖所示，上述接收步驟 S2 係由上述接收端 R 依據上述基底金鑰 K_B 量測上述量子$|Q_M\rangle$而獲得一第二密文 C'，再將該第二密文 C'依據上述數值金鑰 K_V 解密而取得一第二輯文 M'，再依據上述合併規則 A 由該第二輯文 M'中取得上述第二明文 m'。舉例而言，如上表一所示，該接收端 R 可利用雙方共享的基底金鑰 K_B（如：〝0101〞）量測上述量子$|Q_M\rangle$（如：〝$|1\rangle|-\rangle|1\rangle|-\rangle$〞），例如：若該基底金鑰之第 i 位元爲 0，該接收端以 Z 基底量測該量子$|Q_M\rangle$之第 i 位元；若該基底金鑰之第 i 位元爲 1，該接收端以 X 基底量測該量子$|Q_M\rangle$之第 i 位元。進一步獲得該第二密文 C'（如：〝1111〞），再將該第二密文 C'依據雙方共享的數值金鑰 K_V 解密，例如：採用該接收端 R 與發送端 T 雙方認同之方式，將上述第二密文與該數值金鑰進行解密運算，如：採用與上述加密運算方式相對應的

邏輯運算或解密演算法等，以進一步獲得一第二輯文 M'（如：〝1100〞），之後，再依據該接收端 R 與發送端 T 雙方認同之「串連」或「插入」合併規則 A（如：上述第一明文 m 與第一雜湊值 H(m)兩者串連），由該第二輯文 M'中取得該第二明文 m'（如：〝110〞），其中，在該量子$|\varrho_M\rangle$傳輸的過程中還可加入錯誤更正碼，以編成該量子$|\varrho_M\rangle$之位元，例如：採用漢明碼（Hamming Code）等古典錯誤更正碼，或者，採用如「Phys. Rev. Lett. 78, 405–408 (1997)Quantum Error Correction and Orthogonal Geometry」論文所述的量子錯誤更正碼等，惟不以此爲限，，用以避免雜訊干擾，其中，加入錯誤更正碼的過程係熟知該項技藝者可以理解，在此容不贅述。藉此，該發送端 T 與接收端 R 之間僅需傳輸一次量子$|\varrho_M\rangle$，且不需透過「公正第三方」提供認證服務，即可讓該發送端 T 與接收端 R 安全地相互通訊，相較習知量子通訊方法，本發明量子通訊方法較佳實施例僅需傳送一次量子$|\varrho_M\rangle$，而且不需使用傳統通道傳送認證資料，即可供該接收端 R 驗證所接收的訊息是否有效，並認證該發送端 T 的身分是否合法，同時兼具訊息加密及來源認證的功能，達成「提高傳輸效率」及「降低通訊負擔」等功效。

【0035】 請再參閱第 1 及 2 圖所示，本發明量子通訊方法較佳實施例還可以包含一認證步驟 S3，用以驗證上述第二明文 m'是否遭到竄改。該認證步驟 S3 係由上述接收端 R 依據上述合併規則 A 由上述第二輯文 M'中取得一第二雜湊值 H(m)'，依據上述第二明文 m'與上述雜湊函數 H(・)運算而產生一第三雜湊值 H(m)''，判斷該第三雜湊值 H(m)''與該第二雜湊值 H(m)'是否相同，若判斷爲是，認可該第二明文 m'，若判斷爲否，放棄該第二明文 m'。詳言之，由於該第二輯文 M'（如：〝1100〞）中包含該第二明文 m'（如：〝110〞）及第二雜湊值 H(m)'（如：〝0〞），故可利用該第二雜湊值 H(m)'驗證該第二明文 m'是否已被量測或竄改。因此，該接收端 R 可先以該第二明文 m'與雜湊函數 H(・)運算產生該第三雜湊值

H(m)''，倘若該第三雜湊值 H(m)''與該第二雜湊值 H(m)'相同，則表示該量子$|Q_M\rangle$未被量測或竄改，該接收端 R 能夠「認可」該第二明文 m' ，並傳送一回應訊息（ack）a 至上述發送端 T，用以通知該發送端 T 結束通訊。反之，倘若該量子$|Q_M\rangle$已被量測或竄改，則表示該第三雜湊值 H(m)''與該第二雜湊值 H(m)'應不相同，故該接收端 R 可以「放棄」該第二明文 m'，並傳送一重送訊息（res）r 至該發送端 T，用以通知該發送端 T 重新傳送上述第一明文 m。藉此，該發送端 T 與接收端 R 之間除可相互通訊，更可讓該接收端 R 驗證該量子$|Q_M\rangle$是否已被第三者量測或竄改，確保該第一明文 m 可正確無誤地進行傳輸。

【0036】 其中，倘若該量子$|Q_M\rangle$在傳輸過程中被第三者暗中量測，由於該第三者並不知道該第一明文 m 傳輸時所使用的基底金鑰 K_B，當該第三者嘗試擷取該第一明文 m 時，若該基底金鑰 K_B 或數值金鑰 K_V 有誤，例如：該基底金鑰 K_B 只要有 1 位元錯誤，即會影響測量結果，造成雪崩效應（avalanche effect）等，因此，該第三者無法通過公開檢查。而且，在不知道數值金鑰 K_V 情況下，第三者也無法得知該第一明文 m，確保該第一明文 m 不會洩漏。

【0037】 藉由前揭之技術手段，本發明量子通訊方法較佳實施例的主要特點列舉如下：由於上述發送端及接收端共享上述基底金鑰及數值金鑰，並公開約定上述合併規則及雜湊函數，因此，該發送端與接收端欲相互通訊時，可由該發送端將上述第一明文依據上述雜湊函數運算而產生上述第一雜湊值，再將該第一明文與該第一雜湊值依據上述合併規則編輯成爲上述第一輯文，再將該第一輯文依據該數值金鑰加密產生上述第一密文，再將該第一密文依據該基底金鑰轉換成爲上述量子，以便將該量子傳送至上述接收端。之後，該接收端可依據該基底金鑰量測該量子而獲得上述第二密文，再將該第二密文依據上述數值金鑰解密而取得上述第二輯

文，再依據該合併規則由該第二輯文中取得上述第二明文。因此，該發送端與接收端之間僅需傳輸一次量子，即可於通訊過程中同時兼具訊息加密及來源認證功能，且不需透過「公正第三方」提供認證服務，即可相互通訊，進一步提高傳輸效率及降低通訊負擔。

【0038】 再者，上述接收端還可驗證其所取得的第二明文是否已被量測或竄改，主要依據上述合併規則由上述第二輯文中取得上述第二雜湊值，再依據上述第二明文與上述雜湊函數產生上述第三雜湊值，再判斷該第三雜湊值與該第二雜湊值是否相同，若判斷爲是，該接收端認可該第二明文，若判斷爲否，該接收端放棄該第二明文，並可請上述發送端重新傳送上述第一明文。藉此，可以加強通訊過程中的訊息來源認證功能，確保該第一明文不會被洩漏或竄改。

【0039】 本發明量子通訊方法較佳實施例，藉由上述發送端及接收端共享上述基底金鑰及數值金鑰，並公開約定上述合併規則及雜湊函數，使該發送端可據以產生上述量子，而且，該量子同時兼具訊息加密及來源認證功能，當該量子經由一次傳送過程到達該接收端後，該接收端即可據以取得該發送端欲傳送的訊息，並確認該訊息是否有被竄改，以取得正確的通訊內容，達到「提高傳輸效率」、「降低通訊負擔」、「不需第三方認證」、「降低通道設置成本」及「避免訊息遭到截獲或竄改」等功效。

【0040】 雖然本發明已利用上述較佳實施例揭示，然其並非用以限定本發明，任何熟習此技藝者在不脫離本發明之精神和範圍之內，相對上述實施例進行各種更動與修改仍屬本發明所保護之技術範疇，因此本發明之保護範圍當視後附之申請專利範圍所界定者爲準。

【符號說明】

【0041】

〔本發明〕

A	合併規則	C	第一密文
C’	第二密文	H(・)	雜湊函數
H(m)	第一雜湊值	H(m)’	第二雜湊值
H(m)’’	第三雜湊值	K_B	基底金鑰
K_V	數值金鑰	M	第一輯文
M’	第二輯文	N	通道
R	接收端	T	發送端
S1	傳送步驟	S2	接收步驟
S3	認證步驟	$\|Q_M\rangle$	量子
a	回應訊息	r	重送訊息
m	第一明文	m’	第二明文

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

（無）

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

（無）

【序列表】(請換頁單獨記載)

（無）

申請專利範圍

1. 一種量子通訊方法，係藉由一發送端及一接收端相互耦接，使該發送端及該接收端能夠相互通訊，該方法之步驟包含：

由上述發送端將一第一明文依據一雜湊函數運算而產生一第一雜湊值，再將該第一明文與該第一雜湊值依據一合併規則編輯成爲一第一輯文，再將該第一輯文依據一數值金鑰加密而產生一第一密文，再將該第一密文依據一基底金鑰轉換成爲一量子，再將該量子傳送至上述接收端；及

由上述接收端依據上述基底金鑰量測上述量子而獲得一第二密文，再將該第二密文依據上述數值金鑰解密而取得一第二輯文，再依據上述合併規則由該第二輯文中取得一第二明文。

2. 根據申請專利範圍第 1 項所述的量子通訊方法，其中上述接收端依據上述合併規則由上述第二輯文中取得一第二雜湊值，依據上述第二明文與上述雜湊函數運算而產生一第三雜湊值，判斷該第三雜湊值與該第二雜湊值是否相同，若判斷爲是，該接收端認可該第二明文，若判斷爲否，該接收端放棄該第二明文。

3. 根據申請專利範圍第 2 項所述的量子通訊方法，其中若上述接收端判斷該第三雜湊值與該第二雜湊值相同，該接收端傳送一回應訊息至上述發送端，否則，該接收端傳送一重送訊息至該發送端。

4. 根據申請專利範圍第 1 或 2 項所述的量子通訊方法，其中上述基底金鑰、上述第一密文及上述量子分別包含 n 個位元，若該基底金鑰之第 i 位元爲 0，上述發送端將該第一密文之第 i 位元以 Z 基底轉換爲該量子之第 i 位元，上述接收端以 Z 基底量測該量子之第 i 位元；若該基底金鑰之第 i 位元爲 1，該發送端將該第一密文之第 i 位元以 X 基底轉換爲該量子之第 i 位元，該接收端以 X 基

底量測該量子之第 i 位元；$0 \leq i < n$。

5. 根據申請專利範圍第 4 項所述的量子通訊方法，其中上述量子之第 i 位元係如下表所示：

Q_i		C_i	
		0	1
B_i	0	$\|0\rangle$	$\|1\rangle$
	1	$\|+\rangle$	$\|-\rangle$

其中，B_i 爲上述基底金鑰之第 i 位元，C_i 爲上述第一密文及上述第二密文之第 i 位元，Q_i 爲該量子之第 i 位元。

6. 根據申請專利範圍第 1 或 2 項所述的量子通訊方法，其中上述第一輯文與上述數值金鑰所包含之位元數相同，上述發送端將該第一輯文與該數值金鑰進行互斥或邏輯運算而產生上述第一密文，上述接收端將上述第二密文與該數值金鑰進行互斥或邏輯運算而產生上述第二輯文。

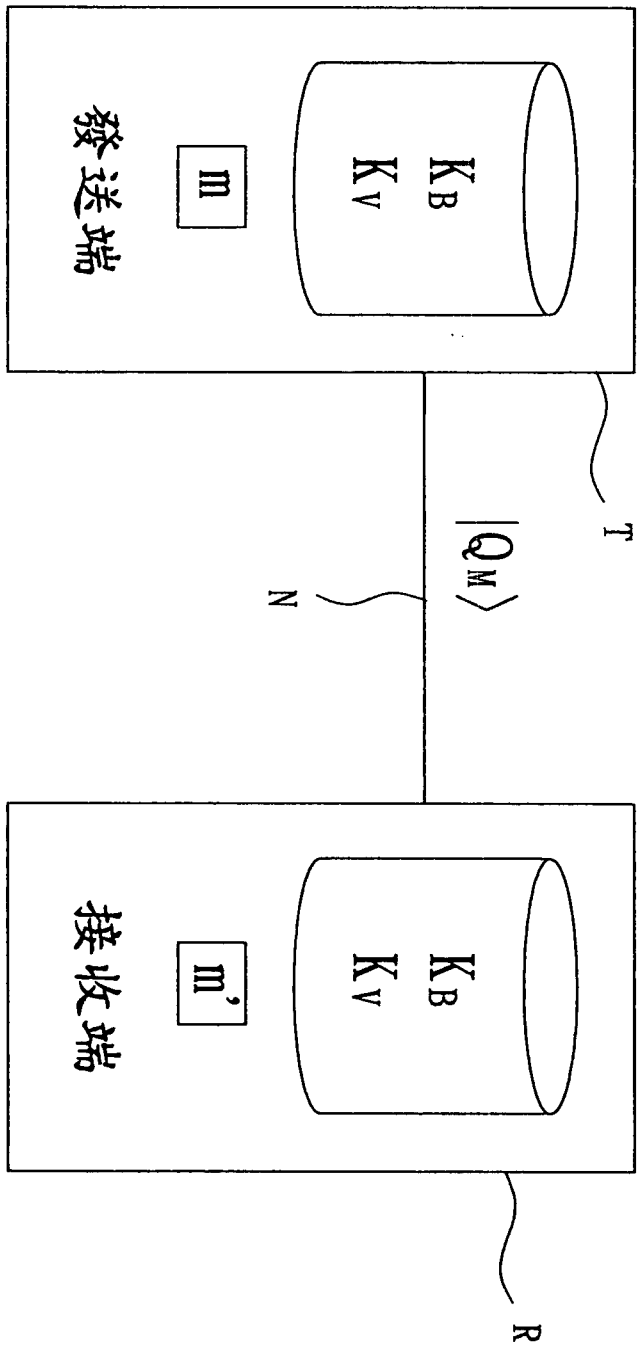
7. 根據申請專利範圍第 1 或 2 項所述的量子通訊方法，其中上述第一輯文與上述數值金鑰所包含之位元數相同，上述發送端將該第一輯文與該數值金鑰進行加密運算而產生上述第一密文，上述接收端將上述第二密文與該數值金鑰進行解密運算而產生上述第二輯文。

8. 根據申請專利範圍第 1 項所述的量子通訊方法，其中上述第一明文及上述第一雜湊值依據上述合併規則串連成上述第一輯文，上述第二輯文中包含上述第二明文及一第二雜湊值，該第二雜湊值依據該合併規則串連該第二明文。

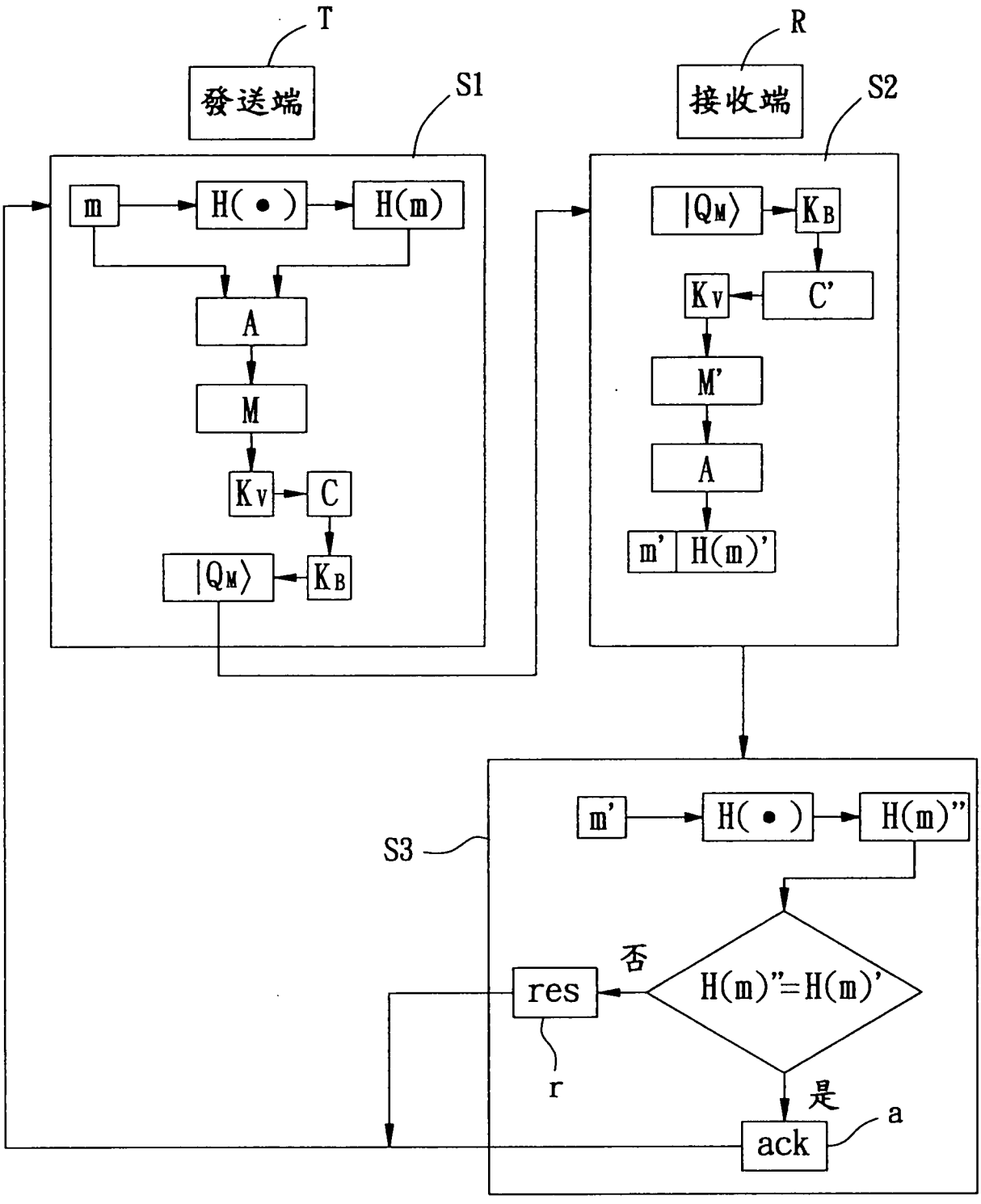
9. 根據申請專利範圍第 1 項所述的量子通訊方法，其中上述第一雜湊值依據上述合併規則插入上述第一明文中而形成上述第一輯

文，上述第二輯文中包含上述第二明文及一第二雜湊值，該第二雜湊值依據該合併規則插入該第二明文中。

圖式



第 1 圖


T
發送端
S1
m
H(•)
H(m)
A
M
Kv
C
|QM⟩
KB
R
接收端
S2
|QM⟩
KB
Kv
C'
M'
A
m'
H(m)'
S3
m'
H(•)
H(m)"
H(m)"=H(m)'
否
res
r
是
a
ack

第 2 圖