I835580

(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 I835580 B**

(45)公告日： 中華民國 113 (2024) 年 03 月 11 日

(21)申請案號：112108749 (22)申請日： 中華民國 112 (2023) 年 03 月 09 日

(51)Int. Cl.： ***H04L9/28 (2006.01)*** ***G06F21/62 (2013.01)***

(71)申請人：中華電信股份有限公司 (中華民國) CHUNGHWA TELECOM CO., LTD. (TW)
桃園市楊梅區電研路 99 號

(72)發明人：賴季夆 LAI, CHI FENG (TW) ；鄭維元 CHENG, WEI YUAN (TW) ；吳治東 WU, JHIH DONG (TW) ；梁俊安 LIANG, CHUN AN (TW) ；蘇嚮權 SU, SHIANG CHIUAN (TW)

(74)代理人：林長榮

(56)參考文獻：

TW I761243B CN 109905236A

JP 2022-519688A

審查人員：黃偉倫

申請專利範圍項數：14 項 圖式數：11 共 49 頁

(54)名稱

多終端之端對端加密通訊方法及電腦可讀媒介

(57)摘要

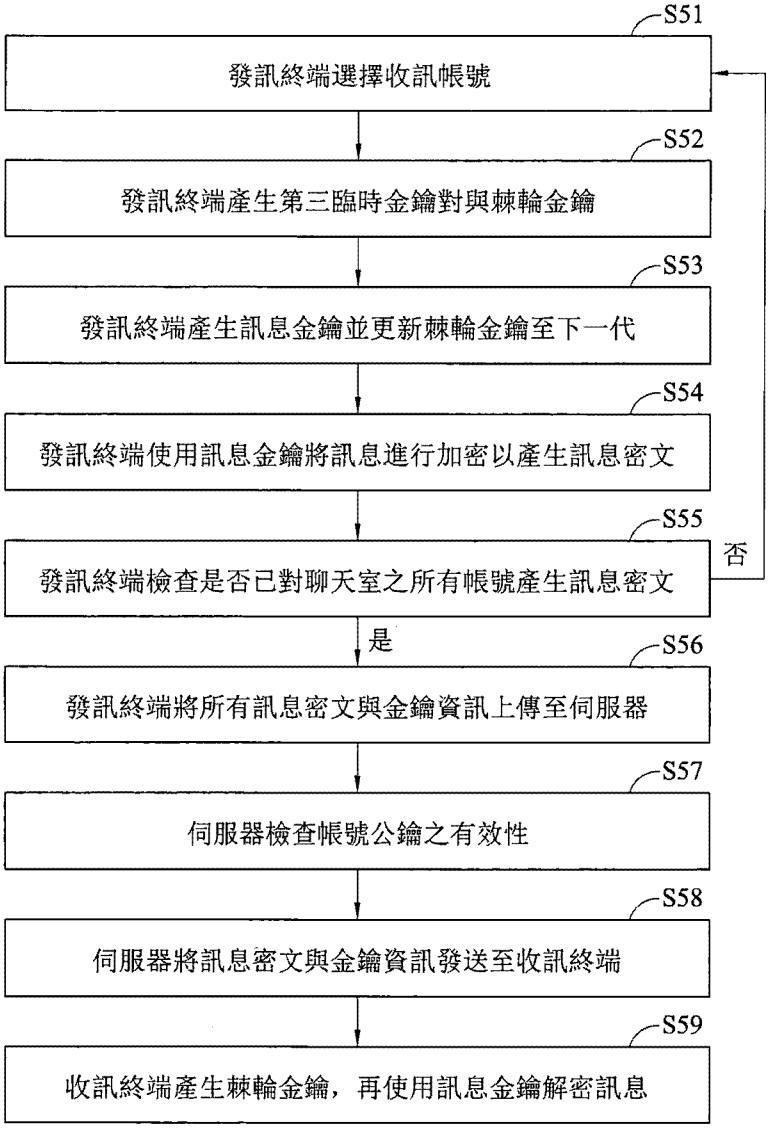
本發明揭露一種多終端之端對端加密通訊方法及電腦可讀媒介，係由發訊終端對收訊帳號產生具有臨時公鑰與臨時私鑰之臨時金鑰對，再將帳號公鑰與臨時私鑰進行運算以產生棘輪金鑰。繼之，由發訊終端使用棘輪金鑰衍生出訊息金鑰，再使用訊息金鑰將訊息加密以產生訊息密文，俾將訊息密文與金鑰資訊上傳至伺服器。然後，由伺服器將訊息密文與金鑰資訊發送至多個收訊終端，以於收訊終端收到訊息密文時，由收訊終端使用金鑰資訊以產生訊息金鑰，俾使用訊息金鑰以從訊息密文中解密出訊息。

The invention discloses a multiple terminal end-to-end encryption communication method and computer readable medium. A sending terminal generates a temporary key pair with a temporary public key and a temporary private key for a receiving account, and then calculates an account public key and the temporary private key to generate a ratchet key. Next, the sending terminal uses the ratchet key to derive a message key, and uses the message key to encrypt a message to generate a message ciphertext, and then uploads the message ciphertext and key information to a server. Thereafter, the server sends the message ciphertext and the key information to multiple receiving terminals. When the receiving terminal receives the message ciphertext, the receiving terminal uses the key information to generate the message key, and then uses the message key to decrypt the message from the message ciphertext.

指定代表圖：

符號簡單說明：

S51 至 S59:步驟



【圖 5】

I835580

【發明摘要】

【中文發明名稱】 多終端之端對端加密通訊方法及電腦可讀媒介

【英文發明名稱】 MULTIPLE TERMINAL END-TO-END ENCRYPTION COMMUNICATION METHOD AND COMPUTER READABLE MEDIUM

【中文】

本發明揭露一種多終端之端對端加密通訊方法及電腦可讀媒介，係由發訊終端對收訊帳號產生具有臨時公鑰與臨時私鑰之臨時金鑰對，再將帳號公鑰與臨時私鑰進行運算以產生棘輪金鑰。繼之，由發訊終端使用棘輪金鑰衍生出訊息金鑰，再使用訊息金鑰將訊息加密以產生訊息密文，俾將訊息密文與金鑰資訊上傳至伺服器。然後，由伺服器將訊息密文與金鑰資訊發送至多個收訊終端，以於收訊終端收到訊息密文時，由收訊終端使用金鑰資訊以產生訊息金鑰，俾使用訊息金鑰以從訊息密文中解密出訊息。

【英文】

The invention discloses a multiple terminal end-to-end encryption communication method and computer readable medium. A sending terminal generates a temporary key pair with a temporary public key and a temporary private key for a receiving account, and then calculates an account public key and the temporary private key to generate a ratchet key. Next, the sending terminal uses the ratchet key to derive a message key, and uses the message key

to encrypt a message to generate a message ciphertext, and then uploads the message ciphertext and key information to a server. Thereafter, the server sends the message ciphertext and the key information to multiple receiving terminals. When the receiving terminal receives the message ciphertext, the receiving terminal uses the key information to generate the message key, and then uses the message key to decrypt the message from the message ciphertext.

【指定代表圖】　圖5。

【代表圖之符號簡單說明】

S51 至 S59:步驟

【特徵化學式】　無。

【發明說明書】

【中文發明名稱】 多終端之端對端加密通訊方法及電腦可讀媒介

【英文發明名稱】 MULTIPLE TERMINAL END-TO-END ENCRYPTION COMMUNICATION METHOD AND COMPUTER READABLE MEDIUM

【技術領域】

【0001】 本發明係關於一種多終端之端對端加密通訊技術(通訊訊息加密技術)，特別是指一種多終端之端對端加密通訊方法及電腦可讀媒介。

【先前技術】

【0002】 現行常見的多終端之端對端加密通訊方法(如即時通訊訊息加密方法)中，大多可分為下列兩類技術。

【0003】 第一類技術：發訊終端對每個收訊終端進行獨立的一對一加密通訊，因各終端間之訊息皆為獨立加密，故隨著終端之數量成長，會增加伺服器與終端之運算量及通訊量。

【0004】 第二類技術：發訊終端隨機產生一組金鑰，將此金鑰透過端對端加密同步至所有收訊終端，且各終端利用金鑰衍生函式(Key Derivation Function; KDF)將金鑰衍生為後續訊息之加解密所使用之訊息金鑰。惟，此第二類技術需將金鑰加密後上傳至伺服器，且在同步金鑰時仍會受到終端之數量影響。

【0005】 再者，目前主流的即時通訊服務商在上述第一類技術與第二類

技術中提出一些方法，但仍會因終端之數量而對效能產生影響，並沒有一個能兼具效能、安全性與可用性之解決方案，而仍存在許多的改善空間。

【0006】因此，如何提供一種創新之多終端之端對端加密通訊技術或通訊訊息加密技術，以解決上述之任一問題或提供相關之方法，已成為本領域技術人員之一大研究課題。

【發明內容】

【0007】本發明之多終端之端對端加密通訊方法包括：由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由發訊終端將收訊帳號之帳號公鑰與臨時金鑰對之臨時私鑰進行運算以產生對收訊帳號之棘輪金鑰(ratchet key)；由發訊終端使用對收訊帳號之棘輪金鑰衍生出訊息金鑰，再由發訊終端使用對收訊帳號之棘輪金鑰所衍生出之訊息金鑰將訊息加密以產生訊息密文，俾由發訊終端將訊息密文與金鑰資訊上傳至伺服器；以及由伺服器將訊息密文與金鑰資訊發送至收訊帳號下之多個收訊終端，以於各收訊終端收到訊息密文時，由各收訊終端使用伺服器所發送之金鑰資訊產生對應棘輪金鑰之訊息金鑰，俾由各收訊終端使用對應棘輪金鑰之訊息金鑰從訊息密文中解密出訊息。

【0008】本發明之電腦可讀媒介應用於計算裝置或電腦中，係儲存有指令，以執行上述之多終端之端對端加密通訊方法。

【0009】因此，本發明提供一種創新之多終端之端對端加密通訊方法及電腦可讀媒介，係能於使用者擁有多個終端(如發訊終端/收訊終端)時，讓使用者可以同時使用多個終端發送與接收訊息密文(加密訊息)，且各終端間之訊

息可以保持一致。亦即，本發明能使各終端間具有訊息之一致性，以利使用者使用任一終端發送或接收一則訊息時，使用者之其餘終端能自動同步此則訊息。

【0010】 再者，本發明能利用棘輪金鑰(棘輪方式)產生訊息金鑰，以利確保訊息或訊息金鑰之前向安全或前向保密(Forward Secrecy; FS)。或者，本發明能於終端(如發訊終端)發送訊息時，終端與收訊帳號之帳號公鑰進行金鑰交換，隨後使用棘輪金鑰衍生出訊息金鑰以進行訊息之加密，此訊息便能被收訊帳號之多個終端解密，有利於達到終端對帳號之端對端加密，且終端所傳送之訊息密文之數量不會受到使用者之終端之數量增加而增加。

【0011】 此外，本發明另揭露一多終端之端對端加密通訊系統包括：發訊終端、收訊終端及伺服器，其中，由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由發訊終端將收訊帳號之帳號公鑰與臨時金鑰對之臨時私鑰進行運算以產生對收訊帳號之棘輪金鑰；由發訊終端使用對收訊帳號之棘輪金鑰衍生出訊息金鑰，再由發訊終端使用對收訊帳號之棘輪金鑰所衍生出之訊息金鑰將訊息加密以產生訊息密文，俾由發訊終端將訊息密文與金鑰資訊上傳至伺服器；以及由伺服器將訊息密文與金鑰資訊發送至收訊帳號下之多個收訊終端，以於各收訊終端收到訊息密文時，由各收訊終端使用伺服器所發送之金鑰資訊產生對應棘輪金鑰之訊息金鑰，俾由各收訊終端使用對應棘輪金鑰之訊息金鑰從訊息密文中解密出訊息。另外，該系統係執行本發明之多終端之端對端加密通訊方法，以提高整體效能、安全性與可用性。

【0012】 為使本發明之上述特徵與優點能更明顯易懂，下文特舉實施例，

並配合所附圖式作詳細說明。在以下描述內容中將部分闡述本發明之額外特徵及優點，且此等特徵及優點將部分自所述描述內容可得而知，或可藉由對本發明之實踐習得。應理解，前文一般描述與以下詳細描述二者均為例示性及解釋性的，且不欲約束本發明所欲主張之範圍。

【圖式簡單說明】

【0013】 圖 1 為本發明之多終端之端對端加密通訊方法中，有關新增終端之流程示意圖。

【0014】 圖 2 為本發明之多終端之端對端加密通訊方法中，有關帳號金鑰對之初始化之流程示意圖。

【0015】 圖 3 為本發明之多終端之端對端加密通訊方法中，有關帳號金鑰對之更新之流程示意圖。

【0016】 圖 4 為本發明之多終端之端對端加密通訊方法中，有關移除終端之流程示意圖。

【0017】 圖 5 為本發明之多終端之端對端加密通訊方法中，有關收發訊息之流程示意圖。

【0018】 圖 6 為本發明之多終端之端對端加密通訊方法中，有關金鑰衍生方法之示意圖。

【0019】 圖 7 為本發明之多終端之端對端加密通訊方法中，有關圖 1 所示新增終端之實施例示意圖。

【0020】 圖 8 為本發明之多終端之端對端加密通訊方法中，有關圖 2 所示帳號金鑰對之初始化之實施例示意圖。

【0021】 圖 9 為本發明之多終端之端對端加密通訊方法中，有關圖 3 所示帳號金鑰對之更新之實施例示意圖。

【0022】 圖 10 為本發明之多終端之端對端加密通訊方法中，有關圖 4 所示移除終端之實施例示意圖。

【0023】 圖 11 為本發明之多終端之端對端加密通訊方法中，有關圖 5 所示收發訊息之實施例示意圖。

【實施方式】

【0024】 以下藉由特定的具體實施形態說明本發明之實施方式，熟悉此技術之人士可由本說明書所揭示之內容瞭解本發明之其他優點與功效，亦可因而藉由其他不同具體等同實施形態加以施行或運用。

【0025】 圖 1 至圖 5 分別為本發明之多終端之端對端加密通訊方法中有關新增終端、帳號金鑰對之初始化、帳號金鑰對之更新、移除終端、收發訊息之流程示意圖。

【0026】 在一實施例中，本發明所述「至少一」代表一個以上(如一、二或三個以上)，「多個」代表二個以上(如二、三、四、五或十個以上)。「終端」可為通訊終端、電子終端、使用者裝置、智慧型手機、平板電腦、個人電腦、筆記型電腦、桌上型電腦等，「新終端」可為新增或新加入之終端，「舊終端」可為舊有或原本之終端。「訊息」可為通訊訊息或即時通訊訊息等，「訊息密文」可為加密訊息等，「發訊」代表發送訊息，「收訊」代表接收訊息。但是，本發明並不以各實施例所提及者為限。

【0027】 本發明之多終端之端對端加密通訊方法亦稱為多終端之端對端

即時通訊加密方法或即時通訊訊息加密方法，並可分為下列所述[1]新增終端、[2]移除終端、[3]收發訊息等三種實施例。

【0028】[1]新增終端：如圖1所示，「新增終端」之流程可包括下列步驟S11至步驟S14。亦即，當使用者新增至少一個(如多個)新終端時，新終端可將公鑰(如終端公鑰)上傳至伺服器，後續再進行帳號金鑰對之新增或更新。

【0029】步驟S11：新終端透過橢圓曲線密碼學(Elliptic Curve Cryptography; ECC)之方式產生一公私鑰對，為避免後續說明混淆，將此公私鑰對命名為終端金鑰對，且此終端金鑰對可具有終端公鑰與終端私鑰。

【0030】步驟S12：新終端上傳終端金鑰對之終端公鑰至伺服器。

【0031】步驟S13：伺服器將使用者目前之帳號下之有效終端資訊列表回傳給新終端。

【0032】步驟S14：新終端依據有效終端資訊列表判斷應進行帳號金鑰對之初始化或更新。例如，若有效終端資訊列表只記錄有新終端(即新增的終端)之資訊，則新終端進行帳號金鑰對之初始化(見圖2)；反之，若有效終端資訊列表不只記錄有新終端(即新增的終端)之資訊，還記錄其他終端(舊終端)之資訊，則新終端進行帳號金鑰對之更新(見圖3)。

【0033】[1-1]如圖2所示，「帳號金鑰對之初始化」之流程可包括下列步驟S21至步驟S22。

【0034】步驟S21：新終端透過橢圓曲線密碼學(ECC)之方式產生一公私鑰對。此公私鑰對可命名為帳號金鑰對，且帳號金鑰對可具有帳號公鑰與帳號私鑰。

【0035】步驟S22：新終端上傳帳號金鑰對之帳號公鑰至伺服器中儲存，

即完成帳號金鑰對之初始化。然後，伺服器可依據帳號金鑰對之帳號公鑰回應具有唯一值之帳號公鑰識別碼 ID 予新終端。

【0036】[1-2] 如圖 3 所示，「帳號金鑰對之更新」之流程可包括下列步驟 S31 至步驟 S38。

【0037】步驟 S31：新終端透過非經由伺服器之方式從舊終端取得目前之帳號私鑰。例如，非經由伺服器之方式可包括：由舊終端之螢幕以 16 進位(HEX)、文字(如數字/字元/特殊符號)或快速響應碼(QR code)等方式顯示目前之帳號私鑰，再由新終端透過此 16 進位(HEX)、文字或快速響應碼(QR code)等方式從舊終端之螢幕上取得目前之帳號私鑰。

【0038】步驟 S32：新終端產生第一更新參數。例如，此第一更新參數可為一數字(如正整數)。

【0039】步驟 S33：新終端使用目前之帳號私鑰與第一更新參數以產生一具有第一新帳號公鑰與第一新帳號私鑰之第一新帳號金鑰對。

【0040】步驟 S34：新終端透過橢圓曲線密碼學(ECC)之方式產生一公私鑰對。此公私鑰對可稱為第一臨時金鑰對，且第一臨時金鑰對可具有第一臨時公鑰與第一臨時私鑰。

【0041】步驟 S35：新終端依序使用多個(所有)舊終端之終端公鑰與第一臨時金鑰對之第一臨時私鑰以加密第一更新參數。

【0042】步驟 S36：新終端將第一新帳號公鑰、第一臨時公鑰與已加密之第一更新參數上傳至伺服器。

【0043】步驟 S37：伺服器將已加密之第一更新參數同步至多個(所有)舊終端。

【0044】步驟 S38：多個(所有)舊終端更新自己之帳號金鑰對。

【0045】[2] 移除終端：如圖 4 所示，「移除終端」之流程可包括下列步驟 S41 至步驟 S48。亦即，當使用者透過操作終端移除另一終端時，需更新帳號金鑰對，再將此帳號金鑰對之更新資訊同步至其餘終端。

【0046】步驟 S41：操作終端產生第二更新參數。例如，此第二更新參數可為一數字(如正整數)。

【0047】步驟 S42：操作終端使用目前之帳號私鑰與第二更新參數以產生一具有第二新帳號公鑰與第二新帳號私鑰之第二新帳號金鑰對。

【0048】步驟 S43：操作終端透過橢圓曲線密碼學(ECC)之方式產生一公私鑰對。此公私鑰對可稱為第二臨時金鑰對，且第二臨時金鑰對可具有第二臨時公鑰與第二臨時私鑰。

【0049】步驟 S44：操作終端依序使用欲移除之終端以外之其餘終端之終端公鑰與第二臨時私鑰以加密第二更新參數。

【0050】步驟 S45：操作終端將第二新帳號公鑰、第二臨時公鑰、已加密之第二更新參數與欲移除之終端之終端識別碼 ID 上傳至伺服器。

【0051】步驟 S46：伺服器將欲移除之終端失效並通知欲移除之終端。

【0052】步驟 S47：伺服器將已加密之第二更新參數同步至欲移除之終端以外之其餘終端。

【0053】步驟 S48：欲移除之終端以外之其餘終端更新自己之帳號金鑰對。

【0054】[3] 收發訊息：如圖 5 所示，「收發訊息」之流程可包括下列步驟 S51 至步驟 S59。亦即，發訊終端對聊天室內之帳號分別發送訊息密文(加

密訊息)，發訊終端與收訊終端透過共同之棘輪金鑰與共同之衍生方法產生出對應之訊息金鑰以進行訊息之加密或解密。

【0055】步驟 S51：發訊終端選擇一聊天室內尚未產生訊息密文(加密訊息)之帳號作為收訊帳號。

【0056】步驟 S52：若發訊終端尚未對收訊帳號產生棘輪金鑰，則發訊終端對收訊帳號產生一具有第三臨時公鑰與第三臨時私鑰之第三臨時金鑰對，再由發訊終端將收訊帳號之帳號公鑰與發訊終端之第三臨時金鑰對之第三臨時私鑰進行運算以產生對收訊帳號之棘輪金鑰(如第 N 代棘輪金鑰)。N 代表正整數，例如 N=1, 2, 3…。

【0057】步驟 S53：發訊終端使用對收訊帳號之棘輪金鑰衍生出訊息金鑰(如第 N 代訊息金鑰)，並更新棘輪金鑰(如第 N 代棘輪金鑰)至下一代棘輪金鑰(如第 N+1 代棘輪金鑰)。

【0058】步驟 S54：發訊終端使用對收訊帳號之棘輪金鑰所衍生出之訊息金鑰將訊息進行加密以產生訊息密文(加密訊息)。

【0059】步驟 S55：發訊終端檢查是否已對聊天室內之多個/所有帳號產生訊息密文(加密訊息)？若是(已對聊天室內之多個/所有帳號產生訊息密文)，則繼續往下執行步驟 S56；反之，若否(未對聊天室內之多個/所有帳號產生訊息密文)，則返回上述步驟 S51。

【0060】步驟 S56：發訊終端將所有訊息密文(加密訊息)與金鑰資訊上傳至伺服器。例如，金鑰資訊可包括使用之棘輪金鑰之代數(如第 N 代)與衍生棘輪金鑰時之帳號公鑰識別碼 ID，若棘輪金鑰為第一代棘輪金鑰，則金鑰資訊需再包括(附加)第三臨時公鑰。

【0061】步驟 S57：伺服器檢查收訊帳號之帳號公鑰之有效性。若此帳號公鑰為無效，則伺服器回覆最新的帳號公鑰予發訊終端，以使發訊終端重新產生棘輪金鑰，並丟棄此訊息密文(加密訊息)；反之，若此帳號公鑰為有效，則繼續往下執行步驟 S58。

【0062】步驟 S58：伺服器將訊息密文(加密訊息)與金鑰資訊發送至收訊帳號下之多個(所有)收訊終端。

【0063】步驟 S59：各個收訊終端收到訊息(訊息密文)時，若各個收訊終端檢查出此訊息不具有對發訊終端之棘輪金鑰，則各個收訊終端將第三臨時公鑰與收訊帳號之帳號私鑰進行運算以產生棘輪金鑰(如第一代或第 N 代棘輪金鑰)。然後，各個收訊終端使用伺服器所發送之金鑰資訊以產生對應棘輪金鑰之代數之訊息金鑰(如第一代或第 N 代訊息金鑰)，再由各個收訊終端使用對應棘輪金鑰之代數之訊息金鑰進行解密此訊息。

【0064】圖 6 為本發明之多終端之端對端加密通訊方法中，有關金鑰衍生方法之示意圖。如圖所示，發訊終端可將收訊帳號之帳號公鑰與第三臨時私鑰進行運算以產生棘輪金鑰(如第一代棘輪金鑰)，而收訊終端則將第三臨時公鑰與收訊帳號之帳號私鑰進行運算以產生棘輪金鑰(如第一代棘輪金鑰)。

【0065】此外，發訊終端可使用金鑰雜湊訊息認證碼(keyed-hash message authentication code; HMAC)配合第一常數將棘輪金鑰衍生為訊息金鑰(如第一代訊息金鑰)，以由發訊終端使用訊息金鑰(如第一代訊息金鑰)進行訊息之對稱式加密以產生訊息密文(加密訊息)。類似地，收訊終端亦可使用金鑰雜湊訊息認證碼(HMAC)配合第一常數將棘輪金鑰衍生為訊息金鑰(如第一代訊息金鑰)，再由收訊終端使用訊息金鑰(如第一代訊息金鑰)將訊息密文(加

密訊息)進行解密出訊息。

【0066】為確保金鑰安全，每次生成完訊息金鑰後，會將棘輪金鑰更新為下一代棘輪金鑰，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第二常數將第 N 代棘輪金鑰衍生至第 N+1 代棘輪金鑰(即下一代棘輪金鑰)。前述 N 代表正整數(如 N=1, 2, 3…)，第一常數與第二常數皆可為任意值，且第一常數不同於第二常數。

【0067】舉一實施例來說，本發明採用橢圓曲線迪菲-赫爾曼金鑰交換(Elliptic Curve Diffie- Hellman key exchange; ECDH)協定，為使說明更易於理解，假設一聊天室內有第一帳號 a 與第二帳號 b，第一帳號 a 擁有有效之終端 a1 與終端 a2，而第二帳號 b 尚未擁有有效之終端。

【0068】關於本實施例之符號之意義，茲舉例說明如下。❶Message：代表訊息(如即時通訊訊息)，且訊息包括但不限於文字、圖片、音訊、影片或檔案格式等。❷$CT_Message^{a1_b}$：代表終端 a1 所產生之訊息密文，且僅第二帳號 b 之終端可以解密。❸$(P^{a1}_{Client}, R^{a1}_{Client})$代表終端 a1 之終端公鑰、終端私鑰。❹$(P^{a}_{Account}, R^{a}_{Account})$：代表第一帳號 a 之帳號公鑰、帳號私鑰。❺$(P^{a1}_{E}, R^{a1}_{E})$：代表終端 a1 所產生之臨時公鑰、臨時私鑰。

【0069】此外，❻ECDH(P, R)：代表透過橢圓曲線密碼學(ECC)之公鑰 P 與私鑰 R 進行橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定之運算結果。❼G：代表橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定所使用之橢圓曲線之基點。❽$AES_{encrypt}$ (Key, Plaintext)：代表透過進階加密標準(Advanced Encryption Standard; AES)演算法(如 AES256 演算法)，將明文 Plaintext(即未加密之訊息)使用金鑰 Key 進行加密以產生訊息密文 Ciphertext。❾$AES_{decrypt}$ (Key,

Ciphertext)：代表透過進階加密標準(AES)演算法(如 AES256 演算法)，將訊息密文 Ciphertext 使用金鑰 Key 進行解密以產生明文 Plaintext(即已解密之訊息)。⑩HMAC (Key, Message)：代表使用金鑰 Key 將訊息Message進行金鑰雜湊訊息認證碼(HMAC)與安全雜湊演算法(Secure Hash Algorithm; SHA)之函數運算，且安全雜湊演算法可為安全雜湊演算法 256 位元(Secure Hash Algorithm 256-bit; SHA256)等。

【0070】 圖 7 為本發明之多終端之端對端加密通訊方法中，有關圖 1 所示「新增終端」之實施例示意圖。如圖 7 所示，新增終端之情境實施時，假設第一帳號 a 新增一新終端 a3，且第二帳號 b 新增一新終端 b1，則本實施例可包括下列程序 P11 至程序 P14 之內容。

【0071】 程序 P11(見圖 1 之步驟 S11)：第一帳號 a 之新終端 a3 與第二帳號 b 之新終端 b1 透過橢圓曲線密碼學(ECC)之方式各自產生一具有終端公鑰與終端私鑰之終端金鑰對。例如，第一帳號 a 之新終端 a3 透過橢圓曲線密碼學(ECC)之方式產生一具有終端公鑰P_{Client}^{a3}與終端私鑰R_{Client}^{a3}之終端金鑰對，第二帳號 b 之新終端 b1 透過橢圓曲線密碼學(ECC)之方式產生一具有終端公鑰P_{Client}^{b1}與終端私鑰R_{Client}^{b1}之終端金鑰對，新終端 a3 保存自己之終端金鑰對之終端私鑰R_{Client}^{a3}，且新終端 b1 保存自己之終端金鑰對之終端私鑰R_{Client}^{b1}。

【0072】 程序 P12(見圖 1 之步驟 S12)：新終端 a3 與新終端 b1 上傳自己之終端金鑰對之終端公鑰至伺服器 c。例如，新終端 a3 上傳自己之終端金鑰對之終端公鑰P_{Client}^{a3}至伺服器 c，且新終端 b1 上傳自己之終端金鑰對之終端公鑰P_{Client}^{b1}至伺服器 c。

【0073】 程序 P13(見圖 1 之步驟 S13)：伺服器 c 將有效終端資訊列表回

傳給新終端 a3 與新終端 b1。例如，伺服器 c 將第一帳號 a 之有效終端資訊列表[a1, a2, a3]回傳給新終端 a3，並將第二帳號 b 之有效終端資訊列表[b1]回傳給新終端 b1。

【0074】程序 P14(見圖 1 之步驟 S14)：新終端 a3 與新終端 b1 分別依據第一帳號 a 之有效終端資訊列表[a1, a2, a3]與第二帳號 b 之有效終端資訊列表[b1]判斷應進行帳號金鑰對之初始化或更新。例如，因第一帳號 a 已擁有有效之終端 a1 與終端 a2，故新終端 a3 需進行帳號金鑰對之更新。而第二帳號 b 尚未擁有有效之終端，新終端 b1 為第二帳號 b 之唯一有效終端，故新終端 b1 需進行帳號金鑰對之初始化。

【0075】圖 8 為本發明之多終端之端對端加密通訊方法中，有關圖 2 所示「帳號金鑰對之初始化」之實施例示意圖。如圖 8 所示，帳號金鑰對之初始化之情境實施時，假設新終端 b1 產生帳號金鑰對，則本實施例可包括下列程序 P21 至程序 P23 之內容。

【0076】程序 P21(見圖 2 之步驟 S21)：新終端 b1 透過橢圓曲線密碼學(ECC)之方式產生一具有帳號公鑰$P^{b}_{Account}$與帳號私鑰$R^{b}_{Account}$之帳號金鑰對。

【0077】程序 P22(見圖 2 之步驟 S22)：新終端 b1 上傳第二帳號 b(見圖 7)之帳號金鑰對之帳號公鑰$P^{b}_{Account}$至伺服器 c 中儲存，即完成帳號金鑰對之初始化。

【0078】程序 P23：伺服器 c 可依據第二帳號 b 之帳號金鑰對之帳號公鑰$P^{b}_{Account}$回應具有唯一值之帳號公鑰識別碼 ID 予新終端 b1。

【0079】圖 9 為本發明之多終端之端對端加密通訊方法中，有關圖 3 所示「帳號金鑰對之更新」之實施例示意圖。如圖 9 所示，帳號金鑰對之更新

之情境實施時，假設新終端 a3 更新帳號金鑰對，則本實施例可包括下列程序 P31 至程序 P39 之內容。

【0080】 程序 P31(見圖 3 之步驟 S31)：新終端 a3 以非經由伺服器 c 之方式從終端 a1(如舊終端)取得第一帳號 a(見圖 7)目前之帳號私鑰$R^{a}_{Account}$。例如，由終端 a1(如舊終端)之螢幕以 16 進位(HEX)等方式顯示第一帳號 a 目前之帳號私鑰$R^{a}_{Account}$，再由使用者於新終端 a3 輸入第一帳號 a 目前之帳號私鑰$R^{a}_{Account}$。

【0081】 程序 P32(見圖 3 之步驟 S32 至步驟 S33)：新終端 a3 產生第一更新參數Parm(如數字或正整數)。然後，新終端 a3 可使用第一帳號 a 目前之帳號私鑰$R^{a}_{Account}$與第一更新參數Parm以產生一具有第一新帳號公鑰與第一新帳號私鑰之第一新帳號金鑰對。

【0082】 例如，由新終端 a3 運算下列二個公式：❶$R^{a}_{Account} = R^{a}_{Account}$ XOR Parm，亦即將第一帳號 a 之帳號私鑰$R^{a}_{Account}$與第一更新參數Parm兩者進行互斥或(XOR)運算以產生第一新帳號金鑰對之第一新帳號私鑰$R^{a}_{Account}$。❷$P^{a}_{Account} = R^{a}_{Account} * G$，亦即依據第一新帳號私鑰$R^{a}_{Account}$與橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定所使用之橢圓曲線之基點G以產生或推論出第一新帳號金鑰對之第一新帳號公鑰$P^{a}_{Account}$。

【0083】 程序 P33(見圖 3 之步驟 S34 至步驟 S35)：新終端 a3 透過橢圓曲線密碼學(ECC)之方式產生一具有第一臨時公鑰P_E^{a3}與第一臨時私鑰R_E^{a3}之第一臨時金鑰對，再由新終端 a3 依序使用多個/所有舊終端(如終端 a1 與終端 a2)之終端公鑰與第一臨時私鑰R_E^{a3}以加密第一更新參數Parm。

【0084】 例如，由新終端 a3 運算下列四個公式：❶$Secret_{a1}^{a3}$ = ECDH

$(P_{Client}^{a1}, R_E^{a3})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將終端 a1(如舊終端)之終端公鑰P_{Client}^{a1}與新終端 a3 之第一臨時私鑰R_E^{a3}進行運算以產生終端 a1(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a1}^{a3}$。❷$Secret_{a2}^{a3} = ECDH\ (P_{Client}^{a2}, R_E^{a3})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將終端 a2(如舊終端)之終端公鑰P_{Client}^{a2}與新終端 a3 之第一臨時私鑰R_E^{a3}進行運算以產生終端 a2(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a2}^{a3}$。❸$CT_Parm^{a1} = AES_{encrypt}\ (Secret_{a1}^{a3}, Parm)$，亦即透過進階加密標準(AES)演算法將終端 a1(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a1}^{a3}$配合第一更新參數Parm進行運算以產生終端 a1(如舊終端)之更新參數密文CT_Parm^{a1}。❹$CT_Parm^{a2} = AES_{encrypt}\ (Secret_{a2}^{a3}, Parm)$，亦即透過進階加密標準(AES)演算法將終端 a2(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a2}^{a3}$配合第一更新參數Parm進行運算以產生終端 a2(如舊終端)之更新參數密文CT_Parm^{a2}。

【0085】程序 P34：新終端 a3 將更新資訊上傳至伺服器 c。例如，此更新資訊可包括下列資訊：(1)終端 a1 之更新參數密文CT_Parm^{a1}與終端 a2 之更新參數密文CT_Parm^{a2}，(2)新終端 a3 之第一臨時公鑰P_E^{a3}。

【0086】程序 P35：伺服器 c 收到來自新終端 a3 之更新資訊後，由伺服器 c 執行合法性檢查。例如，伺服器 c 之合法性檢查可包括：(1)確認無相同終端集合之有效帳號公鑰，(2)確認更新參數密文之對象與帳號之有效終端相同。

【0087】程序 P36：伺服器 c 回應相關資訊予新終端 a3。例如，若伺服器 c 所執行之合法性檢查之結果為合法，則伺服器 c 回應具有唯一值之帳號公鑰識別碼 ID 予新終端 a3；反之，若伺服器 c 所執行之合法性檢查之結果為

不合法，則伺服器 c 回應目前帳號(如第一帳號 a)之有效終端資訊列表予新終端 a3。

【0088】程序 P37：當終端 a1 或終端 a2(如舊終端)上線時，由伺服器 c 將更新資訊同步至終端 a1 或終端 a2(如舊終端)。

【0089】程序 P38：終端 a1 或終端 a2(如舊終端)使用自己之終端金鑰對之終端私鑰解密出第一更新參數Parm。例如，由終端 a1(如舊終端)運算下列二個公式：❶$Secret_{a1}^{a3} = ECDH\ (P_E^{a3}, R_{Client}^{a1})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將新終端 a3 之第一臨時公鑰P_E^{a3}與終端 a1(如舊終端)自己之終端金鑰對之終端私鑰R_{Client}^{a1}進行運算以產生終端 a1(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a1}^{a3}$。❷$Parm = AES_{decrypt}\ (Secret_{a1}^{a3},\ CT_Parm^{a1})$，亦即透過進階加密標準(AES)演算法以使用終端 a1(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a1}^{a3}$配合終端 a1 之更新參數密文CT_Parm^{a1}來解密出第一更新參數Parm。

【0090】此外，由終端 a2(如舊終端)運算下列二個公式：❶$Secret_{a2}^{a3} = ECDH\ (P_E^{a3},\ R_{Client}^{a2})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將新終端 a3 之第一臨時公鑰P_E^{a3}與終端 a2(如舊終端)自己之終端金鑰對之終端私鑰R_{Client}^{a2}進行運算以產生終端 a2(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a2}^{a3}$。❷$Parm = AES_{decrypt}\ (Secret_{a2}^{a3}, CT_Parm^{a2})$，亦即透過進階加密標準(AES)演算法以使用終端 a2(如舊終端)與新終端 a3 兩者之共享臨時金鑰$Secret_{a2}^{a3}$配合終端 a2 之更新參數密文CT_Parm^{a2}來解密出第一更新參數Parm。

【0091】程序 P39(見圖 3 之步驟 S38)：終端 a1 或終端 a2(如舊終端)更新自己之帳號金鑰對。例如，由終端 a1 或終端 a2(如舊終端)運算下列二個公

式：❶$R^a_{Account} = R^a_{Account}$ XOR Parm，亦即將第一帳號 a 之帳號私鑰$R^a_{Account}$與第一更新參數Parm兩者進行互斥或(XOR)運算以產生第一新帳號金鑰對之第一新帳號私鑰$R^a_{Account}$。❷$P^a_{Account} = R^a_{Account} * G$，亦即依據第一新帳號私鑰$R^a_{Account}$與橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定所使用之橢圓曲線之基點G以產生或推論出第一新帳號金鑰對之第一新帳號公鑰$P^a_{Account}$。

【0092】 圖 10 為本發明之多終端之端對端加密通訊方法中，有關圖 4 所示「移除終端」之實施例示意圖。如圖 10 所示，移除終端之情境實施時，假設使用者欲透過第一帳號 a(見圖 7)之終端 a1(如操作終端)移除新終端 a3，則本實施例可包括下列程序 P41 至程序 P49 之內容。

【0093】 程序 P41(見圖 4 之步驟 S41 至步驟 S42)：終端 a1(如操作終端)產生第二更新參數Parm，且終端 a1(如操作終端)可產生一具有第二新帳號公鑰$P^a_{Account}$與第二新帳號私鑰$R^a_{Account}$之第二新帳號金鑰對。

【0094】 例如，由終端 a1(如操作終端)運算下列二個公式：❶$R^a_{Account} = R^a_{Account}$ XOR Parm，亦即將第一帳號 a 之帳號私鑰$R^a_{Account}$與第二更新參數Parm兩者進行互斥或(XOR)運算以產生第二新帳號金鑰對之第二新帳號私鑰$R^a_{Account}$。❷$P^a_{Account} = R^a_{Account} * G$，亦即依據第二新帳號私鑰$R^a_{Account}$與橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定所使用之橢圓曲線之基點G以產生或推論出第二新帳號金鑰對之第二新帳號公鑰$P^a_{Account}$。

【0095】 程序 P42(見圖 4 之步驟 S43)：終端 a1(如操作終端)透過橢圓曲線密碼學(ECC)之方式產生一具有第二臨時公鑰P^{a1}_E與第二臨時私鑰R^{a1}_E之第二臨時金鑰對。然後，終端 a1(如操作終端)可將第二更新參數Parm加密成終端 a2 之更新參數密文CT_Parm^{a2}。

【0096】 例如，由終端 a1(如操作終端)運算下列二個公式：❶$Secret_{a2}^{a1}$ = ECDH (P_{Client}^{a2}, R_E^{a1})，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將終端 a2 之終端公鑰P_{Client}^{a2}與終端 a1(如操作終端)之第二臨時私鑰R_E^{a1}進行運算以產生終端 a1(如操作終端)與終端 a2 兩者之共享臨時金鑰$Secret_{a2}^{a1}$。❷$CT_Parm^{a2} = AES_{encrypt}$ ($Secret_{a2}^{a1}$, Parm)，亦即透過進階加密標準(AES)演算法使用終端 a1(如操作終端)與終端 a2 兩者之共享臨時金鑰$Secret_{a2}^{a1}$將第二更新參數Parm加密成終端 a2 之更新參數密文CT_Parm^{a2}。

【0097】 程序 P43：終端 a1(如操作終端)將更新資訊上傳至伺服器 c。例如，此更新資訊可包括下列資訊：(1)終端 a2 之更新參數密文CT_Parm^{a2}，(2)終端 a1(如操作終端)之第二臨時公鑰P_E^{a1}，(3)新終端 a3(如欲移除之終端)之終端識別碼 ID。

【0098】 程序 P44(見圖 4 之步驟 S46)：伺服器 c 收到來自終端 a1(如操作終端)之更新資訊後，由伺服器 c 執行合法性檢查。例如，此合法性檢查可包括：(1)確認無相同終端集合之有效帳號公鑰，(2)確認更新參數密文之對象與帳號之有效終端(不包括欲移除之終端)相同。若伺服器 c 所執行之合法性檢查之結果為合法，則由伺服器 c 將新終端 a3 失效。

【0099】 程序 P45：伺服器 c 回應相關資訊予終端 a1(如操作終端)。例如，若伺服器 c 所執行之合法性檢查之結果為合法，則伺服器 c 回應具有唯一值之帳號公鑰識別碼 ID 予終端 a1(如操作終端)；反之，若伺服器 c 所執行之合法性檢查之結果為不合法，則伺服器 c 回應目前帳號(如第一帳號 a)之有效終端資訊列表予終端 a1(如操作終端)。

【0100】 程序 P46(見圖 4 之步驟 S46)：伺服器 c 通知新終端 a3 已移除

此新終端 a3。

【0101】程序 P47：當終端 a2 上線時，由伺服器 c 將更新資訊同步至終端 a2。

【0102】程序 P48：終端 a2 使用自己之終端金鑰對之終端私鑰R_{Client}^{a2}進行解密以得到第二更新參數Parm。例如，由終端 a2 運算下列二個公式：❶$Secret_{a2}^{a1} = ECDH\ (P_E^{a1},\ R_{Client}^{a2})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定將終端 a1(如操作終端)之第二臨時公鑰P_E^{a1}與終端 a2 自己之終端金鑰對之終端私鑰R_{Client}^{a2}進行運算以產生終端 a1(如操作終端)與終端 a2 兩者之共享臨時金鑰$Secret_{a2}^{a1}$。❷$Parm = AES_{decrypt}\ (Secret_{a2}^{a1},\ CT_Parm^{a2})$，亦即透過進階加密標準(AES)演算法以使用終端 a1(如操作終端)與終端 a2 兩者之共享臨時金鑰$Secret_{a2}^{a1}$配合終端 a2 之更新參數密文CT_Parm^{a2}來解密出第二更新參數Parm。

【0103】程序 P49(見圖 4 之步驟 S48)：終端 a2(如其餘終端)更新自己之帳號金鑰對。例如，由終端 a2 運算下列二個公式：❶$R_{Account}^{a} = R_{Account}^{a}$ XOR Parm，亦即將第一帳號 a 之帳號私鑰$R_{Account}^{a}$與第二更新參數Parm兩者進行互斥或(XOR)運算以產生第二新帳號金鑰對之第二新帳號私鑰$R_{Account}^{a}$。❷$P_{Account}^{a} = R_{Account}^{a} * G$，亦即依據第二新帳號私鑰$R_{Account}^{a}$與橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定所使用之橢圓曲線之基點G以產生或推論出第二新帳號金鑰對之第二新帳號公鑰$P_{Account}^{a}$。

【0104】圖 11 為本發明之多終端之端對端加密通訊方法中，有關圖 5 所示「收發訊息」之實施例示意圖。如圖 11 所示，收發訊息之情境實施時，假設第二帳號 b(見圖 7)已再成功新增一新終端 b2，且由終端 a1(如發訊終端)初

次發送訊息給第二帳號 b，則本實施例可包括下列程序 P51 至程序 P65 之內容。

【0105】程序 P51(見圖 5 之步驟 S51)：終端 a1(如發訊終端)選擇第二帳號 b 作為收訊帳號，並確認未對第二帳號 b(如收訊帳號)產生棘輪金鑰 $RatchetKey_1^{a1\_b}$(如第一代棘輪金鑰)。

【0106】程序 P52(見圖 5 之步驟 S52)：終端 a1(如發訊終端)產生一具有第三臨時公鑰P_E^{a1}與第三臨時私鑰R_E^{a1}之第三臨時金鑰對。

【0107】程序 P53(見圖 5 之步驟 S52)：終端 a1(如發訊終端)計算棘輪金鑰$RatchetKey_1^{a1_b}$(如第一代棘輪金鑰)。例如，由終端 a1(如發訊終端)運算下列公式：$RatchetKey_1^{a1\_b} = ECDH\ (P_{Account}^{b}, R_E^{a1})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定以使用第二帳號 b(如收訊帳號)之帳號公鑰$P_{Account}^{b}$與終端 a1(如發訊終端)之第三臨時私鑰R_E^{a1}計算出棘輪金鑰$RatchetKey_1^{a1_b}$(如第一代棘輪金鑰)。

【0108】程序 P54(見圖 5 之步驟 S53)：終端 a1(如發訊終端)使用棘輪金鑰 $RatchetKey_1^{a1\_b}$ (如第一代棘輪金鑰)與第一常數衍生出訊息金鑰 $MessageKey_1^{a1\_b}$，並由終端 a1(如發訊終端)使用第二常數將棘輪金鑰 $RatchetKey_1^{a1\_b}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰$RatchetKey_2^{a1_b}$(如第二代棘輪金鑰)。

【0109】例如，由終端 a1(如發訊終端)運算下列二個公式：❶$MessageKey_1^{a1_b} = HMAC\ (RatchetKey_1^{a1_b}, 0x1)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第一常數(如0x1)將棘輪金鑰$RatchetKey_1^{a1_b}$(如第一代棘輪金鑰)衍生為訊息金鑰$MessageKey_1^{a1_b}$(如第一代訊息金鑰)。❷$RatchetKey_2^{a1_b}$ =

HMAC (RatchetKey$_1^{a1_b}$, 0x2)，亦即使用第二常數(如0x2)將棘輪金鑰RatchetKey$_1^{a1_b}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰RatchetKey$_2^{a1_b}$(如第二代棘輪金鑰)。

【0110】程序P55(見圖5之步驟S54)：終端a1(如發訊終端)使用訊息金鑰將訊息Message進行加密以產生訊息密文CT_Message^{a1_b}。例如，由終端a1(如發訊終端)運算下列公式：CT_Message^{a1_b} = AES$_{encrypt}$ (MessageKey$_1^{a1_b}$, Message)，亦即透過進階加密標準(AES)演算法以使用訊息金鑰MessageKey$_1^{a1_b}$(如第一代訊息金鑰)將訊息Message進行加密而產生訊息密文CT_Message^{a1_b}。

【0111】程序P56：終端a1(如發訊終端)選擇第一帳號a作為收訊帳號，並確認未對第一帳號a產生棘輪金鑰RatchetKey$_1^{a1_a}$(如第一代棘輪金鑰)。

【0112】程序P57：終端a1(如發訊終端)產生終端a1之第三臨時公鑰P_E^{a1}與第三臨時私鑰R_E^{a1}。

【0113】程序P58：終端a1(如發訊終端)計算棘輪金鑰RatchetKey$_1^{a1_a}$(如第一代棘輪金鑰)。例如，由終端a1(如發訊終端)運算下列公式：RatchetKey$_1^{a1_a}$ = ECDH ($P_{Account}^{a}$, R_E^{a1})，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定以使用第一帳號a之帳號公鑰$P_{Account}^{a}$與終端a1(如發訊終端)之第三臨時私鑰R_E^{a1}計算出棘輪金鑰RatchetKey$_1^{a1_a}$(如第一代棘輪金鑰)。

【0114】程序P59：終端a1(如發訊終端)使用棘輪金鑰RatchetKey$_1^{a1_a}$(如第一代棘輪金鑰)衍生出訊息金鑰MessageKey$_1^{a1_a}$(如第一代訊息金鑰)，並使用第二常數將棘輪金鑰MessageKey$_1^{a1_a}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰RatchetKey$_2^{a1_a}$(如第二代棘輪金鑰)。

【0115】例如，由終端 a1(如發訊終端)運算下列二個公式：❶$MessageKey_1^{a1_a} = HMAC\ (RatchetKey_1^{a1_a}, 0x1)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第一常數(如0x1)將棘輪金鑰$MessageKey_1^{a1_a}$(如第一代棘輪金鑰)衍生為訊息金鑰$MessageKey_1^{a1_a}$(如第一代訊息金鑰)。❷$RatchetKey_2^{a1_a} = HMAC\ (RatchetKey_1^{a1_a}, 0x2)$，亦即使用第二常數(如0x2)將棘輪金鑰$RatchetKey_1^{a1_a}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰$RatchetKey_2^{a1_a}$(如第二代棘輪金鑰)。

【0116】程序 P60：終端 a1(如發訊終端)將訊息Message進行加密以產生訊息密文$CT_Message^{a1_a}$。例如，由終端 a1(如發訊終端)運算下列公式：$CT\_Message^{a1\_a} = AES_{encrypt}\ (MessageKey_1^{a1\_a}, Message)$，亦即透過進階加密標準(AES)演算法以使用訊息金鑰$MessageKey_1^{a1_a}$(如第一代訊息金鑰)將訊息Message進行加密而產生訊息密文$CT_Message^{a1_a}$。

【0117】程序 P61(見圖 5 之步驟 S56)：終端 a1(如發訊終端)將訊息密文與金鑰資訊上傳至伺服器 c。例如，有關第一帳號 a 之訊息密文與金鑰資訊可包括：(1)訊息密文$CT_Message^{a1_a}$，(2)金鑰資訊(使用之帳號公鑰識別碼 ID、棘輪金鑰之代數)，(3)如為棘輪金鑰為第一代棘輪金鑰，則需再包括(附加)第三臨時公鑰。此外，有關第二帳號 b(如收訊帳號)之訊息密文與金鑰資訊可包括：(1)訊息密文$CT_Message^{a1_b}$，(2)金鑰資訊(使用之帳號公鑰識別碼 ID、棘輪金鑰之代數)，(3)如棘輪金鑰為第一代棘輪金鑰，則需再包括(附加)第三臨時公鑰。

【0118】程序 P62(見圖 5 之步驟 S57)：伺服器 c 接收到訊息密文後，檢查帳號公鑰是否有效。若此帳號公鑰為有效，則伺服器 c 回應帳號公鑰為有

效之相關資訊(如正確或成功)予終端 a1(如發訊終端)，並儲存訊息密文；反之，若帳號公鑰為無效，則伺服器 c 回應帳號公鑰為無效之相關資訊(如錯誤或失敗)予終端 a1(如發訊終端)。

【0119】程序 P63(見圖 5 之步驟 S58)：終端 a2、新終端 b1 或新終端 b2(如收訊終端)上線後，從伺服器 c 收到各自對應之訊息密文(加密訊息)。

【0120】程序 P64(見圖 5 之步驟 S59)：終端 a2、新終端 b1 或新終端 b2(如收訊終端)衍生對應之棘輪金鑰。例如，由新終端 b1 或新終端 b2(如收訊終端)運算下列公式：$RatchetKey_1^{a1\_b} = ECDH\ (P_E^{a1}, R_{Account}^{b})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定以使用終端 a1(如發訊終端)之第三臨時公鑰P_E^{a1}與第二帳號 b(如收訊帳號)之帳號私鑰$R_{Account}^{b}$計算出對應之棘輪金鑰$RatchetKey_1^{a1_b}$。此外，由終端 a2(如收訊終端)運算下列公式：$RatchetKey_1^{a1\_a} = ECDH\ (P_E^{a1}, R_{Account}^{a})$，亦即依據橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定以使用終端 a1(如發訊終端)之第三臨時公鑰P_E^{a1}與第一帳號 a 之帳號私鑰$R_{Account}^{a}$計算出對應之棘輪金鑰$RatchetKey_1^{a1_a}$。

【0121】程序 P65(見圖 5 之步驟 S59)：終端 a2、新終端 b1 或新終端 b2(如收訊終端)使用第一常數或第二常數解密訊息(訊息密文)。例如，由新終端 b1 或新終端 b2(如收訊終端)運算下列三個公式：❶$MessageKey_1^{a1_b} = HMAC\ (RatchetKey_1^{a1_b}, 0x1)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第一常數(如 0x1)將棘輪金鑰$RatchetKey_1^{a1_b}$(如第一代棘輪金鑰)衍生為訊息金鑰$MessageKey_1^{a1_b}$(如第一代訊息金鑰)。❷$RatchetKey_2^{a1_b} = HMAC\ (RatchetKey_1^{a1_b}, 0x2)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第二常數(如0x2)將棘輪金鑰$RatchetKey_1^{a1_b}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰

$RatchetKey_2^{a1\_b}$(如第二代棘輪金鑰)。❸$Message = AES_{decrypt}(MessageKey_1^{a1_b}, CT_Message^{a1_b})$，亦即透過進階加密標準(AES)演算法以使用訊息金鑰$MessageKey_1^{a1_b}$(如第一代訊息金鑰)與訊息密文$CT_Message^{a1_b}$解密出訊息Message。

【0122】此外，由終端 a2(如收訊終端)運算下列三個公式：❶$MessageKey_1^{a1_a} = HMAC(RatchetKey_1^{a1_a}, 0x1)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第一常數(如0x1)將棘輪金鑰$RatchetKey_1^{a1_a}$(如第一代棘輪金鑰)衍生為訊息金鑰$MessageKey_1^{a1_a}$(如第一代訊息金鑰)。❷$RatchetKey_2^{a1_a} = HMAC(RatchetKey_1^{a1a}, 0x2)$，亦即使用金鑰雜湊訊息認證碼(HMAC)配合第二常數(如0x2)將棘輪金鑰$RatchetKey_1^{a1_a}$(如第一代棘輪金鑰)更新成下一代棘輪金鑰$RatchetKey_2^{a1_a}$(如第二代棘輪金鑰)。❸$Message = AES_{decrypt}(MessageKey_1^{a1_a}, CT_Message^{a1a})$，亦即透過進階加密標準(AES)演算法以使用訊息金鑰$MessageKey_1^{a1_a}$(如第一代訊息金鑰)與訊息密文$CT_Message^{a1_a}$解密出訊息Message。

【0123】再者，本發明還提供一種針對多終端之端對端加密通訊方法之電腦可讀媒介，係應用於具有處理器及/或記憶體之計算裝置或電腦中，且電腦可讀媒介儲存有語音指令，並可利用計算裝置或電腦透過處理器及/或記憶體執行電腦可讀媒介，以於執行電腦可讀媒介時執行上述內容。

【0124】在一實施例中，處理器可為微處理器、中央處理器(CPU)、圖形處理器(GPU)、微控制器(MCU)等，記憶體可為隨機存取記憶體(RAM)、唯讀記憶體(ROM)、記憶卡、硬碟(如雲端/網路/外接式硬碟)、光碟、隨身碟、資料庫等，且計算裝置或電腦可為計算機、平板電腦、個人電腦、筆記型電腦、

桌上型電腦、伺服器(如雲端/遠端/網路伺服器)、智慧型手機等，但不以此為限。

【0125】綜上，本發明之多終端之端對端加密通訊方法及電腦可讀媒介至少具有下列特色、優點或技術功效。

【0126】一、本發明於使用者擁有多個終端(如發訊終端/收訊終端)時，使用者可以同時使用多個終端發送與接收訊息密文(加密訊息)，且各終端間之訊息可以保持一致。

【0127】二、本發明能使各終端間具有訊息之一致性，以利使用者使用任一終端發送或接收一則訊息時，使用者之其餘終端能自動同步此則訊息。

【0128】三、本發明能透過使用者之多個(所有)終端擁有一對相同之帳號金鑰對，以利達成使用者之終端之數量增加時，不會增加發送訊息密文(加密訊息)之數量。

【0129】四、本發明利用同一使用者之多個終端共享同一帳號金鑰對，當終端(如發訊終端)發送訊息時，終端與收訊帳號之帳號公鑰進行金鑰交換，隨後使用棘輪金鑰衍生出訊息金鑰以進行訊息之加密，此訊息便能被收訊帳號之多個(所有)終端解密，有利於達到終端對帳號之端對端加密，且終端所傳送之訊息密文(加密訊息)之數量不會受到使用者之終端之數量增加而增加。

【0130】五、本發明之發訊終端可以只需傳送一則訊息密文(加密訊息)，便能使收訊帳號下之多個(所有)終端都可以解密此訊息密文(加密訊息)。

【0131】六、本發明之訊息金鑰皆由多個終端之間協商產生，可以不必上傳訊息金鑰至伺服器，亦可以不使用任何形式加密傳送訊息金鑰。

【0132】七、本發明能於使用者異動終端時，透過帳號金鑰對之更新及

同步機制，以利達成終端之異動後仍具有端對端加密之保護。

【0133】八、當使用者進行終端之異動時，本發明能透過帳號金鑰對之更新來確保端對端加密之安全性，使新終端可以收到並解密新的訊息密文(加密訊息)，而被移除之終端則無法收到且無法解密新的訊息。

【0134】九、當使用者進行終端之異動時，本發明之終端會進行帳號金鑰對之更新，並進行使用者之其餘終端之同步與更新，以利確保各終端之帳號金鑰對一致。

【0135】十、本發明能利用棘輪金鑰(棘輪方式)產生訊息金鑰，以利確保訊息或訊息金鑰之前向安全或前向保密(FS)。

【0136】十一、本發明之訊息加密所使用之訊息金鑰透過單向性之雜湊函數(如金鑰雜湊訊息認證碼 HMAC)來產生，故即便有第三者(如駭客)取得了當代之訊息金鑰，也無法逆推出先前(如前代)之訊息金鑰，以利保有訊息或訊息金鑰之前向安全或前向保密(FS)。

【0137】十二、本發明之同一使用者之多個(所有)終端可以擁有一對相同之帳號金鑰對，當有終端要發送訊息時，能使用橢圓曲線迪菲-赫爾曼金鑰交換(ECDH)協定與金鑰棘輪之方式，對臨時私鑰與收訊帳號之帳號公鑰進行運算出訊息金鑰來加密訊息，以利發送訊息密文(加密訊息)之數量不受使用者之終端之數量影響，亦能保有訊息或訊息金鑰之前向安全或前向保密(FS)。

【0138】上述實施形態僅例示性說明本發明之原理、特點及其功效，並非用以限制本發明之可實施範疇，任何熟習此項技藝之人士均能在不違背本發明之精神及範疇下，對上述實施形態進行修飾與改變。任何使用本發明所揭示內容而完成之等效改變及修飾，均仍應為申請專利範圍所涵蓋。因此，

本發明之權利保護範圍應如申請專利範圍所列。

【符號說明】

【0139】

a:第一帳號

a1, a2:終端

a3:新終端

b:第二帳號

b1, b2:新終端

c:伺服器

P12 至 P13:程序

P22 至 P23:程序

P31, P34, P36 至 P37:程序

P43, P45 至 P47:程序

P61 至 P63:程序

S11 至 S14:步驟

S21 至 S22:步驟

S31 至 S38:步驟

S41 至 S48:步驟

S51 至 S59:步驟

第 112108749 號專利申請案
112 年 12 月 13 日修正替換頁

【發明申請專利範圍】

【請求項1】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端透過橢圓曲線密碼學之方式產生一具有終端公鑰與終端私鑰之終端金鑰對，以由該新終端上傳該終端金鑰對之終端公鑰至該伺服器，再由該伺服器將使用者目前之帳號下之有效終端資訊列表回傳給該新終端，俾由該新終端依據該有效終端資訊列表判斷應進行帳號金鑰對之初始化或更新。

【請求項2】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端透過橢圓曲線密碼學之方式產生一具有帳號公鑰與帳號私鑰之帳號金鑰對，以由該新終端上傳該帳號金鑰對之帳號公鑰至該伺服器中儲存而完成該帳號金鑰對之初始化，再由該伺服器依據該帳號金鑰對之帳號公鑰回應具有唯一值之帳號公鑰識別碼予該新終端。

【請求項3】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺

服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端透過非經由該伺服器之方式從舊終端取得目前之帳號私鑰，且由該新終端產生更新參數，以由該新終端使用目前之該帳號私鑰與該更新參數產生一具有新帳號公鑰與新帳號私鑰之新帳號金鑰對，再由該新終端透過橢圓曲線密碼學之方式產生一具有第一臨時公鑰與第一臨時私鑰之第一臨時金鑰對。

【請求項4】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端使用舊終端之終端公鑰與第一臨時金鑰對之第一臨時私鑰用於加密更新參數，以由該新終端將新帳號公鑰、該第一臨時公鑰與已加密之該更新參數上傳至該伺

服器，再由該伺服器將已加密之該更新參數同步至該舊終端，俾由該舊終端更新自己之帳號金鑰對。

【請求項5】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由操作終端產生更新參數，以由該操作終端使用目前之帳號私鑰與該更新參數產生一具有新帳號公鑰與新帳號私鑰之新帳號金鑰對，再由該操作終端透過橢圓曲線密碼學之方式產生一具有另一臨時公鑰與另一臨時私鑰之另一臨時金鑰對。

【請求項6】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由操作終端使用欲移除之終端以外之其餘終端之終端公鑰與另一臨時私鑰用於加密更新參數，以由該操作終端將新帳號公鑰、另一臨時公鑰、已加密之該更新參數與欲移除之該終端之終端識別碼上傳至該伺服器，再由該伺服器將欲移除之該終端失效，俾由該伺服器將已加密之該更新參數同步至欲移除之該終端以外之其餘終端，進而由欲移除之該終端以外之其餘終端更新自己之帳號金鑰對。

【請求項7】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由該伺服器檢查該收訊帳號之帳號公鑰之有效性，若該帳號公鑰為無效，則該伺服器回覆最新的帳號公鑰予該發訊終端，以使該發訊終端重新產生該棘輪金鑰並丟棄該訊息密文，而若該帳號公鑰為有效，則該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之該多個收訊終端。

【請求項8】如請求項 7 所述之多終端之端對端加密通訊方法，更包括由該發訊終端使用金鑰雜湊訊息認證碼配合第一常數將該棘輪金鑰衍生為該訊息金鑰，以由該發訊終端使用該訊息金鑰進行該訊息之對稱式加密用於產生該訊息密文，再由該收訊終端使用該訊息金鑰將該訊息密文進行解密出該訊息。

【請求項9】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端將帳號私鑰與更新參數兩者進行互斥或運算以產生新帳號金鑰對之新帳號私鑰，且由該新終端依據該新帳號金鑰對之新帳號私鑰與橢圓曲線迪菲-赫爾曼金鑰交換協定所使用之橢圓曲線之基點以產生或推論出該新帳號金鑰對之新帳號公鑰，再由該新終端透過橢圓曲線密碼學之方式產生一具有第一臨時公鑰與第一臨時私鑰之第一臨時金鑰對。

【請求項10】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：由新終端依據橢圓曲線迪菲-赫爾曼金鑰交換協定將舊終端之終端公鑰與該新終端之第一臨時私鑰進行運算以產生該舊終端與該新終端兩者之共享臨時金鑰，再由該新終端透過進階加密標準演算法將該舊終端與該新終端兩者之該共享臨時金鑰配合更新參數進行運算以產生該舊終端之更新參數密文。

【請求項11】一種多終端之端對端加密通訊方法，包括：

由發訊終端對收訊帳號產生一具有臨時公鑰與臨時私鑰之臨時金鑰對，再由該發訊終端將該收訊帳號之帳號公鑰與該臨時金鑰對之臨時私鑰進行運算以產生對該收訊帳號之棘輪金鑰；

由該發訊終端使用對該收訊帳號之棘輪金鑰衍生出訊息金鑰，再由該發訊終端使用對該收訊帳號之棘輪金鑰所衍生出之該訊息金鑰將訊息加密以產生訊息密文，俾由該發訊終端將該訊息密文與金鑰資訊上傳至伺服器；以及

由該伺服器將該訊息密文與該金鑰資訊發送至該收訊帳號下之多個收訊終端，以於各該收訊終端收到該訊息密文時，由各該收訊終端使用該伺服器所發送之該金鑰資訊以產生對應該棘輪金鑰之該訊息金鑰，俾由各該收訊終端使用對應該棘輪金鑰之該訊息金鑰以從該訊息密文中解密出該訊息；

其中，該多終端之端對端加密通訊方法更包括：在該伺服器收到來自新終端之更新資訊後，由該伺服器執行合法性檢查，其中，該伺服器之合法性檢查包括：確認無相同終端集合之有效帳號公鑰，以及確認更新參數密文之對象與帳號之有效終端相同。

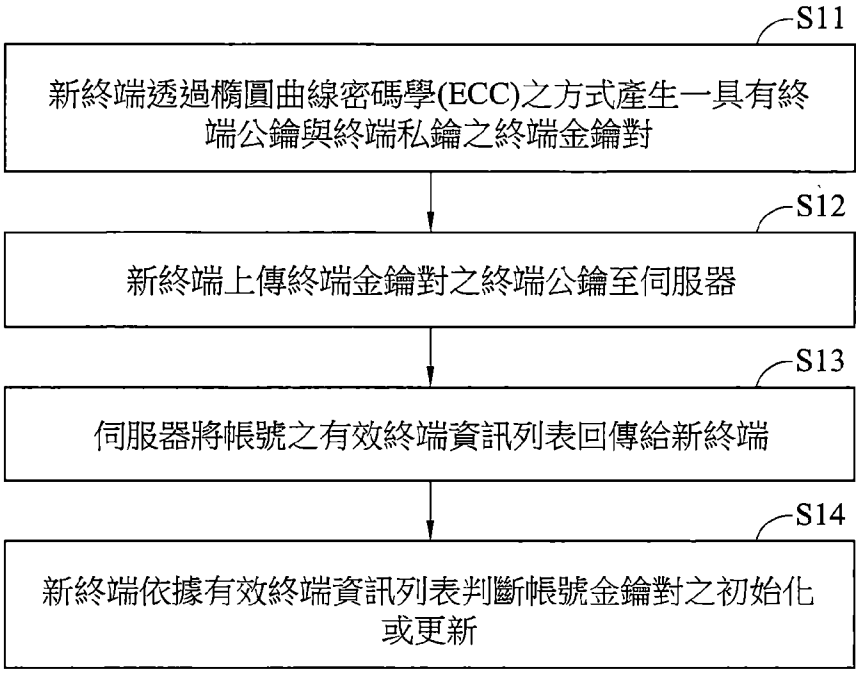
【請求項12】如請求項 11 所述之多終端之端對端加密通訊方法，更包括由該發訊終端依據橢圓曲線迪菲-赫爾曼金鑰交換協定以使用帳號公鑰

與該發訊終端之臨時私鑰計算出該棘輪金鑰，並由該發訊終端使用該棘輪金鑰與第一常數衍生出該訊息金鑰，且由該發訊終端使用第二常數將該棘輪金鑰更新成下一代棘輪金鑰。

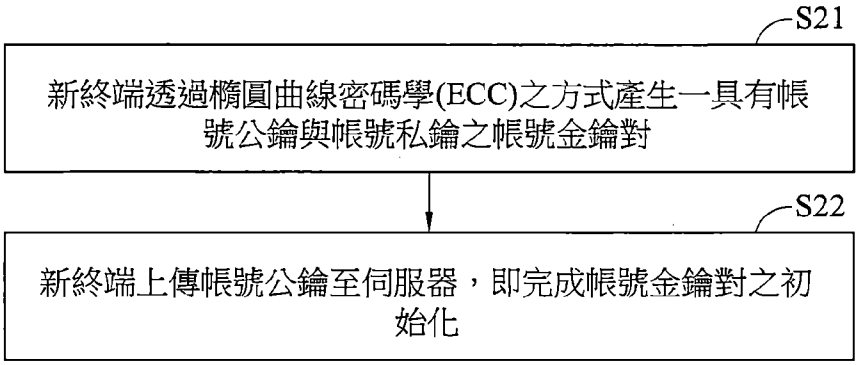
【請求項13】如請求項 11 所述之多終端之端對端加密通訊方法，更包括由該發訊終端使用金鑰雜湊訊息認證碼配合第一常數將該棘輪金鑰衍生為該訊息金鑰，且由該發訊終端使用第二常數將該棘輪金鑰更新成下一代棘輪金鑰。

【請求項14】一種電腦可讀媒介，應用於計算裝置或電腦中，係儲存有指令，以執行如請求項 1 至 13 之任一者所述之多終端之端對端加密通訊方法。

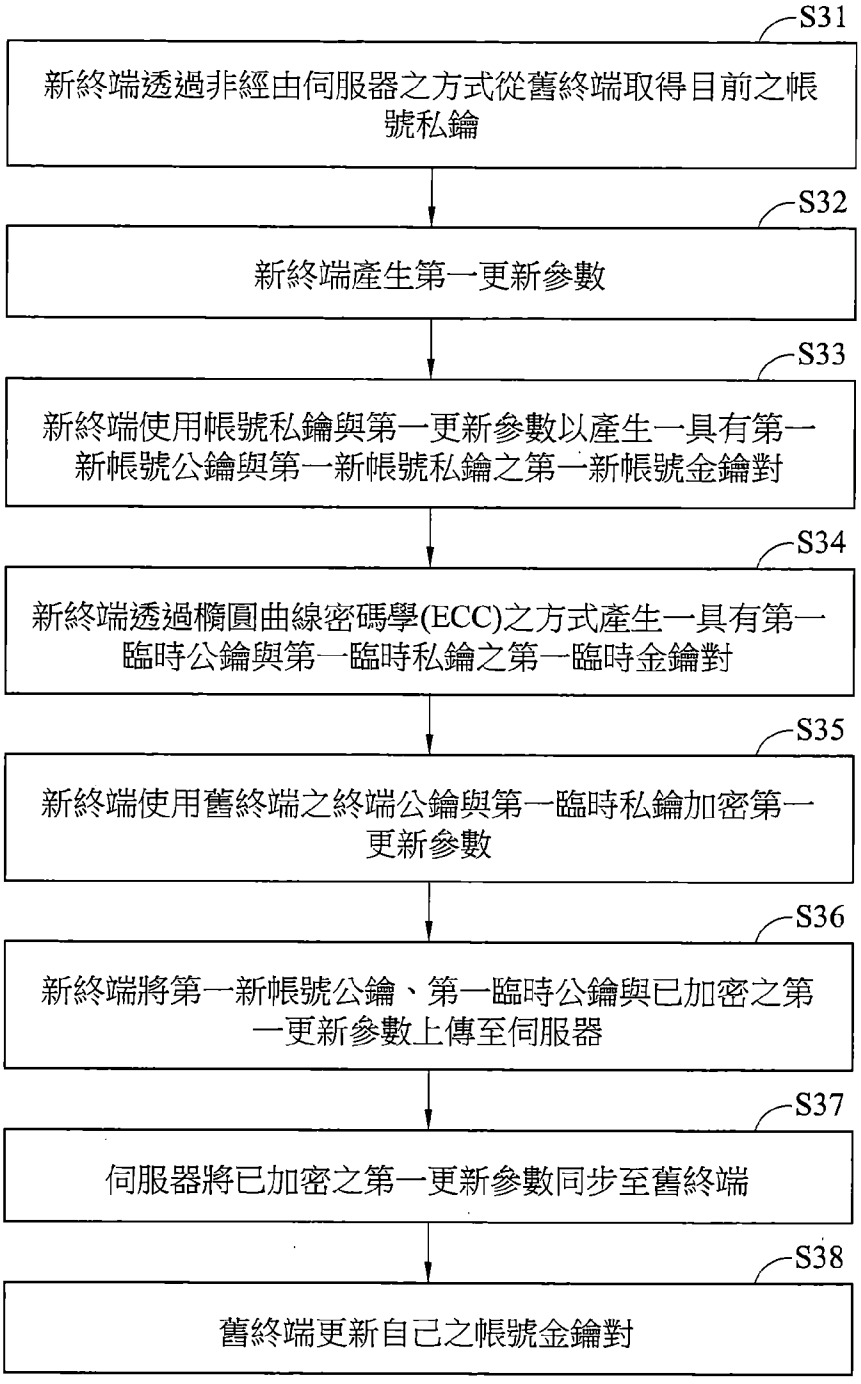
【發明圖式】


S11
新終端透過橢圓曲線密碼學(ECC)之方式產生一具有終端公鑰與終端私鑰之終端金鑰對
S12
新終端上傳終端金鑰對之終端公鑰至伺服器
S13
伺服器將帳號之有效終端資訊列表回傳給新終端
S14
新終端依據有效終端資訊列表判斷帳號金鑰對之初始化或更新

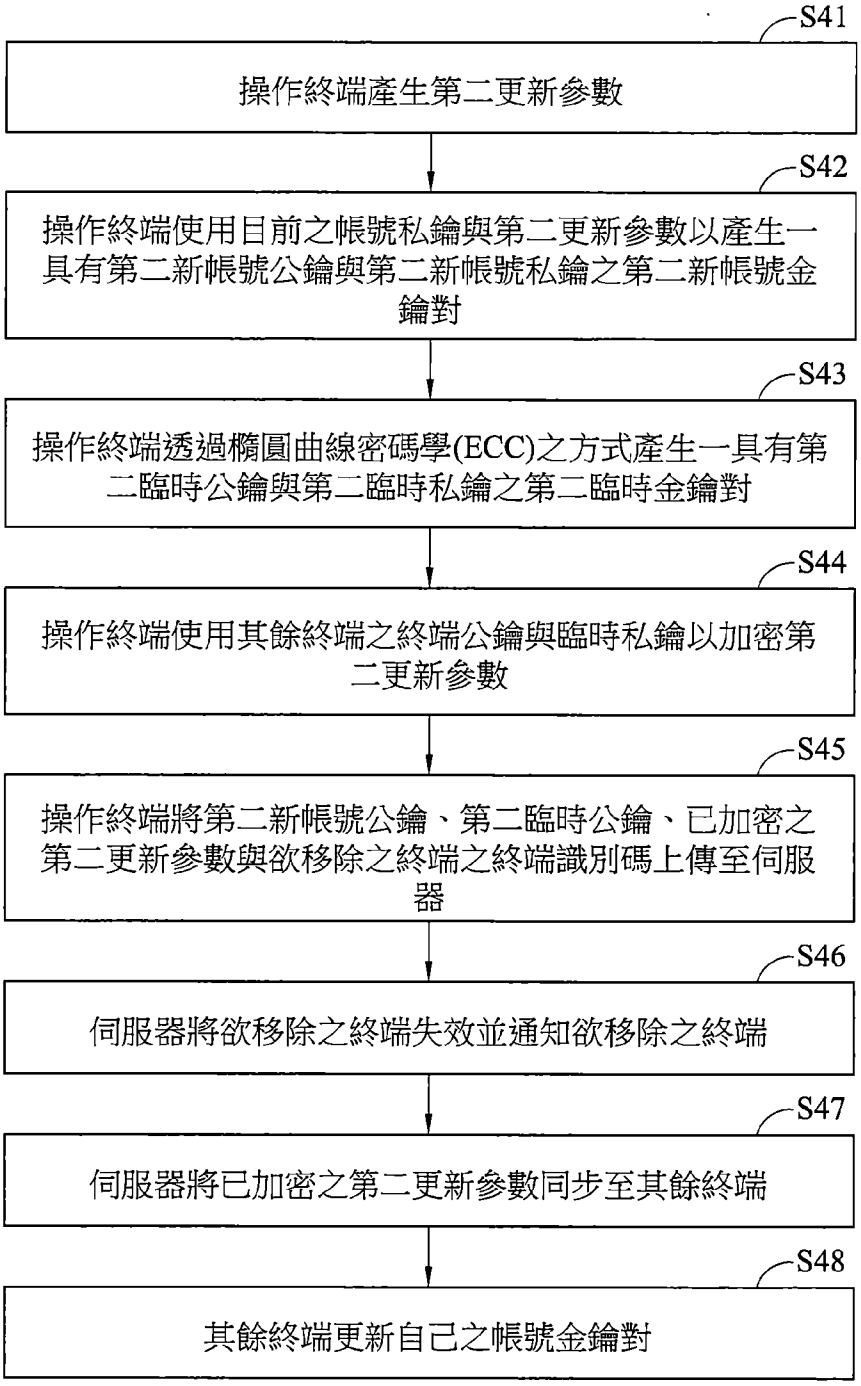
【圖 1】


S21
新終端透過橢圓曲線密碼學(ECC)之方式產生一具有帳號公鑰與帳號私鑰之帳號金鑰對
S22
新終端上傳帳號公鑰至伺服器，即完成帳號金鑰對之初始化

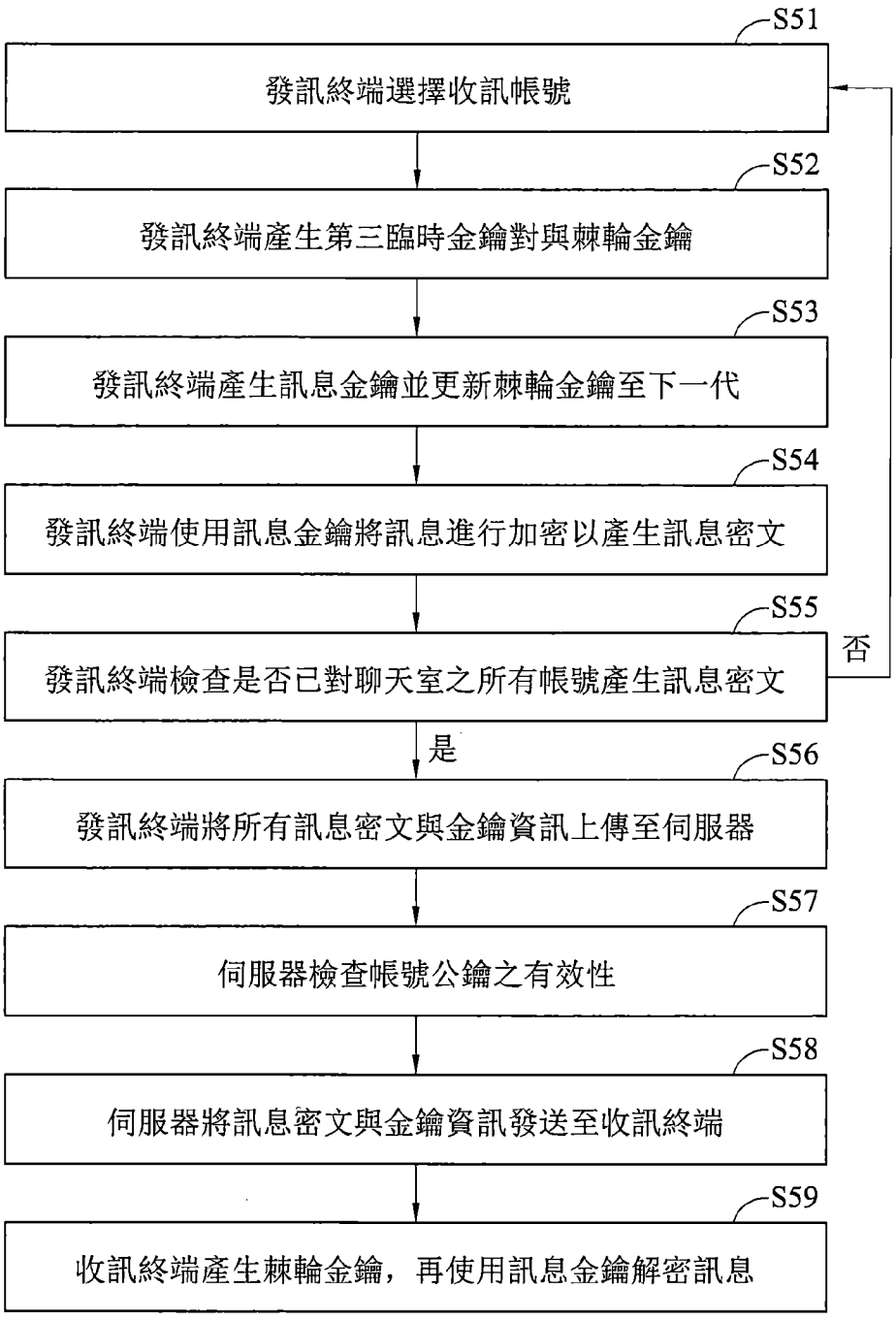
【圖 2】


S31
新終端透過非經由伺服器之方式從舊終端取得目前之帳號私鑰
S32
新終端產生第一更新參數
S33
新終端使用帳號私鑰與第一更新參數以產生一具有第一新帳號公鑰與第一新帳號私鑰之第一新帳號金鑰對
S34
新終端透過橢圓曲線密碼學(ECC)之方式產生一具有第一臨時公鑰與第一臨時私鑰之第一臨時金鑰對
S35
新終端使用舊終端之終端公鑰與第一臨時私鑰加密第一更新參數
S36
新終端將第一新帳號公鑰、第一臨時公鑰與已加密之第一更新參數上傳至伺服器
S37
伺服器將已加密之第一更新參數同步至舊終端
S38
舊終端更新自己之帳號金鑰對

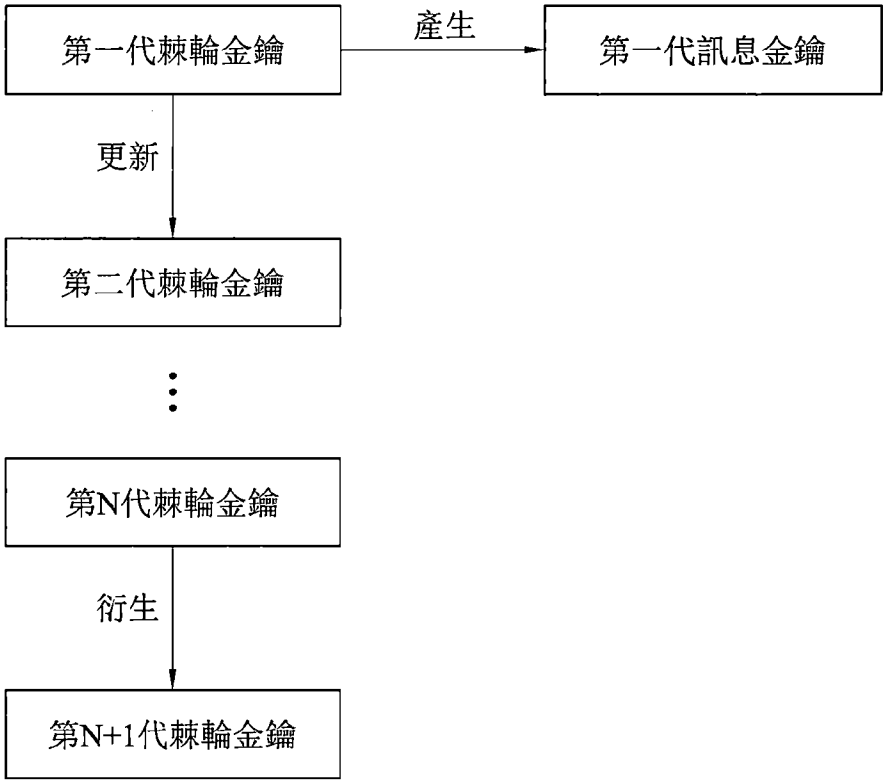
【圖 3】


S41
操作終端產生第二更新參數
S42
操作終端使用目前之帳號私鑰與第二更新參數以產生一具有第二新帳號公鑰與第二新帳號私鑰之第二新帳號金鑰對
S43
操作終端透過橢圓曲線密碼學(ECC)之方式產生一具有第二臨時公鑰與第二臨時私鑰之第二臨時金鑰對
S44
操作終端使用其餘終端之終端公鑰與臨時私鑰以加密第二更新參數
S45
操作終端將第二新帳號公鑰、第二臨時公鑰、已加密之第二更新參數與欲移除之終端之終端識別碼上傳至伺服器
S46
伺服器將欲移除之終端失效並通知欲移除之終端
S47
伺服器將已加密之第二更新參數同步至其餘終端
S48
其餘終端更新自己之帳號金鑰對

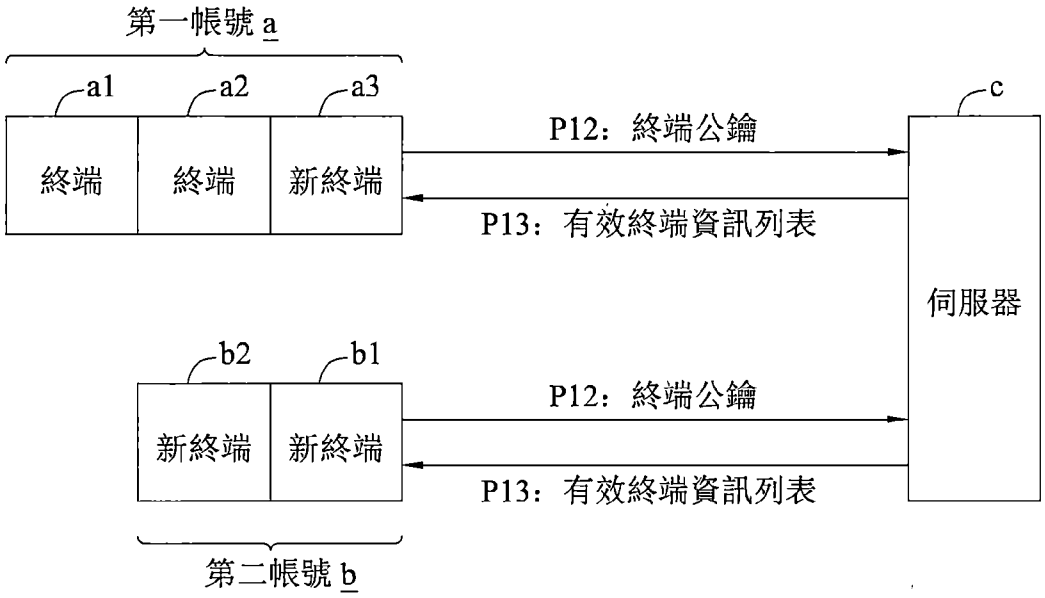
【圖 4】


S51
發訊終端選擇收訊帳號
S52
發訊終端產生第三臨時金鑰對與棘輪金鑰
S53
發訊終端產生訊息金鑰並更新棘輪金鑰至下一代
S54
發訊終端使用訊息金鑰將訊息進行加密以產生訊息密文
S55
發訊終端檢查是否已對聊天室之所有帳號產生訊息密文
否
是
S56
發訊終端將所有訊息密文與金鑰資訊上傳至伺服器
S57
伺服器檢查帳號公鑰之有效性
S58
伺服器將訊息密文與金鑰資訊發送至收訊終端
S59
收訊終端產生棘輪金鑰，再使用訊息金鑰解密訊息

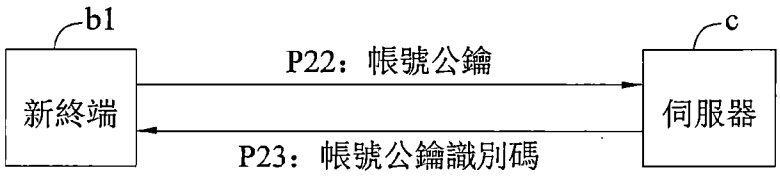
【圖 5】



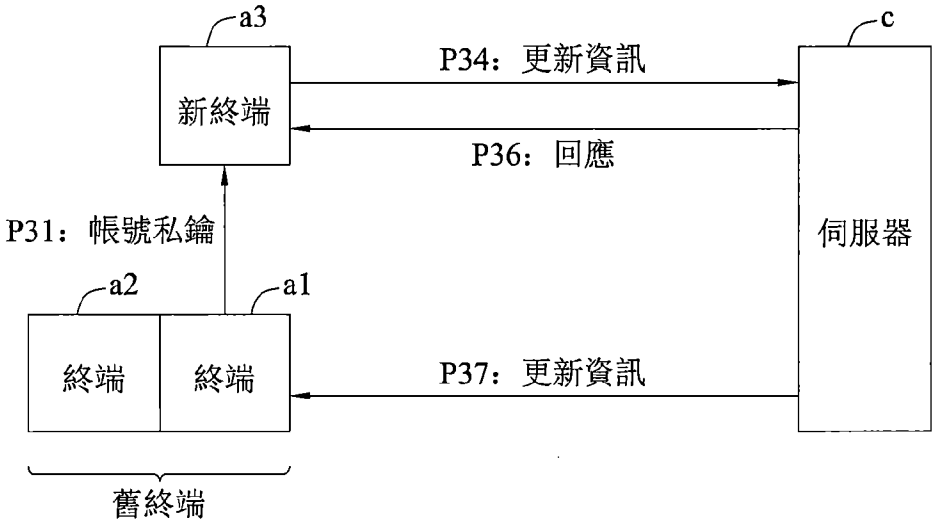
【圖 6】


第一帳號 a
a1
a2
a3
終端
終端
新終端
P12：終端公鑰
P13：有效終端資訊列表
c
伺服器
b2
b1
新終端
新終端
P12：終端公鑰
P13：有效終端資訊列表
第二帳號 b

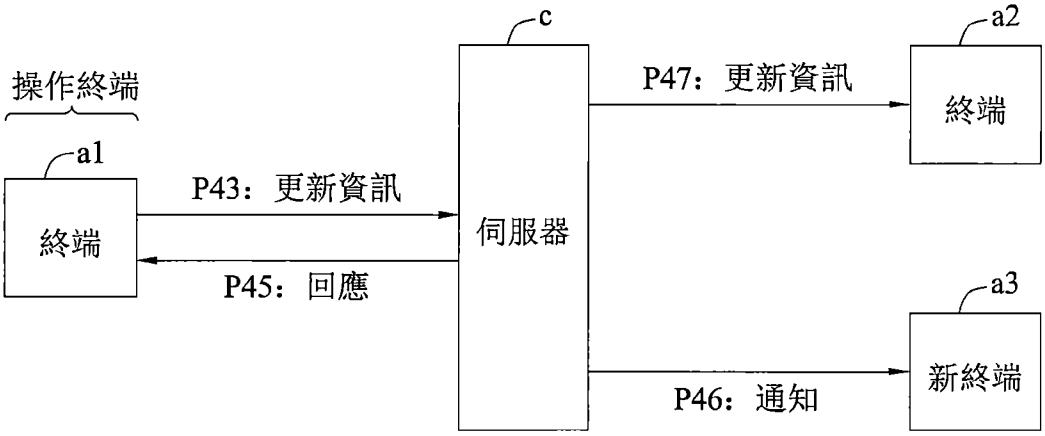
【圖 7】



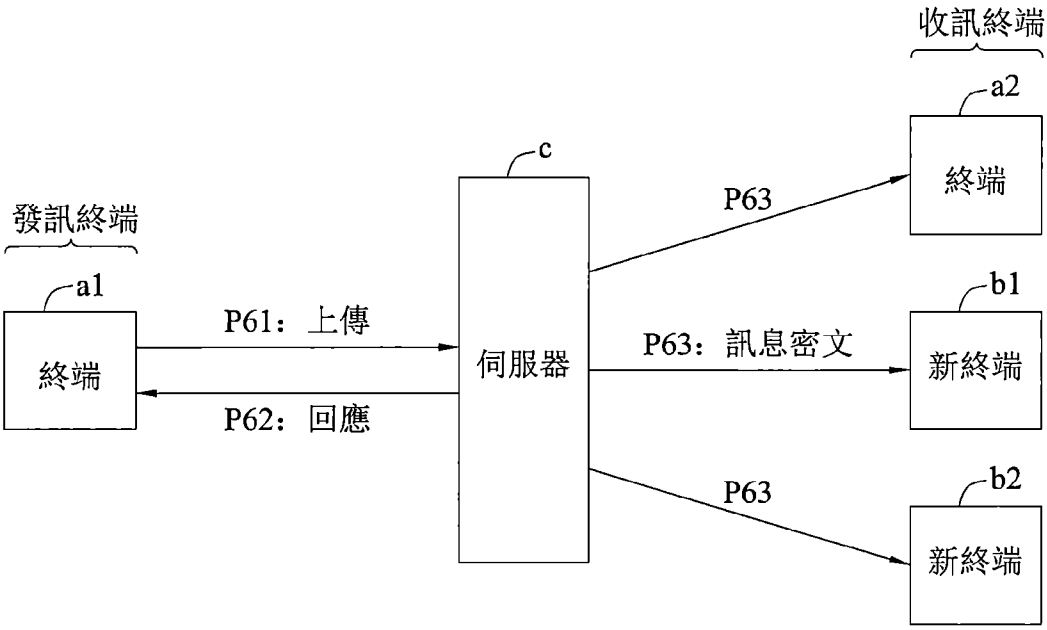
【圖 8】



【圖 9】



【圖 10】


收訊終端
a2
終端
c
P63
發訊終端
a1
終端
P61：上傳
P62：回應
伺服器
P63：訊息密文
b1
新終端
P63
b2
新終端

【圖 11】