201733302

(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 201733302 A

(43)公開日： 中華民國 106 (2017) 年 09 月 16 日

(21)申請案號：106105706 (22)申請日： 中華民國 106 (2017) 年 02 月 21 日

(51)Int. Cl.： *H04L9/14 (2006.01)* *H04L9/28 (2006.01)*
G06Q20/36 (2012.01)

(30)優先權：2016/02/23 英國 1603117.1
2016/03/24 英國 1605026.2
2016/11/15 英國 1619301.3

(71)申請人：恩鏈控股有限公司 (安地卡及巴布達) NCHAIN HOLDINGS LIMITED (AG)
安地卡及巴布達

(72)發明人：賴特 克雷格 WRIGHT, CRAIG (AU)；薩凡納 斯特凡 SAVANAH, STEPHANE (GB)

(74)代理人：王尊民

申請實體審查：無 申請專利範圍項數：25 項 圖式數：5 共 38 頁

(54)名稱

用於基於區塊鏈的系統結合錢包管理系統中的安全多方防遺失儲存及加密金鑰轉移

SECURE MULTIPARTY LOSS RESISTANT STORAGE AND TRANSFER OF CRYPTOGRAPHIC KEYS FOR BLOCKCHAIN BASED SYSTEMS IN CONJUNCTION WITH A WALLET MANAGEMENT SYSTEM

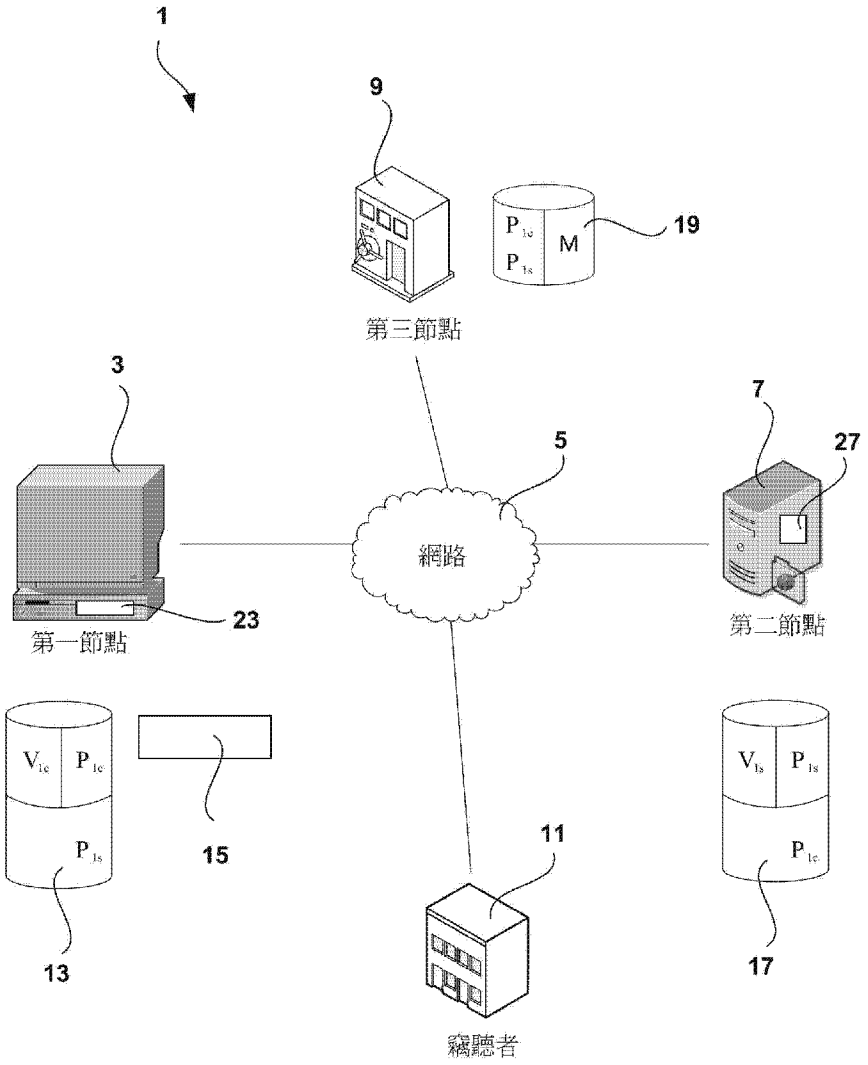
(57)摘要

本發明提供一種以電腦來完成的方法來控制一個與電腦相關的資源，例如數位錢包的存取。在一個或多個實施例中，可使用區塊鏈如比特幣區塊鏈來實現，但本發明並未在此方面上做限制。在錢包的起始設定期間使用本發明，能夠致能後續的操作如錢包交易以安全的方式透過一個不安全的通道，如網際網路來處理。根據本發明的一實施例的方法，包含將一確認元件(如一不對稱加密對中的一私人金鑰)分割成複數個份額；決定一網路中二個或更多節點上的一共同私密；以及使用共同私密以在二個或更多的節點上傳送確認元件的至少一個份額。份額的分割為使得沒有一個份額本身是足夠達成確認元件的。這個是指沒有一方儲存了整個私人金鑰，藉此提供金鑰的加強型安全性。必須要二個或更多的份額來恢復金鑰。份額儲存在分隔開來的位置，其中之一為獨立的備用或安全儲存位置。若其他份額的其中之一無法取得，份額能從備用處取回以確保金鑰(並且因此受控制的資源)仍然可以存取。為了確保份額的安全傳輸，共同私密在二個不同節點上互相獨立地產生，並且接著被使用來產生一加密金鑰。加密金鑰用來加密確認元件的至少一份額，或加密包含它的一信息，以確保份額安全地傳輸。

The invention provides a computer-implemented solution for controlling access to a computer-related resource such as, for example, a digital wallet. In one or more embodiments, the wallet may be implemented using a blockchain such as the Bitcoin blockchain but the invention is not limited in this regard. Use of the invention during the initial set-up of the wallet can enable subsequent operations such as wallet transactions to be handled in a secure manner over an insecure channel such as the internet. A method according to an embodiment of the invention can comprise the steps of splitting a verification element (such as a private key in an asymmetric cryptography pair) into a plurality of shares; determining a common secret at two or more

nodes in a network; and using the common secret to transmit at least one share of the verification element between the two or more nodes. The shares can be split such that no share on its own is sufficient to arrive at the verification element. This means that no one party stores the entire private key, providing for enhanced security of the key. Two or more shares are required to restore the key. The shares are stored at separate locations one of which is an independent back-up or safe-storage location. If one of the other shares becomes unavailable, the share can be retrieved from back up to ensure that the key (and thus the controlled resource) is still accessible. To ensure safe transmission of the share(s), the common secret is generated at two different nodes independently of each other and then used to generate an encryption key. The encryption key can be used to encrypt at least one share of the verification element, or a message comprising it, to ensure that the share(s) are transmitted securely.

指定代表圖：



符號簡單說明：

1・・・系統

3・・・第一節點

23・・・第一處理裝置

13、17、19・・・資料儲存

27・・・第二處理裝置

5・・・網路

7・・・第二節點

9・・・第三節點

11・・・竊聽者

15・・・使用者介面

P_{1C}・・・第一節點主要公用金鑰

P_{1S}・・・第二節點主要公用金鑰

V_{1C}・・・第一節點主要私人金鑰

V_{1S}・・・第二節點主要私人金鑰

M・・・信息

第1圖

201733302
專利案號：106105706
申請日：106/02/21
IPC分類：H04L 9/14 (2006.01)
H04L 9/28 (2006.01)
G06Q 20/36 (2012.01)

【發明摘要】

【中文發明名稱】

用於基於區塊鏈的系統結合錢包管理系統中的安全多方防遺失儲存及加密金鑰轉移

【英文發明名稱】

Secure Multiparty loss resistant Storage and Transfer of Cryptographic Keys for blockchain based systems in conjunction with a wallet management system

【中文】

本發明提供一種以電腦來完成的方法來控制一個與電腦相關的資源，例如數位錢包的存取。在一個或多個實施例中，可使用區塊鏈如比特幣區塊鏈來實現，但本發明並未在此方面上做限制。在錢包的起始設定期間使用本發明，能夠致能後續的操作如錢包交易以安全的方式透過一個不安全的通道，如網際網路來處理。根據本發明的一實施例的方法，包含將一確認元件(如一不對稱加密對中的一私人金鑰)分割成複數個份額；決定一網路中二個或更多節點上的一共同私密；以及使用共同私密以在二個或更多的節點上傳送確認元件的至少一個份額。份額的分割為使得沒有一個份額本身是足夠達成確認元件的。這個是指沒有一方儲存了整個私人金鑰，藉此提供金鑰的加強型安全性。必須要二個或更多的份額來恢復金鑰。份額儲存在分隔開來的位置，其中之一為獨立的備用或安全儲存位置。若其他份額的其中之一無法取得，份額能從備用處取回以確保金鑰(並且因此受控制的資源)仍然可以存取。為了確保份額的安全傳輸，共同私密在二個不同節點上互相獨立地產生，並且接著被使用來產生一加密金鑰。加密金鑰用來加密確認元件的至少一份額，或加密包含它的一信息，以確保份額安全地傳輸。

【英文】

The invention provides a computer-implemented solution for controlling access to a computer-related resource such as, for example, a digital wallet. In one or more embodiments, the wallet may be implemented using a blockchain such as the Bitcoin blockchain but the invention is not limited in this regard. Use of the invention during the initial set-up of the wallet can enable subsequent operations

such as wallet transactions to be handled in a secure manner over an insecure channel such as the internet. A method according to an embodiment of the invention can comprise the steps of splitting a verification element (such as a private key in an asymmetric cryptography pair) into a plurality of shares; determining a common secret at two or more nodes in a network; and using the common secret to transmit at least one share of the verification element between the two or more nodes. The shares can be split such that no share on its own is sufficient to arrive at the verification element. This means that no one party stores the entire private key, providing for enhanced security of the key. Two or more shares are required to restore the key. The shares are stored at separate locations one of which is an independent back-up or safe-storage location. If one of the other shares becomes unavailable, the share can be retrieved from back up to ensure that the key (and thus the controlled resource) is still accessible. To ensure safe transmission of the share(s), the common secret is generated at two different nodes independently of each other and then used to generate an encryption key. The encryption key can be used to encrypt at least one share of the verification element, or a message comprising it, to ensure that the share(s) are transmitted securely.

【指定代表圖】第1圖。

【代表圖之符號簡單說明】

1： 系統

3： 第一節點

23： 第一處理裝置

13、17、19： 資料儲存

27： 第二處理裝置

5： 網路

7： 第二節點

9： 第三節點

11： 竊聽者

15： 使用者介面

P_{1C}： 第一節點主要公用金鑰

P_{1S}： 第二節點主要公用金鑰

V_{1C}： 第一節點主要私人金鑰

V_{1S}： 第二節點主要私人金鑰

M： 信息

【發明說明書】

【中文發明名稱】

用於基於區塊鏈的系統結合錢包管理系統中的安全多方防遺失儲存及加密金鑰轉移

【英文發明名稱】

Secure Multiparty loss resistant Storage and Transfer of Cryptographic Keys for blockchain based systems in conjunction with a wallet management system

【技術領域】

【0001】 本發明一般關於電腦及資料安全，並且更特別的是本發明關於安全處理高敏感度的資料項目如加密金鑰。本發明提供一種存取控制機制。本發明特別適用於，但不限制於，用於電子(軟體)錢包。這個可包含，例如，使用在與加密貨幣，如比特幣有關的錢包。本發明提供一種優勢的存取控制機制。

【先前技術】

【0002】 密碼學牽涉到敏感資料的安全保存，以及在網路中的二個或更多節點之間的安全通信的技術。一節點可包含一行動通信裝置、一平板電腦、一筆記型電腦、桌上型電腦、其他形式的計算裝置及通信裝置、網路中的一伺服器裝置、網路中的客戶端裝置、分散式網路中的一個或多個節點等等。節點可與，例如，一自然人、一群人如公司的員工、一系統如銀行系統，或是一個分散式點對點底帳(例如，區塊鏈)相關。

【0003】 二個或更多的節點可經由一個不安全且容易遭到竊聽或被未授權的第三方給攔截的通信網路來連結。因此，節點間傳送的信息經常是以加密的方式來傳送。在接收時，預期的接收者利用對應的解密金鑰或其他的解密方法來解密信息。因此，此種通信的安全性依賴於避免第三方來決定對應的解密金鑰而定。

【0004】 一種已知的加密方法包含使用對稱金鑰演算法。在相同的對稱金鑰同時使用於平常文字信息的加密及密碼文字信息的解密的意義上，這些金鑰是對稱的。然而，對稱金鑰必須以安全的方式傳送到二個節點，來防止金鑰的未授權存取。這樣可包含，例如，實質上傳遞對稱金鑰到(授

權的)節點使得對稱金鑰永遠都不會透過一個不安全的通信網路來傳遞。然而，實質的傳遞並非永遠都是一個實際的選擇。因此，在這種加密系統中的一個問題在於透過一個不安全的電子網路如網際網路來建立二個節點之間的對稱金鑰(其可基於一個共同私密)。因此，提供一個對稱金鑰 (例如共享私密)的這個步驟是一個潛在的災難弱點。當對稱金鑰及協定是簡易且廣泛使用的話，則二個節點須要能安全地在不安全的網路環境中，決定一個共同私密。

【0005】 不對稱金鑰的使用，又稱為公用金鑰密碼學，將這個問題做了一定程度的緩解。當私人金鑰保持私密時，其對應的公用金鑰可變成可以公開取得的。在網路上攔截到私人金鑰並不會是災難性的事件。現存的協定包含迪菲-赫爾曼密鑰交換 (Diffie–Hellman key exchange)及三通協定(Three Pass Protocol)。

【0006】 然而，私人金鑰的儲存引起了重大的安全憂慮。將一數位錢包，例如一比特幣錢包列入考慮。數位錢包包含能夠讓使用者與其他節點連線的軟體，以便利用他們的電子資產實行交易，例如使用比特基金來購買產品及服務。公用金鑰密碼學經常使用於保護需要用於諸如連線及交易的關鍵資訊。私人金鑰經由安裝在使用者裝置(“客戶端”)上的錢包，抑或經由一錢包服務供應商(“伺服器”)而儲存起來。然而，若私人金鑰僅儲存在客戶端，私人金鑰可能會經由偷竊、遺失，或使用者的硬體，例如電腦手機等等的損壞而喪失。相似地，若是使用者死去或是變成無行為能力，私人金鑰的知識或存取權也會喪失，並且從而與錢包相關的基金也會變成無法存取。當私人金鑰的伺服器端儲存能夠克服這些問題時，使用者必須要有準備來信任服務供應商會將他們的私人金鑰保持私密。伺服器端的安全漏洞是一個實際且重大的風險。

【0007】 因此，令人想要的是提供一種能夠安全處理私密的解決方案。這個私密可為一個加密金鑰及/或可提供金鑰的存取權的事物。此種改良型解決方案現在開發出來了。根據本發明，提供了如後附的請求項所定義的改良型解決方案。

【發明內容】

【0008】 本發明可提供一種電腦來完成的方法。該方法能夠控制一資源的存取。該方法可稱為一種確認或認證方法。該方法也可稱之為加密金鑰管理方案。資源可為任何形式的實體或電子資源。在一實施例中，資源為一數位錢包或其他與一種貨幣形式有關的資源。資源可為一個比特幣錢包或用於加密貨幣資源的管理的錢包。本發明可提供控制一數位錢包(及對應系統)的存取權的方法。

【0009】 本發明可在啟動期間、註冊期間、或經由一個不安全的通信通道(例如網際網路)來創造一個數位錢包期間使用，來讓後續的錢包相關操作，如欲處理、通信及/或創造的交易能夠以安全的型態來完成。

【0010】 本發明的一個或多個實施例可包含自一個現存的加密金鑰對產生加密金鑰的步驟。這個步驟可包含下列步驟：

根據至少一第一實體主要私人金鑰及一產生器值來決定一第一實體第二私人金鑰；

根據至少一第二實體主要私人金鑰及該產生器值來決定一第二實體第二私人金鑰；

根據第一實體第二私人金鑰及第二實體第二公用金鑰來決定在第一實體上的共同私密(CS)，並且根據第二實體第二私人金鑰及第一實體第二公用金鑰來決定在第二實體上的共同私密(CS)； 以及

其中：

第一實體第二公用金鑰及第二實體第二公用金鑰係個別奠基於至少第一/第二實體主要金鑰及產生器值。

【0011】 此外或另可選擇的是，本發明包含控制一數位錢包的存取的方法，該方法包含下列步驟：

根據至少一第一實體主要私人金鑰及一產生器值來決定一第一實體第二私人金鑰；

根據至少一第二實體主要私人金鑰及該產生器值來決定一第二實體第二私人金鑰；

根據第一實體第二私人金鑰及第二實體第二公用金鑰來決定在第一實體上的共同私密(CS)，並且根據第二實體第二私人金鑰及第一實體第二公用

金鑰來決定在第二實體上的共同私密(CS)； 以及

其中：

第一實體第二公用金鑰及第二實體第二公用金鑰係個別奠基於至少第一/第二實體主要金鑰及產生器值。

【0012】 此外或另可選擇的是，該方法可包含下列步驟：

將一確認元件分割成複數個份額(share)；

決定在一個網路上的二個或多個節點上的共同私密；

使用該共同私密自網路的一節點傳送確認元件的至少一份額到至少另一節點。

【0013】 確認元件可為一加密金鑰。其可為一不對稱加密對中的一私人金鑰。此外或另可選擇的是，確認元件可表現為一加密金鑰，或是為可用來存取、計算、產生或取回一加密金鑰的一些事務。其可為能夠使用於確認程序中的一些私密或數值，例如，助記符號(mnemonic)或種子。

【0014】 因此，本發明的一態樣關於將私密，如一私人金鑰，分割成(獨一無二的)多個份額。確認元件可被分割成複數個份額，使得確認元件可以從二個或多個份額中恢復或再生。Shamir秘密共享方案可用來將確認元件分割成多個份額。

【0015】 這些份額可以被分割，使得任何的份額本身是沒有數值的，其意味著份額無法用來達成(原始未分割的)確認元件。分割的實行可導致確認元件僅可在一個預定數量的份額組合時恢復過來。在一實施例中，任何二個份額就已經足夠用來恢復確認元件。

【0016】 本發明的另一態樣關於個別份額的安全處理或儲存。份額可傳送到不同的當事人們，或是由不同的當事人們來將它儲存起來。一些或全部的當事人們可為網路上的節點們。在一實施例中，該方法可包含將確認元件的至少三個份額儲存在彼此互相相關的不同位置上的一步驟。

【0017】 至少一份額可儲存在一個備份或"安全儲存" 設備中。這個設備可與其他儲存份額的地點彼此互相隔開、互相獨立或互相區別。這種方式提供了一個重要的優點，因為這種方式能夠在其他份額的其中之一變成無法取得的條件下，恢復確認元件。在此種情形下，份額可由安全儲存

設備取回。

【0018】 確認程序可在使用份額來恢復確認元件之前實行。確認程序可包含確認一個預先決定的或是指定的個人身分，及/或確認一個計算資源。

【0019】 本發明的另一態樣可包含關於一個或多個份額的安全分布。該方法可包含使用共同私密來產生一個加密金鑰的步驟，其中加密金鑰用來加密確認元件的至少一份額，或包含該至少一份額的信息。

【0020】 共同私密可以在彼此互相獨立的至少二個節點上決定。因此，每個節點可決定或產生自己的私密，而不需要自另一節點或其他當事人輸入或與另一節點或其他當事人通信。這個意味著共同私密可以不需要在一個通信通道上傳遞。因為共同私密無法被未授權的當事人所攔截，這個方式提供了加強的安全性。共同私密對於該至少二個節點而言為共有的(意即，共享的)。共同私密接著可用來產生一個加密金鑰，並且加密金鑰可用來安全傳送份額。其他資料也可以使用加密金鑰來傳送。

【0021】 該方法可包含在一第一節點(C)決定一共同私密(CS)的步驟，該共同私密(CS)在第一節點(C)及一第二節點(S)為共通的，其中第一節點(C)與具有一第一節點主要私人金鑰(V_{1C})及一第一節點主要公用金鑰(P_{1C})的一第一不對稱加密對關連，且第二節點(S)與具有一第二節點主要私人金鑰(V_{1S})及一第二節點主要公用金鑰(P_{1S})的一第二不對稱加密對關連，其中該方法包含：

根據至少第一節點主要私人金鑰(V_{1C})及一產生器值(GV)來決定一第一節點第二私人金鑰(V_{2C})；

根據至少第二節點主要公用金鑰(P_{1S})及該產生器值(GV)來決定一第二節點第二公用金鑰(P_{2S})； 以及

根據第一節點第二私人金鑰(V_{2C})及第二節點第二公用金鑰(P_{2S})來決定共同私密(CS)；

其中第二節點(S)根據一第一節點第二公用金鑰(P_{2C})及一第二節點第二私人金鑰(V_{2S})具有相同的共同私密，其中：第一節點第二公用金鑰(P_{2C})係奠基於第一節點主要公用金鑰(P_{1C})及產生器值(GV)；並且第二節點第二私人金

鑰(V_{2S})係奠基於第二節點主要私人金鑰(V_{1S})及產生器值(GV)。

【0022】 產生器值(GV)可奠基於一信息(M)。該方法可進一步包含：根據信息(M)及第一節點第二私人金鑰(V_{2C})來產生一第一簽名信息(SM1)；以及透過通信網路傳送第一簽名信息(SM1)到第二節點(S)，其中第一簽名信息(SM1)利用第一節點第二公用金鑰(P_{2C})來確認，以認證第一節點(C)。

【0023】 該方法亦包含：透過通信網路自第二節點(S)接收一第二簽名信息(SM2)；利用第二節點第二公用金鑰(P_{2S})來確認第二簽名信息(SM2)；以及根據第二簽名信息(SM2)的確認結果來認證第二節點(S)，其中第二簽名信息(SM2)係根據信息(M)或一第二信息(M2)，及第二節點第二私人金鑰(V_{2S})來產生。

【0024】 該方法更包含：產生一信息(M)；以及透過一通信網路傳送信息(M)到第二節點(S)。可選擇的是，該方法可包含透過通信網路自第二節點(S)接收信息(M)。另外可選擇的是，該方法可包含透過通信網路自另一節點接收信息(M)。又另外可選擇的是，該方法可包含自一資料儲存及/或與第一節點(C)關連的一輸入介面接收信息(M)。

【0025】 第一節點主要公用金鑰(P_{1C})、第二節點主要公用金鑰(P_{1S})可奠基於第一節點主要私人金鑰(V_{1C})及第二節點主要私人金鑰(V_{1S})分別與一產生器(G)的橢圓曲線點乘法。

【0026】 該方法可更包含下列步驟：透過通信網路接收第二節點主要公用金鑰(P_{1S})；以及將第二節點主要公用金鑰(P_{1S})儲存於與第一節點(C)關連的一資料儲存上。

【0027】 該方法可更包含下列步驟：在第一節點(C)上產生第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})；透過通信網路傳送第一節點主要公用金鑰(P_{1C})到第二節點(S)及/或其他節點；以及將第一節點主要私人金鑰(V_{1C})儲存於與第一節點(C)關連的一第一資料儲存上。

【0028】 該方法亦可包含下列步驟：透過通信網路傳送一通知到第二節點，該通知使用代表具有一基準點(G)的一共同橢圓曲線密碼學(ECC)系統於決定共同私密(CS)的方法中。產生第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})的步驟可包含：根據一隨機整數產生第一節點主要私人金

鑰(V_{1C})，該隨機整數位於共同橢圓曲線密碼學系統所指定的一個可允許的範圍內；以及根據第一節點主要私人金鑰(V_{1C})及基準點(G)的橢圓曲線點乘法，按照以下公式來決定第一節點主要公用金鑰(P_{1C})：

$$P_{1C} = V_{1C} \times G$$

【0029】 該方法可進一步包含：取決於信息(M)的一雜湊(hash)來決定產生器值(GV)，其中決定第一節點第二私人金鑰(V_{2C})的步驟，係根據第一節點主要私人金鑰(V_{1C})及產生器值(GV)的純量加法，按照以下公式來求出：

$$V_{2C} = V_{1C} + GV$$

【0030】 決定第二節點第二公用金鑰(P_{2S})的步驟，可根據第二節點主要公用金鑰(P_{1S})以橢圓曲線點加法，加上產生器值(GV)及基準點(G)的橢圓曲線點乘法，按照以下公式來求出：

$$P_{2S} = P_{1S} + GV \times G$$

【0031】 產生器值(GV)可取決於前一個產生器值(GV)的一雜湊來決定。

【0032】 第一不對稱加密對及第二不對稱加密對，可個別奠基於前一個不對稱加密對及前一個第二不對稱加密對的一函數。

【0033】 另一種可選擇的字詞為，本發明可提供一方法，包含下列步驟：

將一確認元件分割成複數個份額；

根據一第一主要不對稱金鑰對，在一第一節點產生一個求得的(或第二)私人加密金鑰；

使用求得的私人金鑰於加密及/或安全傳輸確認元件的至少一部分。

【0034】 該方法亦可包含在一第二節點上產生相同的求得的私人金鑰，這個可以獨立於第一節點且根據於一第二主要不對稱金鑰對的方式來產生。

【0035】 求得的私人金鑰可為由私人金鑰及公用金鑰所組成的一不對稱金鑰對的一部分。第一及/或第二節點可使用橢圓曲線密碼學(ECC)來產生私人金鑰(及其對應的公用金鑰)。

【0036】 該方法可包含下列步驟：

在第一及第二節點之間，對於使用一基準點(G)的標準 ECC 系統達成一致；

在第一及/或第二節點上，使用達成一致的標準 ECC 系統來產生一公用/私人金鑰對並且公開公用金鑰，這個可意味著讓它變得可公開取得；以及/或

在第二節點或另一個位置註冊第一節點的主要公用金鑰(P_{MC})；以及/或在第一節點或另一個位置註冊第二節點的主要公用金鑰(P_{MS})；以及/或

自第一節點傳送信息(M)到第二節點，及/或自第二節點傳送信息(M)到第一節點，並且產生信息的一雜湊；信息可使用求得的金鑰來簽名；這個步驟可代表所需要用以：(1)建立節點間的一共享私密及(2)在節點間起始一個安全的通信的唯一傳輸。第一或第二節點可使用接收的信息(M)來產生自己所求得的(次要的)公用/私人金鑰對。這個可允許節點計算其他節點的求得的公用金鑰；以及/或

接收信息及獨立計算出信息 M 的雜湊(例如，SHA-256(M))；以及/或

計算出一公用金鑰(P_{2C})，求可由主要金鑰(P_{MC})求得；以及/或

針對所計算出的 P_{2C} 來確認簽名(Sig-V_{2C})。

【0037】　求得的私人金鑰可決定性地從第一或第二節點的主要公用金鑰來求得。

【0038】　本發明亦可包含一種電腦完成的系統，其設置且設定為完成上述方法的任何實施例。系統可包含或使用一區塊鏈網路或平台。此外或另可選擇的是，其可包含一數位錢包供應商或管理系統。

【0039】　上述的關於本發明的一個態樣或實施例的任何特點，可被用於關於本發明的任何其他的態樣中。例如，描述於關於方法的特徵可應用於系統，反之亦然。

【0040】　本發明的這些跟其他態樣將參照此間所敘述的實施例來說明及變得明顯易懂。

【0041】　本發明的一實施例現在將藉由參照僅作為範例用的附圖來說明，其中：

【圖式簡單說明】

【0042】

第1圖為用以決定一個第一節點及第二節點的一個共同私密之範例系統的示意圖，根據本發明，其可用於安全地傳輸高敏感度資訊，如一個私人金鑰的一個份額；

第2圖為用來決定一個共同私密之以電腦來完成的方法的流程圖，根據本發明，其可用於安全地傳輸高敏感度資訊，如一個私人金鑰的一個份額；

第3圖為用以註冊第一及第二節點之以電腦來完成的方法的流程圖；

第4圖為用來決定一個共同私密之以電腦來完成的方法的另一個流程圖，根據本發明，其可用於安全地傳輸高敏感度資訊，如一個私人金鑰的一個份額；

第5圖為以電腦來完成的第一節點及第二節點之間的安全通信方法的流程圖。

【實施方式】

【0043】 如上面所解釋者，一直存在有需要加強私密的儲存及/或私密的交換，或是可被用來產生金鑰的私密的需求，私密可為錢包助記符號的一個種子，或是其他與安全性相關的物件。本發明提供了此種方案。下述的一實施例係用於解說之用，並且利用完成於一個區塊鏈中的數位錢包的背景來說明。然而，本發明不限於此種完成方式，且能夠針對任何電腦來完成的網路或系統來完成。

【0044】 如上所言，公用金鑰密碼學的使用經常與數位錢包有關。若是末端使用者(我們在此可稱其為”客戶端”或簡稱為”使用者”)有責任來儲存他們的私人金鑰，當使用者或他們的硬體變得無法取得時，問題可能就此產生，這是因為這會使得私人金鑰，從而錢包的基金，變成無法存取。然而，錢包供應商那一端(我們可稱其為”伺服器端”)的金鑰的儲存，需要對於供應商及他們的安全機制具有一定程度的信任。因此便有將私人金鑰儲存為私人金鑰無法讓未授權的當事人獲得，但是當有需要時可以複製的需求。名詞”使用者”可為一個人類使用者或一種電腦完成的資源。

【0045】 一種已知的密碼演算法，已知為”Shamir 秘密共享方案” (4S)，教導了將私密分割成獨一無二的部分或份額，這些部分或份額接著分配給

不同的當事人。在往後，份額可被用來重建私密。每個個別的份額是沒有數值的或是獨自使用，直到其與一個或多個份額組合。所需用來重建私密的份額的數目會根據情勢的需要來改變。在一些例子中，所有的份額都需要用來重建私密，然而在其他的例子中，只要有足夠數目的份額才需要用來重建私密。這個叫做門檻方案(threshold scheme)，其中份額的任何 k 值就已經足夠來重建原始私密。

【0046】 在這個解說性的例子中，4S 被用來分割一個私密，如私人金鑰或助記符號種子，成數個部分。其亦可被用來自一定數目的部分中重新產生金鑰或助記符號種子。助記符號的使用已知為與數位錢包相聯合。助記符號為一種對人性友善的程式碼或字元的群組，其可轉變成一個二元種子，用於一個錢包或資料的產生。

【0047】 在此間，下列的名詞會被使用：

“私密” (S)為一個秘密(例如，數個數值)，其需要在多個當事人之間安全地分享。

“份額”是私密的一個片段。私密分割成片段，且每個片段稱為一個份額。其為從給定的私密中運算出來。為了恢復私密，吾人必須獲得某些數目的份額。

“門檻” (k)為吾人需要用來重新產生或恢復私密的最小數目的份額。只有在吾人有大於或等於 k 個份額時，才能重新產生私密。

“大質數” (p)為一個隨機質數(random prime)。

【0048】 從一個寬廣的看法看來，解說性的實施例包含如下的方法。在這個例子中，我們使用一個”2-of-3”(意即、 k=2)方案：

使用者向一個錢包供應商註冊，來產生及設定一個與使用者關連的新錢包。在這個例子中，錢包為比特幣錢包，其使用區塊鏈；

產生一個公用-私人金鑰對且與使用者的錢包相關連；

使用 4S 將私人金鑰分割成份額；

私人金鑰的一個份額經由一個安全傳輸傳送到使用者；

私人金鑰的另一個份額為服務供應商所保留且儲存在一個伺服器上；

另一個份額經由一個安全傳輸傳送到一個遠端以安全地儲存著。名詞”

遠端”並未暗示任何特殊的地理距離或位置。取而代之的是，在此間其是用來指份額保留在一個，在某種意義上獨立於錢包供應商或使用者(較佳者為二者)的安全儲存設備或資源中。”獨立”可包括實質地、邏輯地、金融地、政治地，及/或組織地獨立。例如，吾人可以將安全儲存外包給收取費用來提供安全儲存服務的商業實體；或是由使用者的律師來保存，或是一些其他被選上的(且受到信任的)當事人，其接受儲存份額的責任，且若是有需求的話會在收到請求時提供份額。

錢包供應商能夠摧毀任何或所有的完整私人金鑰的副本。這是因為副本不再需要了。當需要私人金鑰來進行後續的使用者授權(例如，因為使用者現在希望進行交易)，會從使用者的份額及錢包供應商的份額來重建金鑰，其中當有需要時使用者的份額會提供給錢包供應商。

【0049】 這種作法的一個優點在於即使錢包供應商的安全有漏洞，未授權的當事人無法獲得使用者的私人金鑰的存取權，這是因為使用者的私人金鑰並未儲存在錢包供應商的系統的任何處，且錢包供應商的系統本身並未包括足夠的份額來讓私人金鑰重建起來。這個優點可同樣應用到客戶端的安全性有漏洞時的情形下。

【0050】 另一個優點為經由儲存份額到一個安全儲存地點，私人金鑰會經由自安全儲存取回，及與錢包供應商的份額組合來重建。因此，若使用者死去或是變成無行為能力，或是若使用者的硬體(並且因此份額)遺失、損壞或是被偷竊，錢包內的基金依然能夠存取。在此種情勢下，使用者的身分可以進行確認。在一些例子中，一個經過證明且受信任的當事人的身分，如一不動產的執行人或律師，可以進行確認。這個可經由，例如，證據的製作來完成，如死亡證明、護照、一份法律文件、或其他形式的身分證明，在確認授權的身分時，私密的份額可由安全儲存中取出。因此，安全儲存作為一種備份設備，其能夠被使用在特別的或預先決定的情形下。

【0051】 因此，本發明提供了加強型的系統/資料安全及便利性的優勢組合。其提供了一種用於存取控制的簡單、有效及安全的解決方案。

【0052】 應注意的是在上面的例子中，私人金鑰經由錢包服務供應商來產生，且個別的部分傳送到使用者及安全儲存資源。然而，在其他實施

例中，這個可能就不會成立。此外，重要的是要注意在當事人(其可稱為"節點")之間的部分的傳輸，必須以安全的方式來實行。這是因為任何對多個份額的未授權攔截，可能會致使攔截者能夠重建私密(例如，經由助記符號或金鑰)。這個安全交換問題亦可由本發明來解決，說明如下。

【0053】 為了解說起見，本發明的更多詳細態樣現在說明。應注意的是 Shamir 秘密共享方案為一項在技藝領域中已知的的技術，且技術熟悉者可了解、明白及使用這項技術。因此，下述者僅提供為完整說明之用。

【0054】 **分割私密成份額**

【0055】 給定一個私密 S，數個參與者 n，一個門檻數字 k，及一些大質數 p，我們以恆定項 S 建立一個多項式：

$y = f(x)$ of degree $k-1$ (modulo our prime p)

【0056】 接下來，我們選擇在 1 及 p-1 之間(包括 1、 p-1)的 n 個獨一無二的隨機整數，並且評估在這些 n 個點上的多項式。N 個關係者每個都賦予了一個(x、 y)對。這個可以經由下列步驟來達成：

【0057】 1. 轉換成整數

對於 4S 演算法而言，私密必須為一個整數。因此，若私密的格式為一些其他的格式(例如，字串、16 進位數等等)，它就必須先換成一個整數。若私密已經為一個整數，這個步驟可以忽略。對於這個例子而言，讓 $S = 1234$ 。

【0058】 2. 決定份額(n)及門檻(k)的數目

要注意 k 個部分為需要用來重新產生私密。因此，選擇 S 及 k 使得在當恢復私密時，k 個部分永遠可以獲得。對這個例子而言，讓 $n=6$、 $k=3$。

【0059】 3. 創造多項式：

【0060】 我們需要創造一個多項式，其形式為： $y = f(x) \bmod p$

i. 決定恆定項及多項式的次數

$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{k-1}x^{k-1}$

恆定項 $a_0 = S$

多項式的次數= $k-1$

因此對於 $k=3$ 及 $S=1234$、 我們需要建立一個次數為 2 且 $a_0 = 1234$ 的

多項式。

$f(x) = 1234 + a_1x + a_2x^2$

ii. 決定係數

選擇 k-1 個隨機數字(使用一個隨機(或偽隨機)數字產生器)，使得：

$0 < a_n < S$

讓 $a_1 = 166$； $a_2 = 94$

因此，$f(x) = 1234 + 166x + 94\ x^2$

iii. 選擇一個隨機質數，使得：

$p > max(S、n)$

讓 $p = 1613$

iv. 最後的多項式為

$y = f(x) \bmod p$

$y = (1234 + 166x + 94\ x^2) \bmod 1613$

【0061】 **創造份額**

【0062】 為了將私密分成n個份額，我們需要使用下列多項式來建立n個點(份額)：

$y = (1234 + 166x + 94\ x^2) \bmod 1613$

對這個例子而言，$n = 6$，我們會有六個點。注意我們以$x = 1$及 $NOT\ x = 0$ 開始。

對於$x = 1\ to\ 6$，六個點列出如下：

$(1、\ 1494)、\ (2、329)、\ (3、965)、\ (4、176)、\ (5、\ 1188)、\ (6、775)$

在這n (6)個點中，任何k (3)個點可被用來重新產生私密金鑰。

【0063】 從一個給定數目的份額中重建私密

i. 獲得私密整數

為了重建私密，我們需要下面資訊：

$n = 6、\ k = 3、\ p = 1613、$

k個份額：$(x0、\ y0) = (1、\ 1494)；\ (x1、\ y1) = (2、329)；\ (x2、\ y2) = (3、965)$

一旦我們有了上面資訊，我們可以使用一項技術如拉格朗日插值法，其

為技藝領域中已知者且可為熟悉技藝者迅速理解。使用這項技術，我們可以重建整個多項式。按照以下公式來計算係數：

$a_i(x)=[\Sigma^{k-1}_{i=0} y_i \prod_{0<=j<=k-1、j\neq i}(x-x_j)/(x_i - x_j)] \bmod p$

但是由於$S=a_0$，我們只需要找出$a_0=a_0(0)$

$$a_0 = \left[\sum_{i=0}^{k-1} y_i \prod_{j=0, j\neq i}^{k-1} \frac{x_j}{x_i - x_j} \right] \bmod p$$

其中$x_i - x_j \neq 0$。

熟悉技術者將會了解到在上述的公式中，指數-1表示進行乘法逆。大部分的程式語言包含內建包來實行數學運算，如乘法逆。

ii. 轉換整數成想要的格式

若實行步驟1來將一個特定的格式轉換成整數，我們遵行反向的操作來轉換整數回到所想要的格式。

【0064】 **份額的安全傳輸**

【0065】 如之前所提到者，將私密的份額以安全的方式傳送到個別的收件人，以避免未授權的當事人能夠重建私密，是重要的。在一較佳實施例中，安全傳輸可以如下說明的方式達成。

【0066】 一個共同私密(CS)建立於二個當事人之間，且接著使用共同私密(CS)來產生一個安全加密金鑰來傳輸一個或多個份額。這個共同私密(CS)不要與上面提到的私密(S)互相混淆。共同私密(CS)產生以用來致能私密(S)，例如金鑰或其份額的安全交換。

【0067】 二邊當事人可為任二個錢包服務供應商、使用者、安全儲存資源或一些其他的合法當事人。此後，為了方便說明之故，他們稱作一第一節點(C)及一第二節點(S)。目的是產生一個共同私密(CS)，其為二個節點所知卻不會讓共同私密經由一通信通道來傳送，藉此消除了共同私密被未授權地發現的可能性。私密的分割及安全儲存技術，結合了如下所述的安全傳輸技術後，提供了一種金鑰管理解決方案。

【0068】 本發明的安全傳輸技術牽涉到共同私密(CS)以獨立的方式產生於傳輸的每一端，使得當二個節點都知道CS時，CS不需要透過潛在不

安全的通信通道來移動。一旦CS在二端都建立時，其可被用來產生二個節點都可以使用來進行之後的傳輸的一安全加密金鑰。在錢包註冊的過程中，這個對於分割的私人金鑰從一方傳送到另一方的傳輸而言，是有特別的助益地。

【0069】 第1圖顯示了系統1，包含一第一節點3，其透過一通信網路5與一第二節點7通信。第一節點3具有相關的一第一處理裝置23，且第二節點7具有相關的一第二處理裝置27。第一及第二節點3、7可包含一電子裝置，如一電腦、電話、平板電腦、行動通信裝置、電腦伺服器等等。在一例子中，第一節點3可為一客戶端(使用者)裝置，而第二節點7可為一伺服器。伺服器可為一數位錢包供應商的伺服器。

【0070】 第一節點3與具有一第一節點主要私人金鑰(V_{1C})及一第一節點主要公用金鑰(P_{1C})的一第一不對稱加密對相關連。第二節點(7)與具有一第二節點主要私人金鑰(V_{1S})及一第二節點主要公用金鑰(P_{1S})的一第二不對稱加密對相關連。換句話說，第一及第二節點每個都個別持有公用-私人金鑰對。

【0071】 第一及第二節點3、7個別的第一及第二不對稱加密對可在註冊過程中產生，如註冊錢包的過程。每個節點的公用金鑰可公開共享，例如透過通信網路5。

【0072】 為了在第一節點3及第二節點7二者上決定共同私密(CS)，節點3、7個別實行方法300、400的步驟，而不需透過通信網路5互相溝通其私人金鑰。

【0073】 第一節點3所實行的方法300包含步驟330，以根據至少第一節點主要私人金鑰(V_{1C})及一產生器值(GV)來決定一第一節點第二私人金鑰(V_{2C})。產生器值可奠基於在第一及第二節點之間分享的一信息(M)，其中第一及第二節點之間的分享可包含透過通信網路5來分享信息，如以下進一步詳述者。方法300亦包含步驟370，以根據至少第二節點主要公用金鑰(P_{1S})及產生器值(GV)來決定一第二節點第二公用金鑰(P_{2S})。方法300亦包含步驟380，以根據第一節點第二私人金鑰(V_{2C})及第二節點第二公用金鑰(P_{2S})來決定共同私密(CS)。

【0074】 重要的是，相同的共同私密(CS)亦可在第二節點7上經由方法400決定出。方法400包含步驟430，以根據第一節點主要公用金鑰(P_{1C})及產生器值(GV)來決定一第一節點第二公用金鑰(P_{2C})。方法400更包含步驟470，以根據第二節點主要私人金鑰(V_{1S})及產生器值(GV)來決定一第二節點第二私人金鑰(V_{2S})。方法400包含步驟480，以根據第二節點第二私人金鑰(V_{2S})及第一節點第二公用金鑰(P_{2C})來決定共同私密(CS)。

【0075】 通信網路5可為一區域網路、一廣域網路、手機網路、無線電通信網路、網際網路等等。這些網路中的資料，可經由通信媒介如電線、光纖或無線來傳送，而容易遭到竊聽，如被一竊聽者11竊聽。方法300、400可允許第一節點3及第二節點7二者獨立決定一共同私密，而不需要將共同私密透過通信網路5傳送。

【0076】 如此的一優點在於共同私密(CS)可由每個節點安全且獨立地決定，而不需要將一個私人金鑰透過一個潛在不安全的通信網路5來傳送。反之，共同私密可當作一私密金鑰(或是做為一私密金鑰的基礎)，透過通信網路5用於第一及第二節點3、7之間的加密通信。

【0077】 方法300、400可包含額外的步驟。方法300可包含在第一節點3上，根據信息(M)及第一節點第二私人金鑰(V_{2C})來產生一簽名信息(SM1)。方法300更包含步驟360，將第一簽名信息(SM1)透過通信網路5，傳送到第二節點7。反之，第二節點7可實行步驟440，以接收第一簽名信息(SM1)。方法400亦包含步驟450，以利用第一節點第二公用金鑰(P_{2C})來確認第一簽名信息(SM1)，以及步驟460，以根據第一簽名信息(SM1)的確認結果來認證第一節點3。有利的是，這個允許了第二節點7來認證有意圖的第一節點(第一簽名信息產生之處)為第一節點3。這是根據只有第一節點3具有第一節點主要私人金鑰(V_{1C})的存取權的假設而定，並且因此只有第一節點3能夠決定用來產生第一簽名信息(SM1)的第一節點第二私人金鑰(V_{2C})。應理解的是，相似地，一第二簽名信息(SM2)可產生於第二節點7且傳送到第一節點3，使得第一節點3能夠認證第二節點7，如以點對點的情形來認證。

【0078】 在第一及第二節點之間，信息(M)的分享可以用各種的方式來達成。在一例子中，信息可在第一節點3上產生，接著透過通信網路5傳

送到第二節點7。在又一個例子中，信息可在一第三節點9上產生，且信息傳送到第一及第二節點3、7。在又一個可選擇的例子中，使用者可經由一使用者介面15輸入信息而由第一及第二節點3、7接收。在又一個例子中，信息(M)可自一資料儲存19取回且傳送到第一及第二節點3、7。在一些例子中，信息(M)可為公開的且因此可透過一個不安全的網路5傳送。

【0079】 進一步的例子為，一個或多個信息(M)可儲存在一資料儲存13、17、19中，其中信息可與一些實體，如數位錢包或建立於第一節點3及第二節點7之間的一通信對談關連。因此，信息(M)可被取回，且被用來在第一及第二節點3、7上個別重新創造出與該錢包或對談關連的共同私密(CS)。

【0080】 有利的是，用來讓共同私密(CS)重新創造出來的記錄可被保存起來，而不需要記錄本身被私自儲存起來或安全地傳送出去。若數個交易實行於第一及第二節點3、7上，這個方式是可有利的，並且將所有的信息(M)儲存在節點自己本身上是不切實際的。

【0081】 註冊方法100、 200

【0082】 註冊方法100、 200的一個例子，將參照第3圖來說明，其中方法100由第一節點3來實行，而方法200由第二節點7來實行。這個包含了為第一及第二節點3、7建立第一及第二不對稱加密對。

【0083】 不對稱加密對包含關連的私人及公用金鑰，如使用於公開金鑰加密中所使用的金鑰。在這個例子中，不對稱加密對係使用橢圓曲線密碼學(ECC)及橢圓曲線操作的特性來產生。

【0084】 ECC的標準包含已知的標準，如Standards for Efficient Cryptography Group (www.sceg.org)中所描述的標準。橢圓曲線密碼學亦說明於美國專利US 5,600,725、US 5,761,305、US 5889,865、US 5,896,455、US 5,933,504、US 6,122,736、US6,141,420、US 6,618,483、US 6,704,870、US 6,785,813、US 6,078,667、US 6,792,530中。

【0085】 在方法100、200中，這個包括了步驟110、210，其中第一及第二節點在一個共同ECC系統上達成協議且使用一個基準點(G)。(注意，基準點可稱為一共同產生器，但是使用名詞”基準點"避免與產生器值GV相混

淆)。在一個例子中，共同ECC系統可奠基於secp256K1，其為比特幣所使用的一個ECC系統。基準點(G)可以被選出來、被隨機產生出來，或是被指定。

【0086】 現在注意力轉向第一節點3，方法100包含步驟110，來安置在共同ECC系統及基準點(G)上。這個包含了自第二節點7或一第三節點9接收共同ECC系統及基準點。可選擇的是，一個使用者介面15可與第一節點3關連，藉此一使用者可選擇性地提供共同ECC系統及/或基準點(G)。又一可選擇的是，共同ECC系統及/或基準點(G)的其中之一或二者，可隨機地由第一節點3來選擇。第一節點3可透過通信網路5，傳送代表使用具有一個基準點(G)的共同ECC系統的通知到第二節點7。依序地，在步驟210中，第二節點7可經由發送代表確認使用共同ECC系統及基準點(G)的通知來安置。

【0087】 方法100包含步驟120，由第一節點3產生包含第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})的一第一不對稱加密對。這個包含了根據至少一部份的一隨機整數來產生第一節點主要私人金鑰(V_{1C})，其中隨機整數位於由共同ECC系統所指定的一個可允許的範圍內。這個也包含了根據第一節點主要私人金鑰(V_{1C})及基準點(G)的橢圓曲線點乘法，按照以下公式來決定第一節點主要公用金鑰(P_{1C})：

$$P_{1C} = V_{1C} \times G \qquad \text{(公式1)}$$

【0088】 因此，第一不對稱加密對包含：

V_{1C}： 由第一節點來保持私密的第一節點主要私人金鑰

P_{1C}： 變成公開已知的第一節點主要公用金鑰。

【0089】 第一節點3可將第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})儲存在與第一節點3相關連的一第一資料儲存13中。為了安全起見，第一節點主要私人金鑰(V_{1C})可儲存在第一資料儲存13的一安全部分，來確保金鑰保持私密。

【0090】 該方法更包含步驟130，以透過通信網路5將第一節點主要公用金鑰(P_{1C})傳送到第二節點7。在步驟220中，在收到第一節點主要公用金鑰(P_{1C})時，第二節點7可將第一節點主要公用金鑰(P_{1C})儲存在與第二節點7相關連的一第二資料儲存17中。

【0091】 類似於第一節點3，方法200包含步驟240，以產生包含第二

節點主要私人金鑰(V_{1S})及第二節點主要公用金鑰(P_{1S})的一第二不對稱加密對。第二節點主要私人金鑰(V_{1S})亦為在可允許範圍內的一個隨機整數。依序地，第二節點主要公用金鑰(P_{1S})係由下列公式來決定：

$$P_{1S} = V_{1S} \times G \qquad \text{(公式2)}$$

【0092】 因此，第二不對稱加密對包含：

V_{1S}： 由第二節點來保持私密的第二節點主要私人金鑰。

P_{1S}： 變成公開已知的第二節點主要公用金鑰。

【0093】 第二節點7可將第二不對稱加密對儲存在第二資料儲存17中。方法200更包含步驟250，以將第二節點主要公用金鑰(P_{1S})傳送到第一節點3。依序地，在步驟140第一節點3可接收第二節點主要公用金鑰(P_{1S})，且在步驟150第一節點3可儲存第二節點主要公用金鑰(P_{1S})。

【0094】 應理解的是在一些可選擇的替代方案中，個別的公用主要金鑰可被接收及儲存在與第三節點9(如一個受信任的第三當事人)相關連的一第三資料儲存19中。這個可包含作用為一個公開目錄的一第三當事人，如數位憑證認證機構。因此在一些例子中，只有在當需要決定共同私密(CS)時，可請求第一節點主要公用金鑰(P_{1C})且由第二節點7接收第一節點主要公用金鑰(P_{1C}) (且反之亦然)。

【0095】 註冊步驟可以只需要發生一次，做為例如數位錢包的一個起始設定。

【0096】 對談起始及由第一節點3來決定共同私密

【0097】 決定共同私密(CS)的一個例子現在將參照第4圖來說明。共同私密(CS)可被用於在第一節點3及第二節點7之間的一個特殊的對談、時間、交易或其他用途中，並且使用相同的共同私密(CS)是令人不想要的或是不安全的。因此共同私密(CS)在不同的對談、時間、交易等等之間是可改變的。

【0098】 下面提供了上述的安全傳輸技術的解說。

【0099】 *步驟310： 產生一信息(M)*

【0100】 在這個例子中，由第一節點3來實行的方法300包含步驟310，以產生一信息(M)。信息(M)可為隨機、偽隨機或使用者定義的。在一個例子中，信息(M)奠基於Unix時間及一個任意值 (nonce)。例如，可提供信息(M)

為：

Message (M) = UnixTime + nonce (公式3)

【0101】 在一些例子中，信息(M)為任意值。然而，應理解的是信息(M)可具有選擇性的值(如Unix時間等等)，其在一些應用中為有用者。

【0102】 方法300包含步驟315，以透過通信網路5傳送信息(M)到第二節點7。當信息(M)並未包含在私人金鑰內的資訊時，信息(M)可透過一個不安全的網路來傳送。

【0103】 *步驟320： 決定一產生器值(GV)*

【0104】 方法300更包含步驟320，以根據信息(M)來決定一產生器值(GV)。在這個例子中，這個包括了決定信息的一加密雜湊。加密雜湊演算法的一個例子包括SHA-256，以創造出一個256位元的產生器值(GV)。也就是說：

GV = SHA-256(M) (公式4)

【0105】 應理解的是可使用其他的演算法。這個包括了其他的演算法包含了在安全雜湊演算法(Secure Hash Algorithm 、SHA)的家族中的演算法。一些特殊的例子包括了SHA-3子集合中的例子，包含SHA3-224、SHA3-256、SHA3-384、SHA3-512、SHAKE128、SHAKE256。其他的雜湊演算法可包含RIPEMD (RACE Integrity Primitives Evaluation Message Digest)家族中的演算法。一個特殊的例子可包含RIPEMD-160。其他的雜湊函數可包含基於Zémor-Tillich雜湊函數的家族成員及以背包為基礎的(knapsack-based)的雜湊函數。

【0106】 *步驟330： 決定一第一節點第二私人金鑰*

【0107】 方法300包含步驟330，以根據第一節點主要私人金鑰(V_{1C})及產生器值(GV)決定第一節點第二私人金鑰(V_{2C})。這個可以根據第一節點主要私人金鑰(V_{1C})及產生器值(GV)的純量家法，按照以下公式求出：

$V_{2C} = V_{1C} + GV$ (公式5)

【0108】 因此，第一節點第二私人金鑰(V_{2C})並未為一隨機數值，而是由第一節點主要私人金鑰中以決定性的方法求出。加密對中對應的公用金鑰，意即第一節點第二公用金鑰(P_{2C})，具有下列的關係：

$P_{2C} = V_{2C} \times G$ (公式6)

【0109】 將公式5的V_{2C}置換到公式6，提供了：

$P_{2C} = (V_{1C} + GV) \times G$ (公式7)

【0110】 其中運算子'+'稱為橢圓曲線點加法。注意橢圓曲線密碼學代數是有分布性的，公式7可表達為：

$P_{2C} = V_{1C} \times G + GV \times G$ (公式8)

【0111】 最後，公式1可被置換到公式7來提供：

$P_{2C} = P_{1C} + GV \times G$ (公式9.1)

$P_{2C} = P_{1C} + SHA\text{-}256(M) \times G$ (公式9.2)

【0112】 因此，對應的第一節點第二公用金鑰(P_{2C})可由第一節點主要公用金鑰(P_{1C})及信息(M)的給定知識來求得。第二節點7可擁有此種知識來獨立地決定第一節點第二公用金鑰(P_{2C})，如將在以下參照方法400來進一步的詳細說明者。

【0113】 *步驟350：根據信息及第一節點第二私人金鑰來產生一第一簽名信息(SM1)*

【0114】 方法300進一步包含步驟350，以根據信息(M)及所決定的第一節點第二私人金鑰(V_{2C})來產生一第一簽名信息(SM1)。產生一簽名信息包含應用一數位簽名演算法來數位簽署信息(M)。在一個例子中，這個包含了應用第一節點第二私人金鑰(V_{2C})到信息中，以橢圓曲線數位簽名演算法(ECDSA)來獲得第一簽名信息(SM1)。

【0115】 ECDSA的例子包含基於具有secp256k1、secp256r1、secp384r1、se3cp521r1的ECC系統的那些演算法。

【0116】 第一簽名信息(SM1)能夠利用在第二節點7上之對應的第一節點第二公用金鑰(P_{2C})來確認。第一簽名信息(SM1)的這項確認可被第二節點7用來認證第一節點3，其將在以下的方法400的說明中討論。

【0117】 *步驟370'： 決定一第二節點第二公用金鑰*

【0118】 在步驟370中，第一節點3可接著決定一第二節點第二公用金鑰(P_{2S})。如上所討論者，第二節點第二公用金鑰(P_{2S})可基於至少第二節點主要公用金鑰(P_{1S})及產生器值(GV)。在這個例子中，由於在步驟370'中，公用

金鑰係為私人金鑰與基準點(G)的橢圓曲線點乘法來決定，第二節點第二公用金鑰(P_{2S})可以類似公式6的方式來表達為：

$$P_{2S} = V_{2S} \times G \quad \text{(公式10.1)}$$

$$P_{2S} = P_{1S} + GV \times G \quad \text{(公式10.2)}$$

【0119】 公式10.2的數學證明，與上述用來求得第一節點第二公用金鑰(P_{2C})的公式9.1者相同。應理解的是在步驟370中，第一節點3能夠獨立於第二節點7來決定第二節點第二公用金鑰。

【0120】 *步驟380： 在第一節點3決定共同私密*

【0121】 在步驟380中，第一節點3接著可根據所決定的第一節點第二私人金鑰(V_{2C})及所決定的第二節點第二公用金鑰(P_{2S})，來決定共同私密(CS)。第一節點3可經由下列公式來決定共同私密(CS)：

$$S = V_{2C} \times P_{2S} \quad \text{(公式11)}$$

【0122】 在第二節點7實行的方法400

【0123】 在第二節點7實行的對應方法400現在將要說明。應理解的是這些步驟中的一些步驟，類似於上面所討論之由第一節點3所實行的步驟。

【0124】 方法400包含步驟410，以透過通信網路5自第一節點3接收信息(M)。這個包含了在步驟315中由第一節點3所發送的信息(M)。接著在步驟420中，第二節點7根據信息(M)來決定一產生器值(GV)。步驟420之由第二節點7決定產生器值(GV)，類似於上述之由第一節點來實行的步驟320。在這個例子中，第二節點7獨立於第一節點3來實行這個決定性步驟420。

【0125】 下個步驟包含步驟430，以根據第一節點主要公用金鑰(P_{1C})及產生器值(GV)來決定一第一節點第二公用金鑰(P_{2C})。在這個例子中，由於在步驟430'中公用金鑰係為私人金鑰與基準點(G)的橢圓曲線點乘法來決定，第一節點第二公用金鑰(P_{2C})可以類似公式9的方式來表達為：

$$P_{2C} = V_{2C} \times G \quad \text{(公式12.1)}$$

$$P_{2C} = P_{1C} + GV \times G \quad \text{(公式12.2)}$$

【0126】 公式12.1及12.2的數學證明與上面所討論的公式10.1及10.2者相同。

【0127】 *第二節點7認證第一節點3*

【0128】 方法400包含由第二節點7所實行的步驟，以認證所稱的第一節點3為第一節點3。如前所討論者，這個包含了步驟440，以自第一節點3接收第一簽名信息(SM1)。接著在步驟450中，第二節點7可利用在步驟430所決定的第一節點第二公用金鑰(P_{2C})，來確認第一簽名信息(SM1)中的簽名。

【0129】 數位簽名的確認可根據如上所討論的橢圓曲線數位簽名演算法(ECDSA)來完成。重要的是，與第一節點第二私人金鑰(V_{2C})一同簽名的第一簽名信息(SM1)應該只能夠利用第一節點第二公用金鑰(P_{2C})來正確確認。這是因為V_{2C}跟P_{2C}形成一加密對。由於這些金鑰對於在第一節點3上註冊時產生的第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})而言，是有決定性的，第一簽名信息(SM1)的確認可被用來當作認證在註冊過程中傳送第一簽名信息(SM1)的號稱第一節點為相同的第一節點3的基礎。因此，第二節點7可進一步實行，根據第一簽名信息的確認結果(步驟450)來認證第一節點3(步驟460)。

【0130】 上述的認證方法是適合時，在二個節點的其中之一為受信任的節點，且只有一個節點需要認證的情形下。例如，第一節點3可為一客戶端且第二節點7可為受到客戶端信任的一伺服器，如一錢包供應商。因此，伺服器(第二節點7)可能必須要去認證客戶端的資格，以便允許客戶端存取伺服器系統。要伺服器認證伺服器的資格給客戶端，可能是不必要的。然而，在一些情形下，讓二個節點彼此互相認證是令人想要的方式，如以點對點的方案來完成。

【0131】 *第二節點7決定共同私密*

【0132】 方法400可進一步包含步驟470，由第二節點7以根據第二節點主要私人金鑰(V_{1S})及產生器值(GV)來決定第二節點第二私人金鑰(V_{2S})。類似於第一節點3所實行的步驟330，第二節點第二私人金鑰(V_{2S})會根據第二節點主要私人金鑰(V_{1S})及產生器值(GV)的純量加法，按照以下公式來求出：

$$V_{2S} = V_{1S} + GV \quad \text{(公式13.1)}$$

$$V_{2S} = V_{1S} + \text{SHA-256}(M) \quad \text{(公式13.2)}$$

【0133】 接著，在步驟480中，第二節點7根據第二節點第二私人金鑰

(V_{2S})及第一節點第二公用金鑰(P_{2C})，以獨立於第一節點3的方式，按照以下公式決定共同私密(CS)：

$$S = V_{2S} \times P_{2C} \quad \text{(公式14)}$$

【0134】 *共同私密(CS)由第一節點3及第二節點7來決定的證明*

【0135】 由第一節點3所決定的共同私密(CS)與在第二節點7上決定的共同私密(CS)是相同的。公式11及公式14提供了相同的共同私密(CS)的數學證明，現在將進行說明。

【0136】 注意力轉移到由第一節點3所決定的共同私密(CS)，公式10.1可置換到公式11，如下所示：

$$S = V_{2C} \times P_{2S} \quad \text{(公式11)}$$

$$S = V_{2C} \times (V_{2S} \times G)$$

$$S = (V_{2C} \times V_{2S}) \times G \quad \text{(公式15)}$$

【0137】 注意力轉移到由第二節點7所決定的共同私密(CS)，公式12.1可置換到公式14，如下所示：

$$S = V_{2S} \times P_{2C} \quad \text{(公式14)}$$

$$S = V_{2S} \times (V_{2C} \times G)$$

$$S = (V_{2S} \times V_{2C}) \times G \quad \text{(公式16)}$$

【0138】 由於ECC代數具有可交換性，公式15及16為相等的，因此：

$$S = (V_{2C} \times V_{2S}) \times G = (V_{2S} \times V_{2C}) \times G \quad \text{(公式17)}$$

【0139】 *共同私密(CS)及私密金鑰*

【0140】 現在共同私密(CS)可當做一個私密金鑰來使用，或是作為用於第一節點3及第二節點7之間的安全通信的一對稱金鑰演算法中的一個私密金鑰的基礎。這樣的通信方式可用來傳達一個私人金鑰的一部分、一個私人金鑰的表現或辨識物，或是一個私人金鑰的助記符號。因此，一旦本發明已經在例如數位錢包或其他受控制的資源設立過程中被使用到，接下來可實行當事人之間的通信。

【0141】 共同私密(CS)的形式可為橢圓曲線點(x_S、y_S)。這個可轉換成使用節點3、7之間所同意的標準公開已知的運算的一個標準金鑰格式。例如，x_S可為一個256位元的整數，其可使用為用於AES_{256}加密演算法的一個金

鑰。x_S也可以使用RIPEMD160演算法來轉換成一個160位元的整數，以使用於任何需要這樣冗長的金鑰的應用中。

【0142】 共同私密(CS)可按照需求來決定。重要的是，第一節點3不需要儲存共同私密(CS)，這是因為這個能夠根據信息(M)來重新決定。在一些例子中，所使用的信息(M)可儲存在資料儲存13、17、19(或是其他的資料儲存)，而不需要如主要私人金鑰所要求的一般的相同安全等級。在一些例子中，信息(M)可為可公開取得的。然而，取決於一些應用，假定共同私密(CS)如同第一節點主要私人金鑰(V_{1C})一般的安全地保存起來，共同私密(CS)可以儲存在與第一節點相關連的第一資料儲存(X)中。

【0143】 應該注意的是上面提及的實施例是在解說本發明，而非限制本發明，且熟悉本技藝的人士將能夠設計出許多替代的實施例，而不離如附請求項所定義的本發明的範圍。在請求項中，任何放在括號內的參考符號不應當解釋為用來限制請求項。文字” 包括”及” 包含”及其相似字並未排除列出在請求項或說明書整體之外的元件或步驟的存在。在本說明書中，”包括及“包含”“意指” “包括或由.....組成。一個元件的單數稱謂並未排除此種元件的複數稱謂，反之亦然。本發明可藉由包括數個獨特元件的硬體，以及藉由一個適當程式化的電腦來完成。在列舉出數個裝置的裝置請求項中，這些裝置中的數個可由一個硬體及相同項目的硬體來實現。在彼此不相同的附屬請求項中列述某些尺寸的單純事實，並未代表這些尺寸的組合無法被用來產生優點。

【符號說明】

【0144】

1： 系統

3： 第一節點

23： 第一處理裝置

13、17、19： 資料儲存

27： 第二處理裝置

5： 網路

7： 第二節點

9： 第三節點

11： 竊聽者

15： 使用者介面

P_{1C}： 第一節點主要公用金鑰

P_{1S}： 第二節點主要公用金鑰

V_{1C}： 第一節點主要私人金鑰

V_{1S}：第二節點主要私人金鑰

M： 信息

【發明申請專利範圍】

【第1項】 一種以電腦完成控制一資源存取的方法，該方法包含下列步驟：

將一確認元件分割成複數個份額；

決定一網路中二個或更多節點上的一共同私密；以及

使用該共同私密在該二個或更多節點之間傳送該確認元件的至少一份額。

【第2項】 如請求項1所述之方法，其中該確認元件為一加密金鑰、一加密金鑰的表現，或是可用來存取、計算或取回該加密金鑰的一些元件。

【第3項】 如請求項1或2所述之方法，更包含使用共同私密來產生一加密金鑰的步驟，其中該加密金鑰係用來加密該確認元件的該至少一份額，或加密包含或相關於該至少一份額的一信息。

【第4項】 如前述請求項之任一項所述之方法，更包含下列步驟：

儲存該確認元件的至少三個份額於彼此互相相關的不同位置上；

其中該三個份額的至少其中之一係儲存於一個備用或安全儲存的設備中，該設備係與至少二個其他的位置為分離、互相獨立或彼此不同的。

【第5項】 如前述請求項之任一項所述之方法，其中該資源係為一數位錢包，或其他與一些貨幣形式相關的資源。

【第6項】 如前述請求項之任一項所述之方法，其中該確認元件分割成複數個份額，使得確認元件可由二個或多個份額來恢復或重新產生；其中該確認元件使用Shamir秘密共享方案來分割成複數個份額。

【第7項】 如前述請求項之任一項所述之方法，其中該共同私密為：

i) 在該至少二個彼此互相獨立的節點上決定，使得該共同私密不需要透過一通信通道在節點之間傳輸；以及/或者

ii) 僅在該至少二節點之間分享。

【第8項】 如前述請求項之任一項所述之方法，包含設立、創造或註冊一數位錢包的步驟，其中該確認元件與該數位錢包相關連。

【第9項】 如前述請求項之任一項所述之方法，其中該共同私密係由網路中的一第一節點(C)及一第二節點(S)來決定，其中該第一節點(C)與具有一第一節點主要私人金鑰(V_{1C})及一第一節點主要公用金鑰(P_{1C})的一第一不對

稱加密對相關連，而該第二節點(S)與具有一第二節點主要私人金鑰(V_{1S})及一第二節點主要公用金鑰(P_{1S})的一第二不對稱加密對相關連；其中該方法更包含下列步驟：

根據至少該第一節點主要私人金鑰(V_{1C})及一產生器值(GV)來決定一第一節點第二私人金鑰(V_{2C})；

根據至少該第二節點主要公用金鑰(P_{1S})及該產生器值(GV)來決定一第二節點第二公用金鑰(P_{2S})；以及

根據該第一節點第二私人金鑰(V_{2C})及該第二節點第二公用金鑰(P_{2S})決定該共同私密；

其中根據一第一節點第二公用金鑰(P_{2C})及一第二節點第二私人金鑰(V_{2S})，該第二節點(S)具有相同的共同私密，其中：

該第一節點第二公用金鑰(P_{2C})係根據於至少該第一節點主要公用金鑰(P_{1C})及該產生器值(GV)；以及

該第二節點第二私人金鑰(V_{2S})係根據於至少該第二節點主要私人金鑰(V_{1S})及該產生器值(GV)。

【第10項】 如請求項9所述之方法，其中該產生器值(GV)係根據於一信息(M)。

【第11項】 如請求項10所述之方法，更包含下列步驟：

根據該信息(M)及該第一節點第二私人金鑰(V_{2C})來產生一第一簽名信息(SM1)；以及

透過該通信網路傳送該第一簽名信息(SM1)到該第二節點(S)；

其中該第一簽名信息(SM1)係利用一第一節點第二公用金鑰(P_{2C})來確認，以認證該第一節點(C)。

【第12項】 如請求項10或11所述之方法，更包含下列步驟：

透過該通信網路，自該第二節點(S)接收一第二簽名信息(SM2)；

利用該第二節點第二公用金鑰(P_{2S})來確認該第二簽名信息(SM2)；以及

根據該第二簽名信息(SM2)的確認結果來認證該第二節點(S)；

其中該第二簽名信息(SM2)係根據該信息(M)或一第二信息(M2)，及該第二節點第二私人金鑰(V_{2S})來產生。

【第13項】 如請求項9至12之任一項所述之方法，更包含下列步驟：

產生一信息(M)；以及

透過一通信網路傳送該信息(M)到該第二節點(S)。

【第14項】 如請求項10至13之任一項所述之方法，更包含下列步驟：

透過該通信網路自該第二節點(S)接收該信息(M)。

【第15項】 如請求項10至14之任一項所述之方法，更包含下列步驟：

透過該通信網路自另一節點接收該信息(M)。

【第16項】 如請求項9至15之任一項所述之方法，其中該第一節點主要公用金鑰(P_{1C})、該第二節點主要公用金鑰(P_{1S})，係個別根據該第一節點主要私人金鑰(V_{1C})及該第二節點主要私人金鑰(V_{1S})分別與一基準點(G)的橢圓曲線點乘法。

【第17項】 如請求項9至16之任一項所述之方法，更包含下列步驟：

透過該通信網路接收該第二節點主要公用金鑰(P_{1S})；以及

將該第二節點主要公用金鑰(P_{1S})儲存於與該第一節點(C)相關連的一資料儲存中。

【第18項】 如請求項9至17之任一項所述之方法，更包含下列步驟：

在一第一節點(C)產生第一節點主要私人金鑰(V_{1C})及第一節點主要公用金鑰(P_{1C})；

透過該通信網路傳送第一節點主要公用金鑰(P_{1C})到第二節點(S)及/或其他節點；以及

儲存第一節點主要私人金鑰(V_{1C})於與該第一節點(C)相關連的一第一資料儲存。

【第19項】 如請求項9至18之任一項所述之方法，其中該產生器值(GV)係根據前一個產生器值(GV)的一雜湊來決定。

【第20項】 如請求項9至19之任一項所述之方法，其中該第一不對稱加密對及該第二不對稱加密對，係分別根據前一個第一不對稱加密對及前一個不對稱加密對的一函數。

【第21項】 一種以電腦為基礎的系統，設置為實行前述請求項的任一項的步驟。

【第22項】 如請求項第21項所述之系統，其中：該資源為一數位錢包或與一些形式的貨幣相關的其他資源。

【第23項】 如請求項20至22所述之系統，其中該系統包含軟體，其設置為致能一數位錢包的設立、創造或註冊，其中該確認元件係與該數位錢包相關連。

【第24項】 一種以電腦來完成的系統，設置為控制一數位錢包的存取，該系統的操作是用來：

根據至少一第一實體主要私人金鑰及一產生器值來決定一第一實體第二私人金鑰；

根據至少一第二實體主要私人金鑰及該產生器值來決定一第二實體第二私人金鑰；

根據該第一實體第二私人金鑰及一第二實體第二公用金鑰來決定該第一實體上的一共同私密(CS)，及根據該第二實體第二私人金鑰及一第一實體第二公用金鑰來決定該第二實體上的共同私密(CS)；以及

其中：

該第一實體第二公用金鑰及該第二實體第二公用金鑰係個別根據於至少該第一/第二實體主要金鑰及該產生器值。

【第25項】 一種控制一數位錢包的存取的方法，該方法包含下列步驟：

根據至少一第一實體主要私人金鑰及一產生器值來決定一第一實體第二私人金鑰；

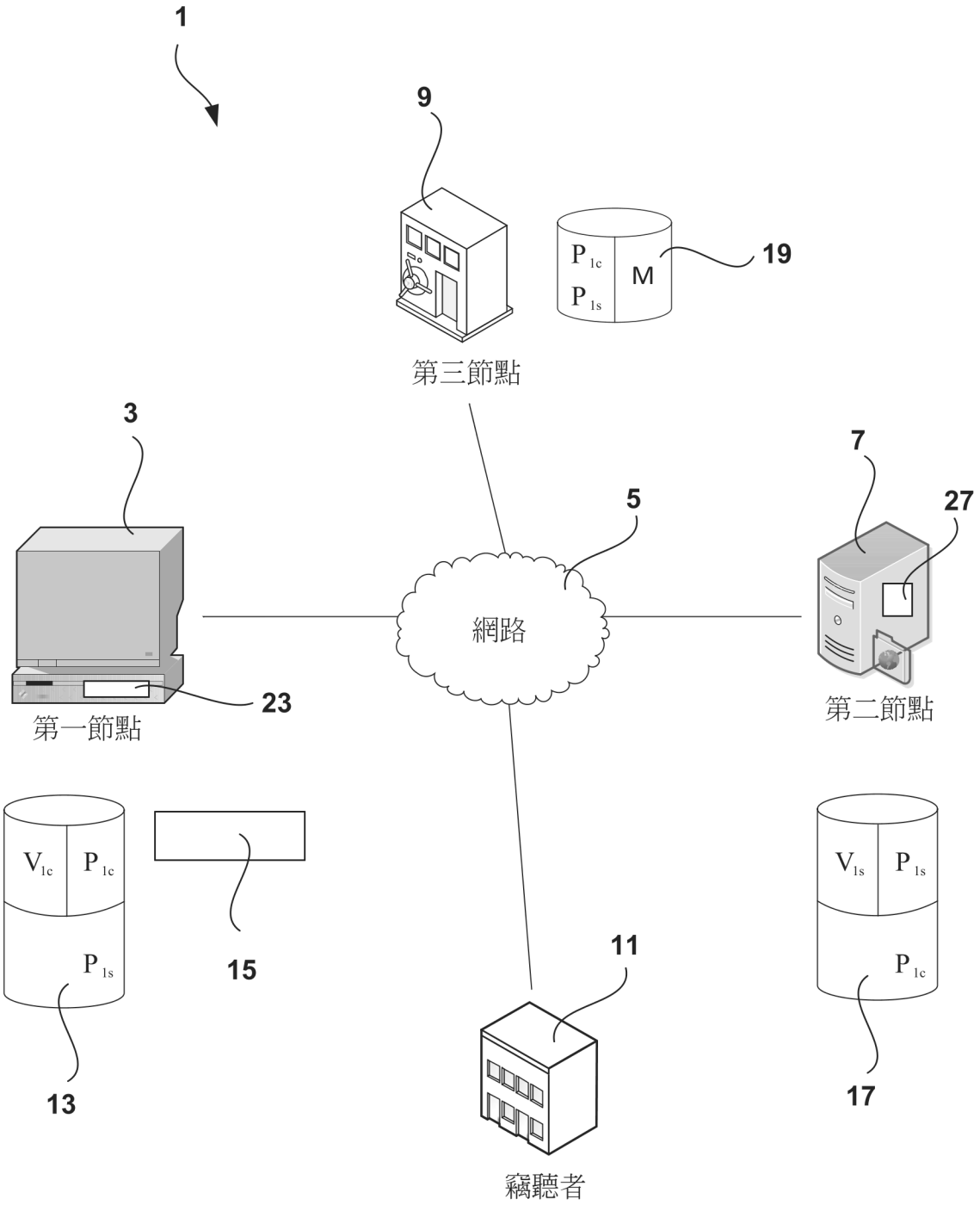
根據至少一第二實體主要私人金鑰及該產生器值來決定一第二實體第二私人金鑰；

根據該第一實體第二私人金鑰及一第二實體第二公用金鑰來決定該第一實體上的一共同私密(CS)，及根據該第二實體第二私人金鑰及一第一實體第二公用金鑰來決定該第二實體上的共同私密(CS)；以及

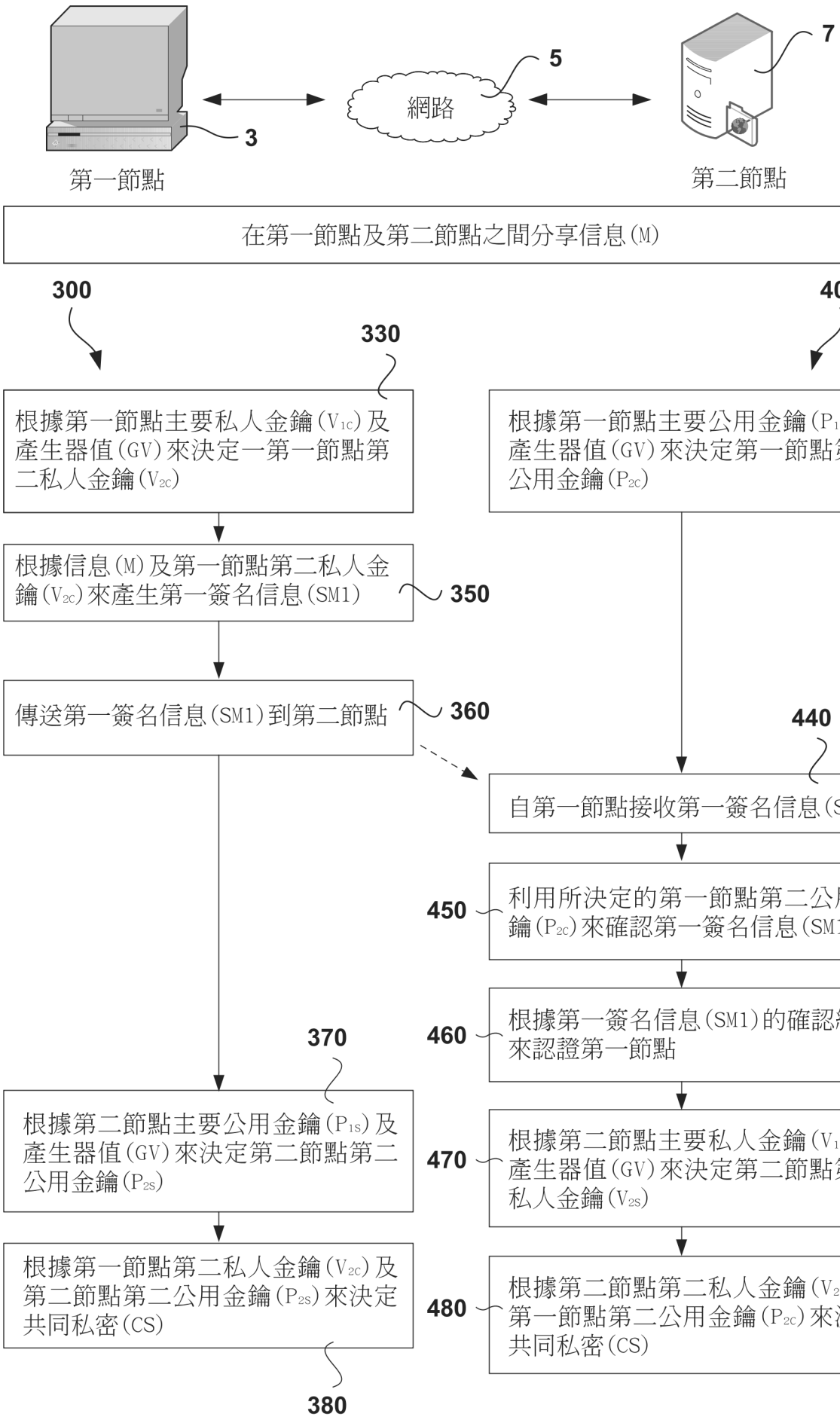
其中：

該第一實體第二公用金鑰及該第二實體第二公用金鑰係個別根據於至少該第一/第二實體主要金鑰及該產生器值。

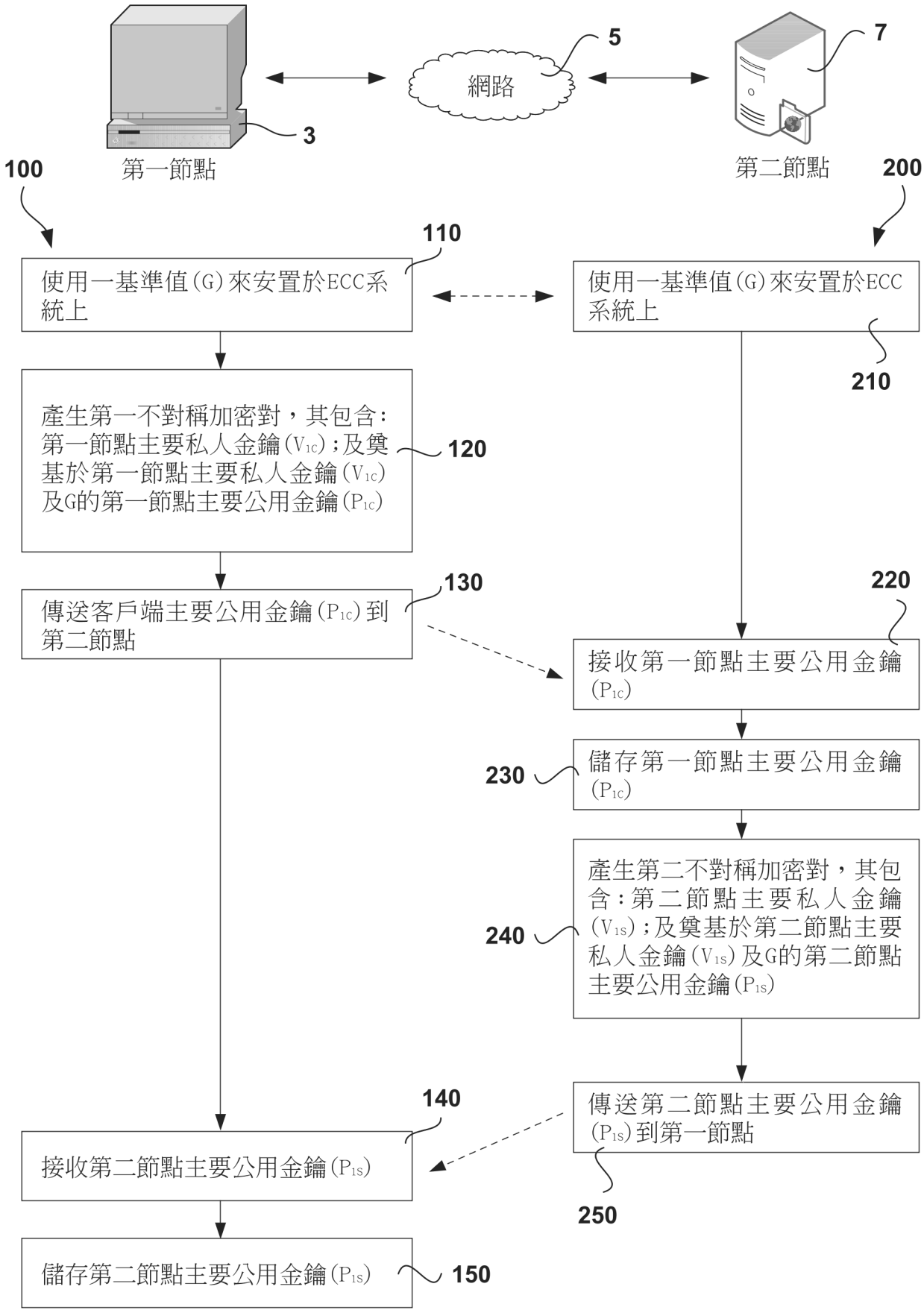
【發明圖式】


1
9
P_{1c}
P_{1s}
M
19
第三節點
3
7
27
5
網路
第一節點
23
第二節點
V_{1c}
P_{1c}
P_{1s}
15
11
V_{1s}
P_{1s}
P_{1c}
13
17
竊聽者

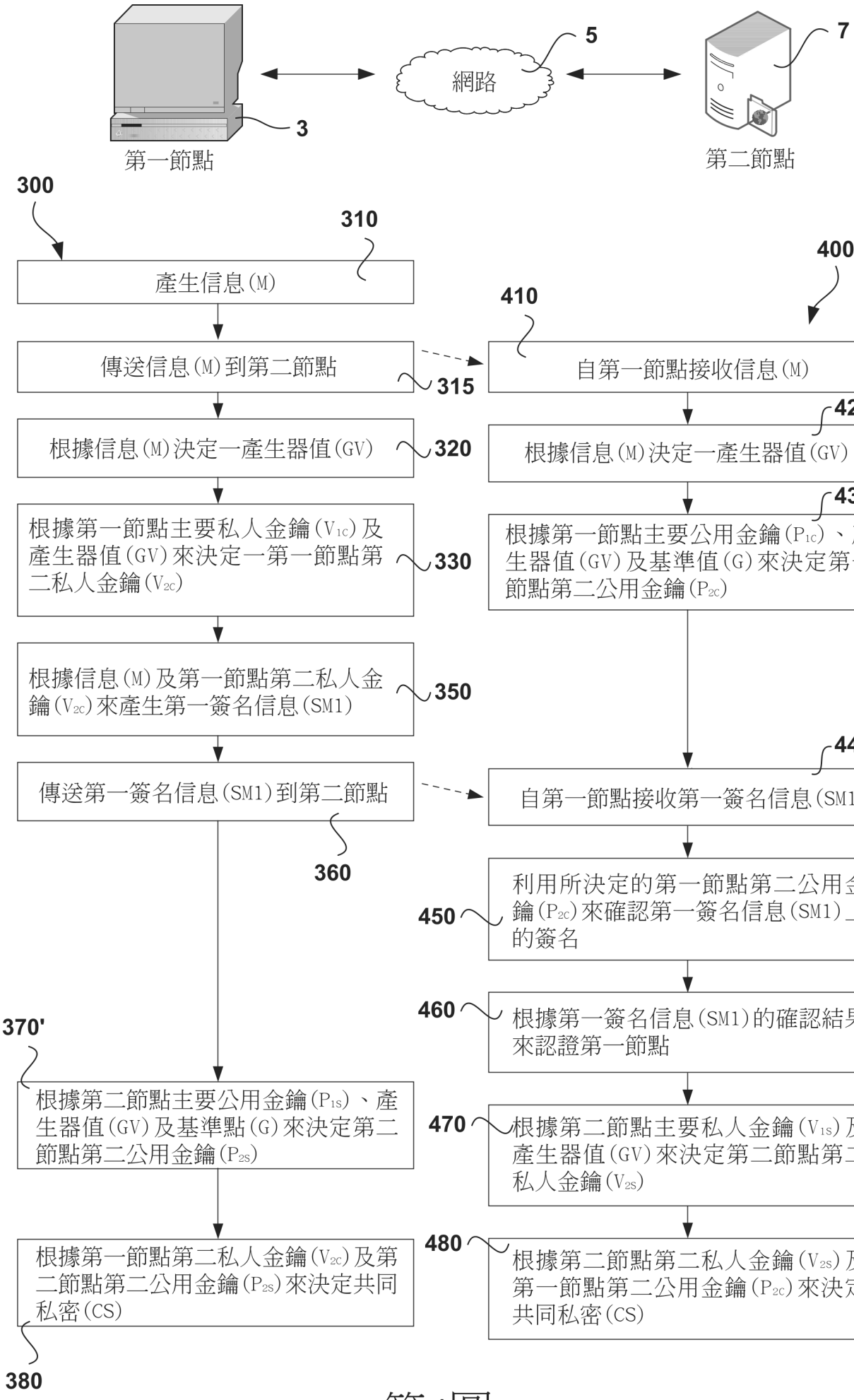
第1圖


第一節點
3
網路
5
第二節點
7
在第一節點及第二節點之間分享信息(M)
300
330
根據第一節點主要私人金鑰(V_{1C})及產生器值(GV)來決定一第一節點第二私人金鑰(V_{2C})
根據信息(M)及第一節點第二私人金鑰(V_{2C})來產生第一簽名信息(SM1)
350
傳送第一簽名信息(SM1)到第二節點
360
370
根據第二節點主要公用金鑰(P_{1S})及產生器值(GV)來決定第二節點第二公用金鑰(P_{2S})
根據第一節點第二私人金鑰(V_{2C})及第二節點第二公用金鑰(P_{2S})來決定共同私密(CS)
380
400
根據第一節點主要公用金鑰(P_{1C})及產生器值(GV)來決定第一節點第二公用金鑰(P_{2C})
430
440
自第一節點接收第一簽名信息(SM1)
450
利用所決定的第一節點第二公用金鑰(P_{2C})來確認第一簽名信息(SM1)上
460
根據第一簽名信息(SM1)的確認結果來認證第一節點
470
根據第二節點主要私人金鑰(V_{1S})及產生器值(GV)來決定第二節點第二私人金鑰(V_{2S})
480
根據第二節點第二私人金鑰(V_{2S})及第一節點第二公用金鑰(P_{2C})來決定共同私密(CS)

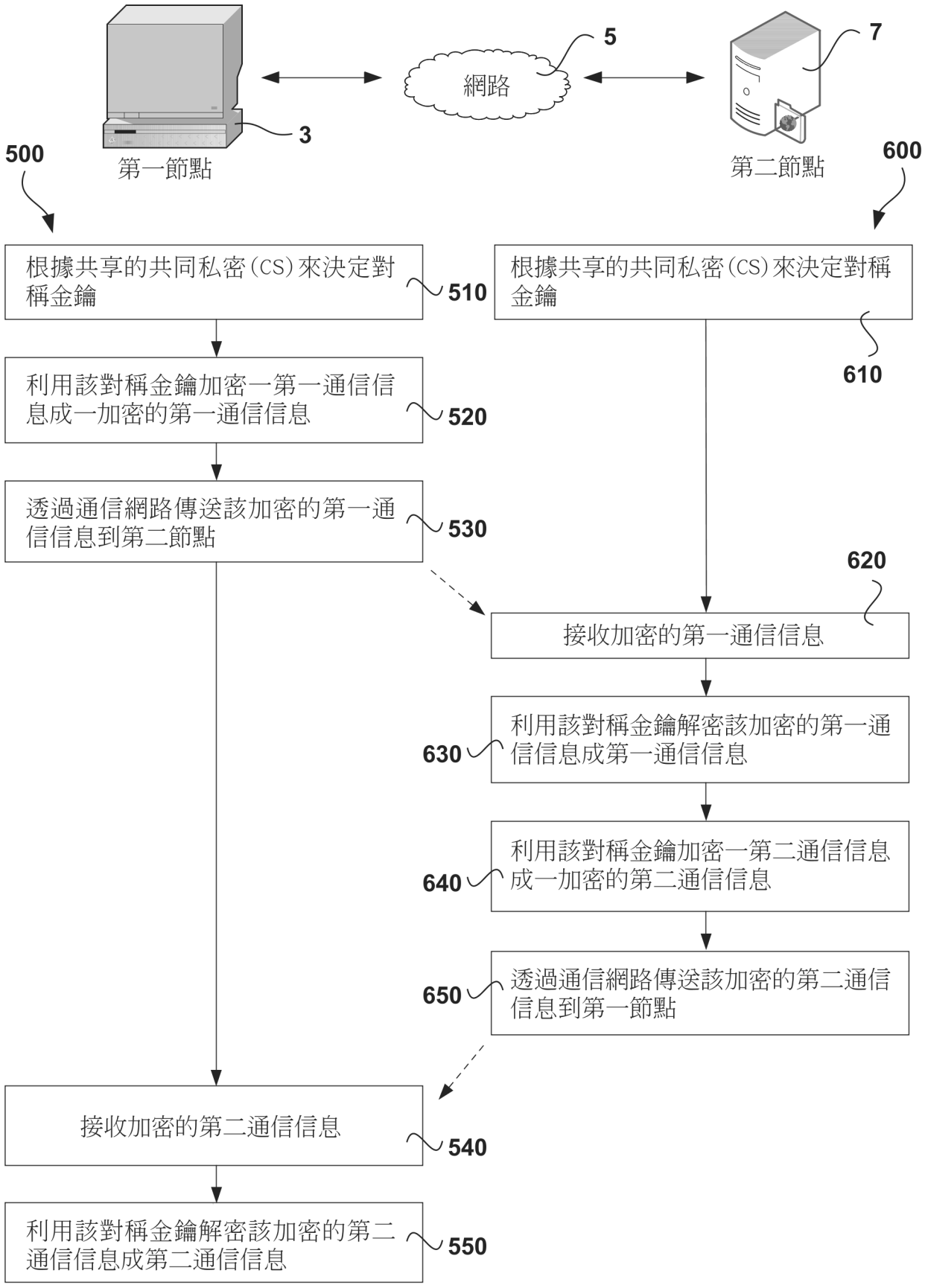
第2圖


網路
5
7
3
第一節點
第二節點
100
200
110
使用一基準值(G)來安置於ECC系統上
使用一基準值(G)來安置於ECC系統上
210
產生第一不對稱加密對，其包含：第一節點主要私人金鑰(V_{1C})；及奠基於第一節點主要私人金鑰(V_{1C})及G的第一節點主要公用金鑰(P_{1C})
120
130
傳送客戶端主要公用金鑰(P_{1C})到第二節點
220
接收第一節點主要公用金鑰(P_{1C})
230
儲存第一節點主要公用金鑰(P_{1C})
240
產生第二不對稱加密對，其包含：第二節點主要私人金鑰(V_{1S})；及奠基於第二節點主要私人金鑰(V_{1S})及G的第二節點主要公用金鑰(P_{1S})
140
傳送第二節點主要公用金鑰(P_{1S})到第一節點
250
接收第二節點主要公用金鑰(P_{1S})
儲存第二節點主要公用金鑰(P_{1S})
150

第3圖


第一節點
3
網路
5
第二節點
7
300
310
產生信息(M)
傳送信息(M)到第二節點
315
根據信息(M)決定一產生器值(GV)
320
根據第一節點主要私人金鑰(V_{1C})及產生器值(GV)來決定一第一節點第二私人金鑰(V_{2C})
330
根據信息(M)及第一節點第二私人金鑰(V_{2C})來產生第一簽名信息(SM1)
350
傳送第一簽名信息(SM1)到第二節點
360
370'
根據第二節點主要公用金鑰(P_{1S})、產生器值(GV)及基準點(G)來決定第二節點第二公用金鑰(P_{2S})
根據第一節點第二私人金鑰(V_{2C})及第二節點第二公用金鑰(P_{2S})來決定共同私密(CS)
380
400
410
自第一節點接收信息(M)
420
根據信息(M)決定一產生器值(GV)
430'
根據第一節點主要公用金鑰(P_{1C})、產生器值(GV)及基準值(G)來決定第一節點第二公用金鑰(P_{2C})
440
自第一節點接收第一簽名信息(SM1)
利用所決定的第一節點第二公用金鑰(P_{2C})來確認第一簽名信息(SM1)上的簽名
450
460
根據第一簽名信息(SM1)的確認結果來認證第一節點
470
根據第二節點主要私人金鑰(V_{1S})及產生器值(GV)來決定第二節點第二私人金鑰(V_{2S})
480
根據第二節點第二私人金鑰(V_{2S})及第一節點第二公用金鑰(P_{2C})來決定共同私密(CS)

第4圖


網路
5
7
3
第一節點
第二節點
500
600
根據共享的共同私密(CS)來決定對稱金鑰
510
根據共享的共同私密(CS)來決定對稱金鑰
610
利用該對稱金鑰加密一第一通信信息成一加密的第一通信信息
520
透過通信網路傳送該加密的第一通信信息到第二節點
530
620
接收加密的第一通信信息
利用該對稱金鑰解密該加密的第一通信信息成第一通信信息
630
利用該對稱金鑰加密一第二通信信息成一加密的第二通信信息
640
透過通信網路傳送該加密的第二通信信息到第一節點
650
接收加密的第二通信信息
540
利用該對稱金鑰解密該加密的第二通信信息成第二通信信息
550

第5圖