(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 201443684 A
(43)公開日： 中華民國 103 (2014) 年 11 月 16 日

(21)申請案號：103101867 (22)申請日： 中華民國 103 (2014) 年 01 月 17 日
(51)Int. Cl.： *G06F21/62 (2013.01)* *H04L9/28 (2006.01)*
(30)優先權：2013/01/18 美國 61/754,524
2013/03/15 美國 13/839,050
2013/03/15 美國 13/839,084
2013/03/15 美國 13/839,126
(71)申請人：蘋果公司 (美國) APPLE INC. (US)
美國
(72)發明人：包威爾 麥可 BROUWER, MICHAEL (NL)；迪 艾特力 達拉斯Ｂ DE ATLEY, DALLAS B. (US)；愛德勒 麥契爾Ｄ ADLER, MITCHELL D. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：20 項 圖式數：28 共 105 頁

(54)名稱

金鑰鏈同步

KEYCHAIN SYNCING

(57)摘要

一些實施例提供儲存一程式之非暫時性機器可讀媒體，該程式在由一裝置之至少一個處理單元執行時使儲存於該裝置上之一組金鑰鏈與一組其他裝置同步。該裝置及該組其他裝置經由一同級間(P2P)網路而通信地互相耦接。該程式接收對儲存於該裝置上之該組金鑰鏈中之一金鑰鏈的一修改。該程式針對該組其他裝置中之每一裝置而產生一更新請求，以便使儲存於裝置上之該組金鑰鏈與該組其他裝置同步。該程式經由該 P2P 網路而經由一組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置。

105：階段

110：階段

115：階段

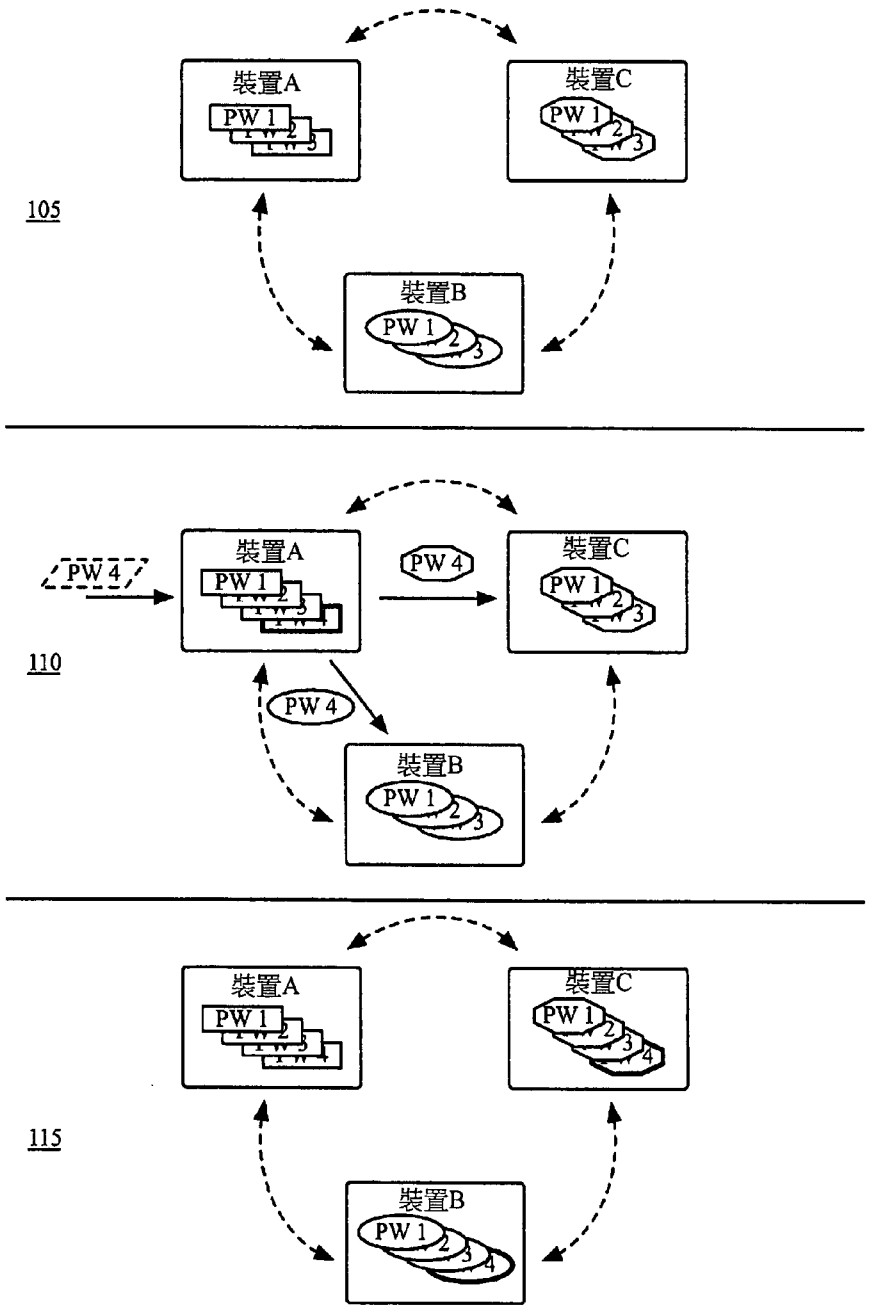

圖1

(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 201443684 A
(43)公開日： 中華民國 103 (2014) 年 11 月 16 日

(21)申請案號：103101867 (22)申請日： 中華民國 103 (2014) 年 01 月 17 日
(51)Int. Cl.： *G06F21/62 (2013.01)* *H04L9/28 (2006.01)*
(30)優先權：2013/01/18 美國 61/754,524
2013/03/15 美國 13/839,050
2013/03/15 美國 13/839,084
2013/03/15 美國 13/839,126
(71)申請人：蘋果公司 (美國) APPLE INC. (US)
美國
(72)發明人：包威爾 麥可 BROUWER, MICHAEL (NL)；迪 艾特力 達拉斯Ｂ DE ATLEY, DALLAS B. (US)；愛德勒 麥契爾Ｄ ADLER, MITCHELL D. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：20 項 圖式數：28 共 105 頁

(54)名稱

金鑰鏈同步

KEYCHAIN SYNCING

(57)摘要

一些實施例提供儲存一程式之非暫時性機器可讀媒體，該程式在由一裝置之至少一個處理單元執行時使儲存於該裝置上之一組金鑰鏈與一組其他裝置同步。該裝置及該組其他裝置經由一同級間(P2P)網路而通信地互相耦接。該程式接收對儲存於該裝置上之該組金鑰鏈中之一金鑰鏈的一修改。該程式針對該組其他裝置中之每一裝置而產生一更新請求，以便使儲存於裝置上之該組金鑰鏈與該組其他裝置同步。該程式經由該 P2P 網路而經由一組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置。

201443684

發明摘要

※ 申請案號：103101867

※ 申請日：103.1.17　　※IPC 分類：G06F 3/162 (2013.01)
H04L 9/38 (2006.01)

【發明名稱】

金鑰鏈同步

KEYCHAIN SYNCING

【中文】

一些實施例提供儲存一程式之非暫時性機器可讀媒體，該程式在由一裝置之至少一個處理單元執行時使儲存於該裝置上之一組金鑰鏈與一組其他裝置同步。該裝置及該組其他裝置經由一同級間(P2P)網路而通信地互相耦接。該程式接收對儲存於該裝置上之該組金鑰鏈中之一金鑰鏈的一修改。該程式針對該組其他裝置中之每一裝置而產生一更新請求，以便使儲存於裝置上之該組金鑰鏈與該組其他裝置同步。該程式經由該P2P網路而經由一組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置。

【英文】

Some embodiments provide non-transitory machine-readable medium that stores a program which when executed by at least one processing unit of a device synchronizes a set of keychains stored on the device with a set of other devices. The device and the set of other devices are communicatively coupled to one another through a peer-to-peer (P2P) network. The program receives a modification to a keychain in the set of keychains stored on the device. The program generates an update request for each device in the set of other devices in order to synchronize the set of keychains stored on device with the set of other devices. The program transmits through the P2P network the set of update requests to the set of other devices over a set of separate, secure communication channels.

【代表圖】

【本案指定代表圖】：第（1）圖。

【本代表圖之符號簡單說明】：

105　　階段

110　　階段

115　　階段

【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】

金鑰鏈同步

KEYCHAIN SYNCING

【先前技術】

在多個裝置當中共用資料對於多個裝置之使用者而言係一日益風行之特徵。該資料共用特徵係藉由更新完整檔案且在一些狀況下更新經指定用於在多個裝置當中同步之若干組完整之檔案而實施。提供資料共用特徵之許多應用程式以無保護之方式在多個裝置當中發送及接收資料。

【發明內容】

本發明之一些實施例提供一種用於促進在被指定為同步群組(亦稱作同步圈)之成員的若干裝置之間金鑰鏈之同步的新穎方法。在一些實施例中，金鑰鏈為可包括密碼(password)、私用金鑰、證書、安全註釋等之已定義之資料集合。在一些實施例中，該方法經由同級間(P2P)網路而在裝置之間使金鑰鏈同步。一些實施例之方法使用通信安全性特徵來防止對裝置之間之通信的未授權存取。

不同實施例使用不同技術來實施P2P網路，裝置經由該P2P網路而彼此通信。例如，一些實施例使用具有充分連接之網狀拓撲的疊加網路，而其他實施例使用具有星形拓撲之疊加網路。仍然，一些實施例利用任何數目之額外及/或不同疊加網路來實施P2P網路。

在一些實施例中，該方法提供用於保護裝置彼此傳達之資料的一安全輸送層。一些實施例之方法藉由使用基於訊息之通信協定(例如，非官方(OTR)傳訊)而在每一裝置之間提供安全通信頻道來實施安

全輸送層，而其他實施例之方法藉由使用基於流之通信協定(例如，安全通訊端層(SSL))而在每一對裝置之間提供安全通信頻道來實施安全輸送層。

一些實施例之方法藉由使一金鑰鏈之個別項目(亦稱作金鑰鏈項目)同步而在裝置之間使該金鑰鏈同步(與使整個金鑰鏈同步相對)。在一些例子中，當使金鑰鏈項目同步時，一些實施例之方法偵測相同金鑰鏈項目之多個版本之間的衝突。不同實施例之方法以不同方式來解析此等衝突。舉例而言，在一些實施例中，方法將金鑰鏈項目之最近版本用作待在裝置之間被同步之金鑰鏈項目。在一些實施例中可使用額外及/或不同方法。

在一些實施例中，方法提供用於根據一組已定義之條件及/或要求來限制對裝置上之金鑰鏈資料(例如，金鑰鏈項目)之存取的一資料保護特徵。舉例而言，在一些實施例中，裝置上之每一金鑰鏈項目被指定為屬於一特定保護域(protection domain)。一些實施例之方法僅當滿足針對一特定金鑰鏈項目所屬之特定保護域所定義的一組條件及/或要求時才允許裝置存取該特定金鑰鏈項目。條件及/或要求之實例包括裝置處於解除鎖定狀態、裝置處於鎖定狀態、裝置之使用者鍵入特定密碼等。按照此方法，可以粒狀方式來控制對裝置上之金鑰鏈項目的存取。

前述【發明內容】意欲充當對本發明之一些實施例之簡短介紹。其並不意謂為此文獻中所揭示之所有發明性標的的介紹或概述。隨後之【實施方式】及【實施方式】中所參考之圖式將另外描述【發明內容】中所描述之實施例以及其他實施例。因此，為理解由此文獻所描述之所有實施例，需要【發明內容】、【實施方式】及【圖式簡單說明】之完整審閱。此外，所主張之標的將不受【發明內容】、【實施方式】及【圖式簡單說明】中之說明性細節的限制，而是將由附加之

申請專利範圍來定義，因為所主張之標的可在不背離標的之精神的情況下以其他特定形式來體現。

【圖式簡單說明】

在附加之申請專利範圍中闡述本發明之新穎特徵。然而，出於解釋之目的，在以下諸圖中闡述本發明之若干實施例。

圖1概念地說明根據本發明之一些實施例之在若干裝置之間使密碼同步。

圖2概念地說明根據本發明之一些實施例之直接型P2P網路之網路架構。

圖3概念地說明根據本發明之一些實施例之間接型P2P網路之網路架構。

圖4概念地說明根據本發明之一些實施例之開始一同步圈及將裝置新增至該同步圈之實例。

圖5概念地說明用於請求加入一同步圈之一些實施例之處理程序。

圖6概念地說明用於處理加入一同步圈之請求之一些實施例之處理程序。

圖7概念地說明一實例資料流程，該資料流程透過**圖2**中所說明之網路架構以用於使密碼同步。

圖8及**圖9**概念地說明一實例資料流程，該資料流程透過**圖3**中所說明之網路架構以用於使密碼同步。

圖10概念地說明根據本發明之一些實施例之金鑰鏈之資料結構。

圖11概念地說明一狀態圖，該狀態圖描述一些實施例之金鑰鏈管理器之不同狀態及在此等狀態之間的轉變。

圖12概念地說明用於將更新推送至同級裝置之一些實施例之處

理程序。

圖13概念地說明用於處理來自同級裝置之更新之一些實施例之處理程序。

圖14概念地說明用於解析相衝突之衝突解析之一些實施例之處理程序。

圖15概念地說明用於解析金鑰鏈項目衝突之一些實施例之處理程序。

圖16概念地說明不同裝置中之不同金鑰鏈項目。

圖17概念地說明一些實施例執行以處理金鑰鏈項目之處理程序。

圖18概念地說明用於存放傳入之金鑰鏈項目之一處理佇列。

圖19概念地說明一些實施例執行以處理自源裝置接收之金鑰鏈項目之處理程序。

圖20說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被解除鎖定以便使屬於該保護域之金鑰鏈項目在裝置處可用。

圖21說明受一保護域保護之金鑰鏈項目，該保護域需要裝置至少一旦在經啟動之後便被解除鎖定以便使屬於該保護域之金鑰鏈項目在裝置處可用。

圖22說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被接通以便使屬於該保護域之金鑰鏈項目在裝置處可用。

圖23說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被解除鎖定且亦需要額外鑑認以便使屬於該保護域之金鑰鏈項目在裝置處可用。

圖24說明受兩個保護域保護之資料，該兩個保護域針對裝置而具有不同組條件。

圖25概念地說明由若干裝置所形成之若干同步圈。

圖26概念地說明一由若干裝置針對若干不同保護域所形成之同步圈。

圖27概念地說明一些實施例之金鑰鏈管理器之軟體架構。

圖28概念地說明一電子系統，可用該電子系統來實施本發明之一些實施例。

【實施方式】

在本發明之以下詳細描述中，闡述及描述本發明之眾多細節、實例及實施例。然而，熟習此項技術者將清楚且顯而易見，本發明並不限於所闡述之實施例且可在沒有所論述之特定細節及實例中之一些特定細節及實例的情況下實踐本發明。例如，出於簡單性及/或解釋之目的，本申請案中之許多圖係關於一特定數目之裝置而描述。一般熟習此項技術者將認識到，本發明並不限於此等圖中所說明之裝置之數目且可用任何數目之不同裝置來實踐本發明。

本發明之一些實施例提供一種用於促進在被指定為同步群組(亦稱作同步圈)之成員的若干裝置之間使金鑰鏈同步的新穎方法。在一些實施例中，金鑰鏈為可包括密碼、私用金鑰、證書、安全註釋等之已定義之資料集合。在一些實施例中，該方法經由P2P網路而在裝置之間使金鑰鏈同步。一些實施例之方法使用通信安全性特徵來防止對裝置之間之通信的未授權存取。

不同實施例使用不同技術來實施P2P網路，裝置經由該P2P網路而彼此通信。例如，一些實施例使用具有充分連接之網狀拓撲的疊加網路，而其他實施例使用具有星形拓撲之疊加網路。仍然，一些實施例利用任何數目之額外及/或不同疊加網路來實施P2P網路。

在一些實施例中，該方法提供用於保護裝置彼此傳達之資料的一安全輸送層。一些實施例之方法藉由使用基於訊息之通信協定(例如，OTR傳訊)而在每一對裝置之間提供安全通信頻道來實施安全輸

送層，而其他實施例之方法藉由使用基於流之通信協定(例如，SSL)而在每一對裝置之間提供安全通信頻道來實施安全輸送層。

一些實施例之方法藉由使一金鑰鏈之個別項目(亦稱作金鑰鏈項目)同步而在裝置之間使該金鑰鏈同步(與使整個金鑰鏈同步相對)。在一些例子中，當使金鑰鏈項目同步時，一些實施例之方法偵測相同金鑰鏈項目之多個版本之間的衝突。不同實施例之方法以不同方式來解析此等衝突。舉例而言，在一些實施例中，方法將金鑰鏈項目之最近版本用作待在裝置之間被同步之金鑰鏈項目。在一些實施例中可使用額外及/或不同方法。

在一些實施例中，方法提供用於根據一組已定義之條件及/或要求來限制對裝置上之金鑰鏈資料(例如，金鑰鏈項目)之存取的一資料保護特徵。舉例而言，在一些實施例中，裝置上之每一金鑰鏈項目被指定為屬於一特定保護域。一些實施例之方法僅當滿足針對一特定金鑰鏈項目所屬之特定保護範圍所定義的一組條件及/或要求時才允許裝置存取該特定金鑰鏈項目。條件及/或要求之實例包括裝置處於解除鎖定狀態、裝置處於鎖定狀態、裝置之使用者鍵入特定密碼等。按照此方法，可以粒狀方式來控制對裝置上之金鑰鏈項目的存取。

圖1概念地說明根據本發明之一些實施例之在若干裝置A至C之間使密碼同步。具體言之，**圖1**說明裝置A至C處於在裝置A至C之間的密碼之實例同步之三個不同階段105至115。在此實例中，裝置A至C被指定為一同步圈之成員，該等成員將密碼彼此同步。裝置A至C中之每一者可為桌上型電腦、膝上型電腦、智慧電話、平板電腦或任何其他類型之計算裝置。

第一階段105說明密碼1至3在裝置A至C之間被同步，如由具有相同密碼1至3之複本之裝置A至C中之每一者所指示。對於此實例而言，裝置A至C中之每一者上的密碼1至3以僅裝置可解密及存取之加

密格式而被儲存於裝置上。此安全性特徵藉由將裝置A至C中之每一者中的一組密碼1至3描繪為特定形狀而在**圖1**中被概念化。詳言之，儲存於裝置A上之密碼1至3經展示為矩形、儲存於裝置B上之密碼1至3經展示為卵形，且儲存於裝置C上之密碼1至3經展示為不規則凸八邊形。因而，在此實例中，裝置A可僅解密及存取矩形密碼，裝置B可僅解密及存取卵形密碼，且裝置C可僅解密及存取不規則凸八邊形密碼。

圖1之第二階段110展示密碼4被新增至裝置A (例如，裝置A之使用者使用裝置A來建立密碼4)。如所示，密碼4得以以矩形形狀被加密及儲存於裝置A上。在第二階段110中，裝置A正向裝置B及C發送密碼4之複本以便使密碼4與裝置B及C同步。在一些實施例中，當裝置A接收到密碼4時，裝置A向裝置B發送以僅裝置B才可解密之格式而被加密之密碼4之複本且向裝置C發送以僅裝置C才可解密之格式而被加密之密碼4之另一複本。此由裝置A將密碼4作為卵形形狀發送至裝置B及將密碼4作為不規則凸八邊形形狀發送至裝置C來指示。

如上文所提及，一些實施例提供通信安全性特徵來防止對裝置之間之通信的未授權存取。為保護與裝置B之通信，在此實例中，裝置A加密密碼4之複本且使用安全通信協定(例如，SSL、OTR等)經由安全頻道將其發送至裝置B。一些實施例之安全通信頻道為經鑑認及加密之通信頻道。在一些實施例中，裝置B以用以經由安全頻道來傳輸密碼4之加密格式來儲存密碼4。類似地，在一些實施例中，裝置C以用以經由安全頻道來傳輸密碼4之加密格式來儲存該密碼。

第三階段115展示密碼104在裝置A至C之間被同步。如所示，裝置B正儲存裝置B自裝置A接收之密碼4之經加密複本且因此與裝置A同步。同樣地，裝置C正儲存裝置C自裝置A接收之密碼4之經加密複本且因此與裝置A同步。如上文所論述，在此實例中，儲存於裝置B

上之密碼4以僅裝置B才可解密之格式而被加密，且儲存於裝置C上之密碼4以僅裝置C才可解密之格式而被加密。

本申請案中描述眾多細節、實例及實施例，該等細節、實例及實施例參考裝置儲存密碼以用於在為一同步圈之成員的裝置當中同步。然而，一般熟習此項技術者將理解，在一些實施例中，同步圈中之裝置中的一或多者亦儲存不與同步圈中之其他裝置中之一些或全部裝置共用(亦即，同步)的密碼。

此外，雖然本申請案中所解釋之大部分細節、實例及實施例係針對使經儲存作為金鑰鏈之部分的密碼同步，但一般熟習此項技術者將認識到，本發明並不限於使密碼同步且可實踐本發明以在位於同步圈中之裝置當中使金鑰鏈中之其他類型之資料(例如，私用金鑰、證書、安全註釋等)同步。另外，一般熟習此項技術者將認識到，可實踐本發明以在位於同步圈中之裝置當中使一個以上之金鑰鏈同步。

在以下之部分中描述本發明之若干較詳細實施例。部分I概念地描述根據本發明之一些實施例之實例P2P網路架構之細節。接下來，部分II概念地描述根據本發明之一些實施例之建立一同步圈及將裝置註冊至該同步圈中。部分III描述根據本發明之一些實施例之在位於同步圈中之裝置之間使金鑰鏈同步的細節。接下來，部分IV描述根據本發明之一些實施例之用於金鑰鏈之資料保護特徵。部分V描述一些實施例之金鑰鏈管理器之軟體架構。最後，部分VI描述一實施本發明之一些實施例之電子系統。

I. 同級間網路架構

如上文所提及，一些實施例經由P2P網路而在為一同步圈之成員的裝置之間使金鑰鏈同步。不同實施例之P2P網路係使用不同網路架構而實施以便促進同步圈中之裝置之間的通信。以下諸圖說明P2P網路架構之不同實施之若干實例。

圖2概念地說明根據本發明之一些實施例之直接型P2P網路之網路架構。在此實例中，裝置A至C為一同步圈之成員。如所示，裝置A至C中之每一者包括：用於儲存密碼之一儲存器210；及一金鑰鏈管理器205。一些實施例之金鑰鏈管理器205負責執行用於促進在裝置A至C之間密碼之同步的功能。例如，在一些實施例中，金鑰鏈管理器205處置以下各者：將裝置註冊至同步圈中、在裝置A至C之間使密碼同步、解析相衝突之密碼之間的衝突、產生金鑰鏈之不同類型之資訊清單、提供用於在裝置A至C之間輸送資料的一安全通信頻道等。

如**圖2**中所說明，裝置A至C經由具有充分連接之網狀拓撲的疊加網路來彼此通信。因而，裝置A至C中之每一者可直接與其他裝置中之每一者通信。亦即，裝置A可直接與裝置B及C通信，裝置B可直接與裝置A及C通信，且裝置C可直接與裝置A及B通信。

如上文所註釋，一些實施例提供一安全輸送層以保護裝置彼此傳達之資料。對於此實例而言，裝置A至C經由在每一對裝置A至C之間所建立之安全通信頻道來彼此通信。可使用任何數目之不同協定(諸如，基於訊息之通信協定(例如，OTR傳訊)、基於流之通信協定(例如，SSL)等)來實施該等安全通信頻道。

圖3概念地說明根據本發明之一些實施例之間接型P2P網路之網路架構。類似於**圖2**，對於此實例而言，裝置A至C為一同步圈之成員且裝置A至C中之每一者包括儲存器210及金鑰鏈管理器205。

如**圖3**中所示，裝置A至C經由具有星形拓撲之疊加網路來彼此通信。詳言之，裝置A至C經由雲端服務305來彼此通信，該雲端服務305充當星形拓撲之中心且提供用於儲存資料之雲端儲存服務以及其他雲端服務(例如，雲端計算服務)。例如，當裝置A想要將資料傳達至裝置B時，裝置A將資料儲存於雲端服務305中，雲端服務305關於該資料而通知(例如，經由推送通知服務)裝置B，且裝置B自雲端服務

305擷取該資料。

如所說明，雲端服務305將同步圈之名稱及同步圈裝置清單儲存於儲存器310中，該同步圈裝置清單指定為同步圈之成員的裝置。在一些實施例中，裝置係由唯一地識別該等裝置之資料而指定。此資料之實例包括用於鑑認裝置之身分之裝置簽署公用/私用金鑰對的公用金鑰、裝置之裝置類型(例如，桌上型電腦、平板電腦、智慧電話等)、裝置之名稱等，或任何數目之此資料之組合。

雲端服務305亦將使用者簽名儲存於儲存器315中。在一些實施例中，使用者簽名係用於將使用者之身分鑑認為訊息、文獻或任何其他類型之資料之簽署人的數位簽名。在一些實施例中，同步圈被鏈接至雲端服務帳戶且與該雲端服務帳戶相關聯之裝置(例如，具有用於存取與該帳戶相關聯之雲端服務之應用程式或程式的裝置)為供註冊至同步圈中之候選者。在一些此等實施例中，儲存器315包括用一基於雲端服務帳戶之密碼所產生之使用者簽署公用/私用金鑰對的私用金鑰所簽署之簽名以指示雲端服務305帳戶之使用者為簽署人。被儲存於儲存器315中之使用者簽名之實例包括用一使用者簽署公用/私用金鑰對之私用金鑰所簽署的同步圈裝置清單之簽名、用使用者簽署金鑰對之私用金鑰所簽署的註冊請求之簽名，及/或用於鑑認雲端服務帳戶之使用者之身分的任何其他簽名。

圖3亦展示雲端服務305將裝置簽名儲存於儲存器320中。在一些實施例中，裝置簽名為用於將同步圈中之裝置之身分鑑認為訊息、文獻或任何其他類型之資料之簽署人的數位簽名。舉例而言，在一些實施例中，儲存器320包括用一裝置簽署公用/私用金鑰對之私用金鑰所簽署的同步圈裝置清單之簽名，該裝置簽署公用/私用金鑰對屬於為同步圈之成員的裝置。此簽名指示簽署裝置將同步圈裝置清單中之裝置之清單肯定為同步圈之成員。在一些實施例中，當同步圈處於穩定

狀態時(例如，無註冊請求係未決或未經同意)，儲存器320中之裝置簽名針對為同步圈之成員的每一裝置而包括用裝置之裝置簽署公用/私用金鑰對之私用金鑰所簽署的同步圈裝置清單之簽名。亦即，在此等例子中，該等簽名共同地指示同步圈裝置清單中所列舉之每一裝置同意同步圈裝置清單中所列舉之裝置為同步圈之成員。

另外，雲端服務305將金鑰鏈資料儲存於儲存器325中以用於在位於同步圈中之裝置之間使金鑰鏈同步，且將其他資料儲存於儲存器330中，該其他資料可包括：使用者簽署公用/私用金鑰對之公用金鑰；在位於同步圈中之裝置之間共用以用於產生使用者簽署金鑰對的隨機串(例如，256位元串)；及未決之註冊請求之清單。在一些實施例中，雲端服務305將儲存器310至330實施為金鑰值儲存器。

雖然**圖3**中將儲存器310至330說明為分開之儲存器，但在一些實施例中，儲存器310至330被實施為單一儲存器，而在其他實施例中，儲存器310至330被實施跨越若干儲存器。

在一些實施例中，利用上文藉由參看**圖2**所描述之安全輸送層以保護裝置經由雲端服務305來彼此傳達之資料。亦即，雖然裝置A至C經由建立於每一對裝置A至C之間的安全通信頻道來彼此通信，但裝置A至C將雲端服務305用作用於輸送通信之機構。在一些實施例中，可使用任何數目之不同協定(例如，基於訊息之通信協定(例如，OTR傳訊)、基於流之通信協定(例如，SSL)等)來實施一些實施例之安全通信頻道。

II. 同步圈

如上文所描述，為圈同步圈之成員的裝置在裝置之間使金鑰鏈同步。在本申請案中，亦將此等裝置稱作同級裝置或簡單地稱作同級者。以下部分描述建立一同步圈以用於在該同步圈之裝置之間使金鑰鏈同步及將裝置新增至該同步圈之實例。

圖4概念地說明根據本發明之一些實施例之開始一同步圈420及將裝置新增至該同步圈420之實例。詳言之，**圖4**說明將裝置A及B註冊至同步圈420中之三個階段405至415。該等階段405至410中之每一者展示同步圈420及一儲存同步圈420之資料之儲存器425的概念性描述。在一些實施例中，儲存器425被實施於雲端儲存服務305中且包括儲存器310至330中之資料，該資料係上文藉由參看**圖3**所描述。在一些實施例，結合在雲端儲存服務中實施儲存器425，為同步圈420之成員的每一裝置將資料之複本本端地儲存於裝置上之儲存器425中。

第一階段405說明同步圈420不具有被註冊至同步圈420中之裝置。如所示，同步圈420為空白且儲存器425不含有關於同步圈420之成員的資料。一些實施例之同步圈420被鏈接至雲端儲存服務帳戶且與該雲端儲存服務帳戶相關聯之裝置(例如，具有用於存取與該帳戶相關聯之雲端儲存器之應用程式或程式的裝置)為供註冊至同步圈420中之候選者。在一些此等實施例中，儲存器425儲存描述與該帳戶相關聯之裝置的後設資料。

第二階段410展示同步圈420具有一被註冊至同步圈420中之裝置。如第二階段410中所示，裝置A被註冊至同步圈420中且儲存器425正儲存將裝置A識別為同步圈420之成員的資料。在一些實施例中，當同步圈420為空白時，同步圈420實際上不存在。在一些此等實施例中，當第一裝置註冊至同步圈420中時，建立同步圈420。當與雲端儲存服務帳戶相關聯之裝置中之一者的使用者啟用裝置上之金鑰鏈同步特徵時，該裝置建立同步圈420且將其自身註冊至同步圈420中。

為註冊至同步圈420中，裝置A將資料儲存於儲存器425中，該資料將裝置A唯一地識別為同步圈420之成員。此種資料之實例包括：用於鑑認裝置A之裝置簽署公用/私用金鑰對之公用金鑰；裝置A之裝置類型(例如，桌上型電腦、平板電腦、智慧電話等)、裝置A之名稱

等，或任何數目之此種資料之組合。

在一些實施例中，位於同步圈420中或可潛在地加入同步圈420之每一裝置使用相同之公用金鑰密碼編譯演算法(例如，RSA演算法、橢圓曲線密碼編譯(ECC)演算法等)以產生裝置簽署金鑰對使得該等裝置可加密及解密彼此之訊息。另外，在一些實施例中，每一裝置隨機地產生裝置簽署公用/私用金鑰對。如此，每一裝置產生與由任一其他裝置所產生之裝置簽署公用/私用金鑰對不同之唯一裝置簽署公用/私用金鑰對。

在一些實施例中，裝置A：(1)藉由用用於鑑認雲端儲存服務帳戶之使用者之使用者簽署公用/私用金鑰對之私用金鑰加密資料而產生識別同步圈420之成員之資料(在此實例中為唯一地識別裝置A之資料)之簽名；及(2)將所簽署之資料儲存於儲存器425中。一些實施例之使用者簽署公用/私用金鑰對係基於以下各者而產生：(1)與雲端儲存服務帳戶相關聯之密碼；及(2)在位於同步圈420中之裝置當中共用的隨機串(例如，256位元串)。

在一些實施例中，位於同步圈420中或可潛在地加入同步圈420之每一裝置使用相同之公用金鑰密碼編譯演算法(例如，RSA演算法、ECC演算法等)，以產生使用者簽署金鑰對。在一些實施例中，此等裝置利用被用以產生裝置簽署金鑰對之公用金鑰密碼編譯演算法以同樣產生使用者簽署金鑰對。該等裝置皆產生相同之公用/私用金鑰對，因為該等裝置各自將與雲端儲存服務帳戶相關聯之密碼及隨機串用作相同之公用金鑰密碼編譯演算法之輸入。因而，在此實例中，識別同步圈420之成員之資料的簽名係用於鑑認雲端儲存服務帳戶之使用者正將裝置A註冊至同步圈420中。由於裝置A為被註冊至同步圈420中之第一個裝置，所以裝置A將使用者簽署金鑰對之公用金鑰及隨機串儲存於儲存器425中。

第三階段415說明另一裝置被註冊至同步圈420中。如所示，裝置B被註冊至同步圈420中，且儲存器425正儲存將裝置B亦識別為同步圈420之成員的資料。另外，由於裝置A及裝置B為同步圈420之成員，所以裝置A及B上之密碼得以同步。

為使裝置B註冊至同步圈420中，一些實施例需要：(1)裝置B藉由將加入同步圈420之請求儲存於儲存器425中來提交該請求；及(2)裝置A核准該請求。不同實施例定義用以核准加入同步圈之請求的不同要求。例如，一些實施例僅需要為同步圈之成員的一個裝置核准該請求，而其他實施例需要為同步圈之成員的每一裝置核准該請求。

圖5概念地說明用於請求加入一同步圈之一些實施例之處理程序500。在一些實施例中，請求加入同步圈之裝置執行處理程序500 (例如，在裝置之使用者啟用裝置上之金鑰鏈同步特徵後)。將藉由參考執行處理程序500之**圖4**之裝置B來描述該處理程序500。

處理程序500藉由提示(在510處)裝置B之使用者鍵入密碼而開始。在一些實施例中，處理程序500藉由在裝置B之顯示螢幕上顯示一快顯視窗來提示使用者鍵入密碼，該快顯視窗請求使用者鍵入至雲端儲存服務帳戶之密碼。

接下來，處理程序500基於由使用者所提供之密碼而產生(在520處)使用者簽署公用/私用金鑰對。在一些實施例中，處理程序500基於供在同步圈420之成員之間共用的密碼及隨機串而產生使用者簽署金鑰對。一些此等實施例之處理程序500自儲存器425擷取隨機串以便產生使用者簽署金鑰對。在不同實施例中，處理程序500使用不同技術來產生使用者簽署金鑰對。例如，在一些實施例中，處理程序500可使用RSA演算法、ECC演算法或任何其他類型之公用金鑰密碼編譯，以產生裝置簽署金鑰對。

處理程序500接著產生(在530處)用於鑑認裝置B之一裝置簽署公

用/私用金鑰對。不同實施例之處理程序500使用不同技術來產生裝置簽署金鑰對。在一些實施例中，處理程序500使用用以在520處產生使用者簽署金鑰對之相同類型之公用金鑰密碼編譯來產生裝置簽署金鑰對。在其他實施例中，處理程序500使用一不同類型之公用金鑰密碼編譯來產生裝置簽署金鑰對。

一旦產生裝置簽署金鑰對，處理程序500便產生(在540處)加入同步圈420之請求。在一些實施例中，該請求包括：用於唯一地識別裝置B的裝置B之裝置簽署金鑰對之公用金鑰；及處理程序500自儲存器425擷取之同步圈420中之裝置之清單。

接下來，處理程序500基於所產生之金鑰對而產生(在550處)請求之簽名。具體言之，處理程序500產生：(1)具有使用者簽署金鑰對之私用金鑰的請求之簽名；及(2)具有裝置B之裝置簽署金鑰對之私用金鑰的請求之簽名。

最後，處理程序500提交(在560處)該請求及所產生之簽名。在一些實施例中，處理程序500藉由將請求新增至儲存於儲存器425中之註冊請求清單來提交該請求。一些實施例之處理程序500藉由將用使用者簽署金鑰對之私用金鑰所簽署的請求之簽名及具有裝置B之裝置簽署金鑰對之私用金鑰的請求之簽名儲存於儲存器425中來提交該等簽名。

圖6概念地說明用於處理加入一同步圈之請求之一些實施例之處理程序。在一些實施例中，當為同步圈之成員的裝置接收到加入同步圈之請求已被提交且為未決之通知(例如，經由推送通知服務)時，該裝置執行處理程序600。將藉由參考執行處理程序600之**圖4**之裝置B來描述該處理程序600。

處理程序600藉由擷取(在610處)將裝置B新增至同步圈420之請求而開始。在一些實施例中，處理程序600藉由存取儲存器425及自註冊

請求清單擷取請求、用裝置B之裝置簽署金鑰對之私用金鑰所簽署的請求之簽名及用使用者簽署金鑰對之私用金鑰所簽署的請求之簽名而擷取該請求。

接下來，處理程序600判定(在620處)該請求是否得以鑑認。在一些實施例中，當處理程序600驗證(1)雲端儲存服務帳戶之使用者提交將裝置B註冊至同步圈420中之請求及(2)將裝置註冊至同步圈420中之請求實際上係用於註冊裝置B時，處理程序600鑑認該請求。為驗證雲端儲存服務帳戶之使用者提交註冊裝置B之請求，一些實施例之處理程序600：(1)用使用者簽署金鑰對之公用金鑰來解密用使用者簽署金鑰對之私用金鑰所簽署的請求之簽名；及(2)檢查自註冊請求清單所擷取之請求資料匹配經解密之簽名。換言之，處理程序600檢查用使用者簽署金鑰對之私用金鑰所簽署的請求之經解密簽名包括裝置B之裝置簽署金鑰對之公用金鑰及同步圈420中之裝置之清單。

在一些實施例中，處理程序600藉由以下步驟來驗證將裝置註冊至同步圈420中之請求係用於註冊裝置B：(1)用裝置B之裝置簽署金鑰對之公用金鑰來解密用裝置B之裝置簽署金鑰對之私用金鑰所簽署的請求之簽名；及(2)檢查自註冊請求清單所擷取之請求資料匹配經解密之簽名。替代地或除解密用裝置B之裝置簽署金鑰對之私用金鑰所簽署的請求之簽名之外，一些實施例之處理程序600還使用其他技術來驗證將裝置註冊至同步圈420中之請求係用於註冊裝置B。例如，處理程序600可：在裝置B請求註冊至同步圈中時提示使用者鍵入經隨機地產生並被顯示於裝置B上之密碼、通行碼(passcode)、個人識別號碼(PIN)碼等；在裝置B正請求註冊至同步圈420中時選擇顯示於裝置A上之匹配顯示於裝置B上之影像的影像；等。

在630處，處理程序600判定請求是否業已得到同步圈中之裝置的核准。在一些實施例中，當儲存器425包括以下各者之簽名時，處

理程序600判定請求業已得到同步圈中之裝置的核准：(1)同步圈420中之裝置之清單；及(2)用屬於同步圈中之裝置之裝置簽署公用/私用金鑰對之私用金鑰所簽署的請求裝置。

當處理程序600判定請求業已得以核准時，處理程序600確認(在640處)對該請求之核准且接著處理程序600結束。一些實施例之處理程序600藉由以下步驟來確認對該請求之核准：(1)用其上正運行有處理程序600之裝置之裝置簽署金鑰對之私用金鑰來產生同步圈裝置清單(其現包括新近核准之裝置)之簽名；及(2)將所產生之簽名與裝置簽名一起儲存於儲存器425中。

當處理程序600判定該請求尚未得以核准時，處理程序600提示使用者(在650處)核准該請求。不同實施例以不同方式來核准請求。舉例而言，一些實施例之處理程序600在使用者將密碼提供至雲端儲存服務帳戶時核准該請求。由於一些實施例之裝置在使用者將密碼鍵入至該裝置中時不將密碼儲存至雲端儲存服務帳戶，所以一些實施例之處理程序600藉由在裝置A之顯示螢幕上顯示快顯視窗而提示使用者鍵入密碼，該快顯視窗：(1)指示裝置B之裝置名稱(例如，「John Doe之智慧電話」)已請求加入同步圈420；及(2)請求使用者鍵入與雲端儲存服務帳戶相關聯之密碼。

接下來，處理程序600判定(在660處)是否自使用者接收到用以核准該請求之輸入。當處理程序600判定未接收到用於核准該請求之輸入時，處理程序返回至660以繼續檢查來自使用者之輸入。當處理程序600判定接收到用於核准該請求之輸入時，處理程序600進行至670。

在670處，處理程序判定使用者核准是否得以鑑認。在使用至雲端儲存服務帳戶之密碼來驗證雲端儲存服務帳戶之使用者核准該請求的例子中，一些實施例之處理程序600藉由基於由使用者在650處所提

供之密碼及儲存於儲存器425中之隨機串而產生使用者簽署公用/私用金鑰對來鑑認使用者核准且驗證處理程序600所產生之公用金鑰匹配儲存於儲存器425中之使用者簽署金鑰對之公用金鑰。在一些實施例中，如上文所解釋，位於同步圈420中或可潛在地加入同步圈420之每一裝置使用相同演算法來產生使用者簽署金鑰對。因此，由處理程序600所產生且匹配儲存於儲存器425中之使用者簽署金鑰對之公用金鑰的公用金鑰驗證雲端儲存服務帳戶之使用者核准該請求。

當處理程序600判定使用者核准未得以鑑認時，處理程序600結束。當處理程序600判定使用者核准得以鑑認時，處理程序600將請求裝置新增(在680處)至同步圈。在一些實施例中，處理程序600藉由以下步驟而將裝置B新增至同步圈420：將唯一地識別裝置B之資料新增至同步圈420之同步圈裝置清單；用裝置A之裝置簽署金鑰對之私用金鑰來產生同步圈裝置清單之簽名；及將所產生之簽名與裝置簽名一起儲存於儲存器425中。

最後，處理程序600將經指定為在位於同步圈420中之裝置之間被同步的金鑰鏈與裝置B同步(在690處)。在一些實施例中，處理程序600使用下文藉由參看**圖7**至**圖15**所描述之技術來使金鑰鏈同步。

雖然**圖6**說明在同步圈中之一個裝置核准該請求後便將一請求裝置新增至同步圈，但一般熟習此項技術者將理解，在不同實施例中可使用任何數目之不同核准要求。例如，在可將請求裝置新增至同步圈之前，一些實施例可需要同步圈中之所有裝置、已定義數目之裝置、已定義百分數之裝置等核准該裝置。

一些實施例允許自同步圈移除一裝置。例如，若同步圈中之裝置之使用者懷疑同步圈中之另一裝置未被授權加入同步圈、使用者丟失同步圈中之裝置、同步圈中之裝置被偷走等，則使用者可自同步圈移除不良裝置。不同實施例不同地處置自同步圈之裝置移除。舉例而

言，在一些實施例中，當自同步圈移除裝置時，同步圈中之剩餘裝置繼續在該等剩餘裝置之間使密碼同步。在一些此等實施例中，需要所移除之裝置再次經歷註冊處理程序(例如，上文藉由參看**圖4**至**圖6**所描述之註冊處理程序)以便將裝置添回至同步圈中。按照另一方法，當自同步圈移除裝置時，毀壞該同步圈(例如，刪除同步圈裝置清單)。在此等狀況下，必須重新建立同步圈且將裝置新增至新近建立之同步圈(例如，使用上文參看**圖4**至**圖6**所描述之實例及處理程序)。

III.使密碼同步

一旦建立同步圈且至少兩個裝置被註冊至同步圈中，便使用一些實施例之方法以促進在經指定為同步圈之成員的裝置之間使金鑰鏈同步。如上文所註釋，在一些實施例中，方法利用P2P網路以在裝置之間傳達資料以便在裝置之間使金鑰鏈同步。

圖7概念地說明一實例資料流程，該資料流程透過**圖2**中所說明之網路架構以用於使密碼同步。具體言之，**圖7**概念地說明用於當在同步圈中之裝置中之一者上建立新密碼時在為同步圈之成員的裝置之間使密碼同步的資料流程操作1至9。在此實例中，使用類似於上文藉由參看**圖4**至**圖6**所描述之技術的技術來實施同步圈之建立及裝置A至C至同步圈中之註冊。

如所提及，**圖7**中所說明之網路架構類似於上文藉由參看**圖2**所描述之網路架構。亦即，裝置A至C中之每一者包括用於促進密碼之同步的金鑰鏈管理器205及用於儲存密碼之儲存器210。另外，裝置A至C經由具有充分連接之網狀拓撲的疊加網路來彼此通信，該網狀拓撲允許裝置A至C中之每一者直接與其他裝置中之每一者通信。在一些實施例中，對於每一對裝置A至C (亦即，裝置A與B、裝置A與C及裝置B與C)而言，裝置上之金鑰鏈管理器205促進在該對裝置之間供應用於在該等裝置之間輸送資料的一安全通信頻道(例如，使用OTR

傳訊、SSL等)。

在開始圖7中之資料流程操作1至9之前，使裝置A至C上之密碼同步。換言之，裝置A至C各自具有儲存於儲存器210中之相同密碼。藉由將密碼705新增(在被圈住之1處)至裝置A而開始資料流程。舉例而言，裝置A之使用者可已安裝一需要使用者鍵入與使用者之社群網路連接帳戶相關聯之使用者名稱及密碼的社群網路連接應用程式(例如，Facebook®應用程式、Twitter®應用程式、Google+®應用程式、LinkedIn®應用程式等)。

當裝置A接收到新密碼705時，裝置A加密及儲存(在被圈住之2處)密碼705於裝置A之儲存器210中。在一些實施例中，使用對稱金鑰演算法(資料加密標準(DES)演算法、三重資料加密演算法(TDEA)、使用256位元區塊大小之進階加密標準(AES)及伽羅瓦計數器模式(GCM)等)及金鑰(例如，供記錄至裝置中之密碼或通行碼、由裝置所產生或已指派的隨機金鑰等，或任何數目之此等金鑰之組合)來保護儲存於裝置A至C之儲存器210中的密碼。當裝置A將密碼705儲存於儲存器210中時，金鑰鏈管理器205使用對稱金鑰演算法及金鑰來加密該密碼。

在儲存密碼705之後，裝置A針對裝置B及C中之每一者來解密及加密(在被圈住之3處)密碼705。為解密儲存於儲存器210中之經加密密碼705，金鑰鏈管理器205使用上文所描述之對稱金鑰演算法及金鑰，該對稱金鑰演算法及該金鑰係用以在裝置A將密碼705儲存於儲存器210中時加密密碼705。

如上文所提及，在每一對裝置A至C之間使用一安全通信頻道來保護在該等裝置之間所輸送之資料。由於一對裝置A與B及一對裝置A與C各自使用分開之安全通信頻道，所以裝置A之金鑰鏈管理器205基於裝置A已與裝置B建立之安全通信頻道而使用第一金鑰或第一組金

鑰來加密待發送至裝置B之密碼705之複本。裝置A之金鑰鏈管理器205亦基於裝置A已與裝置C建立之安全通信頻道而使用一第二不同金鑰或第二組不同金鑰來加密待發送至裝置C之密碼705之另一複本。

作為一實例，在一些實施例中，裝置A與B之間的安全通信頻道及裝置A與C之間的安全通信頻道係各自使用OTR傳訊而實施。在一些此等實施例中，基於裝置A與B之公用/私用金鑰對而在裝置A與B之間建立OTR會話。另外，基於裝置A與B之公用/私用金鑰對而在裝置A與C之間建立另一分開之OTR會話。在一些實施例中，如上文藉由參看**圖4**至**圖6**所描述，裝置簽署金鑰對係所產生之用於將裝置A至C註冊至同步圈中之相同裝置簽署金鑰對。

一旦裝置A之金鑰鏈管理器205針對裝置B而加密密碼705之複本，裝置A便經由建立於裝置A與B之間的安全通信頻道而將密碼705之經加密複本及描述密碼705之後設資料發送(在被圈住之4處)至裝置B。用於描述密碼705之後設資料之實例包括密碼之類型(網際網路密碼、應用程式密碼、網路密碼等)、應用程式或網站(密碼與該應用程式或網站相關聯或密碼被用於該應用程式或網站)之名稱、應用程式或網站之路徑等。

當裝置B接收到密碼705之經加密複本時，裝置B藉由使用針對與裝置A建立之安全通信頻道所產生之一金鑰或一組金鑰來解密(在被圈住之5處)密碼705之複本。在解密密碼705之複本後，裝置B便加密及儲存(在被圈住之6處)密碼705之複本於裝置B之儲存器210中。裝置B現更新有密碼705且因此儲存於裝置B上之密碼得以與儲存於裝置A上之密碼同步。

轉至用於在裝置A與C之間使密碼同步的資料流程操作，在裝置A之金鑰鏈管理器205針對裝置C而加密密碼705之複本之後，裝置A經由建立於裝置A與C之間的安全通信頻道而將密碼705之經加密複本及

描述密碼705之後設資料發送(在被圈住之7處)至裝置C。在一些實施例中，由裝置A與密碼705之經加密複本一起被發送至裝置B的後設資料為裝置A發送至裝置C之相同後設資料。

在接收到密碼705之經加密複本後，裝置C便藉由使用針對與裝置A建立之安全通信頻道所產生之一金鑰或一組金鑰來解密(在被圈住之8處)密碼705之複本。當裝置C已解密密碼705之複本時，裝置C接著加密及儲存(在被圈住之9處)密碼705之複本於裝置C之儲存器210中。裝置C現更新有密碼705且因此儲存於裝置C上之密碼得以與儲存於裝置A上之密碼同步。

圖8及**圖9**概念地說明一實例資料流程，該資料流程透過**圖3**中所說明之網路架構以用於使密碼同步。詳言之，**圖8**及**圖9**概念地說明用於當在同步圈中之裝置中之一者上建立新密碼時在為同步圈之成員的裝置之間使密碼同步的資料流程操作1至11。**圖8**概念地說明回應於建立於裝置C上之新密碼而執行之資料流程操作1至8，該等操作1至8用於在裝置B離線時在裝置C與A之間使密碼同步。**圖9**概念地說明裝置B變成在線且使裝置B之密碼與裝置C及A同步。在此實例中，使用類似於上文藉由參看**圖4**至**圖6**所描述之技術的技術來實施同步圈之建立及裝置A至C至同步圈中之註冊。

如所提及，**圖8**及**圖9**中所說明之網路架構類似於上文藉由參看**圖3**所描述之網路架構。亦即，裝置A至C中之每一者包括用於促進密碼之同步的金鑰鏈管理器205及用於儲存密碼之儲存器210。又，裝置A至C經由具有星形拓撲之疊加網路來彼此通信，該星形拓撲允許裝置A—中之每一者間接地經由雲端服務305來與其他裝置中之每一者通信，該雲端服務305充當星形拓撲之中心且提供用於儲存資料之雲端儲存服務。一些實施例之雲端服務305將同步圈之名稱及同步圈裝置清單儲存於儲存器310中、將用於鑑認裝置之使用者的使用者簽名

儲存於儲存器315中、將用於鑑認同步圈中之裝置的裝置簽名儲存於儲存器320中、將用於在位於同步圈中之裝置之間使金鑰鏈同步的金鑰鏈資料儲存於儲存器325中及將其他資料儲存於儲存器330中。另外，在一些實施例中，對於每一對裝置A至C (亦即，裝置A與B、裝置A與C及裝置B與C)而言，裝置上之金鑰鏈管理器205在該對裝置之間建立一安全通信頻道(例如，使用OTR傳訊、SSL等)，該對裝置經由該安全通信頻道來通信。在此實例資料中，裝置A至C將雲端服務305用作用於輸送通信之構件。

在開始**圖8**及**圖9**中之資料流程操作1至11之前，使裝置A至C上之密碼同步。亦即，裝置A至C各自具有儲存於儲存器210中之相同密碼。另外，資料流程藉由將密碼805新增(在被圈住之1處)至裝置C而開始。例如，裝置C之使用者可已安裝一需要使用者鍵入與使用者之社群網路連接帳戶相關聯之使用者名稱及密碼的社群網路連接應用程式(例如，Facebook®應用程式、Twitter®應用程式、Google+®應用程式、LinkedIn®應用程式等)。

當裝置C接收到新密碼805時，裝置C加密及儲存(在被圈住之2處)密碼805於裝置C之儲存器210中。在一些實施例中，使用對稱金鑰演算法(資料加密標準(DES)演算法、三重資料加密演算法(TDEA)等)及金鑰(例如，供記錄至裝置中之密碼或通行碼、由裝置所產生或已指派的隨機金鑰等，或任何數目之此等金鑰之組合)來保護儲存於裝置A至C之儲存器210中的密碼。當裝置A將密碼805儲存於儲存器210中時，金鑰鏈管理器205使用對稱金鑰演算法及金鑰來加密該密碼805。

在儲存密碼805之後，裝置C針對裝置A及C中之每一者而解密及加密(在被圈住之3處)密碼805。為解密儲存於儲存器210中之經加密密碼805，金鑰鏈管理器205使用上文所描述之對稱金鑰演算法及金

鑰，該對稱金鑰演算法及該金鑰係用以在裝置C將密碼805儲存於儲存器210中時加密密碼805。

如上文所註釋，在每一對裝置A至C之間使用一安全通信頻道來保護在該等裝置之間所輸送之資料。由於一對裝置A與B及一對裝置A與C各自使用分開之安全通信頻道，所以裝置A之金鑰鏈管理器205基於裝置A已與裝置B建立之安全通信頻道而使用第一金鑰或第一組金鑰來加密待發送至裝置B之密碼805之複本。裝置A之金鑰鏈管理器205亦基於裝置A已與裝置C建立之安全通信頻道而使用第二不同金鑰或第二組不同金鑰來加密待發送至裝置C之密碼805之另一複本。

例如，在一些實施例中，裝置C與A之間的安全通信頻道及裝置C與B之間的安全通信頻道係各自使用OTR傳訊而實施。在一些此等實施例中，基於裝置C及A之裝置簽署公用/私用金鑰對而在裝置C與A之間建立OTR會話。另外，基於裝置C及B之裝置簽署公用/私用金鑰對而在裝置C與B之間建立另一分開之OTR會話。如上文藉由參看**圖4**至**圖6**所描述，一些實施例之裝置簽署金鑰對係所產生之用於將裝置A至C註冊至同步圈中之相同裝置簽署金鑰對。

一旦裝置C之金鑰鏈管理器205針對裝置A而加密密碼805之複本且針對裝置B而加密密碼805之另一複本，裝置C便將密碼805之該等經加密複本及描述密碼805之後設資料儲存於雲端服務305之儲存器325中。用於描述密碼805之後設資料之實例包括密碼之類型(網際網路密碼、應用程式密碼、網路密碼等)、應用程式或網站(密碼與該應用程式或網站相關聯或密碼被用於該應用程式或網站)之名稱、應用程式或網站之路徑等。

如上文所解釋，在一些實施例中，儲存器310至330被實施為金鑰值儲存器。用於藉由一意欲用於接收裝置之發送裝置而被儲存於雲端服務305 (例如，儲存器325)中之資料的一些實施例之金鑰係以下各

者之級聯體：第一裝置及第二裝置所屬之同步圈之名稱、發送裝置之識別符及接收裝置之識別符。在一些實施例中，接收裝置向此金鑰值對註冊使得當該金鑰值對之值藉由發送裝置而改變時(例如，值被新增、修改、刪除等)，雲端服務305通知該接收裝置(例如，經由推送通知服務)。

按照此方法，當雲端服務305自裝置C接收到密碼805之複本及用於裝置A之其對應後設資料時，雲端服務305將該資料作為以上文所描述之方式所形成之金鑰之值而儲存(在被圈住之5處)於儲存器325中。雲端服務305接著向裝置A通知(例如，經由推送通知服務)與所改變之金鑰相關聯的值(例如，在此實例中資料被新增)。類似地，當雲端服務305自裝置C接收到密碼805之複本及用於裝置B之其對應後設資料時，雲端服務305將該資料作為以上文所描述之方式所形成之金鑰之值而儲存(在被圈住之5處)於儲存器325中。雲端服務305接著向裝置B通知(例如，經由推送通知服務)與所改變之金鑰相關聯的值(例如，在此實例中資料被新增)。由於在**圖8**中將裝置B展示為離線，所以在此實例中裝置B仍不接收通知。

繼續**圖8**，當裝置A自雲端服務305接收到通知時，裝置A使用裝置C用以將經加密密碼805之複本及後設資料儲存於雲端服務305中之相同金鑰來擷取(在被圈住之6處)經加密密碼805之複本及相關聯之後設資料。一旦裝置A擷取到密碼資料，裝置A便藉由使用針對與裝置C建立之安全通信頻道所產生之一金鑰或一組金鑰來解密(在被圈住之7處)密碼805之複本。在解密密碼805之複本後，裝置A便加密及儲存(在被圈住之8處)密碼805之複本於裝置A之儲存器210中。此時，裝置A更新有密碼805且因此儲存於裝置A上之密碼得以與儲存於裝置C上之密碼同步。

如**圖9**中所說明，裝置B現已在線。當雲端服務305偵測到裝置B

在線時，雲端服務305將通知發送至裝置B，該通知指示與用於自裝置C接收資料之金鑰值對相關聯的值被改變(例如，在此實例中資料被新增)。

當裝置B自雲端服務305接收到通知時，裝置B使用裝置C用以將經加密密碼805之複本及後設資料儲存於雲端服務305中之相同金鑰來擷取(在被圈住之9處)經加密密碼805之複本及相關聯之後設資料。在裝置B擷取到密碼資料之後，裝置B藉由使用針對與裝置C建立之安全通信頻道所產生之一金鑰或一組金鑰來解密(在被圈住之10處)密碼805之複本。

在裝置B解密密碼805之複本之後，裝置B加密及儲存(在被圈住之11處)密碼805之複本於裝置B之儲存器210中。此時，裝置B更新有密碼805且因此儲存於裝置B上之密碼得以與儲存於裝置C上之密碼同步。

雖然以基於**圖7**至**圖9**中所示之被圈住數字之數字次序的特定次序來描述**圖7**至**圖9**中之資料流程操作，但一般熟習此項技術者將認識到，被圈住數字未必表示資料流程操作之次序且資料流程操作可以眾多不同次序出現。例如，在一些實施例中，**圖7**中所說明之一組順序資料流程操作4至6及一組順序資料流程操作7至9係彼此獨立地出現。類似地，**圖8**及**圖9**中所示之一組順序資料流程操作6至8及一組順序資料流程操作9至11係彼此獨立地出現。

A. 金鑰鏈資料結構

如上文所提及，在一些實施例中，金鑰鏈為可包括密碼、私用金鑰、證書、安全註釋等之已定義之資料集合。在一些實施例中，金鑰鏈管理器產生及儲存用以表示金鑰鏈之一資料結構。**圖10**概念地說明如藉由一些實施例之金鑰鏈管理器所儲存之金鑰鏈的資料結構1005。如所示，資料結構1005包括金鑰鏈ID 1010、金鑰鏈項目1至N

及存取資料1015。金鑰鏈ID 1010為用於識別金鑰鏈1005之唯一識別符。存取資料1015係用於控制對金鑰鏈1005自身之存取(例如，什麼應用程式可存取金鑰鏈1005及/或可在金鑰鏈1005上執行什麼操作(例如，讀取、寫入、刪除等)等)且在結構方面類似於下文所描述之存取資料1035。

一些實施例之金鑰鏈項目表示一個別資料片(例如，密碼、金鑰、證書等)。如**圖10**中所示，金鑰鏈項目1020表示金鑰鏈1005之金鑰鏈項目1。金鑰鏈項目1020包括金鑰鏈項目ID 1025、資料1030、屬性1至M、存取資料1035 (亦稱作存取物件)。金鑰鏈項目ID 1025為用於識別金鑰鏈項目1020之唯一識別符。

資料1030為金鑰鏈項目1020之一及/或多個實際資料值。例如，若金鑰鏈1020表示密碼，則資料1030儲存該密碼之值(例如，文數字字符串)。在一些實施例中，當金鑰鏈管理器儲存某些類型之金鑰鏈項目(例如，密碼、私用金鑰等)之資料時，金鑰鏈管理器加密該資料。對於其他類型之金鑰鏈項目(例如，證書)之資料而言，金鑰鏈管理器僅儲存該資料而不加密該資料。

金鑰鏈項目1020之屬性1至M係用於儲存描述金鑰鏈項目1020之後設資料。不同類型之金鑰鏈項目具有不同組屬性。舉例而言，網際網路密碼具有包括諸如以下各者之屬性的屬性：安全域、協定類型(例如，超文字傳送協定(HTTP)、超文字傳送協定安全(HTTPS)、檔案傳送協定(FTP)等)、路徑(例如，網際網路資源之統一資源定位器(URL))等。

在一些實施例中，每一金鑰鏈項目包括一日期欄位屬性，該日期欄位屬性指示對金鑰鏈項目之最近修改的時間及日期(亦稱作時間戳)。在一些實施例中，每一金鑰鏈項目亦包括用於指定該金鑰鏈項目為已被刪除之一金鑰鏈項目(亦稱作標記刪除(tombstone))的屬性。

當該屬性指定金鑰鏈項目為標記刪除時，金鑰鏈管理器保持該金鑰鏈項目之資料欄位，但金鑰鏈管理器將金鑰鏈項目之資料1030之值設定至零點或空白值。在一些實施例中，由對相衝突之金鑰鏈項目之解析所產生的金鑰鏈項目包括一組屬性，該組屬性包括：(1)一旗標，其指示該金鑰鏈項目為衝突解析之結果；(2)用以解析衝突之衝突解析器之版本號；及(3)相衝突之金鑰鏈項目(亦稱作父代金鑰鏈項目)，該金鑰鏈項目係自該等相衝突之金鑰鏈項目解析而得。在一些實施例中，將該組屬性稱作金鑰鏈項目之衝突解析後設資料。

在一些實施例中，將金鑰鏈項目之屬性或屬性之子集用作用於唯一地識別該金鑰鏈項目之主金鑰。亦即，具有相同主金鑰之兩個金鑰鏈項目被視為相同之金鑰鏈項目(而不管該等金鑰鏈項目之資料之值是否相同)。

存取資料1035係用於控制對金鑰鏈項目1020之存取。如所說明，存取資料1035包括用於控制對金鑰鏈項目1020之存取的存取控制清單(ACL)輸入項目1至K。**圖10**說明一表示存取資料1035之ACL輸入項目1的ACL輸入項目1040。ACL輸入項目1040包括指定可對金鑰鏈項目1020執行之操作(例如，讀取、寫入、刪除、解密、鑑認等)的授權標籤1045。在此實例中，授權標籤1045包括授權標籤1至H。

另外，ACL輸入項目1040包括受信任應用程式1050之清單。如所示，受信任應用程式1050之清單包括應用程式ID 1至J。每一應用程式ID係用於識別可在無使用者授權的情況下執行由授權標籤1045所指定之操作之特定應用程式的一唯一識別符。

一般熟習此項技術者將認識到，金鑰鏈資料結構1050僅為金鑰鏈管理器可使用以儲存金鑰鏈之所需資訊的一個可能之資料結構。舉例而言，不同實施例可儲存額外或較少之資訊、以不同次序儲存資訊等。

B. 使金鑰鏈項目同步

如上文所解釋，一些實施例之同步圈中之裝置藉由使一金鑰鏈之個別金鑰鏈項目同步而在裝置之間使該金鑰鏈同步。**圖11**概念地說明一狀態圖1100，該狀態圖1100描述一些實施例之金鑰鏈管理器之不同狀態及在此等狀態之間的轉變。一般熟習此項技術者將認識到，在一些實施例中，金鑰鏈管理器將具有關於所有不同類型之輸入事件的許多不同狀態，且狀態圖1100係具體地集中於此等事件之子集。詳言之，狀態圖1100描述用於將密碼與為同步圈之成員之裝置同步之輸入事件及相關狀態。為描述**圖11**，其上正運行有金鑰鏈管理器之裝置將被稱作本端裝置。

當金鑰鏈管理器不處理用於使金鑰鏈同步之任何事件時，金鑰鏈管理器處於穩定狀態1105。在狀態1105中，金鑰鏈管理器可執行與使金鑰鏈同步無關之其他操作。例如，金鑰鏈管理器可執行註冊操作以接受、否認及/或確認加入同步圈之請求。

在自同步圈中之同級裝置接收到資訊清單摘要後，金鑰鏈管理器便轉變至狀態1110以處理資訊清單摘要請求。在一些實施例中，資訊清單摘要係同級裝置之當前金鑰鏈項目之清單。一些實施例之金鑰鏈管理器儲存同步圈中之每一同級裝置之資訊清單歷史。

在狀態1110下，金鑰鏈管理器藉由將本端裝置針對同級裝置之歷史中的最近資訊清單與自同級裝置接收之資訊清單摘要相比較而產生對資訊清單摘要之回應。若該等資訊清單匹配且本端裝置具有與同級裝置之資訊清單摘要中之金鑰鏈項目相同的金鑰鏈項目，則金鑰鏈管理器產生一指示本端裝置得以與同級裝置同步的訊息。

若本端裝置針對同級裝置之歷史中的最近資訊清單匹配自同級裝置資訊清單接收之資訊清單摘要，但本端裝置具有一組不同之金鑰鏈項目(與同級裝置之資訊清單摘要中之金鑰鏈項目相比)，則金鑰鏈

管理器產生包括差異資訊清單之一訊息。在一些實施例中，差異資訊清單包括：(1)本端裝置之金鑰鏈項目與在同級裝置之資訊清單中所列舉之金鑰鏈項目之間的差異之清單；及(2)清單中之對應金鑰鏈項目的資料。差異資訊清單可包括未被包括於同級裝置之資訊清單摘要中之金鑰鏈項目及/或為相同(例如，具有相同之主金鑰)但具有不同資料值之金鑰鏈項目。

當本端裝置針對同級裝置之歷史中的最近資訊清單及自同級裝置接收之資訊清單摘要不匹配時，金鑰鏈管理器產生包括本端裝置之完整資訊清單的一訊息。在一些實施例中，一完整資訊清單包括：(1)本端裝置之所有金鑰鏈項目之清單；(2)清單中之對應金鑰鏈項目的資料。在處理來自同級裝置之資訊清單摘要後，金鑰鏈管理器便將所產生之回應發送至同級裝置且轉變回至穩定狀態1105。

當處於穩定狀態1105時，若金鑰鏈管理器接收到本端金鑰鏈之改變，則金鑰鏈管理器進行至狀態1115以處理本端金鑰鏈之該改變。在狀態1115下，金鑰鏈管理器用該改變來更新本端金鑰鏈。在一些實施例中，金鑰鏈可包括經指定用於與同步圈中之同級裝置同步的金鑰鏈項目及非用於與同步圈中之同級裝置同步的金鑰鏈項目。若本端金鑰鏈之改變不影響經指定用於與同步圈中之同級裝置同步的任何金鑰鏈項目，則金鑰鏈管理器返回至穩定狀態1105。否則，金鑰鏈管理器轉變至狀態1120以使金鑰鏈項目同步，該等金鑰鏈項目(1)經指定用於與同步圈中之同級裝置同步；及(2)受本端金鑰鏈之改變的影響。

在狀態1120下，金鑰鏈管理器將對本端裝置之金鑰鏈之更新發送至同步圈中之同級裝置中之每一者。在一些實施例中，金鑰鏈管理器執行下文藉由參看**圖12**所描述之處理程序1200以將更新發送至同級裝置。在金鑰鏈管理器將更新發送至同級裝置之後，金鑰鏈管理器返回至穩定狀態1105。

當金鑰鏈管理器處於穩定狀態1105且自同步圈中之同級裝置接收到一完整資訊清單時，金鑰鏈管理器轉變至狀態1125以處理該完整資訊清單。在一些實施例中，金鑰鏈管理器藉由產生一差異資訊清單來處理該完整資訊清單，該差異資訊清單包括：(1)本端裝置之金鑰鏈項目與在同級裝置之完整資訊清單中所列舉之金鑰鏈項目之間的差異之清單；及(2)清單中之對應金鑰鏈項目的資料。若差異資訊清單為空白(亦即，本端裝置具有與在同級裝置之完整資訊清單中所列舉之金鑰鏈項目相同的金鑰鏈項目)，則金鑰鏈管理器將一指示如此情況之訊息發送至同級裝置且接著返回至穩定狀態1105。若差異資訊清單非空白，則金鑰鏈管理器將差異資訊清單發送至同級裝置且接著返回至穩定狀態1105。

在穩定狀態1105下，若金鑰鏈管理器自同級裝置接收到用於更新本端裝置之金鑰鏈的一差異資訊清單，則金鑰鏈管理器轉變至狀態1135以將來自同級裝置之更新應用至本端裝置之金鑰鏈。在一些實施例中，金鑰鏈管理器執行下文藉由參看**圖13**所描述之處理程序1300以將來自同級裝置之更新應用至本端裝置之金鑰鏈。一旦金鑰鏈管理器將同級裝置之更新應用至本端金鑰鏈，金鑰鏈管理器便將同級裝置之更新應用至本端裝置針對同級裝置之歷史中的最近資訊清單、將經修改之資訊清單儲存於本端裝置針對同級裝置之資訊清單的歷史中。金鑰鏈管理器接著將本端裝置針對同級裝置之歷史中的最近資訊清單(其為金鑰鏈管理器剛才儲存之資訊清單)與本端裝置之當前金鑰鏈項目資訊清單相比較。

若該等資訊清單匹配但本端裝置具有一組不同之金鑰鏈項目(與同級裝置之資訊清單摘要中之金鑰鏈項目相比)，則金鑰鏈管理器轉變至狀態1140且排程待發送至同步圈中之同級裝置的更新。否則，金鑰鏈管理器返回至穩定狀態1105。

在狀態1140中，金鑰鏈管理器檢查是否留有待處理之來自同級裝置之任何更新。若如此，則金鑰鏈管理器轉變至狀態1135以繼續處理來自同級裝置之用於更新本端金鑰鏈的任何差異資訊清單。若不存在來自同級裝置之待處理之更新，則金鑰鏈管理器自狀態1140轉變至狀態1145以將經排程之更新發送至同步圈中之同級裝置。在一些實施例中，金鑰鏈管理器執行下文藉由參看**圖12**所描述之處理程序1200以將更新發送至同級裝置。一旦金鑰鏈管理器將所有經排程之更新發送至同級裝置，金鑰鏈管理器便返回至穩定狀態1105。

圖12概念地說明用於將更新推送至同級裝置之一些實施例之處理程序1200。在一些實施例中，本申請案中所描述之金鑰鏈管理器執行處理程序1200以將被應用至本端裝置之本端金鑰鏈的更新發送至同步圈中之同級裝置。例如，當金鑰鏈管理器處於上文藉由參看**圖11**所描述之狀態1120及1145時，金鑰鏈管理器執行處理程序1200。

處理程序1200藉由識別(在1210處)同步圈中之同級裝置而開始。在一些實施例中，處理程序1200藉由存取同步裝置清單之本端複本來識別同級裝置，而在其他實施例中，處理程序1200藉由存取儲存於雲端服務305中(例如，在儲存器310中)之同步裝置清單來識別同級裝置。

接下來，處理程序1200判定(在1220處)本端裝置之資訊清單是否匹配同級裝置之資訊清單。在一些實施例中，處理程序1200將本端裝置針對同級裝置之歷史中的最近資訊清單用作同級裝置之資訊清單。當處理程序1200判定該等資訊清單匹配時，處理程序1200進行至1260。否則，處理程序1200繼續至1230。

在1230處，處理程序1200基於本端裝置及同級裝置之資訊清單而產生一差異資訊清單。如上文所描述，在一些實施例中，差異資訊清單包括：(1)本端裝置之金鑰鏈項目與在同級裝置之資訊清單中所

列舉之金鑰鏈項目之間的差異之清單；及(2)清單中之對應金鑰鏈項目的資料。在一些實施例中，處理程序1200藉由以下步驟而產生差異資訊清單：(1)比較本端裝置之金鑰鏈中之金鑰鏈項目與在同級裝置之資訊清單中所列舉之金鑰鏈項目；及(2)識別該等差異。

處理程序1200接著使用用於同級裝置之該加密金鑰或該組加密金鑰來加密(在1240處)在差異資訊清單中所指定之本端金鑰鏈項目之複本。如上文所解釋，在一些實施例中，在同步圈中之每一對裝置之間使用一安全通信頻道。因而，處理程序1210識別針對用以與同級裝置通信之安全通信頻道所建立之該金鑰或該組金鑰且使用該所識別之金鑰或該組所識別之金鑰來加密本端金鑰鏈項目之複本。

接下來，處理程序1200經由安全通信頻道將經加密之金鑰鏈項目及差異資訊清單發送(在1250處)至同級裝置。一旦處理程序1200將資訊發送至同級裝置，處理程序1200便接著判定(在1260處)是否留有待處理之同步圈中之任何同級裝置。當處理程序1200判定存在留有待處理之同級裝置時，處理程序1200返回至1210以繼續將被應用至本端金鑰鏈之更新發送至同步圈中之剩餘之同級裝置。當處理程序1200判定不存在留有待處理之同級裝置時，處理程序1200接著結束。

圖13概念地說明用於處理來自同級裝置之更新之一些實施例之處理程序1300。在一些實施例中，本申請案中所描述之金鑰鏈管理器執行處理程序1300以將來自同級裝置之更新應用至本端裝置之本端金鑰鏈。舉例而言，當金鑰鏈管理器處於上文藉由參看**圖11**所描述之狀態1135時(例如，當金鑰鏈管理器自同級裝置接收到待處理之差異資訊清單時)，金鑰鏈管理器執行處理程序1300。

處理程序1300藉由識別(在1310處)在自同級裝置接收之差異資訊清單中所指定之經更新之金鑰鏈項目而開始。接下來，處理程序1300解密(在1320處)經更新之金鑰鏈項目。如上文所標註，在一些實施例

中，在同步圈中之每一對裝置之間使用一安全通信頻道。因此，處理程序1310識別針對用以與同級裝置通信之安全通信頻道所建立的該金鑰或該組金鑰且使用該所識別之金鑰或該組所識別之金鑰來解密經更新之金鑰鏈項目。

處理程序1300接著識別(在1330處)經更新之金鑰鏈項目之主金鑰。如上文所解釋，在一些實施例中，將金鑰鏈項目之屬性或屬性之子集用作用於唯一地識別該金鑰鏈項目之主金鑰。

接下來，處理程序1320判定(在1340處)本端金鑰鏈中之金鑰鏈項目是否具有與經更新之金鑰鏈項目之主金鑰相同的主金鑰。當處理程序1300判定本端金鑰鏈中無金鑰鏈項目具有與經更新之金鑰鏈項目之主金鑰相同的主金鑰時，處理程序1300將經更新之金鑰鏈項目應用(在1350處)至本端金鑰鏈。在一些實施例中，處理程序1300藉由將經更新之金鑰鏈新增至本端金鑰鏈而將經更新之金鑰鏈項目應用至本端金鑰鏈。

當處理程序1300判定本端金鑰鏈中之金鑰鏈項目具有與經更新之金鑰鏈項目之主金鑰相同的主金鑰時，處理程序1300解析(在1360處)經更新之金鑰鏈項目與本端金鑰鏈項目之間的衝突且將衝突解析之結果應用至本端金鑰鏈。不同實施例之處理程序1300不同地解析相衝突之金鑰鏈項目之間的衝突。下文藉由參看**圖15**來描述一種此方法。

C. 解析金鑰鏈項目衝突

當使金鑰鏈項目同步時，一些實施例之金鑰鏈管理器可偵測相同金鑰鏈項目之多個版本之間的衝突。在不同實施例中，金鑰鏈管理器使用不同技術來解析金鑰鏈項目衝突。舉例而言，在一些實施例中，方法將金鑰鏈項目之最近版本用作待在裝置之間被同步之金鑰鏈項目。在一些實施例中可使用額外及/或不同方法。

在一些實施例中，裝置可更新其之衝突解析處理程序(亦稱作「衝突解析器」)。在一些例子中，經更新之處理程序及較早、非經更新之處理程序在判定應使用哪些金鑰鏈項目值時提供不同結果。在一些實施例中，同步圈中之一或多個裝置有可能正使用經更新之衝突解析處理程序，而相同同步圈中之一或多個其他裝置正使用衝突解析處理程序之先前版本。**圖14**概念地說明用於解析相衝突之衝突解析器之一些實施例之處理程序1400。在一些實施例中，上文藉由參看**圖13**所描述之處理程序1300執行處理程序1400以實施操作1360。

處理程序1400藉由識別(在1410處)相衝突之金鑰鏈項目之衝突解析後設資料而開始。如上文所註釋，一些實施例之衝突解析後設資料包括：(1)一旗標，其指示金鑰鏈項目為衝突解析之結果；(2)用以解析衝突之衝突解析器之版本號；及(3)相衝突之金鑰鏈項目(亦稱作父代金鑰鏈項目)，該金鑰鏈項目係自該等相衝突之金鑰鏈項目解析而得。

接下來，處理程序1400判定(在1420處)經更新之金鑰鏈項目之衝突解析器是否與本端金鑰鏈項目之衝突解析器相衝突。在一些實施例中，當發生以下各者時，經更新之金鑰鏈項目及本端金鑰鏈項目之衝突解析器相衝突：(1)兩個金鑰鏈項目包括一指示金鑰鏈項目為衝突解析之結果的旗標；(2)經更新之金鑰鏈項目及本端金鑰鏈項目被指定為經更新之金鑰鏈項目之父代金鑰鏈項目；及(3)用以解析經更新之金鑰鏈項目之衝突解析器之版本號不與本端裝置之衝突解析器之版本號相同。

當處理程序1400判定該等衝突解析器不相衝突時，處理程序1400用本端裝置之衝突解析器來解析(在1430處)金鑰鏈項目衝突且接著處理程序1400結束。當處理程序1400判定該等衝突解析器相衝突時，處理程序1400判定(在1450處)是否將使用本端裝置之衝突解析

器。當本端衝突解析器之版本號大於用以解析經更新之金鑰鏈項目之衝突解析器之版本號時，處理程序1400用本端裝置之衝突解析器來解析(在1430處)金鑰鏈項目衝突。否則，處理程序1400將經更新之金鑰鏈項目用作(在1430處)對金鑰鏈項目衝突之解析。處理程序1400接著結束。

圖15概念地說明用於解析金鑰鏈項目衝突之一些實施例之處理程序1500。在一些實施例中，上文藉由參看**圖14**所描述之處理程序1400執行處理程序1500以實施操作1460。

處理程序1500藉由識別(在1510處)相衝突之經更新之金鑰鏈項目與本端金鑰鏈項目之時間戳而開始。如上文所註釋，在一些實施例中，金鑰鏈項目之資料結構包括一指示對該金鑰鏈項目之最近修改之時間及日期的資料欄位。在一些實施例中，處理程序1500藉由存取每一金鑰鏈項目之日期欄位屬性來識別時間戳。

接下來，處理程序1500判定(在1520處)經更新之金鑰鏈項目之時間戳是否係較近的。當處理程序1500判定經更新之金鑰鏈項目之時間戳係較近時，處理程序1500用經更新之金鑰鏈項目來更新(在1540處)本端金鑰鏈項目且接著處理程序1500結束。當處理程序1500判定經更新之金鑰鏈項目之時間戳非係較近時，處理程序1500用本端金鑰鏈項目來更新(在1530處)本端金鑰鏈項目且接著處理程序1500結束。

IV. 將資料保護域用於金鑰鏈

本發明之一些實施例提供用於根據若干組已定義之條件及/或要求來限制對裝置上之金鑰鏈資料(例如，金鑰鏈項目)之存取的一資料保護特徵。在一些實施例中，定義若干不同保護域(亦稱作資料保護類別)且裝置上之每一金鑰鏈項目屬於該等已定義之保護域中之一者。每一保護域與一組條件相關聯。當針對一特定資料保護域而滿足一組條件時，裝置中之屬於該特定保護域的金鑰鏈項目變得可用於供

該裝置使用。

A. 資料保護域

圖16概念地說明不同裝置中之不同金鑰鏈項目。具體言之，此圖說明屬於不同保護域之金鑰鏈項目根據裝置針對該等不同保護域所滿足之條件而變得可用。此圖說明源裝置1605與1610、目的地裝置1615至1635及金鑰鏈項目S1至S3與C4至C5。

在一些實施例中，保護域係預定義型且被提供至裝置以作為該等裝置之作業系統(例如，iOS™、Windows™等)之部分。由此等作業系統所管理之裝置可藉由以下步驟來利用保護域以保護金鑰鏈項目：使該等裝置中之金鑰鏈項目僅在滿足與該等保護域相關聯之條件之後才變成可用。在本專利申請案中，將此等預定義型保護域稱作系統保護域。

在一些實施例中，可由裝置之使用者或運行於裝置上之應用程式之開發商來自定義保護域。在此等實施例中，裝置或作業系統之製造商向使用者提供一工具使得使用者可藉由定義用於自定義型保護域之不同組條件來定義該等保護域。又，裝置或作業系統之製造商向開發商提供軟體開發套件(SDK)使得開發商可藉由針對開發商撰寫以運行於裝置上之應用程式而定義用於自定義型保護域之不同組條件來定義該等保護域。

如上文所提及，不同保護域與不同組條件或要求相關聯。在一些實施例中，可定義保護域從而為某些金鑰鏈項目提供額外安全性等級。亦即，第一保護域之條件係第二保護域之條件的子集使得屬於第二保護域之金鑰鏈項目僅在裝置滿足第二保護域之額外條件(位於第一保護域之條件頂部)的情況下才變得可用於該等裝置。例如，第一保護域之條件包括裝置被啟動及運行且第二保護域之條件包括裝置被解除鎖定以及被啟動及運行。

在一些實施例中，可定義保護域以具有可重疊或可不重疊之不同組條件。例如，第一保護域之條件可包括在裝置被解除鎖定之後的額外鑑認(例如，額外密碼)。第二保護域之條件可包括一特定應用程式在裝置中之存在。第一保護及第二保護之此等條件不重疊。

在此實例中，源裝置1605為將經更新之金鑰鏈項目S1至S3推送至目的地裝置1615至1625的裝置。如所示，裝置1605中之金鑰鏈項目S1至S3分別屬於保護域1至3。在此實例中，保護域1至3為系統保護域。保護域1至3將不同安全性等級提供至金鑰鏈項目。在此實例中，保護域3之條件係保護域2之條件的子集，且保護域2之條件係保護域1之條件的子集。

在此實例中，裝置1615至1625滿足不同組條件。具體言之，裝置1625滿足保護域3之所有條件。裝置1620滿足保護域2之所有條件。裝置1615滿足保護域1之所有條件。結果，金鑰鏈項目S3可用於供裝置1625之使用但金鑰鏈項目S1及S2不可用於供裝置1625之使用。金鑰鏈項目被說明為虛線平行四邊形以指示該等項目之不可用性。金鑰鏈項目S2及S3可用於供裝置1620之使用但金鑰鏈項目S1不可用於供裝置1620之使用。所有三個金鑰鏈項目S1至S3可用於供裝置1615之使用。

不同實施例使用使金鑰鏈項目不可用於供裝置之使用的不同方式。例如，一些實施例之裝置中之金鑰鏈管理器不解密金鑰鏈項目且藉此在裝置不滿足該金鑰鏈所屬之保護域之所有條件時使該金鑰鏈項目變成不可用。替代地或共同地，一些實施例之金鑰鏈管理器使金鑰鏈項目變得不可由運行於裝置中之應用程式存取直至該裝置滿足該金鑰鏈項目所屬之保護域之條件為止。在一些實施例中，目的地裝置之金鑰鏈管理器不接受自源裝置推送之金鑰鏈項目(除非在推送金鑰鏈的時候目的地裝置滿足該金鑰鏈項目所屬之保護域之條件)。

在此實例中，源裝置1610為將經更新之金鑰鏈項目C4及C5推送至目的地裝置1630至1635的裝置。如所示，裝置1610中之金鑰鏈項目C4及C5分別屬於保護域4及5。保護域4及5為自定義型保護域，其具有不同組條件。在此實例中，保護域4之條件不與保護域5之條件重疊。

在此實例中，裝置1630滿足保護域4之所有條件但不滿足保護域5之所有條件，而裝置1635滿足保護域5之所有條件但不滿足保護域4之所有條件。結果，金鑰鏈項目C4可用於供裝置1630之使用但金鑰鏈項目C5不可用於供裝置1630之使用。金鑰鏈項目C5可用於供裝置1635之使用但金鑰鏈項目C4不可用於供裝置1635之使用。

一般熟習此項技術者將認識到，一些實施例之保護域之使用並不限於保護金鑰鏈項目。可定義任何類型之資料以屬於不同保護域以便接收不同安全性等級。例如，可將一些實施例之第一裝置中所更新之文獻推送至第二裝置，但該文獻保持不可用於供第二裝置之使用直至第二裝置滿足該文獻所屬之保護域之所有條件為止。

圖17概念地說明一些實施例執行以處理金鑰鏈項目之處理程序1700。在一些實施例中，藉由一目的地裝置來執行處理程序1700，一或多個源裝置已將金鑰鏈項目推送至該目的地裝置。詳言之，在此等實施例中，目的地裝置之金鑰鏈管理器可執行處理程序1700。一些實施例之目的地裝置將來自源裝置之金鑰鏈項目存放於處理佇列中。下文將另外藉由參看**圖18**來描述一實例處理佇列。在一些實施例中，當目的地裝置被啟動且已自源裝置接收到一或多個金鑰鏈項目時，處理程序1700開始。

處理程序1700藉由自處理佇列擷取(在1710處)金鑰鏈項目而開始。在一些實施例中，該處理佇列為用於保存自源裝置推送之金鑰鏈項目的一儲存結構(例如，檔案系統)。在一些實施例中，源裝置使用

目的地裝置之公用金鑰來加密金鑰鏈項目中之資料(例如，密碼)，該公用金鑰先前由目的地裝置所公開。在此等實施例中，金鑰鏈項目在經加密時被儲存於處理佇列。

目的地裝置使用對應之私用金鑰(亦即，公用-私用金鑰對之私用金鑰，該公用-私用金鑰對包括源裝置用以加密金鑰鏈項目之公用金鑰)來解密金鑰鏈項目。在一些實施例中，目的地裝置針對裝置所支援之保護域中之每一者而產生公用-私用金鑰對。下文將另外藉由參看**圖25**及**圖26**來描述關於用於不同保護域之金鑰對的更多細節。

處理程序1700接著識別(在1720處)所擷取之金鑰鏈項目之保護域。在一些實施例中，金鑰鏈項目亦包括用於識別該金鑰鏈項目所屬之保護域的一識別符或與用於識別該金鑰鏈項目所屬之保護域的一識別符相關聯。在一些實施例中，源裝置用以加密金鑰鏈項目中之資料的公用金鑰充當保護域識別符。處理程序1700讀取金鑰鏈項目之保護域識別符以識別所擷取之金鑰鏈項目所屬的保護域。

接下來，處理程序1700判定(在1730處)所識別之保護域是否可用。亦即，處理程序1700判定目的地裝置是否已滿足所識別之保護域之所有條件。在一些實施例中，目的地裝置獲得該等條件之定義以作為裝置之作業系統之部分。替代地或共同地，一些實施例之目的地裝置可在該目的地裝置及源裝置建立包括該目的地裝置及該源裝置之一同步圈時獲得該等條件之定義。

當處理程序1700判定(在1730處)並不滿足所識別之保護域之所有條件時，處理程序1700藉由將金鑰鏈項目存放回至佇列中而將金鑰鏈項目傳回(在1740處)至處理佇列使得金鑰鏈項目可等待此金鑰鏈項目所屬之保護域之條件得到滿足。處理程序1700接著進行至1760，下文將另外描述1760。

當處理程序1700判定(在1730處)滿足所識別之保護域之所有條件

時，處理程序1700處理(在1750處)金鑰鏈項目。在1750處，一些實施例之處理程序1700藉由起始使金鑰鏈同步來處理金鑰鏈項目。在一些實施例中，處理程序1700將目的地裝置之私用金鑰用於所識別之保護域來解密金鑰鏈項目。

接下來，處理程序1700判定(在1760處)在處理佇列中是否存在尚待處理之其他金鑰鏈項目。當處理程序1700判定在處理佇列中存在其他金鑰鏈項目時，處理程序1700循環返回至1710以擷取另一金鑰鏈項目。否則，處理程序1700結束。

圖18概念地說明用於存放傳入之金鑰鏈項目之一處理佇列。具體言之，此圖說明一些實施例之處理佇列係與不同保護域相關聯之一組貯體。此圖說明源裝置1805、目的地裝置1810及處理佇列1815。

源裝置1805更新一或多個金鑰鏈項目且將該等金鑰鏈項目推送至目的地裝置1810。在一些實施例中，源裝置1805發送之金鑰鏈項目1840與保護域識別符1835相關聯，源裝置1805發送該保護域識別符1835連同金鑰鏈項目1840。在一些實施例中，源裝置1805用目的地裝置1810之公用金鑰(未圖示)來加密金鑰鏈項目1840，目的地裝置1810先前已針對目的地裝置1810所支援之每一保護域而公開該公用金鑰。在此等實施例中之一些實施例中，用以加密金鑰鏈項目之公用金鑰可充當保護域識別符。

目的地裝置1810用以存放金鑰鏈項目之處理佇列1815具有貯體1820至1830。該等貯體中之每一者與保護域相關聯，如所示。目的地裝置1810基於由保護域識別符所識別之保護域而將金鑰鏈項目存放於處理佇列1815之貯體1820至1830中之一者中。在一些實施例中，目的地裝置1810亦存放與每一金鑰鏈項目相關聯之保護域識別符。在其他實施例中，當目的地裝置1810將金鑰鏈項目存放於處理佇列1815中時，目的地裝置1810使識別符與該等金鑰鏈項目無關。如所示，貯體

1820具有三個金鑰鏈項目1845至1855，貯體1825具有一個金鑰鏈項目1860，且貯體1830具有裝置1810在無保護域識別符之情況下已存放的兩個金鑰鏈項目1865及1870。

在一些實施例中，當金鑰鏈項目係在處理佇列1815中時，該等金鑰鏈項目不可用於供裝置1810之使用。該等金鑰鏈項目被描繪為虛線橢圓形以指示金鑰鏈項目對裝置1810之不可用性。

在一些實施例中，目的地裝置1810使金鑰鏈項目與一私用金鑰相關聯，該私用金鑰為源裝置1805用以簽署被推送至目的地裝置1810之金鑰鏈項目的公用金鑰之對應物私用金鑰。目的地裝置1810將私用金鑰與金鑰鏈項目一起存放於處理佇列中且藉此使私用金鑰變成不可用於供裝置1810之使用。

在一些實施例中，目的地裝置1810藉由使用與保護域相關聯之其他金鑰來加密儲存於處理佇列中之私用金鑰而使該等私用金鑰變成不可用。在此等實施例中，僅當裝置滿足保護域之條件時才可用彼等其他金鑰來解密儲存於處理佇列中之私用金鑰。金鑰鏈項目可接著用經解密之私用金鑰加以解密且藉此變得可用於供裝置之使用。在本專利申請案中，將用以加密私用金鑰之彼等其他金鑰稱作本端域保護金鑰。

當裝置1810滿足針對與特定貯體相關聯之保護域所定義的所有條件時，目的地裝置1810可藉由用本端域保護金鑰解密私用金鑰且接著用經解密之私用金鑰解密金鑰鏈而自該特定貯體取出金鑰鏈項目。目的地處理裝置1810接著處理經解密之金鑰鏈項目。在一些實施例中，裝置1810起始一同步處理程序以使所接收之金鑰鏈項目與裝置1810業已具有之金鑰鏈項目(未圖示)同步。

應注意到，當目的地裝置1810自源裝置1805接收到金鑰鏈項目同時目的地裝置1810滿足該等金鑰鏈項目所屬之保護域之條件時，目

的地裝置1810無需針對該等保護域來加密私用金鑰。目的地裝置1810因此可在不將金鑰鏈項目存放於處理佇列1815中的情況下用私用金鑰來解密金鑰鏈項目。

圖19概念地說明一些實施例執行以處理自源裝置接收之金鑰鏈項目之處理程序1900。在一些實施例中，源裝置在單一異動(例如，單一訊息)中推送金鑰鏈項目群組而非每異動推送一個金鑰鏈項目。在一些狀況下，一群組中之金鑰鏈項目係以如此之方式相關以致於該等金鑰鏈項目將不由目的地裝置一同加以處理。在一些實施例中，藉由一目的地裝置來執行處理程序1900，該目的地裝置接收若干群組中之金鑰鏈項目且一同處理一群組中之金鑰鏈項目。詳言之，在此等實施例中，目的地裝置之金鑰鏈管理器可執行處理程序1900。一些實施例之目的地裝置將來自源裝置之若干金鑰鏈項目群組存放於處理佇列中。在一些實施例中，當目的地裝置被啟動且已自源裝置接收到一或多個金鑰鏈項目群組時，處理程序1900開始。

處理程序1900藉由自處理佇列擷取(在1910處)金鑰鏈項目群組而開始，該處理佇列為用於保存自源裝置推送之若干金鑰鏈項目群組的一儲存結構(例如，檔案系統)。在一些實施例中，源裝置藉由將目的地裝置之公用金鑰用於在被儲存於處理佇列中之群組中的每一金鑰鏈項目所屬之保護域來加密該金鑰鏈項目中之資料。目的地裝置使用對應之私用金鑰來解密該群組中之金鑰鏈項目。處理程序1900接著識別(在1920處)所擷取之金鑰鏈項目群組中之每一金鑰鏈項目的保護域。

接下來，處理程序1900判定(在1930處)所擷取之群組之所有所識別的保護域是否可用。亦即，處理程序1900判定目的地裝置是否已滿足所識別之保護域中之每一者的所有條件。一些實施例之處理程序1900迭代地經歷該群組之所識別之保護域中之每一者。

當處理程序1900判定(在1930處)並不滿足所識別之保護域中之任

一者的保護域之所有條件時，處理程序1900藉由將該金鑰鏈項目群組存放回於處理佇列中而將該金鑰鏈項目群組傳回(在1940處)至該佇列。處理程序1900接著進行至1960，下文將另外描述1960。

當處理程序1900判定(在1930處)滿足每一所識別之保護域之所有條件時，處理程序1900處理(在1950處)該金鑰鏈項目群組。在1950處，一些實施例之處理程序1900藉由起始一同步處理程序來處理金鑰鏈項目。在一些實施例中，處理程序1900將目的地裝置之私用金鑰用於所識別之保護域來解密金鑰鏈項目。

接下來，處理程序1900判定(在1960處)在處理佇列中是否存在尚待處理之其他金鑰鏈項目群組。當處理程序1900判定在處理佇列中存在其他金鑰鏈項目群組時，處理程序1900循環返回至1910以擷取另一金鑰鏈項目群組。否則，處理程序1900結束。

B. 用例

圖20說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被解除鎖定以便使屬於該保護域之金鑰鏈項目在裝置處可用。具體言之，此圖在六個不同階段2001至2006中說明處理一金鑰鏈項目2020，該金鑰鏈項目2020係由源裝置2010來更新且被推送至目的地裝置2015。此圖亦說明處理一金鑰鏈項目2025，該金鑰鏈項目2025為待與金鑰鏈項目2020同步之對應金鑰鏈項目。

金鑰鏈項目2020及2025所屬之保護域需要目的地裝置2015被解除鎖定以便使金鑰鏈項目202及2025在目的地裝置2015處可用。在本專利申請案中，裝置被「解除鎖定」可並非意謂裝置之螢幕被解除鎖定以用於取得至螢幕之任何輸入。相反，裝置被解除鎖定意謂使用者已進行鑑認以使用裝置。不同實施例之裝置提供不同鑑認機制。例如，一些實施例之裝置需要使用者提供用以解除鎖定該裝置之通行碼(例如，四數位通行碼)。其他實施例可替代地或共同地允許使用者用

長的密碼、視網膜掃描、指紋掃描、語音辨識等來解除鎖定裝置。

第一階段2001展示分別在源裝置2010及目的地裝置2015中之金鑰鏈項目2020及2025係同步。在此階段，目的地裝置2015處於鎖定狀態。目的地裝置2015處於鎖定狀態係因為自裝置2015被啟動以來裝置2015尚未由裝置2015之使用者解除鎖定或因為裝置2015在閒置時間之週期已流逝之後自動地自解除鎖定狀態轉至鎖定狀態。如所示，金鑰鏈項目2020與2025兩者包括資料1，但目的地裝置2015處之金鑰鏈項目2025被描繪為虛線平行四邊形以指示金鑰鏈2025由於目的地裝置2015處於鎖定狀態而不可用。在此實例中，目的地2015藉由用金鑰鏈項目2025所屬之保護域的本端保護域金鑰加密金鑰鏈項目2025而使該金鑰鏈項目2025不可用。

第二階段2002展示源裝置2010處之金鑰鏈項目2020已自資料1更新至資料2。例如，金鑰鏈項目2020包括用以存取運行於源裝置2010中之應用程式需要之遠端伺服器的密碼，且源裝置2010之使用者已改變該密碼。在此階段，金鑰鏈項目2025由於目的地裝置2015仍處於鎖定狀態而保持在目的地裝置2025處不可用。

下一階段2003展示源裝置2010已將金鑰鏈項目2020推送至目的地裝置2015以便使金鑰鏈項目2020與目的地裝置2015之對應金鑰鏈項目2025同步。在此實例中，在將金鑰鏈項目2020推送至目的地裝置2015之前，源裝置2010用目的地裝置2015之用於保護域之公用金鑰來加密金鑰鏈項目2020。目的地裝置2015接收金鑰鏈項目2020但金鑰鏈項目2020在此階段不可用，因為目的地裝置處於鎖定狀態且因此尚未用用於保護域之對應私用金鑰來解密金鑰鏈項目2020。在此實例中，私用金鑰亦已不可用，因為目的地裝置2015已用用以加密金鑰鏈項目2025之本端保護域金鑰來加密私用金鑰。金鑰鏈項目2025保持在目的地裝置2015處不可用，因為目的地裝置2015處於鎖定狀態且因此尚未

用本端保護域金鑰來解密金鑰鏈項目2025。

在第四階段2004，使用者已解除鎖定目的地裝置2015。結果，金鑰鏈項目2020與2025兩者變得可用於供目的地裝置2015之使用。亦即，在此階段之裝置2015用本端保護域金鑰來解密私用金鑰且接著用經解密之私用金鑰來解密金鑰鏈項目2020。裝置2015亦用本端保護域金鑰來解密金鑰鏈項目2025。目的地裝置2015接著起始使兩個金鑰鏈項目2020與2025同步，因為該等金鑰鏈項目2020與2025變得可用。

第五階段2005展示金鑰鏈項目2020與2025係同步且因此金鑰鏈項目2025具有資料2。目的地裝置2015處於解除鎖定狀態且金鑰鏈項目2025可用於供目的地裝置2015之使用。下一階段2006展示目的地裝置2015已回至鎖定狀態(例如，藉由為閒置歷時一時間週期或因為使用者已鎖定裝置2015)。目的地裝置2015藉由用本端保護域金鑰來加密金鑰鏈項目2025而使金鑰鏈項目2025變成不可用。

圖21說明受一保護域保護之金鑰鏈項目，該保護域需要裝置至少一旦在經啟動之後便被解除鎖定以便使屬於該保護域之金鑰鏈項目在裝置處可用。具體言之，此圖在六個不同階段2101至2106中說明藉由目的地裝置2115來處理金鑰鏈項目2120及2125。此圖亦說明源裝置2110，該源裝置2110更新金鑰鏈項目2120且將其推送至目的地裝置2115以用於與金鑰鏈項目2125同步。

金鑰鏈項目2120及2125所屬之保護域需要目的地裝置2115至少一旦在經啟動(亦即，自切斷狀態而被接通)之後便被解除鎖定以便使金鑰鏈項目2120及2125在目的地裝置2115處變成可用。在一些實施例中，使用此保護域來保護至運行背景中之應用程式的密碼。例如，當裝置閒置時(例如，當裝置不接收任何使用者輸入時)，運行於該裝置上之電子郵件應用程式需要用以存取郵件伺服器之一密碼以便提取電子郵件。

第一階段2101展示分別在源裝置2110及目的地裝置2115中之金鑰鏈項目2120及2125係同步。如所示，兩個金鑰鏈項目2120及2125包括資料1。在此階段，目的地裝置2115自目的地裝置2115被啟動以來仍尚未被解除鎖定。亦即，目的地裝置2115之使用者在啟動裝置2115之後尚未解除鎖定裝置2115。目的地裝置2115處之金鑰鏈項目2125被描繪為虛線平行四邊形以指示金鑰鏈項目2125不可用。在此實例中，目的地2115已用金鑰鏈項目2125所屬之保護域之本端保護域金鑰來加密金鑰鏈項目2125，以便使金鑰鏈項目2125變成不可用。

第二階段2102展示源裝置2110處之金鑰鏈項目2120已自資料1更新至資料2。在此階段，目的地裝置2115處之金鑰鏈項目2125保持不可用，因為目的地裝置2115自被啟動以來仍尚未被解除鎖定。

下一階段2103展示源裝置2110已將金鑰鏈項目2120推送至目的地裝置2115以便使金鑰鏈項目2120及目的地裝置2115之對應金鑰鏈項目2125同步。在此實例中，在將金鑰鏈項目2120推送至目的地裝置2115之前，源裝置2110用目的地裝置2115之用於保護域之公用金鑰來加密金鑰鏈項目2120。目的地裝置2115接收金鑰鏈項目2120但金鑰鏈項目2120在此階段不可用，因為目的地裝置2115自被啟動以來尚未被解除鎖定且因此尚未用用於保護域之對應私用金鑰來解密金鑰鏈項目2120。在此實例中，私用金鑰亦已不可用，因為目的地裝置2115已用用以加密金鑰鏈項目2125之本端保護域金鑰來加密私用金鑰。金鑰鏈項目2125保持在目的地裝置2115處不可用，因為目的地裝置2115處於鎖定狀態且因此尚未用本端保護域金鑰來解密金鑰鏈項目2125。

在第四階段2104，在目的地裝置2115已被啟動之後，使用者已解除鎖定裝置2115歷時第一時間。結果，金鑰鏈項目2120與2125兩者可用於供目的地裝置2115之使用。在此實例中，目的地裝置2115藉由用用於保護域之私用金鑰來解密金鑰鏈項目2120而使金鑰鏈項目2120變

成可用。目的地裝置2115已用用於保護域之本端保護域金鑰來解密私用金鑰以及金鑰鏈項目2125。目的地裝置2115起始使兩個金鑰鏈項目2120及2125同步，因為該等金鑰鏈項目2120與2125變得可用。

第五階段2105展示金鑰鏈項目2120與2125係同步且因此金鑰鏈項目2125具有資料2。目的地裝置2115處於解除鎖定狀態且金鑰鏈項目2125可用於供目的地裝置2115之使用。在此階段，源裝置2110之使用者再次將金鑰鏈項目2120自資料2更新至資料3。

第六階段2106展示目的地裝置2115已回至鎖定狀態(例如，藉由為閒置歷時一時間週期或因為使用者已鎖定裝置2115)。然而，金鑰鏈項目2125仍可用於供裝置2115之使用，因為一旦在裝置2115被啟動之後裝置2115便已被解除鎖定且因此裝置2115並不再次用本端保護域金鑰來加密金鑰鏈項目2125。

在此階段2106，源裝置2110亦已將金鑰鏈項目2120推送至目的地裝置2115以便使金鑰鏈項目2120及目的地裝置2115之對應金鑰鏈項目2125同步。在將金鑰鏈項目2120推送至目的地裝置2115之前，源裝置2110使用用於保護域之公用金鑰來加密金鑰鏈項目2120。目的地裝置2115接收金鑰鏈項目2120且即使目的地裝置2115處於鎖定狀態金鑰鏈項目2120仍變得可用。此係因為目的地裝置2115至少一旦在裝置2115被啟動之後便已被解除鎖定且因此裝置2115不加密私用金鑰，該私用金鑰接著可用於解密金鑰鏈項目2120。即使目的地裝置2115保持處於鎖定狀態，金鑰鏈項目2120將仍得以同步。

圖22說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被接通以便使屬於該保護域之金鑰鏈項目在裝置處可用。具體言之，此圖在四個不同階段2201至2204中說明藉由目的地裝置2215來處理金鑰鏈項目2220及2225。此圖亦說明源裝置2210，該源裝置2210更新金鑰鏈項目2220且將其推送至目的地裝置2215以用於與金鑰鏈項目2225同

步。

金鑰鏈項目2220及2225所屬之保護域需要目的地裝置2215被接通以便使金鑰鏈項目2220及2225變成可用於供裝置2215之使用。亦即，只要目的地裝置2215啟動及運行，金鑰鏈項目2220及2225便總是可用於供裝置2215之使用。由於此保護域幾乎不提供保護，所以一些實施例之裝置將此保護域用於需要總是運行之彼等應用程式。此應用程式之實例包括蘋果公司之Find My iPhone™應用程式。

第一階段2201展示分別在源裝置2210及目的地裝置2215中之金鑰鏈項目2220及2225係同步。如所示，兩個金鑰鏈項目2220及2225包括資料1。在此階段，目的地裝置2215被切斷。

第二階段2202展示源裝置2210處之金鑰鏈項目2220已自資料1更新至資料2。在此階段，目的地裝置2215被啟動但尚未被解除鎖定。然而，金鑰鏈項目2225可用於供目的地裝置2215之使用，因為已滿足保護域之條件(亦即，裝置被啟動及運行)且因此裝置2215並不用用於保護域之本端保護域金鑰來加密金鑰鏈項目2225。在一些實施例中，可仍用集接至裝置2215之金鑰(例如，自裝置2215之UID導出的金鑰)來加密金鑰鏈項目2225，但金鑰鏈項目2215被視為可用，因為該金鑰可用於解密裝置2215處之金鑰鏈項目2225。

下一階段2203展示源裝置2210已將金鑰鏈項目2220推送至目的地裝置2215以便使金鑰鏈項目2220及目的地裝置2215之對應金鑰鏈項目2225同步。在將金鑰鏈項目2220推送至目的地裝置2215之前，源裝置2210加密金鑰鏈項目2220。目的地裝置2215接收金鑰鏈項目2220且即使裝置2215尚未被解除鎖定金鑰鏈項目2220在此階段仍變得在裝置2215處可用。此係因為裝置2215被啟動及運行且因此對應之私用金鑰可用於解密金鑰鏈項目2220。目的地裝置2215起始使兩個金鑰鏈項目2220及2225同步，因為該等金鑰鏈項目2220及2225係可用的。

在第四階段2204，目的地裝置2215尚未被解除鎖定。然而，第四階段2204展示金鑰鏈項目2220及2225係同步。結果，金鑰鏈項目2225現具有資料2。

圖23說明受一保護域保護之金鑰鏈項目，該保護域需要裝置被解除鎖定且亦需要額外鑑認以便使屬於該保護域之金鑰鏈項目在裝置處可用。具體言之，此圖在六個不同階段2301至2306中說明處理一金鑰鏈項目2320，該金鑰鏈項目2320係由源裝置2310來更新且被推送至目的地裝置2315。此圖亦說明處理一金鑰鏈項目2325，該金鑰鏈項目2325為待與金鑰鏈項目2320同步之對應金鑰鏈項目。

金鑰鏈項目2320及2325所屬之保護域需要目的地裝置2315被解除鎖定且亦需要額外鑑認(例如，密碼、視網膜掃描、指紋掃描、語音辨識、裝置在某一位置附近內等)以便使金鑰鏈項目2320及2325變成在裝置2315處可用。在一些實施例中，將此保護域用於保護至需要額外安全性措施之應用程式的密碼。例如，一些實施例之金鑰鏈管理器產生用於使應用程式存取遠端伺服器之安全之一隨機密碼。在一些實施例中，未向使用者曝露此密碼，且金鑰鏈管理器用使用者可記得及使用之較簡單或不同密碼來鑑認使用者。未曝露之密碼在使用者所使用之裝置之間得以同步。當未曝露之密碼在源裝置處被改變且被推送至目的地裝置時，除非使用者提供不同密碼來使用在目的地裝置處運行之相同應用程式，否則即使使用者解除鎖定目的地裝置，未曝露之密碼仍未變得在目的地裝置處可用。

第一階段2301展示分別在源裝置2310及目的地裝置2315中之金鑰鏈項目2320及2325係同步。在此階段，目的地裝置2315處於解除鎖定狀態。如所示，金鑰鏈項目2320與2325兩者包括資料1，但目的地裝置2315處之金鑰鏈項目2325不可用，因為目的地裝置2315處於鎖定狀態。在此實例中，目的地2315已用金鑰鏈項目2325所屬之保護域之

本端保護域金鑰來加密金鑰鏈項目2325，以便使金鑰鏈項目2325變成不可用。

第二階段2302展示源裝置2310處之金鑰鏈項目2320已藉由使用者而自資料1更新至資料2。例如，金鑰鏈項目2320包括實際上被用以存取運行於源裝置2310中之應用程式需要之遠端伺服器的未曝露之密碼，且使用者剛才已藉由改變使用者記得及用來進行鑑認以使用應用程式的不同密碼而改變未曝露之密碼。在此階段，金鑰鏈項目2325保持不可用，因為目的地裝置2315仍處於鎖定狀態且因此尚未滿足保護域之條件。

第三階段2303展示源裝置2310已將金鑰鏈項目2320推送至目的地裝置2315以便使金鑰鏈項目2320及目的地裝置2315之對應金鑰鏈項目2325同步。在此實例中，在將金鑰鏈項目2320推送至目的地裝置2315之前，源裝置2310用目的地裝置2315之用於保護域之公用金鑰來加密金鑰鏈項目2320。目的地裝置2315接收金鑰鏈項目2320但金鑰鏈項目2320在此階段不可用，因為目的地裝置處於鎖定狀態且因此尚未用用於保護域之對應私用金鑰來解密金鑰鏈項目2320。金鑰鏈項目2325亦保持不可用，因為目的地裝置2315處於鎖定狀態。

在第四階段2304，使用者已解除鎖定目的地裝置2315。然而，金鑰鏈項目2320與2325兩者仍不可用於供目的地裝置2315之使用，因為尚未滿足金鑰鏈項目2320及2325所屬之保護域之條件(使用者尚未提供此保護域需要之額外鑑認)。

第五階段2305展示使用者已提供額外鑑認(例如，藉由打入使用者記得之不同密碼)。金鑰鏈項目2320與2325兩者現已變得可用。此係因為已滿足保護域之所有條件且因此裝置2315已用本端保護域來解密私用金鑰及金鑰鏈項目2325。裝置2315已用經解密之私用金鑰來解密金鑰鏈項目2325。目的地裝置2315起始使兩個金鑰鏈項目2320及

2325同步。第六階段2306展示金鑰鏈項目2320及2325係同步且因此金鑰鏈項目2325具有資料2。

圖24說明受兩個保護域保護之資料，該兩個保護域針對裝置而具有不同組條件。具體言之，此圖在四個不同階段2401至2404中說明藉由目的地裝置2415來處理後設資料項目2430與2435及金鑰鏈項目2420與2425。此圖亦說明源裝置2410，該源裝置2410更新金鑰鏈項目2420且將其推送至目的地裝置2415以用於與金鑰鏈項目2425同步。

如上文所提及，一金鑰鏈項目與一後設資料項目相關聯，該後設資料項目載運用於待用以在使兩個金鑰鏈項目同步時解析任何衝突的裝置之資訊。在一些實施例中，將金鑰鏈項目及其相關聯之後設資料項目定義成在不同保護域中使得後設資料項目變得在裝置處可用，而金鑰鏈項目保持不可用。當金鑰鏈項目不可用且相關聯之後設資料項目在裝置處可用時，裝置可使用由相關聯之後設資料項目所載運之資訊來解析金鑰鏈項目之任何衝突。

後設資料項目2430及2435分別與金鑰鏈項目2420及2425相關聯。在此實例中，後設資料項目2430及2435屬於第一保護域，該第一保護域需要目的地裝置2415被接通以便使後設資料項目2430及2435可用於供裝置2415之使用。金鑰鏈項目2420及2425屬於第二保護域，該第二保護域需要目的地裝置2415處於解除鎖定狀態以便使金鑰鏈項目在目的地裝置2415處可用。

第一階段2401展示分別在源裝置2410及目的地裝置2415中之金鑰鏈項目2420及2425係不同步。如所示，金鑰鏈項目2420及2425分別包括資料1及資料2。後設資料項目2430及2435具有不同資訊。如所示，後設資料項目2430載運後設資料1且後設資料項目2435載運後設資料2。在此階段，目的地裝置2415處於鎖定狀態。目的地裝置2415處之金鑰鏈項目2425被描繪為虛線平行四邊形以指示金鑰鏈項目2425

在裝置2415處不可用。在此實例中，裝置2425已藉由用用於第二保護域之本端保護域金鑰加密金鑰鏈項目2425而使金鑰鏈項目2425變成不可用。後設資料項目2435在裝置2415處可用，因為當裝置2425接通時，裝置2425不加密後設資料2435。

第二階段2402展示源裝置2410已將金鑰鏈項目2420與相關聯之後設資料項目2430一起推送至目的地裝置2415以便使金鑰鏈項目2420及目的地裝置2415之對應金鑰鏈項目2425同步。在此實例中，源裝置2410用目的地裝置2415之用於第一保護域之公用金鑰來加密後設資料項目2430。在將後設資料項目2430及金鑰鏈項目2420發送至目的地裝置2415之前，源裝置2410亦用目的地裝置2415之用於第二保護域之公用金鑰來加密金鑰鏈項目2420。

目的地裝置2415接收金鑰鏈項目2420及後設資料項目2435但在此階段2402金鑰鏈項目2420在目的地裝置2415處不可用。此係因為目的地裝置2415仍處於鎖定狀態且因此裝置2415未用用於第二保護域之私用金鑰來解密金鑰鏈項目2425。金鑰鏈項目2425保持不可用，因為裝置2415仍處於解除鎖定狀態。在此階段2402，後設資料項目2435在目的地2415處可用，因為裝置2402係啟動及運行的。裝置2415藉由使用後設資料項目2430及2435來解析兩個經加密之金鑰鏈項目2420與2425之間的衝突而起始使該等金鑰鏈項目2420及2425同步。

在第三階段2403，目的地裝置2415仍處於鎖定狀態。然而，目的地裝置2415已使該等金鑰鏈項目同步。結果，後設資料項目已得以用新衝突解析資訊(後設資料3)加以更新且金鑰鏈項目2425具有資料1。經更新之金鑰鏈項目2425藉由保持用用於第二域之公用金鑰加密而在目的地裝置2415處仍不可用，因為裝置2415仍處於鎖定狀態。在第四階段2404，目的地裝置2415處於解除鎖定狀態。在此實例中，裝置藉由用用於第二域之本端保護域金鑰來解密用於第二保護域之私用

金鑰且接著用經解密之私用金鑰來解密金鑰鏈項目2425而使金鑰鏈項目2425變成可用。

C. 同步圈及保護域

如上文所提及，裝置可加入若干不同同步圈以用於使不同金鑰鏈項目同步(例如，使用上文藉由參看**圖4**至**圖6**所描述之技術)。在一些實施例中，若干裝置形成若干不同同步圈以便使屬於若干不同保護域之金鑰鏈項目同步。

圖25概念地說明由若干裝置所形成之若干同步圈。具體言之，此圖說明三個裝置A至C針對三個不同保護域1至3而形成三個不同同步圈2505至2515。該圖之頂部分說明位於三個同步圈2505至2515中之裝置A至C。該圖之底部分分開地說明三個同步圈2505至2515。

在一些實施例中，一裝置群組針對該等裝置用來保護金鑰鏈項目之保護域中之每一者而形成一同步圈。在一些此等實施例中，該群組之每一裝置使用該裝置用來加密及解密金鑰鏈項目之相同公用/私用金鑰對，以加入同步圈。替代地或共同地，其他實施例之裝置使用分開之金鑰對來加入同步圈及加密與解密金鑰鏈項目。

如所示，裝置A至C針對保護域1而形成同步圈2505。裝置A至C針對保護域2而形成同步圈2510。裝置A至C針對保護域3而形成同步圈2515。**圖25**說明三個同步圈係藉由相同之三個裝置A至C而形成。然而，裝置A至C中之每一者可針對除保護域1至3之外的保護域(未圖示)而與除裝置A至C中之兩個其他裝置之外的裝置形成其他同步圈(未圖示)。

雖然在此圖中將同步圈2505至2515說明為環形或圓形形狀，但每一對裝置建立一安全輸送層以形成同步圈。亦即，在一些實施例中，位於同步圈中之裝置形成一星形網路而非環形網路。

圖26概念地說明由若干裝置針對若干不同保護域所形成之同步

圈。具體言之，此圖說明三個裝置A至C針對三個不同保護域1至3而形成同步圈2605。此圖亦說明三個群組之金鑰鏈項目2610至2620。

在一些實施例中，一裝置群組針對若干不同保護域而形成單一同步圈。在此等實施例中之一些實施例中，該群組之每一裝置針對若干不同保護域而使用若干公用/私用金鑰對中之一對，以加入單一同步圈。亦即，該群組之每一裝置將若干公用/私用金鑰對中之一對選擇用於加密及解密金鑰鏈項目且使用所選之金鑰對來加入單一同步圈。替代地或共同地，在其他實施例中，該群組之每一裝置不使用金鑰對中之哪一者來加密及解密金鑰鏈項目而是使用一分開之金鑰鏈對來加入單一同步圈。

在一些實施例中，該群組之每一裝置針對若干不同保護域而使用所有該等若干公用/私用金鑰對以加入單一同步圈。亦即，在此等實施例中，該群組之每一裝置使用所有該等金鑰對來加密及解密金鑰鏈項目以加入同步圈。因此，在此等實施例中，裝置需要滿足若干不同保護域中之每一者的所有條件以便加入同步圈，因為該裝置需要使所有金鑰對可用。

在此實例中，金鑰鏈項目2610屬於保護域1。金鑰鏈項目2610正藉由裝置C而被推送至裝置A。裝置C將裝置A之公用金鑰(其已向裝置B及C公開)用於保護域1，以加密金鑰鏈項目2610。然而，在此實例中，裝置C已將所有三個公用/私用金鑰對用於保護域1至3以加入同步圈2605。

金鑰鏈項目2620屬於保護域2。金鑰鏈項目2620正藉由裝置B而被推送至裝置C。裝置B將裝置C之公用金鑰(其已向裝置A及B公開)用於保護域2，以加密金鑰鏈項目2610。在此實例中，裝置B已將所有三個公用/私用金鑰對用於保護域1至3以加入同步圈2605。

金鑰鏈項目2615屬於保護域3。金鑰鏈項目2615正藉由裝置A而

被推送至裝置B。裝置A將裝置B之公用金鑰(其已向裝置A及C公開)用於保護域3，以加密金鑰鏈項目2615。在此實例中，裝置B已將所有三個公用/私用金鑰對用於保護域1至3以加入同步圈2605。

V. 軟體架構

在一些實施例中，將上文所描述之處理程序實施為運行於特定機器(諸如，電腦(例如，桌上型電腦、膝上型電腦等)、手持型裝置(例如，智慧電話)或平板計算裝置)上或儲存於機器可讀媒體中之軟體。**圖27**概念地說明一些實施例之金鑰鏈管理器2700之軟體架構。在一些實施例中，金鑰鏈管理器係用於管理在位於同步圈中之裝置之間金鑰鏈之同步的一單機應用程式。一些實施例之金鑰鏈管理器被整合至另一應用程式(例如，金鑰鏈管理應用程式、資料管理應用程式、安全性應用程式等)中，而在其他實施例中，可在作業系統內實施該應用程式。此外，在一些實施例中，可將該應用程式提供作為基於伺服器之解決方案之部分。在一些此等實施例中，經由簡單型用戶端來提供該應用程式。亦即，該應用程式運行於伺服器上，同時使用者經由距伺服器遙遠之分開之機器來與該應用程式互動。在其他此等實施例中，將該應用程式提供作為複雜型用戶端。亦即，該應用程式自伺服器而被分配至客戶端機器且運行於該客戶端機器上。

一些實施例之金鑰鏈管理器2700經實施以操作於不同作業系統上。在一些實施例中，不同作業系統(例如，iOS®、Mac OS X®等)使用不同架構來管理金鑰鏈及金鑰鏈項目。一些實施例之金鑰鏈管理器2700經實施以使用不同金鑰鏈管理架構而在裝置當中使金鑰鏈及金鑰鏈項目同步。例如，在一些實施例中，金鑰鏈管理器2700係針對一特定金鑰鏈管理架構(例如，iOS®)而實施且為帶端口型以藉由另一金鑰鏈管理架構(例如，Mac OS X®)來操作。

如所示，金鑰鏈管理器2700包括同步管理器2705、註冊管理器

2710、金鑰鏈項目管理器2715、密碼編譯模組2720、資訊清單模組2725及衝突解析器2730。金鑰鏈管理器2700亦包括同步圈資料儲存器2735、裝置資訊清單儲存器2740、衝突規則儲存器2745、金鑰鏈儲存器2750及安全性資料儲存器2755。在一些實施例中，同步圈資料2735儲存被儲存於上文藉由參看**圖3**所描述之儲存器310至330中的資料之本端複本。亦即，同步圈資料儲存器2735儲存同步圈之名稱、同步圈裝置清單、使用者簽名、裝置簽名及金鑰鏈資料，及其他資料。裝置資訊清單儲存器2740儲存同步圈中之裝置中之每一者的資訊清單歷史。衝突規則儲存器2745儲存衝突解析之先前版本、用以解析金鑰鏈項目衝突之衝突解析器之當前版本及與衝突解析器之先前版本及當前版本相關聯的各種規則。金鑰鏈儲存器2750儲存供與同步圈中之裝置同步之金鑰鏈。在一些實施例中，金鑰鏈儲存器2750亦儲存不與同步圈中之其他裝置共用(亦即，同步)的金鑰鏈及/或金鑰鏈項目。安全性資料儲存器2755儲存與金鑰鏈管理器2700提供用於促進金鑰鏈同步之安全性特徵(例如，安全通信頻道(例如，安全性金鑰)、資料加密(例如，加密金鑰)、資料解密(例如，解密金鑰)、資料鑑認(例如，解密金鑰)等)相關的資料。在一些實施例中，儲存器2735至2755被儲存於一個實體儲存器中，而在其他實施例中，儲存器2735至2755被儲存於分開之實體儲存器上。仍然，在一些實施例中，儲存器2735至2755中之一些或全部被實施跨越若干實體儲存器。

同步管理器2705負責管理在位於同步圈中之裝置之間金鑰鏈之同步。在一些實施例中，在其上操作有金鑰鏈管理器2700之裝置已成功地註冊至同步圈中之後，同步管理器2705藉由註冊管理器2710而開始。在一些實施例中，同步管理器2705處置上文在部分IV中所描述之資料保護特徵。同步管理器與其他模組2710及2715至2730通信以便實現在位於同步圈中之裝置之間金鑰鏈之同步。

註冊管理器2710處置與將裝置註冊至同步圈中相關的各種功能。例如，當其上正操作有金鑰鏈管理器之裝置想要加入同步圈時，註冊管理器2710建立一同步圈(當同步圈不存在時)。註冊管理器2710亦處置註冊請求產生(例如，藉由執行上文藉由參看**圖5**所描述之處理程序500)、註冊請求核准(例如，藉由執行上文藉由參看**圖6**所描述之處理程序600)、註冊核准確認等。

金鑰鏈項目管理器2715建立及管理金鑰鏈之金鑰鏈項目。在一些實施例中，金鑰鏈項目管理器2715產生及保持表示金鑰鏈中之一些或所有金鑰鏈項目的資料結構(例如，上文藉由參看**圖10**所描述之資料結構)。

安全性模組2720提供用於各種安全性特徵之功能性。舉例而言，安全性模組2720處置與同步圈中之裝置中之每一者的安全通信頻道之建立。安全性模組2720執行不同密碼編譯原始物件(cryptography primitive)、演算法、協定及技術(例如，OTR傳訊、迪菲-赫爾曼金鑰交換、公用/私用金鑰對產生等)，以便實施各種安全性特徵。

資訊清單模組2725負責基於本端金鑰鏈項目而產生不同類型之資訊清單且在一些實施例中同級裝置之資訊清單。例如，資訊清單模組2725產生資訊清單摘要、完整資訊清單及差異資訊清單。為促進產生資訊清單，資訊清單模組2725保持同步圈中之裝置中之每一者的資訊清單歷史。資訊清單模組2725亦在產生差異資訊清單中執行本端金鑰鏈項目(或本端資訊清單)與同級裝置之資訊清單之間的比較。

衝突解析器2730處置對金鑰鏈項目之間的衝突的解析。舉例而言，衝突解析器2730比較本端金鑰鏈項目及同級裝置之金鑰鏈項目以識別衝突。衝突解析器亦執行衝突解析器(例如，儲存於衝突規則儲存器2745中)以便解析金鑰鏈項目衝突。另外，衝突解析器2730負責偵測衝突解析器之間的衝突及判定待用以解析金鑰鏈項目衝突之衝突

解析器。

雖然已將該等特徵中之許多特徵描述為係由一個模組(例如，註冊模組2710、安全性模組2720等)執行，但一般熟習此項技術者將認識到，可將功能分裂成多個模組。類似地，在一些實施例中，可藉由單一模組(例如，金鑰鏈管理器2715及衝突解析器2730)來執行被描述為係由多個不同模組執行之功能。

VI. 電子系統

許多上文所描述之特徵及應用程式被實施為經指定為被記錄於電腦可讀儲存媒體(亦稱作電腦可讀媒體)上之一組指令的軟體處理程序。當此等指令係由一或多個計算或處理單元(例如，一或多個處理器、處理器之核心或其他處理單元)執行時，該等指令使該(該等)處理單元執行該等指令中所指示之動作。電腦可讀媒體之實例包括(但不限於)：CD-ROM、快閃驅動器、隨機存取記憶體(RAM)晶片、硬驅動器、可抹可程式化唯讀記憶體(EPROM)、電可抹可程式化唯讀記憶體(EEPROM)等。電腦可讀媒體不包括無線地或經由有線連接來傳遞的載波及電子信號。

在本說明書中，術語「軟體」意謂包括駐留於唯讀記憶體中之韌體或儲存於磁性儲存器中且可被讀入至記憶體中以供處理器處理的應用程式。又，在一些實施例中，可將多個軟體發明實施為較大程式之子部分同時保持不同之軟體發明。在一些實施例中，亦可將多個軟體發明實施為分開之程式。最後，一同實施此處所描述之軟體發明的分開之程式之任何組合係在本發明之範疇內。在一些實施例中，當經安裝以操作於一或多個電子系統上時，軟體程式定義一或多個特定機器實施，該一或多個特定機器實施執行該等軟體程式之操作。

圖28概念地說明一電子系統2800，可用該電子系統2800來實施本發明之一些實施例。電子系統2800可為電腦(例如，桌上型電腦、

個人電腦、平板電腦等)、電話、PDA或任何其他種類之電子或計算裝置。此電子系統包括各種類型之電腦可讀媒體及用於各種其他類型之電腦可讀媒體的介面。電子系統2800包括匯流排2805、處理單元2810、圖形處理單元(GPU) 2820、系統記憶體2825、網路2815、唯讀記憶體2830、永久性儲存裝置2835、輸入裝置2840及輸出裝置2845。

匯流排2805共同地表示通信地連接電子系統2800之眾多內部裝置的所有系統匯流排、周邊匯流排及晶片組匯流排。例如，匯流排2805通信地將處理單元2810與唯讀記憶體2830、GPU 2820、系統記憶體2825及永久性儲存裝置2835連接。

處理單元2810自此等各種記憶體單元擷取待執行之指令及待處理之資料以便執行本發明之處理程序。在不同實施例中，處理單元可為單一處理器或多核處理器。一些指令被傳遞至GPU 2820且由GPU 2820執行。GPU 2815可卸載各種計算或補充由處理單元2810所提供之影像處理。在一些實施例中，可使用CoreImage之內核陰影語言來提供此功能性。

唯讀記憶體(ROM) 2830儲存由電子系統之處理單元2810及其他模組需要之靜態資料及指令。另一方面，永久性儲存裝置2835為讀寫記憶體裝置。此裝置為即使當電子系統2800斷開時仍儲存指令及資料的非揮發性記憶體單元。本發明之一些實施例將大容量儲存裝置(諸如，磁碟或光碟，及其對應之磁碟驅動器)用作永久性儲存裝置2835。

其他實施例將抽取式儲存裝置(諸如，軟碟、快閃記憶體裝置等，及其對應之驅動器)用作永久性儲存裝置。像永久性儲存裝置2835一樣，系統記憶體2825為讀寫記憶體裝置。然而，不同於儲存裝置2835，系統記憶體2825為揮發性讀寫記憶體(諸如，隨機存取記憶體)。系統記憶體2825儲存處理器在運行時間需要之一些指令及資

料。在一些實施例中，本發明之處理程序被儲存於系統記憶體2825、永久性儲存裝置2835及/或唯讀記憶體2830中。舉例而言，各種記憶體單元包括用於根據一些實施例來處理多媒體剪輯之指令。處理單元2810自此等各種記憶體單元擷取待執行之指令及待處理之資料以便執行一些實施例之處理程序。

匯流排2805亦連接至輸入裝置2840及輸出裝置2845。輸入裝置2840使得使用者能夠將資訊及選擇命令傳達至電子系統。輸入裝置2840包括文數字鍵盤及指標裝置(亦稱為「游標控制裝置」)、相機(例如，網路攝影機)、用於接收語音命令之麥克風或類似裝置等。輸出裝置2845顯示由電子系統所產生之影像或否則輸出資料。輸出裝置2845包括印表機及顯示裝置(諸如，陰極射線管(CRT)或液晶顯示器(LCD))以及揚聲器或類似之音訊輸出裝置。一些實施例包括充當輸入裝置與輸出裝置兩者之裝置(諸如，觸控螢幕)。

最後，如**圖28**中所示，匯流排2805亦經由網路配接器(未圖示)而將電子系統2800耦接至網路2815。以此方式，電腦可為若干電腦之網路(諸如，區域網路(「LAN」)、廣域網路(「WAN」)或企業內部網路)或若干網路之網路(諸如，網際網路)的一部分。可結合本發明來使用電子系統2800之任何或所有組件。

一些實施例包括電子組件，諸如微處理器、將電腦程式指令儲存於機器可讀或電腦可讀媒體(替代地稱作電腦可讀儲存媒體、機器可讀媒體或機器可讀儲存媒體)中之儲存器及記憶體。此等電腦可讀媒體之一些實例包括RAM、ROM、唯讀緊密光碟(CD-ROM)、可記錄之緊密光碟(CD-R)、可重寫之緊密光碟(CD-RW)、唯讀數位影音光碟(例如，DVD-ROM、雙層DVD-ROM)、多種可記錄/可重寫之DVD (例如，DVD-RAM、DVD-RW、DVD+RW等)、快閃記憶體(例如，SD卡、迷你型SD卡、微SD卡等)、磁性及/或固態硬驅動器、唯讀及可

記錄之Blu-Ray®光碟、超密度光碟、任何其他光學或磁性媒體及軟磁碟。電腦可讀媒體可儲存一電腦程式，該電腦程式可由至少一個處理單元執行且包括用於執行各種操作之若干組指令。電腦程式或電腦碼之實例包括機器碼(諸如由編譯器產生)及包括較高階碼之檔案，該等檔案由電腦、電子組件或微處理器使用解譯器來執行。

雖然以上論述主要參考執行軟體之微處理器或多核處理器，但一些實施例係藉由一或多個積體電路(諸如，特殊應用積體電路(ASIC))或場可程式化閘陣列(FPGA))而執行。在一些實施例中，此等積體電路執行被儲存於電路自身上之指令。另外，一些實施例執行儲存於可程式化邏輯裝置(PLD)、ROM或RAM裝置中之軟體。

如在本說明書及本申請案之任何申請專利範圍中所使用，術語「電腦」、「伺服器」、「處理器」及「記憶體」皆指代電子或其他技術裝置。此等術語排除人或人群組。出於說明書之目的，術語顯示意謂在電子裝置上顯示。如在本說明書及本申請案之任何申請專利範圍中所使用，術語「電腦可讀媒體」及「機器可讀媒體」完全被限制至以可由電腦讀取之形式儲存資訊的有形、實體物件。此等術語排除任何無線信號、有線下載信號及任何其他短暫信號。

雖然已參考眾多特定細節描述本發明，但一般熟習此項技術者將認識到，在不背離本發明之精神的情況下可以其他特定形式來體現本發明。另外，諸多圖(包括**圖5**、**圖6**及**圖12**至**圖15**)概念地說明處理程序。可不以所展示及描述之確切次序來執行此等處理程序之特定操作。可不在一個連續系列之操作中執行特定操作，且在不同實施例中可執行不同特定操作。此外，可使用若干子處理程序來實施處理程序，或可將處理程序實施為較大巨集處理程序之部分。因此，一般熟習此項技術者將理解，本發明將不受前述說明性細節的限制，而是將由附加之申請專利範圍來定義。

【符號說明】

105	階段
110	階段
115	階段
205	金鑰鏈管理器
210	儲存器
305	雲端服務
310	儲存器
315	儲存器
320	儲存器
325	儲存器
330	儲存器
405	階段
410	階段
415	階段
420	同步圈
425	儲存器
705	密碼
805	密碼
1005	資料結構
1010	金鑰鏈ID
1015	存取資料
1020	金鑰鏈項目
1025	金鑰鏈項目ID
1030	資料
1035	存取資料

1040 ACL輸入項目

1045 授權標籤

1050 受信任應用程式

1100 狀態圖

1105 穩定狀態

1110 狀態

1115 狀態

1120 狀態

1125 狀態

1135 狀態

1140 狀態

1145 狀態

1605 源裝置

1610 源裝置

1615 目的地裝置

1620 目的地裝置

1625 目的地裝置

1630 目的地裝置

1635 目的地裝置

1805 源裝置

1810 目的地裝置

1815 處理佇列

1820 貯體

1825 貯體

1830 貯體

1835 保護域識別符

1840 金鑰鏈項目

1845 金鑰鏈項目

1850 金鑰鏈項目

1855 金鑰鏈項目

2001 階段

2002 階段

2003 階段

2004 階段

2005 階段

2006 階段

2010 源裝置

2015 目的地裝置

2020 金鑰鏈項目

2025 金鑰鏈項目

2101 階段

2102 階段

2103 階段

2104 階段

2105 階段

2106 階段

2110 源裝置

2115 目的地裝置

2120 金鑰鏈項目

2125 金鑰鏈項目

2201 階段

2202 階段

2203 階段

2204 階段

2210 源裝置

2215 目的地裝置

2220 金鑰鏈項目

2225 金鑰鏈項目

2301 階段

2302 階段

2303 階段

2304 階段

2305 階段

2306 階段

2310 源裝置

2315 目的地裝置

2320 金鑰鏈項目

2325 金鑰鏈項目

2401 階段

2402 階段

2403 階段

2404 階段

2410 源裝置

2415 目的地裝置

2420 金鑰鏈項目

2425 金鑰鏈項目

2430 後設資料項目

2435 後設資料項目

2505 同步圈

2510 同步圈

2515 同步圈

2610 金鑰鏈項目

2615 金鑰鏈項目

2620 金鑰鏈項目

2700 金鑰鏈管理器

2705 同步管理器

2710 註冊管理器

2715 金鑰鏈項目管理器

2720 密碼編譯模組

2725 資訊清單模組

2730 衝突解析器

2735 同步圈資料儲存器

2740 裝置資訊清單儲存器

2745 衝突規則儲存器

2750 金鑰鏈儲存器

2755 安全性資料儲存器

2800 電子系統

2805 匯流排

2810 處理單元

2815 網路

2820 圖形處理單元(GPU)

2825 系統記憶體

2830 唯讀記憶體

2835 永久性儲存裝置

2840 輸入裝置

2845 輸出裝置

申請專利範圍

1. 一種儲存一程式之非暫時性機器可讀媒體，該程式在由一裝置之至少一個處理單元執行時使儲存於該裝置上之一組金鑰鏈與一組其他裝置同步，該裝置及該組其他裝置經由一同級間(P2P)網路而通信地互相耦接，該程式包含用於以下各者之若干組指令：

接收對儲存於該裝置上之該組金鑰鏈中之一金鑰鏈的一修改；

針對該組其他裝置中之每一裝置而產生一更新請求，以便使儲存於裝置上之該組金鑰鏈與該組其他裝置同步；及

經由該P2P網路而經由一組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置。

2. 如請求項1之非暫時性機器可讀媒體，其中對該金鑰鏈之該修改係一金鑰鏈項目至該金鑰鏈之一新增。

3. 如請求項1之非暫時性機器可讀媒體，其中對該金鑰鏈之該修改係對該金鑰鏈中之一金鑰鏈項目的一修改。

4. 如請求項1之非暫時性機器可讀媒體，其中對該金鑰鏈之該修改係對該金鑰鏈中之一金鑰鏈項目的一刪除。

5. 如請求項1之非暫時性機器可讀媒體，其中該P2P網路係藉由根據一充分連接之網狀拓撲所組態之一疊加網路而實施。

6. 如請求項1之非暫時性機器可讀媒體，其中該P2P網路係藉由根據包含複數個節點之一星形拓撲所組態之一疊加網路而實施，其中該星形拓撲之一中心節點為一雲端儲存服務，且該星形拓撲之剩餘節點包含該裝置及該組其他裝置。

7. 一種用於使儲存於一裝置上之一組金鑰鏈與一組其他裝置同步

的方法，該裝置及該組其他裝置經由一同級間(P2P)網路而通信地互相耦接，該方法包含：

接收對儲存於該裝置上之該組金鑰鏈中之一金鑰鏈的一修改；

針對該組其他裝置中之每一裝置而產生一更新請求，以便使儲存於裝置上之該組金鑰鏈與該組其他裝置同步；及

經由該P2P網路而經由一組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置。

8. 如請求項7之方法，其中經由該P2P網路而經由該組分開之安全通信頻道將該組更新請求傳輸至該組其他裝置包含：用一加密金鑰來加密針對該組其他裝置中之每一裝置的該更新請求，使得該更新請求可僅藉由該其他裝置而解密。

9. 如請求項8之方法，其中用於加密針對該組其他裝置中之每一裝置之該更新請求的該加密金鑰包含：該其他裝置之公用/私用金鑰對之一公用金鑰。

10. 如請求項9之方法，其中使該組金鑰鏈同步包含：使該組金鑰鏈中之一或多個金鑰鏈之一部分同步。

11. 一種儲存一程式之非暫時性機器可讀媒體，該程式在由一裝置之至少一個處理單元執行時處理加入一同步圈以用於使金鑰鏈同步的請求，該同步圈包含該裝置及一組其他裝置，該程式包含用於以下各者之若干組指令：

接收針對一特定裝置加入該同步圈之一請求；

判定該請求是否得以鑑認；及

當該請求經判定為得以鑑認時，提示該請求之核准；及

當自該使用者接收到該請求之核准時，將該特定裝置新增至該同步圈。

12. 如請求項11之非暫時性機器可讀媒體，其中用於判定該請求是否得以鑑認之該組指令包含用於以下各者之若干組指令：

驗證與該同步圈相關聯之一使用者提交針對該特定裝置加入該同步圈之該請求；及

驗證針對該特定裝置加入該同步圈之該請求係由該特定裝置而產生。

13. 如請求項12之非暫時性機器可讀媒體，其中針對該特定裝置加入該同步圈之該請求包含該請求之一簽名，其中用於驗證與該同步圈相關聯之該使用者提交針對該特定裝置加入該同步圈之該請求的該組指令包含用於以下各者之若干組指令：

用一使用者簽署公用/私用金鑰對之一公用金鑰來解密該請求之該簽名；及

判定該請求匹配該經解密之簽名。

14. 如請求項12之非暫時性機器可讀媒體，其中針對該特定裝置加入該同步圈之該請求包含該請求之一簽名，其中用於驗證針對該特定裝置加入該同步圈之該請求係由該特定裝置而產生的該組指令包含用於以下各者之若干組指令：

用屬於該特定裝置且由該特定裝置所產生之一公用/私用金鑰對之一公用金鑰來解密該請求之該簽名；及

判定該請求匹配該經解密之簽名。

15. 如請求項11之非暫時性機器可讀媒體，其中用於提示該請求之核准的該組指令包含：用於在該裝置之一顯示螢幕上顯示一視窗的一組指令，該視窗請求鍵入一密碼。

16. 一種針對一裝置之用於處理加入一同步圈以用於使金鑰鏈同步之請求的方法，該同步圈包含該裝置及一組其他裝置，該方法包含：

接收針對一特定裝置加入該同步圈之一請求；

判定該請求是否得以鑑認；及

當該請求經判定為得以鑑認時，提示該請求之核准；及

當自該使用者接收到該請求之核准時，將該特定裝置新增至該同步圈。

17. 如請求項16之方法，其中將該特定裝置新增至該同步圈包含：將唯一地識別該特定裝置之資料新增至經指定為該同步圈之成員的裝置之一清單。

18. 如請求項17之方法，其中將該特定裝置新增至該同步圈進一步包含：用屬於該裝置且由該裝置所產生之一公用/私用裝置簽署金鑰對之一私用金鑰來產生裝置之該清單之一簽名。

19. 如請求項18之方法，其中將該特定裝置新增至該同步圈進一步包含：將裝置之該清單及該所產生之簽名儲存於一中心位置中以用於與該同步圈中之該等其他裝置共用。

20. 如請求項16之方法，其進一步包含在將該特定裝置新增至該同步圈之後使金鑰鏈與該特定裝置同步。

圖式

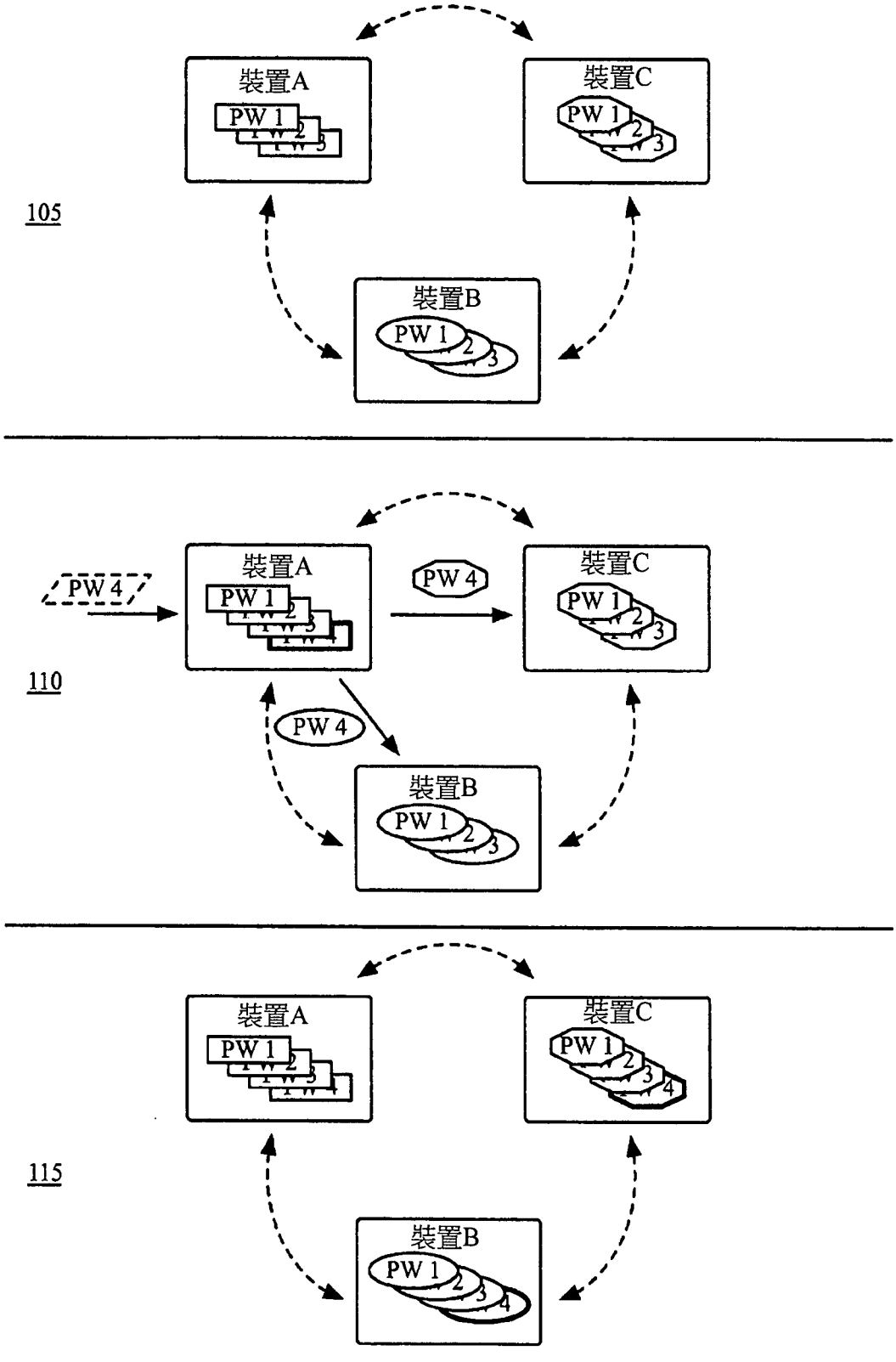
105
裝置A
PW 1
2
3
裝置C
PW 1
2
3
裝置B
PW 1
2
3
110
PW 4
裝置A
PW 1
2
3
4
PW 4
裝置C
PW 1
2
3
PW 4
裝置B
PW 1
2
3
115
裝置A
PW 1
2
3
4
裝置C
PW 1
2
3
4
裝置B
PW 1
2
3
4

圖1

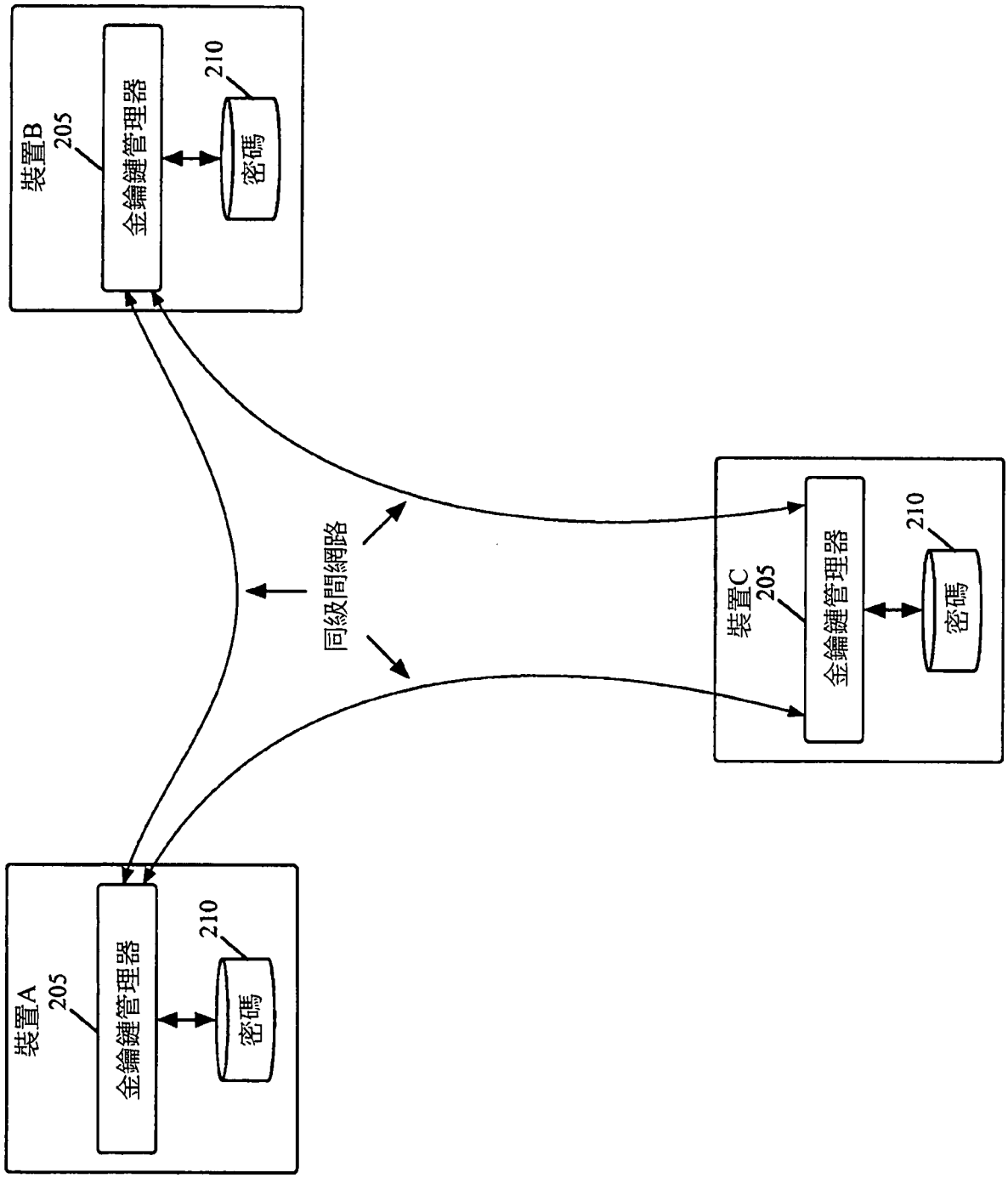
裝置B
205
金鑰鏈管理器
210
密碼
同級間網路
裝置C
205
金鑰鏈管理器
210
密碼
裝置A
205
金鑰鏈管理器
210
密碼

圖2

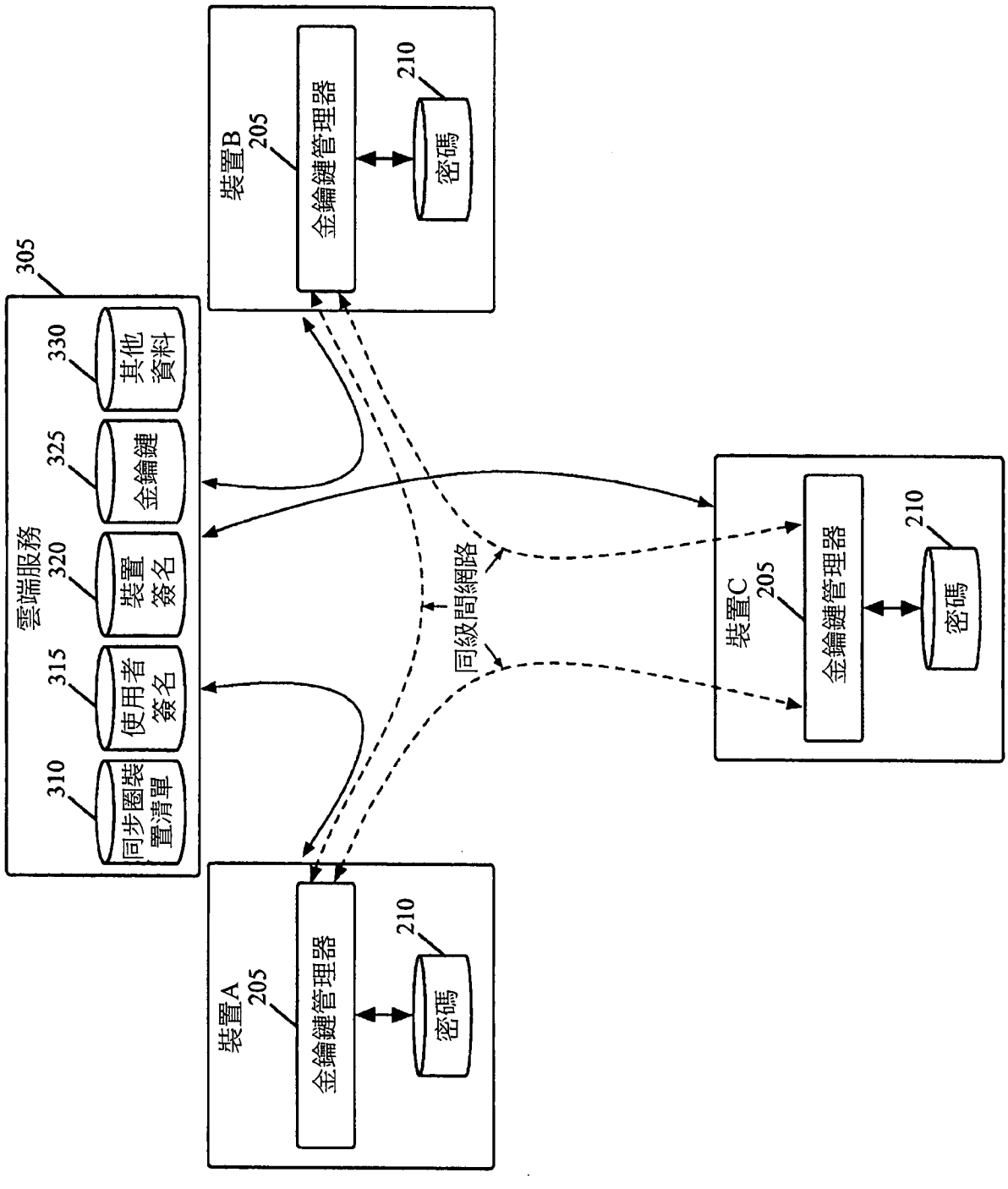
雲端服務
305
同步圈裝置清單
310
使用者簽名
315
裝置簽名
320
金鑰鏈
325
其他資料
330
裝置A
205
金鑰鏈管理器
210
密碼
裝置B
205
金鑰鏈管理器
210
密碼
裝置C
205
金鑰鏈管理器
210
密碼
同級間網路

圖3

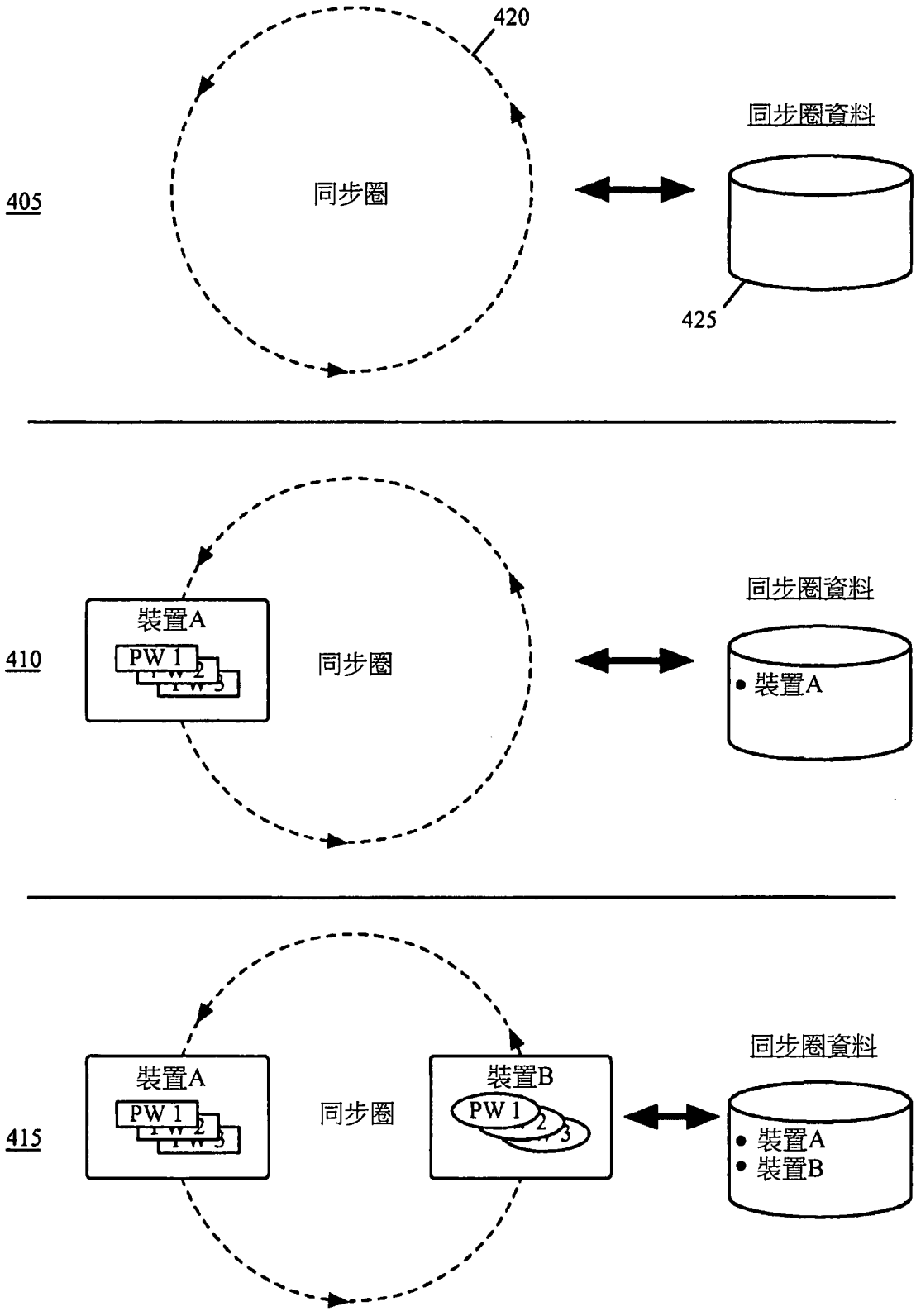
420
同步圈資料
405
同步圈
425
410
裝置A
PW 1
2
3
同步圈
同步圈資料
• 裝置A
415
裝置A
PW 1
2
3
同步圈
裝置B
PW 1
2
3
同步圈資料
• 裝置A
• 裝置B

圖4

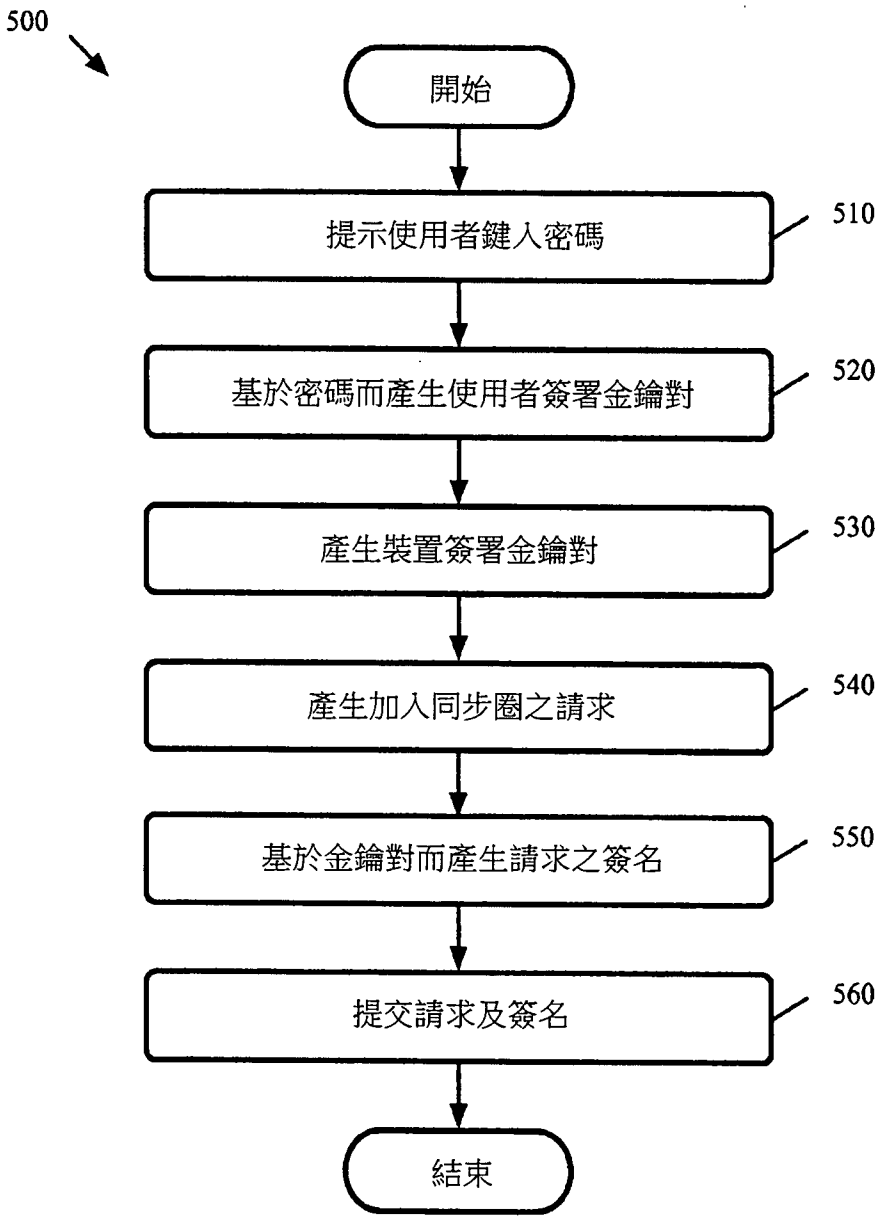
500
開始
提示使用者鍵入密碼
510
基於密碼而產生使用者簽署金鑰對
520
產生裝置簽署金鑰對
530
產生加入同步圈之請求
540
基於金鑰對而產生請求之簽名
550
提交請求及簽名
560
結束

圖5

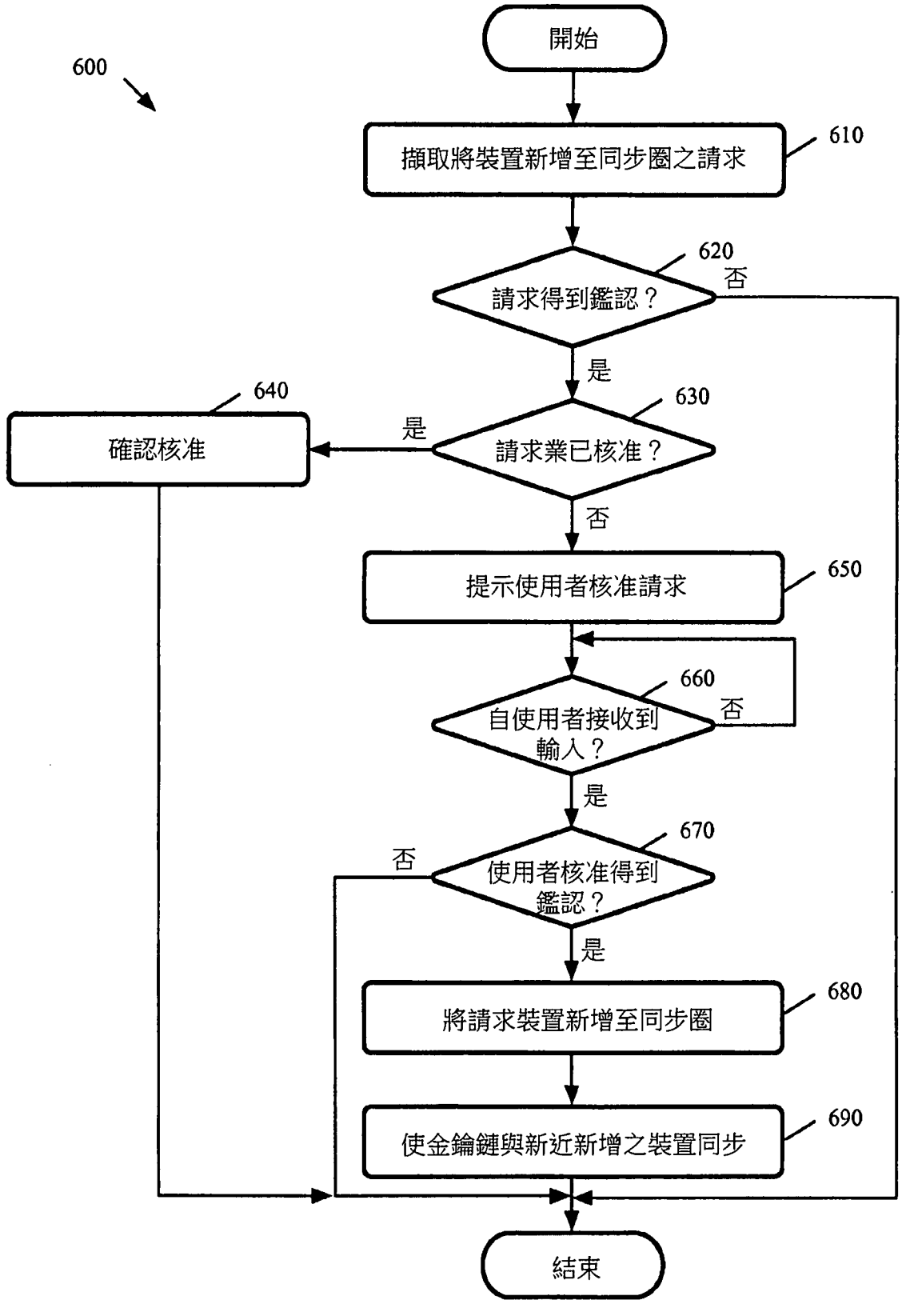
600
開始
擷取將裝置新增至同步圈之請求
610
請求得到鑑認？
620
否
是
請求業已核准？
630
是
確認核准
640
否
提示使用者核准請求
650
自使用者接收到輸入？
660
否
是
使用者核准得到鑑認？
670
否
是
將請求裝置新增至同步圈
680
使金鑰鏈與新近新增之裝置同步
690
結束

圖6

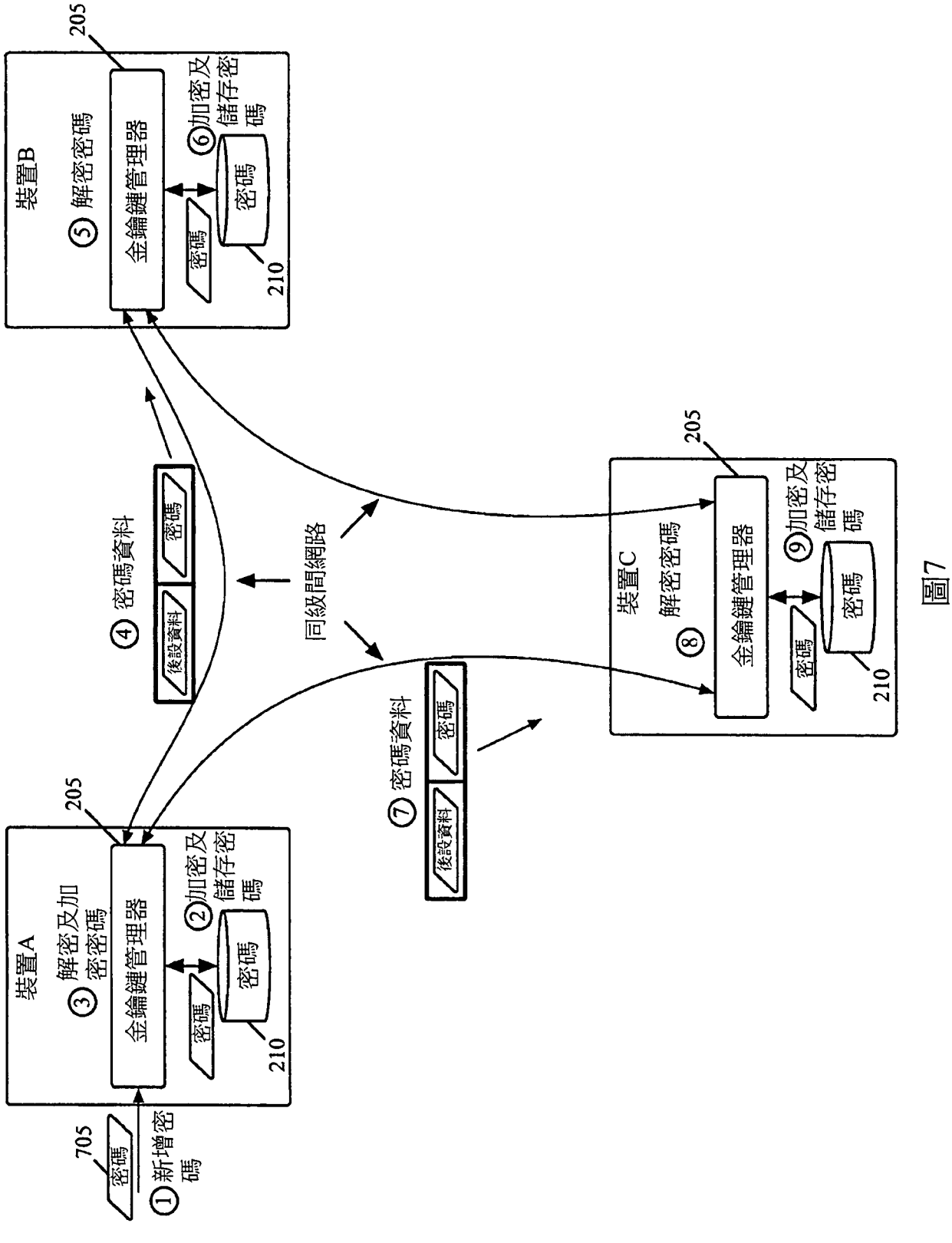
裝置A
205
③ 解密及加密密碼
金鑰鏈管理器
②加密及儲存密碼
密碼
210
705
密碼
① 新增密碼
裝置B
205
⑤ 解密密碼
金鑰鏈管理器
⑥加密及儲存密碼
密碼
密碼
210
④ 密碼資料
後設資料
密碼
同級間網路
⑦ 密碼資料
後設資料
密碼
裝置C
205
解密密碼
⑧
金鑰鏈管理器
⑨加密及儲存密碼
密碼
密碼
210

圖7

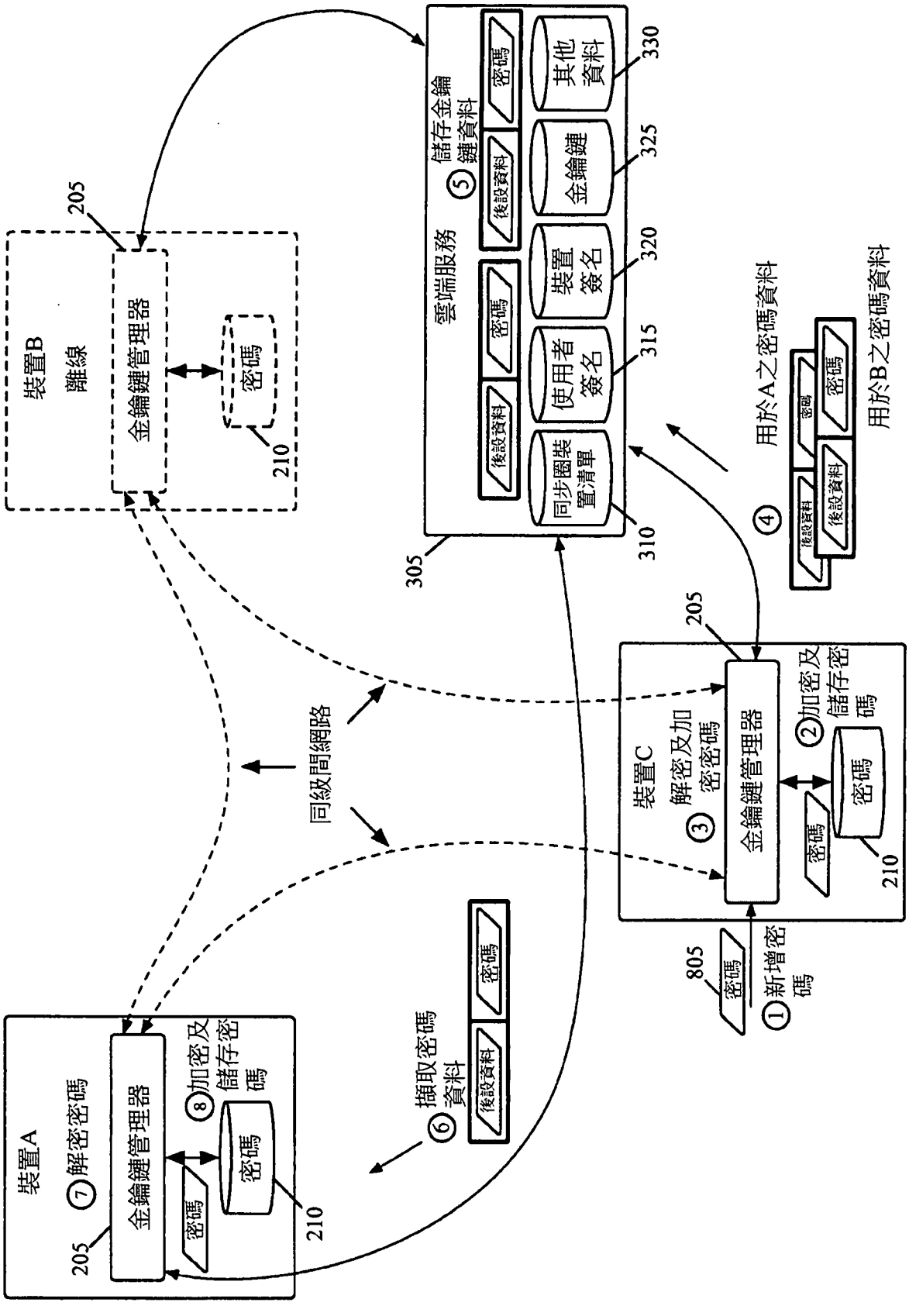
裝置B
離線
205
金鑰鏈管理器
密碼
210
雲端服務
⑤儲存金鑰
鍵資料
後設資料
密碼
使用者簽名
裝置簽名
金鑰鏈
其他資料
330
325
320
315
310
305
同步圈裝置清單
④
用於A之密碼資料
用於B之密碼資料
裝置C
③解密及加密密碼
金鑰鏈管理器
②加密及儲存密碼
①新增密碼
805
同級間網路
裝置A
⑦解密密碼
⑧加密及儲存密碼
⑥擷取密碼資料

圖8

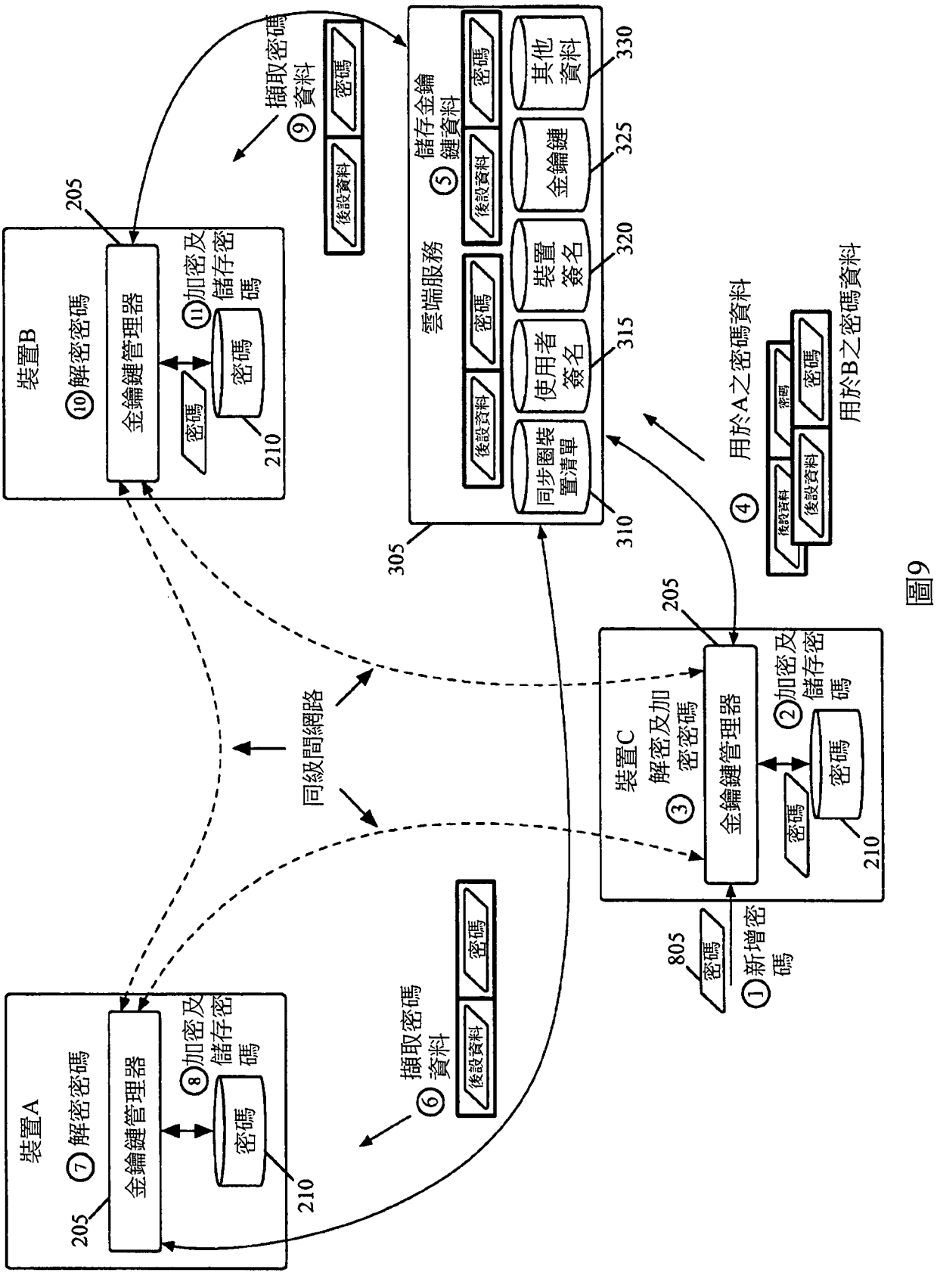
裝置A
⑦解密密碼
金鑰鏈管理器
205
⑧加密及儲存密碼
密碼
210
裝置B
⑩解密密碼
金鑰鏈管理器
205
⑪加密及儲存密碼
密碼
210
密碼
後設資料
⑨擷取密碼資料
雲端服務
⑤儲存金鑰鏈資料
305
後設資料
密碼
同步圈裝置清單
使用者簽名
315
裝置簽名
320
金鑰鏈
325
其他資料
330
310
同級間網路
⑥擷取密碼資料
後設資料
密碼
裝置C
③解密及加密密碼
金鑰鏈管理器
205
②加密及儲存密碼
密碼
210
805
密碼
①新增密碼
④用於A之密碼資料
後設資料
密碼
用於B之密碼資料

圖9

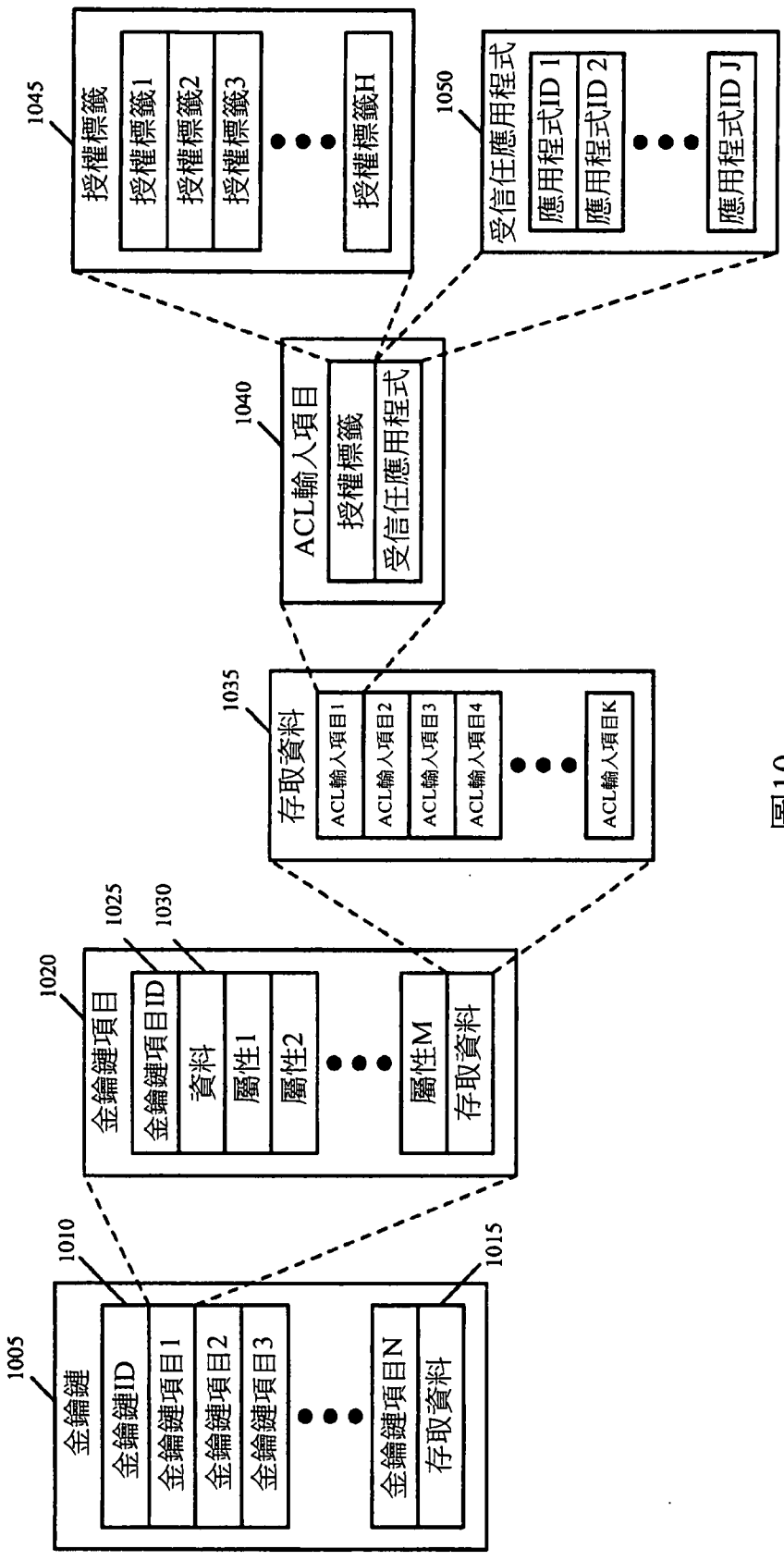
金鑰鏈
金鑰鏈ID
金鑰鏈項目1
金鑰鏈項目2
金鑰鏈項目3
金鑰鏈項目N
存取資料
金鑰鏈項目
金鑰鏈項目ID
資料
屬性1
屬性2
屬性M
存取資料
存取資料
ACL輸入項目1
ACL輸入項目2
ACL輸入項目3
ACL輸入項目4
ACL輸入項目K
ACL輸入項目
授權標籤
受信任應用程式
授權標籤
授權標籤1
授權標籤2
授權標籤3
授權標籤H
受信任應用程式
應用程式ID 1
應用程式ID 2
應用程式ID J
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050

圖10

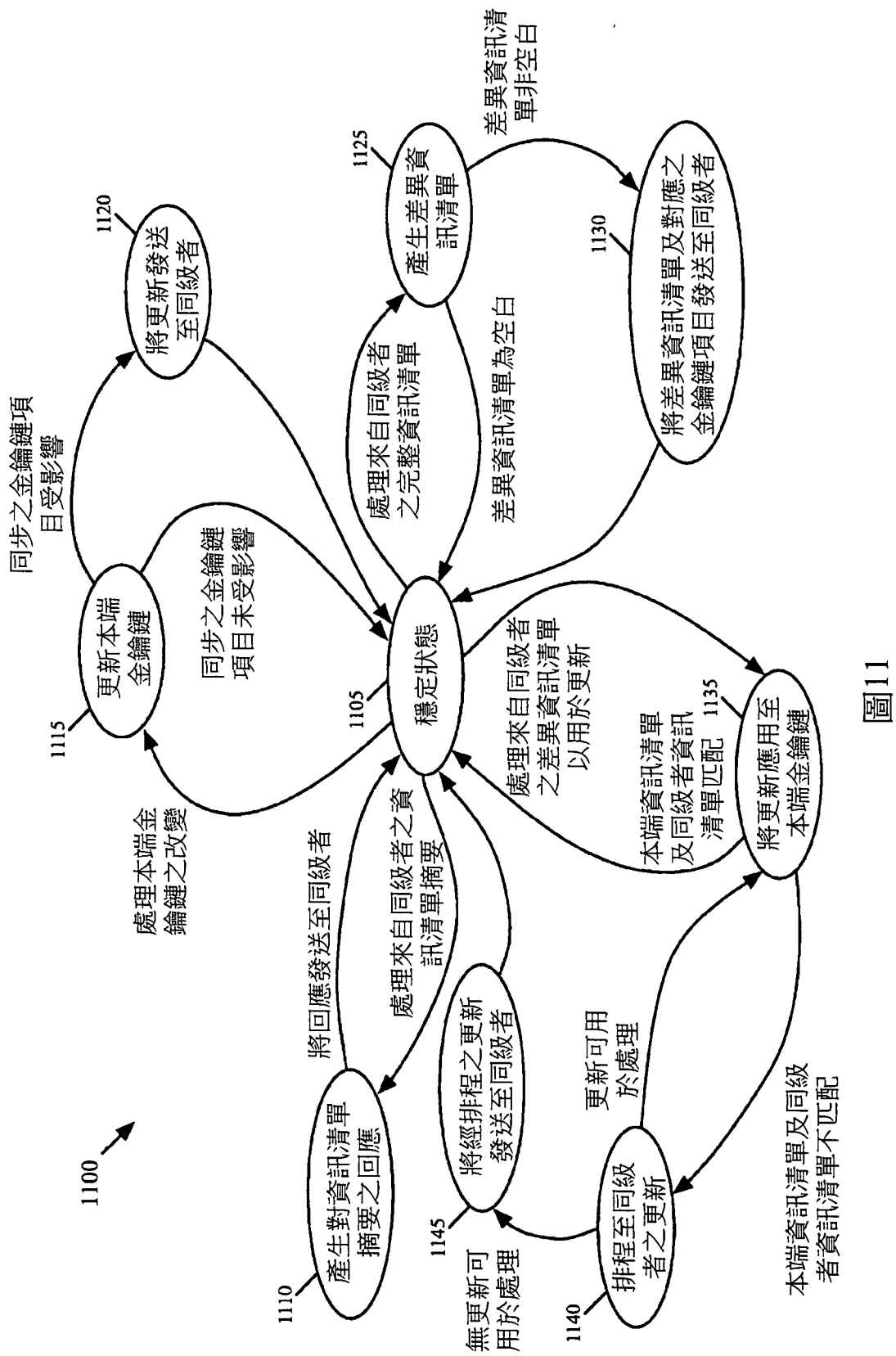
1100
1105
穩定狀態
1110
產生對資訊清單摘要之回應
1115
更新本端金鑰鏈
1120
將更新發送至同級者
1125
產生差異資訊清單
1130
將差異資訊清單及對應之金鑰鏈項目發送至同級者
1135
將更新應用至本端金鑰鏈
1140
排程至同級者之更新
1145
將經排程之更新發送至同級者
同步之金鑰鏈項目受影響
同步之金鑰鏈項目未受影響
處理本端金鑰鏈之改變
將回應發送至同級者
處理來自同級者之資訊清單摘要
處理來自同級者之完整資訊清單
差異資訊清單為空白
差異資訊清單非空白
處理來自同級者之差異資訊清單以用於更新
本端資訊清單及同級者資訊清單匹配
更新可用於處理
無更新可用於處理
本端資訊清單及同級者資訊清單不匹配

圖11

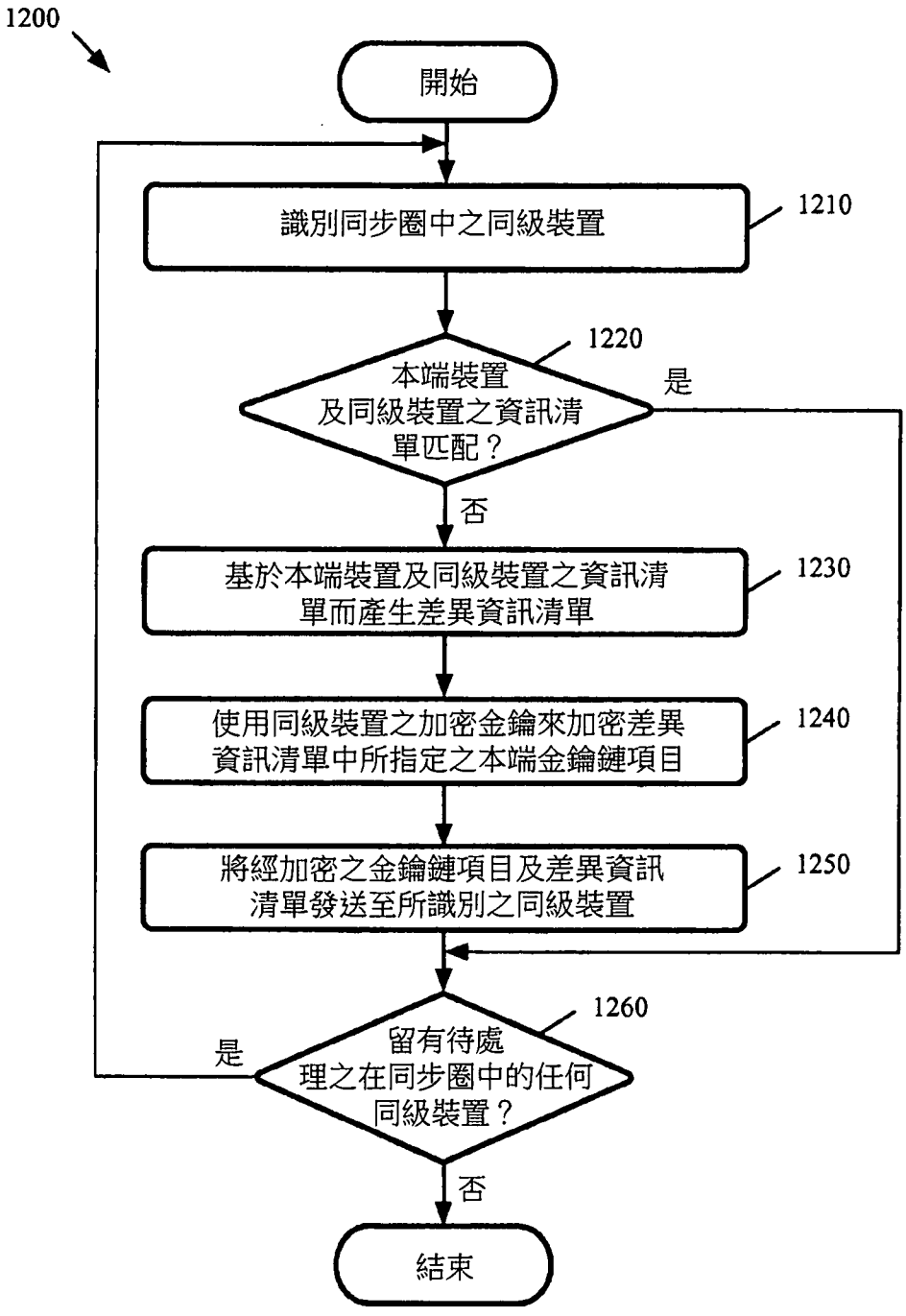
1200
開始
識別同步圈中之同級裝置
1210
1220
本端裝置及同級裝置之資訊清單匹配？
是
否
基於本端裝置及同級裝置之資訊清單而產生差異資訊清單
1230
使用同級裝置之加密金鑰來加密差異資訊清單中所指定之本端金鑰鏈項目
1240
將經加密之金鑰鏈項目及差異資訊清單發送至所識別之同級裝置
1250
1260
留有待處理之在同步圈中的任何同級裝置？
是
否
結束

圖12

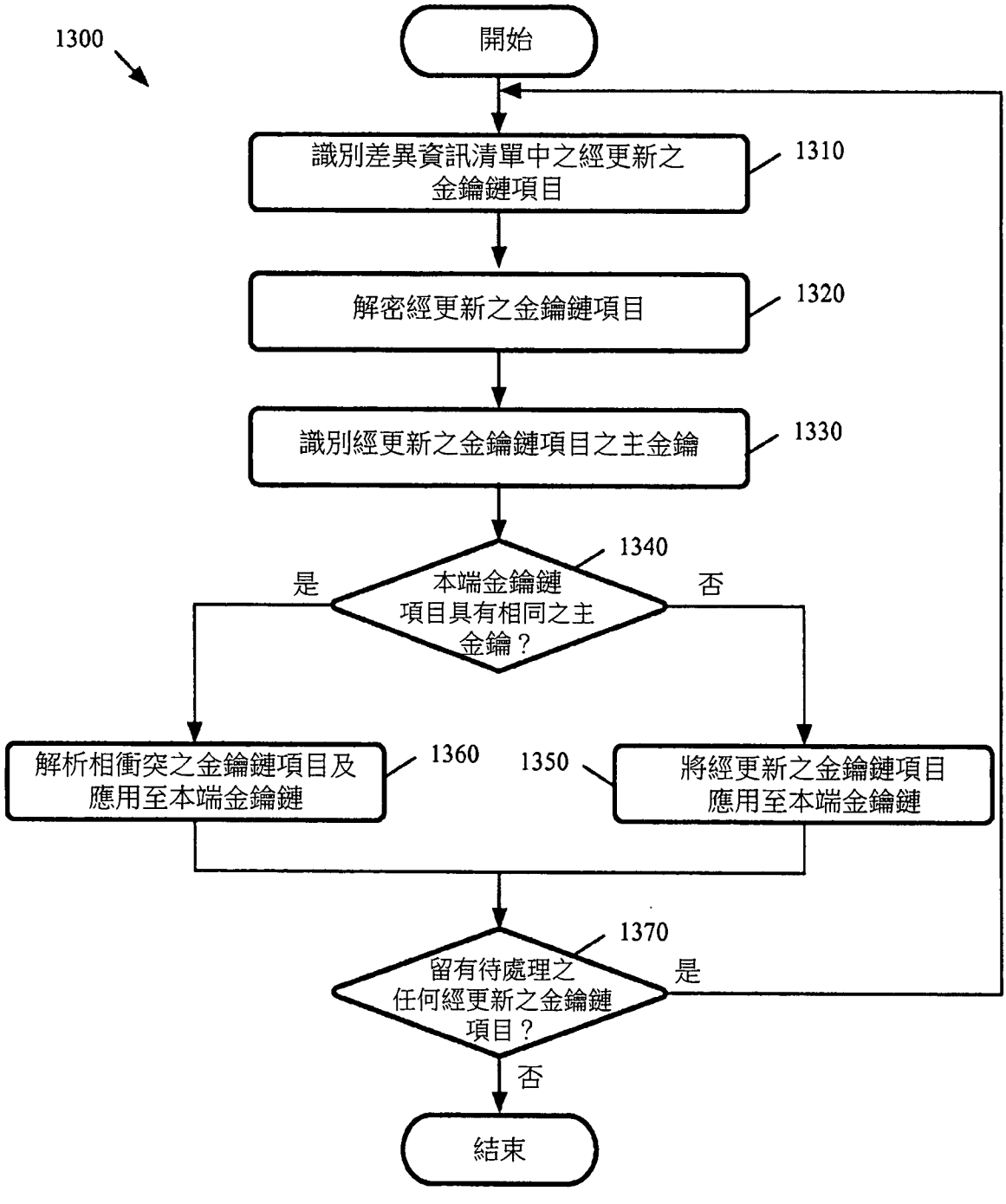
1300
開始
識別差異資訊清單中之經更新之金鑰鏈項目
1310
解密經更新之金鑰鏈項目
1320
識別經更新之金鑰鏈項目之主金鑰
1330
1340
本端金鑰鏈項目具有相同之主金鑰？
是
否
解析相衝突之金鑰鏈項目及應用至本端金鑰鏈
1360
1350
將經更新之金鑰鏈項目應用至本端金鑰鏈
1370
留有待處理之任何經更新之金鑰鏈項目？
是
否
結束

圖13

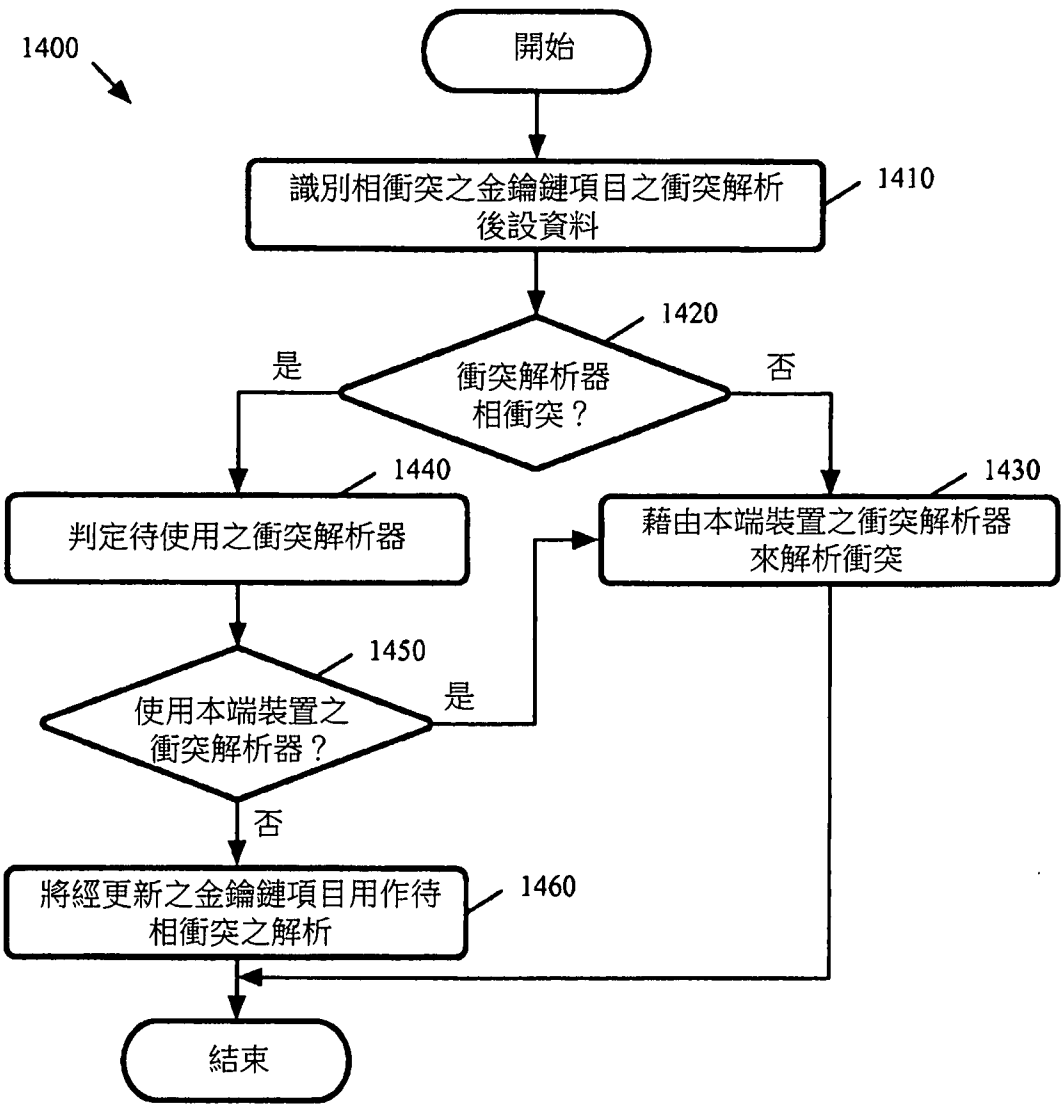
1400
開始
識別相衝突之金鑰鏈項目之衝突解析後設資料
1410
1420
衝突解析器相衝突？
是
否
1440
判定待使用之衝突解析器
1430
藉由本端裝置之衝突解析器來解析衝突
1450
使用本端裝置之衝突解析器？
是
否
將經更新之金鑰鏈項目用作待相衝突之解析
1460
結束

圖14

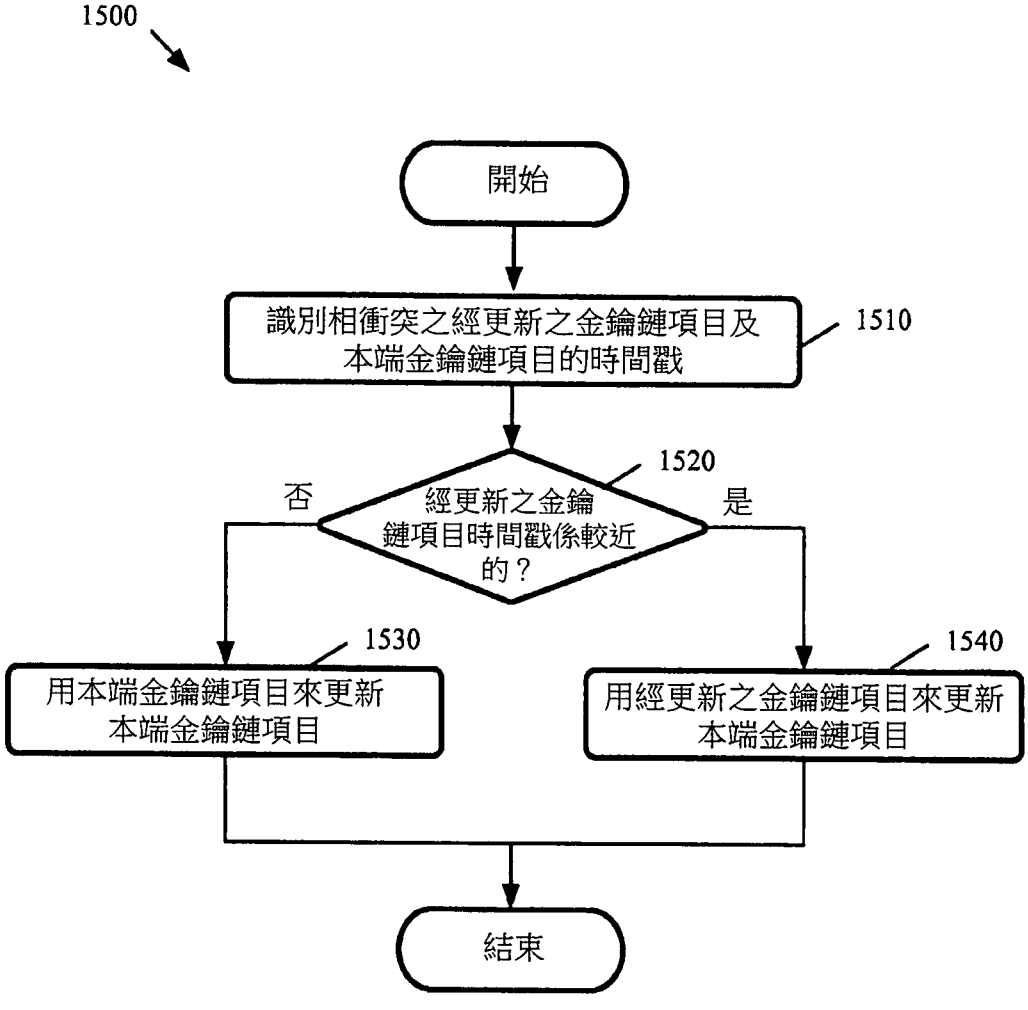
1500
開始
識別相衝突之經更新之金鑰鏈項目及本端金鑰鏈項目的時間戳
1510
1520
經更新之金鑰鏈項目時間戳係較近的？
否
是
1530
用本端金鑰鏈項目來更新本端金鑰鏈項目
1540
用經更新之金鑰鏈項目來更新本端金鑰鏈項目
結束

圖15

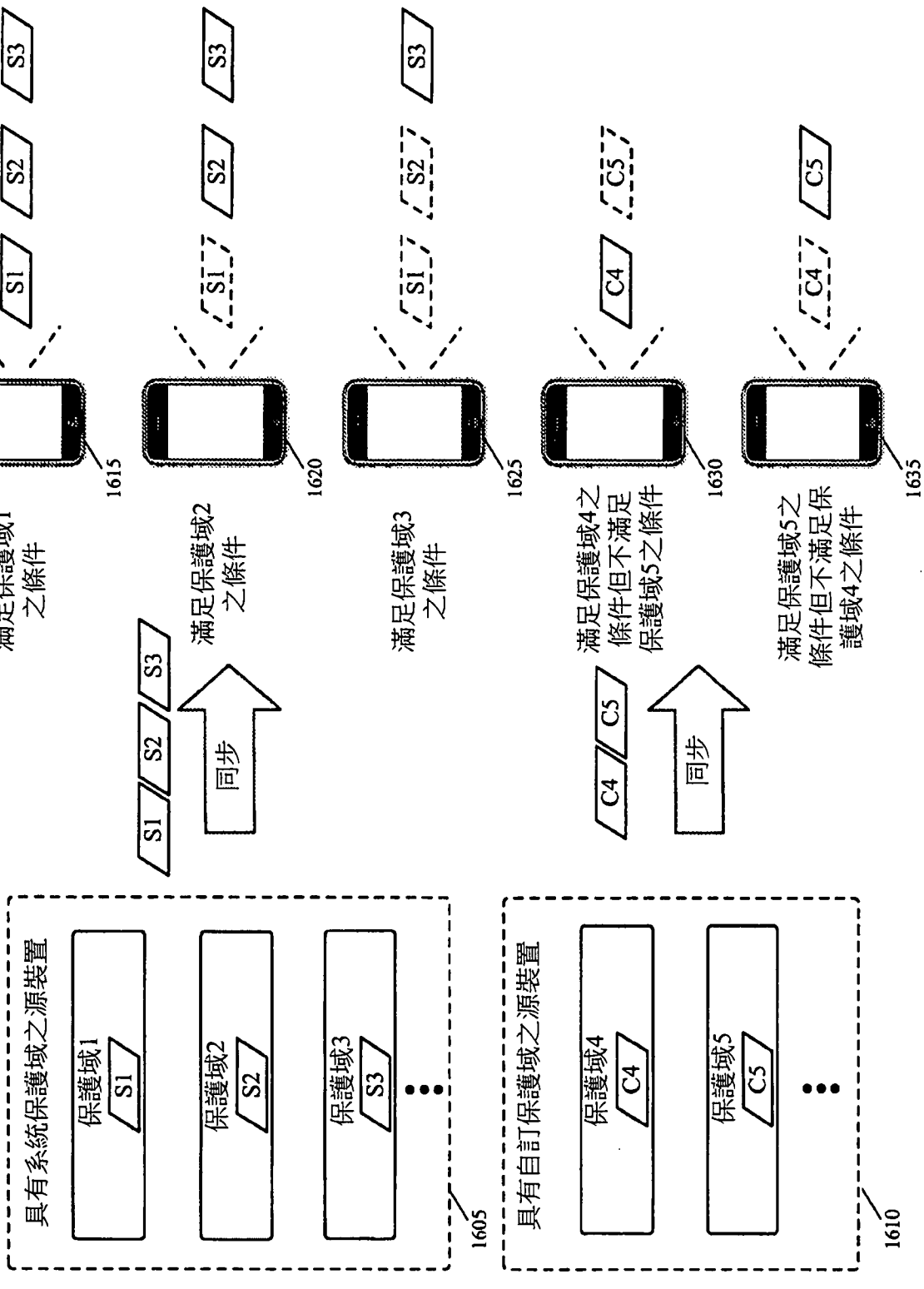
具有系統保護域之源裝置
保護域1
S1
保護域2
S2
保護域3
S3
1605
具有自訂保護域之源裝置
保護域4
C4
保護域5
C5
1610
S1
S2
S3
同步
C4
C5
同步
滿足保護域1之條件
滿足保護域2之條件
滿足保護域3之條件
滿足保護域4之條件但不滿足保護域5之條件
滿足保護域5之條件但不滿足保護域4之條件
1615
1620
1625
1630
1635

圖16

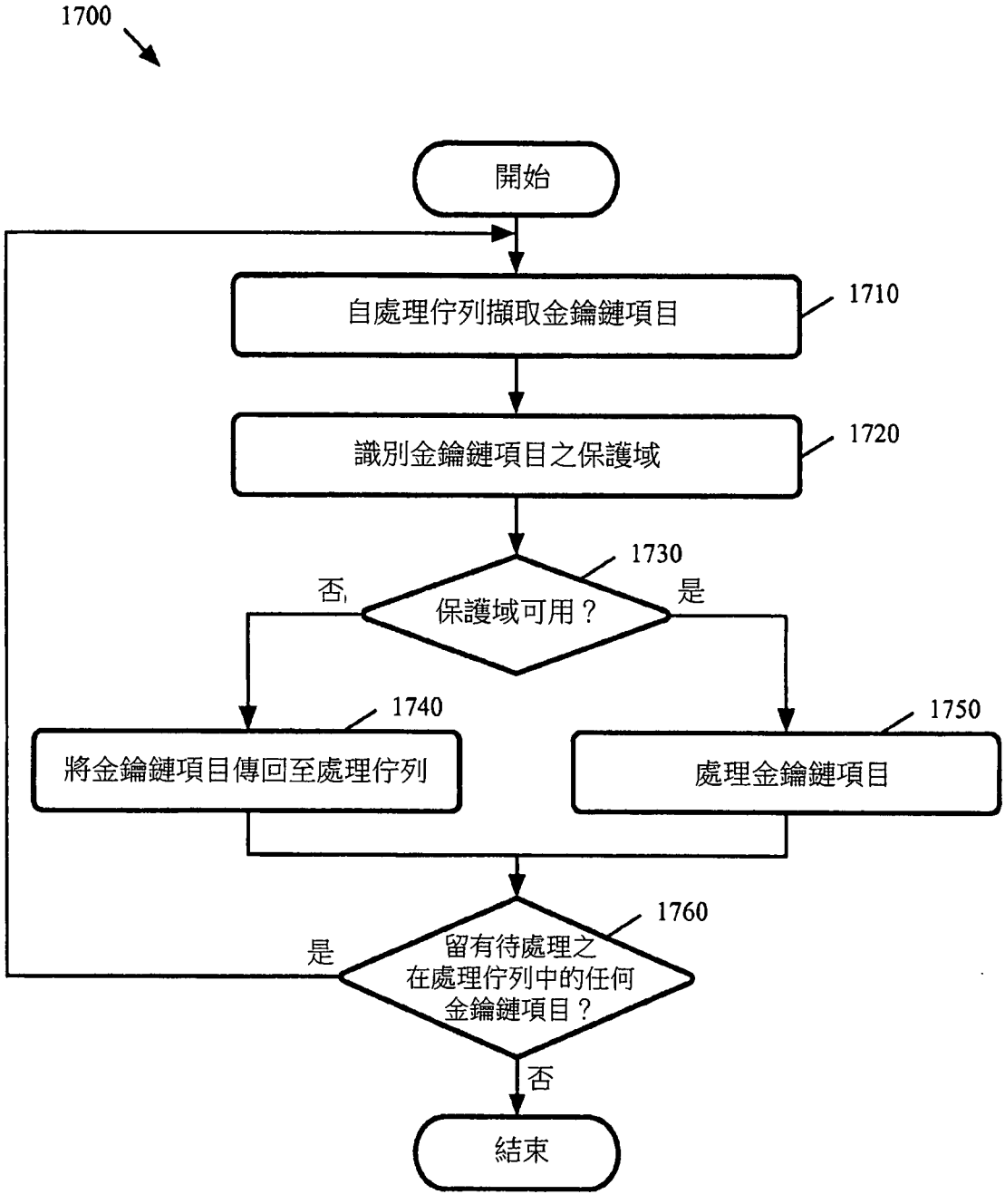
1700
開始
自處理佇列擷取金鑰鏈項目
1710
識別金鑰鏈項目之保護域
1720
1730
否
保護域可用？
是
1740
將金鑰鏈項目傳回至處理佇列
1750
處理金鑰鏈項目
1760
是
留有待處理之
在處理佇列中的任何
金鑰鏈項目？
否
結束

圖17

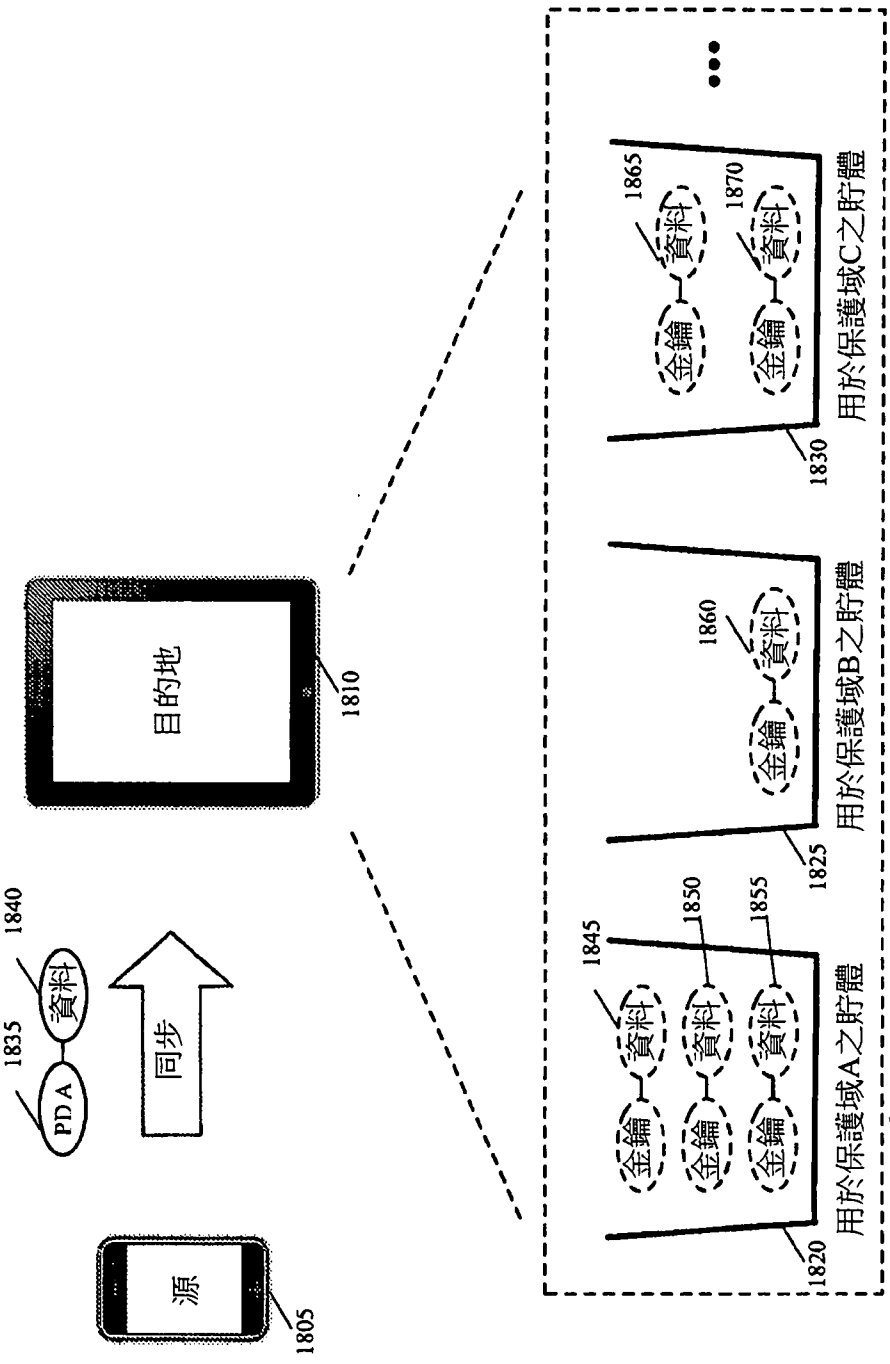
源
1805
PDA
資料
1835
1840
同步
目的地
1810
用於保護域A之貯體
1815
1820
金鑰
資料
1845
1850
1855
用於保護域B之貯體
1825
1860
用於保護域C之貯體
1830
1865
1870

圖18

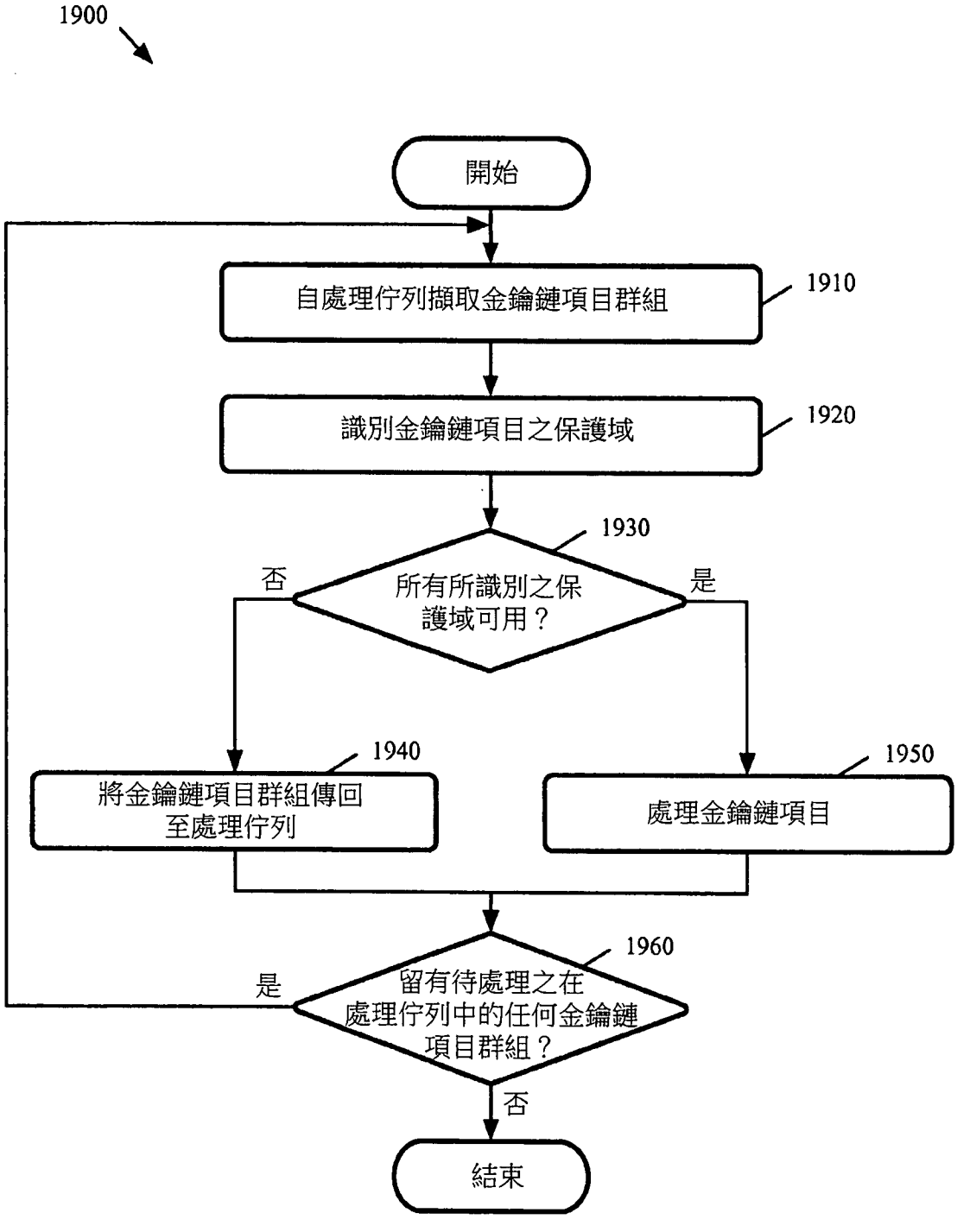
1900
開始
自處理佇列擷取金鑰鏈項目群組
1910
識別金鑰鏈項目之保護域
1920
1930
所有所識別之保護域可用？
否
是
1940
將金鑰鏈項目群組傳回至處理佇列
1950
處理金鑰鏈項目
1960
留有待處理之在處理佇列中的任何金鑰鏈項目群組？
是
否
結束

圖19

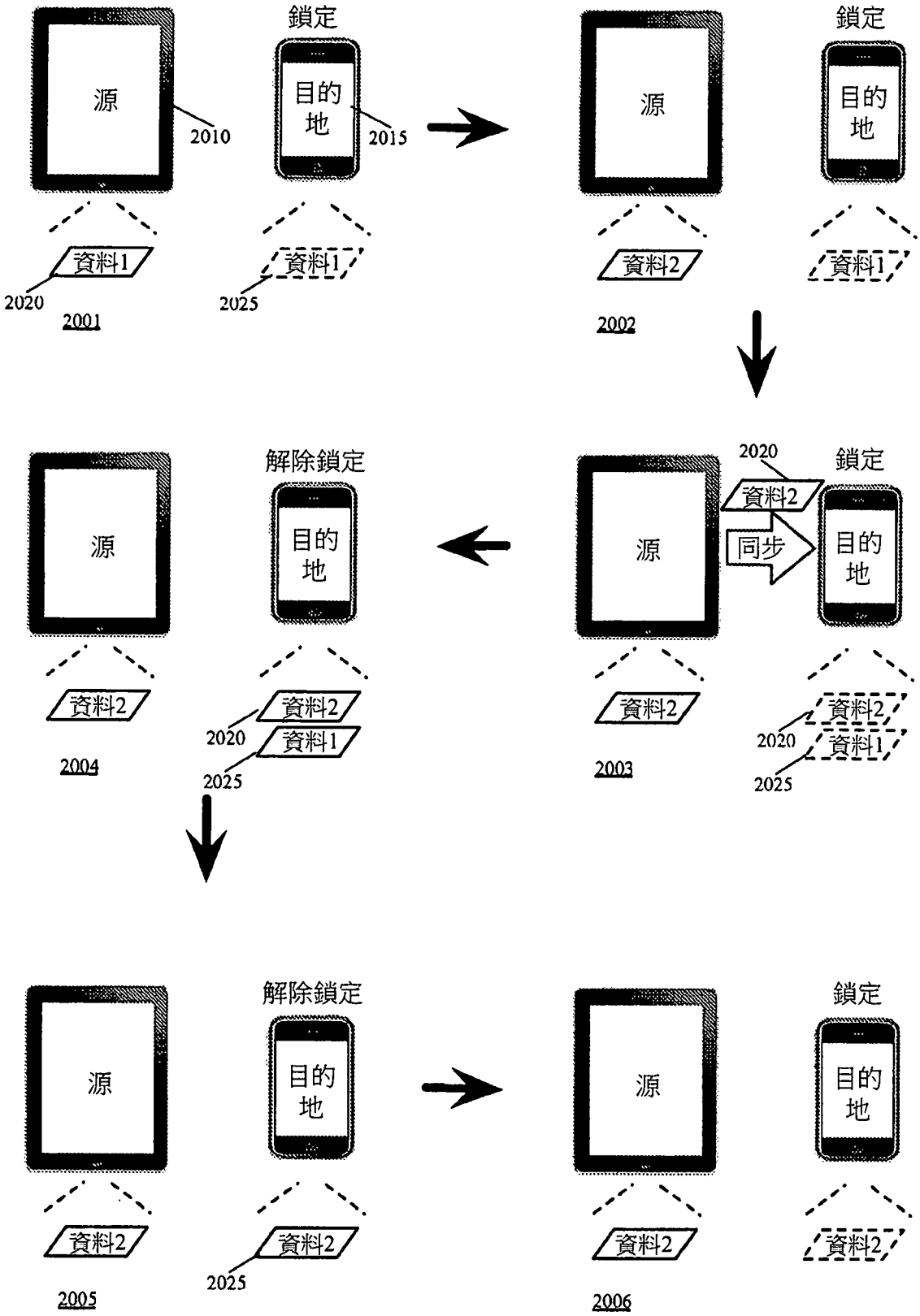
源
2010
鎖定
目的地
2015
資料1
2020
2025
2001
源
鎖定
目的地
資料2
資料1
2002
源
2020
資料2
同步
鎖定
目的地
資料2
2020
資料1
2025
2003
源
解除鎖定
目的地
資料2
2020
資料1
2025
2004
源
解除鎖定
目的地
資料2
2025
2005
源
鎖定
目的地
資料2
2006

圖20

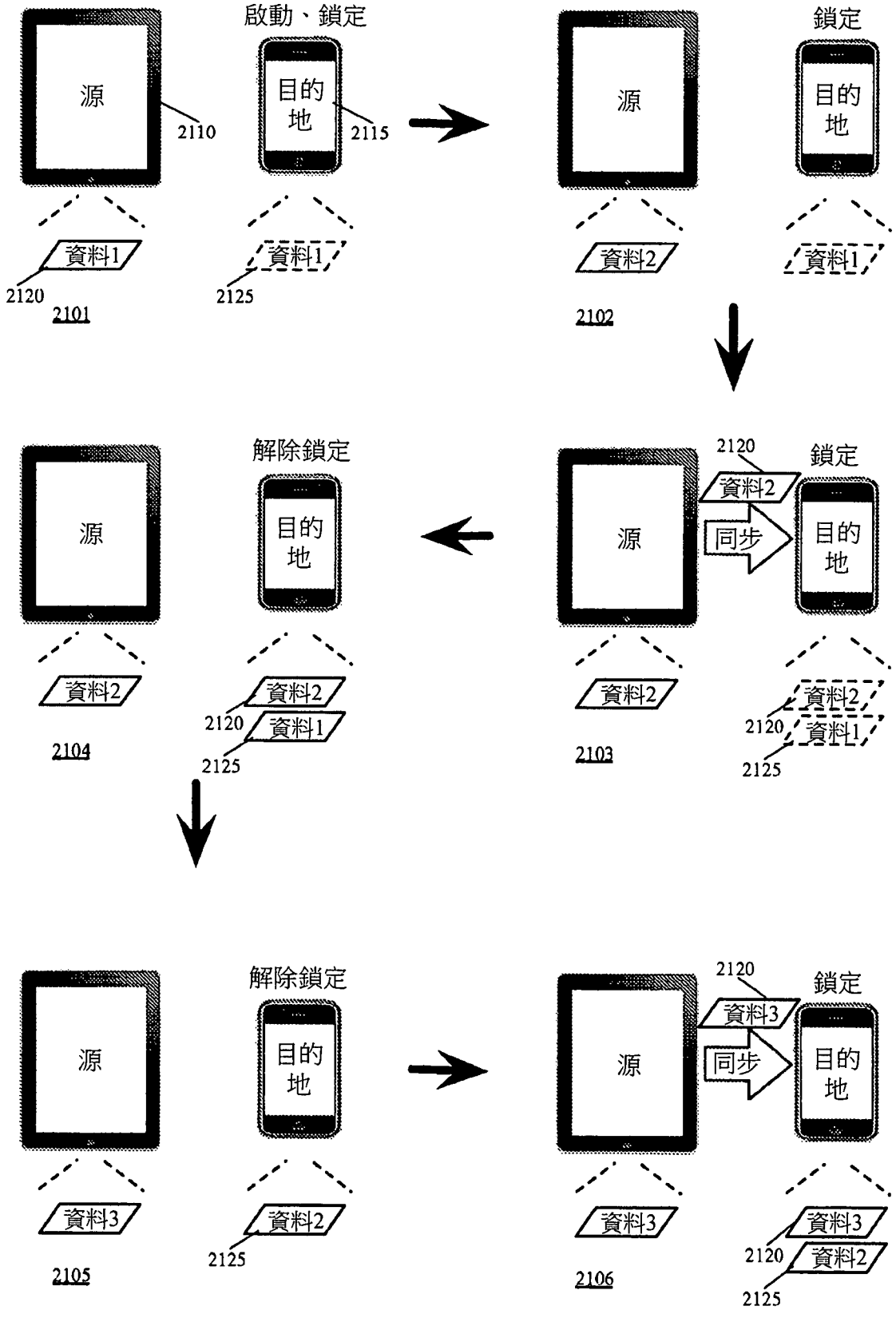
啟動、鎖定
源
目的地
2110
2115
資料1
2120
2125
2101
鎖定
資料2
2102
解除鎖定
同步
2103
2104
2105
2106

圖21

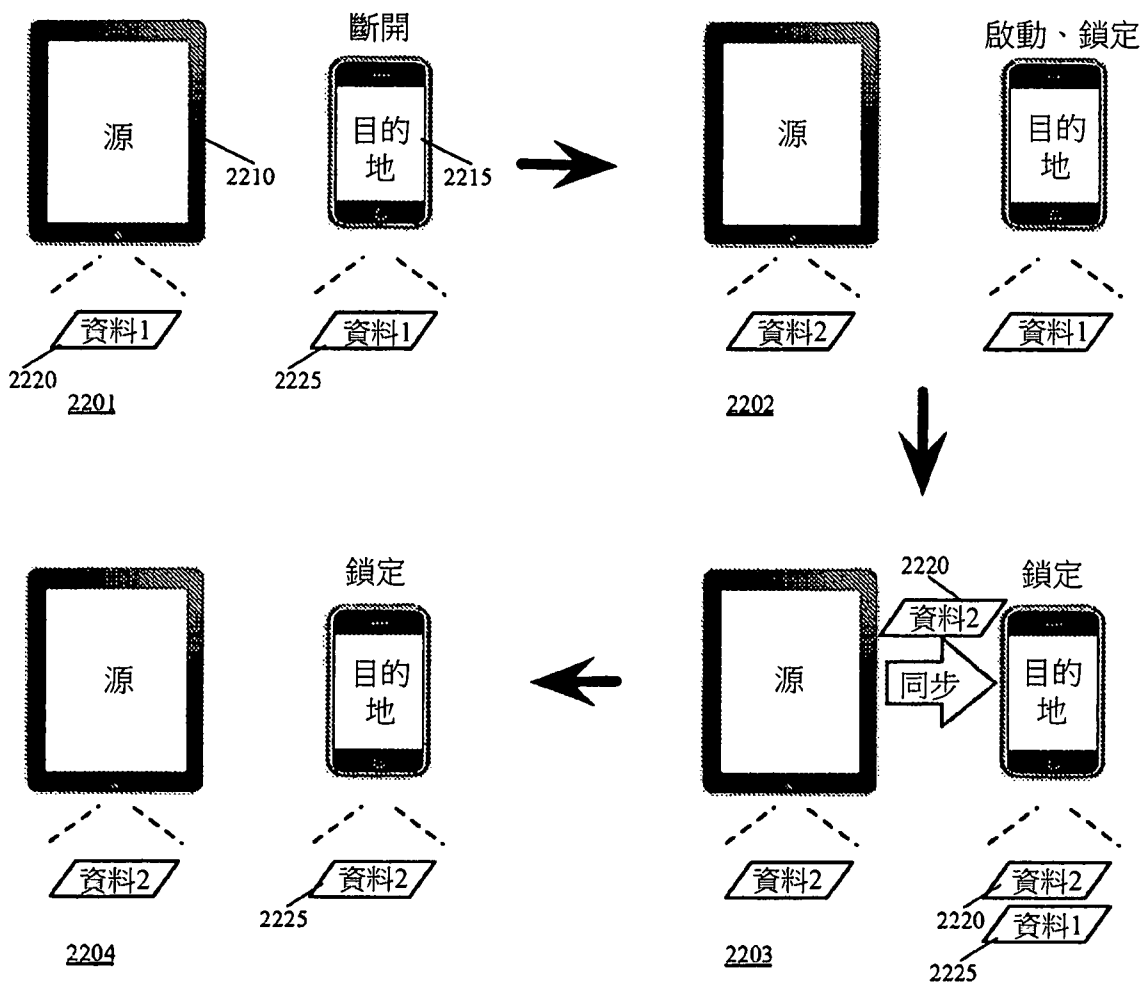
源
2210
斷開
目的地
2215
資料1
2220
2201
資料1
2225
源
啟動、鎖定
目的地
資料2
2202
資料1
源
2220
資料2
同步
鎖定
目的地
資料2
2203
資料2
2220
資料1
2225
源
鎖定
目的地
資料2
2204
資料2
2225

圖22

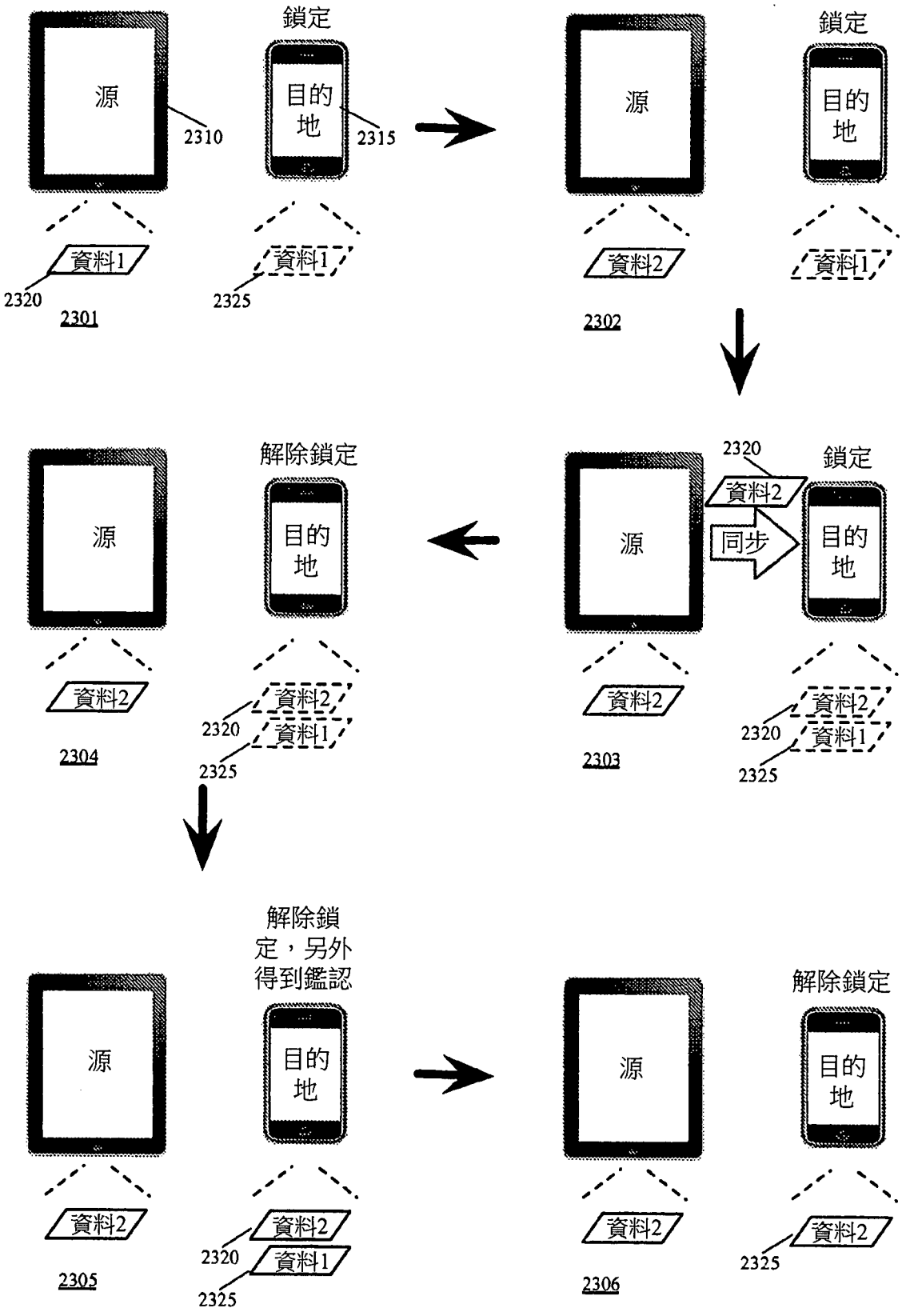
源
2310
鎖定
目的地
2315
資料1
2320
資料1
2325
2301
源
鎖定
目的地
資料2
資料1
2302
源
2320
資料2
同步
鎖定
目的地
資料2
資料2
2320
資料1
2325
2303
源
解除鎖定
目的地
資料2
資料2
2320
資料1
2325
2304
源
解除鎖定，另外得到鑑認
目的地
資料2
資料2
2320
資料1
2325
2305
源
解除鎖定
目的地
資料2
資料2
2325
2306

圖23

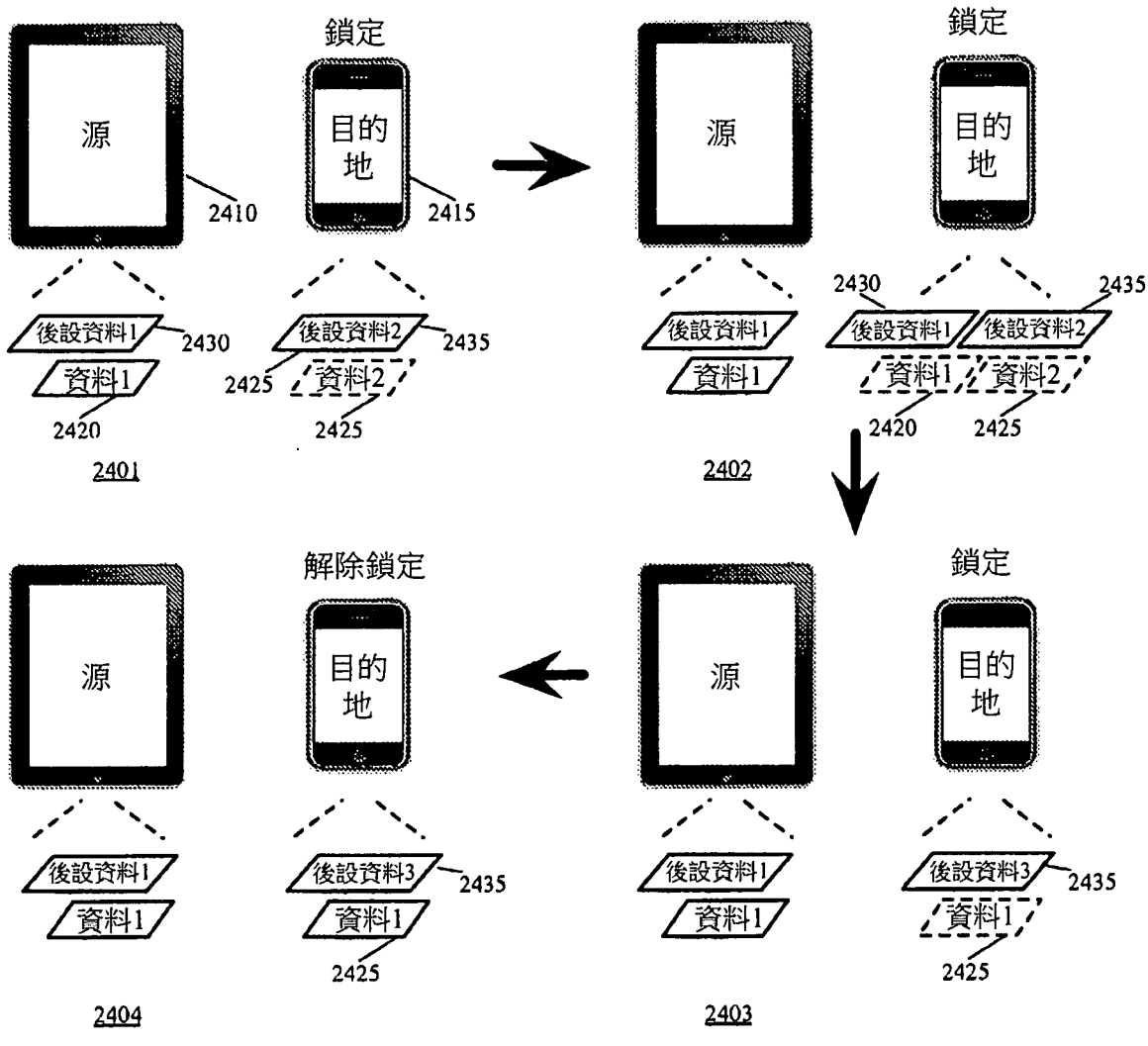
源
2410
鎖定
目的地
2415
後設資料1
2430
資料1
2420
後設資料2
2435
2425
資料2
2425
2401
源
後設資料1
資料1
2402
鎖定
目的地
2430
後設資料1
2435
後設資料2
資料1
資料2
2420
2425
源
後設資料1
資料1
2403
鎖定
目的地
後設資料3
2435
資料1
2425
解除鎖定
目的地
後設資料3
2435
資料1
2425
源
後設資料1
資料1
2404

圖24

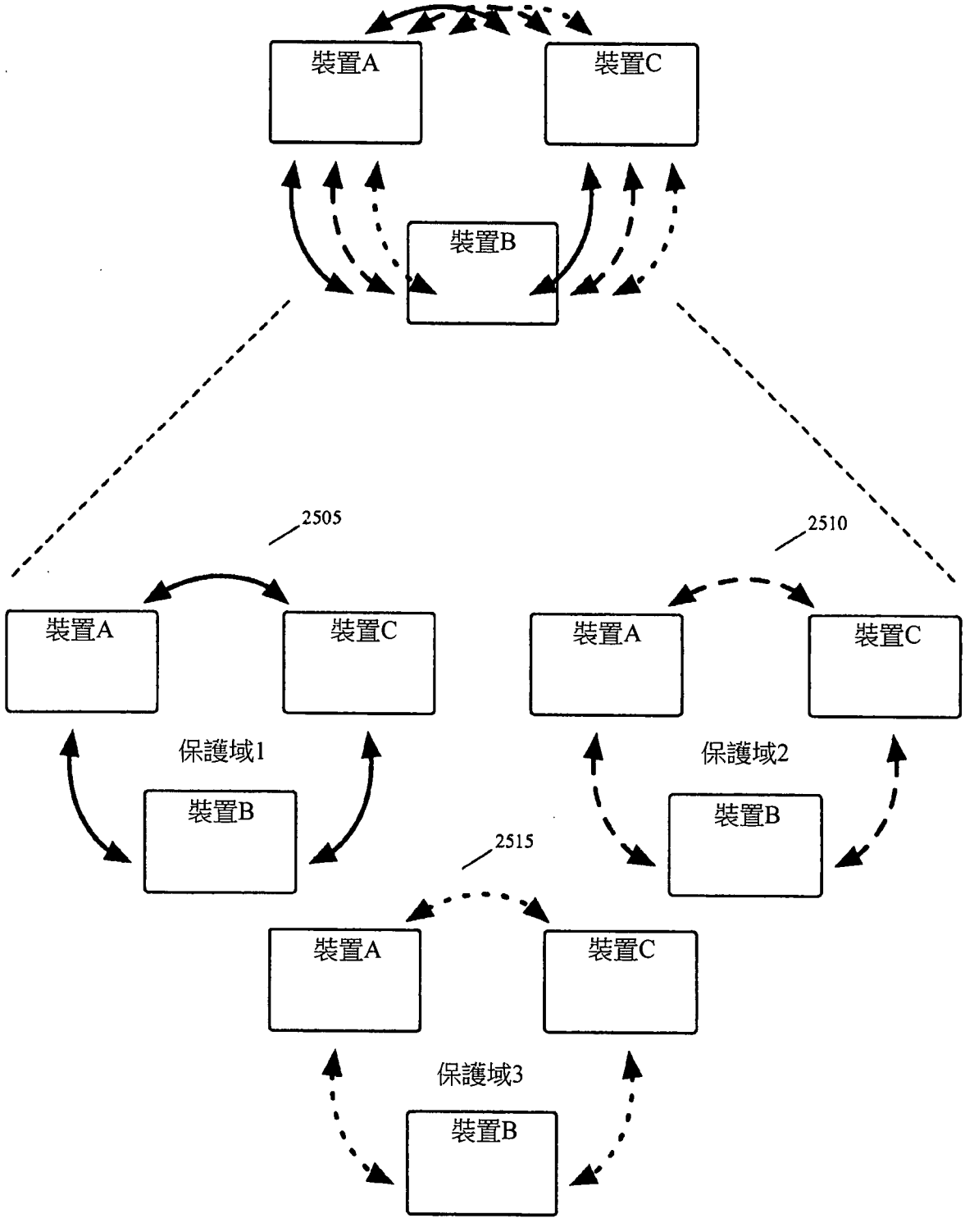
裝置A
裝置C
裝置B
2505
2510
裝置A
裝置C
裝置A
裝置C
保護域1
保護域2
裝置B
裝置B
2515
裝置A
裝置C
保護域3
裝置B

圖25

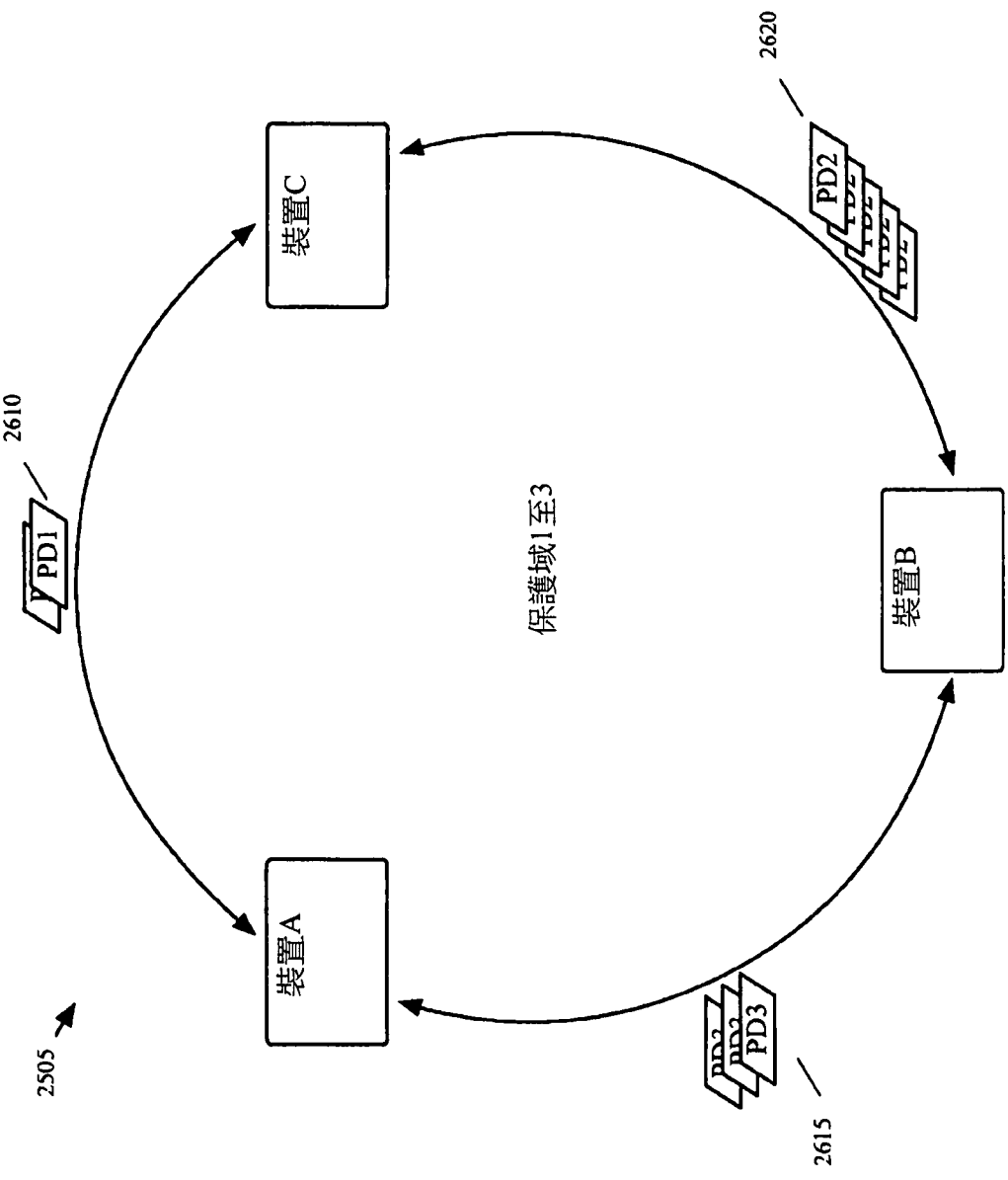

圖26

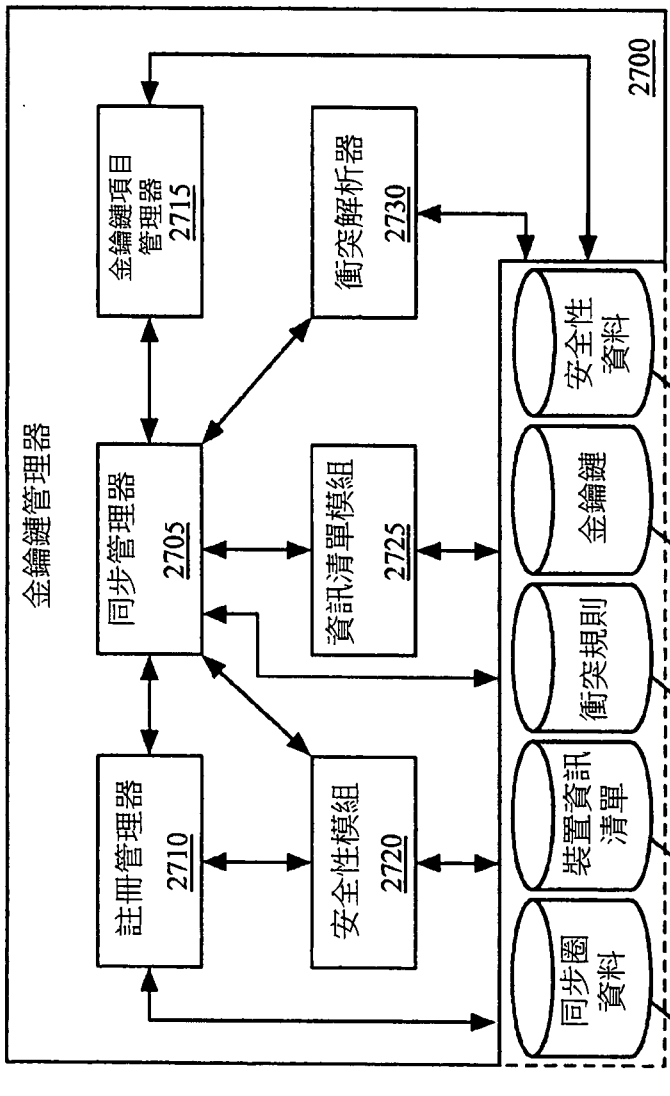
金鑰鏈管理器
同步管理器 2705
註冊管理器 2710
安全性模組 2720
資訊清單模組 2725
金鑰鏈項目管理器 2715
衝突解析器 2730
2700
同步圈資料
裝置資訊清單
衝突規則
金鑰鏈
安全性資料
2735
2740
2745
2750
2755

圖27

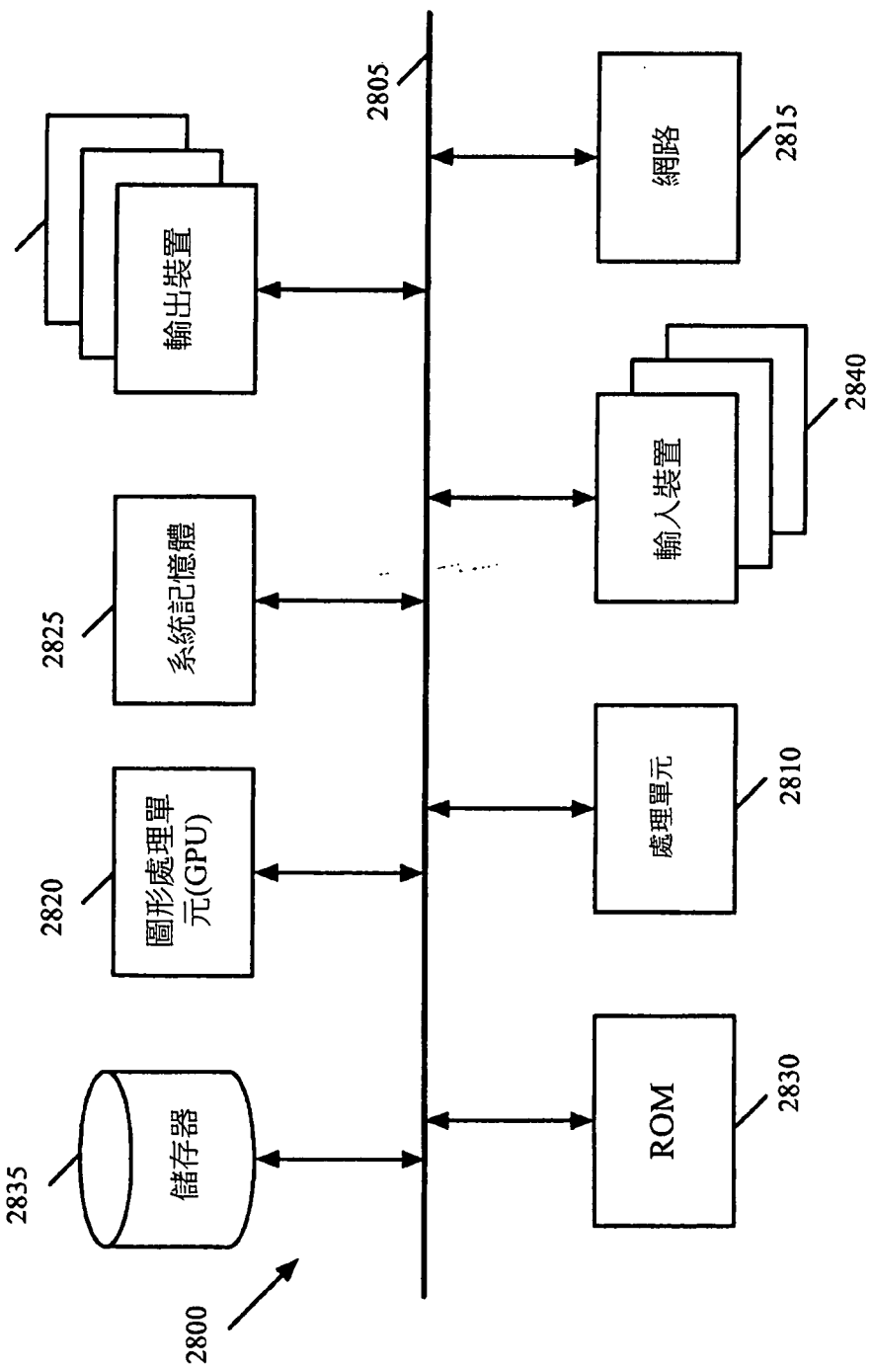
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
處理單元
網路
圖形處理單元(GPU)
系統記憶體
ROM
儲存器
輸入裝置
輸出裝置

圖28