I420339

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I420339 B**

(45)公告日： 中華民國 102 (2013) 年 12 月 21 日

(21)申請案號：099138622 (22)申請日： 中華民國 99 (2010) 年 11 月 10 日

(51)Int. Cl.： *G06F21/31 (2013.01)*

(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)

新竹縣竹東鎮中興路 4 段 195 號

(72)發明人：高銘智 KAO, MING CHIH (TW)

(74)代理人：陳昭誠

(56)參考文獻：

TW	I303764	US	6983371B1
US	7415618B2	US	7430670B1
US	2004/0181489A1	US	2010/0070381A1

審查人員：謝進忠

申請專利範圍項數：16 項 圖式數：4 共 0 頁

(54)名稱

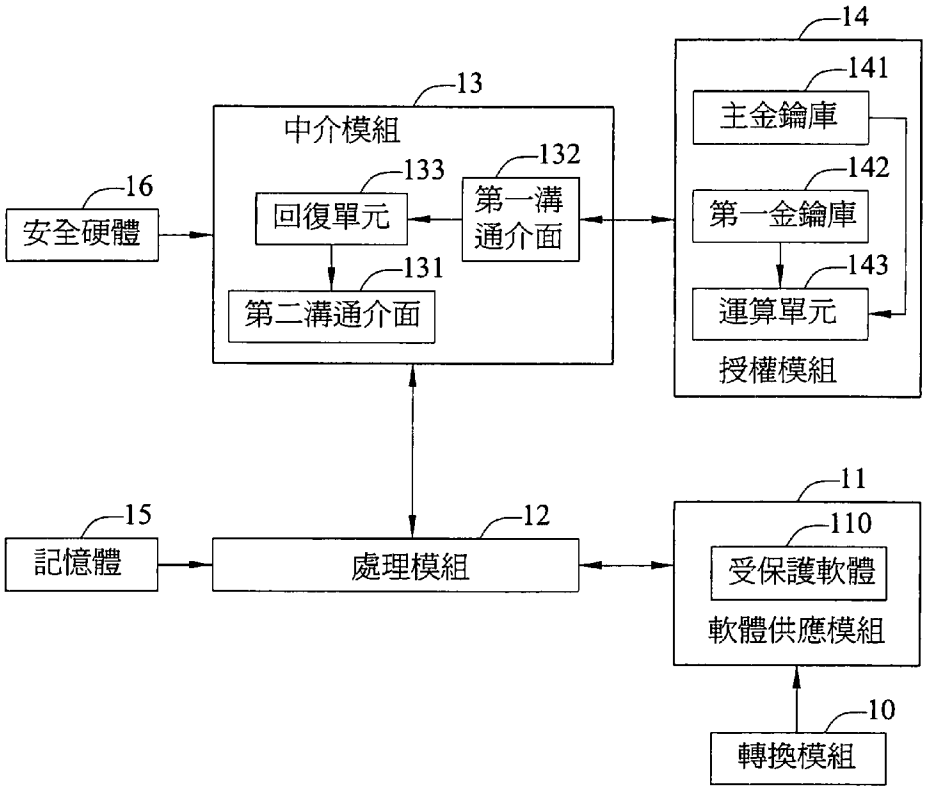
軟體授權系統及方法

SOFTWARE AUTHORIZATION SYSTEM AND METHOD

(57)摘要

一種軟體授權系統及方法，該系統包括伺服端和用戶端。首先，於用戶端自伺服端下載受保護軟體時取得該受保護軟體的軟體識別碼，並將該軟體識別碼及自身所具有之用戶識別碼傳輸至伺服端，接著，伺服端依據該用戶識別碼及該軟體識別碼分別取得相對應的第一金鑰及主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰並傳輸至用戶端，最後，由用戶端結合自身所具有之第一金鑰回復出該主金鑰，再利用該主金鑰對該受保護軟體進行解密。據此，得以增加下載解密受保護軟體的難度，抑止非法下載或合法下載而非法散佈軟體者。

The invention provides a software authorization system having a server end and a user end and a method thereof, the method comprising acquiring a software identification code when the user end downloads the protected software from the server end; transmitting the identification code and the inherent user ID code from the user end to the server end; acquiring the corresponding first key and main key respectively by the server end according to the acquired codes for engendering a second key and further transmitting the second key to the user end; and restoring the main key using the inherent first key by the user end to decrypt the protected software, thereby complicating the process of downloading protected software to help stop the spread of protected software.



第1圖

10・・・轉換模組

11・・・軟體供應模組

110・・・受保護軟體

12・・・處理模組

13・・・中介模組

131・・・第二溝通介面

132・・・第一溝通介面

133・・・回復單元

14・・・授權模組

141・・・主金鑰庫

142・・・第一金鑰庫

143・・・運算單元

15・・・記憶體

16・・・安全硬體

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99138622

※申請日：99.11.10　※IPC分類：G06F21/31 (2006.01)

一、發明名稱：（中文/英文）

軟體授權系統及方法

SOFTWARE AUTHORIZATION SYSTEM AND METHOD

二、中文發明摘要：

一種軟體授權系統及方法，該系統包括伺服端和用戶端。首先，於用戶端自伺服端下載受保護軟體時取得該受保護軟體的軟體識別碼，並將該軟體識別碼及自身所具有之用戶識別碼傳輸至伺服端，接著，伺服端依據該用戶識別碼及該軟體識別碼分別取得相對應的第一金鑰及主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰並傳輸至用戶端，最後，由用戶端結合自身所具有之第一金鑰回復出該主金鑰，再利用該主金鑰對該受保護軟體進行解密。據此，得以增加下載解密受保護軟體的難度，抑止非法下載或合法下載而非法散佈軟體者。

三、英文發明摘要：

The invention provides a software authorization system having a server end and a user end and a method thereof, the method comprising acquiring a software identification code when the user end downloads the protected software from the server end; transmitting the identification code and the inherent user ID code from the user end to the server end; acquiring the corresponding first key and main key respectively by the server end according to the acquired codes for engendering a second key and further transmitting the second key to the user end; and restoring the main key using the inherent first key by the user end to decrypt the protected software, thereby complicating the process of downloading protected software to help stop the spread of protected software.

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

10	轉換模組
11	軟體供應模組
110	受保護軟體
12	處理模組
13	中介模組
131	第二溝通介面
132	第一溝通介面
133	回復單元
14	授權模組
141	主金鑰庫
142	第一金鑰庫
143	運算單元
15	記憶體
16	安全硬體

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

六、發明說明：

【發明所屬之技術領域】

本揭露有關一種軟體授權系統及方法，詳而言之，係涉及一種無需傳輸加密軟體的主金鑰之軟體授權系統及方法。

【先前技術】

內容傳遞網絡(Content Delivery Network；CDN)技術的發展可提高網站回應速度，然隨著雲端運算的風行，CDN 這種可以提高網站傳送速率的技術對軟體授權的應用而言卻是一種限制。

CDN 基本上是將軟體(內容)事先複製到全球多台伺服器，因而網站經營者無法針對每次下載的軟體作個別的保護處理，使得許多保護機制必須在客戶端進行。例如，Microsoft 下載網站的作法係將所有認證檢查放在安裝時期，並在執行時期需執行啟動動作。而 App Store 則是讓使用者在下載軟體時產生一把使用者金鑰，再利用金鑰加密金鑰(Key Encrypt Key；KEK)方式將所謂的主金鑰加密傳送給使用者，故當使用者下載完軟體便可用主金鑰解密。

然而，由於前述這些小程式很容易被逆向工程攻擊，尤其例如 Java byte code，因此 Microsoft 下載網站的作法不適用於軟體市集所賣的小程式，而 App Store 的作法則已被證實有心者可取得使用者金鑰進而於下載程式後多次轉載。另一方面，習知技術亦提出一種軟體授權與保護裝置及方法，係於第一次使用時於用戶端產生註冊碼(random

number-MAC address、硬碟序列碼、軟體名稱)並加密，再向授權系統註冊及寫入資料庫，惟此案每次執行時需線上檢查許可狀態，且取得 MAC address 或硬碟序號已為習知技術，僅需簡單協定分析即可複製相同的參數。其次，另有一種用於協助內容金鑰改變之方法及裝置，能從主金鑰和內容規則導出 CEK，則利用同一把金鑰即可進行加解密，使用者仍可多次複製檔案或內容。此外，相關論文的基本假設為程式被分離成受保護程式及安全參數，其安全參數可被多種裝置重複使用，因而使用者仍可破解程式後多次轉載，若考量安全而作成有差異的安全參數，則由於受保護程式和安全參數需成對使用而使得無法使用 CDN 技術。

是以，如何提供一種軟體授權系統及方法，得以防止合法下載而非法散佈軟體者，在軟體市集中所販賣的軟體生命週期普遍皆不長的情況下，為目前軟體開發業者亟待解決的議題之一。

【發明內容】

本揭露提供一種軟體授權系統及方法，得以增加下載及解密軟體的難度，抑止非法下載或合法下載而非法散佈軟體者。

本揭露提供一種軟體授權系統，包括：軟體供應模組，係提供以主金鑰進行加密的受保護軟體，且該受保護軟體具有軟體識別碼；處理模組，用以自該軟體供應模組下載該受保護軟體，並輸出所下載之受保護軟體的軟體識

別碼；中介模組，係具有用戶識別碼及與該用戶識別碼對應的第一金鑰，且該中介模組用以接收該處理模組所輸出之軟體識別碼；以及授權模組，具有主金鑰庫和第一金鑰庫，該授權模組接收該中介模組所輸出之用戶識別碼及該軟體識別碼，並根據該用戶識別碼及該軟體識別碼分別至該主金鑰庫搜尋與該軟體識別碼相對應的主金鑰及至該第一金鑰庫搜尋與該用戶識別碼對應的第一金鑰，其中，該授權模組以該主金鑰及該第一金鑰進行運算而產生第二金鑰並將該第二金鑰傳輸至該中介模組，以由該中介模組依據自身所具有之第一金鑰結合所接收的該第二金鑰回復出該主金鑰，使該處理模組利用該主金鑰對所下載之受保護軟體進行解密。

於一實施形態中，本揭露軟體授權系統復包括轉換模組，用以將至少一軟體以該主金鑰加密的方式轉換為該受保護軟體並傳輸至該軟體供應模組，復用以將該軟體區分為複數個區塊並利用該主金鑰分別對該些區塊進行加密而轉換為該受保護軟體，藉此混淆該軟體的資料結構和控制程序，而該處理模組係利用該中介模組所回復出的主金鑰分別對該些區塊解密。

本揭露還提供一種軟體授權方法，用於包括伺服端和用戶端的軟體授權系統中，該用戶端具有用戶識別碼和對應該用戶識別碼之第一金鑰，該伺服端具有提供以主金鑰進行加密之受保護軟體的軟體供應模組及儲存有該主金鑰和該第一金鑰的授權模組。該軟體授權方法包括以下步

驟：(1)令用戶端自該軟體供應模組下載受保護軟體時取得該受保護軟體的軟體識別碼，並將自身所具有之用戶識別碼及該受保護軟體的軟體識別碼傳輸至該授權模組；(2)令該授權模組依據該用戶識別碼取得相對應的第一金鑰，並根據該軟體識別碼取得相對應的主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰，並將該第二金鑰傳輸至該中介模組；(3)令該用戶端依據自身所具有之第一金鑰結合所接收的第二金鑰以回復出該主金鑰；以及(4)令該用戶端利用所回復出的主金鑰對下載之受保護軟體進行解密。

本揭露改善原先軟體市集的弱點，更增加攻擊者的破解難度，且由於每個中介模組(或用戶端)具有不同的第一金鑰，因而自授權模組取得之第二金鑰亦不同，進而可抑止合法下載而非法散佈軟體者。

【實施方式】

以下藉由特定的具體實施形態說明本揭露之實施方式，熟悉此技術之人士可由本說明書所揭示之內容輕易地了解本揭露之其他優點與功效，亦可藉由其他不同的具體實施形態加以施行或應用。

請參閱第 1 圖，本揭露之軟體授權系統包括軟體供應模組 11、處理模組 12、中介模組 13 和授權模組 14。

軟體供應模組 11 用以提供以主金鑰加密的方式而成為之受保護軟體 110，受保護軟體 110 具有軟體識別碼。具體言之，軟體供應模組 11 可提供複數種受保護軟體

110(即各種應用程式)，該些受保護軟體 110 具有各自的軟體識別碼。於一實施形態中，本揭露之軟體授權系統復包括轉換模組 10，轉換模組 10 透過加密、混淆或區分等方式將軟體轉換為受保護軟體 110 並傳輸至軟體供應模組 11。於進行加密時，轉換模組 10 可將軟體區分為數個區塊，並利用與軟體識別碼相對應的主金鑰分別加密該些區塊，藉此混淆軟體的資料結構和控制程序，使之成為受保護軟體 110。

處理模組 12 用以自軟體供應模組 11 下載受保護軟體 110，並將所下載的受保護軟體 110 的軟體識別碼傳輸至中介模組 13。

中介模組 13 具有用戶識別碼及與用戶識別碼相對應的第一金鑰，且接收處理模組 12 所傳輸之軟體識別碼，並將用戶識別碼及所下載的受保護軟體 110 的軟體識別碼傳輸至授權模組 14。此外，該第一金鑰可利用混淆技術設置於中介模組 13 中，讓使用者難以存取到該第一金鑰。再者，轉換模組 10 亦可於軟體中加入完整性檢查參數以使其成為受保護軟體 110 再傳輸至軟體供應模組 11，以供中介模組 13 確定受保護軟體 110 是否被竄改。

授權模組 14 具有主金鑰庫 141 和第一金鑰庫 142。主金鑰庫 141 儲存有與受保護軟體 110 的軟體識別碼相對應的主金鑰，第一金鑰庫 142 儲存有與中介模組 13 的用戶識別碼(可是 random number-MAC address、硬碟序列碼、軟體名稱等組合，不限於此，只要能代表用戶端即可)相對應

的第一金鑰。授權模組 14 接收中介模組 13 所傳輸之用戶識別碼及軟體識別碼，並根據該用戶識別碼至第一金鑰庫 142 中搜尋相對應的第一金鑰，根據該軟體識別碼至主金鑰庫 141 搜尋相對應的主金鑰。此外，授權模組 14 以所搜尋出的主金鑰和第一金鑰透過運算單元 143 進行運算而產生第二金鑰，並將該第二金鑰傳輸至中介模組 13，以由中介模組 13 再依據自身所具有的第一金鑰結合所接收之第二金鑰回復出該主金鑰，即授權模組 14 所搜尋出的主金鑰，亦即用以對軟體加密使之成為受保護軟體 110 的主金鑰，進而使處理模組 12 利用該主金鑰對所下載的受保護軟體 110 進行解密。

於軟體供應模組 11 所提供之受保護軟體 110 有被區分為數個區塊的實施形態中，處理模組 12 對受保護軟體 110 的數個區塊以中介模組 13 所回復出的主金鑰分別解密。

其次，中介模組 13 和處理模組 12 可皆設置於同一使用者裝置，如手機或筆記型電腦等，亦可分設於不同的電子裝置。於中介模組 13 設置於使用者裝置的實施形態中，中介模組 13 所具有的第一金鑰及自授權模組 14 所接收之第二金鑰可儲存於該使用者裝置的安全硬體 16，如 IC 卡、SIM 卡或 TPM 卡等。於處理模組 12 設置於使用者裝置的實施形態中，處理模組 12 可將解密完畢的軟體儲存至該使用者裝置的記憶體 15。

詳言之，如第 1 圖所示，中介模組 13 具有第二溝通

介面 131、第一溝通介面 132 及回復單元 133，第一溝通介面 132 用以與授權模組 14 溝通以傳輸該用戶識別碼和所下載之受保護軟體 110 的軟體識別碼並接收該第二金鑰，而第二溝通介面 131 用以與處理模組 12 溝通以將回復單元 133 所回復出的主金鑰提供給處理模組 12。

再者，授權模組 14 的運算單元 143 可對主金鑰(KEY)和第一金鑰(K1)執行除斥運算以產生第二金鑰(K2)，即 $K2 = KEY \oplus K1$，然，運算單元 143 所進行的運算方式不受此限，如可使用秘密分享技術(secret sharing scheme)。

由第 1 圖所示之實施形態得以瞭解，本揭露之中介模組具有用戶識別碼及與該用戶識別碼相對應的第一金鑰，並自授權模組取得第二金鑰，當受保護軟體需執行解密及授權檢查時，中介模組利用第一金鑰和第二金鑰回復出主金鑰。由於不同中介模組自授權模組會取得不同的第二金鑰，若用戶欲將軟體安裝至具有另一中介模組的使用者裝置時則須向授權模組再次索取另一把第二金鑰。此外，軟體經混淆(分成數個區塊)及加密而轉換成受保護軟體後，不容易一次解密完畢，若欲不透過第二金鑰而強行解密該受保護軟體，則需分析受保護軟體並將每一區塊重新組合。故，本揭露之軟體授權系統可增加下載解密受保護軟體的難度，抑止非法下載或合法下載而非法散佈軟體者。

接著請參閱第 2 圖，其係本揭露之軟體授權方法之流程圖。本揭露之軟體授權方法係應用於軟體授權系統，該軟體授權系統主要包括伺服端和用戶端，該用戶端具有用

戶識別碼和對應該用戶識別碼的第一金鑰，該伺服端具有提供以主金鑰進行加密之受保護軟體的軟體供應模組及儲存有該主金鑰和該第一金鑰的授權模組。

於步驟 S201 中，令用戶端自軟體供應模組下載受保護軟體時取得該受保護軟體的軟體授權碼，並將自身所具有之用戶識別碼及所取得之軟體識別碼傳輸至授權模組。接著於步驟 S202，令授權模組分別依據該用戶識別碼及該軟體識別碼取得相對應的第一金鑰及主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰，並將該第二金鑰傳輸至用戶端。進至步驟 S203。

於步驟 S203，用戶端接收該第二金鑰，令用戶端依據自身所具有之第一金鑰結合所接收的第二金鑰以回復出該主金鑰，再於步驟 S204 中，利用所回復出的主金鑰對所下載之受保護軟體進行解密。

具體實施時，請參閱第 3A 及 3B 圖，伺服端具有轉換模組 30、軟體供應模組 31 和授權模組 32，用戶端具有中介軟體 33 及安全硬體 34。需說明的是，本揭露於實際應用上，用戶端可例如為智慧型手機，伺服端可提供該智慧型手機下載各種應用程式。

伺服端透過轉換模組 30 將軟體 310'轉換為受保護軟體 310，如第 3B 圖所示，係先將軟體 310'區分為複數個區塊 P1、P2…Pn，再利用主金鑰分別對該些區塊 P1、P2…Pn 加密而使之成為區塊 C1、C2…Cn，則軟體 230'便轉換為受保護軟體 310。接著，伺服端將受保護軟體 310 發佈

至離使用者最近的網路節點，即第 3A 圖所示之軟體供應模組 31，以供用戶端可就近取得所需的內容，解決網絡擁擠的狀況並提高使用者訪問軟體供應網站的響應速度。另一方面，當轉換模組 30 利用不同的主金鑰加密軟體 310' 時，會將該些主金鑰儲存於授權模組 32 的主金鑰庫 321 中，且第一金鑰庫 322 儲存有多把與用戶識別碼相對應的第一金鑰，換言之，伺服端已預先將用戶識別碼與第一金鑰的對應關係儲存於授權模組 32 中。

用戶端自伺服端下載受保護軟體310時可取得受保護軟體 310 的軟體識別碼，並將該軟體識別碼及所具有之用戶識別碼上傳至伺服端，且伺服端的授權模組 32 分別根據該軟體識別碼及該用戶識別碼取得主金鑰和第一金鑰，進而以該第一金鑰和該主金鑰運算出第二金鑰並將該第二金鑰傳輸至用戶端。換言之，當用戶端連結伺服端以下載受保護軟體時，用戶端可藉由軟體供應模組 31 連結至授權模組 32 以取得該第二金鑰。

於伺服端內，安全硬體 34 係儲存有第一金鑰，安全硬體 34 將該第一金鑰傳予中介軟體 33，以供中介軟體 33 依據該第一金鑰及該二金鑰回復出該主金鑰，且中介軟體 33 與受保護軟體 310 建立連線，進而利用該主金鑰解密受保護軟體 310 的複數個區塊 C1、C2…Cn 進而完成對受保護軟體 310 的解密。

綜上所述，本揭露之軟體授權系統可分為伺服端和用戶端，伺服端可包括軟體供應模組和授權模組，用戶端主

要包括中介模組(或中介軟體)並可包括處理模組。伺服端可事先將受保護軟體放到 CDN 的伺服器上以減少下載反應時間，且每個用戶端有不同的第一金鑰。伺服端可利用處理模組下載受保護軟體，中介模組輸出軟體識別碼及對應該第一金鑰的用戶識別碼至授權模組，供授權模組搜尋出相對應的主金鑰和第一金鑰以算出第二金鑰，則用戶端依據自身所具有的第一金鑰結合所接收之第二金鑰回復出該主金鑰，以與所下載的受保護軟體建立連線而共同對受保護軟體中的區塊解密。

因此，藉由本揭露之軟體授權系統及其方法的應用，攻擊者需多次分散下載受保護軟體，還須先分析中介模組與授權模組的通訊協定取得第二金鑰，更要分析中介模組以取得其中的第一金鑰，最後還要分析下載受保護軟體的解密流程才可能完全解密受保護軟體。因此，攻擊者不容易發展出全自動工具給一般使用者使用，如此可以阻止非法下載或合法下載而非法散佈軟體者，以增加軟體存活時間，而這也剛好符合軟體市集所販賣軟體的生命週期不長的特性。

上述實施形態僅例示性說明本揭露之原理、特點及其功效，並非用以限制本揭露之可實施範疇，任何熟習此項技藝之人士均可在不違背本揭露之精神及範疇下，對上述實施形態進行修飾與改變。任何運用本揭露所揭示內容而完成之等效改變及修飾，均仍應為下述之申請專利範圍所涵蓋。因此，本揭露之權利保護範圍，應如後述之申請專

利範圍所列。

【圖式簡單說明】

第1圖係本揭露之軟體授權系統之應用架構圖之示意圖；

第2圖係本揭露之軟體授權方法之應用流程圖之示意圖；

第3A圖係本揭露之軟體授權方法之具體實施架構圖之示意圖；以及

第3B圖係本揭露之軟體授權方法之轉換軟體成受保護軟體之說明圖之示意圖。

【主要元件符號說明】

10、30	轉換模組
11、31	軟體供應模組
110、310	受保護軟體
310'	軟體
12	處理模組
13	中介模組
131	第二溝通介面
132	第一溝通介面
133	回復單元
14、32	授權模組
141、321	主金鑰庫
142、322	第一金鑰庫
143	運算單元

15	記憶體
16、34	安全硬體
33	中介軟體
P1、P2…Pn、C1、C2…Cn	區塊
S201~S204	步驟

七、申請專利範圍：

1. 一種軟體授權系統，包括：

軟體供應模組，係提供以主金鑰進行加密的受保護軟體，且該受保護軟體具有軟體識別碼；

處理模組，用以自該軟體供應模組下載該受保護軟體，並輸出所下載之該受保護軟體的軟體識別碼；

中介模組，係具有用戶識別碼及對應該用戶識別碼的第一金鑰，且該中介模組用以接收該處理模組所輸出之軟體識別碼；以及

授權模組，具有主金鑰庫和第一金鑰庫，該授權模組接收該中介模組所輸出之該用戶識別碼及該軟體識別碼，並根據該用戶識別碼及該軟體識別碼分別至該主金鑰庫搜尋與該軟體識別碼相對應的主金鑰及至該第一金鑰庫搜尋與該用戶識別碼對應的第一金鑰，其中，該授權模組以該主金鑰及該第一金鑰進行運算而產生第二金鑰並將該第二金鑰傳輸至該中介模組，以由該中介模組依據自身所具有之第一金鑰結合所接收的該第二金鑰回復出該主金鑰，使該處理模組利用該主金鑰對所下載之受保護軟體進行解密。

2. 如申請專利範圍第 1 項所述之軟體授權系統，復包括轉換模組，用以將至少一軟體以該主金鑰加密的方式轉換為該受保護軟體並傳輸至該軟體供應模組。

3. 如申請專利範圍第 2 項所述之軟體授權系統，其中，該轉換模組用以將該軟體區分為複數個區塊並利用該主

金鑰分別對該些區塊進行加密而轉換為該受保護軟體，以混淆該軟體的資料結構和控制程序。

4. 如申請專利範圍第 3 項所述之軟體授權系統，其中，該處理模組係利用該中介模組所回復出的主金鑰分別對該些區塊進行解密。

5. 如申請專利範圍第 1 項所述之軟體授權系統，其中，該中介模組包括：

第一溝通介面，用以將該用戶識別碼及該軟體識別碼傳輸至該授權模組，並自該授權模組接收該第二金鑰；

回復單元，用以結合該第一金鑰及所接收的該第二金鑰以回復出該主金鑰；以及

第二溝通介面，用以接收該處理模組所下載之受保護軟體的軟體識別碼並將該主金鑰傳輸至該處理模組。

6. 如申請專利範圍第 1 項所述之軟體授權系統，其中，該授權模組包含運算單元，係以該主金鑰及該第一金鑰進行互斥運算而產生該第二金鑰。

7. 如申請專利範圍第 1 項所述之軟體授權系統，其中，該第一金鑰係以混淆技術設置於該中介模組。

8. 如申請專利範圍第 1 項所述之軟體授權系統，其中，該中介模組係設置於使用者裝置，且該中介模組所具有之第一金鑰及所接收之該第二金鑰係儲存於該使用者裝置的安全硬體。

9. 如申請專利範圍第 1 項所述之軟體授權系統，其中，該

處理模組係設置於使用者裝置中，且該處理模組將已解密的受保護軟體儲存至該使用者裝置的記憶體。

10. 一種軟體授權方法，係應用於軟體授權系統，該軟體授權系統包括伺服端和用戶端，該用戶端具有用戶識別碼和對應該用戶識別碼之第一金鑰，該伺服端具有提供以主金鑰進行加密之受保護軟體的軟體供應模組及儲存有該主金鑰和該第一金鑰的授權模組，該軟體授權方法包括以下步驟：

(1)令該用戶端自該軟體供應模組下載該受保護軟體時取得該受保護軟體的軟體識別碼，並將自身所具有之用戶識別碼及該受保護軟體的軟體識別碼傳輸至該授權模組；

(2)令該授權模組依據該用戶識別碼取得相對應的第一金鑰，且根據該軟體識別碼取得相對應的主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰，並將該第二金鑰傳輸至該用戶端；

(3)令該用戶端依據自身所具有之第一金鑰結合所接收的第二金鑰以回復出該主金鑰；以及

(4)令該用戶端利用所回復出的該主金鑰對所下載之受保護軟體進行解密。

11. 如申請專利範圍第 10 項所述之軟體授權方法，其中，步驟(1)復包括該伺服端將至少一軟體以主金鑰加密的方式轉換成該受保護軟體，以供該用戶端下載。

12. 如申請專利範圍第 11 項所述之軟體授權方法，其中，

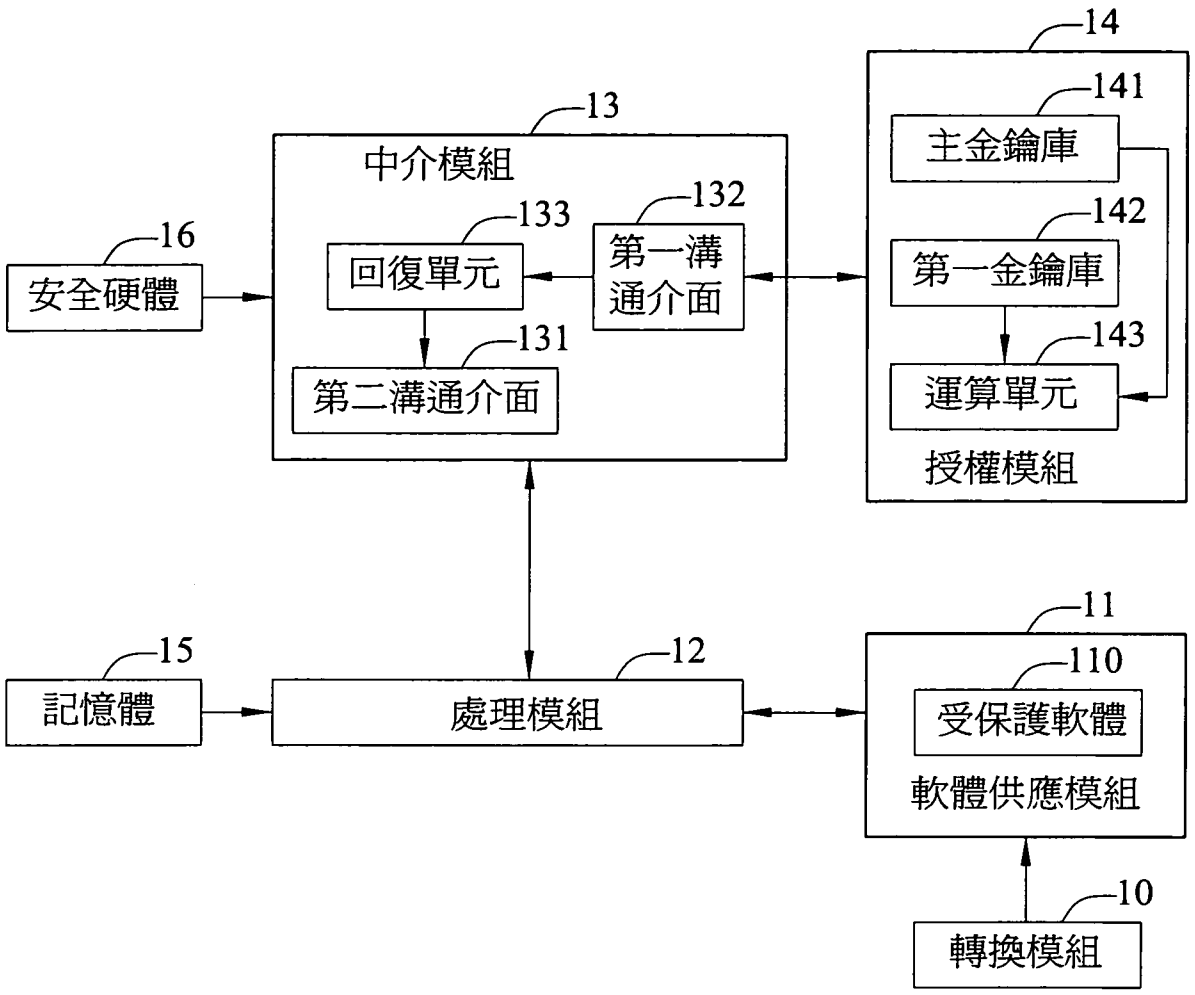
於步驟(1)復包括該伺服端將該軟體區分為複數個區塊並以該主金鑰分別加密而轉換為該受保護軟體，且步驟(4)復包括令該用戶端以所回復之主金鑰對該複數個區塊分別進行解密。

13. 如申請專利範圍第 10 項所述之軟體授權方法，其中，步驟(2)之運算方法為互斥運算或利用秘密分享技術(secret sharing scheme)。

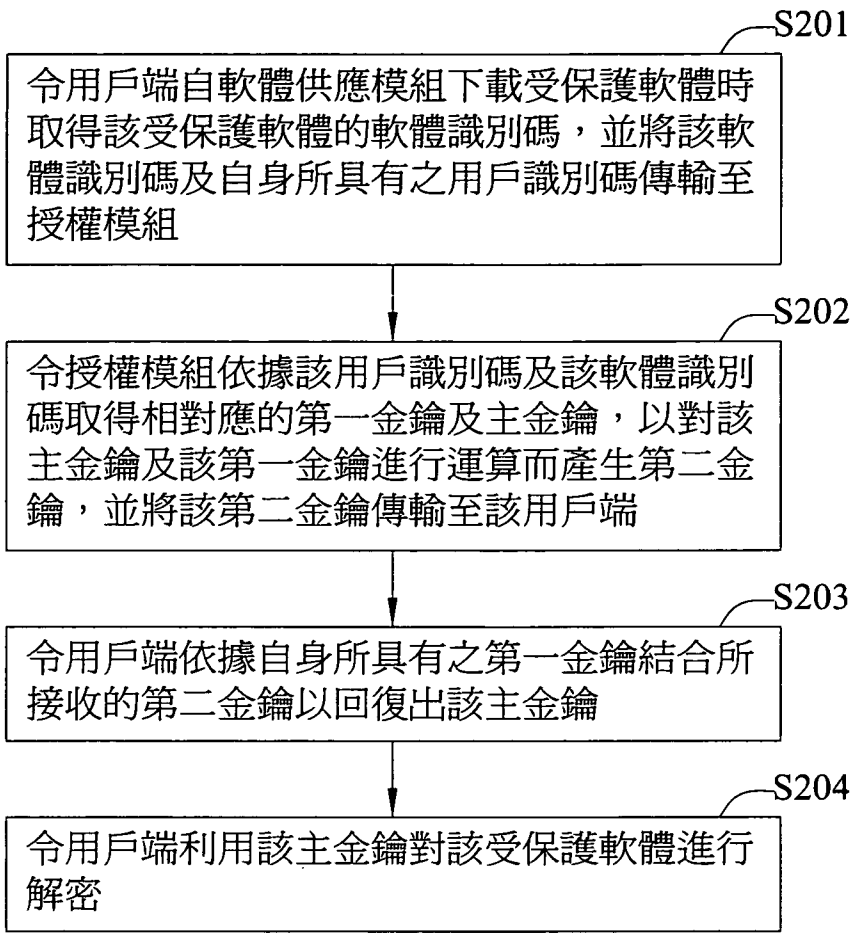
14. 如申請專利範圍第 10 項所述之軟體授權方法，其中，該用戶端復包括用以與所下載的受保護軟體建立連線之中介軟體，於步驟(4)中解密的方式為令該中介軟體利用 IPC(Inter process communication)技術與所下載的受保護軟體建立連線，以利用該主金鑰解密該受保護軟體。

15. 如申請專利範圍第 10 項所述之軟體授權方法，其中，該用戶端復包括中介軟體而該第一金鑰係以混淆技術設置於該中介軟體。

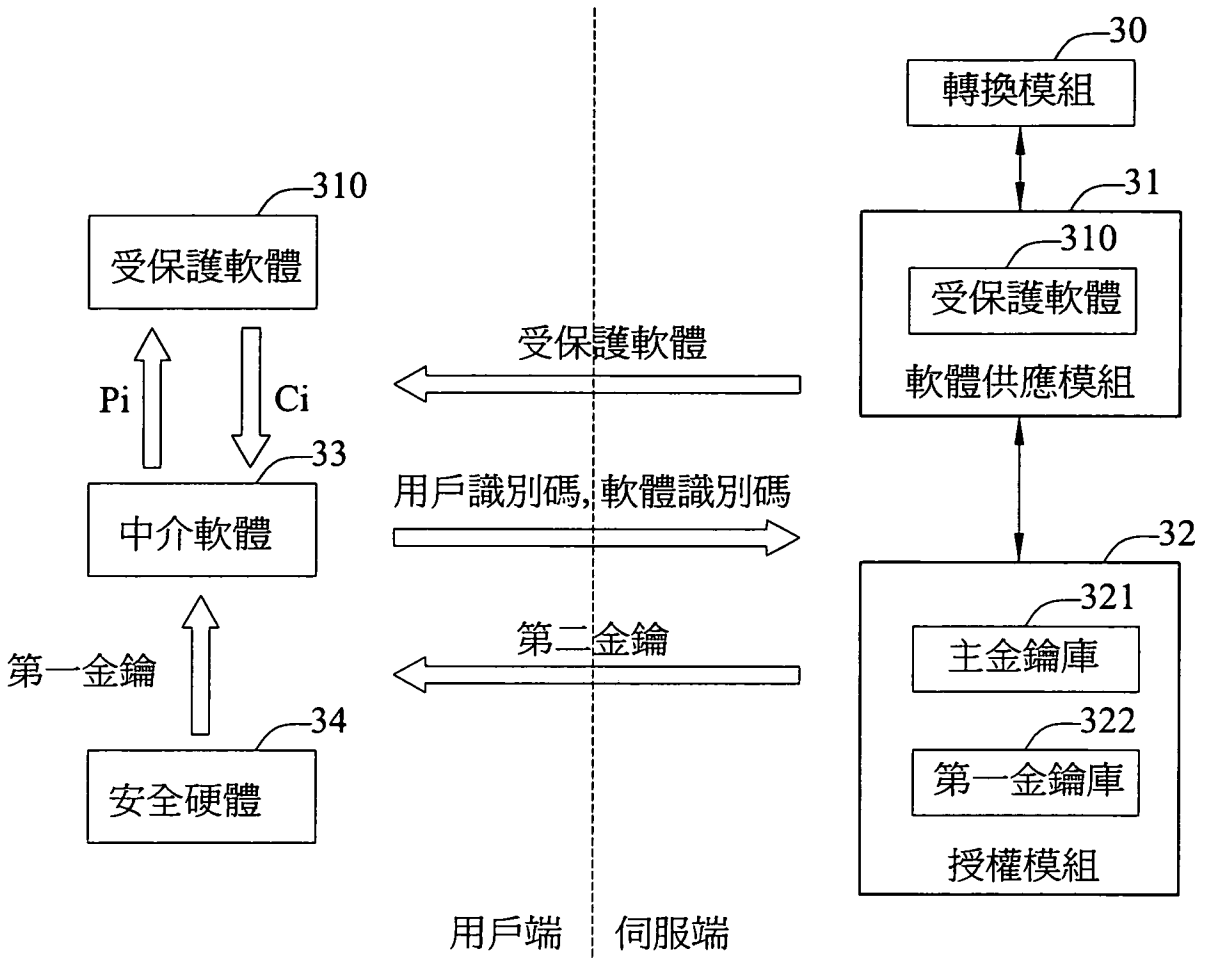
16. 如申請專利範圍第 10 項所述之軟體授權方法，其中，該用戶端復包括安全硬體而該第一金鑰及/或所接收之第二金鑰係儲存於該安全硬體。


14
141
主金鑰庫
13
中介模組
132
133
142
16
回復單元
第一溝
通介面
第一金鑰庫
安全硬體
131
143
第二溝通介面
運算單元
授權模組
11
15
12
110
記憶體
處理模組
受保護軟體
軟體供應模組
10
轉換模組

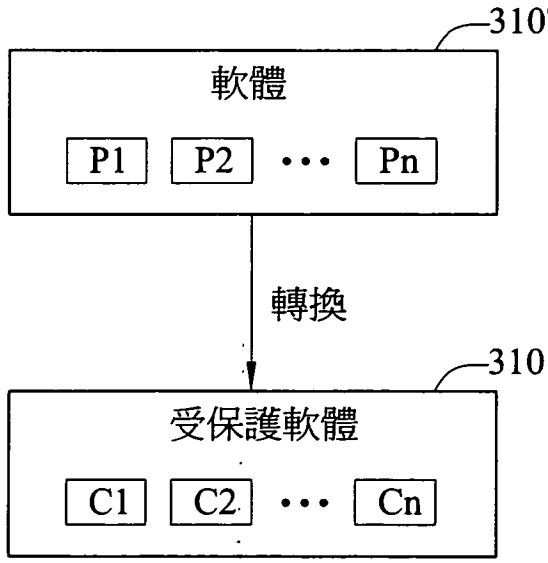
第1圖


S201
令用戶端自軟體供應模組下載受保護軟體時取得該受保護軟體的軟體識別碼，並將該軟體識別碼及自身所具有之用戶識別碼傳輸至授權模組
S202
令授權模組依據該用戶識別碼及該軟體識別碼取得相對應的第一金鑰及主金鑰，以對該主金鑰及該第一金鑰進行運算而產生第二金鑰，並將該第二金鑰傳輸至該用戶端
S203
令用戶端依據自身所具有之第一金鑰結合所接收的第二金鑰以回復出該主金鑰
S204
令用戶端利用該主金鑰對該受保護軟體進行解密

第2圖


30
轉換模組
31
310
受保護軟體
軟體供應模組
310
受保護軟體
受保護軟體
Pi
Ci
33
中介軟體
用戶識別碼, 軟體識別碼
32
321
主金鑰庫
第二金鑰
第一金鑰
322
第一金鑰庫
34
安全硬體
授權模組
用戶端
伺服端

第3A圖


310'
軟體
P1
P2
Pn
轉換
310
受保護軟體
C1
C2
Cn

第3B圖