



(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 I501154 B

(45)公告日：中華民國 104 (2015) 年 09 月 21 日

(21)申請案號：103102741

(22)申請日：中華民國 97 (2008) 年 01 月 31 日

(51)Int. Cl. : G06F9/445 (2006.01)

H04L9/14 (2006.01)

H04L12/24 (2006.01)

(30)優先權：2007/02/01 美國

11/701,232

(71)申請人：微軟公司(美國) MICROSOFT CORPORATION (US)

美國

(72)發明人：修斯艾當 T HUGHES, AIDAN T. (IE)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

TW 200634568A

CN 1756157A

US 2004/0128395A1

審查人員：栗永欣

申請專利範圍項數：20 項 圖式數：7 共 30 頁

(54)名稱

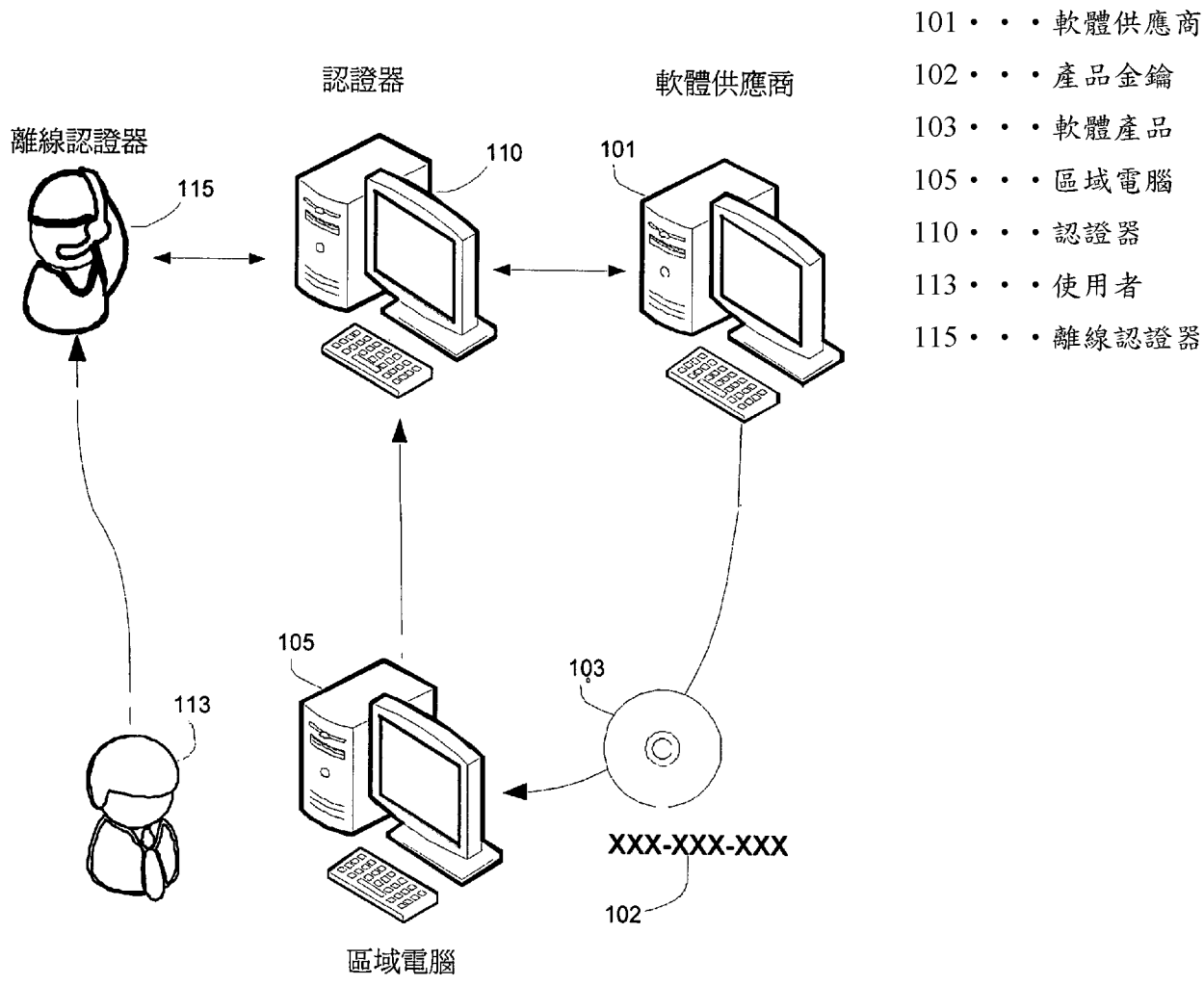
安全化序號

SECURE SERIAL NUMBER

(57)摘要

本發明揭示一軟體產品的序號與一認證碼值安全搭配。一遠端認證伺服器會完整評估該認證碼值與該序號，如此在一安裝該軟體產品的區域電腦上不會發生加密認證。該認證碼值的縮寫部分用於離線認證。

A serial number for a software product is secured with an authenticator value. The authenticator value and the serial number are evaluated entirely by a remote authentication server such that no cryptographic authentication occurs on a local computer on which the software product is being installed. An abbreviated portion of the authenticator value is used for offline authentication.



第 1 圖

發明摘要

※ 申請案號：103102741 (由 97103783 分割)

※ 申請日：97.1.31

※ IPC 分類：G06F 9/445 (2006.01)
H04L 9/14 (2006.01)
H04L 12/24 (2006.01)

【發明名稱】(中文/英文)

安全化序號/SECURE SERIAL NUMBER

【中文】

本發明揭示一軟體產品的序號與一認證碼值安全搭配。
一遠端認證伺服器會完整評估該認證碼值與該序號，如此在一安裝該軟體產品的區域電腦上不會發生加密認證。該認證碼值的縮寫部分用於離線認證。

【英文】

A serial number for a software product is secured with an authenticator value. The authenticator value and the serial number are evaluated entirely by a remote authentication server such that no cryptographic authentication occurs on a local computer on which the software product is being installed. An abbreviated portion of the authenticator value is used for offline authentication.

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：

101 軟體供應商

102 產品金鑰

103 軟體產品

105 區域電腦

110 認證器

113 使用者

115 離線認證器

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

安全化序號/SECURE SERIAL NUMBER

【技術領域】

【0001】 本發明係關於安全化序號。

【先前技術】

【0002】 現代商業盒裝軟體產品通常以內含該軟體程式碼以及一文數字產品金鑰的實體媒體的型態販售。通常一軟體供應商會要求在一特定使用者以及/或電腦啓用與軟體相關聯的所有權利之前，必須完成產品的「啓動」程序。

【0003】 該啓動程序通常牽涉到將該產品金鑰隨同識別該使用者以及/或電腦的某些資訊一起傳輸至一啓動資訊交換中心(通常為該軟體供應商，但是也可能是第三廠商)。該軟體供應商回應一授權碼，啓用存取該軟體的相關權限。該軟體即取得授權。

【0004】 當軟體具有顯著價值時，生產偽造產品金鑰的誘因就會升高。由於軟體的特性，要識別並拒絕偽造品就具有挑戰性。為致力達成此項工作，應用在產品金鑰內的技術在近幾年來已有進步，包含試圖證明該序號合法的數位短簽章。

【0005】 不過，產品金鑰的效用只有在製造系統所知道的偽造金鑰時才能衡量出來。CPU 處理能力的進步讓目前的技術更加無效，因為有「金鑰產生」工具存在，其可以根據現有

技術在幾小時或幾分鐘內產生偽造金鑰。

【0006】 直到現在，精通此技術的人士還是無法對此問題提出有效的解決方案。

【發明內容】

【0007】 本發明一般係關於用在驗證軟體產品的一安全化序號。在一個具體實施例內，一安全化序號停止該區域電腦(其上已安裝軟體產品)的認證功能，然後將此功能移至遠端認證伺服器。在另一具體實施例內，該安全化序號包含根據單次採取的驗證程序所費時間來調整認證值。

【圖式簡單說明】

【0008】 參考下列詳細說明並考慮附圖，將會更清楚了解到本發明的許多優點，其中：

【0009】 第 1 圖為其中可實施本發明具體實施例的計算環境之圖示例證。

【0010】 第 2 圖為根據一個具體實施例包含一安全化序號的產品金鑰圖示。

【0011】 第 3 圖為在安全化產品金鑰製作當中的軟體供應商之圖解。

【0012】 第 4 圖為在產品金鑰認證當中一區域電腦與認證碼的圖解。

【0013】 第 5 圖為可用於實施本發明一或多個具體實施例的示例性計算裝置之功能區塊圖。

【0014】 第 6 圖為一般說明根據一個具體實施例，用於建立產品金鑰的程序之操作流程圖。

【0015】 第 7 圖爲一般說明根據一個具體實施例，用於認證產品金鑰的程序之操作流程圖。

【0016】 此時將參閱圖式來說明本發明的具體實施例，其中相同的編號代表相同的元件。

【實施方式】

【0017】 底下將參考附圖更完整說明許多具體實施例，這形成本說明書的一部分，並且顯示出特定示例性實施來實行多種具體實施例。不過，其他具體實施例也可在許多不同的形式中實施，並且不受此處所公佈的具體實施例所限制；而是提供這些具體實施例讓本說明書更加完善。具體實施例可實施爲方法、系統或裝置。因此，具體實施例可採用一硬體實施、一完整軟體實施或一結合軟硬體態樣的實施。因此，下列詳細說明並不設限。

【0018】 許多具體實施例的邏輯操作實施(1)爲在一計算系統上執行一連串的電腦實施步驟以及/或(2)爲在該計算系統內的互連機器模組。此實施爲取決於實施具體實施例的該計算系統的效能需求最佳選項之一。因此，構成此處所說明具體實施例的邏輯操作或可稱爲操作、步驟或模組。

【0019】 系統說明

【0020】 首先將參閱實施本發明特定具體實施例的一樣本系統來說明基本原理與概念。此樣本系統可使用根據在此揭示所教授來程式編輯的傳統或特殊用途計算設備來實施。

【0021】 第 1 圖爲其中可實施本發明具體實施例的一計算環境 100 圖式。計算環境 100 可使用根據在此揭示所教授所配

置的任何傳統計算裝置來實施，像是第 5 圖內以及底下所描述說明的計算裝置。由第 1 圖內所說明每一組件所執行的特殊操作將結合第 2 圖至第 5 圖來詳細說明。不過，概略來說，這些組件所執行的一般操作將結合第 1 圖來說明。

【0022】 計算環境 100 包含開發並販售或授權軟體的軟體供應商 101。此外，軟體供應商 101 包含根據一個具體實施例來建立安全化產品金鑰的組件。尤其是，軟體供應商 101 配置成產生每一軟體產品的序號。此外，軟體供應商 101 也配置成根據該序號產生認證值。該序號與該認證值會以附帶軟體產品 103 一複本的產品金鑰 102 遞出。產品金鑰 102 並不需以實體與軟體產品 103 結合一起遞出。例如：產品金鑰 102 可利用諸如電子訊息等方式遞送。在第 2 圖以及底下當中將說明產品金鑰 102 的一個特定範例。

【0023】 認證器 110 包含在用於執行認證產品金鑰 102 的工作。認證器 110 包含足以認證軟體供應商 101 所建立該認證值的資訊。此外，認證器 110 配置成產生已經成功認證的每一產品金鑰之啟動碼。該啟動碼(未顯示)允許該軟體產品 103 無限制執行。爲了方便起見，以個別實體來說明認證器 110。另外，認證程式 110 可實施成爲軟體供應商 101 的一部分或組件。

【0024】 一區域電腦 105 可爲任何傳統計算系統，像是第 5 圖內以及底下所說明的計算系統。區域電腦 105 可以或無法線上存取其他計算系統，像是認證器 110。在區域電腦 105 無法線上存取的情況下，使用者 113 可藉由與離線認證器 115

通訊來執行一離線認證。離線認證員 115 可為線上認證器 110 的代理人(例如一人為的或自動的電話接線生)。

【0025】 在操作上，軟體供應商 101 遞送軟體產品 103 和產品金鑰 102 給使用者 113，然後該使用者將軟體產品 103 安裝在區域電腦 105 上。在啟動程序中，軟體產品 103 提示使用者 113 輸入產品金鑰 102。若區域電腦 105 已具有線上存取，則軟體產品 103 傳送至少部分該產品金鑰給線上認證器 110 來認證。若區域電腦 105 不具有線上存取，則軟體產品 103 會提示使用者 113 呼叫打離線認證器 115，並提供至少其他部分產品金鑰 102 給離線認證器 115。為了本討論起見，「離線」一詞表示在輸入該產品金鑰的電腦(例如區域電腦 105)與執行認證的電腦(例如認證器 110)之間線上電子互動以外的任何認證形式。

【0026】 安全產品金鑰 102 為一需要耗費極長時間才能「破解」的金鑰，其中「破解」一詞為一種有系統或蠻力方式猜測與一有效產品金鑰相關聯的一系列號碼。傳統以產品金鑰啟動的技術會在安裝期間於區域電腦 105 上執行認證，不過，計算技術的進步造成在區域電腦 105 上破解產品金鑰 102 所需時間越來越短。本發明者決定從區域電腦 105 上移除認證功能，讓認證器 110 控制認證程序，並據此控制要猜測一個有效產品金鑰所需的時間。接著，在此具體實施例內，該產品金鑰認證功能從區域電腦 105 移除，並移至認證器 110。在此方式中，可更緊密控制整個認證程序，這可避免在區域電腦 105 上發生認證程序時遭蠻力金鑰產生攻擊阻礙。

【0027】 此時請參閱第 2 圖，說明根據一個具體實施例的樣本產品金鑰 202。在此特定實施當中，產品金鑰 202 包含由三個部分組成：一組序號 211、一組認證碼值 212 以及一個核對和 213。吾人應該注意，此處說明的產品金鑰 202 為許多可能的實施之一，並且本揭示所教授也適用於許多實體化或製造的其他產品金鑰。

【0028】 序號 211 可為識別一軟體產品個別實例的任何唯一編號。因此，序號 211 可為一系列線性遞增值的數字。另外，序號 211 應為從一組可能值中隨機選擇的數字。簡單來說，該序號應為使用任何可接收的數值選擇條件所選之任何數字。在一個特定範例中，序號 211 為一長度大約 40 位元的值，不過其他長度值也適用。

【0029】 認證碼值 212 為一以序號 211 和一個像是一機密金鑰的機密碼為依據的值。在一個範例中，認證碼值 212 應為雜湊變數，諸如根據 SHA1 雜湊演算法的雜湊值等。該結果雜湊值應截斷為適當長度。在其他範例中，認證碼值 212 可為一加密變數，像是一使用 RC4 資料流密碼演算法在序號 211 上所產生並結合機密金鑰之值，同樣也截斷為適當長度。仍舊在其他範例中，認證碼值 212 可為透過個別關聯，像是遠端資料庫，只與序號 211 相關聯的完整隨機唯一數字。一般而言，認證碼值 212 為只有遠端認證器知道並且與序號 211 相關聯的唯一值。在一個特定範例中，認證碼值 212 為長度大約 48 位元的值，不過其他長度值也適用。

【0030】 在經過一段努力之後，發明者決定破解產品金鑰 202

的時間長度取決於認證是線上或離線執行。例如：單次嘗試線上驗證產品金鑰 202 只需要等一下子，這樣一天可以有上萬次嘗試。反言之，單次嘗試離線認證產品金鑰 202，像是人們以電話通話，會耗費好幾分鐘，這樣一天之內的嘗試次數大幅減少。

【0031】 在此決定之後，可接受的線上認證之認證碼值 212 要比離線認證所使用的認證碼值複雜許多。反言之，離線認證所使用的認證碼值 212 要比線上認證簡單許多。但是爲了避免建立多重認證碼值，本發明者決定在產品金鑰 202 內使用一個認證碼值 212，但是只有一部分(離線認證碼 217)用於離線認證，並且整個認證碼值 212 應用於線上認證(線上認證碼 219)。在一個特定範例中，離線認證碼 217 爲長度大約 15 位元的值，不過其他長度值也適用。

【0032】 此特色縮短一使用者執行離線認證，像是利用電話，必須唸出的數字。如此避免人爲錯誤所造成的一無效認證。加上如所提到，一使用者透過電話執行離線認證所需花費的時間長度可有效避免一蠻力嘗試猜測一有效產品金鑰。

【0033】 在此特定實施當中，使用認證碼值 212 的開頭幾個字元當成離線認證碼 217。在其他實施當中，可使用認證碼值 212 的其他部分，像是認證碼值 212 的中央或最後部分。吾人應該注意，當產生認證碼值 212 的技術導致隨機均勻分布在整個認證碼值 212 上，應從認證碼值 212 選擇連續字元而非片斷字元來實現隨機之中無不成比例的損失。

【0034】 在此實施當中，核對和值 213 包含在產品金鑰 202

內。從序號 211 和認證碼值 212 的核對和可計算出核對和值 213。在此方式中，在執行實際認證之前，本機處理應計算核對和來偵測使用者是否輸入錯誤的產品金鑰 202。這可避免因為輸入不正確的產品金鑰造成認證失敗，認證失敗會讓使用者非常挫折。在一個特定範例中，核對和值 213 為長度大約 32 位元的值，不過其他長度值也適用。

【0035】 第 3 圖為在安全化產品金鑰 305 製作當中的軟體供應商 301 圖式。第 3 圖說明可具體實施當成軟體供應商計算硬體內電腦可執行指令的特定功能組件。吾人應該瞭解，也可具有與此具體實施例無關的許多其他組件。在不悖離本具體實施例精神之下，額外組件也可實施來執行此處所說明之外的額外功能。

【0036】 第 3 圖內顯示包含雜湊函數 305 以及核對和演算法 317 的軟體供應商 301。雜湊函數 305 代表用於將資料編碼，讓別人無法輕易解碼或甚至不知道資料哪一部分已經編碼的許多機制之一。在此特定具體實施例內，雜湊函數 305 將序號 307 與機密金鑰 309 一起編碼來產生認證碼值 311。一般而言，一金鑰為一控制加密演算法操作的資訊片段。在此特定具體實施例內，機密金鑰 309 可為軟體供應商 301 才知道的任何唯一值。機密金鑰 309 越長或越複雜，就越難以將該編碼的資料解碼。因此，機密金鑰 309 的長度應可選擇，以提供合理的困難度給嘗試破解認證碼值 311 的人。四千位元 (4,096 位元) 機密金鑰 309 應可提供可接受的強度，不過機密金鑰 309 的長度會受所使用的特定雜湊演算法(等等)以及其

他因素所影響。較短或較長的機密金鑰都可適用於其他環境。

【0037】 軟體供應商 301 可額外使用核對和演算法 317 (或類似)來產生序號 307 以及認證碼值 311 的循環冗餘檢查(Cyclic Redundancy Check,"CRC")值 319。核對和演算法 317 代表用於計算一值之許多函數中之任一個，而該值可用來偵測其他值內是否存在錯誤。雖然在技術上核對和演算法 317 為一種雜湊函數，而雜湊函數 305 用於建立認證碼值 311，則核對和演算法 317 並不足以複雜到建立無法輕易破解的值，如此就無法用於保全序號 307。不過，核對和演算法 317 對於偵測簡單錯誤非常有用，像是打印錯誤的產品金鑰。

【0038】 最終結果為包含三個組件的產品金鑰 320：序號 307、認證碼值 311 以及 CRC 值 319。然後，產品金鑰 320 可與一軟體產品(未顯示)複本一起遞出。吾人應該瞭解，產品金鑰 320 並不需要以實體與該軟體產品一起遞出，而是可分別遞送，像是透過電子郵件、電話、其他電子通訊等等。

【0039】 吾人也應該瞭解，不同的產品金鑰 320 或可用或可不用於軟體產品的每一個唯一認證複本。換言之，軟體供應商 301 可將特定序號指派給已知編號的軟體產品，像是在客戶購買一大型全場執照以因應大量軟體產品已安裝複本的情況。類似地，不同的產品金鑰 320 可與該軟體產品的不同版本產生關聯。

【0040】 第 4 圖為在產品金鑰 402 認證當中區域電腦 401 與認證器 430 的圖式。在此特定具體實施例內，區域電腦 401 代表其上可安裝軟體產品的一計算系統之組件。在此具體實

施例內，區域電腦 401 包含一個足以執行常用算術運算來判斷資料序列內使否存在錯誤的核對和演算法 407。核對和演算法 407 為選項，並且在其他具體實施例當中可省略。

【0041】 針對部分啓動程序，會要求該使用者輸入(例如鍵入)產品金鑰 402。產品金鑰 402 包含一組序號 410、一組認證碼值 412 以及一個 CRC 值 414。如上面的詳細說明，序號 410 為一軟體產品隨附的任何數字，認證碼值 412 為只有認證器 430 知道並對應至序號 410 的唯一值，而 CRC 值 414 為用於錯誤偵測的序號 410 和認證碼值 412 之簡單核對和。在其他具體實施例當中可省略 CRC 值 414。

【0042】 區域電腦 401 與認證器 430 通訊。在某些實施當中，區域電腦 401 和認證器 430 透過線上通訊，像是透過網際網路這樣的網絡。在其他實施當中，透過離線媒介，像是人們，發生區域電腦 401 與認證器 430 之間的通訊。在一個範例中，一使用者可透過該電話與認證器 430 的代理人(人爲或自動答錄)通訊。

【0043】 針對部分認證處理，區域電腦 401 將序號 410 和認證碼值 412 通訊給認證器 430。吾人將會瞭解，在特定環境中並不會將全部認證碼值 412 傳給認證器 430，像是在離線認證時。完整認證值碼 412 用於線上認證。

【0044】 認證器 430 包含至少一個雜湊函數 432，其代表用於將資料解碼的許多機制之一，其中該資料已經編碼，讓別人無法輕易解碼或甚至不知道資料哪一部分已經編碼。在此特定實施當中，機密金鑰 434 代表用於將認證碼值 412 編碼

的機密資料，並且為評估認證碼值 412 所需。

【0045】 雜湊函數 432 使用機密金鑰 434 以及序號 410 計算一有效認證碼值，並輸出至比較器 436，該比較器可為比較兩組資料的任何函數。來自區域電腦 401 的認證碼值 412 也提供給比較器 436，用於與雜湊函數 432 的輸出做比較。認證器 430 根據雜湊函數 432 輸出對認證碼值 412 的比較，將適當指示回傳給區域電腦 401。例如：若比較為正面的，則認證器 430 可傳回一授權碼(未顯示)給區域電腦 401，用於指示該軟體產品已授權，並且不受任何使用限制。若比較為負面的，認證器 430 可傳回錯誤給區域電腦 401，將該軟體產品停用，允許在受限的時間內執行、使用功能受到限制或這兩者組合。

【0046】 第 5 圖為可用於實施本發明一或多個具體實施例的示例性計算裝置 500 之功能區塊圖。在基本的組態中，計算裝置 500 包含至少一個處理器 502 以及記憶體 504。根據計算裝置現有的組態與類型，記憶體 504 可為揮發性(像是 RAM)、非揮發性(像是 ROM、快閃記憶體等等)或這兩者的組合。第 5 圖內用虛線 506 說明基本組態。

【0047】 此外，裝置 500 可具有其他特色/功能性。例如：裝置 500 也可包含額外儲存裝置(可移除以及/或不可移除)，含但不受限於磁碟片、光碟片或磁帶。第 5 圖內利用可移除式儲存裝置 508 以及不可移除式儲存裝置 510 來說明這種額外儲存體。電腦儲存媒體包含在任何方法或技術內實施的揮發與非揮發性、可移除與不可移除媒體，用於儲存像是電腦可讀取指令、資料結構、程式模組或其他資料等等資訊。記憶

體 504、可移除式儲存體 508 以及不可移動式儲存體 510 全都是電腦儲存媒體的範例。電腦除儲存媒體包括但不受限於 RAM、ROM、EEPROM、快閃記憶體或其他記憶體技術、CD-ROM、數位多功能光碟(DVD)或其他光學碟片儲存、磁帶、磁匣、磁片儲存或其他磁性儲存裝置，或其他任何可用於儲存所要資訊並且可由裝置 500 存取的媒體。任何這種電腦儲存媒體都可為裝置 500 的一部份。

【0048】 計算裝置 500 包含一或多個通訊連接 514，這允許計算裝置 500 與一或多個電腦以及/或應用程式 513 通訊。裝置 500 也可具有輸入裝置 512，像是一鍵盤、滑鼠、數位板或其他觸碰輸入裝置、語音輸入裝置等等。也可包含輸出裝置 511，像是一顯示器、揚聲器、印表機、PDA、行動電話與其他種數位顯示裝置等等。這些裝置都為業界所熟知，因此不予贅述。

【0049】 程序說明

【0050】 底下將參考特定具體實施例內一計算裝置(像是第 5 圖內說明的計算裝置)可實施的樣本程序來說明原理與概念。該等程序可使用軟體或韌體內電腦可執行指令來實施，但也可用其他方式來實施，像是用可程式化邏輯、電子電路等等。在某些替代具體實施例內，甚至可在有限的人為介入的情況下執行某些操作。再者，該等程序並不用於排除其他具體實施例，而是僅供說明。

【0051】 第 6 圖為一般說明根據一個具體實施例，用於建立產品金鑰的程序 600 之操作流程圖。建立的該產品金鑰可用

於驗證或授權軟體產品。建立的該產品金鑰可採用一或多種實體型態，像是列印在卡片或紙張上的號碼、儲存在資料庫內的值等等。

【0052】 在區塊 601 上，建立序號用於唯一的軟體產品。唯一實例可為該軟體產品的一個特定複本、可為相關實例群組、可為一系列已識別的該軟體產品實例等等。該序號可採取任何所要的形式，像是一系列號碼中的一個號碼、一隨機號碼或產品，像是該軟體產品相關的其他任何值。

【0053】 在區塊 603 上，根據該序號跟一機密碼建立一認證碼值。使用根據與一機密碼結合的其他值來產生一值之任何適當技術來建立該認證碼值。在一個特定實施當中，可使用雜湊函數結合一機密加密金鑰來產生該認證碼值。其他範例也可能，像是加密演算法。

【0054】 在區塊 605 上，可選擇性根據序號與驗證碼值計算核對和值(例如 CRC 值)。CRC 值可用於識別該認證碼值與該序號內的錯誤。

【0055】 在區塊 607 上，每一構成部分(例如該序號、該認證碼值以及核對和值)組合成一產品金鑰。在此點上，該產品金鑰可與新軟體產品一起遞出。

【0056】 第 7 圖為一般說明根據一個具體實施例，用於認證一產品金鑰的程序 700 之操作流程圖。程序 700 可在其上安裝一軟體產品的區域電腦系統上實施。程序 700 可執行當成該軟體產品認證或驗證程序的一部分。

【0057】 在區塊 701 上，接收一產品金鑰。在回應該產品金

鑰的提示上可接收該產品金鑰，像是出現在啟動程序上的對話區塊。在其他實施當中，該產品金鑰可用程式化方式提供，像是利用電子訊息或通訊方法。

【0058】 在區塊 703 上，將該產品金鑰解析成其構成組件。在一個實施當中，構成組件包含至少一個序號以及一個認證碼值。該序號為所安裝該軟體產品所伴隨的唯一號碼。該認證碼值為一種在不知道機密碼的情況下無法輕易破解的值。該產品金鑰可額外與選擇性包含 CRC 值，該值為該序號與該認證碼值的核對和。

【0059】 在區塊 705 上，若該產品金鑰包含一 CRC 值，則會針對該序號與該認證碼值評估該 CRC 值，以判斷是否在輸入任一值有錯誤發生。例如：若一使用者手動將該產品金鑰輸入對話區塊輸入欄位內，人為錯誤便極可能發生。因此，該 CRC 值若存在的話，應啟用簡單檢查來避免這種錯誤。若該產品金鑰未包含一這種 CRC 值，則可省略此操作。

【0060】 在區塊 707 上，驗證產品金鑰的認證技術已決定。在此特定具體實施例內，認證可線上或離線執行。線上就是使用發生在透過一網路耦合的兩計算系統之間電子通訊之一認證程序。離線就是非線上的任何認證程序。若該認證技術為線上認證，則程序 700 前往區塊 709。若該認證技術為離線認證，則程序 700 前往區塊 711。

【0061】 在區塊 709 上，該序號與該認證碼值都傳送至一遠端認證伺服器。該遠端認證伺服器配置有必須的組件來針對該序號評估該認證碼值。在一個範例中，該遠端認證伺服器

可包含適當演算法以及機密金鑰，來根據該序號判斷該認證碼值是否有效。在此特定實施當中，該完整認證碼值都傳送至該遠端認證伺服器。該完整認證碼值為一即便使用自動技術也難以破解的冗長位元串流。

【0062】 在區塊 711 上，顯示用於離線認證的一離線認證碼值。在此具體實施例內，吾人瞭解，使用比線上認證簡短許多的認證碼值，要破解該認證碼值的程序仍舊受到時間上的限制。因此，區塊 711 上顯示的該離線認證碼值可為該完整認證碼值的縮寫或截短版本。該離線認證碼值的長度可根據一單次嘗試使用該離線認證技術來認證該認證碼值所需時間長度來選擇。運用該離線認證碼值而非該完整認證碼值來進行離線認證可減少客戶要讀出一冗長並加密數字給一電話認證代理人時的挫折感。

【0063】 在區塊 713 上，不管該認證碼值(根據情況為線上認證碼或離線認證碼)是否有效都會收到通知。該通知可為許多形式之一，像是與該軟體產品結合儲存的一回傳有效碼來確認有效性並啟動。若該通知為正面的，則在區塊 715 上會將適當存取權限授權給該軟體產品。另外，若該通知為負面的，則在區塊 717 上，拒絕或限制存取該軟體產品，像是在時間或功能方面的限制。

【0064】 雖然以特定結構性特徵語言以及/或方法論的動作來說明所主張主題，吾人可瞭解，申請專利範圍內所定義的主張主題並不必然受限於上述特定特色或動作。而上述特定特色與動作僅當成實施申請專利範圍之範例型式之揭示。

【符號說明】

【0065】

- 100 計算環境
- 101 軟體供應商
- 102 產品金鑰
- 103 軟體產品
- 105 區域電腦
- 110 認證器
- 113 使用者
- 115 離線認證器
- 202 產品金鑰
- 211 序號
- 212 認證碼值
- 213 核對和
- 217 離線認證碼
- 219 線上認證碼
- 301 軟體供應商
- 305 安全化產品金鑰
- 305 雜湊函數
- 307 序號
- 309 機密金鑰
- 311 認證碼值
- 317 核對和演算法
- 319 CRC 值

- 320 產品金鑰
- 401 區域電腦
- 402 產品金鑰
- 407 核對和演算法
- 410 序號
- 412 認證碼值
- 414 CRC 值
- 430 認證器
- 432 雜湊函數
- 434 機密金鑰
- 436 比較器
- 500 計算裝置
- 502 處理器
- 504 記憶體
- 506 虛線
- 508 可移除式儲存裝置
- 510 不可移除式儲存裝置
- 511 輸出裝置
- 512 輸入裝置
- 513 應用程式
- 514 通訊連接

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

申請專利範圍

1. 一種用於產生一產品金鑰之方法，該方法包含以下步驟：
 - 由一電腦建立一序號，該序號唯一地識別一產品之一實例；
 - 由該電腦依據該序號與一機密碼，建立一認證碼值，其中該認證碼值之一部分係為一離線認證碼值，而其中該部分小於該認證碼值之一整體；
 - 依據該序號與該認證碼值，計算一核對和（checksum）值；以及
 - 由該電腦組合該序號、該認證碼值及該核對和值，而成為該產品金鑰，該產品金鑰經配置以用於該產品之該實例之線上與離線授權，其中該線上授權係依據該整體，其中該離線授權係依據該部分而非該整體。
2. 如請求項 1 所述之方法，其中該認證碼值係依據一雜湊函數而建立。
3. 如請求項 1 所述之方法，其中該機密碼係為一加密金鑰。
4. 如請求項 1 所述之方法，其中計算該核對和值之該步驟係依據一雜湊函數。
5. 如請求項 1 所述之方法，進一步包含傳遞該產品金鑰與該產品之該實例之步驟。
6. 如請求項 1 所述之方法，其中該產品之該實例係為該產品之一相關實例群組。
7. 如請求項 1 所述之方法，其中該產品之該實例係為該產品之一系列實例。

8. 一種儲存電腦可執行指令之電腦可讀取媒體，當由一電腦執行時，該等電腦可執行指令造成該電腦實行產生一產品金鑰之步驟，該等步驟包含：

由一電腦建立一序號，該序號唯一地識別一產品之一實例；

由該電腦依據該序號與一機密碼，建立一認證碼值，其中該認證碼值之一部分係為一離線認證碼值，而其中該部分小於該認證碼值之一整體；

依據該序號與該認證碼值，計算一核對和值；以及

由該電腦組合該序號、該認證碼值及該核對和值，而成為該產品金鑰，該產品金鑰經配置以用於該產品之該實例之線上與離線授權，其中該線上授權係依據該整體，其中該離線授權係依據該部分而非該整體。

9. 如請求項 8 所述之電腦可讀取媒體，其中該認證碼值係依據一雜湊函數而建立。

10. 如請求項 8 所述之電腦可讀取媒體，其中該機密碼係為一加密金鑰。

11. 如請求項 8 所述之電腦可讀取媒體，其中計算該核對和值之該步驟係依據一雜湊函數。

12. 如請求項 8 所述之電腦可讀取媒體，該等步驟進一步包含傳遞該產品金鑰與該產品之該實例之步驟。

13. 如請求項 8 所述之電腦可讀取媒體，其中該產品之該實例係為該產品之一相關實例群組。

14. 如請求項 8 所述之電腦可讀取媒體，其中該產品之該實

例係為該產品之一系列實例。

15. 一種包含一計算裝置與至少一個程式模組而一起經配置以用於產生一產品金鑰之系統，該系統依據以下步驟：

建立一序號，該序號唯一地識別一產品之一實例；

依據該序號與一機密碼，建立一認證碼值，其中該認證碼值之一部分係為一離線認證碼值，而其中該部分小於該認證碼值之一整體；

依據該序號與該認證碼值，計算一核對和值；以及

組合該序號、該認證碼值及該核對和值，而成為該產品金鑰，該產品金鑰經配置以用於該產品之該實例之線上與離線授權，其中該線上授權係依據該整體，其中該離線授權係依據該部分而非該整體。

16. 如請求項 15 所述之系統，其中該認證碼值係依據一雜湊函數而建立。

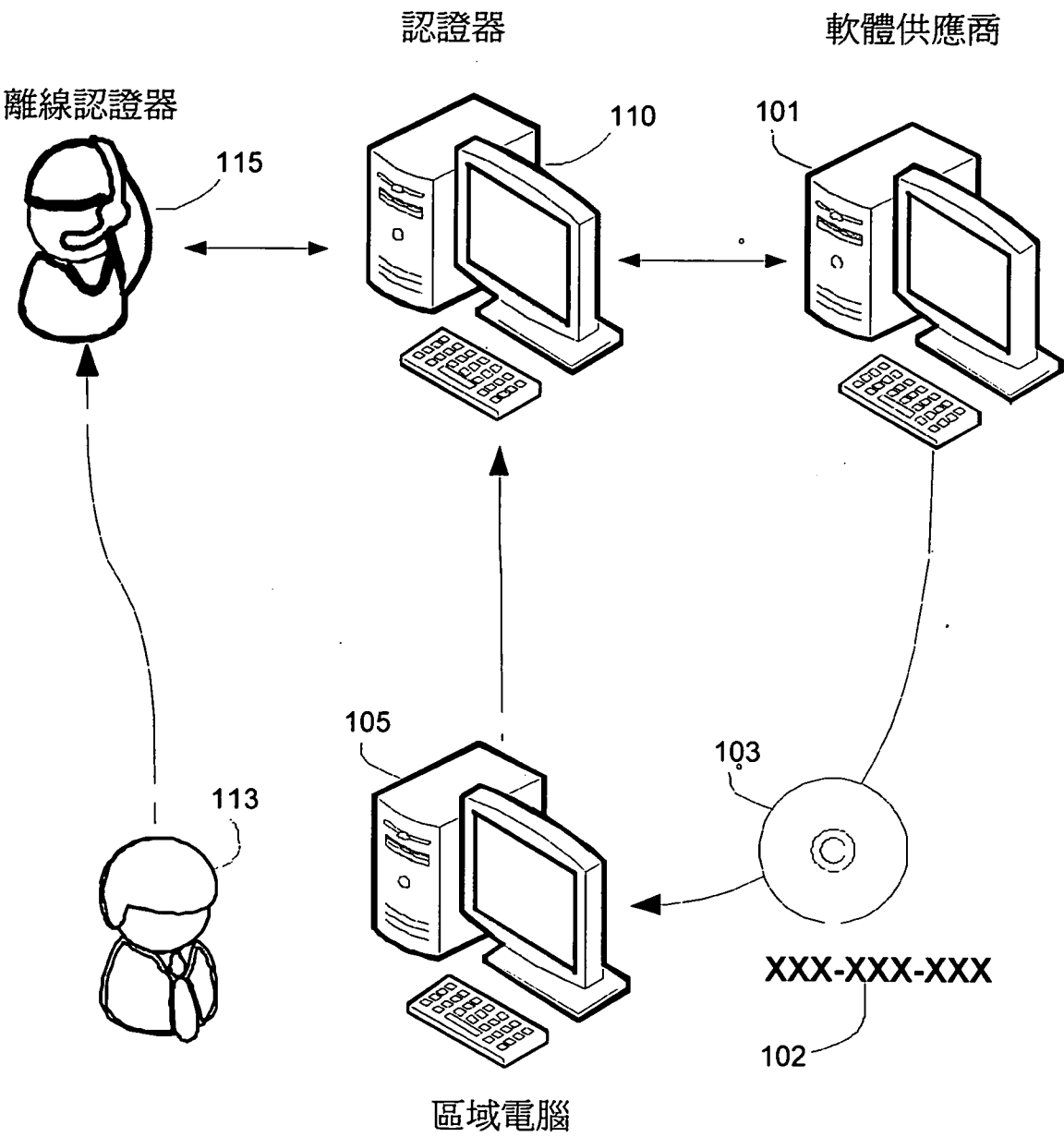
17. 如請求項 15 所述之系統，其中該機密碼係為一加密金鑰。

18. 如請求項 15 所述之系統，其中計算該核對和值之該步驟係依據一雜湊函數。

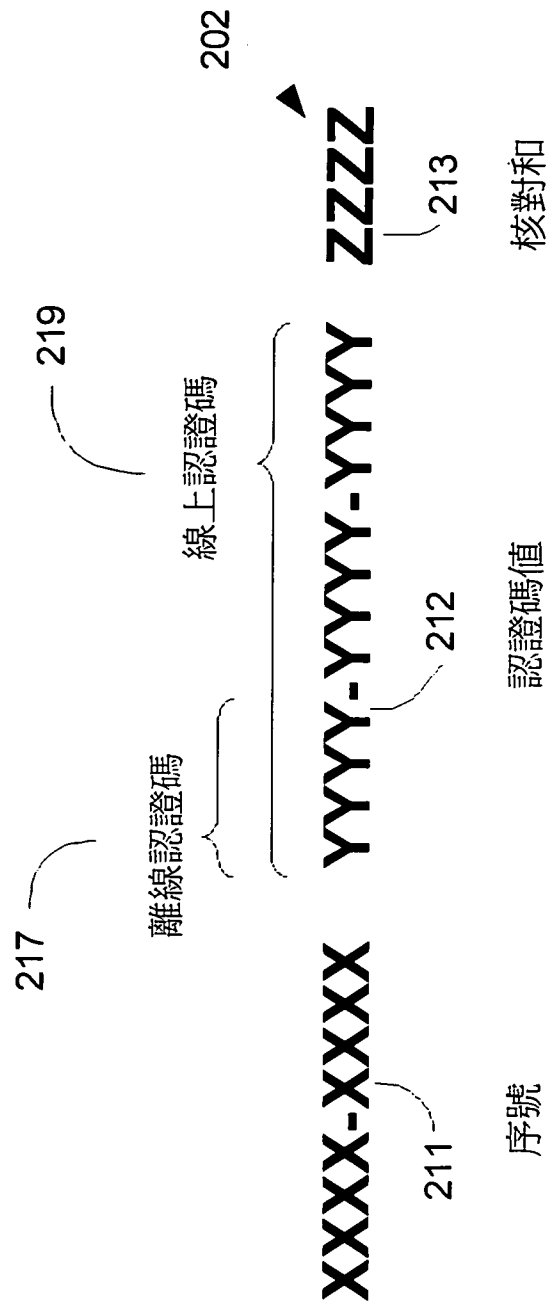
19. 如請求項 15 所述之系統，該等步驟進一步包含傳遞該產品金鑰與該產品之該實例之步驟。

20. 如請求項 15 所述之系統，其中該產品之該實例係為該產品之一相關實例群組或該產品之一系列實例。

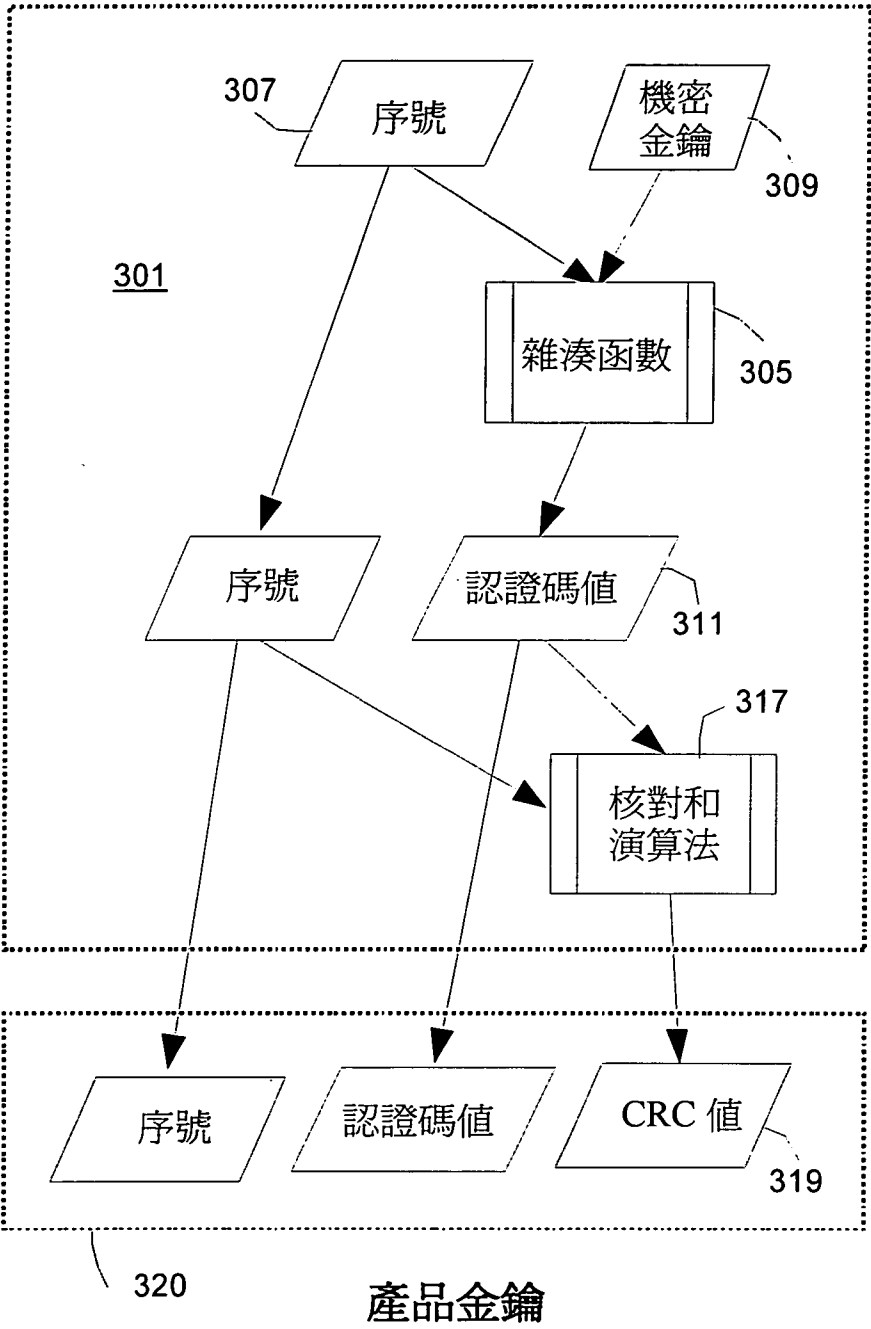
圖式



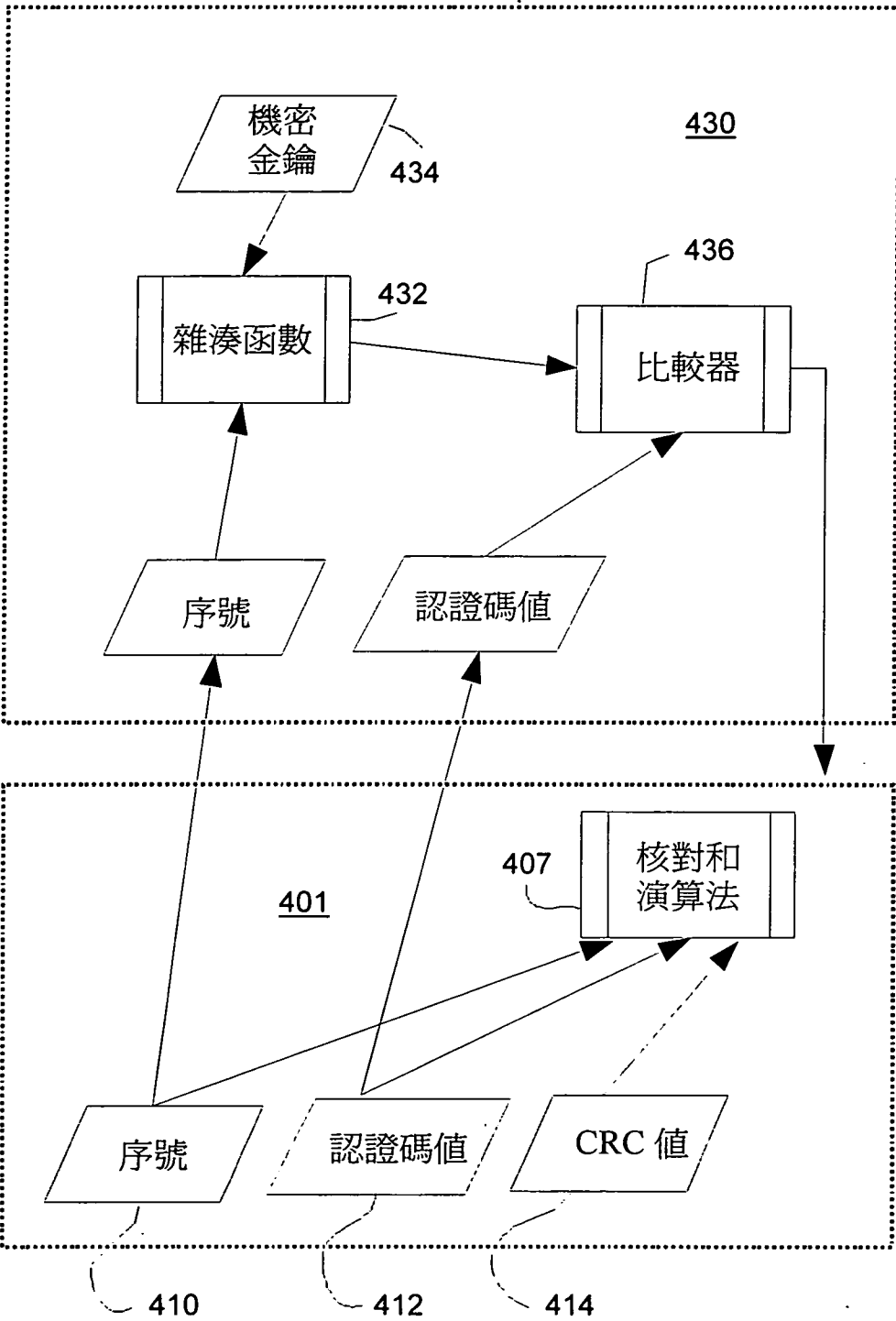
第 1 圖



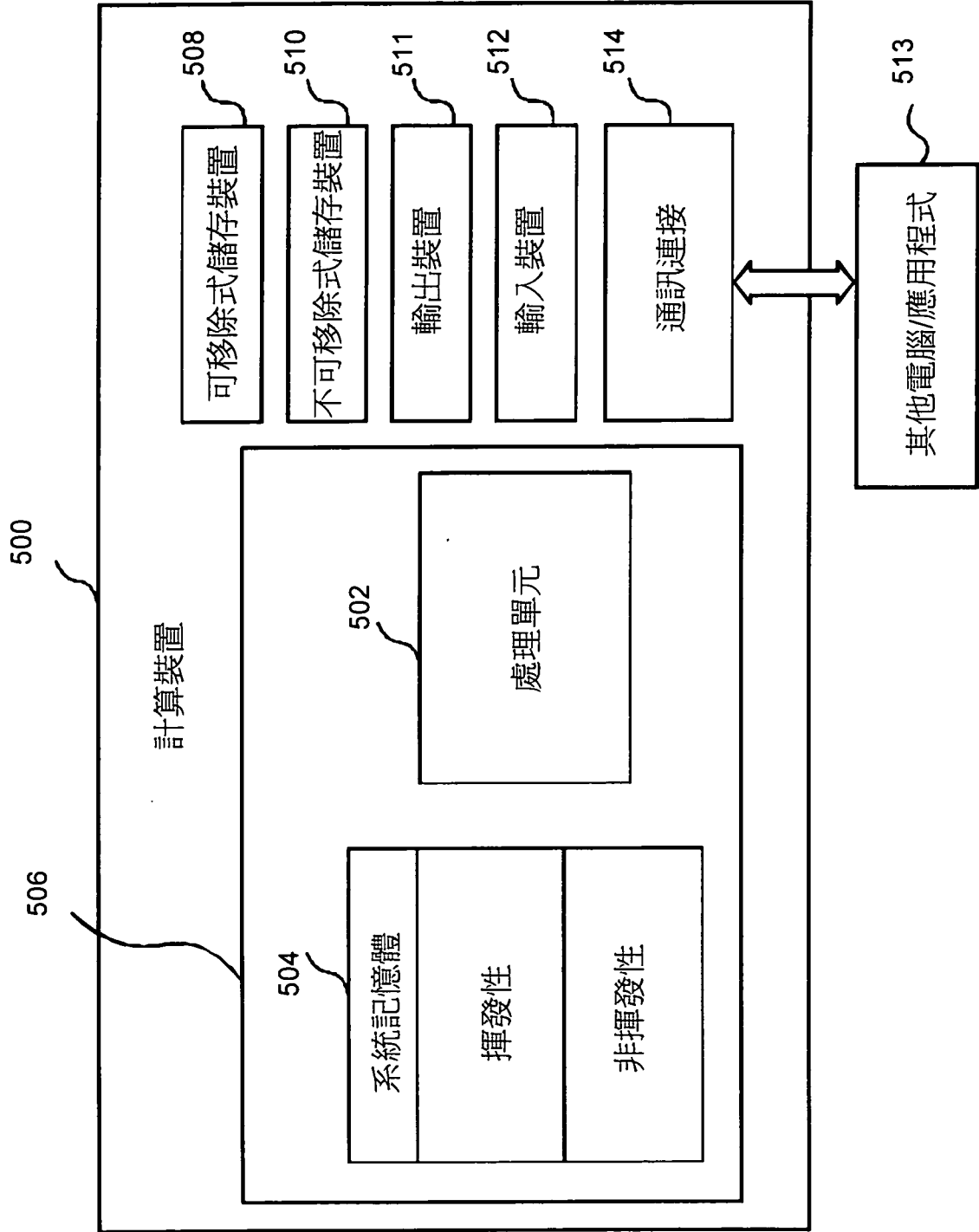
第 2 圖



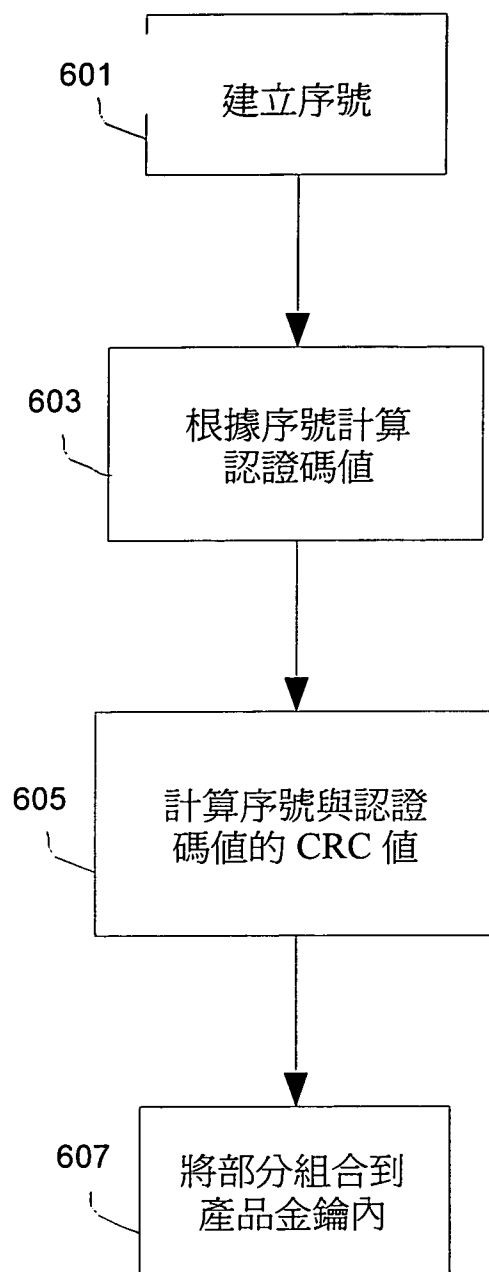
第 3 圖



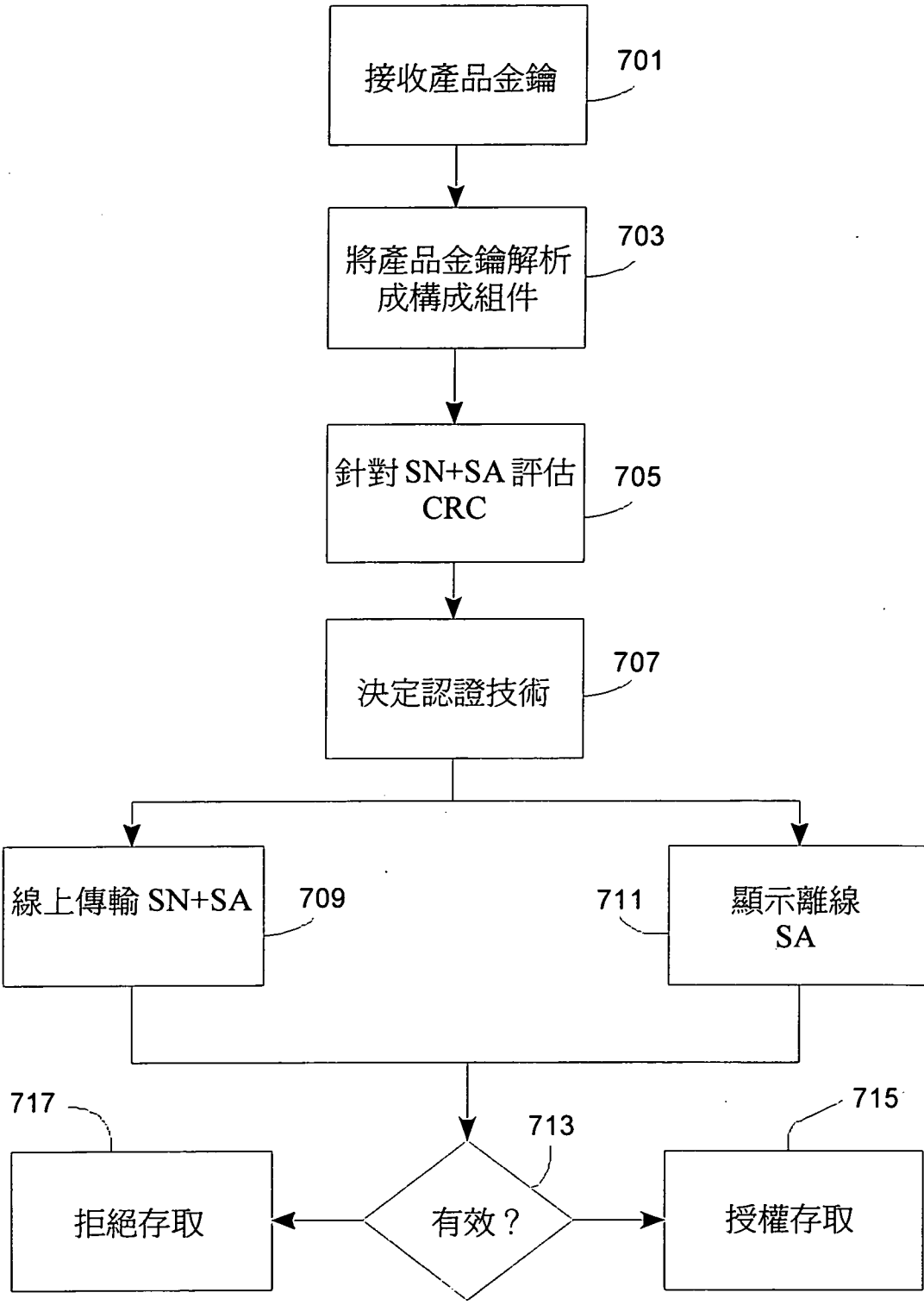
第 4 圖



第 5 圖



第 6 圖



第 7 圖