發明專利說明書 200422945

※ 申請案號：93105188

※ 申請日期：93 年 2 月 27 日　　※IPC 分類：G06F 9/30

壹、發明名稱：（中文/英文）

使機密連結至對於硬體更動具容許度的一電腦系統之系統

SYSTEM FOR BINDING SECRETS TO A COMPUTER SYSTEM HAVING TOLERANCE FOR HARDWARE CHANGES

貳、申請人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, USA

國　籍：（中文/英文）

美國/USA

參、發明人：（共 1 人）

姓　名：（中文/英文）

修斯艾當 T / HUGHES, AIDAN T.

住居所地址：（中文/英文）

美國華盛頓州貝樂夫市東北 8 號街第 E10 公寓 15206 號

15206 NE 8th St. Apartment E-10, Bellevue, Washington 98007, U.S.A.

國　籍：（中文/英文）

愛爾蘭 / Ireland

肆、聲明事項：

◎本案申請前已向下列國家(地區)申請專利 [V] 主張國際優先權：

【格式請依：受理國家(地區)；申請日；申請案號數 順序註記】

美國；2003 年 3 月 3 日；10/378,224

玖、發明說明：

【發明所屬之技術領域】

本發明係有關於連結一機密到指定電腦系統的系統和方法。本發明也關係於在一指定電腦系統上，產生一堅定的硬體識別碼的系統和方法，其中上述堅定的硬體識別碼的一元件是耦接一被連結的機密。依上述電腦系統硬體之變化的程度之堅定的硬體識別碼的結果，可用來控制所指定的該電腦系統上之軟體的使用。

【先前技術】

近年來有相當多的成果在防止或減少不合法使用電腦軟體。由於電腦軟體的可複制性及易於散佈，常出現電腦軟體的著作權侵害和不合法使用電腦軟體超越於使用許可的範圍，明顯危害軟體製造公司。

已發展一些方法以盡力降低電腦軟體盜版之發生以及非法使用超越授權合約的數量之電腦軟體。然而，像這樣的方法常常造成合法軟體之採購者困擾，及以此種消費形式之不便。例如，一升級電腦之使用者，應能合法重新安裝軟體於升級後的電腦。然而，目前可用的方法不是(i)不允許安裝上述軟體，就是(ii)強迫使用者(不高興的使用者)連絡軟體製造商以獲得幫助。

因此，有需要提供一種改善盜版及非法使用的技術解決方案，但其亦了解及提供合法的軟體採購者、使用者的需求及實施。

【發明內容】

本發明解決上述所討論的困難及問題，藉由連結一機密至一指定電腦系統的發現及一改良的耦接於機密之硬體識別。當允許合法軟體使用者進行機器升級的時候，本發明的硬體識別提供一方法，用來減少或防止著作權侵害和不合法使用電腦軟體超越於使用許可的範圍。

本發明之硬體識別，於此被稱為"堅定的硬體識別碼"(SHWID)，至少包含兩個不同的元件：(1)一硬體識別元件，及(2)一局部的機密元件。利用結合(1)一硬體識別元件和(2)一局部的機密元件，在一指定電腦系統上產生一較安全且可靠堅定的硬體識別碼(SHWID)。

當載入一軟體產品於電腦時，上述堅定的硬體識別碼(SHWID)可被用來確認指定的硬體組態。堅定的硬體識別碼(SHWID)可被儲存作為未來的使用，例如(i)當啟動相同的軟體產品在一相同的電腦或一變動之相同的電腦上，或(ii)當重新載入相同的軟體產品在一變動之相同的電腦或一完全不同的電腦上。例如，當啟動相同軟體產品在一相同的電腦或變動之相同電腦上時，會依耦接於原來堅定的硬體識別碼(SHWID)之機密能否產生而決定。若能產生機密，則本發明之方法允許載入軟體。然而，若不能產生上述機密，則由於原來的硬體系統改變超過了變動的閾值，本發明之方法不允許載入軟體。

因此本發明是應用於連結一機密於一指定電腦系統，

及一堅定的硬體識別碼(SHWID)耦接於上述機密之方法。本發明更進一步是應用在，若耦接原來的堅定的硬體識別碼(SHWID)的上述機密不能於電腦系統中取回時，防止在上述電腦系統中使用軟體之方法。

上述及其他特性及本發明的優點，將於檢閱下列之實施方式及申請專利範圍後，變得更加清楚。

【實施方式】

為了更了解本發明的原理，以下使用特定發明實施例的描述及特定的語言以描述特定的實施例。然而需了解使用這些特定的語言並非用以限定本發明的範圍。取而代之的是，熟習本發明相關之技藝之人士通常可經由思慮後進一步地變更或進一步地應用本發明的原理。

本發明應用於連接一種機密到一指定電腦系統，及堅定的硬體識別碼(SHWID)耦接於上述機密的方法。上述機密通常至少包含一個隨機選擇的整數。上述機密最好含有下列的特性：

(1) 機密，S，是在硬體組態 H 上可計算而得；

(2) 機密，S，是在硬體組態 H_1 上可計算而得，硬體組態 H 在一些元件的數量改變到所希望元件改變的數量閾值之後為硬體組態 H_1；及

(3) 機密，S，實際上不可能在任何其他的硬體組態 H_2 上計算而得。

上述機密可以被用來產生一種堅定的硬體識別碼

(SHWID)於一個由多種硬體元件組成的指定電腦系統。一種例示之電腦系統可以包含一些硬體元件種類，包含但不限定於硬碟驅動裝置、光碟驅動裝置如 CD-ROM 驅動裝置，網路卡、顯示介面卡、唯讀記憶體(ROM)、隨機存取記憶體(RAM)，以及一種基本輸入出系統(BIOS)。實施本發明的一種例示之電腦系統和例示之作業環境，於下列描述。

例示作業環境

以下利用圖式描述本發明例示的實施例，其中所有圖式之相同的符號係表示相同的元件。第 1 圖例示一種實施本發明的例示作業系統。上述例示作業系統，包含以一種常見的個人電腦 20 之一般用途的電腦裝置。大體而言，個人電腦包含一處理單元 21、一系統記憶體 22、以及一系統匯排流 23，此系統匯排流 23 耦接包含上述系統記憶體 22 的各種系統元件到處理單元 21。系統匯排流 23 可以是數種的匯排流結構的任何一種，包含記憶體匯排流或記憶體控制器，平行埠匯排流，和包含使用任一各種匯排流結構的局部匯排流。上述系統記憶體包含唯讀記憶體(ROM)24 及隨機存取記憶體(RAM)25。一基本輸入出系統(BIOS)26，含有用來協助個人電腦 20 之中元件的傳遞資訊之基本例行程序，例如在啟始期間，被儲存於 ROM 24。

個人電腦 20 更包含一供從硬碟(圖未顯示)讀取和寫入的硬碟驅動裝置 27；一供從可移動的磁片 29 讀取和寫

入的磁片驅動裝置 28；一供從可移動的光碟 31 讀取和寫入的光碟驅動裝置 30，如 CD-ROM 或其他光學媒體。硬碟驅動裝置 27、磁片驅動裝置 28 和光碟驅動裝置 30，分別由硬碟驅動裝置介面 32、磁片驅動裝介面 33 和光碟驅動裝置介面 34，連接系統匯排流 23。雖然上述例示之環境使用硬碟 27，可移動磁片 29，和可移動光碟 31，

熟悉此技藝之人士應理解，其他類型的電腦可讀取媒體，可由電腦存取儲存資料，如磁帶、快閃記憶卡、數位影音磁碟、卡匣式磁帶(Bernoulli cartridges)、隨機存取記憶體、唯讀記憶體及類似的元件，也可使用在例示之作業環　　這些驅動裝置及與其連結的電腦可讀寫媒體，提供電腦執行指令、資料結構、和其他個人電腦 20 的資料能夠定　的　儲存如，一或多個資料檔案 60(圖未顯示)，可以被儲存在個人電腦 20 的 RAM 25 及/或硬碟 27。

一些程式模組可以被儲存於硬碟 27、磁片 29、光碟 31、ROM 24、或 RAM 25，程式模組包含作業系統 35、一應用程式模組 36，其他程式模組 37，和程式資料 38。

程式模組包含但不限於、例行程序、子例行程序、程式物件、元件、資料結構等，程式模組執行特定的工作或實行特定的抽象資料結構。本發明的觀點，可以一應用程式模組 36 的整體，或以另一程式模組 37 的一部份實行。

使用者可以透過輸入裝置(圖未顯示)，例如一鍵盤 40 和一接觸點裝置 42，輸入命令和資訊進入個人電腦 20。其他的輸入裝置(圖未顯示)可以包含麥克風、控制桿、遊戲

輸入鍵盤、天線接收器、掃描器或其他類似的裝置。這些和其他輸入裝置常常透過一序列埠介面 46，連接至處理單元 21，上述序列埠介面 46 耦接到系統匯排流 23，但可以經由其他介面，如平行埠、遊戲埠、通用序列匯排流(USB)，或其他相近介面耦接到系統匯排流 23。監視器 47 或其他顯示裝置經由介面(例如視訊配接卡 48)連接到系統匯排流 23。除了監視器 47 之外，一般個人電腦也包含其他輸出裝置(圖未顯示)，例如揚聲器與印表機。

個人電腦 20 可以使用邏輯連接至一個或多個遠端電腦 49，而在一個網路環境中操作。遠端電腦 49 可以是其他個人電腦、伺服器、客戶端、路由器、網路 PC、監看裝置或是其他一般網路節點。一般遠端電腦 49，包含許多或所有上述的元件與個人電腦 20 產生連結關係，只有記憶儲存裝置 50 顯示在第 1 圖中。第 1 圖顯示的邏輯連結，包含局域區域網路(LAN)51 與 一 區 域(WAN)52。這樣的網路環境是平常設置在辦公室、廣域電腦網路、企業內部網路、網際網路。

當個人電腦 20 使用於 LAN 網路環境時，上述個人電腦 20 透過網路介面或轉接器 51 連結到區域網路(LAN)51。當個人電腦 20 使用於 WAN 網路環境時，通常包含一數據機 54，或其他可在 WAN 52 建立通信的裝置，例如網際網路。

數據機 54 可以是內建的或外接的，經由序列埠介面 46 連接到系統匯排流 54。在網路的環境下，圖所顯示與個

人電腦 20 或其部分相關的程式模組，可以被儲存在遠端記憶儲存裝置 50。可理解的是，圖示的網路連接是例示的，並且建立電腦之間通訊連結的其他手段可以被使用。

再者，熟悉此技藝之人士將理解本發明可以在其他電腦系統被執行，包含手持裝置；多處理器系統；微處理器為基礎之可程式化消費性電子產品；網路個人電腦；迷你電腦；大型主機電腦以及類似之裝置。本發明也可以在分散的電腦環境下實行，這些任務是由透過連結於通訊網路的遠端處理裝置以完成。在一分散電腦環境下，程式模組可被設在本地與遠端記憶儲存裝置兩者。

本發明示範實施例之執行

如同以上所描述，一般電腦系統通常包含硬體元件的複數類別。再者，上述電腦系統可以包含每個硬體元件類別之複數個元件(如兩個硬碟驅動裝置)。

上述本發明的堅定的硬體識別碼(SHWID)，考慮到在每個硬體的類別之間的每個元件(此處也被稱為每個"實體")。上述本發明的堅定的硬體識別碼(SHWID)也考慮到上述機密 S，其被結合到一指定電腦硬體系統。

本發明之產生一堅定的硬體識別碼的例示之方法，於以下所示。再者，一使用上述堅定的硬體識別碼(SHWID)的方法作為一反侵犯版權的工具，也於下所示。

I. *產生一堅定的硬體識別碼(SHWID)於一電腦系統*

一指定電腦的堅定的硬體識別碼包含 2 個不同的元

件：(1)一硬體元件，和(2)一局部的機密元件。決定每一個上述元件的例示之方法，於以下所示。上述例示之方法的步驟可以由一客戶的電腦的一軟體產品的軟體碼所完成，上述客戶的電腦類似於上述第 1 圖的電腦 20。

A. 決定上述 SHWID 的硬體元件

本發明的 SHWID 包含每個硬體元件的類別的類別產品。如第 2 圖所示，上述 SHWID 的硬體元件可以被決定。

如第 2 圖所示，一例示決定 SHWID 的硬體由步驟 201 開始，其中元件類別的數量 n，被挑選出來識別一指定電腦系統。如以上所示，一指定電腦系統可以包含多種的硬體元件和硬體元件的類別。示範硬體元件類別，包含但不限定於，硬碟驅動裝置、光碟驅動裝置、網路卡、音效卡、顯示介面卡、唯讀記憶體(ROM)、隨機存取記憶體(RAM)，和一 BIOS 系統。n-硬體元件類別的數字，最好是由大約 2 到大約 16 的整數。一般而言，n-最好是儘可能的大，為了(i)較精確地識別一指定電腦系統，(ii)較正確地測量一指定電腦系統的容許度之程度，和(iii)能夠提高機密 S 之安全的等級。

在步驟 201，選定上述元件類別數字 n 之後，每個元件類別在步驟 202 被識別。上述元件類別可以包含任一上述的元件類別，如硬碟驅動裝置的類別。一示範元件類別的清單如下表 1 所示。

表 1 例示之硬體元件的清單

元件類別編號	類別描述	類別識別符
1	光碟機	光碟機裝置識別符
2	硬碟機	硬碟分割區序列號碼
3	網路卡	MAC 位址
4	顯示介面卡裝置	識別符

如表 1 所示，在這個例子中，n 等於 4，並且識別硬體元件類別為：(1)一光碟機類別；(2)一硬碟機類別；(3)一網路卡類別；和(4)一顯示介面卡驅動裝置類別。

在步驟 202，每個元件類別被識別之後，在步驟 203 中在每個硬體元件之所有實體被識別。每個在特定元件類別的實體最好以最唯一而與上述實體相關的識別字串來表示。例如，硬體組態可能包含一由 NEC 股份有限公司所製造的光碟機驅動裝置，其具有一"NEC CDRW24 S15"的識別字串。任何可用來決定一指定實體之最獨一識別字串的方法，可以使用在本發明中，包含裝置資料庫與作業系統 API 函式呼叫。一電腦硬體組態與在每個硬體元件類別之間的實體的一個例子，被顯示於下表 2。

表 2 例示之每個元件類別的元件實例

元件類別編號	類別描述	類別元件實體
1	光碟機	{"NEC CDRW24 S15"，"TOSHIBA DVDR ASB-1425"}
2	硬碟機	{1bcdff1922，7da90024}

3	網路卡	{00b0c31b5923}
4	顯示介面卡裝置	{"NVidia GeForce2 DDR"}

如上表 2 所示，類別 1，一光碟機的類別，包含兩個元件實體；類別 2，一硬碟機的類別，包含兩個元件實體；類別 3，一網路卡的類別，包含一實體；和類別 4，一顯示介面卡驅動裝置的類別，包含一實體。

在步驟 205 中，每個元件實體使用一質數產生函數 $f(x)$，產生一實體的質數。函式 $f(x)$ 最好具下列特性：

(a) $f(x)$ 的結果是一個正的質數；

(b) x 可以是任何長度小於大約 65,000 的字元；和

(c) $f(x) > 2^t$，其中 t 是一個正整數，最好大於約 32 左右。再者，t 最好等於或大於約 64。然而，數值 t 是沒有限制的。

(d) $f(x)$ 的結果是基於 x 的值進行決定的。

任一質數產生函數 $f(x)$ 可以使用在本發明中，用來在每個元件實體產生一質數。如上列所討論，上述質數產生函數 $f(x)$ 最好以上列的特性進行處理。適當的質數產生函數 $f(x)$，包含但不限定於，基於 Rabin-Miller 演算法的質數產生函數 $f(x)$，上述演算法於由 Bruce Schneier 所著的 Applied Cryptography,Second Edition，第 259 至 260 頁中揭露。上述揭露事項，將於本文中引用。

下表 3 提供一個例示之硬體組態的實體質數，$i_{p,q}$，的清單。

表 3 例示之元件實體的實體質數

元件類別編號	類別描述	元件實體之實體質數
1	光碟機	{f("NEC CDRW24 S15")= $i_{1,1}$, f("TOSHIBA DVDR ASB-1425")= $i_{1,2}$}
2	硬碟機	{f(1bcdff1922)= $i_{2,1}$, f(7da90024)= $i_{2,2}$}
3	網路卡	{f(00b0c31b5923)= $i_{3,1}$}
4	顯示介面卡裝置	{f("Nvidia GeForce2 DDR")= $i_{4,1}$}

此處所使用的實體質數 $i_{p,q}$，是在一類別 p 中用來標定實體質數 q。例如，實體質數 $i_{1,2}$，是用來識別在元件類別 1(如 p=1)之元件實體的實體質數，更具體地在上述電腦硬體組態中，元件類別 1 中第 2 元件實體(如 q=2)。

本發明的一種實施例，在產生一指定元件實體的實體質數之前，一“salt 值(以加密法產生的強式亂數)”可以加到元件實體識別子。在本實施例中，加入一 salt 值使根據相同的電腦硬體組態，能有不同 SHWID 的產出物。衍生自應用程式碼或使用者身份的 salt 值，使在相同的硬體組態中之不同應用程式或使用者執行不同的 SHWID 成為可能，如此當僅供特定應用程式或使用者使用機密的資料是有幫助的。一旦產生各元件實體的實體質數時，則可產生每一元件類別的類別乘積 c_p，如步驟 206 所示。類別乘積 c_p 是由在一指定的類別與另一個類別之實體質數的乘

積。例示之類別乘積 c_1 到 c_4，如下列表 4 中所示。

表 4 例示之每個元件類別的類別乘積

元件類別編號	類別描述	每個元件類別之類別乘積
1	光碟機	$c_1 = (i_{1,1}) \times (i_{1,2})$
2	硬碟機	$c_2 = (i_{2,1}) \times (i_{2,2})$
3	網路卡	$c_3 = i_{3,1}$
4	顯示介面卡裝置	$c_4 = i_{4,1}$

如表 4 所示，上述硬體元件類別，光碟機之類別乘積 c_1，是等於 $i_{1,1}$ 和 $i_{1,2}$ 兩個實體的乘積。值得注意的是，由一單獨實體質數得到的類別乘積，如類別乘積 c_3，可以乘上額外的非實體質數來增加分解一指定類別乘積的難度。上述的方法是對由單獨實體質數組成的類別乘積，是特別有用的，如在上表 4 中的類別乘積 c_3 或類別乘積 c_4。當額外非實體質數是用來增加類別乘積值，上述非實體質數最好是大於 2 但小於 2^t，其中 t 是如上述的一個任意的整數。此將降低在各種的硬體組態中，元件間質數意外地衝突的風險。在步驟 207 中，每個類別乘積 c_p 被儲存，輸入至每個元件類別之堅固類別識別 C_p，如下列所示。再者，如下列所示，於一指定電腦硬體系統中，每個元件的每個堅固類別識別的組合 C_p，被用來產生堅定的硬體識別碼(SHWID)。上述類別乘積 c_p，表示在一指定電腦硬體系統之堅定的硬體識別碼(SHWID)的硬體元件。

B. 決定 SHWID 的局部的機密元件

本發明的堅定的硬體識別碼(SHWID)至少包含硬體元件的每個類別之局部的機密元件。一決定 SHWID 的局部的機密元件的例示之方法，於第 3-4 圖所示。該例示之方法的步驟，可於一客戶的電腦中軟體產品中之軟體碼所完成，上述客戶的電腦類似電腦 20，參照上列第 1 圖的描述。

在第 3 圖所示的步驟 301，一隨機的數字 r_p，是由每個使用隨機數字產生器的元件類別所產生的。任何常見的隨機數字產生器，可以被用來產生隨機數字 r_p。適當的隨機數字產生器，包含但不限定於，由 Crandell 與 Pomerance 所著的 Prime Numbers 中第 8 章所揭露，該揭露係併入作為參考。上述隨機數字 r_p 範圍，最好由大於或等於 0 至小於 2^u，此處的 u 最好小於上述的 t。一般而言，u 大約等於 t 除於 3。

利用步驟 301 中所產出之每個硬體元件類別的隨機數字 r_p，進而在步驟 302 中，類別質數 p_p 利用質數產生器函式 $g(r_p)$來產生。上述質數產生函式 $g(r_p)$最好有下列的特性：

(a) $g(r_p)$的結果為一正整數；

(b) $g(r_p) < 2^v$，其中的 v 為大於 u 的整數；及

(c) $u+v=t$；

(d) $g(r_p)$的結果是基於 r_p 的值運算所決定的；

如同以上所述的質數產生函式 $f(x)$，任何質數產生函式 g(x)可以使用在本發明，利用每個元件類別隨機數字 r_p

產生一質數。如上所述，上述質數產生函式 g(x)最好具有上列特性。適當的質數產生函式 g(x)，包含但不限定於，由 Bruce Schneier 所著的 Applied Cryptography,Second Edition，第 259 至 260 頁所揭露的，該揭露係併入作為參考。

在 $g(r_p)$、t、u 及 v 間的關係如下例所示。

$$t=64$$

$$u=20$$

$$v=44$$

$$0<r_p<2^u(2^{20}=1,048,576)$$

$$2<g(r_p)<2^v$$

一例示之每個示範電腦系統的 n 個類別之(如 n=4)類別質數 p_p 清單，如下表 5 所示。

表 5 例示之每個元件類別的類別質數

元件類別編號	類別描述	每個元件類別之類別質數
1	光碟機	$p1=g(r1):0<r_1<2^u$
2	硬碟機	$p2=g(r2):0<r_2<2^u$
3	網路卡	$p3=g(r3):0<r_3<2^u$
4	顯示介面卡裝置	$p4=g(r4):0<r_4<2^u$

在一指定硬體組態下，一顯示介於類別質數間關係的例子，如下所述。

$$2<p_2<p_3<p_1<p_4<2^v$$

在步驟 303，必要元件類別匹配之數量 m 是最好依硬體組態元件改變的容許度之程度而選定的。上述必要元件類別符合的數量 m 可以大到 n，也可小至 1，上述的 n 為元件種類的總數。當 m 增大時，上述電腦硬體組態之改變的容許度之程度減小。例如，若電腦元件類別總數 n 等於 4，及 m 等於 3，來自元件總數 4 個的 3 個，m 需符合至少一個元件實體，以取回機密 S，使得可以載入或執行一軟體產品。若元件類別的符合之數量小於 3，則機密 S 將不會被取回，上述軟體產品將無法在上述電腦硬體組態中執行或載入。

必要元件類別匹配之數量 m 可以是由一軟體製造商預先決定並且編碼至本發明之 SHWID 產生的方法，一旦選定了 m，則可如步驟 304 和步驟 305 來決定額外的參數。

在步驟 304，參數 N 被決定，其中 N 等於上述最小的 m 個類別質數 p_p 的乘積。例如，如上所述之類別質數的例子之類別質數的值，兩個最小類別質數為 p_2 和 p_3。假如 m 等於 2，N 等於 $(p_2)X(p_3)$。

在步驟 305，得到參數 M，其中 M 等於上述最大的 (m-1) 個類別質數的乘積。例如，如上所述之類別質數的例子之類別質數的值，p_4 是最大類別質數。假如 m 等於 2，那麼 M 等於上述單一最大的質數 p_4 的乘積 (即 (M-1)=1)。下例的事項應被注意，M 必需小於 N，以確保指定的一組類別質數有一臨界值 m。

於 S.C. Coutinho 所著的 The Mathematics of Ciphers

第 7 章所描述一臨界基礎的機密共享模式，該揭露係併入作為參考。

一旦參數 N 及 M 被決定之後，則可由步驟 306 可選定機密 S。機密 S 大於 M 小於 N。再者，機密 S 是介於 M 和 N 之間的一個隨機數字。

在步驟 307，類別餘數 d_p 可由下列方程式計算得知。

$d_p = S \bmod p_p$

一例示之一組類別餘數 d_p，如下表 6 所示。

表 6 例示之每個元件類別之類別餘數

元件類別編號	類別描述	每個元件類別之類別餘數
1	光碟機	$d_1 = S \bmod p_1$
2	硬碟機	$d_2 = S \bmod p_2$
3	網路卡	$d_3 = S \bmod p_3$
4	顯示介面卡裝置	$d_4 = S \bmod p_4$

在第 4 圖之步驟 308 中，每個元件類別之類別質數 p_p 被編碼至每個元件類別之第 1 個二進制值。下列之事項應注意，由於下列的關係，每個質數 p_p 可以 u 個位元表示：

$p_p = g(r_p)$， where $0 <= r_p < 2^u$

如果 $g(r_p)$在取回之時間是可利用的，則 p_p 可以 r_p 表示

r_p 能以 u 個位元表示

若 $g(r_p)$在取回之時間是可用的，若因下列的原因，質數數字產生函式 g()是已知的，則 p_p 可以用 r_p 來表示。當

p_p 等於 $g(r_p)$ 並且上述的質數產生器函式 $g()$ 是已知的，則已知的 r_p 可以利用 $g()$ 和參數 r_p，再度產生 p_p。編碼 r_p 需要 u 個位元（或上例的 20 個位元），然而 p_p 需要 v 個位元（或上例的 44 個位元）。利用 r_p 來表示 p_p，可以節省需求位元的數量。

在步驟 309，每個類別餘數 d_p 被編碼至每個元件類別之第 2 個二進制值。上述第 2 個二進制值可用 v 個位元來表示。下列的事項應注意，由於下列的關係，所以元件餘數 d_p 可以 v 個位元來表示：

$$d_p = S \bmod p_p$$

$$0 < p_p < 2v$$

因此，$d_p < 2^v$

在步驟 310 中，由步驟 308 中產生的第 1 個二進制值連接來自於步驟 309 中第 2 個二進制值，以形成一編碼的元件類別局部的機密 P_p，上述 P_p 共有 t 個位元（即 $t = u + v$）。每個元件類別產生一元件類別局部的機密 P_p。

下例的事項應注意，在一給定的元件類別之類別局部的機密 P_p，可包含未使用的位元 z，因為第 2 個二進制值小於 v 個位元。在本例中，上述未使用位元 z，可以移作隨機雜訊以防止一攻擊者，上述攻擊者知悉 $g(r_p)$ 的特性，可以估算上述編碼之類別局部的機密 P_p。

例如，當 p_p 位於 2 至 2^v 的區間內時，d_p 總是小於 p_p。若 p_p 遠小於 2^v，那麼 d_p 將只要求遠小於 v 個位元來進行編碼。一攻擊者可基於 d_p 的值，來大約猜測 p_p 的大小。

增加隨機的雜訊用來填滿未使用的 d_p 的[v-(d_p 的大小)]個位元，有助於隱藏 p_p 的大小。

C. 電腦系統之 SHWID

堅定的硬體識別碼(SHWID)現在可以利用在步驟 207 所得到的類別乘積 c_p 及在步驟 310 所得到的 P_p，來被進行組態。如在第 5 圖中步驟 401 所示，每個元件類別產生類別堅固識別 C_p，其中 $C_p = c_p + P_p$。在步驟 402 中，元件類別的所有類別堅固識別 Cp 結合地形成堅定的硬體識別碼(SHWID)。上述的結果-堅定的硬體識別碼(SHWID)被儲存起來以供日後取回。上述 SHWID 可以儲存於本地端(即在註冊區、檔案系統或安全儲存)或者在一可儲存的遠地端(即一資料庫)。

為了產出一具有較大位元數量的類別局部的機密，下列的事項應被注意，可藉由增加 t 的值來增加安全性。

II 由一使用堅定的硬體識別碼(SHWID)之電腦系統取回一機密

本發明更進一步是被應用在一種方法，上述方法從一指定電腦硬體組態下，取回或試圖取回一被連結的機密 S。本發明實施例在一指定電腦配置下，試圖取回被連結的機密 S 的一種方法是起始於(i)安裝軟體產品期間，(ii)載入已存於一硬體組態之元件的軟體應用程式，(iii)上述都包含。於一硬體組態下，例示之取回被連結的機密 S 之

方法，如第 6-7 圖所示。上述例示之方法的步驟，可在一客戶電腦之軟體產品裡面的軟體碼來實行，上述的客戶的電腦類似於參照第 1 圖所描述之電腦 20。

在第 6 圖的步驟 501，於一指定電腦配置下，堅定的硬體識別碼之堅固類別識別 C_p 被識別。為例示本發明的目的，將描述從三個不同的硬體組態 H、H_1、H_2 中，使用在硬體組態 H 下所決定堅定的硬體識別碼 SHWID 來取回被連結的機密的方法。上述 3 個不同的硬體組態至少包含(i)產生上述 SHWID 之真正的硬體組態 H；(ii)一硬體組態 H_1，至少包含在可接受容許度之程度內，具有一至多個元件改變的硬體配置 H；(iii)硬體組態 H_2，表示改變夠多元件的硬體組態 H，使得硬體組態 H_2 超出與硬體組態 H 比較的可接受容許度之程度。

硬體組態 H、H_1、H_2 下，例示之一組堅固類別識別，如下表 7。

表 7 一硬體組態的例示之堅固類別識別

元件類別編號	類別描述	堅固類別識別
1	光碟機	C_1
2	硬碟機	C_2
3	網路卡	C_3
4	顯示介面卡裝置	C_4

在步驟 502，在一指定硬體組態的每個元件類別內之

所有實體被識別。如上所述，任一常見的方法可被用來識別每個元件實體。一般而言，一元件實體藉由元件的最唯一的識別字串來被識別。在範例配置 H、H_1、H_2 中，每個元件實體的例示識別字串，如下表 8-10 所示。

表 8 硬體組態 H 的例示之元件實體

配置 H		
元件類別編號	類別描述	元件實體
1	光碟機	{“NEC CDRW24 S15”，”TOSHIBA DVDR ASB-1425”}
2	硬碟機	{1bcdff19，7da90024}
3	網路卡	{00b0c31b5923}
4	顯示介面卡裝置	{“NVidia GeForce2 DDR”}

表 9 硬體組態 H_1 的例示之元件實體

配置 H1		
元件類別編號	類別描述	元件實體
1	光碟機	{“NEC CDRW24 S15”，”SONY DVD 1221”}
2	硬碟機	{8146af92}
3	網路卡	{00c0c21b5933}
4	顯示介面卡裝置	{“NVidia GeForce2 DDR”}

表 10 硬體組態 H_2 的例示之元件實體

配置 H2		
元件類別編號	類別描述	元件實體

1	光碟機	{"SONY DVD 1221"}
2	硬碟機	{8146af92}
3	網路卡	{00c0c21b5933}
4	顯示介面卡裝置	{"NVidia GeForce2 DDR"}

一旦一指定硬體組態之每個元件類別內的所有實體被辨識之後，則每個實體之最唯一的識別字串可被取回，如步驟 503 所示。

上述每個實體之識別字串使用質數數字產生函式 f(元件實體識別字)，來產生每個元件實體之實體質數，如步驟 504 所示。熟知此技藝之人士應該知道，質數數字產生函式 f(元件實體識別子)可以是任一種質數數字產生函式。下表 11-13，提供在範例配置 H、H_1、H_2 內的每個元件實體的例示之實體質數

表 11 範例硬體組態 H 的例示之實體質數 $i_{p,q}$

配置 H		
元件類別編號	類別描述	實體質數
1	光碟機	{*f*("NEC CDRW24 S15")=$i_{1,1}$, *f*("TOSHIBA DVDR ASB-1425")=$i_{1,2}$}
2	硬碟機	{*f*(1bcdff19)=$i_{2,1}$, *f*(7da90024)=$i_{2,2}$}
3	網路卡	{*f*(00b0c31b5923)=$i_{3,1}$}
4	顯示介面卡裝置	{*f*("NVidia GeForce2 DDR")=$i_{4,1}$}

表 12 範例硬體組態 H_1 的例示之實體質數 $i_{p,q}$

配置 H_1		
元件類別編號	類別描述	實體質數
1	光碟機	{f("NEC CDRW24 S15")=$i_{1,1}$, f("SONY DVD 1221")=$i_{1,3}$}
2	硬碟機	{f(8146af92)=$i_{2,3}$}
3	網路卡	{f(00c0c21b5933)=$i_{3,1}$}
4	顯示介面卡裝置	{f("NVidia GeForce2 DDR")=$i_{4,1}$}

表 13 範例硬體組態 H_2 的例示之實體質數 $i_{p,q}$

配置 H_2		
元件類別編號	類別描述	實體質數
1	光碟機	{f("SONY DVD 1221")=$i_{1,3}$}
2	硬碟機	{f(8146af92)=$i_{2,3}$}
3	網路卡	{f(00c0c21b5933)=$i_{3,2}$}
4	顯示介面卡裝置	{f("NVidia GeForce2 DDR")=$i_{4,1}$}

下列的事項應被注意，元件實體{f("SONY DVD 1221")}被標定成 $i_{1,3}$，為考慮上述硬體組態(即 H，H_2，H_3)中的光碟機的種類之第 3 個光碟機。

在步驟 505，所有可能之類別局部的機密 $P_{p,q}$ 被決定，其中 $P_{p,q}$ 等於 C_p mod $i_{p,q}$。如上所述，每個元件類別之堅固類別識別 C_p，為每個類別之類別乘積 c_p 加上類別局部的機密 P_p 的總和。若堅固類別識別 C_p 除以一實體質數 $i_{p,q}$ 被表示成基於原來硬體組態之上述堅定的硬體識別碼 SHWID，則在 mod 運算子後的餘數提供了一可能之類別局

部的機密 $P_{p,q}$。在範例硬體組態 H、H_1、H_2 下，例示之可能之類別局部的機密 $P_{p,q}$，如下表 14-16 所示。

表 14 範例硬體組態 H 下，每個元件實體的例示之可能之類別局部的機密 $P_{p,q}$

配置 H		
元件類別編號	類別描述	可能類別之局部機密
1	光碟機	$P_{1,1}=C_1 \bmod i_{1,1}$, $P_{1,2}=C_1 \bmod i_{1,2}$
2	硬碟機	$P_{2,1}=C_2 \bmod i_{2,1}$, $P_{2,2}=C_2 \bmod i_{2,2}$
3	網路卡	$P_{3,1}=C_3 \bmod i_{3,1}$
4	顯示介面卡裝置	$P_{4,1}=C_4 \bmod i_{4,1}$

表 15 範例硬體組態 H_1 下，每個元件實體的例示之可能之類別局部的機密 $P_{p,q}$

配置 H_1		
元件類別編號	類別描述	可能類別之局部機密
1	光碟機	$P_{1,1}=C_1 \bmod i_{1,1}$,$P_{1,3}=C_1 \bmod i_{1,3}$
2	硬碟機	$P_{2,3}=C_2 \bmod i_{2,3}$
3	網路卡	$P_{3,2}=C_3 \bmod i_{3,2}$
4	顯示介面卡裝置	$P_{4,1}=C_4 \bmod i_{4,1}$

表 16 範例硬體組態 H_2 下，每個元件實體的例示之可能類別之局部機密 $P_{p,q}$

配置 H_2		
元件類別編號	類別描述	可能類別之局部機密

1	光碟機	$P_{1,3}=C_1 \bmod i_{1,3}$
2	硬碟機	$P_{2,3}=C_2 \bmod i_{2,3}$
3	網路卡	$P_{3,2}=C_3 \bmod i_{3,2}$
4	顯示介面卡裝置	$P_{4,1}=C_4 \bmod i_{4,1}$

由每個可能之類別局部的機密 $P_{p,q}$，隨機數字 r_p 和類別餘數 d_p 可以被萃取出來，如步驟 506 所示。如上所述，類別質數 $p_{p,q}$ 是可以用函式 $g(r_p)$ 來取回的，其中 r_p 是可能之類別局部的機密 $P_{p,q}$ 之起始的 u 個位元。類別餘數 $d_{p,q}$ 可以由類別局部的機密 $P_{p,q}$ 之最後的 v 個位元中取回。範例硬體組態 H、H_1、H_2 下，所有可能的類別質數 $p_{p,q}$ 和類別餘數 $d_{p,q}$ 的例示之清單，如下表 17-19 所示。

表 17 範例硬體組態 H 的每一可能類別之局部的機密 $P_{p,q}$ 例示之類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$

配置 H		
元件類別編號	類別描述	可能類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$P_{1,1}=>p_{1,1}, d_{1,1}, P_{1,2}=>p_{1,2}, d_{1,2}$
2	硬碟機	$P_{2,1}=>p_{2,1}, d_{2,1}, P_{2,2}=>p_{2,2}, d_{2,2}$
3	網路卡	$P_{3,1} => p_{3,1}, d_{3,1}$
4	顯示介面卡裝置	$P_{4,1} => p_{4,1}, d_{4,1}$

表 18 範例硬體組態 H_1 的每一可能類別之局部的機密 $P_{p,q}$ 例示之類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$

配置 H_1

元件類別編號	類別描述	可能類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$P_{1,1} => p_{1,1}, d_{1,1}, P_{1,3} => p_{1,3}, d_{1,3}$
2	硬碟機	$P_{2,3} => p_{2,3}, d_{2,3}$
3	網路卡	$P_{3,2} => p_{3,2}, d_{3,2}$
4	顯示介面卡裝置	$P_{4,1} => p_{4,1}, d_{4,1}$

表 19 範例硬體組態 H_2 的每個可能之類別局部的機密 $P_{p,q}$ 的例示之類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$

配置 H_2		
元件類別編號	類別描述	可能的類別質數 $p_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$P_{1,3} => p_{1,3}, d_{1,3}$
2	硬碟機	$P_{2,3} => p_{2,3}, d_{2,3}$
3	網路卡	$P_{3,2} => p_{3,2}, d_{3,2}$
4	顯示介面卡裝置	$P_{4,1} => p_{4,1}, d_{4,1}$

在步驟 506，一旦決定所有可能的類別質數和類別餘數，則可表示成一組同餘數。S 是一個大的數字，當上述 S 除以可能的類別質數 $p_{p,q}$，產出指定的一組同餘數之類別餘數 $d_{p,q}$。因為 S 是小心地選擇出來的(即 S 介於 M 和 N 之間)並且所有的除數為質數，因此使用可能之類別質數和類別餘數所得到落在 M 和 N 之間的解，必定為 S。在步驟 306，上述小心地選出的 S，確保僅有 N 個符合該組同餘數之要素被要求以產出 S 的正確解。上述為一古典臨界基礎的機密共享模式，如於 S.C. Coutinho 所著 The Mathematics of Ciphers 的第 7 章所述，該揭露係併入作為參考。

提早決定任何可能的類別質數和餘數，以符合正確的硬體組態，是不可能發生的。因此，在步驟 507 中，利用解出排列之離散的一組同餘，來產生每個類別質數和類別餘數之排列的可能之機密是必需的。如步驟 508 所示，作為結果之可能的機密能使用密文來測試，以達成驗證的目的。如下列的處理過程。

本發明中，已知的純文字(plaintext)使用機密 S 當作鑰匙，編碼形成密文。一般而言，一被加密後的訊息(即密文)是伴隨一驗證符記，使解碼器知道上述訊息已成功地被編碼。上述驗證符記，通常不是一個純文字訊息的雜湊，就是一些選定的純文字。在本發明中，為了簡單化，所以使用選定的純文字。所以當 SHWID 被產生時，選定的純文字(例如"這是一選定的純文字")使用 S(即當作鑰匙)來加密產出密文。解碼器知道上述選定的純文字和上述的密文兩者。

在上述狀況，S(即，每個可能的機密之結果)之候選者的有效性被驗證，利用 S(即，每個可能的機密之結果)之候選者作為鑰匙，來解譯密文。若作為結果的純文字符合選定的純文字，那麼上述 S(即，一可能的機密之結果)之候選者，事實上就是 S。若上述作為結果的純文字不符合選定的純文字，那麼上述 S 之候選者(即，一可能的機密之結果)，並不是 S。

如第 7 圖所示，若已知之純文字藉由使用可能的機密解譯密文而被揭露，那麼可以得知機密 S，並且上述的方

法將處理至步驟 510 中，其中程式允許一指定軟體產品被載入或被安裝在一指定的電腦硬體組態。除此之外，上述方法將處理至步驟 509。若更多排列存在且未進行測試，上述方法返回步驟 507。除此之外，SHWID 不符合而且上述方法處理至步驟 511，以防止載入或安裝軟體產品。

例示之範例配置 H、H1、H2 的結果，如下表 20-22 所示。

表 20 範例硬體組態 H 下，例示之顯示介於可能的機密 $S_{p,q}$ 及實際機密 S 中的符合數量的結果

配置 H		
元件類別編號	類別描述	可能類別質數 $P_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$S = d_{1,1} \pmod{p_{1,1}}$ 或 $S = d_{1,2} \pmod{p_{1,2}}$
2	硬碟機	$S = d_{2,1} \pmod{p_{2,1}}$ 或 $S = d_{2,2} \pmod{p_{2,2}}$
3	網路卡	$S = d_{3,1} \pmod{p_{3,1}}$
4	顯示介面卡裝置	$S = d_{4,1} \pmod{p_{4,1}}$
結果-單一解答 4 個中 4 個符合 S		

表 21 範例硬體組態 H_1 下，例示之顯示介於可能的機密 $S_{p,q}$ 及實際機密 S 中的符合數量的結果

配置 H_1		
元件類別編號	類別描述	可能的類別質數 $P_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$S = d_{1,1} \pmod{p_{1,1}}$ 或 $S = d_{1,3} \pmod{p_{1,3}}$
2	硬碟機	$S = d_{2,3} \pmod{p_{2,3}}$
3	網路卡	$S = d_{3,2} \pmod{p_{3,2}}$
4	顯示介面卡裝置	$S = d_{4,1} \pmod{p_{4,1}}$
結果-二種可能解答，依使用 $d_{1,1}$(4 個中 2 個符合，找到 S)或 $d_{1,3}$(4 個中 1 個符合，找到 Z_1)		

表 22 範例硬體組態 H_2 下，例示之顯示介於可能的機密 $S_{p,q}$ 及實際機密 S 中的符合數量的結果

配置 H_2		
元件類別編號	類別描述	可能的類別質數 $P_{p,q}$ 及類別餘數 $d_{p,q}$
1	光碟機	$S = d_{1,3} \pmod{p_{1,3}}$
2	硬碟機	$S = d_{2,3} \pmod{p_{2,3}}$
3	網路卡	$S = d_{3,2} \pmod{p_{3,2}}$
4	顯示介面卡裝置	$S = d_{4,1} \pmod{p_{4,1}}$
結果-單一解答，4 個中 1 個符合，找到 Z_1		

如上表 20 所示，原來硬體組態 H 會有 4 個中 4 個符合介於可能的機密 $S_{p,q}$ 和實際的機密 S。如上表 21 所示，硬體組態 H_1 最多有 4 個中可能符合 2 個(依使用那個類別餘數 $d_{p,q}$ 而定)，用來依類別餘數 $d_{p,q}$ 使用判斷可能的機密

S。在範例配置中，若 m 等於 2，此程式允許取回被連結的機密 S 並且一軟體產品可在硬體組態 H_1 下被載入或者被安裝。無論如何，在上表 22 所示的硬體組態 H_2 中，4 個中僅有一個符合。若 m 等於 2，則錯誤的非機密 Z_1 被產生，並且上述方法防止特定軟體被載入或被安裝於硬體組態 H_2 中。

如上所述並且例示於第 2 圖，第 3-4、5 和 6-7 圖的上述方法之步驟，可以在一本地端或遠端實行。一般而言，一客戶購買一軟體產品，並可於一指定電腦(如第 1 圖之電腦 20)中執行。上述軟體產品可以是一被膠膜包裝之可運送的電腦可讀媒體，如光碟片或軟式磁碟。上述軟體產品也可以於網路上以電子手段散佈，如一局部地區網路(LAN)，或是廣域網路(WAN)。上述客戶載入上述軟體產品至電腦 20，如同一程式被儲存於系統記憶體 22。於一軟體產品安裝期間，上述客戶一般被提示，輸入一軟體產品識別(PID)以安裝該軟體產品至電腦 20 中。上述 PID 可以為，例如印在膠膜包裝的一 CD 鑰匙。上述客戶輸入上述 PID，以結合上述軟體產品之軟體程式。上述 PID 是本地端地儲存於電腦 20，及(或)遠端地儲存於一可存取區域，上述可存取區域不是位於一區域網路(LAN)51，就是一位於有第 3 方(例如一活化之管理機構)之廣域網路(WAN)52。

如上所述，在軟體安裝期間，利用使用上述軟體產品中程式碼或由軟體產品的安裝所驅動，產生了一堅固硬識別(SHWID)。本發明之方法所產生的堅定的硬體識別碼

SHWID，結合軟體產品識別(PID)，並且與軟體產品識別(PID)一起本地端地儲存於電腦 20，及(或)遠端地儲存於一可存取的區域，上述可存取區域不是位於一區域網路(LAN)51，就是位於一有第 3 方之廣域網路(WAN)52，例如活化的管理機構。

當作安裝處理之一部分，客戶可被要求以活化的管理機構來啟動一軟體產品。管理機構可以為，例如，軟體製造商或一經授權的第 3 方。活化的處理是打算迫使使用者活化軟體產品在(i)一特定電腦安裝及使用，或(ii)根據產品授權合約之條款的安裝及使用。上述的一活化的處理詳述於讓渡給 Microsoft Corporation (Redmoned， WA)之美國專利編號 6,243,468，上述之內容係併入作為參考。

由本發明之方法所產生之堅定的硬體識別碼(SHWID)與軟體產品識別(PID)，可以本地端地儲存於電腦 20，及(或)遠端地儲存於一可存取的區域，上述可存取區域不是位於一區域網路(LAN)51，就是位於一有第 3 方之廣域網路(WAN)52，例如活化的管理機構。當軟體產品第 1 次使用時，最好能自動顯示一圖形化使用者介面(UI)對話方塊，以提示使用者啟使連接一活化的伺服器，以活化上述軟體產品。上述啟動伺服器維護一資料庫以儲存所接收的堅定的硬體識別碼(SHWID)和上述 SHWID 結合之軟體產品識別(PID)。

一指定電腦的堅定的硬體識別碼(SHWID)和與其結合之軟體產品識別可以儲存在不確定之時間週期，直到上述

軟體產品被重新安裝於另一電腦上或在第 1 台電腦上被啟始(即，在初始安裝期間之電腦上使用)。當相同軟體產品被重新安裝於另一電腦或被第 1 台電腦啟始，則在軟體產品內之程式碼啟始一根據本發明來決定是否一軟體產品能使用於一電腦系統的方法。上述軟體產品取回先前儲存的軟體產品之軟體產品識別(PID)結合的堅定的硬體識別碼(SHWID)，上述之 SHWID，從本地端電腦 20 或從一遠地端，經由一區域網路 LAN 或經由廣域網路 WAN 來取回。如上所述，使用先前儲存之堅定的硬體識別碼 SHWID 所產生的決定，作為上述軟體產品能於一電腦組態下使用的依據。

因為第 1 台電腦(即，使用於起始安裝之電腦)之硬體組態顯著的改變，所以使用軟體產品被拒絕時，則一對話方塊可被提供給客戶，上述對話方塊指出使用軟體產品被拒絕並且進一步使用上述軟體產品之進一步的資訊，可以由一指定之來源得到。

III. 堅定的硬體識別碼之其他使用

除了如上所述之使用之外，本發明之堅定的硬體識別碼(SHWID)可以用來加(解)密一僅能使用於一特定硬體組態之資料。

雖然上述係有關於本發明之實施例，但本發明之其他或進一步實施例可以在不脫離本發明之基本範圍下完成，本案之範圍係由以下之申請專利範圍所決定。

【圖式簡單說明】第 1 圖為執行本發明之示範作業環境的一些基本元件之流程圖。

第 2 圖為一流程圖，顯示決定在堅定的硬體識別碼(SHWID)的硬體識別元件的示範步驟。

第 3-4 圖為一流程圖，顯示決定在堅定的硬體識別碼的(SHWID)局部的機密元件的示範步驟。

第 5 圖為一流程圖，顯示組合硬體識別元件和堅定的硬體識別碼(SHWID)的機密元件的示範步驟。

第 6-7 圖為一流程圖，顯示例示之步驟，上述步驟利用被連結的機密之取回作為軟體產品之有效的因子，來決定是否一軟體產品可用於一電腦硬體系統。

【元件代表符號簡單說明】

20 個人電腦	21 處理單元
22 系統記憶體	23 系統匯排流
24 唯讀記憶體	25 隨機存取記憶體
26 基本輸入出系統	27 硬碟驅動裝置
28 磁片驅動裝置	29 磁片
30 光碟驅動裝置	31 光碟
32 硬碟驅動介面	33 磁片驅動介面
34 光碟驅動介面	35 作業系統
36 應用程式模組	37 程式模組
38 程式資料	40 鍵盤
42 滑鼠	46 序列埠介面

48 視訊配接卡
49 遠端電腦伺服器
50 記憶儲存裝置
51 區域網路
52 廣域網路
53 網路介面
54 數據機
100 應用程式
105 函式庫

伍、中文發明摘要：

本發明所揭示為連結一機密至一電腦系統的系統及方法。 也揭示對一指定的電腦系統，用以產生一堅定的硬體識別碼(SHWID)之系統及方法。 上述堅定的硬體識別碼(SHWID)是耦接到一被連結的機密。 依電腦系統之硬體變化的程度，該堅定的硬體識別碼(SHWID)可用來控制軟體的使用於該指定的電腦系統上。

陸、英文發明摘要：

Systems and methods for binding a secret to a computer system are disclosed. System and methods for generating a strong hardware identification (SHWID) for a given computer system are also disclosed. The strong hardware identification (SHWID) is coupled to a bound secret. The strong hardware identification (SHWID) may be used to control the use of software on the given computer system depending on the degree of hardware changes to the computer system.

拾、申請專利範圍：

1. 一種產生一堅定的硬體識別碼(SHWID)用於一具有一第一硬體組態之一第一電腦系統的方法，該方法至少包含下列步驟：

識別在該第一硬體組態內的每一元件類別，其中該元件類別的數量等於 n；

決定每一元件類別之一類別乘積 c_p；

決定每一元件類別之一局部的機密 P_p；及

對每一元件類別，相加該類別乘積 c_p 與該局部的機密 P_p 以形成 n 堅固的類別識別碼；

其中該 n 堅固的類別識別碼以組合的方式形成該第一電腦系統之該堅定的硬體識別碼(SHWID)。

2.如申請專利範圍第 1 項所述之方法，其中 n 是一最大到大約 16 的整數。

3.如申請專利範圍第 1 項所述之方法，其中每一元件類別之該類別乘積 c_p，由下列步驟所決定：

選擇該元件類別的數量 n；

識別該 n 個元件類別；

識別在每一元件類別內之所有實體；

對每一元件實體指定一識別字串；

產生每一元件實體之實體質數 $p_{p,q}$，其中每一實體質數

是一正質數，並且其中 p 表示一範圍由 1 到 n 之指定的元件類別數字，並且其中 q 表示該第一硬體組態中第 q 個元件形態；及

相乘在每一元件類別內的實體質數以形成類別乘積 c_p。

4.如申請專利範圍第 3 項所述之方法，其中該產生實體質數之步驟，至少包含輸入每一元件實體之識別字串至一質數產生函式 *f(x)*，其中 x 是一最大長度至約 65,000 字元之識別字串。

5.如申請專利範圍第 4 項所述之方法，其中 *f(x)* 產生一大於 2^t 之正質數，其中 t 是一整數，其範圍自大約 32 至大約 2,048。

6.如申請專利範圍第 1 項所述之方法，其中每一元件類別之該局部的機密 P_p，由下列步驟所決定：

產生每一元件類別之一隨機數字 r_p；

產生每一元件類別之類別質數 p_p，其中每一類別質數是一正質數；

選擇一必要元件類別符合之數量 *m*，其中 m 是小於或等於 *n*；

決定 *N*，其中 *N* 等於 *m* 個最小類別質數 p_p 之乘積；

決定 *M*，其中 *M* 等於 *m-1* 個最大類別質數 p_p 之乘積，

並且 M 小於 N；

選擇一機密數字 S，其中 $M < S < N$；

決定每一元件類別之類別餘數 d_p，其中 d_p 等於 $[S(\mathrm{mod}\ p_p)]$；

形成每一元件類別之一第一個二進制值，其中該第一個二進制值是類別質數 p_p 對每一類別編碼成為最大達到 u 個位元之一第一個二進制數，其中 u 係小於 t，且 u 和 t 兩者均小於大約 2,048；

形成每一元件類別之一第二個二進制值，其中該第二個二進制值是類別餘數 d_p 對每一類別編碼成為最大達到 v 個位元的一第二個二進制數，其中 v 係小於 t，且 (u + v = t)；及

連結第一個二進制值和第二個二進制值，以形成每一元件類別之局部的機密 P_p，該 P_p 的總位元數等於 t。

7.如申請專利範圍第 6 項所述之方法，其中每一隨機數字 r_p 係由使用一隨機數字產生器所產生，並且具有一範圍由 0 到小於 2^u 的值。

8.如申請專利範圍第 6 項所述之方法，其中產生每一元件類別之類別質數 p_p 的步驟至少包含輸入每一元件類別之該隨機數字至一質數產生函式 g(x)，其中 x 是一最大長度達到約 65,000 字元之該隨機數字。

9.如申請專利範圍第 8 項所述之方法，其中 g(x)產生一正質數，該正質數具有一範圍由大於 2 到小於 2^v 的值。

10.如申請專利範圍第 1 項所述之方法，其中該方法係被啟始於該第一電腦系統上載入一軟體產品之一步驟的期間。

11.一種用來決定是否一軟體產品能使用於具一第二個硬體組態的一第二電腦系統上之方法，其中該第二電腦系統是完全相同或不同於第一電腦系統，該方法至少包含下列步驟：

識別 n 個元件類別，該 n 個元件類別用在決定由如申請專利範圍第 1 項所產生之該堅定的硬體識別碼(SHWID)；

識別該第二硬體組態中的每一元件類別內之所有實體；

取回一識別字串，該識別字串表示每一各自的元件實體；

產生每一元件實體之實體質數 $i_{p,q}$，其中每一實體質數是一正整數，並且其中 p 表示一範圍由 1 到 n 之指定的元件類別數字，及 q 表示在第一硬體組態或第二硬體組態中，第 q 個元件形態；

取回可能類別之局部的機密 $P_{p,q}$，其中：

$$P_{p,q} = [C_p(\text{mod } i_{p,q})]；$$

由該可能類別之局部的機密 $P_{p,q}$，萃取可能的類別質數 $P_{p,q}$ 及可能的類別餘數 $d_{p,q}$；

解出由該可能的類別質數及該可能的類別餘數之排列所提供的一組同餘(congruence)，以產生一可能的機密；及

藉由解密一指定密文以測試該可能的機密，並且測試一對應之已知的純文字(plaintext)所得之測試結果；

其中；

若該結果的純文字與已知的純文字相符時，在第二電腦系統上載入該軟體產品；及

若該結果的純文字與已知的純文字不相符時，則防止在第二電腦系統上載入該軟體產品。

12.如申請專利範圍第 11 項所述之方法，其中產生實體質數之步驟，至少包含輸入表示每個單獨的元件實體之識別字串至一質數產生函式 $f(x)$，其中 x 是一最大長度達到約 65,000 字元之識別字串。

13.如申請專利範圍第 12 項所述之方法，其中 $f(x)$產生一大於 2t 之正質數，其中 t 是一整數，其範圍由大約 32 至大約 2,048。

14.一種包含可用於該電腦系統之至少一應用程式模組的電腦系統，其中該至少一應用程式模組至少包含如申請專利範圍第 1 項所述之方法的應用程式碼。

15.一電腦可讀取的媒體，在其上儲存電腦可執行指令以實行如申請專利範圍第 1 項所述之方法。

16.一種已儲存電腦可執行指令於其上用以對一具有第一硬體組態的第一電腦系統執行一種產生一堅定的硬體識別碼(SHWID)之方法的電腦可讀取媒體，該方法至少包含下列步驟：

識別在該第一硬體組態內的每一元件類別，其中元件類別的數量等於 n；

決定每一元件類別之一類別乘積 c_p；

決定每一元件類別之一局部的機密 P_p；及

對於每一元件類別，相加該類別乘積 c_p 與該局部的機密 P_p 以形成 n 個堅固類別識別，

其中該 n 個堅固類別識別碼以結合的方式形成該第一電腦系統之堅定的硬體識別碼(SHWID)。

17.如申請專利範圍第 16 項所述之電腦可讀取的媒體，其中上述 n 是一最大達到 16 的整數。

18.如申請專利範圍第 16 項所述之電腦可讀取的媒體，其中對每一元件類別之該類別乘積 c_p，由下列步驟所決定：

選擇該元件類別的數量 n；

識別該 n 個元件類別；

識別在每一元件類別之所有實體；

對每一元件實體指定一識別字串；

產生每一元件實體之實體質數 $P_{p,q}$，其中每一實體質數是一正質數，並且其中 p 表示一指定之元件類別數字，範圍由 1 到 n，並且其中 q 表示該第一硬體組態中第 q 個元件形態；及

相乘在每一元件類別內的實體質數以形成類別乘積 c_p。

19.如申請專利範圍第 18 項所述之電腦可讀取的媒體，其中產生實體質數之步驟，至少包含輸入每一元件實體之識別字串至一質數產生函式 *f(x)*，其中 x 是一最大長度達到約 65,000 字元之識別字串。

20.如申請專利範圍第 19 項所述之電腦可讀取的媒體，其中 *f(x)* 產生一大於 2t 之正質數，其中 t 是一整數，其範圍由大約 32 至大約 2,048。

21.如申請專利範圍第 16 項所述之電腦可讀取的媒體，其中對每一元件類別之該局部的機密 P_p，由下列步驟所決定：

產生每一元件類別之一隨機數字 r_p；

產生每一元件類別之一類別質數 p_p，其中每一類別質數是一正質數；

選擇一必要元件類別符合之數量 *m*，其中 *m* 是小於或等於 *n*；

決定 *N*，其中 *N* 等於 *m* 個最小類別質數 p_p 之乘積；

決定 M，其中 M 等於 $(m-1)$ 個最大類別質數 p_p 之乘積，並且 M 小於 N；

選擇一機密數字 S，其中 $M < S < N$；

決定每一元件類別之類別餘數 d_p，其中 d_p 等於 $[S \pmod{p_p}]$；

形成每一元件類別之一第一個二進制值，其中該第一個二進制值是類別質數 p_p 對每一類別編碼至 u 個位元的第一個二進制數，其中 u 小於 t，及 u 和 t 兩者均小於大約 2,048；

形成每一元件類別之一第二個二進制值，其中該第二個二進制值是類別餘數 d_p 對每一類別編碼至 v 個位元的第二個二進制數，其中 v 小於 t，及 (u + v = t)；及

連接第一個二進制值和第二個二進制值，以形成每一元件類別之局部的機密 P_p，該 P_p 的總位元數等於 t。

22.如申請專利範圍第 21 項所述之電腦可讀取的媒體，其中每個隨機數字 r_p 係由一隨機數字產生器所產生，其範圍由 0 到小於 2^u。

23.如申請專利範圍第 21 項所述之該電腦儲存媒體，其中產生每個元件類別之類別質數 p_p 的步驟，至少包含輸入每個元件類別之隨機數字至一質數產生函式 g(x)，其中 x 是一最大長度至約 65，000 字元之隨機數字。

24.如申請專利範圍第 23 項所述之電腦可讀取的媒體，其中

g(x)產生一個正質數，該正質數範圍由大於2到小於2^v。

25.如申請專利範圍第16項所述之電腦可讀取的媒體，其中該方法啟始於該第一電腦系統上載入一軟體產品之步驟的期間。

26.一種已儲存電腦可執行指令於其上用以執行決定一軟體產品是否能使用於具一第二硬體組態之一第二電腦系統的方法之電腦可讀取的媒體，其中該第二電腦系統是完全相同或不同於該第一電腦系統，該方法至少包含下列步驟：

識別n元件類別，該n元件類別用在決定如申請專利範圍第16項所產生之堅定的硬體識別碼(SHWID)；

識別該第二硬體組態的每一元件類別內之所有實體；

取回一識別字串，該識別字串表示每一單獨的元件實體；

產生每一元件實體之實體質數$i_{p,q}$，其中每一實體質數是一正整數，並且其中p表示一指定的元件類別數字，範圍由1到n，及q表示在第一硬體組態或第二硬體組態中，第q個元件形態；

取回可能之類別局部的機密 $P_{p,q}$，其中：

$P_{p,q} = [Cp \pmod{i_{p,q}}]$；

由該可能之類別局部的機密 $P_{p,q}$，萃取可能的類別質數 $P_{p,q}$ 及可能的類別餘數 $d_{p,q}$ ；

解出由該可能的類別質數及該可能的類別餘數之排列所提供的一組同餘，產生一可能的機密；及

藉由解密一指定密文，以測試該可能的機密，並且測試一對應之已知的純文字所得之測試結果；

其中；

若該結果的純文字與已知的純文字相符時，在第二電腦系統上載入該軟體產品；及

若該結果的純文字與已知的純文字不相符時，則防止在第二電腦系統上載入該軟體產品。

27.如申請專利範圍第26項所述之電腦可讀取的媒體，其中產生實體質數之步驟，至少包含輸入表示每一單獨的之元件實體之識別字串至一質數產生函式 $f(x)$，其中 x 是一最大長度達到約 65,000 字元之識別字串。

28.如申請專利範圍第27項所述之電腦可讀取的媒體，其中 $f(x)$ 產生一大於 2t 之正質數，其中 t 是一整數，其範圍由大約 32 至大約 2,048。

29.一種包含可用於該電腦系統之至少一應用程式模組之電腦系統，其中該至少一應用程式模組至少包含應用程式碼用以對一具第一種硬體組態之第一種電腦系統執行一種產生一堅定的硬體識別碼(SHWID)之方法，其中該方法至少包含

步驟：

識別在第一硬體組態中每一元件類別，其中元件類別的數量等於 n；

決定每一元件類別之一類別乘積 c_p；

決定每一元件類別之一局部的機密 P_p；及

對於每一元件類別，相加該類別乘積 c_p 與該局部的機密 P_p，以形成 n 堅固類別識別，其中該 n 堅固類別識別組合地形成該第一電腦系統之堅定的硬體識別碼(SHWID)。

30.如申請專利範圍第 29 項所述之電腦系統，其中上述 n 是一最大達到大約 16 之整數。

31.如申請專利範圍第 29 項所述之電腦系統，其中每一元件類別之該類別乘積 c_p，如下列步驟所決定：

選擇該元件類別的數量 n；

識別該 n 元件類別；

識別在每一元件類別之所有實體；

對每一元件實體指定一識別字串；

產生每一元件實體之實體質數 $P_{p,q}$，其中每一實體質數是一正質數，並且其中 p 表示一指定之元件類別數字，範圍由 1 到 n，並且其中 q 表示該第一硬體組態中第 q 個元件形態；及

相乘在每一元件類別內的實體質數以形成類別乘積 c_p。

32.如申請專利範圍第31項之電腦系統，其中產生實體質數之步驟，至少包含輸入表示每一元件實體之識別字串至一質數產生函式 $f(x)$，其中 x 是一最大長度達到約 65,000 字元之識別字串。

33.如申請專利範圍第32項之電腦系統，其中 $f(x)$ 產生一大於 2t 之正質數，其中 t 是一整數，其範圍由大約 32 至大約 2,048。

34.如申請專利範圍第29項之電腦系統，其中每個元件類別之該局部的機密 P_p，由下列步驟所決定：

產生每一元件類別之一隨機數字 r_p；

產生每一元件類別之一類別質數 p_p，其中每一類別質數是一正質數；

選擇一必要元件類別符合之數量 m，其中 m 是小於或等於 n；

決定 N，其中 N 等於 m 個最小類別質數 p_p 之乘積；

決定 M，其中 M 等於(m-1)個最大類別質數 p_p 之乘積，並且 M 小於 N；

選擇一機密數字 S，其中 $M < S < N$；

決定每個元件類別之類別餘數 d_p，其中 d_p 等於 $[S \pmod{p_p}]$；

形成每一元件類別之一第一個二進制值，其中該第一個二進制值是類別質數 p_p 對每個類別編碼至 u 個位元的第一個二進制數，其中 u 小於 t，及 u 和 t 兩者均小於大約 2,048；

形成每一元件類別之一第二個二進制值，其中該第二個二進制值是類別餘數 d_p 對每一類別編碼至 v 個位元的第二個二進制數，其中 v 小於 t，及 $(u + v = t)$；及

連接第一個二進制值和第二個二進制值，以形成每一元件類別之一局部的機密 P_p，該 P_p 的總位元數等於 t。

35.如申請專利範圍第 34 項之電腦系統，其中每一隨機數字 r_p 係由一隨機數字產生器所產生，其範圍由 0 到小於 2^u。

36.如申請專利範圍第 34 項之電腦系統，其中產生每一元件類別之類別質數 p_p 的步驟，至少包含輸入每一元件類別之隨機數字至一質數產生函式 g(x)，其中 x 是一最大長度達到約 65,000 字元之隨機數字。

37.如申請專利範圍第 36 項之電腦系統，其中 g(x)產生一個正質數，該正質數範圍由大於 2 到小於 2^v。

38.如申請專利範圍第 29 項之電腦系統，其中該方法啟始於該第一電腦系統上載入一軟體產品之一步驟的期間。

39.一種包含可用於該電腦系統之至少一應用程式模組之電腦系統，其中該至少一應用程式模組，至少包含應用程式碼，該應用程式碼執行一種方法，該方法決定是否一軟體產品可使用於具第2個硬體組態的第2個電腦系統上，其中該第2個電腦系統，相同或不同於該第一電腦系統，其中的該方法至少包含步驟：

識別n個元件類別，該n個元件類別用在決定由如申請專利範圍第29項所產生之堅定的硬體識別碼(SHWID)；

識別該第2個硬體組態中的每個元件類別間之所有實體；

取回一識別字串，該識別字串表示每個單獨的元件實體；

產生每個元件實體之實體質數 $i_{p,q}$，其中每個實體質數是一正整數，並且其中p表示一指定的元件類別數字，範圍由1到n，及q表示在第一硬體組態或第2個硬體組態中，第q個元件形態；

取回可能之類別局部的機密 $P_{p,q}$，其中：

$P_{p,q} = [Cp \pmod{i_{p,q}}]$；

由該可能之類別局部的機密 $P_{p,q}$，萃取可能的類別質數 $P_{p,q}$ 及可能的類別餘數 $d_{p,q}$；

解出由該可能的類別質數及該可能的類別餘數之排列所提供的一組同餘，產生一可能的機密；及

藉由解密一指定密文，測試該可能的機密，並並且測試一對應之已知的純文字所得之測試結果；

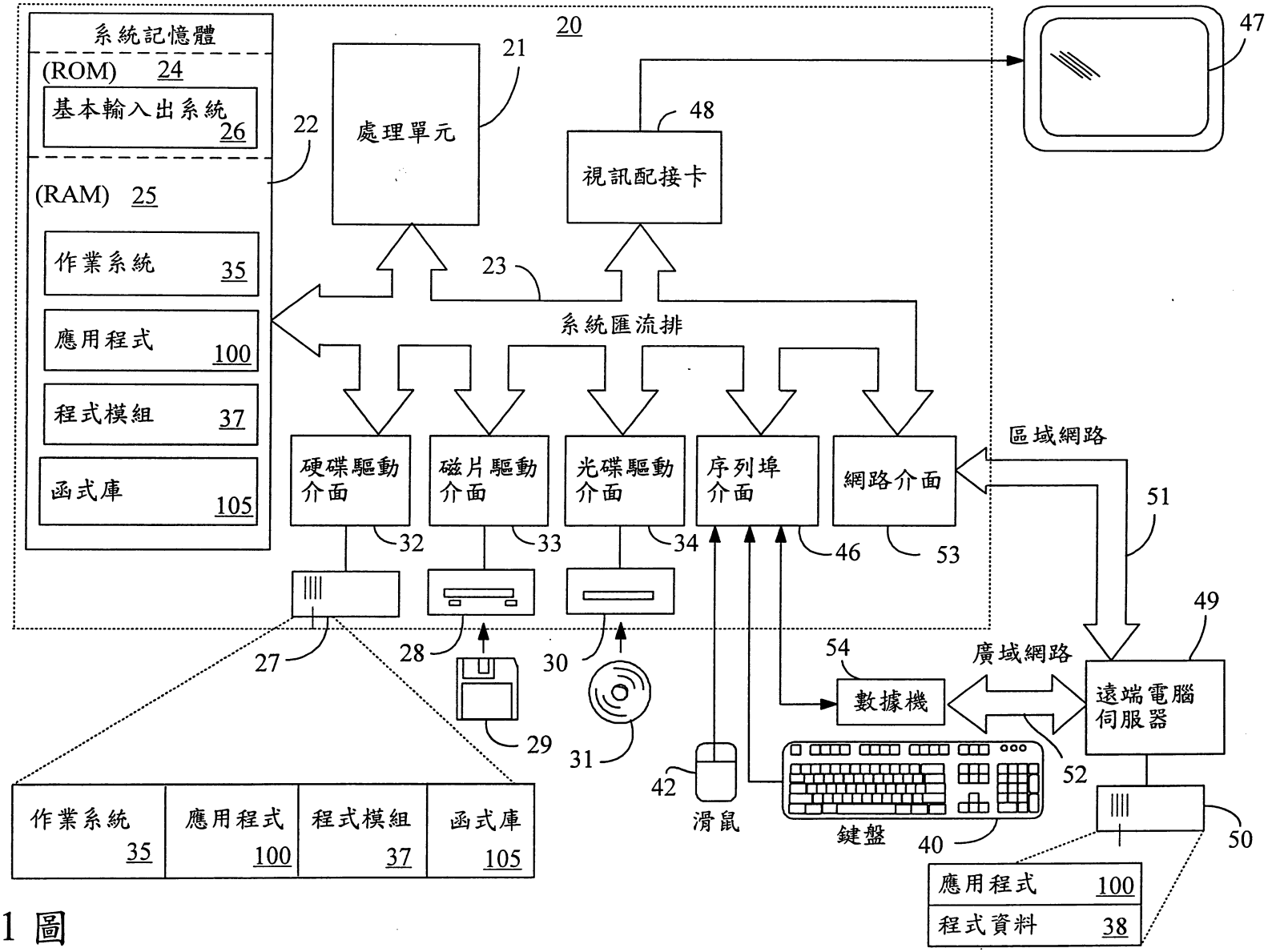
其中；

若作為結果的純文字與已知的純文字相符時，在第 2 個電腦系統載入該軟體產品；及

若作為結果的純文字與已知的純文字不相符時，則在第 2 個電腦系統，防止載入該軟體產品。

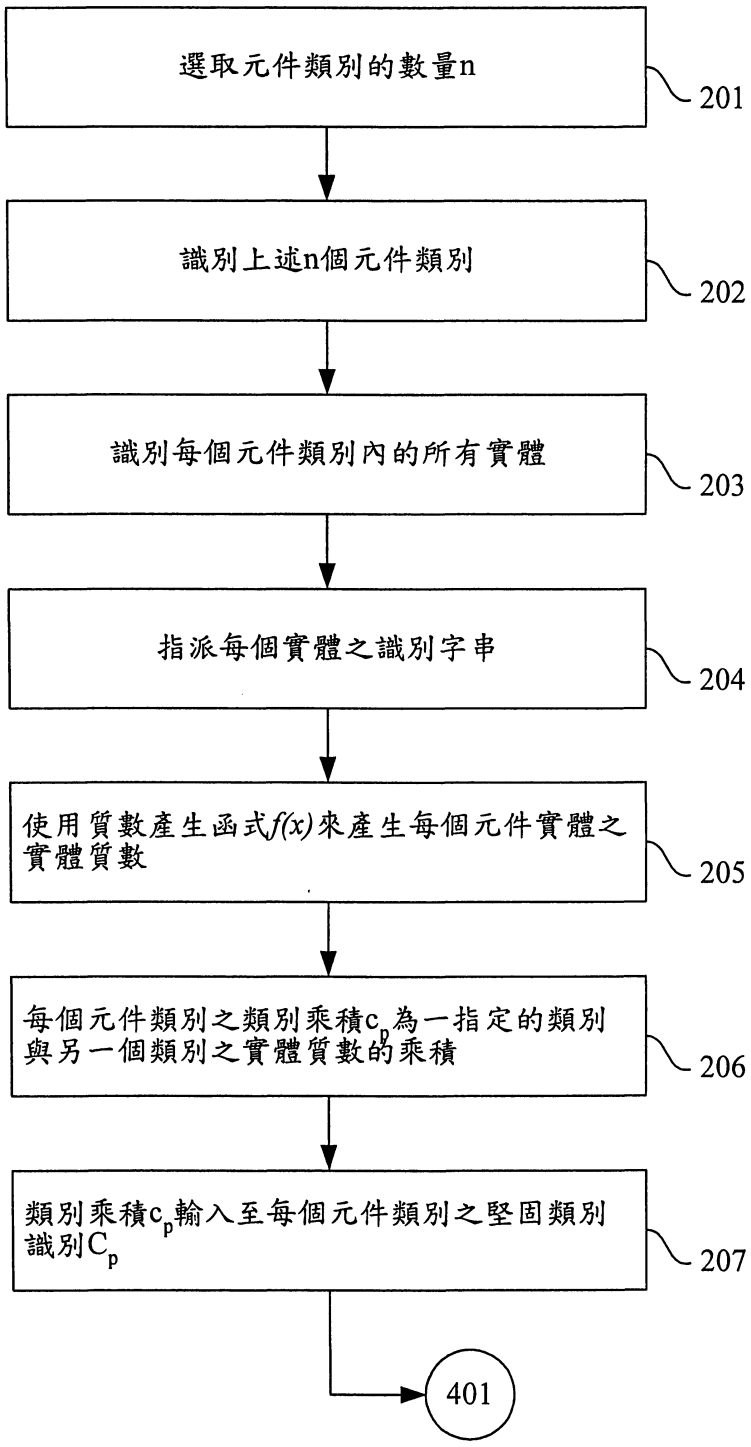
40.如申請專利範圍第 39 項之電腦系統，其中產生實體質數之步驟，至少包含輸入表示每一單獨的元件實體之識別字串至一質數產生函式 $f(x)$，其中 x 是一最大長度達至約 65,000 字元之識別字串。

41.如申請專利範圍第 40 項之電腦系統，其中 $f(x)$ 產生一大於 2t 之正質數，其中 t 是一整數，其範圍由大約 32 至大約 2,048。

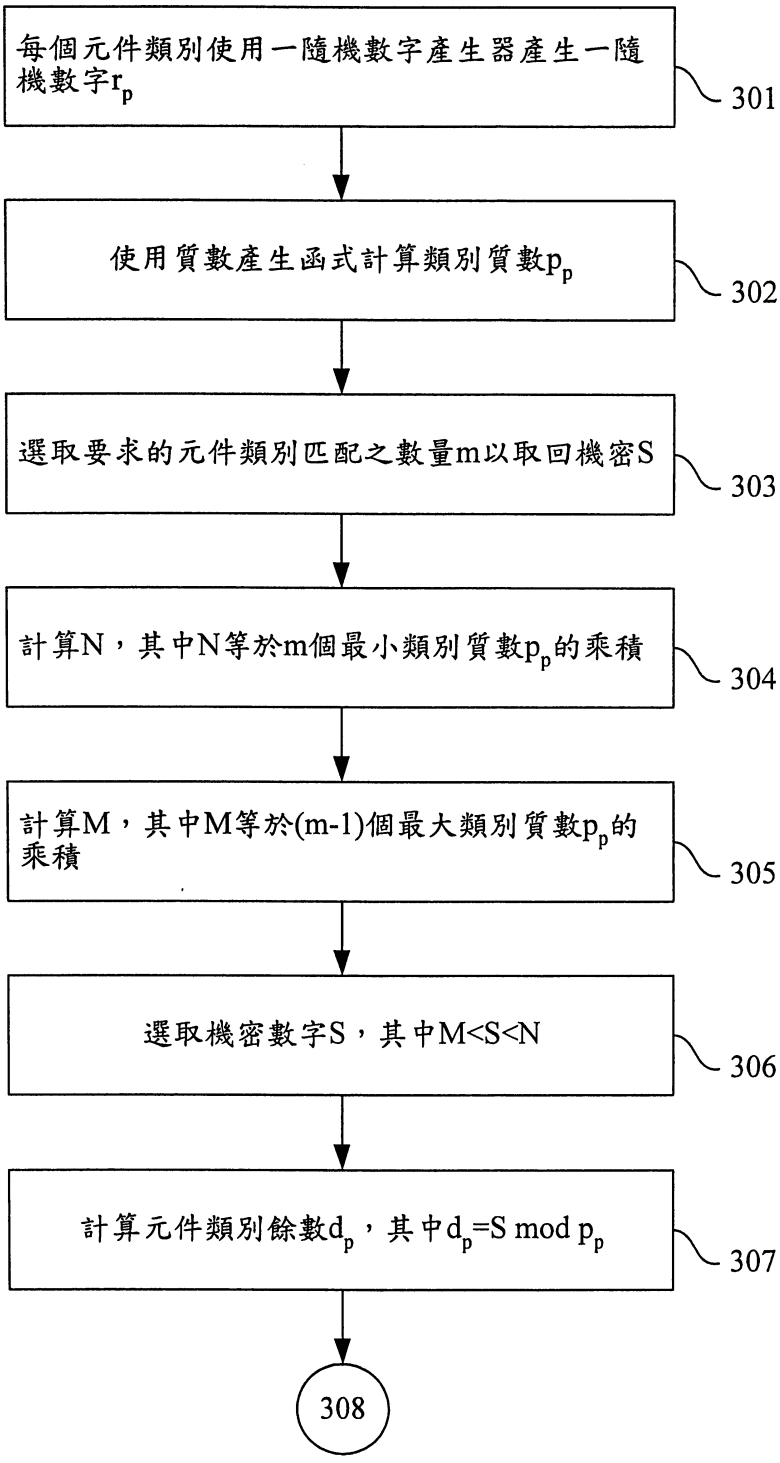


第 1 圖

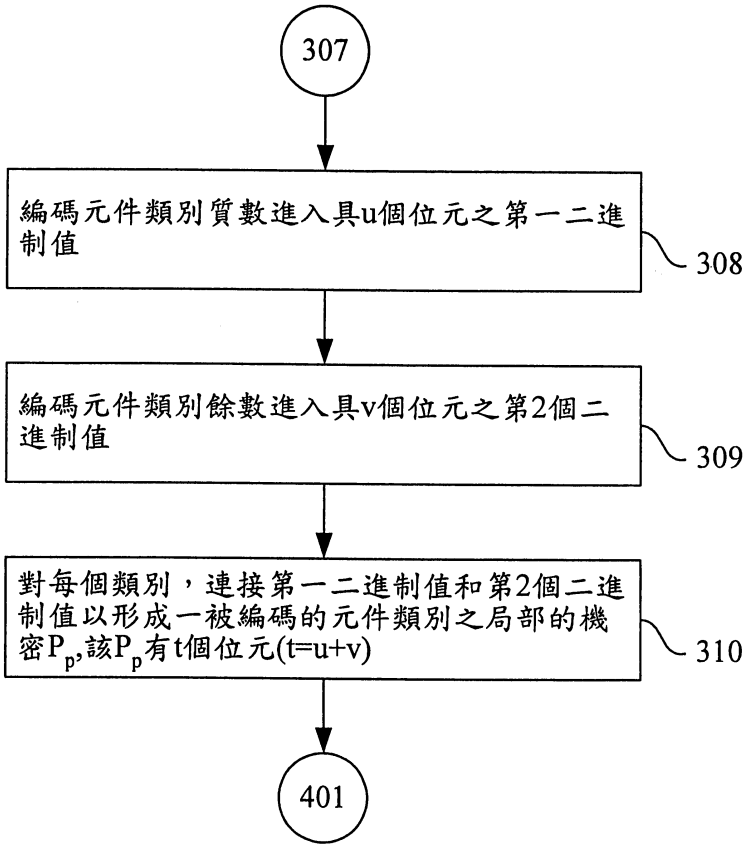
200422945


選取元件類別的數量n
201
識別上述n個元件類別
202
識別每個元件類別內的所有實體
203
指派每個實體之識別字串
204
使用質數產生函式f(x)來產生每個元件實體之實體質數
205
每個元件類別之類別乘積c_p為一指定的類別與另一個類別之實體質數的乘積
206
類別乘積c_p輸入至每個元件類別之堅固類別識別C_p
207
401

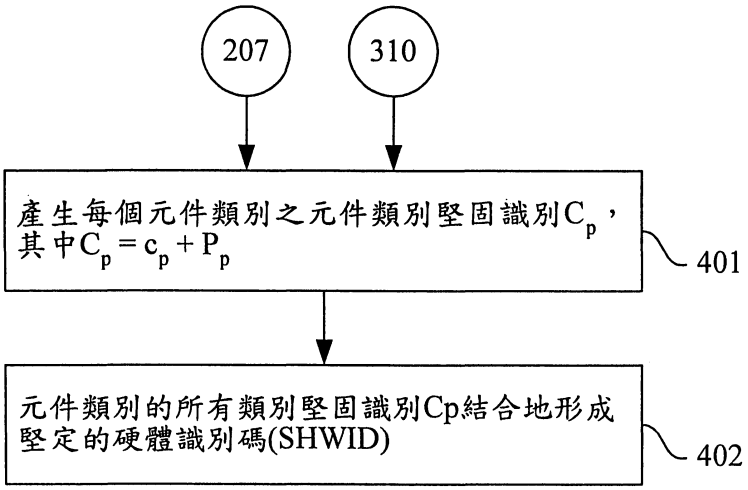
第 2 圖


每個元件類別使用一隨機數字產生器產生一隨機數字r_p
301
使用質數產生函式計算類別質數p_p
302
選取要求的元件類別匹配之數量m以取回機密S
303
計算N，其中N等於m個最小類別質數p_p的乘積
304
計算M，其中M等於(m-1)個最大類別質數p_p的乘積
305
選取機密數字S，其中M<S<N
306
計算元件類別餘數d_p，其中d_p=S mod p_p
307
308

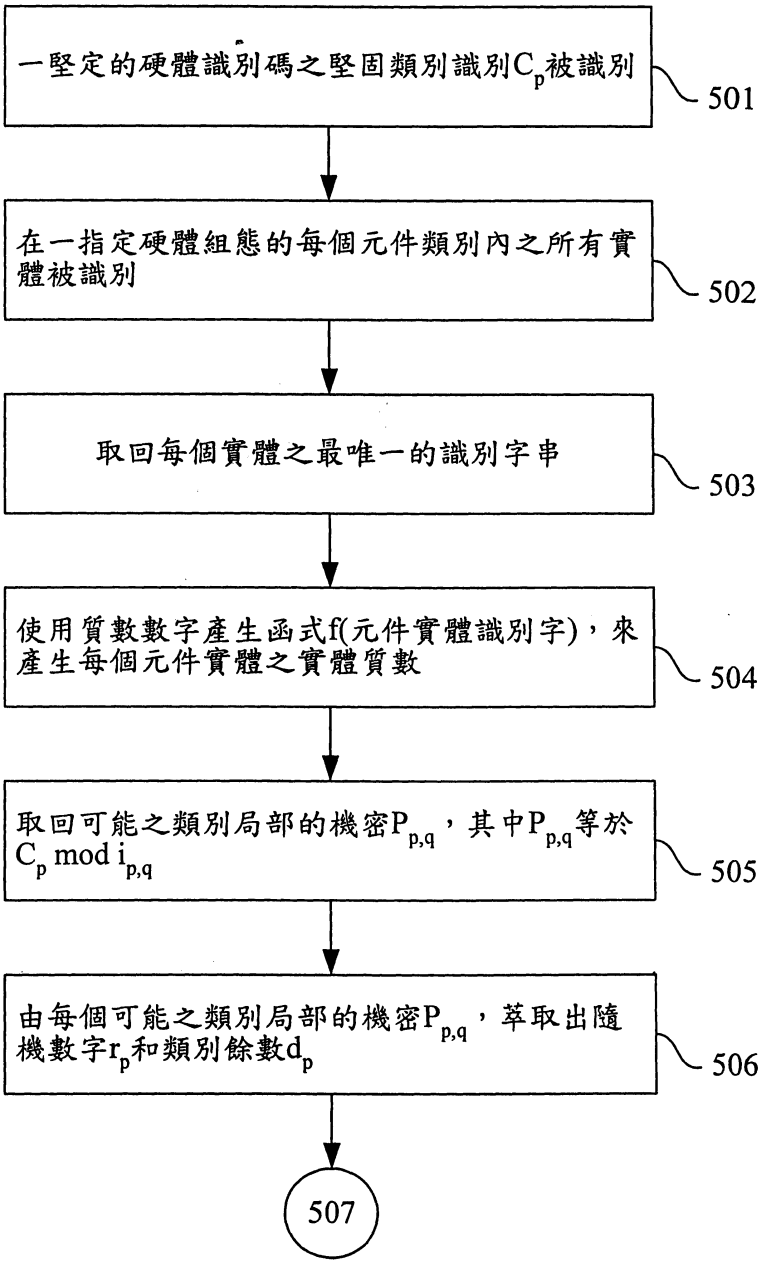
第 3 圖


307
編碼元件類別質數進入具u個位元之第一二進制值
308
編碼元件類別餘數進入具v個位元之第2個二進制值
309
對每個類別，連接第一二進制值和第2個二進制值以形成一被編碼的元件類別之局部的機密P_p,該P_p有t個位元(t=u+v)
310
401

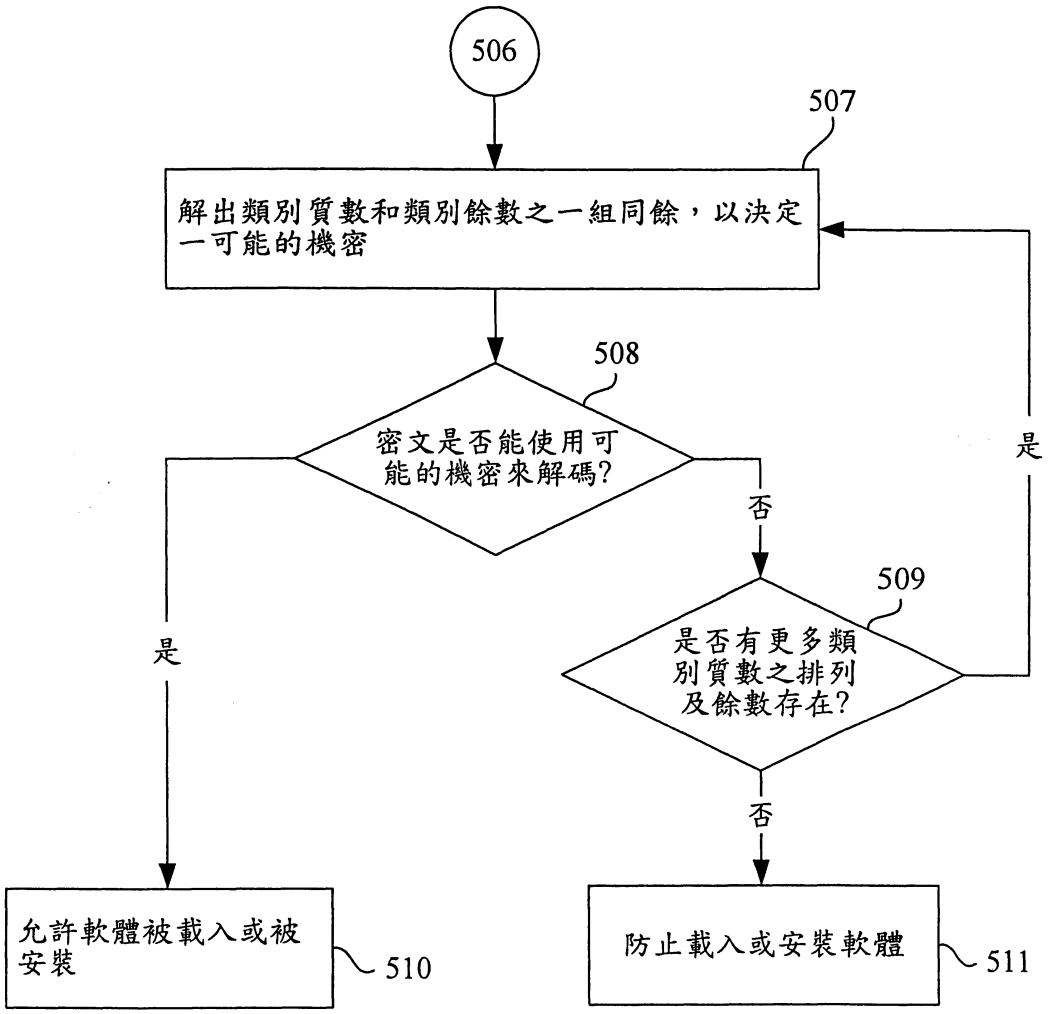
第 4 圖


207
310
產生每個元件類別之元件類別堅固識別C_p，其中$C_p = c_p + P_p$
401
元件類別的所有類別堅固識別Cp結合地形成堅定的硬體識別碼(SHWID)
402

第 5 圖


一堅定的硬體識別碼之堅固類別識別C_p被識別
501
在一指定硬體組態的每個元件類別內之所有實體被識別
502
取回每個實體之最唯一的識別字串
503
使用質數數字產生函式f(元件實體識別字)，來產生每個元件實體之實體質數
504
取回可能之類別局部的機密$P_{p,q}$，其中$P_{p,q}$等於$C_p \bmod i_{p,q}$
505
由每個可能之類別局部的機密$P_{p,q}$，萃取出隨機數字r_p和類別餘數d_p
506
507

第 6 圖


506
507
解出類別質數和類別餘數之一組同餘，以決定一可能的機密
508
密文是否能使用可能的機密來解碼?
是
否
509
是否有更多類別質數之排列及餘數存在?
是
否
允許軟體被載入或被安裝
510
防止載入或安裝軟體
511

第 7 圖

柒、指定代表圖：

(一)、本案指定代表圖為：第 1 圖。

(二)、本代表圖之元件代表符號簡單說明：

20 個人電腦
21 處理單元
22 系統記憶體
23 系統匯排流
24 唯讀記憶體
25 隨機存取記憶體
26 基本輸入出系統
27 硬碟驅動裝置
28 磁片驅動裝置
29 磁片
30 光碟驅動裝置
31 光碟
32 硬碟驅動介面
33 磁片驅動介面
34 光碟驅動介面
35 作業系統
36 應用程式模組
37 程式模組
38 程式資料
40 鍵盤
42 滑鼠
46 序列埠介面
48 視訊配接卡
49 遠端電腦伺服器
50 記憶儲存裝置
51 區域網路
52 廣域網路
53 網路介面
54 數據機
100 應用程式
105 函式庫

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無