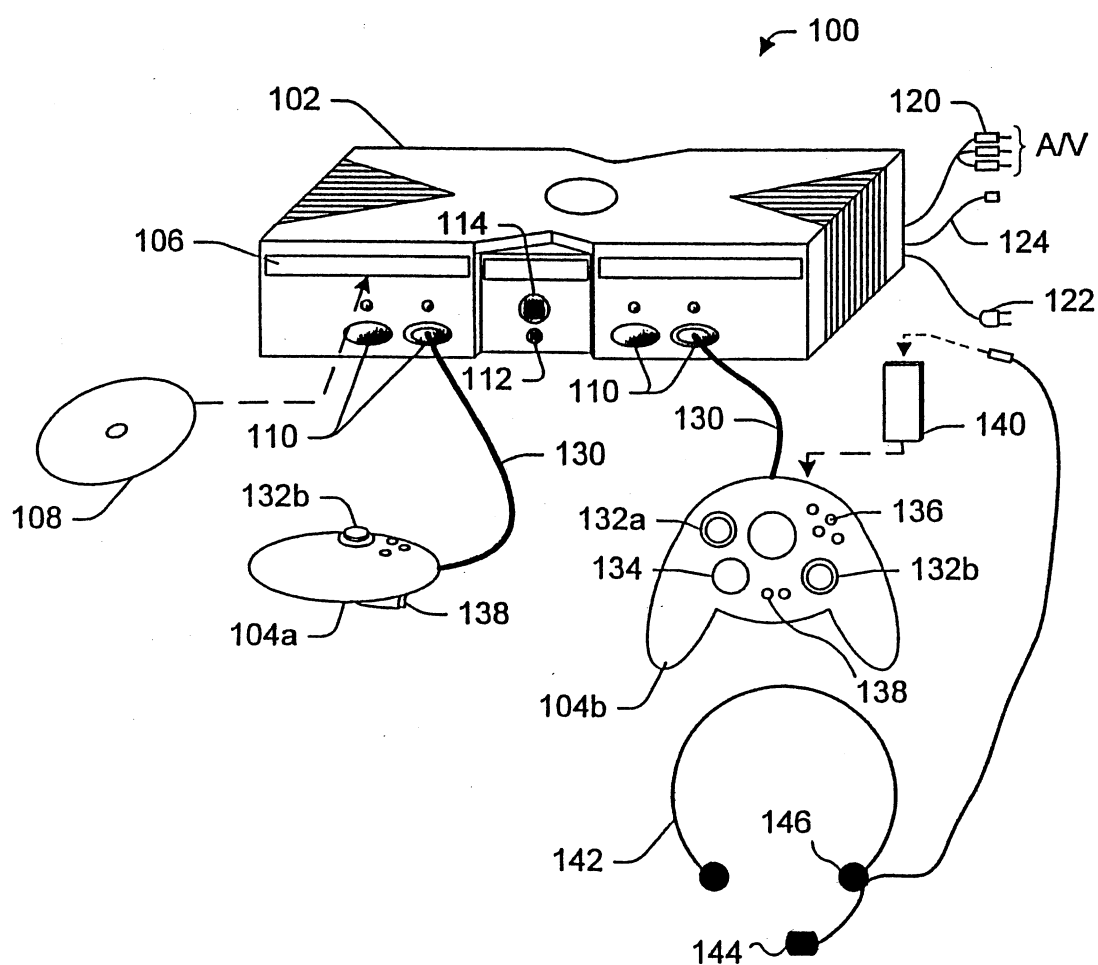
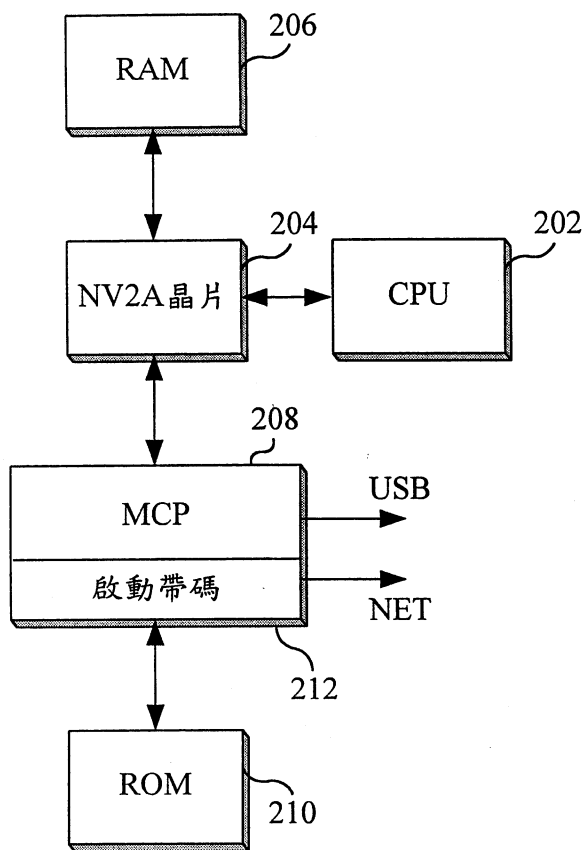


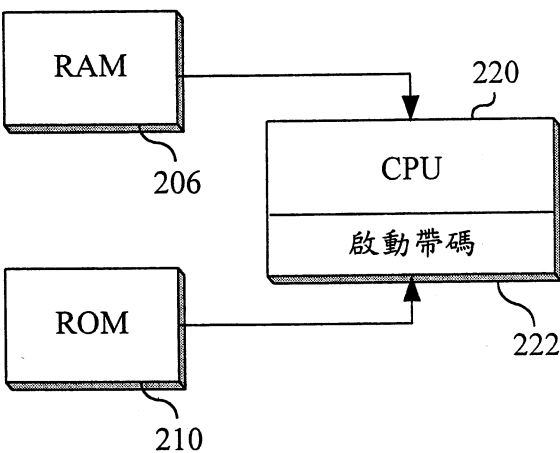
92114953



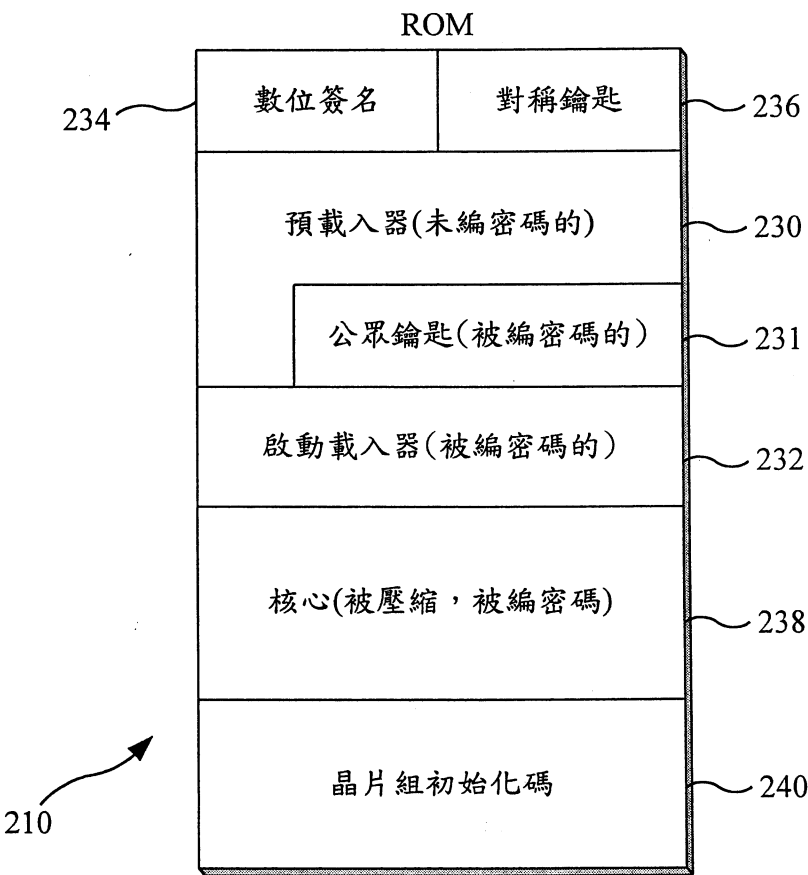
第 1 圖



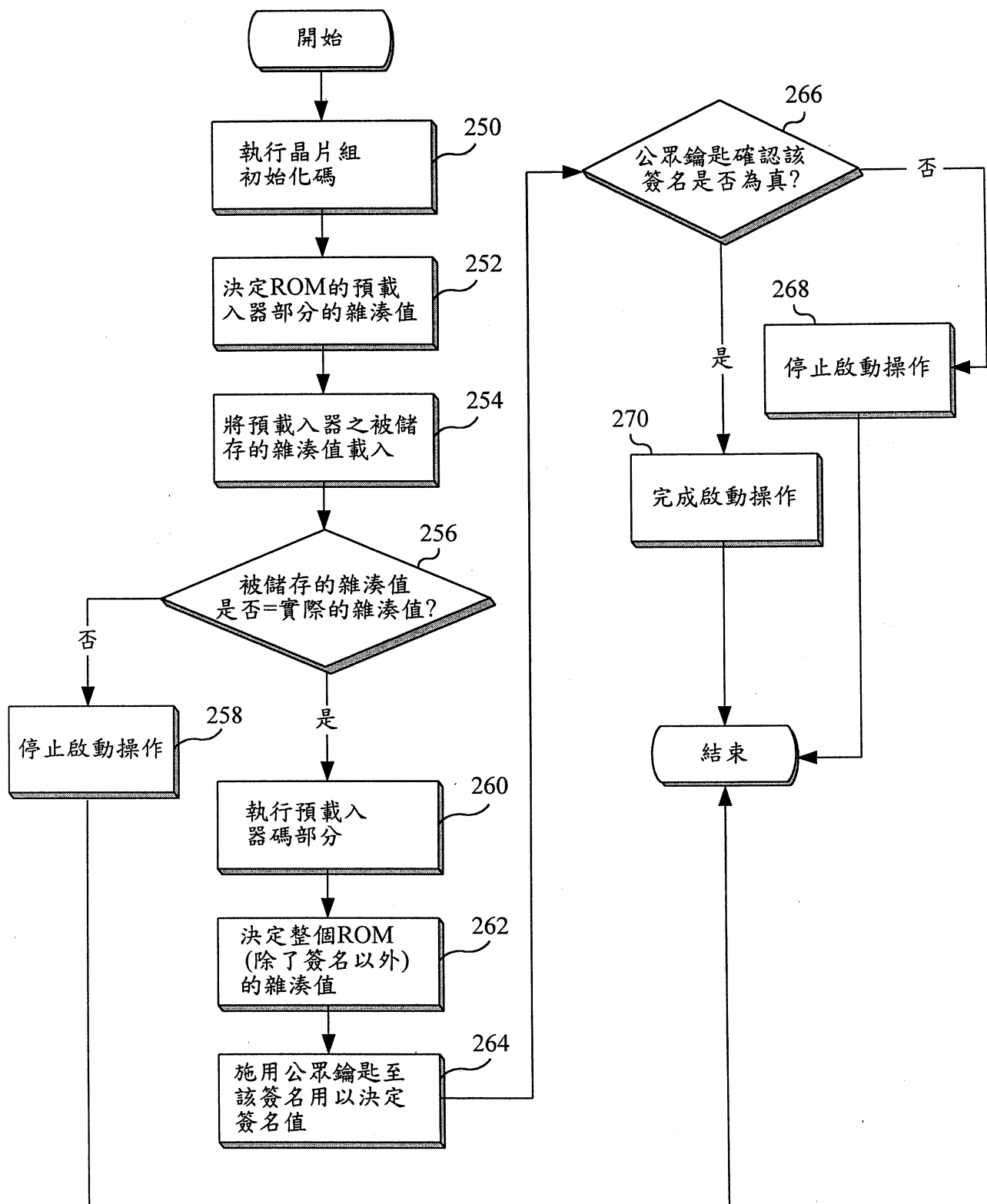
第 2A 圖



第 2B 圖



第 3 圖



第 4 圖

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：92114953

※申請日期：2003 年 6 月 2 日

※IPC 分類：G06F9/44 (2006.01)

一、發明名稱：(中文/英文)

經由雜湊在電子裝置啟動期間執行所提供的碼來安全地啟動電子裝置
的方法及具有相關機器指令之記憶媒體以及與其相關之電子裝置
METHOD AND MEMORY MEDIUM HAVING MACHINE
INSTRUCTIONS FOR SECURELY BOOTING UP ELECTRONIC
DEVICE BY HASHING CODE PROVIDED FOR EXECUTION DURING
BOOT-UP OF ELECTRONIC DEVICE AND ELECTRONIC DEVICE
RELATED THEREWITH

二、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)

丹可萊斯

Dan Crouse

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, U.S.A.

國籍：(中文/英文)

美國/USA

三、發明人：(共 5 人)

姓名：(中文/英文)

1. 帝那特莫瑞斯/Dinarte Morais

2. 強藍格/Jon Lange

3. 丹尼爾 R. 塞門/Daniel R. Simon
4. 陳霖(東尼)/Ling Tony Chen
5. 喬許 D. 貝那隆/Josh D. Benaloh

國 籍：(中文/英文)

1. 美國/USA
2. 美國/USA
3. 加拿大/Canada
4. 美國/USA
5. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家(地區)申請專利：

【格式請依：受理國家(地區)、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

美國；2002年6月7日；10/165,519

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

3. 丹尼爾 R. 塞門/Daniel R. Simon

4. 陳霖(東尼)/Ling Tony Chen

5. 喬許 D. 貝那隆/Josh D. Benaloh

國 籍：(中文/英文)

1. 美國/USA

2. 美國/USA

3. 加拿大/Canada

4. 美國/USA

5. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家(地區)申請專利：

【格式請依：受理國家(地區)、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

美國；2002年6月7日；10/165,519

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明

【發明所屬之技術領域】

本發明大體上係關於安全地啟動一包括有處理器之電子裝置，及更特定地係關於確保在啟動此一電子裝置時只有所想要的機器指令被該處理器所執行，用以防止替代的或其它的機器指令在啟動程序期間被執行。

【先前技術】

有許多的電子裝置在其最初的充電或重設時期必需要經過一啟動(boot-up)程序。在該啟動程序期間，控制著這些電子裝置的基本操作特性的機器指令典型地從唯讀記憶體(ROM)處被存取並被執行用以將該裝置初始化且讓其它的機器指令能夠被載入到隨機存取記憶體(RAM)中，這些指令將會必執行用以讓該電子裝置能夠實施其它的功能。例如，當一個人電腦被啟動時，包含基本輸入-輸出系統(BIOS)的指令會被執行用以讓一作業系統能夠從硬碟機被載入到RAM中且被該電腦的中央處理器(CPU)執行。”啟動(boot-up)”一詞為一較早的且更有說明性之”啟動(bootstrap)”一詞的簡短形式。

其它必需被啟動的電子裝置包括遊戲主機，數位記錄裝置，個人資料系統，及包含有某種形式的處理器之其它電子產品，其必需要執行一組最初的機器指令來在額外的機器指令被載入到記憶體中且被執行時可有具有其它的功能。因為啟動程序決定一電子裝置的最初狀態，其影響到

該裝置的重要操作參數且對於該裝置在啟動程序完成之後是如何被使用具有一實質的影響。防止啟動程序被變更對一家販售該電子裝置的公司而言是很重要的，這可避免導因於該裝置的使用所造成的收入損失。

例如，在電子遊戲產業中，被販賣之可玩電子遊戲的遊戲主機的商業價值是源自於在該遊戲主機上執行之遊戲軟體所產生的授權收入。因此，在啟動程序期間被載入的機器指令可實施防止未經授權的遊戲軟體在該遊戲主機上執行的功能並落實製造商之與遊戲主機用來玩電子遊戲相關的政策。有些使用者會將執行未經授權的軟體的限制及將這些政策落實在遊戲主機上視為一種挑戰以及對於遊戲主機的使用的一種不受歡迎的限制。這些使用者藉由將遊戲主機電路及軟體加以“駭客(hacking)”來突破這些限制。例如，避開這些限制的一個方法為造成在一遊戲主機上執行之啟動程序載入一被修改過的軟體核心，在該軟體核心有某些東西被改變。這些改變將遊戲主機製造商所強加限制移除掉，而這會讓製造商對於該遊戲主機是如何被使用失去控制，且會造成收入損失，如果未經授權的遊戲軟體可在遊戲主機上執行的話。因此，遊戲主機製造商通常都會採取一些作法來防止駭客們在開起程序期間執行一經過改變的軟體核心。

一類似的問題存在於電子裝置必需被啟動的其它科技領域中。例如，衛星電視接收器的製造商根據使用者所付的月費來限制使用者可接收到的頻道，其被需要能夠確保

其安全政策及其產品的使用政策會被遵循，使得消費者只能依據授權的條款來使用該電子裝置。一駭客可能能夠修改軟體碼來造成衛星接收器內的處理器認定該使用者已付費來觀看電視頻道，藉此讓該使用者在沒有付適當的費用下能夠接收到且觀看所有的電視頻道。

因此，確保只有經過授權的軟體碼才可在一電子裝置的啟動期間被執行是所需要的。任何被使用的技術應能夠防止一被修改過的機器指令組取代應在該裝置的啟動期間被執行之經過授權的軟體，並藉此確保該電子裝置實施製造商及/或銷售商所欲實施的功能及政策。被用來防止駭客擊潰一電子裝置的使用限制及政策(它們都被包括在電子裝置的啟動期間載入的軟體碼裝)之已知的方法很明顯地並非完全的成功。藉由使用一包括了替代軟體碼之外加(add-in)電路卡，該已知的安全政策會至少部分地被駭客所破解，其將該電路卡耦合至該電子裝置的電路中。很明顯地，需要一種更安全且更嚴謹的方法來防止一替碼在一電子裝置的啟動程序期間被插入或被執行。

【發明內容】

本發明可一般性地被應用在所有包括一處理器且在最初充電或重設時必需被啟動的電子裝置中，用來確保該電子裝置的其它功能能夠被實施。在此一裝置中，保護在該裝置的操作期間會使用到之所有權資訊及防止未經授權的軟體碼在啟動程序期間被執行是很重要的。

最有可能被取代來顛覆一電子裝置之防竄改政策及功能的構件為儲存有機器指令之非揮發性記憶體，該等機器指令定義該電子裝置是如何被使用。因此，本發明可確保在此記憶體中之包含該等機器指令的程式碼都是經過授權的(即，沒有被可改變該電子裝置的功能及政策之機器碼所修改過或更換過的碼)。在本發明中，經過授權的碼包括一預先定義的部分(亦被稱為預載入器碼)。此預先定義的部分必需保持相同，即使是在對該經過授權的碼的其它部分作出改變，或是該電子裝置將不會被啟動亦然。

一程序被一開始實施用以確保該碼之預先定義的部分是經過授權的。在此程序中，該預先定義的部分被雜湊(hashed)，產生一第一雜湊值。該第一雜湊值然後被拿來與一儲存的雜湊值相比對，該被儲存的雜湊值被保存在該電子裝置的一電路構件中，其與存放該碼之記憶體是分開來的，用以確認該碼之預先定義的部分是經過授權的。如果該第一雜湊值等於被儲存的雜湊值的話，則執行該碼之預先定義的部分，如果不同的話，則該電子裝置的啟動會被終止。如果該碼的預先定義部分被致能(enable)(即，幾乎所有的碼都被雜湊)的話，其可決定一第二雜湊值。一數位簽名被包括在該碼的一部分中，該部分不同於該碼的預先定義部分。該第二雜湊值然後被拿來對該數位簽名作確認，用以確保該簽名的真實性。如果該數位簽名被證實是真的，則該碼即可被執行，而如果不是真的話，則該電子裝置的啟動即被終止。

為了要比對該第一數值與儲存的雜湊值，一被保持在該電路構件上的一非揮發性儲存部分中的初始碼被執行。該初始碼包括該被儲存的雜湊值且被保持在一圖形處理器中，雖然該被儲存的雜湊值亦可被保存在其它種類的輔助處理器中，像是一聲訊處理器，一輸入處理器，一輸出處理器，一通訊處理器，或一數位訊號處理器。更佳的是，將該初始碼及預期的雜湊值存放在一可執行該初始碼的處理器中。此初始碼被執行用以雜湊該預先定義的部分，並實施該第一雜湊值與該被儲存的雜湊值的比對的工作。在本發明的一較佳的形式中，該初始碼被永久地定義在一韌體(firmware)中成為一預設的位元數。此外，該碼的預先定義部分最好是包含一預設的位元碼數，其被設置在該碼的一預設的位置處。很明顯地，除非該被儲存的雜湊值被相對應地改變，否則該碼的預先定義部分的大小及內容即無法被修改，因為該被儲存的雜湊值會不等於該第一雜湊值。

該預先定義的碼亦包括一公眾金鑰其被用來確認該數位簽名且具有可讓該碼的一被編密碼(encrypted)的核心部分被解密碼的機器指令。該被解密碼的核心然後被執行用以完成該電子裝置啟動。該預設的碼使用一串流密碼(stream cipher)來實施該碼的核心部分的解密碼(decryption)。

本發明的另一態樣係關於一記憶媒體其上儲存有碼，該碼包含機器指令，該等機器指令在該電子裝置的啟動期

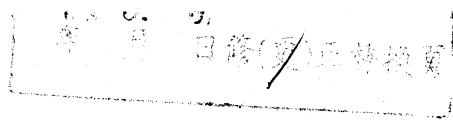
間被取得用以決定該碼是否是經過授權的。該記憶媒體包括該核心部分，該啟動載入器部分，該預載入部分，及數位簽名。

本發明的另一態樣係關於一種電子裝置其必需被啟動才能操作。該電子裝置包括一非揮發性記憶體，其上儲存有多個機器指令。該非揮發性記憶體包括一主要部分及一預載入器部分其具有一預先定義的內容，大小及位置。一處理器被耦合至該非揮發性記憶體用以在啟動期間執行機器指令。一啟動碼韌體元件載明機器指令，該等指令定義一雜湊演算法及一預期的雜湊值。該啟動碼韌體的機器指令在該電子裝置的啟動期間一開始是由該處理器來執行的，造成該處理器實施該預載入部分的的雜湊並將結果與該預期的雜湊值比對。該電子裝置的其它細節及其功能大體上與上文提及的方法步驟相同。

藉由使用本發明於一電子裝置中，如一遊戲主機中，想要改變在啟動程序期間執行的機器指令或用不同的機器指令來取代另一記憶體的嘗試會讓該裝置無法成功地啟動。因此，本發明可藉由確保只有經過授權的碼才可在該電子裝置的啟動期間被執行來防止有人修改基本功能或規避應由該電子裝置實施的政策。

【實施方式】

應被強調的是，本發明並不侷限在使用於遊戲主機上，雖然本案的說明書中之較佳實施例是使用在遊戲機



上。本發明被發展來確保所有權資訊被會被揭示給想要還原工程碼的使用者，並防止使用者規避授權限制及與該遊戲機玩電子遊戲相關的政策。

如第 1 圖所示，一舉例性的電子遊戲系統 100 包括一遊戲主機 102 且支援多達四個使用者裝置，如控制器 104a 及 104b。遊戲主機 102 配備有一內部的硬碟機(未在此圖中示出)及一可攜式媒體機 106 其可支援不同形式的可攜式光學儲存媒體，其以光學儲存碟片 108 來代表。適當的可攜式儲存媒體的例子包括了 DVD 碟片及 CD-ROM 碟片。在此遊戲系統中，遊戲程式最好是以燒在 DVD 碟片上的方式被分銷以使用在該遊戲主機上，惟其它的儲存媒體亦可被使用，用以在使用本發明的系統上實施資料安全政策及確保輸入到該系統中的數位資料的真實性。

在該遊戲機 102 的正面上有四個插槽 110，以供四個控制器連接用，惟插槽數目及安排可以不同。一電源鈕 112 及一退出鈕 114 亦位在該遊戲主機 102 的正面。電源鈕 112 控制著電力供應至該遊戲主機，該退出鈕 114 交替地開啟及關閉可攜式媒體機 106 的托盤(未示出)，讓該儲存光碟 108 能夠放入及取出，使得在碟片上的數位資料可被該遊戲主機讀取及使用。遊戲主機 102 經由影/音(A/V)介面電線 120 而連接至一電視或其它顯示監視器或螢幕。一電源線插頭 122 當其連接至一傳統的交流電源(未示出)時，可將電力輸送至該遊戲主機。遊戲主機 102 可被進一步提供一資料連接器 124 用來經由傳統的電話線數據機，或經由

一寬頻連線來將資料傳送於一網路上，如網際網路。

每一控制器 104a，104b 都經由一導線(或經由一無線介面)耦合至該遊戲主機 102。在被舉出的實施例中，該等控制器為萬用串接匯流排(USB)相容的且經由 USB 線 130 連接至該遊戲主機 102。遊戲主機 102 可配備許多種使用者裝置中的任何一種來與遊戲軟體互動及控制遊戲軟體。雖然控制器 104a 的所有細節並沒有被示於第 1 圖中，但每一控制器 104a，104b 都配備有兩個拇指桿 132a 及 132b，一 D 板 134，按鈕 136，及兩個扳機 138。這些控制器只是代表性的，且其它已知的遊戲輸入與控制機構都可被用來取代或添加至第 1 圖所示的遊戲機上。

一可取下的或可攜式的記憶單元(MU)140 可非必要地被插入到該控制器 104 中用以提供額外的可移除式儲存。可攜式的 MU 可讓使用者儲存遊戲參數及藉由將可攜式 MU 插入到其它的控制器上來讓這些參數能夠在其它的主機上玩。在所示的實施例中，每一控制器都被建構成可容納兩個 MU，但比兩個 MU 多或少的數目亦可被使用。

遊戲系統 100 能夠玩遊戲，放音樂，及播放視訊。其它的功能可使用儲存在硬碟機上的數位資料或從裝置 106 中的光學儲存碟片 108 上讀取的數位資料，來自於線上的資源，或來自於 MU140 的數位資料來實施。遊戲主機被設計成可防止未經授權的電子遊戲碟片在該遊戲主機上遊玩。而且，某些政策是經由該遊戲主機來實施。例如，在一地理區中所販售的軟體是不能在一不同的地理區中所販

售的遊戲主機上玩。而且，一防止影像 DVD 拷備的工業標準 (MACROVISION™) 被該遊戲主機軟體所實施。

某些使用者想要打敗由遊戲主機所實施的功能性限制及政策。規避這些限制及政策的一個方式為安裝一積體電路 (IC) 或模組至該遊戲主機中，用經過修改的版本來取代原來的 ROM 及儲存在 ROM 內用來在該遊戲主機啟動時使用到的碼。在這些取代模組中之對機器指令的修改是要在啟動程序期間操作且消除或改變由該遊戲主機的製造商或設計者所強加，用來防止未經授權的軟體的使用，視訊 DVD 的拷備，及該遊戲主機的其它功能及/或政策等之限制。然而，本發明讓插入一未經授權的取代 ROM 模組來改變啟動程序變得極為困難，並可在該遊戲主機的啟動期間偵測到有人嘗試要使用替代的及未經授權的碼時即可終止啟動程序。

為了要防止與啟動程序有關的所有權資訊被發現及為了要防止經過修改或變造的碼於啟動程序期間被使用，在啟動期間被執行的機器指令的至少一部分必需被保持與包括在該遊戲主機或其它電子裝置中的 ROM 內的絕大部分的機器指令分開。大體上，在一電子裝置的印刷電路板上的 IC，接線，接點，及介層孔是很容易接近的，只要該電子裝置的外殼被打開。雖然很難防止有人接近印刷電路板，但本發明讓接近機器指令變得很困難，這些機器指令被埋設在安裝於該印刷電路板的一 IC 內成為韌體。最好是，一 IC 應被用作此目的且是市面上買不到的，因為其為

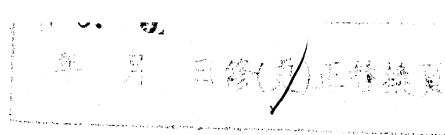
該電子裝置的製造商所定製的。而且，用作此目的的 IC 對於該電子裝置的操作是很關鍵的，使得如果有人嘗試要取得埋設在該 IC 中的韌體的話，則該 IC 的操作及該電子裝置的操作都將會受到不利的影響。

第 2A 圖顯示數種包括在遊戲主機 100 內的 IC 元件。一 CPU202 是主要的處理器且被用來執行該遊戲核心的大部分處理功能。CPU202 必需與大多數一般的處理器一樣在一開始即被啟動，用以讓它能夠執行該遊戲核心被設計來實施之不同的功能。CPU202 被雙向連接至一定製的圖形處理器其亦為由 NVIDIA 公司所製造的匯流排及記憶體控制晶片 204 且被設計為 NV2A 晶片。該 NV2A 晶片被連接至 RAM206 及連接至另一 NVIDIA 定製的晶片其為一媒體通訊處理器 (MCP)208 (該晶片提供聲訊訊號處理器的能力) 且連接至系統記憶體，亦耦合至 USB 埠與乙太網路埠以進行資料通訊。包括在該 MCP208 內的為 512 位元的韌體，其包含一啟動碼 212。啟動碼 212 大體上被埋設在該 MCP208 的其它層底下且無法藉由將此模組掀開來取得。為了要實體上取得啟動碼 212，就必需覆蓋在上面的幾層去除掉，而這會毀壞掉該 MCP 模組，造成該模組及遊戲主機無法使用。又，因為 MCP208 是遊戲主機製造商定製的，所以其它人是無法由公開的市場上取得的。即使是該啟動碼用某種方式而被取得，讓包含此韌體的機器指令被“看到”，本發明亦會讓啟動程序無法被改變。MCP208 耦合至一 ROM210，其包括該遊戲主機 100 在啟動時必需用到的大部分機器指

令。

本發明之一更為一般性的應用被示於第 2B 圖的元件結構中。一定製的 CPU220 可包含”埋設”於其內且在其它 CPU 層底下之韌體啟動碼 222。如第 2B 圖所示的，CPU220 耦合至 RAM206 及 ROM210。因為啟動碼 222 包含韌體於 CPU222 內，所以在 CPU 處理部分與啟動碼 222 之間的訊號是無法取得的。因此，對於第 2B 圖所示的實施例而言，取得啟動碼 222 並決定其內容是更加困難，因此第 2B 圖的實施例可提供比第 2A 圖的實施例更高的安全性。

第 3 圖顯示 ROM210 在本發明中用到的不同的部分。在較佳的實施例中，遊戲主機 100 使用到的 ROM210 包含一 256K 位元組的記憶體模組被包括在 ROM210 中的是一預載入器 230，其未被編密碼(encrypted)。預載入器 230 在較佳的實施例中具有約 11K 位元組的固定大小，且其內容，大小，及在 ROM210 中的位置都是預先定義的。很重要的是，預載入器 230 包括一被編密碼的公眾金鑰 231。同樣很重要的是，必需維持該預載入器 230 的內容不被改變，除非該韌體啟動碼 212 有相對應的改變，這在以下的說明中會清楚地交代。ROM210 亦包括一啟動載入器 232 其是經過編密碼的。此外，ROM210 包括一數位簽名 234 及一對稱金鑰 236。顯然地，大部分的 ROM210 是用來儲存包含一核心(kernel)238 的機器指令。核心 238 是同時被壓縮及編密碼的。包括在該核心 238 內的機器指令定義大部分的功能及建立與該遊戲主機 100 相關的政策。最後，一晶片組



初始化碼 240 在該遊戲主機開始被充電時會被包括及被執行。

第 4 圖顯示該遊戲主機 102 在被開始充電或被重設時會被實施的邏輯步驟。步驟 250 是讓晶片組初始化碼 240 在 ROM210 中執行。包括在晶片組初始化碼 240 中的機器指令是未被編密碼的；它們定義適合使用在該完整的遊戲主機架構中之特定組態的資訊及特定組態的程序。該機器碼必需實施的晶片組組態被包括在啟動碼中；該特定的值及程序係晶片組初始化碼的一部分。而且，該 CPU 的初始化程序被包含在該啟動碼內並在晶片組初始化碼的其餘部分之前被執行。接下來，在方塊 252，包括在埋設於該 MCP208 中之該韌體啟動碼 212 內的機器指令跑一單向雜湊演算法用以決定在該 ROM210 內之預載入器 230 的一雜湊值。如上文提及的，在遊戲主機 100 被製造的當時即被安裝在其內的原始 ROM210 中，該預載入器 230 即具有一特定的內容，大小，及在 ROM210 內的位置。因此，藉由將包括在預載入器 230 內的該等機器指令加以雜湊所得到的雜湊值應永遠保持相同，只要該預載入器 230 沒有被未經授權的碼所改變或替代。在較佳的實施例中，一 SHA-1 單向雜湊演算法被施用，用以將該預載入器雜湊。或者，可使用一 MD5 雜湊演算法，熟悉此技藝者可瞭解到其它的雜湊演算法亦可被使用。被使用的雜湊演算法係包括在啟動碼 212 的機器指令中。

同樣包括在啟動碼 212 中的是一被儲存的雜湊值其為

該預載入器 230 的預期雜湊值，及一對稱金鑰。步驟 254 從該啟動碼載入該儲存的雜湊值。在該啟動碼 212 中的機器指令將來自於啟動碼的被儲存雜湊值與在步驟 252 中由預載入器 230 所決定的雜湊值相比較。該比較是在一決定步驟 256 中實施用以決定該被儲存的雜湊值是否等於被決定的實際雜湊值。如果不相等的話，則在該啟動碼 212 中的機器指令會執行步驟 258，其會將該遊戲主機 102 的啟動程序終止。因此，如果有一不同的 ROM 被拿來取代原始的 ROM 的話，該新的或未經授權的 ROM 並不會包括一相同的預載入器部分，即會在用該單向雜湊演算法處理時可產生該預期的雜湊值的預載入器部分，決定步驟 256 將會偵測對於預載入器 230 的變更並終止該啟動程序。

假設該被儲存的雜湊值等於該被實際決定的雜湊值的話，則步驟 260 將會執行包含 ROM210 的預載入器碼部分的機器指令。此步驟可被實施因為該等預載入器機器指令很清楚地與最初包括在由遊戲主機製造商安裝在該遊戲主機中的 ROM 內的機器指令相同。

接下來，步驟 262 決定整個 ROM210 除了電子簽名 234 之外的一雜湊值。該預載入器亦包括用來決定一單向雜湊值的機器指令且最好是使用 SHA-1 或 MD5 雜湊演算法（或熟悉此技藝者所習知的任何單向雜湊演算法）來決定 ROM210 的大部分內容的雜湊值（數位簽名並不包括在 ROM 被雜湊的內容之內）。只要使用相同的雜湊法則，結果永遠都是相同的，除非機器指令已被改變，或被未經授權的機器指令

所更換。即使是只變更 ROM210 被雜湊的機器指令的一個單一位元，這都將會改變雜湊所得的數值。

在 ROM210 中的公眾金鑰 231 在步驟 264 被用到數位簽名 234 上用以產生一該數位簽名的一對應值。(在該公眾金鑰可被施用之前，其被儲存在該 MCP 的啟動碼內的對稱金鑰所解密碼(decrypted)，但如果該公眾金鑰沒有被此對稱金鑰所編密碼的話則此步驟就不需要。)接下來，在第 4 圖的決定步驟 266 中，在預載入器 230 內的機器指令決定該公眾金鑰是否能夠確認該簽名；此步驟決定來自於步驟 264 的值是否等於在步驟 262 所決定之該 ROM 的雜湊值。如果不等於的話，則步驟 268 會停止啟動操作因為在 ROM 中的簽名已經被改過。如所習知的，如果該簽名值係使用只有該遊戲主機的製造商知道的一私有金鑰所簽名的話，則該簽名的辨視可使用一公眾金鑰來確認。如果某些人攻擊該遊戲主機 100 並嘗試要來變更 ROM210 的任何部分的話，在雜湊值上的改變將會在步驟 266 被偵測到，而造成啟動程序在步驟 268 被終止。相反地，如果該數位簽名與 ROM 的雜湊值相符的話，則 ROM 的內容會與被授權的原始內容相同。

假設在步驟 264 所決定的數位簽名的值確任在決定步驟 266 中的 ROM 的雜湊值的話，則步驟 270 可讓啟動進行到完成為止，讓核心 238 被複製到 RAM206 中，然後被解壓縮及解密碼至 RAM 中。預載入器 230 包括將啟動載入器解密碼的機器指令。被保持在該 MCP 中之在韌體啟動

碼內的對稱金鑰與在 ROM210 內的對稱金鑰 236 相結合用以產生一新的對稱碼，其被用來依據在該預載入器內的機器指令將啟動載入器解密碼。

該啟動載入器包括用來依據熟悉此技藝者所習知的 RC4 串流密碼演算法來實施一被壓縮及被編密碼的核心的串流密碼(stream cipher)解密碼的機器指令。包含已被解壓縮及解密碼至 RAM206 中的核心的機器指令然後可被 CPU202 執行，用以實施該遊戲機之完整的功能，可確保其只載入被授權的遊戲軟體，執行可阻止影像 DVD 的拷貝的演算法，及確保其實施該遊戲主機製造商所想要的且被定義在經過授權的啟動碼中之所有其它的政策及功能。

雖然本發明已依據較佳實施例的形式加以說明，但熟悉此技藝者將可瞭解到在不偏離由以下的申請專利範圍所定義之本發明的範圍下，可以有許多的變化可被達成。因此，本發明的範圍並不侷限於以上的說明內容，而是完全由下面的申請專利範圍來定義。

【圖式簡單說明】

本發明的上述態樣及許多其它的優點在閱讀以下參照了附圖之詳細說明之後將會變得很容易瞭解，其中：

第 1 圖為使用本發明的一遊戲主機的立體圖；

第 2A 圖為包括在第 1 圖的遊戲主機中的數個功能性構件的方塊圖；

第 2B 圖為一需要啟動且包括一處理器與記憶體之一

般電子裝置的功能性方塊圖；

第 3 圖為一示意圖其顯示被建構在本發明中之一記憶體的部分；及

第 4 圖為一流程圖，其顯示在本發明中的邏輯操作。

【元件代表符號簡單說明】

100 電子遊戲系統	102 遊戲主機
104a, 104b 控制器	106 可攜式媒體機
108 光學儲存碟片	110 插槽
112 電源鈕	114 退出鈕
120 影/音(A/V)介面電線	122 電源線插頭
124 資料連接器	130 USB 線
132a, 132b 拇指桿	134 D-板
136 按鈕	138 扳機
140 記憶體單元	202 中央處理器(CPU)
204 匯流排及記譯體控制晶片	
206 RAM	208 媒體通訊處理器(MCP)
210 ROM	212 啟動碼
220 CPU	222 韌體啟動碼
230 預載入器	231 公眾金鑰
232 啟動載入器	234 數位簽名
236 對稱金鑰	238 核心
240 晶片組初始化碼	

五、中文發明摘要

一種包含一啟動碼(bootstrap code)的機器指令係被埋在一電子遊戲主機的一關鍵構件中，該等機器指令在該處不能被輕易地存取或更改。一在唯讀記憶體(ROM)內的預載入器部分被該啟動碼所雜湊且其結果被拿來與一保持在該啟動碼內的預期雜湊值相比對。該啟動程序的進一步確認是由預載入器來實施，其將ROM中的碼加以雜湊用以獲得該碼的一雜湊值。該結果用以數位簽名值來加以確認，該數位簽名值定義此雜湊的一預期值。若無法獲得任何預期的結果，則該啟動程序將會被終止。因為該啟動碼確認該預載入器，及該預載入器確認在ROM中之其餘的碼，所以此技術對於確保用來將該裝置啟動的碼不被更改或更換是很有用的。

六、英文發明摘要

Machine instructions comprising a bootstrap code are buried within a critical component of an electronic game console where they cannot readily be accessed or modified. A preloader portion in a read only memory (ROM) is hashed by the bootstrap code and the result is compared to an expected hash values maintained in the bootstrap code. Further verification of the boot-up process is carried out by the preloader, which hashes the code in ROM to obtain a hash value for the code. The result is verified against a digital signature value that defines an expected value for this hash. Failure to obtain any expected result terminates the boot-up process. Since the bootstrap code confirms the preloader, and the preloader confirms the the remainder of the code in ROM, this technique is useful for ensuring that the code used for booting up the device has not been modified or replaced.

十、申請專利範圍

1. 一種經由雜湊在一電子裝置啟動期間執行所提供的碼來安全地啟動該電子裝置的方法，該方法至少包含以下的步驟：

(a)將該碼的一預定義部分雜湊(hashing)用以產生一第一雜湊值；

(b)將該第一雜湊值與一被保持在該電子裝置的一電路元件中的經儲存雜湊值相比對用以確認該碼之該預定義的部分是被授權的，其中該電路元件與存放該碼的記憶體是分離的；

(c)如果該第一雜湊值等於該經儲存的雜湊值，則允許執行該碼的該預定義部分，而如果是不相等的話，則終止該電子裝置的啟動；

(d)其中執行該碼之經授權的該預定義部分會實施以下的步驟：

(i)實質上將該碼之所有者雜湊用以決定一第二雜湊值；及

(ii)確認包括在該碼中的一數位簽名是否與該第二雜湊值相符，如果是的話，則允許該碼被執行，而如果不是的話，則終止該電子裝置的啟動。

2. 如申請專利範圍第1項所述之方法，其中比對該第一雜湊值與該經儲存的雜湊值的步驟包含執行一被保持在

該電路元件的一非揮發性儲存部分中的初始碼的步驟，該初始碼包括該經儲存的雜湊值。

3. 如申請專利範圍第 2 項所述之方法，其中該初始碼被保持在一輔助處理器中。

4. 如申請專利範圍第 2 項所述之方法，其中該初始碼被保持在以下其中一者：

- (a) 一圖形處理器；
- (b) 一聲訊處理器；
- (c) 一輸入處理器；
- (d) 一輸出處理器；
- (e) 一通訊處理器；及
- (f) 一數位訊號處理器。

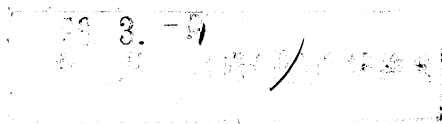
5. 如申請專利範圍第 2 項所述之方法，其中該初始碼被保持在一處理器中，該處理器可執行該初始碼。

6. 如申請專利範圍第 2 項所述之方法，其中該初始碼被執行用以實施申請專利範圍第 1 項中的步驟(a)至(c)。

7. 如申請專利範圍第 2 項所述之方法，其中該初始碼係被永久地定義於韌體中成為一預設的位元組數目。

8. 如申請專利範圍第 1 項所述之方法，其中該碼的預定義部分包含一預載入器碼，其具有設置在該碼的一預設位置處之一預設的位元組數目。
9. 如申請專利範圍第 8 項所述之方法，其中確認該數位簽名的步驟是用一公眾金鑰來實施，該公眾金鑰係包括在該預載入器碼中。
10. 一種其上記錄了包含可經由雜湊在一電子裝置啟動期間執行所提供的碼來安全地啟動該電子裝置之機器指令的記憶媒體，該記憶媒體至少包括：
 - (a)一核心部分，其中包含該碼的機器指令的一主要部分係儲存在該核心部分；
 - (b)一開機載入器部分，其被設計成可載入包括在該核心部分中的機器指令，供該電子裝置執行；
 - (c)一預載入器部分，其具有一預定義的位元組數目及一預定義的內容，該預載入器部分被設置在該記憶媒體上的一預定的位置處；及
 - (d)一數位簽名部分，該數位簽名部分提供一確認雜湊值用來與藉由將該碼雜湊所得到的雜湊值相比對，及使用在判斷該碼是否經授權。

11. 如申請專利範圍第 10 項所述之記憶媒體，其中該預載入器部分包括一公眾金鑰，其可用來將該簽名部分解密碼(decrypting)。
12. 如申請專利範圍第 10 項所述之記憶媒體，其中該記憶媒體包含一唯讀記憶體。
13. 如申請專利範圍第 10 項所述之記憶媒體，其中該預載入器部分包括定義一單向雜湊演算法的機器指令。
14. 如申請專利範圍第 10 項所述之記憶媒體，其中該預載入器部分包括可使用一儲存在該預載入器部分中的公眾金鑰來辨識該數位簽名的機器指令。
15. 如申請專利範圍第 10 項所述之記憶媒體，其中該核心部分係被編碼(encoded)。
16. 如申請專利範圍第 10 項所述之記憶媒體，其中該預載入器部分包括用於實施該核心部分的一串流密碼(stream cipher)解密碼的機器指令。
17. 如申請專利範圍第 10 項所述之記憶媒體，其中該預載入器部分包括至少一公眾金鑰，其用於辨識一用相應的



私有金鑰所簽署的簽名。

18. 一種電子裝置，其經由雜湊在該電子裝置啟動期間執行所提供的碼來安全地啟動，該電子裝置至少包含：

(a) 一非揮發性記憶體，其上儲存有許多機器碼，該非揮發性記憶體包括一主要部分，及一預載入器部分，其內容，大小及位置是預先定義的；

(b) 一處理器，其耦合至該非揮發性記憶體用以執行該等機器指令；

(c) 一啟動碼韌體(bootstrap code firmware)元件，其載明可定義一雜湊演算法的機器指令及一預期的雜湊值，該啟動碼韌體的機器指令在該電子裝置的啟動期間被該處理器所執行，促成該處理器執行以下的動作：

(i) 將該非揮發性記憶體的預載入器部分雜湊用以決定一預載入器雜湊值；

(ii) 比較該預期的雜湊值與該預載入器雜湊值；
及

(iii) 如果該預載入器雜湊值不等於該預期的雜湊值，即終止該電子裝置的啟動。

19. 如申請專利範圍第 18 項所述的電子裝置，其中該非揮發性記憶體的預載入器部分包括機器指令，其可促成該處理器執行以下的動作：



(a)將該非揮發性記憶體雜湊，用以產生一記憶體雜湊值；

(b)將該記憶體雜湊值與一包括在該預載入器部分中的預期記憶體雜湊值相比較；及

(c)如果該記憶體雜湊值不等於該預期的記憶體雜湊值，即終止該電子裝置的啟動。

20. 如申請專利範圍第 19 項所述的電子裝置，其中該預期的記憶體雜湊值如一數位簽名般地被包括在該非揮發性的記憶體中，但當雜湊該發揮發性記憶體時被排除在外。

21. 如申請專利範圍第 20 項所述的電子裝置，其中在該非揮發性記憶體的預載入器部分中的機器指令可進一步促成該處理器辨識該數位簽名，用以決定該預期的記憶體雜湊值。

22. 如申請專利範圍第 20 項所述的電子裝置，其中在該非揮發性記憶體的預載入器部分中的機器指令進一步促成該處理器施用一包括在該預載入器部分中的公眾金鑰來辨識該數位簽名。

23. 如申請專利範圍第 18 項所述的電子裝置，其中該非揮

發性記憶體的主要部分的至少一部分被編密碼(encrypted)，及其中該非揮發性記憶體的預載入器部分包括可促成該處理器將被編密碼的該非揮發性記憶體的主要部分之該至少一部分解密碼的機器指令，讓該電子裝置的啟動能夠以繼續執行包括在該非揮發性記憶體的主要部分中的機器指令。

24. 如申請專利範圍第 18 項所述的電子裝置，其中該啟動碼韌體元件係設置在該電子裝置的另一元件中且在不將其它元件破壞到讓該電子裝置變成不能操作的前題下是實質上無法存取該啟動碼韌體元件。

25. 如申請專利範圍第 24 項所述的電子裝置，其中該其它的元件包含一輔助處理器。

26. 如申請專利範圍第 24 項所述的電子裝置，其中該其它的元件包含以下所列的其中一者：

- (a) 一圖形處理器；
- (b) 一聲訊處理器；
- (c) 一輸入處理器；
- (d) 一輸出處理器；
- (e) 一通訊處理器；及
- (f) 一數位訊號處理器。

27. 如申請專利範圍第 18 項所述的電子裝置，其中該啟動碼韌體元件係設置在該處理器內。

28. 如申請專利範圍第 18 項所述的電子裝置，其中該非揮發性記憶體主要部分的至少一部分係被編密碼(encrypted)，且其中該非揮發性記憶體的預載入器部分包括：

(a) 定義一單向雜湊演算法的機器指令；

(b) 用來將該非揮發性記憶體的主要部分的至少一部分解碼的機器指令；

(c) 包含一啟動載入器的機器指令；及

(d) 至少一公眾金鑰。

29. 如申請專利範圍第 18 項所述的電子裝置，其中該電子裝置包含一遊戲主機。

七、指定代表圖

(一)、本案指定代表圖為：第 4 圖

(二)、本代表圖之元件代表符號簡單說明：

- | | |
|--------------------------|------------|
| 250 執行晶片組初始化碼 | 268 停止啟動操作 |
| 252 決定 ROM 的預載入器部分的雜湊值 | 270 完成啟動操作 |
| 254 將預載入器之被儲存的雜湊值載入 | |
| 256 被儲存的雜湊值是否=實際的雜湊值? | |
| 258 停止啟動操作 | |
| 260 執行預載入器碼部分 | |
| 262 決定整個 ROM(除了簽名以外)的雜湊值 | |
| 264 施用公眾金鑰至該簽名用以決定簽名值 | |
| 266 公眾金鑰確認該簽名是否為真? | |

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無