I436280

(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 I436280 B**

(45)公告日： 中華民國 103 (2014) 年 05 月 01 日

(21)申請案號：100129977 (22)申請日： 中華民國 100 (2011) 年 08 月 22 日

(51)Int. Cl.： *G06F9/445 (2006.01)* *G06F21/00 (2013.01)*

(71)申請人：宏碁股份有限公司 (中華民國) ACER INCORPORATED (TW)
新北市汐止區新台五路 1 段 88 號 8 樓

(72)發明人：鄭博仁 CHENG, PO JEN (TW)；邱屹 CHIOU, YIH (TW)；林榮隆 LIN, RUNG LUNG (TW)

(74)代理人：詹銘文；葉璟宗

(56)參考文獻：

TW	I315849	TW	I317094
TW	201005648A	US	2005/0065890A1
US	2008/0148375A1		

審查人員：郭彥鋒

申請專利範圍項數：10 項 圖式數：6 共 0 頁

(54)名稱

存取基本輸入輸出系統設定的認證方法

AUTHENTICATION METHOD FOR ACCESSING PROFILE OF BASIC INPUT/OUTPUT SYSTEM

(57)摘要

一種存取基本輸入輸出系統設定的認證方法，當應用程式欲將一客製化設定資料存入基本輸入輸出系統，則由應用程式使用安全密鑰對客製化設定資料進行加密以獲得加密資料，以及透過管理介面傳送加密資料至基本輸入輸出系統。由基本輸入輸出系統使用安全密鑰對該加密資料進行解密以獲得該客製化設定資料。若基本輸入輸出系統成功解密該加密資料，則基本輸入輸出系統儲存客製化設定資料。

An authentication method for accessing profile of basis input/output system (BIOS) is provided. When an application program wishes to save a customized profile data into the BIOS, the application program uses a security key to encrypt the customized profile data and derives a encrypted data. The encrypted data is transmitted to the BIOS through a management interface. The BIOS uses the security key to decrypt the encrypted data to derive the customized profile data. If the encrypted data is successfully decrypted by the BIOS, the BIOS saves the customized profile data.

S201~S208・・・步驟

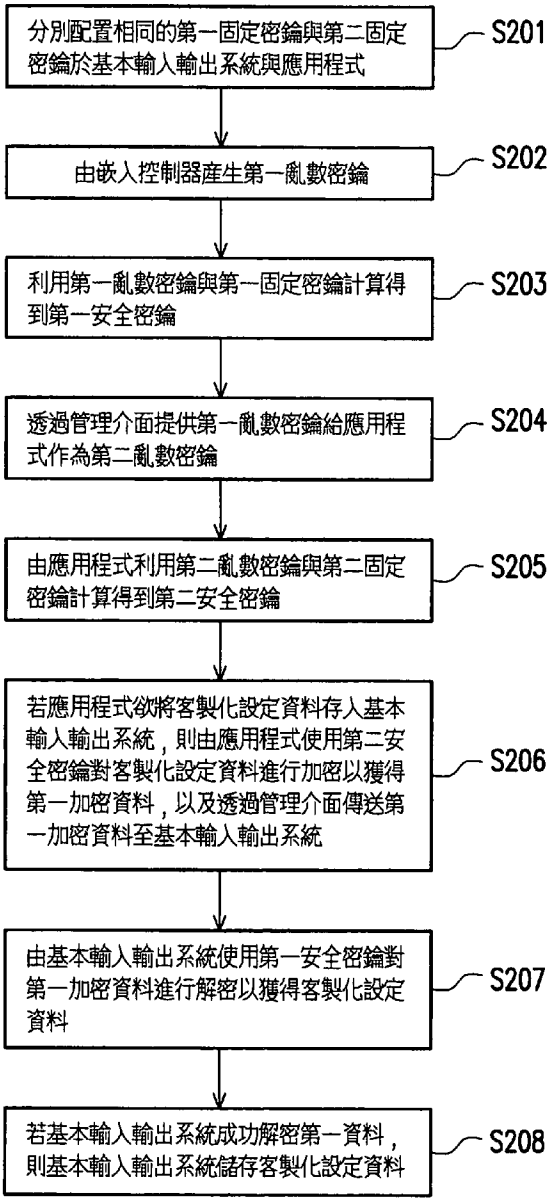

圖 2

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：100129917

※申請日：100.8.22 ※IPC分類：G06F 9/445 (2006.01)

21/00 (2013.01)

一、發明名稱：

存取基本輸入輸出系統設定的認證方法

AUTHENTICATION METHOD FOR ACCESSING PROFILE OF BASIC INPUT/OUTPUT SYSTEM

二、中文發明摘要：

一種存取基本輸入輸出系統設定的認證方法，當應用程式欲將一客製化設定資料存入基本輸入輸出系統，則由應用程式使用安全密鑰對客製化設定資料進行加密以獲得加密資料，以及透過管理介面傳送加密資料至基本輸入輸出系統。由基本輸入輸出系統使用安全密鑰對該加密資料進行解密以獲得該客製化設定資料。若基本輸入輸出系統成功解密該加密資料，則基本輸入輸出系統儲存客製化設定資料。

三、英文發明摘要：

An authentication method for accessing profile of basis input/output system (BIOS) is provided. When an application program wishes to save a customized profile data into the BIOS, the application program uses a security key to encrypt

the customized profile data and derives a encrypted data. The encrypted data is transmitted to the BIOS through a management interface. The BIOS uses the security key to decrypt the encrypted data to derive the customized profile data. If the encrypted data is successfully decrypted by the BIOS, the BIOS saves the customized profile data.

四、指定代表圖：

（一）本案之指定代表圖：圖 2

（二）本代表圖之元件符號簡單說明：

S201~S208：步驟

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】

本發明是有關於一種電腦系統，且特別是有關於電腦系統中一種存取基本輸入輸出系統的設定的認證方法。

【先前技術】

基本輸入輸出系統（Basic Input/Output System，以下稱 BIOS）是電腦在開機時最早載入的一段程式碼，具有初始化和檢測硬體及周邊設備，以及在完成上述工作後引導電腦載入作業系統（Operating System, OS）之功能。而 BIOS 中的設定檔（PROFILE）內容中包括了許多參數，例如各個硬體及周邊設備所對應之裝置編號以及該裝置啟用與否，或是中央處理器（Central Processing Unit, CPU）的操作頻率，甚至開機畫面及電腦製造商或品牌商的商標等，在 BIOS 開始執行時這些參數就會被載入作為初始化的依據。

由於目前的 BIOS 以及其設定檔目前都存放在快閃記憶體（Flash Memory）或電子抹除式可複寫唯讀記憶體（Electrically-Erasable Programmable Read-Only Memory, EEPROM）之中，使用者可以輕易的更新 BIOS 的內容。例如，在作業系統中透過應用軟體將新的設定檔或是韌體程式碼寫入 BIOS，以支援新的硬體及修正舊有的錯誤。

然而，BIOS 的設定檔往往不希望被一般使用者任意存取。例如，電腦銷售商可能不希望設定檔中的商標圖案

被更動。又或者，電腦銷售商可能不希望使用者透過修改BIOS 的設定檔，而在低價位的電腦機種中致能(enable)了高價位電腦的功能。若是在設定檔中的參數有誤，例如超出硬體本身的極限，或啟用了其實並不存在的硬體，就會增加系統在執行時的不穩定因素，甚至造成電腦或裝置無法正常使用。

【發明內容】

本發明提供一種存取基本輸入輸出系統之設定的認證方法，以防止非法應用程式存取基本輸入輸出系統之設定檔。

一種存取基本輸入輸出系統之設定的認證方法，包括以下步驟。首先分別配置相同的第一固定密鑰與第二固定密鑰於基本輸入輸出系統與應用程式。接著由嵌入式控制器產生第一亂數密鑰。然後利用第一亂數密鑰與該第一固定密鑰計算得到第一安全密鑰。再者，透過管理介面提供第一亂數密鑰給應用程式作為一第二亂數密鑰。並且，由應用程式利用第二亂數密鑰與第二固定密鑰計算得到一第二安全密鑰。此外，若應用程式欲將一客製化設定資料存入該基本輸入輸出系統，則由應用程式使用第二安全密鑰對客製化設定資料進行加密以獲得第一加密資料，以及透過管理介面傳送第一加密資料至基本輸入輸出系統。由基本輸入輸出系統使用第一安全密鑰對第一加密資料進行解密以獲得客製化設定資料。若基本輸入輸出系統成功解密

該第一加密資料，則基本輸入輸出系統儲存客製化設定資料。

基於上述，本發明提供了一種存取基本輸入輸出系統之設定的認證方法，使得當應用程式欲將設定資料存入基本輸入輸出系統時，需將設定資料以加密的方式透過一管理介面傳送至基本輸入輸出系統。基本輸入輸出系統會對驗證應用程式的存取要求是否合法。當驗證成功時，基本輸入輸出系統才會儲存這個設定資料。

為讓本發明之上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【實施方式】

圖 1 所繪示一種電腦的裝置方塊圖。請參照圖 1，中央處理器 101、唯讀記憶體單元 103、嵌入式控制器 104、儲存單元 105 及記憶體單元 106 皆與晶片組單元 102 連接，並透過晶片組單元 102 聯繫並交換信息。儲存單元 105 可以是磁碟機、光碟機、隨身碟等可開機儲存裝置。記憶體單元 106 可以是隨機存取記憶體(random access memory, RAM)。一般而言在電腦的電源開啟後，儲存於唯讀記憶體單元 103 的基本輸入輸出系統（Basic Input/Output System，以下稱 BIOS）韌體碼 1031 會開始被讀取執行之。自此以後，BIOS 開始運作。

BIOS 會控制嵌入式控制器 104 以讀取儲存於嵌入式控制器 104 的設定檔（PROFILE），接著 BIOS 根據設定

檔中的內容初始化各個重要的硬體元件(例如嵌入式控制器 104 等)，以及執行電源開啟自我測試（Power On Self Test，簡稱 POST）以診斷並確保這些裝置可以正確運作。在 POST 完成了工作之後，BIOS 將接著使系統讀入儲存於儲存單元 105 上之作業系統程式碼 1051。自此以後，作業系統開始運作。在進入作業系統環境後，製造商可以在作業系統中透過合法應用程式(工具程式)存取 BIOS 設定檔之內容。

圖 2 為根據本發明一實施例所繪示運作於圖 1 之電腦裝置上的一種存取 BIOS 之設定的認證方法的流程圖。請參照圖 2，在步驟 S201 中，分別配置相同的第一固定密鑰與第二固定密鑰於 BIOS 與應用程式。此固定密鑰可以在製造過程中便已被製造商配置於 BIOS 中。唯有製造商的合法應用程式具有相同的固定密鑰。

在步驟 S202 中，在每次電子裝置(例如電腦)開機後，嵌入式控制器即產生第一亂數密鑰。或者，在嵌入式控制器上電(power on)後的初始化階段，嵌入式控制器便可以產生第一亂數密鑰。由於嵌入式控制器隨機決定第一亂數密鑰，因此在每次開機後嵌入式控制器產生的第一亂數密鑰是無法預期的。在步驟 S203 中，利用第一亂數密鑰與該第一固定密鑰計算得到第一安全密鑰。在步驟 S204 中，BIOS 透過管理介面提供第一亂數密鑰給合法應用程式作為一第二亂數密鑰。在步驟 S205 中，由應用程式利用 BIOS 所提供的第二亂數密鑰與本身的第二固定密鑰計算得到一

第二安全密鑰。應用程式會保存此第二安全密鑰，以便稍後存取 BIOS 設定時進行認證與加密。

在步驟 S206 中，若應用程式欲將一客製化設定資料(例如系統組態設定值)存入該 BIOS，則由應用程式使用第二安全密鑰對客製化設定資料進行加密以獲得第一加密資料，以及透過管理介面傳送第一加密資料至 BIOS。在步驟 S207 中，由 BIOS 使用第一安全密鑰對第一加密資料進行解密以獲得客製化設定資料。最後在步驟 S208 中，若 BIOS 成功解密該第一加密資料，則 BIOS 儲存客製化設定資料。

圖 3 為根據本發明一示範實施例所繪示存取 BIOS 之設定的認證方法的時序流程圖。請參照圖 3，應用程式 300 是一個已經經過製造商或品牌商授權的合法程式，因此在應用程式 300 中會預先配置一個第二固定密鑰，而此第二固定密鑰與配置在 BIOS 302 中之第一固定密鑰相同。在本實施例中，第一及第二固定密鑰長度為 16 個位元組（Byte）固定密鑰內容則可以視製造需求而決定之，例如為"88740de3 - 3f73 - 4028 - bfbe - 1c3108a52968"。

首先，在每次電腦開機後，嵌入式控制器 303 即隨機地產生第一亂數密鑰（步驟 S301）。其中，此第一亂數密鑰可由嵌入式控制器 303 擷取系統中的時間函數或一電容器之電壓值等數值經由計算產生一隨機數值。此隨機數值可以是理想亂數或非理想亂數。但本發明不限於上述。第

一亂數密鑰只會在電腦系統的電源開啟後至關閉電源之前被計算/產生一次。若是電腦被重開機，為了提升安全性，則第一亂數密鑰會被再重新計算/產生一次。

應用程式300會向作業系統的管理介面301提出接收亂數密鑰的要求（步驟S302）。其中，所述管理介面301是應用程式300與BIOS 302之間的通訊界面，例如微軟公司（Microsoft Corp.）的視窗管理規範（Windows Management Instrumentation, WMI）的應用程式介面（Application Programming Interface, API）。應用程式301必須透過此管理介面301才能對BIOS 302進行存取。在管理介面301接收到應用程式300的要求後，便轉發此要求至BIOS 302(步驟S303)。在BIOS 302收到此要求後，BIOS 302便傳送第一固定密鑰至嵌入式控制器303(步驟S304)。然後，嵌入式控制器303利用接收到之第一固定密鑰以及本身於步驟S301所產生的第一亂數密鑰計算產生第一安全密鑰（步驟S305）。

在得到第一安全密鑰之後，嵌入式控制器303將第一安全密鑰傳送至BIOS 302（步驟S306）。BIOS 302保留第一安全密鑰並傳送通知至管理介面301，通知已可取得亂數密鑰（步驟S307）。管理介面301則接著轉發通知應用程式300已可取得亂數密鑰（步驟S308）。於是，應用程式300此時透過管理介面301發出取得第一亂數密鑰的要求（步驟S309、S310）。BIOS 302在接收到此要求之後，要求嵌入式控制器303提供第一亂數密鑰(步驟S311)。

嵌入式控制器 303 在接收到要求後回傳第一亂數密鑰至 BIOS 302(步驟 S312)，並在傳送第一亂數密鑰給 BIOS 302 後刪除第一亂數密鑰（步驟 S313）。BIOS 302 接著透過管理介面 301 傳送第一亂數密鑰至應用程式 300（步驟 S314、S315），並在傳送第一亂數密鑰給應用程式 300 後刪除第一亂數密鑰（步驟 S316）。應用程式 300 在收到第一亂數密鑰後，將其做為第二亂數密鑰，並利用此第二亂數密鑰與預先設置的第二固定密鑰計算得到第二安全密鑰（步驟 S317）。至此，應用程式 300 與 BIOS 302 已完成安全密鑰的初始化階段。

在開機後至關機(或重新開機)前，以上所述之步驟(步驟 S301～S317）僅需進行一次。步驟 S301～S317 可在應用程式 300 要第一次存取 BIOS 的設定檔之前才進行，亦可以在應用程式 300 被啟動的初期就預先被執行，但本發明不限定於上述。

請繼續參照圖 3，當應用程式 300 欲將客製化設定資料存入 BIOS 302 時，應用程式 300 利用第二安全密鑰加密此客製化設定資料，獲得第一加密資料（步驟 S320）。此客製化設定資料中可包括電腦之硬體設定參數(組態參數)以及/或是開機畫面圖檔等資料。接著，應用程式 300 將第一加密資料輸出至管理介面 301（步驟 S321）。管理介面 301 依照應用程式 300 的傳送需求，將第一加密資料輸出至 BIOS 302（步驟 S322）。因此，應用程式 300 可以透過管理介面 301 傳送第一加密資料至 BIOS 302。

BIOS 302 在收到第一加密資料後，進行驗證的動作（步驟 S323）。在本實施例中，BIOS 302 首先利用第一安全密鑰解密第一加密資料。在解密後，使用錯誤檢測方法，例如循環冗餘校驗（Cyclic Redundancy Check, CRC）或是資訊摘要演算法 5（Message-Digest Algorithm, MD5）等，來檢測是否成功解密第一加密資料。若 BIOS 302 可成功利用第一安全密鑰成功解密第一加密資料，則表示驗證成功，也就是表示用來加密的第二安全密鑰與用來解密的第一安全密鑰是相吻合(或相同)的。反之，若解密第一加密資料失敗，則代表驗證失敗，因此 BIOS 302 將拒絕存取（步驟 S323）。驗證成功後，BIOS 302 接著傳送步驟 S323 解密後的客製化設定資料至嵌入式控制器 303，並控制嵌入式控制器 303 儲存該客製化設定資料（步驟 S324）。嵌入式控制器 303 在接收到客製化設定資料及 BIOS 302 的控制指令後，嵌入式控制器 303 便將客製化設定資料存放於設定資料所對應的記憶體位置中（步驟 S325）。

上述實施例是由嵌入式控制器 303 計算第一安全密鑰。在其他實施例中，計算第一安全密鑰的操作可以由 BIOS 302 負責完成。例如，BIOS 302 可以向嵌入式控制器 303 讀取第一亂數密鑰，然後利用第一固定密鑰與第一亂數密鑰計算得到第一安全密鑰。在計算得到第一亂數密鑰及第一安全密鑰之後，BIOS 302 將第一亂數密鑰透過管理介面 301 傳送至應用程式 300。

本領域具有通常知識者可以採用任何加密方法實現上述步驟 S305、S317、S320。例如，圖 4 為根據本發明一示範實施例所繪示於應用程式 300 產生第二安全密鑰 SKEY2 與第一加密資料 ECPDATA1 之資料流的示意圖。請參照，首先，由應用程式 300 進行圖 3 中的步驟 S317，也就是圖 4 所示以第二固定密鑰 FKEY2 及第二亂數密鑰 RKEY2 透過單向函數(例如雜湊函數 501)產生第二安全密鑰 SKEY2。雜湊函數 501 是一種單向轉換函數，其可將輸入參數轉換為輸出參數，但極難利用輸出參數反向計算輸入參數。在本實施例中，雜湊函數 501 可以是第一安全雜湊演算法（Secure Hash Algorithm 1, SHA-1），但本發明不限定於上述。上述以雜湊函數 501 計算第二安全密鑰 SKEY2 的教示亦可以類推至圖 3 步驟 S305。

接著，若應用程式 300 欲將客製化設定資料 PRODATA 存入 BIOS 302，則應用程式 300 會將客製化設定資料 PRODATA 與第二安全密鑰 SKEY2 進行互斥或運算（Exclusive OR, XOR）502，而得到第一暫態資料 TMP1。然後，應用程式 300 再將第一暫態資料 TMP1 進行右旋（Rotate Right, ROR）運算 503，得到第一加密資料 ECPDATA1。例如，將第一暫態資料 TMP1 右旋 7 個位元。互斥或運算 502 與右旋計算 503 皆是用於增加加密資料的複雜度，然而本發明並不限定於使用此兩函數運算。

本領域具有通常知識者可以採用任何解密方法實現上述步驟 S323。例如，圖 5 為根據本發明一示範實施例所

繪示於 BOIS 302 解密第一加密資料 ECPDATA1 之資料流的示意圖。圖 5 所示解密的流程是對應於圖 4 所示加密的流程。請參照圖 5，第一加密資料 ECPDATA1 首先經過左旋（Rotate Left, ROL）運算 601 (例如左旋 7 個位元)得到第二暫態資料 TMP2。接著，將第二暫態資料 TMP2 與第一安全密鑰 SKEY1 進行互斥或運算 602 得到客製化設定資料 PRODATA。本發明並不限定於使用此兩函數之運算，惟解密之運算必須對應於加密的運算步驟才能夠解出正確的資料內容。

圖 6 為根據本發明一實施例所繪示應用程式 300 透過管理介面 301 讀取 BIOS 302 設定之動作的時序流程圖。請參照圖 6，首先，應用程式 300 透過管理介面 301 傳送關於當前 BIOS 302 設定資料的讀取需求至 BIOS 302（步驟 S701、S702）。接著，BIOS 302 驗證此讀取需求（步驟 S703）。在本實施例中，讀取需求同樣的在應用程式 300 利用第二安全密鑰加密，如同圖 4 中所述之加密方式。驗證的方法則如同圖 3 之實施例中所述，在此不多贅述。

例如，若應用程式 300 欲從 BIOS 302 讀取系統設定資料，則由該應用程式 300 使用第二安全密鑰 SKEY2 對「讀取資訊」進行加密以獲得第二加密資料，以及透過管理介面 302 傳送該第二加密資料至 BIOS 302。上述「讀取資訊」的內容可以是讀取指令碼、系統設定資料的讀取位址及/或系統設定資料的識別碼等。

BIOS 302 於步驟 S703 使用第一安全密鑰 SKEY1 對

該第二加密資料進行解密，以獲得該「讀取資訊」。如果步驟 S703 驗證失敗，則 BIOS 302 拒絕存取。若 BIOS 302 檢查第二安全密鑰與第一安全密鑰為吻合，即 BIOS 302 成功解密該第二加密資料，則 BIOS 302 根據該讀取資訊向嵌入式控制器 303 要求讀取系統設定資料(步驟 S704)。嵌入式控制器 303 在接收到讀取需求後，便根據讀取需求讀取系統設定資料（步驟 S705），並接著回傳系統設定資料給 BIOS 302（步驟 S706）。BIOS 302 透過管理介面 301 將系統設定資料傳送給應用程式 300（步驟 S707、S708）。

綜上所述，本發明提供了一種存取 BIOS 之設定的認證方法，利用預先配置於 BIOS 與授權的程式端的密鑰及每次開機才隨機產生的另一密鑰產生一安全密鑰，加密透過作業系統的管理介面所傳送的設定資料，並利用此安全密鑰作為認證。此方法使得在作業系統中其他非授權的應用程式不能輕易的存取或編輯 BIOS 的設定，也無法透過管理介面讀取 BIOS 之設定內容，而進而確保了系統不因 BIOS 之設定而產生不穩定之情況。

雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，故本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

圖 1 所繪示一種電腦的裝置方塊圖。

圖 2 為根據本發明一實施例所繪示一種存取基本輸入輸出系統之設定的認證方法的流程圖。

圖 3 為根據本發明一示範實施例所繪示存取基本輸入輸出系統之設定的認證方法的時序流程圖。

圖 4 為根據本發明一示範實施例所繪示於應用程式端產生第一加密資料之資料流的示意圖。

圖 5 為根據本發明一示範實施例所繪示於基本輸入輸出端解密第一加密資料之資料流的示意圖。

圖 6 為根據本發明一實施例所繪示應用程式透過管理介面傳送讀取需求與第二安全密鑰至基本輸入輸出系統之動作的時序流程圖。

【主要元件符號說明】

101：中央處理器單元

102：晶片組單元

103：唯讀記憶體單元

1031：基本輸入輸出系統韌體碼

104：嵌入式控制器

105：儲存單元

1051：作業系統程式碼

106：記憶體單元

300：應用程式

301：管理介面

302：基本輸入輸出系統

303：嵌入式控制器

501：雜湊函數

502、602：互斥或運算

503：右旋運算

601：左旋運算

S201～S208、S301～S317、S320～S325、S701～S708：步驟

ECPDATA1：第一加密資料

FKEY2：固定密鑰

PRODATA：客製化設定資料

RKEY2：亂數密鑰

SKEY2、SKEY1：安全密鑰

TMP1、TMP2：暫態資料

七、申請專利範圍：

1. 一種存取基本輸入輸出系統之設定的認證方法，包括：

分別配置相同的一第一固定密鑰與一第二固定密鑰於一基本輸入輸出系統與一應用程式；

由一嵌入式控制器產生一第一亂數密鑰；

利用該第一亂數密鑰與該第一固定密鑰計算得到一第一安全密鑰；

透過一管理介面提供該第一亂數密鑰給該應用程式作為一第二亂數密鑰；

由該應用程式利用該第二亂數密鑰與該第二固定密鑰計算得到一第二安全密鑰；

若該應用程式欲將一客製化設定資料存入該基本輸入輸出系統，則由該應用程式使用該第二安全密鑰對該客製化設定資料進行加密以獲得一第一加密資料，以及透過該管理介面傳送該第一加密資料至該基本輸入輸出系統；

由該基本輸入輸出系統使用該第一安全密鑰對該第一加密資料進行解密以獲得該客製化設定資料；以及

若該基本輸入輸出系統成功解密該第一加密資料，則該基本輸入輸出系統儲存該客製化設定資料。

2.如申請專利範圍第 1 項所述之認證方法，其中所述對該客製化設定資料進行加密之步驟包括：

將該客製化設定資料與該第二安全密鑰進行一互斥或運算而獲得一第一暫態資料；以及

將該第一暫態資料進行一右旋運算而獲得該第一加密資料。

3.如申請專利範圍第 1 項所述之認證方法，其中所述對該第一加密資料進行解密之步驟包括：

將該第一加密資料進行一左旋運算而獲得一第二暫態資料；以及

將該第二暫態資料與該第一安全密鑰進行一互斥或運算而獲得該客製化設定資料。

4.如申請專利範圍第 1 項所述之認證方法，更包括：

若該應用程式欲從該基本輸入輸出系統讀取一系統設定資料，則由該應用程式使用該第二安全密鑰對一讀取資訊進行加密以獲得一第二加密資料，以及透過該管理介面傳送該第二加密資料至該基本輸入輸出系統；

由該基本輸入輸出系統使用該第一安全密鑰對該第二加密資料進行解密以獲得該讀取資訊；以及

若該基本輸入輸出系統成功解密該第二加密資料，則該基本輸入輸出系統根據該讀取資訊讀取該系統設定資料，並透過該管理介面傳送該系統設定資料給該應用程式。

5. 如申請專利範圍第 1 項所述之認證方法，其中所述管理介面為一視窗管理規範的應用程式介面。

6. 如申請專利範圍第 1 項所述之認證方法，更包括：

在該應用程式獲得該第二亂數密鑰後，刪除該第一亂數密鑰。

7. 如申請專利範圍第 1 項所述之認證方法，其中所述

利用該第一亂數密鑰與該第一固定密鑰計算得到該第一安全密鑰的步驟包括：

由該基本輸入輸出系統傳送該第一固定密鑰至該嵌入式控制器；

由該嵌入式控制器根據該第一亂數密鑰及該第一固定密鑰計算得到該第一安全密鑰；

將該第一安全密鑰傳送至該基本輸入輸出系統；以及

在該基本輸入輸出系統將該第一亂數密鑰傳輸給該應用程式後，該嵌入式控制器與該基本輸入輸出系統刪除該第一亂數密鑰。

8. 如申請專利範圍第 1 項所述之認證方法，其中所述利用該第一亂數密鑰與該第一固定密鑰計算得到該第一安全密鑰的步驟以及所述利用該第二亂數密鑰與該第二固定密鑰計算得到該第二安全密鑰的步驟，是使用單向函數計算該第一安全密鑰與該第二安全密鑰。

9. 如申請專利範圍第 8 項所述之認證方法，其中所述單向函數為雜湊函數。

10.如申請專利範圍第 1 項所述之認證方法，其中所述該基本輸入輸出系統儲存該客製化設定資料之步驟包括：

該基本輸入輸出系統將該客製化設定資料儲存至該嵌入式控制器。

八、圖式:

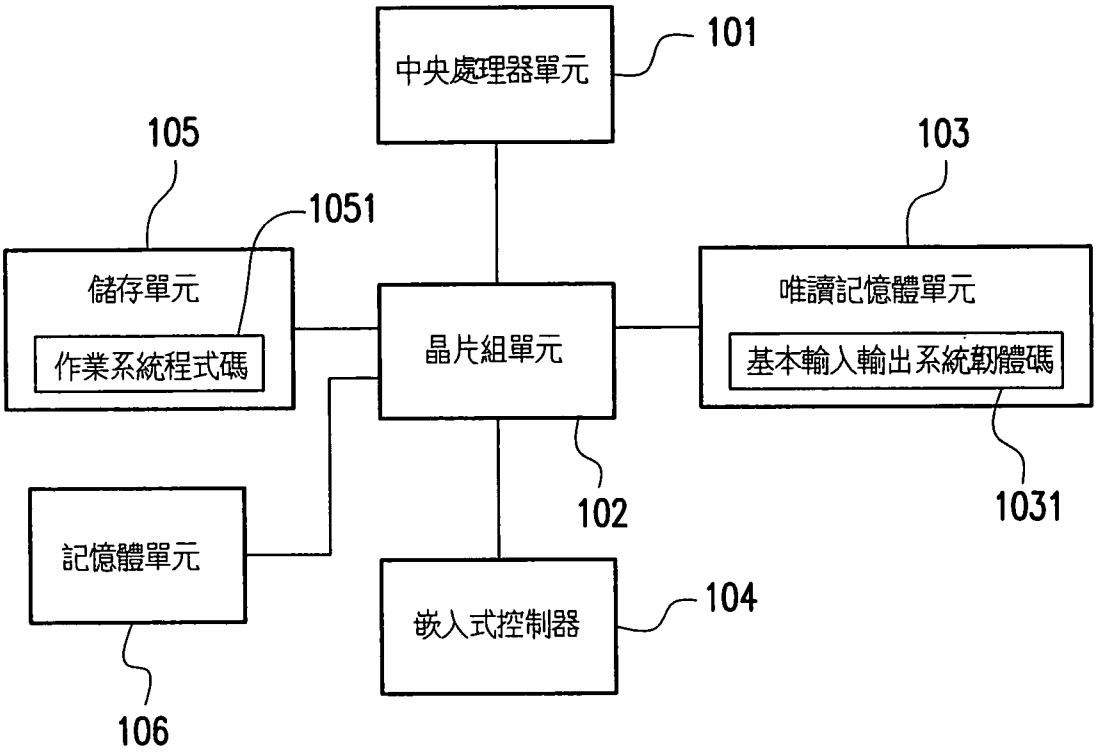
中央處理器單元
101
105
1051
103
儲存單元
作業系統程式碼
晶片組單元
唯讀記憶體單元
基本輸入輸出系統韌體碼
102
1031
記憶體單元
嵌入式控制器
104
106

圖 1

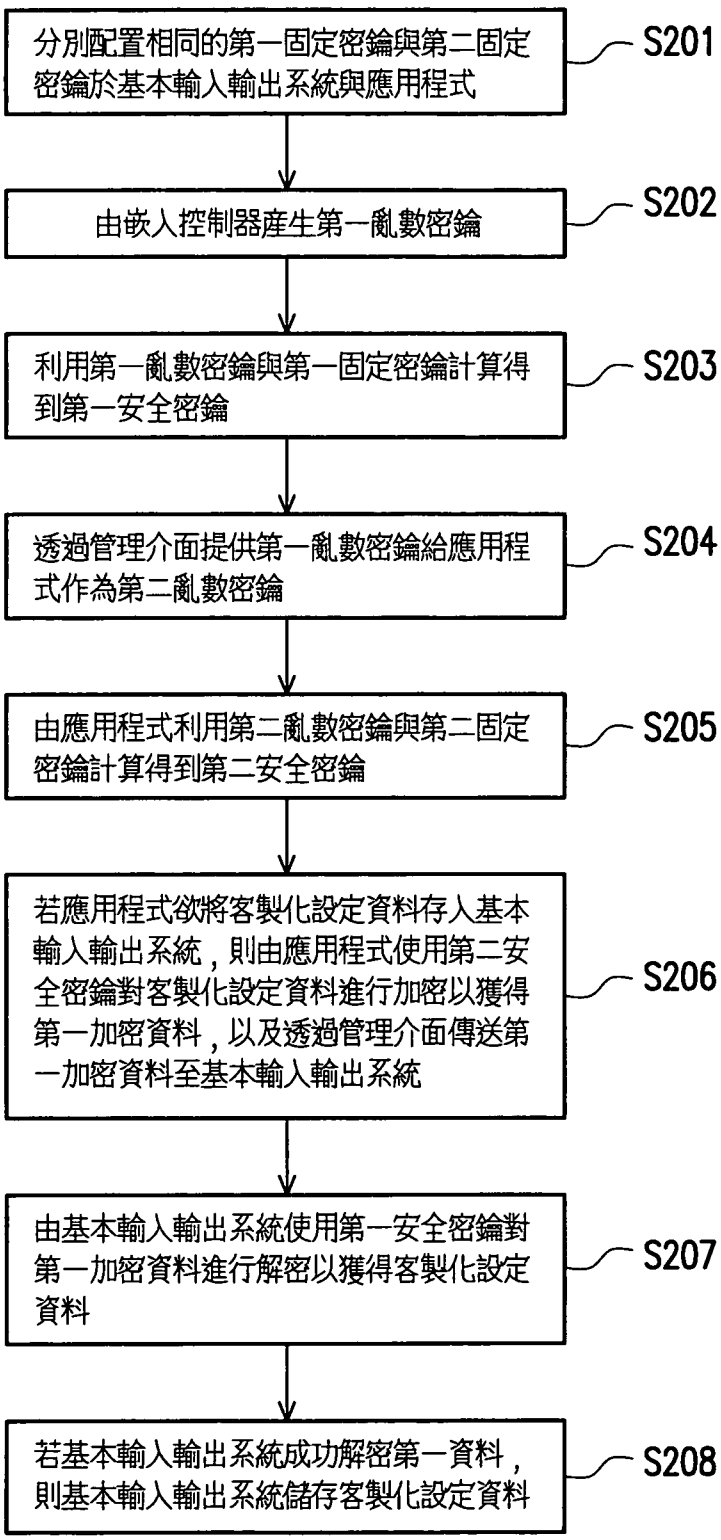
分別配置相同的第一固定密鑰與第二固定密鑰於基本輸入輸出系統與應用程式
S201
由嵌入控制器產生第一亂數密鑰
S202
利用第一亂數密鑰與第一固定密鑰計算得到第一安全密鑰
S203
透過管理介面提供第一亂數密鑰給應用程式作為第二亂數密鑰
S204
由應用程式利用第二亂數密鑰與第二固定密鑰計算得到第二安全密鑰
S205
若應用程式欲將客製化設定資料存入基本輸入輸出系統，則由應用程式使用第二安全密鑰對客製化設定資料進行加密以獲得第一加密資料，以及透過管理介面傳送第一加密資料至基本輸入輸出系統
S206
由基本輸入輸出系統使用第一安全密鑰對第一加密資料進行解密以獲得客製化設定資料
S207
若基本輸入輸出系統成功解密第一資料，則基本輸入輸出系統儲存客製化設定資料
S208

圖 2

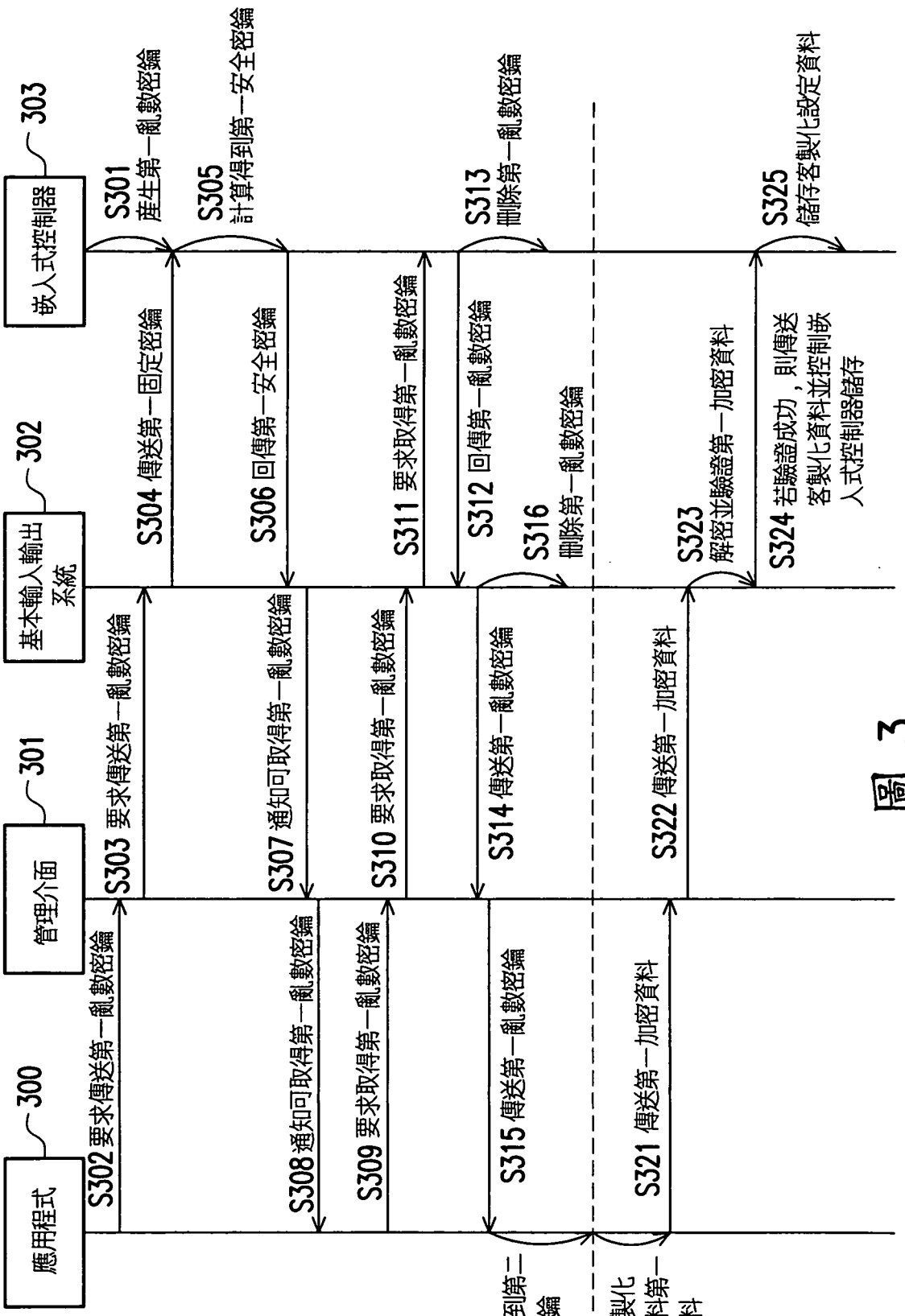
應用程式
300
管理介面
301
基本輸入輸出系統
302
嵌入式控制器
303
S301 產生第一亂數密鑰
S302 要求傳送第一亂數密鑰
S303 要求傳送第一亂數密鑰
S304 傳送第一固定密鑰
S305 計算得到第一安全密鑰
S306 回傳第一安全密鑰
S307 通知可取得第一亂數密鑰
S308 通知可取得第一亂數密鑰
S309 要求取得第一亂數密鑰
S310 要求取得第一亂數密鑰
S311 要求取得第一亂數密鑰
S312 回傳第一亂數密鑰
S313 刪除第一亂數密鑰
S314 傳送第一亂數密鑰
S315 傳送第一亂數密鑰
S316 刪除第一亂數密鑰
S317 計算得到第二安全密鑰
S320 加密客製化設定資料第一加密資料
S321 傳送第一加密資料
S322 傳送第一加密資料
S323 解密並驗證第一加密資料
S324 若驗證成功，則傳送客製化資料並控制嵌入式控制器儲存
S325 儲存客製化設定資料

圖 3

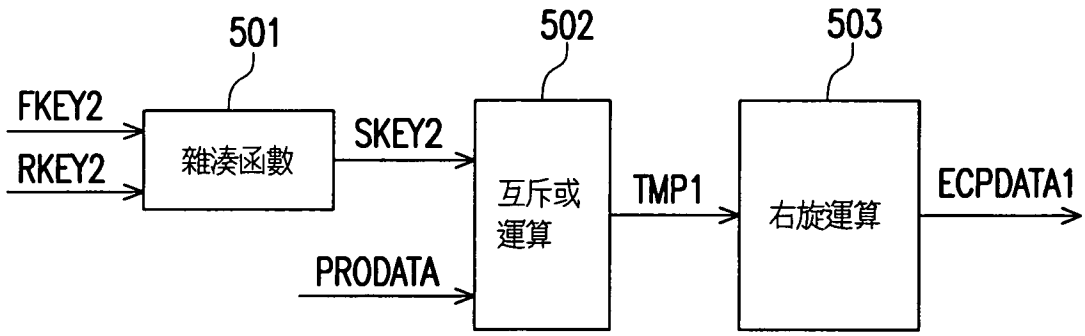
501
502
503
FKEY2
RKEY2
雜湊函數
SKEY2
互斥或
運算
TMP1
右旋運算
ECPDATA1
PRODATA

圖 4

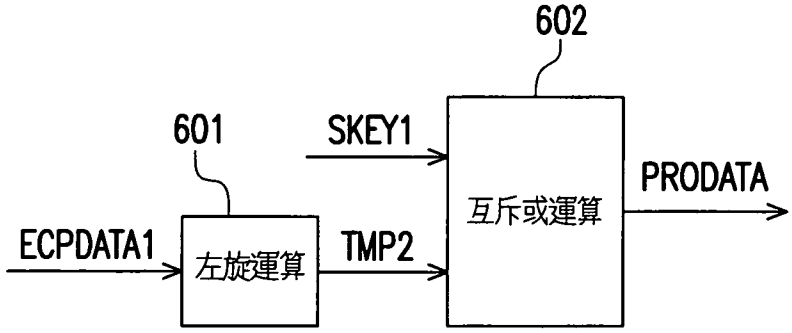
602
601
SKEY1
PRODATA
互斥或運算
ECPDATA1
左旋運算
TMP2

圖 5

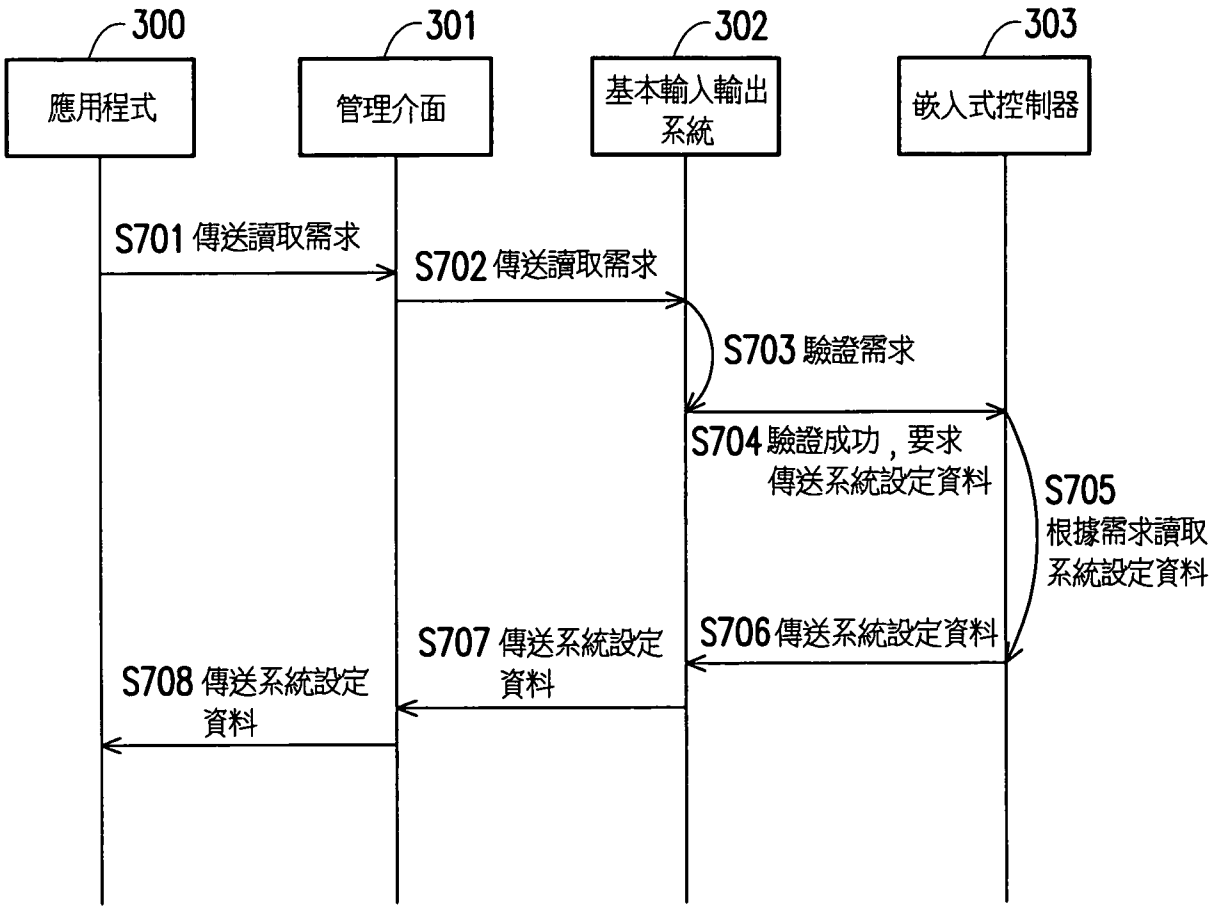
300
301
302
303
應用程式
管理介面
基本輸入輸出系統
嵌入式控制器
S701 傳送讀取需求
S702 傳送讀取需求
S703 驗證需求
S704 驗證成功，要求傳送系統設定資料
S705 根據需求讀取系統設定資料
S706 傳送系統設定資料
S707 傳送系統設定資料
S708 傳送系統設定資料

圖 6