(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201030556 A1
(43)公開日： 中華民國 99 (2010) 年 08 月 16 日

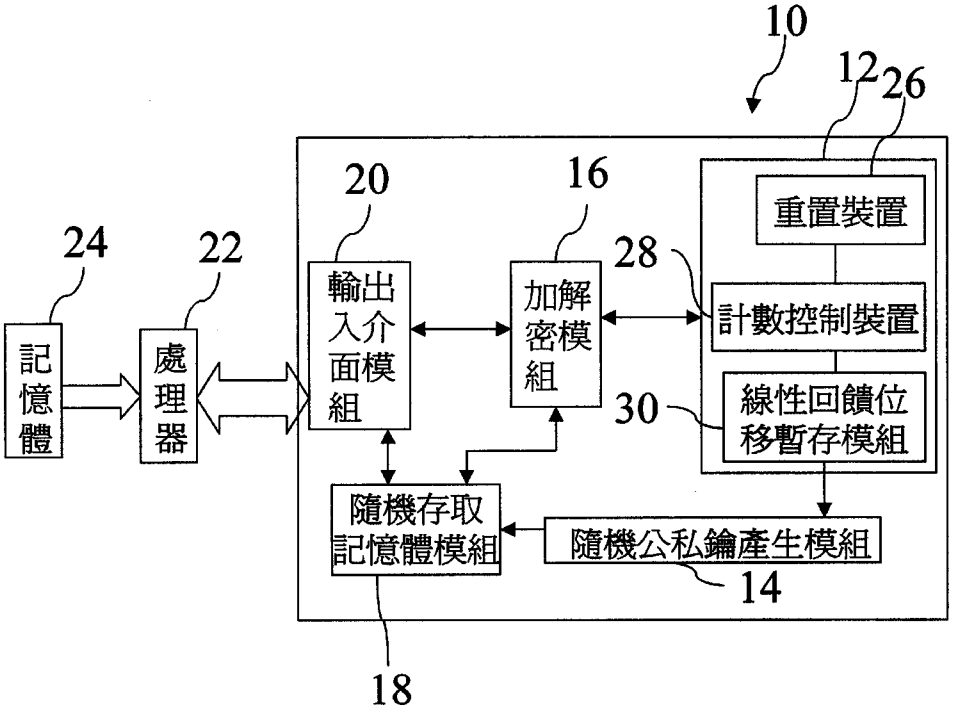
(21)申請案號：098104612 (22)申請日： 中華民國 98 (2009) 年 02 月 13 日
(51)Int. Cl.： *G06F21/22 (2006.01)*
(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號
(72)發明人：林進燈 (TW) ；吳孟哲 (TW) ；鍾仁峰 (TW) ；沈子貴 (TW) ；洪紹航 (TW)
(74)代理人：林火泉
申請實體審查：有 申請專利範圍項數：16 項 圖式數：3 共 18 頁

(54)名稱

保護軟體內容之嵌入式保護裝置及其保護方法

(57)摘要

本發明係揭露一種保護軟體內容之嵌入式保護裝置及其保護方法，其係在一處理器執行嵌入式軟體，即韌體程式時執行授權檢查，此嵌入式保護裝置可接收韌體程式執行時所傳送之授權碼，藉以在內部連續產生一虛擬隨機亂數，之後再利用此亂數產生公、私鑰，對授權碼加密，並形成一加密資料，之後更可對此加密資料進行解密，並將結果傳回執行的處理器，以判斷是否可進行授權。若是，則執行此韌體程式，且重複上述的加密動作；若否，則無法執行此韌體程式。本發明係利用硬體執行加解密動作，進而使嵌入式韌體受到更好的安全保護機制。



10：嵌入式保護裝置
12：隨機亂數產生模組
14：隨機公私鑰產生模組
16：加解密模組
18：隨機存取記憶體模組
20：輸出入介面模組
22：處理器
24：記憶體
26：重置裝置
28：計數控制模組
30：線性回饋位移暫存模組

201030556

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：98104612

※ 申請日：98、2、13　　※IPC 分類：G06F 21/22 (2006.01)

一、發明名稱：（中文/英文）

保護軟體內容之嵌入式保護裝置及其保護方法

二、中文發明摘要：

本發明係揭露一種保護軟體內容之嵌入式保護裝置及其保護方法，其係在一處理器執行嵌入式軟體，即韌體程式時執行授權檢查，此嵌入式保護裝置可接收韌體程式執行時所傳送之授權碼，藉以在內部連續產生一虛擬隨機亂數，之後再利用此亂數產生公、私鑰，對授權碼加密，並形成一加密資料，之後更可對此加密資料進行解密，並將結果傳回執行的處理器，以判斷是否可進行授權。若是，則執行此韌體程式，且重複上述的加密動作；若否，則無法執行此韌體程式。本發明係利用硬體執行加解密動作，進而使嵌入式韌體受到更好的安全保護機制。

三、英文發明摘要：

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	嵌入式保護裝置	12	隨機亂數產生模組
14	隨機公私鑰產生模組	16	加解密模組
18	隨機存取記憶體模組	20	輸出入介面模組
22	處理器	24	記憶體
26	重置裝置	28	計數控制模組
30	線性回饋位移暫存模組		

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明係有關一種保護技術，特別是關於一種保護軟體內容之嵌入式保護裝置及其保護方法。

【先前技術】

於此一資訊科技發達的時代，舉凡資訊、通訊網路與消費性電子產品均為現代人進行訊息交流及資料處理作業所不可缺少之輔助工具。有鑑於此，相關產品製造商對此一龐大的消費商機，莫不傾力進行研發設計，期能製造出符合消費者需求之資訊設備，藉以於該項產品領域中獲得大多數消費者之青睞，而居於領導地位，進而提高企業本身的競爭力，因此，遂使相關產品製造商間之競爭更形激烈。

此些產品製造商除投入產品競爭外，彼此間亦有一共同的的信念，亦即產品若欲具有競爭力，則產品所附加之功能就必須愈接近人性化，使大多數消費者所能接受，而當中的關鍵即在於資訊設備內部所含之嵌入式軟體，此軟體系寫入於硬體內部(稱之為韌體)，用以負責硬體驅動、程序控制及介面處理，是故，一套功能完整的嵌入式軟體可提升資訊設備的價值與競爭優勢，亦可能因此提高該軟體被人所盜拷的機率，而令合法擁有該軟體製造商遭受龐大的利益損失，進而阻礙了日後其他嵌入式軟體的發展。

而過去的軟體或韌體保護方式，大部分是藉由加密技術、序號保護、軟體發送授權，通常在軟體產品開發過程中的安全顧慮，主要包括開發時期研發人員的不適當存取、開發完成後軟體遭盜版的行為、軟體發送授權的安全性，以及軟體流通後的使用狀況等，都有極大可能讓軟體的保護方

式被破解。另一方面，就韌體而言，保護機制就更加薄弱，幾乎只要取得硬體及韌體程式，不需要任何授權即可使用。

雖然為了解決上述問題，有的專利曾提出一種保密器，此種保密器僅利用線性回饋位移暫存器來產生虛擬隨機亂數，但此種設計有一個缺點，因為它具有週期性，所以在每幾個週期之後，會不斷產生一樣的一串亂數。這種方式仍有疑遭人破解之風險。

因此，本發明係在針對上述之困擾，提出一種保護軟體內容之嵌入式保護裝置及其保護方法，其係可改善習知缺點。

【發明內容】

本發明之主要目的，在於提供一種保護軟體內容之嵌入式保護裝置及其保護方法，其係將羅納德·李維斯特、阿迪·薩莫爾和倫納德·阿德曼(RSA)演算法，利用硬體協同加解密的方式來實現，進而使嵌入式韌體受到更好的安全保護機制。

為達上述目的，本發明提供一種保護軟體內容之嵌入式保護裝置，包含一隨機亂數產生模組，其係根據韌體程式在處理器執行時所傳送之授權碼，藉以連續產生一虛擬隨機亂數；一隨機公私鑰產生模組，其係連接隨機亂數產生模組，並利用接收之虛擬隨機亂數對授權碼藉由 RSA 演算法產生公鑰及私鑰，隨機公私鑰產生模組連接一隨機存取記憶體模組，此記憶體模組可儲存接收之授權碼，及其對應的虛擬隨機亂數、公鑰、私鑰。上述三模組皆連接到一加解密模組，此加解密模組利用接收之虛擬隨機亂數、公鑰、私鑰，對隨機存取記憶體模組中所存的授權碼、虛擬隨機亂數、公鑰、私鑰進行加密，形成加密資料後，傳送給韌體程式，而在執行授權

檢查時，加解密模組則接收該韌體程式傳送之加密資料，以進行解密，並將解碼出來之結果數值輸出至隨機存取記憶體模組後，與其中所儲存的授權碼、虛擬隨機亂數、公鑰、私鑰進行比對，以控制該韌體程式之執行狀態；最後尚有一輸出入介面模組，其係連接處理器、加解密模組與隨機存取記憶體模組，並作為上述模組和處理器互相傳遞資料的介面。

本發明亦提供一種保護軟體內容之保護方法，首先根據韌體程式所傳送之授權碼，藉以連續產生一虛擬隨機亂數，接著執行一加密流程，其係首先利用虛擬隨機亂數對授權碼藉由 RSA 演算法產生公鑰及私鑰，接著儲存授權碼及其對應之虛擬隨機亂數、私鑰與公鑰，之後對授權碼及其對應之虛擬隨機亂數、公鑰及私鑰進行加密，形成一加密資料後，傳給韌體程式，至此加密流程結束。再來則執行一授權流程，其係首先接收韌體程式傳送之加密資料，並進行解密，將解碼出來之結果數值與該授權碼及其對應之虛擬隨機亂數、公鑰及私鑰進行比對，以得到一比對結果，接著判斷該比對結果是否可進行授權，若是，則執行該韌體程式，且重複進行上述之加密流程；若否，則無法執行該韌體程式。

茲為使　貴審查委員對本發明之結構特徵及所達成之功效更有進一步之瞭解與認識，謹佐以較佳之實施例圖及配合詳細之說明，說明如後：

【實施方式】

請參閱第 1 圖，當欲使用記憶體 24 中的嵌入式軟體，即韌體程式時，可將此記憶體 24 載入一處理器 22 中，以執行該韌體程式，此記憶體 24 可為電可擦除可編程唯讀記憶體（EEPROM）或快閃記憶體（Flash）。而本發明之嵌入式保護裝置 10 係在一處理器 22 執行韌體程式時執行授權檢查，

其安裝位置係可內建於處理器 22 中，或整合於處理器 22 之匯流排上，處理器 22 可為中央處理器（CPU）或數位訊號處理器（DSP）。此保護裝置 10 包含一隨機亂數產生模組 12，其係根據韌體程式在處理器 22 執行時所傳送之授權碼，藉以連續產生一不具週期性之虛擬隨機亂數；一隨機公私鑰產生模組 14，其係連接隨機亂數產生模組 12，並接收虛擬隨機亂數，該隨機公私鑰產生模組 14 會先檢查此虛擬隨機亂數是否為質數，若否，則繼續選擇下一個參數；若是，則利用此質數藉由羅納德·李維斯特、阿迪·薩莫爾和倫納德·阿德曼（RSA）演算法對授權碼產生公鑰及私鑰，隨機公私鑰產生模組 14 連接一隨機存取記憶體模組 18，此記憶體模組 18 可儲存接收之授權碼，及其對應的虛擬隨機亂數、公鑰、私鑰。上述三模組 12、14、18 皆連接到一加解密模組 16，此加解密模組 16 利用接收之虛擬隨機亂數、公鑰、私鑰，對隨機存取記憶體模組 18 中所存的授權碼、虛擬隨機亂數、公鑰、私鑰進行加密，形成加密資料後，傳送給韌體程式，而在執行授權檢查時，加解密模組 16 則接收該韌體程式傳送之加密資料，以進行解密，並將解碼出來之結果數值輸出至隨機存取記憶體模組 18 後，與其中所儲存的授權碼、虛擬隨機亂數、公鑰、私鑰進行比對，以控制該韌體程式之執行狀態，同時將比對結果透過輸出入介面模組 20 回傳至韌體程式進行授權顯示；最後尚有一輸出入介面模組 20，其係連接處理器 22、加解密模組 16 與隨機存取記憶體模組 18，並作為上述模組 12、14、16、18、20 和處理器 22 互相傳遞資料的介面。

在軟體部分，當韌體程式執行時，輸出入介面模組 20 可隨機插入檢查點，以作為提供軟硬體協定資料溝通時之隨機取樣依據，並配合隨機亂數

產生模組12取得當下所產生的虛擬隨機亂數，分別把此亂數當作分時快速傅立業轉換演算法中運算的中間係數、檢查後結果擺放位置參數、檢查後結果擺放位置延遲參數，此三種參數的解釋說明如下：

（1）快速傅立業轉換演算法中運算的中間係數：利用軟體回傳的隨機檢查點，作為取樣時間，取出當下亂數產生模組12所產生之虛擬隨機亂數，作為在快速傅立業轉換演算法中，運算所需之八個係數，每一個係數為一個位元共八位元，並將此八位元放置於回傳給軟體溝通協定的位元組當中。

（2）檢查後結果擺放位置參數：利用軟體回傳的隨機檢查點，作為取樣時間，取出當下亂數產生模組12所產生之虛擬隨機亂數，作為在快速傅立業轉換演算法中，運算結果八個位置中其中一個，將此位置用八個位元表示，並將此八位元放置於回傳給軟體溝通協定的位元組當中。

（3）檢查後結果擺放位置延遲參數：利用軟體回傳的隨機檢查點，作為取樣時間，取出當下亂數產生模組12所產生之虛擬隨機亂數，作為決定上述回傳檢查後結果擺放位置參數，在整個回傳給軟體的溝通協定當中的第幾個位元組，用八位元表示，並將此八位元放置於回傳給軟體溝通協定的位元組當中。

本發明之隨機亂數產生模組12包含了重置裝置26、計數控制模組28與線性回饋位移暫存模組30。計數控制模組28可計算當啟用重置裝置26時所經過的時脈數以輸出一控制訊號，而線性回饋位移暫存模組30可接收該控制訊號作為延遲給值的依據，並根據控制訊號與授權碼以連續產生不具週期性之虛擬隨機亂數。在此設計中，亂數的產生是為了要給後面做質數檢查，若每次檢查都從頭開始，則每次取到的質數都會一樣，因此利用

一個計數控制模組 28 控制亂數的週期性，讓之後做質數檢查時不會從頭開始檢查，這樣每次取到的質數都將會不一樣。

以下介紹本發明之保護裝置的作動過程，請同時參閱第 1 圖與第 2 圖，首先如步驟 S10 所示，隨機亂數產生模組 12 根據韌體程式所傳送之授權碼，藉以連續產生一不具週期性之虛擬隨機亂數。接著執行一加密流程，其係首先如步驟 S12 所示，隨機公私鑰產生模組 14 接收此隨機虛擬亂數，並先檢查此虛擬隨機亂數是否為質數，若否，則如步驟 S14 所示，回至步驟 S12，以繼續選擇接收下一個參數；若是，則如步驟 S16 所示，利用此質數藉由 RSA 演算法對授權碼產生公鑰及私鑰。執行完步驟 S16 後，接著如步驟 S18 所示，隨機存取記憶體模組 18 儲存接收之授權碼及其對應之虛擬隨機亂數、私鑰與公鑰。之後如步驟 S20 所示，由於虛擬隨機亂數、私鑰與公鑰都是連續產生的，因此加解密模組 16 可利用此時所產生的虛擬隨機亂數、私鑰與公鑰對隨機存取記憶體模組 18 儲存的授權碼及其對應之虛擬隨機亂數、公鑰及私鑰進行加密，形成一加密資料後，傳給韌體程式，至此加密流程結束。再來執行一授權流程，其係首先如步驟 S22 所示，加解密模組 16 接收韌體程式傳送之加密資料，並進行解密，將解碼出來之結果數值傳輸至隨機存取記憶體模組 18，並與其中所儲存的授權碼及其對應之虛擬隨機亂數、公鑰及私鑰進行比對，以得到一比對結果，同時將比對結果透過輸出入介面模組 20 回傳至韌體程式進行授權顯示。接著如步驟 S24 所示，藉由該比對結果判斷是否可進行授權，若是，則如步驟 S26 所示，執行韌體程式，且重複進行上述加密流程；若否，則如步驟 S28 所示，無法執行韌體程式。

當比對結果的判斷為可進行授權時，會重複進行加密流程，不過在執行當中，由於已經不是第一次執行此流程，因此隨機存取記憶體模組 18 此時已經內存有授權碼，不需要再次接收，除此之外，其餘的流程皆相同。

當進行完授權流程後，若下一次還要執行韌體程式時，就會直接再一次執行授權流程，而不會從加密流程開始執行。

上述的隨機亂數產生模組 12 產生虛擬隨機亂數的方式如第 3 圖所示，並請同時參閱第 1 圖，首先如步驟 S102 所示，啟用重置裝置 26。接著如步驟 S104 所示，計數控制模組 28 可計算當啟用重置裝置 26 時所經過的時脈數以輸出一控制訊號。再來如步驟 S106 所示，線性回饋位移暫存模組 30 可接收該控制訊號作為延遲給值的依據，並根據控制訊號與授權碼以連續產生不具週期性之虛擬隨機亂數。

綜上所述，本發明係將 RSA 演算法，利用硬體協同加解密的方式來實現，進而使嵌入式韌體受到更好的安全保護機制，是一相當實用的發明。

以上所述者，僅為本發明一較佳實施例而已，並非用來限定本發明實施之範圍，故舉凡依本發明申請專利範圍所述之形狀、構造、特徵及精神所為之均等變化與修飾，均應包括於本發明之申請專利範圍內。

【圖式簡單說明】

第 1 圖為本發明之裝置架構示意圖。

第 2 圖為本發明之方法流程示意圖。

第 3 圖為本發明之產生虛擬隨機亂數之方法流程示意圖。

【主要元件符號說明】

10　嵌入式保護裝置　　12　隨機亂數產生模組

14 隨機公私鑰產生模組　　16 加解密模組

18 隨機存取記憶體模組　　20 輸出入介面模組

22 處理器　　24 記憶體

26 重置裝置　　28 計數控制模組

30 線性回饋位移暫存模組

七、申請專利範圍：

1. 一種保護軟體內容之嵌入式保護裝置，其係在一處理器執行韌體程式時執行授權檢查，該嵌入式保護裝置包含：

一隨機亂數產生模組，其係根據該韌體程式執行時所傳送之授權碼，藉以連續產生一虛擬隨機亂數；

一隨機公私鑰產生模組，其係連接該隨機亂數產生模組，並利用接收之該虛擬隨機亂數對該授權碼產生公鑰及私鑰；

一隨機存取記憶體模組，其係連接該隨機公私鑰產生模組，並儲存接收之該授權碼，及其對應的該虛擬隨機亂數、該公鑰、該私鑰；

一加解密模組，其係連接該隨機亂數產生模組、該隨機存取記憶體模組與該隨機公私鑰產生模組，該加解密模組利用接收之該虛擬隨機亂數、該公鑰、該私鑰，對該隨機存取記憶體模組中所存的該授權碼、該虛擬隨機亂數、該公鑰、該私鑰進行加密，形成該加密資料後，傳送給該韌體程式，在執行授權檢查時，該加解密模組接收該韌體程式傳送之該加密資料，以進行解密，並將解碼出來之結果數值輸出至該隨機存取記憶體模組後，與其中所儲存的該授權碼、該虛擬隨機亂數、該公鑰、該私鑰進行比對，以控制該韌體程式之執行狀態；以及

一輸出入介面模組，其係連接該處理器、該加解密模組與該隨機存取記憶體模組，並作為上述模組和該處理器互相傳遞資料的介面。

2. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該韌體程式執行時，該輸出入介面模組可隨機插入檢查點，以作為提供軟硬體協定資料溝通時之隨機取樣依據，並配合隨機亂數產生模組取得當

下所產生的虛擬隨機亂數。

3. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該隨機存取記憶體模組中的資料完成比對後，更可將比對結果透過該輸出入介面模組回傳至該韌體程式進行授權顯示。

4. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該虛擬隨機亂數為質數時，該隨機公私鑰產生模組係利用該質數產生該公鑰及該私鑰。

5. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該虛擬隨機亂數不具週期性。

6. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該虛擬隨機亂數藉由羅納德·李維斯特、阿迪·薩莫爾和倫納德·阿德曼（RSA）演算法對該授權碼產生該公鑰及該私鑰。

7. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該隨機亂數產生模組包含：

一重置裝置；

一計數控制模組，其係根據啟用該重置裝置時所經過的時脈數以輸出一控制訊號；以及

一線性回饋位移暫存模組，其係根據該控制訊號與該授權碼以連續產生不具週期性之該虛擬隨機亂數。

8. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該處理器係為中央處理器（CPU）或數位訊號處理器（DSP）。

9. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該

嵌入式保護裝置係內建於該處理器中。

10. 如申請專利範圍第 1 項所述之保護軟體內容之嵌入式保護裝置，其中該嵌入式保護裝置係整合於該處理器之匯流排上。

11. 一種保護軟體內容之保護方法，其係包含下列步驟：

根據韌體程式所傳送之授權碼，藉以連續產生一虛擬隨機亂數；

執行一加密流程，其係包含下列步驟：

利用該虛擬隨機亂數對該授權碼產生公鑰及私鑰；

儲存該授權碼及其對應之該虛擬隨機亂數、該私鑰與該公鑰；以及

對該授權碼及其對應之該虛擬隨機亂數、該公鑰及該私鑰進行加密，形成一加密資料後，傳給該韌體程式；以及

執行一授權流程，其係包含下列步驟：

接收該韌體程式傳送之該加密資料，並進行解密，將解碼出來之結果數值與該授權碼及其對應之該虛擬隨機亂數、該公鑰及該私鑰進行比對，以得到一比對結果；以及

藉由該比對結果判斷是否可進行授權，若是，則執行該韌體程式，且重複進行該加密流程；若否，則無法執行該韌體程式。

12. 如申請專利範圍第 11 項所述之保護軟體內容之保護方法，其中該授權流程執行完成之後，更包含一步驟，其係再一次進行該授權流程。

13. 如申請專利範圍第 11 項所述之保護軟體內容之保護方法，其中產生該虛擬隨機亂數之步驟包含下列步驟：

根據重置時所經過的時脈數以輸出一控制訊號；以及

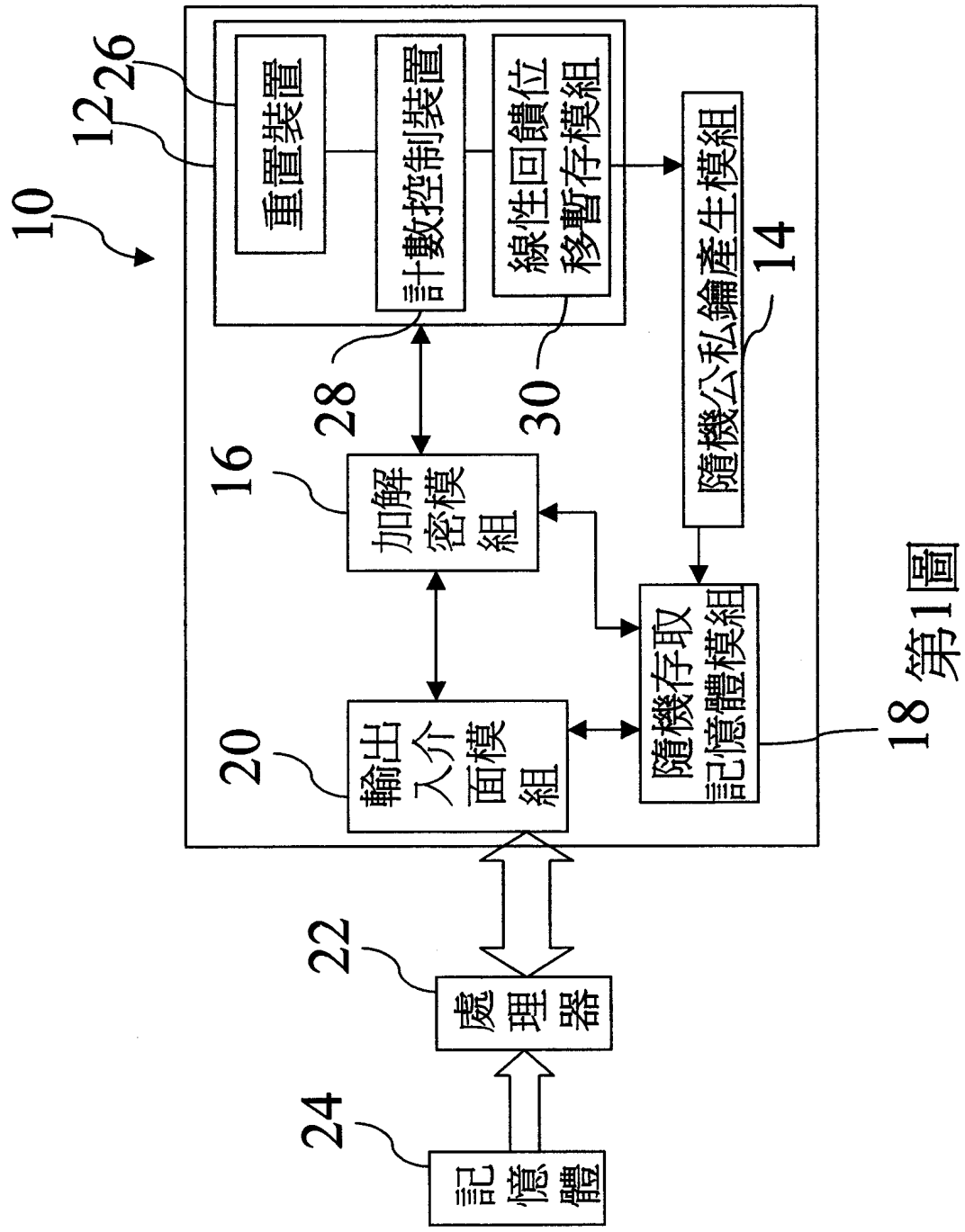
根據該控制訊號與該授權碼以連續產生不具週期性之該虛擬隨機亂數。

14. 如申請專利範圍第 11 項所述之保護軟體內容之保護方法，其中該虛擬隨機亂數為質數時，係利用該質數產生該公鑰及該私鑰。

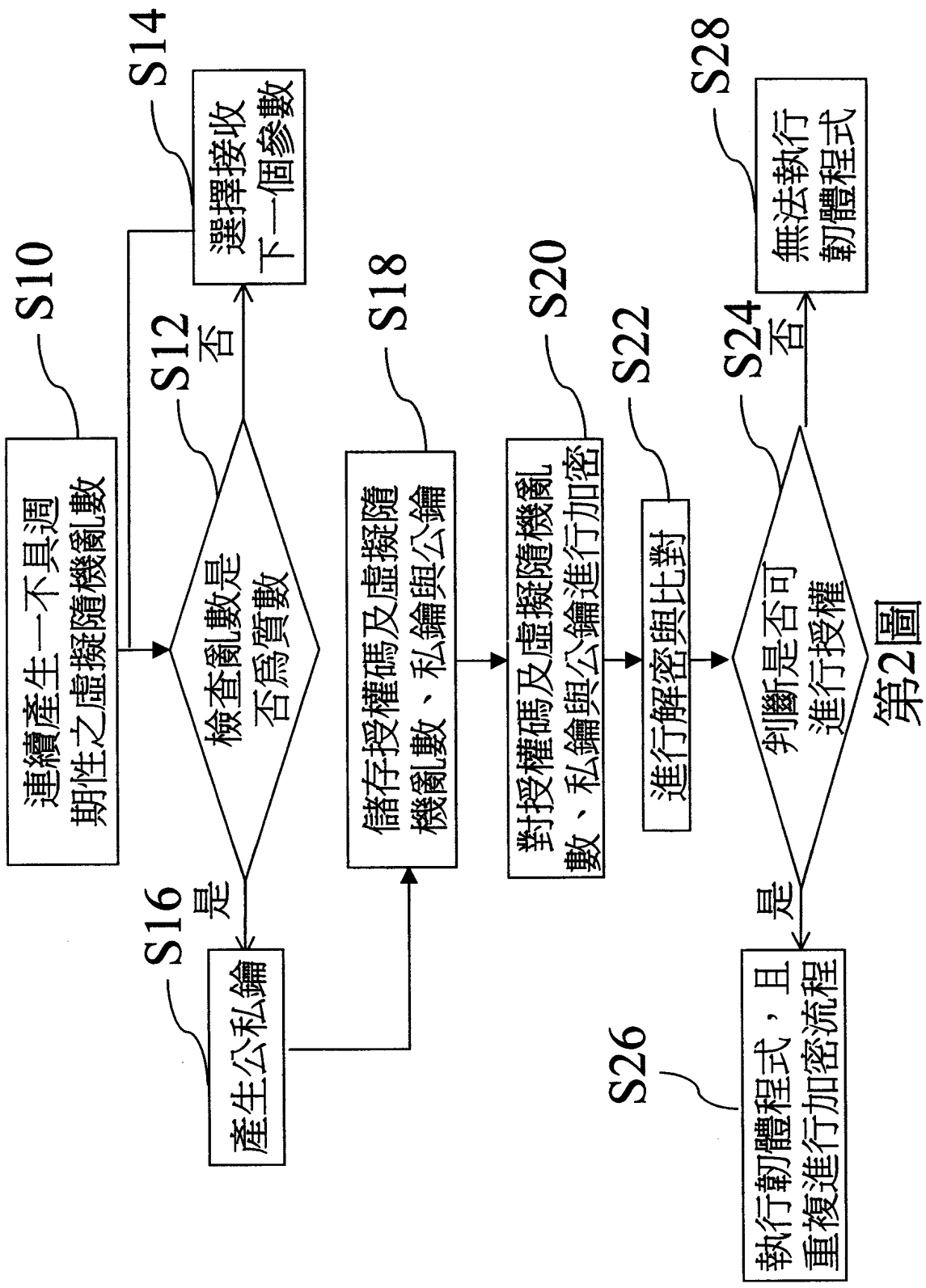
15. 如申請專利範圍第 11 項所述之保護軟體內容之保護方法，其中該虛擬隨機亂數不具週期性。

16. 如申請專利範圍第 11 項所述之保護軟體內容之保護方法，其中該虛擬隨機亂數藉由羅納德·李維斯特、阿迪·薩莫爾和倫納德·阿德曼（RSA）演算法對該授權碼產生該公鑰及該私鑰。

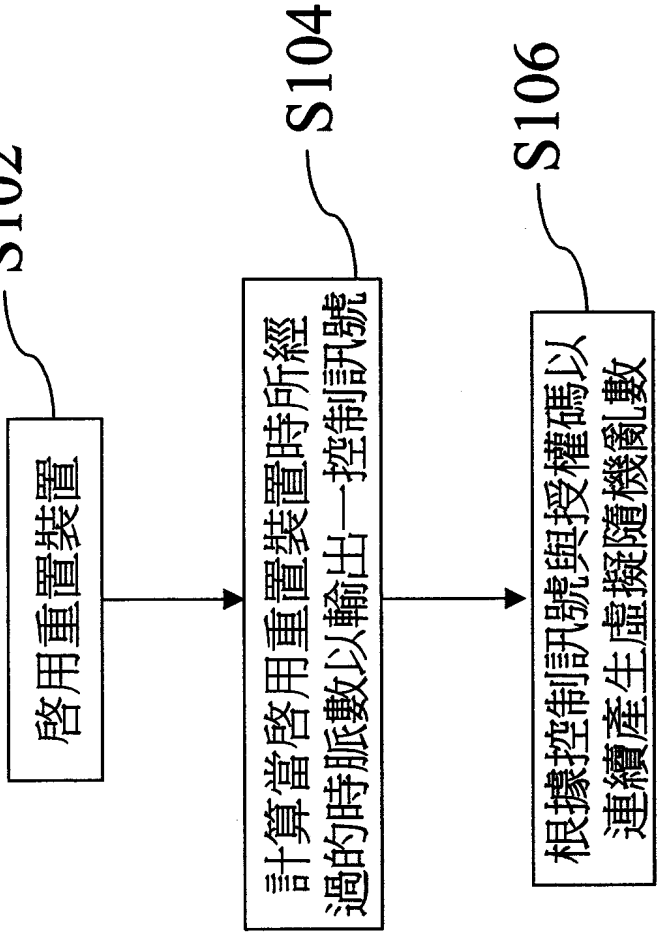
八、圖式：


10
12
26
重置裝置
計數控制裝置
線性回饋位移暫存模組
隨機公私鑰產生模組
14
28
30
16
加解密模組
隨機存取記憶體模組
18
20
輸出入介面模組
22
處理器
24
記憶體

第1圖


S10
連續產生一不具週期性之虛擬隨機亂數
S12
檢查亂數是否爲質數
否
S14
選擇接收下一個參數
是
S16
產生公私鑰
S18
儲存授權碼及虛擬隨機亂數、私鑰與公鑰
S20
對授權碼及虛擬隨機亂數、私鑰與公鑰進行加密
S22
進行解密與比對
S24
判斷是否可進行授權
否
S28
無法執行韌體程式
是
S26
執行韌體程式，且重複進行加密流程

第2圖


S102
啓用重置裝置
S104
計算當啓用重置裝置時所經過的時脈數以輸出一控制訊號
S106
根據控制訊號與授權碼以連續產生虛擬隨機亂數

第3圖