申請日期	89 年 5 月 16 日
案號	89109373
類別	G06F 11/06

（以上各欄由本局填註）

A4
C4

發明 新型 專利說明書 475103

一、發明新型名稱	中文	公眾密碼控制單元及其系統
	英文	Public cryptographic control unit and system therefor
二、發明創作人	姓名	(1) 史蒂芬・史波吉 Sprague, Steven K. (2) 葛雷格利・凱茲默克塞柯 Kazmierczak, Gregory J.
	國籍	(1) 美國　　(2) 美國
	住、居所	(1) 美國麻州里諾克斯瑞瑟維爾路一四七號 147 Reservoir Road, Lenox, MA 12040, U. S. A. (2) 美國新澤西州貝爾麥德雷波道三十六號 36 Labaw Way, Belle Mead, NJ 08502, U. S. A.
三、申請人	姓名（名稱）	(1) 波系統股份有限公司 Wave Systems Corp.
	國籍	(1) 美國
	住、居所（事務所）	(1) 美國麻州李歡喜街四八〇號 480 Pleasant Street, Suite B-200, Lee, MA 01238, U. S. A.
	代表人姓名	(1) 史蒂芬・史波吉 Sprague, Steven K.

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
美國	1999 年 5 月 17 日	09/313,295	☑有主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（１）

發明領域

本發明有關密碼系統，尤其，本發明有關一種鍵碼管理系統及一種共用之公眾密碼控制單元。

發明背景

許多電腦應用需執行一或更多的安全功能，電腦程式之安全功能係該電腦程式之特徵或操作，其係高度阻力於使用者之篡改。

例如，軟體程式會具有屆滿期，在該屆滿期之後該軟體程式呈無法操作。然而，典型之軟體屆滿功能並非安全，因爲其易於藉重設當地電腦時鐘於更早之時間設定，或修飾該軟體而跳越檢查該當地電腦時鐘之部分軟體而予以破解。

例如另一實例，保持接達自當地編密碼之資料庫以用於供當地編密碼之資料庫的計表使用之收費目的之資料記錄的電腦程式典型地具有兩個主要的暫存器，第一暫存器顯示過去資料使用量，而另一暫存器則顯示剩餘之信用量。然而，若更新該使用及信用暫存器並非爲安全功能時，使用者可減少使用暫存器之內容及／或增加信用暫存器之內容來破解該系統。同樣地，保持其本身使用之記錄以用於租用收費目的之租用軟體需要安全功能以防止使用者篡改租用帳目往來暫存器及其他主要之內部暫存器及功能。

例如另一實例，遠距接達資料庫可收費授權之使用者以用於接達於資料庫，安全功能常需鑑認各使用者之身份

五、發明說明（ 2 ）

於給與接達於資料庫之前。再一安全功能係鍵碼管理，亦即，密碼鍵碼分配於授權之使用者。

一種安全功能解決方法係實施安全功能於軟體中具有節省之優點，軟體實施亦具有通用之優點。然而，實施軟體中之軟體安全功能並非如實施安全功能於硬體中一樣地安全，但安全功能的硬體實施會比軟體更費成本且需特殊之硬體以用於各應用。若各應用需其本身特殊之硬體，則安全功能之硬體實施將無法通用。

發明概述

本發明係以一種利用密碼控制單元在多重獨立使用者所共用之系統中當作通用有效之公眾密碼控制單元（密碼單元）的方法及裝置來實施。

該密碼單元含有多用途之電腦處理器，該電腦處理器具有特殊目的之硬體及韌體以准許該密碼單元資源之共用。尤其，該密碼單元含有：具僅讀記憶體（ＲＯＭ）控制程式規劃之專用核心的微處理器中心，多用途之隨機存取記憶體（ＲＡＭ），實時間時鐘及主輸入／輸出界面（亦即，至或自桌上型ＰＣ）。此外，該密碼單元含有ＤＥＳ（資料編密碼標準）發動機，用於密碼鍵碼之安全非揮發儲存器，簽名記錄ＲＡＭ記憶體及特殊目的之存取暫存器。

該密碼單元安裝於諸如桌上型ＰＣ之任何多用途電腦內當作週邊裝置，而使該密碼單元爲〝公眾〞密碼控制單

五、發明說明（ 3 ）

元係其有效於運轉於ＰＣ上之主應用程式而當作安全計算資源。

爲使用密碼單元資源，相對應於安全功能之一部分主應用程式係儲存於ＰＣ之上，此處稱爲安全應用程式（Security applets）之安全功能係饋入及卸載於密碼單元之機載ＲＡＭ之內，在該處會運轉各安全應用程式。類似於下載及運轉於瀏覽器內之爪哇應用程式（Java applets），安全應用程式係易傳，可執行檔而打算將饋入於適合之計算實體內及執行一或更多安全功能。在此方面中，該密碼單元類似於適合運轉安全應用（應用程式）之特殊目的之共處理點。

ＰＣ使安全應用程式饋入於密碼單元之程式控制記憶體之內，該密碼單元會運轉該應用程式及送回安全功能之結果到ＰＣ，然而，不像典型之共處理器，接達於密碼單元並非僅在桌上型ＰＣ之控制下，也就是說，該桌上型ＰＣ可能無法饋入及運轉任一安全應用程式。該密碼單元及該密碼單元爲其一部件之系統會提供其安全內部環境係僅在若干安全應用程式核准饋入及運轉於該密碼單元內部時。

爲保全該計算環境於密碼單元內，配置密碼操作中心（ＯＰＣ）來連絡於密碼單元，尤其當第一次碰到新的安全應用程式時該密碼單元會與ＯＰＣ連絡而在該新的安全應用程式之前則允許該密碼單元運轉於公眾密碼單元中；當第一次安裝新的密碼單元於桌上型ＰＣ時該密碼單元亦

五、發明說明（4）

連絡於ＯＰＣ。該定期週期之基礎上，該密碼單元亦與ＯＰＣ連絡。此外，在分配給定之安全應用程式以用於取得必要之准許供該給定之安全應用程式饋入及運轉於密碼單元中之前，軟體發展器亦連絡於ＯＰＣ。僅當從ＯＰＣ取得所有必要之准許之前將允許給定之安全應用程式饋入及運轉於密碼單元中。

操作系統

密碼單元操作系統（Ｏ／Ｓ）包含兩部分：ＲＯＭ饋入器控制程式，及原有模式安全應用程式，該ＲＯＭ饋入器控制程式係控制程式規劃之小型專用核心，其係儲存於密碼單元之ＲＯＭ中，可藉軟磁碟，ＣＤＲＯＭ或電話數據機分配之原有模式安全應用程式係易傳及可寫入檔而典型地儲存於桌上型ＰＣ之硬碟驅動器中。

主要之安全功能係實施於ＲＯＭ饋入器控制程式中，尤其，該ＲＯＭ饋入器控制程式可控制安全應用程式至及自密碼單元及外部來源之饋入及卸載，含有原有模式安全應用程式之輸入及卸載。

原有模式安全應用程式具有兩個主要功能：一旦第一次使用密碼單元時記錄該密碼單元於ＯＰＣ；以及給予准許以用於第一次使用各個個別應用安全應用程式。通常，該原有模式安全應用程式係使用於無論何時當該密碼單元連絡於ＯＰＣ時。

五、發明說明（ 5 ）

系統操作

在其安全軟體應用中企望使用公眾密碼控制單元之應用發展器必須先提出建議之安全應用程式至ＯＰＣ供考慮用，所建議之安全應用程式必須符合含有安全標準之某些標準，例如所建議之安全應用程式必須足夠小以配裝於密碼單元上之機載ＲＯＭ內，該ＯＰＣ會進一步地檢查所建議之安全應用程式以用於符合安全標準。

在完成所有安全符合測試後，該ＯＰＣ會給予或拒絕准許所建議之安全應用程式來使用密碼單元。准許使用所建議之安全應用程式包含指定序號及密碼之代碼鍵Ｃ於所核准之安全應用程式，該序號及代碼鍵Ｃ係儲存於ＯＰＣ之應用程式記錄中，該發展器在過程中利用該代碼鍵Ｃ來編密碼所核准之安全應用程式，及利用該序號來識別所編密碼之安全應用程式。

當起動桌上型ＰＣ之初始化時，密碼單元ＲＯＭ饋入器控制程式會載入原有模式安全應用程式於密碼單元中之機載ＲＡＭ內，該ＲＯＭ饋入器控制程式處理該原有模式安全應用程式彷彿已先前地從ＯＰＣ給予准許而載入及運轉於該密碼單元中。

該ＲＯＭ饋入器控制程式促成該密碼單元在多重使用者中之共用，尤其，該ＲＯＭ饋入器控制程式會卸載（交換）該原有模式安全應用程式自密碼單元中之機載ＲＡＭ至桌上型ＰＣ之硬碟驅動器內以作成用於饋入（換入）第一應用安全應用程式於該機載ＲＡＭ內之空間。

五、發明說明（ 6 ）

接著，當正饋入第一應用安全應用程式時，ＲＯＭ饋入器控制程式會檢查該第一應用安全應用程式。在確定所饋入之第一應用安全應用程式有資格接達於密碼單元資源時，在該密碼單元中之微處理器會運轉該第一安全應用程式，藉此交付該密碼單元之控制到該第一安全應用程式。

當完成該第一安全應用程式時，該密碼單元以編密碼之形式來卸載（交換）目前所饋入之第一安全應用程式於ＰＣ硬碟驅動器，及饋入（換入）下一個安全應用程式。各安全應用程式之密碼上下文係保存於ＰＣ硬碟驅動器上所儲存之檔案中。以此方式，單一密碼單元可共用於複數之獨立使用者之中。

若碰到未知之應用安全應用程式時（亦即，從未饋入於此特定密碼單元內之安全應用程式），ＲＯＭ饋入器控制程式會換回到原有模式安全應用程式中而建立與ＯＰＣ之安全連絡動作。若寫入該未知之應用安全應用程式的軟體發展器已先前地由ＯＰＣ給予准許來饋入及運轉該安全應用程式時，則該密碼單元將從ＯＰＣ接受所需之密碼鍵碼以解密碼該未知之應用安全應用程式。同時，該ＯＰＣ會記錄密碼單元使用者識別於該應用程式記錄中，藉此結合密碼單元與該ＯＰＣ已給予准許來饋入及運轉之安全應用程式。之後，該密碼單元將饋入及卸載該安全應用程式而不會進一步地與該ＯＰＣ連絡。

最後，當沒有應用安全應用程式運轉時，該ＲＯＭ饋入器控制程式會交換該原有模式安全應用程式回到該密碼

五、發明說明（ 7 ）

單元中之機載ＲＡＭ內，各獨立使用者可利用該密碼單元以用於個別分立之安全應用。因此，使用複數獨立安全應用之複數獨立使用者可共用該密碼單元。

圖式簡單說明

第１圖係根據本發明之公眾密碼系統之方塊圖；

第２圖係根據本發明之公眾密碼控制單元之方塊圖；

第３Ａ圖係流程圖，描繪根據本發明之用於產生編密碼之應用程式的方法及裝置；

第３Ｂ圖係流程圖，描繪根據本發明之用於解密碼所編密碼之應用程式及饋入所解密碼之應用程式於公眾密碼控制單元之機載ＲＡＭ內的方法及裝置；

第４圖係用於儲存編密碼之安全應用程式於ＰＣ硬碟驅動器記憶體中之安全記憶體頁格式之圖示；

第５圖係流程圖，描繪根據本發明在密碼操作中心處安全應用程式之發展器記錄的過程；

第６圖係流程圖，描繪根據本發明在密碼操作中心處安全應用程式之桌上型ＰＣ初始化的過程；

第７圖係流程圖，描繪根據本發明藉Ｏ／Ｓ之ＲＯＭ饋入器控制程式部分之密碼單元初始化的方法；

第８Ａ圖係Ｏ／Ｓ之ＲＯＭ饋入器控制程式部分之流程圖，顯示根據本發明之用於從密碼單元卸載（交換）安全應用程式至ＰＣ的方法；

第８Ｂ圖係Ｏ／Ｓ之ＲＯＭ饋入器控制程式部分之流

五、發明說明（ 8 ）

程圖，顯示根據本發明之用於從ＰＣ饋入（換入）安全應用程式至密碼單元的方法；

第９Ａ圖係方塊圖，描繪根據本發明之用於解密碼及饋入（換入）相對應於來自ＰＣ硬碟驅動器之安全應用程式之密碼上下文到密碼單元ＲＡＭ記憶體的方法及裝置；及

第９Ｂ圖係方塊圖，描繪根據本發明之用於編密碼及卸載（交換）相對應於來自密碼單元ＲＡＭ記憶體之安全應用程式之密碼上下文到ＰＣ硬碟驅動器的方法及裝置。

主要元件對照表

２１，７１６	密碼操作中心（ＯＰＣ）
２２	桌上型ＰＣ
１０	軟體發展器ＰＣ
２０	分配媒體
１２	軟體發展器工具包
１４	安全應用程式
１６	軟體應用
１８	編密碼之
１５	請求
１７，３２Ａ	序號（Ｓ／Ｎ）
１９	代碼鍵Ｃ
２３	應用程式記錄
２６	硬碟驅動器

五、發明說明（9）

28，30，32　編密碼之安全應用程式

24　數據機

34　CPU（中央控制單元）

36　ROM（僅讀記憶體）

38　時鐘

40　RAM（隨機存取記憶體）

25　標準PC匯流排

44　密碼單元

44A　UID（唯一單元實體）

42　輸入／輸出界面

206　微處理器

222，224　RAM記憶體

208　ROM記憶體

224　簽名記錄

218　DES發動機

220　非揮發記憶體

204　經過時間計數器

202　PC界面

210　多用途資料匯流排

212　存取暫存器

216　個別准許位元

214　位址偵測

510，512，514，516，710，712，714　步驟

五、發明說明（10）

322　安全應用程式

320　應用程式序號

304，324，326，328，340　編密碼器

302，306　步驟

316　MAC簽名

310，338　序號

314　編密碼之安全應用程式

336　代碼鍵C

342　比較器

334　及閘

332　解密碼器

610，612，614，616，618，810，812，814，816，818，820，822，830，832，834，836，838，839，840，842　步驟

962A　編密碼之檔

940　第一固定式字串A

956，930　第二固定式字串B

942，914　客戶鍵碼

944，946，948，954，952，915，920，932，920，926　編密碼器

950　安全封包

960　原有模式安全應用程式

五、發明說明（11）

912，918A～918N　密碼上下文

922　解密碼器

924　及閘

928　比較器

發明詳細說明

系統操作

第1圖中所示之公眾密碼系統之方塊圖含有密碼操作中心，OPC21，桌上型PC22，軟體發展器PC10及分配媒體20，該軟體發展器利用軟體發展器工具包12來產生安全應用程式14，該安全應用程式14設計來達成給定之安全功能當作部分之主軟體應用，該軟體發展器經由若干分配媒體20來分配含於所編碼18之安全應用程式14之軟體應用16。

爲編密碼該安全應用程式14，在PC10處之軟體發展器會在諸如連接於OPC21之電話數據機之安全通訊連接上傳送請求15，該請求15含有實際建議之安全應用程式14。響應於該請求15，所建議之安全應用程式14檢查於OPC21處以用於符合安全標準。例如，所建議之安全應用程式14不應企圖接達及輸出禁戒鍵碼，篡改內部經過時間計數器（安全時間時鐘）或設定准許位元（解說於下文中）於密碼單元中而賦予其本身接達敏感區。若所建議之安全應用程式14對於任何理由均不能符合安全標準時，將被拒絕記錄。

五、發明說明（12）

相反地，若ＯＰＣ２１核准安全應用程式１４記錄時，ＯＰＣ２１將選取單一序號（Ｓ／Ｎ）１７及隨意代碼鍵Ｃ１９結合於應用程式１４，該序號１７及代碼鍵Ｃ１９會在例如使用於該請求１５之同一安全電話數據機連接上從ＯＰＣ２１連絡到軟體發展器ＰＣ１０。該ＯＰＣ２１保留所發出之序號（Ｓ／Ｎ）之資料庫及相對應之所發出代碼鍵Ｃ於應用程式記錄２３中。因此，所建議之應用程式會正式地記錄且由ＯＰＣ２１准許由任一公眾密碼控制單元使用（亦即，運轉）。

在ＰＣ１２處之軟體發展器利用所接收之代碼鍵Ｃ於應用程式編碼器１８過程中以用於編密碼所核准之安全應用程式１４；在ＰＣ１２處之軟體發展器尚利用所接收之序號１７於該應用程式解碼器１８過程中以識別所核准之安全應用程式１４，所完成之安全應用程式（利用代碼鍵Ｃ１９編密碼及利用序號１７識別）係置於軟體應用１６中且經由若干分配媒體２０，諸如軟磁碟，ＣＤＲＯＭ，地面廣播，人造衛星，有線電視系統或類似物予以分配至桌上型ＰＣ２２。

在安裝軟體應用１６於桌上型ＰＣ２２之後，所編密碼之安全應用程式係儲存於硬碟驅動器２６中，該硬碟驅動器２６典型地保持相對應於使用於桌上型ＰＣ２２上之複數軟體應用之複數所編密碼之安全應用程式２８，３０，３２，各儲存之應用程式３２含有諸如序號３２Ａ之識別序號（Ｓ／Ｎ）。桌上型ＰＣ２２尚含有標準ＰＣ組件

五、發明說明（13）

，諸如數據機２４，ＣＰＵ３４，ＲＯＭ３６，時間時鐘３８，ＲＡＭ４０及連接於標準ＰＣ匯流排２５上之輸入／輸出界面４２；此外，該桌上型ＰＣ２２含有密碼單元４４，該密碼單元４４具有連接於匯流排２５之唯一單元實體（ＵＩＤ）４４Ａ。

在操作中，當儲存在桌上型ＰＣ２２之軟體應用１６第一次需要執行所編密碼之應用程式時，該桌上型ＰＣ２２會建立與ＯＰＣ２１之安全連絡動作，該桌上型ＰＣ會請求來自ＯＰＣ２１之准許以使用所編密碼之應用程式３２，爲取得准許，該密碼單元２２會傳送其ＵＩＤ４４及安全應用程式３２之序號３２Ａ至ＯＰＣ２１。

該ＯＰＣ２１利用先前所供應之唯一序號１７來對照相對應之隨意供應之代碼鍵Ｃ於應用程式記錄中。同時，該ＯＰＣ１２藉添加於應用程式記錄２３而輸入交易（由密碼單元４４之序號３２Ａ的使用。該應用程式記錄２３係所有記錄之安全應用程式序號，相對應於各序號之代碼鍵Ｃ，及已賦予准許來運轉各相對應之安全應用程式之所有密碼單元ＵＩＤ之記錄，例如該記錄２３顯示相對應於密碼代碼鍵Ｃ＝Ｚ之所編密碼應用程式Ｓ／Ｎ　３２Ａ之記錄２３已予以記錄，且該密碼單元ＵＩＤ＝４４Ａ已准許解密碼及執行（運轉）具有序號＝３２Ａ之所記錄的應用程式。

公眾密碼控制單元

五、發明說明（14）

在第2圖中之公眾密碼控制單元44包含微處理器206，RAM記憶體222，224及ROM記憶體208，該RAM記憶體係配置儲存簽名記錄224及主要密碼程式控制222區，該ROM208含有O／S之饋入器控制程式部；同時，包含於該密碼單元44中係DES發動機218，非揮發記憶體220，經過時間（實時間）計數器204及存取控制暫存器212。主（桌上型）PC界面202係配置供密碼單元44與主PC間之連絡。在密碼單元44內之連絡係配置於載運位址及資料於密碼單元44內之組件間的多用途資料匯流排210之上。

DES發動機218促成該密碼單元44之保護環境內之密碼操作，例如內部非揮發記憶體220會提供密碼鍵碼之安全儲存；經過時間計數器204准許防篡改時間及日期計算於該密碼單元44之安全環境內。諸如讀取或寫入於經過時間計數器204，存取或改變非揮發記憶體220中之鍵碼儲存內容，存取或改變簽名記錄224內容之主要操作係藉硬體予以限制，尤其，接達該密碼單元係藉設定該存取暫存器212之個別准許位元216（解說於下文中）來控制。

存取暫存器212含有特殊之保護特性以預防饋入於程式控制RAM222中之安全應用程式協調於密碼單元44之安全特性。特別地，存取暫存器212含有准許暫存器，而該存取暫存器212之個別准許位元216會界

五、發明說明（15）

定那一個資源將允許所給定之安全應用程式來接達，例如固線式信號（核准控制）２２６會就是否將允許饋入於ＲＡＭ２２２中之所給定的安全應用程式接達所有或部分之簽名記錄２２４，經過時間計數器２０４，以及客戶鍵碼及安全鍵碼儲存區域２２０而言來提固線式限制。秘密之客戶鍵碼係唯一於各密碼單元，且與其他密碼鍵碼在製造時儲存於非揮發記憶體２２０之中。

僅當從存取暫存器２１２賦予准許時，方允許ＲＡＭ２２２中之所給定的安全應用程式來接達（讀取或寫入）主要操作。准許暫存器係藉饋入器控制ＲＯＭ２０８程式而饋入自解密碼之安全應用程式。例如進一步之預防措施以阻止未授權之接達，准許暫存器２１６可僅接達自饋入器控制ＲＯＭ２０８中之指令執行。無論何時當准許暫存器係寫入有新值時會執行位址偵測２１４，尤其，僅當位址偵測２１４指示饋入器控制ＲＯＭ正執行准許位元饋入時，來自該位址偵測２１４之寫入致能信號將活化。在此方式中，該准許暫存器２１６僅可藉來自饋入器控制ＲＯＭ２０８之適當的指令順序予以饋入，因此，在ＲＡＭ２２２之外運轉之安全應用程式不會改變准許暫存器２１６之准許位元。

存取暫存器之准許位元

存取暫存器２１２之個別准許位元提供控制於非揮發記憶體２２０中儲存之客戶鍵碼及安全鍵碼。特別地，一

五、發明說明（16）

准許位元會確定是否應用程式具有接達來讀取（但非寫入）該客戶鍵碼，該客戶鍵碼係工廠安裝且無法改變，該客戶鍵碼可使用於有關任一軟體發展器之安全應用程式的密碼計算中。

儲存在非揮發記憶體２２０中之其他鍵碼含有私用鍵碼以用於特定之軟體發展器，也就是說，給定之軟體發展器無法使用共用之客戶鍵碼。替代性地，私用鍵碼可專用於此給定之軟體發展器。在此例中，相對應於專用之私用鍵碼的准許位元會准許來自所給定軟體發展器之安全應用程式接達專用之私用鍵碼，來自其他軟體發展器之安全應用程式將不能設定此專用之私用鍵碼的准許位元且因此將不具有到該專用之私用鍵碼的接達。此外，存取暫存器２１２之其他准許位元２１６會界定是否所饋入之安全應用程式可寫入新的專用之私用鍵碼於非揮發記憶體２２０之舊的專用之私用密碼之上。除了專用之私用鍵碼之外，非揮發記憶體２２０可儲存數位證明以使用於鑑認公眾私用鍵碼配對之公眾鍵碼部分。

該存取暫存器２１２之個別准許位元２１６係結合ＲＡＭ之簽名記錄部２２４使用而提供有關那些安全應用程式可饋入及卸載於密碼單元內之進一步的接達控制，尤其，設定取消旗標於簽名記錄中之所選取登錄中將取消所選取之安全應用程式，密碼晶片將因而不饋入或卸載該簽名記錄中之取消旗標所指定之安全應用程式。最後，該ＯＰＣ可藉設定使該密碼單元４４不活化之適當准許位元

五、發明說明（17）

216使整個密碼單元不活化。不活化之密碼單元44無法運轉任一安全應用程式，除非密碼單元44藉OPC而再活化。

安全應用程式記錄

如所述，應用發展器會設計安全應用程式來作爲部分之主應用程式，該安全應用程式係特定地寫入以運轉於密碼單元44之上，該安全應用程式必須足夠地小型以便配裝於密碼單元之機載RAM（第2圖中之222）中。可畫分太大以致無法配裝於該機載RAM內之安全應用爲兩部分，亦即，畫分爲兩個安全應用程式。在安全應用程式可分配於主應用程式及運轉於密碼單元上之前，該發展器必須記錄安全應用程式於OPC。如所述，發展器會建立與OPC之安全連絡動作，適用於與OPC安全連絡之系統係顯示於美國專利第5615264，5761283及5764762號中。

第5圖顯示OPC處之發展器記錄過程。在步驟510處，OPC接收請求以用於安全應用程式記錄，該請求含有實際建議之安全應用程式；在步驟512處，OPC檢查所建議之安全應用程式以用於適合之密碼標準，例如所建議之安全應用程式無法意圖發現唯一於各個個別密碼單元之客戶鍵碼或任何其他安全鍵碼。在該處無法輸出代碼或輸入額外代碼。例如索引之程式迴路之間接程式跳越係安全性之危機。從系統安全性上之發作經驗的結

五、發明說明（18）

果，許多測試可設計來確保所建議之安全應用程式係安全的及適當設計的。若所建議之安全應用程式無法通過任一測試時，則在步驟５１２處該ＯＰＣ會拒絕記錄所建議之安全應用程式。

若通過所有測試時，則在步驟５１４處，ＯＰＣ會選取序號Ｓ／Ｎ及密碼代碼鍵Ｃ，同時該ＯＰＣ會在步驟５１４處輸入該序號及代碼鍵Ｃ於應用程式記錄（第１圖中２３）中，該記錄過程係在步驟５１６處藉傳送新記錄之應用程式的序號及代碼鍵Ｃ到軟體發展器而完成。

所使用之密碼規定

第３Ａ，３Ｂ，９Ａ及９Ｂ圖顯示代表密碼操作之符號。如此處所使用者，用於編密碼及解密碼之較佳方法係資料編密碼標準（ＤＥＳ）。

簡言之，用於ＤＥＳ之電子代碼鍵模式，６４位元（８位元組）之輸入方塊係根據５６位元鍵碼而轉換爲６４位元之輸出方塊。用於解密碼係執行反向過程，利用同一５６位元鍵碼來轉換６４輸入位元爲６４輸出位元。ＤＥＳ鍵碼係典型地以６４位元，８位元組數量來表示，具備有各位元組含７個位元加上一配類位元，或５６位元加上８個配類位。

如此處所使用的，在秘密鍵碼裝置之下執行密碼操作於變數上而利用該秘密鍵碼來編碼密（或解密碼）該變數（通常爲鍵碼）以產生另一鍵碼。編密碼可執行於單一鍵

五、發明說明（19）

碼之下，或在諸如三重鍵碼組之多重鍵碼之下。除非另有指示，否則編密碼或解密碼將意指ＤＥＳ編密碼或解密碼在三重鍵碼組之下。用於三重鍵碼編密碼，係使用三鍵碼（鍵碼１，鍵碼２，鍵碼３）之鍵碼組利用ＤＥＳ來編密碼變數如下：以鍵碼１編密碼，以鍵碼２解密碼，及以鍵碼３編密碼；三重鍵碼解密碼係反向的，以鍵碼３來解密碼，以鍵碼２來編密碼，及接著以鍵碼來解密碼。ＣＢＣ將意指利用初始向量之ＤＥＳ標準的密碼方塊成鏈模式Ⅳ，除非另有所述，否則，用於ＣＢＣ　ＤＥＳ編密碼或解密碼之Ⅳ將爲零。

密碼單元初始化及記錄

第７圖描繪藉ＲＯＭ饋入器控制器之密碼單元初始化及記錄之方法。當開機時，ＲＯＭ饋入器控制程式（第２圖之ＲＯＭ２０８中）會在步驟７１０處從硬碟驅動器（第１圖中之２６）饋入初始原有模式安全應用程式至機載ＲＡＭ（第２圖中之２２２）之內，該ＲＯＭ饋入器控制程式認爲該初始原有模式安全應用程式爲預核准且編密碼有固定鍵碼，該初始原有模式安全應用程式係藉致能該存取暫存器２１６之所有准許位元來賦予接達於該密碼單元之整個資源。在饋入之後，傳遞該密碼單元之控制到已饋入於機載ＲＡＭ內之初始原有模式安全應用模式。

若此爲第一次使用該密碼單元時，則在步驟７１２處初始化該記錄過程，與該ＯＰＣ之安全連絡動作係建立於

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 20）

步驟７１４處，以及該密碼單元進入與ＯＰＣ７１６之記錄過程，記錄包含輸入識別使用者之資料（名稱，位址，等）及運送相結合於該密碼單元之ＵＩＤ的使用者資料到ＯＰＣ。在步驟７１４處與ＯＰＣ７１６之連絡動作期間，該ＯＰＣ７１６有機會來下載任何程式改變以更新初始原有模式安全應用程式。在完成記錄過程之後，送回程式控制至桌上型ＰＣ；該密碼單元接著進入等待狀態直到該桌上型ＰＣ準備饋入第一安全應用程式於將運轉之密碼單元中。

記錄之安全應用程式的編密碼

已編密碼安全應用程式，第３Ａ圖係用於安全應用程式編密碼之編密碼鍵碼組的流程圖，該軟體發展器開始於所希求之安全應用程式３２２。如上述，該安全應用程式３２２已先前地藉軟體發展器而傳送至ＯＰＣ，且應用程式序號３２０及代碼鍵Ｃ已先前地接收爲部分之該應用程式記錄過程。

該軟體發展器選取其本身選擇於步驟３０２處之代碼鍵Ａ（程式規劃者鍵碼），接著在代碼鍵Ｃ之下編密碼代碼鍵Ａ於編密碼器３０４中以形成編密碼之代碼鍵Ａ´。安全應用程式３２２係在代碼鍵Ａ之下編密碼於編密碼器３２４中之三重鍵碼ＣＢＣ，信息鑑認代碼（ＭＡＣ）係計算於編碼器３２６中，ＭＡＣ（亦熟知爲調處偵測代碼）係附加於編密碼封包之數位式簽名，其係藉所編密碼之

五、發明說明（21）

封包的接收器所檢查以確認所編密碼之封包的內容已改變。該ＭＡＣ係在步驟３０６處藉組合序號３２０，代碼鍵Ａ´，及來自編密碼器３２４之輸出之所編密碼的安全應用程式於安全封包內而產生。

組合安全封包３０６之目的在於產生ＭＡＣ３１６於編密碼器３２６中且附加其於安全封包而形成安全頁。發展器ＭＡＣ鍵碼係在代碼鍵Ｃ３１８之下藉編密碼序號３２０而形成於編密碼器３２８中。ＭＡＣ簽名本身係藉編密碼３２６於安全封包３０６上之三重鍵碼ＣＢＣ而產生。尤其，編密碼器３２６之輸出的最後部分會形成附加於安全封包３０６之ＭＡＣ簽名３１６。

所計算之ＭＡＣ係與安全封包３０６結合而形成輸出自密碼單元及最後儲存於主ＰＣ之硬碟驅動器２６中之安全頁３０８。

用於儲存所編密碼之安全應用程式於ＰＣ硬碟驅動器記憶體中之安全記憶體頁的格式係顯示於第４圖中，該安全記憶體頁開始於安全封包（由所編密碼之安全應用程式３１４所跟隨之代碼鍵Ａ´　３１２所跟隨之序號３１０）及終止於所計算之ＭＡＣ３１６。

安全應用程式之初始饋入及解密碼

密碼單元解密碼初始所碰到之編密碼的安全應用程式，如第３Ｂ圖之編密碼鍵碼組流程圖中所示，因爲此係初始饋入以前從未運轉之安全應用程式，所以將無法在

五、發明說明（ 22）

ＲＡＭ２２４之應用程式簽名記錄部之序號３１０。（若其中序號係發現於簽名記錄２２４中，則所編密碼之應用程式已在以前運轉過，且將可應用第９Ａ圖）。如先前所述，用於初始所碰到之安全應用程式，該原有模式安全應用程式已傳送該序號３３８至該ＯＰＣ，及接收代碼鍵Ｃ３３６自該ＯＰＣ。

首先，在代碼鍵Ｃ３３６之下藉解密碼代碼鍵Ａ´３１２於解密碼器３３０來恢復軟體開發器代碼鍵Ａ，所編密碼之安全應用程式３１４係在來自解密碼器３３０輸出之所恢復的代碼鍵Ａ之下解密碼於解密碼器３３２中之三重鍵碼ＣＢＣ。用於安全封包之ＭＡＣ（序號３１０，代碼鍵Ａ´ ３１２及所編密碼之安全應用程式３１４）係在發展器ＭＡＣ鍵碼之下計算於三重鍵碼ＣＢＣ編密碼器３４０之中，該發展器ＭＡＣ鍵碼係在代碼鍵Ｃ３３６之下藉編密碼序號３３８而計算於編密碼器３４８之中，該發展器ＭＡＣ鍵碼係耦合於編密碼器３４０之鍵碼輸入。

在編密碼器３４０之輸出處所計算之ＭＡＣ與所接收之ＭＡＣ３１６比較於比較器３４２之中，若所計算之ＭＡＣ與所接收之ＭＡＣ相等３４４時，則致能及閘（AND gate）３３４，且儲存在解密碼器３３２之輸出處之所編密碼之安全應用程式於機載ＲＡＭ之密碼控制部２２２中。然而，若所計算之ＭＡＣ與所接收之ＭＡＣ不相等３４６時，則將不允許安全應用程式饋入於機載

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 23）

ＲＡＭ２２２之內及運轉。取代地，並不致能及閘且不儲存在解編碼器３３２之輸出處所編密碼之安全應用程式於機載ＲＡＭ之密碼控制部２２２中。誤差信息則送回桌上型ＰＣ。

在安全應用程式饋入上之ＯＰＣ控制

本系統給與ＯＰＣ控制於是否安全應用程式可饋入於所給定之密碼單元中。第６圖描繪ＯＰＣ處之初始饋入控制過程。在步驟６１０於ＯＰＣ處接收來自桌上型ＰＣ之序號後，ＯＰＣ會在步驟６１２處檢查是否該應用程式具有有效之序號，若不具有時，則ＯＰＣ會送回該安全應用程式爲〝無效〞之誤差信息；若有效時，則ＯＰＣ會在步驟６１４處檢查是否序號已取消，若取消時，ＯＰＣ會送回該安全應用程式已〝取消〞之誤差信息。該ＯＰＣ檢查是否由其ＵＩＤ所識別之所給定的密碼單元允許饋入此特定之安全應用程式，若不允許時，則ＯＰＣ會送回〝不准〞該安全應用程式之饋入的誤差信息；若序號有效，未取消，且該密碼單元係允許饋入該安全應用程式時，則在步驟６１８處對照代碼鍵Ｃ於ＯＰＣ處之應用程式記錄中且送回該代碼鍵Ｃ至密碼單元。

在此方式中，ＯＰＣ會維持控制於初始之安全應用程式安裝之上，例如若安全應用程式已重寫入以修正問題時，ＯＰＣ將不允許隨後之使用者安裝較早之版本於該密碼單元之內，若知悉所給定之密碼單元ＵＩＤ被協調時，則

五、發明說明（ 24）

將不允許進一步之安全應用程式饋入供該密碼單元ＵＩＤ用。

ＲＯＭ饋入器控制Ｏ／Ｓ－密碼上下文交換

密碼單元之ＲＯＭ饋入器控制程式（Ｏ／Ｓ）支持多重同時之使用者。爲切換於使用者之中，目前之安全應用程式之密碼上下文從密碼單元卸載及儲存於桌上型ＰＣ之硬碟驅動器之中；接著，藉檢索來自桌上型ＰＣ之硬碟驅動器之先前所運轉之安全應用程式的先前所儲存密碼上下文，該密碼單元恢復至相對應於此先前所運轉安全應用程式之先前密碼狀態。例如此處所使用者，該等名辭〝編密碼之安全應用程式〞，〝密碼上下文〞及〝在其密碼上下文中（具有或含有）之編密碼的安全應用程式〞均意圖爲實際等效之名辭。

於本實施例中，軟體發展器建構該安全應用程式而在密碼程式存在之前儲存密碼參數於機載ＲＡＭ之密碼程式控制部２２２（第２圖）中，該軟體發展器預期安全參數需用於其安全應用且將需恢復該密碼單元至其先前之密碼狀態及持續該安全應用。

在若干安全應用中，該密碼單元之所有密碼參數將需再儲存該密碼單元。在其他安全應用中，將僅需一子集之密碼參數。在替換性之實施例中，該密碼單元會自動儲存其本身（密碼單元）之整個密碼狀態於相關各安全應用程式之個別檔之中。在後者之情況中，切換密碼狀態之負荷

五、發明說明（ 25）

（儲存及恢復密碼上下文）係藉密碼單元之操作而自動地執行，且不會受到發展器軟體所干預。

在本實施例中，用於所給定之安全應用程式之密碼上下文檔含有安全應用程式加上該密碼單元之密碼狀態，該密碼上下文之格式係給定如下：

第Ｉ表－密碼上下文（２９Ｋ）

明碼標題：
序號（Ｓ／Ｎ），大小，

修訂＃，時間標示

程式資料－安全應用程式

持續暫存器儲存

堆積（暫時儲存）

堆疊

ＭＡＣ／簽名

除了明碼標題之外，編密碼該密碼上下文，該明碼標題包含下列欄：

序號（Ｓ／Ｎ）：該序號係在記錄過程期間發出至軟體發展器供安全應用程式用之序號。

大小：相對應於將卸載自密碼單元及儲存於硬碟驅動器中之密碼上下文中之位元組數目。

修正＃：使用於追踪對於原來記錄之安全應用程式的改變。

五、發明說明（26）

時間標示：相對應於當卸載時之密碼單元實時間時鐘的內容。

密碼上下文所編密碼部分包含下列欄：

程式資料：含有在程式執行期間所作成任何修飾之安全應用程式。

堆積（暫時儲存）：表示方才在卸載之前之密碼單元之密碼狀態的參數。

堆疊：諸如用於所隱蔽之次常式的返回位址之程式堆疊儲存。

ＭＡＣ／簽名：在整個密碼上下文之上所計算的ＭＡＣ。

第Ⅱ表－簽名記錄

機載ＲＡＭ之簽名記錄２２４具有下列格式：

序號（Ｓ／Ｎ）	ＭＡＣ（簽名）	旗標
序號　1	ＭＡＣ　1	旗標　1
序號　2	ＭＡＣ　2	旗標　2
－－－	－－－	－－－
序號　３１	ＭＡＣ　３１	旗標　3

Ｓ／Ｎ：應用程式之序號

ＭＡＣ：用於ＰＣ硬碟驅動器中所儲存之應用程式密碼上下文之信息鑑認碼。

旗標：儲存於簽名記錄中之旗標含有應用程式取消旗

五、發明說明（27）

標，其係由ＯＰＣ設定以防止任何進一步地使用所取消之應用程式。

第８Ａ圖ＲＯＭ饋入器控制Ｏ／Ｓ－交換

ＲＯＭ饋入器控制程式（Ｏ／Ｓ）之交換部分的流程圖係顯示於第８Ａ圖中，該操作系統之交換部分的功能在於卸載含有其密碼上下文之目前運轉於密碼單元中之安全應用程式到桌上型ＰＣ之硬碟驅動器，例如該安全應用程式可具有內部暫存器儲存器，堆疊指標器，及其他程式參數，其係修正於密碼上下文之執行及建構部分。

在第８Ａ圖中，當目前之安全應用程式完成於步驟８１０時，該密碼單元之密碼狀態係在步驟８１２儲存於機載ＲＡＭ中，所儲存之密碼狀態含有ＤＥＳ發動機（第２圖中之２１８）的狀態及任何其他恢復該密碼單元至其目前條件所需之變數，接著編密碼該ＲＡＭ內容於步驟８１４處（根據第９Ｂ圖中所示之編密碼鍵碼組），用於含有明確標題及序號之編密碼ＲＡＭ內容的ＭＡＣ則計算於步驟８１６處，以及在步驟８１８處儲存該ＭＡＣ於ＲＡＭ簽名記錄２２４中，安全頁係組合於步驟８２０處及在步驟８２２處儲存於桌上型ＰＣ之硬碟驅動器之上。

第８Ｂ圖饋入器控制Ｏ／Ｓ－換入

ＲＯＭ饋入器控制程式（Ｏ／Ｓ）之換入部分的流程圖係顯示於第８Ｂ圖中，該操作系統之此部分的功能在於

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（28）

若有的話，從桌上型ＰＣ之硬碟驅動器饋入含有恢復其個別之先前密碼上下文之下一個安全應用程式於機載ＲＡＭ以運轉於密碼單元中。

在第８Ｂ圖中，當饋入安全應用程式於機載ＲＡＭ內之時，ＲＯＭ饋入器控制程式會先在步驟８３０處檢查是否該序號在ＲＡＭ之簽名記錄部（第２圖中之２２４）中，在該簽名記錄部２２４中之序號的存在與否將確定是否此密碼單元已在以往運轉過此特定之安全應用程式。

若應用程式序號並不在該記錄中之時，則該密碼單元尚未運轉過此特定之安全應用程式，接著在步驟８３４處該程式檢查以確定是否該簽名記錄已滿或是否具有空間供額外之登錄。若該簽名記錄已滿，則送回〝記錄已滿〞之誤差信息；若該簽名記錄並未滿時，則在步驟８３８處該ＲＯＭ饋入器控制程式會以原有模式安全應用程式來交換而建立與ＯＰＣ之安全連絡，如上文根據第６圖所述。

如結合於第６圖之上文所述，該原有模式安全應用程式傳送所建議之安全應用程式之序號到ＯＰＣ於步驟８３８且取得代碼鍵Ｃ於步驟８３９。同時，如上所述，該密碼單元利用所接收之代碼鍵Ｃ以解密碼所建議之安全應用程式及計算該ＭＡＣ以用於安全應用程式於步驟８３７。用於首次饋入於所給定之密碼單元之安全應用程式之解密碼鍵碼組已結合於第３Ｂ圖描繪於上文。

若密碼單元已在以前運轉過此特定之安全應用程式，則在步驟８３０處將會發現該序號在記錄中。在此例中，

五、發明說明（29）

ＭＡＣ係在步驟８３２處檢索自ＲＡＭ之簽名記錄部（第２圖中之２２４）。該安全應用程式係解密碼（以其密碼上下文）及該ＭＡＣ係計算於步驟８３６中。用於解密碼所儲存之應用程式及計算該ＭＡＣ之鍵碼組將結合第９Ａ圖描述於下文。

在過程中之此交換步驟處，具有3個相結合於安全應用程式（以其密碼上下文）而ＲＯＭ饋入器控制程式（Ｏ／Ｓ）正意圖饋入於該密碼單元之機載ＲＡＭ內的ＭＡＣｓ，第一ＭＡＣ檢索自簽名記錄，第二ＭＡＣ與所儲存之密碼上下文接收自桌上型ＰＣ以及第三ＭＡＣ計算於輸入之編密碼安全程式上。若在步驟８４０處所有3個ＭＡＣｓ均彼此相等時，則解密碼之安全應用程式會饋入於ＲＡＭ之密碼程式控制部，且會在步驟８４２處開始安全應用程式的執行。否則〝接達拒絕〞之誤差信息會自步驟８４０回到ＰＣ。

密碼上下文檔

第９Ａ圖（換入）及第９Ｂ圖（交換）顯示個別之解密碼及編密碼鍵碼組以用於交換安全應用程式（在個別之密碼上下文中）於ＲＡＭ之密碼程式控制部２２２與桌上型ＰＣ之硬碟驅動器２６之間。特別地，第９Ａ圖係方塊圖，描繪用於解密碼及饋入（換入）相對應於來自ＰＣ硬碟驅動器之安全應用程式的密碼上下文於密碼單元ＲＡＭ記憶體之方法及裝置；第９圖係方塊圖，描繪用於編密碼

五、發明說明（30）

及卸載（交換）相對應於來自密碼單元ＲＡＭ記憶體之安全應用程式的密碼上下文於ＰＣ硬碟驅動器。

密碼上下文交換－第９Ｂ圖

在第９Ｂ圖中，ＲＡＭ２２２之密碼程式控制程的內容係卸載爲硬碟驅動器２６中之編密碼檔９６２Ａ，ＲＡＭ記憶體之簽名記錄部２２４並不卸載，所產生之種種編密碼鍵碼係根據第一固定式字串Ａ９４０，第二固定式字串Ｂ９５６及稱爲客戶鍵碼９４２之初密鍵碼，該客戶鍵碼９４２係儲存於可程式規劃記憶體（第２圖中之２２０）中，該客戶鍵碼記憶體９４２典型地係非揮發的，且可藉諸如可熔斷連接線，ＥＥＰＲＯＭ，電池後備ＲＡＭ及類似物之任何適合的非揮發記憶體來實施。所儲存之客戶鍵碼９４２係唯一於各密碼單元且安裝於製造時。

第一固定式字串Ａ９４０係在客戶鍵碼９４２之下編密碼於編密碼器９４４中，編密碼器９４４之輸出係在編密碼器９４６中使用作鍵碼以編密碼將卸載之應用程式之序號（明確）；編密碼器９４６之輸出係使用作鍵碼以編密碼該安全應用程式於３鍵碼ＣＢＣ編密碼器９４８。應注意的是，用於安全應用程式交換之編密碼鍵碼（至編密碼器９４８）並不相同於安全應用程式之初始饋入所使用之鍵碼。用於安全應用程式之初始饋入，所使用之鍵碼係發展器代碼鍵Ａ。在第９Ｂ圖中，使用於卸載之鍵碼係固

五、發明說明（31）

定式字串A940，序號及客戶鍵碼942之函數。因爲各客戶鍵碼係唯一於各密碼單元，故儲存於硬碟驅動器26中之所交換的密碼上下文不可交換到另一密碼單元之內，也就是說，一旦安全封包已利用一客戶鍵碼交換到硬碟驅動器26時，則所交換之安全封包（在其密碼上下文中）無法饋入於具有不同客戶鍵碼之不同密碼單元內。

爲產生用於密碼上下文（其含有安全應用程式）之MAC，組合安全封包950，該安全封包950包含序號於明碼及編密碼之安全應用程式中（具其密碼之上下文）。該MAC係在產生自編密碼器954之輸出的鍵碼之下藉編密碼該安全封包之3鍵碼CBC所產生。例如從第9B圖可理解的是，從編密碼器954所輸出之MAC鍵碼係固定式字串B956，（及經由編密碼器944及946）序號，客戶鍵碼942及固定式字串A940之函數。

特別地，編密碼器946之輸出係輸入作爲到編密碼器954之編密碼鍵碼，該編密碼器954編密碼固定式字串B作爲到3鍵碼CBC編密碼器952之MAC鍵碼，在編密碼器952之輸出處的MAC與安全封包組合而形成安全頁958，該安全頁958儲存於硬碟驅動器26中之962A且與其他密碼上下文962N及所交換之原有模式安全應用程式960一起在硬碟驅動器26中。

五、發明說明（32）

密碼上下文換入－第９Ａ圖

當密碼單元切換於多重同時之安全應用之間時，在第９Ａ圖中先前所儲存之密碼上下文９１２，９１８Ａ－９１８Ｎ從硬碟驅動器２６饋入於機載ＲＡＭ之密碼程式控制部２２２，該密碼單元利用簽名記錄２２４之內容來確定是否各先前所儲存之密碼上下文９１２，９１８Ａ至９１８Ｎ將允許饋入及運轉，該密碼上下文９１２中之原有模式安全應用程式係以相同於密碼單元所運轉之其他多重同時之安全應用程式９１８Ａ至９１８Ｎ的方式換入及換出該密碼單元。

第９Ａ圖（換入）之鍵碼組執行反向於第９Ｂ圖（交換）之鍵碼組的密碼過程，尤其，固定式字串Ａ９１０係在客戶鍵碼９１４之下編密碼於編密碼器９１６之中，編密碼器９１６之輸出係使用爲編密碼器９２０中之鍵碼而編密碼將饋入之安全應用程式之序號及密碼上下文９１８Ａ，編密碼器９２０之輸出係使用爲應用程式解密碼鍵碼而解密碼安全應用程式密碼上下文於３鍵碼ＣＢＣ解密碼器９２２中，用於安全應用程式換入之應用程式解密碼鍵碼（至解密碼器９２２）係相同於交換期間使用來編密碼該安全應用程式之鍵碼。

用於密碼上下文９１８Ａ之ＭＡＣ鍵碼係在應用程式解密碼鍵碼（編密碼器９２０之輸出）之下藉首先編密碼固定式字串Ｂ９３０而計算於編密碼器９３２之中，接著使用編密碼器９３２之輸出作爲編密碼器９２６中之鍵碼

五、發明說明（33）

而形成計算之ＭＡＣ於密碼上下文９１８Ａ之安全頁部分之上；爲檢查該ＭＡＣ，檢索來自ＲＡＭ之簽名記錄部２２４之所儲存的ＭＡＣ，接著，所有三個之來自編密碼器９２６之所計算的ＭＡＣ，來自簽名記錄２２４之所儲存的ＭＡＣ及來自密碼上下文９１８Ａ之所接收之ＭＡＣ係比較於比較器９２８中，若所有三個ＭＡＣ均相等於步驟９３４時，則使ＡＮＤ閘（及閘）９２４能饋入所接收之安全應用程式至ＲＡＭ之密碼程式控制部２２２之內；若在步驟９３６處，該三個ＭＡＣｓ之任一並不相等於其他者之時，則使該及閘９２４不能饋入所接收之安全應用程式至ＲＡＭ之密碼程式控制部２２２之內。

安全應用程式交換

安全應用程式可藉單回或雙回過程而換入於密碼單元內，雙回過程已描述於上文，也就是說，該ＲＯＭ饋入器控制程式會在所編密碼之安全應用程式饋入於機載ＲＡＭ之密碼程式控制部之前檢查該編密碼之安全應用程式。在雙回實施中，若通過所有ＭＡＣ簽名測試時，則解密碼該安全應用程式且饋入其於第二回中之機載ＲＡＭ；若在第一回之上不允許饋入時，則在第二回之上並沒有該安全應用程式將饋入於機載ＲＡＭ之內。

在單回實施中，ＲＯＭ饋入器控制程式會檢查所編密碼之安全應用程式而同時地解密碼及饋入所解密碼之安全應用程式於機載ＲＡＭ之密碼程式控制部之內，若ＭＡＣ

五、發明說明（ 34）

簽名測試失敗時（第８Ｂ圖中之步驟８４０），則在密碼單元上之控制並通過到方才所饋入之安全應用。取代地，下一安全應用程式或原有模式安全應用程式會饋入於過寫入先前所饋入之不核准的安全應用程式之機載ＲＡＭ的密碼程式控制部之內。然而，若該ＭＡＣ簽名測試通過時，則該ＲＯＭ饋入器控制程式會在該密碼單元上傳遞控制到方才饋入的安全應用程式。

雙回之實施例大致地較安全，因爲並沒有部分之新的安全應用程式在執行所有ＭＡＣ簽名測試之前饋入於ＲＡＭ２２２之密碼程式控制部之內；單回之實施例通常會造成更快之安全應用程式交換，因爲新的安全應用程式會開始執行於機載ＲＡＭ中無需等待第二回。

藉ＯＰＣ之密碼單元監督

在第１圖中之密碼單元４４係週期性地由ＯＰＣ２１所監督，也就是說，至少每月一次或在任何其他所選擇之時距，該密碼單元４４初始化與ＯＰＣ２１之連絡動作，連絡可經由數據機２４來撥號連接或經由ＴＣＰ／ＩＰ協定於網際網路連接之上，在各情況中，密碼單元４４之狀態會報告於ＯＰＣ２１，週期性連絡之目的在於使密碼單元４４之內容同步於在ＯＰＣ２１處所預期者。

例如，在與ＯＰＣ２１之週期性連絡期間，檢查經過時間計數器２０４（第２圖）以對照於其預期值且若需要時使其同步。經過時間之任何廣義的不一致可爲篡改之指

五、發明說明（35）

示且會由ＯＰＣ造成密碼單元之不激活，該ＯＰＣ可設定一或更多之准許位元２１６於存取暫存器２１２中而不激活密碼單元。一旦使不激活，則不活化之密碼單元無法饋入或運轉任何安全應用程式。

同時，在與ＯＰＣ２１之週期性連絡期間，檢查簽名記錄（第２圖中之２２４）以複查那些安全應用程式已饋入及運轉於該密碼單元中，若安全應用程式已取消（亦即，系統廣泛准許運轉該安全應用程式已撤走）時，則相對應於該安全應用程式之取消旗標將設定於該簽名記錄中，之後，結合於核准控制（第２圖中之２２６），該密碼單元４４將不會換入（饋入）所取消之安全應用程式。

A5
B5

四、中文發明摘要（發明之名稱：　公眾密碼控制單元及其系統　）

一種適用有效之公眾密碼控制單元（密碼單元）係使用於多重獨立使用者所共用之密碼系統中，安裝於多用途電腦當作週邊裝置的密碼單元會饋入及卸載所編密碼之安全應用程式於運轉各安全應用程式之該密碼單元之機載ＲＡＭ記憶體之內，該密碼單元及該密碼單元爲其一部件之系統提供其中僅預核准之安全應用程式會准許以饋入及運轉之安全內部環境，在該密碼單元內之計算環境係藉由與各密碼單元連絡之密碼操作中心（ＯＰＣ）所確保，軟體發展器在分配所給定之安全應用程式之前提出建議之安全應用程式至ＯＰＣ以取得所需之准許以用於所給定之安全應用程式，僅當所有必要之准許取得自ＯＰＣ時，給定之安全應用程式將允許饋入及運轉於該密碼單元中，當完成運轉第一安全應用程式時，該密碼單元會以編密碼之形式卸載（交換）目前所饋入之第一安全應用程式至ＰＣ硬碟驅動器及饋入（換入）下一個安全應用程式，各安全應用程式之密碼上下文保存在ＰＣ硬碟驅動器上之檔案中，在此方式中，單一密碼單元係共用於複數個獨立使用者之中。

英文發明摘要（發明之名稱：　）

PUBLIC CRYPTOGRAHIC CONTROL UNIT AND SYSTEM THEREFOR

A universally available, public cryptographic control unit (crypto unit) is used in a cryptographic system shared by multiple independent users. The crypto unit, which is installed as a peripheral device to a general-purpose computer, loads and unloads encrypted security applets into an onboard RAM memory of the crypto unit, where each security applet is run. The crypto unit and the system of which it is a part, provides a secure internal environment in which only pre-approved security applets are granted permission to load and run. The computing environment within the crypto unit is secured by a cryptographic operation center (OPC) which communicates with each crypto unit. The software developer submits a proposed security applet to the OPC prior to distributing a given security applet in order to obtain the necessary permission for the given security applet. Only if all necessary permissions are obtained from the OPC will a given security applet be allowed to load and run in the crypto unit. When a first security applet is finished running, the crypto unit unloads (swaps out) the presently loaded first security applet in encrypted form to the PC hard drive, and loads (swaps in) the next security applet. The cryptographic context of each security applet is preserved in the file stored on the PC hard drive. In such manner, a single crypto unit is shared among a plurality of independent users.

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

A8
B8
C8
D8

六、申請專利範圍

1．一種在密碼鍵碼分配系統中之方法，該系統含有具密碼控制單元之使用者電腦，軟體發展器電腦及密碼操作中心，該方法包含：

產生第一安全應用程式於該軟體發展器電腦處；

從該軟體發展器電腦傳輸該第一安全應用程式至該密碼操作中心；

在該軟體發展器電腦處接收來自該密碼操作中心之第一密碼鍵碼；

在該軟體發展器電腦處接收來自該密碼操作中心之第一序號；

在過程中利用該第一密碼鍵碼來編密碼該第一安全應用程式以形成第一編密碼之安全應用程式；

附加該第一序號於該第一編密碼之安全應用程式以形成第一安全封包；以及

分配該第一安全封包於該使用者電腦。

2．如申請專利範圍第1項之方法，其中該密碼控制單元含有程式控制記憶體，該方法尚包含：

傳輸來自該密碼控制單元之該第一序號至該密碼操作中心；

在該密碼控制單元處接收來自該密碼操作中心之該第一密碼鍵碼；

在過程中利用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼該第一安全應用程式；以及

饋入該第一安全應用程式於該程式控制記憶體中。

六、申請專利範圍

3．如申請專利範圍第1項之方法，其中在過程中利用該第一密碼鍵碼來編密碼該第一安全應用程式以形成第一編密碼之安全應用程式之該步驟尚包含：

於該軟體發展器電腦處，在程式規劃者鍵碼之下編密碼該第一安全應用程式以形成第一程式規劃者編密碼之安全應用程式；

於該軟體發展器電腦處，在該第一編密碼鍵碼之下編密碼該程式規劃者鍵碼以形成第一編密碼之程式規劃者鍵碼；以及

附加該第一編密碼之程式規劃者鍵碼及該第一程式規劃者編密碼之安全應用程式以形成該第一編密碼之安全應用程式。

4．如申請專利範圍第2項之方法，其中該軟體發展器電腦尚含有程式規劃者鍵碼，在該第一密碼鍵碼之下編密碼以形成第一編密碼之程式規劃者鍵碼於該第一編密碼之安全應用程式中，而在過程中利用該第一密碼鍵碼在該使用者電腦處從該第一編密碼之安全應用程式解密碼該第一安全應用程式的該步驟包含：

在該使用者電腦處接收含有該第一程式規劃者編密碼之安全應用程式之該第一安全封包；

於該使用者電腦處在該第一密碼鍵碼之下解密碼該第一編密碼之程式規劃者鍵碼以形成恢復之程式規劃者鍵碼；以及

在該恢復之程式規劃者鍵碼之下解密碼該第一程式規

六、申請專利範圍

劃者編密碼之安全應用程式以恢復該第一安全應用程式。

5．如申請專利範圍第1項之方法，尚包含：

儲存記錄複數個安全應用程式，密碼鍵碼與序號間之對應關係之安全應用程式記錄表，該安全應用程式記錄表具有指示該第一序號及該第一密碼鍵碼相對應於該第一安全應用程式之登錄。

6．如申請專利範圍第2項之方法，其中該使用者電腦含有第一使用者識別號碼，該方法尚包含：

傳輸來自該使用者電腦之該第一使用者識別號碼到該密碼操作中心；

儲存記錄複數個安全應用程式，密碼鍵碼，序號與使用者識別號碼間之對應關係之安全應用程式記錄表，該安全應用程式記錄表具有指示該第一序號，該第一密碼鍵碼及該第一使用者識別號碼相對應於該第一安全應用程式之登錄。

7．如申請專利範圍第2項之方法，其中該使用者電腦尚含有使用者電腦硬碟驅動器記憶體，以及該系統尚含有第二軟體發展器電腦，第二安全應用程式，該第二安全應用程式具有相對應於該處之個別的第二序號及第二密碼鍵碼，該方法尚包含：

在過程中利用第一使用者電腦鍵碼來編密碼該使用者控制記憶體之內容以形成第一編密碼之安全上下文；

儲存該第一編密碼之安全上下文於該使用者電腦硬碟驅動器記憶體之上；以及

六、申請專利範圍

饋入該第二安全應用程式於該程式控制記憶體之中。

8．如申請專利範圍第7項之方法，尚包含：

在過程中利用第二使用者電腦鍵碼來編密碼該使用者控制記憶體之內容以形成第二編密碼之安全上下文；

儲存該第二編密碼之安全上下文於該使用者電腦硬碟驅動器記憶體之上；

在過程中利用該第一使用者電腦鍵碼來解密碼該第一編密碼之安全上下文以恢復該第一安全上下文；以及

饋入該第一安全上下文於該程式控制記憶體之中。

9．一種在密碼鍵碼分配系統中之裝置，該系統含有具密碼控制單元之使用者電腦，軟體發展器電腦及密碼操作中心，該裝置包含：

用於產生第一安全應用程式於該軟體發展器電腦處之裝置；

用於從該軟體發展器電腦傳輸該第一安全應用程式至該密碼操作中心之裝置；

用於在該軟體發展器電腦處接收來自該密碼操作中心之第一密碼鍵碼之裝置；

用於在該軟體發展器電腦處接收來自該密碼操作中心之第一序號之裝置；

用於在過程中利用該第一密碼鍵碼來編密碼該第一安全應用程式以形成第一編密碼之安全應用程式之裝置；

用於附加該第一序號於該第一編密碼之安全應用程式以形成第一安全封包之裝置；以及

六、申請專利範圍

用於分配該第一安全封包至該使用者電腦之裝置。

１０．如申請專利範圍第９項之裝置，其中該密碼控制單元含有程式控制記憶體，該裝置尚包含：

用於傳輸來自該密碼控制單元之該第一序號至該編密碼操作中心之裝置；

用於在該密碼控制單元處接收來自該密碼操作中心之該第一密碼鍵碼之裝置；

用於在過程中利用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼第一安全應用程式之裝置；以及

用於饋入該第一安全應用程式於該程式控制記憶體中之裝置。

１１．如申請專利範圍第９項之裝置，其中用於在過程中利用該第一密碼鍵碼來編密碼該第一安全應用程式以形成第一編密碼之安全應用程式的該裝置尚包含：

用於在該軟體發展器電腦處於程式規劃者鍵碼之下編密碼該第一安全應用程式以形成第一程式規劃者編密碼之安全應用程式之裝置；

用於在該軟體發展器電腦處於該第一密碼鍵碼之下編密碼該程式規劃者鍵碼以形成第一編密碼之程式規劃者鍵碼之裝置；以及

用於附加該第一編密碼之程式規劃者鍵碼及該第一程式規劃者編密碼之安全應用程式以形成該第一編密碼之安全應用程式之裝置。

１２．如申請專利範圍第１０項之裝置，其中該軟體

六、申請專利範圍

發展器電腦尚含有程式規劃者鍵碼，在該第一密碼鍵碼之下編密碼以形成第一編密碼之程式規劃者鍵碼於該第一編密碼之安全應用程式中，而用於在過程中利用該第一密碼鍵碼在該使用者電腦處解密碼來自該第一程式規劃者編密碼之安全應用程式之該第一安全應用程式的該裝置包含：

用於在該使用者電腦處接收含有該第一程式規劃者編密碼之安全應用程式之該第一安全封包之裝置；

用於在該使用者電腦處於該第一密碼鍵碼之下解密碼該第一編密碼之程式規劃者鍵碼以形成恢復之程式規劃者鍵碼之裝置；以及

用於在該恢復之程式規劃者鍵碼之下解密碼該第一程式規劃者編密碼之安全應用程式以恢復該第一安全應用程式之裝置。

１３．如申請專利範圍第９項之裝置，尚包含：

用於儲存記錄複數個安全應用程式，密碼鍵碼與序號間之對應關係之安全應用程式記錄表的裝置，該安全應用程式記錄表具有指示該第一序號及該第一密碼鍵碼相對應於該第一安全應用程式之登錄。

１４．如申請專利範圍第１０項之裝置，其中該使用者電腦含有第一使用者識別號碼，該裝置尚包含：

用於傳輸來自該使用者電腦之該第一使用者識別號碼到該密碼操作中心之裝置；

用於儲存記錄複數個安全應用程式，密碼鍵碼，序號與使用者識別號碼間之對應關係之安全應用程式記錄表的

六、申請專利範圍

裝置，該安全應用程式記錄表具有指示該第一序號，該第一密碼鍵碼及該第一使用者識別號碼相對應於該第一安全應用程式之登錄。

１５．如申請專利範圍第１０項之裝置，其中該使用者電腦尚含有使用者電腦硬碟驅動器記憶體，以及該系統尚含有第二軟體發展器電腦，第二安全應用程式，該第二安全應用程式具有相對應於該處之個別的第二序號及第二密碼鍵碼，該裝置尚包含：

用於在過程中利用第一使用者電腦鍵碼來編密碼該使用者控制記憶體之內容以形成第一編密碼之安全上下文之裝置；

用於儲存該第一編密碼之安全上下文於該使用者電腦硬碟驅動器記憶體之裝置；以及

用於饋入該第二安全應用程式於該程式控制記憶體中之裝置。

１６．如申請專利範圍第１５項之裝置，尚包含：

用於在過程中利用第二使用者電腦鍵碼來編密碼該使用者控制記憶體之內容以形成第二編密碼之安全上下文之裝置；

用於儲存該第二編密碼之安全上下文於該使用者電腦硬碟驅動器記憶體上之裝置；

用於在過程中利用該第一使用者電腦鍵碼來解密碼該第一編密碼之安全上下文以恢復該第一安全上下文之裝置；以及

六、申請專利範圍

用於饋入該第一安全上下文於該程式控制記憶體中之裝置。

１７．一種在密碼鍵碼分配系統中於密碼操作中心處之密碼鍵碼分配方法，其中該系統含有具密碼控制單元之使用者電腦，軟體發展器電腦及密碼操作中心，該軟體發展器電腦產生第一安全應用程式及在過程中利用第一密碼鍵碼來解密碼該第一安全應用程式而形成第一編密碼之安全應用程式且分配該第一編密碼之安全應用程式至該使用者電腦，該方法包含：

接收來自該軟體發展器電腦之該第一安全應用程式於該密碼操作中心處；

傳輸來自該密碼操作中心之第一序號至該軟體發展器電腦；

傳輸來自該密碼操作中心之第一密碼鍵碼至該軟體發展器電腦；

接收來自該密碼控制單元之該第一序號於該密碼操作中心處；以及

傳輸來自該密碼操作中心之該第一密碼鍵碼至該密碼控制單元。

１８．如申請專利範圍第１７項之方法，其中該密碼控制單元含有程式控制記憶體，該方法尚包含：

接收該第一編密碼之安全應用程式於含有該第一序號之該密碼控制單元處；

傳輸來自該密碼控制單元之該第一序號至該密碼操作

A8
B8
C8
D8

六、申請專利範圍

中心；

接收來自該密碼操作中心之該第一密碼鍵碼於該密碼控制單元處；

在過程中利用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼該第一安全應用程式；以及

饋入該第一安全應用程式於該程式控制記憶體中。

１９．一種在密碼鍵碼分配系統中之方法，其中該系統具有軟體發展器電腦及密碼操作中心，該軟體發展器電腦產生由第一序號所識別之第一安全應用程式，及在過程中利用第一密碼鍵碼來編密碼該第一安全應用程式而形成第一編密碼之安全應用程式，該系統尚含有具有密碼控制單元與程式控制記憶體之使用者電腦，該方法包含：

接收含有該第一序號之該第一安全應用程式於該密碼控制單元處；

傳輸該第一序號至該密碼操作中心；

接收來自該密碼操作中心之該第一密碼鍵碼於該密碼控制單元處；

在過程中使用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼該第一安全應用程式；以及

饋入該第一安全應用程式於該程式控制記憶體中。

２０．一種在密碼鍵碼分配系統中於密碼操作中心處之密碼鍵碼分配裝置，其中該系統含有具密碼控制單元之使用者電腦，軟體發展器電腦及密碼操作中心，該軟體發展器電腦產生第一安全應用程式及在過程中利用第一密碼

六、申請專利範圍

鍵碼來解密碼該第一安全應用程式而形成第一編密碼之安全應用程式且分配該第一編密碼之安全應用程式至該使用者電腦，該裝置包含：

用於接收來自該軟體發展器電腦之該第一安全應用程式於該密碼操作中心處之裝置；

用於傳輸來自該密碼操作中心之第一序號至該軟體發展器電腦之裝置；

用於傳輸來自該密碼操作中心之第一密碼鍵碼至該軟體發展器電腦之裝置；

用於接收來自該密碼控制單元之該第一序號於該密碼操作中心處之裝置；以及

用於傳輸來自密碼操作中心之該第一密碼鍵碼至該密碼控制單元之裝置。

２１．如申請專利範圍第２０項之裝置，其中該密碼控制單元含有程式控制記憶體，該裝置尚包含：

用於接收該第一編密碼之安全應用程式於含有該第一序號之該密碼控制單元處之裝置；

用於傳輸來自該密碼控制單元之該第一序號至該密碼操作中心之裝置；

用於接收來自該密碼操作中心之該第一密碼鍵碼於該密碼控制單元處之裝置；

用於在過程中利用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼該第一安全應用程式之裝置；以及

用於饋入該第一安全應用程式於該程式控制記憶體中

六、申請專利範圍

之裝置。

２２．一種在密碼鍵碼分配系統中之裝置，其中該系統具有軟體發展器電腦及密碼操作中心，該軟體發展器電腦產生由第一序號所識別之第一安全應用程式，及在過程中利用第一密碼鍵碼來編密碼該第一安全應用程式而形成第一編密碼之安全應用程式，該系統尚含有具有密碼控制單元與程式控制記憶體之使用者電腦，該裝置包含：

用於接收含有該第一序號之該第一安全應用程式於該密碼控制單元處之裝置；

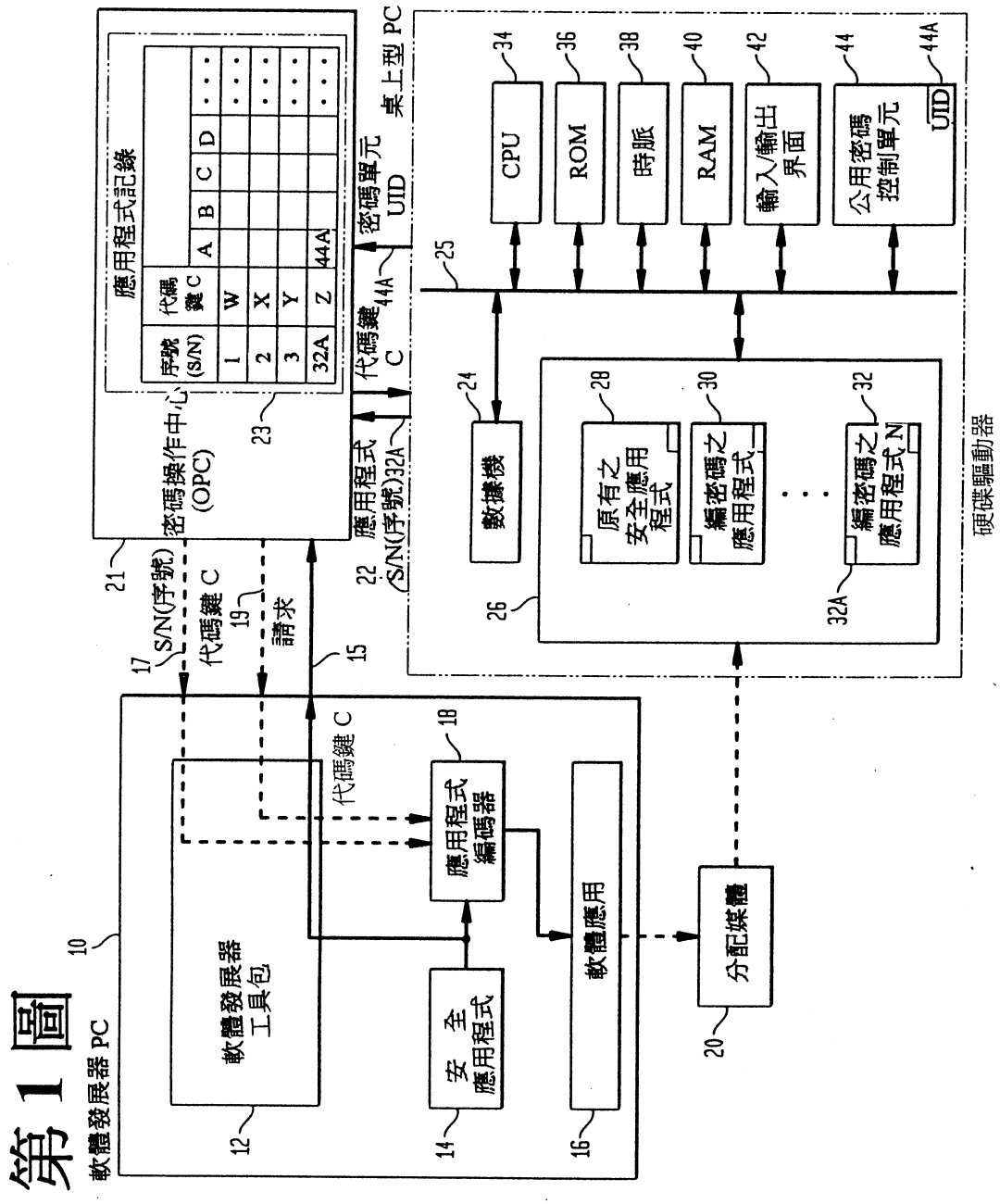
用於傳輸該第一序號至該密碼操作中心之裝置；

用於接收來自該密碼操作中心之該第一密碼鍵碼於該密碼控制單元處之裝置；

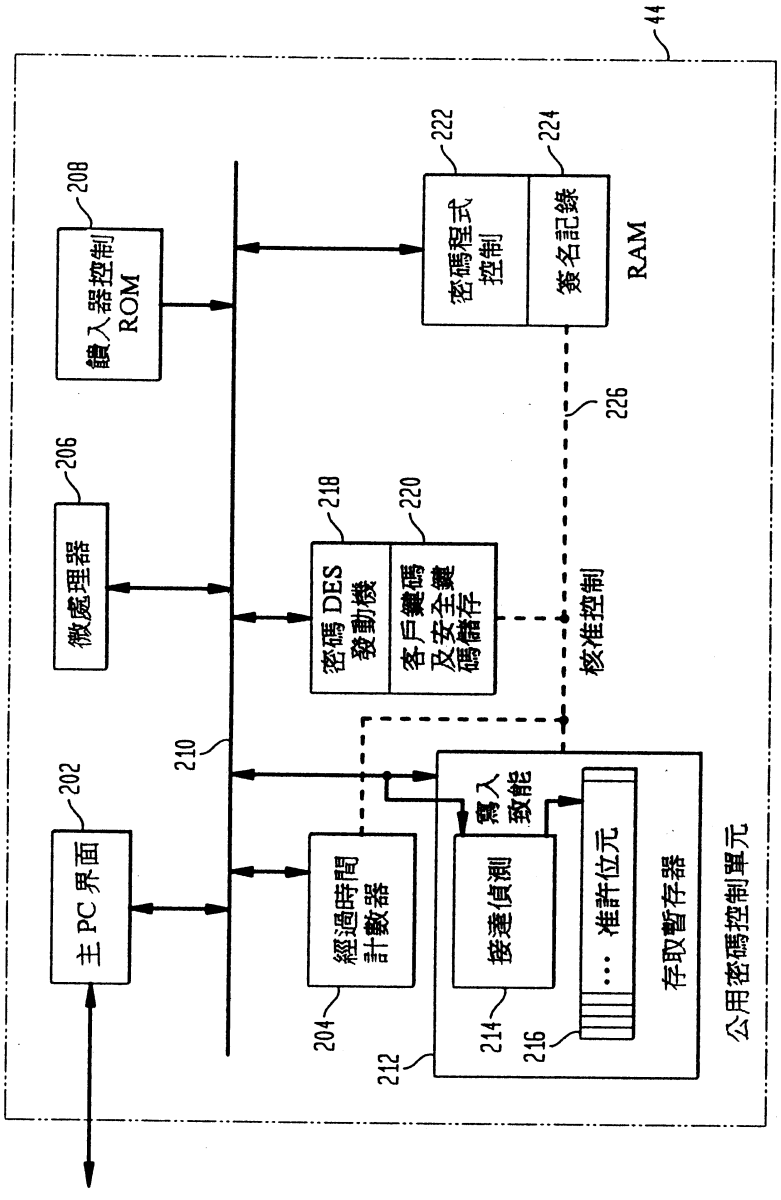
用於在過程中使用該第一密碼鍵碼從該第一編密碼之安全應用程式解密碼該第一安全應用程式之裝置；以及

用於饋入該第一安全應用程式於該程式控制記憶體中之裝置。

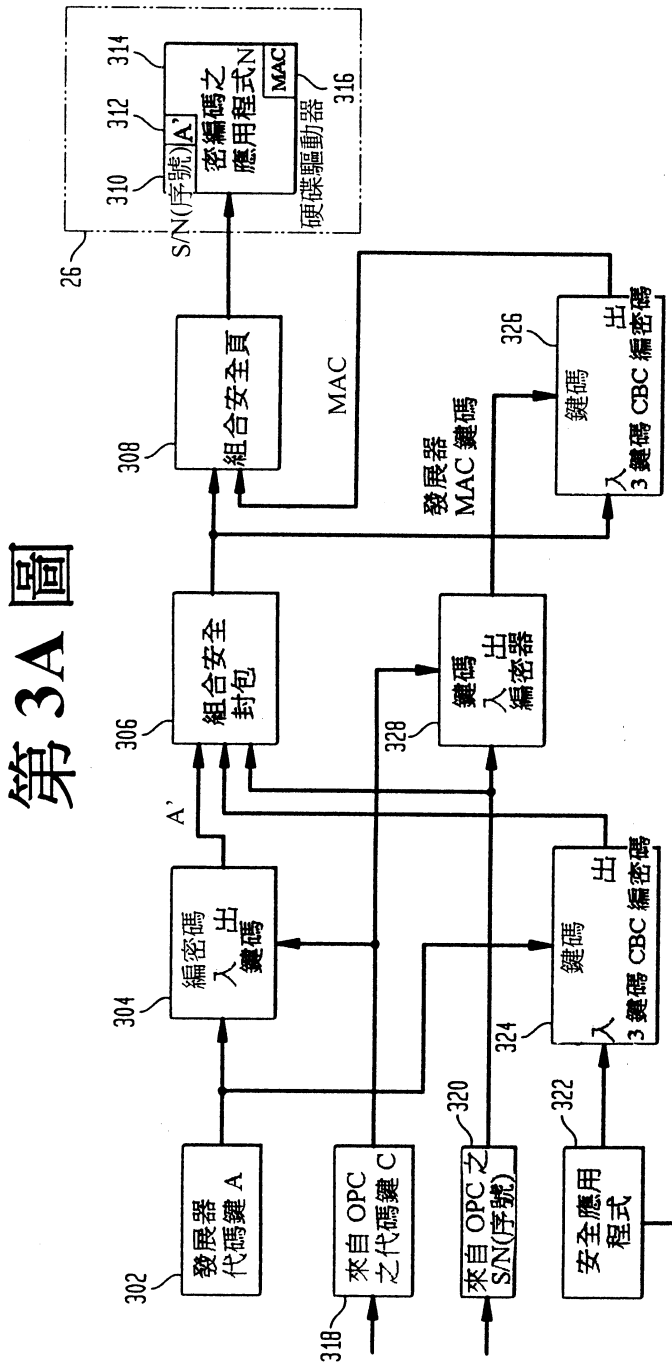
第 1 圖


軟體發展器 PC
10
軟體發展器工具包
12
安全應用程式
14
軟體應用
16
應用程式編碼器
18
代碼鍵 C
17
S/N(序號)
代碼鍵 C
19
請求
15
分配媒體
20
密碼操作中心 (OPC)
21
應用程式記錄
序號 (S/N)
代碼鍵 C
A
B
C
D
1 W
2 X
3 Y
32A Z 44A
23
應用程式 S/N(序號)32A
22
代碼鍵 C
密碼單元 UID 44A
桌上型 PC
25
CPU 34
ROM 36
時脈 38
RAM 40
輸入/輸出界面 42
公用密碼控制單元 44
UID 44A
數據機 24
原有之安全應用程式 28
編密碼之應用程式 30
編密碼之應用程式 N 32
32A
26
硬碟驅動器

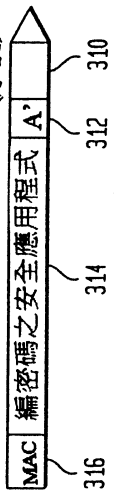
第 2 圖


44
208
鎖入器控制 ROM
222
224
密碼程式控制
簽名記錄
RAM
206
微處理器
218
220
密碼 DES 發動機
客戶鑰碼及安全鑰碼儲存
226
核准控制
210
202
主 PC 界面
經過時間計數器
204
212
解入致能
接達偵測
214
准許位元
216
存取暫存器
公用密碼控制單元

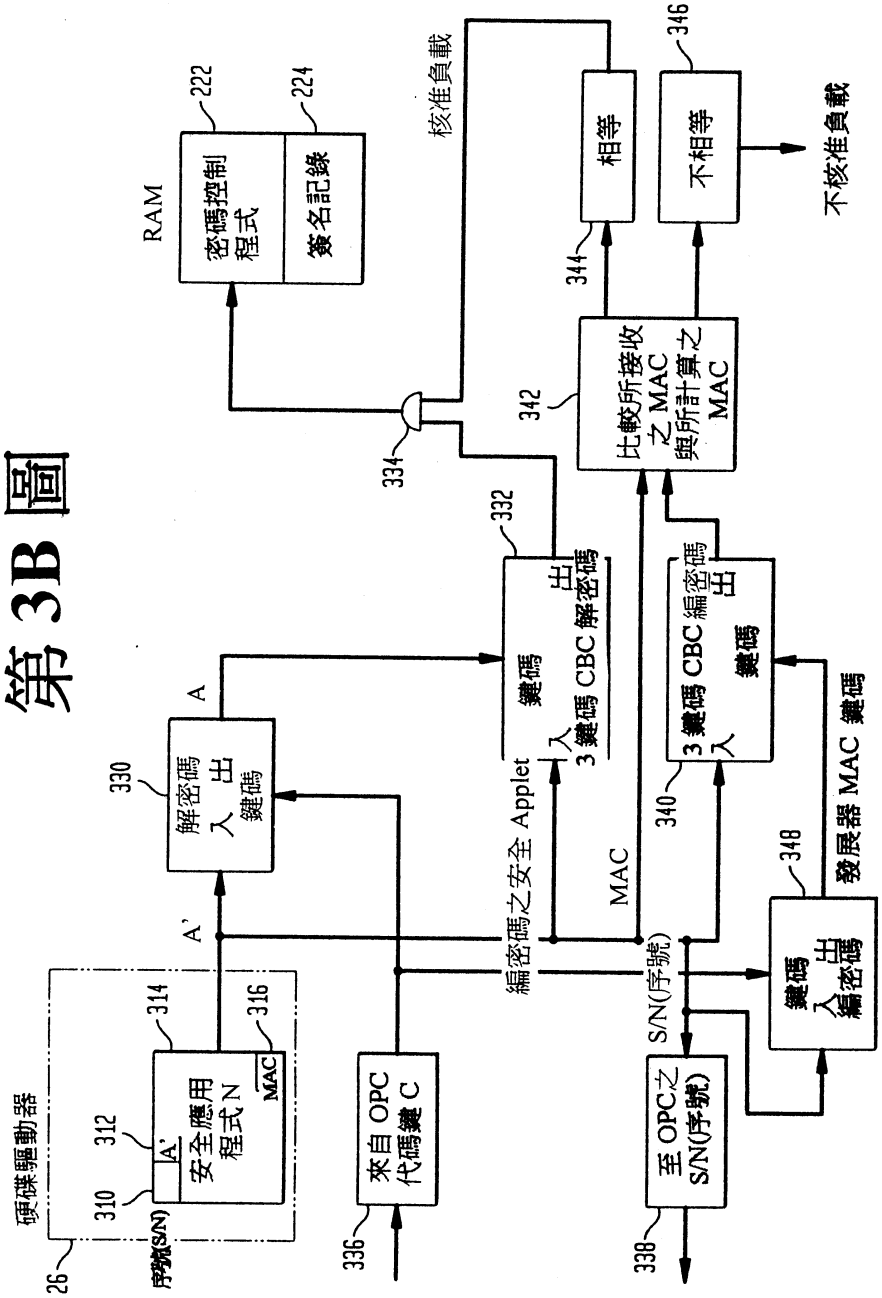
第 3A 圖


26
硬碟驅動器
S/N(序號)
A'
密編碼之應用程式N
MAC
310
312
314
316
組合安全頁
308
MAC
發展器 MAC 鍵碼
326
鍵碼 入 出 3 鍵碼 CBC 編密碼
組合安全封包
306
A'
328
鍵碼 入 出 編密器
編密碼 入 出 鍵碼
304
鍵碼 入 出 3 鍵碼 CBC 編密碼
324
發展器 代碼鍵 A
302
來自 OPC 之代碼鍵 C
318
來自 OPC 之 S/N(序號)
320
安全應用程式
322
至 OPC

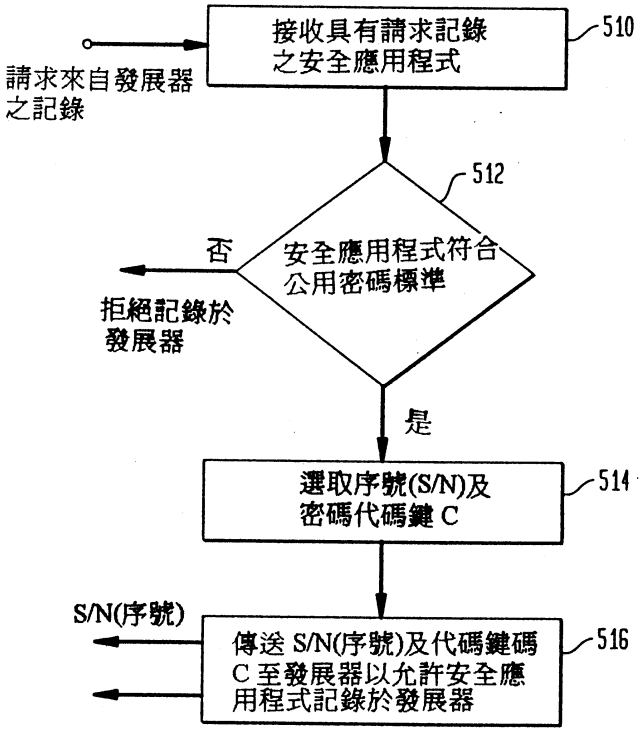
第 4 圖


S/N (序號)
MAC
編密碼之安全應用程式
A'
310
312
314
316

第 3B 圖


硬碟驅動器
26
序號(S/N)
310
312
A'
安全應用程式N
MAC
314
316
A'
A
330
解密碼入出鍵碼
RAM
222
密碼控制程式
224
簽名記錄
核准負載
334
來自 OPC 代碼鍵 C
336
編密碼之安全 Applet
鍵碼入
3 鍵碼 CBC 解密碼出
332
MAC
S/N(序號)
至 OPC之 S/N(序號)
338
3 鍵碼 CBC 編密碼入
鍵碼出
340
鍵碼入出編密碼
348
發展器 MAC 鍵碼
比較所接收之 MAC 與所計算之 MAC
342
344
相等
不相等
346
不核准負載

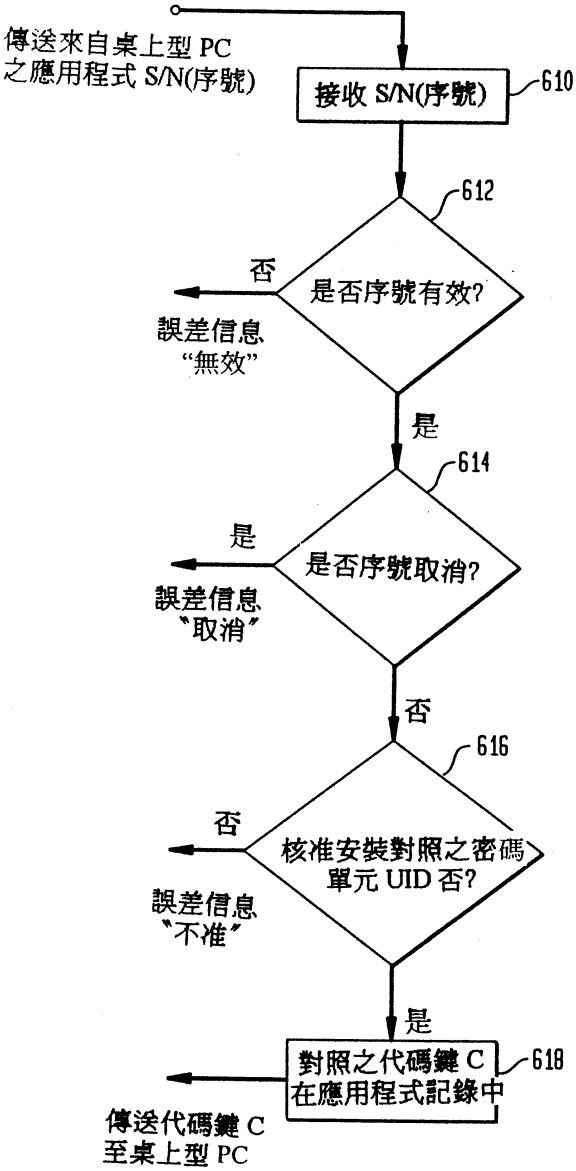
第 5 圖



在 OPC 處之安全應用程式的發展器

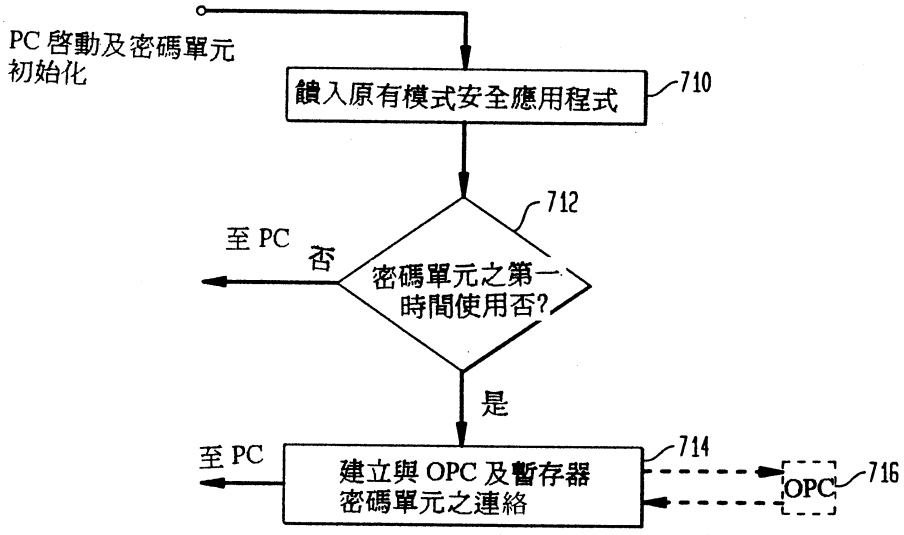
第 6 圖

桌上型 PC 初始化安全應用程式於 OPC 處



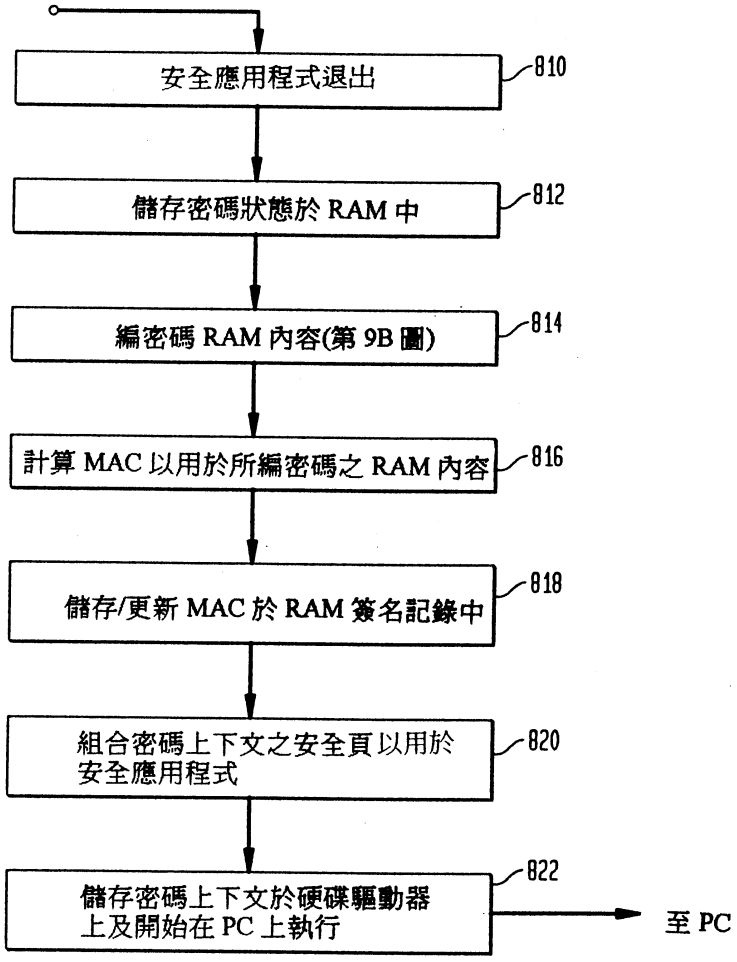
第 7 圖

ROM 饋入器控制操作系統初始化

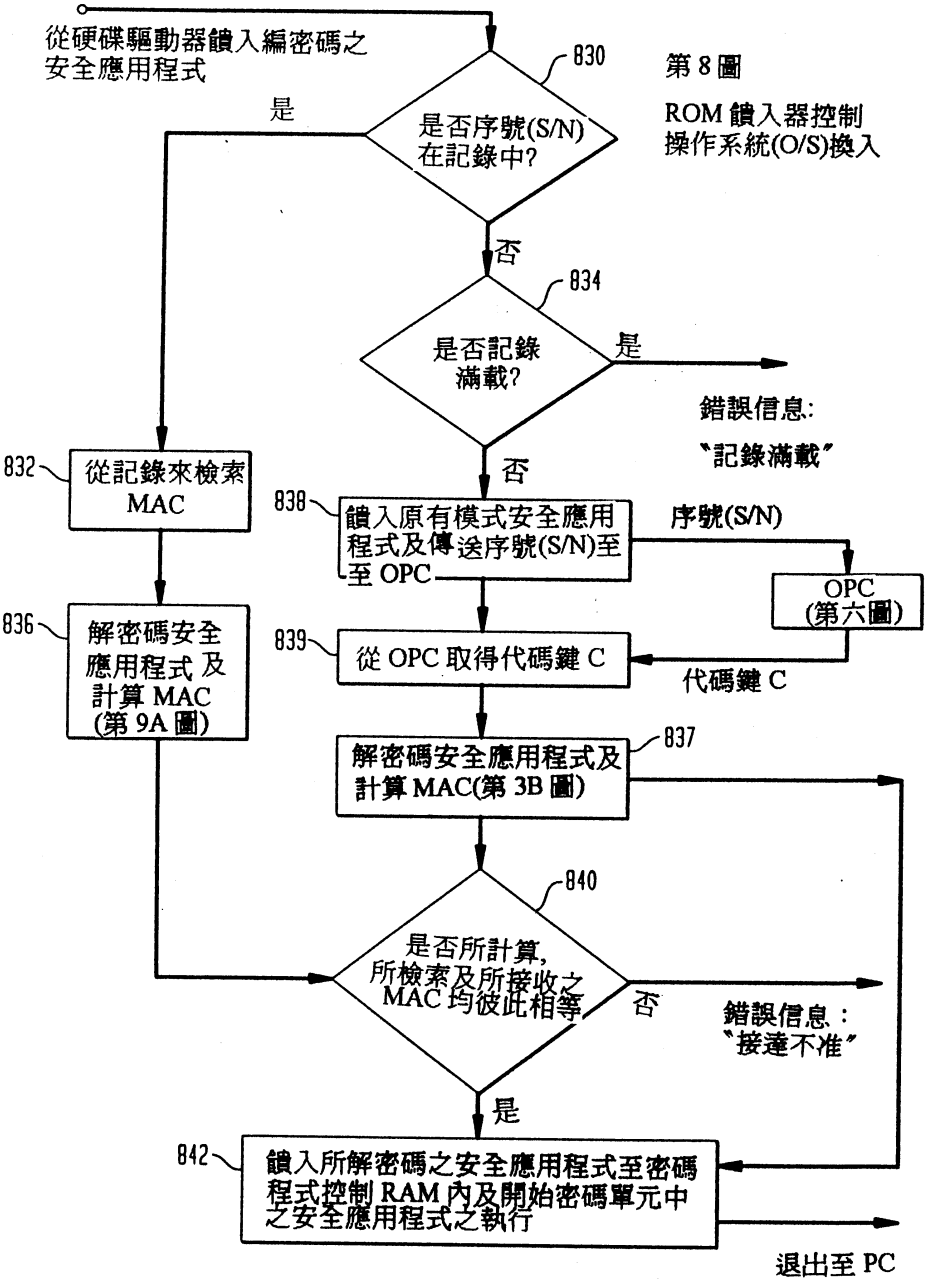


第 8A 圖

ROM 饋入器控制操作系統(O/S)交換



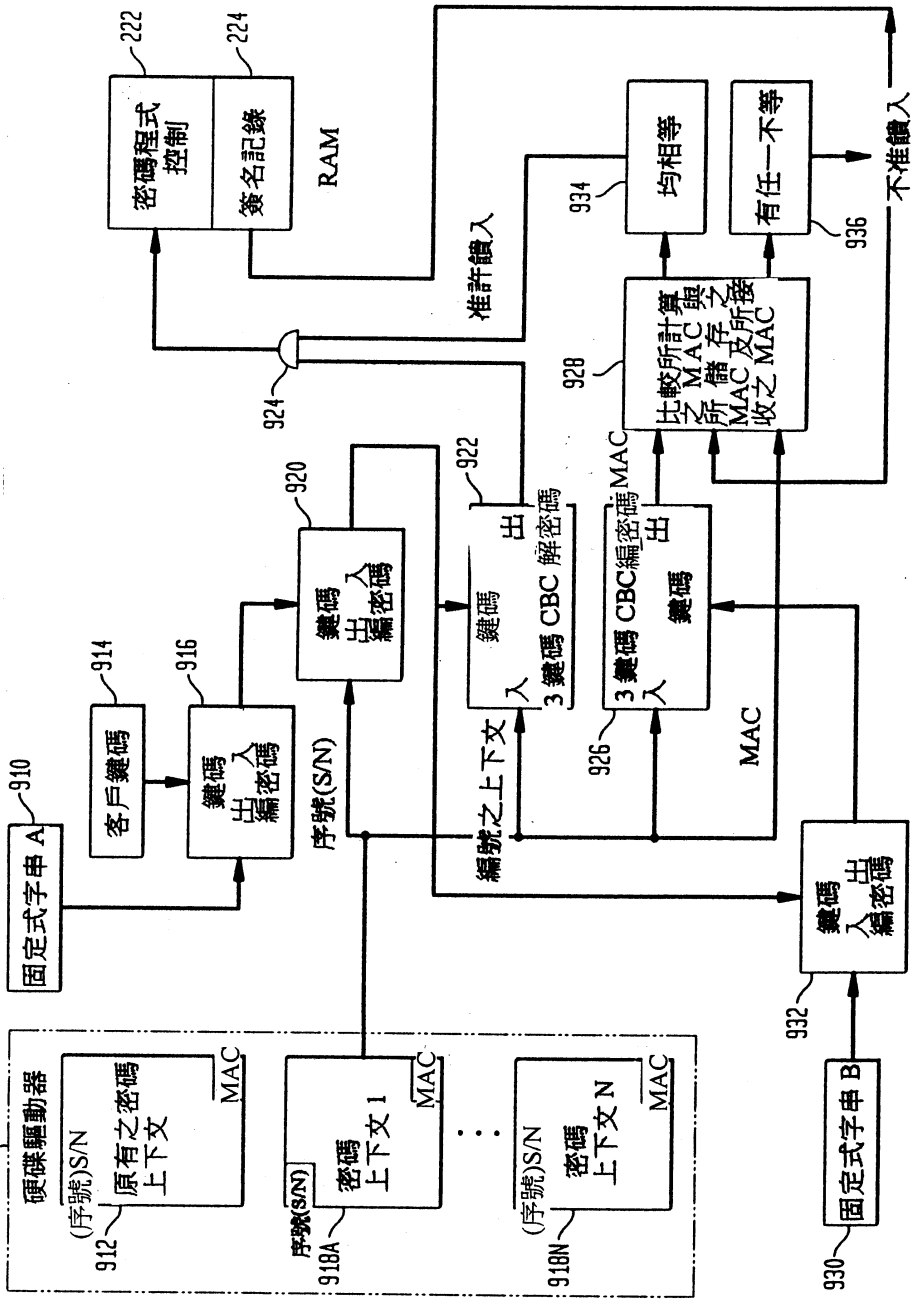
第 8B 圖



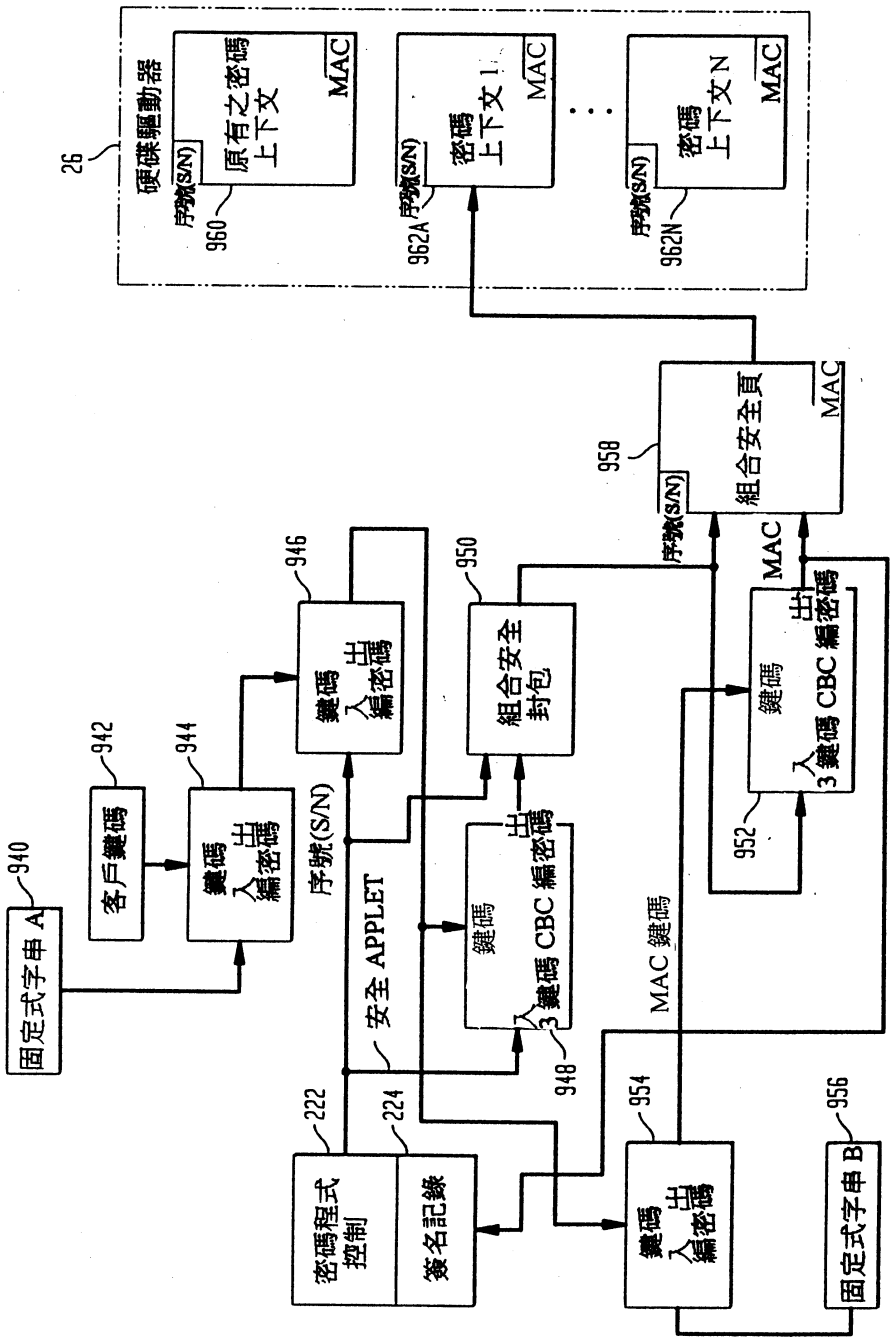
第 8 圖

ROM 饋入器控制操作系統(O/S)換入

第 9A 圖


26
硬碟驅動器
(序號)S/N
912
原有之密碼
上下文
MAC
序號(S/N)
918A
密碼
上下文 1
MAC
(序號)S/N
918N
密碼
上下文 N
MAC
固定式字串 A
910
客戶鑰碼
914
鑰碼
出
編密碼
入
916
序號(S/N)
鑰碼
出
編密碼
入
920
編號之上下文
鍵碼
入
出
922
3 鑰碼 CBC 解密碼
924
密碼程式
控制
222
簽名記錄
224
RAM
准許鎖入
3 鑰碼 CBC編密碼
926
MAC
鑰碼
出
入
MAC
比較所計算
之 MAC 與
所儲存
MAC 及所接
收之 MAC
928
均相等
934
有任一不等
936
不准鎖入
鑰碼
出
入
編密碼
932
固定式字串 B
930

第 9B 圖


26
硬碟驅動器
序號(S/N)
原有之密碼上下文
MAC
960
序號(S/N)
密碼上下文 1
MAC
962A
序號(S/N)
密碼上下文 N
MAC
962N
958
序號(S/N)
組合安全頁
MAC
946
鍵碼入出編密碼
950
組合安全封包
942
客戶鍵碼
944
鍵碼入出編密碼
940
固定式字串 A
序號(S/N)
安全 APPLET
鍵碼
3 鍵碼 CBC 編密碼
948
MAC 鍵碼
952
鍵碼
3 鍵碼 CBC 編密碼
MAC
222
密碼程式控制
224
簽名記錄
954
鍵碼入出編密碼
956
固定式字串 B