# 發明專利說明書 200304020

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：091356P2 ※IPC分類：G06F-3/44

※ 申請日期：91.12.10

## 壹、發明名稱

（中文） 鑒認碼之方法與裝置

（英文） AUTHENTICATED CODE METHOD AND APPARATUS

## 貳、發明人（共 6 人）

發明人 1 （如發明人超過一人，請填**說明書發明人續頁**）

姓名：（中文）安德魯 F. 古魯

（英文）ANDREW F. GLEW

住居所地址：（中文）美國加州聖荷西市菲爾橡街2416號

（英文）2416 FAIR OAKS COURT, SAN JOSE, CALIFORNIA 95125, U.S.A.

國籍：（中文）加拿大 （英文）CANADA

## 參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填**說明書申請人續頁**）

姓名或名稱：（中文）美商英特爾公司

（英文）INTEL CORPORATION

住居所或營業所地址：（中文）美國加州聖塔卡拉瓦市米遜大學路2200號

（英文）2200 MISSION COLLEGE BOULEVARD, SANTA CLARA, CALIFORNIA 95052, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

代表人：（中文）大衛 賽門

（英文）DAVID SIMON

說明書發明人續頁

發明人 2

姓名：（中文）詹姆斯 A. 蘇頓

（英文）JAMES A. SUTTON

住居所地址：（中文）美國歐勒岡州波特蘭市西北保林那路20205號

（英文）20205 NW PAULINA DRIVE, PORTLAND, OREGON 97229, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

發明人 3

姓名：（中文）勞倫斯 O. 史密斯

（英文）LAWRENCE O. SMITH

住居所地址：（中文）美國歐勒岡州比佛頓市西北北烏比亞路14995號

（英文）14995 NW NORTHUMBRIA, BEAVERTON, OREGON 97006, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

發明人 4

姓名：（中文）大衛 W. 葛拉羅克

（英文）DAVID W. GRAWROCK

住居所地址：（中文）美國歐勒岡州阿羅哈市西南第184大道8285號

（英文）8285 SW 184TH AVENUE, ALOHA, OREGON 97007, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

發明人 5

姓名：（中文）吉爾伯 尼格

（英文）GILBERT NEIGER

住居所地址：（中文）美國歐勒岡州波特蘭市東北第11大道2424號

（英文）2424 NE 11TH AVENUE, PORTLAND, OREGON 97212, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

發明人 6

姓名：（中文）邁可 A. 柯蘇

（英文）MICHAEL A. KOZUCH

住居所地址：（中文）美國賓州艾斯伯市傑佛森街280號

（英文）280 JEFFERSON STREET, EXPORT, PENNSYLVANIA 15632, US.A.

國籍：（中文）美國 （英文）U.S.A.

## 捌、聲明事項

☐ **本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：** _____

☑ **本案已向下列國家（地區）申請專利，申請日期及案號資料如下：**

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1.美國；2001 年；12 月 28 日；10/041,071

2._____

3._____

☑ **主張專利法第二十四條第一項優先權：**

【格式請依：受理國家（地區）；日期；案號　順序註記】

1.美國；2001 年；12 月 28 日；10/041,071

2._____

3._____

4._____

5._____

6._____

7._____

8._____

9._____

10._____

☐ **主張專利法第二十五條之一第一項優先權：**

【格式請依：申請日；申請案號　順序註記】

1._____

2._____

3._____

☐ **主張專利法第二十六條微生物：**

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1._____

2._____

3._____

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1._____

2._____

3._____

☐熟習該項技術者易於獲得，不須寄存。

(1)

# 玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

相關申請案

本發明關於美國專利申請案第_/__,__號“Processor Supporting Execution Of An Authenticated Code Instruction”及申請案第_/__,__號“Authenticated Code Module”，此二案皆與本案同一天申請。

技術領域

本發明係關於計算裝置之領域，具體而言，本發明係關於一種鑒認碼之方法與裝置。

先前技術

計算裝置執行韌體及/或軟體碼以執行一些操作，碼可以為使用者應用、BIOS程序、作業系統程序等等之格式。一些作業系統提供用於維護計算裝置之完整之有限維護對抗不良碼。例如，一管理者可以限制使用者或使用者之群組以執行明確前允許碼。一管理者可以進一步組態一沙箱或一隔離環境，其中直到管理者認為該碼可受信任可以執行不受信任碼。在上面技術提供一些維護時，它們通常需要一管理者根據碼之提供者、碼之歷史功能，及/或原始碼本身之再檢查人工產生一受信任決定。

也已經引入其它裝置以提供用於產生一受信任決定之自動裝置。例如，一實體(例如，軟體產生者)可以提供具有一證明之碼，例如數位化簽章碼及證明碼之完整之一X.509證明。一管理者可以組態一作業系統以自動允許使用者執行其提供來自一受信任實體之一證明，不需要管理

員考慮特別分析該碼之碼。在上面技術係可以滿足於一些環境時，上面技術固有受信任作業系統或其它軟體在作業系統之控制之下執行，以正確處理證明。

然而，特定操作無法受信任作業系統產生此一決定。例如，執行之碼可以導致計算裝置決定是否受信任作業系統。受信任作業系統鑒認這種碼將阻止碼之目的。執行之碼可以進一步包含其在計算裝置之作業系統之前執行之系統初始化碼。因此，這種碼不可以藉由作業系統鑒認。

發明內容

本發明提供一種載入、鑒認及/或執行儲存於一私人記憶體中之鑒認碼模組之裝置及方法。

實施方式

下面說明用於開始及終止可以使用於一些操作，例如建立及/或維持一受信任計算環境之鑒認碼(AC)模組之執行之技術。在下面說明中，為提供本發明之一更完整瞭解，提出一些特定細節例如邏輯執行、作業碼、說明運算元之方法、資源分割/共享/複製執行、系統元件之類型及相互關聯，及邏輯分割/整合選擇。然而，藉由一習於此技者將瞭解可以沒有這種特定細節執行。在其它實例中，為不混淆本發明，已經不詳細揭示控制結構，閘位準電路及全部軟體指令排序。習於此技者利用引入之說明，將可以適當執行功能而沒有不當實驗。

在對“某一實施例”、“一實施例”、“一舉例實施例”，等等說明中之參考指示說明之實施例可以包含一特定特徵

、結構，或特性，但是每一實施例係可以不必要包含特定特徵、結構，或特性。而且，這種片語係不必要提到相同實施例。在進一步相關於一實施例說明一特定特徵、結構，或特性時，認為其係習於此技者對產生這種有關於其它不論沒有清楚說明之實施例之特徵、結構或特性之瞭解之內。

在下面說明及申請專利範圍中，可以使用“耦合”及“連接”項目，包含它們之衍生項目。應該瞭解不想要這些項目如用於彼此之同義字。當然，在特定實施例中，“連接”係可以使用於指示二個或更多元件係互相直接實體或電連接。“耦合”可以意謂二個或更多元件係直接實體或電連接。然而，“耦合”也可以意謂二個或更多元件不係互相直接實體連接，但是還仍然互相配合或互動。

一計算裝置100之實例實施例揭示於圖1A-1E中。計算裝置100可以包含一或多個處理器110通過一處理器匯流排130耦合於一晶片組120。晶片組120可以包含一或多個積體電路封包或晶片，其耦合處理器110於系統記憶體140、一實體符記150、私人記憶體160、一媒體界面170，及/或計算裝置100之其它I/O裝置。

各個處理器110可以執行如一單一積體電路、多個積體電路，或具有軟體程序(例如，二進位翻譯程序)之硬體。處理器110可以進一步包含快取記憶體112及控制暫存器114，通過控制暫存器114可以組態快取記憶體112在一正常快取模式中，或在一如RAM快取模式中操作。在正常快取

模式中，快取記憶體112滿足響應於快取擊中之記憶體需求，響應於快取遺失代替快取線，及響應於處理器匯流排130之搜尋需求可以無效或代替快取線。在如RAM快取模式中，快取記憶體112係可以操作如隨機存取記憶體，其中係藉由快取記憶體滿足在快取記憶體112之記憶體範圍內之需求，及不響應於處理器匯流排130之搜尋需求代替或無效快取之線。

處理器110可以進一步包含一密鑰116，例如，一對稱加密演算法(例如，熟知DES、3DES及AES演算法)，或一非對稱加密演算法(例如，熟知RSA演算法)之一密鑰。在執行AC模組190之前，處理器110可以使用密鑰116鑒認一AC模組190。

處理器110可以支援一或多個操作模式，例如一真實模式、一維護模式、一虛擬真實模式及一虛擬裝置模式(VMX模式)。處理器110可以進一步支援在支援操作模式之各個模式中之一或多個特權位準或環。通常，一處理器110之操作模式及特權位準定義適用於執行之指令，及執行這種指令之效能。尤其，可以允許一處理器110執行明確特權指令，僅如果處理器110在一適當操作模式及/或特權位準中。

處理器110也可以支援處理器匯流排130之鎖定。由於鎖定處理器匯流排130，一處理器110可以取得處理器匯流排130之專用權。其它處理器110及晶片組120可以不取得處理器匯流排130之所有權直到釋放處理器匯流排130。在一實例

實施例中，一處理器110可以在處理器匯流排130上配置其提供其它處理器110及晶片組120，具有一LT.PROCESSOR.HOLD訊息之一特定處理。LT.PROCESSOR.HOLD匯流排訊息防止其它處理器110及晶片組120要求處理器匯流排130之擁有權，直到處理器110通過一LT.PROCESSOR.RELEASE訊息釋放處理器匯流排130。

處理器110可以任意支援鎖定處理器匯流排130之變換及/或額外方法。例如，一處理器110藉由配置一處理器內中斷、顯示一處理器匯流排鎖定信號、顯示一處理器匯流排需求信號，可以通知其它處理器110及晶片組120鎖定狀態，及/或導致其它處理器110中止執行。同樣一處理器110藉由配置一處理器內中斷、不顯示一處理器匯流排鎖定信號、不顯示一處理器匯流排需求信號，可以釋放處理器匯流排130，及/或導致其它處理器110繼續執行。

處理器110也可以進一步支援開始AC模組190及AC模組190之終止執行。在一實例實施例中，處理器110可以支援其載入、開始，及初始來自私人記憶體160之一AC模組190之執行之一ENTERAC指令之執行。然而，處理器110可以執行導致處理器110載入、開始，及初始一AC模組190之額外或不同指令。這些其它指令係可以變換用於開始AC模組190，或可以考慮於開始AC模組190之其它操作以幫助完成一較大作業。除非指示之外，後面參考ENTERAC指令及這些其它指令如開始AC模組190指令，不管這些指令中之一些指令可以載入、開始，及初始一AC模組190如其它操

作，例如，建立一受信任計算環境之一副作用之事實。

在一實例實施例中，處理器110進一步支援其終止一AC模組190之執行，及初始一後AC碼(如圖6)之一EXITAC指令之執行。然而，處理器110可以支援導致處理器110終止一AC模組190，及開始後AC碼之額外或不同指令。這些其它指令可以係用於終止AC模組190之EXITAC指令之變換，或可以係主要考慮於導致終止AC模組190如一較大操作之部分之操作之指令。除非指示之外，後面參考EXITAC指令如終止AC指令，不管這些指令中之一些指令可以終止AC模組190及開始後AC碼如其它操作，例如，拆除一受信任計算環境之一副作用之事實。

晶片組120可以包含用於控制對記憶體140之存取之一記憶體控制器122。晶片組120可以進一步包含一密鑰124，處理器110可以使用其於在執行之前鑒認一AC模組190。類似於處理器110之密鑰116，密鑰124可以包含一對稱或一非對稱加密演算法之一密鑰。

晶片組120也可以包含受信任平台暫存器126，以控制及提供關於晶片組120之受信任平台特性之狀態資訊。在一實例實施例中，晶片組120映射受信任平台暫存器126到記憶體140之一私人空間142及/或一公共空間144，以致能處理器110依據一一致方法存取受信任平台暫存器126。

例如，晶片組120可以映射暫存器126之一用戶如在公共空間144中之唯讀位置，及可以映射暫存器126如在私人空間142中之讀取/寫入位置。晶片組120可以依據其僅致能處

理器110於大部分特權模式中之一方法組態私人空間142，以利用特權讀取及寫入位置存取其之映射暫存器126。進一步，晶片組120可以進一步依據其致能處理器110於所有特權模式中之一方法組態公共空間144，以利用正常讀取及寫入位置存取其之映射暫存器126。晶片組120也可以響應於其係寫入於一指令暫存器126之一開啟私人指令開啟私人空間142。由於開啟私人空間142，處理器110可以依據如公共空間144之相同方法，利用正常非特權讀取及寫入處理存取私人空間142。

計算裝置100之實體符記150包含用於記錄完整尺寸及儲存機密，例如，一加密密鑰之維護儲存。實體符記150可以響應於來自處理器110及晶片組120之需求，執行一些完整功能。尤其，實體符記150可以依據一受信任方法儲存完整尺寸，可以依據一受信任方法引用完整尺寸，可以封閉機密如加密密鑰到一特定環境，及可以僅不封閉機密到封閉機密之環境。後面，項目“平台密鑰”係使用於參考其係封閉於一特定硬體及/或軟體之一密鑰。可以依據一些不同方法執行實體符記150。然而，在一實例實施例中，執行實體符記150以遵守在2001年7月31日之受信任計算平台協會(TCPA)主要規格版本1.1中詳細說明之受信任平台模組(TPM)之規格。

私人記憶體160可以依據允許處理器或執行AC模組190之處理器110存取AC模組190，及防止計算裝置100之其它處理器110及元件修改AC模組190，或利用AC模組190之執行

干擾之一方法儲存一AC模組190。如圖1A中所示，可以利用其係執行開始AC指令之處理器110之快取記憶體112執行私人記憶體160。另外，如圖1B中所示，可以執行私人記憶體160如其係在處理器110內，分離於其之快取記憶體112之一記憶體區域。如圖1C中所示，可以執行私人記憶體160如通過一分離專用匯流排，耦合於處理器110之一分離外部記憶體，因此僅致能處理器110具有相關外部記憶體，以正確執行開始AC指令。

也可以通過系統記憶體140執行私人記憶體160。在此一實施例中，晶片組120及/或處理器110可以明確定義記憶體140之範圍如私人記憶體160 (如圖1D)，其可以限制於一特定處理器110，及在一特定操作模式中時其可以僅藉由特定處理器110存取。本執行方式之一缺點係處理器110依賴晶片組120之記憶體控制器122存取私人記憶體160及AC模組190。因此，一AC模組190沒有定義對AC模組190之處理器110存取不可以重建記憶體控制器122，及因此導致處理器110放棄AC模組190之執行。

如圖1E中所示，也可以執行私人記憶體160如耦合於晶片組120之一分離私人記憶體控制器128之一分離記憶體。在這一種實施例中，私人記憶體控制器128可以提供到私人記憶體160之一分離界面。由於一分離私人記憶體控制器128，處理器110依據確保處理器110將可以存取私人記憶體160及AC模組190之一方法，可以重建用於系統記憶體140之記憶體控制器122。通常，分離私人記憶體控制器128

克服在圖1D中所示之實施例在一額外記憶體，及記憶體控制器之費用之一些缺點。

可以在一些裝置可讀取媒體180中之任何媒體提供AC模組190。媒體界面170提供到一裝置可讀取媒體180及AC模組190之一界面。裝置可讀取媒體180可以包含其可以儲存，至少暫時，用於藉由媒體界面170讀取之資訊之任何媒體。這可以包含信號傳送(通過線、光學或空氣做為界面)及/或實體儲存媒體例如一些類型之碟片及記憶體儲存裝置。

請即參考於圖2，依據更多細節揭示AC模組190之一實例實施例。AC模組190可以包含碼210及資料220。碼210包含一或多個碼傳呼212，及資料220包含一或多個資料傳呼222。各個碼傳呼212及資料傳呼222在一實例實施例中相應於一4千位元組連續記憶體範圍；然而，可以利用不同傳送尺寸或依據一非傳呼方法執行碼210及資料220。碼傳呼212包含藉由一或多個處理器110執行之處理器指令，及資料傳呼222包含藉由一或多個處理器110存取之資料，及/或用於儲存藉由一或多個處理器110響應於碼傳呼212之執行指令產生之資料之高速暫存記憶區。

AC模組190可以進一步包含可以係碼210或資料220之部分之一或多個表頭230。表頭230可以提供關於AC模組190之資訊，例如，模組編寫、複製權提示、模組版本、模組執行點位置、模組長度、鑒認方法。AC模組190可以進一步包含可以係碼210、資料220及/或表頭230之一部分之一

簽章240。簽章240可以提供關於AC模組190、鑒認實體、鑒認訊息、鑒認方法及/或概要數值之資訊。

AC模組190也可以包含一模組標印器250之一終止。模組標印器250之終止說明AC模組190之終止，及可以使用如對說明AC模組190之長度之一變換。例如，可以依據一連續方法說明碼傳呼212及資料傳呼222，及模組標印器250之終止可以包含其傳送碼傳呼212及資料傳呼222之終止之一預定位元類型。應該瞭解AC模組190可以依據一些不同方法說明其之長度及/或終止。例如，表頭230可以說明AC模組190包含之位元之數量或傳呼之數量。另外，開始AC及終止AC指令可以預期AC模組190係在長度方面之一預定數量之位元組，或包含一預定數量之傳呼。開始AC及終止AC指令可以進一步包含其說明AC模組190之長度之運算元。

應該瞭解AC模組190可以屬於記憶體140之一連續範圍，其係在實體記憶體空間中連續或在虛擬記憶體空間中連續。不論實體或虛擬連續，可以藉由一開始位置及一長度說明其儲存AC模組190之記憶體140之位置，及/或模組標印器250之終止可以說明。另外，可以依據或者一實體或一虛擬連續方法儲存AC模組190於記憶體140中。例如，可以儲存AC模組190於一資料結構中，例如，其允許計算裝置100依據一非連續方法，儲存及擷取來自記憶體140之AC模組190之一鏈接列表。

如將在下面更多細節中討論，實例處理器110支援其載

入AC模組190進入私人記憶體160之開始AC指令，及來自一執行點260之AC模組190之初始指令。藉由這一種開始AC指令開始之一AC模組190可以包含碼210，其在載入進入私人記憶體160時配置執行點260在一開始AC指令之一或多個運算元說明之一位置。另外，開始AC指令可以導致處理器110從AC模組190本身取得執行點260之位置。例如，碼210、資料220、一表頭230及/或簽章240可以包含其說明執行點260之位置之一或多個範圍。

如將在下面更多細節中討論，實例處理器110支援其在執行之前鑒認AC模組190之開始AC指令。因此，AC模組190可以包含資訊以支援藉由處理器110之鑒認決定。例如，簽章240可以包含一概要數值242。可以藉由通過一雜湊演算法(例如，SHA-1或MD5)或一些其它演算法，通過AC模組190產生概要數值242。也可以加密簽章240以防止概要數值242通過一加密演算法(例如，DES、3DES、AES，及/或RSA演算法)之修改。在實例實施例中，利用其相應於處理器密鑰116、晶片組密鑰120及/或平台密鑰152之一公共密鑰之私人密鑰RSA加密簽章240。

應該瞭解可以通過其它裝置鑒認AC模組190。例如，AC模組190可以利用不同雜湊演算法或不同加密演算法。AC模組190可以進一步包含關於碼210、資料220、表頭230及/或簽章240之資訊，其指示使用那種演算法。也可以藉由加密全部AC模組190用於通過處理器密鑰116、晶片組密鑰124或平台密鑰152之一對稱或非對稱密鑰之解密以維護

AC模組190。

在圖3中依據更多細節說明處理器110之一實例實施例。如說明，處理器110可以包含一前端302、一暫存器檔案306、一或多個指令370及一退出單元或後端380。前端302包含一處理器匯流排界面304、具有指令及指令指標暫存器314及316之一取得單元330、一解碼器340、一指令排序350及一或多個快取記憶體360。暫存器檔案306包含一般用途暫存器312、狀態/控制暫存器318及其它暫存器320。取得單元330從記憶體140通過處理器匯流排界面304，或快取記憶體360取得藉由指令指標暫存器316說明之指令，及儲存取得之指令於指令暫存器314中。

一指令暫存器314可以包含多於一指令。因此，解碼器340識別在指令暫存器314中之指令，及依據適用於執行之一格式配置識別之指令於指令排序350中。例如，解碼器340可以產生及儲存用於在指令排序350中之各個識別指令之一或多個微操作(uops)。另外，解碼器340可以產生及儲存用於在指令排序350中之各個識別指令之一單一微操作(Mop)。除非指示之外，後面使用之項目ops參考uops及Mops二者。

處理器110進一步包含執行藉由指令排序350之ops指示之操作之一或多個執行單元370。例如，執行單元370可以包含其執行可以使用於鑒認AC模組190之鑒認操作之雜湊單元、解密單元及/或微碼單元。執行單元370可以執行儲存於指令排序350中之ops之依序執行。然而，在一實例實

施例中，處理器110支援ops藉由指令排序350之故障執行。在此一實例實施例中，處理器110可以進一步包含一退出單元380，其從指令排序350依序去除ops，及指派執行ops之結果到一或多個暫存器312、314、316、318、320以確保適當依序結果。

解碼器340可以產生用於一識別開始AC指令之一或多個ops，及執行單元370響應於執行相關ops可以載入、鑒認及/或初始一AC模組190之執行。解碼器340可以進一步產生用於一識別終止AC指令之一或多個ops，及執行單元370響應於執行相關ops可以終止一AC模組190之執行，調整計算裝置100之安全狀態，及/或初始後AC碼之執行。

尤其，解碼器340根據開始AC指令可以產生一或多個ops，及相關於開始AC指令之零或更多運算元。各個開始AC指令及其之相關運算元說明用於開始AC模組190之參數。例如，開始AC指令及/或運算元可以說明關於AC模組190之參數例如AC模組位置、AC模組長度，及/或AC模組執行點。開始AC指令及/或運算元可以說明關於私人記憶體160之參數，例如，私人記憶體位置、私人記憶體長度，及/或私人記憶體執行。開始AC指令及/或運算元可以進一步說明用於鑒認AC模組190之參數例如說明其使用鑒認演算法、雜湊演算法、解密演算法及/或其它演算法。開始AC指令及/或運算元可以進一步說明用於演算法之參數，例如，密鑰長度、密鑰位置及/或密鑰。開始AC指令及/或運算元可以進一步說明參數以組態計算裝置100用於AC模組

開始，例如，說明遮罩/非遮罩事件及/或更新之安全容量。

開始AC指令及/或運算元可以提供較少、額外及/或不同於那些上面說明之參數。而且，開始AC指令可以包含零或更清楚運算元及/或默示運算元。例如，開始AC指令可以具有藉由處理器暫存器及/或記憶體位置默示說明之運算元數值，不管開始AC指令本身不包含定義那些運算元之位置之範圍。而且，開始AC指令通過一些技術，例如，中間資料、暫存器識別、絕對位址，及/或相對位址可以默示說明運算元。

解碼器340也可以產生根據終止AC指令之一或多個ops，及相關於終止AC指令之零或更多運算元。各個開始AC指令及其之相關運算元說明用於終止AC模組190之執行之參數。例如，終止AC指令及/或運算元可以說明關於AC模組190之參數例如AC模組位置，及/或AC模組長度。終止AC指令及/或運算元可以說明關於私人記憶體160之參數，例如，私人記憶體位置、私人記憶體長度及/或私人執行。終止AC指令及/或運算元可以進一步用於關於開始後AC碼之參數，例如，開始方法及/或後AC碼執行點。終止AC指令及/或運算元可以進一步說明參數以組態計算裝置100用於後AC碼執行，例如，說明遮罩/非遮罩事件及/或更新之安全容量。

終止AC指令及/或運算元可以提供較少、額外及/或不同於那些上面說明之參數。而且，終止AC指令依據如上面說明屬於開始AC指令之一方法，可以包含零或更清楚運

算元及/或默示運算元。

請即參考於圖4，具有說明開始AC模組190之一方法400。尤其，方法400說明一處理器110響應於執行具有一鑒認運算元、一模組運算元，及一長度運算元之一實例ENTERAC指令之操作。然而，一習於此技者沒有不對稱實驗，應該可以執行具有較少、額外及/或不同運算元之其它開始AC指令。

在區塊404中，處理器110決定是否環境係適用於開始一AC模組190之執行。例如，處理器110可以檢查其之目前特權位準、操作模式，及/或定址模式係適當。如果處理器支援多個硬體執行線，處理器110可以進一步檢查已停止之所有其它執行線。處理器110可以進一步檢查晶片組120符合明確需求。在ENTERAC指令之一實例實施例中，響應於決定處理器110係在操作之一維護平模式中，處理器110決定環境係適當，處理器之目前特權位準係0，處理器110已停止所有其它執行線之執行，及晶片組120提供如藉由一或多個暫存器126指示之受信任平台容量。開始AC指令之其它實施例可以不同定義適當環境。其它開始AC指令及/或相關運算元可以說明其導致處理器110檢查其之環境之較少、額外及/或不同參數之環境需求。

響應於決定環境係適用於開始一AC模組190，處理器110利用一適當誤差碼(區塊408)可以終止ENTERAC指令。另外，處理器110可以進一步抑制更多受信任軟體層以允許ENTERAC指令之行為。

否則，在區塊414中，處理器110可以更新事件程序以支援開始AC模組190。在ENTERAC指令之一實例實施例中，處理器110遮罩INTR、NMI、SMI、INIT及A20M事件之程序。其它開始AC指令及/或相關運算元可以說明遮罩較少、額外及/或不同事件。其它開始AC指令及/或相關運算元可以進一步默示說明遮罩之事件及/或不遮罩之事件。另外，其它實施例藉由導致計算裝置100執行受信任碼，例如，AC模組190響應於這種事件之事件簽章可以避免遮罩事件。

在區塊416中，處理器110可以鎖定處理器匯流排130，以防止其它處理器110及晶片組120在AC模組190之開始及執行時要求處理器匯流排130之擁有權。在ENTERAC指令之一實例實施例中，處理器110藉由產生其具有一LT.PROCESSOR.HOLD匯流排訊息提供其它處理器110及晶片組120之一特別處理，取得處理器匯流排130之專有權。開始AC指令及/或相關運算元之其它實施例可以說明維持釋放處理器匯流排130，或可以說明一不同方法以鎖定處理器匯流排130。

在區塊420中，處理器110可以組態其之私人記憶體160用於接收AC模組190。處理器110可以清除私人記憶體160之內容，及可以組態有關於私人記憶體160之控制結構以致能處理器110存取私人記憶體160。在ENTERAC指令之一實例實施例中，處理器110更新一或多個控制暫存器以切換快取記憶體112到快取如RAM模式，及使快取記憶體112之內容無效。

其它開始AC指令及/或相關運算元可以說明用於私人記憶體160之不同執行之私人記憶體參數(如圖1A-1E)。因此，為準備用於AC模組190之私人記憶體160，在執行這些其它開始AC指令中之處理器110可以執行不同操作。例如，處理器110可以致能/或組態有關於私人記憶體160之一記憶體控制器(如圖1E之PM控制器128)。處理器110也可以具有一清除、重設，及/或無效信號提供私人記憶體160以清除私人記憶體160。另外，處理器110可以寫入零或一些其它位元類型到私人記憶體160，從私人記憶體160關閉電力，及/或利用如藉由開始AC指令及/或運算元說明之一些其它裝置以清除私人記憶體160。

在區塊424中，處理器110載入AC模組190進入其之私人記憶體160。在ENTERAC指令之一實例實施例中，處理器110從藉由位址運算元說明之記憶體140之一位置開始讀取，直到傳送藉由長度運算元說明之一些位元組到其之快取記憶體112。開始AC指令及/或有關運算元之其它實施例依據一不同方法，可以說明用於載入AC模組190進入其之私人記憶體160之參數。例如，其它開始AC指令及/或有關運算元依據一些不同方法可以說明AC模組190之位置、私人記憶體160之位置，其中載入AC模組190，及/或AC模組190之終止於私人記憶體160中。

在區塊428中，處理器110可以進一步鎖定私人記憶體160。在ENTERAC指令之一實例實施例中，處理器110更新一或多個控制暫存器以鎖定其之快取記憶體112，防止外部

事件例如來自處理器及/或I/O裝置修改AC模組190之儲存線之偵測需求。然而，其它開始AC指令及/或有關運算元可以說明用於處理器110之其它操作。例如，處理器110可以組態有關於私人記憶體160之一記憶體控制器(如圖1E之PM控制器128)，以防止其它處理器110及/或晶片組120存取私人記憶體160。在一些實施例中，可以已經完全鎖定私人記憶體160，因此在區塊428中處理器110可以不採取行動。

在區塊432中，處理器決定是否儲存於其私人記憶體160中之AC模組190根據藉由ENTERAC指令之維護運算元說明之一維護裝置鑒認。在ENTERAC指令之一實例實施例中，處理器110擷取藉由維護運算元說明之一處理器密鑰116、晶片組密鑰124，及/或平台密鑰152。然後，處理器110使用擷取密鑰RSA解密AC模組190之簽章240以取得概要數值242。處理器110使用一SHA-1雜湊法進一步雜湊AC模組190以取得一計算概要數值。然後，處理器110決定AC模組190係響應於計算概要數值鑒認，及概要數值242具有一預期關聯(例如，互相相等)。否則，處理器110決定AC模組190係不鑒認。

其它開始AC指令及/或相關運算元可以說明不同鑒認參數。例如，其它開始AC指令及/或相關運算元可以說明一不同鑒認方法、不同加密演算法，及/或不同雜湊演算法。其它開始AC指令及/或相關運算元可以進一步說明用於鑒認AC模組190之不同密鑰長度、不同密鑰位置，及/或密

鑰。

響應於決定AC模組190係不鑒認，在區塊436中，處理器110產生一誤差碼及終止開始AC指令之執行。否則，在區塊440中，處理器110可以更新計算裝置100之安全狀態以支援AC模組190之執行。在ENTERAC指令之一實例實施例中，在區塊440中，處理器110寫入一開始私人指令到晶片組120之一指令暫存器126，以致能處理器110利用正常非特權讀取及寫入處理，通過私人空間142存取暫存器126。

其它開始AC指令及/或相關運算元可以說明其它操作以組態計算裝置100用於AC模組執行。例如，一開始AC指令及/或相關運算元可以說明處理器110依據其之目前狀態離開私人空間142。一開始AC指令及/或相關運算元也可以說明處理器110致能及/或抑制對明確計算資源，例如維護記憶體範圍、維護儲存裝置、儲存裝置之維護部分、儲存裝置之維護檔案等等之存取。

在更新計算裝置100之安全處理之後，在區塊444中，處理器110可以初始AC模組之執行。在ENTERAC指令之一實例實施例中，處理器110利用藉由模組運算元提供之實體位址，載入其之指令簽章暫存器316，導致處理器110跳到藉由實體位址說明之執行點260，及從執行點260執行AC模組190。其它開始AC指令及/或相關運算元依據一些變換方法可以說明執行點260之位置。例如，一開始AC指令及/或相關運算元可以導致處理器110從AC模組190本身取得執行點260之位置。

請即參考於圖5，具有說明終止一AC模組190之一方法500。尤其，方法500說明一處理器110響應於具有一維護運算元、一事件運算元，及一開始運算元之一實例EXITAC指令之操作。然而，一習於此技者沒有不對稱實驗，應該可以執行具有較少、額外，及/或不同運算元之其它終止AC指令。

在區塊504中，處理器110可以消除/或重建私人記憶體160以防止對儲存於私人記憶體160中之AC模組190之進一步存取。在EXITAC指令之一實施例中，處理器110使其之快取記憶體112無效，及更新控制暫存器以切換快取記憶體112到操作之正常快取模式。

一終止AC指令及/或相關運算元可以說明用於私人記憶體160之不同執行之私人記憶體參數(如圖1A-1E)。因此，為準備計算裝置100用於後AC碼執行，一終止AC指令及/或相關運算元可以導致處理器110執行不同操作。例如，處理器110可以抑制有關於私人記憶體160之一記憶體控制器(如圖1E之PM控制器128)，以防止對AC模組190之進一步存取。處理器110也可以具有一清除、重設，及/或無效信號提供私人記憶體160以清除私人記憶體160。另外，處理器110可以寫入零或一些其它位元類型到私人記憶體160，從私人記憶體160關閉電力，及/或利用如藉由開始AC指令及/或運算元說明之一些其它裝置以清除私人記憶體160。

在區塊506中，處理器110根據維護運算元，可以更新計

算裝置100之安全狀態以支援後AC碼執行。在EXITAC指令之一實例實施例中，維護運算元可以說明是否處理器110係關閉私人空間142或依據其之目前狀態離開私人空間142。響應於依據其之目前狀態離開私人空間142，處理器110進行到區塊510。否則，處理器110藉由寫入一關閉私人指令到指令暫存器126，關閉私人空間142以防止處理器110通過對私人空間142之正常無特權讀取及寫入處理，進一步存取指令暫存器126。

一終止AC指令及/或相關運算元之另一實施例可以導致處理器110更新計算裝置100之其它安全狀態，以支援在AC模組190之後之碼之執行。例如，一終止AC指令及/或相關運算元可以說明處理器110致能及/或抑制對明確計算資源，例如維護記憶體範圍、維護儲存裝置、儲存裝置之維護部分、儲存裝置之維護檔案等等之存取。

在區塊510中，處理器110可以釋放處理器匯流排130以致能其它處理器110及晶片組120要求處理器匯流排130之擁有權。在EXITAC指令之一實施例中，處理器110藉由產生提供具有一LT PROCESSOR.RELEASE匯流排訊息其它處理器110及晶片組120之一特定處理，釋放處理器匯流排130之專用權。終止AC指令及/或相關運算元之其它實施例可以說明處理器匯流排130係保持鎖定，或可以說明一不同方法釋放處理器匯流排130。

在區塊514中，處理器110根據遮罩運算元可以更新事件程序。在EXITAC指令之一實例實施例中，遮罩運算元說明

是否處理器110係致能事件程序或依據其之目前狀態離開事件程序。響應於決定依據其之目前狀態離開事件程序，處理器110進行到區塊516。否則，處理器110不遮罩INTR、NMI、SMI、INIT，及A20M事件以致能這種事件之程序。其它開始AC指令及/或相關運算元可以說明不遮罩較少、額外，及/或不同事件。其它開始AC指令及/或相關運算元可以進一步默示說明遮罩之事件及/或不遮罩之事件。

在區塊516中，處理器110終止AC模組190之執行，及開始藉由開始運算元說明之後AC碼。在EXITAC指令之一實例實施例中，處理器110利用一碼部分及藉由開始運算元說明之部分補償，更新其之碼部分暫存器及指令簽章暫存器。因此，處理器110跳到藉由碼部分及部分補償說明之後AC碼之一執行點及從執行點開始執行。

其它終止AC指令及/或相關運算元依據一些不同方法可以說明後AC碼之執行點。例如，一開始AC指令可以導致處理器110儲存目前指令簽章以識別後AC碼之執行點。在這一種實施例中，終止AC指令可以擷取藉由開始AC指令儲存之執行點，及從擷取之執行點初始後AC碼之執行。在本方法中，終止AC指令回報執行到採用開始AC指令之指令。進一步，在此一實施例中，顯示已經呼叫AC模組190，類似藉由要求碼之一功能呼叫或系統呼叫。

計算裝置100之另一實施例揭示於圖6中。計算裝置100包含處理器110、其提供處理器110對一記憶體空間640之存取之一記憶體界面620，及其提供處理器110對媒體180之存

取之一媒體界面170。記憶體空間640包含一位址空間，其可以延伸多個裝置可讀取媒體，處理器110可以由媒體，例如，韌體、系統記憶體140、私人記憶體160、硬碟儲存、網路儲存等等(如圖1A-1E)執行碼。記憶體空間640包含前AC碼642、一AC模組190，及後AC碼646。前AC碼642可以包含作業系統碼、系統庫碼、共享庫碼、應用碼、韌體程序、BIOS程序及/或其可以開始一AC模組190之執行之其它程序。後AC碼646同樣可以包含作業系統碼、系統庫碼、共享庫碼、應用碼、韌體程序、BIOS程序及/或其在AC模組190之後可以執行之其它程序。應該瞭解前AC碼642及後AC碼646可為相同軟體及/或韌體模組，或不同軟體及/或韌體模組。

在圖7A中說明開始及終止一AC模組190之一實例實施例。在區塊704中，計算裝置100響應於執行前AC碼642，儲存AC模組190進入記憶體空間640。在一實例實施例中，計算裝置100擷取來自一裝置可讀取媒體180通過媒體界面170之AC模組190，及儲存AC模組190於記憶體空間640中。例如，計算裝置100可以擷取來自韌體、一硬碟、系統記憶體、網路儲存、一檔案伺服器、一全球資訊網路伺服器等等之AC模組190，及儲存AC模組190進入計算裝置100之一系統記憶體140。

在區塊708中，計算裝置100響應於執行前AC碼642，載入、鑒認，及初始AC模組190之執行。例如，前AC碼642可以包含一ENTERAC指令，或另外開始AC指令，其導致計算裝

置100傳送AC模組190到記憶體空間640之私人記憶體160，鑒認AC模組190，及從前AC碼642之執行點要求AC模組190之執行。另外，前AC碼642可以包含一系列之指令，其導致計算裝置100傳送AC模組190到記憶體空間640之私人記憶體160，鑒認AC模組190，及從前AC碼642之執行點要求AC模組190之執行。

在區塊712中，計算裝置100執行AC模組190之碼210(如圖2)。在區塊716中，計算裝置100終止AC模組190之執行，及初始記憶體空間640之後AC碼646之執行。例如，AC模組190可以包含一EXITAC指令，或另外終止AC指令，其導致計算裝置100終止AC模組190之執行，更新計算裝置100之安全狀態，及從後AC碼646之一執行點初始後AC碼646之執行。另外，AC模組190可以包含一系列之指令，其導致計算裝置100終止AC模組190之執行，更新計算裝置100之安全狀態，及從後AC碼646之執行點初始後AC碼646之執行。

在圖7B中說明開始及終止一AC模組190之另一實例實施例。在區塊740中，計算裝置100響應於執行前AC碼642，儲存AC模組190進入記憶體空間640。在一實例實施例中，計算裝置100擷取來自一裝置可讀取媒體180通過媒體界面170之AC模組190，及儲存AC模組190於記憶體空間640中。例如，計算裝置100可以擷取來自軔體、一硬碟、系統記憶體、網路儲存、一檔案伺服器、一全球資訊網路伺服器等等之AC模組190，及儲存AC模組190進入計算裝置100之一系統記憶體140。

在區塊744中，計算裝置100響應於執行前AC碼642，載入、鑒認，及初始AC模組190之執行。在區塊744中，計算裝置進一步儲存用於其係根據指令簽章之後AC碼646之一執行點。例如，前AC碼642可以包含一ENTERAC指令，或另外開始AC指令，其導致計算裝置100傳送AC模組190到記憶體空間640之私人記憶體160，鑒認AC模組190，從前AC碼642之執行點要求AC模組190之執行，及儲存指令簽章以使處理器110在執行AC模組190之後可以回到採用開始AC指令之指令。另外，前AC碼642可以包含一系列之指令，其導致計算裝置100傳送AC模組190到記憶體空間640之私人記憶體160，鑒認AC模組190，從前AC碼642之執行點要求AC模組190之執行，及儲存指令簽章。

在區塊748中，計算裝置100執行AC模組190之碼210(如圖2)。在區塊752中，計算裝置100終止AC模組190之執行，及載入根據儲存於區塊744中之執行點之指令簽章，及初始採用開始AC指令之指令，或在區塊744中執行之系列之指令之執行。例如，AC模組190可以包含一EXITAC指令，或另外終止AC指令，其導致計算裝置100終止AC模組190之執行，更新計算裝置100之安全狀態，及從藉由儲存於區塊744中之指令簽章說明之後AC碼646之一執行點初始後AC碼646之執行。另外，AC模組190可以包含一系列之指令，其導致計算裝置100終止AC模組190之執行，更新計算裝置100之安全狀態，及從藉由儲存於區塊744中之指令簽章說明之後AC碼646之一執行點初始後AC碼646之執行。

圖8說明用於使用揭示技術之一設計之模擬、模仿，及製造之一些設計說明及格式。資料說明一設計可以說明依據一些方法之設計。第一，如在模擬方面係有用，可以使用一硬體說明語言，或其基本提供預期如何執行設計硬體之一計算化模式之其它功能說明語言說明硬體。硬體模型810係可以儲存於一儲存媒體800例如一電腦記憶體中，以使可以使用模擬軟體820來模擬模型，該模擬軟體820將一測試程式組830套用至該硬體模型810，以決定如果真正功能係如需求。在一些實施例中，模擬軟體係不記錄、捕捉，及包含於媒體中。

另外，在設計程序之一些級可以產生具有邏輯及/或電晶體閘之一電路位準模型。有時藉由其使用可程式化邏輯組成模型之專用硬體模擬器同樣可以模擬本模型。取得一進一步程度之本類型之模擬可以係一模仿技術。在任何狀態中，可重建硬體係另一實施例，其可以要求一裝置可讀取媒體利用揭示之技術儲存一模型。

而且，大部分設計，在一些級，到達說明在硬體模型中之一些裝置之實體配置方式之資料之一位準。在其中使用習知半導體製造技術之狀態中，說明硬體模型之資料可以係說明在用於產生積體電路之遮罩之不同遮罩層上之一些特徵之出現及消失之資料。再次，說明積體電路之資料包含在依據資料可以模擬或製造，以執行這些技術之電路或邏輯中揭示之技術。

在設計之任何說明中，資料係可以儲存於任何格式之一

電腦可讀取媒體中。調變或反之產生傳送這種資訊之一光學或電子波860、一記憶體850，或一磁性或光學儲存840例如一碟片可以係該媒體。說明設計或設計之特定部分之位元組係其本身係可以購買，及藉由其它文件使用於進一步設計或製造之一文件。

儘管明確例示之實施例已經說明及在附圖中揭示，可以瞭解的是這些實施例僅係說明及非限制本發明，且本發明並不限於已揭示及說明之特定結構及配置方式，因為習於此技者可利用學習本揭示而產生一些其它修改。

圖式簡單說明

本發明係藉由舉例說明且不為附圖所限制，為了說明之簡化及清晰，在圖式中說明之元件並不需要依據比例繪製。例如，為了清晰可以相對於其它元件誇大一些元件之尺寸。再者，其中考慮到對稱，在圖式之間已經重複參考數字，以指示相應或類似元件。

圖1A-1E說明具有私人記憶體之一計算裝置之舉例實施例。

圖2說明其可以藉由在圖1A-1E中所示之計算裝置開始之一實例鑒認碼(AC)模組。

圖3說明在圖1A-1E中所示之計算裝置之一處理器之一舉例實施例。

圖4說明開始在圖2中所示之AC模組之一實例方法。

圖5說明終止在圖2中所示之AC模組之執行之一實例方法。

圖6說明在圖1A-1E中所示之計算裝置之另一實施例。

圖7A-7B說明開始及終止在圖2中所示之AC模組之執行之一實例方法。

圖8說明用於模擬、模仿及/或測試在圖1A-1E中所示之計算裝置之處理器之一系統。

圖式代表符號說明

| | |
|---|---|
| 100 | 計算裝置 |
| 110 | 處理器 |
| 112、360 | 快取記憶體 |
| 114 | 控制暫存器 |
| 116 | 密鑰 |
| 120 | 晶片組 |
| 122 | 記憶體控制器 |
| 124 | 晶片組密鑰 |
| 126 | 受信任平台暫存器 |
| 128 | 私人記憶體控制器 |
| 130 | 處理器匯流排 |
| 140 | 系統記憶體 |
| 142 | 私人空間 |
| 144 | 公共空間 |
| 150 | 實體符記 |
| 152 | 平台密鑰 |
| 160 | 私人記憶體 |
| 170 | 媒體界面 |

| | |
|---|---|
| 180 | 媒體 |
| 190 | 鑒認碼模組 |
| 210 | 碼 |
| 212 | 碼傳呼 |
| 220 | 資料 |
| 222 | 資料傳呼 |
| 230 | 表頭 |
| 240 | 簽章 |
| 242 | 概要數值 |
| 250 | 模組標印器 |
| 260 | 執行點 |
| 302 | 前端 |
| 304 | 處理器匯流排界面 |
| 306 | 暫存器檔案 |
| 312 | 一般用途暫存器 |
| 314 | 指令暫存器 |
| 316 | 指令點暫存器 |
| 318 | 狀態/控制暫存器 |
| 320 | 其它暫存器 |
| 330 | 取得單元 |
| 340 | 解碼器 |
| 350 | 指令排序 |
| 370 | 執行單元 |
| 380 | 退出單元 |
| 400、500 | 方法 |
| 620 | 記憶體界面 |

| | |
|---|---|
| 640 | 記憶體空間 |
| 642 | 前AC碼 |
| 646 | 後AC碼 |
| 800 | 儲存媒體 |
| 810 | 硬體模型 |
| 820 | 模擬軟體 |
| 830 | 測試程式組 |
| 840 | 儲存裝置 |
| 850 | 記憶體 |
| 860 | 波 |

## 肆、中文發明摘要

本發明提供一種載入、鑒認及/或執行儲存於一私人記憶體中之鑒認碼模組之裝置及方法。

## 伍、英文發明摘要

Apparatus and method load, authenticate, and/or execute authenticated code modules stored in a private memory.

# 拾、申請專利範圍

1. 一種方法，包含：

傳送一鑒認碼到一私人記憶體；及

執行儲存於該私人記憶體中之該鑒認碼模組，以響應於決定儲存於該私人記憶體中之該鑒認碼模組係有效。

2. 如申請專利範圍第1項之方法，其中傳送進一步包含傳送藉由一記憶體之一運算元所指定之數個位元組。

3. 如申請專利範圍第1項之方法，進一步包含：

組態該處理器之一快取記憶體以類似一隨機存取記憶體方式運作，

其中傳送包含儲存該鑒認碼模組於該快取記憶體中。

4 如申請專利範圍第3項之方法，進一步包含在儲存該鑒認碼模組於該快取記憶體中之前使該快取記憶體無效。

5. 如申請專利範圍第3項之方法，進一步包含鎖定該快取記憶體以防止取代該鑒認碼模組之線。

6. 如申請專利範圍第1項之方法，進一步包含根據該鑒認碼模組之一數位簽章決定該鑒認碼是否有效。

7. 如申請專利範圍第1項之方法，進一步包含：

從儲存於該私人記憶體中之該鑒認碼模組取得一第一數值；

從該鑒認碼模組計算一第二數值；及

響應於具有一預定關聯之該第一及該第二數值而決定該鑒認碼模組係有效。

8. 如申請專利範圍第1項之方法，進一步包含

擷取一密鑰；

利用該密鑰解密該鑒認碼模組之一數位簽章以取得一第一數值；

雜湊該鑒認碼模組以取得一第二數值；及

響應於具有一預定關聯之該第一及第二數值而執行該鑒認碼模組。

9. 如申請專利範圍第8項之方法，其中

解密包含使用該密鑰以RSA解密該數位簽章；及

雜湊包含施加一SHA-1雜湊搜尋法於該鑒認碼模組以取得該第二數值。

10. 如申請專利範圍第8項之方法，進一步包含從該處理器擷取該密鑰。

11. 如申請專利範圍第8項之方法，進一步包含從一晶片組擷取該密鑰。

12. 如申請專利範圍第8項之方法，進一步包含從一符記擷取該密鑰。

13. 如申請專利範圍第1項之方法，其中傳送包含從一裝置可讀取媒體接收該鑒認碼模組。

14. 一種計算裝置，包含：

一晶片組；

一記憶體，其耦合於該晶片組；

一裝置可讀取媒體界面，用以從一裝置可讀取媒體接收一鑒認碼模組；

一私人記憶體，其耦合於該晶片組；及

一處理器，用於將該鑒認碼模組從該裝置可讀取媒體界面將該鑒認碼模組從該裝置可讀取媒體界面傳送到該私人記憶體，及用於鑒認儲存於該私人記憶體中之該鑒認碼模組。

15.如申請專利範圍第14項之裝置，其中該晶片組包含一耦合於該記憶體之記憶體控制器及一耦合於該私人記憶體之分離私人記憶體控制器。

16.如申請專利範圍第14項之裝置，其中

該晶片組包含一密鑰，及

該處理器根據該晶片組之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

17.如申請專利範圍第14項之裝置，其中

該處理器包含一密鑰及根據該處理器之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

18.如申請專利範圍第14項之裝置，進一步包含

一符記，其耦合於該晶片組，該符記包含一密鑰，其中該處理器根據該符記之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

19.一種計算裝置，其包含

一晶片組；

一裝置可讀取媒體界面，用於從一裝置可讀取媒體接收一鑒認碼模組；及

一處理器，其通過一處理器匯流排耦合於該晶片組，該處理器將該鑒認碼模組從該裝置可讀取媒體界面傳

送到該處理器之一私人記憶體，及用於鑒認儲存於該私人記憶體中之該鑒認碼模組。

20.如申請專利範圍第19項之裝置，其中該私人記憶體係通過一專用匯流排耦合於該處理器。

21.如申請專利範圍第19項之裝置，其中該私人記憶體係在該處理器內。

22.如申請專利範圍第19項之裝置，其中該私人記憶體包含該處理器之內部快取記憶體。

23.如申請專利範圍第19項之裝置，進一步包含

其它處理器，該等其它處理器通過該處理器匯流排耦合於該晶片組；其中

該處理器進一步鎖定該處理器匯流排以防止該其它處理器修改該鑒認碼模組。

24.一種計算裝置，包含

一記憶體；

一晶片組，包含一用於定義該記憶體之一部分為私人記憶體之記憶體控制器；

一裝置可讀取媒體界面，用於從一裝置可讀取媒體接收一鑒認碼模組；及

一處理器，用於將該鑒認碼模組從該裝置可讀取媒體界面傳送到該處理器之一私人記憶體，及用於鑒認儲存於該私人記憶體中之該鑒認碼模組。

25.如申請專利範圍第24項之裝置，其中該晶片組包含一耦合於該記憶體之記憶體控制器及一耦合於該私人記憶

體之分離私人記憶體控制器。

26.如申請專利範圍第24項之裝置，其中

該晶片組包含一密鑰，及

該處理器根據該晶片組之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

27.如申請專利範圍第24項之裝置，其中

該處理器包含一密鑰及根據該處理器之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

28.如申請專利範圍第24項之裝置，進一步包含

一符記，其包含一密鑰，其中

該處理器根據該符記之該密鑰鑒認儲存於該私人記憶體中之該鑒認碼模組。

29.一種裝置可讀取媒體，包含響應執行之一或多個指令，用以導致一計算裝置執行下列動作

傳送一鑒認碼到有關於一處理器之一私人記憶體；及

執行儲存於該私人記憶體中之該鑒認碼模組，以響應於決定儲存於該私人記憶體中之該鑒認碼模組係有效。

30.如申請專利範圍第29項之裝置可讀取媒體，其中響應執行之該等一或多個指令導致該計算裝置執行下列動作

根據該鑒認碼模組之一數位簽章決定該鑒認碼是否有效。

31.如申請專利範圍第29項之裝置可讀取媒體，其中響應執行之該等一或多個指令導致該計算裝置執行下列動作

從儲存於該私人記憶體中之該鑒認碼模組取得一第

一數值；

從該鑒認碼模組計算一第二數值；及

響應於具有一預定關聯之該第一及該第二數值而決定該鑒認碼模組係有效。

32.如申請專利範圍第29項之裝置可讀取媒體，其中響應執行之該等一或多個指令導致該計算裝置執行下列動作

擷取一不對稱密鑰；

利用該不對稱密鑰解密該鑒認碼模組之一數位簽章以取得一第一數值；

雜湊該鑒認碼模組以取得一第二數值；及

響應於具有一預定關聯之該第一及該第二數值而初始執行該鑒認碼模組。

33.如申請專利範圍第29項之裝置可讀取媒體，其中該等一或多個指令包含一開始指令，用以響應執行而導致該計算裝置執行下列動作

擷取一不對稱密鑰；

利用該不對稱密鑰解密該鑒認碼模組之一數位簽章以取得一第一數值；

雜湊該鑒認碼模組以取得一第二數值；及

響應於具有一預定關聯之該第一及該第二數值而初始執行該鑒認碼模組。

34.如申請專利範圍第33項之裝置可讀取媒體，其中響應執行之該等一或多個指令導致該計算裝置執行下列動作

通過一裝置可讀取媒體界面接收該鑒認碼模組。

# 拾壹、圖式

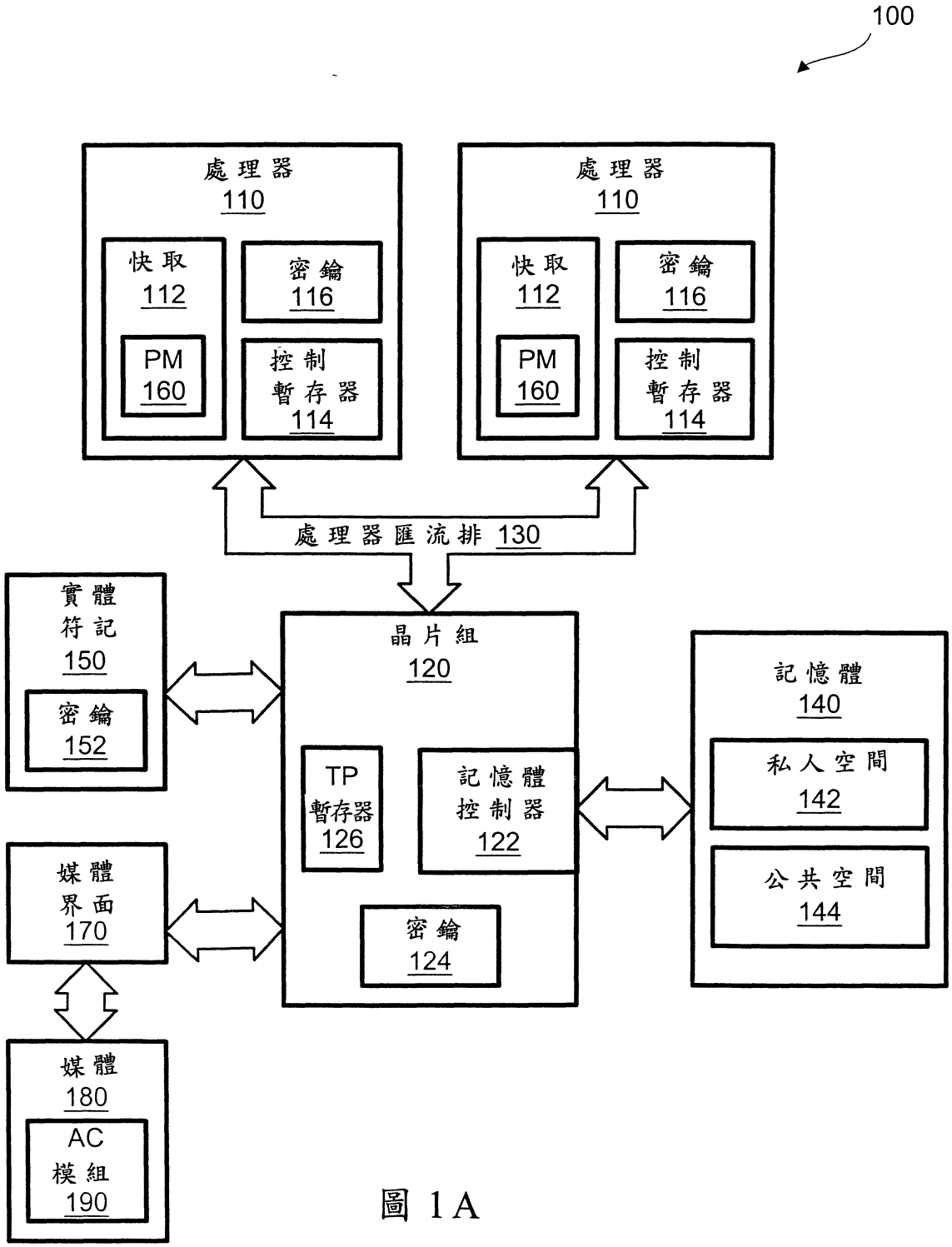
100
處理器
110
快取
112
密鑰
116
PM
160
控制
暫存器
114
處理器
110
快取
112
密鑰
116
PM
160
控制
暫存器
114
處理器匯流排 130
實體
符記
150
密鑰
152
晶片組
120
TP
暫存器
126
記憶體
控制器
122
密鑰
124
記憶體
140
私人空間
142
公共空間
144
媒體
界面
170
媒體
180
AC
模組
190

圖 1A

圖式續頁

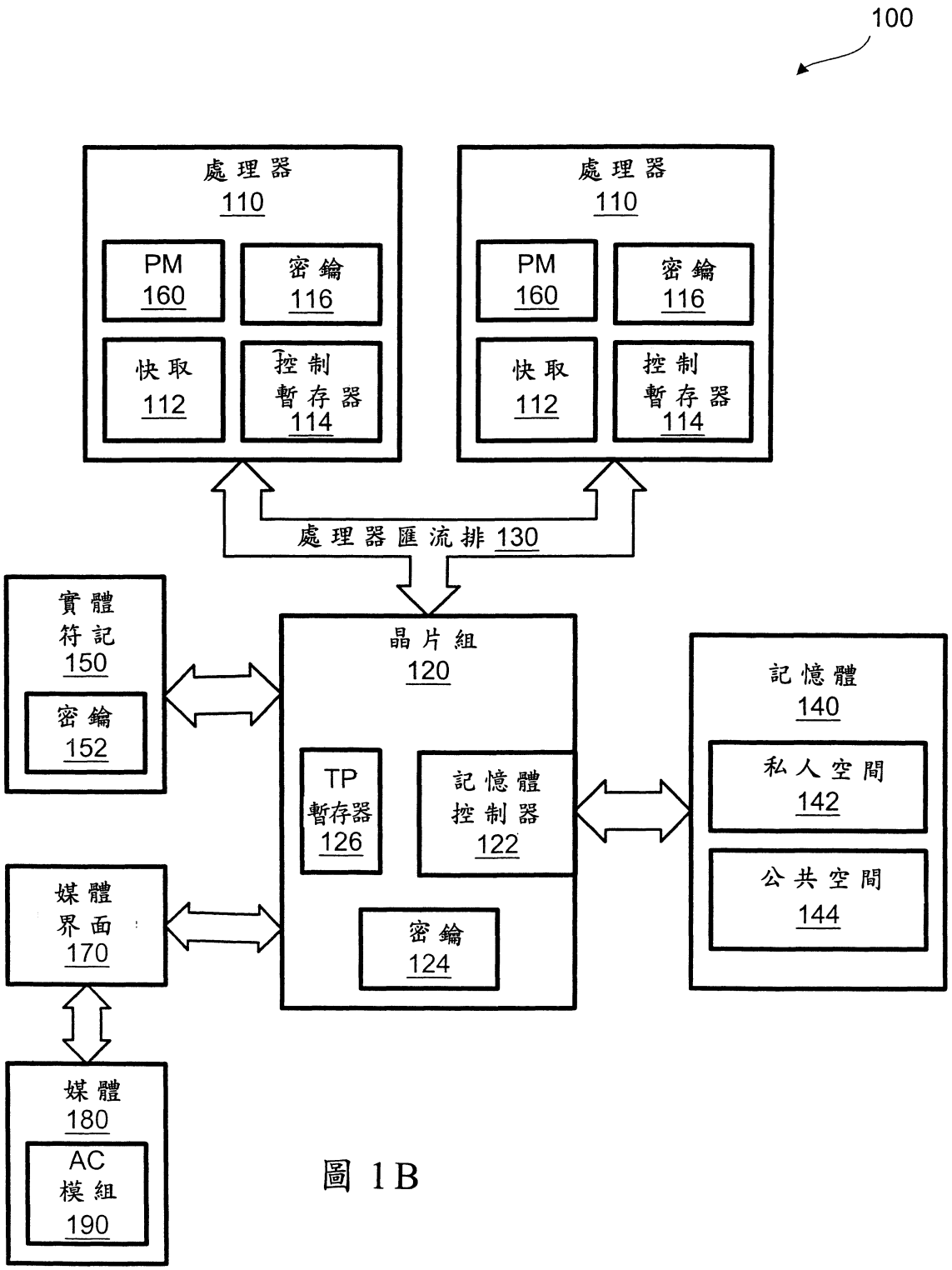
100
處理器
110
PM
160
密鑰
116
快取
112
控制
暫存器
114
處理器
110
PM
160
密鑰
116
快取
112
控制
暫存器
114
處理器匯流排 130
實體
符記
150
密鑰
152
晶片組
120
TP
暫存器
126
記憶體
控制器
122
密鑰
124
記憶體
140
私人空間
142
公共空間
144
媒體
界面
170
媒體
180
AC
模組
190

圖 1B

圖式續頁

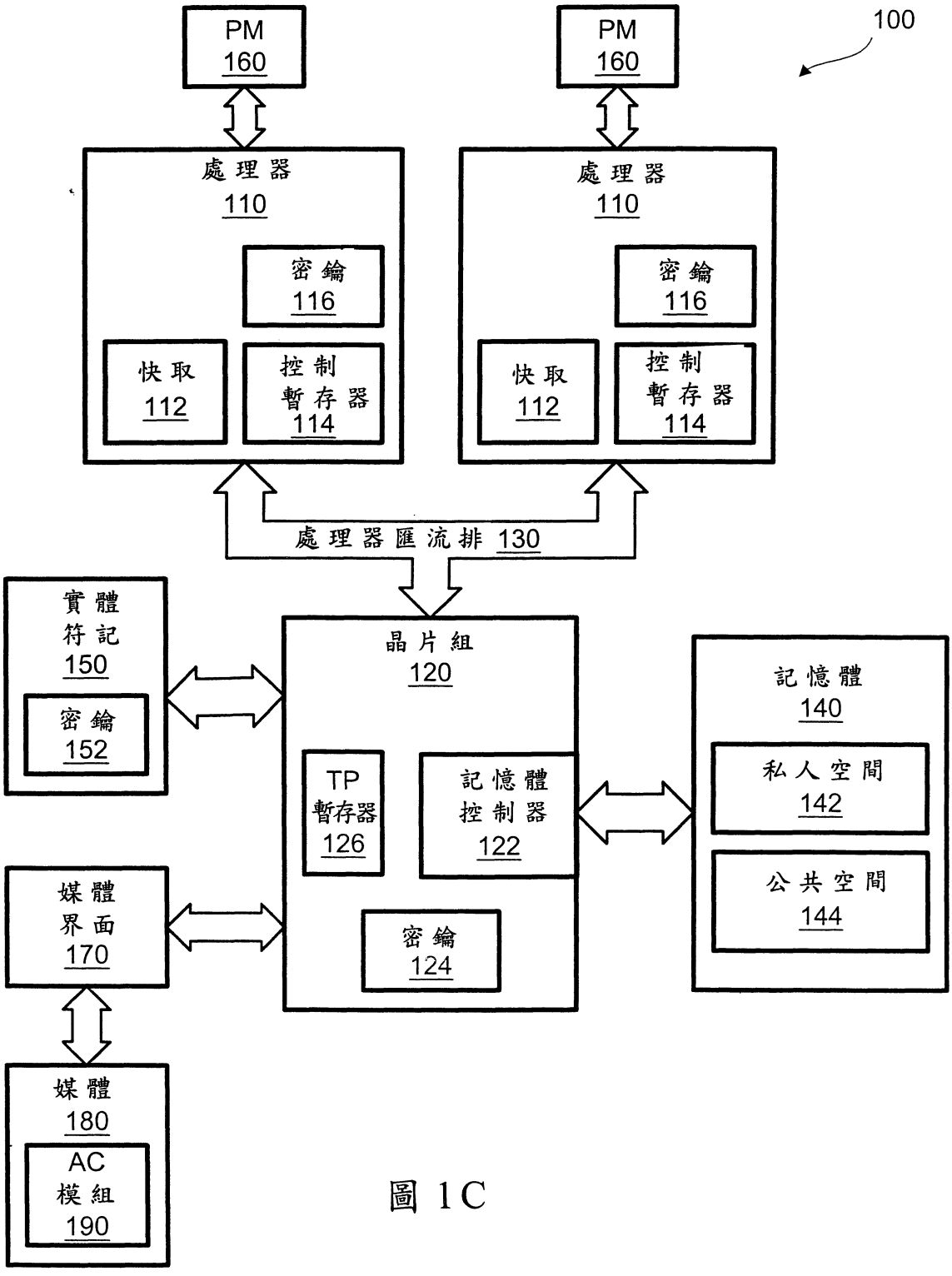
100
PM
160
PM
160
處理器
110
處理器
110
密鑰
116
密鑰
116
快取
112
控制
暫存器
114
快取
112
控制
暫存器
114
處理器匯流排 130
實體
符記
150
密鑰
152
晶片組
120
TP
暫存器
126
記憶體
控制器
122
密鑰
124
記憶體
140
私人空間
142
公共空間
144
媒體
界面
170
媒體
180
AC
模組
190

圖 1C

圖式續頁

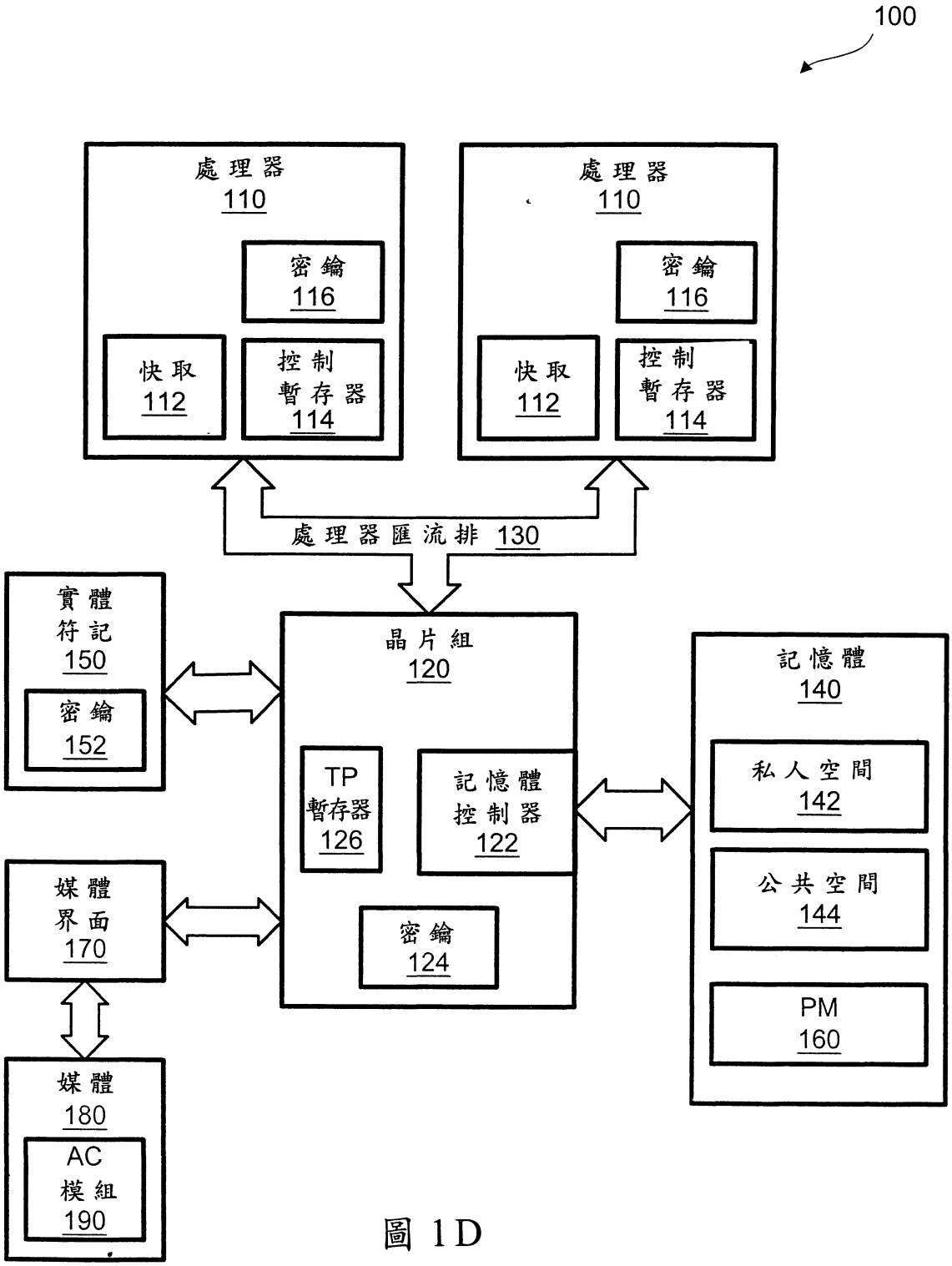
100
處理器
110
密鑰
116
快取
112
控制
暫存器
114
處理器
110
密鑰
116
快取
112
控制
暫存器
114
處理器匯流排 130
實體
符記
150
密鑰
152
晶片組
120
TP
暫存器
126
記憶體
控制器
122
密鑰
124
記憶體
140
私人空間
142
公共空間
144
PM
160
媒體
界面
170
媒體
180
AC
模組
190

圖 1D

圖式續頁

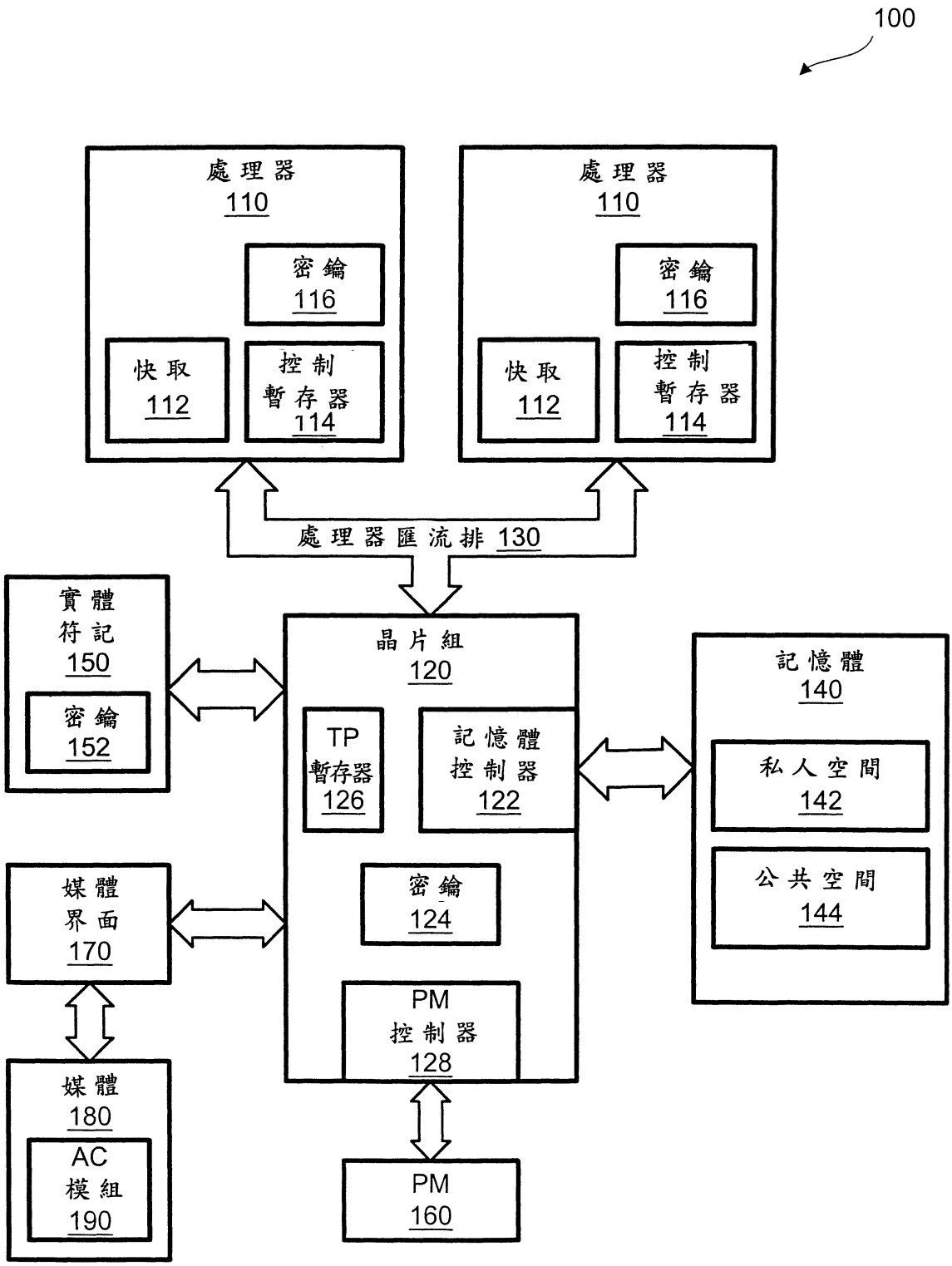
100
處理器
110
密鑰
116
快取
112
控制
暫存器
114
處理器
110
密鑰
116
快取
112
控制
暫存器
114
處理器匯流排 130
實體
符記
150
密鑰
152
晶片組
120
TP
暫存器
126
記憶體
控制器
122
記憶體
140
私人空間
142
公共空間
144
密鑰
124
媒體
界面
170
PM
控制器
128
媒體
180
AC
模組
190
PM
160

圖 1E

圖式續頁

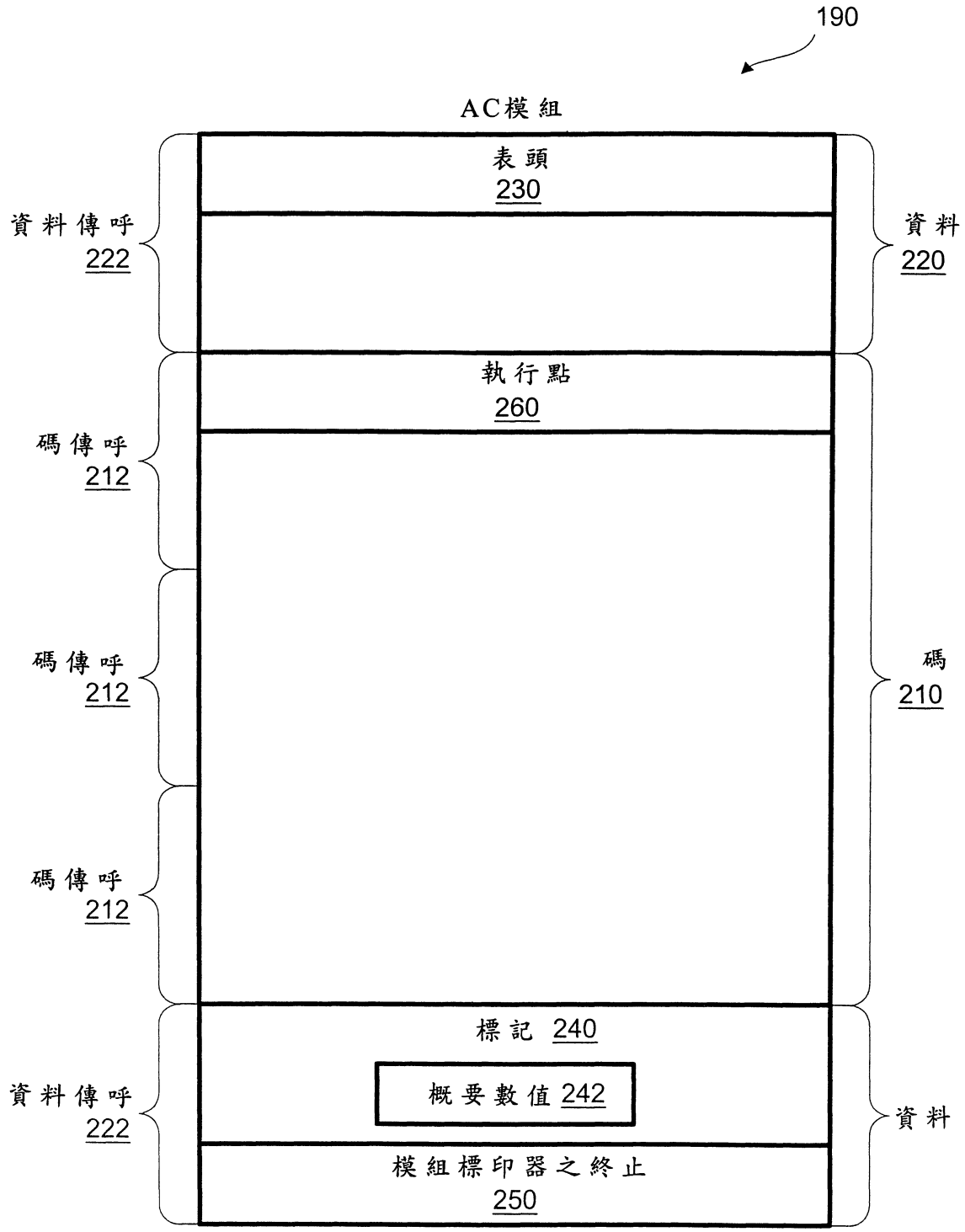
190
AC模組
表頭
230
執行點
260
標記 240
概要數值 242
模組標印器之終止
250
資料傳呼
222
碼傳呼
212
碼傳呼
212
碼傳呼
212
資料傳呼
222
資料
220
碼
210
資料

圖 2

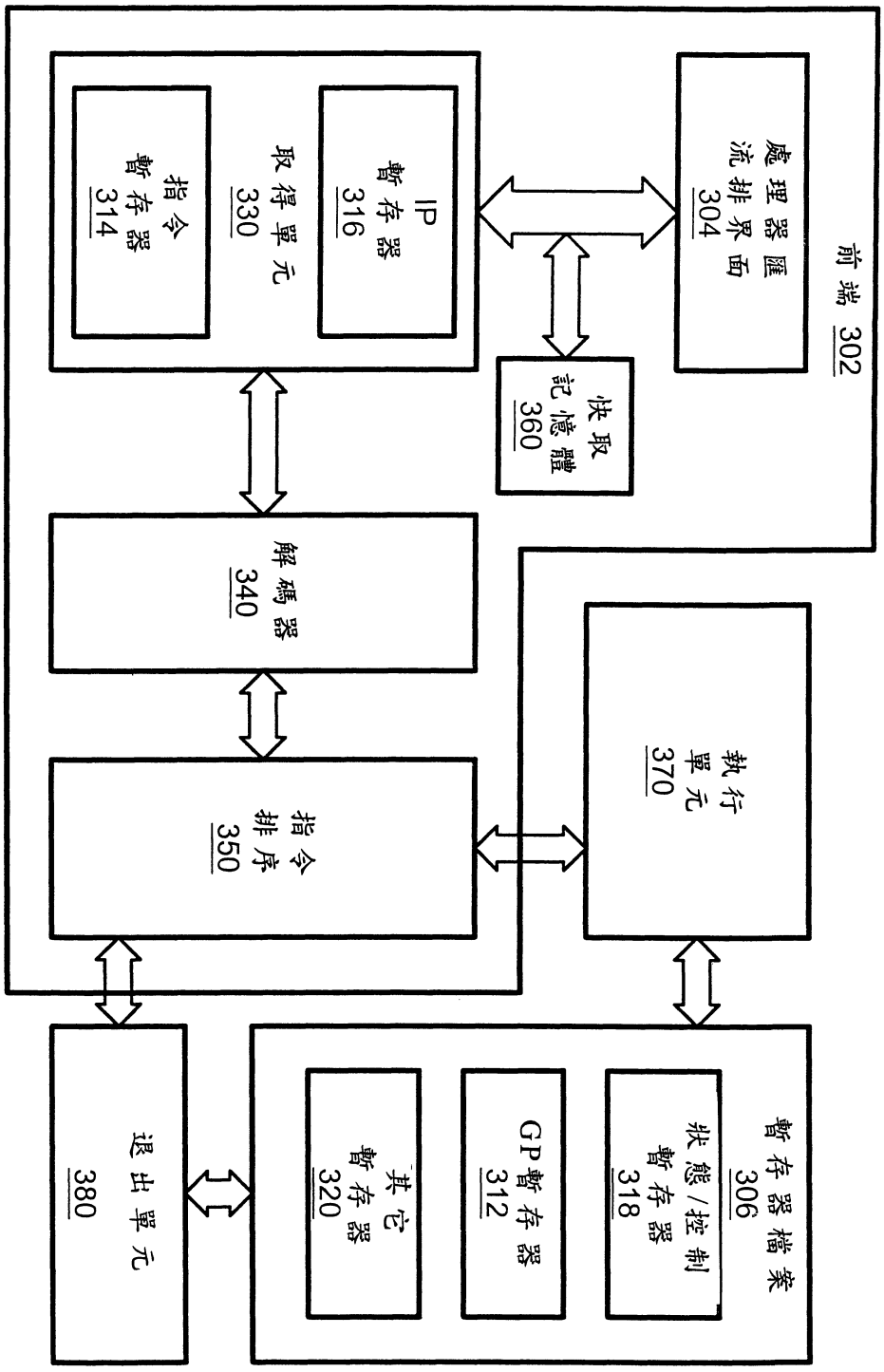
前端 302
處理器匯流排界面 304
快取記憶體 360
取得單元 330
IP 暫存器 316
指令暫存器 314
解碼器 340
指令排序 350
執行單元 370
暫存器檔案 306
狀態/控制暫存器 318
GP暫存器 312
其它暫存器 320
退出單元 380

圖 3

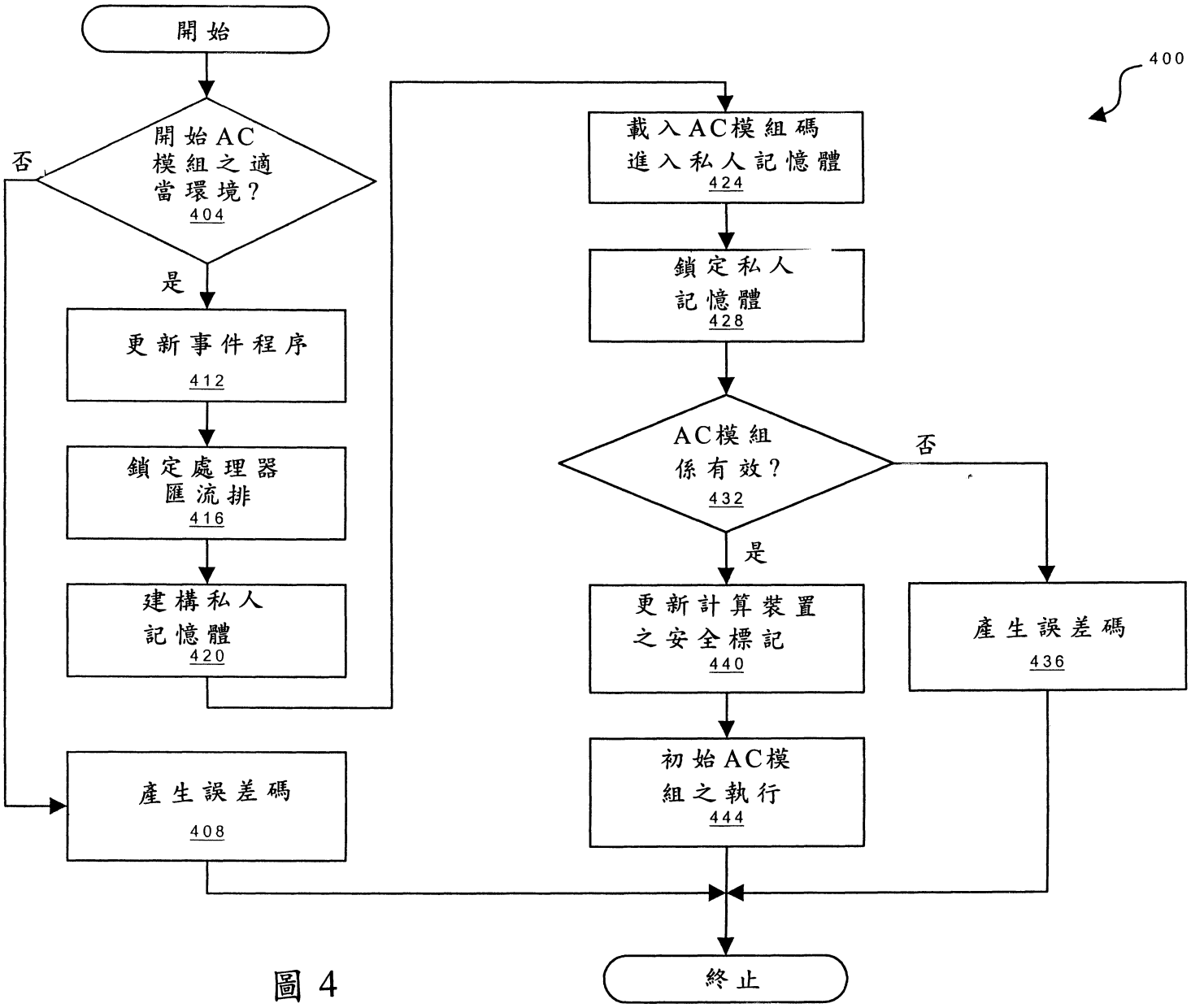
開始
開始AC模組之適當環境？
404
否
是
更新事件程序
412
鎖定處理器匯流排
416
建構私人記憶體
420
產生誤差碼
408
載入AC模組碼進入私人記憶體
424
鎖定私人記憶體
428
AC模組係有效？
432
否
是
更新計算裝置之安全標記
440
初始AC模組之執行
444
產生誤差碼
436
終止
400

圖 4

圖式續頁

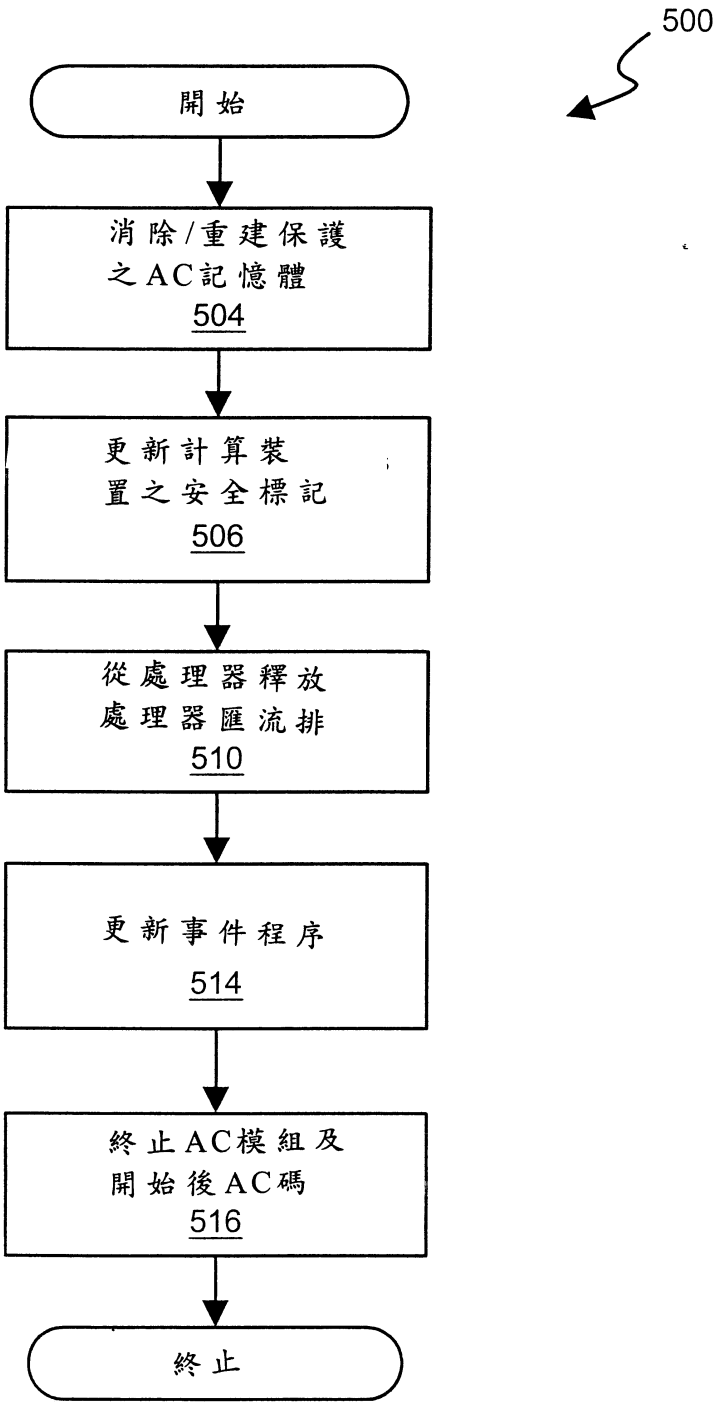
500
開始
消除/重建保護之AC記憶體
504
更新計算裝置之安全標記
506
從處理器釋放處理器匯流排
510
更新事件程序
514
終止AC模組及開始後AC碼
516
終止

圖 5

圖式續頁

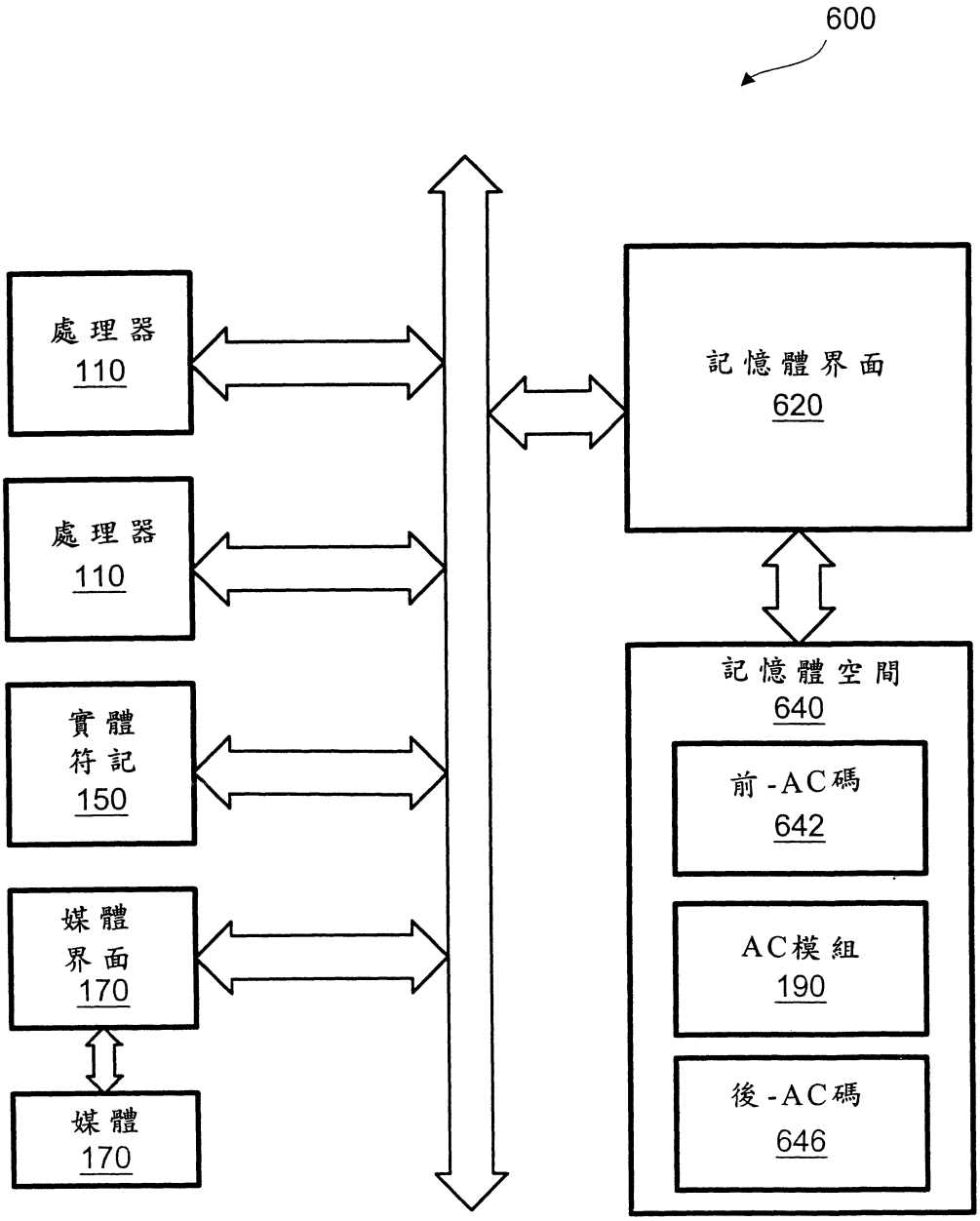
600
處理器
110
處理器
110
實體
符記
150
媒體
界面
170
媒體
170
記憶體界面
620
記憶體空間
640
前-AC碼
642
AC模組
190
後-AC碼
646

圖 6

圖式續頁

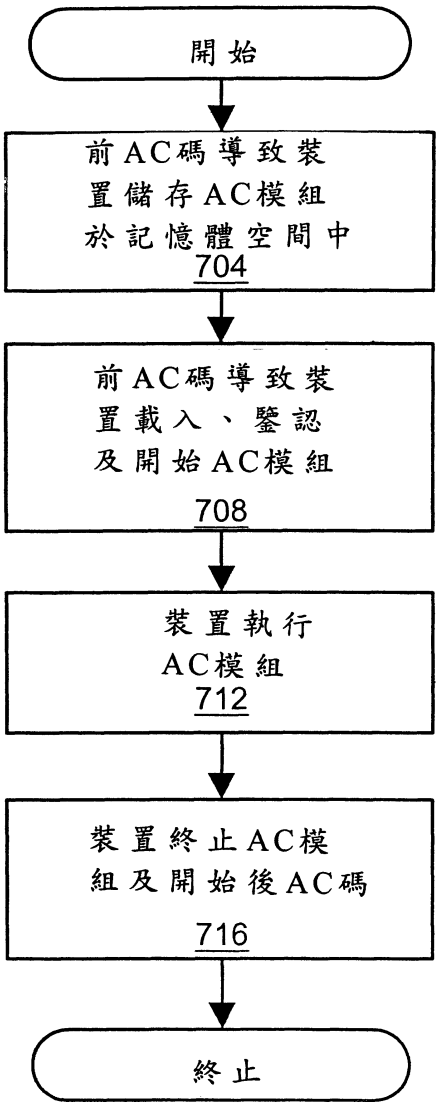
開始
前AC碼導致裝置儲存AC模組於記憶體空間中 704
前AC碼導致裝置載入、鑒認及開始AC模組 708
裝置執行AC模組 712
裝置終止AC模組及開始後AC碼 716
終止

圖 7A

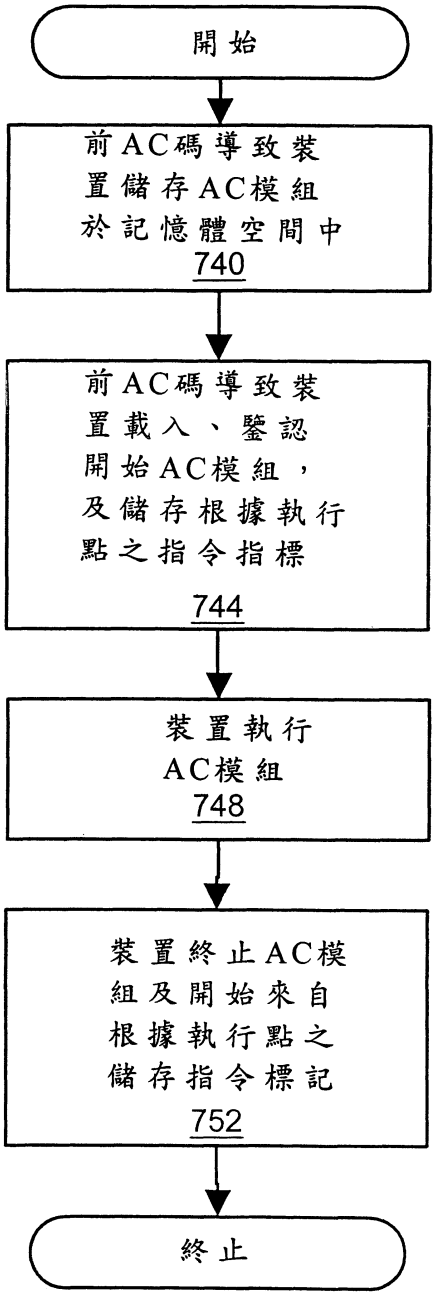
開始
前AC碼導致裝置儲存AC模組於記憶體空間中 740
前AC碼導致裝置載入、鑒認開始AC模組，及儲存根據執行點之指令指標 744
裝置執行AC模組 748
裝置終止AC模組及開始來自根據執行點之儲存指令標記 752
終止

圖 7B

圖式續頁

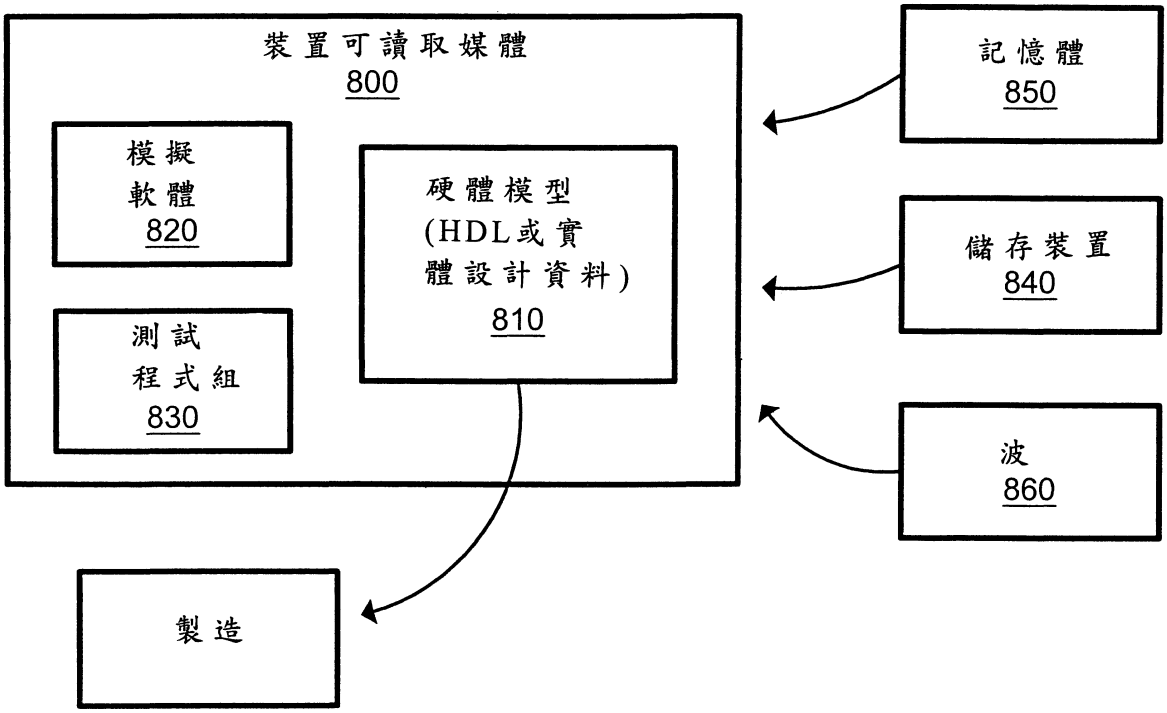
裝置可讀取媒體
800
模擬
軟體
820
測試
程式組
830
硬體模型
(HDL或實
體設計資料)
810
製造
記憶體
850
儲存裝置
840
波
860

圖 8

陸、(一)、本案指定代表圖為：第 1A 圖

(二)、本代表圖之元件代表符號簡單說明：

| | | | |
|---|---|---|---|
| 100 | 計算裝置 | 140 | 系統記憶體 |
| 110 | 處理器 | 142 | 私人空間 |
| 112 | 快取記憶體 | 144 | 公共空間 |
| 114 | 控制暫存器 | 150 | 實體符記 |
| 116 | 密鑰 | 152 | 平台密鑰 |
| 120 | 晶片組 | 160 | 私人記憶體 |
| 122 | 記憶體控制器 | 170 | 媒體界面 |
| 124 | 晶片組密鑰 | 180 | 媒體 |
| 126 | 受信任操作台暫存器 | 190 | 鑒認碼模組 |
| 130 | 處理器匯流排 | | |

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：