



(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 201447584 A

(43)公開日：中華民國 103 (2014) 年 12 月 16 日

(21)申請案號：103107462

(22)申請日：中華民國 103 (2014) 年 03 月 05 日

(51)Int. Cl. : **G06F12/14 (2006.01)**

G06F21/79 (2013.01)

(30)優先權：2013/03/05 美國

13/785,979

(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：曾湯瑪士 ZENG, THOMAS (US)；圖茲尼艾茲狄恩 TOUZNI, AZZEDINE (FR)；曾宗仁 TZENG, TZUNG REN (US)；波士黎斐爾 J BOSTLEY, PHIL J. (US)

(74)代理人：李世章

申請實體審查：有 申請專利範圍項數：19 項 圖式數：8 共 45 頁

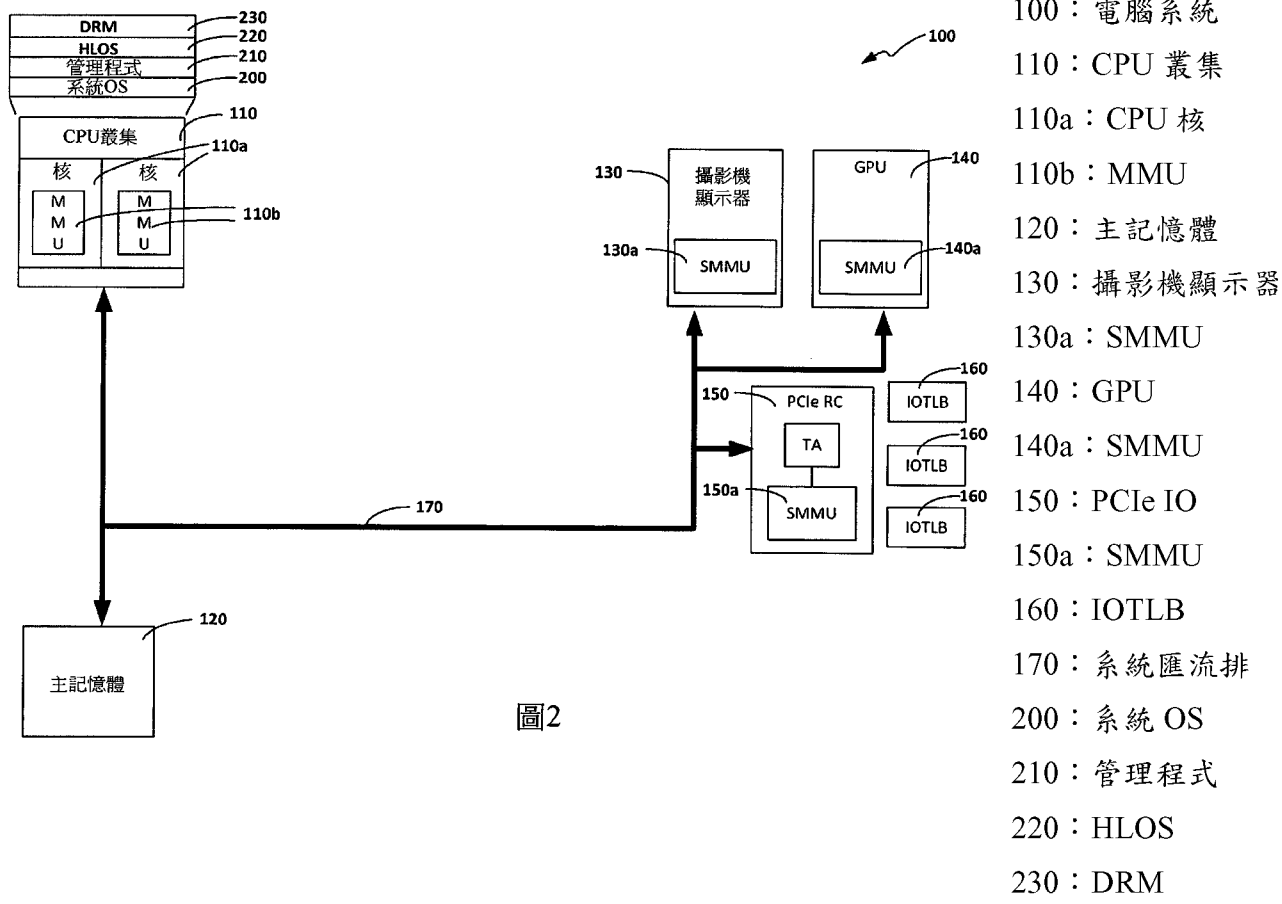
(54)名稱

用於在執行硬體表搜尋〈HWTW〉時在某些條件下防止對暫存器的內容的未經授權式存取的方法和裝置

METHOD AND APPARATUS FOR PREVENTING UNAUTHORIZED ACCESS TO CONTENTS OF A REGISTER UNDER CERTAIN CONDITIONS WHEN PERFORMING A HARDWARE TABLE WALK (HWTW)

(57)摘要

提供了用於執行安全性演算法的安全性裝置和方法，該安全性演算法防止對因在硬體表搜尋期間執行預測演算法故而已被載入到電腦系統的儲存元件中的實體位址(PA)的內容的未經授權式存取，該預測演算法使用預測器來基於虛擬位址(VA)預測 PA。在啟用預測器時，具有關於該系統的知識的人有可能將預測器配置成使得儲存在主記憶體的安全部分的 PA 處的內容被載入到 TLB 中的暫存器中。如此，不應當存取儲存在主記憶體的安全部分中的內容的人可以間接地獲得對彼等內容的未經授權式存取。該裝置和方法經由在某些條件下掩蔽該等內容來防止對該等內容的此類未經授權式存取。





(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 201447584 A

(43)公開日：中華民國 103 (2014) 年 12 月 16 日

(21)申請案號：103107462

(22)申請日：中華民國 103 (2014) 年 03 月 05 日

(51)Int. Cl. : **G06F12/14 (2006.01)**

G06F21/79 (2013.01)

(30)優先權：2013/03/05 美國

13/785,979

(71)申請人：高通公司(美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：曾湯瑪士 ZENG, THOMAS (US)；圖茲尼艾茲狄恩 TOUZNI, AZZEDINE (FR)；曾宗仁 TZENG, TZUNG REN (US)；波士黎斐爾 J BOSTLEY, PHIL J. (US)

(74)代理人：李世章

申請實體審查：有 申請專利範圍項數：19 項 圖式數：8 共 45 頁

(54)名稱

用於在執行硬體表搜尋〈HWTW〉時在某些條件下防止對暫存器的內容的未經授權式存取的方法和裝置

METHOD AND APPARATUS FOR PREVENTING UNAUTHORIZED ACCESS TO CONTENTS OF A REGISTER UNDER CERTAIN CONDITIONS WHEN PERFORMING A HARDWARE TABLE WALK (HWTW)

(57)摘要

提供了用於執行安全性演算法的安全性裝置和方法，該安全性演算法防止對因在硬體表搜尋期間執行預測演算法故而已被載入到電腦系統的儲存元件中的實體位址(PA)的內容的未經授權式存取，該預測演算法使用預測器來基於虛擬位址(VA)預測 PA。在啟用預測器時，具有關於該系統的知識的人有可能將預測器配置成使得儲存在主記憶體的安全部分的 PA 處的內容被載入到 TLB 中的暫存器中。如此，不應當存取儲存在主記憶體的安全部分中的內容的人可以間接地獲得對彼等內容的未經授權式存取。該裝置和方法經由在某些條件下掩蔽該等內容來防止對該等內容的此類未經授權式存取。

發明摘要

※ 申請案號：103107462

※ 申請日：103 年 3 月 5 日

※IPC 分類：G06F 1/14 (2006.01)
G06F 1/19 (2013.01)

【發明名稱】（中文/英文）

用於在執行硬體表搜尋（HWTW）時在某些條件下防止對暫存器的內容的未經授權式存取的方法和裝置

METHOD AND APPARATUS FOR PREVENTING
UNAUTHORIZED ACCESS TO CONTENTS OF A
REGISTER UNDER CERTAIN CONDITIONS WHEN
PERFORMING A HARDWARE TABLE WALK (HWTW)

【中文】

提供了用於執行安全性演算法的安全性裝置和方法，該安全性演算法防止對因在硬體表搜尋期間執行預測演算法故而已被載入到電腦系統的儲存元件中的實體位址（PA）的內容的未經授權式存取，該預測演算法使用預測器來基於虛擬位址（VA）預測PA。在啓用預測器時，具有關於該系統的知識的人有可能將預測器配置成使得儲存在主記憶體的安全部分的PA處的內容被載入到TLB中的暫存器中。如此，不應當存取儲存在主記憶體的安全部分中的內容的人可以間接地獲得對彼等內容的未經授權式存取。該裝置和方法經由在某些條件下掩蔽該等內容來防止對該等內容的此類未經授權式存取。

【英文】

A security apparatus and method are provided for performing a security algorithm that prevents unauthorized access to contents of a physical address (PA) that have been loaded into a storage element of the computer system as a result of performing a prediction algorithm during a hardware table walk that uses a predictor to predict a PA based on a virtual address (VA). When the predictor is enabled, it might be possible for a person with knowledge of the system to configure the predictor to cause contents stored at a PA of a secure portion of the main memory to be loaded into a register in the TLB. In this way, a person who should not have access to contents stored in secure portions of the main memory could indirectly gain unauthorized access to those contents. The apparatus and method prevent such unauthorized access to the contents by masking the contents under certain conditions.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

100 電腦系統

110 CPU 叢集

110a CPU 核

110b MMU

A security apparatus and method are provided for performing a security algorithm that prevents unauthorized access to contents of a physical address (PA) that have been loaded into a storage element of the computer system as a result of performing a prediction algorithm during a hardware table walk that uses a predictor to predict a PA based on a virtual address (VA). When the predictor is enabled, it might be possible for a person with knowledge of the system to configure the predictor to cause contents stored at a PA of a secure portion of the main memory to be loaded into a register in the TLB. In this way, a person who should not have access to contents stored in secure portions of the main memory could indirectly gain unauthorized access to those contents. The apparatus and method prevent such unauthorized access to the contents by masking the contents under certain conditions.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

100 電腦系統

110 CPU 叢集

110a CPU 核

110b MMU

120 主記憶體

130 攝影機顯示器

130a SMMU

140 GPU

140a SMMU

150 PCIe IO

150a SMMU

160 IOTLB

170 系統匯流排

200 系統 OS

210 管理程式

220 HLOS

230 DRM

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

用於在執行硬體表搜尋 (HWTW) 時在某些條件下防止對暫存器的內容的未經授權式存取的方法和裝置

METHOD AND APPARATUS FOR PREVENTING UNAUTHORIZED ACCESS TO CONTENTS OF A REGISTER UNDER CERTAIN CONDITIONS WHEN PERFORMING A HARDWARE TABLE WALK (HWTW)

【技術領域】

【0001】本發明係關於電腦系統，尤其係關於用於在硬體表搜尋 (HWTW) 期間在某些條件下防止對已被載入到暫存器中的實體記憶體位址的內容的未經授權式存取的方法和裝置。

【先前技術】

【0002】現代電腦系統使用記憶體管理單元 (MMU) 來管理向一或多個實體記憶體設備 (諸如舉例而言固態記憶體設備) 寫入資料和從其讀取資料。電腦系統的MMU向該電腦系統的中央處理單元 (CPU) 提供虛擬記憶體，此允許CPU在每個應用程式自身的專用、毗連的虛擬記憶體位址空間中執行該應用程式，而非使所有的應用程式共用往往是成碎片的，或非毗連的實體記憶體位址空間。MMU的目的是為CPU將虛擬記憶體位址 (VA) 轉譯成實體記憶體位址 (PA)。CPU經由直

接向MMU讀寫VA、而MMU將該等VA轉譯成PA並隨後寫或讀PA來間接地讀寫PA。

【0003】爲了執行該等轉譯，MMU存取儲存於系統主記憶體中的頁表。頁表由頁表條目構成。頁表條目是由MMU用來將VA映射成PA的資訊。MMU通常包括轉譯後備緩衝器（TLB），該TLB是被用來快取最近使用過的映射的快取記憶體元件。當MMU需要將VA轉譯成PA時，MMU首先檢查TLB以決定是否存在關於該VA的匹配。若是，則MMU使用TLB中找到的映射來計算PA並隨後存取該PA（亦即，讀或寫該PA）。此被稱爲TLB「命中」。若MMU在TLB中未找到匹配，則此被稱作TLB「失敗」。

【0004】在TLB失敗的情形中，MMU執行所謂的硬體表搜尋（HWTW）。HWTW是耗時的且在計算上管理負擔很大的程序，其涉及執行「表搜尋（table walk）」以尋找MMU中的對應頁表並隨後讀取該頁表中的多個位置以尋找對應的VA到PA位址映射。MMU隨後使用該映射來計算對應的PA並將該映射寫回到TLB。

【0005】在實施作業系統（OS）虛擬化的電腦系統中，虛擬記憶體監視器（VMM）（通常亦被稱爲管理程式）被置於電腦系統的硬體與電腦系統的系統OS之間。管理程式以特權模式執行並且能夠主存一或多個訪客高級OS。在此類系統中，在OS上執行的應用程式使用第一層虛擬記憶體的VA來定址記憶體，並且在管理程式上執行的OS使用第二層虛擬記憶體的中間實體位址（IPA）來定址記憶體。在MMU中，執行階段1

(S1) 轉譯以將每個VA轉譯成IPA，並且執行階段2 (S2) 轉譯以將每個IPA轉譯成PA。

【0006】若在執行此類轉譯時發生TLB失敗，則執行多級二維 (2-D) HWTW以獲得用於計算對應的IPA和PA所需的表條目。執行該等多級2-D HWTW可導致MMU的相當大量的計算管理負擔，此通常導致效能懲罰。

【0007】圖1是已知的三級2-D HWTW的圖形圖示，該三級2-D HWTW在執行讀事務時發生TLB失敗時執行。圖1中示出的HWTW表示三級2-D HWTW的最壞情景，其需要執行15次查表來獲得資料被儲存在實體記憶體中的PA。對於此實例，電腦系統的MMU正執行管理程式，該管理程式主存至少一個訪客高級OS (HLOS)，該HLOS進而正執行至少一個應用程式。在此類配置中，正由訪客HLOS分配的記憶體不是系統的實際實體記憶體，而是前述的中間實體記憶體。管理程式分配實際實體記憶體。因此，每個VA被轉譯成IPA，該IPA隨後被轉譯成實際實體記憶體的實際上儲存正被讀取的資料的PA。

【0008】該程序開始於MMU接收S1頁全域目錄 (PGD) IPA 2。對於此最壞情景實例，將假定在MMU檢查TLB以尋找匹配時發生TLB失敗。由於此失敗，MMU必須執行HWTW。HWTW涉及執行三次S2查表3、4和5以獲得用於將IPA 2轉換成PA所需的映射並執行一次額外查表6以讀取該PA。查表3、4和5分別涉及讀取S2 PGD、頁中間目錄 (PMD) 和頁表條目 (PTE)。在檢視6時讀取PA向MMU提供了S1 PMD IPA 7。對於此最壞情景實例，將假定在MMU檢查TLB以尋找與S1 PMD IPA 7

的匹配時發生TLB失敗。由於此失敗，MMU必須執行另一HWTW。該HWTW涉及執行三次S2查表8、9和11以獲得用於將S1 PMD IPA 7轉換成PA所需的映射並執行一次額外檢視12以讀取該PA。查表8、9和11分別涉及讀取S2 PGD、PMD和PTE。在查表12時讀取PA向MMU提供了S1 PTE IPA 13。

【0009】對於此最壞情景實例，將假定在MMU檢查TLB以尋找與S1 PTE IPA 13的匹配時發生TLB失敗。由於此失敗，MMU必須執行另一HWTW。該HWTW涉及執行三次S2查表14、15和16以獲得用於將S1 PTE IPA 13轉換成PA所需的映射並執行一次額外查表17以讀取該PA。查表14、15和16分別涉及讀取S2 PGD、PMD和PTE。在檢視17時讀取PA向MMU提供了實際IPA 18。對於此最壞情景實例，將假定在MMU檢查TLB以尋找與實際IPA 18的匹配時發生TLB失敗。由於此失敗，MMU必須執行另一HWTW。該HWTW涉及執行三次S2查表19、21和22以獲得用於將實際IPA 18轉換成PA所需的映射。查表19、21和22分別涉及讀取S2 PGD、PMD和PTE。隨後讀取PA以獲得對應的讀取資料。在檢視18時讀取PA向MMU提供了S1 PTE IPA 13。

【0010】因此可以看出，在三級2-D HWTW的最壞情景中，執行了12次S2查表和3次S1查表，此是大量的計算管理負擔，其消耗了大量時間並導致效能懲罰。已使用各種技術和架構來減少在執行HWTW中所涉及的時間和處理管理負擔量，包括例如增加TLB的大小、使用多個TLB、使用平面嵌套的頁表、使用陰影分頁或推測陰影分頁、以及使用頁搜尋快取記憶

體。儘管所有該等技術和架構能夠減少與執行HWTW相關聯的處理管理負擔，但其往往在電腦系統的其他某處造成處理管理負擔的增加。

【0011】因此，存在對減少執行HWTW所需的時間和計算資源量的電腦系統和方法的需要。亦存在對用於防止在HWTW期間對已被載入到TLB暫存器中的PA的內容的未經授權式存取的方法和裝置的需要。

【發明內容】

【0012】本發明針對用於防止在執行HWTW期間對已被載入到電腦系統的儲存元件中的PA的內容的未經授權式存取的安全性裝置和方法。該安全性裝置和方法偵測某些條件以決定是否應當防止對內容的存取，包括偵測預測演算法是否正被用於基於PA來預測VA。

【0013】該裝置包括安全性邏輯，其被配置成在檢查TLB以尋找PA的內容時發生失敗的情況下決定當前是否啓用了將PA預測為IPA的函數的預測演算法。該安全性邏輯被配置成在該預測演算法當前被啓用時防止儲存元件的內容被非特權實體存取。

【0014】該方法包括：

提供安全性邏輯；

【0015】使用該安全性邏輯，在檢查TLB以尋找PA的內容時發生失敗的情況下決定當前是否啓用了將PA預測為IPA的函數的預測演算法；及

【0016】若該安全性邏輯決定該預測演算法當前被啓用，則

該安全性邏輯防止儲存元件的內容被非特權實體存取。

【0017】本發明亦針對其上儲存有電腦代碼的非瞬態電腦可讀取媒體（CRM），該電腦代碼由電腦系統的一或多個處理器執行以用於防止在執行HWTW期間對已被載入到該電腦系統的儲存元件中的PA的內容的未經授權式存取。該電腦代碼包括第一和第二電腦代碼部分。第一電腦代碼部分在檢查TLB以尋找PA的內容時發生失敗的情況下決定當前是否啓用了將PA預測為IPA的函數的預測演算法。第二電腦代碼部分在第一電腦代碼部分決定該預測演算法當前被啓用的情況下防止儲存元件的內容被非特權實體存取。

【0018】該等以及其他特徵和優點從以下描述、附圖和請求項中將變得明顯。

【圖式簡單說明】

【0019】圖1是根據本發明的說明性實施例的電腦系統的方塊圖。

【0020】圖2圖示了根據說明性或示例性實施例的電腦系統的方塊圖，該電腦系統被配置成執行用於減少執行HWTW所需的時間和計算資源量的方法。

【0021】圖3是表示根據說明性實施例的由圖2中所示的管理程式執行以減少執行HWTW讀事務所需的時間和處理管理負擔量的方法的流程圖。

【0022】圖4是根據說明性實施例說明使用由圖3中所示的流程圖所表示的方法來執行HWTW讀事務的方式的圖形示圖。

【0023】圖5是根據說明性實施例的執行由圖3中所示的流程

圖表示的方法的硬體預測器的方塊圖。

【0024】圖6圖示了其中併入圖2中所示的電腦系統的行動智慧型電話的方塊圖。

【0025】圖7是根據說明性實施例的用於執行安全性演算法的安全性邏輯的方塊圖，該安全性演算法防止在圖5中所示的預測器被啓用時對已被載入到TLB中的暫存器中的PA的內容的未經授權式存取。

【0026】圖8是根據說明性實施例圖示由圖7中所示的安全性邏輯執行的程序的流程圖。

【實施方式】

【0027】根據本文描述的說明性實施例，提供了用於減少執行HWTW所需的時間和計算資源量的電腦系統和在電腦系統中使用的方法。若在執行S2 HWTW以尋找儲存S1頁表的PA時發生TLB失敗，則MMU執行使用IPA來預測對應PA的預測演算法，由此避免執行任何S2查表的需要。此舉極大地降低了在執行該等類型的HWTW讀事務時需要執行的檢視的數目，其極大地減少了與執行該等類型的事務相關聯的處理管理負擔和效能懲罰。

【0028】此外，提供了用於執行安全性演算法的安全性裝置和方法的說明性實施例，該安全性演算法防止對由於預測演算法被啓用故而已被載入到儲存元件（例如，TLB中的暫存器）中的PA的內容的未經授權式存取。在啓用預測演算法時，具有關於該系統的知識的人有可能將預測演算法配置成使得儲存在主記憶體的安全部分的PA處的內容被載入到TLB中的

暫存器中。如此，不應當存取儲存在主記憶體的安全部分中的內容的人可能間接地獲得對彼等內容的未經授權式存取。安全性裝置和方法藉由在某些環境下遮蔽該等內容來防止此類未經授權式存取的發生。在描述安全性裝置和方法的說明性實施例之前，將參照圖2-6描述用於執行預測演算法的電腦系統和方法的說明性實施例。隨後將參照圖7和圖8描述安全性裝置和方法的說明性實施例。

【0029】圖2圖示了根據說明性或示例性實施例的電腦系統100的方塊圖，其被配置成執行用於減少執行S2 HWTW以尋找儲存S1頁表的PA所需的時間和計算資源量的方法。圖2中所示的電腦系統100的實例包括CPU叢集110、主記憶體120、攝影機顯示器130、圖形處理單元（GPU）140、快速周邊連接介面（PCIe）輸入/輸出（IO）設備150、多個IO TLB（IOTLB）160和系統匯流排170。CPU叢集110具有多個CPU核110a，每個CPU核110a具有MMU 110b。每個CPU核110a可以是微處理器或任何其他合適的處理器。攝影機顯示器130具有系統MMU（SMMU）130a。GPU 140具有其自身的SMMU 140a。同樣，PCIe IO設備150具有其自身的SMMU 150a。

【0030】處理器核110a的MMU 110b被配置成執行將VA轉譯成IPA以及將IPA轉譯成PA的任務。頁表被儲存於主記憶體120中。MMU 110b以及SMMU 130a、140a和150a中的每一者具有其自身的TLB（出於清楚目的而未圖示），該TLB儲存被儲存在主記憶體120中的頁表的子集。根據本說明性實施例，在發生TLB失敗之後，MMU 110b執行處理IPA以預測PA的預測演

算法。該預測演算法可被數學地表達為：

$$PA=f(IPA), \quad (\text{式 } 1)$$

【0031】其中f表示數學函數。可被用於此目的的函數f在以下參照圖5詳細描述。短語「預測」當該短語在本文中使用时意指「決定」，並且並不暗示隨機或機率性決定，儘管隨機或機率性決定未必從本發明的範疇中排除。由預測演算法作出的預測通常是（但並非必然是）決定性的。

【0032】CPU叢集110執行系統OS 200以及虛擬機器監視器（VMM），或即管理程式210。管理程式210管理轉譯任務，該等轉譯任務除了執行轉譯以外亦包括更新儲存於MMU 110b以及SMMU 130a、140a和150a中的頁表。管理程式210亦執行訪客HLOS 220及/或訪客數位版權管理器（DRM）230。HLOS 220可以與攝影機顯示器130相關聯，並且DRM 230可以與GPU 140相關聯。管理程式210管理HLOS 220和DRM 230。

【0033】在發生TLB失敗之後，管理程式210配置MMU 110b以及SMMU 130a、140a和150a以執行將IPA轉換成PA的預測演算法。在此類情形中，針對與TLB失敗相關聯的VA的起始IPA是按S1轉譯正常開始的典型方式從CPU叢集110的硬體基址暫存器（出於清楚目的而未圖示）獲得的。預測演算法隨後根據式1預測PA，如將在以下更詳細描述的。為了管理和更新SMMU 130a、140a和150a，CPU MMU 110b在匯流排170上向SMMU 130a、140a和150a發送分散式虛擬記憶體（DVM）訊息。MMU 110b以及SMMU 130a、140a和150a存取主記憶體120以執行HWTW。

【0034】根據說明性實施例，CPU MMU 110b將MMU訊務分類成三種事務類，即：(1)用於尋找儲存S1頁表的PA的S2 HWTW讀事務；(2)客戶機事務；及(3)位址故障（AF）/髒標誌寫事務。根據該說明性實施例，預測演算法僅針對類1事務（亦即，HWTW讀事務）將IPA轉換成PA。對於所有其他事務類，根據本說明性實施例，MMU 110b以及SMMU 130a、140a和150a按典型方式執行所有其他轉譯（例如，S1和客戶機事務S2轉譯）。

【0035】圖3是表示根據說明性實施例的由CPU MMU 110b執行以減少執行HWTW讀事務所需的時間和處理管理負擔量的方法的流程圖。方框301表示方法開始，其通常發生在CPU叢集110啟動並開始執行系統OS 200和管理程式210時。MMU 110b將訊務分類成前述的事務類(1)、(2)和(3)，如由方框302所指示的。分類程序可將事務分類成多於或少於該三個類別，但至少一個類別將是類(1)事務，亦即，用於尋找儲存S1頁表的PA的S2 HWTW讀事務。在由方框303表示的步驟處，決定在執行類(1)事務時是否已發生TLB失敗。若否，則該方法行進至方框306，在此MMU 110b或SMMU 130a、140a或150a以正常方式執行HWTW。

【0036】若在由方框303表示的步驟處CPU MMU 110b決定在執行類(1)事務時發生了失敗，則該方法行進至由方框305表示的步驟。在由方框305表示的步驟處，執行前述預測演算法以將IPA轉換或轉譯成PA。

【0037】圖4是根據說明性實施例說明執行HWTW讀事務的

方式的圖形示圖。對於此說明性實施例，爲了示例性目的，假定頁表是三級頁表並且HWTW是2-D HWTW。該實例亦假定TLB失敗最壞情景。該程序開始於MMU接收VA並隨後從控制暫存器（出於清楚目的而未圖示）取得S1 PGD IPA 401。MMU隨後檢查TLB以尋找與S1 PGD IPA 401的匹配。對於此最壞情景實例，將假定在MMU檢查TLB以尋找匹配時發生TLB失敗。由於該失敗，MMU執行預測演算法以將S1 PGD IPA 401轉換成儲存S1 PMD IPA 403的PA 402。因此，使用單次檢視來將S1 PGD IPA 401轉換成PA 402

【0038】對於此最壞情景實例，將假定在MMU檢查TLB以尋找與S1 PMD IPA 403的匹配時發生TLB失敗。由於該失敗，MMU執行預測演算法以將S1 PMD IPA 403轉換成儲存S1 PTE IPA 405的PA 404。因此，使用單次檢視來將S1 PMD IPA 403轉換成PA 404對於此最壞情景實例，將假定在MMU檢查TLB以尋找與S1 PTE IPA 405的匹配時發生TLB失敗。由於該失敗，MMU執行預測演算法以將S1 PTE IPA 405轉換成儲存IPA1 407的PA 406。一旦IPA1 407已被獲得，就執行三次檢視408、409和411以獲得儲存要讀取的資料的最終PA 412。

【0039】因此，根據該實施例可以看出，檢視的總次數已從15（圖1）減少到6，此表示在處理管理負擔方面減少了60%。當然，本發明不限於具有特定級數或特定HWTW維數的MMU配置。本領域技藝人士將理解，本發明的概念和原理無論頁表的配置如何均是適用的。此外，儘管方法和系統在本文是參照IPA到PA轉換來描述的，但其在不使用IPA的系統中亦可

等同地適用於直接VA到PA轉換。

【0040】圖5是執行預測演算法的預測器500的說明性實施例的方塊圖。預測器500通常在MMU 110b中並在SMMU 130a、140a和150a中實施。如以上所指示的，根據說明性實施例，該預測演算法僅在執行類1讀事務時執行。圖5中示出的預測器500的配置是允許針對類1事務啟用預測器500並且針對所有其他事務類（包括類2和3事務）禁用預測器500的一種配置的實例。

【0041】圖5中示出的預測器500的配置亦允許預測器500選擇以上在式1中用於基於IPA來計算PA的函數f。每個虛擬機器（VM）可以使用不同的函數f集，因此被使用的函數集確保在IPA範圍上在IPA與PA之間存在一對一映射是重要的。管理程式210可以管理多個HLOS或DRM，其中的每一個將具有在管理程式210中執行的對應VM。被使用的該等函數集確保所預測的PA與分配給另一VM的所預測PA不交疊。

【0042】函數f的實例是：

【0043】 $PA = IPA$ ；

【0044】 $PA = IPA + \text{Offset_function}(\text{VMID})$ ，其中VMID是跨所有VM識別與HWTW讀事務相關聯的VM的唯一性識別符，並且Offset_function（偏移_函數）是具有基於與VMID相關聯的特定偏移值來選擇的輸出的函數；及

【0045】 $PA = IPA \text{ XOR } \text{Extended_VMID}$ ，其中XOR表示異或運算並且Extended_VMID是擴展VMID。管理程式210選擇函數f以使得避免各VM之間的衝突。

【0046】在圖5中，假定函數f是多項式，並且管理程式210從多個多項式中選擇要被用作函數f的多項式。被選擇的多項式可以基於例如正為其執行HWTW讀事務的VM的VMID。預測器500的配置暫存器510保持一或多個預測賦能位元510a以及一或多個多項式選擇位元510b。預測器500的多項式計算硬體520包括基於從暫存器510接收的多項式選擇位元510b的值來選擇多項式函數的硬體。多項式計算硬體520亦接收IPA到PA轉譯請求並根據所選擇的多項式函數來處理該請求以產生所預測的PA。

【0047】預測賦能位元510a和類1賦能位元在及閘530的輸入端被接收。當在執行類1讀事務時已發生失敗時，類1賦能位元被確定。預測器500的多工器（MUX）540在MUX 540的選擇器埠處接收及閘530的輸出並接收所預測的PA和以正常方式獲得的IPA到PA轉譯結果。當預測賦能位元510a和類1賦能位元兩者均被確定時，S2搜尋控制邏輯和狀態機550被禁用並且MUX 540將所預測的PA選擇為來自MUX 540的輸出。

【0048】當預測賦能位元510a及/或類1賦能位元被否定時，S2搜尋控制邏輯和狀態機550被啟用。當S2搜尋控制邏輯和狀態機550被啟用時，可由S2搜尋控制邏輯和狀態機550在主記憶體120中執行其他類型的S2搜尋（例如，類2和類3）。因此，當S2搜尋控制邏輯和狀態機550被啟用時，MUX 540輸出從S2搜尋控制邏輯和狀態機550輸出的IPA到PA轉譯結果。

【0049】應注意，預測器500可具有許多不同的配置。圖5中所示的預測器500的配置僅僅是用於執行預測演算法的許多

合適的配置中的一種。本領域技藝人士將理解，不同於圖5中所示的配置的許多配置可被用來執行預測演算法。

【0050】圖2中所示的電腦系統100可在其中執行記憶體虛擬化的任何類型的系統中實施，該系統例如包括桌上型電腦、伺服器 and 行動智慧型電話。圖6圖示了其中併入電腦系統100的行動智慧型電話600的方塊圖。智慧型電話600除了其必須能夠執行本文所描述的方法以外不限於任何特定類型的智慧型電話或具有任何特定配置。此外，圖6中圖示的智慧型電話600意欲作為具有上下文感知和用於執行本文描述的方法的處理能力的蜂巢式電話的簡化實例。本領域一般技藝人士將理解智慧型電話的操作和構造，由此實施細節已被省略。

【0051】根據本說明性實施例，智慧型電話600包括在系統匯流排612上連接在一起的基頻子系統610和射頻（RF）子系統620。系統匯流排612通常包括實體和邏輯連接，其將上述元件耦合在一起並賦能其互用性。RF子系統620可以是無線收發機。儘管為了清楚起見未圖示細節，但RF子系統620一般包括發射（Tx）模組630（其具有用於準備基頻資訊信號以供傳輸的調制、升頻轉換和放大電路系統），包括接收（Rx）模組640（其具有用於接收RF信號並將該RF信號降頻轉換到基頻資訊信號以恢復資料的放大、濾波和降頻轉換電路系統），並且包括前端模組（FEM）650（其包括能將發射信號從接收信號中分離出來的雙訊器電路系統、雙工器電路系統，或任何其他電路系統，如本領域技藝人士已知的）。天線660被連接到FEM 650。

【0052】基頻子系統610一般包括電腦系統100、類比電路元件616和數位電路元件618，其經由系統匯流排612電耦合在一起。系統匯流排612通常包括實體和邏輯連接以將上述元件耦合在一起並賦能其互用性。

【0053】輸入/輸出（I/O）元件621經由連接624被連接到基頻子系統610。I/O元件621通常包括例如話筒、小鍵盤、揚聲器、指標設備、使用者介面控制元件、以及允許使用者提供輸入命令並從智慧型電話600接收輸出的任何其他設備或系統。記憶體628經由連接629被連接至基頻子系統610。記憶體628可以是任何類型的揮發性或非揮發性記憶體。記憶體628可以永久安裝在智慧型電話600中，或者可以是可移除式記憶體元件，諸如可移除式記憶卡。

【0054】類比電路系統616和數位電路系統618包括信號處理、信號轉換和將由I/O元件621提供的輸入信號轉換成要傳送的資訊信號的邏輯。類似地，類比電路系統616和數位電路系統618包括用於從收到信號產生包含已恢復資訊的資訊信號的信號處理元件。數位電路系統618可包括例如數位訊號處理器（DSP）、現場可程式設計閘陣列（FPGA），或任何其他處理設備。因為基頻子系統610既包括類比元件又包括數位元件，所以其可被稱為混合信號設備（MSD）。

【0055】智慧型電話600可包括各種感測器中的一或多個，諸如舉例而言，相機661、話筒662、全球定位系統（GPS）感測器663、加速計665、陀螺儀667和數位羅盤668。該等感測器經由匯流排612與基頻子系統610通訊。

【0056】使電腦系統100嵌入在智慧型電話600中允許多個OS和多個相應VM在智慧型電話600上執行。在此環境中，電腦系統100的管理程式210（圖2）提供了智慧型電話600的硬體與正由VM執行的應用軟體之間的安全分隔。

【0057】根據說明性實施例，提供了安全性方法和裝置，其偵測以上參照圖5描述的預測演算法是否正被執行，並且若是，則採取防止某些暫存器及/或緩衝器的內容可被非特權或未經授權的實體存取的安全性預防措施。需要該安全性方法和裝置的原因是因為在啓用預測演算法時，具有關於該系統的知識的人有可能將預測演算法配置成使得儲存在實體主記憶體120（圖2）的安全部分的PA處的內容被載入到TLB中的暫存器中。如此，不應當存取儲存在實體主記憶體120的安全部分中的內容的人可以間接地獲得對彼等PA的未經授權式存取。該方法和裝置防止此類未經授權或非特權的存取。

【0058】圖7是根據說明性實施例的用於執行安全性演算法的裝置700的方塊圖，該安全性演算法在預測演算法被啓用時防止對已被載入到TLB中的暫存器中的PA的內容的未經授權式存取。該方塊圖在本質上是概念性的並且可單獨在硬體中實施，或者在硬體與軟體或韌體的組合中實施。裝置700是被配置成執行安全性演算法的安全性邏輯。安全性邏輯700通常是CPU核110a的一部分並且可以是MMU 110b以及SMMU 130a、140a和150a（圖2）的一部分。本發明關於安全性邏輯700位於電腦系統100中何處不受限制。

【0059】圖5中示出的預測賦能位元510a被連接至安全性邏

輯700的及閘710的輸入端。特權存取位元被施加到及閘710的另一個輸入端。若嘗試存取多個暫存器720之一的實體被給予存取特定暫存器720的特權，則特權存取位元被確定。出於示例性目的，將假定暫存器720在TLB中。及閘710的輸出被施加到或（OR）閘730的輸入端之一。從暫存器存取表740輸出的存取識別符位元被施加到或閘730的另一個輸入端。若正被存取的暫存器720包含來自處於主記憶體120（圖5）的安全，或特權部分中的PA的內容，則存取識別符位元被確定。暫存器存取表740追蹤哪些PA在主記憶體120的安全部分中並相應地確定或否定存取識別符位元。被用於選擇暫存器720之一的暫存器選擇位址750亦被用於選擇暫存器位址表740中的對應條目。因此，若被暫存器選擇位址750選擇的暫存器720被給予特權，則被輸入到或閘730的對應存取識別符位元被確定。

【0060】 或閘730的輸出被施加到MUX 760的選擇器端子。被暫存器選擇位址750定址的暫存器720中的內容被施加到MUX 760的第一組輸入端子。MUX 760的第二組輸入端子接收全邏輯0。在預測演算法被啓用並且特權存取位元被確定時，MUX 760選擇由暫存器選擇位址750定址的暫存器720的內容以從MUX 760輸出並載入到結果暫存器770中。在預測演算法被禁用或者特權存取位元被否定、並且存取識別符位元被否定（指示正被存取的內容來自主記憶體120的非安全部分）時，MUX 760選擇由暫存器選擇位址750定址的暫存器720的內容以從MUX 760輸出並載入到結果暫存器770中。當存取識別符位元被確定（指示正被存取的內容來自主記憶體120的安全部

分)時，MUX 760選擇全邏輯0以從MUX 760輸出並載入到結果暫存器770中。

【0061】因此，由暫存器選擇位址750定址的暫存器720的實際內容將從MUX 760輸出並載入到結果暫存器770中，除了在以下兩種情形中的任一種中以外：(1)預測演算法被啓用並且特權存取位元被確定；或者(2)存取識別符位元被確定。在該兩種情形中的任一種中，全邏輯0被載入到結果暫存器770中以防止暫存器720的實際內容可在結果暫存器770中存取。

【0062】圖8是圖示由以上參照圖7描述的安全性邏輯700執行的判定程序的流程圖。在方框801作出預測演算法是否被啓用的決定。若否，則返回暫存器720的實際內容，如方框802所指示的。若是，則在方框803作出嘗試存取內容的實體是否被給予特權的決定。若是，則在方框802返回暫存器720的實際內容。若否，則在方框804作出暫存器720是否暴露特權資料的決定。若否，則在方框802返回暫存器720的實際內容。若是，則返回邏輯0，如方框805所指示的。

【0063】從安全性邏輯700的描述可以看出，若非特權實體（例如，不同於管理程式的實體）嘗試使用圖5中所示的預測器500來獲得對儲存在主記憶體120的未經授權的PA中的內容的未經授權式存取，則實際內容將被0蓋寫以防止未經授權或非特權實體存取實際內容。可在本發明的範疇內對圖7中所示的安全性邏輯700以及對圖8中所示的程序作出許多修改。例如，參照圖8，該程序可藉由除去方框803、留下方框801、802、804和805來修改。或者，可除去方框804，留下方框801、

802、803和805。可容易地修改圖7中所示的安全性邏輯700以實現經修改的程序，如本領域技藝人士將理解的。

【0064】應注意，不同於或補充於以上參照圖5、圖7和圖8描述的彼等安全性功能的安全性功能亦可在已偵測到未經授權式存取嘗試時實施。用邏輯0蓋寫暫存器的內容僅僅是提供安全性的一種方式的實例。替代方案的實例包括用邏輯1或遮掩真實內容的某一其他二進位值來蓋寫內容，將內容與相等長度的某一其他二進位值進行XOR（異或），返回錯誤訊息而非實際內容，發出中斷，重置處理器110a、MMU 110或者SMMU 130a、140a或150a等等。本領域技藝人士將理解可鑒於本文提供的論述來實施對本文描述的說明性實施例的該等或其他合適替代方案的方式。

【0065】以上參照圖3和圖8描述的程序可單獨在硬體中實施，或者在硬體與軟體的組合或硬體與韌體的組合中實施。同樣，圖2中所示的電腦系統100的許多元件可單獨在硬體中實施，或者在硬體與軟體或韌體的組合中實施。例如，管理程式210可單獨在硬體中實施，或者在硬體與軟體或韌體的組合中實施。在圖3和圖8中所示的程序或者圖2中所示的電腦系統100的元件在軟體或韌體中實施的情形中，對應代碼被儲存在主記憶體120（圖2）中，主記憶體120是電腦可讀取媒體。主記憶體120通常是固態電腦可讀取媒體，諸如非揮發性隨機存取記憶體（RAM）、動態RAM（DRAM）、唯讀記憶體（ROM）設備、可程式設計ROM（PROM）、可抹除PROM（EPROM）等等。然而，其他類型的電腦可讀取媒體可被用於儲存代

碼，諸如舉例而言磁性或光學儲存設備。

【0066】應注意，本文描述的說明性實施例意欲說明本發明的原理和概念。本發明不限於該等實施例，如本領域技藝人士鑒於本文所提供的描述將理解的。亦應注意，可對以上參照圖2-8描述的方法和系統做出許多變動而不偏離本發明的範疇。例如，圖7中所示的安全性邏輯700的配置可按數種方式修改而仍實現以上述及之目標，如本領域技藝人士鑒於本文所提供的描述將理解的。此外，圖6中所示的智慧型電話600僅僅是具有用於執行該方法的合適配置和功能性的行動設備的一個實例。本領域技藝人士鑒於本文提供的描述將理解，可對圖6中所示的智慧型電話600作出許多變動而不偏離本發明的範疇。該等及其他變動均落在本發明的範疇之內。

【符號說明】

【0067】

- 2 S1 PGD IPA
- 3 查表
- 4 查表
- 5 查表
- 6 查表
- 7 S1 PMD IPA
- 8 查表
- 9 查表
- 11 查表
- 12 查表

- 13 S1 PTE IPA
- 14 查表
- 15 查表
- 16 查表
- 17 查表
- 18 IPA 1
- 19 查表
- 21 查表
- 22 查表
- 100 電腦系統
- 110 CPU 叢集
 - 110a CPU 核
 - 110b MMU
- 120 主記憶體
- 130 攝影機顯示器
 - 130a SMMU
- 140 GPU
 - 140a SMMU
- 150 PCIe IO
 - 150a SMMU
- 160 IOTLB
- 170 系統匯流排
- 200 系統 OS
- 210 管理程式

220	HLOS
230	DRM
301	方框
302	方框
303	方框
305	方框
306	方框
401	S1 PGD IPA
402	PA
403	S1 PMD UPA
404	PA
405	S1 PTE IPA
406	PA
407	IPA 1
408	檢視
409	檢視
411	檢視
412	PA
500	預測器
510	暫存器
510a	預測賦能位元
510b	多項式選擇位元
520	多項式計算硬體
530	及閘

540	MUX
550	S2 搜尋控制邏輯和狀態機
610	基頻子系統
612	系統匯流排
616	類比電路元件
618	數位電路元件
620	RF 子系統
621	I/O 元件
624	連接
628	記憶體
629	連接
630	發射模組
640	接收模組
650	FEM
660	天線
661	相機
662	話筒
663	GPS
664	加速計
665	陀螺儀
666	羅盤
700	裝置
710	及閘
720	暫存器

- 730 或聞
- 740 暫存器存取表
- 750 暫存器選擇位址
- 760 MUX
- 770 結果暫存器
- 801 方框
- 802 方框
- 803 方框
- 804 方框
- 805 方框

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

申請專利範圍

1. 一種一電腦系統的裝置，用於防止在執行一硬體表搜尋（HWTW）期間對已被載入到該電腦系統的一儲存元件中的一實體位址（PA）的內容的未經授權式存取，該裝置包括：

安全性邏輯，其被配置成在檢查一轉譯後備緩衝器（TLB）以尋找該PA的該等內容時發生一失敗的情況下決定當前是否啓用了將一PA預測為一中間實體位址（IPA）的一函數的一預測演算法，其中該安全性邏輯被配置成在該安全性邏輯決定該預測演算法當前被啓用的情況下防止該儲存元件的該等內容被一非特權實體存取。

2. 如請求項1述及之裝置，其中該儲存元件是該TLB的一暫存器，在該預測演算法當前被啓用的情況下該所預測的PA的該等內容已被載入到該暫存器中，並且其中該安全性邏輯包括：

第一判定邏輯，其作出該預測演算法當前是否被啓用的決定，並且其中該第一判定邏輯亦決定是一特權實體還是一非特權實體正在嘗試存取該暫存器的該等內容，若該第一判定邏輯決定該預測演算法當前被啓用並且一特權實體正在嘗試獲得對該暫存器的內容的存取，則該第一判定邏輯輸出一第一判定，若該第一判定邏輯決定該預測演算法當前未被啓用，或者一非特權實體正在嘗試獲得對該暫存器的內容的存取，則該第一判定邏輯輸出一第二判定；及

選擇邏輯，其被配置成在該第一判定邏輯輸出該第二判

定的情況下使得該暫存器的該等內容被一遮罩值蓋寫，該選擇邏輯被配置成在該第一判定邏輯輸出該第一判定的情況下維持該暫存器的該等內容。

3. 如請求項2述及之裝置，其中該安全性邏輯進一步包括：

第二判定邏輯，其被配置成決定該PA對應於主記憶體的一安全部分還是一非安全部分，或者決定該第一判定邏輯輸出了該第一判定還是該第二判定，其中若該第二判定邏輯決定該PA對應於主記憶體的一安全部分，則該第二判定邏輯輸出一第一判定，並且其中若該第二判定邏輯決定該PA對應於主記憶體的一非安全部分或者該第一判定邏輯輸出了該第二判定，則該第二判定邏輯輸出一第二判定；及

其中該選擇邏輯被配置成在該第二判定邏輯輸出該第一判定的情況下使得該暫存器的該等內容被遮蔽，並且其中該選擇邏輯被配置成在該第二判定邏輯輸出該第二判定的情況下維持該暫存器的該等內容。

4. 如請求項1述及之裝置，其中該安全性邏輯是該電腦系統的一記憶體管理單元（MMU）的一部分。

5. 如請求項4述及之裝置，其中該MMU是該電腦系統的中央處理單元（CPU）的一部分。

6. 如請求項5述及之裝置，其中該CPU是該電腦系統的一

CPU叢集的一部分。

7. 如請求項1述及之裝置，其中該電腦系統是一行動電話的一部分。

8. 一種在一電腦系統中執行的用於防止在執行一硬體表搜尋（HWTW）期間對已被載入到該電腦系統的一儲存元件中的一實體位址（PA）的內容的未經授權式存取的方法，該方法包括以下步驟：

提供安全性邏輯；

使用該安全性邏輯，在檢查一轉譯後備緩衝器（TLB）以尋找該PA的該等內容時發生一失敗的情況下決定當前是否啓用了將一PA預測為一中間實體位址（IPA）的一函數的一預測演算法；及

若該安全性邏輯決定該預測演算法當前被啓用，則該安全性邏輯防止該儲存元件的該等內容被一非特權實體存取。

9. 如請求項8述及之方法，其中該儲存元件是該TLB的一暫存器，在該預測演算法當前被啓用的情況下該所預測的PA的該等內容已被載入到該暫存器中，並且其中該方法進一步包括以下步驟：

使用該安全性邏輯的第一判定邏輯，作出該預測演算法當前是否被啓用的該決定，並且其中該第一判定邏輯亦決定是一特權實體還是一非特權實體正在嘗試存取該暫存器的該

等內容；

使用該第一判定邏輯，在該第一判定邏輯決定該預測演算法當前被啓用並且一特權實體正在嘗試獲得對該暫存器的內容的存取的情況下，輸出一第一判定；

使用該第一判定邏輯，在該第一判定邏輯決定該預測演算法當前未被啓用，或者一非特權實體正在嘗試獲得對該暫存器的內容的存取的情況下，輸出一第二判定；

使用該安全性邏輯的選擇邏輯，在該第一判定邏輯輸出該第二判定的情況下藉由使得該暫存器的該等內容被一遮罩值蓋寫來防止該暫存器的該等內容被存取；及

使用該選擇邏輯，在該第一判定邏輯輸出該第一判定的情況下維持該暫存器的該等內容。

10. 如請求項9述及之方法，進一步包括以下步驟：

使用該安全性邏輯的第二判定邏輯，決定該PA對應於主記憶體的一安全部分還是一非安全部分，或者決定該第一判定邏輯輸出了該第一判定還是該第二判定；

使用該第二判定邏輯，在該第二判定邏輯決定該PA對應於主記憶體的一安全部分的情況下從該第二判定邏輯輸出一第一判定；

使用該第二判定邏輯，在該第二判定邏輯決定該PA對應於主記憶體的一非安全部分或者該第一判定邏輯輸出該第二判定的情況下從該第二判定邏輯輸出一第二判定；

使用該選擇邏輯，在該第二判定邏輯輸出該第一判定的

情況下使得該暫存器的該等內容被遮蔽；及

使用該選擇邏輯，在該第二判定邏輯輸出該第二判定的情況下使得該暫存器的該等內容被維持。

11. 如請求項8述及之方法，其中該安全性邏輯是該電腦系統的一記憶體管理單元（MMU）的一部分。

12. 如請求項11述及之方法，其中該MMU是該電腦系統的中央處理單元（CPU）的一部分。

13. 如請求項12述及之方法，其中該CPU是該電腦系統的一CPU叢集的一部分。

14. 如請求項8述及之方法，其中該電腦系統是一行動電話的一部分。

15. 一種其上儲存有電腦代碼的非瞬態電腦可讀取媒體（CRM），該電腦代碼由一電腦系統的一或多個處理器執行以用於防止在執行一硬體表搜尋（HWTW）期間對已被載入到該電腦系統的一儲存元件中的一實體位址（PA）的內容的未經授權式存取，該電腦代碼包括：

一第一電腦代碼部分，其用於在檢查一轉譯後備緩衝器（TLB）以尋找該PA的該等內容時發生一失敗的情況下決定當前是否啓用了將一PA預測為一中間實體位址（IPA）的一函

數的一預測演算法；及

一第二電腦代碼部分，其用於在該第一電腦代碼部分決定該預測演算法當前被啓用的情況下防止該儲存元件的該等內容被一非特權實體存取。

16. 如請求項15述及之非瞬態CRM，其中該儲存元件是該TLB的一暫存器，在該預測演算法當前被啓用的情況下所預測的PA的該等內容已被載入到該暫存器中，並且其中該第一電腦代碼部分亦決定是一特權實體還是一非特權實體正在嘗試存取該暫存器的該等內容，並且其中若該第一電腦代碼部分決定該預測演算法當前被啓用並且一特權實體正在嘗試獲得對該暫存器的內容的存取，則該第一電腦代碼部分輸出一第一判定，並且其中若該第一電腦代碼部分決定該預測演算法當前未被啓用，或者一非特權實體正在嘗試獲得對該暫存器的內容的存取，則該第一電腦代碼部分輸出一第二判定，並且其中該第二電腦代碼部分在該第一電腦代碼部分輸出該第二判定的情況下藉由使得該暫存器的該等內容被一遮罩值蓋寫來防止該暫存器的該等內容被存取；並且其中該第二電腦代碼部分在該第一電腦代碼部分輸出該第一判定的情況下使得該暫存器的該等內容被維持。

17. 如請求項16述及之非瞬態CRM，其中該CRM是該電腦系統的一記憶體管理單元（MMU）的一部分。

18. 如請求項17述及之非瞬態CRM，其中該MMU是該電腦系統的中央處理單元（CPU）的一部分。

19. 如請求項18述及之非瞬態CRM，其中該CPU是該電腦系統的一CPU叢集的一部分。

圖式

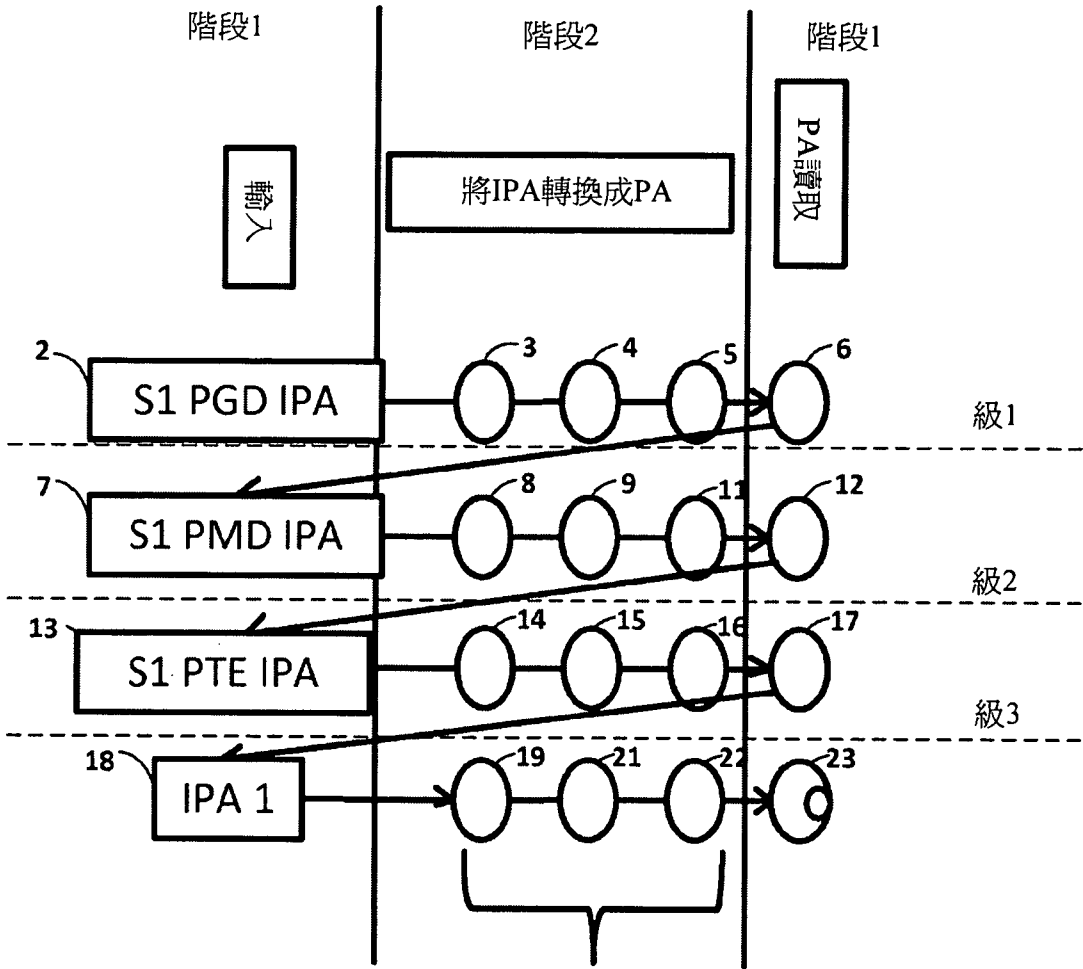


圖1
先前技術

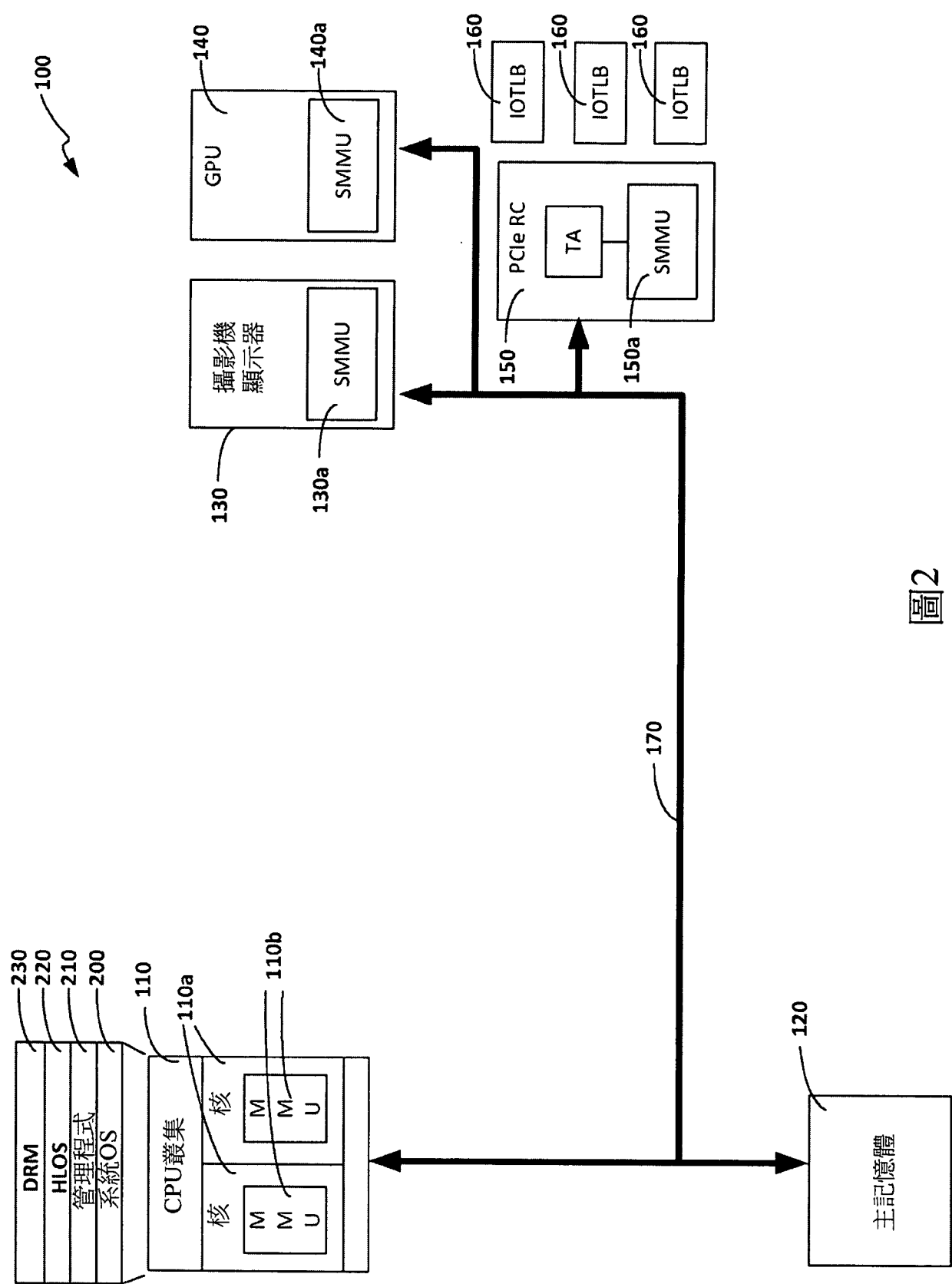


圖2

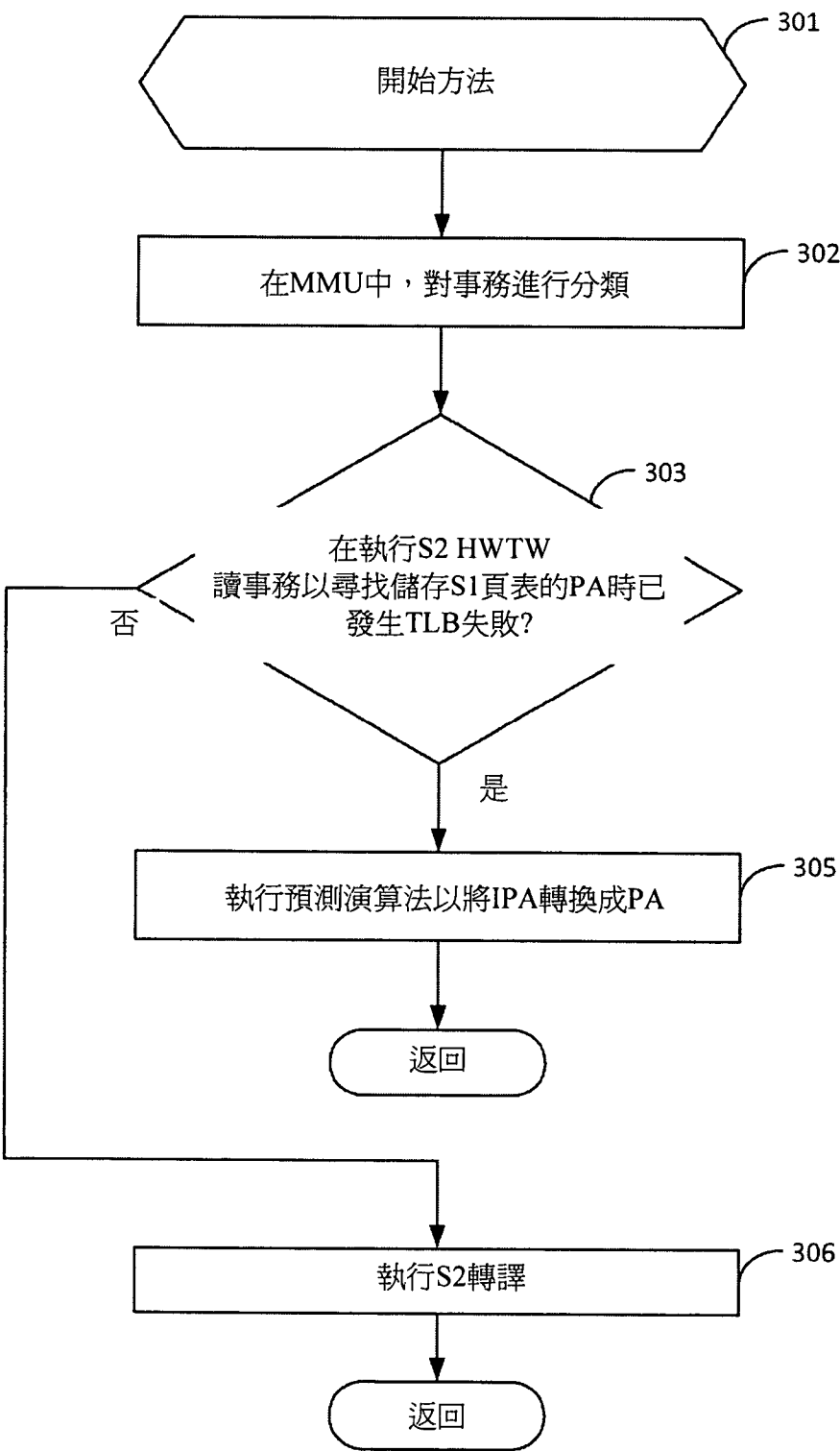


圖3

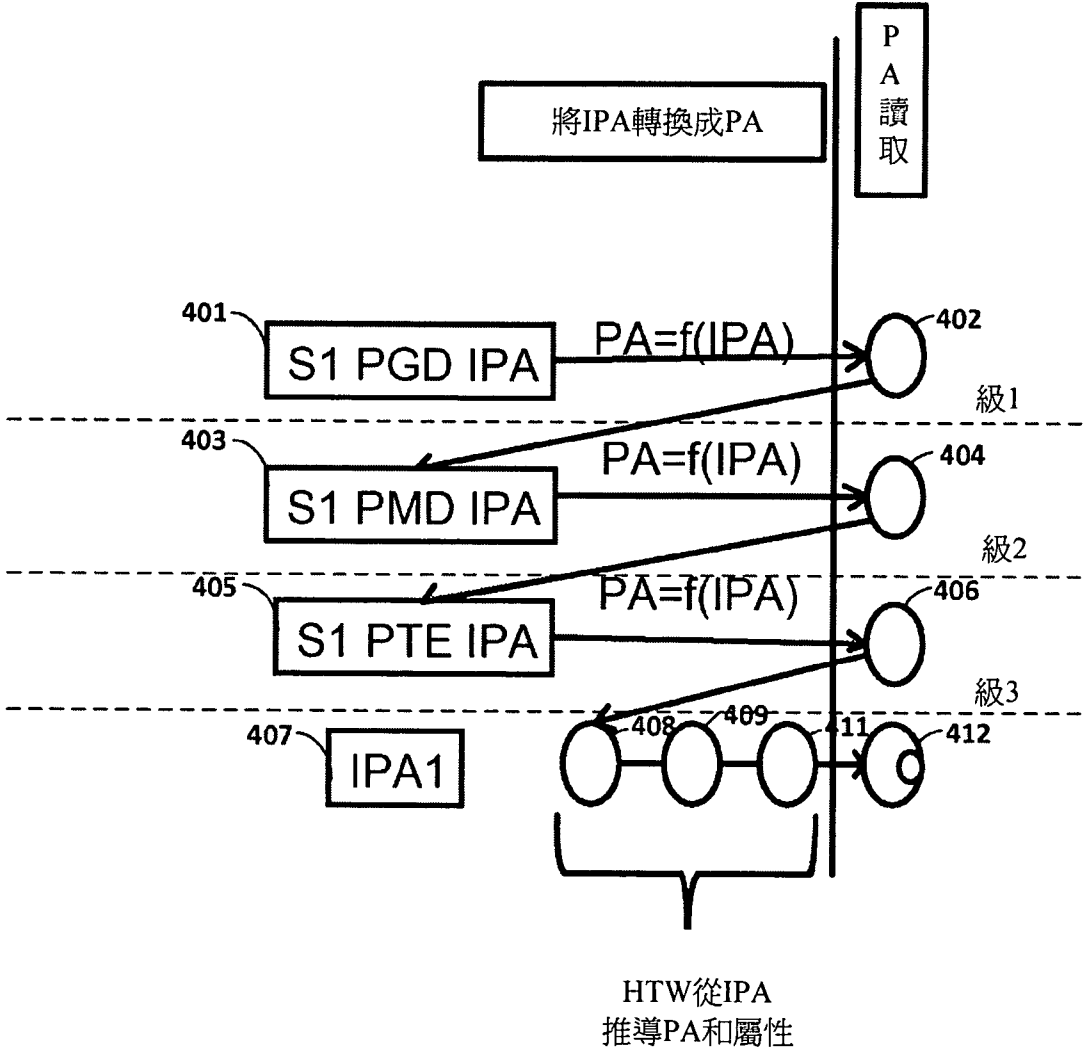


圖4

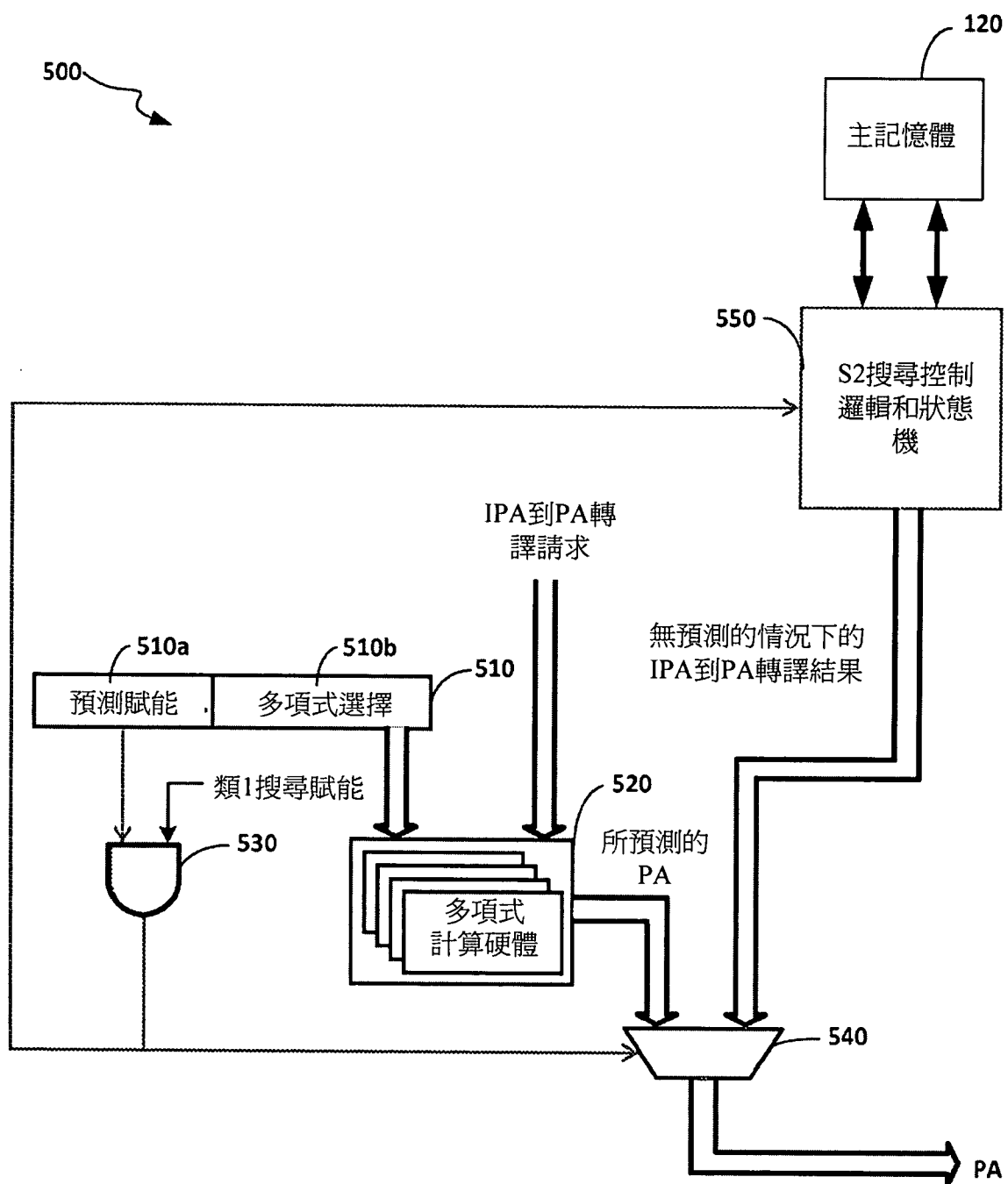


圖5

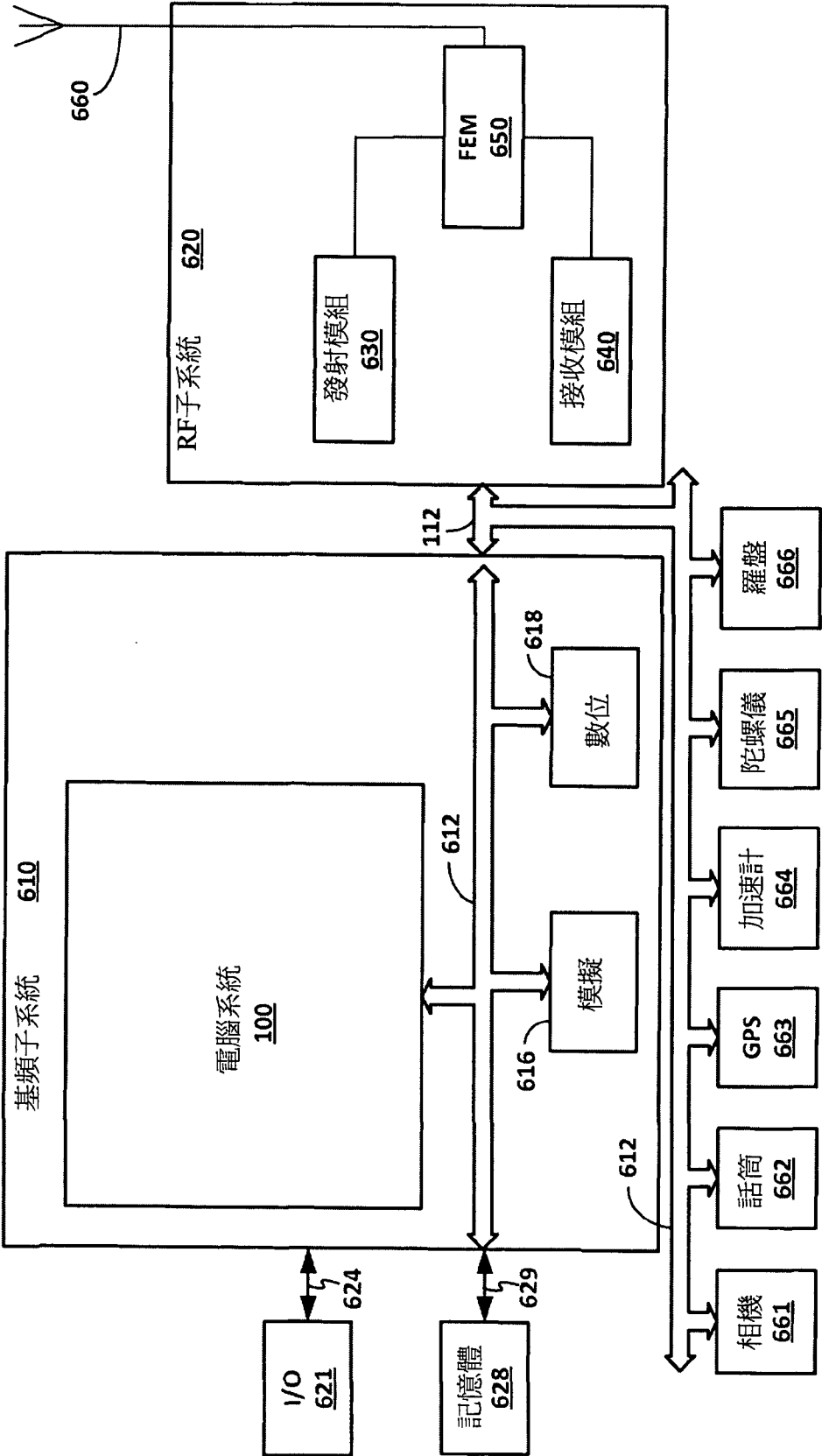


圖6

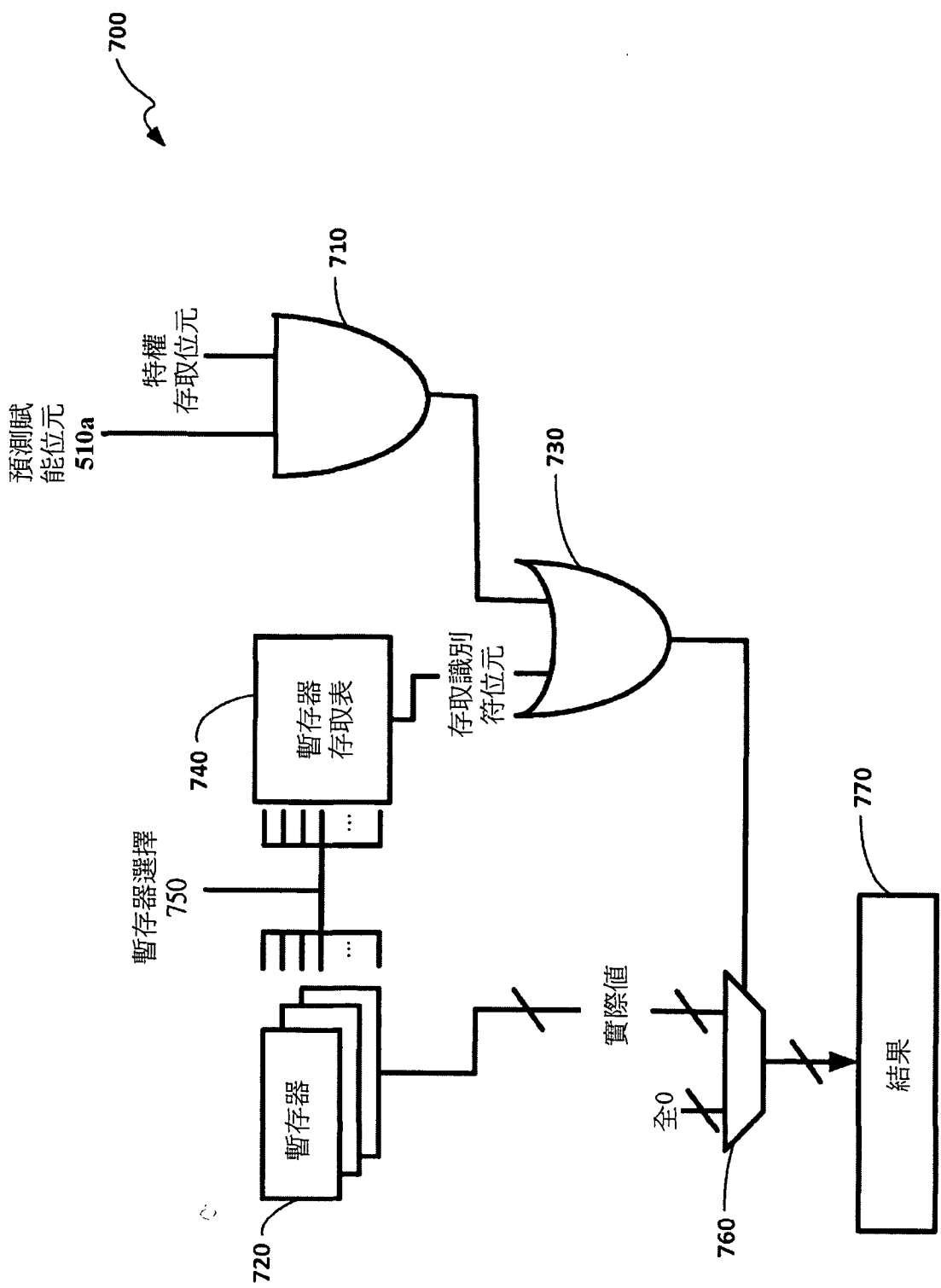


圖7

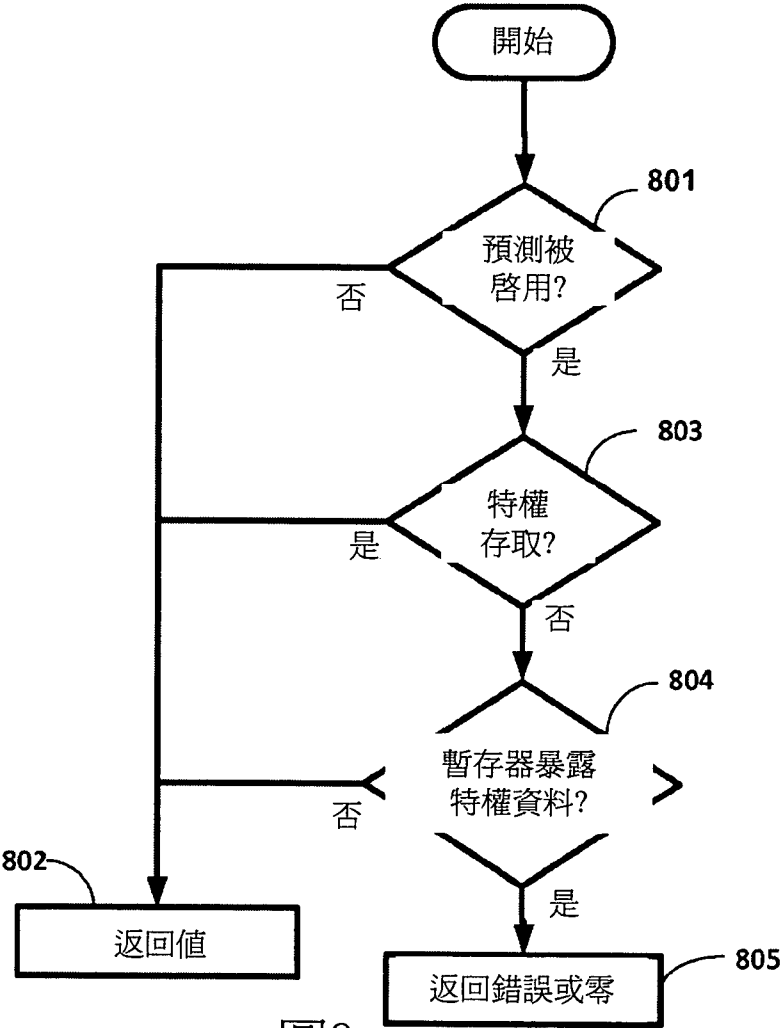


圖8