

(1)

玖、發明說明

【發明所屬之技術領域】

本發明係有關使敏感性資料不會受到 I/O 裝置的不適當存取之安全裝置。更具體而言，本發明係有關一種用來追蹤記憶體中存放有敏感性資料的區段的一無直接記憶體存取表之快取記憶體。

【先前技術】

在運算裝置上執行金融交易及個人交易的比率愈來愈高。然而，此種金融交易次數的持續性成長也已導致對支援這些交易的電腦系統有愈來愈多的攻擊，並導致對防止敏感性資料的未經授權的存取及遺失的安全強化（Security Enhanced；簡稱 SE）環境的一對應之需求。敏感性資料（例如社會安全號碼、帳號、金融資料、帳戶餘額、密碼、及授權金鑰等的敏感性資料）的遺失或未經授權的存取將造成隱私的喪失、私人金融資料的遭竊、及類似的惡意行為。

嘗試存取被保護的資料所用之一種技術是利用周邊裝置經由直接記憶體存取（Direct Memory Access；簡稱 DMA）控制器提出的記憶體存取要求。DMA 控制器可讓諸如網路卡等的周邊裝置在對中央處理單元有最少的使用之情形下讀取及寫入系統記憶體。使用來自 I/O 裝置的記憶體存取要求時，可能會規避作業系統所提供的安全措施。對指定給周邊裝置使用的系統記憶體區段範圍之外的

(2)

存放有敏感性資訊之記憶體區段提出記憶體存取的要求，可能會達到上述的效果。

【發明內容】

本發明揭示了一種包含一超頁欄位之無直接記憶體存取快取記憶體。該超頁欄位指示一組頁存放有受保護的資訊之時機。一電腦系統利用該無直接記憶體存取快取記憶體來拒絕 I/O 裝置對系統記憶體中之受保護的資訊之存取。

【實施方式】

圖 1 示出一電腦系統 (100) 的一實施例，該電腦系統 (100) 包含一晶片組 ("北橋晶片組") (117)、一組中央處理單元 (Central Processing Unit; 簡稱 CPU) (105)、以及系統記憶體 (101)。在一實施例中，該組 CPU (105) 係經由處理器匯流排 (119) 而被連接到北橋晶片組 (117)。在一實施例中，電腦系統 (100) 包含多個處理器 (105)，用以支援一伺服器環境中之多重處理。在另一實施例中，電腦系統 (100) 可含一單一的 CPU。系統記憶體 (101) 係經由記憶體匯流排 (121) 而被連接到北橋晶片組 (117)。系統記憶體 (101) 包含一無直接記憶體存取 (No Direct Memory Access; 簡稱 NoDMA) 表 (103)。

在一實施例中，系統記憶體 (101) 是一組諸如同步

(3)

動態隨機存取記憶體（Synchronous Dynamic Random Access Memory；簡稱 SDRAM）、雙倍資料速率隨機存取記憶體（Double Data Rate Random Access Memory；簡稱 DDR RAM）、或類似的裝置等的隨機存取記憶體裝置。記憶體系統（101）亦可包含暫存器或類似的儲存裝置。在系統記憶體（101）中儲存一 NoDMA 表（103），而係將該 NoDMA 表（103）用來追蹤系統記憶體（101）中存放有敏感性資料的區段。敏感性資料可包括社會安全號碼、金融帳號、密碼、及類似的資料。一作業系統（Operating System；簡稱 OS）可利用該 NoDMA 表（103）的資料來限制對存放有敏感性資料的記憶體區段之存取，其方式為將 NoDMA 表（103）中對應於存放有敏感性資料的記憶體區段之一資料項加上旗標，且只讓被授權可存取祕密資訊的那些程式存取記憶體（101）中受保護的區段。在一實施例中，係將系統記憶體（101）區分為若干頁。頁的容量可改變為作業系統所決定的容量。在一實施例中，頁的容量是四千位元組。

在一實施例中，係將 NoDMA 表（103）建構為一組連續的位元，且每一位元對應於記憶體（101）的一頁。如果一頁存放有敏感性資料，則作業系統將 "設定" 與 NoDMA 表（103）中之該頁對應的位元。可在系統記憶體（101）中重定位 NoDMA 表（103）的基址或起始位址。在一實施例中，諸如在系統（100）啟動之後，一作業系統、基本輸入／輸出系統（Basic Input/Output

(4)

System；簡稱 BIOS）、或類似的系統可重定位 NoDMA 表（103）。係根據基址暫存器中儲存的起始位址，而在系統記憶體（101）中設定 NoDMA 表（103）的位置。係根據一容量暫存器中儲存的資料而決定 NoDMA 表（103）的容量。當 NoDMA 表（103）被起動時，必須將一 I/O 裝置進行的所有存取比對該表（103）。

在一實施例中，對準 NoDMA 表（103），以便開始於一頁邊界，並終止於一頁邊界。該對準簡化了 NoDMA 表（103）的使用。在另一實施例中，NoDMA 表（103）可開始於記憶體（101）中之任何位址，而可有效率地使用表（103）的連續空間。自 NoDMA 表（103）的起始點至終止點的每一位元指示了 CPU 以外的其他裝置對記憶體（101）中自位址 0 開始的每一頁進行存取的存取特權，以便遮蓋需要被保護的整個記憶體位址空間。當北橋晶片組（117）需要檢查對一特定位址的存取特權時，北橋晶片組（117）可容易地決定對該頁的存取特權，這是因為北橋晶片組（117）已取得了 NoDMA 表（103）的起始位址、及所要存取的頁之頁位址。因此，可容易地計算且存取對應的 NoDMA 表（103）資料項。

在一實施例中，北橋晶片組（117）處理系統記憶體（101）、CPU（105）、與 I/O 裝置（115）間之通訊。北橋晶片組（117）包含一中央資料緩衝區（Central Data Buffer；簡稱 CDB），用以處理自 CPU（105）、I/O 裝置及來源（115）進來的記憶體存取要求。中央控制區

(5)

塊（CDB 介面）（113）執行對進來的記憶體存取要求之起始處理、及送出的要求之最後處理。係將等候被 CDB（107）或 CDB 介面（113）處理的記憶體存取要求儲存在佇列中。CDB（107）及 CDB 介面（113）處理來自 I/O 裝置（115）的記憶體要求，並將所要求的資料自系統記憶體（101）傳送到 I/O 裝置（115）。

北橋晶片組（117）包含一組佇列，用以儲存進來的及送出的記憶體存取要求（例如讀取及寫入要求）。在一實施例中，該等佇列是先進先出佇列（FIFO），或採用一類似的佇列管理機制。北橋晶片組（117）亦包含一 NoDMA 快取記憶體（109），用以儲存最近被要求的 NoDMA 表資料項。在存取記憶體（101）之前，CDB 介面（113）先維護並使用該快取記憶體（109）。CDB 介面（113）亦管理各別佇列中之進來的及送出的訊息。在一實施例中，北橋晶片組（117）也包含與 NoDMA 表（103）及 NoDMA 快取記憶體（109）的功能有關的一組暫存器。這些暫存器包括若干狀態暫存器、用來指示 NoDMA 表（103）在記憶體（101）中之起始位址的一基址暫存器、以及用來指示 NoDMA 表（103）在系統記憶體（101）中之容量的一容量暫存器。

在一實施例中，北橋晶片組（117）使記憶體（101）不會受到非 CPU 裝置的存取。一非 CPU 裝置無法讀取或寫入存放有受到保護的資料之各記憶體區段。受到保護的頁不是靜態的，且可將各頁移進及移出受到保護的狀

(6)

態。在一實施例中，北橋晶片組（117）使用 NoDMA 表（103）及 NoDMA 快取記憶體（109）來強制執行該系統。NoDMA 快取記憶體（109）有助於 I/O 效能。在一實施例中，縱使並未起動 NoDMA 表（103），也必然拒絕對記憶體（101）的 NoDMA 表（103）區之 I/O 存取。對系統記憶體（101）的該區之任何存取嘗試將造成一錯誤，且北橋晶片組（117）記錄該等存取嘗試，而且該系統被重設。

I/O 來源（115）可以是一通訊控制裝置（"南橋晶片組"），用以處理各周邊裝置（例如儲存體驅動器、數據機、網路卡、及類似的裝置）與其他周邊裝置或北橋晶片組（117）間之通訊。南橋晶片組（115）或北橋晶片組（117）可以有針對埠的各種位元寬度而設定組態之多個 I/O 單元。該等 I/O 單元可支援其中包括 PCI-Express、Hublink (HL)、周邊組件互連（Peripheral Component Interconnect；簡稱 PCI）、及類似系統的各種通訊協定。每一 I/O 單元或所有單元的一子集可專用一獨立的 NoDMA 快取記憶體（109），以便改善 NoDMA 驗證的效能。在另一實施例中，一 I/O 來源（115）可以是被直接連接到北橋晶片組（117）的一組周邊裝置。

圖 2 是北橋晶片組（117）的一方塊圖。該圖示出用來支援自一周邊裝置（217）至系統記憶體（101）的一記憶體存取要求以及所要求的或送出的資料的送回之結

(7)

構。網路或各周邊裝置（217）經由一實體層（215）及鏈結層（213）而與 I/O 單元（250）的送入處理器或邏輯（209）以及送出處理器或邏輯（211）通訊。送入處理器（209）接收來自鏈結層（213）的記憶體存取要求及訊息，並將這些訊息放置在送入佇列（201）中。在一實施例中，係由用來分別處理一特定類型的訊息或要求或一組規定的要求或訊息類型之若干佇列分別構成送入佇列（201）及送出佇列（203）。送入佇列控制器（207）管理 CDB 介面（113）所讀取且通過佇列（201）的資料之移動。CDB 介面（113）處理記憶體存取要求，且可產生將被傳送到送出佇列（203）的回應訊息（例如，在處理讀取作業時）。送出佇列控制器（205）控制經過送出佇列（203）的資料流。

在一實施例中，設有對應於 PCI-Express、HL、PCI、或其他類似系統所使用的訊息或記憶體存取類型之多個送入及送出佇列（201）及（203）。送出處理器（211）將回應資料經由鏈結層（213）及實體層（215）而傳送到各周邊裝置（217）。在一實施例中，送出邏輯（211）及送入處理器（209）處理來自在與北橋晶片組（117）不同的一速度下運作的一 I/O 通訊匯流排之資料的傳輸。

在一實施例中，CDB 介面（113）及 CDB（107）在送入佇列（201）中進行預測，而執行對所要求記憶體內容的預測式預先提取。CDB 介面（113）負責向 CDB

(8)

提出要求，並服務該等要求。CDB 介面（113）強制執行對系統記憶體（101）的存取權，追蹤向 CDB（107）提出的尚未完成之要求，服務尚未完成的 DMA 讀取要求，執行 DMA 寫入，追蹤送入的完成狀態，中斷及執行類似的功能。

CDB 介面（113）執行對來自 I/O 裝置的記憶體存取之存取權檢查，以便確保系統中之安全。如果一 I/O 裝置嘗試存取記憶體中該 I/O 裝置並無存取權的一區域，則 CDB 介面（113）拒絕所要求的存取。CDB 介面（113）針對記憶體讀取或需要完成的任何存取，而傳送一主控裝置異常中斷回應，將該存取是無效的訊息告知提出要求的裝置。對於記憶體寫入及不需要一回應的其他交易而言，CDB 介面（113）的控制邏輯捨棄該寫入。不論是在哪一種情形，北橋晶片組（117）都記錄安全違反的狀況。

CDB（107）與 CDB 介面（113）、記憶體匯流排介面（231）、CPU 匯流排介面（227）、及其他介面（229）互動，以便在輸入-輸出單元（250）、處理器匯流排（119）、與記憶體匯流排（121）之間繞送及轉送資料。在一實施例中，CDB（107）也處理對系統管理匯流排（System management Bus；簡稱 SMBus）、測試行動聯合組織埠（Joint Test Action Group；簡稱 JTAG）（225）、或類似介面的輸入及輸出。

在一實施例中，當接收到 SMBus、JTAG、及類似介

(9)

面的存取時，北橋晶片組（117）即檢查 NoDMA 快取記憶體（109）及 NoDMA 表（103）。這些介面容許系統管理員或維修人員監視並診斷一系統。係以類似於周邊裝置的記憶體存取之方式處理來自 SMBus、JTAG、或類似介面的記憶體存取。將來自 SMBus、JTAG、或類似介面的記憶體存取與 NoDMA 表（103）及 NoDMA 快取記憶體（109）比對。此種方式甚至可使系統管理員或維修人員無法規避作業系統的保護機制而存取具有祕密資訊的頁。在另一實施例中，可將北橋晶片組（117）的組態設定成不將 SMBus、JTAG、及類似介面的存取比對 NoDMA 表，或者可調整一安全等級設定值，以便起動或關閉對這些介面的 NoDMA 檢查。

圖 3 示出一 NoDMA 快取記憶體（109）之結構。在一實施例中，快取記憶體（109）存取系統記憶體（101）中之 NoDMA 表（103），而降低頻寬耗損。NoDMA 表（103）及快取記憶體（109）不需要用來追蹤具有祕密資訊的頁之一記憶體區塊對映表。在一實施例中，係針對系統快取線容量而將電腦系統（100）中之記憶體存取最佳化。該系統的快取記憶體是用來對系統記憶體進行記憶體存取的一般快取記憶體。

在一實施例中，NoDMA 快取記憶體（109）包含一內容可定址的記憶體（Content Addressable Memory；簡稱 CAM）結構（301）及祕密儲存資訊結構（302）。CAM 結構（301）將資訊儲存在 "各列" 中。每一列對

(10)

應於系統記憶體（101）中儲存的 NoDMA 表（103）中一資料項（例如一頁祕密指示器）。在一實施例中，CAM 結構（301）儲存或固有地包含一索引（303）。係配合快取記憶體取代機制而使用該索引，以便識別並取代各快取線。在一實施例中，CAM 結構（301）並未顯性地儲存索引（303），這是因為硬體中之邏輯電路知道哪一資料項對應於一索引。

位址標記儲存欄位（305）中儲存的位址定址到 CAM 結構（301）。'有效' 儲存位元欄位（307）指示該等列中之資料項是否為有效的。如果寫入或改變了與快取列對應的頁，則將會清除有效位元，這是因為該頁的內容不再是已知的，因而無法知道該頁中是否儲存了受保護的資訊。

在一實施例中，CAM 結構（301）也儲存了諸如最近最少使用（Least Recently Used；簡稱 LRU）位元（309）等的快取記憶體管理資訊。利用 CAM 結構（301）的該欄位（309）來追蹤該資料項的相對存在時間，以便可以最近的或較常被使用的資料項來取代較舊的或不常被使用的資料項。可將任何快取記憶體管理及取代機制用於 NoDMA 快取記憶體（109）。祕密資訊儲存裝置（302）為 NoDMA 表（103）中之每一資料項儲存兩個獨立的祕密指示器。頁祕密欄位（311）指示記憶體（101）的一頁是否存放有受保護的資訊。該頁祕密指示器可以是將對應於快取記憶體（109）的同一列中之

(11)

NoDMA 表位址的頁之狀態（例如存放有受保護的資訊）編碼之一位元或一組位元。

一超頁祕密欄位（313）指示被資料項定址到的頁所屬的一組頁是否包含受保護的資訊。在一實施例中，一超頁是一組連續的頁。可由作業系統、BIOS、或類似的軟體設定一超頁的容量。在一實施例中，每一超頁中有512個頁。在一實施例中，係將一NoDMA表（103）的該等位元聚集到與系統快取線容量及記憶體存取容量對應的各超頁中。超頁祕密指示器（313）可以是一單一的位元或一組位元。在一實施例中，當將一個新的資料項放入NoDMA快取記憶體（109）時，即計算超頁。將對應於該超頁的所有位元以及對應於該新資料項的特定頁位元擷取到快取記憶體（109）中。對這些位元執行邏輯“或”運算，以便決定一單一超頁位元的值。在一實施例中，係以多個位元來代表超頁。然後使用一邏輯“或”運算來計算該超頁，以便決定該超頁中對應於每一位元的每一子區段。例如，可以NoDMA快取記憶體（109）中之四個超頁位元來代表512個連續的頁，而每一超頁位元對應於一組的128個頁。可調整超頁的容量，以便對應於存取的容量。一單一超頁或多個超頁可對應於快取線存取的容量。在一實施例中，該組頁的容量等於記憶體控制器的自然存取容量。

在一實施例中，係由下述兩部分構成CAM的位址標記（305）：一超頁、及該超頁內的一頁位移量。當

I/O 單元 (250) 接收到一存取時，進來的位址通過該 CAM 結構。如果有效位元被設定了，則每一列將該進來的位址與位址標記 (305) 比較。在每一列中共有三種可能的結果。在第一種結果中，超頁及頁位移量都相匹配（且有效位元被設定）；在第二種結果中，只有頁位移量與進來的位址相匹配（且有效位元被設定）；以及在第三種結果中，超頁及頁位移量都不相匹配，或有效位元並未被設定。至多一列將有第一種結果。在此種情形中，使用對應的頁祕密指示器 (311) 來決定對記憶體存取要求的進來的位址之存取權。如果該進來的位址無法匹配位址標記 (305) 的超頁及頁位移量，則使用具有一頁位移量匹配的一快取列。如果超頁祕密指示器 (313) 指示屬於該超頁的任何頁中並無任何祕密資訊，則授予存取權。並不需要進一步查詢 NoDMA 表 (103)。然而，如果超頁祕密指示器 (313) 指示該超頁中之至少一頁具有祕密資訊，則北橋晶片組 (117) 查詢 NoDMA 表 (103)，以便決定所要求的記憶體存取頁是否存放有祕密資訊。快取記憶體 (109) 中之多個資料項可能將有匹配的超頁位址標記 (305)。在此種情形中，可使用任何超頁匹配的列。如果快取記憶體 (109) 中並無任何列有一匹配的超頁位址，則需要存取 NoDMA 表 (103)。

在一實施例中，由於使用了一 NoDMA 表 (103)，所以可將電腦系統 (100) 擴充到較大容量的系統記憶體 (101)（例如大於 4 GB (GB：十億位元組)），且可

動態地調整記憶體容量（例如在可將記憶體熱插拔到系統中之情形下）。由於支援動態調整記憶體的容量且使用超頁及頁，所以可在無須系統重設的情形下，變動驗證記憶體存取時的容量分割程度。一超頁可由多個位元所構成，以便控制一超頁代表的區段容量之分割程度。額外的位元可讓超頁代表較小的記憶體區段，且用來作為受保護的資訊所在位置的更精確之指示。由較少位元所代表的超頁尤其在超頁指示器產生方面降低了 NoDMA 快取系統的複雜性。當使用較少的位元時，簡化了一邏輯 "或" 的實施。由於藉由改變用來代表一超頁的位元數而變動容量的分割程度，所以可根據一系統的需求，而對速度或較小的空間需求方面進行較大幅度的設計客製化。

在一實施例中，NoDMA 快取記憶體（109）及北橋晶片組（117）處理與 NoDMA 快取記憶體（109）的功能有關的一組指令。可以獨立的指令起動或關閉快取記憶體（109）。一起動指令起動 NoDMA 快取記憶體的使用，清除快取記憶體（109）中儲存資料項的所有有效位元，並設定用來指示 NoDMA 快取記憶體（109）的起動狀態的北橋晶片組（117）及快取記憶體暫存器中之狀態位元。一關閉指令關閉 NoDMA 快取記憶體（109），並清除用來指示快取記憶體（109）的起動狀態的北橋晶片組（117）及快取記憶體（109）的暫存器中之狀態位元。可關閉 NoDMA 快取記憶體（109），但同時起動 NoDMA 表（103）。一使無效指令清除快取記憶體中之

所有資料項的有效位元。

在一實施例中，係將一邏輯 "1" 或一組邏輯 "1" 儲存在適當的欄位，而 "設定" 諸如一超頁位元、頁位元、LRU 位元、或類似的被儲存值等的一位元或被儲存值。可儲存其中包括一邏輯 "0" 的任何值，而在邏輯上 "設定" 一位元或被儲存值。係參照一 "設定" 作業而界定該被指定的值。同樣地，一位元或被儲存值的一 "清除" 作業可使用與該 "設定" 指示器的值不同之任何被指定的值。

在一實施例中，係由諸如作業系統等的軟體維護 NoDMA 快取記憶體 (109)。當容許寫入作業時，作業系統負責適當地使 NoDMA 快取記憶體 (109) 中之被寫入區域的參考位址無效。在一實施例中，一作業系統識別 NoDMA 表 (103)，以便識別祕密頁。該作業系統也決定當正在檢查 NoDMA 表 (103) 或 NoDMA 快取記憶體 (109) 時是否有其他的記憶體存取正在進行中。

圖 4 是 NoDMA 快取記憶體 (109) 的作業之一流程圖。在一實施例中，CDB (107) 及 CDB 介面 (113) 在步驟 (401) 中處理記憶體存取要求。CDB 介面 (113) 檢查 NoDMA 快取記憶體 (109)，以便決定被要求存取的一位址是否被儲存在快取記憶體 (109) 中。在步驟 (403) 中，使用 CAM 結構 (301)，而將所要求的位址與快取記憶體 (109) 中儲存的位址標記 (305) 比較。如果在快取記憶體 (109) 中找到與配要求的頁位

(15)

址相匹配的一標記（305），則在步驟（405）中檢查對應的有效位元，以便決定該快取記憶體資料項是否仍然有效。如果該有效位元被設定，則在步驟（409）中檢查頁祕密指示器（311）。如果該祕密指示器被設定，則在步驟（417）中拒絕該存取，並記錄一錯誤。如果該祕密指示器並未被設定，則在步驟（419）中容許該存取。

在一實施例中，當並未為一要求的頁找到快取記憶體（109）中之一資料項，則檢查快取記憶體（109），以便決定受保護的資訊是否被儲存在超頁中。首先，在步驟（411）中檢查位址標記（305），以便決定是否能找到一對應的超頁資料項。如果找到了一資料項，則在步驟（413）中檢查及有效性。如果找到了超頁資料項，且在步驟（415）中決定並無任何受到保護的資料被儲存在該超頁中，則在步驟（419）中容許該記憶體存取要求繼續進行。如果超頁祕密指示器（313）被設定，則在步驟（417）中拒絕該存取，並記錄一錯誤。

在一實施例中，如果在快取記憶體（109）中並未找到所要求的超頁位址，或者該資料項不是有效的，則在步驟（407）中自系統記憶體（101）中儲存的 NoDMA 表（103）擷取該頁的祕密資訊。將位址標記儲存在一可用的快取記憶體列中，並清除該列的有效位元。然後在步驟（421）中，將自 NoDMA 表（103）中擷取的資料儲存在 NoDMA 快取記憶體（109）中。在快取記憶體（109）中產生的資料項包括頁祕密指示器（311）及超頁

祕密指示器（313）。在步驟（423）中，根據對該超頁中之該等頁的一邏輯“或”運算而計算出超頁祕密指示器（313），並儲存該超頁祕密指示器（313）。在一實施例中，將擷取特硬頁的祕密資訊，定將該祕密資訊儲存為一資料項。在另一實施例中，該資料項將對應於該超頁中之第一頁。在另一實施例中，該資料項可對應於該超頁中之任一頁。當產生該資料項時，在步驟（425）中設定該資料項的有效位元。

當一頁中有受保護的資訊時，在步驟（417）中不容許該記憶體存取。可根據記憶體存取的類型（例如讀取或寫入）而送回一錯誤回應訊息（例如，如果拒絕了一讀取作業，則將以一錯誤回應訊息取代正常回應訊息）。記錄錯誤及被拒絕的存取，以供後續的分析，而決定錯誤的原因，或決定是否有人進行了一惡意的要求或攻擊。在一實施例中，可界定（例如由作業系統設定）會產生錯誤或安全記錄的要求類型。在一實施例中，北橋晶片組（117）記錄一嚴重錯誤並重設系統，而回應賴自 NoDMA 快取記憶體（109）的一存取違反。錯誤包括存取一具有祕密資訊的頁、或在不被容許時存取 NoDMA 表（103）。錯誤被記錄在錯誤暫存器中。該等錯誤暫存器可映射所偵測到的某一錯誤之適當信號通知方法。可能要求記憶體存取的 I/O 裝置不得存取該等錯誤暫存器。

在一實施例中，係以軟體（例如微碼或高階電腦語言）來實施 NoDMA 快取記憶體（109）。亦可利用軟體

(17)

實施例來執行 NoDMA 快取記憶體 (109) 的模擬或模仿。可將一軟體實施例儲存在一機器可讀取的媒體中。" 機器可讀取的 " 媒體可包括可儲存或轉移資訊的任何媒體。機器可讀取的媒體之例子包括 ROM、軟碟、CD-ROM、光碟、硬碟、射頻 (RF) 鏈路、或類似的媒體。

在前文的說明書中，已參照本發明的一些特定實施例而說明了本發明。然而，在不脫離最後的申請專利範圍中述及的本發明之廣義精神及範圍下，顯然仍可對本發明作出各種修改及改變。因此，應將本說明書及圖式視為舉例說明，而非對本發明加以限制。

【圖式簡單說明】

係參照各附圖而以舉例說明但非限制性之方式解說本發明的各實施例，而在這些附圖中，相同的代號指示類似的元件。我們當了解，在本說明書的揭示中，參照到 "一" 或 "一個" 實施例時並不必然意指相同的實施例，且此種參照至少一個實施例。

圖 1 是其中包括一 NoDMA 快取記憶體的一電腦系統之一方塊圖。

圖 2 是經過一實施 NoDMA 的晶片組的輸入及輸出資料流之一方塊圖。

圖 3 示出一 NoDMA 快取記憶體結構。

圖 4 是一 NoDMA 快取記憶體系統之一流程圖。

主要元件對照表

100	電腦系統
101	系統記憶體
105	中央處理單元
117	北橋晶片組
119	處理器匯流排
121	記憶體匯流排
103	無直接記憶體存取表
115	I/O 裝置
113	CDB 介面
107	中央資料緩衝區
109	無直接記憶體存取快取記憶體
217	周邊裝置
215	實體層
213	鏈結層
209	送入處理器
211	送出處理器
250	I/O 單元
201	送入佇列
203	送出佇列
205	送出佇列控制器
207	送入佇列控制器
231	記憶體匯流排介面
227	CPU 匯流排介面

2 2 9	其 他 介 面
2 2 5	系 統 管 理 匯 流 排 、 測 試 行 動 聯 合 組 織 埠
3 0 1	內 容 可 定 址 的 記 憶 體 結 構
3 0 2	祕 密 儲 存 資 訊 結 構
3 0 3	索 引
3 0 5	位 址 標 記 儲 存 欄 位
3 0 7	有 效 儲 存 位 元 欄 位
3 0 9	最 近 最 少 使 用 位 元
3 1 1	頁 祕 密 欄 位
3 1 3	超 頁 祕 密 欄 位

圖1

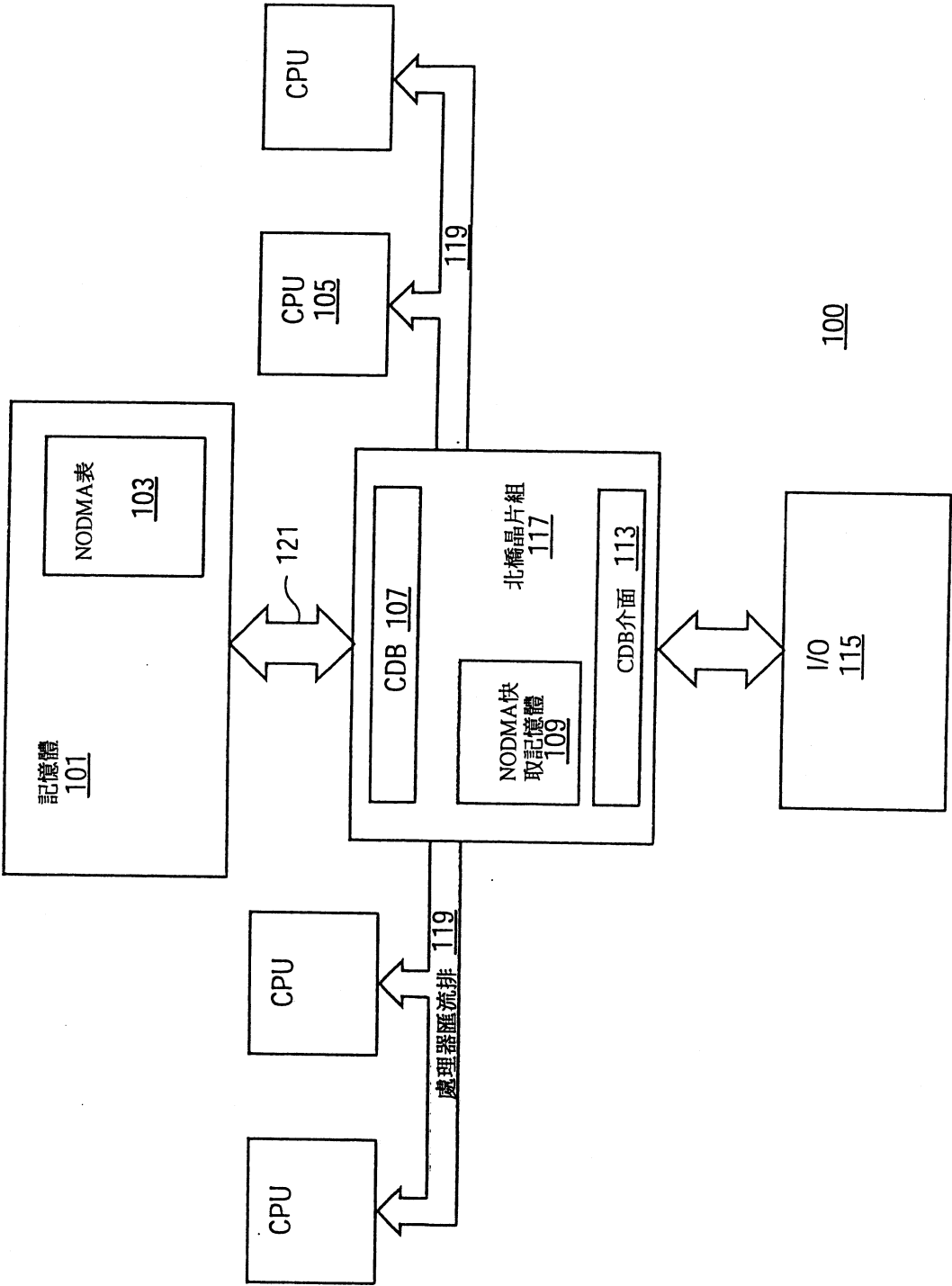


圖 2

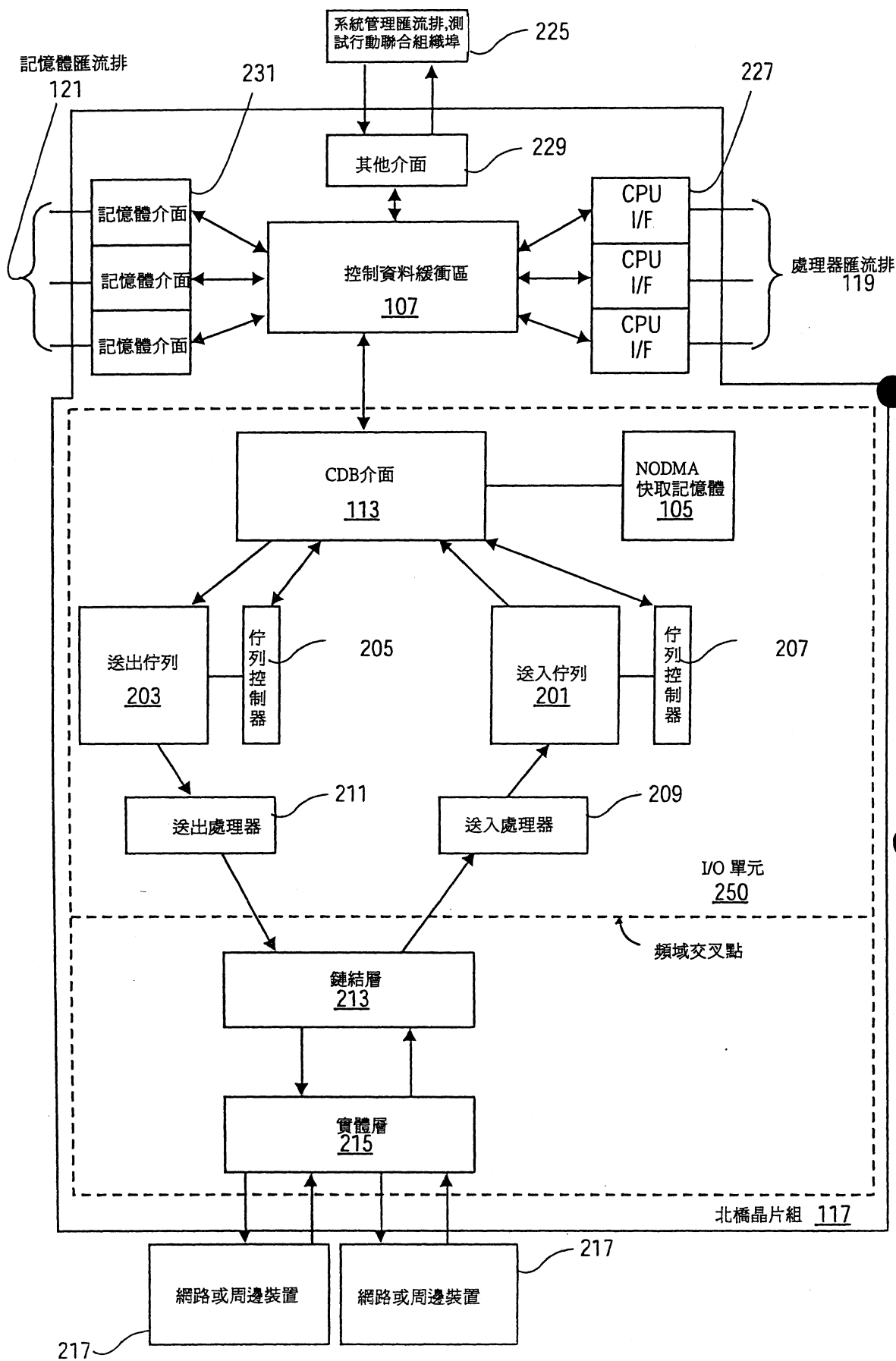


圖 3

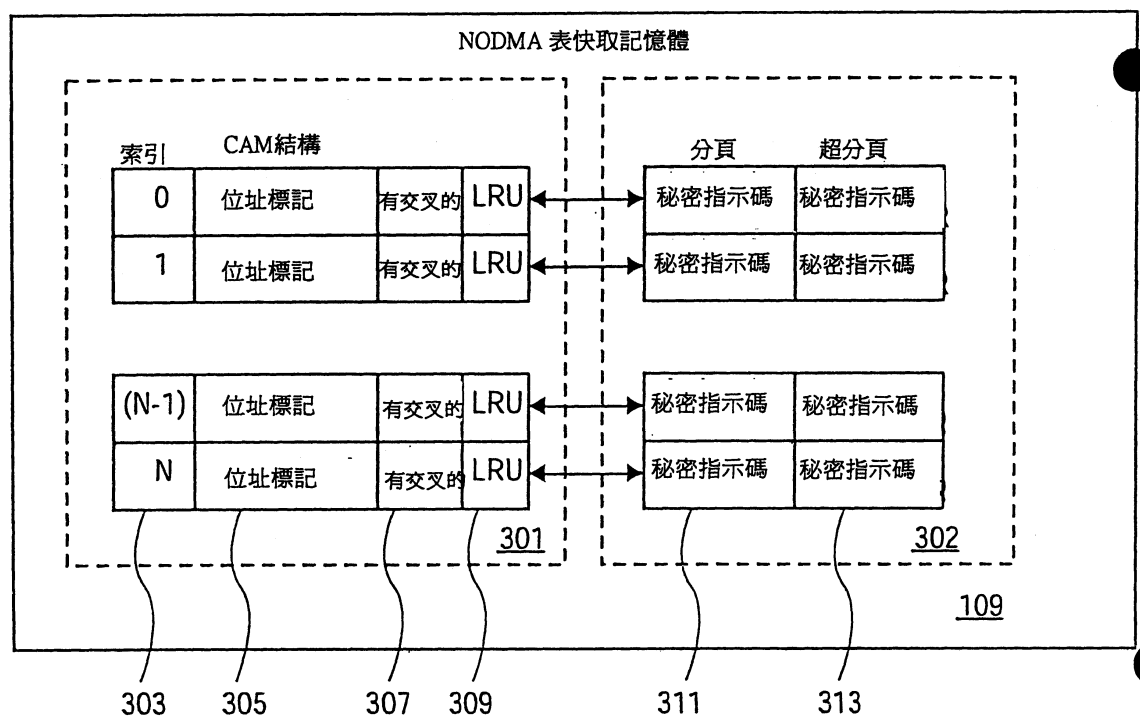
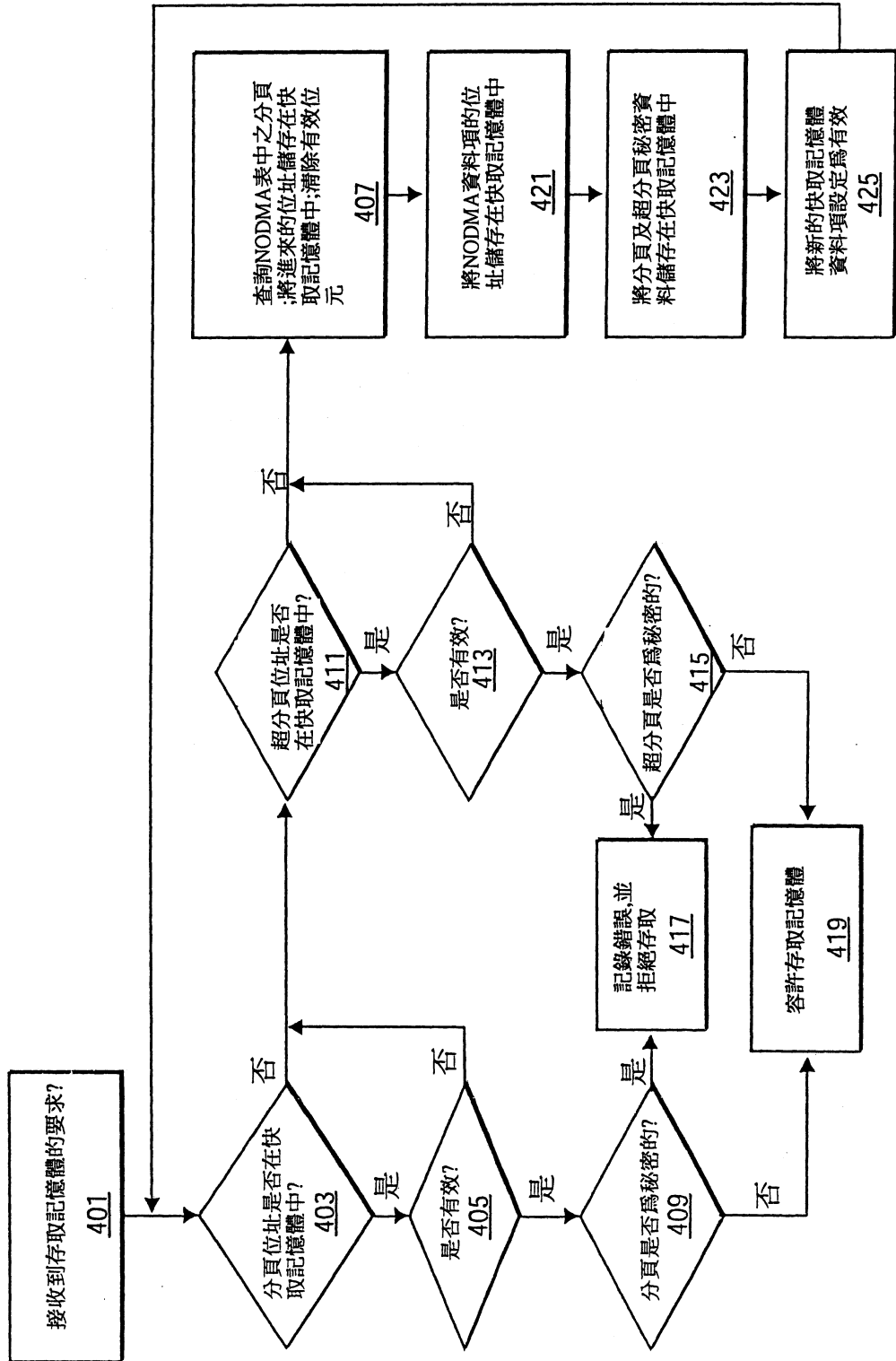


圖4

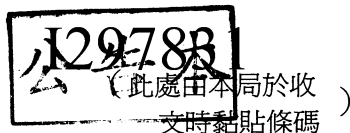


柒、(一)、本案指定代表圖為：第 1 圖

(二)、本代表圖之元件代表符號簡單說明：

100	電腦系統
101	系統記憶體
105	中央處理單元
117	北橋晶片組
119	處理器匯流排
121	記憶體匯流排
103	無直接記憶體存取表
115	I/O 裝置
113	CDB 介面
107	中央資料緩衝區
109	無直接記憶體存取快取記憶體

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無



附件 2A

第 93103219 號專利申請案

中文說明書換頁

97. 2. -5

民國 97 年 2 月 5 日修正

843355

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：93103219

※申請日期：93 年 02 月 11 日

※IPC 分類：G06F12/08 (2006.01)

壹、發明名稱：

(中) 管理記憶體裝置之方法、電腦系統、以及電腦可讀取媒體

(英) Method for managing a memory device, computer system and computer-readable medium

貳、申請人：(共 1 人)

1. 姓 名：(中) 英特爾股份有限公司

(英) INTEL CORPORATION

代表人：(中) 1. 大衛 賽門

(英) 1. SIMON, DAVID

地 址：(中) 美國加州聖大克拉瑞密遜學院路二二〇〇號

(英) 2200 Mission College Blvd., Santa Clara, CA 95052, USA

國籍：(中英) 美國 U.S.A.

參、發明人：(共 2 人)

1. 姓 名：(中) 德班卓拉 沙瑪

(英) SHARMA, DEBENDRA DAS

地 址：(中) 美國加州聖克拉拉艾卡西亞廣場二〇四三號

(英) 2043 Acacia Court, Santa Clara, CA 95050, U. S. A.

2. 姓 名：(中) 羅伯特 沙法蘭克

(英) SAFRANEK, ROBERT

地 址：(中) 美國奧勒岡州波特蘭西北內坎尼肯瓦五八一六號

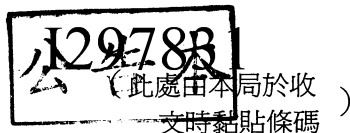
(英) 5816 NW Necanicum Wah, Portland, OR 97229, U. S. A.

肆、聲明事項：

◎本案申請前已向下列國家(地區)申請專利 ☐ 主張國際優先權：

【格式請依：受理國家(地區)；申請日；申請案號數 順序註記】

1. 美國 ; 2003/03/31 ; 10/404,881 ☒ 有主張優先權



附件 2A

第 93103219 號專利申請案

中文說明書換頁

97. 2. -5

民國 97 年 2 月 5 日修正

843355

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：93103219

※申請日期：93 年 02 月 11 日

※IPC 分類：G06F12/08 (2006.01)

壹、發明名稱：

(中) 管理記憶體裝置之方法、電腦系統、以及電腦可讀取媒體

(英) Method for managing a memory device, computer system and computer-readable medium

貳、申請人：(共 1 人)

1. 姓 名：(中) 英特爾股份有限公司

(英) INTEL CORPORATION

代表人：(中) 1. 大衛 賽門

(英) 1. SIMON, DAVID

地 址：(中) 美國加州聖大克拉瑞密遜學院路二二〇〇號

(英) 2200 Mission College Blvd., Santa Clara, CA 95052, USA

國籍：(中英) 美國 U.S.A.

參、發明人：(共 2 人)

1. 姓 名：(中) 德班卓拉 沙瑪

(英) SHARMA, DEBENDRA DAS

地 址：(中) 美國加州聖克拉拉艾卡西亞廣場二〇四三號

(英) 2043 Acacia Court, Santa Clara, CA 95050, U. S. A.

2. 姓 名：(中) 羅伯特 沙法蘭克

(英) SAFRANEK, ROBERT

地 址：(中) 美國奧勒岡州波特蘭西北內坎尼肯瓦五八一六號

(英) 5816 NW Necanicum Wah, Portland, OR 97229, U. S. A.

肆、聲明事項：

◎本案申請前已向下列國家(地區)申請專利 ☐ 主張國際優先權：

【格式請依：受理國家(地區)；申請日；申請案號數 順序註記】

1. 美國 ; 2003/03/31 ; 10/404,881 ☒ 有主張優先權

伍、中文發明摘要

發明之名稱：管理記

憶體裝置之方法、電腦系統、以及電腦
可讀取媒體

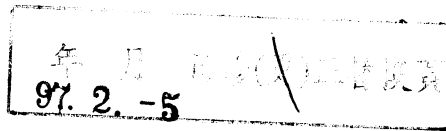
本發明揭示了一種包含一超頁欄位之無直接記憶體存取快取記憶體。該超頁欄位指示一組頁存放有受保護的資訊之時機。一電腦系統利用該無直接記憶體存取快取記憶體來拒絕 I/O 裝置對系統記憶體中之受保護的資訊之存取。

陸、英文發明摘要

發明之名稱：

Method for managing a memory device, computer system and
computer-readable medium

A NoDMA cache including a super page field. The super page field indicates when a set of pages contain protected information. The NoDMA cache is used by a computer system to deny I/O device access to protected information in system memory.



拾、申請專利範圍

附件 4A：第 93103219 號專利申請案

中文申請專利範圍替換本

民國 97 年 2 月 5 日修正

1. 一種管理記憶體裝置之方法，包含：

接收來自客戶端存取記憶體內容的請求；

將記憶體分為數個區段，該些記憶體區段的各個區段代表具有該記憶體內容的分頁；

將記憶體存取表和該些記憶體區段相關聯，該記憶體存取表具有位元連續組；

追蹤該些記憶體區段，以決定該記憶體內容是否包括受保護內容；

藉由檢查該記憶體內容是否包括受保護內容以及該客戶端是否被授權存取該受保護內容，以決定該客戶端是否被允許存取該記憶體內容；

當該記憶體內容未包括該受保護內容時，或是當該記憶體內容包括該受保護內容且該客戶端被授權存取該受保護內容時，則允許該客戶端存取該記憶體內容；以及

當該記憶體內容包括該受保護內容且該客戶端未被授權存取該受保護資料時，則拒絕該客戶端存取該記憶體內容。

2. 如申請專利範圍第 1 項之方法，其中決定該客戶端是否被允許存取該記憶體內容係包括：檢查和該記憶體存取表相關聯的記憶體指示器。

3. 如申請專利範圍第 2 項之方法，更包含：假如該記憶體指示器未被設定，則允許該客戶端存取該記憶體內容，以及假如該記憶體指示器被設定，則拒絕該客戶端存取該記憶體內容。

4. 如申請專利範圍第 3 項之方法，更包含：假如該記憶體指示器被設定，則產生違反指示器，該違反指示器包括一錯誤。

5. 如申請專利範圍第 4 項之方法，其中該錯誤指出由該客戶端存取該記憶體內容的失敗嘗試。

6. 一種電腦系統，包含：

儲存媒體，其耦合至具有快取記憶體和處理器的伺服器，以及輸入/輸出(I/O)裝置，該儲存媒體具有記憶體存取表，以及用以幫助該處理器執行任務的數個指令；以及該處理器用以：

接收來自客戶端存取記憶體內容的請求，該客戶端耦合至該伺服器，

將記憶體分為數個區段，該些記憶體區段的各個區段代表具有該記憶體內容的分頁，

將記憶體存取表和該些記憶體區段相關聯，該記憶體存取表具有位元連續組，

追蹤該些記憶體區段，以決定該記憶體內容是否包括受保護內容，

藉由檢查該記憶體內容是否包括受保護內容以及該客戶端是否被授權存取該受保護內容，以決定該客戶端是否

被允許存取該記憶體內容，

當該記憶體內容未包括該受保護內容時，或是當該記憶體內容包括該受保護內容且該客戶端被授權存取該受保護內容時，則允許該客戶端存取該記憶體內容，以及

當該記憶體內容包括該受保護內容且該客戶端未被授權存取該受保護內容時，則拒絕該客戶端存取該記憶體內容。

7. 如申請專利範圍第 6 項之電腦系統，其中該快取包括無直接記憶體存取 (NoDMA) 之快取記憶體。

8. 如申請專利範圍第 6 項之電腦系統，其中該記憶體存取表包含 NoDMA 表，該 NoDMA 表係與該 NoDMA 快取記憶體相通訊。

9. 如申請專利範圍第 6 項之電腦系統，其中該處理器進一步用以經由錯誤分析器來分析登錄錯誤，其中該登錄錯誤指出由該客戶端存取該記憶體內容的失敗嘗試。

10. 一種電腦可讀取媒體，具有數個指令，當執行該些指令時，致使一機器：

接收來自客戶端存取記憶體內容的請求，該客戶端耦合至該伺服器；

將記憶體分為數個區段，該些記憶體區段的各個區段代表具有該記憶體內容的分頁；

將記憶體存取表和該些記憶體區段相關聯，該記憶體存取表具有位元連續組；

追蹤該些記憶體區段，以決定該記憶體內容是否包括

受保護內容；

藉由檢查該記憶體內容是否包括受保護內容以及該客戶端是否被授權存取該受保護內容，以決定該客戶端是否被允許存取該記憶體內容；

當該記憶體內容未包括該受保護內容時，或是當該記憶體內容包括該受保護內容且該客戶端被授權存取該受保護內容時，則允許該客戶端存取該記憶體內容；以及

當該記憶體內容包括該受保護內容且該客戶端未被授權存取該受保護內容時，則拒絕該客戶端存取該記憶體內容。

11. 如申請專利範圍第 10 項之電腦可讀取媒體，其中當執行該些指令時，進一步致使該機器：經由錯誤分析器來分析登錄錯誤，其中該登錄錯誤指出由該客戶端存取該記憶體內容的失敗嘗試。

12. 如申請專利範圍第 10 項之電腦可讀取媒體，其中當執行該些指令時，決定該客戶端是否被允許存取該記憶體內容係包括：檢查和該記憶體存取表相關聯的記憶體指示器。