I467373

公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：97121218

※ 申請日期：2008 年 6 月 6 日　　※IPC 分類：

G06F 12/08 (2006.01)

一、發明名稱：（中文/英文）

以交換式記憶體為手段來加速虛擬化及仿真化

LEVERAGING TRANSACTIONAL MEMORY HARDWARE TO ACCELERATE VIRTUALIZATION AND EMULATION

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾芊那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 3 人）

姓　名：（中文/英文）

1.泰勒費爾馬丁/TAILLEFER, MARTIN

2.米赫卡德瑞克/MIHOCKA, DAREK

3.席娃布諾/SILVA, BRUNO

國　籍：(中文/英文)

1.加拿大/CANADA

2.加拿大/CANADA

3.巴西/BRAZIL

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

美國；2007 年 6 月 27 日；11/823,224

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

揭示各種技術以供使用交換式記憶體硬體來加速虛擬化或仿真化。經由提供隔離私有狀態於交換式記憶體硬體上及儲存正在該隔離私有狀態中執行一仿真化之一主機的堆疊能夠來促進狀態隔離。由一中央處理單元所執行之記憶體存取能夠由軟體監控來偵測一經仿真化之訪客已經作出一自我修訂至其本身的碼序列。經由採取原子提交特徵之優勢，使用交換式記憶體硬體來促進多重執行緒環境中之配發表單。提供使用一儲存在主要記憶體中之配發表單以轉換一訪客程式計數器至一主機程式計數器的仿真器。可存取該配發表單以檢視該配發表單是否包含一針對一特定訪客程式計數器之特定主機程式計數器。

六、英文發明摘要：

Various technologies and techniques are disclosed for using transactional memory hardware to accelerate virtualization or emulation. State isolation can be facilitated by providing isolated private state on transactional memory hardware and storing the stack of a host that is performing an emulation in the isolated private state. Memory accesses performed by a central processing unit can be monitored by software to detect that a guest being emulated has made a self modification to its own code sequence. Transactional memory hardware can be used to facilitate dispatch table updates in multithreaded environments by taking advantage of the atomic commit feature. An emulator is provided that uses a dispatch table stored in main memory to convert a guest program counter into a host program counter. The dispatch table is accessed to see if the dispatch table contains a particular host program counter for a particular guest program counter.

七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖。

(二)、本代表圖之元件代表符號簡單說明：

120 私有狀態

124 軟體可視記憶體存取

126 原子提交

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

九、發明說明：

【發明所屬之技術領域】

本發明係關於執行交換式記憶體硬體以加速虛擬化及仿真化。

【先前技術】

仿真化（Emulation）係為一種涉及提供來自軟體之中央處理單元之功能的技術。仿真化的一項優勢係為吾人能夠執行針對一特定類型處理器所設計的軟體於任何類型處理器上。虛擬化（Virtualization）係為一種提供在允許超過一作業系統以上同時執行之一方式中分割硬體之能力的技術。使用虛擬化，一物質中央處理單元被分割成多個上下文配置。各上下文配置接著輪流直接執行於該處理器上。雖然虛擬化產品一般較快於仿真化產品，但今日該兩者類型之產品遭受許多限制能夠被達到之速度的障礙。例如，仿真化期間處理一致性需要額化的同步化作業，其能夠降低連續效能。又例如一第二例子，在仿真化下追蹤自我修訂碼通常會受到一實質上的效能負擔。

【發明內容】

各種技術係經揭示以供使用交換式記憶體硬體來加速虛擬化及仿真化。一或多種中央處理單元係經提供以可操作來加速虛擬化之交換式記憶體硬體。該交換式記憶體硬

體具有維持私有狀態之能力、呈現對軟體為可視之其他中央處理單元之記憶體存取的能力、以及該私有狀態之原子提交（atomic commit）的支援。

在一實施中，例如能夠使用該交換式記憶體硬體來促進精確例外語義的仿真化。該私有狀態可操作來致使一仿真狀態能夠維持不一致於一架構狀態且僅同步化於特定範圍。使用塊-精確模擬（chunk-accurate simulation）執行一最佳化的指令序列來嘗試以及達成如隔離在私有狀態中一較慢指令加速仿真化的一相同端效應（end effect），其僅在該整體塊經成功地仿真的案例中提交。

在另外的實施中，狀態隔離能夠經由提供隔離私有狀態於交換式記憶體硬體上及儲存正在該隔離私有狀態中執行仿真化之一主機（host）的堆疊。

在另外的實施中，使用該交換式記憶體硬體能夠偵測自我修訂碼。由一中央處理單元所執行之記憶體存取能夠由軟體監控來偵測一經仿真化的訪客已經作出自我修訂至其本身的碼序列。

在一具體實施例中，可使用交換式記憶體硬體來藉由採取該原子提交特徵之優勢以促進在多執行緒環境中之配發表單（dispatch table）更新。提供一仿真器來使用儲存在主記憶體中之配發表單以轉換一訪客程式計數器成一主機程式計數器。該配發表單可經存取來檢視該配發表單是否包含針對一特定訪客程式計數器之一特定主機程式計數器。當一主機程式計數器未被發現，交換式記憶體硬體能

夠被使用來引入一新映射於該表單中。

在另其他實施中，經由提供交換式記憶體硬體以支援一設施來維持私有記憶體狀態以及一原子提交特徵而能夠促進程式碼回插（code backpatching）。對特定程式碼所作出的改變可經儲存於該私有狀態設施。使用該原子提交特徵，經由企圖一次提交所有的改變至記憶體，頒佈（enact）回插改變。

在一實施中，可經由使用交換式記憶體硬體提供一有效率的呼叫返回快取。一儲存在該私有狀態設施中之呼叫返回快取捕獲一主機位址來返回至在執行一訪客函數完成之後。一直接查找硬體式雜湊表單經使用於該呼叫返回快取。

提供此發明內容係用於按一簡單之形式引介一概念之選項，其將於後之實施方式進一步的詳細說明。此發明內容並不意圖用來識別該所請求標的之關鍵特徵或必要特徵，亦不意圖來使用作為決定所請標的之範圍的協助。

【實施方式】

本技術係描述以在按如一虛擬化或仿真化系統的一般背景中，然而本技術也可用於除此描述外的其他用途。在另外實施中，該系統包含使用交換式記憶體硬體來加速虛擬化及/或仿真化的一或多個中央處理器。

如第1圖所示，使用範例性電腦系統，以供實施該系統之一或多個部份，其包含一計算裝置，例如計算裝置

100。在其最基本的組態中，計算裝置 100 一般包含至少一中央處理單元 102 及記憶體 104。(各)中央處理單元具有交換式記憶體硬體 119，其包含一維持私有狀態 120 的能力、一呈現來自對軟體 124 來說為可視之其他中央處理單元之記憶體存取的能力、以及該私有狀態之原子提交 126 的支援。該私有狀態 120 係不可視於其他中央處理單元，直到經由擁有處理單元其經明確原子化地提交。該私有狀態也為可棄式。當該中央處理放棄該私有狀態，其記憶體之檢視經回復至該目前架構狀態。該軟體可視記憶體存取 124 允許執行在該中央處理單元上之軟體，以偵測另外中央處理單元正存取特定記憶體位置。該原子提交特徵 126 允許該中央處理單元之私有狀態來原子化地進入一主要記憶體系統作為如一原子提交之部分的一單元。該些交換式記憶體硬體特徵係經使用在各種情況以供強化如此中所更進一步細節描述的虛擬化及/或仿真化。

基於精確組態及計算裝置類型，記憶體 104 可為揮發性(例如 RAM)、非揮發性(例如 ROM、快閃記憶體等)、或以上兩種之組合。此基本組係經虛線 106 於第 1 圖中所描述。

此外，裝置 100 也可具有額外的特徵/功能。例如，裝置 100 也可包含額外儲存體(可抽取式及/或非可抽取式)，其包含(但不限於)磁性或光學性碟或帶。這樣的額外儲存體係由可抽取儲存體 108 及非可抽取儲存體 110 描述於第 1 圖中。電腦儲存媒體包含揮發及非揮發性、可抽

取及非可抽取式媒體，其可在儲存資訊之任何方法或技術中經實施，該資訊例如電腦可讀指令、資料結構、程式模組或其他資料。記憶體 104、可抽取儲存體 108 及非可抽取儲存體 110 皆為電腦儲存媒體之範例。電腦儲存媒體包含（但不限於）RAM、ROM、EEPROM、快閃記憶體或其他技術、CD-ROM、DVD 或其他光學性儲存體、磁匣、磁帶、磁碟儲存、或其他磁性儲存裝置、或任何可被用於儲存期望資訊以及可由裝置 100 所存取之其他媒體。任何這樣的電腦儲存媒體可為裝置 100 之部分。

電腦裝置 100 包含一或多個通訊連接 114，其允許電腦裝置 100 與其他電腦/應用程式 115 進行通訊。裝置 100 也可具有輸入裝置 112，例如鍵盤、滑鼠、指示筆、聲音輸入裝置、觸碰輸入裝置等等。也可包含輸出裝置 111，例如顯示器、麥克風、印表機等等。該些裝置在該領域中以為周知，因此將不在此作細節討論。在一實施中，計算裝置 100 包含虛擬化/仿真化應用程式 200。虛擬化/仿真化應用程式 200 將於第 2 圖中作更進一步之討論。

接續第 1 圖現參照第 2 圖，其描述一操作在計算裝置 100 中之虛擬化/仿真化應用程式 200。虛擬化/仿真化應用程式 200 係為駐存在計算裝置 100 上之各應用程式之一者。然而，應可瞭解，虛擬化/仿真化應用程式 200 能夠替換地或額外地被具體實施化為在一或多個電腦電腦上之可執行指令及/或在相較第 1 圖所示之組態的不同變化者上。替代地或額外地，虛擬化/仿真化應用程式 200 之一或

多個部份可為系統記憶體 104 之部分、在其他電腦及/或應用程式 115 上、或其他將發生至該電腦軟體技術中之一者的變化上。

虛擬化/仿真化應用程式 200 包含程式邏輯 204，其係負責於實現如此中所述之各技術之特定者或所有者。程式邏輯 204 包含使用交換式記憶體硬體來加速虛擬化或仿真化 206 之邏輯（如下第 3 圖所相關性的描述）、使用交換式記憶體硬體來促進精確例外語義 208 之仿真化的邏輯（如下第 3-5 圖所相關性的描述）、使用交換式記憶體硬體來促進狀態隔離 210 之邏輯（如下第 6 圖所相關性的描述）、使用交換式記憶體硬體來促進偵測自我修正碼 212 之邏輯（如下第 7 圖所相關性的描述）、使用交換式記憶體硬體來促進配發表單更新 214 之邏輯（如下第 8 圖所相關性的描述）、使用交換式記憶體硬體來促進碼回插 216 之邏輯（如下第 9 圖所相關性的描述）、使用交換式記憶體硬體來促進一有效率之呼叫返回快取 218 的邏輯（如下第 10 圖所相關性的描述）、以及其他操作應用程式 220 之邏輯。在一實施中，程式邏輯 204 係經操作以自另外程式被程式化地呼叫，其例如使用一單一呼叫至程式邏輯 204 中之一程序。

接續第 1-2 圖現參照第 3-10 圖，實施虛擬化/仿真化應用程式 200 之一或多具體實施例係更進一步的描述。在特定實施中，第 3-10 圖之處理係至少部份地實作在計算裝置 100 之操作邏輯中。第 3 圖描述涉及使用交換式記憶體硬體來促進精確例外語義之仿真化的各階段之一具體實施

例。該處理起始於開始點 240，使用非可視式及可棄式之私有狀態於該交易式記憶體硬體中，來致使該仿真化狀態能夠來維持與該架構狀態之不一致性且僅在該粗劣的範圍上進行同步化（階段 242）。該系統使用一塊-精確仿真化來執行各指令之最佳化序列（階段 244）。如果無例外發生（決定點 246），該系統能夠完成具有相較於將可能使用全指令-精確仿真化之一般較佳效能的仿真化。然而，如果意外發生（決定點 246），接著該至記憶體之待決寫入經放棄（階段 248）。該仿真化處理器狀態係捲返回至該上一次同步點（階段 250）。該特定碼序列係使用指令-精確仿真化經再次穩當地執行，以致使該正確架構狀態當該例外第二次遇到時經呈現（階段 252）。在一實施中，該架構狀態係精確相同於真實，經仿真化之非虛擬系統將被置於其中，其對於校正系統-階層仿真化係具重要性。此處理係將於第 4 及 5 圖中更進一步地細節描述。該處理結束於點 254。

現參照第 4 及 5 圖，使用交換式記憶體硬體來在仿真化環境中促進精確例外語義之仿真化。第 4 圖係為一圖式 270，其係描述運作一塊-精確仿真化之實施的具體實施例。該塊-精確仿真化運作一最佳化序列的指令，藉以嘗試及達成如該原始序列之訪客指令的相同端效應，除在相較於可能使用一指令-精確仿真化的最佳化方式外。該塊-精確仿真化允許該仿真化狀態維持與該架構狀態之非一致化且僅在粗劣範圍上進行同步化，其基本上係為該仿真化之起始點及結束點。如果一例外在該塊-精確仿真化期間在任

何點處經遭遇，該在第 5 圖之圖式 290 上所描述之指令-精確仿真化接著經執行。該指令-精確仿真化穩當地運作該碼序列以確保當該例外遭遇第二次時呈現該正確架構狀態。

第 6 圖係描述涉及使用交換式記憶體硬體來促進狀態隔離之各階段的一實施。該處理開始於起始點 310，提供隔離的私有狀態於交換式記憶體硬體上（階段 312）。在一仿真化環境中，執行該仿真化之主機儲存他的堆疊於該隔離的私有狀態中（階段 314）。該隔離的私有狀態致使該主機能夠來將該堆疊保持在一緩衝的模式中，其允許該主機來避免昂貴的執行時間檢查。該隔離的私有狀態係為可棄式。此意指了當該中央處理單元放棄該私有狀態時，回復其記憶體的檢視至該目前的架構狀態。該經仿真化之訪客不具有對該隔離的私有狀態之存取（階段 316）。該處理結束於結束點 318。

第 7 圖係為描述涉及使用交換式記憶體硬體來促進偵測自我修訂碼的各階段之一實施。該處理起始於開始點 340，使用交換式記憶體硬體提供軟體-可視式記憶體存取（階段 342）。該系統監控該由中央處理單元所執行的記憶體存取，藉以偵測經仿真化之訪客已經修改其自我碼序列（階段 344）。即便來自一個別中央處理單元的記憶體存取也能夠被偵測。該系統接著基於該偵測採取適當動作（階段 346）。該些適當動作之一些非限定範圍包含重新編譯該碼序列以併入由該訪客所作出之自我修訂、升起一例外、

及/或停止例外。該適當動作之另外非限定範圍能夠包含切換至僅針對為自我修訂之該碼之部分的各機器指令之一直譯（相對於編譯）。在一實施中，該方法將較慢於編譯，但非常精確且將運作完全如該自我修訂碼所被意圖來進行者。其他適當動作也為可能。該處理結束於結束點 348。

第 8 圖係為描述涉及使用交換式記憶體硬體來促進多執行緒環境中之配發表單更新的各階段之一實施。該處理起始於開始點 370，使用交換式記憶體硬體提供一原子提交特徵（階段 372）。該系統提供一仿真器，其使用一儲存在主要記憶體中之配發表單來轉換一訪客程式計數器成一主機程式計數器（階段 374）。該系統存取該配發表單來檢視其是否包含針對該所給定訪客程式計數器之一主機程式計數器（階段 376）。如果沒有發現主機程式計數器，該系統編譯訪客碼之該相關區塊（階段 378）。至該配發表單之更新係經執行在私有記憶體中，並且當該更新全然執行時，其原子化地提交至主要記憶體。執行該原子提交特徵，該系統按具有最小化間接費用（overhead）之一原子方式更新該配發表單。該處理結束於結束點 382。

第 9 圖係為描述涉及使用交換式記憶體硬體來促進多執行緒環境中之程式碼回插的各階段之一實施。該處理開始於開始點 400，使用交換式記憶體硬體提供非可視式私有狀態及原子提交功能（階段 402）。該系統儲存對程式碼作出的改變於非可視式的私有狀態中（階段 404）。對該程式碼所作出的改變能夠自一或多個執行緒接收。該回插改

變使用原子提交經由企圖一次提交所有改變至記憶體而經頒佈（階段 406）。如果另外執行緒正嘗試執行需要被改變之程式碼，提交將失效且該回插處理經由企圖再次原子地提交所有改變至記憶體而重新執行（階段 408）。經由使用這樣具有交換式記憶體功能的回插處理，安全動態程式碼修訂將在一多執行緒環境中啟動（階段 410）。該處理結束於結束點 412。

第 10 圖係為描述涉及使用交換式記憶體硬體來促進一有效率之呼叫返回快取之各階段之一實施。該處理開始於開始點 430，使用交換式記憶體硬體提供非可視式及可放棄式私有狀態（階段 432）。該系統提供儲存在該私有狀態設備中之一呼叫返回快取，其捕獲該主機位址來返回至該訪客函數之執行完成之後（階段 434）。一直接查找硬體式雜湊表單可經使用於該呼叫返回快取（階段 436）。在一實施中，該呼叫返回快取支援相較於在一配發表單中之一般查找的較有效率查找。該處理結束於結束點 438。

雖然此標的已經以語言來具體說明其結構性特徵與/或方法論的動作，需要瞭解的是，之後的申請專利範圍所定義的標的係非必要地限制於如上所述的具體特徵或動作。如上所述的具體特徵與動作係被揭露以作為實現申請專利範圍的範例。所有敘述於此與/或於之後的申請專利範圍的實施例之精神內的等效物、更動或調整，係均需要被保護。

例如，在電腦軟體技術領域中具有通常知識者，係可

以辨認出討論於此的各個範例可以不同方式，在一或更多電腦上重新組織，包括相較於在範例中所述的較少或更多選項或特徵。

【圖式簡單說明】

第 1 圖係根據本發明具體實施例之一電腦系統之圖式；

第 2 圖係為在第 1 圖之電腦系統上所操作一實施的虛擬化/仿真化應用的圖式；

第 3 圖係為第 1 圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進精確例外語義之仿真化的各階段；

第 4 圖係為第 1 圖之系統之一實施的圖式，其描述執行一塊-精確仿真化；

第 5 圖係為第 1 圖之系統之一實施的圖式，其描述在一塊-精確已經提起一例外之後執行一塊-精確仿真化；

第 6 圖係為第 1 圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進狀態隔離之各階段；

第 7 圖係為第 1 圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進偵測仿真化下之自我修訂碼的各階段；

第 8 圖係為第 1 圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進多執行緒環境中之

配發表單更新的各階段；

第9圖係為第1圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進多執行緒環境中之程式碼回插的各階段；

第10圖係為第1圖之系統之一實施的處理流程圖，其描述涉及使用交換式記憶體硬體來促進一有效率之呼叫返回快取之各階段。

【主要元件符號說明】

120 私有狀態

124 軟體可視記憶體存取

126 原子提交

108 可抽取式儲存

110 非可抽取式儲存

111 輸出裝置

112 輸入裝置

114 其他通訊連結

115 其他電腦/應用程式

200 虛擬化/仿真化應用

204 程式邏輯

206 使用交換式記憶體硬體來加速虛擬化或仿真化之邏輯

208 使用交換式記憶體硬體來促進精確例外語義的邏輯

210 使用交換式記憶體硬體來促進狀態隔離之邏輯

212 使用交換式記憶體硬體來促進偵測自我修正碼之邏輯

214 使用交換式記憶體硬體來促進配發表單更新之邏輯

216 使用交換式記憶體硬體來促進碼回插之邏輯

218 使用交換式記憶體硬體來促進一有效率之呼叫返回堆疊的邏輯

220 其他操作應用程式之邏輯

242 使用非可視式及可棄式之私有狀態於該交易式記憶體硬體中，來致使該仿真化狀態能夠來維持與該架構狀態之不一致性且僅在該粗劣的範圍上進行同步化

244 使用一塊-精確仿真化來執行各指令之最佳化序列

246 例外發生？

248 至記憶體之待決寫入經放棄

250 仿真化處理器狀態係捲返回至該上一次同步點

252 特定碼序列係經再次穩當地執行，以致使當該例外第二次遇到時呈現正確架構狀態

312 提供隔離的私有狀態於交換式記憶體硬體上

314 在一仿真化環境中，執行該仿真化之主機儲存他的堆疊於該隔離的私有狀態中

316 該經仿真化之訪客不具有對該隔離的私有狀態之存取

342 使用交換式記憶體硬體提供軟體-可視式記憶體存取

344 監控該記憶體存取，藉以偵測經仿真化之訪客已經修改其自我碼序列

346 基於該偵測採取適當動作

372 使用交換式記憶體硬體提供一原子提交

374 提供一仿真器，其使用一配發表單來轉換一訪客程式

計數器成一主機程式計數器

376 存取該配發表單來檢視其是否包含針對該所給定訪客程式計數器之一主機程式計數器

378 如果沒有發現主機程式計數器，編譯訪客碼之該相關區塊

380 執行該原子提交特徵，按具有最小化間接費用之一原子方式更新該配發表單

402 使用交換式記憶體硬體提供非可視式私有狀態及原子提交

404 儲存對程式碼作出的改變於非可視式的私有狀態中

406 使用原子提交經由一次提交所有改變至記憶體而經頒佈回插改變

408 如果另外執行緒正嘗試執行需要被改變之程式碼，提交將失效且該回插處理重新執行

410 經由使用這樣具有交換式記憶體功能的回插處理，安全動態程式碼修訂將在一多執行緒環境中啟動

432 使用交換式記憶體硬體提供非可視式及可放棄式私有狀態

434 提供一呼叫返回快取，其捕獲該主機位址來返回至該訪客函數之執行完成之後

436 一直接查找硬體式雜湊表單可經使用於該呼叫返回快取

十、申請專利範圍：

1. 一種使用交換式記憶體硬體來促進狀態隔離之方法，該方法至少包含以下步驟：

存取步驟，存取在交換式記憶體硬體上之隔離的私有狀態；及

儲存步驟，儲存正執行一訪客之一仿真化(emulation)於該隔離的私有狀態中之一主機的一堆疊，其中該隔離的私有狀態確保經仿真化於該主機上之該訪客不可存取該主機之該堆疊。

2. 如申請專利範圍第 1 項所述之方法，其中該隔離的私有狀態係僅可視於一中央處理單元。

3. 如申請專利範圍第 2 項所述之方法，其中該隔離的私有狀態不能夠由其他中央處理單元或硬體裝置所存取。

4. 如申請專利範圍第 1 項所述之方法，其中該隔離的私有狀態致使該主機能夠維持該堆疊於一緩衝模式(buffered mode)中。

5. 如申請專利範圍第 4 項所述之方法，其中該緩衝模式允許該主機能夠避免昂貴的執行時間（runtime）檢查。

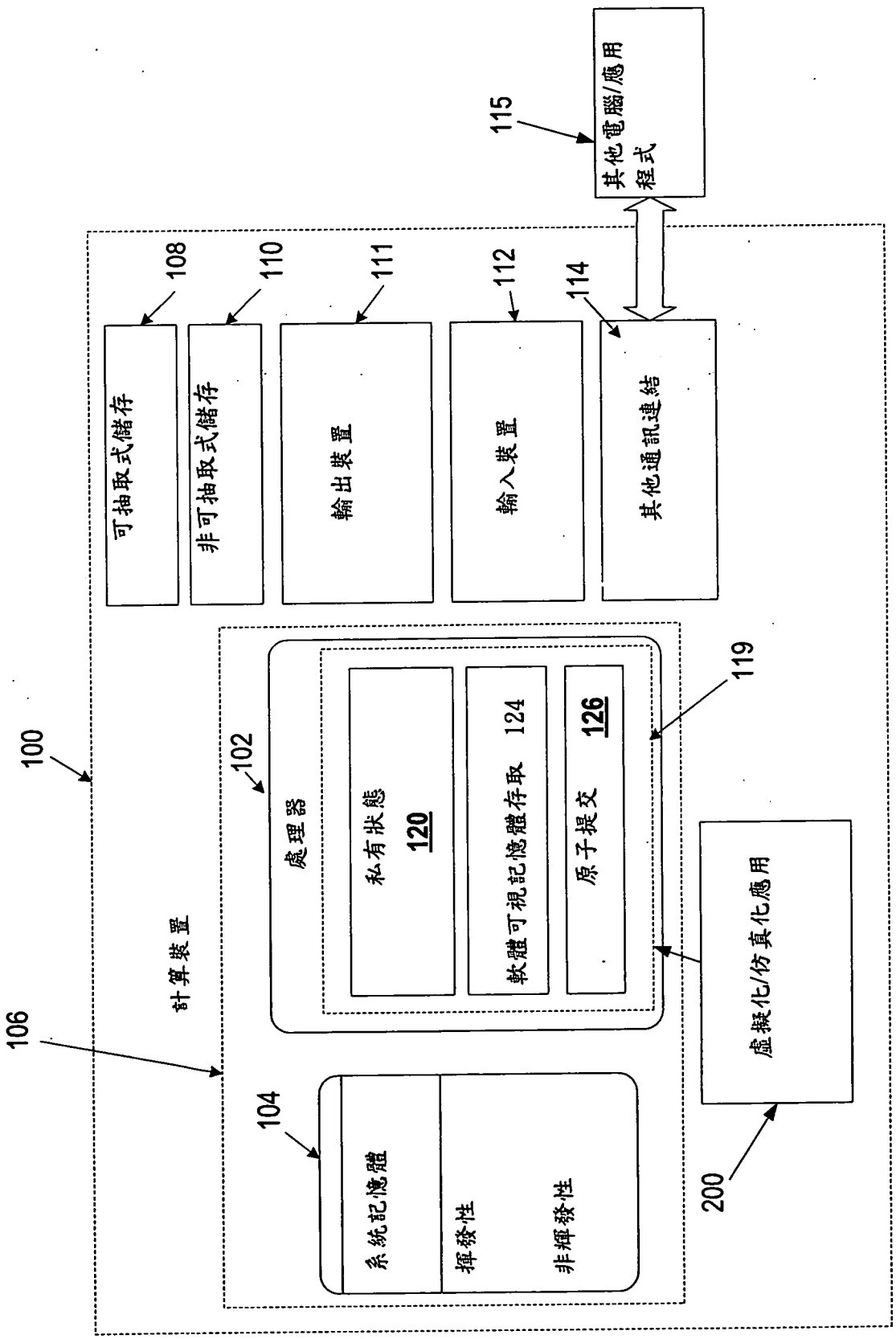
6. 如申請專利範圍第 1 項所述之方法，其中該隔離的私有狀態係為可棄式(discardable)。

7. 如申請專利範圍第 6 項所述之方法，其中當一中央處理單元放棄該私有狀態時，由該中央處理單元之記憶體之一檢視係經回復至一目前架構狀態。

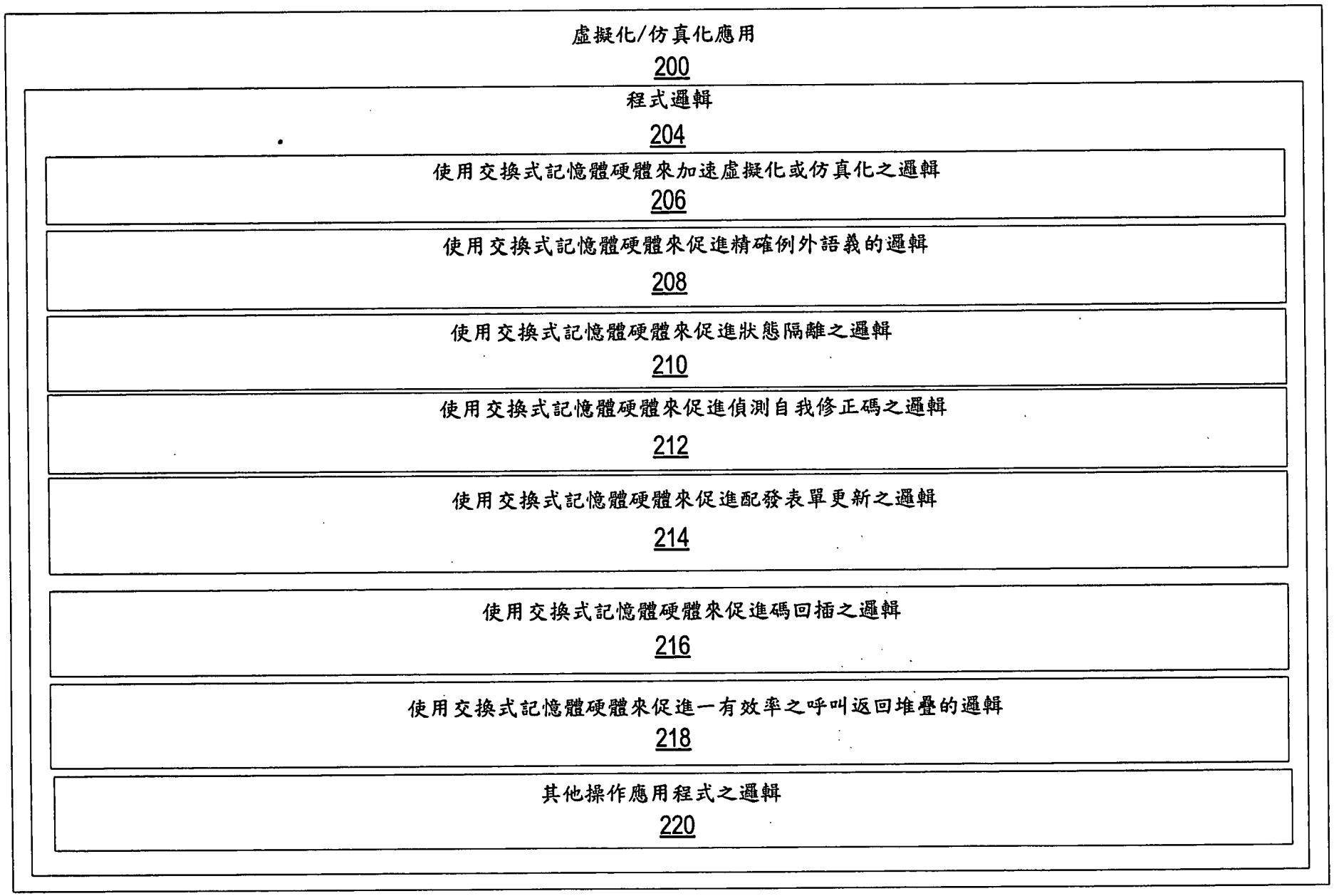
8. 一種儲存電腦可執行指令之電腦儲存媒體，其中該等電腦可執行指令係用於致使一電腦執行一方法，該方法包含以下步驟：

存取步驟，存取在交換式記憶體硬體上之隔離的私有狀態；及

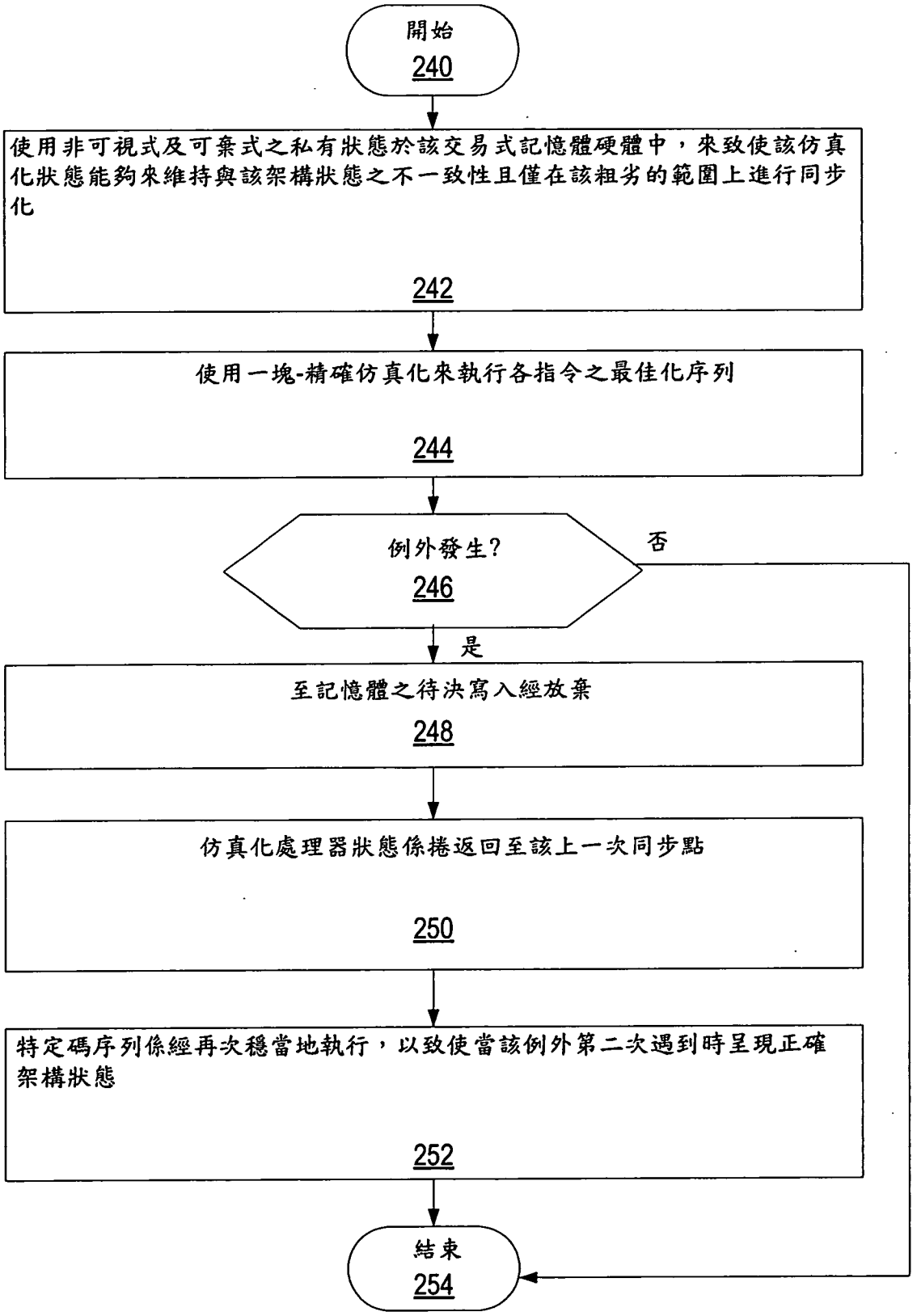
儲存步驟，儲存正執行一訪客之一仿真化於該隔離的私有狀態中的一主機之一堆疊，其中該隔離的私有狀態係確保：經仿真化於該主機上之該訪客不可存取該主機之該堆疊。


100
計算裝置
106
102
處理器
私有狀態
120
軟體可視記憶體存取 124
原子提交 126
119
104
系統記憶體
揮發性
非揮發性
108
可抽取式儲存
110
非可抽取式儲存
111
輸出裝置
112
輸入裝置
114
其他通訊連結
115
其他電腦/應用程式
200
虛擬化/仿真化應用

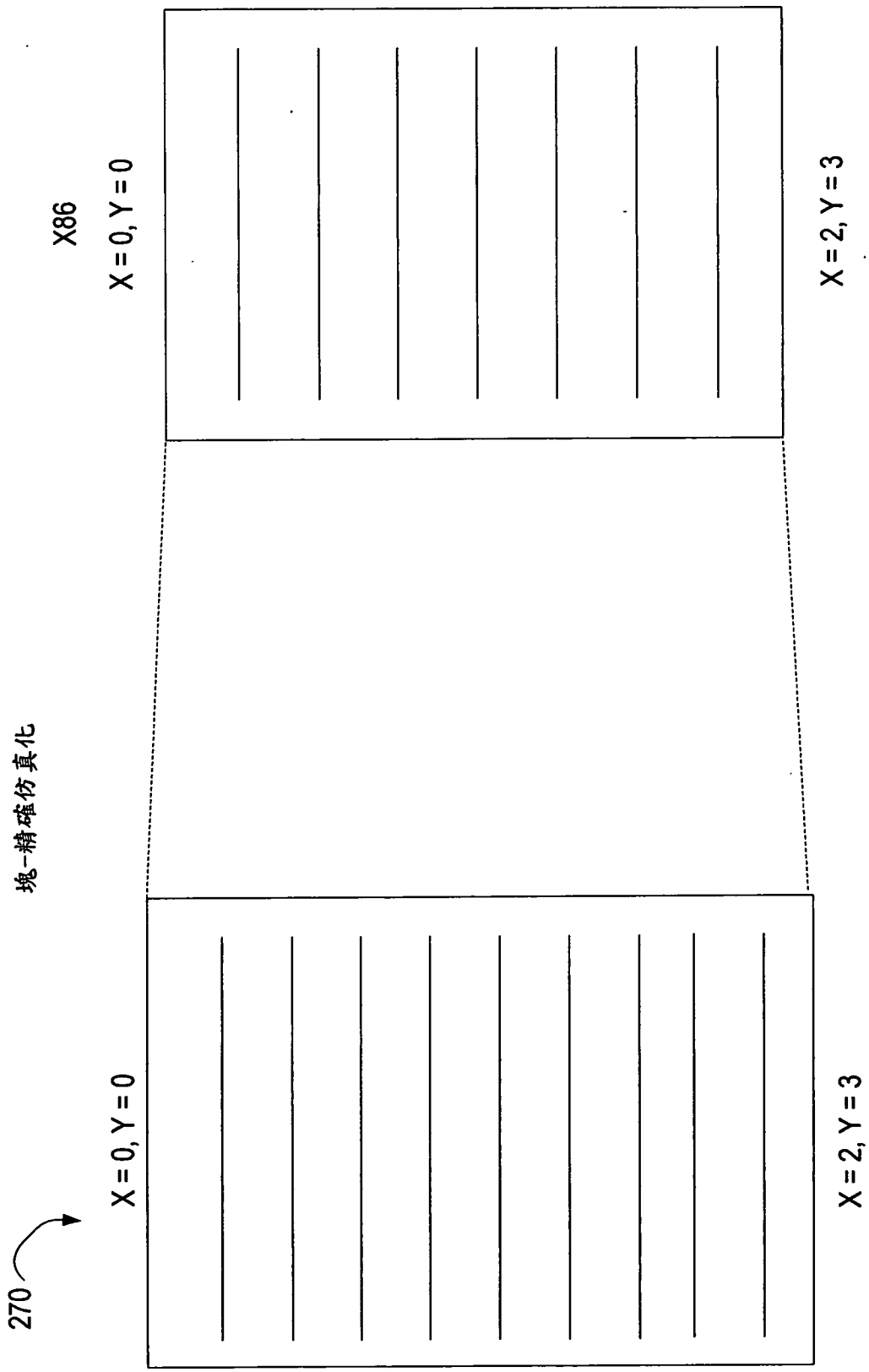
第1圖


虛擬化/仿真化應用
200
程式邏輯
204
使用交換式記憶體硬體來加速虛擬化或仿真化之邏輯
206
使用交換式記憶體硬體來促進精確例外語義的邏輯
208
使用交換式記憶體硬體來促進狀態隔離之邏輯
210
使用交換式記憶體硬體來促進偵測自我修正碼之邏輯
212
使用交換式記憶體硬體來促進配發表單更新之邏輯
214
使用交換式記憶體硬體來促進碼回插之邏輯
216
使用交換式記憶體硬體來促進一有效率之呼叫返回堆疊的邏輯
218
其他操作應用程式之邏輯
220

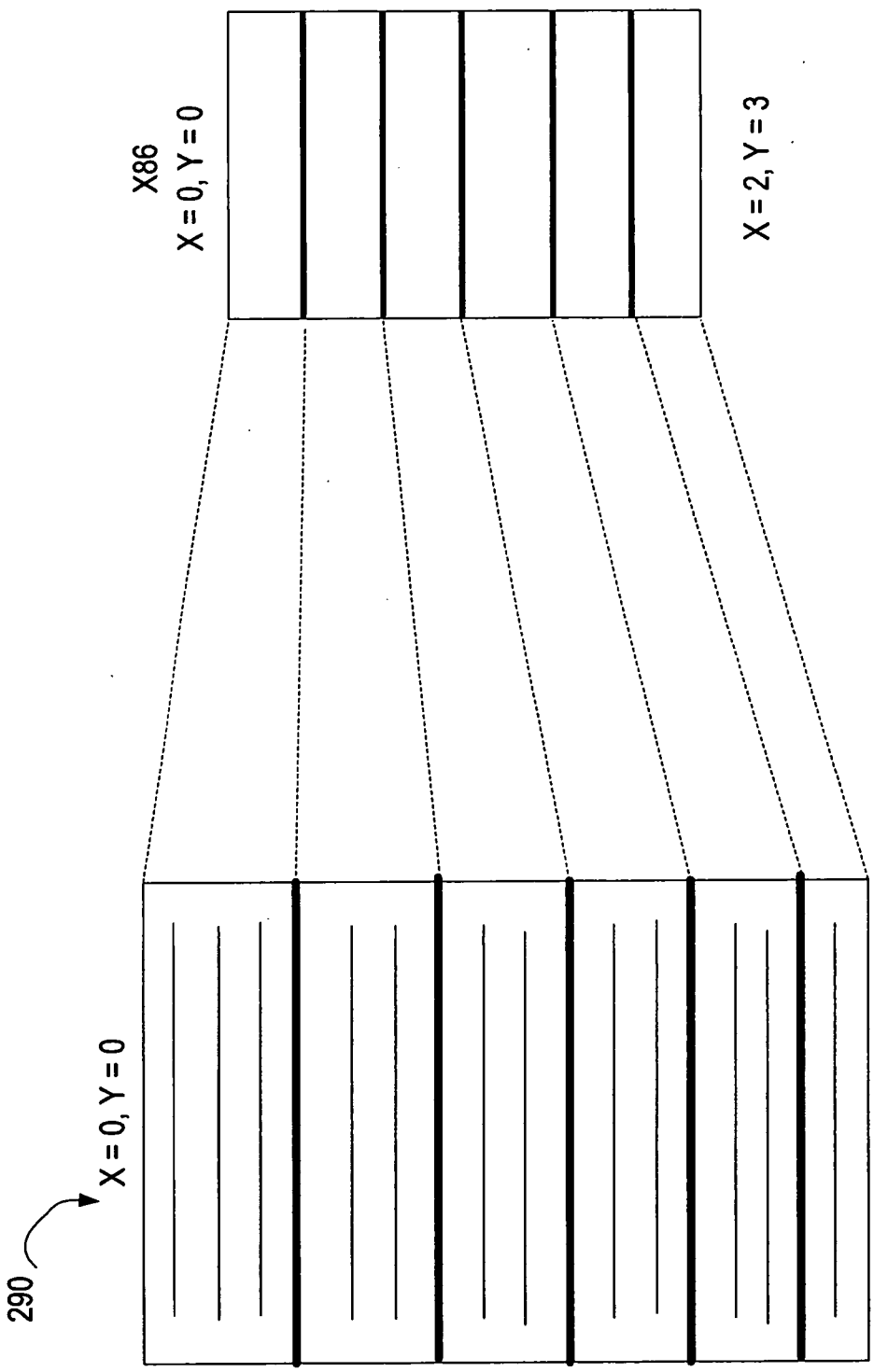
第2圖


開始
240
使用非可視式及可棄式之私有狀態於該交易式記憶體硬體中，來致使該仿真化狀態能夠來維持與該架構狀態之不一致性且僅在該粗劣的範圍上進行同步化
242
使用一塊-精確仿真化來執行各指令之最佳化序列
244
例外發生?
246
否
是
至記憶體之待決寫入經放棄
248
仿真化處理器狀態係捲返回至該上一次同步點
250
特定碼序列係經再次穩當地執行，以致使當該例外第二次遇到時呈現正確架構狀態
252
結束
254

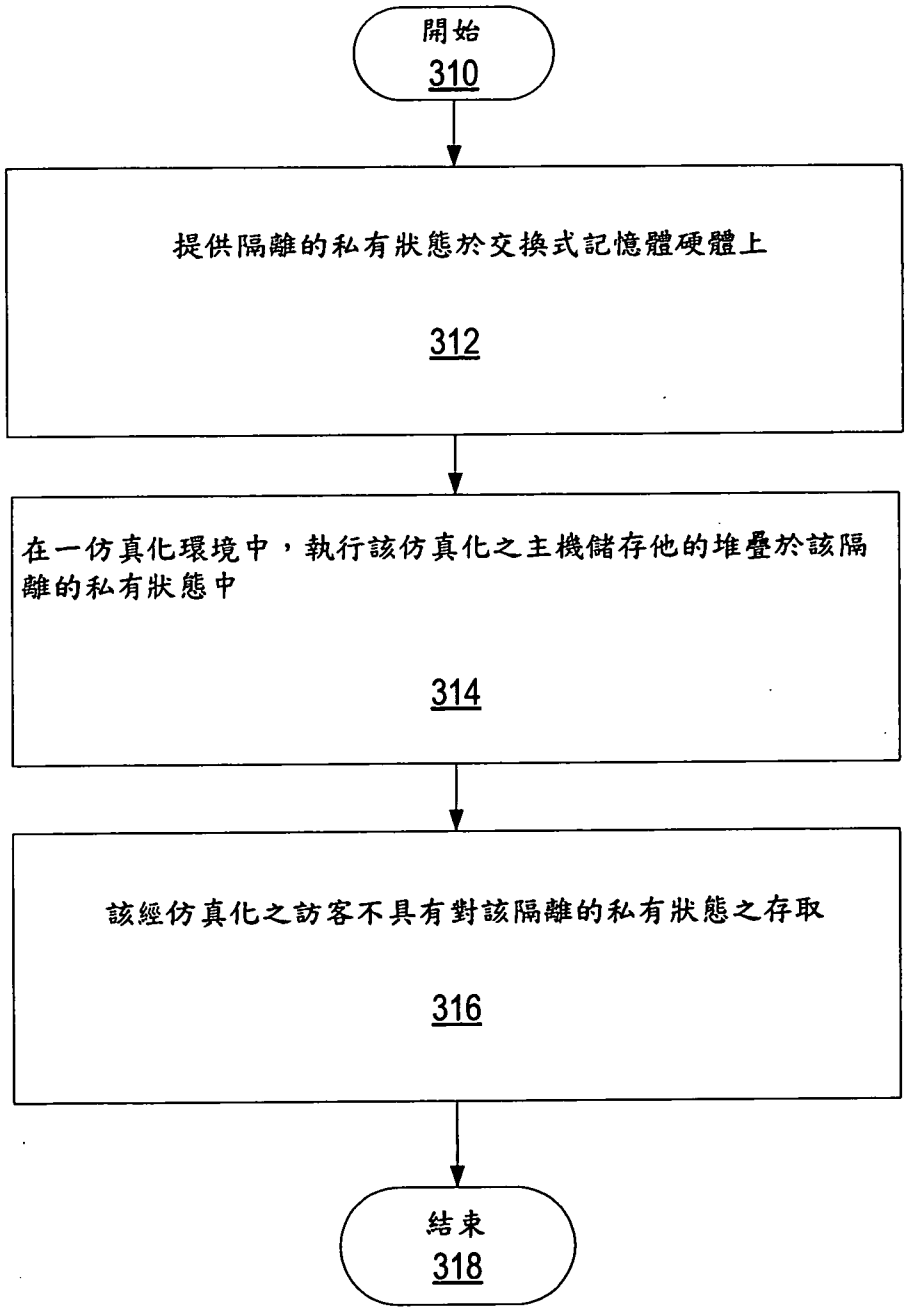
第3圖



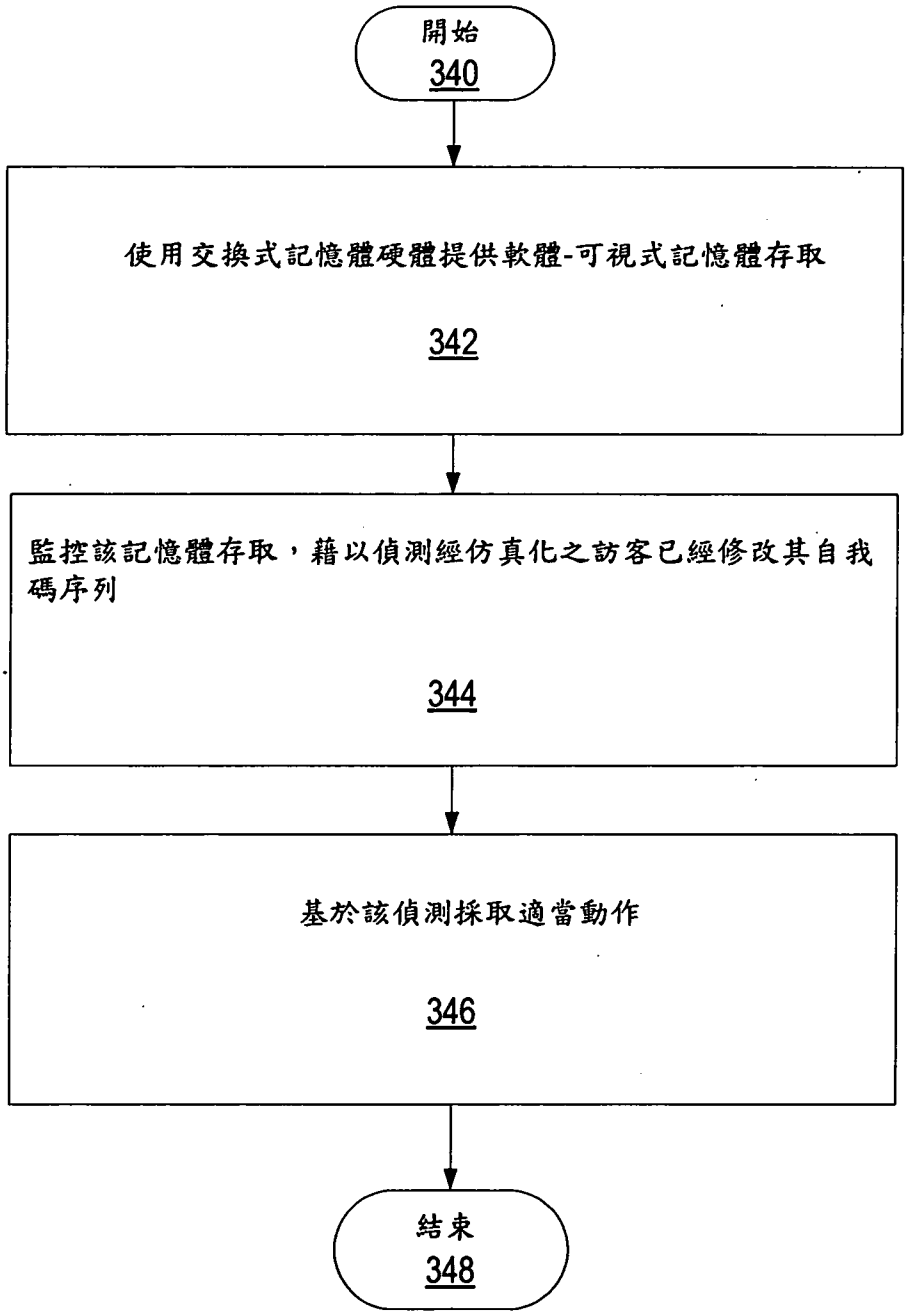
第4圖



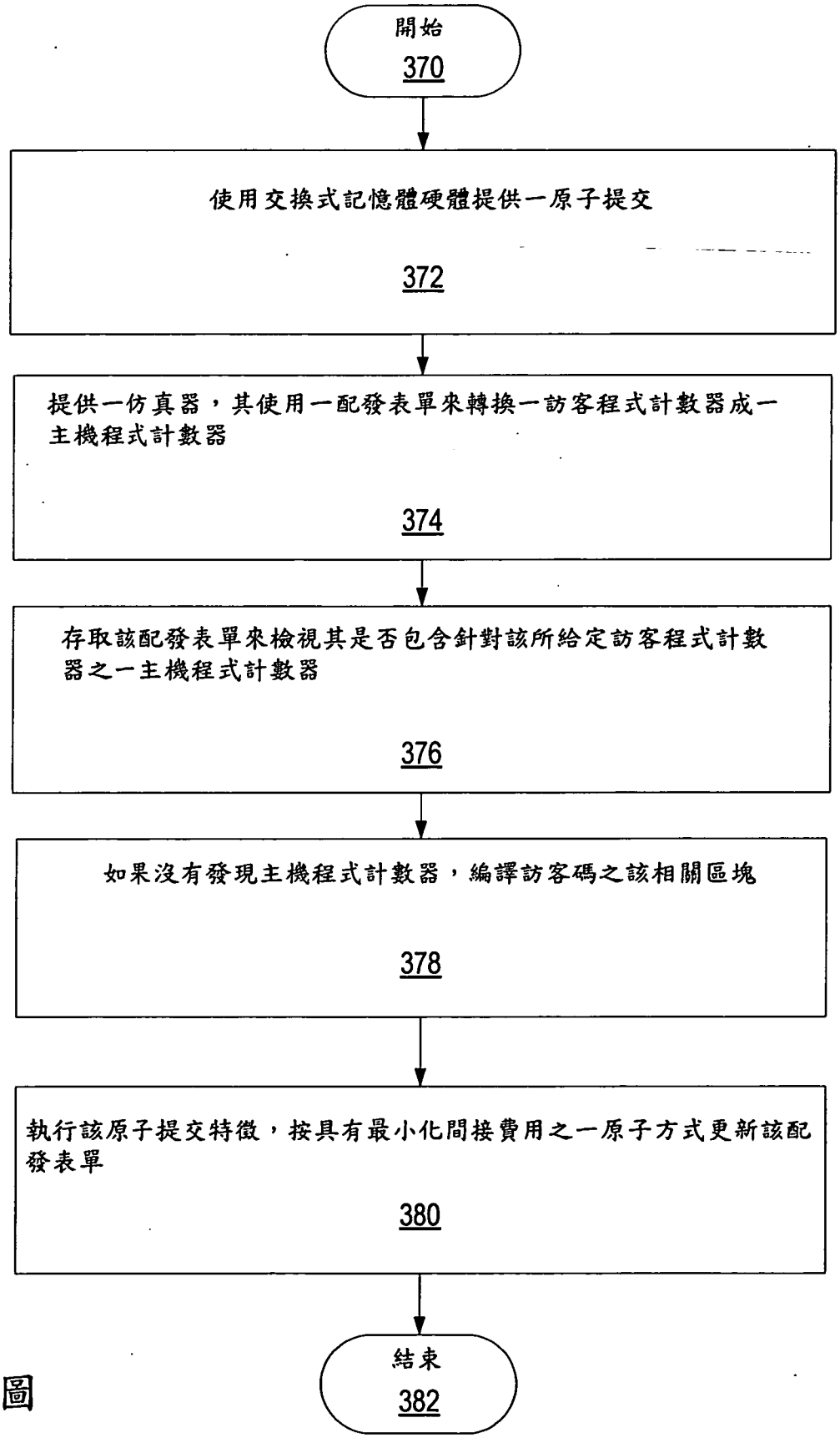
第5圖


開始
310
提供隔離的私有狀態於交換式記憶體硬體上
312
在一仿真化環境中，執行該仿真化之主機儲存他的堆疊於該隔離的私有狀態中
314
該經仿真化之訪客不具有對該隔離的私有狀態之存取
316
結束
318

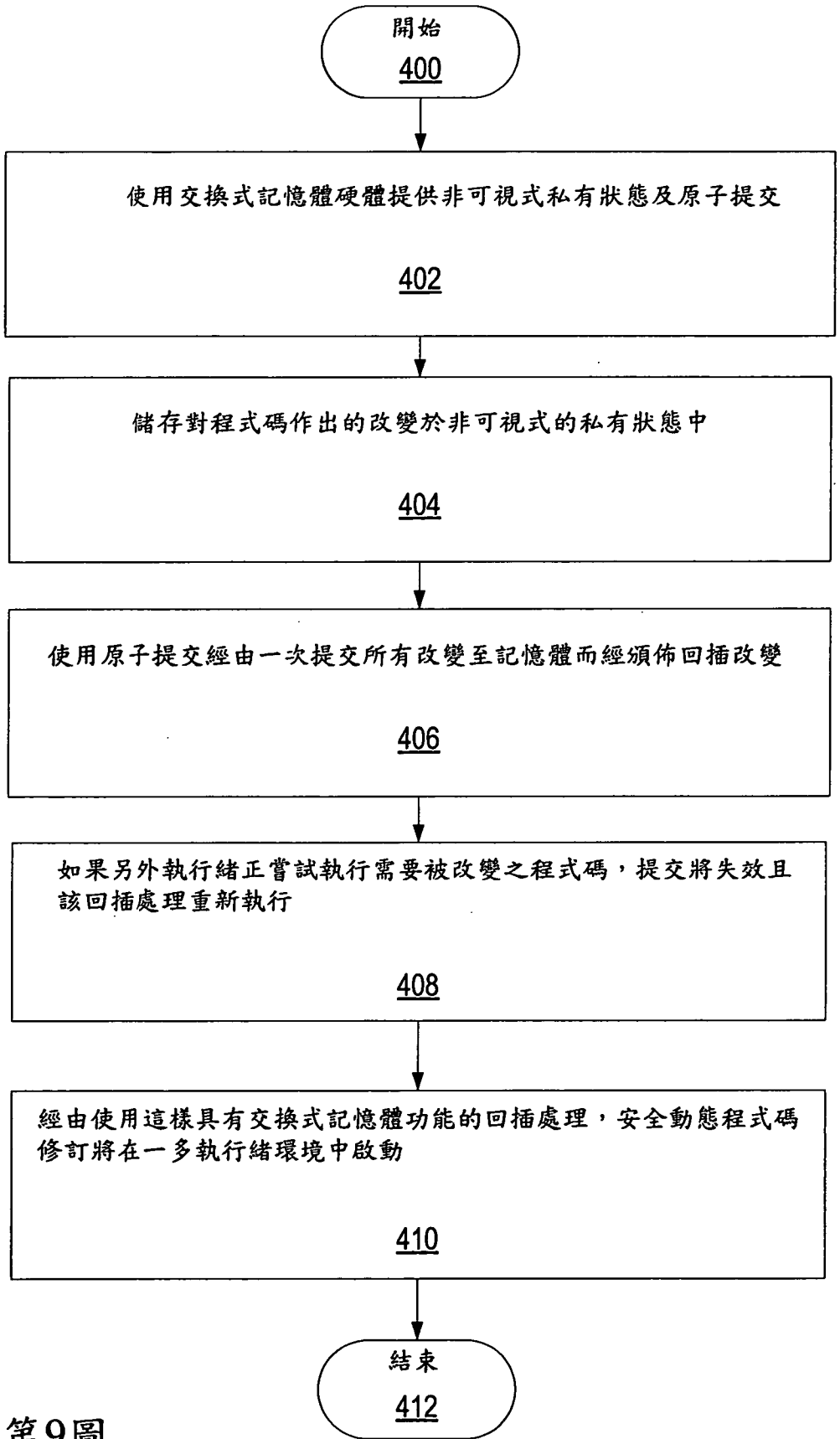
第6圖


開始
340
使用交換式記憶體硬體提供軟體-可視式記憶體存取
342
監控該記憶體存取，藉以偵測經仿真化之訪客已經修改其自我碼序列
344
基於該偵測採取適當動作
346
結束
348

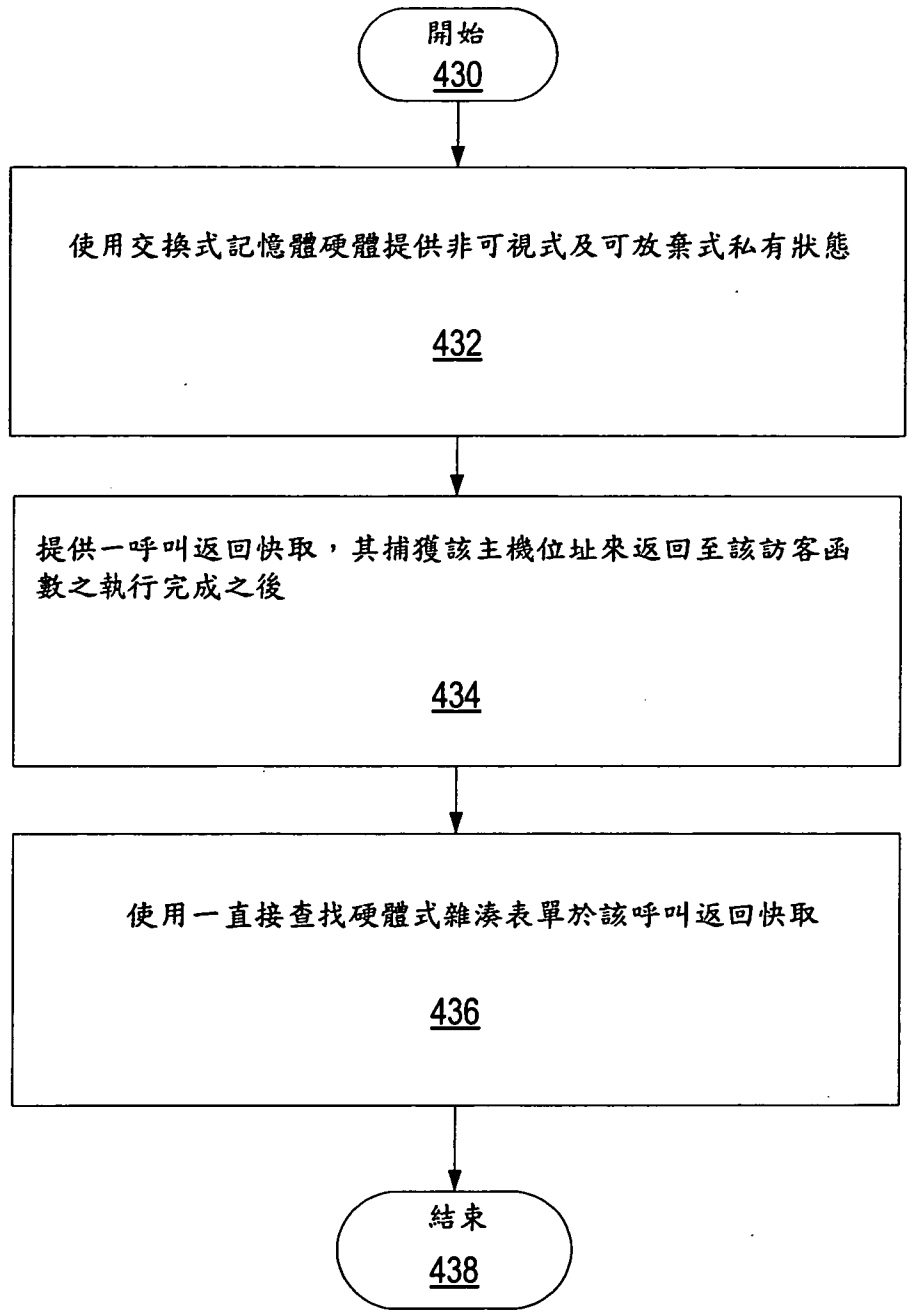
第7圖


開始
370
使用交換式記憶體硬體提供一原子提交
372
提供一仿真器，其使用一配發表單來轉換一訪客程式計數器成一主機程式計數器
374
存取該配發表單來檢視其是否包含針對該所給定訪客程式計數器之一主機程式計數器
376
如果沒有發現主機程式計數器，編譯訪客碼之該相關區塊
378
執行該原子提交特徵，按具有最小化間接費用之一原子方式更新該配發表單
380
結束
382

第8圖


開始
400
使用交換式記憶體硬體提供非可視式私有狀態及原子提交
402
儲存對程式碼作出的改變於非可視式的私有狀態中
404
使用原子提交經由一次提交所有改變至記憶體而經須佈回插改變
406
如果另外執行緒正嘗試執行需要被改變之程式碼，提交將失效且該回插處理重新執行
408
經由使用這樣具有交換式記憶體功能的回插處理，安全動態程式碼修訂將在一多執行緒環境中啟動
410
結束
412

第9圖


開始
430
使用交換式記憶體硬體提供非可視式及可放棄式私有狀態
432
提供一呼叫返回快取，其捕獲該主機位址來返回至該訪客函數之執行完成之後
434
使用一直接查找硬體式雜湊表單於該呼叫返回快取
436
結束
438

第10圖