



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I567642 B

(45)公告日：中華民國 106 (2017) 年 01 月 21 日

(21)申請案號：104115910

(22)申請日：中華民國 104 (2015) 年 05 月 19 日

(51)Int. Cl. : G06F9/30 (2006.01)

G06F12/08 (2016.01)

(30)優先權：2014/06/27 美國

14/318,508

(71)申請人：英特爾公司(美國) INTEL CORPORATION (US)

美國

(72)發明人：羅哲斯 卡洛斯 V ROZAS, CARLOS V. (US)；亞歷山德羅維奇 伊莉亞

ALEXANDROVICH, ILYA (IL)；奈格 吉伯特 NEIGER, GILBERT (US)；麥金

法蘭西斯 X MCKEEN, FRANCIS X. (US)；阿那堤 伊達依 ANATI, ITTAI (IL)；

珊布赫古 維亞斯 SHANBHOGUE, VEDVYAS (US)；古爾翁 夏依 GUERON,

SHAY (IL)

(74)代理人：憚軼群；陳文郎

(56)參考文獻：

TW 200949681A

CN 102473224A

US 2002/0184046A1

審查人員：潘世光

申請專利範圍項數：52 項 圖式數：18 共 133 頁

(54)名稱

用以中斷與回復安全獨立領域中的分頁之指令及邏輯

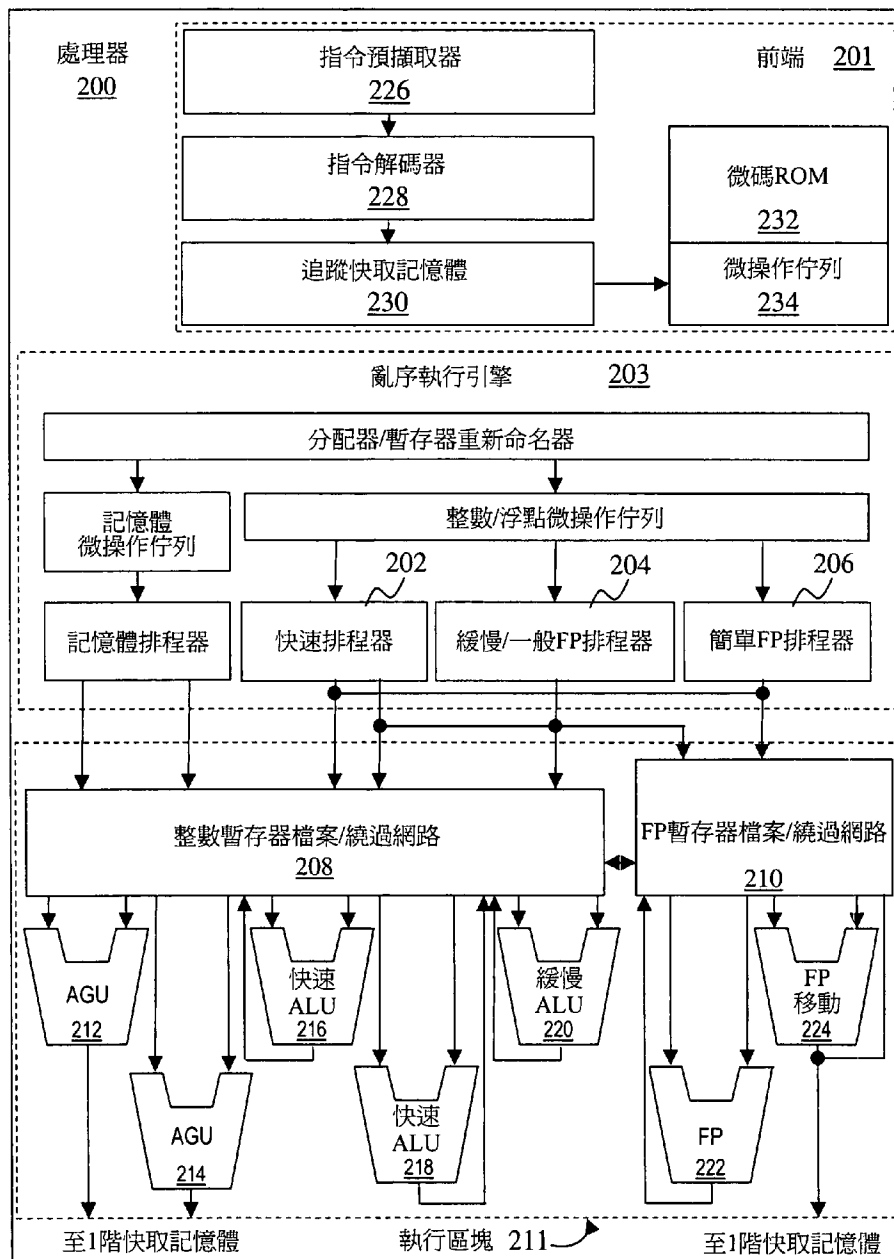
INSTRUCTIONS AND LOGIC TO INTERRUPT AND RESUME PAGING IN SECURE ENCLAVES

(57)摘要

指令及邏輯中斷及回復安全獨立領域中的分頁。實施例包括指令，該等指令指定分配給安全獨立領域的頁位址，該等指令經解碼以用於由處理器執行。該處理器包括獨立領域頁快取記憶體以將安全資料儲存於第一快取列中，且儲存於用於對應於該頁位址的頁之最後快取列中。當用於頁之獨立領域頁快取記憶體映射中的項指示僅部分頁儲存於該獨立領域頁快取記憶體中時，自用於頁之第一快取列或最後快取列讀取頁狀態。用於部分頁之該項可經設定，且當指令之執行中斷時，在寫回時可將新頁狀態記錄於該第一快取列中，或在載入該頁時可將新頁狀態記錄於該最後快取列中。因此，可回復該寫回或載入。

Instructions and logic interrupt and resume paging in secure enclaves. Embodiments include instructions, specify page addresses allocated to a secure enclave, the instructions are decoded for execution by a processor. The processor includes an enclave page cache to store secure data in a first cache line and in a last cache line for a page corresponding to the page address. A page state is read from the first or last cache line for the page when an entry in an enclave page cache mapping for the page indicates only a partial page is stored in the enclave page cache. The entry for a partial page may be set, and a new page state may be recorded in the first cache line when writing-back, or in the last cache line when loading the page when the instruction's execution is being interrupted. Thus the writing-back, or loading can be resumed.

指定代表圖：



符號簡單說明：

- 200 . . . 處理器
- 201 . . . 循序前端
- 202 . . . 快速排程器/微操作排程器/排程器
- 203 . . . 亂序執行引擎
- 204 . . . 緩慢/一般浮點排程器/微操作排程器/排程器
- 206 . . . 簡單浮點排程器/微操作排程器/排程器
- 208 . . . 暫存器檔案/整數暫存器檔案
- 210 . . . 暫存器檔案/浮點暫存器檔案
- 211 . . . 執行區塊
- 212 . . . 執行單元/位址產生單元(AGU)
- 214 . . . 執行單元/AGU
- 216、218 . . . 執行單元/快速 ALU/高速 ALU 執行單元
- 220 . . . 執行單元/緩慢 ALU
- 222 . . . 執行單元/浮點 ALU/浮點單元
- 224 . . . 執行單元/浮點移動單元/浮點單元
- 226 . . . 指令預擷取器
- 228 . . . 解碼器
- 230 . . . 追蹤快取記憶體
- 232 . . . 微碼 ROM

發明摘要

公告本

※ 申請案號：104115910

※ 申請日：104.5.19

※ IPC 分類：G06F 9/30 (2006.01)

12/8 (2016.01)

【發明名稱】(中文/英文)

用以中斷與回復安全獨立領域中的分頁之指令及邏輯
INSTRUCTIONS AND LOGIC TO INTERRUPT AND RESUME
PAGING IN SECURE ENCLAVES

【中文】

指令及邏輯中斷及回復安全獨立領域中的分頁。實施例包括指令，該等指令指定分配給安全獨立領域的頁位址，該等指令經解碼以用於由處理器執行。該處理器包括獨立領域頁快取記憶體以將安全資料儲存於第一快取列中，且儲存於用於對應於該頁位址的頁之最後快取列中。當用於頁之獨立領域頁快取記憶體映射中的項指示僅部分頁儲存於該獨立領域頁快取記憶體中時，自用於頁之第一快取列或最後快取列讀取頁狀態。用於部分頁之該項可經設定，且當指令之執行中斷時，在寫回時可將新頁狀態記錄於該第一快取列中，或在載入該頁時可將新頁狀態記錄於該最後快取列中。因此，可回復該寫回或載入。

【英文】

Instructions and logic interrupt and resume paging in secure enclaves. Embodiments include instructions, specify page addresses allocated to a secure enclave, the instructions are decoded for execution by a processor. The processor includes an enclave page cache to store secure data in a first cache line and in a last cache line for a page corresponding to the page address. A page state is read from the first or last cache line for the page when an entry in an enclave page cache mapping for the page indicates only a partial page is stored in the enclave page cache. The entry for a partial page may be set, and a new page state may be recorded in the first cache line when writing-back, or in the last cache line when loading the page when the instruction's execution is being interrupted. Thus the writing-back, or loading can be resumed.

【代表圖】

【本案指定代表圖】：第（2）圖。

【本代表圖之符號簡單說明】：

200...處理器
 201...循序前端
 202...快速排程器/微操作排程器/排程器
 203...亂序執行引擎
 204...緩慢/一般浮點排程器/微操作排程器/排程器
 206...簡單浮點排程器/微操作排程器/排程器
 208...暫存器檔案/整數暫存器檔案
 210...暫存器檔案/浮點暫存器檔案
 211...執行區塊
 212...執行單元/位址產生單元(AGU)
 214...執行單元/AGU
 216、218...執行單元/快速ALU/高速ALU執行單元
 220...執行單元/緩慢ALU
 222...執行單元/浮點ALU/浮點單元
 224...執行單元/浮點移動單元/浮點單元
 226...指令預擷取器
 228...解碼器
 230...追蹤快取記憶體
 232...微碼ROM
 234...微操作佇列

【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)

用以中斷與回復安全獨立領域中的分頁之指令及邏輯
INSTRUCTIONS AND LOGIC TO INTERRUPT AND
RESUME PAGING IN SECURE ENCLAVES

【技術領域】

發明領域

[0001]本揭示案係關於在由處理器或其他處理邏輯執行時執行載入運算、儲存運算、邏輯運算、數學運算或其他函數運算之處理邏輯、微處理器及相關聯指令集架構的領域。特定而言，本揭示案係關於用以中斷及回復安全獨立領域中的分頁之指令及邏輯。

【先前技術】

發明背景

[0002]用以支援諸如語音、視訊、交易及私用資料的新使用模型及服務之應用程式及高效能網路在安全性領域內呈現新挑戰。對針對機密性及完整性保護在儲存器中或在途中的資料之需要為重要的，但支援高速密碼運算及維持對受保護碼及/或資料之安全存取所需要的儲存器增加複雜性且最終增加費用。

[0003]用於創建及維持安全、受保護或隔離分區或環境之一技術被稱為建立獨立領域。獨立領域為作為整體受保護的一組資訊及處理性能。資訊及處理性能可包括網路、主機或應用程式。當自外部記憶體載入用於獨立領域之資

料及/或指令時，該等資料及/或指令經解密、鑑別且隨後儲存或快取於受保護記憶體中。類似地，當自受保護記憶體移除(evict)用於獨立領域之資料及/或指令時，該等資料及/或指令在儲存回至外部記憶體之前經加密。

[0004]因此，當執行用於安全獨立領域之記憶體頁之頁入(亦即載入)及/或頁出(亦即移除及寫回)時，必須對全部頁執行密碼運算，該等全部分頁之大小可通常為4 KB。因此，載入或移除用於安全獨立領域之頁可需要數十萬處理週期。若頁入或頁出過程中斷，則可需要重新執行頁入或頁出，但因為中斷之出現可相對頻繁，所以載入或移除用於安全獨立領域之頁的正向進展可難以保證。另一方面，若直至用於安全獨立領域之頁之載入或移除已完成才容許中斷服務，則延遲中斷服務可在諸如語音、視訊及即時交易的一些服務中引起不受歡迎的假信號。

[0005]因此，保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展呈現一組獨特的使用者體驗及效能挑戰。至今，尚未充分地研究解決此等挑戰、潛在效能限制問題及即時複雜性的解決方案。

【發明內容】

[0006]依據本發明之一實施例，係特地提出一種處理器，其包含：一獨立領域頁快取記憶體，其用以將安全資料儲存於用於分配給一對應安全獨立領域的一頁位址之一安全儲存器中；一解碼級段，其用以解碼一第一指令以用於由該處理器執行，該第一指令指定該頁位址作為一運算

元；以及一或多個執行單元，其回應於該解碼後第一指令，而用以：當該第一指令執行正中斷時，設定對應於用於該頁位址之一獨立領域頁快取記憶體映射之一項目，以指示該第一指令執行之一部分完成，且當該第一指令執行正中斷時，將一頁狀態部分記錄於用於對應於該頁位址的該頁之該安全儲存器中。

【圖式簡單說明】

[0007]在隨附圖式之各圖中藉由實例而非限制來說明本發明。

[0008]圖**1A**為執行用以中斷及回復安全獨立領域中的分頁之指令的系統之一實施例的方塊圖。

[0009]圖**1B**為執行用以中斷及回復安全獨立領域中的分頁之指令的系統之另一實施例的方塊圖。

[0010]圖**1C**為執行用以中斷及回復安全獨立領域中的分頁之指令的系統之另一實施例的方塊圖。

[0011]圖**2**為執行用以中斷及回復安全獨立領域中的分頁之指令的處理器之一實施例的方塊圖。

[0012]圖**3A**例示根據一實施例之緊縮資料類型。

[0013]圖**3B**例示根據一實施例之緊縮資料類型。

[0014]圖**3C**例示根據一實施例之緊縮資料類型。

[0015]圖**3D**例示根據一實施例之用以中斷及回復安全獨立領域中的分頁之指令編碼。

[0016]圖**3E**例示根據另一實施例之用以中斷及回復安全獨立領域中的分頁之指令編碼。

[0017] 圖**3F**例示根據另一實施例之用以中斷及回復安全獨立領域中的分頁之指令編碼。

[0018] 圖**3G**例示根據另一實施例之用以中斷及回復安全獨立領域中的分頁之指令編碼。

[0019] 圖**3H**例示根據另一實施例之用以中斷及回復安全獨立領域中的分頁之指令編碼。

[0020] 圖**4A**例示用以執行中斷及回復安全獨立領域中的分頁之指令的處理器微架構之一實施例之元件。

[0021] 圖**4B**例示用以執行中斷及回復安全獨立領域中的分頁之指令的處理器微架構之另一實施例之元件。

[0022] 圖**5**為用以執行中斷及回復安全獨立領域中的分頁之指令的處理器之一實施例的方塊圖。

[0023] 圖**6**為用以執行中斷及回復安全獨立領域中的分頁之指令的電腦系統之一實施例的方塊圖。

[0024] 圖**7**為用以執行中斷及回復安全獨立領域中的分頁之指令的電腦系統之另一實施例的方塊圖。

[0025] 圖**8**為用以執行中斷及回復安全獨立領域中的分頁之指令的電腦系統之另一實施例的方塊圖。

[0026] 圖**9**為用以執行中斷及回復安全獨立領域中的分頁之指令的系統單晶片(system-on-a-chip)之一實施例的方塊圖。

[0027] 圖**10**為用以執行中斷及回復安全獨立領域中的分頁之指令的處理器之一實施例的方塊圖。

[0028] 圖**11**為提供用於安全獨立領域頁快取記憶體之

先進分頁性能的IP核心開發系統之一實施例的方塊圖。

[0029]圖**12**例示提供用於安全獨立領域頁快取記憶體之先進分頁性能的架構仿真系統之一實施例。

[0030]圖**13**例示用以轉譯中斷及回復安全獨立領域中的分頁之指令的系統之一實施例。

[0031]圖**14**例示用於使用指令來提供先進分頁性能包括來中斷及回復安全獨立領域中的分頁之處理系統之一實施例。

[0032]圖**15**例示用於使用指令來提供先進分頁性能包括來中斷及回復安全獨立領域中的分頁之處理器中的設備之一實施例。

[0033]圖**16A**例示用以提供先進分頁性能包括用以中斷及回復安全獨立領域中的分頁之過程之一實施例的流程圖。

[0034]圖**16B**例示用以中斷及回復安全獨立領域中的分頁之過程之一實施例的流程圖。

[0035]圖**16C**例示用以中斷及回復安全獨立領域中的分頁之過程之一實施例的流程圖。

[0036]圖**17**例示用以提供用於安全獨立領域頁快取記憶體之先進分頁性能之過程之一替代性實施例的流程圖。

[0037]圖**18A**例示用以提供先進分頁性能包括用以中斷及回復安全獨立領域中的分頁之過程之另一實施例的流程圖。

[0038]圖**18B**例示用以提供先進分頁性能包括用以中

斷及回復安全獨立領域中的分頁之過程之另一實施例的流程圖。

[0039]圖18C例示用以中斷及回復安全獨立領域中的分頁之過程之一實施例的流程圖。

[0040]圖18D例示用以中斷及回復安全獨立領域中的分頁之過程之另一實施例的流程圖。

【實施方式】

較佳實施例之詳細說明

[0041]以下描述揭示用以中斷及回復安全獨立領域中的分頁之指令及處理邏輯，該等指令及處理邏輯在處理器、電腦系統或其他處理設備內或與處理器、電腦系統或其他處理設備相關聯。

[0042]在僅保存例如與獨立領域相關聯的私用或受保護資料的特殊快取記憶體或快取記憶體之部分中，當該私用或受保護資料未加密時，對該私用或受保護資料之存取可僅限於授權處理器核心、硬體執行緒或邏輯處理器。此獨立領域私用記憶體可被稱為獨立領域頁快取記憶體(EPC)記憶體。正如其他實體記憶體的情況，可製作EPC以藉由根據需要頁入及頁出資料及/或碼來支援較大私用或受保護位址空間。

[0043]揭示用以中斷及回復安全獨立領域中的分頁操作之指令及邏輯。在一些實施例中，指令指定分配給安全獨立領域(例如，在安全獨立領域頁快取記憶體中)以用於自外部記憶體載入或用於寫回至外部記憶體的頁位址。此等

指令經解碼以用於由處理器執行。處理器包括獨立領域頁快取記憶體以將安全資料至少儲存於第一快取列中且儲存於用於對應於頁位址的頁之最後快取列中。當用於頁之獨立領域頁快取記憶體映射中的項指示僅部分頁儲存於獨立領域頁快取記憶體中時，自用於頁之第一快取列或最後快取列讀取頁狀態。用於部分頁之項可經設定，且當指令之執行中斷時，在寫回時可將新頁狀態記錄於第一快取列中，或在載入頁時可將新頁狀態記錄於最後快取列中。因此，可回復寫回或載入。

[0044]改變頁之映射通常由普通計算系統中的OS管理，但在獨立領域中，OS未必能夠存取獨立領域私用記憶體之內容。轉譯後備緩衝器(TLB)中之項與一或多個特定處理器核心、硬體執行緒或邏輯處理器相關聯，當頁經頁出至記憶體或非依電性儲存器時，該一或多個特定處理器核心、硬體執行緒或邏輯處理器中無一者被容許修改該頁。因此，改變用於獨立領域之頁之映射，例如移除頁或載入用於獨立領域之新頁，可需要系統藉由將存取獨立領域資源的一或多個處理器核心、硬體執行緒或邏輯處理器置於暫時不活動狀態或禁止狀態中來以某種方式使存取獨立領域資源的一或多個處理器核心、硬體執行緒或邏輯處理器「靜止」，或以其他方式使獨立領域中之任何應用程式停止運行，同時加密且寫回EPC記憶體內容，自記憶體載入且解密新頁，清除且替換TLB項，等等。硬體保護機構可需要用來保護EPC中之頁以保證私用記憶體內容之安全性及/

或完整性，且幫助管理有限量的實體私用記憶體，而無法信賴OS。

[0045]涉及安全獨立領域的一示例性方法描述於2012年6月19日申請之標題為「Method and Apparatus to Provide Secure Application Execution」的同在申請中之美國專利申請案序號13/527,547中。每當EPC記憶體中之頁經移除時，該頁可需要對使用EPC記憶體的所有處理器核心或邏輯處理器傳訊，及/或需要所有處理器核心或邏輯處理器退出獨立領域，以便替換頁內容、清除一或多個TLB項等等。此外，在硬體中保證滿足此需要以便保護獨立領域隱私可涉及大量設計及驗證複雜性。

[0046]一些實施例包括多個硬體執行緒、邏輯處理器或處理核心、用以儲存用於共享頁位址之安全資料的快取記憶體，該等共享頁位址分配給安全獨立領域且可由硬體執行緒、邏輯處理器或處理核心存取。解碼級解碼第一指令(例如，以下更詳細地論述的EBLOCK指令)，該第一指令指定共享頁位址作為運算元。一或多個執行單元標記對應於用於共享頁位址之獨立領域頁快取記憶體映射的項，以阻止用於該等多個硬體執行緒、邏輯處理器或處理核心中任一者之新TLB轉譯之創建，以便存取共享頁。第二指令(例如，以下亦更詳細地論述的ETRACK指令)經解碼以用於執行，該第二指令指定該安全獨立領域作為運算元，且一或多個執行單元記錄當前存取對應於安全獨立領域的獨立領域頁快取記憶體中之安全資料的硬體執行緒。當硬體執行

緒中任一者退出安全獨立領域時，硬體執行緒之所記錄數目遞減。

[0047] OS隨後可將處理器間中斷(IPI)發送至當前存取對應於安全獨立領域的獨立領域頁快取記憶體中之安全資料的任何硬體執行緒、邏輯處理器或處理核心。當硬體執行緒、邏輯處理器或處理核心認可IPI且退出安全獨立領域時，該等硬體執行緒、邏輯處理器或處理核心之一或多個TLB項經清除，且硬體執行緒之所記錄數目遞減。當硬體執行緒之所記錄數目達到零時，OS移除一或多個頁，加密且將該一或多個頁寫回至記憶體或非依電性儲存器為安全的。OS可使用第三指令(例如，以下亦更詳細地論述的EWB指令)來完成移除及寫回。因為安全資料之獨立領域保護可能無法信賴OS，所以若硬體執行緒之所記錄數目尚未達到零，則第三指令之一實施例可失敗。在一替代性實施例中，第三指令可等待，直至硬體執行緒之所記錄數目達到零才執行。

[0048] 將瞭解，管理許可、實體記憶體及/或改變映射仍可由OS管理，但當記憶體內容受保護時，如在獨立領域中，OS可對於存取實際受保護內容不被容許或信賴，因為獨立領域具有私用記憶體。因此，可使用用以中斷及回復安全獨立領域中的分頁之指令及處理邏輯來以分級方式實現在無法信賴OS的情況下保證私用記憶體內容之安全性及/或完整性及管理有限量之實體記憶體之技術約束，而不需要精心硬體支援及/或設計努力。另外，當正加密且寫回安

全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊(例如，儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。隨後可服務中斷，且之後可回復對應分頁操作(例如，使用以下更詳細地論述的 ELOAD RESUME 或 EWRITEBACK RESUME 指令)。因此，可保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0049]在以下描述中，闡述了眾多特定細節，諸如處理邏輯、處理器類型、微架構條件、事件、啓用機構及類似者，以便提供對本發明之實施例之更透徹理解。然而，熟習此項技術者應瞭解，可在無此等特定細節的情況下實踐本發明。另外，未詳細展示一些熟知的結構、電路及類似者，以避免不必要地混淆本發明之實施例。

[0050]雖然參考處理器來描述以下實施例，但其他實施例適用於其他類型之積體電路及邏輯裝置。本發明之實施例之類似技術及教示可應用於其他類型之電路或半導體裝置，該等電路或半導體裝置受益於較高管線通量及改良的效能。本發明之實施例之教示適用於執行資料調處的任何處理器或機器。然而，本發明不限於執行 512 位元、256 位元、128 位元、64 位元、32 位元或 16 位元的資料運算之處理

器或機器，且可應用於執行資料之調處或管理的任何處理器或機器。另外，以下描述提供實例，且隨附圖式展示各種實例來達成例示目的。然而，此等實例不應在限制性意義上來理解，因為其僅僅意欲提供本發明之實施例之實例，而非提供本發明之實施例之所有可能的實行方案之詳盡清單。

[0051]儘管以下實例描述在執行單元及邏輯電路之上下文中的指令處置及分佈，但是本發明之其他實施例可藉由儲存在機器可讀的有形媒體上之資料及/或指令實現，該等資料及/或指令在由機器執行時使機器執行與本發明之至少一實施例一致的功能。在一實施例中，與本發明之實施例相關聯的功能體現於機器可執行指令中。指令可用來使由該等指令規劃的通用或專用處理器執行本發明之步驟。本發明之實施例可提供為電腦程式產品或軟體，其可包括上面儲存有指令之機器或電腦可讀媒體，該等指令可用來規劃電腦(或電子裝置)來執行根據本發明之實施例的一或多個運算。或者，本發明之實施例之步驟可由特定硬體組件來執行，該等特定硬體組件含有用於執行該等步驟的固定功能邏輯；或由已規劃電腦組件與固定功能硬體組件之任何組合來執行。

[0052]用來規劃邏輯來執行本發明之實施例的指令可儲存於系統中的記憶體中，該記憶體諸如DRAM、快取記憶體、快閃記憶體或其他儲存器。此外，可經由網路或藉由其他電腦可讀媒體來分佈該等指令。因此，機器可讀媒

體可包括用於以機器(例如,電腦)可讀的形式儲存或傳輸資訊之任何機構,但不限於:軟碟片、光碟、光碟片唯讀記憶體(CD-ROM),以及磁光碟、唯讀記憶體(ROM)、隨機存取記憶體(RAM)、可抹除可規劃唯讀記憶體(EPROM)、電氣可抹除可規劃唯讀記憶體(EEPROM)、磁性或光學卡、快閃記憶體,或者用來在網際網路上經由電氣、光學、聲響或其他形式的傳播信號(例如,載波、紅外信號、數位信號等)來傳輸資訊之有形的機器可讀儲存器。因此,電腦可讀媒體包括適於以機器(例如,電腦)可讀的形式儲存或傳輸電子指令或資訊之任何類型之有形的機器可讀媒體。

[0053]設計可經歷從創建到模擬到製造的各種級段。表示設計的資料可以許多方式來表示設計。首先,如在模擬中係有用的,可使用硬體描述語言或另一功能描述語言來表示硬體。另外,在設計過程的一些級段可產生具有邏輯及/或電晶體閘的電路層級模型。此外,大多數設計在一些級段達到表示各種裝置在硬體模型中的實體佈局之資料的層級。在使用習知半導體製造技術的狀況下,表示硬體模型的資料可為指定各種特徵在遮罩之不同遮罩層上是否存在的資料,該等遮罩係用來產生積體電路。在設計之任何表示中,資料可儲存於任何形式的機器可讀媒體中。記憶體或者磁性或光學儲存器(諸如碟片)可為儲存經由光波或電波傳輸之資訊的機器可讀媒體,該光波或電波經調變或以其他方式產生來傳輸此資訊。當指示或攜載碼或設計的電載波被傳輸,達到執行電信號之複製、緩衝或重新傳輸

的程度時，製作新的複本。因此，通訊提供者或網路提供者可在有形的機器可讀媒體上至少暫時儲存體現本發明之實施例之技術的物件，諸如編碼至載波中的資訊。

[0054]在現代處理器中，使用許多不同的執行單元來處理且執行多種碼與指令。並非所有指令係產生為均等的，因為一些指令完成速度更快，而其他指令可能需要許多時鐘週期來完成。指令的通量愈快，處理器的整體效能愈好。因此，使盡可能多的指令盡可能快地執行係有利的。然而，有某些指令具有更大複雜性且需要更多的執行時間及處理器資源。例如，浮點指令、載入/儲存操作、資料移動等。

[0055]隨著更多的電腦系統用於網際網路、文字及多媒體應用中，隨時間推移已引入額外的處理器支援。在一實施例中，指令集可與一或多個電腦架構相關聯，該一或多個電腦架構包括資料類型、指令、暫存器架構、定址模式、記憶體架構、中斷與異常處置，以及外部輸入及輸出(I/O)。

[0056]在一實施例中，指令集架構(ISA)可由一或多個微架構來實行，該一或多個微架構包括用來實行一或多個指令集的處理器邏輯及電路。替代性實施例可經由微碼、擴展微碼或微碼輔助、超管理器、二進位轉譯、硬體重新編譯等來實行ISA。因此，具有不同微架構的處理器可共享共同指令集之至少一部分。例如，Intel® Pentium 4處理器、Intel® Core™處理器及來自Advanced Micro Devices公司(Sunnyvale CA)的處理器實行幾乎相同的x86指令集版本(以及一些擴展，較新版本已新增該等擴展)，但具有不同的

內部設計。類似地，由其他處理器開發公司(諸如ARM Holdings公司、MIPS，或其被授權者或採用者)設計的處理器可共享共同指令集之至少一部分，但可包括不同的處理器設計。例如，ISA之相同暫存器架構可在不同微架構中使用新的或熟知的技術以不同方式實行，其中包括：專用實體暫存器、一或多個使用暫存器重新命名機構(例如，使用暫存器別名表(RAT)、重新排序緩衝器(ROB)及引退暫存器檔案)的動態分配實體暫存器。在一實施例中，暫存器可包括一或多個暫存器、暫存器架構、暫存器檔案，或可由或不可由軟體程式設計師定址的其他暫存器集。

[0057]在一實施例中，指令可包括一或多個指令格式。在一實施例中，指令格式可指示各種欄位(位元之數目、位元之位置等)來指定：將要執行之運算，及運算元(將對其執行操作)，以及其他。一些指令格式可進一步斷開，由指令模板(或子格式)定義。例如，給定指令格式之指令模板可定義成具有該指令格式之欄位的不同子集，及/或定義成具有以不同方式解譯的給定欄位。在一實施例中，使用指令格式(且在已定義的情況下，以該指令格式之指令模板中之一給定指令模板)來表達指令，且指令指定或指示了運算及運算元(將對其執行操作)。

[0058]科學、金融、自動向量化通用RMS(辨識、採擷與合成)以及視覺及多媒體應用(例如，2D/3D圖形、影像處理、視訊壓縮/解壓縮、語音辨識演算法及音訊調處)可能需要對大量資料項目執行同一操作)。在一實施例中，單指令

多重資料(SIMD)代表使處理器對多個資料元件執行同一操作的指令類型。SIMD技術可用於可將暫存器中的位元以邏輯方式分成許多固定大小或可變大小的資料元件之處理器，該等資料元件中每一者表示獨立值。例如，在一實施例中，64位元暫存器中之位元可被組織為含有4個獨立的16位元資料元件之來源運算元，該等資料元件中每一者表示獨立的16位元值。此資料類型可被稱為『緊縮』資料類型或『向量』資料類型，且為此資料類型的運算元被稱為緊縮資料運算元或向量運算元。在一實施例中，緊縮資料項目或向量可為儲存在單個暫存器內之緊縮資料元件之序列，且緊縮資料運算元或向量運算元可為SIMD指令(或『緊縮資料指令』或『向量指令』)之來源運算元或目的地運算元。在一實施例中，SIMD指令指定將對兩個來源向量運算元執行，來產生目的地向量運算元(亦稱為結果向量運算元)的單個向量運算，該目的地向量運算元具有相同或不同大小、具有相同或不同數目個資料元件，且按相同或不同的資料元件次序。

[0059] SIMD技術(諸如以下處理器所使用的技術：Intel® Core™處理器，其具有包括x86、MMX™、串流SIMD擴展(SSE)、SSE2、SSE3、SSE4.1及SSE4.2指令的指令集；ARM處理器，諸如ARM Cortex®系列處理器，其具有包括向量浮點(VFP)及/或NEON指令的指令集；以及MIPS處理器，諸如由中國科學院的計算技術研究所(ICT)開發出的Loongson系列處理器)已使應用程式效能的顯著改良成為

可能(Core™及MMX™係Intel公司(Santa Clara, Calif)的註冊商標或商標)。

[0060]在一實施例中，目的地及來源暫存器/資料係表示對應資料或操作之來源或目的地之一般用詞。在一些實施例中，其可由暫存器、記憶體或具有除所述名稱或功能之外的其他名稱或功能之其他儲存區域來實行。例如，在一實施例中，「DEST1」可為暫時儲存暫存器或其他儲存區域，而「SRC1」及「SRC2」可為第一及第二來源儲存暫存器或其他儲存區域，以此類推。在其他實施例中，SRC及DEST儲存區域中之兩者或兩者以上可對應於同一儲存區域(例如，SIMD暫存器)內的不同資料儲存元件。在一實施例中，來源暫存器之一亦可充當目的地暫存器，例如，藉由將對第一及第二來源資料執行的操作之結果寫回至該等兩個來源暫存器中之一者，該一者充當目的地暫存器。

[0061]圖1A為由處理器形成的示範性電腦系統之方塊圖，該處理器包括用以執行根據本發明之一實施例的指令之執行單元。根據本發明，諸如在本文中描述之實施例中，系統100包括諸如處理器102之組件，來使用執行單元，該等執行單元包括用以執行用於處理資料的演算法之邏輯。系統100表示基於PENTIUM® III、PENTIUM® 4、Xeon™、Itanium®、XScale™及/或StrongARM™微處理器(可自Intel公司(Santa Clara, California)獲得)的處理系統，但亦可使用其他系統(包括具有其他微處理器之PC、工程工作站、機上盒(set-top box)及類似者)。在一實施例中，範例系統100可

執行 WINDOWS™ 作業系統(可自 Microsoft 公司(Redmond, Washington)獲得)之一版本，但亦可使用其他作業系統(例如，UNIX 及 Linux)、嵌入式軟體，及/或圖形使用者介面。因此，本發明之實施例不限於硬體電路與軟體之任何特定組合。

[0062] 實施例不限於電腦系統。本發明之替代性實施例可用於其他裝置中，該等其他裝置諸如手持式裝置及嵌入式應用。手持式裝置之一些實例包括蜂巢式電話、網際網路協定裝置、數位相機、個人數位助理(PDA)及手持式 PC。嵌入式應用可包括微控制器、數位信號處理器(DSP)、系統單晶片、網路電腦(NetPC)、機上盒、網路集線器(network hub)、廣域網路(WAN)、交換器(switch)，或可執行根據至少一實施例之一或多個指令的任何其他系統。

[0063] 圖 1A 為由處理器 102 形成的電腦系統 100 之方塊圖，該處理器包括用以執行演算法來執行根據本發明之一實施例的至少一指令之一或多個執行單元 108。可在單處理器桌面或伺服器系統之情況下描述一實施例，但替代性實施例可包括於多處理器系統中。系統 100 係『集線器』系統架構之一實例。電腦系統 100 包括處理資料信號的處理器 102。例如，處理器 102 可為複雜指令集電腦(CISC)微處理器、精簡指令集計算(RISC)微處理器、極長指令字(VLIW)微處理器，實行指令集之組合的處理器，或任何其他處理器裝置，諸如數位信號處理器。處理器 102 耦接至處理器匯流排 110，該處理器匯流排可在處理器 102 與系統 100 中的其

他組件之間傳輸資料信號。系統100之元件執行其習知功能，該等功能係熟習此項技術者所熟知的。

[0064]在一實施例中，處理器102包括1階(L1)內部快取記憶體104。取決於架構，處理器102可具有單個內部快取記憶體或多階內部快取記憶體。或者，在另一實施例中，快取記憶體可駐留在處理器102外部。取決於特定實行方案及需要，其他實施例亦可包括內部與外部快取記憶體兩者之組合。暫存器檔案106可在各種暫存器中儲存不同類型之資料，暫存器包括整數暫存器、浮點暫存器、狀態暫存器及指令指標器暫存器。

[0065]包括執行整數與浮點操作的邏輯之執行單元108亦駐留在處理器102中。處理器102亦包括儲存用於某些巨集指令之微碼的微碼(ucode)ROM。對於一實施例，執行單元108包括處置緊縮指令集109之邏輯。藉由在通用處理器102之指令集中包括緊縮指令集109，連同執行指令的相關聯電路，可使用通用處理器102中的緊縮資料來執行許許多多媒體應用所使用的操作。因此，藉由使用處理器之資料匯流排之全部寬度來對緊縮資料執行操作，可加速且更高效地執行許許多多媒體應用。此可消除對跨越處理器之資料匯流排傳遞較小的資料單元來以一次一個資料元件的方式執行一或多個操作之需要。

[0066]執行單元108之替代性實施例亦可用於微控制器、嵌入式處理器、圖形裝置、DSP及其他類型之邏輯電路中。系統100包括記憶體120。記憶體120可為動態隨機存

取記憶體(DRAM)裝置、靜態隨機存取記憶體(SRAM)裝置、快閃記憶體裝置或其他記憶體裝置。記憶體120可儲存由資料信號表示之指令及/或資料，該等指令及/或資料可由處理器102執行。

[0067]系統邏輯晶片116耦接至處理器匯流排110及記憶體120。系統邏輯晶片116在例示實施例中係記憶體控制器集線器(MCH)。處理器102可經由處理器匯流排110與MCH 116通訊。MCH 116提供高頻寬記憶體路徑118至用於指令與資料儲存且用於圖形命令、資料及紋理的儲存之記憶體120。MCH 116將在處理器102、記憶體120及系統100中的其他組件之間導引資料信號且在處理器匯流排110、記憶體120及系統I/O 122之間橋接資料信號。在一些實施例中，系統邏輯晶片116可提供圖形埠，用於耦接至圖形控制器112。MCH 116經由記憶體介面118耦接至記憶體120。圖形卡112經由加速圖形埠(AGP)互連114耦接至MCH 116。

[0068]系統100使用專屬集線器介面匯流排122來將MCH 116耦接至I/O控制器集線器(ICH) 130。ICH 130經由區域I/O匯流排提供至一些I/O裝置的直接連接。區域I/O匯流排係用於將周邊設備連接至記憶體120、晶片組及處理器102的高速I/O匯流排。一些實例係音訊控制器、韌體集線器(快閃BIOS)128、無線收發器126、資料儲存器124、含有使用者輸入及鍵盤介面的舊式I/O控制器、諸如通用串列匯流排(USB)之串列擴展埠，以及網路控制器134。資料儲存裝置124可包含硬碟機、軟碟機、CD-ROM裝置、快閃記憶

體裝置或其他大容量儲存裝置。

[0069]對於系統之另一實施例，根據一實施例之指令可與系統單晶片一起使用。系統單晶片之一實施例包含處理器及記憶體。用於此一系統的記憶體係快閃記憶體。快閃記憶體可與處理器及其他系統組件位於同一晶粒上。另外，諸如記憶體控制器或圖形控制器之其他邏輯區塊亦可位於系統單晶片上。

[0070]圖1B例示實行本發明之一實施例之原理的資料處理系統140。熟習此項技術者容易瞭解，在不脫離本發明之實施例之範疇的情況下，本文中描述之實施例可與替代性處理系統一起使用。

[0071]電腦系統140包含能夠執行根據一實施例之至少一指令的處理核心159。對於一實施例，處理核心159表示任何類型之架構(包括但不限於CISC、RISC或VLIW型架構)之處理單元。處理核心159亦可適合於以一或多個處理技術來製造，且藉由在機器可讀媒體上足夠詳細地表示，可適合於促進該製造。

[0072]處理核心159包含執行單元142、暫存器檔案145之集合以及解碼器144。處理核心159亦可包括額外電路(圖中未示)，其並非理解本發明之實施例所必需的。執行單元142係用於執行處理核心159接收到之指令。除執行典型處理器指令之外，執行單元142還可執行緊縮指令集143中的指令，以便對緊縮資料格式執行操作。緊縮指令集143包括用於執行本發明之實施例之指令以及其他緊縮指令。執行

單元142由內部匯流排耦接至暫存器檔案145。暫存器檔案145表示處理核心159上用於儲存資訊(包括資料)之儲存區域。如先前所提及，應理解，用於儲存緊縮資料之儲存區域並不關鍵。執行單元142耦接至解碼器144。解碼器144係用於將處理核心159接收到之指令解碼成控制信號及/或微碼進入點。回應於此等控制信號及/或微碼進入點，執行單元142執行適當的操作。在一實施例中，解碼器係用來解譯指令之運算碼，該運算碼將指示應對該指令內所指示之對應資料執行什麼操作。

[0073]處理核心159與匯流排141耦接以便與各種其他系統裝置通訊，其他系統裝置包括但不限於，例如，同步動態隨機存取記憶體(SDRAM)控制146、靜態隨機存取記憶體(SRAM)控制147、高載快閃記憶體介面148、個人電腦記憶卡國際協會(PCMCIA)/緊密快閃(CF)卡控制149、液晶顯示器(LCD)控制150、直接記憶體存取(DMA)控制器151，以及替代性匯流排主控介面152。在一實施例中，資料處理系統140亦可包含I/O橋接器154，以便經由I/O匯流排153與各種I/O裝置通訊。此等I/O裝置可包括但不限於，例如，通用非同步接收器/發射器(UART) 155、通用串列匯流排(USB) 156、藍牙無線UART 157及I/O擴展介面158。

[0074]資料處理系統140之一實施例提供行動通訊、網路通訊及/或無線通訊以及能夠執行包括正文字串比較運算之SIMD運算的處理核心159。處理核心159可由各種音訊、視訊、成像及通訊演算法規劃，該等演算法包括：離

散變換，諸如沃爾什哈達馬德變換(Walsh-Hadamard transform)、快速傅立葉變換(FFT)、離散餘弦變換(DCT)及其個別逆變換；壓縮/解壓縮技術，諸如色彩空間變換、視訊編碼運動估計或視訊解碼運動補償；以及調變/解調變(MODEM)功能，諸如脈衝編碼調變(PCM)。

[0075]圖1C例示資料處理系統之另一替代性實施例，該資料處理系統能夠執行用以中斷及回復安全獨立領域中的分頁之指令。根據一替代性實施例，資料處理系統160可包括主處理器166、SIMD共處理器161、快取記憶體167及輸入/輸出系統168。輸入/輸出系統168可任擇地耦接至無線介面169。SIMD共處理器161能夠執行操作，包括根據一實施例之指令。處理核心170可適合於以一或多個處理技術來製造，且藉由在機器可讀媒體上足夠詳細地表示，可適合於促進包括處理核心170之資料處理系統160的全部或部分之製造。

[0076]對於一實施例，SIMD共處理器161包含執行單元162及暫存器檔案164之集合。主處理器166之一實施例包含解碼器165，用來辨識指令集163之指令(包括根據一實施例之指令)以便由執行單元162執行。對於替代性實施例，SIMD共處理器161亦可包含解碼器165B之至少一部分，用來解碼指令集163之指令。處理核心170亦可包括額外電路(圖中未示)，其並非理解本發明之實施例所必需的。

[0077]在操作中，主處理器166執行資料處理指令之串流，該等資料處理指令控制一般類型之資料處理操作，包

括與快取記憶體167及輸入/輸出系統168之互動。SIMD共處理器指令嵌入於資料處理指令之串流內。主處理器166之解碼器165辨識出此等SIMD共處理器指令係附接之SIMD共處理器161應執行之類型。因此，主處理器166在共處理器匯流排171上發佈此等SIMD共處理器指令(或表示SIMD共處理器指令之控制信號)，附接之SIMD共處理器自該共處理器匯流排接收此等SIMD共處理器指令。在此狀況下，SIMD共處理器161將接受且執行發給該SIMD共處理器的任何所接收SIMD共處理器指令。

[0078]可經由無線介面169接收資料，以便由SIMD共處理器指令處理。對於一實例，可接收呈數位信號形式的語音通訊，其可由SIMD共處理器指令處理來重新產生表示語音通訊的數位音訊樣本。對於另一實例，可接收呈數位位元串流形式的壓縮音訊及/或視訊，其可由SIMD共處理器指令處理來重新產生數位音訊樣本及/或運動視訊圖框。對於處理核心170之一實施例，主處理器166及SIMD共處理器161係整合成單個處理核心170，其包含執行單元162、暫存器檔案164之集合及解碼器165，該解碼器用來辨識指令集163之指令(包括根據一實施例之指令)。

[0079]圖2為處理器200之微架構之方塊圖，該處理器包括執行根據本發明之一實施例之指令的邏輯電路。在一些實施例中，可實行根據一實施例之指令來對資料元件進行操作，該等資料元件具有位元組、字、雙字、四字等大小，以及諸如單精度及雙精度整數及浮點資料類型之資料類

型。在一實施例中，循序前端201係處理器200之部分，其擷取將要執行之指令且使該等指令準備好稍後在處理器管線中使用。前端201可包括若干單元。在一實施例中，指令預擷取器226自記憶體擷取指令且將該等指令饋入至指令解碼器228，該指令解碼器又解碼或解譯該等指令。例如，在一實施例中，解碼器將所接收指令解碼成機器可執行之一或多個操作，稱為「微指令」或「微操作」(亦稱為micro op或uop)。在其他實施例中，解碼器將指令剖析成運算碼及對應的資料與控制欄位，上述各者由微架構用來執行根據一實施例之操作。在一實施例中，追蹤快取記憶體230獲得經解碼的微操作(uop)且將該等解碼的微碼組譯成程式排序序列或在微操作佇列234中追蹤以便執行。當追蹤快取記憶體230遇到複雜指令時，微碼ROM 232提供完成操作所需要的微操作。

[0080]一些指令被轉換成單個微操作(micro-op)，而其他指令需要若干微操作來完成完整的操作。在一實施例中，若需要超過4個微操作來完成指令，則解碼器228存取微碼ROM 232來完成該指令。對於一實施例，在指令解碼器228處可將指令解碼成少量微操作以便處理。在另一實施例中，若需要許多微操作來實現操作，則可將指令儲存於微碼ROM 232內。追蹤快取記憶體230代表進入點可規劃邏輯陣列(PLA)，其用來判定正確的微指令指標以便自微碼ROM 232讀取微碼序列來完成根據本發明之一實施例之一或多個指令。在微碼ROM 232結束針對指令之定序微操作

之後，機器之前端201回復自追蹤快取記憶體230擷取微操作。

[0081]亂序執行引擎203係使指令準備好執行之處。亂序執行邏輯具有許多緩衝器，用來在指令沿著管線進行且得以排程以便執行時平滑化且重新排序指令流以使效能最佳化。分配器邏輯分配每一微操作爲了執行所需要的機器緩衝器及資料。暫存器重新命名邏輯將邏輯暫存器重新命名至暫存器檔案中的項上。分配器亦在指令排程器前爲兩個微操作佇列(一個用於記憶體操作且一個用於非記憶體操作)之一中的每一微操作分配一項目：記憶體排程器、快速排程器202、緩慢/一般浮點排程器204及簡單浮點排程器206。微操作排程器202、204、206判定微操作何時準備執行，此判定係基於：其相依性輸入暫存器運算元來源是否準備就緒及微操作爲了完成其操作所需要的執行資源的可用性。一實施例之快速排程器202可在主時鐘週期的每一半排程，而其他排程器每個主處理器時鐘週期可僅排程一次。該等排程器針對分派埠進行仲裁來排程微操作以便執行。

[0082]暫存器檔案208、210位於排程器202、204、206與執行區塊211中的執行單元212、214、216、218、220、222、224之間。對於整數及浮點操作，分別有獨立的暫存器檔案208、210。一實施例之每一暫存器檔案208、210亦包括繞過(bypass)網路，該繞過網路可繞過尚未寫入至暫存器檔案中之剛剛完成的結果或將該等剛剛完成的結果轉送

至新的相依性微操作。整數暫存器檔案208及浮點暫存器檔案210亦能夠相互傳達資料。對於一實施例，整數暫存器檔案208分成兩個獨立的暫存器檔案，一個暫存器檔案用於資料之低位32個位元且第二暫存器檔案用於資料之高位32個位元。一實施例之浮點暫存器檔案210具有128位元寬的項，因為浮點指令通常具有寬度為64至128個位元的運算元。

[0083] 執行區塊211含有執行單元212、214、216、218、220、222、224，在此等執行單元中實際執行指令。此部分包括暫存器檔案208、210，其儲存微指令需要執行之整數及浮點資料運算元。一實施例之處理器200包含許多執行單元：位址產生單元(AGU) 212、AGU 214、快速ALU 216、快速ALU 218、緩慢ALU 220、浮點ALU 222、浮點移動單元224。對於一實施例，浮點執行區塊222、224執行浮點、MMX、SIMD及SSE或其他操作。一實施例之浮點ALU 222包括64位元乘64位元的浮點除法器，來執行除法、平方根及餘數微操作。對於本發明之實施例，涉及浮點值的指令可由浮點硬體來處置。在一實施例中，ALU操作發生在高速ALU執行單元216、218。一實施例之快速ALU 216、218可執行快速操作，其有效延時為時鐘週期的一半。對於一實施例，大多數複雜的整數操作發生在緩慢ALU 220，因為緩慢ALU 220包括用於長延時型操作之整數執行硬體，諸如乘法器、移位、旗標邏輯及分支處理。記憶體載入/儲存操作由AGU 212、214執行。對於一實施例，在對64位元

的資料運算元執行整數操作的情況下描述整數ALU 216、218、220。在替代性實施例中，可實行ALU 216、218、220來支援各種資料位元，包括16、32、128、256等。類似地，可實行浮點單元222、224來支援具有各種寬度之位元的一系列運算元。對於一實施例，浮點單元222、224可結合SIMD及多媒體指令對128個位元寬的緊縮資料運算元進行操作。

[0084]在一實施例中，微操作排程器202、204、206在父代負載完成執行之前分派相依性操作。因為在處理器200中推測式地排程並執行微操作，所以處理器200亦包括處置記憶體遺漏的邏輯。若資料負載在資料快取記憶體中遺漏，則管線中可能有相依性操作正在進行，該等操作給排程器留下暫時不正確的資料。重新執行機構追蹤並重新執行使用不正確資料的指令。僅需要重新執行相依性操作，且允許獨立操作完成。處理器之一實施例之排程器及重新執行機構亦經設計以擷取中斷及回復安全獨立領域中的分頁之指令。

[0085]「暫存器」一詞可代表用作指令之一部分來識別運算元的板上處理器儲存位置。換言之，暫存器可為自處理器外部(自程式設計師的角度)可使用的暫存器。然而，一實施例之暫存器的含義不應限於特定類型之電路。取而代之，一實施例之暫存器能夠儲存且提供資料並且執行本文中描述之功能。可使用任何數種不同技術藉由電路在處理器內實行本文中描述之暫存器，諸如專用實體暫存器、使用暫存器重新命名之動態分配實體暫存器、專用實體暫存

器與動態分配實體暫存器之組合等。在一實施例中，整數暫存器儲存32位元的整數資料。一實施例之暫存器亦含有用於緊縮資料的8個多媒體SIMD暫存器。對於以下論述，應理解暫存器係經設計來保存緊縮資料的資料暫存器，諸如具備MMX技術的功能之微處理器(來自Intel公司(Santa Clara, California))中的64個位元寬的MMX™暫存器(在一些情況下亦稱為『mm』暫存器)。此等MMX暫存器(整數與浮點形式均可獲得)可對伴隨著SIMD及SSE指令的緊縮資料元件進行操作。類似地，與SSE2、SSE3、SSE4或更先進(一般稱為「SSEx」)技術有關的128個位元寬的XMM暫存器亦可用來保存此等緊縮資料運算元。在一實施例中，在儲存緊縮資料及整數資料時，暫存器不需要在兩個資料類型之間區分。在一實施例中，整數及浮點含於相同暫存器檔案或不同暫存器檔案中。此外，在一實施例中，浮點及整數資料可儲存於不同暫存器或相同暫存器中。

[0086]在以下諸圖的實例中，描述了許多資料運算元。圖3A例示根據本發明之一實施例之多媒體暫存器中的各種緊縮資料類型表示。圖3A例示用於128個位元寬的運算元之緊縮位元組310、緊縮字320及緊縮雙字(dword)330之資料類型。此實例之緊縮位元組格式310係128個位元長且含有16個緊縮位元組資料元件。位元組在此處定義為8個位元的資料。每一位元組資料元件之資訊儲存於位元組0的位元7至位元0中、位元組1的位元15至位元8中、位元組2的位元23至位元16中，且最後儲存於位元組15的位元120至位元127

中。因此，在暫存器中使用所有可利用的位元。此儲存佈置增加了處理器之儲存效率。同樣，在存取了16個資料元件後，現在可平行地對16個資料元件執行一操作。

[0087]通常，資料元件係單獨的資料片段，其與具有相同長度的其他資料元件一起儲存於單個暫存器或記憶體位置中。在與SSEx技術有關的緊縮資料序列中，儲存於XMM暫存器中的資料元件之數目為128個位元除以單獨資料元件之位元長度。類似地，在與MMX及SSE技術有關的緊縮資料序列中，儲存於MMX暫存器中的資料元件之數目為64個位元除以單獨資料元件之位元長度。雖然圖3A中例示的資料類型係128個位元長，但本發明之實施例亦可對64個位元寬、256個位元寬、512個位元寬或其他大小的運算元進行操作。此實例之緊縮字格式320係128個位元長且含有8個緊縮字資料元件。每一緊縮字含有16個位元的資訊。圖3A之緊縮雙字格式330係128個位元長且含有4個緊縮雙字資料元件。每一緊縮雙字資料元件含有32個位元的資訊。緊縮四倍字係128個位元長且含有2個緊縮四倍字資料元件。

[0088]圖3B例示替代性的暫存器中指令儲存格式。每一緊縮資料可包括一個以上的獨立資料元件。例示三個緊縮資料格式：緊縮半字(packed half)341、緊縮單字(packed single)342及緊縮雙字(packed double)343。緊縮半字341、緊縮單字342及緊縮雙字343之一實施例含有定點資料元件。對於一替代性實施例，緊縮半字341、緊縮單字342及緊縮雙字343中一或多者可含有浮點資料元件。緊縮半字

341之一替代性實施例係128個位元長，含有8個16位元的資料元件。緊縮單字342之一實施例係128個位元長，且含有4個32位元的資料元件。緊縮雙字343之一實施例係128個位元長，且含有2個64位元的資料元件。應瞭解，此等緊縮資料格式可進一步擴展至其他暫存器長度，例如，96個位元、160個位元、192個位元、224個位元、256個位元、512個位元或以上。

[0089]圖3C例示根據本發明之一實施例之多媒體暫存器中的各種帶正負號(signed)及不帶正負號(unsigned)的緊縮資料類型表示。不帶正負號的緊縮位元組表示344例示不帶正負號的緊縮位元組在SIMD暫存器中的儲存。每一位元組資料元件的資訊儲存於位元組0零的位元7至位元0中、位元組1的位元15至位元8中、位元組2的位元32至位元16中，等等，且最後儲存於位元組15的位元120至位元127中。因此，在暫存器中使用所有可利用的位元。此儲存佈置可增加處理器之儲存效率。同樣，在存取了16個資料元件後，現在可平行地對16個資料元件執行一操作。帶正負號的位元組表示345例示帶正負號的位元組之儲存。注意，每個位元組資料元件之第8個位元係正負號指示符。不帶正負號的緊縮字表示346例示在SIMD暫存器中如何儲存字7至字0。帶正負號的緊縮字表示347類似於不帶正負號的緊縮字暫存器中表示346。注意，每個字資料元件之第16個位元係正負號指示符。不帶正負號的緊縮雙字表示348展示如何儲存雙字資料元件。帶正負號的緊縮雙字表示349類似於不帶正

負號的緊縮雙字暫存器中表示348。注意，必需的正負號位元係每一雙字資料元件之第32個位元。

[0090]圖3D為對操作編碼(運算碼)格式360之一實施例之描繪，該格式具有32個或更多位元及暫存器/記憶體運算元定址模式，該格式與在以下中所描述之運算碼格式類型相對應：「Intel® 64 and IA-32 Intel Architecture Software Developer's Manual Combined Volumes 2A and 2B: Instruction Set Reference A-Z」，其在全球資訊網(www)於 intel.com/products/processor/manuals/ 獲自 Intel 公司 (Santa Clara, CA)。在一實施例中，且指令可由欄位361及362中之一或多者來編碼。可識別每個指令的至多兩個運算元位置，包括至多兩個來源運算元識別符364及365。對於一實施例，目的地運算元識別符366與來源運算元識別符364相同，而在其他實施例中，該等識別符不同。對於一替代性實施例，目的地運算元識別符366與來源運算元識別符365相同，而在其他實施例中，該等識別符不同。在一實施例中，指令之結果覆寫由來源運算元識別符364及365識別的來源運算元之一，而在其他實施例中，識別符364對應於來源暫存器元件且識別符365對應於目的地暫存器元件。對於一實施例，運算元識別符364及365可用來識別32位元或64位元的來源及目的地運算元。

[0091]圖3E為對另一替代性操作編碼(運算碼)格式370之描繪，該格式具有40個或更多位元。運算碼格式370與運算碼格式360相對應且包含可選擇的前綴位元組378。根據

一實施例之指令可由欄位378、371及372中之一或多者來編碼。藉由來源運算元識別符374及375且藉由前綴位元組378，可識別每個指令的至多兩個運算元位置。對於一實施例，前綴位元組378可用來識別32位元或64位元的來源及目的地運算元。對於一實施例，目的地運算元識別符376與來源運算元識別符374相同，而在其他實施例中，該等識別符不同。對於一替代性實施例，目的地運算元識別符376與來源運算元識別符375相同，而在其他實施例中，該等識別符不同。在一實施例中，指令對由運算元識別符374及375識別的運算元中之一或多者進行操作，且指令之結果覆寫由運算元識別符374及375識別的一或多個運算元，而在其他實施例中，由識別符374及375識別的運算元被寫入至另一暫存器中的另一資料元件。運算碼格式360及370允許暫存器至暫存器定址、記憶體至暫存器定址、暫存器靠記憶體定址、暫存器靠暫存器定址、暫存器靠立即定址、暫存器至記憶體定址，該定址係部分由MOD欄位363及373且由可選擇的比例-索引-基址及位移位元組來指定。

[0092]接下來轉到圖3F，在一些替代性實施例中，可經由共處理器資料處理(CDP)指令來執行64位元(或128位元，或256位元，或512位元或更多)的單指令多資料(SIMD)算術運算。操作編碼(運算碼)格式380描述一此種CDP指令，其具有CDP運算碼欄位382及389。CDP指令之類型，對於替代性實施例，操作可由欄位383、384、387及388中之一或多者來編碼。可識別每個指令的至多三個運算元位

置，包括至多兩個來源運算元識別符385及390及一個目的地運算元識別符386。共處理器之一實施例可對8、16、32及64位元的值進行操作。對於一實施例，對整數資料元件執行指令。在一些實施例中，可依條件而定使用條件欄位381來執行指令。對於一些實施例，來源資料大小可由欄位383來編碼。在一些實施例中，零(Z)、負(N)、進位(C)及溢位(V)偵測可在SIMD欄位上完成。對於一些實施例，飽和類型可由欄位384來編碼。

[0093]接著轉至圖3G，其為對另一替代性操作編碼(運算碼)格式397之描繪，該格式用以根據另一實施例中斷及回復安全獨立領域中的分頁，該格式與以下中所描述之運算碼格式類型相對應：「Intel® Advanced Vector Extensions Programming Reference」，其可在全球資訊網(www)於intel.com/products/processor/manuals/獲自Intel公司(Santa Clara, CA)。

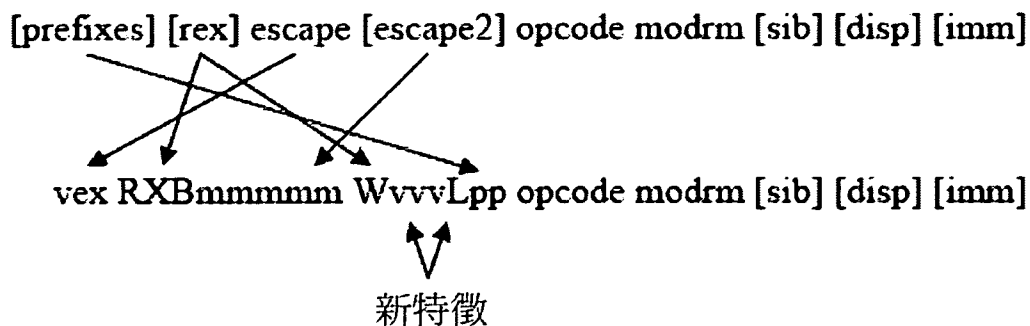
[0094]原始x86指令集提供1位元組的運算碼，各種格式之位址字節及立即運算元含於額外位元組中，自第一「運算碼」位元組已知該等額外位元組之存在。另外，有某些位元組值被保留，作為運算碼之修飾符(稱為前綴，因為該等修飾符必須置於指令之前)。當256個運算碼位元組(包括此等特殊前綴值)之原始工具板被用完時，單個位元組係作為逸出被用於256個運算碼之新集合。因為新增了向量指令(例如，SIMD)，所以產生對更多運算碼之需要，且「兩個位元組」的運算碼映射亦不夠，即使經由使用前綴予以擴

充。為此目的，在額外映射中新增新的指令，該等額外映射將2個位元組加上可選擇的前綴用作識別符。

[0095]另外，爲了促進64位元模式下的額外暫存器，在前綴與運算碼(及判定該運算碼所必需的任何逸出位元組)之間可使用額外前綴(稱爲「REX」)。在一實施例中，REX可具有4個「酬載」位元，來指示在64位元模式下使用額外暫存器。在其他實施例中，REX可具有少於或超過4個位元。至少一指令集之一般格式(其一般與格式360及/或格式370相對應)係由以下來一般例示：

[[prefixes] [rex] escape [escape2] opcode modrm(等)。

[0096]運算碼格式397與運算碼格式370相對應，且包含可選擇的VEX前綴位元組391(在一實施例中開始於C4十六進位)，以替換大多數其他常用舊式指令前綴位元組及逸出碼。例如，以下例示使用兩個欄位來編碼指令之一實施例，當第二逸出碼存在於原始指令中時，或當需要REX欄位中之額外位元(例如，XB欄位及W欄位)以使用時，可使用該實施例。在以下例示之實施例中，舊式逸出由新逸出值表示，舊式前綴完全經壓縮爲「酬載」位元組之部分，舊式前綴經收回且可利用於未來擴展，第二逸出碼經壓縮於具有可利用的未來映射或特徵空間之「映射」欄位中，且增添新特徵(例如，增加的向量長度及額外來源暫存器說明符)。



[0097] 根據一實施例之指令可由欄位391及392中一或多者來編碼。藉由欄位391，結合來源運算元識別符374及375，且結合可選擇的比例-索引-基址(SIB)識別符393、可選擇的位移識別符394及可選擇的立即位元組395，可識別每個指令的至多四個運算元位置。對於一實施例，VEX前綴位元組391可用來識別32位元或64位元的來源及目的地運算元及/或128位元或256位元的SIMD暫存器或記憶體運算元。對於一實施例，運算碼格式397所提供的功能與運算碼格式370重複，而在其他實施例中，該等功能不同。運算碼格式370及397允許暫存器至暫存器定址、記憶體至暫存器定址、暫存器靠記憶體定址、暫存器靠暫存器定址、暫存器靠立即定址、暫存器至記憶體定址，該定址係部分由MOD欄位373且由可選擇的(SIB)識別符393、可選擇的位移識別符394及可選擇的立即位元組395來指定。

[0098] 接著轉至圖3H，其為對另一替代性操作編碼(運算碼)格式398之描繪，該格式用以根據另一實施例之中斷及回復安全獨立領域中的分頁。運算碼格式398與運算碼格式370及397相對應，且包含可選擇的EVEX前綴位元組396(在一實施例中開始於62(十六進位))，以替換大多數其

他常用的舊式指令前綴位元組及逸出碼且提供額外功能。根據一實施例之指令可由欄位396及392中一或多者來編碼。藉由欄位396，結合來源運算元識別符374及375，且結合可選擇的比例-索引-基址(SIB)識別符393、可選擇的位移識別符394及可選擇的立即位元組395，可識別每個指令的至多四個運算元位置及遮罩。對於一實施例，EVEX前綴位元組396可用來識別32位元或64位元的來源及目的地運算元及/或128位元、256位元或512位元的SIMD暫存器或記憶體運算元。對於一實施例，運算碼格式398所提供的功能與運算碼格式370或397重複，而在其他實施例中，該等功能不同。運算碼格式398允許暫存器至暫存器定址、記憶體至暫存器定址、暫存器靠記憶體定址、暫存器靠暫存器定址、暫存器靠立即定址、暫存器至記憶體定址(藉由遮罩)，該定址係部分由MOD欄位373且由可選擇的(SIB)識別符393、可選擇的位移識別符394及可選擇的立即位元組395來指定。至少一指令集之一般格式(其一般與格式360及/或格式370相對應)係由以下來一般例示出：

```
evex1 RXBmmmmm WvvvLpp evex4 opcode modrm [sib]
[disp] [imm]
```

[0099]對於一實施例，根據EVEX格式398編碼的指令可具有額外「酬載」位元，該等「酬載」位元可用來以額外新特徵中斷及回復安全獨立領域中的分頁，該等新特徵諸如使用者可組配遮罩暫存器，或額外運算元，或來自128位元、256位元或512位元的向量暫存器之中的選擇，或更多

暫存器(自該等暫存器選擇)等。例如，在VEX格式397可用來以隱式遮罩中斷及回復安全獨立領域中的分頁的情況下，EVEX格式398可用來以顯式使用者可組配遮罩中斷及回復安全獨立領域中的分頁。另外，在VEX格式397可用來在128位元或256位元的向量暫存器上中斷及回復安全獨立領域中的分頁的情況下，EVEX格式398可用來在128位元、256位元、512位元或更大(或更小)的向量暫存器上中斷及回復安全獨立領域中的分頁。

[0100]用以提供先進分頁性能包括用以中斷及回復安全獨立領域中的分頁之示例性指令由以下實例例示：

指令	目的地	描述
EENTER/ ERESUME	Addr1	進入安全獨立領域，或回復存取對應於安全獨立領域位址 Addr1 的安全獨立領域儲存器，且使當前存取安全獨立領域的邏輯處理器或硬體執行緒之數目增值。
EEXIT/ AEX	Addr1	退出安全獨立領域及/或清除一或多個轉譯以存取對應於安全獨立領域位址 Addr1 的安全獨立領域儲存器，且使已並行存取安全獨立領域的邏輯處理器或硬體執行緒之數目遞減。
EBLOCK	Addr1	在安全獨立領域頁映射中將對應於具有頁記憶體位址 Addr1 的共享頁的項標記為阻擋，以防止任何新轉譯的創建，以便存取共享頁。

ETRAK	Addr1	記錄當前存取對應於安全獨立領域位址 Addr1 的安全獨立領域儲存器的邏輯處理器或硬體執行緒，且隨著任何退出安全獨立領域而使邏輯處理器或硬體執行緒之數目遞減。
EWRIEBACK/ EWB	Addr1	若先前存取安全獨立領域的邏輯處理器或硬體執行緒之數目已遞減至零，則移除、加密且寫回具有頁記憶體位址 Addr1 的共享頁。
EWRIEBACK RESUME/ EWBR	Addr1	在先前獨立領域頁寫回操作中斷之後，回復移除、加密及寫回具有頁記憶體位址 Addr1 的頁。
EBLOCK&TR ACK	Addr1	在安全獨立領域頁映射中將對應於具有頁記憶體位址 Addr1 的共享頁的項標記為阻擋，以防止任何新轉譯的創建，以便存取共享頁。記錄當前存取對應於頁記憶體位址 Addr1 的安全獨立領域的邏輯處理器或硬體執行緒，且隨著任何退出安全獨立領域而使邏輯處理器或硬體執行緒之數目遞減。
ELOAD/ ELD	Addr1	解密且將具有頁記憶體位址 Addr1 的共享頁載入至安全獨立領域頁快取記憶體中。
ELOAD RESUME/ ELDR	Addr1	在先前獨立領域頁載入操作中斷之後，回復解密及將具有頁記憶體位址 Addr1 的頁載入至安全獨立領域頁快取記憶體中。

[0101]將瞭解，藉由用以中斷及回復安全獨立領域中的分頁之以上獨立領域指令之使用，可將分頁過程(例如，其中加密且寫回安全獨立領域頁快取記憶體內容，自記憶體載入新頁且解密新頁，清除且替換TLB項，等等)分成數個級段，其中處理器核心或邏輯處理器在一或多個級段期間僅短暫地中斷。因此，可減少歸因於分頁過程的效能降級，同時保證安全獨立領域資料之安全性且不需要不當的複雜性及設計努力。

[0102]一些實施例包括多個硬體執行緒、邏輯處理器或處理核心、用以儲存對於共享頁位址之安全資料的獨立領域頁快取記憶體，該等共享頁位址分配給安全獨立領域且可由硬體執行緒、邏輯處理器或處理核心存取。EBLOCK指令之一實施例指定共享頁位址作為運算元。一或多個執行單元標記對應於用於共享頁位址之獨立領域頁快取記憶體映射的項，以阻止用於多個硬體執行緒、邏輯處理器或處理核心中任一者之新TLB轉譯之創建，以便存取共享頁。ETRACK指令之一實施例指定安全獨立領域作為運算元，且一或多個執行單元記錄當前存取對應於安全獨立領域的獨立領域頁快取記憶體中之安全資料的硬體執行緒。例如，在一實施例中，獨立領域可具有兩個或兩個以上計數器(本文中稱為「時期」計數器)，以記錄在安全獨立領域之當前時期中當前存取安全資料的硬體執行緒之數目，隨後將該數目複製至最近的先前時期計數器且將無硬體執行緒的新時期初始化為新的當前時期。在一替代性實施例

中，EBLOCK&TRACK指令指定共享頁位址作為運算元。一或多個執行單元標記對應於用於共享頁位址之獨立領域頁快取記憶體映射的項，以阻止對於多個硬體執行緒、邏輯處理器或處理核心中任一者之新TLB轉譯之創建，以便存取共享頁，且記錄當前存取對應於頁記憶體位址Addr1的安全獨立領域的邏輯處理器或硬體執行緒，且隨著任何退出安全獨立領域而使邏輯處理器或硬體執行緒之數目遞減。在一或多個替代性實施例中，時期計數器始終追蹤在安全獨立領域中執行或存取與安全獨立領域相關聯的安全資料的硬體執行緒、邏輯處理器處理核心。

[0103] OS隨後可將處理器間中斷(IPI)發送至當前存取對應於安全獨立領域的獨立領域頁快取記憶體中之安全資料的任何硬體執行緒、邏輯處理器或處理核心。當前存取對應於安全獨立領域的安全資料的每一硬體執行緒、邏輯處理器或處理核心已由指定安全獨立領域的EENTER或ERESUME指令進入安全獨立領域，且在彼時，時期數已與硬體執行緒、邏輯處理器或處理核心相關聯。當硬體執行緒、邏輯處理器或處理核心認可IPI且退出安全獨立領域時，清除該等硬體執行緒、邏輯處理器或處理核心之一或多個TLB轉譯。每當來自最近的先前時期的硬體執行緒退出安全獨立領域(例如，由EEXIT或AEX指令)時，使最近的先前時期計數器中的硬體執行緒之所記錄數目遞減。

[0104] 當硬體執行緒之所記錄數目達到零時，OS移除一或多個頁，加密資料且將該一或多個頁寫回至記憶體或

非依電性儲存器為安全的。在一實施例中，OS可使用指定共享頁位址作為運算元的EWRITEBACK或EWB指令，來完成移除、加密安全資料及將頁寫回至非依電性儲存器。因為安全資料之獨立領域保護可能無法信賴OS，所以若來自最近的先前時期的硬體執行緒之所記錄數目尚未達到零，則EWRITEBACK或EWB指令之一實施例可失敗。在其他替代性實施例中，EWRITEBACK或EWB指令可等待，直至硬體執行緒之所記錄數目達到零才執行，或引起異常。回應於指定新共享頁位址作為運算元的ELOAD或ELD指令之一實施例，OS可將自由儲存器分配給安全獨立領域之新頁且解密用於新頁之安全資料。

[0105]另外，當正加密且寫回安全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作(來自EWRITEBACK或EWB指令或來自ELOAD或ELD指令)之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊(例如，儲存於對於對應頁之快取列中，或儲存於一些其他安全儲存器中)。隨後可服務中斷，且之後可回復對應分頁操作(例如，分別使用EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指令)。因此，可保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0106]將瞭解，管理許可、實體記憶體及/或改變映射仍可由OS管理，但當記憶體內容受保護時，如在安全獨立領域中，OS可對於存取獨立領域私用記憶體之實際受保護內容不被容許或信賴。可使用用以中斷及回復安全獨立領域中的分頁之指令及處理邏輯來以分級方式實現在無法信賴OS的情況下保證專用記憶體內容之安全性及/或完整性及管理使用有限量的實體記憶體來支援較大的、受保護的、獨立領域私用記憶體空間之技術約束，而不需要精心硬體支援及/或設計努力。

[0107]圖4A為例示根據本發明之至少一實施例之循序管線，以及暫存器重新命名級段、亂序發佈/執行管線的方塊圖。圖4B為例示循序架構核心，以及暫存器重新命名邏輯、亂序發佈/執行邏輯之方塊圖，上述各者將包括於根據本發明之至少一實施例的處理器中。圖4A中之實線方框例示循序管線，而虛線方框例示暫存器重新命名、亂序發佈/執行管線。類似地，圖4B中之實線方框例示循序架構邏輯，而虛線方框例示暫存器重新命名邏輯與亂序發佈/執行邏輯。

[0108]在圖4A中，處理器管線400包括擷取級段402、長度解碼級段404、解碼級段406、分配級段408、重新命名級段410、排程(亦稱為分派或發佈)級段412、暫存器讀取/記憶體讀取級段414、執行級段416、寫回/記憶體寫入級段418、異常處置級段422及確認級段424。

[0109]在圖4B中，箭頭表示兩個或兩個以上單元之間

的耦接，且箭頭的方向指示該等單元之間的資料流的方向。圖4B展示處理器核心490，其包括耦接至執行引擎單元450之前端單元430，且該執行引擎單元及該前端單元兩者皆耦接至記憶體單元470。

[0110]核心490可為精簡指令集計算(RISC)核心、複雜指令集計算(CISC)核心、極長指令字(VLIW)核心，或者混合式或替代性核心類型。作為另一選項，核心490可為專用核心，諸如例如，網路或通訊核心、壓縮引擎、圖形核心等。

[0111]前端單元430包括耦接至指令快取記憶體單元434之分支預測單元432，該指令快取記憶體單元耦接至指令轉譯後備緩衝器(TLB)436，該指令TLB耦接至指令擷取單元438，該指令擷取單元耦接至解碼單元440。解碼單元或解碼器可解碼指令，且產生一或多個微操作、微碼進入點、微指令、其他指令或其他控制信號作為輸出，上述各者係自原始指令解碼所得，或以其他方式反映原始指令，或係由原始指令導出。可使用各種不同機構來實行解碼器。適合的機構之實例包括但不限於檢查表、硬體實行方案、可規劃邏輯陣列、微碼唯讀記憶體(ROM)等。指令快取記憶體單元434進一步耦接至記憶體單元470中的2階(L2)快取記憶體單元476。解碼單元440耦接至執行引擎單元450中的重新命名/分配器單元452。

[0112]執行引擎單元450包括重新命名/分配器單元452，該重新命名/分配器單元耦接至引退(retirement)單元

454及一或多個排程器單元456之集合。排程器單元456表示任何數種不同排程器，包括保留站、中央指令窗等。排程器單元456耦接至實體暫存器檔案單元458。實體暫存器檔案單元458中每一者表示一或多個實體暫存器檔案、儲存一或多個不同資料類型(諸如，純量整數、純量浮點、緊縮整數、緊縮浮點、向量整數、向量浮點等)、狀態(例如，為將要執行的下一個指令之位址的指令指標)等的不同實體暫存器檔案。實體暫存器檔案單元458由引退單元454重疊，以例示可實行暫存器重新命名及亂序執行的各種方式(例如，使用重新排序緩衝器及引退暫存器檔案；使用未來檔案、歷史緩衝器及引退暫存器檔案；使用暫存器映射及暫存器池；等等)。通常，架構暫存器自處理器外部或自程式設計師的角度可見。暫存器不限於任何已知特定類型之電路。各種不同類型之暫存器係適合的，只要其能夠儲存並提供如本文中所描述之資料即可。適合的暫存器之實例包括但不限於專用實體暫存器、使用暫存器重新命名的動態分配實體暫存器、專用實體暫存器與動態分配實體暫存器之組合等。引退單元454及實體暫存器檔案單元458耦接至執行聚集460。執行聚集460包括一或多個執行單元462之集合及一或多個記憶體存取單元464之集合。執行單元462可執行各種運算(例如，移位、加法、減法、乘法)且對各種類型之資料(例如，純量浮點、緊縮整數、緊縮浮點、向量整數、向量浮點)進行執行。雖然一些實施例可包括專門針對特定功能或功能集合之許多執行單元，但其他實施例可包

括僅一個執行單元或多個執行單元，該等執行單元均執行所有功能。排程器單元456、實體暫存器檔案單元458及執行叢集460被展示為可能係多個，因為某些實施例針對某些類型之資料/運算產生獨立的管線(例如，純量整數管線、純量浮點/緊縮整數/緊縮浮點/向量整數/向量浮點管線，及/或記憶體存取管線，其中每一管線具有其自有之排程器單元、實體暫存器檔案單元及/或執行叢集；且在獨立的記憶體存取管線的狀況下，所實行的某些實施例中，唯有此管線之執行叢集具有記憶體存取單元464)。亦應理解，在使用獨立的管線之情況下，此等管線中之一或多者可為亂序發佈/執行而其餘管線可為循序的。

[0113]記憶體存取單元464之集合耦接至記憶體單元470，該記憶體單元包括耦接至資料快取記憶體單元474的資料TLB單元472，該資料快取記憶體單元耦接至2階(L2)快取記憶體單元476。在一示範性實施例中，記憶體存取單元464可包括載入單元、儲存位址單元及儲存資料單元，其中每一者耦接至記憶體單元470中的資料TLB單元472。L2快取記憶體單元476耦接至一或多個其他階快取記憶體且最終耦接至主記憶體。

[0114]藉由實例，示範性暫存器重新命名、亂序發佈/執行核心架構可將管線400實行如下：1)指令擷取438執行擷取級段402及長度解碼級段404；2)解碼單元440執行解碼級段406；3)重新命名/分配單元452執行分配級段408及重新命名級段410；4)排程器單元456執行排程級段412；5)實體

暫存器檔案單元458及記憶體單元470執行暫存器讀取/記憶體讀取級段414；執行叢集460執行執行級段416；6)記憶體單元470及實體暫存器檔案單元458執行寫回/記憶體寫入級段418；7)異常處置級段422中可涉及各種單元；及8)引退單元454及實體暫存器檔案單元458執行確認級段424。

[0115]核心490可支援一或多個指令集(例如，x86指令集(以及一些擴展，較新版本已新增該等擴展)；MIPS Technologie公司(Sunnyvale, CA)的MIPS指令集；ARM Holdings公司(Sunnyvale, CA)的ARM指令集(以及可選擇的額外擴展，諸如NEON))。

[0116]應理解，核心可支援多執行緒處理(multithreading)(執行操作或執行緒之兩個或兩個以上並行集合)，且可以各種方式完成此支援，其中包括經時間切割之多執行緒處理、同時多執行緒處理(其中單個實體核心針對該實體核心同時在多執行緒處理的各執行緒中之每一者提供一邏輯核心)或上述各者之組合(例如，經時間切割之擷取及解碼以及隨後同時的多執行緒處理，諸如在Intel®超多執行緒處理(Hyperthreading)技術中)。

[0117]雖然在亂序執行的情況下描述暫存器重新命名，但應理解，暫存器重新命名可用於循序架構中。雖然處理器之所例示實施例亦包括獨立的指令與資料快取記憶體單元434/474以及共享的L2快取記憶體單元476，但替代性實施例可具有用於指令與資料兩者的單個內部快取記憶體，諸如1階(L1)內部快取記憶體或多階內部快取記憶體。

在一些實施例中，系統可包括內部快取記憶體與外部快取記憶體之組合，該外部快取記憶體在核心及/或處理器外部。或者，所有快取記憶體可在核心及/或處理器外部。

[0118]圖5為根據本發明之實施例之單核心處理器及多核心處理器500的方塊圖，該處理器具有整合型記憶體控制器及圖形元件。圖5中之實線方框例示處理器500，該處理器具有單個核心502A、系統代理510、一或多個匯流排控制器單元516之集合，而虛線方框之可選擇的增添例示替代性處理器500，該替代性處理器具有多個核心502A-N、位於系統代理單元510中的一或多個整合型記憶體控制器單元514之集合，以及整合型圖形邏輯508。

[0119]記憶體階層包括該等核心內的一或多階快取記憶體、一或多個共享快取記憶體單元506之集合、耦接至整合型記憶體控制器單元514之集合的外部記憶體(圖中未示)。共享快取記憶體單元506之集合可包括一或多個中階快取記憶體，諸如2階(L2)、3階(L3)、4階(L4)，或其他階快取記憶體、末階快取記憶體(LLC)，及/或上述各者之組合。雖然在一實施例中，環式互連單元512對整合型圖形邏輯508、共享快取記憶體單元506之集合及系統代理單元510進行互連，但替代性實施例可使用任何數種熟知技術來互連此等單元。

[0120]在一些實施例中，核心502A-N中一或多者能夠進行多執行緒處理。系統代理510包括協調並操作核心502A-N之該等組件。系統代理單元510可包括，例如，功率

控制單元(PCU)及顯示單元。PCU可為調節核心502A-N及整合型圖形邏輯508之功率狀態所需要的邏輯及組件，或者包括上述邏輯及組件。顯示單元係用於驅動一或多個外部已連接顯示器。

[0121]核心502A-N就架構及/或指令集而言可為同質的或異質的。例如，核心502A-N中之一些可為循序的，而其他核心係亂序的。作為另一實例，核心502A-N中之兩者或兩者以上可能能夠執行同一指令集，而其他核心可能僅能夠執行該指令集之子集或不同的指令集。

[0122]處理器可為通用處理器，諸如Core™ i3、i5、i7、2 Duo and Quad、Xeon™、Itanium™、XScale™或StrongARM™處理器，其可自Intel公司(Santa Clara, Calif)獲得。或者，處理器可來自另一公司，諸如ARM Holdings公司、MIPS等。處理器可為專用處理器，諸如網路或通訊處理器、壓縮引擎、圖形處理器、共處理器、嵌入式處理器等。處理器可實行於一或多個晶片上。處理器500可為一或多個基板之部分且/或可使用許多處理技術(例如BiCMOS、CMOS或NMOS)中之任一者將處理器500實行於一或多個基板上。

[0123]圖6至圖8為適合於包括處理器500之示範性系統，而圖9為可包括核心502中一或多者的示範性系統單晶片(SoC)。此項技術中已知的關於以下各者之其他系統設計及組態亦適合：膝上型電腦、桌上型電腦、手持式PC、個人數位助理、工程工作站、伺服器、網路裝置、網路集線

器、交換器、嵌入式處理器、數位信號處理器(DSP)、圖形裝置、視訊遊戲裝置、機上盒、微控制器、行動電話、攜帶型媒體播放器、手持式裝置，以及各種其他電子裝置。一般而言，能夠併入如本文中所揭示之處理器及/或其他執行邏輯的多種系統或電子裝置通常適合。

[0124]現參考圖6，所展示為根據本發明之一實施例之系統600的方塊圖。系統600可包括一或多個處理器610、615，該等處理器耦接至圖形記憶體控制器集線器(GMCH)620。圖6中用間斷線表示額外處理器615之可選擇性質。

[0125]每一處理器610、615可為處理器500之某一版本。然而，應注意，整合型圖形邏輯及整合型記憶體控制單元不太可能存在於處理器610、615中。圖6例示GMCH 620可耦接至記憶體640，該記憶體可為例如動態隨機存取記憶體(DRAM)。對於至少一實施例，DRAM可與非依電性快取記憶體相關聯。

[0126]GMCH 620可為晶片組或晶片組之一部分。GMCH 620可與處理器610、615通訊，且控制處理器610、615與記憶體640之間的互動。GMCH 620亦可充當處理器610、615與系統600之其他元件之間的加速匯流排介面。對於至少一實施例，GMCH 620經由多分支匯流排(multi-drop bus)，諸如前端匯流排(FSB)695，與處理器610、615通訊。

[0127]此外，GMCH 620耦接至顯示器645(諸如平板顯示器)。GMCH 620可包括整合型圖形加速器。GMCH 620

進一步耦接至輸入/輸出(I/O)控制器集線器(ICH) 650，該ICH可用來將各種周邊裝置耦接至系統600。在圖6之實施例中，例如展示了外部圖形裝置660(其可為耦接至ICH 650之離散圖形裝置)，以及另一周邊裝置670。

[0128]或者，系統600中亦可存在額外或不同的處理器。例如，額外處理器615可包括：與處理器610相同的額外處理器；與處理器610異質或不對稱的額外處理器；加速器(諸如，圖形加速器或數位信號處理(DSP)單元)；現場可規劃陣列；或任何其他處理器。就優點量度範圍而言，實體資源610與615之間可能有各種差異，其中包括架構特性、微架構特性、熱特性、功率消耗特性等。此等差異可有效表明其本身在處理器610與615之間的不對稱性及異質性。對於至少一實施例，各種處理器610、615可駐留在同一晶粒封裝中。

[0129]現參考圖7，所展示為根據本發明之一實施例之第二系統700的方塊圖。如圖7中所示，多處理器系統700係點對點互連系統，且包括第一處理器770及第二處理器780，該等處理器經由點對點互連750予以耦接。如同處理器610、615中一或多者，處理器770及780中每一者可為處理器500之某一版本。

[0130]雖然展示了僅兩個處理器770、780，但應理解，本發明之範疇不限於此。在其他實施例中，給定處理器中可存在一或多個額外處理器。

[0131]所展示處理器770及780分別包括整合型記憶體

控制器單元772及782。處理器770亦包括點對點(P-P)介面776及778，作為該處理器之匯流排控制器單元的部分；類似地，第二處理器780包括P-P介面786及788。處理器770、780可使用P-P介面電路778、788經由點對點(P-P)介面750交換資訊。如圖7中所示，IMC 772及782將處理器耦接至個別記憶體，亦即，記憶體732及記憶體734，該等記憶體可為局部地附接至個別處理器之主記憶體的部分。

[0132]處理器770、780各自可使用點對點介面電路776、794、786、798經由個別P-P介面752、754與晶片組790交換資訊。晶片組790亦可經由高效能介面739與高效能圖形電路738交換資訊。

[0133]在任一處理器中或兩個處理器外部，可包括共享快取記憶體(圖中未示)，而該共享快取記憶體經由P-P互連與該等處理器連接，使得當處理器被置於低功率模式中時，可將任一處理器或兩個處理器之區域快取記憶體資訊儲存在該共享快取記憶體中。

[0134]晶片組790可經由介面796耦接至第一匯流排716。在一實施例中，第一匯流排716可為周邊組件互連(PCI)匯流排，或者諸如高速PCI匯流排或另一第三代I/O互連匯流排之匯流排，但本發明之範疇不限於此。

[0135]如圖7中所示，各種I/O裝置714以及匯流排橋接器718可耦接至第一匯流排716，該匯流排橋接器將第一匯流排716耦接至第二匯流排720。在一實施例中，第二匯流排720可為低接腳計數(LPC)匯流排。各種裝置可耦接至第

二匯流排720，其中包括，例如，鍵盤及/或滑鼠722、通訊裝置727，及儲存單元728，諸如磁碟機或其他大容量儲存裝置，在一實施例中，該儲存單元可包括指令/碼及資料730。此外，音訊I/O 724可耦接至第二匯流排720。請注意，其他架構係可能的。例如，代替圖7之點對點架構，系統可實行多分支匯流排或其他此種架構。

[0136]現在參考圖8，所展示為根據本發明之一實施例之第三系統800的方塊圖。圖7及圖8中的相似元件帶有相似參考數字，且圖8已省略圖7之某些態樣以避免混淆圖8之其他態樣。

[0137]圖8例示處理器870、880分別可包括整合型記憶體及I/O控制邏輯(「CL」)872及882。對於至少一實施例，CL 872及882可包括整合型記憶體控制器單元，諸如以上關於圖5及圖7所描述之單元。另外，CL 872、882亦可包括I/O控制邏輯。圖8例示不僅記憶體832、834耦接至CL 872、882，而且I/O裝置814亦耦接至控制邏輯872、882。舊式I/O裝置815耦接至晶片組890。

[0138]現在參考圖9，所展示為根據本發明之一實施例之SoC 900的方塊圖。圖5中的類似元件帶有相似參考數字。此外，虛線方框係更先進SoC上之可選擇的特徵。在圖9中，互連單元902耦接至以下各者：應用處理器910，其包括一或多個核心502A-N之集合及共享快取記憶體單元506；系統代理單元510；匯流排控制器單元516；整合型記憶體控制器單元514；一或多個媒體處理器920之集合，其

可包括整合型圖形邏輯508、用於提供靜態及/或視訊攝影機功能的影像處理器924、用於提供硬體音訊加速的音訊處理器926及用於提供編碼/解碼加速的視訊處理器928；靜態隨機存取記憶體(SRAM)單元930；直接記憶體存取(DMA)單元932；以及用於耦接至一或多個外部顯示器的顯示單元940。

[0139]圖10例示含有中央處理單元(CPU)及圖形處理單元(GPU)之處理器，該等單元可執行根據一實施例之至少一指令。在一實施例中，執行根據至少一實施例之操作的指令可由CPU執行。在另一實施例中，該指令可由GPU執行。在又一實施例中，該指令可經由GPU與CPU所執行之操作之組合來執行。例如，在一實施例中，可接收並解碼根據一實施例之指令以便在GPU上執行。然而，在經解碼後指令內之一或多個操作可由CPU執行，且結果被傳回至GPU以便該指令最終引退。相反，在一些實施例中，CPU可充當主處理器而GPU充當共處理器。

[0140]在一些實施例中，受益於高度平行的通量處理器之指令可由GPU執行，而受益於如下處理器的執行之指令可由CPU執行，該等處理器受益於深度管線化的架構。例如，圖形、科學應用、金融應用及其他平行工作負載可受益於GPU的執行且相應地被執行，而更為依序的應用(諸如作業系統核心或應用程式碼)可能更適合於CPU。

[0141]在圖10中，處理器1000包括CPU 1005、GPU 1010、影像處理器1015、視訊處理器1020、USB控制器

1025、UART控制器1030、SPI/SDIO控制器1035、顯示裝置1040、高清晰度多媒體介面(HDMI)控制器1045、MIPI控制器1050、快閃記憶體控制器1055、雙資料速率(DDR)控制器1060、安全引擎1065及I2S/I2C(整合型晶片間聲音/內部整合電路)介面1070。圖10之處理器中可包括其他邏輯與電路，其中包括更多的CPU或GPU及其他周邊介面控制器。

[0142]至少一實施例之一或多個態樣可由儲存於機器可讀媒體上的代表性資料來實行，此資料表示處理器內的各種邏輯，此資料在由機器讀取時使機器製造邏輯來執行本文中描述之技術。此類表示(稱為「IP核心」)可儲存於有形的機器可讀媒體(「磁帶」)上且可供應給各種顧客或製造設施來載入至實際上製造該邏輯或處理器的製造機中。例如，IP核心(諸如由ARM Holdings公司開發出的Cortex™系列處理器，以及由中國科學院的計算技術研究所(ICT)開發出的Loongson IP核心)可被授權給或賣給各種顧客或被授權者，諸如Texas Instruments、Qualcomm、Apple或Samsung，並且實行於由此等顧客或被授權者生產的處理器中。

[0143]圖11展示例示根據一實施例之IP核心的開發之方塊圖。儲存器1130包括模擬軟體1120及/或硬體或軟體模型1110。在一實施例中，可經由記憶體1140(例如，硬碟)、有線連接(例如，網際網路)1150或無線連接1160將表示IP核心設計之資料提供至儲存器1130。由模擬工具及模型產生之IP核心資訊隨後可被傳輸至製造設施，在該製造設施

處，IP核心資訊可由第三方製造來執行根據至少一實施例的至少一指令。

[0144] 在一些實施例中，一或多個指令可對應於第一類型或架構(例如，x86)且在不同類型或架構(例如，ARM)之處理器上被轉譯或仿真。因此可在任何處理器或處理器類型(包括ARM、x86、MIPS、GPU或其他處理器類型或架構)上執行根據一實施例的指令。

[0145] 圖12例示如何由不同類型之處理器來仿真根據一實施例的第一類型之指令。在圖12中，程式1205含有一些指令，該等指令可執行與根據一實施例的指令相同或大體上相同之功能。然而，程式1205之指令之類型及/或格式可能與處理器1215不同或不相容，此意味著程式1205中之類型之指令可無法由處理器1215原型地執行。然而，藉助於仿真邏輯1210，將程式1205之指令轉譯為能夠由處理器1215原型地執行之指令。在一實施例中，仿真邏輯體現於硬體中。在另一實施例中，仿真邏輯體現於有形的機器可讀媒體中，該媒體含有軟體，用來將程式1205中之類型之指令轉譯為可由處理器1215原型地執行之類型。在其他實施例中，仿真邏輯為固定功能或可規劃硬體與儲存於有形的機器可讀媒體上之程式之組合。在一實施例中，處理器含有仿真邏輯，然而在其他實施例中，仿真邏輯存在於處理器外部且由第三方提供。在一實施例中，處理器能夠藉由執行含於處理器中或與處理器相關聯之微碼或韌體來載入仿真邏輯，該仿真邏輯體現於含有軟體之有形的機器可

讀媒體中。

[0146]圖13為對照根據本發明之實施例之軟體指令轉換器的用途之方塊圖，該轉換器係用以將來源指令集中之二進位指令轉換成目標指令集中之二進位指令。在所例示之實施例中，指令轉換器係軟體指令轉換器，但指令轉換器或者可以軟體、韌體硬體、或上述各者之各種組合來實行。圖13展示，可使用x86編譯器1304來編譯用高階語言1302撰寫的程式以產生x86二進位碼1306，該x86二進位碼可由具有至少一x86指令集核心之處理器1316原型地執行。具有至少一x86指令集核心之處理器1316表示可執行與具有至少一x86指令集核心之Intel處理器大體上相同的功能之任何處理器，上述執行係藉由相容地執行或以其他方式處理以下各者：(1)Intel x86指令集核心之指令集的大部分，或(2)旨在在具有至少一x86指令集核心之Intel處理器上運行的應用程式或其他軟體之目標碼版本，以便達成與具有至少一x86指令集核心之Intel處理器大體上相同的結果。x86編譯器1304表示可操作以產生x86二進位碼1306(例如，目標碼)之編譯器，其中該x86二進位碼在經額外連結處理或未經額外連結處理的情況下可在具有至少一x86指令集核心之處理器1316上執行。類似地，圖13展示，可使用替代性指令集編譯器1308來編譯用高階語言1302撰寫的程式以產生替代性指令集二進位碼1310，該替代性指令集二進位碼可由不具有至少一x86指令集核心之處理器1314(例如，具有多個核心的處理器，該等核心執行MIPS

Technologie公司(Sunnyvale, CA)之MIPS指令集，及/或該等核心執行ARM Holdings公司(Sunnyvale, CA)之ARM指令集)原型地執行。使用指令轉換器1312將x86二進位碼1306轉換成可由不具有一個x86指令集核心之處理器1314原型地執行的碼。此轉換後的碼不可能與替代性指令集二進位碼1310相同，因為能夠實現此操作的指令轉換器很難製作；然而，轉換後的碼將實現一般操作且由來自替代性指令集之指令構成。因此，指令轉換器1312表示經由仿真、模擬或任何其他過程來允許不具有x86指令集處理器或核心的處理器或其他電子裝置執行x86二進位碼1306的軟體、韌體、硬體或上述各者之組合。

[0147]圖14例示處理系統1401之一實施例，該處理系統用於使用指令來提供用於安全獨立領域頁快取記憶體，亦即EPC 1460之高級分頁性能，包括來中斷及回復安全獨立領域中的分頁。系統1401包括系統記憶體1490及處理器1402。處理器1402包含第一硬體執行緒或邏輯處理器1420及第二硬體執行緒或邏輯處理器1430。將瞭解，雖然為簡單起見將處理器1402例示為包含各自表示單個硬體執行緒的兩個邏輯處理器，但本發明不限於此。例如，對於諸如處理器1402之處理器或本文所例示之其他處理器而言具有若干邏輯處理器核心係典型的，該等邏輯處理器核心可共享或可並不共享一些實體資源(例如EPC 1460)及或電路(例如SE單元1470)，每一邏輯處理器或處理器核心具有多個硬體執行緒，該等多個硬體執行緒能夠同時或並行執行軟體

執行緒。

[0148]處理器1402亦包含安全獨立領域(SE)單元1470及獨立領域頁快取記憶體，亦即EPC 1460。對於一些實施例，EPC 1460可為較大快取記憶體單元之部分，例如一或多個1階快取記憶體1440及1450，或2階快取記憶體(圖中未示)。對於其他實施例，EPC 1460可為由多個硬體執行緒、邏輯處理器或處理核心共享的獨立的結構或分散式結構(例如快取記憶體1440及快取記憶體1450)，該結構用以儲存用於共享頁1442、1444及1456之位址之安全資料，該等位址經分配給安全獨立領域且可由硬體執行緒、邏輯處理器或處理核心存取。

[0149]類似地，SE單元1470可包含由多個硬體執行緒、邏輯處理器或處理核心共享的獨立的結構或分散式結構(例如，SE單元1427及1437)，該結構具有加密單元、完整性保護單元、存取控制單元、範圍暫存器、獨立領域頁快取記憶體映射，及用以儲存至少一先前時期及一當前時期之兩個或兩個以上時期計數器儲存位置。SE單元1470亦支援用以中斷及回復安全獨立領域中的分頁之獨立領域指令。

[0150]在此實例中，邏輯處理器1420具有解碼級段1422、讀取級段1424、一或多個執行單元(例如執行單元1426)及寫入級段1428。邏輯處理器1420亦具有TLB 1425，在該TLB中，可安裝轉譯以存取EPC 1460。邏輯處理器1430具有解碼級段1432、讀取級段1434、一或多個執行單元(例

如執行單元1436)及寫入級段1438。邏輯處理器1430亦具有 TLB 1435，在該TLB中，可安裝轉譯以存取EPC 1460。邏輯處理器1420及1430之實施例亦可包含其他管線級段(例如，如管線400中所示)，以便執行獨立領域指令來提供用於安全獨立領域頁快取記憶體，亦即EPC 1460之高級分頁性能。邏輯處理器1420及1430之實施例亦可支援用以中斷及回復安全獨立領域中的分頁之獨立領域指令。

[0151]將瞭解，藉由包括用以中斷及回復安全獨立領域中的分頁之指令的獨立領域指令之使用，可將分頁過程(例如，其中加密且寫回安全獨立領域頁快取記憶體內容，自記憶體載入新頁且解密新頁，清除且替換TLB項，等等)分成數個級段，其中處理器核心或邏輯處理器(例如邏輯處理器1420及1430)在一或多個級段期間僅短暫地中斷。因此，可減少歸因於分頁過程的效能降級，同時保證安全獨立領域資料之安全性且不需要不當的複雜性及設計努力。另外，當正加密且寫回安全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊(例如，儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。隨後可服務中斷，且之後可回復對應分頁操作。因此，保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務任何迫近中斷避免諸如語音、視訊

及即時交易的服務中之不受歡迎的假信號。

[0152]在一實施例中，EBLOCK指令指定共享頁(例如頁1442)之位址作為運算元。一或多個執行單元(例如執行單元1426)標記對應於用於共享頁位址之獨立領域頁快取記憶體映射的項目，以阻止用於多個硬體執行緒、邏輯處理器或處理核心中任一者之新TLB轉譯(例如在TLB 1435中)之創建，以便存取共享頁。在一實施例中，ETRACK指令指定安全獨立領域作為運算元，且一或多個執行單元(例如執行單元1426)記錄當前存取對應於安全獨立領域的獨立領域頁快取記憶體，亦即EPC 1460中的安全資料的硬體執行緒。例如，在一實施例中，獨立領域可具有兩個或兩個以上時期計數器，以記錄在安全獨立領域之當前時期中當前存取安全資料的硬體執行緒之數目，隨後將該數目複製至最近的先前時期計數器(例如，回應於ETRACK指令)且將無硬體執行緒的新時期初始化為新的當前時期。

[0153]OS隨後可將IPI發送至當前存取對應於安全獨立領域的獨立領域頁快取記憶體中的安全資料的任何硬體執行緒、邏輯處理器或處理核心。在一實施例中，當前存取對應於安全獨立領域的安全資料的每一硬體執行緒、邏輯處理器或處理核心(例如邏輯處理器1420及1430)已由指定安全獨立領域的EENTER或ERESUME指令進入安全獨立領域，且在彼時，時期數目已與硬體執行緒、邏輯處理器或處理核心相關聯。當硬體執行緒、邏輯處理器或處理核心認可IPI且退出安全獨立領域時，可清除(例如自TLB 1425

及/或TLB 1435)該等硬體執行緒、邏輯處理器或處理核心之一或多個TLB轉譯。每當來自最近的先前時期的硬體執行緒退出安全獨立領域(例如，由EEXIT或AEX指令)時，使最近的先前時期計數器中的所記錄硬體執行緒之數目遞減。

[0154]當硬體執行緒之所記錄數目達到零時，OS移除一或多個頁(例如頁1442)、加密資料且將該一或多個頁寫回至記憶體(例如作為編碼後頁1495)或寫回至非依電性儲存器為安全的。在一實施例中，OS可使用指定共享頁(例如頁1442)之位址作為運算元的EWRITEBACK或EWB指令，以便完成移除、加密安全資料及將頁寫回至記憶體或非依電性儲存器。因為安全資料之獨立領域保護可能無法信賴OS，所以若來自最近的先前時期的硬體執行緒之所記錄數目尚未達到零，則EWRITEBACK或EWB指令之一實施例可失敗。在其他替代性實施例中，EWRITEBACK或EWB指令可等待，直至硬體執行緒之所記錄數目達到零才執行，或可引起異常。在一實施例中，OS隨後可使用ELOAD指令以自記憶體或非依電性儲存器讀取新頁(例如頁1410)，解密資料且將解密後頁儲存於EPC 1460中。因此，可將分頁過程(例如，其中加密且寫回安全獨立領域頁快取記憶體內容，自記憶體載入新頁且解密新頁，清除且替換TLB項，等等)分成數個級段，其中處理器核心或邏輯處理器(例如邏輯處理器1420及1430)在一或多個級段期間僅短暫地中斷(例如由IPI)。

[0155]當正加密且寫回安全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作(例如來自EWRITEBACK或EWB指令或來自ELOAD或ELD指令)之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於用於對應頁之適當未使用快取列中(或儲存於一些其他安全儲存器中)。隨後可服務中斷，且之後可回復對應分頁操作(例如，分別使用EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指令)。因此，可保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0156]圖15例示用於使用指令來提供用於安全獨立領域頁快取記憶體之高級分頁性能包括來中斷及回復安全獨立領域中的分頁的處理器1501中的設備之一實施例。設備包含安全獨立領域(SE)單元1502及獨立領域頁快取記憶體，亦即EPC 1520。對於一些實施例，EPC 1520可為較大快取記憶體單元之部分，例如1階快取記憶體，L1 1540，或2階快取記憶體(圖中未示)。對於其他實施例，EPC 1520可為由多個硬體執行緒、邏輯處理器或處理核心共享的獨立的結構或分散式結構，該結構用以儲存用於共享頁1542之位址之安全資料，該等位址分配給安全獨立領域且可由硬體執行緒、邏輯處理器或處理核心存取。SE單元1502可

包含加密單元1510、完整性保護單元1512、存取控制單元1514、範圍暫存器1516、獨立領域頁快取記憶體映射EPC 1518，及兩個或兩個以上時期計數器儲存位置：先前時期，PE 1517及當前時期，CE 1519。SE單元1502亦可包含獨立領域指令1503，其中包括：EBLOCK指令1531、ETRACK指令1532、EWB指令1533、ELOAD指令1534、EEXIT指令1535、EENTER指令1536、EWR(或EWRITEBACK RESUME)指令1537、ELOADR(或ELOAD RESUME或ELDR)指令1538，及圖中未示之其他獨立領域指令(例如AEX指令、ERESUME指令等)。

[0157]處理器核心1501亦包含TLB 1525，在該TLB中可安裝轉譯以存取EPC 1520。處理器核心1501亦包含解碼級段1522、讀取級段1524、一或多個執行單元(例如執行單元1526)及寫入級段1528。處理器核心1501之實施例亦可包含其他管線級段(例如，如管線400中所示)，以便執行獨立領域指令1503來提供高級分頁性能，包括來中斷及回復安全獨立領域頁快取記憶體，亦即EPC 1520中的分頁。

[0158]在一實施例中，EBLOCK指令1531指定共享頁1542位址作為運算元。一或多個執行單元(例如執行單元1526)標記對應於用於共享頁1542之位址之EPCM 1518中的獨立領域頁快取記憶體映射的項，以阻止用於硬體執行緒、邏輯處理器或處理核心之新TLB轉譯(例如在TLB 1525中或在任何其他TLB中)之創建，以便存取共享頁。在一實施例中，ETRACK指令1532指定安全獨立領域作為運算

元，且一或多個執行單元(例如執行單元1526，或存取控制單元1514)記錄當前存取對應於安全獨立領域的獨立領域頁快取記憶體EPC 1520中的安全資料的硬體執行緒。例如，在一實施例中，獨立領域可具有兩個或兩個以上時期計數器(例如在PE 1517中及在CE 1519中)，以記錄在安全獨立領域之當前時期中(例如在CE 1519中)當前存取安全資料的硬體執行緒之數目，隨後將該數目複製至最近的先前時期計數器(例如在PE 1517中)，且將無硬體執行緒的新時期初始化為新的當前時期(例如在CE 1519中)。

[0159] OS隨後可將IPI發送至當前存取對應於安全獨立領域的獨立領域頁快取記憶體EPC 1520中的安全資料的任何硬體執行緒、邏輯處理器或處理核心。當前存取對應於安全獨立領域的安全資料的每一硬體執行緒、邏輯處理器或處理核心已由指定安全獨立領域的EENTER(或ERESUME)指令1536進入安全獨立領域，且在彼時，時期數已與硬體執行緒、邏輯處理器或處理核心相關聯。當硬體執行緒、邏輯處理器或處理核心認可IPI且退出安全獨立領域時，可清除(例如自TLB 1525)該等硬體執行緒、邏輯處理器或處理核心之一或多個TLB轉譯。每當來自最近的先前時期(例如對應於PE 1517)的硬體執行緒由EEXIT(或AEX)指令1535退出安全獨立領域時，使最近的先前時期計數器中(例如PE 1517中)的硬體執行緒之所記錄數目遞減。

[0160] 當硬體執行緒之所記錄數目(例如在PE 1517中)達到零時，OS移除一或多個頁(例如共享頁1542)、加密資

料及將該一或多個頁寫回至記憶體或非依電性儲存器為安全的。在一實施例中，OS可使用指定共享頁1542之位址作為運算元的EWB(或EWRITEBACK)指令1533，來完成移除、加密安全資料及將頁1542寫回至非依電性儲存器。因為安全資料之獨立領域保護可無法信賴OS，所以若來自最近的先前時期的硬體執行緒之所記錄數目(例如在PE 1517中)尚未達到零，則EWB指令1533之一實施例可失敗。在其他替代性實施例中，EWB指令1533可等待，直至硬體執行緒之所記錄數目(例如在PE 1517中)達到零才執行，或EWB指令1533可引起異常。在移除、加密及頁1542至非依電性儲存器之寫回之後，可執行ELD(或ELOAD)指令1534，該指令在一實施例中指定新的共享頁位址作為運算元。

[0161]當正加密且寫回安全獨立領域頁快取記憶體內容(例如共享頁1542)時，且/或當正自記憶體載入且解密新頁時，取得正向不中斷進展，且可執行週期性檢測以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作(例如來自EWRITEBACK或EWB指令1533，或來自ELOAD或ELD指令1534)之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於用於對應頁(例如共享頁1542中)之快取列中(或儲存於一些其他安全儲存器中)。在一些實施例中，頁狀態資訊可包括指標以記錄位置以便在指令之執行部分完成之後回復。在一些實施例中，可將頁狀態資訊儲存於用於對應頁之第一快取列中(根據EWRITEBACK或EWB指令1533，或亦根據

EWRITEBACK RESUME或EWBR指令1537)。在一些實施例中，可將頁狀態資訊儲存於用於對應頁之最後快取列中(根據ELOAD或ELD指令1534，或亦根據ELOAD RESUME或ELDR指令1538)。隨後可服務中斷，且之後可回復對應分頁操作(例如，分別使用EWRITEBACK RESUME或EWBR指令1537，或ELOAD RESUME或ELDR指令1538)。因此，可保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0162]將瞭解，管理許可、實體記憶體及/或改變映射仍可由OS管理，但當記憶體內容受保護時，如在安全獨立領域中，OS可對於存取獨立領域私用記憶體之實際受保護內容不被容許或信賴。可使用用以中斷及回復安全獨立領域中的分頁之指令及處理邏輯來以分級方式實現在無法信賴OS的情況下保證專用記憶體內容之安全性及/或完整性及管理使用有限量的實體記憶體(例如EPC 1520或EPC 1460)來支援較大、受保護、獨立領域私用記憶體空間之技術約束，而不需要精心硬體支援及/或設計努力。當正加密且寫回安全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊(例如，儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。隨後可服務中

斷，且之後可回復對應分頁操作。因此，保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務任何迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0163]圖16A例示用以提供高級分頁性能包括用以中斷及回復安全獨立領域中的分頁之過程1601之一實施例的流程圖。過程1601及本文所揭示之其他過程由處理區塊執行，該等處理區塊可包含專用硬體或軟體或韌體操作碼，該等操作碼可由通用機器或可由專用機器或者可由兩者之組合執行。

[0164]在過程1601之處理區塊1610中，創建安全獨立領域以保護私用資料及/或指令。在處理區塊1620中，將EPC頁分配給安全獨立領域。在處理區塊1625中，判定是否需要分頁。若否，則EPC頁繼續在處理區塊1620中被分配給安全獨立領域，其中可將安全資料儲存於用於共享頁位址之EPC列中，該等共享頁位址係分配給可由在安全獨立領域中執行的多個硬體執行緒存取的安全獨立領域。否則，在處理區塊1630中，執行一或多個EBLOCK指令，每一EBLOCK指令在一實施例中指定共享頁位址作為運算元。在處理區塊1640中，執行ETRACK指令，ETRACK指令在一實施例中指定安全獨立領域。在處理區塊1650中，將IPI發送至在安全獨立領域中執行的每一邏輯處理器以使該等邏輯處理器退出安全獨立領域。每一邏輯處理器上之中斷處置器可繼而認可IPI。在處理區塊1660中驗證IPI之認可，

且在處理區塊1665中判定是否所有IPI已經認可。若否，則處理在處理區塊1660中繼續，但若所有IPI已經認可，則處理繼續進行處理區塊1670。在處理區塊1670中，執行一或多個EWB指令，每一EWB指令在一實施例中指定受阻共享頁位址之一作為運算元。在處理區塊1680中，執行一或多個ELOAD指令，每一ELOAD指令在一實施例中指定新共享頁位址作為運算元。過程隨後反復在處理區塊1625中開始。當正加密且寫回安全獨立領域頁快取記憶體內容(例如在處理區塊1670中)時，且/或當正自記憶體載入且解密新頁(例如在處理區塊1680中)時，可取得正向不中斷進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊之一部分(例如，儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。在一些實施例中，可能將頁狀態資訊之部分儲存於用於對應頁之第一快取列中(例如，在EWRITEBACK或EWB指令期間，而且亦在EWRITEBACK RESUME或EWBR指令期間)。在一些實施例中，可將頁狀態資訊之部分儲存於用於對應頁之最後快取列中(例如在ELOAD或ELD指令期間，而且亦在ELOAD RESUME或ELDR指令期間)。在一些實施例中，頁狀態資訊之部分可包括用以記錄位置以在指令之執行部分完成之後回復的指示。隨後可服務中斷，且之後可回復對應分頁操作(例如，分別使用EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指

令)。在一些實施例中，對安全獨立領域中的未完成或部分完成的頁之任何其他存取可導致獨立領域頁故障及/或未完成或部分完成的分頁操作之回復。在一些實施例中，亦可將對安全獨立領域中的未完成或部分完成的頁之任何其他存取記錄於用於對應未完成或部分完成的頁之一或多個快取列中。

[0165]圖16B例示用以中斷及回復安全獨立領域中的分頁之過程1607之一實施例的流程圖。在處理區塊1671中，EWB(或EWRITEBACK)指令在將要加密且寫回的頁上開始分頁操作之執行。在處理區塊1672中，在寫回分頁操作中取得正向不中斷進展。在處理區塊1673中，可執行週期性檢查以判定寫回分頁操作是否已結束，在已結束狀況下，處理繼續進行處理區塊1678，或否則在處理區塊1674中判定是否存在任何迫近中斷。若否，則處理在處理區塊1672中繼續。當存在迫近中斷時，處理繼續進行處理區塊1675，其中為寫回分頁操作之狀態設置檢查點(例如，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊之部分儲存於用於對應頁之快取列中或儲存於一些其他安全儲存器中，等等)。在處理區塊1676中，將返回諮詢碼(例如，指示可服務中斷)。在處理區塊1690中，服務中斷，且在處理區塊1677中，使用所儲存檢查點狀態資訊(例如，對於一實施例在用於對應頁之第一快取列中)在將要加密且寫回的頁上回復(例如藉由執行EWRITEBACK RESUME或EWBR指令)寫回分頁操作。處

理隨後反復在處理區塊1672中開始，直至在處理區塊1673中，寫回分頁操作已結束且寫回分頁操作(例如根據執行EWB或EWRITEBACK、EWRITEBACK RESUME或EWRB指令)在處理區塊1678中終止為止。

[0166]圖16C例示用以中斷及回復安全獨立領域中的分頁之過程1608之另一實施例的流程圖。在處理區塊1681中，ELOAD(或ELD)指令在將要自記憶體載入且解密的頁上開始分頁操作之執行。在處理區塊1682中，在頁載入操作中取得正向不中斷進展。在處理區塊1683中，可執行週期性檢查以判定頁載入操作是否已結束，在已結束狀況下，處理繼續進行處理區塊1688，或否則在處理區塊1684中判定是否存在任何迫近中斷。若否，則處理在處理區塊1682中繼續。當存在迫近中斷時，處理繼續進行處理區塊1685，其中為頁載入操作之狀態設置檢查點(例如，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊之部分儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。在處理區塊1686中，返回諮詢碼(例如，指示可服務中斷)。在處理區塊1690中，服務中斷，且在處理區塊1687中，使用所儲存檢查點狀態資訊(例如，對於一實施例在用於對應頁之最後快取列中)在將要自記憶體載入且解密的頁上回復(例如，藉由執行ELOAD RESUME或ELDR指令)頁載入操作。處理隨後反復在處理區塊1682中開始，直至在處理區塊1683中，頁載入操作已結束，且頁載入操作(例如根據執行ELD或ELOAD、

ELOAD RESUME或ELDR指令)在處理區塊1688中終止為止。

[0167]因此，當正加密且寫回安全獨立領域頁快取記憶體內容，且/或自記憶體載入且解密新頁時，可取得正向不中斷進展，且可執行週期性檢查以判定是否存在任何迫近中斷。每當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於快取列中(或儲存於一些其他安全位置中)以回復用於對應對應頁之分頁操作。隨後可服務中斷，且之後可使用所儲存頁狀態資訊回復對應分頁操作。因此，保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務任何迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0168]圖17例示用以提供用於安全獨立領域頁快取記憶體之高級分頁性能之過程1701之一替代性實施例的流程圖。在過程1701之處理區塊1710中，針對共享頁標記項(例如，回應於指定共享頁位址作為運算元的EBLOCK指令)，以阻止任何TLB中的新轉換之創建。在處理區塊1720中，記錄當前存取安全獨立領域中之安全資料的硬體執行緒、邏輯處理器或處理核心(例如，回應於指定安全獨立領域作為運算元的ETRACK指令)。在處理區塊1730中，當任何執行緒退出安全獨立領域(例如，使用EEXIT或AEX指令)時，使所記錄執行緒之數目遞減。在處理區塊1735中，判定執行緒之所記錄數目現是否為零。若否，則處理在處理區塊

1730中繼續，但若執行緒之所記錄數目現為零，則處理繼續進行處理區塊1740。在處理區塊1740中，移除用於共享頁之安全資料，且在處理區塊1750中，加密用於移除共享頁之安全資料(例如，回應於指定共享頁位址作為運算元的EWRITEBACK或EWB指令)。隨後，在處理區塊1760中，將用於移除共享頁之加密安全資料寫回至記憶體或寫回至非依電性儲存器。在處理區塊1770中，將自由儲存器分配給安全獨立領域之新頁。在處理區塊1780中，解密用於新頁之安全資料(例如，回應於指定新共享頁位址作為運算元的ELOAD或ELD指令)。如以上所示，當正加密且寫回安全獨立領域頁內容，且/或正自記憶體載入且解密新頁時，可取得正向不中斷進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於快取列中(或儲存於一些其他安全儲存器中)以回復用於對應頁之分頁操作。隨後可服務中斷，且之後可使用所儲存頁狀態資訊回復對應分頁操作(例如，分別回應於EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指令)。

[0169]圖18A例示用以提供高級分頁性能包括用以中斷及回復安全獨立領域中的分頁之過程1801之另一實施例的流程圖。在過程1801之處理區塊1810中，執行多個硬體執行緒(例如，在多執行緒處理器中)。在處理區塊1808中，將安全資料儲存於用於共享頁之快取記憶體中，該快取記

記憶體分配給可由該等多個執行緒存取的安全獨立領域。在過程 1802 之處理區塊 1830 中，解碼 EBLOCK 指令，EBLOCK 指令在一實施例中指定共享頁位址作為運算元。在處理區塊 1840 中，針對共享頁標記項，以阻止任何 TLB 中的新轉換之創建。在處理區塊 1850 中，記錄當前存取安全獨立領域中之安全資料的硬體執行緒、邏輯處理器或處理核心。在過程 1803 之處理區塊 1860 中，解碼 ETRACK 指令，ETRACK 指令在一實施例中指定安全獨立領域作為運算元。在處理區塊 1870 中，當任何執行緒退出安全獨立領域(例如使用 EEXIT 或 AEX 指令)時，使所記錄執行緒之數目遞減。在處理區塊 1880 中，判定執行緒之所記錄數目現是否為零。若否，則處理在處理區塊 1870 中繼續，但若執行緒之所記錄數目現為零，則處理繼續進行處理區塊 1807。在處理區塊 1807 中，將用於共享頁之安全資料頁出至記憶體或頁出至非依電性儲存器(例如，回應於指定共享頁位址作為運算元的 EWRITEBACK 或 EWB 指令)。

[0170] 藉由用以提供高級分頁性能包括用以中斷及回復安全獨立領域中的分頁之獨立領域指令之使用，可將分頁過程(例如，其中加密且寫回安全獨立領域頁快取記憶體內容，自記憶體載入且解密新頁，清除且替換 TLB 項，等等)分成數個級段，其中處理器核心或邏輯處理器在一或多個級段期間僅短暫地中斷。換 TLB 項，等等)分成數個級段，其中處理器核心或邏輯處理器在一或多個級段期間僅暫時地中斷。因此，可減少歸因於分頁過程的效能降級，同時

保證安全獨立領域資料之安全性且不需要不當的複雜性及設計努力。當正加密且寫回安全獨立領域頁內容，且/或正自記憶體載入且解密新頁時，可保證正向不中斷進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於快取列中(或儲存於一些其他安全儲存器中)以回復用於對應頁之分頁操作。在一些實施例中，頁狀態資訊可包括至少一指標以記錄位置以便在指令之執行部分完成之後回復。隨後可服務中斷，且之後可使用所儲存頁狀態資訊回復對應分頁操作(例如，分別回應於EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指令)。

[0171]圖18B例示用以提供高級分頁性能包括用以中斷及回復安全獨立領域中的分頁之過程1804之另一實施例的流程圖。在過程1804之處理區塊1810中，執行多個硬體執行緒(例如，在多執行緒處理器中)。在處理區塊1808中，將安全資料儲存於用於共享頁之快取記憶體中，該快取記憶體係分配給可由該等多個執行緒存取的安全獨立領域。在過程1805之處理區塊1830中，解碼EBLOCK指令，EBLOCK指令在一實施例中指定共享頁位址作為運算元。在處理區塊1840中，針對共享頁標記項，以阻止任何TLB中的新轉換之創建。在過程1806之處理區塊1860中，解碼ETRACK指令，ETRACK指令在一實施例中指定安全獨立領域作為運算元。在處理區塊1850中，記錄當前存取安全

獨立領域中之安全資料的硬體執行緒、邏輯處理器或處理核心。在處理區塊1870中，當任何執行緒退出安全獨立領域(例如使用EEXIT或AEX指令)時，使所記錄執行緒之數目遞減。在處理區塊1880中，判定執行緒之所記錄數目現是否為零。若否，則處理在處理區塊1870中繼續，但若執行緒之所記錄數目現為零，則處理繼續進行處理區塊1807。在處理區塊1807中，將用於共享頁之安全資料頁出至記憶體或頁出至非依電性儲存器(例如，回應於指定共享頁位址作為運算元的EWRITEBACK或EWB指令)。可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可將頁狀態資訊儲存於快取列中(或儲存於一些其他安全儲存器中)以回復用於對應頁之分頁操作。隨後可服務中斷，且之後可使用所儲存頁狀態資訊回復對應分頁操作(例如，分別回應於EWRITEBACK RESUME或EWBR指令，或ELOAD RESUME或ELDR指令)。

[0172]圖18C例示用以中斷及回復安全獨立領域中的分頁之過程1807之一實例例的流程圖。在處理區塊1817中，解碼EWB(或EWRITEBACK)指令，EWB(或EWRITEBACK)指令在一實施例中指定頁位址作為用於將要加密且寫回的頁之運算元。在處理區塊1827中，關於頁出用於頁之加密資料及執行至記憶體或非依電性儲存器之寫回操作取得正向不中斷進展。在處理區塊1837中，可執行週期性檢查以判定頁出加密資料及執行寫回操作是否已

結束，在已結束狀態下，處理繼續進行處理區塊1887，或否則在處理區塊1847中判定是否存在任何迫近中斷。若否，則處理在處理區塊1827中繼續。當存在迫近中斷時，處理繼續進行處理區塊1857，其中在獨立領域頁快取記憶體映射項中設定分頁操作之部分完成之指示，且在處理區塊1867中，將頁狀態資訊之部分記錄於用於對應頁位址之第一快取列中。在一些實施例中，可返回諮詢碼(例如，指示可服務中斷)。在處理區塊1890中，服務中斷，且在處理區塊1877中，解碼EWBR(或EWRITEBACK RESUME)指令，EWBR(或EWRITEBACK RESUME)指令在一實施例中指定頁位址作為用於頁之運算元，該頁將用以使用頁狀態資訊之所記錄部分(例如，在用於對應頁之第一快取列中)回復被加密及寫回。處理隨後反復在處理區塊1827中開始，直至在處理區塊1837中，頁出加密資料及執行寫回操作已結束，且頁出加密資料及執行寫回至記憶體或非依電性儲存器(例如根據執行EWB或EWRITEBACK、EWRITEBACK RESUME或EWBR指令)在處理區塊1887中終止為止。

[0173]圖18D例示用以中斷及回復安全獨立領域中的分頁之過程1808之另一實施例的流程圖。在處理區塊1818中，解碼ELOAD(或ELD)指令，ELOAD(或ELD)指令在一實施例中指定頁位址作為用於分配給安全獨立領域的頁之運算元，將載入用於該頁之安全資料。在處理區塊1828中，關於載入用於分配給安全獨立領域的頁之安全資料取得正

向不中斷進展。在處理區塊1838中，可執行週期性檢查以判定用於分配給安全獨立領域的頁之安全資料之載入是否已結束，在已結束狀況下，處理繼續進行處理區塊1888，或否則在處理區塊1848中判定是否存在任何迫近中斷。若否，則處理在處理區塊1828中繼續。當存在迫近中斷時，處理繼續進行處理區塊1858，其中在獨立領域頁快取記憶體映射項中設定分頁操作之部分完成之指示，且在處理區塊1868中，將頁狀態資訊之部分記錄於用於對應頁位址之最後快取列中。在一些實施例中，可返回諮詢碼(例如，指示可服務中斷)。在處理區塊1890中，服務中斷，且在處理區塊1878中，解碼ELDR(或ELOAD RESUME)指令，ELDR(或ELOAD RESUME)指令在一實施例中指定頁位址用作用於頁之運算元，該將用以使用頁狀態資訊之所記錄部分(例如，在用於對應頁之中)回復用於分配給安全獨立領域的頁之安全資料之載入。處理隨後反復在處理區塊1828中開始，直至在處理區塊1838中，用於分配給安全獨立領域的頁之安全資料之載入已結束，且用於分配給安全獨立領域的頁之安全資料之載入(例如，根據執行ELD或ELOAD、ELOAD RESUME或ELDR指令)在處理區塊1888中終止為止。

[0174]因此，管理許可、實體記憶體及/或改變映射仍可由OS管理，但OS對於存取獨立領域私用記憶體之實際受保護內容不被容許或信賴。可使用用以中斷及回復安全獨立領域中的分頁之指令及處理邏輯來以分級方式實現保證

專用記憶體內容之安全性及/或完整性及管理使用有限量的實體記憶體來支援較大、受保護、獨立領域私用記憶體空間之技術約束，而不需要精心硬體支援及/或設計努力。另外，當正加密且寫回安全獨立領域頁快取記憶體內容，且/或正自記憶體載入且解密新頁時，取得正向進展，且可執行週期性檢查以判定是否存在任何迫近中斷。當存在迫近中斷時，可將分頁操作之部分完成記錄於獨立領域頁快取記憶體映射項中，且可儲存頁狀態資訊(例如，儲存於用於對應頁之快取列中，或儲存於一些其他安全儲存器中)。隨後可服務中斷，且之後可回復對應分頁操作。因此，保證載入及/或移除用於安全獨立領域之記憶體頁之正向進展，且可藉由及時服務任何迫近中斷避免諸如語音、視訊及即時交易的服務中之不受歡迎的假信號。

[0175]將瞭解，在過程1804之一些替代性實施例中及在本文中所揭示之其他過程中，若可能，則例示為以特定次序執行的處理區塊亦可以另一次序或並行地或彼此平行地執行。

[0176]本文中所揭示之機構的實施例可以硬體、軟體、韌體或者此類實行方法之組合來實行。本發明之實施例可實行為在可規劃系統上執行之電腦程式或程式碼，該等可規劃系統包含至少一處理器、一儲存系統(包括依電性及非依電性記憶體及/或儲存元件)、至少一輸入裝置及至少一輸出裝置。

[0177]可將程式碼應用於輸入指令，用來執行本文中所

描述之功能且產生輸出資訊。可將輸出資訊以已知方式應用於一或多個輸出裝置。出於本申請案之目的，處理系統包括具有處理器之任何系統，該處理器諸如數位信號處理器(DSP)、微控制器、特殊應用積體電路(ASIC)或微處理器。

[0178]程式碼可以高階程序性或物件導向式程式設計語言來實行，以便與處理系統通訊。必要時，程式碼亦可以組合語言或機器語言來實行。事實上，本文中所描述之機構的範疇不限於任何特定的程式設計語言。在任何狀況下，該語言可為編譯語言或解譯語言。

[0179]至少一實施例之一或多個態樣可藉由儲存於機器可讀媒體上之代表性指令來實行，該等指令表示處理器內的各種邏輯，該等指令在由機器讀取時使機器製造邏輯來執行本文中所描述之技術。此類表示(「稱為IP核心」)可儲存於有形的機器可讀媒體上，且可供應給各種用戶端或製造設施以載入至實際上製造該邏輯或處理器的製造機中。

[0180]此等機器可讀儲存媒體可包括但不限於由機器或裝置製造或形成的非暫時性有形物品佈置，其中包括：儲存媒體，諸如硬碟、任何其他類型之碟片(包括軟碟片、光碟、光碟片-唯讀記憶體(CD-ROM)、可重寫光碟片(CD-RW)及磁光碟)、半導體裝置(諸如唯讀記憶體(ROM)、隨機存取記憶體(RAM)(諸如動態隨機存取記憶體(DRAM)、靜態隨機存取記憶體(SRAM))、可抹除可規劃唯讀記憶體(EPROM)、快閃記憶體、電氣可抹除可規劃唯讀

記憶體(EEPROM)、磁性或光學卡)，或者適合於儲存電子指令的任何其他類型之媒體。

[0181]因此，本發明之實施例亦包括含有指令或含有諸如硬體描述語言(HDL)之設計資料的非暫時性有形機器可讀媒體，其中設計資料定義本文中所描述之結構、電路、設備、處理器及/或系統特徵。此類實施例亦可被稱為程式產品。

[0182]在一些狀況下，可使用指令轉換器將指令自來源指令集轉換成目標指令集。例如，指令轉換器可將指令轉譯(例如，使用靜態二進位轉譯、包括動態編譯之動態二進位轉譯)、漸變、仿真或以其他方式轉換成將由核心處理的一或多個其他指令。指令轉換器可以軟體、硬體、韌體或其組合來實行。指令轉換器可位於處理器上、位於處理器外部，或部分位於處理器上而部分位於處理器外部。

[0183]因此，揭示了用於執行根據至少一實施例之一或多個指令的技術。雖然已經在隨附圖式中描述並展示某些示範性實施例，但應理解，此類實施例僅例示且不限制廣泛的本發明，且本發明不限於所展示並描述之特定構造及佈置，因為一般技藝者在學習本揭示內容後可想到各種其他修改。在成長速度快且不容易預見到進一步進步之技術(諸如此項技術)領域中，在不背離本揭示內容之原理或隨附申請專利範圍之範疇的情況下，所揭示實施例可易於在配置及細節方面作出修改，如藉由允許技術進步所促成。

【符號說明】

- 100...系統/電腦系統
- 102...處理器/通用處理器
- 104...1階(L1)內部快取記憶體
- 106、145、164...暫存器檔案
- 108、142、162、462、1426、1436、1526...執行單元
- 109、143...緊縮指令集
- 110...處理器匯流排
- 112...圖形控制器/圖形卡
- 114...加速圖形埠(AGP)互連
- 116...系統邏輯晶片/MCH
- 118...高頻寬記憶體路徑/記憶體介面
- 120、640、732、734、832、834、1140...記憶體
- 122...系統I/O/專屬集線器介面匯流排
- 124...資料儲存器/資料儲存裝置
- 126...無線收發器
- 128...韌體集線器(快閃BIOS)
- 130...I/O控制器集線器(ICH)
- 134...網路控制器
- 140...資料處理系統/電腦系統
- 141...匯流排
- 144、165、165B、228...解碼器
- 146...同步動態隨機存取記憶體(SDRAM)控制
- 147...靜態隨機存取記憶體(SRAM)控制
- 148...高載快閃記憶體介面

- 149...個人電腦記憶卡國際協會(PCMCIA)/緊密快閃(CF)卡控制
- 150...液晶顯示器(LCD)控制
- 151...直接記憶體存取(DMA)控制器
- 152...替代性匯流排主控介面
- 153...I/O匯流排
- 154...I/O橋接器
- 155...通用非同步接收器/發射器(UART)
- 156...通用串列匯流排(USB)
- 157...藍牙無線UART
- 158...I/O擴展介面
- 159、170...處理核心
- 160...資料處理系統
- 161...SIMD共處理器
- 163...指令集
- 166...主處理器
- 167...快取記憶體
- 168...輸入/輸出系統
- 169...無線介面
- 171...共處理器匯流排
- 200、500、870、880、1000、1215、1402...處理器
- 201...循序前端
- 202...快速排程器/微操作排程器/排程器
- 203...亂序執行引擎
- 204...緩慢/一般浮點排程器/微操作排程器/排程器

- 206...簡單浮點排程器/微操作排程器/排程器
- 208...暫存器檔案/整數暫存器檔案
- 210...暫存器檔案/浮點暫存器檔案
- 211...執行區塊
- 212...執行單元/位址產生單元(AGU)
- 214...執行單元/AGU
- 216、218...執行單元/快速ALU/高速ALU執行單元
- 220...執行單元/緩慢ALU
- 222...執行單元/浮點ALU/浮點單元
- 224...執行單元/浮點移動單元/浮點單元
- 226...指令預擷取器
- 230...追蹤快取記憶體
- 232...微碼ROM
- 234...微操作佇列
- 310...緊縮位元組/緊縮位元組格式
- 320...緊縮字
- 330...緊縮雙字/緊縮雙字格式
- 341...緊縮半字
- 342...緊縮單字
- 343...緊縮雙字
- 344...不帶正負號的緊縮位元組表示
- 345...帶正負號的位元組表示
- 346...不帶正負號的緊縮字表示/不帶正負號的緊縮字暫存器中表示
- 347...帶正負號的緊縮字表示

348...不帶正負號的緊縮雙字表示/不帶正負號的緊縮雙字暫存器中表示

349...帶正負號的緊縮雙字表示

360、370...操作編碼(運算碼)格式/運算碼格式/格式

361、362、371、372、383、384、387、388、392...欄位

363、373...MOD欄位

364、365、374、375...來源運算元識別符/識別符/運算元識別符

366、376、386...目的地運算元識別符

378...前綴位元組/欄位

380...操作編碼(運算碼)格式

381...條件欄位

382、389...CDP運算碼欄位

385、390...來源運算元識別符

391...可選擇的VEX前綴位元組/欄位

393...可選擇的比例-索引-基址(SIB)識別符

394...可選擇的位移識別符

395...可選擇的立即位元組

396...可選擇的EVEX前綴位元組/欄位

397...運算碼格式

398...操作編碼(運算碼)格式/EVEX格式

400...處理器管線

402...擷取級段

404...長度解碼級段

406、1422、1432、1522...解碼級段

408...分配級段

- 410...重新命名級段
- 412...排程級段
- 414...暫存器讀取/記憶體讀取級段
- 416...執行級段
- 418...寫回/記憶體寫入級段
- 422...異常處置級段
- 424...確認級段
- 430...前端單元
- 432...分支預測單元
- 434...指令快取記憶體單元
- 436...指令轉譯後備緩衝器(TLB)
- 438...指令擷取單元
- 440...解碼單元
- 450...執行引擎單元
- 452...重新命名/分配器單元
- 454...引退(retirement)單元
- 456...排程器單元
- 458...實體暫存器檔案單元
- 460...執行聚集
- 464...記憶體存取單元
- 470...記憶體單元
- 472...資料TLB單元
- 474資料快取記憶體單元
- 476...2階(L2)快取記憶體單元

490...處理器核心/核心
 502A～502N...核心
 504A～504N...快取記憶體單元
 506...共享快取記憶體單元
 508...整合型圖形邏輯
 510...系統代理
 512...環式互連單元
 514...整合型記憶體控制器單元
 516...匯流排控制器單元
 600...系統
 610、615...處理器/實體資源
 620...圖形記憶體控制器集線器(GMCH)
 645...顯示器
 650...輸入/輸出(I/O)控制器集線器(ICH)
 660...外部圖形裝置
 670...周邊裝置
 695...前端匯流排(FSB)
 700...第二系統/多處理器系統
 714...I/O裝置
 716...第一匯流排
 718...匯流排橋接器
 720...第二匯流排
 722...鍵盤及/或滑鼠
 724...音訊I/O

727...通訊裝置

728...儲存單元

730...指令/碼及資料

738...高效能圖形電路

739...高效能介面

750...點對點互連/點對點(P-P)介面

752、754...P-P介面

770...第一處理器/處理器

772、782...整合型記憶體控制器單元/IMC

776、778、786、788...點對點(P-P)介面/點對點介面電路

780...第二處理器/處理器

790、890...晶片組

794、798...點對點介面電路

796...介面

800...第三系統

814...I/O裝置

815...舊式I/O裝置

872、882...I/O控制邏輯(「CL」)

900...SoC

902...互連單元

910...應用處理器

920...媒體處理器

924、1015...影像處理器

926...音訊處理器

- 928、1020...視訊處理器
- 930...靜態隨機存取記憶體(SRAM)單元
- 932...直接記憶體存取(DMA)單元
- 940...顯示單元
- 1005...CPU
- 1010...GPU
- 1025...USB控制器
- 1030...UART控制器
- 1035...SPI/SDIO控制器
- 1040...顯示裝置
- 1045...高清晰度多媒體介面(HDMI)控制器
- 1050...MIPI控制器
- 1055...快閃記憶體控制器
- 1060...雙資料速率(DDR)控制器
- 1065...安全引擎
- 1070...I2S/I2C(整合型晶片間聲音/內部整合電路)介面
- 1110...硬體或軟體模型
- 1120...模擬軟體
- 1130...儲存器
- 1150...有線連接
- 1160...無線連接
- 1165...製造設施
- 1205...程式
- 1210...仿真邏輯

1302...高階語言

1304...x86編譯器

1306...x86二進位碼

1308...替代性指令集編譯器

1310...替代性指令集二進位碼

1312...指令轉換器

1314...不具有至少一x86指令集核心之處理器

1316...具有至少一x86指令集核心之處理器

1401...處理系統/系統

1410...頁

1420...第一硬體執行緒或邏輯處理器

1424、1434、1524...讀取級段

1425、1435、1525...TLB

1428、1438、1528...寫入級段

1430...第二硬體執行緒或邏輯處理器

1440、1450...1階快取記憶體/快取記憶體

1442、1444、1456、1542...共享頁

1460、1520...獨立領域頁快取記憶體/EPC

1470、1427、1437、1502...安全獨立領域(SE)單元

1490...系統記憶體

1495...編碼後頁

1501...處理器/處理器核心

1503...獨立領域指令

1510...加密單元

- 1512...完整性保護單元
- 1514...存取控制單元
- 1516...範圍暫存器
- 1517...先前時期/PE
- 1518...獨立領域頁快取記憶體映射/EPCM
- 1519...當前時期/CE
- 1531...EBLOCK指令
- 1532...ETRACK指令
- 1533...EWB指令
- 1534...ELOAD指令
- 1535...EEXIT指令
- 1536...EENTER指令
- 1537...EWBR(或EWRITEBACK...RESUME)指令
- 1538...ELOADR(或ELOAD...RESUME或ELDR)指令
- 1540...1階快取記憶體/L1
- 1601、1607、1608、1701、1801~1806...過程
- 1807、1808...處理區塊/過程
- 1610~1680、1625、1665、1671~1678、1690、1681~1688、1710
~1780、1735、1810、1830~1890、1817~1887、1818~
1888...處理區塊

申請專利範圍

1. 一種處理器，其包含：

一獨立領域頁快取記憶體，在該獨立領域頁快取記憶體中用以將安全資料儲存於用於分配給一對應安全獨立領域的一頁位址之一安全儲存器中；

一解碼器，其用以將用於執行之一指令解碼為一經解碼指令，該指令指定該頁位址作為一運算元；以及

一執行單元，其操作地耦接至該獨立領域頁快取記憶體及至該解碼器，其中該執行單元係用以回應於該經解碼指令而：

回應於偵測該指令之一迫近中斷，而設定對應於用於該頁位址之一獨立領域頁快取記憶體映射之一項目，以指示該指令的執行之一部分完成，且

回應於偵測該指令之該迫近中斷，而將一頁狀態部分記錄於用於對應於該頁位址的一頁之該安全儲存器中。

2. 如請求項1之處理器，其中該頁狀態部分包括一指標以記錄該對應頁之一位置，在該位置以在該指令的執行之該部分完成之後，回復執行。

3. 如請求項2之處理器，其中對應於用於該頁位址之該獨立領域頁快取記憶體映射的該項目經設定，以指示該對應頁之一部分載入完成。

4. 如請求項3之處理器，其中該頁狀態部分記錄於用於該

對應頁之一最後快取列中。

5. 如請求項4之處理器，其中該指令為一ELOAD(ELD)指令，該ELD指令指定該頁位址，在該頁位址以將該對應頁載入至該獨立領域頁快取記憶體中。
6. 如請求項4之處理器，其中該指令為一ELOAD RESUME(ELDR)指令，該ELDR指令指定該頁位址，在該頁位址以回復將該對應頁載入至該獨立領域頁快取記憶體中。
7. 如請求項2之處理器，其中對應於用於該頁位址之一獨立領域頁快取記憶體映射之該項目經設定以指示該對應頁之一部分寫回完成。
8. 如請求項7之處理器，其中該頁狀態部分係記錄於用於該頁位址之一第一快取列中。
9. 如請求項8之處理器，其中該指令為一EWRITEBACK(EWB)指令，該EWB指令指定該頁位址，在該頁位址以將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。
10. 如請求項8之處理器，其中該指令為一EWRITEBACK RESUME(EWBR)指令，該EWBR指令指定該頁位址，在該頁位址以回復將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。
11. 如請求項1之處理器，其中回應於經解碼之該指令，該執行單元係進一步用以當對應於用於該頁位址之該獨立領域頁快取記憶體映射的該項目指示用於一部分頁

之安全資料係儲存於該安全儲存器中時，自用於對應於該頁位址的該頁之該安全儲存器讀取該頁狀態部分。

12. 如請求項11之處理器，其中回應於經解碼之該指令，該執行單元係進一步用以檢查對應於用於該頁位址之該獨立領域頁快取記憶體映射的該項目，以判定用於一部分頁之安全資料是否儲存於該獨立領域頁快取記憶體中。

13. 一種機器可讀媒體，其儲存一處理器可存取的指令，該等指令包括在由該處理器讀取時使該處理器執行程序之指令，該等程序包含：

解碼用於由該處理器執行之該指令，該指令指定分配給一對應安全獨立領域的一頁位址作為一運算元；

存取一獨立領域頁快取記憶體，該獨立領域頁快取記憶體用以將安全資料儲存於用於該頁位址之一第一快取列中，且儲存於用於對應於該頁位址的一頁之一最後快取列中；以及

當對應於用於該頁位址之一獨立領域頁快取記憶體映射的一項目指示用於一部分頁之安全資料係儲存於該獨立領域頁快取記憶體中時，自用於該頁位址之該第一快取列或自用於對應於該頁位址的該頁之該最後快取列讀取一頁狀態部分。

14. 如請求項13之機器可讀媒體，其中該指令在由該處理器讀取時進一步使該處理器執行程序，該等程序包含：

檢查對應於用於該頁位址之該獨立領域頁快取記

憶體映射的該項目，以判定用於一部分頁之安全資料是否儲存於該獨立領域頁快取記憶體中。

15. 如請求項13之機器可讀媒體，其中該頁狀態部分包括一指標以記錄一位置以便回復該指令的執行。
16. 如請求項15之機器可讀媒體，其中對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目經設定以指示該對應頁之一部分載入完成。
17. 如請求項16之機器可讀媒體，其中該頁狀態部分係記錄於用於該對應頁之該最後快取列中。
18. 如請求項17之機器可讀媒體，其中該指令為一ELOAD(ELD)指令，該ELD指令指定該頁位址，在該頁位址以將該對應頁載入至該獨立領域頁快取記憶體中。
19. 如請求項17之機器可讀媒體，其中該指令為一ELOAD RESUME(ELDR)指令，該ELDR指令指定該頁位址，在該頁位址以回復將該對應頁載入至該獨立領域頁快取記憶體中。
20. 如請求項15之機器可讀媒體，其中對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目經設定以指示該對應頁之一部分寫回完成。
21. 如請求項20之機器可讀媒體，其中該頁狀態部分係記錄於用於該頁位址之該第一快取列中。
22. 如請求項21之機器可讀媒體，其中該指令為一EWRITEBACK(EWB)指令，該EWB指令指定該頁位址，在該頁位址以將該對應頁自該獨立領域頁快取記憶

體寫回至外部記憶體。

23. 如請求項 21 之機器可讀媒體，其中該指令為一 EWRITEBACK RESUME(EWBR)指令，該EWBR指令指定該頁位址，在該頁位址以回復將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。

24. 如請求項 13 之機器可讀媒體，其中該指令在由該處理器讀取時進一步使該處理器執行程序，該等程序包含回應於偵測該指令之一迫近中斷，而將一新頁狀態部分記錄於用於該頁位址之該第一快取列中或記錄於用於對應於該頁位址的該頁之該最後快取列中。

25. 如請求項 24 之機器可讀媒體，其中該指令在由該處理器讀取時進一步使該處理器執行程序，該等程序包含回應於偵測該指令之該迫近中斷，而設定對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目，以指示該指令的執行之一部分完成。

26. 一種方法，其包含：

解碼用於由一處理器執行之一指令，該指令指定分配給一對應安全獨立領域的一頁位址作為一運算元；

存取一獨立領域頁快取記憶體，該獨立領域頁快取記憶體用以將安全資料儲存於用於該頁位址之一第一快取列中，且儲存於用於對應於該頁位址的一頁之一最後快取列中；以及

當對應於用於該頁位址之一獨立領域頁快取記憶體映射的一項目指示用於一部分頁之安全資料係儲存

於該獨立領域頁快取記憶體中時，自用於該頁位址之該第一快取列或自用於對應於該頁位址的該頁之該最後快取列讀取一第一頁狀態部分；

回應於偵測該指令之一迫近中斷，而設定對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目，以指示該指令的執行之一部分完成，以及

回應於偵測該指令之該迫近中斷，而將一第二頁狀態部分記錄於用於該頁位址之該第一快取列中或記錄於用於對應於該頁位址的該頁之該最後快取列中。

27. 如請求項26之方法，其中該第一頁狀態部分包括一指標以記錄該對應頁之一位置，在該位置以在該指令的執行之該部分完成之後，回復執行。
28. 如請求項27之方法，其進一步包含設定對應於用於該頁位址之該獨立領域頁快取記憶體映射的該項目以指示該對應頁之一部分載入完成。
29. 如請求項28之方法，其進一步包含將第二頁狀態部分記錄於用於該對應頁之該最後快取列中。
30. 如請求項29之方法，其中該指令為一 ELOAD RESUME(ELDR)指令，該ELDR指令指定該頁位址，在該頁位址以回復將該對應頁載入至該獨立領域頁快取記憶體中。
31. 如請求項27之方法，其進一步包含設定對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目，以指示該對應頁之一部分寫回完成。

32. 如請求項31之方法，其中該第二頁狀態部分係記錄於用於該頁位址之該第一快取列中。

33. 如請求項32之方法，其中該指令為一EWRITEBACK RESUME(EWBR)指令，該EWBR指令指定該頁位址，在該頁位址以回復將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。

34. 一種處理系統，其包含：

一外部記憶體；以及

一處理器，其包含：

一獨立領域頁快取記憶體，在該獨立領域頁快取記憶體中用以將安全資料儲存於用於分配給一對應安全獨立領域的一頁位址之一安全儲存位置中；

一解碼器，其用以將用於由該處理器執行之一第一指令解碼成為一經解碼指令，該第一指令指定該頁位址作為一運算元，且該解碼器用以解碼用於由該處理器執行之一第二指令，該第二指令指定該頁位址作為一運算元；以及

一執行單元，其操作地耦接至該獨立領域頁快取記憶體及該解碼器，該執行單元用以回應於解碼後之該第一指令而：

回應於偵測該第一指令之一迫近中斷，而設定對應於用於該頁位址之一獨立領域頁快取記憶體映射之一項目，以指示該第一指

令的執行之一部分完成，且

回應於偵測該第一指令之該迫近中斷，
而將一第一頁狀態部分記錄於用於對應於該
頁位址的該頁之該安全儲存位置中；

其中該執行單元回應於經解碼之該第二指
令，係進一步用以當對應於用於該頁位址之一獨立
領域頁快取記憶體映射的該項目指示用於該對應
頁的一部分頁之安全資料係儲存於該獨立領域頁
快取記憶體中時，自用於對應於該頁位址的該頁之
該安全儲存位置讀取該第一頁狀態部分。

35. 如請求項34之處理系統，其中該執行單元回應於經解碼
之該第二指令，係進一步用以：

回應於偵測該第二指令之一迫近中斷，而設定對應
於用於該頁位址之該獨立領域頁快取記憶體映射的該
項目，以指示該第二指令的執行之一部分完成，以及

回應於偵測該第二指令之該迫近中斷，而將一第二
頁狀態部分記錄於用於對應於該頁位址的該頁之該安
全儲存位置中。

36. 如請求項34之處理系統，其中該第一頁狀態部分包括一
指標以記錄該對應頁之一位置，在該位置以在該第一指
令之該部分完成之後回復執行。

37. 如請求項36之處理系統，其中該第一頁狀態部分係記錄
於用於該對應頁之一最後快取列中。

38. 如請求項37之處理系統，其中該第二指令為一獨立領域

載入回復指令，該獨立領域載入回復指令指定該頁位址，在該頁位址以回復將該對應頁載入至該獨立領域頁快取記憶體中。

39. 如請求項38之處理系統，其中該第一指令為一獨立領域載入指令，該獨立領域載入指令指定該頁位址以將該對應頁載入至該獨立領域頁快取記憶體中。

40. 如請求項36之處理系統，其中該第一頁狀態部分係記錄於用於該頁位址之一第一快取列中。

41. 如請求項40之處理系統，其中該第二指令為一獨立領域寫回回復指令，該獨立領域寫回回復指令指定該頁位址，在該頁位址以回復將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。

42. 如請求項41之處理系統，其中該第一指令為一獨立領域寫回指令，該獨立領域寫回指令指定該頁位址，在該頁位址以將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。

43. 一種機器可讀媒體，其儲存一處理器可存取的指令，該等指令在由該處理器讀取時使該處理器執行程序，該等程序包含：

將安全資料儲存於用於分配給一對應安全獨立領域的一頁位址之一安全儲存位置中；

回應於偵測一分頁操作之一中斷，而設定對應於用於該頁位址之一獨立領域頁快取記憶體映射的一項目，以指示該分頁操作之一部分完成，以及

回應於偵測該分頁操作之執行的一中斷，將一頁狀態部分記錄於用於對應於該頁位址的一頁之該安全儲存位置中。

44. 如請求項43之機器可讀媒體，其中該頁狀態部分包括一指標以記錄一位置，在該位置以在該分頁操作之該部分完成之後回復。
45. 如請求項44之機器可讀媒體，其中該指令進一步致使該處理器用以進行設定對應於用於該頁位址之一獨立領域頁快取記憶體映射的該項目，以指示該對應頁之一部分載入完成。
46. 如請求項45之機器可讀媒體，其中該指令進一步致使該處理器用以進行將該頁狀態部分記錄於用於該對應頁之一最後快取列中。
47. 如請求項46之機器可讀媒體，其中該分頁操作為一獨立領域載入操作，該獨立領域載入操作指定該頁位址以將該對應頁載入至該獨立領域頁快取記憶體中。
48. 如請求項46之機器可讀媒體，其中該分頁操作為一獨立領域載入回復操作，該獨立領域載入回復操作指定該頁位址，在該頁位址以回復將該對應頁載入至該獨立領域頁快取記憶體中。
49. 如請求項44之機器可讀媒體，其中該指令進一步致使該處理器用以進行設定對應於用於該頁位址之該獨立領域頁快取記憶體映射的該項目以指示該對應頁之一部分寫回完成。

50. 如請求項49之機器可讀媒體，其中該頁狀態部分記錄於用於該頁位址之一第一快取列中。
51. 如請求項50之機器可讀媒體，其中該分頁操作為一獨立領域寫回操作，該獨立領域寫回操作指定該頁位址，在該頁位址以將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。
52. 如請求項50之機器可讀媒體，其中該分頁操作為一獨立領域寫回回復操作，該獨立領域寫回回復操作指定該頁位址，在該頁位址以回復將該對應頁自該獨立領域頁快取記憶體寫回至外部記憶體。

圖式

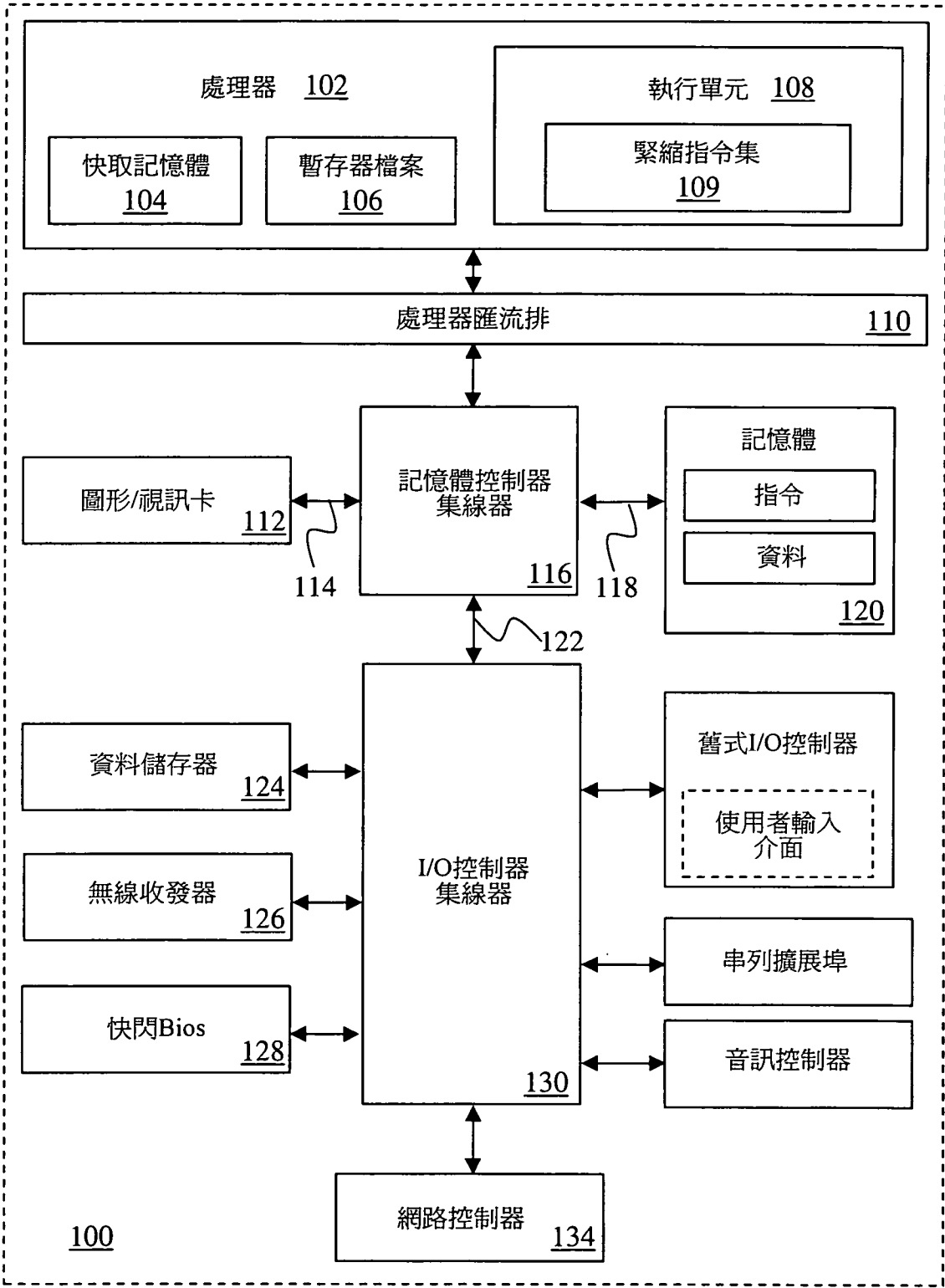


圖 1A

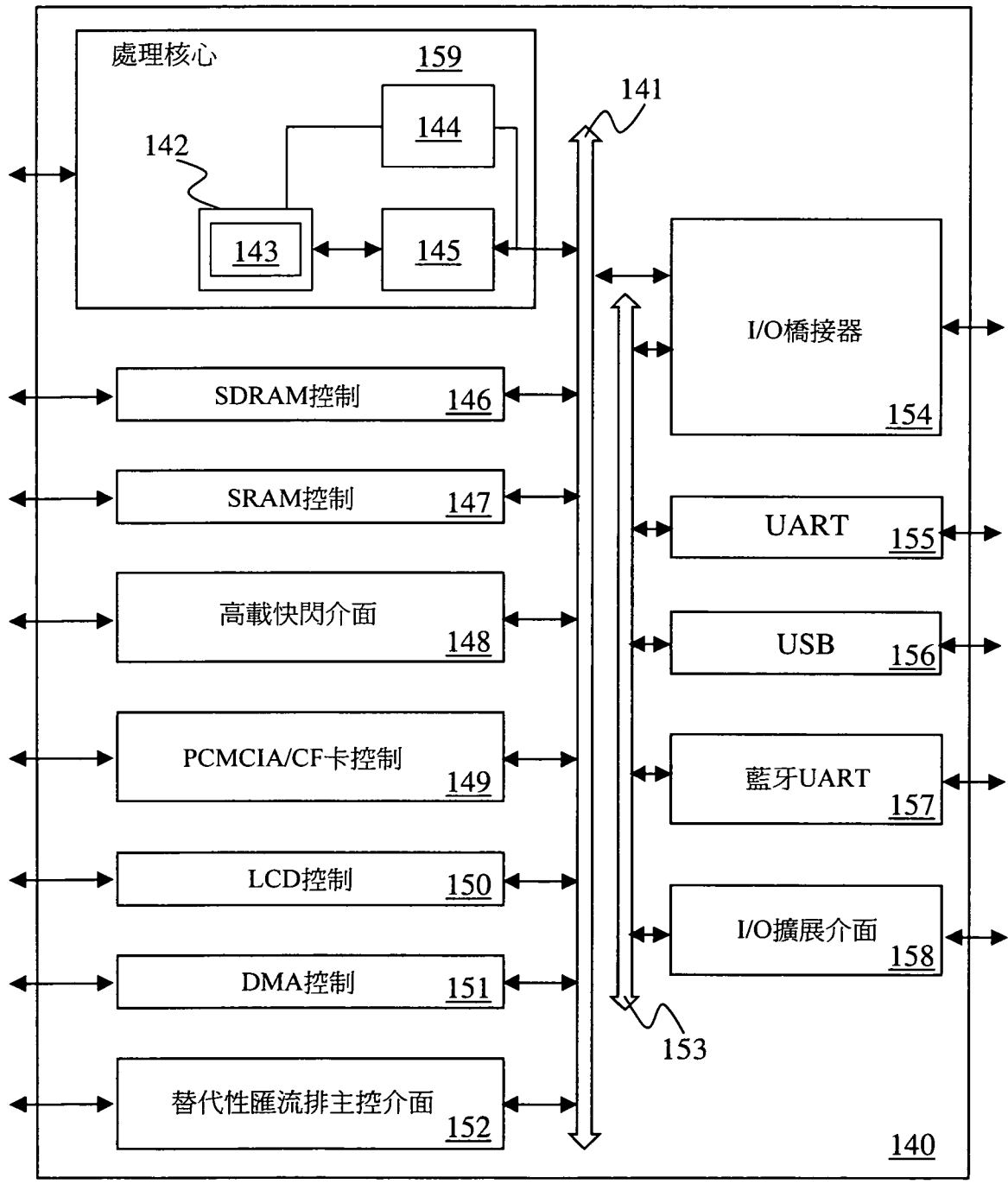


圖 1B

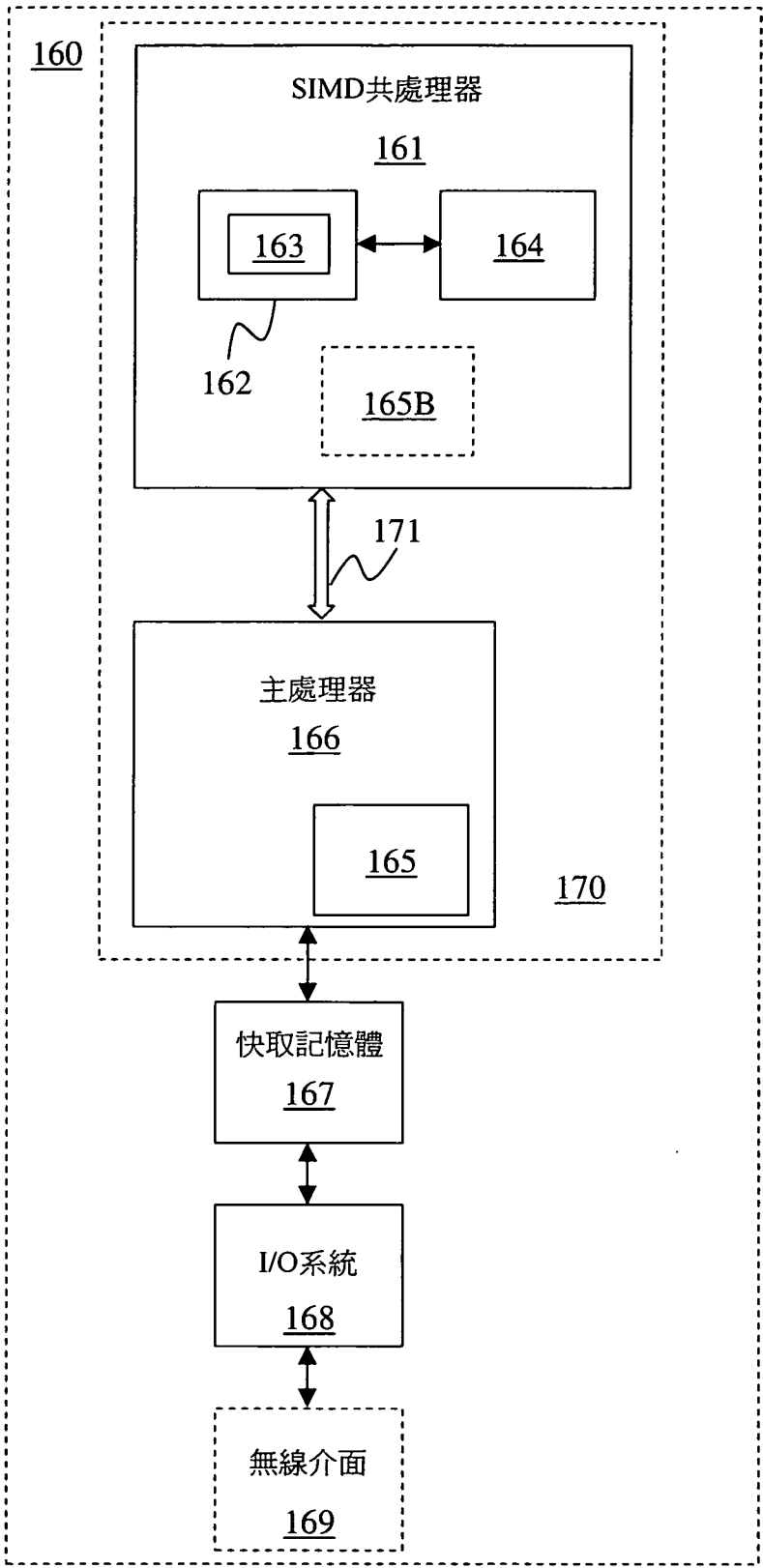


圖 1C

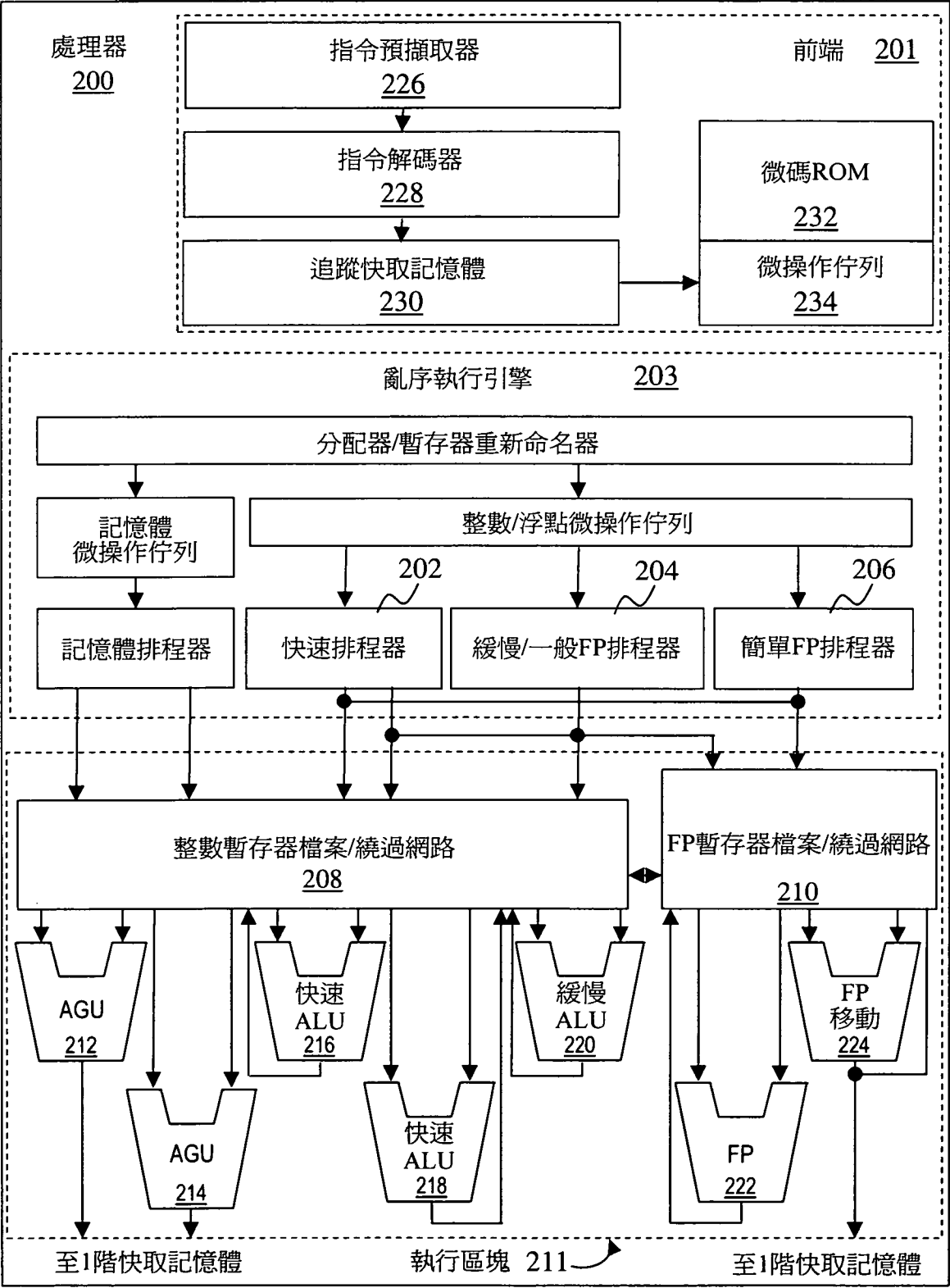
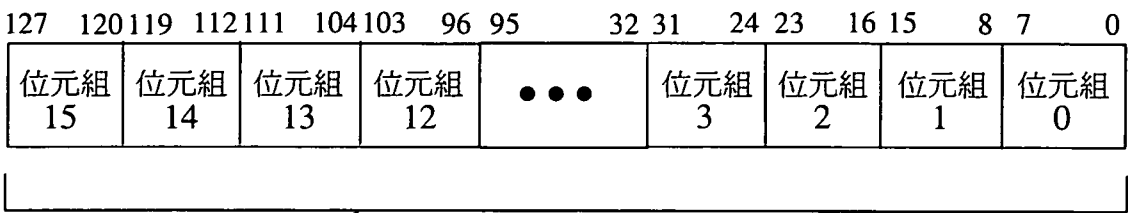
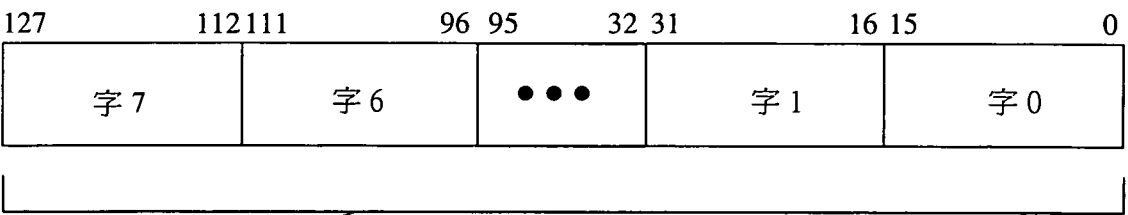


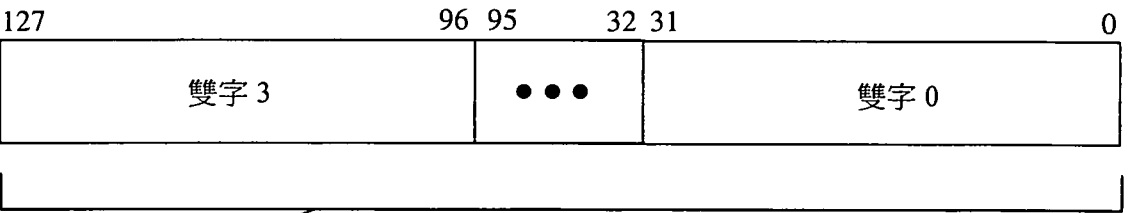
圖 2



310 緊縮位元組



320 緊縮字



330 緊縮雙字

圖 3A

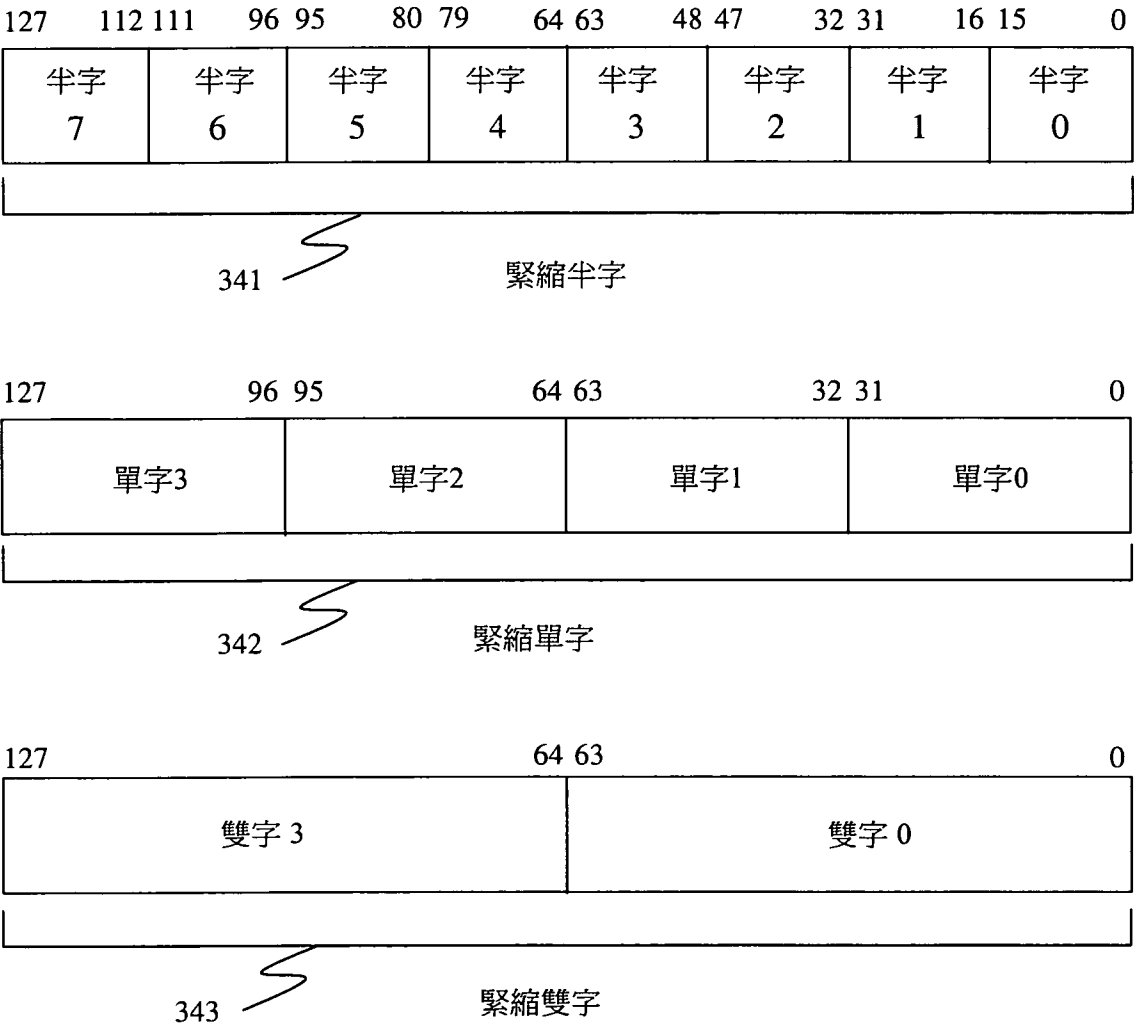
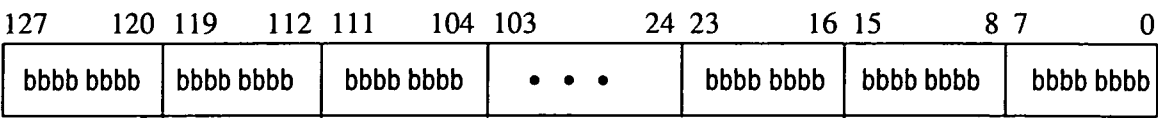
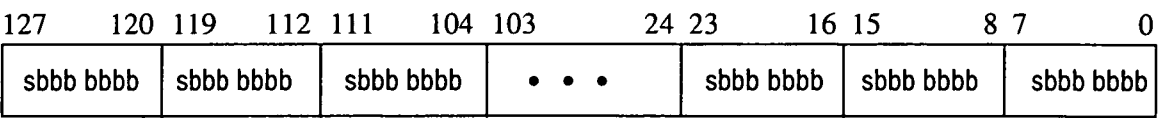


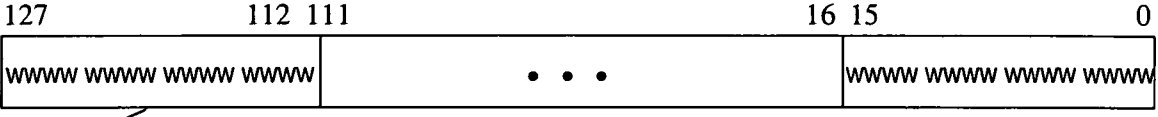
圖 3B



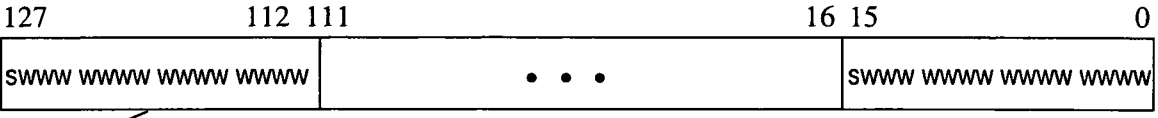
344 不帶正負號的緊縮位元組表示



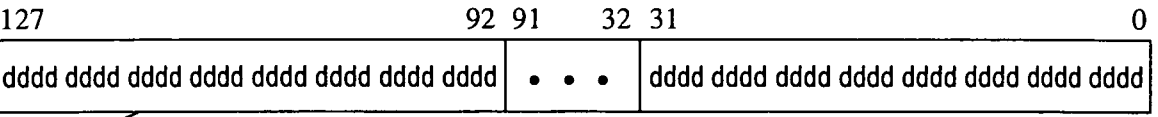
345 帶正負號的位元組表示



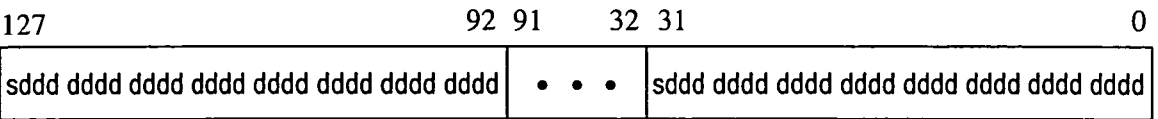
346 不帶正負號的緊縮字表示



347 帶正負號的緊縮字表示



348 不帶正負號的緊縮雙字表示



349 帶正負號的緊縮雙字表示

圖 3C

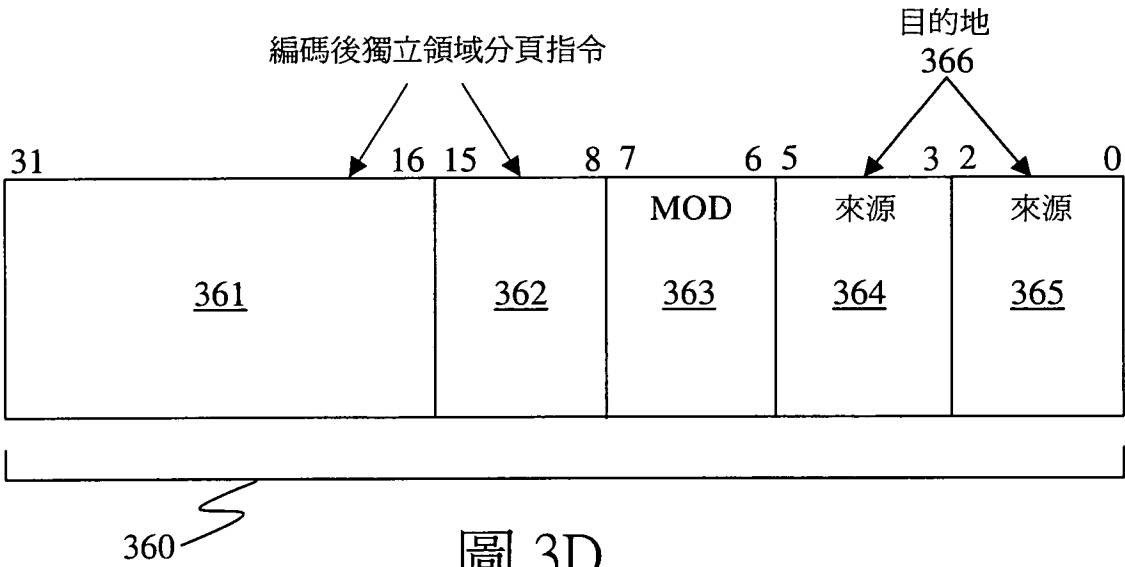


圖 3D

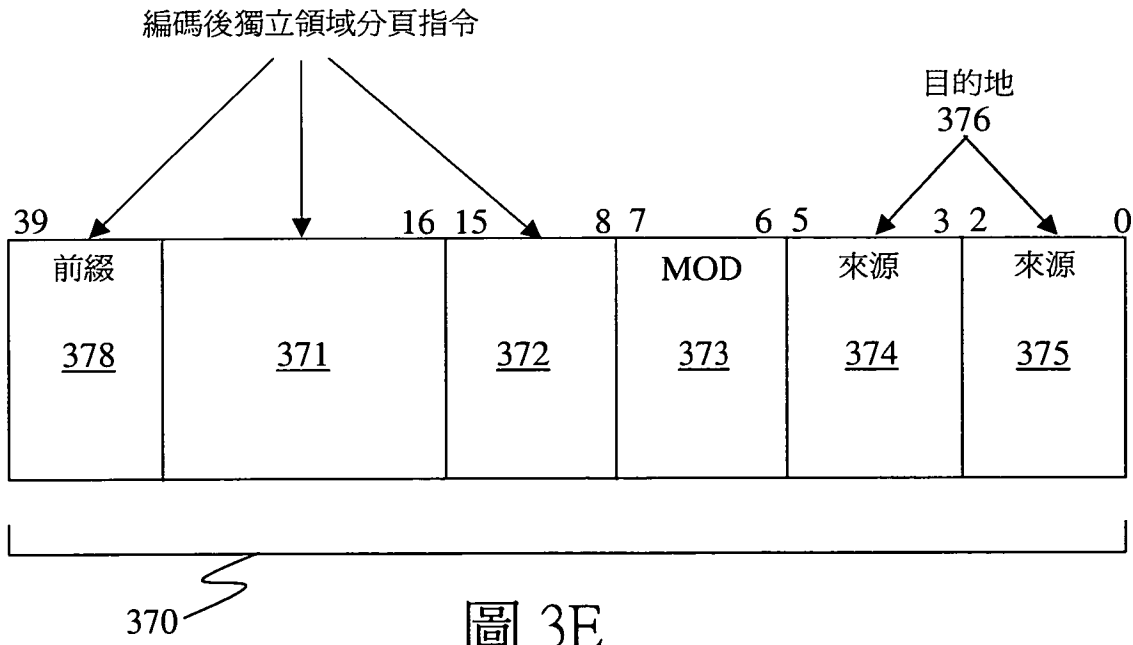


圖 3E

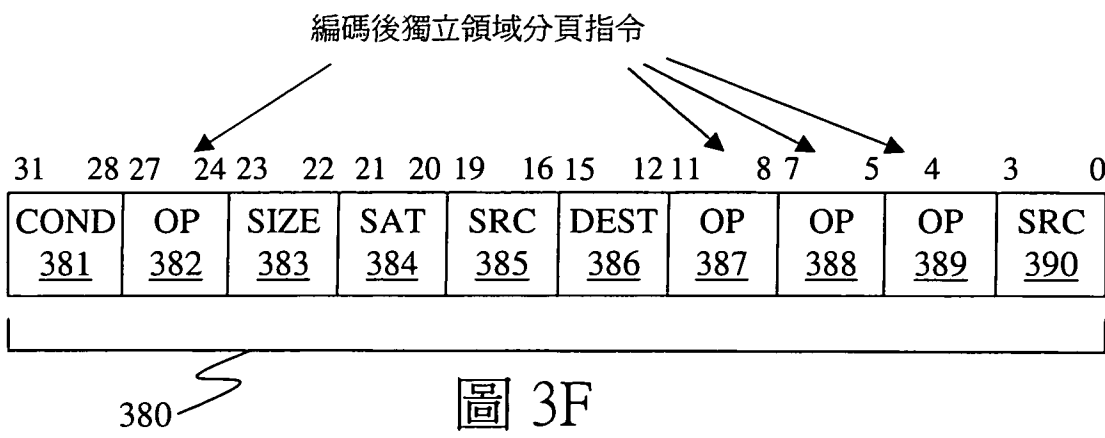


圖 3F

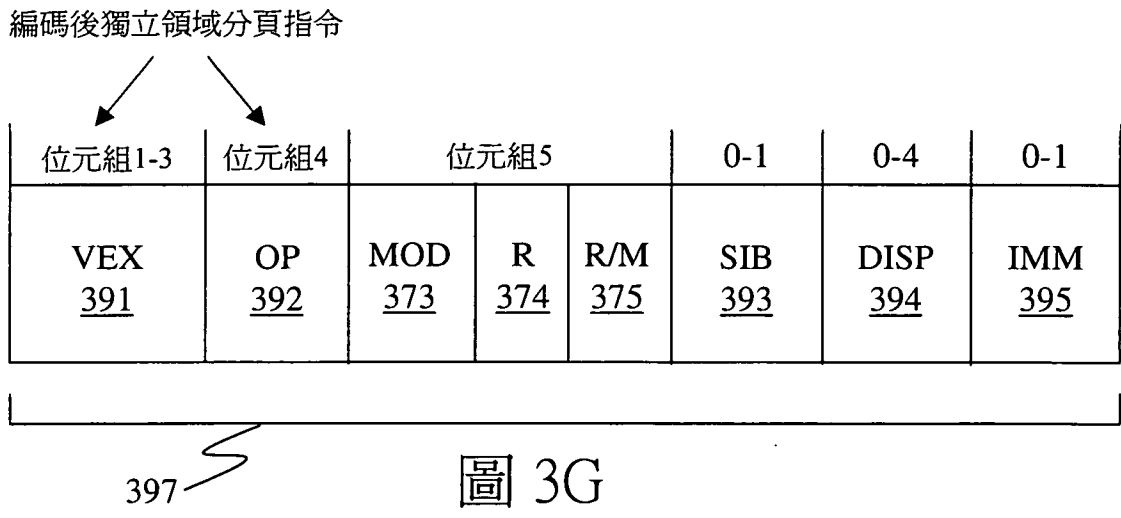


圖 3G

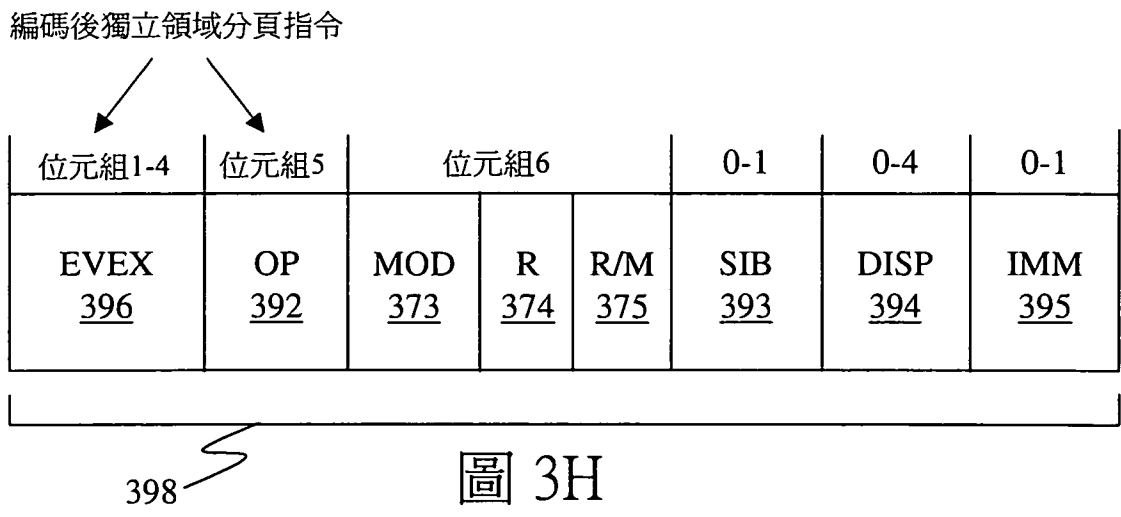
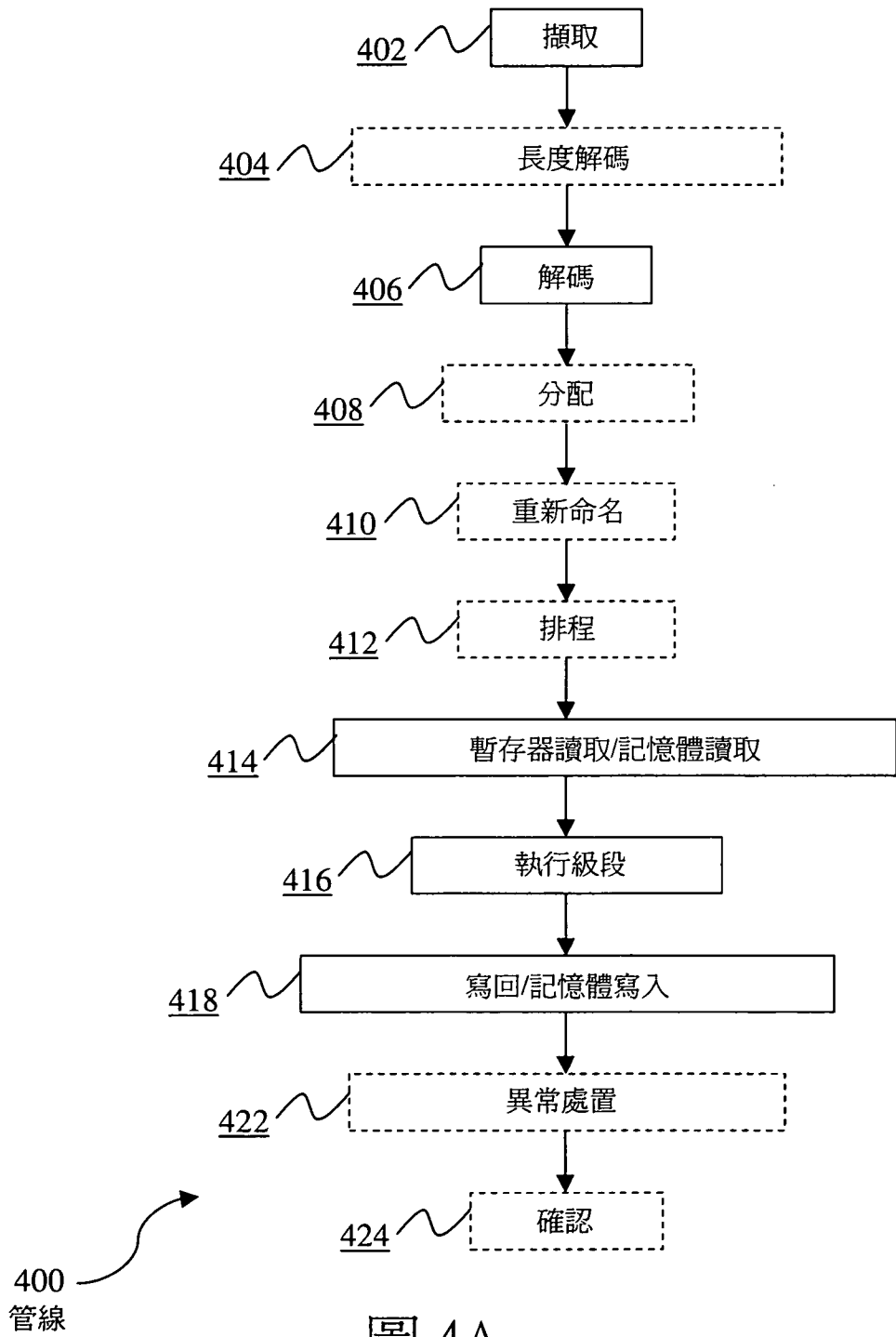


圖 3H



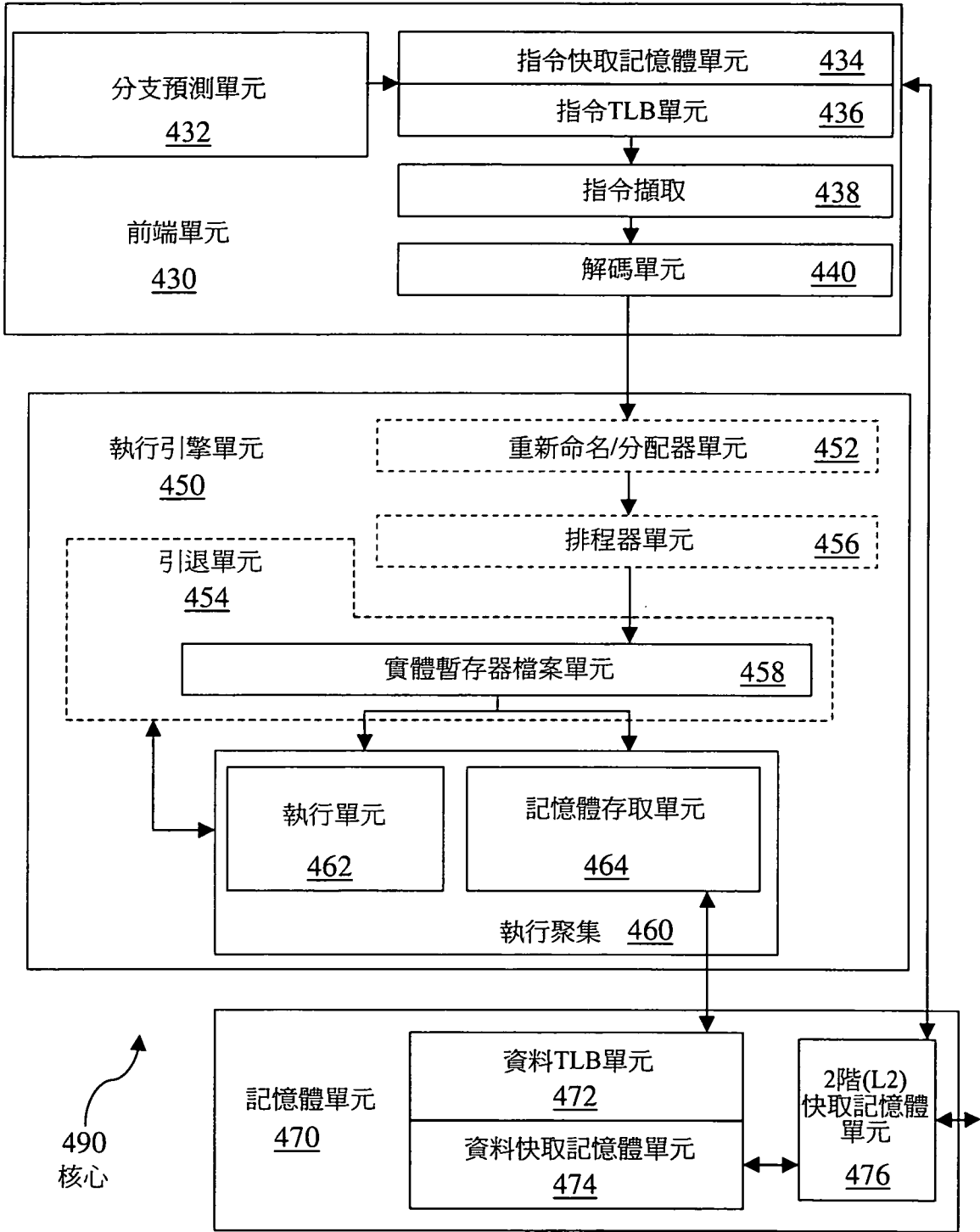


圖 4B

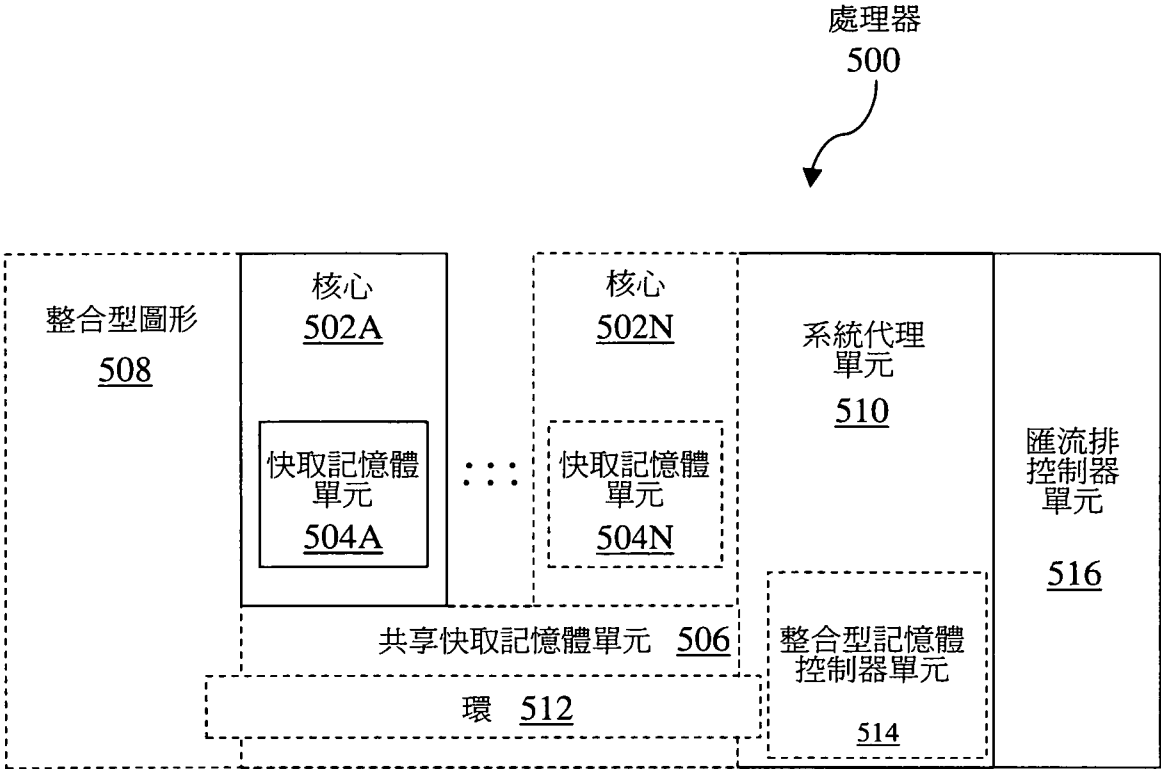


圖 5

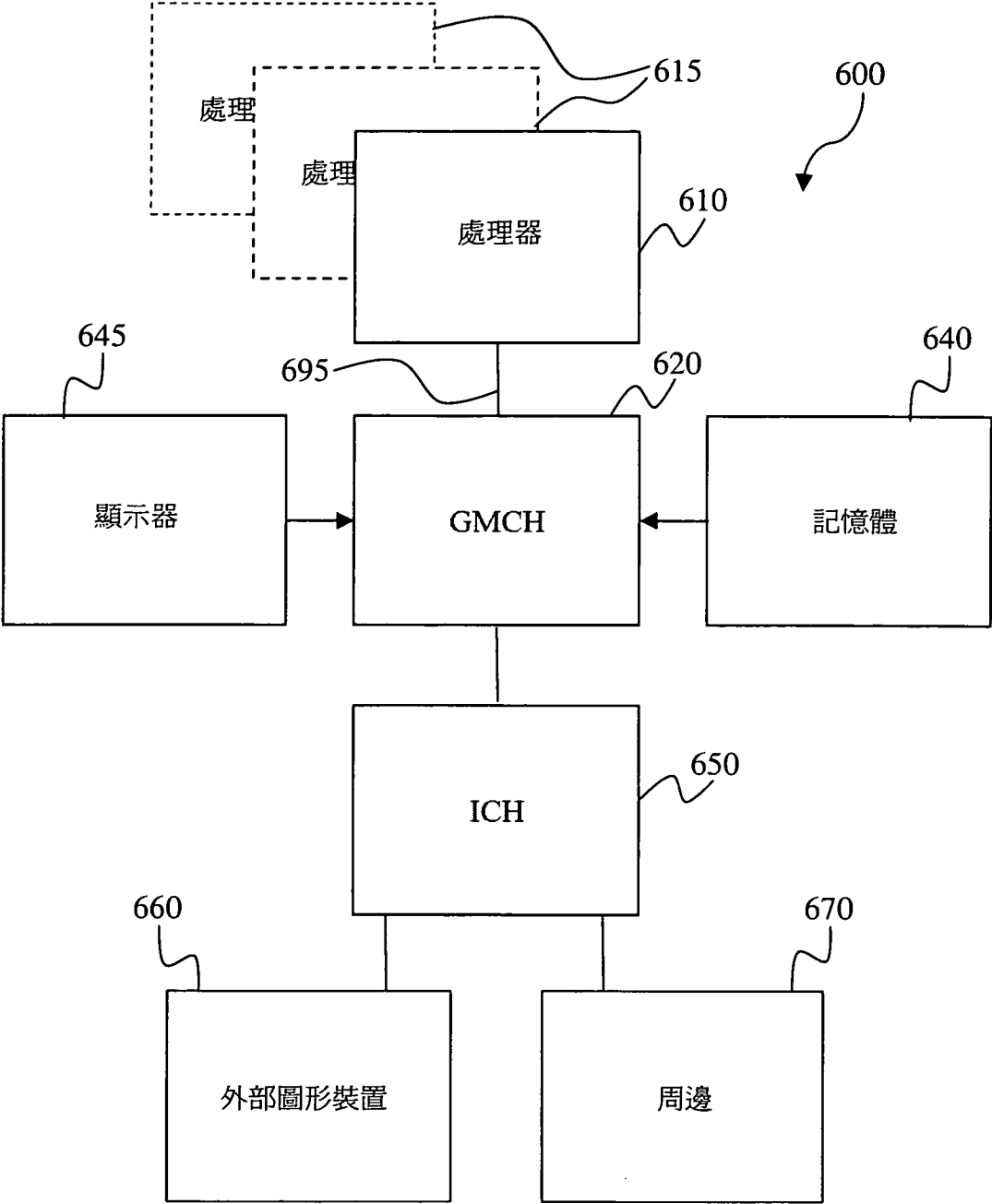


圖 6

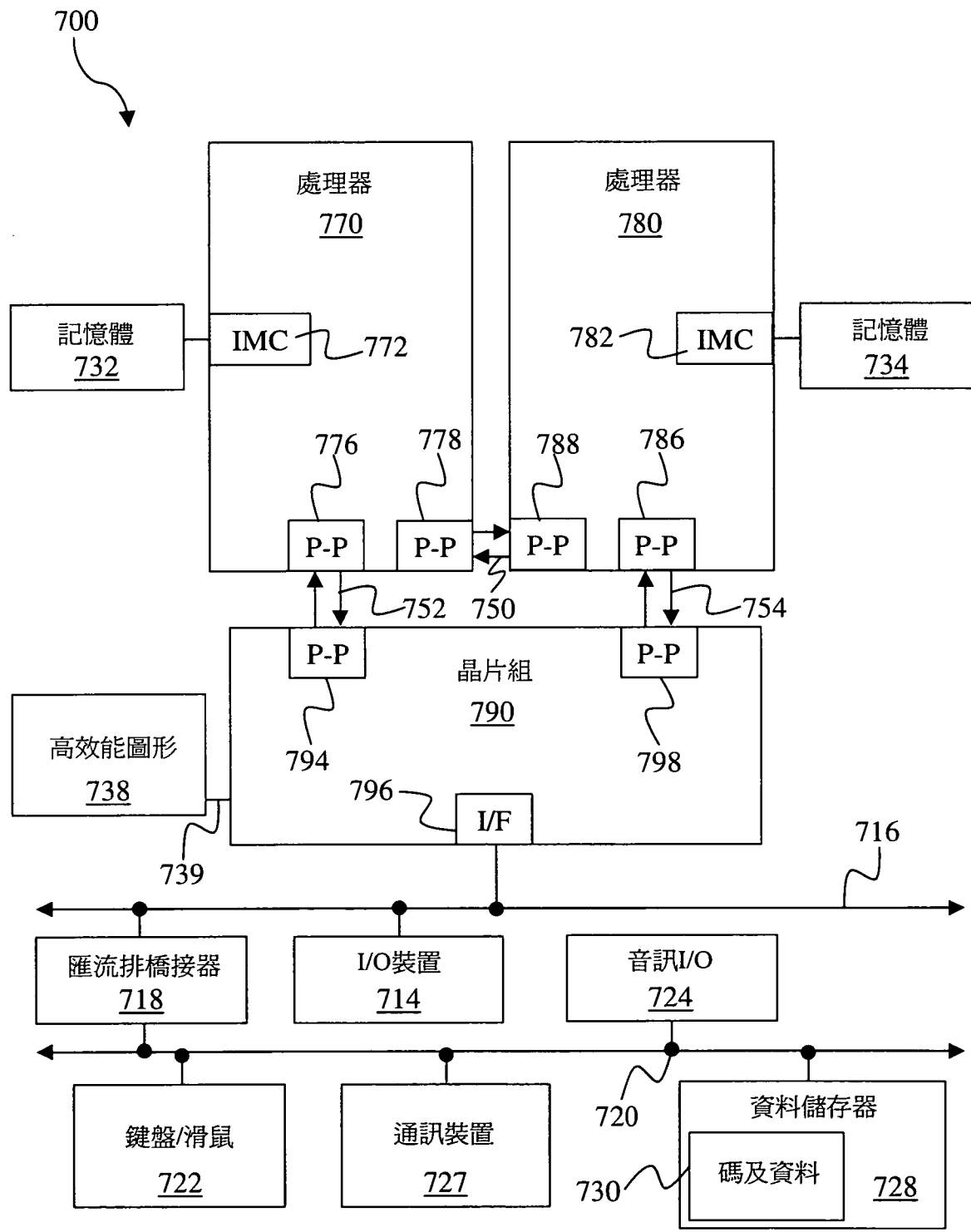


圖 7

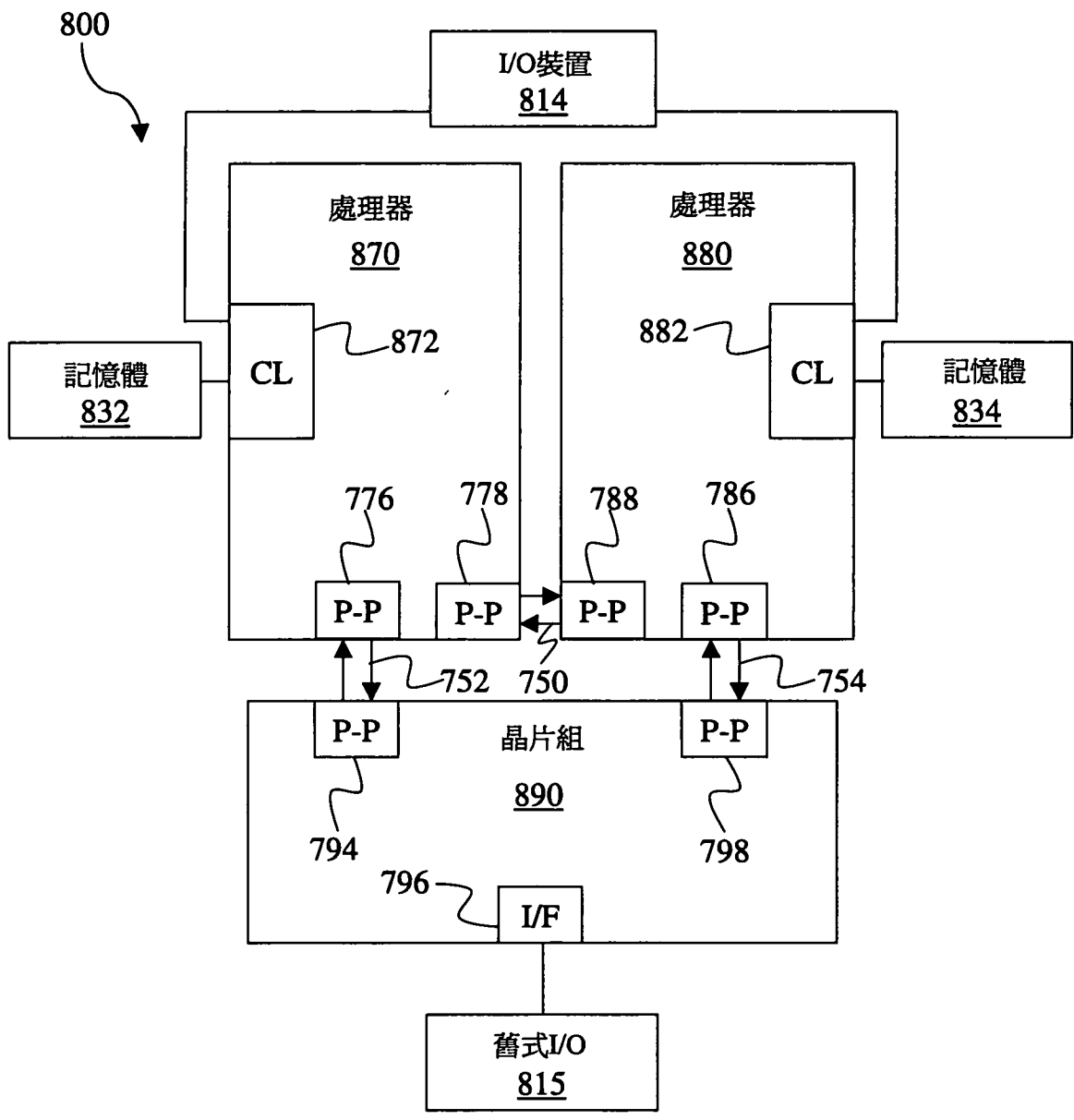


圖 8

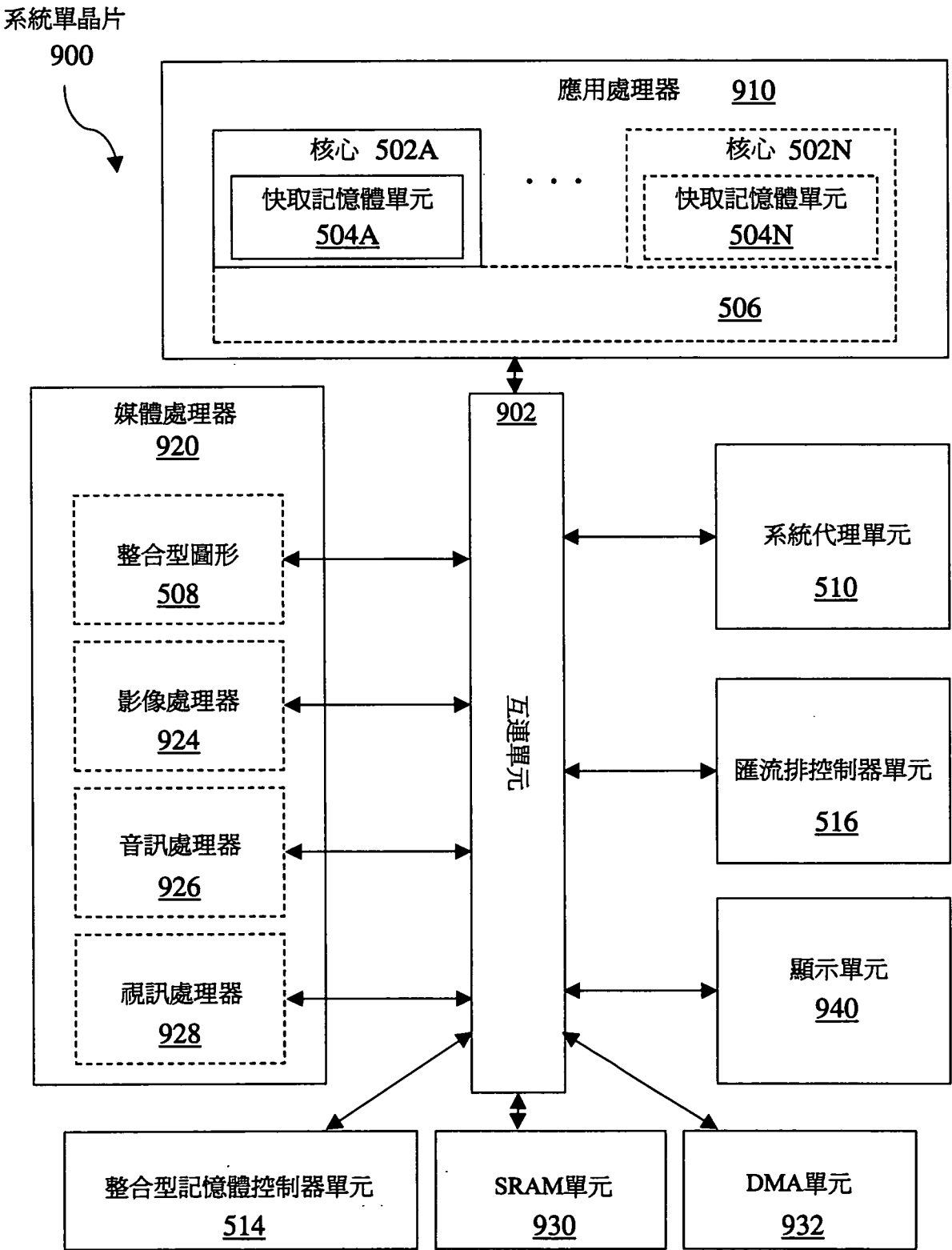


圖 9

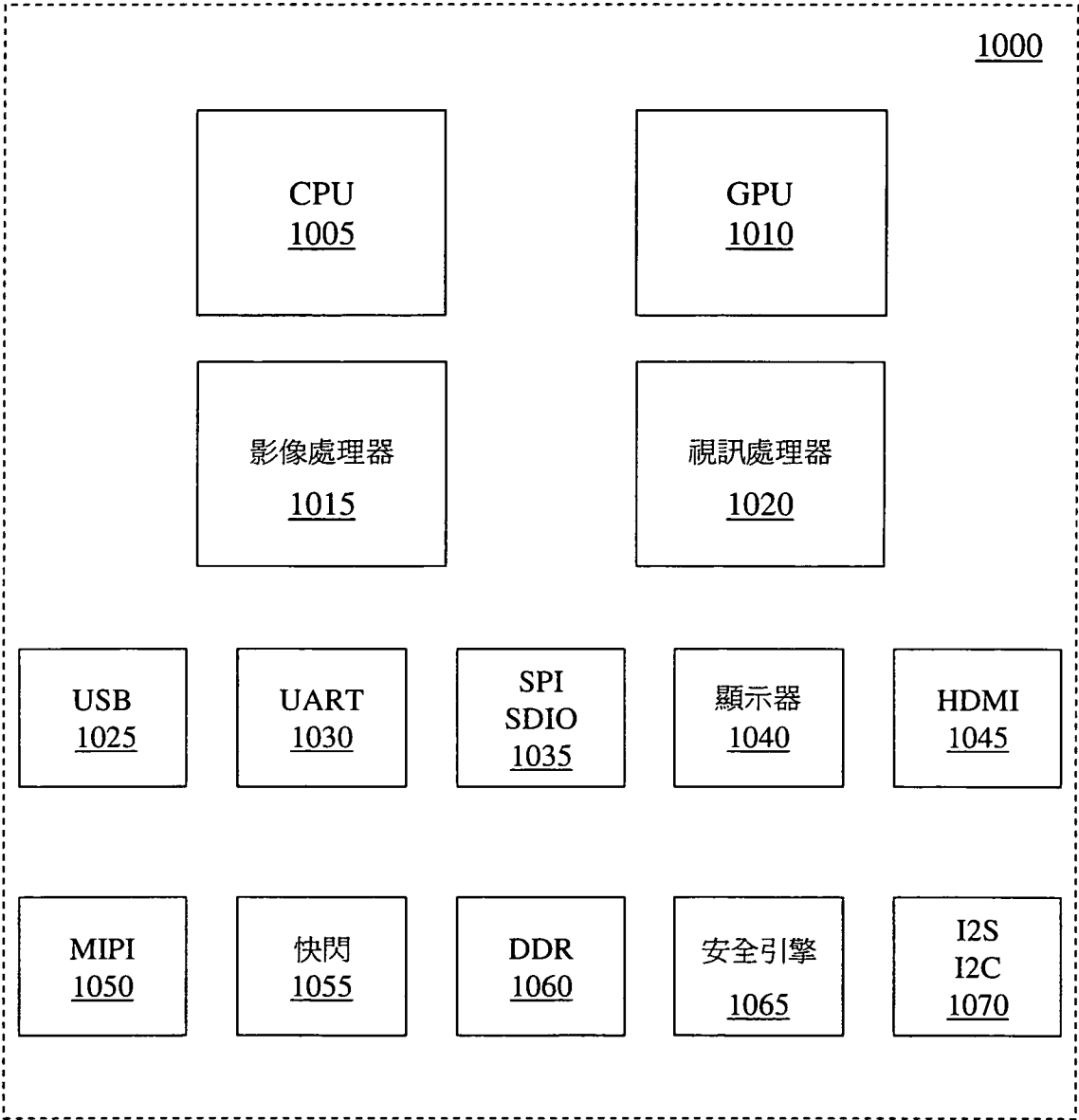


圖 10

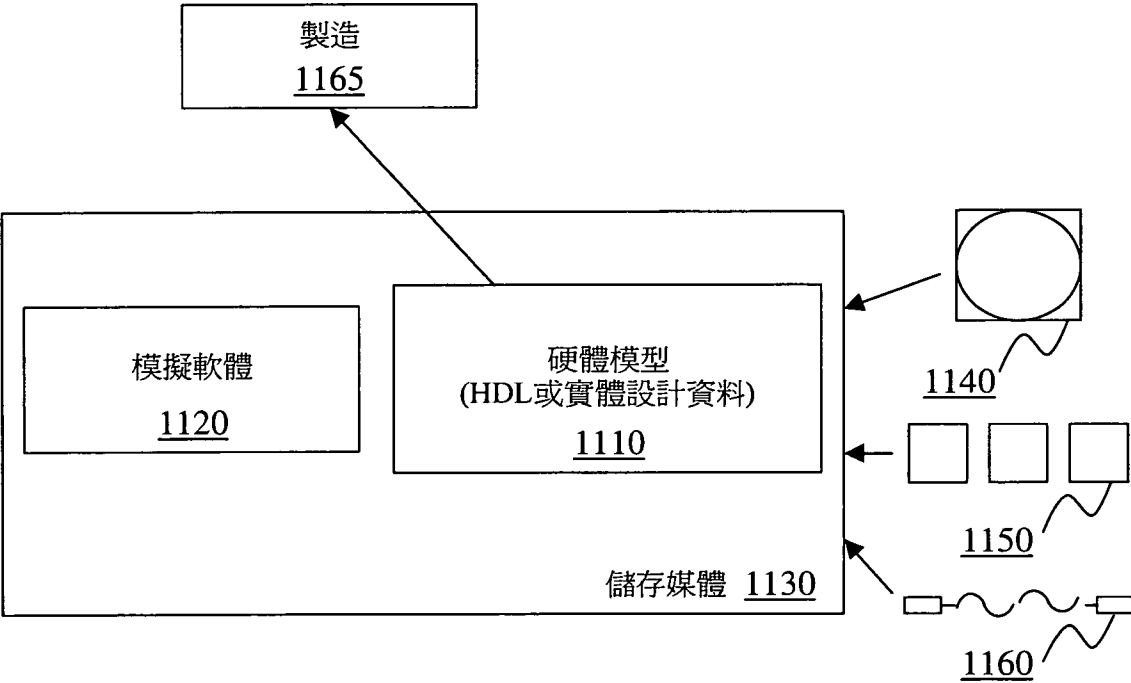


圖 11

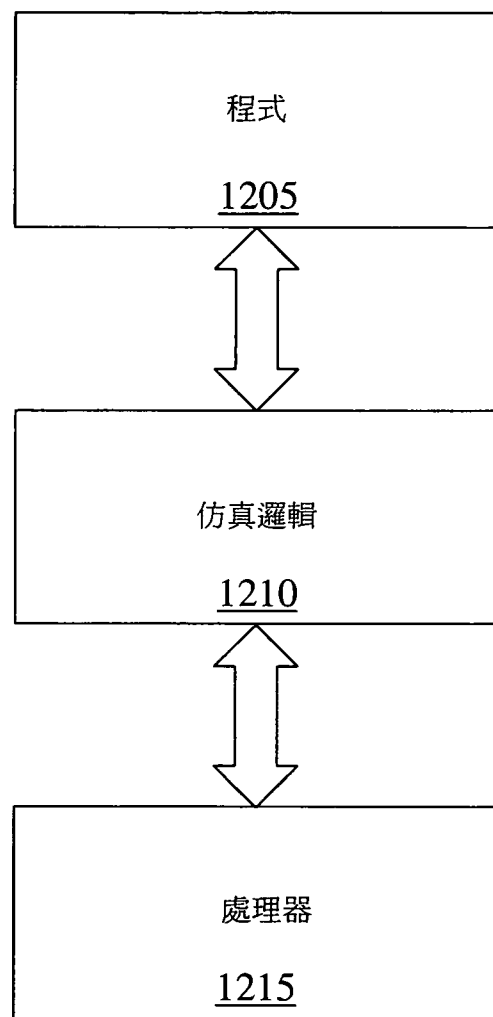


圖 12

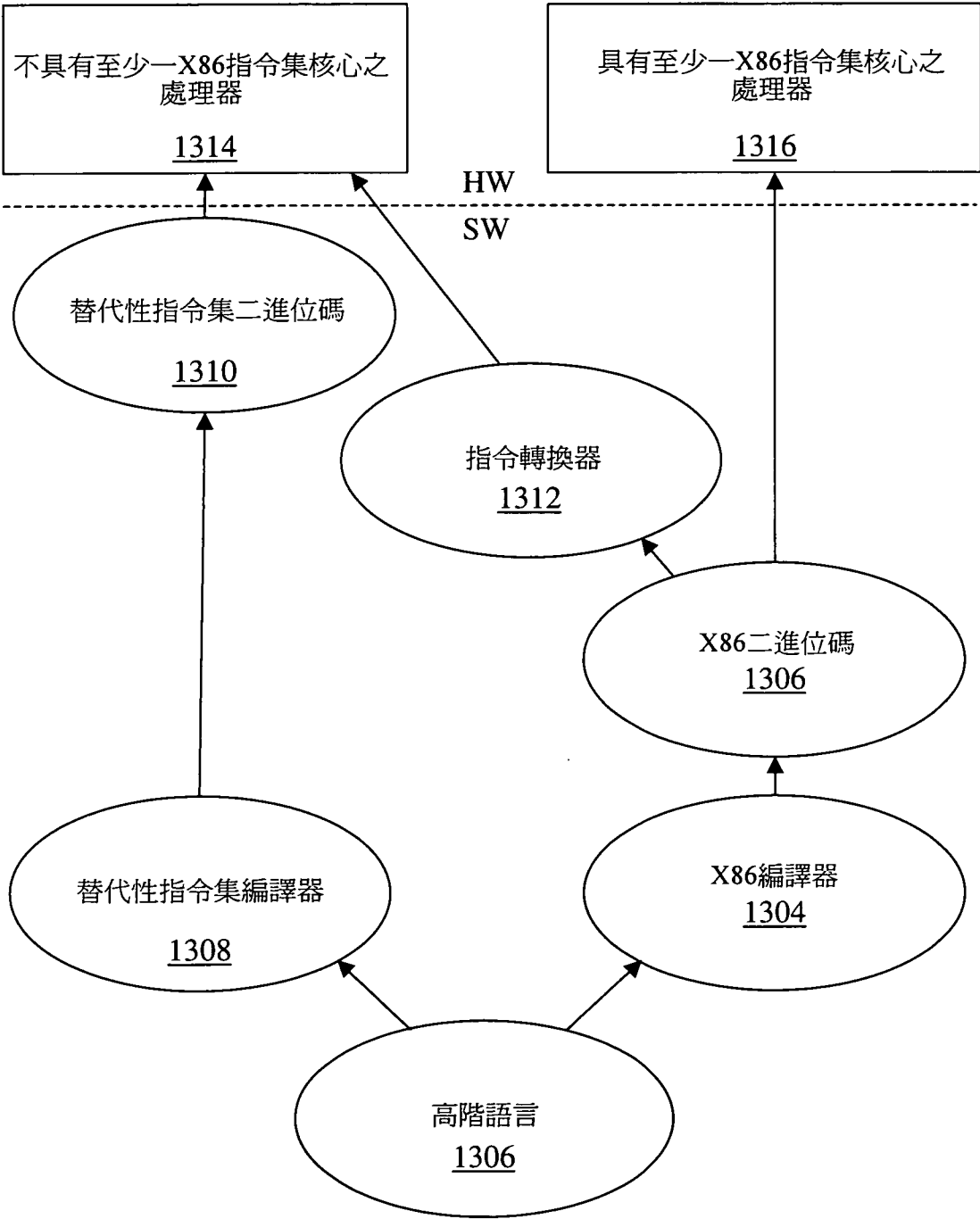


圖 13

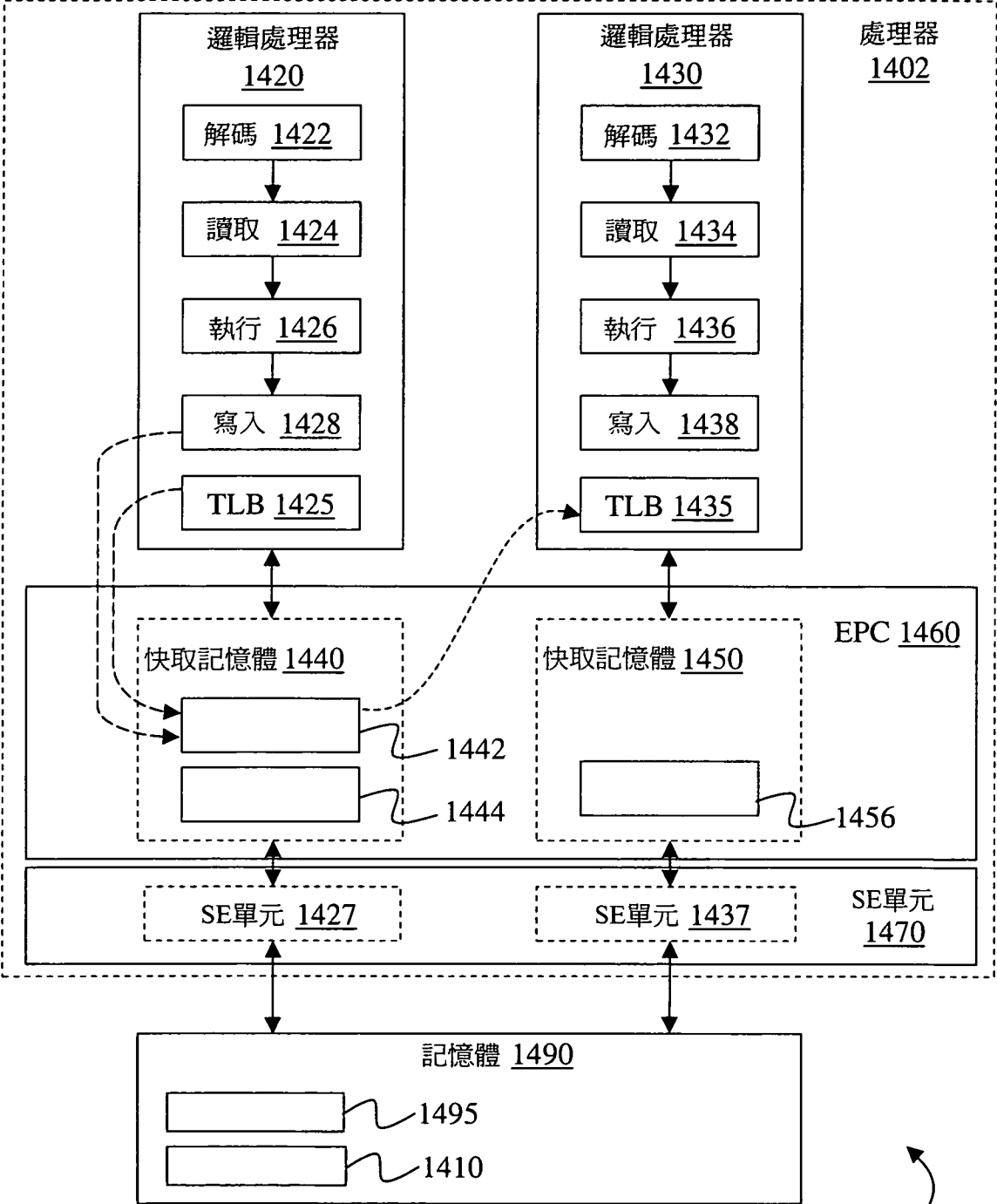


圖 14

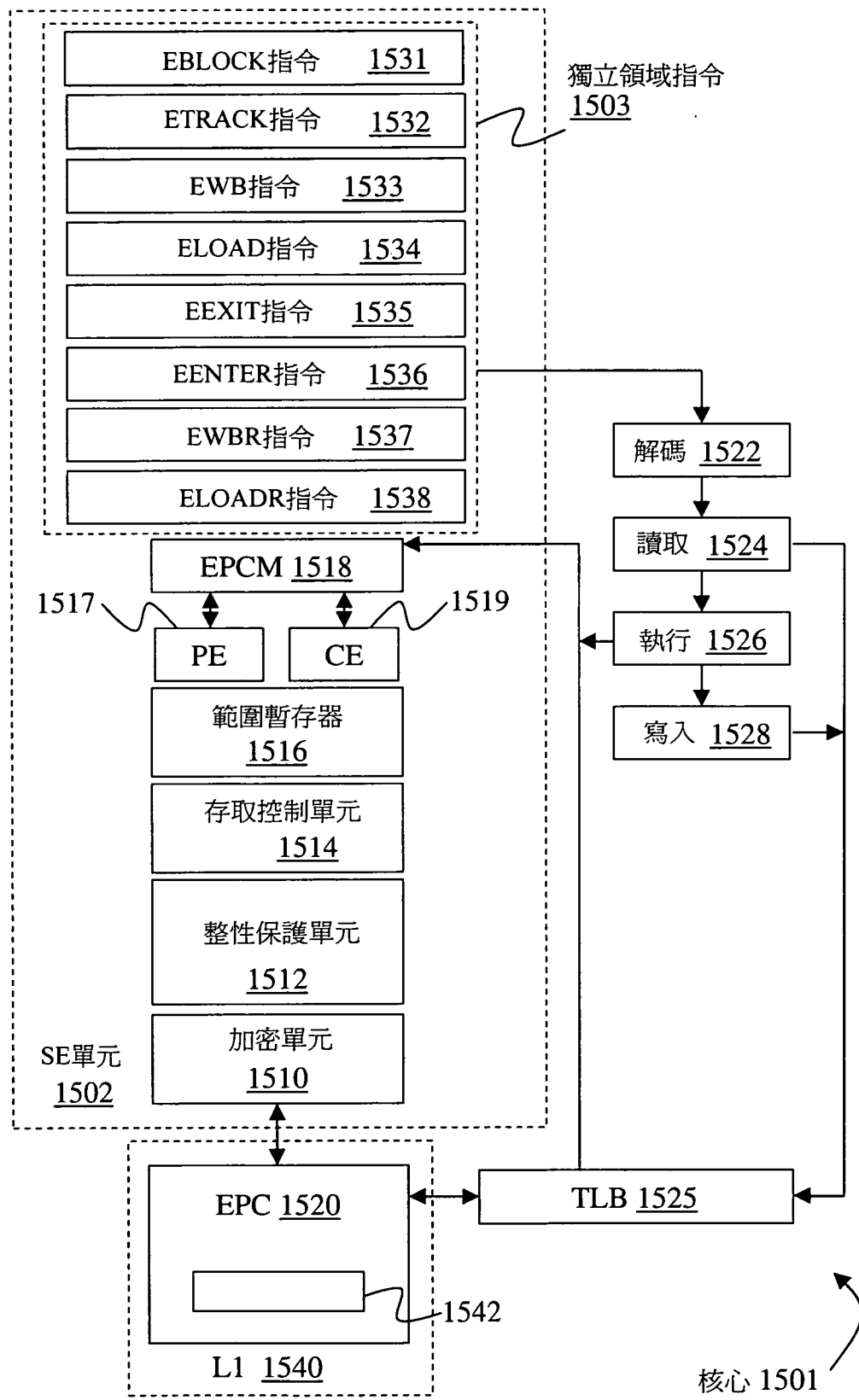


圖 15
22

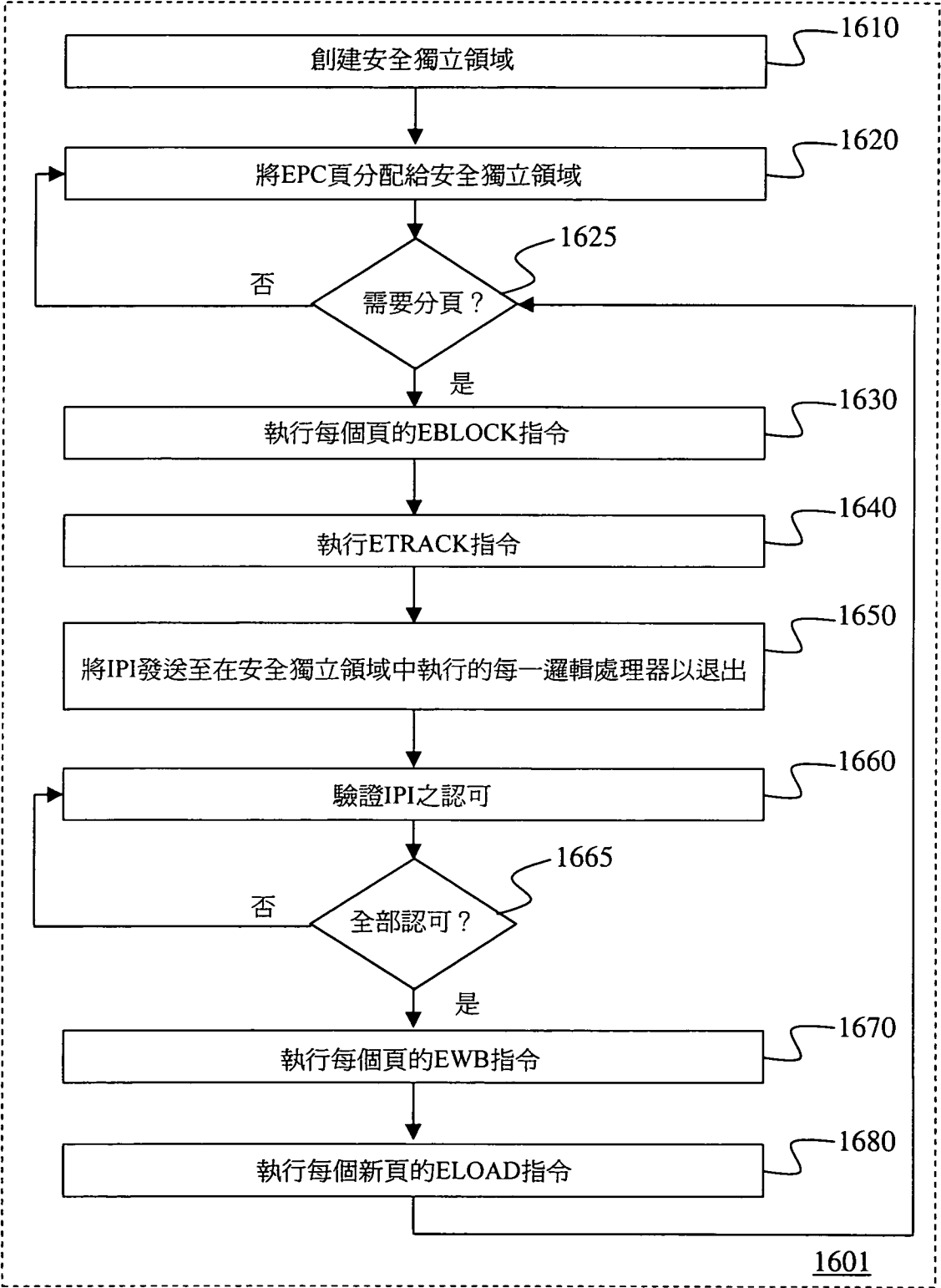


圖 16A

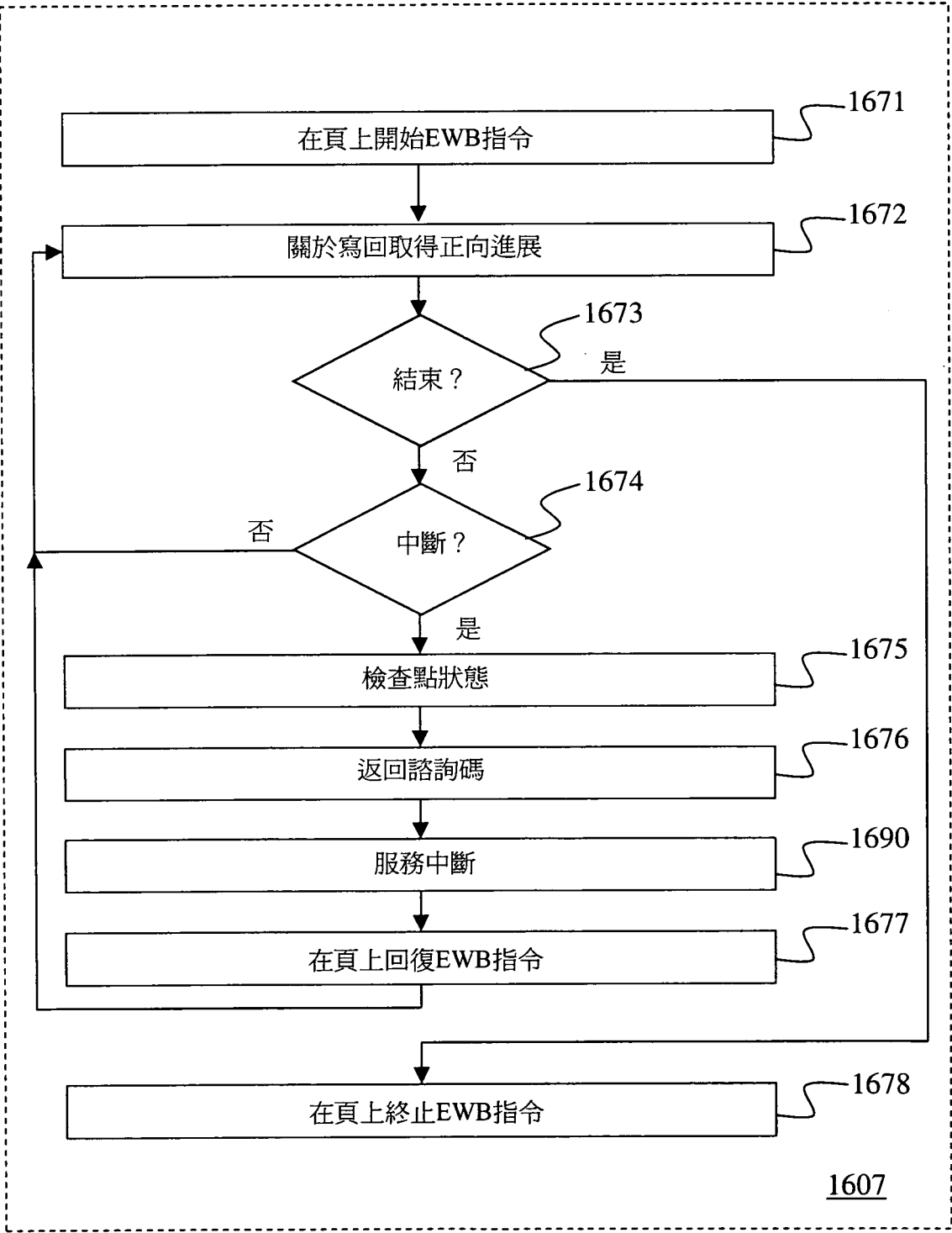


圖 16B

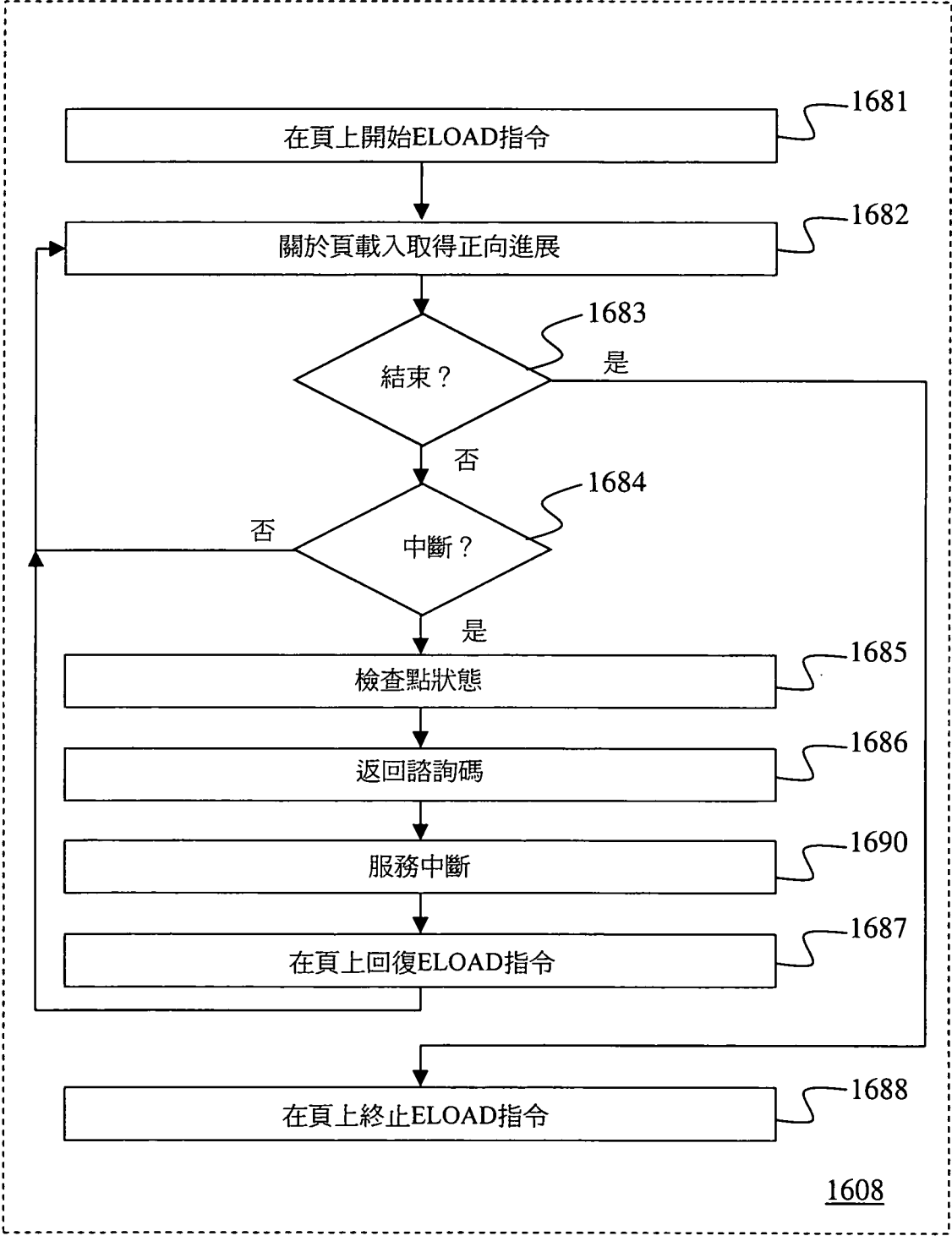


圖 16C

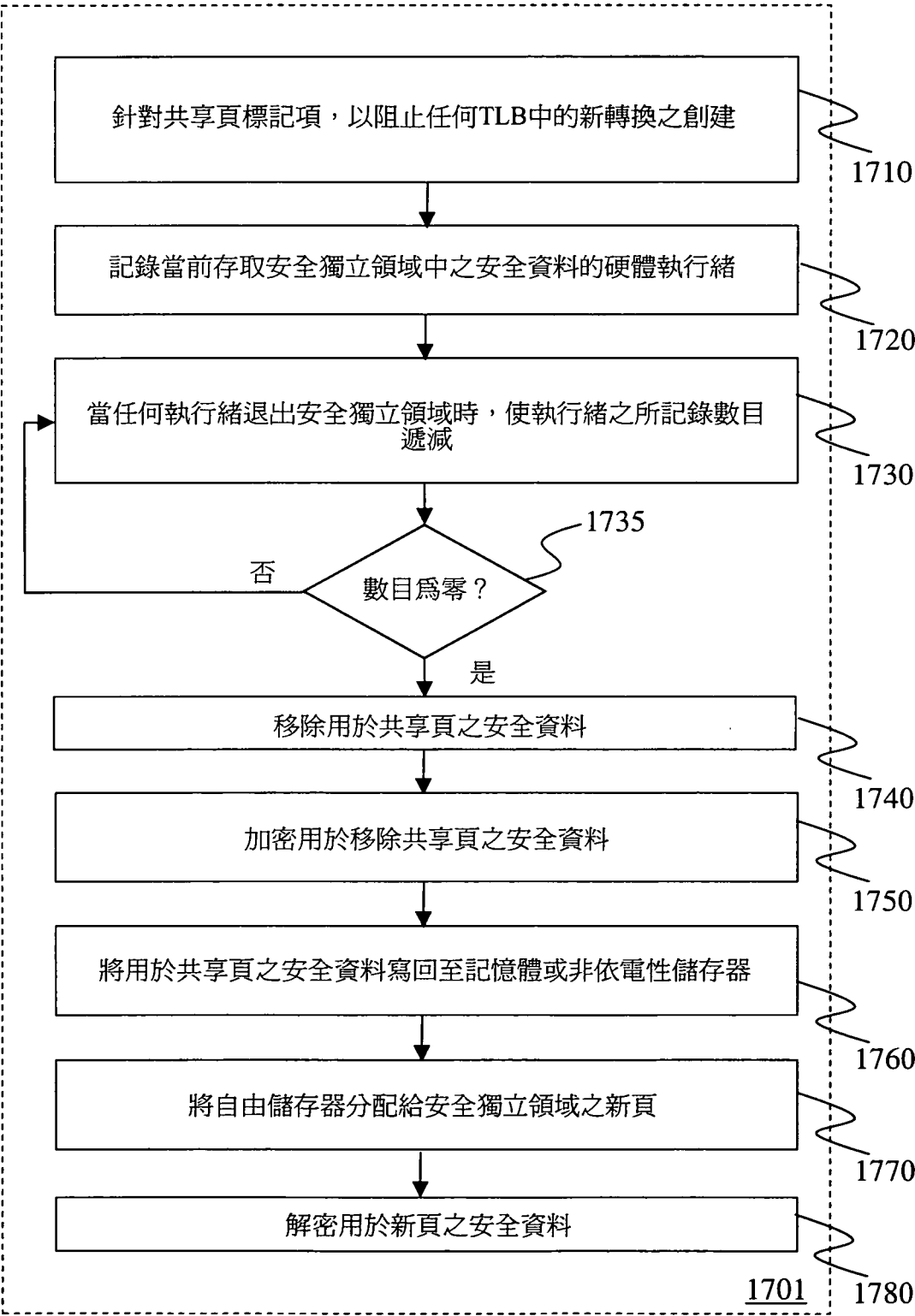


圖 17

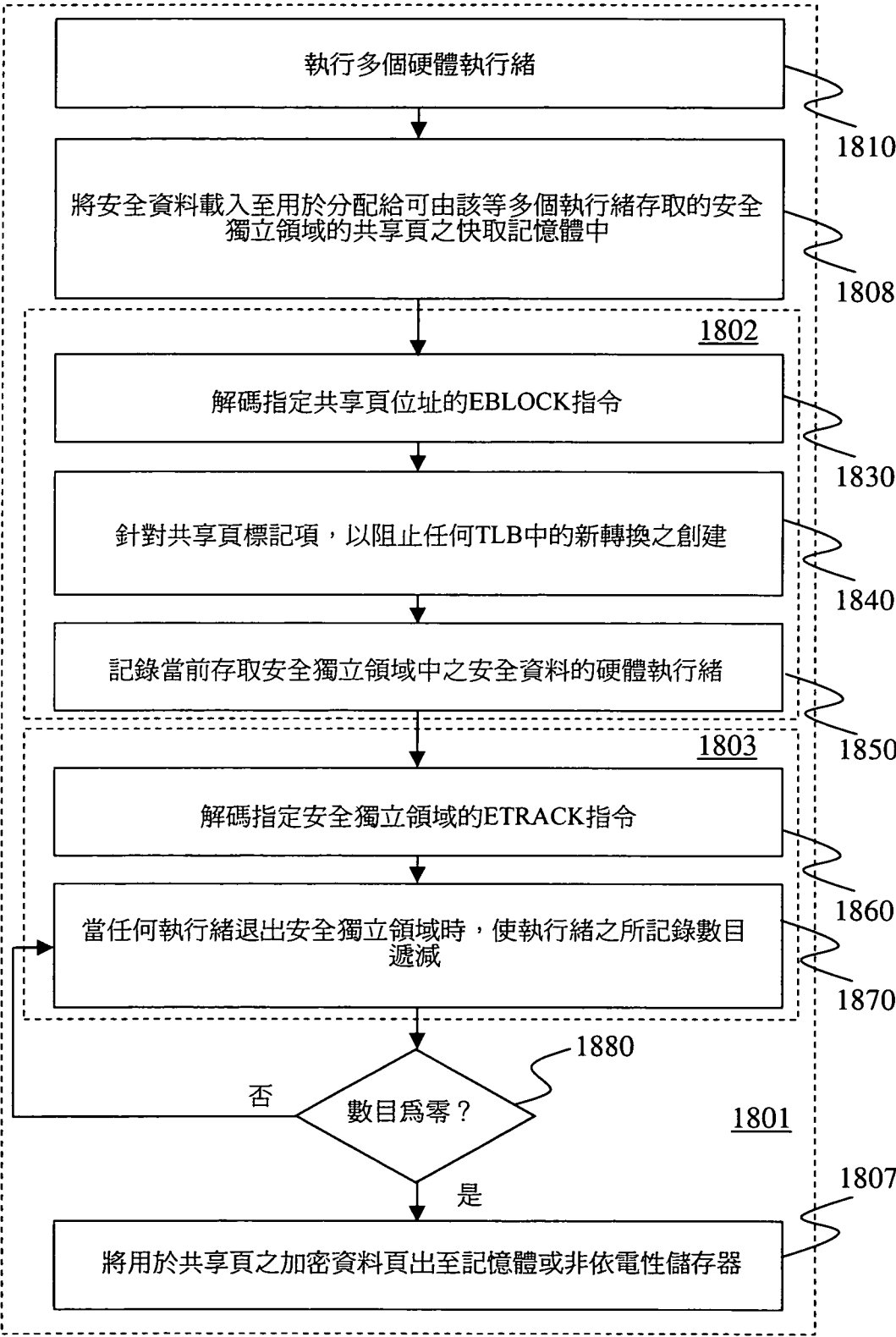


圖 18A

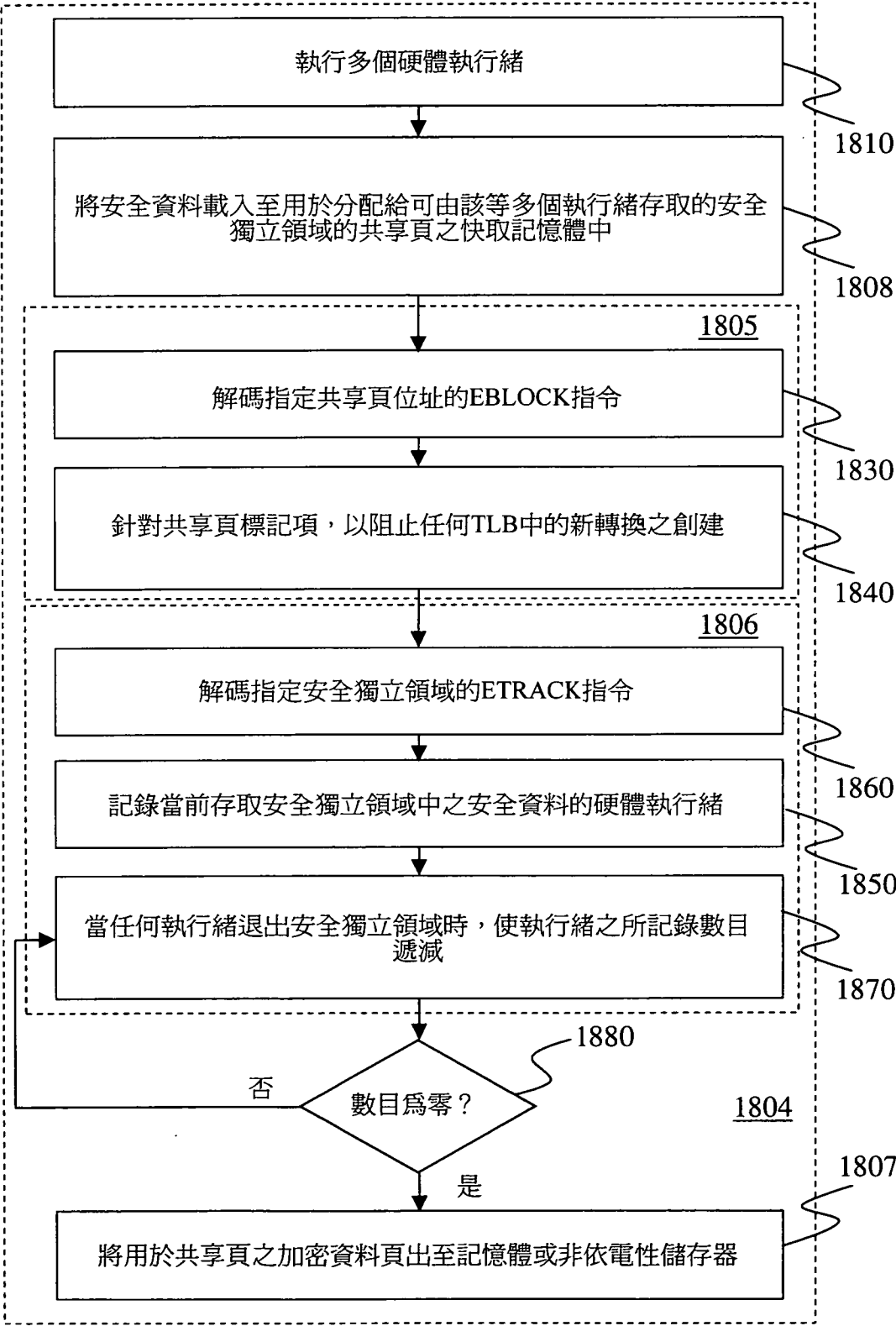


圖 18B

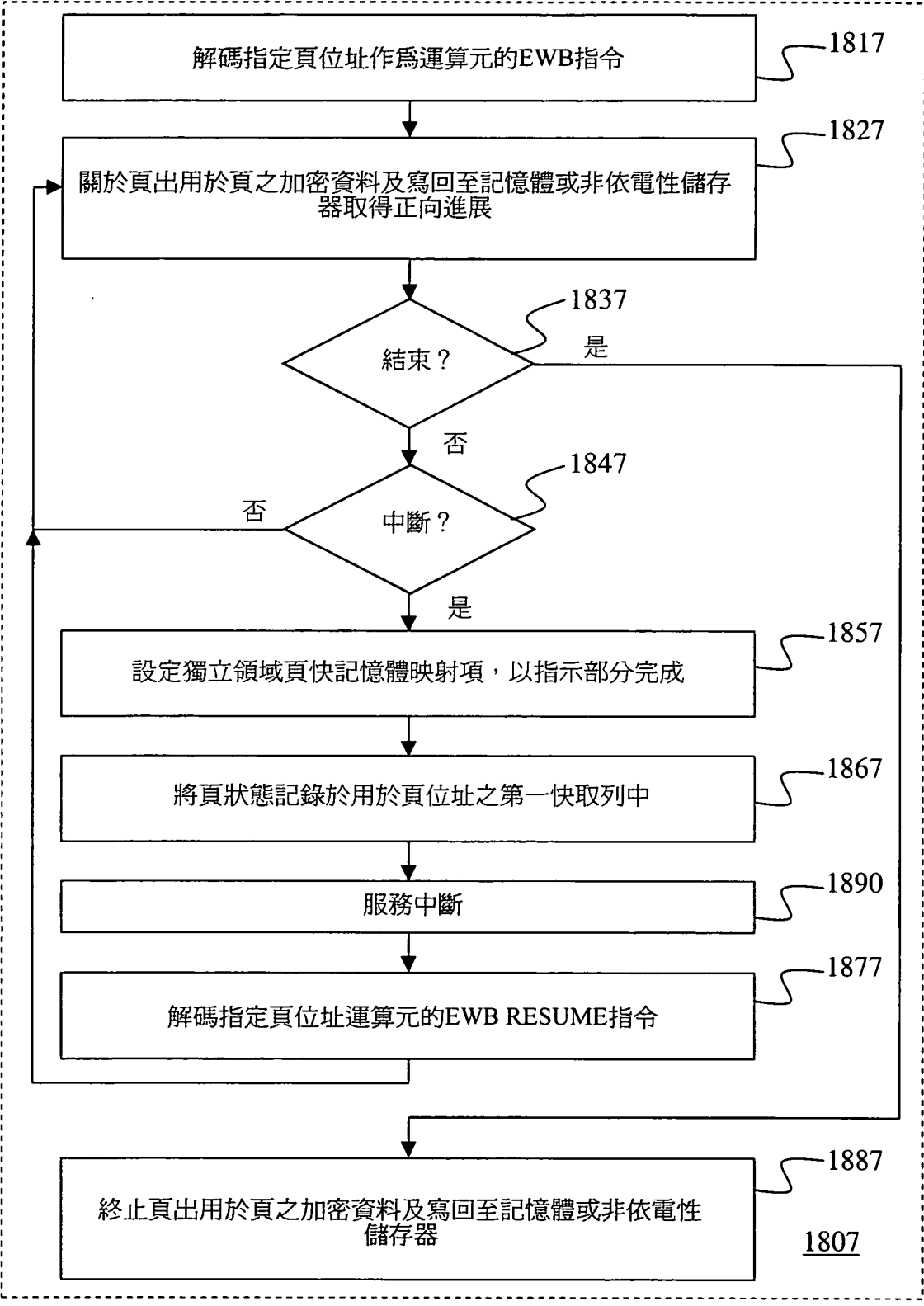


圖 18C

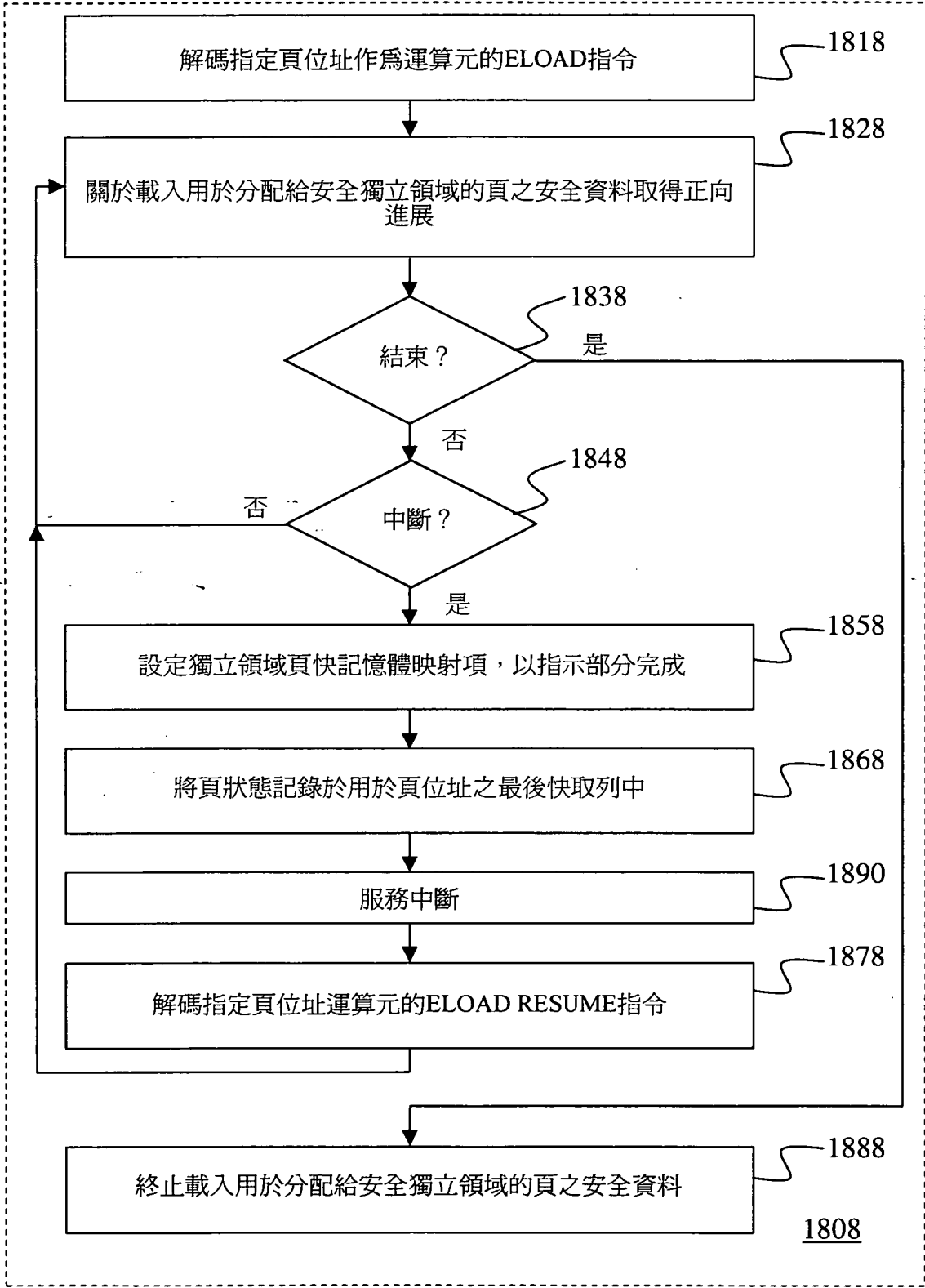


圖 18D