



(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 I852619 B

(45)公告日：中華民國 113 (2024) 年 08 月 11 日

(21)申請案號：112121566

(22)申請日：中華民國 105 (2016) 年 05 月 20 日

(51)Int. Cl. : G06F9/30 (2018.01)

G06F9/305 (2006.01)

(30)優先權：2015/06/26 美國

14/752,221

(71)申請人：美商英特爾股份有限公司 (美國) INTEL CORPORATION (US)
美國(72)發明人：沙巴吉 凡德伊斯 SHANBHOGUE, VEDVYAS (US)；布蘭特 傑森 BRANDT,
JASON W. (US)；沙希塔 拉維 SAHITA, RAVI (IN)；巴瑞 亨特里 HUNTLEY,
BARRY (US)；帕帖爾 貝吉 PATEL, BAIJU V. (US)

(74)代理人：林志剛

(56)參考文獻：

TW 201241627A

US 6128728

US 2004/0168078A1

WO 2013/019350A2

審查人員：簡大翔

申請專利範圍項數：9 項 圖式數：20 共 103 頁

(54)名稱

用以保護影子堆疊之處理器

(57)摘要

一個方面之處理器包括用以解碼指令之解碼單元。該處理器也包括耦接至該解碼單元之執行單元。該執行單元回應於該指令以判定由於該指令至影子堆疊之影子堆疊指標之嘗試的改變將導致該影子堆疊指標超過允許的範圍。該執行單元也用以回應於至該影子堆疊指標之該嘗試的改變將導致該影子堆疊指標超過允許的範圍之判定採取異常。揭露了其它處理器、方法、系統和指令。

A processor of an aspect includes a decode unit to decode an instruction. The processor also includes an execution unit coupled with the decode unit. The execution unit, in response to the instruction, is to determine that an attempted change due to the instruction, to a shadow stack pointer of a shadow stack, would cause the shadow stack pointer to exceed an allowed range. The execution unit is also to take an exception in response to determining that the attempted change to the shadow stack pointer would cause the shadow stack pointer to exceed the allowed range. Other processors, methods, systems, and instructions are disclosed.

指定代表圖：

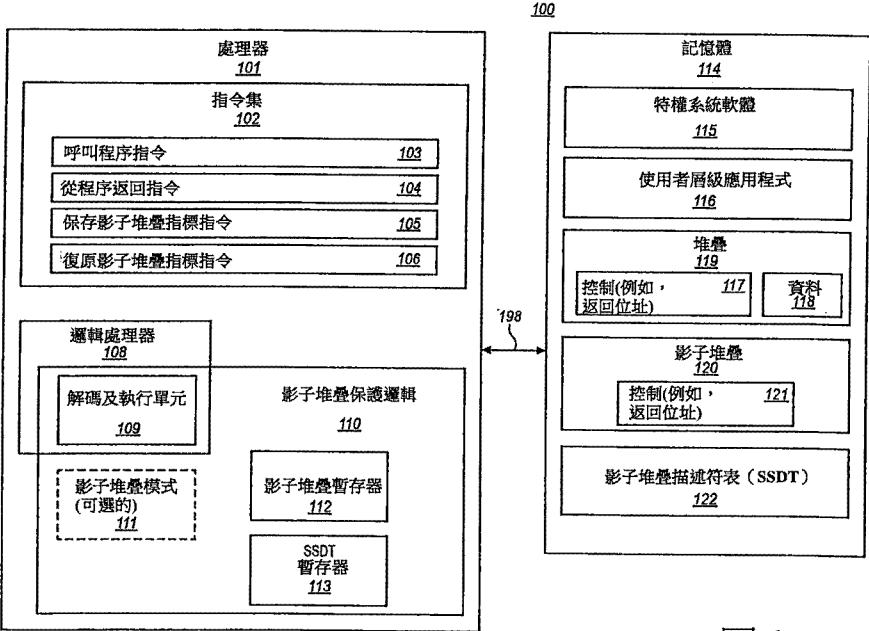


圖 1

符號簡單說明：

- 100:電腦系統
- 101:處理器
- 102:指令集
- 103:呼叫程序指令
- 104:從程序返回指令
- 105:保存影子堆疊指標指令
- 106:復原影子堆疊指標指令
- 108:邏輯處理器
- 109:解碼及執行單元
- 110:影子堆疊保護邏輯
- 111:影子堆疊模式
- 112:影子堆疊暫存器
- 113:SSDT 暫存器
- 114:記憶體
- 115:特權系統軟體
- 116:使用者層級應用程式
- 117,121:控制
- 118:資料
- 119:堆疊
- 120:影子堆疊
- 122:影子堆疊描述符表 (SSDT)
- 198:互連機制



【發明摘要】

【中文發明名稱】

用以保護影子堆疊之處理器

【英文發明名稱】

PROCESSORS TO PROTECT SHADOW STACKS

【中文】

一個方面之處理器包括用以解碼指令之解碼單元。該處理器也包括耦接至該解碼單元之執行單元。該執行單元回應於該指令以判定由於該指令至影子堆疊之影子堆疊指標之嘗試的改變將導致該影子堆疊指標超過允許的範圍。該執行單元也用以回應於至該影子堆疊指標之該嘗試的改變將導致該影子堆疊指標超過允許的範圍之判定採取異常。揭露了其它處理器、方法、系統和指令。

【英文】

A processor of an aspect includes a decode unit to decode an instruction. The processor also includes an execution unit coupled with the decode unit. The execution unit, in response to the instruction, is to determine that an attempted change due to the instruction, to a shadow stack pointer of a shadow stack, would cause the shadow stack pointer to exceed an allowed range. The execution unit is also to take an exception in response to determining that the attempted change to the shadow stack pointer would cause the shadow stack pointer to exceed the allowed range. Other processors, methods, systems, and instructions are disclosed.

【代表圖】

【本案指定代表圖】圖 1

【本代表圖之符號簡單說明】：

100:電腦系統
101:處理器
102:指令集
103:呼叫程序指令
104:從程序返回指令
105:保存影子堆疊指標指令
106:復原影子堆疊指標指令
108:邏輯處理器
109:解碼及執行單元
110:影子堆疊保護邏輯
111:影子堆疊模式
112:影子堆疊暫存器
113:SSDT 暫存器
114:記憶體
115:特權系統軟體
116:使用者層級應用程式
117,121:控制
118:資料
119:堆疊
120:影子堆疊
122:影子堆疊描述符表(SSDT)
198:互連機制

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

【發明說明書】

【中文發明名稱】

用以保護影子堆疊之處理器

【英文發明名稱】

PROCESSORS TO PROTECT SHADOW STACKS

【技術領域】

[0001] 本發明實施例一般係有關於處理器。更具體地，本發明實施例一般係有關具有安全性提升之處理器。

【先前技術】

[0002] 返回導向程式設計（Return-oriented programming，ROP）及跳躍導向程式設計（jump-oriented programming，JOP）為電腦安全劫取技術，電腦安全劫取技術為攻擊者可透過電腦系統或其它電子裝置來得到控制以及用來執行惡意行為。在這些技術中，攻擊者得到呼叫堆疊之控制係為了劫持程式控制流。

[0003] 呼叫堆疊之控制通常藉由緩衝超限（buffer overrun）劫取或攻擊達成。在緩衝超限中，在儲存資料至記憶體之前，未能充分執行邊界檢查之函數可能接收過多其可以合適地儲存的資料。例如，攻擊者可發送比網頁瀏覽器（web browser）能夠合適地儲存更多的資料至網頁瀏覽器。如果資料被儲存在堆疊中，一些資料可能超過分

配給函數的變量之儲存空間且重寫返回位址。返回位址可表示由呼叫程序指令儲存在堆疊上之位址，其目的是用來在呼叫程序完成之後重新導向控制流返回到呼叫函數。然而，在緩衝超限攻擊或劫取中，返回位址可能被重寫為不同的返回位址。這允許攻擊者轉移控制流至不同的返回位址、在不同返回位址上執行碼啟動以及執行潛在不期望和/或惡意行為。

[0004] 例如，在 ROP 攻擊中，攻擊者可能將所謂的「小程式 (gadgets)」之序列鏈接在一起。每個小程式可表示為隨後從程序指令返回的一或一些指令集。攻擊者可能分析例如應用程式、系統層級碼、驅動器、程式館 (libraries) 等等的碼以定位或辨識所需的小程式。例如，攻擊者可能掃描用於從程序指令返回的操作碼 (opcode)。在此種從程序指令返回辨識之前的程序指令可潛在地表示具有不同功能之不同類型的小程式。藉由舉例的方式，攻擊者可辨識隨後作為第一小程式之返回指令的彈出堆疊指令、隨後作為第二小程式之返回指令的暫存器至暫存器移動指令等等。在一些情況下，攻擊者能夠辨識足夠的小程式以便能夠串在一起以及執行各種不同惡意行為。

[0005] 代表性地，緩衝超限攻擊最初用來劫持在堆疊上的返回位址並藉此劫持控制流。第一小程式之第一指令之位址可被儲存在堆疊上而轉移控制流至第一小程式。取代返回至與呼叫程序指令相關聯之呼叫程序，控制流可

轉移至由攻擊者所選的第一小程序之第一指令。接著，第一小程序之返回指令可轉移至第二小程序。在這方式中，串列之小程序之返回位址可順序地儲存在堆上且由鏈接的小程式之返回指令跳躍。藉由以特定順序鏈接小程序在一起，攻擊者能夠從先前存在的碼建立新的程式。攻擊者可使用這些於不良或有害的目的，例如竊取機密信息、干擾或攻擊其他應用程式、發送電子郵件、發送短信、張貼推文(tweets)、或劫取內核的易損性(vulnerabilities)。

【圖式簡單說明】

[0006] 本發明可藉由參考其被用以闡明實施例之以下描述及後附圖形而被最佳地瞭解。在圖式中：

圖 1 為電腦系統實施例之方塊圖，其中本發明實施例可以實施。

圖 2 為影子堆疊暫存器組之實施例和影子堆疊描述符表(descriptor table)暫存器組之實施例的方塊圖。

圖 3 為影子堆疊描述符表之實施例的方塊圖。

圖 4 為合適的影子堆疊描述符表(SSDT)登錄之一特定範例實施例的方塊圖。

圖 5 為影子堆疊描述符表選擇器之範例實施例的方塊圖。

圖 6 為 32 位元任務狀態片段結構之範例實施例之實施例的方塊圖。

圖 7 為 64 位元任務狀態片段結構之範例實施例的方

塊圖。

圖 8 為操作以執行呼叫程序指令之實施例和從程序指令返回之實施例之處理器之實施例的方塊圖。

圖 9 為執行保存影子堆疊指標指令之實施例的方法實施例的方塊流程圖。

圖 10 為操作以執行保存影子堆疊指標指令之實施例的處理器之實施例的方塊圖。

圖 11 為執行復原影子堆疊指標指令之實施例的方法實施例的方塊流程圖。

圖 12 為操作以執行復原影子堆疊指標指令之實施例的處理器之實施例的方塊圖。

圖 13A 為示出有序管線之實施例及暫存器重新命名失序簽發/執行管線之實施例的方塊圖。

圖 13B 為示出包括耦接至執行引擎單元以及耦接至記憶體單元之前端單元的處理器核心之實施例的方塊圖。

圖 14A 為單一處理器核心之實施例的方塊圖，連同其連接至晶粒上互連網路及層級 2(L2)快取記憶體之其本地子集的方塊圖。

圖 14B 為圖 14A 中的處理器核心部分之展開圖之實施例的方塊圖。

圖 15 為處理器之實施例的方塊圖，該處理器可具有多於一個核心、可具有整合記憶體控制器及可具有整合圖形。

圖 16 為電腦架構之第一實施例的方塊圖。

圖 17 為電腦架構之第二實施例的方塊圖。

圖 18 為電腦架構之第三實施例的方塊圖。

圖 19 為電腦架構之第四實施例的方塊圖。

圖 20 為根據本發明實施例之軟體指令轉換器之使用的方塊圖，該轉換器係用以將來源指令集中之二元指令轉換至目標指令集中之二元指令。

【發明內容及實施方式】

[0007] 在本文中揭露的是影子堆疊保護指令、用以執行所述指令之處理器、當處理或執行所述指令時由處理器執行之方法以及整合一或多個用以處理或執行所述指令之處理器的系統。在本文中也揭露的是影子堆疊保護邏輯。在下面敘述中，陳述數個具體細節（例如，具體指令操作、資料格式、處理器、配置、微架構細節、操作序列等等）。然而，實施例可以在無這些具體細節而實施。在其它情況下，為了避免妨礙對本詳細說明部分的了解，眾所皆知的電路、結構及技術而不細節顯示。

[0008] 圖 1 為電腦系統 100 實施例之方塊圖，其中本發明實施例可以實施。在各種實施例中，電腦系統可代表桌上型電腦系統、膝上型電腦系統、筆記型電腦、平板電腦、輕省筆電、可攜式個人電腦、智慧型手機、蜂巢式手機、伺服器、網路元件（例如，路由器或開關）、智慧型電視、桌上型易網機（nettop）、機上盒、視訊遊戲控制器、媒體播放器或其它類型的電腦系統或電子裝置。

[0009] 電腦系統包括處理器 101 和記憶體 114。當在系統中一起採用時，處理器和記憶體可由互連機制 198 彼此耦接。互連機制可包括一或多個匯流排或其它互連、一或多個橋接器或其它晶片組組件以及它們的組合。各種本領域已知的耦接處理器和記憶體的方式都是合適的。雖然記憶體係顯示在闡明的實施例中，其它實施例是關於不與記憶體耦接（例如，不在電腦系統中採用）至單獨處理器。記憶體之其它類型範例包括（但不限制於）動態隨機存取記憶體（DRAM）、快閃記憶體以及常使用於主記憶體之其它類型的記憶體。

[0010] 記憶體可儲存特權系統軟體 115。合適的特權系統軟體的範例包括（但不限制於）一或多個操作系統、虛擬機器監視器（VMM）、超管理器（hypervisor）等等及其它們的組合。記憶體也可儲存一或多個使用者層級應用程式 116。在一些實施例中，使用者層級應用程式可選擇地包括一或多個使用者層級多線（multithreaded）應用程式。如將在下文進一步解釋，此種使用者層級多線應用程式可選擇地使用本文揭露的指令以幫助增加執行使用者層級多線和/或執行使用者層級任務切換的效率。

[0011] 在操作期間，記憶體也可以儲存堆疊 119。堆疊在一些時候指的是呼叫堆疊、資料堆疊或只是堆疊。堆疊可代表可操作以儲存資料 118 和控制 117 兩者的堆疊類型資料結構。資料可表示軟體希望推送到堆疊之任何大範圍中不同類型的資料（例如，通過至次常式之參數和其它

資料等等)。通常，控制可包括用於一或多個先前執行的程序呼叫之一或多個返回位址。這些返回位址可代表指令位址，其中呼叫的程序係用以在呼叫的程序完成和返回時返回控制流。

[0012] 如在先前技術中所討論的，在返回導向程式設計 (ROP)、跳躍導向程式設計 (JOP) 及其它控制流 subversion 攻擊中，攻擊者通常尋求獲得堆疊之控制以劫持程式控制流。一種往往使傳統的資料堆疊容易受到 ROP、JOP 和其它控制流 subversion 攻擊的因素是堆疊通常儲存資料 118 和控制 117 兩者 (例如，資料和返回位址通常在相同的堆疊上混合在一起)。另一個往往使得傳統堆疊容易受到此種攻擊的因素為堆疊之切換一般被執行為非特權操作。這兩個因素可能由於允許堆疊指標和/或控制流資訊 (例如，返回位址) 被修改 (例如，以指向惡意軟體/攻擊者控制的記憶體) 的錯誤 (bug) 驅使增加暴露至控制流 subversion。

[0013] 在一些實施例中，一或多個影子堆疊 120 可被包括及用來幫助保護堆疊 119 不被竄改和/或幫助增加電腦安全性。影子堆疊可代表從堆疊 119 分離之一或多個額外的堆疊類型資料結構。如所示，在一些實施例中，影子堆疊可被用來儲存控制資訊 121 而不是資料 (例如，不是使用者層級應用程式將需要能夠寫入或修改之儲存在堆疊上的參數和其它資料類型)。儲存在影子堆疊上之控制資訊可代表有關於資訊之返回位址 (例如，實際返回位

址、用以驗證返回位址之資訊、其它返回位址資訊）。如一可能的範例，影子堆疊在功能或程序已經呼叫時可被用來儲存已經推送之堆疊 119 之任何返回位址之拷貝（例如，在也已經被推送至一般呼叫堆疊之上的呼叫鏈中的每一返回位址之拷貝）。在一些實施例中，每一影子堆疊也可包括操作辨識影子堆疊之頂部的影子堆疊指標（SSP）。在一些實施例中，影子堆疊可選擇地被配置用於在非特權使用者層級模式（例如，環 3 特權層級）或在特權或監督者特權層級模式（例如，環 0、環 1 或環 2 特權層級）下單獨操作。在一個方面中，多個影子堆疊可潛在地被配置在系統中，但只有每一邏輯處理器在一時間內一影子堆疊可被配置作為當前影子堆疊。

[0014] 如所示，影子堆疊 120 可被儲存在記憶體 114 中。在一些實施例中，當前或有效影子堆疊在推送和/或彈出操作在影子堆疊上執行時可由線性位址範圍定義以幫助偵測和防止堆疊超限和/或堆疊低於下限。在一些實施例中，用以幫助提供額外的保護，影子堆疊可選擇地被儲存在非特權的使用者層級應用程式 116 已經限制和/或不完整的存取之記憶體之保護的部分或存取控制的部分。提供記憶體之合適保護的部分用於儲存影子堆疊之不同方式是可能的。在一些實施例中，影子堆疊可選擇地被儲存在由分頁存取控制保護的記憶體部分中。例如，特權系統軟體 115（例如，操作系統）可配置在相應於其中影子堆疊為了使頁面為可讀取而不是可寫入或可執行而被儲存之頁

面的頁面表登錄中存取權限（例如，讀取-寫入-執行存取權限）。這可幫助防止使用者層級指令（例如，儲存至記憶體指令）移動至記憶體指令以及相似物（從能夠寫入至在影子堆疊中的資料或修改在影子堆疊中的資料）。作為另一部分，在一些實施例中，影子堆疊可選擇地儲存在以那些用於 Intel® Software Guard Extensions (SGX)安全獨立領域中的安全獨立領域、或其它隔離執行環境之容器或相似物等等之相似存取控制保護之被保護的記憶體部分。

[0015] 再次參照圖 1，在一些實施例中，記憶體 101 可為通用（general-purpose）處理器（例如，一般用作為在桌上型、膝上型或其它電腦系統中的中央處理單元（CPU）之類型）。可替代地，處理器可為特定目的處理器。合適的特定目的處理器之範例包括（但不限制於）網路處理器、通訊處理器、密碼處理器、圖形處理器、共處理器、嵌入式處理器、數位訊號處理器（DSP）和控制器（例如，微控制器）。處理器可具有任何各種複雜指令集運算（CISC）架構、精簡指令集運算（RISC）架構、極長指令字（VLIW）架構、混合架構、其它類型架構或具有不同架構之組合（例如，不同核心可具有不同架構）。

[0016] 在一些實施例中，處理器可具有用以幫助管理和保護影子堆疊的一或多個指令和邏輯。處理器具有指令集 102。指令集為處理器之指令集架構（ISA）之一部分且包括處理器操作以執行的本機指令。指令集之指令可代表巨集指令、組合語言指令或提供給處理器執行之機器

層級指令，相對於微指令、微操作或其它已經從指令集之指令解碼之解碼的指令或控制訊號。

[0017] 如所示，在所說明之實施例中，指令集包括呼叫程序或呼叫指令 103 之實施例。指令集也包括從程序返回或返回指令 104 之實施例。指令集也包括保存影子堆疊指標指令 105 之實施例。指令集也包括復原影子堆疊指標指令 106 之實施例。在其它實施例中，處理器可替代選擇地包括如只有這些指令之任何單一個一樣少。實施例係有關於處理器，其用以執行（例如，解碼和執行）任何這些指令中的一或多個。其它實施例係有關於執行（例如，解碼和執行）這些指令中任何一個的方法。

[0018] 在一些實施例中，處理器可包括處理元件或邏輯處理器 108 中的至少一者。為簡單起見，只有顯示單一邏輯處理器，雖然可以理解到處理器可選擇地包括其它邏輯處理器。合適的邏輯處理器範例包括（但不限制於）核心、硬體線程、線程單元、線程擴充槽（slot）以及其它邏輯處理器。邏輯處理器可操作以處理指令集之指令。邏輯處理器可具有用以處理指令的管線或邏輯。藉由舉例的方式，每個管線可包括用以提取指令的指令提取單元、用以解碼指令之指令解碼單元、用以執行解碼的指令之執行單元、用以儲存指令之來源和目的地運算元之暫存器以及相似物。本發明之範圍不限制於任何已知類型或設計的管線。在一些實施例中，邏輯處理器可操作以處理（例如，解碼、執行等等）呼叫指令、返回指令、保存影子堆

疊指標指令和復原影子堆疊指標指令之任何一者或多者。

[0019] 如所示，處理元件或邏輯處理器 108 之至少一者的至少一些邏輯可為處理器之影子堆疊保護邏輯 110 的一部分。在一些實施例中，影子堆疊保護邏輯也可包括可選擇配置影子堆疊模式 111。影子堆疊模式可操作以被配置為交替地賦能和失能影子堆疊之使用。可替代地，影子堆疊可選擇地永遠被賦能且影子堆疊模式可選擇地被省略。影子堆疊保護邏輯也可包括一或多個影子堆疊暫存器 112 之實施例。影子堆疊暫存器可操作以指定有關當前影子堆疊之細節。

[0020] 影子堆疊保護邏輯也可以包括一或多個影子堆疊描述符表（SSDT）暫存器 113 之實施例。SSDT 暫存器可操作以指定有關一或多個 SSDT 122 之細節。如所示，SSDT 可儲存在記憶體中。在一些實施例中，SSDT 可儲存在相同或相似類型之如影子堆疊之保護的記憶體。在一些實施例中，SSDT 可代表操作以儲存有關相應的程式可使用和/或之間切換之影子堆疊的資訊或細節的表或其它資料結構。藉由舉例的方式，特權的系統軟體（例如，操作系統）可儲存有關在 SSDT 中影子堆疊的細節。在一些實施例中，處理器可使用 SSDT 來建立當前影子堆疊以及控制至影子堆疊的存取。藉由舉例的方式，SSDT 可具有多個登錄且每個登錄可定義其中程式允許在程式執行期間使用之相應的影子堆疊的範圍。

[0021] 圖 2 為影子堆疊暫存器 212 之一集合之實施

例和 SSDT 暫存器組 213 之集合的實施例的方塊圖。影子堆疊和 SSDT 暫存器可被包括在處理器之控制暫存器 224 之一集合中。

[0022] 影子堆疊暫存器可操作以指定被用來保護和控制存取至用來儲存當前或有效影子堆疊之記憶體部分的當前或有效影子堆疊之有效範圍。在一些實施例中，所述的範圍可由線性位址範圍指定。影子堆疊暫存器包括影子堆疊基底（SSP base）暫存器 225、影子堆疊限制（SSP limit）暫存器 226 以及影子堆疊指標（SSP）暫存器 227。SSP 基底暫存器可操作以儲存影子堆疊之基底。在一個方面中，SSP 基底可為影子堆疊之最低線性位址。SSP 限制暫存器可操作以儲存影子堆疊之限制。在一個方面中，SSP 基底可為影子堆疊之最高線性位址。SSP 基底至 SSP 限制可以一起指定如作為影子堆疊的記憶體之範圍。處理器中（例如，記憶體管理單元等等）的記憶體存取控制可使用 SSP 基底和 SSP 限制以控制至影子堆疊的存取。在一些實施例中，使用者層級儲存至記憶體指令及相似物可能無法寫入至影子堆疊。寫入至影子堆疊範圍或修改影子堆疊範圍之嘗試可由處理器之硬體來防止（例如，例外情況可以採取）。SSP 暫存器可操作以儲存影子堆疊之當前頂部之位址。例如，SSP 暫存器可儲存表示影子堆疊之當前頂部的線性位址，其係在 SSP 基底和（SSP 限制-1）之間。

[0023] SSDT 暫存器 213 可被操作以指定用來保護和

控制存取至用來儲存當前或有效 SSDT 之記憶體部分的當前或有效 SSDT 之有效範圍。在一些實施例中，在給定的時間中有兩種不同類型之 SSDT 在處理器中有效。也就是，可以為當前或有效特權層級或監督者 SSDT (SSDT-S) 和當前或有效使用者層級 SSDT (SSDT-U)。在一些實施例中，兩個暫存器可被用來為這些不同類型之 SSDT 的每一者撰寫程式至處理器內。在一些實施例中，SSDT 暫存器可包括用來指定當前或有效使用者層級 SSDT (SSDT-U) 之有效範圍的第一對暫存器 228、229 以及用來指定當前或有效監督者 SSDT (SSDT-S) 之有效範圍的第二對暫存器 230、231。使用者 SSDT 基底暫存器 228 可指定用於 SSDT-U 的基底，例如，作為對齊（例如，對齊的 4K 頁面）最低線性位址之頁面。使用者 SSDT 限制暫存器 229 可指定用於 SSDT-U 之限制，例如，作為對齊最高線性位址的頁面。監督者 SSDT 基底暫存器 230 可指定用於 SSDT-S 的基底，例如，作為對齊最低線性位址的頁面。監督者 SSDT 限制暫存器 231 可指定用於 SSDT-S 的限制，例如，作為對齊最高線性位址的頁面。監督 SSDT (SSDT-S) 可由特權系統軟體（例如，操作系統）被撰寫程式至處理器中一次且通常此後可能不需要被改變。在排程新使用者處理時，被有效的每一使用者處理可能有不同使用者 SSDT (SSDT-U)。

[0024] 圖 3 為 SSDT 322 之實施例的方塊圖。SSDT 中可以表示儲存在記憶體中的表或其它資料結構。SSDT

可操作以儲存有關相應的程式被允許在之間使用和/或切換的一或多個影子堆疊資訊或細節。藉由舉例的方式，操作系統或其它特權系統軟體可儲存用於在 SSDT 中每個允許的影子堆疊。SSDT 此後可被檢查（例如，由處理器）以判定影子堆疊之允許的範圍以及控制至影子堆疊的存取。

[0025] 所說明的 SSDT 被佈置為具有複數個列和行的表。不同列表示每一者相應不同有效或無效影子堆疊的不同登錄，其中影子堆疊之相應的程式在程式執行期間被允許被使用。在所說明的範例中，有第一登錄 335-1 至第 N 登錄 335-N，其中登錄之數目（N）可為任何特定實施所需之適當的數目。藉由舉例的方式，每一應用程式可具有由登錄定義之其自身的影子堆疊以及其 SSP 基底和 SSP 限制。所說明的 SSDT 具有三行。

[0026] 第一行儲存用於相應的登錄之有效性指標。如所示，有一個用於第一登錄之第一有效性指標 336-1 以及一個用於第 N 登錄之第 N 有效性指標 336-N。每個有效性指標可被操作以指示無論相應的影子堆疊是有效或無效的。例如，每個有效性指標可具有用以指示相應的影子堆疊是有效的第一值（例如，被設定為二進制一）或可具有用以指示相應的影子堆疊為無效的第二不同值（例如，被清除為二進制零）。

[0027] 第二和第三行指定或儲存用於影子堆疊的有效範圍。具體地，第二行儲存影子堆疊基底（SSP 基底）

及第三行儲存影子堆疊限制（SSP 限制）。如所示，有一個用於第一登錄之第一 SSP 基底 337-1 和用於第 N 登錄之第 N SSP 基底 337-N。同樣地，有一個用於第一登錄之第一 SSP 限制 338-1 和用於第 N 登錄之第 N SSP 限制 338-N。在一些實施例中，SSP 基底和 SSP 限制可分別地表示相應的影子堆疊之最低和最高線性位址。在第一、第二和第三行中的資料在其它實施例中可替代地被不同地重新佈置。此外，在其它實施例中，除了此種表狀結構或佈置外，其它資料結構或資料佈置完全地可任意地被使用。

[0028] 圖 4 為合適的 SSDT 登錄 435 之一特定範例實施例的方塊圖。所說明的特定 SSDT 登錄為 16 位元寬。最低有效位元（位元[0]）表示和/或用於儲存有效性指示。有效性指示當位元[0]被設定為二進制一時具有有效指標以及當位元[0]被清除為二進制零具有無效指標。相反常規為可替代地也是可能的。位元[11:1]和位元[74:64]可表示目前保留的位元（rsvd）。在一特定實施例中，當位元[0]被設定為二進制一且全部在位元[74:64]和[11:1]中保留的位元被清除為二進制零時登錄可以為有效，或以其它方式可能是無效的。可替代地，保留的位元可任意地忽略。位元[63:12]表示和/或使用來儲存 SSP 基底。位元[127:75]表示和/或使用來儲存 SSP 限制。如前面提到的，SSP 基底和 SSP 限制可被用來指定或定義相應於登錄的影子堆疊之有效範圍。在其它實施例中，其他尺寸的 SSDT 登錄可選擇地被使用，且有效性指標、SSP 基底

和 SSP 限制可選擇地以各種不同方式重新佈置或重新定位。

[0029] SSDT 之給定的登錄或列可以使用 SSDT 選擇器來索引。圖 5 為 SSDT 選擇器 540 之範例實施例的方塊圖。特定說明的 SSDT 選擇器為 32 位元數字。可替代地，SSDT 選擇器可選擇地為無論是比 32 位元更寬或更窄。特定說明的 SSDT 選擇器之位元[31]儲存或表示使用者-監督者指標。當位元[31]被設定為二進制一時，使用者監督者指標可具有使用者指標。當位元[31]被清除為二進制零時，使用者監督者指標可具有監督者指標。與此相反的常規也是可能的可選擇地。特定說明的 SSDT 選擇器之位元[30:0]儲存或表示 SSDT 索引。SSDT 索引可被用來索引至 SSDT 內和/或選擇 SSDT 之特定列或登錄。當使用者監督者指標具有使用者指標時 SSDT 索引可索引至使用者 SSDT (SSDT-U) 內，然而當使用者監督者指標具有監督者指標時 SSDT 索引可索引至監督者 SSDT (SSDT-S) 內。在一些實施例中，SSDT 選擇器當在位元[30:0]中的 SSDT 索引係在相應的 SSDT 允許的範圍或邊界內時，可以只有為有效和/或只有允許選擇或索引 SSDT 登錄。此外，SSDT 選擇器可只有選擇或指示選擇的或索引的 SSDT 登錄之有效影子堆疊是有效的（例如，位元[0]被設定為二進制一以及保留的位元全被清除）。

[0030] 在不同實施例中，影子堆疊選擇資訊可儲存在不同位置。作為一可能的範例，在一些實施例中，影子

堆疊選擇可被儲存在一些 Intel®架構相容的電腦內之任務狀態片段（TSS）結構中。可替代地，在其它實施例中，影子堆疊選擇資訊可替代地包括在記憶體內不同資料結構中。在又一其它實施例中，影子堆疊選擇資訊可替代地包括在處理器之控制暫存器內。此種方案之組合也可能是合適的。

[0031] 圖 6 為 32 位元任務狀態片段（TSS）結構 645 之範例實施例之實施例的方塊圖。TSS 可表示管理在被用來儲存有關任務的資訊之 Intel®架構相容的電腦內之記憶體中的資料結構之硬體。處理器和特權系統軟體可使用儲存其中之 TSS 和資訊以執行堆疊切換和/或任務切換。處理器可具有可能指向或指示有效 TSS 片段描述符（descriptor）之任務暫存器（例如，用以儲存片段選擇器之片段暫存器）。為了提升安全性，TSS 可被儲存在記憶體內之其中存取是受控制的和/或其只有對於特權層級軟體為可存取的。

[0032] 如果操作系統或其它特權系統軟體使用處理器特權層級保護機制，任務執行空間可包括用於不同特權層級之不同堆疊（例如，用來儲存控制和資料兩者的呼叫堆疊）。如所示，32 位元 TSS 具有三個 32 位元堆疊指標，標記 ESP0、ESP1 和 ESP2 分別在 SS0、SS1 和 SS2 堆疊片段中偏移。在其它實施中，更少或更多的堆疊指標可選擇地被使用。三個 32 位元堆疊指標可指出或辨識用於三個不同相應的特權層級之三個不同堆疊。具體地，

ESP0 可相應於特權層級零、ESP1 可相應於特權層級一、以及 ESP2 可相應於特權層級二。32 位元堆疊指標當特權層級改變是由當操作在 32 位元模式時的處理器造成時可被用來辨識適當的堆疊。如所示，32 位元 TSS 也具有三個相應的 32 位元堆疊片段選擇器，標記為 SS0、SS1 和 SS2。作為一個範例，當處理器從使用者層級轉換為特權層級零，處理器可檢索堆疊指標 ESP0 和堆疊片段選擇器 SS0（適合用於目標特權層級零），以及儲存它們的值在 ESP 和處理器之 SS 暫存器中。

[0033] 在一些實施例中，如果操作系統或其它特權的系統軟體使用處理器特權層級保護機制，也可能有不同的影子堆疊用於不同特權層級。如所示，在一些實施例中，32 位元 TSS 也可以具有三個 32 位元影子堆疊選擇器，標記為 SSDT 選擇器 0、SSDT 選擇器 1 和 SSDT 選擇器 2。在其它實施中，更少或更多影子堆疊選擇器可選擇地使用。所述三個 32 位元影子堆疊選擇器可指出（或以其他方式辨識）三個不同相應的影子堆疊描述符表（SSDT）登錄用於三個不同相應的特權層級。例如，SSDT 選擇器 0 可指定影子堆疊之 SSDT 登錄在特權層級零使用、SSDT 選擇器 1 可指定影子堆疊之 SSDT 登錄在特權層級一使用、以及 SSDT 選擇器 2 可指定影子堆疊之 SSDT 登錄在特權層級二使用。SSDT 登錄對於相應的處理或任務可被用於儲存用於不同的允許影子堆疊之影子堆疊基底（SSP 基底）和限制（SSP 限制）。32 位元影子堆疊

選擇器（SSDT 選擇器 0、SSDT 選擇器 1 和 SSDT 選擇器 2）可被用來當在處理器之特權層級操作於 32 位元模式下改變時指定合適的 SSDT 登錄用於目標特權層級。例如，當處理器從使用者層級轉變為特權層級零時，處理器（除了檢索 ESP0 和 SS0）可檢索適合用於特權層級零之 32 位元影子堆疊選擇器 SSDT 選擇器 0。檢索的 32 位元影子堆疊選擇器可指出相應的 SSDT 登錄，其中影子堆疊基底（SSP 基底）和影子堆疊限制（SSP 限制）可被獲得。這可允許不同特權層級使用不同的影子堆疊，並且還可以允許不同影子堆疊被用於不同的處理。因此，在 TSS 中的 32 位元影子堆疊選擇器當有特權層級在處理器中改變時，可被用切換影子堆疊。32 位元 TSS 也包括當任務透過相應的 TSS 分配用於執行時，用來建立影子堆疊 TSS SSP 649 和 TSS SSDT 選擇器 648。當處理器執行任務切換時，其可以保存當前任務之 SSP 在當前任務之 TSS 之 TSS SSP 欄位中。接著，處理器可從新任務之 TSS 載入 TSS SSDT 選擇器且使用它來定位 SSP 基底和 SSP 限制用於新的任務之影子堆疊。用於新任務之 SSP 可接著使用來自新任務之 TSS 之 TSS SSP 欄位的值建立。所說明的 SSDT 選擇器、TSS SSP 和 TSS SSDT 之位置和配置不是必需的。在其它實施例中，這些欄位可選擇地位於其他位置及各種重新配置。

[0034] 32 位元 TSS 也具有用以執行任務切換之資料欄位。代表性地，任務可代表可以分配、執行和懸置

(**suspend**) 的處理器之工作單元。藉由舉例的方式，任務可被用於執行一或多個程式、任務或處理、操作系統服務公用程式 (**utility**)、中斷或異常處置器或內核或執行公用程式。在一個方面中，任務切換可在當呼叫程序指令被執行時、跳躍至程序指令被執行時、中斷或異常發生時或其它方式時被執行。當任務切換係從當前任務被執行至新的任務時，當前任務狀態可被保存在相應於當前任務之 **TSS** 中、以及新任務之狀態可從相應於新任務之 **TSS** 載入或檢索。如所示，32 位元 **TSS** 可包括狀態保存欄位 646 來儲存不同類型之處理器狀態。例如，此種欄位可儲存 **CR3** 或頁面目錄基底暫存器 (**PDBR**)、指令指標 (**EIP**)、**EFLAGS** 暫存器、通用目的暫存器 (例如，**EAX**、**ECX**、**EDX** 等等)、片段選擇器 (例如，**ES**、**CS**、**SS** 等等)。32 位元 **TSS** 也可以具有不同欄位 647，其為了簡潔的目的不在本文敘述。

[0035] 圖 7 為 64 位元 **TSS** 結構 745 之範例實施例的方塊圖。64 位元 **TSS** 與 32 位元 **TSS** 具有一些相似性。為了避免模糊敘述，64 位元 **TSS** 之不同或新的特徵將主要進行說明。

[0036] 在 64 位元模式中，如在 32 位元模式，如果操作系統或其它特權系統軟體使用處理器特權層級保護機制，任務執行空間可包括用於不同特權層級之不同堆疊 (例如，用於儲存控制和資料兩者的呼叫堆疊)。如所示，64 位元 **TSS** 具有三個 64 位元堆疊指標，標記

RSP0、RSP1 和 RSP2。64 位元堆疊指標之每一者分為較高和較低 32 位元部分。三個 64 位元堆疊指標可以分別大致對應於 32 位元堆疊指標 ESP0、ESP1 和 ESP2。在其它實施中，更少或更多的堆疊指標可選擇地被使用。RSP0 可相應於特權層級零、RSP1 可相應於特權層級一、以及 RSP2 可相應於特權層級二。64 位元堆疊指標當特權層級改變是由當操作在 64 位元模式時的處理器造成時可被用來辨識適當的堆疊。

[0037] 在一些實施例中，如果操作系統或其它特權的系統軟體使用處理器特權層級保護機制，也可能有不同的影子堆疊用於不同特權層級。如所示，在一些實施例中，64 位元 TSS 也可以具有三個 64 位元影子堆疊選擇器，標記為 SSDT 選擇器 0、SSDT 選擇器 1 和 SSDT 選擇器 2。在其它實施中，更少或更多影子堆疊選擇器可選擇地使用。三個 64 位元影子堆疊選擇器的每一者可指出（或以其他方式辨識）在不同相應的執行特權層級之不同相應的影子堆疊描述符表（SSDT）登錄。SSDT 選擇器 0 可指出影子堆疊之 SSDT 登錄在特權層級零使用、SSDT 選擇器 1 可指出影子堆疊之 SSDT 登錄在特權層級一使用、以及 SSDT 選擇器 2 可指出影子堆疊之 SSDT 登錄在特權層級二使用。64 位元影子堆疊選擇器可被用來當在處理器之特權層級在操作於 64 位元模式下改變時指定合適的 SSDT 登錄用於目標特權層級。如前面所述，辨識的 SSDT 可儲存對於不同用於相應的任務或處理之允許的影

子堆疊之影子堆疊基底（SSP 基底）和 SSP 限制（SSP 限制）。

[0038] 在 64 位元模式中也具有用以在稱為中斷堆疊表（IST）之中斷上切換堆疊的機制。這個機制可允許中斷處置器以使用不同堆疊（例如，儲存控制和資料兩者的呼叫堆疊）。64 位元 TSS 包括七個中斷堆疊表選擇器欄位 IST1 至 IST7。這些欄位之每一者具有下半部和上半部。這七個中斷堆疊選擇器欄位因此可以允許多達七個不同堆疊用於中斷處理。用於呼叫中斷或異常處置器之中斷描述符表登錄可與 IST 索引編寫程式，IST 索引係用來從 IST 選擇七個堆疊中的一者。

[0039] 在一些實施例中，機制也可選擇地用來在中斷或異常處理期間切換影子堆疊。在一些實施例中，64 位元 TSS 可選擇地包括七個中斷影子堆疊表 SSDT 選擇器用於 IST 索引 IST1-IST7 的每一個。這些欄位的每一者可被用來指定被用於中斷處理之影子堆疊。這七個中斷影子堆疊選擇器欄位因此可以允許多達七個不同影子堆疊被用於中斷處理。藉由舉例的方式，當中斷或異常發生時，中斷堆疊表選擇器欄位（例如，IST3）兩者可被用於選擇或辨識新的堆疊，以及中斷影子堆疊表選擇器欄位（例如，SSDT 選擇器 IST3）可被用來選擇或辨識新的影子堆疊。

[0040] 所說明的 SSDT 選擇器之位置和配置和 SSDT 選擇器 IST1-IST7 不是必需的。在其它實施例中，這些欄位可選擇地位於其他位置及各種重新配置。

[0041] 現在，雖然 32 位元模式和 32 位元 TSS 包括硬體管理的任務切換功能，大多數目前的主流操作系統不使用這些硬體管理任務切換功能。因此，64 位元 TSS 省略了許多這些硬體管理任務切換功能。當任務切換係從當前任務執行至新的任務，當前任務之狀態不保存在 64 位元 TSS 中，且新的任務狀態沒有從 64 位元 TSS 檢索。64 位元 TSS 不包含包括在 32 位元 TSS 中的狀態保存欄位 646。

[0042] 圖 8 為操作以執行呼叫程序指令 803 之實施例和從程序指令 804 返回之實施例之處理器 801 之實施例的方塊圖。為簡化敘述，呼叫程序指令將經常簡稱為一個呼叫指令，以及從程序指令的返回將經常簡稱為返回指令。呼叫和返回指令可表示指令或處理器之指令及之控制訊號。

[0043] 在操作期間，處理器可接收呼叫指令 803。例如，呼叫指令可從呼叫次常式、常式、處置器等等之呼叫程序被接收。例如，指令可透過匯流排或其它互連從記憶體接收。在一些實施例中，呼叫指令可明確指定（例如，經由一或多個欄位或位元集）或以其它方式指示（例如，暗示地指示）返回位址 873 作為來源運算元。不限制於，通常返回位址可以為在程式中接著呼叫指令之下一個指令的位址。作為一個範例，指令可具有來源運算元規格欄位以指定暫存器或其它儲存位置，其中返回位址將被儲存。可替代地，暫存器或其它儲存位置可選擇地被暗示至指令

（例如，暗示至指令之操作碼）。作為又一選項，指令可具有直接或其它欄位以提供返回位址之指示。所指示的返回位址可以是實際的位址或至返回位址之偏移（例如，從接著呼叫指令之指令偏移）至返回位址。

[0044] 處理器也包括暫存器 872 之一集合。在一些實施例中，暫存器代表通用目的暫存器。如所示，在一些實施例中，返回位址 873 可選擇地被儲存在暫存器中。可替代地，其它儲存位置可選擇地被使用。

[0045] 處理器有包括解碼單元或解碼器 870。解碼單元可接收或解碼呼叫指令為一或多個解碼的指令或控制訊號。處理器也包括與解碼單元 870 和暫存器 872 耦接並且可操作的耦接或以其它方式與記憶體 874 通訊之呼叫執行單元 871C。呼叫執行單元可接收一或多個解碼的指令或控制訊號。呼叫執行單元也可接收指示的返回位址 873。在一些實施例中，呼叫執行單元可操作以回應和/或作為呼叫指令之結果（例如，回應於一或多個解碼的指令或由此解碼的控制訊號）以推送或其它方式儲存返回位址（以及 CS 如果遠呼叫）到堆疊 875。在一些實施例中，呼叫執行單元也可以被操作以回應和/或作為呼叫指令之結果（例如，回應於一或多個解碼的指令或由此解碼的控制訊號）以推送或其它方式儲存返回位址（以及 CS 如果遠呼叫）到影子堆疊 877。

[0046] 在一些實施例中，即使當關聯於影子堆疊之存取權限指示影子堆疊不可寫入時，呼叫執行單元可操作

以推送或其它方式儲存返回位址（以及 CS 如果遠呼叫）到影子堆疊。例如，在一些實施例中，具有影子堆疊之記憶體部分可由分頁保護。在一些實施例中，特權系統軟體（例如，操作系統）可配置存取權限在用於具有影子堆疊以使它們不可寫入（例如，使它們僅可讀取）之分頁的分頁表登錄中。在一些實施例中，這可有效地防止其它儲存至記憶體、寫入至記憶體、移動至記憶體以及從能夠儲存或寫入至影子堆疊之相同指令集之此種指令。然而，即使當此種存取權限指示影子堆疊為不可寫入時，回應呼叫指令之呼叫執行單元可被操作以儲存返回位址至堆疊上。也就是，回應呼叫指令之呼叫執行單元可忽略在對於使用於影子堆疊之分頁之分頁表登錄中的不可寫入之存取權限。然而，此種存取保護可以防止使用者層級軟體從能夠修改影子堆疊內容（例如，儲存至記憶體指令）中有效。此外，相似異質儲存能力可選擇地替以其它不同類型之存取權限（例如，用於保護的獨立領域或其它保護的容器）實施替代。

[0047] 在一些實施例中，於呼叫執行單元儲存返回位址在影子堆疊上之前，呼叫執行單元可被操作以執行一或多個額外的安全確認或保護。在一些實施例中，呼叫執行單元可確認影子堆疊是否為賦能。如果影子堆疊為賦能的，呼叫執行單元可以繼續，否則它可能停止而沒有儲存返回位址在影子堆疊上。

[0048] 在一些實施例中，於推送或儲存返回位址在

影子堆疊上之前，呼叫執行單元可被操作以確認或判定是否推送或儲存將導致影子堆疊指標（SSP）超過由影子堆疊基底（例如，超過 SSP 基底）所定義之允許的範圍之新的返回位址。例如，呼叫執行單元可被操作以減去影子堆疊之所需寬度以處理來自當前 SSP 之返回位址（例如，被推送之位元組數目）。影子堆疊可以向下增長，如傳統的堆疊常做的。最低位址或 SSP 可在影子堆疊為空的時候使用。在執行儲存之前，儲存返回位址在堆疊上可遞減或減少影子堆疊位址或 SSP。藉由舉例的方式，在一些英特爾架構處理器中，影子堆疊寬度可取決於模式為 4 位元組或 8 位元組。呼叫執行單元可操作以判定所得的 SSP 在藉由影子堆疊之寬度遞減 SSP 之後是否小於影子堆疊基底（SSP 基底）。如果如此，返回位址之嘗試推送可被認為超出邊界且可能不被執行。例如，堆疊故障（#SS）或其他異常情況可以斷言。否則，呼叫執行單元可在結果遞減的或減少的 SSP 推送或儲存返回位址在影子堆疊上。

[0049] 此種確認或防範影子堆疊超過允許的影子堆疊範圍可幫助防範被儲存在保護的影子堆疊範圍外側之一般/標準未保護記憶體中。否則，這可能允許返回位址存在於其中它們可能潛在地被修改或篡改之保護的影子堆疊範圍的外側。因此，影子堆疊範圍可幫助確認呼叫指令僅被允許儲存返回位址在影子堆疊保護的範圍之中。

[0050] 接著，處理器可接收返回指令 804。例如，返回指令可以為返回控制流回到呼叫它的程序中的呼叫次常

式、處置器、常式或程序之最後指令。

[0051] 解碼單元 870 可接收或解碼返回指令為一或多個解碼的指令或控制訊號。處理器包括與解碼單元 870 耦接之返回執行單元 871R 且係操作以與記憶體 874 耦接或以其它方式與記憶體 874 通訊。返回執行單元可以是如用於呼叫指令之相同的執行單元或不同的執行單元。為了增進圖式的明確性，示出不同的執行單元，雖然這不是必須的。

[0052] 在一些實施例中，返回執行單元 871R 可被操作以回應和/或作為返回指令之結果（例如，回應於一或多個解碼的指令或或由此解碼的控制訊號）以從堆疊 875 彈出或其它方式接收 882 返回位址 876（以及 CS 在遠呼叫之情況下）以及從影子堆疊 877 彈出或其它方式接收 884 返回位址 878（以及 CS 在遠呼叫之情況下）。在一些實施例中，返回執行單元可操作以回應和/或作為返回指令之結果成為限制或有關於使用或基於儲存在影子堆疊上之返回位址（例如，返回位址資訊）之到返回位址之返回的控制流的限制。

[0053] 在一些實施例中，返回執行單元可被操作以回應和/或作為返回指令之結果來驗證或確保儲存在堆疊上之返回位址的完整性。例如，返回執行單元可被操作以判定儲存在堆疊上之返回位址和影子堆疊是否相等、匹配或以其它方式相容。返回執行單元可被操作以比較在堆疊上之返回位址與在影子堆疊上之返回位址資訊（例如，返

回位址之拷貝、返回位址之雜湊等等)。在一些實施例中，相同返回位址可被儲存在堆疊和影子堆疊兩者中，所以這兩個值為了匹配或相容而相等或相同。如果返回位址資訊被判定為相容，返回執行單元可允許控制流轉移到返回地址。例如，返回執行單元可被操作以導致返回位址被儲存在指令指標暫存器 880 中。相反，如果返回位址資訊被判定為不相容，接著返回執行單元不允許控制流轉移到堆疊上之返回位址。例如，返回執行單元可被操作以採取異常 885 (例如，控制保護異常) 至處置器模組 (例如，特權系統)。優選地，在不匹配或不相容資訊情況下限制或限定控制流轉移至在堆疊上的返回位址可幫助防止 ROP 和其它控制流子版本攻擊或至少使啟動它們顯著地難。

[0054] 可替代地，取代比較儲存在堆疊上之返回位址資訊和影子堆疊，返回執行單元可使用儲存在影子堆疊上之返回位址資訊以提供其他方式的保護。例如，在其它實施例中，返回執行單元可操作以回應和/或作為返回指令之結果以在影子堆疊上之返回位址覆寫在堆疊上之返回位址。在又一其它實施例中，返回執行單元可被操作以直接地使用儲存在影子堆疊上之返回位址以跳躍或其它方式返回控制流轉移至返回位址，而不是使用堆疊上之返回位址。例如，在影子堆疊上之返回位址可被儲存在指令指標暫存器中。

[0055] 在一些實施例中，在返回執行單元彈出或其它方式檢索來自影子堆疊之返回位址之前，返回執行單元

可選擇地被操作以執行一或多個額外的安全確認或保護。在一些實施例中，返回執行單元可被操作以確認影子堆疊使否被去能。如果影子堆疊被去能，接著返回執行單元可進行，否則其可能暫停而不儲存從影子堆疊檢索的返回位址。在一些實施例中，在彈出或從影子堆疊檢索返回位址之前，返回執行單元可操作以確認或判定是否彈出或檢索將從超過由影子堆疊限制（SSP 限制）定義之允許的邊界的位址所讀取之返回位址。影子堆疊可以向下增長，如傳統的堆疊常做的。當返回位址彈出或以其它方式從堆疊移除，影子堆疊位址或 SSP 在內容從影子堆疊讀取之後可遞增或以其它方式增加。返回執行單元在從影子堆疊讀取內容之第一或最後的位元組之前可操作以判定 SSP 是否超過限制（SSP 限制-1）。藉由舉例的方式，在一些英特爾架構處理器中，影子堆疊寬度可取決於模式為 4 位元組或 8 位元組。如果是這樣，從影子堆疊之返回位址或資料之嘗試彈出或移除可被認為是在邊界外且不得執行。例如，返回執行單元可以斷言堆疊故障（#SS）或其他異常情況。因此嘗試在超出由特權系統軟體定義之影子的限制做出影子堆疊操作可能會失敗且導致異常。否則，該影子堆疊 [SSP] 之頂部的當前內容可彈出或從影子堆疊檢索。

[0056] 此種確認和防範影子堆疊超過允許的影子堆疊範圍有助於防止資料從在一般/標準未保護的記憶體中保護的影子堆疊範圍之外側存取。否則，這可允許潛在地修改在將由返回指令使用之保護的影子堆疊範圍外側之返

回位址。因此，影子堆疊範圍可幫助確認返回指令僅允許從在影子堆疊保護的範圍中檢索返回位址。

[0057] 本文中 also 揭露的是保存 SSP 指令和復原 SSP 指令。在一些實施例中，這些指令可被用來在使用層級或使用使用者模式線程切換期間幫助管理和保護 SSP。線程切換可包括暫停第一線程之執行（例如，在硬體線程、核心或其它邏輯處理器）和開始第二線程之執行。通常，此種線程切換也包括上下文切換。在上下文切換中，暫停的線程（例如，第一線程）之當前上下文或狀態可被保存。接著，當暫停的線程稍後回復時，保存的上下文或狀態可被復原使得重新啟動線程可在其中其離開的點被回復。影子堆疊上下文包括表示以安全和保護的方式下亦應被保存及復原的上下文之 SSP。保存 SSP 指令和復原 SSP 指令可幫助切換影子堆疊以及以不妥協影子堆疊的安全性之安全和保護的方式保存和復原 SSP。在一些實施例中，使用者層級應用程式不應能夠任意操作 SSP。例如，當從第一線程切換至第二線程時，其僅可被允許切換至其中先前執行離開之第二線程中的相同點，而不是在其它任意的點。換句話說，當切換至第二線程時，使用者層級應用程式可能僅能夠使用相同 SSP，其為先前第二線程在當它上次停止運行時有的。有利地，在一些實施例中，保存 SSP 指令和復原 SSP 指令可為在非特權或執行特權之使用者層級執行的使用者層級指令。這可能有助於避免需要特權的系統軟體執行 SSP 之保存和復原且有助於使用者層級多線程。

[0058] 圖 9 為執行保存影子堆疊指標指令之實施例的方法 987 實施例的方塊流程圖。在各種實施例中，方法可由處理器、指令處理設備或其它數位邏輯裝置執行。

[0059] 方法包括在方塊 988 接收保存影子堆疊指標指令。在各種方面中，指令可在處理器或處理器的一部分（例如，指令提取單元、解碼單元、匯流排介面單元等等）接收。在各種方面中，指令可從處理器外和/或晶圓外（例如，從記憶體、互連等等）接收，或從處理器上和/或晶圓上（例如，從指令快取、指令佇列等等）。在一些實施例中，保存影子堆疊指標指令可指定（例如，明確地指定）或以其它方式指定（例如，隱含地指定）目的地暫存器、記憶體中的位置或其它儲存位置。藉由舉例的方式，目的地儲存位置可選擇地為可以是由指令明確地指定或隱含地指定的通用目的暫存器。

[0060] 在方塊 989，當前影子堆疊指標（SSP）可被推送或以其它方式儲存至當前影子堆疊以回應和/或作為指令的結果。在一些實施例中，當前 SSP 可從處理器之控制暫存器存取且接著儲存在當前影子堆疊之當前頂部。

[0061] 在方塊 990，在儲存當前 SSP 至當前影子堆疊之後，新的或更新的 SSP（例如，反應任何由於儲存或推送之 SSP 遞減或減少）可被儲存在回應於和/或作為指令之結果的指定目的地儲存位置。但不限制於，軟體可保存儲存在目的地之 SSP 使得當切換回被暫停之線程時其可以再次呈現（例如，藉由復原 SSP 指令）。這有助於允許

執行在其中線程離開的點回復。

[0062] 所說明的方法包括架構操作（例如，那些從軟體角度為可視）。在其它實施例中，方法可選擇地包括一或多個微架構操作。藉由舉例的方式，指令可被提取、解碼、排程失序、來源運算元可被存取、執行單元可執行微架構操作以實施指令等等。

[0063] 圖 10 為操作以執行保存 SSP 指令 1005 之實施例的處理器 1001 之實施例的方塊圖。在一些實施例中，處理器 1001 可執行圖 9 之方法 987。本文敘述之用於處理器 1001 的組件、特徵及具體可選擇細節也可選擇地應用於方法 987。可替代地，方法 987 可被由執行相似或不同處理器或設備執行或在相似或不同處理器或設備之內。此外，處理器 1001 可執行相似或不同於方法 987 之方法。

[0064] 在操作期間，處理器可接收保存 SSP 指令 1005。例如，指令可透過匯流排或其它互連從記憶體接收。指令可代表處理器之指令集的指令或控制訊號。在一些實施例中，保存 SSP 指令可明確地指定（例如，透過一或多個欄位或位元組）或以其它方式指示（例如，隱含地指示）其中結果被儲存之目的地儲存位置 1097。作為一個範例，指令可具有目的地規格欄位以指定暫存器、記憶體位置或其它作為目的地儲存位置之儲存位置。可替代地，這些儲存位置之一或多個可選擇地對於指令為隱含（例如，對於指令之操作碼隱含）。如所示，在一些實施

例中，目的地儲存位置（DEST）1097 可選擇地為處理器之暫存器組 1072（例如，通用目的暫存器）之暫存器。

[0065] 處理器也包括解碼單元或解碼器 1070。解碼單元可接收和解碼保存 SSP 指令為一或多個解碼的指令或控制訊號。處理器也包括保存 SSP 執行單元 1071。保存 SSP 執行單元也可以簡稱為一個執行單元。執行單元可與解碼單元 1070 和暫存器 1072 耦接。執行單元也可以與處理器之 SSP 暫存器 1012 耦接。當處理器在系統中採用時，執行單元可被操作以與記憶體 1074 耦接或以其它方式與記憶體 1074 通訊。執行單元可接收一或多個解碼的指令或控制訊號。

[0066] 在一些實施例中，執行單元也可以操作以回應和/或作為保存 SSP 指令之結果（例如，回應於一或多個解碼的指令或由此解碼的控制訊號）以檢索或以其它方式從 SSP 暫存器 1012 接收當前 SSP 1096。執行單元也可操作以回應和/或作為指令的結果以推送或以其它方式如當前 SPP 1092 儲存接收的當前 SPP 1096 在影子堆疊 1077 之上。換句話說，執行單元可保存在影子堆疊上之當前 SSP 1096 之拷貝。影子堆疊可提供安全且保護的地方以儲存其中使用者層級軟體不能夠對其進行修改或篡改它之當前 SSP。影子堆疊也可選擇地儲存返回位址資訊 1017，雖然這不是必需的。

[0067] 執行單元也可以操作以回應和/或作為指令之結果（在儲存當前 SSP 至影子堆疊）用以儲存新的或更新

的當前 SSP 1091 至由指令指定的目的地儲存位置 1097。新的 SSP 可反應由於在影子堆疊上之當前 SSP 的儲存之 SSP 遞減或減少。儲存在目的地中的新的 SSP 代表其中線程暫停的執行或離開之點。但不限制於，軟體可保存新的 SSP 使得新的 SSP 可在其中線程以先前離開的點重新啟動或切換回線程的時候呈現。藉由舉例的方式，如將在下面進一步討論，新的 SSP 可提供作為復原 SSP 指令之來源運算元。然而，在一些實施例中，目的地儲存位置可以不為足夠保護的位置（例如，目的地儲存位置可為通用目的暫存器、位於常規/一般記憶體中或相似物）且軟體可潛在地能夠修改在目的地儲存位置中新的 SSP。因此，如將在下面進一步討論，儲存在影子堆疊上之當前 SSP 1092 可被用來驗證任何此種呈現的 SSP（例如，回應於和/或作為復原 SSP 指令之結果）。

[0068] 在一些實施例中，在儲存當前 SSP 1092 在影子堆疊上之前，執行單元可被操作以回應和/或作為指令之結果以確認或判定是否推送或儲存當前 SSP 至將導致 SSP 超過由用於當前影子堆疊之影子堆疊基底定義之允許的邊界之影子堆疊上。例如，執行單元被操作以減去所需用來處理來自當前 SSP 之當前 SSP（例如，被推送之位元組數目）的影子堆疊寬度。執行單元可被操作以判定結果的 SSP 是否將少於影子堆疊基底。如果是，當前 SSP 之嘗試的推送可被認為為超出邊界且可能不被執行。例如，堆疊故障（#SS）或其他異常情況可以斷言。否則，執行

單元可儲存當前 SSP 至影子堆疊上在結果遞減的或減少的 SSP。

[0069] 圖 11 為執行復原影子堆疊指標指令之實施例的方法 1101 實施例的方塊流程圖。在各種實施例中，方法可由處理器、指令處理設備或其它數位邏輯裝置執行。

[0070] 在方塊 1102，方法包括接收復原影子堆疊指標指令。在一些實施例中，復原 SSP 指令可指定（例如，明確地指定）或以其它方式指定（例如，隱含地指定）SSP 以及可指定或以其它方式指定影子堆疊描述符表（SSDT）選擇器。藉由舉例的方式，指令可指定或指示暫存器（例如，通用目的暫存器）或其它具有 SSP 或 SSDT 選擇器之儲存位置。

[0071] 方法包括執行數個回應於和/或作為指令之結果的驗證或保護。

[0072] 在方塊 1103，作出一個 SSDT 選擇器（例如，由指令提供的一者）是否指示在 SSDT 中有效登錄之判定。如果 SSDT 選擇器指示在 SSDT 中的有效登錄（即，如果「是」為做出的判定），方法可前進之方塊 1104。否則，（即，如果「否」為做出的判定）方法可前進之方塊 1108。

[0073] 在方塊 1104，作出一個由指令指示的 SSP 是否在 SSP 基底和 SSP 限制中的判定，其中 SSP 基底和 SSP 限制係指定在由 SSDT 選擇器（例如，由指令提供的一者）指示或選擇的 SSDT 之登錄。如果 SSP 係在 SSP 基

底和 SSP 限制之中（即，如果「是」為做出的判定），方法可前進至方塊 1105。否則，（即，如果「否」為做出的判定）方法可前進之方塊 1108。

[0074] 在方塊 1105，作出一個由指令指示之 SSP 是否等於、匹配或以其它方式相容於從影子堆疊接收的 SSP。在一些實施例中，從影子堆疊接收的 SSP 可以是由前述保存 SSP 指令儲存在那裡的之一者。在其它實施例中，雜湊可被用於 SSP 值的一者使得相容性不需要如此限制為匹配或相等而是可以透過轉換（例如，雜湊）的相容性。如果 SSP 係相容的（即，如果「是」為做出的判定），方法可前進至方塊 1106。否則，（即，如果「否」為做出的判定）方法可前進之方塊 1108。

[0075] 如果任何方塊 1103、1104 和 1105 之驗證或保護失敗，方法可前進至方塊 1108。在方塊 1108，異常可被採取，且指令可接著完成而沒有復原影子堆疊的狀態或上下文。

[0076] 可替代的，如果任何方塊 1103、1104 和 1105 之驗證或保護成功，方法可前進至方塊 1107。在方塊 1107，影子堆疊的狀態或上下文可回應於和/或作為指令之結果被復原。在一些實施例中，如在方塊 1107 所示，從由 SSDT 選擇器選擇的 SSDT 之登錄獲得的 SSP 基底和 SSP 限制可被儲存在處理器（例如，影子堆疊暫存器 112）之控制暫存器中。在一些實施例中，如在方塊 1107 所示，SSP 也可以儲存在處理器（例如，影子堆疊暫存器

112) 之控制暫存器中。在一些實施例中，來自指令之來源運算元之驗證的 **SSP** 可被儲存在控制暫存器內。在其它實施例中，從影子堆疊檢索之 **SSP** 可被儲存在控制暫存器內。

[0077] 所說明的方法包括架構操作（例如，那些從軟體角度為可視）。在其它實施例中，方法可選擇地包括一或多個微架構操作。藉由舉例的方式，指令可被提取、解碼、排程失序、來源運算元可被存取、執行單元可執行微架構操作以實施指令等等。

[0078] 圖 12 為操作以執行復原 **SSP** 指令 1206 之實施例的處理器 1201 之實施例的方塊圖。指令可代表處理器之指令集之指令或控制訊號。

[0079] 在一些實施例中，復原 **SSP** 指令可明確的指定（例如，透過一或多個欄位或位元組）或以其它方式指示（例如，隱含地指示）就是用來儲存 **SSP** 1291 之第一來源運算元（**SRC1**）1295，以及可指定或以其它方式指示就是用來儲存影子堆疊描述符表（**SSDT**）選擇器 1299 之第二來源運算元（**SRC2**）1294。作為一個範例，指令可具有來源和/或目的地運算元規格欄位以指定暫存器、記憶體位置或其它用於運算元之儲存位置。可替代地，這些運算元的一或多個可選擇地對於指令為隱含（例如，對於指令之操作碼隱含）。如所示，在一些實施例中，第一和第二來源運算元可選擇地儲存在處理器之暫存器 1272 之一集合（通用目的暫存器）之暫存器中。可替代地，記

記憶體位置或其它儲存位置可選擇地用於這些運算元之一或多者。

[0080] 處理器也包括解碼單元或解碼器 1270。解碼單元可接收和解碼復原 SSP 指令為一或多個解碼的指令或控制訊號。處理器也包括復原 SSP 執行單元 1271。復原 SSP 執行單元也可以簡單地稱為一個執行單元。執行單元可與解碼單元和暫存器耦接。當處理器在系統中採用時，執行單元可被操作以與記憶體 1274 耦接或以其它方式與記憶體 1274 通訊。執行單元可接收一或多個解碼的指令或控制訊號。執行單元也可接收 SSP 1291 和 SSDT 選擇器 1299。

[0081] 在一些實施例中，執行單元 1271 也可以操作以回應和/或作為復原 SSP 指令之結果（例如，回應於一或多個解碼的指令或由此解碼的控制訊號）以在復原影子堆疊上下文或狀態之前執行數個驗證或保護。在一些實施例中，執行單元可操作以使用 SSDT 選擇器 1299 以選擇或指示在 SSDT 1222 中的登錄 1235，以及判定登錄為有效或無效，以回應於和/或作為指令之結果。如果登錄不是有效的，指令可以完成而不復原影子堆疊的狀態或上下文，且在一些實施例可採取異常 1293（例如，至處置器模組 1279）。否則，執行單元可繼續執行一或多個其它驗證。在一些實施例中，驗證可以以如上面圖 3 所述判定（例如，使用有效性指標和可選擇的保留位元之值）。

[0082] 在一些實施例中，執行單元可被操作以判定

由第一來源運算元指示的 SSP 1291 是否在 SSP 基底 1237 和 SSP 限制 1238，其中 SSP 基底 1237 和 SSP 限制 1238 由回應於和/或作為指令之結果的 SSDT 選擇器 1299 選擇的 SSDT 1222 之驗證的有效登錄 1235 指定。如果 SSP 不在 SSP 基底和 SSP 限制之中，指令可以完成而不復原影子堆疊的狀態或上下文，且在一些實施例可採取異常 1293。否則，執行單元可繼續執行一或多個其它驗證。

[0083] 在一些實施例中，執行單元可被操作以判定第一來源運算元之 SSP 1291 是否等於、匹配或以其它方式相容於儲存在回應於和/或作為指令之結果的影子堆疊 1277 上之當前 SSP 1292。在一些實施例中，SSP 1292 可能已經被一個前面保存的 SSP 指令儲存在影子堆疊（例如，指令 1005）。如果它們不匹配或以其它方式相容，指令可完成而沒有復原影子堆疊的狀態或上下文，且在一些實施例中可能採取異常 1293。此外，在一些實施例中，執行單元可判定由指令指示的 SSDT 選擇器 1299 和 SSP 1291 充分地驗證。確認此種相容性可幫助確保使用者層級應用程式不能夠任意的操作 SSP。

[0084] 在一些實施例中，執行單元可選擇地操作為零、無效、改變或其它方式妥協儲存在回應於和/或作為指令之結果的影子堆疊上之當前 SSP 1292，儘管這不是必需的。這可幫助確保當前 SSP 僅被使用一次且不能再次使用，其可幫助提供進一步保護。

[0085] 在一些實施例中，執行單元可被操作以（在

充分地驗證 SSDT 選擇器 1299 和 SSP 1291 之後) 儲存影子堆疊的上下文或狀態，以回應和/或作為指令的結果。例如，在一些實施例中，執行單元可被操作以儲存來自登錄 1235 之 SSP 基底 1237 在處理器之影子堆疊暫存器 1212 之一集合之 SSP 基底暫存器 1225 中、用以儲存來自登錄之 SSP 限制 1238 在 SSP 限制暫存器 1226 中以及用以儲存 SSP 在 SSP 暫存器 1227 中。在一些實施例中，第一來源運算元之 SSP 1291 可儲存在 SSP 暫存器 1227 中。在其它實施例中，來自影子堆疊之 SSP 1292 可被儲存在 SSP 暫存器 1227 中。

[0086] 應能理解到這僅是復原 SSP 指令之示例性實施例且其由處理器執行。在其它實施例中，更少或更多驗證可在取決於用於特定實施之所需要的保護層級回復影子堆疊的上下文之前被選擇地執行。其它實施例有關於那些執行除了任選的其他驗證或保護外任何上面敘述的驗證或保護一或多者之復原 SSP 指令。

[0087] 處理器已經在圖 8、10 和 12 示出和敘述。在一些實施例中，這些處理器可為通用目的處理器（例如，前面敘述的類型）。可替代地，處理器可為特定目的處理器（例如，前面敘述的類型）。處理器可具有 CISC、RISC、VLIW、混合或其它架構或它們的組合。

[0088] 圖 8、10 和 12 之解碼單元可被操作以執行所接收的更高層級指令，以及輸出一或多個相對更低層級指令或控制訊號（例如，一或多個微指令、微操作、巨集碼

登錄點、解碼的指令或控制訊號等等），其反應、代表相對更高層級指令和/或從接收的相對更高層級指令衍生。在一些實施例中，解碼單元可包括用以接收指令、指令識別和與其耦接用以識別和解碼指令之解碼邏輯的一或多個輸入結構（例如，埠、互連、介面）、以及與其耦接用以輸出較低層級指令或控制訊號的一或多個輸出結構（例如，埠、互連、介面）。解碼單元可使用各種不同包括但不限制於微碼唯讀記憶體（ROM）、查找表（look-up table）、硬體實施、可程式邏輯陣列（PLA）、和其它適合實施解碼單元的機制之不同機制實施。

[0089] 在一些實施例中，取代指令被直接提供至解碼單元，指令仿真器、轉譯器、漸變器(morpher)、解譯器或其他指令轉換模組可選擇地使用。各種類型之指令轉換模組可實行於軟體、硬體、韌體或其組合中。在一些實施例中，指令轉換模組可位於處理器外側，諸如，例如在分開晶粒上和/或記憶體中（例如，靜態、動態或運行時間仿真模組）。藉由舉例的方式，指令轉換模組可接收指令（其可為第一指令集之指令）且可仿真、轉譯、漸變、解釋或以其它方式轉換指令為一或多個相應的中間指令或控制訊號（其可以為第二不同指令集之指令或控制訊號）。第二指令集的一或多個中間指令或控制訊號可提供至解碼單元，其可以解碼它們為可由處理器（例如，執行單元）之本地硬體可執行之一或多個較低層級指令或控制訊號。

[0090] 圖 8、10 和 12 之暫存器可代表可被操作以儲

存資料之晶粒上儲存位置。暫存器可代表可架構地可視或為對於軟體和/或程式編輯器為架構暫存器和/或為由用以辨識運算元之處理器之指令集之指令指示的暫存器。這些架構暫存器對比於在給定的微架構（例如，暫態暫存器、重排序緩衝器、撤回暫存器等等）中的其它非架構暫存器。暫存器可以以不同方式實施在不同微架構中且不限於任何特定類型之設計。合適類型之暫存器範例包括（但不限制於）專用的實體暫存器、使用暫存器重新命名的動態分配實體暫存器及其它們的組合。

[0091] 圖 8、10 和 12 之執行單元可與解碼單元耦接用以接收代表和/或從解碼的指令衍生的一或多個解碼的或以其它方式轉換的指令或控制訊號。執行單元可操作以回應和/或作為相應的指令之結果（例如，從相應的指令解碼的之回應於一或多個指令或控制訊號）用以執行所敘述之相應的指令之操作。執行單元和/或處理器可包括操作以執行相應的指令之具體或特定邏輯（例如，電晶體、積體電路或其它潛在地與韌體（例如，儲存在非揮發性記憶體中的指令）和/或軟體結合之硬體）。

[0092] 為了避免模糊敘述，圖 8、10 和 12 之處理器已經以簡化格式顯示。然而，處理器可選擇地包括其它處理器組件。例如，各種不同實施例可包括各種於任何圖 13-15 中所示和所敘述之組件不同組合和配置。處理器之所有組件可被耦接在一起以允許它們按預期操作。

核心架構、處理器及電腦架構實施例

[0093] 處理器核心可以不同方式、用於不同目的、及於不同處理器實施。舉例言之，此種核心的實施可包括：1)意圖用於通用運算的通用有序核心；2)意圖用於通用運算的高效能通用失序核心；3)主要意圖用於圖形及科學(資料通量)運算的特用核心。不同處理器的實施可包括：1)一 CPU 包括一或多個意圖用於通用運算的通用有序核心和/或一或多個意圖用於通用運算的通用失序核心；及 2)一處理器包括一或多個主要意圖用於圖形及科學(資料通量)運算的特用核心。此等不同處理器結果導致不同的電腦系統架構可包括 1)共處理器在與 CPU 分開的晶片上；2)共處理器在與 CPU 相同封裝體內的分開晶粒上；3)共處理器在與 CPU 相同的晶粒上(於該種情況下，此種共處理器偶爾係稱作特殊用途邏輯，諸如集成圖形和/或科學(資料通量)邏輯，或稱作特用核心)；及 4)單晶片系統可包括在與 CPU 相同的晶粒上(偶爾稱作應用核心或應用處理器)、前述共處理器、及額外功能。其次描述核心架構實施例，接著描述處理器及電腦架構實施例。

核心架構實施例

有序及失序核心方塊圖

[0094] 圖 13A 根據本發明實施例示出有序管線之實施例及暫存器重新命名、失序簽發/執行管線之實施例二者的方塊圖。圖 13B 根據本發明實施例示出包括在處理器

中有序架構核心之範例實施例及範例暫存器重新命名、失序簽發/執行架構核心二者的方塊圖。圖 13A-B 的實線框例示說明有序管線及有序核心，而虛線框的選擇性添加例示說明暫存器重新命名、失序簽發/執行管線及核心。假設有序方面為失序方面的一子集，將描述失序方面。

[0095] 於圖 13A 中，一處理器管線 1300 包括一提取階段 1302、一長度解碼階段 1304、一解碼階段 1306、一配置階段 1308、一重新命名階段 1310、一排程(又稱為調度或簽發)階段 1312、一暫存器讀取/記憶體讀取階段 1314、一執行階段 1316、一回寫入/記憶體寫入階段 1318、一例外處理階段 1322、及一確定階段 1324。

[0096] 圖 13B 顯示處理器核心 1390 包括一前端單元 1330 耦接至一執行引擎單元 1350，二者係耦接至一記憶體單元 1370。核心 1390 可為精簡指令集計算(RISC)核心、複雜指令集計算(CISC)核心、極長指令字組(VLIW)核心、或一混成體或其它核心類別。至於又另一選項，核心 1390 可為特用核心，諸如網路或通訊核心、壓縮引擎、共處理器核心、通用計算圖形處理單元(GPGPU)核心、圖形核心等。

[0097] 前端單元 1330 包括一支預測單元 1332 耦接至一指令快取單元 1334，其係耦接至指令轉譯後備緩衝器(TLB)1336，其係耦接至一指令提取單元 1338，其係耦接至一解碼單元 1340。解碼單元 1340(或解碼器)可解碼指令，產生一或多個微操作、微碼進入點、微指令、其

它指令、或其它控制信號作為輸出，其係從原先指令解碼，或以其它方式反映、或推衍。解碼單元 1340 可使用多種不同機構實施。適當機構的實施例包括但非僅限於詢查表、硬體實施、可規劃邏輯陣列(PLA)、微碼唯讀記憶體(ROM)等。於一個實施例中，核心 1390 包括一微碼 ROM 或針對一些巨集指令儲存微碼的其它媒體(例如於解碼單元 1340 內或否則於前端單元 1330 內部)。解碼單元 1340 係耦接至執行引擎單元 1350 內部的重新命名/配置器單元 1352。

[0098] 執行引擎單元 1350 包括重新命名/配置器單元 1352，耦接至撤回單元 1354 及一或多個程器單元 1356 之集合。排程器單元 1356 表示任何數目的不同排程器，包括保留站、中央指令窗等。排程器單元 1356 係耦接至實體暫存器檔案單元 1358。實體暫存器檔案單元 1358 各自表示一或多個實體暫存器檔案，其中之不同者儲存一或多個不同資料類別，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(例如指令指標器其為欲執行的下個指令的位址)等。於一個實施例中，實體暫存器檔案單元 1358 包含向量暫存器單元、寫入遮罩暫存器單元、及純量暫存器單元。此等暫存器單元可提供架構向量暫存器、向量遮罩暫存器、及通用暫存器。實體暫存器檔案單元 1358 被撤回單元 1354 重疊以例示說明可實施暫存器重新命名與失序執行的多種方式(例如使用重新排序緩衝器及撤回暫存器檔案，使用未來檔案、歷史緩

衝器及撤回暫存器檔案；使用暫存器映射表及一匯集物之暫存器等)。撤回單元 1354 及實體暫存器檔案單元 1358 係耦接至執行叢集 1360。執行叢集 1360 包括一或多個執行單元 1362 之一集合及一或多個記憶體存取單元 1364 之一集合。執行單元 1362 可對各型資料(例如純量浮點、緊縮整數、緊縮浮點、向量整數、向量浮點)執行各項操作(例如移位、加法、減法、乘法)。雖然有些實施例可包括專用於特定功能或功能集合的多個執行單元，但其它實施例可只包括一個執行單元或多個執行單元，其全部一起執行全部功能。排程器單元 1356、實體暫存器檔案單元 1358、及執行叢集 1360 顯示為可能為多數，原因在於一些實施例產生針對一些類別的資料/操作的分開管線(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、和/或記憶體存取管線各自具有其本身的排程器單元、實體暫存器檔案單元、和/或執行叢集且於分開記憶體存取管線之情況下，實施一些實施例其中只有此一管線的執行叢集具有記憶體存取單元 1364)。也須瞭解使用分開管線時，此等管線中之一或多者可為失序簽發/執行及有序靜止。

[0099] 記憶體存取單元 1364 之集合係耦接至記憶體單元 1370，其包括一資料 TLB 單元 1372 耦接至與層級 2(L2)快取單元 1376 的一資料快取單元 1374。在一個具體實施例中，記憶體存取單元 1364 可包括一載入單元、一儲存位址單元、及一儲存資料單元，各單元係耦接至記憶

體單元 1370 中的資料 TLB 單元 1372。指令快取單元 1334 進一步係耦接至在記憶體單元 1370 中的層級 2(L2) 快取單元 1376。L2 快取單元 1376 係耦接至一或多個其它層級的快取記憶體，及最終耦接至一主記憶體。

[0100] 舉例言之，暫存器重新命名失序簽發/執行核心架構之實施例可實施管線 1300 如下：1)指令提取 1338 執行提取及長度解碼階段 1302 及 1304；2)解碼單元 1340 執行解碼階段 1306；3)重新命名/配置器單元 1352 執行配置階段 1308 及重新命名階段 1310；4)排程器單元 1356 執行排程階段 1312；5)實體暫存器檔案單元 1358 及記憶體單元 1370 執行暫存器讀取/記憶體讀取階段 1314；執行叢集 1360 進行該執行階段 1316；6)記憶體單元 1370 及實體暫存器檔案單元 1358 執行回寫入/記憶體寫入階段 1318；7)可能涉及例外處置階段 1322 的例外之各個單元；及 8)撤回單元 1354 及實體暫存器檔案單元 1358 執行確定階段 1324。

[0101] 核心 1390 可支持一或多個指令集(例如 x86 指令集(有些擴延已經增加較新版本)；加州昇陽谷的 MIPS 技術公司之 MIPS 指令集；加州昇陽谷的 ARM 控股公司的 ARM 指令集(具有選擇性額外擴延，諸如霓虹(NEON))，含括此處描述的指令。於一個實施例中，核心 1390 包括支持緊縮資料指令集擴延(例如 AVX1、AVX2)的邏輯，藉此允許許多多媒體應用程式使用的該等操作欲使用緊縮資料執行。

[0102] 應能理解到核心可支持多執行緒(執行二或多個並列的操作或執行緒集合)，且可以多種方式達成支持，包括時間截割多執行緒、同時多執行緒(於該處針對實體核心為同時多執行緒的該等執行緒各自，單一實體核心提供一邏輯核心)、或其組合(例如時間截割提取與解碼及其後同時多執行緒，諸如 Intel® Hyperthreading 技術)。

[0103] 雖然暫存器重新命名係以失序執行脈絡描述，但須瞭解暫存器重新命名可用於有序架構。雖然處理器之具體實施例也包括分開的指令及資料快取單元 1334/1374 及一分享 L2 快取單元 1376，但替代實施例可具有用於指令及資料二者的單一內部快取記憶體，諸如層級 1(L1)內部快取記憶體，或內部快取記憶體的多個層級。在一些實施例中，該系統可包括一內部快取記憶體與在核心和/或處理器外部的一外部快取記憶體之組合。另外，全部外部快取記憶體可位在核心和/或處理器外部。

有序核心架構特例

[0104] 圖 14A-B 例示說明有序核心架構之更特定實施例之方塊圖，該核心將為晶片中數個邏輯區塊中之一者(包括相同類別和/或不同類別的其它核心)。取決於應用用途，邏輯區塊透過高頻寬互連網路(例如環狀網路)而與若干固定功能邏輯、記憶體 I/O 介面、及其它需要的 I/O 邏輯通訊。

[0105] 圖 14A 為根據本發明實施例之單一處理器核心之方塊圖，連同其連接至晶粒上互連網路 1402 及層級 2(L2)快取記憶體 1404 之其本地子集的方塊圖。在一個實施例中，指令解碼器 1400 支持具有緊縮資料指令集擴延的 x86 指令集。L1 快取記憶體 1406 允許低度延遲存取快取記憶體至純量及向量單元。雖然於一個實施例中(為了簡化設計)，純量單元 1408 及向量單元 1410 使用分開的暫存器集合(分別為純量暫存器 1412 及向量暫存器 1414)，在其間傳輸的資料係寫入至記憶體，然後從層級 1(L1)快取記憶體 1406 回讀，本發明之替代實施例可使用不同辦法(例如使用單一暫存器集合或包括通訊路徑，其允許資料在兩個暫存器檔案間移轉而不被寫入及回讀)。

[0106] L2 快取記憶體 1404 之本地子集乃通用 L2 快取記憶體部分，被劃分成分開本地子集，每個處理器核心一個子集。各個處理器核心具有一直接存取路徑至其本身的 L2 快取記憶體 1404 之本地子集。由一處理器核心所讀取的資料係儲存於其 L2 快取子集 1404，且與其它處理器核心存取其本身的本地 L2 快取子集並列地能夠被快速存取。由處理器核心寫入的資料係儲存於其本身的 L2 快取子集 1404，及若有所需，從其它子集刷新。環狀網路確保分享資料的同調。環狀網路乃雙向以允許代理者諸如處理器核心、L2 快取記憶體及其它邏輯區塊在晶片內部彼此通訊。各個環狀資料路徑為每個方向 1012-位元寬。

[0107] 圖 14B 為根據本發明實施例之圖 14A 中的處

理器核心部分之展開圖。圖 14B 包括 L1 快取記憶體 1404 的 L1 資料快取記憶體 1406A 部分，以及有關向量單元 1410 及向量暫存器 1414 之進一步細節。更明確言之，向量單元 1410 為 16-寬向量處理單元(VPU)(參考 16-寬 ALU 1428)，其係執行整數指令、單精度浮點指令、及雙精度浮點指令中之一或多者。向量處理單元(VPU)支持使用調合單元 1420 調合該暫存器輸入，使用數值轉換單元 1422A-B 做數值轉換，及使用複製單元 1424 對記憶體輸入作複製。寫入遮罩暫存器 1426 允許預測所得的向量寫入。

具有集成記憶體控制器及圖形之處理器

[0108] 圖 15 為根據本發明實施例之處理器 1500 的方塊圖，該處理器 1500 可具有多於一個核心、可具有整合記憶體控制器及可具有整合圖形。圖 15 的實線框例示說明一處理器 1500 具有單一核心 1502A、一系統代理 1510、一或多個匯流排控制器單元 1516 之一集合，而選擇性地增加的虛線框例示說明另一個處理器 1500 具有多個核心 1502A-N、於系統代理單元 1510 中之一或多個集成記憶體控制器單元 1514、及特殊用途邏輯 1508。

[0109] 如此，處理器 1500 的不同實施可包括：1)一 CPU 具有特殊用途邏輯 1508 係為集成圖形和/或科學(資料通量)邏輯(可包括一或多個核心)，及核心 1502A-N 係為一或多個通用核心(例如通用有序核心、通用失序核

心、二者的組合)；2)一共處理器具有核心 1502A-N 係為意圖主要用於圖形和/或科學(資料通量)的大量特用核心；3)一共處理器具有核心 1502A-N 係為大量通用有序核心。如此，處理器 1500 可為通用目的處理器、共處理器或特有處理器，諸如網路或通訊處理器、壓縮引擎、圖形處理器、GPGPU(通用圖形處理單元)、高資料通量多集成核心(MIC)共處理器(含 30 或以上核心)、嵌入式處理器等。處理器可在一個或多個晶片上實施。處理器 1500 可為一個或多個基板的一部分，和/或可使用多項處理技術諸如 BiCMOS、CMOS、或 NMOS 而實施在一個或多個基板上。

[0110] 記憶體階層關係包括在核心內部的一個或多個快取層級、一個或多個共享快取單元 1506 之集合、及耦接至集成記憶體控制器單元 1514 之集合的外部記憶體(圖中未顯示)。共享快取單元 1506 之集合可包括一個或多個中階快取記憶體，諸如層級 2(L2)、層級 3(L3)、層級 4(L4)、或其它層級快取記憶體、最末層級快取記憶體(LLC)、和/或其組合。雖然於一個實施例中，一環狀基礎互連單元 1512 互連集成圖形邏輯 1508、共享快取單元 1506 之集合、及系統代理單元 1510/集成記憶體控制器單元 1514，但其它實施例可使用任何數目的眾所周知技術以互連此等單元。於一個實施例中，在一個或多個快取單元 1506 與核心 1502A-N 間維持同調。

[0111] 在一些實施例中，核心 1502A-N 中之一或多者可為多執行緒。系統代理 1510 包括協調與操作核心

1502A-N 的該等組件。系統代理單元 1510 可包括例如電力控制單元(PCU)及一顯示單元。電力控制單元(PCU)可為或包括調節核心 1502A-N 的功率狀態及集成圖形邏輯 1508 所需邏輯及組件。顯示單元係用以驅動一或多個外部連結的顯示器。

[0112] 核心 1502A-N 就架構指令集而言可為同質或異質；換言之，核心 1502A-N 中之二或多者可能可執行相同指令集，而其它者只能執行該指令集之一子集或一不同指令集。

電腦架構實施例

[0113] 圖 16-21 為之電腦架構實施例之方塊圖。本領域已知之針對膝上型電腦、桌上型電腦、手持式個人電腦、個人數位助理器、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、小區式電話、可攜式媒體播放器、手持式裝置及其它多種電子裝置的其它系統設計及組態也屬適宜。概略言之，能夠結合一處理器和/或其它此處揭示的執行邏輯的大量多種系統及電子裝置大致上為適宜。

[0114] 現在參考圖 16，顯示依據本發明之一個實施例一種系統 1600 之方塊圖。系統 1600 可包括一或多個處理器 1610、1615，耦接至控制器集線器 1620。在一個實施例中，控制器集線器 1620 包括一圖形記憶體控制器集

線器(GMCH)1690 及一輸入/輸出集線器(IOH)1650(可位在分開的晶片上)；GMCH 1690 包括記憶體及圖形控制器，其耦接記憶體 1640 及一共處理器 1645；IOH 1650 係耦接輸入/輸出(I/O)裝置 1660 至 GMCH 1690。另外，記憶體及圖形控制器中之一或二者係整合於處理器內部(如此處描述)，記憶體 1640 及共處理器 1645 係直接地耦接至在單一晶片內的處理器 1610 及控制器集線器 1620 與 IOH 1650。

[0115] 額外處理器 1615 的選擇性地本質係以虛線標示於圖 16。各個處理器 1610、1615 可包括此處描述的處理核心中之一或多者且可為處理器 1500 的某個版本。

[0116] 記憶體 1640 例如可為動態隨機存取記憶體(DRAM)、相變記憶體(PCM)或二者的組合。對至少一實施例，控制器集線器 1620 透過多插匯流排諸如前端匯流排(FSB)、點對點介面諸如快速路徑互連(QPI)或類似的連結 1695 而與處理器 1610、1615 通訊。

[0117] 在一實施例中，共處理器 1645 乃特用處理器，諸如高資料通量 MIC 處理器、網路或通訊處理器、壓縮引擎、圖形處理器、GPGPU、嵌入式處理器等。於實施例中，控制器集線器 1620 可包括一集成圖形加速器。

[0118] 就一定範圍的優劣量表而言，包括架構、微架構、熱、功耗特性等，實體資源 1610、1615 間可有多項差異。

[0119] 在一實施例中，處理器 1610 執行指令其控制

通用類別的資料處理操作。該等指令內部嵌入共處理器指令。處理器 1610 識別此等共處理器指令乃屬須由附接的共處理器 1645 執行的類別。據此，處理器 1610 在共處理器匯流排或其它互連上簽發此等共處理器指令(或表示共處理器指令的控制信號)給共處理器 1645。共處理器 1645 接收且執行所接收的共處理器指令。

[0120] 現在參考圖 17，顯示依據本發明之一實施例第一更特定系統 1700 之一方塊圖。如圖 17 所示，多處理器系統 1700 為點對點互連系統，包括透過點對點互連 1750 而耦接的第一處理器 1770 及第二處理器 1780。處理器 1770 及 1780 各自可為處理器 1500 的某個版本。於本發明之一個實施例中，處理器 1770 及 1780 分別為處理器 1610 及 1615，而共處理器 1738 為共處理器 1645。在另一個實施例中，處理器 1770 及 1780 分別為處理器 1610 及共處理器 1645。

[0121] 處理器 1770 及 1780 係顯示為分別包括集成記憶體控制器 (IMC) 單元 1772 及 1782。處理器 1770 也包括點對點(P-P)介面 1776 及 1778 作為其匯流排控制器單元之一部分；同理，第二處理器 1780 可包括 P-P 介面 1786 及 1788。處理器 1770、1780 可使用 P-P 介面電路 1778、1788 透過點對點(P-P)介面 1750 交換資訊。如圖 17 所示，IMC 1772 及 1782 耦接該等處理器至個別記憶體，亦即記憶體 1732 及記憶體 1734，其可為本地附接至個別處理器的主記憶體的一部分。

[0122] 處理器 1770、1780 可使用點對點介面電路 1776、1794、1786、1798 透過點對點 (P-P) 介面 1752、1754 而各自與一晶片組 1790 交換資訊。晶片組 1790 也可透過一高效能介面 1739 而與共處理器 1738 交換資訊。在一個實施例中，共處理器 1738 乃特用處理器，諸如高資料通量 MIC 處理器、網路或通訊處理器、壓縮引擎、圖形處理器、GPGPU、嵌入式處理器等。

[0123] 一分享快取記憶體(圖中未顯示)可含括於任一處理器內或二處理器外部，但仍然透過 P-P 互連而與處理器連結，使得當一處理器被置於低功率模式時，任一處理器的或二處理器的本地快取記憶體資訊可被儲存於該分享快取記憶體。

[0124] 晶片組 1790 可透過一介面 1796 而耦接至第一匯流排 1716。在一個實施例中，第一匯流排 1716 可為周邊組件互連 (PCI) 匯流排，或諸如 PCI 快速匯流排或其它第三代 I/O 互連匯流排之一匯流排，但本發明之範圍不如此限制。

[0125] 如圖 17 所示，多個 I/O 裝置 1714 可連同一匯流排橋接器 1718 而耦接至第一匯流排 1716，該匯流排橋接器 1718 係耦接第一匯流排 1716 至第二匯流排 1720。在一個實施例中，一或多個額外處理器 1715，諸如共處理器、高資料通量 MIC 處理器、GPGPU、加速器(例如圖形加速器或數位信號處理器 (DSP) 單元)、可現場程式規劃陣列、或任何其它處理器係耦接至第一匯流排

1716。在一個實施例中，第二匯流排 1720 可為低接腳數目(LPC)匯流排。在一個實施例中，多個裝置可耦接至第二匯流排 1720，包括例如鍵盤和/或滑鼠 1722、通訊裝置 1727 及儲存單元 1728，諸如磁碟機或其它大容量儲存裝置，可包括指令/碼及資料 1730。此外，音訊 I/O 1724 可耦接至第二匯流排 1720。注意其它架構係屬可能。舉例言之，替代圖 17 之點對點架構，一系統可實施多插匯流排或其它此種架構。

[0126] 現在參考圖 18，顯示依據本發明之一實施例第二更具體範例系統 1800 之一方塊圖。圖 17 與圖 18 中相似的元件具有相似的元件符號，及圖 17 的一些方面已經從圖 18 刪除以免不必要地遮掩圖 18 的其它方面。

[0127] 圖 18 例示說明處理器 1770、1780 分別地可包括集成記憶體及 I/O 控制邏輯(「CL」)1772 及 1782。於至少一實施例中，CL 1772、1782 可包括集成記憶體控制器單元且包括 I/O 控制邏輯。圖 18 例示說明不僅記憶體 1732、1734 耦接至 CL 1772、1782，I/O 裝置 1814 也耦接至控制邏輯 1772、1782。舊式 I/O 裝置 1815 係耦接至晶片組 1790。

[0128] 現在參考圖 19，顯示依據本發明之一個實施例，一個 SoC 1900 之方塊圖。圖 15 中的相似元件具有類似的元件符號。又，虛線框乃更為先進 SoC 上的選擇性特徵。於圖 19 中，一互連單元 1902 係耦接至：一應用程式處理器 1910 其包括一或多個核心 182A-N 與共享快取單

元 1506 之一集合；一系統代理單元 1510；一匯流排控制器單元 1516；一集成記憶體控制器單元 1514；一或多個共處理器 1920 之一集合其可包括集成圖形邏輯、影像處理器、音訊處理器、及視訊處理器；一靜態隨機存取記憶體 (SRAM) 單元 1930；一直接記憶體存取 (DMA) 單元 1932；及用以耦接至一或多個外部顯示器的一顯示單元 1940。在一個實施例中，該(等)共處理器 1920 包括特用處理器，諸如網路或通訊處理器、壓縮引擎、GPGPU、高資料通量 MIC 處理器、嵌入式處理器等。

[0129] 如此處揭示的機構之實施例可於硬體、軟體、韌體或此等實施辦法的組合而予實施。本發明之實施例可實施為電腦程式或在可規劃系統包含至少一處理器、儲存系統(包括依電性及非依電性記憶體和/或儲存元件)、至少一輸入裝置、及至少一輸出裝置上執行的程式碼。

[0130] 程式碼諸如圖 17 例示說明之碼 1730 可施加至輸入指令以執行此處描述的功能及產生輸出資訊。輸出資訊可以已知方式施加至一或多個輸出裝置。用於本應用之目的，處理系統包括具有一處理器的任何系統，諸如數位信號處理器(DSP)、微控制器、特定應用積體電路(ASIC)或微處理器。

[0131] 程式碼可於高階程式或目標導向程式語言實施以與一處理系統通訊。若有所需，程式碼也可於組合語言或機器語言實施。實際上，此處描述的機構之範圍並非限於任何特定程式語言。總而言之，該語言可為彙編語言

或解譯語言。

[0132] 至少一實施例的一或多個方面可藉表示處理器內部的多個邏輯而儲存在機器可讀取媒體上的代表性指令實施，該等指令當由一機器讀取時使得該機器組合邏輯以執行此處描述的技術。此種表示型態稱作為「IP 核心」，可儲存在具體有形的機器可讀取媒體上且供給各個客戶或製造廠以載入實際上生產該邏輯或處理器的組裝機器內。

[0133] 此等機器可讀取儲存媒體可包括但非僅限於由機器或裝置所製造或製成的非過渡具體有形的物件配置，包括儲存媒體諸如硬碟、任何其它類別的碟片包括軟碟、光碟、光碟-唯讀記憶體(CD-ROM)、光碟可覆寫入式(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、可電氣抹除可規劃唯讀記憶體(EEPROM)、相變記憶體(PCM)、磁卡或光卡；或適用以儲存電子指令的任何其它類別的媒體。

[0134] 因此，本發明之實施例也包括非過渡具體有形的機器可讀取媒體含有指令或含有設計資料，諸如硬體描述語言(HDL)其定義此處描述的結構、電路、裝置、處理器和/或系統特徵。此等實施例也可稱作為程式產品。

仿真(包含二進制轉譯、碼變形等)

[0135] 於一些情況下，指令轉換器可用以將指令從來源指令集轉換成目標指令集。舉例言之，指令轉換器可將一指令轉譯(例如使用靜態二進制轉譯、含動態編譯的動態二進制轉譯)、變形、仿真或以其它方式轉換成欲藉核心處理的一或多個其它指令。指令轉換器可於軟體、硬體、韌體或其組合實施。指令轉換器可在處理器上、不在處理器上、或部分在及部分不在處理器上。

[0136] 圖 20 為根據本發明實施例之對比軟體指令轉換器用以將在來源指令集中之二進制指令轉換成在目標指令集中之二進制指令的方塊圖。在該具體實施例中，指令轉換器為軟體指令轉換器，但另外，指令轉換器可於軟體、韌體、硬體、或其各項組合實施。圖 20 顯示可使用 x86 編譯器 2004 編譯以產生 x86 二進制碼 2006 的高階語言 2002，該 x86 二進制碼 2006 可由具有至少一 x86 指令集核心之處理器 2016 本機執行。具有至少一 x86 指令集核心之處理器 2016 表示藉相容式執行或以其它方式處理 (1)英特爾 x86 指令集核心的該指令集之一相當大部分或(2)靶定以在具至少一 x86 指令集核心的一英特爾處理器跑的應用程式或其它軟體之目標碼版本而執行與具至少一 x86 指令集核心的一英特爾處理器實質上相同功能以達成與具至少一 x86 指令集核心的一英特爾處理器實質上相同結果。x86 編譯器 2004 表示可操作而產生 x86 二進制碼 2006(例如目標碼)的一編碼器，該等 x86 二進制碼 2006 有或無額外鏈結處理可在具至少一 x86 指令集核心的該處

理器 2016 上執行。同理，圖 20 顯示於高階語言 2002 的該程式可使用另一指令集編譯器 2008 編譯以產生另一指令集二進制碼 2010，可藉不具至少一 x86 指令集核心的一處理器 2014 本機執行(例如具有執行加州昇陽谷的 MIPS 技術公司之 MIPS 指令集和/或執行加州昇陽谷的 ARM 控股公司的 ARM 指令集之核心的一處理器)。指令轉換器 2012 係用以將 x86 二進制碼 2006 轉換成可由不具一 x86 指令集核心的該處理器 2014 本機執行的碼。此種轉換碼不可能與另一指令集二進制碼 2010 相同，原因在於難以製造可達成此項目的之一指令轉換器；但轉換碼將達成一般操作且係由得自該另一指令集的指令組成。如此，指令轉換器 2012 表示軟體、韌體、硬體或其組合其透過仿真、模擬或任何其它處理允許不具至少一 x86 指令集處理器或核心的一處理器或其它電子裝置執行該 x86 二進制碼 2006。

[0137] 針對圖 1-7 之任一者所述之組件、特徵、及細節也可選擇性地應用於圖 8-12 之任一者。此外，針對設備之任一者所述之組件、特徵、及細節亦可選擇性地應用於其在實施例中可由和/或以此類設備所執行的方法之任一者。本文中所述的處理器之任一者可被包括於文中所揭露的電腦系統之任一者(例如，圖 13-15)。在一些實施例中，電腦系統可包括動態隨機存取記憶體(DRAM)。替代地，電腦系統可包括其不需被更新之揮發性記憶體的類型或者快閃記憶體。本文中所揭露之指令

可被執行以本文中所示之任何處理器，其具有本文中所示之任何微架構，於本文中所示之任何系統上。

[0138] 於說明書及申請專利範圍中，術語「耦接」和/或「連接」（連同其衍生詞）可被使用。這些術語並非被用為彼此的同義詞。反之，於實施例中，「連接」可被用以指示其二或更多元件係彼此直接地實體和/或電氣接觸。「耦接」可表示二或更多元件係彼此直接地物理和/或電氣接觸。然而，「耦接」亦可表示其二或更多元件不是彼此直接接觸，而仍彼此合作或互動。例如，執行單元可透過一或更多中間組件而與暫存器和/或解碼單元耦接。於圖中，箭號被用以顯示連接或耦接。

[0139] 術語「和/或」可已被使用。如本文中所使用，術語「和/或」表示一者或另一者或兩者（例如，A 和/或 B 表示 A 或 B 或 A 與 B 兩者）。

[0140] 於以上說明中，已提出數個特定細節以提供實施例之透徹瞭解。然而，其他實施例可被實行而無這些特定的細節。本發明之範圍並非由以上所提供的特定範例來判定，而僅由底下的申請專利範圍來判定。於其他例子中，眾所周知的電路、結構、裝置、及操作已被顯示於方塊圖形式和/或無細節地，以避免妨礙對描述之瞭解。在適當情況下，參考數字、或參考數字之末端部已被重複於圖中以指示相應的或類似的元件，其可選擇性地具有類似的或相同的特性，除非另有指明或清楚明白的。

[0141] 某些操作可由硬體組件來執行，或者可被實

施以機器可執行或電路可執行指令，其可被用以致使和/或導致以指令編程之機器、電路、或硬體組件（例如，處理器、處理器之部分、電路，等等）執行該些操作。該些操作亦可選擇性地由硬體與軟體之組合來執行。處理器、機器、電路、或硬體可包括特定或特殊的電路或其他邏輯（例如，潛在地與韌體和/或軟體結合之硬體），其可操作以執行和/或處理指令並回應於該指令而儲存結果。

[0142] 一些實施例包括製造物件（例如，電腦程式產品），其包括機器可讀取媒體。媒體可包括一種機制，其係以可由機器讀取之形式提供（例如，儲存）資訊。機器可讀取媒體可提供（或於其上儲存）指令或指令序列，其（假如和/或當由機器執行時）可操作以致使機器執行和/或導致機器執行本文中所揭露的操作、方法、或技術之一。

[0143] 在一些實施例中，機器可讀取媒體可包括非暫態機器可讀取儲存媒體。例如，非暫態機器可讀取儲存媒體可包括軟碟、光學儲存媒體、光碟、光學資料儲存裝置、CD-ROM、磁碟、磁光碟、唯讀記憶體（ROM）、可編程 ROM（PROM）、可抹除且可編程 ROM（EPROM）、電可抹除且可編程 ROM（EEPROM）、隨機存取記憶體（RAM）、靜態 RAM（SRAM）、動態 RAM（DRAM）、快閃記憶體、相位改變記憶體、相位改變資料儲存材料、非揮發性記憶體、非揮發性資料儲存裝置、非暫態記憶體、非暫態資料儲存裝置，等等。非暫態

機器可讀取儲存媒體不包括暫態傳播信號。在一些實施例中，儲存媒體可包括有形媒體，其包括固態物質。

[0144] 適當機器之範例包括（但不限定於）通用目的處理器、特殊目的處理器、數位邏輯電路、積體電路，等等。適當機器之又其他範例包括電腦系統或其他電子裝置，其包括處理器、數位邏輯電路、或積體電路。此類電腦系統或電子裝置之範例包括（但不限定於）桌上型電腦、膝上型電腦、筆記型電腦、平板電腦、小筆電、智慧型手機、行動電話、伺服器、網路裝置（例如，路由器及開關）、行動網際網路裝置（MID）、媒體播放器、智慧電視、桌上型易網機、機上盒、及視頻遊戲控制器。

[0145] 遍及本說明書針對「一實施例」、「實施例」、「一或更多實施例」、「一些實施例」（舉例而言）之參考係指示其特定特徵可被包括於本發明之實施中但並不一定必要。類似地，於說明書中，各個特徵有時被組合在一起於單一實施例、圖形、或其描述中，以供解釋本發明及協助瞭解實施例之各個發明性形態的目的。然而，本發明之方法不應被解讀為反應其本發明需要比各申請專利範圍中所明確記載之更多特徵的企圖。反之，如以下申請專利範圍所反應者，發明性形態在於比單一所揭露實施例之所有特徵更少的特徵。因此，接續著實施方式之申請專利範圍於此被清楚地併入此實施方式中，以各項申請專利範圍本身可獨立成為本發明之一分離的實施例。

範例實施例

[0146] 下列範例係有關進一步的實施例。範例中之明確細節可被使用於一或更多實施例中的任何地方。

[0147] 範例 1 為一種處理器，其包括用以解碼指令之解碼單元、以及與該解碼單元耦接之執行單元。該執行單元回應於該指令以判定由於該指令之有關影子堆疊之影子堆疊指標（SSP）之嘗試的改變將導致該 SSP 超過允許的範圍；以及回應於有關該 SSP 之該嘗試的改變將導致該 SSP 超過允許的範圍之判定採取異常。

[0148] 範例 2 包括申請專利範圍第 1 項所述之處理器，其中回應於該指令的該執行單元係用以比較有關該 SSP 之該嘗試的改變與用以指定該允許的範圍之 SSP 基底和 SSP 限制。

[0149] 範例 3 包括申請專利範圍第 2 項所述之處理器，其中該 SSP 基底係用以代表該影子堆疊之最低允許的邏輯位址，以及該 SSP 限制係用以代表該影子堆疊之最高允許的邏輯位址

[0150] 範例 4 包括申請專利範圍第 2 項所述之處理器，其中該 SSP 基底和該 SSP 限制係由特權系統軟體指定。

[0151] 範例 5 包括申請專利範圍第 2 項所述之處理器，其中該 SSP 基底和該 SSP 限制係被儲存在該處理器之控制暫存器中。

[0152] 範例 6 包括申請專利範圍第 1 項所述之處理

器，其中回應於該指令之該執行單元係用以判定由於該指令至該影子堆疊之資料的嘗試的推送將導致該 SSP 超過該允許的範圍以及將導致資料被儲存在該允許的範圍外側之資料。

[0153] 範例 7 包括申請專利範圍第 1 項所述之處理器，其中回應於該指令之該執行單元係用以判定由於該指令之從該影子堆疊之資料之嘗試的彈出將導致從該允許的範圍外側讀取之資料。

[0154] 範例 8 包括申請專利範圍第 1 項所述之處理器，其中解碼單元係用以解碼用來指示影子堆疊選擇器之該指令，且其中回應於該指令之該執行單元係用以使用該影子堆疊選擇器以選擇該影子堆疊。

[0155] 範例 9 包括申請專利範圍第 8 項所述之處理器，其中該解碼單元係用以解碼該指令，該指令係用以指示影子堆疊描述符表（SSDT）選擇器作為該影子堆疊選擇器，其中該 SSDT 選擇器係用以選擇一登錄，該登錄係相應於在影子堆疊描述符表（SSDT）中的該影子堆疊。

[0156] 範例 10 包括申請專利範圍第 9 項所述之處理器，其中在該 SSDT 中的該登錄係用以儲存 SSP 基底和 SSP 限制，該 SSP 基底和該 SSP 限制係用以指定該允許的範圍。

[0157] 範例 11 包括申請專利範圍第 8 項所述之處理器，其中回應於該指令之該執行單元係用以判定該影子堆疊是否有效，其中該影子堆疊選擇器係用以選擇。

[0158] 範例 12 包括申請專利範圍第 11 項所述之處理器，其中該解碼單元係用以解碼該指令，該指令係用以指示影子堆疊描述符表（SSDT）選擇器作為該影子堆疊選擇器，其中該 SSDT 選擇器係用以選擇一登錄，該登錄係相應於在影子堆疊描述符表（SSDT）中的該影子堆疊，以及其中回應於該指令之該執行單元係用以至少基於在該登錄之有效性指標上的部分判定該影子堆疊是否有效。

[0159] 範例 13 包括申請專利範圍第 1 至 12 項中任一項所述之處理器，其中與採取該異常協同之該處理器係用以：從任務狀態片段結構得到影子堆疊描述符表（SSDT）選擇器；以及使用該影子堆疊描述符表（SSDT）選擇器來判定用於該第二影子堆疊之第二 SSP 之允許的範圍，該第二影子堆疊係由處置器使用，該處置器係用以處理該異常。

[0160] 範例 14 包括申請專利範圍第 1 至 12 項中任一項所述之處理器，其中該允許的範圍為允許的線性位址範圍。

[0161] 範例 15 包括申請專利範圍第 1 至 12 項中任一項所述之處理器，其中該允許的範圍係由特權系統軟體指定的。

[0162] 範例 16 包括申請專利範圍第 1 至 12 項中任一項所述之處理器，其中該影子堆疊係用以儲存返回位址之拷貝，該返回位址之拷貝儲存在呼叫堆疊上，但並不儲

存通過作為參數之使用者層級資料至呼叫的程序。

[0163] 範例 17 為一種處理器，其包括用以解碼保存影子堆疊指標指令之解碼單元、以及與該解碼單元耦接之執行單元。該執行單元回應於該影子堆疊指標指令以判定至影子堆疊之影子堆疊指標（SSP）值之推送將不導致該 SSP 超過允許的範圍；以及在判定至該影子堆疊之該 SSP 值之該推送將不導致該 SSP 超過該允許的範圍之後，推送該 SSP 值至該影子堆疊。

[0164] 範例 18 包括申請專利範圍第 17 項所述之處理器，其中該解碼單元係用以解碼該保存影子堆疊指標指令，該保存影子堆疊指標指令係用以指示目的地儲存位置，且其中回應於該保存影子堆疊指標指令之該執行單元係用以在至該目的地儲存位置中的該影子堆疊的該 SSP 值之該推送之後儲存當前 SSP。

[0165] 範例 19 包括申請專利範圍第 17 至 18 項中任一項所述之處理器，其中該解碼單元係用以解碼該保存影子堆疊指標指令，該保存影子堆疊指標指令是成為使用者層級指令。

[0166] 範例 20 係一種處理器，其包括用以解碼復原影子堆疊指標指令的解碼單元。該復原影子堆疊指標指令用以指示給定的影子堆疊指標（SSP）值。執行單元與該解碼單元耦接。該執行單元回應於該復原影子堆疊指標指令以判定該給定的 SSP 值不超過用於相應的影子堆疊之允許的範圍。該執行單元也用以判定由該指令指示的該給定

的 SSP 值與從該相應的影子堆疊接收的 SSP 值相容。該執行單元也用以改變該相應的影子堆疊之 SSP 為該給定的 SSP 值。

[0167] 範例 21 包括申請專利範圍第 20 項所述之處理器，其中回應於該指令之該執行單元係用以判定該給定的 SSP 值在該 SSP 基底和 SSP 限制中，該 SSP 基底和該 SSP 限制係用以指令該允許的範圍。

[0168] 範例 22 包括申請專利範圍第 21 項所述之處理器，其中該 SSP 基底係用以代表該影子堆疊之最低允許的邏輯位址，以及該 SSP 限制係用以代表該影子堆疊之最高允許的邏輯位址。

[0169] 範例 23 包括申請專利範圍第 20 項所述之處理器，其中該解碼單元係用以解碼該復原影子堆疊指標指令，其中該復原影子堆疊指標指令是用以指示影子堆疊選擇器，該影子堆疊選擇器係用以選擇該相應的影子堆疊。

[0170] 範例 24 包括申請專利範圍第 23 項所述之處理器，其中該解碼單元係用以解碼該指令，該指令係用以指示影子堆疊描述符表（SSDT）選擇器作為該影子堆疊選擇器。也可選擇地，其中回應於該指令之該執行單元係用以使用該 SSDT 選擇器以選擇在該影子堆疊描述符表（SSDT）中的登錄，且其中該登錄係用以指定該影子堆疊之該允許的範圍。

[0171] 範例 25 包括申請專利範圍第 20 至 24 項中任一項所述之處理器，其中回應於該指令之執行單元更用以

妥協該 SSP 值，該 SSP 值在至該給定的 SSP 值之該改變之前，被保存在該相應的影子堆疊上。

[0172] 範例 26 包括申請專利範圍第 20 至 24 項中任一項所述之處理器，其中該解碼單元係用以解碼該保存影子堆疊指標指令，該保存影子堆疊指標指令是成為使用者層級指令。

[0173] 範例 27 係一種處理器，其包括用以解碼返回指令的解碼單元以及與該解碼單元耦接之執行單元。該執行單元回應於該返回指令以接收來自堆疊之返回位址，以及判定來自影子堆疊之返回位址之彈出將不導致值被從該影子堆疊之允許的範圍之外側讀取。該執行單元也用以從該影子堆疊接收該返回位址以及判定來自該堆疊之該返回位址與來自該影子堆疊之該返回位址相容。該執行單元也用以儲存來自該堆疊之該返回位址與來自該影子堆疊之該返回位址中的一者在指令指標暫存器。

[0174] 範例 28 包括申請專利範圍第 27 項所述之處理器，其中該允許的範圍為由特權系統軟體指定之允許的線性位址範圍。

[0175] 範例 29 係一種用以處理指令之系統，其包括互連，以及與該互連耦接的處理器。該處理器係用以接收指令。該處理器回應於該指令以判定由於該指令至影子堆疊之影子堆疊指標（SSP）之嘗試的改變將導致該 SSP 超過允許的範圍，以及回應於至該 SSP 之該嘗試的改變將導致該 SSP 超過允許的範圍之判定採取異常。該系統也包括

與該互連耦接的動態隨機存取記憶體（DRAM）。該 DRAM 儲存特權系統軟體之指令集，當該指令集由該處理器執行時，以導致該處理器執行操作，該操作包含判定用於該 SSP 之該允許的範圍，以及儲存用於該 SSP 之該允許的範圍在該 DRAM 之存取保護的部分中。

[0176] 範例 30 包括申請專利範圍第 27 項所述之系統，其中該允許的範圍包含允許的線性位址範圍，且其中該指令為使用者層級指令。

[0177] 範例 31 包括範例 1 至 16 中任何一者的處理器，更包括用以預測分支之可選擇的分支預測單元以及與該分支預測單元耦接之可選擇的指令提取單元，該指令提取單元用以提取包括指令之指令。該處理器也選擇地包括與該指令提取單元耦接之可選擇的層級 1（L1）指令快取記憶體，該 L1 指令快取記憶體用以儲存指令，用以儲存資料之可選擇的 L1 資料快取記憶體以及用以儲存資料和指令之可選擇的層級 2（L2）快取記憶體。該處理器也可選擇地包括與該解碼單元、L1 指令快取記憶體和 L2 快取記憶體耦接之指令提取單元，其用以提取該指令（在一些其況下從 L1 指令快取記憶體和 L2 快取記憶體中的一者），且用以提供該指令至該解碼單元。處理器也可選擇地包括用以重新命名暫存器之暫存器重新命名單元、用以排程已經從用於執行之該指令解碼的一或多個操作之可選擇的排程器、以及用以確定該指令之執行結果之可選擇的確定單元。

[0178] 範例 32 包括範例 1 至 16 中任一者的處理器或其它設備，且可選擇地組合任何可選擇的動態隨機存取記憶體（DRAM）、可選擇的繪圖裝置和可選擇的無線收發器。

[0179] 範例 33 係一種實質上如本文敘述的處理器或其它設備。

[0180] 範例 34 係一種用以執行（例如，其具有組件來執行或其被操作以執行）任何實質上如本文敘述的指令之處理器或其它設備。

[0181] 範例 35 係一種包括處理器之電腦系統或其它電子裝置，該處理器具有用以解碼第一指令集之指令的解碼單元。該處理器也具有一或多個執行單元。該電子裝置也包括與該處理器耦接之儲存裝置。該儲存裝置用以儲存第一指令，其可以為任何實質上如本文敘述的指令，且其將是第二指令集。該儲存裝置也用以儲存用以轉換第一指令為該第一指令集之一或多個指令。當該第一指令集之一或多個指令由該處理器執行時將使得處理器以仿真該第一指令。

【符號說明】

[0182]

100:電腦系統

101:處理器

102:指令集

103:呼叫程序指令
104:從程序返回指令
105:保存影子堆疊指標指令
106:復原影子堆疊指標指令
108:邏輯處理器
109:解碼及執行單元
110:影子堆疊保護邏輯
111:影子堆疊模式
112:影子堆疊暫存器
113, 213:SSDT 暫存器
114:記憶體
115:特權系統軟體
116:使用者層級應用程式
117,121:控制
118:資料
119:堆疊
120:影子堆疊
122,322:影子堆疊描述符表 (SSDT)
212:影子堆疊暫存器
213:SSDT 暫存器
224:處理器控制暫存器
225:影子堆疊基底 (SSP base) 暫存器
226:影子堆疊限制 (SSP limit) 暫存器
227:影子堆疊指標 (SSP) 暫存器

228:使用者 SSDT 基底暫存器
229:使用者 SSDT 限制暫存器
230:監督者 SSDT 基底暫存器
231:監督者 SSDT 限制暫存器
335-1 ~ 335-N:登錄
336-1 ~ 336-N:有效性指標
337-1 ~ 337-N:SSP 基底
338-1 ~ 338-N:SSP 限制
435:SSDT 登錄
540:SSDT 選擇器
645:32 位元任務狀態片段 (TSS) 結構
646:狀態保存欄位
647:其它欄位
648:TSS SSDT 選擇器
649:TSS SSP
650:SSDT 選擇器 0
651:SSDT 選擇器 1
652:SSDT 選擇器 2
745:64 位元 TSS 結構
758:SSDT 選擇器 0
759:SSDT 選擇器 1
760:SSDT 選擇器 2
761:SSDT 選擇器 IST 1
762:SSDT 選擇器 IST 2

763:SSDT 選擇器 IST 3

764:SSDT 選擇器 IST 4

765:SSDT 選擇器 IST 5

766:SSDT 選擇器 IST 6

767:SSDT 選擇器 IST 7

801:處理器

803:呼叫指令

804:返回指令

870:解碼單元

871C:呼叫執行單元

871R:返回執行單元

872:暫存器

873:返回位址

874:記憶體

875:堆疊

876:返回位址

877:影子堆疊

878:返回位址

879:處置器模組

880:指令指標暫存器

882,884:接收

885:異常

987:方法

988,989,990,1102,1103,1104,1105,1106,1107,1108:方塊

1001:處理器

1005:保存影子堆疊指標指令

1012:SSP 暫存器

1017:返回位址資訊

1070:解碼單元

1071:保存 SSP 執行單元

1072:暫存器

1074:記憶體

1077:影子堆疊

1092,1096:當前 SSP

1097:目的地儲存位置

1201:處理器

1206:回復影子堆疊指標指令

1212:影子堆疊暫存器

1217:返回位址資訊

1222:SSDT

1225:SSP 基底

1226:SSP 限制

1227:SSP

1235:登錄

1237:SSP 基底

1238:SSP 限制

1270:解碼單元

1271:回復 SSP 執行單元

1272:暫存器
 1274:記憶體
 1277:影子堆疊
 1279:處置器
 1291:SSP
 1292:儲存在影子堆疊上之當前 SSP
 1294:第二來源運算元
 1295:第一來源運算元
 1299:SSDT 選擇器
 1300:處理器管線
 1302:提取階段
 1304:長度解碼階段
 1306:解碼階段
 1308:配置階段
 1310:重新命名階段
 812:排程階段
 1314:暫存器讀取/記憶體讀取階段
 1316:執行階段
 1318:回寫/記憶體寫入階段
 1322:例外處置階段
 1324:確定階段
 1330:前端單元
 1332:分支預測單元
 1334:指令快取單元

1336:指令翻譯旁看緩衝器 (TLB)

1338:指令提取單元

1340:解碼單元

1350:執行引擎單元

1352:重新命名/配置器單元

1354:撤回單元

1356:排程器單元

1358:實體暫存器檔案單元

1360:執行叢集

1362:執行單元

1364:記憶體存取單元

1370:記憶體單元

1372:資料 TLB 單元

1374:資料快取單元

1376:第二階 (L2) 快取單元

1390:處理器核心

1400:指令解碼器

1402:晶粒上互連網路

1404:第二階 (L2) 快取記憶體

1406:L1 快取記憶體

1406A:L1 資料快取

1408:純量單元

1410:向量單元

1412:純量暫存器

1414:向量暫存器

1420:調合單元

1422A-B:數值轉換單元

1424:複製單元

1426:寫入遮罩暫存器

1428:16-寬的 ALU

1500:處理器

1502A-N:核心

1506:共享快取單元

1508:特殊用途邏輯

1510:系統代理單元

1512:環式為基的互連單元

1514:集成記憶體控制器單元

1516:匯流排控制器單元

1600:系統

1610,1615:處理器

1620:控制器集線器

1640:記憶體

1645:共處理器

1650:輸入/輸出集線器 (IOH)

1660:輸入/輸出 (I/O) 裝置

1690:圖形記憶體控制器集線器 (GMCH)

1695:連接

1700:多處理器系統

1714:I/O 裝置

1715:額外處理器

1716:第一匯流排

1718:匯流排橋接器

1720:第二匯流排

1722:鍵盤及/或滑鼠

1724:音頻 I/O

1727:通訊裝置

1728:儲存單元

1730:指令/代碼及資料

1732:記憶體

1734:記憶體

1738:共處理器

1739:高性能介面

1750:點對點互連

1752,1754:P-P 介面

1770:第一處理器

1772,1782:集成記憶體控制器 (IMC) 單元

1776,1778:點對點 (P-P) 介面

1780:第二處理器

1786,1788:P-P 介面

1790:晶片組

1794,1798:點對點介面電路

1796:介面

1800:系統

1814:I/O 裝置

1815:舊有 I/O 裝置

1900:SoC

1902:互連單元

1910:應用程式處理器

1920:共處理器

1930:靜態隨機存取記憶體（SRAM）單元

1932:直接記憶體存取（DMA）單元

1940:顯示單元

2002:高階語言

2004:x86 編譯器

2006:x86 二進制碼

2008:指令集編譯器

2010:指令集二進制碼

2012:指令轉換器

2014:不具至少一 x86 指令集核心之處理器

2016:具有至少一 x86 指令集核心之處理器

【發明申請專利範圍】

【請求項 1】一種處理器，包含：

用以儲存當前影子堆疊指標(SSP)的 SSP 暫存器，其用以識別當前影子堆疊的頂部；

解碼單元，其用以解碼回復影子堆疊指標指令，該回復影子堆疊指標指令用以指示來源運算元具有第一 SSP，該第一 SSP 識別第一影子堆疊的頂部；以及

執行單元，其與該解碼單元耦接，該執行單元回應於該回復影子堆疊指標指令而用以：

執行複數個安全確認，包括判定從該第一 SSP 導出的值是否與從第一影子堆疊存取的值相容；

如果至少一該安全確認失敗，則引發異常；以及

如果該等安全確認全部成功，則將 SSP 回復至該 SSP 暫存器，以從該當前影子堆疊切換至該第一影子堆疊。

【請求項 2】如請求項 1 之處理器，其中如果至少一該安全確認失敗，則該執行單元進一步不將該 SSP 回復至該 SSP 暫存器。

【請求項 3】如請求項 1 或 2 之處理器，其中回復至該 SSP 暫存器之該 SSP 包含該第一 SSP。

【請求項 4】如請求項 1 或 2 之處理器，其中該第一影子堆疊是用於不同特權層級的複數個影子堆疊之一。

【請求項 5】如請求項 1 或 2 之處理器，其中如果該等安全確認全部成功，則該執行單元也進一步執行至該第一

影子堆疊的儲存。

【請求項 6】如請求項 1 或 2 之處理器，其中該解碼單元係用以解碼保存影子堆疊指標指令，並且該處理器更用以執行該保存影子堆疊指標指令以將從該第一影子堆疊存取的該值儲存至該第一影子堆疊。

【請求項 7】如請求項 1 或 2 之處理器，其中該第一 SSP 係線性位址。

【請求項 8】如請求項 1 或 2 之處理器，其中該解碼單元係用以解碼呼叫指令，並且該處理器進一步包含執行單元，其用以執行該呼叫指令，包括將該呼叫指令的返回位址儲存在當前影子堆疊上。

【請求項 9】如請求項 1 或 2 之處理器，其中從該第一影子堆疊存取的該值係基於該第一 SSP 的轉換。

【發明圖式】

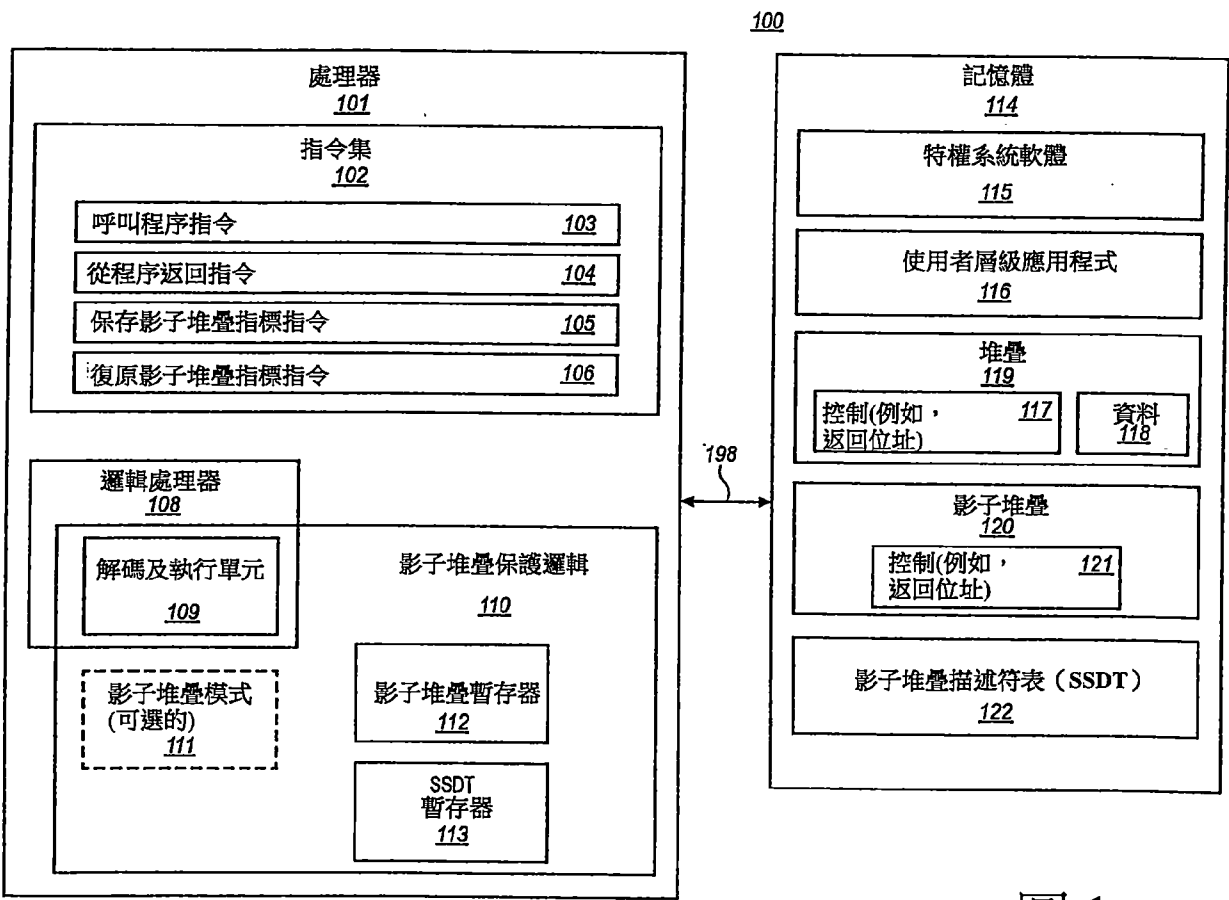


圖 1

圖 2

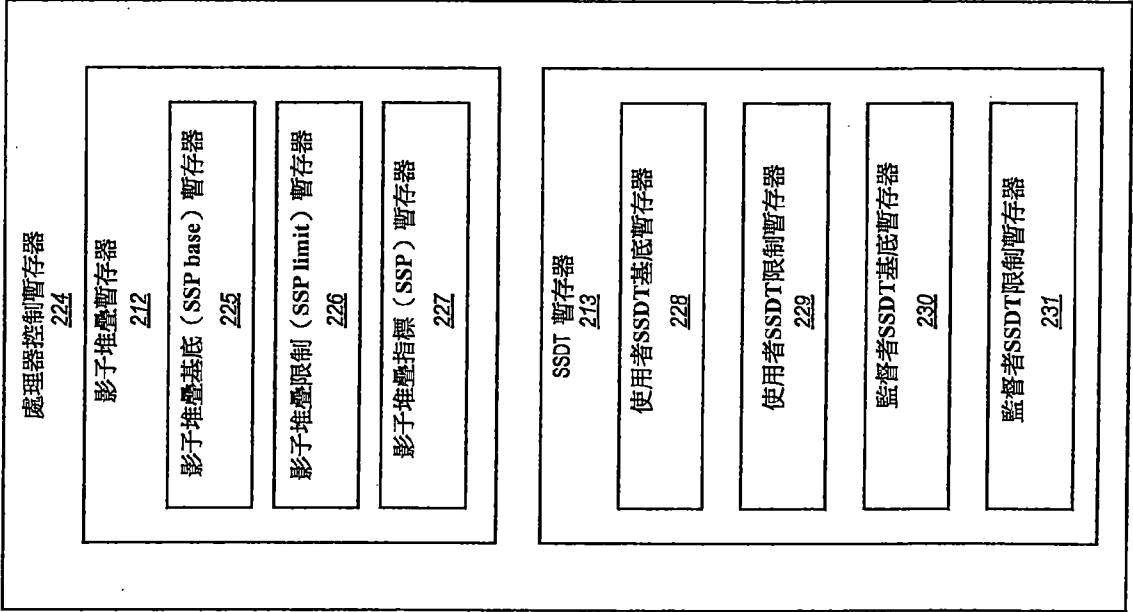
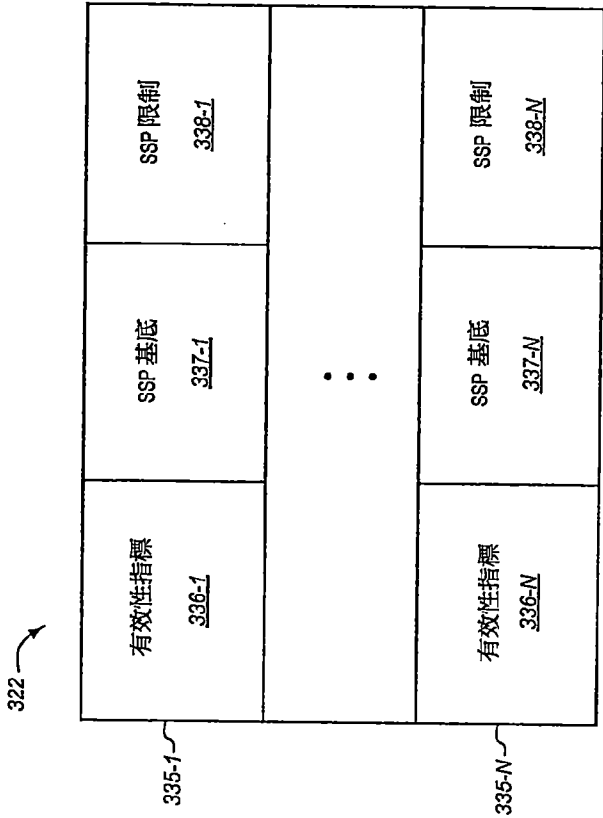


圖 3



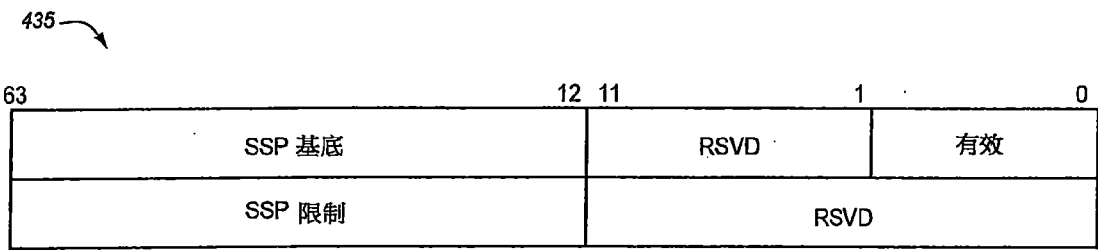


圖 4

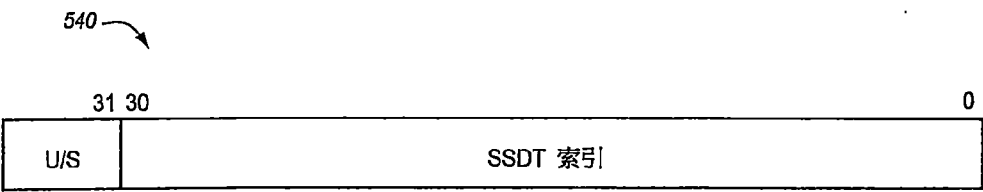


圖 5

圖 6

645 ↗

SSDT 選擇器2	652	120
SSDT 選擇器1	651	116
SSDT 選擇器0	650	112
TSS SSP	649	108
TSS SSDT 選擇器	648	104
其它欄位		100
		72
		68
狀態保存欄位		
646		
		28
保留	SS2	24
ESP2		20
保留	SS1	16
ESP1		12
保留	SS0	8
ESP0		4
保留	先前任務鏈結	0

圖 7

745 →

SSDT 選擇器	IS7	767	140
SSDT 選擇器	IS6	766	136
SSDT 選擇器	IS5	765	132
SSDT 選擇器	IS4	764	128
SSDT 選擇器	IS3	763	124
SSDT 選擇器	IS2	762	120
SSDT 選擇器	IS1	761	116
SSDT 選擇器2		760	112
SSDT 選擇器1		759	108
SSDT 選擇器0		758	104
I/O映射基底位址	保留		100
	保留		96
	保留		92
IS7 (較高32位元)			88
IS7 (較低32位元)			84
IS6 (較高32位元)			80
IS6 (較低32位元)			76
IS5 (較高32位元)			72
IS5 (較低32位元)			68
IS4 (較高32位元)			64
IS4 (較低32位元)			60
IS3 (較高32位元)			56
IS3 (較低32位元)			52
IS2 (較高32位元)			48
IS2 (較低32位元)			44
IS1 (較高32位元)			40
IS1 (較低32位元)			38
	保留		32
	保留		28
RSP2 (較高32位元)			24
RSP2 (較低32位元)			20
RSP1 (較高32位元)			16
RSP1 (較低32位元)			12
RSP0 (較高32位元)			8
RSP0 (較低32位元)			4
	保留		0

圖 8

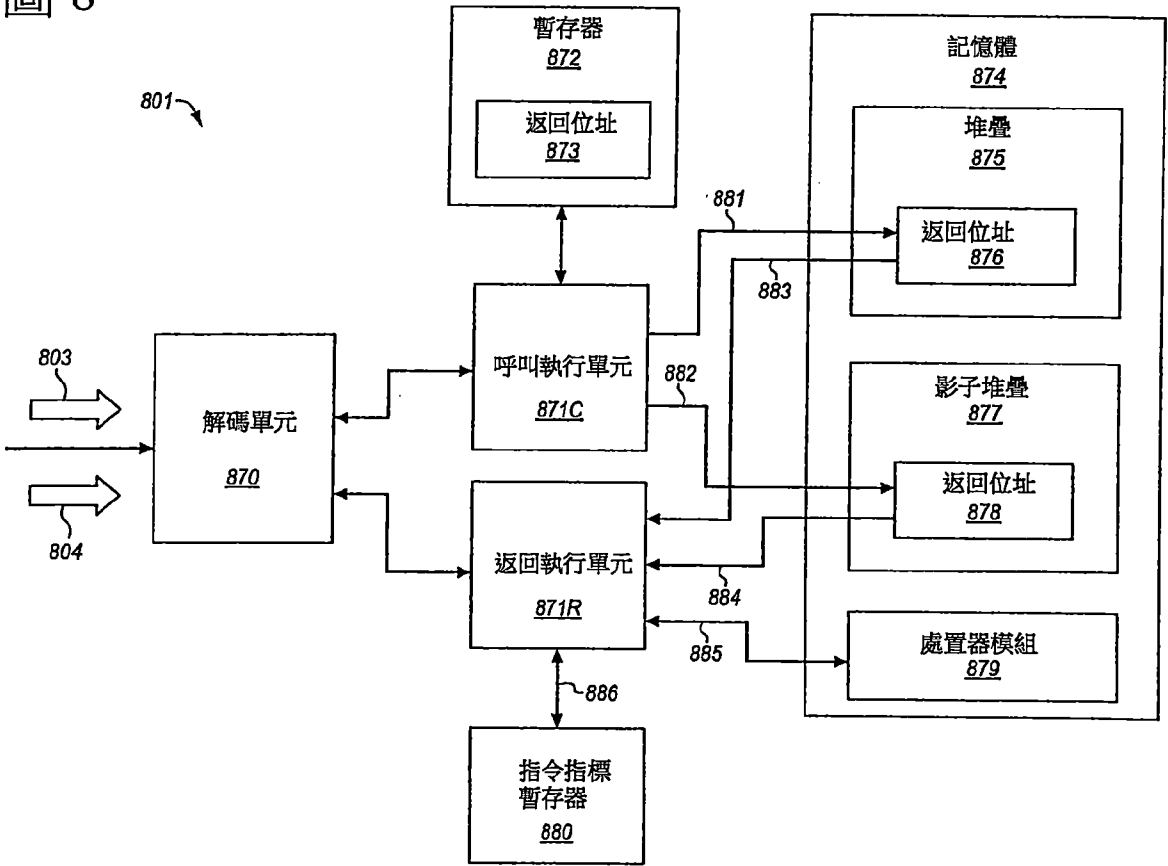


圖 9

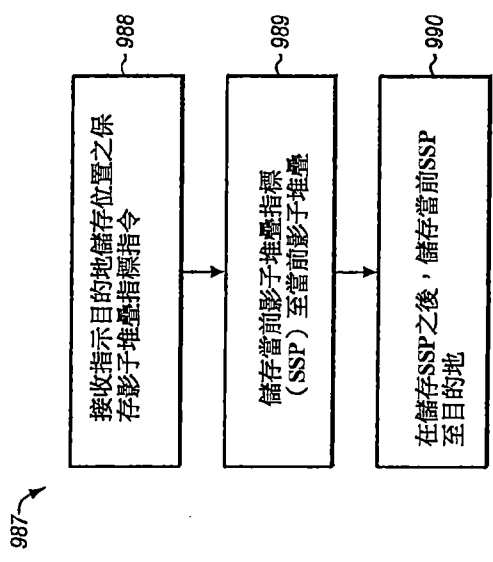


圖 10

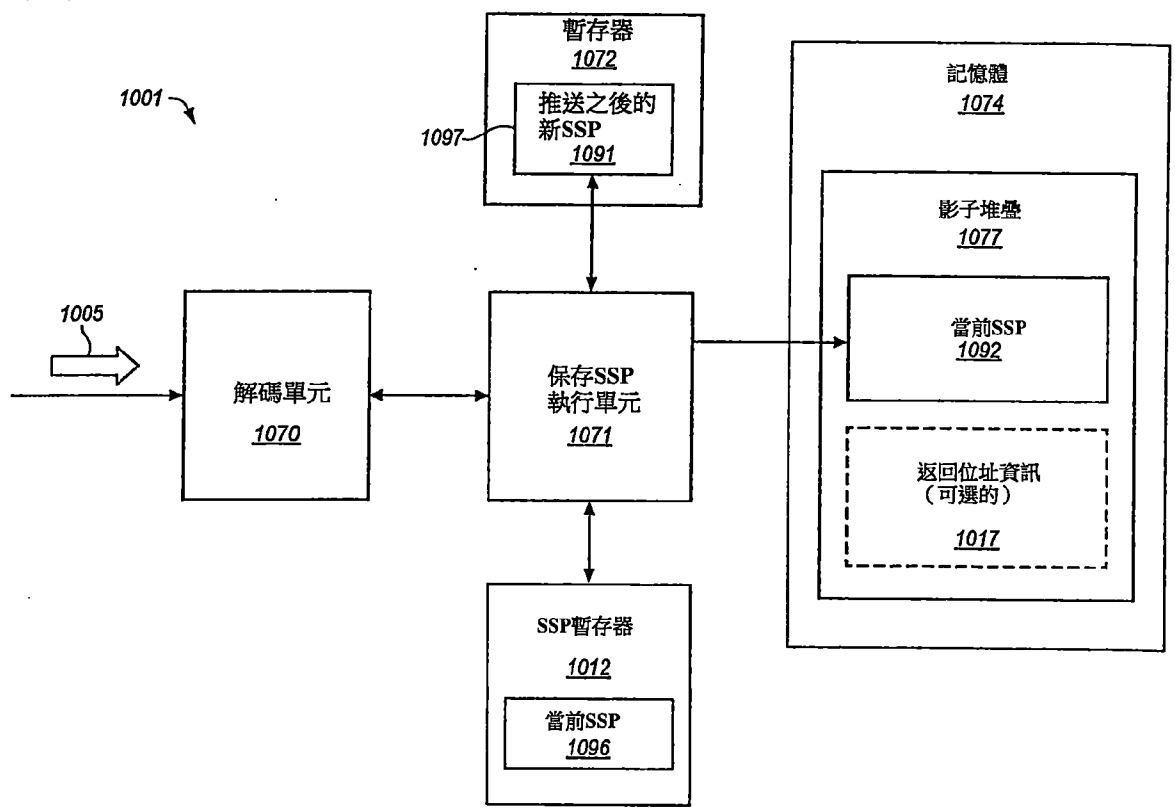
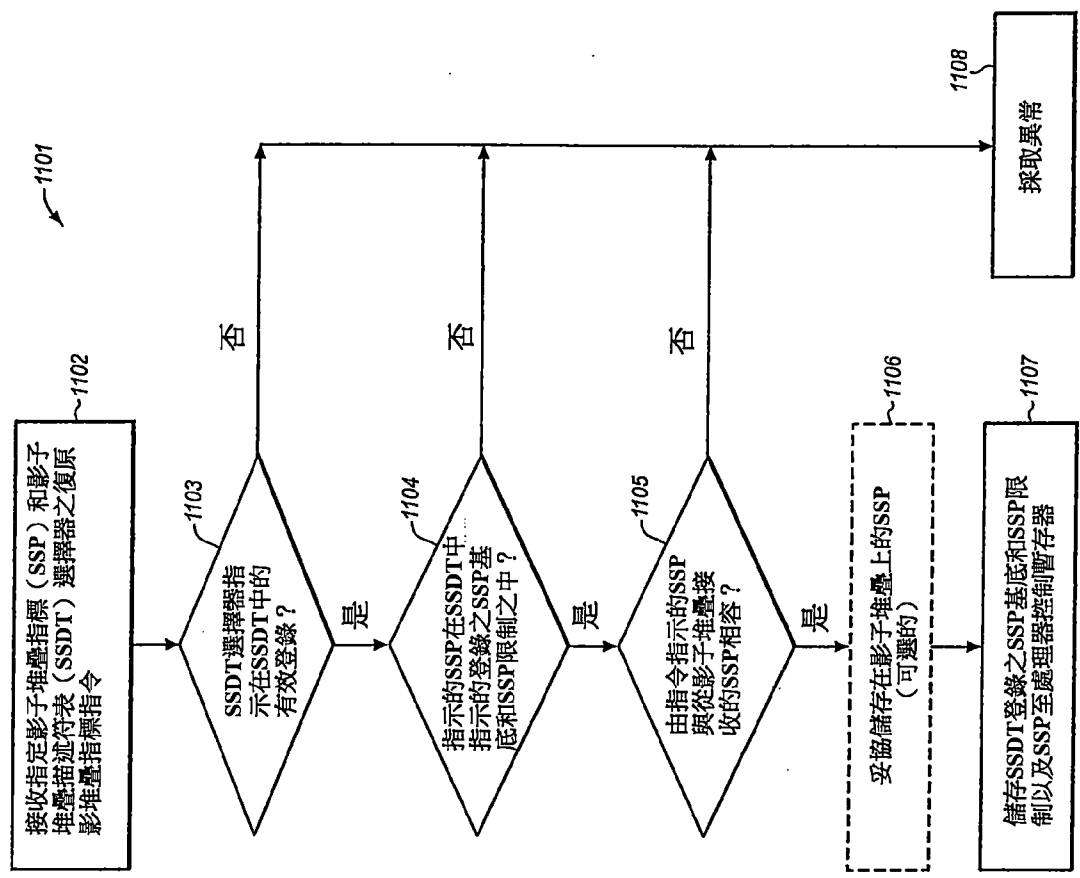


圖 11



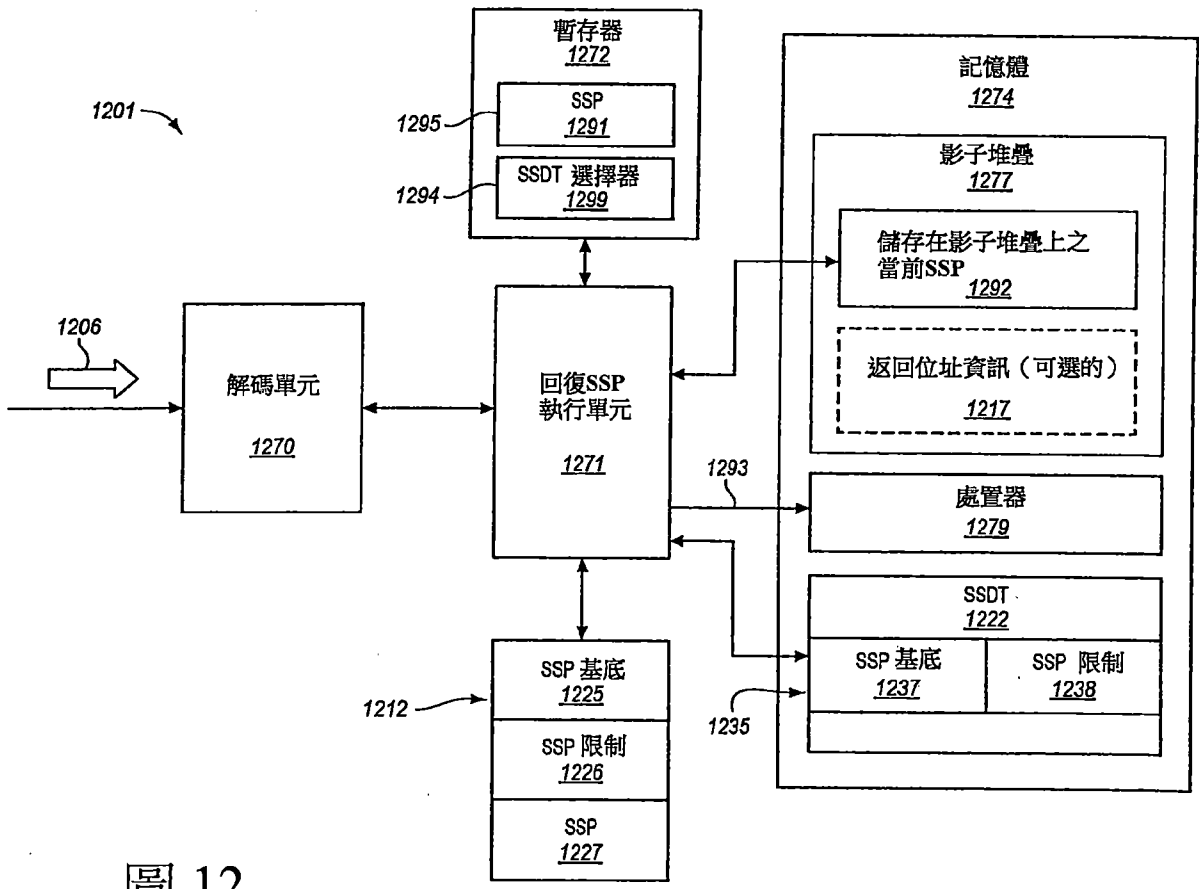


圖 12

圖 13A

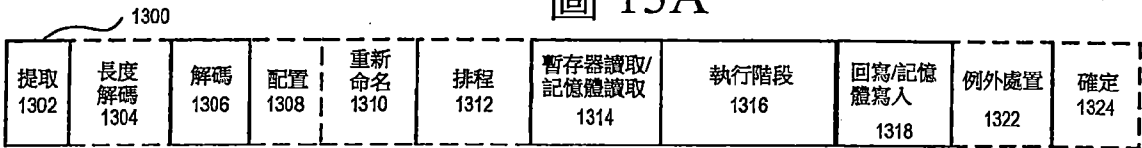
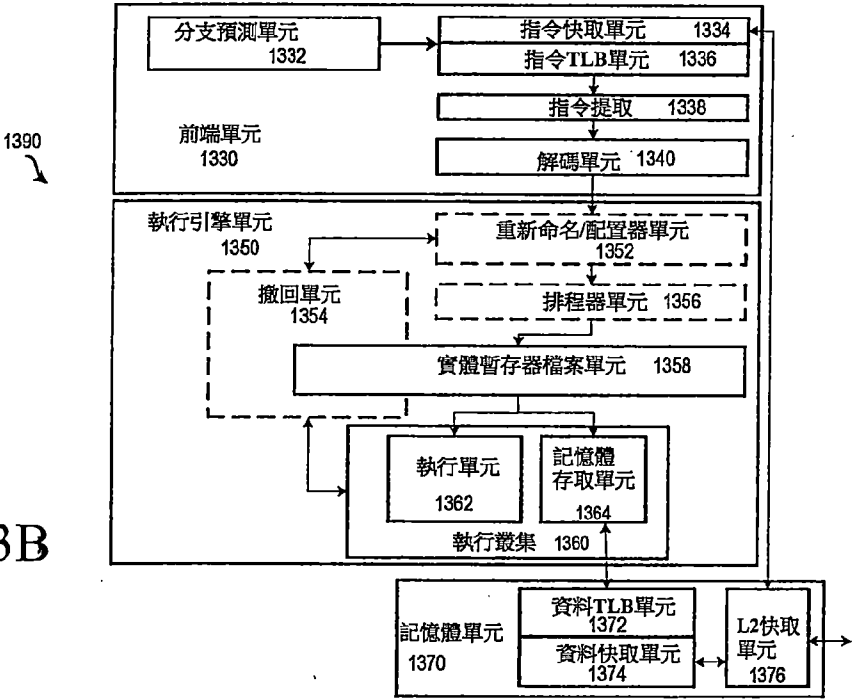


圖 13B



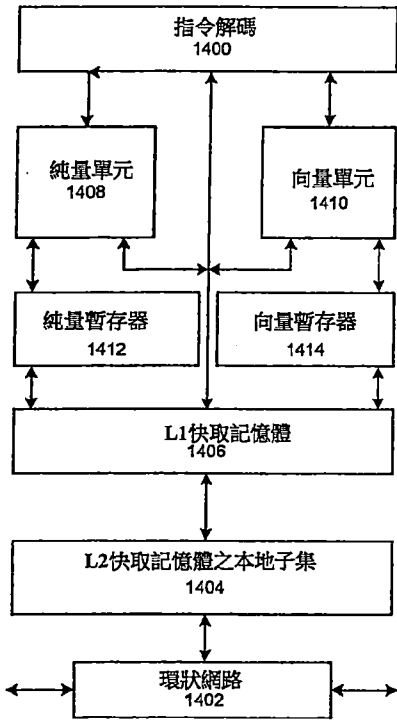


圖 14A

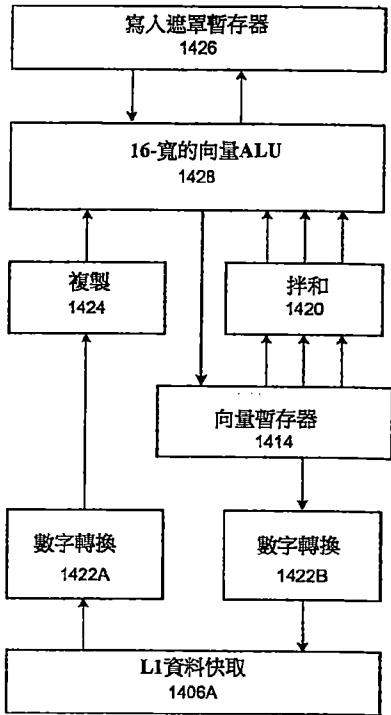


圖 14B

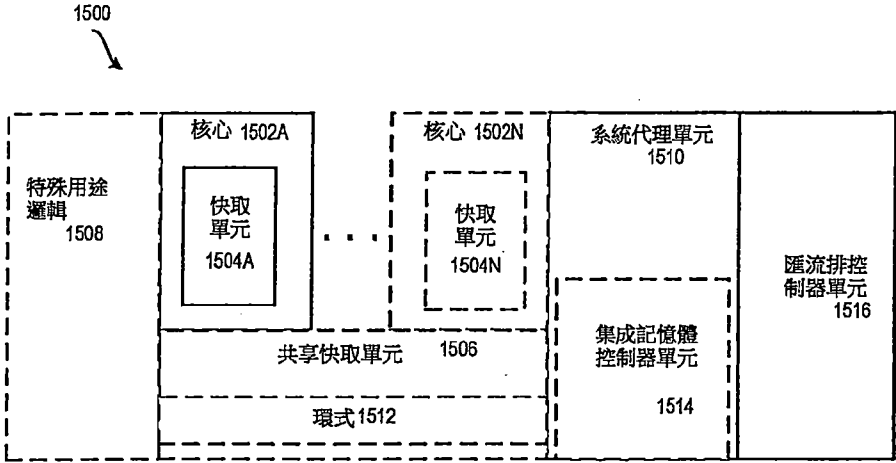


圖 15

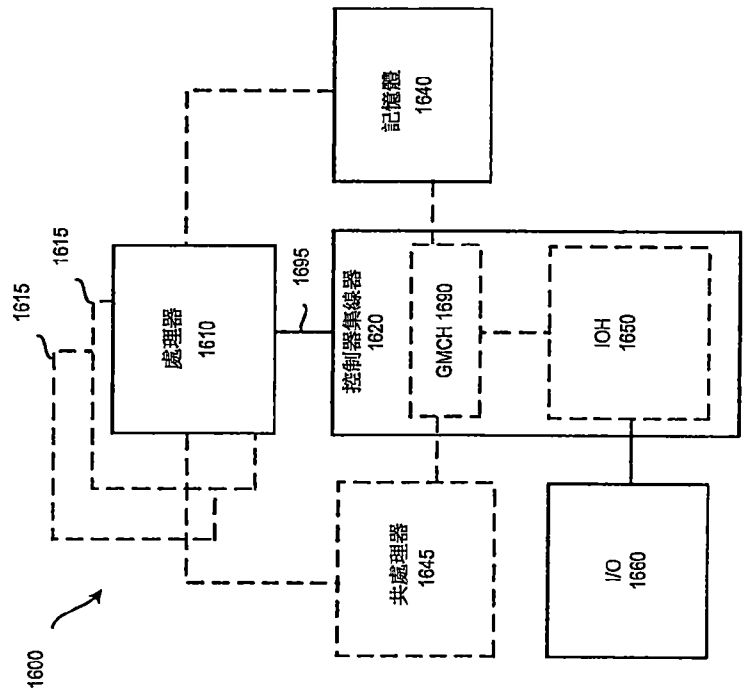


圖 16

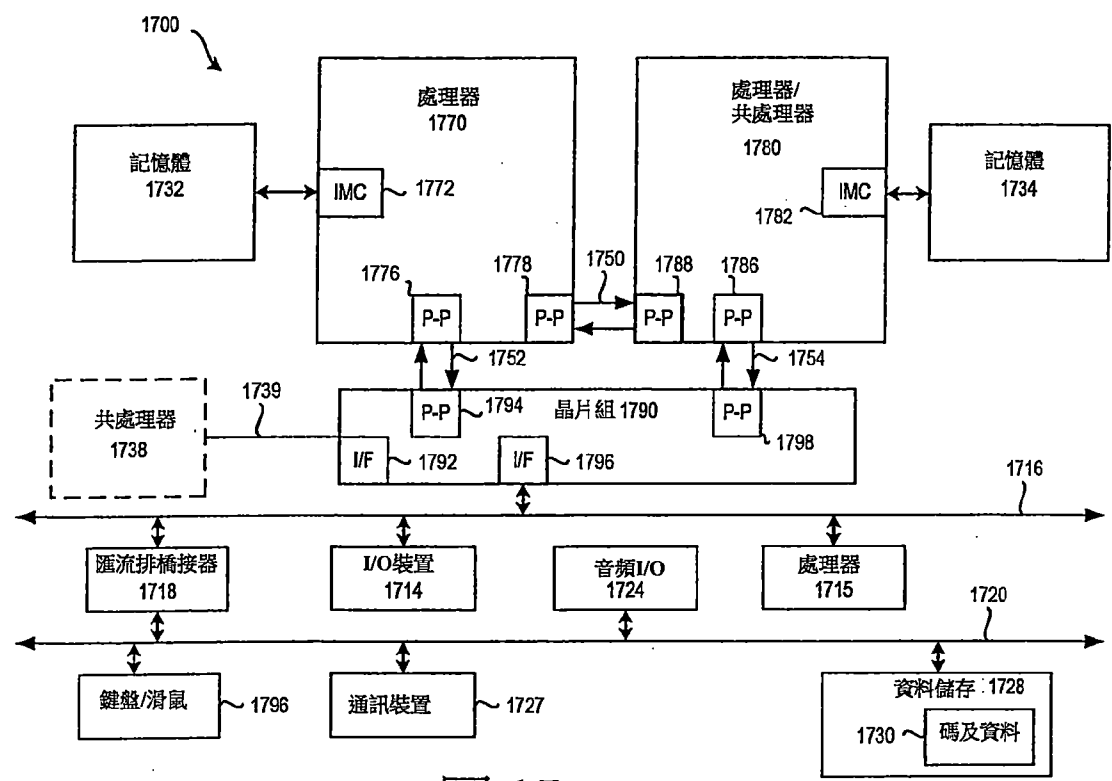


圖 17

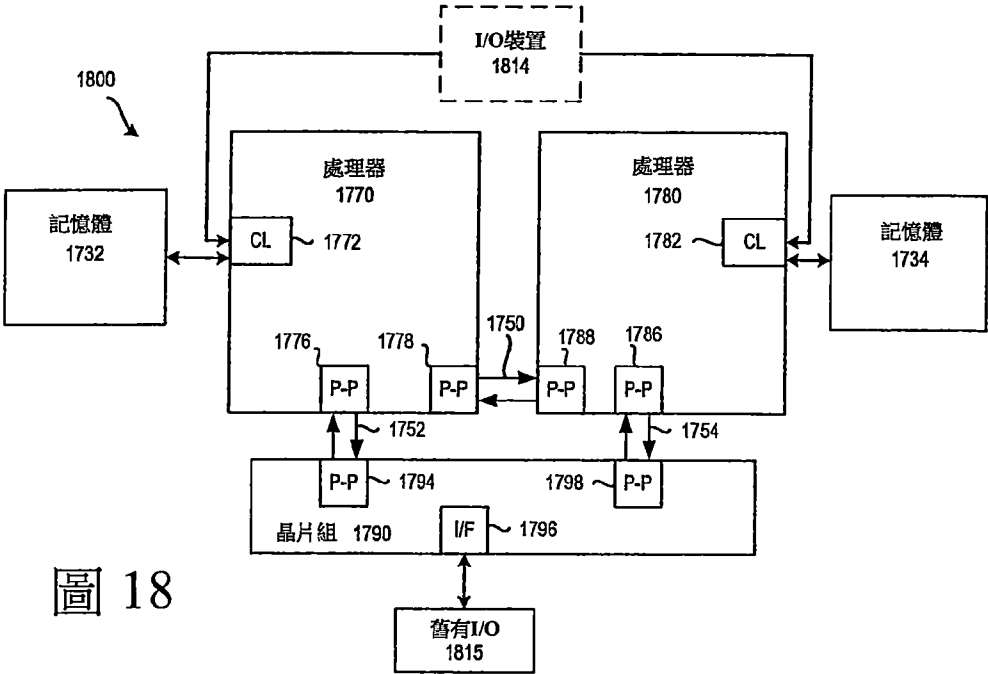


圖 18

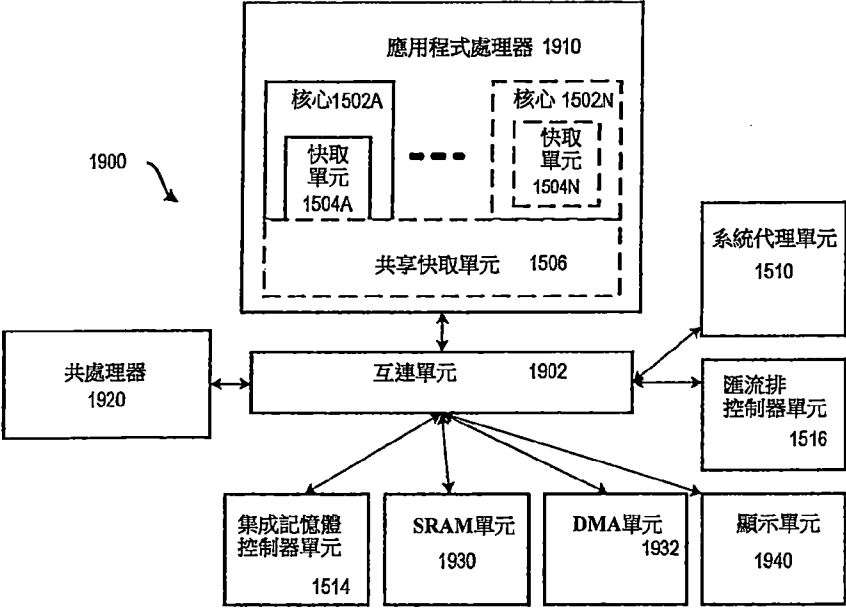


圖 19

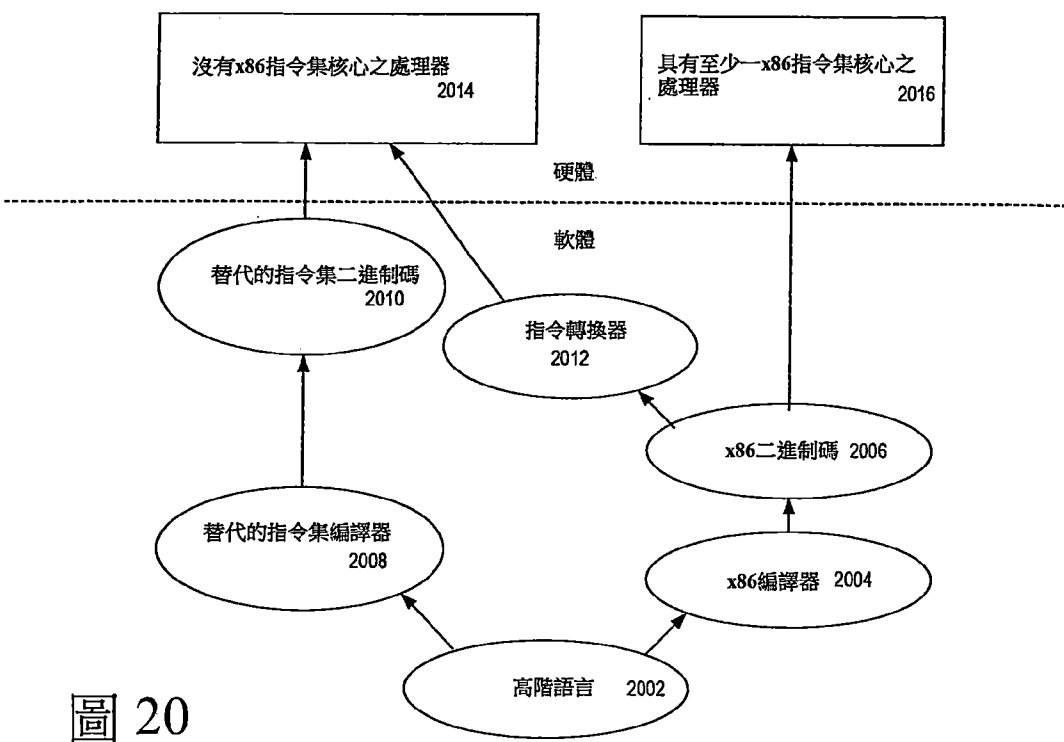


圖 20