發明專利說明書

公告本

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：94139946

※ 申請日期：94. 11. 11　　※IPC 分類：G06F13/38、12/14、H04L9/32 (2006.01)

一、發明名稱：（中文/英文）

安全資料處理及傳輸之方法及裝置

METHODS AND APPARATUS FOR SECURE DATA PROCESSING AND TRANSMISSION

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

日商新力電腦娛樂股份有限公司

SONY COMPUTER ENTERTAINMENT INC.

代表人：（中文/英文）

久多良木　健

KUTARAGI, KEN

住居所或營業所地址：（中文/英文）

日本國東京都港區南青山2-6-21

2-6-21, MINAMI-AOYAMA, MINATO-KU, TOKYO 107-0062, JAPAN

國　籍：（中文/英文）

日本　　JAPAN

三、發明人：（共 2 人）

姓　名：（中文/英文）

1. 鈴置　雅一
   SUZUOKI, MASAKAZU
2. 田山　明之
   HATAKEYAMA, AKIYUKI

國　籍：（中文/英文）

1. 日本　　JAPAN
2. 日本　　JAPAN

四、聲明事項：

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

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2004年11月12日；10/985,354

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係關於用於安全資料處理之方法及裝置，其在(例如)寬頻環境下使用用於安全資料處理之多處理器架構。

【先前技術】

即時多媒體網路應用變得愈來愈重要。此等網路應用需要極快處理速度，例如每秒數千個百萬位元之資料。傳統網路架構，例如網際網路，以及目前嵌入(例如)Java模型之程式化模型使到達此類處理速度變得極為困難。

傳統電腦網路，例如用於辦公網路之區域網路(local area network；LAN)以及網際網路等全球網路，其電腦及計算器件主要係設計用於獨立計算。資料及應用程式("應用程式")於電腦網路上之共享並非此等電腦及計算器件之主要設計目的。此等電腦及計算器件通常也使用由不同製造商製造的各種不同處理器來設計，例如Motorola、Intel、Texas Instruments、Sony及其他公司。此等處理器之各個具有其自身特定的指令集及指令集架構(instruction set architecture；ISA)，即其自身特定的組合語言指令集、用於主要計算單元之結構以及用於執行此等指令之記憶體單元。因此，要求程式設計師瞭解每一處理之指令集及ISA，以寫入用於此等處理器之應用程式。現今電腦網路上電腦及計算器件之此異質組合使資料及應用程式之處理與共享複雜化。此外，常常需要相同應用程式之多個版本，以應付此異質環境。

與全球網路，尤其係網際網路連接的電腦及計算器件之類型十分廣泛。除個人電腦(personal computer；PC)及伺服器外，此等計算器件還包括蜂巢式電話、行動電腦、個人數位助理(personal digital assistant；PDA)、視訊轉換盒、數位電視及許多其他器件。此多種電腦及計算器件中的資料及應用程式共享產生了實質問題。

已使用許多技術來嘗試克服此等問題。該等技術包括複雜介面及複雜程式化技術等等。此等解決方案常常需要實施處理功率之實質增加。其也常常導致處理應用程式以及在網路上發送資料所需時間的實質增加。

通常在網際網路上與對應應用程式分離地發送資料。此方法不需要將應用程式與對應於應用程式之各組被發送資料一起傳送。同時，此方法將所需頻寬減至最小，頻寬也常常給使用者造成困擾。用於被發送資料之正確應用程式或最新應用程式可能無法用於用戶端電腦上。此方法也需要寫入各應用程式之複數個版本，以用於網路上的複數個不同ISA及處理器使用之指令集。

Java模型嘗試解決此問題。此模型使用符合嚴格安全協定的小應用程式("小型應用程式(applet)")。從網路上的伺服器電腦傳送用戶端電腦("用戶端")需要運行的小型應用程式。為避免必須將不同版本之相同微應用程式傳送至使用不同ISA之用戶端，所有Java小型應用程式運行於用戶端的Java虛擬機器上。Java虛擬機器為模擬具有Java ISA及Java指令集之電腦的軟體。然而，此軟體運行於用戶端ISA

及用戶端指令集上。針對每一不同ISA及用戶端指令集提供Java虛擬機器之一版本。因此不需要複數個不同版本之各小型應用程式。每一用戶端僅下載用於其特定ISA及指令集的當前Java虛擬機器，以運行所有Java小型應用程式。

儘管對必須為各不同ISA及指令集寫入不同版本之應用程式的問題提供了解決方案，Java處理模型需要用戶端電腦上的額外軟體層。此額外軟體層明顯地劣化處理器處理速度。此速度降低對於即時多媒體應用尤其明顯。下載的Java應用程式也可能包含病毒、處理故障等。此等病毒及故障可毀損用戶端資料庫並導致其他損壞。儘管用於Java模型之安全協定嘗試藉由實施軟體"沙箱(sandbox)"(即用戶端記憶體空間，超過其則Java微應用程式無法寫入資料)克服此問題，此軟體驅動安全模型在其實施中常常不安全，且需要更多處理。

因此，本技術中需要用於單元架構內的資料安全處理之新方法及裝置。

【發明內容】

為克服上述問題中的至少一部分問題，亦已開發出一新的電腦(及網路)架構。依據此新的電腦架構，電腦網路所有部件，即網路之所有電腦及計算器件，皆係由一共同計算模組(或單元)構成。此共同計算模組具有一致的結構且較佳的係採用相同的ISA。該網路之部件可為(例如)用戶端、伺服器、PC、行動電腦、遊戲機、PDA、視訊轉換盒、器具、數位電視及使用電腦處理器之其他器件。該一致的模組結

構藉由網路部件提供應用程式及資料的有效、高速處理，以及應用程式及資料於網路上的快速傳輸。此"結構"還簡化了各種尺寸及處理功率的網路部件之構建以及此等部件所處理之應用程式的準備。

新的電腦架構亦採用能透過網路發送資料及應用程式以及能在該網路的各部件間處理資料及應用程式之一新程式化模型。此程式化模型採用一軟體單元，其透過該網路發送以便由該網路部件中的任何部件來處理。每一軟體單元皆具有相同的結構並可能兼含應用程式與資料。由於該模組電腦架構所提供的高速處理及傳輸速度，能快速地處理此等單元。該等應用程式之代碼較佳的係基於相同的共同指令集及ISA。每一軟體單元較佳的係包含一全球識別(全球ID)及說明單元處理所需要的計算資源數量之資訊。由於所有計算資源皆具有相同的基本結構並採用相同的ISA，可執行此處理之特定資源可位於該網路上的任何地方並得以動態指派。

該基本處理模組係一處理器元件(processor element；PE)。一PE較佳的係包含耦合於一共同內部位址及資料匯流排之一處理單元(processing unit；PU)、一直接記憶體存取控制器(direct memory access controller；DMAC)以及複數個附著處理單元(attached processing unit；APU)，例如四個APU。PU及APU與一共享動態隨機存取記憶體(dynamic random access memory；DRAM)互動，該動態隨機存取記憶體(DRAM)可具有一交叉架構。PU對APU所作的資料及應用

程式處理進行排程及協調。APU以平行且獨立的方式執行此處理。DMAC控制PU及APU對儲存於該共享DRAM內的資料及應用程式之存取。

依據此模組結構，網路部件所使用的PE之數目基於該部件需要的處理功率。例如，一伺服器可能採用四個PE，一工作站可能採用二個PE而一PDA可能採用一個PE。一PE中被指派以處理一特定軟體單元之APU數目取決於該單元內的程式及資料之複雜性及大小。

該複數個PE可與一共享DRAM相關聯，而DRAM可被分離為複數個區段，此等區段中的每一區段係分離為複數個記憶體儲存庫。可藉由一儲存庫控制器控制DRAM之每一區段，而PE之每一DMAC皆可存取每一儲存庫控制器。此組態中，每一PE之DMAC皆可存取該共享DRAM之任何部分。

DRAM可包括沙箱，以從用於一APU所處理之程式的資料提供一安全位準，其防止用於另一APU所處理之程式的資料之毀損。各沙箱定義共享DRAM之一區域，超過該區域則特定APU或APU集無法讀取或寫入資料。

雖然使用沙箱提供防止資料毀損的某種安全措施，其並未解決故意軟體盜錄的問題。由於給定PE內之複數個APU係耦合於共同內部匯流排上，一APU可監看運行於另一APU上之軟體。寬頻網路情況中，需要給定PE內之兩個或更多APU運行不同應用程式。為確保高系統靈活性，需要使此等軟體程式可從不同實體獲得，例如不同軟體開發公

司。某些實例中，軟體開發公司可能需要保證其軟體應用程式安全、無被複製或以其他方式被監看之憂。

根據本發明的一或多個方面，一裝置包括：一局部記憶體；可操作以向及從該局部記憶體載送資訊之一匯流排；可操作以處理資料並且可操作性耦合至該局部記憶體之一或多個算術處理單元；以及可操作以將該裝置放置於複數個操作模式之至少一個操作模式內的一安全電路，該複數個操作模式包括一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送。

根據本發明之一或多個其他方面，該安全電路係可操作以將該裝置放置於兩個操作模式之至少一個操作模式內，其中該等兩個操作模式包括以下模式之一：(i)一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送，但該外部器件無法啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送；以及(ii)一第二模式，藉此該裝置或該外部器件皆無法啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送，以及該第三模式。

安全電路較佳的係包括安全電路外部之器件不可存取的秘密資料區域，並且該秘密資料區域包含第一密鑰及第二密鑰。安全電路較佳的係還包括安全電路外部之器件可存取的可存取資料區域。另外，安全電路包括邏輯電路，其在該裝置處於第二模式時可操作以將該第一密鑰之副本放置於該可存取資料區域內。使用該裝置前，較佳的係在可控程序中將第一密鑰及第二密鑰儲存於秘密資料區域內，藉此保持安全。

安全電路較佳的係在該裝置運行一鑑別例行程式時將該裝置放置於第二模式中，其包括執行解密程式及執行鑑別程式，該鑑別程式包括第二密鑰之副本，並且已根據第一密鑰加密該鑑別程式。該裝置執行解密程式，以便將可存取資料區域內包含的第一密鑰之副本用於解密該鑑別程式。

安全電路之邏輯電路較佳的係對鑑別程式之執行作出回應而將第二密鑰之副本放置於可存取資料區域內；並且該邏輯電路決定鑑別程式內包含的第二密鑰之副本是否匹配可存取資料區域內包含的第二密鑰之副本。

安全電路可操作以在鑑別程式內包含的第二密鑰之副本匹配可存取資料區域內包含的第二密鑰之副本時將該裝置放置於第三模式中。

根據本發明之一或多個其他方面，將複數個上述裝置置放於單一器件內。

根據本發明之一或多個其他方面，一方法包括將一裝置

放置於複數個操作模式之至少一項中，其中：該裝置包括一局部記憶體、可操作以向及從該局部記憶體載送資訊之一匯流排、可操作以處理資料並且可操作性耦合至該局部記憶體之一或多個算術處理單元以及可操作以將該裝置放置於該等操作模式內之一安全電路；以及該複數個操作模式包括一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送。

根據本發明的一或多個其他方面，一裝置包括：一主要處理單元；複數個附著處理單元，各處理單元包括一局部記憶體及一解密單元，並且各處理單元可操作以進入一正常操作模式或一安全操作模式；以及一共享記憶體，其中：該主要處理單元可操作以啟動該共享記憶體與該等附著處理單元之一給定處理單元間的資料傳輸，當該給定附著處理單元處於正常模式時該等資料傳送繞過該解密單元，且該主要處理單元不能夠：(i)啟動從該給定附著處理單元至該共享記憶體之資料傳送；或(ii)啟動從該共享記憶體至該給定附著處理單元之資料傳送，當該給定附著處理單元處於安全模式時該等資料傳送繞過該解密單元。

該附著處理單元較佳的係能夠啟動與共享記憶體之資料

傳送，而不論其是處於正常操作模式還是安全操作模式。附著處理單元可操作以根據一硬體重設狀況及一啟動狀況之至少一項進入安全操作模式。

各附著處理單元較佳的係包括安全儲存器，其包含實質上唯一的密鑰，該密鑰僅可由給定附著處理單元的解密單元之至少一個來存取；以及經過授權的實體。各附著處理單元之解密單元較佳的係使用密鑰來解密從共享記憶體至局部記憶體之資料傳送，其係在給定附著處理單元處於安全操作模式時由主要處理單元來啟動。各附著處理單元與實質上唯一的ID以及該裝置相關聯，該ID可係給定附著處理單元之至少一個外部的實體已知的。

較佳的係藉由該裝置外部的安全實體加密該等已加密資料，該安全實體係經過授權以使用給定附著處理單元之密鑰。安全實體可包括包含參與的附著處理單元之ID及密鑰的資料庫，用於附著處理單元之各ID及密鑰彼此相關聯。在不安全實體向安全實體提供與該密鑰相關聯之ID後，安全實體採用給定附著處理單元之密鑰加密從不安全實體接收並且未經授權以使用給定附著處理單元之密鑰的資料。

較佳的係安全實體可操作以向不安全實體提供已加密資料：不安全實體可操作以向該裝置提供已加密資料，以便將其儲存於共享記憶體內；主要處理單元可操作以啟動已加密資料從共享記憶體至給定附著處理單元之傳送，以便將加密資料輸入至解密單元內；以及給定附著處理單元之解密單元可操作以使用給定附著處理單元之密鑰解密該等

已加密資料，以便將該等資料儲存於給定附著處理單元之局部記憶體內。

或者，未經授權以使用給定附著處理單元之密鑰的不安全實體較佳的係使用第一對稱密鑰加密該等資料，向安全實體提供已加密資料，並向安全實體提供與給定附著處理單元相關聯之ID。安全實體較佳的係使用第二對稱密鑰解密不安全實體所提供之已加密資料，並使用與從不安全實體接收之ID相關聯的給定附著處理單元之密鑰加密該等資料。

不安全實體較佳的係使用第一對稱密鑰加密資料及給定附著處理器單元之ID，並向該安全實體提供已加密資料/ID。最後，該安全實體可操作以使用第二對稱密鑰加密已加密資料並向不安全實體提供加密已加密資料；該不安全實體可操作以使用第一對稱密鑰解密該等加密已加密資料，以獲得使用給定附著處理單元之密鑰產生的已加密資料，以及向該裝置提供已加密資料，以便將其儲存於共享記憶體內；該主要處理單元可操作以啟動該等已加密資料從共享記憶體至給定附著處理單元之傳送，以便將該等已加密資料輸入至解密單元內；該給定附著處理單元之解密單元可操作以使用給定附著處理單元之密鑰解密該等已加密資料，以便將該等資料儲存於給定附著處理單元之局部記憶體內。

另一替代方案中，該等資料為解密程式；未經授權以使用給定附著處理單元之不安全實體使用第一對稱密鑰加密

該解密程式，向該安全實體提供已加密之解密程式，並向安全實體提供與給定附著處理單元相關聯之ID；並且該安全實體使用第二對稱密鑰解密不安全實體所提供的已加密之解密程式，並使用與從不安全實體接收之ID相關聯的給定附著處理單元之密鑰加密解密程式及第二對稱密鑰。不安全實體較佳的係使用第一對稱密鑰加密解密程式及給定附著處理器單元之ID，並向該安全實體提供已加密資料/ID。

較佳的係，該安全實體可操作以使用第二對稱密鑰加密已加密解密程式及第二對稱密鑰並向不安全實體提供加密已加密之解密程式/第二對稱密鑰；該不安全實體可操作以使用第一對稱密鑰解密該加密已加密之解密程式/第二對稱密鑰，以獲得使用給定附著處理單元之密鑰產生的已加密解密程式/第二對稱密鑰，以及向該裝置提供已加密解密程式/第二對稱密鑰，以便將其儲存於共享記憶體內；該主要處理單元可操作以啟動已加密解密程式/第二對稱密鑰從共享記憶體至給定附著處理單元之傳送，以便將已加密解密程式/第二對稱密鑰輸入至解密單元內；該給定附著處理單元之解密單元可操作以使用給定附著處理單元之密鑰解密已加密解密程式/第二對稱密鑰，以便將解密程式及第二對稱密鑰儲存於給定附著處理單元之局部記憶體內。

另外，不安全實體可操作以使用第一對稱密鑰加密資料並向該裝置提供已加密資料，以便將其儲存於共享記憶體內。給定附著處理單元能夠從共享記憶體接收已加密資料

並繞過解密單元將其傳送至局部記憶體內。當從共享記憶體接收已加密資料並將其傳送至局部記憶體內時，給定附著處理單元可處於正常模式或安全模式。給定附著處理單元可操作以使用解密程式及第二對稱密鑰解密已加密資料。主要處理單元可操作以啟動已加密資料從共享記憶體至給定附著處理單元之局部記憶體的傳送，同時繞過解密單元。

結合附圖閱讀本文之說明，熟悉技藝人士將明白本發明之其他觀點、特徵及優點。

【實施方式】

圖1顯示用於根據本發明之電腦系統1的總體架構。系統1包括網路4，其與複數個電腦及計算器件連接。網路4可為區域網路、全球網路，例如網際網路，或任何其他電腦網路。

例如，與網路4(網路"部件")連接的電腦及計算器件包括用戶端電腦6、伺服器電腦8、個人數位助理(personal digital assistant；PDA)10、數位電視(digital television；DTV)12及其他有線或無線電腦及計算器件。網路4之部件所利用的處理器由相同共同計算模組構成。此等處理器較佳的係全部具有相同ISA並根據相同指令集執行處理。任何特定處理器內包括的模組數目取決於該處理器所需的處理功率。

例如，由於系統1之伺服器8比用戶端6執行更多資料及應用程式之處理，伺服器8比用戶端6包含更多計算模組。另一方面，此範例中PDA 10執行最少數量之處理。因此，PDA

10包含最少數目之計算模組。DTV 12執行用戶端6與伺服器8之間的一處理位準。因此，DTV 12包含用戶端6與伺服器8之間的許多計算模組。如下所述，各計算模組包含處理控制器及複數個相同處理單元，其用於執行在網路4上發送的資料及應用程式之平行處理。

系統1之此均勻組態有助於可調適性、處理速度及處理效率。由於系統1之各部件使用相同計算模組的一或多個(或某部分)來執行處理，因此對資料與應用程式執行實際處理之特定電腦或計算器件係不重要的。此外，可將一特定應用程式及資料之處理分配給該網路之各部件。藉由在整個系統中，對包含由系統1來處理的資料及應用程式之單元作唯一識別，可將處理結果發送給請求進行該處理之電腦或計算器件，而無論此處理係發生於何處。由於執行此處理之模組具有共同的結構且採用一共用的ISA，因此能避免為獲得該等處理器之間的相容性而添加一層軟體以致帶來計算負擔。此架構及程式化模型有助於執行(例如)即時的多媒體應用程式所需要之處理速度。

為進一步利用系統1所促進的處理速度及效率，將此系統所處理的資料及應用程式封裝成經唯一識別且一致格式化之軟體單元2。每一軟體單元2皆兼含或可能兼含應用程式與資料。每一軟體單元還包含一ID以全域性地識別整個網路4及系統1中的單元。該等軟體單元之此結構一致性以及該等軟體單元在整個網路中的唯一識別有助於在該網路的任何電腦或計算器件上處理應用程式及資料。例如，一用

戶端6可能定製一軟體單元2，但是，由於用戶端6之處理能力有限，因此其將此軟體單元發送給一伺服器8以作處理。軟體單元2可在整個網路4中轉移以根據該網路4上處理資源之可用性來進行處理。

系統1之處理器及軟體單元2之均勻結構還避免當今均勻網路所存在問題中的許多問題。例如，可避免採用致力於允許在任何ISA上使用任何指令集處理應用程式之低效程式化模型(例如，諸如Java虛擬機器之類的虛擬機器)。因此，系統1實施寬頻處理之效果及效率可能遠遠超過傳統網路。

參考圖2，顯示可加以調適以用於執行本發明之一或多個特徵的處理系統100之至少一部分。為達到簡潔及清楚的目的，本文對圖2之方塊圖的參考及說明係作為對裝置100的說明，不過應瞭解，本說明可容易地等力應用於一方法之各種方面。

處理系統100包括複數個處理器102A、102B、102C及102D，應瞭解可利用任何數目之處理器，而不會背離本發明之精神與範圍。處理器100亦包括複數個局部記憶體104A、104B、104C、104D及一共享記憶體106。至少處理器102、局部記憶體104及共享記憶體106較佳的係在匯流排系統108上(直接或間接)彼此耦合，該匯流排系統係可操作以根據適當協定向及從各組件傳送資料。

處理器102之各個可具有相同結構或不同結構。可使用能夠從共享(或系統)記憶體106請求資料並操控資料以實現期

望結果的任何已知技術來實施處理器。例如，可使用能夠執行軟體及/或韌體之任何已知微處理器，包括標準微處理器、分散式微處理器等等，來實施處理器102。例如，處理器102之一或多個可為能夠請求及操控資料(例如像素資料，包括灰階資訊、色彩資訊、文字資料、多邊形資訊、視訊訊框資訊等等)之圖形處理器。

系統100之處理器102的一或多個處理器可承擔主要(或管理)處理器之角色。主要處理器可對其他處理器之資料處理進行排程及協調。

系統記憶體106較佳的係透過記憶體介面電路(未顯示)與處理器102耦合的動態隨機存取記憶體(DRAM)。儘管系統記憶體106較佳的係DRAM，記憶體106可使用其他方式來實施，例如靜態隨機存取記憶體(static random access memory；SRAM)、磁性隨機存取記憶體(magnetic random access memory；MRAM)、光學記憶體、全訊記憶體等等。

各處理器102較佳的係包括一處理器核心以及在其中執行程式的局部記憶體104之相關聯局部記憶體。此等組件可整合置放於共同半導體基板上或可根據設計者之需要分離地置放。較佳的係使用處理管線實施處理器核心，其中以管線方式處理邏輯指令。儘管可將該管線分割成處理指令的任何數目之級，管線通常包含擷取一或多個指令、解碼指令、檢查指令間的相依性、發出指令以及執行指令。在此方面，處理器核心可包括指令緩衝器、指令解碼電路、相依性檢查電路、指令發出電路以及執行級。

各局部記憶體104經由匯流排與其相關聯處理器核心102耦合，且較佳的係位於作為處理器核心之相同晶片(相同半導體基板)上。局部記憶體104較佳的並非傳統硬體快取記憶體，因為無晶片上或晶片外硬體快取記憶體電路、快取記憶體暫存器、快取記憶體控制器等等來實施硬體快取記憶體功能。由於晶片上空間常常有限，局部記憶體之大小可能遠小於共享記憶體106。

處理器102較佳的係提供資料存取請求以在匯流排系統108上從系統記憶體106複製資料(其可包括程式資料)至其個別局部記憶體104內，以便用於程式執行及資料操控。用於促進資料存取之機制可利用任何已知技術來實施，例如直接記憶體存取(direct memory access；DMA)技術。較佳的係藉由記憶體介面電路執行此功能。

參考圖3，處理器102之一或多個同樣較佳的係包括安全電路150，其可操作以將處理器102放置於複數個操作模式之至少一操作模式內。安全電路150包括秘密資料區域152、可存取資料區域154及邏輯電路156。秘密資料區域152較佳的係不能由安全電路150外部之任何器件存取。可存取資料區域154較佳的係由安全電路150外部之任何器件存取。可將秘密資料區域152及/或可存取資料區域154實施為局部記憶體106之個別部分、個別暫存器及/或個別其他儲存器件，例如ROM等等。

使用處理器102前，較佳的係在可控程序中將第一密鑰KEY 1及第二密鑰KEY 2儲存於安全電路150之秘密資料區

域152內，藉此保持安全。事實上，預期需要使用KEY 1及KEY 2，以便鑑別處理器102並將其驗證為可信器件。因此，當使用處理器102時以及使用處理器102前，例如製造期間，需要將KEY 1及KEY 2保持秘密且處於經過授權方之控制內。

秘密資料區域152、可存取資料區域154及邏輯電路156較佳的係在連接線路158上彼此耦合，連接線路可使用一匯流排組態來加以實施。邏輯電路156較佳的係藉由一或多個資料線路160耦合至暫存器，資料線路亦可使用一匯流排組態來加以實施。

如上所述，安全電路150較佳的係可操作以將處理器102放置於複數個操作模式之至少一操作模式內。此等模式較佳的係包括第一模式(正常模式)，藉此處理器102及任何一或多個外部器件可啟動資訊進入或離開處理器102之傳送，例如進入或離開局部記憶體104。此等模式較佳的係還包括第二模式(隔離模式)，藉此處理器102及任何一或多個外部器件皆不能啟動資訊進入或離開處理器102之傳送。此等模式較佳的係還包括第三模式(安全模式)，藉此處理器102可啟動資訊進入或離開處理器102之傳送，但任何一或多個外部器件無法啟動資訊進入或離開處理器102之傳送。

參考圖4至6可更好地瞭解安全電路150之操作，該等圖式係流程圖，其說明根據本發明之處理器102的特定安全能力。在此方面，假定處理器102係預設為第一正常操作模式(動作200)。請記得，在第一模式內，處理器102及任何一或

多個外部器件(例如另一處理器)可啟動資訊進入或離開處理器102之局部記憶體104之傳送。應注意在本發明之替代具體實施例中，處理器102在初始化(例如啟動)後可能無法進入第一操作模式，或者僅可進入該模式一較短時間，以利於以下將說明的第二或第三操作模式。

動作202中，處理器102可運行鑑別例行程式，以便達到一可信狀態。可藉由從運行於處理器102上之應用程式呼叫或藉由從運行於處理器102外部之程式呼叫來啟動鑑別例行程式(動作202)。在本發明之替代具體實施例中，處理器102可隨預設狀況在初始化時或稍後運行鑑別例行程式，而不需要從應用程式呼叫。為對啟動鑑別例行程式作出回應，處理器102較佳的係執行一解密程式。應注意可從置放處理器102之模組內的適當記憶體獲得解密程式，或者其可從該模組外部之來源獲得。此類外部來源之範例包括可包含於置放模組的較大系統內之適當記憶體，或與網路4耦合的另一器件，例如執行管理功能等的伺服器8(圖1)。本發明之一或多項具體實施例中，可將解密程式包含於安全、非揮發性ROM中，例如快閃ROM。

動作206中，在處理器102執行解密程式之前、期間或作為該操作之結果，處理器102較佳的係進入第二隔離操作模式。請記得，在第二操作模式中，處理器102及任何一或多個外部器件皆不能啟動資訊進入或離開局部記憶體104之傳送。

動作208中，處理器102較佳的係接收在鑑別例行程式期

間使用的鑑別程式。應注意處理器102接收已加密鑑別程式的時序並非剛性的；事實上，可在執行鑑別例行程式之前或期間的任何適當時間接收程式。較佳的係根據KEY 1加密鑑別程式，以便其僅可藉由經過授權之方式加以利用。另外，鑑別程式較佳的係包括KEY 2，其識別該鑑別程式。例如，KEY 2可為一序號、一雜湊結果等等。

較佳的係將已加密鑑別程式儲存於處理器102中的適當記憶體、包含處理器102之模組或處理器102或模組外部之記憶體內。最佳的係將已加密鑑別程式儲存於包含處理器102之模組外部的記憶體內，但仍在包含該模組之器件中。另外較佳的係藉由經過授權之實體在一可控程序中執行鑑別程式之加密以及其在適當記憶體中的儲存。事實上，需要始終保持鑑別程式之完整性，以便確保其在鑑別處理器102或任何其程式的使用方面較為有效。本發明之一或多項具體實施例中，可將鑑別程式包含於安全、非揮發性ROM中，例如快閃ROM。

動作210中，解密程式之執行較佳的係使KEY 1之安全副本可從秘密資料區域152加以讀取，並被儲存於安全電路150內之可存取資料區域154中。例如，邏輯電路156較佳的係可操作以對處理器102之暫存器(未顯示)內的特定資料之存在作出回應而將KEY 1之副本從秘密資料區域152傳送至可存取資料區域154。由於處理器102處於第二隔離模式，可存取資料區域154內KEY 1之副本的存在並不代表安全之破壞。事實上，處理器102及任何外部器件皆不能啟動KEY

1透過局部記憶體104或以其他方式離開處理器102之傳送。

動作212中，解密程式較佳的係利用KEY 1以解密該已加密鑑別程式，以便其可由處理器102加以執行。執行鑑別程式期間，較佳的係將秘密資料區域152內包含的KEY 2之副本寫入可存取資料區域154(動作214)。例如，邏輯電路156較佳的係可操作以根據鑑別程式對可寫入暫存器的特定資料作出回應而將KEY 2之副本從秘密資料區域152傳送至可存取資料區域154。

動作216中，較佳的係決定可存取資料區域154內之KEY 2的副本是否匹配鑑別程式內包含的KEY 2之副本。請記得，鑑別程式包含KEY 2之副本，其在解密鑑別程式時變得可用(動作212)。例如，可根據鑑別程式本身之執行將鑑別程式內包含的KEY 2之副本暫時儲存於局部記憶體104內或可將其寫入可存取資料區域154。同樣，此不代表安全之破壞，因為處理器102在此程序期間處於隔離模式，因此處理器102外部的未經授權器件無法獲得KEY 2之副本。

若鑑別程式內包含的KEY 2之副本不匹配從秘密資料區域152獲得的KEY 2之副本，則鑑別處理器102之程序終止(動作218)。然而，當KEY 2之此等副本匹配時，較佳的係清除可存取資料區域154內包含的KEY 1及KEY 2之副本(動作220)，且處理器102較佳的係進入第三安全操作模式(動作222)。例如，邏輯電路156可從可存取資料區域154清除KEY 1及KEY 2之副本並可使處理器102進入第三安全操作模式。

請記得，在第三安全操作模式中，處理器102可啟動資訊

進入或離開局部記憶體104之傳送。換言之，在第三安全操作模式中，處理器102可啟動資訊進入或離開處理器102之傳送，但處理器102外部之任何器件無法啟動此類資訊之傳送。一旦處理器102已進入第三安全操作模式，則將其視為可執行操作及操控資料之可信器件，而不必擔心未經授權之實體可獲得此類資料。事實上，若處理器102本身不加以啟動，其他處理器甚至無法取得對處理器102內之資料的存取權。

其優點在於，可信處理器102可提供許多有用功能，例如在圖1所說明的分散式系統內。此等功能包括提供安全外部記憶體控制器，其具有僅可由經過授權之器件存取的記憶體區域、僅可由經過授權之器件修改的安全時脈器件、可信請求機制以及能夠鑑別開機碼之安全處理元件(例如使用已公用密鑰為主之鑑別等等)。

根據本發明之一或多方面，可信處理器102可由包括主要處理器之其他處理器102來使用，以執行解密操作。例如，處理器102之一可需要藉由可信處理器102解密儲存於主要記憶體106內之資料。因此，該處理器可向可信處理器102傳送一請求，其指示資料位於主要記憶體106內的何處以及指示需要執行何種解密例行程式之參數的至少一項。(或，可預定解密例行程式，從而可省略此類參數。)對該請求作出回應，可信處理器102可從主要記憶體106讀取已加密資料並將該等資料發送其至局部記憶體104內，以及執行解密程序。若其他處理器102執行請求前可信處理器102未擁有

解密密鑰(例如KEY 1或KEY 2)，則較佳的係亦藉由請求處理器102提供此類解密密鑰或關於如何獲得此類密鑰之資訊。接著，較佳的係將已解密資料寫回至主要記憶體106內及/或寫入請求處理器102之局部記憶體104。

現在提供用於多處理器系統之較佳電腦架構的說明，其適用於執行本文說明的一或多個特徵。根據一或多個具體實施例，可將多處理器系統實施為單一晶片解決方案，其可操作以用於多媒體應用程式之獨立及/或分散式處理，例如遊戲系統、家用終端、PC系統、伺服器系統及工作站。某些應用程式中，例如遊戲系統及家用終端，可需要即時計算。例如，在即時、分散式遊戲應用程式中，網路影像解壓縮、3D電腦圖形、聲頻產生、網路通信、實體模擬及人工智慧程序之一或多項必須加以足夠迅速地執行，以為使用者提供即時幻視體驗。因此，多處理器系統內之每一處理器必須在一較短及可預測時間內完成任務。

為此目的，以及根據此電腦架構，多處理電腦系統之所有處理器皆係由一共同計算模組(或單元)構成。此共同計算模組具有一致的結構且較佳的係採用相同的指令集架構。該多處理電腦系統可由一或多個用戶端、伺服器、PC、行動電腦、遊戲機、PDA、視訊轉換盒、器具、數位電視及使用電腦處理器之其他器件來形成。

若需要，則複數個電腦系統也可能係一網路之部件。該一致的模組結構使得能藉由該多處理電腦系統對應用程式及資料進行有效、高速處理，而且若採用一網路，則還能

夠透過網路快速傳輸應用程式及資料。此結構還簡化了該網路中不同尺寸及處理功率的部件之構建以及為此等部件之處理而對應用程式作的準備。

參考圖7，基本處理模組為處理器元件(PE)300。PE 300包含輸入/輸出介面302、處理單元(PU)304以及複數個子處理單元308，即子處理單元308A、子處理單元308B、子處理單元308C及子處理單元308D。局部(或內部)PE匯流排312在PU 304、子處理單元308及記憶體介面311之中發送資料及應用程式。該局部PE匯流排312可具有(例如)傳統架構，或可作為封包交換網路來實施。若實施為封包交換網路，儘管需要更多硬體，但可增加可用頻寬。

可使用實施數位邏輯之各種方法來構成PE 300。然而，較佳的係將PE 300構建為在一矽基板上採用一互補金氧半導體(CMOS)之一單一積體電路。基板之替代性材料包括砷化鎵、砷化鎵鋁及採用各種摻雜劑的其他所謂III-B化合物。亦可使用超導材料，例如快速單通量子(rapid single-flux-quantum；RSFQ)邏輯，來實施PE 300。

PE 300經由一高頻寬記憶體連接316而與一共享(主要)記憶體314密切相關。儘管記憶體314較佳的係動態隨機存取記憶體(DRAM)，但亦可使用其他構件而將記憶體314實施為(例如)靜態隨機存取記憶體(SRAM)、磁性隨機存取記憶體(MRAM)、光學記憶體、全訊記憶體等等。

PU 304及子處理單元308較佳的係各與包括直接記憶體存取DMA功能性之一記憶體流控制器(memory flow

controller；MFC)耦合，其與記憶體介面311組合，可促進DRAM 314及子處理單元308與PE 300之PU 304間的資料傳送。應注意，該DMAC及/或該記憶體介面311可能係關於子處理單元308及PU 304整合或分離地加以置放。事實上，該DMAC功能及/或該記憶體介面311功能可與子處理單元308及PU 304之一或多個(較佳的係全部)整合。同樣應注意，DRAM 314可能係關於PE 300整合或分離地加以置放。例如，可如圖示插圖所示意將DRAM 314置放於晶片外，或可用積體方式將DRAM 314置放於晶片上。

例如，PU 304可為如能夠獨立處理資料及應用程式的標準處理器。在操作中，PU 304較佳的係對子處理單元所作的資料及應用程式處理進行排程及協調。子處理單元較佳的係單指令多資料(single instruction, multiple data；SIMD)處理器。在PU 304之控制下，子處理單元以平行且獨立的方式對此等資料及應用程式執行處理。PU 304較佳的係使用PowerPC核心來實施，其係採用精簡指令集計算(RISC)技術之微處理器架構。RISC使用簡單指令之組合執行更複雜之指令。因此，用於該處理器之時序可基於更簡單及更快之操作，從而使微處理器針對給定時脈速度執行更多指令。

應注意，可藉由子處理單元308中有主要處理單元作用之一子處理單元來實施該PU 304，該子處理單元對子處理單元308所執行的資料及應用程式處理進行排程及協調。另外，處理器單元300內可實施多個PU。

依據此模組結構，特定電腦系統所使用的PE 300之數目係基於該系統需要的處理功率。例如，一伺服器可能採用四個PE 300，一工作站可能採用二個PE 300而一PDA可能採用一個PE 300。PE 300中被指派以處理特定軟體單元之子處理單元數目取決於該單元內的程式及資料之複雜性及大小。

圖8說明子處理單元(sub-processing unit；SPU)308之較佳結構及功能。SPU 308架構較佳的係填充通用處理器(其係設計成對廣泛的應用程式集實現高平均性能)與特殊用途處理器(其係設計成對於單一應用程式實現高性能)間的空隙。SPU 308係設計成對遊戲應用程式、媒體應用程式、寬頻系統等實現高性能，以及為即時應用程式之程式設計師提供高控制程度。SPU 308之某些能力包括圖形幾何管線、表面細分、快速富利葉轉換、影像處理關鍵字、資料流處理、MPEG編碼/解碼、加密、解密、器件驅動器擴展、模型化、遊戲物理學、內容建立及聲頻合成與處理。

子處理單元308包括兩個基本功能單元，即SPU核心310A及記憶體流控制器(MFC)310B。SPU核心310A實施程式執行、資料操控等等，而MFC 310B執行與SPU核心310A與系統之DRAM 314間的資料傳送相關之功能。

SPU核心310A包括局部記憶體350、指令單元(instruction unit；IU)352、暫存器354、一或多個浮點執行級356及一或多個定點執行級358。較佳的係可使用單埠式隨機存取記憶體(例如SRAM)實施局部記憶體350。而大部分處理器藉由

採用快取記憶體減小對記憶體之潛時，SPU核心310A實施較小局部記憶體350而非快取記憶體。事實上，為給即時應用程式(以及本文提及的其他應用程式)之程式設計師提供一致且可預測之記憶體存取潛時，SPU 308A內之快取記憶體架構並不理想。快取記憶體之快取記憶體衝擊/遺失特徵導致揮發性記憶體存取時間從數個週期變為數百個週期。此類揮發性削弱了(例如)即時應用程式之程式化中需要的存取時序可預測性。藉由重疊DMA傳送與資料計算，可在局部記憶體SRAM 350中實現潛時隱藏。此方法為即時應用程式之程式設計提供較高控制程度。由於與DMA傳送相關聯之潛時及指令負擔超過伺服快取記憶體遺失之潛時的負擔，SRAM局部記憶體方法在DMA傳送大小足夠大且充分可預測(例如可在需要資料前發出一DMA命令)時實現一優點。

運行於子處理器單元308之給定子處理單元上的程式使用一局部位址參考相關聯之局部記憶體350，不過，亦給局部記憶體350之各個位置指派總體系統記憶體映射內的一真實位址(real address；RA)。此使得權限軟體可將局部記憶體350映射至一程序之有效位址(Effective Address；EA)內，以促進一局部記憶體350與另一局部記憶體350間的DMA傳送。PU 304亦可使用有效位址直接存取局部記憶體350。在一較佳具體實施例中，局部記憶體350包含356千位元組之儲存量，而暫存器352之容量係128X128位元。

SPU核心304A較佳的係使用處理管線來實施，其中以管

線方式處理邏輯指令。儘管可將管線分割為處理指令的任何數目之級，管線通常包含擷取一或多個指令、解碼該等指令、檢查指令間之相依性、發出指令以及執行指令。在此方面，IU 352包括指令緩衝器、指令解碼電路、相依性檢查電路以及指令發出電路。

指令緩衝器較佳的係包括複數個暫存器，其與局部記憶體350耦合並可操作以在擷取指令時暫時儲存指令。指令緩衝器較佳的係操作以便全部指令作為一群組(即實質上同時)離開暫存器。儘管指令緩衝器可為任何大小，較佳係不大於二或三個暫存器之大小。

一般而言，解碼電路分解指令並產生邏輯微操作，其執行對應指令之功能。例如，邏輯微操作可指定算術及邏輯操作，向局部記憶體350載入並儲存操作，暫存來源運算元及/或中間資料運算元。解碼電路亦可指示指令使用哪些資源，例如目標暫存器位址、結構資源、功能單元及/或匯流排。解碼電路亦可供應指示需要資源之指令管線級的資訊。指令解碼電路較佳的係可操作以實質上同時地解碼數目等於指令緩衝器之暫存器數目的指令。

相依性檢查電路包括數位邏輯，其執行測試以決定給定指令之運算元是否取決於管線內其他指令之運算元。若是，則不應執行給定指令，直至更新此類其他運算元(例如藉由使其他指令可完成執行)。較佳的係相依性檢查電路決定同時從解碼器電路112遞送之多個指令的相依性。

指令發出電路可操作以向浮點執行級356及/或定點執行

級358發出指令。

較佳的係將暫存器354實施為較大統一暫存器檔案，例如128項暫存器檔案。此提供了高度管線式高頻率實施方案，而不需要重新命名，以避免暫存器供應不足。重新命名硬體通常消耗處理系統內的極大部分區域及功率。因此，當藉由軟體迴路展開或其他交錯技術覆蓋潛時時，可實現有利操作。

較佳的係SPU核心310A具有超純量架構，以便在每一時脈週期內發出多個指令。較佳的係SPU核心310A之操作的超純量程度對應於指令緩衝器之同時指令遞送數目，例如2與3之間(意味著每一時脈週期發出兩個或三個指令)。根據所需的處理功率，可採用數目更多或更少的浮點執行級356及定點執行級358。一較佳具體實施例中，浮點執行級356係以每秒鐘32億次浮點操作(32 GFLOPS)之速度進行操作，而定點執行級358係以每秒鐘32億次操作(32 GOPS)之速度進行操作。

MFC 310B較佳的係包括匯流排介面單元(bus interface unit；BIU)364、記憶體管理單元(memory management unit；MMU)362及直接記憶體存取控制器(direct memory access controller；DMAC)360。除DMAC 360外，MFC 310B較佳的係採用相較於SPU核心310A及匯流排312之一半頻率(一半速度)來運行，以滿足低功率消耗設計目標。MFC 310B可操作以處理從匯流排312進入SPU 308之資料及指令，並提供用於DMAC之位址轉譯，以及用於資料相關性之探索

操作。BIU 364提供匯流排312與MMU 362及DMAC 360間的介面。因此，SPU 308(包括SPU核心310A及MFC 310B)及DMAC 360以實體及/或邏輯方式與匯流排312連接。

MMU 362較佳的係可操作以將有效位址(從DMA命令取得)轉譯為用於記憶體存取之真實位址。例如，MMU 362可將更高階位元之有效位址轉譯為真實位址位元。不過，較低階位址位元較佳的係不可轉譯的，並且係視為邏輯與實體位址位元，以便用於形成真實位址並請求對記憶體之存取。在一或多項具體實施例中，可根據64位記憶體管理模型實施MMU 362，並且其可提供具有4K、64K、1M及16M位元組之頁面大小及256MB之片斷大小的264位元組之有效位址空間。較佳的係MMU 362可操作以支援最高265位元組之虛擬記憶體，以及用於DMA命令的242位元組(4兆兆位元組)之實體記憶體。MMU 362之硬體可包括8項完全關聯式SLB、256項4路組關聯式TLB以及用於TLB之4x4替換管理表(Replacement Management Table；RMT)-用於硬體TLB遺失處理。

DMAC 360較佳的係可操作以管理來自SPU核心310A以及一或多個其他器件(例如PU 304及/或其他SPU)之DMA命令。可存在三類DMA命令：存進命令，其操作以將資料從局部記憶體350移動至共享記憶體314；接收命令，其操作以將資料從共享記憶體314移動至局部記憶體350內；以及儲存控制命令，其包括SLI命令及同步命令。同步命令可包括原子式命令、傳送信號命令及專用阻障命令。 對DMA

命令作出回應，MMU 362將有效位址轉譯為真實位址，並將真實位址轉遞至BIU 364。

SPU核心310A較佳的係使用通道介面及資料介面，以便採用DMAC 360內之介面進行通信(傳送DMA命令、狀態等)。SPU核心310A透過通道介面遞送DMA命令至DMAC 360內的DMA佇列。一旦DMA命令處於DMA佇列內，則藉由DMAC 360內的發出及完成邏輯加以處理。當用於DMA命令之全部匯流排交易完成時，在通道介面上將完成信號傳送回至SPU核心310A。

圖9說明PU 304之較佳結構及功能。PU 304包括兩個基本功能單元，即SPU核心304A及記憶體流控制器(MFC)304B。PU核心304A實施程式執行、資料操控、多處理器管理功能等等，而MFC 304B執行關於PU核心304A與系統100之記憶體空間之間的資料傳送之功能。

PU核心304A可包括L1快取記憶體370、指令單元(IU)372、暫存器374、一或多個浮點執行級376及一或多個定點執行級378。L1快取記憶體為透過MFC 304B從共享記憶體106、處理器102或記憶體空間之其他部分接收的資料提供資料快取功能性。由於PU核心304A較佳的係實施為超級管線，較佳的係將指令單元372實施為具有許多級之指令管線，該等級包括擷取、解碼、相依性檢查、發出等等。同時較佳的係PU核心304A具有超純量組態，藉此在每一時脈週期內從指令單元372發出多個指令。為實現高處理功率，浮點執行級376及定點執行級378在管線組態內包括複

數個級。根據所需的處理功率，可採用數目更多或更少的浮點執行級376及定點執行級378。

MFC 304B包括匯流排單元(BIU)380、L2快取記憶體、非可快取單元(non-cachable unit；NCU)384、核心介面單元(core interface unit；CIU)386以及記憶體管理單元(MMU)388。大部分MFC 304B採用相較於PU核心304A及匯流排108之一半頻率(一半速度)來運行，以滿足低功率消耗設計目標。

BIU 380提供匯流排108及L2快取記憶體382與NCU 384邏輯區塊間的介面。為此目的，BIU 380可當作匯流排108上之主器件以及從屬器件，以便執行完全連貫之記憶體操作。作為主器件，其可從來源載入/儲存請求至匯流排108，以用於代表L2快取記憶體382及NCU 384之服務。BIU 380亦可針對命令實施流量控制機制，其限制可傳送至匯流排108之命令的總數目。匯流排108上之資料操作可被設計成採用八拍，因此BIU 380較佳的係設計為大約128位元組之快取記憶體線路，且相關性及同步粒度為128KB。

L2快取記憶體382(以及支援硬體邏輯)較佳的係設計成快取312KB之資料。例如，L2快取記憶體382可處理可快取載入/儲存、資料預擷取、指令擷取、指令預擷取、快取記憶體操作及阻障操作。L2快取記憶體382較佳的係8路組關聯式系統。L2快取記憶體382可包括匹配六個(6)逐出佇列之六個重新載入佇列(例如六個RC機器)以及八個(寬64個位元組)儲存佇列。L2快取記憶體382可操作以提供L1快取

記憶體370內之某些或全部資料的備份副本。其優點在於，當對處理節點進行熱交換時，此在重新儲存狀態內較為有用。此組態亦使L1快取記憶體370可採用更少埠更快地加以操作，並可提供更快的快取記憶體對快取記憶體傳送(因為請求可停止於L2快取記憶體382)。此組態也提供用於將快取記憶體相關性管理傳遞至L2快取記憶體382的機制。

NCU 384介接CIU 386、L2快取記憶體382以及BIU 380，並且一般係執行佇列/緩衝電路之功能，其用於PU核心304A與記憶體系統間之非可快取操作。NCU 384較佳的係處理L2快取記憶體382不予處理的與PU核心304A之全部通信，例如禁止快取記憶體之載入/儲存、阻障操作及快取記憶體相關性操作。NCU 384較佳的係採用一半速度來運行，以滿足上述功率消耗目標。

將CIU 386置放於MFC 304B及PU核心304A之邊界，並用作選路、仲裁及流量控制點，其用於來自執行級376、378、指令單元372及MMU單元388並到達L2快取記憶體382及NCU 384之請求。PU核心304A及MMU 388較佳的係全速運行，而L2快取記憶體382及NCU 384可採用2：1速度比率操作。因此，頻率邊界存在於CIU 386內，其功能之一係當其在兩個頻域間轉遞請求及重新載入資料時，準確處理頻率交越。

CIU 386由三個功能區塊組成：載入單元、儲存單元及重新載入單元。此外，資料預擷取功能係由CIU 386來執行，且較佳的係載入單元之功能部分，其可操作以：(i)接受來

自PU核心304A及MMU 388之載入及儲存請求；(ii)將該等請求從全速時脈頻率轉換為半速(2：1時脈頻率轉換)；(iii)將可快取請求選路至L2快取記憶體382，以及將非可快取請求選路至NCU 384；(iv)在到達L2快取記憶體382及NCU 384之請求間公平地仲裁；(v)在對L2快取記憶體382及NCU 384之遞送中提供流量控制，以便在目標窗口中接收請求並避免溢流；(vi)接受載入返回資料並將其選路至執行級376、378、指令單元372或MMU 388；(vii)將探索請求傳遞至執行級376、378、指令單元372或MMU 388；以及(viii)將載入返回資料及探索流量從半速轉換為全速。

MMU 388較佳的係提供用於PU核心304A之位址轉譯，例如藉由第二位準位址轉譯設施。第一位準之轉譯較佳的係藉由可遠小於且快於MMU 388的分離指令及資料ERAT(對真實位址轉譯有效)陣列而提供在PU核心304A中。

一較佳具體實施例中，PU 304採用64位元實施方案在46 GHz、10F04下操作。暫存器較佳的係長64位元(儘管一或多個特殊用途暫存器可更小)，有效位址長64位元。指令單元370、暫存器372及執行級374及376較佳的係使用PowerPC技術來實施，以實現(RISC)計算技術。

美國專利第6,526,491號中可找到關於此電腦系統之模組結構的詳細資料，其整個揭示內容以提及方式併入本文中。

現在參考圖10，其係根據本發明之一或多個其他方面之處理器500的方塊圖。此具體實施例中，處理器500也包括解密單元502及安全記憶體504。安全記憶體504包含不可見

密鑰(IKi)，此處i代表第i個處理器。解密單元502可操作以解密從記憶體流控制器310B流動至局部記憶體350的資料(使用不可見密鑰IKi)。較佳的係不可見密鑰IKi對給定處理器500實質上係唯一密鑰，應瞭解系統內的各處理器包括唯一不可見密鑰。解密單元502可採用任何已知技術，例如簡單XOR演算法或更複雜的演算法。

處理器500較佳的係可操作以進入安全操作模式，其使用上述技術或利用其他技術。較佳的係處理器500在硬體重設狀況或啟動狀況後進入安全操作模式。當處於不安全模式時，PU 304能夠啟動共享DRAM 314與局部記憶體350間之資料傳送，而不用穿過解密單元502。同樣，當處理器500處於不安全模式時，PU 304能夠啟動從局部記憶體350至共享DRAM 314之資料傳送。然而，當處於安全模式時，PU 304不能夠啟動從共享DRAM 314至局部記憶體350之資料傳送，而不用使此類資料穿過解密單元502。PU 304啟動的發自局部記憶體350之資料傳送在安全模式中不允許。因此，PU 304(或任何其他外部實體)所啟動的任何資料傳送將導致資料經受解密，其使用不可見密鑰IKi。然而，處理器500能夠啟動局部記憶體350與共享DRAM 314間的資料傳送，而不論其是否處於安全操作模式。

儲存於安全儲存記憶體504內之不可見密鑰IKi僅可由處理器500之解密單元502或某一其他經過授權之實體存取。最佳的係即使一實體經過授權以得知特定處理器500之不可見密鑰IKi，此類實體必須以某種方式得到對不可見密鑰

IKi之存取權，除了從處理器500之安全記憶體504獲得外。例如，在處理器500之製造程序期間，不可見密鑰IKi較佳的係儲存於安全記憶體504中，恰在或大約在該相同時間，使經過授權之該等實體得知不可見密鑰IKi，以獲得資訊。

處理器500較佳的係還包括實質上唯一之ID，例如序號或其他識別標記。然而，與不可見密鑰IKi不同，較佳的係想要利用處理器500之安全特徵的任何實體皆知道處理器500之ID。因此，ID可視為可見密鑰VKi，此處i代表第i個處理器500。

參考圖11，說明可採用處理器500之安全特徵的一系統。該系統包括處理器500、中間實體510及安全實體(或伺服器)512。安全實體512包括認證伺服器514及資料庫516，以下將予以更詳細說明。應注意雖然圖11顯示本發明某些方面的結構，也顯示了資料/程序流。因此，本文中圖11用於說明本發明之裝置及方法的細節。

中間實體510可為任何實體或系統，其需要以安全方式向處理器500發送資料或發送並執行程式。請記得，處理器500可為共享DRAM 314之複數個附著處理單元中的一個。因此，可能將從中間實體510發送至處理器500的資料至少暫時儲存於共享DRAM 314中。某些情況下，此可使資料遭受其他處理器之盜錄。但是根據本發明，中間實體510可用此一方式將資料發送至處理器500：僅處理器500可取得對資料之存取權及使用權。

特定言之，中間實體510獲得與處理器500相關聯之可見

密鑰VKi。中間實體510向安全伺服器512發送資料(例如需要在處理器500上執行的遠端程式)以及可見密鑰VKi。此傳輸可使用任何已知技術而發生，例如藉由網際網路或任何其他網路、通信鏈路或藉由手動干預。安全伺服器512從傳輸獲得可見密鑰VKi並採用認證伺服器514以搜尋資料庫516，其包含複數個可見密鑰－不可見密鑰對。可見及不可見密鑰對藉由其與特定處理器之相互關係彼此相關聯，例如處理器500。若獲得從中間實體510接收之可見密鑰VKi與資料庫516內之已儲存可見密鑰之一間的匹配，則認證伺服器514較佳的係使用與可見密鑰VKi及處理器500相關聯之不可見密鑰IKi加密資料(此範例中為遠端程式)。安全伺服器512接著將已加密資料發送至中間實體510，例如採用網際網路。

儘管中間實體510獲得提供給安全伺服器512之資料的已加密版本，中間實體510並不具有關於處理器500之不可見密鑰IKi的任何資訊。在此方面，安全伺服器512係經過授權之實體，因為其具有處理器500之安全記憶體504內包含的不可見密鑰IKi之知識。雖然任何實體，例如中間實體510，可具有任何給定處理之可見密鑰VKi的知識，僅經過授權之實體，例如安全伺服器512，具有不可見密鑰IKi及/或其與特定可見密鑰VKi的關聯性之知識。

中間實體510接著可向處理器500發送已加密資料，例如藉由網際網路，或任何其他適當機制。根據處理器500之操作能力，PU 304促進從中間實體510的已加密資料之接收以

及該等資料在共享DRAM 314內之儲存。較佳的係處理器500恰在或大約在PU 304使已加密資料儲存於共享DRAM 314時處於安全操作模式中。因此，當PU 304啟動已加密資料從共享DRAM 314至處理器500之局部記憶體350的傳送時，此類已加密資料必須穿過解密單元502。因此，解密單元502利用儲存於處理器500之安全記憶體504內的不可見密鑰IKi解密已加密資料。其優點在於，以安全方式將中間實體510所發出之已解密資料儲存於處理器500之局部記憶體350內。事實上，安全模式中，PU 304及任何其他外部實體皆無法從局部記憶體350獲得資料，且處理器500可操控此類資料而不經受盜錄。

現在參考圖12，其係圖11之系統的方塊圖，該系統採用替代方法以利用處理器500之安全特徵。如同上文參考圖11所說明之方法，中間實體510獲得與處理器500相關聯之可見密鑰VKi。但與該方法不同，中間實體510使用對稱密鑰1加密至少該等資料(例如遠端程式)。例如，中間實體510所使用之加密技術可為眾所周知的高級加密標準(Advanced Encryption Standard；AES)，其致動一或多個對稱密鑰之使用，以加密及解密敏感資料。應注意中間實體510可利用對稱密鑰1加密資料及可見密鑰VKi兩者。任何情形中，中間實體510較佳的係將已加密資料(以及可見密鑰VKi)發送至安全實體512。認證伺服器514較佳的係可操作以接收已加密資料及可見密鑰VKi，以及利用對稱密鑰2將其解密。

一旦認證伺服器514已獲得已解密資料及可見密鑰VKi，

其搜尋資料庫514以找到可見密鑰－不可見密鑰對。若獲得從中間實體510接收之可見密鑰VKi與資料庫516內之已儲存可見密鑰之一間的匹配，則認證伺服器514較佳的係使用與可見密鑰VKi及處理器500相關聯之不可見密鑰IKi加密資料。認證伺服器514亦利用對稱密鑰2加密該等已加密資料，以獲得加密已加密資料。安全實體512接著將加密已加密資料發送至中間實體510。

中間實體510較佳的係接收加密已加密資料並使用對稱密鑰1將其解密，以獲得藉由不可見密鑰IKi加密之資料。中間實體510接著可向處理器500發送已加密資料，例如藉由網際網路，或任何其他適當機制。PU 304促進已加密資料從中間實體510之接收以及其在共享DRAM 314中之儲存。較佳的係處理器500恰在或大約在PU 304使已加密資料儲存於共享DRAM 314時處於安全操作模式中。當PU 304啟動已加密資料從共享DRAM 314至處理器500之局部記憶體350的傳送時，此類已加密資料必須穿過解密單元502。因此，解密單元502利用儲存於處理器500之安全記憶體504內的不可見密鑰IKi解密已加密資料。其優點在於，以安全方式將中間實體510所發出之已解密資料儲存於處理器500之局部記憶體350內。安全模式中，PU 304及任何其他外部實體皆無法不經處理器500認證而從局部記憶體350獲得資料。因此，處理器500可操控此類資料而不經受盜錄。

現在參考圖13至14，其係圖11之系統的方塊圖，該系統採用另一替代方法以利用處理器500之安全特徵。根據本發

明之此具體實施例，資料包括解密程式及對稱密鑰(例如根據RSA協定)。中間實體510利用對稱密鑰1(其較佳的係僅中間實體510及任何可信實體知道的秘密密鑰)加密解密程式及對稱密鑰2。應注意，中間實體510亦可與解密程式及對稱密鑰2一起加密處理器500之可見密鑰VKi。任何情形中，中間實體510將已加密解密程式/對稱密鑰2及可見密鑰VKi發送至安全伺服器512。認證伺服器514較佳的係可操作以利用對稱密鑰2解密已加密資料，以獲得解密程式及可見密鑰VKi(假定其亦與解密程式一起得以加密)。密鑰2較佳的係公用密鑰，因為其他實體亦可知道密鑰2之細節。(還應注意認證伺服器514所使用的公用密鑰2可不同於與解密程式一起得以加密之公用密鑰2。)認證伺服器514接著搜尋資料庫516以獲得匹配已接收之可見密鑰VKi的可見密鑰－不可見密鑰對。若獲得匹配，認證伺服器514較佳的係使用與可見密鑰VKi及處理器500相關聯之不可見密鑰IKi加密解密程式及對稱密鑰2。認證伺服器514同樣較佳的係利用對稱密鑰2(例如利用RSA加密技術)加密已加密資料。安全伺服器512接著向中間實體510發送加密已加密資料(例如解密程式及對稱密鑰2)，例如利用網際網路。

中間實體510較佳的係利用對稱(秘密)密鑰1解密加密已加密資料，以獲得已加密資料。此時，中間實體510具有解密程式及對稱(公用)密鑰2，其已藉由不可見密鑰IKi加以加密。中間實體510接著可向處理器500發送已加密資料(解密程式及對稱密鑰2)，例如藉由網際網路。如同先前具體實

施例，PU 304促進已加密資料從中間實體510之接收、其在共享DRAM 314中之儲存以及已加密資料透過解密單元502之傳送，以便以安全方式將解密程式及對稱密鑰2儲存於處理器500之局部記憶體350內。

此時，將處理器放置於"安全模式"內，例如上述第三模式。更特定言之，第三模式中，處理器500可啟動資訊進入或離開處理器500之傳送，但任何外部器件(例如PU 304)則不能。

雖然此有利地使處理器500可以安全方式操控解密程式及對稱密鑰2，其也以簡化方式提供稍後之安全資料傳送，以下將參考圖14予以詳細說明。

中間實體510較佳的係利用對稱(公用)密鑰1加密其他資料，並將其發送至處理器500，例如利用網際網路或任何其他適當機制。應注意中間實體510用以加密其他資料之私有密鑰1不必與用於加密需要傳輸至安全伺服器512的解密程式之私有密鑰1相同。PU 304促進已加密資料從中間實體510之接收以及其在共享DRAM 314中之儲存。應注意在本發明之此具體實施例中，處理器500不必處於操作之"隔離模式"。回顧以上說明，在隔離模式(第二模式)中，處理器500及任何器件皆無法啟動資訊進入或離開處理器500之傳送。事實上，處理器500或PU 304可啟動已加密資料從共享DRAM 314至局部記憶體350之傳送，而繞過解密單元502。此係由於其他資料係利用對稱(私有)密鑰1來加以加密，且PU 304及任何其他外部實體皆不具有安全地儲存於局部記

憶體350的解密程式或對稱(公用)密鑰2之知識或存取權。處理器500接著可利用解密程式及對稱密鑰2解密其他已加密資料。其優點在於，處理器500以安全方式接收其他資料並可以相同方式接收其他資料，而無需借助於安全操作模式。

現在參考圖15，其係顯示兩個處理器500A及500B之方塊圖，其可操作以在網際網路或任何其他適當通信通道或機制上彼此通信。根據本發明之此具體實施例，每一處理器500A、500B接收一加密/解密程式及一對稱密鑰，較佳的係利用參考圖13的上述方法。更特定言之，處理器500A較佳的係接收加密/解密程式及對稱密鑰2，而處理器500B接收加密/解密程式及對稱密鑰1。較佳的係加密/解密程式及對稱密鑰附加於AES加密方法。

現在詳細說明處理器500A與處理器500B間的安全資料傳送(亦稱為點對點通信)。特定言之，處理器500B可利用局部記憶體350B內之加密/解密程式及對稱密鑰1加密其他資料。處理器500B接著可將其他已加密資料從局部記憶體350B傳送至共享DRAM 314B。PU 304B接著可藉由網際網路將其他已加密資料從共享DRAM 314B傳送至與處理器500A相關聯之PU 304A。PU 304A接著可傳送與處理器500A相關聯之共享DRAM 314A內的其他已加密資料。處理器500A或PU 304A接著可將已加密其他資料從共享DRAM 314A傳送至局部記憶體350A，而繞過解密單元502A。一旦處於局部記憶體350A內，可利用加密/解密程式及對稱密鑰2解密其他已加密資料。其優點在於，可在處理器500B與處

理器500A間傳送其他資料，而無需與中間實體510(圖13)進一步通信。

亦可利用與上述技術實質上相同之技術將其他資料從處理器500A傳送至處理器500B。事實上，處理器500A可利用加密/解密程式及對稱密鑰2加密其他資料，並將其傳送至共享DRAM 314A。PU 304A可經由網際網路將此類其他已加密資料從共享DRAM 314A傳送至與處理器500B相關聯之PU 304B。PU 304B可將其他已加密資料傳送至與處理器500B相關聯之共享DRAM 314B。處理器500B或PU 304B接著可將其他已加密資料從共享DRAM 314B傳送至局部記憶體350B，此處利用加密/解密程式及對稱密鑰1將其加密。另外，其他資料從處理器500A至處理器500B之安全傳送可不用進一步採用中間實體510或安全伺服器512(圖13)而完成。

現在參考圖16及17，其係與圖11及/或圖12之系統實質上相同的系統之方塊圖，其中採用另一替代方法以利用若干處理器500之安全特徵。根據本發明之此具體實施例，中間實體510(其可為分佈伺服器)向安全伺服器512傳送解密(或解碼)程式及對稱密鑰2，較佳的係在上述安全路徑上。中間實體510另外較佳的係發送與各處理器相關聯之個別可見密鑰VKi，其將以安全方式參與其他資料之傳輸。安全伺服器512向中間實體510發送解碼程式及對稱密鑰2之已加密版本，此處採用與接收之可見密鑰VKi之個別密鑰相關聯的特定不可見密鑰IKi加密各版本。中間實體510接著向個

別處理器500A、500B、……500i發送已加密解碼程式及對稱密鑰2之個別版本。各處理器較佳的係處於安全操作模式，以便已加密解碼程式及對稱密鑰2之個別版本必須穿過個別解密單元502A、502B、……502i。因此，各處理器500A、500B、……500i獲得其相關聯局部記憶體350A、350B、……350i內之解碼程式及對稱密鑰2。

之後，中間實體510可向處理器500之每個發送其他資料之一版本，例如分佈程式，其已藉由對稱密鑰1加密(圖17)。處理器500之每個接著可利用位於其個別局部記憶體350內的解碼程式及對稱密鑰2解密其他已加密資料。其優點在於，可以安全方式發送其他資料，而不需要用於各參與處理器500之不同版本。在此方面，解碼程式可視為使用者"車票"，其使特定處理器500可接收其他資料，例如電影、音樂、遊戲程式等等。由於該車票僅對特定處理器500(或使用者)有效，僅該使用者可接收及解密已加密分佈程式。然而，分佈伺服器510僅需要準備一版本之分佈程式，其儘管已被加密，仍可藉由經過授權之處理器來解密。

從上文應明白，本發明之各種具體實施例可獨立或組合地加以使用，以完成各種安全操作，例如可信碼之處理及分佈。事實上，可驗證可信碼之來源，並決定可信碼是否已被篡改。此外，本發明可用於鑑別資料內容，安全地分配資料內容，管理系統權限，處理電子商務付款、管理點對點並管理用戶端對伺服器鑑別。另外，本發明可用於藉由在啟動前鑑別及驗證操作系統未被篡改而實現給定處理

器之安全啟動程序。本發明之用途並非完整地加以列舉；事實上，熟悉本技藝者應明白本發明之用途數量眾多，難以一一列舉。

現在參考圖18，其說明如何依據本發明之各個方面採用處理器協作之另一範例。更特定言之，圖18顯示在資料匯流排、網路及/或任何其他通信鏈路上彼此通信之複數個處理器600A、600B、……、600F的方塊圖。至少處理器600之一係"隔離的"，因為其局部記憶體內之資料不經同意無法獲得。換言之，一或多個處理器600處於上述安全操作模式。在圖18所說明之範例中，處理器600A、600B、600D及600E處於安全操作模式，而處理器600C及600F處於不安全操作模式。除非另外准許，安全及不安全處理器皆可從安全處理器之局部記憶體接收資料。因此，不安全處理器600C無法從處理器600B之局部記憶體單方面獲得資料。同樣，安全處理器600E無法從安全處理器600B之局部記憶體單方面獲得資料。因此，任何處理器600可從不安全處理器之局部記憶體單方面獲得資料。然而，當獲得准許時，例如藉由手動協作，伺服器處理器(例如處理器600A)可使另一處理器(例如處理器600B)可從其局部記憶體單方面獲得資料。

例如，以上系統可用於資料安全非常重要的多方商業投機管理。例如，處理器600A及600B可為管理實體，其包含專有內容及/或在投機中向其他方提供鑑別功能。因此，處理器600D及600E可鑑別內容，例如驗證及/或加密內容，以

便稍後使用處理器600A及/或處理器600B進行分配或處理。在此方面，處理器600D及600E可視為領執照者之管理實體。另外，第三方內容可在不安全處理器600C及600F上獲得及/或處理。

雖然已參考特定具體實施例來說明本發明，但應明白，這些具體實施例僅係用以說明本發明的原理及應用。因此應瞭解，可以對說明性的具體實施例進行各種修改，並且可在不脫離隨附申請專利範圍所定義之本發明的精神及範疇下設計出其它配置。

產業上的利用可能性

本發明可應用於針對使用多處理器架構之安全資料處理的技術。

【圖式簡單說明】

為達到解釋的目的，圖式中所顯示的係本發明目前之一較佳形式，然而，應瞭解，本發明並不限於所示刻板配置與機制。

圖1說明根據本發明之一或多方面的示範性電腦網路之總體架構；

圖2係說明根據本發明之一或多方面的多處理器系統之方塊圖；

圖3係說明根據本發明之一或多方面的圖2之系統的安全電路之結構的方塊圖；

圖4係流程圖，其說明可由圖2之系統執行以實現根據本發明之一或多方面的鑑別例行程式之程序步驟的一部分；

圖5係流程圖，其說明可由圖2之系統執行以實現根據本發明之一或多方面的鑑別例行程式之程序步驟的一部分；

圖6係流程圖，其說明可由圖2之系統執行以實現根據本發明之一或多方面的鑑別例行程式之程序步驟的一部分；

圖7係說明可用於實施本發明之一或多個其他方面的較佳處理器元件(PE)之方塊圖；

圖8係方塊圖，其說明可根據本發明之一或多個其他方面加以調適的圖7之系統的示範性子處理單元(SPU)之結構；

圖9係方塊圖，其說明可根據本發明之一或多個其他方面加以調適的圖7之系統的示範性處理單元(PU)之結構；

圖10係具有根據本發明之一或多方面的安全特徵之處理器的方塊圖；

圖11係使用圖10之處理器以利用本發明之特定安全特徵的系統之方塊圖；

圖12係使用圖10之處理器以利用根據本發明之其他安全特徵的系統之方塊圖；

圖13係使用圖10之處理器以利用根據本發明之其他安全特徵的系統之方塊圖；

圖14說明圖13之系統的進一步細節；

圖15係使用圖10之處理器以利用根據本發明之其他安全特徵的系統之方塊圖；

圖16係使用圖10之處理器以利用根據本發明之其他安全特徵的系統之方塊圖；

圖17說明圖16之系統的進一步細節；以及

圖18係利用根據本發明之一或多個其他方面的複數個處理器之系統的方塊圖。

【主要元件符號說明】

1	電腦系統
2	軟體單元
4	網路
6	用戶端電腦
8	伺服器電腦
10	個人數位助理
12	數位電視
100	處理系統
102A	處理器
102B	處理器
102C	處理器
102D	處理器
104A	局部記憶體
104B	局部記憶體
104C	局部記憶體
104D	局部記憶體
106	共享記憶體
108	匯流排系統
109	局部記憶體
150	安全電路
152	秘密資料區域

154	可存取資料區域
156	邏輯電路
300	處理器元件
302	輸入/輸出介面
304	處理單元
304A	SPU核心
304B	記憶體流控制器
308	子處理單元
308A	子處理單元
308B	子處理單元
308C	子處理單元
308D	子處理單元
310A	SPU核心
310B	記憶體流控制器
311	記憶體介面
312	PE匯流排
314	記憶體
314A	共享DRAM
315	高頻寬記憶體連接
350	局部記憶體
350A	局部記憶體
350B	局部記憶體
352	指令單元
354	暫存器

356	浮點執行級
358	定點執行級
359	暫存器
360	直接記憶體存取控制器
362	記憶體管理單元
364	匯流排介面單元
370	L1快取記憶體
372	指令單元
374	暫存器
376	浮點執行級
378	定點執行級
380	匯流排單元
382	L2快取記憶體
384	非可快取單元
386	核心介面單元
388	記憶體管理單元
500	處理器
500A	處理器
500B	處理器
502	解密單元
502A	解密單元
502B	解密單元
504	安全記憶體
510	中間實體

512	安全實體
514	認證伺服器
516	資料庫
600	處理器
600A	處理器
600B	處理器
600C	處理器
600D	處理器
600E	處理器
600F	處理器

五、中文發明摘要：

本發明揭示一種用於將一處理單元放置於複數個操作模式之一或多個操作模式內的方法及裝置，其中該裝置包括一局部記憶體、可操作以向及從該局部記憶體載送資訊之一匯流排、可操作以處理資料並且可操作性耦合至該局部記憶體之一或多個算術處理單元以及可操作以將該裝置放置於該等操作模式內之一安全電路；以及該複數個操作模式包括一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送。

六、英文發明摘要：

十一、圖式：

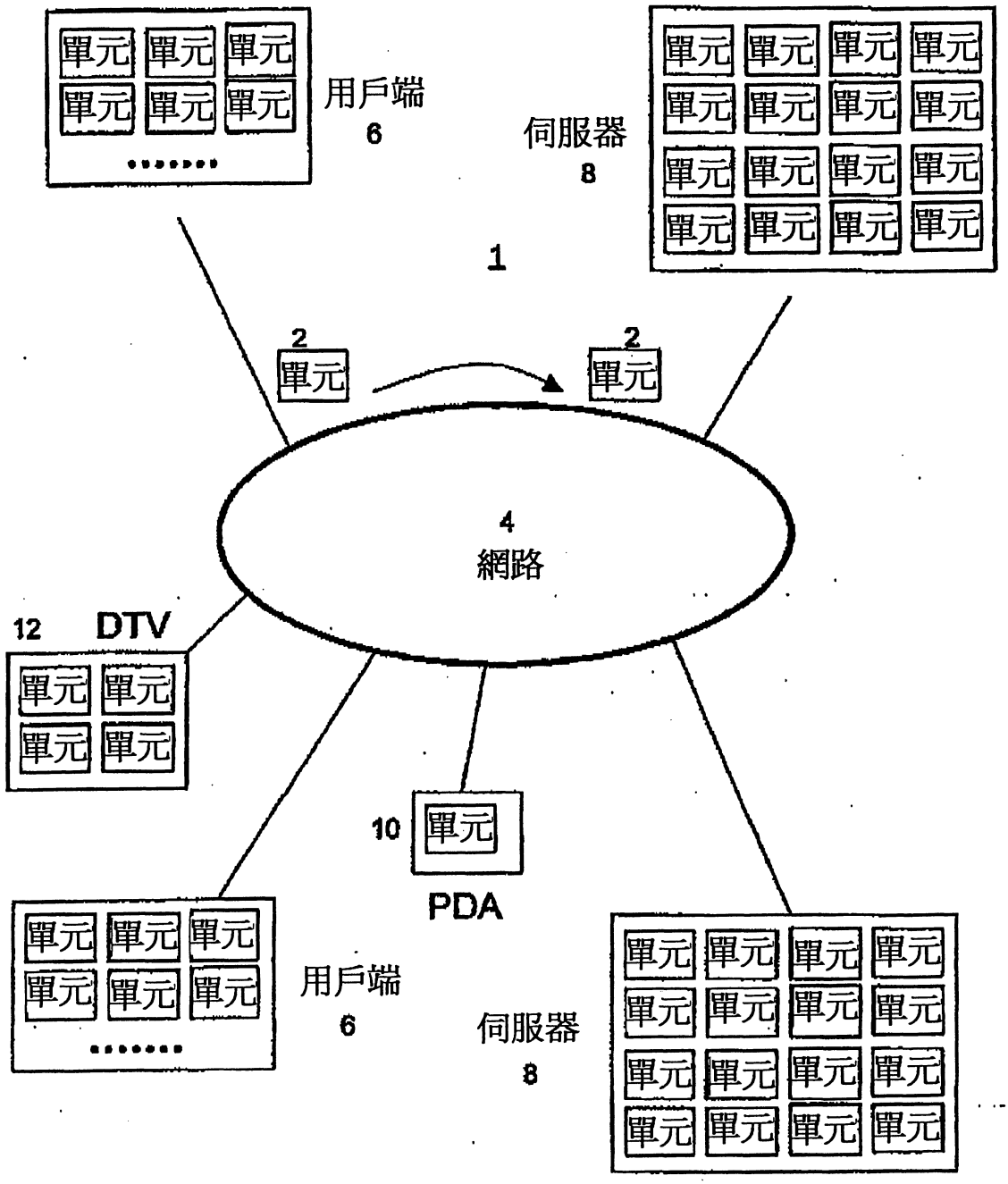

圖 1

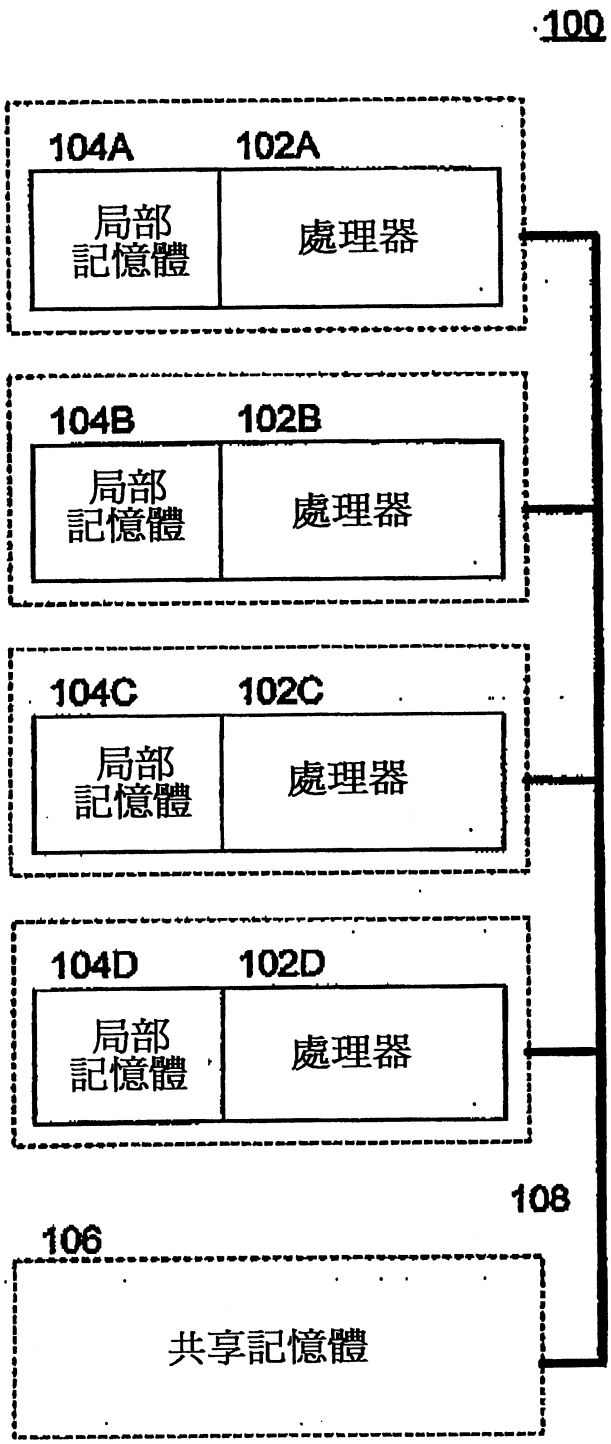
100
104A
102A
局部記憶體
處理器
104B
102B
局部記憶體
處理器
104C
102C
局部記憶體
處理器
104D
102D
局部記憶體
處理器
108
106
共享記憶體

圖 2

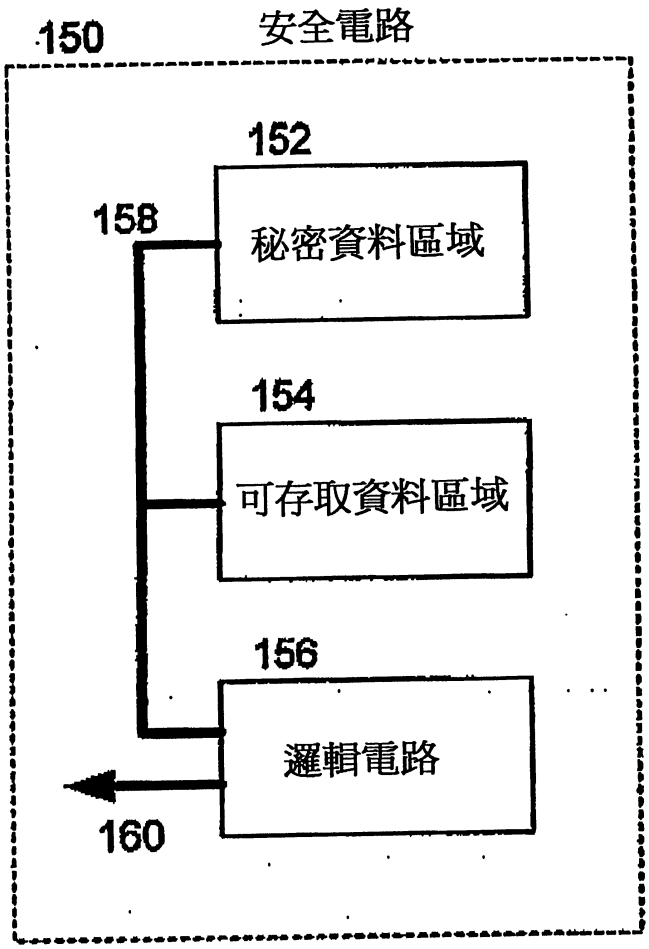

圖 3

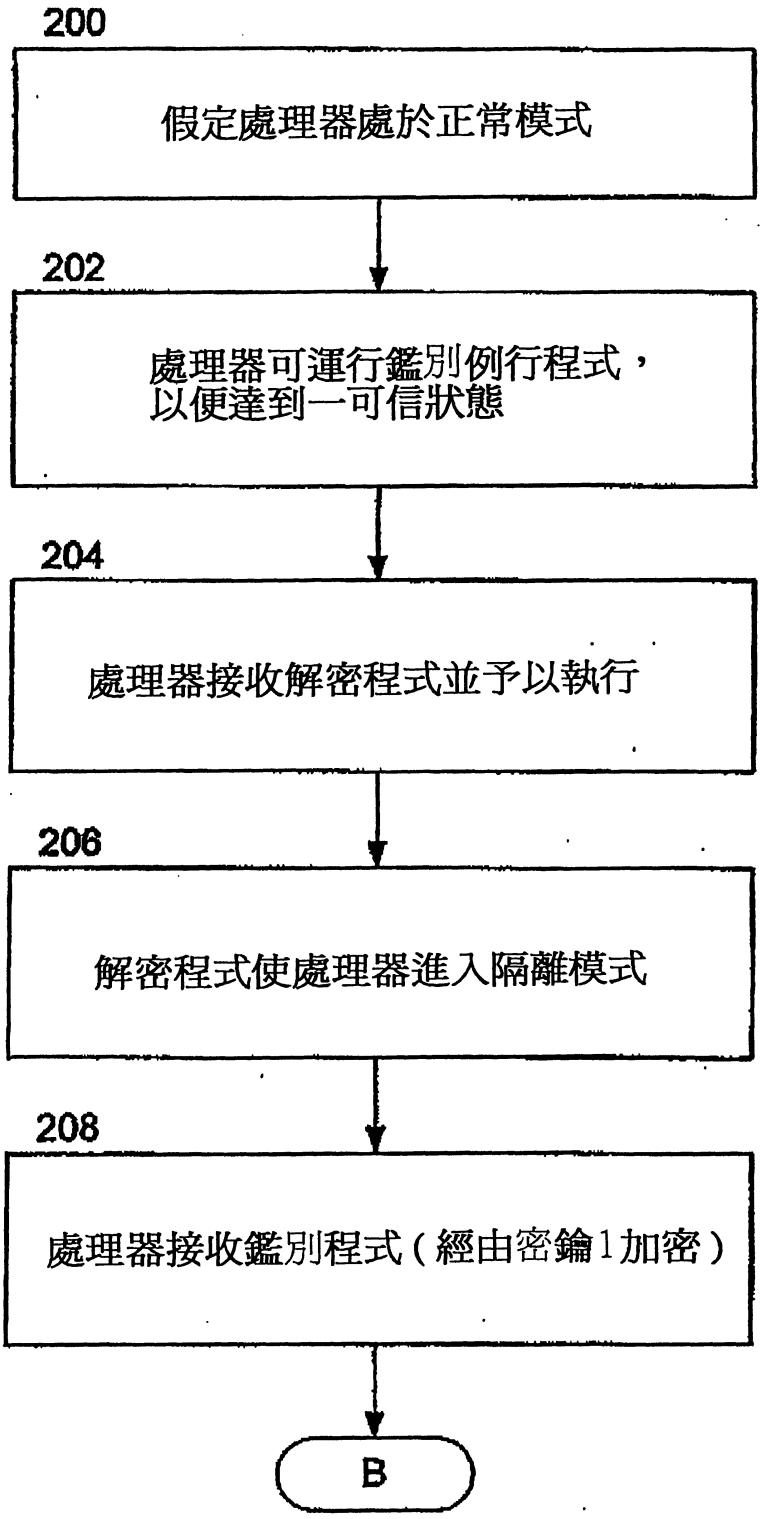
200
假定處理器處於正常模式
202
處理器可運行鑑別例行程式，
以便達到一可信狀態
204
處理器接收解密程式並予以執行
206
解密程式使處理器進入隔離模式
208
處理器接收鑑別程式（經由密鑰1加密）
B

圖 4

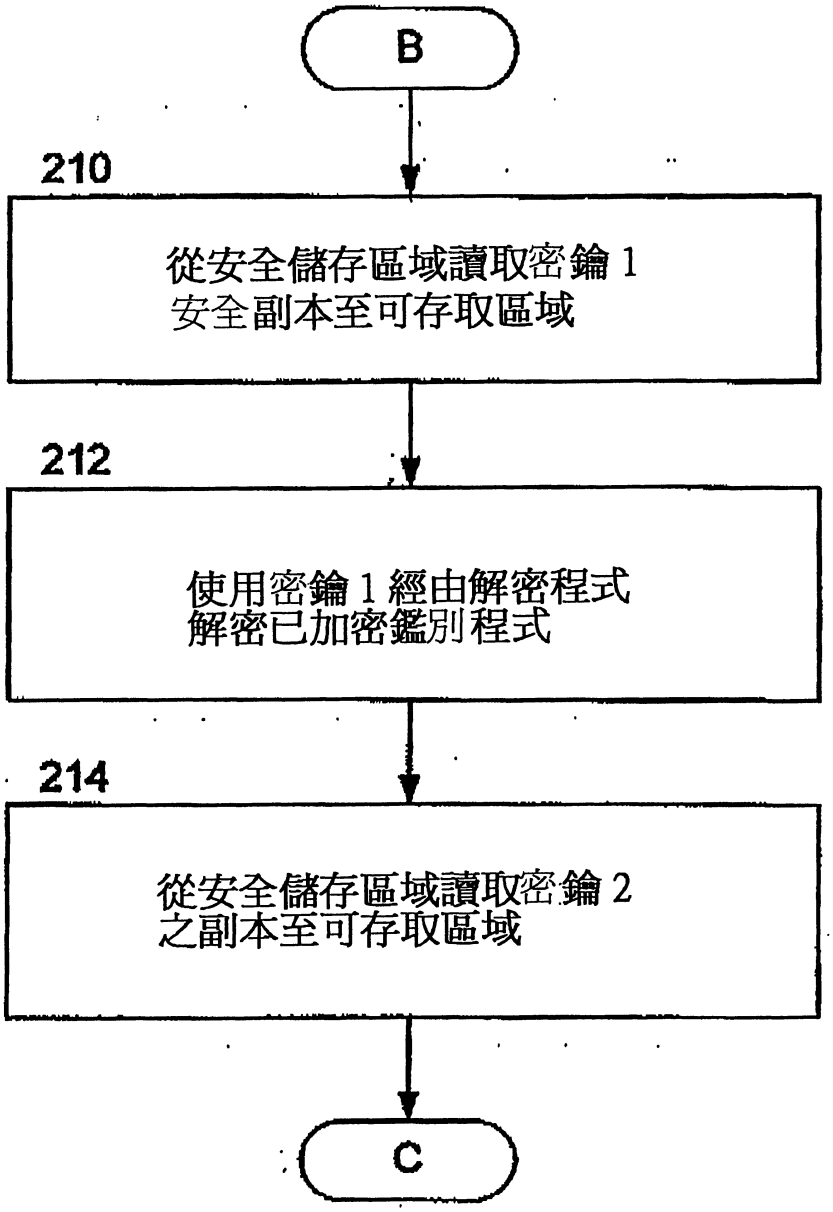
B
210
從安全儲存區域讀取密鑰 1
安全副本至可存取區域
212
使用密鑰 1 經由解密程式
解密已加密鑑別程式
214
從安全儲存區域讀取密鑰 2
之副本至可存取區域
C

圖 5

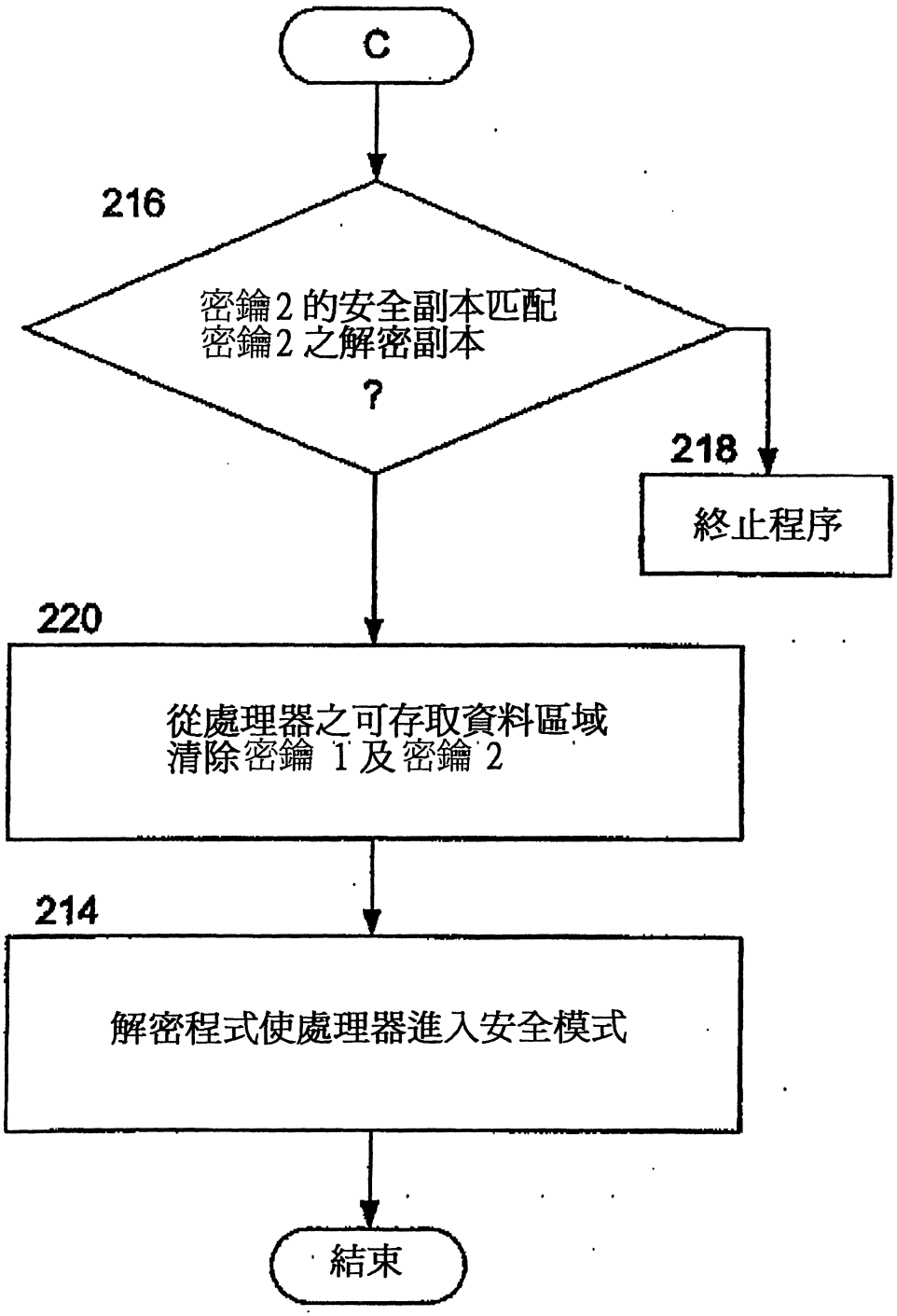
C
216
密鑰 2 的安全副本匹配
密鑰 2 之解密副本
?
218
終止程序
220
從處理器之可存取資料區域
清除密鑰 1 及密鑰 2
214
解密程式使處理器進入安全模式
結束

圖 6

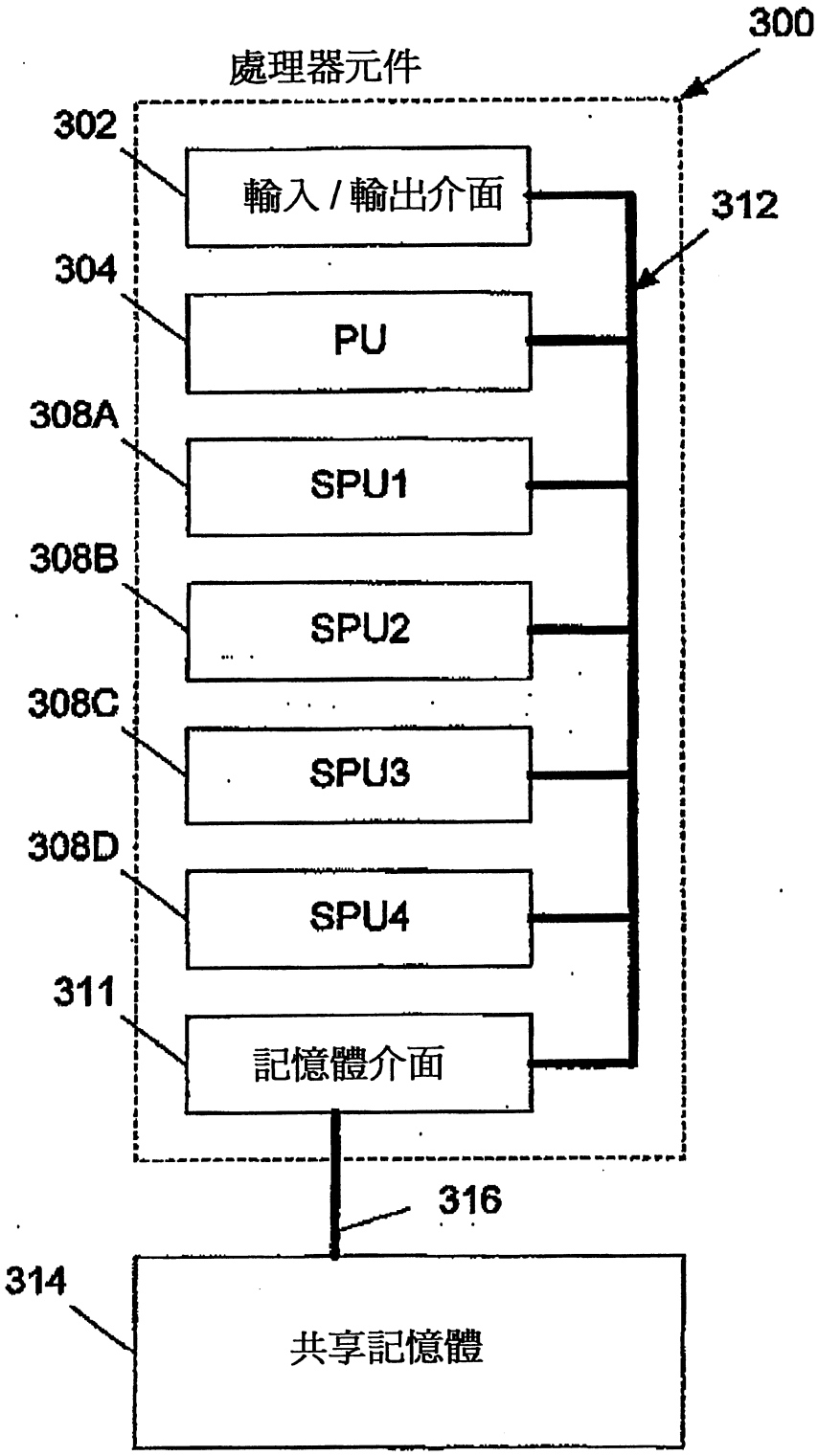
300
處理器元件
302
輸入 / 輸出介面
312
304
PU
308A
SPU1
308B
SPU2
308C
SPU3
308D
SPU4
311
記憶體介面
316
314
共享記憶體

圖 7

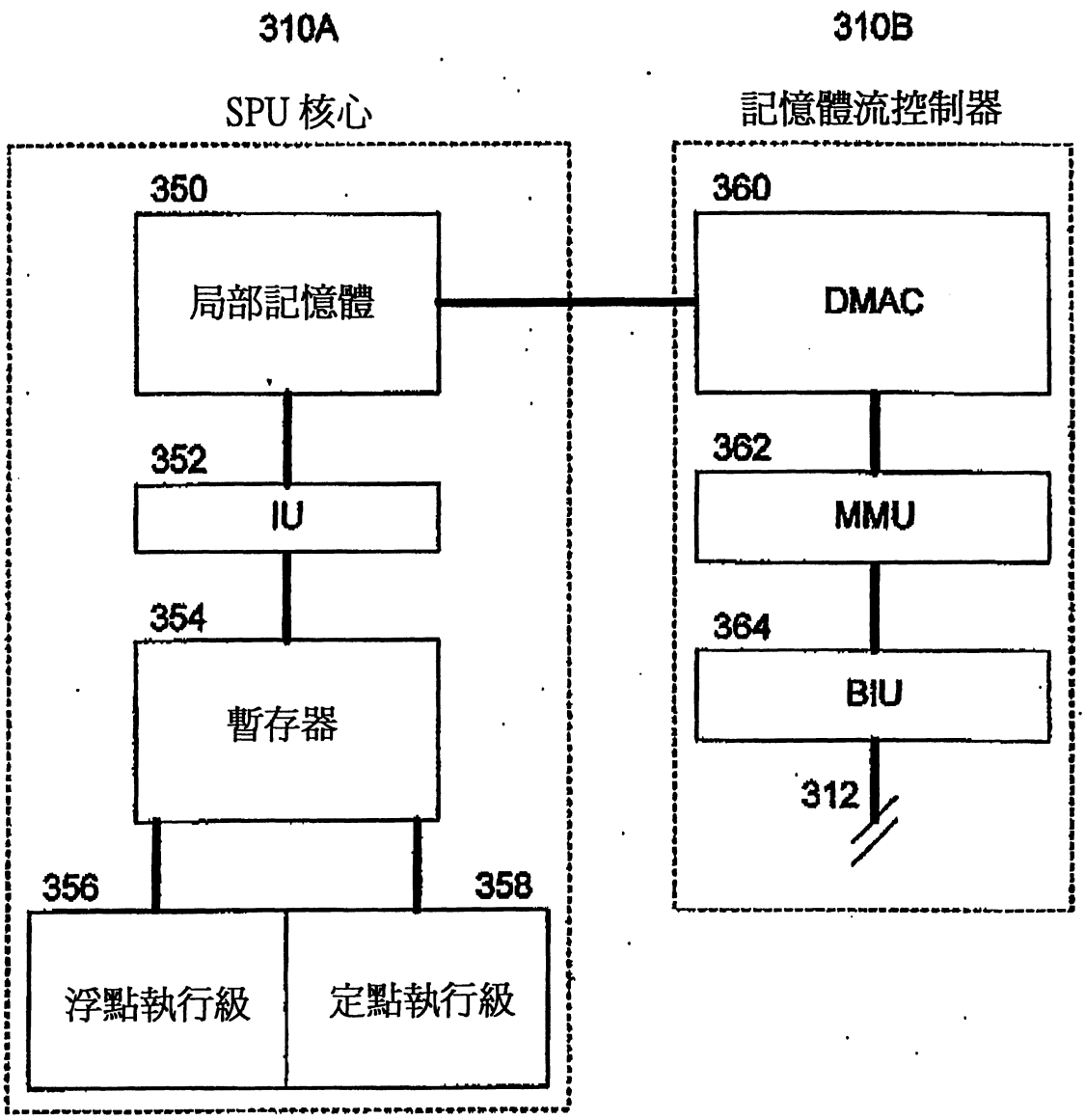
310A
310B
SPU 核心
記憶體流控制器
350
局部記憶體
360
DMAC
352
IU
362
MMU
354
暫存器
364
BIU
312
356
358
浮點執行級
定點執行級

圖 8

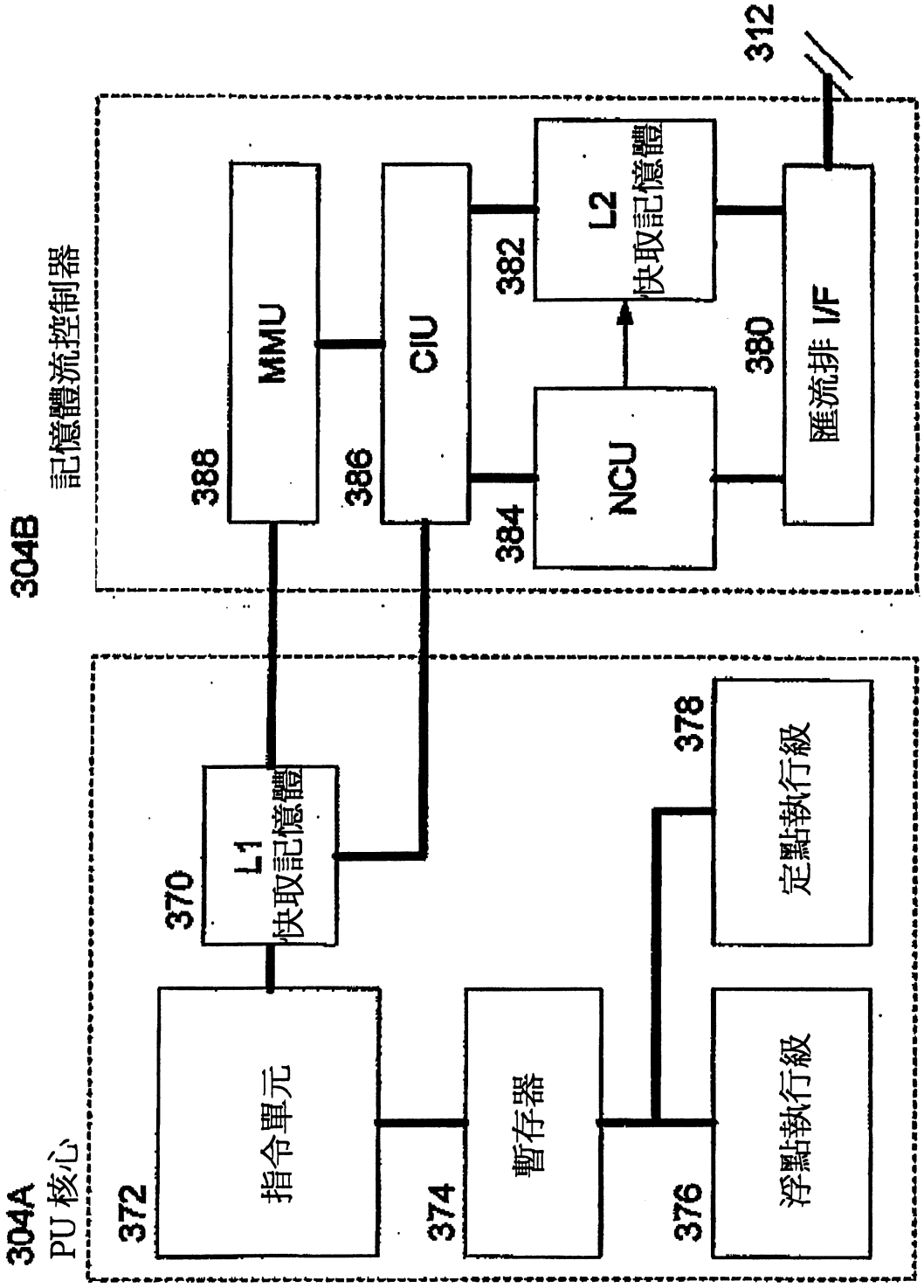
304
304A
PU 核心
372
指令單元
370
L1
快取記憶體
374
暫存器
376
浮點執行級
378
定點執行級
304B
記憶體流控制器
388
MMU
386
CIU
384
NCU
382
L2
快取記憶體
380
匯流排 I/F
312

圖 9

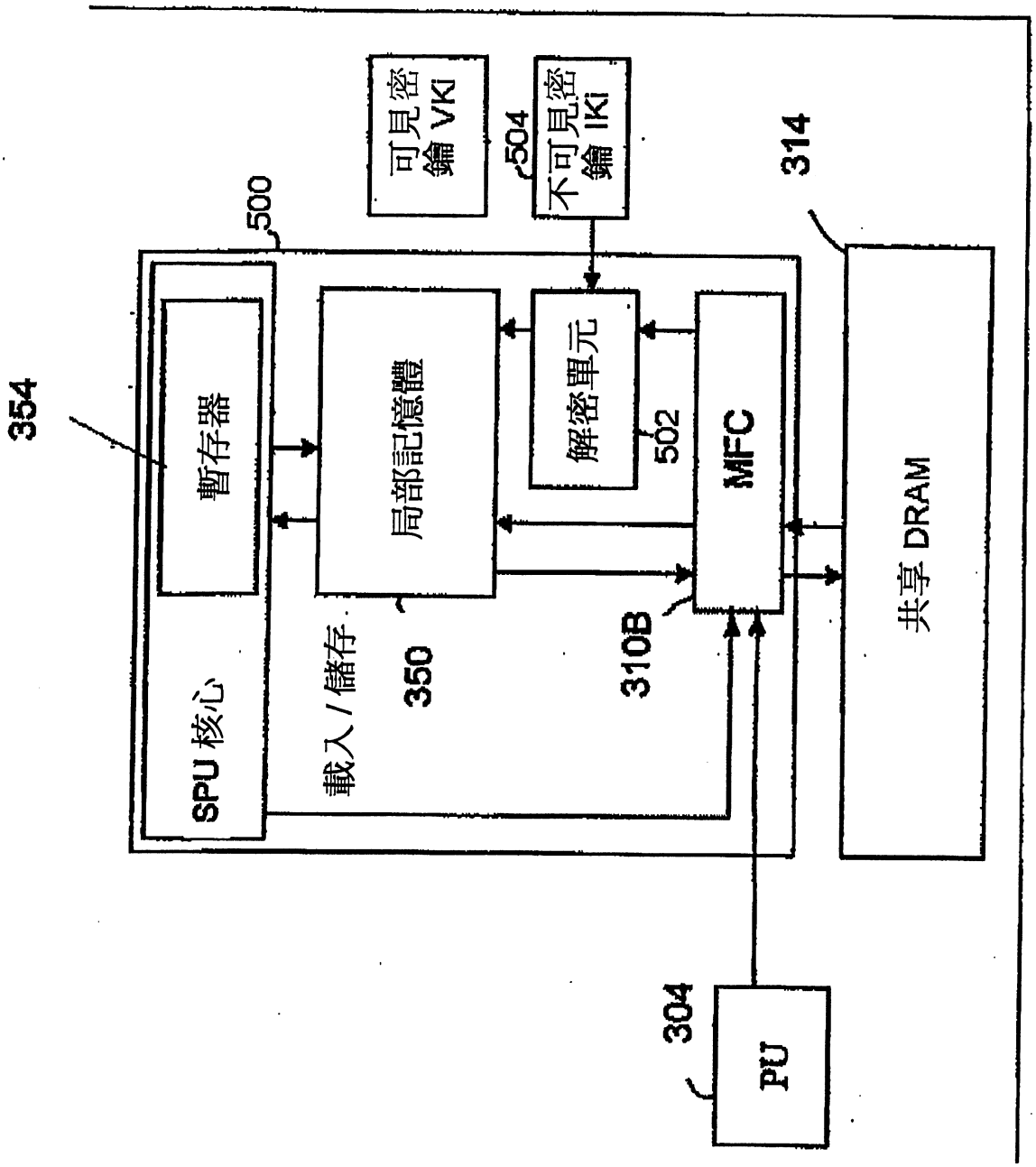
354
暫存器
SPU 核心
500
局部記憶體
載入 / 儲存
350
可見密鑰 VKi
504
不可見密鑰 IKi
解密單元
502
MFC
310B
314
共享 DRAM
304
PU

圖 10

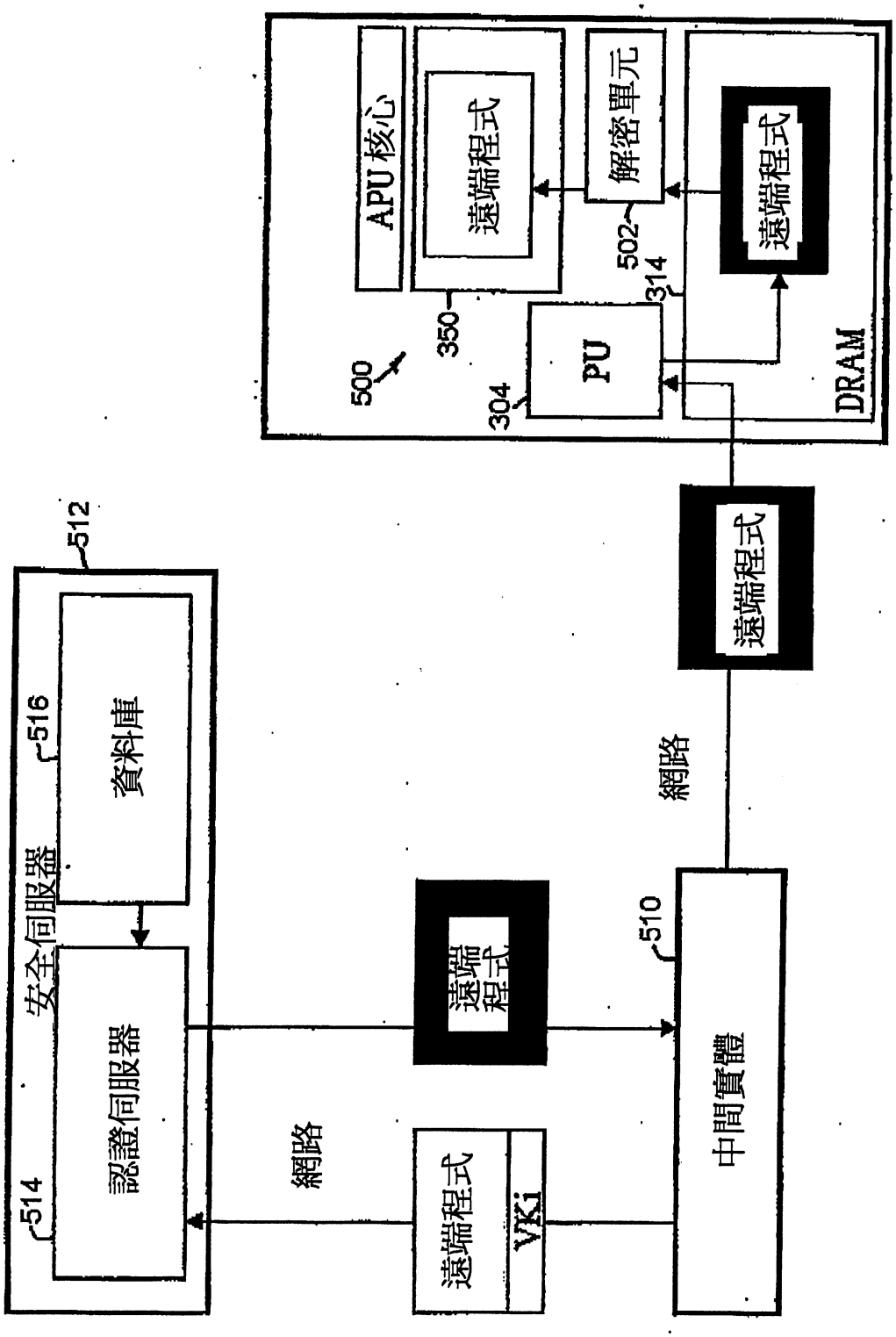
APU 核心
遠端程式
解密單元
遠端程式
500
350
502
314
304
PU
DRAM
遠端程式
網路
512
安全伺服器
資料庫
516
認證伺服器
514
遠端程式
網路
遠端程式
VKi
510
中間實體

圖 11

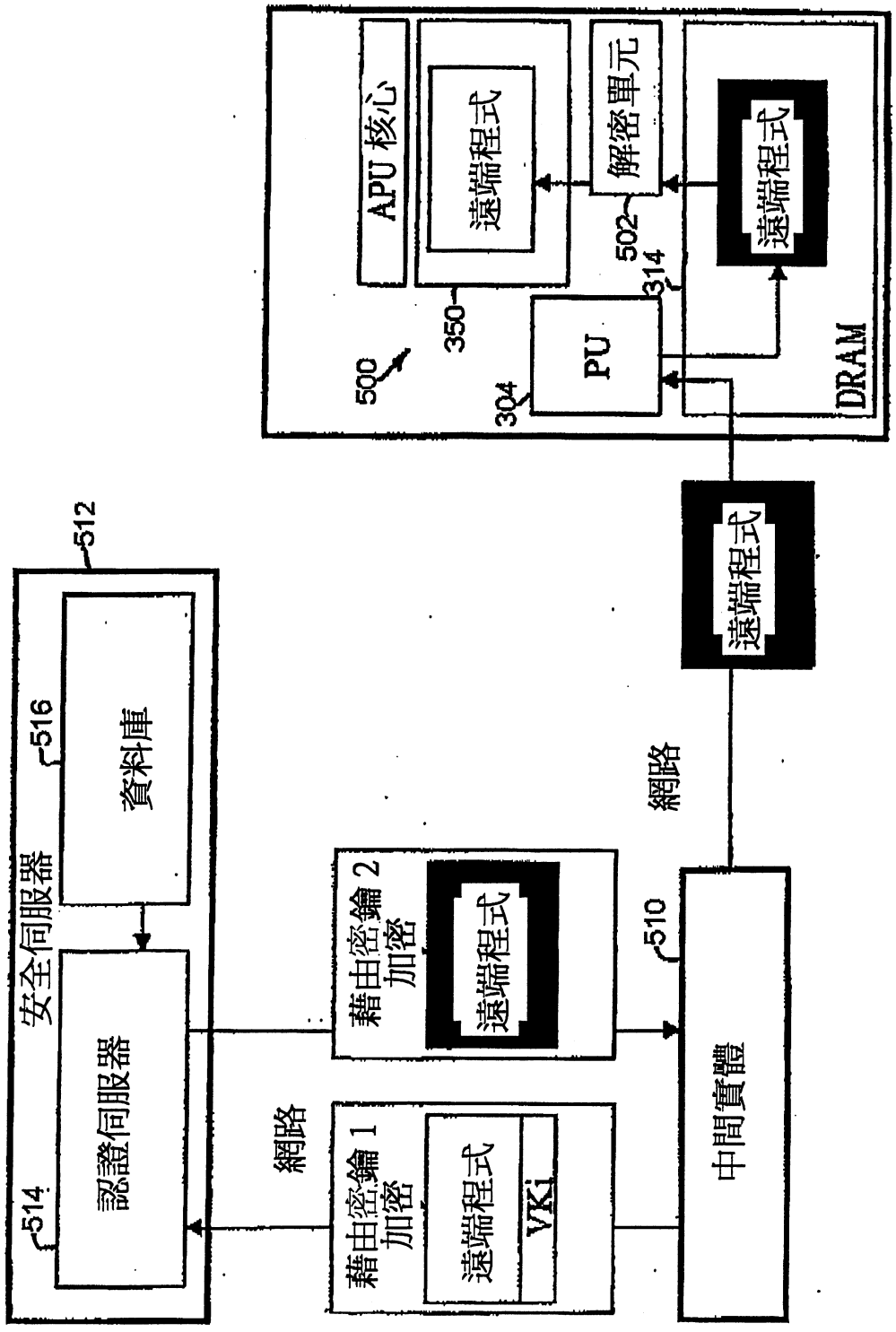
安全伺服器
512
資料庫
516
認證伺服器
514
網路
藉由密鑰 1 加密
遠端程式
VKi
藉由密鑰 2 加密
遠端程式
510
中間實體
網路
遠端程式
500
APU 核心
遠端程式
350
解密單元
502
PU
304
314
遠端程式
DRAM

圖 12

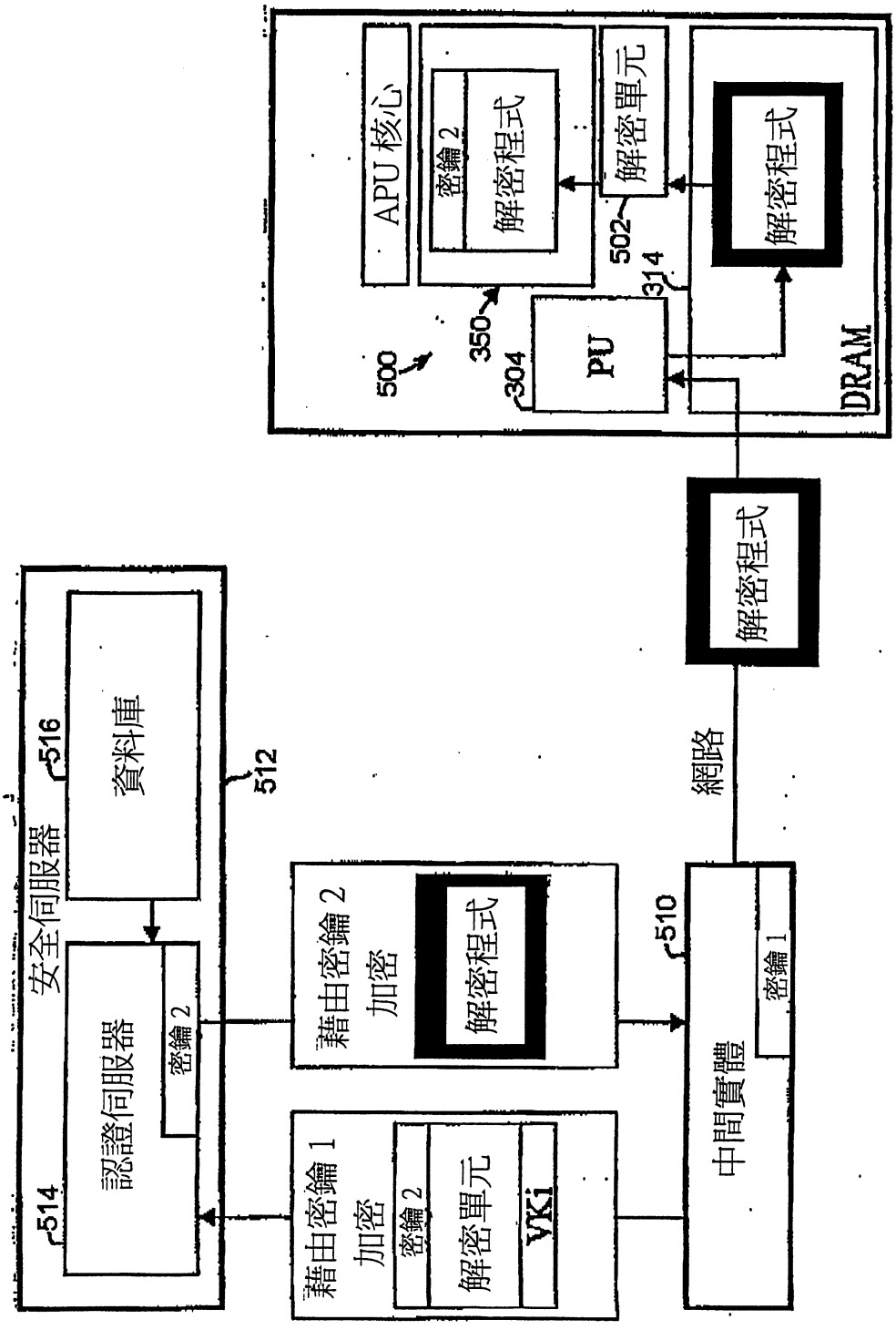
500
APU 核心
密鑰 2
解密程式
解密單元
502
350
304
PU
314
DRAM
解密程式
網路
解密程式
安全伺服器
516
資料庫
512
認證伺服器
密鑰 2
514
藉由密鑰 2
加密
解密程式
藉由密鑰 1
加密
密鑰 2
解密單元
VKi
510
中間實體
密鑰 1

圖 13

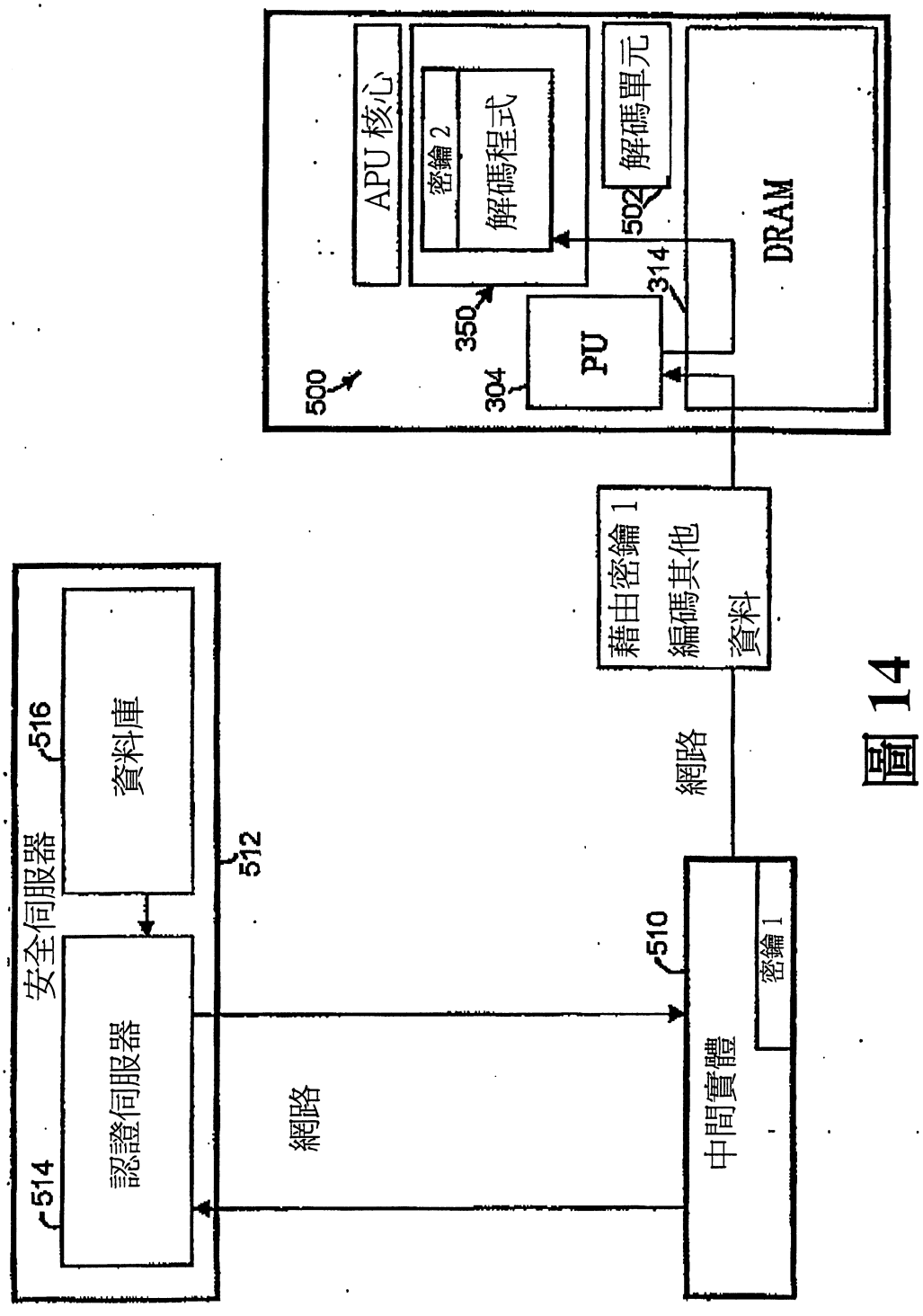
500
APU 核心
密鑰 2
解碼程式
解碼單元
502
350
304
PU
314
DRAM
藉由密鑰 1
編碼其他
資料
網路
安全伺服器
516
資料庫
512
認證伺服器
514
網路
510
中間實體
密鑰 1

圖 14

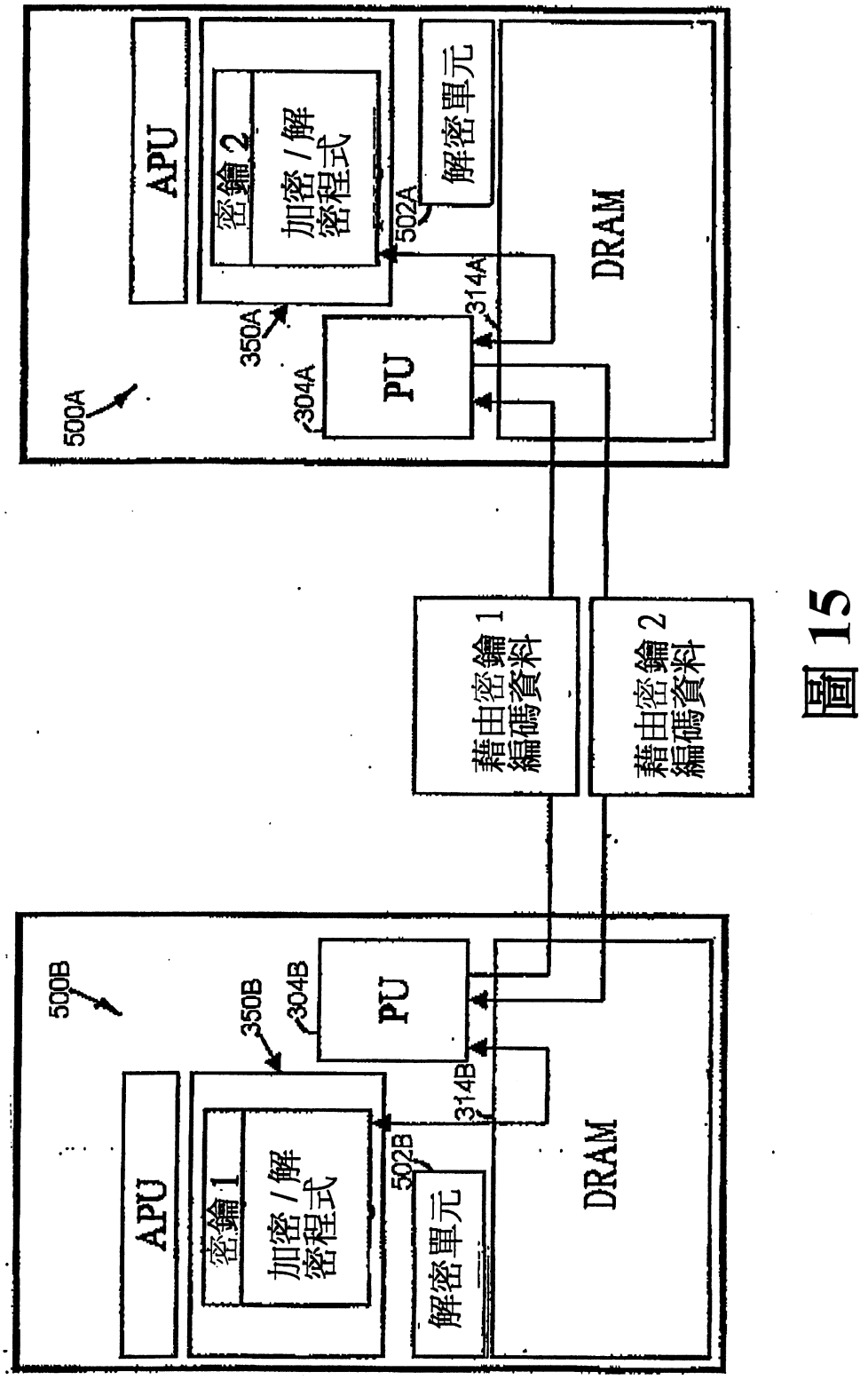
500A
APU
密鑰 2
加密 / 解密程式
350A
304A
PU
314A
502A
解密單元
DRAM
藉由密鑰 1 編碼資料
藉由密鑰 2 編碼資料
500B
APU
密鑰 1
加密 / 解密程式
350B
304B
PU
314B
502B
解密單元
DRAM

圖 15

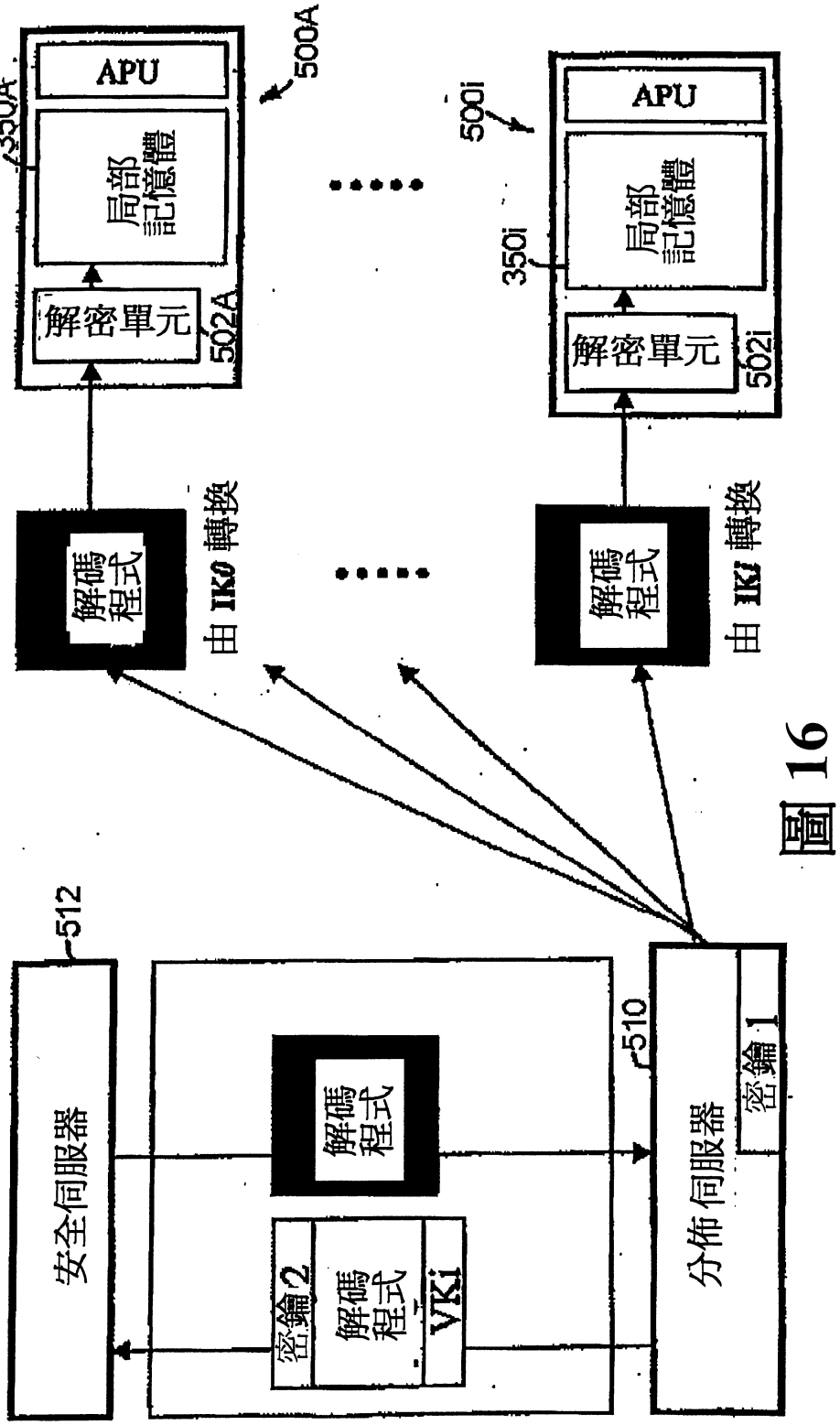
APU
局部記憶體
解密單元
350A
500A
502A
APU
局部記憶體
解密單元
350i
500i
502i
解碼程式
由 IK0 轉換
解碼程式
由 IKi 轉換
安全伺服器
512
解碼程式
密鑰2
解碼程式
VKi
510
分佈伺服器
密鑰 1

圖 16

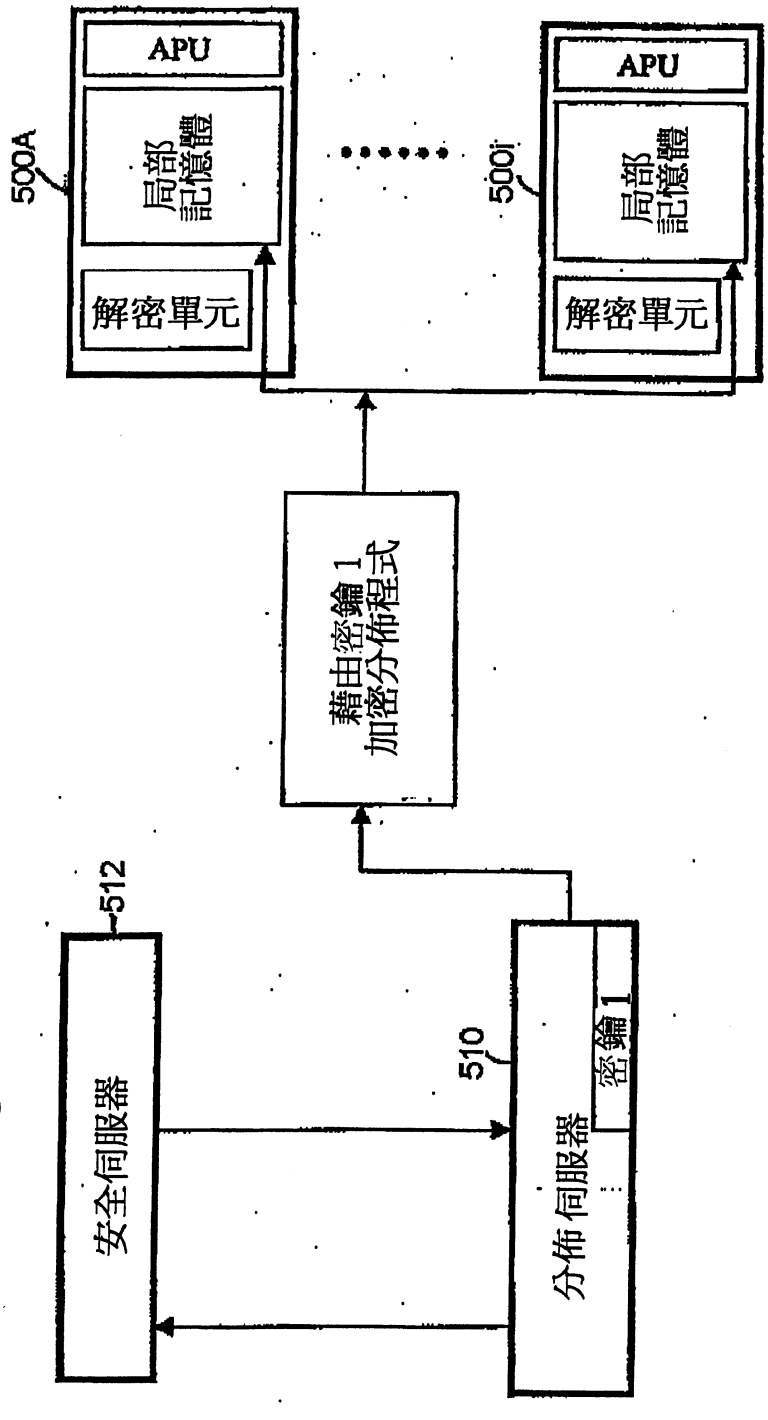
APU
局部記憶體
解密單元
500A
500i
藉由密鑰1加密分佈程式
512
安全伺服器
510
分佈伺服器
密鑰1

圖17

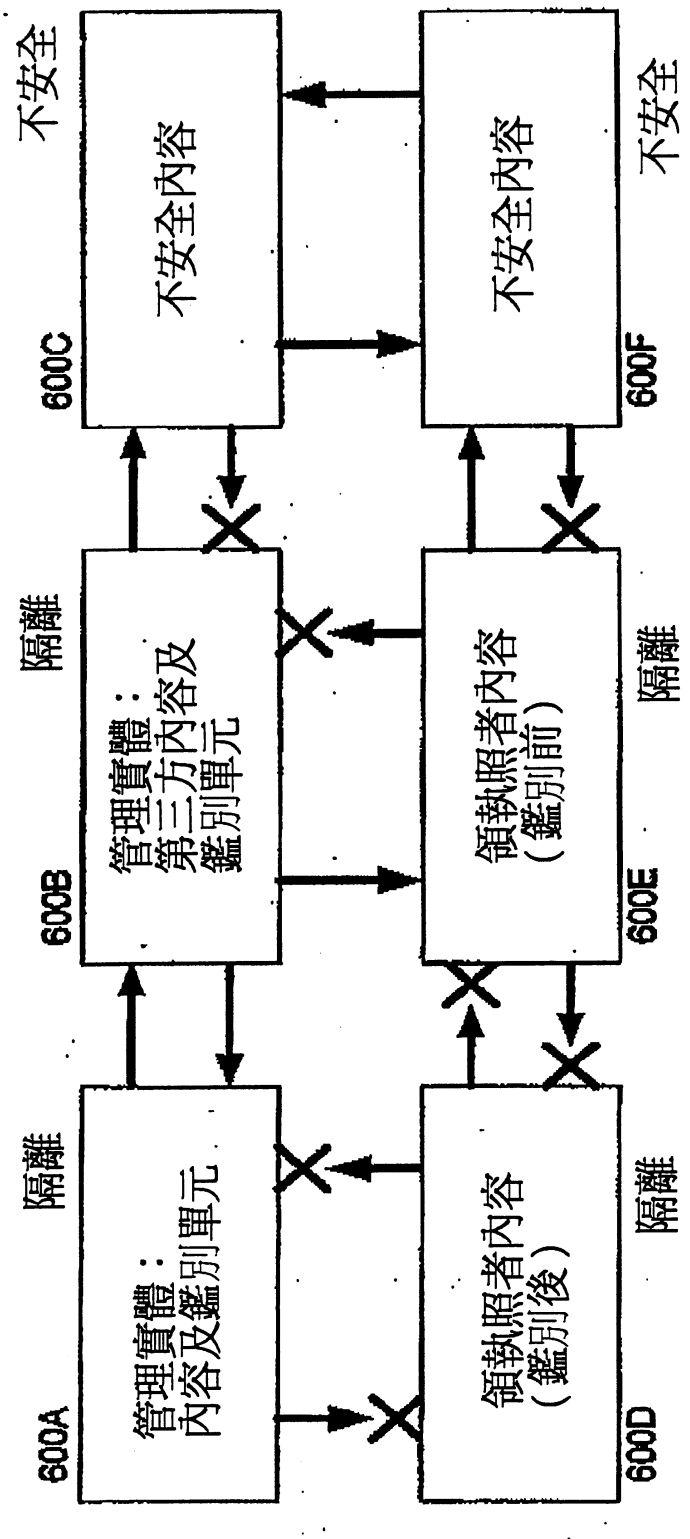
不安全
600C
不安全內容
不安全內容
不安全
隔離
600B
管理實體：
第三方內容及
鑑別單元
領執照者內容
（鑑別前）
600E
隔離
隔離
600A
管理實體：
內容及鑑別單元
領執照者內容
（鑑別後）
600D
隔離

圖 18

七、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明:

150	安全電路
152	秘密資料區域
154	可存取資料區域
156	邏輯電路
158	連接線路
160	資料線路

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

96年2月14日修(更)正替換頁

十、申請專利範圍：

1. 一種安全資料處理及傳輸之裝置，其包含：

一局部記憶體；

一匯流排，其可操作以向及從該局部記憶體載送資訊；

一或多個算術處理單元，其可操作以處理資料並且可操作性耦合至該局部記憶體；以及

一安全電路，其可操作以將該裝置放置於兩個操作模式之至少一個內，其中該等兩個操作模式包括以下各項之一：

(i)一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該局部記憶體之一傳送；以及

(ii)一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及該第三模式。

2. 如請求項1之裝置，其中當該裝置運行一鑑別例行程式時，該安全電路將該裝置放置於該第二模式內。

3. 如請求項1或2之裝置，其中：

該安全電路包括該安全電路外部之器件不可存取的一秘密資料區域，並且該秘密資料區域包含一第一密鑰及一第二密鑰；

該安全電路包括該安全電路外部之器件可存取的一可存取資料區域；以及

該安全電路包括邏輯電路，其在該裝置處於該第二模式時可操作以將該第一密鑰之一副本放置於該可存取資料區域內。

4. 如請求項3之裝置，其中在使用該裝置前在一可控程序中將該第一密鑰及該第二密鑰儲存於該秘密資料區域內，藉此保持安全。

5. 如請求項3之裝置，其中：

該安全電路較佳的係在該裝置運行一鑑別例行程式時將該裝置放置於該第二模式中，其包括執行一解密程式及執行一鑑別程式，該鑑別程式包括該第二密鑰之一副本，並且已根據該第一密鑰加密該鑑別程式；以及

該裝置執行該解密程式，以便將該可存取資料區域內包含的該第一密鑰之該副本用於解密該鑑別程式。

6. 如請求項5之裝置，其中：

該安全電路之該邏輯電路對該鑑別程式之該執行作出回應，將該第二密鑰之一副本放置於該可存取資料區域內；以及

該邏輯電路執行一決定，即該鑑別程式內包含的該第二密鑰之該副本是否匹配該可存取資料區域內包含的該第二密鑰之該副本。

7. 如請求項5之裝置，其中該安全電路可操作以將該裝置放置於該等第三操作模式中，在該鑑別程式內包含的該第

二密鑰之該副本匹配該可存取資料區域內包含的該第二密鑰之該副本時進入該第三模式。

8. 如請求項3之裝置，其中在使該裝置進入該第三模式之該放置前清除該可存取資料區域內包含的該等第一及第二密鑰之該等副本。

9. 一種置放於一單一器件內之複數個處理單元，該等處理單元之至少兩個包含：

一局部記憶體；

一匯流排，其可操作以向及從該局部記憶體載送資訊；

一或多個算術處理單元，其可操作以處理資料並且可操作性耦合至該局部記憶體；以及

一安全電路，其可操作以將該裝置放置於兩個操作模式之至少一個內，其中該等兩個操作模式包括以下各項之一：

(i)一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送；以及

(ii)一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及該第三模式。

10. 一種安全資料處理及傳輸之方法，其包含：

將一裝置放置於複數個操作模式之至少一個操作模式

中，其中：

該裝置包括一局部記憶體、可操作以向及從該局部記憶體載送資訊之一匯流排、可操作以處理資料並且可操作性耦合至該局部記憶體之一或多個算術處理單元以及可操作以將該裝置放置於該等操作模式內之一安全電路；以及

該複數個操作模式包括以下各項之一：

(i)一第一模式，藉此該裝置及一外部器件可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及一第三模式，藉此該裝置可啟動資訊在該匯流排上進入或離開該記憶體之一傳送，但該外部器件不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送；以及

(ii)一第二模式，藉此該裝置及該外部器件皆不能啟動資訊在該匯流排上進入或離開該記憶體之一傳送，以及該第三模式。

11. 如請求項10之方法，其進一步包含當該裝置運行一鑑別例行程式時將該裝置放置於該第二模式中。

12. 如請求項10或11之方法，其中：

該安全電路包括該安全電路外部之器件不可存取之一秘密資料區域，該秘密資料區域包含一第一密鑰及一第二密鑰，並且該安全電路包括該安全電路外部之器件可存取之一可存取資料區域；以及

該方法進一步包含當該裝置處於該第二模式內時將該第一密鑰之一副本放置於該可存取資料區域內。

13. 如請求項12之方法，其進一步包含在使用該裝置前在一可控程序中將該第一密鑰及該第二密鑰儲存於該秘密資料區域內，藉此保持安全。

14. 如請求項12之方法，其進一步包含：

在該裝置運行一鑑別例行程式時將該裝置放置於該第二模式中，其中該例行程式包括執行一解密程式及執行一鑑別程式，該鑑別程式包括該第二密鑰之一副本，並且已根據該第一密鑰加密該鑑別程式；以及

執行該解密程式，以便將該可存取資料區域內包含的該第一密鑰之該副本用於解密該鑑別程式。

15. 如請求項14之方法，其進一步包括：

對該鑑別程式之該執行作出回應，將該第二密鑰之一副本放置於該可存取資料區域內；以及

決定該鑑別程式內包含的該第二密鑰之該副本是否匹配該可存取資料區域內包含的該第二密鑰之該副本。

16. 如請求項14之方法，其中可進入該等三個模式之任何模式，並且該方法進一步包含當該鑑別程式內包含的該第二密鑰之該副本匹配該可存取資料區域內包含的該第二密鑰之該副本時，將該裝置放置於該第三模式內。

17. 如請求項12之方法，其進一步包含在使該裝置進入該第三模式之該放置前清除該可存取資料區域內包含的該等第一及第二密鑰之該等副本。

18. 一種安全資料處理及傳輸之裝置，其包含：

一主要處理單元；

複數個附著處理單元，各附著處理單元包括一局部記憶體及一解密單元，並且各附著處理單元可操作以進入一正常操作模式或一安全操作模式；以及

一共享記憶體，其中：

該主要處理單元能夠啟動該共享記憶體與該等附著處理單元之一給定附著處理單元間的資料傳輸，當該給定附著處理單元處於該正常模式時其繞過該解密單元，以及

該主要處理單元能夠：(i)啟動該給定附著處理單元至該共享記憶體之資料傳送；或者(ii)啟動該共享記憶體至該給定附著處理單元之資料傳送，當該給定附著處理單元處於該安全模式時其繞過該解密單元。

19. 如請求項18之裝置，其中該等附著處理單元能夠啟動與該共享記憶體之資料傳送，而不論其是處於該正常操作模式還是該安全操作模式。

20. 如請求項18或19之裝置，其中該等附著處理單元可操作以根據一硬體重設狀況及一啟動狀況之至少一項進入該安全操作模式。

21. 如請求項18或19之裝置，其中該等資料可包括一軟體程式之至少部分。

22. 如請求項18或19之裝置，其中各附著處理單元包括一安全儲存器，其包含一實質上唯一的密鑰，該密鑰僅可由該給定附著處理單元的該解密單元之至少一個來存取，以及經過授權的實體。

23. 如請求項22之裝置，其中各附著處理單元之該解密單元

使用該密鑰來解密從該共享記憶體至該局部記憶體之資料傳送，其係在該給定附著處理單元處於該安全操作模式時由該主要處理單元來啟動。

24. 如請求項22之裝置，其中該共享記憶體可包含已加密資料，其已使用該等附著處理單元之該等實質上唯一的密鑰之一來加密。

25. 如請求項22之裝置，其中各附著處理單元與一實質上唯一的ID以及該裝置相關聯，該ID可係給定附著處理單元之至少一個外部的實體已知的。

26. 如請求項24之裝置，其中藉由該裝置外部之一安全實體加密該等已加密資料，該安全實體係經過授權以使用該給定附著處理單元之該密鑰。

27. 如請求項22之裝置，其中該安全實體包括一資料庫，其包含參與附著處理單元之該等ID及密鑰，用於一給定附著處理單元之各ID及密鑰彼此相關聯。

28. 如請求項22之裝置，其中在該不安全實體向該安全實體提供與該密鑰相關聯之一ID後，該安全實體採用一給定附著處理單元之該密鑰加密從一不安全實體接收並且未經授權以使用該給定附著處理單元之該密鑰的資料。

29. 如請求項28之裝置，其中：

該安全實體可操作以向該不安全實體提供該等已加密資料；

該不安全實體可操作以向該裝置提供該等已加密資料，以便儲存於該共享記憶體內；

該主要處理單元可操作以啟動該等已加密資料從該共享記憶體至該給定附著處理單元之一傳送，以便將該等已加密資料輸入該解密單元；以及

該給定附著處理單元之該解密單元可操作以使用該給定附著處理單元之該密鑰解密該等已加密資料，以便將該等資料儲存於該給定附著處理單元之該局部記憶體內。

30. 如請求項22之裝置，其中：

未經授權以使用一給定附著處理單元之該密鑰的一不安全實體使用一第一對稱密鑰加密該等資料，向該安全實體提供該等已加密資料，並向該安全實體提供與一給定附著處理單元相關聯之一ID；

該安全實體使用一第二對稱密鑰解密該不安全實體所提供之該等已加密資料，並使用與從該不安全實體接收之該ID相關聯的該給定附著處理單元之該密鑰加密該等資料。

31. 如請求項30之裝置，其中該不安全實體使用該第一對稱密鑰加密該等資料及該給定附著處理器單元之該ID，並向該安全實體提供該等已加密資料/ID。

32. 如請求項30之裝置，其中：

該安全實體可操作以使用該第二對稱密鑰加密該等已加密資料，並向該不安全實體提供該等加密已加密資料；

該不安全實體可操作以使用該第一對稱密鑰解密該等加密已加密資料，以獲得使用該給定附著處理單元之該

密鑰產生的該等已加密資料，以及向該裝置提供該等已加密資料，以便將其儲存於該共享記憶體內；

該主要處理單元可操作以啟動該等已加密資料從該共享記憶體至該給定附著處理單元之一傳送，以便將該等已加密資料輸入該解密單元；以及

該給定附著處理單元之該解密單元可操作以使用該給定附著處理單元之該密鑰解密該等已加密資料，以便將該等資料儲存於該給定附著處理單元之該局部記憶體內。

33. 如請求項22之裝置，其中：

該等資料為一解密程式；

未經授權以使用一給定附著處理單元之該密鑰的一不安全實體使用一第一對稱密鑰加密該解密程式，向該安全實體提供該已加密解密程式，並向該安全實體提供與一給定附著處理單元相關聯之一ID；以及

該安全實體使用一第二對稱密鑰解密該不安全實體所提供之該已加密解密程式，並使用與從該不安全實體接收之該ID相關聯的該給定附著處理單元之該密鑰加密該解密程式及該第二對稱密鑰。

34. 如請求項33之裝置，其中該不安全實體使用該第一對稱密鑰加密該解密程式及該給定附著處理器單元之該ID，並向該安全實體提供該已加密解密程式/ID。

35. 如請求項33之裝置，其中該不安全實體使用該第一對稱密鑰加密該解密程式、該給定附著處理器單元之該ID以及該第二對稱密鑰，並向該安全實體提供該已加密解密

程式/ID/第二對稱密鑰。

36. 如請求項33之裝置，其中：

該安全實體可操作以使用該第二對稱密鑰加密該已加密解密程式及該第二對稱密鑰，並向該不安全實體提供該加密已加密解密程式/第二對稱密鑰；

該不安全實體可操作以使用該第一對稱密鑰解密該加密已加密解密程式/第二對稱密鑰，以獲得使用該給定附著處理單元之該密鑰產生的該已加密解密程式/第二對稱密鑰，以及向該裝置提供該已加密解密程式/第二對稱密鑰，以便將其儲存於該共享記憶體內；

該主要處理單元可操作以啟動該已加密解密程式/第二對稱密鑰從該共享記憶體至該給定附著處理單元之一傳送，以便將該已加密解密程式/第二對稱密鑰輸入該解密單元；以及

該給定附著處理單元之該解密單元可操作以使用該給定附著處理單元之該密鑰解密該已加密解密程式/第二對稱密鑰，以便將該已加密解密程式及該第二對稱密鑰儲存於該給定附著處理單元之該局部記憶體內。

37. 如請求項36之裝置，其中不安全實體可操作以使用第一對稱密鑰加密資料並向該裝置提供該等已加密資料，以便將其儲存於該共享記憶體內。

38. 如請求項36之裝置，其中該給定附著處理單元能夠從該共享記憶體接收該等已加密資料並繞過該解密單元將其傳送至該局部記憶體內。

39. 如請求項38之裝置，其中當從該共享記憶體接收該等已加密資料並將其傳送至該局部記憶體內時，該給定附著處理單元可處於該正常模式或該安全模式。

40. 如請求項36之裝置，其中該給定附著處理單元可操作以使用該解密程式及該第二對稱密鑰解密該等已加密資料。

41. 如請求項40之裝置，其中該等資料可包括一軟體程式。

42. 如請求項36之裝置，其中該主要處理單元可操作以啟動該等已加密資料從該共享記憶體繞過該解密單元至該給定附著處理單元該局部記憶體內的該傳送。

43. 一種安全資料處理及傳輸之方法，其包含：

提供一主要處理單元、複數個附著 處理單元及一共享記憶體，各附著處理單元包括一局部記憶體及一解密單元，並且可操作以進入一安全操作模式；以及

當該附著處理單元之一給定附著處理單元處於該安全模式時，禁止該主要處理單元啟動從該共享記憶體至該給定處理單元的一資料傳送，其繞過該解密單元，以便從外部啟動的進入該局部記憶體之任何資料傳送必須由該解密單元使用對該給定附著處理單元實質上係唯一的且僅經過授權之實體才知道的一密鑰來解密。

44. 如請求項43之方法，其進一步包括：

使該輔助處理單元可啟動與該共享記憶體之資料傳送，而不論其是否處於該安全操作模式。

45. 如請求項43或44之方法，其進一步包含：

根據一硬體重設狀況及一啟動狀況之至少一項使該等附著處理單元進入該安全操作模式。

46. 如請求項43或44之方法，其進一步包含：

從一中間實體向一安全實體發送資料及與該等附著處理單元之一給定附著處理單元相關聯之一ID；

搜尋包含參與附著處理單元的ID及相關聯密鑰之該安全實體的一資料庫，並獲得與接收該ID的該給定附著處理單元相關聯之該密鑰；

使用與接收該ID的該給定附著處理單元相關聯之該密鑰加密發送至該安全實體之該等資料；以及

從該安全實體發送該等已加密資料至該中間實體。

47. 如請求項46之方法，其進一步包括：

從該中間實體發送該等已加密資料至該給定附著處理單元之共享記憶體；

當該給定附著處理單元處於該安全模式時，啟動該等已加密資料從該共享記憶體至該給定附著處理單元之一傳送，以便該解密單元使用該密鑰加密該等已加密資料；以及

將該等資料儲存於該給定輔助處理單元之該局部記憶體內。

48. 如請求項43之方法，其進一步包含：

使用一第一對稱密鑰在該中間實體內加密該等資料及與該等附著處理單元之一給定處理單元相關聯的一ID之至少一項；

從該中間實體發送該等已加密資料及該ID至一安全實體；

使用一第二對稱密鑰在該安全實體內解密該等已加密資料及該ID之至少一項；

搜尋包含參與附著處理單元的ID及相關聯密鑰之該安全實體的一資料庫，並獲得與接收該ID的該給定附著處理單元相關聯之該密鑰；

使用與該給定附著處理單元相關聯之該密鑰在該安全實體加密該等資料，使用該第二對稱密鑰加密該等已加密資料；以及

從該安全實體發送該等加密已加密資料至該中間實體。

49. 如請求項48之方法，其進一步包括：

使用該第一對稱密鑰在該中間實體解密該等加密已加密資料，以獲得藉由與該給定附著處理單元相關聯之該密鑰加密的該等資料；

從該中間實體發送該等已加密資料至該給定附著處理單元之共享記憶體；

當該給定附著處理單元處於該安全模式時，啟動該等已加密資料從該共享記憶體至該給定附著處理單元之一傳送，以便該解密單元使用該密鑰加密該等已加密資料；以及

將該等資料儲存於該給定輔助處理單元之該局部記憶體內。

50. 如請求項49之方法，其中該等資料包括(i)一解密程式，

及(ii)該第二對稱密鑰，該方法進一步包含：

使用該第一對稱密鑰在該中間實體加密其他資料；

將該等已加密其他資料從該中間實體發送至該給定附著處理單元，以便儲存於該共享記憶體內；以及

啟動該等其他已加密資料從該共享記憶體至該局部記憶體之該傳送，同時該給定附著處理單元不在該安全模式內，以便繞過該解密單元。

51. 如請求項50之方法，其進一步包括：

使用該給定附著處理單元以使用該解密程式及該第二對稱密鑰解密該等其他已加密資料。

52. 如請求項49項之方法，其中該資料包括(i)一加密/解密程式，以及(ii)與該加密/解密程式相關聯之一對對稱密鑰之一，以便將其儲存於該給定附著處理單元之該局部記憶體內，該方法進一步包含：

使用其他資料及另一附著處理單元重複該方法之該等步驟，該等其他資料包括(i)另一加密/解密程式，以及(ii)與另一該加密/解密程式相關聯之該對對稱密鑰之另一密鑰，以便將其儲存於該另一附著處理單元之該局部記憶體內。

53. 如請求項52之方法，其進一步包括：

使用該加密/解密程式及該給定附著處理單元之該一個對稱密鑰加密其他資料；

將該等其他已加密資料從該給定附著處理單元發送至該其他附著處理單元，以便儲存於其一共享記憶體內；

以及

啟動該等其他已加密資料從該共享記憶體至該另一附著處理單元的該局部記憶體之該傳送，同時該另一附著處理單元不在該安全模式內，以便繞過該解密單元。

54. 如請求項53之方法，其進一步包括：

使用該另一附著處理單元以使用該另一加密/解密程式及該另一對稱密鑰解密該等其他已加密資料。

55. 如請求項52之方法，其進一步包括：

使用該加密/解密程式及該另一附著處理單元之該其他對稱密鑰加密其他資料；

將該等其他已加密資料從該另一附著處理單元發送至該給定附著處理單元，以便儲存於其一共享記憶體內；以及

啟動該等其他已加密資料從該共享記憶體至該給定附著處理單元的該局部記憶體之該傳送，同時該給定附著處理單元不在該安全模式內，以便繞過該解密單元。

56. 如請求項55之方法，其進一步包括：

使用該給定附著處理單元以使用該加密/解密程式及該一個對稱密鑰解密該等其他已加密資料。

57. 如請求項55之方法，其中該給定附著處理單元之該共享記憶體與該另一附著處理單元之該共享記憶體係相同記憶體。

58. 如請求項49項之方法，其中該資料包括(i)一解密程式，以及(ii)與該解密程式相關聯之該第二對稱密鑰，以便將

其儲存於該給定附著處理單元之該局部記憶體內，該方法進一步包含：

使用其他附著處理單元重複該方法之該等步驟，以便將該解密程式及該第二對稱密鑰儲存於該等附著處理單元之各附著處理單元中。

59. 如請求項58之方法，其進一步包括：

使用該第一對稱密鑰在該中間實體加密其他資料；

將該等已加密其他資料從該中間實體發送至該等附著處理單元之各個，以便儲存於該共享記憶體內；以及

啟動該等其他已加密資料從該共享記憶體至該等附著處理單元的該等個別局部記憶體之該傳送，同時該等附著處理單元不在該安全模式內，以便繞過該等個別解密單元。

60. 如請求項59之方法，其進一步包括：使用該等附著處理單元以使用該等個別解密程式及該等第二對稱密鑰解密該等其他已加密資料。