I546699

(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 I546699 B**

(45)公告日： 中華民國 105 (2016) 年 08 月 21 日

(21)申請案號：104124936 (22)申請日： 中華民國 104 (2015) 年 07 月 31 日

(51)Int. Cl.： *G06F21/71 (2013.01)* *G06F21/78 (2013.01)*

(30)優先權：2014/09/10 美國 14/482,136

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

(72)發明人：利姆 文森特 J ZIMMER, VINCENT J. (US)；貝瑞 彼得 J BARRY, PETER J. (IE)；普納夏德蘭 拉傑許 POORNACHANDRAN, RAJESH (IN)；范德文 阿珍 VAN DE VEN, ARJAN (NL)；戴斯 彼得 A DICE, PETER A. (US)；塞爾瓦拉吉 葛皮納斯 SELVARAJE, GOPINATTH (US)；卡倫諾 朱利安 CARRENO, JULIEN (FR)；羅森保 李 G ROSENBAUM, LEE G. (US)

(74)代理人：惲軼群；陳文郎

(56)參考文獻：

TW	201227390A	TW	201329774A
US	7592829B2	US	2003/0088784A1

審查人員：林民安

申請專利範圍項數：20 項 圖式數：6 共 39 頁

(54)名稱

使用一處理器以提供可信賴執行環境的技術

PROVIDING A TRUSTED EXECUTION ENVIRONMENT USING A PROCESSOR

(57)摘要

在一實施例中，系統單晶片包括：單個核心，其用以執行舊式指令集，該單個核心經組配來進入系統管理模式(SMM)以提供可信賴執行環境來進行至少一安全操作；以及記憶體控制器，其耦接至該單個核心，該記憶體控制器用以與系統記憶體介接，其中該系統記憶體之一部分包含用於該 SMM 之安全記憶體，且該單個核心用以鑑定且執行啟動韌體，且將控制傳遞至該 SMM 以自受保護儲存器獲得金鑰對且將該金鑰對儲存於該安全記憶體中。本發明描述且主張其他實施例。

In an embodiment, a system on a chip includes: a single core to execute a legacy instruction set, the single core configured to enter a system management mode (SMM) to provide a trusted execution environment to perform at least one secure operation; and a memory controller coupled to the single core, the memory controller to interface with a system memory, where a portion of the system memory comprises a secure memory for the SMM, and the single core is to authenticate and execute a boot firmware, and pass control to the SMM to obtain a key pair from a protected storage and store the key pair in the secure memory. Other embodiments are described and claimed.

指定代表圖：

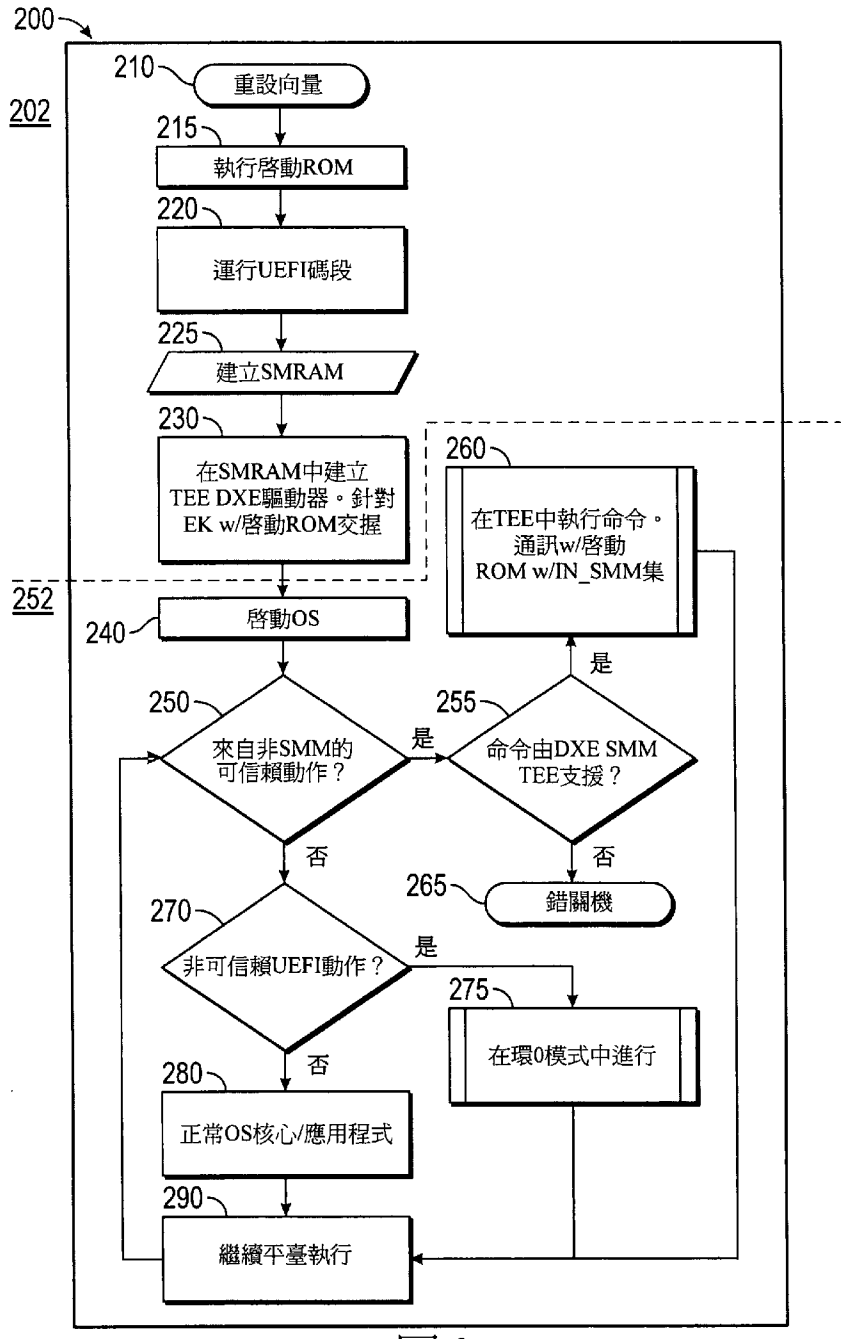

圖 2

符號簡單說明：

200・・・方法

202・・・預啟動環境

210~240、260、265、275~290・・・方塊

250、255、270・・・菱形

252・・・啟動或 OS 環境

I546699

公告本

發明摘要

※ 申請案號：104124936

※ 申請日：104. 7. 31　※IPC 分類：G06F 21/71 (2013.01)
21/78 (2013.01)

【發明名稱】(中文/英文)

使用一處理器以提供可信賴執行環境的技術
PROVIDING A TRUSTED EXECUTION ENVIRONMENT USING A PROCESSOR

【中文】

在一實施例中，系統單晶片包括：單個核心，其用以執行舊式指令集，該單個核心經組配來進入系統管理模式(SMM)以提供可信賴執行環境來進行至少一安全操作；以及記憶體控制器，其耦接至該單個核心，該記憶體控制器用以與系統記憶體介接，其中該系統記憶體之一部分包含用於該SMM之安全記憶體，且該單個核心用以鑑定且執行啓動韌體，且將控制傳遞至該SMM以自受保護儲存器獲得金鑰對且將該金鑰對儲存於該安全記憶體中。本發明描述且主張其他實施例。

【英文】

In an embodiment, a system on a chip includes: a single core to execute a legacy instruction set, the single core configured to enter a system management mode (SMM) to provide a trusted execution environment to perform at least one secure operation; and a memory controller coupled to the single core, the memory controller to interface with a system memory, where a portion of the system memory comprises a secure memory for the SMM, and the single core is to authenticate and execute a boot firmware, and pass control to the SMM to obtain a key pair from a protected storage and store the key pair in the secure memory. Other embodiments are described and claimed.

【代表圖】

【本案指定代表圖】：第（2）圖。

【本代表圖之符號簡單說明】：

200...方法
202...預啓動環境
210～240、260、265、275～290...方塊
250、255、270...菱形
252...啓動或OS環境

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

使用一處理器以提供可信賴執行環境的技術
PROVIDING A TRUSTED EXECUTION ENVIRONMENT USING A PROCESSOR

【技術領域】

發明領域

[0001]實施例係關於爲計算裝置提供安全性。

【先前技術】

發明背景

[0002]隨著諸如智慧型電話、平板電腦等的可攜式計算裝置變得更流行，安全性問題出現，因爲使用者力圖使用可容易監聽的不信賴裝置來執行金融或其他商業交易。另外，一些使用者希望使用可攜式計算裝置來存取安全數位內容，諸如受保護的媒體內容。然而，某些內容在允許對內容之存取之前委任安全環境。另外，不信賴裝置可不允許對此內容之存取。

【發明內容】

[0003]依據本發明之一實施例，係特地提出一種系統單晶片(SoC)，其包含：一單個核心，其用以執行一舊式指令集，其中該單個核心經組配來進入一系統管理模式(SMM)以提供一可信賴執行環境(TEE)來進行至少一安全操作；以及一記憶體控制器，其耦接至該單個核心，該記憶體控制器用以與一系統記憶體介接，其中該系統記憶體之一部分

包含用於該SMM之一安全記憶體，且其中該單個核心係用以鑑定一啓動韌體，用以執行該啓動韌體，且用以將控制傳遞至該SMM以自一受保護儲存器獲得一金鑰對且將該金鑰對儲存於該安全記憶體中。

【圖式簡單說明】

[0004]圖1爲根據本發明之一實施例之處理器的方塊圖。

[0005]圖2爲根據本發明之一實施例之方法的流程圖。

[0006]圖3爲在一實施例中用於處置受保護數位內容的佈置的方塊圖。

[0007]圖4爲根據本發明之一實施例之系統佈置的方塊圖。

[0008]圖5爲另一示例性系統的方塊圖，實施例可與該另一示例性系統一起使用。

[0009]圖6爲另一示例性系統的方塊圖，實施例可與該另一示例性系統一起使用。

【實施方式】

較佳實施例之詳細說明

[0010]在各種實施例中，可爲可攜式計算裝置提供可信賴執行環境(TEE)，甚至在此平台之中央處理器或系統單晶片(SoC)具有低電力單核心設計的情況下亦可提供，該低電力單核心設計固有地不具有用於安全環境之硬體能力(諸如藉由安全性共處理器、硬體可信賴平台模組(TPM)等之方式)。此TEE可藉由硬體/軟體共設計處理器實現，該硬體/

軟體共設計處理器提供基於硬體及軟體的技術之組合以用於例示TEE。因此，使用本發明之一實施例，可在行動平台中創建TEE以執行數位權利管理(DRM)、韌體TPM(fTPM)操作、一次密碼(OTP)及其他高保證用法。儘管本發明之範疇在此方面不受限制，但是安全操作之有關及額外實例包括：可信賴路徑之創建及維持以便提供受保護音訊視訊路徑(PAVP)；以及安全輸入/輸出路徑之創建及維持，等等。

[0011]使用本發明之一實施例，可爲平台提供TEE，該平台具有處理器，該處理器不具有以下任一者：內在安全性能力，諸如Intel®軟體防護延伸(SGX)能力(藉由處理器內部硬體及至給定指令集(例如，Intel架構(IA)32或64指令集)之延伸之方式，該等延伸係經由基於微碼的隔離機構來在使用者環境中提供容器)；或專屬安全性硬體資源，諸如收斂安全性管理引擎(CSME)，其可自身爲根據諸如Intel® Minute設計的給定處理器設計之共處理器。此共處理器可不適合於在給定實施例中，因爲另一Minute IA核心之增添(在單個核心自身爲Minute IA核心的情況下)將增加晶粒大小、電力消耗及成本，此狀況可規定反對使用於各種可攜式計算裝置中，該等可攜式計算裝置範圍包括智慧型電話、平板電腦、隨身裝置(wearable)、嵌入裝置等。當然，實施例不限於基於Intel®的處理器，且同樣地適用於其他製造商或授權人之處理器，諸如具有ARM架構的處理器，諸如基於Cortex的處理器或SoC或可得自AMD公司或其他公司的處理器。

[0012]請注意，如本文所使用，TEE因此包括基於硬體的隔離機構及此硬體受保護領域內之軟體環境。在一實施例中，TEE可提供於處理器之系統管理模式(SMM)內。更具體而言，啓動唯讀記憶體(ROM)之特徵結合SMM工作來在SoC或具有最小計算能力(使得專屬核心、共處理器或其他安全邏輯不可利用於執行TEE創建及安全環境操作)的其他處理器中提供TEE。爲此，可經由如本文所描述之機構使用用以執行至少密鑰儲存的啓動ROM之碼或邏輯及用以使存取此等啓動ROM能力有資格的存取控制邏輯之組合來在此處理器中提供TEE，使得非SMM碼無法存取啓動ROM。

[0013]對於TEE內之軟體機構，可呈現諸如Java™類虛擬機器及/或仿真SGX或『eSGX』的虛擬機器，以便提供一些程度之可信賴軟體應用程式相容性。在一實施例中，可經由全域平台(GP)——風格應用程式設計介面(API)進入至TEE中。

[0014]一般而言，SMM爲在環0/監督器模式(或IA VMX根)下運行的最高特權執行模式。在一實施例中，進入至SMM中可藉由系統管理中斷(SMI)觸發。此觸發器可由諸如系統管理模式範圍暫存器的硬體隔離機構驗證，該硬體隔離機構可經組配來證實對系統記憶體之受保護部分的有效存取。

[0015]作爲總體觀點，TEE可經由啓動ROM碼(及安全密鑰儲存)及此碼與SMM操作之間的互動實現。在製造時間期間，認可金鑰(EK)金鑰對經產生且儲存於諸如私用隔離

金鑰儲存體的啓動ROM私用資源中。隨後在啓動時間期間，啓動ROM首先保證一致可擴展韌體介面(UEFI)韌體爲真實的，且隨後將控制傳遞至UEFI SMM。在一實施例中，此韌體可經簽名且加密驗證(cryptoverified)，諸如在安全啓動中所進行的。類似地，來自例如啓動ROM中之隔離儲存器的EK可經存取且提供至SMM。繼而，SMM將金鑰及/或任何衍生物儲存於諸如系統管理隨機存取記憶體(SMRAM)的記憶體之受保護部分中。

[0016]此記憶體可在再啓動後經重設(例如，經由歸零)，且進一步可與主機存取隔離。以此方式，每一啓動將金鑰資料自啓動ROM及其相關聯金鑰儲存體供應至SMM TEE中。在其他實施例中，金鑰儲存體可位於SoC之另一部分中，諸如SoC之現場可規劃保險絲中。請注意，在各種實施例中，金鑰儲存體及其構成金鑰可在例如處理器製造商或原始設備製造商(OEM)製造商之製造商管理機構下的工廠中供應。在一些實施例中，諸如用於DRM用法的額外金鑰(例如，Google Widevine金鑰盒)可在製造處或由使用者或資訊技術(IT)人員現場供應。

[0017]除TPM之外，SMM韌體驅動器可暴露一或多個Intel® SGX指令以進入SMM模式中且提供軟體PAVP或安全輸入/輸出(IO)能力。例如，在此模式中，SoC可確保僅SMM TEE可藉由在作業系統(OS)重設時使SMM碼禁用用於此圖形裝置之裝置ID來與周邊裝置(例如，PCI裝置)之圖形處理器通訊，使得裝置僅對於SMM TEE爲可見的，且因

此主機/OS不知道此可信賴視訊路徑。在一實施例中，SMM範圍暫存器(例如，一或多個SMRR)可保護韌體之至少某些部分且提供隔絕執行。在一實施例中，SMM埠陷阱允許主機通訊至SMM驅動器以進入/退出SMM模式。總之，經由此供應及I/O陷阱機構，多個基於TEE的應用程式——諸如TPM、DRM黑盒及仿真或軟體SGX——可實行於低電力、低功能性處理器或其他SoC上。

[0018]現參考圖1，展示根據本發明之一實施例之處理器的方塊圖。如圖1中所見，處理器100爲SoC，該SoC包括單個核心110。在本文所描述之各種實施例中，核心110可爲低電力及相對簡單的處理器核心，諸如循序處理器。作爲一此實例，核心110可爲Intel® Quark™處理器核心。此處理器在一實施例中爲單執行緒核心，該單執行緒核心經組配來執行諸如Pentium®相容ISA的舊式指令集架構之指令因而，可利用於較先進處理器(諸如基於Intel® Core™架構的處理器)上的某些指令(例如，如可利用於Intel® SGX環境中的先進向量指令或先進安全性指令)本質上不可利用於核心110中之執行。

[0019]仍參考圖1，核心110耦接至主機橋接器115，該主機橋接器可爲至SoC之各種組件的介面。如所見，主機橋接器115耦接至晶粒上啓動唯讀記憶體(ROM)120，該晶粒上啓動唯讀記憶體在一實施例中可儲存碼及金鑰資料，如本文所描述。主機橋接器115進一步耦接至快取記憶體130，該快取記憶體在一實施例中可爲嵌入靜態隨機存取記

憶體(eSRAM)。主機橋接器115進一步耦接至記憶體控制器140，該記憶體控制器經組配來與晶片外記憶體介接，該晶片外記憶體諸如給定系統記憶體，例如，DRAM。請注意，此DRAM可包括受保護或安全部分，諸如用於如本文所描述之安全操作之SMRAM。

[0020]另外，主機橋接器115耦接至至晶片外裝置的各種介面。此類介面包括舊式橋接器150，至各種晶片外組件之介面可自該舊式橋接器發生。作爲實例，此類晶片外組件可包括外部ROM及平台管理控制器，以及其他晶片外裝置。另外，主機橋接器115進一步耦接至組構160，該組構在一實施例中可爲先進微控制器匯流排架構(AMBA)組構，該先進微控制器匯流排架構組構經組配來諸如經由I2C介面、USB介面及乙太網路介面等介接至額外晶片外組件。另外，主機橋接器115進一步耦接至PCIe介面170，該PCIe介面繼而與一或多個晶片外PCIe裝置介接。應理解，雖然在圖1之實施例中以此等有限組件展示，但本發明之範疇在此方面不受限制且許多替代方案及變化係可能的。

[0021]現參考圖2，展示根據本發明之一實施例之方法的流程圖。如圖2中所示，方法200之部分可在包括TEE能力的系統之重設時以及在系統之正常操作期間進行，以進行將在TEE內執行的一或多個可信賴操作。

[0022]如所見，方法200在重設向量時於預啓動環境202中開始(方塊210)，該重設向量可爲回應於包括SoC的系統之重設的硬連線(hardwired)重定向，以引導至韌體儲存器

中之預定位置，該韌體儲存器在本文中亦被稱爲啓動ROM。接著，在方塊215處，此ROM執行可開始。預啓動可根據信賴根自此硬編碼進入點開始。儘管各種操作可在開始ROM執行時執行，但是出於本文所描述之實施例之目的，一此操作包括認可金鑰對(EK)之產生。在一實施例中，可關於不對稱密碼演算法(Rivest Shamir Adleman; RSA)公用/私用金鑰對產生此金鑰對。此金鑰對可儲存於諸如啓動ROM之受保護金鑰儲存體的給定安全位置中。在一實施例中，此金鑰對可在系統之製造期間產生，且隨後製造商可產生EK證書，該EK證書隨後被公佈。

[0023]仍參考圖2，接著控制傳遞至方塊220，在該方塊處可運行各種預啓動碼。儘管本發明之範疇在提供UEFI碼的系統中在此方面不受限制，但是此預啓動碼可包括安全性部分、預執行初始化碼及驅動器執行環境碼(分別爲SEC、PEI及DXE)。

[0024]控制接著傳遞至方塊225，在該方塊處可建立系統記憶體之受保護部分。在一實施例中，系統記憶體之此受保護部分爲SMRAM。此SMRAM可爲系統記憶體之一分割部分，當處理器處於操作之SMM模式中時僅允許對該分割部分之存取。作爲一此實例，存取控制硬體可例如經由一組記憶體範圍暫存器及存取控制邏輯來保護系統記憶體之此部分，以證實在允許對受保護範圍之存取之前處理器有效地處於SMM中。

[0025]在建立系統記憶體之此受保護部分時，控制傳遞

至方塊230，在該方塊處TEE驅動器可經建立。在一實施例中，此類驅動器可包括一或多個TEE DXE驅動器。另外，可執行交握協定以自啓動ROM獲得先前產生之金鑰對且將此類金鑰儲存於系統記憶體之受保護部分(例如，SMRAM)中。在一實施例中，可設定IN_SMM信號以引發交握來將金鑰傳遞至SMRAM中，其中該等金鑰可對SMM外的系統隱藏，該系統包括OS及在系統上執行的任何惡意程式。

[0026]在此刻，TEE已經建立，且預啓動操作完成。因此，控制傳遞至啓動或OS環境252，在該啓動或OS環境中，OS經啓動(方塊240)。在系統於此環境中之正常操作期間，當接收請求動作時，可判定動作是否爲在非SMM期間接收的可信賴動作(亦即對可信賴動作之請求)(菱形250)。在各種實施例中，請注意，輸入及輸出可經由在TEE內執行的驅動器信賴。此可信賴動作請求之實例可爲對韌體TPM操作之OS請求，該OS請求可觸發用於將要進入的SMM之SMI。作爲另一實例，全域平台API可觸發對可信賴動作之請求，諸如OTP或金融交易。

[0027]若動作爲可信賴動作，則控制傳遞至菱形255以判定用於對應動作之命令是否由可利用的可信賴執行環境支援，該可利用的可信賴執行環境在一實施例中爲DXE SMM TEE。若不支援命令，則控制傳遞至方塊265，在該方塊處執行錯關機。在一實施例中，錯關機包括向使用者指示執行可信賴操作的未授權試圖。在另一實施例中，LED指示器可閃爍以指示該試圖。或平台可簡單地省略操作之

執行，且在錯誤預OS UEFI呼叫程式之狀況下返回至諸如「EFI_SECURITY_VIOLATION」的適當返回碼。

[0028]另外，若支援命令，則控制傳遞至方塊260，在該方塊處命令可在TEE中執行。爲進入TEE中，設定SMM引發信號，例如，IN_SMM信號，以開始所請求可信賴操作在SMM中之執行。請注意，所要操作可採取許多不同形式之可信賴操作。可信賴操作之結果可經置放至OS可存取的諸如RAM的未保護記憶體中。當此執行完成時，控制傳遞至方塊290，在該方塊處，在TEE終止之後，例如，SMM經由回復(RSM)指令之退出發生，繼續平台執行可發生。

[0029]仍參考圖2，若替代地在菱形250處判定所請求動作並非可信賴動作，則控制傳遞至菱形270，在該菱形處，判定是否請求不信賴UEFI動作。若如此，則控制傳遞至方塊275，在該方塊處，可在用於不信賴UEFI動作之執行的監督器模式(例如，環0)中進行操作，該不信賴UEFI動作可使用DXE碼及/或ACPI碼來進行。若所請求動作並非不信賴UEFI動作，則控制替代地傳遞至方塊280，以用於習知無特權OS核心/應用程式處理。儘管在圖2之實施例中以此高階展示，但是本發明之範疇不限於此佈置。

[0030]如以上所論述，根據一實施例之用於TEE之一示例性使用狀況爲用於處置受保護數位內容，例如，具有DRM管理保護。假定使用者希望經由諸如Netflix™的內容遞送服務下載或串流且觀看電影或其他視訊內容。在此狀況下，在系統中經由網路連接接收加密數位內容。請注意，

實際接收係經由未加密通道，然而內容自身經加密。爲允許內容之解密，進入TEE，且在進行譯碼操作中使用安全金鑰。更具體而言，所儲存EK金鑰對可充當金鑰階層根，以便產生受保護儲存根金鑰(SRK)，該受保護儲存根金鑰在安全儲存器中保全，且該受保護儲存根金鑰在TEE中經存取以用於衍生及存取諸如內容解密金鑰的其他金鑰。換言之，EK金鑰對可用於其他金鑰之管理，該等其他金鑰諸如用於內容加密/解密之金鑰。

[0031]爲此，假定使用者先前已執行交換處理以獲得一組金鑰以用於與Netflix™服務一起使用。更具體而言，經由安全儲存器之EK金鑰，一組內容解密金鑰可自身經加密且維持於非安全儲存器中，該非安全儲存器諸如系統之給定非依電性儲存器，例如，系統之未保護快閃記憶體。

[0032]隨後，當加密內容在系統處於TEE中時經接收時，可使用受保護EK金鑰獲得且解開來自未保護儲存器的此等所儲存金鑰。隨後，可使用此等解密金鑰對內容進行解密操作。在內容經解密之後，該內容可經由安全通道發送至目的地，例如，經由安全路徑(例如，經由Intel® PAVP技術)耦接至處理器的區域顯示器，其中此安全路徑不可由諸如在系統中操作的不信賴OS或惡意程式的不信賴源監聽。在一實施例中，安全或可信賴的通道可經由SMM中之專屬控制台驅動器實現，以提供可信賴硬體路徑，該可信賴硬體路徑直接與目的地裝置通訊，且不使用OS顯示器或其他驅動器。以類似方式，使用者或其他輸入在處於TEE

中時亦可經由可信賴輸入路徑，因爲輸入裝置驅動器可在TEE中之SMM內執行，且因此避免惡意程式或不信賴OS輸入驅動器。因此，可以高保證在系統中接收且處理安全內容。

[0033]現參考圖3，展示在一實施例中用於處置受保護數位內容的佈置的方塊圖。如圖3中所示，系統300包括SoC 310，該SoC耦接至記憶體350，該記憶體在一實施例中爲包括安全部分(例如，SMRAM)352及未保護部分354的系統記憶體。另外，SoC 310耦接至顯示裝置360，該顯示裝置可爲觸控螢幕顯示器或系統之其他顯示器。

[0034]回應於SMI之接收，SoC 310進入TEE 320中。出於本文論述之目的，在於TEE 320內之執行期間，解密邏輯330操作來解密輸入加密內容，該輸入加密內容可爲可經由未加密通道接收的任何類型之受保護數位內容，諸如安全視訊、音訊或其他受保護資訊。爲允許解密邏輯330解密加密內容，通訊在解密邏輯330與記憶體350之間發生，且更具體而言對安全部分352發生以獲得SRK 353且對未保護部分354發生以獲得加密金鑰對355。在一實施例中，加密金鑰對355爲與內容提供者相關聯的先前儲存之金鑰對。爲加密/解密儲存於未保護記憶體中的此金鑰對，可使用SRK 353。更具體而言，SRK 353可爲EK金鑰對，例如，在系統之初始化期間供應至SMRAM中(如自啓動ROM獲得)。使用SRK 353之金鑰，加密金鑰對355可經解密，且解密金鑰可在解密邏輯330中用於解密以輸出解密內容。

[0035]如圖3中進一步所例示，TEE 320進一步包括顯示驅動器340，該顯示驅動器爲在系統上執行的OS或惡意程式可存取的可信賴及安全驅動器。因而，在TEE 320與顯示裝置360之間提供可信賴路徑。解密內容可經儲存至顯示裝置之訊框緩衝器370中，該訊框緩衝器隨後將解密內容輸出至顯示器。應理解，雖然在圖3之例示中以此高階展示，但是本發明之範疇在此方面不受限制，且許多變化及替代方案係可能的。

[0036]另一使用狀況可爲在受保護記憶體(例如，SMRAM)不足以用於在TEE中之可信賴操作期間保存指令及/或資料之目的的狀況下用於加密頁面於記憶體中之儲存。亦即，在許多系統中，SMRAM限於例如8百萬位元組(MB)。在一些狀況下，SMM處置器其他安全碼可消耗多於此8 MB限制，且因此，可在SMRAM與未保護記憶體之間調換碼及/或資料。在此狀況下，當使加密頁面進入SMRAM中時，資訊可首先經解密，該解密使用衍生自儲存根金鑰的金鑰。且類似地，當資訊將自受保護儲存器發送回時，在儲存於未保護記憶體中之前，衍生金鑰可再次用來加密資訊。

[0037]現參考圖4，展示根據本發明之一實施例之系統佈置的方塊圖。如圖4中所示，系統400可爲嵌入裝置或隨身裝置，且因而在所示實例中可爲不具有顯示器的無頭系統。CPU 410可爲SoC或具有如本文所描述之單個低電力核心的其他處理器，且經組配來在SMM中執行以提供可信賴

執行環境，以用於如本文所描述之安全操作。在不同實施例中，在TEE中可執行各種安全操作，包括Intel® SGX技術、Intel® TXT技術或ARM TrustZone之仿真。

[0038]如進一步所見，記憶體系統之各種部分耦接至CPU 410，該等各種部分包括系統記憶體415(例如，由動態隨機存取記憶體(DRAM)形成)及非依電性儲存器435，該非依電性儲存器可爲系統之主要大容量儲存器且可例如對應於固態驅動機。請注意，系統記憶體415可包括SMRAM以儲存如本文所描述之EK(及衍生物)。

[0039]在圖4之實施例中，額外組件可存在，包括耦接至CPU 410的感測器/通訊集線器440。集線器440可爲獨立集線器或組配於CPU 440內。如所見，一或多個感測器442可處於與集線器440通訊狀態中。出於使用者鑑定及裝置/情境證實之目的，此類感測器可包括生物特徵量測輸入感測器、一或多個擷取裝置及全球定位系統(GPS)模組或其他專屬位置感測器。諸如慣性及環境感測器的其他感測器亦可存在。作爲若干實例，可提供加速計及力偵測器，且自此等感測器獲得的資訊可用於生物特徵量測鑒定中。另外，在各種實施例中，一或多個無線通訊模組445可存在，以允許根據3G或4G/LTE通訊協定的與諸如給定蜂巢式系統的區域或廣域無線網路的通訊。

[0040]請注意，實施例不限於無頭系統，且可同樣地可適用於提供用於其他裝置中之安全操作之可信賴環境。現參考圖5，展示另一示例性系統的方塊圖，實施例可與該另

一示例性系統一起使用。如所見，系統500可爲智慧型電話或其他無線通訊器。基帶處理器505經組配來關於將要自系統傳輸或由系統接收的通訊信號進行各種信號處理。繼而，除諸如許多熟知的社交媒體及多媒體應用的使用者應用程式之外，基帶處理器505耦接至應用處理器510，該應用處理器可爲用以執行OS及其他系統軟體的系統之主CPU。應用處理器510可進一步經組配來進入SMM以進行用於裝置之安全操作，如本文所描述。

[0041]繼而，應用處理器510可耦接至使用者介面/顯示器520，例如，觸控螢幕顯示器。另外，應用處理器510可耦接至記憶體系統，該記憶體系統包括非依電性記憶體，亦即快閃記憶體530及系統記憶體，亦即DRAM 535。在一些實施例中，DRAM 535可包括安全部分532，諸如EK及衍生金鑰的秘密可儲存於該安全部分中。如進一步所見，應用處理器510亦耦接至諸如一或多個影像擷取裝置的擷取裝置545，該擷取裝置可記錄視訊及/或靜態影像。多個感測器525可耦接至應用處理器510以允許諸如加速計及其他環境資訊的各種感測資訊之輸入。

[0042]如進一步所例示，提供近場通訊(NFC)無觸點介面560，該近場通訊無觸點介面經由NFC天線565在NFC近場中通訊。雖然在圖5中展示分開的天線，但是應理解，在一些實行方案中可提供一天線或天線之不同集合以允許各種無線功能性。

[0043]電力管理積體電路(PMIC)515耦接至應用處理器

510以進行平台級電力管理。爲此，PMIC 515可將電力管理請求發佈至應用處理器510以根據需要進入某些低電力狀態。此外，基於平台約束，PMIC 515可亦控制系統500之其他組件之電力位準。

[0044]爲允許通訊被傳輸且接收，各種電路可耦接在基帶處理器505與天線590之間。具體而言，射頻(RF)收發機570及無線區域網路(WLAN)收發機575可存在。一般而言，RF收發機570可用來根據諸如3G或4G無線通訊協定的給定無線通訊協定接收且傳輸無線資料及呼叫，諸如根據碼分多址(CDMA)、全球行動通訊系統(GSM)、長期演進(LTE)或其他協定接收且傳輸。另外，GPS感測器580可存在，並且位置資訊經提供至安全性處理器550以用於如本文所描述之使用。亦可提供諸如無線電信號之接收或傳輸的其他無線通訊，該等無線電信號例如AM/FM及其他信號。另外，經由WLAN收發機575，亦可實現諸如根據Bluetooth™或IEEE 802.11標準的區域無線通訊。

[0045]現參考圖6，展示另一示例性系統的方塊圖，實施例可與該另一示例性實施例一起使用。在圖6之例示中，系統600可爲行動低電力系統，諸如平板電腦、2:1數位板、fablet或其他可轉換或獨立平板系統。如所例示，SoC 610存在且可經組配來作爲用於裝置之應用處理器操作，且進入SMM中以進行如本文所描述之安全操作。

[0046]各種裝置可耦接至SoC 610。在所示之例示中，記憶體子系統包括耦接至SoC 610的快閃記憶體640及

DRAM 645。爲此，SoC 610可包括整合記憶體控制器以處置與DRAM 645的通訊，且建立並保護此記憶體(例如，SMRAM)內之安全部分，如本文所描述。另外，觸摸面板620耦接至SoC 610以提供顯示能力及經由觸摸的使用者輸入，包括觸摸面板620之顯示器上的虛擬鍵盤之供應。爲提供有線網路連接性，SoC 610耦接至乙太網路介面630。周邊集線器625耦接至SoC 610以允許與各種周邊裝置介接，諸如可藉由各種埠中之任何埠或其他連接器耦接至系統600。

[0047]除SoC 610內之內部電力管理電路及功能性之外，電力管理積體電路(PMIC)680耦接至SoC 610以例如基於系統係由電池690或經由AC配接器695的AC電力供電來提供基於平台的電力管理。除此基於電源的電力管理之外，PMIC 680可進一步基於環境及用法條件來進行平台電力管理活動。更進一步，PMIC 680可將控制及狀態資訊通訊至SoC 610以引起SoC 610內之各種電力管理動作。

[0048]仍參考圖6，爲提供無線能力，WLAN單元650耦接至SoC 610且繼而耦接至天線655。在各種實行方案中，WLAN單元650可根據一或多個無線協定提供通訊，該一或多個無線協定包括IEEE 802.11協定、Bluetooth™協定或任何其他無線協定。

[0049]如進一步所例示，多個感測器660可耦接至SoC 610。此等感測器可包括各種加速計、環境及其他感測器，包括使用者手勢感測器。最後，音訊編解碼器665耦接至SoC

610以提供至音訊輸出裝置670的介面。當然，應理解，雖然在圖6中以此特定實行方案展示，但許多變化及替代方案係可能的。

[0050]以下實例係關於進一步實施例。

[0051]在實例1中，一種SoC包含：單個核心，其用以執行舊式指令集，其中該單個核心經組配來進入SMM以提供TEE來執行至少一安全操作；以及記憶體控制器，其耦接至該單個核心，該記憶體控制器用以與系統記憶體介接，其中該系統記憶體之一部分包含用於SMM之安全記憶體，且該單個核心用以鑑定啓動韌體，執行該啓動韌體，且將控制傳遞至SMM以自受保護儲存器獲得金鑰對且將金鑰對儲存於安全記憶體中。

[0052]在實例2中，單個核心用以在SMM中操作以自受保護儲存器獲得金鑰對，該受保護儲存器包含非依電性儲存器，該非依電性儲存器包括隔離金鑰儲存體以儲存金鑰對，其中該金鑰對將在包括該SoC之系統之製造期間經產生且儲存於非依電性儲存器中。

[0053]在實例3中，安全記憶體選擇性地將在SoC之重設時經重設，使得刪除金鑰對，該安全記憶體將與SMM外的存取隔離。

[0054]在實例4中，以上實例中之任何實例之SoC在TEE中將仿真由單個核心未支援的指令集之至少一安全性指令。

[0055]在實例5中，以上實例中之任何實例之SoC在TEE

中將接收加密內容，使用一或多個儲存於耦接至SoC的未保護儲存器中的一或多個衍生金鑰來解密加密內容，且經由可信賴通道將解密內容輸出至輸出裝置。

[0056]在實例6中，以上實例中之任何實例之SoC在TEE中將加密儲存於安全記憶體中的資訊之頁面且將加密頁面儲存於系統記憶體之未保護部分中。

[0057]在實例7中，單個核心包含SoC之唯一核心，該SoC進一步包含啓動ROM以將金鑰對儲存於該啓動ROM之一受保護部分中。

[0058]在實例8中，以上實例中之任何實例之單個核心用以在金鑰對經儲存於安全記憶體中之後將執行自SMM傳遞至將要啓動的作業系統。

[0059]請注意，以上SoC可使用各種構件來實行。

[0060]在一實例中，SoC可併入使用者設備觸摸允用裝置中。

[0061]在另一實例中，系統包含顯示器及記憶體，且包括以實例中之一或多個實例之SoC。

[0062]在實例9中，至少一電腦可讀媒體包括指令，該等指令在執行時引起系統進行以下操作：在處理器之單個核心中執行預啓動環境之韌體之至少一部分以創建系統記憶體之可信賴部分；以及將執行轉移至與該可信賴部分相關聯的可信賴代理，自非依電性儲存器之受保護部分請求金鑰對，將該金鑰對儲存於該系統記憶體之該可信賴部分中，且此後將執行自該可信賴代理轉移至作業系統。

[0063]在實例10中，實例9之至少一電腦可讀媒體選擇性地進一步包含指令，該等指令在執行時允許系統自非可信賴代理接收可信賴動作請求，且若該可信賴動作請求由可信賴代理支援，則經由可信賴代理進入可信賴執行環境以執行安全操作，該安全操作對應於可信賴執行環境中之可信賴動作請求。

[0064]在實例11中，實例9之至少一電腦可讀媒體選擇性地進一步包含指令，該等指令在執行時允許系統在處於可信賴執行環境中時回應於由單個核心執行的IN_SMM指令而自非依電性記憶體之受保護部分請求金鑰對。

[0065]在實例12中，實例9之至少一電腦可讀媒體選擇性地進一步包含指令，該等指令在執行時允許系統在處於可信賴執行環境中時仿真由單個核心不支援的指令集之至少一安全性指令。

[0066]在實例13中，實例9之至少一電腦可讀媒體選擇性地進一步包含指令，該等指令在執行時允許系統接收加密內容，使用儲存於系統記憶體中的一或多個衍生金鑰來解密加密內容，且經由可信賴通道將解密內容輸出至輸出裝置。

[0067]在實例14中，實例9之至少一電腦可讀媒體選擇性地進一步包含指令，該等指令在執行時允許系統加密儲存於系統記憶體之可信賴部分中的資訊之頁面且將加密頁面儲存於系統記憶體之未保護部分中。

[0068]在實例15中，一種系統包含：處理器，其具有單

個核心以執行舊式指令集，其中該單個核心經組配來進入SMM以實例化TEE，該單個核心進一步具有安全儲存器及記憶體控制器以與記憶體介接，其中該記憶體包含用於SMM之安全部分，且其中該單個核心用以鑑定啓動韌體，執行啓動韌體，且將控制傳遞至SMM以自安全儲存器獲得認可金鑰且將認可金鑰儲存於記憶體之安全部分中；顯示裝置，其耦接至該處理器，該顯示裝置包括訊框緩衝器以儲存將要顯示在顯示裝置上的處理後資料；以及記憶體，其耦接至處理器，該記憶體包括用以儲存認可金鑰的安全部分及用以儲存一或多個解密金鑰的未保護部分，其中在TEE中，該處理器用以接收加密內容，使用一或多個解密金鑰來解密加密內容，且將解密內容輸出至顯示裝置。

[0069]在實例16中，顯示裝置經由可信賴通道耦接至處理器，其中該處理器用以在TEE中執行顯示驅動器以將處理後資料傳遞至顯示裝置以用於儲存於訊框緩衝器中。

[0070]在實例17中，認可金鑰包含儲存根金鑰，該處理器用以在儲存於記憶體之未保護部分中之前使用儲存根金鑰來加密一或多個解密金鑰。

[0071]在實例18中，安全儲存器包含晶片上ROM以儲存啓動韌體之至少一部分。

[0072]在實例19中，安全儲存器包含處理器之一組可規劃保險絲。

[0073]在實例20中，在TEE中，處理器用以加密儲存於記憶體之安全部分中的資訊之頁面且將加密頁面儲存於記

憶體之未保護部分中。

[0074]在實例21中，一種方法包含：在處理器之單個核心中執行預啓動環境之韌體之至少一部分以創建系統記憶體之可信賴部分；以及將執行轉移至與該可信賴部分相關聯的可信賴代理，自非依電性儲存器之受保護部分請求金鑰對，將該金鑰對儲存於該系統記憶體之該可信賴部分中，且此後將執行自該可信賴代理轉移至作業系統。

[0075]在實例22中，實例21之方法進一步包含自非可信賴代理接收可信賴動作請求，及若可信賴動作請求由可信賴代理支援，則經由可信賴代理進入可信賴執行環境以執行安全操作，該安全操作對應於可信賴執行環境中之可信賴動作請求。

[0076]在實例23中，實例21之方法進一步包含在處於可信賴執行環境中時回應於由單個核心執行的IN_SMM指令而自非依電性記憶體之受保護部分請求金鑰對。

[0077]在實例24中，實例21之方法進一步包含在處於可信賴執行環境中時仿真由單個核心不支援的指令集之至少一安全性指令。

[0078]在實例25中，實例21之方法進一步包含接收加密內容，使用儲存於系統記憶體中的一或多個衍生金鑰來解密加密內容，及經由可信賴通道將解密內容輸出至輸出裝置。

[0079]在實例26中，實例21之方法進一步包含加密儲存於系統記憶體之可信賴部分中的資訊之頁面及將加密頁面

儲存於系統記憶體之未保護部分中。

[0080]在實例27中，一種設備包含用以執行以上實例中任一實例之方法的構件。

[0081]在實例28中，機器可讀儲存媒體包括機器可讀指令，該等機器可讀指令在執行時用以實行以上實例中之任何實例之方法。

[0082]在實例29中，一種系統包含：執行構件，其用於在處理器之單個核心中執行預啓動環境之韌體之至少一部分以創建系統記憶體之可信賴部分；轉移構件，其用於將執行轉移至與可信賴部分相關聯的可信賴代理；請求構件，其用於自非依電性儲存器之受保護部分請求金鑰對；儲存構件，其用於將金鑰對儲存於系統記憶體之可信賴部分中；以及轉移構件，其用於將執行自可信賴代理轉移至作業系統。

[0083]在實例30中，實例29之系統進一步包含用於自非可信賴代理接收可信賴動作請求的構件，且若可信賴動作請求由可信賴代理支援，則用於經由可信賴代理進入可信賴執行環境以執行安全操作的構件，該安全操作對應於可信賴執行環境中之可信賴動作請求。

[0084]在實例31中，實例29之系統進一步包含請求構件，其用於在處於可信賴執行環境中時回應於由單個核心執行的IN_SMM指令而自非依電性記憶體之受保護部分請求金鑰對。

[0085]在實例32中，實例29之系統進一步包含：接收構

件，其用於接收加密內容；解密構件，其用於使用儲存於系統記憶體中的一或多個衍生金鑰來解密加密內容；以及輸出構件，其用於經由可信賴通道將解密內容輸出至輸出裝置。

[0086]應理解，以上實例之各種組合係可能的。

[0087]實施例可用於許多不同類型之系統中。例如，在一實施例中，通訊裝置可經佈置來執行本文所描述之各種方法及技術。當然，本發明之範疇不限於通訊裝置，且替代地其他實施例可針對用於處理指令之其他類型之設備或包括指令的一或多個機器可讀媒體，該等指令回應於在計算裝置上執行而引起該裝置實行本文所描述之方法及技術中之一或多者。

[0088]實施例可以碼來實行，且可儲存在非暫時儲存媒體上，該非暫時媒體上儲存有指令，該等指令可用以程式設計系統以執行指令。儲存媒體可包括但不限於：任何類型之碟片，包括軟碟片、光碟片、固態驅動機(SSD)、光碟唯讀記憶體(CD-ROM)、可重寫光碟(CD-RW)及磁光碟；半導體元件，諸如唯讀記憶體(ROM)、隨機存取記憶體(RAM)，諸如動態隨機存取記憶體(DRAM)、靜態隨機存取記憶體(SRAM)、可抹除可規劃唯讀記憶體(EPROM)、快閃記憶體、電氣可抹除可規劃唯讀記憶體(EEPROM)；磁卡或光卡，或適合於儲存電子指令之任何其他類型之媒體。

[0089]雖然已就有限數目之實施例描述本發明，但是熟習此項技術者將瞭解基於該等實施例之許多修改及變化。

隨附申請專利範圍意欲涵蓋如屬於本發明之真實精神及範疇內之所有此等修改及變化。

【符號說明】

100...處理器

110...核心

115...主機橋接器

120...晶粒上啓動唯讀記憶體(ROM)

130...快取記憶體

140...記憶體控制器

150...舊式橋接器

200...方法

202...預啓動環境

210～240、260、265、275～290...方塊

250、255、270...菱形

252...啓動或OS環境

300、400、500...系統

310...SoC

320...TEE

330...解密邏輯

340...顯示驅動器

350...記憶體

352、532...安全部分

353...SRK

354...未保護部分

355...加密金鑰對

360...顯示裝置

370...訊框緩衝器

410...CPU

415...系統記憶體

435...非依電性儲存器

440...感測器/通訊集線器/集線器

442、525、660...感測器

445...無線通訊模組

505...基帶處理器

510...應用處理器

515、680...電力管理積體電路(PMIC)

520...使用者介面/顯示器

530、640...快閃記憶體

535、645...DRAM

545...擷取裝置

560...近場通訊(NFC)無觸點介面

565...NFC天線

570...射頻(RF)收發機

575...無線區域網路(WLAN)收發機

580...GPS感測器

590、655...天線

610...SoC

620...觸摸面板

625...周邊集線器

630...乙太網路介面

650...WLAN單元

690...電池

695...AC配接器

665...音訊編解碼器

670...音訊輸出裝置

申請專利範圍

1. 一種系統單晶片(SoC)，其包含：

一單個核心，其用以執行一舊式指令集，其中該單個核心經組配來進入一系統管理模式(SMM)以提供一可信賴執行環境(TEE)來進行至少一安全操作；以及

一記憶體控制器，其耦接至該單個核心，該記憶體控制器用以與一系統記憶體介接，其中該系統記憶體之一部分包含用於該SMM之一安全記憶體，且其中該單個核心係用以鑑定一啓動韌體，用以執行該啓動韌體且用以將控制傳遞至該SMM以自一受保護儲存器獲得一金鑰對，且用以將該金鑰對儲存於該安全記憶體中。

2. 如請求項1之SoC，其中該單個核心係用以在該SMM中操作以自該受保護儲存器獲得該金鑰對，該受保護儲存器包含一非依電性儲存器，該非依電性儲存器包括一隔離金鑰儲存體以儲存該金鑰對，其中該金鑰對將在包括該SoC的一系統之製造期間被產生且儲存於該非依電性儲存器中。

3. 如請求項2之SoC，其中該安全記憶體將在該SoC之重設時被重設，使得刪除該金鑰對，該安全記憶體將隔離於在該SMM之外的存取。

4. 如請求項１之SoC，其中在該TEE中，該單個核心用於仿真該單個核心不支援的一指令集之至少一安全性指令。

5. 如請求項1之SoC，其中在該TEE中，該單個核心用以接收加密內容，使用儲存於耦接至該SoC的一未保護儲存器中的一或多個衍生金鑰來解密該加密內容，且經由一可信賴通道將該解密內容輸出至一輸出裝置。
6. 如請求項1之SoC，其中在該TEE中，該單個核心用以加密儲存於該安全記憶體中的資訊之一頁面且將該加密頁面儲存於該系統記憶體之一未保護部分中。
7. 如請求項1之SoC，其中該單個核心包含該SoC之唯一核心，該SoC進一步包含一啓動唯讀記憶體(ROM)以將該金鑰對儲存於該啓動ROM之一受保護部分中。
8. 如請求項1之SoC，其中該單個核心用以在該金鑰對經儲存於該安全記憶體中之後，將執行自該SMM傳遞至將要啓動的一作業系統。
9. 一種電腦可讀媒體，其包括指令，該等指令在執行時引起一系統進行以下動作：

   在一處理器之一單個核心中執行一預啓動環境之一韌體之至少一部分，以創建一系統記憶體之一可信賴部分；以及

   將執行轉移至與該可信賴部分相關聯的一可信賴代理，自一非依電性儲存器之一受保護部分請求一金鑰對，將該金鑰對儲存於該系統記憶體之該可信賴部分中，且此後將執行從該可信賴代理轉移至一作業系統。
10. 如請求項9之電腦可讀媒體，其進一步包含指令，該等指令在執行時允許該系統自一非可信賴代理接收一可

信賴動作請求，且若該可信賴動作請求由該可信賴代理支援，則經由該可信賴代理進入一可信賴執行環境以執行一安全操作，該安全操作對應於該可信賴執行環境中之該可信賴動作請求。

11. 如請求項9之電腦可讀媒體，其進一步包含指令，該等指令在執行時允許該系統在處於一可信賴執行環境中時，回應於由該單個核心執行的一IN_SMM指令，而自該非依電性記憶體之該受保護部分請求該金鑰對。

12. 如請求項9之電腦可讀媒體，其進一步包含指令，該等指令在執行時允許該系統在處於該可信賴執行環境中時，仿真由該單個核心不支援的一指令集之至少一安全性指令。

13. 如請求項9之電腦可讀媒體，其進一步包含指令，該等指令在執行時允許該系統接收加密內容，使用儲存於該系統記憶體中的一或多個衍生金鑰來解密該加密內容，且經由一可信賴通道將該解密內容輸出至一輸出裝置。

14. 如請求項9之電腦可讀媒體，其進一步包含指令，該等指令在執行時允許該系統加密儲存於該系統記憶體之該可信賴部分中的資訊之一頁面，且將該加密頁面儲存於該系統記憶體之一未保護部分中。

15. 一種系統，其包含：

一處理器，其具有一單個核心以執行一舊式指令集，其中該單個核心經組配來進入一系統管理模式

(SMM)以實例化一可信賴執行環境(TEE)，該單個核心進一步具有一安全儲存器及一記憶體控制器以與一記憶體介接，其中該記憶體包含用於該SMM之一安全部分，且其中該單個核心用以鑑定一啓動韌體，執行該啓動韌體，且將控制傳遞至該SMM以自該安全儲存器獲得一認可金鑰且將該認可金鑰儲存於該記憶體之該安全部分中；

一顯示裝置，其耦接至該處理器，該顯示裝置包括一訊框緩衝器以儲存將要顯示在該顯示裝置上的處理後資料；以及

該記憶體，其耦接至該處理器，該記憶體包括用以儲存該認可金鑰的該安全部分及用以儲存一或多個解密金鑰的一未保護部分，其中在該TEE中，該處理器用以接收加密內容，使用該一或多個解密金鑰來解密該加密內容，且將該解密內容輸出至該顯示裝置。

16. 如請求項15之系統，其中該顯示裝置經由一可信賴通道耦接至該處理器，其中該處理器用以在該TEE中執行一顯示驅動器以將該處理後資料傳遞至該顯示裝置以用於儲存於該訊框緩衝器中。

17. 如請求項15之系統，其中該認可金鑰包含一儲存根金鑰，該處理器用以在儲存於該記憶體之該未保護部分中之前，使用該儲存根金鑰來加密該一或多個解密金鑰。

18. 如請求項16之系統，其中該安全儲存器包含一晶片上唯讀記憶體(ROM)，該晶片上ROM進一步用以儲存該啓動

韌體之至少一部分。

19. 如請求項16之系統，其中該安全儲存器包含該處理器之一組可規劃保險絲。

20. 如請求項16之系統，其中在該TEE中，該處理器用以加密儲存於該記憶體之該安全部分中的資訊之一頁面且將該加密頁面儲存於該記憶體之該未保護部分中。

圖式

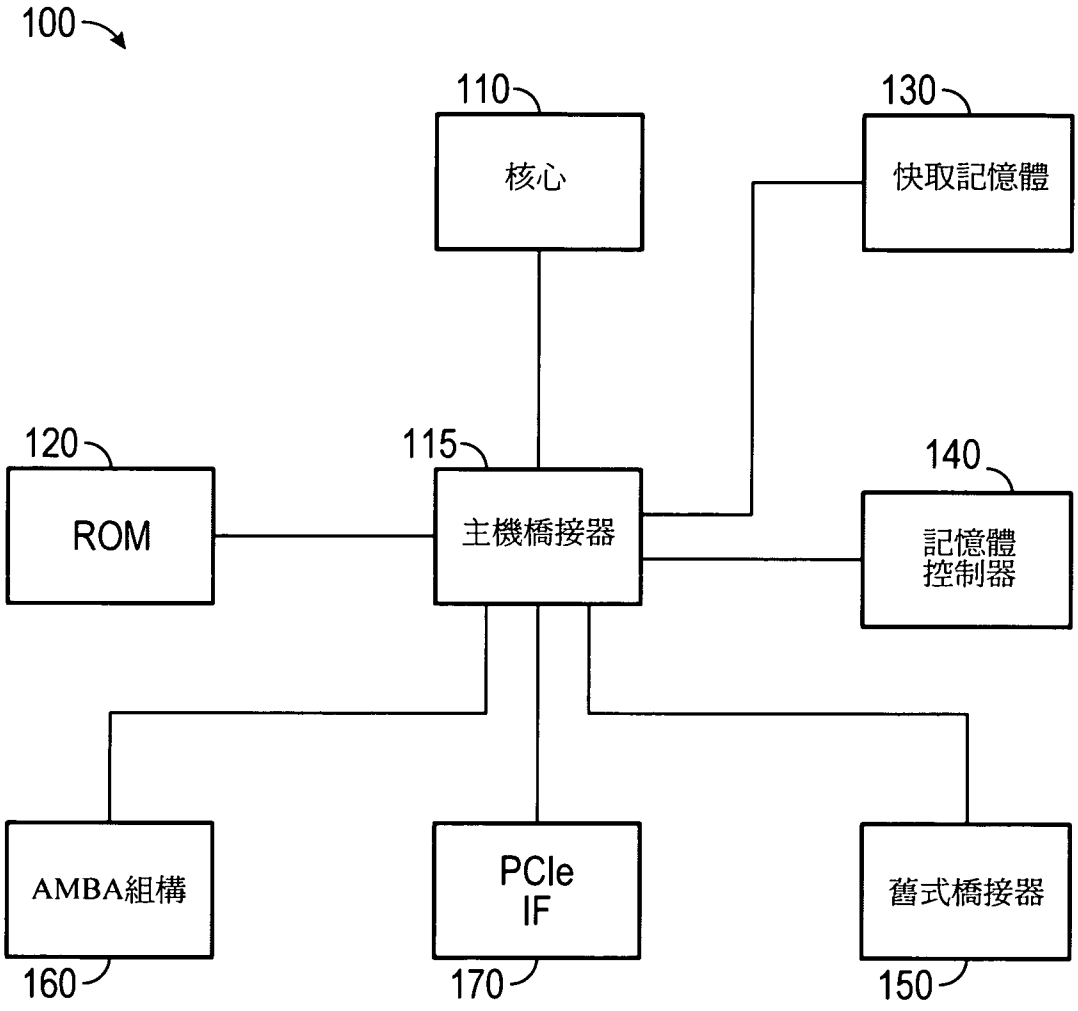
100
110
核心
130
快取記憶體
120
ROM
115
主機橋接器
140
記憶體
控制器
AMBA組構
160
PCIe
IF
170
舊式橋接器
150

圖 1

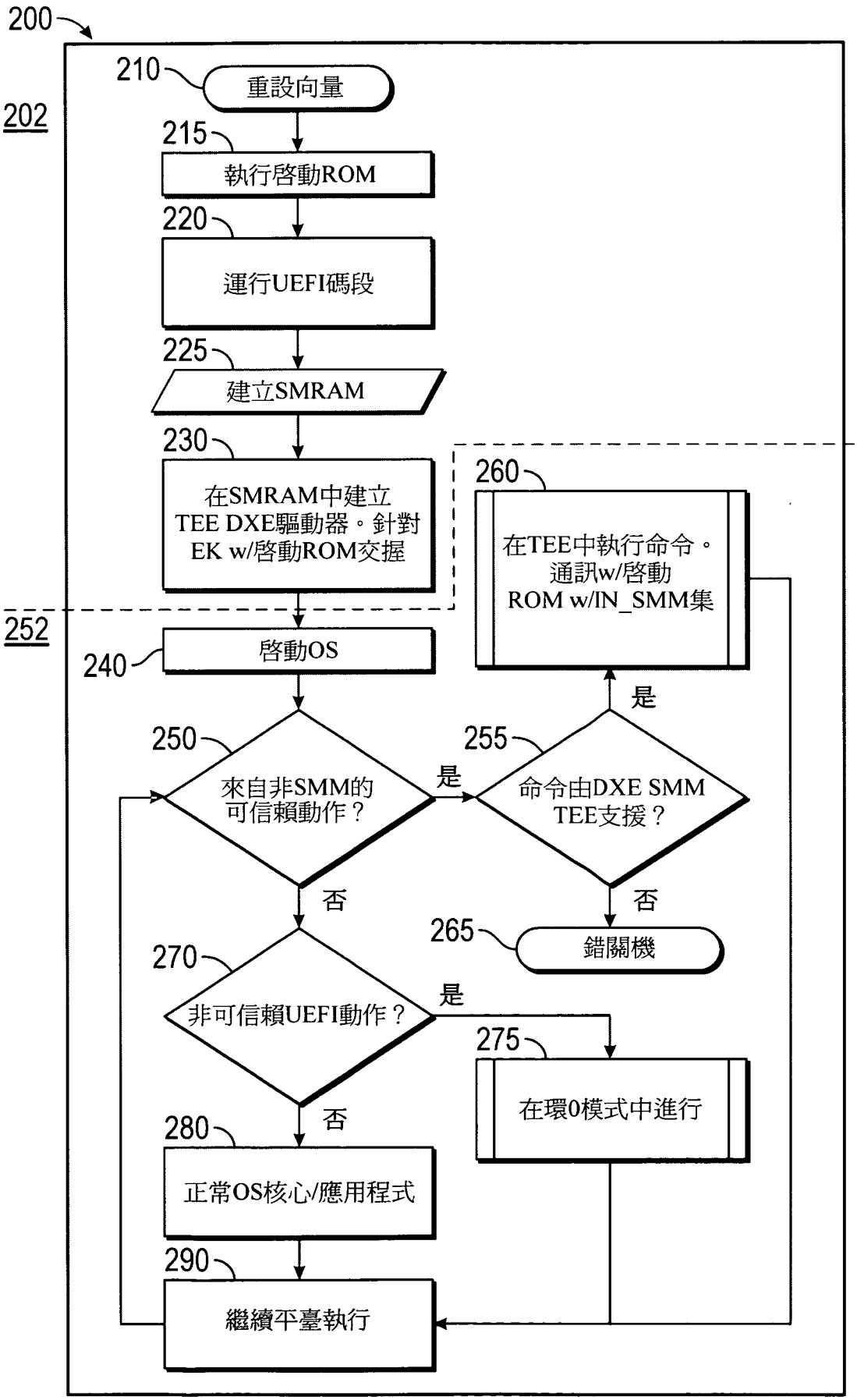
200
202
210
重設向量
215
執行啓動ROM
220
運行UEFI碼段
225
建立SMRAM
230
在SMRAM中建立
TEE DXE驅動器。針對
EK w/啓動ROM交握
252
240
啓動OS
250
來自非SMM的
可信賴動作？
是
否
255
命令由DXE SMM
TEE支援？
是
否
260
在TEE中執行命令。
通訊w/啓動
ROM w/IN_SMM集
265
錯關機
270
非可信賴UEFI動作？
是
否
275
在環0模式中進行
280
正常OS核心/應用程式
290
繼續平臺執行

圖 2

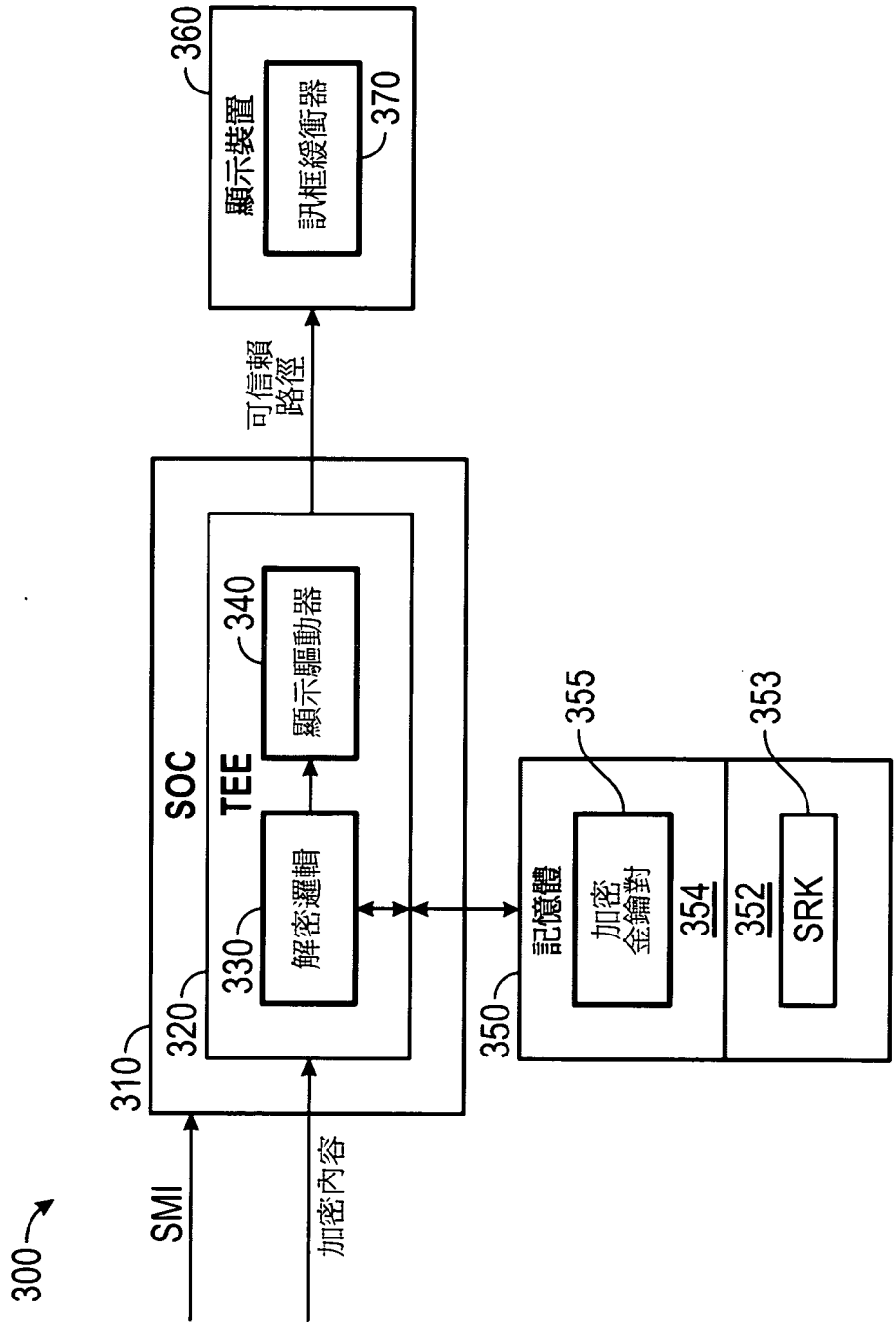
300
SMI
加密內容
310
SOC
320
TEE
330
解密邏輯
340
顯示驅動器
可信賴路徑
360
顯示裝置
370
訊框緩衝器
350
記憶體
355
加密金鑰對
354
353
352
SRK

圖 3

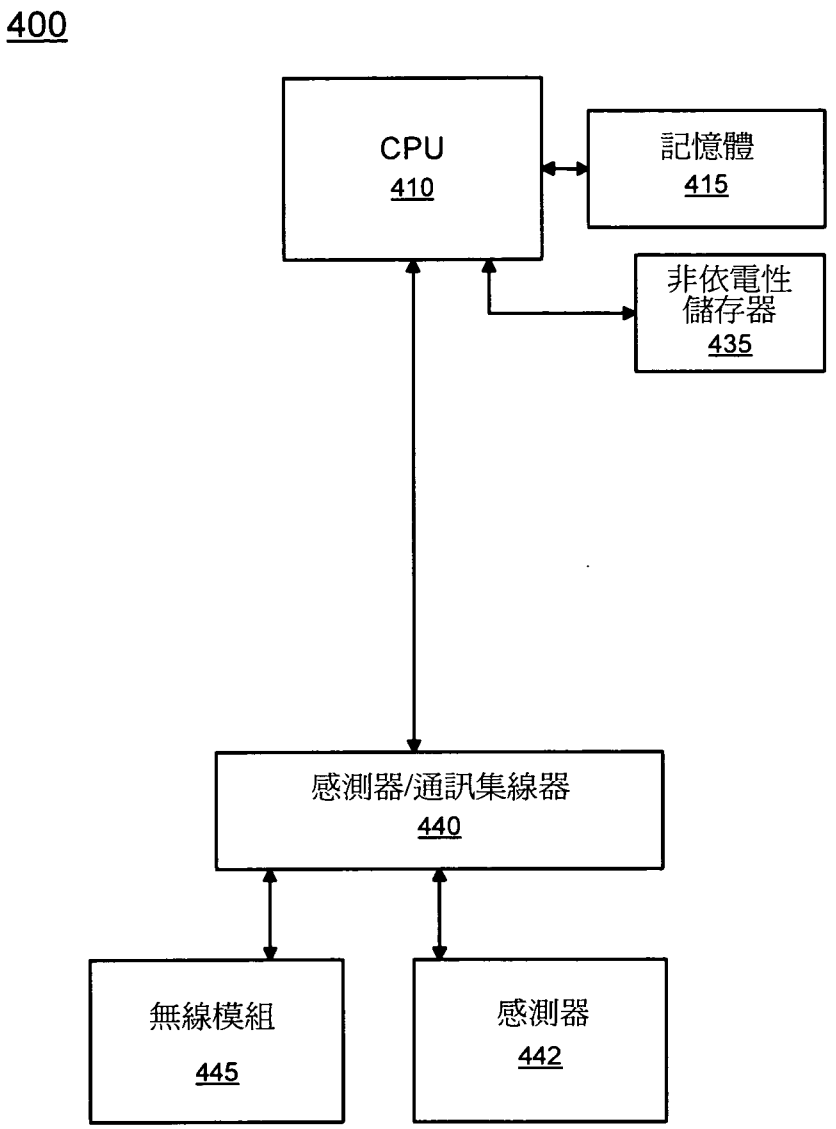

圖 4

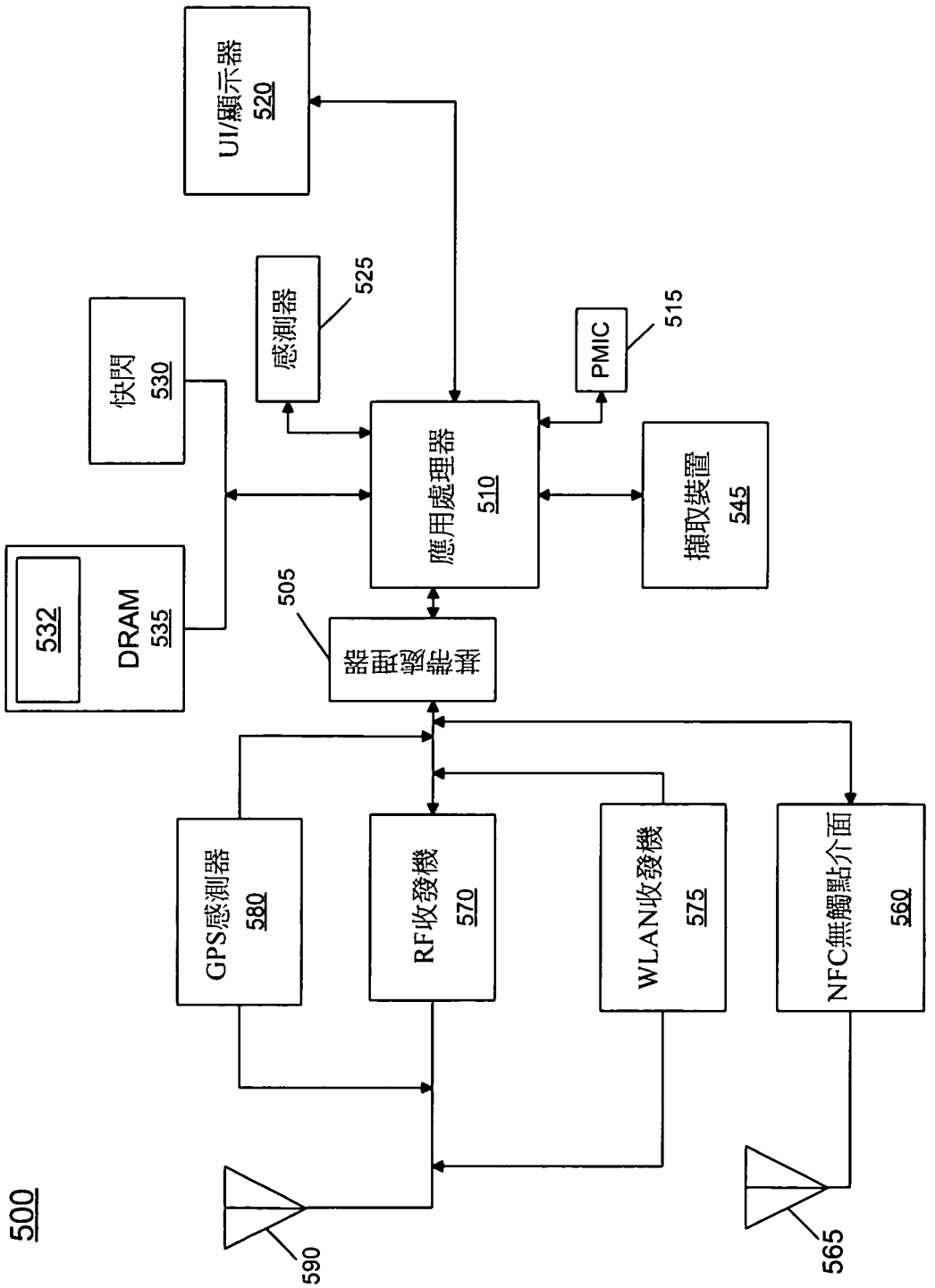
500
UI/顯示器 520
感測器 525
快閃 530
PMIC 515
應用處理器 510
擷取裝置 545
532
DRAM 535
505
GPS感測器 580
RF收發機 570
WLAN收發機 575
NFC無觸點介面 560
590
565

圖 5

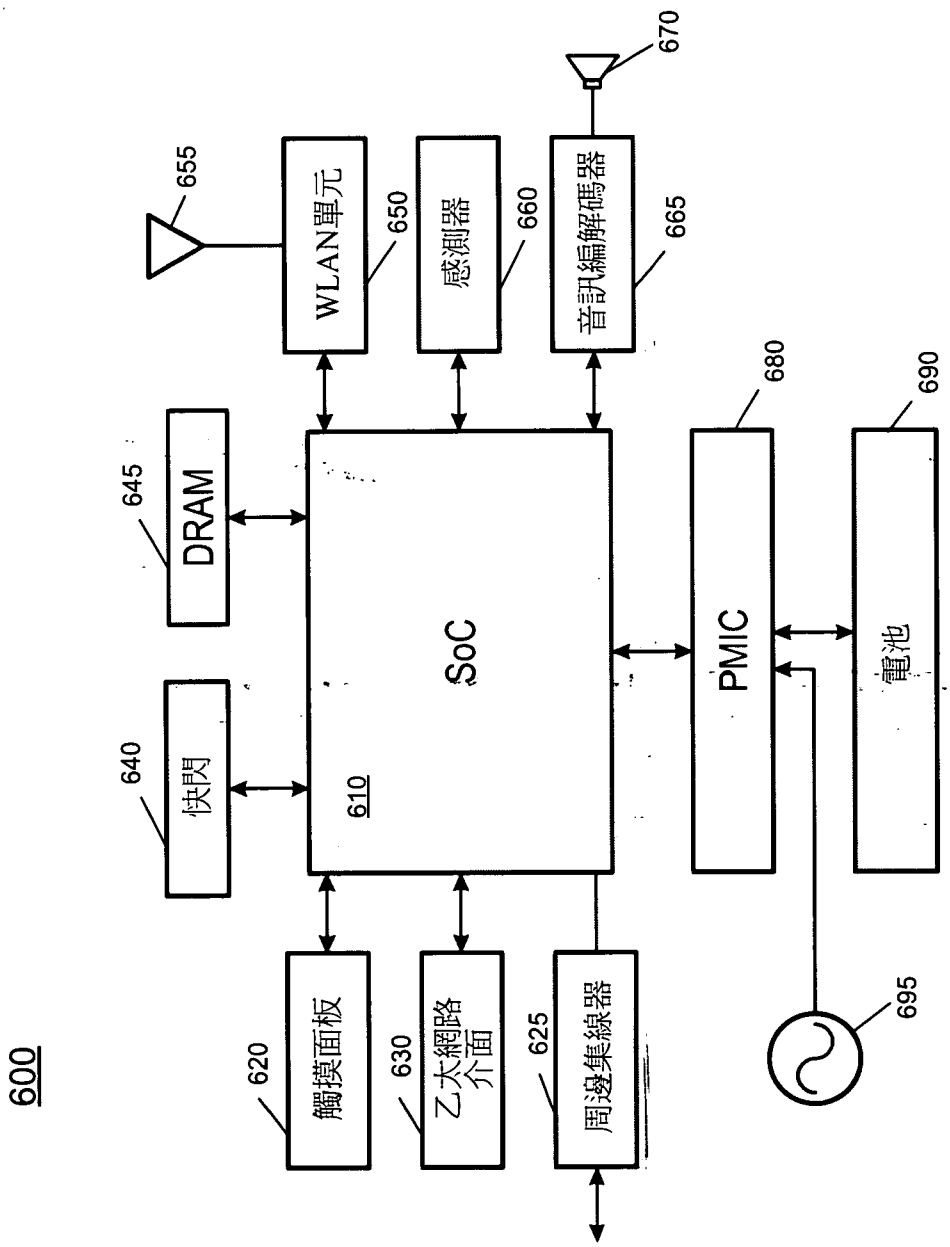
600
610
SoC
DRAM
645
快閃
640
WLAN單元
650
655
感測器
660
音訊編解碼器
665
670
PMIC
680
電池
690
695
觸摸面板
620
乙太網路介面
630
周邊集線器
625

圖 6