I493951

(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 I493951 B**

(45)公告日： 中華民國 104 (2015) 年 07 月 21 日

(21)申請案號：101142871 (22)申請日： 中華民國 101 (2012) 年 11 月 16 日

(51)Int. Cl.： ***H04L9/08 (2006.01)*** ***H04L9/16 (2006.01)***

(30)優先權：2011/12/21 世界智慧財產權組織 PCT/US11/66665

(71)申請人：英特爾股份有限公司 (美國) INTEL CORPORATION (US)
美國

(72)發明人：葛洛伯曼 史蒂芬 GROBMAN, STEVEN L. (US)；布蘭特 傑森 BRANDT, JASON W. (US)

(74)代理人：林志剛

(56)參考文獻：

TW	201121279A	TW	201140369A
US	2008/0205651A1	US	2009/0052659A1
US	2009/0220071A1		

審查人員：蔡鴻璟

申請專利範圍項數：20 項 圖式數：7 共 37 頁

(54)名稱

保護對稱加密鑰的系統及方法

SYSTEMS AND METHODS FOR PROTECTING SYMMETRIC ENCRYPTION KEYS

(57)摘要

說明當執行加密時用於保護對稱加密鑰的系統及方法。在一實施例中，電腦實施方法包含：從安全區取出至少一真實鑰，以及，以處理器執行鑰轉換指令，以根據接收至少一真實鑰來產生至少一轉換鑰。至少一轉換鑰是使用至少一真實鑰由處理器加密的至少一循環鑰的加密版本。處理器能夠將至少一轉換鑰解密及將至少一循環鑰加密。

Systems and methods for protecting symmetric encryption keys when performing encryption are described. In one embodiment, a computer-implemented method includes retrieving at least one real key from a secure area and executing, with a processor, a key transform instruction to generate at least one transformed key based on receiving the at least one real key. The at least one transformed key is an encrypted version of at least one round key that is encrypted by the processor using the at least one real key. The processor is able to decrypt the at least one transformed key and encrypt the at least one round key.

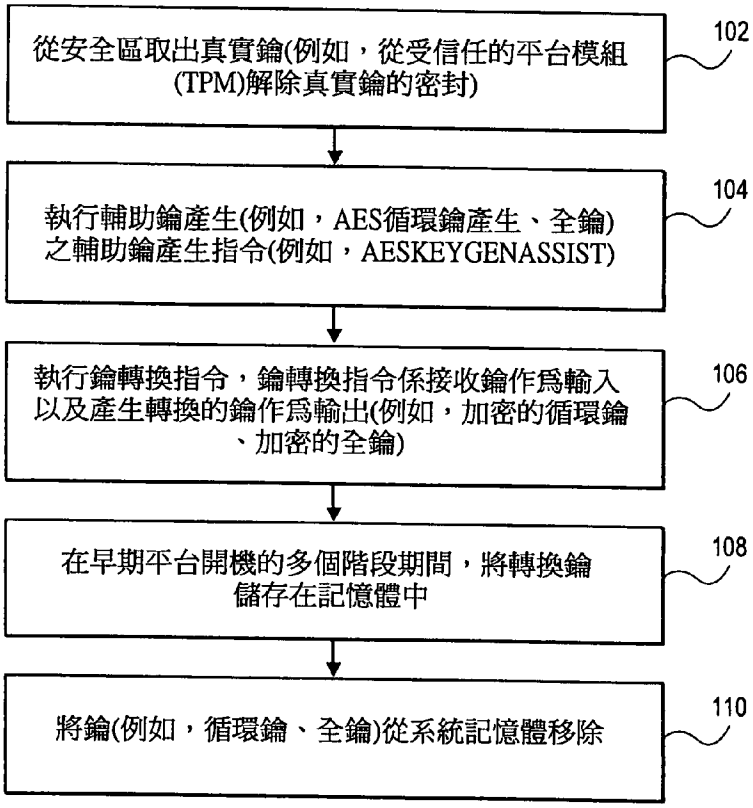
從安全區取出真實鑰(例如，從受信任的平台模組(TPM)解除真實鑰的密封)
102
執行輔助鑰產生(例如，AES循環鑰產生、全鑰)之輔助鑰產生指令(例如，AESKEYGENASSIST)
104
執行鑰轉換指令，鑰轉換指令係接收鑰作爲輸入以及產生轉換的鑰作爲輸出(例如，加密的循環鑰、加密的全鑰)
106
在早期平台開機的多個階段期間，將轉換鑰儲存在記憶體中
108
將鑰(例如，循環鑰、全鑰)從系統記憶體移除
110

圖1

公告本

發明專利說明書

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101142871

※申請日：101 年 11 月 16 日　　※IPC 分類：　H04L 9/08 (2006.01)

H04L 9/16 (2006.01)

一、發明名稱：（中文／英文）

保護對稱加密鑰的系統及方法

Systems and methods for protecting symmetric encryption keys

二、中文發明摘要：

說明當執行加密時用於保護對稱加密鑰的系統及方法。在一實施例中，電腦實施方法包含：從安全區取出至少一真實鑰，以及，以處理器執行鑰轉換指令，以根據接收至少一真實鑰來產生至少一轉換鑰。至少一轉換鑰是使用至少一真實鑰由處理器加密的至少一循環鑰的加密版本。處理器能夠將至少一轉換鑰解密及將至少一循環鑰加密。

三、英文發明摘要：

Systems and methods for protecting symmetric encryption keys when performing encryption are described. In one embodiment, a computer-implemented method includes retrieving at least one real key from a secure area and executing, with a processor, a key transform instruction to generate at least one transformed key based on receiving the at least one real key. The at least one transformed key is an encrypted version of at least one round key that is encrypted by the processor using the at least one real key. The processor is able to decrypt the at least one transformed key and encrypt the at least one round key.

四、指定代表圖：

（一）本案指定代表圖為：第（1）圖。

（二）本代表圖之元件符號簡單說明：無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

六、發明說明：

【發明所屬之技術領域】

本發明的實施例關於當執行主機爲基礎的加密時保護對稱加密鑰。

【先前技術】

先進的加密標準（AES）加密已成爲用於對稱加密的產業標準且用於範圍廣大的資料保護應用及情境。有三個主要機制以在包含同類軟體、硬體加速器、及利用特殊指令（例如，具有新指令的 AES 指令集（AES-NI））的軟體之平台上實施 AES 加密。這些實施方法具有各式各樣的安全、性能、及功率蘊含。功率及性能特徵將隨著工作負載特徵而變。在硬體加速器或 IP 區中執行密碼實施的一優點是在下面的 AES 鑰未曝露至 IP 實施的邊界之外部。在包含根據 AES-NI 的實施之軟體實施上，在下面的加密鑰受到較大的曝露以及大致上依靠作業系統保護以及完整性，以防衛鑰受到軟體及硬體的攻擊。

【發明內容及實施方式】

說明當執行主機爲基礎的加密時保護對稱加密鑰的系統及方法。在一實施例中，電腦實施的方法包含從安全區取出至少一真實鑰，以及，以處理器執行鑰轉換指令以根據接收至少一真實鑰而產生至少一轉換鑰。至少一轉換鑰是由處理器使用至少一真實鑰加密之至少一循環鑰的加密

版本。處理器能夠將至少一轉換鑰解密以及將至少一循環鑰加密。資料被加密發生在爲了主機爲基礎的加密而產生它的瞬間。

在下述說明中，揭示例如邏輯實施、訊號及匯流排的大小和名稱、系統組件的型式及相互關係、以及邏輯分割/整合選擇等眾多具體細節，以提供更完整的瞭解。但是，習於此技藝者將瞭解，不用這些具體細節，仍可實施本發明的實施例。在其它情形中，未顯示控制結構及閘等級電路，以免模糊本發明的實施例。根據所述的說明，不用過度的實驗，具有此技藝的一般技術者將能夠實施適當的邏輯電路。

在下述說明中，使用某些術語以說明本發明的實施例的特點。舉例而言，「邏輯」代表配置成執行一或更多功能的硬體及/或軟體。舉例而言，「硬體」的實例包含但不限於積體電路、有限狀態機或甚至是組合邏輯。積體電路可以採取例如微處理器、特定應用積體電路、數位訊號處理器、微控制器、等等處理器的形式。在晶片之間的互連均是點對點或是均爲多點連接配置，或者某些是點對點而其它是多點連接配置。

本發明的實施例減輕偷取下面的鑰之很多硬體及軟體攻擊情形。對稱鑰保護設計提出對稱鑰保護的增強。舉例而言，設計包含 AES-NI 實施的增強，使得 AES-NI 能夠被用於 AES 演算法有效率實施，並具有下面的鑰不會曝露在記憶體中的附加優點，因而在使用 AES-NI 取代專用的

硬體加密加速器時，減輕使用 AES-NI 時的某些風險。應注意，提出的 AES-NI 增強是本設計舉例說明的實施，且其對實施對稱的密碼化操作（或是例如循環等密碼化操作）之任何指令集，將具有類似的能力。

當存在有軟體脆弱性時，爲了減輕鑰材料的損失，本設計包含一方法，其使用被傳送給 AESNI 指令的 AES 循環鑰的加密形式，以取代真實的循環鑰。使用對話鑰或是對各 CPU（或系統單晶片（SOC））的獨特鑰，由 CPU 將這些循環鑰加密，對話鑰是在電力初始化時隨機導出的，獨特鑰是經由根據熔斷之導出鑰而被內部地導出及持續。也可以使用保險絲、暫存器傳遞語言（RTL）中的隱藏鑰、及可能的實體非複製功能之組合，導出用於各 CPU／SOC 的導出鑰。

於下說明兩個可能的實施且未防止一或二技術實施於平台上。

圖 1 顯示根據本發明的一實施例之當執行主機爲基礎的加密時保護對稱加密鑰之電腦實施的方法 100 的一實施例之流程圖。以處理邏輯執行方法 100，處理邏輯包括硬體（電路、專用邏輯、等等）、軟體（例如在一般用途的電腦系統或專用機或裝置上執行）、或二者的組合。在一實施例中，藉由與此處所述的主機爲基礎的平台相關的處理邏輯，執行方法 100。

在區塊 102，處理邏輯從安全區取出真實鑰（例如，從受信任的平台模組（TPM）解除真實鑰的密封）。在區

塊 104，處理邏輯執行輔助鑰產生（例如，AES 循環鑰產生、全鑰）之輔助鑰產生指令（例如，AESKEYGENASSIST）。在區塊 106，處理邏輯執行鑰轉換指令，接收鑰作爲輸入以及產生轉換的鑰作爲輸出（例如，加密的循環鑰、加密的全鑰）。在區塊 108，在早期平台開機的多個階段期間，轉換鑰儲存在記憶體中。轉換鑰僅對於目前的開機循環及平台有效。在區塊 110，將鑰（例如，循環鑰、全鑰）從系統記憶體移除。

當主機平台從重設開機時，碼路徑的數目增加且累積作業系統、裝置驅動器、及其它含有潛在的目前或未來脆弱性之大量碼的碼基礎。因此，系統對於開發是易受傷的機率以 T 的函數增加，其中，T 等於被執行的軟體碼的量以及與重設後的時間量相關連。假使關鍵鑰被轉換成僅可以爲了此特定開機而用於平台 CPU 核心上的形式時，則轉換鑰的遺失不會透露未經轉換的鑰，且假使由攻擊者偷走時，被偷走的轉換鑰在下一次再開機之後是無用的。這僅適用於假使使用隨機號碼來加密這些鑰以取代製造時隨機產生且被熔斷或永久地配置於 CPU 中的鑰，此鑰對於每一次開機是相同的。

圖 2 是方塊圖，顯示根據一實施例之產生轉換的鑰之機制。此機制包含在區塊 202 將真實鑰從 TPM 解除密封，執行輔助鑰產生指令（例如，AESKEYGENASSIST），輔助 AES 鑰產生（例如，AES 循環鑰產生），以及，導入新指令（例如，KEYTRANSFORM），新指令將區塊 206

的真實循環鑰（例如，真實循環鑰 1、2 等等）作爲輸入以及將鑰的加密版本（例如，TransRound key 1，TransRound key 2、等等）儲存於記憶體位置 208。用以進行加密的真實鑰僅 CPU 可取得且是不可取出的。這使得加密鑰能在早期開機的多個階段期間被置於記憶體中，早期開機的多個階段包含開機載入器執行或 OS 開機處理的早期階段。加密鑰僅對於目前的開機循環及平台有效。在另一實施例中，以單一鑰用於加密，以及在一些循環之後，CPU 自動地建立循環鑰及儲存它們。

假定真實鑰密封在 IP 中，且例如經由密封至平台的受信任平台模組（TPM）上平台配置的暫存器，IP 將在開機處理的這些早期階段期間僅釋放它們。除了硬體假隨機數產生器之外，TPM 還供應用於密碼化鑰的安全產生之設施。其也包含例如遠端證明及密封儲存等能力。在一實施例中，由於循環鑰是固定的 128 位元鑰且與 AES 鑰尺寸及模式要求相獨立，所以，循環鑰被轉換以取代全原地 AES 鑰。在實施例中，全鑰由新指令轉換。一旦鑰轉換指令執行以儲存鑰的加密形式於記憶體中，則應從系統記憶體中抹除真實循環鑰。雖然「keytransform」指令一般最常用在 CPL0，但是，其可以在任何特權等級操作。

加密循環鑰可以儲存在內部表中。指令設計成更容易查詢內部表中的加密循環鑰（例如，具有傳進來的循環數以及使用循環數以查詢表）。

在實施例中，CPU 具有有限的儲存以用於加密鑰且軟

體指定其希望使用的鑰的索引。索引的一優點是由於沒有快取（亦即，在表中選中或是其未作用），所以，設計包含內部性能最佳化機制，例如，假使請求解密的指令的線性位址符合之前登入的位址，則僅允許解密的循環鑰的查詢。在此情形中，循環指令將讀取「將我的循環鑰 X 儲存於表的登錄 3 中」。

產生替代實施，其中，內部加密鑰持續在 CPU 中。這具有鑰能由任何應用限制於平台且不需要依靠早期開機碼的優點。當應用初始安裝時，應用將產生用於平台的轉換鑰，然後，將不再需要真實鑰。此方式保護鑰不被用於另一平台上，但未防止被偷的轉換鑰不被流氓替代惡意軟體堆疊使用。

圖 3 顯示根據一實施例之以對稱加密鑰用於加密之電腦實施的方法 300 的一實施例之流程圖。方法 300 由處理邏輯執行，處理邏輯包括硬體（電路、專用邏輯、CPU、等等）、軟體（例如在一般用途電腦系統或是專用機或裝置上執行）、或二者的組合。在一實施例中，方法 300 由 CPU 執行。

在一實施例中，爲了使用轉換循環鑰，將實施四個 AES-NI 指令（例如，AESENC、AESENCLAST、AESDEC、及 AESDELAST）的新變異。新指令可稱爲 AESENCTR、AESENCLASTTR、AESDECTR、及 AESDELASTTR。這些變異接受轉換的循環鑰以取代原地循環鑰除外，這些變異中的各變異與它們目前的實施都相同地操作。舉例而言

，在區塊 302 的處理邏輯，以變異（AESENCTR [xmm1、xmm2/m12]），根據來自[xmm2/m12]的轉換的循環鑰，對[xmm1]執行一循環的 AES 加密。內部地，在區塊 304，處理邏輯（例如，CPU）將轉換的循環鑰解密至原地循環鑰，然後，在區塊 306，執行其目前的實施（例如，AESENC）。

當使用 AES 以將資料區塊加密或解密時，其將對每 16 位元組區塊迭代循環鑰。用於整個區塊的循環鑰集合在整個加密或解密操作中維持不變。此特性能夠造成映射的積極內部快取，映射是將轉換的循環鑰映射至其對應的真實循環鑰。轉換的循環鑰的解密僅需於快取遺失時發生。舉例而言，假定設計需要對 4K 區塊的資料執行要求 14 個循環鑰的 AES-256 加密操作。在實施例中，循環鑰轉換快取容納所有 14 個鑰且一次僅有一個使用轉換範例 AES 操作正在執行。基本上，一般的 AES-NI 加密對 AESENC 要求 256*14=3484 次呼叫（例如，4K/16B=256 及對 256 位元 AES 有 14 循環）。相對地，假使微架構實施使用 AESDEC 以在快取遺失時將循環鑰解密，則對 AESDEC 將增加 140 次呼叫。以要求 10 循環之 AES-128，將各 128 位元循環鑰加密，以致於對於全部 3724 次 AESENC/AESDEC 呼叫爲 14*10＝140，約爲受處理的第一區塊上的負擔的 7%（加上轉換快取查詢負擔）。應注意，在資料集中所有後續的 4K 區塊將不會引起快取遺失且將返回至初始的 3484 呼叫。因此，負擔僅包含轉換鑰快取查詢。

在另一實施例中，使用表或其它結構以取代快取。CPU 要儲存從其開始時使用的隨機數/保險絲產生的循環鑰，但不儲存真正的隨機數/保險絲。當軟體指定的循環鑰需要加密或解密時，具有那些硬體爲基礎的循環鑰顯著地加速。假使硬體爲基礎的循環鑰未存在時，則不需要原始的隨機數或保險絲。萬一有人能夠擾亂隨機數時，可以與其它事物（例如，CPU 上的隱藏值或保險絲）相結合。以類似的方式，保險絲可以與其它事物相結合。

目前，對稱爲的加密發生在鑰受保護的加速器（或是 IP 區塊）中。在較佳地適合某些工作負擔的目前的軟體方式中，在此處所述的攻擊中不存在鑰保護特性。

在加密或解密演算法的目前的軟體或 AES-NI 實施中，作業系統或應用中的安全脆弱性使得攻擊者能夠偷取加密鑰及清除文字資料。即使在如下所述的事件期間加密資料被偷取或妥協，在提供鑰的增強保護上仍然有實質的值。當開發是未知時，此增強的保護使脆弱性的蘊含最小化。在作業系統中未經確認的脆弱性之挑戰之一是不管是否發生開發，其並非總是清楚的。當組織確認脆弱性存在時，則採取修正動作，例如展開軟體補綴以在開發時防止脆弱性。與未知的開發相關連的一議題是組織不一定知道那些平台（假使有任何平台）是開發由惡意攻擊者使用。作業系統脆弱性提供目前的軟體實施中儲存對稱鑰之記憶體的存取，以及提供使用解密實施以存取資料的能力。因此，組織將需要改變受衝擊的所有平台上的加密鑰，以

及，假使組織要確保攻擊者無法使用已被偷取的鑰時，將存在有脆弱性的每一裝置上的所有資料再加密。假使鑰被偷取時，則鑰不僅在脆弱性時存在的資料存取時有用，也在由相同的鑰加密之未來的資料的存取時有用。假使以僅有解密實施是在脆弱性期間是脆弱，但是鑰受保護的方式，實施加密能力時，則系統被補綴，而不用撤銷鑰且不需將所有目前的資料再加密。當共同軟體應用至例如 PC 客戶端、電話、平板電腦、及消費性電子裝置等大套裝置時，由於 OS 脆弱性將衝擊非常大量的使用者及在下面的對稱鑰的保護將大幅地降低使平台返回至已知的安全狀態之成本及努力，所以，這會是重大的優點。

由於解密能被移至另一平台或軟體堆疊，所以，在提供增強的鑰保護上，有實質的值。取得鑰使得攻擊者能夠在妥協的系統的外部之二次實施中實施解密且不受限於使用妥協的實施作爲監督或強制資料從被加密轉換至明文之唯一手段。舉例而言，考慮古典的「冷開機」攻擊。在此情境中，一旦鑰被取得時，攻擊者能將機器重開機至 OS 及存取/解密平台上的任何資料。假使脆弱性是允許存取解密實施的軟體開發時，則攻擊者可以監督資料轉換但將需要強制攻擊者希望的資料經由妥協的實施而轉換。當有大量的資料時且不知道要被存取的有價值資料位於何處之很多情境中，這是不實際的。可以證明此點的一情境是當系統在開機後的時間點確認開發。在開發偷取鑰的系統中，有機會在未來的任何點追蹤資料。在僅有加密存取能

力妥協的情境中，資料遺失將限於能經由開發與開發偵測之間的妥協實施而傳送的資料量。

由於對稱鑰再鍵入及撤銷是昂貴且通常是不實際的，所以，在提供鑰的增強保護上，有實質的價值。AES 中使用的對稱鑰通常作爲最低等級的加密，以保護鑰正在保護的每一區塊資料之靜止（儲存中）及移動（被傳送）的資料。由於在存取已被加密的每一區塊資料時要求鑰，所以，因爲已被加密的每一區塊資料需要是可存取的以致於其可以由新的鑰材料再加密，所以，撤銷妥協鑰是有挑戰性的。這不僅在正受保護的系統上包含活躍的資料，也包含維持在例如備份或離線儲存器等其它媒體中的任何額外的備份。偷竊鑰將能夠攻擊曾經由鑰加密的所有資料，包含裝置上不再可以存取的資料。

本設計提供產生僅有平台的應用處理器能夠轉換成真實循環（真正）鑰之加密循環鑰（或真正鑰）之概念。本設計在主機爲基礎的軟體密碼機操作中提供加密的平台界限/電力開啓獨特鑰之使用、鑰密封機制（例如 TPM）與早期平台開機之間的互動以便當主機執行限定的碼來降低攻擊之受信任的區域及碼基礎時將鑰移入轉換狀態、以及有效率地快取轉換鑰以致於加密所有循環鑰時導入最小負擔之機制。

圖 4 是功能方塊圖，顯示根據一實施例實施的系統 900。所示的處理系統 900 的實施例包含一或更多處理器（或中央處理單元）、系統記憶體 910、非依電性（NV）

記憶體 915、資料儲存單元（DSU）920、通訊鏈結 925、及晶片組 930。所示的處理系統 900 代表包含桌上型電腦、筆記型電腦、工作站、手持電腦、伺服器、刀峰伺服器、等等任何計算系統。

處理系統 900 的元件如下所述地互連。處理器 905 經由晶片組 930 而通訊地耦合至系統記憶體 910、NV 記憶體 915、DSU 920、及通訊鏈結 925，以對它們傳送或接收指令或資料。在一實施例中，NV 記憶體 915 是快閃記憶體裝置。在其它實施例中，NV 記憶體 915 包含唯讀記憶體（ROM）、可編程 ROM、可抹拭可編程 ROM、電可抹拭可編程 ROM、等等其中任何一個。在一實施例中，系統記憶體 910 包含隨機存取記憶體（RAM），例如動態 RAM（DRAM）、同步 DRAM（SDRAM）、資料倍速 SDRAM（DDR SDRAM）、靜態 RAM（SRAM）、等等。DSU 920 代表用於軟體資料、應用、及/或作業系統之任何儲存裝置，但是，最典型的是非依電性儲存裝置。DSU 920 選加地包含一或更多整合的驅動電子（IDE）硬碟、增強的 IDE（EIDE）硬碟、獨立碟片冗餘陣列（RAID）、小電腦系統介面（SCSI）硬碟、等等。雖然 DSU 920 顯示爲處理系統 900 的內部，但是，DSU 920 可以是外部地耦合至處理系統 900。通訊鏈結 925 將處理系統 900 耦合至網路，以致於處理系統 900 在網路上與一或更多其它電腦通訊。通訊鏈結 925 包含數據機、乙太網路卡、十億位元乙太網路卡、通用串列匯流排（USB）埠、無線網路介

面卡、光纖介面、等等。

DSU 920包含機器可存取的媒體907，在媒體907上儲存具體實施此處所述的一或更多方法或功能之一或更多指令集（例如軟體）。軟體在其由處理器905執行期間也可以完全地或部份地位於處理器905之內，處理器905也構成機器可存取的儲存媒體。

雖然在舉例說明的實施例中機器可存取的媒體907顯示爲單一媒體，但是，「機器可存取的媒體」一詞應被視爲包含儲存一或更多指令集的單一媒體或多個媒體（例如，集中式或分散式資料庫、及/或相關連的快取記憶體和伺服器）。「機器可存取的媒體」一詞也將被視爲包含能夠儲存、編碼或載送用於由機器執行的指令集、以及促使機器執行本發明的實施例之任何一或更多方法之任何媒體。「機器可存取的媒體」一詞因而將被視爲包含但不限於固態記憶體、光學、及磁性媒體。

因此，機器可存取的媒體包含提供（亦即，儲存及/或傳送）可由機器（例如，電腦、網路裝置、個人數位助理、製造工具、設有一或更多處理器組的任何裝置、等等）存取的形式之資訊的任何機制。舉例而言，機器可存取的媒體包含可記錄/不可記錄媒體（例如，唯讀記憶體（ROM）；隨機存取記憶體（RAM）；磁碟儲存媒體；光學儲存媒體；快閃記憶體裝置；等等）、以及電方式、光學方式、聲學方式或其它形式的傳播訊號（例如，載波、紅外線訊號、數位訊號、等等）；等等。

如圖 4 所示，處理系統 900 的各副組件包含輸入/輸出（I/O）電路 950 以用於彼此通訊。I/O 電路 950 包含阻抗匹配電路，阻抗匹配電路可被調整以取得所需的輸入阻抗，藉以降低副組件之間的訊號反射及干擾。

應瞭解，爲了簡明起見，處理系統 900 的各式各樣的其它元件從圖 4 及本說明中排除。舉例而言，處理系統 900 又包含圖形卡、增加的 DSU、其它持續資料儲存裝置、等等。晶片組 930 也包含系統匯流排及例如記憶體控制器集線器及輸入/輸出（I/O）控制器集線器等各式各樣其它的資料匯流排以用於互連副組件，以及，包含資料匯流排（例如，週邊組件互連匯流排）以用於連接週邊裝置至晶片組 930。對應地，處理系統 900 可操作而不用所示的一或更多元件。舉例而言，處理系統 900 無需包含 DSU 920。

圖 5 顯示根據一實施例的系統 1300 的方塊圖。系統 1300 包含耦合至圖形記憶體控制器集線器（GMCH）1320 之一或更多處理器 1310、1315。增加的處理器 1315 的選加本質於圖 5 中以虛線表示。系統 1300 又包含耦合至一或更多處理單元的記憶體 1340。

圖 5 顯示耦合至記憶體 1340 的 GMCH 1320，記憶體 1340 舉例而言可爲動態隨機存取記憶體（DRAM）。對於至少一實施例，DRAM 可與非依電性快取記憶體相關連。

GMCH 1320 可爲晶片組或是晶片組的一部份。GMCH 1320 可以與處理器 1310、1315 通訊以及控制處理器

1310、1315與記憶體1340之間的互動。GMCH 1320也作爲處理器1310、1315與系統1300的其它元件之間的加速匯流排介面。對於至少一實施例，GMCH 1320經由例如前側匯流排（FSB）1395等多接點連接匯流排而與處理器1310、1315通訊。

此外，GMCH 1320耦合至顯示器1345（例如平板顯示器）。GMCH 1320包含整合的圖形加速器。GMCH 1320又耦合至輸入/輸出（I/O）控制器集線器（ICH）1350，其可用以將各種週邊裝置耦合至系統1300。舉例而言，顯示於圖5的實施例中的是外部圖形裝置1360，其是與另一週邊裝置1370耦合至ICH 1350的離散的圖形裝置。

替代地，增加的或不同的處理器也可以存在於系統1300中。舉例而言，增加的處理器1315包含與處理器1310相同的增加處理器、與處理器1310異質的或是不對稱的增加處理器、加速器（例如，圖形加速器或數位訊號處理（DSP）單元）、現場可編程閘陣列、或任何其它處理器。以包含架構、微架構、熱、功率消耗特徵等等特徵領域的觀點而言，在實體資源1310、1315之間有各種差異。這些差異使它們本身有效地顯示爲處理元件1310、1315之間的不對稱及異質性。對於至少一實施例，各式各樣的處理元件1310、1315可於設於相同的晶粒封裝中。

現在參考圖6，顯示根據本發明的實施例之第二系統1400的方塊圖。如圖6所示，多處理器系統1400是點對點互連系統，以及，包含經由點對點互連1450而耦合之

第一處理器 1470 和第二處理器 1480。或者，處理器 1470、1480 中之一或更多可以是處理器以外的元件，例如加速器或現場可編程閘陣列。雖然僅顯示二處理器 1470、1480，但是，要瞭解，本發明的實施例的範圍不限於此。在其它實施例中，一或更多增加的處理元件可以存在於給定的處理器中。

處理器 1470 可以又包含整合的記憶體控制器集線器（IMC）1472 及點對點（P-P）介面 1476 和 1478。類似地，第二處理器 1480 包含 IMC 1482 及點對點介面 1486 和 1488。使用點對點介面電路 1478、1488，處理器 1470、1480 經由點對點（PtP）介面 1450 以交換資料。如圖 6 所示，IMC 1472 和 1482 將處理器耦合至各別的記憶體，亦即記憶體 1432 及記憶體 1434，這些記憶體可爲區域地附著於各別處理器的主記憶體的部份。

使用點對點介面電路 1476、1494、1486、1498，處理器 1470、1480 經由個別的點對點介面 1452、1454，各別與晶片組 1490 交換資料。晶片組 1490 經由高性能圖形介面 1439，也與高性能圖形電路 1438 交換資料。

如圖 6 所示，各處理器 1470 和 1480 包含一或更多處理單元 1471。共用快取記憶體（例如 1481）可以包含在處理器中或是二處理器之外部，還經由點對點互連而與處理器連接，以致於假使處理器被置於低功率模式中時，任一或二處理器的區域快取記憶體資訊可以儲存在共用快取記憶體中。

晶片組 1490 經由介面 1496 而耦合至第一匯流排 1416。在一實施例中，第一匯流排 1416 可爲週邊組件互連（PCI）匯流排、或是例如快速 PCI 匯流排等匯流排或是其它第三代的 I/O 互連匯流排，但是，本發明的實施例的範圍不受限於此。

如圖 6 所示，各式 I/O 裝置 1414 可以與匯流排橋接器 1418 耦合至第一匯流排 1416，匯流排橋接器 1418 將第一匯流排 1416 耦合至第二匯流排 1420。在一實施例中，第二匯流排 1420 是低腳數（LPC）匯流排。各式裝置可以耦合至第二匯流排 1420，在一實施例中，舉例而言，各式裝置包含鍵盤/滑鼠 1422、通訊裝置 1426 及例如磁碟機或其它大量儲存裝置等包含碼 1430 的資料儲存單元 1428。此外，音頻 I/O 1424 耦合至第二匯流排 1420。注意，其它架構是可能的。舉例而言，取代圖 6 的點對點架構，系統可以實施多點連接匯流排或是其它此類架構。

現在參考圖 7，其顯示根據本發明的實施例之第三系統 1500 的方塊圖。圖 6 和 7 中的類似元件帶有類似代號，圖 7 的某些態樣從圖 7 省略，以免模糊圖 7 的其它態樣。

圖 7 顯示處理元件 1470、1480 分別包含整合的記憶體及 I/O 控制邏輯（CL）1472 和 1482。對於至少一實施例，CL 1472、1482 包含記憶體控制器集線器邏輯（IMC），例如上述配合圖 4 及 5 所述的記憶體控制器集線器邏輯。此外，CL 1472、1482 也包含 I/O 控制邏輯。圖 7 顯

示不僅記憶體 1432、1434 耦合至 CL 1472、1482，輸入/輸出（I/O）裝置 1514 也耦合至控制邏輯 1472、1482。舊有 I/O 裝置 1515 耦合至晶片組 1490。

在一實施例中，系統（例如，400、1300、1400、1500、等等）包含處理器（例如，405、1310、1315、1470、1480、等等），該處理器存取至少一真實鑰。記憶體耦合至處理器。記憶體儲存至少一轉換鑰，處理器配置成執行鑰轉換指令，以根據至少一真實鑰來產生至少一轉換鑰。記憶體包含快取記憶體以儲存映射，映射係根據至少一真實鑰而將轉換鑰映射至對應的循環鑰。處理器又配置成假使快取遺失發生時，將轉換鑰解碼。儲存在快取記憶體中的映射導入轉換鑰查詢的有限負擔。在實施例中，記憶體具有用於轉換鑰之有限儲存，以及，處理器執行指令以指明用於選取轉換鑰的索引。除了快取記憶體之外，記憶體還包含表格或其它結構，以儲存將轉換鑰映射至對應的真實鑰之映射。

在替代實施例中，處理器配置成接收單一鑰及自動地產生要由處理器儲存及存取的循環鑰。處理器配置成執行鑰轉換指令，以產生至少一轉換鑰來回應產生至少一循環鑰。

在一實施例中，處理器（例如，405、1310、1315、1470、1480、等等）包含處理單元（例如，1471），以從安全區取出至少一真實鑰以及根據至少一真實鑰來產生至少一循環鑰。記憶體（例如，快取記憶體 1481）耦合至處

理單元。處理單元配置成執行鑰轉換指令，以根據至少一循環鑰來產生至少一轉換鑰。快取記憶體儲存至少一循環鑰以及至少一轉換鑰。至少一轉換鑰是使用對話鑰由處理器加密的至少一循環鑰的加密版本，對話鑰是在電力初始化時隨機地導出的。處理單元（且無其它機器）能夠將至少一轉換鑰解密以及將至少一循環鑰加密。在另一實施例中，至少一轉換鑰是使用用於處理單元的獨特鑰由處理器加密的至少一循環鑰的加密版本，獨特鑰經由導出鑰而內部地導出及持續。藉由熔斷而取得導出鑰。

應瞭解，在本說明書中述及「一實施例」或「實施例」意指配合實施例說明之特定的特點、結構、或特徵包含在至少一實施例中。因此，所強調的及應瞭解的是，在本說明書中的不同部份中二次或多次地提及「實施例」、「一實施例」、或「替代實施例」，並非一定都意指相同的實施例。在一或更多實施例中，特點、結構、或特徵可以適當地結合。

在各種實施例的上述詳細說明中，參考附圖，附圖係形成詳細說明的一部份，以及，其中，以說明方式而非限定方式，顯示可實施本發明的具體實施例。在圖式中，類似的代號說明多個視圖中實質上類似的組件。以充份的細節，說明所示的實施例，以使習於此技藝者能夠實施此處揭示的教示。可以使用及導出其它實施例，以致於在不悖離本揭示的範圍之下，可作出結構及邏輯的替代和改變。因此，上述詳細說明，不應被視爲限定性的，且各式各樣

的實施例的範圍僅由後附的申請專利範圍、以及均等於這些申請專利範圍所賦予的範圍之完全範圍所界定。

【圖式簡單說明】

在附圖的圖式中，以舉例說明而非限定的方式，顯示本發明的各式各樣的實施例，其中：

圖 1 顯示根據本發明的一實施例之當執行主機爲基礎的加密時保護對稱加密鑰之電腦實施的方法 100 的一實施例之流程圖；

圖 2 是方塊圖，顯示根據本發明的一實施例之產生轉換的鑰之機制；

圖 3 顯示根據本發明的一實施例之以對稱加密鑰用於加密之電腦實施的方法 300 的一實施例之流程圖；

圖 4 是功能方塊圖，顯示根據本發明的一實施例實施的系統 900；

圖 5 是根據本發明的一實施例的系統 1300 的方塊圖；

圖 6 是根據本發明的實施例的第二系統 1400 的方塊圖；及

圖 7 是根據本發明的實施例的第三系統 1500 的方塊圖。

【主要元件符號說明】

900：系統

905：處理器

907：機器可存取的媒體

910：系統記憶體

915：非依電性記憶體

920：資料儲存單元

925：通訊鏈結

930：晶片組

950：輸入/輸出電路

1300：系統

1310：處理器

1315：處理器

1320：圖形記憶體控制器集線器

1340：記憶體

1345：顯示器

1350：輸入/輸出控制器集線器

1360：圖形裝置

1370：週邊裝置

1395：前側匯流排

1400：系統

1414：輸入/輸出裝置

1416：第一匯流排

1418：匯流排橋接器

1420：第二匯流排

1422：鍵盤/滑鼠

1424：音頻輸入/輸出

1426：通訊裝置

1428：資料儲存單元

1430：碼

1432：記憶體

1434：記憶體

1438：圖形電路

1439：圖形介面

1450：點對點互連

1452：點對點介面

1454：點對點介面

1470：處理器

1471：處理單元

1472：整合的記憶體控制器集線器

1476：點對點介面電路

1478：點對點介面電路

1480：處理器

1481：快閃記憶體

1482：整合的記憶體控制器集線器

1486：點對點介面電路

1488：點對點介面電路

1490：晶片組

1494：點對點介面電路

1496：介面

1498：點對點介面電路

1500：系統

1514：輸入/輸出裝置

1515：輸入/輸出裝置

七、申請專利範圍：

1.一種電腦實施方法，包括：

從安全區取出至少一真實鑰；

以處理器執行輔助鑰產生指令，該輔助鑰產生指令根據取出該至少一真實鑰而輔助至少一循環鑰產生；以及

以處理器執行鑰轉換指令，以產生至少一轉換鑰來回應該至少一循環鑰的產生。

2.如申請專利範圍第 1 項之電腦實施方法，又包括：

在平台的早期平台開機之多個階段期間，將該至少一轉換鑰儲存在記憶體中。

3.如申請專利範圍第 2 項之電腦實施方法，又包括：

以與該平台相關連的該處理器，將該至少一轉換鑰解密；以及

將該至少一循環鑰從系統記憶體抹除。

4.如申請專利範圍第 3 項之電腦實施方法，其中，該至少一轉換鑰是使用該至少一真實鑰由該處理器加密的該至少一循環鑰的加密版本，其中，該至少一真實鑰包括在電力初始化時隨機地導出的對話鑰，其中，僅有該處理器能夠將該至少一轉換鑰解密以及將該至少一循環鑰加密。

5.如申請專利範圍第 2 項之電腦實施方法，其中，該至少一轉換鑰是使用該至少一真實鑰由該處理器加密的該至少一循環鑰的加密版本，其中，該至少一真實鑰包括用於該處理器的獨特鑰，該獨特鑰是經由根據熔斷的導出鑰而內部地導出及持續。

6.如申請專利範圍第 1 項之電腦實施方法，其中，該至少一轉換鑰包括複數個轉換循環鑰。

7.如申請專利範圍第 2 項之電腦實施方法，其中，從安全區取出真實鑰包括將真實鑰從受信任的平台模組解密封。

8.如申請專利範圍第 7 項之電腦實施方法，其中，該受信任的平台模組與該早期的平台開機互動，以便當該處理器執行有限的軟體碼以降低攻擊的區域及受信任的碼基礎時，產生該等轉換鑰。

9.一種機器可取存的媒體，包含資料，當由機器存取該資料時，該資料促使該機器執行包括下述的操作：

從安全區取出至少一真實鑰；

以處理器執行輔助鑰產生指令，該輔助鑰產生指令根據取出該至少一真實鑰而輔助至少一循環鑰產生；以及

以處理器執行鑰轉換指令，以產生至少一轉換鑰來回應該至少一循環鑰的產生。

10.如申請專利範圍第 9 項之機器可存取的媒體，又包括：

在平台的早期平台開機之多個階段期間，將該至少一轉換鑰儲存在記憶體中；

以與該平台相關連的該處理器，將該至少一轉換鑰解密；以及

將該至少一循環鑰從系統記憶體抹除。

11.如申請專利範圍第 10 項之機器可存取的媒體，其

中，該至少一轉換鑰是使用該至少一真實鑰由該處理器加密的該至少一循環鑰的加密版本，其中，該至少一真實鑰包括在電力初始化時隨機地導出的對話鑰，其中，僅有該處理器能夠將該至少一轉換鑰解密以及將該至少一循環鑰加密。

12.一種處理系統，包括：

處理器，存取至少一真實鑰；以及

記憶體，耦合至該處理器，該記憶體用以儲存至少一轉換鑰，該處理器配置成執行鑰轉換指令，以根據該至少一真實鑰來產生至少一轉換鑰。

13.如申請專利範圍第 12 項之系統，其中，該記憶體包含快取記憶體以儲存映射，該映射係根據該至少一真實鑰而將轉換鑰映射至對應的循環鑰。

14.如申請專利範圍第 13 項之系統，其中，該處理器又配置成假使快取記憶體遺失發生時，將該轉換鑰解密。

15.如申請專利範圍第 12 項之系統，其中，該記憶體具有用於該轉換鑰之有限儲存，以及，該處理器執行指令以指明用於選取轉換鑰的索引。

16.如申請專利範圍第 12 項之系統，其中，該記憶體包含表格或其它結構，以儲存將轉換鑰映射至對應的真實鑰之映射。

17.如申請專利範圍第 12 項之系統，其中，該處理器配置成接收單一鑰及自動地產生要由該處理器儲存及存取的複數循環鑰，其中，該處理器配置成執行該鑰轉換指

令，以產生至少一轉換鑰來回應產生至少一循環鑰。

18.一種處理器，包括：

處理單元，從安全區取出至少一真實鑰以及根據至該少一真實鑰來產生至少一循環鑰；以及

快取記憶體，耦合至該處理單元，該處理單元配置成執行鑰轉換指令，以根據該至少一循環鑰來產生至少一轉換鑰，其中，該快取記憶體儲存該至少一循環鑰以及該至少一轉換鑰。

19.如申請專利範圍第 18 項之處理器，其中，該至少一轉換鑰是使用對話鑰由該處理單元加密的該至少一循環鑰的加密版本，該對話鑰是在電力初始化時隨機地導出的，其中，僅有該處理單元能夠將該至少一轉換鑰解密以及將該至少一循環鑰加密。

20.如申請專利範圍第 18 項之處理器，其中，該至少一轉換鑰是使用用於該處理單元的獨特鑰由該處理器加密的該至少一循環鑰的加密版本，該獨特鑰是經由根據熔斷的導出鑰而內部地導出及持續。

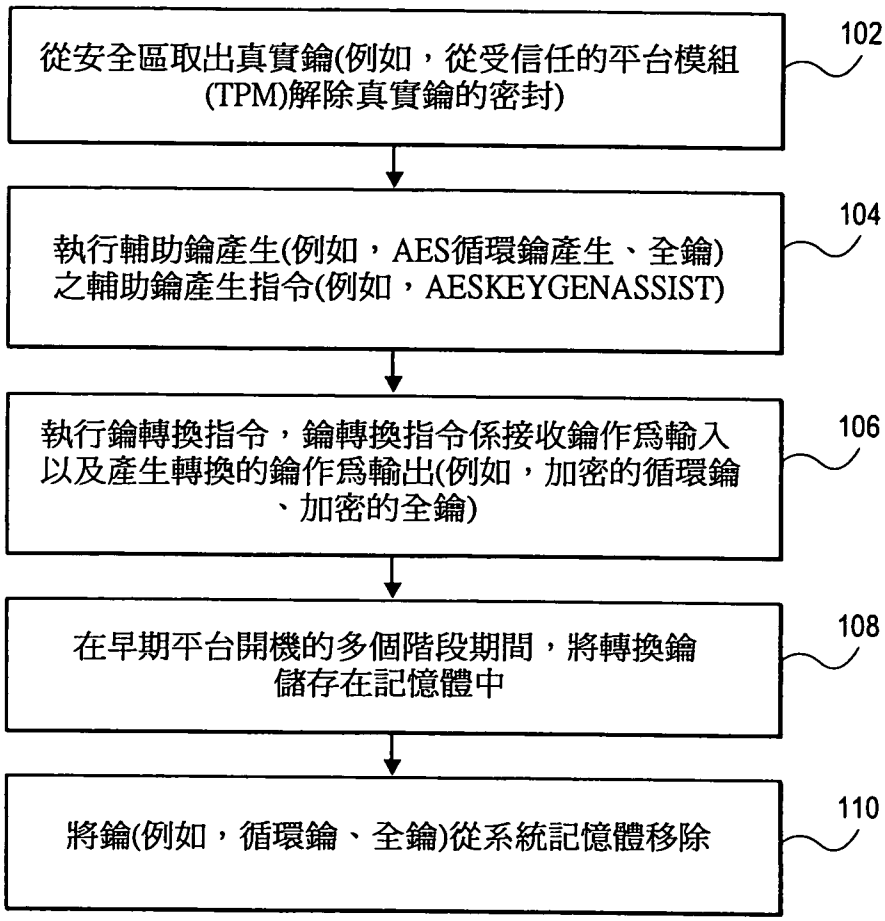
從安全區取出真實鑰(例如，從受信任的平台模組(TPM)解除真實鑰的密封)
102
執行輔助鑰產生(例如，AES循環鑰產生、全鑰)之輔助鑰產生指令(例如，AESKEYGENASSIST)
104
執行鑰轉換指令，鑰轉換指令係接收鑰作爲輸入以及產生轉換的鑰作爲輸出(例如，加密的循環鑰、加密的全鑰)
106
在早期平台開機的多個階段期間，將轉換鑰儲存在記憶體中
108
將鑰(例如，循環鑰、全鑰)從系統記憶體移除
110

圖1

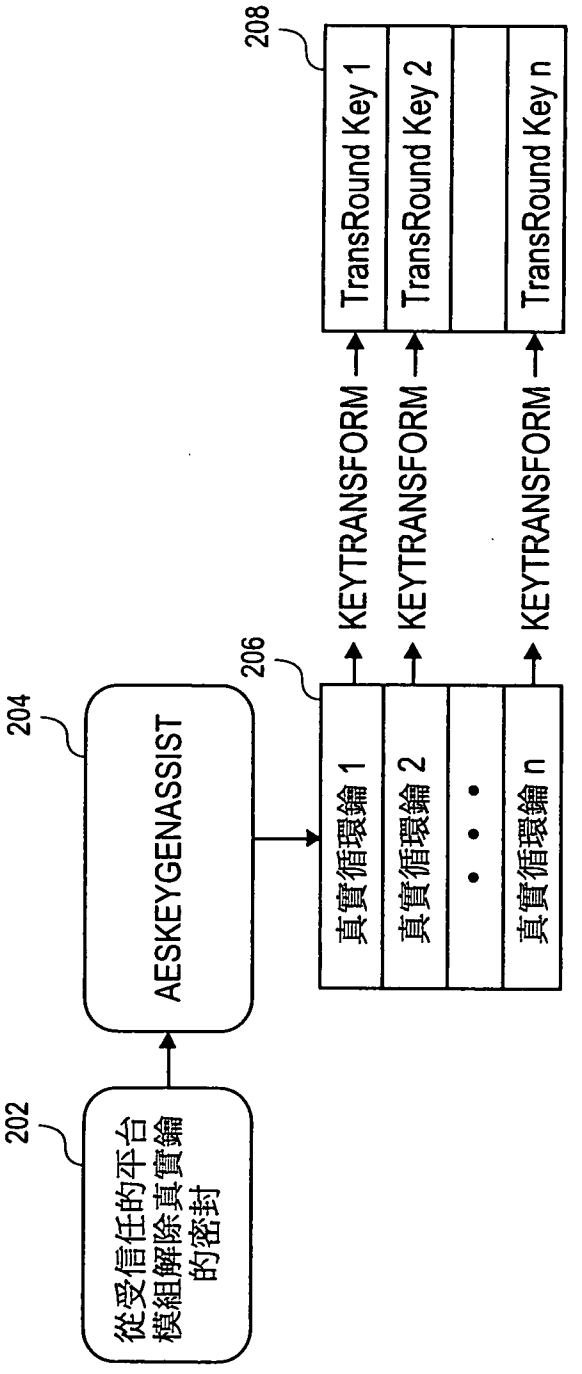
202
從受信任的平台模組解除真實鑰的密封
204
AESKEYGENASSIST
206
真實循環鑰 1
真實循環鑰 2
• • •
真實循環鑰 n
KEYTRANSFORM
KEYTRANSFORM
KEYTRANSFORM
208
TransRound Key 1
TransRound Key 2
TransRound Key n

圖 2

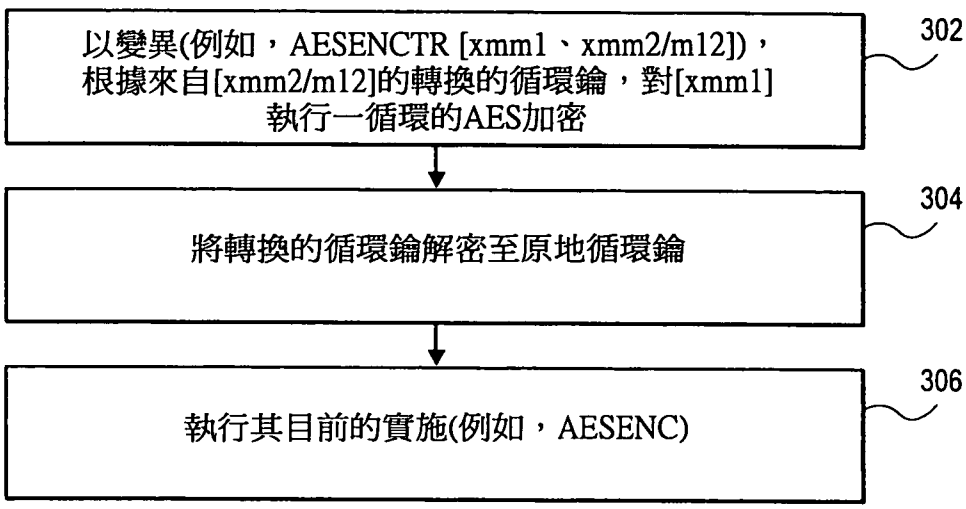
以變異(例如，AESENCTR [xmm1、xmm2/m12])，
根據來自[xmm2/m12]的轉換的循環鑰，對[xmm1]
執行一循環的AES加密
302
將轉換的循環鑰解密至原地循環鑰
304
執行其目前的實施(例如，AESENC)
306

圖3

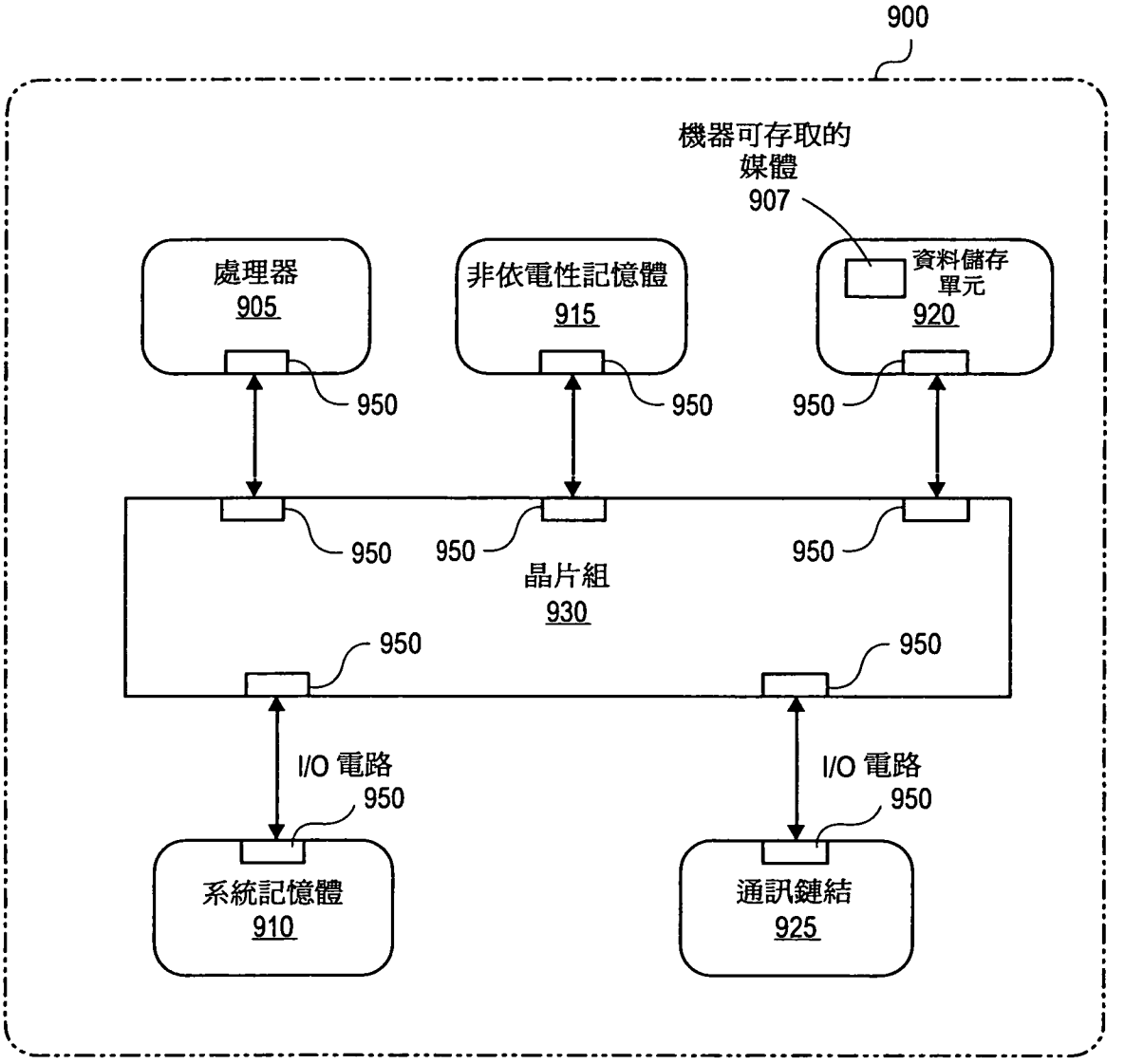
900
機器可存取的
媒體
907
處理器
905
非依電性記憶體
915
資料儲存
單元
920
950
950
950
950
950
950
晶片組
930
950
950
I/O 電路
950
I/O 電路
950
系統記憶體
910
通訊鏈結
925

圖4

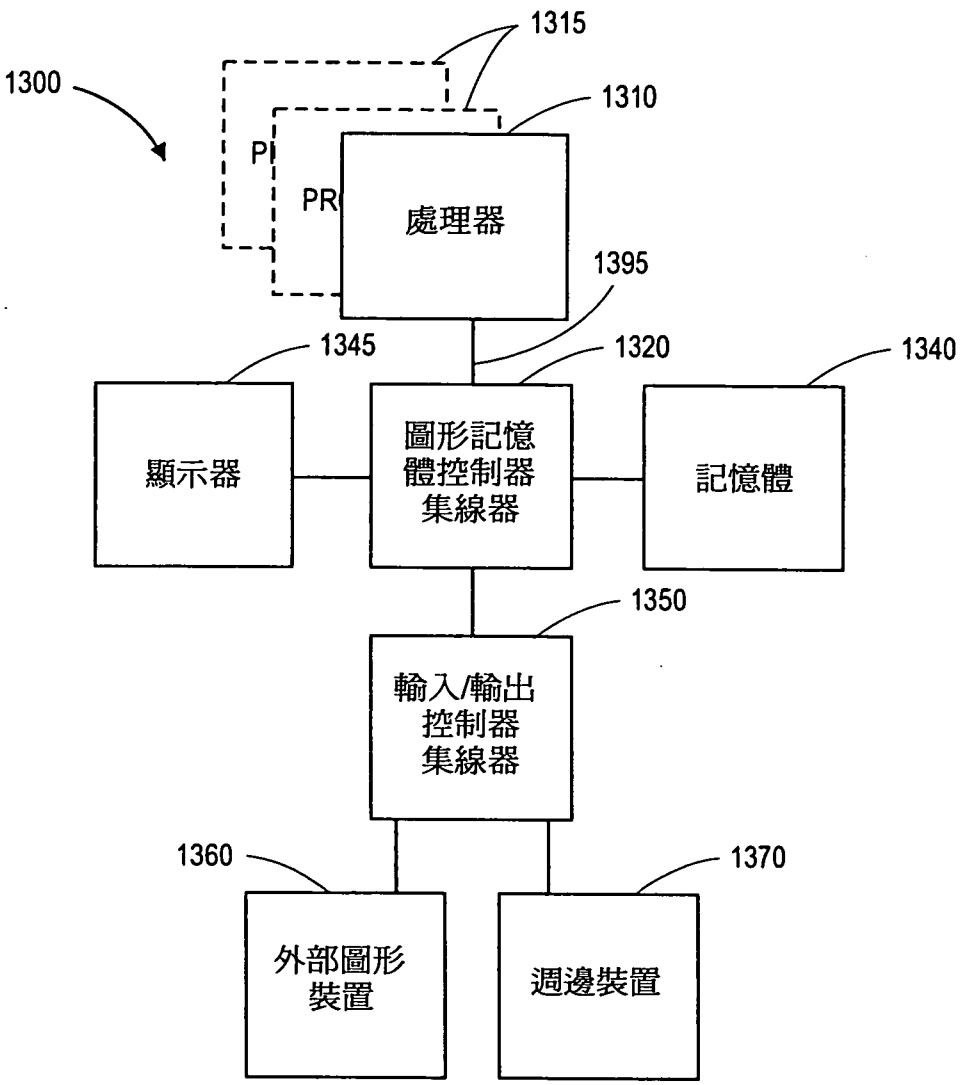
1315
1300
1310
PI
PR
處理器
1395
1345
1320
1340
顯示器
圖形記憶體控制器集線器
記憶體
1350
輸入/輸出控制器集線器
1360
1370
外部圖形裝置
週邊裝置

圖5

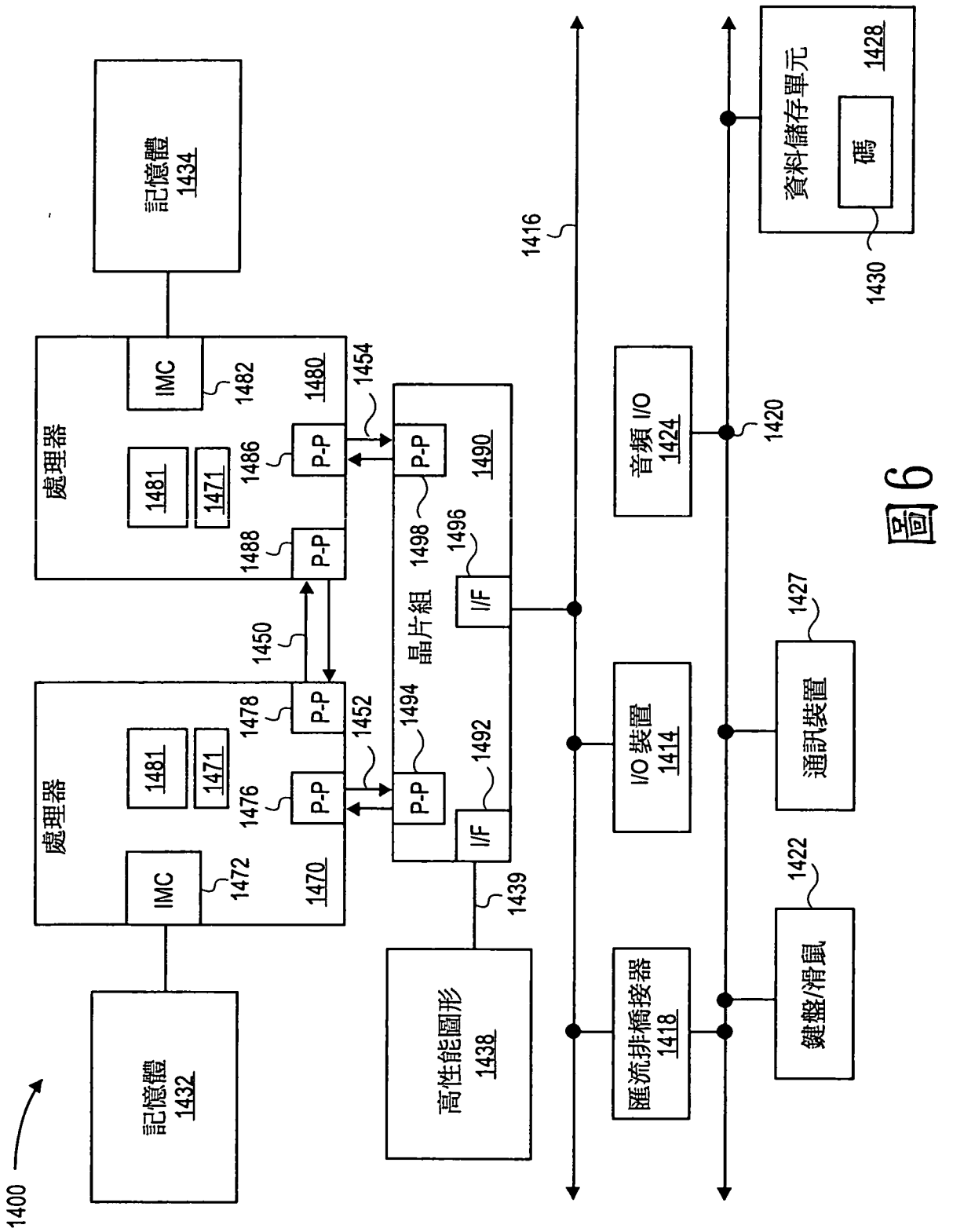
1400
記憶體 1432
記憶體 1434
處理器
IMC
1472
1470
1481
1471
1476
1478
1452
1450
1454
1480
1482
1486
1488
P-P
晶片組
1490
1494
1498
1496
1492
I/F
1439
高性能圖形 1438
匯流排橋接器 1418
I/O 裝置 1414
音頻 I/O 1424
1416
1420
1422
鍵盤/滑鼠
1427
通訊裝置
1428
碼
資料儲存單元
1430

圖 6

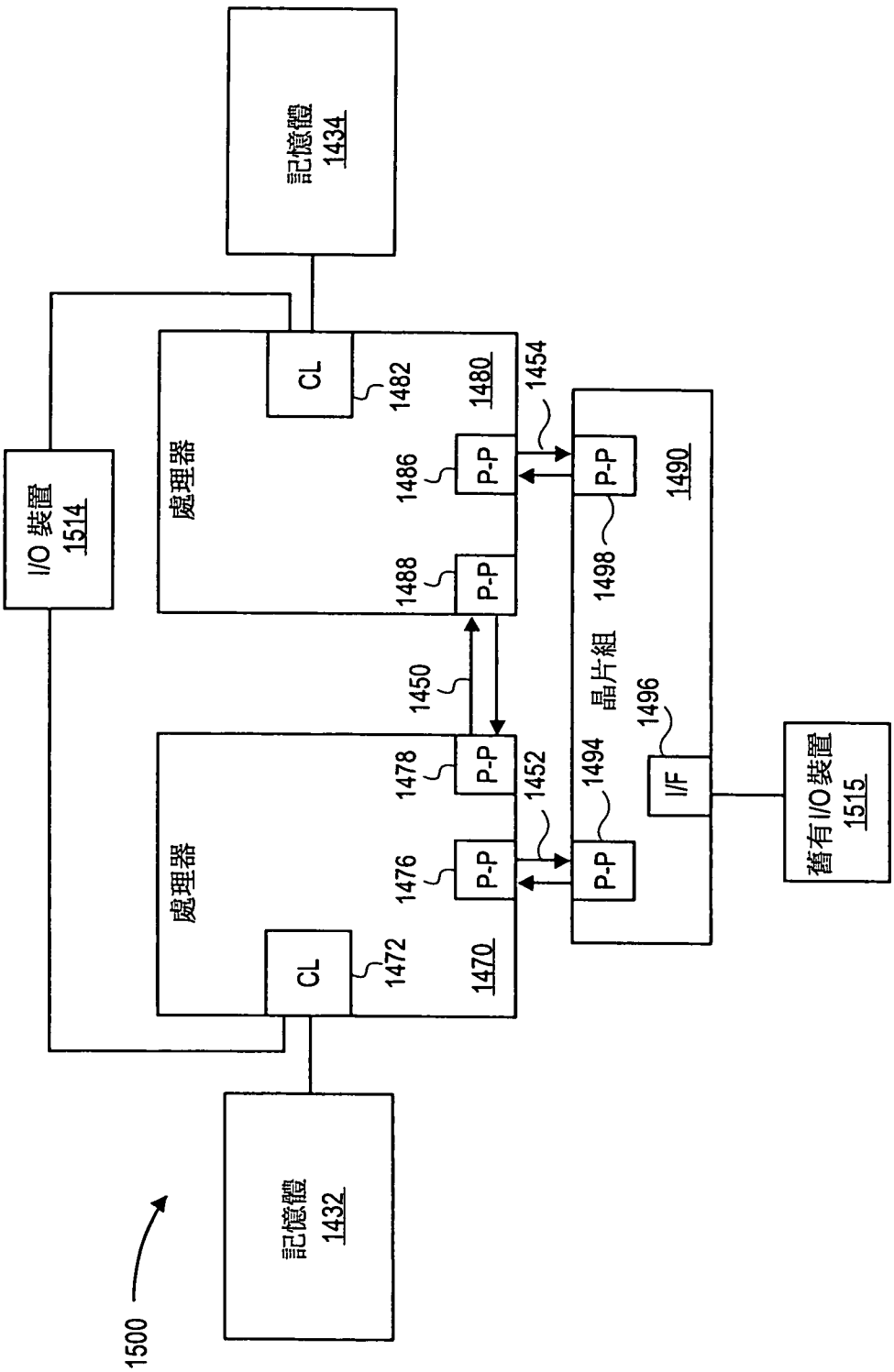
記憶體
1434
I/O 裝置
1514
處理器
CL
1482
1480
1454
1486
P-P
1488
P-P
1450
處理器
1478
P-P
1452
1476
P-P
1470
CL
1472
晶片組
1490
P-P
1498
P-P
1494
1496
I/F
舊有I/O裝置
1515
記憶體
1432
1500

圖7