(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200949681 A1
(43)公開日： 中華民國 98 (2009) 年 12 月 01 日

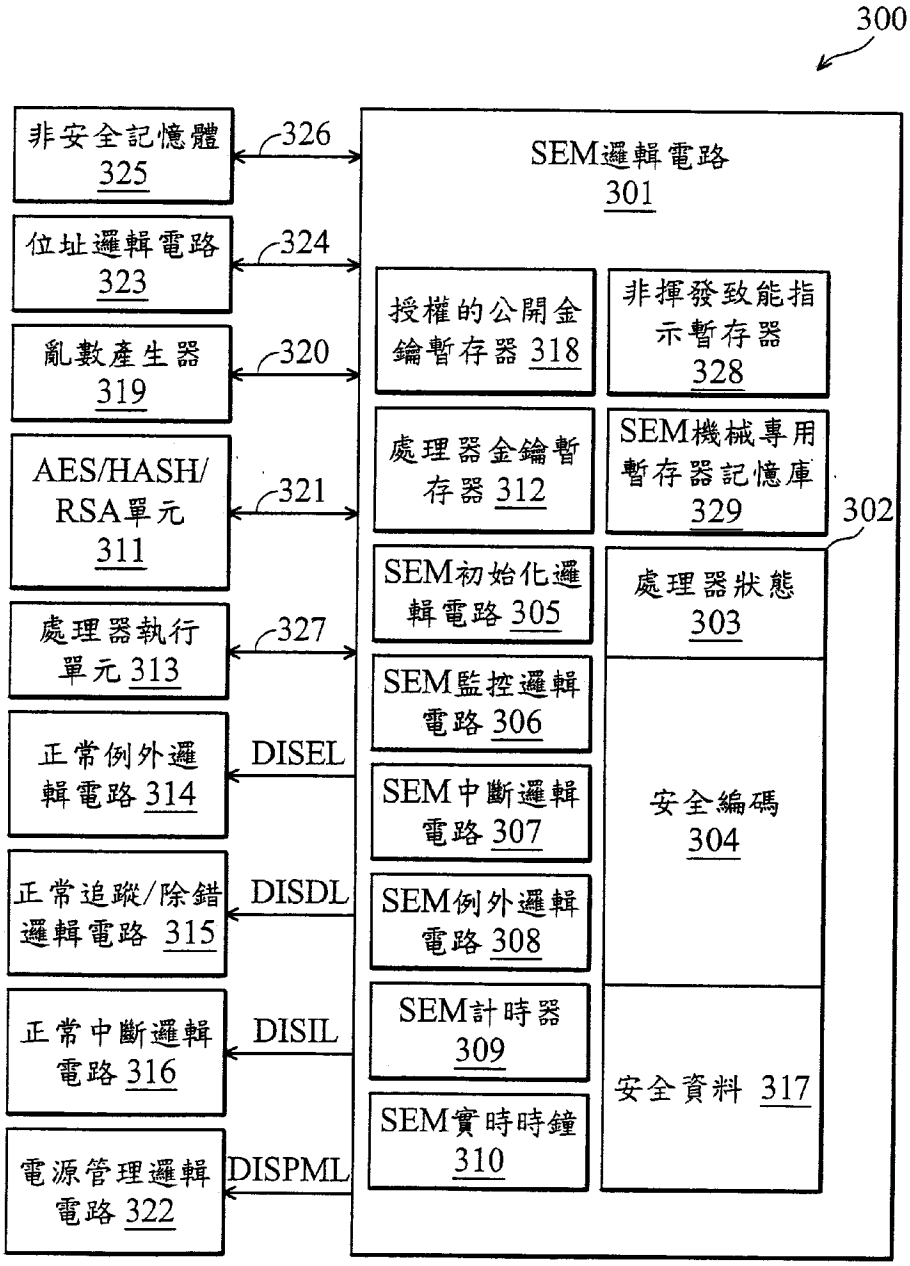
(21)申請案號：098113141 (22)申請日： 中華民國 98 (2009) 年 04 月 21 日
(51)Int. Cl.： *G06F9/30 (2006.01)*
(30)優先權：2008/05/24 美國 61/055,980
2008/10/31 美國 12/263,238
(71)申請人：威盛電子股份有限公司 (中華民國) VIA TECHNOLOGIES, INC. (TW)
臺北縣新店市中正路 535 號 8 樓
(72)發明人：亨利G 葛蘭 HENRY, G. GLENN (US) ；派克斯 泰瑞 PARKS, TERRY (US)
(74)代理人：洪澄文；顏錦順
申請實體審查：有 申請專利範圍項數：24 項 圖式數：12 共 86 頁

(54)名稱

提供安全執行環境之裝置、微處理器裝置、以及在安全執行環境中執行安全編碼之方法
APPARATUS AND METHOD FOR MANAGING A MICROPROCESSOR PROVIDING FOR A SECURE EXECUTION MODE

(57)摘要

一種提供安全執行環境之裝置，其微處理器執行非安全應用程式與安全應用程式。非安全應用程式透過系統匯流排存取自系統記憶體，且安全應用程式在安全執行模式中執行。微處理器包括安全執行模式邏輯電路，其監控對應微處理器且與潛在篡改相關之狀態，並根據狀態中第一者使微處理器自安全執行模式轉換至降級模式。降級模式只提供給 BIOS 指令執行。此裝置之安全非揮發記憶體透過私密匯流排耦接微處理器且儲存安全應用程式。在私密匯流排上微處理器與安全非揮發記憶體之間的資料傳輸隔離於系統匯流排及微處理器內之對應系統匯流排資源。



300：安全執行模式微處理器

301：SEM 邏輯電路

302：安全揮發記憶體

303：處理器狀態

304：安全編碼

305：SEM 初始化邏輯電路

306：SEM 監控邏輯電路

307：SEM 中斷邏輯電路

308：SEM 例外邏輯電路

309：SEM 計時器

310：SEM 實時時鐘

311：AES/HASH/ RSA 單元

312：處理器金鑰暫存器

313：處理器執行單元

314：正常例外邏輯電路

315：正常追蹤/除錯邏輯電路

316：正常中斷邏輯電路

317：對應安全編碼之安全資料

318：授權的公開金鑰暫存器

319：亂數產生器

320：匯流排

321：匯流排

322：電源管理邏輯電路

323：位址邏輯電路

324：匯流排

325：非安全記憶體

326：匯流排

327：匯流排

328：非揮發致能指示暫存器

329：SEM 機械專用暫存器記憶庫

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200949681 A1
(43)公開日： 中華民國 98 (2009) 年 12 月 01 日

(21)申請案號：098113141 (22)申請日： 中華民國 98 (2009) 年 04 月 21 日
(51)Int. Cl.： *G06F9/30 (2006.01)*
(30)優先權：2008/05/24 美國 61/055,980
2008/10/31 美國 12/263,238
(71)申請人：威盛電子股份有限公司 (中華民國) VIA TECHNOLOGIES, INC. (TW)
臺北縣新店市中正路 535 號 8 樓
(72)發明人：亨利G 葛蘭 HENRY, G. GLENN (US) ；派克斯 泰瑞 PARKS, TERRY (US)
(74)代理人：洪澄文；顏錦順
申請實體審查：有 申請專利範圍項數：24 項 圖式數：12 共 86 頁

(54)名稱

提供安全執行環境之裝置、微處理器裝置、以及在安全執行環境中執行安全編碼之方法
APPARATUS AND METHOD FOR MANAGING A MICROPROCESSOR PROVIDING FOR A SECURE EXECUTION MODE

(57)摘要

一種提供安全執行環境之裝置，其微處理器執行非安全應用程式與安全應用程式。非安全應用程式透過系統匯流排存取自系統記憶體，且安全應用程式在安全執行模式中執行。微處理器包括安全執行模式邏輯電路，其監控對應微處理器且與潛在篡改相關之狀態，並根據狀態中第一者使微處理器自安全執行模式轉換至降級模式。降級模式只提供給 BIOS 指令執行。此裝置之安全非揮發記憶體透過私密匯流排耦接微處理器且儲存安全應用程式。在私密匯流排上微處理器與安全非揮發記憶體之間的資料傳輸隔離於系統匯流排及微處理器內之對應系統匯流排資源。

六、發明說明：

【發明所屬之技術領域】

本發明係有關於在微電子領域中，特別是有關於一種微處理器，其提供一安全執行模式的操作，其允許在微處理器內之安全環境中執行運算碼。

【先前技術】

桌上型電腦、筆記型電腦、以及手持式電腦與通訊裝置可作為機密或專用資料與數位權控制內容之數位通訊平台，電腦產業對於這些裝置的使用持續地發展新的安全制度。舉例來說，有許多已建立的應用，用以在網際網路上免費下載與管理數位聲音與影響檔案。透過這些應用，使用者被提供在歌曲、電視節目以及電影上的有限的權利。特別注意的是，以上透過使用建立在這些應用中的安全特性來保護這些權利，而這些安全特性通常依據其主機平台所提供之安全機制。

除了數位內容權利的保護，持續驅動電腦系統安全性的另一因素是實施在主機平台本身的使用限制。目前已知，手機產業已提供特定通訊裝置中所謂的"隨用隨付（Pay-as-you-go）"使用。藉由使用此方案，使用者不需給付月費，但是需預先給付某通話分鐘數的金額。當用盡通話分鐘數時，除了緊急通話以外，使用者被拒絕存取任何關於通話的手機網路存取。

早在 2006 年，MICROSOFT 公司與其合作公司已提供主要指向新興電腦市場之"隨用隨付"個人電腦。在此體制下，透過預付卡的購得，當使用這些公司的電腦時使用者

則給付費用。此外，歸屬於 MICROSOFT 公司的美國專利申請案公開編號 20060282899，揭露一種用於模組化操作系統之傳遞的系統與方法，其包括提供主要操作系統支援的核心功能模組或基礎核心，且包括一或多個允許客製化之操作系統定做的附屬模組。在此應用中，附屬模組可提供對於電腦（其包括硬體、應用軟體、周邊設備、以及支援設備）的支援或延伸能力。在設置之前，數位簽章可使用來確定附屬模組之完整性，且核對證明(certification)以判斷附加模組之設置是否經過授權。藉由此證明，服務提供者可管理對提供之電腦上的非法或非期望修改。此外，數位權利管理可用來執行與許可配置相配之附屬模組的使用項目。

並不意外地，目前已發展出技術方法的真正主機，其提供規避安全措施，而這些安全措施是適當地保護且控制對權利控制數位媒體、通訊裝置、以及電腦平台的存取。最近，"hacking（進行非法入侵，即駭客）"變成研究上的課題。事實上，本案發明人已注意到許多用來篡改或完全地使安全管理無效的作品公開，而這些安全管理係用來防護受保護資產之存取及/或使用。由 Andrew Huang, San Francisco: No Starch Press, 2003 所提出的著作 Hacking the Xbox: An Introduction to Reverse Engineering 則是上述作品的一種。此著作特別著重於教導非法入侵技術以克服 MICROSOFT 所出產之 XBOX 遊戲平台的安全機制，且更提供電腦安全與反向工程的教導主題，並討論所謂"安全的"電腦平台的弱點。

因此，平台建置者與設計者持續從事在避免未被授權的平台處理上更有效的技術與機制，不論此存取是良性的（例如探測或窺察）、惡意的（例如破壞性的或違背權利的入侵）、或是介於兩者之間（例如篡改）。這些機制中許多者係用來防止入侵者實際上存取平台，例如將平台放置在安全底座上（例如一上鎖的金屬圍場）或者將有弱點的電路封裝入環氧化物內。但是已知這些類型的技術增加了系統成本與複雜性。其他機制則係利用特定電腦架構本身提供之安全特性。

考慮已知 x86 架構所提供之兩個主要安全特性：分頁虛擬記憶體(paged virtual memory)以及特許執行(privileged execution)。在分頁虛擬記憶體的情況下，基本的操作系統定義一個分別的虛擬位置空間以及存取權利（例如只執行、只讀取）給每一正被執行的應用程式，因此阻止另一秘密鬼祟的應用程式在所定義的區域內執行，且阻止其修改資料。但是，由於與虛擬位址譯文相關（即分頁表單）之資料存在於系統記憶體，且其出現於主機微處理器外的系統匯流排上，因此此資料可輕易地被被窺察且被改變。

在特許執行的情況下，x86 結構提供數種階級的執行特權 CPL0 至 CPL3。因此，某些系統資源與指令只可由正在較高特權階級上執行的應用程式來存取。一般得知操作系統元件係操作在最高特權階級 CPL0，以及使用者應用係歸類於最低特權階級 CPL3。但是，熟知此技術領域之人士將查知，這些架構特徵主要是發展來阻止軟體錯誤所導致的系統當機，且在防止有意或經指導的侵入(directed hacks)

而言不是非常有效。

因此已發展多種方法與裝置，其更仔細地集中防止對平台之有意侵入與接管。在美國專利編號 5615263 中，Takahashi 教導一種在雙模(dual mode)處理器中的安全模式。在一般/外部模式中，此雙模處理器執行由外部來源所提供之指令。這些指令透過雙模處理器的輸入/輸出來提供給雙模處理器。當接收到專用軟體或硬體發出之中斷時，此雙模處理器進入安全/內部模式。此中斷是指儲存在雙模處理器中唯讀記憶體內的安全功能。根據此接收的中斷，雙模處理器的輸入/輸出被禁能。此已確認的安全功能係由雙模處理器來執行。在此安全功能的執行期間，欲插置非來自唯讀記憶體之指令的任何企圖皆被忽略。然而，雙模處理器可存取由正在執行之安全功能所特別確認的資料。當安全功能之執行完成，則執行一退出程序，以致能雙模處理器之輸入/輸出，並透過輸入/輸出重新開始執行由雙模處理器之外部來源所提供之指令。

Takahashi 教導此安全模式是用作加密與解密，且其中雙模處理器處理透過匯流排且由外部控制通道(external control channel)處理器所提供之正常指令與資料，其中，此匯流排符合一標準匯流排架構，例如工業標準體系結構（Industry Standard Architecture，ISA）。此雙模處理器在非安全模式下開啟，且安全模式透過軟體或硬體發出的中斷來初始化。在安全模式下，可執行關於加密與解密之有限數量的功能（即指令）。這些功能儲存在一個唯讀記憶體中（ROM），其位於雙模處理器之內部。本案之發明人

注意到，Takahashi之雙模處理器並不適當，因為Takahashi之雙模處理器只能執行內部 ROM 所提供之有限數量的功能。因此，包括一般目的指令的應用程式（即在微處理器之指令集中任何的指令）則無法在安全模式下執行。

在美國專利編號 7013484 中，Ellison 揭露一種建立安全環境之晶片組，用於一隔離之儲存器所執行的隔離執行模式，此儲存器被至少一處理器來存取。在正常執行模式或此隔離執行模式下，此至少一處理器具有複數線程與操作。Ellison之安全環境係依據一外部晶片組（被隔離的執行電路），其提供機制給一處理器以在隔離執行模式下操作。此外部晶片組因此配置一個安全記憶體區域，其管理隔離指令之解碼與轉譯、隔離匯流排週期的產生、以及中斷的產生。當此外部晶片組主動地隔離記憶體區域、指令執行等時，注意到此外部晶片組係透過一般系統匯流排而耦接此至少一處理器，因此在任何安全線程的執行期間內容許在匯流排上的窺察與流量篡改。

在美國專利編號 7130951 中，Christie 揭露一種方法，用以控制有安全執行模式能力之處理器，此處理器包括複數中斷，以使得當其正操作在非安全執行模式時，中斷此有安全執行模式能力之處理器。此方法包括當此有安全執行模式能力之處理器正操作在一安全執行模式時，禁能複數中斷以避免此處理器中斷。儘管禁能中斷是在安全執行環境中所期望的安全特性，根據 Christie 之處理器係處理透過系統匯流排且由一操作系統所提供之指令與資料。一旦這些指令被提供時，中斷即被禁能。如同 Ellison 的機制，

此一裝置明確地可被透過匯流排而提供至處理器的指令來做匯流排窺察與篡改。

在美國專利編號 6983374 中，Hashimoto 揭露一種抗篡改微處理器，其保存關於其執行將被中斷之一個程式的內容資訊，其中，此處理器狀態被加密且儲存在系統記憶體。Hashimoto 也教導了自系統記憶體擷取加密指令的技術，以及對加密指令進行解密且執行此加密指令之裝置。此外，Hashimoto 教導了使用一對應金鑰來提供在記憶體內的加密指令，且接著使用非對稱金鑰演算法來對儲存在記憶體內的對稱金鑰加進行加密。對於程式創造者來說，對稱金鑰是已知的，且使用讀取自處理器之公開金鑰來對此對稱金鑰進行加密。此處理器包括一獨特私密金鑰，其對應此公開金鑰，且使用者無法存取。因此，根據分支指令的執行，程式控制被轉移成"起始加密執行"指令，其傳送一指標至加密對稱金鑰。此處理器擷取加密對稱金鑰，且使用其內部私密金鑰來對其解密。接著，加密程式指令自系統記憶體被擷取，且藉由使用解密對稱金鑰來被解密，並由處理器來執行。假使發生中斷或異常，處理器的狀態則對稱地被加密且儲存至記憶體。Hashimoto 揭露了對於非加密與加密編碼的共通快取機制、中斷邏輯、異常處理邏輯的使用。

本案之發明人已注意到，Hashimoto 的微處理器限定編碼者已知對應安全編碼之對稱金鑰，且對稱金鑰可能被洩漏，因此，將具有此編碼之所有系統將有被攻擊的風險。此外，本案之發明人已注意到，Hashimoto 的微處理器缺點

在於，必須在擷取指令運作中執行安全編碼之解密，其花費非常多的時間，因此導致微處理器的處理能力變為緩慢。此外，注意到，Hashimoto之安全編碼利用現存的非安全資源，例如系統記憶體、分頁表單、中斷、與異常機制，這些全部都會遭受到窺察。

因此，本案之發明人瞭解，顯然期望提供一種微處理器，其能在安全執行環境中執行包括一般目的指令（即在微處理器之指令集中任何的指令)的應用程式或應用線程。

此外，同時也期望此安全執行環境係隔離於任何已知之窺察與篡改方法。因此，需要由一安全執行模式微處理器來執行指令，且此安全執行模式微處理器隔離於處理器中提供存取（例如快取窺察、系統匯流排流量、中斷、以及錯誤與追蹤特徵）之硬體。

此外，更期望當此微處理器載入應用程式並安全執行時，提供一機制來混淆來自任何現存監控裝置之應用的結構與內容，且提供一機制來證明此應用的來源且確認其誠實性。

【發明內容】

本發明適用於解決前述問題與對付習知技術之其他問題、缺點與限制。本發明提供較佳的技術，以在一般目的微處理器平台上致能安全應用程式之執行。在一實施例中，揭露一種提供安全執行環境之裝置，其包括微處理器以及安全非揮發記憶體。微處理器執行複數非安全應用程式與一安全應用程式。這些非安全應用程式透過系統匯流排而存取自系統記憶體，且安全應用程式在安全執行模式

中執行。微處理器包括安全執行模式邏輯電路，用以監控對應微處理器且與潛在安全暴露和篡改相關聯之複數狀態，並根據複數狀態之一來使微處理器自安全執行模式轉換至降級模式。降級模式只提供給複數基本輸入/輸出系統（Basic Input/Output System，BIOS）指令之執行，且這些BIOS指令包括允許使用者輸入與訊息顯示之指令。安全非揮發記憶體透過私密匯流排耦接微處理器，用以儲存安全應用程式。在私密匯流排上微處理器與安全非揮發記憶體之間的複數資料傳輸，隔離於系統匯流排以及微處理器內之複數對應系統匯流排資源。

本發明之另一實施例提供一種微處理器裝置，用以在安全執行環境中執行安全編碼，此微處理器裝置包括安全非揮發記憶體以及微處理器。安全非揮發記憶體儲存安全應用程式。微處理器透過私密匯流排耦接安全非揮發記憶體，用以執行複數非安全應用程式與上述安全應用程式。微處理器包括安全執行模式邏輯電路，用以監控對應微處理器且與潛在安全暴露和篡改相關聯之複數狀態，並根據這些狀態之一來使微處理器自安全執行模式轉換至降級模式。降級模式只提供給複數基本輸入/輸出系統（Basic Input/Output System，BIOS）指令之執行，且這些BIOS指令包括允許使用者輸入與訊息顯示之指令。

本發明之又一實施例提供一種在安全執行環境中執行安全編碼之方法，包括提供安全非揮發記憶體，以儲存安全編碼，其中，此安全編碼藉由實現在私密匯流排上之複數私密資料傳輸而存取自安全非揮發記憶體。私密匯流排

耦接安全非揮發記憶體與微處理器之間。私密匯流排隔離於微處理器內之所有系統匯流排資源且配置在微處理器之外部，且私密匯流排只由微處理器之安全執行邏輯電路所得知及存取。此方法更包括監控對應微處理器之複數狀態，其中，這些狀態與潛在安全暴露和篡改相關聯；以及根據這些狀態之一，使微處理器自安全執行模式轉換至降級模式，其中，降級模式只提供給複數基本輸入/輸出系統（Basic Input/Output System，BIOS）指令之執行，且這些BIOS指令包括允許使用者輸入與訊息顯示之指令。

關於產業應用性，本發明可實現於一微處理器內，且此微處理器係使用於一般目的或特殊目的之電腦裝置。

【實施方式】

為使本發明之上述目的、特徵和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下。

本發明雖以較佳實施例揭露如上，然其並非用以限定本發明的範圍，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可做些許的更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

鑑於上述關於在一微處理器中應用程式之安全並隔離地執行且關於用來防止窺察、侵入、篡改、或駭客之現今技術的背景討論，本發明的討論將透過第1至12圖來呈現。

參閱第1圖，其表示根據本發明實施例之安全執行模式（secure execution mode，SEM）微處理器101之示意圖。

此示意圖描述SEM微處理器101配置所在的系統板100(或主機板)。此微處理器101透過系統匯流排102耦接一或多個匯流排主控裝置(bus master)103以及/或者一或多個匯流排管理裝置(bus agent)104。在一實施例中，SEM微處理器101為x86相容微處理器101，其透過x86相容系統匯流排102耦接一或多個x86相容匯流排主控裝置103以及/或者一或多個x86相容匯流排管理裝置104。

此外，SEM微處理器101耦接一電池VP，其配置在系統板(主機板)100上，且透過連接路徑VP1與VP2來耦接至微處理器101。在一實施例中，電池VP之電壓為1.8V直流電壓(DC)。

石英器X1也配置在系統板100上，且透過連接路徑C1與C1來耦接至微處理器101。微處理器101包括SEM邏輯電路105。根據本發明之SEM邏輯電路105係配置來提供在微處理器內一安全執行模式之初始化、操作、以及終止，將於下文詳細說明。此SEM邏輯電路105包括邏輯、電路、裝置、或微碼（即微指令或原生指令）、或者是邏輯、電路、裝置、或微碼的結合、又或者是用來初始化安全執行模式的等效元件，使得SEM邏輯電路105可載入安全應用程式來執行、在一安全環境中執行這些應用程式、為了偵測且阻止篡改而監控一些微處理器與系統特性、在適當情況下終止安全執行模式、且假使偵測到篡改則暫停處理。用來執行這些功能與SEM邏輯電路105內其他功能之元件，可共享用來執行微處理器101內其他功能之其他電路、微碼等等。根據本申請案之範圍，微碼是涉及複數

個微指令的名詞。一微指令（也稱為原生指令）是在一單元執行所處之層級上的指令。例如，微指令係直接由精簡指令集運算（Reduced Instruction Set Computing，RISC）微處理器來執行。對於複雜指令集運算（Complex Instruction Set Computing，CISC）微處理器（例如 x86 相容微處理器）而言，x86 指令首先轉譯為相關的微指令，且此相關的微指令接著直接由 CISC 微處理器中一單元或複數單元來執行。

安全非揮發記憶體 107 也配置在系統板 100 上，其透過私密匯流排（PVT BUS）106 與內存檢測匯流排(presence detection bus)PSNT 來耦接至微處理器 101。根據本發明，安全非揮發記憶體 107 為一種經過電源之除去與重新施加後其內容仍存留之記憶體。即是，當提供至系統板之電源關閉或開啟時，安全非揮發記憶體 107 之內容不會改變。在一實施例中，安全非揮發記憶體 107 包括快閃唯讀記憶體（ROM），其大小相當於將在安全執行模式中執行之安全應用程式的大小。在一實施例中，考慮以 4MB 快閃唯讀記憶體來作為安全非揮發記憶體 107。在私密匯流排 106 上的資料傳輸(transactions)完全地隔離於系統匯流排 102、匯流排主控裝置 103 以及匯流排管理裝置 104，且私密匯流排 106 位於微處理器 101 之外部。在一實施例中，快閃唯讀記憶體 107 可程式化高達 100000 次。在一實施例中，私密匯流排 106 考慮以一序列匯流排來實現，其提供介於安全非揮發記憶體 107 與微處理器 101 之間的資料傳輸。此私密匯流排 106 可符合標準界面協定，例如序列周

邊介面（Serial Peripheral Interface，SPI）協定。

在操作上，電池 VP 與石英器 X1 提供在 SEM 邏輯電路 105 內實時時鐘（Real Time Clock，RTC)（未顯示）之持續操作，其將於下文詳細說明。包括來自主機結構指令集之一或多個安全應用程式，係透過系統匯流排 102 而擷取自系統記憶體（未顯示），且儲存在安全非揮發記憶體 107。在一實施例中，使用屬於授權者(authorizing party)之一私密非對稱金鑰並透過非對稱加密演算規則來加密一或多個安全應用程式，且安全應用程式以其非對稱加密格式而被存取自系統記憶體。在一實施例中，考慮透過 RSA 演算規則來加密一或多個安全應用程式。在此一或多個安全應用程式擷取自系統記憶體後，微處理器 101 利用一對應的公開金鑰來解碼此一或多個安全應用程式並確認此一或多個安全應用程式。根據安全執行模式的致能以及依據一"起始安全執行"指令的執行，SEM 邏輯電路 105 利用微處理器內的複數加密資源，以根據一對稱金鑰演算法並使用處理器獨特加密金鑰來對此一或多個安全應用程式進行加密，此外，SEM 邏輯電路 105 透過私密匯流排 106 來將已加密的一或多個安全應用程式傳送至安全非揮發記憶體 107。之後，SEM 邏輯電路 105 利用微處理器 101 內的複數加密或其他資源，來對此一或多個安全應用程式進行存取、確認以及解密，此一或多個安全應用程式接著載入至微處理器 101 內之一安全且隔離的隨機存取記憶體(RAM)或一快取記憶體（未顯示）。

當執行起始安全執行指令時(當進入至該安全執行模

式)，SEM 邏輯電路 105 禁能安全應用程式得知察覺所有的系統資源，而這些系統資源提供了包括非安全中斷、非安全例外邏輯以及追蹤/除錯邏輯電路等等之監視以及或篡改。儲存在隔離之內部 RAM 的一或多個安全應用程式係藉由使用 SEM 邏輯電路 105 內的專用安全執行資源來被執行。此一或多個安全應用程式接著可將處理器狀態由安全操作模式恢復至正常執行模式，或者假使偵測到潛在的篡改，他們可將微處理器轉換至具有有限的功能之降級模式。假使確定發生篡改，SEM 邏輯電路 105 接著使微處理器完全地關機(硬體關機模式)。

關於此一或多個安全應用程式（或"安全編碼"）之功能類型包括（但不受限於此）執行關鍵安全任務，例如憑證確認、資料加密以及資料解密；監控正常系統軟體活動；確認正常系統軟體之完整性；追蹤資源使用；新軟體的安裝。

在一實施例中，在本發明之安全處理系統中考慮使用表面黏著式微處理器 101、表面黏著式安全非揮發記憶體 107、以及表面黏著式石英器 X1。這些表面黏著式元件包括球閘陣列（ball-grid array）元件或焊接在系統板 100 上的其他相似技術。

本發明之微處理器 101 也執行儲存在系統記憶體內(未顯示）的非安全應用程式，這些非安全應用程式的指令透過系統匯流排 102 來提供。在本發明之觀念中，微處理器 101 能如中央處理單元（Centralized Processing Unit，CPU）般操作，而不用因應協同處理器(coprocessor)的要求。即

是，本發明之微處理器 101 能執行主機指令集的所有指令，且能執行全部的應用程式。與只能執行自一主要 CPU 轉移之單一指令、程式線程或程式片斷的類似功能協同處理器與處理器比較起來，本發明之微處理器 101 直接執行在對應應用程式中的所有指令，不論此應用程式是否是儲存安全非揮發記憶體 107 之安全應用程式或者是透過系統匯流排 102 擷取之非安全應用程式。

接著參閱第 2 圖，狀態圖 200 說明在第 1 圖之微處理器中最高階級操作模式。在此最高階級中，微處理器 101 提供三個主要操作模式 201-203 與一個硬體關機模式 204。非安全執行模式 201 是在微處理器 101 製造後，當第一次供給電源時所默認(default)的第一個狀態。非安全執行模式 201 也稱為"原生未受控（born free）"模式 201。原生未受控模式 201 是微處理器 101 的製造狀態，其提供非安全應用程式的正常執行，其中，這些非安全應用程式係透過系統匯流排 102 而於系統記憶體中存取。在此狀態中，無法得知且無法操作任何與安全應用程式之安全執行相關聯之資源。這些資源包括 SEM 邏輯電路 105、安全非揮發記憶體 107 以及一些其他專用暫存器，這些專用暫存器包括含有對稱與非對稱加密金鑰、安全中斷、安全記憶體（RAM）以及其他硬體，將於下文詳細說明。藉由提供原生未受控模式 201，可實施與非安全微處理器所共通之製造行動類型(type of manufacturing activities)。此外，由於原生未受控模式 201 提供非安全應用程式的執行，因此本發明之微處理器 101 之相同的晶粒設計(the same die design)

可實施在非安全微處理器。在一實施例中，非安全微處理器之接腳配置（pinout）不同於 SEM 微處理器 101，且假使非安全微處理器配置在安全系統板 100 時，非安全微處理器之 SEM 邏輯電路 105 將因電源應用不同而無法操作。

在一實施例中，SEMENABLE(SEM 致能)指令之執行導致微處理器 101 的模式轉換為安全執行模式 202。在安全執行模式 202 下，安全與非安全應用程式都可執行，但是非安全應用程式無法存取安全資源。安全執行模式 202 也稱為 SEM-致能模式 202。在一安全應用程式的控制下(簡稱為程式控制)，微處理器之狀態可轉換回原生未受控模式 201，然而，轉換為原生未受控模式 201 之次數是有限的。在一實施例中，處理器轉換回原生未受控模式可高達 64 次。在另一實施例中，以可確認的授權者來對特殊(particular)機械專用暫存器（Machine Specific Register，MSR）進行寫入，導致微處理器 101 之模式轉換為安全執行模式 202。

SEM 邏輯電路 105 監控對應微處理器且與潛在篡改相關之狀態，並根據這些狀態之一使微處理器自安全執行模式 202 轉換至降級(操作)模式 203。假使某些已定義之狀態被 SEM 邏輯電路 105 偵測到，微處理器 101 自動地轉換為降級模式 203。在降級模式 203 中，允許執行 BIOS 指令，以提供使用者輸入與訊息的顯示的功能，但是更多複雜的軟體（例如操作系統）的執行則不被允許。在降級模式 203 中，在微處理器 101 之安全執行模式 202 的安全編碼操作被關閉，但是仍允許執行 BIOS 指令。在一實施例中，BIOS

指令係透過發出一外部中斷與傳遞狀態給該微處理器且經由一機械專用暫存器來執行。在 x86 相容的實施例中，在此降級模式 203 中實施 SMI 中斷以執行 BIOS 指令。

這些導致微處理器由安全執行模式 202 轉換為降級模式 203 之已定義狀態可以是執行安全編碼的結果、或是複數硬體偵測狀態、或是安全編碼執行結果與硬體偵測狀態之結合。此硬體偵測狀態包括與潛在安全暴露或篡改相關聯的監控狀態。在一實施例中，根據這些已定義狀態之一偵測結果，SEM 邏輯電路 105 試圖清除微處理器內一安全揮發記憶體之一資料區域，且試圖將偵測結果紀錄至安全非揮發記憶體 107。根據該資料區域之成功清除與該偵測結果之成功紀錄，SEM 邏輯電路 105 將微處理器轉換至降級模式 203。此外，執行在降級模式 203 之安全編碼，亦即在一安全應用程式的控制下(簡稱為程式控制)，微處理器之狀態轉換回安全執行模式 202。

某些與配置和完整性確認有關的已定義狀態可導致微處理器 101 轉換為硬體關機模式 204。在一實施例中，根據這些已定義狀態之一偵測結果，SEM 邏輯電路 105 試圖清除微處理器內一安全揮發記憶體之一資料區域、試圖將該偵測結果紀錄至安全非揮發記憶體 107、且使微處理器進入至硬體關機模式 204。在此硬體關機模式下，只可藉由重置微處理器來退出此硬體關機模式。在安全執行模式 202 或降級模式 203 中一安全應用程式之控制下(簡稱為程式控制)，微處理器 202 可進入硬體關機模式 204。

現在參閱第 3 圖，其表示在本發明實施例之微處理器

300 中的 SEM 邏輯電路 301 之詳細方塊圖。SEM 邏輯電路 301 包括授權的公開金鑰暫存器 318、處理器金鑰暫存器 312、SEM 初始化邏輯電路 305、SEM 監控邏輯電路 306、SEM 中斷邏輯電路 307、SEM 例外（exception）邏輯電路 308、SEM 計時器 309、SEM 實時時鐘（RTC)310、非揮發致能指示暫存器 328、SEM 機械專用暫存器記憶庫（bank）329 以及安全揮發記憶體 302。SEM 邏輯電路 301 耦接在微處理器 300 中的一些其他資源，包括透過匯流排 326 耦接非安全記憶體 325、透過匯流排 324 耦接位址邏輯電路 323、透過匯流排 320 耦接亂數產生器 319、透過匯流排 321 耦接 AES/HASH/RSA 單元 311、透過匯流排 327 耦接其他處理器執行單元 313(例如整數單元、浮點單元、MMX/SSE 單元）、耦接正常例外邏輯電路 314、耦接正常追蹤/除錯邏輯電路 315、耦接正常中斷邏輯電路 316 以及電源管理邏輯電路 322。

在一實施例中，由授權者提供公開金鑰，且微處理器 300 之製造期間中，公開金鑰永久地編程在授權的公開金鑰暫存器 318。在一實施例中，此公開金鑰為 1024 位元之 RSA 金鑰，且授權的公開金鑰暫存器 318 包括 1024 位元之熔絲庫(fuse bank)。因此，此公開金鑰可在微處理器 300 之製造期間被編程，而不是在製造之後。或者，公開金鑰藉由離線（off-line）大規模的初始化而被編程至安全非揮發記憶體 107，其中，此離線大規模的初始化是用來編程一些安全非揮發記憶體 107。致能與初始化安全執行模式 202 的能力是非常關鍵的安全操作，且木馬程式(Trojan

Horse)有可能被安裝(installation)進安全非揮發記憶體107。因此，利用提供公開金鑰的方法以避免窺察與篡改來控制安全執行模式初始化程序。

處理器金鑰暫存器 312 是複數熔絲的聚集體，其實際分佈在微處理器晶粒上。這些熔絲係在製造期間以獨特且隨機產生的狀態組來編程以形成處理器的獨特金鑰，其只可被 AES/HASH/RSA 單元 311(也可稱加密單元 311)來讀取，並無提供自處理器金鑰暫存器 312 讀取處理器金鑰的程式介面。在一實施例中，處理器金鑰暫存器 312 包括 128 個熔絲，這些熔絲被編程為 128 位元的 AES（Advanced Encryption Standard，AES）金鑰，而使用此 AES 金鑰來對安全非揮發記憶體 107 之內容進行加密與解密。即是，使用此處理器對稱金鑰來對安全編碼進行加密，以儲存在安全非揮發記憶體中。依據透過私密匯流排 106 來對安全編碼的擷取，來自處理器金鑰暫存器 312 之金鑰被使用來對安全編碼進行解密以進一步執行。因此，私密匯流排 106 之狀態的觀察者無法決定何者正在微處理器 300 與非揮發記憶體 107 之間轉移。

在一實施例中，處理器金鑰暫存器 312 包括 128 熔絲，其隨機地分佈在微處理器 300 中一熔絲庫內的許多其他熔絲之中。此熔絲庫配置在微處理器晶粒上一些金屬層的下方。

根據 SEMENABLE 指令之執行或其他進入安全執行模式 202 的預期機制，SEM 初始化邏輯電路 305 提供安全執行模式 202 之初始化。為了詳細說明，下文將以用來致能

且執行來自安全執行模式 202 的指令(例如 SEMENABLE)執行的方式來說明根據本發明之微處理器 300 之操作，然而，此技術領域之人士將理解有其他方法能致能安全執行模式 202 並執行來自安全執行模式之安全編碼，例如對一隱密暫存器(hidden register)寫入等等。根據 SEMENABLE 指令之執行成功，SEM 初始化邏輯電路 305 將微處理器 300 之狀態記錄在非揮發致能指示暫存器 328。由安全執行模式 202 轉換至原生未受控模式 201 時，SEM 初始化邏輯電路 305 將微處理器 300 之狀態(安全執行模式被致能之狀態)記錄在非揮發致能指示暫存器 328。亦即，非揮發致能指示暫存器 328 用以指示微處理器 300 是否處於安全執行模式或一非安全執行模式。在微處理器之電源移除與重新施加的期間，非揮發致能指示暫存器 328 之內容持續存在。在一實施例中，非揮發致能指示暫存器 328 包括配置在微處理器 300 內之複數熔絲，且微處理器 300 可由安全執行模式 202 轉換至原生未受控模式 201 的次數係對應在這些熔絲中的一特定熔絲數量。微處理器 300 包括配置在一單一晶粒上之一單一積體電路。在一實施例中，SEM 邏輯電路根據進入至該安全執行模式而對非揮發致能指示暫存器 328 進行第一次寫入，以指示出微處理器處於安全執行模式。SEM 邏輯電路根據退出該安全執行模式而對非揮發致能指示暫存器 328 進行第二次寫入，以指示出微處理器處於該非安全執行模式(原生未受控模式)。

SEM 監控邏輯電路 306 係用來監控安全編碼與資料的誠實性，以監控系統的環境與物理屬性，包括溫度、電壓、

匯流排頻率、電池 VP 的存在、石英器 X1 的存在以及安全非揮發記憶體 107 的存在。SEM 監控邏輯電路 306 將篡改或疑似的篡改情況指示給 SEM 邏輯電路 301，其導致微處理器 300 轉換至降級模式 203 或硬體關機模式 204。

SEM 中斷邏輯電路 307 提供複數中斷與相關的中斷邏輯裝置（例如安全中斷描述符號表單（Interrupt Descriptor Table，IDT）），這些只顯現給正在安全執行模式 202 下執行的安全應用程式，且由此安全應用程式來存取。中斷安全編碼執行的機制類似於執行正常模式的機制。亦即，依據 SEM 中斷的設置(assertion)，且藉由 SEM IDT 的出現使得安全編碼狀態被保存並轉移至安全中斷管理者(secure interrupt handler)。由中斷指令的恢復(return)執行將控制權恢復至安全編碼中的中斷點。當微處理器 300 正操作在安全執行模式時，SEM 中斷邏輯電路 307 提供安全中斷以中斷安全應用程式。SEM 中斷邏輯電路 307 不被系統匯流排資源或非安全應用程式所得知或存取。當微處理器 300 正操作在非安全執行模式時，微處理器 300 之正常中斷邏輯電路 316 提供非安全中斷以中斷非安全應用程式。

同樣地，SEM 例外邏輯電路 308 提供複數安全例外與相關的例外管理邏輯裝置。當該微處理器正操作在安全執行模式 202 時，SEM 例外邏輯電路 308 提供複數安全例外並禁能複數非安全例外。SEM 例外邏輯電路 308 無法被該等系統匯流排資源或該等非安全應用程式所得知或存取，其只顯現給正在安全執行模式 202 下執行的安全應用程式，且由此安全應用程式來存取。所有安全編碼程式例外

與中斷係利用預設的 IDT，此預設 IDT 存在於 SEM 中斷邏輯電路 307 內，以在中斷與例外期間內控制分支。在一實施例中，根據該等安全例外之一者的致能，微處理器之狀態被儲存且程式控制轉移至一對應安全例外管理者，其中微處理器之狀態無法被該等非安全應用程式所存取。在安全應用程式執行之前，SEM 邏輯電路 301 禁能正常例外邏輯電路 314，以及當微處理器 300 正操作在非安全執行模式時，正常例外邏輯電路 314 提供對應該等非安全應用程式之複數非安全例外。在一實施例中，假使在該等非安全應用程式之任一者執行的期間發生該等安全中斷之任一者或該等安全例外之任一者，微處理器之狀態被儲存且微處理器 300 進入安全執行模式。

這些安全中斷係配置來提供微處理器 300 外部事件所導致的程式控制轉移，例如鍵盤事件、I/O 埠事件等等。安全例外是用來提供微處理器 300 內部事件所導致的程式控制轉移，例如非定義的運算碼（opcode）、機械檢查錯誤(machine check errors)、以及在一實施例中對一或多個安全機械專用暫存器記憶庫 329 的安全編碼寫入。IDT 包括複數安全暫存器，其被載入複數指標，而這些指標是指向在安全編碼中的安全中斷管理者與安全例外管理者(secure exception handler)。IDT 提供轉移至該安全應用程式內之複數安全中斷管理者與複數安全例外管理者)的程式控制。此預設 IDT 包括關於程式控制轉移至該微處理器將執行的一安全執行模式重置操作的資料。在一實施例中，根據該等安全中斷之一者的致能，該微處理器之狀態被儲存且程式

控制轉移至一對應安全中斷管理者，以及該微處理器之狀態無法由該等非安全應用程式來存取。在一實施例中，根據該等非安全中斷之一者的致能，該微處理器之狀態被儲存且程式控制轉移至一對應非安全中斷管理者，以及該微處理器之狀態無法由該等非安全應用程式來存取。

SEM 計時器 309 是只顯現給正行在安全執行模式 202 下執行的安全應用程式且由此安全應用程式來存取的複數計時器。SEM 計時器 309 包括複數中斷，而這些中斷可由操作在安全執行模式 202 下之安全編碼來存取。SEM 實時時鐘 310 其提供持續時間(persistent time)，其只顯現給正在安全執行模式 202 下執行的安全應用程式且由此安全應用程式來存取。SEM 實時時鐘 310 的值無法由不同於操作在安全執行模式 202 下的安全編碼的任何物件來改變。SEM 機械專用暫存器記憶庫 329 包括複數機械專用暫存器，且這些機械專用暫存器只顯現給正在安全執行模式 202 下執行的安全應用程式且由此安全應用程式來存取。這些機械專用暫存器用來致能對安全非揮發記憶體 107、SEM 實時時鐘 310 以及 SEM 計時器 309 之載入/儲存存取。

非安全記憶體 325 係作為給正在執行之非安全應用程式的指令與資料快取記憶體(instruction and data cache)。非安全記憶體 325 用以儲存複數非安全應用程式以由微處理器來執行。在微處理器 300 內之這些程式與其他系統匯流排資源可得知且存取非安全記憶體 325。安全揮發記憶體 302 係作為給正在安全執行模式 202 下執行之安全應用程式的一指令與資料快取記憶體。進入至安全執行模式 202，

安全揮發記憶體 302 之一堆疊（stack）係提供來儲存處理器狀態 303，其用於對應該等非安全應用程式之該微處理器之狀態的儲存與取回。安全揮發記憶體 302 之其他堆疊係提供來儲存安全編碼 304 與對應安全編碼之安全資料 317。安全揮發記憶體 302 根據微處理器的重置而被清除，且其完全地隔離於系統匯流排，因此，安全揮發記憶體 302 無法被非安全系統資源窺察、載入、除錯或其他方法的存取。安全編碼(安全應用程式)可使用正常處理器載入與儲存指令來存取安全揮發記憶體 302，以載入/儲存安全資料 317，其中，這些正常處理器載入與儲存指令是參考位址邏輯電路 323 內的正常片段暫存器(normal segment register)，此正常片段暫存器是當於安全揮發記憶體 302(而不是正常系統記憶體）進入至安全執行時而被初始化。此正常系統記憶體也被執行在安全執行模式之安全編碼，透過位址邏輯電路 323 且使用正常載入與儲存指令來存取。然而，根據安全編碼的執行，SEM 邏輯電路 301 透過匯流排 324 來命令位址邏輯電路 323 以停止虛擬位址轉譯。亦即，因為虛擬-實體位址轉譯係為了指令與資料而被禁能，因此，透過匯流排 324 且由安全編碼所提供之位址必須為實體位址。藉由這種作法，SEM 邏輯電路阻止了分頁錯誤，藉以消除此篡改來源。

在一實施例中，安全揮發記憶體 302 完全地屬於在微處理器 300 內的晶片上（on-chip）快取記憶體，但安全揮發記憶體 302 快取線具有將這些快取線完全地隔離於微處理器匯流排的特定內部屬性。這些快取線沒有耦接至外部

系統記憶體，因此這些快取線無法自系統記憶體裝載或存入至系統記憶體，這些快取線也無法被任何匯流窺探資源來外部地或內部地窺察。

在一實施例中，安全揮發記憶體 302 包括 4K 64 位元快取線。在安全揮發記憶體 302 中，一快取線係依據由將資料移動至先前沒有涉及(referenced)之一快取線來分配。在一實施例中，安全揮發記憶體 302 包括具有 4096 個位置之一 64 位元快取記憶體，該等位置之每一者包括一內部屬性，且該內部屬性完全地隔離該等位置之每一者。

在另一實施例中，安全揮發記憶體 302 包括隨機存取記憶體，其與微處理器 300 內之晶片上快取記憶體分離。

SEMENTER 指令之執行提供了安全執行模式 202 內安全編碼的執行。在一 x86 相容之實施例中，安全執行模式 202 根據修改的 32 位元 x86 真實模式來提供安全編碼的執行。在執行安全編碼時，禁止由安全執行模式 202 進入一 x86 保護模式。在安全執行模式執行之前，SEM 初始化邏輯電路 305 藉由設置一致能信號 DISIL 來禁能正常（即非安全）中斷邏輯電路 316。在安全執行模式執行之前，SEM 初始化邏輯電路 305 也藉由設置一致能信號 DISEL 來禁能正常（即非安全）例外邏輯電路 314，也藉由設置一致能信號 DISDL 來禁能正常（即非安全）追蹤/除錯邏輯電路 315。此外，在安全執行模式執行之前，電源管理邏輯電路 322 藉由信號 DISPML 的設置而被禁能。透過這些安全措施，不會發生正常匯流排中斷，阻止了除錯例外、避免匯流排追蹤週期、且禁能除錯輸出入埠。此外，信號 DISIL

係用來在安全編碼的執行期間內禁能所有的剩餘處理器資源（例如 JTAG、探測模式、快取測試）。否則，電源管理邏輯電路 322 允許微處理器 300 進入降低功耗狀態，例如在 x86 相容實施例中的 P 狀態與 C 狀態。因此，信號 DISPML 係用來在安全編碼執行期間避免功耗狀態的轉換。

透過匯流排 320、321 及 327，安全編碼可存取處理器執行單元(處理器 300 內的執行單元)313、亂數產生器 319 與 AES/HASH/RSA 單元 311，以執行微處理器指令集的所有指令，其中，這些指令包括真實亂數之硬體產生且可由編程的巨集指令來使用的硬體實施功能，以執行 RSA 加密、解密以及識別核對；AES 加密與解密、以及 SHA-1/SHA-256 雜湊產生(Secure Hash Algorithm，SHA，安全雜湊演算法)。這些硬體實施功能係由 AES/HASH/RSA 單元 311 來執行。

現在參閱第 4 圖，圖示 400 表示在本發明之微處理器內安全編碼如何被儲存、存取及初始化。圖示 400 說明能進行安全執行模式（SEM）之微處理器 401，其透過系統匯流排 425 而耦接 BIOS 記憶體 410 與系統記憶體 420。根據本發明，微處理器 401 也透過私密匯流排 431 而耦接至安全非揮發記憶體 430。微處理器 401 包括安全編碼介面邏輯電路 402，其耦接至亂數產生器 412、處理器金鑰暫存器 413、授權的公開金鑰暫存器 404、AES/HASH/RSA 單元 405（或稱加密單元 405）、安全揮發記憶體 406、SEM 監控邏輯電路 408 以及 SEM 初始化邏輯電路 409。安全編碼介面邏輯電路 402 另外耦接匯流排介面單元 403 與安全

非揮發記憶體介面單元 407。

圖示 400 也表示儲存在系統記憶體 420 與 BIOS 記憶體 410 之安全編碼 411 及 421。在一實施例中，儲存在 BIOS 記憶體 410 之安全編碼 411 主要是用來提供微處理器 401 在降級模式 203 中的操作，而儲存在系統記憶體 420 之安全編碼 421 是用來提供微處理器 401 在安全執行模式 202 中的操作。

在操作上，圖示 400 所示之元件的運作，實質上相似於先前參閱第 1-3 圖而已敘述之相似名稱元件。參閱第 4 圖之討論目的是為了更加明確集中注意在那些元件與技術，而那些元件與技術是用來儲存、存取、初始化、執行在本發明之安全環境中的安全編碼。

此外，關於安全編碼執行的環境是隔離於非安全編碼執行的環境。如先前所述，原生未受控模式 201 只允許非安全編碼的執行。安全執行模式則允許非安全編碼與安全編碼兩者的執行。在安全編碼 421 執行之前，微處理器 401 之狀態被保存。根據回到非安全編碼的執行的轉換，此狀態恢復(restored)。此狀態儲存在安全揮發記憶體 406 內的一個區域，且此狀態不會出現在微處理器匯流排 425 上。此外，安全編碼 411、421 是執行自安全揮發記憶體 406。除了將安全揮發記憶體 406 隔離於與微處理器匯流排 425 聯繫之硬體與軟體，所有其他"從屬通道(side channels)"(例如除錯例外與執行追蹤特徵）被禁能，如關於第 1-3 圖之討論。安全編碼 411、421 只提供給 SEM 中斷邏輯電路 307、SEM 例外邏輯電路 308、SEM 實時時鐘 310、SEM 計時器

310 以及只可由安全編碼 411、421 利用的其他處理器資源獨佔存取。

此外，微處理器 401 提供 SEM 監控邏輯電路 408，其包括之非同步監控與監視機制，其中，此非同步監控與監視機制獨立於安全編碼 411、421 以及非安全編碼的執行。SEM 監控邏輯電路 408 監控微處理器的環境（例如電壓、溫度、匯流排運作）與物理特性，也核對安全編碼 411、421(安全應用程式)與相關資料之誠實性，將於下文詳細說明。當偵測到安全暴露(security exposure)時，SEM 監控邏輯電路 408 可透過匯流排 CHK 將程式控制轉移至安全編碼 411、421 之安全編碼錯誤管理裝置(secure-code error handler)，或者，在偵測到嚴重的安全暴露情況下，SEM 監控邏輯電路 408 將透過匯流排 CHK 來使微處理器 401 進入降級模式 203。

在一實施例中，安全編碼介面邏輯電路 402 監控存在於安全編碼 411、421 中的複數指令，且透過匯流排 INS 將這些指令提供至 SEM 監控邏輯電路 408，以支援微處理器 401 之限定的指令集架構（Instruction set Architecture，ISA）操作。根據此實施例，當微處理器 401 正操作在安全執行模式時，本發明之微處理器 401 只被允許執行主機 ISA 中的某些指令。即是，限定的 ISA 操作使得 SEM 邏輯電路阻止複數非安全指令的執行，而此非安全指令的執行是授權者欲阻止的，且該些非安全指令包括取自對應微處理器之一指令集架構的一或多個運算碼。舉例來說，在 x86 相容之實施例中，超過 100 個微指令的產生與執行的指令或

某類指令要求會被阻止。另一方面，當微處理器 401 正操作在安全執行模式時，一授權者可能期望阻止所有指令的執行，例如任務切換、呼尋閘(call gates)等等。藉由將安全編碼 411、421 內每一指令提供給 SEM 監控邏輯電路 408，本發明之微處理器 401 致能限定的 ISA 操作。在一實施例中，在限定的 ISA 指令集中的指令（即提供在安全執行模式下執行的指令），係由 SEM 監控邏輯電路 408 內指令陣列（未顯示）之值來表示，將於下文詳細說明。當遭遇到上述被阻止的指令時，SEM 監控邏輯電路 408 使微處理器 401 進入降級模式 203。

在一實施例中，安全編碼介面邏輯電路 402 將安全編碼 411、421 中的指令提供給 SEM 監控邏輯電路 408，提供時將安全編碼 411、421 載入至安全揮發記憶體 406 以進行後續執行。

致能與初始化安全執行模式 202 的能力是非常關鍵的安全操作，此外，其表示了關於木馬程式(Trojan Horse)安裝有可能進入至包含安全編碼 411、421 的記憶體 410、420 之區域。透過非對稱加密演算法與一組對應的非對稱加密金鑰的使用，本發明之微處理器 401 藉由控制安全執行模式初始化程序而有利地阻止此暴露。在一實施例中，非對稱金鑰演算法是 RSA 演算法，且對應金鑰則是由授權者所產生之 1024 位元 RSA 公開與私密金鑰。在一實施例中，此授權者或授權物件(entity)提供執行的安全編碼 411、421。如前文關於第 3 圖之說明，在微處理器 401 之製造期間，兩金鑰中之一者儲存在授權的公開金鑰暫存器 318，

且用來根據非對稱金鑰演算法來對資料解密，其中，此資料已由授權者之其他非對稱金鑰（即私密金鑰）來加密。

因此，在一實施例中，此操作系統執行 SEMENABLE 指令（或相似機制）。此指令傳送透過授權者之私密金鑰來加密的一 SEM 致能參數。安全編碼介面邏輯電路 402 接著透過授權的公開金鑰暫存器 404 來存取公開金鑰，且利用 AES/HASH/RSA 單元 405 來對此 SEM 致能參數解密。根據核對 SEM 致能參數，SEM 初始化邏輯電路 409 初始化安全執行模式 202，亦即致能安全執行模式 202 以執行安全應用程式。除此之外，SEM 初始化邏輯電路 409 指示微處理器 401 自 SEMENABLE 指令恢復(return)後，微處理器 401 保持在非安全執行模式 201。在一實施例中，無論是否接受進入安全執行模式 202 的授權(以及有一對應錯誤狀態時，假使有的話)都會提供一回應編碼(return code)。

相對於在微處理器 401 之製造期間將授權的公開金鑰直接編程至授權的公開金鑰暫存器 404，在另一實施例中，授權者將授權的公開金鑰編程至安全非揮發記憶體 430 之授權的公開金鑰區域 432。因此，當微處理器 401 開機(power up)時，安全非揮發記憶體介面單元 407 自此區域 432 偵測並擷取此公開金鑰。安全編碼介面邏輯電路 402 接著將此金鑰以及之後指示此金鑰已被燒錄之參數，燒錄至授權的公開金鑰暫存器 404。此供選擇的實施例在安全非揮發記憶體 430 的製造階段上，提供了更彈性地公開金鑰配置。安全非揮發記憶體介面單元 407 透過私密匯流排 431 將微處理器 401 耦接至安全非揮發記憶體 430，其中，

在私密匯流排 431 上用來存取安全非揮發記憶體 430 之複數私密匯流排資料傳輸被隱藏，以避免被微處理器 401 內複數系統匯流排資源以及耦接該系統匯流排之任何裝置所得知察覺。

安全非揮發記憶體介面單元 407 是由安全編碼介面邏輯電路 402 所管理。根據核對一 SEM 致能參數，安全非揮發記憶體介面單元 407 藉由執行亂數寫入來清除安全非揮發記憶體 430 的內容。在一實施例中，在安全非揮發記憶體 430 中的每一個位置以亂數寫入 64 次。在一實施例中，每次寫入之亂數是由亂數產生器 412 所產生。

SEMENABLE 指令（或是 SEM 致能機制）也傳送關於安全編碼 411、421 在 BIOS 記憶體 410 或系統記憶體 420 之位置的指標和任何初始安全資料(亦即致能參數)。此指標與資料(亦即致能參數)是根據一預設結構來被格式化，且根據非對稱金鑰演算法而被加密。被加密的指標與資料被解密，且格式化被核對。不成功的核對導致錯誤碼的回應。

假使在結構方面此指標與資料被確認且證實，安全編碼介面邏輯電路 402 則指示匯流排介面單元 403 去自 BIOS 記憶體 410 以及/或系統記憶體 420 擷取安全編碼 411 及 421。安全編碼 411、421 也已藉由使用授權者的私密金鑰並根據非對稱金鑰演算法而被加密，且必須與預設結構相稱。安全編碼介面邏輯電路 402 利用授權的公開金鑰暫存器 404 與 AES/HASH/RSA 單元 405 來對加密的安全編碼 411、421 進行解密。在核對為正確格式後，安全編碼介面

邏輯單元 402 利用 AES/HASH/RSA 單元 405 來根據對稱加密演算法並使用處理器金鑰暫存器 413 之內容（作為對稱金鑰）來對安全編碼與資料進行加密。如前所提及，處理器金鑰暫存器 413 之內容是微處理器 401 所特有的 128 位元隨機產生的金鑰，且對稱加密演算法包括使用 128 位元模塊(blocks)以及電子密碼書（Electronic Code Book，ECB）模式的高級加密標準（AES）。此對稱加密的安全編碼接著透過安全非揮發記憶體介面單元 407 而被寫入至安全非揮發記憶體 430。此外，安全編碼介面邏輯電路 402 利用 AES/HASH/RSA 單元 405 與處理器金鑰暫存器 413 來產生安全編碼中已選擇部分之複數雜湊，安全編碼介面邏輯電路 402 對這些雜湊進行加密編碼並寫入至安全非揮發記憶體 430。在一實施例中，這些雜湊是根據 SHA-1 演算法而產生。

此外，SEM 初始化邏輯電路 409 禁能 JTAG、探測模式、快取測試、或者禁能透過第 3 圖所討論之機制而提供安全編碼監視的其他處理器特性。

當被編碼且被雜湊之安全編碼已寫入至安全非揮發記憶體 430，微處理器 401 設定非揮發致能指示暫存器（如第 3 圖中 328 所示）指示出處理器 401 正操作於安全執行模式 202 且 SEM 初始化邏輯電路 409 迫使微處理器 401 執行一重置序列(RESET sequence)。

部分的重置序列導致非揮發致能指示暫存器的內容被讀取，且假使這些內容指示出處理器 401 處於安全執行模式 202 中，則執行安全執行模式 202 所特有的額外操作。

因此，安全編碼 411、421 起初被加密，且由授權者載入至記憶體 410、420。當安全執行模式被致能時，微處理器 401 根據非對稱金鑰演算法並使用授權者所提供之金鑰來擷取且核對安全編碼。接著使用處理器獨特金鑰並根據對稱金鑰演算法來加密且雜湊此編碼，且對稱加密之編碼透過私密匯流排 431 而被寫入至安全非揮發記憶體 430。

以下將進一步詳細說明，當安全編碼將被執行時，安全編碼由安全非揮發記憶體介面單元 407 自安全非揮發記憶體 430 被擷取，且使用存放於處理器金鑰暫存器 413 之處理器金鑰來解碼，且安全編碼被寫入至微處理器 401 內的安全揮發記憶體 406，其中，安全揮發記憶體 406 完全隔離於所有可窺探其內容的硬體及或軟體。安全揮發記憶體 406 之功能包含可存放安全應用程式執行的指令與資料快取記憶體。

在一實施例中，安全非揮發記憶體介面單元 407 包括複數機械專用暫存器，其專有地顯現給安全編碼，這些機械專用暫存器允許一安全應用程式（或安全編碼介面邏輯電路 402）去執行對安全非揮發記憶體 430 的載入與儲存。即是，根據此實施例，藉由執行對隱藏機械專用暫存器的讀取與寫入，來執行對安全非揮發記憶體 403 的讀取與寫入。

授權者可有利地將微處理器 401 之安全操作與安全執行模式環境結合，且由於透過系統匯流排 425 與私密匯流排 431 之資料傳輸被加密，因此安全編碼之結構與功能則被保護以避免任何的反向工程與其他窺察/侵入技術。

現在參閱第5圖，其表示在第1圖之微處理器中之SEM監控邏輯電路500之詳細內容。SEM監控邏輯電路500包括物理環境監控器501，其透過信號PSNT耦接安全非揮發記憶體107、透過信號VP1與VP2耦接電池VP，且透過信號C1與C2耦接石英器。此物理環境監控器501透過匯流排NOBOOT提供一輸出信號。

SEM監控邏輯電路500也包括匯流排時脈監控器502，其具有頻率參考單元503。匯流排時脈監控器502透過信號BUS CLK耦接提供至微處理器的匯流排時脈，且匯流排時脈監控器502之輸出係耦接匯流排TAMPER。

SEM監控邏輯電路500也包括處理器電壓監控器504，其透過信號VDD與BUSTERM耦接電源供應電壓與複數匯流排終端電壓，其中，電源供應電壓與匯流排終端電壓係由系統板提供至微處理器。SEM監控邏輯電路500也包括溫度監控器505，其透過信號TEMP耦接至處理器溫度感測邏輯電路（未顯示）。SEM監控邏輯電路500更包括資料監控器506，其透過匯流排CHK耦接至安全編碼介面邏輯電路402。匯流排時脈監控器502、處理器電壓監控器504、溫度監控器505以及資料監控器506之輸出信號則耦接至匯流排TAMPER。

SEM監控邏輯電路500更包括安全時戳計數器(security time stamp counter)507，其耦接正常時戳計數器(normal time stamp counter)508、信號CORE CLK以及比率（Ratio）機械專用暫存器509。安全時戳計數器507之輸出信號耦接匯流排TAMPER。

SEM 監控邏輯電路 500 也包括指令監控器 511，其耦接指令陣列 512 與匯流排 INS。如關於第 4 圖的討論，當微處理器正執行在安全執行模式時，在安全應用程式內的指令被提供至 SEM 監控邏輯電路 500，以支援在主機 ISA 內限制的指令執行。指令監控器 511 的輸出信號耦接至匯流排 TAMPER。

最後，SEM 監控邏輯電路 500 具有樣式監控器 510，其耦接匯流排 PINCHK，且在匯流排 DESTRUCT 上產生一輸出信號。

匯流排 NOBOOT、TAMPER 以及 DESTRUCT 耦接於監控管理器 513。在一實施例中，監控管理器 513 產生信號 CLASS1、CLASS2、CLASS3 以及 DISABLE。

在操作上，SEM 監控邏輯電路 500 用來執行硬體與軟體檢驗，其監控本發明微處理器之物理與暫時的屬性，以偵測、識別以及分類操作事件(operating events)，其中，操作事件是表示對於安全編碼而言不安全的操作環境，例如改變或移除電池、石英器或者安全非揮發記憶體；以本發明之不安全的微處理器來取代本發明之安全微處理器；修改匯流排時脈頻率；篡改微處理器電源供應電壓 VDD；修改在系統記憶體、BIOS 記憶體或安全非揮發記憶體內的加密安全編碼；以及發生對安全編碼本身的過度呼尋(excessive calls)。

因此，當操作在安全執行模式時，物理環境監控器 501 耦接安全非揮發記憶體 107，藉由監控信號 PSNT 之狀態來判斷安全非揮發記憶體 107 是否移除。信號 PSNT 之禁能

（de-assertion）表示移除安全非揮發記憶體 107。同樣地，監控信號 VP1 與 VP2 來判斷電池電壓是否改變或電池被移除或者判斷對應該電池之電壓是否被充電。在一實施例中，VP1 之值與電池電壓成比例。同樣地，信號 C1 與 C2 之狀態係表示石英器的存在與否。假使物理環境監控器 501 偵測到上述的任何變化，此變化則輸出至匯流排 NOBOOT。

此外，當操作在安全執行模式 202 時，匯流排時脈監控器 502 估計信號 BUS CLK 之頻率，以判斷系統匯流排時脈的短期與長期完整性，其中，系統匯流排時脈透過系統板而提供至微處理器。此匯流排時脈透過信號 BUS CLK 被路由(routed)至匯流排時脈監控器 502，匯流排時脈監控器 502 使用內部相位鎖相迴路（未顯示）來檢驗短期匯流排時脈誤差，其中，內部相位鎖相迴路與匯流排時脈同步化且用來產生內部時脈給微處理器。匯流排時脈監控器 502 判斷匯流排時脈於不適當的週期是否維持平坦，或者判斷時脈變化是否已超出可接受的程度(例如一特定範圍)。在一實施例中，超過百分之六之變化視為是無法接受的。此外，匯流排時脈監控器 502 使用頻率參考單元 503 來作為溫度與電壓非相依的中間速度震盪器電路。頻率參考單元 503 產生與系統匯流排時脈成比例之一參考頻率。匯流排時脈監控器 502 比較系統匯流排時脈的衍生(derivative)與時脈參考單元 503 之輸出(參考頻率)，以判斷匯流排時脈之頻率是否已經歷逐步(gradual)的頻率變化。假使任何上述事件發生，此事件透過匯流排 TAMPER 報導給監控管理器 513(SEM 邏輯電路 301)，其將導致微處理器進入降級模

式或進入硬體關機模式 204。

處理器電壓監控器 504 估計透過信號 VDD 與 BUSTERM 來提供且施加於微處理器之電源供應電壓與複數匯流排終端電壓。上述電壓之高低限制係透過機械專用暫存器（未顯示）來編程。一但電源供應電壓與複數匯流排終端電壓偏離這些編程限制，處理器電壓監控器 504 將透過匯流排 TAMPER 來報導(report)此事件給監控管理器 513。

溫度監控器 505 包括精準的熱監控機制（除了正常熱監控功能以外），其在預設高與低溫度限制下不斷地監控晶粒溫度。該晶粒溫度之一低溫度限制與一高溫度限制係藉由溫度監控器 505 內一機械專用暫存器來編程。此高與低溫度限制儲存在溫度監控器 505 內機械專用暫存器中，其中，這些機械專用暫存器可被安全編碼寫入。一但該晶粒溫度偏離上述預設高與低溫度限制，溫度監控器 505 將透過匯流排 TAMPER 來報導此事件給監控管理器 513。

資料監控器 506 用來當自安全非揮發記憶體擷取該安全應用程式時，用以偵測與報導於安全編碼和安全資料相關的複數加密與配置錯誤。這些複數加密與配置錯誤透過匯流排 TAMPER 來報導給監控管理器 513。舉例來說，這些錯誤為與 SEMENABLE 及 SEMENTER 指令之執行相關之錯誤、當自記憶體擷取安全編碼時所偵測到之解密錯誤、以及在安全編碼中雜湊與格式錯誤。

安全時戳計數器 507 耦接一核心時脈信號 CORE CLK，用來計算當安全編碼正執行時的核心時脈信號 CORE

CLK之週期數。安全時戳計數器507耦接一正常時戳計數器508。正常時戳計數器508則是在非安全編碼或安全編碼執行期間內計算信號CORE CLK之週期數。當安全應用程式正在執行時或當安全應用程式非正在執行時，正常時戳計數器508計算信號CORE CLK之週期數。安全時戳計數器507也耦接一比率機械專用暫存器509，比率機械專用暫存器509只由該安全應用程式所得知且存取。安全執行模式執行期間，安全編碼可對比率機械專用暫存器509執行一機械專用暫存器寫入，以建立介於正常時戳計數器508與安全時戳計數器507之數值之間的一最大比例(maximum ratio)。此最大比例係指示該安全應用程式已被呼尋之次數。假使超過此最大比例，藉此指示出安全編碼已被呼尋多於指定次數，接著，安全時戳計數器507透過匯流排TAMPER報導此事件(最大比例何時被超過)給監控管理器513。亦即，安全時戳計數器507用以比較信號CORE CLK週期數與正常時戳計數器508之數值、且將上述最大比例被超過之事件報導給監控管理器513。上述最大比例係藉由SEM邏輯電路內之一機械專用暫存器來編程。

指令監控器511在與主機ISA內指令子集的對照下用來確認在安全應用程式內的指令，且指示出在此安全應用程式內且非在此子集內的指令何時已被編程以進行後續執行。提供來在安全執行模式內執行的指令子集是由指令陣列512之數值來表示。在一實施例中，此子集包括在ISA內的一或多個特殊指令，如運算碼(opcode)所識別。在另一實施例中，此子集包括一或多個指令種類，如一微碼

(microcode)複雜數值所識別。在一第三實施例中，此子集包括一或多個標籤編碼(tag codes)，每一者與一或多個指令運算碼相關聯。

指令陣列 512 耦接該指令監控器 511，用以識別對應微處理器之一指令集架構內的一所有指令之子集，該子集包括允許在一安全執行模式內執行的指令。用來在安全執行模式下執行的指令子集由指令陣列 512 之數值來識別。在一實施例中，此指令陣列 512 包括一機械專用暫存器，其初始地由安全應用程式來寫入。在另一實施例中，指令陣列 512 包括複數熔絲，其在製造期間被編程(燒斷)。

在安全執行模式之初始化期間，當安全編碼正由安全非揮發記憶體傳送至安全揮發記憶體以進行後續執行時，對應安全編碼內每一特定指令之數值係由安全編碼介面邏輯電路 402 透過匯流排 INS 而提供至指令監控器 511。在一實施例中 INS 之數值表示每一特定指令對應微處理器之一指令集架構內的之特定運算碼或是運算碼子集。在另一實施例中，此數值表示這些指令的種類（例如簡單、複雜等等）。在又一實施例中，此數值是對應在 ISA 內一或多個指令的標籤。

在另一實施例中，於安全編碼之執行之前，當安全非揮發記憶體正被編程時，在安全編碼內每一指令之數值由安全編碼介面邏輯電路 402 透過匯流排 INS 來提供。

指令監控器 511 比較 INS 之數值與指令陣列 512 之數值，以判斷是否允許執行特定指令。假使不允許的話，指令監控器 511 則設置信號於匯流排 TAMPER。

樣式監控器 510，耦接匯流排 DESTRUCT，是偵測本發明之微處理器的非安全版本對系統板的安裝，其中，此系統板是配置給本發明之安全微處理器。在一實施例中，非安全微處理器與安全微處理器具有相異的接腳配置（pinout）。在此兩版本之間相異的特定腳位之狀態係透過匯流排 PINCHK 作為樣式監控器 510 之輸入信號。樣式監控器估計匯流排 PINCHK 之狀態，且假使判斷出此非安全版本被安裝時，則透過匯流排 DESTRUCT 來報導此事件給監控管理器 513。亦即，匯流排 DESTRUCT 提供對應微處理器之特定複數接腳配置之複數狀態，且樣式監控器 510 則估計上述複數狀態以判斷微處理器是否配置一安全版本來操作在該安全執行模式中。

監控管理器 513 藉由注意與估計透過匯流排 NOBOOT、TAMPER 及 DESTRUCT 傳遞之資料，來動態地監控微處理器之物理與操作環境。監控管理器 513 對上述資料進行分類以指示出與安全應用程式之執行相關的安全層級，且使微處理器內之 SEM 邏輯電路根據安全層級來執行反應操作。對安全應用程式之執行而言，SEM 監控邏輯電路 500 包括非同步監控、監視機制與監控器等係獨立地操作。以下某些情況將導致信號 CLASS1 的設置，例如透過匯流排 TAMPER 報導之匯流排 BUS CLK 之頻率的短暫誤差。SEM 邏輯電路響應於 CLASS1 之設置而將此事件紀錄(log) (偵測信號 CLASS1 之設置)至安全揮發記憶體內的安全事件紀錄表，且發出一中斷給安全編碼。假使此中斷沒有被收到(acknowledged)，則監控管理器 513 設置信號

CLASS3。

假使偵測到會導致信號 CLASS1 設置的複數事件（多於一個事件），例如 BUS CLK 之誤差與 VDD 之誤差，監控管理器 513 則設置信號 CLASS2。SEM 邏輯電路則試圖清除安全揮發記憶體之資料區域，且試圖將此事件記錄至安全非揮發記憶體。此外，檢查在 BIOS 之安全編碼的雜湊。假使安全揮發記憶體之資料區域成功清除且此事件(偵測信號 CLASS2 之設置)被紀錄，且假使 BIOS 雜湊被正確地證明，SEM 邏輯電路則開始轉換至降級模式 203。此降級模式提供有限的功能、錯誤顯示以及有限的使用者輸入之相關指令。這些動作中任一者的錯誤會導致信號 CLASS3 之設置。

信號 CLASS3 之設置表示有安全侵害。響應於信號 CLASS3 之設置，SEM 邏輯電路持續試圖清除安全揮發記憶體且試圖將此事件(偵測信號 CLASS3 之設置)記錄至安全非揮發記憶體，此外，使微處理器進入硬體關機模式 204，即微處理器停止操作。

在一實施例中，監控管理器 513 判斷樣式監控器 510 是否已設置信號 DESTRUCT，因此指示出本發明微處理器的非安全版本的安裝。假使信號 DESTRUCT 被設置，且假使在匯流排 NOBOOT 上的資料指示出石英器與安全非揮發記憶體存在時，信號 DISABLE 則被設置。響應於信號 DISABLE 之設置，SEM 邏輯電路使非安全之微處理器停止操作。

以上關於監控管理器 513 設置信號 CLASS1、

CLASS2、CLASS3 以及 DISABLE 皆係用來將程式控制轉移至安全應用程式內複數事件管理者之一，例如有安全侵害時，信號 CLASS3 被設置，SEM 邏輯電路則持續嘗試清除安全揮發記憶體且將此事件記錄至安全非揮發記憶體，持續嘗試迫使微處理器進入硬體關機模式，即微處理器停止操作。關於監控管理器 513 設置信號 CLASS1、CLASS2、CLASS3 以及 DISABLE 的上述情況僅為範例，是用來教導本發明之安全環境管理。此技術領域中具有通常知識者能理解，安全事件類別以及適當反應是受到所需之特定安全環境所約束，因此，本發明包含了上述安全事件類別與適當反應之其他方法。

現在參閱第 6 圖，狀態圖 600 詳細說明本發明之微處理器的操作模式轉換。狀態圖 600 包括原生未受控模式 601（或"非安全"執行模式 601）、降級模式 605 以及硬體關機模式 606，如同第 2 圖中相似命名的元件，相異之處在於，更詳細說明原生未受控模式 601 在程式控制下只可返回至此模式之有限次數。這些返回的有限次數以原生未受控模式(born free mode，BFM)[1:N]來表示。此外，更詳細地解釋在第 2 圖之安全執行模式 202，以說明複數 SEM 致能重置模式[1:N]602、一 SEM 致能正常執行模式 603 以及一 SEM 致能安全執行模式 604。即是，當安全執行模式 202 透過 SEMENABLE 指令的執行（或者其他致能機制）而被致能時，本發明之微處理器被重置（即致能重置[1:N]）其可能正在執行非安全應用程式（致能正常執行模式），或者可能正執行安全編碼（致能安全執行模式）。

如上所示，本發明之微處理器被製造為初始開機即進入原生未受控模式 601。且如狀態圖 600 所指示，有關微處理器的安全的不同版本可持續地被使用於原生未受控模式中。然而，SEMENABLE 指令或致能安全執行模式之交替機制（例如 SEM ENABLE）的執行導致微處理器進入 SEM 致能重置模式 602，以迫使微處理器重置，其中可以進入 SEM 致能重置模式 602 的次數為[1:N]次，且上述為第一次進入 SEM 致能重置模式 602。在 SEM 致能重置模式 602 中，在重置序列期間，微處理器執行關於操作在安全環境之配置與誠實性檢查，如前述關於第 5 圖之敘述。根據在 SEM 致能重置模式下重置的成功執行（即通過），微處理器轉換至 SEM 致能正常執行模式 603，以進行非安全應用程式的執行。然而，假使偵測到某些已定義狀態，例如前述由監控管理器 513 對信號 CLASS3 與 DISABLE 的設置，微處理器將轉換至降級模式 605（即由於 CLASS2 的設置），或轉換至硬體關機模式 606（即由於 DISABLE 的設置）。從硬體關機模式 606 離開，微處理器可被重置以導致其返回至 SEM 致能重置模式 602 中。從降級模式 605 離開，微處理器透過 BIOS 提供受限的指令，允許使用者建立用來在程式控制下致能微處理器以進入 SEM 致能安全執行模式 604 的參數。

從 SEM 致能重置模式 602 離開，在重置序列中的硬體呼尋將迫使微處理器直接進入 SEM 致能安全執行模式 604，於其中執行安全編碼。此外，發生在 SEM 致能正常執行模式 603 中非安全編碼執行期間中或者在 SEMENTER

指令之執行期間中的安全中斷、或者使微處理器開始執行安全編碼之交替機制，將導致微處理器轉換至 SEM 致能安全執行模式 604。命令微處理器開始執行安全編碼的指令與交替機制都參照狀態圖 600 中的"呼尋"。同樣地，SEMEXIT 指令之執行或命令微處理器終止安全編碼執行與開始非安全編碼執行的交替機制，係參照"返回(RETURN)"，此返回導致微處理器轉換為 SEM 致能正常執行模式 603。如上所述，安全編碼可導致微處理器由 SEM 致能安全執行模式 604 轉換為降級模式 605。BIOS 內的安全編碼允許微處理器由降級模式 605 返回至 SEM 致能安全執行模式 604。

最後，在 SEM 致能安全執行模式 604 中執行的安全編碼可藉由寫入一特殊機械專用暫存器，來引發安全機械檢查例外，其導致微處理器轉換回 SEM 致能正常執行模式 603 以執行非安全編碼。此外，假使在 SEM 致能正常執行模式 603 中發生一安全中斷，微處理器之狀態自動地改變至 SEM 致能安全執行模式 604。這些執行在本發明微處理器範例中用來導致狀態圖所述的狀態變化之不同的步驟，將透過第 7-11 圖來詳細說明。

參閱第 7 圖，流程圖 700 表示本發明微處理器中致能安全執行模式操作的高階方法。流程圖開始於方塊 701，於其中，微處理器處於原生未受控模式 601。透過 SEMENABLE 指令的執行或致能安全執行模式之交替機制，例如寫入至一隱藏機械專用暫存器，傳送一致能參數，其中，此致能參數已藉由使用一對非對稱加密金鑰中之一

者並根據非對稱加密演算法來被加密，而一對非對稱加密金鑰中之另一者已被編程至微處理器中授權的公開金鑰暫存器內。流程繼續進行至方塊 702。

在方塊 702 中，利用在微處理器內的加密單元，解密此致能參數以擷取用來致能安全執行模式之一有效指令以及擷取在記憶體內加密安全編碼之指標。在 BIOS 中指向安全編碼的另一指標以及任何加密的初始化資料也一起被提供。流程繼續進行至方塊 703。

在方塊 703 中，加密的安全編碼透過系統匯流排而被擷取自記憶體/BIOS，且被解密。此安全編碼與資料接著藉由使用一處理器金鑰並根據一對稱金鑰演算法來被加密，其中，此處理器金鑰對於本發明之每一處理器而言是獨特的，且在製造時被編程至一處理器金鑰暫存器。此對稱加密的安全編碼與資料接著透過私密匯流排而被寫入至一安全非揮發記憶體，其中，此私密匯流排隔離於系統匯流排資源。寫入至安全非揮發記憶體之部分程序包括在寫入對稱加密編碼與資料之前，對記憶體執行隨機寫入。流程繼續進行至方塊 704。

在方塊 704 中，微處理器內非揮發致能指示暫存器被寫入，以指示出安全執行模式被致能。在一實施例中，非揮發致能指示暫存器包括複數位元，且這些位元中之一者係被寫入以在安全執行模式每次被致能時用來指示出安全執行模式被致能。這些位元中另一者係被寫入以指示出返回至原生未受控模式。因此，根據本發明之 256 位元非揮發致能指示暫存器允許了 128 次由非安全執行模式至安全

執行模式的轉換。流程繼續進行至方塊 705。

在方塊 705 中，重置微處理器，即完成本發明微處理器中致能安全執行模式操作的方法。

第 8 圖之流程圖 800 強調用來在本發明之微處理器中禁能安全執行模式操作之高階方法。即是，流程圖 800 敘述操作在安全執行模式之安全編碼如何命令微處理器返回至原生未受控模式。流程開始於方塊 801，於其中，正於安全執行模式執行安全編碼。流程繼續進行至方塊 802。

在方塊 802 中，安全編碼於安全執行模式執行至非安全執行模式的返回(return)，亦即執行安全執行模式禁能指令。在一實施例中，當安全編碼執行對一 SEM 機械專用暫存器的寫入時，開始實施至非安全執行模式的返回(返回至一非安全執行模式)，其導致一安全例外(secure exception)。程式控制接著轉移至在於安全編碼內一位址上的安全例外管理者，其中，此位址係由前述安全中斷描述符號表單之內容來提供。在一實施例中，安全例外管理者對一機械專用暫存器執行寫入，以指示接受此返回。假使，此機械專用暫存器沒有被正確地寫入，此返回被忽略，且微處理器維持在安全執行模式。假使交握被確認，則流程繼續進行至方塊 803。

在判斷方塊 803 中，評估非揮發致能指示暫存器的內容，以判斷是否禁能安全執行模式(支援返回至非安全執行模式)。假使沒有被禁能(支援返回至非安全執行模式)，流程繼續進行至方塊 806。假使於此非揮發致能指示暫存器之複數位元允許至非安全執行模式的返回，流程則繼續進

行至方塊 804。

在方塊 806 中，維持安全執行模式，且控制權返回至安全編碼。

在方塊 804 中，更新非揮發致能指示暫存器，以指示此微處理器正操作在非安全執行模式。流程繼續進行至方塊 805。

在方塊 805 中，微處理器之狀態返回至原生未受控模式，即完成本發明之微處理器中禁能安全執行模式操作之方法。

第 9 圖表示流程圖 900，其詳細說明本發明微處理器內初始化安全編碼執行的方法。即是，流程圖 900 之方法包括第 7 圖之流程圖 700 的更詳細說明。流程開始於方塊 901，於其中，本發明之微處理器正於原生未受控模式中執行非安全應用程式。流程繼續進行至方塊 902。

在方塊 902 中，在非安全執行模式之一操作系統執行 SEMENABLE 指令或交替的機制（例如寫入至一機械專用暫存器），其傳送一或多個致能參數，其中，此一或多個致能參數是根據屬於授權者之私密金鑰來被非對稱地加密。此一或多個致能參數包括用來指向被執行之非對稱加密安全編碼的指標，此指標可儲存在系統記憶體以及/或 BIOS 記憶體。流程繼續進行至方塊 903。

在方塊 903 中，微處理器使用一對應的授權的公開金鑰來對傳送的一或多個致能參數進行解密。在一實施例中，於微處理器之製造期間，此授權的公開金鑰被編程至一非揮發授權的公開金鑰暫存器。在另一交替的實施例

中，此授權的公開金鑰被編程至本發明之安全非揮發記憶體內的一位置，且根據微處理器的初始開機，此授權的公開金鑰自此安全非揮發記憶體被擷取，且此授權的公開金鑰被編程至非揮發授權的公開金鑰暫存器，接著，在安全非揮發記憶體內的此位置被清除。流程繼續進行至方塊904。

在方塊 904 中，判斷解密的致能參數是否有效。假使有效，流程繼續進行至方塊 905。假使無效，流程則繼續進行至方塊 907。

在方塊 905 中，由於已判斷出此致能參數是有效的，則執行複數隨機寫入於安全非揮發記憶體的所有位置以清除安全非揮發記憶體的內容。流程則繼續進行至方塊 906。

在判斷方塊 906 中，加密的安全編碼自系統記憶體/以及或 BIOS 記憶體被擷取。接著，使用授權的公開金鑰並根據非對稱金鑰演算法來對此加密的安全編碼進行解密。在一實施例中，在微處理器中執行邏輯電路內的一加密單元用來解密此加密的安全編碼。在一實施例中，此加密單元能執行 AES 加密操作、SHA-1 雜湊操作以及 RSA 加密操作。解密後的安全編碼接著被解壓縮，且被檢查格式是否正確。假使解密後的安全編碼格式正確，流程繼續進行至方塊 908。假使解密後的安全編碼格式不正確，流程則繼續進行至方塊 907。

在方塊 907 中，由於解密後的致能參數是無效的，程式控制則返回至非安全執行模式。

在方塊 908 中，解密的安全編碼（以及對應的初始資

料，若有的話）藉由使用處理器金鑰並根據對稱金鑰演算法來加密，其中，此處理器金鑰是此微處理器所獨有的，且在製造時編程至一非揮發處理器金鑰暫存器內。在一實施例中，此對稱金鑰為 128 位元之 AES 金鑰，且此微處理器利用其加密單元來對安全編碼執行 AES 加密。流程繼續進行至方塊 909。

在方塊 909 中，此微處理器建立加密安全編碼中一或多個段落的一或多個雜湊。在一實施例中，微處理器內的加密單元用來建立加密編碼之一或多個 SHA-1 雜湊。流程繼續進行至方塊 910。

在方塊 910 中，微處理器透過私密匯流排將加密的安全編碼（以及資料，若有的話）以及此一或多個雜湊寫入至安全非揮發記憶體，其中，此私密匯流排隔離於系統匯流排資源。此安全編碼與資料被加密，因此阻止了安全編碼內容的偵測。流程繼續進行至方塊 911。

在步驟 911 中，設定非揮發致能指示暫存器以指示安全執行模式被致能。流程繼續進行至方塊 912。

在方塊 912 中，於微處理器內執行安全執行模式致能重置序列(reset sequence)。此重置序列包括硬體檢查（如同第 5 圖中相關的討論）以及初始化安全揮發記憶體為複數亂數，即完成本發明之微處理器內初始化安全編碼執行的方法。

接著參閱第 10 圖，流程圖 1000 表示本發明微處理器中執行安全執行模式致能重置操作的方法，其中，此微處理器已致能安全執行模式的操作。流程開始於方塊 1001，

其中，當微處理器完成安全執行模式的初始化時，微處理器執行安全執行模式致能重置序列。流程繼續進行至方塊1002。

在方塊 1002 中，微處理器執行複數處理器誠實性檢查，包括安全非揮發記憶體、電池與石英器的偵測與確認。此外，核對匯流排時脈的存在與頻率誠實性，並確認提供給匯流排終端與微處理器供應電源之適當電壓。微處理器之溫度確認處於一可接受的範圍內。流程繼續進行至方塊1003。

在方塊 1003 中，微處理器執行非揮發記憶體連結(connectivity)與雜湊檢查。自安全非揮發記憶體內一位置讀取安全簽章，並對此安全簽章進行解密。解密後的簽章被核對以證實非揮發記憶體沒有被洩漏。此外，微處理器亦讀取安全非揮發記憶體之特定位置與對應的雜湊。透過加密（即 AES/HASH/RSA）單元，產生被選擇位置的確認雜湊，且與被讀取的雜湊進行比較。流程繼續進行至方塊1004。

在方塊 1004 中，微處理器執行安全實時時鐘的確認。在一實施例中，安全執行模式實時時鐘估計石英器的狀態，以偵測在頻率上大於百分之五的改變，因此表示出石英器與在電池電壓上大於百分之五的改變，且表示出潛在的安全威脅徵兆。假使上述確認檢查的任一者產生不利的結果，根據偵測到事件的嚴重性與次數，安全執行模式致能重置序列將使此事件被記錄下來，或者迫使微處理器進入降級模式，或硬體關機模式。流程繼續進行至方塊 1005。

在方塊 1005 中，自非揮發記憶體(系統記憶體以及/或 BIOS 記憶體)擷取加密的安全編碼以及資料。流程繼續進行至方塊 1006。

在方塊 1006 中，解碼與解壓縮加密的安全編碼，且確認格式正確後，安全編碼接著被載入至微處理器內的安全揮發記憶體。流程繼續進行至方塊 1007。

在方塊 1007 中，初始化微處理器內的安全資源。這些安全資源無法被非安全編碼所得知或存取，且只對於在安全執行模式中執行的安全編碼而言是可利用的。這些資源包括安全計時器、安全中斷以及安全例外，且包括安全中斷描述符號表單、以及任何安全機械專用暫存器或為了安全編碼的執行而必須被初始化的其他暫存器。初始化包括非安全中斷、非安全例外、非安全追蹤以及除錯邏輯電路的禁能，也包括微處理器之任何電源管理邏輯電路的禁能，其中包括導致核心電壓、核心時脈頻率之變化或者致能或禁能其他元件（例如快取記憶體、分支預測單元等等）的任何元件。流程繼續進行至方塊 1008。

在方塊 1008 中，初始化微處理器內的非安全的快取記憶體（即 L1 快取記憶體、L2 快取記憶體）為亂數。流程繼續進行至方塊 1009。

在方塊 1009 中，產生一安全執行模式中斷，且根據存在於安全中斷描述符號表單內的資料來呼尋(call)安全執行模式重置功能，其中，此安全中斷描述符號表單在方塊 1007 中被初始化，即完成本發明微處理器中執行安全執行模式致能重置操作的方法。

接著參閱第 11 圖，流程圖 1100 表示本發明微處理器中終止安全執行模式操作之方法。此方法開始於方塊 1101，於其中，安全編碼正執行於安全執行模式。概括上，根據本發明，具有三種方法使微處理器由非安全執行模式轉換為安全執行模式，並開始安全編碼的執行。第一種方法允許程式控制轉移為安全編碼的執行。即是，在安全執行模式下的非安全應用程式如同 SEMENTER 指令般執行。在一實施例中，SEMENTER 指令導致微處理器的狀態被儲存在安全揮發記憶體內的堆疊，且程式控制轉移至安全編碼，非常類似 x86 SYSENTER 指令的操作。第二種方法是，當執行非安全或安全重置序列時，導致安全編碼的執行是由於一中斷或例外所致。導致安全編碼執行的最後一個方法，是起因於來自任何數量之安全監控邏輯元件的中斷，就像關於第 5 圖的討論。

如上所述，執行在安全執行模式之安全編碼，永久地存在於安全非揮發記憶體，但是在一安全執行模式致能重置序列的期間，其已被載入至安全揮發記憶體。即是，此安全編碼不再自非安全記憶體中執行，例如系統記憶體或非安全的處理器快取記憶體。因此，藉由兩種方法，執行控制由安全執行模式轉換回非安全執行模式。第一種方法包括執行 SRESUME 指令，其引起來自 SEMENTER 指令的回應(return)。在 x86 實施例中，此 SRESUME 指令以與 x86 RESUME 相似的方法來操作。即是，預先儲存在安全揮發記憶體中的程式狀態被恢復(restored)，且程式控制轉移至操作系統或非安全編碼。第二種方法是考慮強迫一安全例

外，其中，藉由對只可由安全編碼來存取之一機械專用暫存器執行寫入，微處理器之安全元件可存取此安全例外。假使確認微處理器將返回至非安全執行模式，接著產生被操作系統指明且處理的一非安全機械檢查例外，因此影響至非安全執行模式的返回。第 11 圖之流程圖 1100 提出強迫此安全例外以返回至非安全執行模式，而此技術領域中具有通常知識者將理解，SRESUME 指令的執行導致微處理器去執行下文所述的相似步驟。

因此，流程持續於方塊 1102，於其中，將安全編碼寫入至安全執行模式機械專用暫存器(SEM MSR)。SEM MSR 即是，只可被執行在安全執行模式下之安全編碼所存取且得知的複數機械專用暫存器中之一者。流程繼續進行至方塊 1103。

在方塊 1103 中，寫入至安全執行模式機械專用暫存器產生了由 SEM 邏輯電路內安全例外邏輯電路所處理的安全例外。流程繼續進行至方塊 1104。

在方塊 1104 中，安全例外邏輯電路（例如安全中斷描述符號表單）導致程式控制分支至安全編碼內的安全例外管理者。流程繼續進行至方塊 1105。

在方塊 1105 中，安全例外管理者回應一授權的例外編碼。此安全例外管理者執行至安全編碼的返回，藉以將一授權的例外編碼傳送回安全編碼。流程繼續進行至方塊 1106。

在方塊 1106 中，判斷由安全例外管理者所回應之例外編碼是否正確。假使此例外編碼不正確，則假設有一安全

風險，且流程繼續進行至方塊 1112。假使此例外編碼正確，則安全編碼與安全例外管理者之間的交握則被確認以指示返回至非安全執行模式，且流程繼續進行至方塊 1107。

在方塊 1112 中，維持安全執行模式，且控制權返回至安全編碼。

在方塊 1107 中，微處理器執行複數隨機寫入於安全非揮發記憶體的所有位置以清除安全非揮發記憶體之內容。安全應用程式利用微處理器內之一亂數產生器來產生亂數資料且對安全非揮發記憶體內之所有位置執行隨機寫入。流程繼續進行至方塊 1108。

在方塊 1108 中，微處理器藉由將"0"寫入至安全非揮發記憶體之每一位置，來清除安全非揮發記憶體之每一位置。流程繼續進行至方塊 1109。

在方塊 1109 中，設定非揮發致能指示暫存器以指示安全執行模式被禁能，亦即，微處理器正操作在一非安全執行模式中。其受限於安全執行模式可被禁能的次數，如同前文關於第 8 圖之說明。流程繼續進行至方塊 1110。

在方塊 1110 中，安全例外邏輯電路產生一機械檢查例外，此外回應一狀態參數(亦即例外編碼指示狀態)來將程式控制轉移至非安全應用程式中之一。因此，在非安全執行模式下的操作系統處理此機械檢查例外，且完成返回至非安全執行模式。流程繼續進行至方塊 1111。

在方塊 1111 中，即完成本發明微處理器中終止安全執行模式操作之方法。

第 12 圖係表示一安全實時時鐘 1200 之詳細方塊圖，

其位於本發明之微處理中的 SEM 邏輯電路內。安全實時時鐘 1200 只可由正操作在安全執行模式下的安全編碼來得知且存取。安全實時時鐘包括震盪器 1201，其透過信號 VP 耦接電池且透過信號 C1 及 C2 來耦接石英器。此震盪器產生震盪輸出電壓信號 VO，且信號 VO 耦接計數器 1202。此計數器產生輸出信號 CNTO，且輸出信號 CNTO 被路由至轉換邏輯電路 1203。信號 VP、C1、及 C2 也輸入至轉換邏輯電路 1203，此外，信號 ENV 同樣輸入至轉換邏輯電路，其中，信號 ENV 載有對應晶粒溫度之數值。轉換邏輯電路 1203 產生透過信號 TEMP、BATT、COMP、XTAL 以及雙向匯流排 TIME 來提供的複數輸出。此微處理器透過雙向匯流排 TIME 提供輸入至此安全實時時鐘。

震盪器 1201 與計數器 1202 是專用的，即是除了被提供來允許微處理器透過雙向匯流排 TIME 對安全實時時鐘進行讀取和寫入的元件以外，他們無法共享其他電路系統或微處理器的其他元件。此外，只要電池透過信號 VP 提供可接受的電壓時，安全實時時鐘持續其計數。在一交替的實施例中，電池電壓信號 VP 是由系統板上的電容器所產生，以代替只要系統板開機而持續被充電的電池。

在操作上，震盪器 1201 產生震盪輸出電壓信號 VO，其與石英器之頻率成比例，且此震盪輸出電壓被提供至計數器 1202。計數器 1202 包括複數元件，用來計算透過信號 VO 所提供之週期數，並將此週期數轉換為一計數數值。此計數數值被提供至信號 CNTO 上。轉換邏輯電路 1203 包括複數電路，用將 CNTO 之數值轉換為持續時間數值，

此外，轉換邏輯電路 1203 也包括複數暫存器（未顯示），其可透過雙向匯流排 TIME 而被微處理器來讀取與寫入。

此外，轉換邏輯電路 1203 用來偵測電壓信號 VP 的顯著變化，指示出潛在的篡改，且此一事件由信號 BATT 之設置來表示，其中，信號 BATT 之設置係用來中斷正執行的安全編碼。在一實施例中，大於百分之五的變化導致 BATT 中斷被設置。

轉換邏輯電路 1203 也用來透過信號 C1 與 C2 來偵測石英器頻率的顯著變化，因此指示潛在的篡改，且此一事件藉由信號 XTAL 的設置來表示。信號 XTAL 的設置係用來中斷正執行的安全編碼。在一實施例中，大於百分之五的變化導致 XTAL 中斷被設置。

信號 ENV 係由轉換邏輯電路 1203 來估計，以判斷因溫度偏離而使計數器 1202 產生不精準的計數。假使判斷出溫度偏離，信號 TEMP 則被設置，其用來中斷正執行的安全編碼。

轉換邏輯電路 1203 也用來估計上述情況中任一者是否足夠顯著，以指示安全實時時鐘已被洩漏，例如電池的移動與取代。假使被判斷出，信號 COMP 也被設置，因此中斷安全編碼的執行。

本發明提供一些高於現今技術的優點以在安全環境中執行應用程式。例如，根據本發明之設計是以微處理器為基礎。即是，本發明之一目的是修改負責安全編碼的微處理器，這是因為，相對於著重在修改晶片組或其他元件的其他技術，只有微處理器可提供及時執行安全。使用隔離

晶片來監控微處理器的方法有許多的內在安全性缺陷，且對於安全相關的執行而言效能也明顯地降低。

根據本發明中以 x86 為基礎的實施例，由於 x86 程式化技術的普遍性，安全編碼的發展相當地平易。x86 架構已被得知，且對於精通非安全 x86 應用發展的任何程式設計者而言，機械專用指令之附加與專用指令（例如 SEMENABLE、SEMENTER、及 SRESUME 指令）僅提供較少的學習挑戰。

此外，對於微處理器的附加安全執行能力的成本遠小於額外晶片組被加至系統設計所呈現的成本。

此外，由於安全執行環境係被提供至微處理器本身之內，因此內在地對抗那些物理或從屬通道攻擊，其不需要附加外部電路。

此處所揭露的技術非常有利地提供安全的微處理器操作環境，在此環境中，會被洩漏的一般機密（例如一般加密金鑰或程式架構）不會儲存於其中。即是，本發明之每一處理器只具有需要被特定處理器或系統授權、控制等等的機密。來自一處理器/系統之機密不會破壞在另一處理器/系統的安全性。此外，得知如何破壞在一處理器的安全性，應當不會使其更容易地去破壞其他處理器上的安全性。即是，這是由於獨特的處理器金鑰，此獨特的處理器金鑰是由在安全非揮發記憶體匯流排上的資料傳輸所提供且導致的，其中，這些資料傳輸係使用此金鑰來加密。

與提供對抗俗稱阻絕服務攻擊（denial-of-service attack）之保護的習知技術比較起來，根據本發明之微處理

器具有更多的優點。例如，如第 5 圖所討論，提供安全監控元件以偵測並取得在事件上的活動，例如持續對安全執行環境的呼尋（例如來自惡意裝置驅動器），實時時鐘電池、石英器的持續移除等等。

本發明雖以較佳實施例揭露如上，然其並非用以限定本發明的範圍，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可做些許的更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1 圖表示根據本發明之安全執行模式（SEM）微處理器之方塊示意圖；

第 2 圖表示說明第 1 圖之微處理器中最高階級操作模式之狀態圖；

第 3 圖表示根據本發明之微處理器中 SEM 邏輯電路之方塊示意圖；

第 4 圖表示在根據本發明之微處理器內，安全編碼如何被儲存、存取、初始化以及執行的方塊示意圖；

第 5 圖表示在第 1 圖之微處理器中，SEM 監控邏輯電路的詳細方塊示意圖；

第 6 圖表示在根據本發明之微處理器內操作模式轉換之狀態圖；

第 7 圖表示在本發明之微處理器中致能安全執行模式操作的高階方法流程圖；

第 8 圖表示在本發明之微處理器中禁能安全執行模式

操作之高階方法流程圖；

第 9 圖表示在本發明之微處理器內初始化安全編碼執行的方法流程圖；

第 10 圖表示本發明微處理器中執行安全執行模式致能重置操作的方法流程圖；

第 11 圖表示在本發明微處理器中終止安全執行模式操作之方法流程圖；以及

第 12 圖表示在本發明之微處理器內安全實時時鐘之詳細方塊示意圖。

【主要元件符號說明】

100～系統板；　　101～安全執行模式微處理器；

102～系統匯流排；　　103～匯流排主控裝置；

104～匯流排管理裝置；

105～安全執行模式邏輯電路；

106～私密匯流排；　　107～安全非揮發記憶體；

C1、C2～連接路徑/信號；

PSNT～內存檢測匯流排/信號；

VP～電池；　　VP1、VP2～連接路徑/信號；

X1～石英器；

200～狀態圖；

201～非安全執行模式（原生未受控模式）；

202～安全執行模式（SEM-致能模式）；

203～降級模式；　　204～硬體關機模式；

300～安全執行模式微處理器；

301～SEM 邏輯電路；　302～安全揮發記憶體；

303～處理器狀態；　304～安全編碼；

305～SEM 初始化邏輯電路；

306～SEM 監控邏輯電路；

307～SEM 中斷邏輯電路；

308～SEM 例外邏輯電路；

309～SEM 計時器；　310～SEM 實時時鐘；

311～AES/HASH/RSA 單元；

312～處理器金鑰暫存器；

313～處理器執行單元；　314～正常例外邏輯電路；

315～正常追蹤/除錯邏輯電路；

316～正常中斷邏輯電路；

317～對應安全編碼之安全資料；

318～授權的公開金鑰暫存器；

319～亂數產生器；

320、321、324、326、327～匯流排；

322～電源管理邏輯電路；

323～位址邏輯電路；　325～非安全記憶體；

328～非揮發致能指示暫存器；

329～SEM 機械專用暫存器記憶庫；

400～圖示；　401～微處理器；

402～安全編碼介面邏輯電路；

403～匯流排介面單元；

404～授權的公開金鑰暫存器；

405～AES/HASH/RSA 單元；

406～安全揮發記憶體；

407～安全非揮發記憶體介面單元；

408～SEM 監控邏輯電路；

409～SEM 初始化邏輯電路；

410～BIOS 記憶體；　411、421～安全編碼；

412～亂數產生器；　413～處理器金鑰暫存器；

420～系統記憶體；　425～系統匯流排；

430～安全非揮發記憶體；

431～私密匯流排；　432～授權的公開金鑰區域；

CHK、INS～匯流排；

500～SEM 監控邏輯電路；

501～物理環境監控器；

502～匯流排時脈監控器；

503～頻率參考單元；　504～處理器電壓監控器；

505～溫度監控器；　506～資料監控器；

507～安全時戳計數器；

508～正常時戳計數器；

509～比率機械專用暫存器；

510～樣式監控器；　511～指令監控器；

512～指令陣列；　513～監控管理器；

BUSTERM、BUS CLK、CORE CLK、TEMP、VDD、CLASS1、CLASS2、CLASS3、DISABLE～信號；

DESTRUCT、INS、NOBOOT、PINCHK、TAMPER、CHK～匯流排；

600～詳細操作模式圖示；

601～原生未受控模式（非安全執行模式）；

602～SEM 致能重置模式[1:N]；

603～SEM 致能正常執行模式；

604～SEM 致能安全執行模式；

605～降級模式；　606～硬體關機模式；

700～流程圖；　701...705～流程步驟；

800～流程圖；　801...806～流程步驟；

900～流程圖；　901...912～流程步驟；

1000～流程圖；　1001...1009～流程步驟；

1100～流程圖；　1101...1112～流程步驟；

1200～安全實時時鐘；1201～震盪器；

1202～計數器；　1203～轉換邏輯電路；

VP、ENV～信號；　VO、CNTO～輸出信號；

CNTO～輸出信號；

TEMP、BATT、COMP、XTAL～信號；

TIME～雙向匯流排。

200949681

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：98113141

※申請日：98.04.21　※IPC 分類：G06F 9/30 (2006.01)

一、發明名稱：(中文/英文)

提供安全執行環境之裝置、微處理器裝置、以及在安全執行環境中執行安全編碼之方法/APPARATUS AND METHOD FOR MANAGING A MICROPROCESSOR PROVIDING FOR A SECURE EXECUTION MODE

二、中文發明摘要：

一種提供安全執行環境之裝置，其微處理器執行非安全應用程式與安全應用程式。非安全應用程式透過系統匯流排存取自系統記憶體，且安全應用程式在安全執行模式中執行。微處理器包括安全執行模式邏輯電路，其監控對應微處理器且與潛在篡改相關之狀態，並根據狀態中第一者使微處理器自安全執行模式轉換至降級模式。降級模式只提供給 BIOS 指令執行。此裝置之安全非揮發記憶體透過私密匯流排耦接微處理器且儲存安全應用程式。在私密匯流排上微處理器與安全非揮發記憶體之間的資料傳輸隔離於系統匯流排及微處理器內之對應系統匯流排資源。

三、英文發明摘要：

An apparatus providing for a secure execution environment including a microprocessor and a secure non-volatile memory. The microprocessor executes

non-secure application programs and a secure application program. The non-secure application programs are accessed from a system memory via a system bus. The secure application program, executes in a secure execution mode. The microprocessor has secure execution mode logic circuit that monitors conditions corresponding to the microprocessor associated with tampering, and causes the microprocessor to transition to a degraded operating mode from the secure execution mode following detection of a first one or more of the conditions. The degraded operating mode exclusively provides for execution of BIOS instructions. The secure non-volatile memory is coupled to the microprocessor via a private bus and stores the secure application program. Transactions over the private bus are isolated from the system bus and corresponding system bus resources within the microprocessor.

七、申請專利範圍：

1.一種提供安全執行環境之裝置，包括：

一微處理器，用以執行複數非安全應用程式與一安全應用程式，其中，該等非安全應用程式透過一系統匯流排而存取自一系統記憶體，且該安全應用程式在一安全執行模式中執行，該微處理器包括：

一安全執行模式邏輯電路，用以監控對應該微處理器且與潛在安全暴露和篡改相關聯之複數狀態，並根據該等狀態之一來使該微處理器自該安全執行模式轉換至一降級模式，其中，該降級模式只提供給複數基本輸入/輸出系統(Basic Input/Output System，BIOS)指令之執行，且該等 BIOS 指令包括允許使用者輸入與訊息顯示之指令；以及

一安全非揮發記憶體，透過一私密匯流排耦接該微處理器，用以儲存該安全應用程式，其中，在該私密匯流排上該微處理器與該安全非揮發記憶體之間的複數資料傳輸，隔離於該系統匯流排以及該微處理器內之複數對應系統匯流排資源。

2.如申請專利範圍第 1 項所述之提供安全執行環境之裝置，其中，該等 BIOS 指令係透過發出一外部中斷給該微處理器且經由一機械專用暫存器來執行。

3.如申請專利範圍第 1 項所述之提供安全執行環境之裝置，其中，該等狀態包括複數硬體偵測狀態。

4.如申請專利範圍第 1 項所述之提供安全執行環境之裝置，其中，該等狀態更包括執行該安全應用程式之結果。

5.如申請專利範圍第 1 項所述之提供安全執行環境之裝置，其中，根據該等狀態之一偵測結果，該安全執行模式邏輯電路試圖清除該微處理器內一安全揮發記憶體之一資料區域，且試圖將該偵測結果紀錄至該安全非揮發記憶體。

6.如申請專利範圍第 5 項所述之提供安全執行環境之裝置，其中，根據該資料區域之成功清除與該偵測結果之成功紀錄，該安全執行模式邏輯電路將該微處理器轉換至該降級模式。

7.如申請專利範圍第 1 項所述之提供安全執行環境之裝置，其中，根據該等該等狀態之一偵測結果，該安全執行模式邏輯電路使該微處理器轉換至一硬體關機模式，且只可藉由重置該微處理器來退出該硬體關機模式。

8.如申請專利範圍第 7 項所述之提供安全執行環境之裝置，其中，根據該等狀態之該偵測結果，該安全執行模式邏輯電路試圖清除該微處理器內一安全揮發記憶體之一資料區域、試圖將該偵測結果紀錄至該安全非揮發記憶體、且使該微處理器進入至該硬體關機模式。

9.一種微處理器裝置，用以在一安全執行環境中執行安全編碼，該微處理器裝置包括：

一安全非揮發記憶體，用以儲存一安全應用程式；以及

一微處理器，透過一私密匯流排耦接該安全非揮發記憶體，用以執行複數非安全應用程式與該安全應用程式，其中，該微處理器包括：

一安全執行模式邏輯電路，用以監控對應該微處理器且與潛在安全暴露和篡改相關聯之複數狀態，並根據該等狀態之一來使該微處理器自該安全執行模式轉換至一降級模式，其中，該降級模式只提供給複數基本輸入/輸出系統(Basic Input/Output System，BIOS)指令之執行，且該等 BIOS 指令包括允許使用者輸入與訊息顯示之指令。

10.如申請專利範圍第 9 項所述之微處理器裝置，其中，其中，該等 BIOS 指令係透過發出一外部中斷給該微處理器且經由一機械專用暫存器來執行。

11.如申請專利範圍第 9 項所述之微處理器裝置，其中，該等狀態包括複數硬體偵測狀態。

12.如申請專利範圍第 9 項所述之微處理器裝置，其中，該等狀態更包括執行該安全應用程式之結果。

13.如申請專利範圍第 9 項所述之微處理器裝置，其中，根據該等狀態之一偵測結果，該安全執行模式邏輯電路試圖清除該微處理器內一安全揮發記憶體之一資料區域，且試圖將該偵測結果紀錄至該安全非揮發記憶體。

14.如申請專利範圍第 13 項所述之微處理器裝置，其中，根據該資料區域之成功清除與該偵測結果之成功紀錄，該安全執行模式邏輯電路將該微處理器轉換至該降級模式。

15.如申請專利範圍第 9 項所述之微處理器裝置，其中，根據該等該等狀態之一偵測結果，該安全執行模式邏輯電路使該微處理器轉換至一硬體關機模式，且只可藉由

重置該微處理器來退出該硬體關機模式。

16.如申請專利範圍第 16 項所述之微處理器裝置，其中，根據該等狀態之該偵測結果，該安全執行模式邏輯電路試圖清除該微處理器內一安全揮發記憶體之一資料區域、試圖將該偵測結果紀錄至該安全非揮發記憶體、且使該微處理器進入至該硬體關機模式。

17.一種在安全執行環境中執行安全編碼之方法，包括：

提供一安全非揮發記憶體，以儲存一安全編碼，其中，該安全編碼藉由實現在一私密匯流排上之複數私密資料傳輸而存取自該安全非揮發記憶體，且該私密匯流排耦接該安全非揮發記憶體與一微處理器之間，該私密匯流排隔離於該微處理器內之所有系統匯流排資源且配置在該微處理器之外部，以及該私密匯流排只由該微處理器之一安全執行邏輯電路所得知及存取；

監控對應該微處理器之複數狀態，其中，該等狀態與潛在安全暴露和篡改相關聯；以及

根據該等狀態之一，使該微處理器自一安全執行模式轉換至一降級模式，其中，該降級模式只提供給複數基本輸入/輸出系統（Basic Input/Output System，BIOS）指令之執行，且該等 BIOS 指令包括允許使用者輸入與訊息顯示之指令。

18.如申請專利範圍第 17 項所述之在安全執行環境中執行安全編碼之方法，其中，該等 BIOS 指令係透過發出一外部中斷給該微處理器且經由一機械專用暫存器來執行。

19.如申請專利範圍第 17 項所述之在安全執行環境中執行安全編碼之方法，其中，該等狀態包括複數硬體偵測狀態。

20.如申請專利範圍第 17 項所述之在安全執行環境中執行安全編碼之方法，其中，該等狀態更包括執行該安全應用程式之結果。

21.如申請專利範圍第 17 項所述之在安全執行環境中執行安全編碼之方法，其中，使該微處理器自該安全執行模式轉換至該降級模式之步驟包括：

根據該等狀態之一偵測結果，試圖清除該微處理器內一安全揮發記憶體之一資料區域，且試圖將該偵測結果紀錄至該安全非揮發記憶體。

22.如申請專利範圍第 21 項所述之在安全執行環境中執行安全編碼之方法，其中，根據該資料區域之成功清除與該偵測結果之成功紀錄，使該微處理器自該安全執行模式轉換至該降級模式。

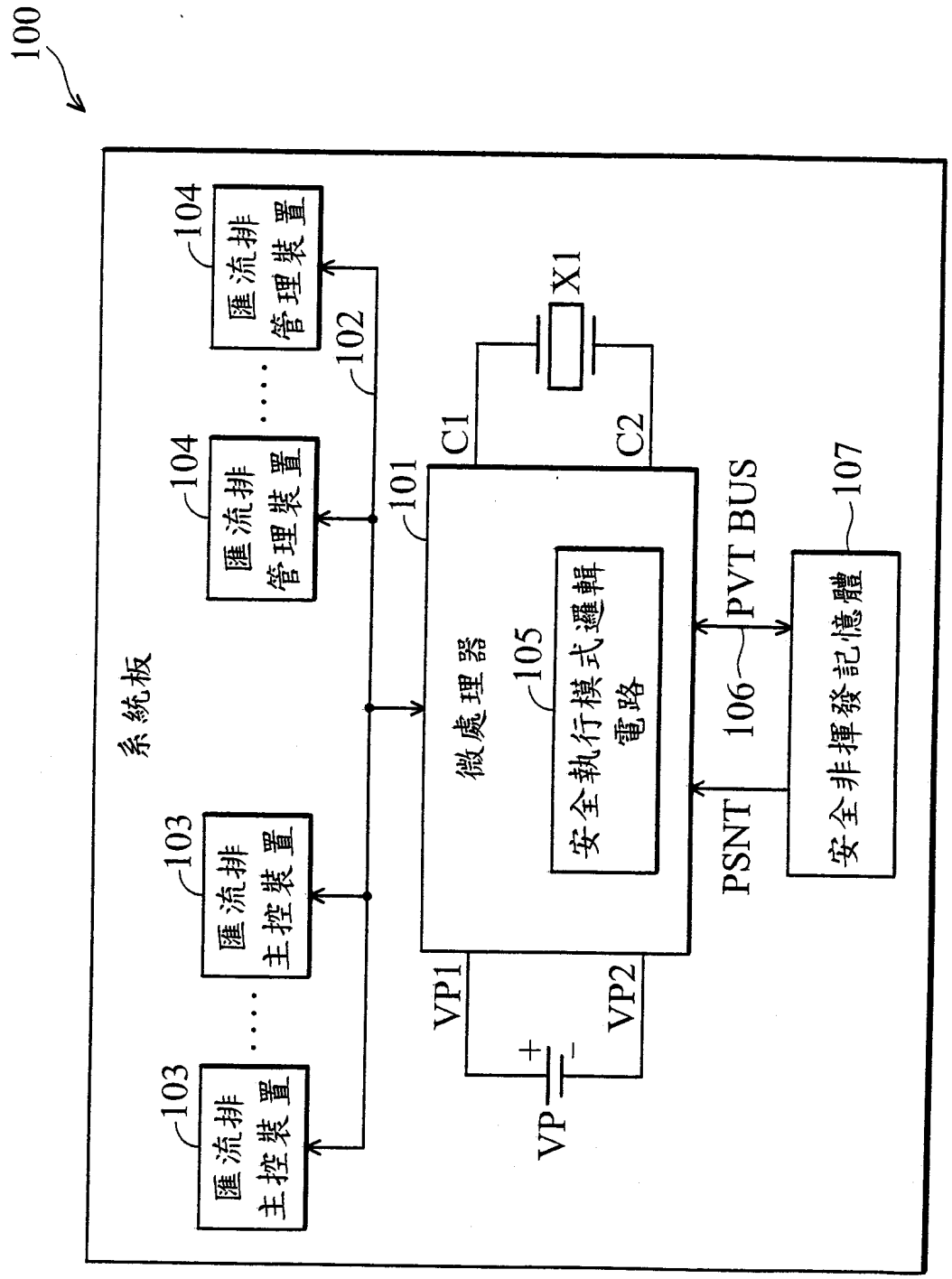
23.如申請專利範圍第 17 項所述之在安全執行環境中執行安全編碼之方法，更包括：

根據該等該等狀態之一偵測結果，使該微處理器轉換至一硬體關機模式，其中，只可藉由重置該微處理器來退出該硬體關機模式。

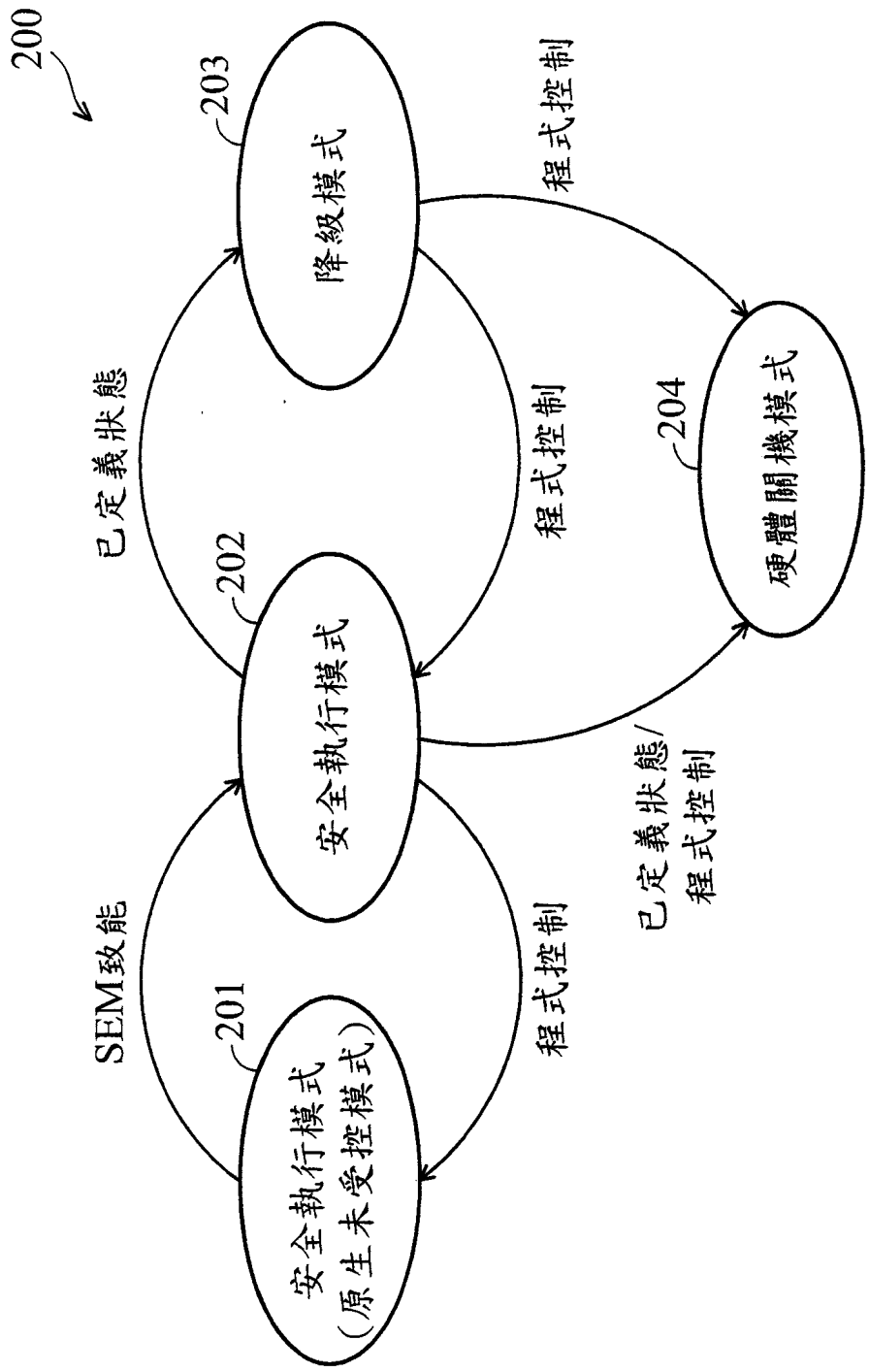
24.如申請專利範圍第 23 項所述之在安全執行環境中執行安全編碼之方法，其中，使該微處理器轉換至該硬體關機模式之步驟包括：

根據該等狀態之該偵測結果，試圖清除該微處理器內

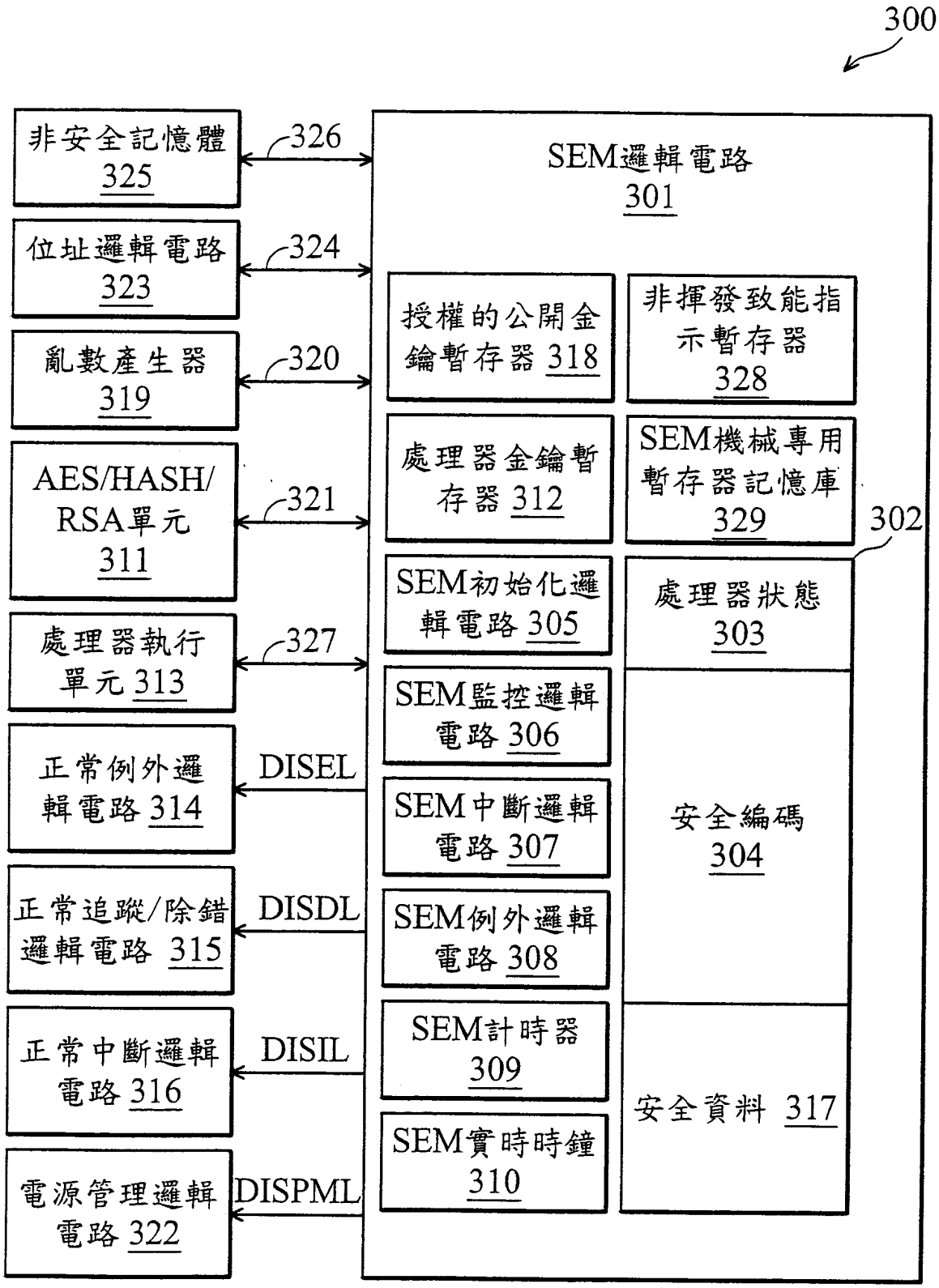
一安全揮發記憶體之一資料區域、試圖將該偵測結果紀錄至該安全非揮發記憶體、且使該微處理器進入至該硬體關機模式。


100
系統板
匯流排主控裝置
匯流排主控裝置
匯流排管理裝置
匯流排管理裝置
102
101
微處理器
105
安全執行模式邏輯電路
C1
C2
X1
VP1
VP2
VP
+
-
PSNT
106
PVT BUS
107
安全非揮發記憶體

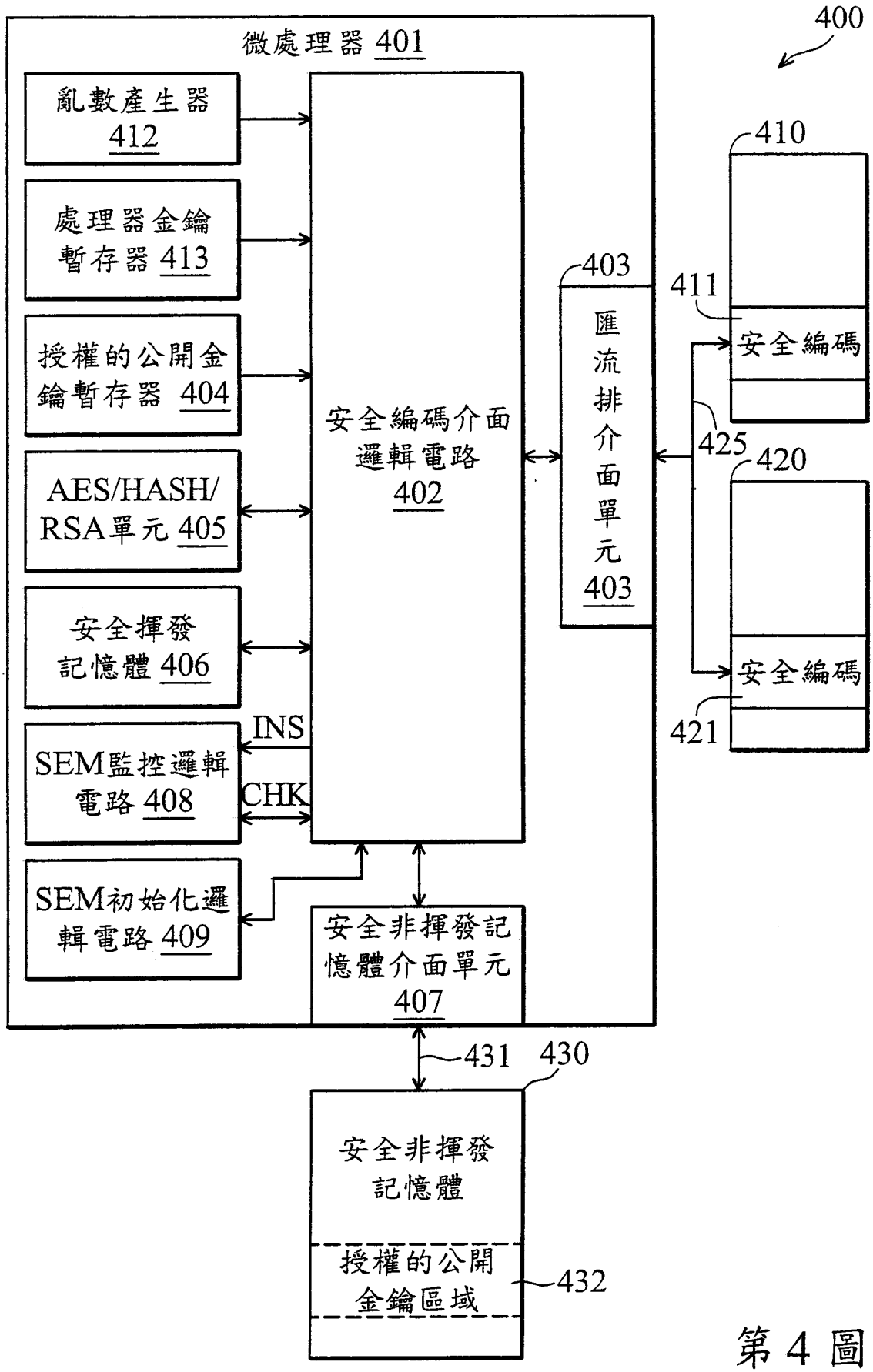
第 1 圖


200
203
降級模式
已定義狀態
程式控制
202
安全執行模式
程式控制
204
硬體關機模式
SEM致能
201
安全執行模式
(原生未受控模式)
程式控制
已定義狀態/
程式控制

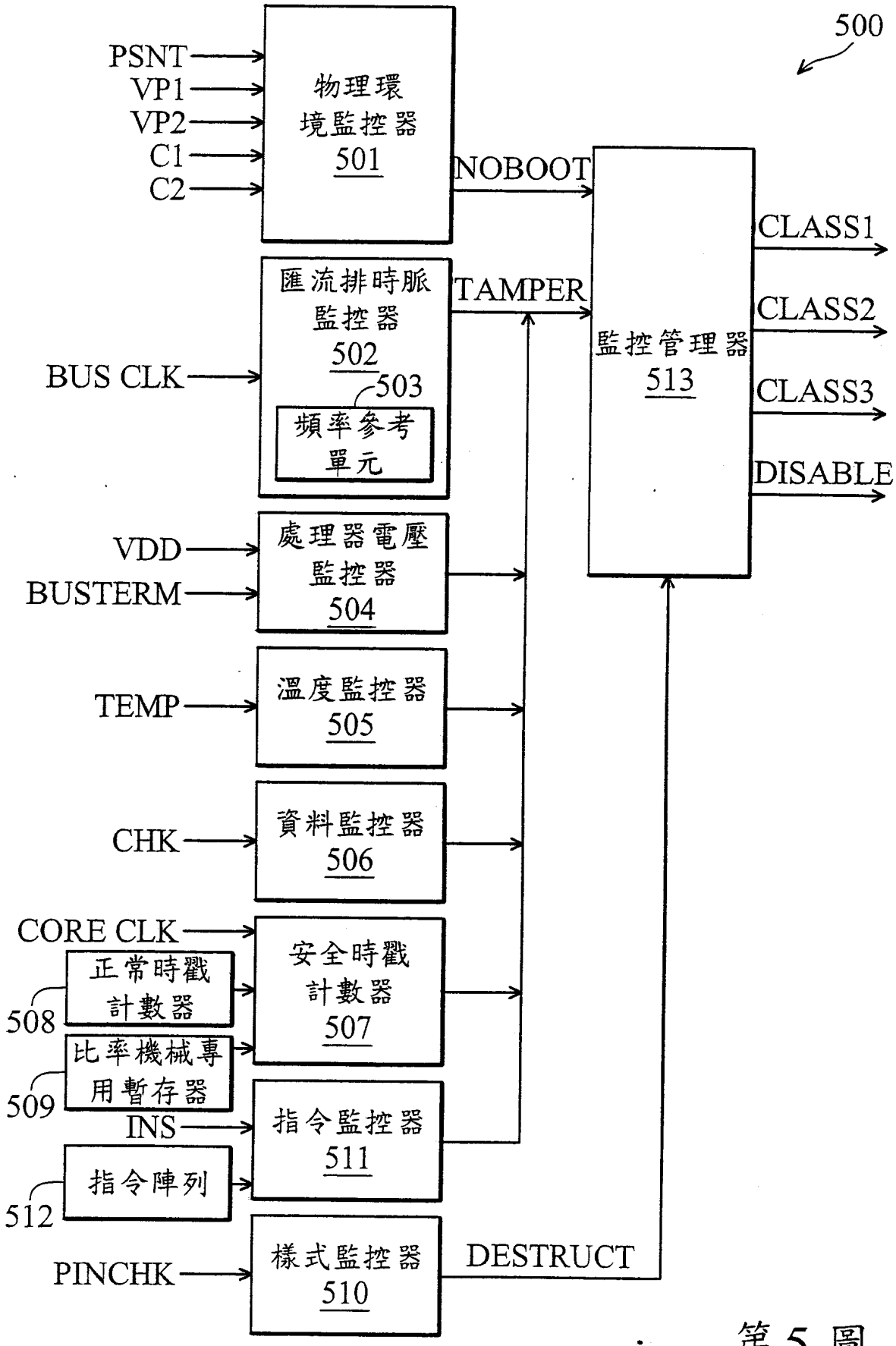
第 2 圖


300
非安全記憶體 325
326
位址邏輯電路 323
324
亂數產生器 319
320
AES/HASH/ RSA單元 311
321
處理器執行單元 313
327
正常例外邏輯電路 314
DISEL
正常追蹤/除錯邏輯電路 315
DISDL
正常中斷邏輯電路 316
DISIL
電源管理邏輯電路 322
DISPML
SEM邏輯電路 301
授權的公開金鑰暫存器 318
非揮發致能指示暫存器 328
處理器金鑰暫存器 312
SEM機械專用暫存器記憶庫 329
302
SEM初始化邏輯電路 305
處理器狀態 303
SEM監控邏輯電路 306
SEM中斷邏輯電路 307
安全編碼 304
SEM例外邏輯電路 308
SEM計時器 309
安全資料 317
SEM實時時鐘 310

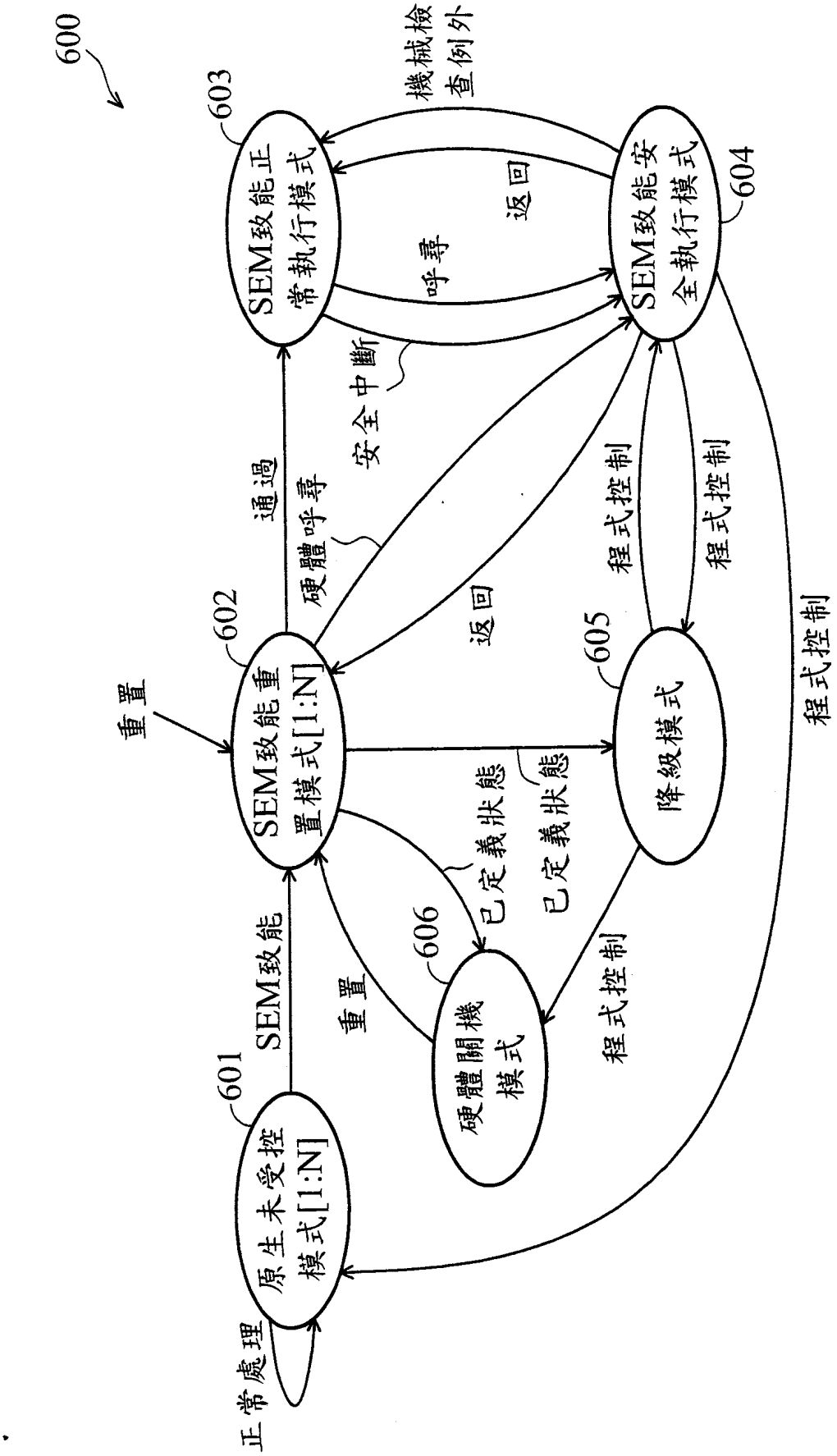
第 3 圖


400
微處理器 401
亂數產生器 412
處理器金鑰暫存器 413
授權的公開金鑰暫存器 404
AES/HASH/RSA單元 405
安全揮發記憶體 406
SEM監控邏輯電路 408
SEM初始化邏輯電路 409
INS
CHK
安全編碼介面邏輯電路 402
安全非揮發記憶體介面單元 407
匯流排介面單元 403
410
411
安全編碼
425
420
安全編碼
421
431
430
安全非揮發記憶體
授權的公開金鑰區域
432

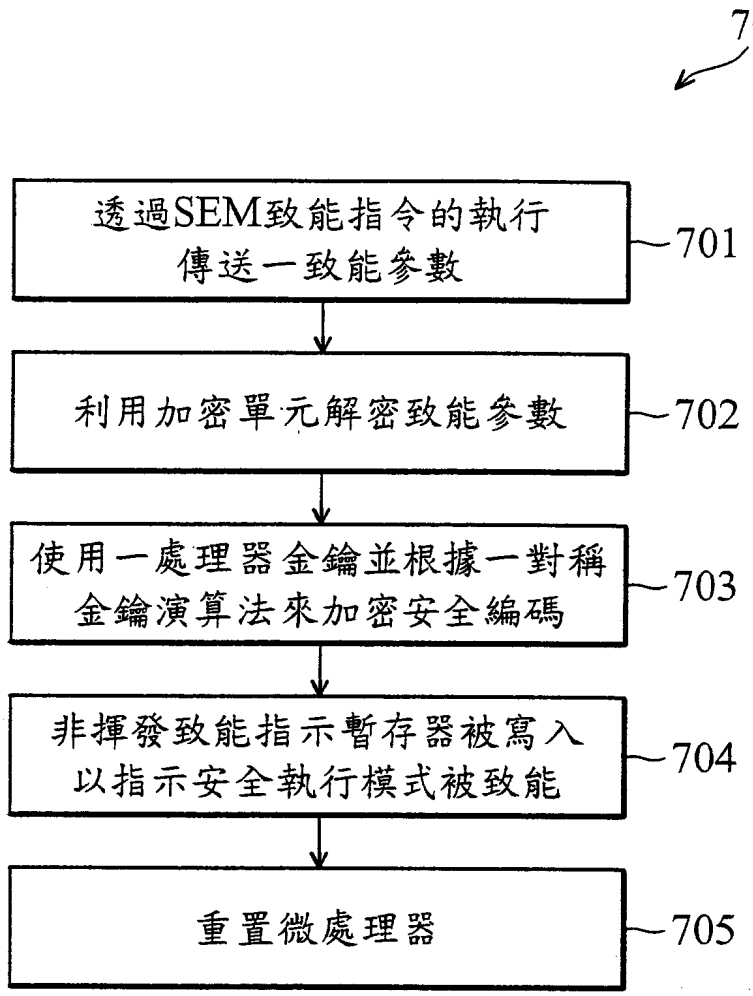
第 4 圖


500
PSNT
VP1
VP2
C1
C2
物理環境監控器
501
NOBOOT
匯流排時脈監控器
502
503
頻率參考單元
TAMPER
BUS CLK
監控管理器
513
CLASS1
CLASS2
CLASS3
DISABLE
VDD
BUSTERM
處理器電壓監控器
504
TEMP
溫度監控器
505
CHK
資料監控器
506
CORE CLK
正常時戳計數器
508
比率機械專用暫存器
509
安全時戳計數器
507
INS
指令監控器
511
指令陣列
512
PINCHK
樣式監控器
510
DESTRUCT

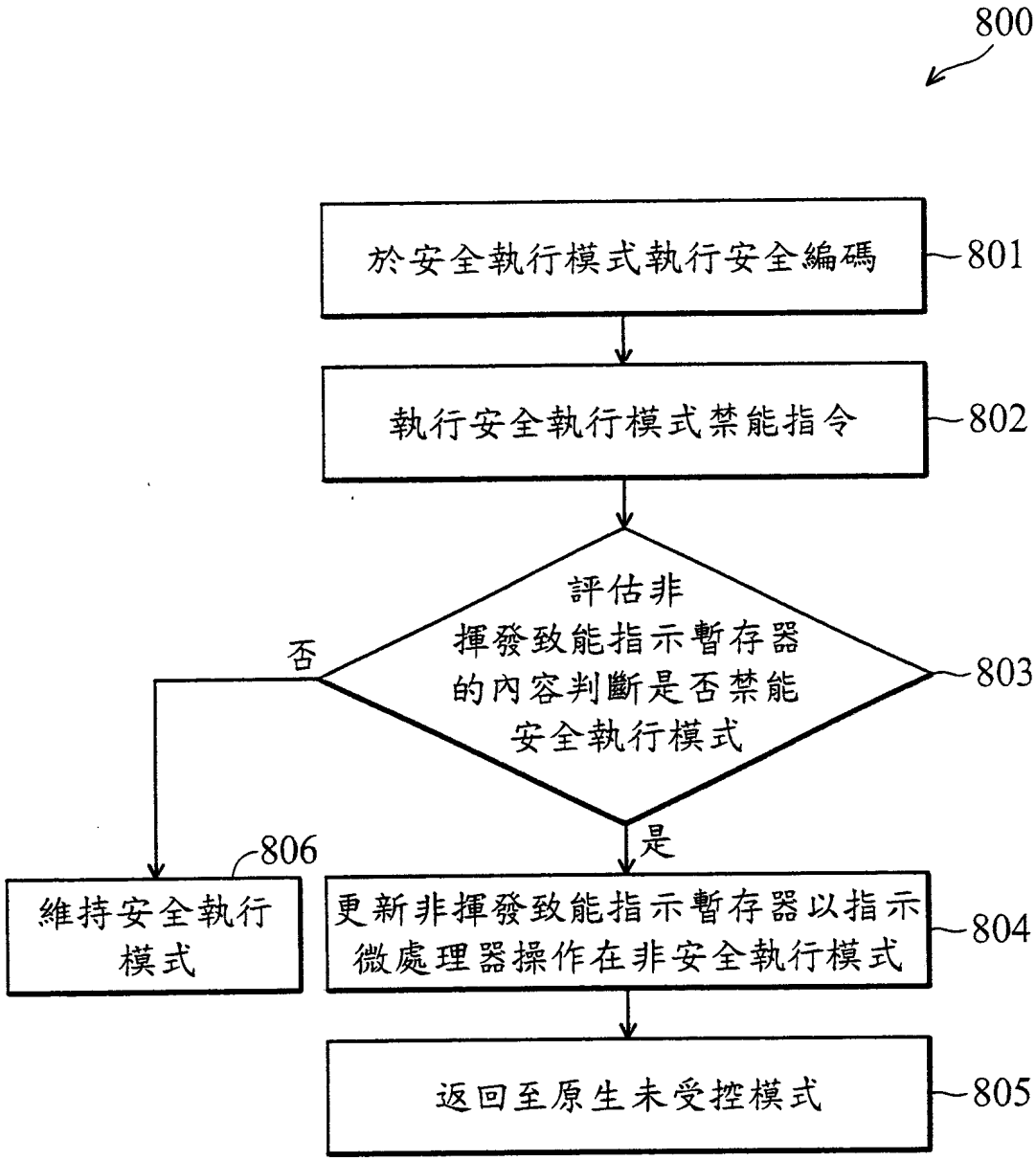
第5圖


600
601
原生未受控模式[1:N]
602
SEM致能重置模式[1:N]
603
SEM致能正常執行模式
604
SEM致能安全執行模式
605
降級模式
606
硬體關機模式
重置
SEM致能
通過
硬體呼尋
安全中斷
機械檢查例外
呼尋
返回
返回
程式控制
程式控制
程式控制
程式控制
已定義狀態
已定義狀態
重置
正常處理

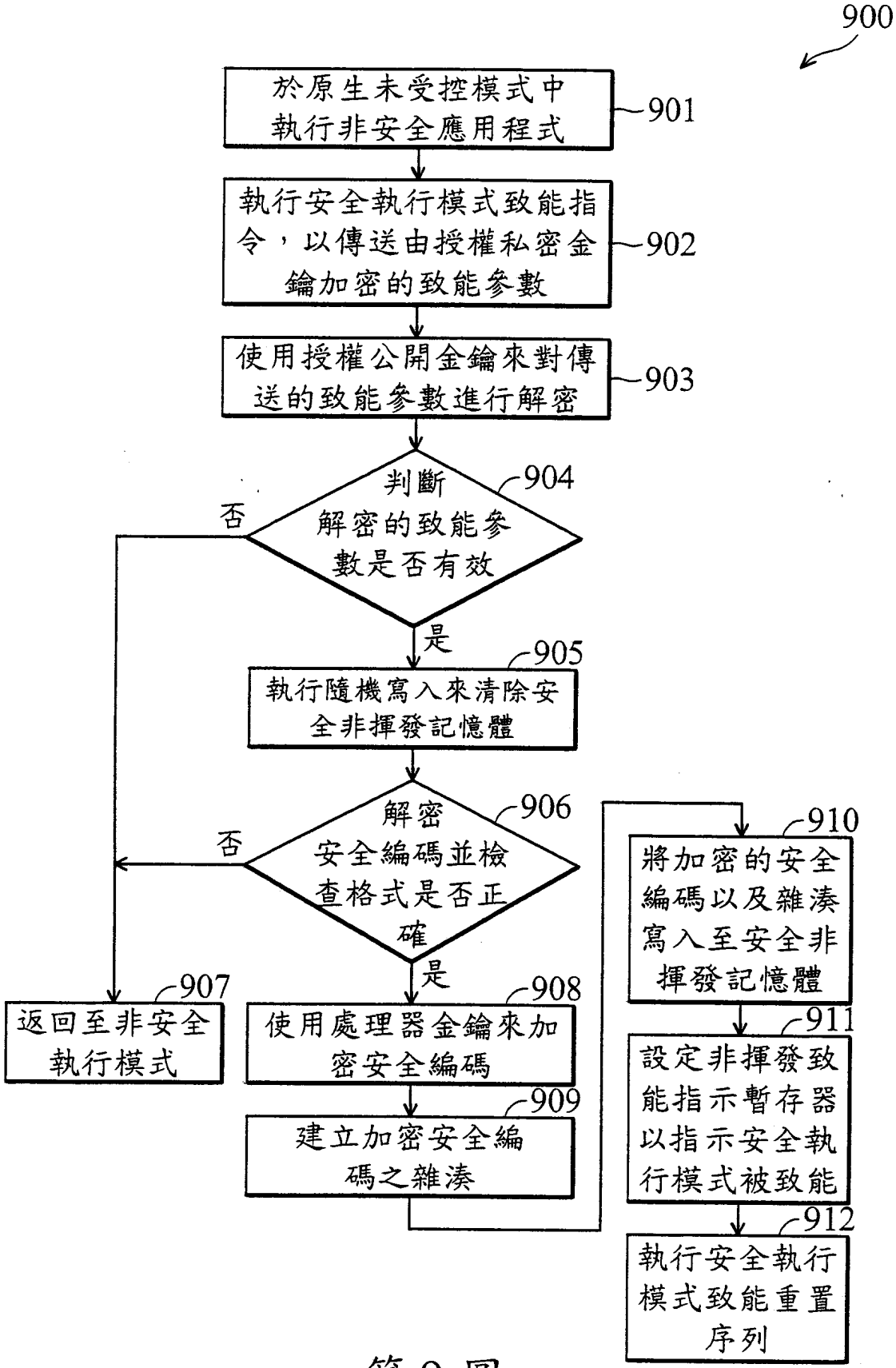
第 6 圖


700
透過SEM致能指令的執行
傳送一致能參數
701
利用加密單元解密致能參數
702
使用一處理器金鑰並根據一對稱
金鑰演算法來加密安全編碼
703
非揮發致能指示暫存器被寫入
以指示安全執行模式被致能
704
重置微處理器
705

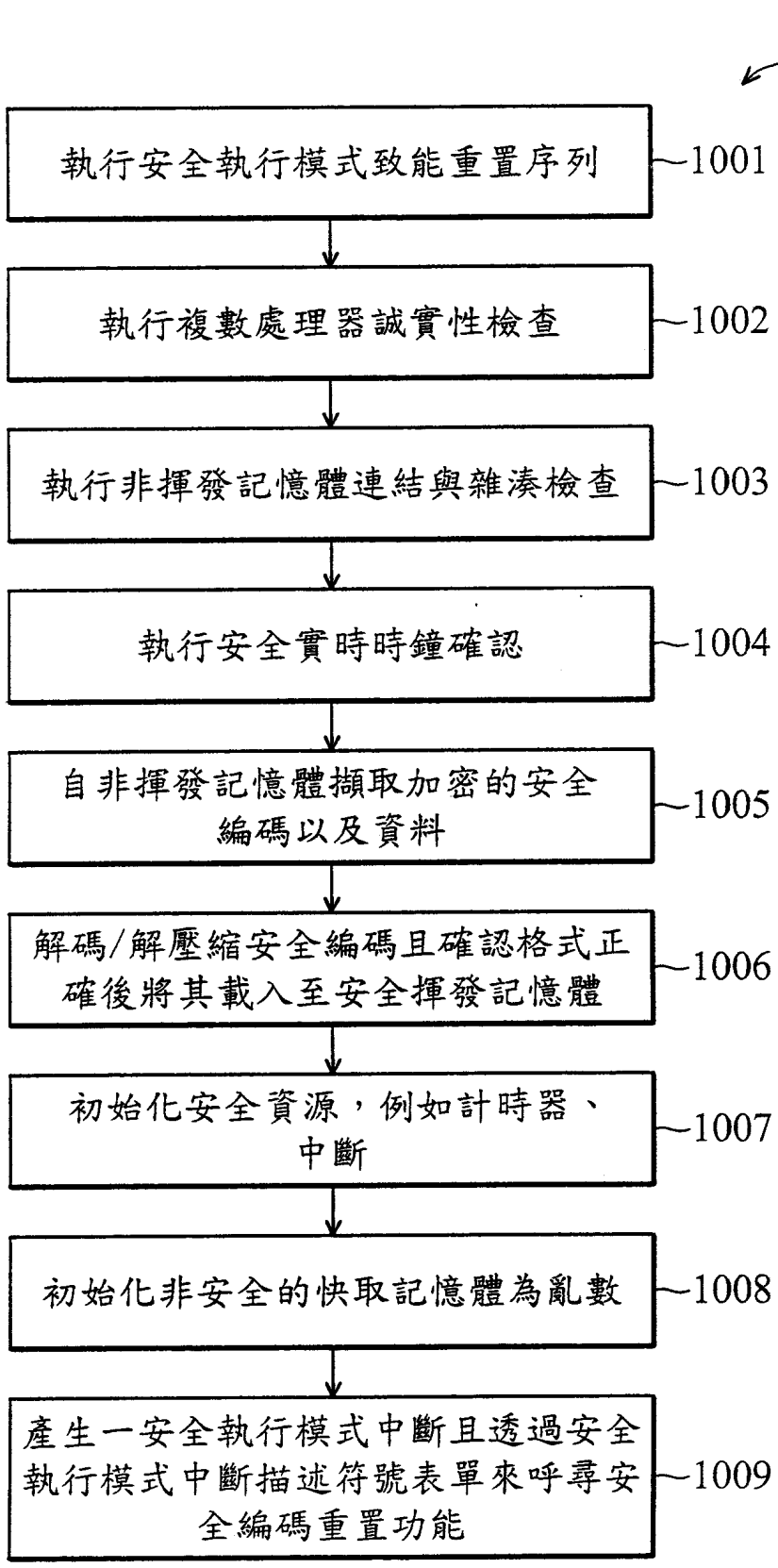
第 7 圖


800
於安全執行模式執行安全編碼
801
執行安全執行模式禁能指令
802
評估非揮發致能指示暫存器的內容判斷是否禁能安全執行模式
803
否
是
806
維持安全執行模式
更新非揮發致能指示暫存器以指示微處理器操作在非安全執行模式
804
返回至原生未受控模式
805

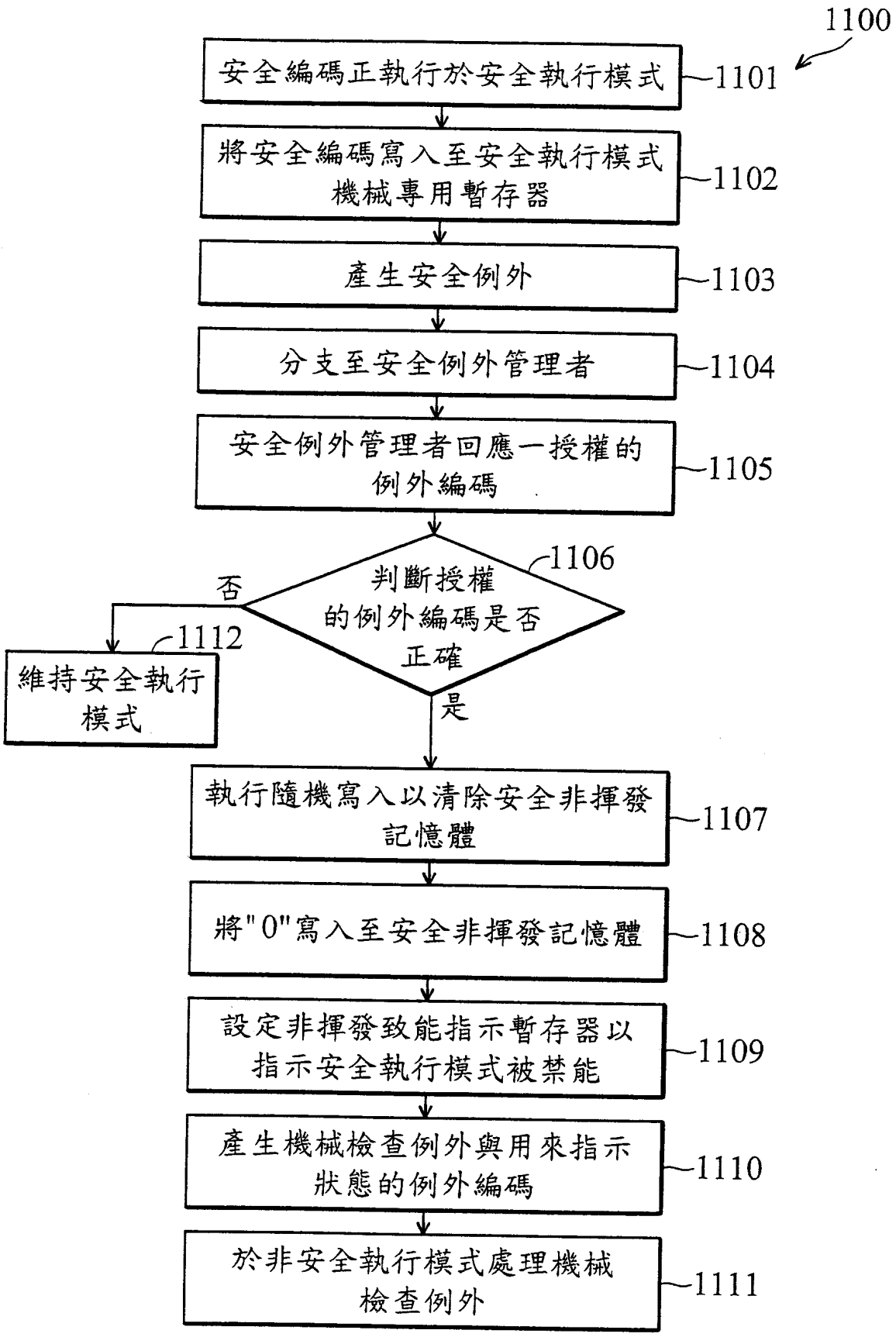
第 8 圖


900
於原生未受控模式中執行非安全應用程式
901
執行安全執行模式致能指令，以傳送由授權私密金鑰加密的致能參數
902
使用授權公開金鑰來對傳送的致能參數進行解密
903
判斷解密的致能參數是否有效
904
否
是
執行隨機寫入來清除安全非揮發記憶體
905
解密安全編碼並檢查格式是否正確
906
否
是
返回至非安全執行模式
907
使用處理器金鑰來加密安全編碼
908
建立加密安全編碼之雜湊
909
將加密的安全編碼以及雜湊寫入至安全非揮發記憶體
910
設定非揮發致能指示暫存器以指示安全執行模式被致能
911
執行安全執行模式致能重置序列
912

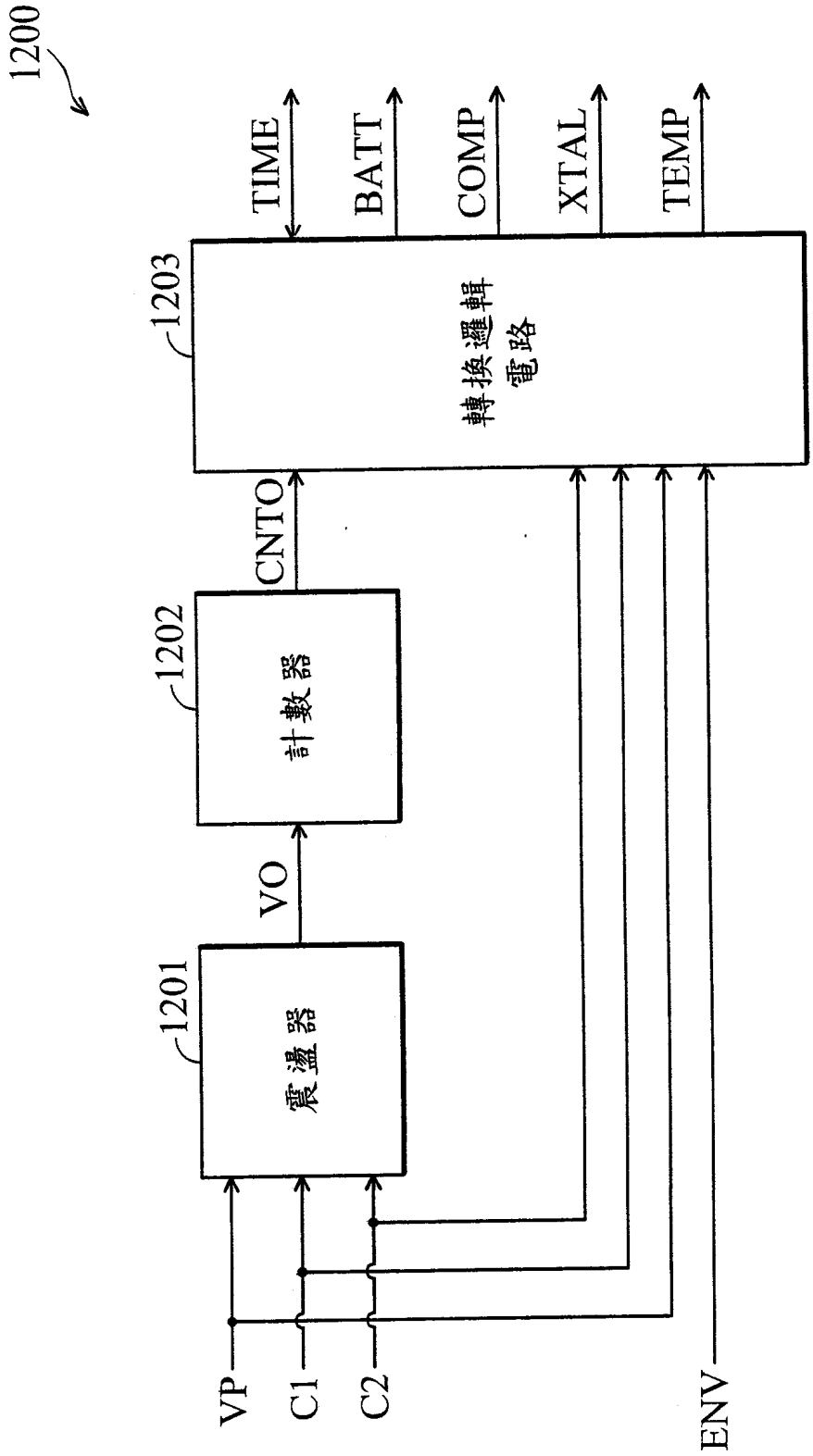
第 9 圖


1000
執行安全執行模式致能重置序列
1001
執行複數處理器誠實性檢查
1002
執行非揮發記憶體連結與雜湊檢查
1003
執行安全實時時鐘確認
1004
自非揮發記憶體擷取加密的安全編碼以及資料
1005
解碼/解壓縮安全編碼且確認格式正確後將其載入至安全揮發記憶體
1006
初始化安全資源，例如計時器、中斷
1007
初始化非安全的快取記憶體為亂數
1008
產生一安全執行模式中斷且透過安全執行模式中斷描述符號表單來呼尋安全編碼重置功能
1009

第 10 圖


1100
安全編碼正執行於安全執行模式
1101
將安全編碼寫入至安全執行模式機械專用暫存器
1102
產生安全例外
1103
分支至安全例外管理者
1104
安全例外管理者回應一授權的例外編碼
1105
判斷授權的例外編碼是否正確
1106
否
是
維持安全執行模式
1112
執行隨機寫入以清除安全非揮發記憶體
1107
將"0"寫入至安全非揮發記憶體
1108
設定非揮發致能指示暫存器以指示安全執行模式被禁能
1109
產生機械檢查例外與用來指示狀態的例外編碼
1110
於非安全執行模式處理機械檢查例外
1111

第 11 圖


1200
1201
震盪器
1202
計數器
1203
轉換邏輯電路
VP
C1
C2
VO
CNTO
ENV
TIME
BATT
COMP
XTAL
TEMP

第 12 圖

四、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：

300～安全執行模式微處理器；301～SEM 邏輯電路；302～安全揮發記憶體；303～處理器狀態；304～安全編碼；305～SEM 初始化邏輯電路；306～SEM 監控邏輯電路；307～SEM 中斷邏輯電路；308～SEM 例外邏輯電路；309～SEM 計時器；310～SEM 實時時鐘；311～AES/HASH/RSA 單元；312～處理器金鑰暫存器；313～處理器執行單元；314～正常例外邏輯電路；315～正常追蹤/除錯邏輯電路；316～正常中斷邏輯電路；317～對應安全編碼之安全資料；318～授權的公開金鑰暫存器；319～亂數產生器；320、321、324、326、327～匯流排；322～電源管理邏輯電路；323～位址邏輯電路；325～非安全記憶體；328～非揮發致能指示暫存器；329～SEM 機械專用暫存器記憶庫。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

略