201935304

(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 201935304 A

(43)公開日： 中華民國 108 (2019) 年 09 月 01 日

(21)申請案號：108104258 (22)申請日： 中華民國 108 (2019) 年 02 月 01 日

(51)Int. Cl.： *G06F21/71 (2013.01)* *H04L9/08 (2006.01)*

(30)優先權：2018/02/08 美國 62/628,123

2018/08/14 美國 16/103,184

(71)申請人：美商美光科技公司 (美國) MICRON TECHNOLOGY, INC. (US)

美國

(72)發明人：愛克爾 納珊 A ECKEL, NATHAN A. (US)；炔克 史蒂芬 D CHECK, STEVEN D. (US)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：20 項 圖式數：9 共 66 頁

(54)名稱

金鑰加密處理

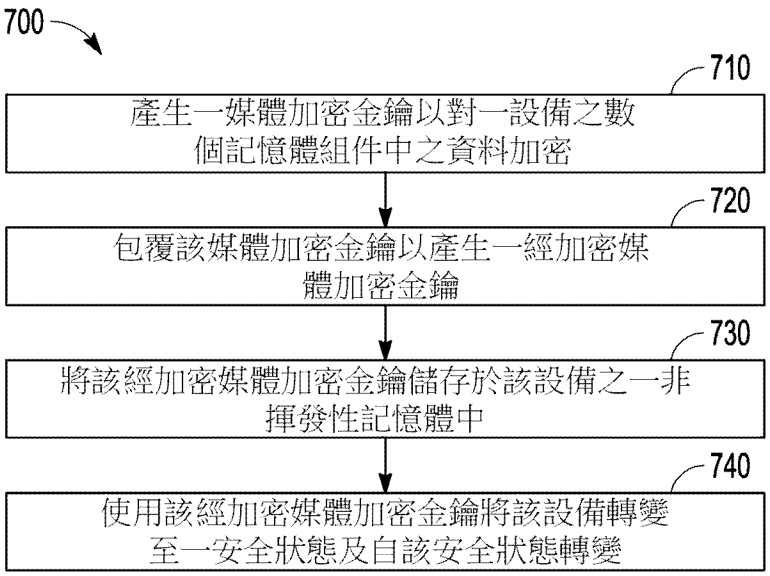
KEY ENCRYPTION HANDLING

(57)摘要

一種設備包括用以產生一媒體加密金鑰以對數個記憶體組件中之資料加密之一加密金鑰產生器，其中該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰。該經加密媒體加密金鑰係儲存於一非揮發性記憶體中。該設備包括具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令之韌體。

An apparatus comprises an encryption key generator to generate a media encryption key to encrypt data in number of memory components, where the encryption key generator is configured to wrap the media encryption key to generate an encrypted media encryption key, The encrypted media encryption key is stored in a non-volatile memory. The apparatus comprises firmware having instructions to transition the apparatus to and from a secure state using the encrypted media encryption key.

指定代表圖：



【圖7】

符號簡單說明：

700・・・方法

710・・・方塊

720・・・方塊

730・・・方塊

740・・・方塊

【發明說明書】

【中文發明名稱】

金鑰加密處理

【英文發明名稱】

KEY ENCRYPTION HANDLING

【技術領域】

【0001】 本發明之實施例大體上係關於記憶體子系統，且更明確言之係關於管理一記憶體子系統，包含關於對該記憶體子系統中之資料加密之金鑰加密處理。

【先前技術】

【0002】 一記憶體子系統可為一儲存系統，諸如一非揮發性雙直列記憶體模組(NVDIMM)，且可包含儲存資料之一或多個記憶體組件。例如，該等記憶體組件可為非揮發性記憶體組件及揮發性記憶體組件。一般而言，一主機系統可利用一記憶體子系統以將資料儲存於記憶體組件處及自記憶體組件擷取資料。

【發明內容】

【0003】 本申請案係關於一種設備，其包括：複數個記憶體組件；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令。

【0004】 本申請案亦係關於一種非揮發性雙直列記憶體模組，其包

括：複數個揮發性記憶體組件；一第一非揮發性記憶體，在偵測一電力故障之後在其中轉儲該等揮發性記憶體組件之內容；一非揮發性控制器，其用以控制該複數個揮發性記憶體組件及該非揮發性記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一第二非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【0005】 本申請案亦係關於一種系統，其包括：一非揮發性雙直列記憶體模組，其經組態以可操作地耦合至一主機裝置，該非揮發性雙直列記憶體模組包含：動態隨機存取記憶體組件；一NAND快閃記憶體，在偵測一電力故障之後在其中轉儲該等動態隨機存取記憶體組件之內容；一非揮發性控制器，其用以控制該等動態隨機存取記憶體組件及該NAND快閃記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該等動態隨機存取記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一NOR快閃記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【0006】 本申請案亦係關於一種方法，其包括：產生一媒體加密金鑰以對一設備之複數個記憶體組件中之資料加密；包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；將該經加密媒體加密金鑰儲存於該設備之一非揮發性記憶體中；及使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變。

【圖式簡單說明】

【0007】 將自下文給出之詳細描述及自本發明之各項實施例之附圖更充分理解本發明。然而，圖式不應被視為將本發明限於特定實施例，而是僅供解釋及理解。

【0008】 圖1繪示根據各項實施例之包含一記憶體子系統之一實例性運算環境。

【0009】 圖2係根據各項實施例之包含經結構化具有用於安全加密之金鑰管理能力之一實例性非揮發性具暫存器之雙直列記憶體模組之一實例性系統的一方塊圖。

【0010】 圖3A係根據各項實施例之產生一經加密媒體加密金鑰以保護一媒體加密金鑰之一包覆方法之一圖解說明。

【0011】 圖3B係根據各項實施例之恢復圖3A之媒體加密金鑰之一解包方法之一圖解說明。

【0012】 圖4係根據各項實施例之一裝置狀態應用程式介面狀態圖之一實例。

【0013】 圖5繪示根據各項實施例之實例性裝置狀態功能應用程式介面。

【0014】 圖6係根據各項實施例之一金鑰產生/恢復單元之一方塊圖。

【0015】 圖7係根據各項實施例之處理加密金鑰之一實例性方法之一流程圖。

【0016】 圖8係根據各項實施例之處理加密金鑰之一實例性方法之一流程圖。

【0017】 圖9係本發明之實施例可在其中操作之一實例性電腦系統之一方塊圖。

【實施方式】

【0018】

優先權申請案

本申請案主張於2018年2月8日申請之美國臨時申請案第62/628,123號及於2018年8月14日申請之美國申請案第16/103,184號之優先權利，該等案之全文以引用的方式併入本文中。

【0019】 本發明之態樣係關於管理一記憶體子系統，該管理包含關於對該記憶體子系統中之資料加密之金鑰加密處理。加密係將資料、程式、影像或其他資訊轉換成不可讀密文之一安全技術。此轉換可使用應用於原始內容意欲用於加密之複雜演算法來執行。一加密金鑰係為對資料攪碼及解攪碼而明確建立之一隨機位元字串且通常經設計具有意欲確保每個金鑰不可預測且唯一之演算法。如本文中所論述，金鑰加密包含對一加密金鑰加密。一記憶體子系統在下文亦被稱為一「記憶體裝置」。一記憶體子系統之一實例係一儲存系統，諸如一非揮發性雙直列記憶體模組(NVDIMM)。在一些實施例中，該記憶體子系統係一混合記憶體/儲存子系統。一般而言，一主機系統可利用包含一或多個記憶體組件之一記憶體子系統。該主機系統可提供待儲存於該記憶體子系統處之資料且可請求自該記憶體子系統擷取資料。

【0020】 一NVDIMM係具有用於正常操作之揮發性記憶體及(若電力出現故障則)使用一機載備份電源在其中轉儲該揮發性記憶體之內容之非揮發性記憶體之一隨機存取記憶體類型。NVDIMM-N係在相同模組上

具有快閃儲存裝置及傳統動態隨機存取記憶體(DRAM)之一雙直列記憶體模組(DIMM)。一主機處理單元可直接存取傳統DRAM。倘若發生電力故障，NVDIMM-N將資料自其揮發性傳統DRAM複製至其永久性快閃儲存裝置，且在電力恢復時將資料複製回至揮發性傳統DRAM。NVDIMM-N之一類型係一NVRDIMM-N。NVRDIMM-N係一非揮發性具暫存器之雙直列記憶體模組(DIMM)，其係針對企業級伺服器系統之一標準具暫存器之DIMM (RDIMM)。就具暫存器而言，意謂具暫存器之記憶體模組(亦被稱為緩衝記憶體模組)包含介於動態隨機存取記憶體(DRAM)模組與一各自系統記憶體控制器之間的一暫存器，其中一DRAM模組含有數個DRAM (其等係揮發性記憶體)。RDIMM使用將控制信號緩衝至模組之一硬體暫存器。

【0021】 在用於NVRDIMM-N之一架構中，作為以組態其基本記憶體胞元之反及(NAND)邏輯形式命名之一永久性儲存裝置之一NAND記憶體係與標準DRAM一起配置。因為一DRAM係揮發性的，所以在移除該DRAM之電力時，該DRAM中之資料丟失。當在NVRDIMM-N中偵測斷電或自一主機接收偵測一即將斷電之一信號時，擷取DRAM之當前狀態並將其移動至藉由NVRDIMM-N之一NAND提供之永久性儲存裝置中。藉由記錄電腦之當前狀態，當再次提供電力時，可將資料自NAND拉回至DRAM，且一應用程式之執行可自由於電力移除而導致執行停止之點繼續進行。此能力為企業級伺服器系統提供價值。

【0022】 在NVRDIMM-N中，對DRAM提供一DRAM控制器且對NAND提供一NAND控制器，其中NVRDIMM-N負責將NVRDIMM-N之DRAM之所有資料之狀態轉換為NVRDIMM-N之NAND上之永久性資

料。可在一電力循環上執行將所有DRAM資料之狀態轉換為NAND上之永久性資料。隨後，NVRDIMM-N負責將NAND中之永久性資料傳送回至DRAM中。

【0023】 一企業級系統通常儲存保密資訊，且因此在永久性地儲存此資料時，傳送至NAND之資料受到保護。例如，在將資料自DRAM傳送至NAND時，可藉由密文竊取(XTS)加密引擎(其係用於資料之一標準加密引擎)透過基於高級加密標準(AES) 256位元互斥或-加密-互斥或(XEX)之調整碼本模式運行資料傳送，使得所有資料皆藉由此加密儲存。一AES-XTS加密引擎需要金鑰(即，一加密AES金鑰及一XTS金鑰)。通常，此等金鑰自一主機傳遞至NVRDIMM-N中。對關於一記憶體子系統之處理加密金鑰及傳遞金鑰之加強可提供一機制以避免與駭客試圖經由來自一主機之命令或一主機之預期動作存取加密金鑰相關聯之問題，該等問題可能不利地影響經儲存之安全資料。

【0024】 本發明之態樣藉由對用於一記憶體子系統之一存取加密金鑰加密，將該經加密之加密金鑰儲存於該記憶體子系統之非揮發性記憶體中，使用韌體以使用該經加密媒體加密金鑰將該記憶體子系統轉變至資料之安全狀態及自資料之安全狀態轉變，從而解決與該存取加密金鑰相關聯之上述及其他缺點。在各項實例性實施例中，用一存取金鑰或一擦除金鑰(此取決於操作)對一金鑰加密及存取該金鑰以保護該金鑰免受一記憶體子系統中之駭客攻擊。可透過使金鑰在統計上不可破解之各種演算法處理金鑰。一裝置(諸如但不限於一NVDIMM-N)可作為一多狀態裝置操作，其中可藉由用於安全加密之金鑰管理來處理NVDIMM-N之狀態之間的轉變，其中狀態可藉由裝置儲存之資料之安全性予以定義。

【0025】 圖1繪示根據本發明之一些實施例之包含一記憶體子系統110之一實例性運算環境100。記憶體子系統110可包含媒體(諸如記憶體組件112A至112N)。記憶體組件112A至112N可為揮發性記憶體組件、非揮發性記憶體組件或此等之一組合。在一些實施例中，記憶體子系統110係一儲存系統。一儲存系統之一實例係一NVDIMM。在一些實施例中，記憶體子系統110係一混合記憶體/儲存子系統。一般而言，運算環境100可包含使用記憶體子系統110之一主機系統120。例如，主機系統120可將資料寫入至記憶體子系統110及自記憶體子系統110讀取資料。

【0026】 主機系統120可為一運算裝置，諸如一桌上型電腦、膝上型電腦、網路伺服器、行動裝置，或包含一記憶體及一處理裝置之此運算裝置。主機系統120可包含記憶體子系統110或耦合至記憶體子系統110使得主機系統120可自記憶體子系統110讀取資料或將資料寫入至記憶體子系統110。主機系統120可經由一實體主機介面耦合至記憶體子系統110。如本文中所使用，「耦合至」大體上係指組件之間之一連接，該連接可為一間接通信連接或直接通信連接(例如，無中介組件)，無論有線或無線，包含諸如電連接、光學連接、磁性連接等之連接。一實體主機介面之實例包含(但不限於)一串列進階附接技術(SATA)介面、一周邊組件快速互連(PCIe)介面、通用串列匯流排(USB)介面、光纖通道、串列附接SCSI(SAS)等。該實體主機介面可用於在主機系統120與記憶體子系統110之間傳輸資料。主機系統120可進一步利用一NVM快速(NVMe)介面以在記憶體子系統110藉由PCIe介面與主機系統120耦合時存取記憶體組件112A至112N。實體主機介面可提供用於在記憶體子系統110與主機系統120之間傳遞控制項、位址、資料及其他信號之一介面。

【0027】 記憶體組件112A至112N可包含不同類型之非揮發性記憶體組件及/或揮發性記憶體組件之任何組合。非揮發性記憶體組件之一實例包含一反及(NAND)類型快閃記憶體。記憶體組件112A至112N之各者可包含一或多個記憶體胞元陣列，諸如單位階胞元(SLC)或多位階胞元(MLC) (例如，三位階胞元(TLC)或四位階胞元(QLC))。在一些實施例中，一特定記憶體組件可包含記憶體胞元之一SLC部分及一MLC部分兩者。記憶體胞元之各者可儲存供主機系統120使用之一或多個資料位元(例如，資料區塊)。儘管描述非揮發性記憶體組件(諸如NAND類型快閃記憶體)，但記憶體組件112A至112N可基於任何其他類型之記憶體(諸如一揮發性記憶體)。在一些實施例中，記憶體組件112A至112N可為(但不限於)隨機存取記憶體(RAM)、唯讀記憶體(ROM)、動態隨機存取記憶體(DRAM)、同步動態隨機存取記憶體(SDRAM)、相變記憶體(PCM)、磁式隨機存取記憶體(MRAM)、反或(NOR)快閃記憶體、電可擦除可程式化唯讀記憶體(EEPROM)及一交叉點陣列之非揮發性記憶體胞元。一交叉點陣列之非揮發性記憶體可結合一可堆疊交叉柵格式資料存取陣列一起基於體電阻之一變化執行位元儲存。此外，與許多基於快閃之記憶體相反，交叉點非揮發性記憶體可執行一原處寫入操作，其中可程式化一非揮發性記憶體胞元而無需在先前擦除該非揮發性記憶體胞元。此外，記憶體組件112A至112N之記憶體胞元可分組為可係指用於儲存資料之記憶體組件之一單元之記憶體頁或資料區塊。

【0028】 記憶體系統控制器115 (在下文被稱為「控制器」)可與記憶體組件112A至112N通信以執行操作，諸如在記憶體組件112A至112N處讀取資料、寫入資料或擦除資料及其他此等操作。控制器115可包含硬

體，諸如一或多個積體電路及/或離散組件、一緩衝記憶體或其等之一組合。控制器115可為一微控制器、專用邏輯電路(例如，一場可程式化閘陣列(FPGA)、一特定應用積體電路(ASIC)等)，或其他合適處理器。控制器115可包含經組態以執行儲存於本端記憶體119中之指令之一處理器(處理裝置) 117。在所繪示實例中，控制器115之本端記憶體119包含經組態以儲存用於執行控制記憶體子系統110之操作(包含處理記憶體子系統110與主機系統120之間的通信)之各種程序、操作、邏輯流程及常式之指令之一嵌入式記憶體。在一些實施例中，本端記憶體119可包含儲存記憶體指標、經提取資料等之記憶體暫存器。本端記憶體119亦可包含用於儲存微碼之唯讀記憶體(ROM)。雖然圖1中之實例性記憶體子系統110已繪示為包含控制器115，但在本發明之另一實施例中，一記憶體子系統110可能不包含一控制器115，且可代替性地依靠(例如，藉由一外部主機或藉由與該記憶體子系統分離之一處理器或控制器提供之)外部控制。

【0029】 一般而言，控制器115可自主機系統120接收命令或操作且可將該等命令或操作轉換成用以實現對記憶體組件112A至112N之所要存取之指令或適當命令。控制器115可負責其他操作，諸如損耗平衡操作、廢棄項目收集操作、錯誤偵測及錯誤校正碼(ECC)操作、加密操作、快取操作及一邏輯區塊位址與記憶體組件112A至112N所相關聯之一實體區塊位址之間的位址變換。控制器115可進一步包含經由實體主機介面與主機系統120通信之主機介面電路。該主機介面電路可將自主機系統接收之命令轉換成用以存取記憶體組件112A至112N之命令指令以及將與記憶體組件112A至112N相關聯之回應轉換成用於主機系統120之資訊。

【0030】 記憶體子系統110亦可包含未繪示之額外電路或組件。在

一些實施例中，記憶體子系統110可包含一快取區或緩衝器(例如，DRAM)及可自控制器115接收一位址且解碼該位址以存取記憶體組件112A至112N之位址電路(例如，一列解碼器及一行解碼器)。

【0031】 記憶體子系統110包含一金鑰加密處理組件113，金鑰加密處理組件113可用於對一加密金鑰加密，儲存該經加密加密金鑰及使用該經加密媒體加密金鑰管理進出資料之安全狀態之轉變。在一些實施例中，控制器115包含金鑰加密處理組件113之至少一部分。例如，控制器115可包含經組態以執行儲存於本端記憶體119中之指令以用於執行本文中所描述之操作之一處理器117 (處理裝置)。在一些實施例中，金鑰加密處理組件113係記憶體系統110、一應用程式或一作業系統之部分。

【0032】 金鑰加密處理組件113可產生一媒體加密金鑰以對記憶體子系統110之記憶體組件112A至112N之資料加密。金鑰加密處理組件113可經組態以產生一經加密媒體加密金鑰。金鑰加密處理組件113可將該經加密加密金鑰儲存於記憶體子系統110之非揮發性記憶體中。金鑰加密處理組件113可存取儲存經加密加密金鑰之非揮發性記憶體且解包經加密加密金鑰以在改變關於記憶體子系統110中保護之資料之狀態時使用加密金鑰。關於金鑰加密處理組件113之操作之進一步細節將在下文描述。

【0033】 圖2係根據各項實施例之包含經結構化具有用於安全加密之金鑰管理能力之一實例性非揮發性具暫存器之雙直列記憶體模組之一實例性系統的一方塊圖。一NVRDIMM-N 200可包含：一非揮發性控制器(NVC) 204；用以儲存資料之揮發性記憶體組件222-0至222-17，其中該等記憶體之各者可為雙倍資料速率第四代動態隨機存取記憶體(DDR4)類型之DRAM；一非揮發性記憶體224，其可為一NAND快閃記憶體，若電

力出現故障則在其中轉儲揮發性記憶體之內容；及一DIMM電力單元226，其自一主機230接收數個不同電壓且將數個不同電壓提供至NVRDIMM-N 200之組件。NVC 204可包含控制DRAM 222-0至222-17之一DRAM控制器211及控制NAND快閃記憶體224之一NAND快閃控制器218。NVC 204可包含一電力控制及狀態212、用以維持時序關係之一計時及鎖相迴路(PLL) 213、一暫存器/主機介面214、一本端通信介面(LCOM) 216、一內部積體電路(I^2C) 217、可具有一先進先出(FIFO)格式之資料緩衝器219、一處理器208及一串列周邊介面(SPI) 209。NVRDIMM-N 200亦可包含識別NVRDIMM-N 200之一串列存在偵測(SPD) 223。

【0034】 NVRDIMM-N 200可與主機230一起操作以保存資料及返回資料或提供關於NVRDIMM-N 200上之事件之其他資訊。NVRDIMM-N 200與主機230之間的通信可透過一匯流排240。NVRDIMM-N 200包含耦合至NVC 204之LCOM 216且可與主機230通信之一非揮發性暫存時脈驅動器(NVRCD) 229。

【0035】 可使用加密金鑰保護儲存於NVRDIMM-N 200中之資料。該等加密金鑰可儲存於NVRDIMM-N 200上之非揮發性記憶體中(諸如儲存於一NOR快閃記憶體206中)。在資料處於一受保護條件下時，NVRDIMM-N 200係在一安全狀態中。可藉由一韌體201使用一金鑰產生及恢復單元202控制進入及退出一安全狀態之轉變。可藉由在NVC 204內部之處理器208執行韌體201中之指令以處理儲存於NOR快閃記憶體206中及透過SPI 209自NOR快閃記憶體206擷取之金鑰。處理器208可為一精簡指令集電腦(RISC)處理器。儘管主機230可提供用於金鑰產生及恢復之輸

入，但NVRDIMM-N 200可經結構化使得韌體201控制來自主機230之輸入，其中主機230並不直接存取或控制金鑰產生及恢復單元202。韌體201可提供NVRDIMM-N 200中之金鑰處理程序與來自NVRDIMM-N 200外部之來源之侵入之一隔離。

【0036】 可能涉及許多加密金鑰。加密金鑰之一者係一媒體加密金鑰(MEK)，其係保護靜態資料之主要金鑰。靜態意謂資料並不處於對資料執行操作之一狀態中。MEK係使用一確定性隨機數產生器(DRBG)在NVRDIMM-N 200內部產生。該產生可依許多方式進行。可根據一政府標準(例如，國家標準與技術研究院(NIST) SP800-90A)產生MEK。所產生之MEK可為由一AES-XTS-256加密引擎用於資料之一256位元金鑰。

【0037】 256位元金鑰實際上為512個位元，因為使用DRBG產生用於加密之AES部分之一金鑰及產生用於加密之XTS部分之一金鑰。若此MEK係在內部產生並在內部儲存，則在電力消失時，該金鑰將因為其在揮發性儲存裝置中而消失。實施一程序以保護此媒體加密金鑰。

【0038】 在此一程序中，可藉由主機經由一I^2C匯流排將一存取金鑰(AK)供應至NVRDIMM-N之一NVC。在該NVC接收該AK之後即可對該AK加密，以提供保護MEK之一媒體金鑰加密金鑰MKEK。此加密可依許多方式進行。例如，可用基於密碼之金鑰導出函數(PBKDF)或基於密碼之金鑰導出函數2 (PBKDF2)根據一政府標準(例如，NIST SP800-232)對MEK金鑰加密。

【0039】 如上文所提及，DRBG在內部產生藉由產生MKEK之一加密演算法(諸如一PBKDF演算法)保護之MEK。接著，使用另一演算法藉由MKEK包覆MEK以產生一經加密媒體加密金鑰(EMEK)。金鑰包覆構造

係經設計以囊封(即，加密)密碼編譯金鑰材料之一類對稱加密演算法。用MKEK包覆MEK可使用一包覆演算法根據NIST SP800-38F來進行。所產生之EMEK可儲存於NVRDIMM-N之一非揮發性記憶體中。例如，可將EMEK寫入至NVRDIMM-N之一NOR快閃，其中NOR快閃係以組態基本記憶體胞元之邏輯形式命名之一快閃。NOR快閃記憶體與NAND快閃記憶體相比讀取更快，但與用NAND快閃記憶體相比耗費更長時間來擦除及寫入新資料，而NAND快閃記憶體通常具有高於NOR快閃記憶體之一儲存容量。

【0040】 為使用MEK來存取受保護資料，自NOR快閃記憶體擷取EMEK。對EMEK與MKEK之組合執行金鑰解包以產生可對於受保護資料使用之MEK。解包提供完整性檢查。若解包有效，則金鑰之授權遵循解包。

【0041】 圖3A係根據各項實施例之產生一經加密媒體加密金鑰以保護一媒體加密金鑰之一包覆方法之一圖解說明。此圖繪示如上文所論述之產生一EMEK以保護一MEK之一包覆程序。DRBG 303產生放置於一MEK暫存器305中之一MEK，其中該MEK係用於保護資料。DRBG 303亦產生一鹽值(salt)。一鹽值係可實施為隨機位元之用於使攻擊者之解密效率降低之一隨機數。例如，可將一鹽值增加至一加密演算法之頂上之另一散列層。當一通行片語用於對資料加密時，一鹽值可為序連至該通行片語或金鑰之額外資料。作為該序連之結果，一攻擊者之字典現需要含有更多條目，每個條目針對用於各可能通行片語之各可能鹽值。鹽值係用於包覆一經接收存取金鑰，其中該包覆可經由一PBKDF 307進行以產生一MKEK。一金鑰包覆件310使用MKEK來包覆MEK以產生EMEK。EMEK

可儲存於一NOR快閃記憶體中。

【0042】 圖3B係根據各項實施例之恢復圖3A之媒體加密金鑰之一解包方法之一圖解說明。此圖繪示恢復圖3A之MEK之一解包程序。用於包覆存取金鑰之鹽值可與來自主機之相同存取金鑰一起使用以經由PBKDF 307產生MKEK。可擷取儲存於NOR快閃記憶體中之EMEK。一金鑰解包件320使用所產生之MKEK及經儲存之EMEK產生MEK。可使用習知解包演算法(例如)根據一政府標準(諸如NIST SP800-38F)執行解包。若解包程序成功，則僅將MEK恢復(例如)至MEK暫存器305。

【0043】 如所提及，當在具有一NVRDIMM-N之一機器斷電之後對該機器通電時，已在該NVRDIMM-N之一NAND中加密之資料將被恢復至NVRDIMM-N之適當DRAM。存取此經加密資料之唯一方式係產生在NOR快閃中經包覆及保護使得一駭客無法將其撤銷之MEK。為獲取MEK，應將存取金鑰傳遞至NVRDIMM-N中。將包覆程序中之鹽值返回至存取金鑰，PBKDF演算法再次對存取金鑰操作以提供MKEK。自NOR快閃記憶體讀取EMEK並使用MKEK將EMEK解包(此與包覆程序相反)以產生MEK。MEK係用於對靜態受保護資料解密。

【0044】 NVC (諸如圖2之NVC 204)可經配置以具有四種裝置狀態，其中該四種裝置狀態之間的轉變使用藉由一主機(諸如圖2之主機230)發送至NVC之兩種類型之金鑰。該兩種類型之金鑰係一AK及一擦除金鑰(EK)。該AK係用於存取資料，解除鎖定NVC及使存取金鑰旋轉。該EK係用於破壞資料或取消部件安全性以改變部件中之金鑰。EK可用一隨機數包覆且作為一經包覆擦除金鑰(WEK)儲存於NOR快閃記憶體中。EK維持與AK完全相同之安全層級。四種裝置狀態係一無主狀態、一不安全狀

態、一安全解除鎖定狀態及一安全鎖定狀態。裝置所有權區分使用加密與不使用加密。一旦一裝置移至鎖定狀態中，就會阻止對資料之基於安全性動作。NAND是否可讀及可寫入意謂是否存在一有效MEK，呈經包覆形式之MEK是否儲存於NOR快閃記憶體中，是否已產生任何金鑰，或是否已獲取NVC裝置之所有權，此涉及不安全狀態、安全解除鎖定狀態或安全鎖定狀態。

【0045】 關於一存取金鑰及一擦除金鑰之實施方案可依許多方式進行。該實施方案之一部分可包含暫存器轉移層級(RTL)且該實施方案之一部分可包含韌體。RTL提供依據硬體暫存器之間的數位信號(資料)流及對該等信號執行之邏輯操作模型化一同步數位電路之一技術。RTL層級之設計係設計數位組件之典型做法。可在RTL中執行之用於金鑰處理之引擎包含DRBG、金鑰加密(諸如PBKDF2)、包覆及解包。

【0046】 韌體係在一硬體裝置上程式化之一軟體程式或指令集。其提供該裝置如何與其他電腦相關硬體通信之指令。韌體可涉及用於金鑰處理之移動及追蹤。其可處理金鑰傳遞，即，其引導金鑰之移動且呼叫金鑰加密(諸如PBKDF2)。韌體亦處理NOR快閃存取以用於儲存經包覆加密之金鑰及用於恢復經包覆加密之金鑰。韌體可處理控制串列周邊介面(SPI)對NOR快閃之存取。SPI係通常用於在微控制器與小週邊設備(諸如移位暫存器、感測器及SD卡)之間發送資料之一介面匯流排。SPI可使用分離時脈及資料線連同選擇將與哪一裝置通信之一選擇線。

【0047】 韌體可執行應用程式介面(API)呼叫。一API係指定軟體組件應互動所藉助之方式之一組常式、協定及工具。一API呼叫(其亦可被稱為一API請求)表示使一應用程式執行藉由該應用程式定義之任務之一特定

操作。韌體可執行針對待使用之一正確硬體引擎之一API呼叫，以設置資料路徑。韌體亦可處理裝置狀態以控制裝置狀態之檢查、追蹤及更新。韌體之功能可包含維持用於錯誤處理之紀錄狀態。控制API呼叫之韌體提供使韌體定位所處之NVRDIMM-N介接至可操作地耦合至NVRDIMM-N之一主機之一機制。該主機可首先將金鑰傳遞至NVRDIMM-N中且接著設定與NVRDIMM-N相關聯之API。此韌體可實施於其他NVDIMM裝置上。

【0048】 關於最初出廠之NVRDIMM-N裝置之四種不同裝置狀態，裝置係在一無主狀態中(此係工廠預設狀態且金鑰係預設)，此意謂不具有對使用者資料之保護。在此狀態中，若主機將資料自一DRAM儲存至一NAND，則可藉由可耦合至NVRDIMM-N之任何裝置(諸如一駭客裝置)讀取資料。若應受保護之使用者資料係在一無主狀態中(諸如裝置在出廠時般)，則使用者資料不受保護。三個API可連同在該等API之間傳遞且透過演算法處理之金鑰一起使用(如參考上文圖3A至圖3B論述)以保護使用者資料。裝置之狀態可自一無主狀態移動至一受保護解除鎖定狀態。在一安全解除鎖定狀態中，可在內部產生之一有效MEK可用於保存及恢復經加密資料。該MEK可使用解包程序自快閃恢復。裝置係在一受保護狀態中，但裝置經解除鎖定。當資料應受保護或裝置斷電時，可將裝置置於安全鎖定狀態中。在安全鎖定狀態中，可用儲存於NOR快閃中之一EMEK刪除揮發性記憶體中之所有內容。NAND中之使用者資料不可存取。所有內容係鎖定在一防駭客條件下。

【0049】 四種裝置狀態可根據許多特徵特性化。處於無主狀態中之裝置狀態對應於具有預設金鑰之一工廠預設狀態。在不安全狀態中，不存

在對裝置之NAND之資料存取。在secure_unlocked狀態中，一所產生MEK係有效的且裝置係在一保存及恢復模式中。在secure_unlocked狀態中，MEK之來源可為新的，自使用一存取金鑰及擦除金鑰建立新MEK之一DRBG產生。在secure_unlocked狀態中，MEK之來源在一恢復程序中可為在一解包程序中使用一存取金鑰之NOR快閃。在secure_locked狀態中，一EMEK係儲存於NOR快閃中，EMEK所基於之MEK經刪除，且資料不可存取。

【0050】 圖4係根據各項實施例之一裝置狀態應用程式介面狀態圖之一實例。操作狀態係在韌體中使用API呼叫及自主機傳入之存取金鑰實施，其中主機可在主機基本輸入/輸出系統(BIOS)中實施金鑰傳遞，BIOS係用於在通電啟動期間執行硬體初始化及對作業系統及程式提供運行時服務之非揮發性韌體。在一裝置狀態API狀態圖400中，在430，具有可藉由在431檢查裝置狀態而開始初始化之一初始狀態或一重設狀態。在先前裝置狀態處於一secure_locked狀態之情況下，裝置可進入該secure_locked狀態448中。在先前裝置狀態處於一不安全狀態之情況下，裝置可進入一不安全狀態446中。在先前裝置狀態處於一無主狀態之情況下，裝置可進入一無主狀態442中，主機可供應進入一secure_unlocked狀態444中之初始金鑰及API，裝置可自secure_unlocked狀態444鎖定於一secure_locked狀態448中。

【0051】 為將無主狀態442轉變至secure_unlocked狀態444，供應存取密碼及擦除密碼且接著產生初始化金鑰(init_keys)以使裝置置於secure_unlocked狀態444中。此轉變係以與用於自不安全狀態446轉變至secure_unlocked狀態444相同之方式執行。自secure_unlocked狀態444至

無主狀態442之轉變係將裝置返回至工廠預設狀態之一轉變。為執行此轉變，需要一擦除金鑰。該擦除金鑰經檢查為有效的。若擦除金鑰有效，則自揮發性記憶體及非揮發性記憶體清除金鑰及EMEK兩者。一般而言，此在安全圈中亦被稱為加密擦除。

【0052】若裝置接著將經解除鎖定，則檢查自主機接收之存取金鑰，因為裝置係在secure_locked狀態448中。為自secure_locked狀態448進入secure_unlocked狀態444，自NOR快閃記憶體讀出一EMEK，解包該EMEK並在433根據藉由主機傳入以執行解除鎖定之存取金鑰對該EMEK進行檢查。由於運行統計上應保護先前產生之存取金鑰之解包演算法及判定存取金鑰並不相配，可記錄可呈「Key Not Valid」之形式之一錯誤。例如，若一駭客在試圖存取資料時傳入一猜測存取金鑰，則使用儲存於NOR快閃記憶體中之經加密金鑰之檢查將該猜測存取金鑰識別為無效且記錄一錯誤。可實施一計時器及數次檢查使得若經接收存取金鑰之檢查在一特定時間或特定次數檢查內並不匹配來自NOR快閃記憶體之經解包金鑰，則嘗試存取資料之機器或應用程式將被鎖定在外。例如，檢查之次數可為十次以在嘗試存取資料之存取機器或應用程式被鎖定在外之前容許十次存取嘗試。經指定嘗試之次數可具有一增加參數，即在一指定時間內將進行之經指定嘗試之次數。經指定之嘗試次數可為大於或小於十次。可選擇經指定之嘗試次數使得在統計上在經指定之嘗試次數中不可能挑選(即，猜測)正確金鑰。

【0053】除了解除鎖定API之外，可能具有更多API（諸如一change_keys API及一旋轉金鑰API)。該改變金鑰API提供更換經加密、包覆並儲存於NOR快閃記憶體中之存取金鑰。改變存取金鑰包含擦除操

作。為更換經加密、包覆並儲存於NOR快閃記憶體中之存取金鑰，在434根據經加密、包覆並儲存於NOR快閃記憶體中之EK (其係舊EK)檢查藉由主機輸入之一EK。該EK維持與AK完全相同之安全層級。若檢查指示藉由主機供應以用於當前改變金鑰操作之EK並不有效，則可記錄一錯誤(諸如「Key Not Valid」)。

【0054】 rotate_keys API提供將一當前存取金鑰旋轉至一新存取金鑰。為旋轉出經加密、包覆並儲存於NOR快閃記憶體中之存取金鑰，可在436根據經加密、包覆並儲存於NOR快閃記憶體中之AK (其係舊AK)檢查藉由主機輸入之一AK。若檢查指示藉由主機供應以用於當前旋轉金鑰操作之AK並不有效，則可記錄一錯誤(諸如「Key Not Valid」)。例如，週期性地(諸如一月一次)，主機可出於安全原因旋轉出以獲取一新存取金鑰以提供另一安全層級。在另一實例中，若一給定NVRDIMM-N移動至一不同機器，則主機可改變存取金鑰。主機具有旋轉或改變存取金鑰之控制，但在此控制中，該給定NVRDIMM-N中之資料係受到藉由儲存於NVRDIMM-N之NOR快閃記憶體中之經加密、包覆之金鑰檢查存取金鑰之程序保護。

【0055】 在任何時間，可將NVRDIMM-N裝置置於不安全狀態446中。再一次，自secure_locked狀態448至不安全狀態446之轉變受到保護。在未傳遞在432檢查之一EK之情況下，裝置不會自secure_locked狀態448轉變至不安全狀態446。若檢查指示藉由主機供應以用於當前轉變操作之EK並不有效，則可記錄一錯誤(諸如「Key Not Valid」)。關於其他轉變，可實施一計時器及數次檢查使得若經接收EK之檢查在一特定時間或特定次數檢查內並不匹配來自NOR快閃記憶體之經解包金鑰，則嘗

試存取資料之機器或設備將被鎖定在外。因此一駭客應用程式或裝置無法試圖取消部件安全性。若資料經取消安全性，則再次存取該資料之能力將失去，因為一旦資料經取消安全性，資料就被加密擦除。加密擦除意謂你丟棄金鑰，因此加密擦除係不安全操作。在不安全狀態446中，裝置可經重新初始化、執行維護及執行其他命令。重新初始化可包含所產生之初始化金鑰(init_keys)將裝置置於secure_unlocked狀態444中。

【0056】 圖5繪示根據各項實施例之實例性裝置狀態功能應用程式介面。展示可相對於一裝置可能具有之狀態執行之許多功能。相對於所論述之四種狀態以表格形式展示實例性數目個功能。又針對各功能展示下一狀態(裝置針對各給定功能自四種狀態之各者轉變至該下一狀態)。例如，作為init_keys列出之一給定功能處理初始化金鑰。如所展示，此功能可在無主狀態中及在不安全狀態中執行。在兩種情況下，可在下一狀態為一secure_unlocked狀態之情況下執行此等功能。如所展示，功能change_keys、unsecure、unlock、rotate_access_keys及其他功能並不在無主狀態中執行。

【0057】 圖6係根據各項實施例之一金鑰產生/恢復單元之一方塊圖。一金鑰產生/恢復單元600具有用於加密之硬體區塊，該等硬體區塊可經實施以支援執行裝置狀態之間的轉變之API之動作，如本文中所論述。此等硬體區塊可配置於NVDIMM層級處。硬體區塊可包含類似於圖3A及圖3B中所展示之組件配置之一DRBG區塊603、一加密區塊607及包覆/解包區塊610。DRBG區塊603可藉由一DRBG 303實現且加密區塊607可基於經實施之加密(諸如圖3A及圖3B之PBKDF 307之一形式)。包覆/解包區塊610可實現為兩個單元(諸如金鑰包覆件310及金鑰解包件320)或實現為

金鑰包覆件310與金鑰解包件320之一組合之一單個單元。此等區塊可整合為一裝置(諸如圖2之NVRDIMM-N 200或其他NVDIMM)中之單元。

【0058】 DRBG區塊603可由一雜訊產生器651及一金鑰散列訊息認證碼(HMAC) DRBG (HMAC_DRBG) 652構造。雜訊產生器651可為一環形振蕩器。例如，雜訊產生器651可為一非計時伽羅華(Galois)環。一伽羅華環係一環形振蕩器之一般化且由以級聯方式與數個XOR邏輯閘連接在一起以形成一回饋之數個反相器組成。伽羅華環可經容許以自由運行。用於應用伽羅華環之一積體電路設計之製造參數之程序、電壓及溫度(PVT)變動效應可影響伽羅華環之輸出。

【0059】 HMAC係涉及一密碼編譯散列函數及一秘密密碼編譯金鑰之一特定類型之訊息認證碼(有時被稱為一標籤)。其可用於同時確認資料完整性及一訊息之認證兩者。HMAC_DRBG 652可使用一HMAC-SHA-256引擎遵循(例如) NIST SP 800-90a建置。SHA (安全散列演算法)係許多密碼編譯散列函數之一者。例如，一SHA-256產生一固定大小256位元(32位元組)散列，其中一散列係單向函數，因為其無法被返回解密。雜訊產生器651之輸出可具有256個位元至HMAC_DRBG 652之一熵輸入。熵輸入係對一DRBG機制提供一經評估之最低量不可預測性之一輸入位元字串。雜訊產生器651之輸出可包含具有256個位元之一隨機數(nonce)。一隨機數係包含於藉由一協定通常出於保證實時資料而非重播資料之傳輸之目的而交換以偵測及保護免受重播攻擊之資料中之隨機或不重複值。

【0060】 至HMAC_DRBG 652之選用輸入可包含一個人化字串。該個人化字串可為(但不限於) 256位元且可用於HMAC_DRBG 652之初始種子植產生。至HMAC_DRBG 652之額外選用輸入可包含藉由

HMAC_DRBG 652用於重新點火(re-seed)及產生操作之數個位元。額外位元可為(但不限於) 256位元。

【0061】 HMAC_DRBG 652之輸出係一隨機值。使用HMAC-SHA-256引擎連同與雜訊產生器651相關聯之256個位元參數、個人化字串及來自主機之額外輸入，該隨機值具有256個位元。HMAC_DRBG 652之輸出係作為一MEK提供至一MEK暫存器605 (諸如圖3A之MEK暫存器305)及作為一鹽值提供至加密區塊607或至將該鹽值自DRBG 603傳送至加密區塊607之一緩衝器或暫存器。HMAC_DRBG 652之輸出亦可作為擦除金鑰(其可被稱為一RND)提供。類似於圖3A之MEK，RND可提供至一RND暫存器656，隨後自RND暫存器656包覆RND。MEK暫存器605及RND暫存器656可包含來自對未成功傳遞一金鑰之嘗試次數計數之一計數器之啟用輸入。小於或等於一最大嘗試次數之計數可用於控制來自MEK暫存器605或來自RND暫存器656之輸出。

【0062】 加密區塊607可配置為一密碼加密區塊(諸如圖3A之PBKDF 307)。加密區塊607可包含遵循NIST SP 800-232之一PBKDF2。加密區塊607可包含子區塊，諸如遵循NIST SP 800-232之一HMAC及遵循NIST FIPS 280-4之一SHA-256。至加密區塊607之輸入可包含來自主機之可具有256位元之一密碼輸入。該密碼係來自主機之藉由裝置(諸如圖2之NVRDIMM-N 200)上之韌體載入至加密區塊607中之一金鑰，其中該韌體獲取來自裝置之I^2C之金鑰。

【0063】 至加密區塊607之輸入亦可包含一鹽值，該鹽值係在裝置之韌體之控制下自主機輸入或作為自DRBG區塊603擷取之一隨機值輸入。鹽值可為128個位元。加密區塊607可相對於一迭代操作，該迭代可

為在裝置之韌體之控制下來自一主機之輸入或為儲存或永久設定於裝置內之一預設值。迭代計數可包含32個位元。迭代計數可大於或小於32個位元。

【0064】 來自加密區塊607之輸出包含一經導出金鑰。該經導出金鑰可為一256位元金鑰。經導出金鑰之位元係作為經加密金鑰輸入至內部暫存器658 (其可被稱為KEK暫存器658)。來自此等內部暫存器658之輸出係提供至包覆/解包區塊610。

【0065】 包覆/解包區塊610可使用遵循NIST SP 800-38F之一AES-256金鑰包覆/解包程序。對於一金鑰包覆模式，輸入可包含自加密區塊607產生之在內部暫存器中擷取之經導出金鑰，如上文所提及。來自此等內部暫存器之輸入係可具有256個位元之被稱為金鑰加密金鑰(KEK)之一散列金鑰。一KEK係一加密金鑰，其之功能係用於加密及解密一加密金鑰，該加密金鑰之功能係加密及解密資料，該加密金鑰係所產生之MEK。在此配置中，KEK係圖3A之MKEK。又至包覆/解包區塊610之輸入係可具有256個位元之一純文字輸入。此輸入係來自MEK暫存器605之MEK或來自RND暫存器656之RND。

【0066】 在金鑰包覆模式中，包覆/解包區塊610之輸出可為一密文輸出。該密文輸出可包含(但不限於) 320個位元。包覆/解包區塊610之輸出可作為一EMEK耦合至一EMEK暫存器659。裝置之韌體可經結構化以讀取該EMEK並將其儲存至一非揮發性記憶體。例如，EMEK可經由韌體之一保存操作經由一SPI儲存至一NOR快閃記憶體。韌體可經由一解包程序之一恢復操作經由該SPI讀取該NOR快閃記憶體並將EMEK寫入至EMEK暫存器659。

【0067】在金鑰解包模式中，至包覆/解包區塊610之輸入包含MKEK（其係來自從加密區塊607擷取輸出之內部暫存器658之散列金鑰）。至包覆/解包區塊610之輸入包含來自保存經加密之MEK或RND之EMEK暫存器659之一密文輸入。該密文輸入可包含(但不限於) 320個位元。在金鑰解包模式中，包覆/解包區塊610之輸出可為一純文字輸出。密文輸出可包含(但不限於) 256個位元。此輸出可提供至MEK暫存器605或RND暫存器656。

【0068】金鑰產生/恢復單元600係在控制資料之儲存及安全性之裝置內部組態。例如，金鑰產生/恢復單元600可在一NVDIMM (諸如但不限於圖2之NVRDIMM-N 100)內部組態。金鑰產生/恢復單元600之組件可經配置使得其等不可供I^2C或JTAG介面存取至各自NVDIMM。JTAG係指為電子裝置之標準測試存取埠及邊界掃描架構提供建議之聯合測試行動小組。藉由相對於各自NVDIMM之組件結構化之韌體處理對自一主機輸入之信號及參數之控制以提供對各自NVDIMM之狀態之控制之隔離以保護NVDIMM之資料。

【0069】金鑰產生/恢復單元600提供用於韌體進行金鑰處理之金鑰以相對於一NVDIMM執行不同API呼叫以保護該NVDIMM中保護之資料。一主機可經由一I^2C將許多API命令傳遞至一裝置(諸如一NVDIMM)。此等API命令可包含起始金鑰、改變金鑰、取消裝置安全性、解除鎖定裝置、鎖定裝置、旋轉一存取金鑰、測試一存取金鑰、測試一擦除金鑰之命令。相對於藉由裝置保護之資料提出解除鎖定、鎖定及取消安全性之請求。取決於控制資料之儲存及安全性之裝置，可包含其他API命令。此等係韌體將暫存及提供執行之API命令。韌體將與金鑰產生/

恢復單元600圖之硬體區塊介接以在相對於藉由資料儲存及保護之資料之安全性轉變裝置之狀態時保護使用者資料。裝置(諸如一NVDIMM)內部之韌體控制裝置之狀態之間的轉變及金鑰之路由以保護裝置之資料。

【0070】 在一NVDIMM (諸如圖2之NVRDIMM-N 200)中，在非揮發性控制器(NVC)內部之處理器運行以執行各種API之功能時，設定一忙碌位元。若執行在任何方面皆不成功，則可記錄一錯誤。不同錯誤之實例可包含重試存取金鑰計數錯誤、重試擦除金鑰計數錯誤、裝置狀態錯誤、未發送舊擦除金鑰、未發送舊存取金鑰、未發送擦除金鑰、未發送存取金鑰及無效金鑰。例如，假定一使用者主機由於裝置在一安全鎖定狀態中而嘗試將裝置解除鎖定且傳入一存取金鑰以執行解除鎖定。所提供之該存取金鑰將經受加密區塊607之PDKF2且其將在包覆/解包區塊610中藉由來自NOR快閃之經加密金鑰進行解包。若此失敗，則設定陳述無效金鑰之錯誤。在主機意外將一無效金鑰傳遞至裝置中之情況下，裝置提供錯誤資訊至主機，此容許主機再次嘗試。若一駭客裝置試圖傳遞一猜測存取金鑰，則在未驗證該猜測存取金鑰時亦設定此無效金鑰錯誤。導致產生一錯誤程式碼之其他動作可包含諸如未針對嘗試命令或裝置在錯誤狀態中而將一存取金鑰發送至裝置之動作。特定API可僅藉由處於一正確狀態中之裝置執行。若執行一API之嘗試次數超過重試命令之一設定次數(例如，但不限於超過十次重試)，則記錄一錯誤。該錯誤可記錄為一重試存取金鑰計數錯誤或一重試擦除金鑰計數錯誤。

【0071】 在一裝置(諸如一NVDIMM)中執行API呼叫時，韌體可經配置以接收一API命令。與韌體相關聯之該NVDIMM中之硬體設定一忙碌位元以指示API執行正在進行中。韌體可清除任何舊狀態、執行API、設

定裝置之適當狀態並記錄錯誤，以及在執行完成時清除忙碌位元。以下係上文提及之可藉由傳遞加密金鑰而實施之實例性API功能。

【0072】 對於初始化金鑰(init_keys) API命令之執行，所使用之金鑰包含存取金鑰及擦除金鑰。首先，裝置之狀態必須在不安全狀態或無主狀態中。若裝置之狀態係secure_unlocked狀態或secure_locked狀態，則設定裝置狀態錯誤且退出程序。在檢查裝置之狀態之此程序中，處於不安全狀態中之裝置保持不安全直至稍後處理。第二，進行一檢查以判定主機已發送一存取金鑰及一擦除金鑰。若未自主機供應金鑰或供應金鑰之一者，則設定未發送存取金鑰及/或未發送擦除金鑰且退出程序。第三，在連續程序中，使用裝置之DRBG硬體區塊產生一MEK。第四，使用存取金鑰產生一EMEK且經由一SPI將該EMEK儲存於裝置中之非揮發性記憶體(諸如一NOR快閃記憶體)中。第五，使用RND產生一WEK (其係一經包覆擦除金鑰)且經由SPI將該WEK儲存至裝置中之非揮發性記憶體。第六，將裝置狀態設定至secure_unlocked。

【0073】 對於change_keys API命令之執行，所使用之金鑰包含一存取金鑰、一擦除金鑰及一舊擦除金鑰。首先，裝置狀態必須在secure_unlocked狀態或secure_locked狀態中。若裝置狀態係secure_unlocked，則呼叫鎖定API。若裝置狀態係不安全，則設定裝置狀態錯誤狀態且退出。若裝置狀態係不安全，則裝置狀態保持不安全。第二，檢查主機已發送一存取金鑰、擦除金鑰及舊擦除金鑰。若未供應任何金鑰，則設定未發送x金鑰錯誤(其中x金鑰係存取金鑰、擦除金鑰及舊擦除金鑰之一或多者)且退出。第三，經由裝置上之SPI自裝置之非揮發性記憶體(諸如一NOR快閃記憶體)讀取WEK (經包覆擦除金鑰)。第四，使用

一舊擦除金鑰解包WEK。第五，檢查解包有效。若解包失敗則設定無效金鑰錯誤且退出。遞增重試EK計數。裝置狀態保持於secure_locked狀態中。第六，使用裝置之DRBG硬體區塊產生一MEK。第七，使用存取金鑰包覆該MEK以形成EMEK。經由SPI將EMEK儲存至裝置之非揮發性記憶體(諸如一NOR快閃記憶體)。第八，使用RND將擦除金鑰包覆至一WEK且經由SPI將該WEK儲存至裝置之非揮發性記憶體(諸如一NOR快閃記憶體)。第九，將裝置狀態設定至secure_unlocked。

【0074】 對於rotate_keys API命令之執行，所使用之金鑰可包含一存取金鑰及一舊存取金鑰。首先，裝置狀態必須在secure_unlocked狀態或secure_locked狀態中。若裝置狀態係在不安全狀態中，則設定裝置狀態錯誤且退出。第二，檢查主機已發送一存取金鑰及一舊存取金鑰。若未供應任何金鑰，則設定未發送x金鑰(其中x金鑰係存取金鑰及舊存取金鑰之一或多者)且退出。第三，經由一SPI自裝置中之非揮發性記憶體(諸如一NOR快閃記憶體)讀取EMEK。第四，使用舊存取金鑰解包EMEK。第五，檢查解包有效。若解包失敗則設定無效金鑰錯誤且退出。遞增重試AK計數。第六，使用存取金鑰包覆MEK以形成EMEK，且經由SPI將EMEK儲存至裝置之非揮發性記憶體(諸如一NOR快閃記憶體)。第七，將裝置狀態設定至secure_unlocked狀態。

【0075】 對於不安全API命令之執行，所使用之金鑰包含一擦除金鑰。首先，裝置狀態必須在secure_unlocked狀態中或在secure_locked狀態中。若裝置狀態係在不安全狀態中，則此係一無操作(NOP)狀態且退出。第二，檢查主機已發送一擦除金鑰。若未供應任何擦除金鑰，則設定未發送擦除金鑰錯誤且退出。第三，經由SPI自裝置之非揮發性記憶體(諸

如一NOR快閃記憶體)讀取WEK (經包覆擦除金鑰)。第四，使用主機提供之擦除金鑰解包WEK。第五，檢查解包有效。若解包失敗則設定無效金鑰錯誤且退出。遞增重試EK計數。裝置狀態保持於secure_locked狀態中或secure_unlocked狀態中。第六，刪除MEK及EMEK且經由SPI將EMEK及WEK在裝置之非揮發性記憶體(諸如一NOR快閃記憶體)中歸零。第七，將裝置狀態設定至不安全。

【0076】 對於解除鎖定API命令之執行，所使用之金鑰包含一存取金鑰。首先，裝置狀態必須在secure_locked狀態中。若裝置狀態係不安全狀態或secure_unlocked狀態，則此係一NOP且退出。第二，檢查主機已發送一存取金鑰。若未供應任何存取金鑰，則設定未發送存取金鑰錯誤且退出。第三，經由SPI自裝置之非揮發性記憶體(諸如一NOR快閃記憶體)讀取EMEK。第四，使用存取金鑰解包EMEK，其中目的地係MEK暫存器。第五，檢查解包有效。若解包失敗則設定無效金鑰錯誤且退出。遞增重試AK計數。裝置狀態保持於secure_locked狀態中。第六，將裝置狀態設定至secure_unlocked狀態。

【0077】 對於鎖定API命令之執行，不需要金鑰。首先，裝置狀態必須在secure_unlocked狀態中。若裝置狀態係在不安全狀態中，則設定裝置狀態錯誤且退出。若裝置狀態係secure_locked狀態，則此係一NOP且退出。第二，藉由裝置之非揮發性記憶體(諸如一NOR快閃記憶體)中之有效EMEK刪除MEK及揮發性EMEK。第三，將裝置狀態設定至secure_locked狀態。

【0078】 對於test_AK API命令之執行，所使用之金鑰包含一存取金鑰。首先，檢查主機已發送一存取金鑰。若未供應任何存取金鑰，則設

定未發送存取金鑰錯誤且退出。第二，自裝置之非揮發性記憶體(諸如一NOR快閃記憶體)讀取EMEK。第三，使用存取金鑰解包EMEK。第四，檢查解包有效。若解包失敗，則遞增重試AK計數。若解包失敗則設定無效金鑰錯誤且退出。若解包通過，則清除重試AK計數。

【0079】 對於test_EK API命令之執行，所使用之金鑰包含一擦除金鑰。首先，檢查主機已發送一擦除金鑰。若未供應任何擦除金鑰，則設定未發送擦除金鑰錯誤且退出。第二，自裝置之非揮發性記憶體(諸如一NOR快閃記憶體)讀取WEK。第三，使用擦除金鑰解包WEK。第四，檢查解包有效。若解包失敗，則遞增重試EK計數。若解包失敗則設定無效金鑰錯誤且退出。若解包通過，則清除重試EK計數。

【0080】 對於工廠預設API命令之執行，由於狀態將改變回至無主，所以擦除金鑰係用於確認。首先，檢查裝置狀態。若裝置狀態係無主狀態，則繼續工廠預設操作。或者若裝置狀態並不在secure_unlocked狀態中，則設定裝置狀態錯誤。第二，檢查主機已發送一擦除金鑰。第三，自裝置之非揮發性記憶體(諸如一NOR快閃記憶體)讀取WEK。第四，使用擦除金鑰解包EMEK。第五，檢查解包有效。第六，清除MEK/EMEK。第七，繼續一位元組可定址能量支持介面(BAEBI)定義之工廠預設操作。

【0081】 對於重設/初始化/監視API命令之執行，首先，在通電時，一重設(諸如一NVC重設)將執行。第二，除了其他初始任務之外，亦將檢查先前裝置狀態。若先前裝置狀態不安全，則將裝置狀態設定至不安全狀態。MEK將為用於不安全模式使用者之預設金鑰。第三，若永久裝置狀態係secure_unlocked狀態或secure_locked狀態，則將裝置狀態設定至

secure_locked狀態。可設定事件引腳以觸發主機傳遞一存取金鑰以進入secure_unlocked狀態。

【0082】 關於認證失敗之重試計數，對於各金鑰維持一各自認證重試計數。此重試計數可由使用者調整。重試計數對於各金鑰可具有十次之一預設。每當認證成功時，就將一認證重試計數重設至0。一特定失敗等級係良好的。失敗計數不會持續存在。歸因於達到之最大重試計數，裝置將不會改變操作模式，除了停用進一步嘗試。在達到最大重試計數時做出之決策可取決於系統應用於之應用程式。可向主機提供重試超出錯誤。

【0083】 圖7係根據各項實施例之處理加密金鑰之一實例性方法700之一流程圖。方法700可藉由可包含硬體(例如，處理裝置、電路、專用邏輯、可程式化邏輯、微碼、一裝置之硬體、積體電路等)、軟體(例如，在一處理裝置上運行或執行之指令)或其等之一組合之處理邏輯來執行。在一些實施例中，方法700係藉由圖1之金鑰加密處理組件113執行。儘管以一特定序列或順序展示，然除非另有指定，否則可修改程序之順序。因此，所繪示之實施例應僅理解為實例，且所繪示之程序可以一不同順序執行，且一些程序可並行執行。此外，一或多個程序可在各項實施例中省略。因此，每項實施例中並非需要所有程序。其他程序流程係可行的。

【0084】 方法700可在NVRDIMM-N 200上部署。將瞭解，方法700可在其他硬體組態上部署。同樣地，NVRDIMM-N 200可用於部署處理加密金鑰之其他方法。在方塊710，一處理裝置(諸如與圖2之NVRDIMM 200之金鑰產生及恢復單元202相關聯)產生一媒體加密金鑰以對一設備之數個記憶體組件中之資料加密。在方塊720，處理裝置包覆該媒體加密金鑰以產生一經加密媒體加密金鑰。在方塊730，處理裝置將該經加密媒體

加密金鑰儲存於該設備之一非揮發性記憶體(諸如圖2之NVRDIMM 200之NOR快閃記憶體206)中。在方塊740，處理裝置使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變。該設備可為一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0085】 方法700或類似於方法700之方法之變動可包含可取決於此等方法之應用及/或其中實施此等方法之系統之架構而組合之許多不同實施例。此等方法可包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。方法700或類似方法可包含：接收用於自secure_locked狀態轉變之一操作之一存取金鑰或一擦除金鑰；及使用用於該操作之該存取金鑰或該擦除金鑰基於相對於用於該操作之各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作來執行該操作。

【0086】 圖8係根據各項實施例之處理加密金鑰之一實例性方法800之一流程圖。方法800可藉由可包含硬體(例如，處理裝置、電路、專用邏輯、可程式化邏輯、微碼、一裝置之硬體、積體電路等)、軟體(例如，在一處理裝置上運行或執行之指令)或其等之一組合之處理邏輯來執行。在一些實施例中，方法700係藉由圖1之金鑰加密處理組件113執行。儘管以一特定序列或順序展示，然除非另有指定，否則可修改程序之順序。因此，所繪示之實施例應僅理解為實例，且所繪示之程序可以一不同順序執行，且一些程序可並行執行。此外，一或多個程序可在各項實施例中省略。因此，每項實施例中並非需要所有程序。其他程序流程係可行的。

【0087】 方法800可在NVRDIMM-N 200上部署。將瞭解，方法800

可在其他硬體組態上部署。同樣地，NVRDIMM-N 200可用於部署用於處理加密金鑰之其他方法。在方塊810，記憶體子系統之一處理裝置(諸如與圖2之NVRDIMM 200之金鑰產生及恢復單元202相關聯)產生一媒體加密金鑰，該媒體加密金鑰經組態以對一非揮發性雙直列記憶體模組之數個揮發性記憶體組件中之資料加密，其中該非揮發性雙直列記憶體模組具有一非揮發性控制器。在方塊820，記憶體子系統(諸如圖2之NVRDIMM-N 200)接收源自於一主機裝置之一存取金鑰。在方塊830，處理裝置使用存取金鑰產生一媒體金鑰加密金鑰。在方塊840，處理裝置包覆該媒體加密金鑰與該媒體金鑰加密金鑰之組合，以形成一經加密媒體加密金鑰。在方塊850，處理裝置將該經加密媒體加密金鑰儲存於非揮發性雙直列記憶體模組之一非揮發性記憶體(諸如圖2之NVRDIMM 200之NOR快閃記憶體206)中。在方塊860，處理器使用該經加密媒體加密金鑰將非揮發性控制器自一安全狀態轉變。非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0088】 方法800或類似於方法800之方法之變動可包含可取決於此等方法之應用及/或其中實施此等方法之系統之架構而組合之許多不同實施例。此等方法可包含：自一主機裝置接收一存取金鑰；使用該存取金鑰解除鎖定非揮發性控制器或旋轉至另一存取金鑰；及基於相對於經接收之存取金鑰對經加密媒體加密金鑰之一成功解包來執行非揮發性控制器之該解除鎖定或至另一存取金鑰之該旋轉。

【0089】 方法800或類似方法可包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性

記憶體。方法800或類似方法可包含：自一主機裝置接收一擦除金鑰；使用該擦除金鑰取消非揮發性控制器之安全性或改變非揮發性記憶體中之一金鑰；及基於相對於經接收之擦除金鑰對經包覆擦除金鑰之一成功解包來執行非揮發性控制器之該取消安全性或該金鑰之該改變。

【0090】 方法700及800以及類似於方法700及800之方法可包含與圖1至圖6之任一者相關聯之特徵。方法700及800以及類似於方法700及800之方法亦可包含與如本文中教示之加密金鑰處理技術相關聯之特徵。

【0091】 韌體可包括在藉由一控制器執行時可引起執行包括以下操作之指令(諸如一微碼)：產生一媒體加密金鑰以對一設備之數個記憶體組件中之資料加密；包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；將該經加密媒體加密金鑰儲存於該設備之一非揮發性記憶體中；及使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變。該設備可為一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0092】 韌體之指令在藉由一控制器執行時可引起執行操作，該等操作可包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。該等指令可包含執行包含以下操作之指令：接收用於自secure_locked狀態轉變之一操作之一存取金鑰或一擦除金鑰；及使用用於該操作之該存取金鑰或該擦除金鑰基於相對於用於該操作之各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作來執行該操作。

【0093】 韌體可包括在藉由一控制器執行時可引起執行包括以下操作之指令(諸如一微碼)：產生一媒體加密金鑰，該媒體加密金鑰用以對一

非揮發性雙直列記憶體模組之數個揮發性記憶體組件中之資料加密，該非揮發性雙直列記憶體模組具有一非揮發性控制器；接收源自於一主機裝置之一存取金鑰；使用該存取金鑰產生一媒體金鑰加密金鑰；包覆該媒體加密金鑰與該媒體金鑰加密金鑰之組合，以形成一經加密媒體加密金鑰；將該經加密媒體加密金鑰儲存於非揮發性雙直列記憶體模組之一非揮發性記憶體中；及使用該經加密媒體加密金鑰自非揮發性控制器之一安全狀態轉變。非揮發性控制器可作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0094】 韌體之指令在藉由一控制器執行時可引起執行操作，該等操作可包含：自一主機裝置接收一存取金鑰；使用該存取金鑰解除鎖定非揮發性控制器或旋轉至另一存取金鑰；及基於相對於經接收之存取金鑰對經加密媒體加密金鑰之一成功解包來執行非揮發性控制器之該解除鎖定或至另一存取金鑰之該旋轉。韌體之指令在藉由一控制器執行時可引起執行操作，該等操作可包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。該等操作可包含：自一主機裝置接收一擦除金鑰；使用該擦除金鑰取消非揮發性控制器之安全性或改變非揮發性記憶體中之一金鑰；及基於相對於經接收之擦除金鑰對經包覆擦除金鑰之一成功解包來執行非揮發性控制器之該取消安全性或該金鑰之該改變。

【0095】 韌體可包括在藉由一控制器執行時可引起執行包括以下操作之指令(諸如一微碼)：與一裝置中之加密金鑰處理相關聯之操作；及與圖1至圖8所相關聯之裝置相關聯之操作。韌體之指令在藉由一控制器執行時可引起執行操作，該等操作可包含如本文中教示之操作。

【0096】 在各項實施例中，一種設備包括：數個記憶體組件；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令。該設備可為一四狀態設備，其中該四種狀態係一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0097】 韌體可具有執行以下一操作之指令：使用自一主機裝置接收之一存取金鑰自secure_locked狀態轉變至secure_unlocked狀態，包含相對於該經接收之存取金鑰對經加密媒體加密金鑰之一成功解包操作。加密金鑰產生器可經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。韌體可具有執行以下一操作之指令：使用自一主機裝置接收之一擦除金鑰自secure_locked狀態轉變至secure_unlocked狀態，包含相對於該經接收之擦除金鑰對經包覆擦除金鑰之一成功解包操作。設備可包含如本文中教示之各種特徵或特徵組合。

【0098】 設備之加密金鑰產生器可包含：一確定性隨機數產生器，其用以產生作為媒體加密金鑰之一隨機數；一加密區塊，其用以接收該隨機數及藉由一主機裝置產生之一存取金鑰及藉由使用一第一加密演算法產生一媒體金鑰加密金鑰；及一包覆區塊，其用以接收該媒體金鑰加密金鑰及該媒體加密金鑰及藉由使用一第二加密演算法產生經加密媒體加密金鑰。

【0099】在各項實施例中，一種非揮發性雙直列記憶體模組可包括：數個揮發性記憶體組件；一第一非揮發性記憶體，在偵測一電力故障之後即在其中轉儲該等揮發性記憶體組件之內容；一非揮發性控制器，其用以控制該數個揮發性記憶體組件及該非揮發性記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一第二非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。該非揮發性控制器可作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。非揮發性雙直列記憶體模組可包含如本文中教示之各種特徵或特徵組合。

【0100】加密金鑰產生器可經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至第二非揮發性記憶體。韌體可具有執行以下一操作之指令：使用自一主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作自secure_locked狀態轉變。

【0101】非揮發性雙直列記憶體模組之韌體可具有執行以下操作之指令：移動金鑰及呼叫一加密演算法以產生用於包覆或解包之一媒體金鑰加密金鑰；控制對第二非揮發性記憶體之存取；執行應用程式介面呼叫，包含設置用於各自應用程式介面呼叫之硬體之資料路徑；檢查、追蹤及更新非揮發性控制器之狀態；及維持關於錯誤處理之一紀錄狀態。

【0102】 在各項實施例中，一種系統包括：一主機裝置；及一非揮發性雙直列記憶體模組，其可操作地耦合至該主機裝置。該非揮發性雙直列記憶體模組可包含：動態隨機存取記憶體組件；一NAND快閃記憶體，在偵測一電力故障之後即在其中轉儲該等動態隨機存取記憶體組件之內容；一非揮發性控制器，其用以控制該等動態隨機存取記憶體組件及該NAND快閃記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該等動態隨機存取記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一NOR快閃記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。該非揮發性控制器可作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。該系統可包含如本文中教示之各種特徵或特徵組合。

【0103】 加密金鑰產生器可經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至第二非揮發性記憶體。韌體可具有執行以下一操作之指令：使用自一主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作自secure_locked狀態轉變。

【0104】 主機裝置可提供用於產生經加密媒體加密金鑰之一存取金鑰。韌體可具有處理加密金鑰之產生及恢復之指令使得加密金鑰之產生及恢復與藉由主機裝置之直接存取隔離。

【0105】 圖9繪示一電腦系統900之一實例性機器，在該機器內可執

行用於引起該機器執行本文中所論述之方法論之任一或多者之一指令集。在一些實施例中，電腦系統900可對應於一主機系統(例如，圖1之主機系統120)，該主機系統包含、耦合至或利用一記憶體子系統(例如，圖1之記憶體子系統110)或可用於執行一控制器之操作(例如，執行一作業系統以執行對應於圖1之金鑰加密處理組件113之操作)。在替代實施例中，機器可連接(例如，網路連接)至一LAN、一內部網路、一商際網路及/或網際網路中之其他機器。該機器可在客戶端-伺服器網路環境中作為一伺服器機器或一客戶端機器而操作，在一同級間(或分散式)網路環境中作為一同級機器操作，或在一雲端運算基礎設施或環境中作為一伺服器機器或一客戶端機器操作。

【0106】 機器可為一個人電腦(PC)、一平板電腦PC、一機上盒(STB)、一個人數位助理(PDA)、一蜂巢式電話、一網路設備、一伺服器、一網路路由器、一交換器或橋接器，或能夠執行指定藉由該機器採取之行動之一指令集(循序或以其他方式)之任何機器。此外，雖然僅繪示一單個機器，但術語「機器」亦應被視為包含個別或聯合執行之一(或多個)指令集以執行本文中所論述之方法論之任一或多者之機器之任何集合。

【0107】 實例性電腦系統900包含一處理裝置902、一主記憶體904(例如，唯讀記憶體(ROM)、快閃記憶體、動態隨機存取記憶體(DRAM)，諸如同步DRAM (SDRAM)或Rambus DRAM (RDRAM)等)、一靜態記憶體906 (例如，快閃記憶體、靜態隨機存取記憶體(SRAM)等)及一資料儲存系統918，其等經由一匯流排930彼此通信。

【0108】 處理裝置902表示一或多個通用處理裝置，諸如一微處理器、一中央處理單元或類似者。更特定言之，處理裝置可為一複雜指令集

運算(CISC)微處理器、精簡指令集運算(RISC)微處理器、極長指令字(VLIW)微處理器，或實施其他指令集之一處理器，或實施指令集之一組合之處理器。處理裝置902亦可為一或多個專用處理裝置，諸如一特定應用積體電路(ASIC)、一場可程式化閘陣列(FPGA)、一數位信號處理器(DSP)、網路處理器或類似者。處理裝置902經組態以執行用於執行本文中所論述之操作及步驟之指令926。電腦系統900可進一步包含經由網路920通信之一網路介面裝置908。

【0109】 資料儲存系統918可包含其上儲存體現本文中所描述之方法論或功能之任一或多者之一或多個指令926集或軟體之一機器可讀儲存媒體924 (亦被稱為一電腦可讀媒體)。指令926亦可完全或至少部分駐留於主記憶體904內及/或在該等指令由電腦系統900執行期間駐留於處理裝置902內，主記憶體904及處理裝置902亦構成機器可讀儲存媒體。機器可讀儲存媒體924、資料儲存系統918及/或主記憶體904可對應於圖1之記憶體子系統110。

【0110】 在一項實施例中，指令926包含實施對應於一金鑰加密處理組件(例如，圖1之金鑰加密處理組件113)之功能性之指令。雖然機器可讀儲存媒體924在一實例性實施例中展示為一單個媒體，但術語「機器可讀儲存媒體」應被視為包含儲存一或多個指令集之一單個媒體或多個媒體。術語「機器可讀儲存媒體」亦應被視為包含能夠儲存或編碼藉由機器執行且引起機器執行本發明之方法論之任一或多者之一指令集之任何媒體。術語「機器可讀儲存媒體」應相應地視為包含(但不限於)固態記憶體、光學媒體及磁性媒體。

【0111】 前文詳細描述之一些部分已在對一電腦記憶體內之資料位

元之操作之演算法及符號表示方面呈現。此等演算法描述及表示係熟習資料處理技術者用於更有效地向其他熟習此項技術者傳達其等工作之實質之方式。一演算法在此處且通常被設想為導致一所要結果之一自相一致序列操作。該等操作係需要實體操縱物理量之該等操作。通常但並非一定地，此等量採用能夠經儲存、組合、比較及以其他方式操縱之電信號或磁信號之形式。有時，主要出於常用之原因，將此等信號指代為位元、值、元件、符號、字母、術語、數字或類似者已證明為方便的。

【0112】 然而，應牢記，所有此等及類似術語應與適當物理量相關聯且僅為應用於此等量之方便標記。本發明可係指將表示為一電腦系統之暫存器及記憶體內之物理(電子)量之資料轉變成類似地表示為電腦系統記憶體或暫存器或其他此等資訊儲存系統內之物理量之其他資料之該電腦系統或類似電子運算裝置之動作及程序。

【0113】 本發明亦係關於用於執行本文中之操作之一設備。此設備可專門為預期目的而構造，或其可包含藉由儲存於電腦中之一電腦程式選擇性啟動或重新組態之一通用電腦。此一電腦程式可儲存於一電腦可讀儲存媒體中，諸如(但不限於)任何類型之磁碟(包含軟磁碟、光學磁碟、CD-ROM及磁光碟)、唯讀記憶體(ROM)、隨機存取記憶體(RAM)、EPROM、EEPROM、磁卡或光卡，或適於儲存電子指令之任何類型之媒體，上述各者耦合至一電腦系統匯流排。

【0114】 本文中呈現之演算法及顯示並非固有地與任何特定電腦或其他設備有關。各種通用系統可藉由程式根據本文中之教示使用，或構造一更專門設備來執行方法證明為方便的。用於各種此等系統之結構將如下文描述中所闡述。另外，本發明並不參考任何特定程式設計語言描述。將

瞭解，各種程式設計語言可用於實施如本文中所描述之本發明之教示。

【0115】 本發明可提供為可包含其上儲存有指令之一機器可讀媒體之一電腦程式產品或軟體，該等指令可用於程式化一電腦系統(或其他電子裝置)以執行根據本發明之一程序。一機器可讀媒體包含用於儲存呈可藉由一機器(例如，一電腦)讀取之一形式之資訊之任何機構。在一些實施例中，一機器可讀(例如，電腦可讀)媒體包含一機器(例如，一電腦)可讀儲存媒體，諸如一唯讀記憶體(「ROM」)、隨機存取記憶體(「RAM」)、磁碟儲存媒體、光學儲存媒體、快閃記憶體組件等。

【0116】 下文係根據本文中之教示之方法、設備及系統之實例性實施例。

【0117】 一種實例性設備1可包括：複數個記憶體組件；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令。

【0118】 一實例性設備2可包含實例性設備1之元件，其中該設備係一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0119】 一實例性設備3可包含任何前述實例性設備之元件，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之一存取金鑰自secure_locked狀態轉變至secure_unlocked狀態，包含相對於該經接收之存取金鑰對該經加密媒體加密金鑰之一成功解包操作。

【0120】一實例性設備4可包含任何前述實例性設備之元件，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。

【0121】一實例性設備5可包含任何前述實例性設備之元件，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之一擦除金鑰自secure_locked狀態轉變至secure_unlocked狀態以更換一存取金鑰，包含相對於該經接收之擦除金鑰對經包覆擦除金鑰之一成功解包操作。

【0122】一實例性設備6可包含任何前述實例性設備之元件，其中該加密金鑰產生器包含：一確定性隨機數產生器，其用以產生作為媒體加密金鑰之一隨機數；一加密區塊，其用以接收該隨機數及藉由一主機裝置產生之一存取金鑰及藉由使用一第一加密演算法產生一媒體金鑰加密金鑰；及一包覆區塊，其用以接收該媒體金鑰加密金鑰及該媒體加密金鑰及藉由使用一第二加密演算法產生經加密媒體加密金鑰。

【0123】一種實例性非揮發性雙直列記憶體模組1包括：複數個揮發性記憶體組件；一第一非揮發性記憶體，在偵測一電力故障之後即在其中轉儲該等揮發性記憶體組件之內容；一非揮發性控制器，其用以控制該複數個揮發性記憶體組件及該非揮發性記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一第二非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【0124】一實例性非揮發性雙直列記憶體模組2可包含任何前述實

例性設備及實例性非揮發性雙直列記憶體模組1之元件，其中該非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0125】 一實例性非揮發性雙直列記憶體模組3可包含任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至第二非揮發性記憶體。

【0126】 一實例性非揮發性雙直列記憶體模組4可包含任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作自secure_locked狀態轉變。

【0127】 一實例性非揮發性雙直列記憶體模組5可包含任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該韌體具有執行以下操作之指令：移動金鑰及呼叫一加密演算法以產生用於包覆或解包之一媒體金鑰加密金鑰；控制對第二非揮發性記憶體之存取；執行應用程式介面呼叫，包含設置用於各自應用程式介面呼叫之硬體之資料路徑；檢查、追蹤及更新非揮發性控制器之狀態；及維持關於錯誤處理之一紀錄狀態。

【0128】 一種實例性系統1包括：一非揮發性雙直列記憶體模組，其經組態以可操作地耦合至一主機裝置，該非揮發性雙直列記憶體模組包含：動態隨機存取記憶體組件；一NAND快閃記憶體，在偵測一電力故障

之後即在其中轉儲該等動態隨機存取記憶體組件之內容；一非揮發性控制器，其用以控制該等動態隨機存取記憶體組件及該NAND快閃記憶體；一加密金鑰產生器，其用以產生一媒體加密金鑰以對該等動態隨機存取記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；一NOR快閃記憶體，其用以儲存該經加密媒體加密金鑰；及韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【0129】 一實例性系統2可包含實例性系統1之元件及任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0130】 一實例性系統3可包含任何前述實例性系統之元件，及任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至第二非揮發性記憶體。

【0131】 一實例性系統4可包含任何前述實例性系統之元件，及任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作自secure_locked狀態轉變。

【0132】 一實例性系統5可包含任何前述實例性系統之元件，及任

何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該主機裝置提供用於產生經加密媒體加密金鑰之一存取金鑰。

【0133】 一實例性系統6可包含任何前述實例性系統之元件，及任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件，其中該韌體具有處理加密金鑰之產生及恢復之指令使得加密金鑰之產生及恢復與藉由主機裝置之直接存取隔離。

【0134】 一種實例性方法1包括：產生一媒體加密金鑰以對一設備之複數個記憶體組件中之資料加密；包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；將該經加密媒體加密金鑰儲存於該設備之一非揮發性記憶體中；及使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變。

【0135】 一實例性方法2可包含實例性方法1之元件，其中該設備係一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0136】 一實例性方法3可包含任何前述實例性方法之元件，其中該實例性方法包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。

【0137】 一實例性方法4可包含任何前述實例性方法之元件，其中該實例性方法包含：接收用於自secure_locked狀態轉變之一操作之一存取金鑰或一擦除金鑰；及使用用於該操作之該存取金鑰或該擦除金鑰基於相對於用於該操作之各自經接收之存取金鑰或經接收之擦除金鑰對經加密媒體加密金鑰或經包覆擦除金鑰之一成功解包操作來執行該操作。

【0138】 一種實例性方法5包括：產生一媒體加密金鑰，該媒體加

密金鑰用以對一非揮發性雙直列記憶體模組之數個揮發性記憶體組件中之資料加密，該非揮發性雙直列記憶體模組具有一非揮發性控制器；接收源自於一主機裝置之一存取金鑰；使用該存取金鑰產生一媒體金鑰加密金鑰；包覆該媒體加密金鑰與該媒體金鑰加密金鑰之組合，以形成一經加密媒體加密金鑰；將該經加密媒體加密金鑰儲存於非揮發性雙直列記憶體模組之一非揮發性記憶體中；及使用該經加密媒體加密金鑰自非揮發性控制器之一安全狀態轉變。

【0139】 一實例性方法6可包含實例性方法5之元件及任何前述實例性方法之元件，其中該非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【0140】 一實例性方法7可包含任何前述實例性方法之元件，其中該實例性方法包含：自一主機裝置接收一存取金鑰；使用該存取金鑰解除鎖定非揮發性控制器或旋轉至另一存取金鑰；及基於相對於經接收之存取金鑰對經加密媒體加密金鑰之一成功解包來執行非揮發性控制器之該解除鎖定或至另一存取金鑰之該旋轉。

【0141】 一實例性方法8可包含任何前述實例性方法之元件，其中該實例性方法包含：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至非揮發性記憶體。

【0142】 一實例性方法9可包含任何前述實例性方法之元件，其中該實例性方法包含：自一主機裝置接收一擦除金鑰；使用該擦除金鑰取消非揮發性控制器之安全性或改變非揮發性記憶體中之一金鑰；及基於相對於經接收之擦除金鑰對經包覆擦除金鑰之一成功解包來執行非揮發性控制

器之該取消安全性或該金鑰之該改變。

【0143】 一實例性方法10可包含關於任何前述實例性系統之元件、任何前述實例性設備及任何前述實例性非揮發性雙直列記憶體模組之元件之任何前述實例性方法之元件。

【0144】 在前文說明書中，本發明之實施例已參考其之特定實例性實施例進行描述。很顯然，可在不脫離如以下發明申請專利範圍中所闡述之本發明之實施例之更寬廣精神及範疇之情況下對該等實施例進行各種修改。因此，說明書及圖式應被視為具闡釋性意義而非限制性意義。

【符號說明】

【0145】

100	運算環境
110	記憶體子系統
112A至112N	記憶體組件
113	金鑰加密處理組件
115	記憶體系統控制器/控制器
117	處理器
119	本端記憶體
120	主機系統
200	非揮發性具暫存器之雙直列記憶體模組(NVRDIMM)-N/非揮發性具暫存器之雙直列記憶體模組(NVRDIMM)
201	韌體
202	金鑰產生及恢復單元

204	非揮發性控制器(NVC)
206	反或(NOR)快閃記憶體
208	處理器
209	串列周邊介面(SPI)
211	動態隨機存取記憶體(DRAM)控制器
212	電力控制及狀態
213	計時及鎖相迴路(PLL)
214	暫存器/主機介面
216	本端通信介面(LCOM)
217	內部積體電路(I^2C)
218	反及(NAND)快閃控制器
219	資料緩衝器
222-0至222-17	揮發性記憶體組件/動態隨機存取記憶體(DRAM)
223	串列存在偵測(SPD)
224	非揮發性記憶體/反及(NAND)快閃記憶體
226	雙直列記憶體模組(DIMM)電力單元
229	非揮發性暫存時脈驅動器(NVRCD)
230	主機
240	匯流排
303	確定性隨機數產生器(DRBG)
305	媒體加密金鑰(MEK)暫存器
307	基於密碼之金鑰導出函數(PBKDF)
310	金鑰包覆件

320	金鑰解包件
400	裝置狀態應用程式介面(API)狀態圖
430	步驟
431	步驟
432	步驟
433	步驟
434	步驟
436	步驟
442	無主狀態
444	secure_unlocked狀態
446	不安全狀態
448	secure_locked狀態
600	金鑰產生/恢復單元
603	確定性隨機數產生器(DRBG)區塊
605	媒體加密金鑰(MEK)暫存器
607	加密區塊
610	包覆/解包區塊
651	雜訊產生器
652	金鑰散列訊息認證碼(HMAC)確定性隨機數產生器(DRBG) (HMAC_DRBG)
656	RND暫存器
658	內部暫存器/金鑰加密金鑰(KEK)暫存器
659	經加密媒體加密金鑰(EMEK)暫存器

700	方法
710	方塊
720	方塊
730	方塊
740	方塊
800	方法
810	方塊
820	方塊
830	方塊
840	方塊
850	方塊
860	方塊
900	電腦系統
902	處理裝置
904	主記憶體
906	靜態記憶體
908	網路介面裝置
918	資料儲存系統
920	網路
924	機器可讀儲存媒體
926	指令
930	匯流排

【發明摘要】

【中文發明名稱】

金鑰加密處理

【英文發明名稱】

KEY ENCRYPTION HANDLING

【中文】

一種設備包括用以產生一媒體加密金鑰以對數個記憶體組件中之資料加密之一加密金鑰產生器，其中該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰。該經加密媒體加密金鑰係儲存於一非揮發性記憶體中。該設備包括具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令之韌體。

【英文】

An apparatus comprises an encryption key generator to generate a media encryption key to encrypt data in number of memory components, where the encryption key generator is configured to wrap the media encryption key to generate an encrypted media encryption key, The encrypted media encryption key is stored in a non-volatile memory. The apparatus comprises firmware having instructions to transition the apparatus to and from a secure state using the encrypted media encryption key.

【指定代表圖】

圖7

【代表圖之符號簡單說明】

700 方法

710 方塊

720 方塊

730 方塊

740 方塊

【發明申請專利範圍】

【第1項】

一種設備，其包括：

複數個記憶體組件；

一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；

一非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及

韌體，其具有使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全狀態轉變之指令。

【第2項】

如請求項1之設備，其中該設備係一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【第3項】

如請求項2之設備，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之一存取金鑰自該secure_locked狀態轉變至該secure_unlocked狀態，包含相對於該經接收之存取金鑰對該經加密媒體加密金鑰之一成功解包操作。

【第4項】

如請求項2之設備，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至該非揮發性記憶體。

【第5項】

如請求項4之設備，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之一擦除金鑰自該secure_locked狀態轉變至該secure_unlocked狀態以更換一存取金鑰，包含相對於該經接收之擦除金鑰對該經包覆擦除金鑰之一成功解包操作。

【第6項】

如請求項1之設備，其中該加密金鑰產生器包含：

一確定性隨機數產生器，其用以產生作為該媒體加密金鑰之一隨機數；

一加密區塊，其用以接收該隨機數及藉由一主機裝置產生之一存取金鑰及藉由使用一第一加密演算法產生一媒體金鑰加密金鑰；及

一包覆區塊，其用以接收該媒體金鑰加密金鑰及該媒體加密金鑰及藉由使用一第二加密演算法產生該經加密媒體加密金鑰。

【第7項】

一種非揮發性雙直列記憶體模組，其包括：

複數個揮發性記憶體組件；

一第一非揮發性記憶體，在偵測一電力故障之後即在其中轉儲該等揮發性記憶體組件之內容；

一非揮發性控制器，其用以控制該複數個揮發性記憶體組件及該非揮發性記憶體；

一加密金鑰產生器，其用以產生一媒體加密金鑰以對該複數個記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；

一第二非揮發性記憶體，其用以儲存該經加密媒體加密金鑰；及

韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【第8項】

如請求項7之非揮發性雙直列記憶體模組，其中該非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【第9項】

如請求項8之非揮發性雙直列記憶體模組，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至該第二非揮發性記憶體。

【第10項】

如請求項9之非揮發性雙直列記憶體模組，其中該韌體具有執行以下一操作之指令：使用自一主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對該經加密媒體加密金鑰或該經包覆擦除金鑰之一成功解包操作自該secure_locked狀態轉變。

【第11項】

如請求項7之非揮發性雙直列記憶體模組，其中該韌體具有執行以下操作之指令：

移動金鑰及呼叫一加密演算法以產生用於包覆或解包之一媒體金鑰加密金鑰；

控制對該第二非揮發性記憶體之存取；

執行應用程式介面呼叫，包含設置用於該等各自應用程式介面呼叫之硬體之資料路徑；

檢查、追蹤及更新該非揮發性控制器之該狀態；及

維持關於錯誤處理之一紀錄狀態。

【第12項】

一種系統，其包括：

一非揮發性雙直列記憶體模組，其經組態以可操作地耦合至一主機裝置，該非揮發性雙直列記憶體模組包含：

動態隨機存取記憶體組件；

一NAND快閃記憶體，在偵測一電力故障之後即在其中轉儲該等動態隨機存取記憶體組件之內容；

一非揮發性控制器，其用以控制該等動態隨機存取記憶體組件及該NAND快閃記憶體；

一加密金鑰產生器，其用以產生一媒體加密金鑰以對該等動態隨機存取記憶體組件中之資料加密，該加密金鑰產生器經組態以包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；

一NOR快閃記憶體，其用以儲存該經加密媒體加密金鑰；及

韌體，其具有使用該經加密媒體加密金鑰將該非揮發性控制器轉變至一安全狀態及自該安全狀態轉變之指令。

【第13項】

如請求項12之系統，其中該非揮發性控制器係作為一四狀態裝置操作，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【第14項】

如請求項13之系統，其中該加密金鑰產生器經組態以：產生一擦除金鑰；包覆該擦除金鑰以形成一經包覆擦除金鑰；及將該經包覆擦除金鑰發送至該第二非揮發性記憶體。

【第15項】

如請求項14之系統，其中該韌體具有執行以下一操作之指令：使用自該主機裝置接收之用於該操作之一存取金鑰或一擦除金鑰基於相對於用於該操作之該各自經接收之存取金鑰或經接收之擦除金鑰對該經加密媒體加密金鑰或該經包覆擦除金鑰之一成功解包操作自該secure_locked狀態轉變。

【第16項】

如請求項12之系統，其中該主機裝置提供用於該經加密媒體加密金鑰之該產生之一存取金鑰。

【第17項】

如請求項12之系統，其中該韌體具有處理加密金鑰之產生及恢復之指令使得加密金鑰之產生及恢復與藉由該主機裝置之直接存取隔離。

【第18項】

一種方法，其包括：

產生一媒體加密金鑰以對一設備之複數個記憶體組件中之資料加密；

包覆該媒體加密金鑰以產生一經加密媒體加密金鑰；

將該經加密媒體加密金鑰儲存於該設備之一非揮發性記憶體中；及

使用該經加密媒體加密金鑰將該設備轉變至一安全狀態及自該安全

狀態轉變。

【第19項】

如請求項18之方法，其中該設備係一四狀態設備，該四種狀態為一無主狀態、一secure_unlocked狀態、一secure_locked狀態及一不安全狀態。

【第20項】

如請求項19之方法，其中該方法包含：

產生一擦除金鑰；

包覆該擦除金鑰以形成一經包覆擦除金鑰；及

將該經包覆擦除金鑰發送至該非揮發性記憶體。