(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 201214445 A1
(43)公開日： 中華民國 101 (2012) 年 04 月 01 日

(21)申請案號：099138057 (22)申請日： 中華民國 99 (2010) 年 11 月 05 日
(51)Int. Cl.： *G11C16/14 (2006.01)*
(30)優先權：2010/09/27 美國 12/891,631
(71)申請人：擎泰科技股份有限公司 (中華民國) SKYMEDI CORPORATION (TW)
新竹市力行一路 10 號之 1 6 樓
(72)發明人：翁武坤 WENG, WU KUN (TW) ；吳信賢 WU, HSIN HSIEN (TW)
(74)代理人：陳達仁
申請實體審查：有 申請專利範圍項數：20 項 圖式數：7 共 26 頁

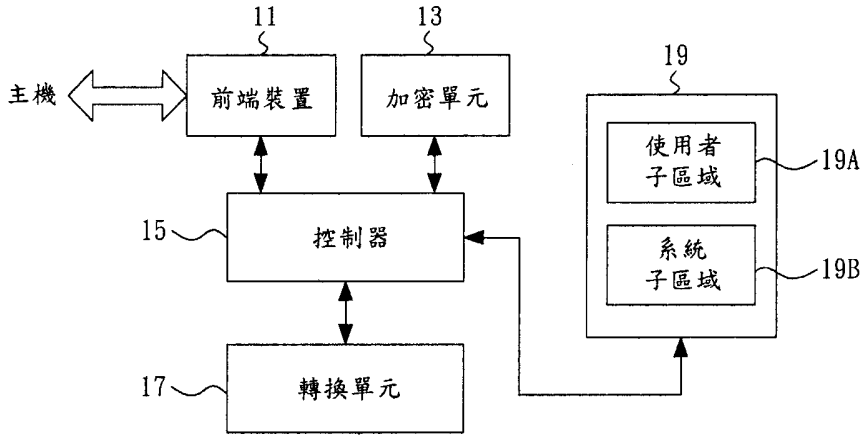
(54)名稱

固態非揮發性記憶體裝置的安全抹除系統

SECURE ERASE SYSTEM FOR A SOLID STATE NON-VOLATILE MEMORY DEVICE

(57)摘要

一種固態記憶體裝置的安全抹除系統。記憶體區域提供資料區塊及金鑰區塊，用以分別儲存資料及至少一金鑰。轉換（translation）單元將記憶體區域相關的邏輯位址映射至實體位址。加密單元使用相應之金鑰，將寫入記憶體區域的明文資料予以加密，且使用相應之金鑰，將主機所讀取之加密資料予以解密。其中，當接收一命令以要求將邏輯抹除單位（logical erase group）的相應資料予以抹除時，則將邏輯抹除單位相應之金鑰予以刪除。



11：前端裝置
13：加密單元
15：控制器
17：轉換單元
19：記憶體區域
19A：使用者子區域
19B：系統子區域

(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 201214445 A1
(43)公開日： 中華民國 101 (2012) 年 04 月 01 日

(21)申請案號：099138057 (22)申請日： 中華民國 99 (2010) 年 11 月 05 日
(51)Int. Cl.： *G11C16/14 (2006.01)*
(30)優先權：2010/09/27 美國 12/891,631
(71)申請人：擎泰科技股份有限公司 (中華民國) SKYMEDI CORPORATION (TW)
新竹市力行一路 10 號之 1 6 樓
(72)發明人：翁武坤 WENG, WU KUN (TW) ；吳信賢 WU, HSIN HSIEN (TW)
(74)代理人：陳達仁
申請實體審查：有 申請專利範圍項數：20 項 圖式數：7 共 26 頁

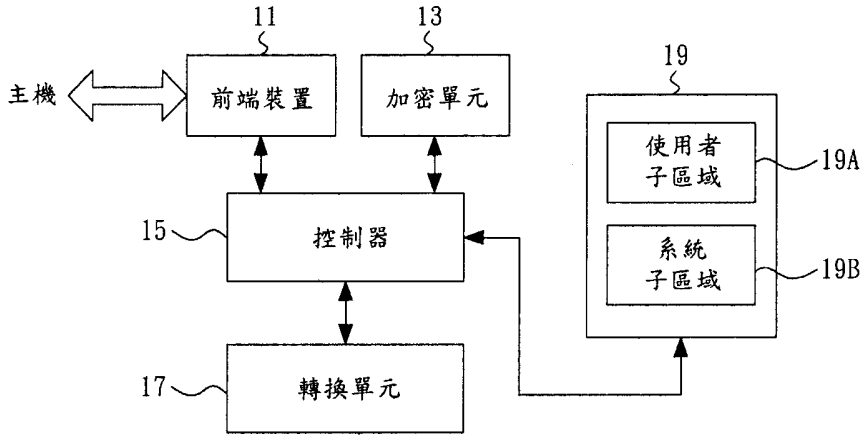
(54)名稱

固態非揮發性記憶體裝置的安全抹除系統

SECURE ERASE SYSTEM FOR A SOLID STATE NON-VOLATILE MEMORY DEVICE

(57)摘要

一種固態記憶體裝置的安全抹除系統。記憶體區域提供資料區塊及金鑰區塊，用以分別儲存資料及至少一金鑰。轉換（translation）單元將記憶體區域相關的邏輯位址映射至實體位址。加密單元使用相應之金鑰，將寫入記憶體區域的明文資料予以加密，且使用相應之金鑰，將主機所讀取之加密資料予以解密。其中，當接收一命令以要求將邏輯抹除單位（logical erase group）的相應資料予以抹除時，則將邏輯抹除單位相應之金鑰予以刪除。



11：前端裝置
13：加密單元
15：控制器
17：轉換單元
19：記憶體區域
19A：使用者子區域
19B：系統子區域

六、發明說明：

【發明所屬之技術領域】

[0001] 本發明係有關一種固態記憶體裝置，特別是關於固態非揮發性記憶體裝置的安全抹除（secure erase）系統。

【先前技術】

[0002] 快閃（flash）記憶體屬於一種非揮發性固態記憶體裝置，其可被電性抹除及程式化。由於快閃記憶體已普遍應用於電子系統當中，快閃記憶體的資料安全因而成為目前的主要課題。

[0003] 當接收到抹除或刪除命令時，大部分的作業系統並非真正將資料從快閃記憶體移除。實際上，作業系統僅將鏈結（link）或位址予以移除或作變更，而實際的資料則保留於快閃記憶體中，直到資料被覆蓋為止。於真正移除之前，資料仍可被入侵者擷取或回復。

[0004] 因此，許多系統使用安全抹除（或資料擦拭）程序，當接收到安全抹除命令時，則徹底地將資料予以抹除。傳統安全抹除技術通常使用於檔案或磁碟系統，其鏈結或指標（pointer）與待抹除資料之間具有一對一的對應關係。因此，關連於鏈結的待抹除資料即可直接且快速地抹除。然而，此種傳統安全抹除技術卻無法適用於固態非揮發性記憶體裝置，例如快閃記憶體，其原因在於，單一鏈結（或邏輯至實體映射）往往對應至快閃記憶體當中的多個資料單位（groups）。若要將所有資料單位都予以抹除則要耗費相當的時間，且要搜尋出所有資料單位也是一項複雜的工作。這些原因往往讓安全抹除變

得困難或甚至不實際。

[0005] 鑑於傳統安全抹除程序無法適用於固態非揮發性記憶體，因此亟需提出一種新穎的安全抹除系統，其可快速且有效地對非揮發性記憶體的資料進行安全抹除。

【發明內容】

[0006] 鑑於上述，本發明實施例的目的之一在於提出一種固態記憶體裝置的安全抹除系統，用以減少安全抹除的時間，且防止入侵者對資料進行回復。

[0007] 根據本發明實施例，固態記憶體裝置的安全抹除系統包含記憶體區域、轉換（translation）單元及加密單元。記憶體區域提供一資料區塊，用以儲存資料，及提供一金鑰區塊，用以儲存至少一金鑰。轉換單元將記憶體區域相關的一邏輯位址映射至一實體位址。加密單元使用相應之金鑰，將寫入記憶體區域的明文資料予以加密，且使用相應之金鑰，將主機所讀取之加密資料予以解密。其中，當接收一命令以要求將一邏輯抹除單位（logical erase group）的相應資料予以抹除時，則將該邏輯抹除單位相應之金鑰予以刪除。

【實施方式】

[0008] 第一圖之方塊圖顯示本發明實施例之固態記體裝置的安全抹除（secure erase）系統。固態記憶體裝置可以是固態非揮發性記憶體裝置，例如反及閘（NAND）快閃記憶體或相位改變（phase change）記憶體，但不限定於此。

[0009] 在本實施例中，安全抹除系統包含前端（front end）裝置11、加密（encryption）單元13、控制器15、轉換（translation）單元17及記憶體區域19。其中，前端裝置11作為安全抹除系統與主機（例如電腦或處理器）之間的介面。常見的前端裝置有安全數位卡（Secured Digital, SD）、多媒體卡（MultiMediaCard, MMC）、內嵌式MMC（embedded MMC, eMMC）、序列進階技術附加裝置（Serial Advanced technology Attachment, SATA）、周邊元件快速連接（Peripheral Component Interconnect Express, PCIe）、整合驅動電路（Integrated Drive Electronics, IDE）、通用序列匯流排（Universal Serial Bus, USB）、IEEE 1394及智慧卡（SmartCard）。

[0010] 記憶體區域19可分為使用者子區域19A及系統子區域19B。每一子區域可再分割為多個區塊。使用者子區域19A通常用於儲存使用者資料，但不限定於此；系統子區域19B通常用以儲存系統程式及相關參數。可根據個別應用以分割記憶體區域19並安排每一子區域的配置。

[0011] 根據本實施例的特徵之一，如第二圖所示，加密單元13使用相應加密金鑰（或簡稱金鑰）將明文（plain text）資料予以加密後寫入記憶體區域19，且使用相應金鑰將加密資料（或密文資料（ciphertext data））予以解密後讀至主機。加密資料儲存於記憶體區域19的資料區塊，而金鑰則儲存於記憶體區域19的金鑰區塊。上述之資料區塊及金鑰區塊可位於同一子區域（例如使用者

子區域19A）的相同或相異儲存單位（記憶區塊或記憶頁，如以NAND型快閃記憶體而言，記憶區塊可為記憶體區域中最小的抹除單位，記憶頁為最小的寫入單位。），也可位於相異子區域（例如使用者子區域19A及系統子區域19B）中的儲存單位（記憶區塊或記憶頁）。換句話說，金鑰區塊可位於使用者子區域19A、系統子區域19B或記憶體區域19的備用區（圖未示）。

[0012] 本實施例的加密單元13採用對稱金鑰演算法（symmetric-key algorithm），其對每一資料或每一邏輯抹除單位（logical erase group）產生單一金鑰，該金鑰可使用硬體或軟體的亂數產生器來產生。控制器15監督前端裝置11、加密單元13及記憶體區域19，用以從記憶體區域19讀取資料至主機，或者從主機將資料寫入記憶體區域19。第三A圖顯示從記憶體區域19讀取資料的流程圖，而第三B圖顯示將資料寫入記憶體區域19的流程圖。

[0013] 如第三A圖所示的資料讀取流程，主機首先發出讀取命令（步驟31）。接著，於步驟32，控制器15讀取儲存於金鑰區塊的金鑰。如果金鑰存在（步驟33），則加密單元13使用金鑰將儲存於記憶體區域19的加密資料予以解密（步驟34）；否則，產生異於原始讀取資料的預設樣式（例如全為”0”或”1”的樣式）並儲存於緩衝器內（步驟35），用以表示無效資料或未有資料。最後，於步驟36，將解密資料或預設樣式送至主機。

[0014] 如第三B圖所示的資料寫入流程，主機首先發出寫入命令（步驟37）。接著，於步驟38，控制器15讀取儲存於金

鑰區塊的金鑰。如果金鑰不存在（步驟39），則產生一新金鑰（步驟40），並將金鑰儲存於金鑰區塊（步驟41）。接著，於步驟42，加密單元13使用已存在金鑰或產生之金鑰將資料予以加密。最後，於步驟43，將加密資料寫至記憶體區域19。

[0015] 轉換單元17使用快閃記憶體轉換層（flash translation layer, FTL）將邏輯區塊位址（logical block address, LBA）映射至實體區塊位址（physical block address, PBA）。其中，邏輯區塊位址（LBA）可由主機來定址，而實體區塊位址（PBA）則由控制器15來定址。對於快閃記憶體，其通常會使用頁層級演算法（page level algorithm）及區塊層級演算法（block level algorithm）。第四A圖至第四D圖顯示採用頁層級演算法以進行資料寫入時，邏輯區塊位址（LBA）和實體區塊位址（PBA）之間的一系列映射。在此特殊例子中，主機將資料多次（例如n次）寫至記憶體區域19的相同邏輯位址。如圖所示，由於頁層級演算法係為一種以記錄（log）為基礎的演算法，因此當主機將資料寫至同一邏輯位址時，其更新頁會被置放於不同的實體位址。因此，從舊的至最新的更新頁會佔用記憶體區域19總共n頁記憶體空間。

[0016] 第五A圖至第五C圖顯示採用區塊層級演算法以進行資料寫入時，邏輯區塊位址（LBA）和實體區塊位址（PBA）之間的一系列映射。在此特殊例子中，主機將資料多次（例如3次）寫至記憶體區域19的相同邏輯位址。如圖所

示，當主機將資料寫至同一邏輯位址時，其更新區塊會被置放於記憶體區域19中的其中之一可用的記憶區塊（如記憶區塊B0或記憶區塊B1）。因此，最新的及其前一個更新區塊會佔用記憶體區域19總共二區塊記憶體空間。

[0017] 無論是頁層級演算法（第四A圖至第四D圖）或者區塊層級演算法（第五A圖至第五C圖），當主機將資料寫至同一邏輯位址時，資料會存放於記憶體區域19的多組記憶體空間或資料儲存單位。

[0018] 根據本實施例的另一特徵，當主機發出安全抹除命令時，該命令要求將邏輯抹除單位（logical erase group）的相應資料予以抹除，則只要將該資料或邏輯抹除單位相應的金鑰予以刪除。一般來說，每一邏輯抹除單位（其可為記憶體區域19可定義之任何資料抹除單元）可相應一金鑰。第六圖顯示本發明實施例之安全抹除資料的流程圖。首先，於步驟61，主機發出安全抹除命令。接著，於步驟62，讀取儲存於金鑰區塊的金鑰。如果存在有金鑰（步驟63），則刪除該金鑰，例如藉由快閃記憶體的抹除命令（步驟64）。當金鑰被刪除後，則相應的加密資料則無法再予以回復。雖然本實施例的安全抹除命令係由主機所發出，然而安全抹除命令也可由安全抹除系統本身（例如控制器15）來發出。

[0019] 第七A圖至第七B圖顯示本發明實施例中採用頁層級演算法的一個安全抹除例子。如第七A圖所示，於進行安全抹除之前，相應於不同邏輯位址的（加密）資料1及資料2位於實體區塊1及區塊2。較大計數值Cnt即表示相應的資

料較晚寫入實體區塊內。例如，Cnt=6的相應資料2比Cnt=5的相應資料2較晚寫入實體區塊2內。再者，資料1及資料2的相應金鑰儲存於金鑰區塊內。

[0020] 如第七B圖所示，於進行安全抹除之後，資料2的金鑰被刪除，並儲存一新金鑰。在另一實施例中，並不需要在資料2被抹除時立即產生該新金鑰。取而代之的是，在進行下一寫入操作時才產生該新金鑰。於圖示的例子中，由於Cnt=1至6之資料2所對應之金鑰已被刪除，因此，資料2即無法再被正確的讀取並予以回復。

[0021] 藉此，相較於傳統安全抹除方法係將資料一個一個地進行抹除，本發明實施例之安全抹除系統於進行安全抹除時的執行速度將較傳統方法來得快。

[0022] 以上所述僅為本發明之較佳實施例而已，並非用以限定本發明之申請專利範圍；凡其它未脫離發明所揭示之精神下所完成之等效改變或修飾，均應包含在下述之申請專利範圍內。

【圖式簡單說明】

[0023] 第一圖之方塊圖顯示本發明實施例之固態記體裝置的安全抹除系統。

第二圖顯示第一圖之加密單元進行資料加密及解密。

第三A圖顯示從記憶體區域讀取資料的流程圖。

第三B圖顯示將資料寫入記憶體區域的流程圖。

第四A圖至第四D圖顯示採用頁層級演算法以進行資料寫入時，邏輯區塊位址（LBA）和實體區塊位址（PBA）之間的一系列映射。

第五A圖至第五C圖顯示採用區塊層級演算法以進行資料寫入時，邏輯區塊位址（LBA）和實體區塊位址（PBA）之間的一系列映射。

第六圖顯示本發明實施例之安全抹除資料的流程圖。

第七A圖至第七B圖顯示本發明實施例中採用頁層級演算法的一個安全抹除例子。

【主要元件符號說明】

[0024]

11	前端裝置
13	加密單元
15	控制器
17	轉換單元
19	記憶體區域
19A	使用者子區域
19B	系統子區域
31-36	步驟
37-43	步驟
61-64	步驟

201214445

專利案號：099138057

智專收字第0992066319-0

DTD版本：1.0.1

日期：99年11月05日

發明專利說明書

※申請案號：099138057　　※ＩＰＣ分類：G11C 16/14 (2006.01)

※申請日：99.11.05

一、發明名稱：

固態非揮發性記憶體裝置的安全抹除系統

SECURE ERASE SYSTEM FOR A SOLID STATE NON-VOLATILE MEMORY DEVICE

二、中文發明摘要：

一種固態記憶體裝置的安全抹除系統。記憶體區域提供資料區塊及金鑰區塊，用以分別儲存資料及至少一金鑰。轉換（translation）單元將記憶體區域相關的邏輯位址映射至實體位址。加密單元使用相應之金鑰，將寫入記憶體區域的明文資料予以加密，且使用相應之金鑰，將主機所讀取之加密資料予以解密。其中，當接收一命令以要求將邏輯抹除單位（logical erase group）的相應資料予以抹除時，則將邏輯抹除單位相應之金鑰予以刪除。

三、英文發明摘要：

A secure erase system for a solid state memory device is disclosed. A memory area provides a data block for storing data and a key block for storing at least one key. A translation unit maps a logical address to a physical address associated with the memory area. An encryption unit encrypts plaintext data to be written to the memory area with the associated key and decrypts the encrypted data to be read by a host with the associated key. The key associated with a logical erase group to be secure erased is deleted after receiving a command requesting to erase the data associated with the logical erase group.

七、申請專利範圍：

1．一種固態記憶體裝置的安全抹除系統，包含：

一記憶體區域，其提供一資料區塊，用以儲存資料，及一金鑰區塊，用以儲存至少一金鑰；

一轉換（translation）單元，用以將該記憶體區域相關的一邏輯位址映射至一實體位址；及

一加密單元，其使用相應之該金鑰，將寫入該記憶體區域的明文資料予以加密，且使用相應之該金鑰，將一主機所讀取之加密資料予以解密；

其中，當接收一命令以要求將一邏輯抹除單位（logical erase group）的相應該資料予以抹除時，則將該邏輯抹除單位相應之該金鑰予以刪除。

2．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之記憶體區域為一固態非揮發性記憶體裝置。

3．如申請專利範圍第2項所述固態記憶體裝置的安全抹除系統，其中上述之固態非揮發性記憶體裝置為快閃記憶體或相位改變（phase change）記憶體。

4．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，更包含一前端裝置，作為該安全抹除系統的介面。

5．如申請專利範圍第4項所述固態記憶體裝置的安全抹除系統，其中上述之前端裝置為下列之一：安全數位卡（Secured Digital, SD）、多媒體卡（MultiMediaCard, MMC）、內嵌式MMC（embedded MMC, eMMC）、序列進階技術附加裝置（Serial

Advanced technology Attachment, SATA）、周邊元件快速連接（Peripheral Component Interconnect Express, PCIe）、整合驅動電路（Integrated Drive Electronics, IDE）、通用序列匯流排（Universal Serial Bus, USB）、IEEE 1394及智慧卡（SmartCard）。

6．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之記憶體區域分為：一使用者區域，用以儲存使用者資料；及一系統區域，用以儲存系統程式及相關參數。

7．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之資料區塊及該金鑰區塊位於該記憶體區域之一子區域的相同或相異儲存單位。

8．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之資料區塊及該金鑰區塊分別位於該記憶體區域之不同子區域的儲存單位。

9．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之金鑰區塊位於該記憶體區域的一使用者子區域、一系統子區域或一備用區。

10．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之加密單元採用對稱金鑰演算法（symmetric-key algorithm），以產生單一金鑰。

11．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之金鑰係由一亂數產生器所產生。

12．如申請專利範圍第4項所述固態記憶體裝置的安全抹除系統，更包含一控制器，其監督該加密單元、該前端裝置及

該記憶體區域，用以從該記憶體區域讀取資料至該主機，或者從該主機將資料寫入該記憶體區域。

13．如申請專利範圍第12項所述固態記憶體裝置的安全抹除系統，於接收到一讀取命令後，該控制器讀取儲存於該金鑰區塊的金鑰；如果該金鑰存在，則該加密單元使用該金鑰將儲存於該記憶體區域的加密資料予以解密並送至該主機；否則，產生一預設樣式至該主機，用以表示無效資料或未有資料。

14．如申請專利範圍第12項所述固態記憶體裝置的安全抹除系統，於接收到一寫入命令後，該控制器讀取儲存於該金鑰區塊的金鑰；如果該金鑰不存在，則產生一新金鑰並儲存於該金鑰區塊；使用已存在之該金鑰或產生之該新金鑰將待寫入資料予以加密，並將該加密資料寫至該記憶體區域。

15．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之邏輯位址係藉由一快閃記憶體轉換層（flash translation layer, FTL）將其映射至該實體位址。

16．如申請專利範圍第15項所述固態記憶體裝置的安全抹除系統，其中上述之快閃記憶體轉換層採用頁層級演算法（page level algorithm）或區塊層級演算法（block level algorithm）。

17．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，其中上述之邏輯抹除單位係為該記憶體區域可定義之資料抹除單元。

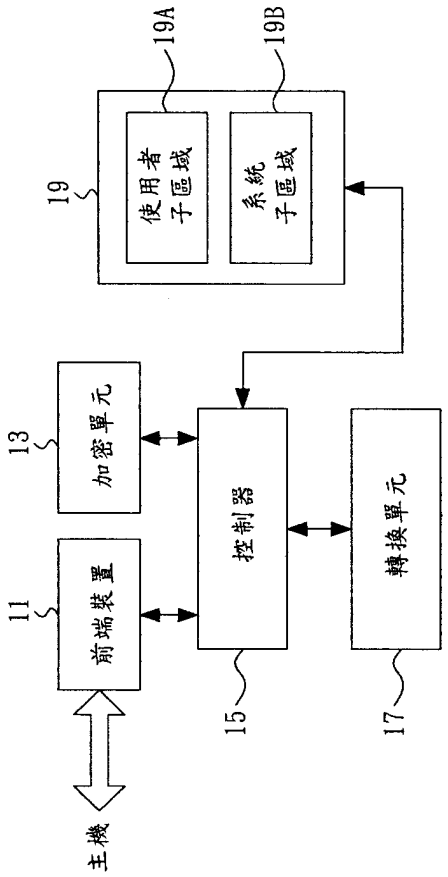
18．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系

統，其中上述之命令係由一主機所發出。

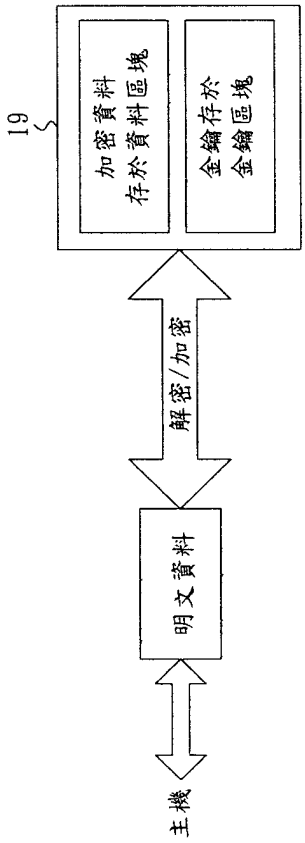
19．如申請專利範圍第12項所述固態記憶體裝置的安全抹除系統，其中上述之命令係由該控制器所發出。

20．如申請專利範圍第1項所述固態記憶體裝置的安全抹除系統，於接收到該命令後，從該金鑰區塊讀取該金鑰；如果該金鑰存在，則將該金鑰刪除。

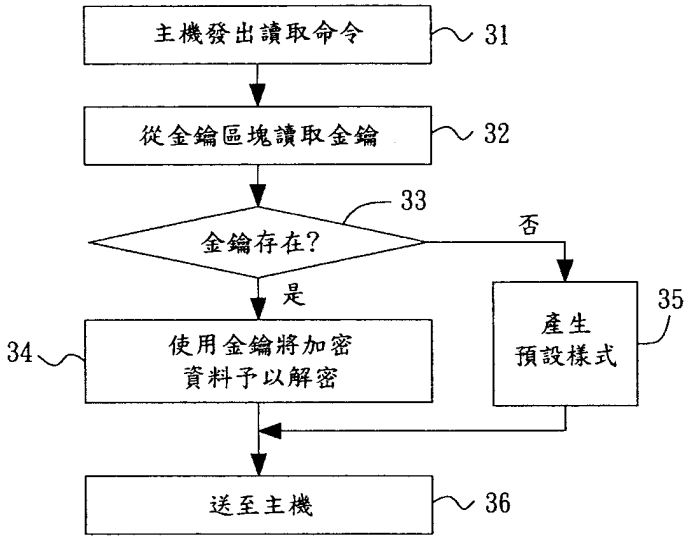
八、圖式：



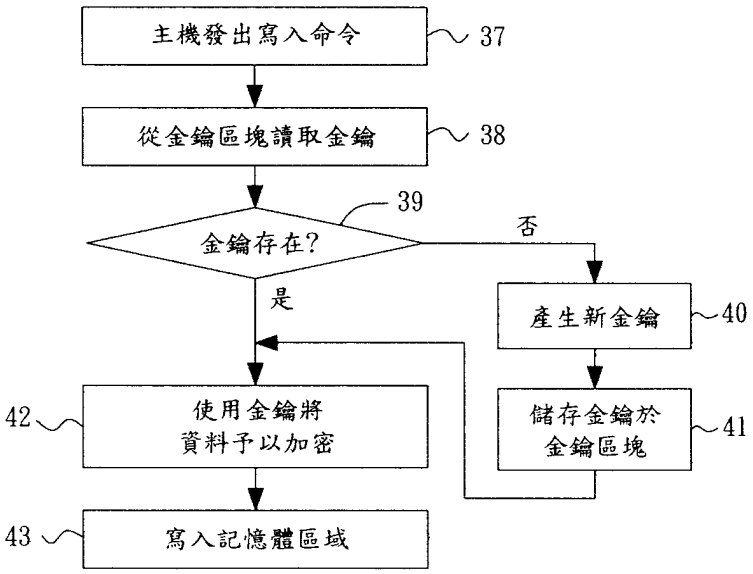
第一圖



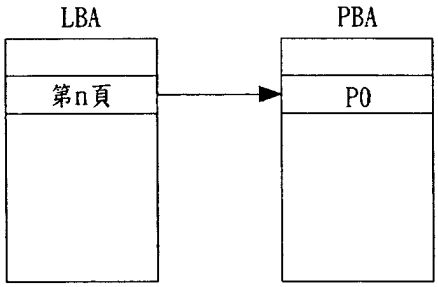
第二圖


主機發出讀取命令
31
從金鑰區塊讀取金鑰
32
33
金鑰存在?
否
是
34
使用金鑰將加密
資料予以解密
35
產生
預設樣式
送至主機
36

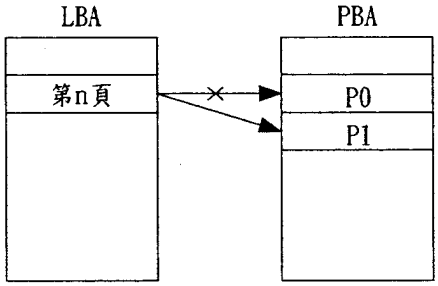
第三A圖


主機發出寫入命令
37
從金鑰區塊讀取金鑰
38
39
金鑰存在?
否
是
產生新金鑰
40
使用金鑰將
資料予以加密
42
儲存金鑰於
金鑰區塊
41
寫入記憶體區域
43

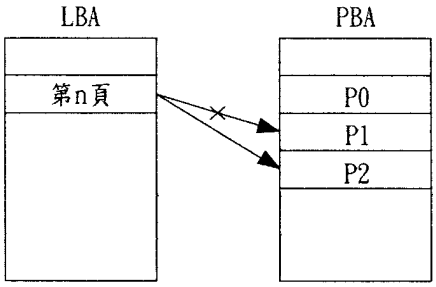
第三B圖



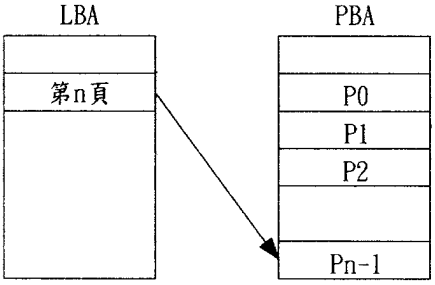
第四A圖



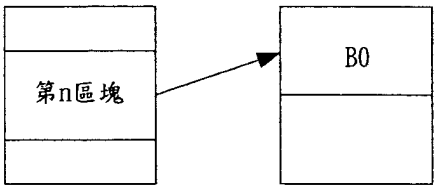
第四B圖



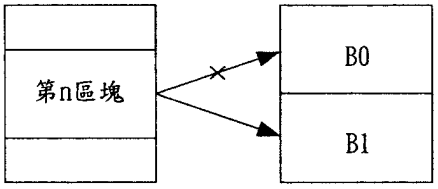
第四C圖



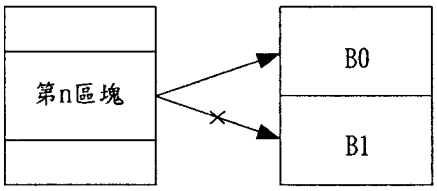
第四D圖



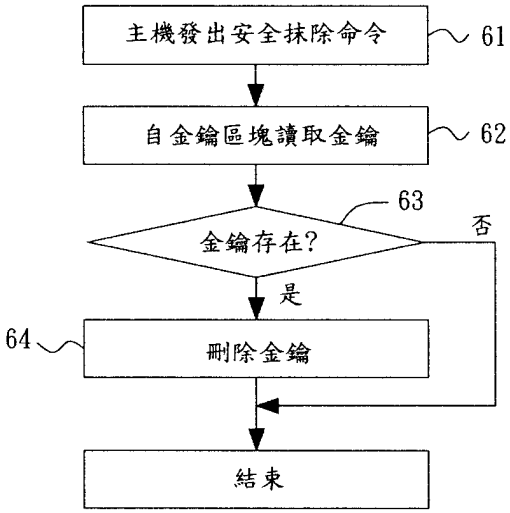
第五A圖



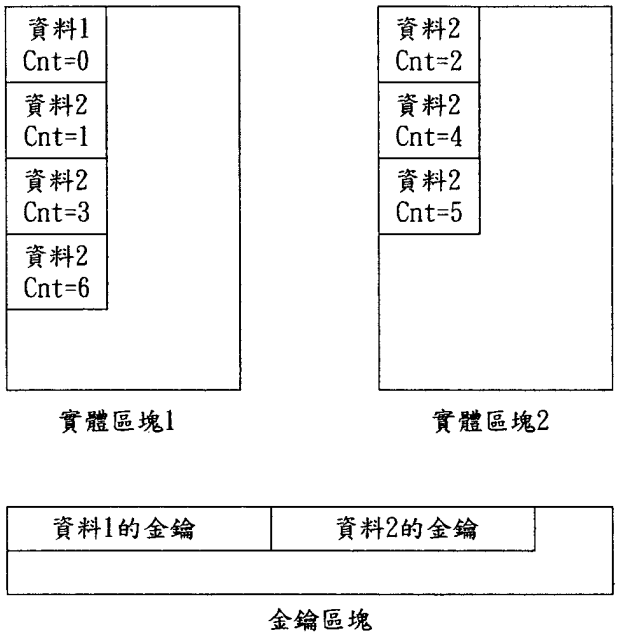
第五B圖



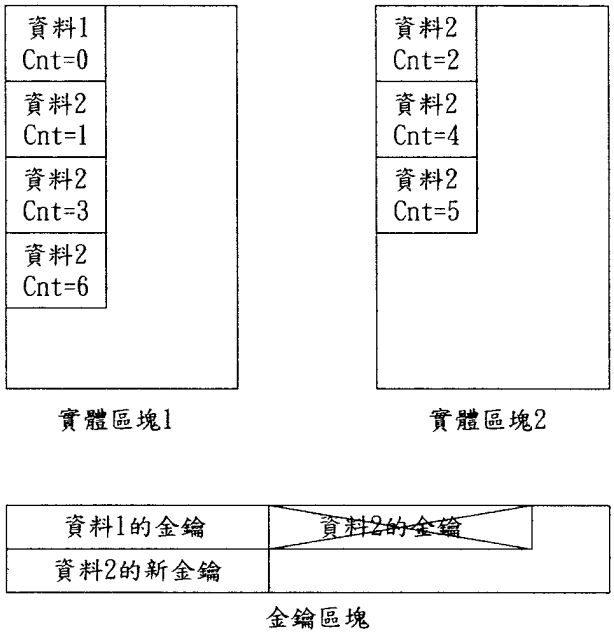
第五C圖



第六圖


資料1
Cnt=0
資料2
Cnt=1
資料2
Cnt=3
資料2
Cnt=6
資料2
Cnt=2
資料2
Cnt=4
資料2
Cnt=5
實體區塊1
實體區塊2
資料1的金鑰
資料2的金鑰
金鑰區塊

第七A圖


資料1
Cnt=0
資料2
Cnt=1
資料2
Cnt=3
資料2
Cnt=6
資料2
Cnt=2
資料2
Cnt=4
資料2
Cnt=5
實體區塊1
實體區塊2
資料1的金鑰
~~資料2的金鑰~~
資料2的新金鑰
金鑰區塊

第七B圖

四、指定代表圖：

(一)本案指定代表圖為：第一圖

(二)本代表圖之元件符號簡單說明：

11	前端裝置
13	加密單元
15	控制器
17	轉換單元
19	記憶體區域
19A	使用者子區域
19B	系統子區域

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：