



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I536199 B

(45)公告日：中華民國 105 (2016) 年 06 月 01 日

(21)申請案號：104100960 (22)申請日：中華民國 104 (2015) 年 01 月 12 日

(51)Int. Cl. : G06F21/79 (2013.01) G06F21/62 (2013.01)

(71)申請人：群聯電子股份有限公司 (中華民國) PHISON ELECTRONICS CORP. (TW)
苗栗縣竹南鎮群義路 1 號

(72)發明人：伍漢維 NG, HON WAI (TW)；羅仁瑋 LO, JEN WEI (TW)；李乾輔 LEE, CHIEN FU (TW)；許家榮 HSU, CHIA JUNG (TW)

(74)代理人：葉璟宗；詹東穎；劉亞君

(56)參考文獻：

TW	I438777	TW	I451248
TW	I467376	US	7444523B2
US	7478235B2	US	2010/0058073A1

審查人員：何旭智

申請專利範圍項數：22 項 圖式數：7 共 43 頁

(54)名稱

資料保護方法、記憶體控制電路單元及記憶體儲存裝置

DATA PROTECTION METHOD, MEMORY CONTROL CIRCUIT UNIT AND MEMORY STORAGE DEVICE

(57)摘要

本揭露提出一種資料保護方法、記憶體控制電路單元及記憶體儲存裝置。資料保護方法包括：透過無線通訊網路與電子裝置建立安全通道；透過建立於無線通訊網路上的安全通道取得識別碼；使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中；使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料以加解密金鑰來被加密；偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置的確認訊號；倘若在預定時間內未接收到來自於電子裝置的確認訊號，清除儲存於緩衝記憶體中的加解密金鑰。

The present disclosure provides a data protection method, a memory control circuit unit and a memory storage device. The data protection method includes: establishing a security channel with a electronic device through a wireless communication network; acquiring an identification code through the secure session established through the wireless communication network; acquiring a encryption/decryption key with the identification code and storing the encryption/decryption key in a buffer memory; decoding the data read from the rewritable non-volatile memory with the encryption/decryption key, wherein the data in the rewritable non-volatile memory is encoded with the encryption/decryption key; detecting whether a confirmation signal is received from the secure session established through the wireless communication network; erasing the encryption/decryption key stored in the buffer memory if the confirmation signal from the electronic device is not received in a predetermined period of time.

指定代表圖：

符號簡單說明：

S602、S604、S606、
S608、S610、
S612 . . . 資料保護
方法的步驟

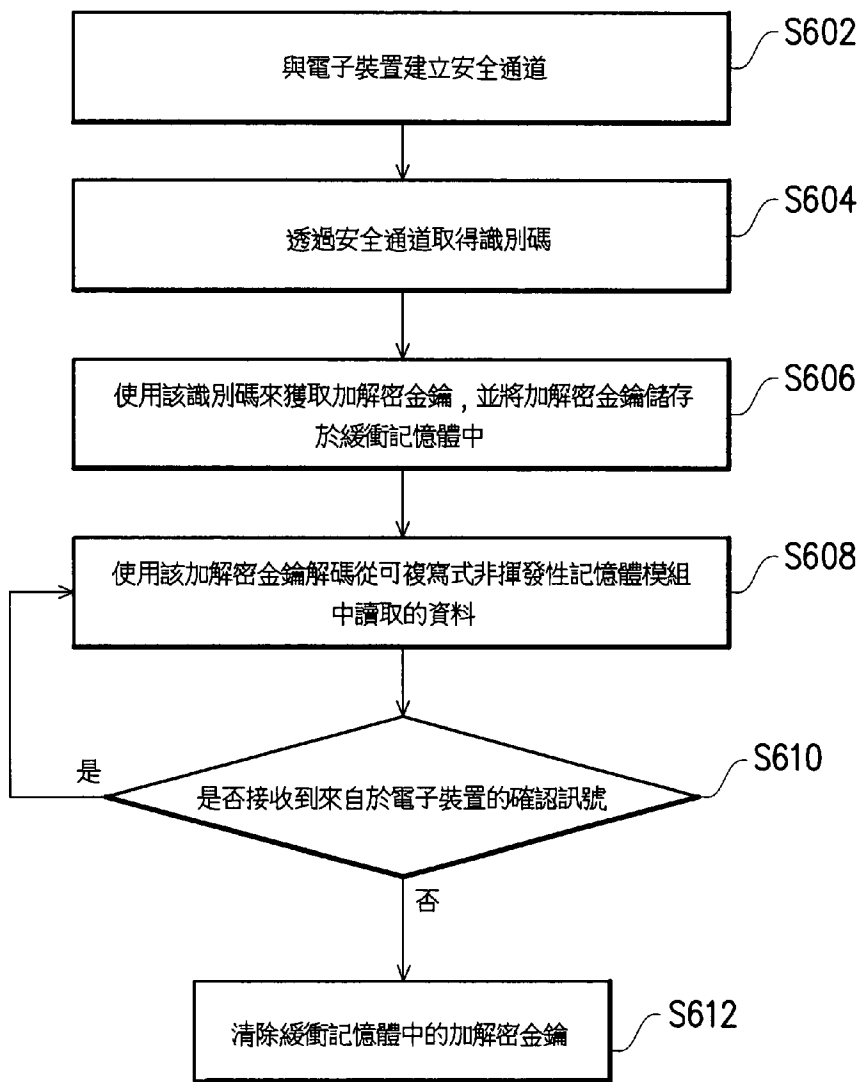


圖6

公告本

發明摘要

※ 申請案號：

※ 申請日：

※IPC 分類：

【發明名稱】

資料保護方法、記憶體控制電路單元及記憶體儲存裝置

DATA PROTECTION METHOD, MEMORY CONTROL CIRCUIT
UNIT AND MEMORY STORAGE DEVICE

【中文】

本揭露提出一種資料保護方法、記憶體控制電路單元及記憶體儲存裝置。資料保護方法包括：透過無線通訊網路與電子裝置建立安全通道；透過建立於無線通訊網路上的安全通道取得識別碼；使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中；使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料以加解密金鑰來被加密；偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置的確認訊號；倘若在預定時間內未接收到來自於電子裝置的確認訊號，清除儲存於緩衝記憶體中的加解密金鑰。

【英文】

The present disclosure provides a data protection method, a memory control circuit unit and a memory storage device. The data

protection method includes: establishing a security channel with a electronic device through a wireless communication network; acquiring an identification code through the secure session established through the wireless communication network; acquiring a encryption/decryption key with the identification code and storing the encryption/decryption key in a buffer memory; decoding the data read from the rewritable non-volatile memory with the encryption/decryption key, wherein the data in the rewritable non-volatile memory is encoded with the encryption/decryption key; detecting whether a confirmation signal is received from the secure session established through the wireless communication network; erasing the encryption/decryption key stored in the buffer memory if the confirmation signal from the electronic device is not received in a predetermined period of time.

【代表圖】

【本案指定代表圖】：圖 6。

【本代表圖之符號簡單說明】：

S602、S604、S606、S608、S610、S612：資料保護方法的步驟

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無。

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】

資料保護方法、記憶體控制電路單元及記憶體儲存裝置

DATA PROTECTION METHOD, MEMORY CONTROL CIRCUIT
UNIT AND MEMORY STORAGE DEVICE

【技術領域】

● 【0001】 本揭露是有關於一種用於可複寫式非揮發性記憶體模組的資料保護方法以及使用此方法的記憶體控制電路單元和記憶體儲存裝置。

【先前技術】

● 【0002】 隨身碟是一種資料儲存設備，其一般是以快閃記憶體作為儲存媒體。快閃記憶體是一種電氣抹除式可編程唯讀記憶體 (Electrically Erasable Programmable Read Only Memory, EEPROM)，其具有可寫入、可抹除、以及斷電後仍可保存數據的優點。此外，快閃記憶體為非揮發性記憶體 (Non-Volatile Memory) 的一種，其具有體積小、存取速度快、耗電量低的優點，且因其資料抹除 (Erasing) 時是採用「一次一個區塊」 (Block by Block) 的抹除方式，所以具有操作速度快的優點。由於隨身碟體積小容量大且攜帶方便，因此已廣泛用於個人資料的儲存。然而，當隨身碟不小心遺失時，其所儲存的大量資料也可能隨之被盜用。

【0003】 爲了解決以上問題，廠商開發了無線相容認證(Wireless Fidelity, WiFi)隨身碟及安全數位(Secure Digital, SD)卡、Wi-Fi 無線讀卡機或無線外接式硬碟盒等產品，其可設立個人 Wi-Fi 保護存取(Wi-Fi Protected Access Personal, WPA-Personal)等安全機制，但在此機制中各裝置之間都是使用共享金鑰方式來進行連線，因此每位在分享網路的使用者都可在連線中竊取或竄改他人資料。基於上述，如何在無線通訊網路環境下確保記憶體儲存裝置的安全性是本領域中待解決的問題。

【發明內容】

【0004】 本揭露提供一種資料保護方法、記憶體控制電路單元及記憶體儲存裝置，其利用建立於無線通訊網路的安全通道傳輸識別碼，並使用識別碼產生加解密金鑰來讀取記憶體儲存裝置，以提高記憶體儲存裝置的安全性。

【0005】 本揭露的一範例實施例提出一種資料保護方法，用於保護記憶體儲存裝置中可複寫式非揮發性記憶體模組的資料。本資料保護方法包括：透過無線通訊網路與電子裝置建立安全通道。本方法更包括：透過建立於無線通訊網路上的安全通道取得識別碼。本方法更包括：使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中。本方法更包括：使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料以加解密金鑰來被加密。本方法更包

括：偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置的確認訊號。本方法更包括：倘若在預定時間內未接收到來自於電子裝置的確認訊號，清除儲存於緩衝記憶體中的加解密金鑰。

【0006】 在本揭露的一實施例中，上述資料保護方法更包括：在清除儲存於緩衝記憶體中的加解密金鑰之後，將記憶體儲存裝置設定為無媒體狀態。

● 【0007】 在本揭露的一實施例中，上述透過建立於無線通訊網路上的安全通道取得識別碼的步驟包括：透過建立於無線通訊網路上的安全通道取得從電子裝置輸入的識別碼，其中電子裝置為手持電子裝置。

● 【0008】 在本揭露的一實施例中，上述透過建立於無線通訊網路上的安全通道取得識別碼的步驟包括：透過建立於無線通訊網路上的安全通道取得電子裝置產生的識別碼，其中電子裝置為伺服器並耦接至無線網路存取點。

【0009】 在本揭露的一實施例中，其中無線通訊網路為藍芽網路、無線相容性認證網路、近場通訊網路或無線射頻識別網路。

【0010】 在本揭露的一實施例中，上述使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中的步驟包括：在可複寫式非揮發性記憶體模組中儲存個人識別碼訊息摘要及密鑰。上述步驟更包括：使用單向雜湊函數產生對應識別碼的訊息摘要。上述步驟更包括：判斷訊息摘要與個人識別碼訊息摘要是否相

符，其中當訊息摘要及個人識別碼訊息摘要相符時，依據識別碼使用加解密函數解碼密鑰以獲得加解密金鑰。

【0011】 在本揭露的一實施例中，上述在可複寫式非揮發性記憶體模組中儲存個人識別碼訊息摘要及密鑰的步驟包括：初始地藉由單向雜湊函數依據個人識別碼產生個人識別碼訊息摘要。上述步驟更包括：初始地依據個人識別碼使用加解密函數加密加解密金鑰以產生密鑰。

【0012】 在本揭露的一實施例中，上述初始地依據個人識別碼使用加解密函數加密加解密金鑰以產生密鑰的步驟包括：初始地以隨機方式產生加解密金鑰。

【0013】 在本揭露的一實施例中，上述使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料的步驟包括：依據加解密金鑰使用加解密函數解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料依據加解密金鑰使用加解密函數被加密。

【0014】 本揭露的一範例實施例提出一種記憶體控制電路單元，用於控制可複寫式非揮發性記憶體模組，其包括主機介面、記憶體介面、記憶體管理電路及無線通訊介面。主機介面耦接至主機系統。記憶體介面耦接至可複寫式非揮發性記憶體模組。記憶體管理電路耦接至主機介面及記憶體介面。無線通訊介面耦接至記憶體管理電路。其中記憶體控制電路單元透過無線通訊介面以無線通訊網路與電子裝置建立安全通道。其中無線通訊介面透過建

立於無線通訊網路上的安全通道取得識別碼。其中記憶體管理電路使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中。其中記憶體管理電路使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料以加解密金鑰來被加密。其中無線通訊介面偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置的確認訊號。其中，倘若無線通訊介面在預定時間內未接收到來自於電子裝置的確認訊號，記憶體管理電路清除儲存於緩衝記憶體中的加解密金鑰。

【0015】 在本揭露的一實施例中，上述記憶體管理電路在記憶體管理電路清除儲存於緩衝記憶體中的加解密金鑰之後，當記憶體管理電路接收到主機系統的存取訊號時，記憶體管理電路傳送無媒體訊號到主機系統。

【0016】 在本揭露的一實施例中，上述無線通訊網路為藍芽網路、無線相容性認證網路、近場通訊網路或無線射頻識別網路。

【0017】 在本揭露的一實施例中，上述記憶體管理電路在可複寫式非揮發性記憶體模組中儲存個人識別碼訊息摘要及密鑰。上述記憶體管理電路更使用單向雜湊函數產生對應識別碼的訊息摘要。上述記憶體管理電路更判斷訊息摘要與個人識別碼訊息摘要是否相符，其中當訊息摘要及個人識別碼訊息摘要相符時，記憶體管理電路依據識別碼使用加解密函數解碼密鑰以獲得加解密金鑰。

【0018】 在本揭露的一實施例中，上述記憶體管理電路初始地依據個人識別碼使用加解密函數加密加解密金鑰以產生密鑰。

【0019】 本揭露的一範例實施例提出一種記憶體儲存裝置，其包括連接介面單元、可複寫式非揮發性記憶體模組、記憶體控制電路單元及無線通訊介面。連接介面單元耦接至主機系統。記憶體控制電路單元耦接至連接介面單元及可複寫式非揮發性記憶體模組。無線通訊介面耦接至記憶體控制電路單元。其中記憶體控制單元透過無線通訊介面以無線通訊網路與電子裝置電子裝置建立安全通道。其中記憶體控制電路單元透過建立於無線通訊網路上的安全通道取得識別碼。其中記憶體控制電路單元使用識別碼來獲取加解密金鑰並且將加解密金鑰儲存於緩衝記憶體中。其中記憶體控制電路單元使用加解密金鑰解碼從可複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料以加解密金鑰來被加密。其中記憶體控制電路單元偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置的確認訊號。其中，倘若記憶體控制電路單元在預定時間內未接收到來自於電子裝置的確認訊號，記憶體控制電路單元清除儲存於緩衝記憶體中的加解密金鑰。

【0020】 在本揭露的一實施例中，上述記憶體控制電路單元在記憶體控制電路單元清除儲存於緩衝記憶體中的加解密金鑰之後，當記憶體控制電路單元接收到主機系統的存取訊號時，記憶體控制電路單元傳送無媒體訊號到主機系統。

【0021】 在本揭露的一實施例中，上述記憶體控制電路單元透過建立於無線通訊網路上的安全通道取得從電子裝置輸入的識別碼，其中電子裝置為手持電子裝置。

【0022】 在本揭露的一實施例中，上述記憶體控制電路單元透過建立於無線通訊網路上的安全通道取得電子裝置產生的識別碼，其中電子裝置為伺服器並耦接至無線網路存取點。

【0023】 在本揭露的一實施例中，上述無線通訊網路為藍芽網路、無線相容性認證網路、近場通訊網路或無線射頻識別網路。

【0024】 在本揭露的一實施例中，上述記憶體控制電路單元在可複寫式非揮發性記憶體模組中儲存個人識別碼訊息摘要及密鑰。上述記憶體控制電路單元更使用單向雜湊函數產生對應識別碼的訊息摘要。上述記憶體控制電路單元更判斷訊息摘要與個人識別碼訊息摘要是否相符，其中當訊息摘要及個人識別碼訊息摘要相符時，記憶體管理電路依據識別碼使用加解密函數解碼密鑰以獲得加解密金鑰。

【0025】 在本揭露的一實施例中，上述記憶體控制電路單元初始地依據個人識別碼使用加解密函數加密加解密金鑰以產生密鑰。

【0026】 在本揭露的一實施例中，上述記憶體控制電路單元初始地以隨機方式產生加解密金鑰。

【0027】 在本揭露的一實施例中，上述記憶體控制電路單元依據加解密金鑰使用加解密函數解碼從複寫式非揮發性記憶體模組中讀取的資料，其中可複寫式非揮發性記憶體模組的資料依據加解

密金鑰使用加解密函數被加密。

【0028】 基於上述，本揭露的資料保護方法透過建立於無線通訊網路上的安全通道從電子裝置取得識別碼，使用識別碼與預先儲存於記憶體儲存裝置中的密鑰獲取加解密金鑰，並使用加解密金鑰解碼記憶體儲存裝置的資料。若在預定時間內沒有從安全通道接收到確認訊號，可判斷記憶體儲存裝置已遠離電子裝置，則清除加解密金鑰，並將記憶體儲存裝置設定為無媒體狀態。

【0029】 為讓本揭露的上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【圖式簡單說明】

【0030】

圖 1 是根據本揭露一範例實施例所繪示的主機系統、記憶體儲存裝置及電子裝置。

圖 2 是根據本揭露一範例實施例所繪示的主機系統與輸入/輸出裝置的示意圖。

圖 3 是根據本揭露一範例實施例所繪示的主機系統與記憶體儲存裝置的示意圖。

圖 4 是繪示圖 1 所示的記憶體儲存裝置的概要方塊圖。

圖 5 是根據本揭露一範例實施例所繪示的記憶體控制電路單元的概要方塊圖。

圖 6 是根據本揭露一範例實施例所繪示的資料保護方法的流

程圖。

圖 7 是根據本揭露另一範例實施例所繪示的資料保護方法的流程圖。

【實施方式】

【0031】 一般而言，記憶體儲存裝置(亦稱，記憶體儲存系統)包括可複寫式非揮發性記憶體模組與控制器(亦稱，控制電路)。通常記憶體儲存裝置是與主機系統一起使用，以使主機系統可將資料寫入至記憶體儲存裝置或從記憶體儲存裝置中讀取資料。

【0032】 圖 1 是根據本揭露一範例實施例所繪示的主機系統、記憶體儲存裝置及電子裝置。

【0033】 請參照圖 1，電子裝置 2000 可為手機、平板電腦等可攜式電子裝置，透過無線網路與記憶體儲存裝置 100 進行無線通訊。電子裝置 2000 也可為伺服器，透過無線網路存取點與記憶體儲存裝置 100 進行無線通訊。然而，本揭露並不以此為限，電子裝置 2000 也可為其他具有無線通訊網路功能的裝置，透過無線網路與記憶體儲存裝置 100 進行無線通訊。

【0034】 主機系統 1000 一般包括電腦 1100 與輸入/輸出(input/output, I/O)裝置 1106。電腦 1100 包括微處理器 1102、隨機存取記憶體(random access memory, RAM) 1104、系統匯流排 1108 與資料傳輸介面 1110。輸入/輸出裝置 1106 包括如圖 2 的滑鼠 1202、鍵盤 1204、顯示器 1206 與印表機 1208。必須瞭解的是，

圖 2 所示的裝置非限制輸入/輸出裝置 1106，輸入/輸出裝置 1106 可更包括其他裝置。

【0035】 在一範例實施例中，記憶體儲存裝置 100 是透過資料傳輸介面 1110 與主機系統 1000 的其他元件耦接。藉由微處理器 1102、隨機存取記憶體 1104 與輸入/輸出裝置 1106 的運作可將資料寫入至記憶體儲存裝置 100 或從記憶體儲存裝置 100 中讀取資料。例如，記憶體儲存裝置 100 可以是如圖 2 所示的隨身碟 1212、記憶卡 1214 或固態硬碟(Solid State Drive, SSD)1216 等的可複寫式非揮發性記憶體儲存裝置。

【0036】 一般而言，主機系統 1000 為可實質地與記憶體儲存裝置 100 配合以儲存資料的任意系統。雖然在本範例實施例中，主機系統 1000 是以電腦系統來作說明，然而，在另一範例實施例中，主機系統 1000 可以是數位相機、攝影機、通信裝置、音訊播放器或視訊播放器等系統。例如，在主機系統為數位相機(攝影機)1310 時，可複寫式非揮發性記憶體儲存裝置則為其所使用的安全數位(Secure Digital, SD)卡 1312、多媒體儲存卡(Multi Media Card, MMC)1314、記憶棒(memory stick)1316、小型快閃(Compact Flash, CF)卡 1318 或嵌入式儲存裝置 1320(如圖 3 所示)。嵌入式儲存裝置 1320 包括嵌入式多媒體卡(Embedded MMC, eMMC)。值得一提的是，嵌入式多媒體卡是直接耦接於主機系統的基板上。

【0037】 圖 4 是根據一範例實施例所示的記憶體儲存裝置的概要方塊圖。

【0038】 請參照圖 4，記憶體儲存裝置 100 包括連接介面單元 102、記憶體控制電路單元 104、可複寫式非揮發性記憶體模組 106 與無線通訊介面 108。在本範例實施例中，記憶體儲存裝置 100 為隨身碟。但必須瞭解的是，在另一範例實施例中，記憶體儲存裝置 100 亦可以是記憶卡或固態硬碟(Solid State Drive, SSD)。

【0039】 在本範例實施例中，連接介面單元 102 是相容於通用序列匯流排(Universal Serial Bus, USB) 標準。然而，必須瞭解的是，本揭露不限於此，連接介面單元 102 亦可以是符合並列先進附件(Parallel Advanced Technology Attachment, PATA)標準、電氣和電子工程師協會(Institute of Electrical and Electronic Engineers, IEEE) 1394 標準、高速周邊零件連接介面(Peripheral Component Interconnect Express, PCI Express) 標準、序列先進附件(Serial Advanced Technology Attachment, SATA)標準、超高速一代(Ultra High Speed-I, UHS-I)介面標準、超高速二代(Ultra High Speed-II, UHS-II)介面標準、安全數位(Secure Digital, SD)介面標準、記憶棒(Memory Stick, MS)介面標準、多媒體儲存卡(Multi Media Card, MMC)介面標準、小型快閃(Compact Flash, CF)介面標準、整合式驅動電子介面(Integrated Device Electronics, IDE)標準或其他適合的標準。在本範例實施例中，連接介面單元 102 可與記憶體控制電路單元 104 封裝在一個晶片中，或佈設於一包含記憶體控制電路單元 104 之晶片外。

【0040】 記憶體控制電路單元 104 用以執行以硬體型式或軟體型

式實作的多個邏輯閘或控制指令，並且根據主機系統 1000 的指令在可複寫式非揮發性記憶體模組 106 中進行資料的寫入、讀取與抹除等運作。

【0041】 可複寫式非揮發性記憶體模組 106 是耦接至記憶體控制電路單元 104，並且用以儲存主機系統 1000 所寫入之資料。可複寫式非揮發性記憶體模組 106 具有實體抹除單元 410(0)~410(N)。例如，實體抹除單元 410(0)~410(N)可屬於同一個記憶體晶粒(die)或者屬於不同的記憶體晶粒。每一實體抹除單元分別具有複數個實體程式化單元，並且屬於同一個實體抹除單元之實體程式化單元可被獨立地寫入且被同時地抹除。例如，每一實體抹除單元是由 128 個實體程式化單元所組成。然而，必須瞭解的是，本揭露不限於此，每一實體抹除單元是可由 64 個實體程式化單元、256 個實體程式化單元或其他任意個實體程式化單元所組成。

【0042】 更具體來說，每一個實體抹除單元包括多條字元線與多條位元線，每一條字元線與每一條位元線交叉處配置有一個記憶胞。每一個記憶胞可儲存一或多個位元。在同一個實體抹除單元中，所有的記憶胞會一起被抹除。在此範例實施例中，實體抹除單元為抹除之最小單位。亦即，每一實體抹除單元含有最小數目之一併被抹除之記憶胞。例如，實體抹除單元為實體區塊。另一方面，同一個字元線上的記憶胞會組成一或多個實體程式化單元。若每一個記憶胞可儲存 2 個以上的位元，則同一個字元線上的實體程式化單元可被分類為下實體程式化單元與上實體程式化

單元。一般來說，下實體程式化單元的寫入速度會大於上實體程式化單元的寫入速度。在此範例實施例中，實體程式化單元為程式化的最小單元。即，實體程式化單元為寫入資料的最小單元。例如，實體程式化單元為實體頁面或是實體扇(sector)。若實體程式化單元為實體頁面，則每一個實體程式化單元通常包括資料位元區與冗餘位元區。資料位元區包含多個實體扇，用以儲存使用者的資料，而冗餘位元區用以儲存系統的資料（例如，錯誤更正碼）。在本範例實施例中，每一個資料位元區包含 32 個實體扇，且一個實體扇的大小為 512 位元組(byte, B)。然而，在其他範例實施例中，資料位元區中也可包含 8 個、16 個或數目更多或更少的實體扇，本揭露並不限制實體扇的大小以及個數。

【0043】 在本範例實施例中，可複寫式非揮發性記憶體模組 106 為多階記憶胞(Multi Level Cell, MLC)NAND 型快閃記憶體模組，即一個記憶胞中可儲存至少 2 個位元。然而，本揭露不限於此，可複寫式非揮發性記憶體模組 106 亦可是單階記憶胞(Single Level Cell, SLC)NAND 型快閃記憶體模組、複數階記憶胞(Trinary Level Cell, TLC) NAND 型快閃記憶體模組、其他快閃記憶體模組或其他具有相同特性的記憶體模組。

【0044】 無線通訊介面 108 耦接至記憶體控制電路單元 104 並且具有短距離無線通訊功能。無線通訊介面 108 可以是支援藍芽(Bluetooth)、無線相容性認證(Wireless Fidelity, WiFi)、近場通訊(Near Field Communication, NFC)、無線射頻識別(Radio Frequency

Identification, RFID)等短距離無線通訊功能的通訊晶片。

【0045】 圖 5 是根據本揭露一範例實施例所繪示的記憶體控制電路單元的概要方塊圖。

【0046】 請參照圖 5，記憶體控制電路單元 104 包括記憶體管理電路 202、主機介面 204 及記憶體介面 206。

【0047】 記憶體管理電路 202 用以控制記憶體控制電路單元 104 的整體運作。具體來說，記憶體管理電路 202 具有多個控制指令，並且在記憶體儲存裝置 100 運作時，這些控制指令會被執行以進行資料的寫入、讀取與抹除等運作。以下說明記憶體管理電路 202 的操作時，等同於說明記憶體控制電路單元 104 的操作，以下並不再贅述。

【0048】 在一範例實施例中，記憶體管理電路 202 的控制指令是以韌體型式來實作。例如，記憶體管理電路 202 具有微處理器單元(未繪示)、唯讀記憶體(未繪示)及隨機存取記憶體(未繪示)，並且這些控制指令是被燒錄至此唯讀記憶體中。當記憶體儲存裝置 100 運作時，這些控制指令會由微處理器單元來執行以進行資料的寫入、讀取與抹除等運作。

【0049】 在另一範例實施例中，記憶體管理電路 202 的控制指令亦可以程式碼型式儲存於可複寫式非揮發性記憶體模組 106 的特定區域(例如，可複寫式非揮發性記憶體模組中專用於存放系統資料的系統區)中。此外，記憶體管理電路 202 具有微處理器單元(未繪示)、唯讀記憶體(未繪示)及隨機存取記憶體(未繪示)。特別是，

此唯讀記憶體具有開機碼(boot code)，並且當記憶體控制電路單元 104 被致能時，微處理器單元會先執行此開機碼來將儲存於可複寫式非揮發性記憶體模組 106 中之控制指令載入至記憶體管理電路 202 的隨機存取記憶體中。之後，微處理器單元會運轉此些控制指令以進行資料的寫入、讀取與抹除等運作。

【0050】 此外，在另一範例實施例中，記憶體管理電路 202 的控制指令亦可以一硬體型式來實作。例如，記憶體管理電路 202 包括微控制器、記憶體管理單元、記憶體寫入單元、記憶體讀取單元、記憶體抹除單元與資料處理單元。記憶體管理單元、記憶體寫入單元、記憶體讀取單元、記憶體抹除單元與資料處理單元是耦接至微控制器。其中，記憶體管理單元用以管理可複寫式非揮發性記憶體模組 106 的實體抹除單元；記憶體寫入單元用以對可複寫式非揮發性記憶體模組 106 下達寫入指令以將資料寫入至可複寫式非揮發性記憶體模組 106 中；記憶體讀取單元用以對可複寫式非揮發性記憶體模組 106 下達讀取指令以從可複寫式非揮發性記憶體模組 106 中讀取資料；記憶體抹除單元用以對可複寫式非揮發性記憶體模組 106 下達抹除指令以將資料從可複寫式非揮發性記憶體模組 106 中抹除；而資料處理單元用以處理欲寫入至可複寫式非揮發性記憶體模組 106 的資料以及從可複寫式非揮發性記憶體模組 106 中讀取的資料。

【0051】 主機介面 204 是耦接至記憶體管理電路 202 並且用以接收與識別主機系統 1000 所傳送的指令與資料。也就是說，主機系

統 1000 所傳送的指令與資料會透過主機介面 204 來傳送至記憶體管理電路 202。在本範例實施例中，主機介面 204 是相容於 USB 標準。然而，必須瞭解的是本揭露不限於此，主機介面 204 亦可以是相容於 PATA 標準、IEEE 1394 標準、PCI Express 標準、SATA 標準、SD 標準、UHS-I 標準、UHS-II 標準、MS 標準、MMC 標準、eMMC 標準、UFS 標準、CF 標準、IDE 標準或其他適合的資料傳輸標準。

【0052】 記憶體介面 206 是耦接至記憶體管理電路 202 並且用以存取可複寫式非揮發性記憶體模組 106。也就是說，欲寫入至可複寫式非揮發性記憶體模組 106 的資料會經由記憶體介面 206 轉換為可複寫式非揮發性記憶體模組 106 所能接受的格式。

【0053】 緩衝記憶體 252 是耦接至記憶體管理電路 202 並且用以暫存來自於主機系統 1000 的資料與指令或來自於可複寫式非揮發性記憶體模組 106 的資料。

【0054】 在一範例實施例中，記憶體管理電路 202 會透過無線通訊介面 108 與電子裝置 2000(例如，使用者的手機)建立安全通道。例如，在無線通訊介面 108 是支援藍芽規範的例子中，此安全通道可藉由無線通訊介面 108 傳輸藍芽配對密碼並經由電子裝置 2000 確認後而建立。

【0055】 記憶體管理電路 202 還可透過無線通訊介面 108 從建立於藍芽通訊的安全通道取得識別碼。在此，識別碼可為使用者識別碼、使用者密碼、手機識別碼或手機密碼等的其中之一或其組

合，並可由使用者透過電子裝置 2000 自行輸入，但本揭露並不以此為限。識別碼也可以是透過電子裝置 2000 上的應用程式自動輸入。

【0056】 當記憶體管理電路 202 取得識別碼時，記憶體管理電路 202 可使用識別碼來獲取加解密金鑰，並且將加解密金鑰儲存於緩衝記憶體 252 中。詳細來說，可複寫式非揮發性記憶體模組 106 中會儲存個人識別碼訊息摘要(personal identification number message digest)及密鑰(encrypted key)。記憶體管理電路 202 具有一單向雜湊函數，並可利用此單向雜湊函數計算出對應上述識別碼的訊息摘要(message digest)。在本範例實施例中，上述單向雜湊函數是利用 SHA-256 來被實作在記憶體管理電路 202 中。然而，本揭露並不以此為限。在本揭露另一範例實施例中，記憶體管理電路 202 中的單向雜湊函數亦可以由 MD5、RIPEMD-160、SHA1、SHA-386、SHA-512 或其他適合的函數來實作。之後，記憶體管理電路 202 會將所計算出的訊息摘要與可複寫式非揮發性記憶體模組 106 中所儲存的個人識別碼訊息摘要進行比對，若所計算出的訊息摘要與可複寫式非揮發性記憶體模組 106 中所儲存的個人識別碼訊息摘要相符時，則記憶體管理電路 202 會根據此識別碼，使用加解密函數解碼密鑰以獲得加解密金鑰。在記憶體管理電路 202 獲得加解密金鑰之後，便可利用加解密金鑰解碼從可複寫式非揮發性記憶體模組 106 中讀取的資料。類似地，在記憶體管理電路 202 獲得加解密金鑰之後，便可利用加解密金鑰加密欲寫入可

複寫式非揮發性記憶體模組 106 中資料。

【0057】 在本範例實施例中，記憶體管理電路 202 中的加解密函數是以高級加密標準(Advanced Encryption Standard, AES)128 來實作，然而，本揭露並不以此為限。在本揭露另一範例實施例中亦可使用 AES256 或資料加密標準(Data Encryption Standard, DES) 來實作記憶體管理電路 202 中的加解密函數。

【0058】 值得一提的是，儲存在可複寫式非揮發性記憶體模組 106 中的個人識別碼訊息摘要是藉由此記憶體儲存裝置 100 的使用者設定個人識別碼，並且利用上述單向雜湊函數所產生。例如，在此記憶體儲存裝置 100 出廠時會由製造商預存一組個人識別碼訊息摘要，並且製造商會將此個人識別碼訊息摘要對應的個人識別碼提供給使用者。之後，使用者可使用製造商所提供的個人識別碼成功地通過記憶體儲存裝置 100 的驗證。此外，當使用者重新設定一組新個人識別碼時，記憶體管理電路 202 會根據使用者的新個人識別碼以單向雜湊函數來重新計算一組新個人識別碼訊息摘要，並且將新個人識別碼訊息摘要儲存在可複寫式非揮發性記憶體模組 106 中以取代原始的個人識別碼訊息摘要。之後，記憶體管理電路 202 會使用最新的個人識別碼訊息摘要來驗證使用者所輸入的識別碼。

【0059】 另外，加解密金鑰會在記憶體儲存裝置 100 出廠時，透過一亂數產生器(未繪示)以一隨機方式產生。特別是，記憶體管理電路 202 會依據個人識別碼使用加解密函數來加密此加解密金

鑰，並且將加密此加解密金鑰所獲得的密鑰儲存於記憶體儲存裝置 100 中。因此，當識別碼通過上述驗證時，此識別碼即可正確地解碼儲存在記憶體儲存裝置 100 中的密鑰，而獲取此加解密金鑰。

【0060】 在本範例實施例中，在記憶體管理電路 202 透過無線通訊介面 108 與電子裝置 2000 建立安全通道之後，記憶體儲存裝置 100 可每隔一段預定時間，例如 5 秒，發送一個輪詢(polling)訊號給電子裝置 2000，當電子裝置 2000 收到輪詢訊號時，則會回傳一個確認(ack)訊號給記憶體儲存裝置 100，以確認電子裝置 2000 與記憶體儲存裝置 100 的無線連線狀況。只要記憶體儲存裝置 100 在此環境中定期接收到電子裝置 2000 回應輪詢訊號的確認訊號，記憶體管理電路 202 便可利用加解密金鑰來存取可複寫式非揮發性記憶體模組 106。

【0061】 反之，當記憶體儲存裝置 100 離開此環境時，若記憶體儲存裝置 100 在一預定時間都沒收到電子裝置 2000 回應輪詢訊號的確認訊號，記憶體管理電路 202 會清除緩衝記憶體 252 中的加解密金鑰並且將記憶體儲存裝置 100 設定為無媒體狀態。具體來說，當記憶體儲存裝置 100 被設定為無媒體狀態時，若記憶體管理電路 202 接收到主機系統 1000 所傳送的存取訊號，記憶體管理電路 202 會回應一個無媒體訊號給主機系統 1000，使得主機系統 1000 無法識別或存取記憶體儲存裝置 100，也就是說，主機系統 1000 的作業系統會判斷記憶體儲存裝置 100 處於中斷連結的狀

態。如此一來，他人難以取得可複寫式非揮發性記憶體模組 106 中的資料，即使取得了其中資料，由於加解密金鑰已從緩衝記憶體 252 中刪除，因此他人也無法解碼可複寫式非揮發性記憶體模組 106 中經過加密的資料。

【0062】 雖然以上說明了透過使用者從電子裝置 2000 輸入識別碼，並經由藍芽無線通訊網路傳送識別碼以確保記憶體儲存裝置 100 的安全性，但本揭露並不以此為限。在另一範例實施例中，記憶體儲存裝置 100 可利用儲存於其中的個人識別碼訊息摘要登錄一個存取點(AP)的 Wi-Fi 無線通訊網路環境，在本實施例中，電子裝置 2000 可為連接到存取點的伺服器。在記憶體儲存裝置 100 以個人識別碼訊息摘要登錄 Wi-Fi 之後，伺服器可搜尋對應個人識別碼訊息摘要的一識別碼，並將該識別碼透過存取點傳送給記憶體儲存裝置 100。記憶體儲存裝置 100 接收識別碼並以單項雜湊函數產生對應識別碼的訊息摘要。若此訊息摘要相同於儲存在記憶體儲存裝置 100 個人識別碼訊息摘要，則此識別碼即可正確地解碼儲存在記憶體儲存裝置 100 中的密鑰，從而獲取加解密金鑰。因此，使用者可透過加解密金鑰存取記憶體儲存裝置 100。

【0063】 在又一範例實施例中，記憶體儲存裝置 100 可利用預設的登錄碼登錄存取點。在此，電子裝置 2000 可為連接到存取點的伺服器。在記憶體儲存裝置 100 成功登錄存取點並建立 Wi-Fi 網路連線之後，使用者可直接在存取點利用輸入裝置輸入識別碼，使得識別碼藉由存取點傳送到記憶體儲存裝置 100。接著，記憶體

儲存裝置 100 可接收識別碼並以單項雜湊函數產生對應識別碼的訊息摘要。若此訊息摘要相同於儲存在記憶體儲存裝置 100 個人識別碼訊息摘要，則此識別碼即可正確地解碼儲存在記憶體儲存裝置 100 中的密鑰，從而獲取加解密金鑰。因此，使用者可透過加解密金鑰存取記憶體儲存裝置 100。

【0064】 值得注意的是，當記憶體儲存裝置 100 進入上述 Wi-Fi 無線通訊網路環境時，可同時從電子裝置 2000 取得一把資料傳輸金鑰，以對此無線通訊網路環境中傳輸或接收的資料進行加密或解密。舉例來說，當記憶體儲存裝置 100 成功登錄上述 Wi-Fi 無線通訊網路環境時，記憶體儲存裝置 100 可從電子裝置 2000 接收一把資料傳輸金鑰並將其儲存於緩衝記憶體 252 中。電子裝置 2000 在傳輸識別碼之前會先利用資料傳輸金鑰加密。當記憶體儲存裝置 100 接收到電子裝置 2000 在 Wi-Fi 環境中傳送的資料，也就是經由資料傳輸金鑰所加密的識別碼時，記憶體儲存裝置 100 可利用緩衝記憶體 252 中的資料傳輸金鑰解密資料以取得識別碼。

【0065】 在本揭露一範例實施例中，記憶體控制電路單元 104 還包括電源管理電路 254 與錯誤檢查與校正電路 256。

【0066】 電源管理電路 254 是耦接至記憶體管理電路 202 並且用以控制記憶體儲存裝置 100 的電源。

【0067】 錯誤檢查與校正電路 256 是耦接至記憶體管理電路 202 並且用以執行錯誤檢查與校正程序以確保資料的正確性。具體來說，當記憶體管理電路 202 從主機系統 1000 中接收到寫入指令

時，錯誤檢查與校正電路 256 會為對應此寫入指令的資料產生對應的錯誤更正碼(Error Correcting Code, ECC)，並且記憶體管理電路 202 會將對應此寫入指令的資料與對應的錯誤更正碼寫入至可複寫式非揮發性記憶體模組 106 中。之後，當記憶體管理電路 202 從可複寫式非揮發性記憶體模組 106 中讀取資料時會同時讀取此資料對應的錯誤更正碼，並且錯誤檢查與校正電路 256 會依據此錯誤更正碼對所讀取的資料執行錯誤檢查與校正程序。

【0068】 圖 6 是根據本揭露一範例實施例所繪示的資料保護方法的流程圖。

【0069】 請參照圖 6，在步驟 S602 中，記憶體管理電路 202 會透過無線通訊介面 108 與電子裝置 2000 建立安全通道，此安全通道可藉由無線通訊介面 108 傳輸無線網路配對識別碼並經由電子裝置 2000 確認後而建立。

【0070】 在建立記憶體儲存裝置 100 與電子裝置之間的安全通道之後，進入步驟 S604 中，記憶體管理電路 202 透過無線通訊介面 108 從安全通道取得識別碼。在此，識別碼可以是使用者透過電子裝置 2000 自行輸入或是透過電子裝置 2000 上的應用程式自動輸入。

【0071】 在步驟 S606 中，記憶體管理電路 202 使用識別碼來獲取加解密金鑰，並將加解密金鑰儲存於緩衝記憶體 252 中。

【0072】 在記憶體管理電路 202 獲取加解密金鑰之後，會進入步驟 S608，使用加解密金鑰與加解密函數來存取可複寫式非揮發性

記憶體模組 106 中的資料。詳細來說，當使用者欲寫入資料到可複寫式非揮發性記憶體模組 106 時，記憶體管理電路 202 可根據加解密金鑰使用高級加密標準(AES)對寫入資料加密，接著再將加密過的資料寫入可複寫式非揮發性記憶體模組 106。同理，當使用者欲從可複寫式非揮發性記憶體模組 106 讀取資料時，記憶體管理電路 202 可根據加解密金鑰使用高級加密標準(AES)對資料解密，接著再讀取解密後的資料。值得注意的是，使用者除了透過 USB 或 SATA 等有線介面存取可複寫式非揮發性記憶體模組 106 中的資料，使用者還可透過無線通訊介面 108，從遠端藉由無線網路來存取可複寫式非揮發性記憶體模組 106 中的資料。

【0073】 在記憶體管理電路 202 會透過無線通訊介面 108 與電子裝置 2000 建立安全通道之後，電子裝置 2000 會經由回應記憶體儲存裝置 100 的輪詢訊號發送一個確認訊號到記憶體儲存裝置 100，以確認電子裝置 2000 與記憶體儲存裝置 100 的無線連線狀況。在步驟 S610 中，無線通訊介面 108 會偵測是否從建立於無線通訊網路上的安全通道接收到來自於電子裝置 2000 的確認訊號。若無線通訊介面 108 偵測到確認訊號，則回到步驟 S608，繼續存取可複寫式非揮發性記憶體模組 106 中的資料。

【0074】 倘若記憶體儲存裝置 100 的無線通訊介面 108 超過一預定時間內，例如 10 秒，沒有收到電子裝置 2000 所傳送の確認訊號時，代表此電子裝置 2000 已經不在無線通訊介面 108 短距離通訊的範圍之內，則在步驟 S612 中，記憶體管理電路 202 會清除緩

衝記憶體 252 中的加解密金鑰，並且將記憶體儲存裝置 100 設定為無媒體狀態。具體來說，當記憶體儲存裝置 100 被設定為無媒體狀態時，若記憶體管理電路 202 接收到主機系統 1000 所傳送的存取訊號，記憶體管理電路 202 會回應一個無媒體訊號給主機系統 1000，使得主機系統 1000 無法識別或存取記憶體儲存裝置 100，也就是說，主機系統 1000 的作業系統會判斷記憶體儲存裝置 100 處於中斷連結的狀態。如此一來，他人便難以取得可複寫式非揮發性記憶體模組 106 中的資料，即使取得了其中資料，由於加解密金鑰已從緩衝記憶體 252 中刪除，他人也無法解碼可複寫式非揮發性記憶體模組 106 中經過加密的資料。

【0075】圖 7 是根據本揭露另一範例實施例所繪示的資料保護方法的流程圖。

【0076】請參照圖 7，在步驟 S702 中，記憶體管理電路 202 會透過無線通訊介面 108 與電子裝置 2000 建立安全通道，此安全通道可藉由無線通訊介面 108 傳輸無線網路配對密碼並經由電子裝置 2000 確認後而建立。

【0077】在建立記憶體儲存裝置 100 與電子裝置之間的安全通道之後，在步驟 S704 中，記憶體管理電路 202 透過無線通訊介面 108 從安全通道取得識別碼。在此，識別碼可以是使用者透過電子裝置 2000 自行輸入或是透過電子裝置 2000 上的應用程式自動輸入。

【0078】在步驟 S706 中，記憶體管理電路 202 會利用雜湊函數對接收到的識別碼作運算以產生對應的訊息摘要，接著在步驟 S708

中，記憶體管理電路 202 會判斷上述訊息摘要與個人識別訊息摘要是否相符。在此，個人識別碼訊息摘要及密鑰是預先儲存在可複寫式非揮發性記憶體模組 106 中，其中個人識別碼訊息摘要是初始地藉由單向雜湊函數依據個人識別碼產生，而密鑰是初始地依據個人識別碼，使用例如高級加密標準或資料加密標準等加解密函數，加密由隨機方式產生的加解密金鑰而產生。

【0079】 若記憶體管理電路 202 判斷上述訊息摘要與個人識別訊息摘要不相符時，則回到步驟 S704，以再一次從電子裝置 2000 取得識別碼。若記憶體管理電路 202 判斷上述訊息摘要與個人識別訊息摘要相符時，則在步驟 S710 中，記憶體管理電路 202 依據識別碼使用加解密函數解碼密文以獲得加解密金鑰，並將加解密金鑰儲存於緩衝記憶體 252 中。

【0080】 獲得加解密金鑰之後，在步驟 S712 中，記憶體管理電路 202 使用加解密金鑰與加解密函數來存取可複寫式非揮發性記憶體模組 106 中的資料。由於使用加解密金鑰與加解密函數來存取可複寫式非揮發性記憶體模組 106 中的資料的過程已於第 6 圖中說明過，因此不在贅述。

【0081】 在記憶體管理電路 202 透過無線通訊介面 108 與電子裝置 2000 建立安全通道之後，電子裝置 2000 會經由回應記憶體儲存裝置 100 的輪詢訊號發送一個確認訊號到記憶體儲存裝置 100，以確認電子裝置 2000 與記憶體儲存裝置 100 的無線連線狀況。在步驟 S714 中，無線通訊介面 108 會偵測是否從建立於無線

通訊網路上的安全通道接收到來自於電子裝置 2000 的確認訊號。若無線通訊介面 108 偵測到確認訊號時，則回到步驟 S712，以繼續存取可複寫式非揮發性記憶體模組 106 中的資料。

【0082】 倘若記憶體儲存裝置 100 的無線通訊介面 108 超過一預定時間內，例如 10 秒，沒有收到電子裝置 2000 所傳送的確認訊號時，代表此電子裝置 2000 已經不在無線通訊介面 108 短距離無線通訊網路的範圍之內，則在步驟 S716 中，記憶體管理電路 202 會清除緩衝記憶體 252 中的加解密金鑰並將記憶體儲存裝置 100 設定為無媒體狀態。具體來說，當記憶體儲存裝置 100 被設定為無媒體狀態時，若記憶體管理電路 202 接收到主機系統 1000 所傳送的存取訊號，記憶體管理電路 202 會回應一個無媒體訊號給主機系統 1000，使得主機系統 1000 無法識別或存取記憶體儲存裝置 100，也就是說，主機系統 1000 的作業系統會判斷記憶體儲存裝置 100 處於中斷連結的狀態。如此一來，他人便難以取得可複寫式非揮發性記憶體模組 106 中的資料，即使取得了其中資料，由於加解密金鑰已從緩衝記憶體 252 中刪除，他人也無法解碼可複寫式非揮發性記憶體模組 106 中經過加密的資料，從而達到保護儲存裝置中的資料的效果。

【0083】 綜上所述，本揭露範例實施例的資料保護方法、記憶體控制電路單元及記憶體儲存裝置，建立記憶體儲存裝置與電子裝置之間的安全通道，且利用電子裝置透過無線網路傳送的識別碼獲得加解密金鑰以存取可複寫式非揮發性記憶體模組。當一定時

間內沒有收到來自電子裝置的確認訊號時，記憶體儲存裝置判斷其已經不在電子裝置的短距離無線通訊網路的範圍之內，並刪除緩衝記憶體中的加解密金鑰。如此一來，記憶體儲存裝置一旦遠離使用者的手持電子裝置或不在特定的無線網路環境內就無法運作。即使記憶體儲存裝置被他人持有，也因為加解密金鑰已被刪除，而無法解碼可複寫式非揮發性記憶體模組中經過加密的資料，從而確保記憶體儲存裝置中資料的安全性。

● **【0084】** 雖然本揭露已以實施例揭露如上，然其並非用以限定本揭露，任何所屬技術領域中具有通常知識者，在不脫離本揭露的精神和範圍內，當可作些許的更動與潤飾，故本揭露的保護範圍當視後附的申請專利範圍所界定者為準。

【符號說明】

【0085】

- 1000：主機系統
- 1100：電腦
- 1102：微處理器
- 1104：隨機存取記憶體
- 1106：輸入/輸出裝置
- 1108：系統匯流排
- 1110：資料傳輸介面
- 1202：滑鼠

- 1204：鍵盤
- 1206：顯示器
- 1208：印表機
- 1212：隨身碟
- 1214：記憶卡
- 1216：固態硬碟
- 1310：數位相機
- 1312：SD 卡
- 1314：MMC 卡
- 1316：記憶棒
- 1318：CF 卡
- 1320：嵌入式儲存裝置
- 2000：電子裝置
- 100：記憶體儲存裝置
- 102：連接介面單元
- 104：記憶體控制電路單元
- 106：可複寫式非揮發性記憶體模組
- 108：無線通訊介面
- 410(0)~410(N)：實體抹除單元
- 202：記憶體管理電路
- 204：主機介面
- 206：記憶體介面

252：緩衝記憶體

254：電源管理電路

256：錯誤檢查與校正電路

S602、S604、S606、S608、S610、S612、S702、S704、S706、

S708、S710、S712、S714、S716：資料保護方法的步驟

申請專利範圍

1. 一種資料保護方法，用於保護一記憶體儲存裝置中一可複寫式非揮發性記憶體模組的資料，該資料保護方法包括：

透過一無線通訊網路與一電子裝置建立一安全通道；

透過建立於該無線通訊網路上的該安全通道取得一識別碼；

使用該識別碼來獲取一加解密金鑰並且將該加解密金鑰儲存於一緩衝記憶體中；

使用該加解密金鑰解碼從該可複寫式非揮發性記憶體模組中讀取的資料，其中該可複寫式非揮發性記憶體模組的資料以該加解密金鑰來被加密；

偵測是否從建立於該無線通訊網路上的該安全通道接收到來自於該電子裝置的一確認訊號；以及

倘若在一預定時間內未接收到來自於該電子裝置的該確認訊號，清除儲存於該緩衝記憶體中的該加解密金鑰。

2. 如申請專利範圍第 1 項所述的資料保護方法，更包括：

在清除儲存於該緩衝記憶體中的該加解密金鑰之後，將該記憶體儲存裝置設定為無媒體狀態。

3. 如申請專利範圍第 1 項所述的資料保護方法，其中透過建立於該無線通訊網路上的該安全通道取得該識別碼的步驟包括：

透過建立於該無線通訊網路上的該安全通道取得從該電子裝置輸入的該識別碼，其中該電子裝置為一手持電子裝置。

4. 如申請專利範圍第 1 項所述的資料保護方法，其中透過建

立於該無線通訊網路上的該安全通道取得該識別碼的步驟包括：

透過建立於該無線通訊網路上的該安全通道取得該電子裝置產生的該識別碼，其中該電子裝置為一伺服器並耦接至一無線網路存取點。

5. 如申請專利範圍第 1 項所述的資料保護方法，其中該無線通訊網路為一藍芽網路、一無線相容性認證網路、一近場通訊網路或一無線射頻識別網路。

6. 如申請專利範圍第 1 項所述的資料保護方法，其中使用該識別碼來獲取該加解密金鑰並且將該加解密金鑰儲存於該緩衝記憶體中的步驟包括：

在該可複寫式非揮發性記憶體模組中儲存一個人識別碼訊息摘要及一密鑰；

使用一單向雜湊函數產生對應該識別碼的一訊息摘要；以及
判斷該訊息摘要與該個人識別碼訊息摘要是否相符，其中當該訊息摘要及該個人識別碼訊息摘要相符時，依據該識別碼使用一加解密函數解碼該密鑰以獲得該加解密金鑰。

7. 如申請專利範圍第 6 項所述的資料保護方法，更包括：

初始地藉由該單向雜湊函數依據一個人識別碼產生該個人識別碼訊息摘要；以及

初始地依據該個人識別碼使用該加解密函數加密該加解密金鑰以產生該密鑰。

8. 如申請專利範圍第 7 項所述的資料保護方法，其中初始地

依據該個人識別碼使用該加解密函數加密該加解密金鑰以產生該密鑰的步驟更包括：

初始地以一隨機方式產生該加解密金鑰。

9. 如申請專利範圍第 1 項所述的資料保護方法，其中使用該加解密金鑰解碼從該可複寫式非揮發性記憶體模組中讀取的資料的步驟包括：

依據該加解密金鑰使用一加解密函數解碼從該可複寫式非揮發性記憶體模組中讀取的資料，其中該可複寫式非揮發性記憶體模組的資料依據該加解密金鑰使用該加解密函數被加密。

10. 一種記憶體控制電路單元，用於控制一可複寫式非揮發性記憶體模組，該記憶體控制電路單元包括：

一主機介面，耦接至一主機系統；

一記憶體介面，耦接至該可複寫式非揮發性記憶體模組；以及

一記憶體管理電路，耦接至該主機介面及該記憶體介面；

其中該記憶體控制電路單元透過一無線通訊介面以一無線通訊網路與一電子裝置建立一安全通道，

其中該無線通訊介面透過建立於該無線通訊網路上的該安全通道取得一識別碼，

其中該記憶體管理電路使用該識別碼來獲取一加解密金鑰並且將該加解密金鑰儲存於一緩衝記憶體中，

其中該記憶體管理電路使用該加解密金鑰解碼從該可複寫式

非揮發性記憶體模組中讀取的資料，其中該可複寫式非揮發性記憶體模組的資料以該加解密金鑰來被加密，

其中該無線通訊介面偵測是否從建立於該無線通訊網路上的該安全通道接收到來自於該電子裝置的一確認訊號，

其中，倘若該無線通訊介面在一預定時間內未接收到來自於該電子裝置的該確認訊號，該記憶體管理電路清除儲存於該緩衝記憶體中的該加解密金鑰。

11. 如申請專利範圍第 10 項所述的記憶體控制電路單元，其中在該記憶體管理電路清除儲存於該緩衝記憶體中的該加解密金鑰之後，當該記憶體管理電路接收到該主機系統的一存取訊號時，該記憶體管理電路傳送一無媒體訊號到該主機系統。

12. 如申請專利範圍第 10 項所述的記憶體控制電路單元，其中該無線通訊網路為一藍芽網路、一無線相容性認證網路、一近場通訊網路或一無線射頻識別網路。

13. 如申請專利範圍第 10 項所述的記憶體控制電路單元，其中該記憶體管理電路在該可複寫式非揮發性記憶體模組中儲存一個人識別碼訊息摘要及一密鑰，

其中該記憶體管理電路使用一單向雜湊函數產生對應該識別碼的一訊息摘要，

其中該記憶體管理電路判斷該訊息摘要與該個人識別碼訊息摘要是否相符，其中當該訊息摘要及該個人識別碼訊息摘要相符時，該記憶體管理電路依據該識別碼使用一加解密函數解碼該密

鑰以獲得該加解密金鑰。

14. 一種記憶體儲存裝置，包括：

一連接介面單元，耦接至一主機系統；

一可複寫式非揮發性記憶體模組；

一記憶體控制電路單元，耦接至該連接介面單元及該可複寫式非揮發性記憶體模組；以及

一無線通訊介面，耦接至該記憶體控制電路單元，

其中該記憶體控制電路單元透過該無線通訊介面以一無線通訊網路與一電子裝置建立一安全通道，

其中該記憶體控制電路單元透過建立於該無線通訊網路上的該安全通道取得一識別碼，

其中該記憶體控制電路單元使用該識別碼來獲取一加解密金鑰並且將該加解密金鑰儲存於一緩衝記憶體中，

其中該記憶體控制電路單元使用該加解密金鑰解碼從該可複寫式非揮發性記憶體模組中讀取的資料，其中該可複寫式非揮發性記憶體模組的資料以該加解密金鑰來被加密，

其中該記憶體控制電路單元偵測是否從建立於該無線通訊網路上的該安全通道接收到來自於該電子裝置的一確認訊號，

其中，倘若該記憶體控制電路單元在一預定時間內未接收到來自於該電子裝置的該確認訊號，該記憶體控制電路單元清除儲存於該緩衝記憶體中的該加解密金鑰。

15. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該

記憶體控制電路單元清除儲存於該緩衝記憶體中的該加解密金鑰之後，當該記憶體控制電路單元接收到該主機系統的一存取訊號時，該記憶體控制電路單元傳送一無媒體訊號到該主機系統。

16. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該記憶體控制電路單元透過建立於該無線通訊網路上的該安全通道取得從該電子裝置輸入的該識別碼，其中該電子裝置為一手持電子裝置。

17. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該記憶體控制電路單元透過建立於該無線通訊網路上的該安全通道取得該電子裝置產生的該識別碼，其中該電子裝置為一伺服器並耦接至一無線網路存取點。

18. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該無線通訊網路為一藍芽網路、一無線相容性認證網路、一近場通訊網路或一無線射頻識別網路。

19. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該記憶體控制電路單元在該可複寫式非揮發性記憶體模組中儲存一個人識別碼訊息摘要及一密鑰，

其中該記憶體控制電路單元使用一單向雜湊函數產生對應該識別碼的一訊息摘要，

其中該記憶體控制電路單元判斷該訊息摘要與該個人識別碼訊息摘要是否相符，其中當該訊息摘要及該個人識別碼訊息摘要相符時，該記憶體控制電路單元依據該識別碼使用一加解密函數

解碼該密鑰以獲得該加解密金鑰。

20. 如申請專利範圍第 19 項所述的記憶體儲存裝置，其中該記憶體控制電路單元初始地藉由該單向雜湊函數依據一個人識別碼產生該個人識別碼訊息摘要，

其中該記憶體控制電路單元初始地依據該個人識別碼使用該加解密函數加密該加解密金鑰以產生該密鑰。

21. 如申請專利範圍第 20 項所述的記憶體儲存裝置，其中該記憶體控制電路單元初始地以一隨機方式產生該加解密金鑰。

22. 如申請專利範圍第 14 項所述的記憶體儲存裝置，其中該記憶體控制電路單元依據該加解密金鑰使用一加解密函數解碼從該可複寫式非揮發性記憶體模組中讀取的資料，其中該可複寫式非揮發性記憶體模組的資料依據該加解密金鑰使用該加解密函數被加密。

圖式

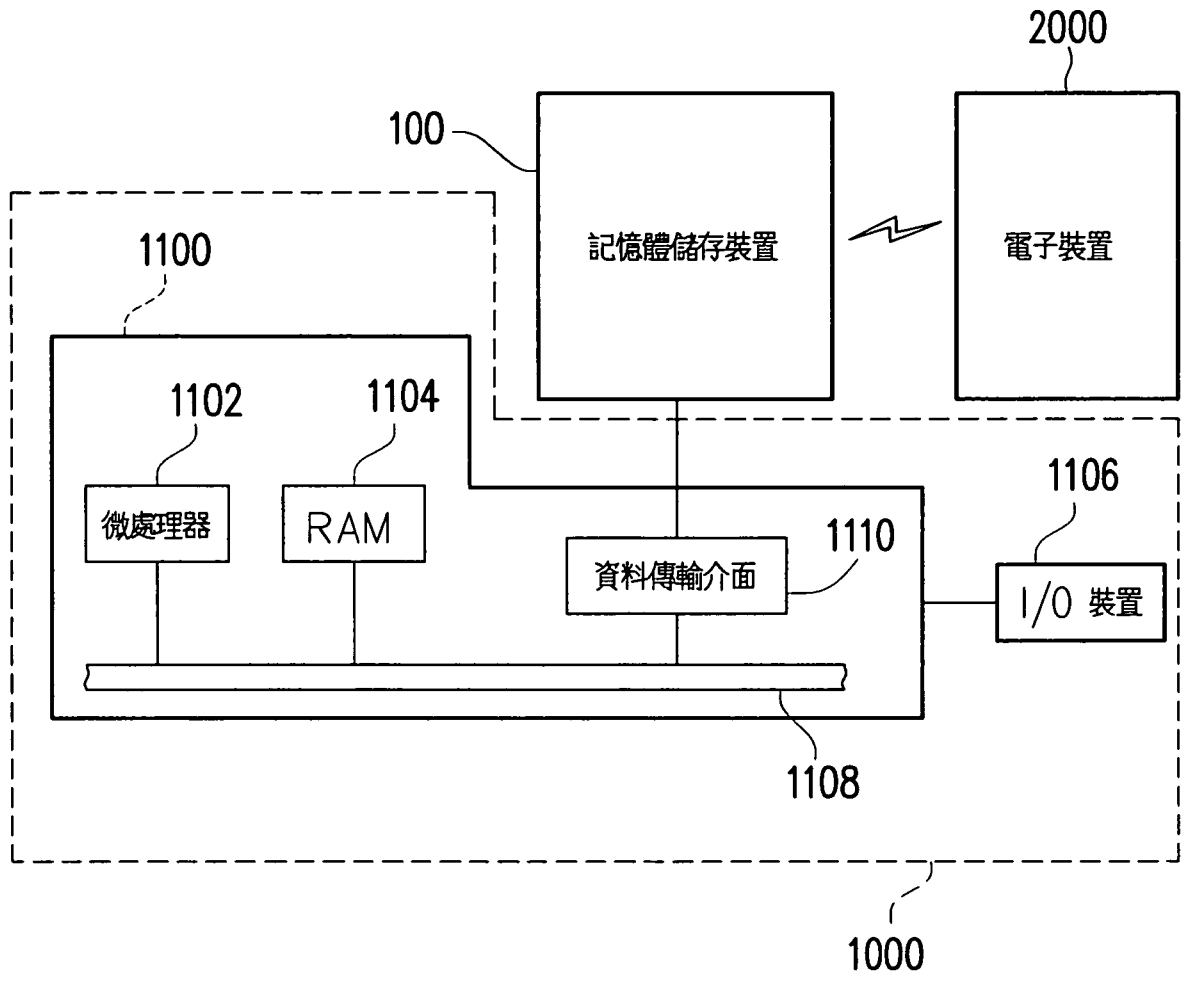


圖 1

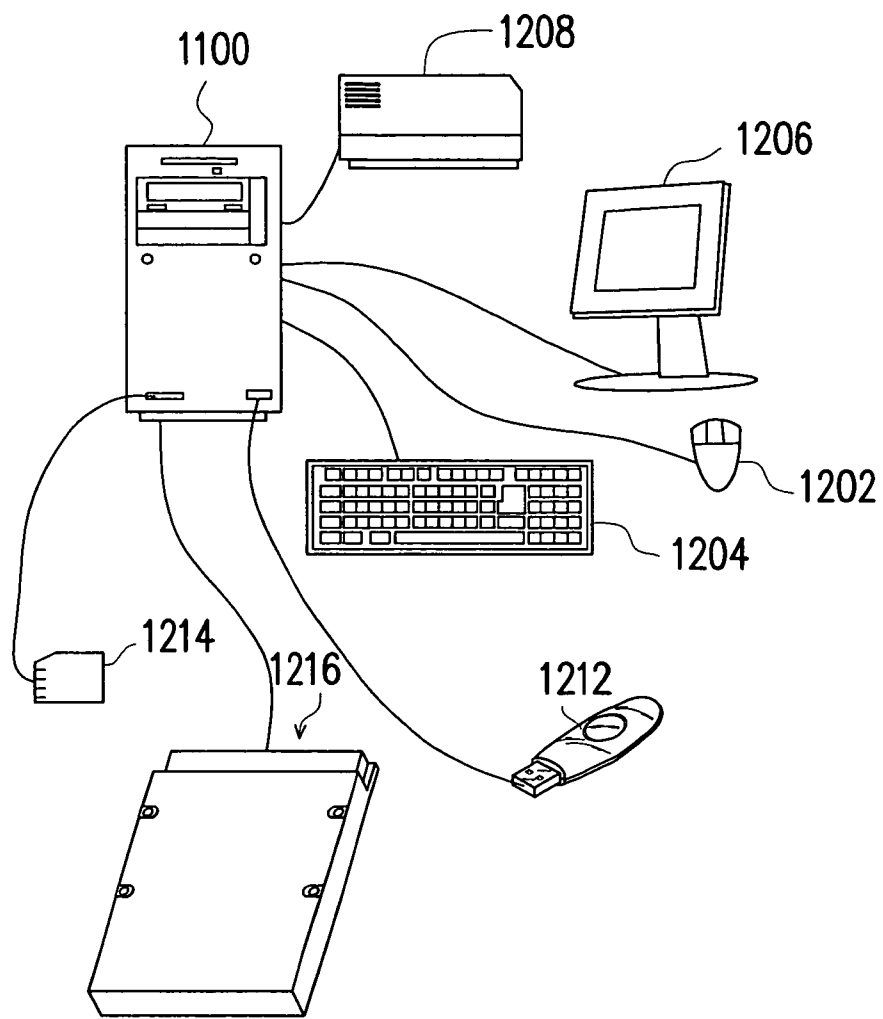


圖 2

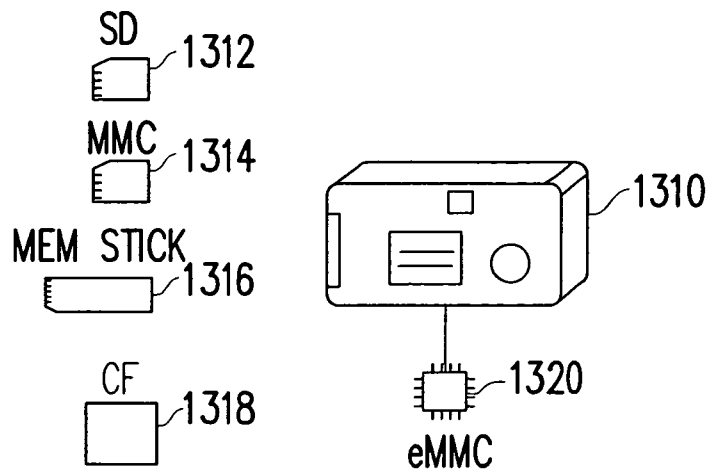


圖 3

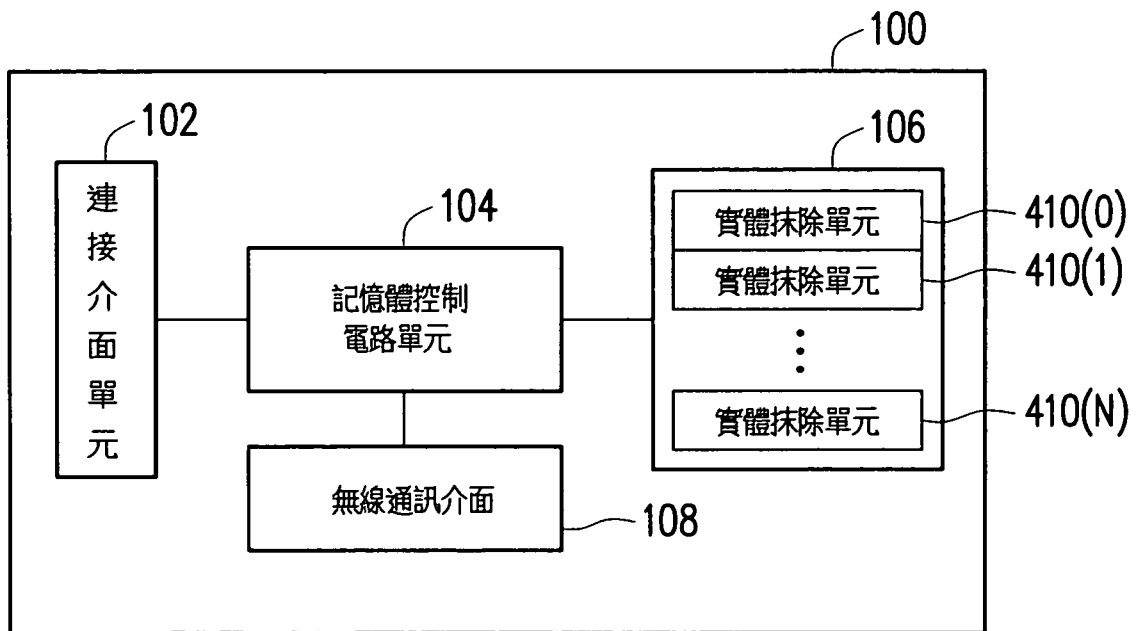


圖 4

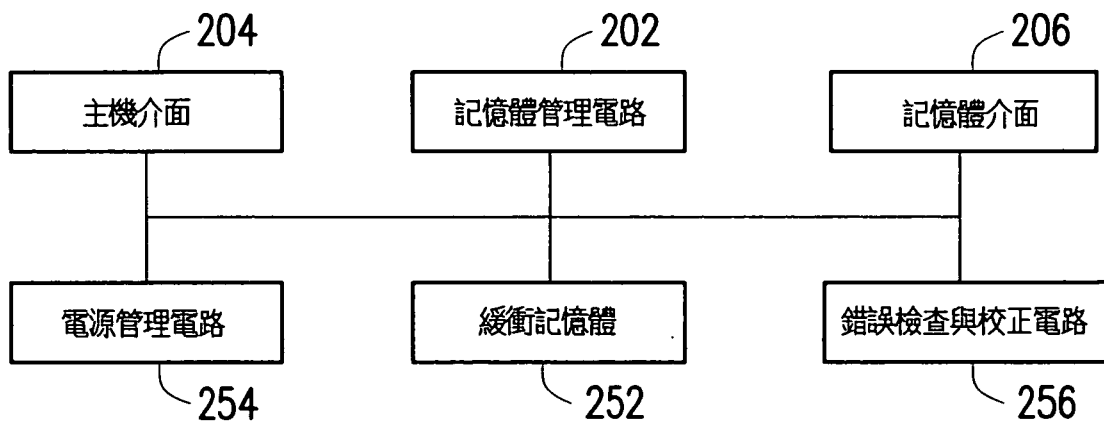


圖 5

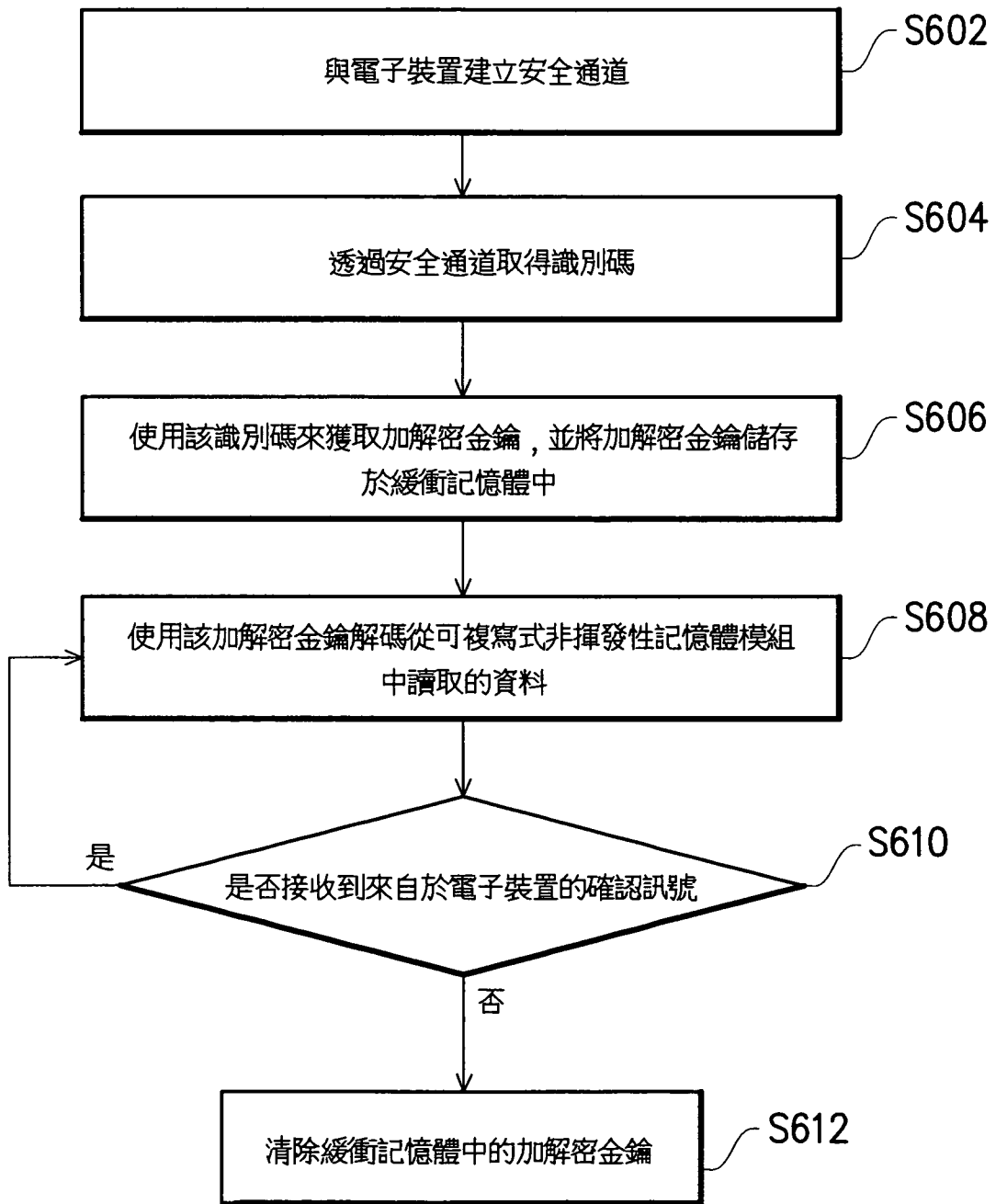


圖 6

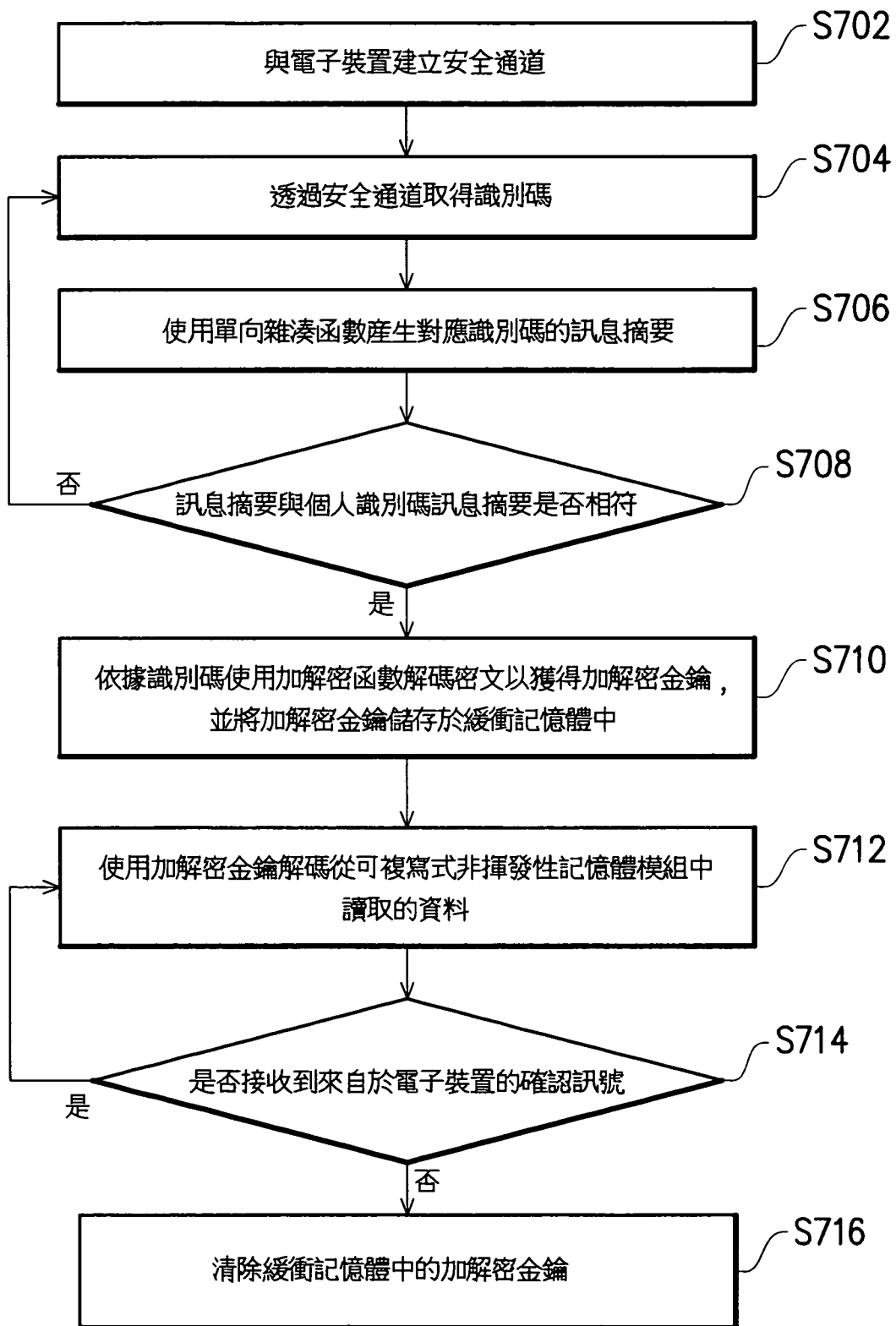


圖 7