200924479

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96144543

※ 申請日期：96.11.23　　※IPC 分類：H04L 9/30 (2006.01)

一、發明名稱：（中文/英文）　　G06F 12/14 (2006.01)

基於記憶體介面的保密裝置通訊機制

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）李殿基

代表人：（中文/英文）

住居所或營業所地址：（中文/英文）

台中縣大肚鄉沙田路 2 段 756 號

國　籍：（中文/英文）　中華民國

三、發明人：（共 1 人）

姓　名：（中文/英文）李殿基

國　籍：（中文/英文）中華民國

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種保密裝置通訊機制，尤指基於記憶體介面的保密裝置通訊機制。

【先前技術】

目前對於保護資料安全性最佳的方式，應該是智慧卡的應用。相較於市面上所廣泛使用的一般塑膠卡片，智慧卡具有許多良好的特性，例如記憶容量大、具邏輯運算與資料控管的能力、高安全性與降低成本等，其中又以高安全性為智慧卡優於其他塑膠磁條卡片的主要原因之一。智慧卡因為具備了包括鑑別卡片真偽、持卡者身分鑑別、資料存取控管以及資料加密等多層安全保護措施，使得高安全性為其重要的特點。

在智慧卡論壇的辭彙解釋中，對於智慧卡有一個正式的定義---智慧卡為具有決策能力記憶體的積體電路卡。在智慧卡內部有一個微電腦CPU以及作業系統，使得它具有執行運算的能力及儲存記憶的功能。智慧卡的外型和一般的信用卡大小一樣，只不過多了一小塊IC晶片，使得原本普通的一小張卡片具有邏輯運算、資料控管的能力。所有對智慧卡的讀取與寫入動作都必須透過專門的智慧卡讀取機(Smart Card Reader)。

在智慧卡內部，可以預先儲存如 DES、RSA、Hash 等演算法的加密軟體或是具有加密功能的硬體電路設備。這些儲存在卡內的軟硬體設備可以用來讓讀卡機與智慧卡之間達到相互認證的功能，即可達到鑑別卡片真偽的目的。

在目前已被提出的整合智慧卡與快閃記憶卡的方案中，舉例來說，中華民國專利公告號第 M288702 號「可辨識使用者身份之可攜式儲存裝置」、中華民國專利公告號第 M318764 號「多功能辨識卡」，大多只是利用智慧卡所提供的驗證功能，進而保護快閃記憶卡的資料。

另外，雖然智慧卡有著上述優越之處，但是相對於快閃記憶卡來說，在現有電子裝置中仍然只有少數具有智慧卡的讀取介面，以至於智慧卡的實際應用上受到了些許阻礙。為了解決這個問題，在中華民國專利公告號第 M288420 號「具智慧卡晶片之多媒體記憶卡」中，特別提出透過記憶卡介面來同時存取快閃記憶卡以及智慧晶片的架構。只是，在這個習知架構中，為了檢查所接收到的寫入命令到是屬於快閃記憶模組 16 或保密裝置模組 14 的，通常需要檢查寫入命令的格式本身到底屬於何種命令，以至於在實作上會顯得過於複雜。

【發明內容】

本發明之主要目的在提供一種基於記憶體介面的保密裝置通訊機制，其利用判斷資料封包的封包頭中是否額外包含有特殊的預定資料，以便決定資料封包轉送給保密裝置模組或快閃記憶體模組，進而達到整合的目的。

基於上述目的，本發明基於記憶體介面的保密裝置通訊機制主要包含記憶體介面、保密裝置模組、快閃記憶體模組、以及電性連接至記憶體介面、保密裝置、以及快閃記憶體模組之控制模組。由於來自記憶體介面的資料封包，在其封包頭中額外包含有特殊的預定資料，這使得控制模組得以在發覺資料封包的封包頭中含有預定資料時，將資料封包轉送給保密裝置模組。若來自記憶體介面的資料封包在其封包頭中沒有額外包含有預定資料時，控制模組將資料封包轉送給快閃記憶體模組。

關於本發明之優點與精神可以藉由以下的發明詳述及所附圖式得到進一步的瞭解。

【實施方式】

請參閱第1圖，第1圖為本發明基於記憶體介面的保密裝置通訊機制之示意圖。如第1圖所示，在本發明基於記憶體介面的保密裝置通訊機制中，主要包含有記憶體介面10、保密裝置模組14、快閃記憶體模組16、以及電性連接至記憶體介面10、保密裝

置模組 14、以及快閃記憶體模組 16 之控制模組 12。這其中，記憶體介面 10 可電性連接至主機端相對介面，例如 SDIO(SD 卡的 I/O 介面)，並接受來自主機端的資料封包。保密裝置模組 14 為智慧卡模組或晶片卡模組或爪哇卡(JAVA card)、用戶識別卡、生物護照及生物身分證。控制模組 12 與保密裝置模組 14 之間的介面可為串列周邊介面(Serial Peripheral Interface, SPI)、通用串列匯流排(Universal Serial Bus, USB)或 ISO 7816。

請參閱第 2 圖，第 2 圖為本發明資料封包之示意圖。如第 2 圖所示，本發明資料封包 20 主要包含了資料頭 20a 與封包本體 20b。封包本體 20b 中則進一步包含了(命令組(commend sets)、資料負荷(data payload))。資料頭 20a 可能會含有預定資料(可為特殊字串或符號)，例如：IO*WRITE*HEADER*。須特別注意的是，為了讓資料封包 20 能夠順利經過記憶體介面 10 被輸入，因此資料封包 20 的格式必須相對於記憶體介面 10。

簡單來講，使用者透過主機端對著本發明基於記憶體介面的保密裝置通訊機制發出資料封包時，控制模組 12 會依據資料封包 20 的封包頭 20a 中是否含有預定資料或是含有特定的預定資料，而決定將資料封包 20 轉送給保密裝置模組 14 或快閃記憶體模組 16，進而達到整合的目的。如此一來，不論是對於快閃記憶模組 16 或保密裝置模組 14 所發出的寫入命令，只須簡單地檢查是否含有預定資料或是含有特定的預定資料，就能簡單地判斷出寫入命

令的目的對象，進而轉送寫入命令至快閃記憶模組 16 或保密裝置模組 14，但卻無須檢查寫入命令的格式本身到底屬於快閃記憶模組 16 或保密裝置模組 14 的寫入命令。

舉例來說，若來自記憶體介面 10 的資料封包 20 中，其封包頭 20a 含有預定資料時，控制模組 12 將資料封包 20 轉送給保密裝置模組 14。若來自記憶體介面 10 的資料封包 20 中，其封包頭 20a 未含有預定資料時，控制模組 12 將資料封包 20 轉送給快閃記憶體模組 16。

換句話說，在主機端被執行中的應用程式，若需要對快閃記憶體模組 16 寫入資料時，資料封包 20 的格式只須相對於記憶體介面 10 即可，但是需要對保密裝置模組 14 寫入資料時，資料封包 20 的格式除了相對於記憶體介面 10 以外，還需額外在資料封包 20 的封包頭 20a 內寫入預定資料，以便讓控制模組 12 作辨識。

藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本發明之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本發明之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本發明所欲申請之專利範圍的範疇內。

【圖式簡單說明】

第 1 圖為本發明基於記憶體介面的保密裝置通訊機制之示意圖。

第 2 圖為本發明資料封包之示意圖。

【主要元件符號說明】

10 記憶體介面

12 控制模組

14 保密裝置模組

16 快閃記憶體模組

20 資料封包

20a 封包頭

20b 封包本體

五、中文發明摘要：

本發明基於記憶體介面的保密裝置通訊機制主要包含記憶體介面、保密裝置模組、快閃記憶體模組、以及電性連接至記憶體介面、保密裝置、以及快閃記憶體模組之控制模組。由於來自記憶體介面的資料封包，在其封包頭中額外包含有特殊的預定資料，這使得控制模組得以在發覺資料封包的封包頭中含有預定資料時，將資料封包轉送給保密裝置模組。若來自記憶體介面的資料封包在其封包頭中沒有額外包含有預定資料時，控制模組將資料封包轉送給快閃記憶體模組。

六、英文發明摘要：

十、申請專利範圍：

1、一種基於記憶體介面的保密裝置通訊機制，包含：

一記憶體介面，係用以接收一資料封包，該資料封包至少包含一封包頭(head)與一封包本體；

一保密裝置模組，提供在公共金鑰架構下之加密、解密、憑證產生與儲存功能；

一快閃記憶體模組；

一控制模組，電性連接至該記憶體介面、該保密裝置、以及該快閃記憶體模組，並依據該資料封包的該封包頭中是否含有一預定資料，而決定將該資料封包轉送給該保密裝置模組或該快閃記憶體模組。

2、如申請專利範圍第1項所述之基於記憶體介面的保密裝置通訊機制，其中該保密裝置模組為智慧卡模組或晶片卡模組或爪哇卡(JAVA card)、用戶識別卡、生物護照及生物身分證。

3、如申請專利範圍第1項所述之基於記憶體介面的保密裝置通訊機制，其中該控制模組與該保

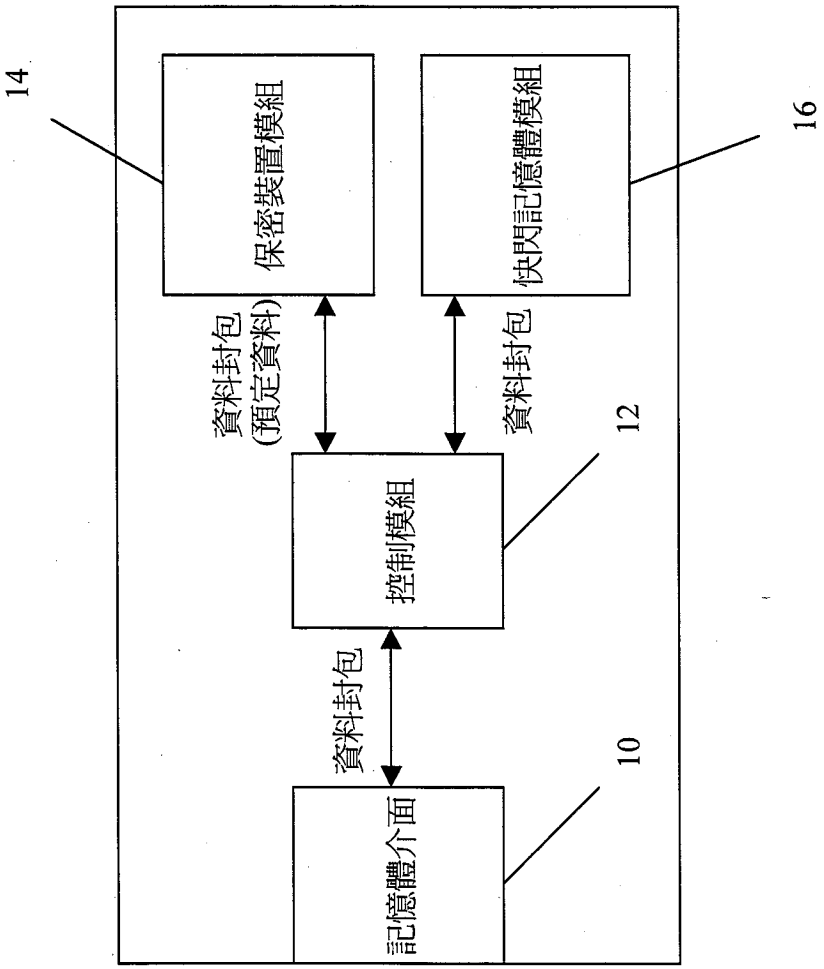
密裝置模組之間的介面可為串列周邊介面(Serial Peripheral Interface, SPI)、通用串列匯流排(Universal Serial Bus,USB)或ISO 7816。

4、如申請專利範圍第1項所述之基於記憶體介面的保密裝置通訊機制，其中該預定資料為特殊字串或符號。

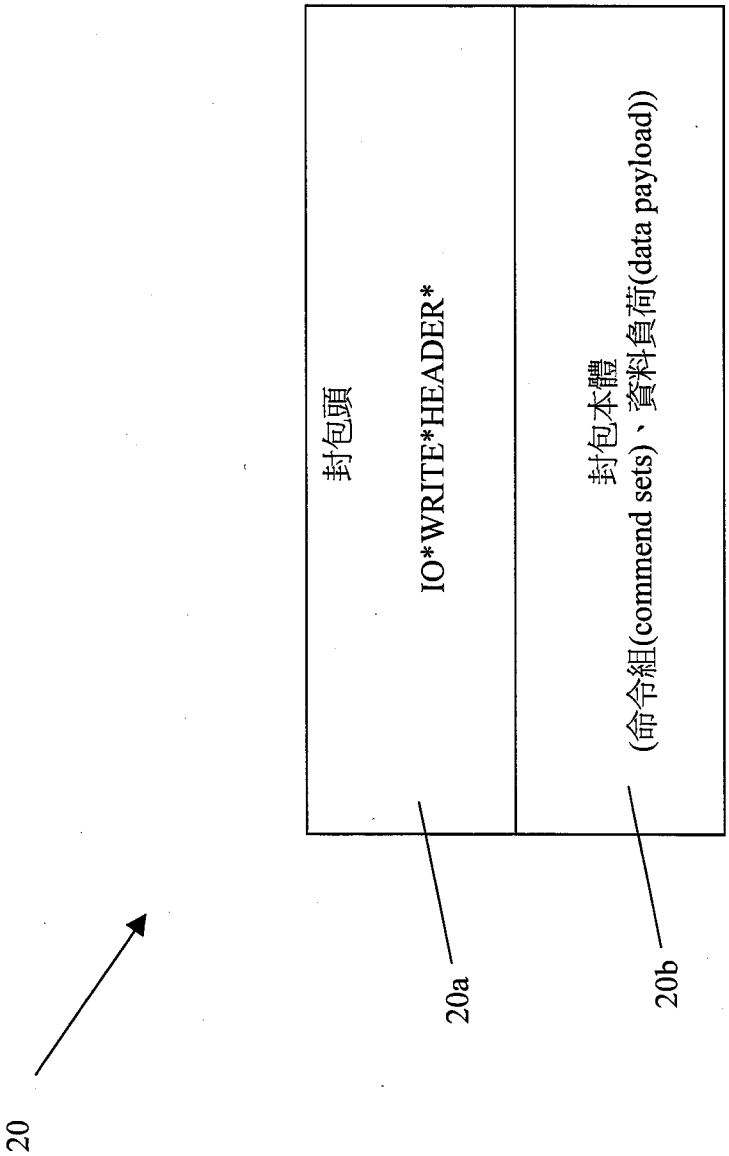
5、如申請專利範圍第1項所述之基於記憶體介面的保密裝置通訊機制，其中來自該記憶體介面的該資料封包中，其該封包頭含有該預定資料時，該控制模組將該資料封包轉送給該保密裝置模組。

6、如申請專利範圍第1項所述之基於記憶體介面的保密裝置通訊機制，其中來自該記憶體介面的該資料封包中，其該封包頭未含有該預定資料時，該控制模組將該資料封包轉送給該快閃記憶體模組。

200924479



第1圖


封包頭
IO*WRITE*HEADER*
封包本體
(命令組(commend sets)、資料負荷(data payload))
20a
20b
20

第2圖

七、指定代表圖：

(一)本案指定代表圖為：第（　1　）圖。

(二)本代表圖之元件符號簡單說明：

10 記憶體介面

12 控制模組

14 保密裝置模組

16 快閃記憶體模組

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：