公告本

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：95104117

※ 申請日期：95.2.7　　※IPC 分類：G06K 19/073 (2006.01)

G01R 31/26 (2006.01)

一、發明名稱：(中文/英文)

具有生命周期階段之安全記憶卡

SECURE MEMORY CARD WITH LIFE CYCLE PHASES

二、申 請 人：(共 2 人)

姓名或名稱：(中文/英文)

1.美商桑迪士克股份有限公司

SANDISK CORPORATION

2.以色列商狄斯奎科技公司

DISCRETIX TECHNOLOGIES LTD.

代表人：(中文/英文)

1. 查爾斯　樊　歐登

VAN ORDEN, CHARLES

梅根　康普特

COMPORT, MEGAN

2. 大衛　黛伊齊

DEITCHER, DAVID

住居所或營業所地址：(中文/英文)

1. 美國加州謬佩塔斯市麥卡錫大道 601 號
601 MCCARTHY BOULEVARD, MILPITAS, CA 95035, U. S. A.

2. 以色列那坦亞市郵政信箱 8718 號保里格工業區漢拉奇街伊格雷大樓 45 號
45 HAMELACHA ST., ETGARIM BLDG., POLEG INDUSTRIAL ZONE, P.O. BOX 8718, NETANYA, ISRAEL 42502

國　籍：(中文/英文)

1.美國　　U.S.A.

2.以色列　　ISRAEL

三、發明人：(共 5 人)

姓　名：(中文/英文)

1.邁可　哈得茲曼

HOLTZMAN, MICHAEL

2.巴奇　布魯斯　柯漢

COHEN, BARUCH BORIS

3.羅　巴利列

BARZILAI, RON

4.哈吉依　巴-艾爾

BAR-EL, HAGAI

5.大衛　黛伊齊

DEITCHER, DAVID

國　籍：(中文/英文)

1.以色列　ISRAEL

2.以色列　ISRAEL

3.以色列　ISRAEL

4.以色列　ISRAEL

5.以色列　ISRAEL

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：

1. 美國；2005年02月07日；60/651,128
2. 美國；2005年12月22日；11/317,390
3. 美國；2005年12月22日；11/317,862

☐ 無主張專利法第二十七條第一項國際優先權：

1.
2.

☐ 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。

五、中文發明摘要：

本發明揭示一種具加密能力之安全記憶卡，其包括各種生命週期狀態，該等生命週期狀態允許在其中某些狀態下測試該卡之硬體及軟體。測試機制在某些其它狀態下被去能，因而關閉安全資料及密碼密鑰之潛在後門。經控制之可用性及資料加密及解密所需之密鑰之產生因而即使後門得以存取先前經加密之資料，也不可能解密該資料，因此縱然一後門被發現且經惡意窺探後亦不重要。

六、英文發明摘要：

七、指定代表圖：

(一)本案指定代表圖為：第(2A)圖。

(二)本代表圖之元件符號簡單說明:

110	NVM狀態
120	恆定賦能狀態
130	隨機賦能狀態
140	最後密鑰狀態
150	安全狀態
160	RMA狀態
170	去能狀態

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

九、發明說明：

【發明所屬之技術領域】

本發明大體而言係關於記憶卡及加密，且具體言之係關於藉由該卡中之測試機制來消除對安全資料及密鑰之存取。

【先前技術】

不久以前，研製出通常被稱為智慧卡的智能型記憶卡且以識別及支付之形式取得市場的接受。智慧卡含有用於儲存一使用者之識別資料及用於儲存交易相關資料的少量記憶體。智慧卡亦經常被稱為晶片卡(chip card)且在日本被用於各種事物(諸如國民身份證(national identity card))及各種場所，如一類型之信用卡或轉帳卡。為了防止身份盜竊及其它貨幣詐欺，該等卡及利用該等卡之系統中已採用了各種晶片設計及加密方案。

在設計及製造任何類型之安全記憶卡時，存在兩種競爭性利益。一種利益為最大化卡之安全性，而另一種利益為最大化卡之可靠性。為了最大化卡之可靠性，能夠在卡自工廠運輸之前於各種製造階段測試卡之軟體及硬體，且在一些時候，甚至是在卡已離開工廠後測試卡之軟體及硬體以執行故障分析係重要的。測試可包括訊號經由晶片上之測試墊或接觸墊之輸入及輸出以測試卡之硬體及軟體兩者。此等測試常式及測試墊為確保品質控制所必需，但卻為卡之安全資料、演算法及密鑰之一潛在弱點或"後門"。因此，(測試所必需)最大化可靠性與最大化安全性之間總

是存在一些程度之妥協。已提出不同方法以在測試完成後關閉此"後門"。然而，出於各種原因，到目前為止之先前解決辦法各自具有商業及技術上的缺點。

在一咸信被用於前述智慧卡之製作中之方法中，在將來自晶圓之記憶體晶粒單一化之前測試卡之晶粒。用於一特定晶粒之測試墊係定位於晶圓之一鄰近晶粒上，且在測試後，單一化處理使測試墊與鄰近晶粒之所有電路分離。因此，作為最後記憶卡之安全資料之一潛在後門的存在於一經單一化之晶粒上之任何測試墊被完全隔離並關閉得以。然而，完全移除測試墊並非總是實用或需要的。舉例而言，可用測試墊之缺乏排除記憶體的一些量之隨後基於硬體之測試，其(例如)限制故障分析之潛在方法。

雖然此方法對一智慧卡(其通常僅具有保存識別及交易資料所必需之少量記憶體)而言可能較佳，但是其對測試用於儲存多個大檔案(諸如相片及音樂)之大量儲存記憶卡中採用的相對大量之記憶體及複雜安全性常式而言係不足的。此等大量儲存記憶卡之一些實例為緊密快閃記憶卡、MMC卡及SD卡。數位內容之傳播及相關版權問題加大了安全性之重要性，但與此同時，卡之測試及可靠性仍極為重要。需要一種更加全面且靈活之系統以用於製造、測試及操作大量儲存安全記憶卡且該系統係由將於下文描述之本發明來提供。

另一重要態樣為成本。若干不同技術(諸如非揮發性記憶體、邏輯及揮發性記憶體)可以製造於一單一積體電路

晶粒(晶片)上。然而，在一晶粒中混合不同技術使生產成本顯著增加。在成本為主要驅動力之競爭環境中，極其需要限制提供於一晶粒上之不同技術的量。然而，使用多個晶粒可能意味著：在最終產品中，敏感資訊不得不自一個晶粒傳遞至另一個晶粒。若未採用適當之防護措施，則此為駭客可利用之另一潛在弱點。

詳言之，在相同晶粒內，將非揮發性記憶體位元與邏輯混合係昂貴的。智慧卡將相同晶粒中用於資料儲存之非揮發性記憶體用作為操作該智慧卡之邏輯，此為最大化安全性之一方式。然而，現今，一受益於本發明之記憶卡必須儲存更大的音樂、相片、電影及其它使用者檔案。因此，從成本考慮，製造可儲存大量資訊(在2005年，其為大約數十億個位元組且還在增加)之單一積體電路晶粒記憶卡被禁止，且需要研製一採用多個晶粒之安全系統。詳言之，極需要創建一利用一或多個離散(節省成本)快閃記憶體晶粒之安全系統(採用加密及解密)，該等快閃記憶體晶粒晶粒與控制器晶粒分離且可在組裝之前及之後、經由測試機制來加以徹底測試，而不易為攻擊所傷。

【發明內容】

因為利用一既具有控制器功能亦具有當今數位裝置所要求之大儲存量的單一晶片過度昂貴且在可調能力上存在問題，所以已研製出一替代系統。對於一單一晶片解決辦法而言，安全性可用獨特的晶片設計來達成，此設計使存取測試機制、加密密鑰及經加密之內容變困難。然而，對於

內容係自一分離記憶體晶片傳遞至一控制器晶片(加密於其中發生)之一多晶片設計而言，必需特別注意保護對加密密鑰及經加密之內容的存取。此外，在一在最後組裝中(較佳)仍具有測試墊以允許測試經組裝之系統的系統中，必需特別注意軟體及硬體中可能用作一用於未授權地存取經加密之密鑰及內容之後門的任何機構。

本發明具有在卡之生命期間進入且經過的眾多生命週期階段。視階段而定，卡中之邏輯賦能或去能加密引擎，控制對硬體(在晶圓單一化及卡組裝之前及之後)及軟體測試機制之存取，並控制密鑰產生。此等階段不僅允許在製造之前及之後徹底地測試卡之硬體及軟體兩者(與測試墊經移除之智慧卡中不同)，亦使當卡處於一安全階段(該卡被運輸至使用者時其所處之操作階段)時存取經加密之密鑰及因此經加密之內容實際上不可能。因此，本發明提供一種記憶卡，其可加以良好測試，但其亦抵抗對卡中之受保護之資料的未授權存取。

此外，需要一種更加全面且靈活之系統以用於製造、測試及操作大量儲存安全記憶卡之且該系統係由將於下文描述之本發明來提供。

本發明之額外態樣、優點及特徵包含於示範性實例之下列描述中，此描述應結合隨附圖式，其中相似數字用於描述所有圖中之相同特徵。因此，為達成所有目的，本文中參考之所有專利案、專利申請案、文章及其它公開案係以全文引用之方式併入本文中。

【實施方式】

記憶體系統架構

一其中可建構本發明之各種態樣之實例記憶體系統係由方塊圖1A來說明。如圖1A所示，記憶體系統10包括一中央處理單元(CPU)或控制器12、一緩衝區管理單元(BMU)14、一主機介面模組(HIM) 16、快閃介面模組(FIM) 18、一快閃記憶體20及一周邊存取模組22。記憶體系統10經由一主機介面匯流排26及埠26a與主機裝置24通信。快閃記憶體20 (其可為NAND類型)為主機裝置24提供資料儲存。CPU 12之軟體程式碼亦可儲存於快閃記憶體20中。FIM 18經由一快閃介面匯流排28連接至快閃記憶體20，且在一些情況下，若快閃記憶體20為一抽取式組件，則FIM 18經由一埠(未圖示)連接快閃記憶體20。HIM 16適於連接至一主機系統，諸如數位相機、個人電腦、個人數位助理(PDA)及MP-3播放器、行動電話或其它數位裝置。周邊存取模組22選擇適當之控制器模組(諸如FIM、HIM及BMU)以用於與CPU 12通信。在一實施例中，虛線框內的系統10之所有組件可封閉於一單一單元中，諸如封閉於記憶卡中且較佳封閉於卡中。

緩衝區管理單元14包含一主機直接記憶體存取單元(HDMA)32、一快閃直接記憶體存取單元(FDMA) 34、一仲裁器36、一CPU匯流排仲裁器35、暫存器33、緩衝區隨機存取記憶體(BRAM) 38及一密碼引擎40 (其亦被稱為加密引擎40)。仲裁器36為一共享匯流排仲裁器，使得在任

何時候僅一個主控器或啟動器(其可為HDMA 32、FDMA 34或CPU 12)可起作用且受控器或目標為BRAM 38。該仲裁器負責通道化適當啟動器請求至BRAM 38。HDMA 32及FDMA 34負責HIM 16、FIM 18與BRAM 38或RAM 11之間的資料傳輸。CPU匯流排仲裁器35允許經由系統匯流排15將資料自密碼引擎40及快閃DMA 34直接傳送至RAM 11，在某些情況下(諸如當需要旁路該密碼引擎時)使用該系統匯流排。HDMA 32及FDMA 34之運作係習知的且不必在本文中予以詳述。BRAM 38用於儲存在主機裝置24與快閃記憶體20之間傳遞之資料。HDMA 32及FDMA 34負責在HIM 16/FIM 18與BRAM 38或CPU RAM 12a之間傳送資料且負責指示扇區完成。

當來自快閃記憶體20之資料係由主機裝置24讀取時，記憶體20中之經加密資料係經由匯流排28、FIM 18、FDMA 34及密碼引擎40 (經加密之資料係於其中解密)來提取且儲存於BRAM 38中。接著，該經解密資料係經由HDMA 32、HIM 16、匯流排26自BRAM 38發送至主機裝置24。自BRAM 38提取之資料可在其被傳遞至HDMA 32之前借助於密碼引擎40而再次加密，以使得發送至主機裝置24之資料被再次加密，但係借助於一與加密儲存於記憶體20中之資料所用之彼等密鑰及/或演算法相比不同之密鑰及/或演算法。或者，不同於上述過程中之將經解密之資料儲存於BRAM 38中(其可使資料變得易受到未經授權之存取攻擊)，來自記憶體20之資料可在其被發送至BRAM 38之前

藉由密碼引擎40來再次解密並加密。接著，如前所述，BRAM 38中之經加密資料被發送至主機裝置24。此說明一讀取過程中之資料流。

當資料係藉由主機裝置24寫至記憶體20時，資料流之方向相反。舉例而言，若未經加密之資料係藉由主機裝置、經過匯流排26、HIM 16、HDMA 32而發送至密碼引擎40，則該資料可在其被儲存於BRAM 38中之前由引擎40來加密。或者，未經加密之資料可儲存於BRAM 38中。接著，該資料係在其至記憶體20之途中被發送至FDMA 34之前來加密。

生命週期階段

一在建構於一記憶卡中時尤其有用之保全系統或安全操作系統(諸如上述之系統)具有不同階段或狀態。較佳地，依序進入此等階段，以使得自一個階段進展至下一個階段之後，不能再次進入先前階段。因此，該等階段可被認為是生命週期階段。

在詳述該等階段之前，將簡要論述另一系統位準圖。圖1B說明系統10之另一實施例。為簡單及明晰起見，在此圖中僅說明系統10之某些組件。記憶體系統10包含測試墊(其亦被稱為硬體測試輸入/輸出(I/O)端) 54。硬體匯流排(HW匯流排)56較佳係連接至測試墊54。此等測試墊及HW匯流排56係連接至系統10之各種硬體及電路(未圖示)且用於測試系統10之該硬體及電路。JTAG匯流排62係連接至系統匯流排15 (參見圖1A)且可用於替換該控制器韌體並自

系統10之外部驅動硬體塊。其用於要求暫存器讀取/寫入操作之硬體測試。因為JTAG匯流排62可存取RAM及ROM，所以其亦用於測試系統10之韌體。主機匯流排26被用於發送診斷指令至系統10且用於測試該系統之韌體。

亦展示加密引擎40之NVM 50。儲存於NVM 50中的係生命週期狀態77(之值)及秘密密鑰99。NVM測試埠58用於測試加密引擎40中之該NVM。

狀態指示符熔絲66用於指示產品係處於NVM狀態110(如下所述)而不依賴NVM內容。其原因係在製造期間儲存於NVM中之一初始值之可靠性不能得到保證。因此，使用另一更為可靠之指示符，諸如使用一熔絲。若熔絲經設定，則該系統確定該產品處於狀態110。若系統10經重置，則其將查看NVM生命週期狀態77以確定狀態。

圖2A說明各種狀態及狀態之間的轉換次序。在製造卡之前及其後，每一狀態界定該卡(或其中建構有該卡之其它系統)之不同行為及能力，如下表中所示，其亦如圖2B中所再現的。

狀態	密鑰產生	NVM測試	HW測試	FW測試	密碼引擎
110	於每次電力開啟時重新產生	E	E	E	D
120	恆定且硬式佈線	D	E	E	E
130	產生一次	D	E	E	E
140	產生一次	D	D	D	E
150	-	D	D	D	E
160	於每次電力開啟時重新產生	D	E	E	E
170	-	D	E	E	D

狀態較佳係儲存為加密引擎之非揮發性記憶體中之一32位元的值。存在出自於代表狀態120-170的大量(~10^9)可能

組合之6個預分配值。所有其它值指示狀態110。如此係因為不能保證可在製造及此後之檢索期間可靠地儲存一確定值，因為製造、組裝、測試及運輸期間的各種處理操作可能改變記憶體中之任何儲存值。

密鑰值亦較佳儲存為加密引擎之非揮發性記憶體中之一128位元的欄位。該密鑰值通常係藉由一播種演算法(seeded algorithm)隨機地產生。密鑰之重新產生極有可能改變密鑰之值，但是，因為一(偽)隨機數產生器事實上可能連續產生相同值，所以此不能得到保證。然而，即使鹹知密鑰之值在重新產生期間不會改變，改變密鑰之術語在此應用中仍係與重新產生密鑰之術語交換地使用。不言而喻，用於加密資訊之密鑰之值至關重要。相同之密鑰值必須既用於加密亦用於解密。因此，若在系統之每次電力開啟時重新產生一密鑰值，則在彼電力開啟之前經加密之資料因為不能以該新密鑰解密而事實上係無價值的。雖然資料仍實體地存在於該卡之記憶體中，但是若無適當密鑰值來解鎖，則該資料即係無用的。因此，若一駭客不知何故得以強迫該卡退至一不同於安全狀態150之狀態，則他不能得到任何有用資訊。在狀態110及160中，每一電力開啟時將產生一新的密鑰，且在狀態150中，先前用於儲存資訊之密鑰將不可用於解密彼資訊。在狀態170及110中，不管密鑰值如何，該加密引擎係完全不可用的。

另一安全性措施包含限制韌體及硬體測試機制之可用性。該系統包含賦能或去能該等機制之邏輯。先前描述之

主機匯流排係用於測試該卡之該韌體之該等機構之一。該主機可經由該主機匯流排發出診斷指令以測試該韌體。該硬體亦可於執行此等指令時加以測試。該硬體亦可經由該硬體匯流排以及該JTAG埠來直接加以測試，該JTAG埠提供對該系統之各種記憶體之直接存取。請注意，在狀態140及150中，NVM測試機制、HW測試機制及FW測試機制皆被去能。

現將進一步詳述如圖2A所示之該等狀態及狀態之間的通道。

狀態110係指控制器非揮發性記憶體(NVM)測試。此狀態為記憶體晶粒製造後之初始狀態，且係用於在封裝該晶粒且將其安裝至記憶卡中之前測試控制器晶粒之非揮發性記憶體的狀態。此狀態下出現之測試可在單一化之前執行且該等晶粒仍係以晶圓格式整合，或者該測試可在單一化之後替代地執行於個別晶粒上。一旦NVM得到測試，其內容(使用該NVM測試器)即被初始化以指示狀態120，且熔絲66被燒斷。在此狀態下，加密引擎40被去能。在卡之生命週期中，此狀態僅經設計以進入一次，且在系統中不存在方法可用於使卡返回至此狀態。然而，如先前所述的，此狀態可由除用於界定生命週期狀態之32位元值之許多可能組合的6個預分配值之外的任一者來指示。若偵測到一非法值且熔絲燒斷(不允許進入NVM狀態110)，則該密碼引擎將不能就緒且系統將不啟動，或旁路下面參看圖3描述之步驟302。因此，每次該卡被電力開啟且處於此狀態

時，將隨機產生一新的密鑰，且不可能解密先前經加密之資料。即使加密引擎在此模式下未被賦能(因為該模式經設計以於製造期間在晶圓仍完整時使用)，密鑰仍係於每次電力開啟時重新產生以保護免受一駭客危害，該駭客可能以一些無法預料之方法進入此狀態且試圖經由各種測試埠及機制探測該卡之安全資料。另外，藉由設計，在退出狀態110之後，該等NVM測試機制將不再可用。

狀態120被稱為恆定賦能狀態。在此狀態下，加密引擎40被賦能。該加密引擎將使用之密鑰不係由隨機數產生器產生，且不儲存於記憶體中，但是經硬式佈線至一些外部源且在此階段期間恆定。硬體及軟體測試機制在此狀態下可用。此狀態係藉由一硬體測試器進入。

狀態130被稱為隨機賦能狀態。此狀態類似於狀態120，然而，秘密密鑰係於進入狀態130時隨機產生(一次)而不非恆定且硬式佈線的。此係用於記憶卡之最後測試、特性化及鑑定之狀態。利用使用一秘密密鑰或自該秘密密鑰衍生之密鑰之韌體，包括加密及解密之密碼操作係可能的。此狀態係藉由經由主機裝置24加載至系統10中且接著由系統10執行之程式碼而進入。

狀態140被稱為最終密鑰狀態。在此狀態下，該卡使用將與該卡一起運輸之最後秘密密鑰。硬體及軟體測試機制係藉由該卡之邏輯來去能且不能被存取。此包括硬體測試匯流排及測試墊(參見圖1B)。此狀態用於給該卡加載最後韌體及必須加以保護之具有與產品一同運輸之密鑰的組態

資料。該產品可在此狀態下加以組態，但在狀態150中則不能。此狀態係藉由一主機指令而進入。該指令可包含於自主機下載且由該卡執行之程式碼中("DLE程式碼")。該指令可替代地直接自主機發出。此在如下任何時候利用術語DLE程式碼時為真。

狀態150被稱為安全狀態。此為卡自工廠運輸時所處之狀態。硬體及軟體測試機制係藉由卡之邏輯來去能且不能被存取。此狀態係於在製造現場測試及組態產品結束時進入。密鑰未重新產生且在狀態150期間利用在狀態140期間儲存於記憶體中之值。雖然衍生之密鑰可用於卡之各種操作，但總是需要密鑰99以衍生彼等密鑰且加密及解密資料。此密鑰意欲用於安全卡之有效期(當其作為一持於消費者手中之安全卡，而非其後)。卡中之韌體不可將秘密密鑰用於任何操作。加密引擎之硬體負責執行卡中之所有加密及解密。此狀態係藉由DLE程式碼而進入。

狀態160被稱為返回之商品授權或RMA狀態。此狀態經設計以允許測試一因為未正常工作而由一消費者退回之卡。此為可執行卡之故障分析之狀態。軟體及硬體測試機制再次可用。注意此狀態僅由工廠可存取係重要的。此外，在進入RMA狀態之後，該卡絕不能再次作為一安全卡來使用。換而言之，該卡絕不能再次進入狀態150或另外用於解密常駐於該卡上之資訊或將經加密之資訊保存至卡。秘密密鑰係在進入此模式時重新產生，且在卡處於此狀態下每一晶片經重置執行期間時。使用秘密密鑰來解密

之操作係僅在啟動時間賦能且韌體不能將該秘密密鑰用於任何操作。此狀態係藉由一作為主機指令之結果的ROM程式碼而進入。

狀態170被稱為去能狀態。在該去能狀態下，密碼引擎40處於一旁路模式，並且所有密碼能力被去能。僅非安全演算法可於該卡中使用。因為沒有加密引擎，侵入或其它干預係沒有價值的，所以硬體及軟體測試機制被再次賦能。任何經加密之資訊不能再加以解密且變得無價值。同樣，無額外資訊可加密且隨後解密。此狀態可用於生產一非安全或"普通"卡。以此方式，相同系統既可用於生產安全記憶卡亦可用於生產非安全記憶卡。不同之處在於：在非安全卡中，卡之保全系統係處於去能狀態，或更大體而言，該卡可處於狀態170。該去能狀態亦可用於重新運輸一產品，該產品已被發送回至工廠以進行故障分析且因此已進入RMA狀態160。如上所提及的，在一卡進入RMA狀態160之後，其絕不能返回任何先前狀態中之任一者，且絕不可再次作為一安全卡來銷售。然而，一有功能或可在工廠再次製造得有功能之卡可被置於去能狀態170且作為一非安全卡來銷售。以此方式，該卡可加以回收且與一新的非安全或"普通"卡一樣用於所有深層用途。該回收之非安全卡及一新的非安全卡均可在相同狀態下操作相同韌體。

現在，大多數卡為非安全卡。雖然將安全卡推向市場之動力很高(其主要歸因於內容提供者之需求)，但是不清楚

安全卡對比非安全卡之未來記憶卡銷售之百分比將如何。所清楚的是，很可能總是存在許多非安全內容且因此存在對非安全卡之需求。本發明不僅允許測試一安全卡之所有硬體及軟體(僅由經授權之人員進行)，而且提供回收返回之安全卡以用於各種非安全使用者之能力。此外，本發明之系統允許一卡具有穩固安全性，但其無需加以廢除或使其保全系統妥協(具有可存取之"後門")以執行故障分析。因為使用記憶卡之裝置之廣泛傳播及日益增加之擴散化，回收另外可成為一有缺陷安全卡之卡的能力對消費者及製造者而言有很大益處。

圖3說明建構上述系統之一記憶卡的啟動過程。為得到關於該啟動過程之更多資訊，請參考一同在申請中之Micky Holtzman等人的申請案"Method of Hardware Driver Integrity Check Of Memory Card Controller Firmware"、申請案第11/284,623號、代理人案號第SNDK.408US1號，其以全文引用之方式併入本文中。

在步驟302中，該系統檢查密碼硬體(包括密碼引擎40及其它組件)是否準備就緒。該系統將等待直到該硬體就緒後才繼續。當該硬體就緒時，該系統前進至步驟304。在步驟304中，該系統檢查該卡是否處於狀態170(去能狀態)。若該卡處於狀態170，則在步驟306中，該系統將啟動載入器("BLR")自快閃記憶體20上載至RAM 11，該啟動載入器係最少量之起動碼。接下來，在步驟308中，該系統檢查該BLR是否被完全上載。若是，則在步驟310中，

該系統將上載在非安全模式下操作所需之韌體(標準韌體減去密碼功能)。若如步驟308中所判定的，該BLR未能完全上載，則該系統將前進至下述步驟324。

若在步驟304中，該系統判定該卡不處於狀態170，則該系統將在步驟312中清除RAM內容。在彼步驟之後，該系統將在步驟314中再次檢查該卡處於何種狀態。若該卡處於狀態120、130或140，則將在步驟316中上載該BLR。在步驟318中，該系統將檢查該BLR是否被完全加載。接下來，在步驟320中，將執行BLR程式碼之完整性檢查。此完整性檢查係一由計算訊息鑑別程式碼(MAC)值且將該等值與參考值進行比較來執行的基於硬體之檢查。該完整性檢查之結果係一儲存於記憶體中之簡單旗標。在步驟322中，該韌體檢查該旗標以判斷完整性是否經驗證。若完整性經驗證，則該系統將在步驟342中上載於安全模式下操作所必需之韌體，其亦當然允許儲存及檢索非安全資料。若如步驟322中判定的，該完整性未經驗證，則該系統將等待一來自主機之診斷指令以下載且執行來自主機之某些指令(DLE指令)如步驟324所代表。若如步驟326中所示，接收到一DLE指令，則該系統將繼續在步驟328中將DLE程式碼加載至RAM中。在步驟330中，DLE程式碼將由控制器來執行。

若在步驟314中判定該卡不處於狀態120、130或140，則該系統將在步驟332中檢查該卡是否處於狀態150。若是，則該系統將接著在步驟334中上載該BLR。此係藉由ROM

程式碼來完成執行。若如步驟336中所判定的，BLR加載完成，則將在步驟338中執行一基於硬體之完整性檢查，如上面之步驟320中所述的。在此基於硬體之完整性檢查之後，將在步驟340中執行另一完整性檢查(此次為一基於軟體之完整性檢查)。若完整性經驗證，則該系統將接著在步驟342中上載於安全模式下操作所必需之韌體，其當然亦允許儲存及檢索非安全資料。

若在步驟332中判定該卡不處於狀態150，則該系統將接著檢查卡之狀態及該卡是否處於狀態160，且若是，則其將等待一由步驟348所表示之診斷指令。然而，若在步驟344中判定該卡不處於狀態160，則該系統將等待一指令以進入RMA狀態160 (參見步驟346)。

【圖式簡單說明】

圖1A為根據本發明之一實施例之系統10的示意圖。

圖1B為系統10之另一實施例的示意圖。

圖2A為說明本發明之一實施例中各種生命週期階段的流程圖。

圖2B為各種生命週期階段的表。

圖3為說明啟動過程及生命週期階段的流程圖。

【主要元件符號說明】

10	記憶體系統/系統
11	RAM
12	中央處理單元(CPU)/控制器/CPU
12a	CPU RAM

14	緩衝區管理單元(BMU)
15	系統匯流排
16	主機介面模組(HIM)/HIM
18	快閃介面模組(FIM)/FIM
20	快閃記憶體/記憶體
22	周邊存取模組
24	主機裝置
26	主機介面匯流排/匯流排
26a	埠
28	快閃介面匯流排/匯流排
32	主機直接記憶體存取單元/HDMA
33	暫存器
34	快閃直接記憶體存取單元/FDMA/快閃DMA
35	CPU匯流排仲裁器
36	仲裁器
38	緩衝區隨機存取記憶體/BRAM
40	密碼引擎/加密引擎/引擎
50	NVM
54	硬體測試輸入/輸出(I/O)/測試墊
56	硬體匯流排/HW匯流排
58	NVM測試埠
62	JTAG匯流排
66	狀態指示符熔絲/熔絲
77	生命週期狀態
99	秘密密鑰/密鑰

十、申請專利範圍：

102年1月30日修正本

1. 一種操作一記憶卡之方法，其包括：

當一主機耦接至一記憶卡時在該主機中執行多個步驟，其中該記憶卡包括具有測試埠之一記憶體晶粒及一保全系統，且該記憶卡係可在測試、操作、故障分析及去能狀態中操作，該保全系統包括：

一密碼引擎及一密碼密鑰，

其中在該測試狀態該測試埠可用於硬體測試，且軟體測試常式可用於賦能該密碼引擎之運作及該記憶卡之軟體的測試，

其中在該操作狀態該等測試埠係不可用的，該軟體測試常式係不可用的，及該記憶卡經組態以用以操作為一安全記憶卡，及

其中去能該密碼引擎且該記憶卡操作為一非安全記憶卡時，該去能狀態係不可逆的，其步驟包括：

當該記憶卡處於該測試狀態時，測試該記憶卡軟體；

傳輸一指令至該記憶卡以使該記憶卡不可逆地自該測試狀態切換至該操作狀態；及

在偵測到該記憶卡之一故障之後，使該記憶卡操作在賦能該記憶卡之該軟體及硬體之故障測試之該故障分析狀態中、防止該記憶卡再次解密該記憶卡上之先前儲存之資訊或進入一安全操作狀態，及組態該記憶卡使得該記憶卡僅可轉換至該去能狀態。

2. 如請求項1之方法，其中該記憶卡之一當前狀態之一指示符係儲存於該記憶卡之一非揮發性記憶體中。

3. 如請求項1之方法，其中使該記憶卡操作在該故障測試狀態中可使該記憶卡在該故障分析狀態下每次隨後電力開啟時，產生一新的密鑰值，且其中在最近一次之電力開啟不能由該記憶卡解密之前加密資料。

4. 一種建構於一記憶卡中之保全系統，其包括：

一密碼引擎，其經組態以加密並解密資訊以保全儲存於該記憶卡上之資訊；以及

該記憶卡中之一秘密密鑰，其用於加密及解密，

其中該保全系統操作轉換於一測試狀態、一安全操作狀態和一旁路操作狀態之間，

其中在一測試狀態，

該加密引擎被賦能，

該秘密密鑰係於進入該測試狀態之後產生，該記憶卡中之韌體之測試被賦能，及

該記憶卡之硬體之測試被賦能，

其中在該安全操作狀態，

該密碼引擎被賦能，

該記憶卡中之韌體之測試被去能，

該記憶卡之硬體之測試被去能，及

該秘密密鑰係由該加密引擎使用以加密並解密資訊，及

其中在該旁路操作狀態，

該加密引擎被去能；

該記憶卡之該硬體之測試被賦能，

該記憶卡之該韌體之測試被賦能，

若該記憶卡操作為一普通記憶卡，則使用該旁路操作狀態，其中一旦在該旁路操作狀態中該保全系統操作該記憶卡以運作為一非安全記憶卡且不能再次轉換至該安全操作狀態。

5. 如請求項4之系統，其中該加密引擎係基於硬體的。

6. 如請求項4之系統，其中該秘密密鑰係儲存於該加密引擎之一非揮發性記憶體中。

7. 如請求項4系統，其進一步包括：

一故障分析操作狀態，其中：

該記憶卡之硬體可加以測試；

該記憶卡之韌體可加以測試；且

該秘密密鑰係於每當在該故障分析狀態下，電力開啟該系統時重新產生。

8. 如請求項7之系統，其中在進入該故障分析操作狀態之後，該記憶卡絕不能再次在該安全操作狀態下使用。

9. 如請求項8之系統，其中該故障分析操作狀態係於進入該旁路狀態之前啟動。

10. 如請求項4之保全系統，其中該測試狀態包括在該記憶卡之測試期間可用的操作之一或多個測試狀態，該等測試狀態允許使用在一積體電路上之測試埠及在該記憶卡之韌體中之測試機制；

其中在該記憶卡之正常使用期間該安全操作狀態是可用的，該安全操作狀態禁止使用該等測試埠及該韌體中之該等測試機制；以及

其中該記憶卡更包括用於在該或該等測試狀態之一測試狀態與該安全操作狀態之間切換的邏輯，其中一旦該記憶卡經切換至該安全操作狀態，該或該等測試狀態即絕不能再次被存取，從而藉由防止存取該韌體中之該等測試機制及該等測試埠來禁止存取該記憶卡上之安全資料。

11. 如請求項10之系統，其進一步包括一故障分析狀態，其中一用於加密及解密資料之新密鑰係於每次電力開啟時產生，且其中以一個密鑰加密之資料不能以另一密鑰來解密。

12. 如請求項11之系統，其中該故障分析狀態係於可進入該旁路狀態之前進入。

13. 如請求項10之系統，其進一步包括一最後密鑰狀態，其用於加載將在該安全狀態下使用之最後韌體至該記憶卡，該韌體中之該等測試機制在該最後密鑰狀態下被去能。

14. 如請求項13之系統，其中在該最終密鑰狀態下，與該等測試埠之通信係不可用的。

15. 如請求項4之系統，其進一步包括一最後密鑰狀態，其中：

一可在該安全操作狀態下使用之最終密鑰被利用於該

記憶卡中；

該記憶卡可加以組態；

該記憶卡之硬體測試機制不能加以測試；且

該記憶卡之軟體測試機制不能加以測試。

16. 一種快閃記憶卡，其包括：

一加密引擎，其加密並解密儲存於該快閃記憶卡中之資料；

一用於測試該快閃記憶卡之第一操作狀態，其中該快閃記憶卡產生一第一密鑰，該第一密鑰使用該加密引擎來賦能加密及解密；

一用於該快閃記憶卡之消費者使用之第二操作狀態，其中該快閃記憶卡操作為一安全記憶卡，其中該快閃記憶卡利用一第二密鑰來加密及解密儲存於該快閃記憶卡中之資料，在該第二操作狀態期間該第二密鑰之一值為恆定的且儲存於該快閃記憶卡之一非揮發性記憶體中，

界定一旁路操作狀態之一第三操作狀態，其中該快閃記憶卡操作為一非安全記憶卡，且其中在該第三操作狀態中去能該加密引擎、賦能該快閃記憶卡之硬體測試、賦能該快閃記憶卡之韌體測試，且

其中該快閃記憶卡經組態以使得該快閃記憶卡在自該第二狀態轉換之後不能重新進入該第二操作狀態，且

其中以該第一密鑰加密之資料不能以該第二密鑰來解密，且以該第二密鑰加密之資料不能以該第一密鑰來解密，且

其中該加密引擎可在該第一狀態下加以測試，但當該快閃記憶卡處於該第二狀態時，不能讀取在該快閃記憶卡處於該第一狀態時加密之資料。

17. 如請求項16之快閃記憶卡，其中每當電力開啟該快閃記憶卡時，該第一密鑰之值改變。

18. 如請求項16之快閃記憶卡，其中該第一密鑰之該值係恆定的。

19. 如請求項16之快閃記憶卡，其中每當進入該第一操作狀態時，該第一密鑰之該值即重新產生一次。

20. 如請求項16之快閃記憶卡，其中該第二密鑰之該值等於在該第一狀態期間最後儲存於記憶體中之該第一密鑰之該值。

21. 如請求項16之快閃記憶卡，其中在該第一狀態下，硬體及韌體測試機制可用於測試。

22. 如請求項16之快閃記憶卡，其中在該第二狀態下，硬體及韌體測試機制不可用於測試。

十一、圖式：

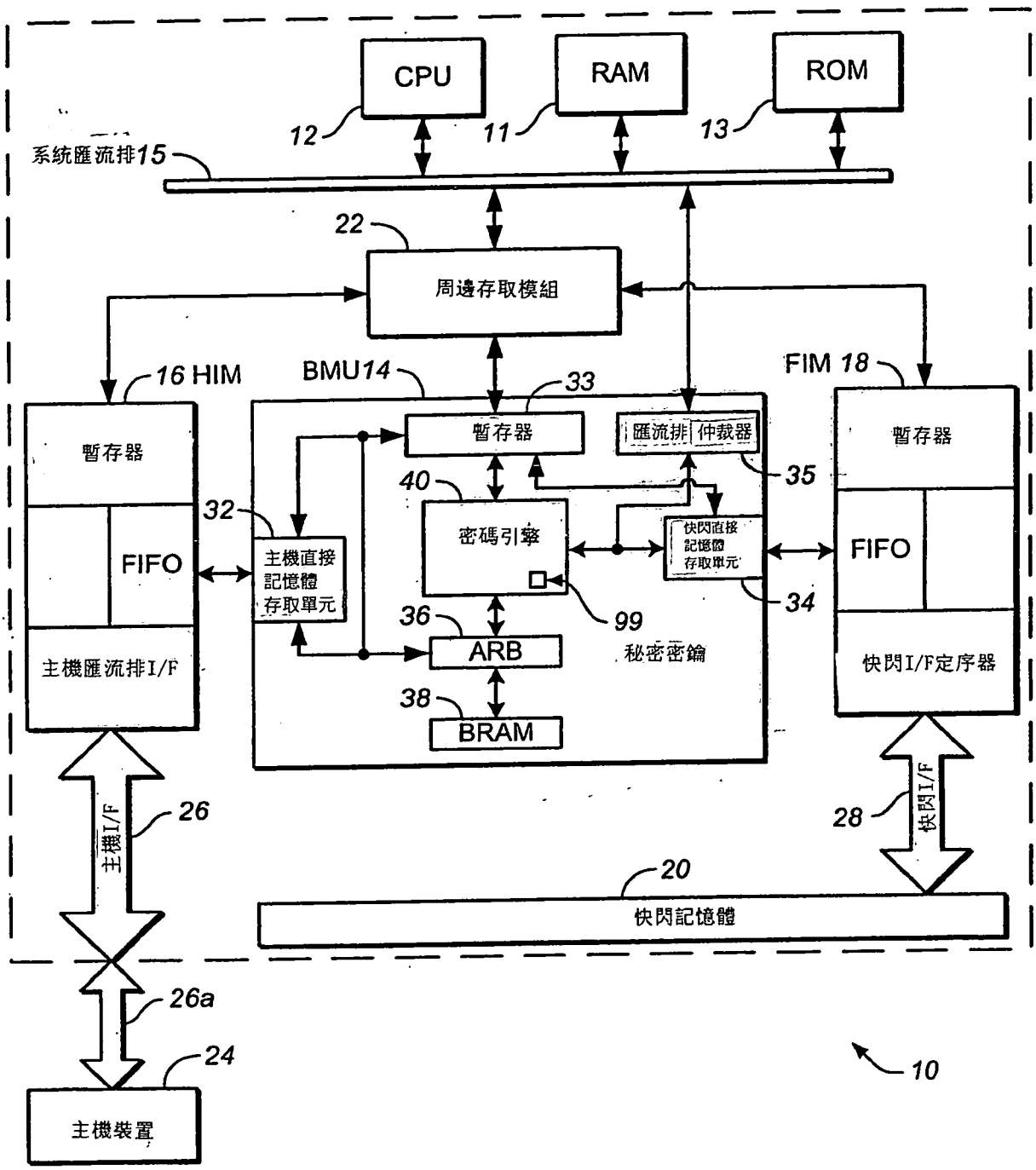

CPU
RAM
ROM
12
11
13
系統匯流排15
22
周邊存取模組
16 HIM
BMU14
33
FIM 18
暫存器
匯流排 仲裁器
35
40
密碼引擎
32
主機直接記憶體存取單元
FIFO
主機匯流排I/F
36
ARB
99
秘密密鑰
38
BRAM
快閃直接記憶體存取單元
34
暫存器
FIFO
快閃I/F定序器
主機I/F
26
28
快閃I/F
20
快閃記憶體
26a
24
主機裝置
10

圖1A

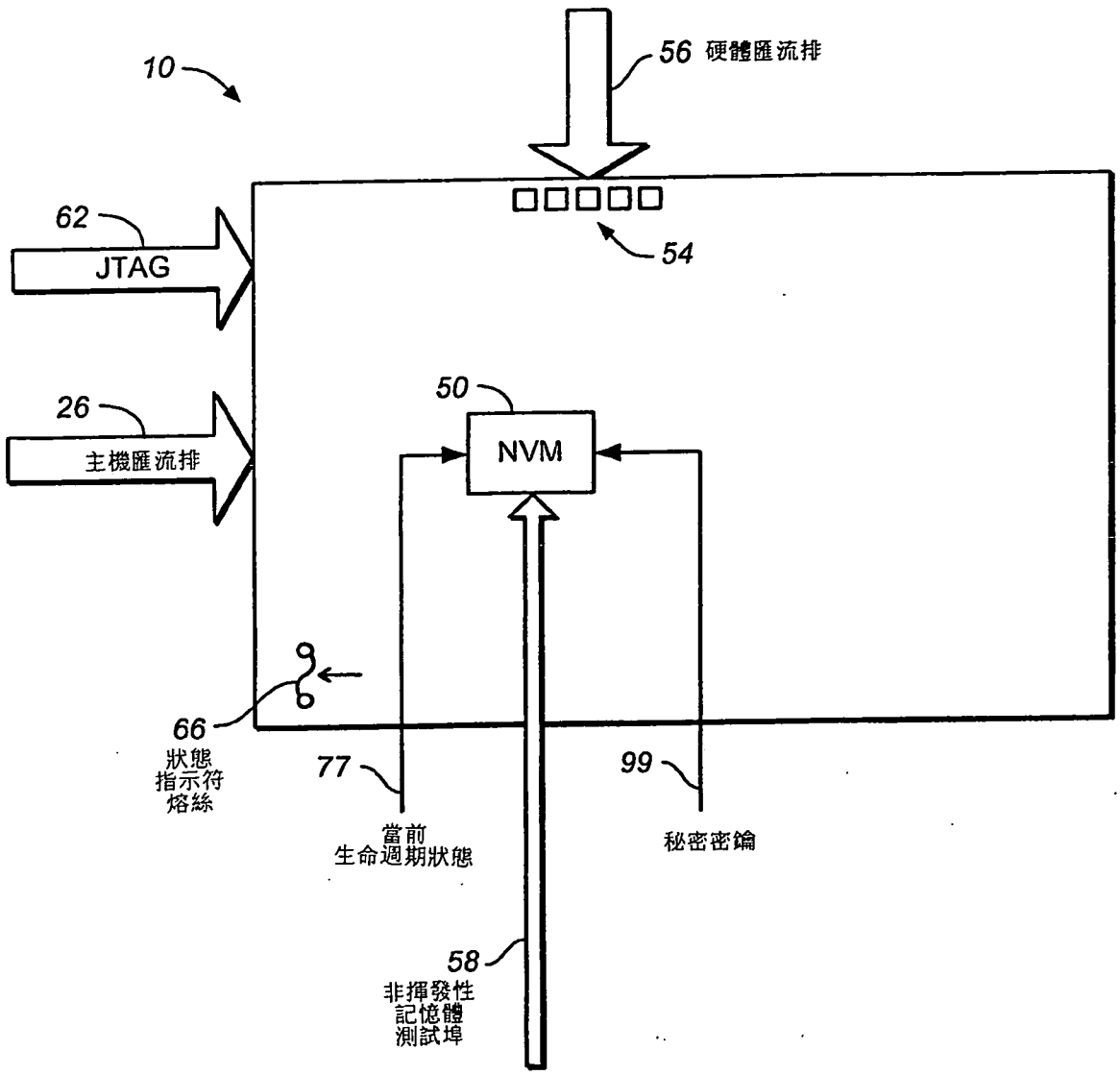

10
56 硬體匯流排
62
JTAG
54
26
主機匯流排
50
NVM
66
狀態
指示符
熔絲
77
當前
生命週期狀態
99
秘密密鑰
58
非揮發性
記憶體
測試埠

圖1B

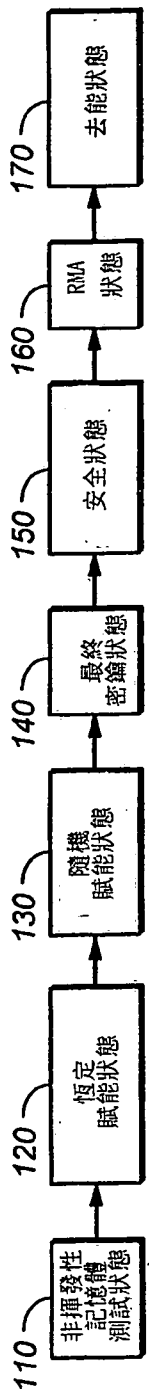


圖2A

狀態	密鑰生成	非揮發性記憶體測試	硬體測試	韌體測試	密碼引擎
110	於每次電力開啟時重新生成	E	E	E	D
120	恆定且硬式佈線	D	E	E	E
130	生成一次	D	E	E	E
140	生成一次	D	D	D	E
150		D	D	D	E
160	於每次電力開啟時重新生成	D	E	E	E
170	-	D	E	E	D

圖2B

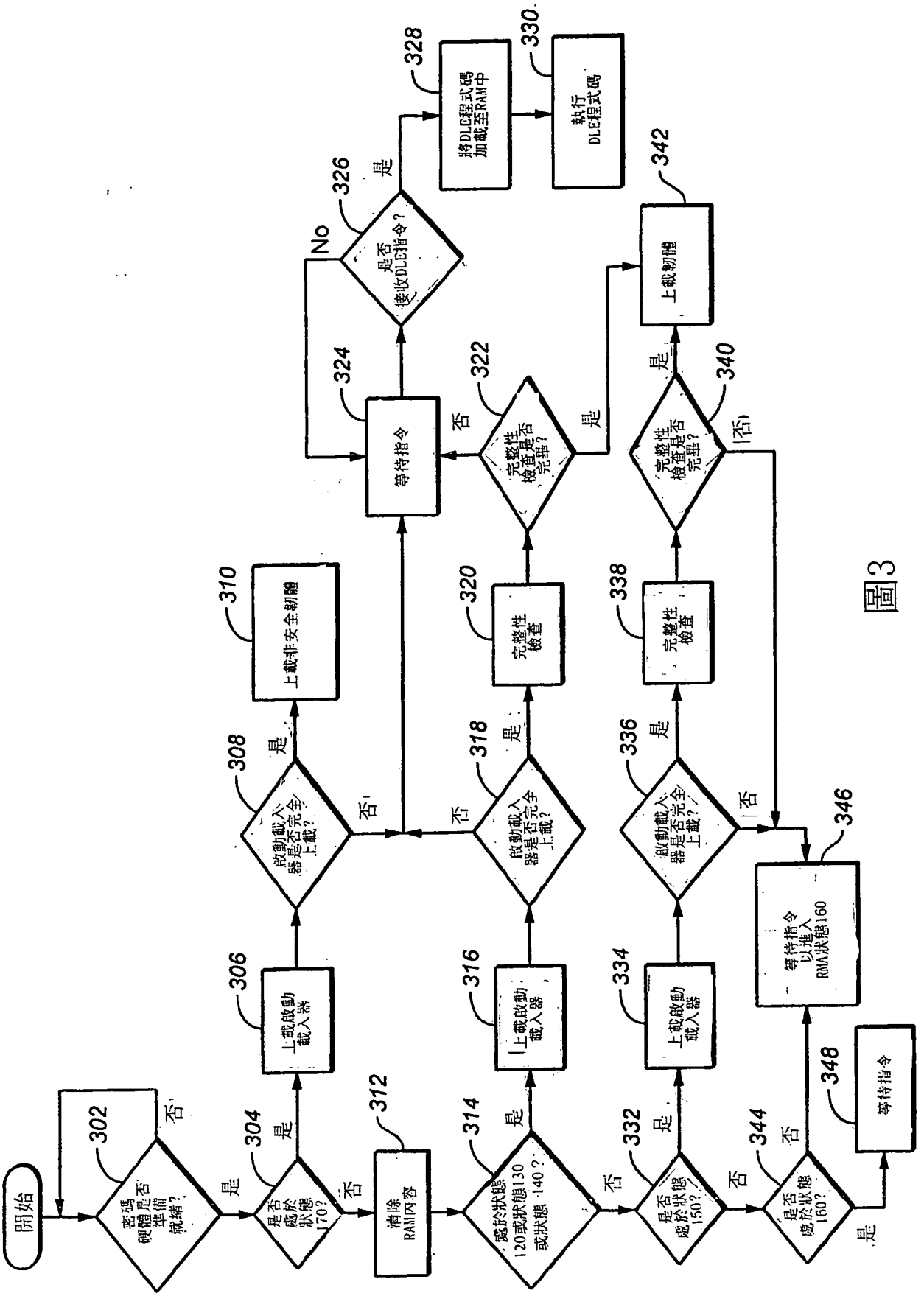

開始
302
密碼體是否準備就緒?
否
是
304
是否處於狀態170?
是
否
306
上載啟動載入器
308
啟動載入器是否完全上載?
是
否
310
上載非安全韌體
312
清除RAM內容
314
處於狀態130或狀態140?
是
否
316
上載啟動載入器
318
啟動載入器是否完全上載?
是
否
320
完整性檢查
322
完整性檢查是否完畢?
是
否
324
等待指令
326
是否接收DLC指令?
是
No
328
將DLC程式碼加載至RAM中
330
執行DLC程式碼
332
是否處於狀態150?
是
否
334
上載啟動載入器
336
啟動載入器是否完全上載?
是
否
338
完整性檢查
340
完整性檢查是否完畢?
是
否
342
上載韌體
344
是否處於狀態160?
是
否
346
等待指令以進入RMA狀態160
348
等待指令

圖3