



申請日期	91. 2. 7
案 號	9 1 1 0 2 2 0 5
類 別	G07F 7/12, G06F 13/00

A4
C4

525104

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	用以儲存演算法碼具易失性記憶體之保全模組
	英 文	"SECURITY MODULE WITH VOLATILE MEMORY FOR STORING AN ALGORITHM CODE"
二、發明人	姓 名	馬可士 詹奇 MARCUS JANKE
	國 籍	德國 GERMANY
	住、居所	德國慕尼黑市史畢進普拉茲路3號 SPITZINGPLATZ 3, 81539 MUNICH, GERMANY
三、申請人	姓 名 (名 稱)	德商億恒科技公司 INFINEON TECHNOLOGIES AG
	國 籍	德國 GERMANY
	住、居所 (事務所)	德國慕尼黑市馬汀街53號 ST.-MARTIN-STR. 53, 81669 MUNICH, GERMANY
	代 表 人 姓 名	1. 彼得 季里茲 PETER ZEDLITZ 2. H. 舒伯特 H. SCHUBERT

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6

B6

本案已向：

國（地區） 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權德國 2001年02月16日 10107373.9 ☒有☐無主張優先權

有關微生物已寄存於： 寄存日期： ，寄存號碼：

裝

訂

線

五、發明說明(1)

描述

本發明和保全模組有關，其可用於例如付費電視應用、信用卡、電話卡或信任平台模組(TPM)嵌入卡，且本發明特別和保全演算法碼有關，其用於在保全模組及終端機模組間通訊以防止外部駭客攻擊。

由於非現金付費交通之日漸進步以及資訊技術網路已深入每一家庭(像是例如付費電視應用)，對於密碼演算法之需求已有增加之趨勢俾能執行數位簽章、認證以及加密等工作。一般所熟知之密碼演算法包含非對稱性密碼演算法(像是例如RSA演算法)、對稱性加密處理(像是例如DES處理)、以及基於圓弧曲線進行之處理等等。

為能在一方面能於每日以可接受之速度充份執行密碼演算法所訂定之各項運算，且在另一方面儘可能便利地供使用者使用，乃使用諸如智慧卡或簽章卡等晶片卡，其包含個殊加密處理器用以執行密碼演算法。植基於特定應用或用途，該加密處理器必須能依據各式密碼演算法執行認證、簽章、証明及加密或解密。除了密碼演算法之應用外，該晶片卡尚包含所儲存之晶片卡個殊資訊，像是加密金鑰等，而以信用卡而言晶片卡儲存之資訊可包含信用卡號、帳號及收支，而以付費電視智慧卡而言則為智慧卡辨識碼(ID)、客戶ID以及其化和客戶有關之資訊。一晶片卡可令該晶片卡之使用者執行某些交易，像是透過指定終端機或其他諸如付費電視解碼器之終端裝置以簡單有效之方式進行扣款(debiting)，在此考量下，用於該晶片卡上

五、發明說明(2)

之密碼演算法可對該晶片卡交易提供保護使其免為犯罪行為所乘。

為保護晶片卡終端機系統免受犯罪行為破壞，在終端機及晶片卡間乃使用特殊協定，包含(例如)利用該晶片卡處理器內之密碼演算法進行相互認證及加密、解密處理。傳統晶片卡之問題為用於該密碼功能(例如用於加密)之演算法係以固定式電路型式及/或儲存型式固定於晶片卡上，因此易為潛在駭客所竊取。駭客對晶片卡內之密碼演算法竊取之手段包含(例如)對密碼處理器之電路結構進行化學移除以及對暴露之半導體結構進行光學分析等。若駭客持續自所持有之晶片卡擷取密碼演算法，則該駭客將可基於其對該密碼演算法之認知且可能利用相同方式對該晶片卡進行某種攻擊以獲取諸如晶片卡之秘密金鑰或其他關鍵保全資料。當晶片卡之密碼演算法為駭客所知時，該等駭客將極有可能攻擊成功，且晶片卡交易之保全鏈將暴露於危險下。

就傳統晶片卡而言，資訊竊取問題僅藉由特殊硬體處理或諸如隱匿接觸處理技術進行反制，在此種處理作業下，其試圖防止對移除半導體結構進行光學分析及防止對所屬電子電路進行瞭解，其手段係藉由隱匿接觸及對於所屬閘極使用特殊設計圖庫而達成，其中各類閘極(像是AND閘或OR閘極)僅因其換離不同而相異。此般硬體隱匿處理著實增加了潛在駭客獲取晶片卡內密碼演算法之成本，但是另一方面亦增加了電路及設計之花費、晶片面積且因此分

五、發明說明 (3)

別增加了密碼術處理器及晶片卡之成本。

對於晶片卡製造廠商而言，一晶片卡具有較高安全性可防制外部攻擊且減少電路成本是非常具有吸引力的，特別對於具有高市場潛力以及大量生產數目之晶片卡更需如此。

本發明之目的在於提出一保全模組、一終端機及一處理作業，使具有較高階安全之保全模組交易得以確保。

上述之保全模組係依據申請專利範圍第1項、終端機係依據申請專利範圍第13項、而作業係依據申請專利範圍第11、14或15項而達成。

本發明乃基於發掘一保全模組(像是例如晶片卡)，予以提昇其安全性俾防制外部攻擊，其中至少該演算法碼之一部份非固定儲存於保全模組上，而是恰在該終端機和該保全模組進行通訊期間將此演算法碼之遺漏部份儲存於該保全模組之易失性記憶體內，該演算法碼包含關鍵保全之功能(像是扣款(debiting)功能)、或密碼演算法、或是一般有關密碼處理功能等，其可因此有效地避免將保全模組上之完整演算法碼暴露於潛在駭客之威脅下，且因此對於該潛在攻擊者將不可能存取該演算法碼以竊取秘密金鑰或其他私密資料，且無法進而使用相同手段進行特定攻擊行動(像是嚐試錯誤攻擊或資訊漏洩攻擊等)。易言之，對一潛在攻擊者而言，其幾乎不可能有機會濫用該演算法碼(像是一加密演算法)，因為該演算法碼已非永久以完整型式儲存於該保全模組內，且因此該駭客將無法隨意操控一終

五、發明說明(4)

端機行非法作為。

依據本發明，一諸如晶片卡之保全模組包含一信任平台模組(TPM)，其以電腦嵌入模組或一智慧卡之型式存在並伴隨一終端機使用(其附有一資料介面和該終端機耦合)，且自該終端機接收至少一部份之該演算法碼或完整演算法碼，該保全模組亦包含一能量介面以接收能量供應，且包含一易失性記憶體用於儲存經由該資料介面接收之部份演算法碼或完整演算法碼，該易失性記憶體和該能量介面耦合以獲得能量供應。一處理器用以執行該演算法碼以獲致一演算法碼運算結果並將其傳送至終端機。其餘未經接收之演算法碼可儲存於(例如)一非易失性記憶體內(像是一唯讀記憶體-ROM)，若無足夠之能量供應，則該保全模組內之該非易失性記憶體將不會擁有完整演算法碼，且因此對一潛在駭客而言，其將無法獲取完整演算法碼。

一適於使用上述保全模組之終端機(像是自動提款機、具有卡面讀取器之行動電話、一付費電話解碼器或一具有可嵌入TPM之電腦)包含(例如)一和該保全模組耦合之資料介面，且該資料介面將部份演算法碼或完整演算法碼自該終端機傳輸至該保全模組之該易失性記憶體，並自該保全模組接收該演算法碼結果，該終端機亦包含一能量介面以將供應能量傳送至該保全模組。

依據一具體實施例，一認證(像是基於挑戰及回應機制之認證機制)係於該終端機及保全模組通訊時在該終端機

五、發明說明(5)

及保全模組間進行，自該終端機傳送至該保全模組之演算法碼將以加密及簽章型式執行以防制該終端機及保全模組間通訊鏈結遭竊取或挪動。為達此目的之該終端機或保全模組包含適當之裝置以分別執行認證、加密及解密、以及簽章及簽章檢測。為增加安全性且為有效防止潛在駭客對該演算法碼傳輸部份進行擷取，該保全模組可附加一監測裝置，使其在滿足預設安全狀況之情況下，清除該易失性記憶體，此類安全狀況可包含中斷、供應電壓及/或受保全模組影響之處理器或系統時序或其他作業參數出現不規則及波動，後者安全狀況和終端機互動有關。若該監測裝置並未真正地開始清除該記憶體，則該易失性記憶體及所儲存之部份演算法碼最終會分別於該終端機及保全模組通訊結束時或能量供應中斷時藉由自該終端機撤回或移除該保全模組而予以清除，而該部份之演算法碼將可不再受潛在駭客掌控加諸各類攻擊行為。

為進一步減少系統遭受攻擊，吾人可自該終端機間續將該演算法碼以更改型式傳送至保全模組，且藉由重覆進行以將每次新傳送之演算法碼更改部份儲存於該易失性記憶體內以取代該演算法碼之原先儲存部份，這使得當終端機及保全模組進行通訊時能在密碼演算法中產生可能之變化(像是例如付費電視應用)，且亦可在每次於終端機及保全模組間啟始通訊時改變演算法碼(像是例如信用卡)，其將進一步增加一潛在駭客試探或發掘所使用演算法碼所需之成本。

五、發明說明(6)

除了保護該保全模組之演算法碼免於為一潛在駭客竊取之外，本發明之另一優點為其可應用至各類應用領域，像是(例如) EC卡、信用卡、多重應用卡或付費電視智慧卡等等，植基於特定應用，由該保全模組所接收之該演算法碼或保全功能包含和關鍵保全功能有關之部份碼或該保全模組之一或多項密碼演算法。對於晶片卡生產者或保全模組製造者而言，各類複雜之應用以及對抗潛在攻擊之安全性之提昇亦意謂著將使市場之接受度增加，且可因此增加市場銷售盈餘。除此之外，保全模組之安全性係以低成本方式進行提昇的，因為所增加之安全性係藉由將軟體載入易失性記憶體而達成的。用以保護演算法碼免於遭受上述潛在攻擊者威脅之傳統及複雜之硬體解決方法可採附加方式或由較低價之硬體技術予以取代，因為關鍵安全性之功能或保全模組所使用之密碼演算法並非永久儲於晶片卡上。

本發明之進一步發展及進一步各項具體實施例係定義於所附之申請專利範圍內。

本發明之較佳具體實施例將於以下參考所附圖示進行詳細說明，其中：

圖1 顯示一圖示說明依據本發明在晶片卡和一終端機進行通訊時之作業順序；

圖2 顯示依據本發明之具體實施例之晶片卡結構方塊圖；及

圖3 顯示依據本發明之具體實施例之終端機架構。

五、發明說明(7)

吾人應注意，以下本發明有關晶片卡應用之特殊具體實施例之詳細描述僅為範例說明之目的，且本發明亦可應用於其他保全模組(像是以嵌入式卡型式存在之TPMs)，以下描述將可輕易地轉換至此類相關應用，因此，以下描述論及和晶片卡有關之終端機(像是(例如)自動提款機)亦是作為範例說明之目的，依據本發明之終端機在其他應用領域中亦可為(例如)具有一TPM嵌入座之電腦、或具有一智慧卡插於讀卡器之行動電話、或一般具有能和該保全模組通訊之任何裝置。

現請先參考圖1，圖1說明在一終端機和一晶片卡通訊期間之作業順序，其在一晶片卡和一終端機介接時進行。以收費式無線電廣播為例，該晶片卡可為(例如)一付費式TV智慧卡，且該終端機可為一付費TV客戶之個別之終端裝置或解碼器。而在該晶片卡為信用卡之情況下，該終端機則為(例如)提款機等。

圖1說明兩相鄰之晶片卡10及終端機20位於具有圓角狀之方塊內，位於其下則為該晶片卡10和該終端機20進行通訊或互動時之各項步驟，其藉由箭號及方塊以其出現順序依次向下顯示，該等箭號之方向指出資料進行傳輸之資料流方向，而該等方塊則代表在晶片卡10上執行之動作。

顯示於圖1之步驟其前提為在該終端機及晶片卡間之通訊已有可能產生，例如，當該晶片卡 and 該終端機介接時，在此情況下，該終端機20可為非接觸式或接觸式終端

五、發明說明(8)

機，且因此該通訊連結可不經由接觸產生或藉由接觸而產生。為了執行必要之進一步通訊，晶片卡10必須自終端機20獲取能量供應，其亦可透過電磁輻射之非接觸方式或以接觸方式達成。在終端機20及晶片卡10之間通訊連結已完成構建且所供應之能量已傳送至晶片卡10之後，可先行執行啟始化步驟，像是(例如)雙方在相關通訊協訂上能相互一致。

當執行供應能量至晶片卡10(未顯示)、及在終端機20及晶片卡10間建立通訊連結以及啟始該通訊作業等步驟完成後，步驟30將執行終端機20及晶片卡10間之相互認證(例如依據挑戰及回應進行之認證作業)。該相互認證可包含(例如)由卡片使用者進行個人識別碼(PIN)輸入，其中該相互認證30利用(例如)儲存於該晶片卡10上之晶片卡個殊資料(像是例如晶片卡識別號碼及個人識別碼)和儲存於該晶片卡上之晶片卡金鑰及儲存於該晶片卡上且代表密碼演算法(像是例如一對稱式或非對稱式密碼演算法)之認證碼進行通聯，該認證作業在於確保僅有經允許之晶片卡可和經允許之終端機進行通聯。若該認證產生錯誤，則終止該通訊連結。

在成功完成相互認證時30，步驟40之終端機20即以加密及簽章型式傳送部份之演算法碼至晶片卡10，所傳輸之該演算法碼之加密部份可保護該傳輸資料免於遭受潛在攻擊者之竊取，而晶片卡10之位於終端機20內之簽章在於保證該演算法碼傳輸部份為原稿。為將該演算法碼之傳

五、發明說明(9)

輸部份解密且為檢測該簽章及執行相互認證30，晶片卡10包含適當之認證、解密及簽章檢測裝置，其由部份硬體及儲存於晶片卡之非易失性記憶體之數碼(像是例如認證碼)所組成。該相互認證30以及該加密及簽章40所使用之密碼演算法可包含對稱式或非對稱式密碼作業，像是例如RSA或DES演算法或任何其他密碼演算法亦可。

若簽章檢測結果顯示該簽章係屬偽造，則中斷終端機20及晶片卡10間之通訊，且可訂下規則使該晶片卡10不再進行原預設處理時間長度之處理作業，其可因此避免潛在攻擊者竊取終端機20及晶片卡10間之通訊連結並在晶片卡10正進行數碼取存時將"假(false)"數碼輸入至該晶片卡10之易失性記憶體內，而導致(例如)儲存於晶片卡10之秘密資料洩漏。

若簽章檢測顯示該簽章為真，則以加密或解密型式將該演算法碼之傳輸部份儲存於晶片卡10之易失性記憶體中(步驟50)，基於以加密或解密儲存之型式，該演算法碼會在儲存之前或在為晶片卡10之密碼處理器使用之前進行解密。步驟40所傳輸之部份演算法碼可包含一或複數個和晶片卡10關鍵保全相關之功能(像是(例如)用以對晶片卡10進行匯出之扣款(debiting)或入帳功能)，或是包含用以在進一步通訊步驟期間使用一密碼演算法之必要程式碼，像是(例如)一對稱性或非對稱性密碼作業、RSA演算法、依據DES標準之加密處理、橢圓曲線處理法或其他密碼演算法等(並不限於上述之演算法)。以付費TV應

五、發明說明(10)

用為例，該演算法碼包含(例如)和收費節目電視資料之解密有關之資訊(像是(例如)和電視資料影像之影像線條反覆變換有關之資訊)。因此僅當終端機20及晶片卡10間之通訊進行時，所保護之演算法碼方會以完整型式顯現於晶片卡10上。

在步驟60中，位於晶片卡10之處理器現在使用並處理以完整型式儲存於晶片卡10上之演算法碼。以先前所述及之付費TV為例，晶片卡10之處理器依據所儲存之演算法碼執行(例如)電視影像之影像線條重行變換。在一晶片卡10之扣款應用中(像是(例如)電視付費卡)，其使用(例如)代表一扣款或入帳功能之演算法碼執行該晶片卡10之入帳或扣款收支作業。而以信用卡應用為例，步驟60包含(例如)利用晶片卡10之密碼處理器處理代表一密碼演算法之演算法碼以進行(例如)金額轉匯要求。

在步驟70中，儲存於易失性記憶體內之部份演算法碼再次清除，而清除該演算法碼之作業可藉由(例如)卡片使用者自終端機20取出晶片卡10且因此中斷終端機20對晶片卡10之能量供應而達成。為了防止潛在攻擊者嚐試保留儲存於易失性記憶體(例如一RAM)內之部份演算法碼資料而獲致完整演算法碼，晶片卡10可配賦一特別監測裝置以主動清除晶片卡10之易失性記憶體，且在監測作業發現一特定安全狀況產生像是系統時序中斷、能量傳輸供應中斷或顯示其他可能之攻擊時(像是電壓波動等等)即主動清除易失性記憶體。因此，在晶片卡10於終端機20

五、發明說明 (11)

使用之後，或是和該通訊程序互動之後，該演算法碼將不再出現於晶片卡10上，且因此將不再暴露於潛在攻擊者之潛在攻擊及竊取之危險之下。一持有晶片卡之潛在攻擊者無法基於完整演算法碼進行安全資訊計算，因為該演算法碼無法為攻擊者完整存取，因此可有效地防止金鑰或演算法碼遭到竊取。

在已參照圖1對晶片卡及終端機之通訊期間之作業程序進行描述之後，以下將首先描述部份演算法碼自終端機傳輸至晶片卡易失性記憶體之各類可能性。若該演算法碼包含一秘密、尚不為人知之密碼演算法程式碼，則其可(例如)自該終端機完整地將該演算法碼傳輸至晶片卡之易失性記憶體內，且此秘密之密碼演算法將可有效防護免於遭受一潛在攻擊者之竊取。

若所傳輸或轉移之部份演算法碼包含一已知密碼演算法之部份程式碼，而所傳輸之部份程式碼包含(例如)進行密碼計算時使用之計算單元所在之記憶體位址，其可有效地防止持有該晶片卡之潛在攻擊者基於此密碼演算法進行保全資訊相關計算，因為執行程式碼所需之該記憶體位址以及由晶片卡處理器進行記憶體存取作業所需之記憶體位址皆無法獲得。

在一已知密碼演算法之情況下，該演算法碼之傳輸部份可包含跳躍位址以指向一指定程式碼開始處之啟始位址或是如傳統式或非傳統式之程式跳躍般指向特定部份迴圈之啟始處。在不知這些跳躍位址之情況下，一攻擊者欲自所

五、發明說明 (12)

持有之晶片卡竊取資料是十分困難的。

在一特定之例子中，用於各式密碼演算法之複數個程式碼可伴隨傳輸之部份演算法碼置於晶片卡10之內，該部份演算法碼內含終端機剛自各類密碼演算法程式碼中選定一特定演算法程式碼之啟始位址。該終端機(例如)為每一晶片卡終端機新通訊作業而自複數個密碼演算法中選取一新的密碼演算法，或者該選擇作業係在一通訊作業期間動態地執行更新數次，俾能動態地改變選擇之密碼演算法。

吾人可進一步地令傳輸之該部份演算法碼包含一必須使用於扣款或入帳或該晶片卡其他關鍵功能之程式碼啟始位址、跳躍位址或記憶體位址。進一步而言，說明於圖1之步驟40、50及60可伴隨以預定方式進行改變之傳輸部份演算法碼重覆進行，在每一次執行過程中，儲存於晶片卡易失性記憶體內之舊演算法碼將被以新傳輸之部份演算法碼覆寫，該新演算法碼然後會由該晶片卡之處理器運用，藉由此種將儲存於易失性記憶體內之演算法碼部份進行動態改變，其可獲致額外之安全防護。

請參閱圖2暨圖3，其分別顯示用於建構一晶片卡及終端機之可能具體實施例，且將於以下進行描述。圖2顯示以100表示之晶片卡方塊圖，晶片卡100包含一資料介面110、一能源介面120、一RAM 130、一處理器140以及一ROM 150。資料介面110(例如)經由一無接觸式耦合方式或經由一接觸方式和一終端機(未顯示)耦合，且可自該晶片卡至終端機間互傳資料或自終端機接收資料，資料介

五、發明說明 (13)

面110和處理器140連接，該介面所傳輸及接收之資料可分別傳輸至處理器140或自處理器傳出。能源介面120亦和終端機耦合俾自終端機處以(例如)電磁能源或一供應電壓型式獲得能源，能源介面120將供應之能源傳播至處理器140及RAM 130。

處理器140由一中央處理單元(CPU，未顯示)及由CPU控制且用於執行晶片卡100內一或多個密碼演算法之特定運算(像是例如係數或算術運算)所需之複數個密碼協同處理器組。除了控制該等密碼協同處理器之外，該CPU亦藉由資料介面110和終端機進行通訊，且對和處理器140連接之ROM 150進行記憶體存取作業。ROM 150包含(例如)晶片卡特定資訊，像是晶片卡識別碼、個人識別碼、帳號號碼、收支平衡表等。

處理器140之CPU負責一終端機和晶片卡100之通訊啟始作業，以及依據本發明在接獲演算法碼傳輸部份時進行認證、解密及簽章檢測工作，所需進行該等工作之程式碼可儲存於ROM 150內。為執行和終端機之進一步通訊(例如執行保全相關功能如自ROM 150擷取收支資訊或執行密碼演算法以進行帳號入帳/扣款交易)，處理器140之CPU係由程式碼進行程式控制，依據本發明，至少部份之該程式碼在晶片卡100和終端機通訊期間係儲存於和處理器140連接之RAM 130內，其亦可完全不儲存於(或僅部份儲存於)晶片卡100之ROM 150內。因此，如先前所述之持有該晶片卡100之潛在攻擊者無法透過處理器140執行

五、發明說明 (14)

保全資訊運算，因為其無法獲得部份之演算法碼，且其僅在該晶片卡和終端機通訊時儲存於易失性記憶體130內。

圖3顯示一方塊圖說明依據本發明具體實施例之終端機建構。編號200之終端機包含一資料介面210、一能量介面220、一和資料介面210及能量介面220連接之處理器230、以及和處理器230連接之記憶體240。資料介面210用於和相關晶片卡之資料介面耦合，俾執行終端機200及晶片卡(未顯示)間之資料交換。能量介面220亦用於和特定晶片卡之能量介面耦合，俾對其傳送供應能量。處理器230控制(例如)終端機200和晶片卡通訊期間之作業程序，且執行(例如)將進行傳輸之演算法碼(儲存於記憶體240內)之初始化、認證及加密作業、以及簽章，並將加密及簽章後之演算法碼傳送至資料介面210進而傳送至晶片卡。

吾人須注意記憶體240可能已內含(例如)具加密型式之演算法碼，故處理器230無需將該碼加密，且該碼不會存在於未編碼之文字內，亦可不存在於記憶體240內或他處。

依據先前描述，吾人應注意所舉之例子僅為特定具體實施例，例如傳輸之部份演算法碼之相互認證及加密以及簽章可在某些特定應用中省略。依據本發明之設計，至少部份之演算法碼係儲存於晶片卡之易失性記憶體內，因此對於一潛在攻擊者而言，欲刺探晶片卡之關鍵保全功能(像是加密演算法及對於晶片卡特殊資訊之存取功能)是非常

五、發明說明 (15)

困難的，因為這些資訊並非常駐於晶片卡內且因此該潛在攻擊者無法取得，而且在供應能量接收中斷之情況下，該等資訊將會消失，嚐試去保護易失性記憶體免於喪失此項功能是十分困難的，且吾人認為目前在實際應用上可能尚未能有有效解決方法。

吾人應進一步注意依據本發明之作業，依據本發明之終端機及依據本發明之晶片卡可以各類方式加以應用，相關之步驟或裝置可藉由軟體、韌體或硬體並聯合非易失性記憶體加以應用。除了上述之外，於先前所使用之晶片卡乙詞不應將其限制於卡片型式，而是亦應包含所有其他以類似方式使用之晶片載體型式。

目前實現本發明之可能作法之一包含(例如)使用Infineon AG公司之SLE66CX320P系列之處理器產品，藉由記憶體管理單元(MMU)以執行儲存於一RAM內之數碼，且該MMU控制處理器對於RAM之記憶體存取作業。在最簡單之例子中，自終端機將加密之跳躍位址或記憶體位址完成傳輸至該晶片卡後，將可有效地防止一"原始碼(native code)"或機器碼為一潛在攻擊者所載入。藉由本發明之此等簡單之實踐方式，一攻擊者將無法在晶片卡中進行保全資訊運算，因為跳躍位址及順序皆是未知的。此項觀念可藉由製作應用注意事項而分享予此一元件之客戶，且配合晶片卡控制器軟體及終端機軟體內之實踐方法而增加應用之安全性。

依據本發明之持有晶片卡之潛在攻擊者僅擁有已受保護

五、發明說明 (16)

之資料，但是其無法啟動帳目運作亦無法實際觸及演算法碼。藉由將保全終端機和智慧型存取防護機制結合同時搭配程式碼部份之可重覆載入性，本發明因此可達成非常高階之安全防護水準。

裝

訂

線

四、中文發明摘要(發明之名稱：用以儲存演算法碼具易失性記憶體之保全模組)

一種配合一終端機使用之保全模組(100)，其包含一和該終端機耦合之資料介面(110)用以自該終端機接收至少一部份之演算法碼或是完整演算法碼；其亦包含一能量介面(120)用以接收供應能量。一易失性記憶體(130)和該能量介面(120)耦合以獲取能量供應俾儲存經由資料介面接收之部份演算法碼或完整演算法碼，並伴有一執行該演算法碼之處理器(140)以獲取一演算法碼結果其可被傳送至該終端機。因為該保全模組(100)之易失性記憶體(130)儲存至少部份之演算法碼，依據本發明該保全模組(100)之演算法碼可有效地防護來自潛在駭客之竊取行為。

英文發明摘要(發明之名稱："SECURITY MODULE WITH VOLATILE MEMORY FOR STORING AN ALGORITHM CODE")

A security module (100) for use with a terminal comprises a data interface (110) adapted to be coupled to a terminal, for receiving at least part of an algorithm code or the complete algorithm code from the terminal, as well as an energy interface (120) for receiving supply energy. A volatile memory (130) coupled to the energy interface (120) in order to have energy supplied thereto stores the part of the algorithm code or the complete algorithm code received via the data interface, with a processor (140) implementing the algorithm code in order to obtain an algorithm code result that can be delivered to the terminal. Due to the storing of at least part of an algorithm code in the volatile memory (130) of the security module (100), according to the invention, the algorithm code of the security module (100) is effectively protected against spying out by a potential attacker.

六、申請專利範圍

1. 一種搭配一終端機使用之保全模組，其包含：
 - 一用於和一終端機耦合之資料介面(110)，該資料介面接收來自該終端機之至少一演算法碼之一部份或是完整之演算法碼；
 - 一能量介面(120)，用於接收供應之能量；
 - 一易失性記憶體(130)，用於儲存經由資料介面(110)接收之部份演算法碼或完整之演算法碼，該易失性記憶體(130)和該能量介面(120)耦合以獲得能量供應；以及
 - 一用以執行該演算法碼之處理器(140)，俾獲得演算法碼執行結果以傳送至該終端機。
2. 如申請專利範圍第1項之保全模組，進一步包含：
 - 一非易失性記憶體(150)，其用以儲存該演算法碼之其餘未接收部份。
3. 如申請專利範圍第1項之保全模組，進一步包含：
 - 一用以執行該終端機及該保全模組間認證作業之裝置(140，150)。
4. 如申請專利範圍第1項之保全模組，其中該資料介面(110)用於接收來自該終端機之以加密型式及/或簽章型式存在之部份演算法碼或完整演算法碼，該保全模組進一步包含：
 - 一用以對加密之部份演算法碼或加密之完整演算法碼進行解碼之裝置(140，150)；以及
 - 一用以檢驗該簽章之裝置(140，150)，以在該簽章為偽造時防止該演算法碼之執行。

六、申請專利範圍

5. 如申請專利範圍第1項之保全模組，進一步包含：

一用以控制處理器對記憶體存取之記憶體管理單元，且所傳輸之演算法碼部份包含演算法碼之位址。

6. 如申請專利範圍第1項之保全模組，進一步包含：

一用以監測預設保全狀況且在面臨該預設保全狀況時用以清除該易失性記憶體(130)之裝置，該安全狀況係自複數個狀況中選取，包含中斷、不規則性、以及供應電壓及系統時序及附加作業參數之波動。

7. 如申請專利範圍第1項之保全模組，其中該演算法碼包含一選取之程式碼用於執行自一群組中選擇之工作，該群組包含一對稱性密碼演算法、一非對稱性密碼演算法、一RSA演算法、一依據DES標準之密碼處理作業、一圓弧曲線處理、用於存取之存取功能以及一用以變更儲存於保全模組上數值之存取功能。

8. 如申請專利範圍第1項之保全模組，其中接收之部份演算法碼包含該演算法碼之啟始位址、用於執行該演算法碼之必要計算單元之記憶體位址、或該演算法碼之跳躍位址。

9. 如申請專利範圍第1項之保全模組，其中該易失性記憶體(130)用於將一新接收之演算法碼之變更部份覆蓋於該演算法碼之儲存部份，或是覆蓋於所儲存之完整演算法碼上。

10. 如申請專利範圍第1項之保全模組，其中該保全模組設計為一晶片卡。

六、申請專利範圍

11. 一種使用保全模組以計算一演算法碼結果之方法，其包含下列步驟：

接收(40)至少部份之演算法碼或完整之演算法碼；

以易失性方式儲存(50)該部份之演算法碼或該完整演算法碼於該保全模組之易失性記憶(130)內；

在該保全模組上執行(60)該演算法碼以獲致演算法碼結果；

傳送(60)該演算法碼結果至該終端機；以及

清除(70)該易失性記憶體(130)。

12. 如申請專利範圍第11項之處理作業，其中該清除(70)步驟包含將該保全模組自該終端機移除。

13. 一種用以搭配一保全模組使用之終端機，包含：

一用以和該保全模組(100)耦合之資料介面(210)，該資料介面自該終端機傳送至少一演算法碼之一部份或是完整演算法碼至保全模組(100)之易失性記憶體(130)，且用以自該保全模組接收該演算法碼之結果；以及

一能量介面(220)，用以傳送供應能量至該保全模組。

14. 一種使用一終端機以控制一保全模組進而自該保全模組獲得一演算法碼結果之處理作業，包含下列步驟：

傳送供應能量至該保全模組；

自該終端機傳送(60)至少一演算法碼之一部份或是完整演算法碼至該保全模組之易失性記憶體；以及

六、申請專利範圍

自該保全模組接收(60)該演算法碼之結果。

15. 一種用於在一保全模組及一終端機間通訊之方法，包含下列步驟：

自該終端機傳送(40)至少一演算法碼之一部份或是完整演算法碼至該保全模組；

以易失性方式儲存(50)該部份之演算法碼或該完整演算法碼於該保全模組之易失性記憶(130)內；

在該保全模組上執行(60)該演算法碼以獲致演算法碼結果；

傳送(60)該演算法碼結果至該終端機；以及

清除(70)該易失性記憶體(130)。

16. 如申請專利範圍第15項之~~作業~~，進一步包含：

重覆傳送複數個不同版本之該演算法碼之一部份或完整之該演算法碼；以及

將該重覆傳輸版本之該演算法碼之一部份或完整之該演算法碼儲存覆蓋於已儲存之演算法碼部份或覆蓋於儲存之完整演算法碼上。

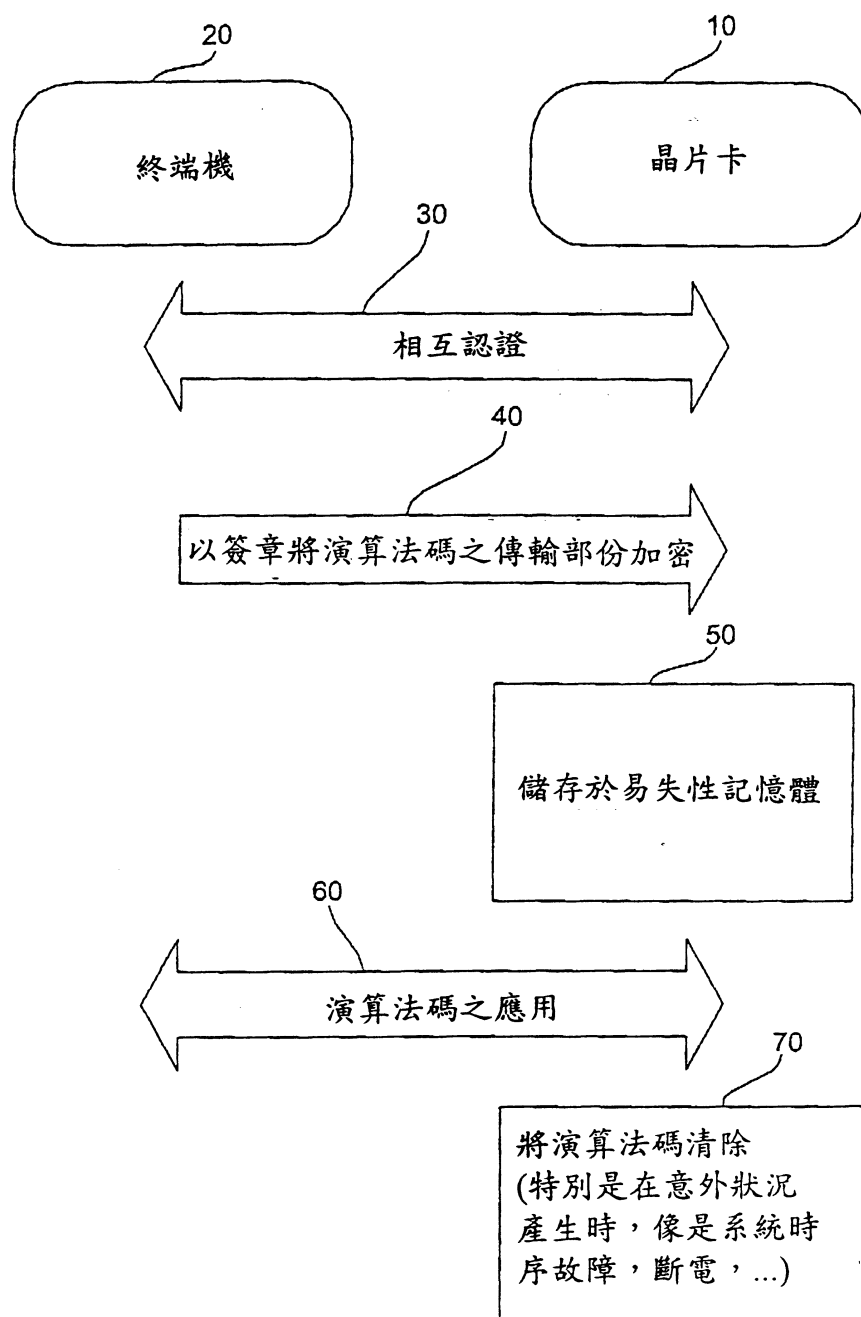


圖 1

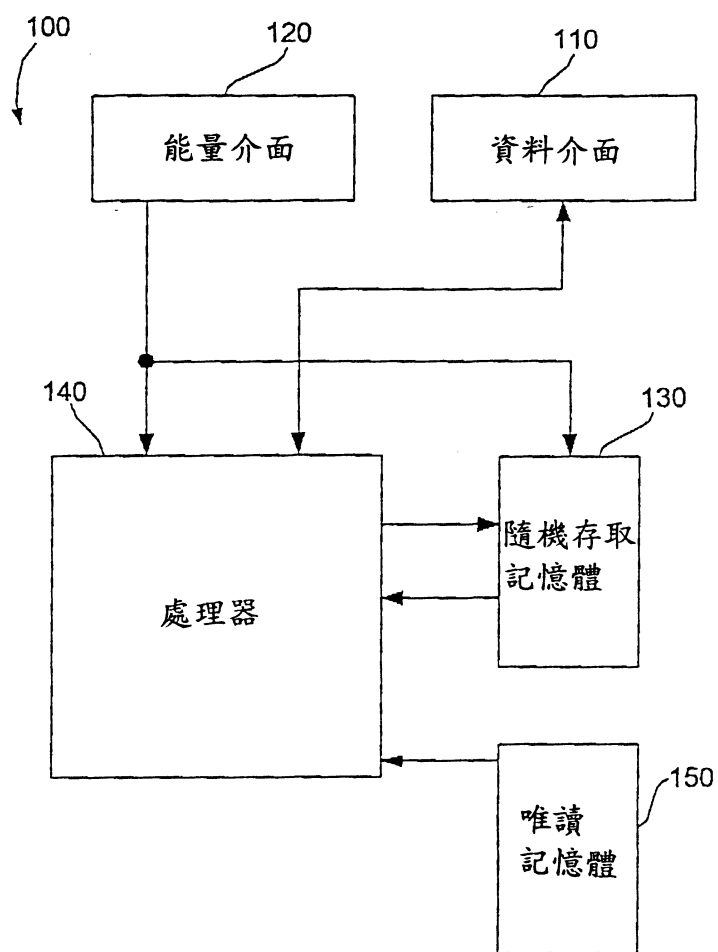


圖 2

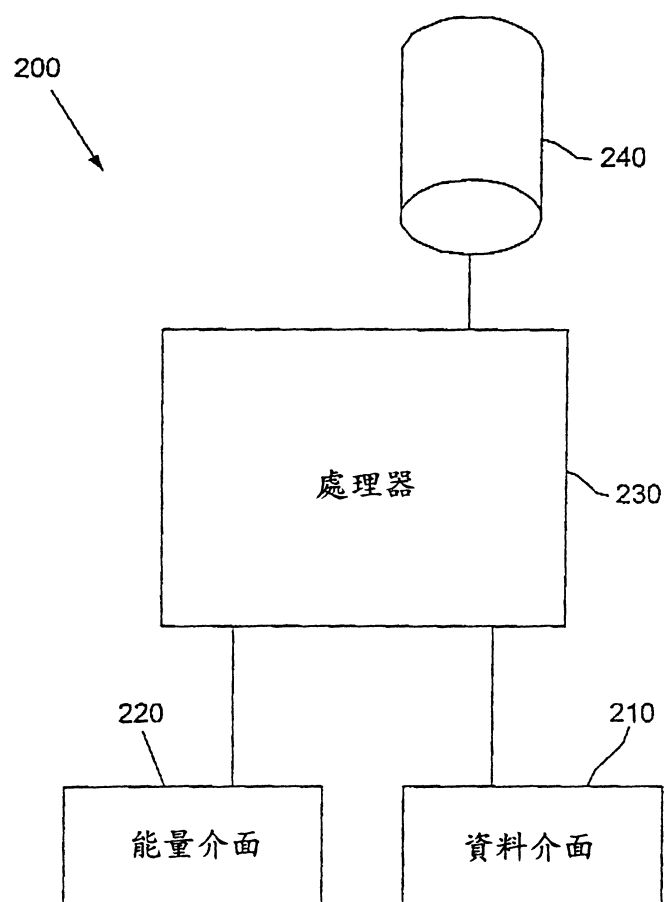


圖 3