I500042

(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 I500042 B**

(45)公告日： 中華民國 104 (2015) 年 09 月 11 日

(21)申請案號：097139850 (22)申請日： 中華民國 97 (2008) 年 10 月 17 日

(51)Int. Cl.： *G11C7/24 (2006.01)*

(30)優先權：2007/10/17 美國 11/873,980

(71)申請人：菲力裝置管理有限公司 (美國) VALLEY DEVICE MANAGEMENT LLC (US)
美國

(72)發明人：奇沛堤爾 弗瑞迪 CHERPANTIER, FREDRIC (FR)

(74)代理人：陳長文

(56)參考文獻：

US	5581978	US	2002/0169960A1
US	2006/0023486A1	US	2006/0026417A1
US	2006/0026569A1	WO	01/63994A2

審查人員：蕭明椿

申請專利範圍項數：26 項 圖式數：13 共 77 頁

(54)名稱

確保資料免於竄改攻擊之竄改反應性記憶體裝置

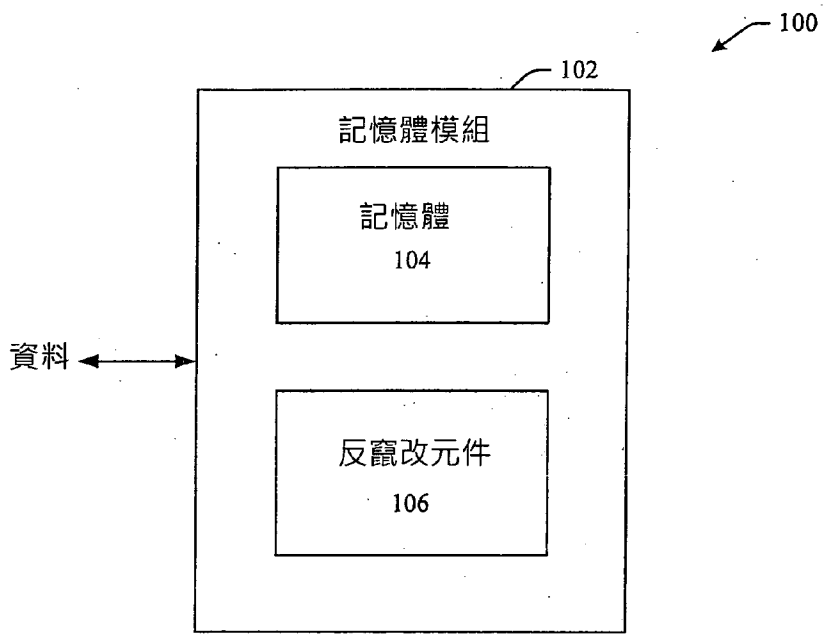
TAMPER REACTIVE MEMORY DEVICE TO SECURE DATA FROM TAMPER ATTACKS

(57)摘要

本發明提出一種可幫助保全與記憶體相關聯的資料免於竄改的系統與方法。反竄改元件可偵測與記憶體及/或儲存於該記憶體中或與該記憶體相關聯的資料相關聯的竄改攻擊或竄改企圖並對於這樣的竄改攻擊/企圖作出反應，而該反竄改元件可提供竄改攻擊/企圖的證據、提供竄改攻擊/企圖的回應、及/或抵擋竄改攻擊/企圖。該反竄改元件可與包含記憶體裝置模組且容納在電子裝置中的記憶體模組結合，且該記憶體模組可改變色彩狀態以提供竄改證據。放置視窗元件在該電子裝置的該外殼上，使得該使用者能看到該記憶體模組，故該使用者可察覺與該模組相關聯的竄改攻擊已經發生。

Systems and methods that can facilitate securing data associated with a memory from tampering are presented. A counter tamper component can detect tamper attacks or tamper attempts associated with a memory and/or data stored therein or associated therewith and reacts to such tamper attacks/attempts, as the countei tamper component can provide evidence of, provide a response to, and/or resist tamper attacks/ attempts. The counter tamper component can be associated with a memory module that includes a memory device(s)module and is contained in an electronic device and the memory module can change a color state to provide evidence of tampering. A window component is positioned on the casing of the electronic device so that the memory module is visible to the user so the user can perceive that a tamper attack associated with the module has occurred.

100・・・系統
102・・・記憶體模組
104・・・記憶體
106・・・反竄改元件



第 1 圖

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：97139850

※申請日：97.10.17 ※IPC分類：G11C 7/24(2006.01)

一、發明名稱：（中文/英文）

確保資料免於竄改攻擊之竄改反應性記憶體裝置

TAMPER REACTIVE MEMORY DEVICE TO SECURE DATA FROM TAMPER ATTACKS

二、中文發明摘要：

本發明提出一種可幫助保全與記憶體相關聯的資料免於竄改的系統與方法。反竄改元件可偵測與記憶體及/或儲存於該記憶體中或與該記憶體相關聯的資料相關聯的竄改攻擊或竄改企圖並對於這樣的竄改攻擊/企圖作出反應，而該反竄改元件可提供竄改攻擊/企圖的證據、提供竄改攻擊/企圖的回應、及/或抵擋竄改攻擊/企圖。該反竄改元件可與包含記憶體裝置模組且容納在電子裝置中的記憶體模組結合，且該記憶體模組可改變色彩狀態以提供竄改證據。放置視窗元件在該電子裝置的該外殼上，使得該使用者能看到該記憶體模組，故該使用者可察覺與該模組相關聯的竄改攻擊已經發生。

三、英文發明摘要：

Systems and methods that can facilitate securing data associated with a memory from tampering are presented. A counter tamper component can detect tamper attacks or tamper attempts associated with a memory and/or data stored therein or associated therewith and reacts to such tamper attacks/attempts, as the counter tamper component can provide evidence of, provide a response to, and/or resist tamper attacks/attempts. The counter tamper component can be associated with a memory module that includes a memory device(s) module and is contained in an electronic device and the memory module can change a color state to provide evidence of tampering. A window component is positioned on the casing of the electronic device so that the memory module is visible to the user so the user can perceive that a tamper attack associated with the module has occurred.

四、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：

100　系統

102　記憶體模組

104　記憶體

106　反竄改元件

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種系統及方法，其可幫助確保記憶體裝置中的資料免於竄改該記憶體裝置及/或儲存在該記憶體裝置或與該記憶體裝置相關的資料的企圖。

【先前技術】

許多種記憶體裝置可使用來維持與儲存用於不同電腦與相似系統的資料與指令。具體說來，快閃記憶體是一種可覆寫（rewrite）且不需消耗電力就能保持內容的電子記憶體媒體。不同於可抹除單一位元組（byte）之動態隨機存取記憶體（dynamic random access memory，簡稱DRAM）裝置與靜態隨機存取記憶體（static random access memory，簡稱 SRAM）裝置，快閃記憶體裝置通常抹除固定的多位元資料段（block）或磁區（sector）。快閃記憶體技術可包含例如 NOR 快閃及/或 NAND 快閃。NOR 快閃是從電子可抹除可程式化唯讀記憶體（electrically erasable programmable read only memory，簡稱 EEPROM）晶片技術發展而來，其中，不同於快閃，其可抹除單一位元組；而 NAND 快閃是從 DRAM 技術發展而來。快閃記憶體裝置相較於許多其他記憶體裝置可較不貴且可較密集，意謂著快閃記憶體裝置可在每單位面積儲存更多資料。

快閃記憶體至少在某種程度上已經變得普遍，這是因為它結合了 EPROM 的高密度和低成本與 EEPROM 的電子可抹除性的優點。快閃記憶體是非揮發性的；它可被覆寫

且不用電力就可保持內容。它可使用在許多可攜式電子產品，例如行動電話、電腦、錄音機、拇指碟（thumbnail drive）與其相似物，也可使用在許多較大電子系統中，例如汽車、飛機、工業控制系統等等。事實上，快閃記憶體已經結合可覆寫且不需電源就能保持資料、以及小尺寸和重量輕等優點，以使得快閃記憶體裝置成為用來運送與維持資料的有用和普遍的手段。

例如快閃記憶體的非揮發性記憶體可使用來儲存與使用者相關的機密及/或個人資訊，例如銀行帳戶資訊、個人識別號碼、照片、法律文件等。其他個體（entity）可企圖獲得對於儲存在該記憶體中的這些資料的存取，而這可能造成該使用者的（例如財務的、個人的、職業的等等的）損害。因此期望以安全的方式來維持記憶體裝置中的資料，也期望使該使用者能獲知未授權個體企圖要獲得對於該記憶體裝置的非授權存取。

【發明內容】

以下提出本發明之簡化概述，以提供在此描述的某些態樣之基本理解。此概述非本發明之廣泛概觀。此外，此概述並非意欲識別本發明之關鍵或必要元件，也非意欲描述本發明之範圍。此概述的唯一目的係以簡化形式提出一些關於本發明之概念，以作為下面更詳細敘述之序言。

本發明係關於一種系統及/或方法，其可幫助確保記憶體裝置中的資料免於竄改該記憶體裝置及/或儲存在該記憶體裝置或與該記憶體裝置相關的資料的企圖。反竄改元

件（counter tamper component）可監控與含有記憶體裝置的外殼相關聯的事件及/或與該記憶體裝置相關聯的存取資訊，且可對於竄改（例如竄改事件、竄改攻擊）該外殼及/或儲存在該記憶體中的資料的企圖作出反應（例如回應（respond）、抵抗（resist）、及/或提供證據（evidence））。該反竄改元件可評估與該外殼及/或儲存在該記憶體中的資料相關聯的資訊，且可判定竄改事件是否發生或是否已經發生。依據竄改事件的種類，該反竄改元件可提供該竄改事件的證據，以使該記憶體裝置的使用者（例如所有者）能夠獲知該竄改事件、提供對於該竄改事件的回應、及/或可抵抗該竄改事件。

根據一種態樣，記憶體裝置可被容納在記憶體外殼（例如記憶體模組）中，該記憶體外殼可被包含在電子裝置外殼內，其中，該電子裝置可例如為行動電話、個人數位助理（PDA）、或智慧卡。該反竄改元件可被包含在該記憶體模組內且可與該模組和該記憶體裝置結合。該反竄改元件可提供某個體已經藉由企圖存取安全地儲存在該記憶體裝置中的資料以竄改該記憶體裝置的證據。在一個態樣中，該反竄改元件可接收已有預定數量的不成功企圖要存取保全在該記憶體中的資料的資訊，且可判定竄改事件已經發生。舉例來說，該反竄改元件可接收某個體為了存取該記憶體裝置已經企圖鑑別（authenticate）達到預定次數（例如三次）的資訊，而所有的企圖都由於該個體所提供的錯誤的鑑別資訊而不成功。該反竄改元件可提供已經發

生此種竄改事件的證據，舉例來說，藉由改變含有該記憶體裝置的該記憶體模組的顏色及/或使可在該模組上或於該模組相關聯的發光二極體（LED）發光。當該記憶體模組可被包含在該電子裝置內時，為了使該竄改的證據能夠被該使用者察覺，可將該電子裝置建構成有可位於該電子裝置的外殼上的視窗（window）或其他透明元件，以使得該使用者可看到該電子裝置內的該記憶體模組而能注意到該竄改的證據（例如該記憶體模組的色彩狀態的改變）。在一個態樣中，該記憶體模組的外殼可依照使用者的喜好來設計。

在另一態樣中，當個體企圖要實體地存取該記憶體模組或記憶體裝置的內部時（例如藉由企圖開啟該記憶體外殼），該外殼及/或被包含在該外殼中的記憶體裝置可由一種使得該外殼及/或記憶體裝置會破裂及/或破碎成好幾片的材料形成，使得該記憶體裝置無法使用、或幾乎不能用，而使得其中的資料是無法存取的、或幾乎無法存取的。

在又另一態樣中，該反竄改元件可對竄改事件提供回應。在企圖要開啟該記憶體外殼的過程中，該外殼的分解（disruption）可導致相關聯的開關被轉動，並造成電路改變（例如電路的開路（opening）、電路的閉路（closing）），而這改變可被該反竄改元件所偵測到。該反竄改元件可藉由抹除該記憶體裝置的分割區（partition）與儲存在這些分割區內的資料的全部或子集來回應該攻擊。在另一態樣中，該反竄改元件可藉由啟動（initiating）該記憶體裝置

的一個或多個元件的災難性故障（catastrophic failure）或從容性故障（graceful failure）來回應攻擊。可利用可被包含在該記憶體外殼內的輔助電路和電源來執行反竄改回應。

在另一態樣中，該記憶體裝置可被納入至涵蓋該記憶體模組以及印刷電路板（PCB）上的一個或多個路徑的「網目（mesh）」中，該電路板連接該記憶體模組上的一個或多個接腳。電子訊號可經由該記憶體模組的接腳來通過該「網目」。在企圖要從該 PCB 中移除及/或去銲（desolder）該記憶體模組的過程中，訊號的擾亂及/或連接中斷可被該反竄改元件所偵測，而因此該反竄改元件可對於該攻擊產生想要的回應（例如抹除資料、導致元件的災難性故障）。

在又另一態樣中，該反竄改元件可對竄改事件提供抵抗。可實施攻擊以獲得可從該記憶體裝置中輸出的與電磁及/或射頻相關聯的資訊，以判定與該記憶體裝置相關聯的例如密碼資訊（cryptographic information）（例如指數（exponent）、密碼協定）的資訊，以獲得對於該記憶體及/或儲存在該記憶體的內容的存取。該反竄改元件可包含可在該記憶體外殼內使用的屏蔽（shielding）以幫助抵抗這樣的攻擊，因為該屏蔽可減低或消除來自該記憶體裝置的電磁輻射及/或射頻的放射，且可因此減低基於此種電磁輻射及/或射頻的資訊的攻擊的風險。

下列敘述與附加的圖式提出本發明的某些例示態樣的細節。然而，這些態樣僅代表可利用本發明的原理的許

多方式中的其中一些態樣，而本發明係意欲包含所有此等態樣與它們的等效物。從下列本發明的實施方式，並配合所附加的圖式，將更清楚地了解本發明的其他優點和新穎特徵。

【實施方式】

本發明是參照圖式來描述，其中，全文使用相同的元件符號來指代相似的元件。在下列敘述中，為了解釋的目的，提出許多具體細節以提供本發明的徹底了解。然而，顯然也可不需要這些具體細節來實行本發明。在其他情況中，已知結構與裝置是以方塊圖形式來顯示，以幫助描述本發明。

快閃記憶體可發現使用在許多應用中，其中，可利用其相對小尺寸、高記憶體密度、與可攜性以及不需電力而保持儲存在其中之資料的能力。可使用快閃記憶體裝置以儲存使用者期望是安全及/或私密的資料，以使其他人不能存取資料。快閃記憶體裝置通常可使用在電子裝置中（例如行動電話、個人數位助理（PDA）等等），其中，可儲存個人資料及/或其他機密資料到該快閃記憶體裝置中。傳統上，該快閃記憶體裝置是位於該電子裝置內，以至於該記憶體裝置無法被該電子裝置的使用者或其他人所看見。攻擊者與其他不受歡迎的人可企圖獲得未授權的存取（例如竄改）該記憶體裝置以得到或獲知該安全/私密的資料。期望的是保護該記憶體裝置免於對該記憶體裝置本身的攻擊以及免於存取儲存在該記憶體裝置的資料或於該記憶體裝

置相關聯的資訊的非授權企圖。也期望提供該記憶體裝置的使用者（例如所有者）與其他要攻擊或存取該記憶體裝置的企圖相關的資訊。

本發明提出一種系統及/或方法，係可幫助偵測竄改記憶體裝置的企圖與保護記憶體裝置免於此種竄改企圖。該記憶體裝置（例如快閃記憶體裝置）可包含反竄改元件，該反竄改元件可幫助偵測竄改事件（例如竄改攻擊）、產生及/或提供竄改事件的證據、提供對於竄改事件的抵抗、及/或產生對要竄改該記憶體裝置及/或儲存在該記憶體裝置裡的資料的企圖的回應。

參照至圖式，第 1 圖說明依照本發明之可確保資料免於竄改的系統 100。系統 100 可包含含有記憶體 104 的記憶體模組 102，可儲存資料在該記憶體 104 內的個別記憶體位置中。

根據一種態樣，該記憶體 104 可為非揮發性記憶體，例如快閃記憶體（例如單位元快閃記憶體、多位元快閃記憶體）、唯讀記憶體（ROM）、可程式化唯讀記憶體（programmable ROM，簡稱 PROM）、電子可程式化唯讀記憶體（EPROM）、電子可抹除可程式化唯讀記憶體（EEPROM）、及/或非揮發性隨機存取記憶體（NVRAM）（例如鐵電式隨機存取記憶體（Ferroelectric random access memory，簡稱 FeRAM）、及其相似物。進一步地，該快閃記憶體可含有 NOR 快閃記憶體及/或 NAND 快閃記憶體。

記憶體模組 102 可進一步包含反竄改元件 106，該反

竄改元件 106 可與該記憶體 104 和記憶體模組 102 結合，且可幫助確保儲存在該記憶體元件 104 中的資料免於受到不受歡迎之個體（例如攻擊者）的未授權存取。該反竄改元件 106 可幫助抵抗及/或回應竄改該記憶體模組 102 及/或記憶體元件 104 的企圖，及/或可提供竄改該記憶體模組 102 及/或記憶體元件 104 的企圖的證據。

根據一種態樣，該反竄改元件 106 可被納入作為該記憶體模組 102 的外殼的一部分，且可提供竄改的證據，其中，舉例來說，如果該記憶體模組 102 的外殼被開啟則會破裂，以至於可防止該記憶體模組 102 的外殼的重新閉合（re-closure）及/或如果重新閉合該記憶體模組 102 的外殼則可察覺到該破裂。在另一態樣中，該反竄改元件 106 可被納入作為該記憶體模組 102 的外殼的一部分，此時該記憶體模組 102 的外殼可由可改變狀態（例如改變色彩狀態）的材料所形成，以對竄改事件（例如竄改攻擊）作出反應。

舉例來說，如果某個體企圖要鑑別以獲得對於該記憶體元件 104 中的資料的存取，但卻提供錯誤的認證資訊且被拒絕此種存取的要求，則該記憶體模組 102 的外殼可改變其色彩狀態，例如從第一色彩（例如黑色）成為不同的色彩（例如橘色），進而可指示該記憶體模組 102（與該記憶體模組 102 所屬的該電子裝置（未圖示））的使用者（例如所有者）有個體已經竄改該記憶體模組 102 及/或記憶體 104。可設計該電子裝置的外殼以使該記憶體模組 102 可被該使用者所看見，以使該使用者可察覺該記憶體模組的色

彩狀態的改變，在例如參照第 4a 與 4b 圖時會在此作更完整的敘述。

根據又另一態樣，該反竄改元件 106 可抵擋竄改攻擊（例如旁通道（side-channel）或其他攻擊），其中，攻擊者企圖獲得與資料操縱（例如密碼協定）相關聯的電力消耗、電磁輻射、及/或射頻放射相關聯的資訊，以得到對於儲存在該記憶體及/或該密碼協定（例如指數）中的資料的非授權存取。該反竄改元件 106 可包含一種材料，該材料可用在該記憶體模組 102 中及/或該非揮發性記憶體 104 中，且該材料可抵擋這樣的攻擊，因為該材料可防止、最小化、及/或減低由該記憶體模組 102 及/或記憶體元件 104 所發出的電力消耗量、電磁輻射、及/或射頻放射，及/或可使這些電力消耗量、電磁輻射、及/或射頻放射不易察覺。

在又另一態樣中，該反竄改元件 106 可利用許多種可用來偵測是否有從該記憶體模組 102 中移除該記憶體元件 104 的企圖的檢查電路（check circuit）（例如網目電路、轉動開關電路（throw switch circuit））。該反竄改元件 106 可提供回應給這樣的攻擊（例如竄改事件），藉由例如抹除儲存在該記憶體元件 104 內的全部或一部分資料及/或啟動一個或多個元件（例如記憶體陣列（未圖示））的故障（例如將電路元件熔接在一起），以使得該元件無法操作及/或無法存取。

參照第 2a 圖，係描述一種根據本發明之一個實施例的可幫助保全儲存在記憶體中的資料的系統 200。系統 200

可包含記憶體模組 102，該記憶體模組 102 可包含記憶體 104（例如非揮發性記憶體），該記憶體 104 可儲存資料在該記憶體 104 內的個別記憶體位置中。該記憶體模組 102 可進一步包含可幫助偵測竄改事件與提供需要的反應給此種竄改事件的反竄改元件 106，以幫助保全儲存在該記憶體 104 中的資料。該記憶體模組 102、記憶體 104、與反竄改元件 106 各能包含它們個別的功能，在例如關於系統 100 及/或系統 300 的敘述時會作更完整的敘述。

該記憶體模組 102 與其中的元件（例如記憶體 104）可與主處理器（host processor）202 結合，該主處理器 202 可為可管理通訊與執行應用程式的應用程式處理器（applications processor）。在一個態樣中，該主處理器 202 可為由電腦、行動電話、個人數位助理（PDA）、或幾乎任何其他電子裝置所使用的處理器。該主處理器 202 可產生命令（command），例如可個別執行用來從該記憶體 104 中讀取資料、寫入資料、及/或抹除資料的讀取命令、寫入命令、及/或抹除命令。寫入至記憶體 104 或從記憶體 104 中讀出的資料可經由匯流排（例如系統匯流排）（可為多位元匯流排）而在該記憶體 104 與該主處理器 202 及/或其他元件（未圖示）之間通訊或傳送。

該記憶體模組 102 可進一步包含密碼元件（cryptographic component）204，該密碼元件 204 可幫助加密及/或解密資料，以幫助保全被寫入至該記憶體 104、儲存在該記憶體 104、及/或從該記憶體 104 中讀出的資

料。根據本發明的態樣，密碼元件 204 可提供對稱密碼工具與加速器（例如兩魚演算法（Twofish）、Blowfish 密碼法（Blowfish）、AES、TDES、IDEA、CAST5、RC4 等）以確保該記憶體 104 中的特定分割區（未圖示）或其部分只可被那些已被授權及/或被授權這麼做的個體來存取。密碼元件 204 也可提供非對稱密碼加速器與工具（例如 RSA、數位簽章標準（Digital Signature Standard，簡稱 DSS）等等）以確保該記憶體 104 中的特定分割區或其部分只可被那些已被授權及/或被認證（certified）這麼做的個體來存取。此外，密碼元件 204 可提供加速器與工具（例如保全散列演算法（Secure Hash Algorithm，簡稱 SHA）與其不同版本，例如 SHA-0、SHA-1、SHA-224、SHA-256、SHA-384、與 SHA-512），以確保對於該記憶體 104 中的特定分割區的存取是限制給那些被授權來獲得存取的個體。

該記憶體模組 102 也可包含可從個體請求（solicit）鑑別資料的鑑別元件（authentication component）206，而在依此請求該鑑別資料之後，該記憶體模組 102 可個別地利用及/或結合經由所利用的生物辨識形態（biometric modality）而取得且確定的資訊以幫助控制對於該記憶體 104 的存取。該鑑別資料可例如為通行字（password）（例如人類可認知的字元的序列）、通行片語（pass phrase）（例如字母數字字元（alphanumeric character）的序列，係可相似於一般通行字但卻是傳統上較大長度且包含除了人類可認知的字元之外的非人類可認知的字元）、通行碼（例如

個人識別碼（PIN））等等的形式。除此之外地及/或可選擇性地，也可藉由鑑別元件 206 來利用公鑰基礎建設（public key infrastructure，簡稱 PKI）資料。PKI 約定（arrangement）可提供給受信賴的第三者來透過公鑰的使用以檢驗與確認個體身份，該公鑰通常可為由該受信賴的第三者所發佈的認證（certificate）。此種約定可使得個體能夠互相鑑別、及使用認證（例如公鑰）與私鑰（private key）、會期金鑰（session key）、流量編碼金鑰（Traffic Encryption Keys，簡稱 TEKs）、加密系統特定的（cryptographic-system-specific）金鑰、及/或其他金鑰中的資訊，以加密與解密在個體之間通訊的訊息。

該鑑別元件 206 可藉由其獨一無二的實體與行為的特性和屬性來實現一個或多個機器實現的（machine-implemented）技術用以識別個體。可利用的生物辨識形態可例如包含：臉部辨識，其中，在個體的臉上的關鍵點的量測可提供與該個體相關聯的獨一無二之圖案；虹膜辨識（iris recognition），從瞳孔的外部邊緣測量與眼睛之有色部分（虹膜）相關聯的圖案，以偵測與該個體的虹膜相關聯的獨特特徵；指紋（或掌紋）識別，掃描不連續的皮膚波狀隆起部並形成可提供用以分辨特徵的圖案以識別個體；及/或聲音辨識（voice recognition），可根據部分的口音型態、腔調等（可分辨出該個體與另一個體）來分析該個體的聲音。

該鑑別元件 206 可與鑑別介面元件 208 結合，該鑑別

介面元件 208 可被納入該記憶體模組 102 且可幫助鑑別使用者或其他人。在一個態樣中，該鑑別介面元件 208 可與鍵盤組（未圖示）結合且可接收鑑別資訊（例如通行字、PIN 碼等等），該鑑別元件可評估該鑑別資訊以判定是否同意對於該記憶體 104 的存取。在另一態樣中，該鑑別介面元件 208 可包括掃描器或其他可獲得及/或接收生物辨識資訊（例如與指紋、眼睛特徵、臉部特徵、人聲辨識等等相關聯的資訊）的適合元件，該資訊可從該使用者或其他個體提供或獲得。該鑑別元件 206 可評估（例如比較）該生物辨識資訊與可儲存在該記憶體 104 中的模板（template）資訊或其他資訊，以判定該生物辨識資訊是否可與被授權與可被同意來存取該記憶體 104 或部分該記憶體 104 的該使用者或其他個體相關聯。如果此種生物辨識資訊與該模板資訊或其他資訊匹配，則部分依據同意給該使用者或其他個體的存取權利的等級，而可同意與該生物辨識資訊相關聯的該使用者或其他個體來存取儲存在該記憶體 104 內的該資料或部分該資料。舉例來說，鑑別介面元件 208 可包括指紋感測器（未圖示），該指紋感測器可與該記憶體模組 102 的外殼或該記憶體模組 102 所存在的電子裝置（未圖示）的外殼的表面結合。該使用者可放置一個或多個數字（digit）在該指紋感測器上，該指紋感測器可掃描該一個或多個數字以獲得生物辨識資訊。可擷取該生物辨識資訊並與可儲存在該記憶體 104 中的該模板資訊作比較。如果該生物辨識資訊匹配而達到準確性的預定

閾值（threshold）等級，則可同意該使用者與那使用者相關聯的預定存取權利，以存取該記憶體 104 中的資料的子集（subset）。

依據本發明的一個實施例，該記憶體模組 102（包含該記憶體 104、至少一部分的該反竄改元件 106、該密碼元件 204、該鑑別元件 206、及/或至少一部分的該鑑別介面元件 208）可設於或實現在單一積體電路晶片（例如晶粒）上，該晶片可提供被程式化至該記憶體 104、被儲存在該記憶體 104、及/或讀取自該記憶體 104 的資料有改良及/或增加的資料保全性。根據另一個實施例，該記憶體模組 102（包含該記憶體 104、至少一部分的該反竄改元件 106、該密碼元件 204、該鑑別元件 206、及/或至少一部分的該鑑別介面元件 208）可實現在特定應用積體電路（application-specific integrated-circuit，簡稱 ASIC）晶片上。

參照至第 2b 圖，係描述根據本發明的另一實施例的可幫助保全資料的系統 250。系統 250 可包含描述關於系統 200 的元件（例如記憶體 104、反竄改元件 106 等等），其中，每個元件可包含如在此更完整敘述（例如關於系統 200）的個別功能。系統 250 可包含該主處理器 202，其中，該主處理器 202 可被容納在該記憶體模組 102 內。藉由將該主處理器 202 納入該記憶體模組 102 內，可改善及/或幫助在該主處理器 202 與該記憶體模組 102 內的該記憶體 104 及/或其他元件之間通訊的資料的保全性。

第 3 圖說明系統 300，該系統 300 可依據本發明來利用反竄改技術以幫助保全記憶體裝置中的資料。系統 300 可包含反竄改元件 106，該反竄改元件 106 可使用來監控與評估與存取記憶體模組 102（未圖示）中的記憶體 104（未圖示）的授權或非授權企圖相關聯的事件，且可利用反竄改技術來保全寫入至該記憶體 104、儲存在該記憶體 104、及/或讀取自該記憶體 104 中的資料免於竄改攻擊。該反竄改元件 106 可偵測與該記憶體模組 102 及/或記憶體 104 相關聯的竄改攻擊、或要竄改的企圖，且可部分地依據竄改攻擊或竄改企圖的類型來對該竄改攻擊作出反應（例如提供該攻擊/竄改的證據、抵擋該攻擊/竄改、提供對於該攻擊/竄改的回應）。舉例來說，如果非授權個體企圖要存取該記憶體模組 102 及/或記憶體 104，則該反竄改元件 106 可提供該攻擊發生的證據、提供對於該攻擊的抵抗、及/或提供對於該攻擊的回應。該反竄改元件 106 可包含相同或相似的功能，例如關於系統 100 及/或系統 200 而在此更完整敘述者。

依據一態樣，該反竄改元件 106 可包含可聚集及/或組織資料的聚集元件 302，該資料包含與存取該記憶體 104 及/或記憶體模組 102 相關聯的資料，該資料可被該反竄改元件 106 接收或獲得，以幫助判定是否發生或已經發生竄改攻擊、判定關於竄改攻擊而可產生的反應、產生及/或提供竄改攻擊的證據、產生及/或提供對於竄改攻擊的回應、抵抗竄改攻擊等等。該聚集元件 302 可過濾、選擇、及/

或組織由該反竄改元件 106 所接收的資料。舉例來說，該聚集元件 302 可識別可與竄改攻擊及/或存取該記憶體 104 及/或記憶體模組 102 的企圖相關聯的部分資料。應了解到，該聚集元件 302 可與該反竄改元件（如描述的）、獨立（stand-alone）元件、及/或其大部分任何的合適組合相結合。

依據另一態樣，該反竄改元件 106 可包含評估元件 304，該評估元件 304 可監控、收集、及/或分析接收到的資料，且該評估元件 304 可幫助判定例如是否有存取該記憶體 104 及/或該記憶體模組 102 的企圖、是否發生或已經發生竄改攻擊、發生或已經發生的竄改攻擊的類型、關於竄改攻擊而可產生的反應等等。

舉例來說，該聚集元件 302 可接收關於要輸入鑑別憑證（authentication credential）以存取該記憶體 104 的企圖的資訊。該聚集元件 302 可計數（count）輸入此種鑑別憑證的企圖次數。每個輸入該鑑別憑證的企圖可由該聚集元件 302 來登入（logged）並由該評估元件 304 來評估。該聚集元件 302 可傳遞該計數資訊至該評估元件 304。該評估元件 304 可評估與該鑑別企圖相關聯的資訊，且在已經達到不成功企圖的預定次數(例如三個連續的不成功企圖）之後，該評估元件 304 可判定此種無效企圖構成關於該記憶體 104 的竄改攻擊，而該反竄改元件 106 可以想要的方式對於該竄改攻擊作出反應（例如模組 102 的外殼可改變色彩狀態），如在此更完整描述者。

在又另一態樣中，該反竄改元件 106 可利用竄改證據元件 306，該竄改證據元件 306 可幫助提供竄改攻擊（例如竄改事件）或竄改該記憶體 104 及/或該記憶體模組 102 的企圖的證據。在一態樣中，該反竄改元件 106 可部分地結合成該記憶體模組 102 的外殼的一部分。該記憶體模組 102 的外殼可由例如易碎材料（例如易碎塑性材料）的材料所構成，該材料可導致如果打開它則外殼會分解（disrupt），以使得幾乎不可能在沒有可察覺的指示（例如證據）的情況（該包體（例如外殼）的實體分解的形式的竄改）下而再閉合。舉例來說，該記憶體模組 102 的外殼及/或該記憶體 104 的外殼可破裂及/或碎裂成多塊，而可防止該記憶體模組 102 的外殼及/或該記憶體 104 的外殼回復到它們原始、未受竄改的狀態。雖然該記憶體 104 之後可能為無法存取的且儲存在其中的資料可能被破壞，但仍舊可保全該資料免於攻擊者的非授權存取。在另一態樣中，該記憶體模組 102 的外殼可由可具有易延展（ductile）材料特性的材料來製造。如果企圖開啟或進入該記憶體模組 102 的外殼（例如企圖要開啟該記憶體模組 102 的外殼以存取容納其內的該記憶體 104），在企圖要開啟該記憶體模組 102 的外殼的開啟過程中，由於施加的應力及/或應變，可使這樣的外殼變形，且這樣的外殼可保持該變形。該變形可足以防止該外殼回到其原始、未受竄改的狀態，而該變形可為可由該使用者所看得見的該竄改攻擊的證據。

在另一態樣中，該竄改證據元件 306 可包含可利用的覆蓋體（cover），該覆蓋體可例如為封條（seal）或貼紙（sticker），而該覆蓋體可貼至該記憶體模組 102。在企圖從該記憶體模組 102 剝去及/或移除該封條/貼紙的過程中，舉例來說，該封條或貼紙可能起皺（wrinkle）或扯破（tear），而可成為可由使用者所識別得出的該封條/貼紙受到打擾的證據。

在又另一態樣中，該記憶體模組 102 的外殼可由可部分依據此種外殼在由於要竄改該記憶體模組 102 的外殼、該記憶體 104、及/或其他包括該記憶體模組 102 的元件的企圖而過程中發生的物理、熱、及/或電子的改變與事件而改變狀態（例如顏色）的材料所組成。

舉例來說，該反竄改元件 106 可接收某個體已經企圖鑑別要存取該記憶體 104 的預定次數數字（例如三次）的資訊，且所有企圖由於該個體所提供的錯誤鑑別資訊而不成功。該竄改證據元件 306 可提供此種竄改事件已經發生的證據，舉例來說，藉由改變可能含有該記憶體 104 的記憶體模組 102 的外殼的色彩狀態及/或點亮可在該記憶體模組 102 上或可與該記憶體模組 102 結合的發光二極體（LED）（例如 LED 顯示器、多色彩 LED 顯示器）（未圖示）並顯示這樣的色彩狀態改變，以使使用者能夠看到。該竄改證據元件 306 可在該記憶體模組 102 是在未竄改狀態中時幫助顯示色彩的第一子集（一個或多個色彩）在該模組 102 的外殼（例如該外殼本身、整合至該外殼的顯示

器）上，並可在該記憶體模組 102 是在竄改狀態中時幫助顯示色彩的不同子集（一個或多個色彩）在該模組 102 的外殼上。

在提出可識別該使用者為一個已授權的使用者的正確鑑別憑證以重置（re-set）該記憶體模組 102 的色彩狀態及/或存取該記憶體 104 之後，該反竄改元件 106 可幫助使得已授權之使用者（例如所有者）可將與該記憶體模組 102 的外殼相關聯的色彩狀態重置成為可對應至未竄改狀態的色彩。經由該竄改證據元件 306 及/或包含在該模組 102 的外殼上或整合至該模組 102 的外殼的可改變色彩的顯示器（例如 LED 顯示器）來使該模組 102 的外殼顯示竄改的證據，例如，藉由使該模組 102 的外殼改變色彩，相較於僅提供竄改證據給該記憶體模組 102 所屬的該電子裝置的顯示器（例如圖形使用者介面（GUI）而使得攻擊者可企圖藉由擾亂該竄改證據至該電子裝置顯示器的通訊來繞過此種保全措施的情形，這可幫助改善該模組 102、其中的記憶體 104、及/或儲存在該記憶體 104 中的資料的保全性。此種模組外殼及/或該竄改證據元件 306 的顯示器可減低攻擊者中斷連線或繞過該竄改證據元件 306 的風險，因為該模組 102 的外殼本身是提供竄改的證據及/或可提供竄改證據的該顯示器可整合在該模組 102 的外殼中。再者，可利用其他反竄改技術（例如網目電路、切換電路等等）以及該模組 102 的色彩狀態的改變來減低被攻擊者竄改的風險，以進一步保全該模組 102、記憶體 104、與儲存在其

中的資料。

如同另一例子，在企圖要從可包含有該記憶體模組102的該電子裝置中移除該記憶體模組102的解銲過程中，該反竄改元件106可偵測該竄改事件，而該竄改證據元件306可提供該竄改攻擊的證據，因為該記憶體模組102的外殼可藉由色彩狀態的改變（例如該記憶體模組102的外殼可從黑色改變成紅色）來對該解銲過程的熱干擾作出反應。該記憶體模組102的外殼的色彩狀態的改變可為該電子裝置的使用者所看見且可在外表上通知該使用者已經發生要竄改該記憶體模組102的企圖。

因為該記憶體模組102能被容納在該電子裝置（未圖示）內，為了使該竄改的證據能夠被該使用者所察覺，可將該電子裝置建構成有可位於該電子裝置的外殼上的視窗或其他透明元件，以使得該使用者可看到該電子裝置內的該記憶體模組而能注意到該竄改的證據（例如該記憶體模組的色彩狀態的改變），如同在此例如關於第4a與4b圖的更完整描述。在一個態樣中，可依照使用者的喜好設計該記憶體模組102的外殼，例如其上具有想要的形狀、想要的識別標誌（logo）、想要的顏色、及/或可客製化的表面，其中，例如，使用者可輸入可顯示於該記憶體模組102的外殼的表面上的他/她的名字或詞或片語，以個人化該記憶體模組102與該記憶體模組102所屬的該電子裝置。

在又另一態樣中，該竄改證據元件306可利用揚聲器（speaker）（未圖示）與擴音器（amplifier）（未圖示），而

當發生竄改攻擊（例如個體在鑑別之後被拒絕存取已經失敗了預定的次數數字）時，該竄改證據元件 306 可幫助產生可由該擴音器所擴音與經由該揚聲器來呈現為聲音輸出的聲音訊號，該聲音訊號可為該竄改攻擊已經發生或正在發生的證據。根據一態樣，為了節省電力消耗，可提供該聲音訊號一段預定期間的時間（例如一分鐘）且可在這時間之後終止。舉例來說，如果發生竄改攻擊，該竄改證據元件 306 可幫助改變該記憶體模組 102 的外殼的色彩與輸出聲音訊號，以做為該竄改攻擊的證據。在預定時期的時間之後，該竄改證據元件 306 可導致該聲音訊號停止，以幫助節省電力，但是該色彩狀態的改變可維持，以使得如果該使用者沒機會聽到該聲音訊號，則該使用者仍可注意到該竄改的證據。

依照另一態樣，該竄改證據元件 306 可利用可振動的感測元件（sensory component）（未圖示），而因此在當發生竄改攻擊時，使得該記憶體模組 102 的外殼及/或該記憶體模組 102 所屬的該電子裝置的外殼振動，而可為竄改攻擊已經發生或正在發生的證據。依照一態樣，為了節省電力消耗，可提供該振動一段預定期間的時間（例如一分鐘）且可在這時間之後終止。舉例來說，如果發生竄改攻擊，該竄改證據元件 306 可幫助改變該記憶體模組 102 的外殼的色彩與產生振動，以做為該竄改攻擊的證據。在預定時期的時間之後，該竄改證據元件 306 可導致該振動停止，以幫助節省電力，但是該色彩狀態的改變可維持，以使得

如果該使用者沒機會察覺該振動，則該使用者仍可注意到該竄改的證據。

該反竄改元件 106 可包含電力供應器 308（例如鋰電池），該電力供應器 308 可提供合適的電力，以幫助改變該記憶體模組 102 的外殼的色彩狀態、產生與放大聲音訊號、及/或產生與該感測元件相關聯的振動。該電力供應器 308 可為可再充電的且可經由供應至該記憶體模組 102 所屬的該電子裝置的電荷來充電。

依據本發明的另一態樣，該反竄改元件 106 可包含可幫助抵擋由個體所要竄改（例如獲得對於資料的非授權存取）該記憶體 104 的企圖的竄改抵擋元件 310。攻擊者可企圖獲得旁通道資訊，例如與該電子裝置（例如關於可被包含在該記憶體模組 102 中的該密碼元件 204）相關的電力消耗、電磁輻射、及/或射頻特性相關聯的資訊。

該密碼元件 204 可利用密碼協定來幫助加密及/或解密被寫入至該記憶體 104 或從該記憶體 104 讀出的資料。該密碼元件 204 可執行根據密碼協定的計算以幫助資料加密/解密。不同類型的計算（例如乘法、開平方等等）可有攻擊者可獲得並分析之不同且個別的電力消耗等級、電磁輻射等級、及/或射頻特性，以獲知該攻擊者可用以獲得存取及或解密儲存在該記憶體 104 中的資料的資訊（例如密碼演算法、指數）。

為了進一步說明，該記憶體模組 102 的操作可包含處理與儲存該記憶體 104 本身內與元件相關聯的資訊，以及

與可在該記憶體模組 102 外部的處理器（例如主處理器 202）的互動。舉例來說，在操作過程中，當電流在該記憶體模組 102 及/或包含該記憶體模組 102 的該電子裝置內波動時，可產生無線電波（radio wave）。該無線電波及/或其他放射物（emanation）可被攻擊者攔截及分析，以判定與該記憶體模組 102 及/或該電子裝置的操作相關所可包含與揭露的智能方位資訊（intelligence-bearing information）。

依據一態樣，該竄改抵擋元件 310 可包括屏蔽材料（shielding material），其可消除、最小化、及/或減低電力消耗等級、電磁輻射等級、及/或輸出射頻資訊的等級，及/或可改變與該電力消耗、電磁輻射、及/或射頻相關聯的資訊以幫助抵擋攻擊者的竄改攻擊。在一個態樣中，該竄改抵擋屏蔽可用在該記憶體模組 102 及/或該模組 102 所屬的該電子裝置內。在另一態樣中，該竄改抵擋屏蔽可包括可幫助減低輸出及/或改變與電力消耗、電磁輻射、及/或射頻相關聯的資訊的金屬或其他合適材料。

在另一態樣中，該竄改抵擋元件 310 也可結合該鑑別元件 206 來作用，以幫助抵擋竄改攻擊，如同可利用鑑別協定來抵擋或禁止想要存取該記憶體 104 及/或儲存於其中的資料的非授權企圖。舉例來說，該竄改抵擋元件 310 可幫助抵擋個體企圖提供鑑別憑證給該記憶體模組 102 以存取該記憶體 104 的竄改攻擊。結合該評估元件 304 的該竄改抵擋元件 310 可分析提出的該鑑別憑證且可判定該憑證是否正確。如果該憑證不正確，則該竄改抵擋元件 310

可幫助拒絕該個體對於該記憶體 104 與儲存於其中的資料的存取。

根據本發明的又另一態樣，該反竄改元件 106 可包含竄改回應元件 312，該竄改回應元件 312 可幫助判定是否已經發生關於該記憶體模組 102、記憶體 104、電子裝置等的竄改攻擊，且可對於竄改攻擊提供想要的回應。在一個態樣中，如果該竄改回應元件 312 判定竄改攻擊已經發生且需要竄改回應，則該竄改回應元件 312 能啟動想要的竄改回應。

在一個態樣中，該竄改回應元件 312 可利用能幫助偵測與該記憶體模組 102 及/或記憶體 104 相關的竄改攻擊的「網目」電路。該記憶體模組 102 可包含能用以電性連接該記憶體模組 102 至 PCB（未圖示）的複數個接腳（未圖示），該接腳可焊接至該 PCB 或可插入至可焊接至該 PCB 的插座（未圖示）。該網目電路可建構在該記憶體模組 102 的一個或多個接腳與和 PCB（該記憶體模組 102 所屬的 PCB）結合的導電路徑之間。舉例來說，該網目電路可依需要而以從該記憶體模組 102 的接腳到該 PCB 的對應導電路徑、到該 PCB 的另一導電路徑並進入對應另外導電路徑的另一接腳的方式運行，以形成該網目。在一個態樣中，該「網目」可為線網目（wire mesh），該線網目位於/夾在該記憶體模組與該 PCB 之間且連接一或多個該記憶體模組 102 上的接腳。

一旦建構該網目電路，可施加預定電壓等級及/或強度

的電子檢測訊號（例如電壓）橫跨該網目電路。用以產生該電子檢測訊號的電力可例如由該電力供應器 308 來提供。舉例來說，可由該評估元件 304 及/或該竄改回應元件 312 來監控並分析該電子檢測訊號，用以評估訊號連續性及/或訊號強度。如果偵測到該訊號中斷及/或訊號強度改變（例如不一致）（例如電壓降低），該竄改回應元件 312 可啟動竄改回應。在一個態樣中，該竄改回應元件 312 可啟動抹除（例如歸零（zeroization））儲存在該記憶體 104 中的資料的全部或子集。舉例來說，如果與該網目電路相關聯的該檢測訊號改變而使得判定為竄改攻擊發生，則該竄改回應元件 312 可抹除在該記憶體 104 的保全分割區中的資料，以使得這些資料（例如機密資料、個人資料）不會被非授權個體（例如攻擊者）所存取。

依據另一態樣，回應於此種竄改攻擊，該竄改回應元件 312 可啟動該記憶體模組 102 中或與該記憶體模組 102 相關聯的一個或多個元件（例如記憶體 104）的災難性故障及/或從容性故障。元件的災難性故障可為破壞（例如電路短路、電路熔接）以使得該元件無法更換或操作。元件（例如記憶體 104）的從容性故障可為可使該元件及/或記憶體模組 102 無法操作，但是該故障的元件能夠可操作及/或可替換而使得該記憶體模組 102 能再次變得功能完整。

在本發明的又另一態樣中，該竄改回應元件 312 可利用可置於該記憶體模組 102 的外殼的部分之間的凹陷位置中的轉動開關。在企圖要開啟或移除該記憶體模組 102 的

外殼或其一部分的過程中，可在開啟或移除該外殼時藉由該開關致動器上的壓力移除而啟動該轉動開關以改變其狀態。該竄改回應元件 312、及/或可與其相關聯的評估元件 304 可判定已經發生竄改攻擊且可提供回應給該竄改事件。在一個態樣中，對於此種竄改攻擊的回應可為抹除（例如歸零）儲存在該記憶體 104 中的資料的全部或子集。在另一態樣中，對於該竄改攻擊的回應可為與該記憶體模組 102 相關聯的一或多個元件（例如記憶體 104）的災難性故障及/或從容性故障。

依據本發明的不同其他態樣，該反竄改元件 106 可偵測其他竄改形式（例如凍結該記憶體模組 102、施加超出規格的電壓給該記憶體模組 102、供給至該記憶體模組 102 的電力激增、與該資料相關聯的錯誤攻擊（fault attack）、及/或與該記憶體 104 相關聯的時脈訊號的變化等等）並對其作出反應。在偵測到這樣的攻擊之後，該反竄改元件 106 可部分依據該竄改攻擊的類型來對該竄改攻擊啟動想要的回應（例如改變該記憶體模組 102 的色彩狀態）。

參照第 4a 圖，其描述根據本發明的實施例而可幫助保全資料免於竄改的系統 400。系統 400 可為或可包含電子裝置（例如行動電話、PDA 等），該電子裝置可包括不同元件，包含例如記憶體模組 102、記憶體 104（未圖示）、反竄改元件 106、主處理器 202（未圖示）、密碼元件 204（未圖示）、及/或鑑別元件 206（未圖示）。應了解到，該記憶體模組 102、記憶體 104、反竄改元件 106、主處理器

202、密碼元件 204、及/或鑑別元件 206 各可包含如在此更完整敘述(例如關於系統 100、系統 200、及/或系統 300)的相同或相似的個別功能。該系統 400 的電子裝置可包括可容納與該電子裝置相關聯的元件與電路系統的電子裝置外殼 402。位於該電子裝置外殼 402 的表面上的可以是可用來顯示資訊給使用者及/或其他人的顯示元件 404(例如 GUI)。在一個態樣中,該顯示元件 404 可為可顯示文字及/或影像(例如照片、影片、圖像等)給使用者的所需尺寸和形狀的彩色 GUI。在另一態樣中,該顯示元件 404 也可為可接收使用者所輸入的資訊(例如觸控螢幕)的介面,可輸入該資訊至該電子裝置並部分依據所提供的資訊來加以處理(例如從記憶體 104 讀出資料、寫入資料至記憶體 104、從事與該電子裝置相關聯的功能等),以幫助操縱(navigate)儲存在該記憶體 104 中的資訊及/或與該電子裝置相關聯的功能。

系統 400 也可包含能用以幫助操縱儲存在該記憶體 104 中的資訊及/或與該電子裝置的功能並鍵入資訊(例如姓名、電話號碼、及/或文字訊息)的輸入元件 406(例如鍵盤組)。使用者可經由該輸入元件 406 來鍵入資訊以提供可儲存在該記憶體 104 中的資料及/或從該記憶體 104 中擷取資料、及/或從事與該電子裝置相關聯的功能。

該電子裝置可復包含可為透明、或大體上透明的視窗元件 408,使得該電子裝置的內部元件(例如該記憶體模組 102)能被使用者及/或其他人所察覺。在一個態樣中,

該視窗元件 408 可幫助偵測竄改攻擊及/或提供竄改攻擊的證據給該記憶體模組 102 及/或可被容納於其中的該記憶體 104。依據一態樣，該視窗元件 408 可置於該顯示元件 404 與該輸入元件 406 之間與該顯示元件 404 相同側的該電子裝置的外殼上。在另一態樣中，該視窗元件 408 與該記憶體模組 102 的個別位置可為使得可容納在該電子裝置的該記憶體模組 102 可被使用者及/或其他人透過該視窗元件 408 來察覺，以至於該使用者及/或其他人可注意到該記憶體模組 102 的狀態（例如色彩狀態）及/或情況（例如模組 102 變形或沒有變形）。在又另一態樣中，該視窗元件 408 可為一塊乾淨的塑膠或其他透明材料，該使用者及/或其他人可經由透過該材料以觀看容納該顯示元件 404 的該電子裝置的該側來察覺該記憶體模組 102。

舉例來說，如果某個體企圖藉由企圖鍵入鑑別憑證資訊以被同意存取該資料來從該記憶體 104 中存取資料（例如保全資料），但是提供錯誤的鑑別憑證資訊，則該反竄改元件 106 可判定已經發生竄改攻擊。在一個態樣中，該反竄改元件 106 可藉由改變該記憶體模組 102 的色彩狀態來指示已發生該竄改攻擊，例如，藉由把該記憶體模組 102 的外殼的色彩從第一色彩（例如黑色）改變成不同的色彩（例如紅色），及/或藉由把顯示器（例如 LED 顯示器）的色彩從第一色彩改變成不同的色彩，該顯示器可整合至模組 102 的外殼。該電子裝置的使用者（例如所有者）可透過該視窗元件 408 來觀看該記憶體模組 102 並可察覺該記

憶體模組 102 的該色彩狀態改變，該色彩狀態改變可對該使用者指示關於該記憶體模組 102 及/或記憶體 104 所發生的竄改攻擊。

關於第 4b 圖，其說明根據本發明的實施例而可幫助保全資料免於竄改的系統 400 的剖視圖。該系統 400 的剖視圖可為或可包含該電子裝置，該電子裝置可包括如第 4a 圖所描述的各種元件（例如記憶體 104（未圖示）、反竄改元件 106 等）。該電子裝置可包括可容納與該電子裝置相關聯的各種元件的電子裝置外殼 402。在一個態樣中，該電子裝置可包含含有該記憶體裝置 104（未圖示）的該記憶體模組 102，該記憶體裝置 104 可儲存記憶體位置中的資料在其中。該記憶體模組 102 可置於該電子裝置內且可與其他元件（例如主處理器 202（未圖示））結合，以幫助儲存資料在該記憶體 104 中並從該記憶體 104 中擷取資料。該視窗元件 408 可置於該電子裝置的表面上，以使得位在該電子裝置內部的該記憶體模組 102 可被該使用者與其他人所察覺，該使用者與其他人可看透該視窗元件 408 以觀察該記憶體模組 102 的該狀態（例如色彩狀態）及/或情況（例如形態，如已變形或未變形）。雖然未圖示，但該電子裝置外殼 402 也可包含該顯示元件 404 及/或輸入元件 406。

根據本發明的一個態樣，可依照喜好設計該記憶體模組 102 的外殼（例如護罩（shroud））且可加入裝飾的特色到裝有該記憶體模組 102 的該電子裝置。如果該記憶體模組已經遭到竄改，則啟動竄改證據回應且可經由該窗戶元

件 408 來看到該回應（例如該護罩的色彩狀態的改變）。

參照第 5 圖，係說明根據本發明的實施例的可幫助儲存資料的系統 500。系統 500 可包含可儲存資料的記憶體 104，該資料包含想要資料保全的機密及/或個人資料。根據一個態樣，該記憶體 104 可為快閃記憶體裝置（例如單位元快閃記憶體、多位元快閃記憶體）。該記憶體 104 一般可包含可形成其中有一個或多個高密度核心區 504 與一個或多個低密度周邊區的半導體基板 502。該高密度核心區 504 通常可包含各自可定址、實質上相同之多位元記憶體單元（未圖示）的一個或多個 M 乘 N 陣列（未圖示）。另一方面，該低密度周邊區通常可包含輸入/輸出（I/O）電路系統 506 與用以選擇性定址該各自記憶體單元的程式化電路系統。該程式化電路系統可部分地由 x 解碼器 508 與 y 解碼器 510 來代表且可包含 x 解碼器 508 與 y 解碼器 510，該 x 解碼器 508 與 y 解碼器 510 係和 I/O 電路系統合作用以將所選擇的定址記憶體單元的源極、閘極、及/或汲極選擇性地連接到預定電壓或阻抗，從而對個別記憶體單元產生指定的操作（例如程式化、讀取、與抹除，以及產生出必要電壓來產生此種操作）。可利用該反竄改元件 106 以幫助保護被寫入至該較高密度核心區 504、儲存在該較高密度核心區 504、及/或讀取自該較高密度核心區 504 的資料。

翻到第 6 圖，係說明根據本發明的實施例而能利用智能來幫助保全資料免於竄改的系統 600。系統 600 可包含

記憶體模組 102、記憶體 104、反竄改元件 106、密碼元件 204、及/或鑑別元件 206。該記憶體模組 102、記憶體 104、反竄改元件 106、密碼元件 204、與鑑別元件 206 各可大體相似於個別元件且可包含如在此敘述（例如關於系統 100、系統 200、系統 300、系統 400、及/或系統 500）的此種個別功能。

該系統 600 可復包含能與該反竄改元件 106 結合的智能元件 602，以幫助分析資料且可提供推論（inference）及/或決定，例如關於是否已經發生竄改事件（例如攻擊）、竄改事件的類型、可利用或開始關於竄改事件的反應的類型（例如提供竄改證據、提供竄改回應、抵抗竄改）、鑑別憑證是否有效等。

舉例來說，該反竄改元件 106 可偵測與網目電路相關聯的訊號的強度的變化，該網目電路與該記憶體模組 102 和 PCB 連接，該記憶體模組 102 係電性連接於該 PCB 上。關於該偵測變化的資訊可提供給該智能元件 602，並且部分地依據現有及/或歷史證據，該智能元件 602 可推斷該訊號的偵測變化是否與竄改攻擊相關聯。

要了解的是，該智能元件 602 可從經由事件及/或資料所獲得的一組觀察來提供關於該系統、環境、及/或使用者的狀態的推斷或推論其狀態。可利用推論來辨識特定內容或動作、或例如可利用該推論產生橫跨所有狀態的可能性分佈。該推論可為機率性的，也就是，依據資料與事件的考慮而計算橫跨所有感興趣的狀態的可能性分佈。推論也

可視作用以從一組事件及/或資料中構成較高等級事件的技術。此種推論會導致從一組觀察的事件及/或儲存的事件資料（例如歷史資料）中建構新的事件或動作，不論事件是否關聯於相近的鄰近時間，以及是否該事件與資料是來自一個或數個事件與資料來源。各種的分類（明確地或暗示地訓練）體制及/或系統（例如支持向量機（support vector machine）、神經網路、專家系統、貝氏信賴網路（Bayesian belief network）、模糊邏輯（fuzzy logic）、資料融合引擎……）可用以執行與本發明有關的自動及/或推論動作。

分類器（classifier）是將輸入屬性向量（input attribute vector）x=（x1,x2,x3,x4,xn）映射到該輸入所屬的分類的信賴度的函數，也就是，f(x)=信賴度（分類）。此種分類可利用機率性的及/或以統計為基礎的（statistical-based）分析（例如分解成該分析效用與成本）以預測或推論使用者想要自動履行的動作。支持向量機（support vector machine，簡稱SVM）是可利用之分類器的例子。該SVM藉由在可能輸入的空間中找到超曲面（hypersurface）來操作，該超曲面企圖從不觸發事件（non-triggering event）中分割出觸發準則（triggering criteria）。直覺地，這使得該分類對於測試近的資料是正確的，但是不相同於訓練資料。其他直接與非直接的模型分類方法包含可利用例如自然Bayes（naïve Bayes）、貝氏網路（Bayesian network）、決策樹（decision tree）、神經網路、模糊邏輯模型、與提供獨立性的不同模式的機率性分類模型。在此使用的分類

也是包含使用來發展優先權模型的統計回歸（statistical regression）。

系統600也可包含可呈現與該主處理器202相關聯的資料的呈現元件（presentation component）604。應了解到，該呈現元件604可結合至該主處理器202及/或獨立單元中。該呈現元件604可提供各種類型的使用者介面以幫助在使用者與耦接至該主處理器202的任何元件之間的互動。

該呈現元件604可提供一個或多個圖形使用者介面（GUI）、命令行（command line）介面等等。舉例來說，可使GUI提供使用者用以載入、引進（import）、讀取資料等等的區域或手段，且該GUI可包含呈現此種結果的區域。這些區域可包括已知文字及/或圖形區域（包括對話方塊（dialogue box）、靜態控制、下拉式選單、列表方塊、彈出式選單、如編輯控制、結合方塊（combo box）、無線電鈕、檢測方塊、按鈕、與圖形方塊）。此外，可利用用以幫助呈現的公用程式（例如用以導航的垂直及/或水平捲軸與工具列鈕），以判定區域是否將是可觀看的。舉例來說，該使用者可與耦接於及/或結合至該處理器706的一或個多個元件互動。

該使用者也可藉由各種裝置（例如滑鼠、滾動球、鍵盤組、鍵盤、筆及/或人聲啟動）來與該區域互動而用以選擇並提供資訊。典型上，可在後續輸入資訊時利用例如按鈕或鍵盤上的鍵入鍵的機制來啟動搜尋。然而，應了解到

本發明並不限於如此。舉例來說，僅反白檢測方塊可啟動資訊傳送。在另一例子中，可利用命令行介面。舉例來說，該命令行介面可經由提供文字訊息以提示（例如經由顯示器上的文字訊息與聲音音調）資訊給該使用者。該使用者之後可提供合適的資訊，例如對應於在該介面提示中所提供的選項或對應於在該提示中提出的問題的答案之字母-數字輸入。應了解到，可利用該命令行介面來連接 GUI 及/或應用程式界面（application program interface，簡稱 API）。此外，可利用該命令行介面來連接具有有限圖形支援、及/或低頻寬通訊通道的硬體（例如影像卡）及/或顯示器（例如黑白、與增強型圖形配接器（enhanced graphics adaptor，簡稱 EGA））。

參照到第 7 圖，係說明根據本發明的態樣而可利用記憶體分割來幫助保全記憶體中的資料的系統 700。可利用系統 700 來幫助保全儲存在記憶體（例如可為非揮發性記憶體的記憶體 104）中的資料。

為了說明的目的，該記憶體 104 可分成三組分割區（例如所描述的主平台分割區（Host Platform Partition）、主應用程式分割區（Host Application partition）、與高保全分割區（High Security Partition））。該主平台分割區可包括早期開機與緊急碼分割區 702、作業系統分割區 704、及/或操作子（operator）與 OEM 信任碼與資料分割區 706。再者，主應用程式分割區可包含第三方信任碼分割區 708、保全使用者資料（加密）分割區 710、與普通使用者資料

與可疑碼分割區 712。此外，該高保全分割區可包含保全裝置金鑰分割區 714 與保全認證與金鑰儲存分割區 716。

如所描述的，該分割系統 700 可提供多層方法以確保記憶體竄改保護與有效的病毒回復。舉例來說，主平台分割區、與容納於其中的分割區（例如分割區 702、704、706）可以是被所有個體可觀看的與可存取的，但是只能被某些個體所修改，例如與該記憶體 104 及/或記憶體模組所屬的該電子裝置的製造者相關的個體。因此，分割區 702 可例如允許所有個體來讀取與觀看容納在分割區 702 中的內容，但是只可允許提供合適憑證（例如 PKI 鑑別資訊）的個體來寫入或修改分割區 702 的內容。另一方面，分割區 704 與 706 可允許選擇個體讀取與寫入這些分割區 704、706 的內容，且更具體地說，一旦例如已經建立開機後（afterboot）狀態，可只許可個體讀取分割區 704 及/或 706 的內容，且可只額外地允許進一步提供合適憑證（例如 PKI 鑑別資訊）的個體來寫入或修改分割區 704 及/或 706。

再者，主應用程式分割區與其圖示的子分割區（例如 708、710、712）只可允許對這些特定的分割區選擇性存取。舉例來說，分割區 708-第三方信任碼-一旦已經查明開機後狀態，可允許個體讀取分割區 708 的內容，且可允許提出適當鑑別憑證的個體寫入存取，分割區 710-保全使用者資料（例如加密的）-可允許讀取與寫入存取給供應與該分割區 710 相關聯的適當鑑別憑證的那些個體，以及分割區 712-普通使用者資料與可疑碼-可允許讀取與寫入存取而

不需要個體提供鑑別憑證。

此外，該高保全分割區與相關聯的分割區（例如 714、716）只可允許讀取存取給非常精選與限制的群組個體，例如該記憶體 104 本身，指示這些是最保全的分割區，而且在沒有可產生個別的分割區 714、716 的該反竄改元件 106 或其他元件（未圖示）的情況下，不可存取（例如讀取）這些分割區 714、716。然而，雖然該高保全分割區與相關聯的分割區 714、716 可限制挑選與有限的群組來對這些分割區 714、716 作讀取存取，但是如果個體提供正確的鑑別憑證，則可寫入資料至這些分割區 714、716。

應了解到，系統 700 只是可幫助保全記憶體（例如 104）中的資料的分割系統的一個範例，而非用以限制本發明。本發明可設想該記憶體可維持一個分割區或可分割成幾乎任何想要數量的分割區，該分割區之各者可與提供給儲存於其中的資料的個別保全等級以及關於對儲存在這些分割區中的資料存取的個別協定相關聯。

前述系統已經描述關於在許多元件之間的互動。應了解到，這樣的系統與元件可包含在其中所指定的那些元件或子元件、某些指定元件或子元件、及/或額外元件。子元件也可實現為連通地耦接至不含在母元件內的其他元件的元件。又再者，可將一個或多個元件及/或子元件結合成為提供聚集功能性的單一元件。該等元件也可與一個或多個其他元件互動，這些元件為了簡潔而沒有具體敘述於此，但為熟悉本領域之技藝人士所習知。

第 8 至 12 圖說明根據本發明的方法及/或流程圖。為了簡化說明，所以將該方法描述與敘述為一連串動作。應知道與了解，本發明並不限於說明的該等動作及/或該等動作的順序，舉例來說，動作可以不同順序及/或同時地發生，並具有在此沒有提出與描述的其他動作。此外，並非需要所有說明的動作以實現根據本發明之該方法。此外，熟悉本領域之技藝人士將知道並了解，該方法也可經由狀態圖或事件來表示為一連串相互關聯的狀態。此外，應該進一步了解的是，在下文中所揭露與遍及本說明書的方法係能夠儲存在製造成品（article of manufacture）上，以幫助運送與轉換這些方法至電腦。在此使用的用語「製造成品」是意指涵蓋可從任何電腦可讀（computer-readable）裝置、載體、或媒體來存取的電腦程式。

參照至第 8 圖，係說明根據本發明的態樣而可幫助保全記憶體中的資料免於竄改的方法 800。在 802 處，可偵測及/或接收已經發生竄改事件(例如竄改攻擊、企圖竄改)的指示。在一個態樣中，反竄改元件（例如 106）可偵測及/或接收可指示已經發生竄改事件的資訊。該指示可包含例如藉由提供鑑別資訊而要存取該記憶體（例如 104）的無效企圖、檢測電路（例如網目電路）的擾亂、在企圖要從 PCB 移除該記憶體模組(例如 102)的過程中轉動開關、在該記憶體模組與相關聯之電路系統/感測裝置之間的路徑毀壞等等。

在 804 處，可部分依據偵測到或遭遇到的竄改事件類

型來產生反竄改反應。根據一態樣，該反竄改反應可為提供竄改攻擊的證據。舉例來說，如果竄改攻擊涉及提供無效鑑別資訊給鑑別元件（例如 206）及/或竄改證據元件（例如 306），則該竄改證據元件可幫助改變該記憶體模組的色彩狀態以提供已經發生竄改攻擊的證據給該使用者（例如所有者）及/或其他個體。在另一態樣中，該記憶體模組可抵擋竄改攻擊。舉例來說，如果攻擊者企圖破壞打開該記憶體模組，該記憶體模組及/或容納其中的記憶體可由可破裂成多塊的材料所建構而成，而使得該記憶體無法操作且儲存於其中的資料無法存取。根據又另一態樣，該反竄改元件 106 可提供對於竄改攻擊的回應。舉例來說，網目電路可置於該記憶體模組與 PCB 之間，可供應檢測訊號（例如電壓）至該網目電路。如果攻擊者企圖從該 PCB 移除該記憶體模組，則可能擾亂或中斷連接該檢測訊號，而該反竄改元件可偵測此種擾亂/中斷連接並判定已經發生竄改攻擊。該竄改回應元件（例如 312）可藉由抹除儲存在該記憶體中的資料或部分資料來提供回應給此種攻擊，及/或可幫助導致記憶體元件及/或電路系統熔接在一起，以至於該記憶體成為無法操作及/或無法存取。此時，方法 800 可結束。

第 9 圖描述根據本發明的態樣而可幫助保全與記憶體裝置相關聯的資料免於竄改的方法 900。在 902 處，可接收能指示竄改事件（例如竄改攻擊、竄改企圖）已經發生的資訊。在一個態樣中，反竄改元件（例如 106）可接收

已發生關於記憶體模組（例如 102）或與其相關聯的記憶體（例如 104）的竄改事件的資訊。在一個態樣中，可把該記憶體模組裝入護罩中，該護罩可由能提供竄改事件的證據的材料所組成。舉例來說，該材料可為可置於該記憶體模組的表面上的貼紙或封條、塑及/或脆性材料（如果企圖打開該記憶體模組及/或記憶體的外殼，則會破裂）、及/或延性材料（如果企圖破壞打開該記憶體模組的外殼，則會變形）。貼紙或封條的破壞、該記憶體模組及/或記憶體的破裂、及/或該記憶體模組的變形可指示（例如提供證據）竄改事件已經發生。在另一態樣中，該記憶體模組可由能改變色彩狀態以提供竄改事件（例如個體為了存取記憶體模組內的記憶體而提供預定數量的次數（例如預定的連續次數的數量）的無效鑑別憑證而被拒絕存取該記憶體）的證據的材料所建構而成。在又另一態樣中，開關可用來結合至該記憶體模組的外殼，如果開啟或毀壞該記憶體模組的外殼，則會轉動該開關，而可提供竄改事件已經發生的指示。

在 904 處，可評估與竄改事件的指示相關聯的資訊。在一個態樣中，可為該反竄改元件（例如 106）的一部份的評估元件（例如 304）可分析與評估此種資訊且可判定竄改事件是否已經發生及/或可判定已經發生的竄改事件（例如關於該記憶體的無效鑑別企圖、與網目電路相關聯的檢測電壓的擾亂、關於該記憶體模組的外殼的已轉動開關等等）的類型。

在 906 處，可部分依據該竄改事件的類型來提供竄改證據。根據一個態樣，竄改證據元件可部分依據該記憶體模組及/或記憶體所遭遇的竄改事件的類型來提供竄改事件的證據。在一個態樣中，如果來存取該記憶體的無效企圖被鑑別達到預定次數，則該竄改證據元件可判定竄改事件已經發生且可提供此種竄改的證據，例如，藉由幫助改變該記憶體模組的外殼的色彩狀態，其中，該使用者（例如所有者）及/或其他個體可察覺這樣的色彩改變是竄改該記憶體模組的證據。在另一態樣中，如果該記憶體模組建構有包含於其上的封條或貼紙，且該竄改事件涉及開啟或企圖開啟該記憶體模組，則該封條或貼紙可能會撕破及/或變形，以使得該撕破或變形可被該使用者（例如所有者）及/或其他個體察覺而成為竄改該記憶體模組的證據。

在又另一態樣中，如果該記憶體模組是由塑性及/或脆性材料所建構而成，且該竄改事件涉及開啟或企圖開啟該記憶體模組，則該記憶體模組的外殼可能會破裂或斷裂成多塊，以使得該破裂或斷裂（例如斷裂的片段）可被該使用者及/或其他個體察覺而成為竄改該記憶體模組的證據。根據另一態樣，如果該記憶體模組是由延性材料所建構而成，且該竄改事件涉及開啟或企圖開啟該記憶體模組，則該延性材料可能會變形，以使得該變形無法回復且可被該使用者（例如所有者）及/或其他個體察覺而成為竄改該記憶體模組的證據。此時，方法 900 可結束。

翻到第 10 圖，係描述根據本發明而可提供竄改攻擊

的證據以幫助保全與記憶體相關聯的資料免於竄改的方法1000。在1002處，可接收鑑別憑證資訊。舉例來說，鑑別元件（例如206）及/或反竄改元件（例如106）可接收鑑別憑證資訊。此種資訊可為通行字、通行片語、PIN、生物辨識資訊的形式、或其他可使用來判定提供此種資訊的該個體是否可被同意來存取該記憶體中的資料及/或可同意該個體的存取權利等級的資訊。在一個態樣中，可經由例如鑑別介面元件（例如208）來提供該鑑別憑證資訊。

在1004處，可判定該鑑別憑證資訊是否有效。如果該鑑別憑證資訊判定為有效，則在1006處，可部分依據該鑑別憑證資訊以同意該個體來存取。在一個態樣中，同意給該個體的該存取權利的等級可依據該個體、所提供的該鑑別憑證、及/或與該記憶體及/或儲存於其中的資料相關聯的其他準則。

如果在1004處，該鑑別憑證資訊判定為無效，則在1008處，可依企圖鑑別的次數是否已經達到預定的最大值來判定。舉例來說，聚集元件（例如302）及/或評估元件（例如304）可追蹤為了存取該記憶體而企圖要鑑別的次數（例如連續的企圖次數）。如果已經達到無效鑑別企圖的預定次數，則在1010處，可判定已經發生竄改事件。舉例來說，如果要鑑別以存取該記憶體而沒有成功的企圖次數已經達到最大值，則該評估元件可判定竄改事件已經發生。

在1012處，可提供與該竄改事件相關聯的證據，其中，提供的該證據及/或對該竄改事件的反應可部分依據發

生的竄改事件的類型。在一個態樣中，該竄改證據元件（例如 306）可幫助改變該記憶體模組的色彩狀態來作為關於無效鑑別的竄改事件的反應，以提供關於該記憶體的竄改的證據。因為記憶體通常被容納在電子裝置（例如行動電話、PDA 等）內，所以該電子裝置可包含可為透明、或大體上透明的視窗元件，且該視窗元件可相對於該記憶體模組與容納於其中的記憶體來放置，以使得使用者及/或其他個體可在外表上察覺該記憶體模組的色彩狀態的改變，此改變可為竄改事件的證據。根據另一態樣，該竄改證據元件可提供可提供竄改證據的聲音訊號及/或其他感測訊號（例如振動），而這樣的聲音訊號及/或其他感測訊號可持續直到因為提出可重置該記憶體模組的適當鑑別資訊才停止，及/或該訊號可持續一段預定的時間，其中，該聲音或感測訊號可終止以幫助節省電力。該記憶體模組的色彩改變可維持，直到由於向該鑑別元件提出適當的鑑別憑證而重置為原始、未竄改的狀態。

轉回到元件符號 1008，如果判定鑑別企圖的次數並未達到最大值，則在 1014 處，關於鑑別企圖（例如連續的鑑別企圖）的次數的計數可增加一。舉例來說，與該竄改證據元件相關聯的計數器可計數並追蹤鑑別企圖的次數且可增加一。在 1016 處，可提供能提供鑑別憑證的提示給（例如）個體。在一個態樣中，該提示可提供給與該記憶體模組及/或與該記憶體模組相關聯的電子裝置相關聯的顯示元件（例如 404）。此時，方法 1000 可回到元件符號 1002

（可接收鑑別憑證資訊），而方法 1000 可從那點繼續進行，舉例來說，直到已經接收適當鑑別資訊及/或不成功的鑑別企圖已經達到預定的最大次數。此時，方法 1000 可結束。

參照至第 11 圖，係描述根據本發明的態樣而可抵擋竄改攻擊以幫助保全與記憶體相關聯的資料免於竄改的方法 1100。在 1102 處，可接收能指示竄改事件（例如竄改攻擊、竄改企圖）已經發生的資訊。在一個態樣中，反竄改元件（例如 106）可接收關於記憶體模組（例如 102）或與該記憶體模組相關聯的記憶體（例如 104）的竄改事件已經發生的資訊。在一個態樣中，該記憶體模組可裝進可由能抵抗竄改的材料所組成的外殼中。舉例來說，該材料可為塑性及/或脆性材料，如果開啟該記憶體模組的外殼，則該材料會抵抗開啟並可能會破裂及/或斷裂。

在 1104 處，可依據竄改事件是否發生來評估，且如果是如此，則評估已經發生的竄改事件的類型以（例如）判定是否可經由對於竄改的抵抗來反擊該竄改事件。在 1106 處，可提供對於該竄改事件的抵抗，其中，舉例來說，該竄改事件是可能是對於竄改想要抵抗的類型。在一態樣中，對於竄改（例如個體企圖開啟該記憶體模組及/或容納於其中的記憶體）的反應，該記憶體模組及/或記憶體可破裂成多塊，以至於使該記憶體是無法操作的及/或可使儲存於其中的資料是無法存取的。此時，方法 1100 可結束。

當此種由於企圖開啟該記憶體模組的外殼及/或記憶

體外殼而造成的記憶體外殼破裂可造成儲存在該記憶體中的資料對於可能被授權來存取這樣資訊的使用者（例如所有者）是無法存取的情況時，可判定儲存在該記憶體中的該資料可為這樣的機密本質，而使得儲存在該記憶體中的該資料無法被可能的攻擊者所存取的好處凌駕於授權使用者失去對於該資料的存取的不利之處。

第 12 圖描述根據本發明的態樣而可提供對於竄改攻擊的回應以幫助保全與記憶體相關聯的資料免於竄改的方法 1200。在 1202 處，可接收能指示竄改事件（例如竄改攻擊、竄改企圖）已經發生的資訊。在一個態樣中，反竄改元件（例如 106）可接收關於記憶體模組（例如 102）或與該記憶體模組相關聯的記憶體（例如 104）的竄改事件已經發生的資訊。

在一個態樣中，該反竄改元件可利用網目電路，該網目電路位於記憶體模組（例如 102）（與其中的記憶體（例如 104））與 PCB 之間及/或可連接至記憶體模組（例如 102）（與其中的記憶體（例如 104））與 PCB，其中，該記憶體模組與記憶體可電性連接於該 PCB。可提供檢測訊號（例如電壓）至該網目電路，該訊號的擾亂（例如訊號等級及/或強度的變化）及/或中斷連接可指示竄改事件已經發生。

根據另一態樣，可利用開關並放置該開關在該記憶體模組的外殼的鄰近部分之間及/或在該記憶體模組與該 PCB 之間或可置於其間的插座之間。當在未竄改狀態中時，該開關可為抑制模式（depressed mode）。如果開啟該

記憶體模組的外殼及/或從該 PCB 或插座中移除該記憶體模組，則可啟動該開關以使得該開關不再被抑制並可因此改變狀態（可提供竄改事件已經發生的指示）。

在 1204 處，可依據竄改事件是否已經發生來評估，且如果是如此，則評估已經發生的竄改事件的類型以（例如）判定是否可藉由啟動對於該竄改的回應來反擊該竄改事件。在 1206 處，可提供對於該竄改事件的回應，其中，例如該竄改事件是可能是對於竄改想要回應的類型。在一態樣中，對於竄改（例如偵測到與網目電路相關聯的檢測訊號的擾亂或中斷連接）的反應，竄改回應元件（例如 312）可依需要藉由抹除儲存在該記憶體中的資料、或部分資料以對於此種竄改提供回應，使得非授權個體（例如攻擊者）不能存取或觀看這些資料。在另一態樣中，對於竄改（例如用在該記憶體模組的外殼中的開關因為該記憶體模組從該 PCB 被移除及/或該記憶體模組的外殼被打開或分解而被轉動至不同狀態）的回應，該竄改回應元件可依需要例如藉由抹除儲存在該記憶體中的資料、或部分資料以提供回應，使得非授權個體不能存取或觀看這些資料。

在又另一態樣中，對於與該網目電路及/或開關相關聯的這些竄改攻擊的回應可為與該記憶體相關聯的一個或多個元件（例如電晶體、導電路徑等）的災難性故障及/或從容性故障，以使得該記憶體無法被個體所操作或無法存取。舉例來說，與該記憶體相關聯的一個或多個元件可被熔接在一起，以使得該記憶體無法使用且儲存其中的該資

料無法存取。此時，方法 1200 可結束。

參照至第 13 圖，係說明可結合系統 100、系統 200、系統 250、系統 300、系統 400、系統 500、及/或系統 600、或其一部分的例示性而非限制性的電子裝置 1300 的方塊圖。該電子裝置可包含（但不限於）電腦、膝上型電腦、網路設備（例如路由器、存取點）、媒體播放器及/或記錄器（例如聲音播放器及/或記錄器、影像播放器及/或記錄器）、電視、智慧卡、電話、行動電話、智慧型電話、電子記事簿（electronic organizer）、PDA、可攜式電子郵件讀取器、數位相機、電子遊戲（例如影像遊戲）、與數位權利管理相關聯的電子裝置、個人電腦記憶卡國際協會（Personal Computer Memory Card International Association，簡稱 PCMCIA）卡、信任平台模組（trusted platform module，簡稱 TPM）、硬體保全模組（Hardware Security Module，簡稱 HSM）、機上盒（set-top box）、數位影像記錄器、遊戲平台（gaming console）、導航系統（例如全球定位衛星（GPS）系統）、具有計算能力的保全記憶體裝置、具有防竄改（tamper-resistant）晶片的裝置、與工業控制系統相關聯的電子裝置、機器（例如飛機、影印機、機動車、微波爐）中的嵌入式電腦等等。

該電子裝置 1300 的元件可包含（但不限於）處理單元 1302、系統記憶體 1304（具有非揮發性記憶體 1306）以及能耦接各種系統元件（包含該系統記憶體 1304）至該處理單元 1302 的系統匯流排 1308。該系統匯流排 1308 可

為任何許多類型的匯流排結構（包含記憶體匯流排或記憶體控制器、周邊匯流排、或使用任何各種匯流排架構的區域匯流排）。

電子裝置 1300 通常可包含各種電腦可讀媒體。電腦可讀媒體可為能被該電子裝置 1300 所存取的任何可得到的媒體。作為範例但非用以限制，電腦可讀媒體可包括電腦儲存媒體與通訊媒體。電腦儲存媒體包含以任何方法或技術來實現用以儲存資訊（例如電腦可讀指令、資料結構、程式模組或其他資料）的揮發性與非揮發性、可移除性與非可移除性媒體。電腦儲存媒體包含（但不限於）RAM、ROM、EEPROM、非揮發性記憶體 1306（例如快閃記憶體）、或其他記憶體技術、CD-ROM、數位多功能碟片（DVD）或其他光碟儲存器、卡式磁盒、磁帶、磁碟儲存器或其他磁性儲存裝置、或可使用來儲存需要的資訊與可被電子裝置 1300 所存取的任何其他媒體。通訊媒體通常具體表現為電腦可讀指令、資料結構、程式模組或調變資料訊號（例如載波或其他傳輸機制）中的其他資料且包含任何資訊傳遞媒體。

該系統記憶體 1304 可包含揮發性及/或非揮發性記憶體 1306（例如記憶體 104）的形式的電腦儲存媒體。基本輸入/輸出系統（BIOS）（含有幫忙轉移在電子裝置 1300 內的組件之間的資訊的基本常式）可在例如起動（start-up）期間儲存在記憶體 1304 中。記憶體 1304 通常也包含可立即存取及/或目前由處理單元 1302 所操作的資料及/或程式

模組。作為範例但非用以限制，系統記憶體 1304 也可包含作業系統、應用程式、其他程式模組、與程式資料。

該非揮發性記憶體 1306 可為可移除式或不可移除式。舉例來說，該非揮發性記憶體 1306 可為可移除式記憶卡或 USB 快閃碟的形式。根據一個態樣，該非揮發性記憶體 1306 可包含例如快閃記憶體（例如單位元快閃記憶體、多位元快閃記憶體）、ROM、PROM、EPROM、EEPROM、或 NVRAM（例如 FeRAM）或其組合。再者，該快閃記憶體可包括 NOR 快閃記憶體及/或 NAND 快閃記憶體。

使用者可經由輸入裝置（未圖示）（例如鍵盤組、麥克風、書寫板（tablet）或觸控螢幕，但也可利用其他輸入裝置）來鍵入命令與資訊到該電子裝置 1300 中。這些與其他輸入裝置可經由可連接至該系統匯流排 1308 的輸入介面元件 1310 來連接至該處理單元 1302。也可利用其他介面與匯流排結構，例如平行埠、遊戲埠或通用序列匯流排（USB）。圖形子系統（未圖示）也可連接至該系統匯流排 1308。顯示裝置（未圖示）也可經由介面（例如可依序與影像記憶體連接的輸出介面元件 1312）來連接至該系統匯流排 1308。除了顯示器之外，該電子裝置 1300 也可包含其他周邊輸出裝置，例如可透過輸出介面元件 1312 來連接的揚聲器（未圖示）。

在此使用的用語「元件（component）」、「系統（system）」、「介面（interface）」等等係意指為電腦相關之個體，不論是硬體、軟體（例如執行中的）、及/或韌體。

舉例來說，元件可為在處理器運行的程序、處理器、物件、可執行物、程式、及/或電腦。經由圖示說明，在伺服器運行的應用程式與該伺服器兩者都可為元件。一個或多個元件可歸屬於程序且元件可局限在一個電腦及/或分佈在兩個或多個電腦之間。

在此使用的單字「範例（exemplary）」是意謂當作例子、實例、或圖例。在此描述成為「範例」的任何態樣或設計並不必要理解為較佳的或比其他態樣或設計更有好處的。

上面已經描述了包含本發明的態樣的例子。當然，雖然不可能為了描述本發明而描述元件或方法的每個可想到的組合，但是該技術領域中具有通常知識者可了解到本發明的許多進一步組合與排列都是可能的。因此，本發明係意欲涵蓋落入所附申請專利範圍之精神與範疇內的所有這類替代、修改及各種變化。再者，用於實施方式或申請專利範圍中之詞彙「包含（includes）」、「具有（has）」、或「具有（having）」、或其變化之範圍，此等詞彙將含括相似於詞彙「包括（comprising）」之方式，如同「包括（comprising）」被當作連接詞（transitional word）使用在申請專利範圍中那樣來詮釋。

【圖式簡單說明】

第 1 圖說明根據本發明的態樣而保全資料免於竄改的系統；

第 2a 圖說明根據本發明的一個實施例而保全資料的

系統；

第2b圖描述根據本發明的實施例而保全資料的系統；

第3圖說明根據本發明的態樣而保全資料的系統；

第4a圖說明根據本發明的態樣之包含記憶體裝置的電子裝置的例子的上視圖；

第4b圖描述根據本發明的態樣之包含記憶體裝置的電子裝置的例子的剖視圖；

第5圖說明根據本發明的態樣而幫助資料儲存的系統的方塊圖；

第6圖說明根據本發明的態樣而利用智能來幫助保全資料的系統的方塊圖；

第7圖描述根據本發明的態樣而用以幫助資料保全的分割記憶體的方塊圖；

第8圖說明根據本發明的態樣而幫助保全資料的方法；

第9圖說明根據本發明的態樣而可提供竄改證據以幫助保全與記憶體相關聯的資料的方法；

第10圖描述根據本發明的另一態樣而可提供竄改證據以幫助保全與記憶體相關聯的資料的方法；

第11圖描述根據本發明的態樣而可抵擋竄改攻擊以幫助保全與記憶體相關聯的資料的方法；

第12圖說明根據本發明的態樣而可提供回應給竄改攻擊以幫助保全與記憶體相關聯的資料的方法；以及

第13圖為根據本發明的態樣之可使用記憶體裝置的

例示電子裝置的方塊圖。

【主要元件符號說明】

100、200、250、300、400、500、600、700　系統

102	記憶體模組
104	記憶體
106	反竄改元件
202	主處理器
204	密碼元件
206	鑑別元件
208	鑑別介面元件
302	聚集元件
304	評估元件
306	竄改證據元件
308	電力供應器
310	竄改抵擋元件
312	竄改回應元件
402	電子裝置外殼
404	顯示元件
406	輸入元件
408	視窗元件
502	半導體基板
504	高密度核心區
506	電路系統
508	x解碼器

510 y解碼器

602 智能元件

604 呈現元件

702 早期開機與緊急碼分割區

704 作業系統分割區

706 操作子與OEM信任碼與資料分割區

708 第三方信任碼分割區

710 保全使用者資料（加密）分割區

712 普通使用者資料與可疑碼分割區

714 保全裝置金鑰分割區

716 保全認證與金鑰儲存分割區

800、900、1000、1100、1200 方法

802、804、902、904、906、1002、1004、1006、1008、1010 方塊

1012、1014、1016、1102、1104、1106、1202、1204、1206 方塊

1300 電子裝置

1302 處理單元

1304 系統記憶體

1306 非揮發性記憶體

1308 系統匯流排

1310 輸入介面元件

1312 輸出介面元件

七、申請專利範圍：

1. 一種幫助與一記憶體相關聯之資料保全之電子裝置，其包含：

該記憶體經組態以包含於該電子裝置內且包含複數個記憶體位置以幫助資料儲存，其中該記憶體進一步經組態以回應於與該記憶體相關聯之至少一竄改攻擊而提供至少一指示符；

一與該電子裝置之一外殼相關聯之視窗元件，其中該視窗元件經組態以幫助該至少一指示符之偵測以幫助與該記憶體相關聯之資料保全；及

一反竄改元件，其與該記憶體相關聯且經組態以對該至少一竄改攻擊做出反應以至少部分基於竄改攻擊之一類型幫助與該記憶體相關聯之資料保全，其中，當該至少一竄改攻擊涉及一企圖存取該記憶體之個體之鑑別時，該反竄改元件進一步經組態以幫助該至少一指示符之提供，其中該至少一指示符包含一含有該記憶體之記憶體外殼之一部分之至少一者之一色彩狀態改變或包含於該記憶體外殼內一指示符元件之一色彩狀態改變之至少一者，使得該至少一指示符可經由該視窗元件感知以幫助該至少一竄改攻擊之偵測。

2. 如請求項 1 之電子裝置，其進一步包含：

一鑑別元件，其經組態以接收一鑑別憑證，判斷

該鑑別憑證係有效或該鑑別憑證係無效之至少一者，且若該鑑別憑證係有效時同意與該記憶體相關聯之存取權之一子集，其中存取權之該子集係至少部分基於該鑑別憑證。

3. 如請求項 2 之電子裝置，其中該鑑別元件進一步經組態以評估與一無效鑑別憑證相關聯之資訊，判斷達到一預定之鑑別企圖之最大數目或未達到該預定之鑑別企圖之最大數目之至少一者，若未達到該預定之鑑別企圖之最大數目則增加與該等鑑別企圖相關聯之一計數，若未達到該預定之鑑別企圖之最大數目則提示該個體提供另外的鑑別憑證，且至少部分基於該計數判定該至少一竄改事件發生或一竄改事件並未發生之至少一者。

4. 如請求項 1 之電子裝置，其中至少部分基於該竄改攻擊之類型回應於該至少一竄改攻擊，下列至少一者成立：該記憶體外殼包含改變其顏色狀態之一材料或該指示符元件包含改變其顏色狀態之一光源。

5. 如請求項 1 之電子裝置，竄改攻擊之該類型係下列至少一者：與無效鑑別資訊相關聯之該記憶體之一存取、將該記憶體自一印刷電路板移除、與該記憶體相關聯之一殼體之一斷裂、一旁通道攻擊、或一錯誤攻擊。

6. 一種幫助與一記憶體相關聯之資料保全之系統，其包含：

該記憶體經組態以包括複數個記憶體位置以幫助資料儲存；

一反竄改元件，其經組態以與該記憶體相關聯且經組態以對與該記憶體相關聯之至少一竄改攻擊做出反應以至少部分基於竄改攻擊之一類型幫助與該記憶體相關聯之資料保全，其中，當該至少一竄改攻擊涉及一企圖存取該記憶體之個體之鑑別時，該反竄改元件進一步經組態以回應於該至少一竄改攻擊提供至少一指示符，其中該至少一指示符包含一含有該記憶體之記憶體模組之一部分之至少一者之一色彩狀態改變或與該記憶體模組相關聯之一指示符元件之一色彩狀態改變之至少一者，使得該至少一指示符可經由一視窗元件感知以幫助該至少一竄改攻擊之偵測，該視窗元件與一電子裝置相關聯，該記憶體模組經組態位於該電子裝置內。

7. 如請求項 6 之系統，竄改攻擊之該類型係下列至少一者：與無效鑑別資訊相關聯之該記憶體之一存取、將該記憶體自一印刷電路板移除、與該記憶體相關聯之一殼體之一斷裂、一旁通道攻擊、或一錯誤攻擊。

8. 如請求項 6 之系統，該反竄改元件進一步經組態以回應於該至少一竄改攻擊提供下列至少一者：該至少一竄改攻擊的證據、該至少一竄改攻擊的抵擋、或該至少一竄改攻擊的回應。

9. 如請求項 6 之系統，其進一步包含該記憶體模組，該

記憶體模組經組態以包含至少該記憶體。

10. 如請求項 9 之系統，該反竄改元件進一步經組態以使用一與該記憶體模組及一印刷電路板相關聯之網目（mesh）電路，且進一步經組態以幫助施加一預定電壓位準至該網目電路，其中該反竄改元件進一步經組態以至少部分基於該預定電壓位準的變化來判定該至少一個竄改攻擊已經發生且進一步經組態以藉由儲存在該記憶體中的至少一部分資料的抹除、該記憶體的災難性故障、或該記憶體的從容性故障的至少其中一者來回應該至少一個竄改攻擊。

11. 如請求項 9 之系統，該記憶體模組之一殼體係由一材料組成，該材料至少部分基於竄改攻擊之該類型改變其色彩狀態，該反竄改元件進一步經組態以偵測存取該記憶體之一未授權企圖且幫助該材料之該色彩狀態之該改變以指示該至少一竄改攻擊已經發生。

12. 如請求項 11 之系統，其進一步包含該視窗元件，其中該記憶體模組經組態以包含於與該電子裝置相關聯之一殼體內且該視窗元件經組態以相對於該記憶體模組於與該電子裝置相關聯之該殼體內之位置定位於與該電子裝置相關聯之該殼體之一表面上，使得該記憶體模組之該殼體可以被至少一使用者經由該視窗元件之一透明部分看見，該視窗元件之該透明部分使該至少一使用者感知該記憶體模組之該殼體。

13. 如請求項 9 之系統，該記憶體模組之一殼體、或該記

憶體之一殼體之至少一者係由脆性材料形成，其回應於被打開斷裂成多片且使得儲存於該記憶體中之資料無法存取。

14. 如請求項9之系統，該至少一竄改攻擊包含打開該記憶體模組之一殼體，該反竄改元件進一步經組態以採用與該記憶體模組之該殼體相關聯之一開關，其中該開關經組態以當該記憶體模組之該殼體被打開時改變狀態，該反竄改元件進一步經組態以偵測該開關之狀態改變、將該狀態改變識別為該至少一竄改攻擊、且藉由儲存在該記憶體中的至少一部分資料的抹除、該記憶體的災難性故障、或該記憶體的從容性故障的至少其中一者來回應該至少一個竄改攻擊。

15. 如請求項9之系統，其進一步包含：

一鑑別元件，其經組態以幫助與該個體相關聯之一鑑別憑證之驗證以至少部分基於一有效鑑別憑證控制該記憶體之存取；及

一密碼元件，其經組態以執行資料加密及解密，其中該至少一竄改攻擊包含一旁通道攻擊、或一錯誤攻擊之至少一者，其中該反竄改元件進一步經組態以採用放置於該記憶體模組之該殼體內之一屏蔽（shield）且幫助降低放射與該資料加密或資料解密相關聯之資訊至該記憶體模組的該殼體外部以幫助抵抗該至少一竄改攻擊，其中該旁通道攻擊與相關於該記憶體或該密碼元件之至少一者之相關聯的電磁輻射、

電力消耗、或射頻特性的資訊之至少一者相關聯。

16. 如請求項6之系統，該記憶體包含非揮發性記憶體。

17. 一種包含請求項6之系統之電子裝置。

18. 如請求項17之電子裝置，其中該電子裝置包含電腦、膝上型電腦、網路配備、媒體播放器、媒體記錄器、電視、智慧卡、電話、行動電話、智慧型電話、電子記事簿、個人數位助理、可攜式電子郵件讀取器、數位相機、電子遊戲、與數位權利管理相關聯的電子裝置、個人電腦記憶卡國際協會（Personal Computer Memory Card International Association，簡稱 PCMCIA）卡、信任平台模組（trusted platform module，簡稱 TPM）、硬體保全模組（Hardware Security Module，簡稱 HSM）、機上盒（set-top box）、數位影像記錄器、遊戲平台（gaming console）、導航系統、具有計算能力的保全記憶體裝置、具有至少一個防竄改晶片的裝置、與工業控制系統相關聯的電子裝置、或機器中的嵌入式電腦、或其組合中的至少一者，其中，該機器包括飛機、影印機、機動車、或微波爐中之一者。

19. 一種幫助與一記憶體相關聯之資料保全之方法，其包含：

接收關於與該記憶體相關聯的至少一個竄改事件的資訊；以及

部分基於竄改事件的類型來對該至少一個竄改事件作出反應以幫助保全與該記憶體相關聯之該資料，

其中該至少一竄改事件涉及一企圖存取該記憶體之個體之鑑別，且其中對該至少一個竄改事件作出反應進一步包含當判定該至少一個竄改事件發生，則至少提供該至少一個竄改事件的證據，與該至少一個竄改事件相關聯的該證據包括改變與容納該記憶體的殼體相關聯的色彩狀態或使容納該記憶體的該殼體變形的至少一者。

20. 如請求項 19 之方法，該部分基於竄改事件的類型來對該至少一個竄改事件作出反應進一步包含下列至少一者：提供與該至少一竄改事件相關聯的證據、抵擋該至少一竄改事件、或回應該至少一竄改事件。

21. 如請求項 20 之方法，其進一步包含：

接收與該至少一個竄改事件相關聯的資訊，該竄改事件包括以下至少一者：企圖獲得對該記憶體的未經授權的存取、開啟容納該記憶體的殼體、或破壞與容納該記憶體的該殼體相關聯的封條；

評估該接收的資訊；

判定該至少一個竄改事件發生或竄改事件未發生的至少其中一者；以及

當判定該至少一個竄改事件發生，則提供與該至少一個竄改事件相關聯的證據，與該至少一個竄改事件相關聯的該證據包括改變與容納該記憶體的殼體相關聯的色彩狀態或使容納該記憶體的該殼體變形的至少一者。

22. 如請求項 20 之方法，其進一步包含：

接收一鑑別憑證；

判定該鑑別憑證是有效或該鑑別憑證是無效的至少一者；

當該鑑別憑證是有效的，則同意與該記憶體相關聯的存取權利的子集，該存取權利的子集係部分依據該鑑別憑證；

評估與一無效鑑別憑證相關聯的資訊；

判定要鑑別的企圖次數已達到預定的最大次數或要鑑別的企圖次數未達到該預定的最大次數的至少其中一者；

當要鑑別的企圖次數未達到該預定的最大次數，則增加與要鑑別的該企圖相關聯的一計數；

當要鑑別的企圖次數未達到該預定的最大次數，則提示該個體以提供鑑別憑證；及

部分依據該計數來判定該至少一個竄改事件發生或竄改事件未發生的至少其中一者。

23. 如請求項 20 之方法，其進一步包含：

接收與該至少一個竄改事件相關聯的資訊，該竄改事件包括企圖開啟容納該記憶體的一殼體；

評估該接收的資訊；

判定該至少一個竄改事件發生或竄改事件未發生的至少其中一者；以及

當判定該至少一個竄改事件發生，則抵擋該至少

一個竄改事件，其中抵擋該至少一個竄改事件包括將容納該記憶體的該殼體破裂成為多塊，並且使得儲存在該記憶體中的該資料無法存取。

24. 如請求項 20 之方法，其進一步包含：

接收與該至少一個竄改事件相關聯的資訊，該竄改事件包括改變與容納該記憶體的殼體相關聯的開關的狀態或擾亂與該記憶體相關聯的一網目電路相關聯的電壓訊號之至少一者；

評估該接收的資訊；

判定該至少一個竄改事件發生或竄改事件未發生的至少一者；以及

當判定該至少一個竄改事件發生，則回應該至少一個竄改事件，對於該至少一個竄改事件的該回應包括下列至少一者：抹除儲存在該記憶體中的至少一部分資料、產生該記憶體的災難性故障、或產生該記憶體的從容性故障。

25. 一種幫助與一記憶體相關聯之資料保全之系統，其包含：

用於將資料儲存於該記憶體中之構件；

用於至少部分基於竄改攻擊之類型，提供一竄改攻擊的證據、抵擋一竄改攻擊、或回應一竄改攻擊以幫助與該記憶體相關聯之資料保全的構件；及

用於改變與包括該記憶體之一記憶體殼體相關聯的一色彩狀態以幫助至少部分基於竄改攻擊之類型提

供該竄改攻擊的證據的構件，其中，回應於該竄改攻擊，該用於改變一色彩狀態之構件改變該記憶體殼體之一表面之至少一部分之一色彩狀態、或改變容納於該記憶體殼體中且與其相關聯之一指示器元件之一色彩狀態之至少一者，其中該記憶體殼體之該表面之該至少一部分之該色彩狀態之改變或該指示器元件之該色彩狀態之改變可經由一視窗元件感知以幫助該竄改攻擊之偵測，該視窗元件與一電子裝置相關聯，該記憶體位於該電子裝置內。

26. 如請求項25之系統，其進一步包含：

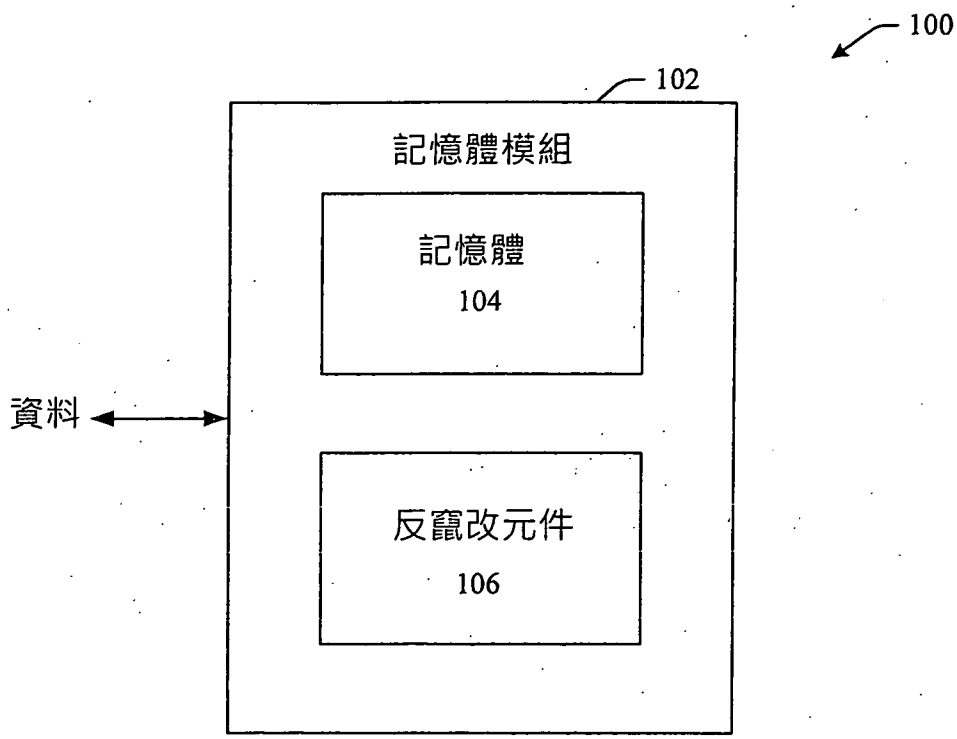
用於鑑別至少一使用者之構件；

用以提供對於容納包含該記憶體的該記憶體殼體的一電子裝置有一透明的視野，以幫助察覺該色彩狀態的一改變的構件；

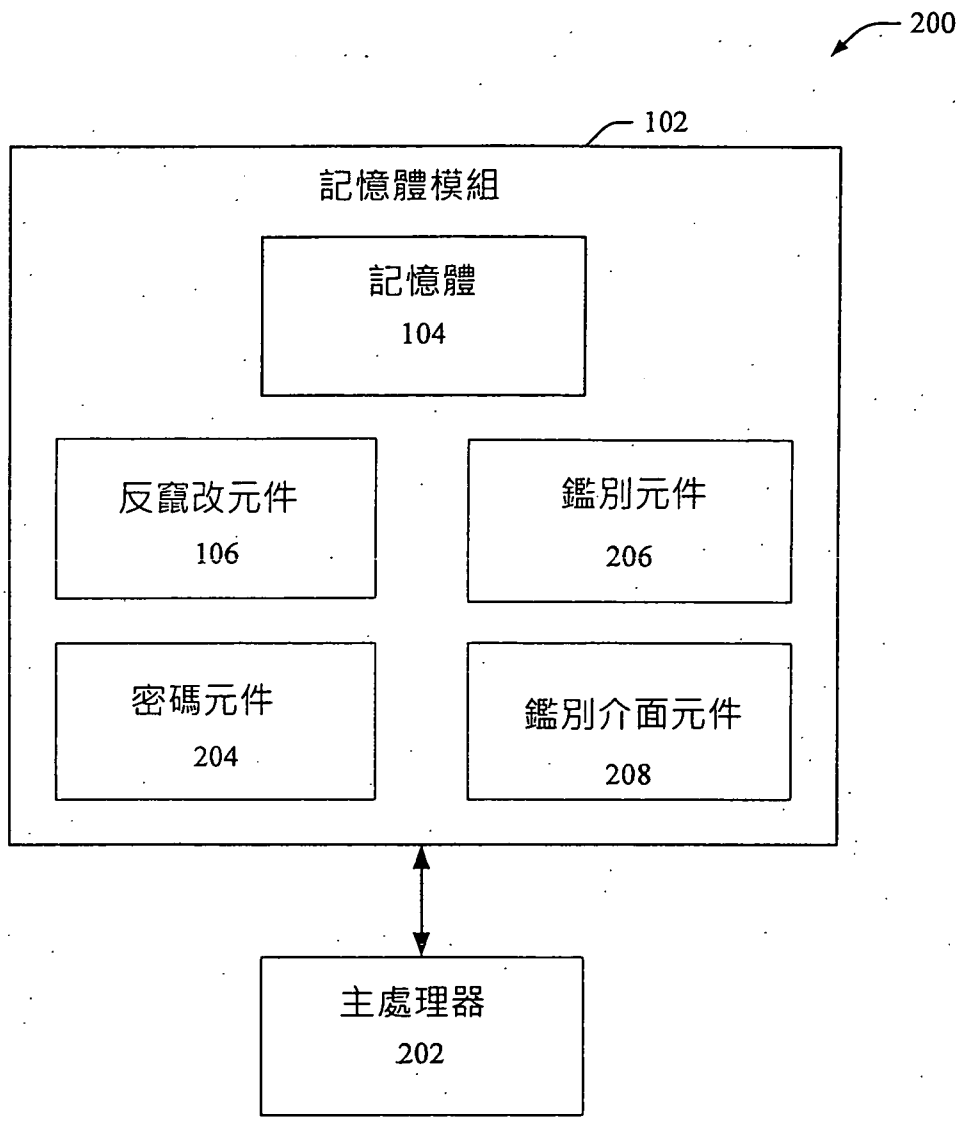
用以供應電力以幫助保全與該記憶體相關聯的該資料的構件；以及

用以評估與一竄改攻擊相關聯的資訊的構件。

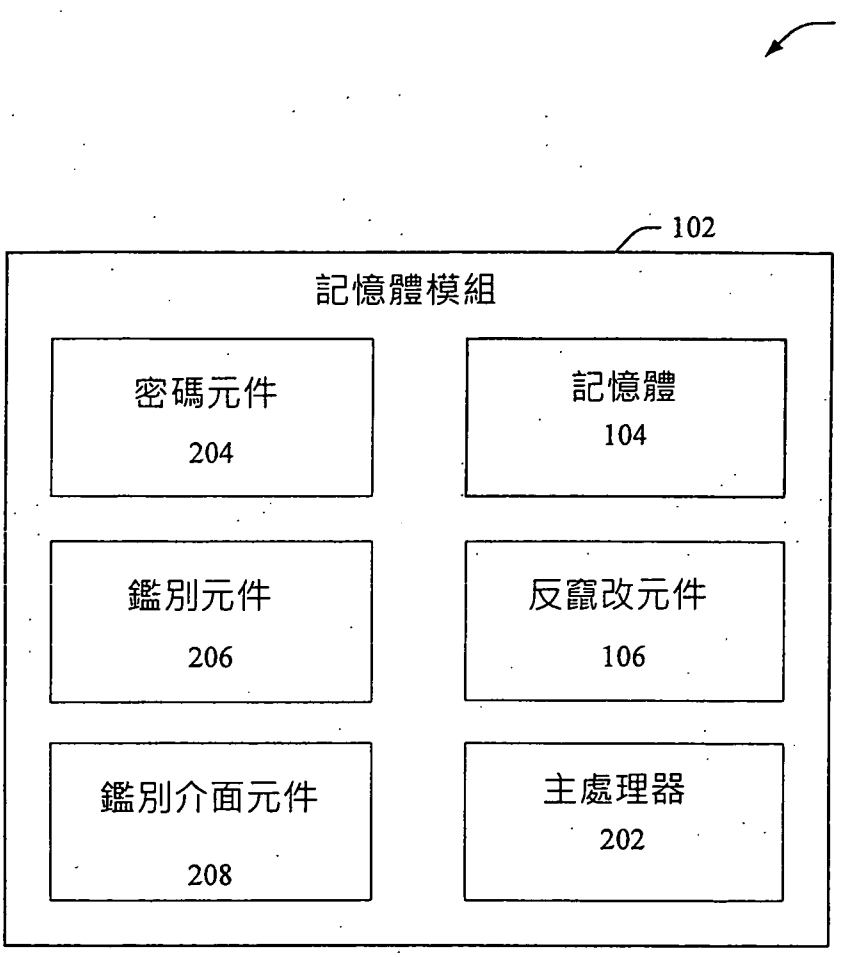
八、圖式:



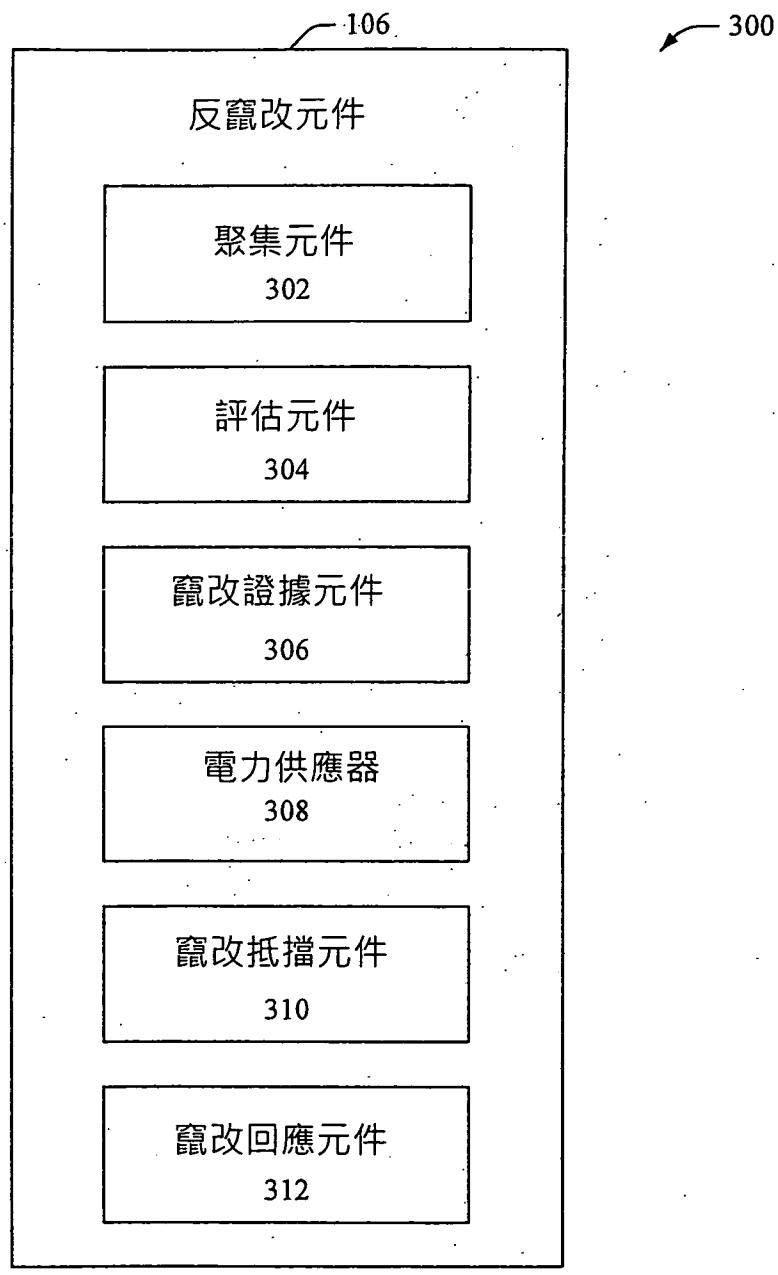
第 1 圖


200
102
記憶體模組
記憶體
104
反竄改元件
106
鑑別元件
206
密碼元件
204
鑑別介面元件
208
主處理器
202

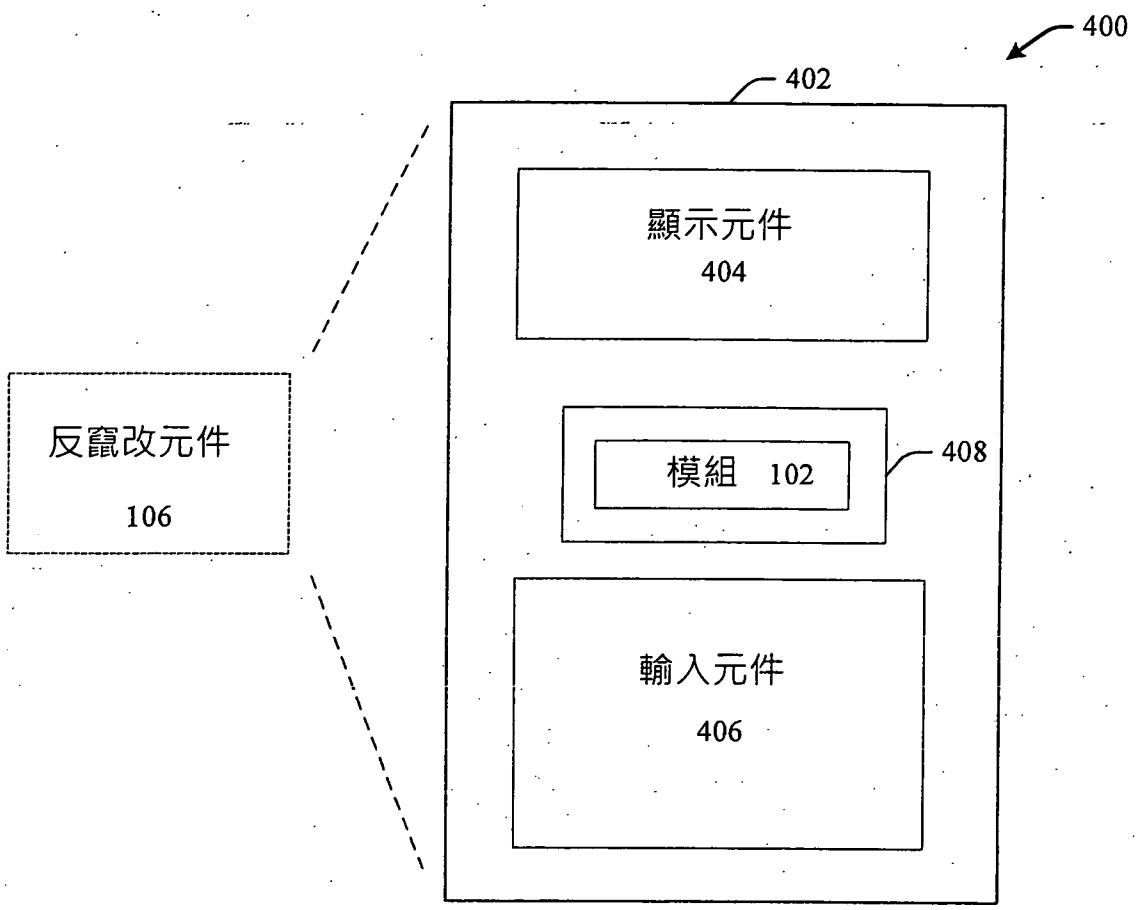
第 2a 圖


250
102
記憶體模組
密碼元件
204
記憶體
104
鑑別元件
206
反竄改元件
106
鑑別介面元件
208
主處理器
202

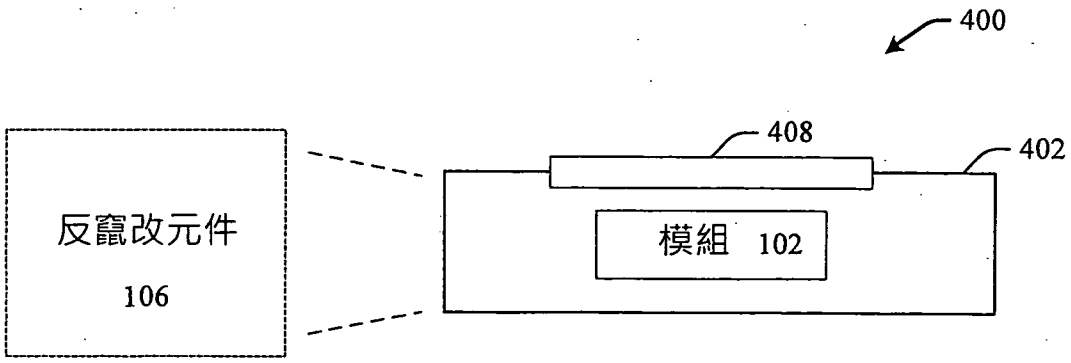
第 2b 圖


106
300
反竄改元件
聚集元件
302
評估元件
304
竄改證據元件
306
電力供應器
308
竄改抵擋元件
310
竄改回應元件
312

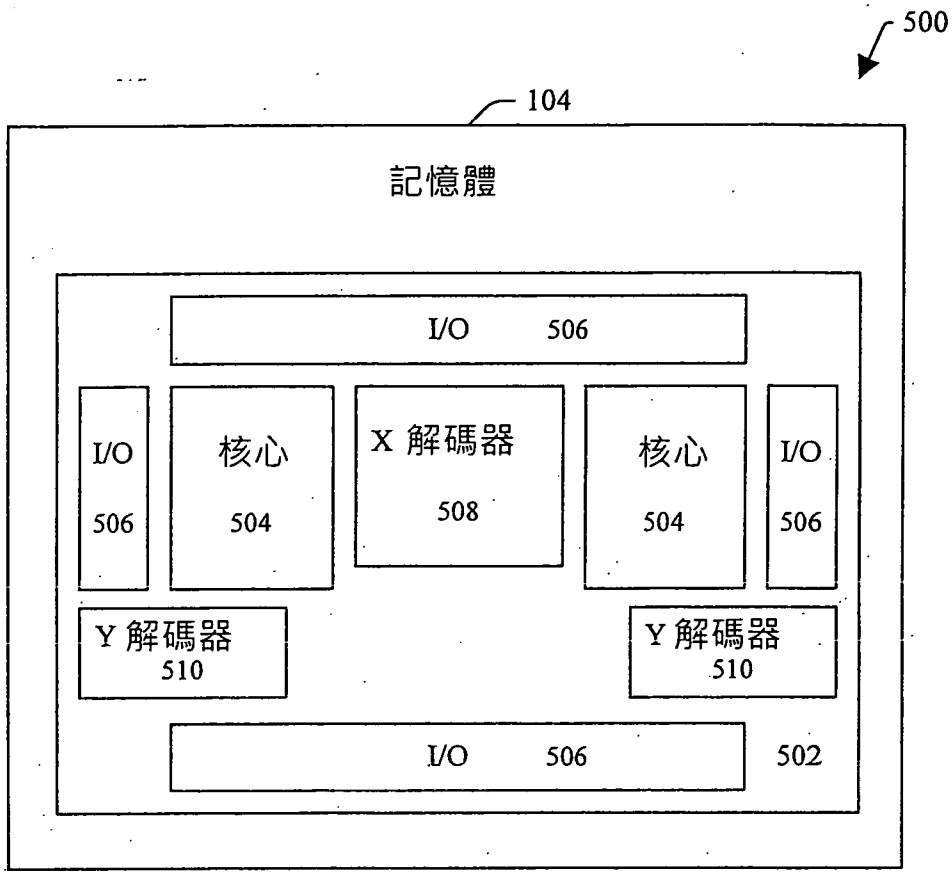
第 3 圖


400
402
顯示元件
404
反窺改元件
106
模組 102
408
輸入元件
406

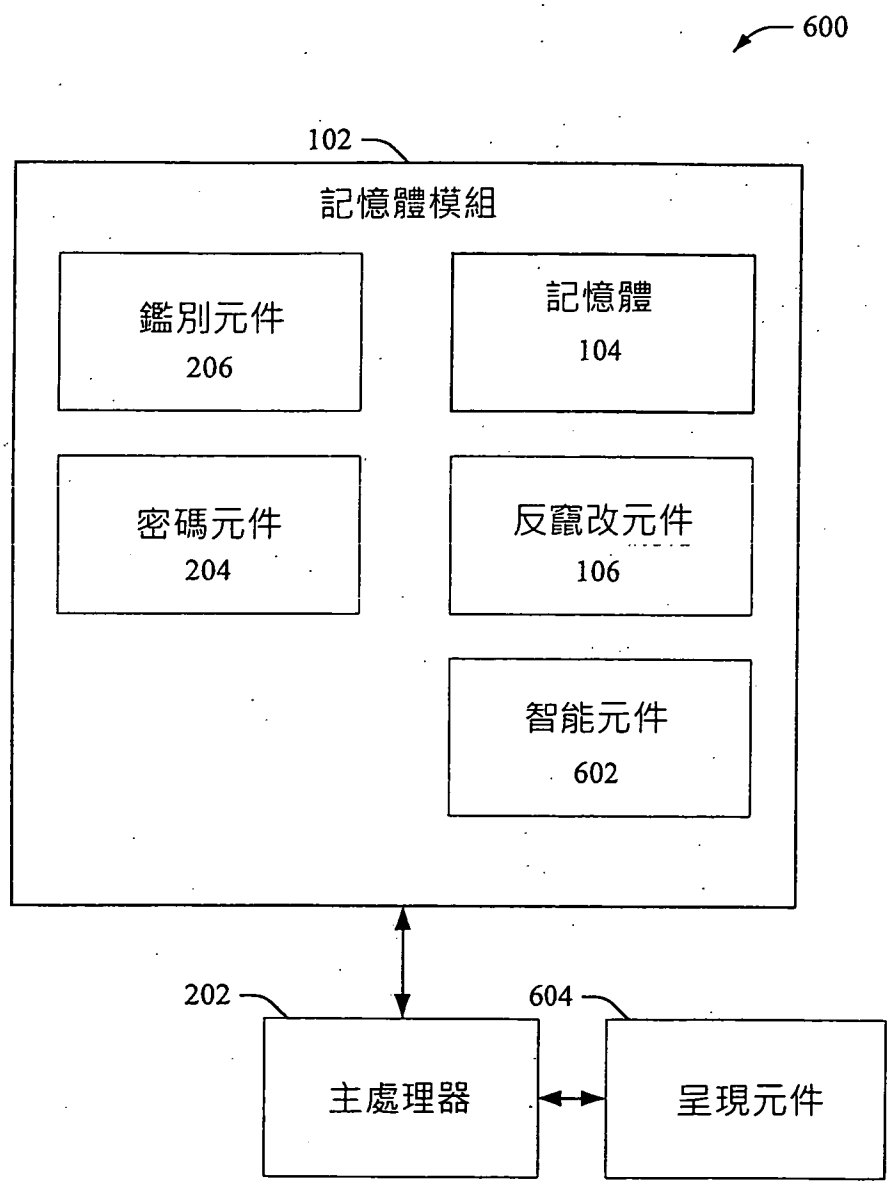
第 4a 圖


400
408
402
反窺改元件
106
模組 102

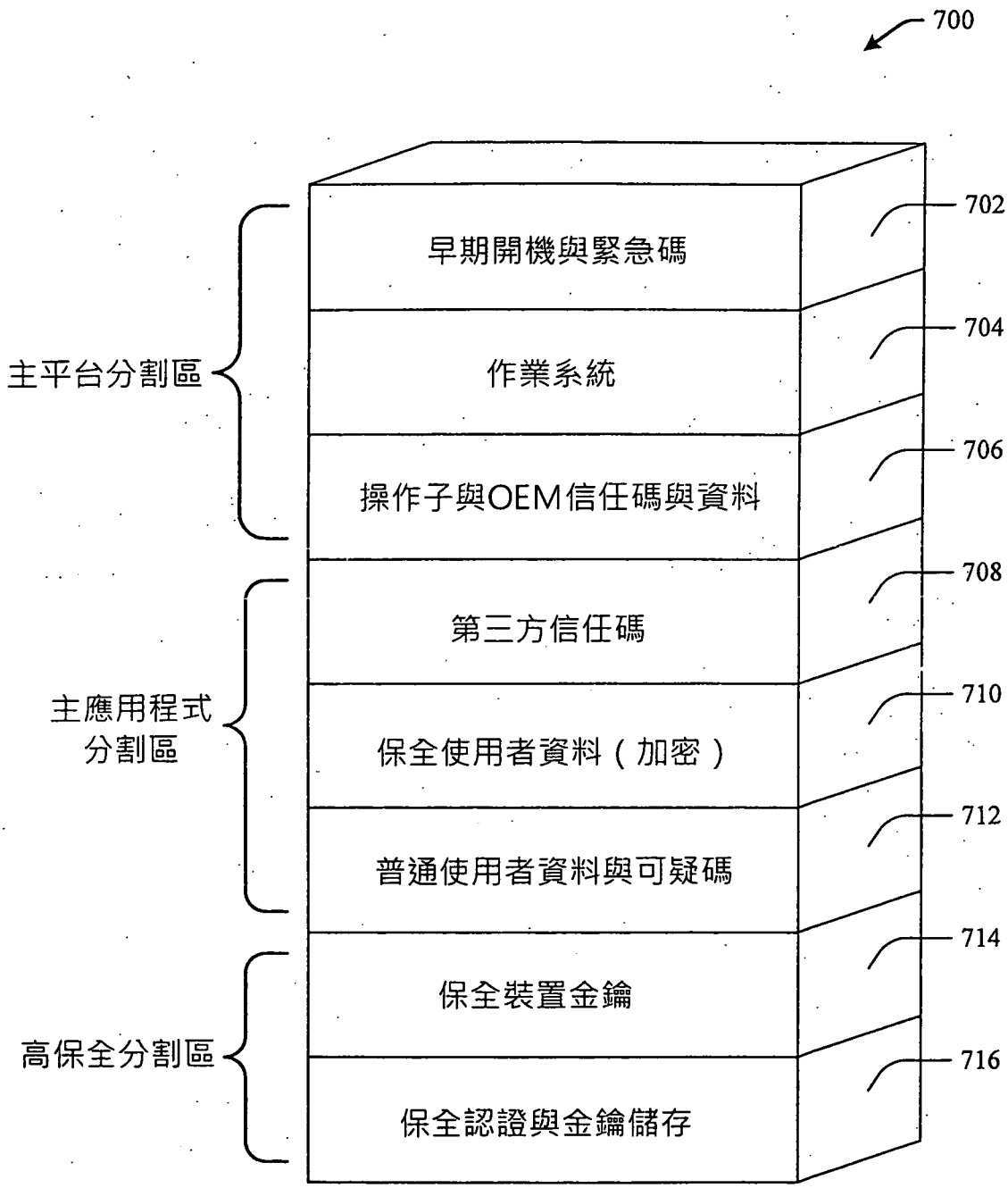
第 4b 圖


500
104
記憶體
I/O 506
I/O 506
核心 504
X 解碼器 508
核心 504
I/O 506
Y 解碼器 510
Y 解碼器 510
I/O 506
502

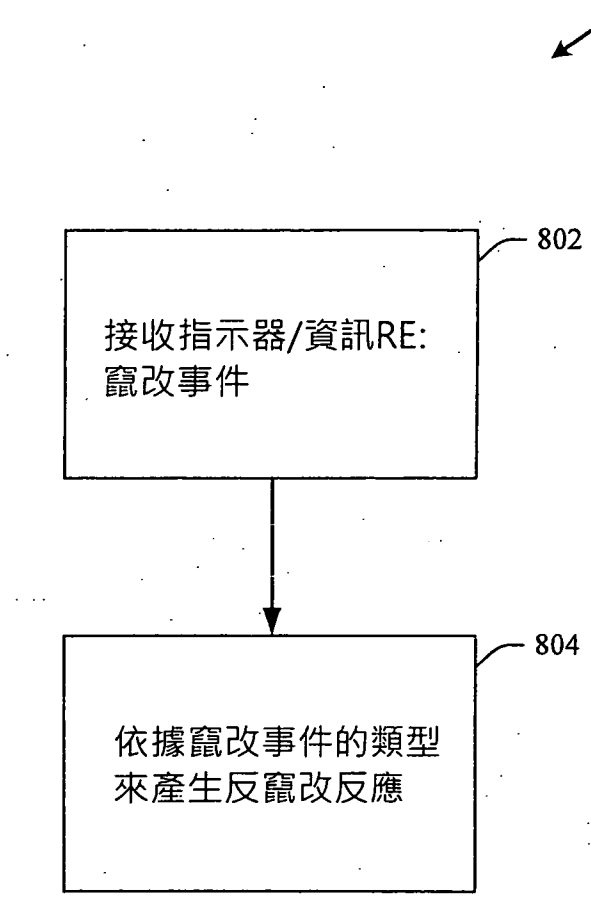
第 5 圖


600
102
記憶體模組
鑑別元件
206
記憶體
104
密碼元件
204
反竄改元件
106
智能元件
602
202
604
主處理器
呈現元件

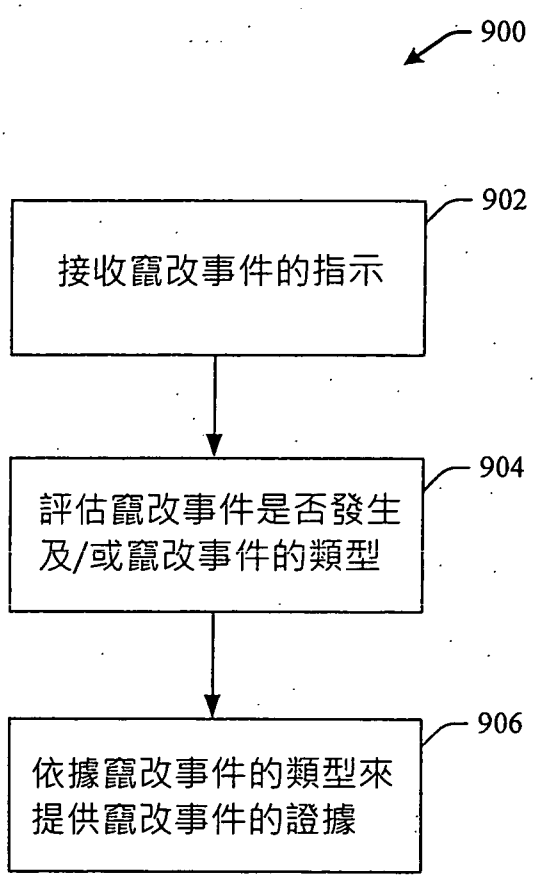
第 6 圖


700
早期開機與緊急碼
作業系統
操作子與OEM信任碼與資料
第三方信任碼
保全使用者資料（加密）
普通使用者資料與可疑碼
保全裝置金鑰
保全認證與金鑰儲存
主平台分割區
主應用程式分割區
高保全分割區
702
704
706
708
710
712
714
716

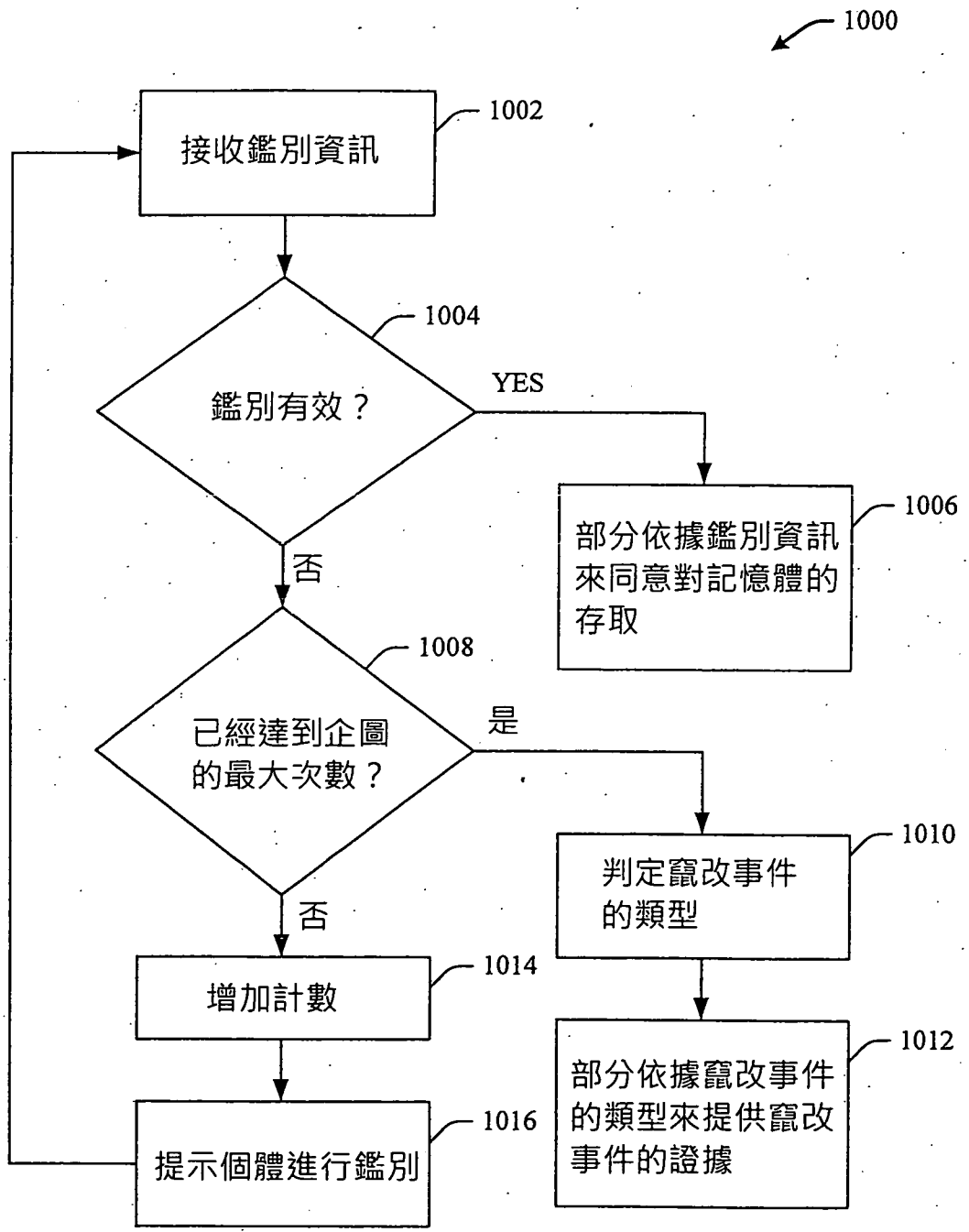
第 7 圖



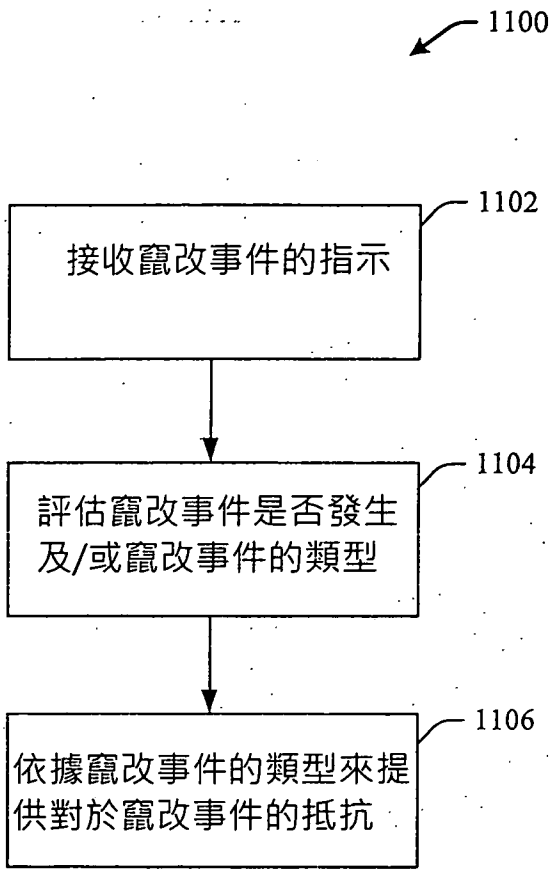
第 8 圖


900
902
接收竄改事件的指示
904
評估竄改事件是否發生及/或竄改事件的類型
906
依據竄改事件的類型來提供竄改事件的證據

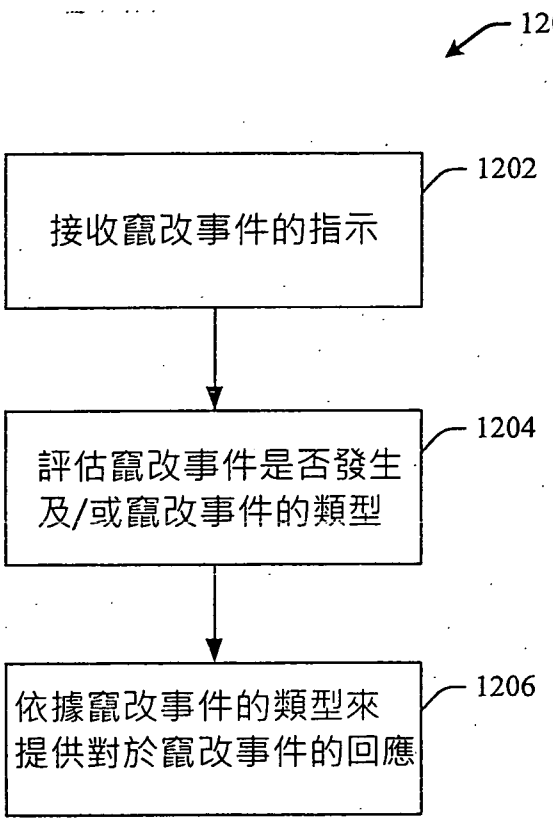
第 9 圖


1000
接收鑑別資訊
1002
鑑別有效？
1004
YES
否
部分依據鑑別資訊來同意對記憶體的存取
1006
已經達到企圖的最大次數？
1008
是
否
判定竄改事件的類型
1010
增加計數
1014
部分依據竄改事件的類型來提供竄改事件的證據
1012
提示個體進行鑑別
1016

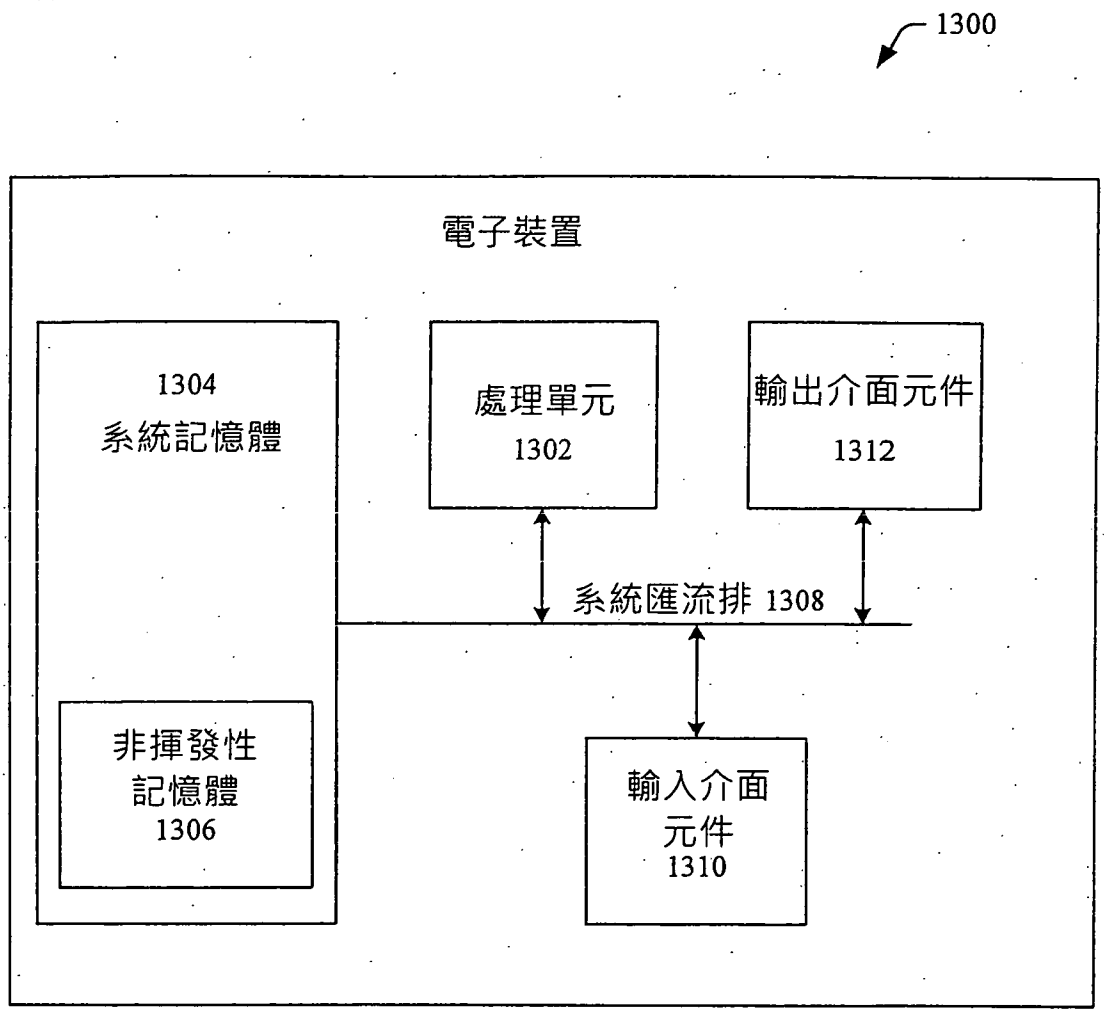
第 10 圖


1100
1102
接收竄改事件的指示
1104
評估竄改事件是否發生及/或竄改事件的類型
1106
依據竄改事件的類型來提供對於竄改事件的抵抗

第 11 圖


1200
接收竄改事件的指示
1202
評估竄改事件是否發生及/或竄改事件的類型
1204
依據竄改事件的類型來提供對於竄改事件的回應
1206

第 12 圖


1300
電子裝置
1304
系統記憶體
處理單元
1302
輸出介面元件
1312
系統匯流排 1308
非揮發性
記憶體
1306
輸入介面
元件
1310

第 13 圖