201939341

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201939341 A

(43)公開日： 中華民國 108 (2019) 年 10 月 01 日

(21)申請案號：108107471 (22)申請日： 中華民國 108 (2019) 年 03 月 06 日

(51)Int. Cl.： *G06F21/72 (2013.01)*

(30)優先權：2018/03/15 美國 62/643,539

2018/08/21 美國 16/106,564

(71)申請人：美商阿它佧瑪有限公司 (美國) ATAKAMA LLC (US)

美國

(72)發明人：格蘭斯 丹尼爾H GALLANCY, DANIEL H. (US)；阿若捏斯逖 艾瑞克A ARONESTY, ERIK A. (US)；捏米偌弗斯基 帝米崔 NEMIROVSKY, DIMITRI (US)

(74)代理人：陳昭明

申請實體審查：無 申請專利範圍項數：24 項 圖式數：10 共 55 頁

(54)名稱

用於靜止資料之免密碼保全系統

(57)摘要

本發明所揭露之實施例包括用於保全靜止資料的免密碼方法。該方法包括以密碼金鑰加密及/或解密資料。例如，經加密之資料可被儲存於第一裝置之非暫態運算電腦記憶體上。該方法可包括基於密碼金鑰產生金鑰碎片，密碼金鑰可自金鑰碎片重建，並將金鑰碎片分布於裝置中，使得由於第一裝置因缺乏密碼金鑰而無法解密經加密之資料，而將經加密之資料保全於第一裝置。

The disclosed embodiments include a passwordless method for securing data-at-rest. The method includes encrypting and/or decrypting data with a cryptographic key. For example, the encrypted data can be stored on a non-transitory computer memory of a first device. The method can include generating key shards based on the cryptographic key, which can be reconstituted from the key shards, and distributing the key shards among devices such that the encrypted data is secured at the first device because the first device is incapable of decrypting the encrypted data due to an absence of the cryptographic key.

指定代表圖：

TW 201939341 A

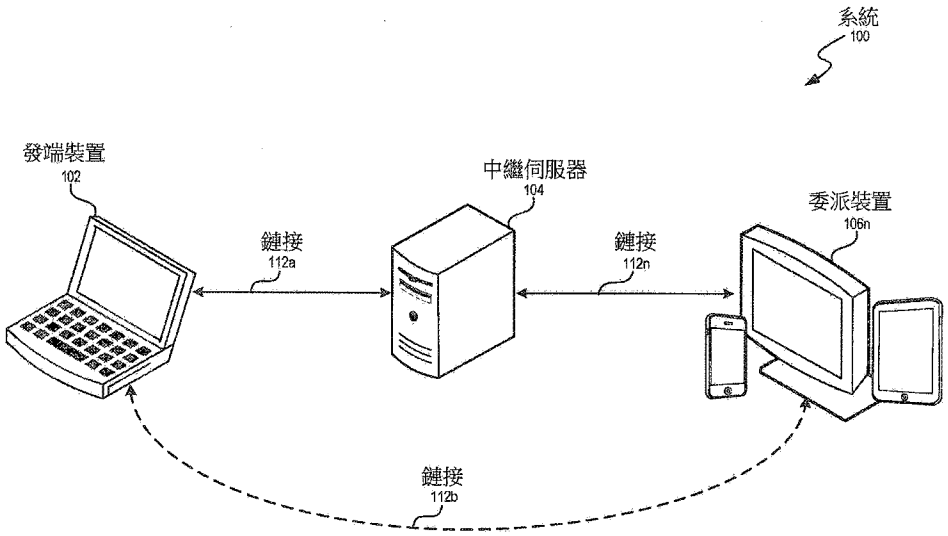


圖1

符號簡單說明：

100・・・系統

102・・・發端裝置

104・・・中繼伺服器

106n・・・委派裝置

112a、112b、

112n・・・鏈接

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】（中文/英文）

用於靜止資料之免密碼保全系統／PASSWORDLESS SECURITY SYSTEM FOR DATA-AT-REST

相關申請案之交互參照

【0001】 本申請案主張2018年8月21日申請之美國發明專利申請案第16/106,564號的優先權，該美國發明專利申請案主張2018年3月15日申請之美國臨時發明專利申請案第62/643,539號之優先權，發明名稱為「靜止資料之免密碼加密」，上述兩件申請案以其等之整體併入此處作為參考。

【技術領域】

【0002】 所揭示之教示一般而言是有關於資料加密及/或解密。所揭示之教示更特別是有關於用以保全靜止資料之免密碼加密及/或解密技術。

【先前技術】

【0003】 該用語「靜止資料(data-at-rest)」通常是用作「使用中資料(data-in-use)」及「傳輸中資料(data-in-transit)」之互補詞，其等共同界定了數位資料的三個階段。靜止資料通常表示以數位形式被實體儲存(stored physically)的非活動資料(inactive data)(例如，資料庫、資料倉庫(data warehouses)、試算表、檔案室(archives)、磁帶(tapes)、異地備份(off site backups)、行動裝置)。例如，靜止資料可以表示被儲存於不變性存儲器(non-volatile storage，例如，磁碟、磁帶)的資料，而使用中資料可表示正由一運算電腦之處理器處理或是被暫時儲存於揮發性記憶體(例如，隨機存取

記憶體)中的資料。雖然一般接受的是無論其儲存媒體為何，歸檔資料(archive data，即，從不改變者)是靜止資料，且受到頻繁改變之現用資料(active data)為使用中資料，「非活動」資料可包括可能不頻繁地改變的資料。因此，靜止資料之不精確的本質可涵蓋更廣的資料之狀態。

【0004】 靜止資料的保全對於商業、政府單位及其他機構具有增加的顧慮。行動裝置(例如，智慧型手機)通常受到在遺失或被偷時保護靜止資料被未授權存取之特定保全協定所保護。越來越多之認知在於，資料庫管理系統及檔案伺服器應亦被考量具有風險。特別是，資料在儲存器中留置未使用的時間越長，其越容易由惡意行為者(bad actors)擷取。

【0005】 資料的加密預防了在未授權之存取事件中的被窺見性(visibility)，其通常被用以保護使用中資料或傳輸中資料，及/或用以保護儲存靜止資料之儲存媒體。例如，可在容置(houses)資料的資料庫以及在資料庫被儲存的實體儲存器上實行加密。對資料容器之存取可要求解鎖容器以解密其所有內容之一密碼及/或密碼金鑰(encryption key)。在一些情形中，某些敏感檔案(sensitive files)是以個別的密碼金鑰加密，該等密碼金鑰是與該資料分開儲存。因此，保全靜止資料通常涉及高風險之「無法妥協(all or nothing)」途徑，或與該檔案分開儲存及管理之令人望而卻步的複雜金鑰集合。

【發明內容】

【0006】 所揭示的實施例包括至少一免密碼方法及至少一用於保全靜止資料的裝置。該方法包括以一密碼金鑰加密資料。經加密之資料被儲

存於一第一裝置之一非暫態運算電腦記憶體上。該方法包括基於該密碼金鑰產生金鑰碎片，該密碼金鑰可自該等金鑰碎片重建。該方法進一步包括將該等金鑰碎片分布(distributing)於裝置中(among devices)，使得由於缺乏該密碼金鑰，該第一裝置無法解密該加密資料而將該加密資料保全於該第一裝置。

【0007】 在一些實施例中，將該等金鑰碎片分布包括經由一運算電腦網路使一金鑰碎片與遠離該第一裝置之一裝置通訊。在一些實施例中，將該等金鑰碎片分布包括經由一短距無線電鏈(short-range radio link)而使一金鑰碎片與遠離該第一裝置之一裝置通訊。於一些實施例中，將該等金鑰碎片分布包括於該第一裝置及該等裝置之間建立一無線鏈(wireless link)及一有線鏈(wired link)，以與個別的金鑰碎片通訊。於一些實施例中，將該等金鑰碎片分布包括經由藍芽(BLUETOOTH)、Wi-Fi、乙太網路、視覺鏈接(visual link)、聽覺鏈接(auditory link)、或USB鏈接的任一者而於該第一裝置及一裝置之間建立一通訊鏈(communication link)。於一些實施例中，將該等金鑰碎片分布包括通過蜂巢式鏈(cellular link)於該第一裝置及一裝置之間建立一通訊鏈。於一些實施例中，將該等金鑰碎片分布包括以一獨特公共金鑰加密一金鑰碎片，使得經加密之金鑰碎片被分布至具有一對應私人金鑰的一裝置，該對應私人金鑰使經加密之金鑰碎片的解密得以進行。

【0008】 於一些實施例中，該等裝置包括消費者電子裝置(例如，手持行動裝置)。於一些實施例中，該等裝置及該第一裝置屬於一單一使用者，該單一使用者是被授權以存取該加密資料。於一些實施例中，該等裝置包括一運算裝置，其屬於未被授權以存取該加密資料的一使用者。於一些實

施例中，該第一裝置及該等裝置包含一伺服器、一個人電腦及一智慧型手機的各者。於一些實施例中，該等裝置是間歇式通訊耦接至(intermittently communicatively coupled to)該第一裝置。於一些實施例中，該非暫態運算電腦記憶體是一智慧型手機或平板電腦的一局部記憶體，且經加密之資料包括儲存於該局部記憶體上的檔案。

【0009】 於一些實施例中，該密碼金鑰是一第一密碼金鑰且該非暫態運算電腦記憶體儲存有各自以個別密碼金鑰所加密之資料檔，包括以該第一密碼金鑰加密的一第一資料檔。

【0010】 於一些實施例中，該第一裝置具有用於該等裝置之各者的一公共金鑰，該等裝置各自具有一對應私人金鑰，且將該等金鑰碎片分布至該等裝置包含以一個別公共金鑰加密各裝置之各金鑰碎片，使得多個經加密之金鑰碎片被分布至該等裝置，且各裝置可在被請求時解密其經加密之金鑰碎片，並將經解密之金鑰碎片返還給一請求者。

【0011】 於一些實施例中，該方法進一步包括自該等裝置收集至少一部分之該等金鑰碎片、自經收集之該等金鑰碎片重建該密碼金鑰，並以經重建之該密碼金鑰解密儲存於該第一裝置之該非暫態運算電腦記憶體上之經加密之資料。

【0012】 於一些實施例中，需要該等金鑰碎片之至少一部分(或全部)以重建該密碼金鑰。於一些實施例中，各裝置是彼此物理性地分離，且該等裝置包括該第一裝置。於一些實施例中，回應存取該加密資料之請求，該等金鑰碎片之至少一部分被自動收集。於一些實施例中，該等金鑰碎片是藉由將該密碼金鑰作為對一閾值加密資料分享方案(threshold

cryptography data-sharing scheme)之輸入而處理所產生的輸出。於一些實施例中，該密碼金鑰是一區塊加密器(block cipher)中使用的金鑰。於一些實施例中，該等金鑰碎片是共同建構該密碼金鑰之該密碼金鑰的個別部分。

【0013】 於一些實施例中，多個各種裝置可被用於簽署(sign)它們的碎片，使得其等個別的簽署可提供該等碎片是源自適當的裝置而來的證明。

【0014】 於一些實施例中，經加密之資料包括儲存於資料庫中之該資料庫的紀錄。於一些實施例中，經加密之資料包括儲存於一電子郵件檔案室(email archive)中之電子郵件。於一些實施例中，經加密之資料包括影像、文件、試算表、音訊檔或視訊檔的任一者。

【0015】 於一些實施例中，該方法進一步包括刪除該密碼金鑰並刪除該第一裝置處的任何金鑰碎片，使得該第一裝置沒有任何可用於解密經加密之資料的密碼金鑰。

【0016】 於一些實施例中，該等金鑰碎片為一第一組金鑰碎片(first set of key shards)，且該等裝置建構一第一裝置組合(first combination of devices)。該方法進一步包括自一第一最小閾值數(minimum threshold number) 之該第一組金鑰碎片產生一第二組金鑰碎片；將該第二組金鑰碎片分布至一第二裝置組合中；及自該第二組金鑰碎片產生一第三組金鑰碎片，使得該密碼金鑰得以基於該第二裝置組合的一第二最小閾值數之該第三組金鑰碎片而重建。

【0017】 於一些實施例中，一主要公共金鑰(master public key)可衍生自多個裝置公共金鑰，且一獨特資料辨識符(unique data identifier)可被用於自此主要公共金鑰衍生一公共金鑰。此機制，已知為基於閾值身分(threshold

identity)的加密可被用於加密各資料物件(data object)。於此實施例中，多個裝置可產生用於解密且衍生自該資料辨識符的組合私人金鑰(combined private key)。於此實施例中，增加網路效能是以犧牲一些安全保障為代價的。

【0018】 於一些實施例中，該第二裝置組合包括該第一裝置組合的至少一部分。於一些實施例中，該第一最小閾值數相等於該第二最小閾值數，且該密碼金鑰得以基於該第一最小閾值數之該第一組金鑰碎片而重建。於一些實施例中，該第二最小閾值數是與該第一最小閾值數不同。於一些實施例中，該第二組金鑰碎片之總數是與該第一組金鑰碎片之總數不同。

【0019】 於一些實施例中，該方法進一步包括自一第三最小閾值數之該第三組金鑰碎片產生一第四組金鑰碎片；將該第四組金鑰碎片分布至一第三裝置組合中；及自該第四組金鑰碎片產生一第五組金鑰碎片，使得該密碼金鑰得以基於該第三裝置組合的一第四最小閾值數之該第五組金鑰碎片重建，且此可被無限重複。

【0020】 於一些實施例中，儲存該等金鑰碎片之該等裝置建構儲存一第一組金鑰碎片之第一組裝置，且該方法進一步包括將該第一組裝置之種類及數量改變為儲存基於該第一組金鑰碎片產生之一第二組金鑰碎片的一第二組裝置，且該密碼金鑰可自該第二組金鑰碎片重建。

【0021】 被揭示之該等實施例亦包括具有一處理器及記憶體之運算裝置。該記憶體包括資料物件及指令，當該等資料物件和指令由該處理器執行時，致使該運算電腦裝置以一個別獨特密碼金鑰加密該等資料物件；針對各獨特密碼金鑰產生多個金鑰碎片；及將該等金鑰碎片分布於多個裝置之間，使得任何該等資料物件的解密需要自分布於該等裝置中的一閾值

數之該等金鑰碎片重建一獨特密碼金鑰。

【0022】 於一些實施例中，該運算裝置包括一檔案系統，其具有對應至該等資料物件的多個檔案，且包括用於加密該等資料物件的該等指令。於一些實施例中，該運算裝置包括一電子郵件歸檔系統，其包括對應至該等資料物件的多封電子郵件，且包括用於加密該等資料物件的該等指令。

【0023】 於一些實施例中，任何資料物件的加密、該等金鑰碎片的產生，以及任何金鑰碎片的分布是由該發端裝置(originating device)所控制。於一些實施例中，該等裝置的各者是由被授權以存取該加密資料物件的一使用者預先選擇。

【0024】 被揭示之實施例包括另一用於解密儲存於一非暫態運算電腦記憶體上之經加密之資料的方法。該方法包括自多個裝置獲得金鑰碎片，自該等金鑰碎片重建一密碼金鑰，並以經重建之密碼金鑰使得儲存於一運算裝置之一非暫態運算電腦記憶體上的加密資料得以被解密。於一些實施例中，經重建之該密碼金鑰只能在足以解密該加密資料的一期間內使用。於一些實施例中，該方法包括在該加密資料的解密被完成後自動刪除經重建之該密碼金鑰。

【0025】 此發明內容是被提供以簡化的形式介紹一系列的概念，其在以下實施方式中將被進一步敘述。此發明內容並非意欲指出所實施之標的之關鍵特徵或必要特徵，亦非意欲被用於限制所實施之標的之範圍。被揭示之實施例的其他態樣自所附的圖式及詳細說明將顯而易見。

【圖式簡單說明】

【0026】 本發明之一或多個實施例於隨附之圖式中是被顯示作為實例而非限制，其中類似元件編號表示相似的元件。

圖1是顯示用於實施根據本發明之一些實施例的用於靜止資料之免密碼加密之系統的方塊圖；

圖2是顯示根據本發明之一些實施例之用於靜止資料之免密碼保全之各種程序的流程圖；

圖3是根據本發明之一些實施例，基於一密碼金鑰產生金鑰碎片的例示程序的方塊圖，其中一閾值數之該金鑰碎片可被用於重建一密碼金鑰；

圖4是根據本發明之一些實施例的一歸檔檔案(archive file)的一方塊圖；

圖5是根據本發明之一些實施例的一例示金鑰碎片再分布(redistribution)程序的方塊圖；

圖6是根據本發明之一些實施例的能夠操作以保全靜止資料之一發端裝置(originating device)之組件的方塊圖；

圖7是根據本發明之一些實施例之一發端裝置之組件中的資料流的方塊圖；

圖8是顯示根據本發明之一些實施例的一保全第三方通道(secure third-party channel，STPC)裝置鏈接的流程圖；

圖9是顯示根據本發明之一些實施例的工作程序(onboarding procedures)的設置方法的方塊圖；及

圖10是得以被操作以實施所揭示之實施例的態樣的運算裝置之方塊圖。

【實施方式】

【0027】 下列實施例代表使所屬技術領域具有通常知識者得以實行該等實施例之必要資訊，且顯示實行該等實施例之最佳態樣。在參考隨附圖式閱讀下列敘述時，所屬技術領域具有通常知識者將理解揭露內容的概念且將認知到此處未特別指出之這些概念的應用。應理解的是，這些概念及應用落於本揭露內容及隨附之申請專利範圍的範圍內。

【0028】 此處所使用之用詞的目的僅是為了敘述實施例，且並非意欲限制該揭露內容的範圍。在上下文允許的情況下，使用單數形式或複數形式的字彙也可以分別包括複數形式或是單數形式。

【0029】 諸如「處理(processing)」、「運算(computing)」、「計算(calculating)」、「決定(determining)」、「顯示(displaying)」、「產生(generating)」等用語，除非另外特別指明，可表示將在該電腦之記憶體或是暫存器中以物理(電子)量(physical (electronic) quantities) 代表的資料操縱及轉換為在該電腦之記憶體、暫存器或其他此種儲存媒體、傳輸或顯示裝置內類似地以物理量代表的其他資料的一運算裝置之動作及程序。

【0030】 此處所使用的「連接(connected)」、「耦接(coupled)」或其等的變化態樣等用語可表示二或多個元件之間的任何連接或是耦接-無論是直接或是間接的。該等元件之間的耦接或連接可為物理地(physical)、邏輯地(logical)或是其等之組合。

【0031】 用語「通道(channel)」或「鏈接(link)」描繪資料或資訊的通訊手段-無論是有線或無線的，且可使用數位蜂巢式傳輸標準(digital cellular

transmission standards，例如，CDMA、W-CDMA、LTE、HSPA+)。實例包括藍芽、Wi-Fi、乙太網路、USB、USB-C、Thunderbolt、音訊鏈接或視訊鏈接(例如，QR碼及攝影機)。一訊息可在兩個裝置之間直接通訊或是通過一或多個通道/鏈接上的另一裝置間接通訊。

【0032】 此處使用之用語「目標資料(target data)」可表示欲作為加密標的之資料。目標資料的實例可包括相片、文件、試算表、音訊檔、視訊檔，或任何種類之可加密的資料檔。其他實例包括儲存於資料庫表單中的資料、密碼、儲存於電腦上的電子郵件，或任何資料物件。

【0033】 被揭示之實施例包括用於保全儲存於一運算裝置之記憶體上的資料的技術。於一些實施例中，一方法包括使用密碼金鑰而以一區塊加密器(block cipher)加密儲存於一電腦裝置之記憶體上的資料。基於任何該等加密資料，數個金鑰碎片可經由一閾值加密資料分享方案(threshold cryptography data-sharing scheme)而產生。於一些實施例中，一密碼金鑰之各金鑰碎片可以其自己的獨特公共金鑰加密。一經加密之碎片可被分布於實體上分開(physically distinct)之運算裝置之陣列之一者，該等運算裝置可各自具有用於其經加密之金鑰碎片的私人金鑰。該密碼金鑰可以一閾值數之運算裝置而重建，該閾值數之運算裝置使用它們的私人金鑰解密其等之對應金鑰碎片。具體而言，該閾值數之該經解密之金鑰碎片可被用於重建該密碼金鑰，其可接著被用於解密該加密資料。

【0034】 在傳統系統中，由於密碼及密碼金鑰管理的挑戰，儲存於運算裝置中之靜止資料的相當部分(significant portion)是未預設被加密。維持充足量的獨特金鑰及密碼以充分保全所有目標資料對於任何系統-從消費者

層級到事業層級-都是具有挑戰性的。家庭及事業使用者需要定期存取數百或甚至數千個別的資料物件，且無法記憶或充分記住對於保全目標資料將會需要的許多高亂度(high-entropy)密碼。因此，使用者排斥接受用於資料加密之額外的密碼，由於其已經被用於不同網站、服務及應用程式的密碼淹沒。

【0035】 保全大量靜止資料的解決方法包括使用單一主密碼作為金鑰以解密儲存於儲存在記憶體中之一容器(例如，一資料夾)中的無數資料物件。此種資料保全系統對於攻擊為脆弱的，假使其被破解，將暴露具有該單一主密碼的無數資料物件。例如，密碼管理工具諸如DASHLINE及LASTPASS使用一單一密碼，其若被破解，將提供攻擊者對所有以該單一密碼加密之資料的存取權。由於電腦駭侵(computer hacking)的增加以及由惡意行為者開發以利用現有金鑰及密碼管理工具的弱點之病毒、惡意軟體(malware)和勒索軟體(ransomware)的氾濫，此風險呈指數增長。

【0036】 保全靜止資料由於金鑰或密碼的遺失之風險而為複雜的。不幸地，使用者已經習慣於網站之密碼找回機制(password retrieval mechanism)，因此其等期望能夠重設保全他們的靜止資料之遺失的密碼。例如，當一使用者遺失用以存取一事業系統之資料的密碼，該使用者期望一網路管理員可輕易地傳送一重設鏈接或是編碼以促使該遺失之密碼的重設。然而，由於一個解密演算法在沒有對於該金鑰或密碼之存取權時是無法運行的，對於靜止資料之加密的密碼重設是不可能的。此問題的一個解決方案包括稱為「後門(back doors)」者，其已被利用以在一金鑰或密碼遺失時提供對於資料的緊急存取。然而，後門產生可由惡意行為者利用的弱

點。基於這些限制，大多數的個別使用者及事業並不將其等絕大多數的靜止資料加密。

【0037】 另一解決方案是全磁碟加密(full-disk encryption)，其已被利用以對實體上的遺失(physical loss)或硬體被竊提供保全。然而，全磁碟加密無法保護免受於病毒、惡意軟體、勒索軟體或是能夠取得系統控制權的駭客的入侵。在一事業體中，若靜止資料是被加密的，密碼金鑰之中央管理通常被使用以在密碼被誤放、遺失或遺忘時使資料得以被回復。然而，中央化(centralized)系統產生一個弱點-成為攻擊者的金鑰寶庫(treasure-trove of keys)。另外，全磁碟加密並不保護儲存於第三方平台上，諸如雲端儲存提供者之使用者資料(例如，電子郵件)。

【0038】 被揭示之實施例藉由以「免密碼(passwordless)」加密而得以具有保全大量靜止資料的能力而克服傳統系統之缺陷。因此，不像傳統系統，被揭示之實施例不必然需要一個使用者來採取輸入密碼以存取任何靜止資料之累贅步驟。事實上，各資料物件可以使用者不須要明確地儲存、記憶、管理以及保全之分離的獨特密碼金鑰加密，以在稍後解密任何經加密之資料物件。反而是，被揭示之實施例需要由一使用者進行有限且週期性的參與，以在以區塊加密器保全各資料物件時解密任何數量之資料物件。此處所使用的一個「密碼金鑰」或是「金鑰」可表示由一加密器(cipher)使用位元串(string of bits)以將明碼(plain text)轉換為加密文字，或是將加密文字轉換為明碼。該金鑰仍為私人的並確保直到解密事件為止的安全儲存及通訊。

【0039】 如下將詳細敘述的，數個金鑰碎片可基於用於加密一資料物

件之區塊加密器之密碼金鑰而被產生。於一些實施例中，該等金鑰碎片是通過一閾值加密資料分享方案而自該密碼金鑰衍生。該金鑰碎片可為，例如，共同形成密碼金鑰的該密碼金鑰之部分，使得金鑰碎片的組合(assembling)可以重建該密碼金鑰。雖然此處所敘述之實施例一般是有關靜止資料，或一般而言有關資料物件，所屬技術領域具有通常知識者將理解各實施例可包含對於資料庫條目(database entries)、智慧型手機檔案(例如，影像檔)、包含於收件匣中之電子郵件(例如，在MS交換伺服器上或是在Gmail收件匣中的電子郵件)等的實施。

【0040】 所揭示之實施例可包括硬體及/或軟體的組合。例如，一實施例包括一安全服務(security service)，其可在儲存於一電腦儲存媒體上的資料上操作。在另一個實例中，一實施例可包括與一操作系統或是檔案系統區隔的應用程式，以對儲存在該檔案系統中的資料進行分開操作。在再一實例中，一實施例是被整合至已存在之檔案系統中以提供一簡化介面給使用者，以輕易儲存及存取加密靜止資料。

【0041】 圖1是顯示用於實施根據本發明之一些實施例的用於靜止資料之免密碼加密之系統的方塊圖。如圖所示，該系統100包括諸如發端裝置102(originating device 102)、中繼伺服器104，以及委派裝置106n之陣列(array of delegate devices 106n)之組件。該發端裝置102可經由鏈接112a而與中繼伺服器104通訊，該中繼伺服器104可經由鏈接112n而與委派裝置106n通訊。於一些實施例中，該系統100之該等組件是作為該發端裝置102之安全服務的一部分而通訊。於一些實施例中，該發端裝置102以及該委派裝置106n可跳過(bypass)該中繼伺服器104以經由鏈接112b，諸如無線無線電鏈接(例

如，藍芽)或其他直接或間接的通訊手段而通訊。

【0042】 此處所使用的「發端裝置」，是一個靜止資料可自其被存取的運算裝置。該靜止資料可被儲存於該發端裝置102的一局部記憶體或是被儲存於另一運算裝置之遠端(remotely located)的記憶體。於一些實施例中，一發端裝置是其中新的內容被產生或是預先存在之內容被修改的裝置。於一些實施例中，一發端裝置可操作為運行特殊用途軟體的一般用途電腦或是一特殊用途硬體裝置。

【0043】 發端裝置之實例包括一電腦、智能終端或是啞終端(smart or dumb terminal)、一銷售點(point-of-sale，POS)裝置、網路電腦、機上盒(set-top box)、遊戲機(game player)、行動裝置、無線裝置、無線電話、個人數位助理、媒體(例如，音樂及/或視訊)播放器、攝影機、資訊家電、工作站、迷你電腦、主機電腦(mainframe computer)，或任何可儲存或存取靜止資料的其他裝置。發端裝置的特定實例包括桌上型電腦、膝上型電腦(例如、Apple MacBook, Lenovo 440)、智慧型手機(例如，Apple iPhone、Samsung Galaxy、Nokia Lumina)、平板電腦(例如，Apple iPad, Samsung Note, Amazon Fire, Microsoft Surface)，或其他可儲存或存取靜止資料的運算裝置。雖然系統100中顯示單一發端裝置102，所揭示之實施例可包括任何數量的發端裝置。

【0044】 該發端裝置102可存取儲存資料的一或多個記憶體。該等記憶體可包括用於儲存靜止資料之不變性記憶體(non-volatile memory)。例如，該發端裝置102可包括或存取儲存一檔案系統或是一電子郵件檔案室之記憶體。該等記憶體可包括儲存靜止資料之揮發性記憶體。於一些實施例中，該等記憶體包括一局部儲存裝置及/或基於雲端之儲存裝置，其可分開

地或共同地儲存資料物件。該等儲存裝置可為可移除或不可移除之電腦可讀取儲存媒體，諸如磁性硬碟驅動機、固態硬碟驅動機、網路附接儲存器、快閃記憶體裝置、光學驅動機、遠端雲端儲存器等。可使用於例示性操作環境之其他種類之儲存媒體包括但不限於，卡式磁帶(magnetic tape cassettes)、快閃記憶卡(flash memory cards)、DVDs、數位視訊磁帶、固態隨機存取記憶體(random-access memory，RAM)、固態唯讀記憶體(read-only memory，ROM)等。該儲存器媒體通常經由一可移除或不可移除記憶體介面而連接至一系統匯流排。

【0045】 於一些實施例中，一特殊用途軟體應用程式可被安裝於該發端裝置102上以執行所揭示之操作的元件，並用以促進與該系統100之其他組件的通訊，包括該中繼伺服器104及委派裝置106n。於一些實施例中，該發端裝置102亦可當作一委派裝置。該發端裝置102以及該委派裝置106之間的區別在於其等在以一或多個密碼金鑰加密或解密靜止資料之方法中的功能。特別是，該發端裝置102可存取儲存於局部或遠端記憶體中的經加密之靜止資料，而該委派裝置106n可提供用以衍生出用於加密或解密由該發端裝置102儲存之靜止資料的該密碼金鑰的個別金鑰碎片。如此一來，該委派裝置106n可保全經加密之靜止資料並藉由將金鑰碎片之訊息傳送給該發端裝置102而授權經加密之靜止資料的解密。

【0046】 此處所使用的「委派裝置」可表示一運算裝置，私人金鑰可被儲存於其上，且密碼金鑰之金鑰碎片可被儲存於其上。此處所使用的一「金鑰碎片」可表示一閾值數之資料項目中的一資料項目，一密碼金鑰可自該閾值數之資料項目被重建(例如，被衍生)。該委派裝置106n可包括諸如

此處針對發端裝置102所敘述者之運算裝置之任何組合。

【0047】 該委派裝置106n可包括任何經由軟體或硬體而已組態(configured)的裝置，用以與該發端裝置102安全地通訊(例如，通過該中繼伺服器104)或在該等委派裝置106n之間安全地通訊。於一些實施例中，該等委派裝置106n為可攜式運算裝置(例如，智慧型手機、平板裝置、筆記型電腦裝置)，但可進一步包括任何使用者可存取且得以與該發端裝置102通訊或在該等委派裝置106n之間通訊的裝置。實例包括桌上型電腦、智能終端或是啞終端、POS裝置、網路電腦、機上盒、遊戲機、行動裝置、無線裝置、無線電話、個人數位助理、媒體播放器(例如，音樂及/或視訊)、攝影機、資訊家電、工作站、迷你電腦、主機電腦，或任何具有類似運算功能的其他裝置。

【0048】 該中繼伺服器104可安全地在發端裝置102及該等委派裝置106n之間傳送訊息及通知。例如，該中繼伺服器104可代表可以在該發端裝置102及該委派裝置106n之間經由鏈接112a-n而中繼金鑰碎片的任何數量之伺服器電腦。該使用者介面可被使用以藉由在該等委派裝置106n之間分布及收集金鑰碎片而促進經加密之靜止資料的管理。於一些實施例中，該中繼伺服器104可收集並儲存由該發端裝置102及/或該等委派裝置106所提供的加密資料，並將該資料提供給任何其他裝置。該中繼伺服器104可包括對於所屬技術領域具有通常知識者已知之硬體及軟體的組合，如此一來，為了簡明的目的，此處省略相關敘述。

【0049】 該等鏈接112a-n可包括私人、公開、有線或無線部分的任何組合。任何經由該等鏈接112a-n通訊的資料可在各種位置或在該等鏈接

112a-n之不同部分處被加密或解密。該系統100的各組件可包括硬體及/或軟體的組合以處理資料、執行功能、經由該等鏈接112a-n通訊等。例如，該系統100之任何組件可包括一處理器、記憶體或儲存器、一網路收發器、一顯示器、操作系統及應用程式軟體(例如，用以提供一使用者介面)等。為了簡潔起見，包括於該系統100中對於所屬技術領域中具有通常知識者為熟知的其他組件、硬體，及/或軟體並未在此顯示或討論。

【0050】 經由一無線無線電鏈接112b(例如，藍芽、Wi-Fi)通訊的能力允許該發端裝置102跳過該中繼伺服器104，以藉由直接自委派裝置擷取金鑰碎片以加密及解密靜止資料。由該發端裝置102對該等委派裝置106n之直接存取在任何鏈接112a或112n為失效(down)或無法存取(inaccessible)時為有用的。通訊鏈接，特別是在該等委派裝置106n及該發端裝置102之間所建立者，可能需要對該等委派裝置或是呈現於一行動裝置上的資訊，諸如一快速回應(QR)碼進行修改(modifications)。於一些實施例中，所有的通訊，無論是何種中介(intermediary)，都是以目的地裝置之公共金鑰加密資料而被保全。

【0051】 因此，該系統100可使用由多個運算裝置所實施之對稱加密、不對稱加密及閾值加密之組合而實施靜止資料的免密碼加密。例如，進階加密標準(advanced encryption standard，AES)或另一加密器可由發端裝置102使用。於一些實施例中，該等金鑰碎片是一密碼金鑰之碎片，其等是一可結構化閾值祕密分享方案(configurable threshold secret-sharing scheme)，諸如沙米爾的祕密分享方案(Shamir's secret sharing scheme)、巴克利方案(Blakley's scheme)、基於中國剩餘定理的祕密分享方案。於一些實施

例中，該分享方案是可被操作以代表具有N個碎片之密碼金鑰，其中只有M個是被需要用以重建該原本的BC密碼金鑰。因此，該等委派裝置106n可提供被需要以重建一密碼金鑰之閾值數的金鑰碎片。所以，發端裝置102可藉由存取該閾值數的金鑰碎片解密資料而不是需要將該密碼金鑰以其整體輸入。

【0052】 圖2顯示所揭示之用以保全靜止資料之免密碼技術。所揭示之技術包括使用對稱加密、不對稱加密及可結構化閾值加密法之組合以管理靜止資料之加密及/或解密。該等程序200可由發端裝置102及委派裝置106a-b作為一安全服務之部分而進行。該發端裝置102或委派裝置106a-b可包括各種不同的裝置，諸如參考圖1而討論者。

【0053】 該發端裝置102及/或委派裝置106a-b可屬於被授權以藉由該發端裝置存取及解密資料物件的使用者。在一些情況中，委派裝置106a-b之至少一部分可以屬於未被授權以存取經加密之資料的使用者。儲存該加密資料之該記憶體可為發端裝置102及/或遠端記憶體的局部記憶體，且該加密資料是儲存於該局部或遠端記憶體中。

【0054】 在步驟202中，該發端裝置102之使用者可指派一組運算裝置作為委派裝置106a或授權該等委派裝置106a之使用者。於一些實施例中，各委派裝置106a是自彼此實體上分離及/或可包括該發端裝置102。

【0055】 於步驟204中，該發端裝置102以一密碼金鑰加密目標資料。該密碼金鑰可被特別生成以加密該目標資料。例如，該密碼金鑰可為一對稱金鑰之位元串，以使用於得以將明碼轉換為加密文字(及自加密文字轉換為明碼)的一區塊加密器中。於一些實施例中，該密碼金鑰是被暫時產生以

加密靜止資料，且隨後被刪除。

【0056】 該目標資料可包括各種種類之資料物件(例如，影像、文件、試算表、音訊檔、視訊檔)，其等各自以個別的密碼金鑰加密。實例包括具有各種檔案及指示之用於加密該等檔案的檔案系統、具有電子郵件及指示之用於加密該等電子郵件的電子郵件歸檔系統、具有紀錄及指示之用於加密該等訊息的資料庫系統等。經加密之目標資料被儲存於可由該發端裝置102存取之非暫態電腦記憶體。

【0057】 於步驟206中，該發端裝置102基於該密碼金鑰產生N個金鑰碎片。該等金鑰碎片可自N個金鑰中的一必要且充分的閾值數M而衍生(重建)。例如，該組N個金鑰碎片可經由一閾值加密資料分享方案產生。當該使用者希望解密經加密之目標資料，N個金鑰碎片中的M個被處理以重建該密碼金鑰。該組金鑰碎片可被局部的(locally)儲存及/或分布於委派裝置160a-b之間。如此處所使用的，一密碼金鑰之「金鑰碎片」亦可表示組件、片段或是表示一組金鑰碎片之一部分或元件的其他用語。

【0058】 為了助於理解資料分享方案，假設一個W階多項式可由該多項式的W+1個點重建。例如，假設二階多項式aX^2+bX+c，其中該密碼金鑰是由該常數項c所表示。該多項式可以該多項式的任何三個點重建。分享方案之實例包括沙米爾的祕密分享方案、巴克利方案、基於中國剩餘定理的祕密分享方案，或任何其他由所屬技術領域中具有通常知識者所理解的分享方案。於一個簡單的實例中，一密碼金鑰諸如可被用於加密目標資料之密碼「secret」，被拆解成碎片「sec」和「ret」，且稍後被重組以解密經加密之目標資料。

【0059】 例如，圖3為用於產生一組金鑰碎片之方法的實例的方塊圖，其是基於一密碼金鑰，該密碼金鑰之一閾值數的該等金鑰碎片可被用於重建一密碼金鑰。如圖所示，裝置A是一發端裝置且裝置B到F為委派裝置。一組金鑰碎片可被分布於該等運算裝置A、B、C、D、E及/或F的組合中。被顯示的實例是一個五之三(three-of-five)組態，其中僅需要三個金鑰碎片以重建該密碼金鑰，且剩下的裝置是多餘的(superfluous)。因此，失去對於運算裝置B到F中任何五之二的存取權不會使得該發端裝置102無法重建該密碼金鑰，因為來自剩餘的運算裝置之該等金鑰碎片已足以重建該密碼金鑰。然而，須注意的是，該密碼金鑰無法自少於該閾值數的金鑰碎片的子集重建(例如，兩個金鑰碎片)。經過重建之密碼金鑰可接著被用於解密或加密資料。

【0060】 所揭示的實施例包括針對各委派裝置106a所產生的一不對稱金鑰對(asymmetric key pair)。該金鑰對包括一委派公共金鑰以及一委派私人金鑰。這兩個金鑰可使用一金鑰產生技術，諸如RSA或橢圓曲線金鑰對(elliptic curve key pairs) 一起產生。該委派不對稱金鑰對(delegate asymmetric key pair)可在一委派裝置被產生。該委派私人金鑰可專被留置(kept exclusively)在該委派裝置且從不與另一運算裝置分享或是輸出至另一運算裝置。相對而言，該委派公共金鑰係與另一委派裝置或該發端裝置分享或是輸出供另一運算裝置或該發端裝置使用。於一些實施例中，該等金鑰碎片可以該等委派公共金鑰加密以產生加密之金鑰碎片，該等金鑰碎片可與其等之委派裝置安全地通訊。用於加密之機制及金鑰強度的選擇為可設定的且可包括，例如，RSA、ECIES、ElGamal及其他具有類似功能的加密方

案。

【0061】 各委派裝置可產生包括委派私人金鑰及委派公共金鑰的委派金鑰對。各委派裝置可保有其個別的委派私人金鑰。例如，委派裝置D1可保有私人金鑰K-1，委派裝置D2可保有私人金鑰K-2，依此類推。N個委派裝置的各者亦可將其委派公共金鑰分布至任何其他的委派裝置及各發端裝置，使得所有的委派裝置及發端裝置具有所有的委派公共金鑰以及發端裝置公共金鑰。

【0062】 一個備用金鑰對(backup key pair)亦可被以分布至各種發端裝置的備用公共金鑰產生。對於是否產生一備用公共金鑰的決定可依據使用者或管理者偏好而定。因此，所揭示之實施例可採用其他改良保全的金鑰對。例如，一個實施例可採用一備用不對稱金鑰對，其包括一備用公共金鑰及一備用私人金鑰。這些備用金鑰對可在離線時藉由使用一金鑰產生技術，諸如RSA或橢圓曲線金鑰產生技術而由一運算裝置產生。該備用私人金鑰可被留置於離線電腦，而備用公共金鑰可被輸出以由其他運算裝置使用。

【0063】 在步驟208中，該等N個金鑰碎片的各者是以與一個別委派裝置相關聯的N個公共金鑰的一個加密，以產生N個經加密之金鑰碎片。另外，任何與該原始資料相關聯的元數據是被認證的，例如經由MAC或藉由將該元數據包括於該碎片中。該發端裝置102可具有對於該等委派裝置106a之所有公共金鑰的存取權，使得該發端裝置102可使用公共金鑰以加密用於個別委派裝置106a的金鑰碎片。該等委派裝置106a持有個別的對應私人金鑰，該等對應私人金鑰可在需要時被用於解密其等個別的金鑰碎片。

【0064】 在一些實施例中，該密碼金鑰是選擇性地使用一備用公共金鑰加密以生成可以使用備用私人金鑰解密的經加密之密碼金鑰。該等備用金鑰通常是在一離線環境下被生成並儲存。例如，一檔案系統(FS)可藉由使用該密碼金鑰而將目標資料加密。該FS可將經加密之金鑰碎片與經加密之目標資料儲存於磁碟上的歸檔檔案(archive file)中。此外，若一個備用公共金鑰被生成，其可被用於加密該密碼金鑰，該密碼金鑰接著可被加入該歸檔檔案中。

【0065】 此處所使用之「歸檔檔案」是一個客製化檔案格式，其中已被以，例如，使用一密碼金鑰之BC加密的目標資料可被與該密碼金鑰(或相關金鑰) 之加密版本、密碼金鑰碎片 ，或經加密金鑰之次金鑰碎片(sub-key shards)的任何組合一同儲存。例如，圖4是顯示根據本發明之一些實施例的一歸檔檔案400的方塊圖。該歸檔檔案400具有包括一碎片片段402以及備用片段404的一檔案結構。

【0066】 如圖所示，該歸檔檔案400可包括已被以備用公共金鑰或另一非對稱加密技術所加密之整個密碼金鑰。因此，歸檔檔案之解密可能需要額外的加密資訊以產生該密碼金鑰之解密版本。在一些情形中，額外的經加密金鑰碎片組被加入該歸檔檔案中。該等額外的經加密金鑰碎片組可被用於開啟檔案。隨著經加密之金鑰碎片被添加至歸檔檔案，加密程序即完成。於一些實施例中，至少一些經加密之金鑰碎片是可擇地被送至該等委派裝置106a以進一步改良安全性。可擇地將N個經加密金鑰碎片分布至該等委派裝置106a降低解密資料及再分布碎片所需的網路流量。加密目標資料可以儲存於該等委派裝置106a的金鑰碎片回復(recoverable)。

【0067】 例如，在圖2之步驟210中，N個經加密金鑰碎片是被分布於第一組的委派裝置106a中，使得發端裝置102由於缺少密碼金鑰及可重建該密碼金鑰的金鑰碎片而無法解密經加密之目標資料。例如，該發端裝置可與中繼伺服器通訊以將該等碎片分布於委派裝置106a中。

【0068】 於一些實施例中，將N個經加密金鑰碎片分布涉及在發端裝置102及委派裝置106a之間建立一無線鏈接(例如，Wi-Fi、藍芽、蜂巢式網路)、一有線鏈接(例如，乙太網路、USB)、視覺鏈接或音訊鏈接。例如，N個金鑰碎片之至少一者可經由電腦網路與遠離發端裝置102設置之該組委派裝置106的至少一者通訊。在另一實例中，N個金鑰碎片的至少一者是經由一短距無線電鏈而與遠離發端裝置102設置之該組委派裝置106的至少一者通訊。委派裝置106a可暫時或是間歇式耦接至發端裝置102以與金鑰碎片通訊。

【0069】 於一些實施例中，一局部安全服務可自一歸檔檔案抽取一組經加密之金鑰碎片。該發端裝置102可將該組經加密之金鑰碎片轉給(pass)一通訊服務，其將經加密之碎片分布至各自的委派裝置。在該等委派裝置106a之間的通訊可為直接的(例如，經由藍芽或乙太網路連接而在相同的LAN上進行)，或是經由中繼伺服器或是洋蔥路由方案(onion routing scheme)進行。

金鑰碎片再分布程序(Key Shard Redistribution Process)

【0070】 所揭示之實施例包括一金鑰碎片再分布程序以替換或添加委派裝置至一已存在的一組委派裝置中。若一已存在之委派裝置遺失(lost)、被竊取(stolen)、被摧毀、作廢，或是以其他方式成為無法存取的，

其可根據再分布程序而由另一委派裝置取代。於一些實施例中，重建一密碼金鑰所需的金鑰碎片的閾值數可與用於該再分布程序所需的金鑰碎片之閾值數相同或不同。再者，該再分布方法可被用於改變用以重建一密碼金鑰所需之裝置的閾值數。

【0071】 在步驟214中，該可擇地再分布程序被進行以基於該第一組金鑰碎片(first set of key shards)之組合產生一第二組金鑰碎片(second set of key shards)。該第二組金鑰碎片是從一第一閾值數之該第一組金鑰碎片所產生，且可包括該第一組金鑰碎片的其中一部分，或是不包括該第一組金鑰碎片。該第二組金鑰碎片的數量可與該第一組金鑰碎片的數量相同或不同。該密碼金鑰得以從該第一組金鑰碎片或是該第二組金鑰碎片重建。再者，該第二組金鑰碎片甚至可在不重建該密碼金鑰的情形下被產生。

【0072】 於一些實施例中，該再分布程序涉及自該第一組金鑰碎片產生中間次金鑰碎片(intermediary sub-key shards)，且接著自該等次金鑰碎片產生該第二組金鑰碎片。該等次金鑰碎片被分布於第二裝置組合(second combination of devices)中，第二裝置組合可基於該等次金鑰碎片產生該第二組金鑰碎片。如此一來，持有該第一組金鑰碎片的該第一組委派裝置的種類及數量可改變為持有該第二組金鑰碎片的一第二組委派裝置。因此，該第二委派裝置組合可包括該第一委派裝置組合的一部分，或是不包括該第一委派裝置組合。

【0073】 圖5為根據本發明之一些實施例，顯示用於自已存在之閾值數的金鑰碎片產生新金鑰碎片的例示性程序的方塊圖，如此一來一密碼金鑰可自一新的閾值數之該新的金鑰碎片重建。於經顯示的實例中，需要一

五之三(three-of-five)組態以進行該再分布程序以及重建該密碼金鑰。亦即，只需要三個金鑰碎片以取代任何數量的該第一組委派裝置且只需要三個新的金鑰碎片以重建該密碼金鑰。

【0074】 該再分布程序僅需解密一閾值數的經加密之金鑰碎片。未加密之金鑰碎片的閾值數可自該歸檔檔案或是自其等所位於的個別委派裝置上取得。該閾值數的未加密之金鑰碎片被輸入至一再分布程序，其產生新的一組未加密之金鑰碎片，其可以該第二組委派裝置(包括任何新的委派裝置)的私人金鑰加密，產生相較於金鑰碎片的原始數量更多的經加密之金鑰碎片。新的經加密之金鑰碎片可被添加至該發端裝置之歸檔檔案，且可被分布至額外的委派裝置。

【0075】 如圖所示，該發端裝置A基於一密碼金鑰產生五個金鑰碎片，並將五個金鑰碎片分布至第一組委派裝置B至F。該裝置B是一主要委派裝置(例如，使用者的智慧型手機)，且委派裝置C至F為備用委派裝置(例如，各別是平板電腦)。假設裝置B及/或C被遺失或以其他方式成為無法存取的。使用者可操作該發端裝置A(或是剩下的委派裝置)上的GUI(圖形使用者介面)以觸發一再分布程序於新的委派裝置B'至F'。

【0076】 一組次金鑰碎片被產生，此作為生成新的一組金鑰碎片給該第二組委派裝置B'至F'的程序中的中間步驟。此處所使用之「次金鑰碎片」可表示基於其他金鑰碎片所產生的金鑰碎片，且其已根據延長分享方案之再分布程序而生成，用以自一閾值數之金鑰碎片之預先存在之子集產生新的一組金鑰碎片。在新的一組金鑰碎片中，只有另一個閾值數是可被需要以重建該原本的密碼金鑰。因此，金鑰碎片的新的閾值以及新的數量不須

各自與金鑰碎片的原本閾值及原本數量相同。

【0077】 如圖所示，該發端裝置A是與委派裝置D、E及F配合使用以產生用於委派裝置B’至F’之次金鑰碎片。該委派裝置D將產生次金鑰碎片D-1至D-5，該委派裝置E將產生次金鑰碎片E-1至E-5，且該委派裝置F將產生次金鑰碎片F-1至F-5。次金鑰碎片D-1、E-1及F-1是用於新的委派裝置B’。次金鑰碎片D-2、E-2及F-2是用於新的委派裝置C’。次金鑰碎片D-3、E-3及F-3是用於新的委派裝置D’。次金鑰碎片D-4、E-4及F-4是用於新的委派裝置E’，而次金鑰碎片D-5、E-5及F-5是用於新的委派裝置F’。該等新的金鑰碎片是衍生自在各別的新委派裝置B’至F的次金鑰碎片。

【0078】 因此，新的一組委派裝置B’至F’取代舊的一組委派裝置B至F。新的金鑰碎片可以委派裝置B’至F’之各別的公共金鑰加密。新的經加密之金鑰碎片可被添加至該發端裝置A的歸檔檔案，且可被分布至其他剩餘的委派裝置。除了遺失的碎片，剩下的經加密之金鑰碎片可在歸檔檔案或是其所位於的個別委派裝置上取得。不需要在該再分布程序期間重建該密碼金鑰，在該再分布期間任何裝置處也不需要五個中的三個經解密之碎片。反而是，該密碼金鑰只需要被重建以解密或加密目標資料。再者，需要最小閾值數之委派裝置及個別的金鑰碎片以重建該密碼金鑰。在此情形中，需要五個中的三個新金鑰碎片用以重建該密碼金鑰。

【0079】 將重建該密碼金鑰之需求僅限制於解密或加密目標資料的能力改良了目標資料的安全性。例如，由於可能產生漏洞，需要針對無數資料物件重建密碼金鑰以產生新的多組金鑰碎片是不被希望的。特別是，一惡意行為者知悉將進行一再分布程序，因為該竊取委派裝置之惡意行為

者可在該過程中窺探而獲取用於資料物件之密碼金鑰。因此，藉由避免除了加密或解密資料物件之外之重建任何密碼金鑰的必要性，該等實施例減輕此漏洞的風險。

【0080】 雖然圖5顯示以該第二組委派裝置替代整個第一組委派裝置的程序，該再分布程序可被利用以取代任何數量的委派裝置，只要該閾值數之原本委派裝置對於金鑰碎片的再分布是可用的。再者，該再分布程序可被用於添加無限數量的不同委派裝置之組合。例如，考量一個情形中該第一組委派裝置只包括D、E及F。在進行再分布程序後，第二組委派裝置可包括B'、C'、D、E及F。

【0081】 因此，所揭示之實施例包括用於將其他運算裝置併入儲存金鑰碎片的一組裝置中的技術。此包括添加或取代經選擇之運算裝置以產生儲存該組金鑰碎片的運算裝置之新的組合，該組金鑰碎片對於自該閾值數之金鑰碎片重建一密碼金鑰為必須的，且接著將該密碼金鑰再次拆解(re-sharding)以產生用於運算裝置之新的組合的一組新的金鑰碎片。

解密程序(Decryption Process)

【0082】 在步驟216中，該解密程序可在該發端裝置102之使用者試圖打開一個檔案、自一資料庫讀取資料，或以其他方式存取加密資料物件時被調用(invoked)。例如，一檔案開啟程序可能由一個檔案系統(file system，FS)處置器或操作系統處置器打斷，該處置器辨認包含加密資料物件的檔案。在一些實施例中，該發端裝置102自該委派裝置106a及/或106b收集至少閾值數的解密之金鑰碎片。例如，該發端裝置102可致使委派裝置106a-b將其等個別的金鑰碎片與發端裝置102通訊。

【0083】 於一些實施例中，委派裝置106a-b可與持有個別委派裝置之使用者確認是否允許該解密事件。對於允許的請求可以各種形式表示，諸如以文字或SMS訊息、跳出通知(popup notification)、LED顯示器，或其他內建於操作系統中或由系統軟體及可行的硬體提供的形式。該使用者可接受對於解密事件的請求。於一些實施例中，在一預定期間過期後，一請求被自動拒絕。

【0084】 在一個N之M(M-of-N)組態中，只有總共N個金鑰碎片中之閾值M個被需要以重建一密碼金鑰。在N個對應的委派裝置中，一或多個為主要(即，授權)裝置而剩餘的為次級裝置(secondary devices)。例如，在有一膝上型電腦、一智慧型手機以及一平板的三之二(2-of-3)組態中，該膝上型電腦可以是該發端裝置，該智慧型手機可以是該主要委派裝置，而該平板可為一個委派次級裝置。在此實例中，密碼金鑰的重組(reassembly)僅需兩個裝置之參與：該發端裝置以及該智慧型手機。次級裝置的參與是不必要的，除非該主要委派裝置無法使用(unavailable)。

【0085】 在一些實施例中，取決於名稱、種類、路徑或其他目標資料元數據，持有一委派裝置的一使用者可以針對解密請求設定數個自動肯定回應(automatic affirmative responses)之閾值。例如，該閾值可被設置以自動解密接下來被接收的10個碎片或是自動解密在接下來12小時期間接收的所有碎片。若解密被允許，該委派裝置可解密其各別的加密金鑰碎片，並通過一中繼伺服器或其他通訊通道而將解密金鑰碎片返還至發端裝置102，或可以被再次加密以傳送至發端裝置102。由發端裝置接收之金鑰碎片可被用於重建該密碼金鑰，其是被傳送至該FS或操作系統。該目標資料可接著被

解密及開啟。

【0086】 於步驟218，該發端裝置102自從該發端裝置102及/或該等委派裝置106a-b收集之金鑰碎片重建一密碼金鑰。於一些實施例中，需要至少一些或是全部的金鑰碎片以重建該密碼金鑰。具體而言，該密碼金鑰是從該發端裝置102及/或該等委派裝置106a-b收集之一閾值數的該等金鑰碎片重建。接著，在步驟220中，該發端裝置以該重建之密碼金鑰解密儲存於一非暫態電腦記憶體上的該加密之目標資料。

【0087】 於一些實施例中，任何經重建之密碼金鑰僅在一段足以解密該經加密之資料的期間內得以使用(enabled)。例如，在步驟222中，任何經重建的密碼金鑰在該經加密之目標資料被解密完成後被自動刪除。於一些實施例中，一密碼金鑰及任何金鑰碎片的複本是成為無法操作(inoperable)或自該發端裝置102刪除，使得用於解密該加密資料的任何密碼金鑰除非在目標資料的解密或加密期間，其是無法使用(unavailable)或是無法衍生的(underivable)。

【0088】 所揭示之實施例亦包括用於修改經加密之資料的程序。已根據此處所敘述之加密程序所加密的資料可根據此處所述的解密程序而解密。經解密的資料可接著被修改，並再次根據此處所敘述的加密程序而加密。

【0089】 所揭示之實施例亦包括一金鑰輪替程序(key rotation process)。例如，一使用者或系統可能希望輪替或改變用於加密目標資料之密碼金鑰。金鑰輪替可藉由使用此處所敘述之解密程序中的一第一密碼金鑰來解密該目標資料，並接著使用此處所敘述的加密程序而再次加密該目

標資料，但此次使用與該第一密碼金鑰不同的一第二密碼金鑰。

【0090】 該發端裝置可在一操作系統的控制下操作，該操作系統提供一檔案系統，其控制資料如何被儲存及擷取。於一些實施例中，該操作裝置可被設定以運行將應用程式從檔案系統實行(file system implementation)隔離之虛擬檔案系統(virtual file system，VFS)、一個介面層或抽象化層，且可提供一常用介面給多種種類之檔案系統。若一VFS被使用，該VFS可以回應用於檔案操作之應用等級的呼叫(application-level calls)，該檔案操作包括對儲存於該裝置上的檔案進行開啟、讀取、寫入及附加(appending)。該VFS亦可回應處理可應用於各檔案操作的加密事件。若該發端裝置未運行一VFS，該發端裝置之操作系統可直接回應對於檔案操作以及處理可應用於各檔案操作之加密事件的應用等級呼叫。

【0091】 例如，圖6為顯示得以被操作以進行該程序200之至少一部分的發端裝置的組件的方塊圖。例如，該發端裝置可包括一圖形化使用者介面(graphical user interface，GUI)模組602，其促進與一使用者的互動。該發端裝置亦可包括一安全服務604(security service 604)、一檔案系統606及各種經由API呼叫608及610為可存取或是得以使用的功能。諸如添加或移除委派裝置、系統組態、控制警示及其他特徵之任務可由一使用者通過該GUI模組602管理。

【0092】 在一些實施例中，該發端裝置之安全服務604是在一發端裝置運行的程式，雖然其可在其他處，諸如在一專用伺服器上運行。例如，該安全服務可自一檔案系統(例如，虛擬檔案系統(VFS)、內建於電腦之操作系統中的檔案系統、一客製化檔案系統或其他者)接收請求以重建被用於解

密一歸檔檔案之內容的密碼金鑰。於一些實施例中，該安全服務是安裝於該發端裝置上的特殊用途軟體應用的一部份，用以使所揭示之加密操作得以進行，並促進與中繼伺服器及/或委派裝置通訊。

【0093】 圖7是顯示根據本發明之一些實施例，在一發端裝置之組件之間的資料流之方塊圖。該安全服務702可經由中繼網路、金鑰儲存及金鑰管理而控制通訊。該安全服務702是通訊地耦接至檔案系統704(例如，VFS)及該GUI模組706。作為一實例，該安全服務702可使訊息及通知經過一中繼網路而通訊以產生、升級並分享憑證(credentials)。

【0094】 在一些實施例中，一加密程序起始於一使用者或程式意圖開啟位於檔案系統704中的檔案。該檔案系統704可顯示為使用者的起始目錄內的資料夾。自該使用者的觀點，該檔案系統164可像是該發端裝置上的其他資料夾一樣的方式操作。在後端，該檔案系統704資料夾內的該等檔案是以加密方式儲存於歸檔檔案內的資料。該使用者不需要知悉該等歸檔檔案及其等實際位置，其可能是在雲端儲存器中、在檔案伺服器上，或位於局部裝置上並使該資料鏡像(mirrored)存於一雲端伺服器(例如，DROPBOX、GOOGLE DRIVE)。

【0095】 該檔案系統704(作為虛擬檔案系統)可管理與該發端裝置之儲存裝置之該檔案系統之間的互動。一應用程式介面(application programming interface (API))可被提供以允許該發端裝置中的該等模組之間的通訊。例如，該檔案系統704可與安全服務702通訊，該檔案系統704需要金鑰以解密歸檔檔案中之資料。該安全服務702接著聯絡各種委派裝置、擷取相關金鑰碎片、重建該密碼金鑰，並將經重建之密碼金鑰傳送至該檔案

系統704。該檔案系統704可接著解密該歸檔檔案中的資料。於一些實施例中，該檔案系統704通常會將該歸檔檔案內發現的相關加密金鑰碎片傳給該安全服務702。該安全服務702可接著將該些經加密之金鑰碎片傳送至一中繼伺服器以最終由相關的委派裝置接收。該等相關的委派裝置可使用其等個別之私人金鑰，解密該等經加密之金鑰碎片，並將未加密之金鑰碎片返還至安全服務702，其可重建該密碼金鑰並將其返還至檔案系統704。該檔案系統704可使用經重建之密碼金鑰以解密歸檔檔案中儲存的資料，且接著將經解密之資料呈現給相關程式。

【0096】 於一些實施例中，該歸檔檔案可能不包含某些關聯的加密金鑰碎片。缺少(missing)的金鑰碎片可以僅被儲存於委派裝置。在這些情形下，安全服務702可指示委派裝置藉由使用針對該歸檔檔案的參考號碼(reference number)產生相關的金鑰碎片。

【0097】 該安全服務702亦可負責產生用於檔案系統704的新的密碼金鑰(例如，在產生一個新檔案時)、使用一分享方案以產生金鑰碎片，以及以各別的委派裝置之公共金鑰加密這些金鑰碎片。經加密之金鑰碎片可被傳送至委派裝置，且亦被傳送回該檔案系統704以儲存於歸檔檔案內。

【0098】 該安全服務702亦可與該GUI模組706互動以處理數種操作，包括委派裝置之遺失或移除、委派裝置之取代或添加，及改變M或N個金鑰碎片之數量。這些操作可能需要根據此處所敘述之金鑰碎片再分布程序而再分布金鑰碎片。

【0099】 該安全服務702可與GUI模組706互動以進行用於授權或備份用途的該使用者之委派裝置的改變。例如，一種實施方式可具有一個四

之二(2-of-4)組態，表示需要儲存個別分布之金鑰碎片的四個運算裝置中的至少兩個以組裝使得目標資料之解密得以進行的密碼金鑰。該使用者之運算裝置可包括一膝上型電腦作為一發端裝置、一智慧型手機作為主要委派裝置、一平板作為一備用委派裝置，及一朋友的智慧型手機作為另一備用委派裝置。所有的四個裝置儲存需要用於解密之個別的經加密之金鑰碎片以及該關聯的私人金鑰。在正常情形下，該使用者將只在該使用者的主要委派裝置上收到解密請求，而該發端裝置將預設地(by default)提供經解密之金鑰碎片。若該使用者之主要委派裝置(例如，智慧型手機)的電池電量不足(discharged)，該使用者可能希望將該主要委派裝置的責任暫時轉換至該備用委派裝置(例如，平板)。轉換至該備用委派裝置將不需要一再分布操作，但可能需要經由該中繼伺服器通訊。

設置程序(Setup Process)

【0100】 所揭示之實施例包括用於安全地將裝置連接以交換諸如金鑰碎片之資料的程序。例如，圖8是顯示根據本發明之一些實施例的一安全第三方通道(secure third-party channel，STPC)裝置連接程序800。更具體而言，程序800採用用於交換公共金鑰的保全通訊通道。

【0101】 在步驟802中，一客戶裝置(一第一裝置)可藉由選擇一通道而請求一保全通道種類(例如，QR、電子郵件、SMS)，且接著將其裝置ID諸如，例如一個隨機16位元單次使用的金鑰以及其公共金鑰的散列(hash)傳送至該授權裝置(一第二裝置)。於步驟804中，該授權裝置請求該客戶裝置的公共金鑰。於步驟806中，該客戶裝置開始傳送該公共金鑰至該授權裝置。最後，在步驟808中，該授權裝置傳送具有一憑證裝置ID的回覆訊息、

單次使用之金鑰(one-time key (OTK))及公共金鑰以完成在該等裝置之間建立安全鏈接所需要之該保全交換。

【0102】 圖9是顯示根據本發明之一些實施例的用於工作程序(onboarding procedures)的設置程序的方塊圖。階段1顯示一發端裝置可經由使用圖6的STPC機制而與委派裝置進行安全的公共金鑰的交換。在此之後所有的通訊可被加密並簽署。階段2顯示在與該等委派裝置連接後，該發端裝置可將整個工作資訊(on-boarding information)傳送至委派裝置，其會在階段3中將它們彼此連接。階段3中所顯示的完成步驟使得所有的裝置彼此之間以安全的方式交換它們的公共金鑰。包括該發端裝置及委派裝置之群組接著已準備好安全地與金鑰碎片通訊。

【0103】 圖10是得以被操作以實施所揭示之實施例的態樣之運算裝置1000的方塊圖。該運算裝置1000可為一通用電腦或特別設計以執行該系統100之特徵者。該運算裝置1000可為一發端裝置、一中繼伺服器，或作為如晶片上系統(system-on-chip，SOC)、一單板電腦(single-board computer，SBC)系統、一伺服器、一桌上型或膝上型電腦、一資訊站(kiosk)、一主機(mainframe)、一網狀電腦系統、一手持行動裝置，或其等之組合而實施的一委派裝置。

【0104】 該運算裝置1000可為一獨立裝置或跨越多個網路、位置、機器或其等之組合之一分布系統之部分。於一些實施例中，該運算裝置1000作為一客戶-伺服器網路環境中的一伺服器電腦(例如，中繼伺服器)或是客戶裝置(例如，發端裝置、委派裝置)而運作，或是做為一點對點系統(peer-to-peer system)中的同級機器(peer machine)而運作。於一些實施例中，

該運算裝置1000可即時或是近即時、離線、藉由批次處理或其等組合而進行所揭示之實施例的一或多個步驟。

【0105】 如圖所示，該運算裝置1000包括可操作以在硬體組件之間傳送資料的匯流排1002。這些組件包括一控制器1004(即，處理系統)、一網路介面1006、一輸入輸出(Input/Output，I/O)系統1008，及一定時系統1010(clock system 1010)。該運算裝置1000可包括其他為了簡潔之目的而未顯示或是未詳加討論的組件。所屬技術領域中具有通常知識者將了解任何被包括但未顯示於圖10中之硬體及軟體。

【0106】 該控制器1004包括一或多個處理器1012(例如，中央處理單元(central processing units (CPU)、應用特定積體電路(application specific integrated circuits，ASICs)，及/或現場可程式閘陣列(field programmable gate arrays，FPGAs))及記憶體1014(其可包括軟體1016)。該記憶體1014可包括，例如，揮發性記憶體，諸如隨機存取記憶體(RAM)，及/或不變性記憶體，諸如唯讀記憶體(ROM)。該記憶體1014可為局部、遠端或分布式。

【0107】 一軟體程式(例如，軟體1016)，當稱為 「於一電腦可讀儲存媒體中實施(implemented in a computer-readable storage medium)」，其包括儲存於一記憶體(例如，記憶體1014)中之電腦可讀指示。當至少一個與該軟體程式相關聯之值是儲存於可由一處理器所讀取之一暫存器中，該處理器(例如，處理器1012)是「被設定以執行一軟體程式」。於一些實施例中，被實施以執行所揭示之實施例的常規(routines)可做為操作系統(operating system，OS)軟體(例如，Microsoft Windows、Linux) 的一部分或被稱為「電腦程式」之一特定軟體應用程式、組件、程式、物件、模組或指示之順序

而被實施。

【0108】 如此一來，該電腦程式通常包含在一電腦(例如，運算裝置1000)之各種記憶體裝置中，在各種時間下設定的一或多個指示，且當由至少一個處理器(例如，處理器1012)讀取及執行時，致使該電腦進行操作以執行涉及所揭示之實施例之各種態樣的特徵。於一些實施例中，包含前述電腦程式產品的載體(carrier)被提供。該載體是電子訊號、光學訊號、無線電訊號，或一非暫態電腦可讀取儲存媒體(例如，記憶體1014)之一者。

【0109】 該網路介面1006可包括一數據機(modem)或其他介面(未顯示)，用於例如通過網路1024而將該運算裝置1000耦接至其他電腦。該輸入輸出系統1008可操作以控制各種I/O裝置，包括周邊設備諸如顯示器系統1018(例如，一螢幕或觸控式顯示器)以及一或多個輸入裝置1020(例如，一鍵盤及/或指向裝置)。其他輸入輸出裝置1022可包括，例如，磁碟驅動機、印表機、掃描機或類似者。最後，該定時系統1010控制一計時器供所揭示之實施例使用。

【0110】 一記憶體裝置(例如，記憶體1014)之操作，諸如自二進制一(binary one)改變為二進制零(或相反的改變)之狀態可包含一視覺可感知的物理性變換。該變換可包含一物件變為不同的狀態或物體(thing)之一物理性變換。例如，狀態的改變可涉及儲存之電荷的充入(charge)或釋放之累計(accumulation)及儲存。同樣地，狀態的改變可包含磁性取向(magnetic orientation)之物理性改變或變換或分子結構的物理性改變或變換，諸如從晶體轉變為非晶體，或是相反的轉變。

【0111】 所揭示之實施例的態樣可以儲存於記憶體上的資料位元上

之操作的演算法或是符號表達而敘述。這些演算敘述及符號性的表達通常包括導致所欲結果的一系列操作。該等操作需要物理量的物理操縱(physical manipulations)。通常，雖然不是必要的，這些量是以得以被儲存、轉換、結合、比較及以其他方式操縱之電性或磁性訊號的形式存在。習慣上，且為了方便起見，這些訊號被稱為位元、值、元素、符號、字符、用語、數字或類似者。這些用語及相似的用語是與物理量相關聯且僅是被應用於這些量的方便性標識。

【0112】 雖然實施例是以完整發揮功能之電腦為前提進行敘述，所屬技術領域具有通常知識者將理解各種實施例是得以作為各種形式之程式產物而被分布，且揭露內容可同等地應用無論是使用何種特別種類之機器或電腦可讀取媒體以實際讓該等實施例產生效果。

【0113】 雖然本揭露內容已以數種實施例進行敘述，所屬技術領域具有通常知識者將認知到本發明並未受限於此處所敘述之實施例且可以本發明之精神及範圍內之改良及替代方案實行。所屬技術領域具有通常知識者亦認知到對於本發明之實施例的改良。所有這些改良都被認定為在此處所揭示之申請專利範圍的範圍內。因此，該敘述被認為是例示性的而不是限制性的。

【符號說明】

系統	100	委派裝置	106n
發端裝置	102	鏈接	112a、112b、112n
中繼伺服器	104	程序	200、800

步驟	202、204、206、208、210、214、216、218、220、222、802、804、806、808
歸檔檔案	400
碎片片段	402
備用片段	404
GUI模組	602
安全服務	604、702
檔案系統	606、704
API呼叫	608、610
GUI模組	706
運算裝置	1000
匯流排	1002
控制器	1004
網路介面	1006
輸入輸出系統	1008
定時系統	1010
處理器	1012
記憶體	1014
軟體	1016
顯示器系統	1018
輸入裝置	1020
其他輸入輸出裝置	1022

201939341

發明摘要

【發明名稱】（中文/英文）

用於靜止資料之免密碼保全系統／PASSWORDLESS SECURITY SYSTEM FOR DATA-AT-REST

【中文】

本發明所揭露之實施例包括用於保全靜止資料的免密碼方法。該方法包括以密碼金鑰加密及/或解密資料。例如，經加密之資料可被儲存於第一裝置之非暫態運算電腦記憶體上。該方法可包括基於密碼金鑰產生金鑰碎片，密碼金鑰可自金鑰碎片重建，並將金鑰碎片分布於裝置中，使得由於第一裝置因缺乏密碼金鑰而無法解密經加密之資料，而將經加密之資料保全於第一裝置。

【英文】

The disclosed embodiments include a passwordless method for securing data-at-rest. The method includes encrypting and/or decrypting data with a cryptographic key. For example, the encrypted data can be stored on a non-transitory computer memory of a first device. The method can include generating key shards based on the cryptographic key, which can be reconstituted from the key shards, and distributing the key shards among devices such that the encrypted data is secured at the first device because the first device is incapable of decrypting the encrypted data due to an absence of the cryptographic key.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

系統	100
發端裝置	102
中繼伺服器	104
委派裝置	106n
鏈接	112a、112b、112n

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

申請專利範圍

1. 一種用於保全靜止資料之免密碼方法，其包含：

以一密碼金鑰(cryptographic key)加密資料，經加密之資料被儲存於一第一裝置之一非暫態運算電腦記憶體上；

基於該密碼金鑰而產生多個金鑰碎片(key shards)，使得該密碼金鑰可自該等金鑰碎片重建；及

將該等金鑰碎片分布於多個裝置中，使得由於該第一裝置因缺乏該密碼金鑰而無法解密該經加密之資料，而令該經加密之資料被保全於該第一裝置。

2. 如請求項1所述之方法，其中需要該等金鑰碎片的至少一部分以重建該密碼金鑰。

3. 如請求項1所述之方法，其中該等裝置之各者是彼此物理性地分離，且該等裝置包括該第一裝置。

4. 如請求項1所述之方法，其中將該等金鑰碎片分布包含：

在該第一裝置及該等裝置之間建立一通訊鏈以與個別的金鑰碎片通訊；及

經由該通訊鏈使一金鑰碎片與該等裝置之至少一者通訊，該通訊鏈包括一運算電腦網路、一短程無線電鏈或一蜂巢式鏈的至少一者。

5. 如請求項1所述之方法，其中該第一裝置屬於被授權以存取該經加密之資料的一單一使用者，且該等裝置之至少一者屬於未被授權以存取該經加密之資料的一使用者。

6. 如請求項1所述之方法，其中該第一裝置及該等裝置包含一伺服器、

一個人運算電腦，及一智慧型手機各者。

7. 如請求項1所述之方法，其中該密碼金鑰是一第一密碼金鑰且該非暫態運算電腦記憶體儲存多個資料檔，該等資料檔各自以一個別密碼金鑰加密且包括以該第一密碼金鑰加密的一第一資料檔。

8. 如請求項1所述之方法，其中該第一裝置具有用於該等裝置之各者的一公共金鑰，該等裝置各自具有一對應私人金鑰，且將該等金鑰碎片分布至該等裝置包含：

以一個別公共金鑰加密各裝置之各金鑰碎片，使得多個經加密之金鑰碎片被分布至該等裝置，且各裝置可在被請求時解密其經加密之金鑰碎片，並將經解密之金鑰碎片返還給一請求者。

9. 如請求項1所述之方法，其進一步包含：

回應存取該經加密之資料的一請求，自該等裝置自動收集閾值(threshold) 的該等金鑰碎片；

自經收集之該等金鑰碎片重建該密碼金鑰；及

以經重建之該密碼金鑰解密儲存於該第一裝置之該非暫態電腦記憶體上的該經加密之資料。

10. 如請求項1所述之方法，其中該等金鑰碎片是藉由將該密碼金鑰作為對一閾值加密資料分享方案之輸入而處理所產生的輸出。

11. 如請求項1所述之方法，其中將該等金鑰碎片分布包含：

以一獨特公共金鑰加密一金鑰碎片，使得經加密之該金鑰碎片被分布至具有一對應私人金鑰之該等裝置的至少一者，該對應私人金鑰使經加密之該金鑰碎片的解密得以進行。

12.如請求項1所述之方法，其中該等金鑰碎片是共同建構該密碼金鑰之該密碼金鑰的個別部分。

13.如請求項1所述之方法，其中該非暫態運算電腦記憶體是一智慧型手機或一平板電腦之局部記憶體，且經加密之該資料包含儲存於該局部記憶體上的檔案。

14.如請求項1所述之方法，其中該等金鑰碎片是一第一組金鑰碎片，且該等裝置是一第一裝置組合，該方法進一步包含：

自一第一最小閾值數(first minimum threshold number)之該第一組金鑰碎片產生一第二組金鑰碎片；

將該第二組金鑰碎片分布至一第二裝置組合中；及

自該第二組金鑰碎片產生一第三組金鑰碎片，使得該密碼金鑰得以基於該第二裝置組合的一第二最小閾值數之該第三組金鑰碎片而重建。

15.如請求項14所述之方法，其中該第二裝置組合包括至少一部分之該第一裝置組合。

16.如請求項14所述之方法，其中該第一最小閾值數相等於該第二最小閾值數且該密碼金鑰得以基於該第一最小閾值數之該第一組金鑰碎片而重建。

17.如請求項14所述之方法，其中該第二最小閾值數是與該第一最小閾值數不同。

18.如請求項14所述之方法，其中該第二組金鑰碎片之總數是與該第一組金鑰碎片之總數不同。

19.如請求項14所述之方法，其進一步包含：

自一第三最小閾值數之該第三組金鑰碎片產生一第四組金鑰碎片；

將該第四組金鑰碎片分布至一第三裝置組合中；及

自該第四組金鑰碎片產生一第五組金鑰碎片，使得該密碼金鑰得以基於該第三裝置組合的一第四最小閾值數之該第五組金鑰碎片而重建。

20.一種運算裝置，其包含：

一處理器；及

一或多個記憶體，其包括資料物件(data objects)和指令，當該等資料物件和指令由該處理器執行時，致使該運算電腦裝置：

以一個別獨特密碼金鑰加密該等資料物件的各者；

針對各獨特密碼金鑰產生多個金鑰碎片；及

將該等金鑰碎片分布於多個裝置之間，使得任何該等資料物件的解密需要自分布於該等裝置中的一閾值數之該等金鑰碎片重建一獨特密碼金鑰。

21.如請求項20所述之運算裝置，其進一步包含：

一檔案系統，其包括對應至該等資料物件的多個檔案，且包括用於加密該等資料物件的該等指令。

22.如請求項20所述之運算裝置，其進一步包含：

一電子郵件歸檔系統，其包括對應至該等資料物件的多封電子郵件，且包括用於加密該等資料物件的該等指令。

23.一種用於解密儲存於一非暫態運算電腦記憶體上的加密資料的方

法，該方法包含：

自多個裝置獲得多個金鑰碎片；

自該等金鑰碎片重建一密碼金鑰；以及

使得以以經重建之該密碼金鑰進行儲存於一運算裝置之一非暫態運算電腦記憶體上的經加密之資料的解密。

24.如請求項23之方法，其進一步包含：

在該經加密之資料的解密被完成後自動刪除經重建之該密碼金鑰，使得經重建之該密碼金鑰只能在足以解密該經加密之資料的一期間內使用。