200822066

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：096116559

※ 申請日期：96 年 5 月 9 日　　※IPC 分類：G11B 29/00 (2006.01)
G06F 21/00 (2006.01)
G11B 19/12 (2006.01)

一、發明名稱：（中文/英文）

資料寫入媒體裝置/Apparatus for Writing Data to A Medium

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

德商諾爾羅股份有限公司/Nero AG

代表人：（中文/英文）

里夏德・雷瑟爾/Richard LESSER

住居所或營業所地址：（中文/英文）

德國卡爾斯巴德 76307 史考特梅德 13-15 號/Im Stoeckmaedle 13-15, 76307 Karlsbad, Germany.

國　籍：（中文/英文）德國/DE

三、發明人：（共 3 人）

1. 姓　名：（中文/英文）里夏德・雷瑟爾/Richard LESSER
   國　籍：（中文/英文）德國/DE
2. 姓　名：（中文/英文）安德里亞斯・埃克雷德爾/Andreas ECKLEDER
   國　籍：（中文/英文）德國/DE
3. 姓　名：（中文/英文）萊內爾・科夫/Reiner KOPF
   國　籍：（中文/英文）德國/DE

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 US；2006/05/10；60/746,964
2. 美國 US；2006/05/16；60/747,363
3. 歐洲 EU；2007/04/13；07007647.6

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

本發明係在資料安全及資料保護的領域，特別是在攜帶式媒體。

盜拷防護及資料安全為一種得到數位數據及媒體成功的更重要意義的課題，在現今時代當個人電腦普及率包含私人家庭，盜拷防護及資料安全更為一種課題，每一年顯著經濟損失因為盜取資料而發生。而且，為使任何數位媒體使用者可保密及保護私人內容，其包含盜拷防護與完整性及加密機構。

例如，在習知電腦系統拷貝數位內容為相當簡單的，然而存在至少阻礙產品盜版的一些盜拷防護機構，然而，若無法達到，對盜版者要為相當複雜地寫入經盜拷防護的資料。已知一些機構以加密私人資料，例如 PGP(PGP=加密寶貝)，使用這些機構，可使用私人加密密鑰加密資料，使用公開加密密鑰可辨識資料為已使用私人加密密鑰加密的資料。加密可以相反方式作用，以公開加密密鑰加密數位內容而允許私人加密密鑰得持有人解密該數位內容。然而，這些機構的確具它們為複雜的及仍缺乏適當盜拷防護之問題。

所以本發明目的在於提供一種資料寫入媒體裝置，其為較不複雜的及其使私人內容的盜拷防護可行。

此目的係藉由根據申請專利範圍第 1 項的寫入裝置，根據申請專利範圍第 13 項的寫入資料之方法，根據申請專利範圍第 15 項的提供加密資料裝置及根據申請專利範圍

第 27 項的提供加密資料之方法而達到。此目的係藉由根據申請專利範圍第 29 項的系統及根據申請專利範圍第 30 項的光碟機進一步達到。

此目的係藉由寫入資料至媒體的裝置達到，該裝置包含自資料提供器接收寫入要求及經加密資料的裝置，該裝置進一步包含在接收寫入要求時產生媒體 ID(ID=身份)的裝置及提供媒體 ID 至資料提供者以產生加密資料的裝置，該裝置進一步包含在產生媒體 ID 時儲存該經加密資料於該媒體及儲存該媒體 ID 於該媒體的裝置，其中該經加密資料係基於該媒體 ID 加密。

此目的係藉由提供該經加密資料至資料寫入器的裝置進一步達到，該裝置包含將寫入要求傳送至資料寫入器的裝置及當將寫入要求傳送至資料寫入器自該資料寫入器接收該媒體 ID 的裝置。所提供裝置進一步包含使用加密密鑰加密純文本數據以得到該經加密資料的裝置，該加密密鑰係基於該媒體 ID 及用於傳送的媒體係進一步採用以傳送該經加密資料至資料寫入器。

具體實施例係基於盜拷防護可藉由加密儲存於儲存媒體的數位內容而可達到的發現，其中該加密係基於具多重加密組成的加密密鑰，加密組成的其中一個可為 ID，其在一個具體實施例可為獨一的，及其亦寫至儲存媒體。寫至儲存媒體的媒體 ID 僅可在接收寫入要求時由具體實施例產生，一旦媒體 ID 產生，其被提供至資料提供器，在一個具體實施例其可由在例如一個 PC(PC=個人電腦)上操作的

應用軟體實施，該應用軟體接著基於媒體 ID 及進一步基於，例如，密碼、撤銷金鑰、等加密該資料。該經加密資料接著由資料寫入器寫至儲存媒體。無論何時資料被讀取時，媒體 ID 會自儲存媒體讀出及提供至讀取器應用軟體，其重新組合加密密鑰與所涉及加密組成，及解密該資料。然而，資料寫入器並未寫入媒體 ID，此媒體 ID 並未由其本身產生，而是由來自外界的任何應用軟體所提供。而且在另一具體實施例，應用軟體及寫入器可在，例如，磁光機實施。

具體實施例可提供完整的解決方法組其允許內容的加密以促進盜拷防護及內容存取控制，與經由冗餘的增加資料可靠性，儘管內容存取控制係由使用經使用者提供的密碼加密儲存於例如光碟的資料而完成，盜拷防護允許使用者防止其他人產生此種媒體的拷貝，冗餘地儲存資料及數位地簽名該資料的可能性之結合以證實授權性，所有這些可能性以使用如光碟媒體安全地分享資料所需要的裝置提供企業及私人終端使用者，使用者可接著藉由使用密碼保護資料的方式控制具有該資料存取權的人，及使用者亦可確保沒有任何未經授權的資料拷貝被製作。

在另一具體實施例上述機構與密碼結合，在一個具體實施例該密碼可與該媒體 ID 結合及結果亦寫至該儲存媒體，使用者接著具在稍後時間點控制盜拷防護的可能性，此係假設密碼為已知。一些具體實施例提供傳統儲存媒體及傳統讀取器或寫入器不受影響之優點，若資料未被盜拷

防護，傳統讀取器仍可讀取資料，使用傳統寫入器寫入的資料仍可由具體實施例讀取。

隨後的一些具體實施例提供對未經授權拷貝的防護，不僅以著作權保護的觀點，亦相關於保密文件的分發及儲存。具體實施例藉由盜拷防護使得使用者有效地減少保密資料洩漏至大眾或是進入未經授權第三方的手中之風險。

具體實施例使得使用在市場上可提供的軟或硬體加密須被保護的內容及儲存密鑰於一部分無法被拷貝的媒體為可行，拷貝經保護文件的存取可經由專屬瀏覽器或閱讀器應用軟體(例如提供用於自受保護磁片的未加密部分之裝設)的具體實施例提供。

第 1a 圖顯示用於寫入資料至媒體的裝置 100 之具體實施例。該裝置 100 包含接收來自資料提供器的寫入要求及經加密資料的裝置 110，而且，該裝置 100 包含裝置 120 以在接收寫入要求時產生媒體 ID，該裝置 100 進一步包含提供該媒體 ID 至該資料提供者以產生加密資料的裝置 130 及在產生該媒體 ID 時儲存該經加密資料於該媒體及儲存該媒體 ID 於該媒體的裝置 140，其中該經加密資料係基於該媒體 ID 加密。

在一些具體實施例該裝置 140 可適用以儲存該經加密資料於媒體上的資料區段及儲存該媒體 ID 於媒體上的 ID 區段，其中該資料區段係與 ID 區段隔開或分開。第 1b 圖顯示媒體 150 的具體實施例，其係示例為一種磁片，例如光碟，如 CD(CD=光碟)、DVD(DVD=數位影音光碟)、或

是藍光盤等。說明於第 1b 圖的媒體 150 顯示資料區段 155 及 ID 區段 160，在一個具體實施例，該 ID 區段係在媒體的一處，此處僅一個具體實施例具存取途徑，換言之，在一些具體實施例，該 ID 區段可在傳統寫入器所無法存取的實體位置，說明於第 1b 圖的媒體為一個具體實施例，但是 ID 區段 160 及資料區段 155 的許多其他實現為可料到的，其在磁片或其他媒體為分開的例如 USB-記憶體-裝置(USB=通用串列匯流排)、記憶卡等。

在其他具體實施例該儲存裝置 140 可適用於僅儲存媒體 ID 於 ID 區段 160，接著藉由產生媒體 ID 的裝置 120 以產生媒體 ID，產生媒體 ID 的裝置 120 可適用於利用隨機或虛擬隨機數目產生該 ID。在另一具體實施例用於儲存的該裝置 140 可適用於儲存該媒體 ID 及密碼的組合於該媒體。

第 2 圖顯示用於寫入的裝置 100 之另一具體實施例。在說明於第 2 圖的具體實施例，產生媒體 ID 的裝置 120 係包含隨機數目產生器(RNG=隨機數目產生器)165，在另一具體實施例其亦可為虛擬隨機數目產生器。說明於第 2 圖的具體實施例進一步包含接收讀取要求的裝置 170，自該媒體讀取媒體 ID 及經加密資料的裝置 175 及，而且，提供該媒體 ID 及經加密資料的裝置 180。在另一具體實施例用於接收的該裝置 110 及用於接收的該裝置 170 可一起實施。以類似方式，用於提供的該裝置 130 及用於提供的該裝置 180 可一起實施。而且，用於寫入的裝置 100 可於晶

片或 ROM(ROM=唯讀記憶體)實施，其亦可包含於光碟。

在裝置 110 的另一具體實施例，可包含用於認證的裝置以使用資料提供器或資料讀取器認證。而且，用於接收的該裝置 110 可適用於自資料提供器接收經加密寫入要求及以解密該寫入要求。結果，用於接收讀取要求的裝置 170 可適用於接收經加密讀取要求及以解密該經加密讀取要求。結果，用於提供的該裝置 130 及 180 可適用於加密該媒體 ID 及用於提供該經加密媒體 ID 至資料提供器或資料讀取器。

第 3a 圖顯示用於提供經加密資料至資料寫入器的裝置 200 之具體實施例，該裝置 200 包含用於傳送寫入要求至該資料寫入器的裝置 210 及在傳送該寫入要求時自該資料寫入器接收媒體 ID 的裝置 220。而且，該裝置 200 包含使用加密密鑰加密純文本數據的裝置 230 以得到該經加密資料，該加密密鑰係基於該媒體 ID 及其中用於傳送的裝置 210 係適用於傳送該經加密資料至該資料寫入器。

在一個具體實施例用於加密的裝置 230 係進一步適用以使用加密密鑰，其係進一步基於密碼，例如，該加密密鑰可自在媒體 ID 及密碼及可能其他密鑰成分之間的 XOR 操作產生。在另一具體實施例用於加密的裝置 230 係適用以使用加密密鑰，其係進一步基於撤銷金鑰。在一個具體實施例該加密密鑰可為媒體 ID、密碼及撤銷金鑰三者之間的 XOR 操作。

第 3b 圖說明用於提供經加密資料至資料寫入器的裝

置 200 之另一個具體實施例，第 3b 圖說明與第 3a 圖類似的組件，然而，其進一步包含用於傳送讀取要求至該資料寫入器的裝置 235，接收經加密資料及媒體 ID 的裝置 240 及用於基於解密密鑰解密資料以得到純文本數據的裝置 245。在一個具體實施例用於解密的裝置 245 係適用於使用基於媒體 ID、密碼或撤銷金鑰的解密密鑰。在一個具體實施例該解密密鑰係基於在媒體 ID、密碼或撤銷金鑰三者之間的 XOR 操作。

在一個具體實施例用於傳送的裝置 210 及用於傳送的裝置 235 可一起實施。以類似方式，用於接收的裝置 220 及用於接收的裝置 240 可一起實施。在另一具體實施例用於加密的裝置 230 係進一步適用於加密於資料中的經加密密碼的資訊。在另一具體實施例該裝置 200 進一步包含用於偵測來自該經加密資料或純文本資料的盜拷防護顯示的裝置 250，用於傳送的裝置 210 可適用於不傳送寫入要求，當偵測到盜拷防護顯示時。以類似方式，用於接收媒體 ID 的裝置 220 可適用於不接收媒體 ID 當偵測到盜拷防護顯示時及用於加密的裝置 230 可適用於不加密資料，當偵測到盜拷防護顯示時。在另一具體實施例該盜拷防護顯示係對應於在該經加密或純文本資料內的控制資訊，該經加密或純文本資料具純文本控制資訊。

在另一具體實施例，類似於已於上文所說明的具體實施例，用於提供經加密資料的裝置 200 可進一步包含用於使用資料寫入器認證的裝置，用於傳送的裝置 210 及 235

可適用於傳送經加密讀取或寫入要求及，據此，用於接收的裝置 220 及 240 可適用於接收經加密媒體 ID。

在另一具體實施例系統可包含根據以上具體實施例的用於寫入資料的裝置 100 及用於提供經加密資料的裝置 200，而且，該系統可包含於光碟，及該媒體可對應於光學儲存媒體例如 CD、DVD 或是藍光盤。

這些具體實施例藉由確定例如碟片的各部分無法使用可提供軟體/錄音指令拷貝而使盜拷防護為可行。為完成此目的，這些具體實施例產生每一個磁片的媒體 IDs 當其第一次用於具體實施例時。在該媒體 ID 為分別獨一的具體實施例相同媒體 IDs 重複或被產生的機會為非常稀少的。在下文該媒體 ID 亦稱為獨特 ID，其顯示這些 IDs 重複機會非常稀少，在一個具體實施例該獨特 ID 可為要由具體實施例的韌體或隨機數目產生器，或是虛擬隨機產生器所產生的 128-位元隨機數目，當該盜拷防護特徵第一次施用於特定碟片時。雖然該獨特 ID 不為明確獨特的，因為存在重複的可能性當取用該例如 128-位元數目時，在下文它們可稱之為獨特。

接著將獨特 ID 寫至在該磁片的位置，於此位置無法被拷貝若不改良該寫入器，例如改良韌體，此種位置可包含在 DVDs 的引入，該獨特 ID 可由該韌體讀出及用於計算內容存取鍵及，一旦該內容存取鍵已被辨識，其可由主機應用系統經由專屬多媒體讀取指令而要求，其接著轉移至由總線密鑰(其已使用驅動主機認證於先前建立)所保護的主

機應用系統，在自一個媒體至另一個媒體的拷貝方法期間該獨特 ID 會遺失。沒有相對應的獨特 ID，該內容無法被解密，所以，藉由使用該獨特 ID 做為存取鍵成分而受保護免於拷貝的此種媒體的備份會成為無用的，因為該備份不會具該相同獨特 ID。如已於上文所敘述，在一些具體實施例，此機構可與密碼保護合併。

在下文中，敘述一種詳細具體實施例，其係稱為 SecurDisc。盜拷防護及存取控制係由加密寫至該媒體的該資料而使之可進行，使得僅當該加密密鑰為已知時該驅動或驅動器傳送該正確資料，該加密密鑰係得自使用者密碼短語、DUID(DUID=磁片獨特 ID)、或是二者，及與僅為經授權應用系統已知的分享秘密合併。此分享秘密在被折衷的應用系統，對應於撤銷金鑰，之情況為廢除的。建構該撤銷金鑰的來源係稱為密鑰成分 x。

該 DUID 可得自資料寫入器，其在下文稱做驅動器，或是光學驅動器。該 DUIO 並不儲存於該磁片的使用者資料區域，而是儲存於對每一個光碟形式個別選擇的特殊位置，使得其必須韌體更改才能拷貝，在上文所敘述具體實施例中此區段亦稱為 ID 區段。SecurDisc 並不需要任何專屬形式的光學儲存媒體。

第 4 圖說明密碼系統的具體實施例及提供用於 SecurDisc 的密碼系統之總覽，然而，並非示於第 4 圖的所有組件皆與使盜拷防護及存取控制為可行的具體實施例相關。第 4 圖顯示組件 410，其係用於創作媒體 420 的內容。

而且，第 4 圖顯示組件 430，其係用於讀取媒體 420 的內容。

密碼功能性係包含於磁光機及主機，且資料自媒體 420 讀取及寫至媒體 420。第 4 圖顯示說明保護媒體 420 對抗拷貝未經授權路徑及數位地簽名資料所需的密碼功能性的圖。

該創作組件 410 的其中一個為使用者提供的密碼 440，其係供應至產生第一密鑰成份的 AES 雜湊 442 功能 (AES=進階加密標準)，其係提供至 XOR 操作區塊 444。該 XOR 操作區塊 444 係進一步提供為具磁片獨特 ID 446 及授權授與密鑰 448，其訂定一種得自撤銷區塊的密鑰。自 XOR 操作區塊 444 所得結果，加密密鑰係提供至該 AES 加密區塊 450，該 AES 加密區塊 450 進一步接收邏輯扇區號 452 及密碼短語認證檢查和(PVC=短語認證檢查和)454，其為一種許可值，用於認證使用者施用的密碼短語之有效性，該 AES 加密區塊 450 的輸出接著提供至該 AESCBC 加密區塊 456(CBC=密碼塊鏈接)，其為區塊密碼的特殊操作模式，該 AESCBC 加密區塊 456 係進一步提供為具扇區內容 458，故經加密邏輯扇 460 可寫至該媒體 420。

另一個 AES 加密區塊 462 係基於該 PVC454 及該 AES 雜湊 442 衍生 EPVC(EPVC=經加密 PVC)464，基於公開密鑰 446 另一個 AES 雜湊 468 提供一種 RSA 公開密鑰雜湊 470(RSA=發明者，Rivest、Shamir 及 Adleman 的性氏之首字母)。使用私密金鑰 472，RSA 簽名區塊 474，其亦基於

該 AESCBC 加密區塊 456 輸出，衍生數位 RSA 簽名 476，其亦可儲存於該媒體 420。

在讀取側，可發現類似組件 430，由使用者提供的密碼 480 及 AES 雜湊 482 可提供密鑰成份至 XOR 操作區塊 484。該 XOR 操作區塊 484 進一步接收來自媒體 420 的授權授與 486 及磁片獨特 ID 446，以提供加密密鑰至 AES 加密區塊 488。基於邏輯扇區號 490，該 AES 加密區塊 488 可提供解密密鑰至 AESCBC 解密區塊 492，其可接著解密該經加密邏輯扇 460 及提供扇內容 494。基於 AES 雜湊區塊 482 及該經加密 PVC 464 的輸出，AES 解密區塊 496 提供一種經解密 PVC 以在區號 498 進行比較，其比較該值與該 PVC 500，及使得該使用者密碼短語的認證為可行。

基於公開密鑰 502 另一個 AES 雜湊區塊 504，另一個比較可在比較區塊 506 使用來自該媒體 420 的 RSA 雜湊密鑰 470 進行比較。基於公開密鑰 502 及該 AES 解密區塊 496 的輸出及 RSA 認證區塊 508 可辨識來自該媒體 420 的數位 RSA 簽名 476。

該授權授與密鑰 448 及 486，訂定一種得自撤銷區塊的密鑰，在上文所述具體實施例亦稱為撤銷密鑰，撤銷區塊訂定一種可被追蹤以得到撤銷區塊節點密鑰的二元樹。在一些具體實施例至該追蹤功能的登錄可為 32-位元值，追蹤此值的位元之功能係自最顯著的位元開始，如同其追蹤該二元樹。於根節點開始，若目前位元設定為例如零位元則其會向左分支，及若目前位元設定為例如一位元則其會

向右分支，除非其遇到不具左子樹或右子樹的節點，其係依據根據目前位元需要那一個。若此種節點進行 NK(NK=關鍵節點)，此密鑰隨著在該 32-位元值內的目前位元位置送回，若該節點不進行NK，該功能吸收一種錯誤，其顯示伴隨該32-位元值的成分已被撤銷。

一旦得到撤銷區塊NK，其可用於產生最後密鑰值，當與單一登錄或一種登錄或是由 32-密鑰所組成的陣列 KC[] 組合時，該登錄係由當追蹤該二元樹時最後處理的位元位置 x 所決定，該最後密鑰值 K 可使用下列式子產生：

K=KESencrypt (KC[x], NK)。

該二元樹係儲存為一種位元流，當自路由節點開始，例如以母樹、左子樹及右子樹的順序開始時，其被重複，此表示當處理一種節點時，第一寫出該目前節點，接著，若左子樹節點存在，重複方法遞歸回地以左子樹節點持續，最後，該重複方法遞歸回地處理該子樹節點。例如，對每一個節點其寫出說明於第 5 圖的結構。第 5 圖顯示一種表格表示法，其中 8 個位元或是一個位元組以表中的列說明及列的數目係對應於在結構內位元組的數目。該結構自右上角開始詳述，其係對應於該結構的第一位元及於第5圖係標示"左"。在一個具體實施例，例如若此位元設定為一，此節點具左手側子樹節點，下一個位元係標示"右"及例如若此位元設定為一，此節點具右手側子樹節點，以"密鑰"標示的位元顯示節點密鑰緊接在此位元之後，以"選擇性節點密鑰"標示的區域訂定 128-位元節點密鑰，該區域僅

在若緊接在此區域之前的"密鑰"位元設定為一時存在。

已使用 SecurDisc 特徵的其中一個寫入的媒體包含訂定用於資料安全性及盜拷防護的冗餘定義、密鑰及辨識碼的額外資訊，此資訊的一些可儲存於使用者資料區域外，做為例如在光碟上的 ID 區段，其支援用 SecurDisc 盜拷防護。第 6 圖顯示媒體 ID 或磁片獨特 ID 的具體實施例，顯示於第 6 圖的磁片獨特 ID 係為當其所儲存區域被寫入時，於一次寫入，或循序寫入媒體，一種由光碟驅動所產生的 128-位元隨機數目，當其第一次被要求時。主機僅能藉由成功完成驅動器主機認證而得到至該磁片獨特 ID 的存取，如同將於下文所敘述。在該磁片獨特 ID 的儲存位置係依據實體媒體格式而定，在下文中，將詳細敘述由 SecurDisc 所支援的不同媒體格式。例如，在 DVD+R/+RW 媒體，磁片可儲存於緩衝區 2，然而，其他位置亦為可能的，可選擇不會與其他盜拷防護技術干擾的儲存位置。

根據第 2 圖，SecurDisc 媒體可包含在使用者資料區域或資料區段 155 的加強安全性及可靠性所需的資訊中的一些，此資訊可為獨立的檔案系統及亦使用 ISO 9660/Joliet 運作及所有偏好 UDF(UDF=通用數據格式)。

第 7 圖顯示基本 SecurDisc 技術錨結構(BTAS=基本 SecurDisc 技術錨結構)。BTAS 可例如放置於 RLSN 15(RLSN=相對邏輯扇區號)，相對於在偏移 RBP 64(RBP=相對位元組位置)的 SecurDisc 啟動紀錄區段的開始，而且，一個 BTAS 的冗餘拷貝可放置在 SecurDisc 啟動紀錄區段的

最後一個 LSN，或是緊接在第二 AVDP(AVDP=卷描述符關鍵指針)之前的邏輯扇區。該 BTAS 參考 FFIT(FFIT=檔案片段資訊表)及冗餘資訊區塊，及這些結構的每一個的第二冗餘備份拷貝，及於是提供用做位於使用者資料區域的所有 SecurDisc 結構的錨。第 7 圖顯示示例 BTAS 的具體實施例。

第 7 圖顯示結構尺寸的域其以位元組訂定結構總尺寸為大端字節，其可例如總是為 56-位元組。而且，第 7 圖顯示結構辨識碼"BTAS"，其包含"BTAS"的 ASCII(ASCII=美國資訊交換標準碼)表示，其識別該結構為 SecurDisc 技術錨結構。

域 DSILSN(DSI=磁片安全資訊)以大端字節訂定該磁片安全資訊結構的邏輯扇區號，若此安全資訊不存在，此域的所有位元組被設定為零。而且，第 7 圖顯示 FFITLSN，其以 64-位元大端字節訂定該 FFIT 的邏輯扇區號。

示於第 7 圖的另一個域係為 ARBLSN(ARB=應用撤銷鎖)及以 64-位元大端字節訂定該 ARB 的邏輯扇區號，或是以零填入的域，若沒有任何 ARB 存在。在使用 SecurDisc 的盜拷防護或密碼短語保護特徵的所有媒體的具體實施例 ARB 為需要的，ARB 為一種撤銷區塊，其可用於撤銷經折衷應用。

第 7 圖進一步顯示"Backup DSILSN"-，"Backup FFITLSN"-及"Backup ARBLSN"-域，其訂定該個別備份結構的邏輯扇區號。該 FFIT 包含關於由 SecurDisc 所管理的該磁片每一個相連區域的資訊，此種相連區域包含由盜拷

防護或密碼短語所保護的檔案，及由檢查和所保護的檔案，該 FFIT 係在所有其他檔案之後儲存於磁片上，以允許檢查和在紀錄方法期間於作業中產生，FFIT 的位置為彈性的，FFIT 係由 BTAS 參考，其係以標頭開始及結構的具體實施例係示於第 8 圖。

標頭資訊係包含於含有版本信息的 FFITH(FFITH=FFIT 標頭)域及顯示用於該媒體任何部分的不同 SecurDisc 特徵的域。FFIT 的備分係如上文所敘述由 BTAS 參考，其位置可自由選擇。然而，為達到最大可信度，最低需求為該備份 FFIT 應實體上遠離 FFIT 的第一拷貝，該備份 FFIT 可儲存於與主要 FFIT 不同的封包。

如在第 8 圖所顯示，結構以"FFITH Size"-域(FFITHS=FFITH 尺寸)開始，其以大端字節訂定結構總尺寸及位元組，在一個具體實施例該結構尺寸總是為 40 位元組，而且，第 8 圖顯示 FFIT 辨識碼，其包含辨識該結構為 SecurDisc 檔案片段信息表的字串"BFIT"的 ASCII 表示。

而且，第 8 圖顯示一種 SecurDisc FFIT 版本信息，其訂定該結構的版本數。該第一位元組包含高版本數第二位元組包含低版本數，在一個具體實施例該高版本數係為 01h。一個實施僅依靠 FFITH 及其 FFITE(FFIT 登錄)的其於信息的配置若高版本數為 01h。僅若低版本數高於實施所支持的版本數，該實施仍依靠已在前一個具體實施例版本所定義的結構。

而且，第 8 圖顯示一種 SecurDisc"盜拷防護回復"-域，

其包含衍生自如上文所計算的特殊盜拷防護回復密碼短語的 128-位元 AES 密鑰值。在另一具體實施例可能沒有對此值的密碼短語認證檢查和。若在創作期間沒有任何盜拷防護回復密碼短語被指定，此域的所有位元組可設定為零。

而且，第 8 圖顯示一種 SecurDisc 密碼短語認證檢查和，其包含可用於認證由使用者所輸入的密碼短語正確性的 128-位元檢查和。該密碼短語認證檢查和具一種固定值 PVC，其可使用得自該使用者密碼短語的密鑰貢獻加密之，如在上文所敘述。

而且，在第 8 圖有一種 SecurDisc 整體特徵標誌屏蔽，其包 XOR 運算的結果，結合此 FFIT 所有 FFITE 的所有特徵標誌屏蔽。第 8 圖亦顯示 FFITE 塊大小，在此具體實施例其係為一種 32-位元大端字節值，及所有 FFITE 可以具固定塊大小的塊狀信息單儲存。在第 8 圖所示結構底部，存率個 FFITE 塊，其以 64-位元大端字節值訂定包含於檔案片段信息表的 FFITE 塊的數目。FFITE 的塊狀清單在 FFITH 之後立即開始，如在第 8 圖所說明。

在其他具體實施例當增加額外域時 FFITH 可生長，FFITH 的位置可以下式計算

EFITEOFFSET[0]=FFITLSN*BPS+FFITHS

FFITELSN[0]=FFITEOFFSET[0] DIV BPS

FFITERBP[0]=FFITEOFFSET[0] MOD BPS

FFITEOFFSET[0]係為第一 FFITE 相對於磁片使用者區域的開始的相對位元位置(RBP=相對位元位置)，BPS 係

為位元組數目每扇區及 FFITELSM 係為 FFIT 的 LSM。

此運算的結果係為 FFITELSN[0]，第一個 FFITE 及 FFITERBP[0]，自該扇區開始的第一 FFITE 的相對組位元位置係由 FFITELSN[0]所訂定。

FFITE 係以它們的片段的 LSN 之遞增順序儲存。特別登錄 x 的位置係計算為

EFITEOFFSET[x]= FFITEOFFSET[0]+x * FFITHS

FFITELSN[x]=FFITEOFFSET[x] DIV BPS

FFITERBP[x]=FFITEOFFSET[x] MOD BPS

其中 FFITEOFFSET[x]係為第 x 個 FFITE 相對於磁片使用者區域的開始的 RBP，x 係為介於 0 及 NUMFFITE-1 之間的數目及 FFITECS 係為 FFITE 內容大小。

此運算的結果係為 FFITELSN[x]、第 x 個 FFITE 的 LSN 及 FFITERBP[x]，自該扇區開始的第 x 個 FFITE 的相對組位元位置係由 FFITELSN[x]所訂定。

FFITE 結構的具體實施例係是於第 9 圖，第 9 圖顯示一種"檔案片段的 LSN"-域，其訂定由 FFITE 所管理的檔案片段的 LSN。而且，一種域係專屬於在邏輯扇區的檔案片段的大小，其訂定在邏輯扇區由 FFITE 所管理的檔案片段的大小。邏輯扇區係為 SecurDisc 的最小邏輯單元，若未完全使用扇區，在此具體實施例剩餘空間可由零填入。

密碼短語保護域"PP"係包含一種標誌，亦為該 SecurDisc 特徵標誌屏蔽的一部分，若為確實，由 FFITE 所管理的檔案片段係為密碼短語保護的。該"CS"-域，亦為該

SecurDisc 特徵標誌屏蔽的一部分，若為確實，由此 FFITE 所管理的檔案片段的內容可使用儲存於此 FFITE 的"檔案片段的檢查和"-域辨認。

該"CP"-域為該 SecurDisc 特徵標誌屏蔽的一部分，其可假設關於由此 FFITE 所管理的檔案片段的盜拷防護的四個不同條件，如在第 10a 圖的表所訂定。第 10a 圖顯示盜拷防護值的具體實施例，其顯示盜拷防護是否用於此檔案片段，及特殊保護輸出原則是否應用。

第 9 圖顯示在該"CP"-標誌確實的情況下該檔案片段檢查和，此域可包含由此 FFITE 所管理的檔案片段的 AES-128 加密雜湊，若該 CP 標誌為錯誤的，此域包含所有零。而且第 9 圖在列 9 顯示保留用於 SecurDisc 特徵標誌屏蔽銀身的一種空間。

第 10b 圖顯示應用撤銷區塊結構的具體實施例(ARB=應用撤銷區塊)，主要及備份 ARB 係由 BTAS 參考，該放置可為自由選擇的，然而，為達到最大可信度，該備份 ARB 應實體上遠離該主要 ARB 拷貝。在一個具體實施例，最低要求為應儲存該備份 ARB 於與主要 ARB 不同的封包。

如在第 10b 圖所示例，該應用撤銷區塊可用做密鑰成份極具兩個域，根據第 10b 圖，該"ABB 長度"-域使用位元組以大端字節訂定該應用撤銷區塊的長度，該"應用撤銷區塊"-域以撤銷區塊的格式訂定該應用撤銷區塊，如上文所敘述。

在 ODD 及主機之間的所有通訊可使用延伸至現有

MtFuji 或 MMC 指令或是新指令的方式進行。在一些具體實施例一些常數及辨識碼已被指定暫時的值但是在標準化方法中可被指定不同的值，具體實施例可使用官方辨識碼及常數，所以具體實施例並不限於在此專利說明書所提及的絕對值。

SecurDisc 的具體實施例的一部份，可為 SecurDisc 特徵描述子允許主機決定 SecurDisc 是否由光碟驅動支援及目前存在於驅動的該光碟是否可隨 SecurDisc 使用。在一個具體實施例該特徵會設定為主動的無論是否已使用 SecurDisc 寫至該光碟。光碟驅動(ODD=光碟驅動)可支援一 GET 構形指令當由該 MMC/MtFuji(MCC=多媒體指令)說明書所訂定時及其可用於自該 ODD 得到該特徵描述子，此指令的執行在驅動主機授權之前可不為需要的。

特徵描述子結構的一個具體實施例係敘述於第 11 圖，第 11 圖的結構顯示一種特徵碼，其可例如為 SecurDisc 具體實施例的 0113h(大端字節)。"目前"-域係包含顯示可用於 SecurDisc 紀錄的光碟是否存在於驅動器的標誌。"持續"-域係包含顯示目前標誌的狀態可在任何時間改變的標誌，在其他具體實施例其可總是設定為真。而且，該"版本"-域可對一個具體實施例的版本設定為零，此表示僅若任何光碟驅動機側的變化在未來發生時會變化。"保留"-域為保留的及在此具體實施例可僅包含零。該"額外長度"-域可設定為 4 以允許未來的擴充。若 CPA(CPA=盜拷防護主動的)設定為真，此標制訂定 SecurDisc 盜拷防護可隨目前插在驅動

器的光碟使用。

在讀取該 SecurDisc 特徵描述子之後，該主機確認其與許可的 SecurDisc 驅動器工作，在一些具體實施例讀取該 SecurDisc 特徵描述子對驅動器主機認證為非進行不可的。在驅動器主機認證期間，除了主機應用及光碟驅動皆為許可組件，亦可建立總線密鑰，此總線密鑰稍後用於交換盜拷防護的加密資料，在寫入任何 SecurDisc 內容之前驅動器主機認證為必要的。

在認證期間，主機及驅動器皆被指定一組密鑰，這些密鑰可用於建立一種分享的機密，總線密鑰可用於主機應用及 ODD 之間的經加密通信。第 12 圖說明驅動主機認證。

主機可要求來自驅動器的 AGID(AGID=認證授與 ID)以進行方法辨識。

由那時起 AGID 可以每一個 REPORT KEY 或是 SEND KEY 指令通過以使的驅動器可區別在具體實施例的並行認證序列。該驅動器可以 AGID 及通訊協定版本數回覆。在一個具體實施例若主機支援更近期的通訊協定版本，其可選擇以支援較舊通訊協定版本，若此為最終個別相符原則所允許。除了該 AGID 及版本數，該驅動器可送回其 DEVID(DEVID=裝置 ID)。若主機選擇吸收認證其可藉由發佈 REPORT KEY INVALIDATE AGID 指令而如此進行。

在一些具體實施例該驅動器可確認通訊協定版本數與所支援通訊協定版本一致。

若該媒體允許使用盜拷防護，亦即若 CPA 在特徵敘述

係設定為確實，該主機可發佈 REPORT KEY 磁片獨特 ID 以接收以總線密鑰 KB 加密的 DUID，其在下文係稱為驅動器主機認證形式 I，其會解密及儲存該 QUID 以隨檔案片段的加密/解密使用，該 REPORT KEY QUID 僅發佈做為驅動器主機認證序列的部份若 CPA 標誌係設定為確實，亦即在驅動器主機認證形式 I 內。即使若 CPA 標誌係為確實，該 REPORT KEY 指令可被省略，此係使用一般稱的驅動器主機認證形式 2，其將敘述於下文及在此情況該驅動器不會產生或讀取 DUID。

該主機可接著釋出由發佈 REPORT KEY INVALIDATE AGID 所獲得的 AGID 做為該認證序列的最後步驟。驅動器主機認證可經由該 REPORT KEY 及 SEND KEY 指令執行，如在例如 MMC/MtFuji 所定義。可定義 SecurDisc 的新密鑰類以區別新的認證方法與現有的認證方法，SecurDisc 的中間密鑰類的值可設定為 21h，其目前係儲存於 MMC/MtFuji。若任何 SEND KEY 或 REPORT KEY 指令以錯誤順序傳送，該驅動器可以 CHECK CONDITION 狀態終結該不適當的指令。

第 13 圖顯示 REPORT KEY 指令結構的具體實施例。根據第 13 圖可使用 REPORT KEY 指令的該指令解密子區塊以強調來自該 ODD 的資訊，在一個具體實施例該運算模式可總是設定為 A4h，對 SecurDisc 的一個具體實施例該密鑰類可訂定該密鑰類及可設定為 21h。該放置長度以大端字節 WORD 值定義驅動器至主機通訊的最大轉移長度。其

可相符在主機側保留的緩衝器大小以接收由該主機送回的資料，若該域為零，則沒有任何資料會被傳送，此情況不必要必須為錯誤。

該"密鑰格式"-域以 6 位元大端字節值訂定由該主機所要求的資訊種類。該"AGID"-域可包含該 REPORT KEY AGID 指令的認證授與 ID，該 AGID 可設定為零，其將詳細敘述於下文。對所有其他 REPORT KEY 要求，其可設定為由該 REPORT KEY AGID 所送回的 AGID。該"控制"-域包含控制位元組如由 MMC/MtFuji 所定義，其語意係依據用於傳送該 MMC 指令的匯流排形式而定。

該 ODD 會隨回覆封包回覆至 REPORT KEY AGID 及通訊協定版本指令，其中結構的具體實施例係詳細敘述於第 14 圖。該資料長度可定義該回覆封包的長度而不需"資料長度"-域本身，在該 REPORT KEY AGID 回覆封包的一個具體實施例此值總是為 0Ah。該"經保留"-域包含經保留位元，在此具體實施例其可設定為零。該"ODD 通訊協定版本數"-域可訂定由該 ODD 所提及的認證序列的通訊協定版本，若該主機支援更近期的通訊協定版本但仍支援由該 ODD 所支援的通訊協定版本，該主機可選擇使用該舊的通訊協定版本以完成該認證順序。對該具體實施例的版本，該通訊協定版本數姆可為 00h。

該 AGID 包含由該 ODD 保留用於此認證方法的 AGID，該 AGID 可傳送至所有下列 REPORT KEY 及 SEND KEY 指令，該 DEVID 訂定指定至該 ODD 的該裝置 ID，

該 ODD 會隨回覆封包回覆至 REPORT KEY ODD Key Contribution 指令，其係詳細敘述於第 15 圖。該"資料長度"-域可定義該回覆封包的長度而不需"資料長度"-域本身，在此具體實施例該 REPORT KEY ODD Key Contribution 回覆封包可為 36h。該"經保留"-域包含經保留位元，其可皆設定為零。如下文該"經加密 ODD 隨機數目"-域可包含由該 ODD 所產生的 128 位元隨機數目 R1，使用已指定至該應用的機密密鑰 PK2 加密，該"經加密主機隨機數目"-域可包含由該主機先前傳送至該 ODD 的 128 位元隨機數目 R2，使用已指定至該應用的機密密鑰 PK2 加密，其中 R1 及 R2 係以 AES-CBC 模式加密，該主機必須使用

R1 || R2=AESCBCDecrypt (PK2, R1 || R2)

以得到正確結果。

"位元位置指標值"-域可訂定在由該 ODD 送回的應用撤銷區塊中對應於該節點號的位元位置，其亦為由該應用所使用的密鑰貢獻陣列內的指標以計算 PK2。再次，該"經保留"-域包含所有經保留位元，其可皆設定為零。該"AARB 節點號"訂定在由該 ODD 送回的節點，其可與儲存於該應用內的密鑰貢獻陣列合併及允許該應用計算 PK2。

該 ODD 以回覆封包回覆 REPORT KEY ODD 磁片獨特 ID，其係示例於第 16 圖，第 16 圖顯示一種"資料長度"-域，其可定義該回覆封包的長度而不需"資料長度"-域本身，在此具體實施例的回覆封包中該 REPORT KEY 磁片獨特 ID

總是為 12h。再次，該"經保留"-域顯示經保留位元，其可皆設定為零。該"經加密磁片獨特 ID"係包含，以總線密鑰 KB 加密的 128 位元 DUID，該 REPORT KEY INVALIDATE AGID 指令使該 AGID 無效，該 ODD 以空的回覆封包及"GOOD"-狀態顯示回覆 REPORT KEY INVALIDATE AGID 指令。之後，主機不再使用該 AGID 發佈任何 SEND KEY 或 REPORT KEY 指令直到其被重新指定至該主機做為另一個 REPORT KEY AGID 及通訊協定版本指令。

用於傳送資訊至該 ODD 的 SEND KEY 指令的共同描述子區塊係說明於第 17 圖。在此具體實施例該"運算碼"-域可總是設定為 A3h，在一個具體實施對 SecurDisc 該密鑰類可訂定該密鑰類及可設定為 21h。該"參數列長度"-域以大端字節 WORD 值訂定要自該傳送的位元組數目，在一些具體實施若該域為零，沒有任何資料會被傳送。該"密鑰格式"-域以 6 位元大端字節值訂定要傳送至該 ODD 的資訊種類，該"AGID"-域係包含該認證授與密鑰及可設定為對所有 SEND KEY 要求由該 REPORT KEY AGID 所送回的該 AGID。該"控制"-域係包含控制位元組如由 MMC/MtFuji 所定義，其語意係依據用於傳送該 MMC 指令的匯流排形式而定。

接附於 SEND KEY 主機隨機數目及通訊協定版本指令該主機可傳送資訊封包，其係示例於第 18 圖，該"資料長度"-域可訂定該資訊封包的大小而不需"資料長度"-域本身，在該 SEND KEY 主機隨機數目及通訊協定版本封包，

對該此值總是為 2Ah。該"經保留"-域顯示經保留位元，其可皆設定為零。該"經加密主機隨機數目"係包含由該主機所產生的，使用已指定至該 ODD 的機密密鑰 PK1 加密的 128 位元隨機數目 R1，該"通訊協定版本"-域可包含一種通訊協定及在此具體實施例可設定為 00h。該"位元位置指標值"-域可訂定指定至該 ODD 的 PK1[]陣列內的指標，其應由該驅動器使用以建立 PK1。該"撤銷區塊節點號"-域以 128 位元密鑰值訂定伴隨在該 DRB 的位置 x 的節點號。該"應用認證獨特 ID"可訂定一種應用認證獨特 ID，其可由該 ODD 使用以進行 AARB 分析。

在任何 SecurDisc 特徵用於紀錄之前，該主機實施可確保該驅動器為一種許可的 SecurDisc 驅動器及該媒體可用於 SecurDisc 紀錄或是已使用該 SecurDisc 特徵寫入。讀取器實施需要 SecurDisc 驅動器僅若 SecurDisc 的盜拷防護特徵用於鑰被讀取的媒體。依據該實施為讀取器或紀錄器實施，在到達起始化狀態之前可進行數種不同核對。

第 19 圖以流程圖的觀點顯示起始化及 SecurDisc 特徵偵測實施的具體實施例，該流程圖說明 SecurDisc 起始化順序的讀取器觀點，此順序在每一次磁片變更事件發生時重複。在第一步驟 1910 該讀取器試著讀取該 BTAS，藉由讀取該 BTAS，該主機確認在該驅動器的媒體使用已啟動的 SecurDisc 寫入。若沒有找到該 BTAS 結構，在步驟 1915 可裝設該媒體而不需 SecurDisc 支援，若找到該 BTAS 結構，該主機檢查該 SecurDisc FFIT 的整體特徵標誌屏蔽以

決定盜拷防護是否於步驟 1920 使用，若使用該盜拷防護特徵，在步驟 1930 該主機恢復該 SecurDisc 驅動器特徵敘述子及檢查該 SecurDisc 特徵是否被支援及目前媒體形式是否支援該盜拷防護特徵，亦即該 CPA 標誌是否設定為確實，若該驅動器完全未支援 SecurDisc，或是在該驅動器沒有任何盜拷防護相容媒體，在步驟 1915 可裝設該媒體而不需 SecurDisc 支援。否則驅動器主機認證形式 1 步驟可在步驟 1935 進行。在認證失敗的情況該驅動器係認為是不能處理經盜拷防護的 SecurDisc 媒體，在步驟 1915 可裝設該媒體而不需 SecurDisc 盜拷防護支援，形式 1 驅動器主機認證自該媒體讀取該磁片獨特 ID。若該認證是成功的，在步驟 1940 可使用 SecurDisc 裝設該媒體。在無法讀取該 BTAS 結構的第一拷貝的情況，例如因為在該媒體的缺陷，可藉由向後掃描該媒體，例如以最後寫入的 LSN 開始，搜尋該備份 BTAS 結構。

與讀取器相反，當創作該媒體時紀錄應用不依據該 SecurDisc 媒體形式而定，而是，其總是促使使用者依所需插入正確形式的空白媒體。紀錄應用的起始化步驟的具體實施例係說明於第 20 圖。注意產生 SecurDisc 影像為允許的僅若 SecurDisc 紀錄器接附於該系統。在此情況，該 SecurDisc 紀錄器係用於執行驅動器主機認證形式 2 以確保其為授權的，使用支援盜拷防護的 SecurDisc 編譯可能無法寫入影像。

第 20 圖顯示在步驟 2010 如上文所敘述該主機恢復該

SecurDisc 驅動器特徵敘述子，及該主機檢查該 SecurDisc 特徵是否被支援，若該驅動器完全未支援 SecurDisc，在步驟 2015 創作方法持續而不需 SecurDisc 支援。

在步驟 2020 該應用允許使用者創作及構形一計畫，結果為據所使用 SecurDisc 特徵的獨特組合之計畫。當產生 SecurDisc 影像時，可能未使用盜拷防護，此係在步驟 2025 檢查，若該影像為盜拷防護的，紀錄被吸收，否則根據步驟 2030 執行驅動器主機認證形式 2。若沒有任何影像產生，在步驟 2035 使用者需要支援 SecurDisc 的媒體，該媒體接著基於如上文所敘述的具 SecurDisc 特徵設定為活性的特徵敘述子辨識之。

若該計畫係構形為盜拷防護的，即使若其為部分盜拷防護的，僅在如上文所敘述的特徵敘述子具 CPA 標誌設定為活性的媒體可被接受用於寫入，所以，該 CPA 標誌於步驟 2040 檢查，若該計畫具經啟動的盜拷防護。若盜拷防護為啟動的但媒體不支持盜拷防護，在步驟 2035 使用者再次需要其他媒體，否則，該 CPA 標誌於步驟 2045 檢查該 CPA 標誌是否為確實在步驟 2050 執行驅動器主機認證形式 1，否則驅動器主機認證形式 2 在步驟 2055 執行。形式 1 驅動器主機認證自該媒體讀取該磁片獨特 ID。在認證失敗的情況，該驅動器係認為是不能處理 SecurDisc 媒體，裝設該媒體而不需 SecurDisc 支援。若任何認證是成功的，在步驟 2060 該主機將該計畫寫至該 SecurDisc 媒體及若該驅動器主機認證失敗，該主機會將錯誤報告至在步驟 2065 的使用

者，該應用亦會提供在組件已宣告無效的情況如何使SecurDisc再次工作的提示。

為計算加密特定檔案片段的某內容存取密鑰(CAK=內容存取密鑰)，如上文所敘述儲存於該FFIT的SecurDisc特徵標誌屏蔽可用於決定哪一個密鑰成分可被組合以形成該CAK。在一個具體實施例有兩種密鑰成分來源，由創作人所提供密碼短語所產生的雜湊及該 DUID，對每一個個別檔案片段這兩種密鑰成分可自由地合併。第21圖顯示盜拷防護標誌及密碼短語標誌及它們的相對應敘述之所有組合，在第21圖表中的第一組合為無關重要的，因為該檔案片段為一種未經加密的檔案，當域道具所敘述標誌組合的檔案片段，沒有任何加密已施用於該檔案且其可立即使用而不需任何進一步的轉換。在其餘情況，CAK係依據盜拷防護(CP)而計算及考慮DUIO的密碼短語(PP)標誌，該密碼短語雜湊或二者，總是與該 AGK(AGK=認證授與密鑰)組合如同將在下文所詳細敘述。

檔案片段的CAK，可例如如下計算，其中每一個密鑰成分具例如128位元的寬度。

$$CAK=KI_0 \text{ XOR } KI_1 \text{ XOR } [...] \text{ XOR } KI_{n-1}，$$

其中n為至該存取密鑰的成分數目。

對在該FFITE具PP標誌組的檔案片段，該主機可自使用者所提供密碼短語計算該128位元密鑰成分，為此目的，可將16位元單一碼表示的使用者密碼短語拷貝至緩衝器，其接著以要為128位元的倍數的零值位元組填入，接

著如下文計算密鑰成分 KI_x：

KI_x=AESHash(緩衝器)。

使用者密碼短語總是對情況為敏感的及可具 16 字元的最低長度。

在使用密鑰成分 KI_x 之前該主機可辨識正確的密碼短語由使用者提供，此可由使用如下文的密鑰成分 KI_x 如上文所敘述地解密該經加密 SecurDisc PVC 而完成：

PVC'=AESDescrypt(KI_x, EPVC)。

接著將該值 PVC'與 PVC 相較，若 PVC 等於 PVC'，正確的密碼短語已由使用者提供。

對在該 FFITE 具 PP 標誌組的檔案片段，該主機可如上文所敘述地使用協定自驅動器得到該 DUID。接著如下文計算成分 KI_x：

KI_x=AESHash(DUID)。

若磁片的原先作者已設定盜拷防護的回復密碼短語，如上文所敘述可使用該 FFITE 的 SecurDisc"盜拷防護回復"-域以恢復該 DUID 而不需自該驅動器得到該 DUID 如上文所指定。在此操作模式，該 DUID 可如下文自該"SecurDisc 盜拷防護回復"-域(BCPRF=得到 SecurDisc 盜拷防護回復域)：

4. 若 BCPRF 的所有位元為零，沒有任何回復密碼短語已被設定，可不解除該盜拷防護。

2.如上文所指定自由使用者所輸入的密碼短語計算盜拷防護回復密鑰(CPRK=盜拷防護回復密鑰)。

5. 如下文計算該 DUID：

DUID=AESDescrypt(CPRK, BCPRF)。

為得到 AGK(AGK=認證授與密鑰)，該主機如上文所敘述處理該 ARB，所得 AGK 係由該 AUID 及該 AGKC(AGKC=AGK 貢獻者)產生，如上文所敘述其二者皆為許可的加密機密及常數。為加密及解密在磁片上的個別邏輯扇，可使用如上文所敘述的自該 CAK 加密地得到的密鑰。

為計算用於特定扇區的密鑰，使用在計數器模式的 AES-128 以如下文自該 CAK 得到扇區密鑰：

KS_x=AESEnscrypt(CAK, x)。

其中 x 為要解密的扇區的 LSN。

該扇區密鑰接著用於加密/解密該相對應扇區，其係使用

AESCRCEnscrypt(KS_x, 內容)/ AESCRCDescrypt(KS_x, 內容)。

若檔案片段的相對應 FFITE 的 CS 標誌被設定，該部份可使用儲存餘相同 FFITE 的 128 位元檢查和辨識。

該檢查和可由檔案片段的內容計算，例如使用下列功能：

CHECKSUM=AESHash(FFC)。

於此 FFC 係為該檔案片段由連鎖組成的所有邏輯扇的內容，若未完全使用最後一個邏輯扇，其可以零填入。所有邏輯扇的內容表示所有邏輯扇的用戶有效負載當寫於媒

體且沒有任何預先處理例如施用解密。

主機可藉由檢查所有相對應檔案片段與它們的檔案片段檢查和辨識於 SecurDisc 啟動磁片上檔案的有效性，若任何檔案片段具錯的檢查和，該檔案係被考慮為毀壞的。若當讀取檔案時發現缺陷封包該主機可使用冗餘資訊(若存在)以再構建該正確檢查和。

該驅動器可計算該 DUID 做為該認證順序的一部份當 CPA 等於確實，該 DUID 可產生為 128 位元隨機數目當該 REPORT KEY DUID 發布及沒有任何 DUID 存在於該磁片。

當自該主機接收 FEATURE REQUEST 指令，該 ODD 可試著自該媒體讀取該 DUID，其可隱藏該 DUID 於其 RAM 值到其由該主機使用該 REPORT KEY DUID 指令要求時。或者，在驅動器主機認證期間當如上文所指定執行該 REPORT KEY DUID 指令時該 ODD 可讀取該 DUID。該 ODD 可僅執行後者若計算該 CPA 標誌不需要知道該 DUID 狀態。

當該主機要求該 SecurDisc 特徵敘述子時，該 ODD 計算為該特徵敘述子一部份的該 CPA 標誌及決定該驅動器主機認證的形式，其係如在第 22 圖所指示而執行。在步驟 2210，立即變化事件發生，其接著為標準磁片識別步驟 2215。在磁片已識別後，構形在步驟 2220 讀取及磁片形式在步驟 2225 檢查。

可區別四個不同形式的磁片，在步驟 2230 偵測到具盜拷防護能力的空白磁片，隨後在步驟 2235 該 CPA 設定為

確實。在步驟2240，偵測到具DUID蓋掉能力的部份紀錄可重寫媒體，及據此在步驟2235該CPA標誌亦設定為確實。在步驟2245偵測到不具DUID蓋掉的部份紀錄寫入一次媒體或是可重寫媒體，據此，在步驟2250該DUID被讀取及在步驟2255若該DUID存在則據此在步驟2235該CPA係設定為確實。若該DUID不存在如在步驟2260所示，該CPA標誌係設定為假如在步驟2265所示。若在步驟2270偵測到任何其他媒體在步驟2265該CPA標誌亦設定為假。

第23圖顯示相關於SecurDisc具體實施不同ODD狀態表的流程圖。再次，存在兩種形式的驅動器主機認證，其中在第23圖流程圖的形式1表示具讀取該DUID的驅動器主機認證，然而形式2表示不具讀取該DUID的驅動器主機認證，此與上文所敘述一致。形式1認證僅當該CPA標誌設定為確實時發生，形式2認證可在形式1認證發生的任何時間執行但其從不改變該驅動器的內部狀態。當該CPA標誌設定為假時形式2認證亦可發生，即使在該驅動器沒有任何磁片。

在第23圖流程圖的每一個狀態可使用三種變數敘述，第一個變數為稱之為"髒"的標誌，若此標誌為真，該DUID為該ODD所知道，其可能已由該ODD產生但未與該媒體同步化。若此標誌為假，該DUID不為該ODD所知道或是其係與儲存在該媒體的該DUID同步化。換言之，若該DUID為該ODD所知道，則此標制訂定該DUID是否已寫至該媒體。

下一個標至為"DUID 已知"標誌。若此設定為真，該DUID為該ODD所知道因為其係自該媒體產生或是自該媒體讀取。若此設定為假，該 DUID 為不知道因為其係尚未自該媒體讀取，或是因為其未存在於該媒體。隨後該標誌訂定該DUID是否為該ODD所知道。

"CPA"標誌訂定在該驅動器的媒體是否可用於盜拷防護，若其被設定為真，則該媒體可用於寫入經盜拷防護的檔案，若其為假，則該媒體無法用於寫入經盜拷防護的檔案。若該標誌為未知的，則尚未評估該標誌。

當磁片變化發生時，該ODD的第一狀態為狀態2310，其中髒標誌為假的，DUID 為未知的及 CPS 亦為未知的。該主機接著發布 GET CONFIGURATION 指令以恢復該SecurDisc特徵的特徵敘述子。該 ODD 的狀態係相關於該CPA 特徵(其已知為真或假)而變化，當指令完成時，及在該CPA設定為真的情況其由步驟2315顯示及在該CPA設定為假的情況其由步驟2320顯示。由步驟2315進一步進行，可執行該驅動器主機認證形式 2，此認證形式不改變該 ODD 的狀態。當執行該驅動器主機認證形式 1 時，該DUID 變為已知，若該 DUID 係自該媒體讀取，根據步驟2315，該髒標誌會設定為假的。若該 DUID 在該驅動器主機認證形式 1 期間產生，根據步驟 2330 該髒標誌變為真的，可讀取該SecurDis媒體而不需離開步驟2330。然而，若該資料係寫至 SecurDis，該髒標誌會再度設定為假的，及該ODD據此轉換至狀態2325，該狀態變更因為該DUID

被寫至該 SecurDisc 媒體而發生，一旦此狀態在步驟 2325 達到，自該 SecurDisc 讀取資料，或是寫入資料至該 SecurDisc 不會產生任何狀態變更。

若在開始時該 CPA 標誌偵測為假的，該 ODD 變更至狀態 2320，在狀態 2320 資料可寫至該 SecurDisc 媒體及亦可自該 SecurDisc 媒體讀取。而且，可執行驅動器主機認證形式 2。所有這些動作不會產生自狀態 2320 變化的任何狀態。

具體實施例提供盜拷防護及存取控制可由商業及私人使用者控制的優點。使用 SecurDisc 的具體實施例，有力的特徵組被提供，其使得盜拷防護及存取控制、資料安全及資料辨識，與數位簽名及內容辨識為可行。

依據本發明方法的某些實施要求而定，本發明方法可在硬體或在軟體實施，該實施可使用數位儲存媒體執行，特別是具可電讀取控制信號儲存於其上的磁片、DVD 或 CD，其與可程式電腦系統合作，使得本發明方法被執行。概略言之，所以，本發明為一種具儲存於機器可讀載體的程式代碼之電腦產品，該程式代碼為運算用的以執行本發明方法當該電腦程式產品在電腦上操作時。換言之，所以，本發明方法為一種具程式代碼以執行至少一種本發明方法的電腦程式當該電腦程式在電腦上操作時。

【圖式簡單說明】

將使用相關圖式於下文詳細敘述具體實施例，其中：

第 1a 圖顯示用於寫入的裝置之具體實施例；

第 1b 圖顯示儲存媒體的具體實施例；

第 2 圖顯示用於寫入的裝置之另一具體實施例；

第 3a 圖顯示用於提供經加密資料的裝置之具體實施例；

第 3b 圖顯示用於提供經加密資料的裝置之另一具體實施例；

第 4 圖顯示密碼系統的具體實施例；

第 5 圖顯示選擇節點密鑰結構的具體實施例；

第 6 圖顯示媒體 ID 結構的具體實施例；

第 7 圖顯示錨結構的具體實施例；

第 8 圖顯示檔案片段信息表結構的具體實施例；

第 9 圖顯示檔案片段信息表登錄結構的具體實施例；

第 10 圖顯示盜拷防護域結構的具體實施例；

第 11 圖顯示特徵描述子及特徵控制域結構的具體實施例；

第 12 圖顯示驅動主機認證的具體實施例；

第 13 圖顯示 REPORT KEY 指令的具體實施例；

第 14 圖顯示 REPORT KEY 指令的回覆封包之具體實施例；

第 15 圖顯示 KEY CONTRIBUTION 指令的回覆封包之具體實施例；

第16圖顯示DISC UNIQUE ID指令的回覆封包之具體實施例；

第17圖顯示SEND KEY指令的具體實施例；

第18圖顯示接附於SEND KEY HOST RANDOM NUMBER AND PROTOCOL VERSION指令的信息封包之具體實施例；

第19圖顯示資料讀取器實施的起始化及特徵偵測步驟的流程圖之具體實施例；

第20圖顯示寫入器實施的起始化及特徵偵測步驟的流程圖之具體實施例；

第21圖顯示盜拷防護的特徵標誌屏障之具體實施例；

第22圖顯示計算盜拷防護狀態的流程圖之具體實施例；及

第23圖顯示光碟機狀態表的流程圖之具體實施例。

【主要元件符號說明】

100	寫入設備
110、170、220、240	接收裝置
120	產生裝置
130、180	提供裝置
140	儲存裝置
150	媒體
155	資料區段
160	ID 區段
165、RNG	隨機或虛擬隨機產生器
175	讀取裝置
200	提供設備
210、235	傳送裝置
230	加密裝置
245	解密裝置
250	偵測裝置
410	創作組件
420	媒體組件
430	讀取組件
440、480	使用者施用的密碼
442、468、482、504	AES 雜湊

444、484	XOR
446、DUID	磁片獨特 ID
448、486	授權授與密鑰
450	AES 加密
452、490、LSN	邏輯扇區號
454、500、PVC	短語認證檢查和
456、492	AESCBC 加密
458、494	扇區內容
460	經加密邏輯扇
462	AES 加密器
464、EPVC	經加密 PVC
466、502	公開密鑰
470	RSA 公開密鑰雜湊
472	私密金鑰
474	RSA 簽名
476	數位 RSA 簽名
488	AES 加密
496	AES 解密
498、506	比較
500	PVC
508	RSA 辨識

1910	讀取 BTAS
1915	裝設而不需 SecurDisc
1920	檢查盜拷防護
1930	讀取特徵敘述子
1935、2050	驅動器主機認證形式 1
1940	使用 SecurDisc 裝設媒體
2010	SecurDisc 特徵敘述子
2015	持續而不需 SecurDisc 功能性
2020	創作計畫
2025	檢查盜拷防護
2030、2055	驅動器主機認證形式 2
2035	激勵媒體
2040、2045	檢查 CPA 標誌
2060	寫入 SecurDisc 媒體
2065	報告錯誤
2210	媒體變化事件
2215	標準磁片識別
2220	得到構形
2225	檢查磁片形式
2235	具盜拷防護能力的空白磁片
2240	具 DUID 蓋掉能力的部份紀錄可重

	寫磁片
2245	不具 DUID 蓋掉的部份紀錄煤體
2250	讀取 DUID
2255	DUID 存在
2260	DUID 不存在
2265	CPA 等於假
2270	其他媒體
2310	不髒，DUID 未知，CPA 未知
2315	不髒，DUID 未知，CPA 真
2320	不髒，DUID 未知，CPA 假
2325	不髒，DUID 已知，CPA 真
2330	髒，DUID 已知，CPA 真
AES	進階加密標準
AGID	認證授與 ID
AGK	認證授與密鑰
ARB	應用撤銷鎖
BFIT	檔案片段信息表的字串
CAK	內容存取密鑰
CP	拷貝防護
CPA	拷貝防護主動的
DEVID	裝置 ID

DSI	磁片安全資訊
FFIT	檔案片段資訊表
FFITHS	FFITH 尺寸
FFITECS	FFITE 內容大小
ID	身份
ODD	光碟驅動
ONK	選擇性節點密鑰
PGP	加密寶貝
PP	密碼短語
R1、R2	隨機數目

五、中文發明摘要：

一種用以將資料寫入至媒體的裝置(100)，該裝置(100)包含一用以接收來自資料提供器的寫入要求及經加密資料的裝置(110)，該裝置(100)進一步包含一用以在接收該寫入要求時產生媒體 ID 的裝置(120)，而且，該裝置(100)包含一用以將該媒體 ID 提供至該資料提供器以產生該經加密資料的裝置(130)及一用以在產生該媒體 ID 時將該經加密資料儲存於該媒體及用以將該媒體 ID 儲存於該媒體的裝置(140)，其中該經加密資料係基於該 ID 而加密。

六、英文發明摘要：

An apparatus (100) for writing data to a medium. The apparatus (100) comprises a means (110) for receiving a write request and encrypted data from a data provider. The apparatus (100) further comprises a means (120) for creating a medium ID upon reception of the write request. Furthermore, the apparatus (100) comprises a means (130) for providing the medium ID to the data provider for generating the encrypted data and a means (140) for storing the encrypted data on the medium and for storing the medium ID on the medium upon creation of the medium ID, wherein the encrypted data is encrypted based on the medium ID.

十、申請專利範圍：

1.一種用以將資料寫入至一媒體的裝置(100)，其包含：

一用以接收來自一資料提供器的一寫入要求及經加密資料的裝置(110)；

一用以在接收該寫入要求時產生一媒體 ID 的裝置(120)；

一用以將該媒體 ID 提供至該資料提供者以產生該經加密資料的裝置(130)；及

一用以在產生該媒體 ID 時將該經加密資料儲存於該媒體及將該媒體 ID 儲存於該媒體的裝置(140)，其中該經加密資料係基於該 ID 而加密。

2.如申請專利範圍第 1 項的裝置(100)，其中該用以儲存的裝置(140)係適用以將該經加密資料儲存於該媒體的一資料區段(155)及將該媒體 ID 儲存於該媒體的一 ID 區段(160)，其中該資料區段(155)係與該 ID 區段(160)隔開或分開。

3.如申請專利範圍第 2 項的裝置(100)，其中該用以儲存的裝置(140)係適用以在由該用以產生該媒體 ID 的裝置(120)產生該 ID 之後僅將該媒體 ID 儲存於 ID 該區段(160)。

4.如先前申請專利範圍中任一項的裝置(100)，其中該用以產生的裝置(12)係適用以藉由產生一隨機或虛擬隨機數目而產生一媒體 ID。

5.如先前申請專利範圍中任一項的裝置(100)，其中該用以儲存的裝置(140)係適用以將該媒體 ID 及一密碼的一

組合儲存於該媒體。

6.如先前申請專利範圍中任一項的裝置(100)，進一步包含一用以接收來自一資料讀取器的一讀取要求的裝置(170)及用以自一媒體讀取一媒體 ID 及經加密資料的裝置(175)。

7.如申請專利範圍第 6 項的裝置(100)，進一步包含一用以將來自該媒體的該媒體 ID 及經加密資料提供給該資料讀取器的裝置(180)。

8.如先前申請專利範圍中任一項的裝置(100)，其係於一晶片、一 ROM 或一光碟實施。

9.如先前申請專利範圍中任一項的裝置(100)，進一步包含一用以使用一資料提供器或一資料讀取器進行認證的裝置。

10.如先前申請專利範圍中任一項的裝置(100)，其中該用以接收的裝置(110)係適用於自該資料提供器接收一經加密寫入要求及用以解密該寫入要求。

11.如申請專利範圍第 6 至 10 項中任一項的裝置(100)，其中該用以接收該讀取要求的裝置(170)係適用於接收一經加密讀取要求及用以解密該讀取要求。

12.如先前申請專利範圍中任一項的裝置(100)，其中該用以提供的裝置(130；180)係適用於加密該媒體 ID 及用於將該經加密媒體 ID 提供至該資料提供器或該資料讀取器。

13.一種用以將資料寫入至一媒體的方法，其包含步驟：

接收來自一資料提供器的一寫入要求；

在接收該寫入要求時產生一媒體 ID；

將該媒體 ID 提供至該資料提供器以產生該經加密資料；

自該資料提供器接收該經加密資料；及

於產生該媒體 ID 時將該經加密資料儲存於該媒體及將該媒體 ID 儲存於該媒體，其中該經加密資料係基於該媒體 ID 而加密。

14.一種具有一程式代碼以在該程式代碼在電腦上操作時執行申請專利範圍第 13 項的方法的電腦程式。

15.一種用以將經加密資料提供至一資料寫入器的裝置(200)，其包含；

一用以將一寫入要求傳送至該資料寫入器的裝置(210)；

一用以在傳送該寫入要求時自該資料寫入器接收一媒體 ID 的裝置；及

一用以使用一加密密鑰加密純文本資料以得到該經加密資料的裝置(230)，該加密密鑰係基於該媒體 ID；及其中該用以傳送的裝置(210)係適用於將該經加密資料傳送至該資料寫入器。

16.如申請專利範圍第 15 項的裝置(200)，其中該用以加密的裝置(230)係進一步適用以進一步基於一密碼使用一加密密鑰。

17.如申請專利範圍第 15 或 16 項的裝置(200)，其中該

用以加密的裝置(230)係適用以進一步基於撤銷金鑰而使用一加密密鑰。

18.如申請專利範圍第 15 至 17 項中任一項的裝置(200)，進一步包含一用以將讀取要求傳送至一資料讀取器的裝置(235)、一用以接收經加密資料及一媒體 ID 的裝置(240)及一用以基於一解密密鑰解密資料以得到純文本資料的裝置(245)。

19.如申請專利範圍第 18 項的裝置(200)，其中該用以解密的裝置(245)係適用於使用基於一媒體 ID、一密碼或一撤銷金鑰的一解密密鑰。

20.如申請專利範圍第 15 至 19 項中任一項的裝置(200)，其中該用以加密的裝置(230)進一步適用以該經加密資料中的一經加密密碼加密一資訊。

21.如申請專利範圍第 18 或 19 項的裝置(200)，進一步包含一用以偵測來自該經加密資料或該純文本資料的一拷貝防護顯示的裝置。

22.如申請專利範圍第 21 項的裝置(200)，其中該用以傳送該寫入要求的裝置(210)係適用於當偵測到一拷貝防護顯示時不傳送一寫入要求。

23.如申請專利範圍第 21 或 22 項的裝置(200)，其中該用以接收一媒體 ID 的裝置(220)係適用於當偵測到該拷貝防護顯示時不接收該媒體 ID。

24.如申請專利範圍第 21 至 23 項中任一項的裝置(200)，其中該用加密的該裝置(230)係適用於當偵測到該拷

貝防護顯示時不加密資料。

25.如申請專利範圍第 21 至 24 項中任一項的裝置(200)，其中該拷貝防護顯示係對應於在該經加密或純文本資料內的一控制位元，該經加密或純文本資料具有一純文本控制資訊。

26.如申請專利範圍第 15 至 25 項其中一項的裝置(200)，進一步包含一用於使用該資料寫入器以進行認證的裝置，及其中該用以傳送的裝置(210；235)係適用於傳送一經加密讀取或寫入要求及該用以接收的裝置(220；240)係適用於接收一經加密媒體 ID。

27.一種用於將經加密資料提供至一資料寫入器的方法，其包含下列步驟：

將一寫入要求傳送至該資料寫入器；

當傳送該寫入要求時，自該資料寫入器接收一 ID；

使用一加密密鑰加密一純文本數據以得到該經加密資料，該加密密鑰係基於該媒體 ID；及

將該經加密資料傳送至該資料寫入器。

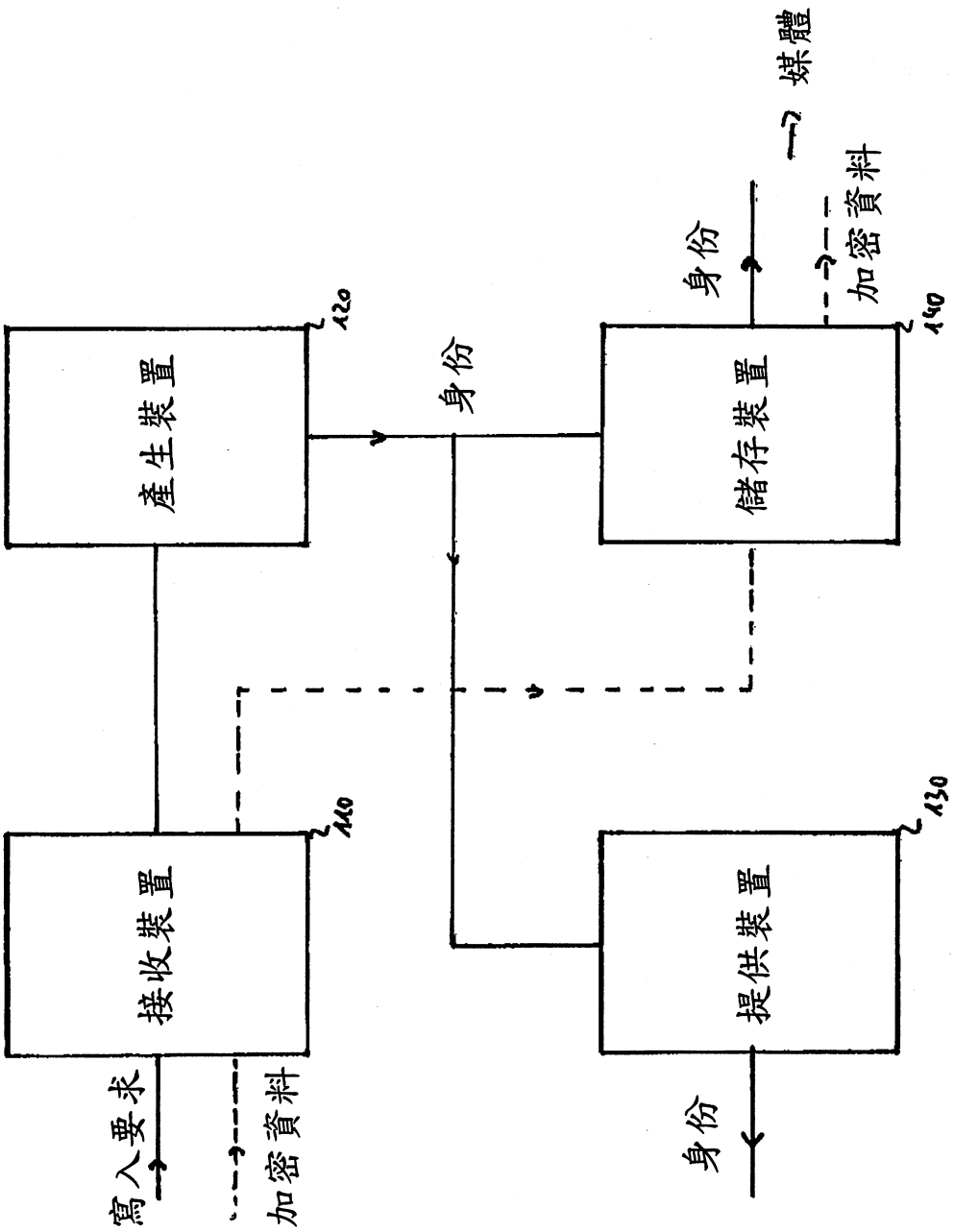
28.一種具有一程式代碼以在該電腦程式於一電腦上操作時執行申請專利範圍第 27 項的方法的電腦程式。

29.一種包含如申請專利範圍第 1 至 12 項中任一項的用以提供資料的裝置及如申請專利範圍第 15 至 26 項的用以提供經加密資料的裝置的系統。

30.一種包含如申請專利範圍第 28 項所述系統的光學驅動器。

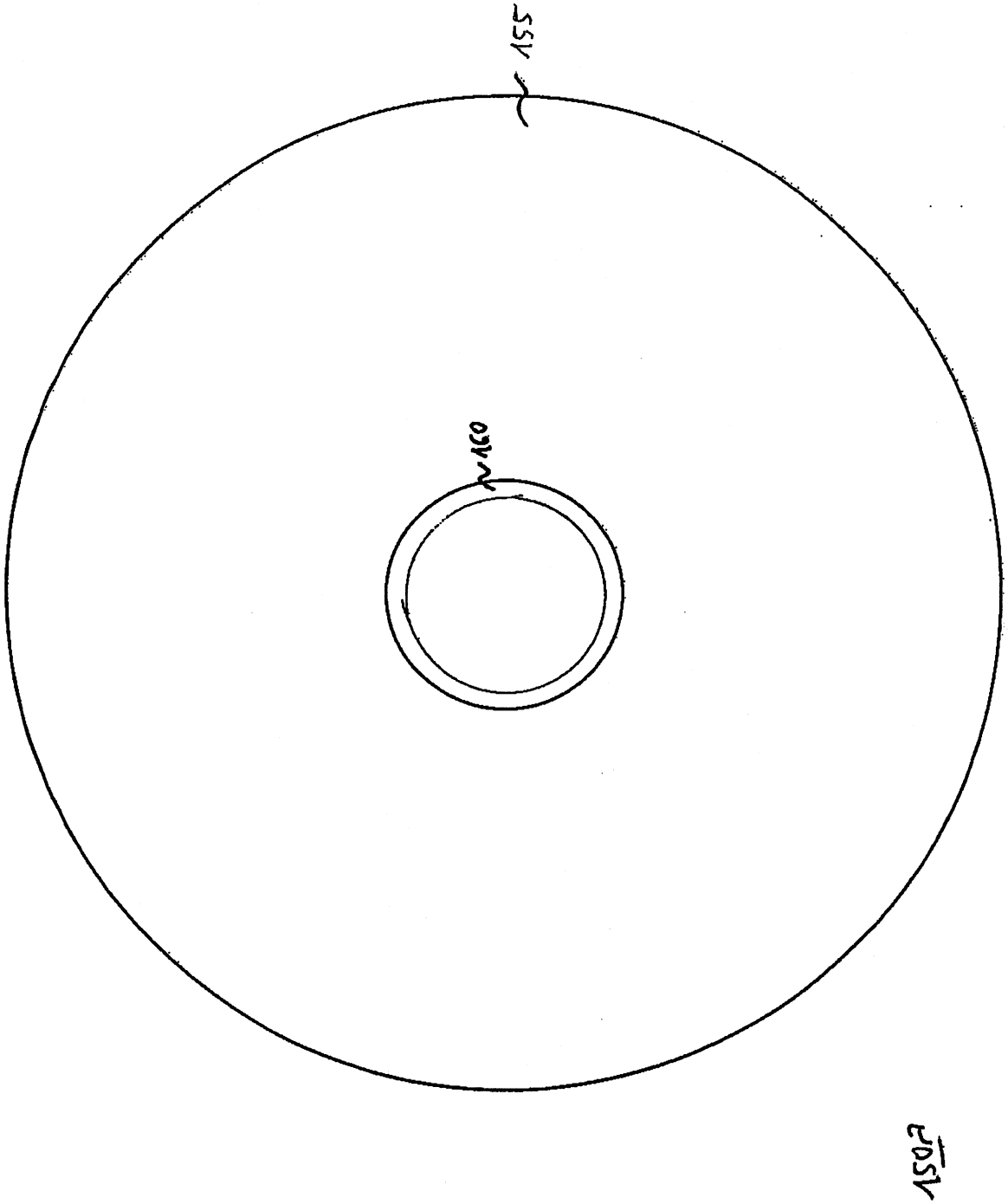
31.一包含如申請專利範圍第 14 或 28 項所述一韌體的光學驅動器。

十一、圖式：

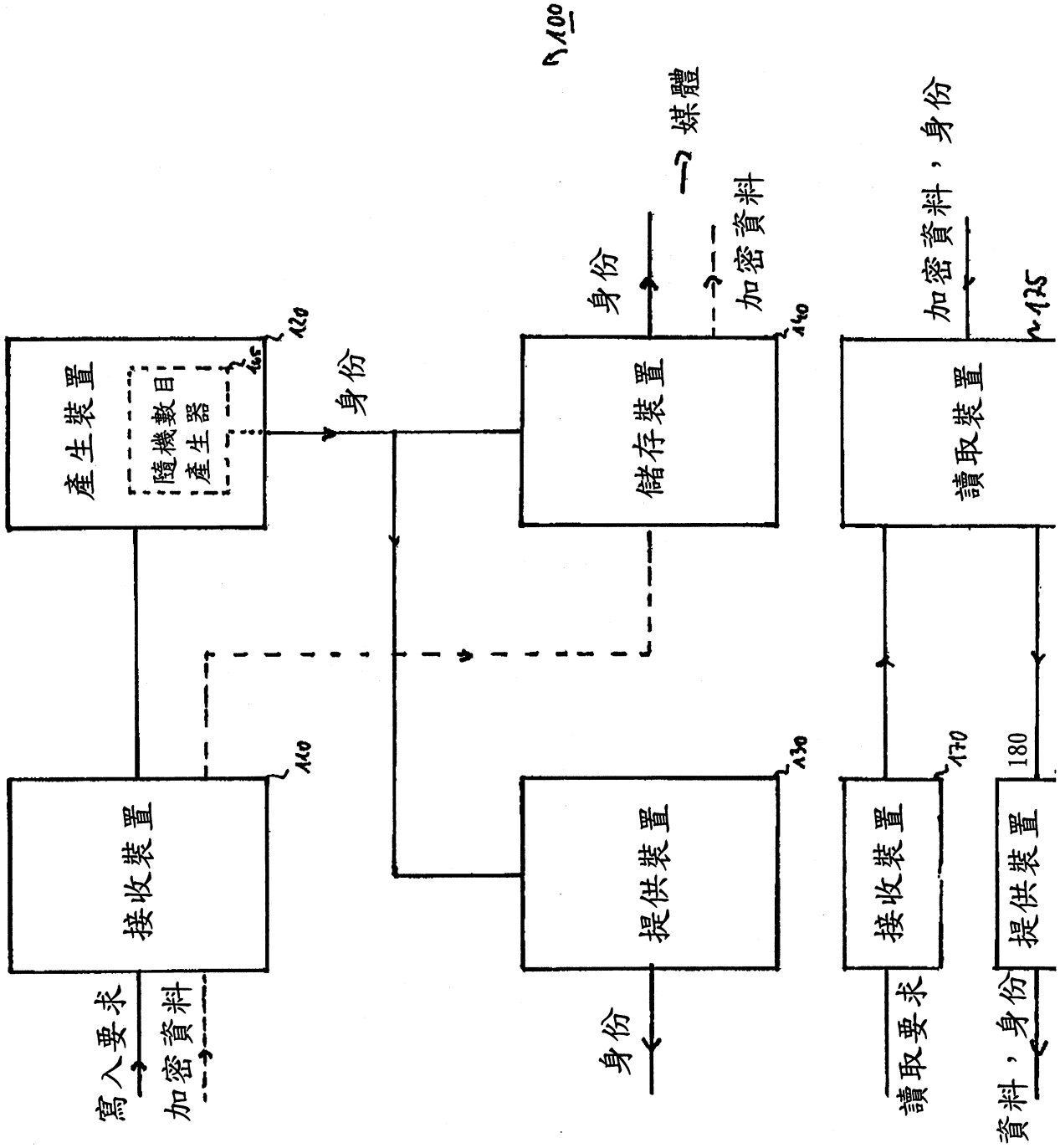


第 1a 圖

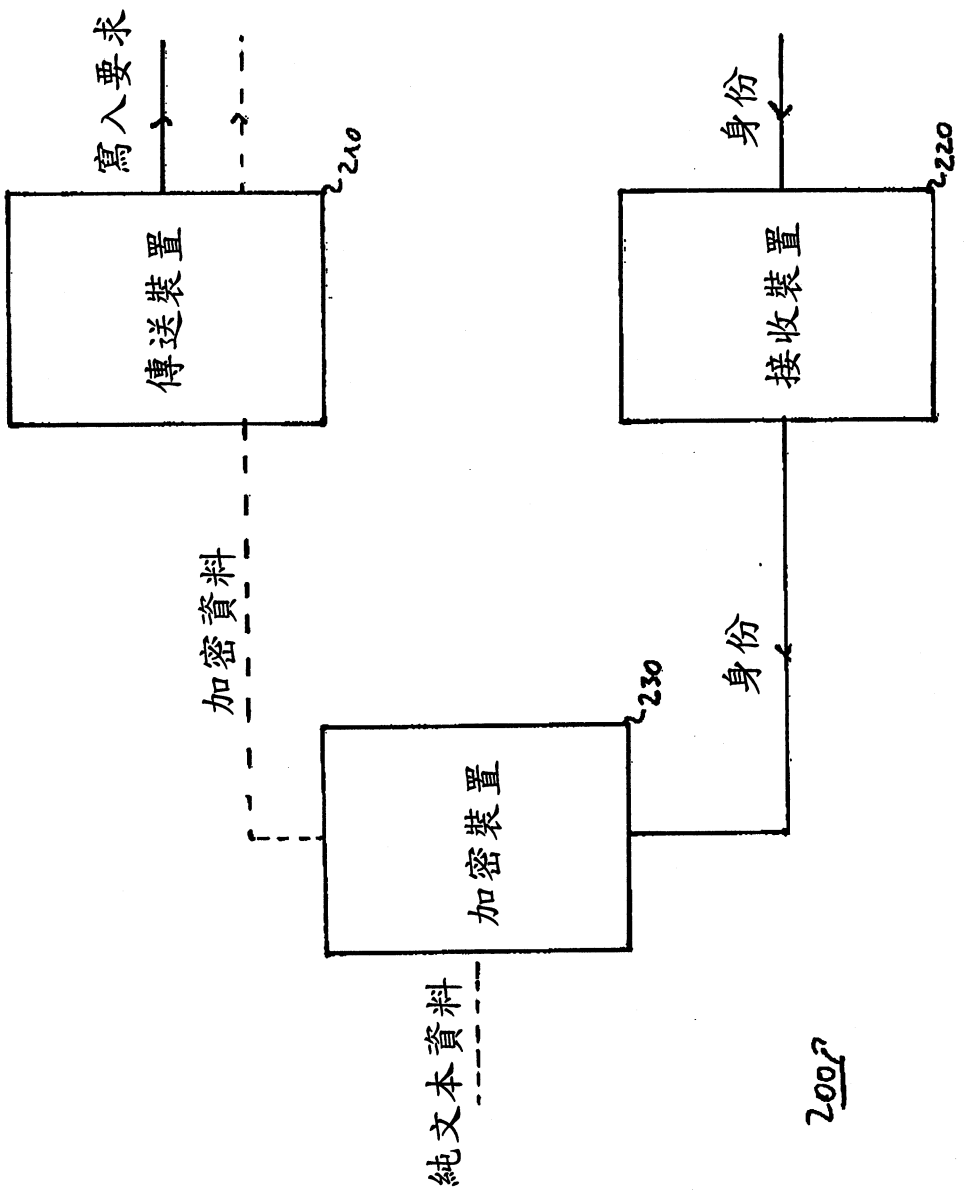
1007



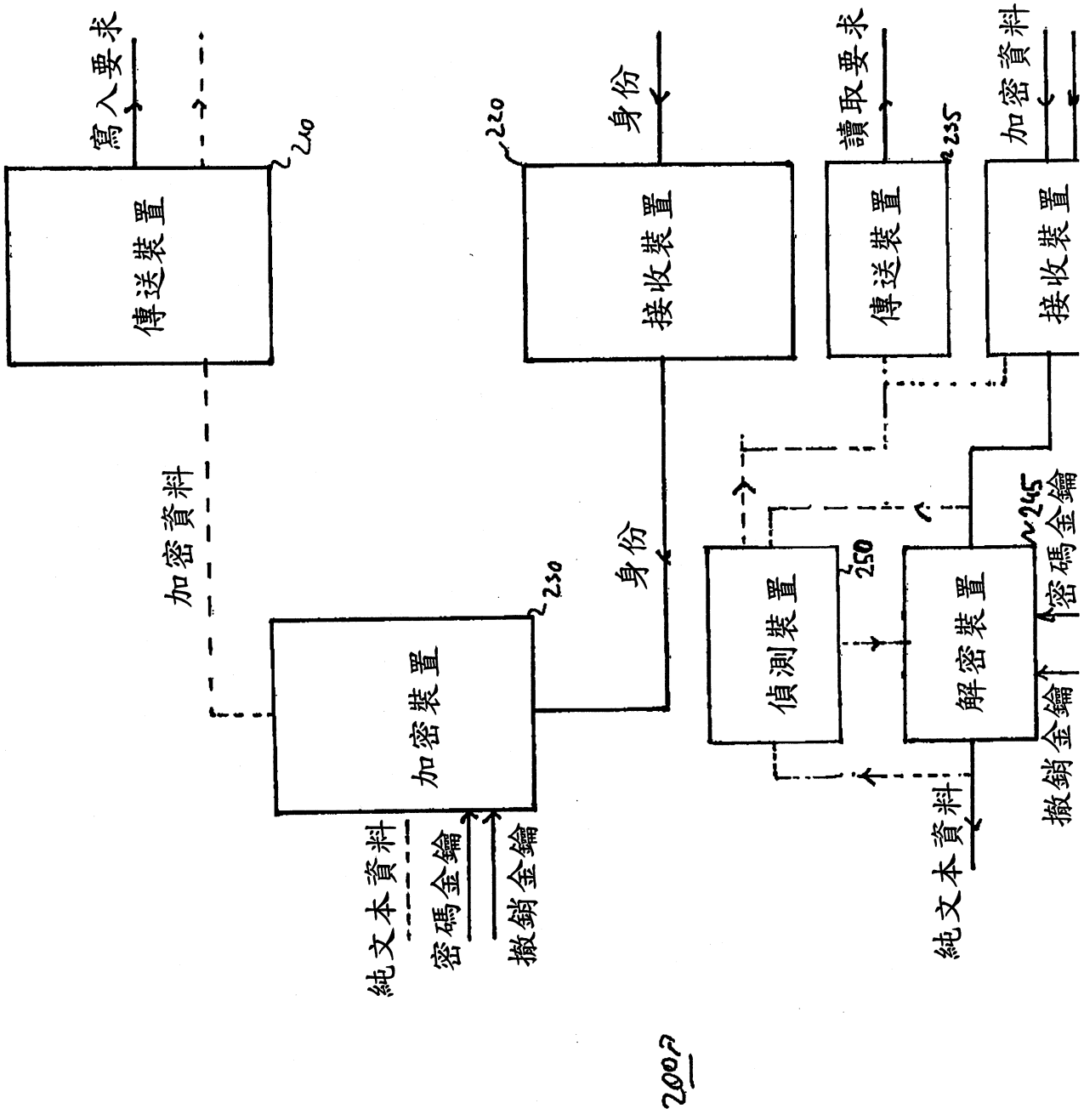
第 1b 圖


100
產生裝置
隨機數目產生器
105
120
身份
儲存裝置
媒體
加密資料
140
寫入要求
加密資料
接收裝置
110
身份
提供裝置
130
加密資料，身份
讀取裝置
125
讀取要求
接收裝置
170
加密資料，身份
提供裝置
180

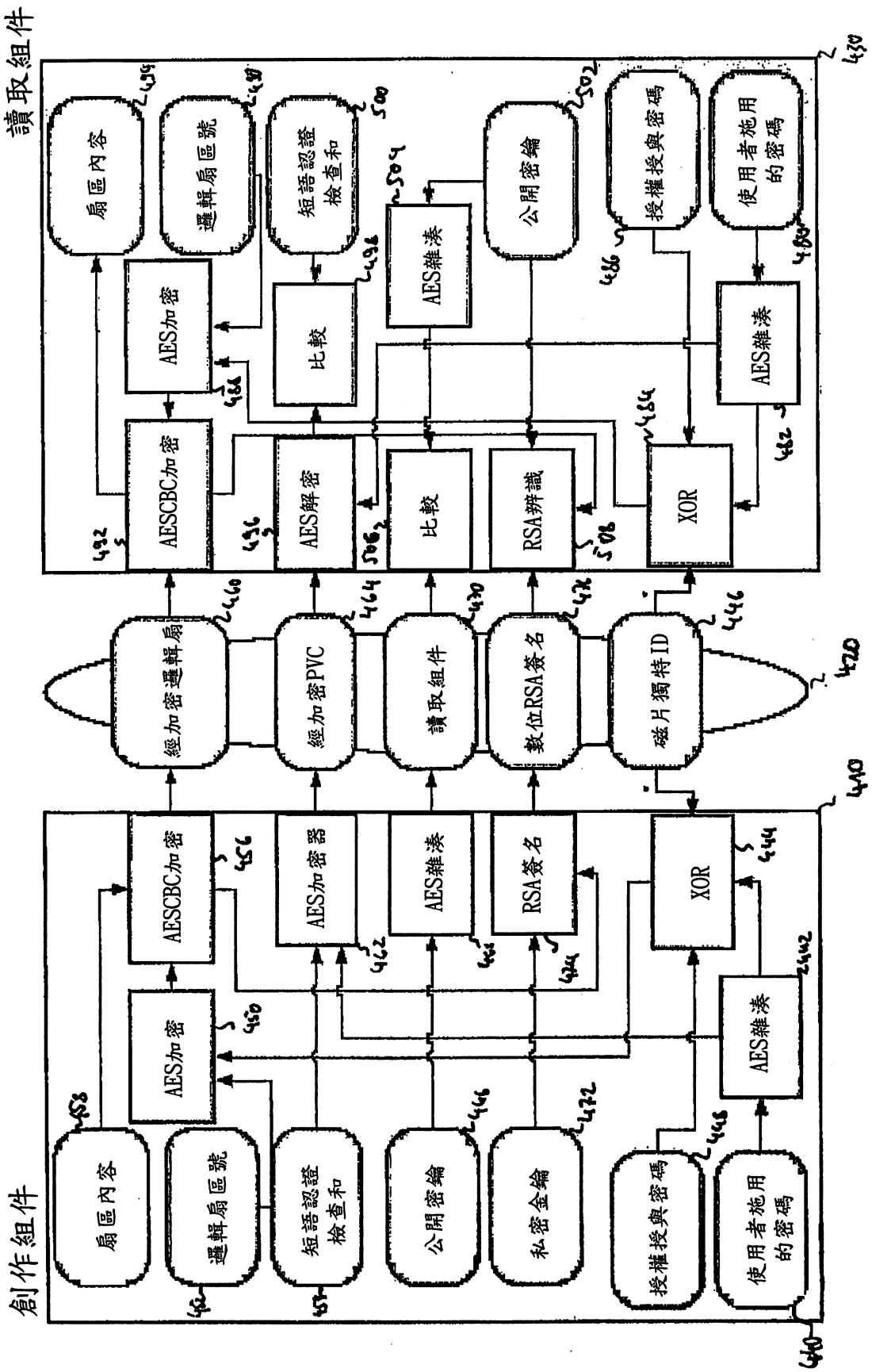
第 2 圖



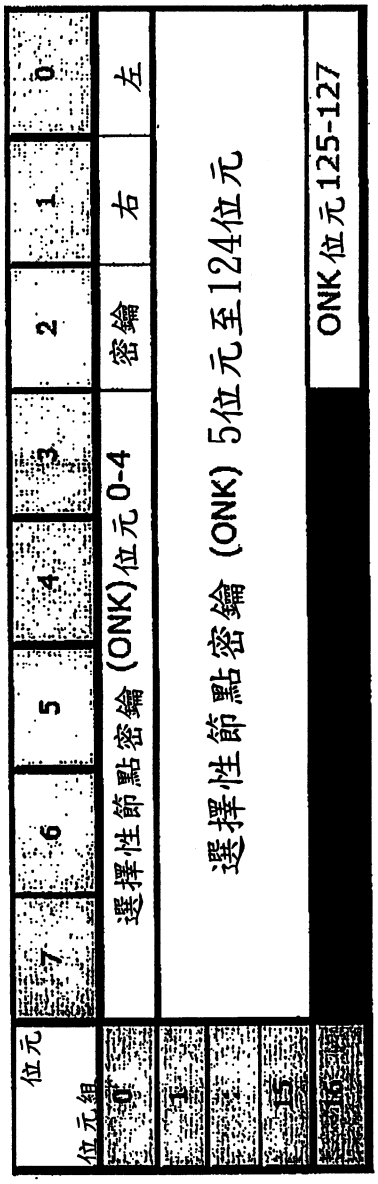
第 3a 圖


寫入要求
傳送裝置
240
加密資料
加密裝置
230
純文本資料
密碼金鑰
撤銷金鑰
身份
接收裝置
220
身份
偵測裝置
250
讀取要求
傳送裝置
235
加密資料
接收裝置
解密裝置
245
密碼金鑰
撤銷金鑰
純文本資料
200

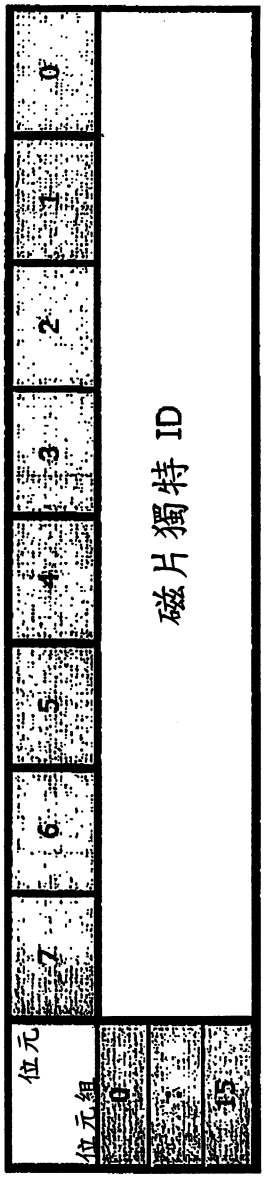
第 3b 圖


讀取組件
扇區內容
邏輯扇區號
短語認證檢查和
AES加密
AESCBC加密
比較
AES雜湊
公開密鑰
授權授與密碼
使用者施用的密碼
AES解密
RSA辨識
XOR
經加密邏輯扇
經加密PVC
讀取組件
數位RSA簽名
磁片獨特ID
創作組件
AES加密器
RSA簽名
私密金鑰

第 4 圖


位元
位元組
7
6
5
4
3
2
1
0
0
選擇性節點密鑰 (ONK)位元 0-4
密鑰
右
左
1
選擇性節點密鑰 (ONK) 5位元至124位元
2
15
16
ONK位元125-127

第 5 圖



第 6 圖

位元 / 位元組	7	6	5	4	3	2	1	0
0 : 3	結構尺寸							
4 : 7	結構識別碼 'BTAS'							
8 : 15	磁片安全資訊邏輯扇區號							
16 : 23	檔案片段資訊表邏輯扇區號							
24 : 31	應用撤銷鎖邏輯扇區號							
32 : 39	磁片安全資訊邏輯扇區號備份							
40 : 47	檔案片段資訊表邏輯扇區號備份							
48 : 55	應用撤銷鎖邏輯扇區號備份							

第 7 圖

位元 位元組	7	6	5	4	3	2	1	0
0 : 3	檔案片段資訊表標頭尺寸(FFITH尺寸)							
4 : 7	FFIT 辨識碼 'BFIT'							
8 9	SecurDisc FFIT 版本訊息 （高，低）							
10 : 25	SecurDisc 拷貝防護回復域							
26 : 41	SecurDisc 密碼短語認證檢查和 (EPVC)							
42 43	SecurDisc 整體特徵標誌屏蔽							
44 : 47	FFITE 塊大小 (FFITECS)							
48 : 55	存率個 FFITE 塊 (NUMFFITE)							

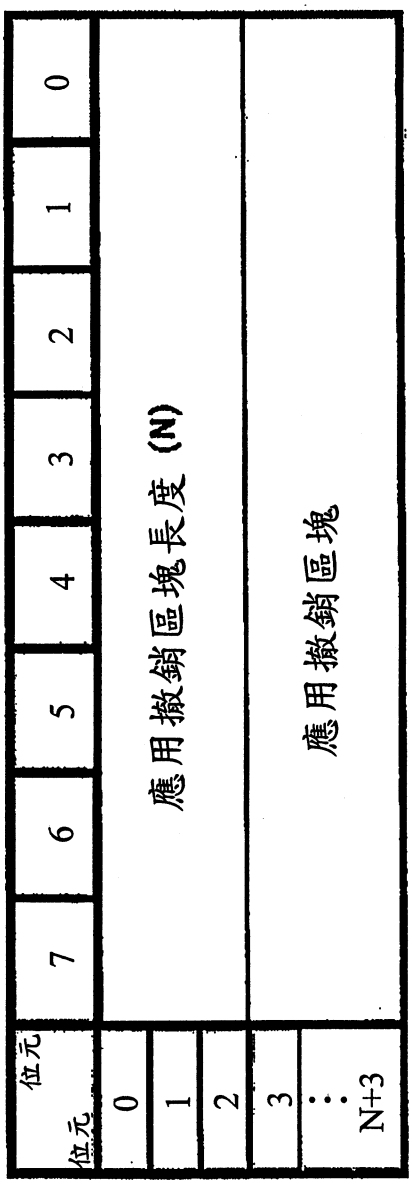
第 8 圖

位元 位元組	7	6	5	4	3	2	1	0
0 ⋮ 7	檔案片段的邏輯扇區號							
8 ⋮ 15	邏輯扇區的檔案片段大小							
8					CS	PP	拷貝防護	
9	保留(SecurDisc 特徵標誌屏蔽)							
10 ⋮ 25	檔案片段檢查和							

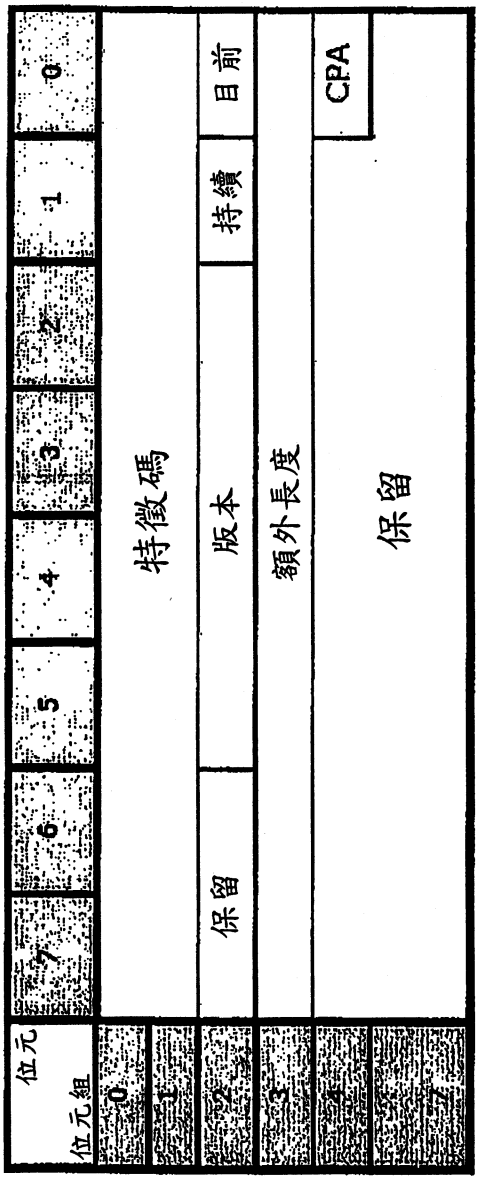
第 9 圖

拷貝防護值	敘述
00b	拷貝防護不是用於此檔案片段
01b	標準拷貝防護是用於此檔案片段
10b	拷貝防護是用於此檔案片段。特定保護輸出原則是根據用於檢視者應用的準則中所規則而應用。
11b	保留

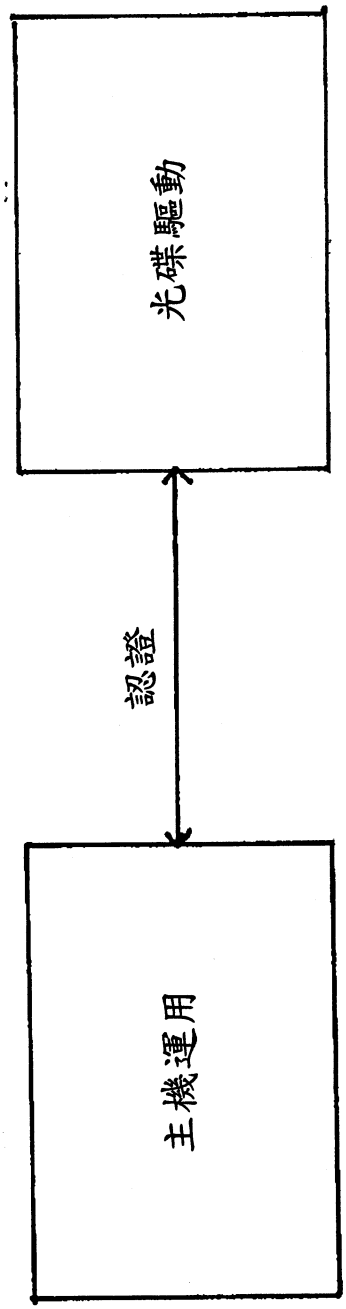
第 10a 圖



第 10b 圖



第 11 圖



第 12 圖

位元 位元組	7	6	5	4	3	2	1	0
0	運算模式 (A4h)							
1	保留							
2 3 4 5	保留							
6	保留							
7	密鑰類 (21h)							
8 9	放置長度							
10	認證授與ID				密鑰格式			
11	控制							

第 13 圖

位元 / 位元組	7	6	5	4	3	2	1	0
0	資料長度 (0Ah)							
1								
2	保留							
3								

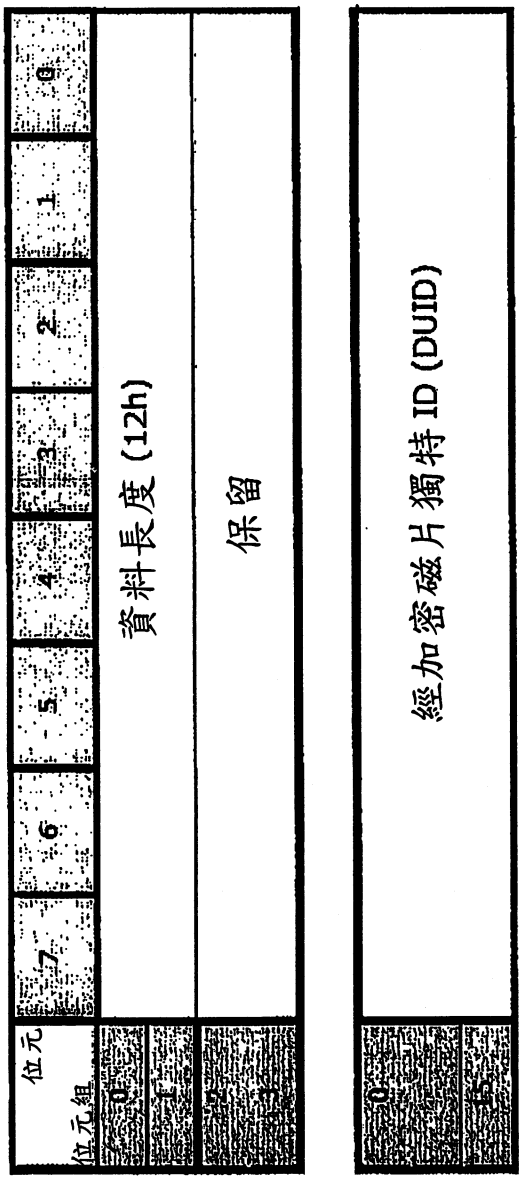
0	保留	
1		
2	光碟驅動通訊協定版本數	
3	認證授與ID	保留
4	裝置ID	
5		
6		
7		

第 14 圖

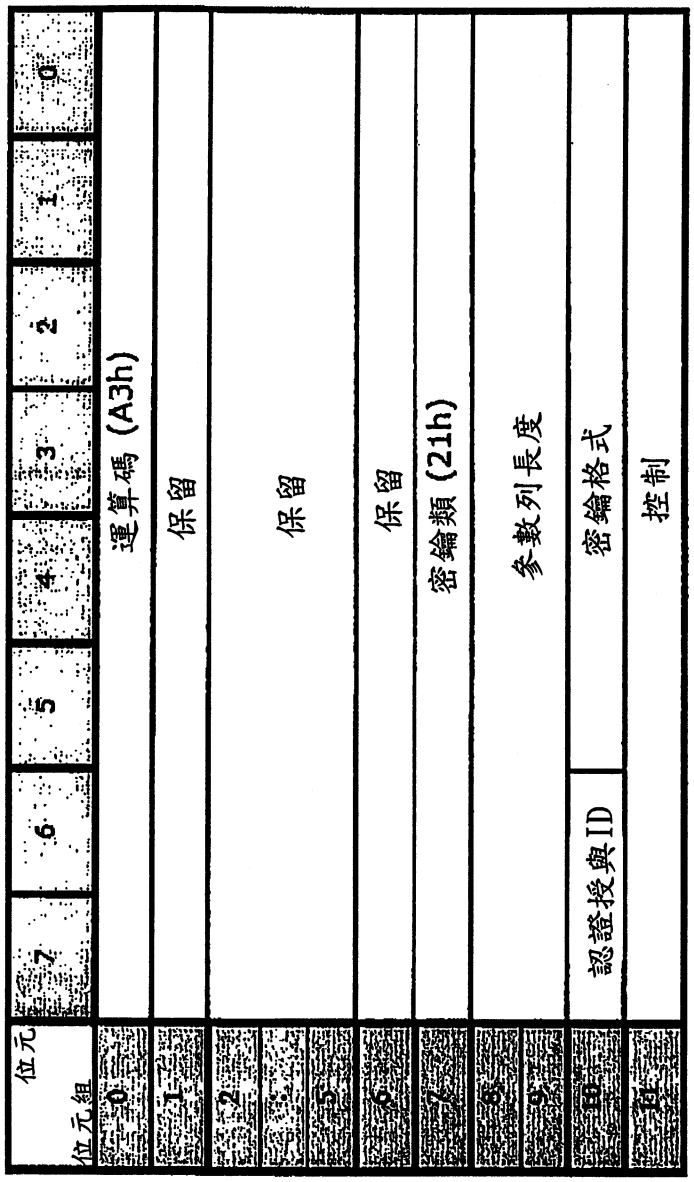
位元 位元組	7	6	5	4	3	2	1	0
0 1	資料長度 (36h)							
2 3	保留							

0 15	經加密 ODD 隨機數目 (R1)
16 31	經加密主機隨機數目 (R2)
32	位元位置指標值
33	保留
34 49	AARB 節點號
50 51	保留

第 15 圖



第 16 圖



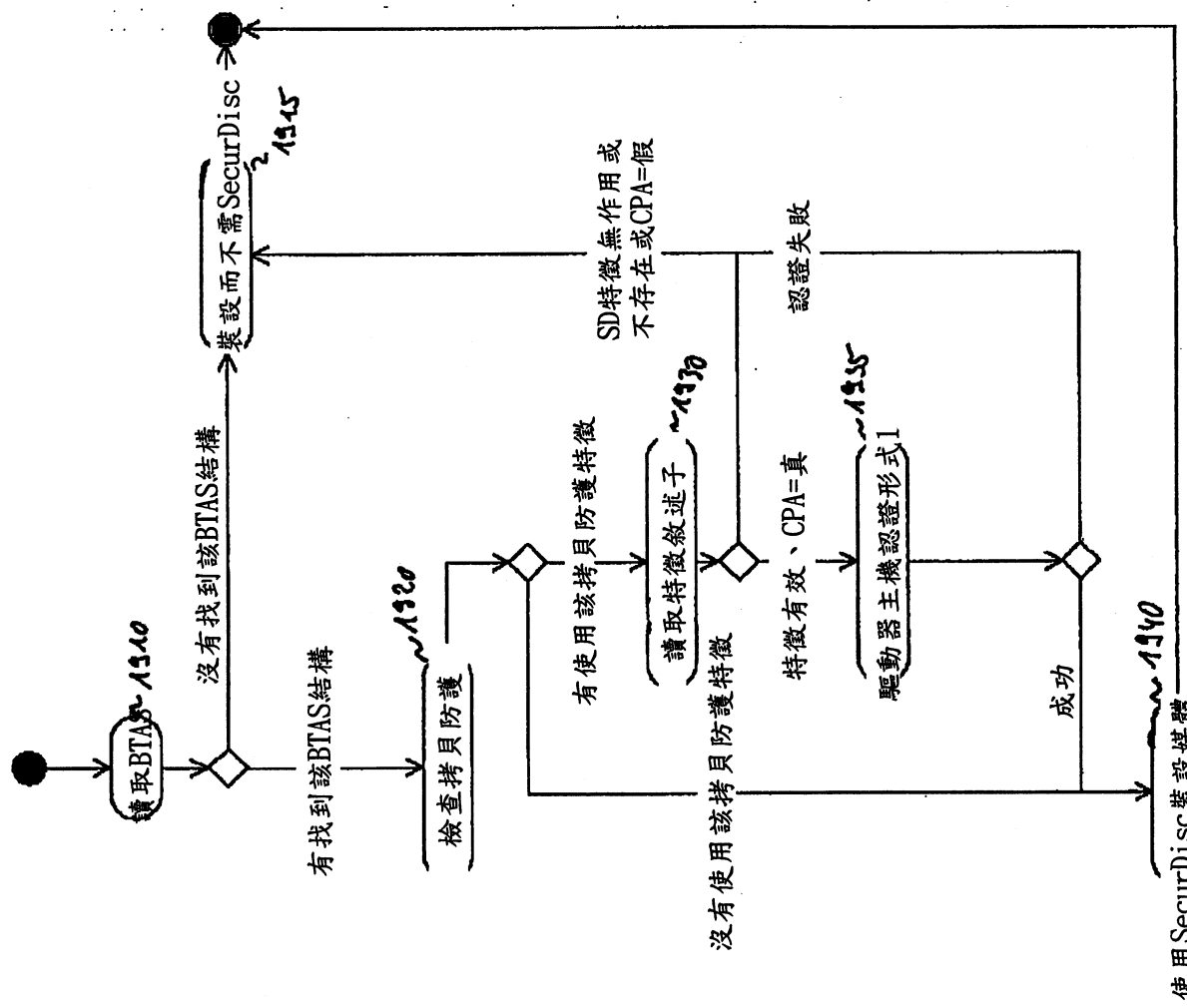
位元 / 位元組	7	6	5	4	3	2	1	0
0	運算碼 (A3h)							
1	保留							
2	保留							
5								
6	保留							
7	密鑰類 (21h)							
8	參數列長度							
9								
10	認證授與ID			密鑰格式				
11	控制							

第 17 圖

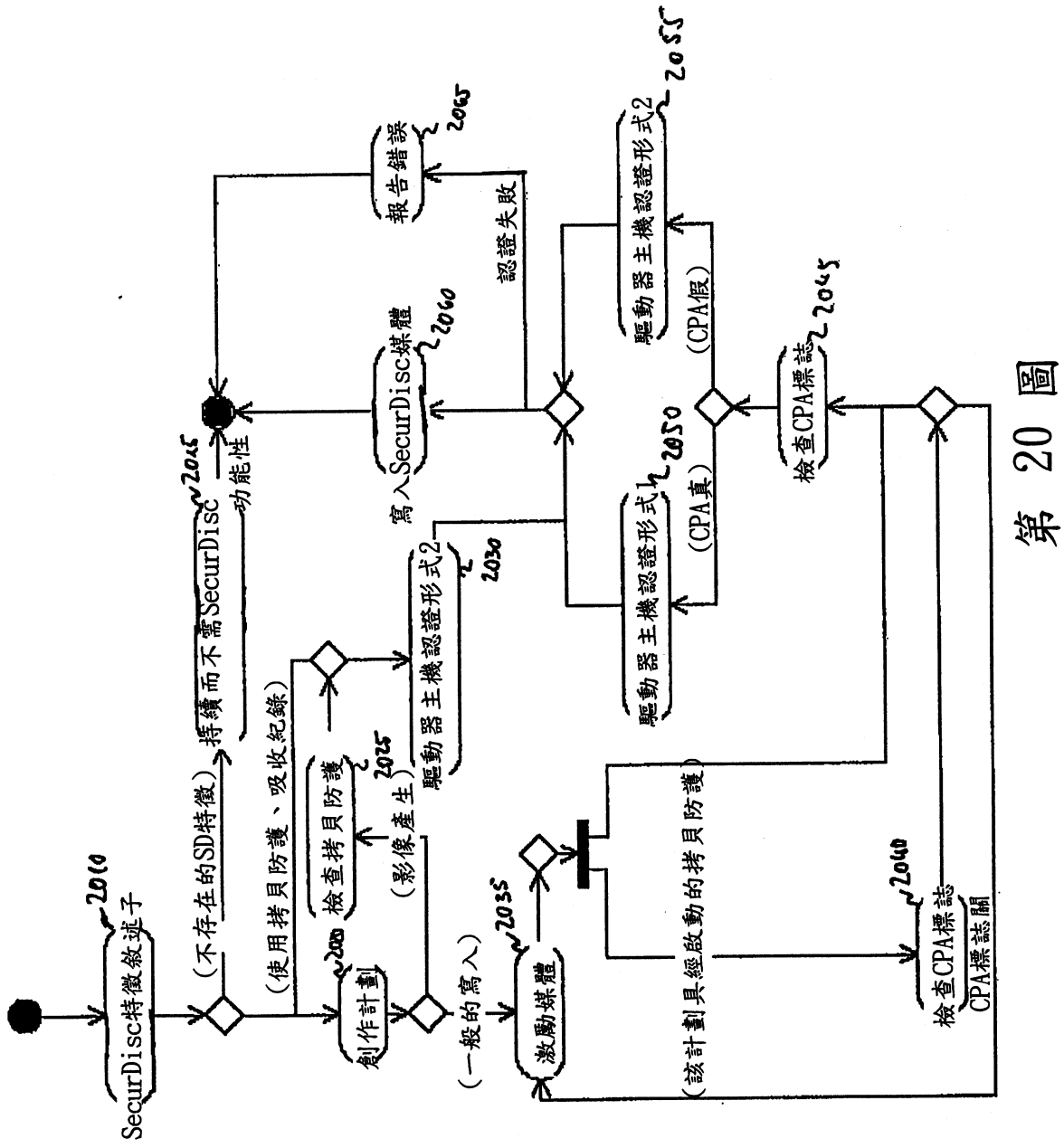
位元 位元組	7	6	5	4	3	2	1	0
0 1	資料長度(2Ah)							
2 3	保留							

0 15	經加密主機隨機數目(R2)
16	通訊協定版本
17	位元位置指標值(X)
18 33	撤銷區塊節點號(RBNK)
34 37	應用認證獨特ID(AAUID)
38 39	保留

第 18 圖


讀取BTAS
1340
沒有找到該BTAS結構
裝設而不需SecurDisc
2
1345
有找到該BTAS結構
檢查拷貝防護
1320
有使用該拷貝防護特徵
SD特徵無作用或
不存在或CPA=假
讀取特徵敘述子
1330
沒有使用該拷貝防護特徵
特徵有效、CPA=真
認證失敗
驅動器主機認證形式1
1335
成功
使用SecurDisc裝設媒體
1310

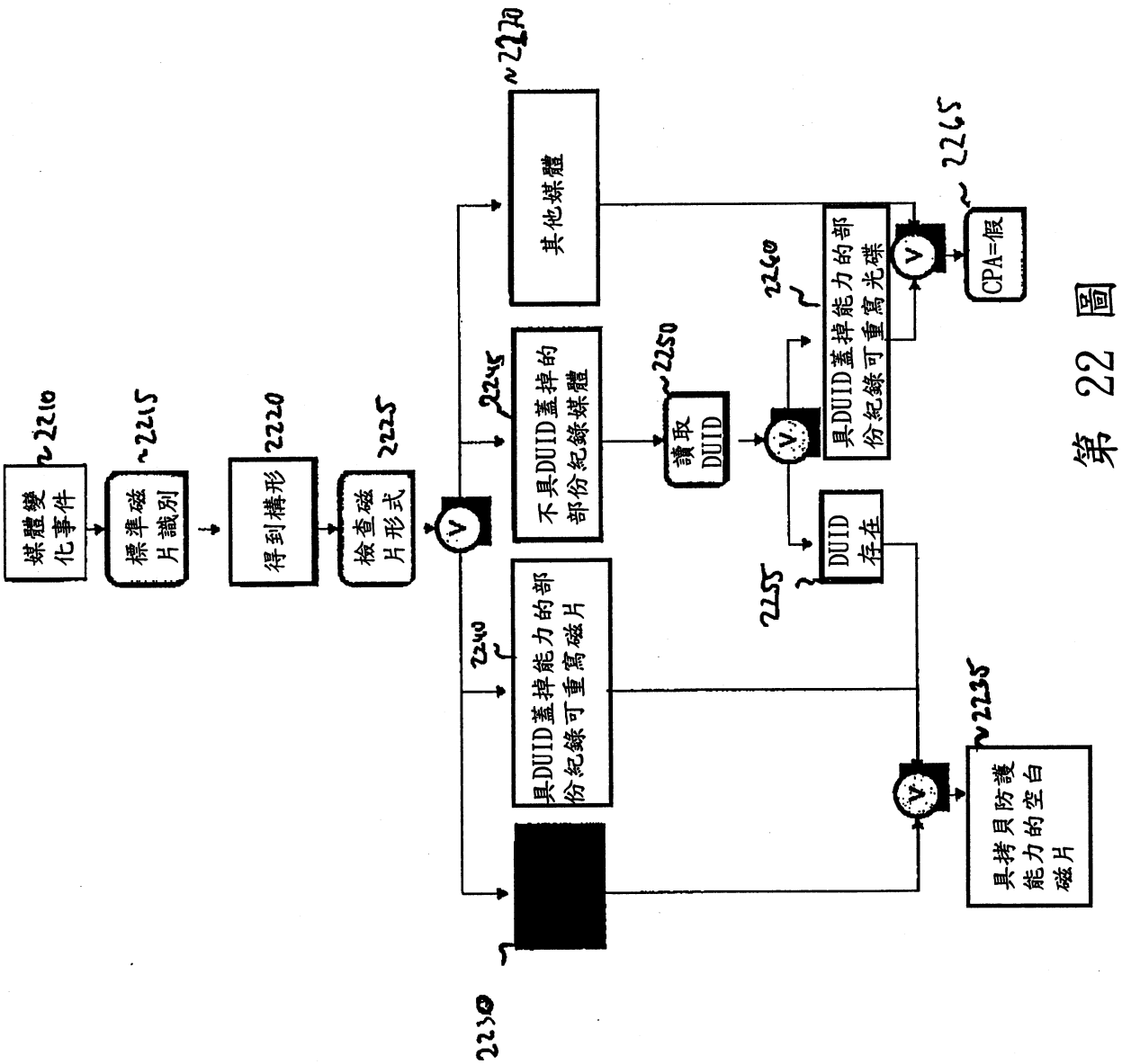
第 19 圖


SecurDisc特徵鈕子
2010
(不存在的SD特徵)
持續而不需SecurDisc功能性
2045
(使用拷貝防護、吸收紀錄)
創作計劃
2000
檢查拷貝防護
2025
(影像產生)
驅動器主機認證形式2
2030
(一般的寫入)
激勵媒體
2035
寫入SecurDisc媒體
2040
報告錯誤
2065
認證失敗
驅動器主機認證形式1
2050
(CPA真)
驅動器主機認證形式2
2055
(CPA假)
檢查CPA標誌
2045
(該計劃具經啟動的拷貝防護)
檢查CPA標誌
2040
CPA標誌關

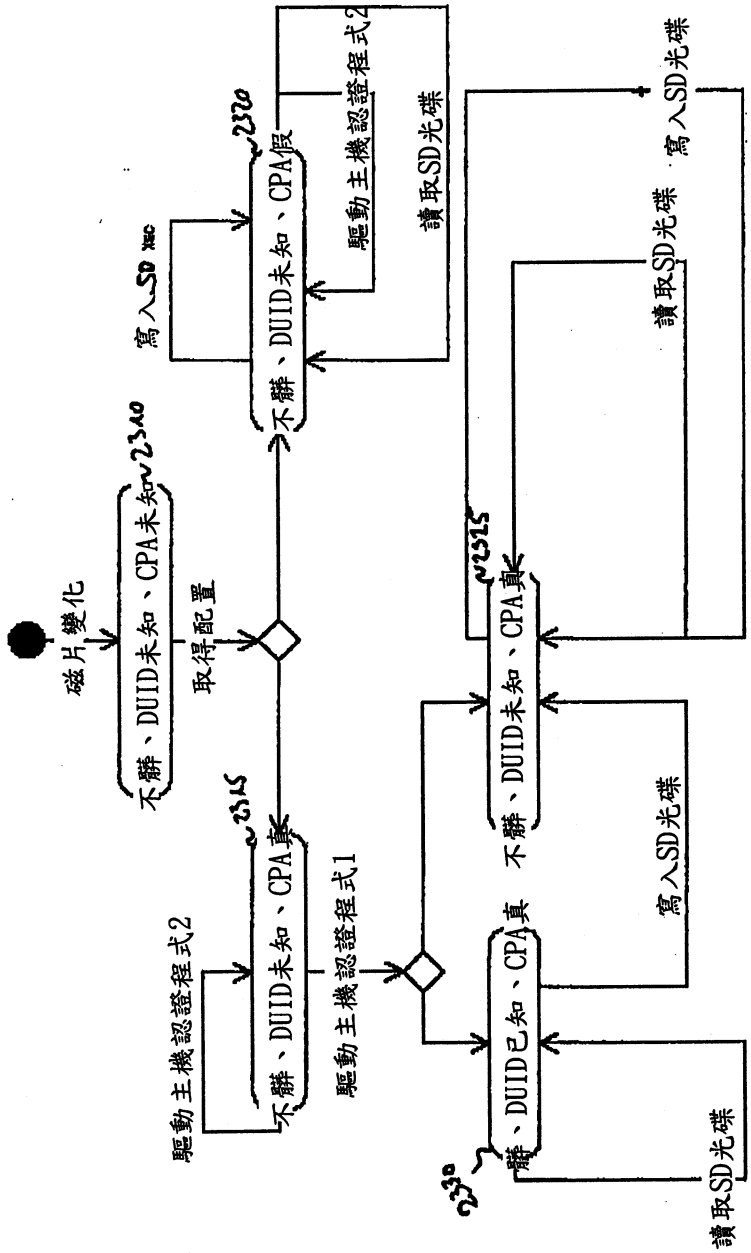
第 20 圖

CP標誌	PP標誌	密鑰成分	敘述
關	關	-	未加密的檔案片段
開	關	磁片獨特ID、 認證授與密鑰	利用磁片獨特ID和認證授與密碼加密的檔案片段
關	開	密碼短語標誌、 認證授與密碼	利用密碼短語標誌和認證授與密碼加密的檔案片段
開	開	磁片獨特ID、 密碼短語標誌、 認證授與密碼	利用認症授與密碼、密碼短語標誌和磁片獨特ID構成內容存取密鑰加密的檔案片段(見下圖)

第 21 圖


媒體變化事件
2210
標準磁片識別
2215
得到構形
2220
檢查磁片形式
2225
2230
具DUID蓋掉能力的部份紀錄可重寫磁片
2240
不具DUID蓋掉的部份紀錄媒體
2245
其他媒體
2270
讀取DUID
2250
DUID存在
2255
具DUID蓋掉能力的部份紀錄可重寫光碟
2260
CPA=假
2265
具拷貝防護能力的空白磁片
2235

第 22 圖


磁片變化
不驊、DUID未知、CPA未知
2340
取得配置
驅動主機認證程式2
不驊、DUID未知、CPA真
2345
驅動主機認證程式1
寫入SD光碟
不驊、DUID未知、CPA假
2370
驅動主機認證程式2
讀取SD光碟
驊、DUID已知、CPA真
2330
讀取SD光碟
寫入SD光碟
不驊、DUID未知、CPA真
2315
讀取SD光碟
寫入SD光碟

第 23 圖

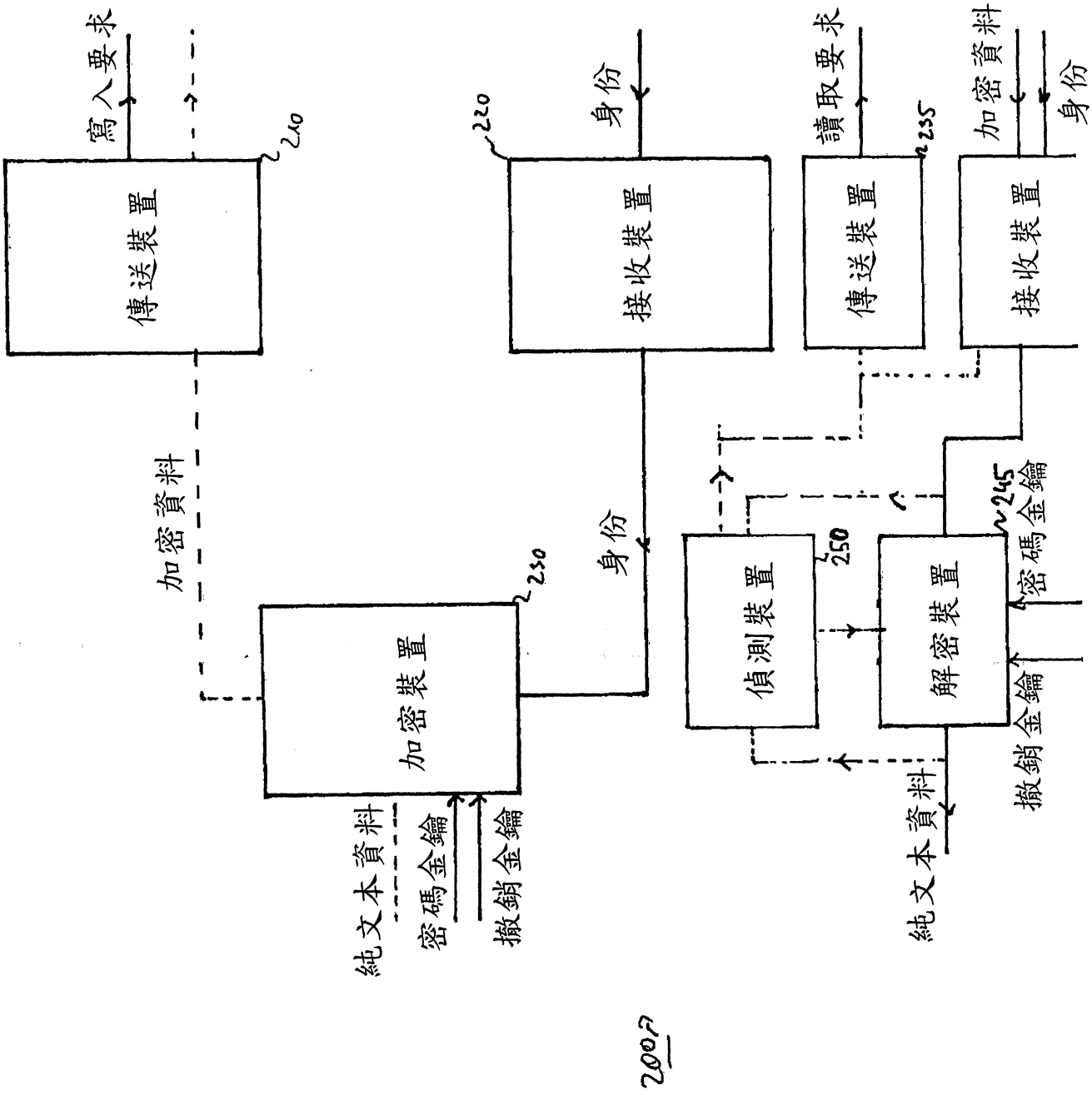
七、指定代表圖：

(一)本案指定代表圖為：第（ 1a ）圖。

(二)本代表圖之元件符號簡單說明:

100	寫入設備
110	接收裝置
120	產生裝置
130	提供裝置
140	儲存裝置
ID	身份

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：


寫入要求
傳送裝置
240
加密資料
加密裝置
230
純文本資料
密碼金鑰
撤銷金鑰
身份
220
接收裝置
身份
偵測裝置
250
讀取要求
傳送裝置
235
加密資料
接收裝置
身份
解密裝置
245
密碼金鑰
撤銷金鑰
純文本資料
2002

第 3b 圖