

發明專利說明書

公告本

(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：95138741

※ 申請日期：95.10.20

※IPC 分類：H0XN 7/167

(2006.01)

一、發明名稱：(中文/英文)

拌碼加密內容之存取控制方法

METHOD FOR ACCESS CONTROL TO A SCRAMBLED CONTENT

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

薇瑟斯公司 / VIACCESS

代表人：(中文/英文)

克里斯汀 毛瑞-派寧斯 / CHRISTINE, MAURY-PANIS

住居所或營業所地址：(中文/英文)

法國巴黎德芬斯希德克斯·杜爾歐普拉 C·柯林斯亞契

Les Collines de l' Arche, Tour Opera C , 92057 PARIS LA DEFENSE CEDEX,

FRANCE

國 籍：(中文/英文)

法國 / FRANCE

三、發明人：(共 3 人)

姓 名：(中文/英文)

1. 雀凡利爾 安東尼 / CHEVALLIER, ANTHONY

2. 蘭凡奇 史蒂芬 / LANFRANCHI, STEPHANE

3. 馬吉斯 爾文 / MAGIS, ERWANN

國 籍：(中文/英文)

1. 法國 / FRANCE

2. 法國 / FRANCE

3. 法國 / FRANCE

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：。

☒ 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. 法國、 2005/12/13、 0553852

2. 法國、 2006/03/31、 0651130

☐ 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。

五、中文發明摘要：

本發明是關於一種用於對分配給一組被安裝的接收終端機的一數位拌碼內容之存取控制的方法，該組被安裝的接收終端機包含一主終端機及與該主終端機相依的至少一從屬終端機，在該方法中，透過一點至點鏈結，該從屬終端機經常性地或偶爾將與該存取情況有關的資訊中的至少一項返回給該主終端機，以使該主終端機能夠控制該從屬終端機對該內容之存取。

六、英文發明摘要：

The invention relates to a method for access control to a digital scrambled content distributed to a set of installed reception terminals comprising one master terminal and at least one slave terminal dependent on said master terminal, method in which the slave terminal systematically or occasionally returns at least one item of information about said access condition to the master terminal through a point-to-point link, to enable said master terminal to control access of said slave terminal to the content.

七、指定代表圖：

(一)本案指定代表圖為：第 (8) 圖。

(二)本代表圖之元件符號簡單說明：

100...操作者	109...智慧卡
102...主終端機	110...內容
104...從屬終端機	111...本地記憶體
105...內容	112...內容
106...從屬終端機	115...鏈結
107...內容	120...本地記憶體
108...從屬終端機	

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

發明領域

本發明是關於內容之分配的領域，且本發明尤其是關於一種對一操作者提供給一接收終端機的被拌碼內容之存取控制的方法，一存取管理單元與該接收終端機連接，該接收終端機被提供至少一存取控制模組，該方法包含以下步驟：

-將一存取情況(access condition)與該內容連接，該存取情況包含用於解拌碼該內容所必需的多數個資訊，

-將具有該存取情況的內容發送給該終端機。

本發明也是關於一存取控制系統，該存取控制系統包括一包含一拌碼內容伺服器的發射裝置，與該裝置連接的一存取管理單元、被提供至少一存取控制模組的一接收終端機，該伺服器所提供的該拌碼內容，且與該拌碼內容連接的一存取情況包含解拌碼該內容所需的多數個資訊。

本發明也是關於一電腦程式，該電腦程式包含儲存在該終端機內的一第一處理模組，該第一處理模組與儲存在該存取管理單元內的一第二處理模組一起運作，該程式被設計以實現與本發明一致的存取控制方法。

當該拌碼的數位內容被分配給一組被安裝接收終端機時，本發明也是可應用的，該組被安裝接收終端機包含一主終端機及多數個與該主終端機相依的從屬終端機，該主終端機充當一存取管理單元。

【先前技術】

發明背景

在一多點發送廣播內文中，有效地對一些盜版形式反應是困難的，例如存取內容所需的權利或金鑰之欺騙產生，或者嘗試阻止接收系統考慮操作者所發送的計數測量
5 訊息。

然後此情況意味，當所有用戶改變其信號時，該操作者需要對該接收系統作出修改，因此該信號不再被盜版裝置使用。因此，需作出的修改必須充分地隨之而來，且其
10 等的配置是一困難且昂貴的運作。

此等不利特別與以下事實有關：已知存取控制系統一般具有沒有返回路徑的架構。在此類型的架構中，該終端機獨立於網路標頭運作。因此，一旦該內容已被提供給用戶，則該操作者不再具有即時控制目標用戶之權利的任何
15 裝置，因為所有存取控制在該接收終端機內完成。

一種欺詐地使用該數位內容之形式由使用相同安全處理器(一般是一有效智慧卡)組成，透過幾個終端機，以處理幾個ECM通道。在此情況下，一個單一用戶被相同卡的幾個有效使用者的操作者所知。

20 此種形式的欺詐使有關的解碼器存取許多不同的程式，不同程式之數目等於實際上存在該共用卡內的權利之數目，多達至控制字重新更新期間的該卡可處理的ECMs之數目。幾個解碼器對該用戶卡的欺詐性使用被完成，而不用操作者之任何控制，該操作者不能阻止其或者甚至限

制其。

當一用戶具有幾個資料接收及/或拌碼服務終端機時，另一問題產生。除非一特定用戶之終端機被認為是與此用戶之“複本”之對應數目相關聯的獨立終端機，該操作者不具有他藉以可控制不同用戶終端機之相依存取權利或公共權利之分配的任何簡單解決方法。

本發明之目的是克服此等缺點。

更特別地，本發明之目的是在該系統之輸入端及輸出端分配存取控制運作，換句話說，在該操作者處被安裝的第一設備(其運作在該操作者之直接控制下)與第二接收終端(利用該存取控制模組，對用戶權利執行檢查)之間。在存取控制處理期間，此分配可從該操作者中限制或甚至去除該終端機之自治性。

本發明之另一目的是考慮該接收終端機可在其內具有低處理功率的配置。此可能是移動終端機被用作接收終端機(行動電話、PDA、可攜式電腦等)的情況，具有按照能量及處理功率的限制自治性。

本發明之另一目的是對操作者提供一種簡單的解決方案，用於控制相依存取權利或者對屬於相同用戶的不同終端機共用的存取權利之分配。

本發明在該終端機被提供實體存取控制模組(一般是一智慧卡)的習知情況中是可應用的，但是當存取控制模組不是一實體模組，而是以一安全方式較佳地被儲存在該終端機之一記憶體內的軟體模組時，其更可有利地被應用。

【發明內容】

發明概要

本發明建議一種方法，用於存取控制由一操作者提供給一接收終端機的拌碼內容，一存取管理單元與該接收終端機連接，該終端機被提供至少一存取控制模組，該方法包含以下步驟：

a-將一存取情況與該內容連接，該存取情況包含用於解拌碼該內容所必需的多數個資訊；

b-將具有該存取情況的內容發送給該終端機；
根據本發明，該方法也包含以下步驟：

當該終端機接收該存取情況時，

c-透過一點至點鏈結，經常性(systematically)或偶爾將來自該終端機的與該存取情況有關的資訊中的至少一項發送給該存取管理單元，

d-該存取管理單元處理該資訊，以根據該處理之結果，致能或阻止該接收終端機對該內容之使用。

因此，當該接收終端機透過該點至點鏈結建立與該存取管理單元的通訊時，此點至點鏈結控制該終端機之權利以存取該被請求的內容，且根據此檢查之結果致能或阻止該終端機對該內容之使用。在本發明之一較佳實施例中，被該存取管理單元接收的資訊之處理包括一第一步驟及一第二步驟，該第一步驟由以下組成：檢查此資訊是否與儲存在該終端機內的存取資料相容，且該第二步驟由以下組成：傳送至少一控制參數給該終端機，以第一步驟之結果

的函數致能或阻止內容之使用。

利用依據本發明的方法，存取控制不再唯一地在該接收終端機內被執行。此增強了該內容之保護。

較佳地，當該終端機接收該存取情況時，利用先前儲
5 存在該接收終端機內的存取資料，該存取控制模組驗證該被接收的存取情況是否被滿足。

在一可變實施例中，該終端機將與該存取情況有關的該資訊之部分或所有發送給該存取管理單元，只要該被接收的存取情況不被滿足。

10 在一可變實施例中，該終端機經常性地發送該資訊，獨立於該存取控制模組執行的檢查之結果。此第二可變實施例是特別地有利，當存取控制實質上在該操作者內被管理以改進該內容保護系統之安全，而沒有增加該終端機內的安全機制之數目，或者減少它們。

15 在本發明之較佳實施例中，在該操作者定義的一時間階段內，在處理該存取管理單元接收的資訊內的第一步驟及該接收終端機對該存取情況之檢查經常性地或偶爾地獨立於彼此執行。

因此，該操作者能夠對該操作者及該接收終端機之間
20 的該存取控制之空間及時間分配作出一良好調變。

較佳地，該操作者所定義的時間階段不可在該接收終端機內被預測。

在本發明之第一應用中，該存取情況在一ECM訊息內被傳送給該終端機，該ECM訊息包含至少一存取準則CA，

被一金鑰 K_{ecm} 加密的一被加密控制字 CW 之一密碼 $CW * K_{ecm}$ 。在此應用中，儲存在該終端機內的存取資料包括該內容之存取權利及至少一解密金鑰。

該方法內的步驟c)由以下組成：若該存取控制模組不具有解密該密碼 $CW * K_{ecm}$ 的金鑰 K_{ecm} ，將來自該終端機的至少該密碼 $CW * K_{ecm}$ 發送給該存取管理單元。然後被該存取管理單元發送給該終端機的參數是利用該金鑰 K_{ecm} 解密且被該終端機特定所知的金鑰 K_{ter} 重新加密的一控制字 CW 。

在一第二應用中，該方法被用以控制重新使用一內容的權利。在此情況下，該存取管理單元發送給該終端機的參數是一將被儲存在具有該內容的終端機內的 ECM_R 訊息，且包括被用以檢查該內容之向後讀取的存取準則。

在一第三應用中，該方法也可被用以控制被一DRM許可證保護的內容之存取。

在此情況下，該終端機發送給該存取管理單元的資訊是該DRM許可證。

依據本發明的系統之特徵在於：該接收終端機透過一點至點鏈結連接到該存取管理單元，該存取控制模組透過該點至點鏈結經常性地或偶爾將與該存取情況有關的資訊中的至少一項返回給該存取管理單元，以使該存取管理單元能夠處理該資訊，並根據該存取管理單元所執行的處理之結果，致能或阻止該接收終端機對該內容之使用。

該系統內的該存取管理單元包括：用以驗證自該存取控制模組接收的該資訊是否與儲存在該終端機內的存取資

料相容的裝置，以及用以產生及傳送至少一控制參數給該終端機的裝置，以致能或阻止該內容之使用，以該驗證之結果的函數。

本發明也是關於一種接收終端機，用於與一存取管理
5 單元連接的一內容分配裝置所分配的一拌碼內容相關。

該終端機包括至少一存取控制模組，該存取控制模組透過一點至點鏈結與該存取管理單元進行通訊。

本發明也是關於一種被設計成實現一存取控制方法的電腦程式，在包含一存取控制模組的一接收終端機內，該
10 存取控制方法控制對一操作者所提供的一拌碼內容之存取，一存取管理單元與該操作者連接。

該程式包括儲存在該終端機內的一第一模組，該第一模組包含：用以透過一點至點鏈結，經常性地或偶爾地將來自該終端機的該存取情況之資訊的至少一項轉發給該存
15 取管理單元，該第一模組與儲存在該存取控制管理單元內的第二模組一起運作，該第二模組包含用以處理該資訊的指令，以及根據該處理之結果，致能或阻止該接收終端機對該內容之使用的指令。

依據本發明的方法也應用於一存取控制系統，該存取
20 控制系統包含一包含一內容伺服器的發射裝置、一主終端機、與該主終端機相依的一從屬終端機，該內容伺服器包含用以分配與一存取情況連接的一拌碼數位內容給該終端機的裝置，該存取情況包含解拌碼該內容所需的多數個資訊。

該系統其特徵在於以下事實：該從屬終端機可透過一

點至點鏈結連接到該主終端機，該從屬終端機透過該點至點鏈結將自該被接收的存取情況中取出的資訊中的至少一項返回給該終端機，以使該主終端機能夠處理該資訊，以致能或禁能該從屬終端機對該內容之使用。

5 為了獲得此目的，該主終端機包括：

-用以驗證自該從屬終端機接收的資訊是否與先前被分配給該從屬終端機的存取權利相容的裝置，以及

-用以產生及傳送至少一控制參數給該從屬終端機的裝置，以致能或阻止該內容之使用，取決於該驗證之結果。

10 該主終端機可被整合到該發射裝置，或整合到一收集接收天線。

在所有情況下，該主終端機包括能夠處理該從屬終端機所傳送的資訊之軟體，以致能或阻止該從屬終端機對該內容之使用。

15 在此架構中，該方法包括以下預備步驟：

-將一存取情況與該內容連接，該存取情況包含用於解拌碼該內容所必需的多數個資訊，

-分配一公共對話金鑰 K_s 給該主終端機及該從屬終端機，

-傳送一資料串流給包含該拌碼數位內容及該存取情

20 況的該等終端機，

-當接收到該資料串流時，該從屬終端機自該被接收的資料串流中取出該存取情況，透過與該主終端機建立的一點至點鏈結，經常性地或偶爾將與該存取情況有關的資訊中的至少一項返回給該主終端機，

-且當接收該從屬終端機轉發的該資訊時，該主終端機驗證該資訊是否與先前被分配給該從屬終端機的存取權利相容，且將被該對話金鑰 K_s 加密的至少一指令參數返回給此從屬終端機，若該資訊與該等存取權利相容，則授權該內容之使用，或者若該資訊與該等存取權利不一致，則阻止該內容之使用。

因此，藉由控制該對話金鑰 K_s 對一主終端機及該相關從屬終端機之分配，本發明使該操作者能夠控制一主終端機及從屬終端機之間的連接。因此，該操作者可使用該主終端機控制該從屬終端機對一內容之存取。

藉由傳送來自該從屬終端機的權利控制函數給該主終端機，在幾個不具有一安全處理器的輔助終端機內使用數位內容也是可行的，且在該安全處理器上，該製造商避免了一讀卡器之需要。此最小化與一主終端機連接的被安裝輔助終端機之成本。當有許多被安裝的終端機時(旅館或醫院等)，此優點是特別地有利。

在一可變實施例中，該主終端機不具有一智慧卡，而是僅僅執行被安裝從屬終端機與該操作者連接的該存取管理單元之間的一閘道功能。在此情況下，該主終端機經常性地要求(call upon)與該操作者連接的該存取管理單元，以處理來自一從屬終端機的存取請求。

在另一可變實施例中，該主終端機被提供一智慧卡，只是偶爾使用。

在此情況下，當該主終端機不使用一智慧卡時，該主

終端機要求該管理單元，以處理來自一從屬終端機的一存取請求。

如在先前的例子中，若該主終端機不利用該智慧卡執行該處理時，該主終端機所能做的是作為該被安裝從屬終端機與該操作者連接的該存取管理單元之間的一閘道。

當該方法被用於一條件存取系統(CAS)時，該存取情況在一ECM訊息內被發送，該ECM訊息包含至少一存取準則CA及一被用以加密該內容的一控制字CW之一密碼 $CW *_{K_{ecm}}$ 。

當接收該存取情況時，該從屬終端機將至少該密碼 $CW *_{K_{ecm}}$ 返回給該主終端機，且一般地為該存取準則CA。

在驗證該從屬終端機之該等權利之後，若該從屬終端機被授權使用該內容，則該主終端機將利用該金鑰 K_{ecm} 解密且利用該對話金鑰 K_s 重新加密的控制字CW發送給該從屬終端機。

在另一可變實施例中，該主終端機發送給該從屬終端機的參數是一 ECM_R 訊息，該 ECM_R 訊息將與該內容保存，且包括將被用於控制該內容之重複使用的存取準則。

當該被分配的內容被一DRM許可證保護時，被該從屬終端機返回給該主終端機的資訊是該DRM許可證(license)。

在兩個應用中(CAS及DRM)，依據本發明的方法被一電腦程式使用，該電腦程式包含一儲存在該從屬終端機內的第一模組，該第一模組包含用以從該被接收的資料串流中取出該存取情況的指令，及透過與該主終端機建立的點

- 至點鏈結，用以將與該存取情況有關的資訊中的至少一項返回給該主終端機的指令，該第一模組與儲存在該主終端機內的一第二模組一起運作，該第二模組包含用以處理該資訊的指令，及用以致能或阻止該從屬終端機對該內容之
- 5 使用的指令，取決於該處理之結果。

圖式簡單說明

本發明之其他特徵及優點從以下作為非限制例子給出的描述中將變得清楚，參看該等附圖，其中：

- 第1圖顯示了依據本發明之一存取控制系統的總方案；
- 10 第2圖示意性地顯示了第1圖中的該系統之一第一例子；
- 第3圖是描述了依據本發明之方法的特定應用之方塊圖；
- 第4-6圖表示描述了依據本發明之該方法的時間階段的時序圖；

- 第7圖是描述了依據本發明之方法的一實施例的該等
- 15 步驟之流程圖；

第8圖示意性地描述了依據本發明之方法的一第二應用，其中該存取控制由一主終端機管理，幾個從屬終端機與該主終端機連接；

- 第9圖示意性地描述了用於授權一從屬終端機使用該
- 20 數位內容的控制程序。

【實施方式】

較佳實施例之詳細說明

我們現在描述以下發明，藉由該方法之一特定應用的裝置，來控制存取程式或將多媒體內容傳送到具有存取權

利的用戶。

在以下描述中，相同的參考將被用於不同的圖示，以表示執行相同或等效功能的元件。注意到，本方法可被用於任何已連接且具有一足夠高速返回通道的網路，例如，

5 一DSL(數位用戶線)有線網路，或者該Wi-Fi或Wi-Max(或ASFI-無線網際網路存取)之無線網路，或者一3G移動類型。

第1圖描述了依據本發明的方法可在其內被使用的內容分配系統之概略圖。

該系統包括與一存取管理單元4及一接收終端機6連接

10 的發射裝置2。

該發射裝置2包括一內容伺服器8，該內容伺服器8透過一傳輸網路7將拌碼內容分配給該終端機6，例如透過一有線網路或一無線電廣播網路；或者透過一DSL線，且該終端機6包括一存取控制模組10，該存取控制模組10可是一智慧卡，或者較佳的是一執行控制功能的軟體模組。

15

該終端機6透過一雙向點至點鏈結12，連接到該存取管理單元4。

參看第2圖，第2圖示意性地描述了第1圖中的一系統之特定例子，該接收終端機6是一安裝在該用戶端的數位解碼器，且該操作者與用戶之間的鏈結透過一DSL線實現，經過一包含一DSLAM(數位用戶線存取多工器)15的中間設備14，該DSLAM 15與一存取管理單元4(UGA)進行通訊。此UGA被整合到該設備14。

20

注意到該存取管理單元4可被安裝到被信任的第三

方，該第三方在該操作者之監督下，具有控制用戶之權利的功能，而沒有超出本發明之架構。

該發射裝置2包括一ECM-G(用於權利控制訊息產生器)模組16、一SAS模組18(用戶授權系統)，以及一MUX多工器20，該模組16將計算且廣播作業訊息ECM，且該SAS模組18被設計以計算且廣播為了實現以下目的所需的EMM(權利管理訊息)訊息：發送權利及金鑰給用戶，該MUX多工器20將形成自程式及/或該操作者提供的服務開始的內容之封包。

例如，該終端機6可由一多媒體內容解碼器/解拌碼器組成，在先前技術中被稱為轉頻器(STB)。其被提供一安全處理器10，該安全處理器10被特別設計，以處理內容的存取控制及權利及密碼(金鑰)的管理。此一安全處理器之一眾所周知的例子是連接到該終端機的智慧卡。該安全處理器10之另一例子也可由被整合到該終端機的專用軟體功能實現。

現在參看第3-7圖，描述依據本發明的方法。

被提供的內容代表以拌碼形式的多媒體程式廣播是以一控制字CW表示。

該終端機6被提供一金鑰 K_{Diff} (為該操作者所採用的終端機所共用)、一被指定給此終端機的金鑰 K_{Ter} 及一權利 D_{Oper} 。此等金鑰及此權利先前一般被一EMM訊息被載入該安全處理器。此外，若該用戶執行一非法動作，則該安全處理器包含一欺詐要求權利 D_{Fraud} 。

該存取管理單元4已具有金鑰 K_{Oper} 、每個終端機之金鑰

K_{Ter} ，且知道每一終端機擁有哪一權利 D_{Oper} 。

參看第3圖，該存取情況在該發射裝置2之該ECM-G 16所產生的一ECM訊息內被發送給終端機(箭頭22)。該ECM訊息包括一存取準則 CA_{Oper} 及由一金鑰 K_{ecm} 加密的該控制字CW之密碼 CW^*_{kecm} 。該金鑰 K_{ecm} 是只為該操作者所知的金鑰 K_{Oper} ，或者是為所有操作者之終端機所知的金鑰 K_{Diff} 。因此若該終端機具有至少滿足存取準則 CA_{Oper} 的權利 D_{Oper} ，及被用以藉由解密該密碼 CW^*_{kecm} 而獲得控制字CW的金鑰 K_{ecm} ，則存取該ECM連接的程式是可行的，若金鑰 K_{ecm} 是金鑰 K_{Diff} ，則就是以上情況。

當接收程式時，該終端機6將該被接收的ECM返回(箭頭24)給該存取管理單元4。

在該方法之第一可變實施例中，該操作者想要經常性地(systematically)利用該終端機控制該內容之解拌碼，該金鑰 K_{ecm} 是沒有被發送給該終端機6的金鑰 K_{Oper} 。在此情況下，該終端機經常性地將該ECM返回給該存取管理單元4。

在另一可變實施例中，對內容之解拌碼的控制在該終端機與該操作者之間被共用，在該模組10已對該存取準則作出先前檢查時，該終端機偶爾將該ECM發送給該存取管理單元4。

在此變化中，該終端機返回該ECM，若(例如)，該用戶沒有讓驗證存取準則成為可能的權利 D_{Oper} 時，或者若該終端機沒有該密碼 CW^*_{kecm} 之解密金鑰 K_{ecm} 時。另一方面，若該終端機沒有滿足該存取準則的權利，以及若該密碼

CW^*_{kecm} 可利用該金鑰 K_{Diff} 被解密，則該終端機如先前技術中之方式存取該程式。

當該存取管理單元4接收來自該終端機6的ECM時，其驗證該終端機6是否具有存取該等被接收程式所需的該等
5 權利。

在一第一實施例中，該存取管理單元具有一資料庫，其中該操作者發送給該用戶終端機的權利之描述已被儲存在該資料庫內。因此，該存取管理單元對該用戶正式具有的權利檢查該存取準則。此模式不能對用戶欺詐性地載入
10 其終端機內的非法權利檢查存取準則。

在一第二實施例中，該存取管理單元具有該終端機之該安全處理器之內容的遠端讀取，且對實際存在該終端機內的該等權利檢查存取準則。此模式去除了該存取管理單元支援所有用戶之權利的一資料庫之需求，且也使以下變
15 得可行：藉由檢查校驗求和或另一類似的方式，檢查安全處理器之內容。

當該存取管理單元對該終端機之該等權利所作出的檢查成功時，該存取管理單元將一控制參數返回給該終端機，使能夠對該內容之存取。

20 否則，其沒有將此參數返回給該終端機，從而阻止了對該內容之存取。

當該存取準則實際上可被該存取管理單元4滿足時，該存取管理單元4利用該金鑰 K_{ecm} 解碼該密碼 CW^*_{kecm} ，利用該終端機特定所知的 K_{ter} 重新加密(recrypt)該控制字CW，因

此將該重新被加密的控制字之密碼 $CW^*_{K_{ter}}$ 返回給該終端機(箭頭26)。當利用依據現有技術及該方法之外的任何認證方法建立點至點鏈結12時，該金鑰 K_{ter} 被決定為該存取管理單元所給出的該終端機之識別的函數。

5 在該方法之一特別可變實施例中，該終端機將從該ECM取出的密碼 CW^*_{kecm} 只發送該存取管理單元。在此情況下，該存取管理單元4考慮以下情況：該存取準則總是明確被滿足，且只實施該控制字 CW 之解密/重新加密。因此，透過使用特定金鑰 K_{Ter} ，該操作者繼續控制該終端機的解拌碼。

10 依據本發明之一有利特徵，該接收終端機6之存取控制模組10對該存取準則的檢查及該存取管理單元4的該ECM之處理被執行，彼此獨立於該操作者所定義的時間階段(time phasing)。

該時間階段將參看第4至6圖在以下被描述。

15 如以上所描述，該終端機6一般被提供如下參數：

-表示 K_{ecm} 之一實例的 K_{Diff} ，使其當該ECM傳輸該密碼 $CW^*_{K_{Diff}}$ 時能夠獲得該 CW 。該金鑰為一組終端機共用。

-該終端機6專用的金鑰 K_{Ter} ，被用以獲得該控制字 CW ，起始於該存取管理單元4發送給該終端機的密碼

20 $CW^*_{K_{Ter}}$ 。

-一自該存取管理單元4正式接收的存取證書， D_{oper} ，該存取管理單元4知道該存取證書存在該終端機6內。

-該終端使用者欺詐性地獲得的存取證書 D_{Fraud} 。因此，該存取管理單元4不知道該終端機持有該存取證書。

該存取管理單元4一般具有：

-該金鑰 K_{Oper} 表示 K_{ecm} 之另一實例，使當該ECM傳輸該密碼 $CW^*_{K_{Oper}}$ 時，能夠獲得該控制字 CW 。此金鑰只為該存取管理單元4所知。

5 -為被考慮的終端機6專用的金鑰 K_{Ter} ，被用於以一密碼 $CW^*_{K_{Ter}}$ 之形式提供該控制字 CW 給此終端機6。

-該存取管理單元4正式發送給該終端機6的存取證書 D_{Oper} 。

10 為了描述不同的情況，三個特別的值對該存取情況 CA 而定義：

- CA_{Oper} ：此情況被滿足於該終端機合法持有該權利 D_{Oper} 。

- CA_{Fraud} ：此情況被滿足於該終端機欺詐性地持有一權利 D_{Fraud} ；

15 - CA_{Autre} ：此情況不被滿足於不持有任何對應權利的一終端機。

階段A、B及C描述了在存取該程式時，該終端機對該存取情況之檢查的時間階段之影響。

20 在A內：該ECM被該終端機6發送給該存取管理單元4，因為該終端機沒有檢查該ECM，或者因為其發現滿足該存取情況的一權利，但是該控制字被該終端機不具有的金鑰 K_{Oper} 加密。該程式可在此期間內被存取，因為該存取管理單元4觀察出該存取情況被滿足。該存取管理單元4將利用該終端機之金鑰加密的控制字之該密碼 $CW^*_{K_{Ter}}$ 發送給

該終端機。

在B內：該ECM被返回給該存取管理單元4，因為該終端機6不控制該ECM，或者因為該終端機6發現滿足該存取情況的一非法權利，而其沒有該金鑰 K_{Oper} 。在此期間，對該程式的存取是禁止的，因為該存取管理單元4觀察出，該終端機6之正式權利不滿足此存取情況。該存取管理單元4沒有發送該控制字CW之一密碼。

在C內：該ECM沒有被發送給該存取管理單元4，因為該終端機具有被用以解密該密碼 $CW^*_{K_{ecm}}$ 的金鑰 K_{Diff} 。若該終端機在其必須控制該存取準則的時間階段(C1)內，則對該程式沒有存取，因為該終端機內可用的權利不滿足該存取準則 CA_{Autre} 。若該終端機在時間階段沒有控制該存取準則(C2)，則該程式只可藉由該控制字之解密被存取。很明顯，當該方法被使用時，後一情況C2必須被避免，例如，若該密碼 $CW^*_{K_{ecm}}$ 可被該終端機解密，則藉由使該存取準則之控制獨立於該時間階段。

階段D及E描述了在存取該程式時，存取管理單元4對該存取情況之檢查的時間階段之影響。

在D內：該程式被存取，因為該存取管理單元4沒有檢查該存取情況，且預設視其被滿足，或者因為該存取管理單元4檢查該存取情況，且發現其被滿足。

在E內：該程式被存取，因為該存取管理單元4沒有驗證該存取情況，且預設視其被滿足，而該終端機6使用一非法權利。

階段K至P描述了在存取該程式時，該終端機和存取管理單元4對程式之聯合(joint)存取之情況之檢查的時間階段之影響。

5 在K內：該程式之存取被授權，因為該存取情況被顯示為終端機6及/或該存取管理單元4滿足，且可能被此兩模組中的唯一一者評估預設滿足。

在L內：該程式之存取被致能，因為該存取情況被觀察出，為該終端機6及該存取管理單元4預設滿足。此兩決策符合該存取情況/正式權利組合。

10 在M內：該程式之存取被授權，因為該存取情況實際上可被觀察出為該終端機6所滿足，且被觀察出為該存取管理單元4預設滿足。在此情況下，該存取管理單元4沒有偵測出該終端機6正使用一非法權利。

15 在N內：沒有對該程式的存取，因為該存取情況被觀察出不被該存取管理單元4所滿足，該存取管理單元4不知道該終端機6正使用的非法權利。

在此情況之第一部分內，該存取管理單元4偵測出該終端機6具有一非法權利，若該終端機6對該存取管理單元4指出其具有一有效權利。

20 在O內：該程式之存取被授權，因為該存取情況被認為被該終端機6及該存取管理單元4預設滿足。

在P內：該ECM沒有被發送給該存取管理單元4，因為該終端機具有被用以估計該控制字CW的金鑰 K_{Diff} 。該存取管理單元的控制是無效的。此階段與以上所描述的階段C

類似，且當該終端機沒有處於控制之中時，它必須受益於相同特定實現以避免對該程式之存取。

現在參看第7圖，其描述依據本發明的方法內的步驟。

在此第7圖中，左部分所表示的該等步驟對應該終端機
5 6所執行的處理，且右部分所顯示的步驟對應該存取管理單元4所執行的處理。

當該用戶想要存取一程式時，該終端機6需要包含視訊、音訊及程式之其他成分的數位資料串流，以及該ECM訊息。

10 對每一被接收的ECM訊息(步驟30)，該終端機驗證其是否在需要控制該存取情況的週期內(步驟32)。在步驟32內執行的測試具體化在該終端機6內的方法之時間階段。若該終端機需執行此檢查(箭頭34)，則被包含在該ECM內的存取情況與出現在該終端機內的權利相比(步驟36)。

15 若沒有權利滿足該存取情況(箭頭38)，則對該ECM執行的處理被終止，沒有對該程式的存取，且該終端機6等待下一ECM訊息(步驟30)。若出現在該終端機的一權利滿足該存取條件(箭頭40)，則該終端機6驗證(步驟42)其是否具有能夠解密該控制字CW的金鑰 K_{ecm} 。此步驟具體化該操作
20 者之方法的動作。

若該終端機6具有金鑰 K_{ecm} (箭頭44)，則該終端機解密該控制字CW(步驟46)，且可藉由解拌碼而存取該程式(步驟48)。

否則，該終端機6將該ECM訊息發送給該存取管理單元4(步驟52)。

若該終端機6沒有在其需要控制該存取情況(箭頭54)的週期內，可設想兩情形：

-該終端機驗證(步驟42)該終端機是否可獲得該控制字CW本身，而沒有使用該存取管理單元4，

- 5 -或者該終端機經常性地將該ECM返回(步驟52)給該存取管理單元4。

在第一種情況下(如以上所描述)，若該驗證是正的，則該終端機解密(步驟46)該控制字CW。然後，該終端機6處理該存取控制。

- 10 在第二種情況下，該終端機6必須經常性地利用該存取管理單元4。在此情況下，若該存取管理單元4沒有檢查該存取情況，就沒有該程式的存取。

當該終端機發送(步驟52)一ECM給該存取管理單元4時，該存取管理單元檢查(步驟60)其是否在其必須檢查該

- 15 ECM之存取情況的期間內。

該步驟60具體化該存取管理單元4內該方法之時間階段。

若該存取管理單元4必須檢查該存取情況(步驟62)，則該存取管理單元4將此存取情況與該終端機6之該等權利比較(步驟64)。

- 20 如以上所描述，該存取管理單元4自用戶終端權利之其本身的資料庫開始作出此比較，而沒有明確地發送一查詢給該終端機6。在此處理中只有合法權利被考慮，以同意或拒絕對程式的存取。作為一變化，其也可藉由對該終端機之安全處理器作出一遠端查詢而執行此比較。在此情況

下，非法權利之存在可被偵測出，例如，藉由在此處理器內對被觀察的權利檢驗求和。

若該存取情況被滿足(箭頭66)，或者若該存取管理單元4不需要檢查該存取情況(箭頭68)，則該存取管理單元4解密該ECM之該控制字CW(步驟70)，加密該控制字CW(步驟72)，利用一該終端機6專用的一金鑰而獲得，且將獲得的密碼發送(步驟74)給該終端機6。此終端機利用其專用金鑰解密(步驟76)該控制字CW，且解拌碼(步驟48)該程式。

若該存取管理單元4認為該存取情況沒有被滿足(箭頭78)，則依據該終端機6之該等權利，該存取管理單元4不將解拌碼該程式所需的控制字CW提供給該終端機6。

在該等虛線所描述的該方法之一變化實施例中(箭頭80)，該終端機6已透過該ECM且在步驟52期間指定，該終端機6具有滿足該存取情況的一權利，然後該存取管理單元4將此資訊與其本身的推斷相關聯(步驟84)，且該存取管理單元4可偵測(箭頭86)出，該終端機6嘗試非法存取該內容，且對此一被嘗試的欺詐觸發(步驟88)一適當的處理。

依據本發明的方法也可被用於先前所獲得的一重新使用內容之內文內，例如，用於讀取或重新分配一被儲存的內容。

在此情況下，該存取管理單元4發送給該終端機6的參數是一需被儲存在具有該內容的終端機內的ECM_R訊息，且包含被設計成檢查該內容之重複使用(例如，讀取或重新分配)的存取準則。當讀取或重新使用該內容時，該ECM_R訊

息將依據該方法(取決於其組成)被處理，藉由呼叫該存取管理單元4，或者依據單一終端機的先前技術。

該方法也可被應用於加強一DRM系統內的存取控制。

在此情況下，一單一金鑰一般被需要用以未拌碼
5 (unscramble)整個內容。此金鑰獨立於該內容本身被提供，被封裝(encapsulated)在一指定給該目的接收系統的許可證中。

在此內文中，該被提出的方法藉由以一指定給上行串流(upstream)系統的方式建立許可證而被應用，使得該接收系統不可使用沒有利用該上行串流系統的許可證，然後該
10 上行串流系統能夠驗證該接收系統之權利，以存取被考慮的內容，然後若需要，以指定給該接收系統的方式重新產生該許可證。

第8圖示意性地描述了內容及/或在以下被指定為「內容」的服務之分配架構，其中一操作者100提供一拌碼的內容給一個單一實體內的一組終端機(102、104、106、108)，
15 例如一個單一家庭系列(包含幾個能夠使一用戶在幾個視聽接收器上顯示不同內容的終端機，以該操作者分配給此用戶之不同權利的函數)。

在第8圖所描述的例子中，該主終端機102及該從屬終端機被提供解調變裝置(DVB-S、DVB-C、DVB-T解調變器、IP數據機等)，該等解調變裝置適用於與其等連接的分配網路。在此例中進一步地，該主終端機102被提供一安全處理器(例如一智慧卡109)，且該等從屬終端機(104、106、
20 108)沒有一智慧卡，但是藉由連接到該主終端機102，他們

可存取該操作者之內容，該等從屬終端機可透過該主終端機102獲得該等內容之存取。

注意到，該用戶可以一習知的方式，利用該主終端機102存取該等內容。

5 該主終端機102及該從屬終端機104接收直接來自該操作者100的一拌碼內容(箭頭105)，該從屬終端機106透過該主終端機102接收(箭頭107)一內容，該從屬終端機108接收(箭頭110)儲存在該主終端機102之一本地記憶體111或者該從屬終端機106之一本地記憶體內的一內容(箭頭112)。

10 然而，注意到，一從屬終端機(104、106、108)可被提供一智慧卡，因此內容之存取控制可部分由該從屬終端機執行，且部分由該主終端機執行，利用如以上所描述的該操作者控制的時間階段。

第8圖所描述的架構也被應用於其他實體(例如，一家庭
15 庭間道或一聚集天線)，沒有超出本發明之框架。

在所有情況下，從屬終端機104、106及108各自具有與該主終端機102的一點至點鏈結(箭頭115)，且透過此點至點鏈結，將從與該內容有關的存取情況中取出的資訊返回給該主終端機102，以使一主終端機102能夠管理對該內容之
20 存取控制。

該架構也可被擴展到該等終端機之一級聯(cascade)類型組織。一從屬終端機可能是與其連接的其他從屬終端機的主終端機。此擴展能力提供了建立終端機之特定功能態樣的裝置。此一架構擴展之限制來自於終端機之多個級聯

所引入的響應時間。

在本發明之一較佳實施例中，該等從屬終端機被配置一安全電子晶片，該等從屬終端機可利用該安全電子晶片解密該主終端機所提供的該控制字之密碼。

5 在此情況下，藉由被插入該主終端機102的單個智慧卡與該等從屬終端機104、106及108中的每個內的電子晶片之聯合使用，獲得該等從屬終端機104、106及108中的一者對該內容之存取的改進安全性。在另一實施例中，此解密功能由該從屬終端機之一專用安全軟體模組完成。

10 此解決方案同樣良好地應用於直接廣播的內容，及被該主終端機102或另一從屬終端機106事先儲存的內容。

 該操作者可定義被授權的從屬終端機由來自其上行串流系統的該主終端機管理，從而引進一領域概念。因此，一未被授權的從屬終端機將不能夠解密自該主終端機輸出
15 的內容。

 在一較佳實施例中，藉由控制該對話金鑰(session key)之分配，該操作者控制被授權的從屬終端機與一主終端機運作，這將在之後被描述。

 作為一變化，藉由產生包含被授權或被禁止終端機之
20 識別符的一明確列表，該操作者也可限制要求一單一主終端機的從屬終端機之數目。在此情況下，一從屬終端機之控制取決於其對使用一與該主終端機建立的點至點鏈結之授權。然後，該操作者可選擇該列表中的被授權終端機之數目。

在所有情況下，只有被授權的從屬終端機接收與其等相連接的該主終端機相容的對話金鑰。

從該被授權的終端機之列表中去除一從屬終端機也由該操作者控制，一般藉由自從屬終端機之列表中去除一新

5 對話金鑰被發送給其的終端機。

《主》終端機對內容的接收及記錄

該主終端機對使用內容的存取，記錄或讀取該等內容

依據以上所描述的第1圖中的方法被控制，若該終端機具有

一及/或該操作者的存取管理單元4，則使用其智慧卡。當

10 該存取情況被接收時，透過該點至點鏈結12，該主終端機

102將與該存取情況有關的資訊中的至少一項返回給該存

取管理單元4。此存取管理單元處理該資訊，以允許或阻止

該主終端機102使用該內容。該主終端機對該等內容之處理

沒有被修改，因為從屬終端機可在其他各處請求。

15 另一方面，由於其作為主終端機的狀態，該主終端機

102具有一額外的功能，該主終端機102可藉由該額外的功

能被從屬終端機104、106、108要求(call upon)，以檢查其

等對內容之存取。也可提供此能力：傳送其所接收到(終端

機106)的內容或其已儲存(終端機108)的內容給從屬終端

20 機。藉由在該主終端機102內程式化資料串流/服務，此操

作由該操作者控制，該主終端機102可重新導向一(或所有)

從屬終端機104、106或108。

從屬終端機對內容的使用

一從屬終端機接收直接(終端機104)來自該上行串流來

源的內容/服務，例如，透過一衛星鏈結，透過(終端機106)該主終端機，或者在其等已被儲存(終端機108)在另一主或從屬終端機上。

當接收該內容及有關的存取情況(ECM)時，該從屬終端機104、106或108透過通訊通道115連接到該主終端機102，且其發送該ECM訊息給該主終端機102以處理。因為被該從屬終端機104、106及108發送給該主終端機102的資料被加密，所以該通訊通道115不必是安全的。

然後，該主終端機102將該ECM提交給該智慧卡109，若存取情況被滿足，則該智慧卡109解密該控制字CW，且利用一對話金鑰 K_S 在本地重新加密。

因此，該主終端機102發送在本地重新加密的控制字CW給該從屬終端機104、106或108。

因此，當接收被重新加密的控制字CW時，該從屬終端機104、106或108將該CW之密碼提交給該安全電子晶片，該安全電子晶片利用對話金鑰 K_S 解密該CW之密碼，且將該已解密的控制字CW提供給該解拌碼器。

注意到，藉由控制該從屬終端機內的對話金鑰 K_S 之存在，該操作者可檢查一終端機104、106或108是否與該主終端機102連接。因此，只有一個具有正確對話金鑰 K_S 的從屬終端機能夠獲得該控制字CW，因此解密該主終端機102重新分配的內容，或者直接接收。

也注意到，該安全電子晶片之功能可被一安全處理器(例如，一智慧卡或一軟體模組)執行，沒有超出本發明之框架。

當該從屬終端機106將該內容記錄在一本地記憶體120內而不是直接使用其時(一般用於顯示),依據本發明的方法也是可應用的。在此情況下,若該等存取情況被滿足,則該主終端機102將與該資料串流儲存的ECM訊息提供給該

5 從屬終端機106。

當讀取一被保存的內容時,該從屬終端機106或108要求該主終端機102以處理該等存取情況,其方式與當接收時所處理的內容之方式相同。

對話金鑰之管理

10 被設計以加密該控制字CW(該主終端機102發送此控制字CW給該從屬終端機104、106或108)的對話金鑰為該主終端機102及一組單一被安裝設備內的該等從屬終端機104、106及108所知。

在初始化此等終端機的一步驟期間,當該被安裝的設備被建立時,此對話金鑰被載入終端機102、104、106、108。

15 在一較佳實施例中,利用一管理訊息(EMM),該操作者將此對話金鑰載入該主終端機102之該智慧卡。該操作者也將該對話金鑰發送給該從屬終端機104、106或108,例如,使用一EMM訊息,以儲存在該安全電子晶片內。由EMM執行的此等載入操作可應用於該對話金鑰本身或者被兩參與者

20 使用的一資料(一般是秘密的),以計算該對話金鑰。

第9圖示意性地描述了用於檢查一從屬終端機之授權以使用數位內容的程序。

在此第9圖所描述的例子中,一位址@i被分配給每一被

安裝的終端機。該等終端機102及104(分別具有位址@0及@1)具有由該操作者載入的相同對話金鑰K1，而具有位址@2的該終端機106具有另一對話金鑰K2。該從屬終端機104可與該主終端機102共同運作，因為該從屬終端機104可利用該金鑰K1解密該密碼 CW^*_{K1} ，以獲得該控制字CW。

另一方面，具有對話金鑰K2的該從屬終端機106不可解密將由該主終端機102發送給其的密碼 CW^*_{K1} (其是使用對話金鑰K1的)。

此結果是該操作者完全控制該等終端機之間的卡之共用，透過對該主終端機102及該等從屬終端機(104、106)共用的對話金鑰之檢查。

檢查終端機之正常使用

依據本發明的方法可被一單一的主終端機用以處理一或幾個ECMs。一終端機可要求該存取管理單元4(第1圖)以處理將用以存取一內容的ECM通道。該終端機也可要求該存取管理單元4，以同時處理幾個內容，這導致對應數目的ECM通道將被處理。

一個單一主終端機102對幾個內容之同時存取可能是正常的。這是一程式由幾個部分組成的情況，例如一影像及原始音軌之存取情況、一不同語言之另一存取情況、以及收聽困難之個人的字幕的又一存取情況。這也是該終端機是一閘道終端機的情況，換句話說，作為一單個實體之一進入點的設備(例如，一單一家庭)，且幾個終端機之聯合存取為分佈內容。

另一方面，一個單一主終端機102對幾個內容的同時存取可被用以轉向一正式存取，且增加內容之未授權存取之數目。

偵測其欺詐使用的可能裝置由以下組成：在一給定週期，觀察一個單一主終端機102對該存取管理單元4作出的請求數目及類型，且取決於該內文，診斷該終端機是否被欺詐使用。

特別地，該請求類型之觀察被用以判定該主終端機102是否提交一個單一的ECM通道或幾個ECM通道用以處理，且是否幾個通道被處理，且用以判定該等ECM通道是否相關聯(換句話說，與相同程式相關聯)或者是否獨立(換句話說，是對不同的程式相關聯)。相同的，以下觀察也是真的：該主終端機重複存取其沒有正常的存取權利的一內容之請求。

取決於其等類型，被儲存的請求之數目與一臨界值相比，在此臨界值之外，該存取管理單元4診斷出，其是一盜版嘗試，且採取相應措施，例如，停止將能夠存取該等內容的資料傳輸給此終端機。

請求之接收、請求類型之考慮、觀察週期之判定、臨界值之調整都可被改變，取決於被分配給此檢查的許可性或嚴重性。

該主終端機也可使用相同的程序檢查該從屬終端機是否被正常使用。

在以上所描述的實施例中，每當一終端機不能處理一ECM以從其取出控制字時，該終端機就將此ECM發送給該

管理單元4，或者給該主終端機102，以獲得此等控制字，因此該終端機可解密該內容。如以上所描述，一ECM之此傳輸/處理偶爾執行，或者在每一加密週期被執行。

從接收終端機來看，該管理單元4或主終端機102的
5 ECM傳輸/處理的總體(global)持續時間必須少於一加密週期之持續時間，因此該終端機可及時具有控制字以解拌碼該內容。

與總體傳輸/處理持續時間有關的條件在對一內容的
《簡單》存取期間致能整個系統的正確運作，換句話說，
10 以其平常執行的大約10秒等級的加密週期之正常速度。

然而，其他使用情況發生在總體傳輸/處理持續時間在技術上不可被滿足的條件下，這會導致解拌碼的不連續或者甚至是不可能。

在一第一例子中，如讀取被儲存在該終端機(PVR)或該
15 網路(Npvr)內的內容此類的功能或如VOD(隨選視訊)此類的服務可允許使用者以高於正常的速率使用接收一內容的可能性，向前傳送或向後傳送(《欺騙模式》)。在快速向前或向後存取期間，該內容內的ECMs之明顯頻率增加且明顯的加密週期減少。此結果是該接收終端機將兩ECM提交給
20 該管理單元或該主終端機之間的時間間隔減少。在超過該內容的某一存取速度，兩ECM提交之間的持續時間短於總體ECM傳輸/處理週期。該系統發散且不再作動。

在另一例中，該操作者可減少該加密週期之長度，以加速控制字之更新，因此增加了對控制字之密碼或該拌碼

內容的強力襲擊的困難，從而增強了內容之保護。超過該加密週期內的一特定減少，兩ECM提交之間的期間變得比總體ECM傳輸/處理期間更短。如以上所描述的例子一樣，該系統分散且不再作動。

5 使用快速向前或向後存取方法

一種克服該系統在特定使用情況下的發散及故障之間題的方式是，減少該接收終端機提交ECMs給該管理單元4或該主終端機102的頻率，同時保持被該管理單元4或該主終端機102之存取控制的部分。這使用了本方法特徵，依據該方法特徵，該接收終端機偶爾將ECMs發送給該管理單元或該主終端機。

本解決方法之原理包含將內容之期間分解為時間片段，在每個時間片段期間，該接收終端機可處理ECMs，而沒有要求該管理單元或該主終端機。然而，當從一片段改變到另一片段時，該接收終端機必須要求該管理單元或該主終端機以得到資訊(一般是解密控制字或存取滿足該內容存取準則的證書所需的金鑰)，使其能夠在此新片段期間處理ECMs。

較佳地，該終端機應要求該管理單元或該主終端機，以獲得下一時間片段的該等控制字之解密金鑰，這意味著其總是滿足存取情況，藉由具有所需的存取證書，或者藉由不檢查此條件。

此解決方案可應用於以上所呈現的各種使用，且以下描述連接到一管理單元4的一接收終端機對一內容的快速

向前及向後存取的情況。

為了完成此，當該內容被一操作者(一存取管理單元4與該操作者連接)提供給該接收終端機6，該方法包括該操作者對該內容的調整階段(conditioning phase)，以及該接收終端機對該內容的使用階段。

該內容調整階段包括以下步驟：

- a)該內容之期間被分解為N個時間片段，每一時間片段與一識別符 S_j 、一金鑰 K_j 及一與此金鑰相關聯的資料 D_j 相關，每一片段 S_j 包含加密週期 CP_i 之整數 M_j ，其中 $i=1$ 到 M_j 。
- 10 b)該內容利用控制字 $CW_{i,j}$ 拌碼，其中 $i=1$ 到 M_j ，且 $j=1$ 到N，
- c)每一控制字 $CW_{i,j}$ 利用該金鑰 K_j 被加密，
- d)然後，該內容在每一加密週期 CP_i 的每一時間片段 S_j 被傳送、拌碼給該終端機，其中一ECM訊息包含至少利用
- 15 目前金鑰 K_j 加密的控制字 $CW_{i,j}$ 之密碼、與目前金鑰 K_j 相關聯的資料 D_j 、與前一金鑰 K_{j-1} 相關聯的資料 D_{j-1} ，以及與下一金鑰 K_{j+1} 相關聯的資料 D_{j+1} 。

《目前片段》是該終端機目前接收的片段 S_j ；相關的金鑰 K_j 被稱為《目前金鑰》。需明白的是，在對該內容的向前存取期間，該終端機以順序... S_j 、 S_{j+1} 、 S_{j+2} ...接收連續的片段，該片段 S_{j+1} 是該內容中的片段 S_j 之後的《下一片段》且使用《下一金鑰》 K_{j+1} ，而在對該內容之向後存取期間，該終端機以順序... S_j 、 S_{j-1} 、 S_{j-2} ...接收連續的片段，該片段 S_{j-1} 是該內容中片段 S_j 之前的《前一片段》且使用《前一金

鑰 K_{j-1} 。

該內容之使用階段使用三偶對，且該終端機在之前被配置以儲存此等偶對。此等偶對 (K_c, D_c) , (K_p, D_p) , (K_s, D_s) 分別由一目前金鑰 K_c 及與該金鑰相關的資料 D_c 、前一金鑰 K_p 及與相關的資料 D_p 、下一金鑰 K_s 及相關的資料 D_s 組成。

當接收每一 ECM 訊息時，該使用階段包括以下步驟：

e) 該終端機分析包含在該 ECM 訊息中的資料 D_j ，且評估該等對中其可獲得的相對應資料。

f) 若包含在該 ECM 訊息中的資料 D_j 對應先前儲存在該終端機內的資料 D_c ，則該終端機利用對應偶對內的與該資料 D_c 有關的金鑰 K_c 解密該等控制字 $CW_{i,j}$ 。在此情況下，該終端機不請求該管理單元執行該 ECM 之任何補充 (complementary) 處理。

g) 若包含在該 ECM 訊息中的資料 D_j 對應先前儲存在該終端機內的資料 D_p ，則該終端機利用對應偶對內的與該資料 D_p 有關的金鑰 K_p 解密該等控制字 $CW_{i,j}$ 。這發生在進入之前片段向後讀取一內容時。類似地，若包含在該 ECM 訊息中的資料 D_j 對應資料 D_s ，則該終端機利用金鑰 K_s 解密控制字 $CW_{i,j}$ 。這發生在進入下一片段向前讀取一內容時。

h) 最後，若包含在該 ECM 訊息中的資料 D_j 不對應先前儲存在該終端機內的資料 D_c ，則該終端機將該被接收的 ECM 訊息發送給該存取管理單元 4，該存取管理單元 4 從該資料 D_j 決定目前金鑰 K_j 、從該資料 D_{j-1} 決定前一金鑰 K_{j-1} 且從該資料 D_{j+1} 決定下一金鑰 K_{j+1} ，且發送此等金鑰及與其等相

關聯的資料給該終端機，該終端機將其等對應值儲存為該等金鑰 K_c ， K_p 與 K_s 及與該等金鑰有關的資料 D_c ， D_p 及 D_s 之新值。每當相同內容中從一片段變化到另一片段，以上情況就發生，用於向前讀取及向後讀取，當從一內容變化到
 5 另一內容時，且當該終端機剛剛完成重新初始化，且此三偶對還沒有被更新時。

依據產生的問題，步驟f)、g)及h)之組合被用以補償一過多的總體傳輸/處理時間(與該加密週期相比)，同時維持該管理單元對該內容之存取的控制。該終端機內的目前金
 10 鑰 K_c 之存在使得該終端機能夠解密控制字，而沒有要求該管理單元。然而，此金鑰只在該目前片段之期間是有效的(步驟f，目前金鑰之使用)。在該片段之末端，該終端機必須使用另一解密金鑰。該終端機已具有此新的金鑰(步驟g，前一金鑰或下一金鑰之使用)，以能夠解拌碼該內容，
 15 沒有任何中斷。然而，為了確保該終端機在此新片段之末端仍可解拌碼而不會中斷，該終端機必須要求該管理單元以處理該ECM，因此該終端機可更新其金鑰之系統(步驟h)。當接收此更新之後的ECM時，該終端機將其本身集中(recentre)到其新的目前金鑰(返回到步驟f)。因此，解拌碼
 20 繼續，即使該管理單元提供金鑰之期間比該加密週期更長，且因為該終端機必須在每個片段期間要求該管理單元，該管理單元維持對該內容之存取的控制。

需明白的是，該終端機必須滿足該存取情況，藉由具有存取證書，或者藉由不知道該情況，因為否則該終端機

將要求每個ECM的管理單元，這將會導致如上所提到的系統之發散。也注意到，當該管理單元接收一ECM以決定該終端機之該等金鑰時，該管理單元可驗證該終端機實際上具有滿足該存取準則且不是非法證書的存取證書，如該基

5 本方法。

依據本發明之一特徵，透過一點至點鏈結，該終端機將該被接收的ECM訊息返回給該存取管理單元4。

該終端機必須在其偶對中具有在目前金鑰 K_j 、前一金鑰 K_{j-1} 及下一金鑰 K_{j+1} (取決於該解決方案)從與出現在該
10 ECM內的該等金鑰相關聯的資料中決定。

在一第一實施例中，與該ECM內所發送的該等金鑰有關的資料包括至少對應該等金鑰 K_j ， K_{j-1} 及 K_{j+1} 的密碼，該等密碼可由為該管理單元4專知的管理金鑰解碼。

在一第二實施例中，與該ECM內所發送的金鑰有關的
15 資料包括至少該等對應片段的識別符 S_j 、 S_{j-1} 及 S_{j+1} 。當該相關聯的資料不包括該等金鑰之密碼時，該等金鑰 K_j 、 K_{j-1} 及 K_{j+1} 由該管理單元4自此等片段識別符開始決定。

在此實施例之一第一實施態樣中，該存取管理單元4藉由搜尋自片段識別符內預先定義的一資料庫，而決定該
20 等新金鑰 K_j ， K_{j-1} 及 K_{j+1} 。

在另一實施例中，該存取管理單元4藉由自片段識別符多樣化一根金鑰，而決定該等新金鑰 K_j ， K_{j-1} 及 K_{j+1} 。

在步驟e)至h)期間，該終端機評估該被接收的相關聯的資料 D_j 與其在偶對中可獲得的資料 D_c ， D_p 及 D_s 之間的對

應性。較佳地，此對應性基於片段識別符是相同的。當片段識別符沒有被使用時，搜尋對應性由比較金鑰密碼組成。

在一第三實施例中，只有與該目前金鑰 K_j 有關的資料 D_j 出現在該ECM訊息中，且該存取管理單元4使用該資料推出與前一金鑰 K_{j-1} 及下一金鑰 K_{j+1} 有關的其他兩資料 D_{j-1} 及 D_{j+1} 。在一第一例中，與該等金鑰有關的資料是具有連續數值...X-2、X-1、X、X+1、X+2的片段識別符。在另一例中，與該等金鑰相關聯的資料是該等金鑰的密碼，且該管理單元具有此等密碼之一先前列表，其序列順序與該等片段相同。當金鑰 K_j 之密碼在此列表中時，在其之前的密碼是金鑰 K_{j-1} 之密碼，且在其之後的密碼是金鑰 K_{j+1} 之密碼。

作為一變化，若一內容之向後讀取沒有被使用，則與前一金鑰 K_{j-1} 有關的資料 D_{j-1} 沒有被用於ECM訊息，且對應前一片段的該偶對 (K_p, D_p) 可被刪除，而沒有超出本發明之範圍。

作為一變化，對應前一片段的該偶對 (K_p, D_p) 可被與前 n_p 連續片段有關的幾個偶對替換，且對應下一片段的該偶對 (K_s, D_s) 可被與後 n_s 連續片段有關的幾個偶對替換，而沒有超出本發明之框架。偶對之擴展意味著，該解決方案是可應用的，甚至在以一速度對該內容之存取期間，使得該ECM之總體傳輸/處理時間變得比一或幾個連續片段之明顯期間更大。然後，前 n_p 偶對或後 n_s 偶對的數目取決於對該內容之存取速度所需的最大值。

以上所描述的解決方案也可被使用，當該拌碼的內容

被分散給一組被安裝的接收終端機時，該組被安裝的接收終端機包含一主終端機(102)及與該主終端機(102)相依的至少一從屬終端機(104、106、108)。在此情況下，該接收終端機被該從屬終端機替換，且從該從屬終端機來看，該

5 管理單元被該主終端機替換。

在一實施例中，該從屬終端機發送給該主終端機以獲得該 (K_c, D_c) ， (K_p, D_p) ， (K_s, D_s) 偶對之新值的該ECM之處理被該主終端機本身執行，該主終端機被提供與被用於一管理單元的裝置類似的裝置，例如一根金鑰多樣函數、

10 使用一管理金鑰的解密函數、一密碼資料庫，取決於該實施態樣。

在另一實施例中，該主終端機(102)決定將被發送給該從屬終端機的該 (K_c, D_c) ， (K_p, D_p) ， (K_s, D_s) 偶對之新值，藉由發送其接收的該ECM訊息給一管理單元(4)或者給一

15 與其相依的主終端機(且其充當一從屬終端機)，以供處理。

以上所描述的較佳方案由將一不同金鑰與一片段連接組成，該存取情況總是被該終端機滿足或不為該終端機所知。此解決方案也可明顯地被提供給一不同的存取情況與每一片段連接的情況，該解密金鑰不被改變，且可在該終

20 端機內獲得。在此情況下，該資料 D_j 與權利相關聯，且該管理單元提供存取目前、下一個及之前片段所需的權利給該終端機，而不是金鑰。

【圖式簡單說明】

第1圖顯示了依據本發明之一存取控制系統的總方案；

第2圖示意性地顯示了第1圖中的該系統之一第一例子；

第3圖是描述了依據本發明之方法的特定應用之方塊圖；

第4-6圖表示描述了依據本發明之該方法的時間階段的時序圖；

5 第7圖是描述了依據本發明之方法的一實施例的該等步驟之流程圖；

第8圖示意性地描述了依據本發明之方法的一第二應用，其中該存取控制由一主終端機管理，幾個從屬終端機與該主終端機連接；

10 第9圖示意性地描述了用於授權一從屬終端機使用該數位內容的控制程序。

【主要元件符號說明】

2...發射裝置	18...SAS 模組 (用戶授權系統)
4...存取管理單元	20...MUX 多工器
6...終端機	22...ECM
7...傳輸網路	24...ECM
8...內容伺服器	26...CW* _{kter}
10...存取控制模組/安全處理器	30~88...步驟
12...雙向點至點鏈結	100...操作者
14...設備	102...主終端機
15...數位用戶線存取多工器	104...從屬終端機
16...ECM-G (用於權利控制訊息產生器) 模組	105...內容
	106...從屬終端機

107…內容

108…從屬終端機

109…智慧卡

110…內容

111…本地記憶體

112…內容

115…鏈結

120…本地記憶體

103年05月27日修正頁(本)
封條

第 95138741 號申請案修正本

103.05.27

P45~48

十、申請專利範圍：

1. 一種用於存取控制拌碼加密內容之方法，該拌碼加密內容係由與一存取管理單元合作之一操作者提供給一接收終端機，該終端機被提供有至少一存取控制模組，該方法包含以下步驟：

將該內容與用於解拌碼該內容所必需的多數資訊相關聯；

將具有該等多數資訊的該內容發送給該終端機；

當該終端機接收該等多數資訊時，

透過一點至點鏈結，系統性或偶爾將該等多數資訊中的至少一項資訊傳回給該存取管理單元；

使用該存取管理單元以驗證所傳送之該資訊是否與先前分配給該終端機之存取權利相容；

傳送至少一控制參數給該終端機以在如果所傳送之該資訊與先前分配給該終端機之存取權利相容時啟用該內容；

否則，該管理單元不將該參數傳送至該終端機；

該方法其中之由該存取管理單元發送至該終端機的該控制參數係一ECM_R訊息，其紀錄有該內容且包含控制該內容之重複使用的存取準則。

2. 如請求項1所述之方法，其中用於解拌碼該內容所必需的該等多數資訊係在一ECM訊息中被發送給該終端機，該ECM訊息包含至少一存取準則CA、由一金鑰K_{ecm}加密的一控制字之一密碼CW*_{K_{ecm}}。

3. 如請求項1所述之方法，其中被提供給該終端機的內容被一DRM許可證保護。
4. 如請求項1所述之方法，其中該拌碼加密內容係分配給一組接收終端機，且其中該存取管理單元為整組接收終端機中之一主終端機，且該接收終端機為整組接收終端機中之一從屬終端機。
5. 如請求項4所述之方法，其中該從屬終端機傳回至少該密碼 $CW *_{K_{ecm}}$ 給該主終端機。
6. 一種存取控制系統，包含：包含一內容伺服器的一發射裝置、與該發射裝置關聯的一存取管理單元、被提供有至少一存取控制模組的一接收終端機，該至少一存取控制模組控制由該伺服器所傳送的一拌碼加密內容之存取且用於解拌碼該內容所必需的多數資訊係與該拌碼內容相關聯，該接收終端機透過一點至點鏈結連接到該存取管理單元，該存取控制模組係適以系統性地或偶爾將包含在用於解拌碼該內容所必需的該等多數資訊中的至少一項資訊傳回給該存取管理單元，且其中該存取管理單元係適以驗證該傳回資訊是否與先前分配給該終端機之該存取權利相容，且如果該傳回資訊與先前分配給該終端機之存取權利相容，則發送至少一控制參數給該終端機以啟用該內容，或者如果該傳回資訊與先前分配給該終端機之存取權利不相容，則不將該參數發送至該終端機，

該系統其中之由該存取管理單元發送至該終端機

的該控制參數係要被紀錄有該內容之一ECM_R訊息且其包含將被用來控制該內容之重複使用的存取準則。

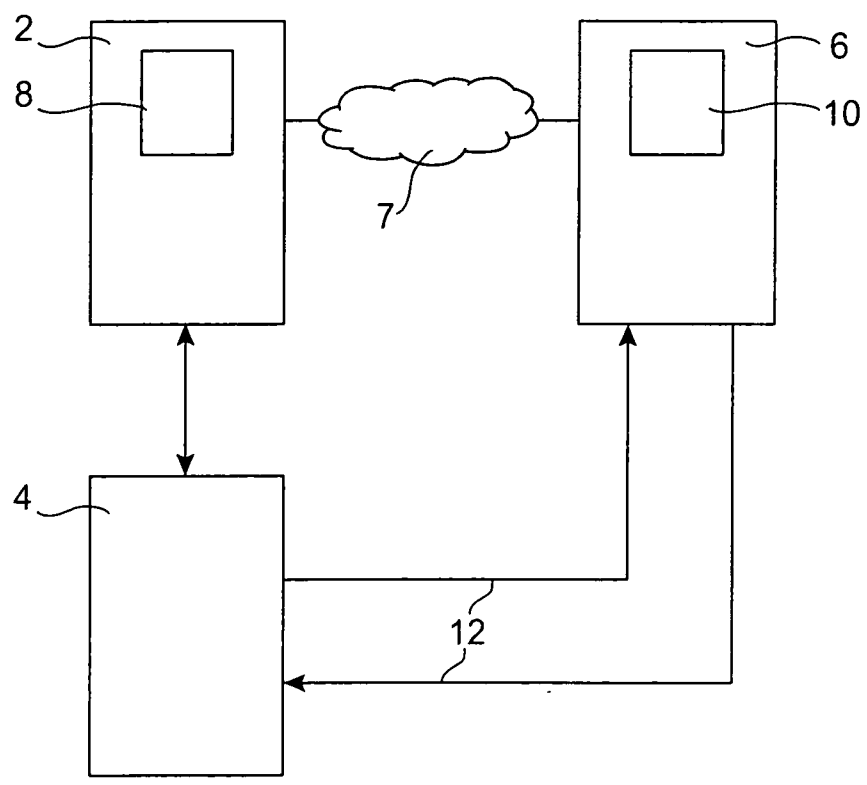
7. 如請求項6所述之存取控制系統，其中用於解拌碼該內容所必需的該等多數資訊係在一ECM訊息中被發送給該終端機，該ECM訊息包含至少一存取準則CA、由一金鑰K_{ecm}加密的一控制字CW之一密碼CW*_{K_{ecm}}。
8. 如請求項7所述之存取控制系統，其中該存取管理單元係與該發射裝置區別開。
9. 如請求項6所述之存取控制系統，其中該存取管理單元係被整合進該發射裝置。
10. 如請求項9所述之存取控制系統，其中該主終端機係被整合進該發射裝置。
11. 如請求項9所述之存取控制系統，其中該主終端機被整合到一收集接收天線。
12. 如請求項11所述之系統，其中該主終端機在該內容伺服器與整組從屬終端機之間執行一橋接功能。
13. 一種用於接收一拌碼加密內容之接收終端機，該拌碼加密內容係與用以解拌碼該內容所必需的多數資訊傳送，該終端機係透過一點至點鏈結連接至一存取管理單元且包含一存取控制模組，該存取控制模組包括傳回構件，其系統性地或偶爾將在用於解拌碼該內容所必需的該等多數資訊中的至少一項資訊透過一點至點鏈結傳回給該存取管理單元，而啟用該存取管理單元以驗證該

傳回資訊是否與先前分配給該終端機之該存取權利相容，且如果該傳回資訊與先前分配給該終端機之存取權利相容，則發送至少一控制參數給該終端機以啟用該內容，或者如果該傳回資訊與先前分配給該終端機之存取權利不相容，則不將該參數發送至該終端機，

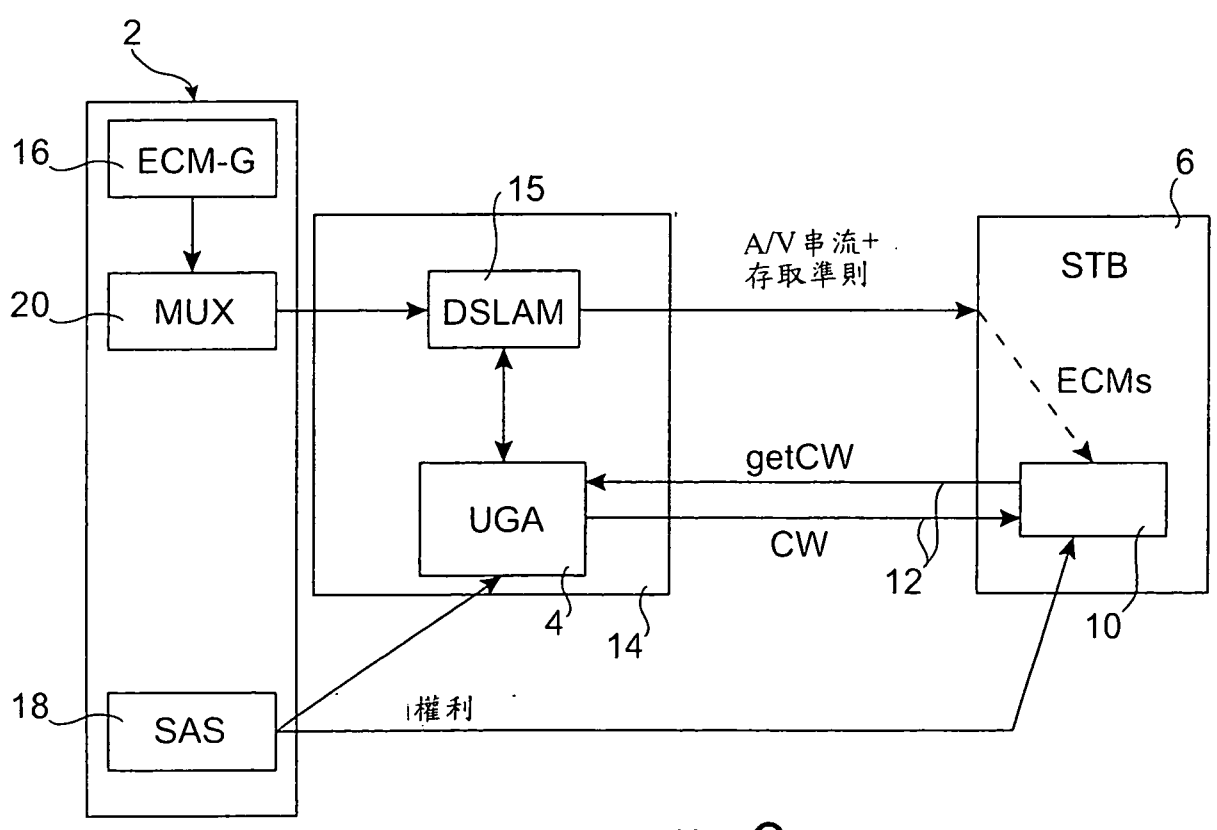
由該存取管理單元傳送至該存取控制模組的該控制參數係將被紀錄有該內容且包含將被用來控制該內容之重複使用的存取準則之一 ECM_R 訊息。

14. 一種儲存在一儲存媒體上且包含指令之電腦程式，該指令用以當該電腦程式在一電腦上運行時使用如請求項1之存取控制方法。

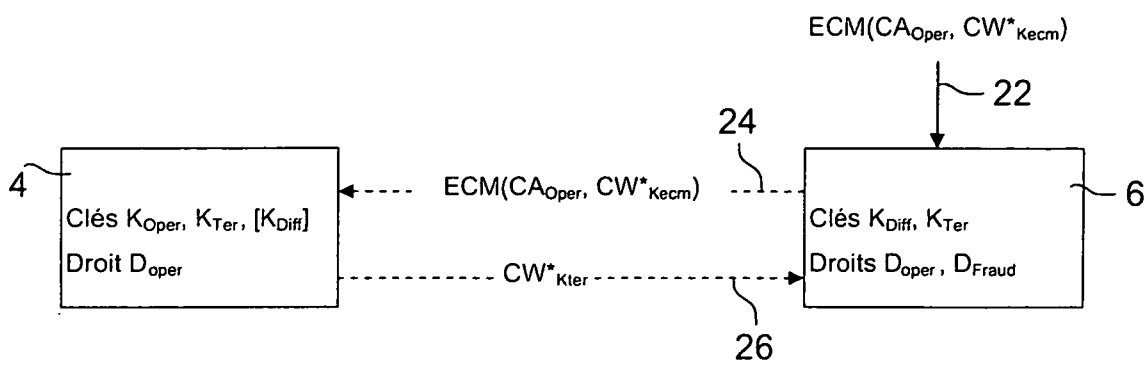
15. 如請求項14之電腦程式，其中該拌碼加密內容係分配給一組接收終端機，且其中該存取管理單元為整組接收終端機中之一主終端機，且該接收終端機為整組接收終端機中之一從屬終端機。



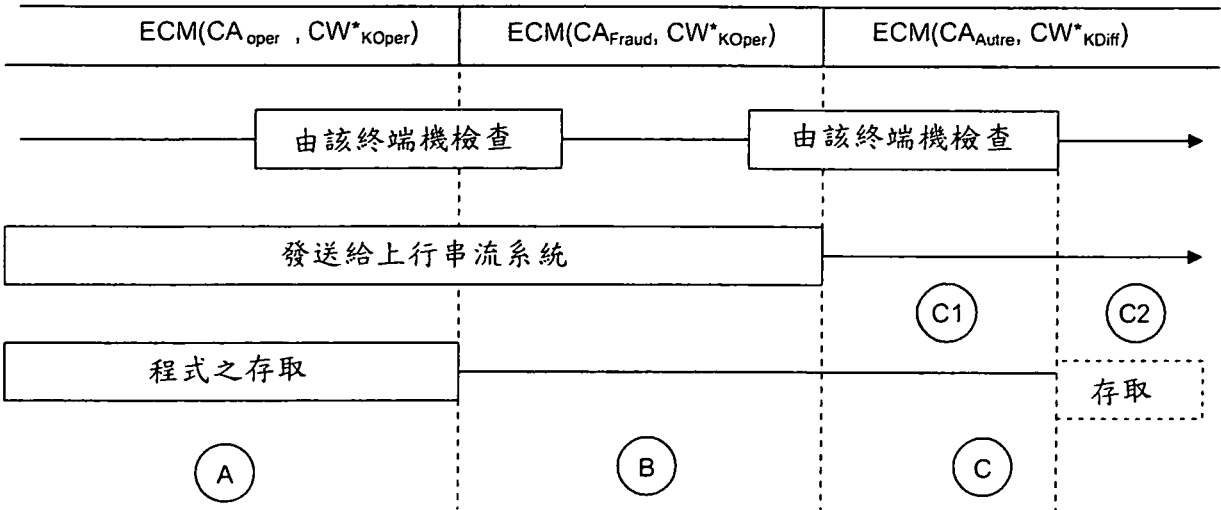
第 1 圖



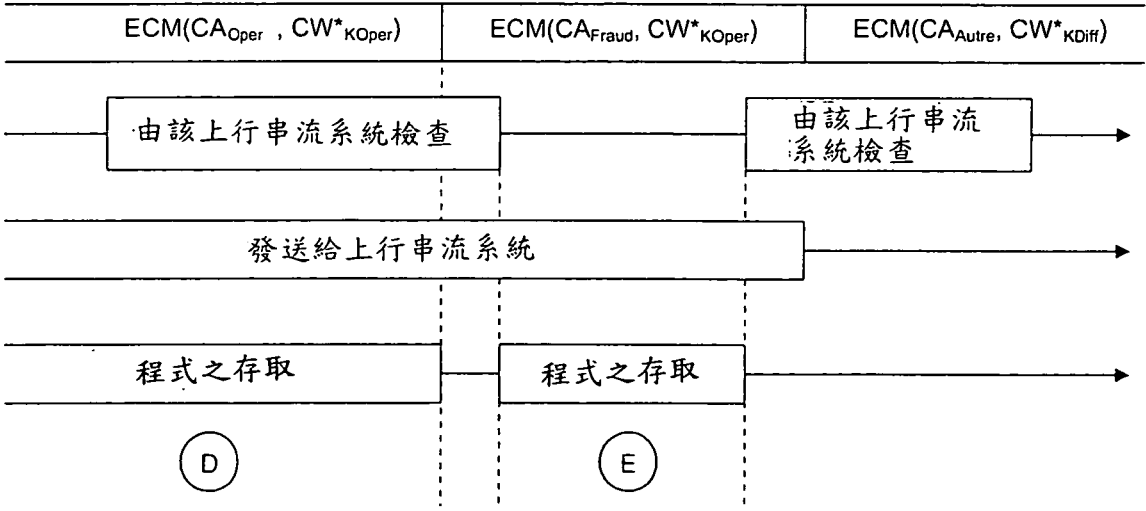
第 2 圖



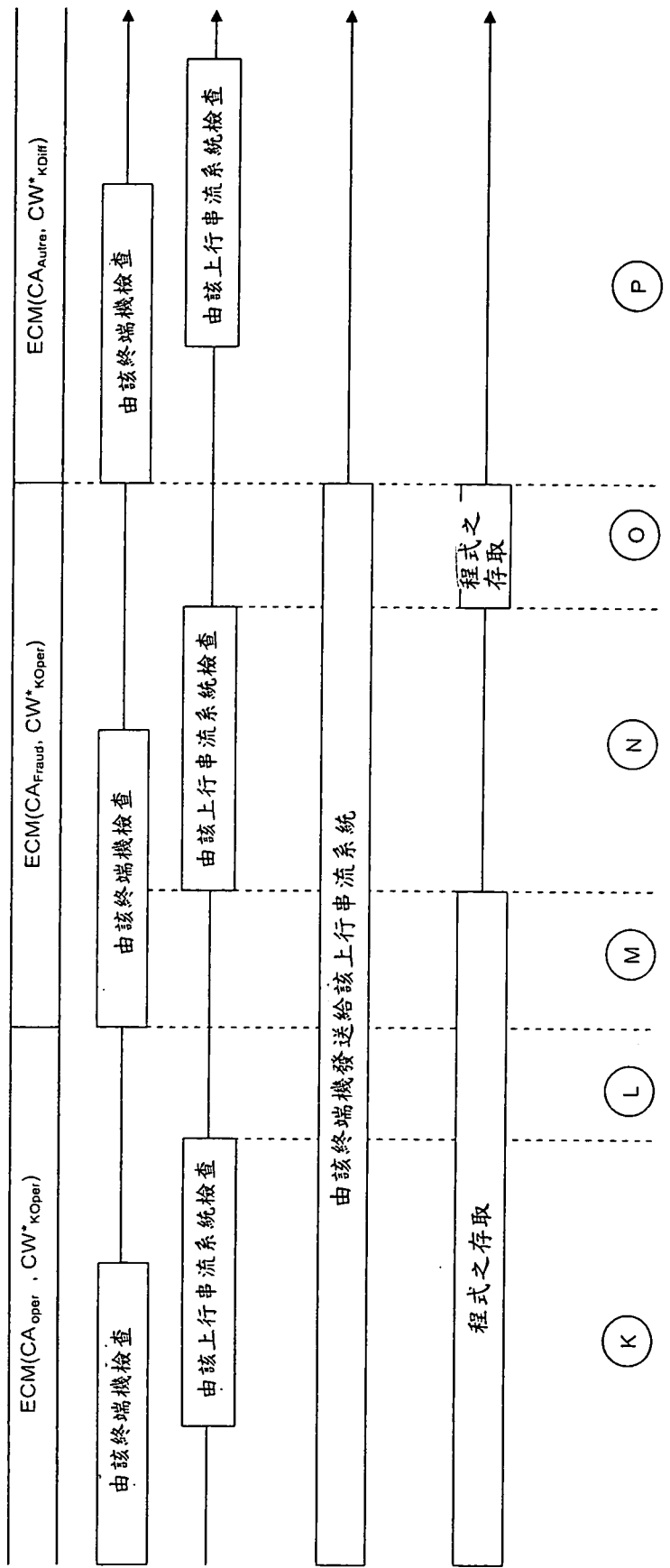
第 3 圖



第 4 圖

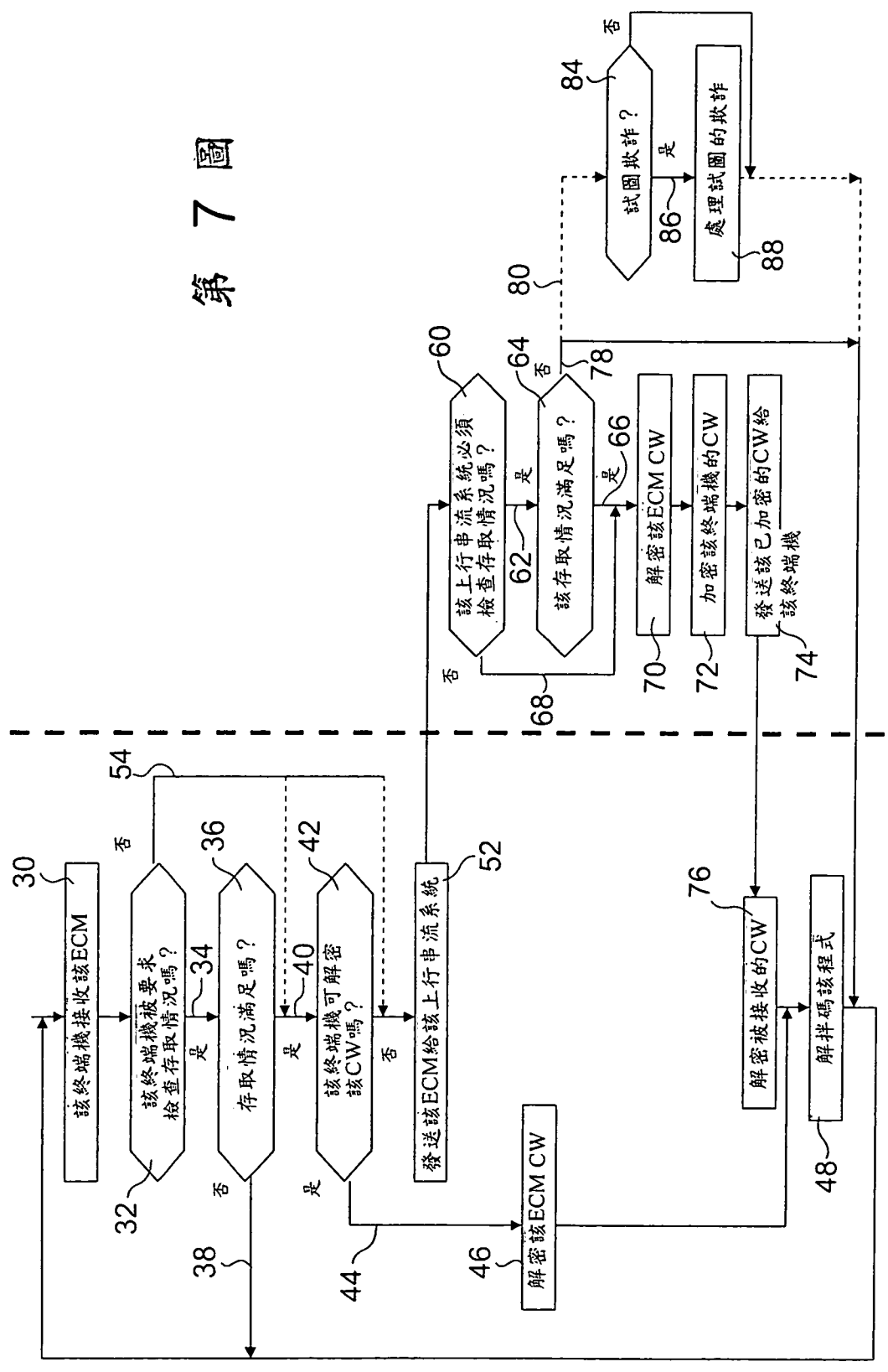


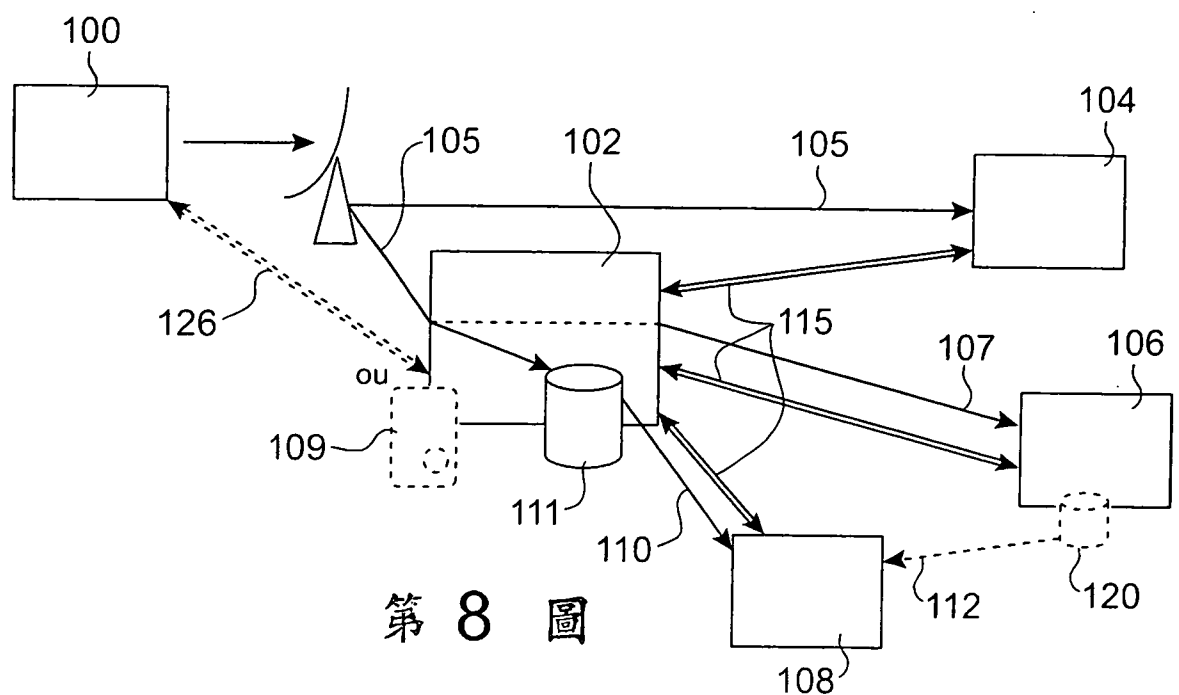
第 5 圖



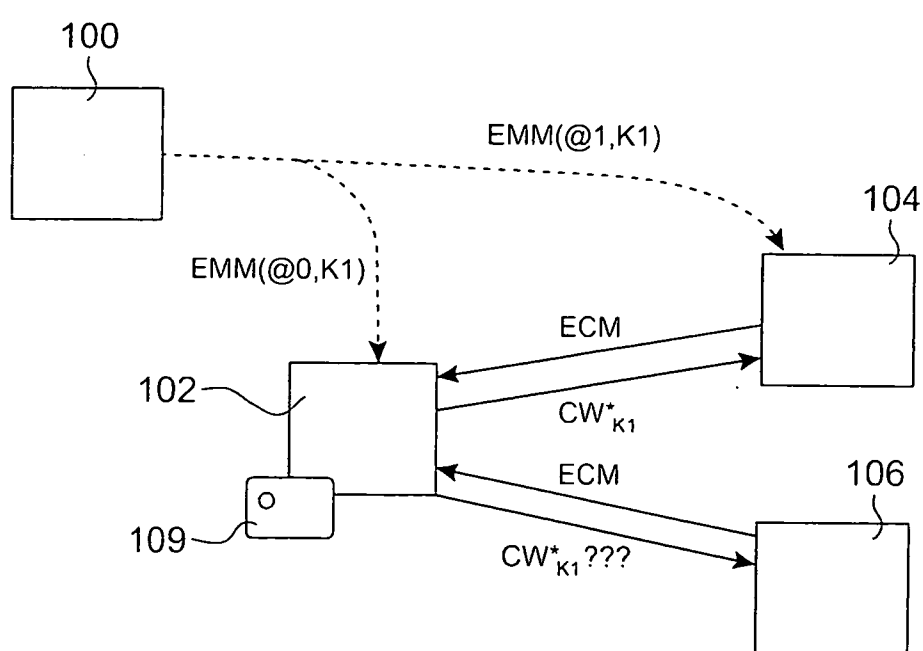
第 6 圖

第 7 圖





第 8 圖



第 9 圖