

公告本

申請日期:

89.3.29

案號:

89105742

類別:

H04L12/00

(以上各欄由本局填註)

發明專利說明書

502513

一、 發明名稱	中文	數位式局部網路及其產生和更新方法
	英文	DIGITAL LOCAL NETWORK, NOTABLY DIGITAL HOME NETWORK, AND METHOD FOR CREATING AND UPDATING SUCH A NETWORK
二、 發明人	姓名 (中文)	1. 魁斯 2. 安德瑞克 3. 弗羅恩
	姓名 (英文)	1. Ques, Florence 2. Andreaux, Jean-Pierre 3. Furon, Teddy
	國籍	1. 法國 2. 法國 3. 法國
	住、居所	1. 法國勒恩市路傑瑪羅瑞納特14號 2. 法國勒恩市路里察雷諾33號 3. 法國勒恩市路德拉生特13號
三、 申請人	姓名 (名稱) (中文)	1. 法商·湯姆生多媒體公司
	姓名 (名稱) (英文)	1. THOMSON multimedia S.A.
	國籍	1. 法國
	住、居所 (事務所)	1. 法國布羅格比倫寇特市魁里加羅46號
	代表人 姓名 (中文)	1. 建固漢
	代表人 姓名 (英文)	1. ZHANG, Jianguo



本案已向

國(地區)申請專利
法國 FR

申請日期
1999/04/13 9904767

主張優先權
有

有關微生物已寄存於

寄存日期
寄存號碼

無



五、發明說明 (1)

本發明一般係關於局部數位式網路場域，尤指數位式家庭網路場域。

此種網路包含一組設備，利用數位式匯流排，例如按照 IEEE 1394 標準的匯流排相連接。包括二種主要設備：

一存取設備，可接收源自局部網路外界的資料，並在網路上連接設備的點發送；和

一呈現設備，適於接收流入網路內之資料，以便在連接此等設備的網路另一點加以呈現。此第二種設備不與局部網路之外界連接。

因此，若以旨在把聲頻和 / 或視頻資料輸送入屋內各房間之數位式家庭網路為例，存取設備係例如數位式解碼器或設定頂箱，接生來自網路外界的視頻節目，經由衛星天線和電纜連接，或在網路上以數位型式廣播的光碟閱讀機，從碟片（在此情況下，碟片含有源自網路外界的資料）閱讀之資料。呈現設置有例如電視機，可以觀看從網路接到的視頻程式，或更一般而言，可將接收的數位式資訊轉變成類比信號之任何裝置，以便將此信號廣播給末端使用者。

上述家庭網路亦可包括第三種設備，與網路外界無連接，而具有流入網路內資料之記錄功用者。以此第三類裝置為例，可資一提者特別有數位式視頻記錄器，或記錄光碟之 DVD 型裝置（DVD 縮寫代表「數位式多樣化碟片」）。

須知一種同樣裝置可屬於二種或甚至三種不同類型之上述設備。例如，光碟記錄裝置亦可閱讀商業性預錄碟片



五、發明說明 (2)

，因而同時屬於上述第一和第三類設備。

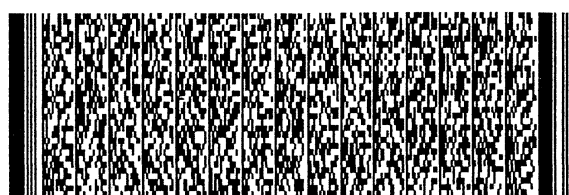
若顧及提供行自局部網路外界之資料之內容提供者觀點，尤其是廣播付費電視節目的服務提供者，或例如光碟之其他出版者，則必須防止此等發送資料受到複印，或容易從一局部網路流至另一局部網路（例如被複印到光碟或任何其他記錄媒質上）。

如此做時，已知實務是以祕密方式發送資料，使用授權設備預先已知的鍵碼，借助於密碼演算加以鎖碼，以接收此等資料，不然就按照內容提供者和此等設備間的特別安全協議交換。

若顧及擁有數位式家庭網路的使用者觀點，當網路設備之一獲准從內容提供者接收資料，則此等資料需能發送至網路的所有其他設備。因此，付費電視服務訂戶的使用者，在位於其客廳（獲准解碼）的設定頂箱接收節目（以鎖碼形式發送），會想在例如位於其臥室內的電視看這些節目。此外，使用者有興趣錄下接收的節目，然後在網路的若干設備上觀看，即使付費電視服務訂約已期滿。

考慮到內容提供者和使用者的願望，本發明之目的即在提供一種機構，使局部數位式網路接收的資料可在網路的諸設備間自由流通，同時防止其在不同局部網路之間流動。

為達此目的，本發明擬議的局部數位式網路，尤其是數位式家庭網路，包括至少一存取設備，可接收源自網路外界之資料，並在網路之一點發送；和至少一呈現設備，



五、發明說明 (3)

適於接收流入網路內之資料，以便在網路之一點呈現；其中，資料適於只以鎖碼形式流通。按照本發明，為了流入網路內資料的鎖碼和解碼，網路的所有設備使用網路專屬的單一鎖碼鍵；網路之局部鍵。

由於各局部網路擁有其本身的局部鍵，與其他局部網路不同，進入該網路的任何資訊可由網路的所有設備平等閱讀，但不能複印到另一局部網路上閱讀。更正確言之，資訊可以鎖碼型式複印，但不能在非複印的局部網路內再顯示。因此，本發明可以符合內容提供者和使用者的願望。

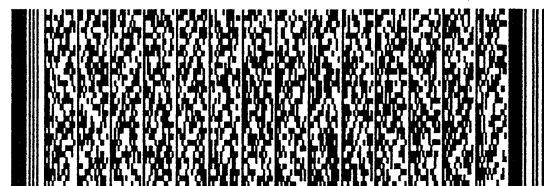
按照本發明較佳要旨，資料是使用密碼系統，以公鍵鎖碼，亦稱為非對稱密碼系統。在此情況下，網路的局部鍵是由一對公鍵和私鍵形成：網路之局部公鍵和局部私鍵。

最好是只有接到網路的呈現設備知道局部私鍵。

按照特殊具體例，在指定時刻，網路之單一呈現設備獲准發送局部私鍵至適於接至網路的新呈現設備。此設備以下稱為網路繁殖器。

因此，若此繁殖器從局部網路除去，尤其是產生私用局部網路，擁有和原先局部網路同樣的局部勁，則原先局部網路不再能改變，因為原先網路的設備不再能發送網路之局部私鍵，至適於接至原先局部網路的新呈現設備。

按照本發明另一要旨，在指定時刻，呈現設備只能是下列狀態之一：



五、發明說明 (4)

(i) 第一狀態，初生態，當呈現設備初次接至網路；

(ii) 第二狀態，繁殖態，呈現設備獲准發送網路的局部私鍵，至適於接至網路的任何新呈現設備；

(iii) 第三狀態，滅絕態，呈現設備不再獲准發送網路的局部私鍵，至適於接至該網路的任何新呈現設備。

呈現設備只能變化狀態，以通到較高階狀態，意即從初生態至繁殖態，或從繁殖態至滅絕態，或另外從初生態至滅絕態。

按照本發明較佳要旨，網路之單一呈現設備在第二狀態是繁殖態：網路之繁殖器。

按照特殊具體例，在指定時刻，網路之繁殖器是最後接至網路得呈現設備。

因此，網路的「繁殖器」標題，即發送至接到局部網路的各新裝置。此舉從單一繁殖器呈現設備起，防止具有同樣局部鍵之全部串聯局部網路內產生盜用。

本發明亦涉及一種呈現設備，適於連接至數位式網路，如上所述，而在指定時刻，只有上述狀態，即初生態、繁殖態或滅絕態之一，該呈現設備只能改變狀態，往更高階的狀態。

按照本發明一要旨，當呈現設備呈初生態時，擁有本身的一對公鍵和私鍵，並獲准接收適於連接的網路之成對局部鍵，代替其本身的成對鍵加以儲存。

按照本發明另一要旨，當呈現在滅絕態時，不再獲准



五、發明說明 (5)

接收適於連接的網路之成對局部鍵。

按照本發明又一要旨，呈現設備包括該呈現設備佔有的狀態儲存機構，此儲存機構係整合於智慧卡內。

按照本發明再一要旨，網路之成對局部鍵容納在提供該設備之智慧卡內。

本發明亦涉及上述網路之產生和更新方法，詳後。

本發明其他特徵和優點由參照附圖說明本發明非限制性之特殊具體例即可明白，附圖中：

第1圖表示本發明局部數位式網路；

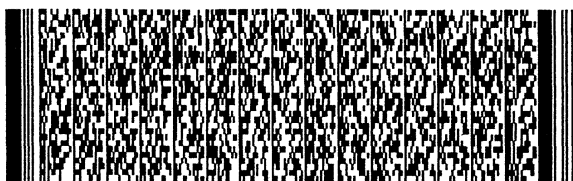
第2圖表示如第1圖所示數位式網路之產生方法；

第3圖表示新呈現設備對例如按照第2圖方法所產生局部數位式網路之連接方法。

圖中只呈現瞭解本發明及特殊具體例有關之元件。

第1圖所示為數位式家庭網路，包括存取設備1，二呈現設備2、3，以及數位式錄影機4，通常稱為DVCR（縮寫DVCR代表「數位式卡式錄影機」）。設備1, 2, 3, 4之總成接至家用數位式匯流排B，例如為按照IEEE 1394標準之匯流排。

存取設備1包括數位式解碼器10，裝設智慧卡閱讀機，提供智慧卡11。此數位式解碼器10接至衛星天線或電纜網路，以便接收服務提供者分配之視頻節目。此等節目例以MPEG-2格式，在資料流F內接收。按前此所知方式，以保密形式發送，內容以控制字CW保密。此等控制字本身是按照指定的鎖碼演算，在資料流F內，以使用鍵K鎖碼的型



五、發明說明 (6)

式發送，在發送中可以保密。

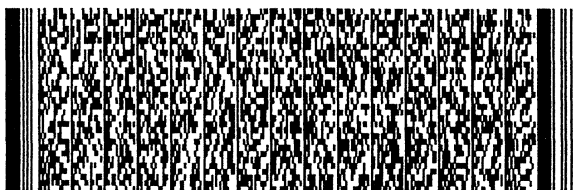
因此，只有服務提供者授權的使用者才有權把發送的資料解碼（例如付費）。如此一來，提供者以K鍵供應授權使用者，用來對控制字CW解碼。往往授權收看節目只有臨時性，即使用者付費時間。所以，K鍵被服務提供者規則性更換。

基於本發明，並由下述可見，使用者可以在其付費期間錄下發送的節目，可隨意經常在其自己網路上重播，即使不再是訂戶。另方面，由於資料是以保密形式錄影，只能在做錄影的使用者網路上重播。

在第1圖內，網路只在佔有的狀態呈現，若全部裝置均按以下參照第2和3圖所述方法連接。

茲說明在解碼器10接收的流F內所發送資料如何處理。凡精於技藝人士已知，以按照MPEG-2格式發送的資料而言，資料流F包括接續的視頻資料訊包、聲頻資料訊包、和管理資料訊包。管理資料訊包特別包括指稱ECM的控制訊息（縮寫ECM代表「權利控制訊包」），使用K鍵把控制字CW以鎖碼形式發送進入，用來把視頻和聲頻資料訊包內發送的資料保密。

此資料流F發送至智慧卡11，在其中處理。利用多工解訊器電路(DEMUX)12接收，該電路一方面把ECM發送至存取控制電路(CA)13，另方面把指明DE的保密視頻和聲頻資料訊包發送至多光化電路(MUX)15。電路CA含有K鍵，因此可將ECM內所含控制字CW解碼。電路CA把此等控制字CW發



五、發明說明 (7)

送至轉換器電路14，此電路14按照本發明含有網路的局部公鍵 $K_{PUB.LOC}$ ，轉換器14使用鍵 $K_{PUB.LOC}$ 把控制字CW鎖碼，並把使用局部公鍵鎖碼的此等控制字，發送到指明LECM的控制訊息內之多工化電路。此等訊息LECM功能和初期資料流F內所接收訊息ECM相同，即發送控制字CW，但在訊息LECM內，控制字CW是使用局部公鍵 $K_{PUB.LOC}$ 鎖碼，以代替使用服務提供者的K鍵鎖碼。

多工化電路15即發送利用解碼器10接收的資料流F'內之資料訊包DE和轉換之控制訊息LECM。此資料流F'再繞家用匯流B流通，可由呈現設備2或3之一，或由數位式錄影機4接收，以便錄影。按照本發明，資料即始終以鎖碼形式流入匯流排B，只有含網路局部私鍵 $K_{PRI.LOC}$ 的裝置，才能把控制字CW解碼，因而將資料DE解碼。此舉即可防止在第1圖家用網路內所做任何複印在其他局部網路播放。

在第1圖例中，電路12至15整合於智慧卡11內，但在變化例中，可把電路DEMUX和MUX放入解碼器10內，只有電路13和14保留整合於智慧卡內。尤其是因為電路CA13和轉換器14含有鎖碼和解碼鍵，必須整合在智慧卡等安全媒質內。

呈現設備2包括數位式電視機(DTV1)20，裝設有使用智慧卡21的智慧卡閱讀機。電視機20接收源自解碼器10或數位式錄影機4，透過匯流排B的資料流F'。資料流F'發送至智慧卡21。由多工解訊器電路(DEMUX)22接收，一方面發送保密視頻和聲頻資料訊包DE至解密電路(DES.)24，另



五、發明說明 (8)

方面發送轉換控制訊息LECM至終端模組23。終端模組含有網路成對的公鍵($K_{\text{PUB. LOC}}$)和私鍵($K_{\text{PRI. LOC}}$)。由於控制訊息LECM含有控制字CW，已用網路的局部公鍵KPUB.LOC鎖碼，終端模組即可用局部私鍵KPRI.LOC將此等控制字解碼，而得清晰控制字CW。此等控制字CW再發送至解密電路24，用來把資料訊包DE解碼，並輸出清晰資料訊包DC至電視機20。

為確保在智慧卡21和電視機20顯示電路之間最後發送清晰資料DC，在該智慧卡和電視機20的卡閱讀機間之介面I，可按照保障智慧卡的美國NRSS標準(NRSS為國家更新安全標準的縮寫)製成保全。

第二呈現設備3包括數位式電視機(DTV2)30，裝設使用智慧卡31的智慧卡閱讀機，操作方式和呈現設備2相同，不再贅述。

由於上述局部數位式網路，源自內容提供者的資料流F，利用接收的存取設備，依賴網路的局部公鍵 $K_{\text{PUB. LOC}}$ 轉型為資料流F'。此資料源F'因此包含具有局部網路專屬格式之資料，此資料除了含有網路局部私鍵之局部網路呈現設備外，無法解碼。

茲說明如何產生第1圖的局部數位式網路，和如何管理新裝置連接至該網路，以保證網路的全部裝置都享有網路的獨特局部成對鍵。

在第2圖內，簡略表示第1圖所示數位式網路之產生方法。



五、發明說明 (9)

為產生本發明數位式網路，必須把存取設備和呈現設備連接在一起。

在第2圖內，假設起初經由數位式匯流排B連接存取設備1和呈現設備2，產生網路。沿時間座標 t 呈現網路產生方法之各項步驟，時間座標 t 加倍，以表示二設備間替換。

在方法第一步驟100中，若二設備連接在一起，呈現設備含有一對公鍵 K_{PUB2} 和私鍵 K_{PRI2} ，按照本發明是在初生態。

設備狀態宜利用位在呈現設備終端模組23(第1圖)內的2位元暫存器之狀態指示器IE儲存。按慣例，假定設備在初生態，狀態指示器IE等於00；當設備在繁殖態， $IE=01$ ，而設備在滅絕態時， $IE=10$ 。

狀態指示器IE容納在智慧卡的積體電路內，以保險防止篡改。

若呈現設備由廠商售出，必須能夠連接到本發明類型的現有局部數位式網路。也必須能連接到存取設備，以產生新網路。此即何以按照本發明製造的任何呈現設備，例行包括一對公鍵和私鍵的緣故，此對鍵為獨一無二，彼此不同，故保證事實上按照本發明產生的各局部網路亦擁有獨特的成對鍵。此外，為保證更換安全，所用全部成對私鍵/公鍵，均按照精於技藝人士所知方法認證。

另方面，存取設備產銷不含任何鎖碼/解碼鍵。同時最好含有本發明轉換器電路(容納在智慧卡內)，如前參



五、發明說明 (10)

見第1圖所述，可儲存適於連接的網路之局部鍵。

再參見第2圖，對呈現設備2而言，方法步驟101包含把適於連接至匯流排B的全部存取設備(在此例中即為存取設備1)注定的公鍵 K_{PUB2} 遞送越過匯流排B。

對存取設備1言，步驟102包含接收公鍵 K_{PUB2} ，做為網路的新局部公鍵儲存($K_{PUB.LOC}=K_{PUB2}$)。

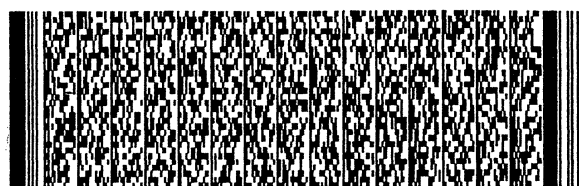
在步驟103中，存取設備1把呈現設備2注定的狀態變化信號，遞送越過匯流排B。此步驟目的在於對呈現設備2指示，是首先連接至網路，所以必須成為網路的繁殖器，意即只有獲授權的呈現設備發送其私鍵 K_{PRI2} (成為網路的局部私鍵 $K_{PRI.LOC}$)，至適於接至網路的任何新呈現設備。

所以，對呈現設備2而言，步驟104包含接收狀態變化信號，並改變其狀態指示器，以便通到繁殖態($IE=01$)。

方法結束時，即有本發明局部數位式網路，包括獨特局部公鍵 $K_{PUB.LOC}$ (等於呈現設備2的初期公鍵 K_{PUB2})，為網路的二設備所知，以及獨特的局部私鍵 $K_{PRI.LOC}$ ，只為呈現設備2所知。按照本發明，網路亦包括繁殖器呈現設備，可容許連接新呈現設備而加以改變。

茲參見第3圖說明新呈現設備(在此例中為呈現設備3)與按照第2圖方法產生的網路之連接方法。

在方法之第一步驟200, 200', 200"中，包含經由數位式匯流排B，把呈現設備3連接到現有局部網路，呈現設備2含有其本身的成對公鍵 K_{PUB3} 和私鍵 K_{PRI3} ，並在初生態($IE=00$)。存取設備1和呈現設備2分別在第2圖方法結束時的同



五、發明說明 (11)

樣狀態，意即存取設備1含有網路的局部公鍵 $K_{\text{PUB. LOC}}$ ，而呈現設備為網路的繁殖器($IE=01$)，並含有網路的成對局部鍵($K_{\text{PUB. LOC}}, K_{\text{PRI. LOC}}$)。

以呈現設備3而言，第二步驟201包含把適於連接至匯流排B的全部存取設備(在此例中為存取設備1)注定的公鍵 K_{PUB3} 遞送越過匯流排B。此步驟與產生方法的步驟101(第2圖)相同。

對存取設備1而言，步驟202包含接收公鍵 K_{PUB3} ，並證明是否已含有公鍵($\text{VERIF. PRESENCE } K_{\text{PUB. LOC}}$)。

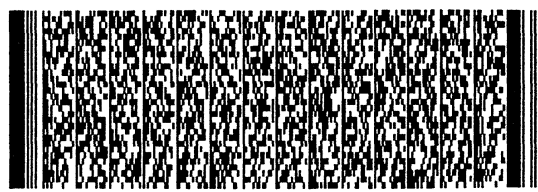
在正面證實時，亦即在此例，對存取設備1而言，次一步驟203包含把局部公鍵 $K_{\text{PUB. LOC}}$ 遞送越過新呈現設備3注定的匯流排B。

在步驟204中，呈現設備3接收局部公鍵 $K_{\text{PUB. LOC}}$ ，並儲存於最好是終端模組內。

對呈現設備3而言，次一步驟205包含把信號以要求網路繁殖器設備回應的訊息(繁殖器)形式，遞送越過設址於網路所有呈現設備之匯流排B。

在步驟206內，網路的繁殖器設備，在此例中為呈現設備2，接收此訊息，一旦在呈現設備2和3之間以依賴方式建立通訊，即改狀態以通到滅絕狀態($IE=10$)。

對呈現設備2而言，步驟207則包含以鎖碼形式遞送網路的局部私鍵($E(K_{\text{PRI. LOC}})$)，可利用呈現設備3解碼。具體而言，局部私鍵在呈現設備2、3間的安全發送，可用呈現設備3的初期公鍵 K_{PUB3} 進行，將局部私鍵鎖碼，呈現設備3



五、發明說明 (12)

則可用其私鍵 K_{PRI3} 將此訊息解碼。鍵 K_{PUB3} 例如在步驟 205 中發送至呈現設備 2。

在步驟 208 內，呈現設備 3 接收局部私鍵加以解碼並儲存，最好儲存於其終端模組內，整合於智慧卡 31（第 1 圖）。

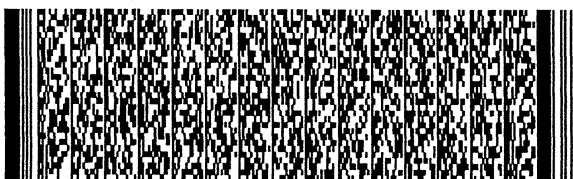
對呈現設備 3 而言，步驟 209 包含把局部私鍵接受的信號遞送（接收（ $K_{PRI,LOC}$ ）），越過呈現設備 2 注定的匯流排 B。

在步驟 210，呈現設備 2 接收此接受信號，並因應遞送狀態變化信號至新呈現設備 3，而在步驟 211，呈現設備 3 接收此信號，改變狀態，變成網路的新繁殖器（ $IE=01$ ）。

由於呈現設備 2 從此在滅絕狀態，不再授權發送網路的局部私鍵至另一呈現設備。如此可防止此設備 2 從網路除去，以產生另一私用局部網路，擁有上述網路同樣的成對局部鍵。

方法結束時，即有二呈現設備 2、3 和一存取設備 1，連接於局部網路。全部共有網路的成對局部鍵 $K_{PUB,LOC}$ ， $K_{PRI,LOC}$ ，網路內始終有一獨特繁殖器，為最後接至網路的呈現設備。

新存取設備連接至局部網路的部份遠較簡單，因本發明的任何存取設備是不含鍵出售。尤其可以構想在新存取設備插入網路內時，即遞送訊息超過匯流排 B，要求接收網路的私鍵。即可提供接收此訊息的第一網路設備，或只有繁殖器設備，以因應此訊息，遞送網路的私鍵至新存取設備。

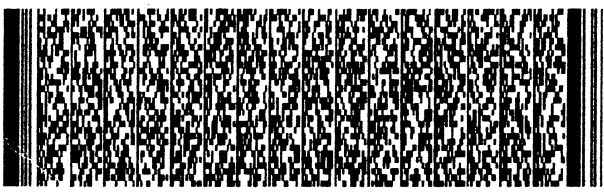


第1圖表示本發明局部數位式網路；
第2圖表示如第1圖所示數位式網路之產生方法；
第3圖表示新呈現設備對例如按照第2圖方法所產生局部數位式網路之連接方法。

元 件 符 號 說 明

- | | |
|----------------|---------|
| 1 | 存取設備 |
| 2, 3 | 呈現設備 |
| 4 | 數位式錄影機 |
| 10 | 數位式解碼器 |
| 11, 21, 31 | 智慧卡 |
| 12 | 多工解訊器電路 |
| 13 | 存取控制電路 |
| 14 | 轉換器電路 |
| 15 | 多工化電路 |
| 20, 30 | 數位式電視機 |
| 22 | 多工解訊器電路 |
| 23 | 終端模組 |
| 24 | 解密電路 |
| 100, 101, 102, | |
| 103, 104, 200, | |
| 200', 200" | 方法第一步驟 |
| 201, 202 | 第二步驟 |
| 203, 204, 205, | |
| 206, 207, 208, | |
| 209, 210, 211 | 步驟 |

煩請委員明示
修正本有無變更實質內容是否准予修正
90年12月20日所提之



四、中文發明摘要 (發明之名稱：數位式局部網路及其產生和更新方法)

局部數位式網路，包括：

— 存取設備(1)，以接收源自網路外界的資料，並在網路的一點發送；和

— 呈現設備(2,3)，以接收流入網路內之資料，並在網路的一點呈現。

資料以鎖碼形式在網路內流通，網路的所有設備使用單鍵，網路的局部鍵，以供資料鎖碼和解碼。網路的局部鍵以一對公鍵和私鍵形成為佳。

此網路之目的，在於可複印局部網路內的資料，同時防止盜印專屬於其他局部網路用之資料。

第1圖。

英文發明摘要 (發明之名稱：DIGITAL LOCAL NETWORK, NOTABLY DIGITAL HOME NETWORK, AND METHOD FOR CREATING AND UPDATING SUCH A NETWORK)

The local digital network comprises:

- access devices (1), for receiving data originating from outside the network and transmitting them at a point of the network ; and
- presentation devices (2,3) for receiving the data flowing in the network and presenting them at a point of the network.

The data flow in the network in encrypted form and all the devices of the network use a single key, the local key of the network, for the



四、中文發明摘要 (發明之名稱：數位式局部網路及其產生和更新方法)

英文發明摘要 (發明之名稱：DIGITAL LOCAL NETWORK, NOTABLY DIGITAL HOME NETWORK, AND METHOD FOR CREATING AND UPDATING SUCH A NETWORK)

encryptino and decryption of the data. Preferably, the local key of the network is formed by a pair of public and private keys.

The purpose of this network is to make it possible to copy data in the local network whilst preventing pirate copies destined for other local networks.

Figure 1.



六、申請專利範圍

1. 一種局部數位式網路，尤指數位式家庭網路，包括
 —至少一存取設備(1)，可接收源自該網路外界的資料，並在該網路之一點發送；和

—至少一呈現設備(2,3)，適於接收流入網路之資料，以便在網路之一點呈現；

其中資料適於只以鎖碼型式流動，其特徵為，該網路的全部設備對於流入網路內資料之鎖碼和解碼，使用網路專屬之單一鎖碼鍵：網路局部鍵($K_{\text{PUB. LOC}}$, $K_{\text{PRI. LOC}}$)者。

2. 如申請專利範圍第1項之數位式網路，其中資料係使用公鍵密碼系統鎖碼，其特徵為，網路之該局部鍵是由一對公鍵和私鍵所形成：網路之局部公鍵($K_{\text{PUB. LOC}}$)和局部私鍵($K_{\text{PRI. LOC}}$)者。

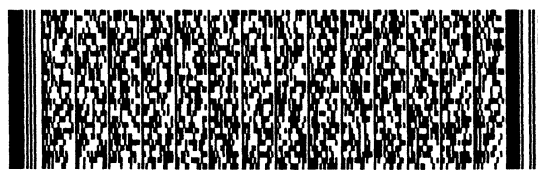
3. 如申請專利範圍第2項之數位式網路，其中只有接至該網路的呈現設備(2,3)才含有局部私鍵($K_{\text{PRI. LOC}}$)者。

4. 如申請專利範圍第3項之數位式網路，其中在指定情況下，網路有單一呈現設備獲准發送局部私鍵($K_{\text{PRI. LOC}}$)至適於連接至該網路之新呈現設備者。

5. 如申請專利範圍第3項之數位式網路，其中在指定情況下，呈現設備只能有下列狀態之一：

(i) 第一狀態，初生態($IE=00$)，呈現設備首度接至該網路；

(ii) 第二狀態，繁殖態($IE=01$)，呈現設備獲准發送網路之局部私鍵，至適於接至該網路之任何新呈現設備；



六、申請專利範圍

(iii) 第三狀態，滅絕態 ($IE=10$)，呈現設備不再獲准發送網路之局部私鍵，至適於接至該網路之任何新呈現設備；

呈現設備適於只變化狀態，以便通至較高階狀態者。

6. 如申請專利範圍第5項之數位式網路，其中網路之單一呈現設備在第二態，繁殖態：網路之繁殖器者。

7. 如申請專利範圍第6項之數位式網路，其中在指定情況下，網路之繁殖器為最後接至該網路之呈現設備者。

8. 一種呈現設備，適於接至申請專利範圍第2項之數位式網路，其特徵為，在指定情況下，該呈現設備只能下列狀態之一：

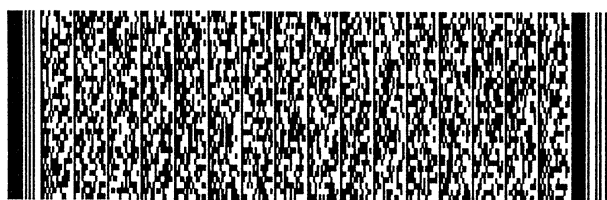
(i) 第一狀態，初生態 ($IE=00$)，呈現設備首度接至該網路；

(ii) 第二狀態，繁殖態 ($IE=01$)，呈現設備獲准發送網路之局部私鍵，至適於接至該網路之任何新呈現設備；

(iii) 第三狀態，滅絕態 ($IE=10$)，呈現設備不再獲准發送網路之局部私鍵，至適於接至該網路之任何新呈現設備；

該呈現設備係適於只變化狀態，以便通至較高階狀態者。

9. 如申請專利範圍第8項之呈現設備，其中當該呈現設備在初生態時，含有本身成對之公鍵和私鍵，並獲准接



修正
00-12-20
六六申請專利範圍

收適於連接的網路之成對局部鍵，加以儲存，以代替其本身之成對鍵者。

10. 如申請專利範圍第8或9項之呈現設備，其中當該呈現設備在滅絕態時，不再獲准接收適於連接的網路之成對局部鍵者。

11. 如申請專利範圍第8項之呈現設備，其中包括該呈現設備所佔狀態之儲存機構(IE)，整合於智慧卡(21, 31)內者。

12. 如申請專利範圍第8項之呈現設備，其中在智慧卡(21, 31)內含有網路之成對局部鍵，以提供該設備者。

13. 一種產生申請專利範圍第5項局部數位式網路之方法，其特徵為，包括下列接續步驟：

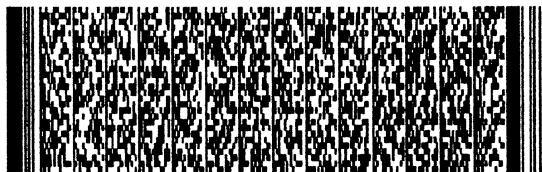
(a)經由數位式匯流排(B)，把存取設備(1)和初生態的呈現設備(2)連接在一起，含有一對公鍵(K_{PUB2})和私鍵(K_{PRI2})；

(b)對於呈現設備(2)，遞送其公鍵(K_{PUB2})越過該匯流排(B)；

(c)對於存取設備(1)，接收該公鍵(K_{PUB2})，儲存成為網路之新局部公鍵($K_{PUB.LOC}=K_{PUB2}$)，並將呈現設備的狀態變化信號遞送越過該匯流排；

(d)對於呈現設備(2)，接收該狀態變化信號，並通至繁殖態(IE=01)者。

14. 一種將在初生態(IE=00)並含有一對公鍵(K_{PUB3})和私鍵(K_{PRI3})的新呈現設備(3)，接至申請專利範圍第5項局部



六、申請專利範圍

數位式網路之方法，包括如下接續步驟：

(e)經由數位式匯流排(B)，將新呈現設備(3)接至該局部網路；

(f)對於新呈現設備(3)，遞送其公鍵($K_{\text{PUB}3}$)越過該匯流排；

(g)對於該網路之至少一存取設備(1)，接收新呈現設備之公鍵($K_{\text{PUB}3}$)，證實該存取設備已含有公鍵，網路之局部公鍵($K_{\text{PUB.LOC}}$)，以及在正面證實時，遞送網路之局部公鍵越過匯流排(B)；

(h)對於新呈現設備(3)，接收網路之局部公鍵($K_{\text{PUB.LOC}}$)，加以儲存，並將設址於網路所有呈現設備的信號，遞送越過該匯流排，要求從繁殖態呈現設備回應；

(i)對於網路(2)之繁殖器呈現設備，通至滅絕態($\text{IE}=10$)，並回應新呈現設備(3)，以鎖碼型式遞送網路之局部私鍵($K_{\text{PRI.LOC}}$)，可利用新呈現設備(3)解碼；

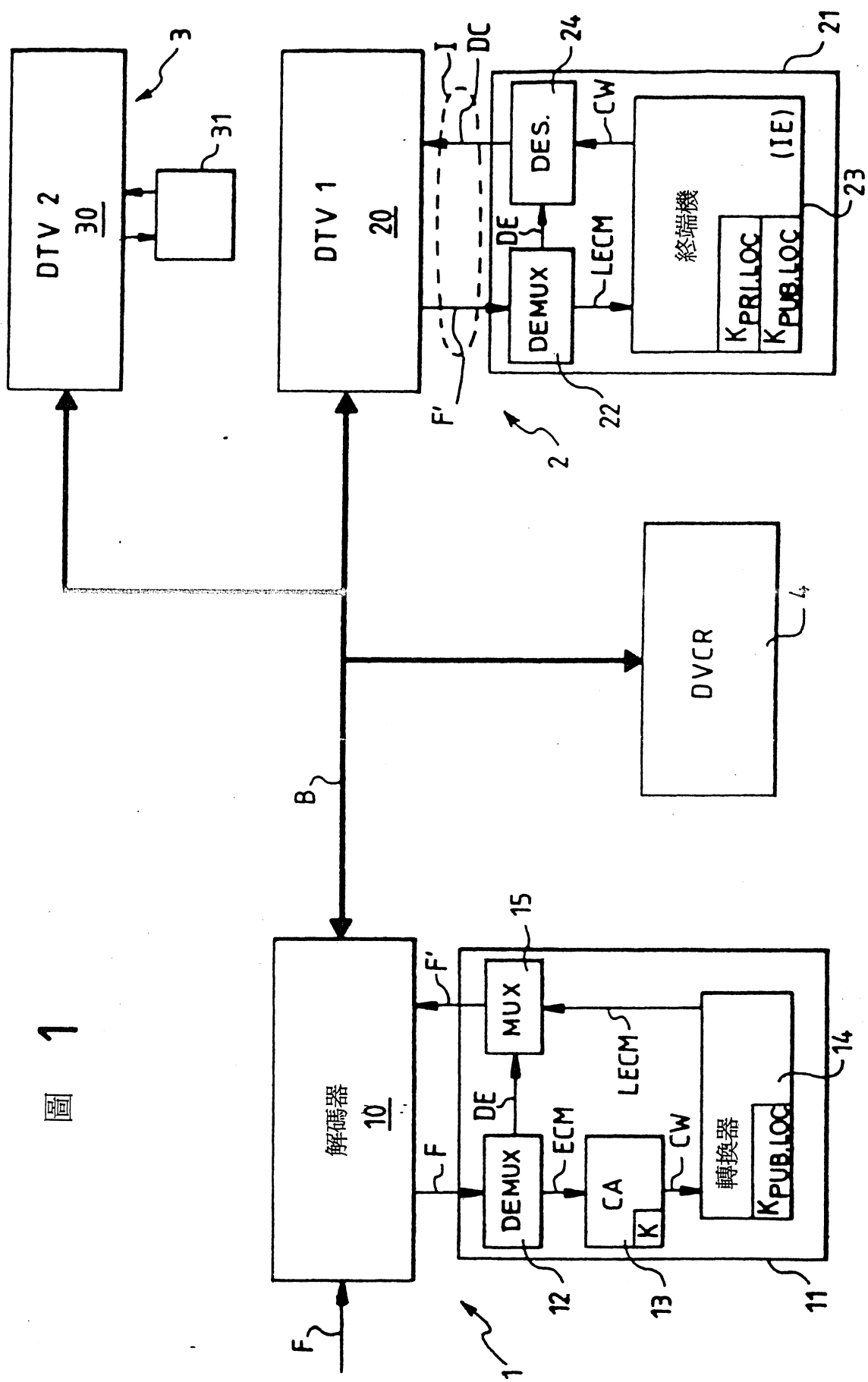
(j)對於新呈現設備(3)，接收網路之該局部私鍵($K_{\text{PRI.LOC}}$)，加以儲存，並遞送接受信號至原先為網路(2)繁殖器之呈現設備；

(k)對於原先為網路(2)繁殖器之呈現設備，接收該接受信號，並遞送狀態變化信號至新呈現設備(3)；

(l)對於新呈現設備(3)，接收該狀態變化信號，並通至繁殖態($\text{IE}=01$)者。



圖 1



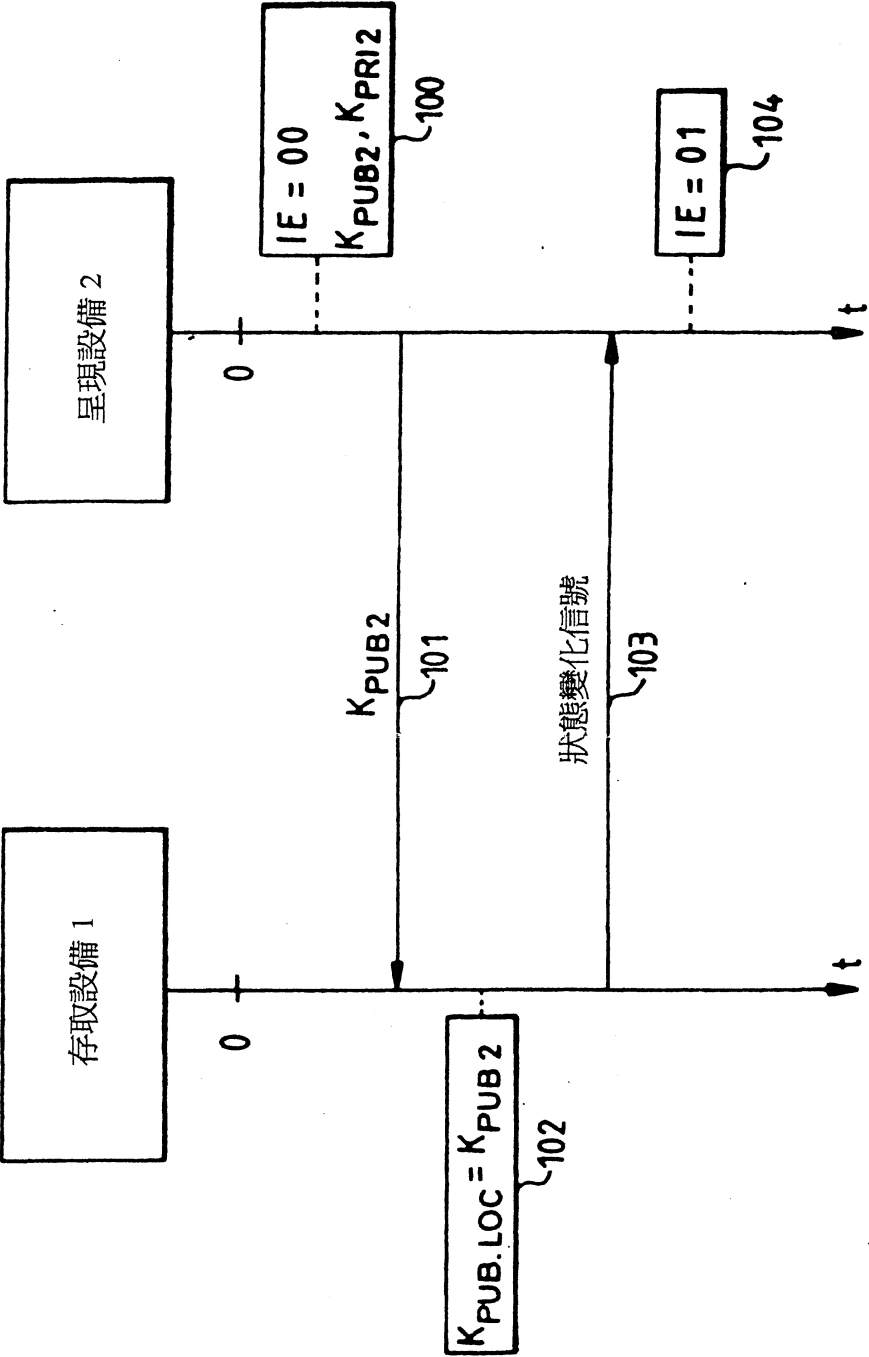


圖 2

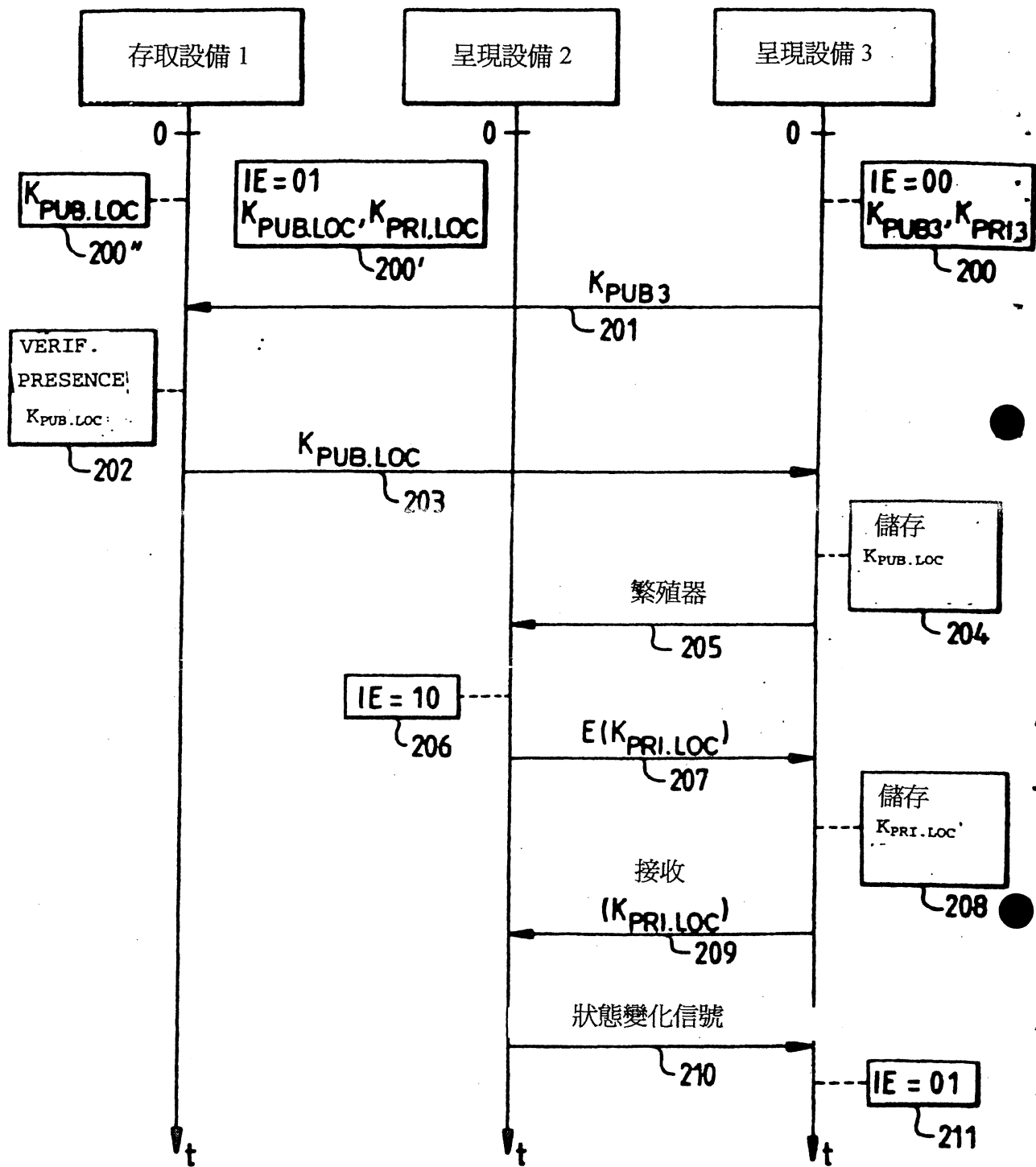


圖 3