公告本

申請日期： 94.4.11	案號： P1107266
類別： H04L 29/06	

（以上各欄由本局填註）

發明專利說明書 I221719

一、發明名稱	中文	通訊網路中對稱鍵之管理方法及其裝置
	英文	PROCESS FOR MANAGING A SYMMETRIC KEY IN A COMMUNICATION NETWORK AND DEVICES FOR THE IMPLEMENTATION OF THIS PROCESS
二、發明人	姓名（中文）	1.迪哈爾 2.安德瑞克 3.杜瑞德
	姓名（英文）	1.Diehl, Eric 2.Andreaux, Jean-Pierre 3.Durand, Alain
	國籍	1.法國 2.法國 3.法國
	住、居所	1.法國萊福爾市拉巴勒戴爾 2.法國勒恩市盧德羅格尼爾20號 3.法國勒恩市盧德迪納79號
三、申請人	姓名（名稱）（中文）	1.法商・湯姆生特許公司
	姓名（名稱）（英文）	1.Thomson Licensing 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.盧籃
	代表人姓名（英文）	1.Ruellan, Brigitte

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
法國 FR	2001/04/25	0105568	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)

發明領域

本發明一般係關於局部數位網路領域，尤指數位家庭網路領域。

背景技藝

此種網路包含集體裝置，利用數位匯流排聯結在一起，例如按照IEEE 1394標準之匯流排。尤其包括二種裝置：

—源裝置，可發射資料跨越網路：此等裝置可經網路外部的「波道」回收資料；

—接收裝置，適於接收流過網路之資料，以便加以處理或呈給使用者。

因此，以旨在傳送聲頻和／或視頻資料至屋內各室的數位家庭網路為例，源裝置係例如為數位解碼器，從網路外接收視頻節目，經由衛星天線或電纜接線，或是光碟閱讀機，越過網路廣播，以數位形式，從碟片（在此情況下，碟片含有源自網路外的資料）閱讀資料（聲頻和／或視頻）。接收裝置為例如電視機，可以觀看從網路接收到的視頻程式，或更一般言之，包含可將鎖碼資料解碼能力之任何器具。

從提供源自局部網路外的資料之內容提供者，尤其是廣播每次觀看付費的電視節目或例如其他光碟出版者之服務提供者觀點言，必須防止此等發射資料受到拷貝，和容易（例如拷貝到光碟或任何其他記錄媒質上）從一局部網路流至其他網路。

為此，已知以祕密方式實施發射資料，即借助密碼學

五、發明說明 (2)

演算加以鎖碼，使用獲得授權接收此等資料的器具，或按照內容提供者與此等器具間之特別安全議定，事先所知之鍵。

Thomson Multimedia於2000年3月31日提出的PCT專利申請案WO 00/62505，並主張1999年4月13日同一申請人所申請法國專利案公告FR 2792482號為優先權，係關於家用網路，使用網路專屬的公鍵，把網路器具間，典型上為前述源裝置至接收裝置流動之資料鎖碼。只有此網路的器具擁有私鍵，相當於公鍵。(私鍵－公鍵)成對專屬於網路，此網路的架構內之鎖碼資料，不能用另一網路的器具解碼。

使用成對不對稱鍵有些優點，但也有若干缺點。主要優點之一是，源器具內不儲存祕密；此等器具明知公鍵，但不知私鍵。然而，不對稱鍵的實施較對稱鍵為少。再者，不對稱鍵的壽命短，需要定期變更，而創造新鍵。在此情況下，用鍵鎖碼再記錄之資料，會在網路上突然不再解碼。此外，必須要有相當大量的成對不對稱鍵。

實施對稱鍵把資料鎖碼頗引人注目。然而，需要源裝置明白此鍵，而此舉會賦予更多安全上的拘束，因而成本更高。

發明概述

本發明之標的係通訊網路中對稱鍵管理方法，包括第一種裝置，具有要經網路廣播的資料源，和至少一個第二種裝置，旨在接收該資料。此法包括如下步驟：

五、發明說明 (3)

(a)利用第一種裝置，決定第一種對稱鍵，並以安全方式傳輸第一鍵，到至少一個第二種裝置；

(b)利用至少一個第二種裝置，接收第一對稱鍵，借助網路第二種裝置已知之第二對稱鍵，把第一對稱鍵鎖碼，並將此鎖碼結果傳輸到第一種裝置；

(c)利用第一種裝置，回收和儲存第一對稱鍵之鎖碼。

若第一種裝置必須發射資料到至少一個第二種裝置，則方法繼續下列步驟：

(d)利用第一種裝置，借助第一對稱鍵，把要發射到至少一個第二種裝置的資料鎖碼；

(e)利用第一種裝置，把鎖碼資料和第一鎖碼對稱鍵，傳輸到至少一個第二種裝置；和

(f)利用至少一個第二種裝置，借助第二對稱鍵，把至少一個第二種裝置鎖碼之第一對稱鍵解碼，並借助如此回收的第一對稱鍵，把鎖碼資料解碼。

因此，借助對稱鍵(上述第一鍵)可達成把要從第一種器具，典型上為網路存取通路，諸如衛星接收機／解碼器，發射至第二種器具，典型上為顯示裝置之資料鎖碼。

此第一鍵之傳輸是借助第二鍵，按照較佳具體例，亦為對稱，以鎖碼方式進行。

對稱鍵較不對稱鍵為短，可節省記憶空間。此外，對稱演算較不對稱演算為快：必要的計算電力較少。同時，在第一種裝置內未儲存長期祕密(典型上為第二鍵)，此裝

五、發明說明 (4)

置只擁有第一鍵，容易經常更換，以所構想用途為函數，即時而且是對使用者透明的方式。

此外，第一和第二鍵，只要是對稱，即可隨機選用，不需由第三者權威證明，因而節省成本。

鎖碼的記錄資料(按照非限制性具體例的保密器控制字)亦借助對稱鍵，不擁有任何預程式規劃的屆止日期。所以，在回放之際沒有第一鎖碼鍵不再可行之虞：後者可以儲存，本身借助第二鍵鎖碼，連同相同資料。

按照特殊具體例，第一種裝置與複數之第一非鎖碼對稱鍵，和相對於非鎖碼鍵的第一鎖碼對稱鍵並聯儲存。尤其是此舉容許第一種裝置預測一或以上第二種裝置停掉或其他原因不可得之時機，此時即不產生新的第一對稱鍵。因此，第一種裝置即可得預先產生的複數第一鍵，甚至在網路上第二種器具不可得時，可以前後接踵使用。尤其是鎖碼資料可充分良好供第三種器具(例如記錄裝置)之用。

按照特殊具體例，第一對稱鍵是至少在新系列資料傳輸之際更新，或在系列資料傳輸之際有若干次。視安全性的需要，意即視所構想的用途，第一對稱鍵會或多或少頻頻更新。

按照特殊具體例，本發明方法又包括第二種新裝置在網路內安裝階段，安裝階段包括步驟為，證明在網路內預先有第二種裝置存在，擁有第二對稱鍵，有能力安全發射，還有在正面時，把第二對稱鍵傳輸至第二種新裝置之步驟，在負面時，利用第二種新裝置產生第二對稱鍵之步

五、發明說明 (5)

驟。

安裝階段旨在使第二對稱鍵，亦稱網路鍵，通訊至網路的全部接收機。

本發明標的亦涉及適於連接至通訊網路之通訊裝置，包括：

— 資料鎖碼機構，部署鎖碼演算，實施第一對稱鍵；

— 記憶體，包括借助聯結於網路的至少一接收裝置已知第二鍵，加以鎖碼之第一對稱鍵；和

— 在網路上傳輸借助鎖碼機構加以鎖碼的資料之機構。

最好是第二鍵亦為對稱鍵。

按照特殊具體例，利用上述通訊裝置鎖碼的資料，首先被解鎖。

按照特殊具體例，利用通訊裝置鎖碼的資料是首先鎖碼，但利用裝置解碼，以便以所示方式再度鎖碼。為此，裝置可有源自鎖碼資料源的解碼機構。此源可例如為衛星、地面或有線電視網路，其中資料以鎖碼方式流動。

按照另一特殊具體例，要利用通訊裝置鎖碼的資料首先鎖碼，再以所示方式鎖碼一次。

然而，較佳具體例中，資料在再度鎖碼饋送入網路之前，加以解碼。

按照另一較佳具體例，設有鎖碼機構以便頻頻更新第一對稱鍵。

五、發明說明 (6)

本發明標的又涉及在通訊網路中之資料處理裝置，包括：

—從網路器具以鎖碼方式接收第一對稱鍵之鎖碼機構，第一對稱鍵的鎖碼是借助第二對稱鍵完成；

—含有網路指定類別器具全部共同的第二對稱鍵之記憶體；和

—借助第一對稱鍵把從網路所接收鎖碼資料之解碼機構。

按照具體例，該裝置包括從網路所接收資料之解密機構，解密機構使用借助第一對稱鍵進行資料解碼的結果。

按照特殊具體例，含有第二對稱鍵的記憶體，又包括一對不對稱鍵，用於安全傳輸第一對稱鍵至該處理裝置。處理裝置又包括借助第二對稱鍵將第一對稱鍵鎖碼之機構，回到已發射第一對稱鍵之網路器具。

圖式簡單說明

本發明其他特徵和優點，參見附圖所示非限制性特殊具體例之說明，即可更為明白，附圖中：

第1圖為實施本發明方法具體例連接若干器具的通訊網路方塊圖；

第2圖為通訊網路內新接收裝置安裝過程之流程圖；

第3圖為說明對稱網路鍵在此鍵(Progenitor)的處理裝置和進行安裝於網路的接收裝置間交換對稱網路鍵之時序圖；

第4圖為說明送出鎖碼資料的源裝置和接收該資料的

五、發明說明 (7)

接收裝置間通訊之時序圖，通訊按照本具體例實施對稱鍵。

本發明具體例之詳細說明

先說明通訊網路例，以詳細表明資料和各種鍵交換方式。隨後，產生和傳輸各種鍵，在接收裝置安裝於網路的架構內，或在源裝置和接收裝置間之資料傳輸。

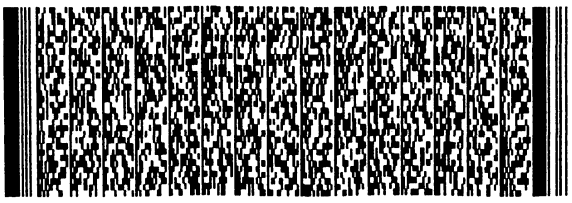
1. 網路說明

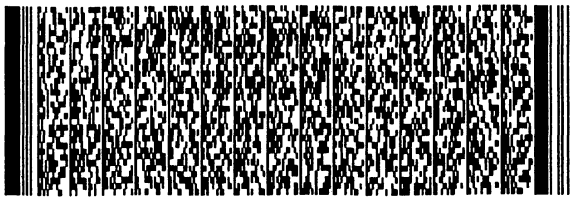
第1圖所示為數位家庭網路，包括源裝置1、二接收裝置2和3、數位視頻記錄器4，通常稱為DVCR(數位視頻卡匣記錄器)。裝置1,2,3,4集體插入家用數位匯流排B，例如為IEEE 1394標準之匯流排。

源裝置1包括數位解碼器10，裝有晶片卡閱讀機，提供晶片卡11。此數位解碼器10具體而言，是插入衛星天線或有線網路內，以接收服務提供者分佈之視頻節目。此等節目接收在資料流下內，例如以MPEG-2格式。按現有已知方式，是以利用控制字CW保密的形式發射，此等控制字本身是在資料流下內，按照指定鎖碼演算，以借助K鍵鎖碼的形式發射，以便在傳輸之際保持祕密。

因此，只有服務提供者授權的使用者，才准許對發射資料解密(例如經訂戶付費)。為此，提供者對授權的使用者供應K鍵，用來對控制字CW解碼。往往授權接收節目只是暫時，只有在使用者付訂費期間。所以，K鍵要由服務提供者規則性修改。

鑑於本發明，由下述可見，使用者誠然在作為訂戶時





五、發明說明 (8)

可記錄所發射節目，並在其本身網路上隨他願意回放多次，甚至K鍵已更換。另方面，由於資料是按上述以保密方式記錄，可僅在使用者已記錄的網路上回放。

在第1圖內，網路所示狀態是全部器具已按照下述方法插入。第1圖特別對源裝置1和接收裝置2，表示各裝置內所含全部鍵，所示鍵不一定呈現在裝置內的每一時刻。典型上，裝置1不儲存裝置2的公鍵PUB2超過後述對稱鍵Kc之交換，而裝置2不儲存對稱鍵Kc超過同樣的交換。

尤其是，各接收裝置包括記憶體內之對稱網路鍵Kn。此鍵分佈給利用所謂「正統」接收器具之一新接於網路的接收器具。

此外，各接收裝置擁有一對不對稱鍵(PRIVx,PUBx)，第一鍵為私鍵，第二為公鍵。此等鍵可在網路器具確認架構內使用，並供交換對稱鍵。

茲說明如何處理解碼器10所接收流F內所發射資料。以按照MPEG-2格式發射的資料而言，資料流F包括接續之視頻資料訊包、聲頻資料訊包、管理資料訊包。管理資料訊包特別包括控制訊息ECM(代表「定名控制訊息」)，其中以借助K鍵鎖碼的形式發射的控制字CW，用來對在視頻和聲頻資料訊包中發射的資料保密。

此資料流F發射至晶片卡11，以便在其內處理。利用多工解訊器模組(DEMUX)12接收，模組一方面把ECM發射至存取控制模組(CA)13，另方面把保密視頻和聲頻資料訊包DE發射至多工化模組(MUX)15。CA模組含有K鍵，因此把

五、發明說明 (9)

ECM內所含控制字CW解碼。CA模組把此等控制字CW發射至按照本發明含有對稱鍵Kc之轉換器模組14。隨後可見此鍵之產生和器具間之傳輸。

轉換器模組14使用對稱鍵Kc，把控制字CW鎖碼，並將借助對稱鍵Kc鎖碼的此等控制字發射至控制訊息LECM內之多工化模組15。此等訊息LECM與初始資料流F內所接收功能相同，即發射控制字CW，但是在訊息LECM內，控制字CW借助對稱鍵Kc在其內鎖碼，而非借助服務提供者的K鍵鎖碼。

鍵Kc最好經常更新，例如在發起各資料傳輸時，旨在防止源裝置包括長期祕密，否則需要增進保護。

多工化模式15再發射利用解碼器10所接收資料流F'內之資料訊包DE和轉化之控制訊息LECM。就是此資料流F'再流過室內匯流排B，以便利用接收裝置2或3之一，或利用數位視頻記錄器4，加以接收，以便記錄。

除借助對稱鍵Kc鎖碼的控制字傳輸外，源裝置把鍵Kc本身發射至接收裝置，但利用演算E2借助鍵Kn加以鎖碼，意即發射E2{Kn}(Kc)。

在其餘說明中，記號"E{K}(D)"始終用來意指利用演算E以鍵K將資料D鎖碼。

鍵Kn(以下稱為網路鍵)不在於源器具，而在接收器具。隨著鍵Kc的創造，以安全方式發射至接收器具，借助Kn加以鎖碼，把結果再發射至源器具，供隨後使用。

按照本發明，所以資料始終以鎖碼方式在匯流排B內

五、發明說明 (10)

流動，只有存取於對稱鍵Kc的器具可將控制字CW解碼，所以把該資料DE解碼。此等器具係擁有網路鍵Kn。此舉可防止廣播至在第1圖室內網路所為任何拷貝之其他局部網路。

在第1圖實施例內，模組12至15係整合於晶片卡11內，但在變化具體例中，可把模組DEMUX和MUX放入解碼器10內，只留模組13和14整合於晶片卡內。尤其是因為模組CA 13和轉換器模組14含有解碼和鎖碼鍵，必須整合於晶片卡等安全媒質內。

接收裝置2包括數位電視接收機(DTV1)20，裝有晶片卡閱讀機，提供晶片卡21。接收機20接收源自解碼器10或數位視頻記錄器4，通過匯流排B之資料流F'。資料流F'發射至晶片卡21。利用多工解訊器模組(DEMUX)22接收，一方面發射保密視頻和聲頻資料訊包DE呈解密模組(DES)24，另方面把轉化控制訊息LECM發射至終端模組23，以及鎖碼鍵E2{Kn}(Kc)。

終端模組23首先借助所擁有的網路鍵Kn解碼E2{Kn}(Kc)，以獲得對稱鍵Kc。再者，因控制訊息LECM含有已借助鍵Kc鎖碼的控制字CW，終端模組可借助剛算出的鍵Kc，把此等控制字解碼，以獲得明碼電文的控制字CW。控制字CW再發射至解密模組24，用來把資料訊包DE解密，並輸出明碼電文資料訊包DC至電視接收機20。

E2{Kn}(Kc)宜包含於各LECM訊息內。在此情況下，鍵Kc不必利用接收裝置長期儲存。此外，可快速(快如控制

五、發明說明 (11)

字CW)回收，以容許有用資料快速解密。當使用者逐站躍進(「跳台」)，或新接收器具插入網路內，同時發射視頻流(「熱插」)，此舉特別重要，有助於鎖定。

為了在晶片卡21和電視接收機20的顯示電視間之明碼電文資料DC最後傳輸安全起見，該晶片卡和接收機20的卡閱讀機間之介面，可按照NRSS美國標準(國家更新性安全標準)使晶片卡安全。

第二接收裝置3包括數位電視接收機(DTV2)30，裝有晶片卡閱讀機，供應晶片卡31，其操作方式與接收裝置2完全相同，不再贅述。

鑑於上述局部數位網路，源自內容提供者的資料流F，是利用接收之源裝置轉型入資料流F'內，其中資料(更準確而言為電碼字CW)以對稱鍵Kc鎖碼。鍵Kc連同借助其鎖碼的資料一同發射，而其本身借助另一對稱鍵，即網路鍵Kn鎖碼。此資料流F'即包含具有局部網路專屬格式之資料，該資料可以只能利用都含有網路鍵Kn的局部網路之接收裝置解碼。

此外，由於鍵Kc是和資料(以鎖碼形式)一同廣播，可在資料同時例如利用數位視頻記錄器(DVCR)4加以記錄，因而容許隨後存取於鎖碼資料。

此外，由於網路鍵Kn不儲存於源裝置，後者即不含有需要增加安全注意的任何「長期」祕密。

2.對稱網路鍵(Kn)之分佈

網路的全部接收裝置必須擁有對稱網路鍵(或祕密鍵)

五、發明說明 (12)

Kn。此鍵利用網路的特殊接收裝置(正統)發射至新的接收裝置。

各接收裝置可為如下狀態之一：處女(Virgin)、正統(Progenitor)、「不孕」(Sterile)。

處女接受裝置的界定是，事實上不包括對稱網路鍵Kn。此典型上為尚未連接於網路之裝置。此為接收裝置的預設狀態。

不孕裝置的界定是事實上擁有對稱網路鍵Kn，但不能發射至另一裝置。

正統裝置的界定是事實上擁有對稱網路鍵Kn，而且可發射至網路的其他裝置。在網路內只能存在一正統裝置。

裝置狀態利用狀態指示器IE(為位於接收裝置的終端模組23內的2位元暫存器)儲存。在習知上，假設裝置為處女狀態，則狀態指示器IE等於00，若裝置為正統狀態，IE=01，而裝置在不孕狀態時，IE=10。

狀態指示器IE最好包含在晶片卡的積體電路內，以保證其防竊。

在接收裝置安裝中，有若干情況需要分辨，視情形為網路內業已存在的接收裝置之狀態。

第2圖的流程表示在安裝過程中由接收裝置採取的各種核對和動作。

第一次安裝步驟2.0後，新的接收裝置先核對網路內是否為正統裝置(步驟2.1)。若答案為正，對新接收機之興起進行新接收機和正統裝置之認證步驟(步驟2.2)。此

五、發明說明 (13)

項認證是基於例如使用二裝置之成對不對稱鍵，並實施迄今為精於此道之士所知之認證演算。一旦已進行此認證，正統裝置即以安全方式發射鍵Kn至新的接收機(步驟2.3)。後者即採取不孕狀態，因而修飾其暫存器IE，因而終止安裝(步驟2.9)。

按照變化具體例，當安裝新的接收裝置，並檢測網路內有正統裝置存在時，新裝置即採取正統狀態，強迫前述正統裝置進入不孕狀態。

若網路內無正統裝置存在，新裝置核對是否網路之至少有一不孕接收機存在(步驟2.4)，雖然無正統裝置存在。若情況如此，則不可能安裝，而程序停止(步驟2.5和2.9)。誤差訊息發射給使用者，例如在新接收機的顯示板上。然而，即使在此情況下，現有不孕裝置可接收來自網路源裝置的鎖碼資料，並加以解碼。

回到第2圖之流程，以網路包括既無正統裝置又無不孕裝置的情況而言，新的接收機產生鍵Kn(步驟2.6)，此鍵典型上為128位元鍵，以便與目前所用的對稱鎖碼演算一致(例如AES演算，字母代表「高級鎖碼標準」，亦稱為Rijndael，由J. Daemen和V. Rijmen在〈國家標準科技協會(NIST)第一屆高級鎖碼標準候選會議記錄〉(1998年8月)內有說明，或是TwoFish演算，載於B. Schneier, J. Kelsey, D. Whiting, D. Wagner, N. Feignson等人所寫論文〈TwoFish，一種方塊鎖碼演算〉，發表於同一NIST會議報告)。

五、發明說明 (14)

鍵Kn可隨機選擇。一旦此鍵已產生，新接收機即宣稱其本身為正統裝置，並因而修飾其暫存器IE之內容(步驟2.7)。則產生接收器具的網路(步驟2.8)，製程即告結束(步驟2.9)。

第3圖說明新接收機安裝之際，在新接收裝置和預存在正統裝置間的交換。

當網路上安裝新的接收裝置時，接收裝置含有一對證明鍵，公鍵PUBr和私鍵PRIVr，按照本發明，是在處女狀態(狀態指示器IE=00)。接收裝置起先發射(步驟3.1)其公鍵PUBr至正統裝置。後者借助公鍵PUBr把鍵Kn鎖碼(步驟3.2)，並將鎖碼結果發射至接收裝置(步驟3.3)。後者借助私件PRIVr把此等資料解碼(步驟3.4)，因此回收鍵Kn。接收裝置變成網路的新正統裝置(其暫存器IE成為01狀態)，而前一正統裝置如今在步驟3.5中成為不孕(暫存器IE=10)。

為保證鍵Kn的完整性和原點，正統裝置根據此鍵並經由已知演算，發生訊息認證電碼(MAC)，此電碼連同鎖碼資料E{PUBr}(Kn)，在步驟3.3內送出。在步驟3.4內，利用接收機核對。演算HMAC-SHA-1(代表Keyed-Hash Message Authentication Code)，是可在此架構內使用的演算之一例。

3.短期對稱鍵和資料鎖碼之交換

假設剛安裝且成為上述方法中對稱網路鍵Kn處理機的新接收裝置，係第1圖之接收裝置2。此裝置即備妥從源裝

五、發明說明 (15)

置1接收資料。

第4圖表示在此方面交換的訊息。

首先(步驟4.0)，源裝置1發出對網路的要求，要求公鍵PUBx傳輸至任何接收裝置。網路上存在的全部接收裝置此時以送回其公鍵加以响應。假設在源裝置1所接收第一鍵之後，是在步驟4.1過程中利用接收裝置2送出的公鍵PUB2。源裝置考慮到所接收的第一訊息，則相當於相對應接收裝置。

源裝置產生並儲存「短期」對稱鍵Kc(步驟4.2)，該鍵用來把控制字CW鎖碼。按照本發明具體例，對稱鍵是隨機選用，最好擁有128位元長度。鍵Kc借助公鍵PUB2，經由非對稱鎖碼演算E1鎖碼，例如RSA-OAEP演算(代表Rivest, Slanir, Adlenan Optimal Asymmetric Encryption Padding，載於PKCS#1:RSA密碼學規格，2.0版，1998年10月)，然後以鎖碼方式E1{PUB2}(Kc)發射至接收裝置(步驟4.4)。後者借助私鍵PRIV2把鍵Kc鎖碼，又按照對稱鎖碼演算E2，借助對稱網路鍵Kn再度鎖碼(步驟4.5)，把如此鎖碼的Kc(即E2{Kn}(Kc))送回到源裝置(步驟4.6)，把此資訊項儲存(步驟4.7)。

須知源裝置不知祕密鍵Kn。

按照本發明具體例，在源裝置和接收裝置間連接開始時，創造鍵Kc。Kc可在實施連接之前，充分產生Kc，在連接之際，Kc亦可修飾一次或多次。在此情況下，步驟4.0至4.7，基本上旨在從網路的接收裝置，利用需要重複的

五、發明說明 (16)

網路鍵，獲得鍵Kc的鎖碼。

步驟4.8至4.11係關於有用資料的傳輸。

由源裝置1接收之資料包括訊息ECM。源裝置把後者解碼，以便由此抽出控制字CW，再借助對稱鍵Kc，經由對稱鎖碼演算E3，把控制字CW解碼(步驟4.8)。源裝置再把此等鎖碼控制字(即E3{Kc}(CW))又插入資料流內，全部發射越過匯流排B，前往接收裝置(步驟4.9)。又在步驟4.9中，源裝置送出借助Kn鎖碼並已在步驟4.7中儲存的鍵Kc。

又須知在步驟4.9內發射之有用資料，係按照對稱鎖碼演算E4，借助控制字CW鎖碼。

接收裝置可借助Kn解碼E2{Kn}(Kc)(步驟4.10)，並處理Kc，可存取控制字CW，因而將有用資料解密(步驟4.11)。

演算E2,E2,E4可相同或不同。例如可用上述AES演算或TwoFish演算。

發射借助對稱網路鍵Kn鎖碼的Kc，暗示只有網路的接收裝置可存取Kc。此外，若干接收裝置可同時把送出的資料解碼。

在鍵Kc創造之際，必須有至少一接收裝置以上述方式安裝，置於網路內，把經網路鍵Kn鎖碼的Kc發射至已發生此鍵Kc的源裝置。然而，利用源裝置發射並部份借助此鍵鎖碼之資料，可充用於網路之另一器具，諸如記錄器具，不一定擁有所記錄資料的解碼功能。

按照具體例之變化，源裝置把借助網路鍵Kn鎖碼的若

五、發明說明 (17)

干鍵Kc，在下一次資料傳輸之先，以相對應鍵Kc儲存。

雖然按照本實施例，基本上控制字CW是利用源裝置解碼，並借助對稱鍵Kc再鎖碼，惟本發明不限於此實施例。尤其是其他資料可以解碼，再借助此鍵鎖碼。此外，某些資料可借助對稱鍵鎖碼，然而不需利用源裝置先加以解碼。在後一情況下，必須思考到使接收裝置可以安全方式製成鍵K(為進行將第一鎖碼加以解碼所需)。

最後，要利用源裝置鎖碼的資料可以非鎖碼形式達成。

此外，本發明不限於聲頻／視頻資料的傳輸。任何種資料，均可以規定方式發射。

圖式簡單說明

第1圖為實施本發明方法具體例連接若干器具的通訊網路方塊圖；

第2圖為通訊網路內新接收裝置安裝過程之流程圖；

第3圖為說明對稱網路鍵在此鍵(Progenitor)的處理裝置和進行安裝於網路的接收裝置間交換對稱網路鍵之時序圖；

第4圖為說明送出鎖碼資料的源裝置和接收該資料的接收裝置間通訊之時序圖，通訊按照本具體例實施對稱鍵。

四、中文發明摘要　(發明之名稱：通訊網路中對稱鍵之管理方法及其裝置)

通訊網路包括第一種裝置(1)，設有要在網路上廣播的資料源，以及至少一個第二種裝置(2)，旨在接受該資料。對稱鍵管理方法包括如下步驟：

－源裝置(1)決定第一對稱鍵(Kc)，安全發射(E1{PUB2}(Kc))到至少一接收裝置(2)；

－接收裝置(2)接收第一對稱鍵(Kc)，借助網路的接收裝置(2)所知第二對稱鍵(Kn)鎖碼，並發射至源裝置；

－源裝置(1)回收第一對稱鍵(Kc)之鎖碼(E2{Kn}(Kc))，並加以儲存。

在資料(CW)發射到至少一接收裝置(2)之前，源裝置(1)借助第一對稱鍵(Kc)鎖碼(E3)此等資料，再將編碼資料(E3{Kc}(CW))附帶第一鎖碼對稱鍵(E2{Kn})(Kc))發射

英文發明摘要　(發明之名稱：PROCESS FOR MANAGING A SYMMETRIC KEY IN A COMMUNICATION NETWORK AND DEVICES FOR THE IMPLEMENTATION OF THIS PROCESS)

The communication network comprises a device of a first type (1) furnished with a source of data to be broadcast over the network and at least one device of a second type (2) intended to receive the said data. The symmetric key management process comprises the following steps:

- the source device (1) determines a first symmetric key (Kc) and transmits it securely (E1{PUB2}(Kc)) to at least one receiver device (2);

四、中文發明摘要　（發明之名稱：通訊網路中對稱鍵之管理方法及其裝置）

到至少一接收裝置(2)。

接收裝置借助其擁有的第二鍵(Kn)，把第一對稱鍵(Kc)解碼，再借助所回收第一對稱鍵，把鎖碼資料解碼。

本發明亦涉及實施此法用之裝置。

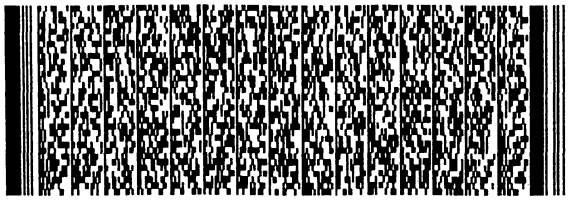
第4圖。

英文發明摘要　(發明之名稱：PROCESS FOR MANAGING A SYMMETRIC KEY IN A COMMUNICATION NETWORK AND DEVICES FOR THE IMPLEMENTATION OF THIS PROCESS)

- a receiver device (2) receives the first symmetric key (Kc), encrypts it (E2) with the aid of a second symmetric key (Kn), known to the receiver devices (2) of the network and transmits it to the source device;

- the source device (1) recovers the encryption (E2{Kn}(Kc)) of the first symmetric key (Kc) and stores it.

Before transmitting the data (CW) to at least one reception device (2), the source device (1)



四、中文發明摘要　(發明之名稱：通訊網路中對稱鍵之管理方法及其裝置)

英文發明摘要　(發明之名稱：PROCESS FOR MANAGING A SYMMETRIC KEY IN A COMMUNICATION NETWORK AND DEVICES FOR THE IMPLEMENTATION OF THIS PROCESS)

encrypts (E3) these data with the aid of the first symmetric key (Kc), then it transmits these encryped data (E3{Kc}(CW)), accompanied by the first encrypted symmetric key (E2{Kn}(Kc)), to at least one receiver device (2).

The receiver device (2) decrypts the first symmetric key (Kc) with the aid of the second key (Kn) which it possesses, then it decrypts the encrypted data with the aid of the first symmetric key thus recovered.

四、中文發明摘要　（發明之名稱：通訊網路中對稱鍵之管理方法及其裝置）

英文發明摘要　（發明之名稱：PROCESS FOR MANAGING A SYMMETRIC KEY IN A COMMUNICATION NETWORK AND DEVICES FOR THE IMPLEMENTATION OF THIS PROCESS）

The invention also pertains to devices for implementing the process.

Figure 4.

六、申請專利範圍

1.一種通訊網路內的對稱鍵管理方法，網路包括：

—第一種裝置(1)，提供資料源，可供在網路上廣播，和

—至少一個第二種裝置(2)，旨在接收該資料，此方法之特徵為，包括如下步驟：

(a)利用第一種裝置(1)，決定(4.2)第一對稱鍵(Kc)，並以安全方式(E1{PUB2}(Kc))把第一鍵(Kc)傳輸(4.4)到至少一個第二種裝置(2)；

(b)利用至少一個第二種裝置(2)，接收第一對稱鍵(Kc)，借助網路第二種裝置(2)已知的第二對稱鍵(Kn)把該第一對稱鍵鎖碼(E2)，並將此鎖碼結果傳輸(4.6)到第一種裝置；

(c)利用第一種裝置(1)，把第一對稱鍵(Kc)的鎖碼(E2{Kn}(Kc))回收和儲存者。

2.如申請專利範圍第1項之方法，又包括如下步驟：

(d)利用第一種裝置(1)，借助第一對稱鍵(Kc)，把要發射到至少一個第二種裝置(2)之資料(CW)鎖碼(E3)；

(e)利用第一種裝置(1)，把鎖碼資料(E3{Kc}(CW))和第一鎖碼對稱鍵(E2{Kn}(Kc))傳輸(4.9)到至少一個第二種裝置(2)；

(f)利用至少一個第二種裝置(2)，借助第二對稱鍵(Kn)把至少一個第二種裝置所鎖碼的第一對稱鍵(Kc)解碼(4.10)，並借助如此回收的第一對稱鍵(Kc)，把鎖碼資料解碼(4.11)者。

六、申請專利範圍

3.如申請專利範圍第1或2項之方法，其中第一種裝置(1)把複數的第一非鎖碼對稱鍵(Kc)和相當於非鎖碼鍵的第一鎖碼對稱鍵(E2{Kn}(Kc))並行儲存者。

4.如申請專利範圍第1項之方法，其中第一對稱鍵係至少在新系列資料傳輸中更新，或在系列資料傳輸中更新多次者。

5.如申請專利範圍第1項之方法，其中又包括第二種新裝置在網路上安裝階段，安裝階段包括網路上預先第二種裝置存在，擁有第二對稱鍵(Kn)並具有安全發射能力之證明步驟(2.1)，以及

在正面時，把第二對稱鍵(Kn)傳輸至第二種新裝置之步驟，和

在負面時，利用第二種新裝置，發生第二對稱鍵(Kn)之步驟(2.6)者。

6.一種通訊裝置(1)，適於連接至通訊網路，該裝置包括：

—鎖碼資料(CW)之解碼機構(14)，

其特徵為，鎖碼機構(14)採用解碼演算(E3)，實施第一對稱鍵(Kc)，而其中裝置又包括：

—記憶體，包括借助連接至網路的至少一接收裝置(2)已知的第二鍵(Kn)加以鎖碼(E2{Kn}(Kc))之第一對稱鍵；和

—在網路上傳輸借助鎖碼機構(14)加以鎖碼的資料之機構(10,15)者。

六、申請專利範圍

7.如申請專利範圍第6項之裝置，又包括源自鎖碼資料源的資料之解碼機構(13)者。

8.如申請專利範圍第7項之裝置，其中設有鎖碼機構(14)，以便對第一對稱鍵(Kc)頻頻更新者。

9.如申請專利範圍第6項之裝置，其中第二鍵(Kn)係對稱性者。

10.一種在通訊網路上資料(2)之處理裝置，包括：

—從網路上器具以鎖碼方式(E2{Kn}(Kc))接收的第一對稱鍵(Kc)之解碼機構(23)，第一對稱鍵已借助第二對稱鍵(Kn)進行鎖碼；

—記憶體，含有網路上指定器具全部共用的第二對稱鍵(Kn)；和

—借助第一對稱鍵(Kc)，把從網路(LECM)接收的鎖碼資料加以解碼之機構(23)者。

11.如申請專利範圍第10項之裝置，其中該裝置包括把從網路接收的資料解密之機構(24)，該解密機構係使用借助第一對稱鍵(Kc)進行資料解碼(LECM)之結果(CW)者。

12.如申請專利範圍第10或11項之裝置，其中記憶體又包括對該處理裝置(2)安全傳輸第一對稱鍵(Kc)用之一對不對稱鍵(PRIV2,PUB2)，而該裝置又包括第一對稱鍵(Kc)借助第二對稱鍵(Kn)之鎖碼機構(23)，以便回到已發射第一對稱鍵(Kc)之網路器具(1)者。

P11072266

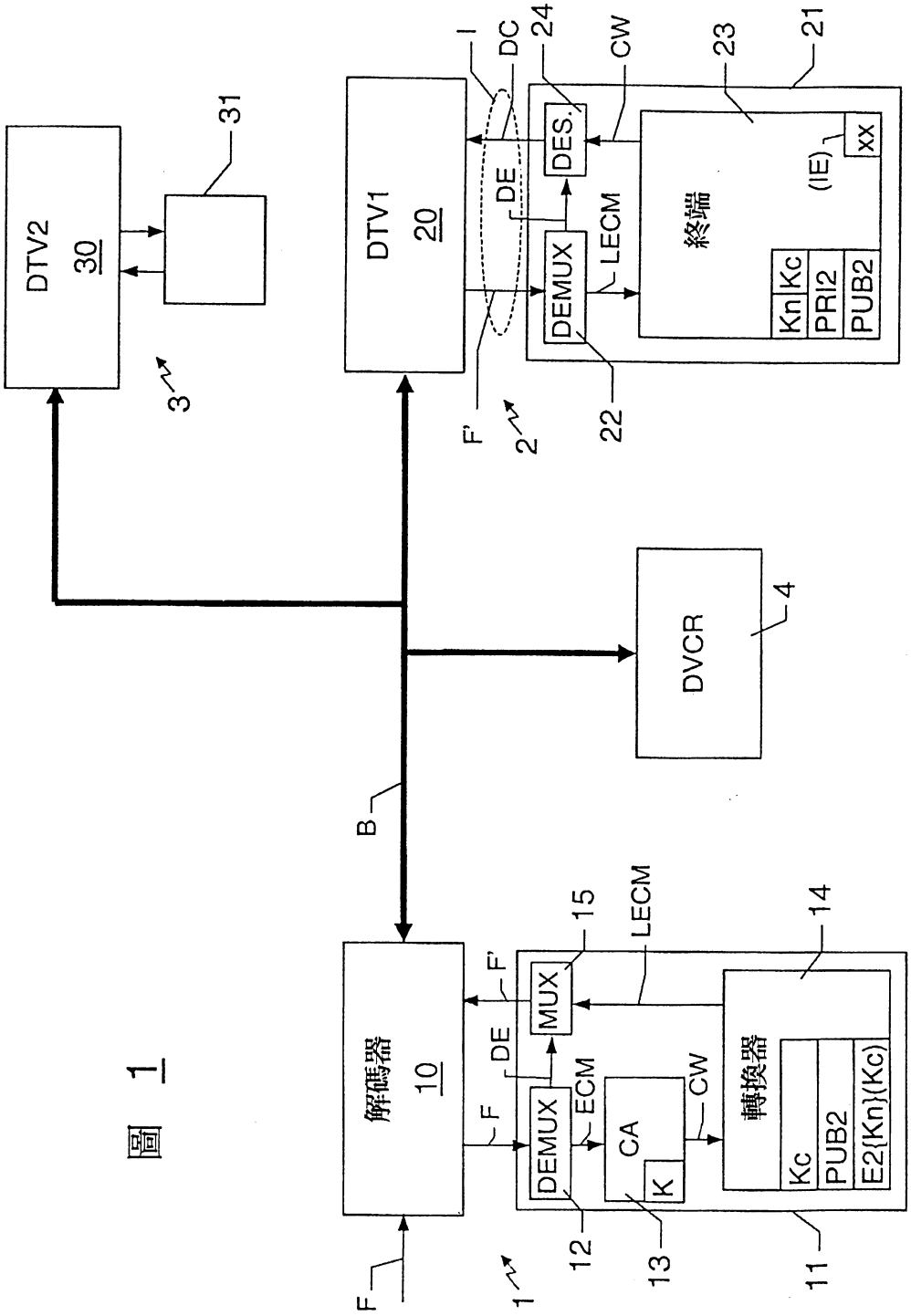


圖 1

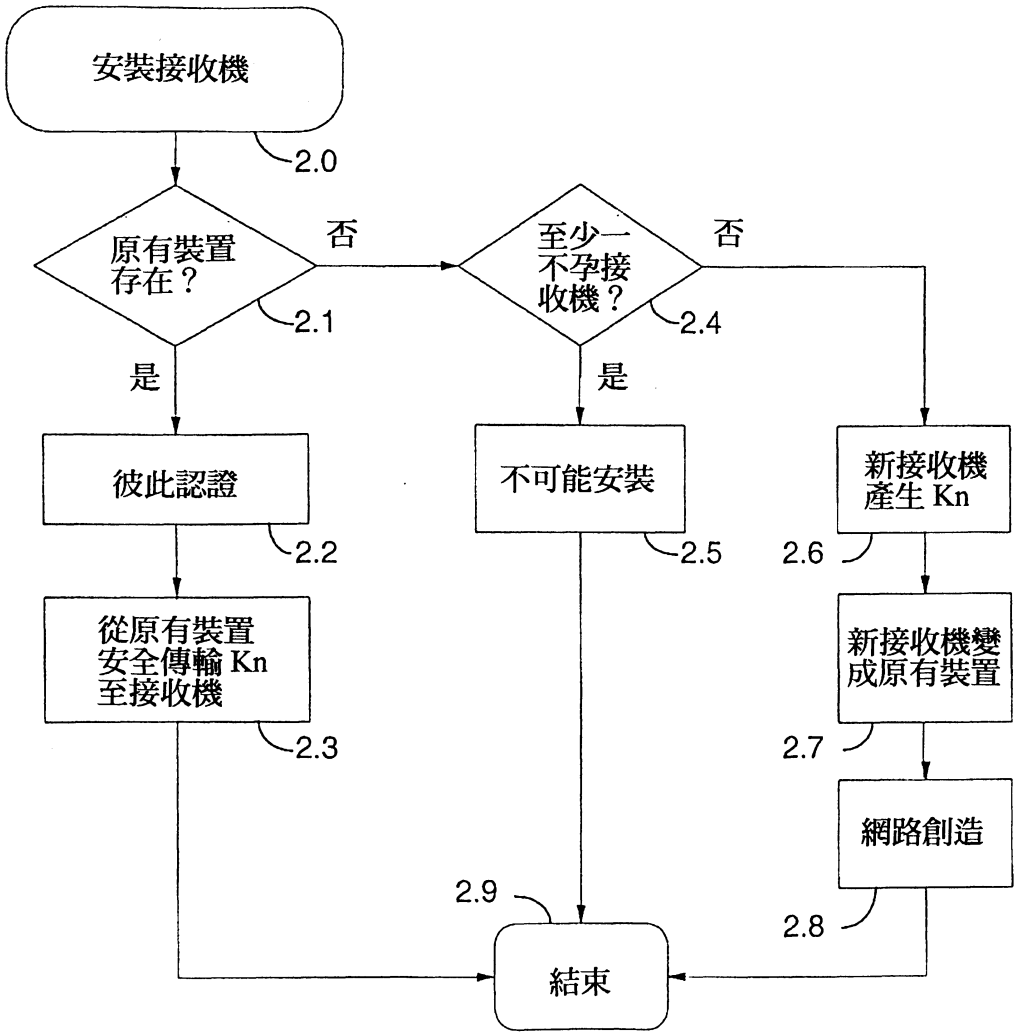

安裝接收機
2.0
原有裝置存在？
否
2.1
是
至少一不孕接收機？
否
2.4
是
彼此認證
2.2
從原有裝置安全傳輸 Kn 至接收機
2.3
不可能安裝
2.5
新接收機產生 Kn
2.6
新接收機變成原有裝置
2.7
網路創造
2.8
2.9
結束

圖 2

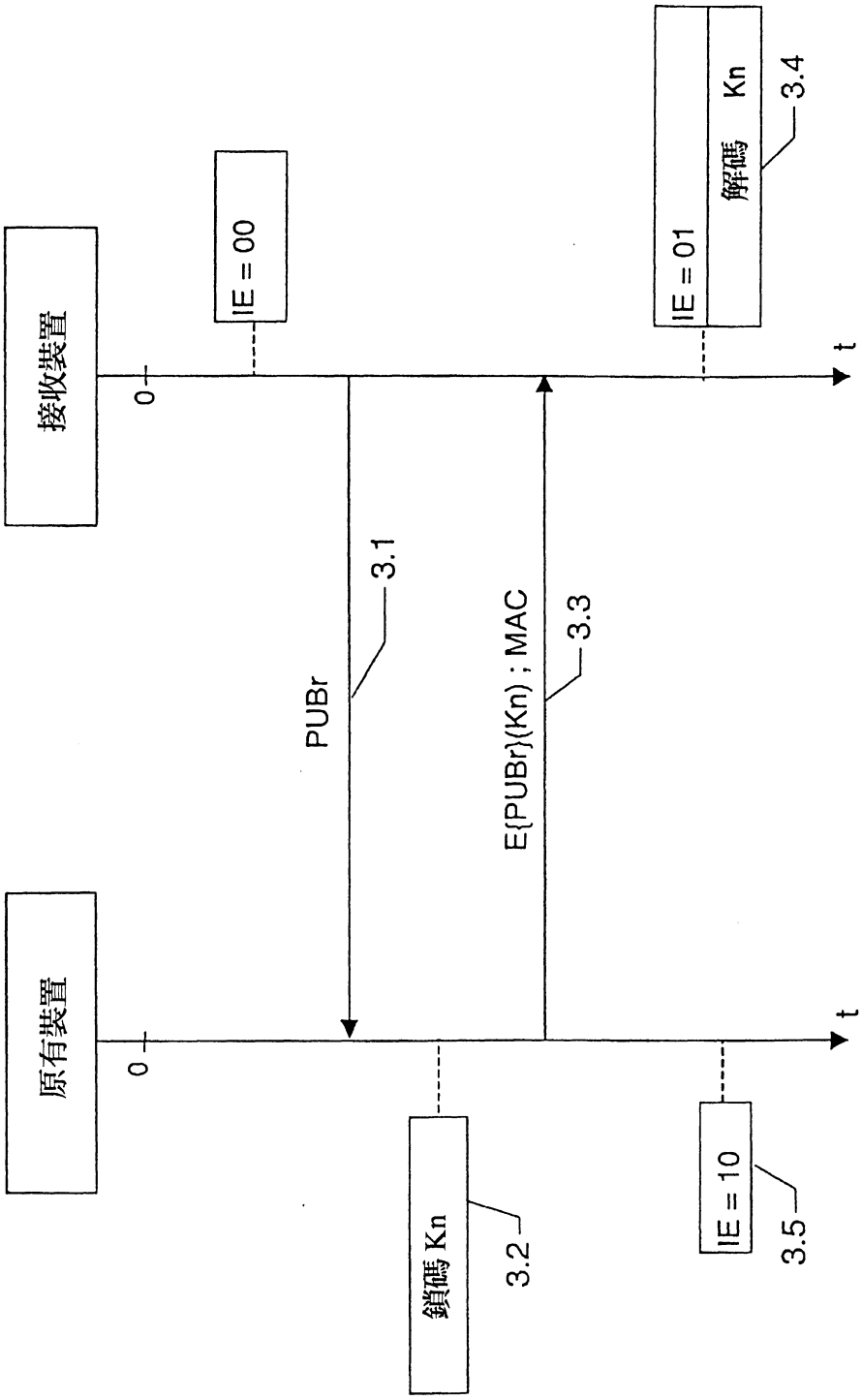

接收裝置
原有裝置
0
0
IE = 00
IE = 01
解碼 Kn
3.4
PUBr
3.1
E{PUBr}(Kn) ; MAC
3.3
鎖碼 Kn
3.2
IE = 10
3.5
t
t

圖 3

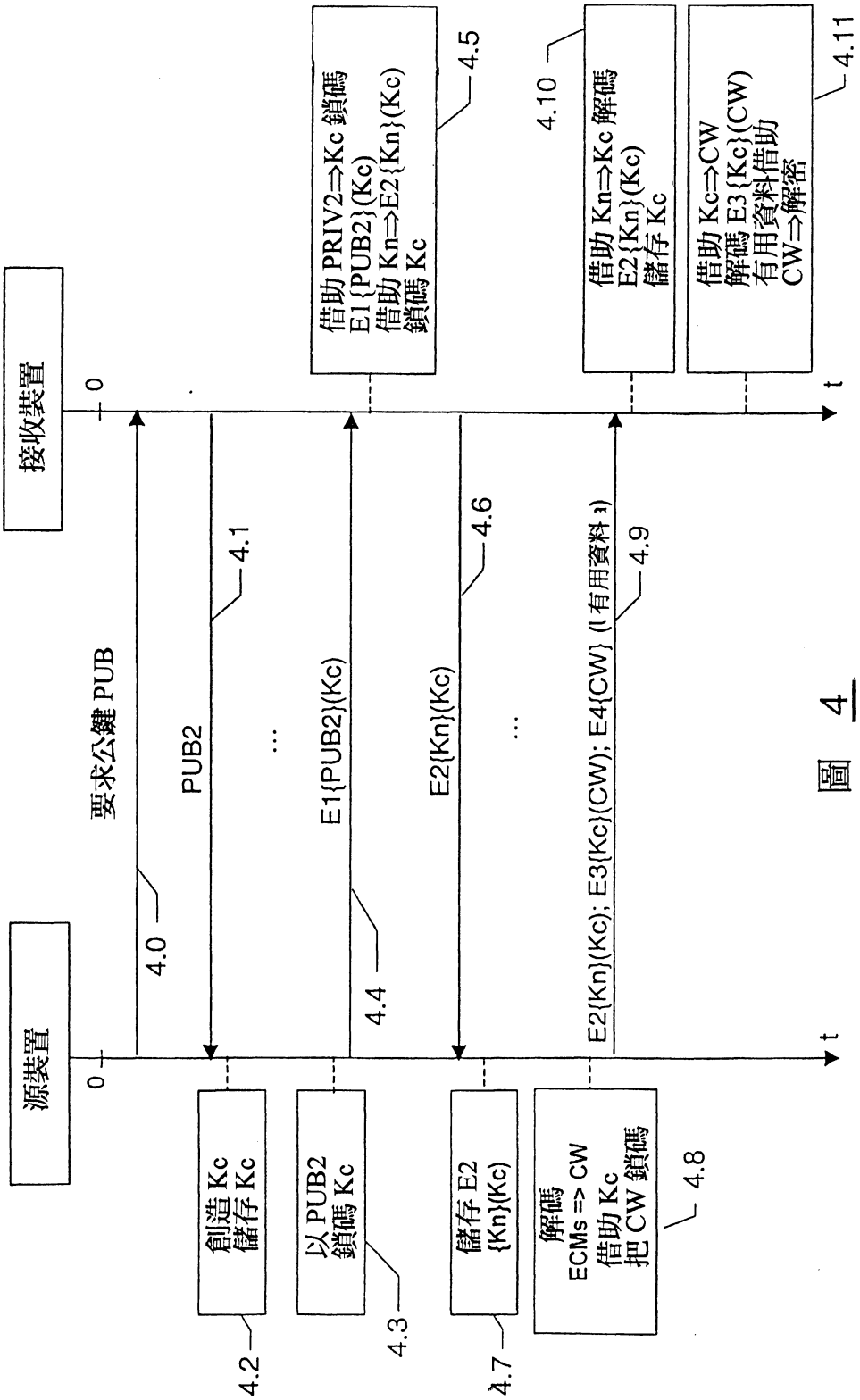

源裝置
接收裝置
0
0
t
t
要求公鍵 PUB
4.0
PUB2
4.1
...
E1{PUB2}(Kc)
4.4
E2{Kn}(Kc)
4.6
...
E2{Kn}(Kc); E3{Kc}(CW); E4{CW} (1有用資料1)
4.9
借助 PRIV2⇒Kc 鎖碼
E1{PUB2}(Kc)
借助 Kn⇒E2{Kn}(Kc)
鎖碼 Kc
4.5
借助 Kn⇒Kc 解碼
E2{Kn}(Kc)
儲存 Kc
4.10
借助 Kc⇒CW
解碼 E3{Kc}(CW)
有用資料借助
CW⇒解密
4.11
創造 Kc
儲存 Kc
4.2
以 PUB2
鎖碼 Kc
4.3
儲存 E2
{Kn}(Kc)
4.7
解碼
ECMs => CW
借助 Kc
把 CW 鎖碼
4.8

圖 4