

公告本

申請日期	90.10.26
案 號	90126590
類 別	H04L12/64, H04L12/66, G06F11/00

A4
C4

550949

(以上各欄由本局填註)

發明專利說明書

一、發明 名稱	中 文	用於多媒體多重播放內容的初始自由預覽
	英 文	"INITIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT"
二、發明 人	姓 名	1.佩 佩特卡 PETR PETERKA
	國 籍	美國
	住、居所	美國加州珊迪格市卡明多為司塔露喬路5126號
三、申請人	姓 名 (名 稱)	美商通用儀器公司 GENERAL INSTRUMENT CORPORATION
	國 籍	美國
	住、居所 (事務所)	美國賓夕法尼亞州哈爾宣市東奈曼特路101號
	代 表 人 姓 名	查爾斯 M. 費雪 CHARLES M. FISH

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6
B6

本案已向：

國（地區） 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權

美國 2000年10月26日 60/243,925 ☒有☐無主張優先權

有關微生物已寄存於： 寄存日期： ，寄存號碼：

裝
訂
線

五、發明說明(1)

相關專利之交互參照

本專利申請案是在2000年10月26日所申請的美國專利案號60/243,925，其在此僅列出供參考。

本發明大致係有關於多重播放網路的領域。更明確而言，本發明係有關在網路上提供配送給客戶端的一節目預演部分。

發明背景

有多種系統可將例如視聽內容配送給網路使用者。一範例是觀賞付費，其中一使用者可在觀看節目前付費。另一範例是以預約為基礎的節目，其中一使用者可對一服務供應者預約付費，為了要於一預先配置的時段接收一特殊頻道節目。例如，HBO™或SHOWTIME™是以預約為基礎的節目範例，其中一使用者可按月付費，為了要在指定的頻道上接收有關這些節目的任何廣播節目。因此，使用者不需要針對在這些特殊頻道上發生的每一個別秀或事件付費。相反地，預約付費可涵蓋所有節目。

隨著多重播放網路的出現，例如電影及音樂的節目內容目前可於網路以多重播放傳輸配送。例如，一伺服器可於網際網路上將一電影多重播放給客戶端電腦。此可藉著將內容同時配送給每位客戶端的位址達成。然而，沒有編密系統的出現有助於此傳輸的商業化。即是，沒有編密系統允許一使用者可預先觀看稍後可變成編密及無法由使用者利用的一節目。

結果，大部分的多重播放傳輸必須傳輸給預先已知對節

五、發明說明(2)

目內容感興趣的一組客戶端。節目內容供應者不能藉著提供節目的一自由預覽而將其他感興趣的觀眾引誘購買節目，此將減少節目內容供應者的商業利益。

發明概述

在本發明的一具體實施例中，用以多重播放節目內容的一方法可藉由提供配送給一客戶端的編密節目內容而提供；提供可由客戶端使用的密鑰；將編密節目內容的一第一部分編密；將該編密節目內容的第一部配送送給客戶端，其中該編密節目內容的該第一部分可編密，所以客戶端可使用該密鑰將節目內容解密，如此可獲得節目內容的一自由預覽。

在本發明的一具體實施例中，一內容密鑰可提供給客戶端，以允許客戶端可將編密節目內容的第一部分解密。同樣地，一自由預覽密鑰可在伺服器上用來將節目內容的第一部分編密、或將內容密鑰編密。

在另一具體實施例中，一使用者界面允許在一客戶端電腦上的使用者可購買在自由預覽期間提供的內容。

例如，在實際電影、或節目內容廣告、或實際電影的第一部分播放之前，自由預覽可採用一電影預告片形式。

在本發明的另一具體實施例中，用以多重播放該節目內容的一方法可藉由下列提供：提供配送給一客戶端的節目內容、以一未編密格式將該節目內容的一第一部配送送給客戶端、及將該節目的一其餘部配送送給客戶端。

一具體實施例允許提供一密鑰及利用該密鑰來完成節目

五、發明說明(3)

其餘部分的編密。此外，一具體實施例允許使用者可購買節目內容；及將一密鑰提供給使用者，用以將節目的編密部分解密。

本發明的仍然另一具體實施例可用以在一多重播放系統將節目內容提供給多重客戶端的一方法。該方法包含提供伺服器。用以與多重客戶端電腦通訊；配置伺服器，用以將一節目提供給複數個客戶端電腦；將節目的一自由預覽提供給多重客戶端電腦；及在自由預覽期間將密鑰提供給多重客戶端電腦，用以將該編密節目的至少一部分解密。

本發明的另一具體實施例提供具有可執行上述方法的電腦可執行指令之製造物件。

本發明的進一步具體實施例對於在技藝中熟諳此技者可從下連同附圖的描述而更顯然。用以實施本發明具體例的某些方法、裝置、與物件將說明。然而，可了解到本發明並未局限於揭露的細節，而是包括在本發明的精神及申請專利範圍內的所有此變化與修改。

圖式之簡單說明

圖1係例如在網際網路上用於節目內容多重播放之一內容配送系統的具體實施例方塊圖。

圖2是在圖1所示內容配送系統之一客戶端電腦部分的具體實施例方塊圖。

圖3係描述用以將一自由預覽提供給客戶端之本發明的一具體實施例流程圖。

圖4係描述用以提供自由預覽內容之本發明的另一具體

五、發明說明 (4)

實施例流程圖。

圖5係描述用以配送一節目的未編密部分及一節目的編密部分之本發明的一具體實施例流程圖。

圖6係描述允許顯示一自由預覽之本發明的一具體實施例流程圖。

圖7A和7B係顯示一節目部分期間的編密密鑰配送圖式。

圖8係描述在本發明的一具體實施例下的配送密鑰流程圖。

圖9係根據本發明的另一具體實施例的用以將該等密鑰配送的另一流程圖。

圖10係描述密鑰多重播放給多重客戶端之本發明的一具體實施例流程圖。

圖11係描述客戶端可從一伺服器接收密鑰，而用以接收多重播放內容之本發明的一具體實施例流程圖。

圖12係描述用以將密鑰配送給客戶端之本發明的一具體實施例，其中客戶端可傳送一密鑰接收的確認訊息。

圖13係描述本發明的一具體實施例流程圖，其中接收一節目的主動參加者清單可建立，而且客戶端可傳送表示他們是否保持在清單上的確認訊息。

圖14係描述本發明的一具體實施例流程圖，其中一修改的RTP封包可被建立，用以發信編密密鑰變化。

圖15係根據本發明的一具體實施例而描述用以在一多重播放系統中將一共同密鑰提供客戶端的流程圖。

五、發明說明(5)

圖16A和16B係根據本發明的一具體實施例而描述用以提供節目內容的一初始預演流程圖。

圖17係根據本發明的一具體實施例而描述一流程圖，用以提供購買節目內容的一調整初始密鑰配送時段。

圖18係根據本發明的一具體實施例而描述用以在節目內容的一最近購買客戶端上提供不中斷觀看。

圖19係顯示根據本發明的一具體實施例而使用的一網路。

圖20A和20B係根據本發明的一具體實施例而描述將資料記錄從一來源內容伺服器傳遞給一儲存伺服器的流程圖。

圖21係根據本發明的一具體實施例而描述一流程圖，其係基於與一儲存伺服器所使用節目內容有關的至少一規則而提供決定一客戶端是否需要節目內容。

圖22係根據本發明的一具體實施例而描述一資料結構，用以將資訊從一來源內容伺服器傳遞給一儲存伺服器。

圖23係根據本發明的一具體實施例而描述一資料記錄，其可提供一個別客戶端定義不同節目內容的特殊客戶端權限。

較佳具體實施例之說明

請即參考圖1，其係顯示一內容配送系統100的方塊圖。在此具體實施例中，內容配送系統100包括一主動清單104、一或多個來源伺服器108、一或多個客戶端電腦112、一或多個內容交換116、一或比較外部來源伺服器118、例如網際網路120的一網路、及一蠕動目錄124。一特殊客戶端電腦112的顯示是與主動清單104交談，以

五、發明說明(6)

選取用以下載的一內容物件。如果物件是一流傳媒體或可儲存而於稍後顯示，物件可在下載期間播放。內容物件可以是各種不同類型的資訊，例如聲訊、視訊、或可從網路下載的資料。此外，它可用於多重播放及/或單一播放。

在一些具體實施例中，來源伺服器108可決定客戶端電腦的較佳來源，為了要下載內容物件。客戶端電腦112的偏愛與內容物件副本的位置皆考慮來源伺服器108可用於將客戶端電腦重新導向給資訊的一較佳來源。來源可以是來源伺服器108本身、或該等內容交換116之中一者。

一外部來源伺服器118的內容物件可預先載入到一內容交換，以允許提供這些內容物件。若要當一內容物件首次要求而減少潛伏時，主動清單104可喚起外部來源伺服器118，以決定內容物件是否可從外部來源伺服器118獲得。可用內容物件可加入蠕動目錄124。只要可用內容物件已知，主動清單104便可從相關內容交換要求每個內容物件，為了要在相關的內容交換上載入每個內容物件。如此，內容物件可在相關的內容交換上預先載入。

圖2係廣泛描述來自圖1的個別系統元件如何在各種不同通常類似配置處理系統內以一分開或更整合方式實施。系統200的顯示係包含經由匯流排208而電耦合的硬體元件，包含一處理器201、輸入裝置202、輸出裝置203、儲存裝置204、電腦可讀儲存媒體讀取器205a、處理加速(例如，DSP、或特殊目的處理器)207的通訊系統206、與記憶體209。電腦可讀儲存媒體讀取器205a是進一步連

五、發明說明(7)

接到電腦可讀儲存媒體205b，該組合廣泛表示遠端、區域、固定及/或可移除儲存裝置與儲存媒體、記憶體等，用以暫時及/或更永久包含電腦可讀資訊，其中該電腦可讀資訊包括儲存裝置204、記憶體209及/或任何其他此存取系統200資源。系統200亦包含軟體元件(在工作記憶體291內顯示的目前位置)，包括一作業系統292及其他程式碼293，例如Applets、資料等的程式。

系統200可由於具有較大彈性及建構性而大規模選擇性實施。因此，例如，單一結構可根據目前想要的協定、協定變化、擴展等一步限制而用來實施一或多個伺服器。然而，在技藝中熟諳此技者可了解到實質各種不同變化可根據更特殊應用需求而實施。例如，一或多個元件可如同在一系統200元件(例如在通訊系統206內)內的子元件實施。自訂硬體亦可利用及/或特殊元件能以硬體、軟體(包括所謂例如applets的"可攜式軟體")、或兩者實施。此外，當連接到例如網路輸入/輸出裝置(未在圖顯示)的其他計算裝置可採用時，可了解到有線、無線、數據機及/或其他連接、或連接到其他計算裝置亦可利用。分散處理、多重位置檢視、資訊轉送、協同、遠端資訊取回與合併、及相關能力的每一者可考慮。作業系統的利用亦可改變，其是因特殊主機裝置及/或處理類型(例如電腦、設備、可攜式裝置等)而定，當然，不是所有系統200元件在所有情況皆需要。

圖1的網路能以各種方式實施。例如，根據一具體實施

五、發明說明 (8)

例，我們假設使用者資料封包協定(UDP)的使用可傳送"即時傳輸協定"/"即時控制協定"(RTP/RTCP)、"網際網路群管理協定"(IGMP)、"即時流協定"(RTSP)與可能的"交談聲明協定"/"交談描述協定"(SAP/SDP)。此外，對於多重播放定址目的而言，假設，多重播放IP位址配置與指定對於任何網際網路協定權限管理系統是顯而易見的。交談描述可使用SAP協定、RTSP ANNOUNCE命令或經由HTTP配送。而且，如一生業模型，可假設觀賞付費、預約、與按時間付費皆是所有想要的購買選項。此外。假設，相似電視的頻道是多重播放分散的一預期使用者廣播經歷。

在本專利中所使用的下列各項可如下面說明了解：

內容供應者 - 一實體，其可在不需使用內容時，將內容配送給例如儲存伺服器。

消費者 - 一實體，其可使用從一儲存伺服器獲得的內容，並且選擇性將內容配送給系統的其他消費者。消費者、儲存伺服器、與內容供應者的角色可視同與允許行為與傳輸有關的內容來源與接收端的一矩陣。

節目 - 具有一開始與結束的一段特別確認內容。

服務 - 在相同流的一連續節目收集。

進行中的節目 - 沒有一明確定義開始與結束的節目，觀賞者可隨時參加及離開。此適於"家庭購物"、"流行式樣顯示"、進行中的運動內容等。

購買選項 - 一機構，用以允許一客戶端購買內容。

預約 - 一購買機構，其中客戶端可註冊及可實質預先針

五、發明說明(9)

對內容付費。客戶端典型經認可獲得超過一節目(例如, 整個服務)。當只有一節目認可時, 此便是已知的呼叫前的觀賞付費(PPV)。

觀賞付費(PPV) - 一購買機構, 其中客戶端可每次駐冊及針對單一節目或錄音節目付費。此機構可網路啟動、或區域性啟動。在網路啟動情況, 只要想要購買, 客戶端便可接觸核心構造, 而且核心構造允許購買。由於在節目前的高度要求, 所以此方法時常具有計數問題。在時常稱為 "IPPV"、或"脈衝" PPV的區域啟動情況, 客戶端本身可區域購買, 並且可儲存購買的一記錄。在稍後時間, 記錄可向付費的核心構造系統報告。當事件多重播放, 例如, 在節目開始前, 沒有要求尖峰觸擊網路時, 此方法便有效的。而且, 客戶端可立即觀看內容, 當沒有網路潛伏或訊息交換延遲時, 在區域允許情況。在任何情況, PPV購買典型適用於整個節目, 而不管實際觀看多少。

按時間付費(PBT) - 一購買機構, 其中客戶端可依實際觀看內容持續時間付費。非連續時間增量於不同節目或服務會有不同的持續時間。PBT是局限於一觀眾可容許任意存取, 而沒有可感覺實用性損失的一小部分節目與服務。一些運動與音樂事件是屬於此類型。

依品質付費(PBQ) - 內容可亦一不同品質(亦即, 位元率)提供, 其中該品質可以是具品質加入內容的每個額外層的個別流或分層流。客戶端可報告它可使用的最高位元率, 及提供購買具品質或無品質內容。伺服器亦可基於網

五、發明說明 (10)

路的立即狀態而即時調整位元率。如果偵測到暫時網路阻塞，內容品質便會有一些時段降低，然後恢復廣告品質。伺服器可保持追蹤此發生，並且將他們報告給費用中心，費用中心可向使用者索取低於最初價格的費用。客戶端亦可根據使用者選擇而調整使用者可感覺的位元率。例如，一極短的節目對於使用者具有價值，但是並非是其成本等於一全螢幕客廳可觀看的節目。

購買時序 - 客戶端可於不同時間購買內容：

超越時間 - 客戶端可決定是否預先購買內容。此一購買是與例如預約的整個服務有關，而不是單一節目。

節目以前、或期間 - 客戶端可決定是否在內容開始之前、或非常接近開始的內容期間購買一短暫時間內容。

隨選即播 - VOD是基於儲存內容個別選擇而服務於單一消費者的點對點傳遞系統。消費者可喚起例如 '暫停'、'快速向前'、與 '回轉' 功能而控制他立即需要的觀看。

多重播放 - 多重播放是類似既有的電視廣播。它可同時將相同內容傳遞給一或多位消費者。此通常是被排程，而且可以是具活力的內容。

自由預覽 - 自由預覽是在消費者必須針對內容付費之前，允許他觀看一小部分內容(例如，數分鐘)的一機構。此可用來吸引使用者的滿足性。另一使用是可排除高伺服器路由的週期，例如當大部分消費者對內容註冊時，便開始PPV事件。當他的適合性有效時，消費者便允許觀看。(在自由預覽時段結束之後、或如果沒有預演，它便可藉由利

五、發明說明 (11)

用預先註冊客戶端所已知的一個別群密鑰而進一步排除高伺服器路由週期。)自由預覽能以較低品質提供。

來源內容伺服器(OCS) - 例如，可將內容提供給一儲存伺服器的一內容供應者電腦的伺服器。

購買模型

在內容的點對點VOD傳遞模型中，既然每個內容(事件)可個別協議，所以購買選項是相當簡單。因此，觀賞付費模型適於點對點VOD傳遞。此外，既然消費者-伺服器通訊典型是一雙向連接，所以存取內容協議的主要機構可在內容觀看之前完成(與傳統系統所採用的儲存及轉送IPPV機構相反)。

多重播放模型可提供不同機構，以便基於下列銷售內容：(1)消費者履行、(2)內容性質、或(3)內容的廣告方式。

觀賞付費

多重播放模型的觀賞付費(PPV)是類似點對VOD模型，其在於一客戶端可購買單一事件。一不同在於事件可編密一次，而且可由多客戶端共用；因此，一使用者電腦與儲存伺服器可不協議每位使用者的唯一內容編密密鑰。

另一不同是同時是在事件開始的同時有許多客戶端要求存取相同事件。此將會在相當小的時間窗框內於系統上產生較大負荷。若要允許可縮放，您可設定一自由預覽時段而將充足時間提供給儲存伺服器，以便將內容編密密鑰配送給所有參加者。

下列範例係描述觀賞付費模型實施的一具體實施例。此

五、發明說明 (12)

PPV 情況是類似 "隨選內容" 情況，其中使用者可決定獲得什麼內容及何時可獲得它。如果來源內容伺服器 (OCS) 偵測到客戶端並未預約，它便可藉著一組購買選項及其他內容存取規則與限制而指導客戶端。只要客戶端選取購買選項，它便可包括在安全物件內。安全物件亦可包括與特定內容有關的所有或一部分規則。

客戶端可將安全物件與具權限資料 (例如預約服務、位置、針對內容付費能力等的一清單) 的一憑單傳遞給儲存伺服器。儲存伺服器可檢查由客戶端所提供的安全物件與憑單，以決定來自安全物件的客戶端選擇及來自憑單的權限資訊是否符合內容存取規則。如果所有規則可滿足，當內容密鑰在節目密鑰下編密時，儲存伺服器將可藉著經由節目密鑰傳遞內容編密密鑰，例如節目密鑰可使用他唯一密鑰而傳遞給客戶端而存取要求的內容。

預約

在一具體實施例中，假設有許多 (數千或數萬) 隨選影像伺服器、及相當小量 (數百或數千) 的伺服器將可提供多重播放內容。當具有大部分時間可用內容的一連續流、且消費者想要回去時，預約模型便具有深遠意義。

如果觀眾預約服務，第一次觀眾可存取提供一服務密鑰給觀眾的服務，其中該服務密鑰具有比指定給單一節目事件的一節目密鑰更長的壽命。隨著此密鑰，觀眾可返回服務，必且觀看內容，而無需協議任何新密鑰。此將有助於建立電視頻道尖峰體驗。

五、發明說明 (13)

此一模型相關具體實施例的一目標是供儲存伺服器保持追蹤有多少客戶端、及客戶端何時實際觀看內容。為了說明目的，每次消費者造訪類似地面電視的Nielsen觀眾追蹤的此一服務時，一些消費者可要求接觸該伺服器，除了只有一新節目密鑰之外，一服務密鑰並不會提供給這些消費者電腦。此將會是在憑單中包括的一結構或一預約選項。

注意，預約模型對於當作影像租金的一致性月費率的點對點VOD情況亦是很有意義的。

下列範例係描述一預約模型實施的具體實施例。當一來源內容伺服器(OCS)變成一部分分散網路時，此表示它是否提供VOD內容或多重播放內容。如果一預約選項的多重播放提供，一供應中心可將一或多個服務IDs配送給OCS。

當客戶端/消費者想要預約此服務時，它需要提供一信用卡號或計帳的任何其他適當方法，而且在例如ESBroker環境的憑單認可憑單或伺服器憑單將使用預約服務清單及例如授權、支付能力等的其他授權資料更新。

當客戶端/消費者開始連接到一OCS時，它便可提供下列資訊：它的唯一消費者識別符、它的購買能力(信用卡號記錄及確認的一指示)、及它預約的一服務清單。如果OCS是提供付費內容，它便要先檢查客戶端/消費者是否可支付節目內容。如果內容可在一預約基礎上使用，預約服務的清單便能與OCS的服務IDs相比較檢查。如果OCS是在清單上，購買選單便可省略，而且客戶端可重新寫到適當的儲存伺服器。如果客戶端並未預約服務，它將可提

五、發明說明 (14)

供購買選項。在兩情況中，OCS將可建立一安全物件，其包括OCS服務ID、來源ID、選擇購買方法(例如，預約、PPV、PBT等)、與是否免費或支付內容的一指示、及其他存取規定。

當客戶端/消費者連接到可服務選取內容的儲存伺服器時，它便可將憑單提供給儲存伺服器，包括有關客戶端識別、購買能力、及從OCS獲得安全物件與預約服務清單的資訊。注意，客戶端不能讀取或改變來自OCS的憑單或安全物件。

儲存伺服器可將來自安全物件的資訊與憑單相比較。如果資訊符合，客戶端便允許存取內容(它將可提供在此情況可直接傳遞、或間接利用一服務密鑰的內容編密密鑰)。否則，存取內容將被拒絕。儲存伺服器亦可報告選取的購買選項及傳遞給計帳服務的費用資料。

客戶端可快取安全物件及服務密鑰，所以當它離開服務及隨後回來時，它便必重新接觸OCS或儲存伺服器(雖然對於使用者是簡明的，但是在取得時間會有延遲發生)。

注意，預約模式可經由下述PPV模式來模擬，而無需使用服務密鑰。儲存伺服器或費用系統將可偵測此客戶端是否為一用戶，因此不會對此服務的個別事件計帳。

按時間付費

按時間付費(PBT)適於不具有一充份定義開始或結束時間、或一自我包含時隙的內容，例如流行式樣秀或持續的運動事件(例如奧林匹克運動)。

五、發明說明 (15)

本發明的一些既有選擇性方法是基於密鑰的一樹狀結構、及當一消費者離開群時，可用以將子樹狀結構重新編密鑰之一演算法。這些既有的選擇性方法可處理較大的多重播放群，但是只有在如果離開群的消費者次數相當低及在整個時間上充份配送。另一方面，本發明的一具體實施例的設計可處理嘗試離開一多重播放消費者數量巔峰。

對於一對PBT方法而言，一儲存伺服器可將內容分成付費片段，而且可將片段密鑰配送給他們。所有消費者電腦可於每個片段中協議一密鑰，為了要保持追蹤他們觀看多少片段。此會在片段邊界上造成儲存伺服器的較大負荷。此可使用一密鑰管理方法而將負荷減少，其中每個片段可將密鑰提供給目前及下一片段。此將足夠時間提供給儲存伺服器，以便在目前片段期間配送下一片段密鑰。

下列範例係描述按時間付費模型實施的一具體實施例。一些內容不適於如同PPV銷售。一範例是沒有一明確定義開始與結束或一特殊構想的內容。此包括例如流行樣式秀、某類型運動事件等的內容。當觀眾使用OCS協議購買選項時，觀眾可依需要選取按時間付費選項。觀眾可被告知付費週期、及每個付費週期成本。觀眾的選擇將包括在一安全物件。

當客戶端將編密密鑰與儲存伺服器協議時，它將可開始接收多重播放內容。客戶端可監視每個付費週期的到期時間，及從儲存伺服器要求一新組的密鑰。如果觀眾停止觀看或移到另一服務，客戶端將不會要求新的密鑰，或它將

五、發明說明 (16)

主動通知儲存伺服器有關它想要離開目前多重播放期間。當每位客戶端參加及為了付費目的而離開多重播放時，儲存伺服器將可將時間記錄。

自由預覽

在本發明的一具體實施例中，一節目的自由預覽可提供給在多重播放系統的客戶端電腦。請即參考圖3，用以實施本發明的此具體實施例的一流程圖300可看出。在方塊304中，編密材料的可為了配送而提供給客戶端。例如，此編密材料可經由一內容交換而提供，例如一大都市影像交換、或內容起源的一來源伺服器。在方塊308中，一密鑰可在例如供應期間預先提供，以便供客戶端電腦將編密節目內容的第一部分解密。在方法300的方塊312中，編密節目內容的第一部分是配送給該等客戶端之中至少一者。最後，在方塊316中，客戶端允許利用可供獲得節目自由預覽部分的密鑰。因此，直到節目使用一不同密鑰編密為止，客戶端將可將節目內容解密，並且獲得節目的一預演，而無需收費。

因此，服務供應者可經由等待一預定時間量將編密的密鑰改變而允許一使用者獲得節目內容的一第一部分。此將允許一使用者藉由編密密鑰的使用而觀看預演。

圖4係仍然描述本發明的另一具體實施例。在圖4的流程圖400中，一自由預覽密鑰可於例如供應期間預先提供給在方塊420顯示的一客戶端。編密材料的提供可在方塊404中配送給一客戶端。在方塊408中，一內容密鑰可被

五、發明說明 (17)

提供。內容密鑰可使用如方塊412所示的一自由預覽密鑰而編密。編密的內容密鑰然後可如方塊416所示而提供給複數個客戶端。然後，如方塊424所示，客戶端可利用客戶端的自由預覽密鑰而將編密的內容密鑰解密。在方塊428中，編密節目內容的一第一部分可配送給複數個客戶端。客戶端可利用提供的自由預覽密鑰而將編密的內容密鑰解密。編密節目內容的一第一部分可如方塊428所示而配送給複數個客戶端。然後，客戶端可利用內容密鑰將編密的節目內容解密，並且如方塊436所示，藉此獲得節目內容的一自由預覽。在此處理期間，經由螢幕的顯示而可提示一使用者購買節目440。在那時，使用者可表示經由一使用者界面的接受，而且藉此購買節目內容。在那時，一新的密鑰可配送給使用者將節目的編密部分解密。

或者，沒有直接地運送有的內容密鑰編密，FPK可用來將內容的開始部分直接編密，而不是傳遞使用一自由預覽密鑰(FPK)編密的一內容密鑰，其此情況，開始內容密鑰是與FPK的值相同。

仍然另一選擇是要配送使用FPK編密的一節目片段密鑰(PSK)。PSK然後可用來傳遞使用PSK編密的內容密鑰。

可了解到，在專利中描述的各種不同具體實施例可在例如一節目多重播放期間使用重複動作達成。因此，在圖4中，方塊412和428可重複超過一次。同樣地，可了解到，一些描述的行爲可同時發生。再者，例如，方塊412和428可同時發生。此外，為了簡化緣故，雖然一些範例係

五、發明說明 (18)

描述在一伺服器與一客戶端之間的一關係，但是可了解到超過一客戶端可加入。

請即參考圖5，其係本發明的仍然另一具體實施例。在圖5的方法500中，節目內容可如方塊504所示用以配送而先提供。節目內容的第一部分可如方塊508所示在網路上配送給客戶端電腦。在方塊512，使用者允許購買其餘的節目內容。雖然節目內容的第一部分並未編密，但是節目的其餘部分可如方塊516所示而編密。如此，一密鑰可在例如伺服器上提供，以便將節目的其餘部分編密。在方塊520，節目的其餘部分可在方塊512中配送給要求其節目內容的客戶端電腦，如此可避免在沒有適當的解密工具而將可接收及觀看節目編密其餘部分的客戶端電腦重新分析。如此，可將一密鑰提供給使用者，其中該密鑰可將節目內容的編密部分解密。此是提供一自由預覽的仍然另一方法，其在於開始的節目內容是未編密配送，而其餘部分是編密。因此，客戶端電腦不需要一解密密鑰來觀看節目內容的開始部分。因此，一使用者可免費觀看節目內容的開始部分，而且可隨意決定是否購買節目的其餘部分。

圖6係描述本發明的仍然另一具體實施例。在圖6的方法600中，一伺服器的提供可在方塊604中用於與多重客戶端電腦通訊。伺服器配的配置可如方塊608所述而將一節目內容提供給多重客戶端電腦。例如，一多重播放配置可實施。在方塊612，一自由預覽節目部分可由客戶端電腦提供用於觀賞。因此，在方塊616，一密鑰可提供給一或

五、發明說明 (19)

多個客戶端將節目內容的一編密部分方解密。方塊620係描述一開始觀看週期可於一預定時段提供，以允許一預定數量的客戶端可接收密鑰，用以將節目的編密部分解密。因此，開始觀看週期允許足夠時間使一伺服器可例如將密鑰配送給購買節目的人。

圖7A係描述一節目與節目持續時間相比較的要求次數繪圖。從圖7A可看出，一開始的自由預覽時段可提供給客戶端電腦要求一初始密鑰，用以觀看節目的一編密部分。要求次數在自由預覽時段可能較高，然後在其餘節目期間可能會消失。因此，自由預覽節目週期允許系統可於開始觀看節目期間適於密鑰的高度要求。

在圖7A的底部是顯示內容密鑰0、1、和2的配送。內容密鑰0在一具體實施例中是提供給使用者可獲得自由預覽。內容密鑰1和2係描述只有兩密鑰需要將其餘節目內容解密的範例。

如一範例所示，密鑰0是一眾所週知的自由預覽密鑰，在自由預覽密鑰下編密的內容編密密鑰、或內容可在自由預覽時間期間不編密。密鑰1是代表在開始觀看時間期間於所使用群密鑰下編密的群密鑰本身、或一內容編密密鑰。而且，密鑰2將會是只傳遞給購買內容客戶端的實際內容編密密鑰。

密鑰配送

在例如按時間付費、觀賞付費、預約基礎等的各種不同配送方法下，編密密鑰可配送給客戶端，以幫助節目內容

五、發明說明 (20)

的接收。本發明的一具體實施例可提供多層密鑰階層組織，以適合例如觀看付費或按時間付費的各種不同購買選項。在本發明的一具體實施例中，不同類型的密鑰其關係可依下列配置：

唯一密鑰(UK)：例如，此可以是一交談密鑰，其可在TGS-REQ/TGS-REP訊息交換期間經由KDC而提供給在一ESBroker環境中的客戶端。此密鑰對於每位觀眾與每個交談是唯一的。客戶端可保存多重唯一密鑰的一清單；一是用於每個儲存伺服器。每個唯一密鑰可用來開始與一特殊儲存伺服器進行KEY REQ/KEY-REP訊息交換。唯一密鑰亦可用來傳遞具一編密CK、SK、PK、或PSK的EMM訊息。

服務密鑰(SK)：此密鑰可長達超過一節目重要事件，並且可於數天到數月期間當作一預約密鑰使用。它是可經由所有用戶共用的服務，但是在儲存伺服器之間可能不同。如果一客戶端從一特殊儲存伺服器要求一預約服務，首先，儲存伺服器會讓客戶端拜訪，服務密鑰可在使用客戶端服務密鑰所編密的KEY REQ/KEY-REP訊息交換期間提供給它。只要客戶端具有密鑰，客戶端便可將此服務內容解密，直到服務密鑰屆滿為止。此時(或最好是預先的足夠需要量，如此可避免伺服器過載)，客戶端可從儲存伺服器要求下一版本的服務密鑰。

此機構允許預約客戶端在沒有儲存伺服器的協議密鑰可很快取得服務，如此可減少儲存伺服器上的負荷。此假設內容編密密鑰(CK)、節目片段密鑰(PSK)、與節目密鑰

五、發明說明 (21)

(PK)可時常配送。

節目密鑰(PK)：此密鑰可於一節目重大事故發生時期有效。它可用來存取使用觀賞付費選項所購買的一個別節目事件。類似服務密鑰，它可在KEY REQ/KEY-REP訊息交換期間提供給客戶端。節目密鑰亦可經由服務密鑰編密，並且配送給擁有服務密鑰的所有客戶端。

節目片段密鑰(PSK)：此密鑰可用來將單一節目事件或一整個服務分成可購買的片段。PSKs可使用單一播放或多重播放配送而傳遞。使用按時間付費購買選項的客戶端將可使用KEY REQ/KEY-REP訊息交換獲得PSK。使用PPV購買選項的客戶端可使用多重播放配送接收在PK下編密的PSK。一預約客戶端可使用多重播放配送而接收在SK或PK下編密的PSK。(或者，一預約客戶端可接收在SK下直接編密的CK)。

這些片段可重疊，為了要幫助可縮放性。兩個PSKs可於任意特定時間配送：目前的PSK及下一PSK。當從儲存伺服器要求下一組PSKs時，此允許客戶端可持續接收內容。

內容密鑰(CK)：此密鑰可用來將內容本身編密。它應該至少時常改變PSK。它能夠以數個方法配送，例如：
(1)在選取按時間付費選項觀眾的PSK下編密，(2)在選取PPV選項使用者的PK或UK下編密；或(3)在服務用戶的一SK下的編密。

群密鑰(GK)：此密鑰可用來配送CK或PSK，其接著可於開始的觀看週期將CK編密。客戶端可獲得於PBT基礎

五、發明說明(22)

的PPV上所銷售節目事件前的GK，例如在供應期間。當客戶端與儲存伺服器協議另一密鑰時，此可將選項提供給觀眾，以觀看內容的開始部分。

自由預覽密鑰(FPK)：此密鑰用來配送CK或PSK，其接著可於開始的自由預覽時段將CK的內容編密。此是所有客戶端已知的一固定密鑰，或可在供應期間配送。

表1係顯示用以將各種不同密鑰配送給客戶端的本發明各種不同具體實施例。如表1所示，只有配送給使用UK個別客戶端(如同在UK下編密密鑰的顯示)的密鑰能以一單一播放方式傳遞。這些定址單元訊息可實施定名管理訊息(EMM)功能。或者，為了改良效率，使用不同UKs的編密的多重EMMs可組合成單一多重播放訊息。其他密鑰對於一群經認可的客戶端只可編密一次及多重播放，因為他們只可由擁有較高階層密鑰的客戶端解密。這些群定址的多重播放訊息可扮演定名控制訊息(ECM)的角色。

五、發明說明 (23)

	PPV	預約	按時間付費
UK			
SK		(SK)UK	
PK	(PK)UK	(PK)SK	
PSK	(PSK)GK 或 (PSK)PK 或 (PSK)FPK	選擇性： (PSK)SK 或 (PSK)PK	(PSK) UK
CK	(CK)PK 或 (CK)FPK 或 (CK)GK 或 (CK)UK	(CK)PSK 或 (CK)SK 或 (CK)PK	(CK)PSK (CK)FPK (CK)GK
GK	(GK)UK 或 供應的		(GK)UK 或 供應的
FPK	(FPK)UK 或供應 的		(FPK)UK 或 供應的

表 1

本發明的不同具體實施例可提供用以配送上述密鑰的。例如"拉曳"模型、"推"模型、及一組"推挽式"模型可使用。在拉曳模型下，每位客戶端可保持追蹤密鑰及其屆滿時間，而可在目前密鑰時間屆滿之前主動要求新密鑰，如此可避免服務中斷。或者，推模型可負予伺服器責任，以便保持追蹤主動客戶端，及在目前密鑰屆滿之前將新的密鑰配送給他們。例如，既然伺服器為了要將客戶端計帳而需

五、發明說明 (24)

要知道哪位客戶端購買節目，所以觀賞付費購買模型可利用密鑰配送的拉曳模式。內容密鑰，亦即，用來將節目內容本身編密的密鑰不需要在觀賞付費事件期間改變。一客戶端可拉曳一節目密鑰，其可用來將觀賞付費節目的內容密鑰編密。因此，其他密鑰在觀賞付費事件期間是不需要；伺服器仍然可追蹤哪一客戶端拉曳用以接收觀賞付費事件的密鑰。同樣地，一使用者付費一預約價格以便在一延伸時段上接收一節目的預約付費模型亦可利用拉曳模式。例如，在預約模型下的開始要求中，客戶端可要求預約及拉曳在客戶端唯一密鑰下編密的一服務密鑰。然後，預約模型允許推模式使用在觀賞付費事件的節目密鑰、或按時間付費事件的節目片段密鑰可推向給在服務密鑰下編密的客戶端。同樣地，內容密鑰可推向給在節目片段密鑰下編密的客戶端。因此，預約模型兩利用拉曳與推向模式。拉曳密鑰配送模型、推曳密鑰配送模型、與組合拉曳/推進密鑰配送模型將在下面進一步詳細說明。

拉曳密鑰配送模型允許每位客戶端可從伺服器主動要求密鑰。在圖8中，一流程圖800係描述用以實施一拉曳密鑰配送系統。在方塊810，一伺服器可從一客戶端接收一編密密鑰的要求。伺服器可在方塊814中記錄密鑰的要求。例如，此一記錄登錄可在例如伺服器中維護的資料庫記錄達成。在方塊818，密鑰及其屆滿時間可反應客戶端的要求而配送給客戶端。如此，伺服器不需要監視客戶端密鑰的狀態；相反地，決定何時需要一新密鑰的責任可托付

五、發明說明 (25)

給客戶端。在方塊822，節目內容可由利用要求編密密鑰的客戶端配送功解密。最後，在方塊826，記錄登錄可用來基於計帳配置的計帳參數而向客戶端取費。

圖9係根據本發明的仍然另一具體實施例而描述一流程圖900。例如，方法900係描述兩節目片段密鑰可用來將兩不同多重播放訊息的相同內容密鑰傳送給一客戶端。因此，如果一使用者並未接收一新節目片段密鑰，內容密鑰便可經由利用舊的節目片段密鑰獲得。再者，在方塊910，一要求可從一編密密鑰的客戶端接收。密鑰的要求可如方塊914所示記錄。在方塊918，密鑰可使用的節目內容片段可記錄在記錄內。再者，伺服器不需要監視一客戶端密鑰的需要。最好，客戶端可要求密鑰而對伺服器獨立行動。在方塊926，想要的密鑰是使用一第一節目片段密鑰編密。在方塊930，編密的密鑰可如同一部分的第一多重播放訊息配送。或者，在不同具體實施例中，密鑰可單一播放給客戶端。因此，一特殊客戶端的唯一密鑰可將新密鑰配送給特殊客戶端。想要的密鑰亦可如同一部分的第二多重播放訊息配送這。此是在方塊934顯示，其中密鑰是在一第二節目片段密鑰下編密，而是如同一部分的第二多重播放訊息配送。在方塊938，節目內容的配送可藉由利用傳輸密鑰而由客戶端解密。最後，在方塊942，客戶端是基於任何記錄登錄而計帳。

在記錄一密鑰的要求中，一伺服器可記錄有關要求的多種資訊。例如，要求密鑰的時間與片段可記錄。然後，這

五、發明說明 (26)

些記錄稍後可轉送給費用系統，以便將他們分析，為了要決定每位客戶端所觀看的內容長度。伺服器不必保持追蹤，並且將密鑰主動配送給客戶端；最好是它只等待要求一新密鑰的客戶端。

伺服器典型將不會使用一新內容密鑰開始編密，直到它將反應傳送給要求新內容密鑰的每位客戶端為止。因此，圖9係描述內容密鑰可配送兩次的一方法。第一，它是在舊節目片段密鑰下編密，而且在一第一多重播放訊息中多重播放。第二，它是在新節目片段密鑰下配送，而且是在一第二多重播放訊息中配送。雖然此應該允許未要求新節目片段密鑰的客戶端可接收下一片段，但是它可避免確實要求新節目片段密鑰的客戶端服務中斷。此問題可藉著將節目片段分成兩或多個內容編密新紀元而減輕。

在一拉曳密鑰配送模型下，每位客戶端可要求一新密鑰，而且可個別反應該密鑰配送伺服器。伺服器可基於此第一密鑰要求而在一多重播放期間中維持主動參加者的清單。然後，在此清單的所有客戶端可使用一多重播放UDP訊息而週期性提供新密鑰，其中該等新密鑰具有於使用參加者唯一密鑰的每位參加者編密的一新節目片段密鑰。當一客戶端決定離開多重播放期間時，客戶端可將一認證要求傳送給伺服器，以詢問是否從清單移除。此可發信通知伺服器將客戶端停止接收內容的時間記錄，所以客戶端將不會於稍後的內容收費。因此，客戶端可從主動參加者的清單移除，而且將不能接收下一密鑰更新訊息。理論上，客

五、發明說明 (27)

戶端可擁有密鑰，而且可將內容解密；然而，伺服器能以固定間隔將新的密鑰送給主動參加者，如此可避免移除的客戶端從進一步內容解密。

在本發明的另一具體實施例下，一推進密鑰配送模型可實施，以便將密鑰從一伺服器配送給一客戶端。因此，圖10係描述用以實施一推進密鑰配送模型的流程圖1000。在方塊1010，一伺服器可從一客戶端接收一第一密鑰的要求。在方塊1020，伺服器可建立要求第一密鑰的一客戶端清單。在方塊1030，一多重播放訊息可配送給客戶端，如此可配送直接或間接使用在解密節目內容的一第二密鑰。

圖11係描述一流程圖1100，其係顯示在圖10所示方法的一更詳細具體實施例。在方塊1110，一要求可從客戶端接收一第一密鑰。伺服器可在方塊1120中建立要求該第一密鑰的一客戶端清單。在方塊1130，該等客戶端之中每一者的唯一密鑰可在將第二密鑰配送給該等相對客戶端之中每一者之前用來將一第二密鑰編密。伺服器然後可將一多重播放訊息配送給客戶端，以便如方塊1140所示，配送例如在每位客戶端唯一密鑰下編密的第二密鑰。在方塊1150，一客戶端可表示離開多重播放期間的伺服器。此時，客戶端可如方塊1160所示反應客戶端訊息而從清單移除。在方塊1170，一登錄可記錄，如此當客戶端離開交談時便可記錄，所以客戶端將不會於額外內容收費。一第三密鑰可如方塊1180所示而配送給留在清單中的客戶端，以避免從接收稍後發生內容將客戶端移除。如此，第三密鑰可配送給

五、發明說明 (28)

留在清單的客戶端。因此，第一、第二及第三密鑰可當作節目片段密鑰使用，用以將節目內容的相對內容密鑰解密。

推進密鑰配送模型可於縮放目的而利用上述分層密鑰。推進密鑰配送模型可藉由客戶端而減少新密鑰的個別要求，所以一伺服器不會充滿新密鑰的各種不同客戶端的時常要求。最好是伺服器只可將單一節目片段密鑰多重播放給留在清單的客戶端，而當作主動參加者，而且節目片段密鑰然後可用來將一對應內容密鑰解密，其中該對應的內容密鑰可用來將節目內容解密。因此，伺服器只需要維持用以接收一特別節目的一主動參加者清單。

推進密鑰模型與拉曳密鑰模型可組合成用以將密鑰配送給客戶端的一組合模型。如圖12所示，一方法1200可用於本發明的此具體實施例。在方塊1210，一密鑰可配送給用於解密節目內容的一客戶端。配送密鑰的伺服器可如方塊1220所示等待客戶端接收密鑰的確認1220。在方塊1230，伺服器可等待客戶端一預定時段，以確認密鑰是否接收。如果確認訊息未由伺服器接收，伺服器可如方塊1240所示將客戶端從清單移除，其中該確認訊息如同一"激勵訊息"的確認訊息。因此，伺服器不僅可將密鑰推進給客戶端，而且它亦可從類似拉曳模式的每位客戶端接收訊息。

完成此的一方法是使每位客戶端於每個節目片段期間可至少一次傳送一"保持有用"的訊息。伺服器將可獲得主動參加者的一清單，並且將經由一多重播放UDP訊息而將

五、發明說明 (29)

新的片段密鑰配送他們，其中該多重播放UDP訊息具有在每位客戶端的各種不同唯一密鑰下編密的新密鑰。如果一伺服器不能於一片段持續時間看見一"保存有用"的訊息，它可將客戶端從主動清單移除。如果基於一些理由而客戶端未能傳送一"保存有用"的訊息而想要持續接收內容，它可監視節目片段密鑰的屆滿時間，並且在密鑰屆滿之前傳送一個別密鑰更新要求。再者，此是實施組合模型"拉曳"觀點的一方法。

圖13係描述用以實施本發明的具體實施例流程圖1300。在方塊1310，一伺服器可開始將節目內容多重播放給複數個客戶端。在方塊1320，主動參加者的一清單的建立係顯示客戶端正在接收節目。在方塊1330，一訊息是從一客戶端接收，例如表示客戶端是否應該在清單的一"保持有用"訊息。在方塊1340，伺服器可將一多重播放訊息傳送給包括新密鑰的主動參加者清單，例如，用以將節目內容的下一片段解密的節目片段密鑰。如此，當一客戶端從清單移除時，主動參加者的一第二清單便可建立。

作為一部分的密鑰配送系統，內容密鑰可在整個節目內容配送過程中用於節目內容解密。因此，當一新內容密鑰實施時，實施將可發信通知客戶端，所以客戶端可開始利用提供的新內容密鑰。時常地，客戶端可提供例如解密的內容密鑰之一編密版本，而且具有一節目片段密鑰。同樣地，節目片段密鑰可使用一服務密鑰或甚至唯一的密鑰來編密。

五、發明說明 (30)

一發信方法可用來表示一新密鑰的實施。例如，一預定位元可用來表示一舊或目前的內容密鑰是否應該當作與最近配送給客戶端的一新內容密鑰的相反而使用。因此，一客戶端可檢查一封包的預定位元，並且決定可使用的適當內容密鑰。如一範例所示，如果使用單一位元，一"1"可用來表示目前內容密鑰使用中，而"0"可用來表示新內容密鑰應該使用。圖14係顯示用以實施一發信方法的流程圖1400。圖14係參考用以配送節目內容的一RTP封包；然而，它同樣可適於配送內容所採用的其他協定。因此，它只描述亦能與其他協定實施的一方法。在方塊1410，一封包的提供可當作一RTP封包使用，其中該封包具有有效載荷部分及標題部分。在方塊1420，一欄位是在標題部分與有效載荷部分之間插入，而且其操作是表示一密鑰變化。此可以是例如一延伸標題的固定欄位，其中該固定欄位的一預定值係表示封包有效載荷部分的內容密鑰已改變。或者，它可表示下一發生的有效載荷部分可利用新內容密鑰、或此類似實施而解密。在方塊1430，一修改的RTP封包可被建立。此修改的RTP封包可在方塊1440中從伺服器傳送給客戶端。客戶端可接收如方塊1450所示的修改RTP封包，並且從插入的欄位決定密鑰是否如方塊1460所示而改變。方塊1470可從修改的RTP封包將插入的欄位部分移除，並且可如方塊1470所示將最初的RTP封包復原。然後，復原的RTP封包可如方塊1480所示處理，而且封包可藉由使用目前或下一密鑰而解密，其是因延伸標題中的一指示符

五、發明說明 (31)

號而定。

其他發信方法亦可利用。例如，一RTP標題延伸可利用。如此，標題的延伸部分可包括至少內容密鑰同等位元，以表示密鑰是否改變。

同樣地，一有效載荷特殊符號位元可利用。此位元已在例如MPEG 4有效載荷的一些有效載荷類型中利用，而且其可使用該符號位元以表示一訊框的開始。

此外，一墊補位元可利用。RTP標題的墊補位元可用來表示密鑰變化。此假設編運用於RTP封包的編密方法不能使用任何墊補。

在例如聲訊與視覺材料的多重播放節目內容中，定名管理訊息與定名控制訊息可從一伺服器傳送給客戶端電腦。本發明的一具體實施例可提供此訊息的一格式。在此格式下，保護防止再現攻擊的一序號或一時間記錄可提供。此外，在EMM和ECM訊息的另一欄位中，一認證數位簽署的密鑰訊息認證碼(MAC)可提供。在多重播放中，用來編密MAC的密鑰對於多重播放期間的所有參加者是已知；因此，認證功能會被限制。使用簽署的一個人權限控制(EC)密鑰可認證流傳伺服器。公眾密鑰可在KEY-REP配送給每個參加者。注意，沒有訊息認證(HMAC)的密鑰雜湊、或簽署可被確認，直到一客戶端接收它的KEY-REP訊息為止。然而，另一欄位包含在訊息中所包括的密鑰類型，例如一內容密鑰、一群密鑰、一節目片段密鑰、一服務密鑰等。此外，一欄位可提供用來將訊息的密鑰編密的密鑰

五、發明說明 (32)

類型。因此，唯一密鑰可表示例如傳輸一服務密鑰的訊息。另一欄位可提供保留密鑰壽命的時間。此外，一密鑰同等位元匹配在RTP封包的同等位元可提供。而且，當多重EMMs是在單一播放訊息中傳遞時，時常需要的一使用者確認可提供。資料結構的每個欄位可適用於這些欄位之中每一者。因此，他們能以任何順序配置，以致於資料結構包括一或多個這些欄位。

圖7B係描述一自由預覽時段的定名控制訊息，其中一內容密鑰CK0是使用一自由預覽密鑰(ECM: [CK0] FPK)而編碼。同樣地，圖7B係顯示一定名控制訊息，其中一內容密鑰是使用一群密鑰(ECM: [CK1] GK)而編碼。一第二定名控制訊息的顯示可傳遞使用節目密鑰(ECM: [CK2] PK)編密的一第二內容密鑰。此外，顯示的數個定名管理訊息係使用一特殊客戶端電腦的唯一密鑰編密的新節目密鑰。PK可個別單一播放給個別客戶端。或者，單一訊息可建立，如此可形成可多重播放給多重客戶端的節目密鑰的連結訊息。因此，每位客戶端可剖析及解密客戶端的新節目密鑰。

或者，CK0不需要在一ECM內配送。複數個客戶端擁有的FPK值可如同CK0採用。

或者，CK1不需要在一ECM內配送。複數個客戶端擁有的GK值可如同CK1採用。

或者，CK2可使用UK編密，並且以一EMM形式直接傳遞給客戶端，以取代在圖上顯示的ECM形式。

開始觀看週期

五、發明說明 (33)

對於例如觀賞付費事件的一些多重播放事件而言，預期一系統會經歷到最大負荷，即是路由要求節目密鑰，非常接近一節目的排程開始。如果參加多重播放期間的客戶端群非常大，一伺服器便不能立即將密鑰配送給所有參加者。因此，一系統需要允許觀眾在當伺服器將密鑰配送給已購買節目內容的客戶端期間接受一節目的開始。圖15係描述用以在一開始觀看週期期間配送密鑰之一方法的具體實施例。

實施一開始觀看週期的一方法是預先將一共同密鑰配送給潛在的參加者，例如，在節目內容配送之前。此一密鑰在此稱為一群密鑰。當他們要求一特殊儲存伺服器時，一群密鑰可提供給客戶端；或當他們在供應期間在配送系統開始時，它可能是客戶端獲得的一實際通用密鑰。既然每位客戶端可在此一情況接收一群密鑰，所以理論上，全部客戶端可接收免費內容的第一部分。圖15係描述用以實施本發明的一具體實施例的流程圖1500。在圖15的方塊1510中，例如一群密鑰的第一密鑰可提供給客戶端。在方塊1520，一第二密鑰的提供可用來解密該節目內容的一第一部分。此一密鑰可稱為一內容密鑰。第二密鑰可如方塊1530所示而提供給在第二密鑰下編密的複數個客戶端之中至少一者。此第二密鑰可在配送給客戶端之前經由群密鑰編密。在方塊1540，此第二密鑰可在伺服器用來編密該節目內容的一第一部分。節目內容的編密第一部分然後可如方塊1550所示而配送給客戶端群。因此，接收第二密鑰的

五、發明說明 (34)

客戶端可將該編密的節目內容解密。即是，客戶端可利用群密鑰將內容密鑰解密，然後可利用內容密鑰將編密的節目內容解密。此是在方塊1560顯示。

因此，當一多重播放事件開始時，開始的內容密鑰可在觀賞付費事件的群密鑰及節目密鑰、或按時間付費事件的一第一節目片段密鑰下配送(PSK亦可在GK下編密)。既然群密鑰是預先配送，所以客戶端不必等待接收最後可配送給他們的節目密鑰或節目片段密鑰。最好是，伺服器可在群密鑰下建構"N"數量的內容密鑰。配送的內容密鑰數量可基於客戶端對節目內容的預期要求；或亦可基於購買節目的客戶端立即負荷而動態調整。因此，伺服器可基於一特別節目的要求而即時調整。

圖16A和16B係描述用以實施本發明具體實施例的一流程圖1600。在方塊1610，節目內容的提供可用於多重播放給複數個客戶端。節目內容的一第一部分可利用例如群密鑰的一第一密鑰編密，以便在方塊1620中產生節目內容的編密第一部分。在方塊1630，客戶端可提供此第一密鑰，以便例如在供應期間可預先用來將節目內容解密。在方塊1640，節目內容的編密第一部分可在這些客戶端購買之前多重播放給客戶端。在方塊1650，既然此節目內容的第一部分可例如經由先前配送的群密鑰解密，所以該第一部分可於一時段編密，以允許一使用者可獲得節目內容的開始觀看。此時段可基於節目的預期要求而預先決定。在方塊1660，例如在自由預覽時段結束時，可藉由客戶端的一使

五、發明說明 (35)

用者界面而提示使用者購買節目內容。然後，方塊1670係顯示的供一保證時段，以允許一使用者可購買節目內容，而無需中斷節目服務。因此，如果一使用者在保證時段期間購買節目，使用者能以一適時流行樣式而可預期接收需要的密鑰，所以節目觀看的損失不會發生。在方塊1674，一伺服器可產生第二密鑰，其然後可如方塊1680所示用來編密該節目內容的一第二部分。如方塊1684所示，一第二密鑰亦可提供給在保證時段期間購買節目內容的該等客戶端之中每一者。例如，只要購買節目密鑰，一節目密鑰可配送給客戶端。當第二密鑰傳送給客戶端時，此節目密鑰然後可用來解密該第二密鑰。如此，在方塊1690，節目內容的編密第二部分可多重播放給複數個客戶端。因此，購買節目內容及接收第二密鑰的這些客戶端可解密該節目內容的第二部分。

圖7B係顯示在本發明的一範例中的保證時段。在圖7B中，保證時段是在群密鑰可用來將一內容密鑰解密的期間，其中該內容密鑰可將解密該編密的節目內容。在保證時段期間購買節目內容的任何使用者可接收在初始密鑰配送內的下一需要的解密密鑰。如此，初始密鑰配送時段的顯示是時間持續長於保證時段，如此允許一密鑰配送給在保證時段期間購買的一客戶端。如此，內容密鑰(CK1)的顯示是持續於整個初始密鑰配送時段。因此，下一內容密鑰可在初始密鑰配送時段過去之前經由一購買使用者獲得。

因此，若要提供一滿意的使用者經驗，在"保證時段"期

五、發明說明 (36)

間要求存取一事件(例如,他們要求觀賞付費事件的一節目密鑰)的所有客戶端將可確保接受沒有中斷的內容。此表示伺服器在群密鑰下不會停止配送密鑰,直到在保證時段期間接收要求的所有客戶端具有配送給他們的節目密鑰為止。再者,此稱為初始密鑰配送。

在保證時段之後要求內容的客戶端錯過例如電影的開始;因此,節目密鑰或節目片段密鑰的傳遞不是決定性的,而且一輕微延遲對於這些觀眾是可容忍的。事實上,它是最好是一使用者可稍後開始一連續觀看體驗,而不是較早開始暫時中斷的觀看體驗。

如先前的描述,初始密鑰配送時段可基於一特別節目的預測流行而初始設定,然後由伺服器修改以調整目前負荷。因此,基於要求次數、或伺服器電腦的性能,配送時段可延伸。圖17係描述用以完成此的本發明具體實施例的方法。在方塊1710,節目內容可用於多重播放。在方塊1720,節目內容的一第一部分可在沒有改變而多重播放給複數個客戶端。如方塊1730所示,一保證時段是在節目內容第一部分的多重播放期間提供。方塊1740係顯示在保證時段期間購買節目內容的客戶端數量可評估。在方塊1750,一初始密鑰配送時段的提供具有一足夠長的持續時間,以便將編密密鑰提供給購買客戶端,如此可避免節目內容的接收於購買客戶端中斷。在方塊1760,初始密鑰配送時段可被調整。初始密鑰配送時段的調整可例如經由只擴展初始密鑰配送時段發生。因此,一內容密鑰可於適合購買內容

五、發明說明 (37)

觀眾額外負荷的一時段用來將節目內容編密。此外，購買客戶端的實際數量可被決定，而且能與預期購買節目內容的客戶端評估數量相比較。初始密鑰配送時段可基於客戶端的額外負荷而延伸。此外，延遲可能是由於伺服器或網路上的負荷，其中這些元件性能可被分析，而且因此初始配送時段可調整。

圖18係描述用以在上述保證時段屆滿之後允許使用者購買內容的一方法1800。在方塊1810，節目內容可提供複數個客戶端的配送。於不中斷購買節目內容的觀看的第一時段可在方塊1820提供。因此，此符合前述的保證時段。來自一節目內容購買客戶端的購買要求可如方塊1830所示而在第一時段期間接收。如方塊1840所述，一第二時段的提供可用於購買節目內容，其中在第一時段之後，該第二時段便會發生。如方塊1850所示，來自一最近購買客戶端的購買要求可在此第二時段期間接收。如方塊1860所示，節目內容可配送給購買客戶端，而不會中斷節目內容的觀看，而配送給最近購買客戶端的節目內容解密延遲會發生，直到節目內容解密而不會中斷最近購買客戶端的觀看。此是在方塊1870顯示。因此，此方法會延遲一密鑰與一最近購買客戶端的通訊，直到伺服器決定最近購買客戶端接收可供不中斷節目內容觀看所需的一密鑰。

內容權限與情況

請即參考圖19，一系統可看出是用以實施在多重播放環境中提供內容的規則與情況。系統1900係顯示包含至少一

五、發明說明 (38)

客戶端 1908 的一客戶端伺服器網路，其是經由例如網際網路的網路 1916 而耦合到例如起源內容伺服器 1904 的伺服器。此外，圖 19 係顯示一儲存伺服器 1912，而且一授權中心 1920 亦耦合到網路。起源內容伺服器係描述可儲存或控制節目內容存取的一伺服器。例如，此內容可以是多媒體、或它可以是經由一網站廣播系統的一分散式電影。儲存伺服器 1912 可使用在此多重播放環境，以儲存在來源內容伺服器上發生的一節目內容副本。

在本發明的一具體實施例中，一客戶端可向授權中心 1920 註冊，以獲得定義何種內容類型可獲得的一輪廓。因此，當一客戶端想要獲得內容時，多種程序可實施，以確定客戶端是否要是具有權限接收特殊節目內容。用以獲得節目內容的至少 3 個選項可利用。例如，在圖 19 的起源內容伺服器 1904 的內容供應者可執行檢查。或者，圖 19 的儲存伺服器 1912 可執行檢查常式、或檢查可由客戶端本身執行。

在起源內容伺服器執行檢查的情況中，來源內容伺服器可分析節目內容的客戶端要求，及檢查授權中心，以決定客戶端是否於特殊內容授權。此方法可特別允許較早決定是否拒絕客戶端存取，可免除拒絕內容存取的進一步處理及可能的觀看不滿意。

或者，檢查可在客戶端本身執行。例如，客戶端能以一硬體安全裝置或安全晶片形成，以實施將規則配送給每一個別客戶端。如此，經由此硬體安全裝置使用的規則能與

五、發明說明 (39)

客戶端觀看權限或例如客戶端所在國家的實際位置的其他屬性相比較。當不同國家擁有有關何種節目內容類型可配送的各種不同法律時，此實際位置會是重要的。

本發明的仍然另一具體實施例允許在儲存伺服器上執行檢查。儲存伺服器可將內容規則與客戶端權限相比較，而且可安全實施規則。客戶端權限可安全包含在一資料記錄，其中該資料記錄是客戶端可提功給儲存伺服器、或儲存伺服器可經由其他裝置接收。該等規則可從來源伺服器配送給儲存伺服器。此外，購買選項可從來源伺服器配送給客戶端，而且客戶端然後可將購買選項傳遞給儲存伺服器。

除了將內容規則與一使用者(客戶端)的權限相比較之外，使用者的選擇購買選項亦能與授權決定的規則相比較。

圖20A和20B係描述用以實施本發明的一具體實施例的方法2000。在圖20A的方塊2004中，一規則的建議是定義一客戶端是否授權接收節目內容。客戶端允許從例如在圖19起源內容伺服器1904的一伺服器要求節目內容。此是在方塊2008描述。在方塊2012，一要求可於節目內容接收。例如，客戶端可從來源內容伺服器要求節目內容。在方塊2016，包含一識別符的資料記錄可被格式化，以識別節目內容、及定義何者可存取節目內容的規則、及使用者可選取的購買選項。在方塊2020，資料記錄可簽署及編密。方塊2024係描述一信賴的第三者可用來簽署資料記錄。例如，此一信賴的第三者可用來將一簽署密鑰送給來源內容伺服器，以使用於簽署資料記錄。同樣地，相同信賴的第

五、發明說明(40)

三者可用來將一確認密鑰提供給一儲存伺服器，而且稍後可使用該認證的資料記錄。在方塊2028，顯示的資料記錄可傳遞給客戶端。客戶端然後可如方塊2032所示將資料記錄傳遞給儲存伺服器，其中資料完整性可如方塊2034所示經由檢查簽署而確認。或者，資料記錄可無需經由客戶端而從來源內容伺服器直接傳遞給儲存伺服器。在圖20B的方塊2036中，一決心可在儲存伺服器達成，以判斷客戶端是否授權接受節目內容。儲存伺服器可利用資料記錄，包含定義何者授權接收節目內容的規則、及特別是要求節目內容客戶端的權限。藉由此決定，儲存伺服器可決定是否提供客戶端使用的節目內容密鑰。儲存伺服器可如方塊2040所述而配送由客戶端(或複數個客戶端)使用的節目內容材料的編密副本。

從儲存伺服器的預期所描述本發明的另一具體實施例是在圖21顯示。在圖21的流程圖2100中，儲存伺服器可如方塊2110所述從一客戶端接收一節目內容識別符。此節目內容識別符可用來識別客戶端電腦的使用者想要獲得的特殊節目內容。方塊2120係描述使用者選取付費方法亦能與伺服器通訊。例如，由客戶端與來源伺服器協議的付費方法能與儲存伺服器通訊。在方塊2130，與節目內容有關的規則可經由儲存伺服器獲得，其中該儲存伺服器可用來決定內容是否授權給節目內容。節目內容識別符、使用者選擇付費方法、及與節目內容有關的規則可在由客戶端傳送給儲存伺服器的一安全物件中與儲存伺服器通訊。此安全物

五、發明說明 (41)

件或資料記錄然後可經由儲存伺服器剖析，如此可獲得相關資訊。此外，一憑單可如方塊2140所示從客戶端獲得。注意，方塊2110、2120、2130和2140能以彼此相關的任何順序發生。此憑單包含權限資訊，其可用來決定客戶端是否授權接受節目內容。例如，憑單可儲存客戶端預約的一服務清單、例如在美國的客戶端位置等、客戶端內容付費等。如方塊2150所示，此憑單資訊能與經由儲存伺服器獲得的規則相比較，以決定客戶端是否享有節目內容。如方塊2160所示，如果客戶端授權接收節目內容，一密鑰便可傳遞給客戶端，用以直接或間接用來將編密的節目內容解密。如果客戶端未享有節目內容，那麼沒有此密鑰需要配送。因此，對於享有及接收節目內容密鑰的客戶端而言，節目內容的多重播放可使用接收的密鑰解密。

儲存伺服器可將節目材料的內容規則與每位客戶端的權限相比較，並且可安全實施規則。客戶端的權限可安全包含在資料記錄，其中當儲存伺服器要求特殊內容時，客戶端可將該資料記錄提供給儲存伺服器。內容規則能以至少兩方式傳遞。例如，內容規則可例如與內容一起直接傳遞給儲存伺服器。如此，規則只可一次傳送給每個儲存伺服器。在節目材料的預約購買情況中，既然它包括在他的預約協議中，所以一觀眾不需要個別協議每一段內容。當一觀眾確實需要選取例如觀賞付費或按時間付費的購買選項時，觀眾可將他們與來源內容伺服器協議。選取的購買選項可簽署及編密，並且可傳遞給客戶端(與內容規則的傳

五、發明說明 (42)

遞機構無關)，然後在要求中所包括的可經由客戶端傳送給儲存伺服器。既然選取的購買選項是在儲存伺服器已知的一密鑰下編密而不是客戶端，所以購買選項可經由客戶端修改。或者，當客戶端與來源內容伺服器協議內容存取時，內容規則可經由例如來源內容伺服器的內容供應者建立。此規則能與觀眾選取的特殊購買選項組合，例如觀賞付費或按時間付費。與選取的購買選項組合的內容規則然後可簽署及編密，並且傳遞給客戶端，然後在要求中包括的可經由客戶端傳送給儲存伺服器。既然內容規則是在儲存伺服器已知的一密鑰下編密而不是客戶端，所以他們不能由客戶端修改。此方法可移除在一來源內容伺服器及用以傳遞內容規則的一儲存伺服器之間的一直接界面需要。

在來源內容伺服器與客戶端之間協議一購買中，起源內容伺服器可區域性維持規則與購買選項資訊。它然後可將所有不同購買選項提供給客戶端，如此允許客戶端決定。因此，購買選項可封裝到安全資料記錄，以傳回給客戶端（在內容伺服器與儲存伺服器之間共用的一交談密鑰下編密的一KEY-REQ訊息形式）。然後，客戶端可將全資料記錄與包括客戶端權限資訊（例如，購買能力、預約服務清單等）一起轉送給適當的儲存伺服器。當客戶端在多重播放系統註冊時，在圖19的客戶端可從授權中心1920獲得權限資訊。

圖22係描述可由來源內容伺服器所提供的一資料記錄。此資料記錄可在傳遞給客戶端或儲存伺服器之前編密。圖

五、發明說明(43)

22係描述可選擇性當作一部分資料記錄使用的不同欄位。如此，圖22係顯示可識別例如一電影名稱的特殊節目內容的節目內容ID欄位。此外，資料記錄2200包含一欄位，用以儲存定義何者可存取節目內容的一規則。在圖22顯示的具體實施例中，一評估資訊欄位亦顯示，而且符合一特殊評估標準。而且，一欄位可如圖22所示提供，以儲存可由客戶端與來源內容伺服器協議的例如觀賞付費或按時間付費的客戶端購買喜好。

圖23係描述可提供給個別客戶端的一資料記錄。此一資料記錄可用來定義不同節目內容的特殊客戶端權限。因此，例如，圖23係顯示包含用以識別一客戶端位置欄位的一資料記錄，例如客戶端所在位置國家。而且顯示可識別客戶端預約的一欄位，例如HBO™或SHOWTIME™。額外欄位亦可提供。此資訊可被認證及編密，所以客戶端不能校正他自己的權限。

雖然本發明的各種不同具體實施例是使用用以實施本發明的方法或裝置描述，但是可了解到本發明可經由耦合到電腦的程式碼實施，例如，存在一電腦或可由電腦存取的程式碼。例如，軟體與資料庫可用來實施上述的許多方法。因此，除了本發明可經由硬體完成的具體實施例之外，同時注意，這些具體實施例可經由包含具有一電腦可讀程式碼的電腦可用媒體的製造物件使用而達成，其可產生在此描述中所揭露的功能。因此，本發明的具體實施例在他們的程式碼中亦受到此專利保護。

五、發明說明 (44)

本發明的具體實施例可如同在載波中具體實施的電腦信號完成，而且信號(例如電與光)可藉由一傳輸媒體傳遞。因此，上述的各種不同資訊能以例如一資料結構的一結構格式化、及可藉由一傳輸媒體的電信號傳輸、或儲存在一電腦可讀媒體。

同時注意，在此引用的許多結構、材料、與行為可以是用以執行一功能的裝置、或用以執行一功能的步驟。因此，可了解到此描述涵蓋在此規格及其類似中所揭露的所有結構、材料、或行為。

本發明的具體實施例的裝置與方法及許多伴隨的優點可從此規格了解，而且很顯然，各種不同變化能以這些部分的形、結構、與配置達成，而不致於違背本發明的精神與範圍、或犧牲所有他的材料優點，前述的形式在此只是具體實施例。

四、中文發明摘要(發明之名稱： 用於多媒體多重播放內容的初始自由預覽)

根據本發明的一具體實施例，一節目的自由預覽可在一多重播放系統中提供給客戶端電腦。此允許多重播放系統的觀眾可在決定是否訂購節目內容之前，觀看該節目內容的一第一部分。根據另一具體實施例，各種不同配送方法可藉著使用配送給該節目內容的編密密鑰達成。根據仍然另一具體實施例，一初始觀看週期的提供允許編密密鑰的協議。根據另一具體實施例，可利用用以在一多重播放環境中提供內容的規則及條件。

英文發明摘要(發明之名稱： " INITIAL FREE PREVIEW FOR MULTIMEDIA MULTICAST CONTENT ")

According to one embodiment of the invention, a free preview of a program can be provided to client computers in a multicasting system. This can allow viewers in the multicasting system to view a first portion of the program before deciding whether to order the program content. According to another embodiment, various distribution methods can be accomplished using encryption keys to distribute program content. According to yet another embodiment, an initial viewing period can be provided to allow negotiation of the encryption keys. According to another embodiment, rules and conditions for providing content in a multicasting environment can be utilized.

五、發明說明(44a)

圖式元件符號說明

100	內容配送系統	205b	電腦可讀取儲存媒體
104	主動清單	206	通訊系統
108	來源伺服器	207	處理加速
112	客戶端電腦	208	匯流排
116	內容交換器	209	記憶體
118	外部來源伺服器	291	工作記憶體
120	網際網路	292	作業系統
124	蠕動目錄	293	其他碼
200	系統	1900	系統
201	中央處理器	1904	來源內容伺服器
202	輸入裝置	1908	客戶端
203	輸出裝置	1912	快取伺服器
204	儲存裝置	1916	網路
205a	電腦可讀取儲存媒體 讀取器	1920	授權中心
		2200	資料記錄

六、申請專利範圍

1. 一種用以多重播放節目內容之方法，該方法包含：

提供用以配送給一客戶端而當作一部分的多重播放
配送的編密節目內容；

提供可由該客戶端使用的一密鑰，用以將該編密的
節目內容的一第一部分解密；及

將該編密節目內容的一第一部分配送給該客戶端，
當作一部分的該多重播放配送，其中該編密節目內容
的該第一部分可編密，如此可藉由使用該密鑰而經由
該客戶端解密，如此可獲得該節目內容的一自由預覽。

2. 如申請專利範圍第1項之方法，其中該提供一密鑰包含
提供可由該客戶端使用的一內容密鑰，用以將該編密
節目內容的該第一部分解密。

3. 如申請專利範圍第1項之方法，其進一步：

提供一自由預覽密鑰；及

在該配送該編密節目內容的該第一部分之前，將該
自由預覽密鑰提供給該客戶端。

4. 如申請專利範圍第3項之方法，其進一步包含：

提供一內容密鑰；

使用該自由預覽密鑰將該內容密鑰編密；及

將該編密的內容密鑰提供給該客戶端。

5. 如申請專利範圍第1項之方法，其進一步包含：

將該節目內容的該自由預覽提供給該客戶端。

6. 如申請專利範圍第5項之方法，其進一步包含：

六、申請專利範圍

提供可由該客戶端使用的一使用者界面，用以購買該節目內容。

7. 如申請專利範圍第1項之方法，其中該自由預覽包含一電影預告片。
8. 如申請專利範圍第1項之方法，其中該自由預覽包含該節目內容的一廣告。
9. 如申請專利範圍第1項之方法，其中該節目內容包含一電影，而且其中該自由預覽包含該電影的開始。
10. 一種用以多重播放節目內容之方法，該方法包含：

提供節目內容，其可當作一部分的多重播放配送而配送給一客戶端；

以一未編密的格式而將該節目內容的一第一部分配送送給該客戶端，如此可提供該節目內容的一自由預覽；

編密該節目內容的一其餘部分；

將該節目內容的該編密其餘部分配送給該客戶端。

11. 如申請專利範圍第10項之方法，其進一步包含：

提供一密鑰；及

利用該密鑰完成該節目內容的該其餘部分的該編密。

12. 如申請專利範圍第11項之方法，其進一步包含：

允許該客戶端購買該節目內容；

在該客戶端購買該節目內容之後，將一密鑰提供給該客戶端，用以將該編密的節目內容解密。

13. 一種用以在一多重播放系統中將節目內容提供給複數



六、申請專利範圍

個客戶端之方法，該方法包含：

提供一伺服器，用以與複數個客戶端電腦通訊；

建構該伺服器，如此用以將該節目內容提供給該等複數個客戶端電腦；

將該節目內容的一自由預覽提供給該等複數個客戶端電腦；及

在該自由預覽期間，將一密鑰提供給每一購買客戶端電腦，以便將一部分的該節目內容的編密部分解密。

14. 如申請專利範圍第13項之方法，其進一步包含：

提供一足夠時段的該自由預覽，以允許一預定數量的該等購買客戶端電腦可接收該等密鑰，用以將該節目內容的該編密部分解密。

15. 一種電腦可讀取媒體，具有電腦可執行指令，可用以執行一方法，該方法包含：

提供編密的節目內容，其可當作一部分的多重播放配送而配送給一客戶端；

提供可由該客戶端使用的一密鑰，用以將該編密節目內容的一第一部分解密；及

將該編密節目內容的一第一部分配送給該客戶端，當作一部分的該多重播放配送，其中該編密節目內容的該第一部分可編密，如此可藉由使用該密鑰而經由該客戶端解密，如此可獲得該節目內容的一自由預覽。

16. 如申請專利範圍第15項之電腦可讀取媒體，其中該一密鑰包含提供可由該客戶端使用的一內容密鑰，用以將該

六、申請專利範圍

編密節目內容的該第一部分解密。

17. 如申請專利範圍第15項之電腦可讀取媒體，其進一步包含：

提供一自由預覽密鑰；及

在該配送該編密節目內容的該第一部分之前，將該自由預覽密鑰提供給該客戶端。

18. 如申請專利範圍第15項之電腦可讀取媒體，其進一步包含：

提供一內容密鑰；

使用該自由預覽密鑰將該內容密鑰編密；及

將該編密的內容密鑰提供給該客戶端。

19. 一種電腦可讀取媒體，具有電腦可執行指令用以執行一方法，該方法包含：

提供配送給一客戶端的節目內容，作為一多重播放配送的一部分；

以一未編密的格式而將該節目內容的一第一部分配送至該客戶端，如此可提供該節目內容的一自由預覽；

編密該節目內容的一其餘部分；

將該節目內容之編密的其餘部配送至該客戶端。

20. 一種電腦可讀取媒體，具有電腦可執行指令，用以執行一提供節目內容給複數個客戶的方法，該方法包含：

提供一伺服器，用以與複數個客戶端電腦通訊；

建構該伺服器，如此用以將該節目內容提供給該等複數個客戶端電腦；

將該節目內容的一自由預覽提供給該等複數個客戶



六、申請專利範圍

端電腦；及

在該自由預覽期間，將一密鑰提供給每一購買客戶端電腦，以便將一部分的該節目內容的編密部分解密。

92.2.27 修正
年 月 日
補充

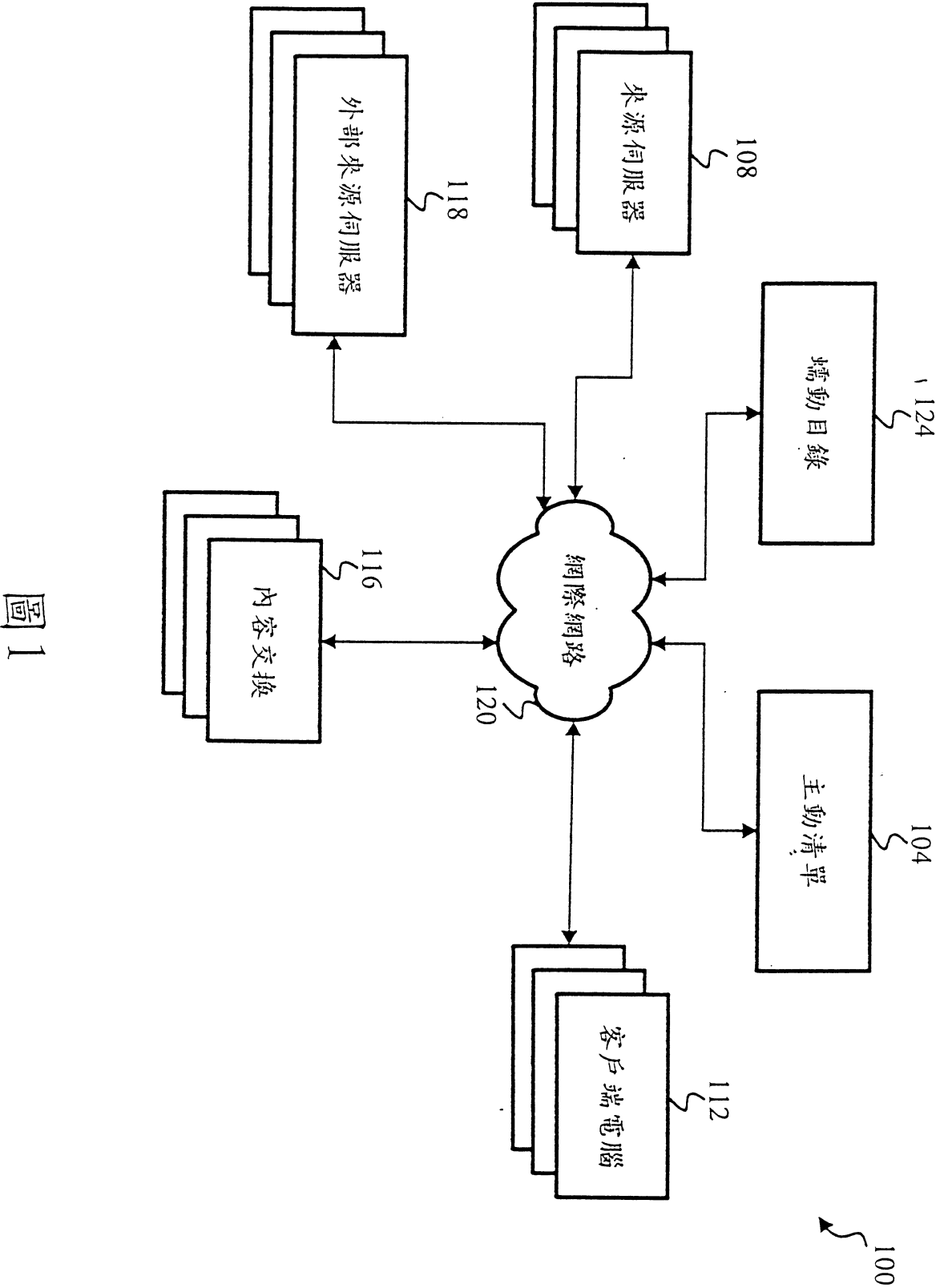


圖 1

92.2.27 修正
年 月 日
初版

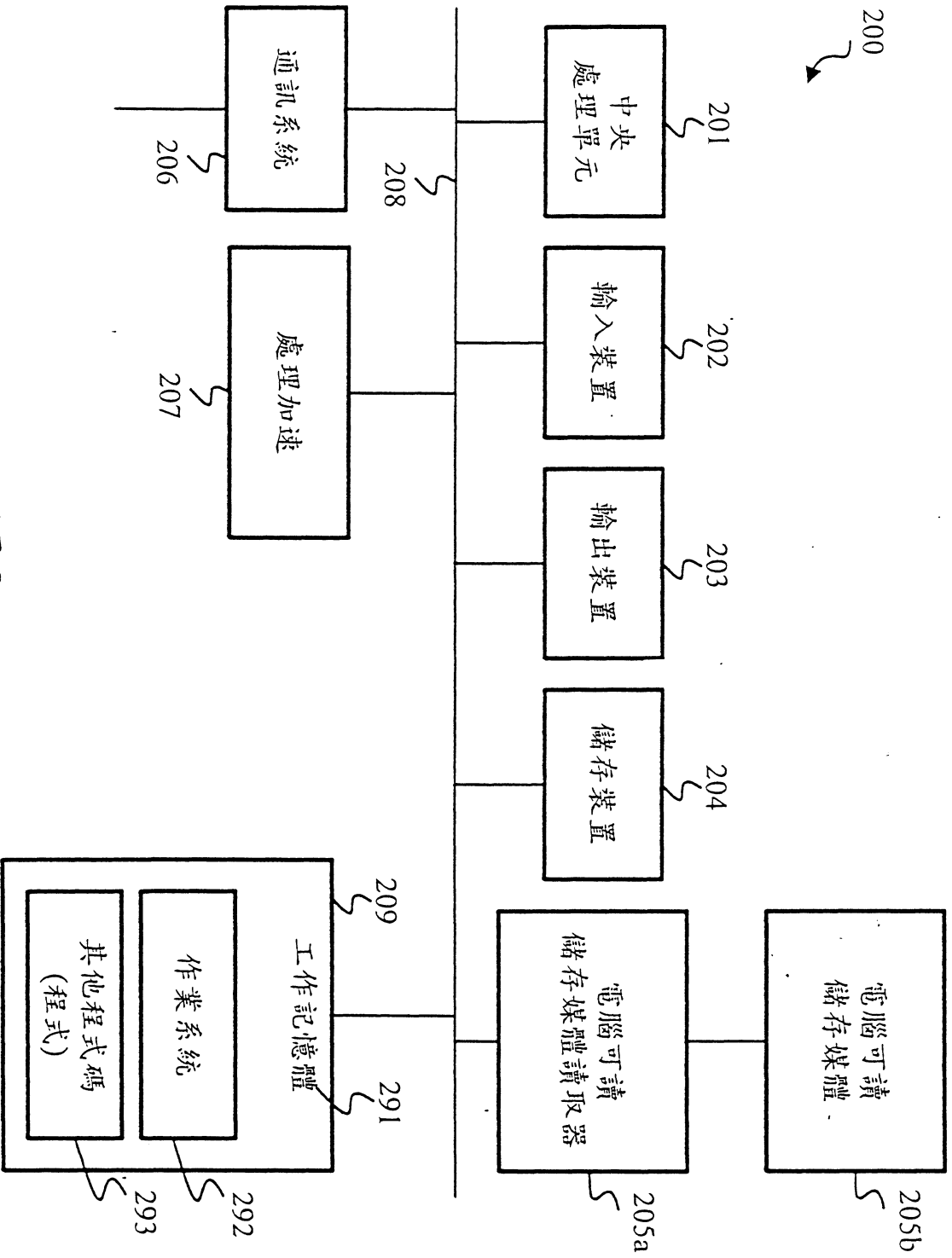


圖 2

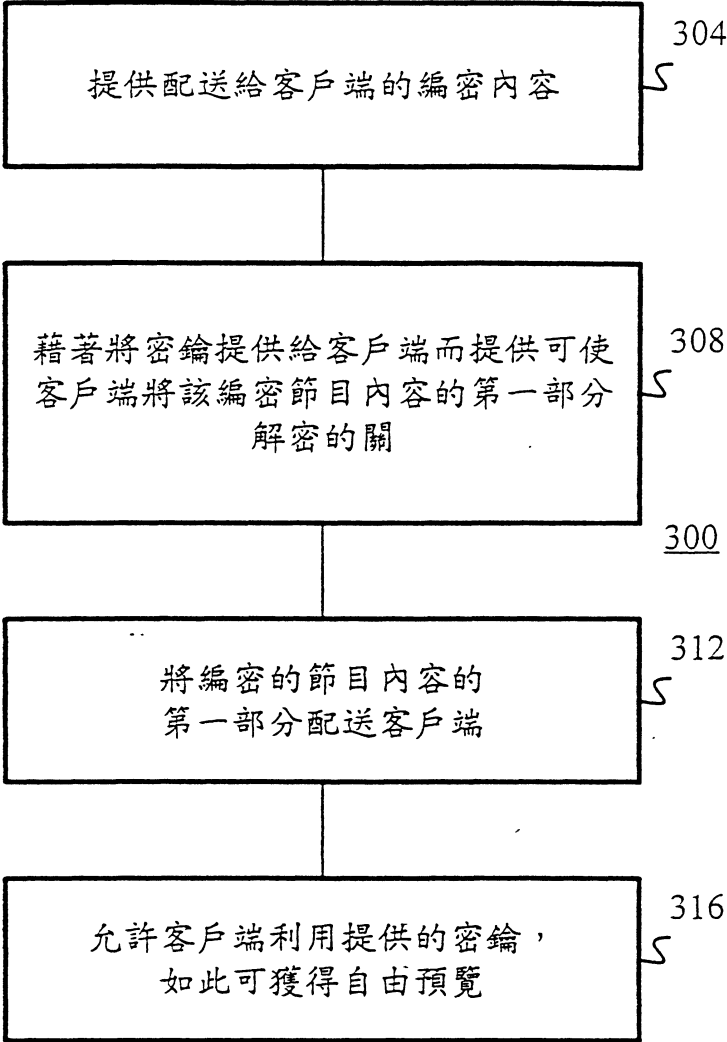
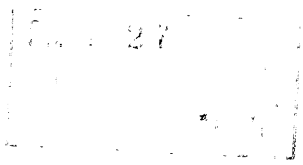


圖3

92.2.27 修正
年 月 日

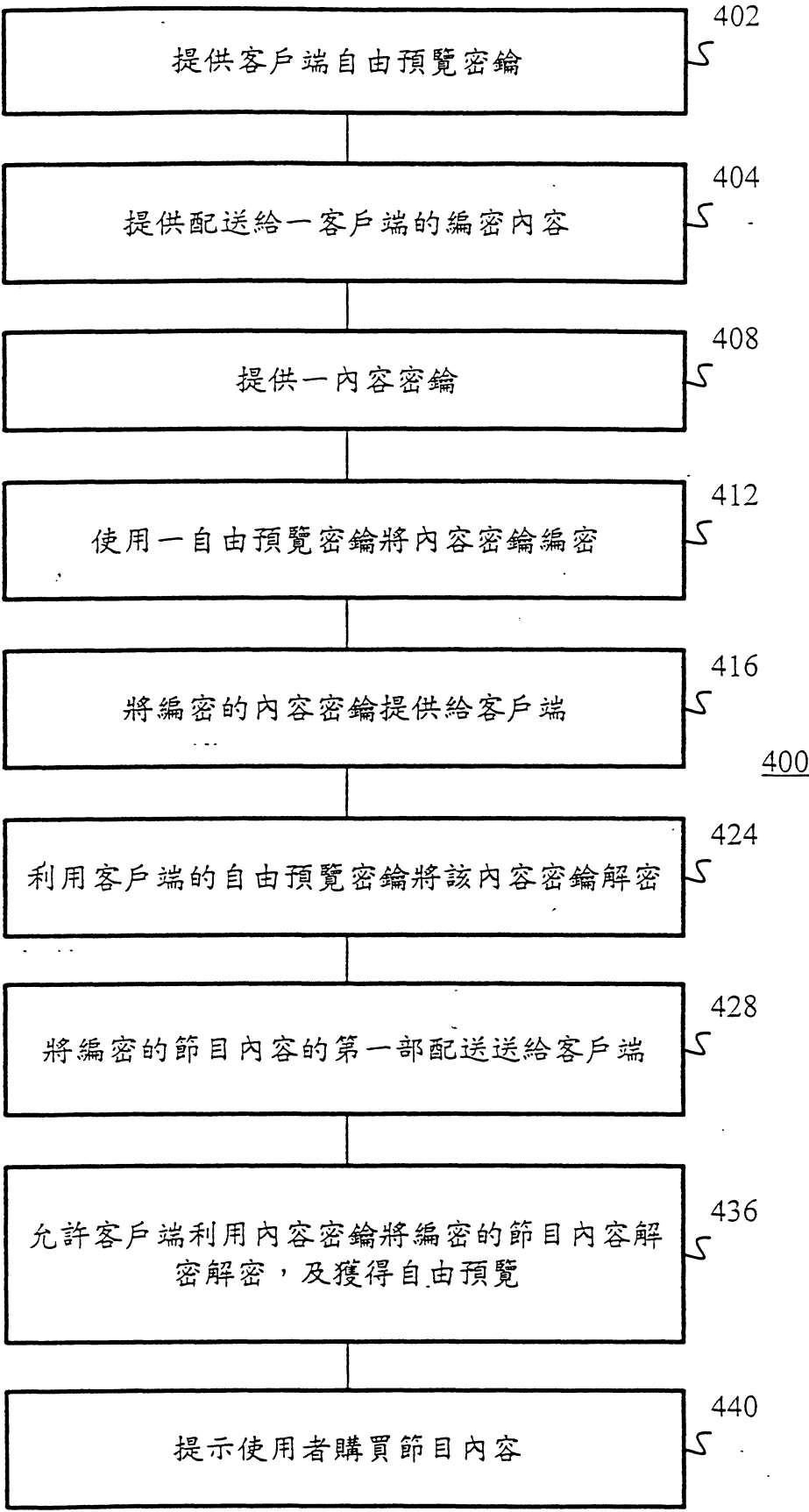


圖 4

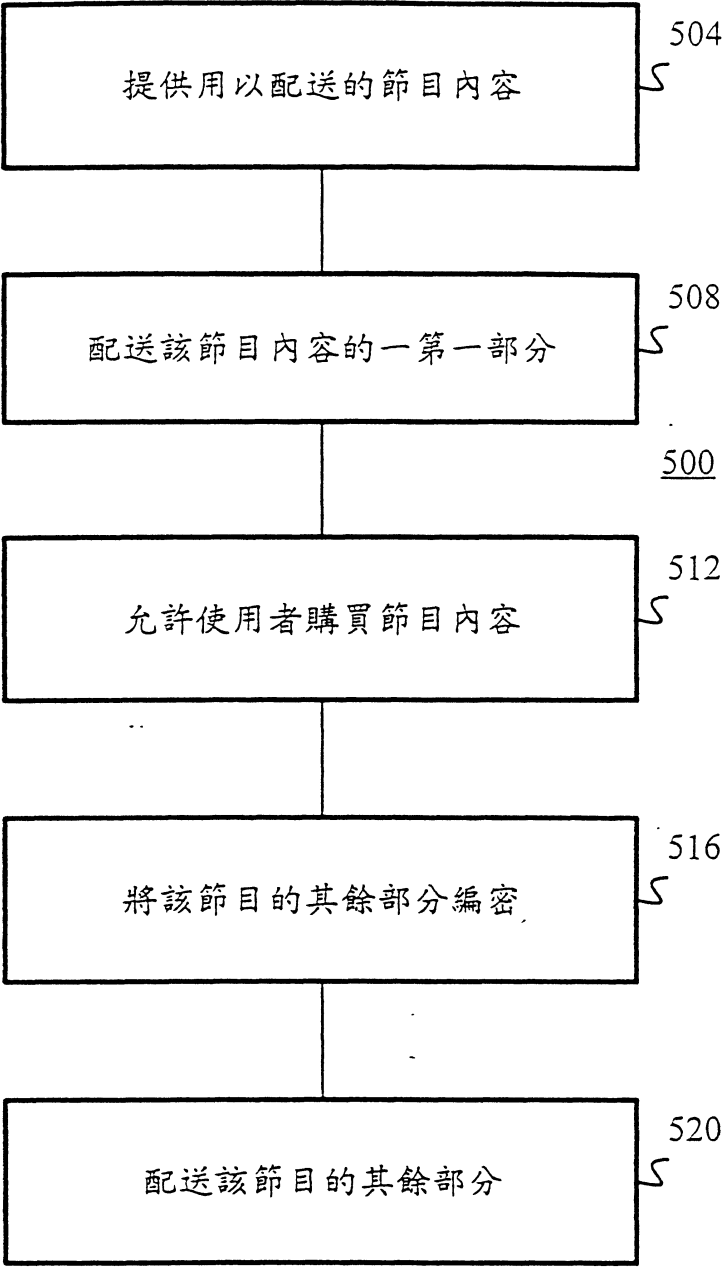


圖5

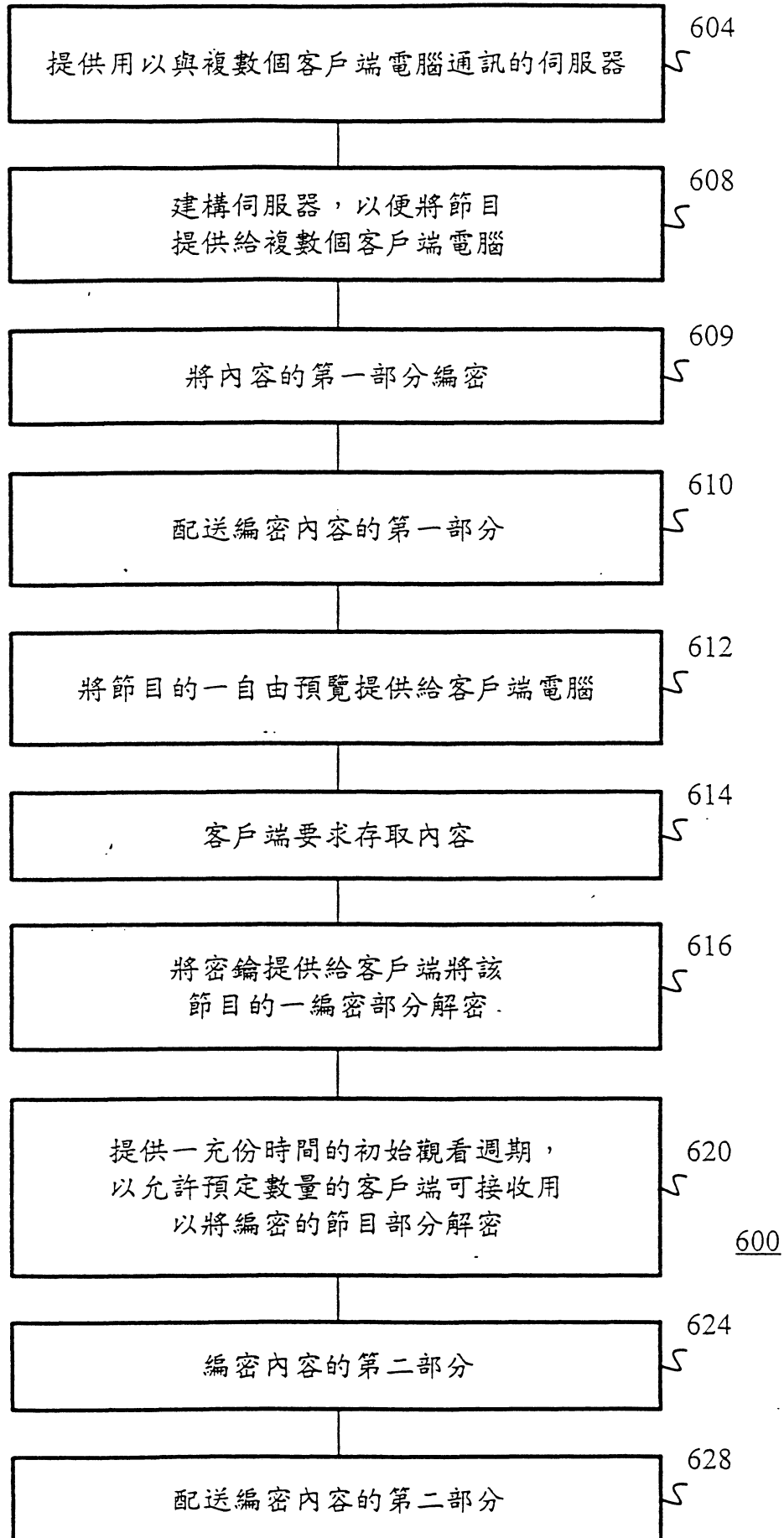


圖 6

92.2.27 修正
年 月 日

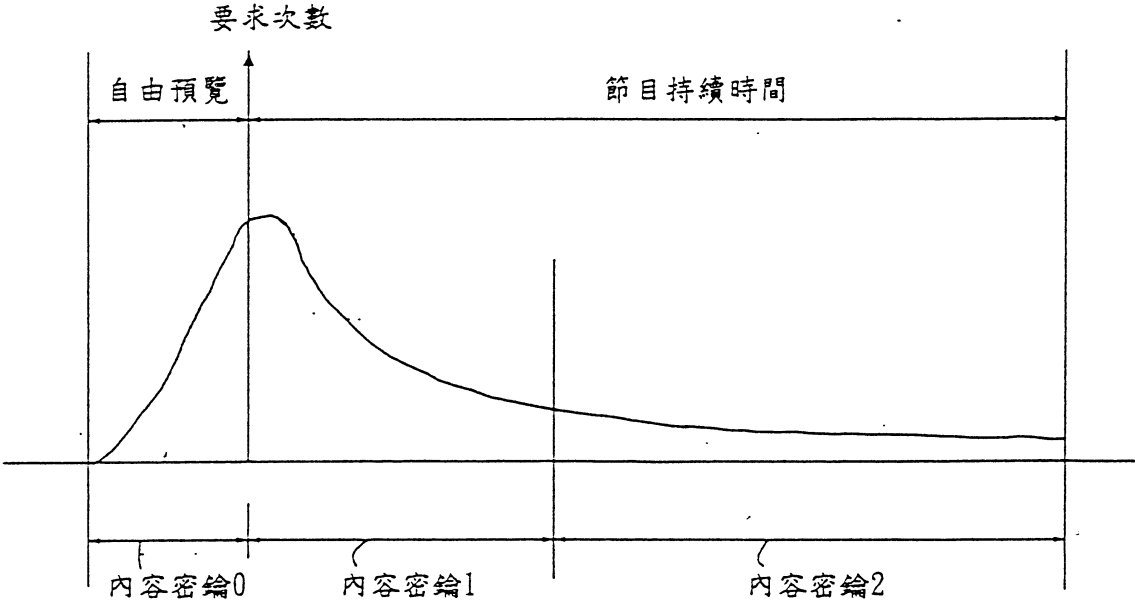


圖 7A

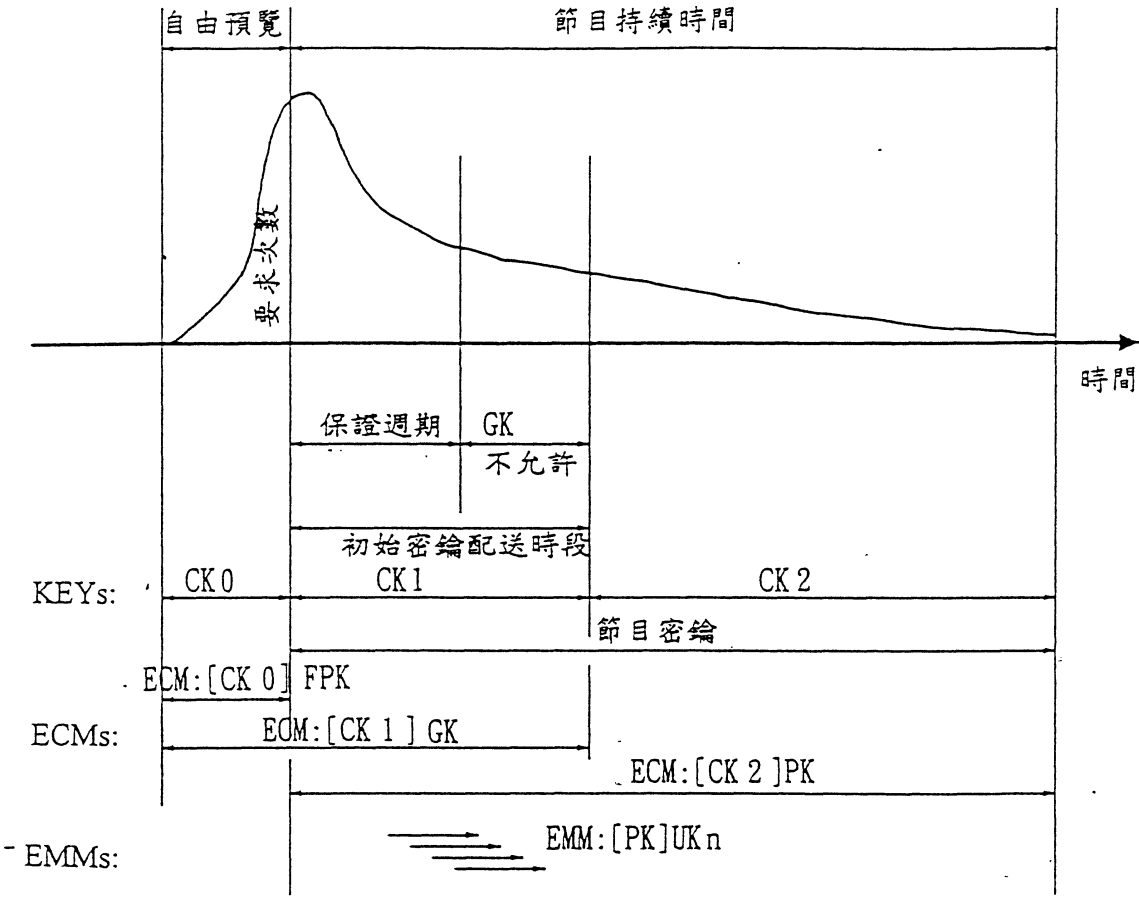
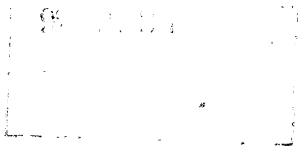


圖 7B

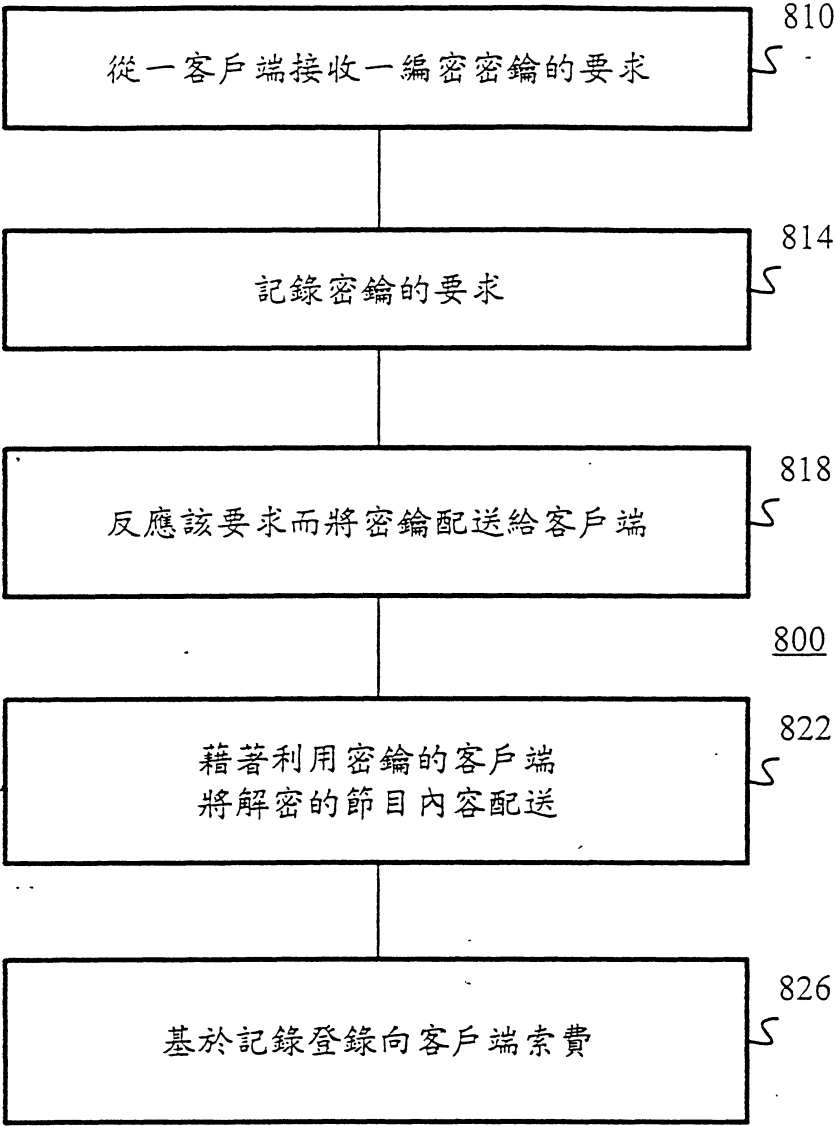
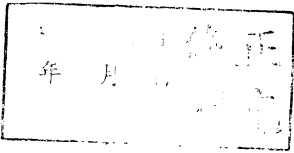


圖 8

92.9.27

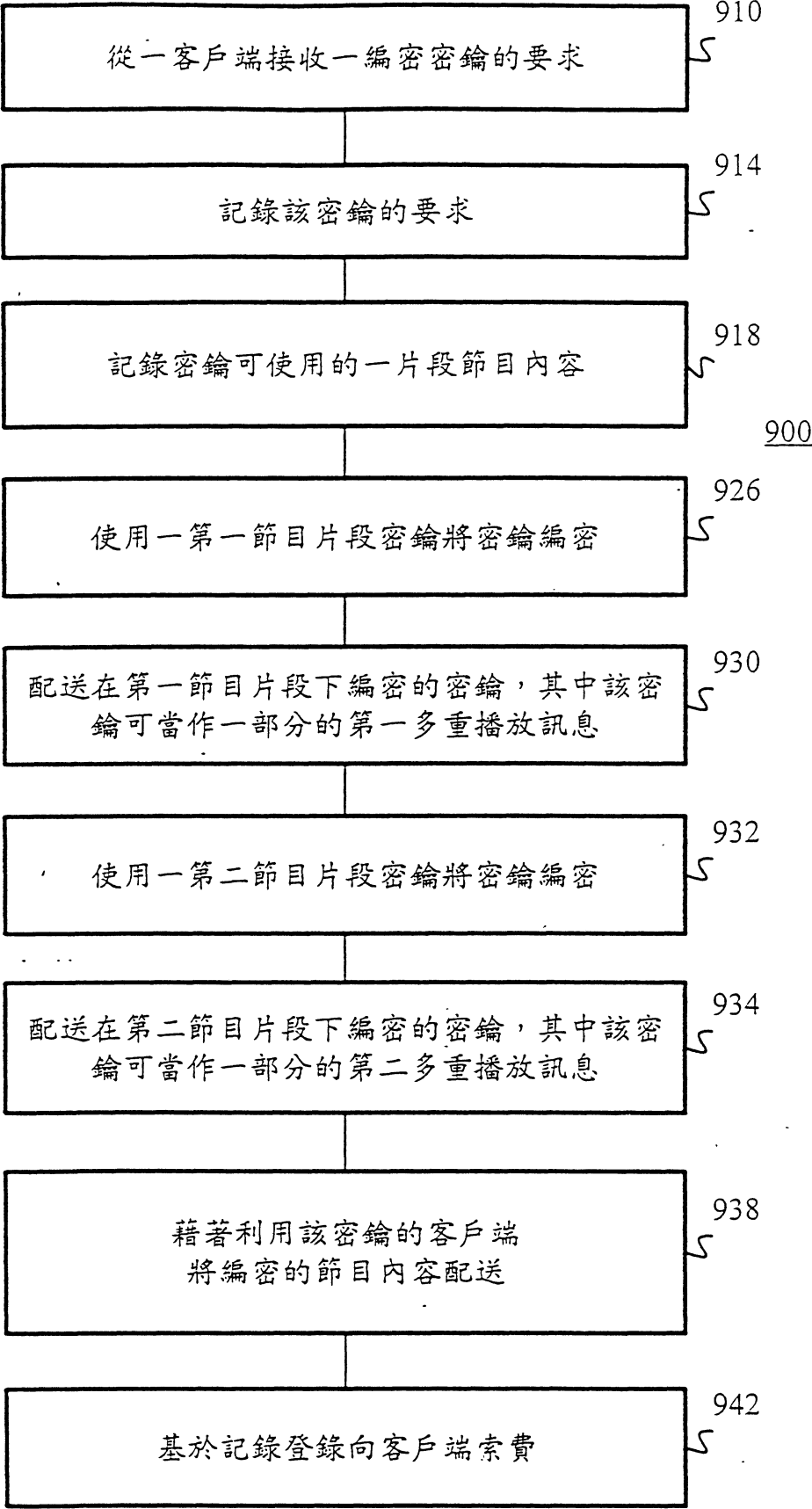


圖9

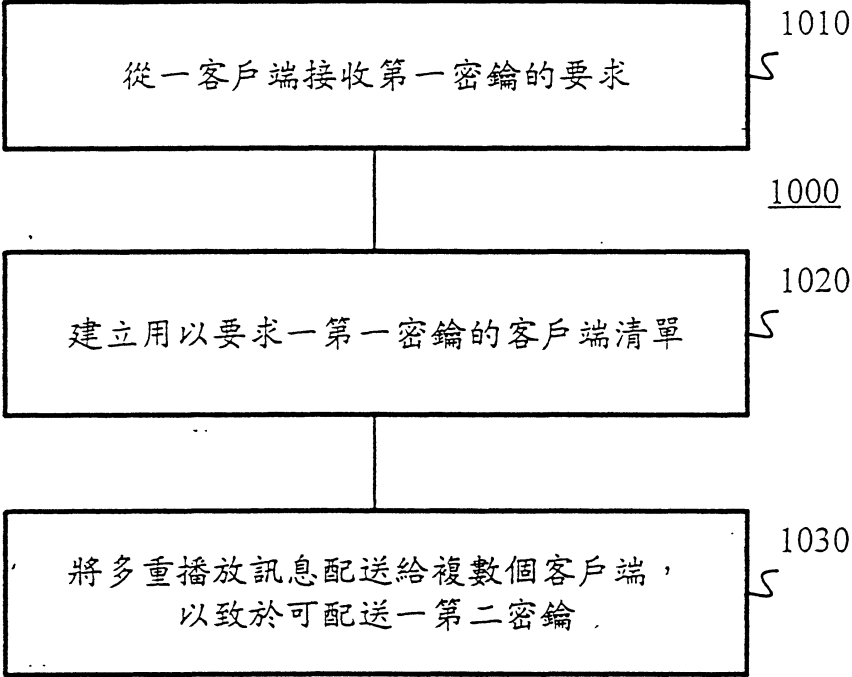
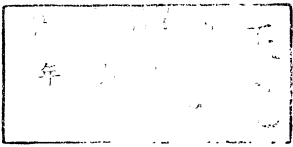


圖 10

92.2.27
4
6

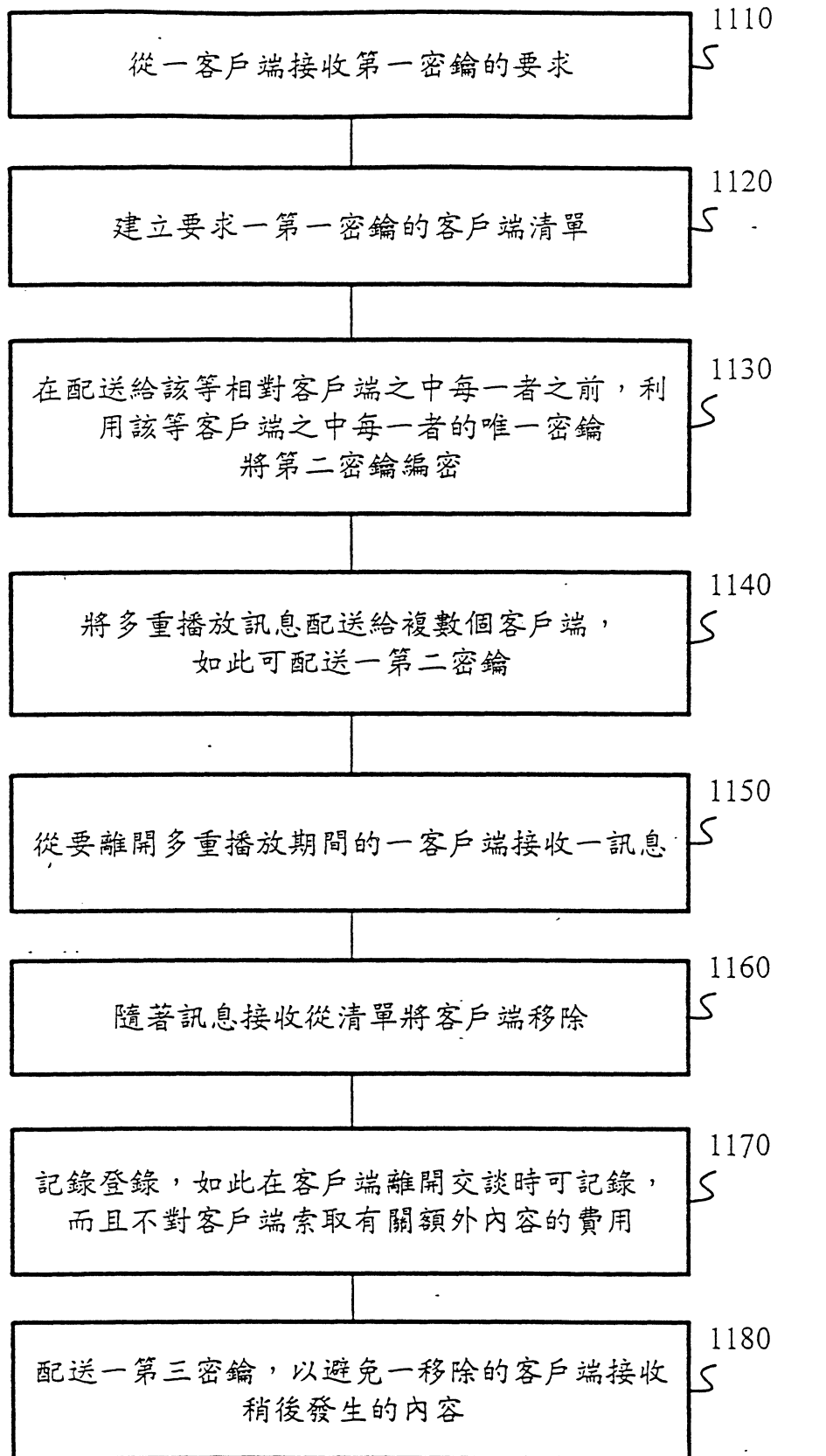
1100

圖 11

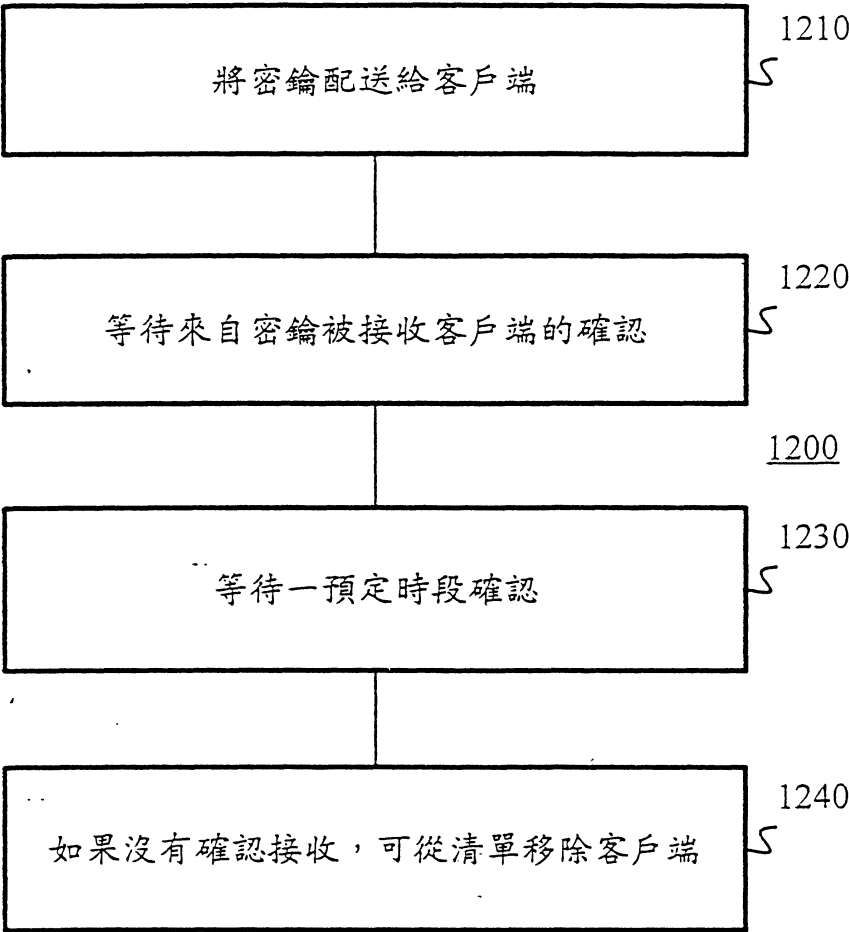
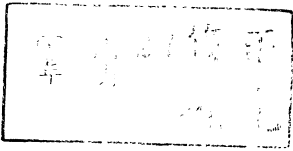


圖 12

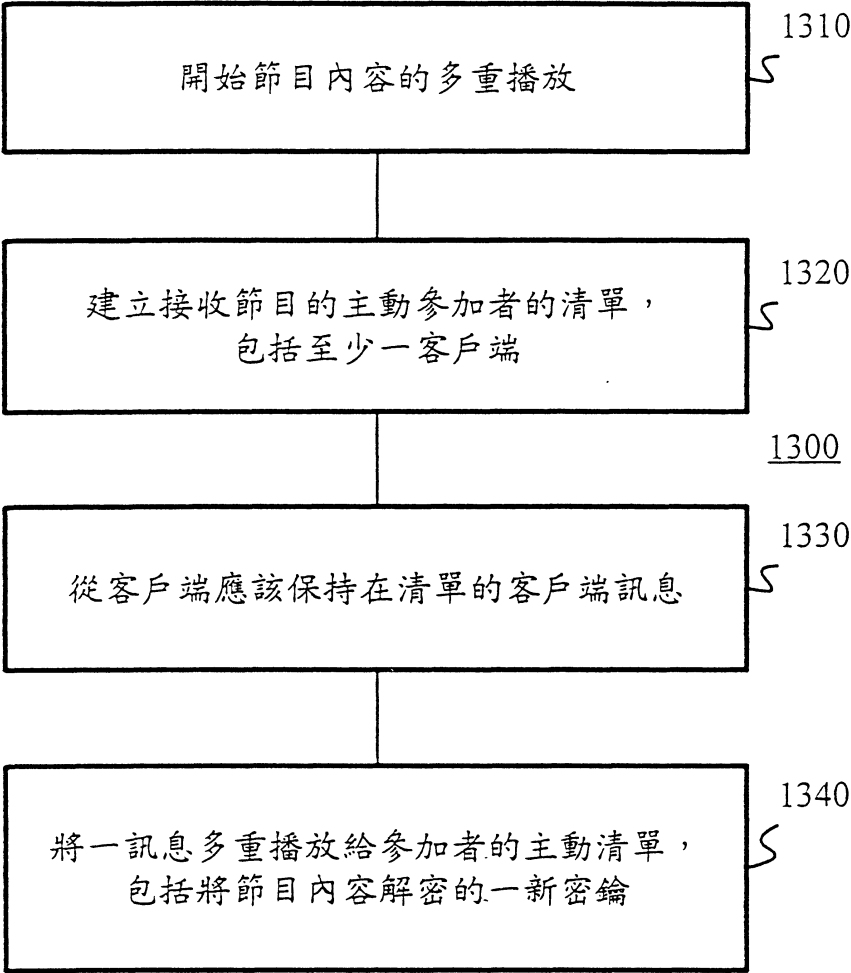


圖 13

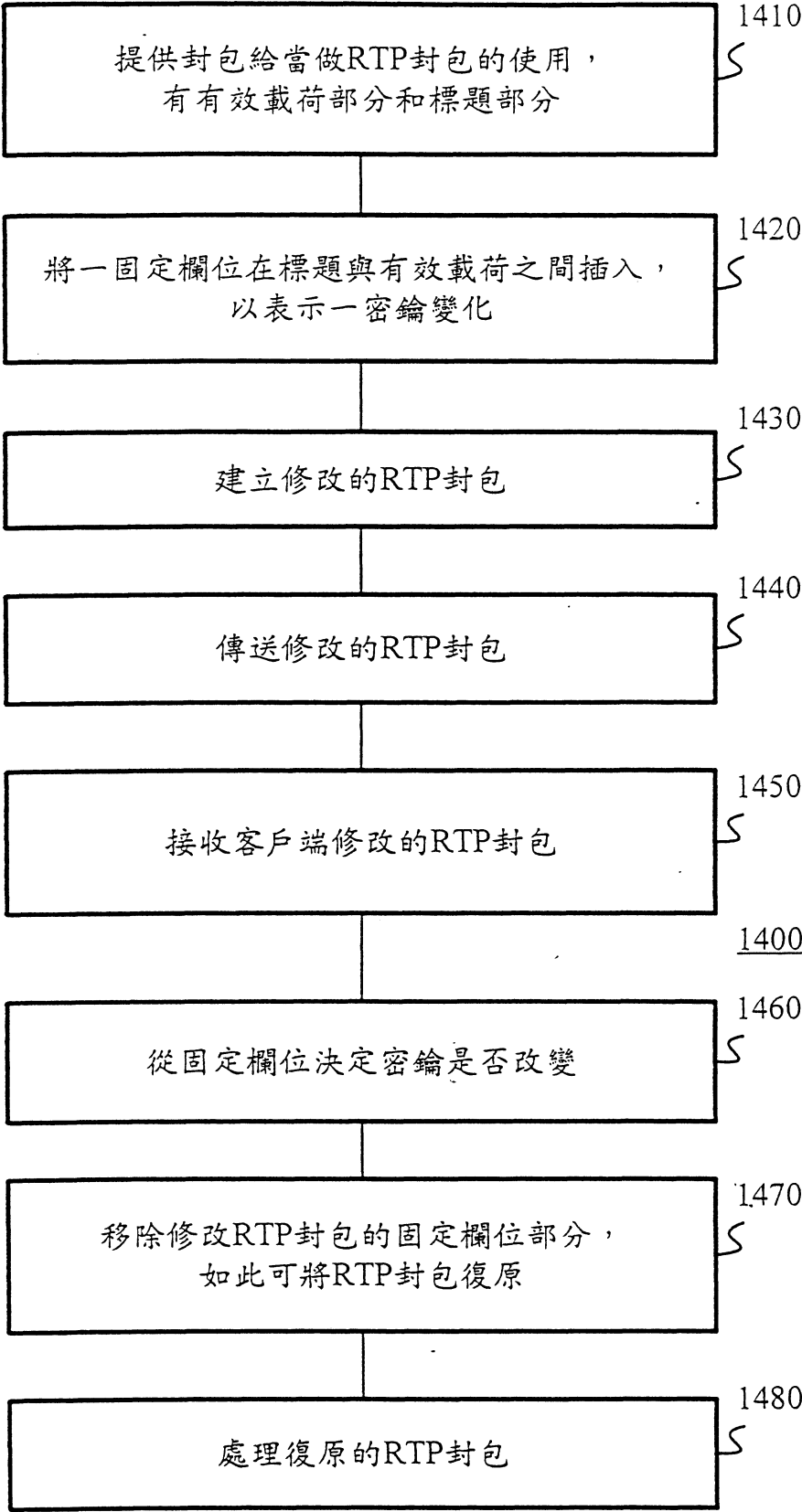
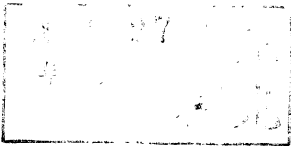


圖 14

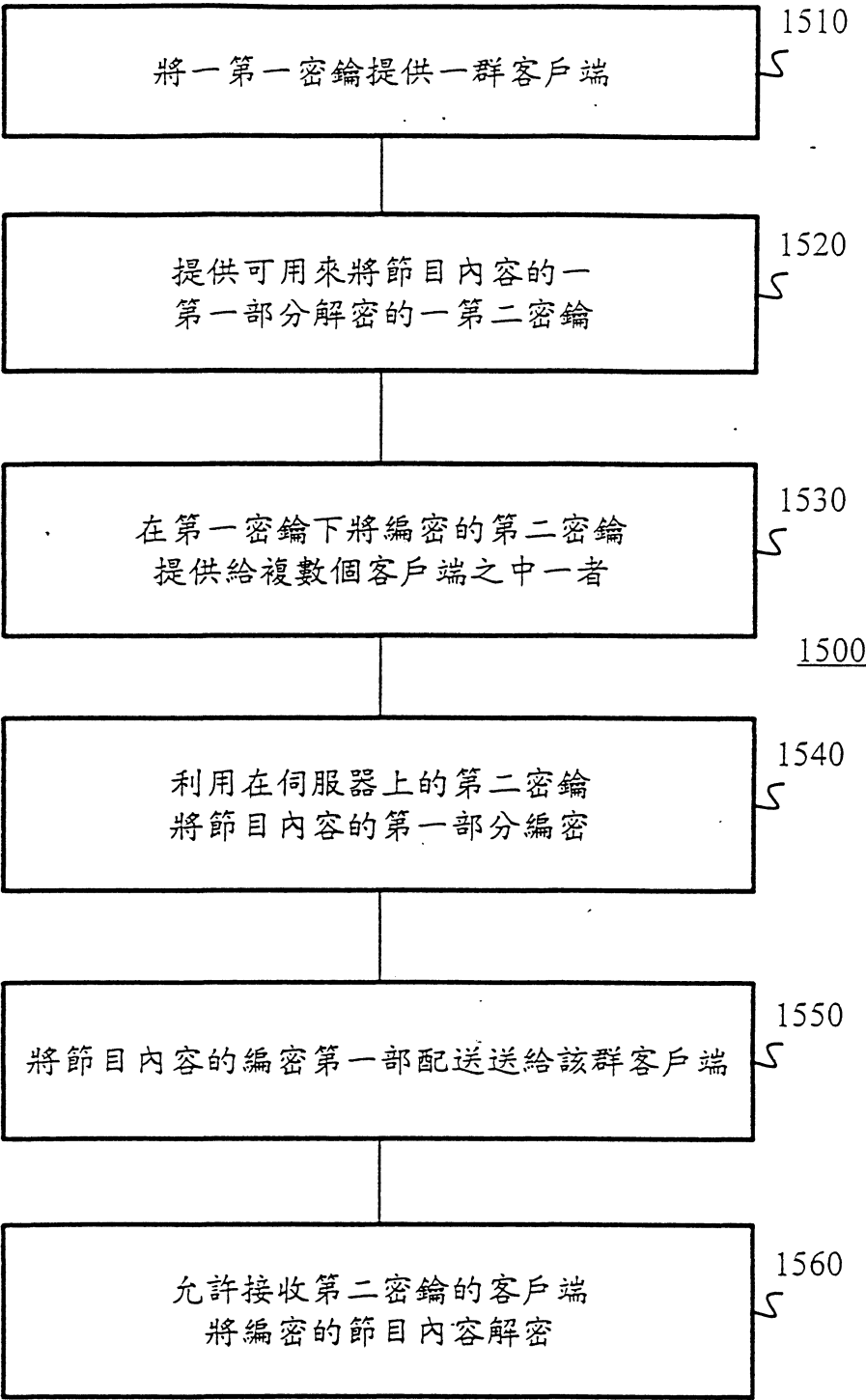
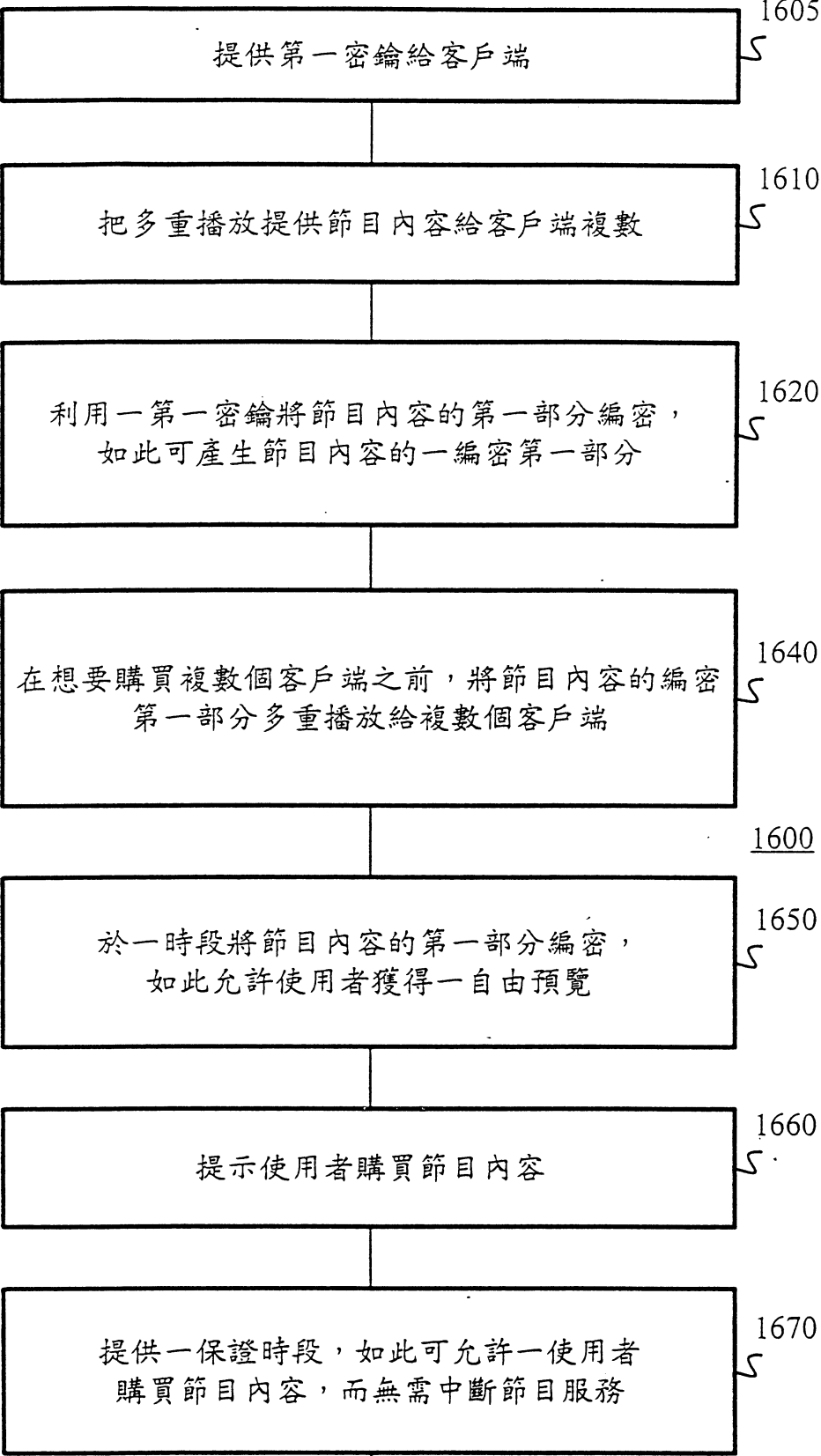


圖 15



A

圖 16A

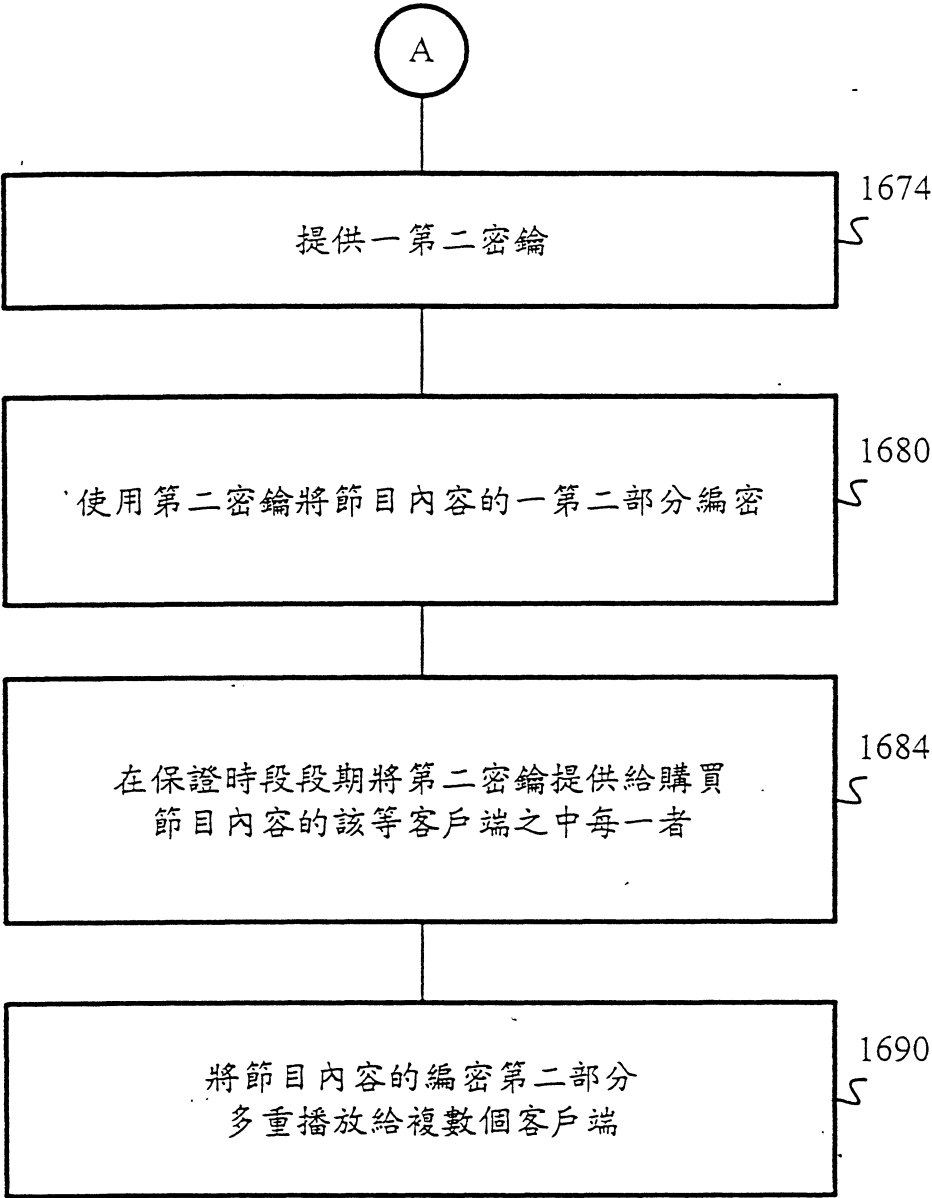


圖 16B

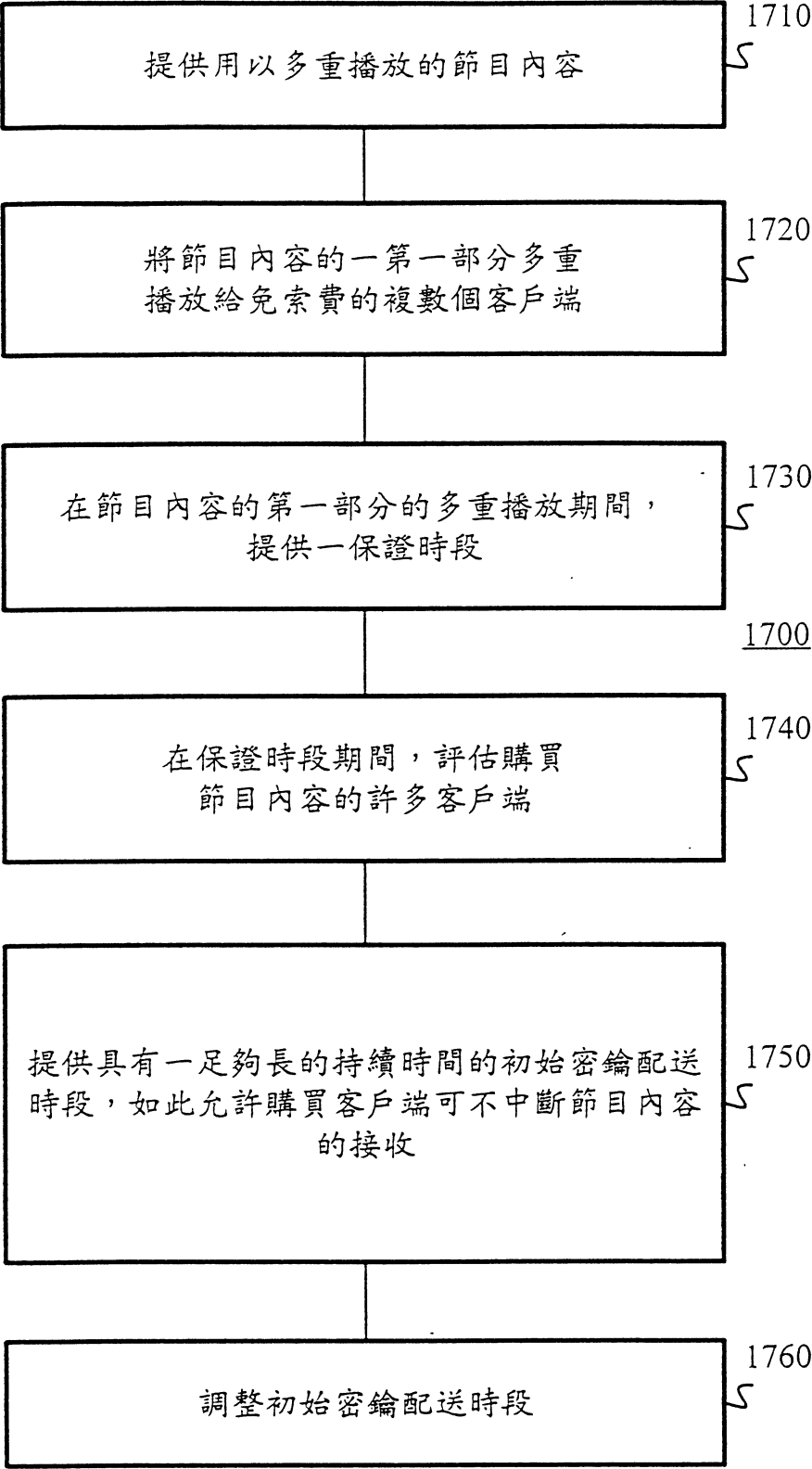


圖 17

92. 2. 27
年 月 日

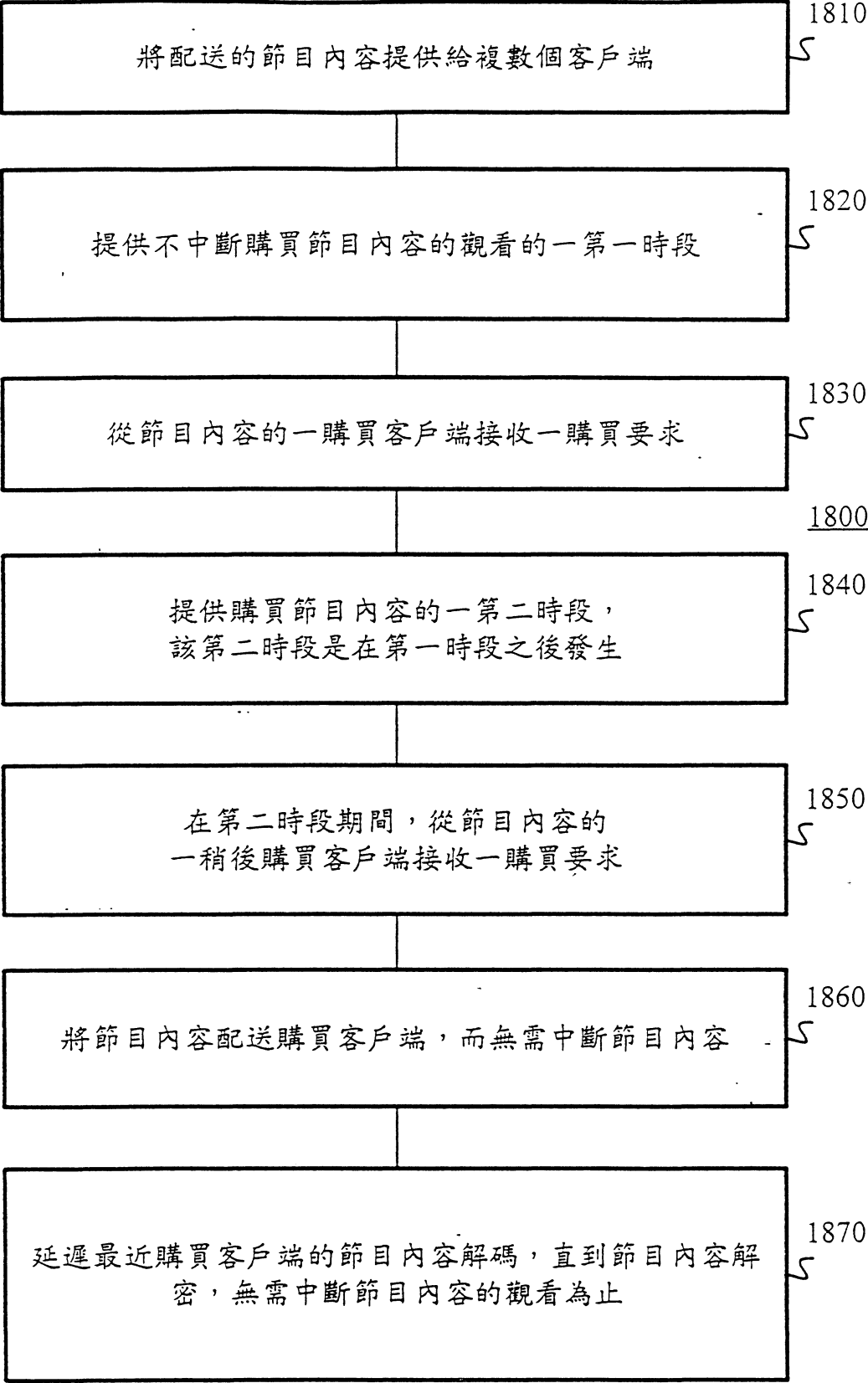


圖18

06. 7. 2003 正
年 月 日 刊
利 元

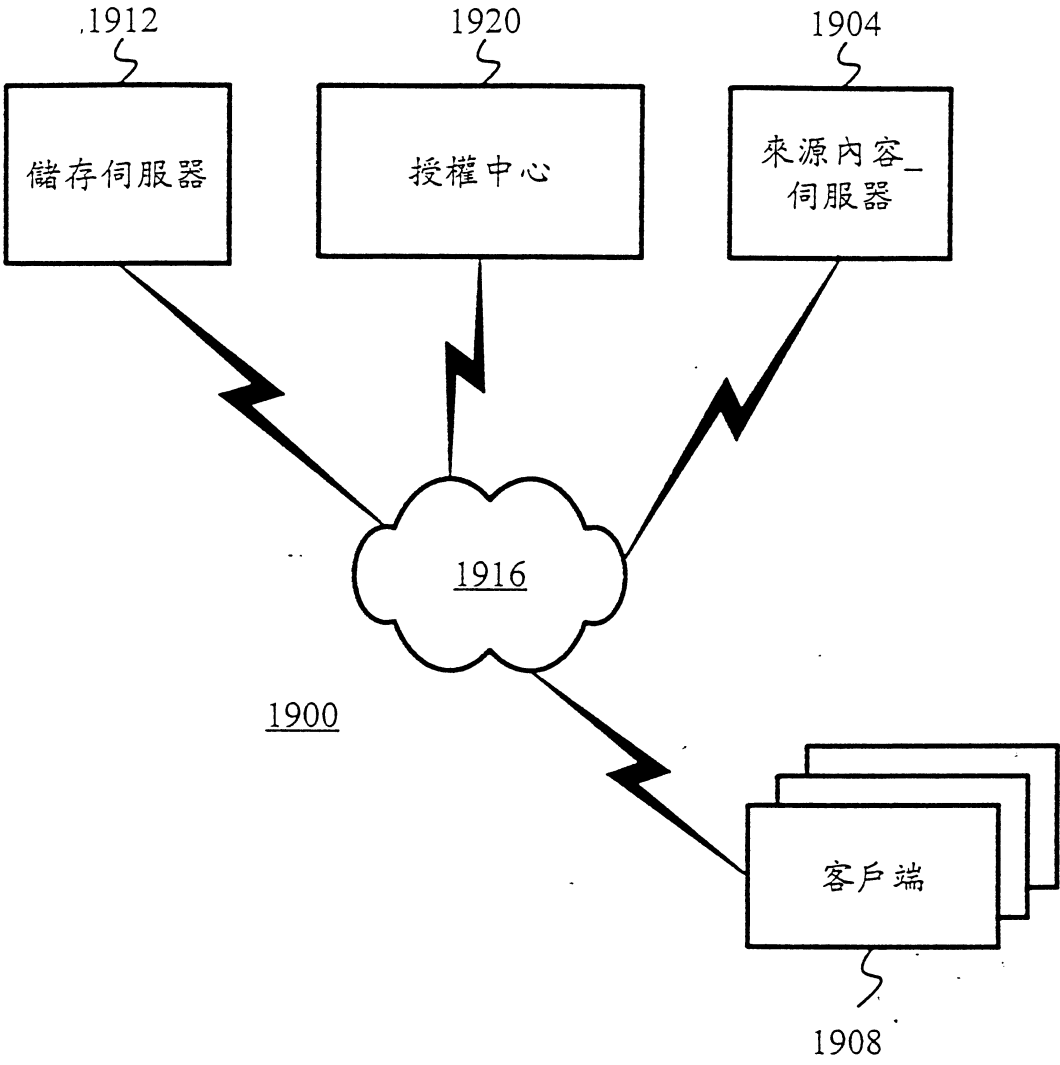


圖 19

92.2.27 修正
完

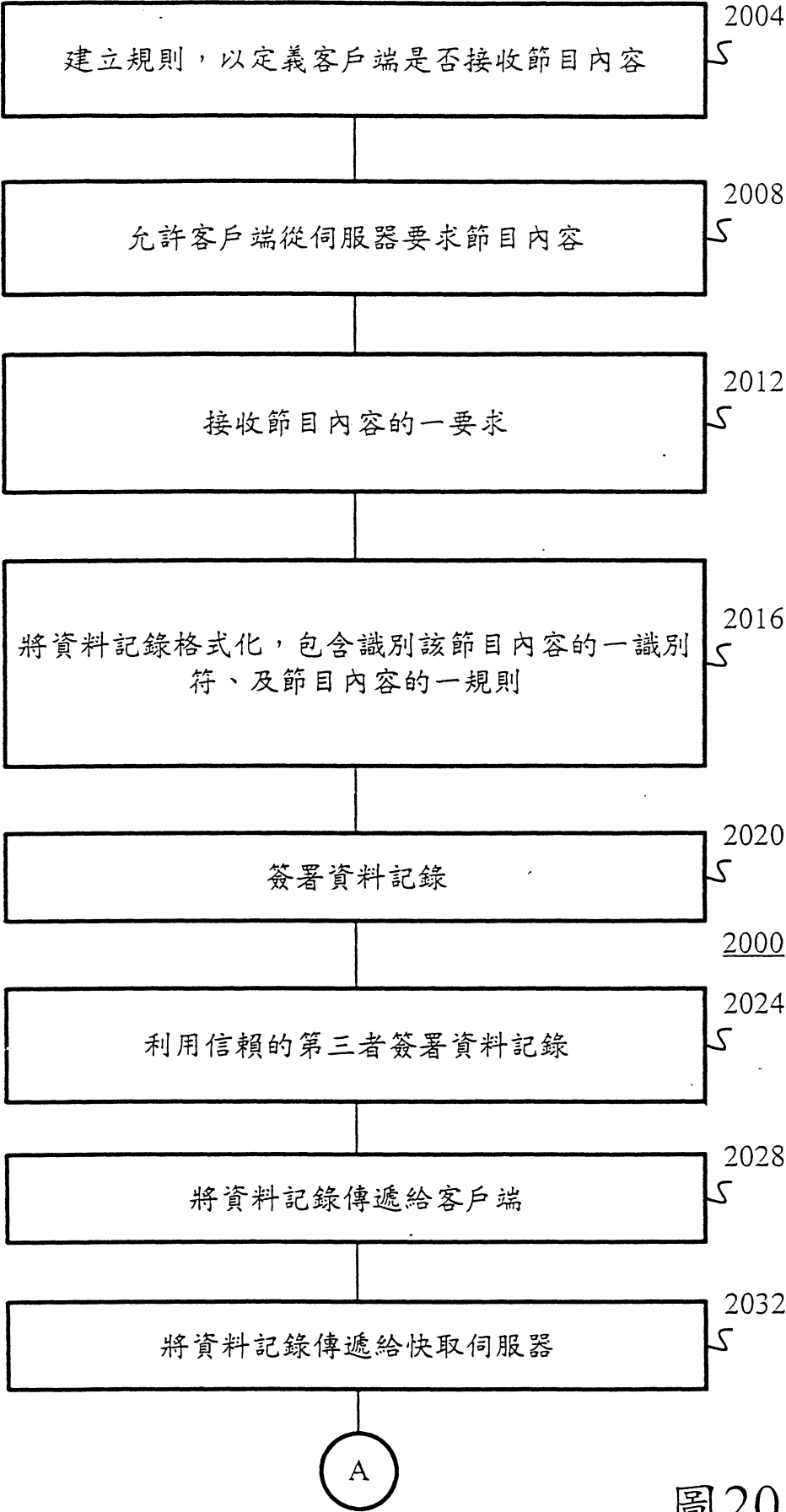


圖 20A

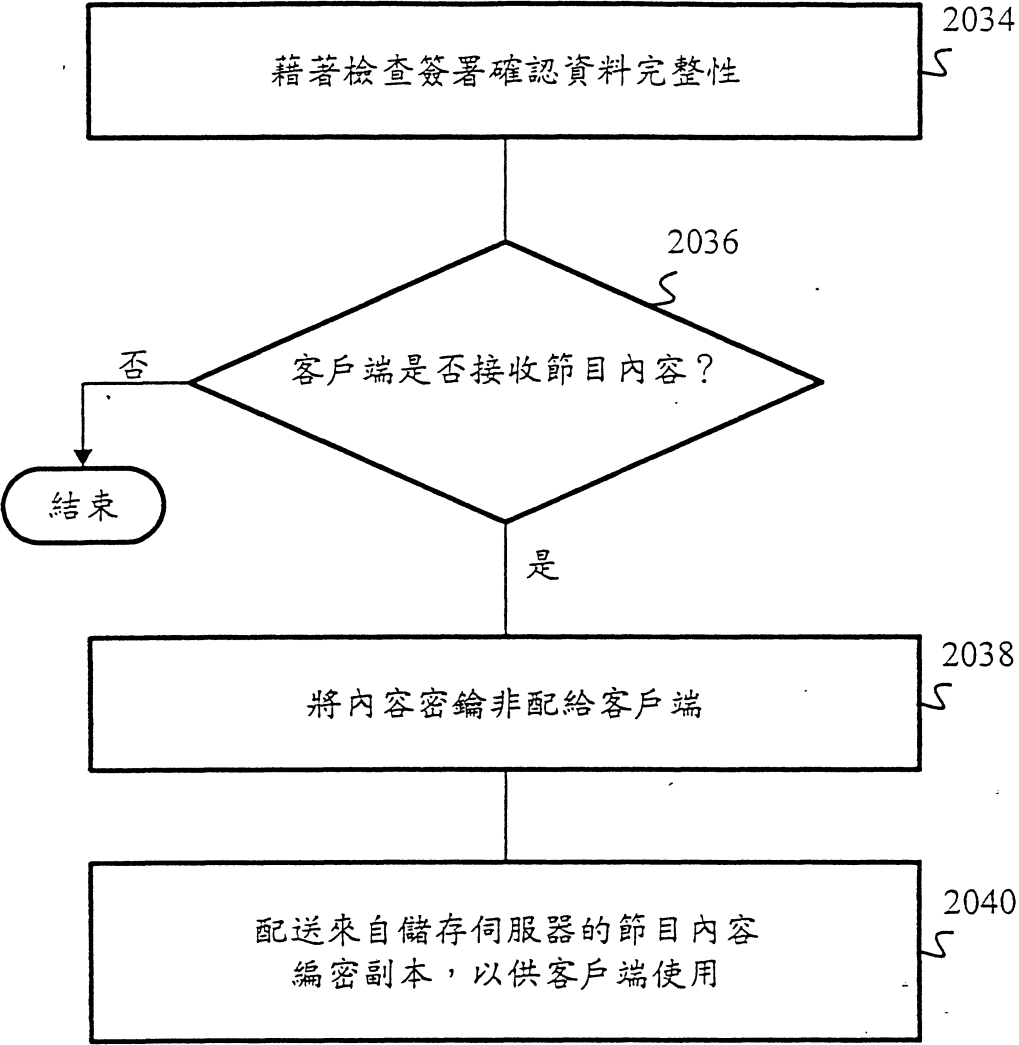


圖 20B

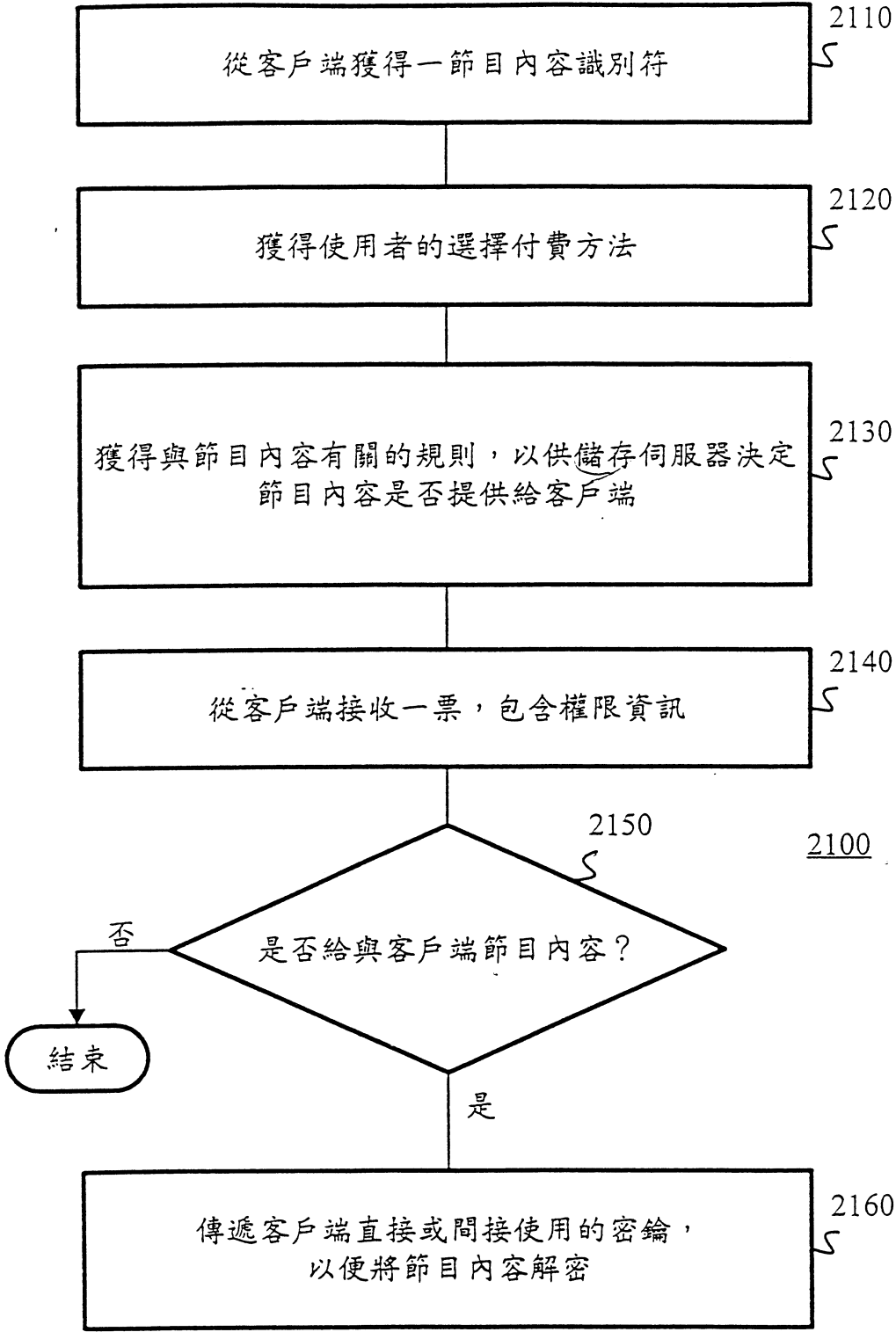
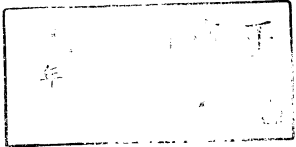


圖21

2200

節目內容ID	定義存取內容的規則	等級資訊	客戶端購買偏愛	認證資料
--------	-----------	------	---------	------

圖 22

客戶端位置	客戶端預約	認證資料	...
-------	-------	------	-----

圖 23