公告本

申請日期	88. 12. 28
案號	88123104
類別	H04L 9/32

（以上各欄由本局填註）

A4
C4

453089

發明專利說明書

一、發明名稱	中文	在一系統中保護資訊之技術
	英文	PROTECTING INFORMATION IN A SYSTEM
二、發明人	姓名	(1)理查J.高橋 (2)章明達
	國籍	(1)美國(2)中國大陸
	住、居所	(1)美國亞利桑那州鳳凰市南第35區14033號 (2)美國麻州威斯特福・巴登巷3號
三、申請人	姓名（名稱）	美商・英特爾公司
	國籍	美國
	住、居所（事務所）	美國加州聖塔克萊拉市密遜大學道2200號
	代表人姓名	小湯瑪斯F.唐洛普

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
IPC分類：	

本案已向：

美　國（地區）　申請專利，申請日期：1999,02,26　案號：09/259,426，☑有　□無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（1）

本發明係有關於一系統中之資訊保護。

電視節目與相關的資料可在數個不同的運用媒體上被播放，其可包括有線網路、數位衛星電視鏈路與其他有線或無線鏈路。消費者就其所喜歡觀看之特定節目或頻道（如電影頻道、每次觀賞須付費之節目）須付費之付費電視播放已變得逐漸普遍。為提供付費電視服務，條件存取系統已被播放者使用以促成有授權觀看者觀看此付費電視播放。

在條件存取系統中，播放節目內容典型上依據某些條件存取訊息通訊協定被加密。此外，一授權過程典型上被實施以促成加密內容被有授權的接收器之接收。該授權過程可包括傳送指令至每一可能的大量可定位址之接收器（例如位於機頂盒者）的每一個。

授權可藉由傳送以一接收器為目標或定位址之授權信號與該加密內容而被實施。該授權信號促成該被定位址之接收器依據條件存取通訊協定來將加密之內容解密，使得節目內容之清潔複製可被生產以便觀賞。

然而，在條件存取系統被傳輸之加密資訊可被未授權之解散碼器（descrambler）相當容易地被破解。此未授權之存取造成服務提供者之收益損失以及因額外未預期的負載而致之傳輸信號的品質惡化。因此播放信號或其他傳輸資訊需要有改進的保護做法。

一般而言，一種在一第一裝置與一第二裝置間安全地通訊內容之方法包括傳送該等第一與第二裝置之辨識資

五、發明說明（2）

訊至一第三裝置。該第三裝置根據該辨識資訊產生一預設的訊息。該等第一與第二裝置使用該預設的訊息被認證。

其他的特點與實施例將由下列的描述與由申請專利範圍變得明白的。

第 1A 圖為一資訊傳輸系統之一實施例的方塊圖。

第 1B 圖為依據第 1A 圖之系統之一實施例的接收器方塊圖。

第 2 圖圖示在第 1A 圖之通訊路徑與所儲存之資訊。

第 3A-3B 圖為依據第 1A 圖之系統中保護通訊的一實施例的過程之流程圖。

第 4 圖為第 3A-3B 圖之過程的狀態圖，其運用依據一實施例的公用鍵碼密碼通訊協定的離散對數版本。

第 5 圖為第 3A-3B 圖之過程的狀態圖，其運用依據另一實施例之單向雜湊函數訊息通訊協定。

第 6 與 7 圖為第 3A-3B 圖之過程的狀態圖，其運用更另一個實施例之數位簽名通訊協定以實施個體認證與運用一鍵碼交換密碼通訊協定以導出連線鍵碼（session key）。

在下列的描述中，許多細節被設立以提供對本發明之了解。然而，其將被熟習該技藝者了解本發明可被實作而不須這些細節，且由所描述之實施例來的許多變化與修改為可能的。

在此描述中，下列的術語可被使用。將被加密之訊息可被稱為明碼及已加密之訊息可被稱為密碼。將密碼回復

五、發明說明（ 3 ）

為明碼之過程可被稱為解密。保護訊息安全性之技術可被稱為密碼學，及破解密碼之技術可被稱為解密學。因此，明碼被加密以產生密碼，其再被解密以產生原始的明碼。密碼法則亦稱為綴字，係為一數學函數，或用以加密與解密之函數。藉由某些密碼法則，其有二相關的函數：一個用於加密及另一個用於解密不同。許多密碼法則存在，包括公用鍵碼法則(亦稱為非對稱法則)，其被設計成使得用於加密之鍵碼與用於解密之鍵碼不同。在實施公用鍵碼之系統中，該加密鍵碼可被稱為公用鍵碼，及解密鍵碼可被稱為私用鍵碼(亦被稱為祕密鍵碼)。另一個密碼法則包括鍵碼交換法則及使用單向雜湊函數之法則。

一種密碼技術使用連線鍵碼以對通訊加密與解密。一連線鍵碼通常僅被使用於一個或有限數目之通訊連線然後被丟棄。就不同的通訊使用分別的鍵碼使得該鍵碼較不可能損害。

參照第 1A 圖，一資訊傳輸系統可為一播放系統(如電視節目或其他型式視頻播放系統)，其包括一服務提供者 10 與數個接收處 12(如接收 TV 節目之家庭)。在其他實施例中，該資訊傳輸系統可包括其他型式之系統，如包括有網路(如地區網路、廣域網路、網際網路等)之系統、用於傳輸音頻信號之系統，如電話網路或細胞或其他無線通訊網路、或其他任何系統，其中資訊須在通訊頻道上被傳輸。在下列的描述中，實施例被參照，其中電視節目或視頻內容被傳輸到數個接收處；然而，其將被了解本發明不

五、發明說明（ 4 ）

受限於此層面，而是可包括其他者。

就如圖示於第 1A 圖者，服務提供者 10 可包括一頭端系統 14，其接收將被傳輸之內容（明碼）並依據某些資訊保護通訊協定（如條件存取通訊協定）來應用加密法則以產生加密後之資訊（密碼）。該加密後之資訊可在一輸送媒體 15 上被傳輸，例如纜線鏈路 16、衛星鏈路 18、電話線、地球鏈路、無線鏈路等。被傳輸之資訊在位於對應的接收處 12 之一個以上的接收器 20 被接收。每一接收器 20 適用於依據如條件存取通訊協定之特定保護通訊協定來將所接收之資訊解密，以再生該原來的節目內容（明碼）以被一個以上的顯示單元 22 顯示。

接收器 20 可包括一主機裝置 24，其可為一整合接收器 20 裝置（IRD），如一機頂盒，其被耦合於一展開點（POD）模組 26，如一條件存取模組（CAM）。該 POD 模組 26 可為一積體電路卡（如智慧卡）或其他電子裝置，亦可被插入該主機裝置 24 之一槽內，否則可與之電氣式地被耦合。為保護在 POD 模組 26 與主機裝置 24 間的通訊資訊，一複製或內容保護（CP）通訊協定可如下面進一步描述地被實施。

在接收器 20 內之 POD 模組 26 可被規劃以將某些型式之被傳輸資訊（包括依據條件存取通訊協定被加密之內容）加以解密及將若有之服務提供者 10 所傳輸的任何授權訊息解碼。其他型式之主機裝置 24 可包括電視、卡式錄音機、電腦或其他已整合接收器 20 以由頭端系統 14 接收資訊之裝置。

五、發明說明（ 5 ）

被頭端系統 14 在鏈路 15 被傳輸之加密後資訊被接收器 20 內之主機裝置 24 接收。根據該特定的接收器 20 是否被授權以將所接收之資訊解除散碼（例如根據一授權訊息），POD 模組 26 將所接收之信號解密以產生明碼。一授權訊息例如可在回應於一使用者要求在一接收處 12 觀看一特定節目或頻道下被頭端系統 14 被送至接收器 20。

為依據本發明之某些實施例來保護資訊，一複製或內容保護（CP）作法可在接收器 20 內被應用以防止或降低未獲授權之使用者可獲得對該資訊存取系統之存取的可能性。

為防止未獲授權之存取，一內容保護作法運用一密碼通訊協定以保護在 POD 模組 26 與主機裝置 24 間於鏈路 28 上被傳輸之資訊。為了驗證通訊協定與主機裝置 24 之身份，個體認證在 POD 模組 26 與主機裝置 24 間根據被頭端系統 14 傳輸之特殊具結訊息被實施。此外，使用由頭端系統 14 來之此訊息，POD 模組 26 與主機裝置 24 可產生一連線鍵碼用於將在 POD 模組 26 與主機裝置 24 間被傳輸之訊息加密及解密。有效的是，該內容保護作法在現存的條件存取系統（包括頭端系統 14 與 POD 模組 26）做為橋樑或鏈路通至在接收器 20（包括 POD 模組 26 與主機裝置 24）被實施之複製保護系統。

因此，依據一實施例，為了促成 POD 模組 26 與主機裝置 24 間之認證，一個第三個體被涉入，在此例中為頭端系統 14。該頭端系統 14 可儲存一個以上之資料庫，包

五、發明說明（ 6 ）

含為裝置 24 與 26 產生特殊具結訊息所由來之資訊。該具結訊息可由頭端系統 14 在回應於由接收器 20 來之對條件存取內容具結服務(其包括實施個體認證與連線鍵碼導出)的要求下被產生。一隨機計數機構亦可被放入於該認證過程中以更強健以抵抗「中間人」及一再播放攻擊，其中於 POD 模組 26 與主機裝置 24 間被傳輸之訊息可能被一入侵者監測以破解在接收器 20 被運用之該內容保護的綴字。一旦個體認證已被實施以確保 POD 模組 26 與主機裝置 24 二者均為驗證後之單元，一共用的連線鍵碼便可被導出以保護 POD 模組 26 與主機裝置 24 間之訊息。

依據某些實施例之內容保護系統運用許多可用的密碼通訊協定之一，其允許相當低的實施成本。可被使用之密碼通訊協定包括公用鍵碼法則(如 ElGamal 訊息認證碼)、單向雜湊函數法則(如 SHA-1 之保全雜湊法則)、與鍵碼交換法則(如 Diffie-Hellman 法則)。其他型態之密碼通訊協定亦可被使用，如 Rivest-Shamir-Adleman(RSA)法則(一種公用鍵碼法則)、數位簽名法則(一種公用鍵碼法則)、如 MD4 或 MD5 之訊息消化法則(單向雜湊函數)與其他法則。在本發明某些實施例中可被使用之這些列出的法則與許多其他型式之密碼法則被描述於 Bruce Schneier 所著的 "Applied Cryptograph"，John Wiley & Sons 公司出版，1996 年第二版。

參照第 2 圖，本發明之某些實施例所運用的個體認證過程雇用被信任之第三者 112，其能通過一個以上之主機

五、發明說明（ 7 ）

裝置 24 與 POD 模組 26 在一個以上之接收處 12 至頭端系統 14 於一保全頻道 114 上之公用或祕密鍵碼。舉例而言，此被信任之第三者可為 Cable Television Laboratories 公司(CableLabs)或某些其他複式系統操作者(MSO)。該被信任之第三者 112 產生公用或私用鍵碼(與/或其他驗證資訊)的清單，其被配以 POD 模組 26 與主機裝置 24 之裝置辨識元(如序列號碼)。此清單可在保全頻道 114 上與頭端系統 14 通訊。頭端系統 14 可由這些清單產生一個以上儲存於該頭端系統內之儲存媒體中的資料庫。例如，在所圖示的實施例中，頭端系統 14 包括資料庫 104 以儲存與 POD 模組 26 有關之驗證資訊與資料庫 106 以儲存與主機裝置 24 有關之驗證資訊。該等一個以上之資料庫被頭端系統 14 存取以為主機裝置 24 與 POD 模組 26 產生具結訊息，及在某些實施例中於個體認證過程之際用以驗證主機裝置 24 與 POD 模組 26 之身份。一旦個體認證已被實施，POD 模組 26 與主機裝置 24 可進一步產生連線鍵碼(其亦可以頭端系統 14 所送出之通訊為基礎)以保護彼此的通訊。

在此描述中，該資訊傳輸系統亦稱為條件存取/內容保護(CA-CP)系統。依據一實施例之 CA-CP 系統可包括數個元件，包括頭端系統 14，其為用於在輸送媒體 15 設立及加密內容之條件存取系統的一部分。頭端系統 14 亦儲存一個以上之資料庫(如 104 與 106)，包含有裝置 24 與 26 之驗證資訊。CA-CP 系統之另一個元件為輸送媒體 15 以允許頭端系統 14 與接收器 20 間(在上游路徑 116 與下游路

五、發明說明（ 8 ）

徑 118 上)之雙向通訊。在雙向通訊鏈路 15 上，接收器 20 依據一實施例可要求頭端系統 14 提供 CA-CP 具結服務以讓裝置 24 與 26 實施個體認證。由頭端系統 14 至接收器 20 的路徑 118 上之下游通訊包括在條件存取通訊協定下被傳輸之被保護內容以及被產生作為該 CA-CP 具結服務之一部分的訊息。

在個體認證與連線鍵碼導出已實施後，POD 模組 26 可依據 CA 通訊協定將由頭端系統 14 接收之密碼解密以產生被傳輸內容之乾淨的複製。POD 模組 26 接著使用依據在傳輸至主機裝置 24 前被導出之連線鍵碼來將該乾淨的內容加密，主機裝置 24 使用儲存在其內之連線鍵碼將被傳輸之資訊解密。主機裝置 24 與 POD 模組 26 間之介面可為一開放應用程式介面(API)。

進一步參照第 3 圖，個體認證與連線鍵碼導出之實施過程(亦被稱為具結服務)被圖示。接收器 20(在 302)在輸送媒體 15 之上游路徑 116 上傳輸主機裝置 24 與 POD 模組 26 二者之認證欄位(或認證欄位的部分)至頭端系統 14。在 POD 模組 26 內之 POD 認證欄位 100 可包括 POD 模組 26 之裝置辨識元 P_ID 以及其他資訊(如下面描述者)，且主機裝置 24 內之主認證欄位 102 可包括主機 24 之裝置辨識元 H_ID 以及其他資訊。被傳輸至頭端系統 14 之認證欄位 100 與 102(或此等認證欄位之部分)有效地提供一要求至頭端系統 14 以實施具結服務(包括個體認證與連線鍵碼導出)。在其他實施例中，一分離的訊息或一預先定義的旗

五、發明說明（9）

標或其他指標可構成一要求以開始一具結服務。

在頭端系統 14 內之一控制器 130 使用在被接收之認證欄位部分內的裝置辨識元 P_ID 與 H_ID 以分別(在 304)映象成為在資料 104 與 106 內對應的位置。在一實施例中，控制器 130 可被實作為硬體與軟體之組合。其硬體例如可包括如微處理器之處理器、被實作為特定用途積體電路(ASIC)或可程式閘陣列(PGA)之有限狀態機器之類。該硬體亦包括一個以上之儲存元件。在頭端系統 14 內之軟體包括一個以上之常規以在回應於由一個以上的接收器 20 來之要求下實施條件存取作業以及產生具結訊息。

PI_D 映象成為 POD 資料庫 104 內之位置 108，且 H_ID 映象成為主資料庫 106 內之位置 110。分別儲存於 POD 資料庫 104 與主資料庫 106 內之位置 108 與 110 的驗證資訊可包括下列配以 POD 模組 26 與主機裝置 24 之項目：一私用或秘密鍵碼、一公用鍵碼、一預定的簽名或其他的驗證資訊。儲存於 POD 與主資料庫 104 與 106 內之驗證資訊可被頭端控制器 130 使用以為提出要求之接收器 20 產生具結訊息，以選備地確認實際由被認證裝置 24 與 26 起源之認證欄位。認證可僅是簡單地檢查配以提出要求之接收器 20 的裝置 24 與 26 的認證資訊係被儲存於資料庫 104 與 106 中而被實施。或者，認證可藉由分別比較所接收之認證欄位部分之內容與儲存於資料庫 104 與 106 之位置 108 與 110 的認證資訊而被實施。若頭端控制器 130(在 306)能認證裝置 24 與 26，接著頭端系統 14(在 308)在輸送媒

五、發明說明（ 10 ）

體 15 之下游路徑 118 上送出具結訊息至 POD 模組 26。若頭端系統 14 不能認證提出接收器 20 之裝置 24 或 26 的至少之一，則一預設的錯誤訊息可(在 310)被送出。

POD模組 26由頭端系統 14所送出之具結訊息(在 312)決定主機裝置 24 是否為被認證之裝置。若該認證為成功的，則 POD 模組 26(在 316)傳輸具結資訊至主機 24 並(在 318)產生及儲存連線鍵碼以在 POD 模組 26 與主機裝置 24 間通訊保護使用。然而，若 POD 模組 26 不能認證主機裝置 24，則一錯誤訊息可(在 314)被產生。

在主機裝置 24 中，所接收之具結資訊被用以(在 320)認證 POD 模組 26。若認證不成功，則一錯誤訊息可(在 322)被產生。然而，若認證為成功的，則主機裝置 24 產生及儲存(在 324)該連線鍵碼以使用來將 POD 模組 26 所接收之內容解密。使用分離地被儲存於 POD 模組 26 與主機裝置 24 中獨立被導出之連線鍵碼，在接收器 20 中鏈路 28 上的保全通訊可(在 324)被實施。該等連線鍵碼被儲存於抗擅改之主機裝置 24 與 POD 模組 26 的儲存元件內。因此如所描述者，主機裝置 24 與 POD 模組 26 能根據被頭端系統 14 傳輸至主機裝置 24 與 POD 模組 26 之具結訊息來彼此認證。藉由使用依據本發明之某些具結處理，系統整合性可藉由降低所使用之保護通訊協定被未獲授權之使用者與裝置破解的可能性而被維持。此外，該認證可獨立於頭端系統 14 所運用之條件存取機構是何種而被實施。進而言之，本發明之某些實施例在具結處理之際為 POD 模組 26

五、發明說明（ 11）

與主機裝置 24 允許相當地之計算負荷。

參照第 1B 圖，主機裝置 24 與 POD 模組 26 之元件與層被圖示。每一主機裝置 24 與 POD 模組 26 分別包括一鏈路介面 200 與 202，其被耦合於鏈路 28。在一例中，主機裝置 24 中之鏈路介面 200 可被耦合於一槽以承接 POD 模組 26，其可為如智慧卡之電子卡。主機裝置 24 與 POD 模組 26 亦分別包括控制裝置 204 與 206 以控制個別裝置之作業。儲存於個別儲存元件之控制常規可分別在控制裝置 204 與 206 上被執行以實施各種工作。在 POD 模組 26 中，控制常規 207 可依據具結服務實施由頭端系統 14、個體認證與連線鍵碼導出被傳輸之條件存取密碼之解密，以依據一內容保護通訊協定之內容加密以在鏈路 28 上傳輸。在主機裝置 24 中，控制常規 205 可實施依據該具結服務之個體認證與連線鍵碼導出、在鏈路 28 上接收之內容的解密、及被解密內容之處理（包括用於顯示與/或其他操縱）。

儲存元件 208 與 210 亦分別被包括於裝置 24 與 26 內，以儲存如認證欄位、源於頭端系統 14 之具結訊息、由頭端系統 14 來之被傳輸內容、軟體指令及資料等。控制裝置 204 與 206 可為各種型式之控制裝置，包括微處理器、微控制器、ASIC、PGA、與其他可程式之裝置。儲存元件 208 與 210 可為一種以上各式記憶體，如動態隨機存取記憶體（DRAM）、靜態隨機存取記憶體（SRAM）、電氣可擦拭且可程式唯讀記憶體（EEPROM）、閃記憶體、及其他型式

五、發明說明（ 12）

之記憶體，如硬碟驅動器、磁碟片驅動器、CD與DVD驅動器。

為實施各種訊息作業，主機裝置24與POD模組26可分別包括下列單元：算術處理單元212與214、互斥OR(XOR)單元216與218、隨機數字產生器220與222、及計數器224與226。在主機裝置24內之單元212，216，220與224可被整合為單一的可程式裝置，如控制204，或被實作為離散的單元。POD模組26內之單元214，218，222與226亦可類似地被配置。此類單元亦可在軟體中被實作，例如為控制常規205與207之部分。或者，被控制常規205與207實施之工作可被硬體實施。

由於敏感的資訊可分別被保存於主機裝置24與POD模組26之儲存元件208與210中，對這些儲存元件之外部存取被防止。敏感資訊可包括公用與私用鍵碼或在具結處理被使用之其他資訊，以及被內容保護通訊協定保護之用於通訊之任何被導出的連線鍵碼。

下列描述資訊傳輸系統之實施例，其實施下列密碼法則之一用於具結服務之績效：ElGamal法則，其為公用鍵碼之離散對數版本(第4圖)、SHA-1法則，其為單向雜湊函數法則(第5圖)、與Diffie-Hellman鍵碼交換法則及數位簽名法則之組合(第6-7圖)。然而，其將被了解本發明將不受限於此所描述之實施例，而其他型式之密碼法則亦可在進一步之實施例中被實施。

參照第4圖，依據一實施例之保護通訊協定的狀態圖

五、發明說明（13）

被圖示，其實施 ElGamal 法則以進行個體認證與連線鍵碼導出。在所圖示之實施例中，三個分離的階段被包括。在第 1 階段中，包括有 POD 模組 26 與主機裝置 24 之內容保護系統的建立被實施。在此預置化之際發生，如在 POD 模組 26 於初期被插入主機裝置 24 時或在主機裝置 24 被電力循環時。第 1 階段包括五個狀態，其中訊息在主機裝置 24、POD 模組 26 與頭端系統 14 間被交換，以確保傳送主機裝置 24 與 POD 模組 26 之認證欄位中的資訊至主機裝置 24。在第 2 階段中，個體認證與連線鍵碼導出被實施。第 2 階段包括三個狀態(6，7 與 8)。一旦第 2 階段已完成，POD 模組 26 與主機裝置 24 間之通訊可依據內容保護通訊協定被保護，其可包括密碼法則，如對稱緩字法則，其運用分離地在裝置 24 與 26 被導出及被儲存之一連線鍵碼。

如第 4 圖顯示者，儲存在主機裝置 24 之儲存元件 208 的認證欄位可包括其裝置辨識元（H_ID）、其私用鍵碼 H、其公用鍵碼 G^HmodN 與一隨機數字產生器(RNG)種子 S_H(在下面描述)。POD 模組 26 可在其儲存元件 210 儲存下列認證欄位：其裝置辨識元 P_ID、其私用鍵碼、其公用鍵碼 G^PmodN 與 RNG 種子 S_P。N 為一預先定義之質數、G 為一預先定義作為產生器之隨機數字；及 modN 代表 N 之模數。在頭端系統 14 中，依據所圖示之實施例，POD 模組公用鍵碼 G^PmodN 之倒數(G^{-P}modN)被儲存為資料庫 104 中之驗證資訊，及主公用鍵碼 G^HmodN 之倒數(G^{-H}modN)被儲存為資料庫 106 中之驗證資訊。

五、發明說明（ 14 ）

在設立階段(第 1 階段)之際，主機裝置 24 在狀態 1 產生一隨機數字 M_H 並在鏈路 28 上傳輸下列之字{H_ID||M_H}至 POD 模組 26。就如在此描述中所使用者，"A||B" 項表示在資料流中欄位 A 與 B 之連結。在狀態 2，POD 模組 26 產生其隨機數字 M_P 並導出一共同計數值 M_O，其為 M_P 與 M_H 之互斥 OR 值：

$$M_O = M_P \oplus M_H$$

接著，POD 模組 26 送出含有連接裝置 ID{P_ID||H_ID}之資料流至頭端系統 14，其為 POD 模組 26 與主機裝置 24 之認證欄位的部分。該認證欄位部分為具結服務已被求之對頭端系統 14 的指示。在狀態 3 中，根據所接收之 P_ID 與 H_ID 值，頭端控制器 130 分別存取資料庫 104 與 106 之位置 108 與 110，以擷取驗證資訊 G^{-P}modN 與 G^{-H}modN。在狀態 3 中，頭端控制器 130 計算所擷取之值的模數乘數以獲得具結訊息 $G^{-(P+H)}$modN：

$$G^{-(P+H)}\text{mod}N = [G^{-P}\text{mod}N][G^{-H}\text{mod}N]\text{mod}N$$

該具結訊息在頭端系統 14 與接收器 20 間之鏈路 15 上被傳輸回到 POD 模組 26。在狀態 4 中，POD 模組 26 實施所接收之值 $G^{-(P+H)}$modN 與其公用鍵碼 G^{P}modN 的模數乘數以獲得 G^{-H}modN：

$$G^{-H}\text{mod}N = [G^{-(P+H)}\text{mod}N][G^{P}\text{mod}N]\text{mod}N$$

然後 POD 模組 26 在鏈路 28 上送 $G^{-(P+H)}$modN 與隨機數字 M_P 連結後之{$G^{-(P+H)}$modN ||M_P}至主機裝置 24。

接著在狀態 5，主機裝置 24 藉由實施 M_P 與 M_H 之互斥 OR

五、發明說明（15）

亦獨立地導出共同計數值 Mo。此外，主機裝置 24 藉由實施被頭端系統 14 連線鍵碼之具結訊息與主裝置之公用鍵碼的模數乘數而計算 $G^{-P}modN$：

$$G^{-P}modN = [G^{-(P+H)}modN][G^{H}modN]\ modN$$

狀態 1-5 完成設立階段，其中包括主機裝置 24 與 POD 模組 26 之裝置 ID、隨機數字 M_H 與 M_P 與具結訊息之訊息已在主機裝置 24、POD 模組 26 與頭端系統 14 間交換。

在設立階段後，個體認證與連線鍵碼導出於第 2 階段在 POD 模組 26 與主機裝置 24 間被實施。POD 模組 26 與主機裝置 24 在一旦被認證後被授權依據在接收器 20 中所使用之內容保護做法獨立地導出該連線鍵碼。在一實施例中，所導出之連線鍵碼可包括一個 1024 位元之熵，其足以用於 16 個連續的連線以在 POD 模組 26 與主機裝置 24 間綴字。在于某些實施例中，接收器 20 中之內容保護通訊協定運用包括該連線鍵碼之對稱密碼法則。

在狀態 6，其為認證與連線鍵碼導出階段之第 1 個狀態，M 值被預置為該共同計數值 Mo。接著，M 被以 1(或某些其他預設值)增量而更新：

$$M \leftarrow M + 1$$

此外，POD 模組 26 使用一修正過之 ElGamal 法則藉由產生一隨機整數 s 並計算 $G^{S}modN$ 與 $M(G^{-H})^{S}modN$ 而為主機裝置 24 亦加密 M。資料流 $\{G^{S}modN || M(G^{-H})^{S}modN\}$ 由 POD 模組 26 被送至主機裝置 24。

接著在狀態 7，主機裝置 24 亦預置一變數 M 為該共同

五、發明說明（16）

計數值 Mo。同時，M 亦為增加 1 而被更新以與 POD 模組 26 中之 M 等時化。主機裝置 24 藉由首先產生一隨機整數 t，然後再計算 $G^t \text{mod} N$ 以及 $M(G^{-P})^t \text{mod} N$ 使用修正後的 ElGamal 法則為 POD 模組 26 加密 M。然後主機裝置 24 送出下列的資料流〔$G^t \text{mod} N || M(G^{-P})^t \text{mod} N$〕至 POD 模組 26。同時在狀態 7，主機裝置 24 亦將 POD 模組 26 所送出之密碼解密以藉由實施下列的模數乘法來導出 M'：

$$M' = \{[M(G^{-H})^S \text{mod} N] \bullet (G^S \text{mod} N)^H\} \text{mod} N$$

若參數 M'等於參數 M，則主機裝置 24 已認證 POD 模組 26，且主機裝置 24 導出共用鍵碼 k，其如下列般地被計算：

$$k = (G^{tS} \text{mod} N) = [(G^S \text{mod} N)^t \text{mod} N]$$

接著在狀態 8，POD 模組 26 由主機裝置 24 接收該密碼並藉由實施下列的運算來計算參數 M'：

$$M' = \{[M(G^{-P})^t \text{mod} N] \bullet (G^t \text{mod} N)^P\} \text{mod} N$$

然後 M'之值與 M 之值被比較，若相等，POD 模組 26 認證主機裝置 24 並如下列般地導出一共用連線鍵碼 k：

$$k = (G^{tS} \text{mod} N) = [(G^t \text{mod} N)^s \text{mod} N]$$

在個體認證與共用鍵碼導出完成後，最後的鍵碼 K 由連線鍵碼 k 在目標緩字鍵碼大小之模數下被計算：

K = k mod(緩字鍵碼大小)

此運算在 k 之資料欄位循環直至耗盡 k 之熵為止。

在建立共用連線鍵碼 K 之際，POD 模組 26 現在可依據內容保護通訊協定來對接收器 20 內鏈路 28 上被傳輸之內容緩字。為保護在主機裝置 24 與 POD 模組 26 被傳輸之內

五、發明說明（ 17）

容的內容保護通訊協定在狀態 9 與 10 間被實施，其被包括於第 4 圖之狀態圖的第 3 階段中。此內容可包括播放視頻與音頻資料。

依據一實施例，在狀態 9 中 POD 模組 26 依據頭端系統 14 與 POD 模組 26 間之條件存取通訊協定將由頭端系統 14 接收之被輸送資料流解密。接著 POD 模組 26 使用所導出之連線鍵碼 K 依據對稱綴字將由頭端系統 14 來之內容加密並在鏈路 28 上將該密碼送至主機裝置 24。接著在狀態 10，主機裝置 24 使用所導出之連線鍵碼 K 依據對稱綴字將密碼解密以獲得乾淨的資料，其可被主機裝置 24 進一步地處理(如用於顯示給觀賞者或其他操作)。

分別在主機裝置 24 與 POD 模組 26 中之隨機數字產生器 220 與 222 適用產生隨機數字 M_H 與 t(在主機裝置 24 中)及 M_P 與 s(在 POD 模組 26 中)。該等隨機數字可為實際隨機或虛擬隨機數字用於藉由提供主機裝置 24 與 POD 模組 26 間之隨機化的盤問而強化保全性。在一實施例中，在每一裝置 24 與 26 中所使用的隨機數字產生器(RNG)運用 ElGamal 加密引擎作為一單向函數，雖然產生隨機數字之其他技術亦為意圖的。隨機數字產生器 220 或 226 的輸入包括一 RNG 種子 S(在 POD 模組 26 為 S_P，在主機裝置 24 為 S_H)，其可為一 160 位元之字串、一私用鍵碼 K，其亦可為 160 位元之長度(在 POD 模組 26 中私用鍵碼為 P 及在主機裝置 24 中為 H)與一 b-位元字串 c，其中 $160<b<1024$。該位元流 c 被選擇之方式可為任何二連續值為不同的。

五、發明說明（ 18）

隨機數字產生器 220 或 222 之輸出為以 G(s，k，c)代表之字串，其在一實施例中為一個 1024 位元之字串。在一實施例中，隨機數字產生器 220 或 222 可如下列地產生隨機數字。起先，一參數被定義，其包括 c 之 160 最小有效位元：

$$u \leftarrow c_{1sb-160}$$

接著，一訊息方塊 X 藉由填充 0 至 c 字串被創立，以獲得一個 1024 位元之訊息方塊 X：

運用 ElGamal 加密引擎作為一單向函

$$X \leftarrow c \| 0^{1024-b}$$

然後一互斥 OR 對 RNG 種子 s 與參數 u 被實施以獲得一隨機數字 v：

$$v \leftarrow s \oplus u$$

ElGamal 加密步驟再以訊息 X、隨機數字 v 與私用鍵碼 K 被執行，以獲得訊息 Y：

$$Y \leftarrow X(G^K)^V \bmod N$$

然後輸出 G(s，K，c)被設定等於加密後之訊息 Y，其為一隨機數字。

輸出 G(s，K，c)為一 1024 位元之整數。在依據某些實施例之認證過程中，在 POD 模組 26 被產生之隨機數字為輸出 $G(s，p，c)_{1sb-160}$ 之 160 最小有效位元，且在主機裝置 24 產生之隨機數字為輸出 $G(s，H，c)_{1sb-160}$ 之 160 最小有效位元。

依據另一個實施例，單向雜湊函數可在頭端系統 14，

五、發明說明（ 19）

主機裝置 24 與 POD 模組 26 間之具結服務中被運用。單向雜湊函數法則之一例為如 SHA-1 之保全雜湊法則(SHA)。

參照第 5 圖，依據一實施例用於保護主機裝置 24 與 POD 模組 26 間之通訊的個人認證與鍵碼導出過程使用 SHA-1 法則。此處過程被分為三個階段：預置化階段(第 1 階段)、個人認證與鍵碼導出階段(第 2 階段)與通訊階段，其中 POD 模組 26 與主機裝置 24 間之資料交換被所導出之連線鍵碼保護。

一個受信任之第三者 112(第 2 圖)為資訊通訊系統中之 POD 模組 26 與主機裝置 24 供應裝置辨識元與所對應的祕密鍵碼(如 160 位元之祕密鍵碼)及 RNG 種子(如 160 位元之 RNG 種子)之佇列。該等祕密鍵碼被儲存於 POD 與主資料庫 104 與 106 中之各種位置，其可分別用 POD 裝置辨識元(P_ID)與主裝置辨識元(H_ID)定位位址。

在此實施例中，POD 模組 26 用之認證欄位以{P_ID‖P‖S_P}表示，其分別包括 POD 模組裝置辨識元、祕密鍵與 RNG 種子之連結。通訊協定與主機裝置 24 之祕密鍵碼 P 與 H 分別被儲存於抗擅改之儲存元件 210 與 208 內。

在預置化之際，在 POD 模組 26 已被插入或與主機裝置 24 操作式地耦合後，或主機裝置 24 已被電力循環後，POD 模組 26 與主機裝置 24 交換新近分別由 POD 模組 26 與主機裝置 24 被產生之隨機整數 N_P 與 N_H。然後每一裝置獨立地設定一共同的預置計數值 N_0，$N_0 = N_P \oplus H$。

接著，在狀態 1 之預置化後，主機裝置 24 設定 N 等

五、發明說明（ 20 ）

於 N_0，然後以 1(或某些預設值)使 N 增量。然後主機裝置 24 計算 SHA-1(N⊕H)，其為 N⊕H 之保全雜湊函數，並送出下列之資料流{H_ID‖ SHA-1(N⊕H)}至 POD 模組 26。在狀態 2，POD 模組 26 亦將 N 預置為 N_0並以 1(或某些其他值)使 N 增量。然後通訊協定計算單向雜湊函數 SHA-1(N⊕P)。接著 POD 模組 26 送出下列資料流{P_ID‖ H_ID‖ N ‖ SHA-1(N⊕H)‖ SHA-1(N⊕P)}至主機裝置 24。此指示頭端系統 14 一具結服務已被要求。在狀態 3，頭端控制器 130 根據接收之 P_ID與 H_ID值分別存取資料庫 104與 106 中之儲存位置 108與 110，以分別擷取 POD 模組 26與主機裝置 24之祕密鍵碼 P與 H。在擷取 P與 H後，由於 P，H 與 N 在頭端系統 14 中為已知的，頭端控制器 130 計算 SHA-1(N⊕P)與 SHA-1(N⊕H)。計算後之 SHA-1 值與所接收之 SHA-1 值被比較。若其值相符，則 POD 模組 26與主機裝置 24被頭端系統 14辨識為受信任之玩手。

在狀態 3 中，頭端控制器 130 便計算下列的值，其在一具結流中被送回 POD模組 26：SHA-1[SHA-1(N⊕H)⊕P]、SHA-1[SHA-1(N⊕P)⊕H]、SHA-1(H‖N)⊕SHA-1(P)及 SHA-1(P‖N)⊕SHA-1(H)。其中前二項被用於個體認證及後二者被用於共用鍵碼導出。在狀態 4，POD 模組 26 藉由計算下列雜湊函數 SHA-1[SHA-1(N⊕H)⊕P]來認證主機裝置 24，SHA-1(N⊕H)由其自主機裝置 24 被接收及 P為 POD 模組 26之祕密鍵碼。該被導出之值與被頭端系統 14傳輸之雜湊函數比較。若其符合，則 POD 模組 26已認證主機

五、發明說明（ 21 ）

裝置 24。一旦被認證，POD 模組 26 導出鍵碼 k：

$$k = SHA\text{-}1(H \| N) \oplus SHA\text{-}1(P \| N)$$

在上述的運算中，SHA-1(P‖N)項係藉由由頭端系統 14 取得 SHA-1(H‖N)⊕SHA-1(P)之結果及對 SHA-1(P)項及該結果實施互斥 OR 運算而被導出。

再來，POD 模組 26 送出包括有下列項之資料流至頭端系統 14：SHA-1(N⊕P)、SHA-1[SHA-1(N⊕P)⊕H]與 SHA-1(P‖N)⊕SHA-1(H)。

在狀態 5，在由 POD 模組 26 接收該具結流之際，頭端系統 14 計算下項：SHA-1[SHA-1(N⊕P)⊕H]，SHA-1(N⊕P)由其自 POD 模組 26 被接收。

此結果與被 POD 模組 26 送出之同一個雜湊函數(起源於頭端系統 14)被比較。若其相符，則頭端系統 14 已認證 POD 模組 26，且頭端系統 14 導出共用鍵碼 k：

$$k = SHA\text{-}1(H \| N) \oplus SHA\text{-}1(P \| N)$$

在上面的運算中，SHA-1(P‖N)項係藉由對下列由 POD 模組 26 被接收之值 SHA-1(P‖N)⊕SHA-1(H)與雜湊函數 SHA-1(H)實施互斥 OR 運算而被導出。互斥 OR 運算之結果為 SHA-1(P‖N)值。

一旦個體認證與共用鍵碼導出已被 POD 模組 26 與主機裝置 24 實施，最後的共用連線鍵碼 K 藉由取得鍵碼 k 在目標綴字鍵碼大小之模數下被每一裝置計算：

$$K = k \bmod (\text{綴字鍵碼大小})$$

在使用該共用連線鍵碼 K 下，POD 模組 26 可將在鏈路 28

五、發明說明（ 22 ）

上被傳輸至頭端系統 14 之內容綴字。

因此在第 5 圖之狀態 6，POD 模組 26 將使用條件存取通訊協定已被解密之頭端系統被接收之資料流解密。然後 POD 模組 26 使用連線鍵碼 K 依據對稱綴字將乾淨的內容加密，並在鏈路 28 上將該綴字內容送至頭端系統 14。在狀態 7，頭端系統 14 接收該綴字內容並將之解密以獲得該內容之乾淨複製以被頭端系統 14 進一步處理。

依據此實施例之隨機數字產生器(RNG)220 或 222 在裝置 24 或 26 中)可運用 SHA-1 作為單向雜湊函數。在此實施例中，隨機數字產生可依據 1994 年 5 月 19 日之美國聯邦資訊處理標準(FIPS)公告 186 號且可在{http：//www.itl.nist.gov}可取得之隨機數字產生規格被實施。RNG 220 或 222 之輸入可為 160 位元之 RNG 種子 S(在 POD 模組 26 為 Sp 及在頭端系統 14 為 S_H)及一個 b 位元之字串 c，其中 $160 < b < 512$。RNG 220 或 222 之輸出為一個 160 位元之字串，以 G(s，c)表示之。

依據另一個實施例，POD 模組 26 與主機裝置 24 間之個體認證使用數位簽名法則被實施，且一連線鍵碼依據 Diffie-Hellman 鍵碼交換作法被導出。

參照第 6 圖，依據另一實施例之認證與鍵碼交換法則的狀態圖被顯示。此實施例所用之主機裝置 24 中的認證欄位可包括{H_ID，S_H-1(H_ID)，H，H^{-1}}，此處 H_ID 為主機裝置 24 之私用鍵碼 H^{-1} 所創立之 H_ID 的數位簽名，及 H 為頭端系統 14 之公用鍵碼。POD 模組 26 在其認證欄位中

五、發明說明（23）

包括下列的資訊：P_ID、S_P-1(P_ID)，P^{-1}及P。

可使用之簽名法則包括如國家技術標準研究所(NIST)在其1993年1月之數位簽名標準公告之數位簽名標準。該數位簽名標準(DSS)亦被習知為聯邦資訊處理標準(FIPS)186號。DSS之一變形為DSS之橢圓版本。另外可使用之數位簽名法則為如RSA Data Security公司在其網址{http://www.rsa.com./rsalabs/}所描述之1998年的Rivest-Shamir-Adleman(RSA)法則。

為開始認證處理，主機裝置24在狀態1送出其認證欄位{H_ID‖S_H^{-1}(H_ID)}之部分至POD模組26。接著在狀態2，POD模組26送出其認證欄位{P_ID‖S_P^{-1}(P_ID)}之部分以及POD模組26之認證資訊至頭端系統14。在狀態3，頭端系統14比較所接收之認證欄位與儲存在資料庫104與106中之資料。P_ID被用以由位置108擷取資訊，其儲存POD模組26之公用鍵碼P以及其數位簽名S_P^{-1}(P_ID)。類似地，H_ID由資料庫106中之位置110擷取資訊，其包括主機裝置24之公用鍵碼H以及其數位簽名S_H^{-1}(H_ID)。因此在狀態3中，頭端系統14驗證所接收之認證欄位資訊係根據由位置108與110被擷取之資訊之比較而由獲授權之裝置而來。

在狀態4，一旦頭端系統14驗證裝置26與24為有效的裝置，頭端系統14以主機裝置24之公用鍵碼H使用對稱綴字作法將POD模組26之公用鍵碼加密以導出E_H[P]。可能的對稱綴字作法可為方塊綴字作法、資料流綴字作法

五、發明說明（ 24 ）

及其他者。

然後頭端系統 14 將 $E_H[P]$送回 POD 模組 26。在接收到 $E_H[P]$之際，POD 模組 26 已隱然認證主機裝置 24。為了讓主機裝置 24 認證 POD 模組 26，POD 模組 26 在狀態 5 送出下列的資料流{$E_H[P] \| P\_ID \| S_P^{-1}(P\_ID)$}至主機裝置 24。此允許主機裝置 24 藉由使用 POD 模組之公用鍵碼 P 來實施 $V_P[P_ID \| S_P^{-1}(P_ID)]$運算而認證 POD 模組 26。P 係被主機 24 藉由以主機之鍵碼 H 將 $E_H[P]$解密而被導出。$V_P[\ ]$運算係由主機裝置 24 中之驗證引擎依據數位簽名法則被實施。

在狀態 1-5 之個體認證完成後，連線鍵碼之創立被啟動。在狀態 7，每一 POD 模組 26 與主機裝置 24 產生其各別的隨機整數 x 與 y 並分別計算 $G^x \bmod N$ 與 $G^y \bmod N$，此處 N 為一共同模數及 G 為一共同產生器。主機裝置 24 送出 $G^y \bmod N$ 至 POD 模組 26，且類似地，POD 模組 26 送出 $G^x \bmod N$ 至主機裝置 24。在狀態 8，POD 模組 26 計算共用連線鍵碼 k：$k = (G^y \bmod N)^x \bmod N = G^{yx} \bmod N$。該共用連線鍵碼 k 被 POD 模組 26 與主機裝置 24 使用以保護鏈路 28 上之通訊。在 POD 模組 26 依據酬載緩字法則(即一種條件存取法則)將由頭端系統接收之資料解密後，POD 模組 26 便使用該連線鍵碼 k 將該內容加密並送出該緩字內容至主機裝置 24，其使用連線鍵碼 k 之其複製將該緩字內容解密。

參照第 7 圖，為進一步加強保全性，除了與第 6 圖有

五、發明說明（25）

關之運算外數個額外者可被實施。特別是，安全性水準升級階段可藉由修改第6圖之狀態4與7而被達成。

在第7圖中，該升級階段後之保全作法包括除了狀態4與7外與第6圖者相同的運算。在第7圖之狀態4*中，在由POD模組26與主機裝置24接收認證欄位資訊後，頭端系統14產生二個加密後之公用鍵碼：$E_H[P]$與$E_P[H]$。然後此二加密後之公用鍵碼被傳輸回到POD模組26，其由$E_P[H]$擷取主機裝置之公用鍵碼H。當資料流{$E_H[P] \| P\_ID \| S_P^{-1}(P\_ID)$}被POD模組26傳輸至主機裝置24時，主機裝置24可由$E_H[P]$擷取POD模組26之公用鍵碼P。由裝置24與26之公用與私用鍵碼二者受到良好的保護，中間人之攻擊將不可能在於保全頻道上彼此傳送該等公用鍵碼時破解該系統。

狀態7藉由將第6圖者分解為狀態7a，7b與7c而被修改。在此實施例中，POD模組26與主機裝置24二者產生一隨機化後之盤問Xn與Yn以及隨機整數x與y，其被用於導出裝置26與24間之共用連線鍵碼。此外，在狀態7a中，POD模組26與主機裝置24分別計算$G^x \bmod N$與$G^y \bmod N$。隨機數字Xn與Yn在POD模組26與主機裝置24被交換。在狀態7b中，POD模組26藉由使用POD模組之私用鍵碼P即$S_P^{-1}(Yn \| G^x \bmod N)$來計算一第一相位之Diffie-Hellman變數而對由主機裝置24接收之盤問Yn產生其數位簽名。類似地，在狀態7b，主機裝置24產生$S_H^{-1}(Xn \| G^y \bmod N)$。該等各別的數位簽名與$G^x \bmod N$及$G^y \bmod N$在

五、發明說明（26）

POD模組26及主機裝置24間被交換。在狀態7c中之接收之際，每一POD模組26與主機裝置24驗證該簽名並擷取該第一相位之Diffie-Hellman變數。成功的驗證來自於POD模組26與主機裝置24的彼此認證之結果。接著在狀態8，共用連線鍵碼k如第6圖之實施例般地被導出。

本發明之某些實施例具有一個以上的下列益處。脆弱性被局部化使得一裝置之退讓不會導致整個系統面之退讓。為達到此點，依據某些實施例，局部的密碼變數被使用及被選擇以不致在退讓事件中威脅整體系統。此外，依據某些實施例之系統可抵抗消費者階層之攻擊，此包括安裝破解裝置或介面產品。主機裝置24外之電纜或裝置的連接不會造成在主機裝置24中實施之複製保護作法之退讓的結果。

依據某些實施例之系統的其他特點為條件存取系統(在此情形中包括主機裝置24與POD模組26)可限制POD模組可與那一個主機裝置通訊。該條件存取系統能辨識可疑的主機裝置並使之失能，此在某些實施例中是僅要POD模組26與主機裝置24已根據被受信任之第三者所提供的一個以上儲存資料庫中的值之比較被頭端系統14驗證，藉由頭端系統14傳輸該具結訊息而被完成。

該個體認證與連線鍵碼導出過程可獨立於如條件存取法則之酬載綴字法則而被實施。該認證與連線鍵碼導出過程在主機裝置24與POD模組26中可執行的軟體在減少涉及硬體下實施係相當簡單的。在其他的實施例中，該認

五、發明說明（ 27）

證鍵碼導出過程可在硬體中實施。在依據某些實施例之SA-CP系統中，頭端系統14在系統破壞的情形中能撤回對主機裝置之存取的授權。該複製保護作法保護POD模組與主機裝置間及POD模組與頭端系統間的曝現之匯流排。

各種軟體與韌體(例如由模組、常規或層所構成)包括應用程式與常規可被儲存抑或確實地被實施於資訊傳輸系統中一個以上的機器可讀的儲存媒體內。適於確實地實施軟體與韌體指令之儲存媒體可包括不同型式之記憶體，包括半導體記憶體裝置，如動態或靜態隨機存取記憶體、可擦拭且可程式唯讀記憶體(EPROM)、電氣可擦拭且可程式唯讀記憶體(EEPROM)、閃記憶體、磁片，如固定、軟式與可拆卸式碟片、其他的磁性媒體，包括磁帶、以及光學媒體如CD或DVD。儲存於一個以上之儲存媒體的指令在被執行時造成該資訊傳輸系統實施被規劃之動作。

該軟體或韌體可用許多不同的方法之一被載入該資訊傳輸系統中。例如，被儲存於一個以上之儲存媒體或經由網路介面卡、數據機或其他介面機構被輸送之指令或其他碼區段可被載入該資訊傳輸系統並被執行以實施所規劃之動作。在載入或輸送過程中，被實施為負載波(在電話線路、網路線路、電纜之類上被傳輸)之資料信號可將該等指令或碼區段通訊至該資訊傳輸系統。

雖然本發明已針對有限數目之實施例被揭示，但熟習該技藝者將了解其很多修改與變化。其意圖所附之申請專利範圍涵蓋所有此類修改與變化而落入本發明之真實精

五、發明說明（ 28 ）

神與領域中。

元 件 標 號 對 照 表

元件編號	譯名	元件編號	譯名
10	服務提供者	130	控制器
12	接收處	200	鏈路介面
14	頭端系統	202	鏈路介面
15	輸送媒體	204	控制裝置
16	纜線鏈路	205	控制常規
18	衛星鏈路	206	控制裝置
20	接收器 20	207	控制常規
22	顯示單元	208	儲存元件
24	主機裝置 24	210	儲存元件
26	展開點模組，POD 模組	212	算術處理單元
28	鏈路	214	算術處理單元
100	POD 認證欄位	216	互斥 OR 單元
102	主認證欄位	218	互斥 OR 單元
104	資料庫	220	隨機數字產生器
106	資料庫	222	隨機數字產生器
108	位置	224	計數器
110	位置	226	計數器
112	第三者		
114	保全頻道		
116	上游路徑		
118	下游路徑		

A5
B5

四、中文發明摘要（發明之名稱：在一系統中保護資訊之技術）

一種在一第一裝置(24)與一第二裝置(26)間安全地通訊內容之方法與裝置包括傳送該等第一與第二裝置之辨識資訊至一第三裝置(14)。該第三裝置(14)根據該辨識資訊產生一預設的訊息。該等第一與第二裝置(24，26)使用該預設的訊息被認證。

英文發明摘要（發明之名稱：PROTECTING INFORMATION IN A SYSTEM）

A method and apparatus of securely communicating content between a first device (24) and a second device (26) includes sending identification information of the first and second devices to a third device (14). The third device (14) generates a predetermined message based on the identification information. The first and second devices (24, 26) are authenticated using the predetermined message.

A8
B8
C8
D8

六、申請專利範圍

1. 一種認證第一與第二裝置之方法，包含：

在一第三裝置接收該等第一與第二裝置之辨識元；

根據該等辨識元擷取該第三裝置中之資訊；

根據所擷取之資訊由該第三裝置傳輸一訊息；以及

根據該訊息在該等第一與第二裝置中驗證該等第一與第二裝置的其他之一的身份。

2. 如申請專利範圍第1項所述之方法，其中該傳輸包括傳輸一訊息，其包括該等第一與第二裝置之公用鍵碼。

3. 如申請專利範圍第2項所述之方法，其中該傳輸包括傳輸一訊息，其包括該等第一與第二裝置之公用鍵碼的倒數。

4. 如申請專利範圍第1項所述之方法，其中該驗證包括使用一公用鍵碼密碼通訊協定來實施認證。

5. 如申請專利範圍第4項所述之方法，其中該驗證包括使用一公用鍵碼密碼通訊協定之離散對數版本來實施認證。

6. 如申請專利範圍第5項所述之方法，其中該驗證包括使用ElGamal密碼通訊協定來實施認證。

7. 如申請專利範圍第1項所述之方法，進一步包含在該等第一與第二裝置中產生一隨機數字，其中該驗證包括使用在每一該等第一與第二裝置中之該隨機數字。

8. 一種在一第一裝置與第二裝置間安全地通訊內容之方法，包含：

傳送該等第一與第二裝置之辨識資訊至一第三裝置；

根據該辨識資訊在該第三裝置中產生一預設的訊息

六、申請專利範圍

；以及

使用該預設的訊息認證該等第一與第二裝置。

9.一種用於與一第一系統通訊之裝置，包含：

一接收器包括一第一模組與一第二模組被耦合於該第一模組，該等第一與第二模組適用於在回應於該辨識資訊下，根據被該第一系統所創立及傳送之預設的資訊來傳輸辨識資訊至該第一系統及彼此認證。

10.如申請專利範圍第9項所述之裝置，其中該等第一與第二模組適用於使用一公用鍵碼通訊協定來彼此認證。

11.如申請專利範圍第9項所述之裝置，其中該公用鍵碼通訊協定包括一ElGamal通訊協定。

12.如申請專利範圍第9項所述之裝置，其中該接收器適用於由被一第一保全通訊協定保護之該第一系統接收內容。

13.如申請專利範圍第12項所述之裝置，其中該等第一與第二模組適用於依據包括有一公用鍵碼通訊協定之離散對數版本的一第二保全通訊協定來實施認證。

14.一種通訊系統，包含：

一條件存取系統適用於依據一第一保全通訊協定來通訊內容；

一輸送媒體，該內容在其上被通訊；以及

一接收器被耦合於該輸送媒體並包括一第一單元與一第二單元被一通訊頻道耦合，該等第一與一第二單元適用於提供一第二保全通訊協定以保護在該等第一與第二

六、申請專利範圍

單元間被傳輸之資訊，且

該條件存取系統適用於產生一預設的訊息及該等第一與第二單元適用於根據該預設的訊息來彼此認證。

15. 如申請專利範圍第 14 項所述之系統，其中該接收器包括一內容保護系統。

16. 如申請專利範圍第 15 項所述之系統，其中該條件存取系統包括傳輸頭端與該接收器之第一單元。

17. 如申請專利範圍第 14 項所述之系統，其中該等第一與第二單元適用於根據該預設的訊息產生一連線鍵碼以保護在該通訊頻道上被傳輸之資訊。

18. 如申請專利範圍第 14 項所述之系統，其中該條件存取系統包括一傳輸頭端適用於將視頻內容加密以在該輸送媒體上傳輸。

19. 如申請專利範圍第 14 項所述之系統，其中該等第一與第二單元適用於依據一公用鍵碼密碼通訊協定之離散對數版本來彼此認證。

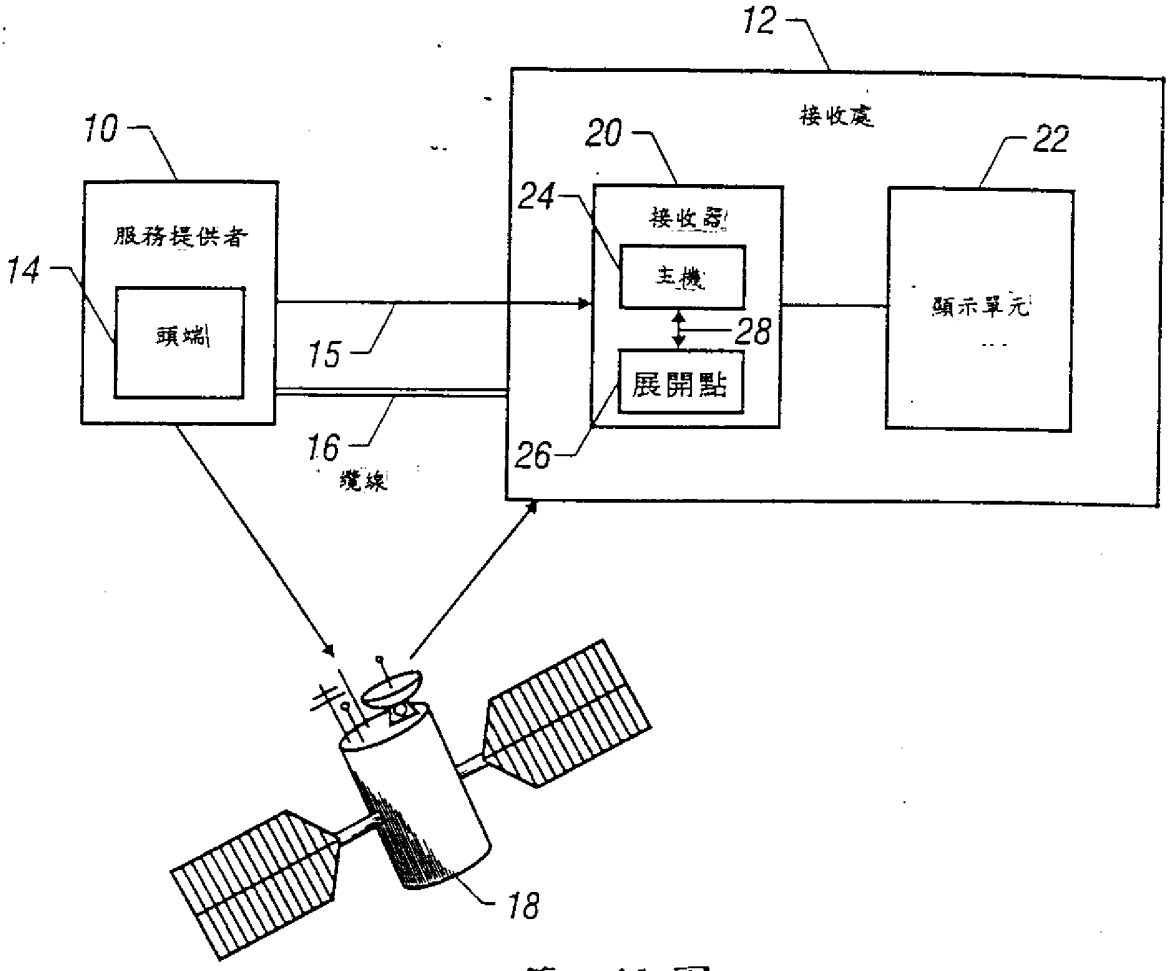
20. 一種包括一個以上機器可讀之儲存媒體的物品，包含指令以保護在一系統中於第一與第二裝置間之通訊，該等指令在被執行時會造成系統來進行：

傳輸該等第一與第二裝置之辨識元至一外部系統；

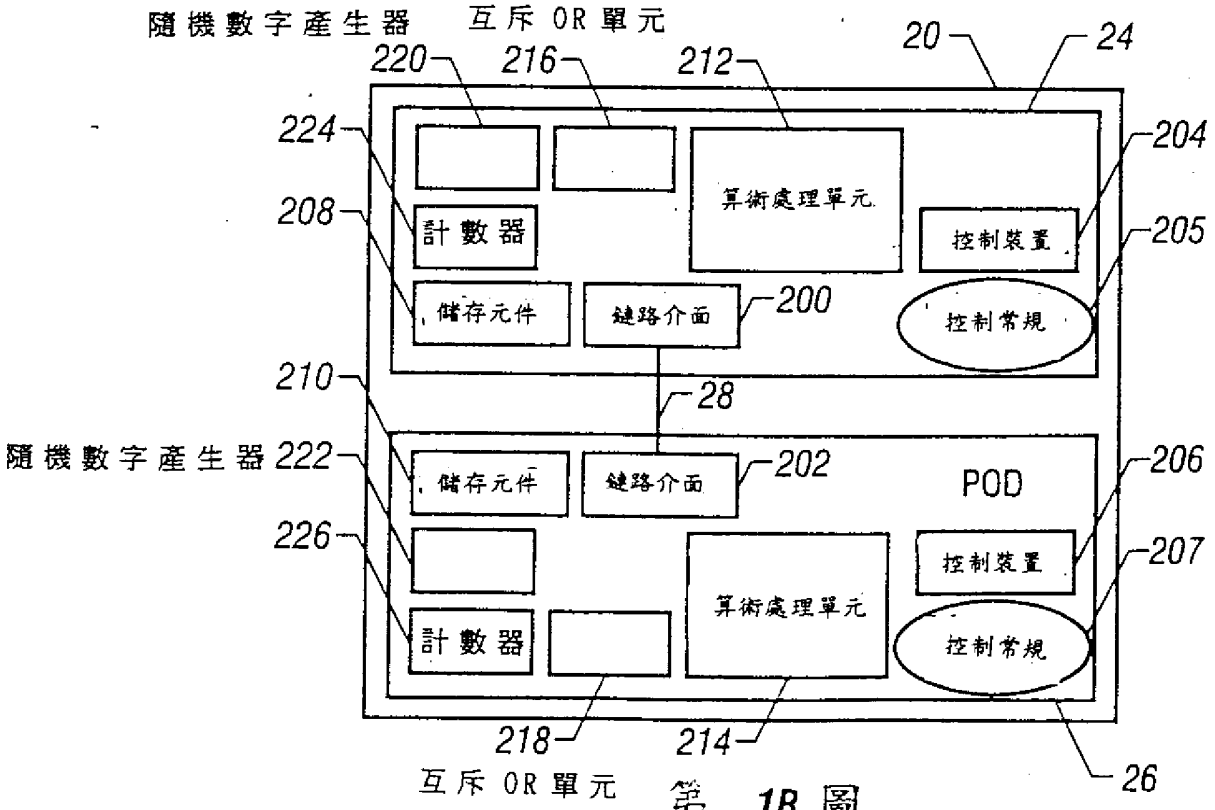
由以該等辨識元為基礎之該外部系統接收一預設的訊息；以及

根據該預設的訊息認證該等第一與第二裝置。

修正補充 90年5月7日

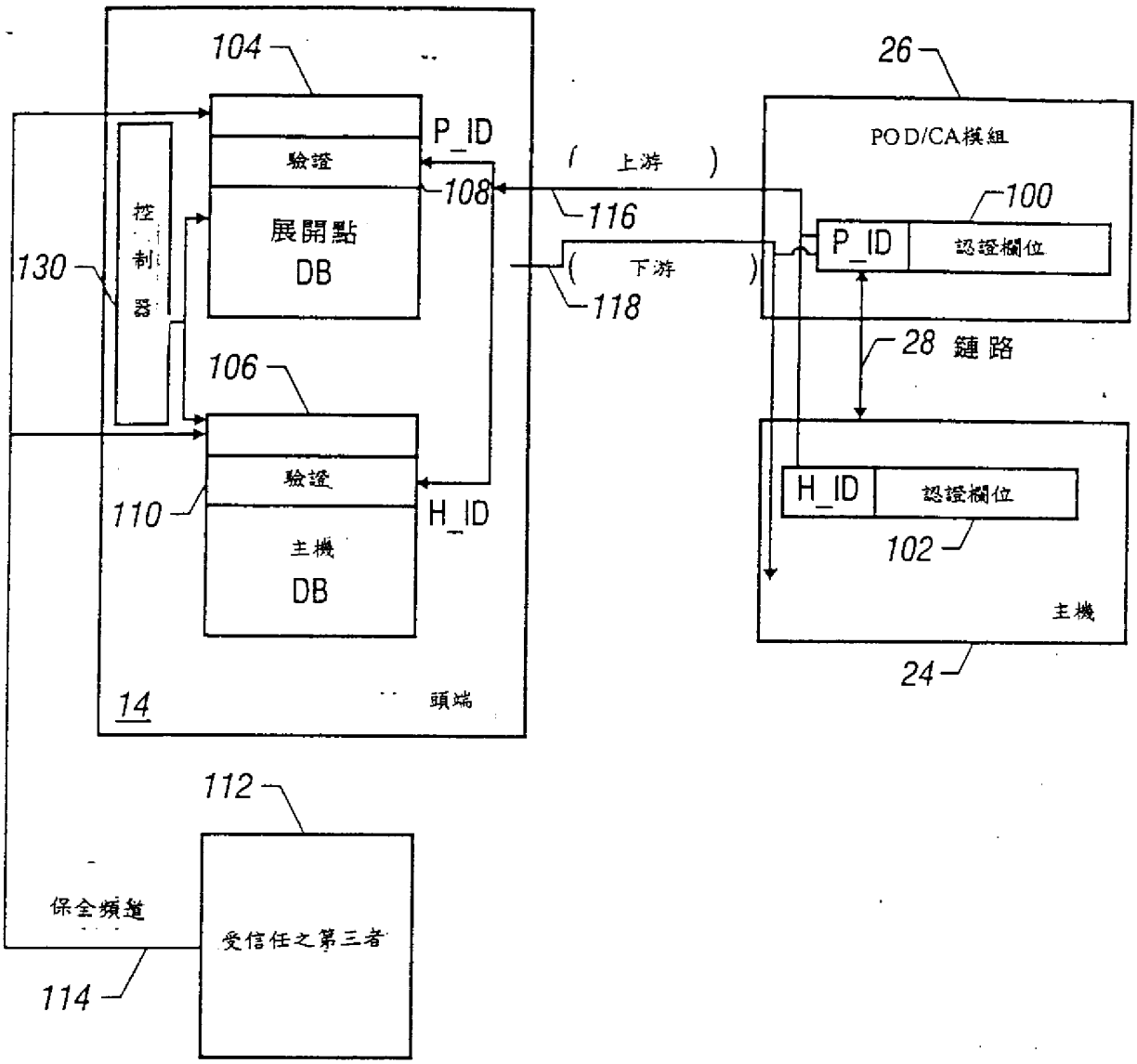


第 1A 圖

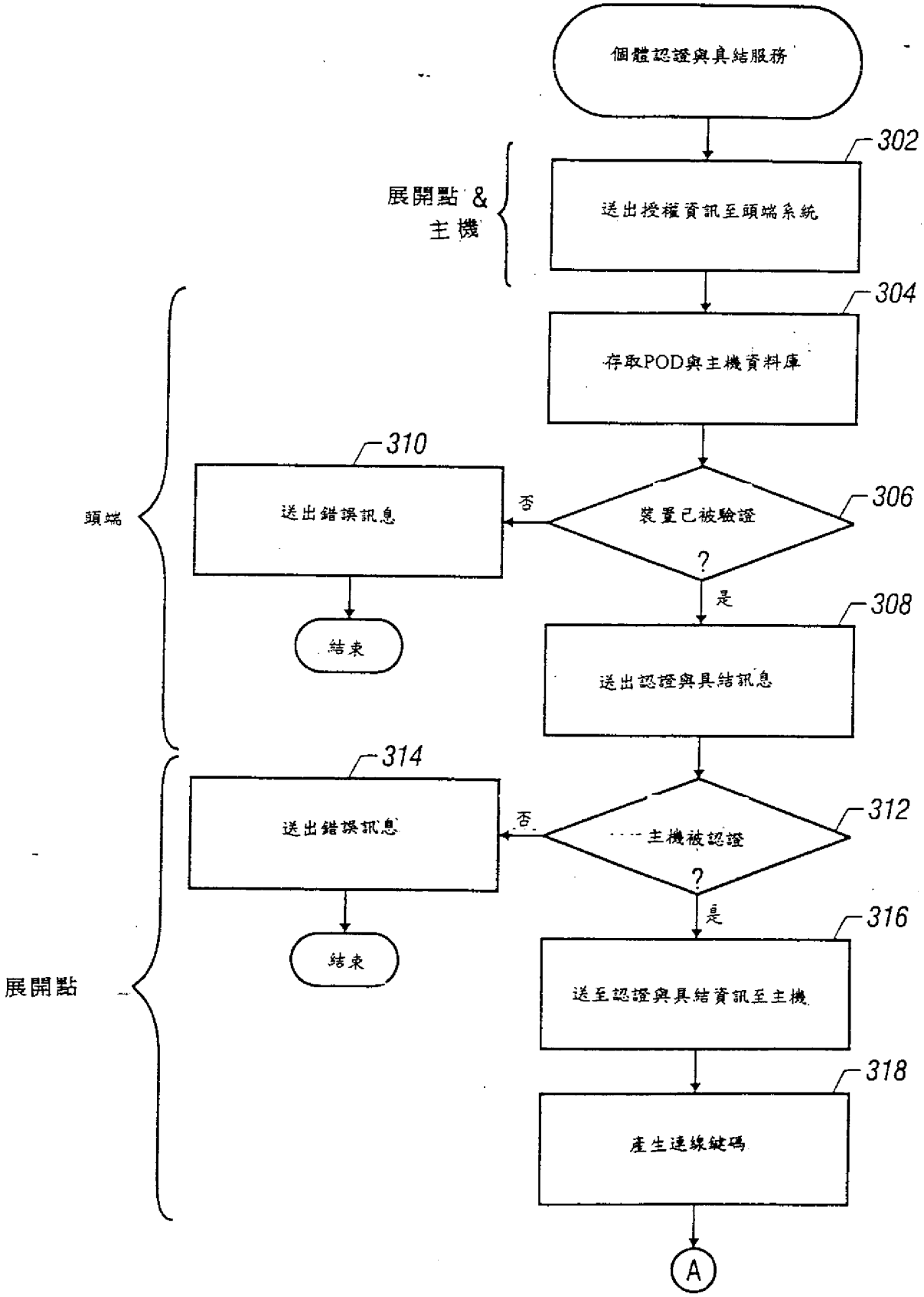


第 1B 圖

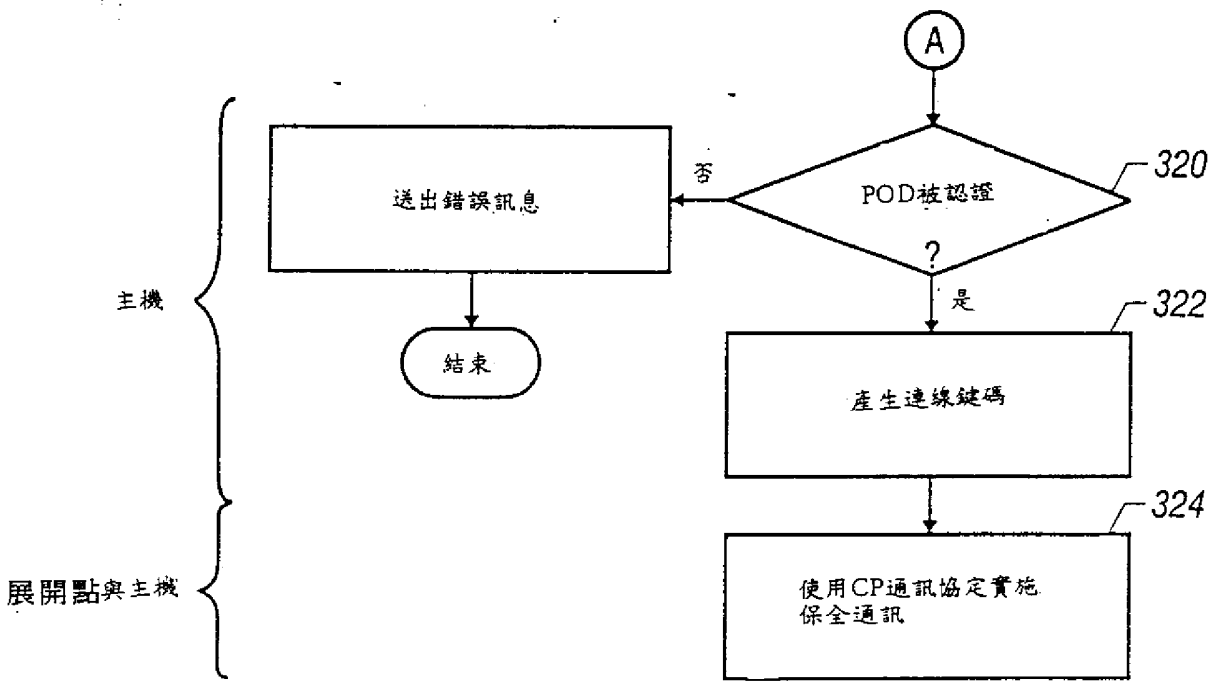
煩請委員明示 90 年 7 月 7 日所提之修正本有無變更實質內容是否准予修正。


104
P_ID
驗證
108
展開點
DB
130
控制器
106
驗證
110
H_ID
主機
DB
14
頭端
112
保全頻道
受信任之第三者
114
26
POD/CA模組
(上游)
116
100
P_ID
認證欄位
(下游)
118
28 鏈路
H_ID
認證欄位
102
主機
24

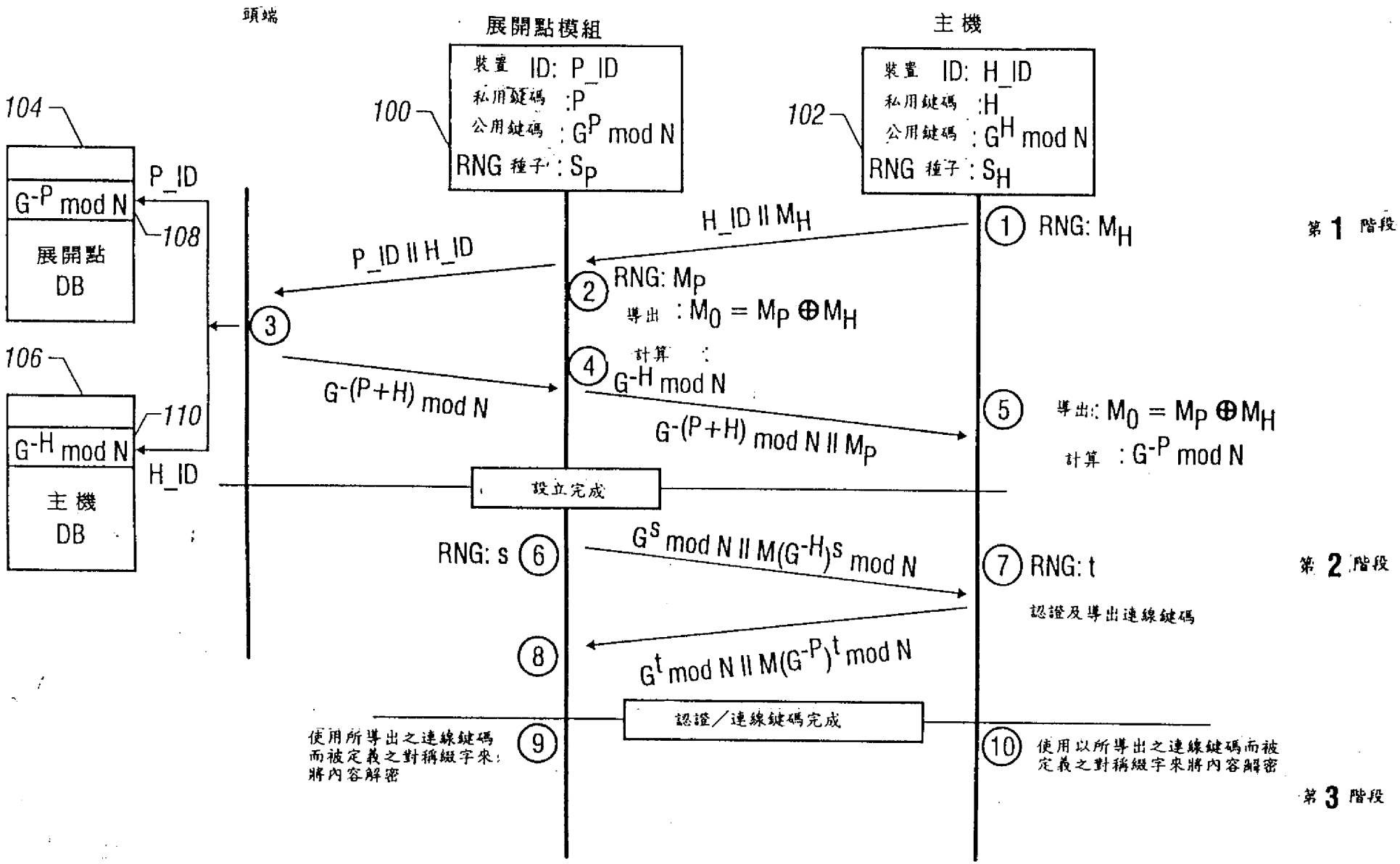
第 2 圖


個體認證與具結服務
302
送出授權資訊至頭端系統
展開點 &
主機
304
存取POD與主機資料庫
310
送出錯誤訊息
否
裝置已被驗證
?
306
是
308
送出認證與具結訊息
結束
頭端
314
送出錯誤訊息
否
主機被認證
?
312
是
316
送至認證與具結資訊至主機
結束
展開點
318
產生連線鍵碼
A

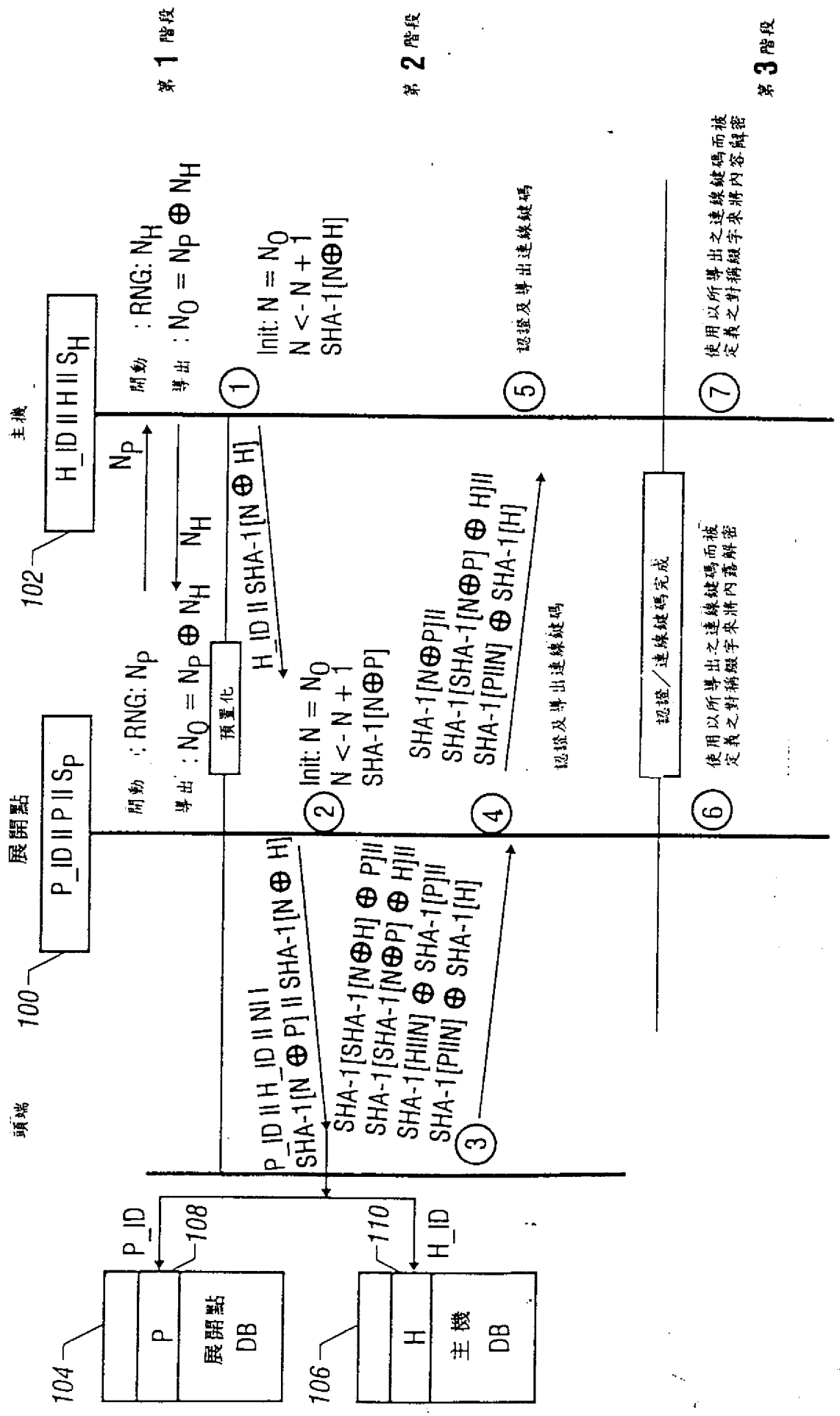
第 3A 圖


A
送出錯誤訊息
否
POD被認證
?
320
是
322
結束
產生連線鍵碼
324
使用CP通訊協定實施
保全通訊
主機
展開點與主機

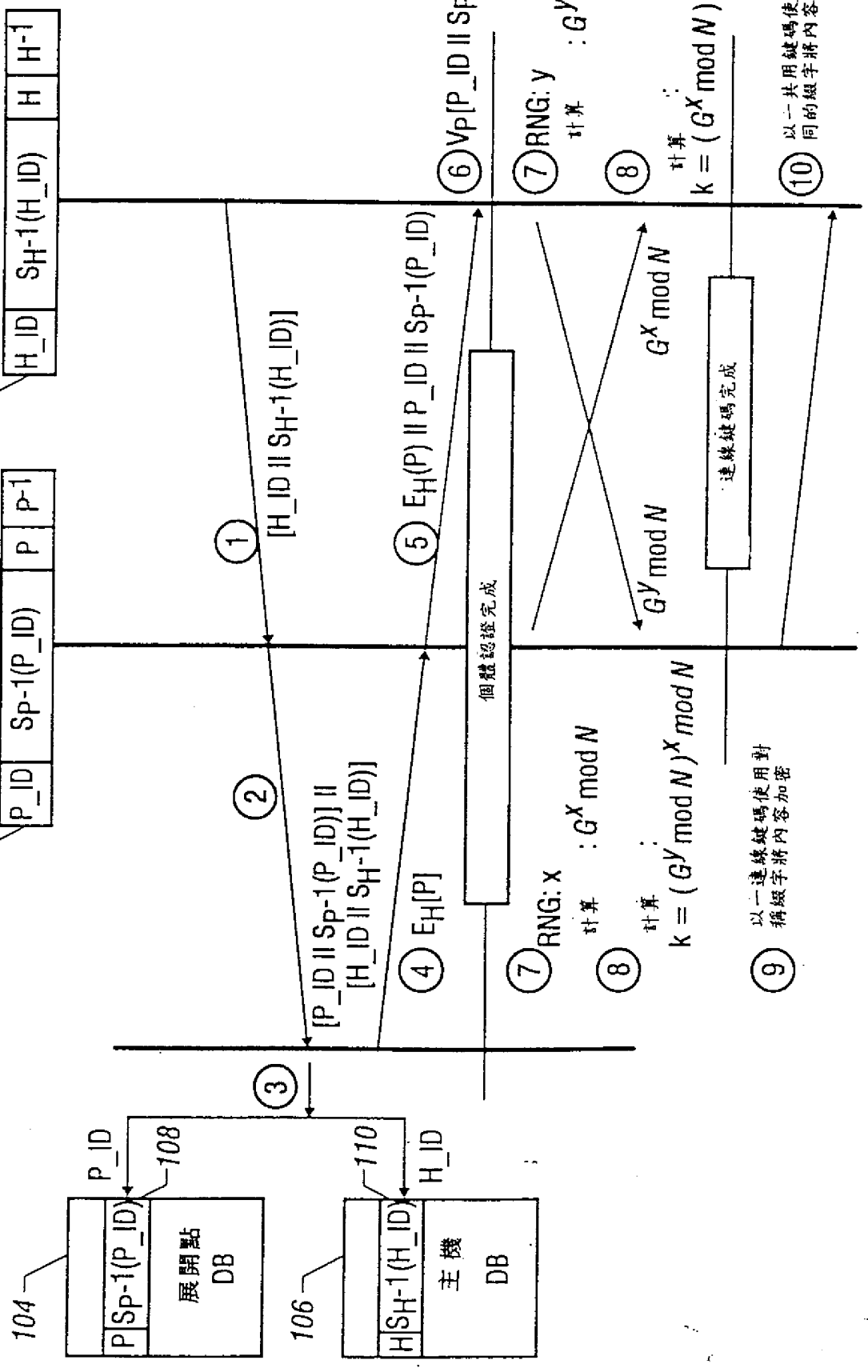
第 3B 圖


頭端
展開點模組
主機
裝置 ID: P_ID
私用鍵碼 :P
公用鍵碼 : $G^P \bmod N$
RNG 種子 : S_P
100
裝置 ID: H_ID
私用鍵碼 :H
公用鍵碼 : $G^H \bmod N$
RNG 種子 : S_H
102
104
$G^{-P} \bmod N$
展開點 DB
P_ID
108
106
$G^{-H} \bmod N$
主機 DB
H_ID
110
$H\_ID \| M_H$
① RNG: M_H
第 1 階段
$P\_ID \| H\_ID$
② RNG: M_P
導出 : $M_0 = M_P \oplus M_H$
③
④ 計算 : $G^{-H} \bmod N$
$G^{-(P+H)} \bmod N$
$G^{-(P+H)} \bmod N \| M_P$
⑤ 導出: $M_0 = M_P \oplus M_H$
計算 : $G^{-P} \bmod N$
設立完成
RNG: s ⑥
$G^s \bmod N \| M(G^{-H})^s \bmod N$
⑦ RNG: t
第 2 階段
認證及導出連線鍵碼
⑧
$G^t \bmod N \| M(G^{-P})^t \bmod N$
認證／連線鍵碼完成
使用所導出之連線鍵碼而被定義之對稱級字來將內容解密
⑨
⑩ 使用以所導出之連線鍵碼而被定義之對稱級字來將內容解密
第 3 階段

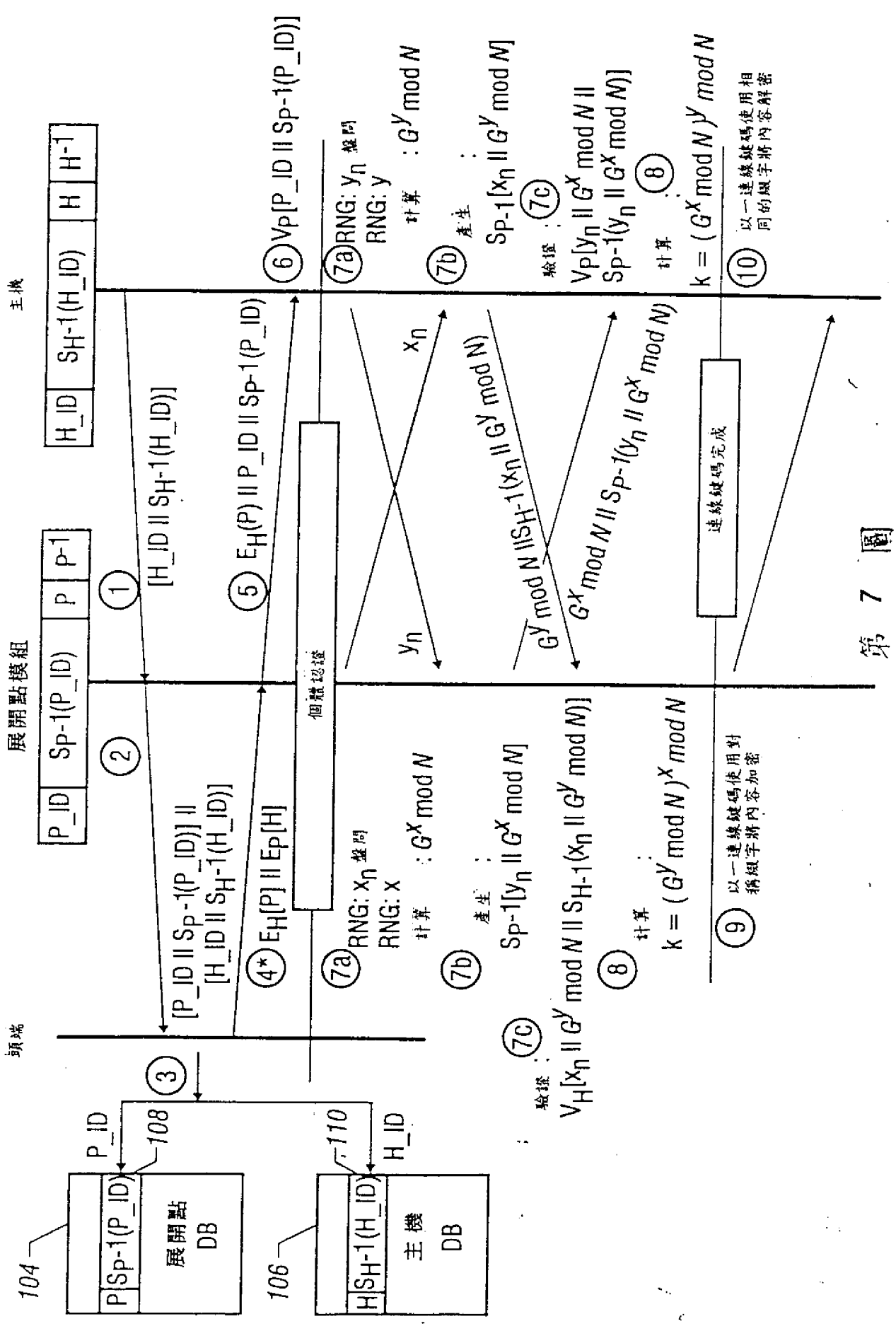
第 4 圖


第 1 階段
第 2 階段
第 3 階段
頭端
展開點
主機
100
102
104
106
108
110
P_ID II P II Sp
H_ID II H II SH
開動 : RNG: Np
導出 : No = Np ⊕ NH
開動 : RNG: NH
導出 : No = Np ⊕ NH
Np
NH
預置化
H_ID II SHA-1[N ⊕ H]
Init: N = No
N <- N + 1
SHA-1[N⊕P]
SHA-1[N⊕P]II
SHA-1[SHA-1[N⊕P] ⊕ H]II
SHA-1[P|IN] ⊕ SHA-1[H]
認證及導出連線鍵碼
認證／連線鍵碼完成
使用以所導出之連線鍵碼而被定義之對稱鍵字來將內容解密
使用以所導出之連線鍵碼而被定義之對稱鍵字來將內容解密
P_ID II H_ID II NI I SHA-1[N ⊕ P] II SHA-1[N ⊕ H]
SHA-1[SHA-1[N⊕H] ⊕ P]II
SHA-1[SHA-1[N⊕P] ⊕ H]II
SHA-1[H|IN] ⊕ SHA-1[P]II
SHA-1[P|IN] ⊕ SHA-1[H]
P_ID
H_ID
P
展開點 DB
H
主機 DB
Init: N = No
N <- N + 1
SHA-1[N⊕H]
① ② ③ ④ ⑤ ⑥ ⑦

第 5 圖


頭端
展開點模組
主機裝置
100
102
P_ID
Sp-1(P_ID)
P
P-1
H_ID
SH-1(H_ID)
H
H-1
① [H_ID II SH-1(H_ID)]
② [P_ID II Sp-1(P_ID)] II [H_ID II SH-1(H_ID)]
③
④ EH[P]
⑤ EH(P) II P_ID II Sp-1(P_ID)
⑥ VP[P_ID II Sp-1(P_ID)]
⑦ RNG: x
計算 : G^X mod N
⑧ 計算 k = (G^Y mod N)^X mod N
⑦ RNG: y
計算 : G^Y mod N
⑧ 計算 k = (G^X mod N)^Y mod N
個體認證完成
G^Y mod N
G^X mod N
連線鍵碼完成
⑨ 以一連線鍵碼使用對稱級字將內容加密
⑩ 以一共用鍵碼使用相同的級字將內容解密
104
106
108
110
P_ID
H_ID
P|Sp-1(P_ID)
H|SH-1(H_ID)
展開點 DB
主機 DB

第 6 圖


頭端
主機
展開點模組
P_ID
Sp-1(P_ID)
P
P-1
H_ID
SH-1(H_ID)
H
H-1
① [H_ID || SH-1(H_ID)]
② [P_ID || Sp-1(P_ID)] || [H_ID || SH-1(H_ID)]
③
④* EH[P] || EP[H]
⑤ EH(P) || P_ID || Sp-1(P_ID)
⑥ VP[P_ID || Sp-1(P_ID)]
個體認證
⑦a RNG: xn 整問 RNG: x
計算 : G^x mod N
⑦b 產生 : Sp-1[yn || G^x mod N]
⑦c 驗證 : VH[xn || G^y mod N || SH-1(xn || G^y mod N)]
⑧ 計算 : k = (G^y mod N)^x mod N
⑨ 以一連線鍵碼使用對稱型字將內容加密
xn
yn
G^y mod N || SH-1(xn || G^y mod N)
G^x mod N || Sp-1(yn || G^x mod N)
連線鍵碼完成
⑦a RNG: yn 整問 RNG: y
計算 : G^y mod N
⑦b 產生 : Sp-1[xn || G^y mod N]
⑦c 驗證 : VP[yn || G^x mod N || Sp-1(yn || G^x mod N)]
⑧ 計算 : k = (G^x mod N)^y mod N
⑩ 以一連線鍵碼使用相同的對稱字將內容解密
104
P Sp-1(P_ID)
展開點 DB
108
P_ID
106
H SH-1(H_ID)
主機 DB
110
H_ID

第 7 圖

A8
B8
C8
D8

六、申請專利範圍

1. 一種認證第一與第二裝置之方法，包含：

在一第三裝置接收該等第一與第二裝置之辨識元；

根據該等辨識元擷取該第三裝置中之資訊；

根據所擷取之資訊由該第三裝置傳輸一訊息；以及

根據該訊息在該等第一與第二裝置中驗證該等第一與第二裝置的其他之一的身份。

2. 如申請專利範圍第1項所述之方法，其中該傳輸包括傳輸一訊息，其包括該等第一與第二裝置之公用鍵碼。

3. 如申請專利範圍第2項所述之方法，其中該傳輸包括傳輸一訊息，其包括該等第一與第二裝置之公用鍵碼的倒數。

4. 如申請專利範圍第1項所述之方法，其中該驗證包括使用一公用鍵碼密碼通訊協定來實施認證。

5. 如申請專利範圍第4項所述之方法，其中該驗證包括使用一公用鍵碼密碼通訊協定之離散對數版本來實施認證。

6. 如申請專利範圍第5項所述之方法，其中該驗證包括使用ElGamal密碼通訊協定來實施認證。

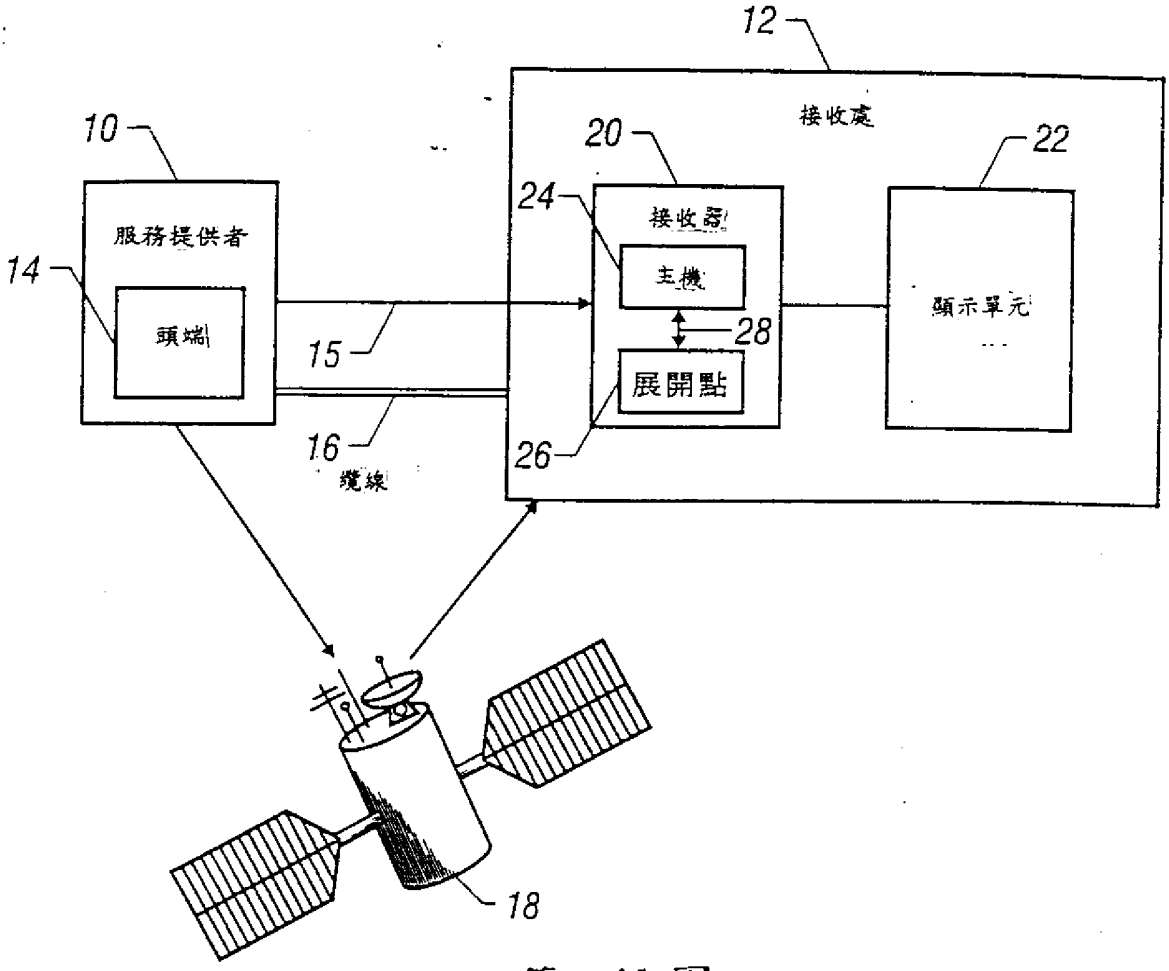
7. 如申請專利範圍第1項所述之方法，進一步包含在該等第一與第二裝置中產生一隨機數字，其中該驗證包括使用在每一該等第一與第二裝置中之該隨機數字。

8. 一種在一第一裝置與第二裝置間安全地通訊內容之方法，包含：

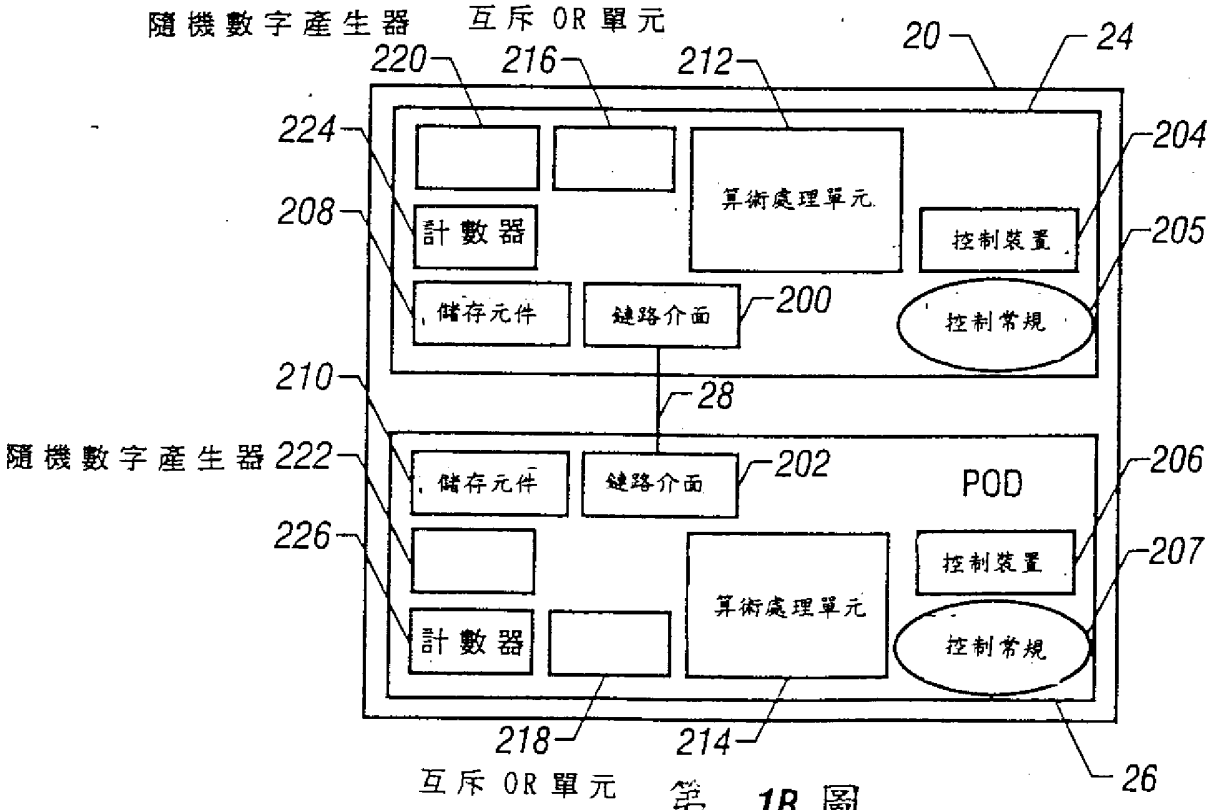
傳送該等第一與第二裝置之辨識資訊至一第三裝置；

根據該辨識資訊在該第三裝置中產生一預設的訊息

修正補充 90年5月7日



第 1A 圖



第 1B 圖

煩請委員明示 90 年 7 月 7 日所提之修正本有無變更實質內容是否准予修正。