(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201014249 A1
(43)公開日： 中華民國 99 (2010) 年 04 月 01 日

(21)申請案號：097151422 (22)申請日： 中華民國 97 (2008) 年 12 月 30 日
(51)Int. Cl.： *H04H60/23 (2008.01)*
(30)優先權：2008/09/24 美國 12/236,971
(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)
新竹縣竹東鎮中興路 4 段 195 號
(72)發明人：王景行 WANG, KING HANG (HK) ；陳錦德 CHEN, CHIN DER (TW) ；孫宏民 SUN, HUNG MIN (TW) ；高億憲 KAO, YIH SIEN (US)
(74)代理人：詹銘文；蕭錫清
申請實體審查：有 申請專利範圍項數：35 項 圖式數：5 共 36 頁

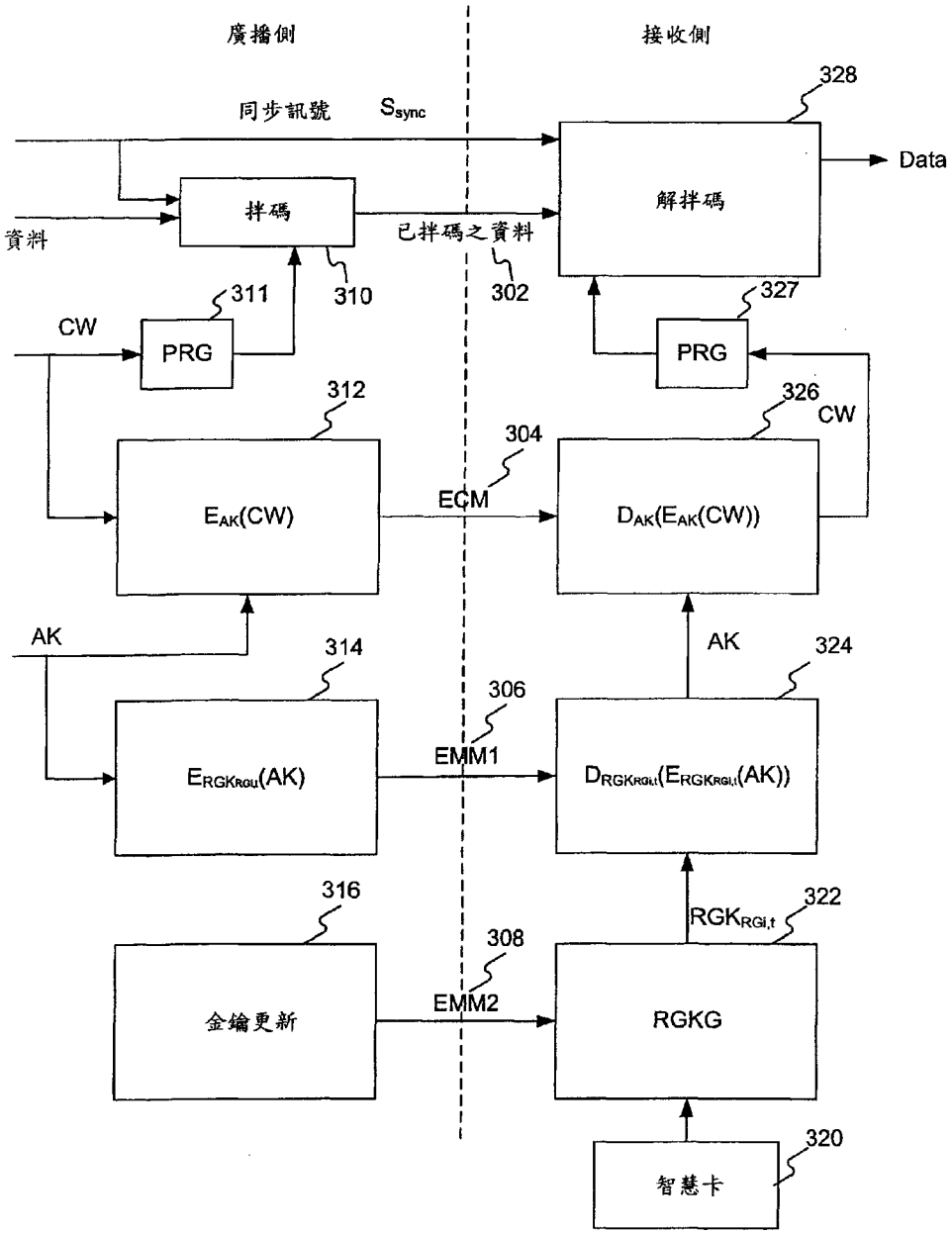
(54)名稱

金鑰管理系統與方法

SYSTEMS AND METHODS FOR KEY MANAGEMENT

(57)摘要

一種廣播系統的金鑰管理方法，其包含：產生由廣播系統所提供之接收方群組的接收方群組金鑰種子及多個參數；以及依據所述接收方群組金鑰種子值及所述多個參數來計算所述接收方群組的接收方群組金鑰。



300：廣播方法

302：已拌碼的資料

304：授權控制訊息（ECM）

306：第一授權管理訊息（EMM1）

308：第二授權管理訊息（EMM2）

310～328：步驟

320：智慧卡

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201014249 A1
(43)公開日： 中華民國 99 (2010) 年 04 月 01 日

(21)申請案號：097151422 (22)申請日： 中華民國 97 (2008) 年 12 月 30 日
(51)Int. Cl.： *H04H60/23 (2008.01)*
(30)優先權：2008/09/24 美國 12/236,971
(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)
新竹縣竹東鎮中興路 4 段 195 號
(72)發明人：王景行 WANG, KING HANG (HK) ；陳錦德 CHEN, CHIN DER (TW) ；孫宏民 SUN, HUNG MIN (TW) ；高億憲 KAO, YIH SIEN (US)
(74)代理人：詹銘文；蕭錫清
申請實體審查：有 申請專利範圍項數：35 項 圖式數：5 共 36 頁

(54)名稱

金鑰管理系統與方法

SYSTEMS AND METHODS FOR KEY MANAGEMENT

(57)摘要

一種廣播系統的金鑰管理方法，其包含：產生由廣播系統所提供之接收方群組的接收方群組金鑰種子及多個參數；以及依據所述接收方群組金鑰種子值及所述多個參數來計算所述接收方群組的接收方群組金鑰。

六、發明說明：

【發明所屬之技術領域】

本發明係有關於金鑰管理的系統與方法。

【先前技術】

廣播系統可能為有條件存取系統，其將數位媒體廣播至有存取權之用戶裝置。舉例而言，數位付費電視之廣播系統使得服務提供商能夠依據服務封裝方法提供各種付費服務，所述付費服務是用於經由衛星或電纜傳輸之視訊資料及音訊資料。所述視訊資料及音訊資料通常已用金鑰加密。用戶裝置需要用金鑰來解密已加密之視訊資料及音訊資料。

圖 1 說明廣播系統所執行之習知服務封裝方法 100。通常，廣播系統提供多個資料/內容通道。舉例而言，在圖 1 中，廣播系統提供八個資料/內容通道 Ch-1 102-1、Ch-2 102-2、...、Ch-8 102-8。每一通道 Ch-1 102-1、Ch-2 102-2、...、Ch-8 102-8 均可定義為獨立資源。

依據習知服務封裝方法，廣播系統除提供通道 Ch-1 102-1、Ch-2 102-2、...、Ch-8 102-8 之外，可進而提供多個通道封包，諸如第一、第二及第三通道封包 G-1 104-1、G-2 104-2 及 G-3 104-3。舉例而言，第一通道封包 G-1 104-1 可包含通道 Ch-1 102-1、Ch-2 102-2 及 Ch-6 102-6，第二通道封包 G-2 104-2 可包含通道 Ch-2 102-2、Ch-3 102-3 及 Ch-4 102-4，且第三通道封包 G-3 104-3 可包含通道 Ch-2

102-2、Ch-4 102-4 及 Ch-5 102-5。每一通道封包 G-1 104-1、G-2 104-2 及 G-3 104-3 可定義為一資源群組。

每一通道 Ch-1 102-1、Ch-2 102-2、....、Ch-8 102-8 及通道封包 G-1 104-1、G-2 104-2 及 G-3 104-3 可進而定義為一接收方群組。因此，在圖 1 中存在十一個接收方群組，包含八個通道 Ch-1 102-1、Ch-2 102-2、...、Ch-8 102-8 及三個通道封包 G-1 104-1、G-2 104-2 及 G-3 104-3。用戶裝置可預訂接收方群組中之一或多者。舉例而言，若用戶裝置之使用者對於通道 Ch-1 102-1、Ch-2 102-2、Ch-3 102-3 及 Ch-6 102-6 之內容感興趣，則用戶裝置可預訂分別對應於通道 Ch-3 104-3 及通道封包 G-1 104-1 的第一接收方群組及第二接收方群組。

圖 2 說明習知廣播方法 200。依據習知廣播方法 200，廣播系統可自廣播側（即廣播系統）向接收側（即用戶裝置）廣播已拌碼之資料 202、授權控制訊息（entitlement control message，以下簡稱為 ECM）204、第一授權管理訊息（first entitlement management message，以下簡稱為 EMM1）206 以及第二授權管理訊息（second entitlement management message，以下簡稱為 EMM2）208。

在廣播側，依據同步訊號 S_{sync} 用隨機訊號來加密或拌碼原始資料（例如數位媒體資料）之通道（步驟 210）並廣播已拌碼之資料 202。第一偽隨機產生器（pseudorandom generator，以下簡稱為 PRG）依據控制字碼（control word，以下簡稱為 CW）產生隨機訊號（步驟 211）。用對應於通

道之授權金鑰（authorization key，以下簡稱為 AK）來加密 CW（步驟 212），並在 ECM 訊息 204 內廣播已加密之 CW。通常諸如資料/內容通道之每一獨立資源可具有一 AK。用對應於接收方群組（包含所述通道）之接收方群組金鑰（receiver group key，RGK）來加密所述 AK（步驟 214），並在 EMM1 訊息 206 內廣播已加密之 AK。通常每一接收方群組可具有一 RGK。用主私密金鑰(master private key，以下簡稱為 MPK）來加密所述 RGK（步驟 216），並在 EMM2 訊息 206 內廣播已加密之 RGK。通常每一用戶裝置可具有或被提供有 MPK。MPK 對於每一用戶裝置是唯一的。

在接收側，用 MPK 解密接收到之 EMM2 訊息 208 以擷取 RGK（步驟 220）。舉例而言，可將 MPK 儲存於提供至用戶裝置的智慧卡內。隨後用所擷取之 RGK 來解密接收到之 EMM1 訊息 206 以擷取 AK（步驟 224），並用所擷取之 AK 來解密接收到之 ECM 訊息 204 以擷取 CW(步驟 226）。進而將所擷取之 CW 輸入至第二偽隨機產生器（pseudorandom generator，PRG）以產生隨機訊號（步驟 227），依據同步訊號 S_{sync} 使用所述隨機訊號來解拌碼接收到之已拌碼資料 202，以獲得原始資料（步驟 228）。

出於安全目的，通常例如每個月更新接收方群組的 RGK。此外，當新用戶裝置預訂接收方群組或現存用戶裝置自接收方群組取消預訂時，可能亦需更新 RGK。舉例而言，當新用戶裝置預訂接收方群組時，廣播系統更新接收

方群組之 RGK，以防新用戶裝置在更新之前獲得 RGK 以解密在新用戶裝置預訂接收方群之前廣播的資料。更舉例而言，當現存用戶裝置對於接收方群組之預訂到期時，廣播系統更新接收方群組之 RGK，使得用戶裝置不可在預訂到期後解密資料。進一步舉例而言，當現存用戶裝置在預訂到期前取消預訂或改變至另一接收方群組時，廣播系統更新接收方群組之 RGK，使得用戶裝置不可在取消或改變之後解密資料。

每當更新接收方群組之 RGK 時，廣播系統需向預訂接收方群組之用戶裝置廣播 EMM2 訊息，其包含更新後之 RGK。當 EMM2 訊息之資料量增加時，廣播系統之廣播負擔可能增加。

【發明內容】

根據本發明，提供一種廣播系統的金鑰管理方法，包括：產生由廣播系統所提供之接收方群組之接收方群組金鑰（receiver group key，RGK）種子及多個參數；以及依據所述接收方群組金鑰種子值及所述多個參數來計算接收方群組之 RGK。

亦根據本發明，提供一種廣播系統的廣播方法，包括：產生由廣播系統所提供之接收方群組的接收方群組金鑰（receiver group key，RGK）種子；依據所述接收方群組金鑰種子值計算接收方群組之 RGK；使用計算出之 RGK 來計算資料通道之授權金鑰（authorization key，AK）；以及

廣播包含已加密之 AK 的授權管理訊息（entitlement management message，EMM）。

進而根據本發明，提供一種用戶裝置存取自廣播系統廣播之資料通道的方法，包括：自廣播系統接收授權管理訊息（entitlement management message，EMM），所述 EMM 包含對應於所述通道之已加密之授權金鑰（authorization key，AK）；依據接收方群組金鑰種子值及多個金鑰來計算接收方群組之接收方群組金鑰（receiver group key，RGK），接收方群組包含所述通道；以及使用計算出之 RGK 來解密已加密之 AK。

進而根據本發明，提供一種用於提供多個接收方群組的廣播系統，所述系統用以：為每一所述多個接收方群產生一接收方群組金鑰（receiver group key，RGK）種子；以及依據相應接收方群組金鑰種子值為每一所述多個接收方群計算一 RGK。

應瞭解，前述一般說明及以下詳細說明均僅為例示性及解釋性的，而並不限制所主張的本發明。

【實施方式】

現在將詳細參照例示性實施例，附圖中說明了例示性實施例之實例。以下說明是關於附圖，其中不同圖中之相同標號指代相同或相似之元件，除非用其它方式來表示。以下對於例示性實施例之說明中闡述的符合本發明之實施方案並不代表所有符合本發明之實施方案。實情為，所述

實施方案僅為符合與隨附申請專利範圍內敘述之本發明有關之態樣的系統及方法的實例。

圖 3 說明根據例示性實施例之用以提供廣播系統之改良效能的廣播方法 300。舉例而言，所述廣播系統可提供多個接收方群組，諸如通道或通道封包，每一通道封包具有多個通道。

參看圖 3，廣播系統廣播已拌碼之資料 302、授權控制訊息（entitlement control message，ECM）304 以及第一授權管理訊息（first entitlement management message，EMM1）306。廣播系統可更包含廣播第二授權管理訊息（second entitlement management message，EMM2）308。

在符合本發明之例示性實施例中，廣播系統依據同步訊號 S_{sync} 用隨機訊號來加密（例如拌碼）諸如數位媒體資料之原始資料通道，以產生已拌碼之資料 302（步驟 310），並廣播已拌碼之資料 302。第一偽隨機產生器（pseudorandom generator，PRG）依據控制字碼（a control word，CW）產生隨機訊號（步驟 311）。廣播系統用對應於通道之授權金鑰（authorization key，AK）來加密 CW（步驟 312），並廣播包含已加密之 CW 的 ECM 訊息 304。廣播系統亦用對應於包含通道之接收方群組 RGi 並隨時間 *t* 而改變的接收方群組金鑰（receiver group key，RGK）$RGK_{RGi,t}$ 來加密 AK（步驟 314），並廣播包含已加密之 AK 的 EMM1 訊息 306。

在一個例示性實施例中，廣播系統產生多個接收方群

組金鑰種子值 RGK_{RGi}（i＝1,2,…，N，其中 N 為廣播系統提供之接收方群組的總數）或初始 RGK，其中一者會提供給每一所述多個接收方群組。舉例而言，廣播系統可隨機產生多個接收方群組金鑰種子值 RGK_{RGi} (i = 1, 2.....N)。

廣播系統依據相應接收方群組金鑰種子值 RGK_{RGi} (i = 1, 2.....N)為每一所述多個接收方群組計算一 RGK。舉例而言，廣播系統可例如每天為接收方群組 RGi 計算 $RGK_{RGi,t}$，以便每天更新 $RGK_{RGi,t}$。因此，$RGK_{RGi,t}$ 隨時間變化。亦舉例而言，更新計算是依據接收方群組 RGi 之接收方群組金鑰種子值 RGK_{RGi}，下文進一步說明此種更新計算。

在符合本發明之例示性實施例中，廣播系統可向預訂接收方群之一者的用戶裝置指派用於接收方群組之該者的接收方群組金鑰種子值。舉例而言，對於預訂接收方群組 RGi 之用戶裝置 U0，廣播系統向用戶裝置 U0 指派用於接收方群組 RGi 的接收方群組金鑰種子值 RGK_{RGi}。

若用戶裝置 U0 在預訂到期之前自接收方群組 RGi 取消預訂，則廣播系統可依據隨機數值更新接收方群組金鑰種子值 RGK_{RGi}（步驟 316），並使用下述金鑰更新方法來加密所述隨機數值。廣播系統進一步廣播 EMM2 訊息 308，包含已加密之隨機數值，使得預訂接收方群組 RGi 之其餘用戶裝置對應地接收已加密之隨機數值、解密已加密之隨機數值並使用隨機數值來更新接收方群組金鑰種子值 RGK_{RGi}。

然而，若用戶裝置 U0 在預訂到期時自接收方群組 RGi

取消預訂，則廣播系統無需廣播 EMM2 訊息 308。如上所述，廣播系統可每天計算接收方群組 RGi 之 $RGK_{RGi,t}$，以便每天更新 $RGK_{RGi,t}$。因此，$RGK_{RGi,t}$ 之值隨時間變化。用戶裝置 U0 使用下述金鑰導出方法，依據接收方群組金鑰種子值 RGK_{RGi} 及多個金鑰執行實質相同的更新計算，並因此獲得接收方群組 RGi 之 $RGK_{RGi,t}$。舉例而言，可將接收方群組 RGi 之接收方群組金鑰種子值 RGK_{RGi} 及所述多個金鑰儲存於提供至用戶裝置 U0 的智慧卡 320 內，使得用戶裝置 U0 可使用所述接收方群組金鑰種子值 RGK_{RGi} 及所述多個金鑰來計算 $RGK_{RGi,t}$。

然而，與廣播系統不同，用戶裝置 U0 僅可在預訂期間依據金鑰導出方法來執行更新計算。當預訂到期時，用戶裝置 U0 將無法執行更新計算。換言之，在預訂到期時，用戶裝置 U0 自動撤銷。

仍參看圖 3，在預訂期間，用戶裝置 U0 依據所述接收方群組金鑰種子值 RGK_{RGi} 及所述多個金鑰來計算 $RGK_{RGi,t}$（步驟 322）。舉例而言，用戶裝置 U0 可包含用以計算 $RGK_{RGi,t}$ 之值的 RGK 產生器（RGK generator，RGKG）。用戶裝置 U0 接收 EMM1 訊息 306 並用 $RGK_{RGi,t}$ 之計算出的值來解密接收到的 EMM1 訊息 306，以擷取 AK（步驟 324）。用戶裝置 U0 亦接收 ECM 訊息 304 並用所擷取之 AK 來解密接收到之 ECM 訊息 304 以擷取 CW（步驟 326）。依據所擷取之 CW，第二偽隨機產生器（pseudorandom generator，PRG）產生隨機訊號（步驟 327）。用戶裝置 U0

進一步接收已拌碼之資料 302，並依據同步訊號 S_{sync} 使用隨機訊號來對接收到之已拌碼資料 302 進行解拌碼以獲得原始資料（步驟 328）。

在符合本發明之例示性實施例中，為使用廣播方法 300 之廣播系統提供多個金鑰管理方法。金鑰管理方法可包含初始化方法、金鑰指派方法、上述金鑰導出方法以及上述金鑰更新方法。下文中進一步說明此等金鑰管理方法。

圖 4 說明根據例示性實施例之金鑰管理用的初始化方法 400。依據初始化方法 400，廣播系統在系統電力開啟期間產生多個接收方群組金鑰種子值（其中之一會提供至每一接收方群組）以及多個參數。舉例而言，廣播系統依據與橢圓曲線密碼學（elliptic curve cryptography，ECC）中之雙線性配對函數以及離散對數問題有關之密碼學方法來產生所述多個參數。

參看圖 4，廣播系統選擇第一質數 a 及第二質數 b，並設定等於 a 與 b 之乘積的數字 n，即 n＝axb（步驟 402）。舉例而言，數字 a 與 b 可為大質數。廣播系統在第 n 次橢圓曲線 E 上定位點 P（步驟 404），並在橢圓曲線 E 上識別雙線性配對函數 e（步驟 406）。

廣播系統亦選擇大數字 z，例如 $z=10^6$（步驟 408）。廣播系統進一步隨機選擇第一非零整數 s 及第二非零整數 k，其每一者均小於數字 n（步驟 410）。整數 s 與數字 n 是相對質數，且整數 k 與數字 n 亦為相對質數。此外，廣播系統產生多個接收方群組金鑰種子值，其中之一會提供

給每一接收方群組（步驟 412）。步驟 402 至步驟 412 可用不同順序執行。舉例而言，可首先執行步驟 412，接下來執行步驟 402 至步驟 410。

在一例示性實施例中，依據初始化方法 400，廣播系統可進一步產生多個樹狀結構，其中之一會提供給每一接收方群組。舉例而言，當用戶裝置 U0 在預訂到期前自接收方群 RGi 取消預訂時，接收方群 RGi 之樹狀結構可提供私密金鑰以更新接收方群組金鑰種子值 RGK_{RGi}。

圖 5 說明根據例示性實施例由廣播系統產生之例示性樹狀結構 500。例示性樹狀結構 500 是廣播系統針對接收方群 RGi 產生的二元樹。僅出於說明之目的，假定最多四個用戶裝置將預訂接收方群組 RGi。

參看圖 5，樹狀結構 500 具有多個節點 V0、V1、...、V6，其中節點 V3、V4、V5 及 V6 為葉節點。在所說明之實施例中，可向葉節點指派用戶裝置。因此，樹狀結構 500 中之四個葉節點 V3、V4、V5 及 V6 構成預訂接收方群組 RGi 之四個用戶裝置。

節點 Vi（i＝0, 1, ..., 6）每一者與一質數 εvi 相關聯，質數 εvi 在圖 5 中繪示為經過標記。舉例而言，節點 V0 與質數 2 相關聯，即 $\varepsilon vo = 2$。亦舉例而言，節點 V6 與質數 17 相關聯，即 $\varepsilon v6 = 17$。分別用於節點 V0、V1、...、及 V6 之質數 εvi（i＝0, 1, ..., 6）為公開資訊，且可用於依據等式（1）及（2）產生私密金鑰 I_{vi}（i= 1, 2.....6），其每一者與節點 V1, V2, ..., 及 V6 之一相關聯：

$$I_{vi} = g^{e_{vi}} (\mathrm{mod}\, n) \qquad \text{等式(1)}$$

$$e_{vi} = \prod_{v} \varepsilon_v / (\varepsilon_{vi} \cdot \prod_{vj<vi} \varepsilon_{vj}) \qquad \text{等式(2)}$$

其中 g 為非零整數，e_{Vi} 為對應於節點 Vi 之臨時數值，且僅用於說明目的，mod 為模數運算子，且 Π 為對兩個或兩個以上數字之乘法運算。等式（2）展示對應於節點 Vi 之臨時數值 e_{Vi} 等於第一值與第二值之間的比率，第一值為用於樹狀結構 500 內之所有節點 V0、V1、...，及 V6 之質數 ε_{v1}, ε_{v2}.....ε_{V6} 的乘積，第二值為用於節點 Vi 之質數 ε_{vi} 之質數與分別用於節點 Vi 之後代節點 Vj 之質數的乘積。若節點 Vi 為葉節點例如節點 V6 且因此無後代節點，則第二值將為節點 Vi 之質數 εvi。

舉例而言，對應於節點 V1 之臨時數值 e_{v1} 等於第一值與第二值之間的比率。第一值等於用於樹狀結構 500 內之所有節點 V0、V1、...，及 V6 之質數 ε_{v1}, s_{v2}.....ε_{V6} 的乘積，即第一值等於 2 x 3 x 5x 7 x 11 x 13 x 17。第二值等於節點 V1 之質數 e_{v1} 與分別用於節點 V1 之後代節點 Vj 之質數的乘積。在所說明之實施例中，節點 V3 及 V4 為節點 V1 之後代節點。因此，第二值等於 3x7x11。結果，對應於節點 V1 之臨時數值 e_{v1} 等於(2x3x5x7x11x13x17)/(3x7x11)=2 x5x13x17。

亦舉例而言，對應於節點 V6 之臨時數值 e_{v6} 等於第一

值與第二值之間的比率。第一值等於樹狀結構 500 內之所有節點 V0、V1、...，及 V6 之質數 $\varepsilon_{v1}, \varepsilon_{v2}, \ldots, \varepsilon_{V6}$ 的乘積，即第一值等於 2x3x5x7x11x13x17。第二值等於節點 V6 之質數 ε_{V6} 與節點 V6 之後代節點 Vj 之質數的乘積。然而，在所說明之實施例中，節點 V6 為葉節點，且因此無後代節點。因此，第二值等於節點 V6 之質數 ε_{V6}，即 17。因此，對應於節點 V6 之臨時數值 ε_{V6} 等於 (2x3x5x7x11x13x17)/17=2x3x5x7x11x13。

如上所述，分別用於節點 V0、V1、...，及 V6 之質數 ε_{vi}(i = 0, 1.....6)為公開資訊。因此，用於葉節點 V3、V4、V5 及 V6 之私密金鑰 I_{V3}、I_{V4}、I_{V5} 及 I_{V6} 可每一者自用於節點 V1 及 V2 之私密金鑰 I_{V1} 及 I_{V2} 導出。舉例而言，葉節點 V3 之私密金鑰 I_{V3} 可依據質數 ε_{v1} 及 ε_{v4} 自母代節點 V1 之私密金鑰 I_{V1} 導出。然而，節點 V1 之私密金鑰 I_{V1} 可能不可自節點 V3 之私密金鑰 I_{V3} 導出，其為密碼學中基於 RSA 之問題。

在符合本發明之例示性實施例中，依據金鑰指派方法，廣播系統向自開始時間 *t1* 至結束時間 *t2* 預訂接收方群之一者之用戶裝置指派多個金鑰及用於接收方群之該者的接收方群組金鑰種子值之一。舉例而言，開始時間 *t1* 與結束時間 *t2* 可每一者相對於執行系統電力啟動時之時間而量測。

在所說明之實施例中，對於預訂接收方群組 RGi 之用戶裝置 U0，廣播系統向用戶裝置 U0 指派金鑰 s/k、$s^{t1}P$、

$a^{t1}P$、$K^{(t2-t1)}b^{(z-t2)}P$、$ka+b/k$、$t1$ 及 $t2$ 以及接收方群組金鑰種子值 RGK_{RGi}，其中 s、k、P、a 及 b 為在上述初始化方法下產生之參數。可將此等金鑰及接收方群組金鑰種子值 RGK_{RGi} 儲存於提供至用戶裝置 U0 的智慧卡內。

此外，廣播系統向樹狀結構內對應於用戶裝置 U0 預訂之接收方群組之一的葉節點之一指派用戶裝置 U0。舉例而言，廣播系統向樹狀結構 500 內對應於接收方群組 RGi 之葉節點 V6 指派用戶裝置 U0。

廣播系統進一步例如在用戶裝置 U0 執行向廣播系統之註冊時向用戶裝置 U0 指派私密金鑰 I_{vi}（i＝1，2，…6）之一。舉例而言，廣播系統向用戶裝置 U0 指派用戶裝置 U0 已指派的節點 V6 之同輩節點之私密金鑰。在所說明之實施例中，廣播系統向用戶裝置 U0 指派節點 V5 之私密金鑰 I_{v5}，節點 V5 為節點 V6 之同輩節點。亦舉例而言，廣播系統向用戶裝置 U0 指派深度與節點 V6 之母代節點相同之節點（即節點 V6 之母代節點之相鄰節點）的私密金鑰。在所說明之實施例中，節點 V6 之母代節點為節點 V2，節點 V2 之相鄰節點為 V1。因此，廣播系統向用戶裝置 U0 指派節點 V1 之私密金鑰 I_{v1}。然而，廣播系統並不向用戶裝置 U0 指派用戶裝置 U0 已指派的節點 V6 之私密金鑰 I_{v6}。

在以上私密金鑰指派之後，指派給葉節點 V6 之用戶裝置 U0 知曉樹狀結構 500 內之每一其餘葉節點的私密金鑰或可導出所述私密金鑰。舉例而言，用戶裝置 U0 知曉葉節點 V5 之私密金鑰 I_{v5}。亦舉例而言，可如上所述依據

質數 ε_{v1} 及 ε_{v4} 根據節點 V1 之私密金鑰 I_{V1} 來導出葉節點 V3 之私密金鑰 I_{V3}。然而，用戶裝置 U0 並不知曉用戶裝置 U0 已指派的節點 V6 之私密金鑰 I_{V6}。換而言之，若將用戶裝置指派給樹狀結構 500 內之葉節點之一，則該用戶裝置知曉樹狀結構 500 內每一其餘葉節點之私密金鑰或可導出所述私密金鑰，而非該用戶裝置所指派之葉節點的私密金鑰。

在符合本發明之例示性實施例中，依據金鑰導出方法，廣播系統計算每一接收方群組的 RGK。舉例而言，廣播系統依據接收方群組金鑰種子值 RGK_{RGi} 及多個參數中之參數來計算接收方群組 RGi 之 $RGK_{RGi,t}$。

在一例示性實施例中，廣播系統依據以下等式例如每天計算接收方群組 RGi 之 $RGK_{RGi,t}$，以便每天更新 $RGK_{RGi,t}$：

$$RGK_{RGi,t} = (RGK_{RGi})^{TK_t} \qquad \text{等式(3)}$$

$$TK_t = e(P,P)^{(a^t + b^{z-t})s^t} \qquad \text{等式(4)}$$

其中 TK_t 為計算出之金鑰，e、P、a、b 及 z 為在上述初始化方法下產生之參數，且 t 為相對於執行系統電力啟動時之時間的當前時間。因此，$RGK_{RGi,t}$ 隨時間變化。

用戶裝置 U0 亦依據等式（3）執行計算，並因此獲得接收方群組 RGi 之 $RGK_{RGi,t}$。舉例而言，假設 $t = t1+x =$

$t2\text{-}y(x \geqq 0, y \geqq 0)$，其中 t 為當前時間。在所說明之實施例中，用戶裝置 U0 使用儲存於智慧卡內之金鑰 s/k、$s^{t1}P$、$a^{t1}P$、$K^{(t2-t1)}b^{(z-t2)}P$、$ka+b/k$、$t1$ 及 $t2$ 來執行以下計算：

$$A = a^{t1}P \times (ka + b/k)^x = k^x a^{t1+x} P = k^x a^t P, \quad \text{等式(5)}$$

$$B = k^{(x+y)} b^{z-t2} p \times (ka+b/k)^y = k^{x+y} k^{-y} b^{z-t2+y} P = k^x b^{z-t} P, \quad \text{等式(6)}$$

$$C = S^{t1}P \times (s/k)^x = (s^{t1+x}/k^x)P = (s^t/k^x)P \quad \text{等式 (7)}$$

$$\begin{aligned} e(A+B, C) &= e((k^x a^t + k^x b^{z-t})P, (s^t/k^x)P) \\ &= e((a^t + b^{z-t})P, s^t P) \\ &= e(P,P)^{(a^t + b^{z-t})s^t} \end{aligned} \quad \text{等式(8)}$$

其中 A、B 及 C 為臨時數值，且 e 為上述初始化方法下產生的參數。

等式（8）中由用戶裝置 U0 計算之 $e(A+B, C)$的值實質上等於等式（4）中由廣播系統計算之金鑰 TK_t。因此，用戶裝置 U0 可在依據等式（5）至（8）執行計算後獲得金鑰 TK_t，即 $TK_t = e(A+B, C)$。用戶裝置 U0 進一步基於等式(3)執行計算，並因此獲得接收方群組 RGi 之 $RGK_{RGi,t}$。

不同於廣播系統，用戶裝置 U0 可依據等式(5)至(8)來執行計算，且因此僅在預訂期間（即，當 $t1 \leqq t \leqq t2$ 時）依據等式（3）執行計算。將開始時間 $t1$ 及結束時間 $t2$ 作為金鑰之一儲存於提供至用戶裝置 U0 的智慧卡內。當預

訂到期時，用戶裝置 U0 將無法執行計算。換而言之，用戶裝置 U0 在預訂到期時自動撤銷。

在符合本發明之例示性實施例中，依據金鑰更新方法，當用戶裝置在預訂到期時自接收方群組之一者取消預訂時，廣播系統更新對應於接收方群組之該者的接收方群組金鑰種子值之一。舉例而言，當用戶裝置 U0 在預訂到期之前自接收方群組 RGi 取消預訂時，廣播系統依據隨機數值更新接收方群組 RGi 之接收方群組金鑰種子值 RGK_{RGi}。廣播系統進一步加密所述隨機數值，並將包含已加密之隨機數值的 EMM2 訊息 306（圖 3）廣播至其它用戶裝置。

再次參看圖 5，僅出於說明目的，假定用戶裝置 U1、U2 及 U3 以及用戶裝置 U0 預訂接收方群組 RGi，且因此被分別指派給對應於接收方群組 RGi 的樹狀結構 500 之葉節點 V3、V4、V5 及 V6。

在所說明之實施例中，當用戶裝置 U0 自接收方群組 RGi 取消預訂時，廣播系統產生隨機數值 X，並依據隨機數值 X 更新接收方群組 RGi 之接收方群組金鑰種子值 RGK_{RGi}。舉例而言，廣播系統使用以下等式來更新接收方群組金鑰種子值 RGK_{RGi}。

$$RGK_{RGi}' = (RGK_{RGi})^{X}, \quad \text{等式(9)}$$

其中 RGK_{RGi}' 為接收方群組 RGi 之經更新的 RGK。

廣播系統亦用用戶裝置U0已指派的節點V6之私密金鑰 I_{v6} 來加密數字 X，並向其它預訂接收方群組 RGi 之用戶裝置（即，用戶裝置 U1、U2 及 U3）廣播包含已加密之數字 X 的 EMM2 訊息 308（圖 3）。廣播系統進一步依據以下等式來更新每一者與節點 V1, V2.....及 V6 之一相關聯之私密金鑰 I_{vi} (i = 1, 2, ..., 6)。

$$I_{vi}' = I_{vi}^{X} \pmod{n} \quad \text{等式} \quad (10)$$

其中 n 為在上述初始化方法中產生之數字，且 I_{vi}' 為經更新之 I_{vi}。

用戶裝置 U1、U2 及 U3 接收包含已加密之數字 X 的 EMM2 訊息 308（圖 3）。如上所述，對於指派給樹狀結構 500 之葉節點之一的用戶裝置，該用戶裝置知曉樹狀結構 500 內每一其餘葉節點之私密金鑰或可導出所述私密金鑰。在所說明之實施例中，用戶裝置 U1 及 U2 分別指派給葉節點 V3 及 V4，且因此可依據節點 V2 之私密金鑰 I_{v2} 導出葉節點 V6 之私密金鑰 I_{v6}。指派給葉節點 V5 之用戶裝置 U3 知曉葉節點 V6 的私密金鑰 I_{v6}。因此，用戶裝置 U1、U2 及 U3 每一者可解密已加密之數字 X 以獲得數字 X，並亦依據等式（9）來更新接收方群組金鑰種子值 RGK_{RGi}。此外，用戶裝置 U1、U2 及 U3 可進一步使用數字 X 來依據等式（10）更新其相應所指派的私密金鑰。

熟習此項技術者藉由考慮此處揭露之本發明的說明及

實踐而將容易明白本發明的其它實施例。本申請案意欲涵蓋對本發明之遵循本發明之一般原理且包含屬於此項技術中之已知或慣例實踐內的與本發明之偏離的任何更改、使用或調適。希望僅將說明書及實例視為例示性的，本發明之真正範疇及精神由隨附申請專利範圍指示。

將明白，本發明不限於上文已描述並在附圖中說明之確切構造，且在不偏離本發明之範疇的情況下可對其進行各種修改及變化。希望本發明之範疇僅受隨附申請專利範圍之限制。

【圖式簡單說明】

附圖併入本說明書並構成本說明書的一部分，附圖與說明內容一起說明本發明之實施例，並用以解釋本發明之原理。

圖 1 說明廣播系統執行之習知服務封裝方法。

圖 2 說明習知廣播方法。

圖 3 說明根據例示性實施例之廣播系統用的廣播方法。

圖 4 說明根據例示性實施例之金鑰管理用的初始化方法。

圖 5 說明根據例示性實施例之由廣播系統產生的例示性樹狀結構。

【主要元件符號說明】

100：服務封裝方法

200：廣播方法

202：已拌碼之資料

204：授權控制訊息（ECM）

206：第一授權管理訊息（EMM1）

208：第二授權管理訊息（EMM2）

210～228：步驟

300：廣播方法

302：已拌碼之資料

304：授權控制訊息（ECM）

306：第一授權管理訊息（EMM1）

308：第二授權管理訊息（EMM2）

310～328：步驟

320：智慧卡

400：初始化方法

402～412：方法步驟

500：樹狀結構

Ch-1 102-1～Ch-8 102-8：通道

G-1 104-1、G-2 104-2、G-3 104-3：通道封包

V0～V6：節點

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號： 97151422

※ 申請日期： 97.12.30 ※IPC 分類：H04H 60/23 (2008.01)

一、發明名稱：

金鑰管理系統與方法 / SYSTEMS AND METHODS FOR KEY MANAGEMENT

二、中文發明摘要：

一種廣播系統的金鑰管理方法，其包含：產生由廣播系統所提供之接收方群組的接收方群組金鑰種子及多個參數；以及依據所述接收方群組金鑰種子值及所述多個參數來計算所述接收方群組的接收方群組金鑰。

三、英文發明摘要：

A method for key management for a broadcasting system includes generating a receiver group key (RGK) seed and a plurality of parameters for a receiver group provided by the broadcasting system; and calculating an RGK for the receiver group based on the RGK seed and the plurality of parameters.

七、申請專利範圍：

1.一種金鑰管理方法，適於一廣播系統，該金鑰管理方法包括：

產生一接收方群組金鑰種子值與多個參數值給由該廣播系統所提供的一接收方群組；以及

依據該接收方群組金鑰種子值及該些參數值以計算該接收方群組的一接收方群組金鑰。

2.如申請專利範圍第 1 項所述之金鑰管理方法，更包括：

隨機產生該接收方群組金鑰種子值。

3.如申請專利範圍第 1 項所述之金鑰管理方法，更包括：

依據一橢圓曲線以及該橢圓曲線上之一雙線性配對函數來產生該些參數。

4.如申請專利範圍第 1 項所述之金鑰管理方法，更包括：

向預訂該接收方群組的一用戶裝置指派該接收方群組金鑰種子值以及多個金鑰，所述每一個金鑰係由該些參數中的多者所產生。

5.如申請專利範圍第 4 項所述之金鑰管理方法，更包括：

若該用戶裝置在該用戶裝置之預訂到期之前自該接收方群組取消預訂時，則更新該接收方群組的該接收方群組金鑰種子值。

6.如申請專利範圍第 4 項所述之金鑰管理方法，更包括：

當該用戶裝置之預訂到期時，計算該接收方群組沒有廣播該已計算出之接收方群組金鑰的該接收方群組金鑰。

7.如申請專利範圍第 4 項所述之金鑰管理方法，其中指派該接收方群組金鑰種子值以及該些金鑰的步驟包括：

將該接收方群組金鑰種子值以及該些金鑰儲存於提供至該用戶裝置的一智慧卡內。

8.如申請專利範圍第 1 項所述之金鑰管理方法，更包括：

為該接收方群組產生包含多個節點之一樹狀結構；

向每一個節點指派一質數；以及

依據該指派的質數產生多個私密金鑰，而該些私密金鑰其中之一會提供給每一個節點。

9.如申請專利範圍第 8 項所述之金鑰管理方法，其中該些節點包含多個葉節點，而該金鑰管理方法更包括：

向該些葉節點其中之一指派預訂該接收方群組的一用戶裝置；以及

向該用戶裝置指派該些私密金鑰中的多者，藉以使得該用戶裝置得知或者可導出該些葉節點中之每一其餘葉節點的該私密金鑰。

10.如申請專利範圍第 9 項所述之金鑰管理方法，其中當該用戶裝置在該用戶裝置之預訂到期之前自該接收方群組取消預訂時，該金鑰管理方法更包括：

更新該接收方群組的該接收方群組金鑰種子值。

11.如申請專利範圍第 10 項所述之金鑰管理方法，其中更新該接收方群組的該接收方群組金鑰種子值的步驟包括：

產生一隨機數值；

依據該隨機數值來更新該接收方群組金鑰種子值；

使用所述該些葉節點之其中之一的該私密金鑰來對該隨機數值進行加密；以及

廣播該已加密的隨機數值。

12.如申請專利範圍第 11 項所述之金鑰管理方法，其中產生該接收方群組金鑰種子值的步驟包括：

產生該接收方群組金鑰種子值給一通道或一通道封包。

13.一種廣播方法，適於一廣播系統，該廣播方法包括：

產生由該廣播系統所提供之一接收方群組的一接收方群組金鑰種子；

依據該接收方群組金鑰種子值計算該接收方群組的一接收方群組金鑰；

使用該已計算出的接收方群組金鑰而對一資料通道之一授權金鑰進行加密；以及

廣播包含該已加密之授權金鑰的一授權管理訊息。

14.如申請專利範圍第 13 項所述之廣播方法，更包括：

向預訂該接收方群組的一用戶裝置指派該接收方群組金鑰種子值。

15.如申請專利範圍第 14 項所述之廣播方法，更包括：

若該用戶裝置在該用戶裝置之預訂到期之前自該接收方群組取消預訂時，則更新該接收方群組金鑰種子值。

16.如申請專利範圍第 15 項所述之廣播方法，其中所述更新該接收方群組金鑰種子值的步驟包括：

產生一隨機數值；

依據該隨機數值來更新該接收方群組金鑰種子值；

對該隨機數值進行加密；以及

廣播該已加密的隨機數值。

17.如申請專利範圍第 14 項所述之廣播方法，更包括：

在該用戶裝置之預訂到期時，計算該接收方群組沒有廣播該已計算出之接收方群組金鑰的該接收方群組金鑰。

18.如申請專利範圍第 13 項所述之廣播方法，更包括：

使用該授權金鑰來加密一控制字碼；以及

廣播包含該已密之控制字碼的一授權控制訊息。

19.如申請專利範圍第 18 項所述之廣播方法，更包括：

依據該控制字碼來產生一隨機訊號；

使用該隨機訊號對該資料通道進行加密；以及

廣播該已加密的資料通道。

20.如申請專利範圍第 19 項所述之廣播方法，其中加密該資料通道的步驟包括：

使用該隨機訊號來拌碼該資料通道。

21.如申請專利範圍第 13 項所述之廣播方法，其中產生由該廣播系統所提供之該接收方群組的該接收方群組金鑰種子之步驟包括：

產生該接收方群組金鑰種子值給一通道或一通道封

包。

22.如申請專利範圍第 13 項所述之廣播方法，其中產生由該廣播系統所提供之該接收方群組的該接收方群組金鑰種子之步驟包括：

產生由一數位廣播系統或一付費電視系統所提供之一接收方群組的該接收方群組金鑰種子值。

23.一種用於用戶裝置存取自廣播系統廣播之資料通道的方法，包括：

自該廣播系統接收一授權管理訊息，該授權管理訊息包含對應於該資料通道的一已加密過的授權金鑰；

依據一接收方群組金鑰種子值以及多個金鑰計算一接收方群組的一接收方群組金鑰，該接收方群組包含該資料通道；以及

使用該計算出的該接收方群組金鑰對該已加密的授權金鑰進行解密。

24.如申請專利範圍第 23 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，更包括：

自該廣播系統接收一授權控制訊息，該授權控制訊息包含一已加密過的控制字碼；以及

使用該已解密的授權金鑰來解密該已加密的控制字碼。

25.如申請專利範圍第 24 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，更包括：

自該廣播系統接收一已拌碼的資料；

依據該已解密之控制字碼產生一隨機訊號；以及

使用該隨機訊號來解拌碼該已拌碼的資料。

26.如申請專利範圍第 23 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，其中將該接收方群組金鑰種子值及該些金鑰儲存於提供至該用戶裝置的一智慧卡內。

27.如申請專利範圍第 23 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，其中該用戶裝置為一第一用戶裝置，所述用於用戶裝置存取自廣播系統廣播之資料通道的方法更包括：

若一第二用戶裝置在該第二用戶裝置之預訂到期之前自該接收方群組取消預訂時，則更新該接收方群組的該接收方群組金鑰種子值。

28.如申請專利範圍第 27 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，其中更新該接收方群組的該接收方群組金鑰種子值的步驟包括：

接收對應於該第二用戶裝置之一受私密金鑰加密的隨機數值；

解密該已加密的隨機數值；以及

依據該已解密的隨機數值更新該接收方群組的該接收方群組金鑰種子值。

29.如申請專利範圍第 23 項所述之用於用戶裝置存取自廣播系統廣播之資料通道的方法，其中該用戶裝置為一第一用戶裝置，且該授權管理訊息為一第一授權管理訊息，該用於用戶裝置存取自廣播系統廣播之資料通道的方法更包括：

當一第二用戶裝置對該接收方群組之預訂到期時，計算該接收方群組不自該廣播系統接收一第二授權管理訊息的該接收方群組金鑰。

30.一種提供多個接收方群組的廣播系統，該廣播系統用以：

為每一個接收方群組產生一接收方群組金鑰種子；以及

依據該相應接收方群組金鑰種子值為每一個接收方群組計算一接收方群組金鑰。

31.如申請專利範圍第 30 項所述之廣播系統，更用以：

向預訂該些接收方群組之一者的用戶裝置指派該些接收方群組之一者的該接收方群組金鑰種子值。

32.如申請專利範圍第 31 項所述之廣播系統，更用以：

若該用戶裝置在該用戶裝置之預訂到期之前自該些接收方群組之一者取消預訂時，則更新所述該些接收方群組之一者的該接收方群組金鑰種子值。

33.如申請專利範圍第 31 項所述之廣播系統，更用以：

在該用戶裝置之預訂到期時，計算所述該些接收方群組之一者沒有廣播該已計算出之接收方群組金鑰的該接收方群組金鑰。

34.如申請專利範圍第 30 項所述之廣播系統，其中該廣播系統為一用於廣播數位媒體的數位廣播系統。

35.如申請專利範圍第 30 項所述之廣播系統，其中該廣播系統為一付費電視系統。

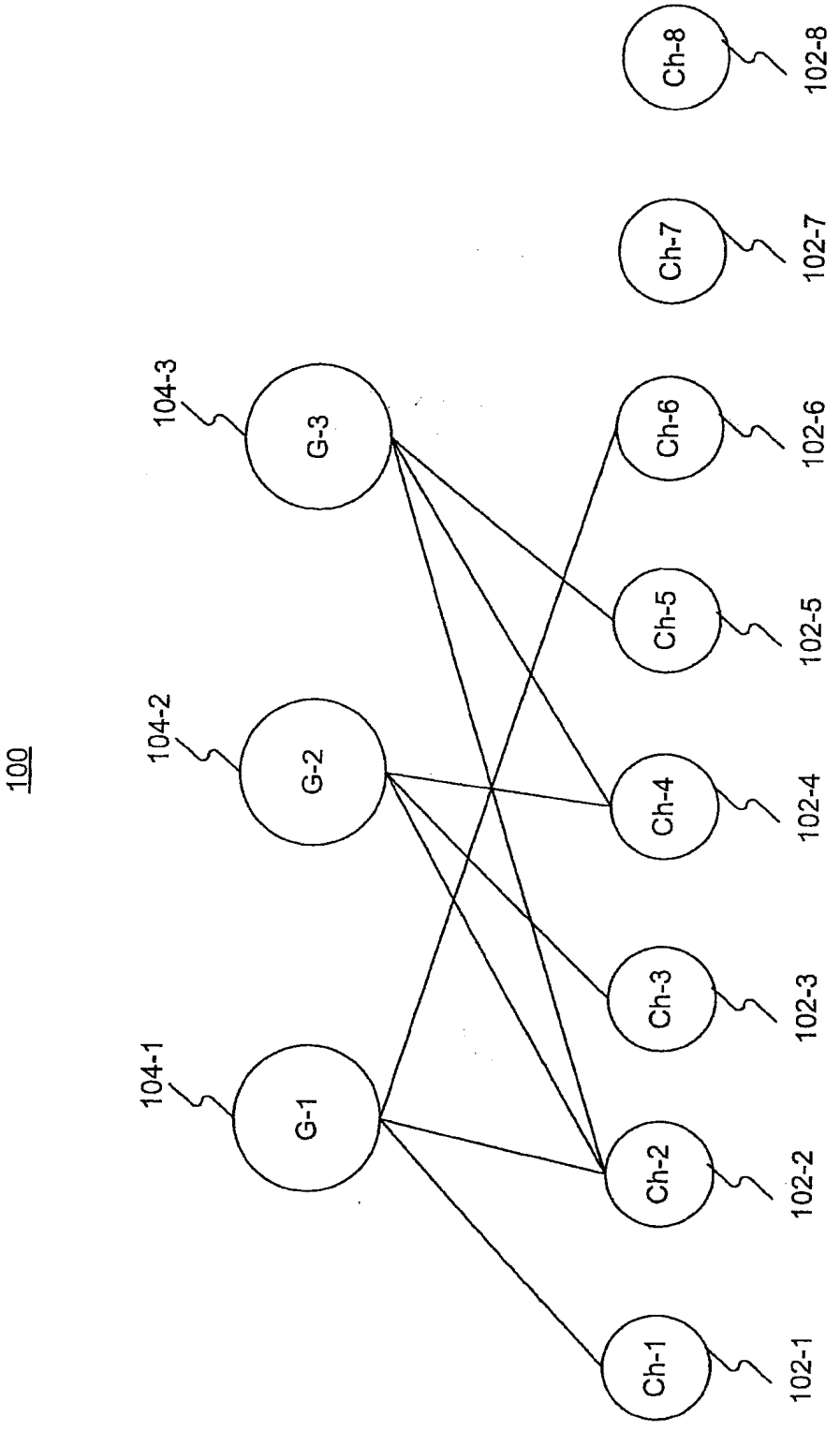

100
104-1
G-1
104-2
G-2
104-3
G-3
Ch-1
102-1
Ch-2
102-2
Ch-3
102-3
Ch-4
102-4
Ch-5
102-5
Ch-6
102-6
Ch-7
102-7
Ch-8
102-8

圖 1

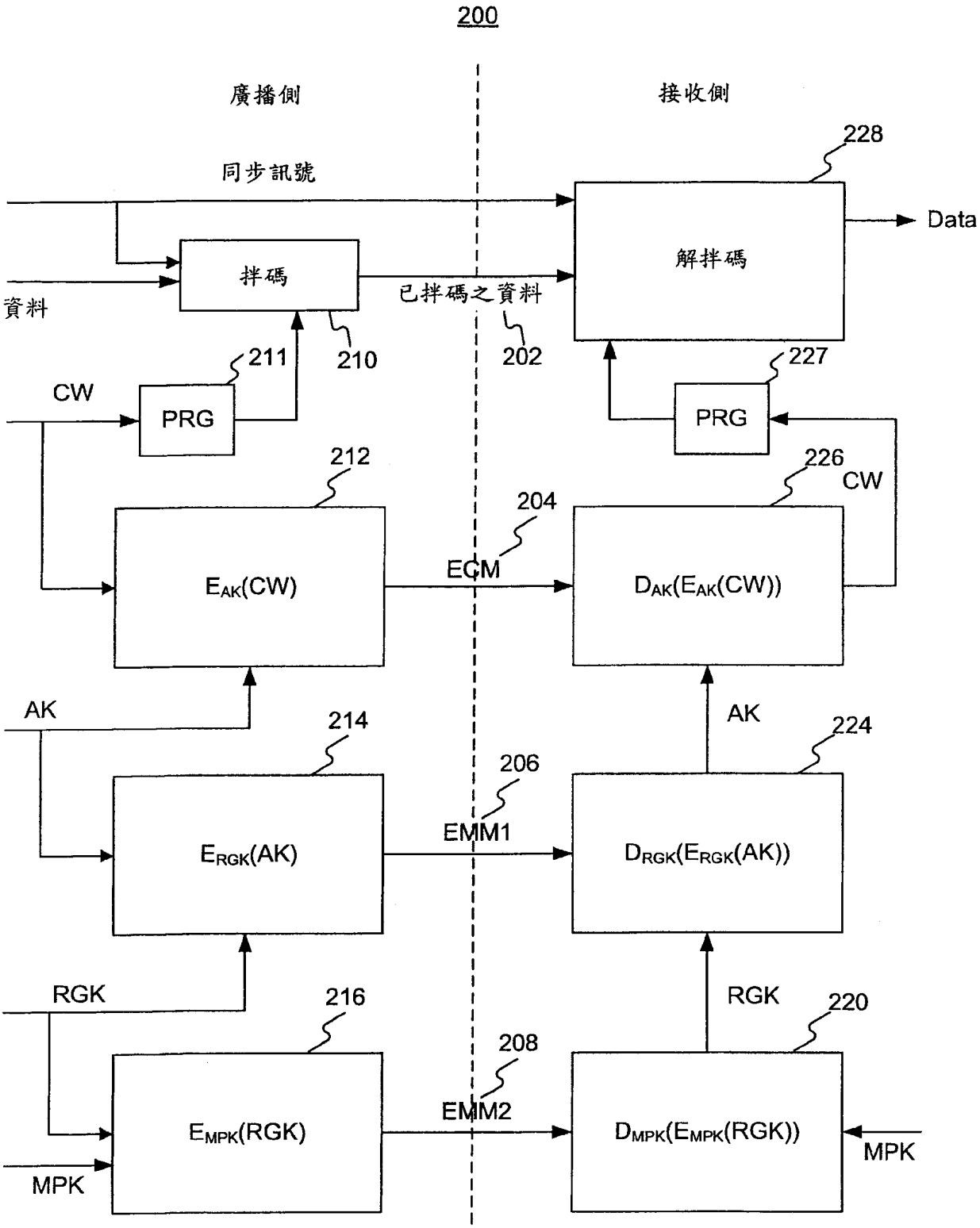

200
廣播側
接收側
同步訊號
資料
拌碼
已拌碼之資料
解拌碼
Data
228
210
202
211
227
CW
PRG
PRG
212
226
CW
204
ECM
$E_{AK}(CW)$
$D_{AK}(E_{AK}(CW))$
AK
AK
214
224
206
EMM1
$E_{RGK}(AK)$
$D_{RGK}(E_{RGK}(AK))$
RGK
RGK
216
220
208
EMM2
$E_{MPK}(RGK)$
$D_{MPK}(E_{MPK}(RGK))$
MPK
MPK

圖 2

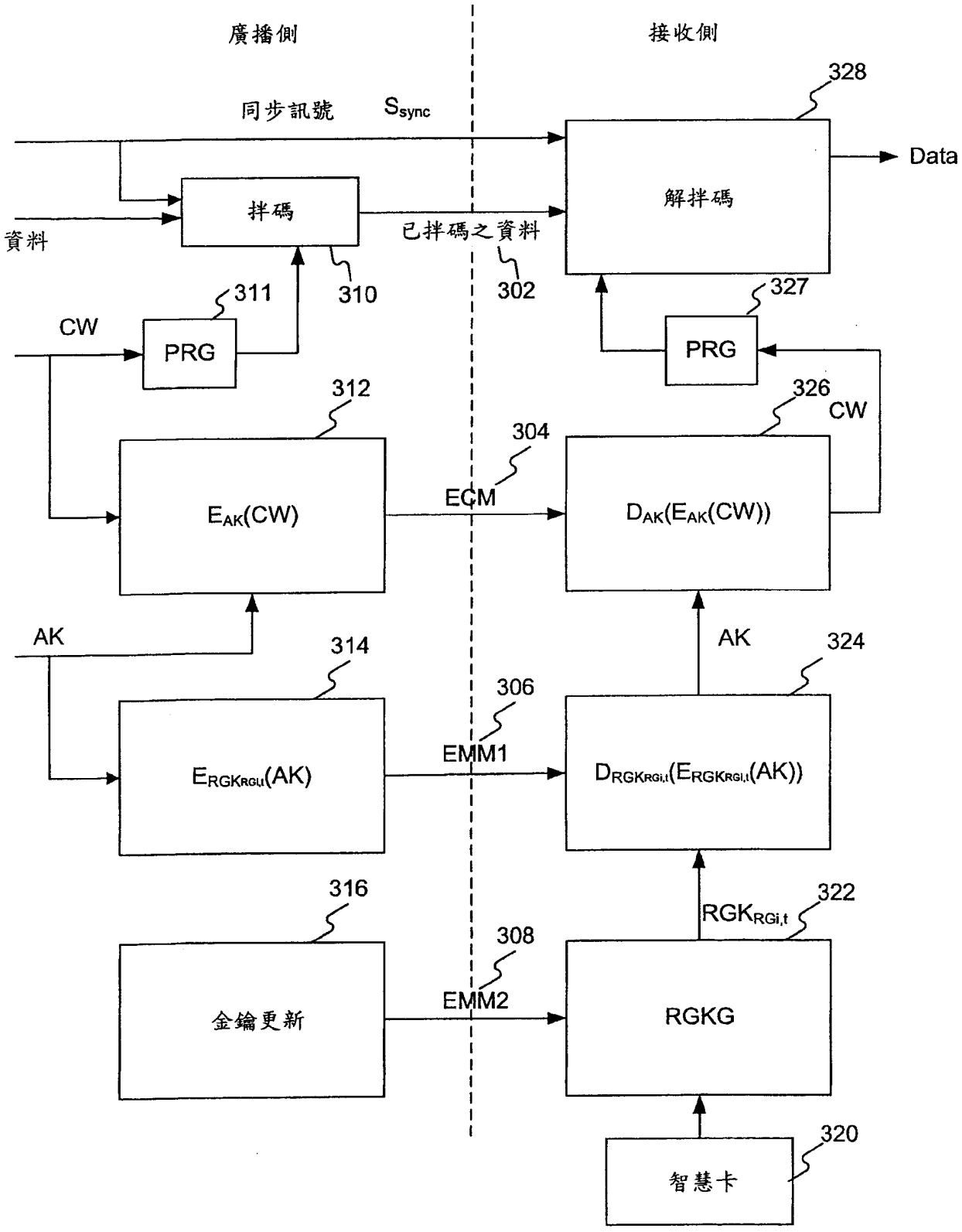

廣播側
接收側
同步訊號 S_{sync}
328
Data
解拌碼
拌碼
資料
已拌碼之資料
310
302
311
CW
PRG
327
PRG
312
326
CW
304
ECM
$E_{AK}(CW)$
$D_{AK}(E_{AK}(CW))$
AK
AK
314
324
306
EMM1
$E_{RGK_{RGi,t}}(AK)$
$D_{RGK_{RGi,t}}(E_{RGK_{RGi,t}}(AK))$
316
322
$RGK_{RGi,t}$
308
EMM2
金鑰更新
RGKG
320
智慧卡

圖 3

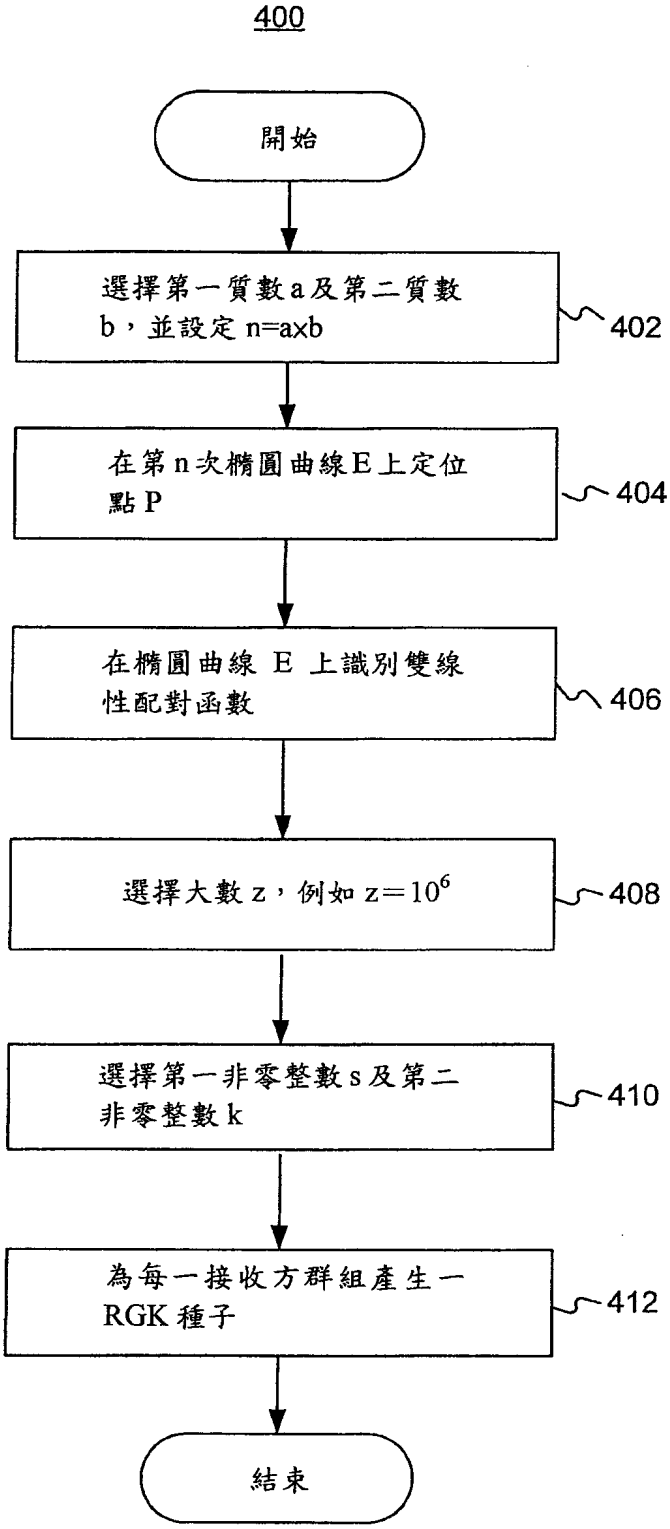

400
開始
選擇第一質數a及第二質數b，並設定 n=axb
402
在第n次橢圓曲線E上定位點P
404
在橢圓曲線 E 上識別雙線性配對函數
406
選擇大數 z，例如 z=10^6
408
選擇第一非零整數s及第二非零整數k
410
為每一接收方群組產生一RGK種子
412
結束

圖4

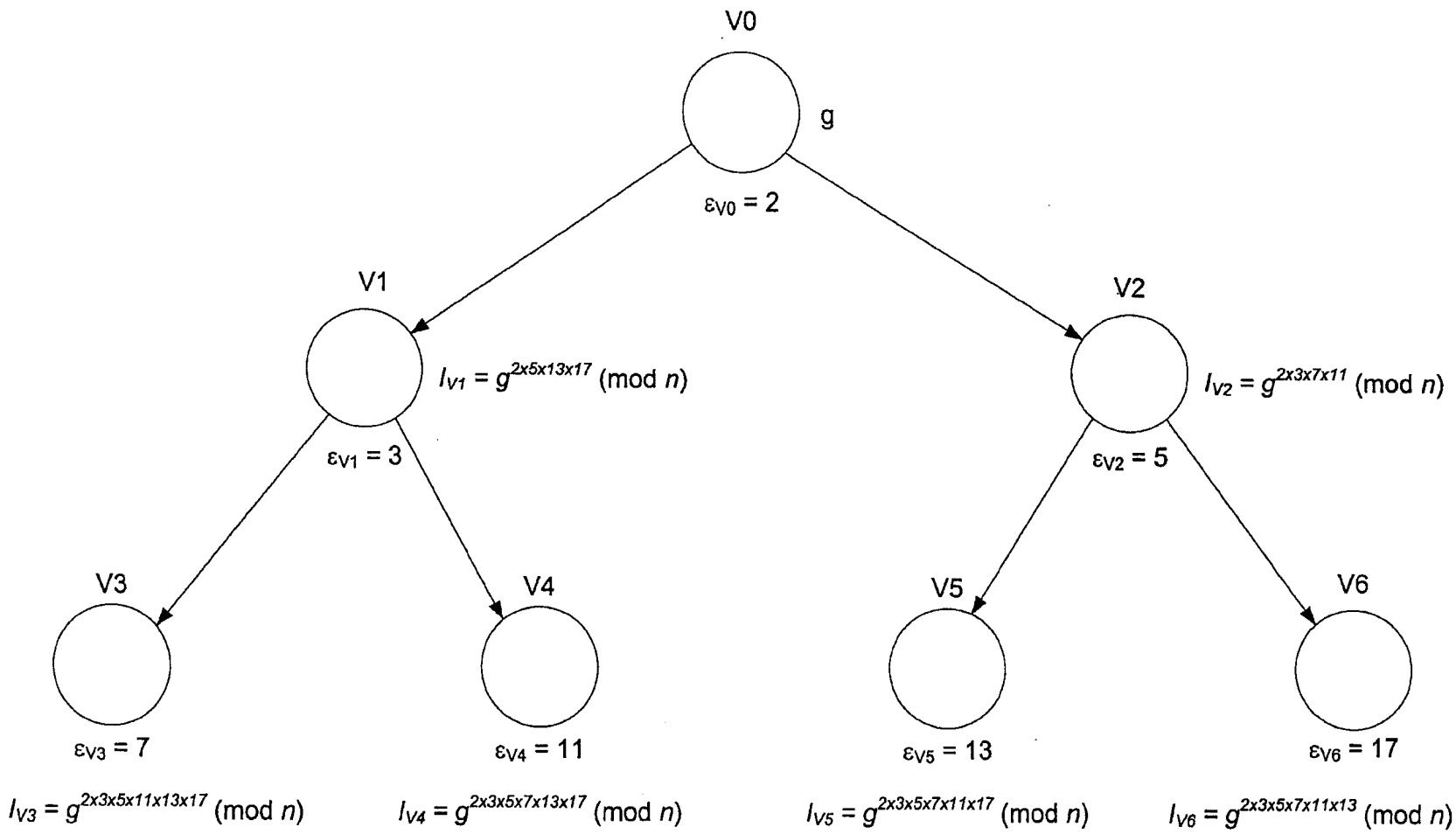

500
V0
g
$\varepsilon_{V0} = 2$
V1
$I_{V1} = g^{2x5x13x17} \pmod{n}$
$\varepsilon_{V1} = 3$
V2
$I_{V2} = g^{2x3x7x11} \pmod{n}$
$\varepsilon_{V2} = 5$
V3
$\varepsilon_{V3} = 7$
V4
$\varepsilon_{V4} = 11$
V5
$\varepsilon_{V5} = 13$
V6
$\varepsilon_{V6} = 17$
$I_{V3} = g^{2x3x5x11x13x17} \pmod{n}$
$I_{V4} = g^{2x3x5x7x13x17} \pmod{n}$
$I_{V5} = g^{2x3x5x7x11x17} \pmod{n}$
$I_{V6} = g^{2x3x5x7x11x13} \pmod{n}$

圖 5

四、指定代表圖：

(一)本案指定代表圖為：圖 3。

(二)本代表圖之元件符號簡單說明：

300：廣播方法

302：已拌碼的資料

304：授權控制訊息（ECM）

306：第一授權管理訊息（EMM1）

308：第二授權管理訊息（EMM2）

310～328：步驟

320：智慧卡

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無