I307594
公告本

發明專利說明書

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：91132578 ※IPC分類：H04L 9/14, H04Q 7/32

※ 申請日期：91.11.5 (2006.01)

壹、發明名稱

（中文）供於一分碼多向近接通信系統中訊息整合之方法及裝置

（英文）METHOD AND APPARATUS FOR MESSAGE INTEGRITY IN A CDMA COMMUNICATION SYSTEM

貳、發明人（共 2 人）

發明人 1 （如發明人超過一人，請填說明書發明人續頁）

姓名：（中文） 羅伊 法蘭克林 奎克 二世

（英文） ROY FRANKLIN QUICK JR.

住居所地址：（中文） 美國加州聖地牙哥市巴賽隆那道 1150 號

（英文） 1150 BARCELONA DRIVE, SAN DIEGO, CALIFORNIA 92107, U.S.A.

國籍：（中文） 美國 （英文） U.S.A

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填說明書申請人續頁）

姓名或名稱：（中文） 美商奎康公司

（英文） QUALCOMM INCORPORATED

住居所或營業所地址：（中文） 美國加州聖地牙哥市摩豪斯大道 5775 號

（英文） 5775 MOREHOUSE DRIVE, SAN DIEGO, CALIFORNIA 92121-1714, U.S.A.

國籍：（中文） 美國 （英文） U.S.A

代表人：（中文） 菲力普 R. 華德渥斯

（英文） PHILIP R. WADSWORTH

發明人 2

姓名：（中文） 賽 尤 當肯 何

（英文） SAI YIU DUNCAN HO

住居所地址：（中文） 美國加州聖地牙哥市小河道 11559 號

（英文） 11559 TRAILBROOK LANE, SAN DIEGO, CA 92128, U.S.A.

國籍：（中文） 加拿大 （英文） CANADA

捌、聲明事項

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：＿＿＿＿＿＿＿＿

☑ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1. 美國；2001/11/05；10/011,964
2.
3.

☑ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1. 美國；2001/11/05；10/011,964
2.
3.
4.
5.
6.
7.
8.
9.
10.

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.
2.
3.

☐ 主張專利法第二十六條微生物：

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1.
2.
3.

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.
2.
3.

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

技術領域

本發明通常係有關於通信領域，而更明確而言，係有關在細胞式通信系統的通信。

先前技術

分碼多向近接(CDMA)通信系統是從早先的一代進化到較高等的一代。在更新系統方面，與系統的各種操作有關的一或多個參數可能改變。在進階系統的行動台亦更新可在新參數中操作。早先一代系統之一是根據在TIA/EIA-95A/B標準中所定義的參數來操作，其中TIA/EIA-95A/B標準在此僅列出供參考。較進階系統之一是根據TIA/EIA-IS-2000-A標準來操作，其中TIA/EIA-IS-2000-A標準在此僅列出供參考。TIA/EIA-IS-2000-A標準的較新版本是在發展，且是在TIA/EIA-IS-2000-B標準下發行，其在此僅列出供參考。標準的副本可透過全球資訊網網址：http://WWW.3gpp2.org或寫信到TIA, Standards and Technology Department, 2500 Wilson Boulevard, Arlington, VA 22201, United States of America獲得。

一通信系統具有許多不同元件。每個元件的工作參數是由對應的標準定義。一系統可透過變更某元件而部份更新，以根據對應標準的較新版本來操作。提議的TIA/EIA-IS-2000-B標準執行與必要特徵之一是在一行動台與一基地台之間提供通信訊息整合。訊息整合是保証訊息寄件者的合法性。若要達成訊息整合，一認證與密鑰協議

(AKA)程序已在標準的相關部份中發展及定義。一認證中心(AC)是一元件，以管理與在系統操作的行動台有關的認證資訊。在一行動交換中心(MSC)與AC之間的一介面工作參數需要從一較早期版本更新，以執行AKA程序。在沒有MSC-AC介面升級，可執行AKA程序的升級行動台與基地台會由於系統缺乏經由MSC-AC介面來運送AKA資訊而不能實際執行AKA程序。結果，不能執行訊息整合。在更新MSC-AC介面之前，當基地台與行動台根據提議的TIA/EIA-IS-2000-B標準來升級操作時，此一情況便會變成一重要配置問題。

為了這個目的，需要一方法及裝置允許較進階一代行動台與基地台來執行訊息整合。

發明內容

在一通信系統中，一方法與裝置的提供是用於訊息整合，而不管在認證中心與一行動交換中心之間的認證中心或一介面的操作版本。方法及裝置包括一細胞式訊息加密演算法(CMEA)密鑰；及根據在一行動台與一基地台之間的訊息整合的CMEA密鑰來產生一CMEA密鑰取得的整合密鑰(CIK)。行動台是將一註冊訊息傳送給基地台，且根據行動台是否從基地台接收一認證向量的接受順序或一元件來決定與基地台通信的認證中心操作版本。如果行動台從基地台接收一有效的註冊接受順序，CIK可根據AMEA密鑰來產生。CIK可透過將CMEA密鑰重複兩次來產生。行動台與基地台是根據分別在通信系統的反向與前向通信的CMEA密

鑰而區域產生CIK。

圖式簡單說明

本發明的特徵、目的、及優點可從下面參考附圖的詳細描述而變得更了解，其中相同參考編號是表示類似元件：

圖1係根據本發明的各種具體實施例來描述操作的通信系統；

圖 2係根據本發明的各種觀點而描述以一資料率來接收及解碼接收資料的一通信系統接收器；

圖3係根據本發明的各種觀點而描述以一排程的資料率來傳送資料封包的一通信系統發射器；

圖4係根據本發明的各種觀點而描述認證與密鑰設定程序；

圖5係根據TIA/EIA-IS-2000-B標準而描述認證與密鑰設定程序；及

圖6係根據本發明的各種觀點而描述一行動台在通信系統中執行訊息整合的處理流程。

實施方式

本發明的各種具體實施例可合併在根據由電信工業協會(TIA)及其他標準組織所發行的各種標準描述及揭示的分碼多向近接(CDMA)技術的無線通信系統操作。圖1係結合本發明各種不同具體實施例，而根據分碼多向近接(CDMA)通信系統標準的任一者的一般通信系統100操作方塊圖。通信系統100可以是語聲音、資料或兩者的通信。通常，通信系統100包括一基地台101，以提供在例如行動台102-104的

許多行動台、及在行動台102-104、與一公眾交換電話與資料網路105之間的通信鏈路。在圖1的行動台可視為資料存取終端機，且基地台可視為資料存取網路，而不致於違背本發明的主要範圍與各種優點。基地台101包括許多元件，例如一基地台控制器及一基地收發器系統。為了簡化，此元件並未顯示。基地台101亦與例如基地台160的其他基地台通信。耦合到基地台101和160的一MSC 199可控制通信系統 100的各種操作觀點。一AC 198能與MSC 199通信，以執行在系統100提供的認證服務管理。在AC 198與MSC 199之間的一介面197是提供與認證處理有關的相關資訊通信的通信媒體。

基地台101在它的涵蓋能經由從基地台101傳送的一前向鏈路信號而與每個行動台通信。提供給行動台102-104的前向鏈路信號可匯整形成一前向鏈路信號106。用以接收前向鏈路信號106的該等行動台102-104的每一者可解碼前向鏈路信號106，以擷取提供給使用者的資訊。基地台160亦經由一前向鏈路信號而與在它涵蓋區域的行動台相通信。行動台102-104是經由對應的反向鏈路而與基地台101和160通信。每個反向鏈路是透過相對行動台102-104的例如反向鏈路信號107、109的一反向鏈路信號來維繫。

圖2係描述用於處理及解調變該接收CDMA信號的一接收器200方塊圖。接收器200可用於解碼在反向與前向鏈路信號上的資訊。接收(Rx)的取樣可儲存在RAM 204。接收取樣是透過一無線電頻率/中頻(RF/IF)系統290與一天線系

(5)

統292產生。RF/IF系統290與天線系統292包括：一或多個元件，用以接收多重信號；及接收信號的RF/IF處理，以接收不同增益。多工接收信號是來自經由不同傳遞路徑來傳遞的一共通來源。天線系統292可接收RF信號，且將RF信號傳遞給RF/IF系統290。RF/IF系統290可以是任何傳統RF/IF接收器。接收的 RF信號可被濾波、向下轉換與數位化，以便在基帶頻率上形成RX取樣。取樣是供應給一解多工器(demux)202。解多工器202的輸出是供應給一搜尋器單元206與指狀物元件208。一控制單元210是耦合到那裡。一組合器212是將一解碼器214耦合到指狀物元件208。控制單元210可以是由軟體控制的一微處理器，且可位於相同的積體電路或在一分開的積體電路上。在解碼器 214的解碼功能是根據一渦輪解碼器或任何其他適當演算法。

在操作期間，接收取樣是供應給解多工器202。解多工器202是將取樣供應給搜尋器單元206與指狀物元件208。控制單元210是建構指狀物元件208，以便在不同時間偏移上根據來自搜尋器單元206的搜尋結果來執行接收信號的解調變與解展佈。解調變的結果會組合及傳遞給解碼器 214。解碼器214是將資料解碼，及輸出解碼的資料。解碼處理包括將該接收資料解密的處理。通道的解展佈時常使用一整合與傾印累加器電路(未在圖顯示)可透過將接收的取樣乘以PN 序列的組成結合，及在單一時序假設性的指定Walsh函數，及數位濾波結果取樣而執行。此一技術在技藝中是普遍已知的。

圖3係描述用以傳送反向與前向鏈路信號的一發射器300方塊圖。用以傳輸的路由通道資料是輸入調變的調變器301。調變是根據例如QAM、PSK或BPSK的 任何普遍已知的調變技術。資料是以在調變器301的一資料率來編碼。調變器301的輸入資料包括用以執行訊息整合的資料。資料率是經由一資料率與功率位準選擇器303選取。對於反向鏈路信號而言，資料率選擇是根據來自一接收基地台的回授資訊。因此，資料率與功率位準選擇器303可選取調變器301的資料率。調變器301的輸出是藉由一信號展佈操作來傳遞，及在一方塊302中放大，以便從天線304傳送。一導頻信號亦在方塊307產生。導頻信號是放大到一適當位準方塊307。導頻信號功率位準是根據在一接收基地台上的通道狀況。導頻信號是與在一組合器308的路由通道信號組合。組合的信號是在一放大器309放大，並且從天線304傳送。天線304 可以是包括天線陣列與多重輸入多重輸出建構的任何組合數量。資料率與功率位準選擇器303亦根據回授資訊來選取傳輸信號放大位準的功率位準。選取的資料率與功率位準的組合允許在接收基地台上將傳送的資料適當解碼。

行動台102是從基地台101的涵蓋區域漫遊到基地台160的涵蓋區域。行動台能與基地台101和160進行一軟交遞處理。交遞處理是普遍已知的。行動台102可透過從基地台160接收前向鏈路信號161來持續使用通信服務，並且傳送該反向鏈路信號117。AC 198是用來認證及提供在一行動台與基

台亦使用行動台而根據訊息整合 CMEA密鑰來產生相同的CIK。基地台是根據認證反應訊息393而將一註冊接受順序395傳送給行動台。註冊接受順序395是包括一訊息認證碼(MAC)。MAC的值是根據在基地台所產生的CIK。產生的CIK是處理器的輸入使用，以根據一預先定義的功能來產生MAC。同樣地，根據他本身產生CIK的行動台可確認用以傳送註冊接受順序395的基地台合法。在此點之後，在行動台與基地台之間一般通信396是根據一已知的加密演算法而經由CCK來加密。而且，在基地台與行動台之間的一般通信396根據在基地台與行動台上產生的CIK係包括訊息整合檢查。因此，訊息整合特徵是提供用於在行動台與基地台之間的通信，而不需要AC 198來操作除了在TIA/EIA-IS-2000A標準中定義的操作之外。

請即參考在圖5描述的訊息流程400，其係顯示認證與加密的訊息流程。基地台與行動台是根據提議的TIA/EIA-IS-2000-B標準來操作。AC 198是根據提議的TIA/EIA-IS-2000-B標準中定義的相關標準來操作。MSC-AC介面197亦根據標準ANSI-41的相關部份來更新，以允許如TIA/EIA-IS-2000-B標準所定義的認證參數的通信。訊息流400是使用在一行動台、一基地台與AC 198之間。基地台是將一任意存取數目(RAND)訊息421廣播給所有行動台。行動台是使用RAND來產生一註冊訊息401。基地台然後將一認證請求訊息408傳送給AC 198。AC 198然後傳送一認證反應訊息402。訊息402是根據TIA/EIA-IS-2000-B來

運送一組認證向量(AV)。每個AV包含用於認證的許多元件，包括整合密鑰(IK)與密碼密鑰(CK)。基地台係選取認證向量之一，及在一認證請求訊息403上將選取AV 的一些元件傳送給行動台。AV的元件是根據在AC 198保持的一根密鑰來產生。相同的根密鑰亦儲存在行動台。行動台會內部檢查通信的AV 元件是否符合根據儲存的根密鑰產生的AV元件。如果符合，行動台便有效認證基地台。根據根密鑰與通信的AV元件，行動台可經由內部訊息405而區域性產生IK和CK。行動台亦根據通信的AV元件來產生一使用者反應(RES)。行動台然後將在一認證反應404中的RES傳送給基地台。基地台亦經由內部訊息406而區域性產生IK和CK。基地台是將接收的RES與預期的RES相比較。如果一符合存在，基地台便有效認證行動台。此時，通信407可根據TIA/EA-IS-2000-B標準來執行訊息整合與加密。

本發明的各種觀點允許從認證處理產生的CMEA密鑰當作執行訊息整合的整合密鑰使用。既然行動台可漫遊到基地台根據提議TIA/EIA/IS-2000-B標準操作的系統，但是具有AC 198 或 MSC-AC介面197的不同版本，行動台沒有方法預先知道AC 198或MSC-AC介面197的版本已合併在系統。更明確而言，如果根據提議TIA/EIA-IS-2000-B標準操作的一行動台與一基地台是與通信系統100通訊，而AC 198是根據TIA/EIA-IS-95-B或TIA/EIA-IS-2000-A操作，及/或MSC-AC介面197是據與TIA/EIA-IS-95-B或TIA/EIA-IS-2000-A有關的ANSI-41來操作，行動台便會拒絕與基地台

的通信，因為缺乏訊息整合特徵。因此，在不增加複雜度原則下，行動台需要一方法及裝置來區別那個AC 198或MSC-AC介面197版本已合併在系統。

請即參考圖6，一流程圖600係描述一演算法，以允許行動台來建立與基地台的一訊息整合密鑰，及執行認證，而不管AC 198 或MSC- AC介面197版本。在步驟601，行動台可或未認證。在步驟602，假設AC 198是根據TIA/EIA-IS-95B或TIA/EIA-IS-2000-A來操作，行動台是將一註冊訊息392傳送給基地台，並且計算CMEA密鑰，及經由內部訊息397 和398來產生CIK和CCK。如果行動台經由一成功的認證處理，行動台便具有一整合密鑰CIK或IK，其是因認證的要式而定。在此情況，註冊訊息的訊息認證碼(MAC)是包括在註冊訊息。MAC 的出現允許基地台來執行與行動台的區域認證，以減少網路的認證相關路由。行動台是預期從基地台來接收一註冊接受順序395。在步驟603，行動台可決定AC 198或MSC-AC介面197是否根據TIA/EIA -IS-95B與TIA/EIA-IS-2000-A或TIA/EIA-IS-2000-B來操作。根據TIA/EIA-IS-95B與TIA/EIA-IS-2000-A的認證可視為2G認證。根據TIA/EIA-IS-2000-B的認證可視為3G 認證。一計時器可用來限制在此一模式的行動台停留的時間量。如果計時器是在步驟604屆滿，處理會在步驟602開始，除非行動台具有整合密鑰，在此情況，行動台是直接移到步驟606。如果行動台從基地台接收註冊接受順序395，AC 198與MSC-AC介面197可根據2G 認證程序來操作。在步驟605的

處理會移到步驟606。在步驟606，行動台是使用產生的CMEA密鑰而經由內部訊息397和398來取得CIK和CCK，以便在與基地台的共同通道上執行有關通信的訊息整合與加密。如果行動台是從基地台接收一認證請求訊息403，AC 198或MSC-AC介面197便會根據3G認證程序來操作。同樣地，在步驟605的處理流程會移到步驟607，以丟棄產生的CMEA密鑰及任何未決定的CIK和CCK，而且產生IK和CK。在步驟607的處理包括一或多個步驟。在步驟608，IK和CK是經由內部訊息405產生。在步驟609和610，認證是使用連同一計時器使用的基地台來確認，以避免行動台長時間保持在此一模式。在步驟611，行動台是建立訊息整合與加密的IK和CK。在步驟612，行動台是使用基地台來保持訊息整合與加密的一正確組的參數。處理可於行動台需要執行註冊的每次來重複。

在技藝中熟諳此計者可進一步了解到在此揭示具體實施例的各種說明邏輯方塊、模組、電路、與演算法能以電子硬體、電腦軟體、或組合實施。為了要清楚描述硬體與軟體的互換性，上面各種說明的元件、方塊、模組、電路、與步驟是從他們功能觀點來描述。此功能是否以硬體或軟體實施是因特殊應用與設計是強諸在整個系統上。熟諳此技者能以每個特殊應用的不同方式來實施描述的功能，但是此實施決定應不視為違背本發明的範圍。

在此揭示具體實施例中描述的各種說明邏輯方塊、模組、與電路能以一般目的處理器、一數位信號處理器(DSP)

、一應用特殊積體電路(ASIC)、一場可程式閘陣列(FPGA)或其他可程式邏輯裝置、非連續閘或電晶體邏輯、非連續硬體元件、或任何組合來實施或執行在此描述的功能。一般目的處理器可以是一微處理器；或者，處理器可以是任何傳統處理器、控制器、微控制器、或狀態機器。一處理器亦能以計算裝置的組合實施，例如，一DSP與一微處理器、複數個微處理器、一或多個微處理器連同一DSP核心、或任何其他此結構的組合。

在此揭示具體實施例中描述的方法或演算法的步驟能以硬體、一處理器執行的軟體模組、或組合來直接具體實施。一軟體模組可在RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、一可移除磁碟、光碟、或在技藝中已知的任何其他形式的儲存媒體。一儲存媒體係耦合到處理器，以致於處理器可從儲存媒體讀取資訊，及將資訊寫到儲存媒體。或者，儲存媒體對於處理器是必需的。處理器與儲存媒體是在ASIC。ASIC是在一使用者終端機。或者，處理器與儲存媒體可當作在使用者終端機的非連續元件。

較佳具體實施例的先前描述的提供是允許在技藝中熟諳此技者製造或使用本發明。這些具體實施例的各種修改對於在技藝中熟諳此技者是顯然的，且在此定義的一般原理可運用在其他具體實施例，而無需使用創作性設施。因此，本發明並未侷限於在此顯示的具體實施例，而是符合在此揭示的一般原理與新特徵的廣泛範圍。

圖式代表符號說明

100	通信系統
101	基地台
102-104	行動台
105	公眾交換電話機資料網路
106	前向鏈路信號
107-109	反向鏈路信號
117	反向鏈路信號
160	基地台
161	前向鏈路信號
197	介面
198	認證中心
199	行動交換中心
200	接收器
202	解多工器
204	隨機存取記憶體
206	搜尋器單元
208	指狀物元件
210	控制單元
212,308	組合器
214	解碼器
290	射頻/中頻系統
292,304	天線
300	發射器

301	調變器
302,307	方塊
303	資料率與功率位準選擇器
309	放大器
380,405,406	內部訊息
391	隨機存取數
392,401	認證訊息
393,403	認證請求訊息
394	細胞式訊息加密演算法密鑰
395	註冊接受程序
399,400	訊息流程
402	認證反應訊息
404	認證反應
407	通信
600	流程圖
600-612	步驟

肆、中文發明摘要

一種在通信系統(100)中用以提供訊息整合之方法及裝置，而不管在認證中心(198)與一行動交換中心(199)之間的認證中心(198)或介面(197)操作版本。該方法及裝置包括：產生一細胞式訊息加密演算法(CMEA)密鑰；及根據在一行動台與一基地台之間訊息整合的CMEA密鑰來產生一CMEA密鑰取得的整合密鑰(CIK)。該行動台是將一註冊訊息傳送給該基地台，且根據該行動台是否從該基地台接收一認證向量的註冊接收順序或一些元件來決定與基地台通信的認證中心(198)的操作版本。如果該行動台從基地台接收一有效註冊接受順序，該CIK便能根據該CMEA密鑰產生。

伍、英文發明摘要

In a communication system (100), a method and apparatus provides for message integrity regardless of the operating version of an authentication center (198) or an interface (197) between the authentication center (198) and a mobile switching center (199). The method and apparatus include generating a cellular message encryption algorithm (CMEA) key, and generating a CMEA-key-derived integrity key (CIK) based on the CMEA key for message integrity between a mobile station and a base station. The mobile station transmits a registration message to the base station, and determines an operating version of the authentication center (198) in communication with the base station based on whether the mobile station receives a registration accepted order or some elements of an authentication vector from the base station. The CIK is generated based on the CMEA key, if the mobile station receives a valid registration accepted order from the base station.

拾、申請專利範圍

1. 一種用於通信系統之方法，其包含：

用以產生一細胞式訊息加密演算法(CMEA)密鑰；及

根據在一行動台與一基地台之間訊息整合的該CMEA密鑰來產生一CMEA密鑰取得的的整合密鑰(CIK)。

2. 如申請專利範圍第1項之方法，其中該產生該CIK包括重複該CMEA密鑰兩次，以產生該CIK。

3. 如申請專利範圍第1項之方法，其中該行動台與該基地台是根據分別在該通信系統的反向與前向通信的該CMEA密鑰而區域執行該產生該CIK。

4. 一種用於通信系統之裝置，其包含：

產生裝置，用以產生一細胞式訊息加密演算法(CMEA)密鑰；及

產生裝置，其可根據在一行動台與一基地台之間訊息整合的該CMEA密鑰來產生一CMEA密鑰取得的整合密鑰(CIK)。

5. 如申請專利範圍第4項之裝置，其中該用以產生該CIK的裝置包括將該CMEA密鑰重複兩次的裝置，以產生該CIK。

6. 如申請專利範圍第4項之裝置，其中該行動台與該基地台包括執行裝置，用以根據分別反向與前向通信的該CMEA密鑰來區域執行該產生該CIK。

7. 一種用於通信系統之處理器，其包含：

產生裝置，用以產生一細胞式訊息加密演算法(CMEA)

密鑰；及

產生裝置，其可根據在該通信系統中的一行動台與一基地台之間的訊息整合的該CMEA密鑰來產生一CMEA密鑰取得的整合密鑰(CIK)。

8. 如申請專利範圍第7項之處理器，其中該用以產生該CIK的裝置包括重複裝置，用以將該CMEA密鑰重複兩次來產生該CIK。

9. 一種用於行動台之方法，其包含：

將一註冊訊息傳送給一基地台；及

根據該行動台是否從該基地台接收一註冊接收順序或一認證向量的元件來決定與該基地台通信的一認證中心作業版本。

10. 如申請專利範圍第9項之方法，其進一步包含：

產生一細胞式訊息加密演算法(CMEA)密鑰；及

如果該行動台從該基地台接收該註冊接受的順序，可根據在該行動台與一基地台之間訊息整合的該CMEA密鑰來產生一CMEA密鑰取得的整合密鑰(CIK)。

11. 如申請專利範圍第10項之方法，其中該產生該CIK包括將該CMEA密鑰重複兩次，以產生該CIK。

12. 如申請專利範圍第10項之方法，其中該行動台與該基地台是根據分別在通信系統中的反向與向前通信的該CMEA密鑰來區域執行該產生該CIK。

13. 如申請專利範圍第10項之方法，其進一步包含：

根據該CIK來產生一訊息認證碼(MAC)；及

使用該行動台的該註冊接受順序通信的該MAC來確認該基地台的合法性。

拾壹、圖式

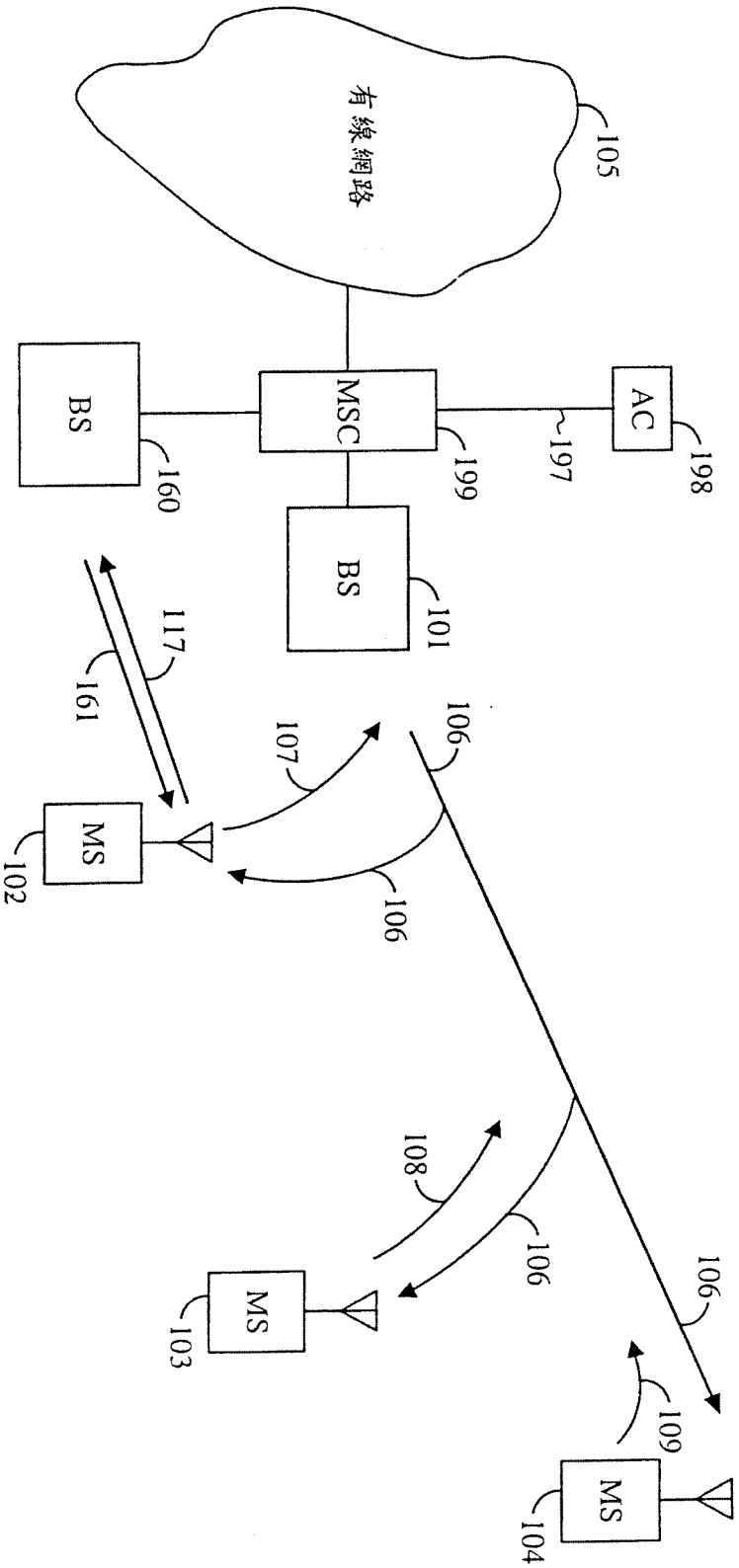
100
有線網路
105
BS
160
MSC
199
197
AC
198
BS
101
117
161
107
106
MS
102
106
108
MS
103
106
109
MS
104

圖 1

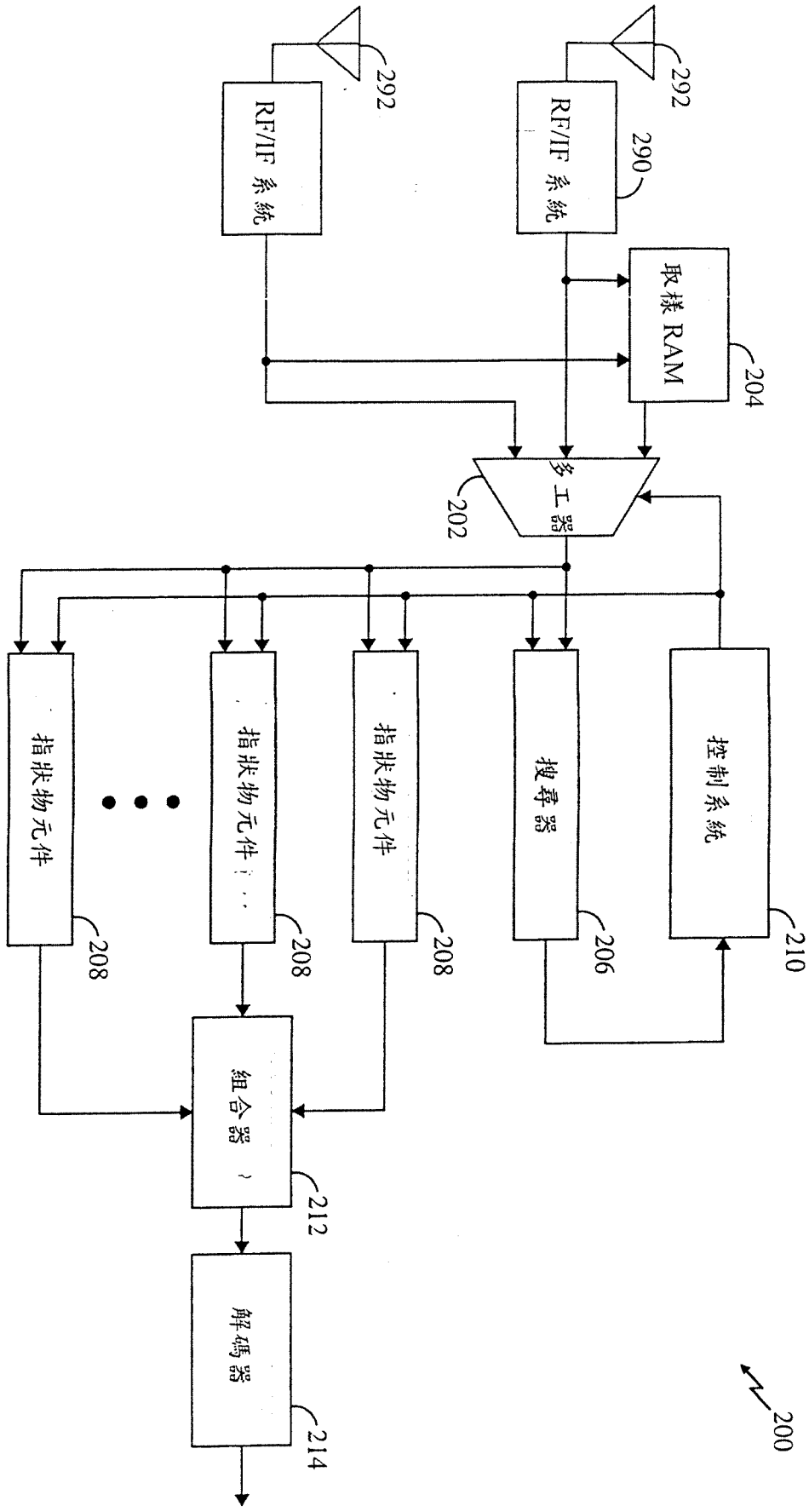
292
RF/IF 系統
290
292
RF/IF 系統
取樣 RAM
204
多工器
202
指狀物元件
208
指狀物元件
208
指狀物元件
208
搜尋器
206
控制系統
210
組合器
212
解碼器
214
200

圖 2

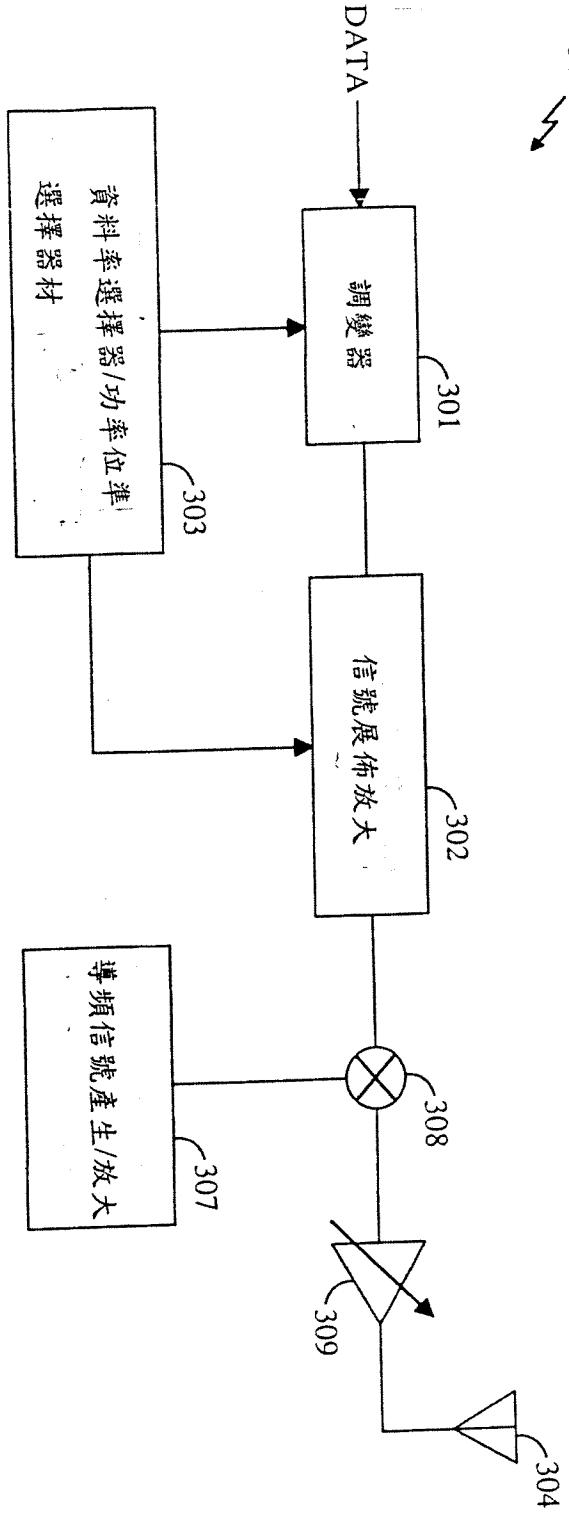
300
DATA
調變器
301
資料率選擇器/功率位準選擇器材
303
信號展佈放大
302
導頻信號產生/放大
307
308
309
304

圖 3

圖式續頁

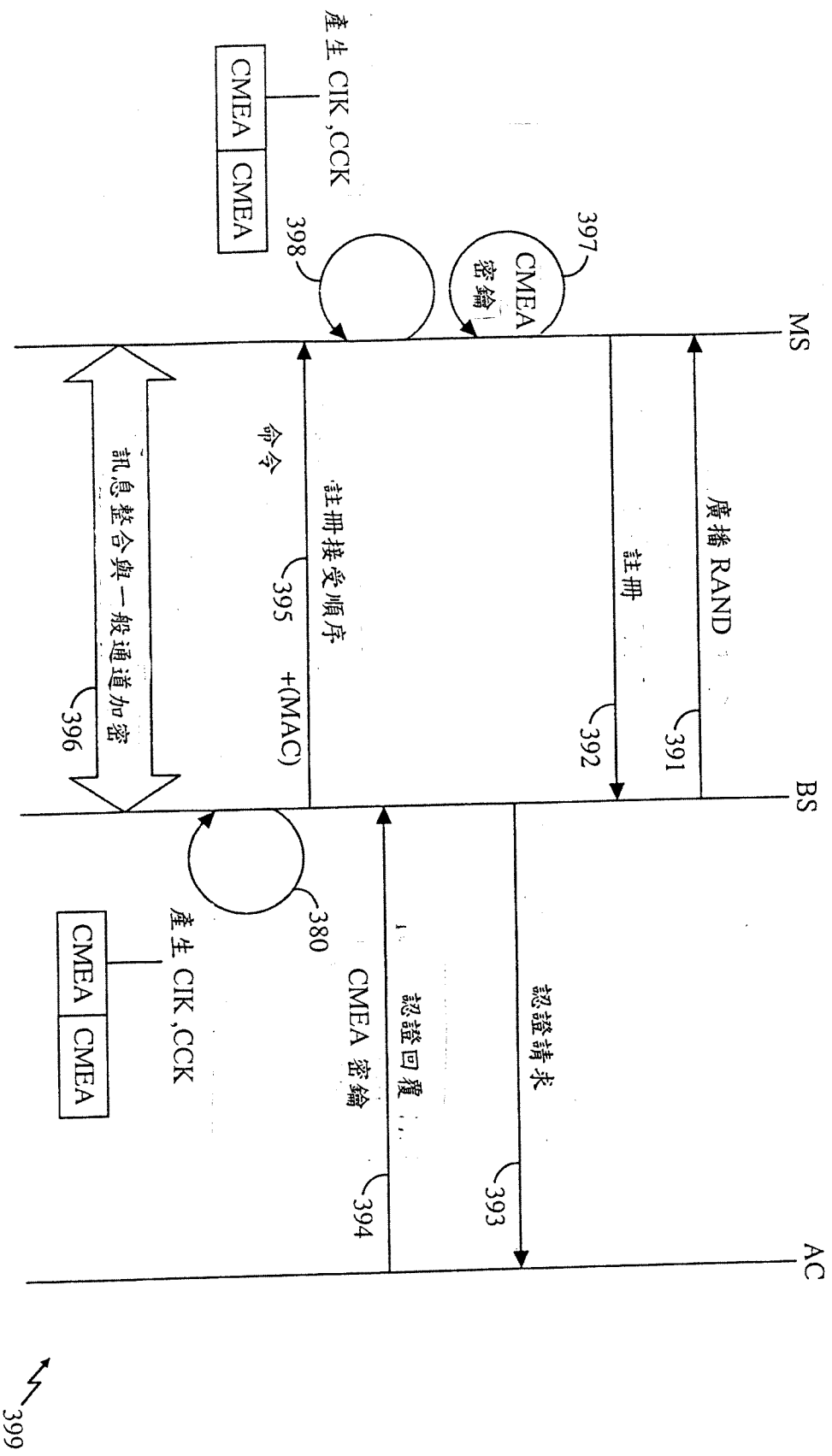
MS
BS
AC
廣播 RAND
391
註冊
392
認證請求
393
CMEA 密鑰
394
認證回覆
CMEA 密鑰
397
產生 CIK ,CCK
CMEA
CMEA
398
註冊接受順序
命令
395
+(MAC)
訊息整合與一般通道加密
396
產生 CIK ,CCK
CMEA
CMEA
380
399

圖 4

圖式續頁

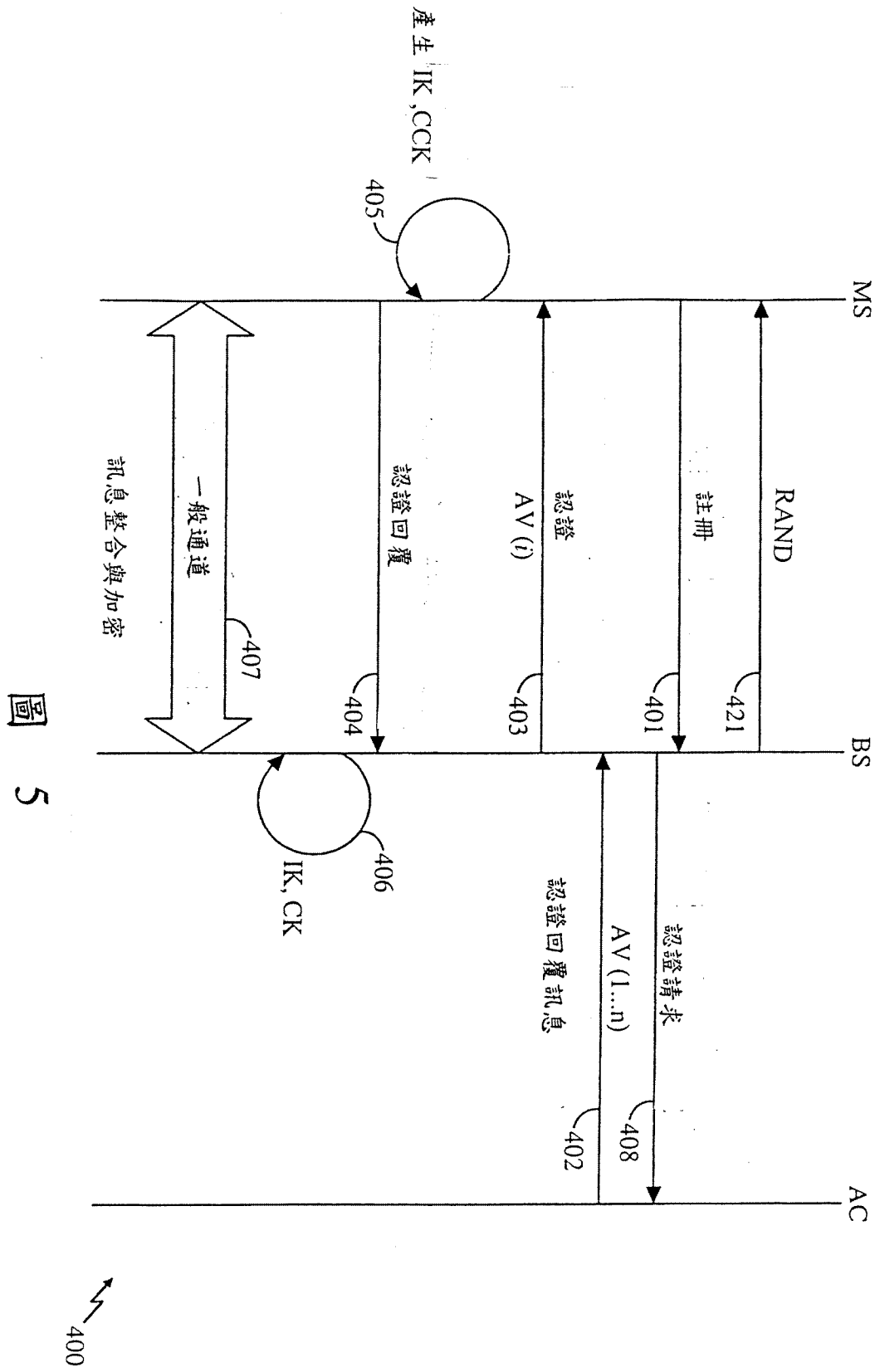
MS
BS
AC
RAND
421
註冊
401
認證
AV (i)
403
認證回覆
404
一般通道
407
訊息整合與加密
產生 IK ,CCK
405
IK, CK
406
認證回覆訊息
AV (1...n)
402
認證請求
408
400

圖 5

圖式續頁

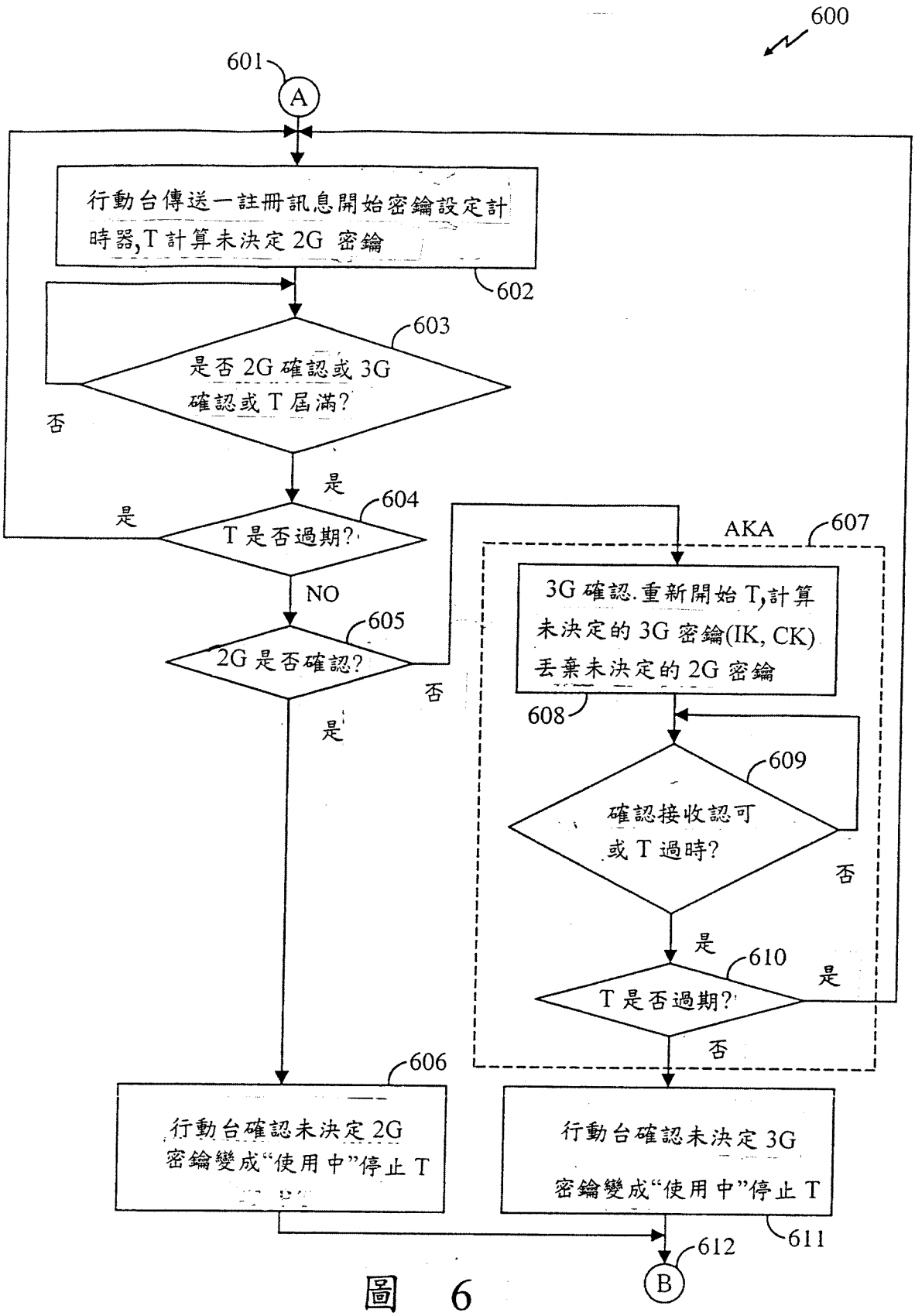
600
601
A
行動台傳送一註冊訊息開始密鑰設定計時器,T 計算未決定 2G 密鑰
602
603
是否 2G 確認或 3G 確認或 T 屆滿?
否
是
是
604
T 是否過期?
NO
605
2G 是否確認?
否
是
AKA
607
3G 確認.重新開始 T,計算未決定的 3G 密鑰(IK, CK) 丟棄未決定的 2G 密鑰
608
609
確認接收認可或 T 過時?
否
是
610
T 是否過期?
是
否
606
行動台確認未決定 2G 密鑰變成"使用中"停止 T
行動台確認未決定 3G 密鑰變成"使用中"停止 T
611
612
B

圖 6

陸、(一)、本案指定代表圖為：第 1 圖

(二)、本代表圖之元件代表符號簡單說明：

100	通信系統
101	基地台
102-104	行動台
105	公眾交換電話及資料網路
106	前向鏈路信號
107-109	反向鏈路信號
117	反向鏈路信號
160	基地台
161	前向鏈路信號
197	介面
198	認證中心
199	行動交換中心

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

地台101和160任一者之間的一安全通信的加密密鑰。

請即參考在圖4描述的訊息流程399，用以認證及加密的訊息流是根據本發明的各種觀點顯示。在訊息流程399中包括的基地台與行動台是根據提議的TIA/EIA-IS-2000-B標準來操作。在此情況，AC 198並未根據在提議TIA/EIA-IS-2000-B標準中的標準相關選擇來更新操作。在AC 198與MSC 199之間的介面並未更新符合ANSI-41標準操作，ANSI-41標準在此僅列出供參考，且該ANSI-41標準是與TIA/EIA-IS-2000-B略述的訊息整合與加密操作有關。基地台傳播一隨機存取數(RAND)訊息391至所有行動台，該基地台是使用RAND來產生一註冊訊息392。基地台是在一認證請求訊息393上經由MSC-AC介面197來通信由註冊訊息運送給AC 198的認證資訊。AC 198是在內部將在認證請求訊息中的認證資訊與一預期值相比較，確定行動台的認證，及產生一認證反應訊息來運送細胞式訊息加密演算法密鑰(CMEA密鑰)394。CMEA密鑰的產生允許在行動台與基地台之間的加密通信。在行動台，相同CMEA密鑰是亦透過內部訊息397產生。行動台是根據區域性產生的CMEA密鑰而透過內部訊息398來區域性產生一CMEA密鑰取得的密碼密鑰(CCK)。CCK是用於加密。根據本發明的一具體實施例，行動台亦基地台來產生一CMEA密鑰取得的整合密鑰(CIK)，用以執行訊息整合。CIK可根據CMEA密鑰。CMEA密鑰會被重複兩次，以根據本發明的一具體實施例來產生CIK。基地台亦透過內部訊息380來區域性產生CCK。基地