一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
美國 US	2003/05/13	10/249,851	有

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張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

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

發明所屬之技術領域

本發明有關於無線通信，更明確地說，是有關當執行無線接取技術間交接(Inter Radio Access Technology Handover; Inter-RAT Handover)的程序時，3GPP系統中安全服務的處理方法。

先前技術

在此本說明書引述第三代合作計畫(3rd Generation Partnership Project；3GPP)規格書之3GPP TS 25.331 V3.13.0(2002-12)"無線資源控制層協定規格(Radio Resource Control (RRC) Protocol Specification)"與3GPP TS 33.102 V3.12.0(2002-06)"安全結構 (Security architecture)"來作為全球行動通信系統(Universal Mobile Telecommunications System；UMTS)與其相關之安全規約之技術性參考文獻。UMTS描述了一個稱為使用者設備(User Equipment；UE)的裝置(通常為行動裝置)，其在無線通信環境中，與一個或數個基地台相通訊。這些基地台(也就是所謂的Node Bs)與其對應的無線網路控制器(Radio Network Controllers；RNCs)被統稱為UMTS地面無線接取網路(UMTS Terrestrial Radio Access Network；UTRAN)。一般站在安全性的觀點上，在UE和UTRAN端相互對應實體的無線資源控制(RRC)層間會建立一至多個無線接取鏈路(radio access links)，再以RRC規約資料單元(Protocol Data Units; PDUs)經由所建立的無線接取鏈路交換信號與用戶資料。下文相關技術背景的

五、發明說明 (2)

簡述出自於先前提到的3GPP TS 33.102文件，這裡假設讀者對3GPP的規約已有一定的熟悉度。

請參閱第1圖，第1圖說明利用完整演算法(integrity algorithm)f9鑑定傳信訊息的資料完整性。f9演算法的輸入參數包括一完整鑰匙(IK)、一完整序列號碼(COUNT-I)、網路端產生的一隨機值(FRESH)、一方向位元(DIRECTION)、以及包含在RRC PDU內的傳信訊息資料(MESSAGE)。根據這些輸入參數，無線設備使用完整演算法f9計算出一確證密碼(MAC-I)以確定資料的完整性。於是當訊息在無線接取鏈路上傳送時，MAC-I會附加在所對應的傳信訊息上。接收端(Receiver)以相同於傳送端(Sender)計算MAC-I之方法，從接收到的傳信訊息計算一確認密碼XMAC-I。接收端依據比較計算出的XMAC-I密碼和所接收到的MAC-I密碼，以確認所傳遞之傳信訊息的資料完整性。

請參閱第2圖，第2圖係第1圖中描述到的完整序列號碼(COUNT-I)之資料結構方塊圖。完整序列號碼有32位元，係由兩個部分構成的：一"短"序列號碼及一"長"序列號碼。短序列號碼構成完整序列號碼的低效位位元，而長序列號碼構成完整序列號碼的高效位位元。短序列號碼係出現於每一RRC PDU裡的4位元RRC序列碼(RRC SN)。長序列號碼則係28位元的RRC超碼框號碼(RRC Hyper Frame Number; RRC HFN)，係隨著RRC SN的週期循序增加。也就係當偵查到RRC PDU中RRC SN循環一圈時，RRC層即把RRC

五、發明說明 (3)

HFN值加一。雖然RRC SN係與RRC PDU一起傳遞的，RRC HFN卻不被傳遞，而係被保留在無線裝置與UTRAN中各自的RRC層內。

按照上述3Gpp TS 33.102文件所敘述之第6.4.8節，RRC層以一稱為開始值(START)的參數作為RRC HFN的初始值。UE以及UE所分配到的RNC將RRC HFN中最高有效位的20個位元設成此開始值，而RRC HFN中剩下的其他位元則設為零。

請參閱第3圖，第3圖描述在無線接取鏈路上，將用戶及訊號資料譯成密碼。如同先前所述之資料完整性的檢驗，此加密計算演算法（ciphering algorithm）f8的輸入參數有密碼鑰匙(CK)、隨時間改變的密碼序列號碼(COUNT-C)、負載識別(BEARER)、傳輸方向位元(DIRECTION)、以及串流所需之長度值(LENGTH)。藉著這些輸入參數，f8演算法產生出一輸出串流塊(KEYSTREAM BLOCK)，用來將一輸入純文字塊(PLAINTEXT BLOCK)譯成密碼，製造出加過密的輸出密碼文字塊(CIPHERTEXT BLOCK)。這裡輸入參數中的長度值只會影響輸出串流塊的長度，而不會影響輸出串流塊真正的位元值。

密碼序列號碼(COUNT-C)的長度為32位元。不論係用無線鏈路控制(RLC)中的回應模式(acknowledged mode；AM)或是RLC中的無須回應模式(unacknowledged mode；UM)的連線，每一個上傳及下傳無線電負載(radio bearers)都分別有一個密碼序列號碼(COUNT-C)。RLC層係

五、發明說明 (4)

在RRC層之下，也可以被想作係第二層的通信介面。所有透明模式(transparent mode；TM)裡，屬於同一核心網路領域內的RLC無線電負載之密碼序列號碼(COUNT-C)都係相同的，而且在TM連線中不論上傳或下傳，密碼序列號碼(COUNT-C)也係相同。

請參閱第4圖，第4圖係第3圖中密碼序列號碼(COUNT-C)在所有不同連線模式下的方塊示意圖。密碼序列號碼係由兩個部分構成的：一"短"序列號碼及一"長"序列號碼。短序列號碼構成密碼序列號碼的低效位位元，而長序列號碼構成密碼序列號碼的高效位位元。下文描述了依照傳輸模式來更新密碼序列號碼的方法。

-對使在專用通道(dedicated channel；DCH)上的RLC TM而言，短序列號碼係密碼序列號碼裡8位元的連線框號碼(connection frame number；CFN)，係獨立保存在UE與服務無線電網路控制器(serving RNC；SRNC)裡各自的MAC-d實體。SRNC係UE分配到的RNC，UE藉由SRNC與網路通信。長序列號碼係隨每一個CFN週期而增加的24位元MAC-d HFN。

-對RLC UM模式而言，短序列號碼係從RLC UM PDU標頭(header)中得到的7位元的RLC序列號碼(RLC SN)。長序列號碼則係隨每一個RLC SN週期而增加的25位元RLC UM HFN。從定義上來看，RLC HFNs與RRC HFNs是很相似的，差別在於前者是保存在無線裝置(UE與RNC兩端)的RLC層內，而後者則是在RRC層內。

五、發明說明 (5)

－對RLC AM模式而言，短序列號碼係由RLC AM PDU標頭中得到的12位元RLC序列號碼(RLC SN)。長序列號碼則係隨每一個RLC SN週期而增加的20位元RLC AM HFN。

在3GPP TS 33.102規格中第6.4.8節中提到，上述超碼框號碼(HFNs)的初始值來自一稱為開始值的參數。UE及RNC以此開始值作為RLC AM HFN、RLC UM HFN、以及MAC-d HFN之初始值中最高有效位的20個位元，剩下的其他位元則被設為零。

用來產生密碼/完整鑰匙(cipher/integrity keys)的確證(Authentication)和鑰匙協定(Key agreement)程序並非在每次建立通話連線時都會執行，所以有可能發生無限制且惡意的不斷重複使用妥協好的鑰匙之情況。這時需要一種機制來確定特定的一副密碼/完整鑰匙不被無限制的重複使用，以防止利用妥協好的鑰匙來侵入該系統。USIM係UE裡面的非揮發性記憶體，於是含有一機制用以限制被一副接取鏈路鑰匙保護之資料的數量。

CN被分成兩個不同且分開的領域(domain):電路交換(CS)領域、以及封包交換(PS)領域。當每一次RRC連線被解除時，在RRC連線裡被保護的負載的開始值$_{CS}$以及開始值$_{PS}$就被拿來與最大值即上限值(THRESHOLD)做比較。開始值$_{CS}$係CS領域所用的開始值，而開始值$_{PS}$係PS領域所用的開始值。當開始值$_{CS}$及/或開始值$_{PS}$達到或超過上限值時，UE就將開始值$_{CS}$及開始值$_{PS}$設為上限值，相當於把在USIM中對應的CN領域的開始值作記號使成為無效的。接著UE刪除儲

五、發明說明 (6)

存在USIM裡的密碼鑰匙以及完整鑰匙，並將鑰匙組的識別(key set identifier；KSI)設成無效(參閱3GPP TS 33.102中第6.4.4節)。否則就把開始值$_{CS}$及開始值$_{PS}$儲存在USIM裡。在3GPP TS 25.331中第8.5.9節中定義開始值的計算方式，開始值通常係從該領域裡COUNT-C值與COUNT-I值之中最大值的最高效位位元得到的。上限值係由通信網路營運商所設定的，並將之儲存在USIM裡。

當建立下一個RRC連接時，開始值係從USIM裡適當的領域中讀出的。如果任何一個開始值$_{CS}$或開始值$_{PS}$達到其對應的核心網路領域的上限值，UE便會觸發產生一副新的接取鏈路鑰匙組(一密碼鑰匙以及一完整鑰匙)。

在建立無線電連接給一特定服務網路領域(CS或PS)時，UE會在"RRC建立連接線完成"訊息裡傳送開始值$_{CS}$與開始值$_{PS}$至RNC。然後UE利用將開始值$_{CS}$與開始值$_{PS}$設為等於上限值，做標記表示在USIM裡的開始值為無效的。此舉動之目的係防止萬一在新的開始值被寫回到USIM裡之前，UE被關閉或失去電源時，造成該開始值被無意的重複使用。

此外3GPP TS 25.331中第8.3.7、8.3.9、8.3.11、以及8.5.2節也有描述何時該將開始值儲存至USIM裡。

3GPP規約可讓一UE切換到另一個無線規約，如數位式行動電話系統(Global System for Mobile；GSM)通信規約，係由多種稱為無線接取技術間(Inter-Radio access technology；Inter-RAT)程序的其中之一項程序來執行的。請參閱第5圖；第5圖係執行Inter-RAT程序之簡易方

五、發明說明 (7)

塊意示圖。最初，UE 20與3GPP UTRAN 10間有一已建立的RRC連線21。雖然任何Inter-RAT程序中的RRC連線21通常會連於CS領域12，但此RRC連線21其實可連於CS領域12或PS領域14其中之一，而在此範例中也假設RRC連線21係連於CS領域21的。當UE 20移動至靠近GSM網路30的範圍內時，UTRAN 10會決定把UE 20切換到GSM網路30裡。而當Inter-RAT程序成功地完成後，UE 20將會與GSM網路30建立一連線23，與UTRAN的連線21也就被切斷。而在UE 20裡USIM 20u的開始值因此需要被更新。在此範例中，USIM 20u中的開始值$_{CS}$ 22必須被更新。可是如果在Inter-RAT交接的時候，開始值超過了上限值，便會產生問題。

假設UE 20在UTRAN 10內被打開，UMTS鑑定程序便會執行(詳細說明請參閱3GPP TS 33.102中6.8節)，利用USIM 20u中儲存的包括密碼鑰匙CKcs 24與完整鑰匙IKcs 26的密碼鑰匙組，製造GSM密碼鑰匙Kc 28。UE 20在CS領域12中撥打電話，並使用密碼鑰匙CKcs 24與完整鑰匙IKcs 26啟動加密。UE 20於是開始移向GSM網路30中一個基地台子系統(Base Station Subsystem; BSS)的涵蓋範圍。根據UE 20傳來的訊號量測報告，當訊號強度轉弱至一定程度時，UTRAN 10會決定將與UE 20的通訊交接至GSM網路30。因此藉著UTRAN 10傳給UE 20"從UTRAN交接(HANDOVER FROM UTRAN)"的指令，啟動Inter-RAT交接程序。假設當Inter-RAT程序發生時，開始值cs 22達到上限值，藉由先前所述之安全程序，會將密碼鑰匙CKcs 24與

五、發明說明 (8)

完整鑰匙IKcs 26刪除。然而，GSM密碼鑰匙Kc 28並不會被刪除，且會被UE 20在GSM網路30中用來執行加密。假設UE 20這時開始移向UTRAN 10的基地台(node B)，根據UE 20傳來的訊號量測報告，當訊號強度轉弱至一定程度時，GSM BSS會決定將與UE 20的通訊交接給UTRAN 10。藉著UTRAN 10經由GSM網路30傳至UE 20" 交接給UTRAN (HANDOVER TO UTRAN)" 的指令執行這樣的通訊交接。根據3GPP TS 25.331中第8.3.6.3節所規定，UE 20應於接收到" 交接給UTRAN" 指令後立即加密。可是因為CKcs 24與IKcs 26不再存在於USIM 20u內，UE 20就不能執行加密。這樣可能會造成執行這項協定的軟體失靈。

發明內容

有鑑於此，本發明主要的目的就在於提供一種方法與相關裝置，處理當執行Inter-RAT交接程序時的安全服務。

這裡簡要敘述本發明之最佳實施例，在無線接取技術間(Inter-RAT)交接程序中執行加密的方法與無線裝置。" 從UTRAN交接(HANDOVER FROM UTRAN)" 程序是用來將無線裝置從全球行動通信系統(UMTS)地面無線接取網路(UTRAN)交接至第一網路。此第一網路定義為非UMTS網路，比如一個GSM網路。無線裝置經由第一網路傳送"Inter-RAT交接資訊(INTER RAT HANDOVER INFO)" 的訊息至UTRAN。這個"Inter-RAT交接資訊" 訊息包括保留在無線裝置內，為了加密所使用的安全開始值。接收到此安全開

五、發明說明 (9)

始值後，UTRAN檢驗此安全開始值是否大於或等於上限值，當執行"交接給UTRAN"的Inter-RAT程序，使得無線裝置從第一網路交接至UTRAN的時候，UTRAN會將與無線裝置的加密作業取消。同樣地，當執行"交接給UTRAN"時，如果開始值大於或等於上限值，無線裝置也會將加密作業取消。就算在執行"交接給UTRAN"程序之前，第一網路與無線裝置已經正在進行加密作業，加密作業仍會被取消。在完成"交接給UTRAN"程序後，UTRAN與無線裝置之間可以執行慣用的標準安全服務，以製造一組新的鑰匙並重新啟動加密作業。

在第二實施例中，"從UTRAN交接"程序會將無線裝置從UTRAN交接至第一網路。當連線至第一網路時，慣用的確證與鑰匙協定(Authentication and Key Agreement; AKA)程序會被執行，以提供無線裝置一組新的鑰匙。AKA程序是因應無線裝置內保存的開始值大於或等於上限值而被執行的。在得到一組新的鑰匙後，無線裝置會將開始值設為零。之後，當"交接給UTRAN"程序執行時，無線裝置會利用新的鑰匙組與UTRAN在"交接給UTRAN"程序中執行加密作業。

本發明之優點在於當無線裝置與第一網路連線時，藉由傳送開始值至UTRAN，或藉由執行AKA程序，可以保留無線裝置與UTRAN之間加密的同步性。因此在Inter-RAT程序進行中，通訊可以繼續而不被中斷。

經由熟悉此技術人士閱讀下列藉由圖表及圖畫之說明

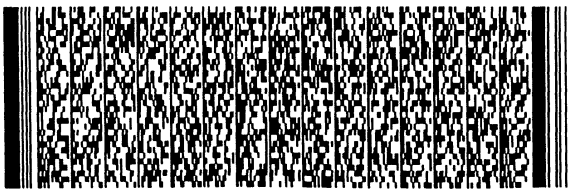
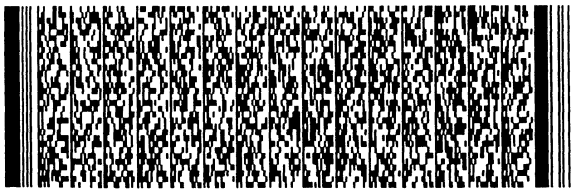
五、發明說明 (10)

對最佳實施例的詳細描述後，將會顯然地明白本發明之目的。

實施方式

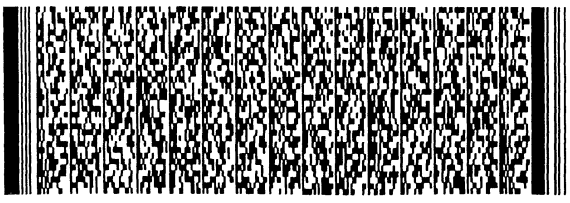
請參閱第6圖；第6圖為本發明之最佳實施例所述之無線裝置100的簡易方塊圖。該無線裝置100包括連接並接受一中央處理機(CPU)130控制之一輸入/輸出(I/O)硬體110、一無線電收發機120、以及一記憶體140，而這樣的連接方法與先前技術接近。上述I/O硬體110可包括如顯示器和喇叭等輸出，以及如鍵盤和麥克風等輸入。上述無線電收發機120使無線裝置100能傳送及接收無線訊號。上述CPU 130按照記憶體140內的程式碼142執行，以控制無線裝置100之功能。上述無線裝置100之大部分方面都與習知技術相同，除了必須對上述程式碼142做些許更改以實現本發明。而熟悉此技術之人士在讀完以下本發明之詳細描述後，將會清楚明白如何對上述程式碼142作更改。

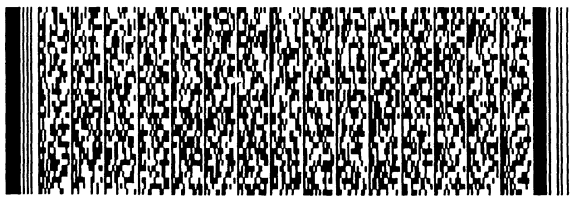
請參閱第7圖，並以第6圖為參考，第7圖為本發明之第一實施例的訊號順序圖。本發明之無線裝置，UE 100與習知技術相同，可以執行第一Inter-RAT程序，將3GPP協定切換至其他協定，如GSM。無線裝置100需要先與UTRAN203建立無線資源控制(RRC)連線。此RRC連線可以是PS領域或CS領域。本發明之方法與相關無線裝置100在這裡的敘述說明中，是假設在CS領域的，可是本發明之方法也適用於PS領域。無線裝置100執行第一Inter-RAT程序，如藉由"從UTRAN交接"指令產生的Inter-RAT交接程序，讓

五、發明說明 (11)

UE 100改為連接至第二系統，也就是非UMTS系統，如GSM GSS 202系統中。當執行"從UTRAN交接"指令201時，UE 100與UTRAN203之間正在執行加密，因此UE 100會利用舊的鑰匙組141o，以及對應的安全開始值cs 141s以舊有方式執行加密。舊的鑰匙組141o包括給CS領域的密碼鑰匙CKcs與完整鑰匙IKcs。因為加密作業是在UE 100與GSM BSS 202之間執行的，UE 100以標準方式從舊鑰匙組141o製造密碼鑰匙Kc 141c。也就是Kc=f(CKcs, IKcs)，這裡的f()是習知技術就有的預先定義函數。函數f()可以包括其他的參數，例如從PS領域來的現有鑰匙組。在第一實施例中，假設當"從UTRAN交接"指令201完成時，開始值cs 414s大於或等於由通信網路營運商或系統設記者預先設定的上限值146，標示該鑰匙已經太舊了，因此需要被更新。如此一來，在"從UTRAN交接"指令201完成後，UE 100便將舊的一組鑰匙141o刪除。然而UE 100因為有GSM密碼鑰匙Kc 141c，還是可以繼續與GSM BSS 202進行加碼通訊。在UE 100的連線轉交至UTRAN 203之前，會以標準方式經由GSM BSS 202傳送一個"INTER RAT交接資訊"訊息204至UTRAN 203，其中包括下一次交接給UTRAN時為了加密同步性所需的開始值cs 141s。最後，執行第二Inter-RAT程序，將UE 100的連線交接給UTRAN 203。此第二Inter-RAT程序是藉由GSM BSS202傳送"交接給UTRAN"指令205至UE 100而執行的。此"交接給UTRAN"指令是藉著密碼鑰匙Kc 141c加密而成的。UE 100以標準方式處理此"交

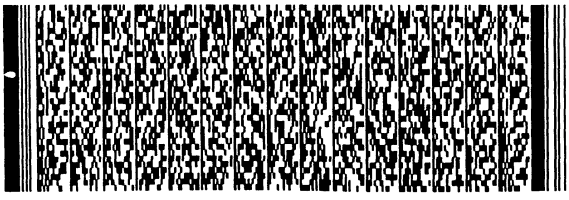


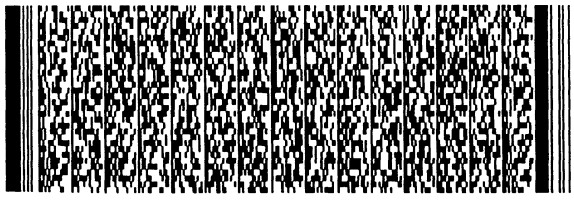


五、發明說明 (12)

接給UTRAN"指令205，並以傳送"交接給UTRAN完成"訊息206給UTRAN 203作為回應。不過儘管當"交接給UTRAN完成"訊息206傳送時，UE 100以習知方式通常會加密，但是在第一實施例中UE 100不會在"交接給UTRAN"回應與應答程序中給予加密，因為開始值cs 141s已經超過(或等於)上限值146，因此UE 100沒有一組鑰匙可以用來執行加密。相同地，UTRAN 203會藉由"INTER RAT交接資訊"訊息204所接收到的開始值cs 141s，知道開始值cs大於或等於上限值146，UTRAN 203於是將加密作業取消，以等待接收由UE 100傳來"交接給UTRAN完成"訊息206。因此在第二Inter-RAT交接程序中UE 100與UTRAN 203的加密可以同步。之後UE 100與UTRAN 203可啟動習知的安全程序，製造新的一組鑰匙141n以及新的開始值cs 141s(通常為零)，使加密作業再次開始進行。

本發明之下列方法使用習知確證與鑰匙協定(AKA)服務，在連接至非UTMS網路時讓UE 100取得新的一組鑰匙141n。AKA程序為AKA伺服器，例如訪客位置暫存器(Visitor Location Register; VLR)，與UE 100之間的習知安全盤問與回應(challenge-and-response)程序，用來製造鑰匙組。AKA程序的作業的詳細內容並不包括在本發明範圍內，且可以視UE 100的安全結構而變(例如依據UE 100是否包括USIM 144)。藉由完成AKA程序，UE 100會有一組新的鑰匙141n，並且AKA程序會將這組新的鑰匙141n通知UTRAN。





五、發明說明 (13)

請參閱第8圖，第8圖為本發明第二實施例的訊息順序圖。此第二實施例假設UE 100包括USIM 144，因此可以與UMTS AKA伺服器301一起執行UMTS AKA程序。UMTS AKA伺服器301可以是，例如一個VLR/SGSN。如同第一實施例中，第一Inter-RAT程序，例如藉由"從UTRAN交接"程序304將UE 100連線到非UMTS的第一網路，例如GSM BSS 302。在"從UTRAN交接"指令304完成後，UE 100的開始值cs 141s會大於或等於上限值146，所以舊的鑰匙組141會被刪除(這組鑰匙在這之前是用來執行加碼以及製造GSM密碼鑰匙Kc 141c)。加碼作業會藉由GSM密碼鑰匙Kc 141c，在UE 100與GSM BSS 302之間繼續執行。在交接UE 100的連線回UTRAN 303之前，UE 100會經由GSM BSS 302傳送"INTER RAT交接資訊"訊息309至UTRAN 303。另外，因為開始值cs 141s大於或等於上限值146，當UE 100還是與第一網路(即GSM BSS 302)連線時，UE 100與UMTS AKA伺服器之間會執行UMTS AKA程序。啟動UMTS AKA程序的方式包括藉由UTRAN 303接收"INTER RAT交接資訊"訊息309，並注意到開始值cs已超過上限值，因此命令UMTS AKA伺服器301與UE 100執行UMTS AKA程序。UMTS AKA伺服器301傳送"UMTS確證請求"305至UE 100，並且UE 100以"UMTS確證回應"306對該請求做回應。這樣的盤問與回應動作完成之後，UE 100將有一組新的鑰匙141n，UE 100設定開始值cs 141s的值小於上限值146，開始值的理想值為零，因為這樣可以提供這組新鑰匙141n最長的可能壽命。同樣地，在

五、發明說明 (14)

UE 100與UMTS AKA伺服器301之間UMTS AKA盤問與回應對話成功的結束時，UMTS AKA伺服器301將UE 100製造的一組新鑰匙141n向UTRAN 303通報。於是UTRAN 303也將開始值cs設定為零(即設定與UE 100的開始值cs 141s相同的值)。最後決定將UE 100的連線交接回UTRAN 303。結果GSM BSS 302會將"交接給UTRAN"指令307傳至UE 100。UE 100在接收到"交接給UTRAN"指令307後，會立即以新鑰匙組141n與新的開始值cs 141s執行加密作業。因此最後當UE 100傳送"交接給UTRAN完成"訊息308至UTRAN 303，表示第二Inter-RAT程序已結束時，加密作業仍然是不間斷的。

請參閱第9圖，第9圖為本發明之第三實施例的訊息順序圖。在第三實施例中，假設UE 100沒有包括USIM 144，因此無法執行UMTS AKA程序。UE 100卻包括了SIM 148，因此可以與GSM AKA伺服器401一同執行GSM AKA程序。如同先前的實施例所述，第一Inter-RAT程序會產生例如"從UTRAN交接"程序404，將UE 100連線至非UMTS網路的第一網路，例如GSM BSS 402。"從UTRAN交接"指令404完成後，UE 100的開始值cs 141s會大於或等於上限值146，因此舊的鑰匙組141o會被刪除。UE 100與GSM BSS 402之間利用GSM密碼鑰匙Kc 141c而繼續保持加密作業。在交接回UTRAN 403之前，UE 100經由GSM BSS 402傳送"INTER RAT交接資訊"訊息409給UTRAN 403。另外，因為開始值cs 141s大於或等於上限值146，當UE 100仍然與第一網路(即

五、發明說明 (15)

GSM BSS 402)連線時，GSM AKA程序會在UE 100與GSM AKA伺服器401之間執行。啟動GSM AKA程序的方法包括，藉由UTRAN 403或GSM BSS 402接收"INTER RAT交接資訊"訊息409，並注意到開始值cs已經超過上限值，因此命令GSM AKA伺服器401與UE 100執行GSM AKA程序。GSM AKA伺服器401傳送"GSM確證請求"405至UE 100，並且UE 100以"GSM確證回應"406對該請求做回應。這樣的盤問與回應動作完成之後，UE 100將有一副新的密碼鑰匙Kc。這副新的密碼鑰匙Kc可或不可用來執行UE 100與GSM BSS 402之間的加密作業。UE 100對該副新的密碼鑰匙Kc的回應是利用習知的預先定義函數，從此密碼鑰匙Kc製造出一組新鑰匙141n。也就是新鑰匙組=F(新Kc)。在獲得新鑰匙組141n後，UE 100設定開始值cs 141s的值小於上限值146，開始值的理想值為零。UTRAN 403察覺到新的GSM密碼鑰匙Kc後，也同樣的製造一組新的鑰匙與UE 100相配。因此UTRAN 403也同樣地將開始值cs設為零。當GSM BSS 402將"交接給UTRAN"指令407傳至UE 100時，UE 100立即以新鑰匙組141n以及新的開始值cs 141s執行加密作業。因此最後當UE 100傳送"交接給UTRAN完成"訊息408至UTRAN 403，表示第二Inter-RAT程序已結束時，加密作業仍然是不間斷的。

雖然本發明所列舉的範例皆為GSM系統，不過本發明也可被應用在其他無線接取技術(Radio Access Technologies; RATs)。

五、發明說明 (16)

與習知技術相比，本發明提供UE與UTRAN之間加密的同步性，適用於將UE從第二RAT交接回UTRAN的時候。如果舊的鑰匙組被刪除，加密作業可以在交接程序中被停用；或是如果當UE連線至第二RAT系統的交接中，已經獲得了一組新的鑰匙，加密作業就可以被啟動。

雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

圖式簡單說明

第1圖說明利用完整演算法f9鑑定傳信訊息的資料完整性；

第2圖為第1圖中描述的完整序列號碼(COUNT-I)值之資料結構方塊圖；

第3圖描述在無線接取鏈路上將用戶及訊號資料譯成密碼；

第4圖為第3圖中密碼序列號碼(COUNT-C)值在所有不同連線模式下之資料結構示意圖；

第5圖為Inter-RAT程序之簡易方塊圖；

第6圖為本發明之最佳實施例所述之無線裝置的簡易方塊圖；

第7圖為本發明之第一實施例的訊息順序圖；

第8圖為本發明之第二實施例的訊息順序圖；

第9圖為本發明之第三實施例的訊息順序圖。

符號說明

10 ~ UMTS地面無線接取網路(UTRAN)；

12 ~ 電路交換(CS)領域；

14 ~ 封包交換(PS)領域；

20 ~ 用戶端設備(UE)；

20u ~ USIM/非揮發性記憶體；

21 ~ RRC連線；

22 ~ 開始值cs；

23 ~ GSM連線；

圖式簡單說明

24 ~ 密碼鑰匙(CKcs)；

26 ~ 完整鑰匙(IKcs)；

28 ~ GSM密碼鑰匙(Kc)；

30 ~ GSM網路；

100 ~ 用戶端設備(UE)；

110 ~ I/O硬體；

120 ~ 無線電收發機；

130 ~ 中央處理器(CPU)；

140 ~ 記憶體；

141 ~ 電路交換(CS)領域；

141n ~ CS新鑰匙；

141o ~ CS舊鑰匙；

141s ~ 開始值CS；

141c ~ GSM密碼鑰匙；

144 ~ USIM記憶體；

144c ~開始值CS；

148 ~ SIM；

201、304、404 ~ "從UTRAN交接"程序；

202、302、402 ~ GSM BSS；

203、303、403 ~ UTRAN；

204、309、409 ~ "INTER RAT交接資訊"訊息；

205、307、407 ~ "交接至UTRAN"程序；

206、308、408 ~ "交接至UTRAN完成"訊息；

301 ~ UMTS AKA伺服器；

圖式簡單說明

305 ~ UMTS確證請求；

306 ~ UMTS確證回應；

401 ~ GSM AKA伺服器；

405 ~ GSM確證請求；

406 ~ GSM確證回應。

四、中文發明摘要　（發明名稱：無線接取技術間交接程序中的加密作業方法）

六、英文發明摘要　（發明名稱：CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE）

device is attached to the second network, and ciphering is performed during the HANDOVER TO UTRAN procedure, utilizing the new key set.

六、申請專利範圍

1. 一種加密作業的方法，係執行於無線接取技術間(Inter Radio Access Technology; Inter-RAT)交接程序中，此方法包括:

執行一第一Inter-RAT程序，將一無線裝置從一全球行動通信系統地面無線接取網路(Universal Mobile Telecommunication System Terrestrial Radio Access Network；UTRAN)交接至一第一網路；

該無線裝置經由該第一網路傳送一第一訊息至該UTRAN，該第一訊息包括該無線裝置中保存的一安全開始值；以及

該UTRAN在接收到該安全開始值並且判斷該安全開始值大於或等於一上限值之後，於執行將該無線裝置從該第一網路交接至該UTRAN的一第二Inter-RAT程序中，取消該第一網路與該無線裝置之間的加密作業；

其中，該第一網路與該無線裝置之間的加密作業，在執行該第二Inter-RAT程序之前是存在的。

2. 如申請專利範圍第1項所述之加密作業的方法，其中該第一網路為一非全球行動通信系統(non Universal Mobile Telecommunication System; non-UMTS)網路。

3. 如申請專利範圍第1項所述之加密作業的方法，其中該第一訊息為一無線接取技術間交接資訊(INTER RAT HANDOVER INFO)訊息。

4. 如申請專利範圍第1項所述之加密作業的方法，更包括該無線裝置於該安全開始值大於或等於該上限值時，

六、申請專利範圍

在該第二Inter-RA程序中，取消與該UTRAN之間加密作業。

5. 如申請專利範圍第1項所述之加密作業的方法，更包括:

該無線裝置執行一確證與鑰匙協定(Authentication and Key Agreement; AKA)程序，並且於該第二Inter-RAT程序完成後，與該UTRAN執行一安全程序以獲得一組新安全鑰匙；以及

該無線裝置利用該組新安全鑰匙與該UTRAN開始加密作業。

6. 一種無線裝置，係包括一處理器及一記憶體，該記憶體更包括可被該處理器執行之下列步驟的程式碼:

執行一第一無線電相互間接取技術(Inter-RAT)程序，將該無線裝置從一全球行動通信系統地面無線接取網路(UTRAN)交接至一第一網路；

經由該第一網路傳送一第一訊息至該UTRAN，該第一訊息包括該無線裝置中保存的一安全開始值；以及

該安全起始值大於或等於一上限值時，於執行將該無線裝置從該第一網路交接至該UTRAN的一第二Inter-RAT程序中，取消與該UTRAN之間加密作業；

其中該第一網路與該無線裝置之間加密作業，在執行該第二Inter-RAT程序之前是存在的。

7. 如申請專利範圍第6項所述之無線裝置，其中該第一網路為一非全球行動通信系統(non-UMTS)網路。

六、申請專利範圍

8. 如申請專利範圍第6項所述之無線裝置，其中該第一訊息為一無線接取技術間交接資訊(INTER RAT HANDOVER INFO)訊息。

9. 如申請專利範圍第6項所述之無線裝置，其中該程式碼更包括執行下列步驟:

執行一確證與鑰匙協定(AKA)程序，並且於該第二Inter-RAT程序成功完成後，與該UTRAN執行一安全程序以獲得一組新安全鑰匙；以及

利用該組新安全鑰匙與該UTRAN開始加密作業。

10. 一種加密作業的方法，係執行於一無線接取技術間(Inter-RAT)交接程序中，此方法包括:

執行一第一Inter-RAT程序，將一無線裝置從一全球行動通信系統地面無線接取網路(UTRAN)交接至一第一網路；

當保留在該無線裝置的一開始值大於或等於一上限值，執行一確證與鑰匙協定(AKA)程序，以提供該無線裝置一組新鑰匙；

該無線裝置獲得該組新鑰匙時，設定該開始值為比該上限值小的一預先決定值；以及

執行一第二Inter-RAT程序，將該無線裝置從該第一網路交接至該UTRAN；

其中該無線裝置在該第二Inter-RAT程序中，利用該組新鑰匙與該UTRAN之間執行加密作業。

11. 如申請專利範圍第10項所述之加密作業的方法，

六、申請專利範圍

其中該預先決定值為零。

12. 如申請專利範圍第10項所述之加密作業的方法，更包括該無線裝置經由該第一網路傳送一第一訊息至該UTRAN，該第一訊息包括該無線裝置中保存的一安全開始值。

13. 如申請專利範圍第12項所述之加密作業的方法，其中該第一訊息為一無線接取技術間交接資訊(INTER RAT HANDOVER INFO)訊息。

14. 如申請專利範圍第13項所述之加密作業的方法，其中該第一網路為一非全球行動通信系統(non-UMTS)網路。

15. 如申請專利範圍第10項所述之加密作業的方法，其中該AKA程序更提供一鑰匙Kc，並藉由該鑰匙Kc產生出該組新鑰匙。

16. 一種無線裝置，係包括一處理器及一記憶體，該記憶體更包括可被該處理器執行之下列步驟的程式碼:

執行一第一Inter-RAT程序，將該無線裝置從一全球行動通信系統地面無線接取網路(UTRAN)交接至一第一網路；

執行一確證與鑰匙協定(AKA)程序，以提供該無線裝置一組新鑰匙；

當連線至該地第一網路中，該無線裝置獲得該組新鑰匙時，將有關該組新鑰匙的一安全開始值設定為比一上限值小的一預先決定值；以及

六、申請專利範圍

執行一第二Inter-RAT程序，將該無線裝置從該第一網路交接至該UTRAN；

其中該無線裝置在該第二Inter-RAT程序中，利用該組新鑰匙與該UTRAN之間執行加密作業。

17.如申請專利範圍第16項所述之無線裝置，其中該預先決定值為零。

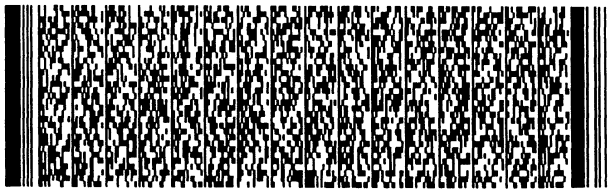
18.如申請專利範圍第16項所述之無線裝置，其中該程式碼更包括執行下列步驟:

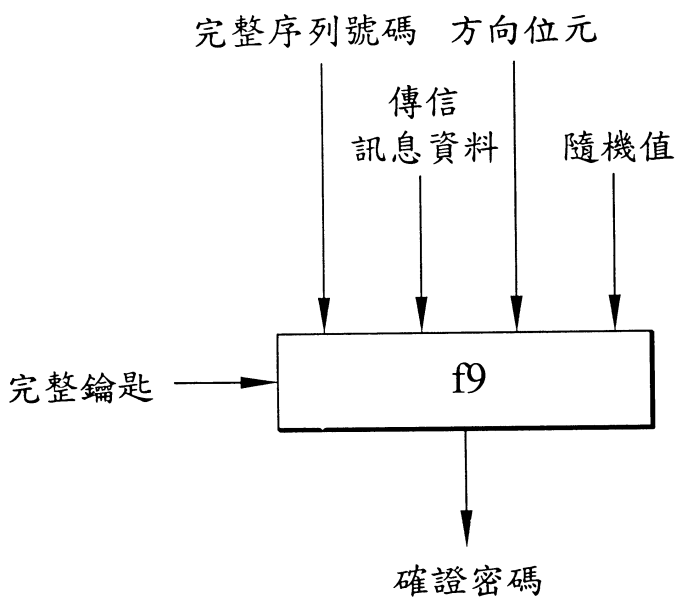
經由該第一網路傳送一第一訊息至該UTRAN，該第一訊息包括該無線裝置中保存的一安全開始值。

19.如申請專利範圍第18項所述之無線裝置，其中該第一訊息為一無線接取技術間交接資訊(INTER RAT HANDOVER INFO)訊息。

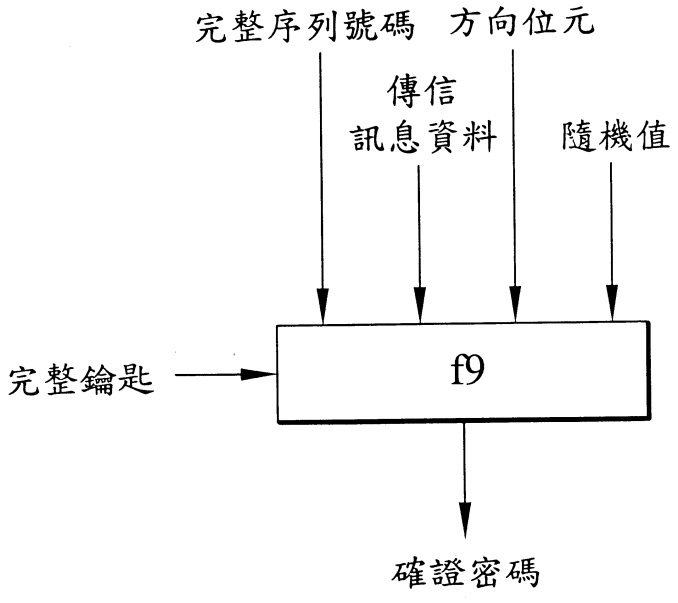
20.如申請專利範圍第16項所述之無線裝置，其中該第一網路為一非全球行動通信系統(non-UMTS)網路。

21.如申請專利範圍第16項所述之無線裝置，其中該AKA程序更提供一鑰匙Kc，並藉由該鑰匙Kc產生出該組新鑰匙。



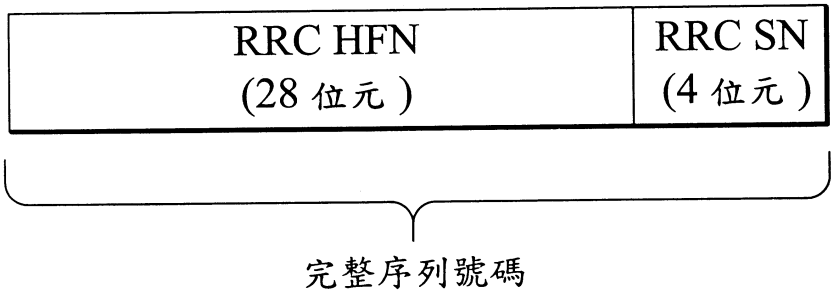


傳送端UE或RNC

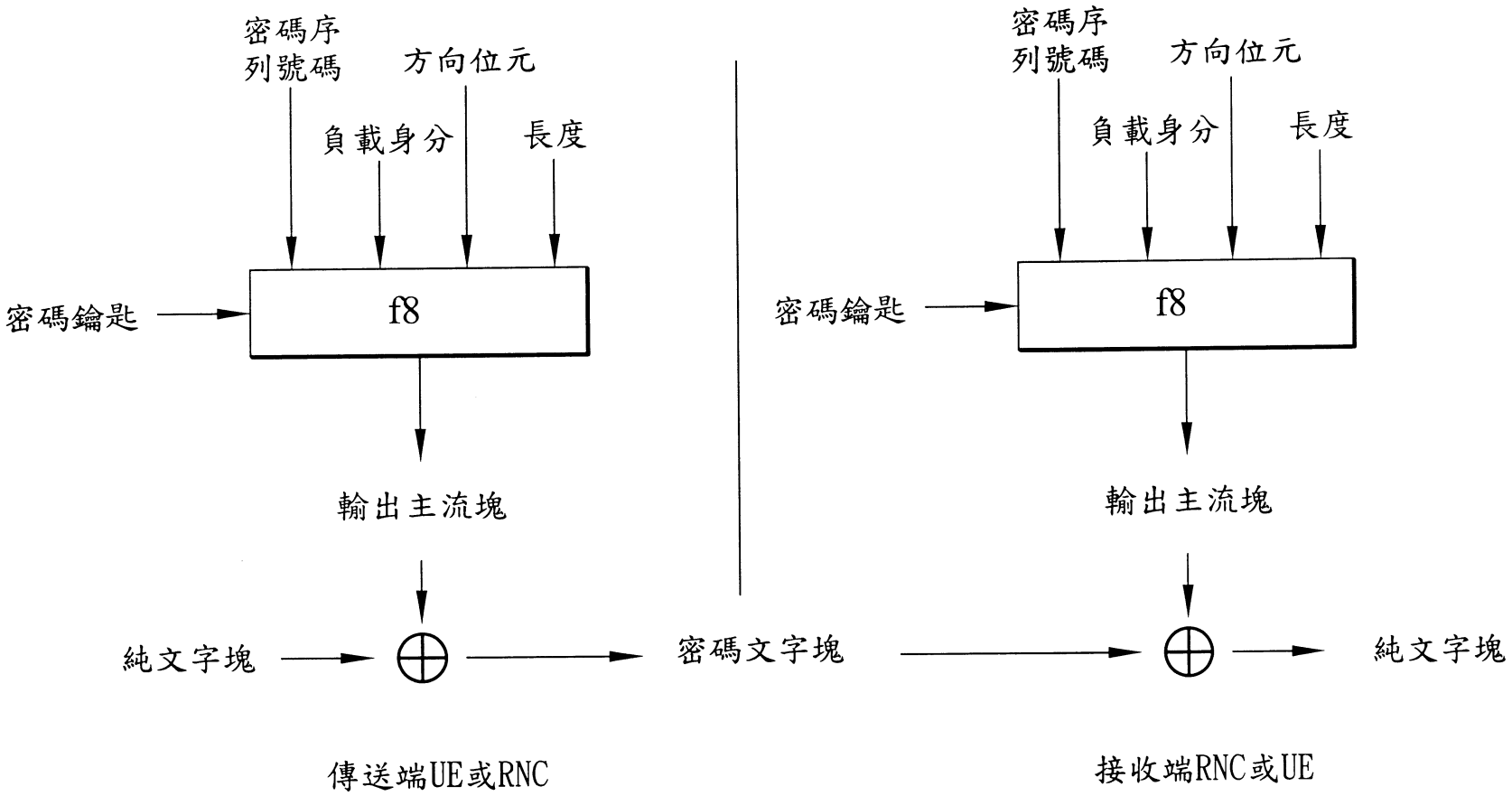


接收端RNC或UE

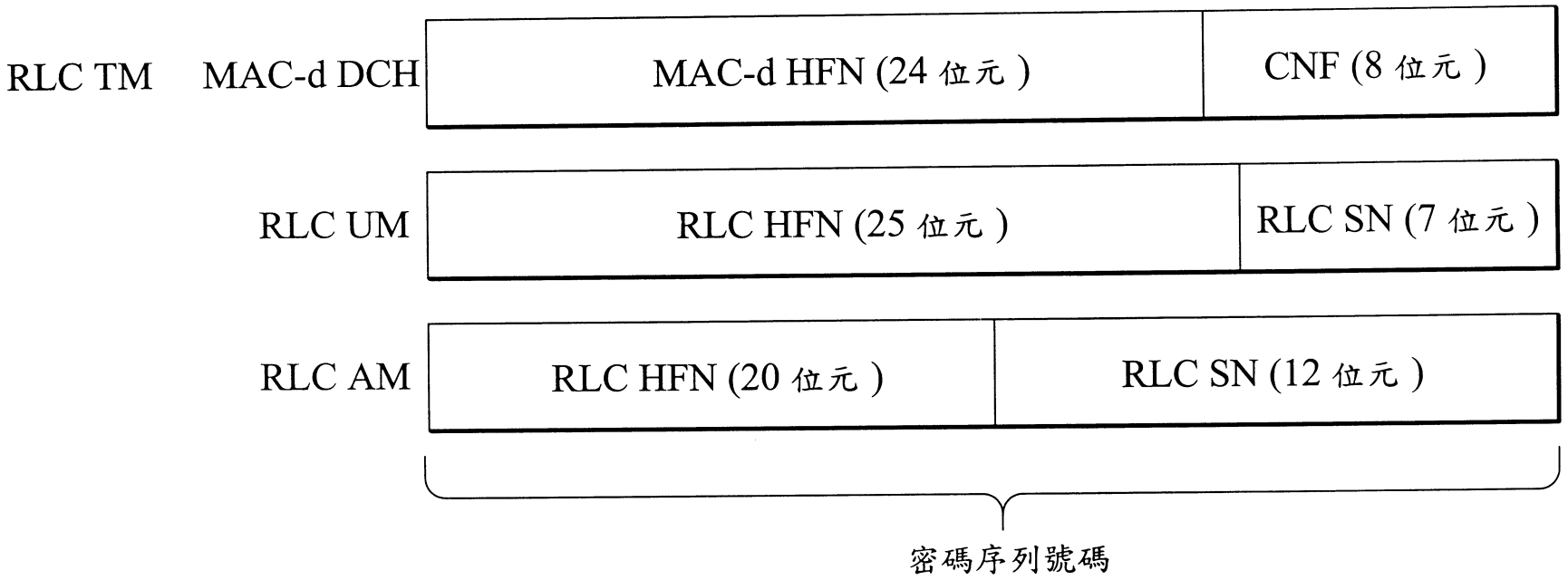
第 1 圖



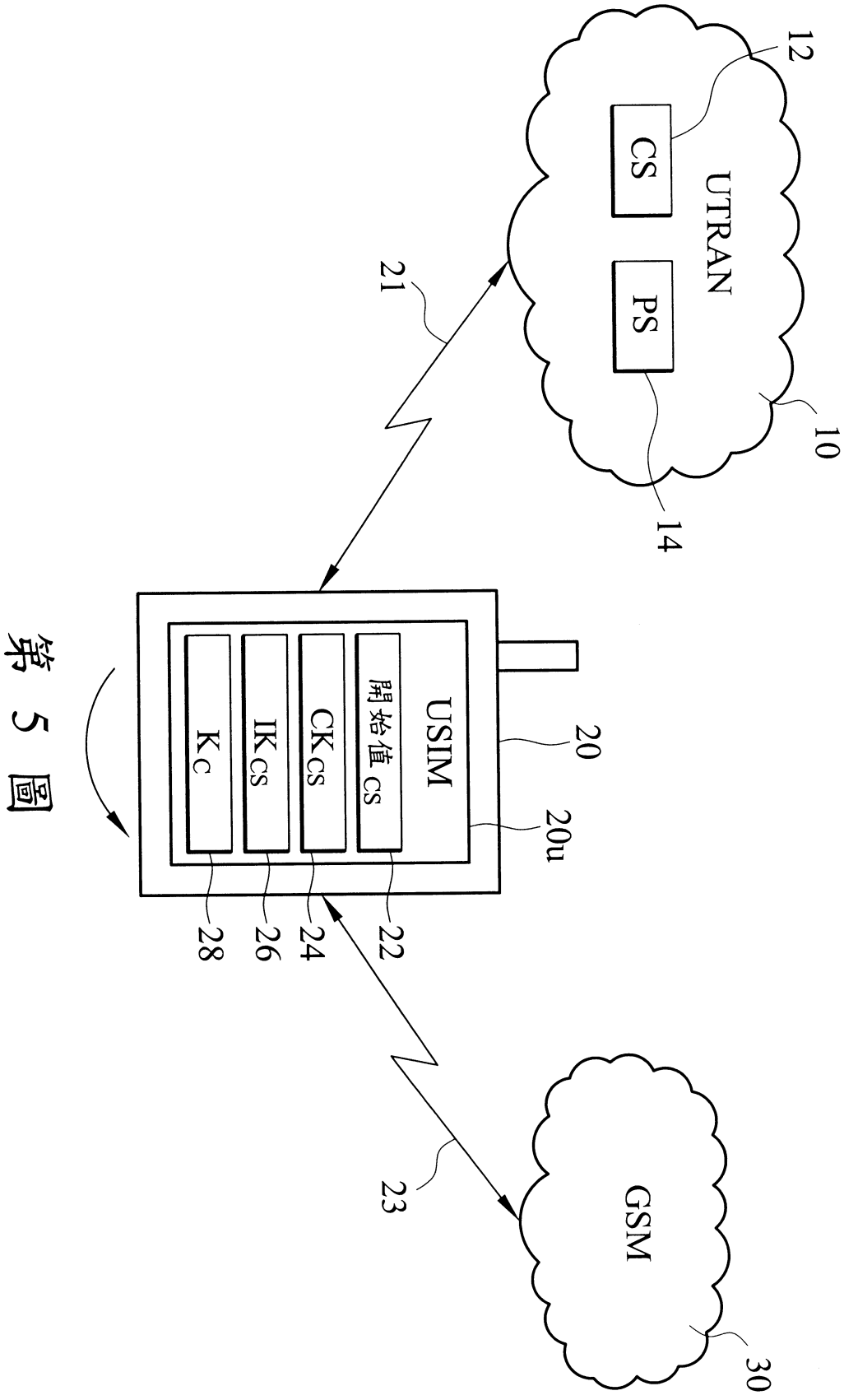
第 2 圖


密碼序
列號碼
方向位元
負載身分
長度
密碼鑰匙
f8
輸出主流塊
純文字塊
密碼文字塊
傳送端UE或RNC
密碼序
列號碼
方向位元
負載身分
長度
密碼鑰匙
f8
輸出主流塊
純文字塊
接收端RNC或UE

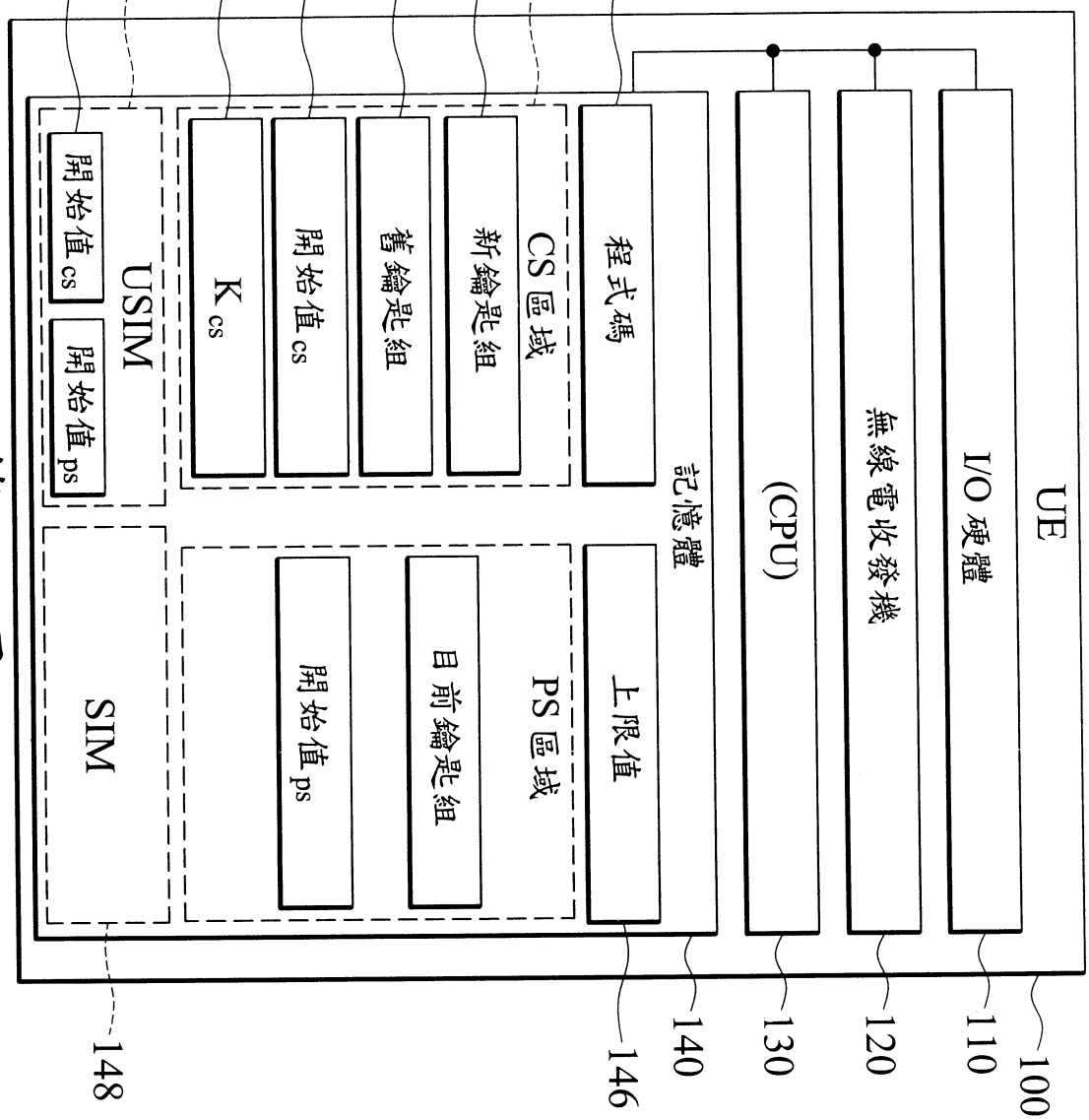
第 3 圖


RLC TM
MAC-d DCH
MAC-d HFN (24 位元)
CNF (8 位元)
RLC UM
RLC HFN (25 位元)
RLC SN (7 位元)
RLC AM
RLC HFN (20 位元)
RLC SN (12 位元)
密碼序列號碼

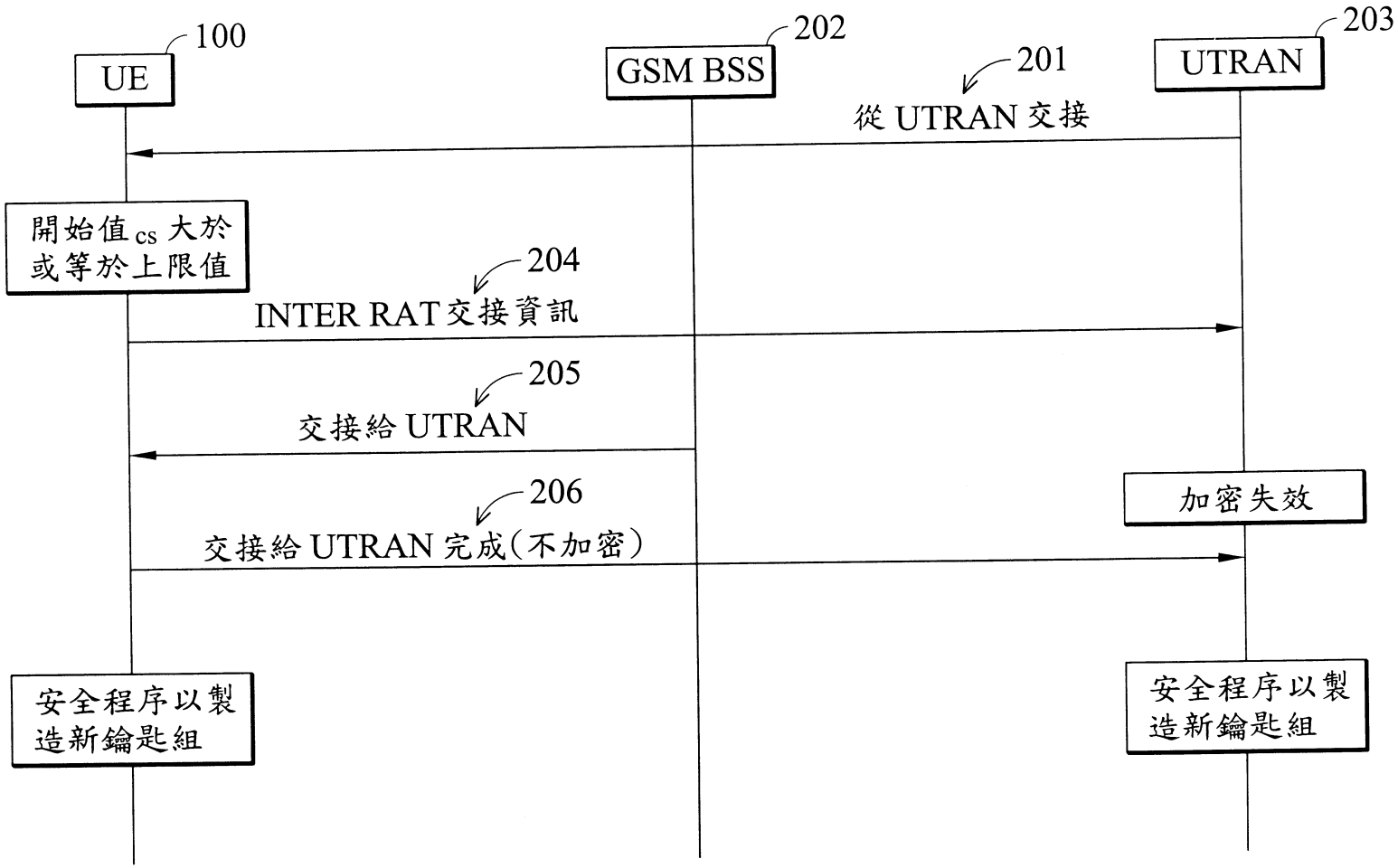
第 4 圖


12
CS
UTRAN
PS
10
14
21
USIM
開始值 CS
CKCS
IKCS
KC
20
20u
22
24
26
28
23
GSM
30

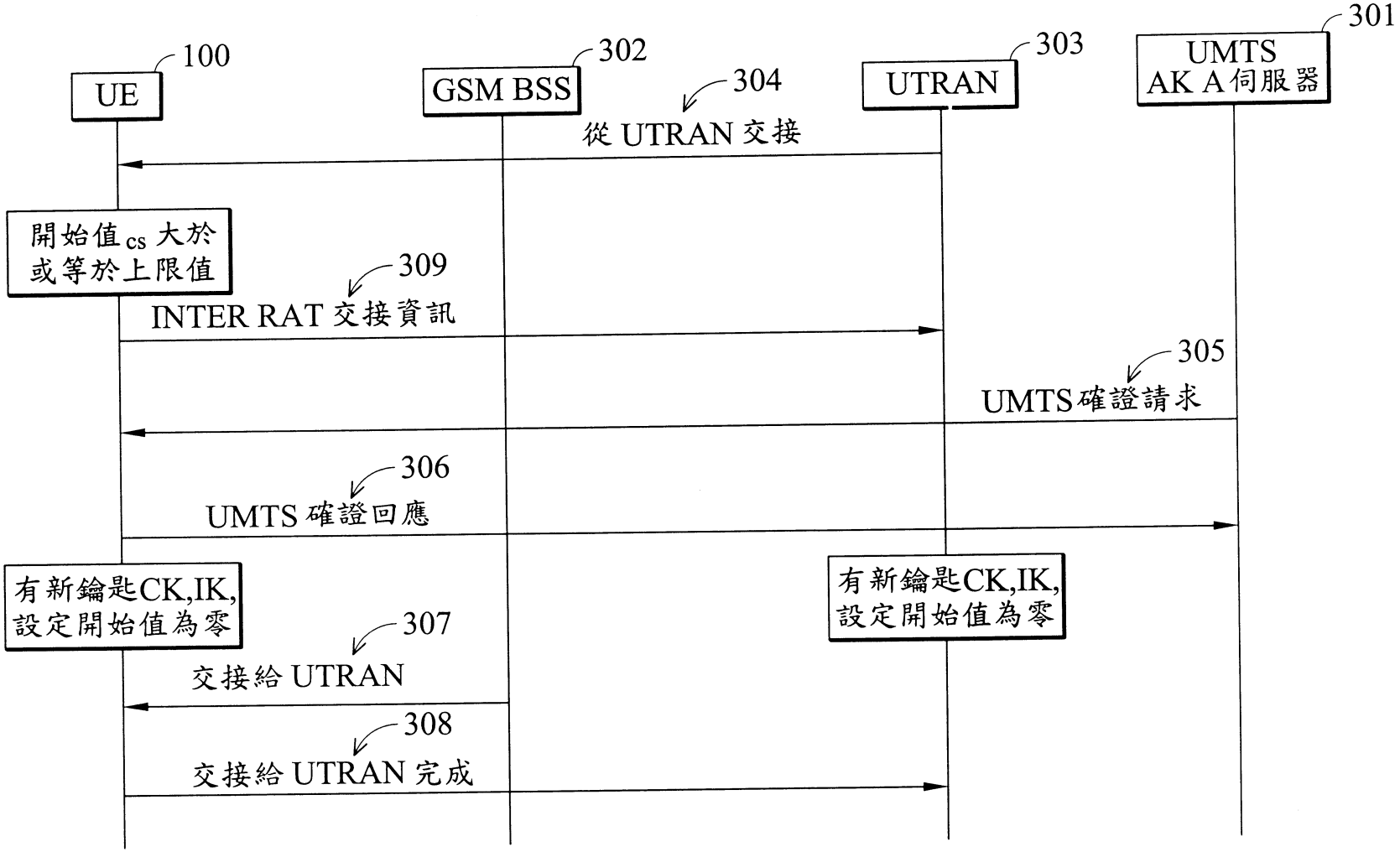
第 5 圖


UE
I/O 硬體
無線電收發機
(CPU)
記憶體
程式碼
上限值
CS 區域
新鑰匙組
舊鑰匙組
開始值 cs
K cs
PS 區域
目前鑰匙組
開始值 ps
USIM
開始值 cs
開始值 ps
SIM
100
110
120
130
140
142
141
141n
141o
141s
141c
144
144c
146
148

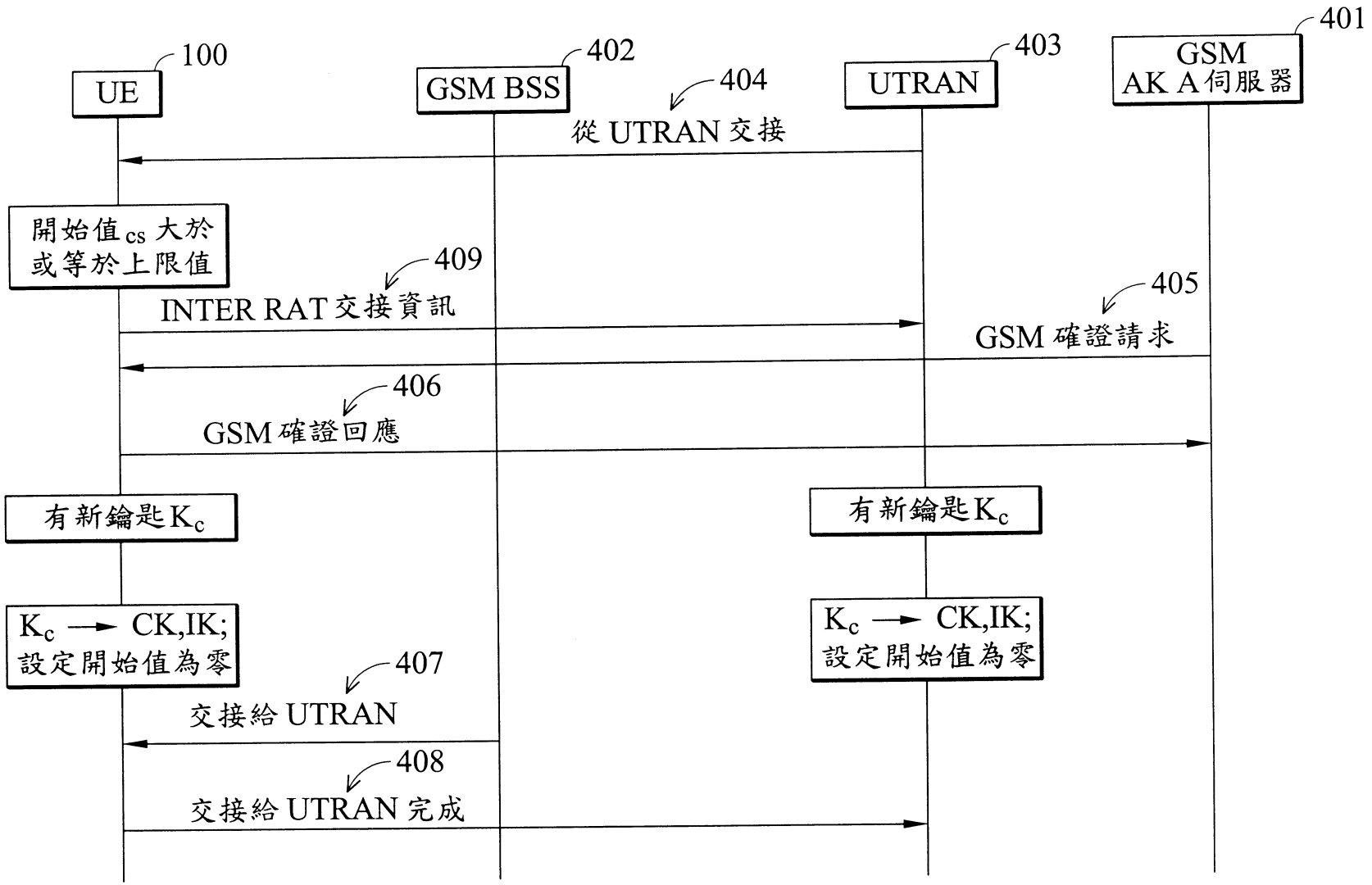
第 6 圖


100
UE
202
GSM BSS
201
從 UTRAN 交接
203
UTRAN
開始值cs 大於
或等於上限值
204
INTER RAT交接資訊
205
交接給 UTRAN
206
交接給 UTRAN 完成(不加密)
加密失效
安全程序以製
造新鑰匙組
安全程序以製
造新鑰匙組

第 7 圖


UE
100
GSM BSS
302
304
從 UTRAN 交接
UTRAN
303
UMTS
AK A 伺服器
301
開始值cs 大於
或等於上限值
309
INTER RAT 交接資訊
305
UMTS確證請求
306
UMTS 確證回應
有新鑰匙CK,IK,
設定開始值為零
有新鑰匙CK,IK,
設定開始值為零
307
交接給 UTRAN
308
交接給 UTRAN 完成

第 8 圖


UE
100
GSM BSS
402
404
UTRAN
403
GSM
AK A伺服器
401
從 UTRAN 交接
開始值cs 大於
或等於上限值
409
INTER RAT 交接資訊
405
GSM 確證請求
406
GSM 確證回應
有新鑰匙Kc
有新鑰匙Kc
Kc → CK,IK;
設定開始值為零
Kc → CK,IK;
設定開始值為零
407
交接給 UTRAN
408
交接給 UTRAN 完成

第 9 圖

公告本

95年5月10日 修正頁 I262010

申請日期： 93.2.4	IPC分類 H04L 9/28
申請案號： 93102459	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中文	無線接取技術間交接程序中的加密作業方法與無線裝置
	英文	CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE
二、發明人(共1人)	姓名(中文)	1.吳志祥
	姓名(英文)	1.Chi-Hsiang Wu
	國籍(中英文)	1.中華民國 TW
	住居所(中文)	1.台北縣新店市二十張路25巷18弄38號5樓
	住居所(英文)	1.
三、申請人(共1人)	名稱或姓名(中文)	1.華碩電腦股份有限公司
	名稱或姓名(英文)	1.ASUSTeK COMPUTER INC.
	國籍(中英文)	1.中華民國 ROC
	住居所(營業所)(中文)	1.台北市北投區立德路150號4樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.4F, No. 150, Li-Te Rd., Peitou, Taipei City, Taiwan, R.O.C.
	代表人(中文)	1.施崇棠
	代表人(英文)	1.SHIH CHUNG TANG

四、中文發明摘要 （發明名稱：無線接取技術間交接程序中的加密作業方法與無線裝置）

"從UTRAN交接"程序是為了要將一無線裝置從UTRAN交接至一第一網路而執行的。當無線裝置連線至第一網路時，無線裝置傳送"INTER RAT交接資訊"訊息給UTRAN。"INTER RAT交接資訊"訊息包括保存在無線裝置中，用在加密作業的安全開始值。當執行"交接給UTRAN"程序時，因應安全開始值大於或等於上限值，UTRAN將與無線裝置之間的加密作業取消。同樣地，如果開始值大於或等於上限值，無線裝置也會在執行"交接給UTRAN"程序中，將加密作業取消。另一個可行的作法是當無線裝置連線於第一網路時，產生一組新的密碼鑰匙，並可利用該組新鑰匙在"交接給UTRAN"程序中執行加密作業。

五、（一）、本案代表圖為：第__7、8、9__圖

（二）、本案代表圖之元件代表符號簡單說明：

六、英文發明摘要 （發明名稱：CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE）

A HANDOVER FROM UTRAN procedure is performed to handover a wireless device from the UTRAN to a second network. While attached to the second network, the wireless device sends an INTER RAT HANDOVER INFO message to the UTRAN. The INTER RAT HANDOVER INFO message includes the security START value maintained by the wireless device for ciphering purposes. In response to determining

四、中文發明摘要 （發明名稱：無線接取技術間交接程序中的加密作業方法與無線裝置）

100 ~ 用戶端設備(UE)；
201、304、404 ~ "從UTRAN交接"程序；
202、302、402 ~ GSM BSS；
203、303、403 ~ UTRAN；
204、309、409 ~ "INTER RAT交接資訊"訊息；
205、307、407 ~ "交接至UTRAN"程序；
206、308、408 ~ "交接至UTRAN完成"訊息；
301 ~ UMTS AKA伺服器；
305 ~ UMTS確證請求；
306 ~ UMTS確證回應；
401 ~ GSM AKA伺服器；
405 ~ GSM確證請求；
406 ~ GSM確證回應。

六、英文發明摘要 （發明名稱：CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE）

that the security START value equals or exceeds a THRESHOLD value, the UTRAN disables ciphering with the wireless device when performing a HANDOVER TO UTRAN procedure. Similarly, the wireless device disables ciphering when performing the HANDOVER TO UTRAN procedure if the START value equals or exceeds the THRESHOLD value. Alternatively, a new ciphering key set is generated while the wireless

四、中文發明摘要 （發明名稱：無線接取技術間交接程序中的加密作業方法與無線裝置）

"從UTRAN交接"程序是為了要將一無線裝置從UTRAN交接至一第一網路而執行的。當無線裝置連線至第一網路時，無線裝置傳送"INTER RAT交接資訊"訊息給UTRAN。"INTER RAT交接資訊"訊息包括保存在無線裝置中，用在加密作業的安全開始值。當執行"交接給UTRAN"程序時，因應安全開始值大於或等於上限值，UTRAN將與無線裝置之間的加密作業取消。同樣地，如果開始值大於或等於上限值，無線裝置也會在執行"交接給UTRAN"程序中，將加密作業取消。另一個可行的作法是當無線裝置連線於第一網路時，產生一組新的密碼鑰匙，並可利用該組新鑰匙在"交接給UTRAN"程序中執行加密作業。

五、（一）、本案代表圖為：第__7、8、9__圖

（二）、本案代表圖之元件代表符號簡單說明：

六、英文發明摘要 （發明名稱：CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE）

A HANDOVER FROM UTRAN procedure is performed to handover a wireless device from the UTRAN to a second network. While attached to the second network, the wireless device sends an INTER RAT HANDOVER INFO message to the UTRAN. The INTER RAT HANDOVER INFO message includes the security START value maintained by the wireless device for ciphering purposes. In response to determining

四、中文發明摘要 （發明名稱：無線接取技術間交接程序中的加密作業方法與無線裝置）

100 ~ 用戶端設備(UE)；
201、304、404 ~ "從UTRAN交接"程序；
202、302、402 ~ GSM BSS；
203、303、403 ~ UTRAN；
204、309、409 ~ "INTER RAT交接資訊"訊息；
205、307、407 ~ "交接至UTRAN"程序；
206、308、408 ~ "交接至UTRAN完成"訊息；
301 ~ UMTS AKA伺服器；
305 ~ UMTS確證請求；
306 ~ UMTS確證回應；
401 ~ GSM AKA伺服器；
405 ~ GSM確證請求；
406 ~ GSM確證回應。

六、英文發明摘要 （發明名稱：CIPHERING ACTIVATION DURING AN INTER-RAT HANDOVER PROCEDURE）

that the security START value equals or exceeds a THRESHOLD value, the UTRAN disables ciphering with the wireless device when performing a HANDOVER TO UTRAN procedure. Similarly, the wireless device disables ciphering when performing the HANDOVER TO UTRAN procedure if the START value equals or exceeds the THRESHOLD value. Alternatively, a new ciphering key set is generated while the wireless