



(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I507059 B

(45)公告日：中華民國 104 (2015) 年 11 月 01 日

(21)申請案號：098114361

(22)申請日：中華民國 98 (2009) 年 04 月 30 日

(51)Int. Cl. : *H04W36/18 (2009.01)*
*H04L29/06 (2006.01)**H04W12/06 (2009.01)*

(30)優先權：	2008/04/30	美國	61/048,965
	2008/05/09	美國	61/051,819
	2008/05/14	美國	61/053,041
	2009/04/30	美國	12/432,841

(71)申請人：聯發科技股份有限公司 (中華民國) MEDIATEK INC. (TW)

新竹市新竹科學工業園區篤行一路 1 號

(72)發明人：吳怜儀 WU, LIN YI (TW)；李吉真 LEE, CHI CHEN (TW)；傅宜康 FU, IKANG (TW)

(74)代理人：洪澄文；顏錦順

(56)參考文獻：

TW 200708131A

WO 2007/046630A2

審查人員：李京歡

申請專利範圍項數：23 項 圖式數：13 共 54 頁

(54)名稱

行動台、基地台及流量加密密鑰之產生方法

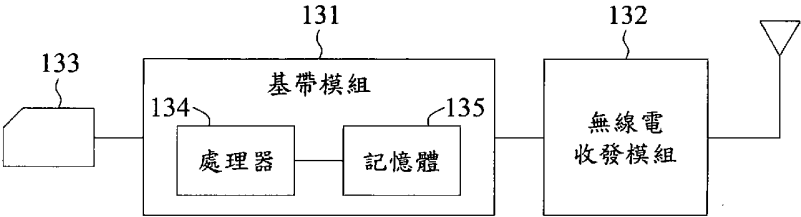
MOBILE STATION AND BASE STATION AND METHOD FOR DERIVING TRAFFIC ENCRYPTION KEY

(57)摘要

本發明提供一種行動台、基地台及流量加密密鑰之產生方法。其中，行動台包含一個或多個無線電收發模組與處理器。處理器與服務基地台執行交遞協商程序，經由無線電收發模組發送和接收多個交遞協商消息，以交遞通信服務至目標基地台，並產生認證密鑰與相關內文，為目標基地台推導出至少一流量加密密鑰，認證密鑰與相關內文包含與目標基地台共享之多個密鑰，用以對發送至目標基地台之多個消息進行加密，流量加密密鑰為與目標基地台共享之密鑰，用以對流量資料進行加密。利用本發明可實現無間隙之交遞，避免流量資料傳送之長時間中斷，提高通信服務品質。

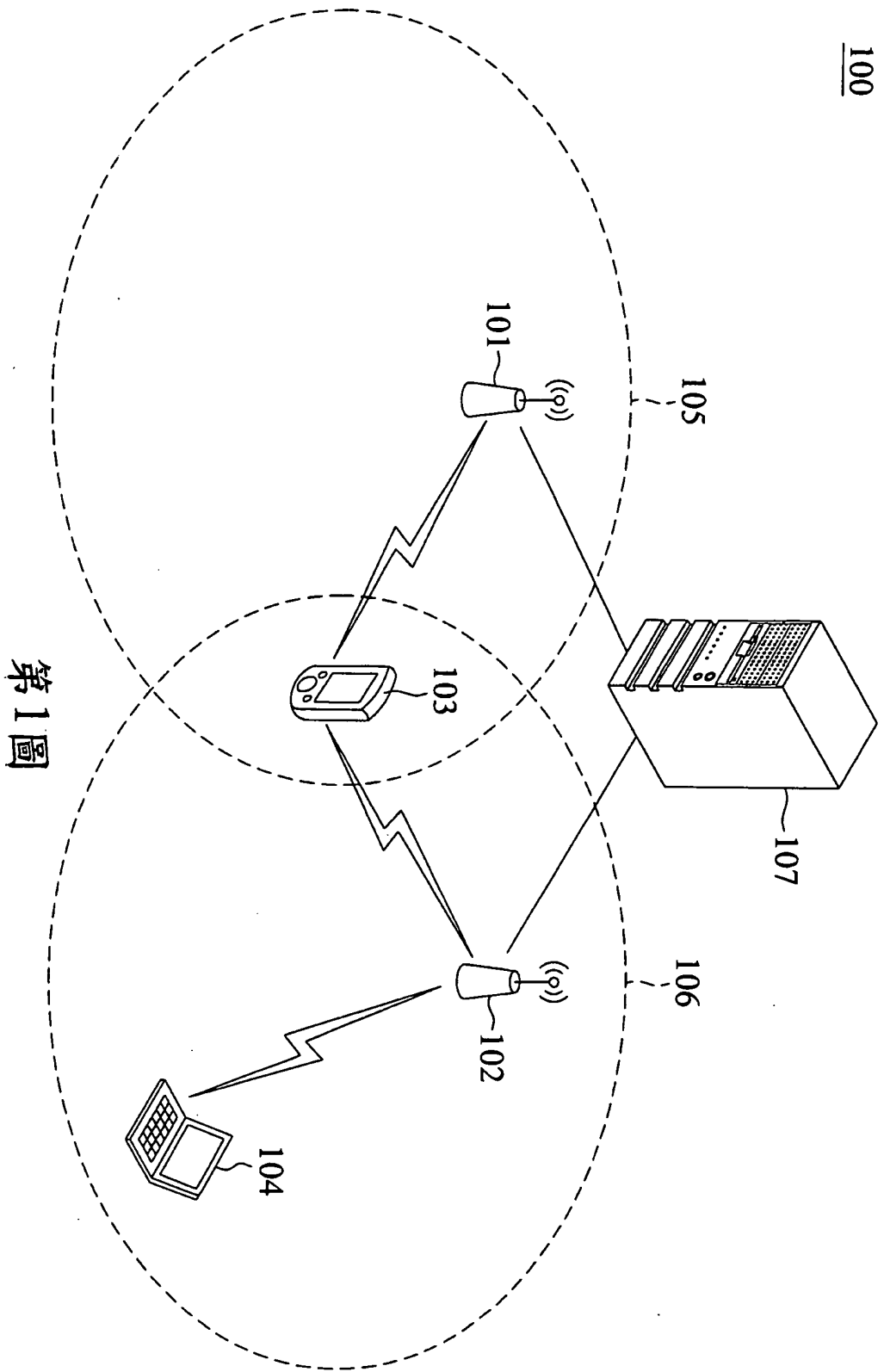
A mobile station is provided. The mobile station includes one or more radio transceiver module and a processor. The processor performs a handover negotiation procedure with a serving base station so as to handover communication services to a target base station by transmitting and receiving a plurality of handover negotiation messages via the radio transceiver module, and generates an Authorization Key (AK) context and derives at least one Traffic Encryption Key (TEK) for the target base station. The AK context includes a plurality of keys shared with the target base station for encrypting messages to be transmitted to the target base station, and the TEK is a secret key shared with the target base station for encrypting traffic data.

103



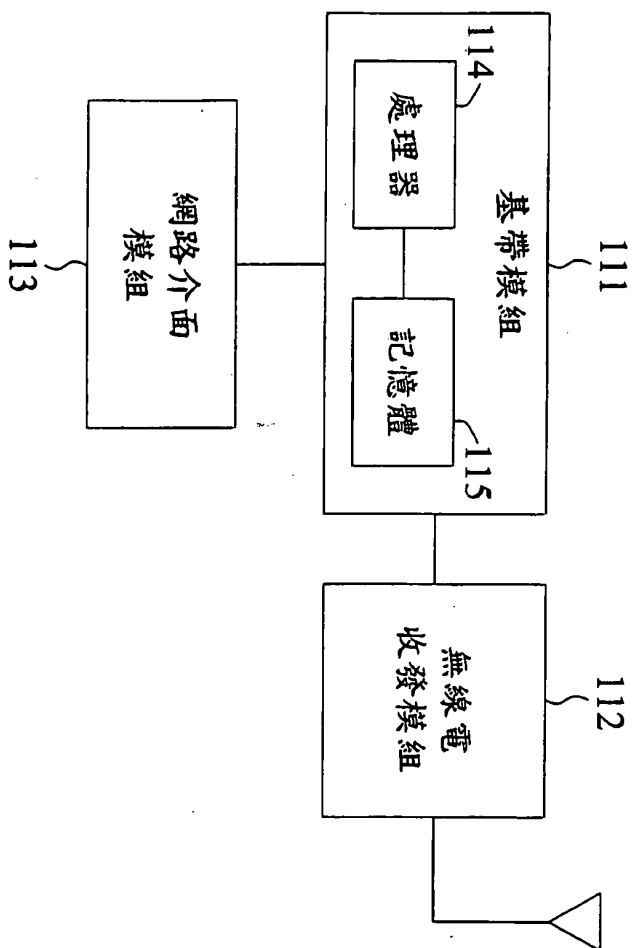
- 103 . . . 行動台
- 131 . . . 基帶模組
- 132 . . . 無線電收發模組
- 133 . . . 用戶識別卡
- 134 . . . 處理器
- 135 . . . 記憶體

第3圖



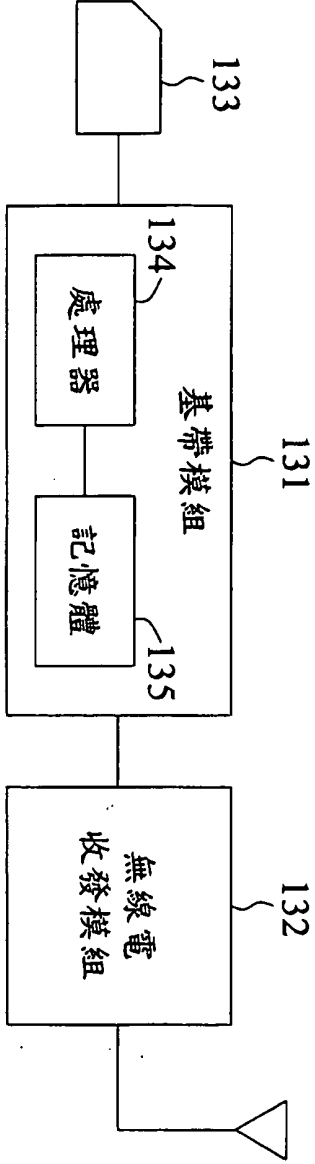
第1圖

101

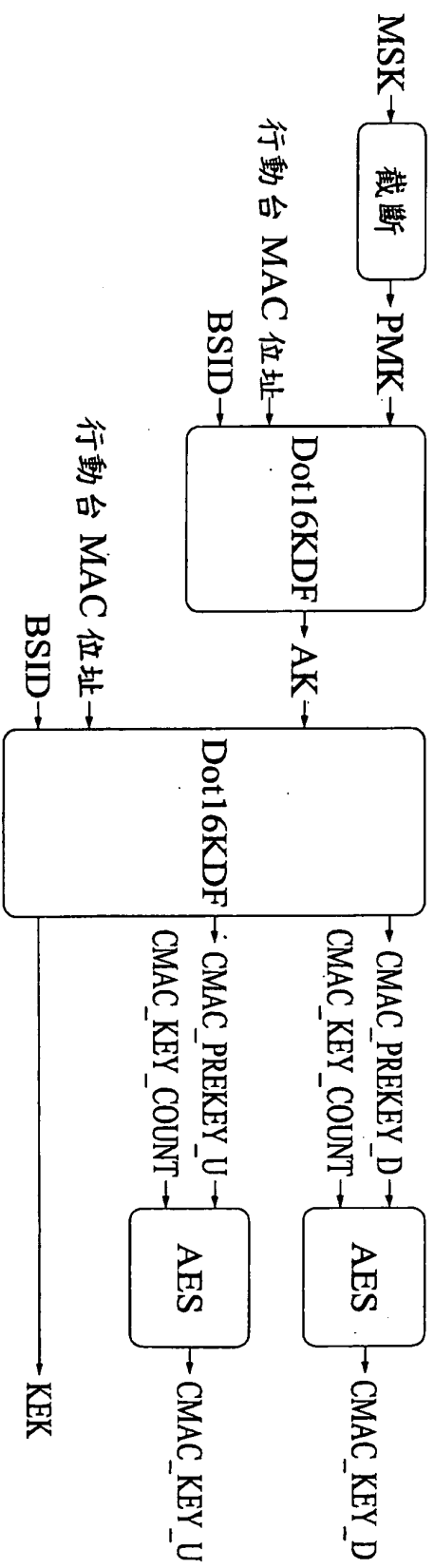


第2圖

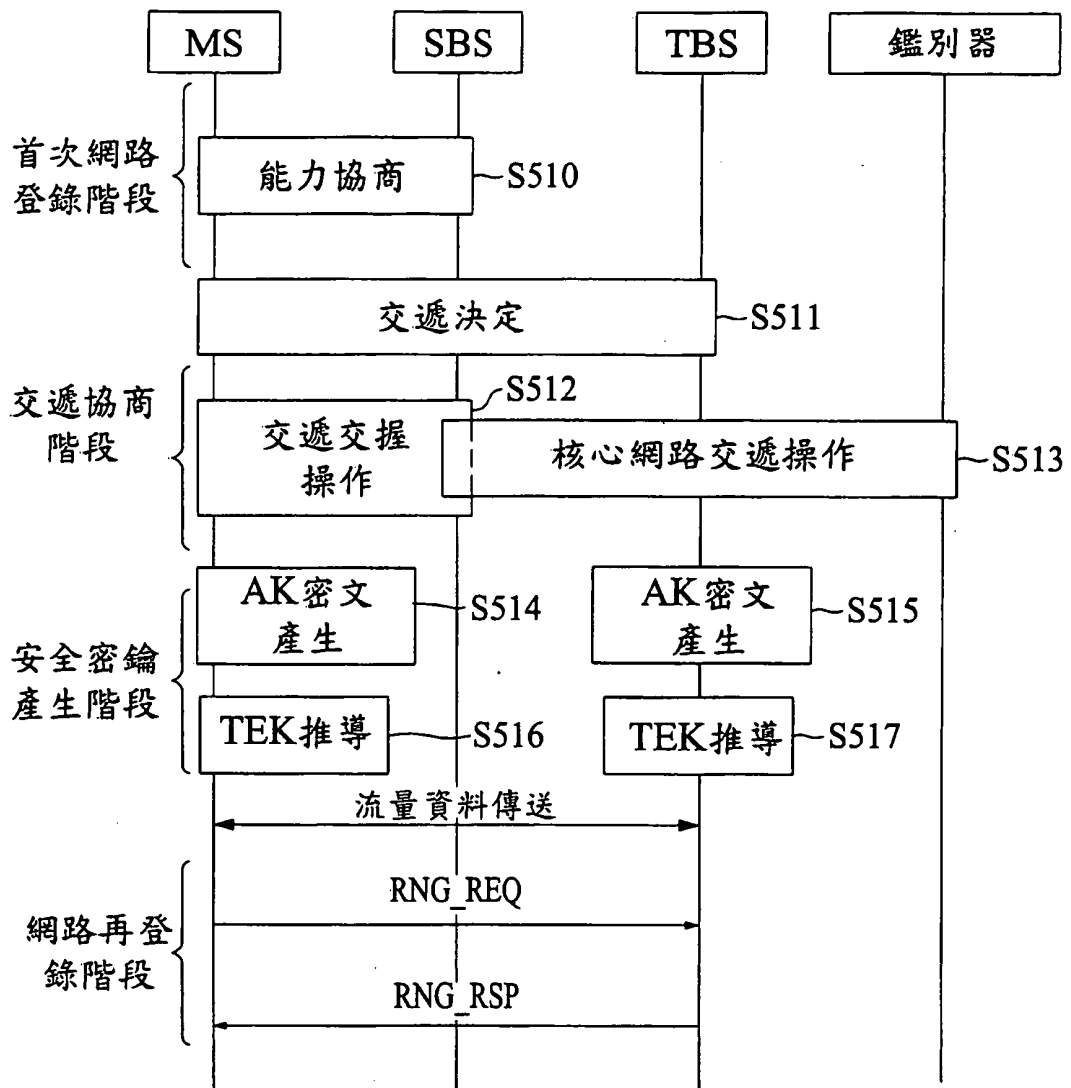
103



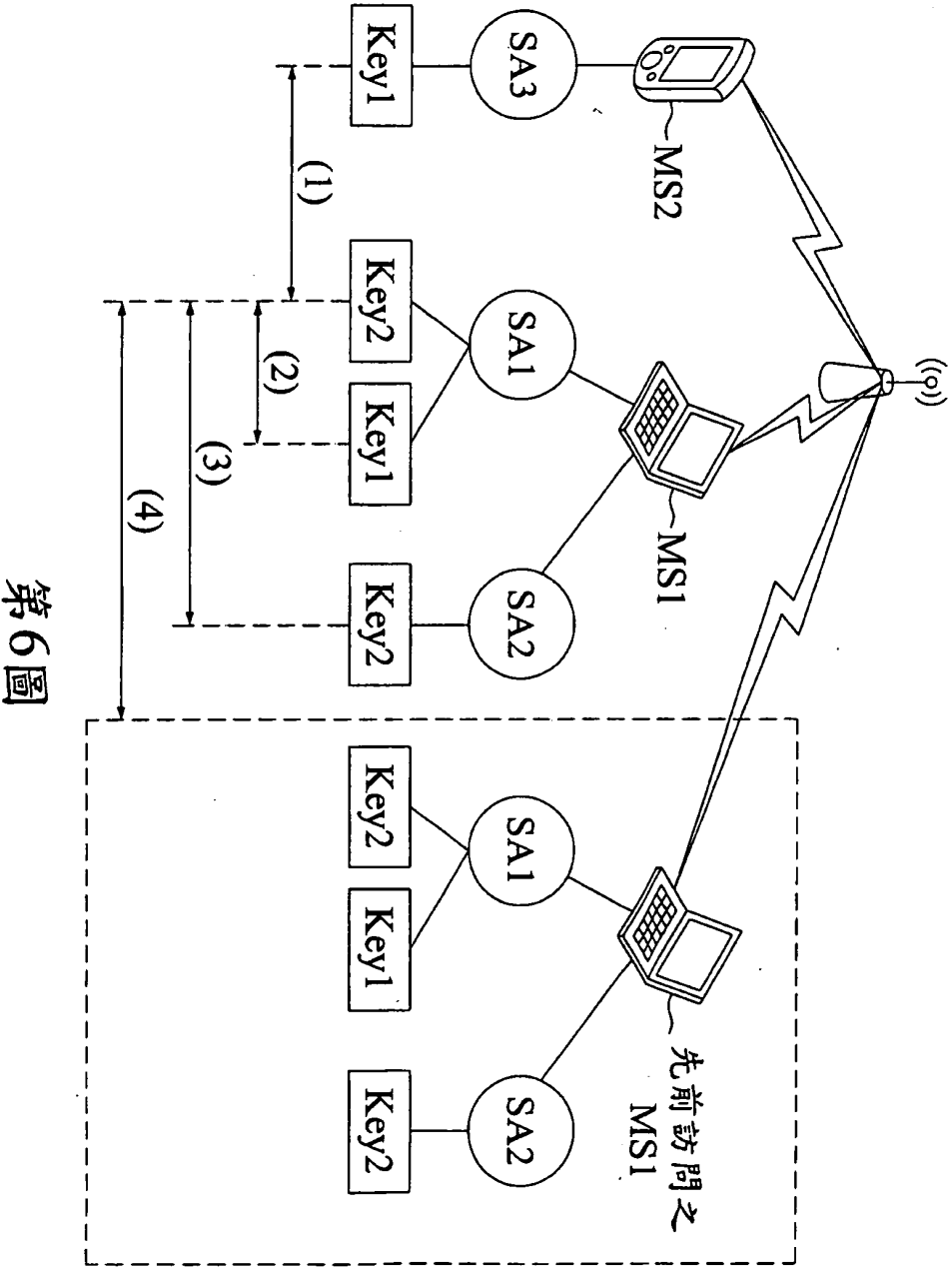
第3圖



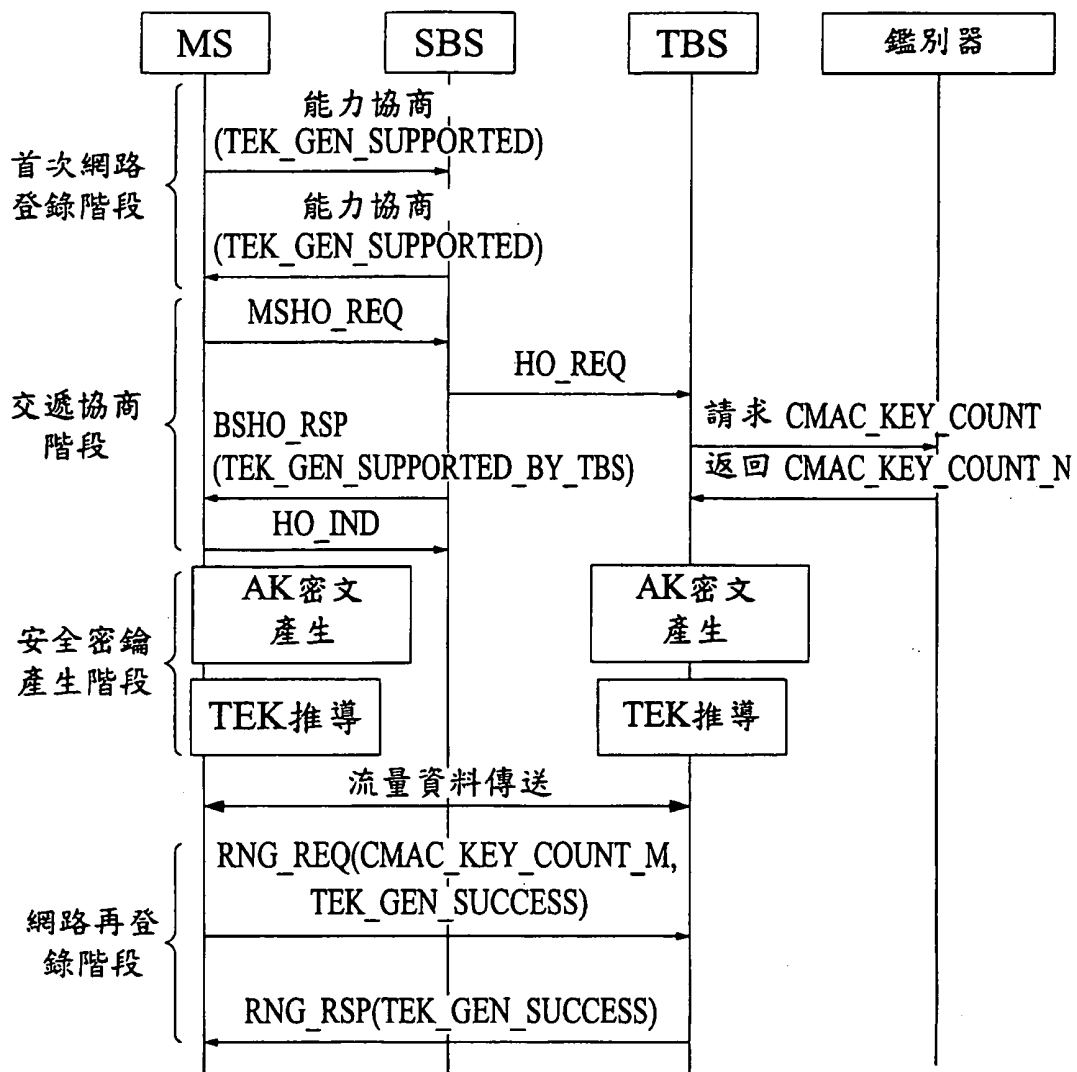
第4圖



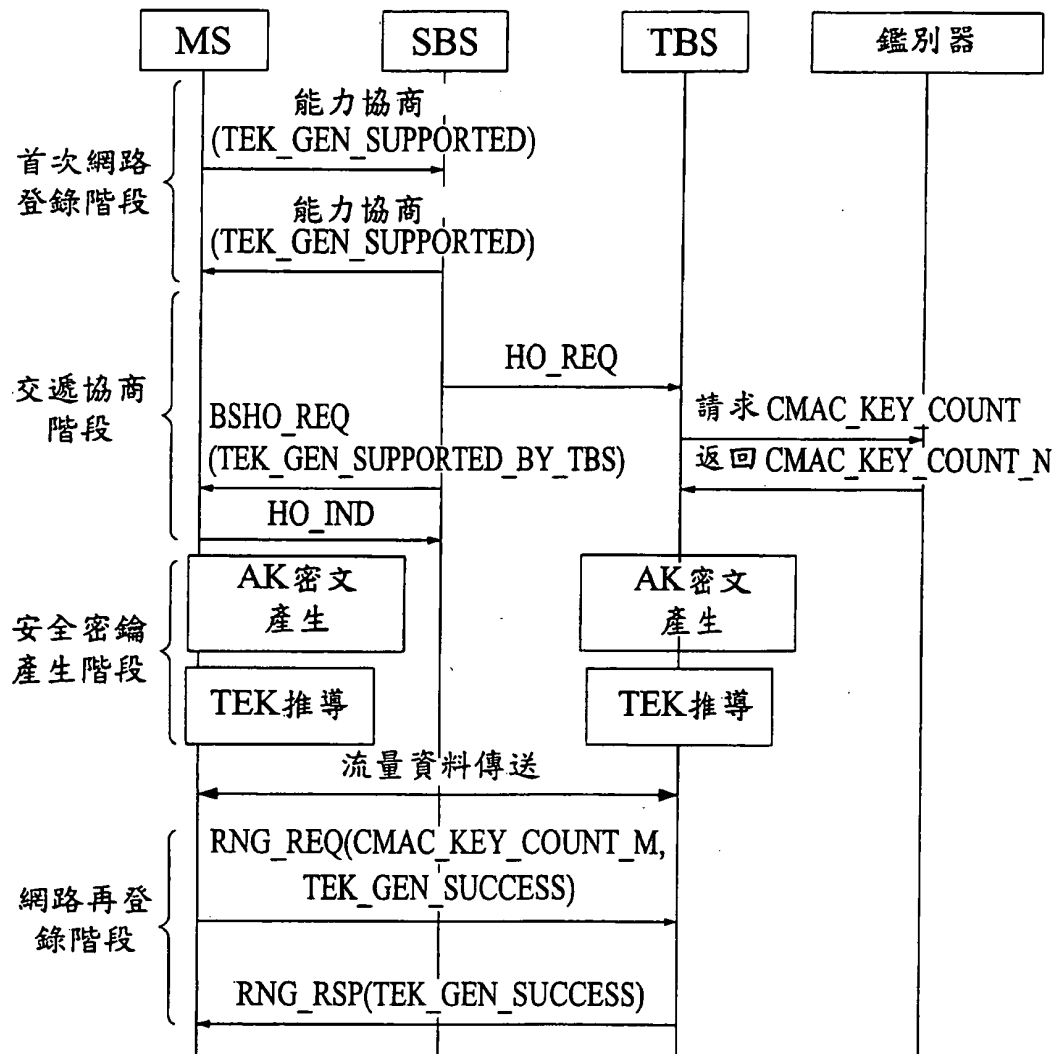
第5圖



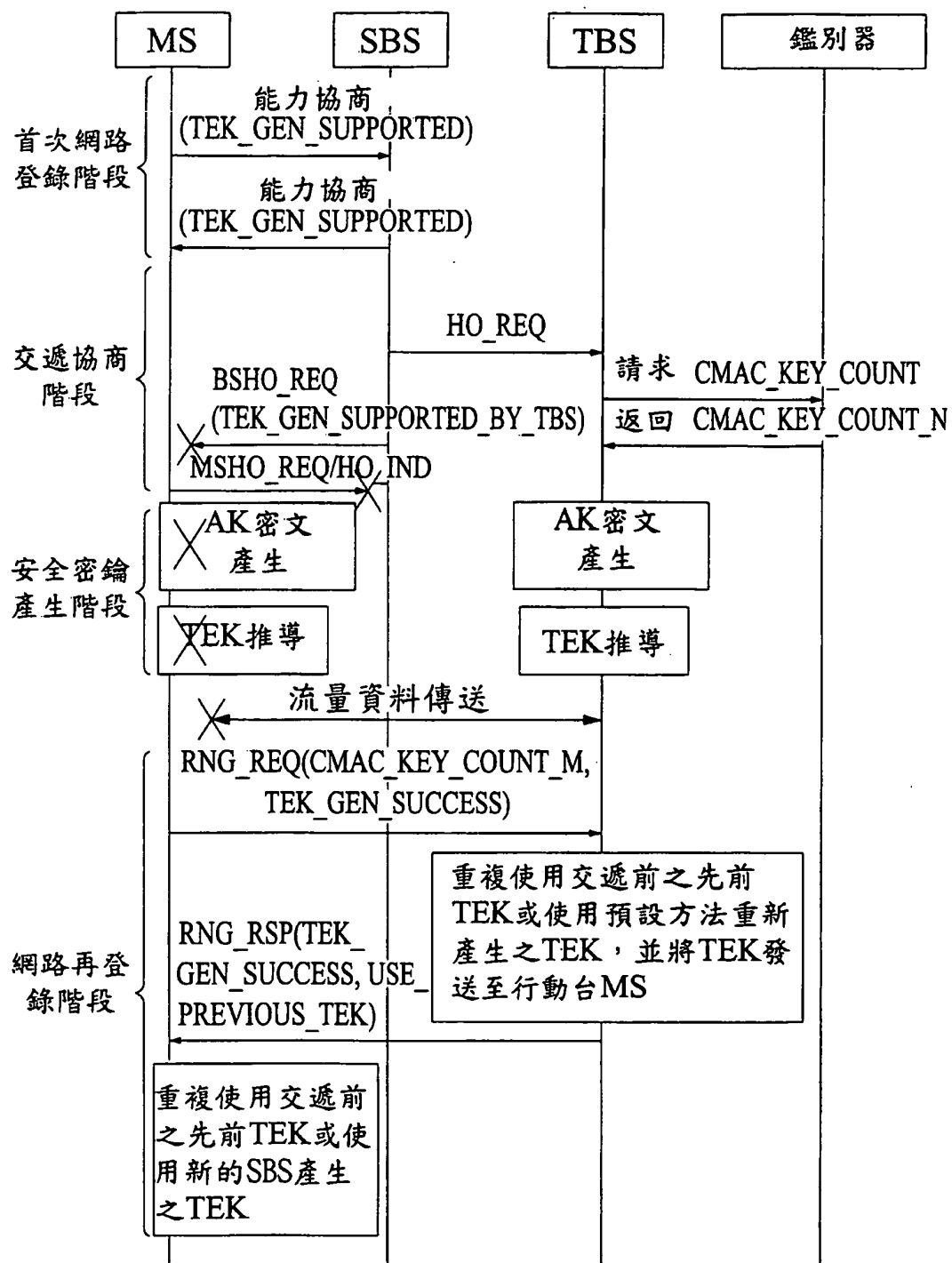
第6圖



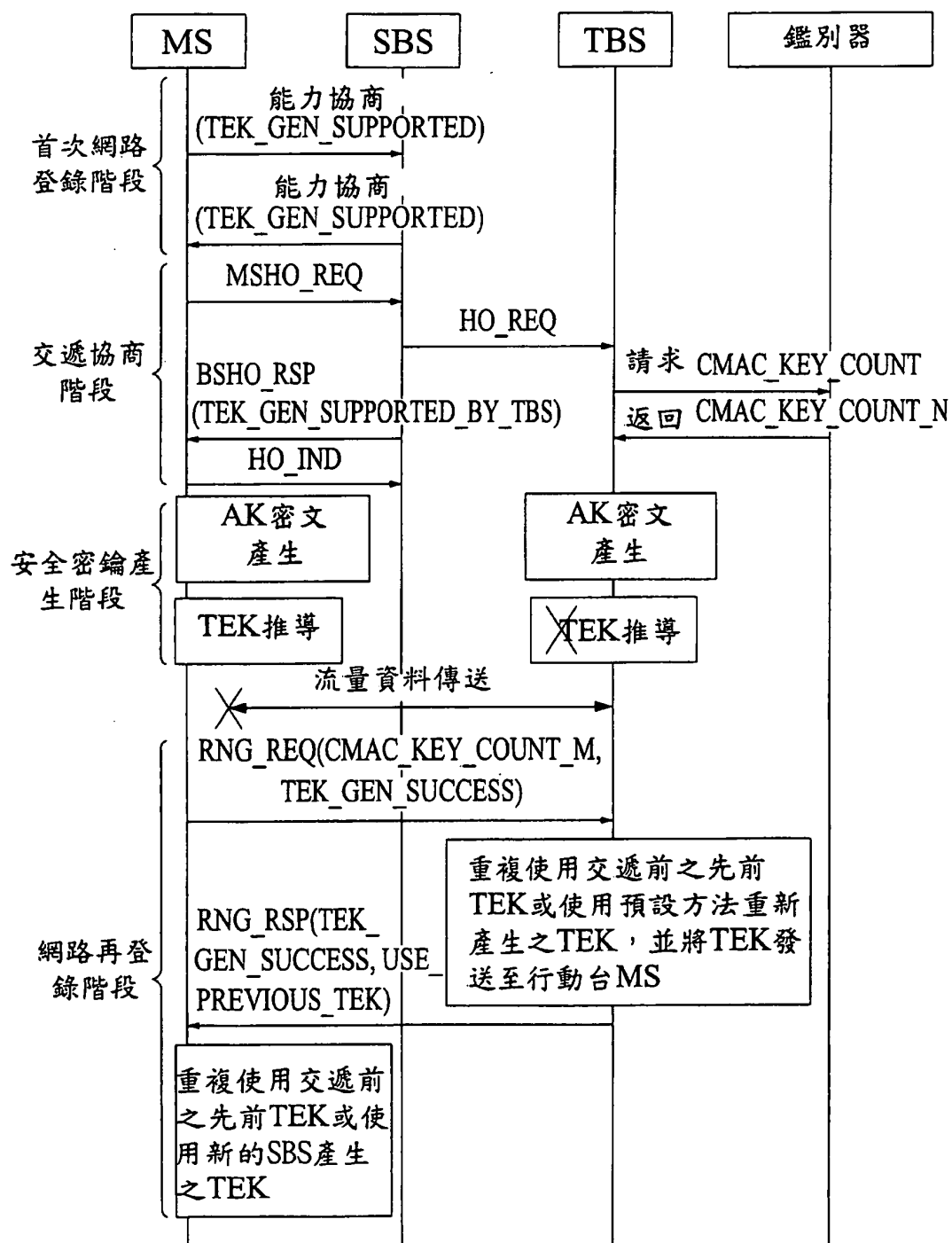
第7圖



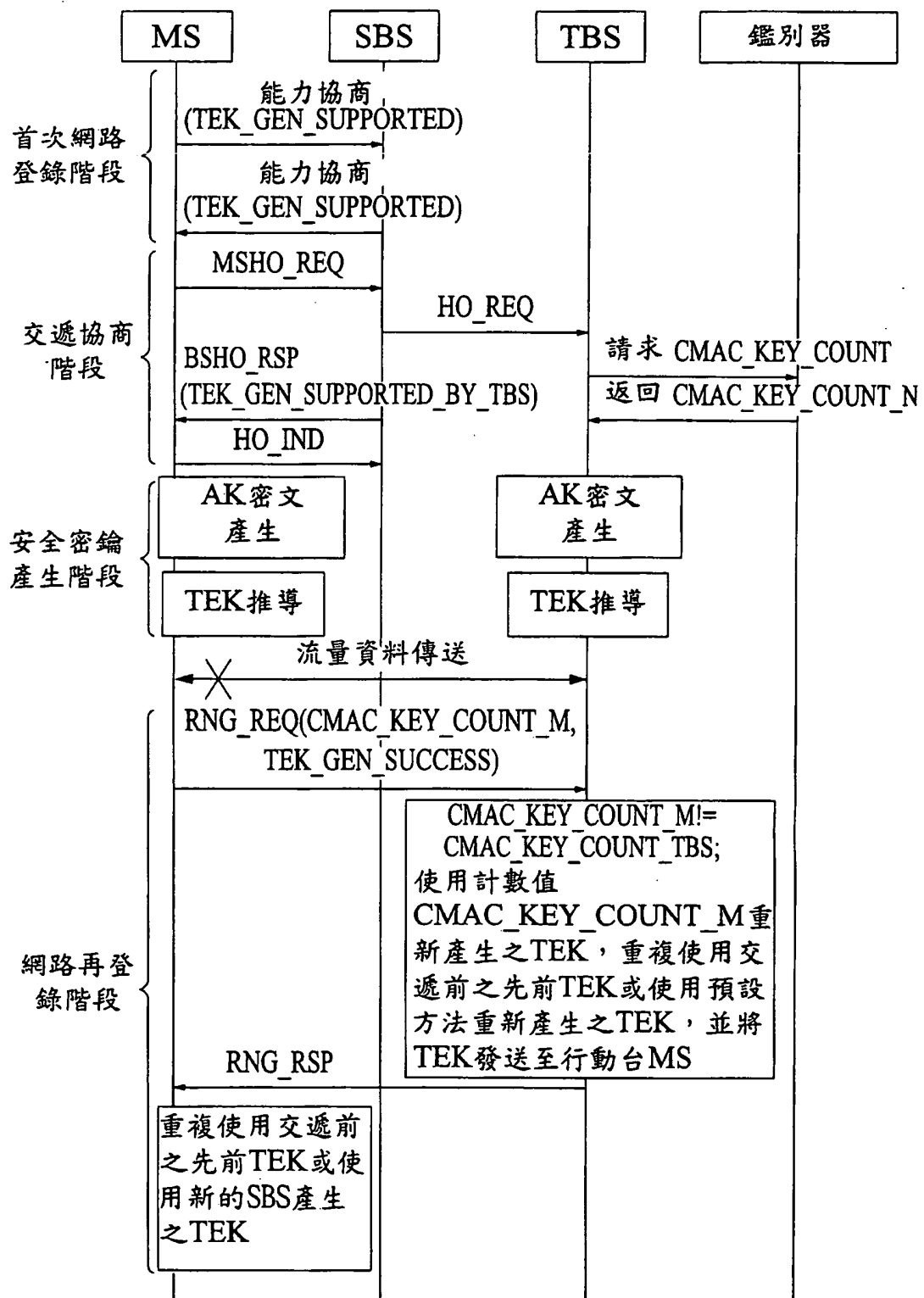
第8圖



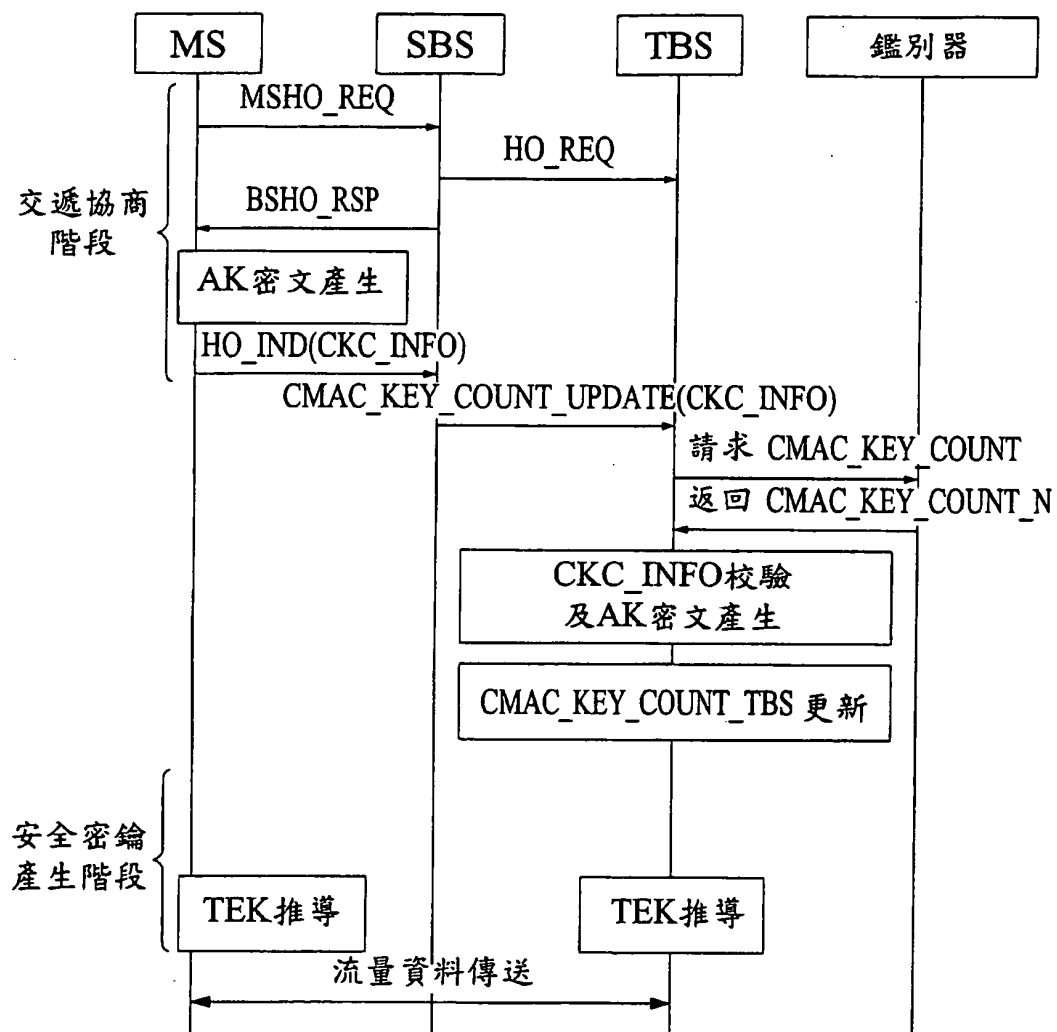
第9圖



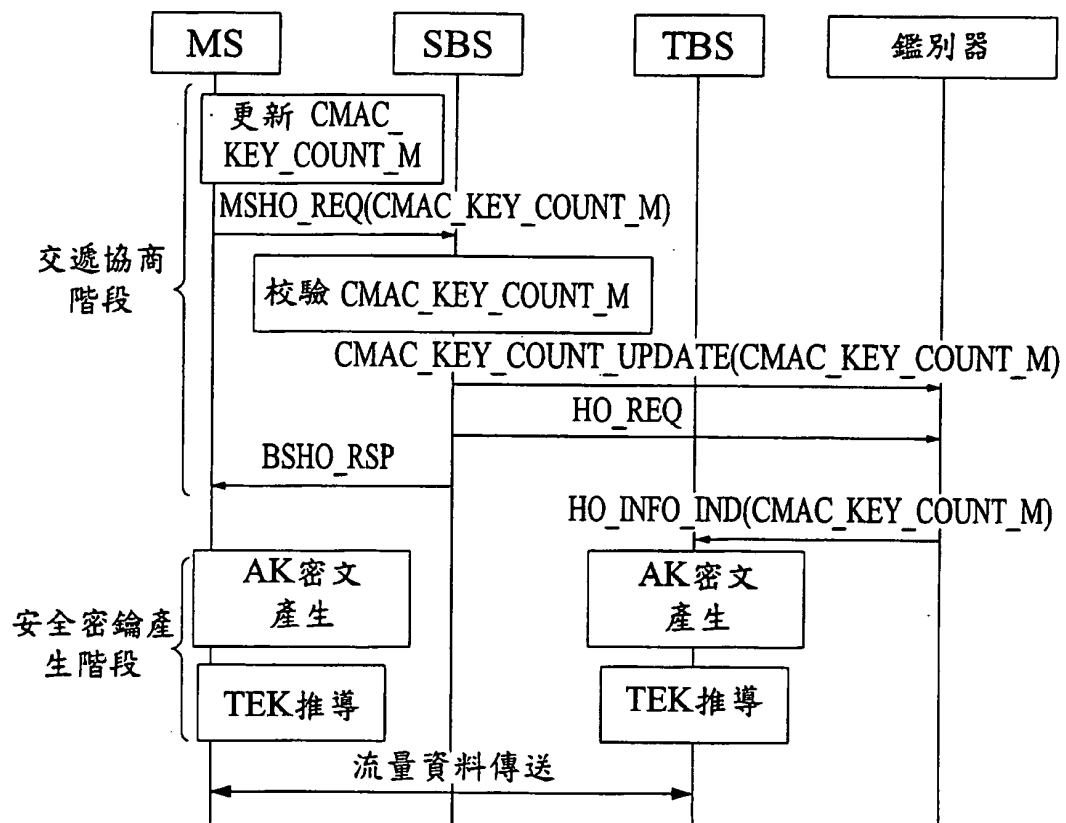
第10圖



第11圖



第12圖



第13圖

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種流量加密密鑰(Traffic Encryption Key, TEK)之產生(deriving)方法，更具體地，是關於一種無間隙(seamless)交遞(handover)程序中之 TEK 之產生方法。

【先前技術】

在無線通信系統中，基地台(Base Station, BS)為位於一個地理區域內之多個終端提供多項服務。通常地，基地台在空氣介面(air interface)中廣播資訊，以輔助終端識別必要系統資訊與服務配置，從而使行動台能夠獲取必要之網路登錄資訊(network entry information)，並提供是否使用基地台所提供之多項服務之決定資訊。

在全球互通微波存取 (Worldwide Interoperability for Microwave Access, 簡稱 WiMAX) 通信系統中，或適用 IEEE802.16 及類似系統中，若資料加密在基地台與終端之間進行協商(negotiated)，則允許在 TEK 產生之後再發送流量資料。TEK 是一種密鑰，用於對流量資料進行加密和解密。基地台隨機產生 TEK，藉由密鑰加密密鑰 (Key Encryption Key, 簡稱 KEK) 對 TEK 進行加密，並將加密後的 TEK 分配至終端。KEK 也是一種密鑰，且 KEK 為終端與基地台所共享。KEK 是由終端與基地台根據預設算法所各別產生。當接收到來自於基地台之加密後的 TEK 後，終端藉由 KEK 對 TEK 進行解密。當獲取 TEK 後，終端藉

由 TEK 對流量資料進行加密，並將加密後的流量資料發送至基地台。

根據傳統技術，在最佳化交遞(handover)程序中，當目標基地台(target base station，簡稱 TBS)接收到來自終端之範圍請求消息(ranging request message)後產生 TEK，並經由範圍回應消息(ranging response message)以加密後的 TEK 來回應終端。然而，在交遞消息被發送後直至 TEK 被接收及解密這一時段內，流量資料之傳送不可避免地被中斷。長時間之中斷嚴重降低了通信服務之品質。因此，需要一種新的 TEK 產生方法及大致上無間隙(seamless)之交遞程序。

【發明內容】

有鑒於此，本發明提供一種行動台(Mobile Station，MS)、一種基地台及一種 TEK 之產生方法，避免傳統交遞過程中因行動台與基地台之間傳遞密鑰而造成流量資料傳送長時間中斷，從而實現無間隙之交遞。

根據本發明一實施例之行動台包含無線電收發模組與處理器。處理器與服務基地台執行交遞協商程序，經由無線電收發模組發送和接收多個交遞協商消息，以交遞多項通信服務至目標基地台，以及產生認證密鑰與相關內文(Authorization Key context，簡稱 AK 與相關內文)，並為目標基地台產生至少一 TEK，其中，AK 與相關內文包含與目標基地台共享之多個密鑰，用以對發送至目標基地台之多個消息進行加密，以及 TEK 為與目標基地台共享之

密鑰，用以對流量資料進行加密而無需密鑰分配。

根據本發明一實施例之 TEK 之產生方法，用於產生無線通信網路中之行動台與基地台之間所共享之至少一 TEK，而無需密鑰分配，該 TEK 之產生方法包含：獲取行動台與基地台之間所共享之至少一密鑰與資訊；以及根據該資訊與該至少一密鑰，經由預設函數產生 TEK。

根據本發明一實施例之無線通信網路中之基地台包含網路介面模組、一個或多個無線電收發模組及處理器。處理器經由網路介面模組接收交遞指示消息，交遞指示消息來自於無線通信網路中之網路裝置，當接收到交遞指示消息後，處理器產生 AK 與相關內文，並為行動台產生至少一 TEK，處理器經由無線電收發模組接收來自於行動台之認證消息，並根據接收到的認證消息對基地台所產生之 TEK 與行動台所產生之 TEK 之一致性進行校驗。交遞指示消息係為一消息，用於指示行動台中由網路裝置所提供且欲傳送至基地台之通信服務，認證消息係為一消息，用於認證行動台之身份，以及 TEK 係為與行動台所共享之密鑰，用於對流量資料進行加密。

利用本發明所提供之行動台、基地台及 TEK 之產生方法，能夠實現無間隙之交遞，避免了流量資料傳送之長時間中斷，從而提高了通信服務品質。

以下係根據多個圖式對本發明之較佳實施例進行詳細描述，本領域習知技藝者閱讀後應可明確了解本發明之目的。

【實施方式】

以下描述之實施例僅用來例舉本發明之實施態樣，以及闡釋本發明之技術特徵，並非用來限制本發明之範疇。任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利範圍應以申請專利範圍為準。

第 1 圖所示為根據本發明一實施例之無線通信系統之網路拓撲示意圖。如第 1 圖所示，無線通信系統 100 包含位於一個或多個區段(如第 1 圖所示之區段 105 與區段 106)中之一個或多個基地台(如第 1 圖所示之基地台 101 與基地台 102)，基地台 101 與基地台 102 對無線通信信號進行接收、發送、中繼(repeat)等操作，並互相提供多項服務以及/或者提供多項服務至一個或多個行動台(如第 1 圖所示之行動台 103 與行動台 104)。無線通信系統 100 更包含位於基幹網路(backbone network)中之一個或多個網路裝置(如第 1 圖所示之網路裝置 107)，其中，基幹網路也稱為核心網路(Core Network，簡稱 CN)，網路裝置 107 與多個基地台(如第 1 圖所示之基地台 101 與基地台 102)進行通信，用於為多個基地台提供並維持多項服務。根據本發明之一實施例，行動台(如第 1 圖所示之行動台 103 與行動台 104)可為行動電話、計算機(computer)、筆記型電腦、個人數位助理(簡稱 PDA)、用戶端設備(Customer Premises Equipment, CPE)等，然本發明並不以此為限。基地台 101 與基地台 102 可連接至主從式無線網路(infrastructure network)(例如，網際網路 Internet)，從而

提供與 Internet 之連接。根據本發明之一實施例，基地台 101 與基地台 102 可支持對等式(peer-to-peer)通信服務(例如，行動台 103 與行動台 104 之間可直接進行通信)。根據本發明之該實施例，無線通信系統 100 可配置為 WiMAX 通信系統，或採用基於一個或多個由 IEEE802.16 相關標準系列定義之規格書之技術。

第 2 圖所示為根據本發明一實施例之基地台 101 之示意圖。基地台 101 可包含基帶模組 111、一個或多個無線電收發模組 112 及網路介面模組 113。無線電收發模組 112 可包含一個或多個天線、接收器鍊接(receiver chain)及發送器鍊接(transmitter chain)，其中，接收器鍊接接收無線頻率信號並將接收到的無線頻率信號轉換為基帶信號，以傳送至基帶模組 111 進行處理，以及發送器鍊接接收來自於基帶模組 111 之基帶信號，並將接收到的基帶信號轉轉為無線頻率信號，以發送至空氣介面。無線電收發模組 112 可包含用於執行無線電頻率轉換之多個硬體裝置。網路介面模組 113 耦接於基帶模組 111，並用以與基幹網路中之網路裝置(如第 1 圖所示之網路裝置 107)進行通信。基帶模組 111 更將基帶信號轉換為多個數位信號，並對該多個數位信號進行處理；反之亦然，基帶模組 111 亦可將多個數位信號轉換為基帶信號。基帶模組 111 也可包含用於執行基帶信號處理之多個硬體裝置。基帶信號處理可包含類比至數位轉換(簡稱 ADC)/數位至類比轉換(簡稱 DAC)、增益調整、調變/解調、編碼/解碼等等。基帶模組 111 更包含處理器 114 與記憶體 115。為使行動台 103 與行動台 104

能夠訪問(access)基地台 101 與基地台 102 及使用所提供之服務，或者為將頻譜應用於無線通信，基地台 101 與基地台 102 廣播某些系統資訊。記憶體 115 可儲存基地台 101 之系統資訊，並進一步儲存多個軟體/韌體代碼和/或指令以提供及維持無線通信服務。處理器 114 執行儲存在記憶體 115 中之代碼和/或指令，並控制記憶體 115、基帶模組 111 及無線電收發模組 112 之運作。

第 3 圖所示為根據本發明一實施例之行動台 103 之示意圖。行動台 103 可包含基帶模組 131 及一個或多個無線電收發模組 132，並選擇性地包含用戶識別卡 133。無線電收發模組 132 接收無線頻率信號，並將接收到的無線頻率信號轉換為基帶信號，以傳送至基帶模組 131 進行處理，或者無線電收發模組 132 接收來自基帶模組 131 之基帶信號，並將接收到的基帶信號轉換為無線頻率信號，以傳送至同級裝置。無線電收發模組 132 可包含用於執行無線電頻率轉換之多個硬體裝置。例如，無線電收發模組 132 可包含一混頻器，該混頻器將基帶信號與載波信號相乘，其中，載波信號係於無線通信系統之無線頻率處振盪產生。基帶模組 131 更將基帶信號轉換為多個數位信號，並處理該多個數位信號；反之亦然，基帶模組 131 亦可將多個數位信號轉換為基帶信號。基帶模組 131 也可包含用於執行基帶信號處理之多個硬體裝置。基帶信號處理可包含類比至數位轉換（簡稱 ADC）/數位至類比轉換（簡稱 DAC）、增益調整、調變/解調等等。基帶模組 131 更包含記憶體裝置 135 及處理器 134。記憶體 135 可儲存多個軟體/韌體代

碼和/或指令，用以維持行動台之運作。需要注意，記憶體裝置 135 也可配置於基帶模組 131 之外部，本發明並不僅限於此。處理器 134 執行儲存在記憶體 135 中之代碼和/或指令，並分別控制基帶模組 131、無線電收發模組 132 及插入行動台 103 中之用戶識別卡 133 之運作。當行動台 103 中包含用戶識別卡 133 且用戶識別卡 133 插入行動台 103 中時，處理器 134 可從用戶識別卡 133 中讀取資料及向用戶識別卡 133 中寫入資料。請注意，行動台 103 也可包含其他類型之識別模組，來取代用戶識別卡 133，本發明並不僅限於此。

根據 WiMAX 標準所定義之多個協議，包括 IEEE802.16、802.16d、802.16e、802.16m 及相關協議，基地台與終端（也稱為行動台）經由認證程序識別通信方。舉例而言，認證程序可藉由基於延伸驗證協定（Extensible Authentication Protocol，簡稱 EAP）之認證進行處理。當認證後，行動台與基地台分別產生 AK 與相關內文，以作為共享密鑰用於加密與完整性保護。AK 與相關內文包含用於消息完整性保護之多個密鑰。第 4 圖所示為根據本發明一實施例之 AK 與相關內文產生程序之示意圖。首先，經由基於 EAP 之認證產生一主會談密鑰（Master Session Key，簡稱 MSK）。MSK 係為行動台與基地台所共享之特定密鑰。MSK 被截斷(truncated)以產生成對主密鑰（Pairwise Master Key，簡稱 PMK），接著，根據 PMK、行動台媒體存取控制層（Media Access Control layer，簡稱 MAC）位址及基地台識別碼（Base Station Identifier，簡稱

BSID) 經由 Dot16KDF 操作產生 AK。然後，根據 AK、行動台 MAC 位址及 BSID，經由 Dot16KDF 操作產生兩個預備密鑰(pre-key)(如第 4 圖所示之密鑰 CMAC_PREKEY_D 與密鑰 CMAC_PREKEY_U) 及 KEK。KEK 也是行動台與基地台所共享之密鑰，用以對 TEK 進行加密。最後，根據預備密鑰(密鑰 CMAC_PREKEY_D 與密鑰 CMAC_PREKEY_U) 及計數值 CMAC_KEY_COUNT，並經由高階加密標準(Advanced Encryption Standard，簡稱 AES)，分別產生兩個消息認證密鑰(如第 4 圖所示之密鑰 CMAC_KEY_D 與密鑰 CMAC_KEY_U)，用以保護上行鏈路與下行鏈路管理消息之完整性。計數值 CMAC_KEY_COUNT 用於將新產生之加密消息認證碼(Cipher Message Authentication Code，簡稱 CMAC)密鑰區別於先前已有之 CMAC 密鑰。例如，每當行動台從一個服務行動台所覆蓋之區域移動至由目標基地台所覆蓋之區域，並執行交遞以將通信服務由服務基地台傳送至目標基地台時，計數值 CMAC_KEY_COUNT 增大，以回應上述新密鑰之產生，從而確保密鑰之更新。

在 WiMAX 通信系統中，基地台可為行動台建立多條服務流(service flows)。為了保護每條服務流中之流量資料傳送，當網路登錄後，行動台與基地台之間協商一個或多個安全群組(Security Association，SA)。SA 藉由一個 SA 識別碼(SA identifier，簡稱 SAID)來識別，且 SA 描述了用於流量資料進行加密和解密之密碼演算法。舉例而言，SA 可於 SA-TEK 三向交握(3-way handshake)階段進行協

商。行動台可於請求消息 SA-TEK-REQ 中將行動台之能力 (capability) 告知基地台，以及基地台所建立之 SA (包含 SAID) 可承載於回應消息 SA-TEK-RSP 中，以發送至行動台。請注意，行動台也可經由本領域習知技藝者所了解之其他特定方式來獲取 SA，本發明並不以此為限。對於每個 SA，產生行動台與基地台所共享之一個或多個 TEK，以作為密碼函數中之加密密鑰及解密密鑰。在 IEEE 802.16e 中，基地台隨機產生多個 TEK，並以一種安全之方式分配給行動台。然而，如前所述，當交遞請求消息發送後直至 TEK 被接收並解密這一時段內，資料傳送不可避免地發生中斷，其中，長時間之中斷嚴重降低了通信服務之品質。因此，根據本發明之實施例，提供了一種新的 TEK 產生方法及大致上無間隙之交遞程序。

第 5 圖所示為根據本發明一實施例之首次網路登錄與交遞操作程序之示意圖。如圖所示，基地台 SBS(serving BS) 為服務基地台 (例如，第 1 圖所示之基地台 101)，最初服務於行動台 MS (例如，第 1 圖所示之行動台 103)，基地台 TBS(target BS) 為目標基地台 (例如，第 1 圖所示之基地台 102)，行動台計劃將通信服務交遞至基地台 TBS，以及鑑別器 (Authenticator) 可為基幹網路中之一個網路裝置 (如第 1 圖所示之網路裝置 107)，用以儲存與安全相關之資訊並處理通信系統中與安全相關之程序。下文將詳細說明所提出之 TEK 產生方法與交遞程序在如第 5 圖所示之首次網路登錄階段、交遞協商階段、安全密鑰產生階段及網路再登錄階段之運作。需要注意，簡潔起見，此處僅

對所提出之方法與程序所涉及之階段與程序進行說明。本領域具有通常知識者能夠輕易了解第 5 圖中未說明之階段與程序，本發明並不以此為限。因此，在不脫離本發明之精神與範疇之情形下，任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利範圍應以申請專利範圍為準。

根據本發明之實施例，與先前基地台 TBS 隨機產生 TEK 之方法不同，當 SA 建立後，行動台 MS 與基地台 TBS 可分別產生 TEK，且在進入網路再登錄階段之前，行動台 MS 與基地台 TBS 之間不存在消息交換。舉例而言，在第 5 圖所示之步驟 S516 與步驟 S517 中，行動台 MS 與基地台 TBS 可分別產生 TEK。根據本發明之該實施例，TEK 可根據 TEK 推導(derivation)函數來產生，以確保 TEK 之唯一性。第 6 圖所示為根據本發明一實施例之說明 TEK 產生模型之通信網路之示意圖。為了確保 TEK 之唯一性，最好保證新產生之 TEK 不同於(1)連接至相同基地台 TBS 之其他行動台之 TEK (如第 6 圖所示，行動台 MS2 之 SA3 中之 Key1 不同於 MS1 之 SA1 中之 Key2)，(2)相同行動台 MS 之相同 SA 之先前 TEK (如第 6 圖所示，在行動台 MS1 之 SA1 中，Key2 不同於 Key1)，(3)相同行動台 MS 之其他 SA 之 TEK (如第 6 圖所示，在行動台 MS1 中，SA1 中之 Key1 與 Key2 均不同於 SA2 中之 Key2)，以及(4)先前訪問該基地台 TBS 之相同行動台 MS 之相同 SA 之 TEK (如第 6 圖所示，在行動台 MS1 中，當前訪問建立之 SA1 之 Key1 與 Key2 不同於先前訪問時建立之 SA1 之 Key1 與

Key2，當前訪問建立之 SA2 之 Key2 亦不同於先前訪問時建立之 SA2 之 Key2)。根據本發明之一實施例，為了滿足上述四個需求，TEK 最好根據行動台 MS 與基地台 TBS 所共享之至少一密鑰、及行動台 MS 與基地台 TBS 之已知資訊來產生。例如，根據本發明之該實施例，TEK 推導可設計為：

$$\text{TEK} = \text{Function}(\text{KEK}, \text{Sequence Number}, \text{SAID}, \text{CMAC_KEY_COUNT}) \quad \text{Eq.1}$$

Eq.1 所代表之函數使用了四個輸入參數 KEK，Sequence Number，SAID 與 CMAC_KEY_COUNT 來產生新的 TEK。輸入參數 KEK 為基地台與行動台所共享之至少一密鑰，以確保在某個時刻相同基地台中對應不同行動台的 TEK 不同。由於一個特定行動台之 KEK 不同於連接至相同基地台之其他行動台之 KEK，因此，KEK 可用於區分連接至相同基地台之不同行動台。輸入參數 Sequence Number 為一個計數值，每當產生一個新的 TEK 時該計數值增大，以確保對於同一個 SA，新產生之 TEK 不同於先前已存在之 TEK。根據本發明之一實施例，基地台 TBS 可重置行動台 MS 之參數 Sequence Number，並使其在第 5 圖所示之 TEK 推導步驟 S516 與 S517 中從零開始。由於每當產生一個新的 TEK 時，參數 Sequence Number 增大，因此，TEK 推導之參數 Sequence Number 可用於區分相同行動台之相同 SA 中所產生之不同的 TEK。輸入參數 SAID 為每個 SA 之識別碼，用於確保行動台對不同 SA 具有不同 TEK。由於 SAID 為 SA 之識別碼，且 SA 由基地台為行動台所建立

並對應於 TEK，因此，參數 SAID 可用於區分相同行動台中之不同 SA 之 TEK。輸入參數 CMAC_KEY_COUNT 為一個計數值，原本用於將新的 CMAC 密鑰區分於先前已有之 CMAC 密鑰，在此是用以確保在標準所定義之 AK 有效期間，不論行動台 MS 是否已經訪問過該基地台 TBS，在行動台 MS 至基地台 TBS 之交遞中，所產生之 TEK 均不相同。例如，計數值 CMAC_KEY_COUNT 可在基地台之每次網路再登錄時增大，因此，計數值 CMAC_KEY_COUNT 可用以確保產生之 TEK 不同於先前訪問相同基地台 TBS 之相同行動台中之相同 SA 之 TEK。

根據本發明之該實施例，由於參數 KEK、Sequence Number、SAID 與 CMAC_KEY_COUNT 均可在行動台 MS 與基地台 TBS 處獲取，因此，當 SA 建立之後，TEK 可由行動台 MS 與基地台 TBS 各自推導，無需消息交換。根據本發明之一實施例，TEK 推導函數可使用 KEK 作為加密密鑰，並使用其他輸入參數作為密碼函數中之明文(plaintext)資料。密碼函數可為 AES 電子編碼本(AES Electronic Code Book，簡稱 AES-ECB)模式、三次運算資料加密標準(Triple-Data Encryption Standard，簡稱 3-DES)、國際資料加密演算法(International Data Encryption Algorithm，簡稱 IDEA)等。例如，TEK 推導函數可表達如下：

$$\text{TEK} = \text{AES_ECB}(\text{KEK}, \text{SAID} | \text{Sequence Number} | \text{CMAC_KEY_COUNT}) \quad \text{Eq.2}$$

其中，操作「|」表示附加(append)操作，用以將後續參數附加至先前參數之尾部。根據本發明之另一實施

例，TEK 推導函數也可表達如下：

$$\text{TEK} = 3\text{DES_EDE}(\text{KEK}, \text{SAID} \parallel \text{Sequence Number} \parallel \text{CMAC_KEY_COUNT}) \quad \text{Eq.3}$$

根據本發明之再一實施例，密碼函數也可為 WiMAX 標準中訂定之密鑰推導函數 Dot16KDF，則 TEK 推導函數可表達如下：

$$\text{TEK} = \text{Dot16KDF}(\text{KEK}, \text{SAID} \parallel \text{Sequence Number} \parallel \text{CMAC_KEY_COUNT}, 128) \quad \text{Eq.4}$$

需要注意，任何可達到與上述密碼函數大致相同之加密結果之密碼函數均可應用於此，因此，本發明並不以此為限。

根據本發明之一實施例，由於 TEK 可經由行動台與基地台各別地產生，因此，最好於執行 TEK 推導步驟之前對新的 TEK 之推導能力進行協商。請再回到第 5 圖，在首次網路登錄階段，行動台 MS 與基地台 SBS 互相通信以執行多個網路登錄之相關程序，包括能力協商、認證、註冊等。根據本發明之該實施例，在首次網路登錄階段之交握期間，行動台 MS 與基地台 SBS 可相互告知是否支持 TEK 推導。舉例而言，如第 5 圖所示，可在能力協商步驟（步驟 S510）可互相告知。傳統地，能力協商是經由發送相對應管理消息來執行，以協商行動台與基地台所支持之基本能力。例如，行動台可經由承載相對應旗標之相對應協商消息，來通知基地台行動台是否支持交遞、行動台支持何種密碼函數，相對應地，基地台也通知行動台基地台是否支持交遞、及基地台支持何種密碼函數。因此，根據本發明

之該實施例，TEK 推導能力之協商可藉由簡單添加一個旗標來輕易實施，其中，該旗標指示行動台與基地台之 TEK 推導能力。需要注意，用於支持 TEK 推導能力之旗標不必命名為「TEK 推導支持」，也可為包括支持 TEK 推導能力之其他能力支持旗標，如「無間隙交遞支持」。

在網路登錄階段後，行動台 MS 開始訪問網路並使用基地台 SBS 所提供之多項服務。假設行動台 MS 或基地台 SBS 根據相對應規格書所定義之某個預設交遞準則決定將行動台 MS 交遞至基地台 TBS（步驟 S511），則進入交遞協商階段以執行必要之交遞操作。在交遞協商階段，行動台 MS 與基地台 SBS 執行交遞交握操作（步驟 S512），以及基地台 SBS、基地台 TBS 與鑑別器執行核心網路交遞操作（步驟 S513）。根據本發明之一實施例，在交遞交握操作期間，基地台 SBS 可將基地台 TBS 之 TEK 推導能力通知行動台 MS。例如，當基地台 SBS 發起交遞程序時，基地台 SBS 可在交遞請求消息中承載一個旗標，以指示基地台 TBS 之 TEK 推導能力，或當行動台 MS 發起交遞程序時，基地台 SBS 可在交遞回應消息中承載該旗標。在核心網路交遞操作期間，基地台 TBS 也可與基地台 SBS 及鑑別器進行協商，以獲取行動台 MS 之資訊（詳細描述請參見下文）。請注意，用於支持 TEK 推導能力旗標之旗標不必命名為「TEK 推導支持」，也可為包括支持 TEK 推導能力之其他能力支持旗標，如「無間隙交遞支持」。

根據本發明之一實施例，當交遞協商完成之後，進入安全密鑰產生階段。在安全密鑰產生階段，AK 與相關內文

最初可分別由行動台 MS(步驟 S514)及由基地台 TBS(步驟 S515)產生。請注意，本領域習知技藝者能夠輕易得知，AK 與相關內文也可由鑑別器或核心網路中之任意其他網路裝置來產生(例如，在如第 5 圖所示之核心網路交遞操作步驟 S513 中)，並傳遞至基地台 TBS。因此，本發明並不以此為限。根據本發明之該實施例，AK 與相關內文可根據如第 4 圖所示之程序及對應的段落進行更新。當新的 AK 與相關內文產生之後，根據如 Eq.1 至 Eq.4 之 TEK 推導函數或類似方式，行動台 MS(步驟 S516)與基地台 TBS(步驟 S517)可分別產生 TEK。當行動台 MS 與基地台 TBS 分別產生 TEK 之後，開始傳送流量資料。例如，根據本發明之一實施例，在網路再登錄階段，行動台 MS 可對流量資料進行加密和/或解密，並在 TBS 執行交遞程序之前將加密後的流量資料發送至基地台 TBS，或接收來自基地台 TBS 之加密後的流量資料。由於流量資料可在 TEK 產生後馬上進行傳送，因此，可大致實現無間隙交遞。流量資料之所以可在 TEK 推導產生後馬上進行傳送，是因為用於識別行動台 MS 與基地台 TBS 身份之必要資訊已經承載於經由 Eq.1 新產生之 TEK 中。只有正確的行動台 MS 與基地台 TBS 能夠解碼經由新產生之 TEK 加密之流量資料。根據本發明之該實施例，在網路再登錄階段，行動台 MS 與基地台 TBS 可進一步互相確認身份。因為範圍請求消息 RNG_REQ 與範圍回應消息 RNG_RSP 中包含多個參數，這些參數可用於認證行動台 MS 與基地台 TBS 之身份，所以行動台 MS 與基地台 TBS 可相互驗證對方之身份。例如，

範圍請求消息 RNG_REQ 與範圍回應消息 RNG_RSP 可包含行動台 MS 之識別碼、計數值 CMAC_KEY_COUNT 及 CMAC 摘要(digest)，其中，CMAC 摘要係根據消息認證密鑰（如第 4 圖所示之消息認證密鑰 CMAC_KEY_U 與消息認證密鑰 CMAC_KEY_D）來產生，計數值 CMAC_KEY_COUNT 與 CMAC 摘要可用於認證發送方(sender)。舉例而言，CMAC 摘要可經由基於相關內文之消息認證碼函數（簡稱 CMAC 函數）來產生，CMAC 函數使用密鑰 CMAC_KEY_U 作為消息認證密鑰來計算某些預設資訊。

在交遞協商階段需要進行確認是因為，交遞消息有可能因不可靠之無線電鏈路而丟失，或者新的 TEK 可能因某些原因未能成功產生。因此，如果需要，在網路再登錄階段可進一步執行錯誤復原(error recovery)程序。第 7 圖至第 11 圖所示為根據本發明一實施例之在不同情況下首次網路登錄之消息流及交遞操作程序之示意圖。請參照第 7 圖，第 7 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。如圖所示，行動台 MS 發起交遞程序。在首次網路登錄階段，行動台 MS 與基地台 SBS 之 TEK 推導能力可經由能力協商消息進行協商。如先前所述，行動台 MS 可經由旗標 TEK_GEN_SUPPORTED 通知基地台 SBS 行動台 MS 是否支持 TEK 推導（或產生），同樣，基地台 SBS 也可經由旗標 TEK_GEN_SUPPORTED 通知行動台 MS 基地台 SBS 是否支持 TEK 推導，其中，旗標 TEK_GEN_SUPPORTED 由能力協商消息所承載。當行動

台 MS 決定基地台 SBS 之信號品質變弱並需要發起交遞程序時，行動台 MS 發送交遞請求消息 MSHO_REQ 至基地台 SBS。當接收到交遞請求消息 MSHO_REQ 後，基地台 SBS 與基幹網路中之基地台 TBS、鑑別器和/或其他網路裝置執行核心網路交遞操作（圖中未示）。在核心網路交遞操作期間，基地台 SBS 可經由消息 HO_REQ 將行動台 MS 之交遞需求通知基地台 TBS，基地台 TBS 也可經由任意回應消息通知基地台 SBS 是否支持 TEK 推導。基地台 TBS 可從鑑別器獲取行動台 MS 之計數值 CMAC_KEY_COUNT。鑑別器所記載之計數值 CMAC_KEY_COUNT 藉由 CMAC_KEY_COUNT_N（N 表示網路）來標記。本領域習知技藝者能夠輕易理解，在每次成功認證後，鑑別器獲取行動台 MS 之計數值 CMAC_KEY_COUNT（以 CMAC_KEY_COUNT_M 表示，其中，M 表示行動台 MS）。

當核心網路交遞操作之後，基地台 SBS 藉由發送消息 BSHO_RESP 以回應交遞請求消息 MSHO_REQ。根據本發明之一實施例，基地台 SBS 可經由旗標 TEK_GEN_SUPPORTED_BY_TBS 將基地台 TBS 是否支持 TEK 推導通知行動台 MS，其中，旗標 TEK_GEN_SUPPORTED_BY_TBS 由回應消息 BSHO_RSP 所承載。請注意，支持 TEK 推導能力之旗標不必命名為「TEK_GEN_SUPPORTED_BY_TBS」，也可為包括支持 TEK 推導能力之其他能力支持旗標，如表示支持無間隙交遞的旗標「SEAMLESS_HO_SUPPORTED_BY_TBS」。當行動台 MS 發出交遞指示消息 HO_IND 後，交遞交握完成。

根據本發明之一實施例，當交遞交握完成後可進入安全密鑰產生階段。行動台 MS 與基地台 TBS 可根據如第 4 圖所示之程序產生一個新的 AK 與相關內文，並分別根據如 Eq.1 至 Eq.4 所示之 TEK 推導函數或其他類似方式來產生新的 TEK。行動台 MS 與基地台 TBS 應保證用於推導 AK 與相關內文之計數值 CMAC_KEY_COUNT 值與 TEK 值同步。例如，若鑑別器在每次成功認證後將計數值 CMAC_KEY_COUNT_N 設置為與計數值 CMAC_KEY_COUNT_M 相同的值，並且行動台 MS 於每次交遞期間將計數值 CMAC_KEY_COUNT_M 加一，則基地台 TBS 將自身的計數值 CMAC_KEY_COUNT 值（用 CMAC_KEY_COUNT_TBS 表示）設置為計數值 CMAC_KEY_COUNT_N 加一。當產生 TEK 之後，流量資料可藉由新產生之 TEK 進行加密，並開始傳送流量資料。由於行動台 MS 與基地台 TBS 使用同步輸入參數而使得新產生之 TEK 相同，因此，行動台 MS 與基地台 TBS 可分別對加密後的流量資料進行解密及解碼。

根據本發明之一實施例，在網路再登錄階段可執行進一步的身份確認。例如，如第 7 圖所示，新的旗標 TEK_GEN_SUCCESS 可添加到範圍請求消息 RNG_REQ 中，用以指示行動台 MS 使用計數值 CMAC_KEY_COUNT_M 成功產生 TEK，其中，計數值 CMAC_KEY_COUNT_M 由範圍請求消息 RNG_REQ 所承載。請注意，用於指示行動台 MS 成功產生 TEK 之旗標不必命名為「TEK_GEN_SUCCESS」，也可為用於指示 TEK

成功產生之其他旗標，如範圍請求消息 RNG-REQ 中之「無間隙 HO 指示」。基地台 TBS 也可經由一個額外的旗標將基地台 TBS 是否成功產生 TEK 通知行動台 MS。例如，當基地台 TBS 校驗得到在範圍請求消息 RNG_REQ 中之計數值 CMAC_KEY_COUNT_M 等於基地台 TBS 中之計數值 CMAC_KEY_COUNT_TBS 時，基地台經由範圍回應消息 RNG_RSP 中之旗標 TEK_GEN_SUCCESS，使用範圍請求消息 RNG_REQ 中之計數值 CMAC_KEY_COUNT_M，將基地台 TBS 成功產生 TEK 通知行動台 MS。請注意，用於指示 TEK 產生之旗標不必命名為「TEK_GEN_SUCCESS」，也可為用於指示行動台 MS 成功產生 TEK 之其他已存在旗標，如範圍回應消息 RNG-RSP 中之 HO 最優化位元。

第 8 圖所示為根據本發明一實施例之首次網路登錄與交遞操作程序之消息流之示意圖，其中，在本實施例中，基地台 SBS 發起交遞。如前所述，行動台 MS 可經由旗標 TEK_GEN_SUPPORTED 通知基地台 SBS 行動台 MS 是否支持 TEK 推導（或產生），同樣，基地台 SBS 也可經由旗標 TEK_GEN_SUPPORTED 通知行動台 MS 基地台 SBS 是否支持 TEK 推導，其中，旗標 TEK_GEN_SUPPORTED 由能力協商消息所承載。當基地台 SBS 決定行動台 MS 之信號品質變弱並需要發起交遞程序時，基地台 SBS 與基幹網路中之基地台 TBS、鑑別器和/或其他有關聯之網路裝置執行核心網路交遞操作。（圖中未示）。在核心網路交遞操作期間，基地台 SBS 可經由消息 HO_REQ 將基地台 TBS 之

交遞需求通知基地台 TBS，基地台 TBS 也可經由回應消息通知基地台 SBS 是否支持 TEK 推導。基地台 TBS 可從鑑別器獲取行動台 MS 之計數值 CMAC_KEY_COUNT（及關於 TEK 序列號之資訊）。根據本發明之一實施例，基地台 SBS 可經由旗標 TEK_GEN_SUPPORTED_BY_TBS 將基地台 TBS 是否支持 TEK 推導通知基地台 SBS，其中，旗標 TEK_GEN_SUPPORTED_BY_TBS 由交遞請求消息 BSHO_REQ 所承載。請注意，用於指示支持 TEK 推導能力之旗標不必須命名為「TEK_GEN_SUPPORTED_BY_TBS」，也可為包含支持 TEK 推導能力之其他能力支持旗標，如表示支持無間隙交遞的旗標「SEAMLESS_HO_SUPPORTED_BY_TBS」。當行動台 MS 發出交遞指示消息 HO_IND 後完成交遞交握。

根據本發明之一實施例，當交遞交握完成後可進入安全密鑰產生階段。行動台 MS 與基地台 TBS 根據如第 4 圖所示之程序產生新的 AK 與相關內文，並分別根據 Eq.1 至 Eq.4 所示之 TEK 推導函數或類似函數產生新的 TEK。如前所述，在 AK 與相關內文產生步驟，行動台 MS 可更新計數值 CMAC_KEY_COUNT_M。行動台 MS 與基地台 TBS 保持用於 AK 與相關內文與 TEK 推導中之計數值 CMAC_KEY_COUNT_M 與計數值 CMAC_KEY_COUNT_TBS 同步。當 TEK 產生後，流量資料可藉由新產生之 TEK 進行加密，並開始傳送流量資料。由於行動台 MS 與基地台 TBS 新產生之 TEK 相同，因此，行動台 MS 與基地台 TBS 可分別對加密後的流量資料進行

解密及解碼。

根據本發明之一實施例，在網路再登錄階段可執行進一步身份確認。如第 8 圖所示，旗標 TEK_GEN_SUCCESS (值設置為一) 可承載在範圍請求消息 RNG_REQ 中，用於指示行動台 MS 藉由使用範圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 成功產生了 TEK。當基地台 TBS 校驗得到在範圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 等於基地台 TBS 所包含之計數值 CMAC_KEY_COUNT_TBS 時，基地台 TBS 也可經由在範圍回應消息 RNG_RSP 中將旗標 TEK_GEN_SUCCESS 設置為一來通知行動台 MS，基地台 TBS 使用範圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 成功產生 TEK。請注意，用於指示 TEK 成功產生之旗標不必命名為「TEK_GEN_SUCCESS」，也可為用於指示 TEK 成功產生之其他已存在旗標，如範圍回應消息 RNG-RSP 中之 HO 最優化位元。

第 9 圖所示為根據本發明一實施例之首次網路登錄與交遞操作程序之消息流之示意圖，其中，在本實施例中，交遞協商未完成且應用了錯誤復原程序。在本發明之該實施例中，能力協商的詳細描述，請參照第 7 圖與第 8 圖。簡潔起見，此處不再贅述。根據本發明之該實施例，行動台 MS 與基地台 SBS 決定信號品質變弱並發起交遞程序。然而，交遞請求消息和/或交遞指示消息因不良網路條件而無法傳播至另一方。如第 9 圖所示，基地台 TBS 收到來自

基地台 SBS 之交遞請求 HO_REQ，但是行動台 MS 因交遞請求消息 BSHO_REQ 與 MSHO_REQ/HO_IND 傳輸失敗而無法獲知交遞需求。當交遞請求消息 MSHO_REQ/HO_IND 之幾次重發嘗試失敗後，行動台 MS 放棄交遞協商並直接連接至基地台 TBS，用以將通信服務交遞至基地台 TBS。在此情形下，基地台 TBS 產生一個新的 AK 與相關內文並產生新的 TEK，但是行動台 MS 並不產生新的 AK 與相關內文及新的 TEK（然而，計數值 CMAC_KEY_COUNT_M 可能因交遞操作而繼續增加）。在此情形下，基地台 TBS 與行動台 MS 間之流量資料傳送有可能失敗，這是因為行動台 MS 與基地台 TBS 無法利用不同之 TEK 來對流量資料進行成功解密及解碼。因此，在網路再登錄階段，旗標 TEK_GEN_SUCCESS（值為零時指示沒有 TEK 產生）可承載於範圍請求消息 RNG_REQ 中，用以指示行動台 MS 藉由使用承載於範圍請求消息中之計數值 CMAC_KEY_COUNT_M 沒有產生 TEK。請注意，用於指示 TEK 沒有產生之旗標不必命名為「TEK_GEN_SUCCESS」，也可為用於指示 TEK 成功產生之其他旗標，如 RNG-REQ 消息中之「無間隙 HO 指示」。

當基地台 TBS 接收到範圍請求消息 RNG_REQ 後，若範圍請求消息 RNG_REQ 中之旗標 TEK_GEN_SUCCESS 設置為零，則基地台 TBS 可決定是重複使用交遞前之先前 TEK 還是使用預設方法（例如，隨機產生）重新產生之 TEK，並將新產生之 TEK 發送至行動台 MS。基地台 TBS 經由設置為零之旗標 TEK_GEN_SUCCESS 通知行動台

MS，基地台 TBS 使用範圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 未成功產生 TEK，並且基地台 TBS 經由範圍回應消息 RNG_RSP 中之旗標 USE_PREVIOUS_TEK 通知行動台 MS，是否使用交遞前之先前 TEK。當行動台 MS 接收到範圍回應消息 RNG_RSP 後，根據旗標 USE_PREVIOUS_TEK，行動台 MS 決定是重複使用交遞前之先前 TEK 還是使用新的基地台 SBS（也就是，如第 9 圖所示之基地台 TBS）產生之 TEK。以此方式，在網路再登錄階段，TEK 不一致之錯誤得以消除。請注意，用於指示 TEK 未產生之旗標不必命名為「TEK_GEN_SUCCESS」，也可為用於指示 TEK 成功產生之其他已存在旗標，如範圍回應消息 RNG-RSP 中之 HO 最優化位元。

第 10 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖，其中，在本實施例中，TEK 推導失敗並應用了錯誤復原程序。在本發明之該實施例中，關於能力協商及交遞交握之詳細描述請參照第 7 圖與第 8 圖，簡潔起見，此處不再贅述。在本實施例中，在交遞協商階段完成了交遞交握，但是在基地台 TBS 一側之 TEK 推導失敗。新的 TEK 推導失敗導致流量資料傳送失敗，這是因為行動台 MS 與基地台 TBS 無法對流量資料成功解密及解碼。

因此，當進入網路再登錄階段時，範圍請求消息 RNG_REQ 中可承載旗標 TEK_GEN_SUCCESS，用於指示行動台 MS 使用計數值 CMAC_KEY_COUNT_M 成功產生

了 TEK，其中，計數值 CMAC_KEY_COUNT_M 承載於範圍請求消息 RNG_REQ 中。然而，由於基地台 TBS 沒有成功產生 TEK，因此，基地台 TBS 可以決定是重複使用交遞前之先前 TEK 還是使用預設方法重新產生之 TEK，並當接收到範圍請求消息 RNG_REQ 後將新產生之 TEK 發送至行動台 MS。基地台 TBS 經由設置為零之旗標 TEK_GEN_SUCCESS 通知行動台 MS，基地台 TBS 使用範圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 未成功產生 TEK，並且基地台 TBS 經由範圍回應消息 RNG_RSP 中之旗標 USE_PREVIOUS_TEK 通知行動台 MS，是否使用交遞前之先前 TEK。當行動台 MS 接收到範圍回應消息 RNG_RSP 後，根據旗標 USE_PREVIOUS_TEK，行動台 MS 決定是重複使用交遞前之先前 TEK 還是使用新的基地台 SBS（也就是，第 10 圖所示之基地台 TBS）產生之 TEK。以此方式，在網路再登錄階段，TEK 不一致之錯誤得以消除。

第 11 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖，其中，在本實施例中，計數值 CMAC_KEY_COUNT_M 與 CMAC_KEY_COUNT_TBS 不一致並應用了錯誤復原程序。在本發明之該實施例中，能力協商及交遞協商之詳細描述請參照第 7 圖與第 8 圖，簡潔起見，此處不再贅述。在本實施例中，在交遞協商階段完成了交遞交握，並且行動台 MS 與基地台 TBS 成功產生了安全密鑰。然而，行動台 MS 與基地台 TBS 所獲取之計數值 CMAC_KEY_COUNT_M 與

計數值 CMAC_KEY_COUNT_TBS 不一致。這種情況可能發生在，例如，若行動台 MS 最初計劃與另一基地台進行交遞，但最終丟棄交遞程序計劃。由於計數值 CMAC_KEY_COUNT_M 在每當行動台 MS 計劃執行交遞時進行更新，因此，無論交遞是否執行成功，計數值 CMAC_KEY_COUNT_M 都可能與網路一側之計數值 CMAC_KEY_COUNT_N 變得不同步。因此，基地台 TBS 有可能取得不同步之計數值並利用不同步之計數值產生 TEK。在此情形下，行動台 MS 與基地台 TBS 所產生之 TEK 有可能不一致，並且流量資料傳送有可能失敗，這是因為行動台 MS 與基地台 TBS 無法利用不同的 TEK 對流量資料成功解密及解碼。

因此，當進入網路再登錄階段時，範圍請求消息 RNG_REQ 中可承載旗標 TEK_GEN_SUCCESS，用於指示行動台 MS 使用計數值 CMAC_KEY_COUNT_M 成功產生了 TEK，其中，計數值 CMAC_KEY_COUNT_M 承載於範圍請求消息中。然而，若基地台 TBS 決定行動台 MS 之計數值 CMAC_KEY_COUNT_M 大於基地台 TBS 所獲取之計數值 CMAC_KEY_COUNT_TBS，則基地台 TBS 接下來可決定是重複使用交遞前之先前 TEK，還是根據如 Eq.1 至 Eq.4 所示之 TEK 推導函數或類似方式使用計數值 CMAC_KEY_COUNT_M 重新產生之 TEK，或是使用預設方法重新產生之 TEK，並將新產生之 TEK 發送至行動台 MS。基地台 TBS 經由設置為零之旗標 TEK_GEN_SUCCESS 通知行動台 MS，基地台 TBS 使用範

圍請求消息 RNG_REQ 中所承載之計數值 CMAC_KEY_COUNT_M 未成功產生 TEK，並且基地台 TBS 經由範圍回應消息 RNG_RSP 中之旗標 USE_PREVIOUS_TEK 通知行動台 MS，是否使用交遞前之先前 TEK。當行動台 MS 接收到範圍回應消息 RNG_RSP 後，根據旗標 USE_PREVIOUS_TEK，行動台 MS 決定是重複使用交遞前之先前 TEK 還是使用新的 SBS（也就是，第 11 圖所示之基地台 TBS）產生之 TEK。以此方式，在網路再登錄階段，TEK 不一致之錯誤得以消除。

如第 11 圖所示，由於計數值 CMAC_KEY_COUNT 有可能僅在首次網路登錄階段與網路再登錄階段更新至核心網路，因此，行動台 MS 中之計數值 CMAC_KEY_COUNT_M 與基地台 TBS 所獲取之計數值 CMAC_KEY_COUNT_TBS 可能不同。因此，最好提前對計數值進行同步。請回到第 5 圖，根據本發明之一實施例，行動台 MS 可在交遞交握階段將計數值 CMAC_KEY_COUNT_M 與基地台 TBS 進行同步。根據本發明之另一實施例，行動台 MS 可將計數值 CMAC_KEY_COUNT_M 發送至核心網路中之任意網路裝置，然後網路裝置將計數值中繼(relay)至基地台 TBS。根據本發明之再一實施例，行動台 MS 可將計數值 CMAC_KEY_COUNT_M 發送至鑑別器，然後鑑別器可將計數值 CMAC_KEY_COUNT_M 中繼至基地台 TBS。

第 12 圖所示為根據本發明一實施例之交遞操作程序之消息流之示意圖。根據本發明之該實施例，行動台 MS

可產生一個新的 AK 與相關內文，並對計數值 CMAC_KEY_COUNT_M 進行更新，以用於交遞協商階段之交遞。更新後的計數值 CMAC_KEY_COUNT_M 可經由交遞指示消息發送至基地台 SBS，或經由對應消息發送至核心網路中之任意其他網路裝置。計數值 CMAC_KEY_COUNT_M 可進一步藉由核心網路中之任意網路裝置中繼最終到達基地台 TBS。如第 12 圖所示，基地台 SBS 經由指示消息 CMAC_KEY_COUNT_UPDATE 對資訊進行中繼。根據本發明之該實施例，由於基地台 TBS 需要一些資訊來確認計數值 CMAC_KEY_COUNT_M 之完整性與來源，因此，行動台 MS 所提供之完整性證明可與計數值 CMAC_KEY_COUNT_M 承載在一起。如第 12 圖所示，經由承載於交遞指示消息 HO_IND 中之參數 CKC_INFO，基地台 TBS 可以驗證計數值 CMAC_KEY_COUNT_M 實際上是由行動台 MS 所發送並且未被任意第三方所修改。根據本發明之一實施例，參數 CKC_INFO 可根據行動台 MS 與基地台 TBS 所共享之至少一個安全密鑰與基地台 TBS 所已知之至少一資訊來產生。例如，參數 CKC_INFO 可根據如下函數來獲取：

$$\text{CKC_INFO} = \text{CMAC_KEY_COUNT_M} \mid \text{CKC_Digest}$$

Eq.5

其中，CKC_Digest 可根據任意安全密鑰或行動台 MS 與基地台 TBS 所共享之資訊來產生，操作「|」表示附加操作。例如，CKC_Digest 可經由 CMAC 函數來產生，其中，CMAC 函數接收一些共享資訊作為明文資料，並使用安全

密鑰 CMAC_KEY_U 作為加密密鑰 (cipher key)。
CKC_Digest 可經由以下函數來獲取：

$$\text{CKC_Digest} = \text{CMAC}(\text{CMAC_KEY_U}, \text{AKID}|\text{CMAC_PN}|\text{CMAC_KEY_COUNT_M}) \quad \text{Eq.6}$$

其中，參數 AKID 為 AK 之識別碼，從 AK 中可產生安全密鑰 CMAC_KEY_U，以及參數 CMAC_PN (CMAC 封包號碼) 為一個計數值，該計數值於每次 CMAC 摘要計算後增大。

當接收到承載關於行動台 MS 之計數值之資訊之指示消息 CMAC_KEY_COUNT_UPDATE 後，基地台 TBS 可檢測計數值之完整性與來源，以校驗資訊之真實性，並當接收到的計數值 CMAC_KEY_COUNT_M 通過校驗時，對計數值 CMAC_KEY_COUNT_TBS 進行更新。基地台 TBS 可從核心網路中獲取計數值 CMAC_KEY_COUNT_N，並藉由獲取的計數值 CMAC_KEY_COUNT_N 來對參數 CKC_Info 進行校驗。根據本發明之一實施例，基地台 TBS 首先決定獲取後的計數值 CMAC_KEY_COUNT_M 大於還是等於計數值 CMAC_KEY_COUNT_N。由於每當行動台 MS 計劃執行交遞程序時，計數值 CMAC_KEY_COUNT_M 進行更新，因此，計數值 CMAC_KEY_COUNT_M 應大於或等於在首次網路登錄階段或網路再登錄階段上傳至核心網路之計數值 CMAC_KEY_COUNT_N。當計數值 CMAC_KEY_COUNT_M 大於或等於計數值 CMAC_KEY_COUNT_N 時，基地台 TBS 利用接收到的計數值 CMAC_KEY_COUNT_M 產生 AK 與相關內文，並使

用 AK 與相關內文中之密鑰校驗行動台 MS 之計數值 CMAC_KEY_COUNT_M 之完整性。例如，基地台 TBS 經由消息認證密鑰 CMAC_KEY_U 校驗如 Eq.6 所示之 CKC_Digest。當 CKC_Digest 可經由密鑰 CMAC_KEY_U 驗證通過時，計數值 CMAC_KEY_COUNT 之完整性及來源可得到保證。當計數值 CMAC_KEY_COUNT_M 之完整性校驗通過時，基地台 TBS 設置計數值 CMAC_KEY_COUNT_TBS 等於計數值 CMAC_KEY_COUNT_M，從而更新計數值 CMAC_KEY_COUNT_TBS。當對參數 CKC_Info 進行校驗時，由於 AK 與相關內文是根據同步後的計數值 CMAC_KEY_COUNT_TBS 來產生的，因此，基地台 TBS 可於校驗及更新步驟後馬上產生 TEK。流量資料傳送可於行動台 MS 與基地台 TBS 分別產生 TEK 之後開始，其中，行動台 MS 與基地台 TBS 根據同步後之計數值 CMAC_KEY_COUNT_M 與計數值 CMAC_KEY_COUNT_TBS 分別產生 TEK。請注意，本領域習知技藝者能夠輕易了解，AK 與相關內文也可由鑑別器或核心網路中之任意其他網路裝置來產生，並傳遞至基地台 TBS，因此，本發明並不以此為限。最後，在網路再登錄階段（圖中未示），計數值 CMAC_KEY_COUNT_M 更新至核心網路。

第 13 圖所示為根據本發明另一實施例之交遞操作程序之消息流之示意圖：根據本發明之該實施例，行動台 MS 可更新計數值 CMAC_KEY_COUNT_M，以用於交遞協商

階段之交遞。更新後的計數值 CMAC_KEY_COUNT_M 可經由交遞請求消息發送至基地台 SBS。基地台 SBS 可藉由決定計數值 CMAC_KEY_COUNT_M 大於還是等於基地台 SBS 中之計數值 $\text{CMAC_KEY_COUNT_SBS}$ ，來校驗計數值 CMAC_KEY_COUNT_M 。當計數值 CMAC_KEY_COUNT_M 大於或等於計數值 $\text{CMAC_KEY_COUNT_SBS}$ 時，基地台 SBS 可經由任意消息進一步將計數值 CMAC_KEY_COUNT_M 發送至鑑別器。舉例而言，如第 13 圖所示，基地台 SBS 經由指示消息 $\text{CMAC_KEY_COUNT_UPDATE}$ 將計數值 CMAC_KEY_COUNT_M 發送至鑑別器。鑑別器接著可經由，例如 HO_INFO_IND 消息，將計數值 CMAC_KEY_COUNT_M 傳遞至基地台 TBS。根據本發明之該實施例，由於基地台 TBS 信任鑑別器，因此，行動台 MS 不需要發送任何額外資訊以校驗計數值之完整性。當基地台 TBS 接收到行動台 MS 之計數值 CMAC_KEY_COUNT_M 後，基地台 TBS 可根據計數值 CMAC_KEY_COUNT_M 產生 AK 與相關內文並產生 TEK。流量資料傳送可於行動台 MS 與基地台 TBS 根據同步後的計數值分別產生 TEK 之後開始。請注意，本領域習知技藝者當可輕易了解，AK 與相關內文也可由鑑別器或核心網路中之任意其他網路裝置來產生，並傳遞至基地台 TBS，因此，本發明並不以此為限。最後，在網路再登錄階段（圖中未示），計數值 CMAC_KEY_COUNT_M 可更新至核心網路。在本發明之該實施例中，由於計數值

CMAC_KEY_COUNT_TBS 已提前與計數值 CMAC_KEY_COUNT_M 進行同步，因此，行動台 MS 與基地台 TBS 所產生之 TEK 是一致的並且流量資料能夠被正確解密及解碼。

上述之實施例僅用來例舉本發明之實施態樣，以及闡釋本發明之技術特徵，並非用來限制本發明之範疇。任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利範圍應以申請專利範圍為準。

【圖式簡單說明】

第 1 圖所示為根據本發明一實施例之無線通信系統之網路拓撲示意圖。

第 2 圖所示為根據本發明一實施例之基地台之示意圖。

第 3 圖所示為根據本發明一實施例之行動台之示意圖。

第 4 圖所示為根據本發明一實施例之 AK 與相關內文產生程序之示意圖。

第 5 圖所示為根據本發明一實施例的首次網路登錄及交遞操作程序之示意圖。

第 6 圖所示為根據本發明一實施例之說明 TEK 產生模型之通信網路之示意圖。

第 7 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。

第 8 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。

第 9 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。

第 10 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。

第 11 圖所示為根據本發明一實施例之首次網路登錄及交遞操作程序之消息流之示意圖。

第 12 圖所示為根據本發明一實施例之交遞操作程序之消息流之示意圖。

第 13 圖所示為根據本發明一實施例之交遞操作程序之消息流之示意圖。

【主要元件符號說明】

- 100~無線通信系統；
- 101、102~基地台；
- 103、104~行動台；
- 105、106~區段；
- 107~網路裝置；
- 111、131~基帶模組；
- 112、132~無線電收發模組；
- 113~網路介面模組；
- 114、134~處理器；
- 115、135~記憶體；
- 133~用戶識別卡；

S510~S517：步驟。

發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※ 申請案號： 98114361

※ 申請日： 98.4.30

※IPC 分類：

H04W 36/18 (2009.01)

H04W 12/06 (2009.01)

H04L 29/06 (2006.01)

一、發明名稱：(中文/英文)

行動台、基地台及流量加密密鑰之產生方法

Mobile Station and Base Station and Method for Deriving Traffic

Encryption Key

二、中文發明摘要：

本發明提供一種行動台、基地台及流量加密密鑰之產生方法。其中，行動台包含一個或多個無線電收發模組與處理器。處理器與服務基地台執行交遞協商程序，經由無線電收發模組發送和接收多個交遞協商消息，以交遞通信服務至目標基地台，並產生認證密鑰與相關內文，為目標基地台推導出至少一流量加密密鑰，認證密鑰與相關內文包含與目標基地台共享之多個密鑰，用以對發送至目標基地台之多個消息進行加密，流量加密密鑰為與目標基地台共享之密鑰，用以對流量資料進行加密。利用本發明可實現無間隙之交遞，避免流量資料傳送之長時間中斷，提高通信服務品質。

三、英文發明摘要：

A mobile station is provided. The mobile station includes one or more radio transceiver module and a processor. The processor performs a handover negotiation

procedure with a serving base station so as to handover communication services to a target base station by transmitting and receiving a plurality of handover negotiation messages via the radio transceiver module, and generates an Authorization Key (AK) context and derives at least one Traffic Encryption Key (TEK) for the target base station. The AK context includes a plurality of keys shared with the target base station for encrypting messages to be transmitted to the target base station, and the TEK is a secret key shared with the target base station for encrypting traffic data.

七、申請專利範圍：

1.一種行動台，用於無線通信網路中，包含：

一個或多個無線電收發模組；以及

一處理器，與一服務基地台執行一交遞協商程序，經由該無線電收發模組發送和接收多個交遞協商消息，以交遞多項通信服務至一目標基地台，以及該處理器產生一認證密鑰與相關內文，並根據由該認證密鑰與相關內文得出的與該目標基地台共享之一基礎密鑰、一識別碼、一序列號及該目標基地台已知之一計數值為該目標基地台推導出至少一流量加密密鑰，其中，該認證密鑰與相關內文包含與該目標基地台共享之多個密鑰，用以對發送至該目標基地台之多個消息進行加密，以及該至少一流量加密密鑰係為與該目標基地台共享之密鑰，用以對流量資料進行加密。

2.如申請專利範圍第 1 項所述之行動台，其中，在與該目標基地台執行一交遞程序之前，該處理器更加密和/或解密該流量資料以分別產生加密後的該流量資料和/或解密後的該流量資料，並發送加密後的該流量資料至該目標基地台和/或接收來自該目標基地台之加密後的該流量資料。

3.如申請專利範圍第 1 項所述之行動台，其中，當推導出該流量加密密鑰後，該處理器更發送一消息至該目標基地台，以認證該行動台之身份。

4.如申請專利範圍第 1 項所述之行動台，其中，該處理器根據由該認證密鑰與相關內文得出之至少一基礎密鑰及該識別碼、該序列號及該目標基地台已知之該計數值，

推導出該至少一流量加密密鑰。

5.如申請專利範圍第 1 項所述之行動台，其中，該基礎密鑰係為一密鑰，用於區分連接至該目標基地台之不同的行動台，該識別碼係由該目標基地台所建立並對應於該流量加密密鑰之一群組之識別碼，該序列號係為一號碼，用於區分所產生之不同的該流量加密密鑰，以及該計數值係為一數值，該數值於該目標基地台之每個再登錄期間增大，並用以區分在每個再登錄期間對應該同一目標基地台所產生之不同的消息認證密鑰。

6.如申請專利範圍第 5 項所述之行動台，其中，該基礎密鑰係為該認證密鑰與相關內文中之一密鑰加密密鑰，以及該群組之識別碼係為一安全群組之識別碼。

7.如申請專利範圍第 1 項所述之行動台，其中，於一交遞協商階段執行該交遞協商程序期間，該處理器更經由該無線電收發模組發送一計數值至該無線通信網路中之至少一網路裝置，其中，該計數值用於區分該認證密鑰與相關內文中所產生之不同的消息認證密鑰。

8.如申請專利範圍第 7 項所述之行動台，其中，該處理器發送該計數值至該無線通信網路中之一鑑別器，以經由該鑑別器將該計數值中繼至該目標基地台，其中，該鑑別器處理與安全有關之程序。

9.如申請專利範圍第 7 項所述之行動台，其中，該處理器更產生校驗資料，以校驗該計數值之完整性與來源，以及該處理器將該校驗資料與該計數值一起發送至該至少一網路裝置，以經由該至少一網路裝置將該計數值與該校

驗資料中繼至該目標基地台，其中，該校驗資料係根據與該目標基地台共享之至少一密鑰及該目標基地台已知之至少一資訊來產生的。

10.如申請專利範圍第 9 項所述之行動台，其中，該校驗資料係藉由將該認證密鑰與相關內文中之該密鑰作為該共享密鑰、並將該計數值作為該被保護資訊來產生的。

11.一種流量加密密鑰之產生方法，用於產生無線通信網路中之一行動台與一基地台之間所共享之至少一流量加密密鑰，包含：

獲取該行動台與該基地台之間所共享之至少一密鑰與資訊；以及

根據該資訊與該至少一密鑰，經由一預設函數產生該至少一流量加密密鑰，

其中，該至少一密鑰係為一基礎密鑰，該資訊包含一識別碼、一序列號及該行動台與該基地台所共享之一計數值。

12.如申請專利範圍第 11 項所述之流量加密密鑰之產生方法，其中，該基礎密鑰用以區分連接至該基地台之不同的行動台，以及該計數值用以區分該行動台中所產生之多個不同的消息認證密鑰。

13.如申請專利範圍第 11 項所述之流量加密密鑰之產生方法，其中，該基礎密鑰用以區分連接至該基地台之不同的行動台，該識別碼係由該目標基地台為該行動台所設定並對應於該流量加密密鑰之一群組之識別碼，該序列號係為一號碼，用於區分所產生之不同的該流量加密密鑰，

以及該計數值係為一數值，該數值於該基地台之每個再登錄期間增大，並用於區分在每個再登錄期間對應該同一基地台之所產生之多個不同的消息認證密鑰。

14.如申請專利範圍第 13 項所述之流量加密密鑰之產生方法，其中，該基礎密鑰係為該行動台與該基地台所共享之一密鑰加密密鑰，以及該識別碼係為一安全群組之識別碼。

15.如申請專利範圍第 13 項所述之流量加密密鑰之產生方法，其中，該預設函數係為一密碼函數，該密碼函數接收該識別碼、該序列號及該計數值以作為一明文資料，並使用該基礎密鑰對該明文資料進行加密。

16.一種基地台，用於無線通信網路中，包含：

一網路介面模組；

一個或多個無線電收發模組；以及

一處理器，經由該網路介面模組接收一交遞指示消息，該交遞指示消息來自於該無線通信網路中之一網路裝置，當接收到該交遞指示消息後，處理器產生一認證密鑰與相關內文，並根據由該認證密鑰與相關內文所得出的與該行動台所共享之一基礎密鑰、一識別碼、一序列號及該行動台已知之一計數值推導出對應一行動台之至少一流量加密密鑰，處理器經由該一個或多個無線電收發模組接收來自於該行動台之一認證消息，並根據接收到的該認證消息對該至少一流量加密密鑰與該行動台所產生之至少一流量加密密鑰之一致性進行校驗，

其中，該交遞指示消息係為一消息，由該網路裝置向

行動台提供之該通信服務欲傳送至該基地台，該認證消息係為一消息，用於認證該行動台之身份，以及該基地台所推導出之該至少一流量加密密鑰係為與該行動台所共享之一密鑰，用於對流量資料進行加密。

17.如申請專利範圍第 16 項所述之基地台，其中，該處理器更使用已推導出的該至少一流量加密密鑰，來對該流量資料進行加密和/或解密。

18.如申請專利範圍第 16 項所述之基地台，其中，該處理器於接收該網路再登錄程序中之該認證消息之前，更發送該流量資料至該行動台，以及/或者接收來自該行動台之該流量資料。

19.如申請專利範圍第 16 項所述之基地台，其中，該認證密鑰包含與該行動台所共享之至少一密鑰，用以保護欲發送至該行動台之消息，以及該處理器根據該至少一密鑰中之至少一個與該行動台已知之資訊，來推導出該至少一流量加密密鑰。

20.如申請專利範圍第 16 項所述之基地台，其中，該處理器根據該認證消息所承載之一計數值，來校驗該多個流量加密密鑰之一致性，其中，該計數值係為一數值，該數值用於區分該行動台之該認證密鑰與相關內文中所產生之多個不同的消息認證密鑰。

21.如申請專利範圍第 16 項所述之基地台，其中，該基礎密鑰係為一密鑰，用於區分使用該處理器所提供之該通信服務之不同的行動台，該識別碼係由該處理器所設定並對應於該流量加密密鑰之一安全群組之識別碼，該序列

號係為一號碼，用於區分該行動台中所產生之不同的該流量加密密鑰，以及該計數值係為一數值，用於區分該行動台之認證密鑰與相關內文中所產生之多個不同的消息認證密鑰。

22.如申請專利範圍第 21 項所述之基地台，其中，該處理器更接收該計數值與校驗資料，以校驗該計數值之完整性，其中該校驗資料係由該行動台發送至該網路裝置，以及該處理器接收來自於該無線通信網路中之一鑑別器之一參考計數值，其中，該鑑別器處理與安全有關之程序，該處理器根據該計數值產生該認證密鑰與相關內文，並於該流量加密密鑰被推導出之前，根據已產生的該認證密鑰與相關內文、該校驗資料及該參考計數值對該計數值之正確性進行校驗，其中，該校驗資料先前係由該行動台所保護。

23.如申請專利範圍第 21 項所述之基地台，其中，該處理器更接收來自於該無線通信網路中之一鑑別器之該計數值，其中，該鑑別器處理與安全有關之程序，該計數值係由該行動台發送至該鑑別器。

四、指定代表圖：

(一)本案指定代表圖為：第(3)圖。

(二)本代表圖之元件符號簡單說明：

103~行動台；

131~基帶模組；

132~無線電收發模組；

133~用戶識別卡

134~處理器；

135~記憶體。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：