公告本

102 年 9 月 23 日修正替換頁

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：096121604

※ 申請日期：96 年 6 月 14 日　　※IPC 分類：H04L 9/30 (2006.01)

一、發明名稱：（中文/英文）

初始傳信訊息中原始用戶識別碼安全保護的方法及裝置/Method and Apparatus for Security Protection of An Original User Identity In An Initial Signaling Message

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

美商內數位科技公司/InterDigital Technology Corporation

代表人：（中文/英文）

唐納爾德・伯萊斯/Donald M. Boles

住居所或營業所地址：（中文/英文）

美國德拉威州 19810 威明頓席爾佛賽路 3411 號康科特廣場海格雷大廈 105 室/3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, DE 19810, U.S.A.

國　籍：（中文/英文）美國/US

三、發明人：（共 3 人）

1. 姓　名：（中文/英文）彼得・王/Peter S. WANG
　國　籍：（中文/英文）美國/US
2. 姓　名：（中文/英文）路易斯・古奇諾/Louis J. GUCCIONE
　國　籍：（中文/英文）美國/US
3. 姓　名：（中文/英文）史蒂芬・泰利/Stephen E. TERRY
　國　籍：（中文/英文）美國/US

102 年 9 月 23 日修正替換頁

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國 US；2006/06/19；60/815,245
2. 美國 US；2006/07/21；60/832,632

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

無線發射/接收單元(WTRU)包括一控制平面(C 平面)封包資料聚合協定(C-PDCP)層，其執行一傳信訊息的加密。C-PDCP 層在 WTRU 加電後被啟動並且初始安全參數被載入到 C-PDCP 層。初始連接傳信訊息和用戶識別碼甚至在 WTRU 被驗證之前使用該初始安全參數而被加密。包括加密密鑰(CK)的初始安全參數可以從網路所廣播的系統資訊中產生。CK 可以是非對稱加密的公鑰，並且可以從網路系統資訊所廣播的或者源自於網路系統資訊的公鑰組中選擇。選定的公鑰的索引可以分開地進行編碼。或者，索引可以透過使用 Diffie-hellman 密鑰交換方法而被傳送。

六、英文發明摘要：

A wireless transmit/receive unit (WTRU) includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message and a user identity are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters including a ciphering key (CK) may be generated from system information broadcast from the network. The CK may be a public key for asymmetric encryption, and may be selected from a public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Hellman key exchange method.

102 年 9 月 23 日修正替換頁

七、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:

210、WTRU	無線發射/接收單元
211	NAS 層
212	RRC 層
213	C-PDCP 層
250	eNode-B
260	aGW
270	HLR/AuC
NAS	非存取層
RRC	無線電資源控制
C-PDCP	控制平面(C 平面)封包資料聚合協定
HLR	暫存器
AuC	驗證中心

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本發明與無線通信系統有關。更具體地說，本發明與一種在包括第三代(3G)長期演進(LTE)在內的無線通信系統中用於對初始存取傳信訊息中的原始用戶識別碼(ID)進行安全保護的方法和設備有關。

【先前技術】

在第三代(3G)通用行動電信系統(UMTS)中，在用於附加和驗證程序的初始連接期間，無線發射/接收單元(WTRU)識別碼(即國際行動用戶識別碼(IMSI))是經由無線電介面被發射給核心網路以用於驗證目的。可是，IMSI 和一些在用於附加和驗證程序的初始連接期間交換的資訊未被保護，而是在一個無保護的開放環境中被發射。

第 1 圖顯示出 3G UMTS 網路 10 中的初始附加和驗證程序。在 WTRU 12 加電後，WTRU 12 的非存取層(Non-Access Stratum, NAS)層 14 發送一信號(附加(ATTACH))給 WTRU 12 的無線電資源控制(RRC)層 16 以觸發 RRC 連接(步驟 102)。RRC 層 16 發送一具有 WTRU 初始識別碼(即 IMSI)的 RRC 連接請求到通用陸地無線電存取網路(UTRAN)18 以建立 RRC 連接(步驟 104)。UTRAN 18 以 RRC 建立請求訊息進行回應(步驟 106)。RRC 層 16 發送一 RRC 建立完成訊息到 UTRAN 18(步驟 108)。RRC 層 16 然後發送一層 3 訊息(初始直接轉移(INITIAL DIRECT

TRANSFER))到 UTRAN 18(步驟 110)。UTRAN 18 然後發送一具有 IMSI 的初始 UE 訊息到訪問者位置暫存器(VLR)20，(或者到服務通用封包無線服務(GPRS)支援節點(SGSN))(步驟 112)。透過使用 IMSI 而識別用戶。在一定條件下(例如，如果用戶未被驗證)，則 VLR/SGSN 20 需要驗證和密鑰協商(AKA)並發送一驗證資料請求到本地位置暫存器(HLR)22(或者到驗證中心(AuC))，(步驟 114)。一旦接收到驗證資料請求，HLR/AuC 22 發送一組驗證向量(AV)到 VLR/SGSN 20(步驟 116)。

每個 AV 包含五組數字，其包括亂數(RAND)、用於驗證該用戶的期望回應(XRES)、用於建立保密性的密碼密鑰(CK)、完整性密鑰(IK)以及驗證權杖(AUTN)。AUTN 包括用匿名密鑰(AK)所隱藏的序列號(SQN)、規定了某個驗證要素(諸如待使用的演算法、密鑰使用期限等等)的驗證管理欄位(AMF)、以及與 SQN、AMF 和 RAND 函數相關的訊息驗證碼(MAC)。

VLR/SGSN 20 經由 UTRAN 18 從其已經選擇的 AV 中發送 RAND 和 AUTN 到 NAS 層 14(步驟 118、120)。NAS 層 14 然後透過計算一期望的 MAC(XMAC)並確定該 XMAC 是否與 MAC 匹配來驗證該網路(步驟 122)。NAS 層 14 在步驟 122 亦計算對於 WTRU 12 的會話加密密鑰(即 AV 中的 CK 和 IK)。使用採用 RAND 作為輸入並應用共用密鑰 K 的預定義 UMTS 演算法來執行該密鑰的產生。

NAS 層 14 計算一回應(RES)並經由 UTRAN 18 將該

RES 發送到 VLR/SGSN 20(步驟 124、126)。VLR/SGSN 20 確定 RES 是否與 XRES 匹配以驗證 WTRU 12(步驟 128)。如果在步驟 122 和 128 中的這些驗證嘗試中的任一個失敗，則驗證都失敗。一旦相互驗證已經成功，則 VLR/SGSN 20 發送一驗證完成訊息到 HLR/AuC 22(步驟 130)，並且開始一本地安全啟動程序。

VLR/SGSN 20 發送一安全模式命令到 UTRAN 18，其包括經協商的 UMTS 加密演算法(UEA)和 UMTS 完整性演算法(UIA)，以及目前會話密鑰、CK 和 IK(步驟 132)。隨著安全通信現在可以開始，UTRAN 18 發送一具有用於完整性的訊息驗證碼(MAC-I)的安全模式命令到 RRC 層 16(步驟 134)。MAC-I 值保護安全模式命令訊息的完整性。MAC-I 是透過訊息內容上的 UIA 使用會話密鑰 IK 所計算出的一種散列。

RRC 層 16 發送一安全模式指示符到 NAS 層 14(步驟 136)，並且 NAS 層 14 載入安全性會話密鑰 IK 和 CK 到 RRC 層 16(步驟 138)。RRC 完整性保護實體透過以類似的方式使用安全模式命令訊息內容上具有 IK 的 UIA 來計算 MAC-I、並將計算出的 MAC-I 與接收到的 MAC-I 進行比較，由此來驗證接收到的訊息的完整性。RRC 層 16 還將 CK 載入到 RLC 密碼實體以開始加密(步驟 140)。如果驗證碼匹配，則 RRC 層 16 發送一安全模式完成訊息到 UTRAN 18(步驟 142)。VLR/SGSN 20 發送一附加接受訊息到 NAS 層 12(步驟 144)。

對於第 1 圖中說明的程序，具有 IMSI 的 RRC 連接請求訊息、RRC 建立請求訊息、RRC 建立完成訊息、具有可選 IMSI 的初始直接轉送訊息、驗證請求訊息以及驗證回應訊息未被保護，而是在一個無保護的開放環境中被發射。重要的 WTRU 識別碼(即 IMSI)通過無保護的空中介面被發送的事實引起了“IMSI 捕獲威脅”。被捕獲的 IMSI 可以由惡意的拒絕服務(DoS)攻擊或者對網路和用戶的其他可能攻擊所用。

因此，所希望的是提供一種對於附加和驗證程序的初始連接期間用於保護初始控制傳信訊息以及尤其是 WTRU 識別碼(即 IMSI)的方法和系統。

【發明內容】

本發明與一種在包括第三代(3G)LTE 的無線通信系統中用於對初始存取傳信訊息中的原始用戶識別碼進行安全保護的方法和設備有關。WTRU 包括控制平面(C-平面)封包資料聚合協定(C-PDCP)層，其執行傳信訊息的加密和完整性保護。C-PDCP 層在 WTRU 加電後被啟動並且初始安全參數被載入到 C-PDCP 層。對於網路附加的初始連接傳信訊息和用戶 ID(例如 IMSI)甚至在 WTRU 被驗證之前就使用初始安全參數而被加密。初始安全參數從通用用戶識別模組(USIM)中被載入並從網路所廣播的系統資訊中產生。該系統資訊包括公鑰組，其具有用於 IMSI 或者從中可以導出(一或多個)公鑰的資訊的非對稱加密的至少一公鑰。用於加

密的初始安全參數包括 CK。CK 可以是公鑰或者可以從網路系統資訊中所廣播或者導出的公鑰組中選擇。選定的公鑰的索引可以分開地進行編碼。或者，索引可以透過使用 Diffie-Hellman 密鑰交換方法而被傳送。

【實施方式】

在下文中，術語“WTRU”包括但不侷限於用戶設備(UE)、行動站、固定或行動用戶單元、傳呼機、蜂窩電話、個人數位助理(PDA)、電腦或者能夠在無線環境中操作的任何其他類型的設備。在下文中，術語“eNode-B”包括但不侷限於基地台、站點控制器、存取點(AP)或能夠在無線環境中操作的任何其他類型的周邊設備。

第 2 圖顯示出根據本發明的無線通信系統 200。該系統 200 包括 WTRU 210 和 LTE 網路 230。WTRU 210 包括：NAS 層 211、RRC 層 212、C -PDCP 層 213、U-平面 PDCP(U-PDCP)層 214 和較低層，該較低層包括：RLC 層 215、媒體存取控制層 216 和實體層 217。RRC 層 212 包括完整性保護實體 218。C-PDCP 層 213 包括 C-平面密碼實體 219，而 U-PDCP 層 214 包括 U-平面密碼實體 220。LTE 網路 230 包括 NAS 層 231、RRC 層 232、C-PDCP 層 233 和 U-PDCP 層 234。RRC 層 232 包括完整性保護實體 235。C-PDCP 層 233 包括 C-平面密碼實體 236，而 U-PDCP 層 234 包括 U-平面密碼實體 237。在 C-平面中，RRC 層 212 和 232 負責完整性保護，並且 C-PDCP 層 213 和 233 負責

NAS/RRC 控制傳信訊息的加密，而在 U-平面中，U-PDCP 層 214 和 234 負責網際網路協定(IP)標頭壓縮和加密。

根據本發明，C-PDCP 層 213 和 233 執行對先前無保護的初始 NAS 傳信訊息和 WTRU IMSI 傳輸的加密。另外，對傳信訊息的控制是透明的。本發明提供方法以用於安全參數的初始載入和產生、WTRU 210 和網路之間的加密密鑰佈置、IMSI 加密、以及初始 NAS 傳信訊息的 IMSI 加密的 WTRU 傳信調整，這將在下文中詳細解釋。

第 3 圖是根據本發明的用於附加和驗證的方法 300 的傳信圖。在 WTRU 加電後，WTRU 210 的 C-PDCP 層 213 被啟動(步驟 302)。RRC 層 212 接收由 eNode-B 250 所廣播的系統資訊並將其轉發到 C-PDCP 層 213(步驟 304)。系統資訊包括初始安全參數的資訊，該初始安全參數的資訊包括但不限於公鑰或者密鑰導出資訊、亂數(RAND)及/或密鑰種子 g_{KI} 。

初始安全參數在步驟 306 被載入到 C-PDCP 層 213 中，這將在下文中詳細解釋。C-PDCP 初始安全參數載入主要來自 WTRU 210 的通用用戶識別模組(USIM)中，其中用於 WTRU 210 的一致安全參數和運行值被更新並儲存。C-PDCP 初始安全參數另外可以是來自 eNode-B 250 所廣播的系統資訊，其可以包括公鑰資訊。用於加密的初始安全參數包括 CK 和 IK。CK 可以是公鑰或者可以從網路系統資訊所廣播或者導出的公鑰組中選擇。當第一 NAS/RRC 傳信訊息(例如 ATTACH 或者由它觸發的那些訊息)甚至在

WTRU 210 被驗證之前要被發射時，C-PDCP 層 213 準備操作(即準備執行加密/解密)。

NAS 層 211 透過發送附加訊息以及 IMSI 到 RRC 層 212 來觸發 RRC 連接(步驟 308)。RRC 層 212 發送一 LTE RRC 連接請求到 C-PDCP 層 213，該請求包括附加訊息和 MAC-I，並且較佳地包括公共陸地行動網路(PLMN)識別碼(ID)(步驟 310)。C-PDCP 層 213 然後用(來自 USIM 或者所廣播的系統資訊中的)初始 CK 對附加訊息和 IMSI 執行加密，並且發送包括經加密的附加訊息和 IMSI 在內的 LTE RRC 連接請求訊息以及來自 RRC 層 212 的 MAC-I(步驟 312、314)。與傳統附加程序不同，附加訊息和 IMSI 用初始 CK 和 IK 來保護。

LTE RRC 連接請求訊息還可以包括用於 Diffie-Hellman 密鑰交換的第二種子 g_{FRESH}，這將在下文中詳細解釋。eNode-B 250 基於包括在連接請求訊息中的 PLMN ID 來選擇合適的 aGW 260(步驟 316)。eNode-B 250 轉發附加訊息與 IMSI 到選定的 aGW 260(步驟 318)。

如果用戶未被驗證，則 aGW 260 發送一驗證資料請求到 HLR 270(或者 AuC)(步驟 320)。一旦收到驗證資料請求，HLR/AuC 270 發送一包括一組驗證向量(AV)的驗證資料回應到 aGW 260(步驟 322)。

aGW 260 發送驗證請求訊息到 WTRU 210 的 NAS 層 211，該驗證請求訊息包括來自第一 AV 的 RAND 和 AUTN(步驟 324)。連接回應訊息不必被加密或者進行完整

性保護。或者，連接回應訊息可以在 eNode-B 250 處利用傳統對稱加密演算法用來自 HLR/AuC 270 的具有索引的公鑰進行加密。NAS 層 211 然後通過計算期望的 MAC(XMAC)並確定該 XMAC 是否與 MAC 匹配來驗證該網路(步驟 326)。NAS 層 211 在步驟 326 亦計算新的會話密鑰(即 AV 中的 CK 和 IK)。使用採用 RAND 作為輸入並應用共用密鑰 K 的預定義演算法來執行密鑰的產生。

NAS 層 211 計算一回應(RES)並將包括 RES 在內的一驗證回應訊息發送到 aGW 260(步驟 328)。可選地，驗證回應訊息可以用初始 CK 及/或 IK 來保護。aGW 260 確定 RES 是否與 XRES 匹配以便驗證 WTRU 210(步驟 330)。如果在 326 和 330 中的這些驗證嘗試中任意一個失敗，則驗證都失敗。一旦相互驗證已經成功，則 aGW 260 發送一驗證完成訊息到 HLR/AuC 270(步驟 332)。

aGW 260 發送一安全模式命令訊息到 WTRU 210 的 RRC 層 212(步驟 334)。RRC 層 212 發送一安全模式指示符到 NAS 層 211(步驟 336)。NAS 層 211 將會話密鑰載入到 RRC 層 212(步驟 338)以及 C-PDCP 層 213(步驟 340)。RRC 層 212 然後用一用於 U-平面加密的新 CK 來配置 U-PDCP 層(第 3 圖中未示出)(步驟 342)。RRC 層 212 透過使用安全模式命令訊息內容上的 IK 計算 MAC-I 並將計算出的 MAC-I 與接收到的 MAC-I 進行比較來驗證接收到的安全模式命令訊息的完整性。如果它們匹配，則 RRC 層 212 發送一安全模式完成訊息到 eNode-B 250(步驟 344)。aGW 260

發送一附加接受訊息到 NAS 層 211(步驟 346)，並且安全通信(加密、解密以及完整性保護)開始。

在下文中會對在步驟 306 的加密參數的初始載入進行解釋。要被使用的加密演算法是將被選擇的參數中的一個。初始加密演算法可以是非對稱加密演算法並且稍後的預設加密演算法可以是諸如 f8 演算法之類的對稱演算法。可是，任何其他加密演算法都可以被使用。在下文中，為了說明的目的，將參考 f8 演算法參數解釋本發明。

第 4 圖顯示出包括傳統 f8 加密和密碼參數的加密方法。加密演算法可以是諸如 f8 之類的傳統對稱加密演算法或者是被用於以公鑰和私鑰進行加密的非對稱加密演算法。f8 演算法所必需的加密參數包括：CK 402、COUNT-C 值 404、承載 ID 406、方向值 408 和長度值 410。WTRU 210 使用 f8 演算法產生密鑰流塊 412，並把密鑰流塊 412 添加到未加密的明文輸入資料塊 414 中以產生已加密的資料塊 416，該資料塊被發射到網路 230。網路 230 也使用相同的 f8 演算法和相同的參數產生密鑰流塊 418，並將所產生的密鑰流塊 418 添加到接收到的加密資料塊 416 中以恢復明文資料塊 420。非對稱加密演算法的加密參數可能至少具有用於公鑰/私鑰對的 CK 402 並且可能具有其他參數。

CK 402 可以是非對稱加密系統中的公鑰/私鑰。WTRU 210 使用公鑰以用於加密整個上行鏈路 NAS 訊息或其一部分及/或包括 IMSI 在內的整個 RRC 初始存取訊息或其一部分，並且網路 230 用相應的私鑰來解密該已加密的 NAS 訊

息。CK 402 可以是 WTRU 210 和網路 230 之間所預置的公鑰/私鑰。或者，公鑰可以經由系統資訊被廣播。網路 230 可以只廣播一個公鑰，或者一組 n 個公鑰(k_1，…，k_n)或者用於密鑰導出的資訊。

如果一組公鑰被廣播，則 WTRU 210 從公鑰組中選擇一公鑰。在選擇公鑰時，WTRU 210 可以使用 FRESH 值來計算進入公鑰組內的索引(例如，索引 $a=FRESH\ \%\ n$)，以選擇初始 CK 402。或者，WTRU 210 可以對於密鑰索引使用它的 IMSI 值(即索引 $a=IMSI\ \%\ n$)，以選擇初始 CK 402。利用這個方案，增加了密鑰使用的隨機性並且對於安全攻擊者變得更困難。

因為網路 230 在 IMSI 已被正確解碼之前不知道 FRESH 值，並且因此不能夠獨立地計算選定公鑰的索引，所以與選定公鑰有關的資訊應該在 WTRU 210 和網路 230 之間被傳送。WTRU 210 可以在 NAS 訊息中包括選定公鑰的索引。例如，WTRU 210 用預先協商的公鑰(所述的 k_1)對選定公鑰的索引 a 進行編碼，並且 NAS 或 RRC 訊息的剩餘部分包括具有選定公鑰 k_a 的 IMSI。網路 230 首先解碼索引 a，然後解碼包括 IMSI 的具有選定公鑰 k_a 的整個訊息。

或者，可以使用 Diffie-Hellman 密鑰交換方法來選擇公鑰。LTE 網路 230 和 WTRU 210 商定已知的兩個值(一個非常大的質數 p 和欄位 F_p 的乘法群 F_p^* 的產生器 g)。LTE 網路 230 經由系統資訊廣播一組具有第一種子 g_{KI} 的公鑰，(其中隨機選擇的 KI 是 $1 \le KI \le p-2$ 並且 $g_{KI} \equiv g^{KI} \bmod p$)。公鑰組可以

來自於具有隨機週期性和順序的更大的加密密鑰群。WTRU 210 隨機選擇一值 $KIn2(1 \le KIn2 \le p-2)$來計算第二種子 $g_{KIn2} \equiv g^{KIn2} \bmod p$。WTRU 210 然後計算 $k' \equiv (g_{KI})^{KIn2} \bmod p$。公鑰索引 $a=k' \bmod n$，其中：n 是從系統資訊中廣播的具有第一種子 g_{KI} 的目前公鑰數量。計算出的 a 是所選公鑰 k_a 的公鑰組的索引。WTRU 210 對包括具有選定公共 k_a 的 IMSI 在內的 NAS 或 RRC 訊息進行加密並且在對 LTE 網路 230 的 NAS 或 RRC 訊息中包括第二種子 g_{KIn2}。第二種子不被加密。LTE 網路 230 首先採用未加密的第二種子 g_{KIn2} 並且計算 $k \equiv (g_{KIn2})^{KI} \bmod p$。然後對於私鑰索引 a 透過 $a \equiv k \bmod n$ 獲得索引 a。LTE 網路 230 然後用對應於公鑰 k_a 的私鑰解碼整個訊息。

COUNT-C 值 404 在初始階段可以是只有 WTRU 210 和 LTE 網路 230 知道的預置值。或者，COUNT-C 值 404 可以是被儲存在 USIM 中的 START（啟動）值(或者等價物)及其與只在 WTRU 210 和 LTE 網路 230 之間已知的其他值(例如 NAS 訊息序列號)結合的網路相應物。或者，COUNT-C 值 404 可以是如在 FRESH 值推導情況下由 WTRU 210 和 LTE 網路 230 計算出的值。

承載 ID 406 可以是已配置的通道的無線電承載 ID 值，比如對於傳信無線電承載 3(SRB-3)為'3'。或者，承載 ID 406 可以是某個預置的值。方向值 408 對於上行鏈路被設定為'0'。長度值 410 是以位元為單位的 NAS 或 RRC 訊息(包括 IMSI)長度。

在下文解釋步驟 306 的完整性保護參數的初始載入。

初始完整性保護能夠幫助抗擊拒絕服務攻擊。待使用的完整性保護演算法是將被選擇的參數中的一個。預設完整性保護演算法可以是 f9 演算法。可是，任何其他完整性保護演算法都可以被使用。在下文中，為了說明的目的，將參考 f9 演算法來解釋本發明。

第 5 圖顯示出傳統 f9 完整性保護程序和參數。f9 演算法所必需的參數包括 IK 502、COUNT-I 值 504、訊息 506、方向值 508 和 FRESH 值 510。WTRU 210 使用初始 IK 502 來為第一 NAS/RRC 訊息產生 MAC-I 512，並將所產生的 MAC-I 512 以及 NAS/RRC 訊息發送到網路 230。LTE 網路 230 產生具有相同參數 502-510 的期望 MAC-I(XMAC-I) 514 並將接收到的 MAC-I 512 和 XMAC-I 514 進行比較，以便在其已經為 WTRU 210 解碼 IMSI 之後驗證訊息完整性。

IK 502 可以由 WTRU 210(和網路 230)在初始 C-PDCP 啟動和配置期間使用從系統資訊中接收的 RAND 值來產生。例如，如第 6 圖所示，IK 502 可以透過使用 f4 演算法用亂數(RAND) 602 和共用密鑰(K) 604 來產生。給定經由 IMSI 在 WTRU 210 和網路 230 之間共用的密鑰 K 604，則所產生的 IK 502 承載 WTRU 210 與網路 230 之間的唯一關聯性的類似。它接著致能由完整性保護演算法 f9 所產生的 MAC-I，其承載了特定 WTRU 的簽名。

COUNT-I 值 504 可以是在初始階段只有 WTRU 210 和網路 230 知道的預置值。或者，COUNT-I 值 504 可以被設定為被儲存在 USIM 中的 START(啟動)值(或者等價物)及其

與只在 WTRU 210 和網路 230 之間已知的其他值(例如 NAS 訊息序列號)結合的網路相應物。或者，COUNT-I 值 504 可以是如在 FRESH 值推導情況下由 WTRU 210 和網路 230 計算出的值。

訊息參數 506 可以是在訊息前面附加了無線電承載識別碼的 NAS/RRC 訊息本身。方向值 508 對於上行鏈路被設定為某個值(例如，'0')。FRESH 值 510 可以從 WTRU 210 和網路 230 之間的一組預置的 FRESH 值($FRESH_0$，$FRESH_1$，…，$FRESH_{n-1}$)中選擇，其使用 IK 來計算索引 m(例如，m=IK % n)。或者，可以透過使用具有 RAND 602 和共用密鑰 604 的 FRESH 值作為輸入來產生 FRESH 值 510，如第 7 圖所示。

當第一 NAS 信號訊息要從 WTRU 210 中被發射時，這些安全參數的初始載入使 C-PDCP 層 212 能夠進入運轉狀態。必要時，這還使 C-PDCP 層 212 能夠加密隨後輸入和輸出的 NAS 傳信訊息。在正常 AKA 程序被成功執行時，C-PDCP 層 212 可以切換到從該程序中所產生的安全參數。

本發明還適用於在 AKA 完成之前在初始階段中的下行鏈路 NAS 訊息加密。為了在 AKA 之前讓下行鏈路加密工作，LTE 網路 230 需要使用 WTRU 210 用於第一上行鏈路訊息/IMSI 的相同“公鑰”(假定網路具有所有的公共/私鑰並且還已知密鑰索引)來加密 NAS/RRC 訊息並且加密演算法需要是諸如 f8 之類的對稱演算法。

實施例

1．一種在包括 WTRU 的無線通信系統中用於對初始連接傳信訊息中的用戶 ID 進行安全保護的方法，其中 WTRU 包括用於執行初始連接傳信訊息的加密和完整性保護的 C-PDCP 層。

2．如實施例 1 所述的方法，包括：在 WTRU 加電後啟動 C-PDCP 層。

3．如實施例 2 所述的方法，包括：將初始安全參數載入到 C-PDCP 層。

4．如實施例 3 所述的方法，包括：使用初始安全參數加密包括用戶 ID 的初始連接傳信訊息。

5．如實施例 4 所述的方法，包括：發送已加密的初始連接傳信訊息和用戶 ID 到網路。

6．如實施例 3-5 中任一實施例所述的方法，其中從 USIM 中載入初始安全參數。

7．如實施例 3-6 中任一實施例所述的方法，其中從網路中廣播的系統資訊中所產生初始安全參數。

8．如實施例 7 所述的方法，其中該系統資訊包括至少一公鑰或用於導出公鑰的資訊。

9．如實施例 1-8 中任一實施例所述的方法，其中初始連接傳信訊息包括 PLMN 識別碼。

10．如實施例 5-9 中任一實施例所述的方法，更包括：該網路發送驗證請求訊息到 WTRU，該驗證請求訊息包括亂數和驗證權杖。

11．如實施例 10 所述的方法，包括：WTRU 基於該亂數和該驗證權杖來驗證該網路。

12．如實施例 11 所述的方法，包括：WTRU 計算會話密鑰和 RES。

13．如實施例 12 所述的方法，包括：WTRU 發送包括 RES 在內的驗證回應訊息到網路。

14．如實施例 13 所述的方法，包括：網路使用該 RES 來驗證 WTRU。

15．如實施例 14 所述的方法，包括：網路發送安全模式命令訊息到 WTRU。

16．如實施例 13-15 中任一實施例所述的方法，其中透過使用初始安全參數來保護驗證回應訊息。

17．如實施例 15-16 中任一實施例所述的方法，其中該網路使用對稱加密演算法以被用來加密初始連接傳信訊息的密鑰來加密包括安全模式命令資訊的下行鏈路控制訊息。

18．如實施例 15-17 中任一實施例所述的方法，更包括：利用新會話密鑰來配置 U-平面 PDCP 層以用於 U 平面資料加密。

19．如實施例 3-18 中任一實施例所述的方法，其中待使用的加密演算法是初始安全參數的其中之一。

20．如實施例 19 所述的方法，其中加密演算法是 f8 演算法並且初始安全參數包括 CK、COUNT-C 值、承載 ID、方向值和長度值。

21．如實施例 20 所述的方法，其中 COUNT-C 值是只有 WTRU 和網路已知的預置值。

22．如實施例 20 所述的方法，其中 COUNT-C 值是儲存在 USIM 中與 WTRU 和網路之間已知的預協商值結合的啟動值。

23．如實施例 22 所述的方法，其中預協商值是 NAS 層序列號。

24．如實施例 20 所述的方法，其中 COUNT-C 值是由 WTRU 和網路所計算出的計算值。

25．如實施例 20-24 中任一實施例所述的方法，其中承載 ID 是傳信無線電承載 ID 號。

26．如實施例 20-24 中任一實施例所述的方法，其中承載 ID 是 WTRU 與網路之間的預置值。

27．如實施例 20-26 中任一實施例所述的方法，其中對於上行鏈路，方向值被設定為‘0’。

28．如實施例 4-19 中任一實施例所述的方法，其中加密演算法是非對稱加密演算法。

29．如實施例 28 所述的方法，其中加密演算法使用 CK，CK 是 WTRU 與網路之間的預置公鑰/私鑰對。

30．如實施例 29 所述的方法，其中，由網路經由系統資訊來廣播公鑰。

31．如實施例 30 所述的方法，其中 WTRU 從包括多個公鑰的公鑰組中選擇一公鑰。

32．如實施例 31 所述的方法，其中 WTRU 使用其 IMSI

值來選擇進入公鑰組內的索引以選擇一公鑰。

33·如實施例 31 所述的方法，其中 WTRU 使用 FRESH 值來選擇進入公鑰組內的索引以選擇一公鑰。

34．如實施例 33 所述的方法，其中 WTRU 以預協商的公鑰來加密該索引，並且在連接請求訊息中包括已加密的索引。

35·如實施例 30-34 中任一實施例所述的方法，其中該系統資訊包括第一密鑰索引種子，並且連接請求訊息包括第二密鑰索引種子，並且使用 Diffie-Hellman 密鑰交換方法來選擇公鑰。

36．如實施例 1-35 中任一實施例所述的方法，其中待使用的完整性保護演算法是初始安全參數的其中之一。

37．如實施例 36 所述的方法，其中完整性保護演算法是 f9 演算法，並且初始安全參數包括 IK、COUNT-I 值、訊息、方向值和 FRESH 值。

38．如實施例 37 所述的方法，其中，由 WTRU 使用經由系統資訊從網路所接收的亂數、和共用密鑰 K 來產生 IK。

39．如實施例 37 所述的方法，其中，使用 f4 演算法來產生 IK。

40．如實施例 37-39 中任一實施例所述的方法，其中 COUNT-I 值是 WTRU 和網路已知的預置值。

41．如實施例 37-40 中任一實施例所述的方法，其中 COUNT-I 值被設定為儲存在 USIM 中與 WTRU 和網路之間

已知的預協商值結合的啟動值。

42．如實施例 41 所述的方法，其中預協商值是 NAS 層序列號。

43．如實施例 37-42 中任一實施例所述的方法，其中 COUNT-I 值是由 WTRU 和網路所計算出的計算值。

44．如實施例 37-43 中任一實施例所述的方法，其中對於上行鏈路，方向值被設定為'0'。

45．如實施例 37-44 中任一實施例所述的方法，其中訊息是無線電承載 ID 加上第一 NAS 訊息。

46．如實施例 37-45 中任一實施例所述的方法，其中，從 WTRU 與網路之間的一組預置的 FRESH 值中選擇 FRESH 值。

47．如實施例 46 所述的方法，其中 IK 被用來計算 FRESH 值的索引。

48．如實施例 37-45 中任一實施例所述的方法，其中，使用 FRESH 值產生演算法用經由系統資訊所廣播的亂數、和共用密鑰 K 來產生 FRESH 值。

49．如實施例 1-48 中任一實施例所述的方法，其中該無線通信系統是 3G LTE。

50．一種在無線通信系統中用於對初始連接傳信訊息中的用戶 ID 進行安全保護的 WTRU。

51．如實施例 50 所述的 WTRU，包括：NAS 層，經配置成產生第一控制傳信訊息並觸發對網路的連接。

52．如實施例 50-51 中任一實施例所述的 WTRU，包

括：RRC 層，經配置成產生第二控制傳信訊息並執行第一和第二控制傳信訊息的完整性保護。

53．如實施例 51-52 中任一實施例所述的 WTRU，包括：C-PDCP 層，經配置成使用初始安全參數來執行包括初始連接傳信訊息和用戶 ID 在內的第一和第二控制傳信訊息的至少其中之一的加密，其中初始安全參數在 C-PDCP 層加電後被載入到 C-PDCP 層，該 C-PDCP 層更經配置成發送加密的初始連接傳信訊息和用戶 ID 到網路。

54．如實施例 53 所述的 WTRU，其中，從 USIM 中載入初始安全參數。

55．如實施例 53 所述的 WTRU，其中，從網路所廣播的系統資訊中產生初始安全參數。

56．如實施例 55 所述的 WTRU，其中該系統資訊包括至少一公鑰或用於導出公鑰的資訊。

57．如實施例 53-56 中任一實施例所述的 WTRU，其中初始連接傳信訊息包括 PLMN 識別碼。

58．如實施例 51-57 中任一實施例所述的 WTRU，其中 NAS 層經配置成基於包括在來自網路的驗證請求訊息中的亂數和驗證權杖來驗證網路、計算會話密鑰以及發送包括 RES 的驗證回應訊息到網路，使得網路使用 RES 驗證 WTRU。

59．如實施例 58 所述的 WTRU，其中，透過使用初始安全參數來保護驗證回應訊息。

60．如實施例 52-59 中任一實施例所述的 WTRU，更

包括 U-平面 PDCP 層，以用於處理 U-平面資料，RRC 層載入新會話密鑰到 U-平面 PDCP 層以用於 U-平面加密。

61．如實施例 53-60 中任一實施例所述的 WTRU，其中待使用的加密演算法是初始安全參數的其中之一。

62．如實施例 61 所述的 WTRU，其中加密演算法是 f8 演算法，其中初始安全參數包括 CK、COUNT-C 值、承載 ID、方向值和長度值的至少其中之一。

63．如實施例 62 所述的 WTRU，其中 COUNT-C 值是只有 WTRU 和網路已知的預置值。

64．如實施例 62 所述的 WTRU，其中 COUNT-C 值是儲存在 USIM 中與 WTRU 和網路之間已知的預協商值結合的啟動值。

65．如實施例 64 所述的 WTRU，其中預協商值是 NAS 層序列號。

66．如實施例 62 所述的 WTRU，其中 COUNT-C 值是由 WTRU 和網路所計算出的計算值。

67．如實施例 62-66 中任一實施例所述的 WTRU，其中承載 ID 是傳信無線電承載 ID 號。

68．如實施例 62-66 中任一實施例所述的 WTRU，其中承載 ID 是 WTRU 與網路之間的預置值。

69．如實施例 62-68 中任一實施例所述的 WTRU，其中對於上行鏈路，方向值被設定為'0'。

70．如實施例 53-69 中任一實施例所述的 WTRU，其中加密演算法是非對稱加密演算法。

71．如實施例 70 所述的 WTRU，其中加密演算法使用 CK，CK 是 WTRU 與網路之間的預置公鑰/私鑰對。

72．如實施例 71 所述的 WTRU，其中，經由系統資訊來廣播公鑰。

73．如實施例 72 所述的 WTRU，其中 C-PDCP 層從包括多個公鑰的公鑰組中選擇一公鑰。

74．如實施例 73 所述的 WTRU，其中 C-PDCP 層使用用戶 ID 來選擇進入公鑰組內的索引。

75．如實施例 73 所述的 WTRU，其中 C-PDCP 層使用 FRESH 值來選擇進入公鑰組內的索引。

76．如實施例 74-75 中任一實施例所述的 WTRU，其中 C-PDCP 層用預協商的公鑰來加密該索引，並在連接請求訊息中包括已加密的索引。

77．如實施例 74-76 中任一實施例所述的 WTRU，其中系統資訊包括第一密鑰索引種子，並且連接請求訊息包括第二密鑰索引種子，其中使用 Diffie-Hellman 密鑰交換方法來選擇公鑰。

78．如實施例 53-77 中任一實施例所述的 WTRU，其中待使用的完整性保護演算法是初始安全參數的其中之一。

79．如實施例 78 所述的 WTRU，其中完整性保護演算法是 f9 演算法，並且參數包括 IK、COUNT-I 值、訊息、方向值和 FRESH 值。

80．如實施例 79 所述的 WTRU，其中，由 WTRU 使

用經由系統資訊所接收的亂數、和共用密鑰 K 來產生 IK。

81．如實施例 79 所述的 WTRU，其中，透過使用 f4 演算法來產生 IK。

82．如實施例 79-81 中任一實施例所述的 WTRU，其中 COUNT-I 值是 WTRU 與網路已知的預置值。

83．如實施例 79-81 中任一實施例所述的 WTRU，其中 COUNT-I 值被設定為儲存在 USIM 中與 WTRU 和網路之間已知的預協商值結合的啟動值。

84．如實施例 83 所述的 WTRU，其中預協商值是 NAS 層序列號。

85．如實施例 79-81 中任一實施例所述的 WTRU，其中 COUNT-I 值是由 WTRU 和網路所計算出的計算值。

86．如實施例 79-85 中任一實施例所述的 WTRU，其中對於上行鏈路，方向值被設定為'0'。

87．如實施例 79-86 中任一實施例所述的 WTRU，其中訊息是無線電承載 ID 加上第一 NAS 訊息。

88．如實施例 79-87 中任一實施例所述的 WTRU，其中，從 WTRU 與網路之間的一組預置 FRESH 值中選擇 FRESH 值。

89．如實施例 88 所述的 WTRU，其中 IK 被用來計算 FRESH 值的索引。

90．如實施例 88 所述的 WTRU，其中，使用 FRESH 值產生演算法用經由系統資訊所廣播的亂數、和共用密鑰 K 來產生 FRESH 值。

91．如實施例 50-90 中任一實施例所述的 WTRU，其中無線通信系統是 3G LTE。

92．如實施例 50-91 中任一實施例所述的 WTRU，其中網路使用對稱加密演算法以被用來加密初始連接傳信訊息的密鑰來加密下行鏈路控制訊息。

雖然本發明的特徵和元件在較佳的實施方式中以特定的結合進行了描述，但每個特徵或元件可以在沒有所述較佳實施方式的其他特徵和元件的情況下單獨使用，或在與或不與本發明的其他特徵和元件結合的各種情況下使用。本發明提供的方法或流程圖可以在由通用電腦或處理器執行的電腦程式、軟體或韌體中實施，其中該電腦程式、軟體或韌體是以有形的方式包含在電腦可讀儲存媒體中的，關於電腦可讀儲存媒體的實例包括唯讀記憶體（ROM）、隨機存取記憶體（RAM）、暫存器、緩衝記憶體、半導體記憶裝置、內部硬碟和可移動磁片之類的磁性媒體、磁光媒體以及 CD-ROM 碟片和數位多功能光碟（DVD）之類的光學媒體。

舉例來說，恰當的處理器包括：通用處理器、專用處理器、傳統處理器、數位信號處理器（DSP）、多個微處理器、與 DSP 核心相關聯的一或多個微處理器、控制器、微控制器、專用積體電路（ASIC）、現場可編程閘陣列（FPGA）電路、任何一種積體電路（IC）及/或狀態機。

與軟體相關聯的處理器可以用於實現射頻收發信機，以在無線發射接收單元（WTRU）、用戶設備、終端、基地

台、無線電網路控制器或是任何一種主機電腦中加以使用。WTRU 可以與採用硬體及/或軟體形式實施的模組結合使用，例如相機、攝像機模組、視訊電路、揚聲器電話、振動裝置、揚聲器、麥克風、電視收發機、免持耳機、鍵盤、藍牙®模組、調頻(FM)無線電單元、液晶顯示器(LCD)顯示單元、有機發光二極體（OLED）顯示單元、數位音樂播放器、媒體播放器、視訊遊戲機模組、網際網路瀏覽器及/或任何一種無線區域網路（WLAN）模組。

【圖式簡單說明】

從以下關於較佳實施例的描述中可以更詳細地瞭解本發明，這些較佳實施例是作為實例而提供，並且是結合所附圖式而被理解的，其中：

第 1 圖顯示出 3G UMTS 網路中的初始附加和驗證程序；

第 2 圖顯示出根據本發明的無線通信系統；

第 3 圖是根據本發明的用於附加和驗證的程序的傳信圖；

第 4 圖顯示出包括傳統 f8 加密和加密參數的一個加密程序；

第 5 圖顯示出傳統 f9 完整性保護程序和參數；

第 6 圖顯示出根據本發明使用具有亂數(RAND)和共用密鑰(K)的 f4 演算法的 IK 的產生；以及

第 7 圖顯示出具有 RAND 和共用密鑰 K 的 FRESH 值的產生實例。

【主要元件符號說明】

10	3G UMTS 網路	18	UTRAN
20	VLR/SGSN	213、233	C-PDCP 層
250	eNode-B	260	aGW
22、270	HLR/AuC	200	無線通信系統
214、234	U- PDCP 層	215	RLC 層
216	媒體存取控制層	217	實體層
218、235	完整性保護實體	219、236	C-平面密碼實體
220、237	U-平面密碼實體	230	LTE 網路

402、CK	加密密鑰	404	COUNT-C 值
406	承載 ID	408、508	方向值
410	長度值	414	明文輸入資料塊
416	已加密的資料塊	420	明文資料塊
502、IK	完整性密鑰	504	COUNT-I 值
506	訊息	510	FRESH 值
512	MAC-I	514	XMAC-I
604、K	密鑰	602、RAND	亂數
NAS	非存取層	RRC	無線電資源控制
HLR	暫存器	AuC	驗證中心
LTE	長期演進	ID	用戶識別碼

12、210、WTRU	無線發射/接收單元
14、211、231	NAS 層
16、212、232	RRC 層
412、418	f8 演算法產生密鑰流塊
C-PDCP	控制平面(C 平面)封包資料聚合協定
PDCP	封包資料聚合協定
3G UMTS	第三代通用行動電信系統
UTRAN	通用陸地無線電存取網路
VLR	訪問者位置暫存器
SGSN	通用封包無線服務支援節點

十、申請專利範圍：

1. 一種對一初始連接傳信訊息中的一用戶識別碼(ID)進行安全保護的方法，該方法包括：

在一無線發射/接收單元(WTRU)加電後，啟動一控制平面(C-平面)封包資料聚合協定(C-PDCP)層；

在該 WTRU 加電後，從由該 WTRU 接收到的一系統資訊產生複數個初始安全參數；

將該複數個初始安全參數載入到該 C-PDCP 層；

使用該複數個初始安全參數加密包括該用戶 ID 的該初始連接傳信訊息，一 f8 演算法被用於該加密，以及該複數個初始安全參數包括一加密密鑰(CK)、一 COUNT-C 值、一承載 ID、一方向值和一長度值，該 COUNT-C 值是一預置值；以及

發送該加密的初始連接傳信訊息和該用戶 ID，該初始連接傳信訊息包括一公共陸地行動網路(PLMN)識別碼。

2. 如申請專利範圍第 1 項的方法，其中該複數個初始安全參數被載入至一通用用戶識別模組(USIM)。

3. 如申請專利範圍第 1 項所述的方法，其中該系統資訊包括至少一公鑰或用於導出一公鑰的一資訊。

4. 如申請專利範圍第 1 項所述的方法，更包括：

接收至該 WTRU 的一驗證請求訊息，該驗證請求訊息包括一亂數和一驗證權杖；

基於該亂數和該驗證權杖來驗證該網路；

計算一會話密鑰和一回應(RES)；

發送包括該 RES 的一驗證回應訊息到該網路；以及

接收至該 WTRU 的一安全模式命令訊息。

5. 如申請專利範圍第 4 項所述的方法，其中，藉由使用該複數個初始安全參數來保護該驗證回應訊息。

6. 如申請專利範圍第 4 項所述的方法，其中一網路使用一對稱加密演算法以被用來加密該初始連接傳信訊息的一密鑰來加密包括該安全模式命令訊息的一下行鏈路控制訊息。

7. 如申請專利範圍第 4 項所述的方法，更包括：

利用一新會話密鑰來配置一用戶平面(U 平面)PDCP 層以用於 U 平面資料加密。

8. 如申請專利範圍第 1 項所述的方法，其中該 COUNT-C 值是由該 WTRU 和一網路所計算出的一計算值。

9. 如申請專利範圍第 1 項所述的方法，其中該承載 ID 是一傳信無線電承載 ID 號。

10. 如申請專利範圍第 1 項所述的方法，其中該承載 ID 是一預置值。

11. 如申請專利範圍第 1 項所述的方法，其中，對於上行鏈路，該方向值被設定為'0'。

12. 如申請專利範圍第 1 項所述的方法，其中一非對稱加密演算法被用於加密。

13. 如申請專利範圍第 12 項所述的方法，其中該加密演算

法使用一加密密鑰(CK)，該 CK 是一預置公鑰/私鑰對。

14. 如申請專利範圍第 13 項所述的方法，其中，該公鑰是經由系統資訊來廣播。

15. 如申請專利範圍第 14 項所述的方法，其中該 WTRU 該公鑰是來自包括多個公鑰的一公鑰組。

16. 如申請專利範圍第 15 項所述的方法，其中一國際行動用戶識別碼(IMSI)值被用於選擇進入該公鑰組內的一索引以便選擇一公鑰。

17. 如申請專利範圍第 15 項所述的方法，其中一 FRESH 值被用於選擇進入該公鑰組內的一索引以便選擇一公鑰。

18. 如申請專利範圍第 17 項所述的方法，其中，以一預協商的公鑰來加密該索引並且在該初始連接傳信訊息中包括該加密的索引。

19. 如申請專利範圍第 15 項所述的方法，其中該系統資訊包括一第一密鑰索引種子，並且該連接請求訊息包括一第二密鑰索引種子，並且使用一 Diffie-Hellman 密鑰交換方法來選擇該公鑰。

20. 如申請專利範圍第 1 項所述的方法，其中一 f9 演算法被使用，並且該複數個初始安全參數包括一完整性密鑰(IK)、一 COUNT-I 值、一訊息、一方向值和一 FRESH 值。

21. 如申請專利範圍第 20 項所述的方法，其中，使用經由系統資訊接收到的一亂數、和一共用密鑰 K 來產生該

IK。

22. 如申請專利範圍第 21 項所述的方法，其中，使用一 f4 演算法來產生該 IK。

23. 如申請專利範圍第 20 項所述的方法，其中該 COUNT-I 值是一預置值。

24. 如申請專利範圍第 20 項所述的方法，其中該 COUNT-I 值被設定為儲存在一通用用戶識別模組(USIM)中與一預協商值結合的一啟動值。

25. 如申請專利範圍第 24 項所述的方法，其中該預協商值是一非存取層(Non-Access Stratum, NAS)層序列號。

26. 如申請專利範圍第 20 項所述的方法，其中該 COUNT-I 值是一計算值。

27. 如申請專利範圍第 20 項所述的方法，其中，對於上行鏈路，該方向值被設定為'0'。

28. 如申請專利範圍第 20 項所述的方法，其中該訊息是一無線電承載 ID 加上一第一非存取層(NAS)訊息。

29. 如申請專利範圍第 20 項所述的方法，其中，從一組預置 FRESH 值中選擇該 FRESH 值。

30. 如申請專利範圍第 29 項所述的方法，其中該 IK 被用來計算該 FRESH 值的一索引。

31. 如申請專利範圍第 20 項所述的方法，其中，使用一 FRESH 值產生演算法以利用經由系統資訊所廣播的一亂數、和一共用密鑰 K 來產生該 FRESH 值。

32. 如申請專利範圍第 1 項所述的方法，其中該無線通信

系統是一第三代(3G)長期演進(LTE)。

33. 一種對一初始連接傳信訊息中的一用戶識別碼(ID)進行安全保護的方法，該方法包括：

在一無線發射/接收單元(WTRU)加電後，啟動一控制平面(C-平面)封包資料聚合協定(C-PDCP)層；

在該 WTRU 加電後，接收一系統資訊；

從該系統資訊產生複數個初始安全參數；

將該複數個初始安全參數載入到該 C-PDCP 層；

使用該複數個初始安全參數以及一 f8 演算法來加密包括該用戶 ID 的該初始連接傳信訊息，該複數個初始安全參數包括一加密密鑰(CK)、一 COUNT-C 值、一承載 ID、一方向值和一長度值，該 COUNT-C 值是儲存在一通用用戶識別模組(USIM)中與一預協商值結合的一啟動值；以及

發送該加密的初始連接傳信訊息和該用戶 ID，該初始連接傳信訊息包括一公共陸地行動網路(PLMN)識別碼。

34. 如申請專利範圍第 33 項所述的方法，其中該預協商值是一非存取層(Non-Access Stratum, NAS)層序列號。

35. 一種用於對一初始連接傳信訊息中的一用戶識別碼(ID)進行安全保護的無線發射/接收單元(WTRU)，該 WTRU 包括：

一非存取層(NAS)層，經配置以產生一第一控制傳信訊息並觸發對一網路的一連接；

一無線電資源控制(RRC)層，經配置以產生一第二控制傳信訊息並執行該第一控制傳信訊息和該第二控制傳信訊息的完整性保護；以及

一控制平面(C 平面)封包資料聚合協定(C–PDCP)層，經配置以使用複數個初始安全參數來執行包括一初始連接傳信訊息和該用戶 ID 的該第一和該第二控制傳信訊息中的至少其中之一的加密，該複數個初始安全參數在該 WTRU 加電後被載入到該 C-PDCP 層，該 C-PDCP 層經配置以發送該加密的初始連接傳信訊息和該用戶 ID 到一網路，該複數個初始安全參數是在該 WTRU 加電後從該 WTRU 接收到的系統資訊產生，一 f8 演算法被用於該加密，以及該複數個初始安全參數包括一加密密鑰(CK)、一 COUNT-C 值、一承載 ID、一方向值和一長度值，該 COUNT-C 值是一預置值，以及該初始連接傳信訊息包括一公共陸地行動網路(PLMN)識別碼。

36. 如申請專利範圍第 35 項所述的 WTRU，其中該複數個初始安全參數被載入至一通用用戶識別模組(USIM)。

37. 如申請專利範圍第 35 項所述的 WTRU，其中該系統資訊包括至少一公鑰或用於導出一公鑰的一資訊。

38. 如申請專利範圍第 35 項所述的 WTRU，其中該 NAS 層經配置以基於被包括在來自該網路的一驗證請求訊息中的一亂數和一驗證權杖來驗證該網路、計算一會話密鑰以及發送包括一回應(RES)的一驗證回應訊息

到該網路，使得該網路使用該 RES 來驗證該 WTRU。

39. 如申請專利範圍第 38 項所述的 WTRU，其中，該驗證回應訊息是藉由使用該複數個初始安全參數來保護。

40. 如申請專利範圍第 38 項所述的 WTRU，更包括：

一用戶平面(U 平面)PDCP 層，用於處理一 U 平面資料，該 RRC 層載入一新會話密鑰到該 U 平面 PDCP 層以用於 U-平面加密。

41. 如申請專利範圍第 35 項所述的 WTRU，其中該 COUNT-C 值是由該 WTRU 和該網路所計算出的一計算值。

42. 如申請專利範圍第 35 項所述的 WTRU，其中該承載 ID 是一傳信無線電承載 ID 號。

43. 如申請專利範圍第 35 項所述的 WTRU，其中該承載 ID 是該 WTRU 與該網路之間的一預置值。

44. 如申請專利範圍第 35 項所述的 WTRU，其中，對於上行鏈路，該方向值被設定為'0'。

45. 如申請專利範圍第 35 項所述的 WTRU，其中該加密演算法是一非對稱加密演算法。

46. 如申請專利範圍第 45 項所述的 WTRU，其中該加密演算法使用一加密密鑰(CK)，該 CK 是該 WTRU 與該網路之間的一預置公鑰/私鑰對。

47. 如申請專利範圍第 46 項所述的 WTRU，其中，該公鑰是經由系統資訊來廣播。

48. 如申請專利範圍第 47 項所述的 WTRU，其中該

C-PDCP 層從包括多個公鑰的一公鑰組中選擇一公鑰。

49. 如申請專利範圍第 48 項所述的 WTRU，其中該系統資訊包括一第一密鑰索引種子，並且該連接請求訊息包括一第二密鑰索引種子，其中使用一 Diffie-Hellman 密鑰交換方法來選擇該公鑰。

50. 如申請專利範圍第 47 項所述的 WTRU，其中該 C-PDCP 層使用該用戶 ID 來選擇進入該公鑰組內的一索引。

51. 如申請專利範圍第 47 項所述的 WTRU，其中該 C-PDCP 層使用一 FRESH 值來選擇進入該公鑰組內的一索引。

52. 如申請專利範圍第 51 項所述的 WTRU，其中該 C-PDCP 層用一預協商的公鑰來加密該索引，並在該連接請求訊息中包括該加密的索引。

53. 如申請專利範圍第 35 項所述的 WTRU，其中一 f9 演算法被使用，並且該複數個初始安全參數包括一完整性密鑰(IK)、一 COUNT-I 值、一訊息、一方向值和一 FRESH 值。

54. 如申請專利範圍第 53 項所述的 WTRU，其中，由該 WTRU 使用經由系統資訊所接收的一亂數和一共用密鑰 K 來產生該 IK。

55. 如申請專利範圍第 54 項所述的 WTRU，其中，該 IK 是使用一 f4 演算法來產生。

56. 如申請專利範圍第 53 項所述的 WTRU，其中該

COUNT-I 值是該 WTRU 和該網路已知的一預置值。

57. 如申請專利範圍第 53 項所述的 WTRU，其中該 COUNT-I 值被設定為儲存在一通用用戶識別模組(USIM)中與該WTRU和該網路之間已知的一預協商值結合的一啟動值。

58. 如申請專利範圍第 57 項所述的 WTRU，其中該預協商值是一非存取層(Non-Access Stratum, NAS)層序列號。

59. 如申請專利範圍第 53 項所述的 WTRU，其中該 COUNT-I值是由該WTRU和該網路所計算出的一計算值。

60. 如申請專利範圍第 53 項所述的 WTRU，其中，對於上行鏈路，該方向值被設定為'0'。

61. 如申請專利範圍第 53 項所述的 WTRU，其中該訊息是一無線電承載 ID 加上一第一非存取層(Non-Access Stratum, NAS)訊息。

62. 如申請專利範圍第 53 項所述的 WTRU，其中該 FRESH 值是從該 WTRU 與該網路之間的一組預置 FRESH 值中選擇。

63. 如申請專利範圍第 62 項所述的 WTRU，其中該 IK 被用來計算該 FRESH 值的一索引。

64. 如申請專利範圍第 53 項所述的 WTRU，其中該 FRESH 值是藉由使用一FRESH值產生演算法以經由系統資訊所廣播的一亂數、和一共用密鑰 K 來產生。

65. 如申請專利範圍第 35 項所述的 WTRU，其中該無線通

信系統是一第三代(3G)長期演進(LTE)。

66. 如申請專利範圍第 35 項所述的 WTRU，其中該網路使用一對稱加密演算法以被用來加密該初始連接傳信訊息的一密鑰來加密一下行鏈路控制訊息。

67. 一種用於對一初始連接傳信訊息中的一用戶識別碼(ID)進行安全保護的無線發射/接收單元(WTRU)，該 WTRU 包括：

一非存取層(NAS)層，經配置以產生一第一控制傳信訊息並觸發對一網路的一連接；

一無線電資源控制(RRC)層，經配置以產生一第二控制傳信訊息並執行該第一控制傳信訊息和該第二控制傳信訊息的完整性保護；以及

一控制平面(C 平面)封包資料聚合協定(C–PDCP)層，經配置以至少部分：

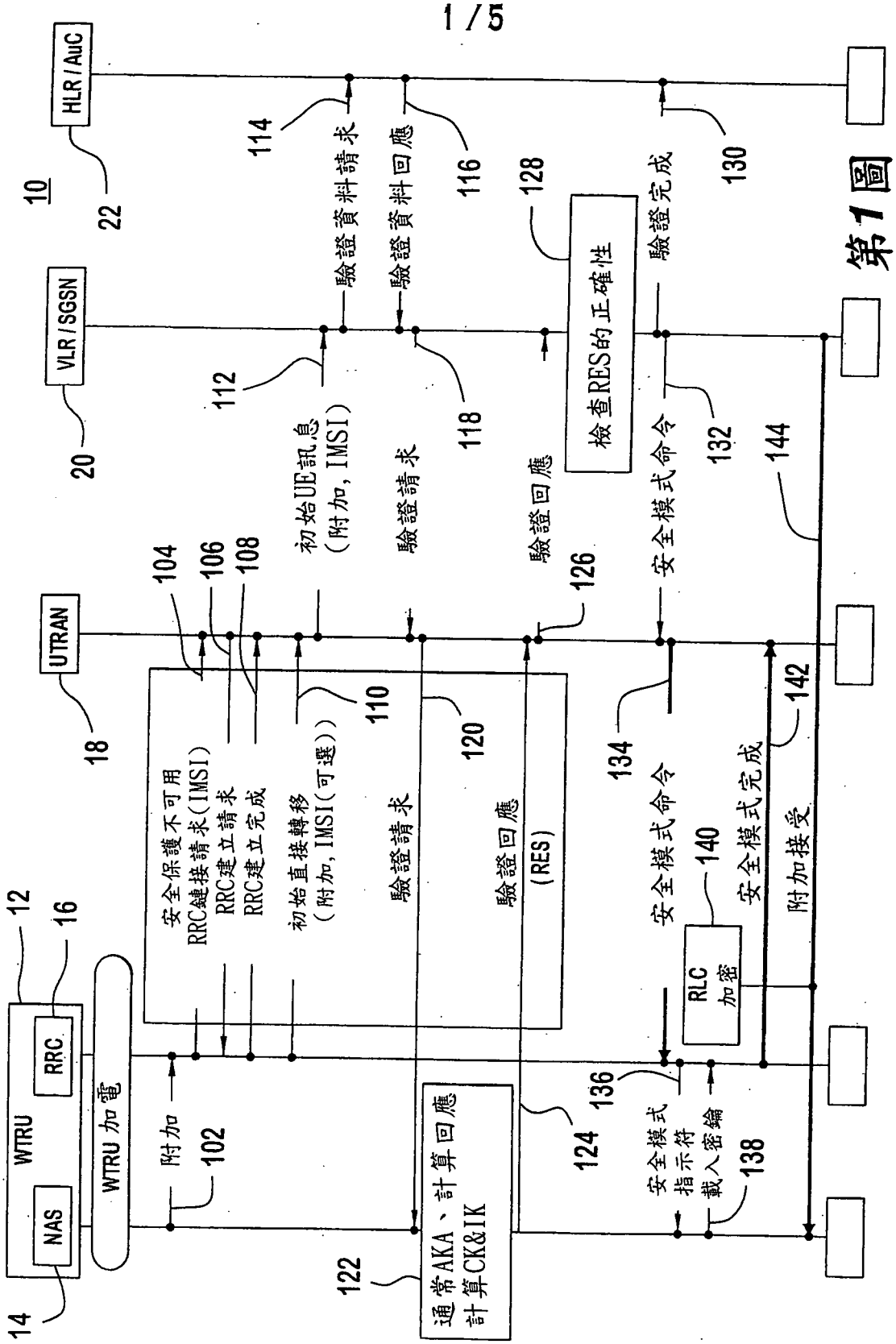
使用一 f8 演算法以及複數個初始安全參數來執行包括一初始連接傳信訊息和該用戶 ID 的該第一和該第二控制傳信訊息中的至少其中之一的加密，該複數個初始安全參數是在該 WTRU 加電後從接收到的一系統資訊產生，以及該複數個初始安全參數被載入到該 C-PDCP 層；以及

發送該加密的初始連接傳信訊息和該用戶 ID 到一網路，該複數個初始安全參數包括一加密密鑰(CK)、一 COUNT-C 值、一承載 ID、一方向值和一長度值的至少其中之一，以及該 COUNT-C 值是儲存在一

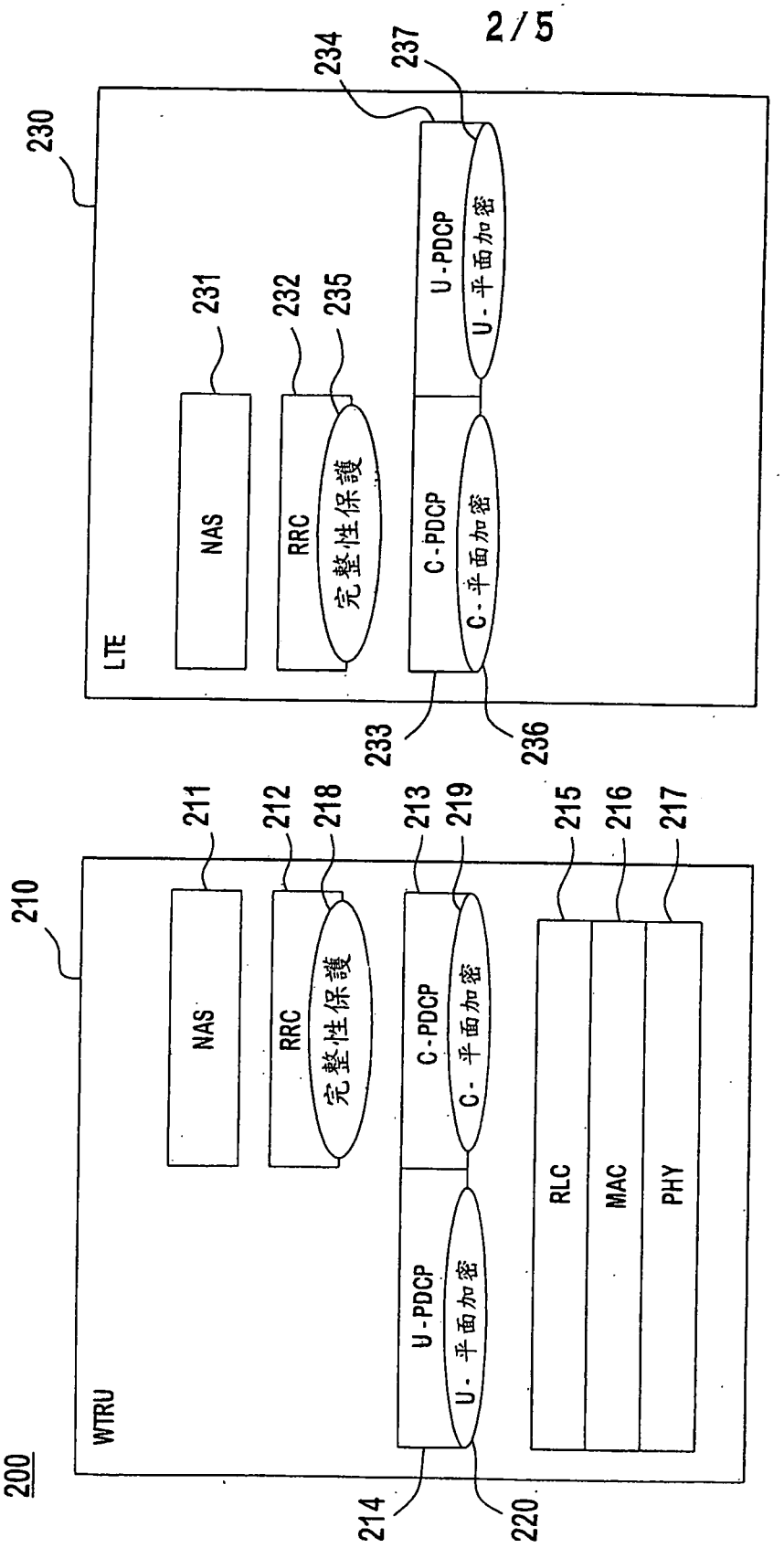
通用用戶識別模組(USIM)中與一預協商值結合的一啟動值，該初始連接傳信訊息包括一公共陸地行動網路(PLMN)識別碼。

68. 如申請專利範圍第 67 項所述的 WTRU，其中該預協商值是一非存取層(NAS)層序列號。

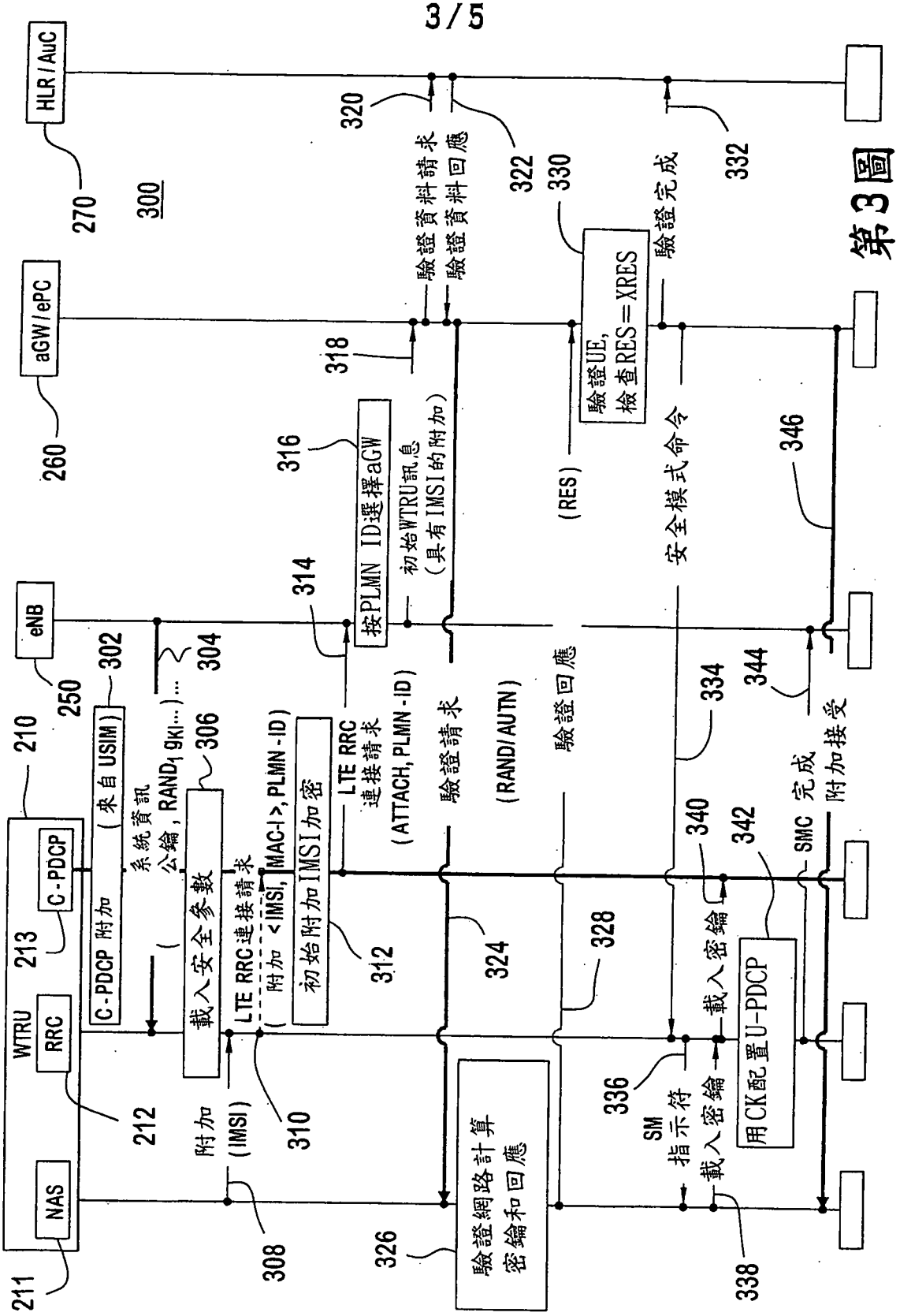
十一、圖式：


10
HLR / AuC
22
VLR / SGSN
20
UTRAN
18
WTRU
NAS
RRC
14
12
16
WTRU 加電
附加
102
安全保護不可用
RRC鏈接請求(IMSI)
RRC建立請求
RRC建立完成
104
106
108
初始直接轉移
(附加, IMSI(可選))
110
初始UE訊息
(附加, IMSI)
112
驗證請求
114
驗證資料請求
116
驗證資料回應
118
驗證請求
120
通常AKA、計算回應
計算CK&IK
122
驗證回應
(RES)
124
檢查RES的正確性
128
驗證回應
126
驗證完成
130
安全模式命令
132
安全模式命令
134
RLC
加密
140
安全模式完成
142
附加接受
144
安全模式
指示符
載入密鑰
136
138

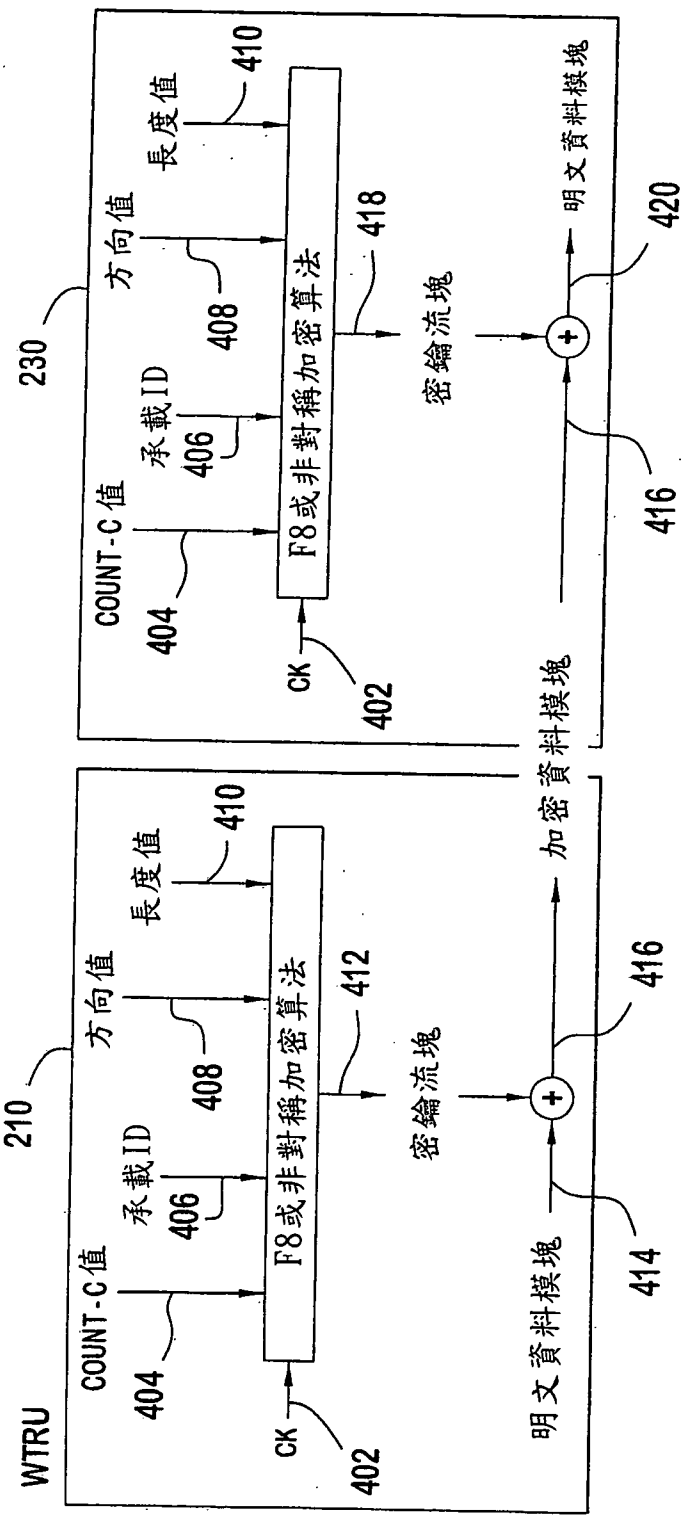
第1圖


200
WTRU
210
211
212
218
213
219
215
216
217
NAS
RRC
完整性保護
C-PDCP
C-平面加密
U-PDCP
U-平面加密
RLC
MAC
PHY
214
220
LTE
230
231
232
235
234
237
NAS
RRC
完整性保護
C-PDCP
C-平面加密
U-PDCP
U-平面加密
233
236

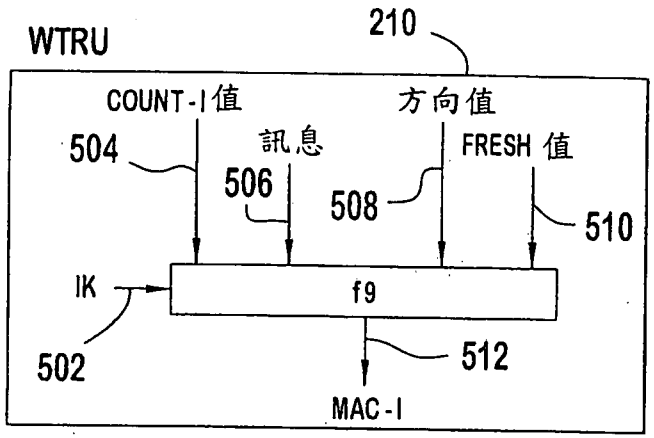
第2圖

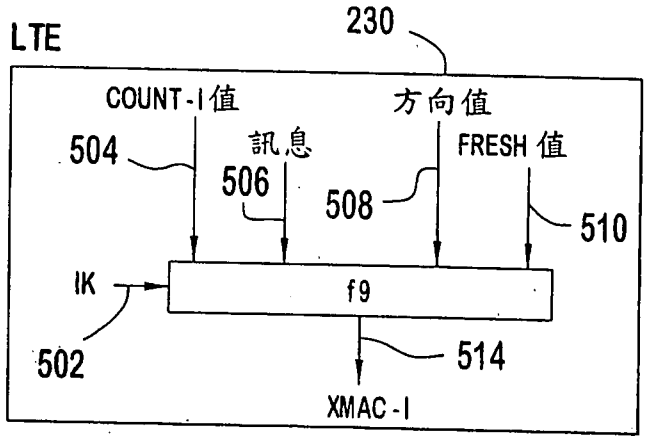

HLR/AuC
270
300
aGW/ePC
260
eNB
250
210
WTRU
RRC
NAS
211
C-PDCP
213
212
C-PDCP 附加 (來自USIM)
302
系統資訊
(公鑰, RAND1, gKI...)...
304
載入安全參數
306
附加 (IMSI)
LTE RRC連接請求
附加 <IMSI, MAC-I>, PLMN-ID)
310
308
初始附加IMSI加密
312
LTE RRC
連接請求
(ATTACH, PLMN-ID)
314
按PLMN ID選擇aGW
316
初始WTRU訊息
(具有IMSI的附加)
318
驗證資料請求
驗證資料回應
320
322
驗證請求
(RAND/AUTN)
324
驗證回應
328
330
驗證UE,
檢查RES=XRES
(RES)
安全模式命令
334
驗證完成
332
346
344
SMC 完成
附加接受
載入密鑰
340
342
用CK配置U-PDCP
SM
指示符
載入密鑰
336
338
驗證網路計算
密鑰和回應
326

第3圖

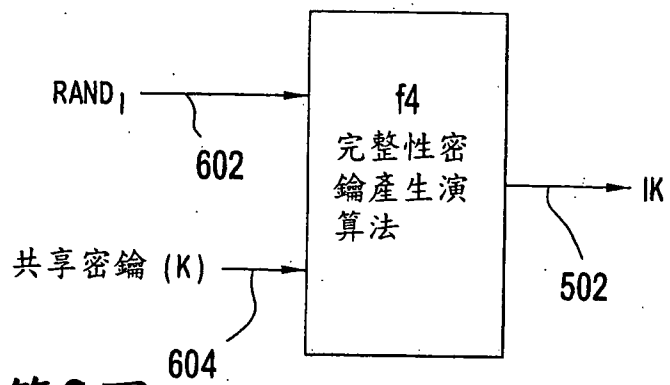

WTRU
210
COUNT-C值
404
承載ID
406
方向值
408
長度值
410
CK
402
F8或非對稱加密算法
412
密鑰流塊
414
明文資料模塊
416
加密資料模塊
230
COUNT-C值
404
承載ID
406
方向值
408
長度值
410
CK
402
F8或非對稱加密算法
418
密鑰流塊
416
明文資料模塊
420

第4圖

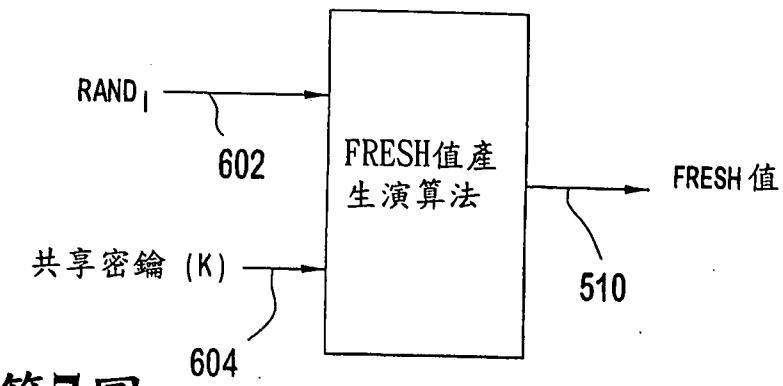

WTRU
210
COUNT-I值
方向值
504
訊息
506
508
FRESH 值
510
IK
f9
502
512
MAC-I


LTE
230
COUNT-I值
方向值
504
訊息
506
508
FRESH 值
510
IK
f9
502
514
XMAC-I

第5圖


RAND I
602
f4
完整性密鑰產生演算法
IK
共享密鑰 (K)
502
604

第6圖


RAND I
602
FRESH值產生演算法
FRESH 值
共享密鑰 (K)
510
604

第7圖