I672933

(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 I672933 B**

(45)公告日： 中華民國 108 (2019) 年 09 月 21 日

(21)申請案號：104135269 (22)申請日： 中華民國 104 (2015) 年 10 月 27 日

(51)Int. Cl.： ***H04L9/16*** ***(2006.01)*** ***H04L9/14*** ***(2006.01)***
H04L9/28 ***(2006.01)*** ***H04W84/02*** ***(2009.01)***
H04L12/70 ***(2013.01)***

(30)優先權：2014/10/29 美國 62/072,388
2015/10/26 美國 14/923,223

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED (US)
美國

(72)發明人：李秀凡 LEE, SOO BUM (KR)；霍恩蓋文伯納德 HORN, GAVIN BERNARD (US)；
帕拉尼古德艾納德 PALANIGOUNDER, ANAND (IN)

(74)代理人：李世章

(56)參考文獻：

US	8452957B2	US	2013/0097418A1
US	2013/0322347A1	WO	2014/002351A1
WO	2014/059657A1	WO	2014/088120A1

審查人員：林東威

申請專利範圍項數：26 項 圖式數：28 共 130 頁

(54)名稱

用於下一代蜂巢網路的使用者面安全

(57)摘要

經由在設備(例如，晶片組件、客戶端設備)處獲得第一共用金鑰，並在該設備處，獲得基於第一共用金鑰的第二共用金鑰，可以在該設備處實現確保該設備和封包資料網路閘道(P-GW)之間的使用者面資料傳輸量安全。第二共用金鑰可以用於確保使用者面資料傳輸量在該設備和 P-GW 之間傳輸期間的安全。該設備和 P-GW 共用第二共用金鑰。可以基於第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量。可以經由存取節點來向 P-GW 發送第一安全的資料傳輸量。P-GW 和存取節點是不同的網路實體。第二共用金鑰是存取節點不知道的。P-GW 從與該設備不同的網路實體獲得第二共用金鑰。

Securing user-plane data traffic between a device and a packet data network gateway (P-GW) may be accomplished at the device (e.g., chip component, client device) by obtaining, at the device, a first shared key, and obtaining, at the device, a second shared key based on the first shared key. The second shared key may be for securing user-plane data traffic during transit between the device and the P-GW. The second shared key is shared by the device and the P-GW. The data traffic may be secured based on the second shared key to produce first secured data traffic. The first secured data traffic may be sent to the P-GW via an access node. The P-GW and the access node are distinct network entities. The second shared key is unknown to the access node. The P-GW obtains the second shared key from a network entity that is distinct from the device.

指定代表圖：

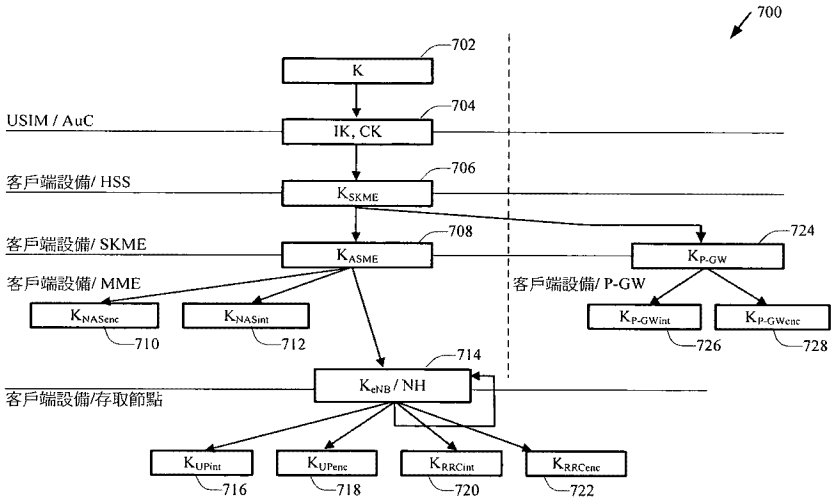

圖7

符號簡單說明：

700・・・金鑰等級

702・・・K 金鑰

704・・・IK、CK 金鑰

706・・・K_{SKME} 金鑰

708・・・K_{ASME} 金鑰

710・・・K_{NASenc} 金鑰

712・・・K_{NASint} 金鑰

714・・・K_{eNB} 金鑰

716・・・K_{UPint} 金鑰

718・・・K_{UPenc} 金鑰

720・・・K_{RRCint} 金鑰

722・・・K_{RRCint} 金鑰

724・・・K_{P-GW} 金鑰

726・・・$K_{P-GWint}$ 金鑰

728・・・$K_{P-GWenc}$ 金鑰

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

用於下一代蜂巢網路的使用者面安全

USER-PLANE SECURITY FOR NEXT GENERATION CELLULAR NETWORKS

【0001】本專利申請案主張享有2014年10月29日在美國專利和商標局提交的美國臨時申請案第62/072,388號，以及2015年10月26日在美國專利和商標局提交的美國專利申請案第14/923,223號的優先權和利益，以引用方式將它們的全部內容併入本文。

【技術領域】

【0002】概括地說，本案內容係關於通訊系統，並且更特別地，本案內容係關於用於在無線通訊系統中保護使用者面訊息傳遞的系統。

【先前技術】

【0003】圖1是根據先前技術的第四代（4G）蜂巢網路100的元素的視圖。4G蜂巢網路100可以包括存取部分（例如，無線電存取網路（RAN））和核心部分（例如，核心網路），本文可以將存取部分稱爲進化型通用陸地無線電存取網路（E-UTRAN）102，本文可以將核心部分稱爲進化型封包核心（EPC）104。E-UTRAN 102和EPC 104一起構成進化型封包系統（EPS）。

【0004】EPS可以與客戶端設備106（例如，行動設備、行動終端、使用者設備（UE）、終端）進行通訊。客戶端設備106可以包括通用用戶辨識模組（USIM）108（其通常稱爲SIM卡）。USIM 108可以是安全地儲存例如國際行動用戶標識（IMSI）號和其相關的金鑰K的積體電路晶片。金鑰K可以是根金鑰。

【0005】將EPS中的通訊劃分爲多個平面（亦即，使用者面（UP）和控制面（CP））中。在圖1中，一個特定的控制面訊號傳遞路徑經由存取節點112（例如，eNodeB）和行動性管理實體（MME）114之間的虛線110來標識，而一個特定的使用者面資料傳輸量路徑經由存取節點112和服務閘道（S-GW）118之間的實線116來標識。本發明所屬領域中具有通常知識者知道用於控制面訊號傳遞和使用者面資料傳輸量的額外的和替代的路徑。圖1的視圖是示例性的，並不意欲是限制性的。

【0006】E-UTRAN 102包括存取節點112，存取節點112包括與客戶端設備106進行無線通訊的硬體。在長期進化型（LTE）網路中，存取節點112可以稱爲進化型節點B（eNodeB）。舉例而言，單個LTE存取節點可以服務一或多個E-UTRAN 102細胞。

【0007】EPC 104包括封包資料網路（PDN）閘道（P-GW）120。P-GW 120用作至封包資料網路122（例如，網際網路及/或專用的企業網）的閘道。P-GW 120可以被視作爲至封包資料網路122的通道；其是網路策略實施的點。可以將存取節點

112視作爲用於客戶端設備106到核心網路（例如，EPC 104）的空中存取的通道。存取節點112可以與P-GW 120並置在一起，但存取節點112的功能與P-GW 120的功能不同。換言之，即使它們並置在一起，存取節點112和P-GW 120亦是具有單獨功能的單獨實體。

【0008】此外，EPC 104亦包括歸屬用戶伺服器（HSS）124。HSS 124儲存每個客戶端設備106的唯一標識。認證中心（AuC）126可以耦合到HSS 124。當客戶端設備106嘗試連接到EPC 104時，AuC 126可以用於對USIM 108進行認證。AuC 126可以儲存與在USIM 108中所儲存的金鑰相同的金鑰（例如，根金鑰K）。換言之，AuC 126可以儲存在USIM 108中儲存的根金鑰K的第二例子。不經由空中來發送根金鑰。當客戶端設備106加電時，通常可以發生AuC 126對USIM 108的認證。

【0009】EPC 104亦包括S-GW 118。S-GW 118執行與傳輸使用者面IP訊息往返客戶端設備106有關的功能。通常，應當理解的是，訊息可以包括一或多個封包。封包和訊息可以具有不同的格式，並經由不同的標頭進行封裝。爲了本文便於引用起見，通篇使用術語訊息。

【0010】EPC 104亦包括MME 114。MME 114執行與建立、維持和釋放各個實體通道有關的功能。MME 114可以準備用於訊息通訊的承載。MME 114包含在控制面中，而客戶端設備106、存取節點112、S-GW 118、P-GW 120和HSS 124包含在控制面和使用者面兩者中。

【0011】當客戶端設備106與網路（例如，EPC 104）進行通

訊時，使用由MME 114在連接程序期間分配的臨時行動用戶標識（TMSI）進行標識。亦經由IP位址來標識客戶端設備106，只要客戶端設備106一加電，P-GW 120就分配該IP位址。

控制面

【0012】在控制面中，當客戶端設備106尋求連接到網路時，其將聯絡存取節點112。存取節點112將選擇用於該客戶端設備106的MME 114。MME 114將選擇S-GW 118和P-GW 120。可以根據存取點名稱（APN）來選擇P-GW 120，其中該APN通常是由使用者或使用者的操作者提供的。從所選定的P-GW 120向客戶端設備106分配IP位址，並且客戶端設備106因此連接到蜂巢網路100。

使用者面

【0013】一旦進行了連接，客戶端設備106就可以經由存取節點112，在使用者面上向P-GW 120發送訊息（例如，用於語音和資料的資料傳輸量）和從P-GW 120接收訊息。爲了確保客戶端設備106和存取節點112之間的使用者面鏈路安全，這兩個節點目前匯出稱爲K_{UPenc}金鑰的加密金鑰。結合在圖3中描述的金鑰等級裡提供的K_{UPenc}金鑰316，來提供K_{UPenc}金鑰的匯出的解釋。爲了確保存取節點112和P-GW 120之間的使用者面回載鏈路安全，這兩個節點依賴於網際網路協定安全（IPSEC）。IPSEC是用於經由對通訊通信期的每一個IP封包進行認證和加密，來確保網際網路協定（IP）通訊安全的協定組。應當注意的是，在承載基礎中沒有定義回載安全，但網路域安全（NDS）進行了定義。

【0014】蜂巢網路100在下行鏈路和上行鏈路方向兩者中，提供了用於使用者面資料傳輸量流動往返存取節點112的安全。在下行鏈路方向中，當攜帶使用者資料傳輸量的IP訊息（例如，來自諸如網際網路的封包資料網路122）到達P-GW 120時，可以使用IPSEC對該訊息進行加密，並將其安全地傳送到存取節點112。可以在存取節點112處，對該訊息進行解密。因此，在存取節點112上可以存在未加密的訊息資料。隨後，再次對該訊息進行加密，並使用K_{UPenc}金鑰將其從存取節點112安全地傳送到客戶端設備106。在上行鏈路方向中，當攜帶使用者資料的IP訊息被設置爲經由空中來從客戶端設備106向存取節點112發送時，可以使用K_{UPenc}金鑰對該訊息進行加密並將其安全地傳送到存取節點112。可以存取節點112處，對該訊息進行解密。同樣，因此在存取節點112上可以存在未加密的訊息資料。隨後，可以再次對該訊息進行加密，並使用IPSEC將其從存取節點112安全地傳送到P-GW 120。

【0015】加密提供的安全應當優選地保持訊息安全，免受協力廠商或者甚至在不信任位置中部署或者被損害的存取節點的攻擊。如下面將描述的，客戶端設備106和存取節點112均匯出K_{UPenc}金鑰，該K_{UPenc}金鑰用於確保在客戶端設備106和存取節點112之間的上行鏈路方向和下行鏈路方向，在空中行進的資料傳輸量安全。使用者面安全終止在存取節點112處。使用者面安全取決於存取節點112的正確行爲，如前述，當訊息資料等待輪到其在其路徑上從存取節點112傳送到P-GW 120或者客戶端設備106時，存取節點112保持未加密的該資料。

【0016】應當注意，如在非存取層（NAS）和存取層（AS）之間，單獨地定義安全。NAS提供對核心網路節點（例如，MME 114）和客戶端設備106之間的通訊的處理。AS提供存取節點112和客戶端設備106之間的通訊。另外，與使用者面上的安全相比，單獨地定義控制面上的安全。

【0017】幾個實例圖示維持使用者面上的安全的重要性。例如，若協力廠商損害了存取節點112的安全，則該協力廠商可以能夠直接從存取節點112擷取未加密的資料。經由第二個實例，攻擊者可以使用其自己資料來替換使用者的資料。接收方將不能夠斷定該資料不是來自於使用者。經由第三個實例，攻擊者可能翻轉使用者的訊息中的位元，這將導致傳輸不能進行適當地解密的訊息，因此浪費寶貴的資源。

【0018】由於存取節點112可以位於公共場所（例如，不信任或不安全的位置），這使其更容易受到敵對攻擊，存取節點112可以是攻擊的目標。另外，許多存取節點（如，類似於存取節點112）由多個行動網路服務供應商（MNO）共用。行動網路服務供應商可能不是都根據相同級別的安全和監管進行操作，這使得一個惡意實體可以經由具有鬆懈安全實踐的行動網路服務供應商來獲得至存取節點112的存取。

【0019】在4G網路中，使用者面安全終止於存取節點112處，存取節點112是發送和接收客戶端設備106訊息的地方。因此，使用者面資料的客戶端設備106私密性取決於存取節點112的完整性（或者安全狀態）。若存取節點112被損害或部署在不信任位置，則客戶端設備106的使用者面資料傳輸量的

安全性亦處於被損害的危險之中。

【0020】這種使用者面安全對於存取節點112的依賴性與4G安全架構的設計原則之間關係緊張，其中4G安全架構尋求不太信任存取節點112，並因此更少依賴於存取節點112。與在4G網路中相比，在所提出的下一代蜂巢網路（例如，5G）中，甚至可以更不信任存取節點112的，這是由於需要進行網路緻密化以支援更高的容量及/或頻寬、網格節點或者中繼節點，其中這些節點涵蓋存取節點或者存取節點功能。

【0021】因此，爲了P-GW 120和客戶端設備106之間的安全通訊起見，去除存取節點112作爲受信任實體將是有益的。

【發明內容】

【0022】根據一個態樣，一種在設備處操作的方法可以包括：在該設備處，獲得第一共用金鑰；及在該設備處，獲得基於第一共用金鑰的第二共用金鑰。第二共用金鑰可以用於確保資料傳輸量在該設備和封包資料網路閘道（P-GW）之間傳輸期間的安全。該設備和P-GW可以共用第二共用金鑰；但是，它們可以彼此之間獨立地獲得第二共用金鑰。

【0023】該設備可以基於第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量。隨後，該設備可以經由存取節點來向P-GW發送第一安全的資料傳輸量，其中P-GW和該存取節點是不同的網路實體。

【0024】第一共用金鑰可以是該P-GW不知道的。可以在該設備處本端地匯出第一共用金鑰和第二共用金鑰，並且不是將其發送給該設備的。第二共用金鑰可以確保使用者面通訊的

至少一些層安全，而不同的金鑰確保控制面通訊安全。

【0025】根據一些態樣，該設備可以獲得基於第一共用金鑰的第三共用金鑰，以確保在該設備和行動性管理實體（MME）之間發送的控制訊息傳遞安全，其中第三共用金鑰由該設備和MME共用，並且P-GW、MME和該存取節點是不同的網路實體。該設備可以獲得基於第三共用金鑰的第四共用金鑰，以確保該設備和該存取節點之間的資料傳輸量以及該設備和MME之間的控制訊息傳遞安全，其中第四共用金鑰由該設備和該存取節點共用。隨後，該設備可以基於第四共用金鑰來確保第一安全的資料傳輸量安全，以產生第二安全的資料傳輸量，其中第一安全的資料傳輸量封裝在第二安全的資料傳輸量之中。隨後，該設備可以替代第一安全的資料傳輸量，經由該存取節點向P-GW發送第二安全的資料傳輸量，其中該P-GW、該MME和該存取節點是不同的網路實體。

【0026】根據一些態樣，第二共用金鑰在使用者面的網際網路協定（IP）層中，保護第二安全的資料傳輸量，而第四共用金鑰在使用者面的封包資料會聚協定（PDCP）層中，保護第二安全的資料傳輸量。根據一些態樣，第四共用金鑰在使用者面的某些層上保護傳輸量的某些傳輸，而第二共用金鑰用於在使用者面的其它層上保護傳輸量的其他傳輸。

【0027】第一共用金鑰可以在該設備和網路實體之間共用。該網路實體可以從歸屬用戶伺服器（HSS）獲得第一共用金鑰。該設備可以獨立於P-GW來獲得第二共用金鑰。獲得第二共用金鑰亦包括：在該設備處，根據第一共用金鑰和封包資料

網路閘道辨識符（GW ID）來匯出第二共用金鑰。

【0028】在本文所描述的態樣中，資料傳輸量與控制訊息傳遞不同。可以在使用者面上發送資料傳輸量，而且可以在控制面上發送控制訊息傳遞，其中使用者面和控制面是不同的傳輸路徑。

【0029】在一些態樣中，確保資料傳輸量安全包括：基於第二共用金鑰，對資料傳輸量進行加密。確保資料傳輸量安全可以包括：包含基於第二共用金鑰的認證簽名。

【0030】根據一些態樣，本文描述的方法亦可以包括：經由該存取節點來從P-GW接收第三安全的資料傳輸量，其中第三安全的資料傳輸量是基於第二共用金鑰來確保安全的。該方法亦可以進一步包括：基於第二共用金鑰對第三安全的資料傳輸量進行解密及/或認證，以產生不安全的資料傳輸量。

【0031】本文描述了用於執行上面所舉例的方法的設備。另外，本文亦描述了其上儲存有一或多個指令的非臨時性機器可讀儲存媒體，其中當該一或多個指令被至少一個處理器執行時，使得該至少一個處理器執行上面所舉例的方法的步驟。

【0032】根據另一個態樣，一種在封包資料網路閘道（P-GW）處操作的方法可以包括：在該P-GW處，從封包資料網路接收資料傳輸量。該P-GW可以從網路實體獲得秘密共用金鑰，以確保該資料傳輸量在該P-GW和設備之間傳輸期間的安全，其中該秘密共用金鑰由該P-GW和該設備共用。隨後，該P-GW可以基於該秘密共用金鑰來確保該資料傳輸量安全，以

產生第一安全的資料傳輸量。隨後，該P-GW可以經由存取節點來向該設備發送第一安全的資料傳輸量，其中該P-GW、該存取節點和該網路實體是不同的網路實體。

【0033】根據一些態樣，該秘密共用金鑰是該存取節點不知道的。可以經由控制面介面，將該秘密共用金鑰從該網路實體提供給該P-GW。根據一些態樣，該秘密共用金鑰確保使用者面通訊的至少一些層安全，而不同的共用金鑰確保控制面通訊安全。例如，該秘密共用金鑰可以在使用者面的網際網路協定（IP）層中，保護該資料傳輸量。該P-GW可以獨立於該設備來獲得該秘密共用金鑰。該秘密共用金鑰可以是P-GW辨識符（GW ID）的函數。獲得該秘密共用金鑰亦可以包括：從位於歸屬用戶伺服器（HSS）和行動性管理實體（MME）之間的該網路實體，獲得該秘密共用金鑰。優選地，該秘密共用金鑰是從處於與該P-GW相同的域中的該網路實體獲得的。亦即，該P-GW與該網路實體處於一個域中。

【0034】在P-GW處操作的該方法亦可以包括：在該P-GW處，經由該存取節點從該設備接收經由該秘密共用金鑰來確保安全的安全的上行鏈路資料傳輸量。該P-GW可以利用該秘密共用金鑰對該安全的上行鏈路資料傳輸量進行解密及/或認證，以獲得上行鏈路資料傳輸量。隨後，該P-GW可以向封包資料網路發送該上行鏈路資料傳輸量。

【0035】本文描述了用於執行上面所舉例的在P-GW處實現的方法的設備。

【0036】一種在網路實體（例如，片段金鑰管理實體）處操

作的方法，可以包括：在該網路實體處，獲得第一共用金鑰。在該網路實體處，亦可以獲得基於第一共用金鑰的第二共用金鑰。第二共用金鑰可以用於確保資料傳輸量在設備和封包資料網路閘道（P-GW）之間傳輸期間的安全。該設備和該P-GW可以共用第二共用金鑰；但是，它們彼此之間獨立地來獲得第二共用金鑰。該方法亦可以包括：向該P-GW發送第二共用金鑰。該方法亦可以進一步包括：在該網路實體處，獲得基於第一共用金鑰的第三共用金鑰，以確保在該設備和行動性管理實體（MME）之間發送的控制訊息傳遞安全。第三共用金鑰由該設備和該MME共用。可以向該MME發送第三共用金鑰。該網路實體、該P-GW和該MME可以是不同的網路實體。

【0037】根據一些態樣，獲得第二共用金鑰可以包括：根據第一共用金鑰和封包資料網路閘道辨識符（GW ID）來匯出第二共用金鑰。

【0038】根據本文所描述的態樣，資料傳輸量與控制訊息傳遞不同。例如，可以在使用者面上發送資料傳輸量，並且可以在控制面上發送控制訊息傳遞，其中使用者面和控制面是不同的傳輸路徑。

【0039】根據一些態樣，該網路實體位於歸屬用戶伺服器（HSS）和該MME之間，並且該網路實體與該HSS和該MME不同。

【0040】本文描述了用於執行上面所舉例的方法的設備。另外，本文亦描述了其上儲存有一或多個指令的非臨時性機器

可讀儲存媒體，其中當該一或多個指令被至少一個處理器執行時，使得該至少一個處理器執行上面所舉例的方法的步驟。

【圖式簡單說明】

【0041】圖1是根據先前技術的第四代（4G）蜂巢網路的元素的視圖。

【0042】圖2是在圖1的4G蜂巢網路的使用者面中實現的各個協定堆疊的方塊圖。

【0043】圖3是在圖1的4G蜂巢網路中實現的金鑰等級。

【0044】圖4根據先前技術，圖示4G（例如，LTE（版本8））蜂巢網路的元素，其中根據控制面和使用者面來對元素進行分組。

【0045】圖5是根據本案內容的態樣的示例性下一代（例如，5G）蜂巢網路的元素的視圖。

【0046】圖6是在圖5的下一代蜂巢網路的使用者面中實現的各個協定堆疊的方塊圖。

【0047】圖7是在圖5的示例性下一代蜂巢網路中實現的金鑰等級。

【0048】圖8根據本案內容的態樣，圖示示例性下一代（例如，5G）蜂巢網路的元素，其中根據控制面和使用者面來對元素進行分組。

【0049】圖9根據本案內容的態樣，圖示與在封包資料網路（PDN）連接建立期間，在控制面中初始地提供共用金鑰（本文稱爲$K_{P\text{-}GW}$金鑰），隨後在使用者面中傳送利用該$K_{P\text{-}GW}$金鑰

進行加密/認證的訊息相關聯的撥叫流的實例。

【0050】圖10A圖示示例性下一代蜂巢網路的元素，其中根據控制面和使用者面來對元素進行分組，其中P-GW處於歸屬網路中並被標識成H-P-GW。

【0051】圖10B圖示示例性下一代蜂巢網路的元素，其中根據控制面和使用者面來對元素進行分組，其中P-GW處於拜訪網路中並被標識成V-P-GW。

【0052】圖11根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0053】圖12根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0054】圖13根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0055】圖14根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0056】圖15根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0057】圖16根據本文所描述的態樣，圖示在設備（例如，晶片組件、客戶端設備）處操作的示例性方法，以保護下一

代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0058】圖17根據本文所描述的態樣，圖示在例如存取節點處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0059】圖18根據本文所描述的態樣，圖示在存取節點（例如，eNodeB）處操作的示例性方法，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0060】圖19根據本文所描述的態樣，圖示在P-GW處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息的安全及/或完整性。

【0061】圖20根據本文所描述的態樣，圖示在至封包資料網路的閘道（例如，P-GW）處操作的示例性方法，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0062】圖21根據本文所描述的態樣，圖示在本文稱爲片段金鑰管理實體（SKME）的網路實體處操作的示例性方法，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0063】圖22根據本文所描述的態樣，圖示在SKME處操作的示例性方法，以匯出保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的金鑰。

【0064】圖23圖示被配置爲執行本文所描述的方法的設備的示例性硬體實現方式的方塊圖。

【0065】圖24根據本文所描述的態樣，圖示在設備（例如，

晶片組件、客戶端設備）處操作的示例性方法，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0066】圖25圖示被配置爲執行本文所描述的方法的封包資料網路閘道（P-GW）的示例性硬體實現方式的方塊圖。

【0067】圖26根據本文所描述的態樣，圖示在P-GW處操作的示例性方法，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0068】圖27圖示被配置爲執行本文所描述的方法的、本文稱爲片段金鑰管理實體（SKME）的網路實體的示例性硬體實現方式的方塊圖。

【0069】圖28根據本文所描述的態樣，圖示在SKME處操作的、結合保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的示例性方法。

【實施方式】

【0070】下面結合附圖闡述的具體實施方式，意欲對各種配置進行描述，而不是意欲表示在這些配置中可以實踐本文所描述的概念的唯一配置。爲了對各種概念提供透徹理解，具體實施方式包括具體的細節。但是，對於本發明所屬領域中具有通常知識者來說將顯而易見的是，可以在不使用這些具體細節的情況下實踐這些概念。在一些例子中，爲了避免對這些概念造成模糊，公知的結構和元素以方塊圖形式示出。

【0071】如本文所使用的，術語「獲得」可以意指本端地匯出或者從另一個實體獲取。如本文所使用的，術語「設備」可以描述晶片組件及/或諸如客戶端設備之類的使用者設備（

例如，行動設備、使用者裝備、使用者設備、終端、行動電話、行動通訊設備、行動計算裝置、數位平板、智慧型電話、可穿戴智慧設備等等其它設備）。如本文所使用的，「基於B來匯出A」的構造以及類似的結構可以用於意指從B直接地或間接地匯出/產生A。如本文所使用的，術語「確保安全」可以意指結合對使用者面資料傳輸量中的封包或訊息進行認證，來加密/解密及/或執行某一動作。

【0072】爲了克服在已知的系統中存在的問題和缺陷，本文提出了減少對於存取節點112的完整性（或安全狀態）的依賴，以便在客戶端設備106和P-GW 120之間實現安全通訊的態樣。

概述

【0073】爲了在下一代蜂巢網路（例如，相對於4G網路）中提供增加的安全性，客戶端設備和至封包資料網路的蜂巢網路閘道（下文稱爲封包資料網路（PDN）閘道（P-GW））得知、獲得及/或匯出第一共用金鑰。客戶端設備經由用於蜂巢網路的存取節點，與P-GW進行通訊。客戶端設備和P-GW獨立地得知、獲得、產生及/或匯出第一共用金鑰。亦即，在兩個實體之間不存在相對於第一共用金鑰的得知、獲得、產生及/或匯出的協商。在兩個實體之間不交換與金鑰有關的資訊。換言之，獨立地得知、獲得、產生及/或匯出意指，兩個實體單獨地得知、獲得、產生及/或匯出相同金鑰的兩個例子，而在它們之間不進行任何互換。第一共用金鑰可以用於對客戶端設備和P-GW之間發送的訊息進行加密及/或認證。由於第

一共用金鑰是存取節點不知道的，因此確保了客戶端設備和P-GW之間經由存取節點發送的訊息的安全，以防止篡改及/或存取節點的不可存取。

【0074】客戶端設備和存取節點可以得知、獲得、產生及/或匯出第二共用金鑰，其中第二共用金鑰與第一共用金鑰不同。第二共用金鑰可以用於對在客戶端設備和存取節點之間發送的空中（over-the-air）訊息進行加密及/或認證。

【0075】舉一個實例，可以首先使用第一共用金鑰，對客戶端設備和P-GW之間經由存取節點發送的第一訊息進行加密及/或認證，隨後將其封裝在第二訊息中，其中第二訊息是利用第二共用金鑰來加密及/或認證的。

4G蜂巢網路使用者面安全

【0076】圖2是在圖1的4G蜂巢網路的使用者面中實現的各個協定堆疊200的方塊圖。將各個協定堆疊200示爲在客戶端設備202、存取節點204、P-GW 206和應用伺服器（APP伺服器）208中實現。根據標準的執行支撐系統（OSS）模型，在客戶端設備202中實現的協定堆疊可以包括網際網路協定層（IP層）210、封包資料會聚協定（PDCP）層212、無線電鏈路控制（RLC）層214、媒體存取控制（MAC）層216和實體（PHY）層218。在存取節點204中實現的協定堆疊可以包括與客戶端設備106中的那些層相對應的層。例如，存取節點204層可以包括PDCP層220、RLC層222、MAC層224和PHY層226。此外，亦包括用於使用者面的通用封包式無線電服務（GPRS）隧道協定（GTP-U）層228、使用者資料包通訊協定（UDP

）層230、網際網路協定層（IP）層232、MAC層234和乙太網路層236，用於與封包資料網路閘道（P-GW）206進行通訊。在P-GW 206中實現的協定堆疊可以包括對應的（GTP-U）層238、使用者資料包通訊協定（UDP）層240、IP層242、MAC層244和乙太網路層246，用於與存取節點204進行通訊。在APP伺服器208中實現的協定堆疊可以包括IP層248。APP伺服器208的IP層248可以用於與P-GW 206的IP層250進行通訊。P-GW 206的IP層250可以與客戶端設備202的IP層210進行通訊。剛剛標識的層是本發明所屬領域中已知的。這些層的詳細解釋是本發明所屬領域中具有通常知識者可獲得的，故爲了簡明起見，本文將不進行描述。

【0077】圖2指示客戶端設備202的PDCP層212和存取節點204的PDCP層220之間的通訊是基於共用金鑰（K_{eNB}金鑰252）來加密/解密的，其中K_{eNB}金鑰252可以用於匯出共用的使用者面加密金鑰K_{UPenc}。換言之，客戶端設備202的PDCP層212和存取節點204的PDCP層220之間的通訊可以基於共用金鑰（K_{eNB}金鑰252）來確保安全。此外，圖2提供了存取節點204的IP層232和P-GW 206的IP層242之間的通訊，是使用網際網路協定安全（IPSEC）254來確保安全的指示。

【0078】參見圖1和圖2，在4G中，若客戶端設備106向封包資料網路122（例如，網際網路）發送使用者面訊息，則客戶端設備106必須首先向存取節點112發送使用者面訊息。爲了保護使用者面訊息，客戶端設備106可以基於K_{eNB}金鑰252來對該訊息進行加密（亦即，使用K_{eNB}金鑰252來匯出K_{UPenc}金

鑰）。一旦進行了加密，則客戶端設備106可以向存取節點112發送該訊息。存取節點112可以基於K_{eNB}金鑰252對該使用者面訊息進行解密（亦即，使用K_{eNB}金鑰252來匯出K_{UPenc}金鑰）。因此，存取節點112可獲得該使用者面訊息的未加密的內容。因此，很大地依賴存取節點112來保護穿過該存取節點112的通訊的安全。如前述，儘管具有安全擔憂，但存取節點112可以被視作爲4G通訊的受信任實體。

【0079】在解密之後，存取節點112可以將該使用者面訊息轉發給P-GW 120。存取節點112可以利用IPSEC 254來確保從存取節點112的IP層向P-GW 120的對應IP層傳送的每一個IP訊息安全。一旦確保了安全，則存取節點112可以根據IPSEC協定，向P-GW 120發送每一個IP訊息。IPSEC協定是本發明所屬領域已知的。IPSEC協定的詳細描述是本發明所屬領域中具有通常知識者可獲得的，故爲了簡明起見，本文將不進行描述。

【0080】圖3是在圖1的4G蜂巢網路中實現的金鑰等級300。本文標識爲K 302金鑰的根金鑰可以儲存在客戶端設備的通用用戶辨識模組（USIM）上，亦可以儲存在核心網路的認證中心（AuC）處。在客戶端設備和核心網路之間的授權通訊期，USIM和AuC中的每一個可以基於K 302金鑰，獨立地匯出完整性金鑰（IK）和密碼金鑰（CK）（本文統一地稱爲IK、CK 304金鑰）。IK、CK 304金鑰可以稱爲片段金鑰。

【0081】在認證和金鑰協商（AKA）程序期間，IK、CK金鑰304可以從AuC發送給HSS。換言之，HSS可以從AuC獲得IK

、CK 304金鑰。客戶端設備已經具有IK、CK 304金鑰（憑藉在客戶端設備處由USIM來匯出的IK、CK金鑰）。

【0082】客戶端設備和HSS中的每一個可以基於IK、CK金鑰304，獨立地匯出存取安全管理實體（ASME）金鑰（K_{ASME}金鑰）306。可以從HSS向MME發送K_{ASME}金鑰306。換言之，MME可以從HSS獲得K_{ASME}金鑰306。客戶端設備已經具有K_{ASME}金鑰306（憑藉在客戶端設備處基於IK、CK 304金鑰來匯出K_{ASME}金鑰306）。MME可以視作爲受信任的金鑰實體。

【0083】客戶端設備和MME中的每一個可以基於K_{ASME}金鑰306，獨立地匯出非存取層加密金鑰（K_{NASenc}金鑰）308和非存取層完整性金鑰（K_{NASint}金鑰）310。K_{NASenc}金鑰308和K_{NASint}金鑰310意欲保護客戶端設備和MME之間的控制面訊息。這種保護防止其他元素對控制面中的訊息進行解密或修改。

【0084】客戶端設備和MME中的每一個亦可以基於K_{ASME}金鑰306，獨立地匯出存取節點金鑰（本文稱爲K_{eNB}金鑰312）。可以從MME向存取節點發送K_{eNB}金鑰312。換言之，存取節點可以從MME獲得K_{eNB}金鑰312。此時，客戶端設備和存取節點中的每一個皆擁有標識爲K_{eNB}金鑰312的金鑰。換言之，客戶端設備和存取節點共用K_{eNB}金鑰312。

【0085】在包括K_{eNB}金鑰312的塊之內，引用下一跳（NH）計數器。MME匯出用於存取節點的第一K_{eNB}金鑰。每當客戶端設備從第一存取節點「向前」運動到第二存取節點，MME就匯出新的K_{eNB}金鑰來替代第一K_{eNB}金鑰。隨後，MME向第二存取節點發送該新的K_{eNB}金鑰，以便保護來自前一存取節

點的連接。因此，NH計數器提供了用於在MME和客戶端設備中匯出中間K_{eNB}金鑰的方式。這稱爲前向安全程序。由於前向安全程序，因此當結合客戶端設備從第一存取節點切換到第二存取節點，第一金鑰改變爲新的金鑰時，第一存取節點不能使用第一K_{eNB}金鑰來對經由第二存取節點發送的訊息進行解密或修改。

【0086】使用基於K_{ASME}金鑰306所匯出的K_{eNB}金鑰312，客戶端設備和存取節點可以獨立地匯出四個不同的金鑰，但是在實踐中，通常匯出三個金鑰。這四個可能的金鑰包括使用者面完整性金鑰（其表示爲K_{UPint}金鑰314）、使用者面加密金鑰（其表示爲K_{UPenc}金鑰316）、控制面（無線電資源控制）完整性金鑰（其表示爲K_{RRCint}金鑰318）和控制面（無線電資源控制）加密金鑰（其表示爲K_{RRCenc}金鑰320）。具有下標「enc」的金鑰用於加密。具有下標「int」的金鑰用於完整性。在4G中，不考慮使用者面完整性；因此，通常不匯出K_{UPint}金鑰314。

【0087】返回到圖2，4G蜂巢網路的使用者面協定堆疊，在客戶端設備202的PDCP層212和存取節點204的PDCP層220之間傳送的訊息可以基於K_{eNB}金鑰252來加密（亦即，使用K_{eNB}金鑰252來匯出K_{UPenc}金鑰）。可以對客戶端設備202的PDCP層212和存取節點204的PDCP層220之間傳送的訊息，使用K_{UPenc}金鑰（類似於圖3的K_{UPenc}金鑰316）來執行加密，而不考慮該訊息的方向。在4G使用者面訊息中，在客戶端設備202和存取節點204之間不對完整性進行控制。

【0088】如圖2中所示，將描述使用者面訊息加密步驟。考慮其中客戶端設備202試圖向APP伺服器208發送訊息的場景。客戶端設備202和APP伺服器208可以使用傳輸控制協定/網際網路協定（TCP/IP）或使用者資料包通訊協定/網際網路協定（UDP/IP）協定進行通訊。爲了在使用者面中發送該訊息，客戶端設備202可以根據該協定堆疊，使用PDCP層212。稱爲第三代合作夥伴計畫（3GPP）的標準制定機構可以定義PDCP層212。PDCP層212可以負責對從客戶端設備202向存取節點204發送的訊息進行加密（例如，加解密）和認證（如，完整性保護）。爲了對該訊息進行加密，客戶端設備202可以使用K_{UPenc}金鑰，其中K_{UPenc}金鑰是客戶端設備202基於K_{eNB}金鑰252匯出的。存取節點204基於K_{eNB}金鑰252的共用複本，獨立地匯出相同的K_{UPenc}金鑰。其是共用金鑰，其原因在於客戶端設備202和存取節點204皆擁有相同的金鑰。該K_{UPenc}金鑰只有在客戶端設備202和存取節點204之間是有價值的。不能夠使用該K_{UPenc}金鑰來對客戶端設備202和任何其他存取節點之間的訊息進行加密或解密。

【0089】客戶端設備202的PDCP層212使用K_{UPenc}金鑰對使用者面訊息進行加密（其中K_{UPenc}金鑰是基於K_{eNB}金鑰252匯出的），並將其發送給低層（RLC層214、MAC層216、PHY層218），使得可以向該訊息增加低層標頭，並使得可以將該訊息發送到存取節點204。在從高層接收到該訊息之後，低層根據3GPP所建立的標準對該訊息進行處理，並將其發送給存取節點204。

【0090】在接收之後，存取節點204的PDCP層220可以使用K_{UPenc}金鑰對該訊息進行解密，其中該K_{UPenc}金鑰是存取節點204基於共用金鑰（K_{eNB}金鑰252）匯出的。隨後，存取節點204可以（根據解密後的資料）決定該訊息所轉發到的P-GW（例如，P-GW 206）的IP位址。隨後，使用IPSEC 254來封裝該訊息。在存取節點204和P-GW 206之間建立IPSEC隧道。隨後，基於IPSEC隧道所建立的互連，存取節點204在增加了額外的標頭之後，對整個IP訊息進行封裝，並將其發送給P-GW 206。IPSEC 254保護存取節點204和P-GW 120之間的連接，所以可以假定其是安全的。一旦P-GW 206接收到經由IPSEC 254來保護的訊息，則其可以對該訊息進行驗證。一旦驗證成功，則P-GW 206可以去除存取節點204所添加的所有標頭，並最終將從客戶端設備202接收的訊息發送給APP伺服器208。

【0091】似乎，將該訊息從客戶端設備保護直到P-GW。但是，從客戶端設備202的角度來看，4G使用者面安全可以在存取節點204處終止。在4G中，客戶端設備202依賴於存取節點204來實現使用者面安全，這是由於客戶端設備202不能夠判斷存取節點204是否具有到P-GW 206的安全連接。存取節點204必須信任：若訊息安全地到達存取節點204，則存取節點204將使該訊息安全地發送到P-GW 206。存取節點204亦必須信任：若訊息沒有成功地到達P-GW 206，則網際網路服務提供者（ISP）將安全地將該訊息從P-GW 206發送到APP伺服器208。因此在4G蜂巢網路中，客戶端設備202可以只關注於對該訊息進行加密，以提供該訊息在客戶端設備202自身和存取節點

204之間的安全，使得例如空中竊聽者不能夠對該訊息進行解密。

【0092】圖4根據先前技術，圖示4G（例如，LTE（版本8））蜂巢網路400的元素，其中根據控制面和使用者面來對元素進行分組。在圖4中，使用隧道或管道的圖形圖示來表示安全的信號路徑。圖4圖示核心網路402的元素。圖4亦圖示存取節點404，存取節點404可以與客戶端設備406進行無線通訊。核心網路402包括HSS 408、MME 410、S-GW 412和P-GW 414。存取節點404包括RRC 416實體（在控制面中發現的實體）、PDCP/RLC實體418和IP實體420（其中PDCP/RLC實體和IP實體在使用者面中發現）。

【0093】因此，如上面所解釋的，4G蜂巢網路中的使用者面安全取決於存取節點404（例如，eNodeB）的正確行爲。由於在4G中，與MME 410相比，存取節點404是較爲不受信任的實體，因此將MME 410視作爲本端信任錨節點或者本端金鑰錨節點。在需要時，MME 410可以向存取節點404傳遞K_{eNB}金鑰。可以基於K_{eNB}金鑰來匯出K_{UPenc}金鑰。

【0094】圖4從視覺上圖示某些匯出的加密金鑰的使用以及IPSEC隧道426的使用。根據圖4的態樣，MME 410是K_{ASME}金鑰的本端信任錨節點或本端金鑰錨節點。MME 410和客戶端設備406之間的管道422描述了利用K_{NASenc}和K_{NASint}金鑰的安全性，來發送MME 410和客戶端設備406之間的控制面訊息。如上面結合圖3所描述的，客戶端設備406和MME 410中的每一個可以基於K_{ASME}金鑰，獨立地匯出非存取層加密K_{NASenc}金

鑰和非存取層完整性K_{NASint}金鑰。存取節點404的PDCP/RLC實體418和客戶端設備406之間的管道424描述了利用K_{UPenc}金鑰的安全性，來發送PDCP/RLC實體418和客戶端設備406之間的使用者面訊息。如上面結合圖3所描述的，客戶端設備406和存取節點404中的每一個可以獨立地匯出K_{UPenc}金鑰（亦即，使用者面加密金鑰）。存取節點404的IP實體420和核心網路402的P-GW 414之間的IPSEC隧道426描述了利用IPSEC的安全性，來發送IP實體420和P-GW 414之間的使用者面訊息。

下一代蜂巢網路使用者面安全

【0095】上面所描述的4G場景舉例說明了4G蜂巢安全架構的有問題的設計原理。使用者面安全或者私密性取決於存取節點的完整性（或安全狀態）的問題，可以在下一代（例如，5G）蜂巢網路中治癒。在本文所體現的下一代蜂巢網路中，可以建立客戶端設備和P-GW之間的直接安全關係，以減少對於存取節點的完整性（或安全狀態）的依賴。如本文所使用的，直接安全關係可以意指可以在無需信任任何中間實體或節點的情況下，提供客戶端設備和P-GW之間的安全連接（例如，用於通訊/訊息/封包的交換）。可以經由使用客戶端設備和P-GW共用的金鑰，來建立這種直接安全關係，而該金鑰不是客戶端設備和P-GW之間的任何協商或互換的結果。換言之，客戶端設備獨立於P-GW來獲得該共用金鑰，同樣，P-GW獨立於客戶端設備來獲得該共用金鑰。

【0096】圖5是根據本案內容的態樣的示例性下一代（例如，5G）蜂巢網路500的元素的視圖。蜂巢網路500可以包括存取

部分（例如，無線存取網路（RAN））和核心部分（例如，核心網路），可以將存取部分描述爲進化型通用陸地無線電存取網路（E-UTRAN）502，本文可以將核心部分稱爲進化型封包核心（EPC）504。E-UTRAN 502和EPC 504一起構成進化型封包系統（EPS）。

【0097】EPS可以與客戶端設備506（例如，行動設備、行動終端、使用者設備（UE）、終端）進行通訊。客戶端設備506可以包括通用用戶辨識模組（USIM）508（其通常稱爲SIM卡）。USIM 508可以是安全地儲存例如國際行動用戶標識（IMSI）號和其相關的金鑰K的積體電路晶片。金鑰K可以是根金鑰。在不偏離本文所描述的任何態樣的情況下，可以以任意數量的方式，將根金鑰K安全地儲存在客戶端設備506處，其包括但不限於安全儲存在USIM 508上。

【0098】將EPS中的通訊劃分爲平面（亦即，使用者面（UP）和控制面（CP））中。在圖5中，一個特定的控制面訊號傳遞路徑經由存取節點512（例如，eNodeB）和行動性管理實體（MME）514之間的虛線510來標識，而一個特定的使用者面資料路徑經由存取節點512和服務閘道（S-GW）518之間的實線516來標識。本發明所屬領域中具有通常知識者知道用於控制面訊號傳遞和使用者面資料的額外的和替代的路徑。圖5的視圖是示例性的，並不意欲是限制性的。

【0099】E-UTRAN 502包括存取節點512，存取節點512包括與客戶端設備506進行無線通訊的硬體。在長期進化型（LTE）網路中，例如，存取節點512可以稱爲進化型節點B（eNodeB

）。舉例而言，單個LTE存取節點可以服務一或多個E-UTRAN 502細胞。

【0100】 EPC 504包括諸如封包資料網路（PDN）閘道（P-GW）520之類的各個網路實體。P-GW 520用作至封包資料網路522（例如，網際網路及/或專用的企業網）的閘道。P-GW 520可以被視作爲至封包資料網路522的通道和網路策略實施的點；而可以將存取節點512視作爲用於客戶端設備506到核心網路（例如，EPC 504）的空中存取的通道，其中經由核心網路來連接封包資料網路522。存取節點512可以與P-GW 520並置在一起，但存取節點512的功能與P-GW 520的功能不同。換言之，即使它們並置在一起，存取節點512和P-GW 520亦是具有單獨功能的單獨實體。

【0101】 EPC 504亦包括諸如歸屬用戶伺服器（HSS）524之類的網路實體。HSS 524儲存每個客戶端設備506的唯一標識。認證中心（AuC）526可以耦合到HSS 524。當客戶端設備506嘗試連接到EPC 504（例如，核心網路）時，AuC 526可以用於對USIM 508進行認證。AuC 526可以儲存與在USIM 508中所儲存的金鑰相同的金鑰。當客戶端設備506加電時，通常可以發生對USIM 508卡的認證。

【0102】 EPC 104亦包括諸如S-GW 518之類的網路實體。S-GW 518執行與傳輸使用者面IP訊息往返客戶端設備506有關的功能。通常，應當理解的是，訊息可以包括一或多個封包。封包和訊息可以具有不同的格式，並經由不同的標頭進行封裝。爲了本文便於引用起見，通篇使用術語訊息。EPC 504

亦包括MME 514。MME 514包含在控制面中，而客戶端設備506、存取節點512、S-GW 518、P-GW 520和HSS 524包含在控制面和使用者面兩者中。MME 514執行與建立、維持和釋放各個實體通道有關的功能。

【0103】EPC 504亦可以包括本文可以稱爲片段金鑰管理實體（SKME）528的網路實體。用於SKME 528的替代名稱亦是可接受的，例如，本端金鑰錨節點、本端信任錨節點、金鑰匯出和維持儲存單元等等。一或多個SKME可以位於給定的域/網路/服務網路中。例如，在本文所描述的態樣中，一個SKME可以稱爲歸屬片段金鑰管理實體（H-SKME）528（當其被視作爲位於客戶端設備的歸屬網路中時）。再舉一個實例，在本文所描述的態樣中，一個SKME可以稱爲拜訪片段金鑰管理實體（V-SKME）530（當其被視作爲位於客戶端設備的拜訪網路中時）。H-SKME 528及/或V-SKME 530可以位於HSS 524和MME 514之間。在一些態樣中，可以將H-SKME 528及/或V-SKME 530描述爲邏輯實體，可以在專門被配置爲執行H-SKME 528及/或V-SKME 530的任務的硬體中實現它們的功能。儘管將V-SKME 530示出爲經由H-SKME 528來串列地連接到HSS 524，但V-SKME 530可以直接與HSS 524進行通訊。在一些態樣中，一個SKME可以執行H-SKME 528和V-SKME 530二者的功能。下一代蜂巢網路的EPC 504亦可以包括拜訪P-GW（其亦稱爲V-P-GW 532）。在如本文所揭示的下一代蜂巢網路中，H-SKME 528及/或V-SKME 530可以用作本端信任錨節點或者本端金鑰錨節點。H-SKME 528和P-GW 520之間的

虛線標識第一控制面訊號傳遞路徑534。V-SKME 530和V-P-GW 532之間的虛線標識第二控制面訊號傳遞路徑536。第一控制面訊號傳遞路徑534及/或第二控制面訊號傳遞路徑536可以用於根據需要，從本端信任錨節點或者本端金鑰錨節點（H-SKME 528、V-SKME 530）向P-GW 520、V-P-GW 532傳遞第一共用金鑰（例如，圖7的$K_{P\text{-}GW}$金鑰724）。

【0104】爲了在下一代蜂巢網路中從客戶端設備506直到P-GW 520提供使用者面安全，在HSS 524和MME 514之間引入了H-SKME 528及/或V-SKME 530。H-SKME 528及/或V-SKME 530可以負責對共用金鑰進行匯出、維持及/或儲存。客戶端設備506和P-GW 520（及/或V-P-GW 532）可以共用該共用金鑰。H-SKME 528可以向其歸屬網路中的P-GW 520提供該共用金鑰。V-SKME 530可以向拜訪網路的V-P-GW 532提供該共用金鑰。可以使用該共用金鑰來保護下一代蜂巢網路中的使用者面資料。該共用金鑰可以稱爲$K_{P\text{-}GW}$金鑰（例如，圖7的$K_{P\text{-}GW}$金鑰724）。客戶端設備和P-GW 520及/或V-P-GW 532獨立地得知、獲得及/或匯出第一共用金鑰。亦即，在客戶端設備506和P-GW 520及/或V-P-GW 532之間不存在相對於第一共用金鑰的得知、獲得及/或匯出的協商。在客戶端設備506和P-GW 520及/或V-P-GW 532之間不交換與金鑰有關的資訊。

【0105】在歸屬網路的情況下，H-SKME 528的功能可能可以在HSS 524中實現。

【0106】根據本文所描述的一些態樣，在下一代蜂巢網路中，可以將本端信任錨節點或者本端金鑰錨節點的角色（由MME

在4G蜂巢網路中扮演的角色）分配給H-SKME 528及/或V-SKME 530。

【0107】圖6是在圖5的下一代蜂巢網路的使用者面中實現的各個協定堆疊600的方塊圖。將各個協定堆疊600示爲在客戶端設備602、存取節點604、封包資料網路閘道（P-GW）606和應用伺服器（APP伺服器）608中實現。根據標準的OSS模型，在客戶端設備602中實現的協定堆疊可以包括網際網路協定層（IP層）610、封包資料會聚協定（PDCP）層612、無線電鏈路控制（RLC）層614、媒體存取控制（MAC）層616和實體（PHY）層618。在存取節點604中實現的協定堆疊可以包括對應的PDCP層620、RLC層622、MAC層624和PHY層626，用於與客戶端設備106進行通訊。此外，亦包括用於使用者面的GPRS隧道協定（GTP-U）層628、使用者資料包通訊協定（UDP）層630、網際網路協定層（IP）層632、MAC層634和乙太網路層636，用於與P-GW 606進行通訊。在P-GW 606中實現的協定堆疊可以包括對應的（GTP-U）層638、使用者資料包通訊協定（UDP）層640、網際網路協定（IP）層642、MAC層644和乙太網路層646，用於與存取節點604進行通訊。在APP伺服器608中實現的協定堆疊可以包括IP層648，用於與P-GW 606的IP層650進行通訊。P-GW 606的IP層650可以與客戶端設備602的IP層610進行通訊。剛剛標識的層是本發明所屬領域中已知的。這些層的詳細解釋是本發明所屬領域中具有通常知識者可獲得的，故爲了簡明起見，本文將不進行描述。

【0108】圖6亦示出在客戶端設備602和P-GW 606中實現的協定堆疊中的新層。亦即，客戶端設備602中的使用者面安全（UP-SEC）層656和P-GW 606中的UP-SEC層658是新的。用於這些層的替代名稱亦是可接受的。UP-SEC層656可以負責使用基於$K_{P\text{-}GW}$金鑰660來匯出的金鑰（例如，使用$K_{P\text{-}GWenc}$、$K_{P\text{-}GWint}$），對客戶端設備602的IP封包（例如，IP訊息）進行加密及/或認證。一旦進行了加密及/或完整性保護，存取節點604就不能夠對該IP訊息進行解密，其只可以將該訊息轉發給P-GW 606。只有P-GW 606可以對該訊息進行解密及/或認證，這是由於基於$K_{P\text{-}GW}$金鑰660來匯出的這些金鑰只由客戶端設備602和P-GW 606共用；它們是存取節點604不可獲得的。相同的情形亦在相反方向成立。與在客戶端設備602中實現的PDCP層612相比，在客戶端設備602中實現的UP-SEC層656更高。與P-GW 606的GTP-U層638相比，P-GW 606的UP-SEC層658更高。儘管存取節點604和P-GW 606之間不需要IPSEC隧道，但除了在UP-SEC層656、658中利用$K_{P\text{-}GW}$金鑰660來保護訊息之外，網路可以可選地實現IPSEC隧道。例如，P-GW 606可以使用IPSEC來驗證接收的訊息是從給定的存取節點604來接收的。但是，對於使用者面安全，不需要依賴於IPSEC。因此，客戶端設備602和P-GW 606可以使用基於共用的$K_{P\text{-}GW}$金鑰660來匯出的共用金鑰（例如，$K_{P\text{-}GWenc}$、$K_{P\text{-}GWint}$），來向使用者面傳輸量中的訊息提供加密（保密）及/或完整性保護。

【0109】在本文所描述的態樣中，存取節點604可以被使得（

或者可以被配置爲）基於是否啓用了在客戶端設備602和P-GW 606之間使用者面安全（UP-SEC）保護的新態樣，來對訊息進行加密及/或認證。可以經由使用該選項來避免管理負擔。更確切地說，若沒有啓用在客戶端設備602和P-GW 606之間UP-SEC保護的新態樣，則存取節點604可以執行與在目前的4G實踐中的相同行爲。若啓用了在客戶端設備602和P-GW 606之間UP-SEC保護的新態樣，則可以基於第一共用金鑰（$K_{P\text{-}GW}$金鑰660）對IP層中的訊息進行加密/解密及/或認證/完整性驗證（其中$K_{P\text{-}GW}$金鑰660可以用於匯出共用金鑰$K_{P\text{-}GWenc}$和$K_{P\text{-}GWint}$）。此外，亦可以可選地基於第二共用金鑰（K_{eNB}金鑰652）對PDCP層中的訊息進行加密/解密及/或認證/完整性驗證（其中K_{eNB}金鑰652可以用於匯出共用金鑰K_{UPenc}和K_{UPint}）。如上所描述的，K_{eNB}金鑰652的匯出是基於K_{ASME}金鑰的，其中該K_{ASME}金鑰是MME已知的。但是，在本文所描述的態樣中，不向MME提供$K_{P\text{-}GW}$金鑰660（亦即，MME不知道$K_{P\text{-}GW}$金鑰660）。事實上，K_{eNB}金鑰652和$K_{P\text{-}GW}$金鑰660不具有相關性（它們是不相關的）。UP-SEC基於使用$K_{P\text{-}GW}$金鑰660、以及客戶端設備和存取節點之間可選的額外使用者面安全基於使用K_{eNB}金鑰652的特徵，可以基於例如根據網路的配置或者根據客戶端設備602、根據承載的配置，來進行啓用/禁用。

【0110】在下一代（例如，5G）蜂巢網路的示例性實踐使用中，未加密的IP訊息可以與目前在4G蜂巢網路中發現的相同。但是，可以在本文所描述的示例性下一代蜂巢網路的態樣中，引入金鑰產生的方法，以及增加客戶端設備602中的

UP-SEC層656和P-GW 606中的UP-SEC層658。客戶端設備602中的UP-SEC層656和P-GW 606中的UP-SEC層658可以負責使用基於K_{P-GW}金鑰660所匯出的共用金鑰（例如，$K_{P-GWenc}$、$K_{P-GWint}$），對客戶端設備602 IP訊息進行加密及/或認證。在本文所舉例說明的下一代蜂巢網路中，一旦基於第一共用金鑰（例如，K_{P-GW}金鑰660）對IP訊息進行了加密及/或完整性保護，則存取節點112就不能對該IP訊息進行解密及/或認證。在本文所舉例說明的下一代蜂巢網路中，優選的是，僅僅P-GW 606可以對使用基於第一共用金鑰（例如，K_{P-GW}金鑰660）的金鑰進行加密及/或完整性保護的訊息進行解密及/或認證。這可以表示相對於4G蜂巢網路的安全性改進，這在下一代蜂巢網路中是可能的，這是由於在下一代蜂巢網路中，客戶端設備602和P-GW 606可以共用基於K_{P-GW}金鑰660的一或多個金鑰（例如，$K_{P-GWenc}$和$K_{P-GWint}$）。基於K_{P-GW}金鑰660，客戶端設備602和P-GW 606可以向使用者面的訊息提供保密性及/或完整性。如上面所解釋的，亦應當注意的是，存取節點604可以可選地用於經由利用第二共用金鑰（例如，K_{eNB}金鑰652），對利用基於第一共用金鑰（K_{P-GW}金鑰660）的共用金鑰來進行加密及/或完整性保護的訊息增加額外的安全。亦即，存取節點604可以利用基於第二共用金鑰（K_{eNB}金鑰652）的金鑰，對利用基於第一共用金鑰（K_{P-GW}金鑰660）的金鑰進行加密及/或完整性保護的訊息進行加密及/或完整性保護。隨後，存取節點112可以向P-GW 606發送該安全的訊息。

【0111】 圖7是在圖5的示例性下一代蜂巢網路中實現的金鑰

等級700。本文標識爲K金鑰702的根金鑰可以儲存在客戶端設備的通用用戶辨識模組（USIM）上，亦可以儲存在核心網路的認證中心（AuC）處。在本文所描述的態樣中，不經由空中來發送K金鑰702。在客戶端設備和核心網路之間的授權通訊期，USIM和AuC中的每一個可以基於K金鑰702（它們中的每一個分別擁有），獨立地匯出完整性金鑰（IK）和密碼金鑰（CK）（本文統一地稱爲IK、CK金鑰704）。IK、CK金鑰704可以稱爲片段金鑰，更具體而言，稱爲授權片段金鑰。

【0112】在認證和金鑰協商（AKA）程序期間，IK、CK金鑰704可以從AuC發送給HSS。在本文所描述的態樣中，不經由空中來發送IK、CK金鑰704。換言之，HSS可以從AuC獲得IK、CK金鑰704。客戶端設備已經具有IK、CK金鑰704（憑藉由客戶端設備處的USIM來匯出IK、CK金鑰）。

【0113】不是由客戶端設備和HSS中的每一個獨立地匯出K_{ASME}金鑰（如在目前的4G蜂巢網路中），客戶端設備和HSS中的每一個可以基於IK、CK金鑰704，獨立地匯出本文稱爲K_{SKME}金鑰706的新金鑰，其中SKME可以代表片段金鑰管理實體。不從HSS向MME發送K_{SKME}金鑰706。相反，可以從HSS向SKME（例如，圖5的H-SKME 528）發送K_{SKME}金鑰706。換言之，SKME可以從HSS獲得K_{SKME}金鑰706。在本文所描述的態樣中，不經由空中來發送K_{SKME}金鑰706。客戶端設備已經具有K_{SKME}金鑰706（憑藉在客戶端設備處基於IK、CK金鑰704來匯出K_{SKME}金鑰706）。

【0114】客戶端設備和SKME中的每一個可以基於K_{SKME}金鑰

706，獨立地匯出K_{ASME}金鑰708。可以從SKME向MME發送K_{ASME}金鑰708。換言之，MME可以從SKME獲得該K_{ASME}金鑰708。在本文所描述的態樣中，不經由空中來發送K_{ASME}金鑰708。應當注意的是，剛剛所描述的SKME是本端SKME，而不管該客戶端設備是連接到歸屬網路還是連接到拜訪網路。亦應當注意的是，K_{ASME}金鑰708可以類似於4G中的K_{ASME}金鑰；但是，在本文所描述的態樣中，K_{ASME}金鑰708的匯出是基於K_{SKME}金鑰706的，而不是基於IK、CK金鑰704的。客戶端設備已經具有K_{ASME}金鑰708（憑藉在客戶端設備處基於K_{SKME}金鑰706來匯出K_{ASME}金鑰708）。

【0115】與（如圖3中所舉例說明的）4G金鑰等級中的相比，在本文所描述的態樣中引入SKME，提供了HSS和MME之間的額外的金鑰等級層。

【0116】客戶端設備和MME中的每一個可以基於K_{ASME}金鑰708，獨立地匯出非存取層加密金鑰（K_{NASenc}金鑰710）和非存取層完整性金鑰（K_{NASint}金鑰712）。K_{NASenc}金鑰710和K_{NASint}金鑰712意欲保護客戶端設備和MME之間的控制面訊息。這種保護阻止其他元素對控制面中的訊息進行解密或修改。

【0117】客戶端設備和MME中的每一個亦可以基於K_{ASME}金鑰708，獨立地匯出存取節點金鑰（本文稱爲K_{eNB}金鑰714）。可以從MME向存取節點發送K_{eNB}金鑰714。換言之，存取節點可以從MME獲得該K_{eNB}金鑰714。客戶端設備已經具有K_{eNB}金鑰714（憑藉在客戶端設備處基於K_{ASME}金鑰708來匯出K_{eNB}金鑰714）。在本文所描述的態樣中，不經由空中來發送K_{eNB}

金鑰714。

【0118】此時，客戶端設備和存取節點中的每一個皆擁有標識爲K_{eNB}金鑰714的金鑰。換言之，客戶端設備和存取節點共用K_{eNB}金鑰714。

【0119】在包括K_{eNB}金鑰714的塊之內，引用下一跳（NH）計數器。上面描述了NH計數器的功能，故爲了精簡起見，這裡不進行重複。

【0120】使用K_{eNB}金鑰714，客戶端設備和存取節點可以獨立地匯出四個不同的金鑰。這四個可能的金鑰包括使用者面完整性金鑰（其表示爲K_{UPint}金鑰716）、用戶面加密金鑰（其表示爲K_{UPenc}金鑰718）、控制面完整性金鑰（其表示爲K_{RRCint}金鑰720）和控制面加密金鑰（其表示爲K_{RRCenc}金鑰722）。具有下標「enc」的金鑰用於加密。具有下標「int」的金鑰用於完整性。針對於客戶端設備和存取節點之間經由空中傳送的訊息，K_{UPint}金鑰716和K_{UPenc}金鑰718分別用於使用者面資料的完整性保護和加密。它們可以用於在客戶端設備和存取節點之間對PDCP層中的訊息進行加密/完整性保護。K_{RRCint}金鑰720和K_{RRCenc}金鑰722分別用於無線電資源控制（RRC）資料的完整性保護和加密。

【0121】另外，可以基於K_{SKME}金鑰706來匯出另一個金鑰。該額外的金鑰可以稱爲$K_{P\text{-}GW}$金鑰724，其示出在圖7的右邊。與4G蜂巢網路的特徵相比，$K_{P\text{-}GW}$金鑰724和K_{SKME}金鑰706可以是下一代蜂巢網路中的新特徵。客戶端設備和SKME中的每一個可以基於K_{SKME}金鑰706，獨立地匯出$K_{P\text{-}GW}$金鑰724。

SKME可以向P-GW提供該K_{P-GW}金鑰724。在本文所描述的態樣中，不經由空中來發送K_{P-GW}金鑰724。K_{P-GW}金鑰724是共用金鑰，其原因在於客戶端設備和P-GW兩者擁有相同的金鑰。換言之，該金鑰是共用的是因爲這兩個實體擁有它們自己獨立匯出或者獲得的該金鑰的複本，而不是因爲一個實體將其金鑰的複本分發給另一個實體或者與另一個實體協商該金鑰的匯出或產生。K_{P-GW}金鑰724的共用並不需要在客戶端設備和P-GW之間的任何訊號傳遞、協商或者互動。應當注意的是，若客戶端設備經由拜訪域中的P-GW（例如，V-P-GW）來連接到封包資料網路（例如，網際網路），則由拜訪SKME（V-SKME）提供該K_{P-GW}金鑰724。若客戶端設備經由歸屬P-GW（例如，H-P-GW）來連接到封包資料網路，則應當由歸屬SKME（H-SKME）來提供該K_{P-GW}。至於是使用H-P-GW（亦即，歸屬域/歸屬網路P-GW）還是使用V-P-GW（亦即，拜訪域/拜訪網路P-GW），可以基於例如客戶端設備的用戶資訊（例如，來自於用戶簡檔）及/或歸屬域的服務策略及/或某一其他網路存取策略，由網路服務供應商進行配置。

【0122】因此，可以在客戶端設備和P-GW之間共用該K_{P-GW}金鑰724。客戶端設備和P-GW可以基於K_{P-GW}金鑰724，來獨立地匯出$K_{P-GWint}$金鑰726（完整性金鑰）和$K_{P-GWenc}$金鑰728（加密金鑰）。可以使用完整性金鑰（$K_{P-GWint}$金鑰726）來產生訊息認證碼。加密金鑰（$K_{P-GWenc}$金鑰728）可以用於加密。

【0123】從網路角度來看，存取節點可以是層2（L2）連接點（亦即，其支援MAC/PHY層），而P-GW可以是層3（L3）連

接點（亦即，IP層）。這兩個不需要並置在一起，但L2連接點可以改變，而保持L3連接點不變。

【0124】可以使用K_{eNB}金鑰714（在本文的一些態樣中，其可以稱爲第二共用金鑰）來保護使用者面層2空中訊息。使用者面層2空中訊息可以位於封包資料會聚協定（PDCP）層。可以使用$K_{P\text{-}GW}$金鑰724（在本文的一些態樣中，其可以稱爲第一共用金鑰）來保護使用者面層3訊息。使用者面層3訊息可以位於網際網路協定層（IP層）（例如，圖6的IP層610、650）或者使用者面安全（UP-SEC層）（例如，圖6的656、658）中。

【0125】在一些態樣中，$K_{P\text{-}GW}$金鑰724可以是例如K_{SKME}金鑰706和特定閘道的辨識符（GW ID）的函數（例如，$K_{P\text{-}GW}=F(K_{SKME}, \text{GW ID})$）。MME在通信期建立期間，向客戶端設備通知該GW ID。函數F可以是金鑰匯出函數。

【0126】圖8根據本案內容的態樣，圖示示例性下一代（例如，5G）蜂巢網路800的元素，其中根據控制面和使用者面來對元素進行分組。在圖8中，使用隧道或管道822、824、826的圖形描述來表示安全的信號路徑。圖8圖示核心網路802的元素。圖8亦圖示存取節點804，存取節點804可以與客戶端設備806進行無線通訊。核心網路802包括HSS 808、SKME 809、MME 810、S-GW 812和P-GW 814。存取節點804包括RRC 816實體（在控制面中發現的實體）、PDCP/RLC實體818和IP實體820（其中PDCP/RLC和IP實體在使用者面中發現）。圖8與歸屬網路連接場景中的客戶端設備有關。

【0127】圖8在視覺上圖示某些匯出的加密金鑰的使用。根據圖8的態樣，SKME 809是用於片段金鑰管理實體金鑰（K_{SKME}金鑰811）的本端信任錨節點或本端金鑰錨節點。MME 810是用於K_{ASME}金鑰813的本端信任錨節點或本端金鑰錨節點。

【0128】MME 810和客戶端設備806之間的管道822描述了利用K_{NASenc}和K_{NASint}加密金鑰的安全性，來發送MME 810和客戶端設備806之間的控制面訊息。如上面結合圖7所描述的，客戶端設備806和MME 810中的每一個可以基於K_{ASME}金鑰813，獨立地匯出非存取層加密K_{NASenc}金鑰和非存取層完整性K_{NASint}金鑰。具體而言，HSS 808向SKME 809發送K_{SKME}金鑰811，SKME 809基於K_{SKME}金鑰811來匯出K_{ASME}金鑰813並向MME 810發送該K_{ASME}金鑰813，MME 810基於該K_{ASME}金鑰813來匯出K_{NASenc}和K_{NASint}加密金鑰（參見管道822）。

【0129】客戶端設備806和P-GW 814之間的管道824描述了利用$K_{P\text{-}GW}$加密金鑰的安全性，來發送客戶端設備406和P-GW 814之間的使用者面訊息。如上面結合圖7所描述的，客戶端設備806和SKME 809中的每一個可以基於K_{SKME}金鑰811，獨立地匯出$K_{P\text{-}GW}$金鑰。SKME可以向P-GW 814提供$K_{P\text{-}GW}$金鑰。具體而言，HSS 808向SKME 809發送K_{SKME}金鑰811，SKME 809基於K_{SKME}金鑰811來匯出$K_{P\text{-}GW}$金鑰並向P-GW 814發送該$K_{P\text{-}GW}$金鑰。利用第一共用金鑰（$K_{P\text{-}GW}$金鑰）的安全性，來發送客戶端設備806和P-GW 814之間的訊息（參見管道824）。

【0130】圍繞客戶端設備806和存取節點804的PDCP/RLC實體818之間的管道824的管道826描述了第二共用金鑰（K_{eNB}金

鑰），其可以可選地用於對基於$K_{P\text{-}GW}$金鑰已經進行加密及/或認證的訊息進行加密及/或認證。可選的第二加密及/或認證可用於該訊息（當其在存取節點804和客戶端設備806之間進行發送時），無論是在上行鏈路方向還是下行鏈路方向。

【0131】如上面所指示的，SKME 809可以負責匯出稱爲$K_{P\text{-}GW}$金鑰的金鑰。客戶端設備806可能可以基於在自己和AuC之間共用的根金鑰（K）來匯出每一個金鑰，因此其亦可以匯出$K_{P\text{-}GW}$；但是，P-GW 814不能夠匯出用於客戶端設備806的資料連接的$K_{P\text{-}GW}$金鑰。因此，SKME 809可以基於K_{SKME}金鑰811來匯出$K_{P\text{-}GW}$金鑰，並經由例如控制面信號路徑828來向P-GW 814發送該$K_{P\text{-}GW}$金鑰。因此，客戶端設備806和P-GW 814共用金鑰（$K_{P\text{-}GW}$金鑰）。將理解的是，當兩個實體共用金鑰時，則它們可以確保連接安全（無論經由什麼方式）。

【0132】與4G網路中的K_{ASME}金鑰不同，不向MME 810提供$K_{P\text{-}GW}$金鑰。由於客戶端設備806可能在切換期間重定位到不同的MME，所以不向MME 810提供該$K_{P\text{-}GW}$金鑰。在該情況下，需要將$K_{P\text{-}GW}$金鑰從第一MME 810傳送到第二MME（未圖示）。但是，在下一代蜂巢網路中，可以對安全架構進行設計，以將MME 810視作爲不太受信任的實體。

【0133】可以期望的是，與目前使用4G蜂巢網路的相比，越來越多的行動設備將使用下一代蜂巢網路。根據一種估計，行動設備的數量在十年內將增至一百倍。考慮到這種較大數量的客戶端設備，MME的數量可能顯著地增加。今天，在4G網路中，將MME視作爲受信任實體。如今，一個全國性的大

型電話公司可能只需要四個MME來覆蓋它們整個的網路。由於該數量較小，因此可以針對每一個MME來建立較強的安全。例如，今天的MME可以安置在具有有限的存取的安全設施之內。但是，若MME的數量增加到數百個，則維持相同水平的安全級別將很有可能是困難的。可以預料的是，一旦下一代（5G）蜂巢網路變得廣泛使用，則MME的數量將增加。另外，應當理解的是，在「可重新定位的」MME上進行工作。這些類型的MME可以接近存取節點佈置，以支援快速的切換。因此，這可以意指可重新定位的MME可以位於公共區域中，這將增加它們的易受攻擊性。由於這些和其他原因，可以期望將MME 810視作爲不太受信任的實體。這可以是引入SKME 809的另一個原因，其中SKME 809可以用於金鑰匯出和金鑰管理（例如，維持、儲存）。應當注意的是，金鑰匯出功能可以包括長度X的散列訊息認證碼（HMAC）（HMAC-X），其中X是金鑰長度。

【0134】因此，$K_{P\text{-}GW}$可以由SKME 809來匯出，並將其提供給P-GW 814；因此，客戶端設備806可以基於該共用金鑰（$K_{P\text{-}GW}$）而與P-GW 814具有直接安全關係。這可以導致使用者面信任錨定在P-GW 814（而不是如4G中的存取節點804）。換言之，爲了保護使用者面資料，不需要或者亦不要求客戶端設備806信任自己和P-GW 814之間的任何實體/元素。客戶端設備806不需要信任存取節點804或者位於其和P-GW 814之間的路徑上的任何其他設備或路由器，如同今天在4G中必須做的一樣。

【0135】然而，在一些態樣中，除了基於第一共用金鑰（由客戶端設備806和P-GW 814共用的K_{P-GW}金鑰）對使用者面訊息進行加密及/或認證之外，客戶端設備806亦可以利用使用由自己和下一代（例如，5G）蜂巢網路的其他元素或實體共用的其他金鑰的額外的加密及/或認證。在這些方式中的一或多個中，與4G相比，本文所描述的態樣可以在5G中提供更佳的使用者面安全。可以至少經由共用第一共用金鑰、K_{P-GW}金鑰來實現提高的使用者面安全，使得下一代蜂巢網路可以向傳遞往返客戶端設備806和P-GW 814的訊息提供保密和完整性保護。

【0136】4G和下一代蜂巢網路之間的另一個差異可以是：在4G網路中，基於K_{eNB}金鑰來匯出K_{UPenc}金鑰。使用K_{UPenc}金鑰來對客戶端設備和存取節點之間的空中傳輸量進行加密。這意指空中傳輸量是沒有完整性保護的。完整性保護的這種缺失可能是由於4G規範的設計時代期間的頻寬的缺乏。可以設計下一代（例如，5G）蜂巢網路來克服4G蜂巢網路的這些和其他缺陷，並且與4G相比，其通常提供更佳的安全。這可以使得能爲使用者面訊息提供完整性訊息（其在4G中沒有提供）。因此，可以在下一代蜂巢網路中使用有用的特徵，例如，爲使用者面傳輸量提供完整性保護的特徵。以同樣的方式，該完整性保護可以是可選的，例如，加密在一些國家是可選的。在一些態樣中，客戶端設備806和P-GW 814可以關於下面進行協商：它們是否應當對在它們之間傳遞的訊息進行加密、爲在它們之間傳遞的訊息提供完整性保護或者二者。

完整性保護

【0137】為了保密起見，可以對訊息進行加密。若接收方具有用於對該訊息進行加密的金鑰，則接收方可以對該訊息進行解密。若接收方不具有該金鑰，則不能對該訊息進行解密，並維持該訊息保密性。但是，在一些場景中，位於中間位置的攻擊者可能只是改變加密的訊息中的一些位元。位於中間位置的攻擊者可能不知道該訊息的任何內容，但卻可能能夠擷取加密的訊息，對一或多個位元進行改變，並向其目的接收者發送該訊息。現在，接收方對該訊息進行解密，但卻不知道這些位元中的一些已經被改變；接收方信任該訊息。為了確保該訊息安全，除了密碼（其用於對訊息進行加密）之外，亦可以對訊息進行保護，使得接收方可以判斷該訊息在傳輸期間是否被修改過。

【0138】為了完成這種保護，可以計算/產生/匯出/獲得訊息認證碼，並在向接收方發送該訊息之前，將其添加到該訊息的結尾。訊息認證碼可以用於提供關於訊息的完整性和真實性保證。完整性保證偵測意外的和故意的訊息改變（例如，訊息的完整性），而真實性保證確認該訊息的來源（例如，訊息建立者的身份驗證）。訊息認證碼的計算/產生/匯出/獲得可以涉及：利用完整性保護金鑰（例如，$K_{P\text{-}GWint}$）來對訊息進行加密。如本文所描述的，$K_{P\text{-}GWint}$可以由客戶端設備和P-GW來獨立地匯出。可以基於$K_{P\text{-}GW}$金鑰來匯出$K_{P\text{-}GWint}$。$K_{P\text{-}GWint}$可以由客戶端設備基於在該客戶端設備處匯出的$K_{P\text{-}GW}$金鑰來本端地匯出。$K_{P\text{-}GWint}$可以由P-GW基於該P-GW從

SKME獲得的K_{P-GW}金鑰來本端地匯出。因此，客戶端設備和P-GW兩者可以共用該$K_{P-GWint}$金鑰。接收方（例如，客戶端設備或P-GW）可以驗證該訊息認證碼，這是由於接收方具有發送方使用的完整性保護金鑰（例如，客戶端設備和P-GW兩者皆具有$K_{P-GWint}$）。因此，接收方可以從所接收的訊息中計算/產生/匯出/獲得訊息認證碼，並將其與同該訊息一起接收的訊息認證碼進行比較。若接收方的訊息認證碼與發送方的訊息認證碼相匹配，則可以驗證完整性和真實性。應當注意的是，可以使用完整性演算法來執行訊息認證。完整性演算法的實例係包括：基於密碼的訊息認證碼（CMAC）、密碼塊連結訊息認證碼（CBC-MAC）、鍵控散列訊息認證碼（HMAC）、伽羅瓦訊息認證碼（GMAC）、以及3GPP中的進化型封包系統完整性演算法1、2或3（EIA1/EIA2/EIA3）。

【0139】若在存取節點處可以驗證訊息的完整性，則存取節點不需要向P-GW發送缺少完整性的訊息。若在P-GW處可以對該訊息的完整性進行驗證，則P-GW不需要向封包資料網路發送缺少完整性的訊息。這可以減少否則可能在發送損壞的訊息時使用的資源的量。因此，相對於只保護使用者面中的保密性的4G蜂巢網路，在本文所揭示的下一代蜂巢網路的某些態樣中，可以實現保護在使用者面中的保密性和完整性兩者的利益。

控制面/使用者面撥叫流

【0140】圖9根據本案內容的態樣，圖示與在封包資料網路（PDN）連接建立期間，在控制面中初始地提供共用金鑰（本

文稱爲K_{P-GW}金鑰），隨後在使用者面中傳送基於該K_{P-GW}金鑰進行加密/認證的訊息相關聯的撥叫流900的實例。圖9基於3GPP TS 23.401（圖5.10.2-1）。但是，與3GPP TS 23.401（圖5.10.2-1）中所示出的相比，增加了標識爲UP金鑰請求918和UP金鑰回應920的新撥叫。

【0141】圖9描述了設備902（例如，晶片組件、客戶端設備）、存取節點904（例如，eNodeB、eNB）、MME 906、P-GW 908和片段金鑰管理實體（SKME）（910）。該設備可以向MME發送912PDN連接請求。MME可以向P-GW發送914建立通信期請求。P-GW可以與策略控制和收費規則功能單元（PCRF）進行互動916。例如，P-GW可以分配IP位址和準備承載。爲了精簡起見，省略了在與PCRF互動程序中涉及的步驟的詳細解釋。P-GW可以向SKME發送918使用者面（UP）金鑰請求（例如，若P-GW不具有用於設備902的K_{P-GW}的話）。例如，UP金鑰請求可以用於獲得諸如圖7的K_{P-GW}金鑰724之類的金鑰。隨後，SKME可以向P-GW發送920 UP金鑰回應。該UP金鑰回應可以包括共用金鑰（K_{P-GW}）。用此方式，P-GW可以從SKME獲得該共用的K_{P-GW}金鑰。

【0142】接著，P-GW可以向MME發送922建立通信期回應。MME可以向存取節點發送924承載建立請求/PDN連接接受。隨後，存取節點可以向設備發送926 RRC連接重新配置請求。該設備可以向存取節點發送928 RRC連接重新配置完成。存取節點可以向MME發送930承載建立回應。設備可以向存取節點發送932直接傳輸。存取節點可以向MME發送934 PDN連接完

成。本發明所屬領域中具有通常知識者將理解，元件符號912-916和922-934所表示的撥叫。爲了精簡起見，省略了這些撥叫的詳細解釋。

【0143】相對於在3GPP TS 23.401（圖5.10.2-1）中所示出的，增加了標識爲UP金鑰請求918和UP金鑰回應920的新撥叫。根據本文所闡述的本案內容的態樣，進行去往和來自SKME的新撥叫（UP金鑰請求918和UP金鑰回應920）。

【0144】若P-GW不具有針對給定設備的共用$K_{P\text{-}GW}$金鑰，則其可以從SKME請求該共用金鑰。可以經由利用UP金鑰請求918來進行該請求。隨後，SKME可以向P-GW發送$K_{P\text{-}GW}$金鑰。可以使用UP金鑰回應920，來向P-GW提供該$K_{P\text{-}GW}$金鑰。

【0145】在設備匯出其$K_{P\text{-}GW}$金鑰的複本之後，設備可以經由P-GW，在使用者面中向網路發送936第一訊息。可以基於共用的$K_{P\text{-}GW}$金鑰，對第一訊息進行加密及/或認證。另外，設備可以經由P-GW，從網路接收938第二訊息，其中第二訊息可以是基於共用的$K_{P\text{-}GW}$金鑰來加密及/或認證的。由於設備已經具有了其共用的$K_{P\text{-}GW}$金鑰的複本，因此該設備可以對所接收的第二訊息進行解密及/或認證。

【0146】在一些態樣中，用於保護使用者面訊息的方法可以包括：在客戶端設備處，匯出用於對訊息進行加解密及/或認證的第一共用金鑰（$K_{P\text{-}GW}$），其中第一共用金鑰由客戶端設備和P-GW（亦即，至封包資料網路的閘道）共用。可以利用第一共用金鑰對第一訊息進行加密或者認證，以產生第一加密及/或認證的訊息。可以經由空中，從客戶端設備向存取節

點發送第一加密及/或認證的訊息。在另外的態樣中，利用第一共用金鑰對第一訊息進行加密及/或認證，可以另外包括：在客戶端設備處，匯出用於對訊息進行加解密及/或認證的第二共用金鑰，其中客戶端設備和存取節點共用第二共用金鑰。第二共用金鑰與第一共用金鑰不同。它們是不相關的。該方法亦可以進一步包括：利用第二共用金鑰對第一加密及/或認證的第一訊息進行加密及/或認證，以產生第二加密及/或認證的訊息。可以經由空中，從客戶端設備向存取節點發送第二加密及/或認證的訊息。

拜訪網路

【0147】圖10A圖示示例性下一代蜂巢網路1000的元素，其中根據控制面和使用者面來對元素進行分組，其中P-GW處於歸屬網路中，並被標識爲H-P-GW 1010。在圖10A中，客戶端設備1002連接到拜訪網路1015中的MME 1018，但在客戶端設備1002和歸屬網路的H-P-GW 1010之間進行使用者面中的資料連接。歸屬網路中的H-SKME 1012和H-P-GW 1010之間的虛線表示控制面介面1034。控制面介面1034可以用於在H-P-GW 1010和H-SKME 1012之間或者在V-P-GW和V-SKME之間，傳輸使用者面（UP）金鑰請求（例如，圖9的918）和UP金鑰回應（其包括K_{P-GW}）（例如，圖9的920）。

【0148】圖10A圖示歸屬網路1014中的HSS 1008、H-P-GW 1010和歸屬SKME（H-SKME）1012。圖10A亦圖示全部位於拜訪網路1015中的拜訪SKME（V-SKME）1016、MME 1018和S-GW 1020。客戶端設備1002可以經由存取節點1022，具有

與拜訪網路1015的無線通訊。

【0149】在圖10A中，客戶端設備1002可以連接到拜訪網路1015的MME 1018，以及連接到與拜訪網路1015相關聯的存取節點1022。但是，客戶端設備1002可以具有從H-P-GW 1010分配的其自己的IP位址。因此，可以在拜訪網路1015中的客戶端設備1002和其歸屬網路1014中的H-P-GW 1010之間，進行資料連接。當H-P-GW 1010具有要向客戶端設備1002發送的訊息時，H-P-GW 1010可以向拜訪網路1015中的S-GW 1020發送該訊息，並且拜訪網路1015中的S-GW 1020可以向客戶端設備1002發送該訊息。

【0150】根據一個態樣，當P-GW（H-P-GW 1010）處於歸屬網路1014中時，儘管客戶端設備1002處於拜訪網路1015中，但可以基於從歸屬網路1014獲得的K_{SKME}金鑰1011來匯出K_{P-GW}金鑰。換言之，歸屬網路1014的HSS 1008將匯出K_{SKME}金鑰1011，並向歸屬網路1014的H-SKME 1012提供該K_{SKME}金鑰1011。隨後，H-SKME 1012可以基於K_{SKME}金鑰1011來匯出K_{P-GW}金鑰。隨後，H-SKME 1012可以使用控制面介面1034，向H-P-GW 1010提供該K_{P-GW}金鑰。用此方式，可以對使用者面訊息進行加密及/或認證，用於在拜訪網路1015中的客戶端設備1002和歸屬網路1014中的H-P-GW 1010之間進行交換。同時，歸屬網路1014的HSS 1008可以匯出K_{SKME}'金鑰1013，並向拜訪網路1015的V-SKME 1016提供該K_{SKME}'金鑰1013。可以經由H-SKME 1012，將K_{SKME}'金鑰1013從HSS 1008提供給V-SKME 1016（如圖10A中所示），或者直接將其提供給

V-SKME 1016（經由圖10B中未圖示的HSS 1008和V-SKME 1016之間的直接通訊）。K_{SKME}'金鑰1013與K_{SKME}金鑰1011不同（例如，不相關，無關）。用此方式，每一個片段金鑰管理實體金鑰（例如，K_{SKME}金鑰1011和K_{SKME}'金鑰1013）被限定到其自己的網路，或者換言之，限定到其自己的域中。將K_{SKME}金鑰1011限定到歸屬網路1014，並將K_{SKME}'金鑰1013限定到拜訪網路1015。儘管限定到不同的網路，但它們均結合客戶端設備1002來使用。例如，在圖10A的場景中，V-SKME 1016基於K_{SKME}'金鑰1013來匯出K_{ASME}金鑰1019，並將該K_{ASME}金鑰1019提供給拜訪網路1015中的MME 1018。在歸屬網路1014和拜訪網路1015之間使用不相關的片段金鑰管理實體金鑰（例如，K_{SKME}金鑰1011和K_{SKME}'金鑰1013），確保拜訪網路1015將不能夠匯出歸屬網路1014所使用的$K_{P\text{-}GW}$（亦即，不能夠匯出由H-SKME 1012所匯出、並經由控制面介面1034來提供給H-P-GW 1010的$K_{P\text{-}GW}$金鑰）。

【0151】圖10B圖示示例性下一代蜂巢網路1004的元素，其中根據控制面和使用者面來對元素進行分組，其中P-GW處於拜訪網路1017中，並被標識爲V-P-GW 1024。在圖10B中，客戶端設備1006連接到拜訪網路1017中的MME 1028。在客戶端設備1006和拜訪網路1017的V-P-GW 1024之間進行使用者面中的資料連接。拜訪網路1017中的V-SKME 1026和V-P-GW 1024之間的虛線表示控制面介面1036。控制面介面1036可以用於在V-P-GW 1024和V-SKME 1026之間，傳輸使用者面（UP）金鑰請求（例如，圖9的918）和UP金鑰回應（其包括$K_{P\text{-}GW}$）

（例如，圖9的920）。

【0152】圖10B圖示圖10A的歸屬網路1014的相同的HSS 1008。此外，圖10B亦圖示全部處於拜訪網路1017中的拜訪P-GW（V-P-GW 1024）、拜訪SKME（V-SKME 1026）、MME 1028和S-GW 1030。客戶端設備1006可以經由存取節點1032，具有與拜訪網路1017的無線通訊。

【0153】如圖10B中所示，當客戶端設備1006處於拜訪網路1017中時，可能需要本端SKME（例如，V-SKME 1026）來啓用客戶端設備1006和本端P-GW（例如，V-P-GW 1024）之間的直接安全關係。V-SKME 1026可以匯出$K_{P\text{-}GW}$，並將該$K_{P\text{-}GW}$提供給V-P-GW 1024。該提供可以是經由控制面介面1036的。經由遵循該程序，拜訪網路1017中的V-SKME 1026不需要配置歸屬網路1014中的H-P-GW 1010。這可以是有益的，這是由於拜訪網路1017的V-SKME 1026處於與H-P-GW 1010的域不同的域中（拜訪網路1017的域）。來自拜訪域的SKME（V-SKME 1026）（很可能的情況是）不具有配置另一個域的P-GW（H-P-GW 1010）的特權。這可以是建立歸屬SKME（H-SKME 1012）和拜訪SKME（V-SKME 1016、1026）的另一個有益原因；其每一個處於具有對應的P-GW的域，並可以在相同的域中向對應的P-GW提供。

【0154】根據一個態樣，當V-P-GW 1024處於拜訪網路1017中時，儘管客戶端設備1006亦處於拜訪網路1017中，但可以基於從拜訪網路1017獲得的K_{SKME}金鑰1027來匯出$K_{P\text{-}GW}$金鑰。換言之，歸屬網路1014的HSS 1008可以匯出K_{SKME}金鑰1027

，並向拜訪網路1017的V-SKME 1026提供該K_{SKME}金鑰1027（例如，在圖10B的場景中，HSS 1008可以直接與V-SKME 1026進行通訊）。隨後，V-SKME 1026可以基於K_{SKME}金鑰1027來匯出$K_{P\text{-}GW}$金鑰。隨後，V-SKME 1026可以經由控制面介面1036，向V-P-GW 1024提供該$K_{P\text{-}GW}$。用此方式，可以對使用者面訊息進行加密及/或認證，用於在拜訪網路1017中的客戶端設備1006和拜訪網路1017中的V-P-GW 1024之間進行交換。

【0155】總之，當使用H-P-GW 1010來錨定客戶端設備1002的使用者面傳輸量時，使用H-SKME 1012來向H-P-GW 1010提供$K_{P\text{-}GW}$金鑰（經由控制面介面1034）。當使用V-P-GW 1024來錨定客戶端設備1006的使用者面傳輸量時，使用V-SKME 1026來向V-P-GW 1024提供$K_{P\text{-}GW}$金鑰（經由控制面介面1036）。歸屬域和拜訪域的$K_{P\text{-}GW}$金鑰是不同的金鑰，它們是不相關的。

【0156】在建立通信期請求期間，可以發生金鑰傳送（例如，$K_{P\text{-}GW}$的傳送）。例如，在圖10B中，MME 1028可以在客戶端設備1006連接到拜訪網路1017期間，發送用於建立承載的建立通信期請求。該建立通信期請求可以轉到V-P-GW 1024（例如，拜訪網路1017的P-GW）。若V-P-GW 1024不具有用於客戶端設備1006的$K_{P\text{-}GW}$金鑰，則其可以發送請求以從本端SKME（例如，拜訪網路1017中的SKME，V-SKME 1026）獲得$K_{P\text{-}GW}$。在這個意義上，在客戶端設備1006是使用歸屬網路來進行資料連接（此時，H-P-GW 1010從H-SKME 1012獲得$K_{P\text{-}GW}$金鑰）還是使用拜訪網路1017來進行資料連接（此時，

V-P-GW 1024從V-SKME 1026獲得$K_{P\text{-}GW}$金鑰）之間存在一致性。

【0157】例如，在圖10B中，可以允許處於拜訪網路1017中的客戶端設備1006經由拜訪網路1017的V-P-GW 1024來進行資料連接。拜訪網路1017的V-P-GW 1024可以從拜訪網路1017的V-SKME 1026獲得$K_{P\text{-}GW}$金鑰。再舉一個例子，若使用者（其具有作爲其提供商的公司Y）旅行到歐洲，則該使用者可以連接到公司X的網路（其位於歐洲）。使用者可以具有經由公司X的P-GW（例如，V-P-GW 1024）來發送訊息的選項。當客戶端設備1006若在漫遊合作夥伴的網路（亦即，拜訪網路1017）中漫遊時可以使用拜訪網路1017的V-P-GW 1024時，上述方式是可能的。若客戶端設備1006當旅行時被配置爲使用拜訪網路1017的V-P-GW 1024，則本端SKME（例如，V-SKME 1026）可以配置其網路的V-P-GW 1024，從而在客戶端設備1006和V-P-GW 1024之間啓用訊息的交換（其具有基於$K_{P\text{-}GW}$金鑰的安全）。應當注意的是，在圖10B的視圖中，不包括H-SKME 1012，這是由於其是使用者不可獲得的（例如，由於使用者正在外國旅行）。

【0158】因此，在圖10B中，若客戶端設備1006從一個存取節點1032切換到另一個存取節點（未圖示），則拜訪網路1017中的MME 1028可以在每一個傳輸期間（以及在客戶端設備1006連接期間）建立承載，隨後訊息可以從客戶端設備1006轉到V-P-GW 1024。但是，若V-P-GW 1024不具有與客戶端設備1006相關聯的$K_{P\text{-}GW}$，則其可以經由本端SKME（亦就是

V-SKME 1026）來請求該K_{P-GW}。

【0159】經由實現本文所描述的態樣，使用者面安全可能並不依賴於外部安全機制（例如，空中介面安全（如，K_{UPenc}）以及客戶端設備和P-GW之間的安全隧道（例如，IPSEC））。受損害的存取節點將不破壞使用者面安全。存取節點維持空中使用者面傳輸量的保密性和完整性保護。在HSS和MME之間引入SKME以做爲本端信任錨節點或本端金鑰錨節點，實現靈活的進一步金鑰匯出，用於未來新的網路功能。根據一些態樣，SKME可以僅僅負責金鑰匯出、維持和向網路元素（例如，MME、存取節點、P-GW）提供金鑰。

額外態樣

【0160】圖11根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法1100，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0161】客戶端設備和第二實體可以獨立地匯出對使用者面中的訊息進行認證及/或加解密（加密/解密）所基於的共用金鑰（例如，K_{P-GW}），其中第二實體向蜂巢網路和封包資料網路之間的閘道（例如，P-GW）提供該共用金鑰，1102。

【0162】可以經由與該蜂巢網路相關聯的存取節點，從該客戶端設備向閘道發送訊息，其中基於共用金鑰（例如，K_{P-GW}）來對該訊息進行加密和認證中的至少一項，並且該共用金鑰由該客戶端設備和閘道共用，1104。

【0163】客戶端設備可以經由閘道和存取節點，從封包資料網路接收訊息，其中閘道利用共用金鑰來對該訊息進行加密

和認證中的至少一項，1106。

【0164】圖12根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法1200，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0165】客戶端設備和HSS可以獨立地匯出K_{SKME}金鑰，1202。

【0166】HSS可以向SKME提供該K_{SKME}金鑰，1204。

【0167】客戶端設備和SKME可以基於該K_{SKME}金鑰來獨立地匯出$K_{P\text{-}GW}$金鑰，1206。共用的$K_{P\text{-}GW}$金鑰的匯出可以是K_{SKME}和閘道的辨識符（GW ID）的函數。例如，$K_{P\text{-}GW}=F(K_{SKME}, GW ID)$。

【0168】可以由SKME將該共用金鑰$K_{P\text{-}GW}$提供給該蜂巢網路和封包資料網路之間的閘道（例如，經由GW ID標識的閘道），1208。

【0169】圖13根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法1300，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0170】客戶端設備的USIM（或者使用者客戶端設備中的安全處理）基於其擁有的認證片段金鑰K，來匯出完整性金鑰（IK）和加解密金鑰（CK）。認證中心（AuC）自己亦擁有該認證片段金鑰K的相同實例。AuC基於其擁有的相同的認證片段金鑰K，來獨立地匯出完整性金鑰（IK）和加解密金鑰（CK）。兩個認證金鑰K是相同的，因此IK、CK金鑰是相同的。AuC將IK、CK金鑰提供給HSS。客戶端設備和HSS現在皆擁有

共用的秘密（例如，IK、CK），1302。

【0171】客戶端設備和HSS基於共用的秘密（例如，IK、CK），獨立地匯出K_{SKME}金鑰，1304。K_{SKME}可以是客戶端設備和HSS之間的共用的秘密（SS）和服務網路辨識符（SN_ID）的函數F。例如，K_{SKME}=F(SS, SN_ID)。函數F可以是金鑰匯出函數，例如HMAC-x，其中x可以是金鑰長度，例如HMAC-256、HMAC-384。

【0172】HSS可以向片段金鑰管理實體（SKME）提供該K_{SKME}金鑰，1306。

【0173】客戶端設備和SKME可以基於該K_{SKME}金鑰，獨立地匯出K_{ASME}金鑰，1308。並行地，客戶端設備和SKME可以基於該K_{SKME}金鑰，獨立地匯出$K_{P\text{-}GW}$金鑰，1310。

【0174】SKME可以向行動性管理實體（MME）提供K_{ASME}金鑰，1312。並行地，SKME可以向閘道（例如，P-GW）提供$K_{P\text{-}GW}$金鑰，1314。因此，客戶端設備和閘道（例如，P-GW）共用$K_{P\text{-}GW}$金鑰。

【0175】客戶端設備和MME可以基於K_{ASME}金鑰，獨立地匯出K_{eNB}金鑰，1316。MME可以向存取節點提供該K_{eNB}金鑰，1318。因此，客戶端設備和存取節點共用K_{eNB}金鑰。

【0176】圖14根據本文所描述的態樣，圖示在客戶端設備處操作的示例性方法1400，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0177】客戶端設備和第二實體可以獨立地匯出對使用者面中的訊息進行認證及/或加解密（加密/解密）所基於的共用金

鑰（例如，K_{P-GW}），其中第二實體向蜂巢網路和封包資料網路之間的閘道（例如，P-GW）提供該共用金鑰，1402。

【0178】可以從該客戶端設備向網路發送訊息，其中基於共用金鑰（例如，K_{P-GW}）來對該訊息進行加密和認證中的至少一項，並且其中該訊息的加密和認證可以使用例如IPSEC、傳輸層安全預共用金鑰（TLS-PSK）或者資料包TLS-PSK（DTLS-PSK），並且該共用金鑰由客戶端設備和閘道（P-GW）共用，1404。

【0179】客戶端設備可以從網路接收訊息，其中基於共用金鑰來對該訊息進行加密和認證中的至少一項，並且該訊息的加密和認證使用IPSEC、DTLS-PSK或者TLS-PSK，1406。此外，當啓用加密和認證時，可以使用與P-GW共用的共用金鑰（例如，K_{P-GW}）來執行加密和認證。此外，若啓用加密和認證二者，則可以結合與閘道的共用金鑰（例如，K_{P-GW}）來使用具有額外資料的認證加密（AEAD）密碼。示例性AEAD密碼包括伽羅瓦/計數器模式（GCM）中的高級加密標準（AES）（亦即，AES-GCM）和具有密碼塊連結（CBC）-訊息認證碼（CBC-MAC）模式（CCM）的計數器中的高級加密標準（AES）（亦即，AES-CCM）。將理解的是，AEAD密碼以及其實例的記載是示例性而不是限制性的，亦可以使用其他密碼。此外，IPSEC是用於對資料封包進行加密和認證的選項。IPSEC包括在金鑰建立階段期間，在兩個通訊方之間建立共用金鑰的金鑰協商協定。

【0180】圖15根據本文所描述的態樣，圖示在客戶端設備處

操作的示例性方法1500，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0181】客戶端設備和第二實體（例如，SKME）可以獨立地匯出對使用者面中的訊息（例如，使用者面資料傳輸量）進行認證及/或加解密（加密/解密）所基於的第一共用金鑰（例如，$K_{P\text{-}GW}$），其中第二實體向蜂巢網路和封包資料網路之間的閘道（例如，封包資料網路閘道（P-GW））提供該第一共用金鑰，1502。

【0182】客戶端設備和第三實體（例如，MME）可以獨立地匯出對使用者面中的訊息（例如，使用者面資料傳輸量）進行認證及/或加解密（加密/解密）所基於的第二共用金鑰（例如，K_{eNB}），其中第三實體向存取節點（例如，eNodeB）提供該第二共用金鑰，1504。

【0183】客戶端設備可以經由存取節點（例如，eNodeB），從閘道（例如，P-GW）接收第一訊息，其中基於第一共用金鑰（例如，$K_{P\text{-}GW}$）來對該第一訊息進行加密和認證中的至少一項，並且第一訊息進一步封裝在第二訊息中，其中基於第二共用金鑰（例如，K_{eNB}）來對該第二訊息進行加密和認證中的至少一項，1506。

【0184】可以對第二訊息進行解密，並可以基於第二共用金鑰的使用，來驗證第二訊息的認證標籤（例如，可以基於K_{eNB}來匯出K_{UPenc}及/或K_{UPint}），1508。

【0185】因此，可以基於第一共用金鑰的使用，對不再封裝在第二訊息之內的第一訊息（當第二訊息被解密時）進行解

密及/或認證（例如，可以基於K_{P-GW}來匯出$K_{P-GWenc}$及/或$K_{P-GWint}$），1510。

【0186】圖16根據本文所描述的態樣，圖示在設備（例如，晶片組件、客戶端設備）處操作的示例性方法1600，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0187】該方法可以包括：在該設備處，獲得對使用者面訊息進行認證及/或加密所基於的第一共用金鑰，其中第一共用金鑰由該設備和至封包資料網路的閘道共用，並且該設備獨立於該閘道來獲得第一共用金鑰，1602。

【0188】該方法亦可以包括：基於第一共用金鑰對第一訊息進行加密及/或認證，以產生第一加密及/或認證的訊息，1604。

【0189】該方法亦可以進一步包括：經由蜂巢網路的存取節點，經由空中從該設備向閘道發送第一加密及/或認證的訊息，1606。

【0190】可選地，該方法亦可以包括：在該設備處，匯出對訊息進行認證及/或加密所基於的第二共用金鑰，其中第二共用金鑰由該設備和存取節點共用，並且第二共用金鑰與第一共用金鑰不同，1608。該設備可以獨立於該存取節點來獲得第二共用金鑰。第一共用金鑰（例如，K_{P-GW}）和第二共用金鑰（例如，K_{eNB}）是不相關的。

【0191】可選地，該方法亦可以進一步包括：基於第二共用金鑰，對第一加密及/或認證的訊息進行加密及/或認證，以產

生第二加密及/或認證的訊息，其中將第一加密及/或認證的訊息封裝在第二加密及/或認證的訊息之中用於發送給閘道，1610。

【0192】圖17根據本文所描述的態樣，圖示在例如存取節點處操作的示例性方法1700，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0193】可以從存取節點向客戶端設備發送訊息，其中對該訊息進行加密和完整性保護中的至少一項，其中加密和認證基於使用其共用金鑰的、與客戶端設備的協商演算法，其中該共用金鑰是與客戶端設備共用的，1702。另外地或替代地，加密和認證可以基於根據網路或者根據網路服務供應商的配置。另外地或替代地，加密和認證可以基於根據客戶端設備、根據承載的配置。另外地或替代地，加密和認證可以基於承載配置的一部分（例如，根據承載安全配置）。

【0194】在該存取節點處可以從該客戶端設備接收訊息，其中對該訊息進行加密和完整性保護中的至少一項，1704。

【0195】若該訊息被正確地解密或者攜帶有效的認證標籤，則可以將該訊息從網路上的節點轉發到閘道，1706。

【0196】圖18根據本文所描述的態樣，圖示在存取節點（例如，eNodeB）處操作的示例性方法1800，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0197】該方法可以包括：在該存取節點處，經由至封包資料網路的閘道（例如，P-GW），從封包資料網路接收去往設

備的第一訊息，或者從該設備接收去往P-GW的第一訊息，1802。在該設備和P-GW之間的傳輸期間，已經利用由該設備和P-GW共用的第一共用金鑰確保第一訊息安全。該方法亦可以包括：從MME接收配置資訊，其中該配置資訊基於在該設備和P-GW之間是否已經存在安全，來向該存取節點指示是否進一步確保第一訊息安全，1804。

【0198】例如，若沒有利用該設備和閘道共用的第一共用金鑰來確保第一訊息安全，則MME可以經由配置資訊指示：應當利用該設備和存取節點共用的第二共用金鑰來確保第一訊息安全，以產生第一加密的訊息。但是，若已經利用該設備和P-GW共用的第一共用金鑰來確保第一訊息安全，則MME可以經由配置資訊指示：可以在沒有額外安全的情況下，經由空中從存取節點向該設備發送第一訊息。儘管可能不需要進一步的安全，但可以可選地實現。類似地，在相反方向中，MME可以基於在該設備和P-GW之間是否已經存在安全，向存取節點指示是否進一步確保第一訊息安全。隨後，可以基於來自MME的配置資訊，在有或者沒有進一步安全的情況下，從存取節點發送第一訊息，1806。

【0199】圖19根據本文所描述的態樣，圖示在P-GW處操作的示例性方法1900，以保護下一代蜂巢網路中的使用者面訊息的安全及/或完整性。

【0200】可以從封包資料網路閘道（例如，P-GW）向片段金鑰管理實體（SKME）請求共用金鑰（例如，$K_{P\text{-}GW}$），其中該金鑰是與客戶端設備共用的，1902。

【0201】在P-GW處，可以從SKME接收該共用金鑰（例如，K_{P-GW}），1904。

【0202】P-GW可以向客戶端設備發送訊息，其中該訊息基於該共用金鑰（例如，K_{P-GW}）進行了加密及/或認證，1906。換言之，可以使用基於該共用金鑰來匯出的金鑰（例如，$K_{P-GWenc}$、$K_{P-GWint}$），對該訊息進行加密及/或認證。

【0203】P-GW可以從客戶端設備接收訊息，其中該訊息基於該共用金鑰（例如，K_{P-GW}）進行了加密及/或認證，1908。換言之，可以使用基於該共用金鑰來匯出的金鑰（例如，$K_{P-GWenc}$、$K_{P-GWint}$），對該訊息進行加密及/或認證。

【0204】圖20根據本文所描述的態樣，圖示在至封包資料網路的閘道（例如，P-GW）處操作的示例性方法2000，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0205】該方法可以開始於：在P-GW處，從封包資料網路接收第一訊息，2002。

【0206】該方法可以包括：在該閘道處，獲得對第一訊息進行認證及/或加密所基於的第一共用金鑰，其中第一共用金鑰由該閘道和設備共用，且該閘道獨立於該設備來獲得第一共用金鑰，2004。

【0207】該方法亦可以包括：基於第一共用金鑰，對第一訊息進行加密及/或認證，以產生第一加密及/或認證的訊息，2006。

【0208】該方法亦可以包括：經由蜂巢網路的存取節點，向

該設備發送第一加密及/或認證的訊息，2008。

【0209】在相反的方向中（例如，在上行鏈路方向中），閘道可以從存取節點接收第二訊息，其中第二訊息是利用第一共用金鑰來加密及/或認證的，第一共用金鑰僅僅由該客戶端設備和該閘道之間共用，2010。

【0210】可以使用第一共用金鑰對第二訊息進行解密及/或認證，以獲得第三訊息，2012。

【0211】可以將第三訊息發送給封包資料網路，2014。

【0212】圖21根據本文所描述的態樣，圖示在本文稱爲片段金鑰管理實體（SKME）的網路實體處操作的示例性方法2100，以保護下一代蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的安全及/或完整性。

【0213】在片段金鑰管理實體(SKME)處，可以從閘道(P-GW）接收針對客戶端設備的使用者面（UP）金鑰請求，2102。該UP金鑰請求可以包括客戶端設備辨識符。

【0214】臨時行動用戶標識（TMSI）可以由MME來分配，並用於在MME 114處爲了私密性來標識客戶端設備。此外，TMSI是全球唯一臨時客戶端設備標識（GUTI）的一部分。

【0215】例如，根據3GPP TS 23.003：GUTI的格式和大小如下所示：

<GUTI> = <GUMMEI><M-TMSI>,

其中<GUMMEI> = <MCC><MNC><MME Identifier>

以及，<MME Identifier> = <MME Group ID><MME Code>

MCC和MNC應當與先前的3GPP系統具有相同的欄位大小。

M-TMSI的長度應當是32位元。

MME組ID的長度應當是16位元。

MME代碼的長度應當是8位元。

【0216】在服務網路處使用GUTI，因此若服務網路中的P-GW用於封包資料網路連接，則可以使用GUTI來標識客戶端設備。通常，在P-GW處，可以使用國際行動用戶標識（IMSI）和承載ID（其包括隧道端點辨識符（TEID））來標識客戶端設備。

【0217】SKME可以基於K_{SKME}來匯出用於該客戶端設備的UP金鑰（例如，K_{P-GW}），其中$K_{P-GW}=F(K_{SKME}, GW\ ID)$，2104。

【0218】SKME可以向P-GW發送所匯出的UP金鑰（例如，K_{P-GW}），2106。

【0219】圖22根據本文所描述的態樣，圖示在SKME處操作的示例性方法2200，以匯出保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的金鑰。

【0220】該方法可以開始於：從第一實體（例如，HSS）獲得第一共用金鑰（例如，K_{SKME}金鑰）；第一共用金鑰可以由第一實體和設備共用，2202。SKME可以基於第一共用金鑰來匯出第二共用金鑰（例如，K_{P-GW}金鑰）；第二共用金鑰可以由至封包資料網路的閘道和該設備共用，2204。SKME亦可以基於第一共用金鑰，來匯出第三共用金鑰（例如，K_{eNB}金鑰）；第三共用金鑰可以由行動性管理實體（MME）和該設備共用，2206。接著，SKME可以向閘道發送第二共用金鑰，2208

。最後，SKME可以向MME發送第三共用金鑰，2210。

示例性設備以及在其上操作的方法

【0221】圖23圖示被配置爲執行本文所描述的方法的設備2300的示例性硬體實現方式的方塊圖。例如，設備2300可以體現晶片組件、客戶端設備、使用者設備、終端或者某一其他類型的設備。

【0222】設備2300可以包括耦合到無線通訊電路2302和記憶體/存放裝置2306的處理電路、功能單元或模組2304。無線通訊電路2302可以用於將設備2300無線地耦合到服務網路。處理電路/功能單元/模組2304可以包括加密/解密/認證電路、功能單元或模組2308，其中該加密/解密/認證電路、功能單元或模組2308被配置爲使用由該設備和P-GW共用的共用金鑰，執行使用者面資料傳輸量的加密/解密/認證。處理電路/功能單元/模組2304亦可以包括金鑰獲得/產生/匯出電路/功能單元/模組2310，其中該金鑰獲得/產生/匯出電路/功能單元/模組2310被配置爲獲得、產生及/或本端地匯出用於在該設備2300和P-GW之間的傳輸期間對使用者面資料傳輸量進行保護的某些金鑰。爲了有助於使用者面資料傳輸量的保護，除了可以在設備2300的記憶體/存放裝置2306中本機儲存用於加密/解密和認證的其他金鑰（未圖示）之外，記憶體/存放裝置2306可以儲存秘密根金鑰（K金鑰2312（或者該金鑰可以儲存在設備2300的USIM（未圖示）中）），IK、CK金鑰2314，K_{SKME}金鑰2316，K_{ASME}金鑰2318，$K_{P\text{-}GW}$金鑰2320和K_{eNB}金鑰2322。

【0223】通常，處理電路/功能單元/模組2304可以是適於對用於設備2300的資料進行處理的一或多個處理器（例如，第一處理器等）。例如，處理電路/功能單元/模組2304可以是專門處理器，例如，用作用於執行本文所描述的處理或方法中的任何一個的單元的特殊應用積體電路（ASIC）。處理電路/功能單元/模組2304用作用於驗證認證資訊、產生認證資訊、維持存取表、決定命令處於該存取表之中、建立秘密頻道、允許執行、標識設備或者建立秘密頻道的單元的一個實例。處理電路/功能單元/模組2304亦可以用作用於進行接收及/或發送的單元的一個實例。

【0224】處理電路/功能單元/模組2304的實例係包括微處理器、微控制器、數位訊號處理器（DSP）、現場可程式設計閘陣列（FPGA）、可程式設計邏輯裝置（PLD）、狀態機、門邏輯、離散硬體電路、以及被配置爲執行本案內容通篇描述的各種功能的其他適當硬體。處理電路/功能單元/模組2304亦可以負責管理一或多個通訊匯流排，以及執行在可以在記憶體/存放裝置2306中體現的電腦可讀取儲存媒體上儲存的指令。當這些指令（其可以具有軟體的形式）由處理電路/功能單元/模組2304執行時，可以使得電路功能單元/模組2304執行各種功能、步驟及/或本文描述的方法。可以在記憶體/存放裝置2306中體現的電腦可讀取儲存媒體，可以用於儲存在處理電路/功能單元/模組2304執行軟體指令時所操縱的資料。

【0225】記憶體/存放裝置2306可以是非揮發性記憶體，例如但不限於：快閃記憶體、磁或光硬碟等等。在一些態樣中，

記憶體可以是諸如DRAM（如，DDR SDRAM）、SRAM等等之類的揮發性記憶體，它們可以連續地加電以便無限期地儲存資訊。記憶體/存放裝置2306用作用於儲存金鑰的單元的一個實例。

【0226】軟體或指令應當被廣泛地解釋爲意指軟體、指令、指令集、代碼、程式碼片段、程式碼、程式、副程式、軟體模組、應用、軟體應用、套裝軟體、常式、子常式、物件、可執行檔、執行的執行緒、程序、函數等等，無論其被稱爲軟體、韌體、仲介軟體、微代碼、硬體描述語言還是其他術語。軟體可以位於在記憶體/存放裝置2306中體現的電腦可讀取儲存媒體上。該電腦可讀取儲存媒體可以是非臨時性電腦可讀取儲存媒體。舉例而言，非臨時性電腦可讀取儲存媒體包括磁存放裝置（例如，硬碟、軟碟、磁帶）、光碟（例如，壓縮光碟（CD）或數位多功能光碟（DVD））、智慧卡、快閃記憶體設備（例如，卡、棒或鍵式磁碟動）、隨機存取記憶體（RAM）、唯讀記憶體（ROM）、可程式設計ROM（PROM）、可抹除PROM(EPROM)、電子可抹除PROM(EEPROM）、暫存器、抽取式磁碟、以及用於儲存能由電腦存取和讀取的軟體及/或指令的任何其他適當媒體。該電腦可讀取儲存媒體可以位於處理電路/功能單元/模組2304之中、位於其之外、或者分佈在包括處理電路/功能單元/模組2304的多個實體之中。該電腦可讀取儲存媒體可以體現在電腦程式產品中。此外，設備2300可以與電腦可讀取媒體進行互動，舉例而言，該電腦可讀取媒體可以包括載波波形、傳輸線、以及用於發

送能由電腦存取和讀取的軟體及/或指令的任何其他適當媒體。

【0227】圖24根據本文所描述的態樣，圖示在設備（例如，晶片組件、客戶端設備）處操作的示例性方法2400，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0228】該方法可以包括：在該設備處，獲得第一共用金鑰，2402。在該設備處，亦可以獲得基於第一共用金鑰的第二共用金鑰，2404。第二共用金鑰可以用於確保資料傳輸量在該設備和封包資料網路閘道（P-GW）之間傳輸期間的安全。第二共用金鑰可以由該設備和P-GW共用。該方法可以包括：基於第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量，2406。在確保該資料安全之後，該方法可以包括：經由存取節點來向P-GW發送第一安全的資料傳輸量，2408。P-GW和該存取節點可以是不同的網路實體。

【0229】在本文所描述的態樣中，第一共用金鑰可以是P-GW不知道的。可以在該設備處本端地匯出第一共用金鑰和第二共用金鑰，並且不是將其發送給該設備的。換言之，不經由空中將它們發送給該設備。第二共用金鑰可以確保使用者面通訊的至少一些層安全，而不同的金鑰確保控制面通訊安全。

【0230】可選地，該方法可以包括：在該設備處，獲得基於第一共用金鑰的第三共用金鑰，以確保在該設備和行動性管理實體（MME）之間發送的控制訊息傳遞（例如，控制面控

制訊息傳遞）安全，2410。第三共用金鑰可以由該設備和MME共用。該P-GW、該MME和該存取節點可以是不同的網路實體。

【0231】可選地，該方法可以包括：在該設備處，獲得基於第三共用金鑰的第四共用金鑰，以確保該設備和存取節點之間的資料傳輸量以及該設備和MME之間的控制訊息傳遞安全，2412。第四共用金鑰可以由該設備和存取節點共用。可選地，該方法亦可以包括：基於第四共用金鑰來確保第一安全的資料傳輸量安全，以產生第二安全的資料傳輸量，2414。在一些態樣中，第一安全的資料傳輸量封裝在第二安全的資料傳輸量之中。該方法亦可以進一步包括：替代第一安全的資料傳輸量，經由存取節點向P-GW發送第二安全的資料傳輸量，2416。該P-GW、該MME和該存取節點可以是不同的網路實體。

【0232】根據本文所描述的額外態樣，第二共用金鑰在使用者面的網際網路協定（IP）層中，保護第二安全的資料傳輸量，而第四共用金鑰在使用者面的封包資料會聚協定（PDCP）層中，保護第二安全的資料傳輸量。換言之，第四共用金鑰在使用者面的某些層上保護傳輸量的某些傳輸，而第二共用金鑰用於在面的其他層上保護傳輸量的其他傳輸。

【0233】根據本文所描述的態樣，第一共用金鑰可以在該設備和網路實體之間共用。該網路實體可以從歸屬用戶伺服器（HSS）獲得第一共用金鑰。該設備可以獨立於P-GW來獲得第二共用金鑰。獲得第二共用金鑰可以包括：在該設備處，

根據第一共用金鑰和封包資料網路閘道辨識符（GW ID）來匯出第二共用金鑰。

【0234】根據本文所描述的態樣，資料傳輸量與控制訊息傳遞不同。可以在使用者面上發送資料傳輸量，且可以在控制面上發送控制訊息傳遞。使用者面和控制面是不同的傳輸路徑。

【0235】根據本文所描述的一些態樣，確保資料傳輸量安全包括：基於第二共用金鑰，對該資料傳輸量進行加密。根據本文所描述的其他態樣，確保資料傳輸量安全可以包括：包含基於第二共用金鑰的認證簽名。

【0236】關於接收資料傳輸量而言，根據一些態樣，該設備可以經由存取節點來從P-GW接收第三安全的資料傳輸量。第三安全的資料傳輸量可以是基於第二共用金鑰來確保安全的。隨後，該設備可以基於第二共用金鑰對第三安全的資料傳輸量進行解密及/或認證，以產生不安全的資料傳輸量。

示例性封包資料網路閘道（P-GW）以及在其上操作的方法

【0237】圖25圖示被配置爲執行本文所描述的方法的封包資料網路閘道（P-GW）2500的示例性硬體實現方式的方塊圖。

【0238】P-GW 2500可以包括耦合到網路通訊電路2502和記憶體/存放裝置2506的處理電路、功能單元或模組2504。網路通訊電路2502可以用於將P-GW 2500通訊地耦合到封包資料網路及/或蜂巢式系統的核心網路。處理電路/功能單元/模組2504可以包括加密/解密/認證電路、功能單元或模組2508，其中該加密/解密/認證電路、功能單元或模組2508被配置爲使用

由該P-GW 2500和設備共用的共用金鑰，執行使用者面資料傳輸量的加密/解密/認證。處理電路/功能單元/模組2504亦可以包括金鑰獲得/產生電路/功能單元/模組2510，其中該金鑰獲得/產生電路/功能單元/模組2510被配置爲獲得及/或本端地匯出用於在該P-GW 2500和設備之間的傳輸期間對使用者面資料傳輸量進行保護的某些金鑰。在本文所描述的示例性態樣中，金鑰獲得/產生電路/功能單元/模組2510通常可以從SKME獲得共用金鑰（例如，K_{P-GW}），其中該共用金鑰是在SKME處匯出的，並由SKME提供給金鑰獲得/產生電路/功能單元/模組2510。爲了有助於使用者面資料傳輸量的保護，記憶體/存放裝置2506可以將所獲得的K_{P-GW}金鑰2512本機儲存在P-GW 2500的記憶體/存放裝置2506中。

【0239】圖26根據本文所描述的態樣，圖示在P-GW處操作的示例性方法2600，以保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）。

【0240】方法2600可以包括：在P-GW處，從封包資料網路接收資料傳輸量，2602。該方法亦可以包括：在P-GW處，從網路實體獲得秘密共用金鑰，以確保該資料傳輸量在P-GW和設備之間傳輸期間的安全，其中該秘密共用金鑰由P-GW和該設備共用，2604。該方法可以包括：基於該秘密共用金鑰來確保該資料傳輸量安全，以產生第一安全的資料傳輸量，2606。該方法亦可以進一步包括：經由存取節點來向設備發送第一安全的資料傳輸量，其中該P-GW、該存取節點和該網路實體是不同的網路實體，2608。

【0241】根據本文所描述的態樣，該秘密共用金鑰可以是該存取節點不知道的。可以經由控制面介面，將該秘密共用金鑰從網路實體提供給P-GW。該網路實體可以是SKME。

【0242】根據本文所描述的態樣，該秘密共用金鑰可以確保使用者面通訊的至少一些層安全，而不同的共用金鑰確保控制面通訊安全。例如，該秘密共用金鑰可以在使用者面的網際網路協定（IP）層中，保護資料傳輸量。P-GW可以獨立於該設備來獲得該秘密共用金鑰。該秘密共用金鑰可以是P-GW辨識符（GW ID）的函數。

【0243】根據一些態樣，獲得該秘密共用金鑰亦可以包括：從位於歸屬用戶伺服器（HSS）和行動性管理實體（MME）之間的網路實體，獲得該秘密共用金鑰。同樣，該網路實體可以是SKME。

【0244】根據一些態樣，該秘密共用金鑰可以是從與P-GW在相同的域中的網路實體獲得的。

【0245】可選地，該方法亦可以包括：在P-GW處，經由存取節點從該設備接收經由該秘密共用金鑰來確保安全的安全的上行鏈路資料傳輸量，2610。可選地，該方法亦可以包括：利用該秘密共用金鑰對安全的上行鏈路資料傳輸量進行解密及/或認證，以獲得上行鏈路資料傳輸量，2612。可選地，該方法亦可以包括：向封包資料網路發送該上行鏈路資料傳輸量，2614。

示例性網路實體（例如，SKME）以及在其上操作的方法

【0246】圖27圖示被配置爲執行本文所描述的方法的本文稱

爲片段金鑰管理實體（SKME）的網路實體2700的示例性硬體實現方式的方塊圖。

【0247】網路實體2700可以包括耦合到網路通訊電路2702和記憶體/存放裝置2706的處理電路、功能單元或模組2704。網路通訊電路2702可以用於將網路實體2700通訊地耦合到蜂巢式系統的其他網路實體或節點。處理電路/功能單元/模組2704可以包括金鑰獲得/產生電路/功能單元/模組2710，其中該金鑰獲得/產生電路/功能單元/模組2710被配置爲獲得及/或本端地匯出用於在P-GW和設備之間的傳輸期間對使用者面資料傳輸量進行保護的某些金鑰。在本文所描述的示例性態樣中，金鑰獲得/產生電路/功能單元/模組2710通常可以匯出共用金鑰（例如，$K_{P\text{-}GW}$），其中該共用金鑰是在SKME處匯出的，並將其提供給P-GW。在一些態樣中，不需要SKME來儲存$K_{P\text{-}GW}$。在其他態樣中，SKME可以可選地儲存$K_{P\text{-}GW}$。因此，記憶體/存放裝置2706可以可選地本機儲存網路實體2700的$K_{P\text{-}GW}$金鑰2712。

【0248】圖28根據本文所描述的態樣，圖示在SKME處操作的結合保護蜂巢網路中的使用者面訊息（例如，使用者面資料傳輸量）的示例性方法2800。

【0249】方法2800可以開始於：在網路實體處，獲得第一共用金鑰，2802。該網路實體可以獲得基於第一共用金鑰的第二共用金鑰，2804。第二共用金鑰可以用於確保資料傳輸量在設備和封包資料網路閘道（P-GW）之間傳輸期間的安全，其中第二共用金鑰由該設備和P-GW共用。該方法可以繼續：

向P-GW發送第二共用金鑰，2606。

【0250】該方法可以繼續：在該網路實體處，獲得基於第一共用金鑰的第三共用金鑰，2808。第三共用金鑰可以用於確保在該設備和行動性管理實體（MME）之間發送的控制訊息傳遞安全，其中第三共用金鑰由該設備和MME共用。該方法亦可以包括：向MME發送第三共用金鑰，2810。該網路實體、該P-GW和該MME可以是不同的網路實體。

【0251】根據一些態樣，獲得第二共用金鑰亦可以包括：根據第一共用金鑰和封包資料網路閘道辨識符（GW ID）來匯出第二共用金鑰。

【0252】根據一些態樣，資料傳輸量與控制訊息傳遞不同。例如，可以在使用者面上發送資料傳輸量，且可以在控制面上發送控制訊息傳遞，其中使用者面和控制面是不同的傳輸路徑。

【0253】根據一些態樣，該網路實體位於歸屬用戶伺服器（HSS）和MME之間，且該網路實體與HSS和MME不同。

【0254】可以將附圖中所示出的組件、步驟、特徵及/或功能單元裡的一或多個進行重新排列及/或組合到一個單一組件、步驟、特徵或功能單元中，或者體現在幾個組件、步驟或功能單元中。在不偏離本文所揭示的新穎特徵的基礎上，亦可以增加額外的元素、組件、步驟及/或功能單元。附圖中所示出的裝置、設備及/或組件，可以被配置爲執行本文所描述的方法、特徵或者步驟中的一或多個。本文所描述的新穎演算法亦可以高效地實現在軟體中及/或嵌入到硬體中。

【0255】應當理解的是，所揭示方法中步驟的特定順序或等級是對於示例性方法及/或處理的說明。應當明白的是，基於設計偏好，可以重新排列這些方法中步驟的特定順序或等級。所附方法請求項以示例的順序提供了各個步驟的元素，但這並不意指將其限制到所提供的特定順序或等級，除非本文特別地指出。在不偏離本案內容的情況下，亦可以增加或者不使用額外的元素、組件、步驟及/或功能單元。

【0256】儘管已相對於某些實現方式和附圖論述了本案內容的特徵，但本案內容的所有實現方式可以包括本文所論述的優勢特徵中的一或多個。換言之，儘管已將一或多個實現方式論述爲具有某些優勢特徵，但根據本文所論述的各種實現方式中的任何一種，亦可以使用這些特徵中的一或多個。用類似的方式，儘管本文已示例性實現方式論述爲設備、系統或者方法實現方式，但應當理解的是，這些示例性實現方式可以用各種設備、系統和方法來實現。

【0257】此外，應當注意的是，已將至少一些實現方式作爲方法進行描述，其中該方法被描述爲流程圖、流程表、結構圖或方塊圖。儘管流程圖可以將操作描述爲順序方法，但很多操作可以並行或同時地執行。此外，可以重新排列操作的順序。當操作結束時，方法亦就終結了。在一些態樣中，處理可以對應於方法、函數、程序、子常式、副程式等。當處理對應於函數時，該處理的終結對應於該函數到調用函數或主函數的返回。本文所描述的各種處理中的一或多個可以部分地或者全部地通程序式設計（例如，指令及/或資料）來實

現，其中該程式設計可以儲存在機器可讀儲存媒體、電腦可讀取儲存媒體及/或處理器可讀儲存媒體中，並由一或多個處理器、機器及/或設備執行。

【0258】本發明所屬領域中具有通常知識者亦將明白，結合本文所揭示的實現方式描述的各種說明性的邏輯區塊、模組、電路和演算法步驟均可以實現爲硬體、軟體、韌體、仲介軟體、微代碼或者其任意組合。爲了清楚地說明這種可互換性，上文已整體上根據其功能對各種說明性的組件、方塊、模組、電路和步驟進行了描述。至於這種功能是實現爲硬體還是實現爲軟體，取決於特定的應用和對整個系統所施加的設計約束條件。

【0259】在本案內容中，詞語「示例性」用於意指「用作實例、例子或說明」。在本文中描述爲「示例性」的任何實現方式或者態樣不必解釋爲比本案內容的其他態樣更優選或更具有優勢。同樣，術語「態樣」並不要求本案內容的所有態樣皆包括所論述的特徵、優點或操作模式。本文使用術語「耦合」來代表兩個物體之間的直接或者間接耦合。例如，若物體A實體地接觸物體B，並且物體B接觸物體C，則物體A和C仍然可以被視作爲彼此耦合（即使它們彼此不直接地實體接觸）。例如，即使第一晶粒（die）從沒有與第二晶粒直接地實體接觸，第一晶粒亦可以耦合到封裝中的第二晶粒。術語「電路」和「電子線路」被廣義地使用，其意欲包括電子設備和導體的兩種硬體實現方式（當對該電子設備和導體進行連接和配置時，實現本案內容中所描述的功能的效能，而受

不限於電子電路的類型）以及資訊和指令的軟體實現方式（當該資訊和指令由處理器執行時，實現本案內容中所描述的功能的效能）。

【0260】如本文所使用的，術語「決定」涵蓋很多種動作。例如，「決定」可以包括計算、運算、處理、匯出、調查、檢視（例如，查詢表、資料庫或另一資料結構）、查明等等。此外，「決定」可以包括接收（例如，接收資訊）、存取（例如，存取記憶體中的資料）等等。此外，「決定」亦可以包括解析、選定、選擇、建立等等。

【0261】爲使本發明所屬領域中任何具有通常知識者能夠實踐本文所描述的各個態樣，提供了上面的描述。對於本發明所屬領域中具有通常知識者來說，對這些態樣的各種修改皆將是顯而易見的，並且本文所定義的整體原理亦可以適用於其他態樣。因此，本發明並不意欲限於本文示出的態樣，而是被賦予與請求項語言相一致的全部範疇，其中除非特別說明，否則單數形式的元素並不意欲意指「一個和僅僅一個」，而是「一或多個」。除非另外特別說明，否則術語「一些」代表一或多個。代表專案列表「中的至少一個」的短語是指這些專案的任意組合，其包括單一成員。舉例而言，「a、b或c中的至少一個」意欲覆蓋：a；b；c；a和b；a和c；b和c；及a、b和c。本案內容通篇描述的各個態樣的元素的所有結構和功能均等物以引用方式明確地併入本文中，並且意欲由請求項所涵蓋，這些結構和功能均等物對於本發明所屬領域中具有通常知識者來說是公知的或將要是公知的。此外，本

文中沒有任何揭示內容是意欲奉獻給公眾的，不管此類揭示內容是否明確記載在申請專利範圍中。不應依據專利法的規定來解釋任何請求項元素，除非該元素明確採用了措辭「用於.....的單元」進行記載，或者在方法請求項的情形中，該元素是用措辭「用於.....的步驟」來記載的。

【0262】因此，在不偏離本案內容的範疇的情況下，可以在不同的實例和實現方式中實現與本文所描述以及附圖中所示出的實例相關聯的各種特徵。因此，儘管在附圖中描述並圖示某些特定的構造和排列，但這些實現方式僅僅是說明性的，其並不限制本案內容的範疇，這是由於對於本發明所屬領域中具有通常知識者來說，對於所描述實現方式的各種其他增加、修改和刪除皆將是顯而易見的。因此，本案內容的範疇僅僅由所附請求項的文字語言及法律均等物決定。

【符號說明】

【0263】

100 第四代（4G）蜂巢網路

102 進化型通用陸地無線電存取網路（E-UTRAN）

104 進化型封包核心（EPC）

106 客戶端設備

108 通用用戶辨識模組（USIM）

110 虛線

112 存取節點

114 行動性管理實體（MME）

116 實線

118 服務閘道（S-GW）

120 封包資料網路（PDN）閘道（P-GW）

122 封包資料網路

124 歸屬用戶伺服器（HSS）

126 認證中心（AuC）

200 協定堆疊

202 客戶端設備

204 存取節點

206 P-GW

208 應用伺服器（APP 伺服器）

210 網際網路協定層（IP 層）

212 封包資料會聚協定（PDCP）層

214 無線電鏈路控制（RLC）層

216 媒體存取控制（MAC）層

218 實體（PHY）層

220 PDCP 層

222 RLC 層

224 MAC 層

226 PHY 層

228 通用封包式無線電服務（GPRS）隧道協定（GTP-U）層

230 通用封包式無線電服務（GPRS）隧道協定（GTP-U）層

232 網際網路協定層（IP）層

234 MAC 層

236 乙太網路層

238 （GTP-U）層

240 使用者資料包通訊協定（UDP）層

242 IP 層

244 MAC 層

246 乙太網路層

248 IP 層

250 IP 層

252 K_{eNB} 金鑰

254 網際網路協定安全（IPSEC）

300 金鑰等級

302 K 金鑰

304 CK 金鑰

306 K_{ASME} 金鑰

308 非存取層加密金鑰（K_{NASenc} 金鑰）

310 非存取層完整性金鑰（K_{NASint} 金鑰）

312 K_{eNB} 金鑰

314 使用者面完整性金鑰

316 使用者面加密金鑰

318 控制面（無線電資源控制）完整性金鑰

320 控制面（無線電資源控制）加密金鑰

400 4G 蜂巢網路

402 核心網路

404 存取節點

406 客戶端設備

408 HSS

410 MME

412 S-GW

414 P-GW

416 RRC 實體

418 PDCP/RLC 實體

420 IP 實體

422 管道

424 管道

426 IPSEC 隧道

500 下一代（例如，5G）蜂巢網路

502 進化型通用陸地無線電存取網路（E-UTRAN）

504 進化型封包核心（EPC）

506 客戶端設備

508 通用用戶辨識模組（USIM）

510 虛線

512 存取節點

514 行動性管理實體（MME）

516 實線

518 服務閘道（S-GW）

520 封包資料網路（PDN）閘道（P-GW）

522 封包資料網路

524 歸屬用戶伺服器（HSS）

526 認證中心（AuC）

528 片段金鑰管理實體（SKME）

530 拜訪片段金鑰管理實體（V-SKME）

532 V-P-GW

534 第一控制面訊號傳遞路徑

536 第二控制面訊號傳遞路徑

600 協定堆疊

602 客戶端設備

604 存取節點

606 封包資料網路閘道（P-GW）

608 應用伺服器（APP 伺服器）

610 網際網路協定層（IP 層）

612 封包資料會聚協定（PDCP）層

614 無線電鏈路控制（RLC）層

616 媒體存取控制（MAC）層

618 實體（PHY）層

620 PDCP 層

622 RLC 層

624 MAC 層

626 PHY 層

628 GPRS 隧道協定（GTP-U）層

630 使用者資料包通訊協定（UDP）層

632 網際網路協定層（IP）層

634 MAC 層

636 乙太網路層

638 （GTP-U）層

640 使用者資料包通訊協定（UDP）層

642 網際網路協定（IP）層

644 MAC 層

646 乙太網路層

648 IP 層

650 IP 層

656 使用者面安全（UP-SEC）層

658 UP-SEC 層

660 $K_{P\text{-}GW}$ 金鑰

700 金鑰等級

702 K 金鑰

704 IK、CK 金鑰

706 K_{SKME} 金鑰

708 K_{ASME} 金鑰

710 K_{NASenc} 金鑰

712 K_{NASint} 金鑰

714 K_{eNB} 金鑰

716 K_{UPint} 金鑰

718 K_{UPenc} 金鑰

720 K_{RRCint} 金鑰

722 K_{RRCint} 金鑰

724 $K_{P\text{-}GW}$ 金鑰

726 $K_{P\text{-}GWint}$ 金鑰

728 $K_{P\text{-}GWenc}$ 金鑰

800 下一代（例如，5G）蜂巢網路

802 核心網路

804 存取節點

806 客戶端設備

808 HSS

809 SKME

810 MME

811 K_{SKME} 金鑰

812 S-GW

813 K_{ASME} 金鑰

814 P-GW

816 RRC 實體

818 PDCP/RLC 實體

820 IP 實體

822 管道

824 管道

826 管道

828 控制面信號路徑

900 撥叫流

902 設備

904 存取節點

906 MME

908 P-GW

910 片段金鑰管理實體（SKME）

912 PDN 連接請求

914 建立通信期請求

916 互動

918 使用者面（UP）金鑰請求

920 UP 金鑰回應

922 建立通信期回應

924 承載建立請求/PDN 連接接受

926 RRC 連接重新配置請求

928 RRC 連接重新配置完成

930 承載建立回應

932 直接傳輸

934 PDN 連接完成

936 第一訊息

938 第二訊息

1000 下一代蜂巢網路

1002 客戶端設備

1004 下一代蜂巢網路

1006 客戶端設備

1008 HSS

1010 H-P-GW

1011 K_{SKME} 金鑰

1012 H-SKME

1013 K_{SKME}'金鑰

1014 歸屬網路

1016 V-SKME

1017 拜訪網路

1018 MME

1019 K_{ASME} 金鑰

1020 S-GW

1022 存取節點

1024 V-P-GW

1026 V-SKME

1027 K_{SKME} 金鑰

1028 MME

1030 S-GW

1032 存取節點

1034 控制面介面

1036 控制面介面

1100 方法

1102 方塊

1104 方塊

1106 方塊

1200 方法

1202 方塊

1204 方塊

1206 方塊

1208 方塊

1300 方法

1302 方塊

1304 方塊

1306 方塊

1308 方塊

1310 方塊

1312 方塊

1314 方塊

1316 方塊

1318 方塊

1400 方法

1402 方塊

1404 方塊

1406 方塊

1500 方法

1502 方塊

1504 方塊

1506 方塊

1508 方塊

1510 方塊

1600 方法

1602 方塊

1604 方塊

1606 方塊

1608 方塊

1610 方塊

1700 方法

1702 方塊

1704 方塊

1706 方塊

1800 方法

1802 方塊

1804 方塊

1806 方塊

1900 方法

1902 方塊

1904 方塊

1906 方塊

1908 方塊

2000 方法

2002 方塊

2004 方塊

2006 方塊

2008 方塊

2010 方塊

2012 方塊

2014 方塊

2100 方法

2102 方塊

2104 方塊

2106 方塊

2200 方法

2202 方塊

2204 方塊

2206 方塊

2208 方塊

2210 方塊

2300 設備

2302 無線通訊電路

2304 處理電路、功能單元或模組

2306 記憶體/存放裝置

2308 加密/解密/認證電路、功能單元或模組

2310 金鑰獲得/產生/匯出電路/功能單元/模組

2312 K 金鑰

2314 IK、CK 金鑰

2316 K_{SKME} 金鑰

2318 K_{ASME} 金鑰

2320 $K_{P\text{-}GW}$ 金鑰

2322 K_{eNB} 金鑰

2400 方法

2402 方塊

2404 方塊

2406 方塊

2408 方塊

2410 方塊

2412 方塊

2414 方塊

2416 方塊

2500 封包資料網路閘道（P-GW）

2502 封包資料網路閘道（P-GW）

2504 處理電路、功能單元或模組

2506 記憶體/存放裝置

2508 加密/解密/認證電路、功能單元或模組

2510 金鑰獲得/產生電路/功能單元/模組

2512 $K_{P\text{-}GW}$ 金鑰

2600 方法

2602 方塊

2604 方塊

2606 方塊

2608 方塊

2610 方塊

2612 方塊

2614 方塊

2700 片段金鑰管理實體（SKME）的網路實體

2702 網路通訊電路

2704 處理電路、功能單元或模組

2706 記憶體/存放裝置

2710 金鑰獲得/產生電路/功能單元/模組

2712 $K_{P\text{-}GW}$ 金鑰

2800 方法

2802 方塊

2804 方塊

2806 方塊

2808 方塊

2810 方塊

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

公告本

發明摘要

I672933

※ 申請案號：104135269

※ 申請日： 104 年 10 月 27 日　　※IPC 分類：

【發明名稱】（中文/英文）

用於下一代蜂巢網路的使用者面安全

USER-PLANE SECURITY FOR NEXT GENERATION CELLULAR NETWORKS

【中文】

經由在設備（例如，晶片組件、客戶端設備）處獲得第一共用金鑰，並在該設備處，獲得基於第一共用金鑰的第二共用金鑰，可以在該設備處實現確保該設備和封包資料網路閘道（P-GW）之間的使用者面資料傳輸量安全。第二共用金鑰可以用於確保使用者面資料傳輸量在該設備和P-GW之間傳輸期間的安全。該設備和P-GW共用第二共用金鑰。可以基於第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量。可以經由存取節點來向P-GW發送第一安全的資料傳輸量。P-GW和存取節點是不同的網路實體。第二共用金鑰是存取節點不知道的。P-GW從與該設備不同的網路實體獲得第二共用金鑰。

【英文】

Securing user-plane data traffic between a device and a packet data network gateway (P-GW) may be accomplished

at the device (e.g., chip component, client device) by obtaining, at the device, a first shared key, and obtaining, at the device, a second shared key based on the first shared key. The second shared key may be for securing user-plane data traffic during transit between the device and the P-GW. The second shared key is shared by the device and the P-GW. The data traffic may be secured based on the second shared key to produce first secured data traffic. The first secured data traffic may be sent to the P-GW via an access node. The P-GW and the access node are distinct network entities. The second shared key is unknown to the access node. The P-GW obtains the second shared key from a network entity that is distinct from the device.

【代表圖】

【本案指定代表圖】：第（ 7 ）圖。

【本代表圖之符號簡單說明】：

700 金鑰等級

702 K 金鑰

704 IK、CK 金鑰

706 K_{SKME} 金鑰

708 K_{ASME} 金鑰

710 K_{NASenc} 金鑰

712 K_{NASint} 金鑰

714 K_{eNB} 金鑰

716 K_{UPint} 金鑰

718 K_{UPenc} 金鑰

720 K_{RRCint} 金鑰

722 K_{RRCint} 金鑰

724 K_{P-GW} 金鑰

726 $K_{P-GWint}$ 金鑰

728 $K_{P-GWenc}$ 金鑰

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

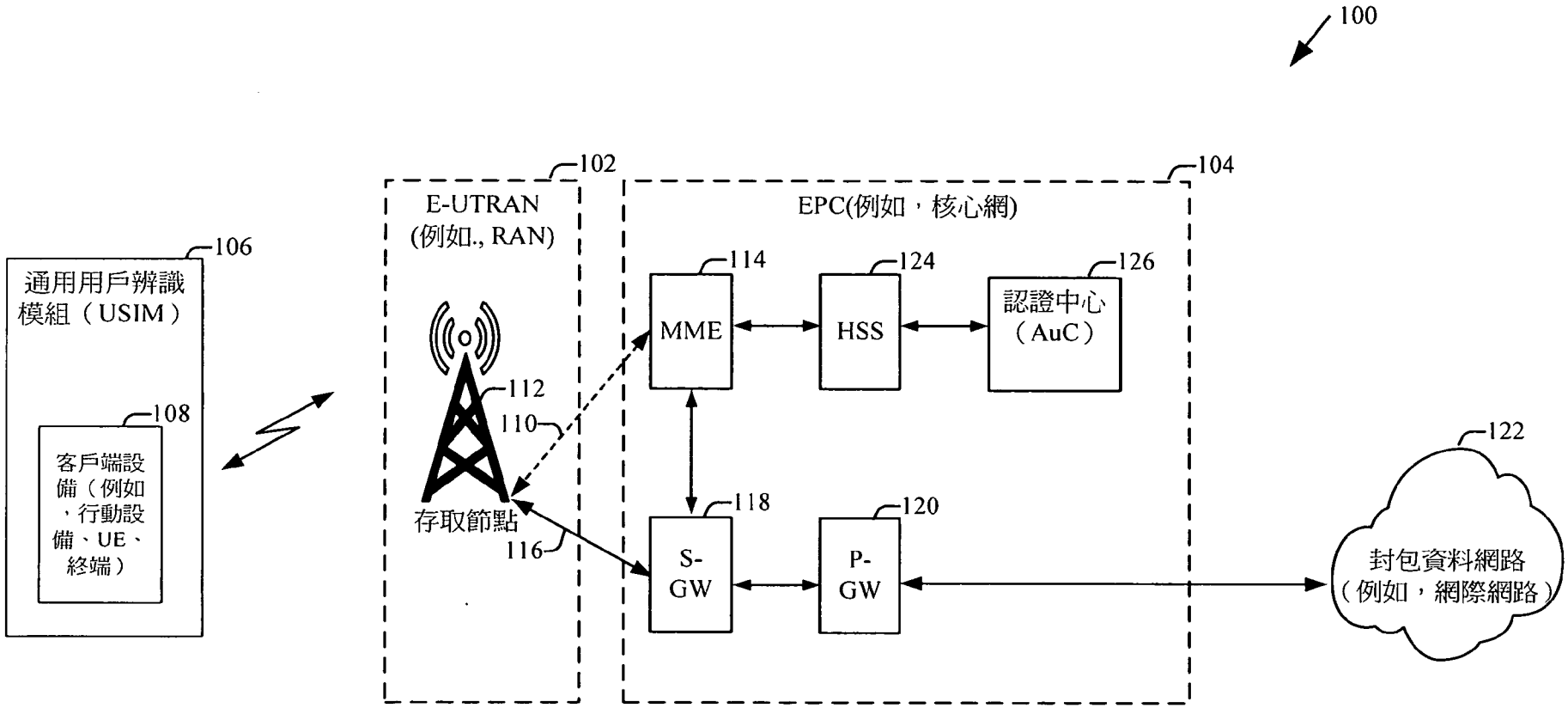
100
102
E-UTRAN
(例如., RAN)
104
EPC(例如，核心網)
106
通用用戶辨識
模組（USIM）
108
客戶端設
備（例如
，行動設
備、UE、
終端）
112
110
存取節點
116
114
MME
124
HSS
126
認證中心
（AuC）
118
S-
GW
120
P-
GW
122
封包資料網路
（例如，網際網路）

圖1
先前技術

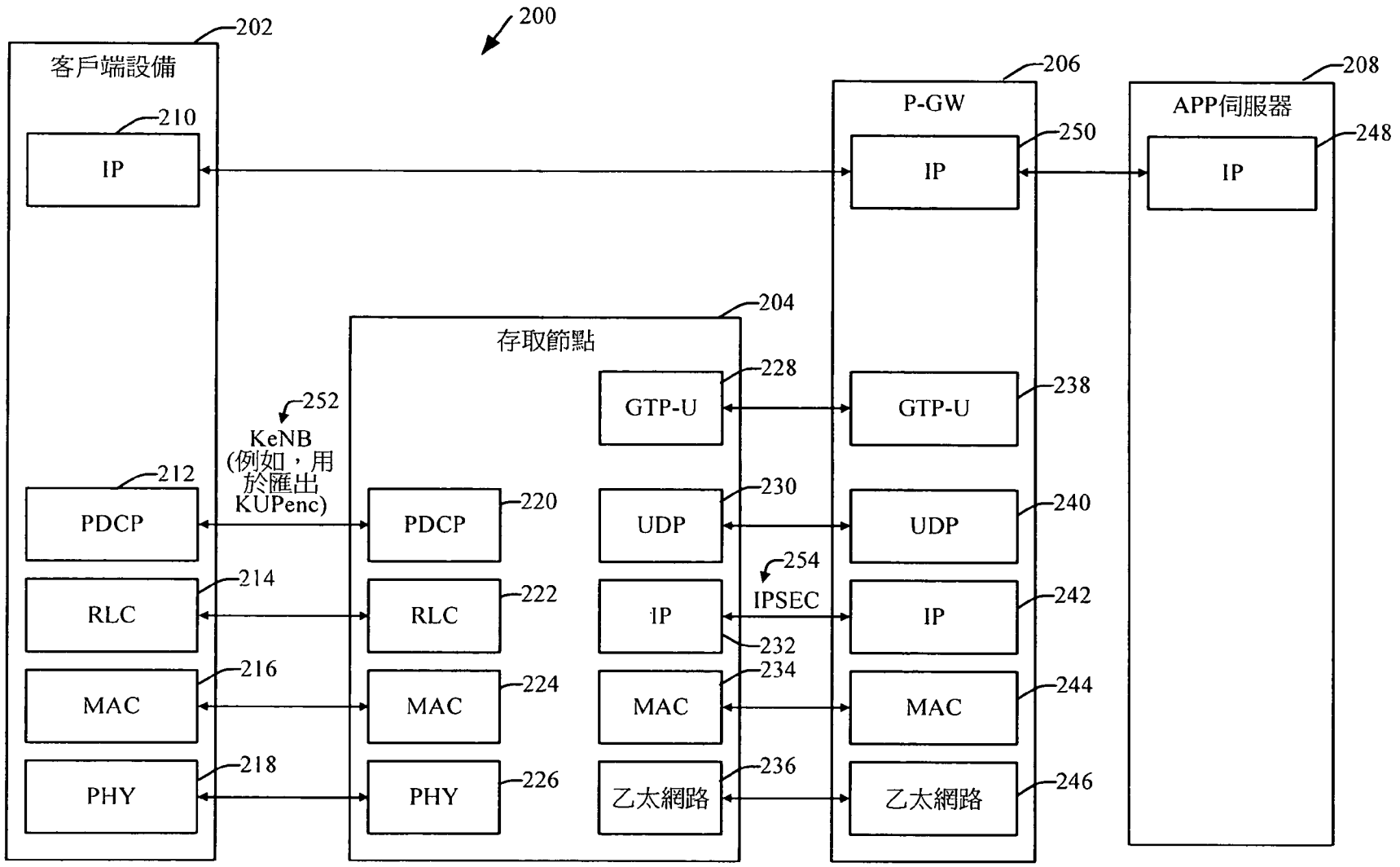
200
202
客戶端設備
210
IP
206
P-GW
250
IP
208
APP伺服器
248
IP
204
存取節點
228
GTP-U
238
GTP-U
252
KeNB
(例如，用
於匯出
KUPenc)
212
PDCP
220
PDCP
230
UDP
240
UDP
254
IPSEC
214
RLC
222
RLC
IP
232
242
IP
216
MAC
224
MAC
234
MAC
244
MAC
218
PHY
226
PHY
236
乙太網路
246
乙太網路

圖2
先前技術

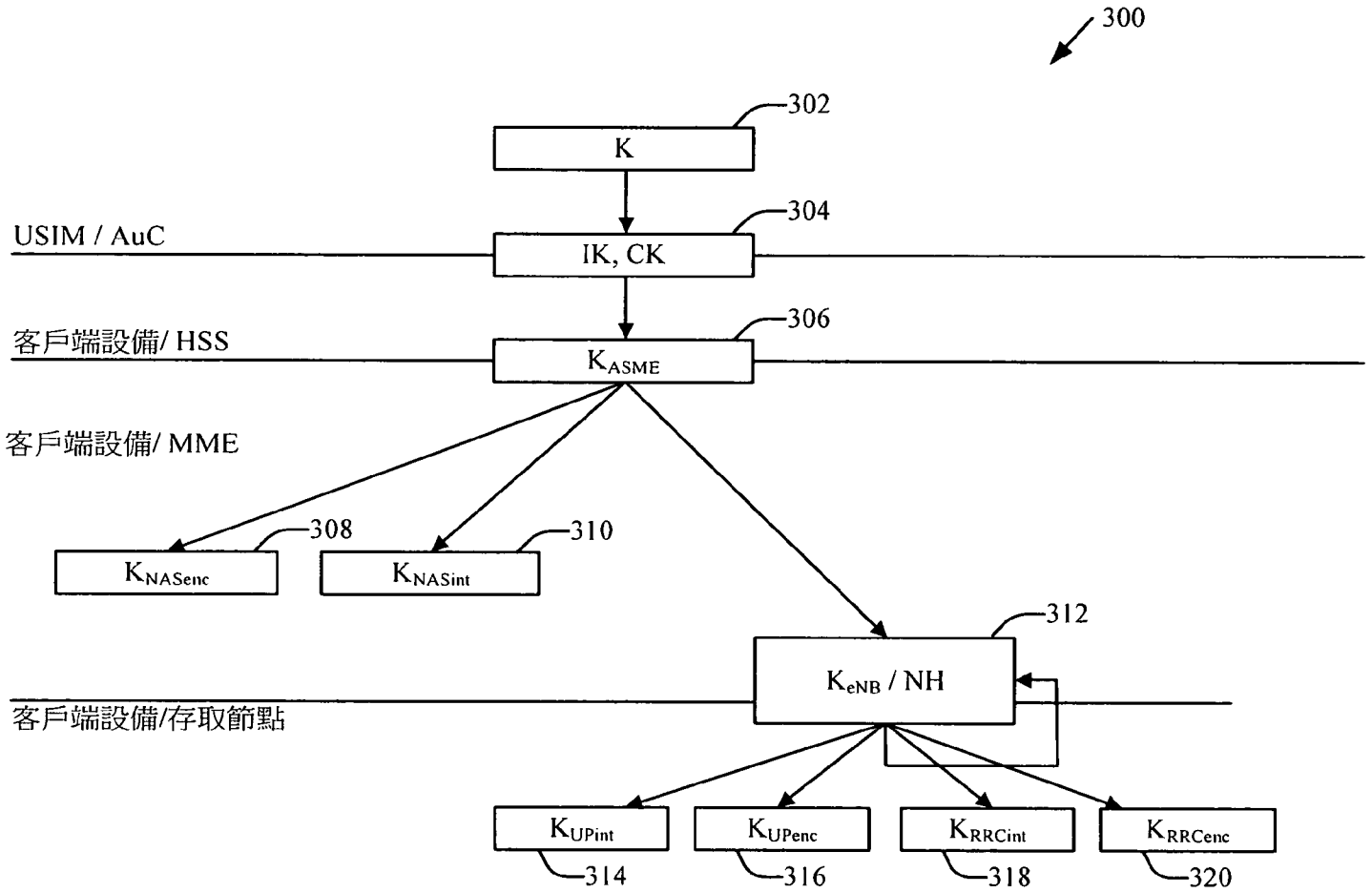
300
302
K
304
USIM / AuC
IK, CK
306
客戶端設備/ HSS
K_{ASME}
客戶端設備/ MME
308
310
K_{NASenc}
K_{NASint}
312
K_{eNB} / NH
客戶端設備/存取節點
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}
314
316
318
320

圖3
先前技術

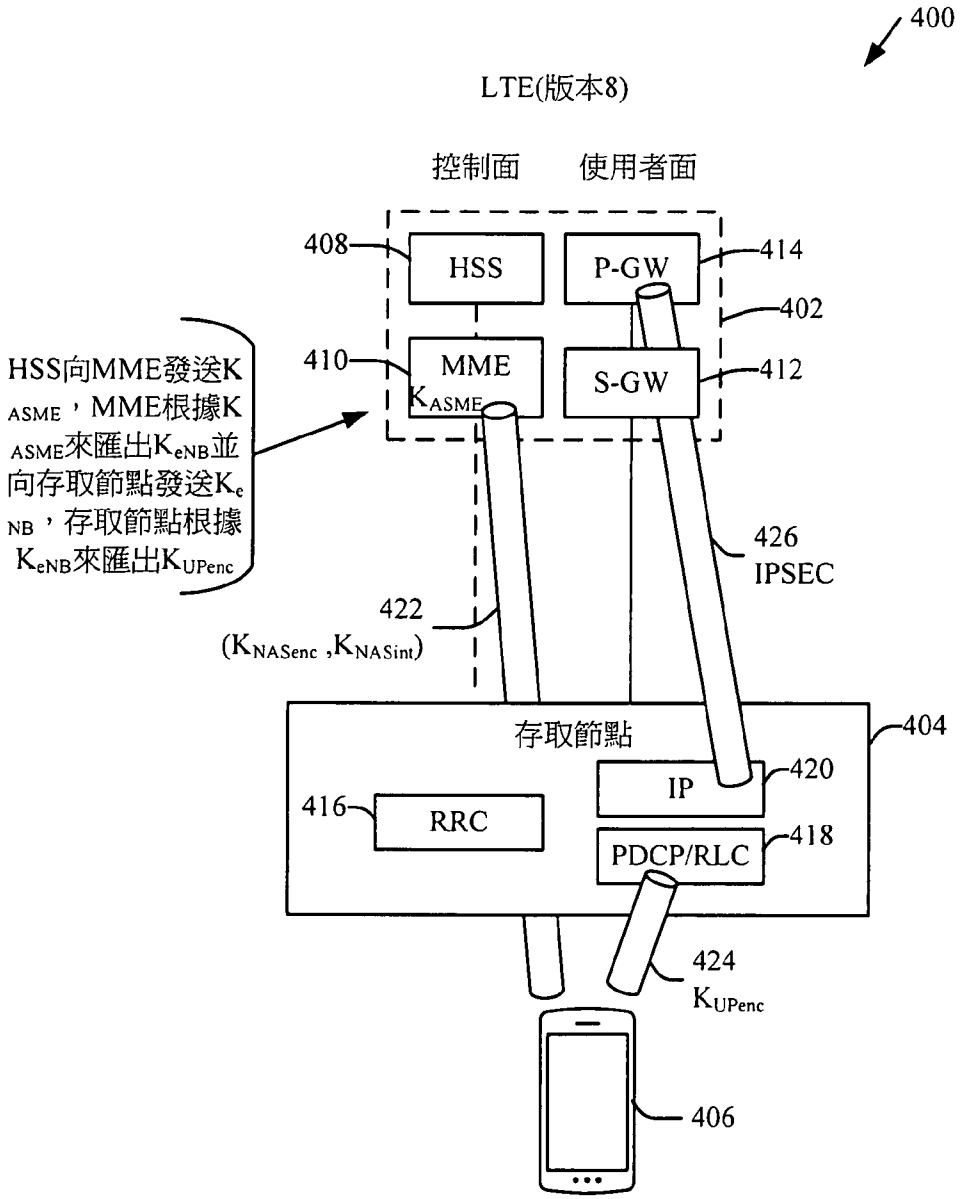
400
LTE(版本8)
控制面
使用者面
408
HSS
P-GW
414
402
410
MME
K_{ASME}
S-GW
412
HSS向MME發送K ASME，MME根據K ASME來匯出K_{eNB}並向存取節點發送K_{eNB}，存取節點根據K_{eNB}來匯出K_{UPenc}
426
IPSEC
422
(K_{NASenc} ,K_{NASint})
存取節點
404
IP
420
416
RRC
PDCP/RLC
418
424
K_{UPenc}
406

圖4
先前技術

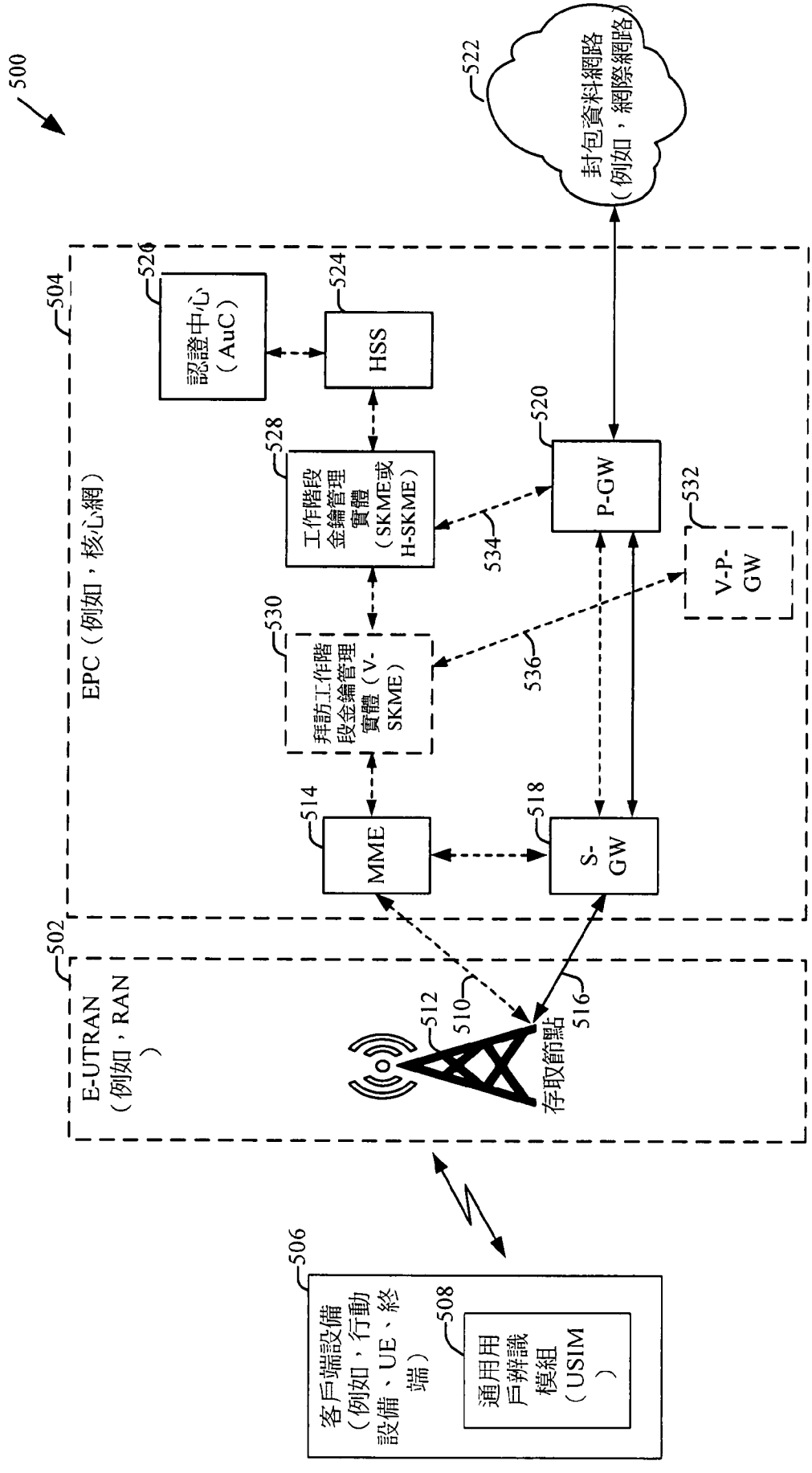
500
502
E-UTRAN（例如，RAN）
504
EPC（例如，核心網）
506
客戶端設備（例如，行動設備、UE、終端）
508
通用用戶辨識模組（USIM）
510
存取節點
512
514
MME
516
518
S-GW
520
P-GW
522
封包資料網路（例如，網際網路）
524
HSS
526
認證中心（AuC）
528
工作階段金鑰管理實體（SKME或H-SKME）
530
拜訪工作階段金鑰管理實體（V-SKME）
532
V-P-GW
534
536

圖5

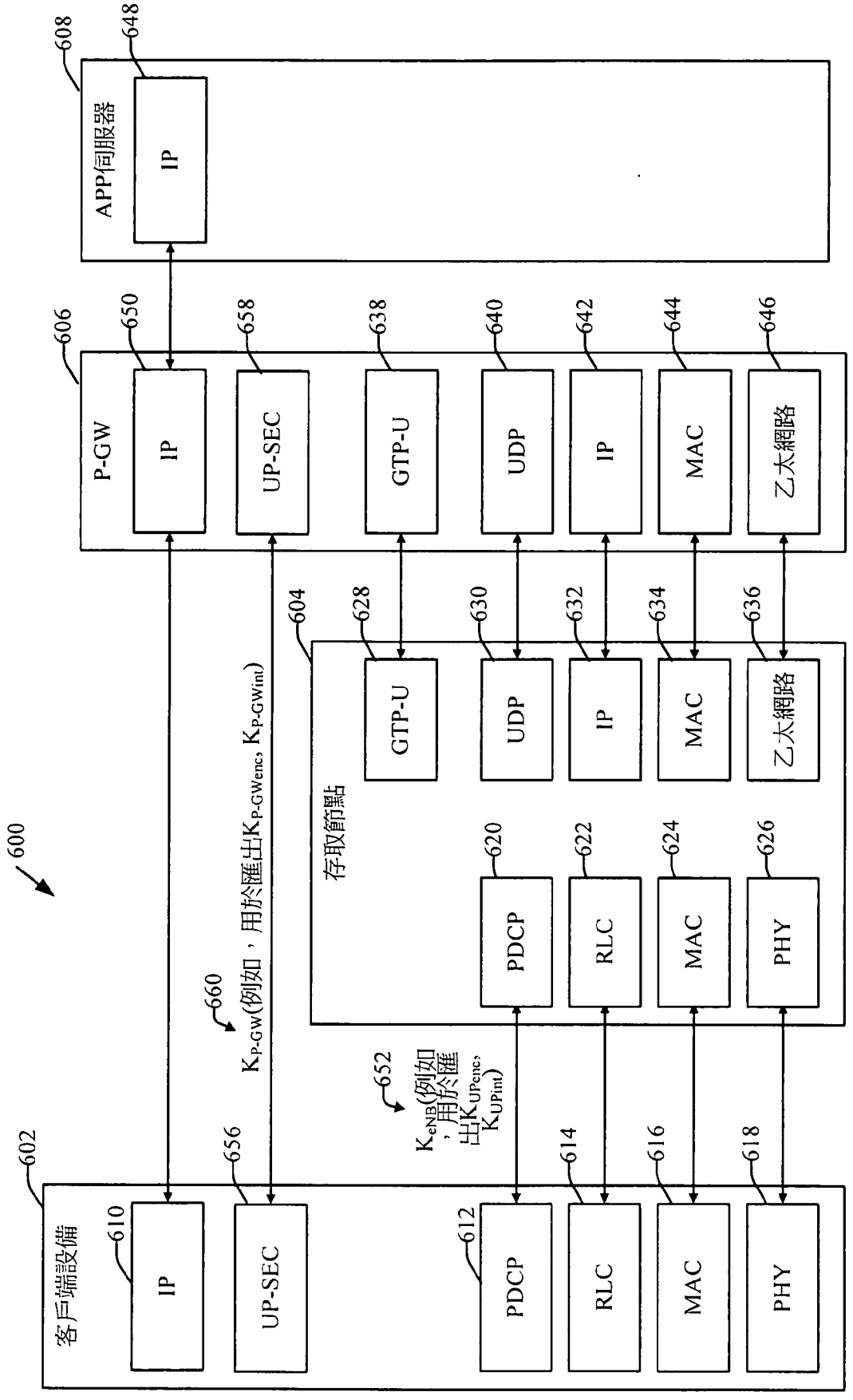
600
602
客戶端設備
610
IP
656
UP-SEC
612
PDCP
614
RLC
616
MAC
618
PHY
604
存取節點
620
PDCP
622
RLC
624
MAC
626
PHY
628
GTP-U
630
UDP
632
IP
634
MAC
636
乙太網路
606
P-GW
650
IP
658
UP-SEC
638
GTP-U
640
UDP
642
IP
644
MAC
646
乙太網路
608
APP伺服器
648
IP
660
$K_{P\text{-}GW}$(例如，用於匯出$K_{P\text{-}GWenc}$, $K_{P\text{-}GWint}$)
652
K_{eNB}(例如，用於匯出K_{UPenc}, K_{UPint})

圖6

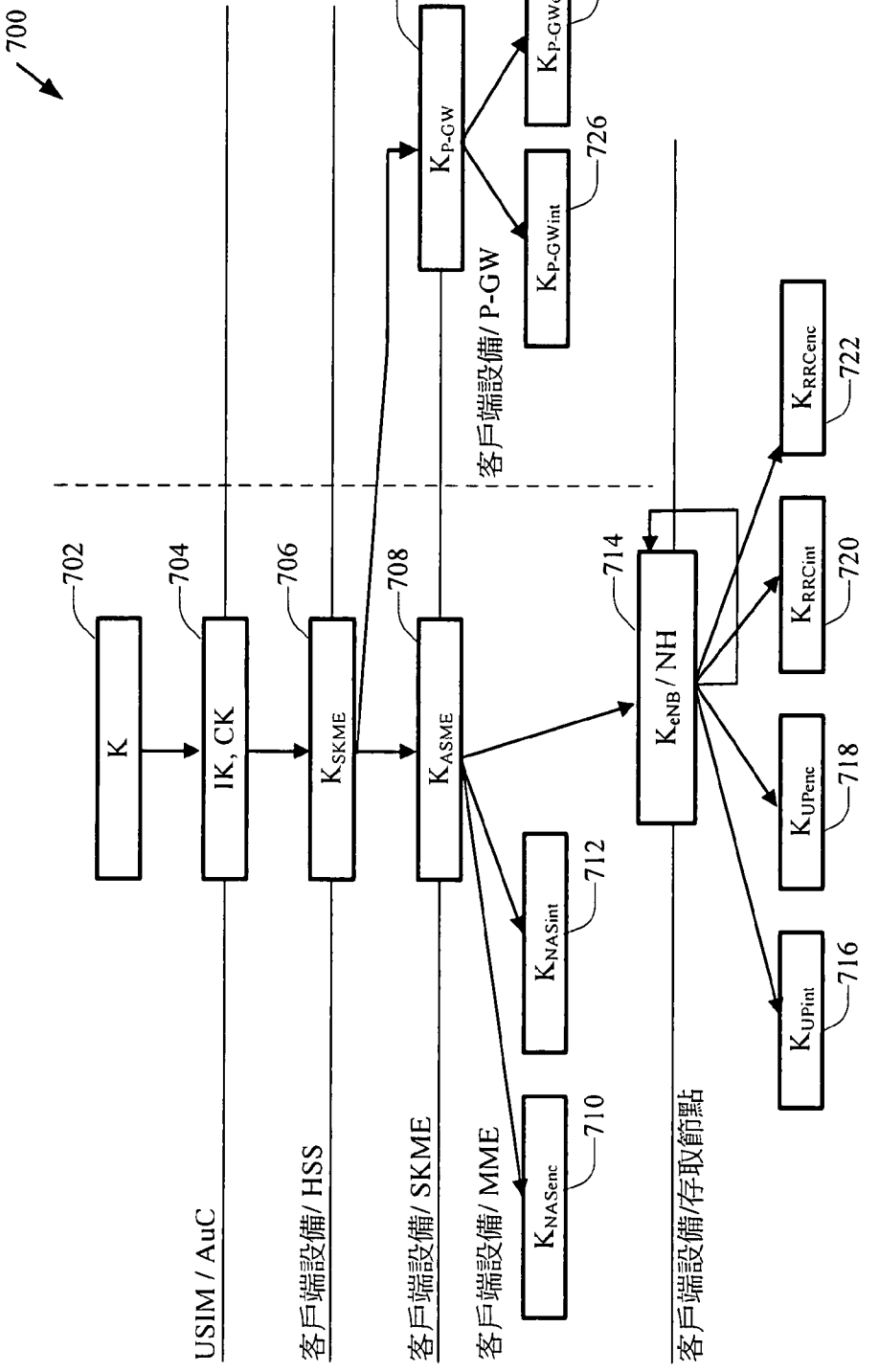
700
K
IK, CK
K_{SKME}
K_{ASME}
K_{eNB} / NH
K_{NASenc}
K_{NASint}
K_{UPenc}
K_{UPint}
K_{RRCenc}
K_{RRCint}
K_{P-GW}
$K_{P-GWenc}$
$K_{P-GWint}$
702
704
706
708
710
712
714
716
718
720
722
724
726
728
USIM / AuC
客戶端設備/ HSS
客戶端設備/ SKME
客戶端設備/ MME
客戶端設備/存取節點
客戶端設備/ P-GW

圖7

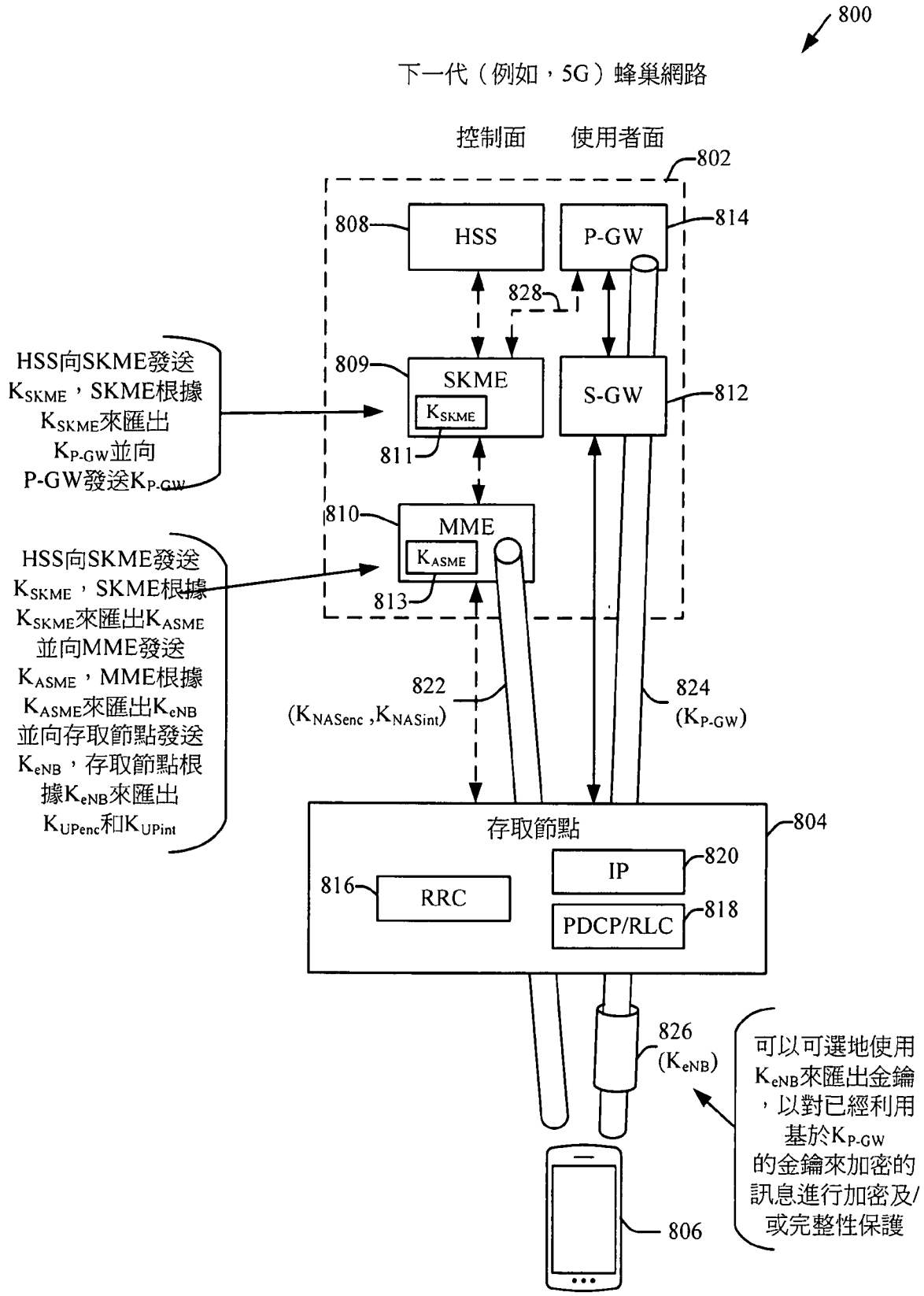
800
下一代（例如，5G）蜂巢網路
控制面
使用者面
802
808
HSS
P-GW
814
828
809
SKME
K_{SKME}
S-GW
812
811
810
MME
K_{ASME}
813
HSS向SKME發送K_{SKME}，SKME根據K_{SKME}來匯出K_{P-GW}並向P-GW發送K_{P-GW}
HSS向SKME發送K_{SKME}，SKME根據K_{SKME}來匯出K_{ASME}並向MME發送K_{ASME}，MME根據K_{ASME}來匯出K_{eNB}並向存取節點發送K_{eNB}，存取節點根據K_{eNB}來匯出K_{UPenc}和K_{UPint}
822
(K_{NASenc} ,K_{NASint})
824
(K_{P-GW})
存取節點
804
820
IP
816
RRC
818
PDCP/RLC
826
(K_{eNB})
可以可選地使用K_{eNB}來匯出金鑰，以對已經利用基於K_{P-GW}的金鑰來加密的訊息進行加密及/或完整性保護
806

圖8

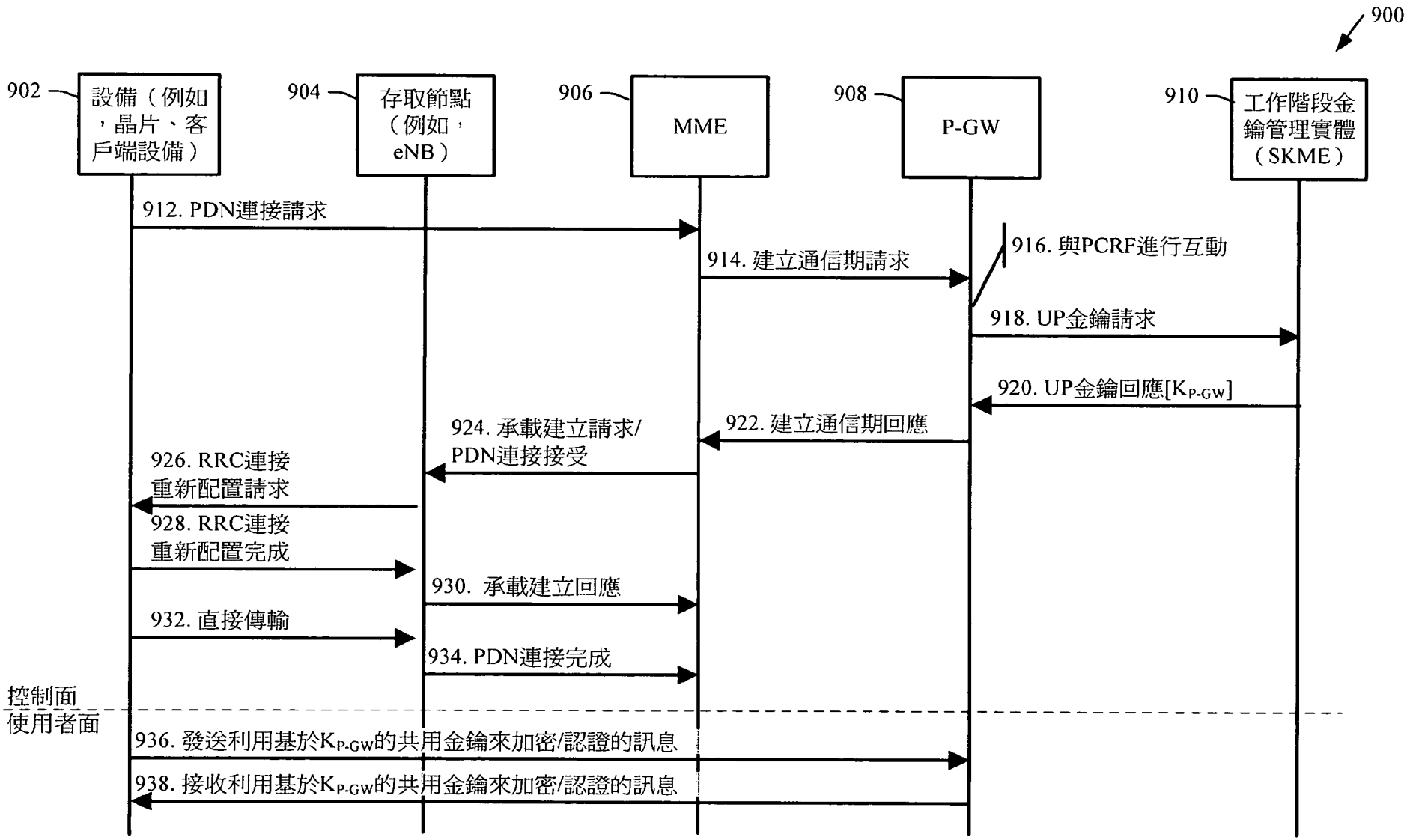
900
902
設備（例如，晶片、客戶端設備）
904
存取節點（例如，eNB）
906
MME
908
P-GW
910
工作階段金鑰管理實體（SKME）
912. PDN連接請求
914. 建立通信期請求
916. 與PCRF進行互動
918. UP金鑰請求
920. UP金鑰回應[$K_{P\text{-}GW}$]
922. 建立通信期回應
924. 承載建立請求/PDN連接接受
926. RRC連接重新配置請求
928. RRC連接重新配置完成
930. 承載建立回應
932. 直接傳輸
934. PDN連接完成
控制面
使用者面
936. 發送利用基於$K_{P\text{-}GW}$的共用金鑰來加密/認證的訊息
938. 接收利用基於$K_{P\text{-}GW}$的共用金鑰來加密/認證的訊息

圖9

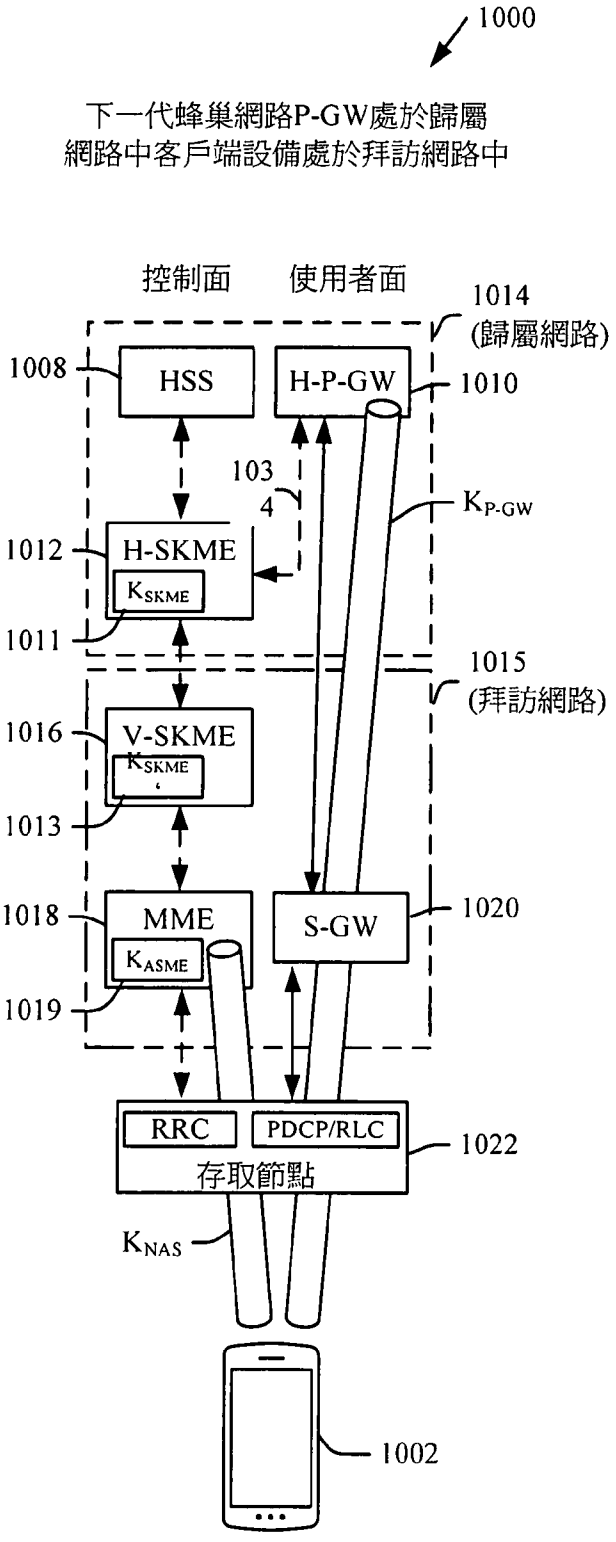
1000
下一代蜂巢網路P-GW處於歸屬網路中客戶端設備處於拜訪網路中
控制面
使用者面
1014
(歸屬網路)
1008
HSS
H-P-GW
1010
103
4
$K_{P\text{-}GW}$
1012
H-SKME
K_{SKME}
1011
1015
(拜訪網路)
1016
V-SKME
K_{SKME}
1013
1018
MME
K_{ASME}
S-GW
1020
1019
RRC
PDCP/RLC
存取節點
1022
K_{NAS}
1002

圖10A

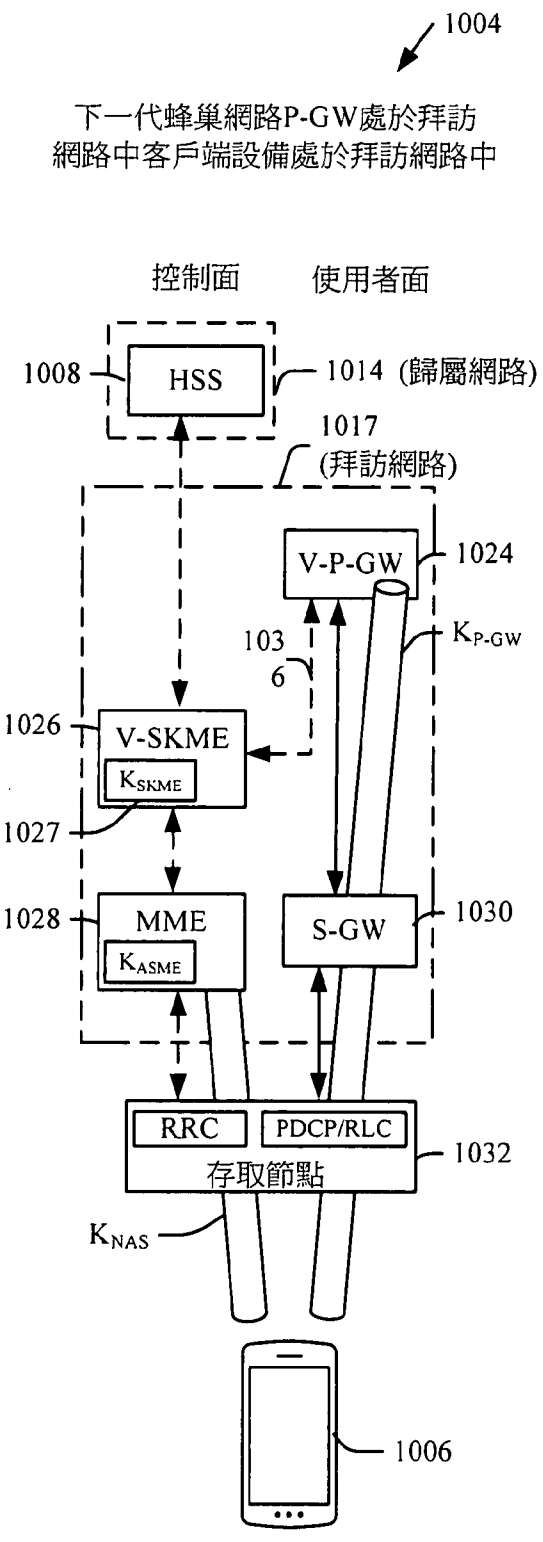
1004
下一代蜂巢網路P-GW處於拜訪網路中客戶端設備處於拜訪網路中
控制面
使用者面
1008
HSS
1014 (歸屬網路)
1017
(拜訪網路)
V-P-GW
1024
$K_{P\text{-}GW}$
103
6
1026
V-SKME
K_{SKME}
1027
1028
MME
K_{ASME}
S-GW
1030
RRC
PDCP/RLC
存取節點
1032
K_{NAS}
1006

圖10B

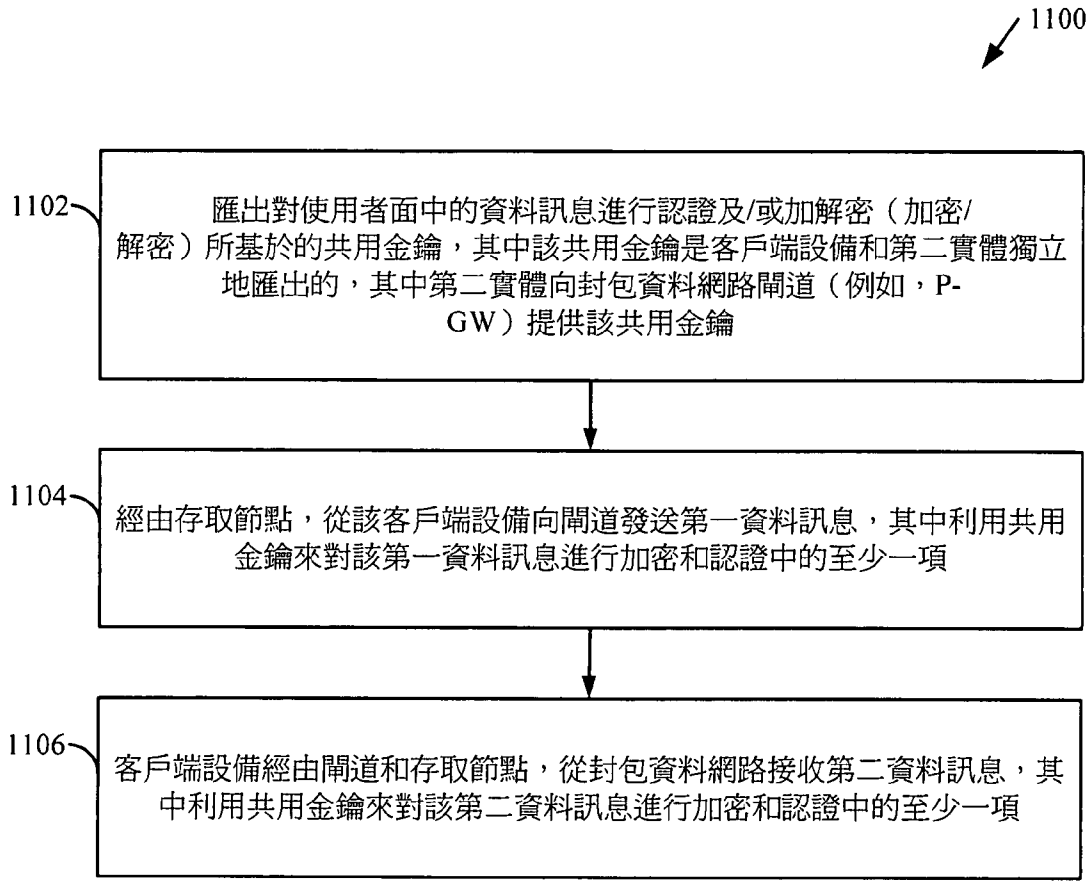
1100
1102
匯出對使用者面中的資料訊息進行認證及/或加解密（加密/解密）所基於的共用金鑰，其中該共用金鑰是客戶端設備和第二實體獨立地匯出的，其中第二實體向封包資料網路閘道（例如，P-GW）提供該共用金鑰
1104
經由存取節點，從該客戶端設備向閘道發送第一資料訊息，其中利用共用金鑰來對該第一資料訊息進行加密和認證中的至少一項
1106
客戶端設備經由閘道和存取節點，從封包資料網路接收第二資料訊息，其中利用共用金鑰來對該第二資料訊息進行加密和認證中的至少一項

圖11

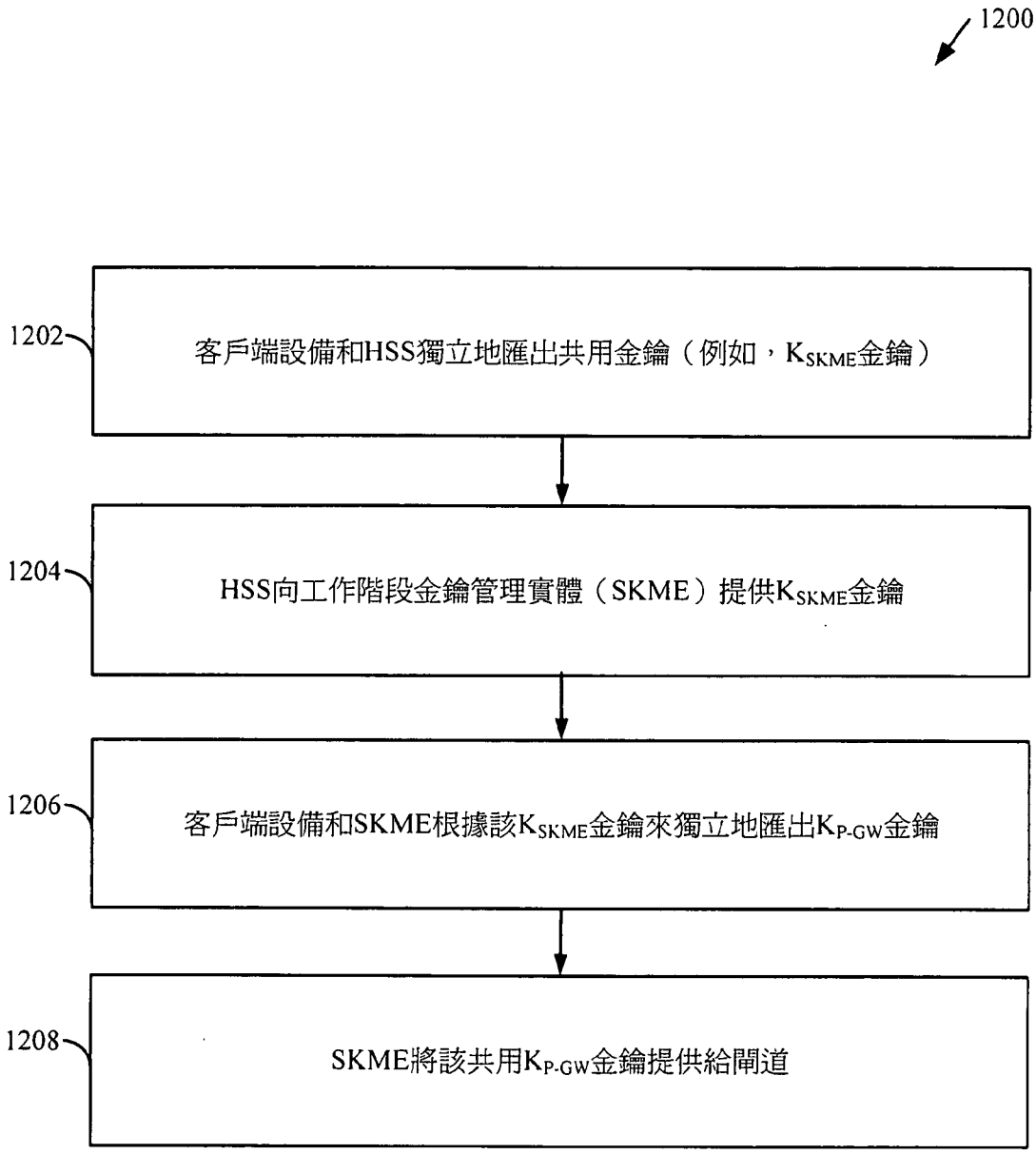
1200
1202
客戶端設備和HSS獨立地匯出共用金鑰（例如，K_{SKME}金鑰）
1204
HSS向工作階段金鑰管理實體（SKME）提供K_{SKME}金鑰
1206
客戶端設備和SKME根據該K_{SKME}金鑰來獨立地匯出$K_{P\text{-}GW}$金鑰
1208
SKME將該共用$K_{P\text{-}GW}$金鑰提供給閘道

圖12

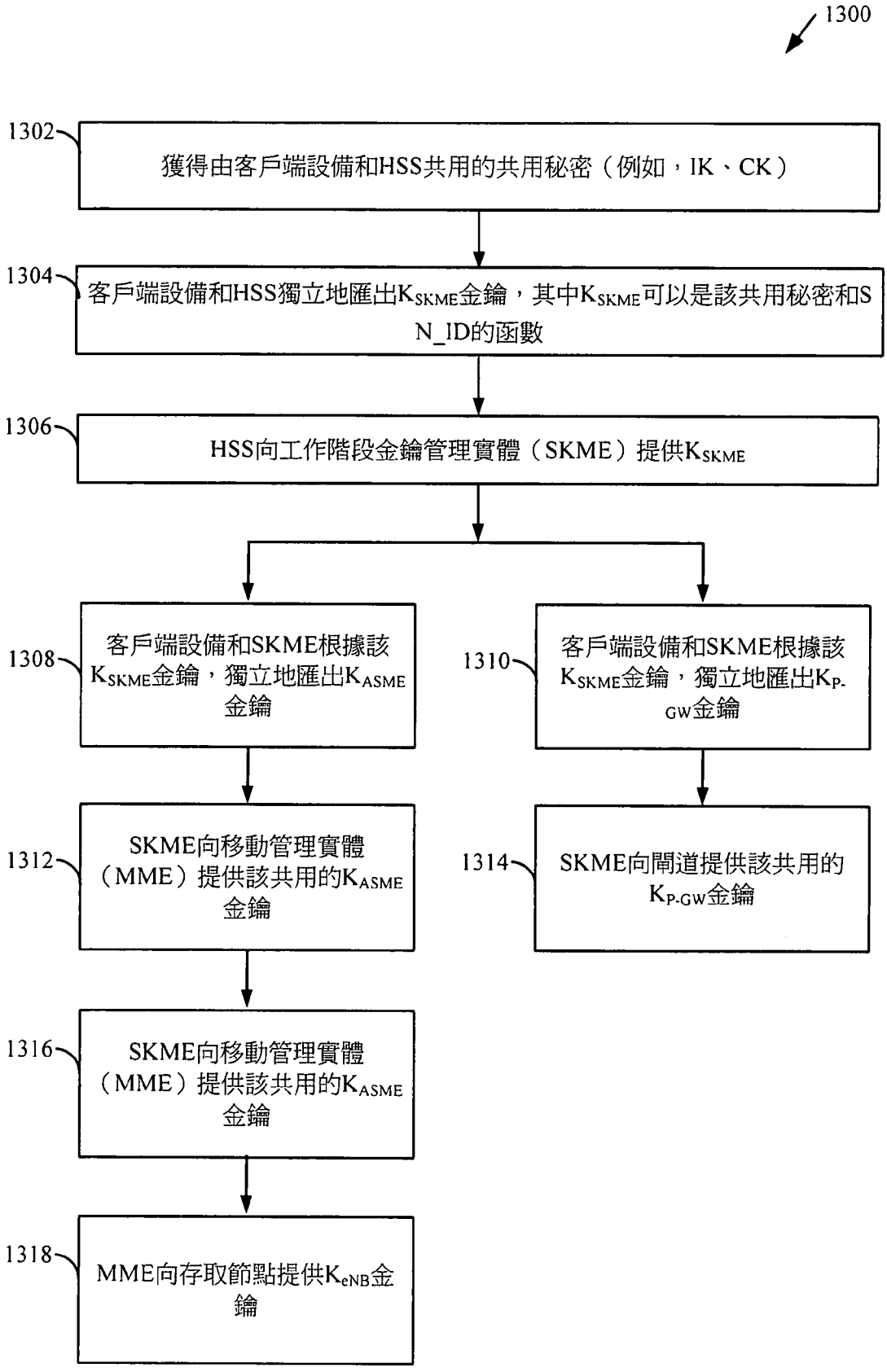
1300
1302
獲得由客戶端設備和HSS共用的共用秘密（例如，IK、CK）
1304
客戶端設備和HSS獨立地匯出K_{SKME}金鑰，其中K_{SKME}可以是該共用秘密和SN_ID的函數
1306
HSS向工作階段金鑰管理實體（SKME）提供K_{SKME}
1308
客戶端設備和SKME根據該K_{SKME}金鑰，獨立地匯出K_{ASME}金鑰
1310
客戶端設備和SKME根據該K_{SKME}金鑰，獨立地匯出K_{P-GW}金鑰
1312
SKME向移動管理實體（MME）提供該共用的K_{ASME}金鑰
1314
SKME向閘道提供該共用的K_{P-GW}金鑰
1316
SKME向移動管理實體（MME）提供該共用的K_{ASME}金鑰
1318
MME向存取節點提供K_{eNB}金鑰

圖13

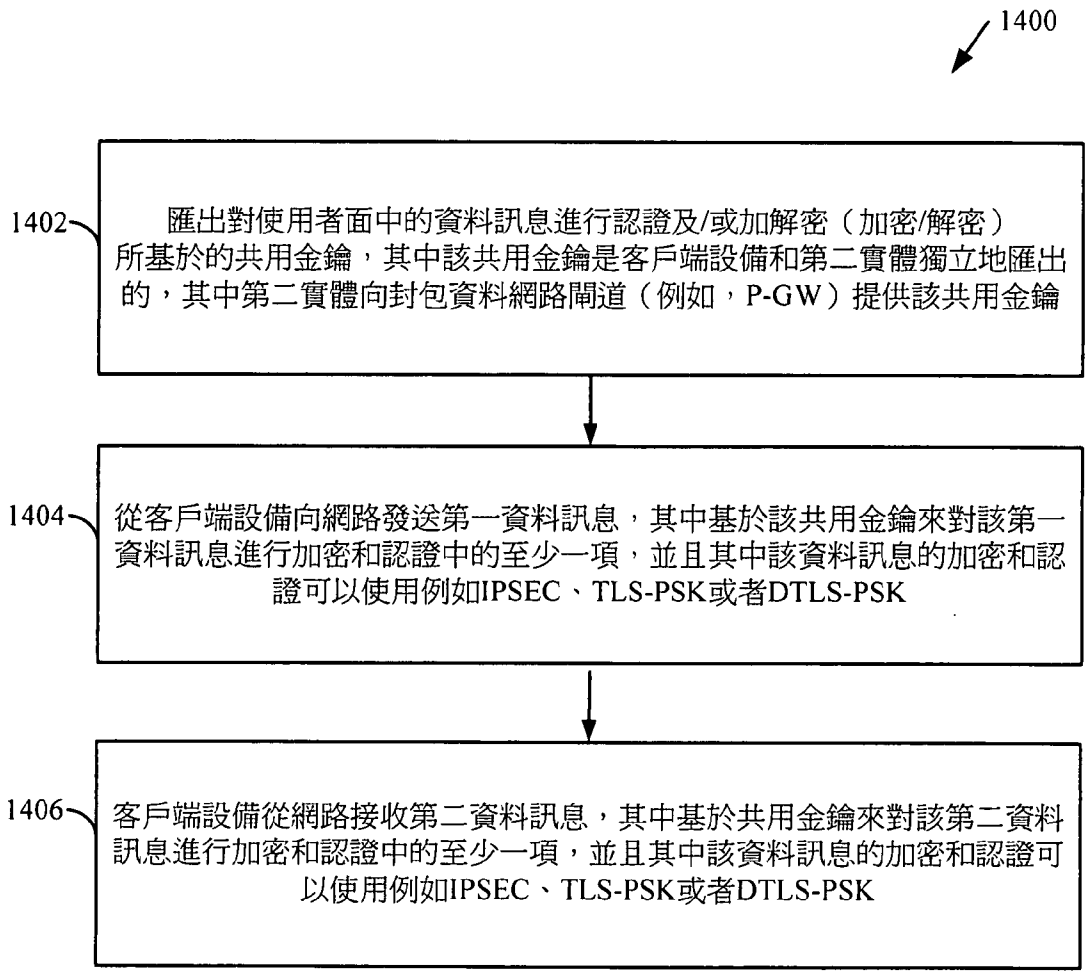
1400
1402
匯出對使用者面中的資料訊息進行認證及/或加解密（加密/解密）所基於的共用金鑰，其中該共用金鑰是客戶端設備和第二實體獨立地匯出的，其中第二實體向封包資料網路閘道（例如，P-GW）提供該共用金鑰
1404
從客戶端設備向網路發送第一資料訊息，其中基於該共用金鑰來對該第一資料訊息進行加密和認證中的至少一項，並且其中該資料訊息的加密和認證可以使用例如IPSEC、TLS-PSK或者DTLS-PSK
1406
客戶端設備從網路接收第二資料訊息，其中基於共用金鑰來對該第二資料訊息進行加密和認證中的至少一項，並且其中該資料訊息的加密和認證可以使用例如IPSEC、TLS-PSK或者DTLS-PSK

圖14

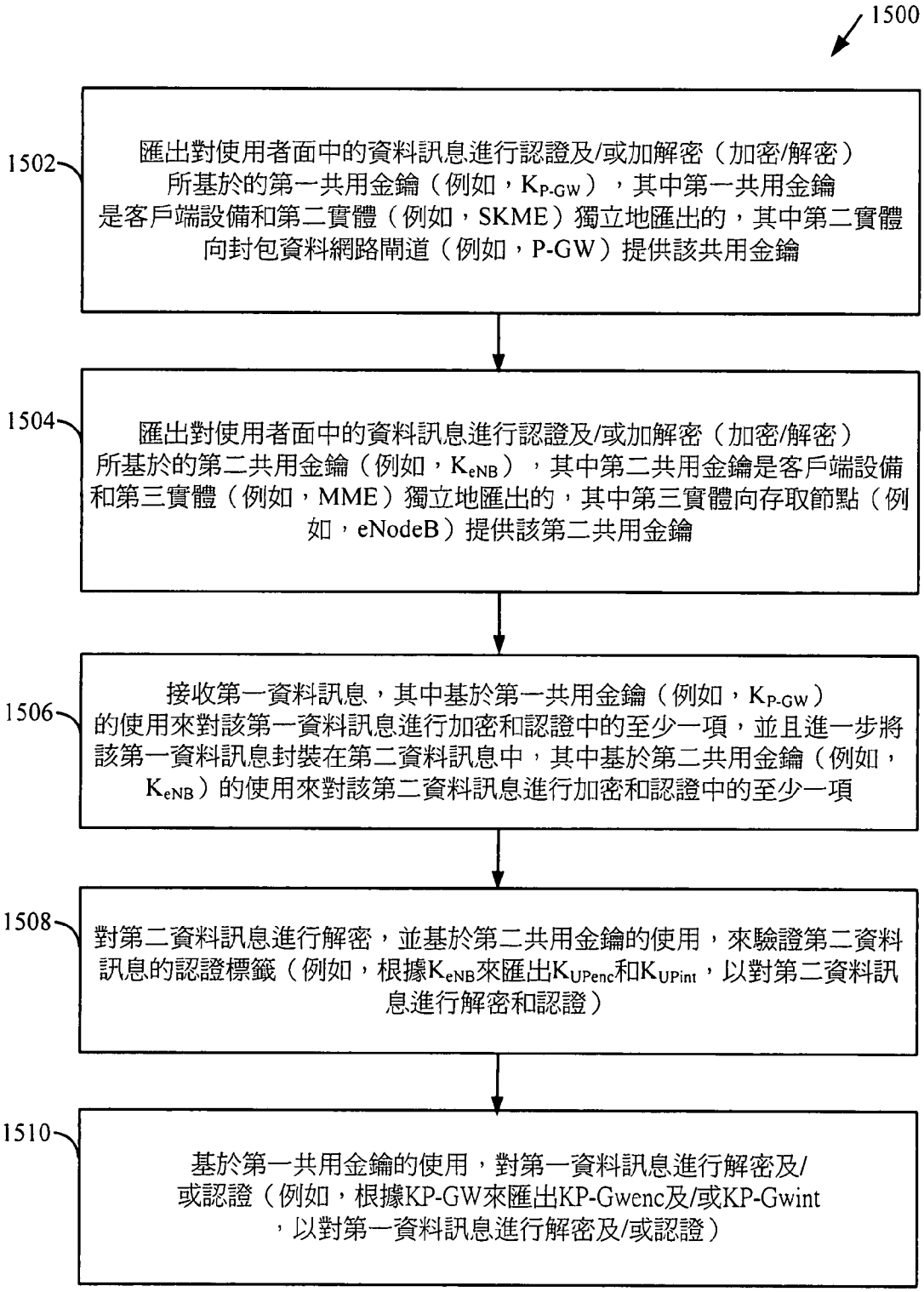
1500
1502
匯出對使用者面中的資料訊息進行認證及/或加解密（加密/解密）所基於的第一共用金鑰（例如，K_{P-GW}），其中第一共用金鑰是客戶端設備和第二實體（例如，SKME）獨立地匯出的，其中第二實體向封包資料網路閘道（例如，P-GW）提供該共用金鑰
1504
匯出對使用者面中的資料訊息進行認證及/或加解密（加密/解密）所基於的第二共用金鑰（例如，K_{eNB}），其中第二共用金鑰是客戶端設備和第三實體（例如，MME）獨立地匯出的，其中第三實體向存取節點（例如，eNodeB）提供該第二共用金鑰
1506
接收第一資料訊息，其中基於第一共用金鑰（例如，K_{P-GW}）的使用來對該第一資料訊息進行加密和認證中的至少一項，並且進一步將該第一資料訊息封裝在第二資料訊息中，其中基於第二共用金鑰（例如，K_{eNB}）的使用來對該第二資料訊息進行加密和認證中的至少一項
1508
對第二資料訊息進行解密，並基於第二共用金鑰的使用，來驗證第二資料訊息的認證標籤（例如，根據K_{eNB}來匯出K_{UPenc}和K_{UPint}，以對第二資料訊息進行解密和認證）
1510
基於第一共用金鑰的使用，對第一資料訊息進行解密及/或認證（例如，根據KP-GW來匯出KP-Gwenc及/或KP-Gwint，以對第一資料訊息進行解密及/或認證）

圖15

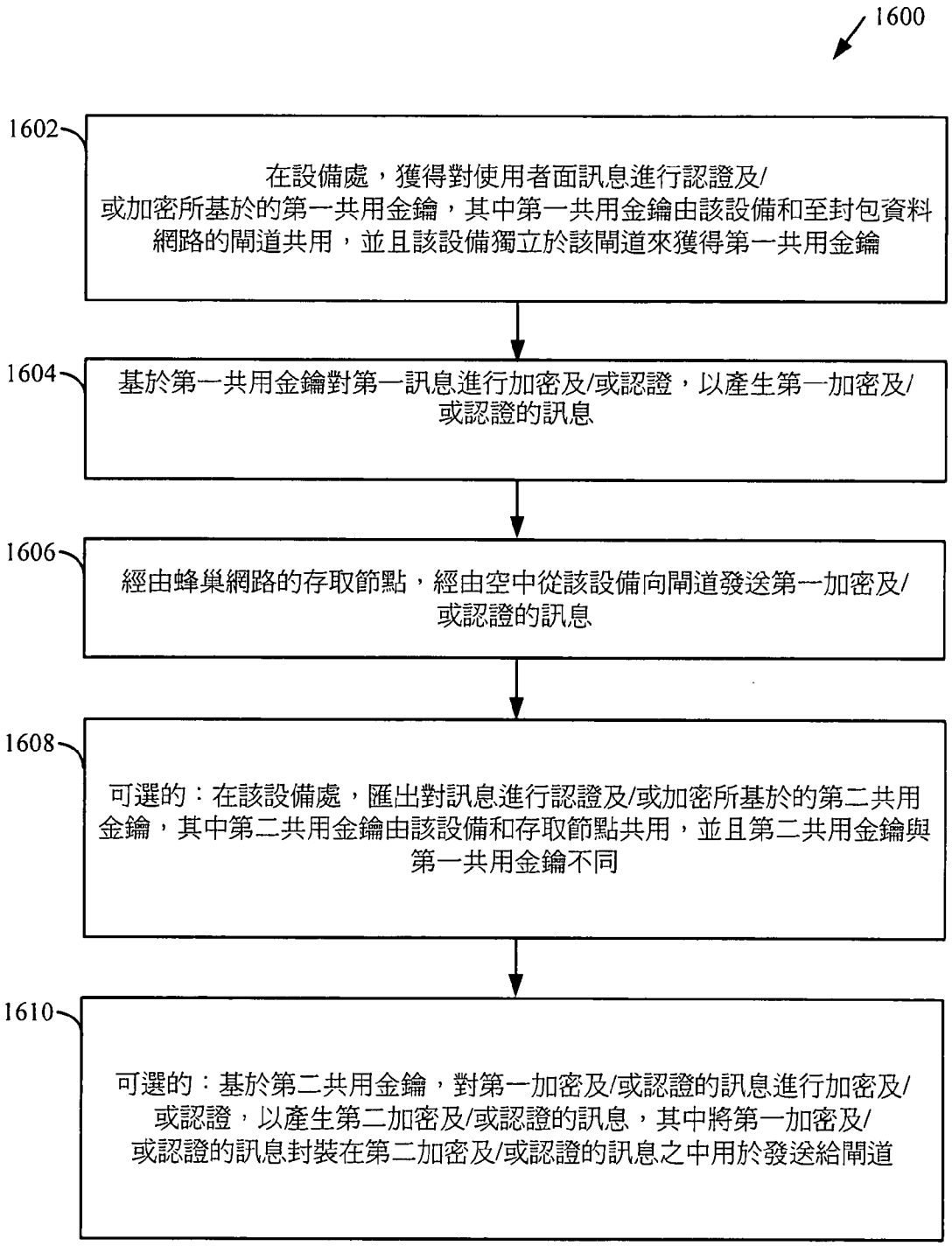
1600
1602
在設備處，獲得對使用者面訊息進行認證及/或加密所基於的第一共用金鑰，其中第一共用金鑰由該設備和至封包資料網路的閘道共用，並且該設備獨立於該閘道來獲得第一共用金鑰
1604
基於第一共用金鑰對第一訊息進行加密及/或認證，以產生第一加密及/或認證的訊息
1606
經由蜂巢網路的存取節點，經由空中從該設備向閘道發送第一加密及/或認證的訊息
1608
可選的：在該設備處，匯出對訊息進行認證及/或加密所基於的第二共用金鑰，其中第二共用金鑰由該設備和存取節點共用，並且第二共用金鑰與第一共用金鑰不同
1610
可選的：基於第二共用金鑰，對第一加密及/或認證的訊息進行加密及/或認證，以產生第二加密及/或認證的訊息，其中將第一加密及/或認證的訊息封裝在第二加密及/或認證的訊息之中用於發送給閘道

圖16

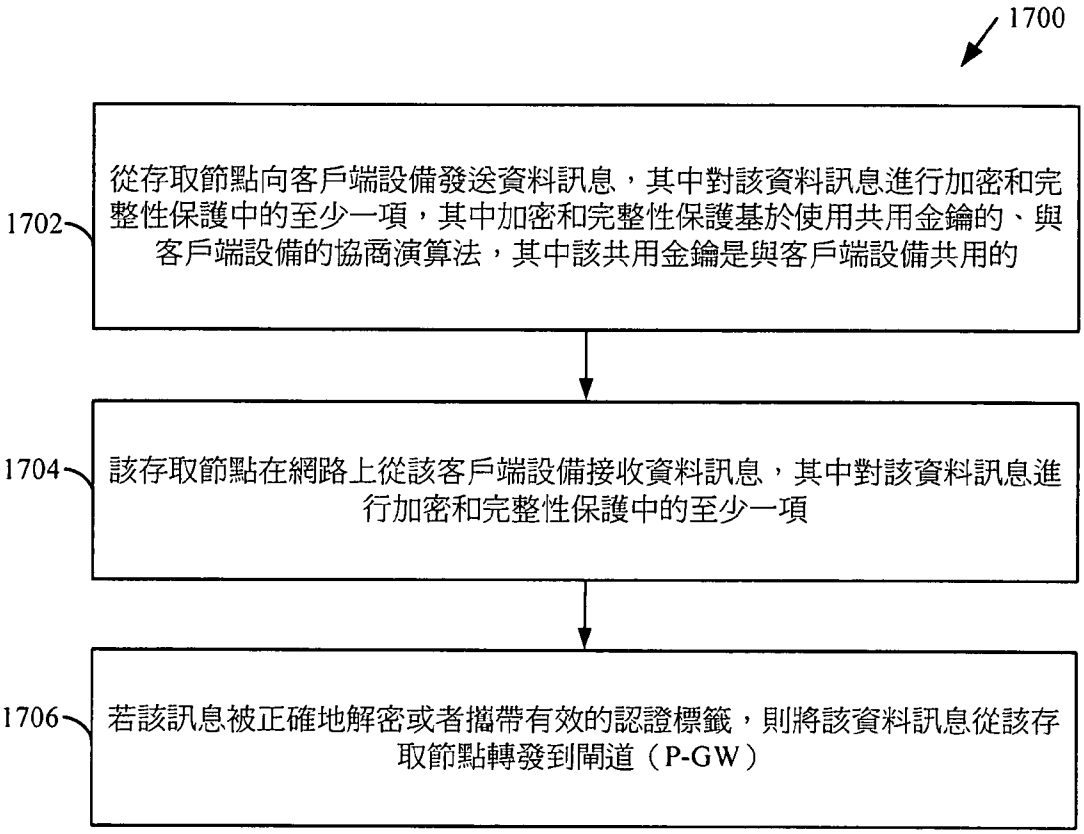
1700
1702
從存取節點向客戶端設備發送資料訊息，其中對該資料訊息進行加密和完整性保護中的至少一項，其中加密和完整性保護基於使用共用金鑰的、與客戶端設備的協商演算法，其中該共用金鑰是與客戶端設備共用的
1704
該存取節點在網路上從該客戶端設備接收資料訊息，其中對該資料訊息進行加密和完整性保護中的至少一項
1706
若該訊息被正確地解密或者攜帶有效的認證標籤，則將該資料訊息從該存取節點轉發到閘道（P-GW）

圖17

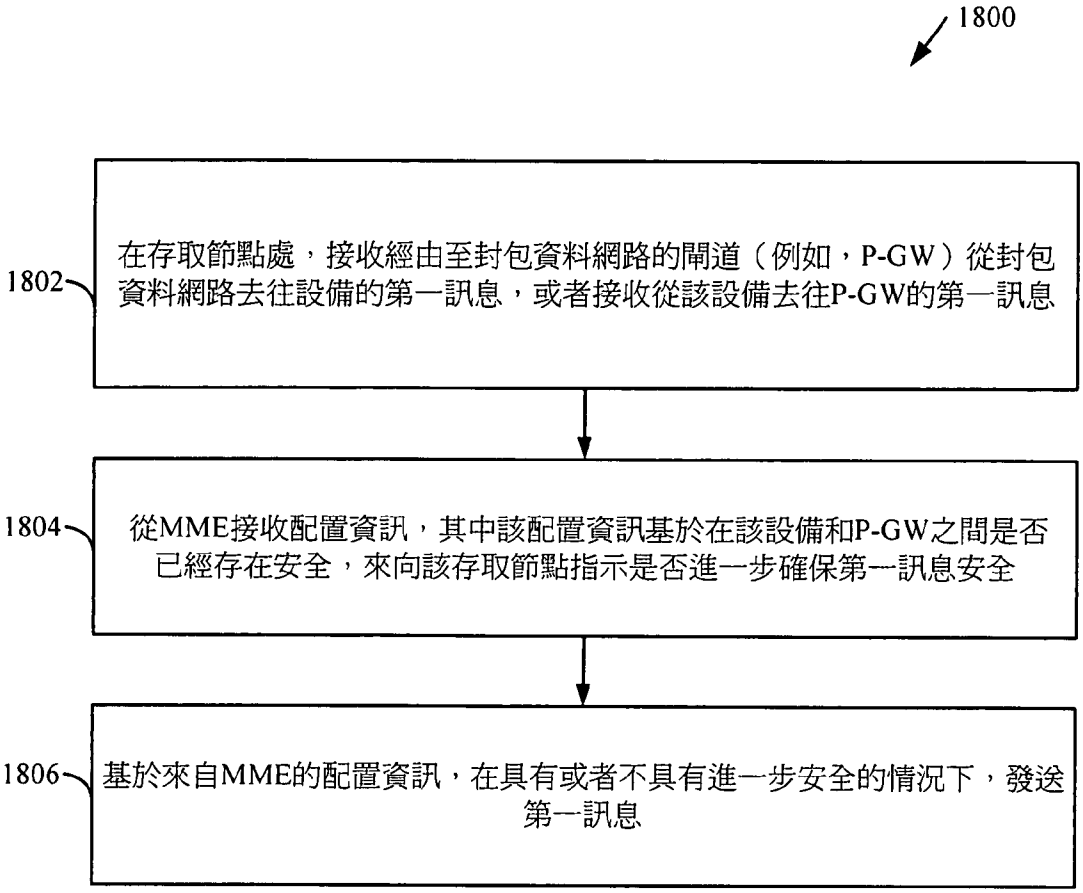
1800
1802
在存取節點處，接收經由至封包資料網路的閘道（例如，P-GW）從封包資料網路去往設備的第一訊息，或者接收從該設備去往P-GW的第一訊息
1804
從MME接收配置資訊，其中該配置資訊基於在該設備和P-GW之間是否已經存在安全，來向該存取節點指示是否進一步確保第一訊息安全
1806
基於來自MME的配置資訊，在具有或者不具有進一步安全的情況下，發送第一訊息

圖18

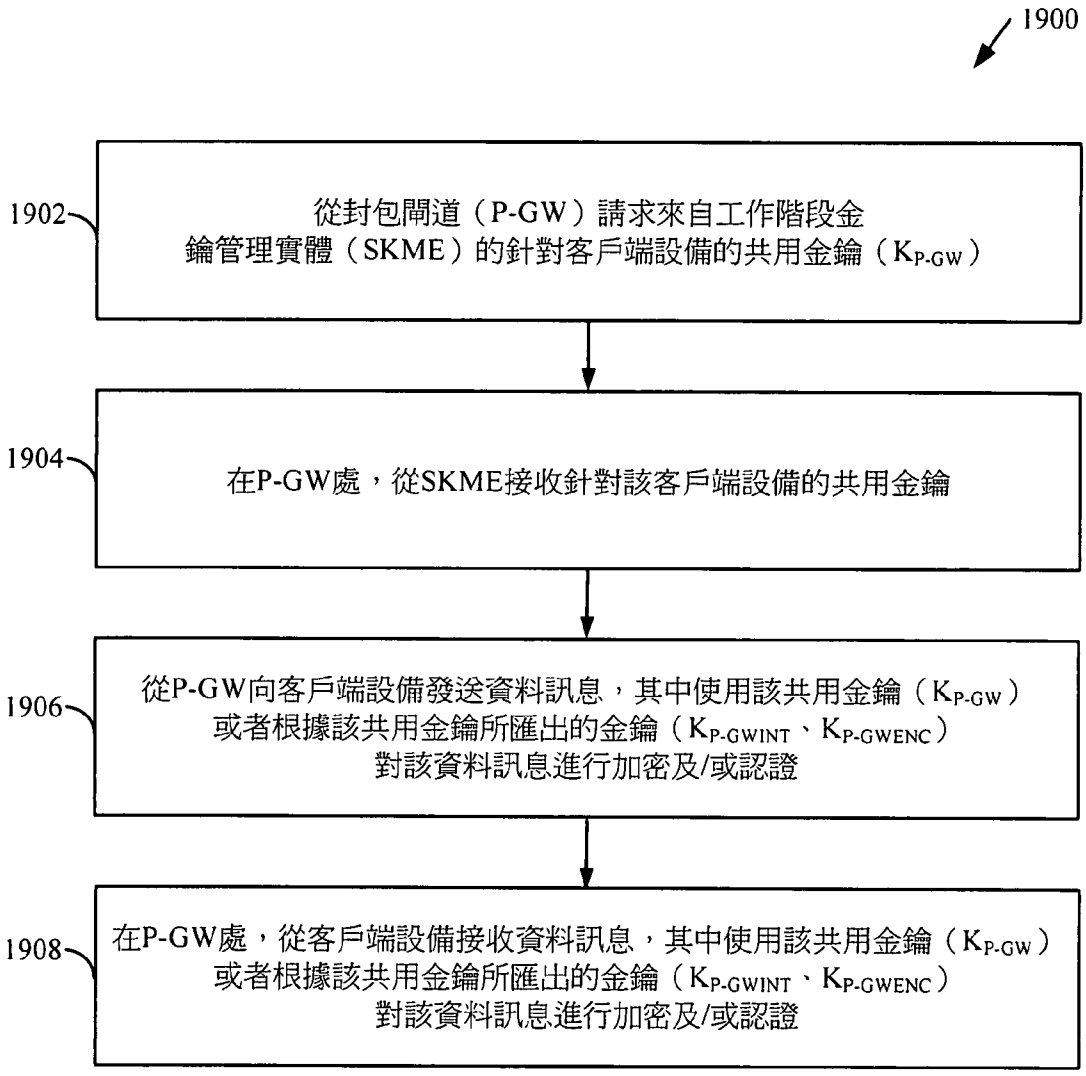
1900
1902
從封包閘道（P-GW）請求來自工作階段金鑰管理實體（SKME）的針對客戶端設備的共用金鑰（$K_{P\text{-}GW}$）
1904
在P-GW處，從SKME接收針對該客戶端設備的共用金鑰
1906
從P-GW向客戶端設備發送資料訊息，其中使用該共用金鑰（$K_{P\text{-}GW}$）或者根據該共用金鑰所匯出的金鑰（$K_{P\text{-}GWINT}$、$K_{P\text{-}GWENC}$）對該資料訊息進行加密及/或認證
1908
在P-GW處，從客戶端設備接收資料訊息，其中使用該共用金鑰（$K_{P\text{-}GW}$）或者根據該共用金鑰所匯出的金鑰（$K_{P\text{-}GWINT}$、$K_{P\text{-}GWENC}$）對該資料訊息進行加密及/或認證

圖19

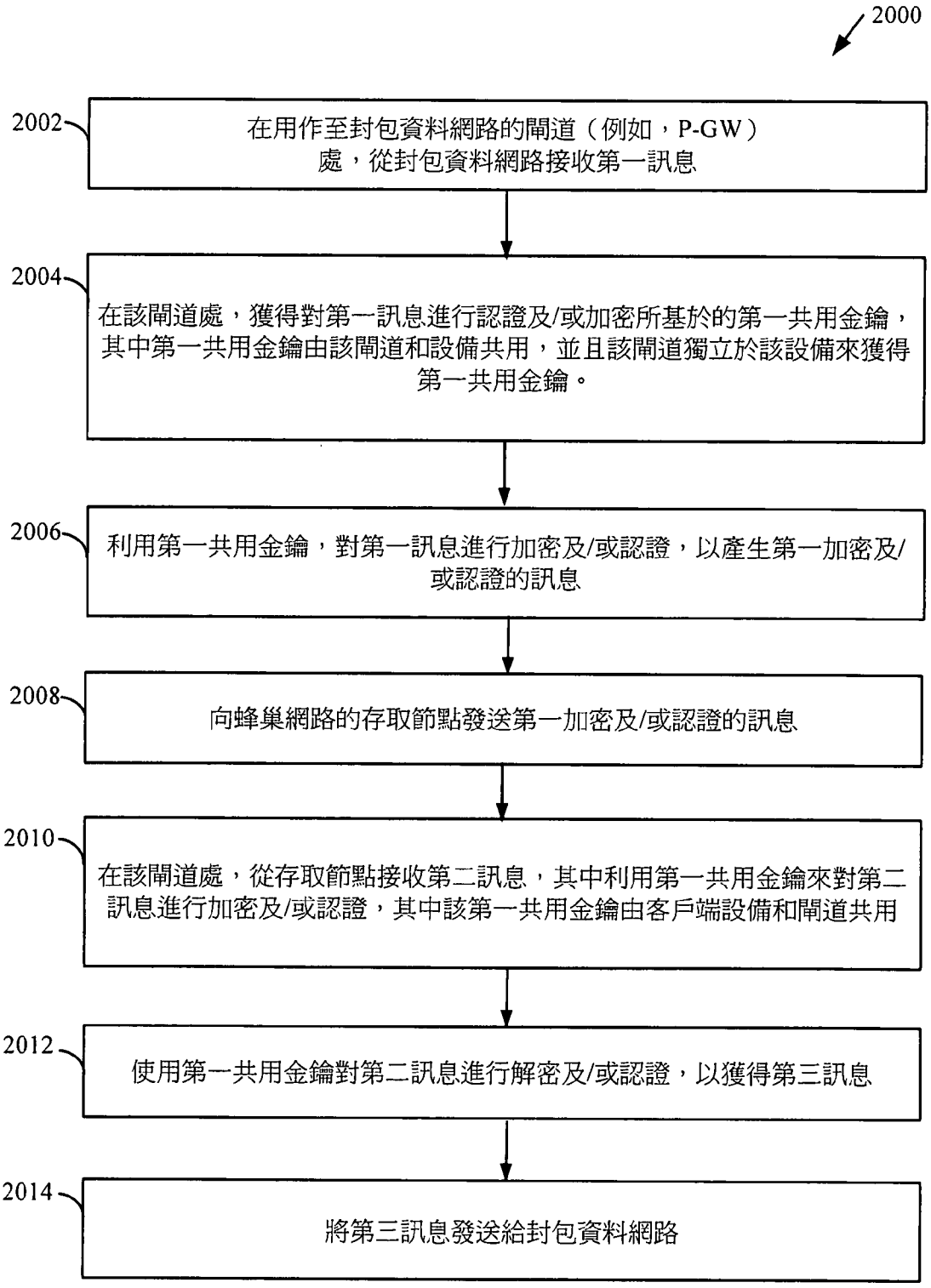
2000
2002
在用作至封包資料網路的閘道（例如，P-GW）處，從封包資料網路接收第一訊息
2004
在該閘道處，獲得對第一訊息進行認證及/或加密所基於的第一共用金鑰，其中第一共用金鑰由該閘道和設備共用，並且該閘道獨立於該設備來獲得第一共用金鑰。
2006
利用第一共用金鑰，對第一訊息進行加密及/或認證，以產生第一加密及/或認證的訊息
2008
向蜂巢網路的存取節點發送第一加密及/或認證的訊息
2010
在該閘道處，從存取節點接收第二訊息，其中利用第一共用金鑰來對第二訊息進行加密及/或認證，其中該第一共用金鑰由客戶端設備和閘道共用
2012
使用第一共用金鑰對第二訊息進行解密及/或認證，以獲得第三訊息
2014
將第三訊息發送給封包資料網路

圖20

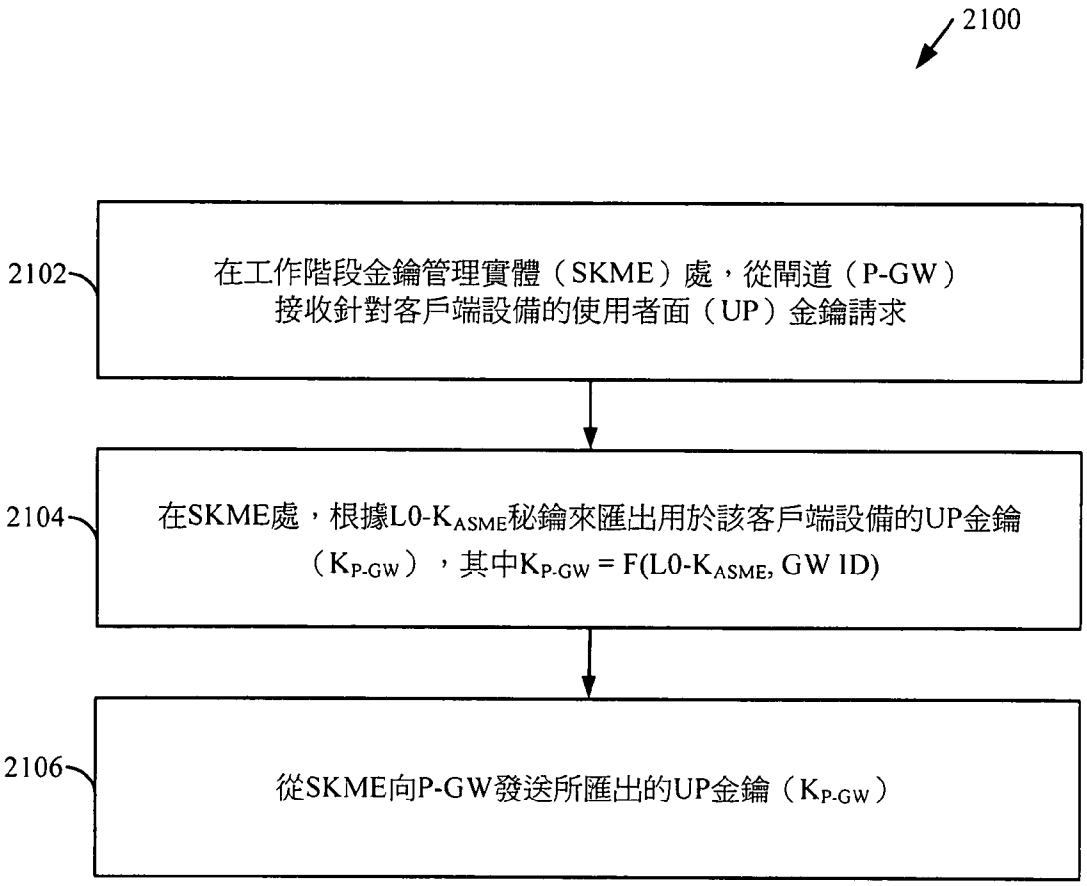
2100
2102
在工作階段金鑰管理實體（SKME）處，從閘道（P-GW）接收針對客戶端設備的使用者面（UP）金鑰請求
2104
在SKME處，根據L0-K_{ASME}秘鑰來匯出用於該客戶端設備的UP金鑰（K_{P-GW}），其中K_{P-GW} = F(L0-K_{ASME}, GW ID)
2106
從SKME向P-GW發送所匯出的UP金鑰（K_{P-GW}）

圖21

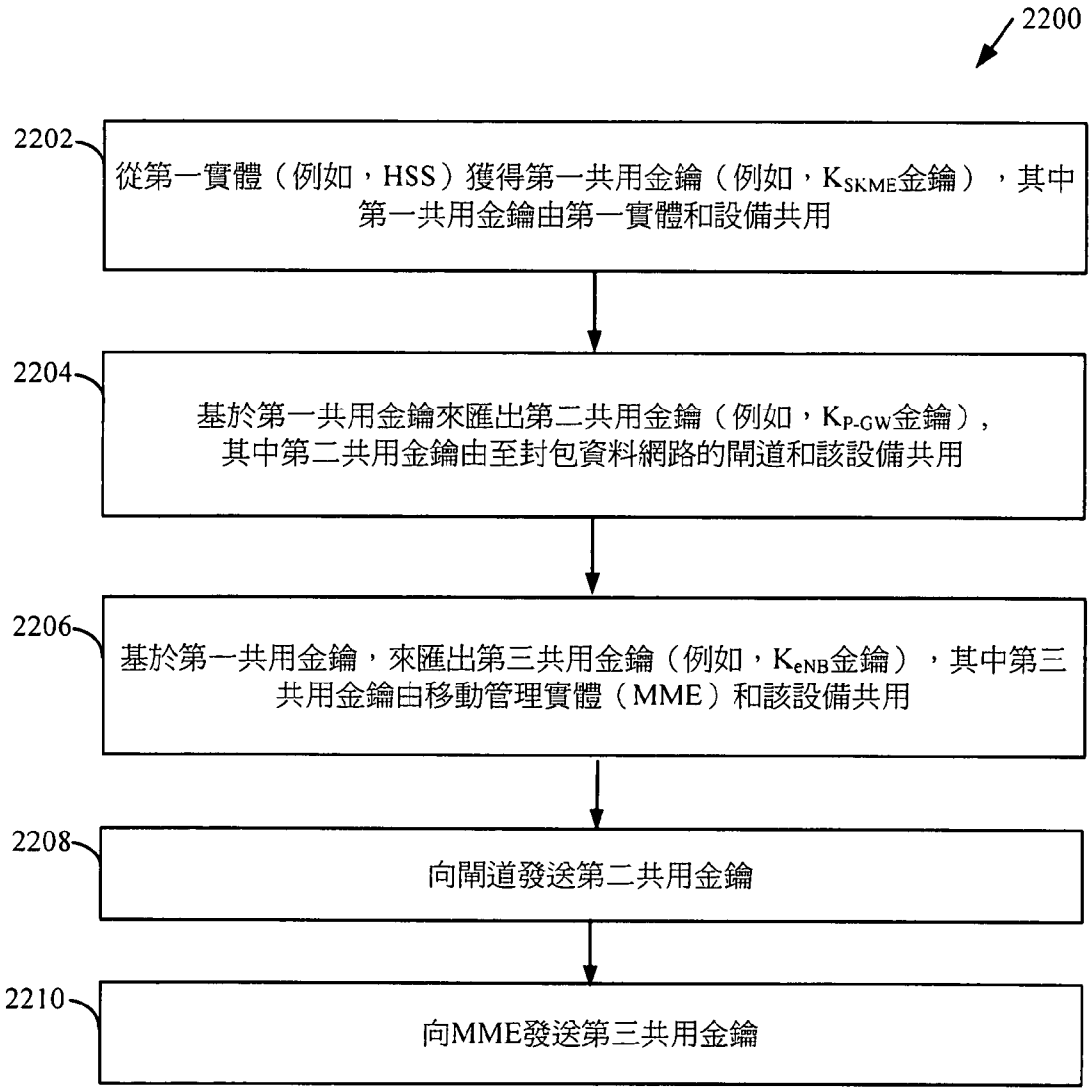
2200
2202
從第一實體（例如，HSS）獲得第一共用金鑰（例如，K_{SKME}金鑰），其中第一共用金鑰由第一實體和設備共用
2204
基於第一共用金鑰來匯出第二共用金鑰（例如，K_{P-GW}金鑰），其中第二共用金鑰由至封包資料網路的閘道和該設備共用
2206
基於第一共用金鑰，來匯出第三共用金鑰（例如，K_{eNB}金鑰），其中第三共用金鑰由移動管理實體（MME）和該設備共用
2208
向閘道發送第二共用金鑰
2210
向MME發送第三共用金鑰

圖22

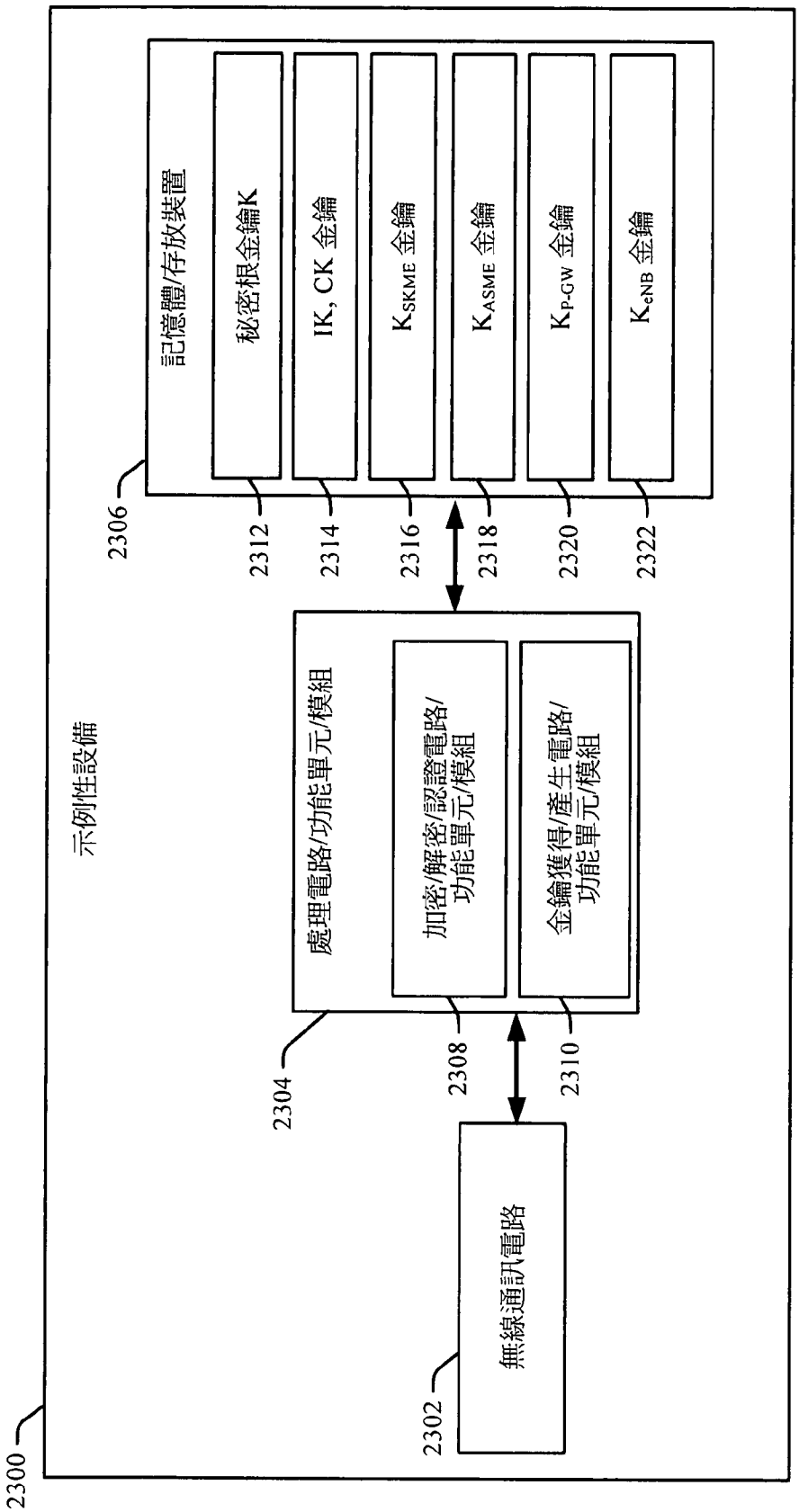
2300
示例性設備
2302
無線通訊電路
2304
處理電路/功能單元/模組
2306
記憶體/存放裝置
2308
加密/解密/認證電路/功能單元/模組
2310
金鑰獲得/產生電路/功能單元/模組
2312
秘密根金鑰K
2314
IK, CK 金鑰
2316
K_{SKME} 金鑰
2318
K_{ASME} 金鑰
2320
$K_{P\text{-}GW}$ 金鑰
2322
K_{eNB} 金鑰

圖23

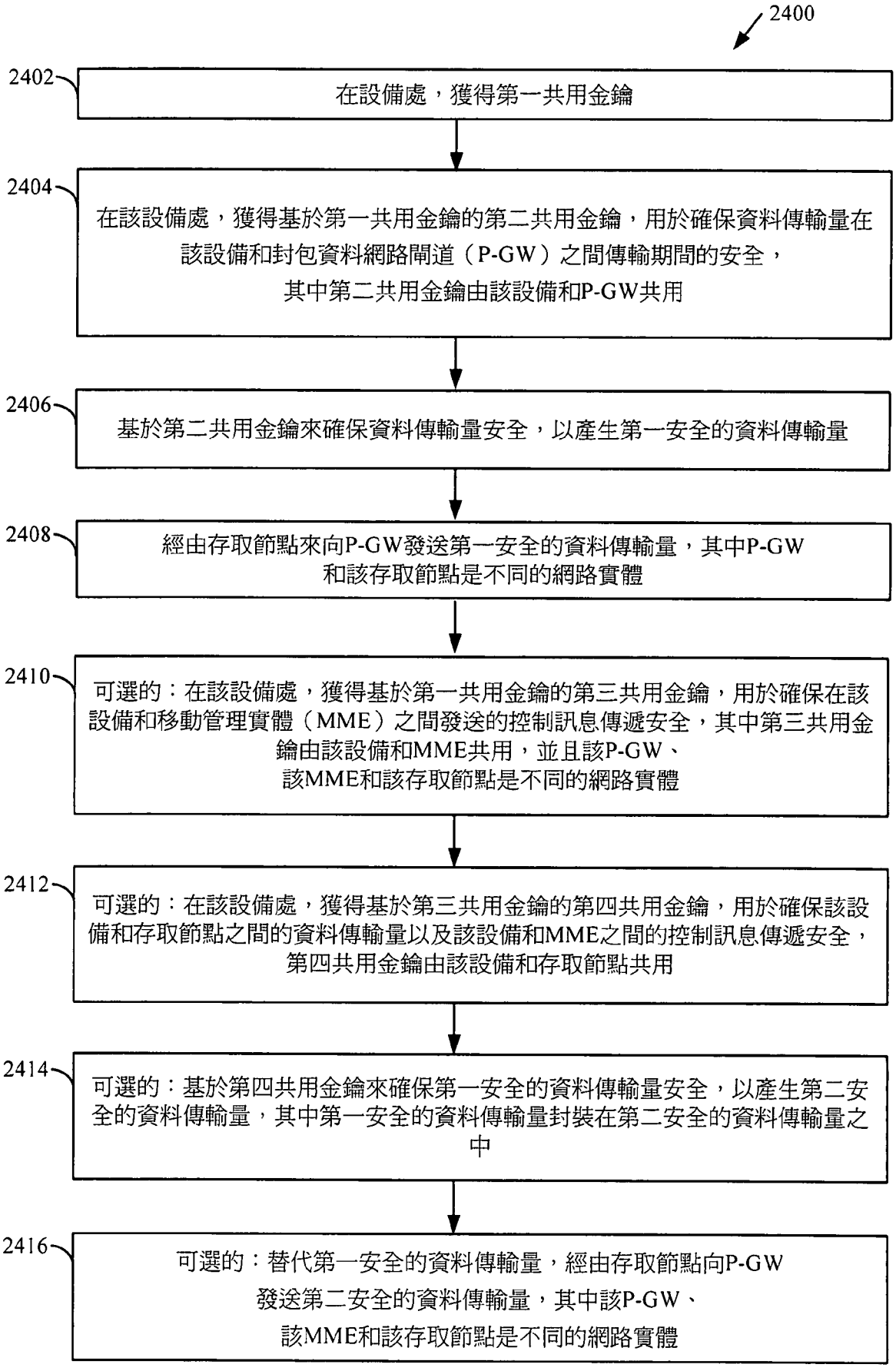
2400
2402
在設備處，獲得第一共用金鑰
2404
在該設備處，獲得基於第一共用金鑰的第二共用金鑰，用於確保資料傳輸量在該設備和封包資料網路閘道（P-GW）之間傳輸期間的安全，其中第二共用金鑰由該設備和P-GW共用
2406
基於第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量
2408
經由存取節點來向P-GW發送第一安全的資料傳輸量，其中P-GW和該存取節點是不同的網路實體
2410
可選的：在該設備處，獲得基於第一共用金鑰的第三共用金鑰，用於確保在該設備和移動管理實體（MME）之間發送的控制訊息傳遞安全，其中第三共用金鑰由該設備和MME共用，並且該P-GW、該MME和該存取節點是不同的網路實體
2412
可選的：在該設備處，獲得基於第三共用金鑰的第四共用金鑰，用於確保該設備和存取節點之間的資料傳輸量以及該設備和MME之間的控制訊息傳遞安全，第四共用金鑰由該設備和存取節點共用
2414
可選的：基於第四共用金鑰來確保第一安全的資料傳輸量安全，以產生第二安全的資料傳輸量，其中第一安全的資料傳輸量封裝在第二安全的資料傳輸量之中
2416
可選的：替代第一安全的資料傳輸量，經由存取節點向P-GW發送第二安全的資料傳輸量，其中該P-GW、該MME和該存取節點是不同的網路實體

圖24

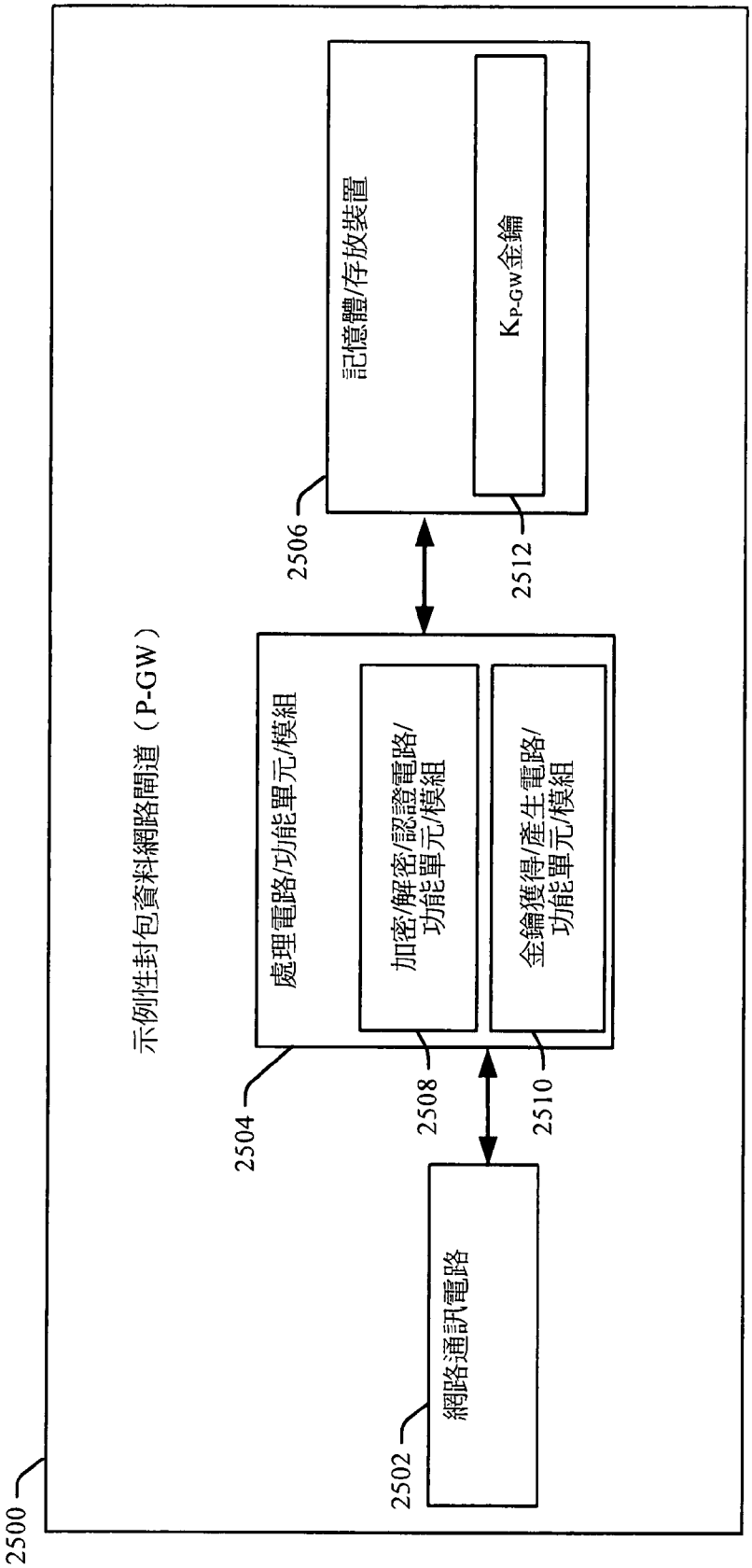
2500
示例性封包資料網路閘道（P-GW）
2502
網路通訊電路
2504
處理電路/功能單元/模組
2508
加密/解密/認證電路/
功能單元/模組
2510
金鑰獲得/產生電路/
功能單元/模組
2506
記憶體/存放裝置
2512
$K_{P\text{-}GW}$金鑰

圖25

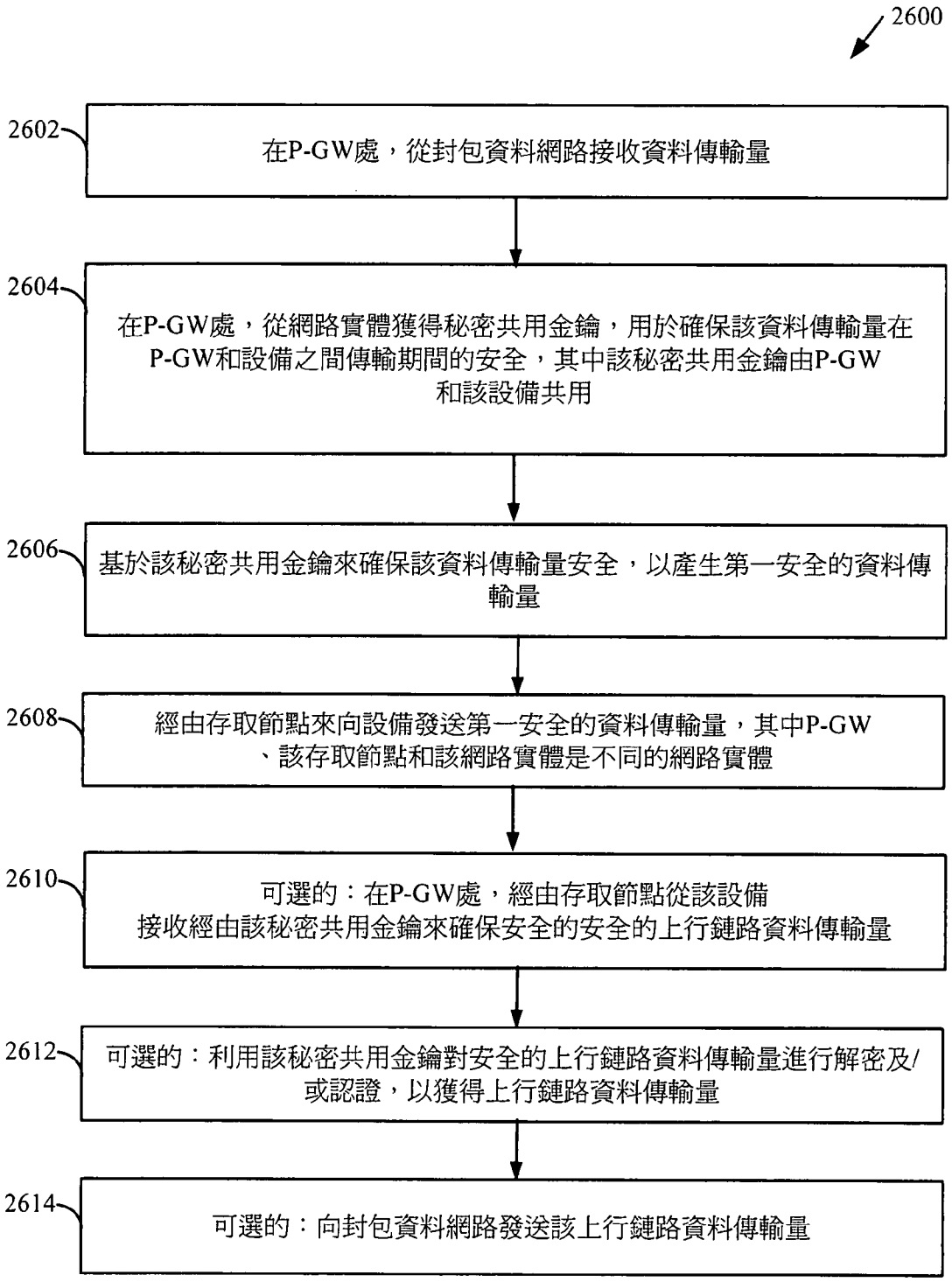
2600
2602
在P-GW處，從封包資料網路接收資料傳輸量
2604
在P-GW處，從網路實體獲得秘密共用金鑰，用於確保該資料傳輸量在P-GW和設備之間傳輸期間的安全，其中該秘密共用金鑰由P-GW和該設備共用
2606
基於該秘密共用金鑰來確保該資料傳輸量安全，以產生第一安全的資料傳輸量
2608
經由存取節點來向設備發送第一安全的資料傳輸量，其中P-GW、該存取節點和該網路實體是不同的網路實體
2610
可選的：在P-GW處，經由存取節點從該設備接收經由該秘密共用金鑰來確保安全的安全的上行鏈路資料傳輸量
2612
可選的：利用該秘密共用金鑰對安全的上行鏈路資料傳輸量進行解密及/或認證，以獲得上行鏈路資料傳輸量
2614
可選的：向封包資料網路發送該上行鏈路資料傳輸量

圖26

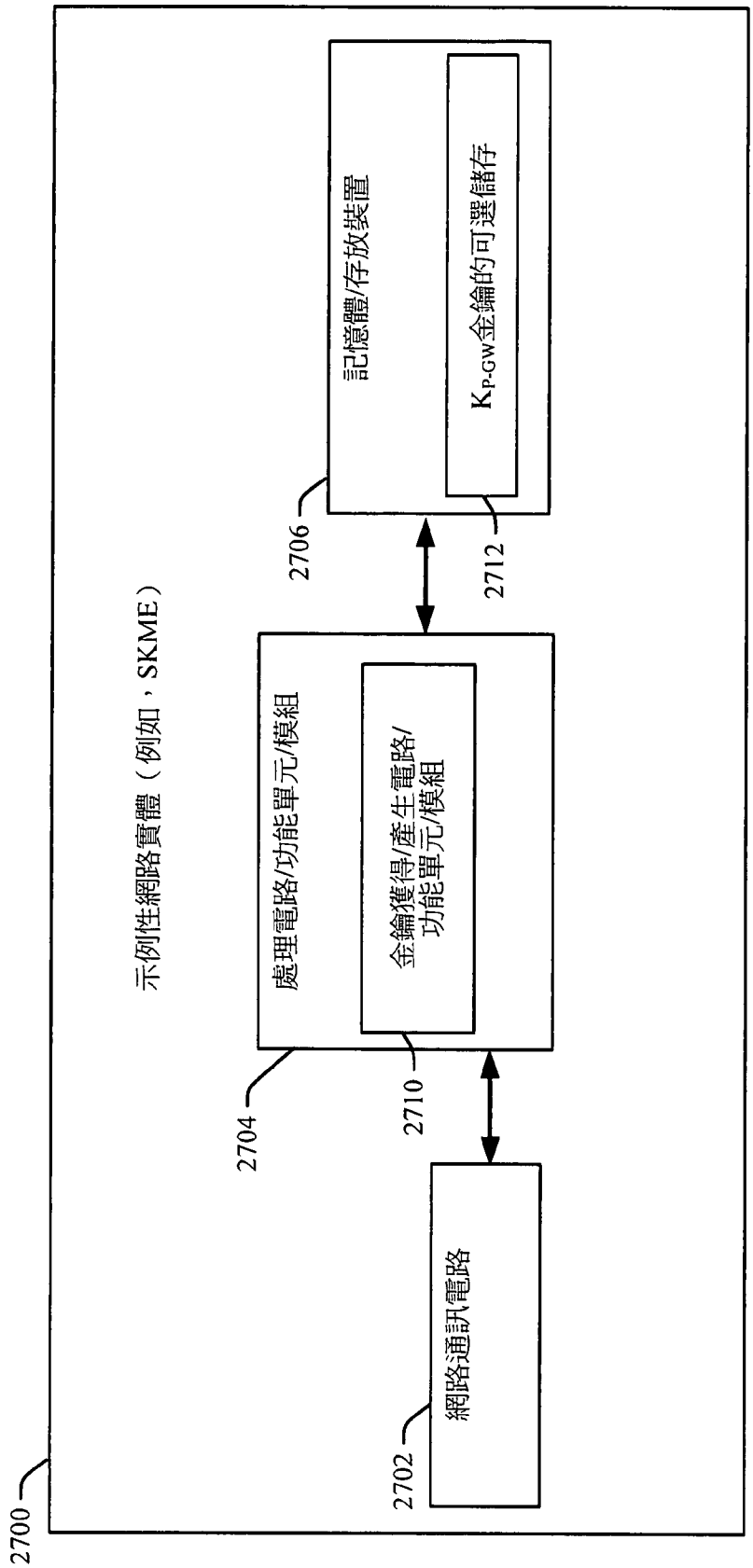
2700
示例性網路實體（例如，SKME）
2702
網路通訊電路
2704
處理電路/功能單元/模組
2710
金鑰獲得/產生電路/
功能單元/模組
2706
記憶體/存放裝置
2712
$K_{P\text{-}GW}$金鑰的可選儲存

圖27

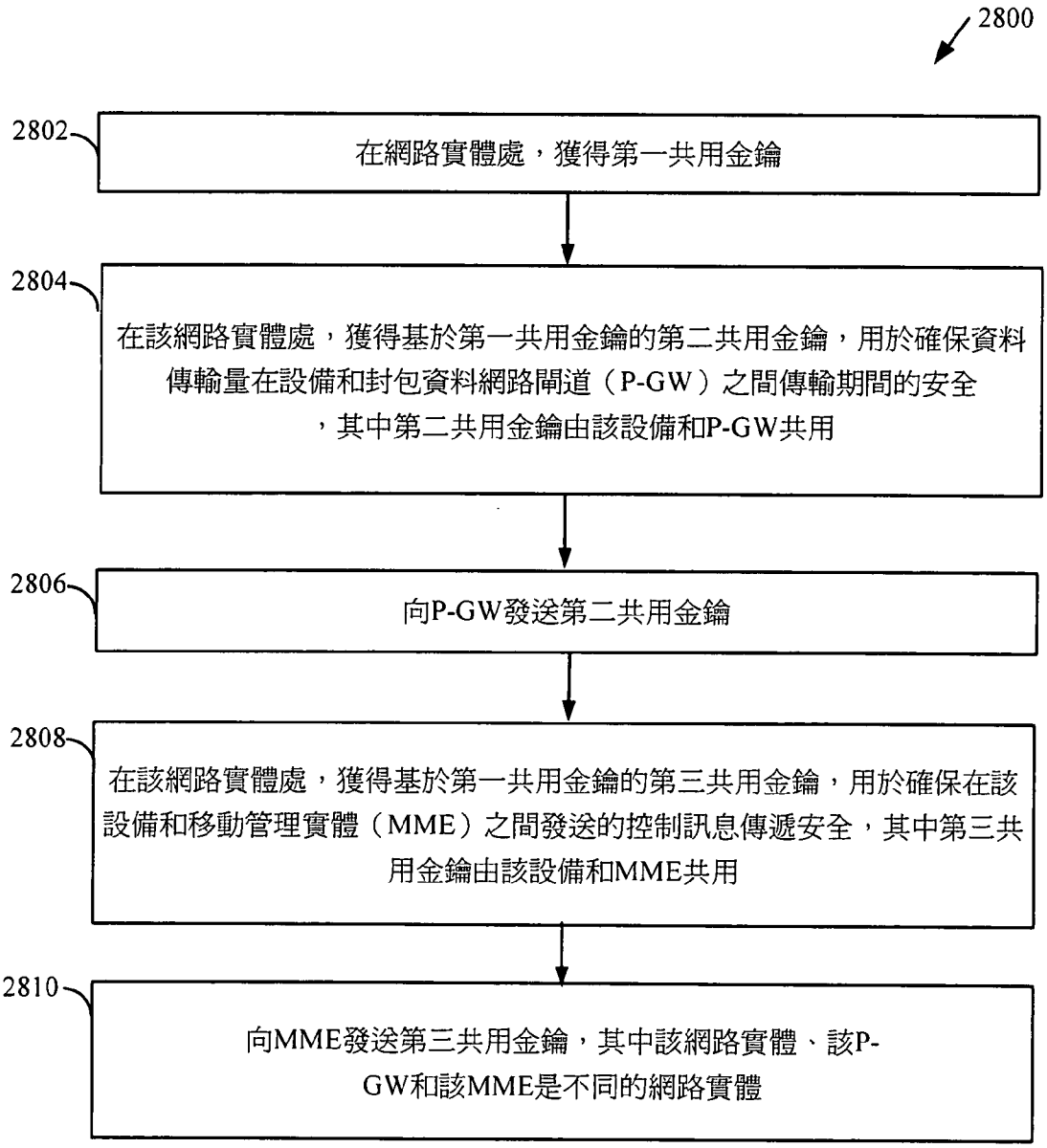
2800
2802
在網路實體處，獲得第一共用金鑰
2804
在該網路實體處，獲得基於第一共用金鑰的第二共用金鑰，用於確保資料傳輸量在設備和封包資料網路閘道（P-GW）之間傳輸期間的安全，其中第二共用金鑰由該設備和P-GW共用
2806
向P-GW發送第二共用金鑰
2808
在該網路實體處，獲得基於第一共用金鑰的第三共用金鑰，用於確保在該設備和移動管理實體（MME）之間發送的控制訊息傳遞安全，其中第三共用金鑰由該設備和MME共用
2810
向MME發送第三共用金鑰，其中該網路實體、該P-GW和該MME是不同的網路實體

圖28

申請專利範圍

1. 一種在一設備處操作的方法，包括以下步驟：

在該設備處，獲得一第一共用金鑰，其中該第一共用金鑰是由該設備和一核心網路實體共用的，其中該第一共用金鑰是基於一秘密共用金鑰獲得的，該秘密共用金鑰不是經由空中發送的；

在該設備處，獲得基於該第一共用金鑰的一第二共用金鑰，以確保資料傳輸量在該設備和一封包資料網路閘道（P-GW）之間傳輸期間的安全，其中該第二共用金鑰是由該設備和該P-GW共用的；

基於該第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量；及

經由一存取節點來向該P-GW發送該第一安全的資料傳輸量，其中該核心網路實體、該P-GW和該存取節點是不同的網路實體。

2. 根據請求項1之方法，其中該第一共用金鑰是該P-GW不知道的。

3. 根據請求項1之方法，其中該第一共用金鑰和該第二共用金鑰是在該設備處本端地匯出的，並且不是發送給該設備的。

4. 根據請求項1之方法，其中該第二共用金鑰確保使用者面

通訊的至少一些層安全，而一不同的金鑰確保控制面通訊安全。

5. 根據請求項1之方法，亦包括以下步驟：

在該設備處，獲得基於該第一共用金鑰的一第三共用金鑰，以確保在該設備和一行動性管理實體（MME）之間發送的控制訊息傳遞安全，其中該第三共用金鑰是由該設備和該MME共用的，並且該P-GW、該MME和該存取節點是不同的網路實體。

6. 根據請求項5之方法，亦包括以下步驟：

在該設備處，獲得基於該第三共用金鑰的一第四共用金鑰，以確保該設備和該存取節點之間的資料傳輸量以及該設備和該MME之間的控制訊息傳遞安全，其中該第四共用金鑰是由該設備和該存取節點共用的；

基於該第四共用金鑰來確保該第一安全的資料傳輸量安全，以產生一第二安全的資料傳輸量，其中該第一安全的資料傳輸量是封裝在該第二安全的資料傳輸量之中的；及

替代該第一安全的資料傳輸量，經由該存取節點向該P-GW發送該第二安全的資料傳輸量，其中該P-GW、該MME和該存取節點是不同的網路實體。

7. 根據請求項6之方法，其中該第二共用金鑰在一使用者面的一網際網路協定（IP）層中，保護該第二安全的資料傳輸

量。

8. 根據請求項6之方法，其中該第四共用金鑰在一使用者面的一封包資料會聚協定（PDCP）層中，保護該第二安全的資料傳輸量。

9. 根據請求項6之方法，其中該第四共用金鑰在一使用者面的某些層上保護傳輸量的某些傳輸，而該第二共用金鑰用於在該使用者面的其他層上保護傳輸量的其他傳輸。

10. 根據請求項1之方法，其中該核心網路實體從一歸屬用戶伺服器（HSS）獲得該第一共用金鑰。

11. 根據請求項1之方法，其中該設備獨立於該P-GW來獲得該第二共用金鑰。

12. 根據請求項1之方法，其中獲得該第二共用金鑰亦包括以下步驟：

在該設備處，根據該第一共用金鑰和一封包資料網路閘道辨識符（GW ID）來匯出該第二共用金鑰。

13. 根據請求項1之方法，其中資料傳輸量與控制訊息傳遞不同。

14. 根據請求項1之方法，其中資料傳輸量是在一使用者面上發送的，並且控制訊息傳遞是在一控制面上發送的，其中該使用者面和該控制面是不同的傳輸路徑。

15. 根據請求項1之方法，其中確保該資料傳輸量安全包括以下步驟：基於該第二共用金鑰，對該資料傳輸量進行加密。

16. 根據請求項1之方法，其中確保該資料傳輸量安全包括以下步驟：包含基於該第二共用金鑰的一認證簽名。

17. 根據請求項1之方法，亦包括以下步驟：

經由該存取節點來從該P-GW接收第三安全的資料傳輸量，其中該第三安全的資料傳輸量是基於該第二共用金鑰來確保安全的；及

基於該第二共用金鑰對該第三安全的資料傳輸量進行解密及/或認證，以產生不安全的資料傳輸量。

18. 一種用於無線通訊的設備，包括：

一無線通訊電路，其被配置為與一蜂巢網路的一存取節點進行通訊；

耦合到該無線通訊電路的一處理電路，該處理電路被配置為：

獲得一第一共用金鑰，其中該第一共用金鑰是由該設備和一核心網路實體共用的，其中該第一共用金鑰是基於一秘

密共用金鑰獲得的，該秘密共用金鑰不是經由空中發送的；

獲得基於該第一共用金鑰的一第二共用金鑰，以確保使用者面資料傳輸量在該設備和一封包資料網路閘道（P-GW）之間傳輸期間的安全，其中該第二共用金鑰是由該設備和該P-GW共用的；

基於該第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量；及

經由該存取節點來向該P-GW發送該第一安全的資料傳輸量，其中該核心網路實體、該P-GW和該存取節點是不同的網路實體。

19. 根據請求項18之設備，其中該處理電路亦被配置為：

獲得基於該第一共用金鑰的一第三共用金鑰，以確保在該設備和一行動性管理實體（MME）之間發送的控制訊息傳遞安全，其中該第三共用金鑰是由該設備和該MME共用的，並且該P-GW、該MME和該存取節點是不同的網路實體。

20. 根據請求項19之設備，其中該處理電路亦被配置為：

獲得基於該第三共用金鑰的一第四共用金鑰，以確保該設備和該存取節點之間的資料傳輸量以及該設備和該MME之間的控制訊息傳遞安全，其中該第四共用金鑰是由該設備和該存取節點共用的；

基於該第四共用金鑰來確保該第一安全的資料傳輸量安全，以產生一第二安全的資料傳輸量，其中該第一安全的資

料傳輸量是封裝在該第二安全的資料傳輸量之中的；及

替代該第一安全的資料傳輸量，經由該存取節點向該P-GW發送該第二安全的資料傳輸量，其中該P-GW、該MME和該存取節點是不同的網路實體。

21. 一種用於無線通訊的設備，包括：

用於獲得一第一共用金鑰的單元，其中該第一共用金鑰是由該設備和一核心網路實體共用的，其中該第一共用金鑰是基於一秘密共用金鑰獲得的，該秘密共用金鑰不是經由空中發送的；

用於獲得基於該第一共用金鑰的一第二共用金鑰，以確保使用者面資料傳輸量在該設備和一封包資料網路閘道（P-GW）之間傳輸期間的安全的單元，其中該第二共用金鑰是由該設備和該P-GW共用的；

用於基於該第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量的單元；及

用於經由一存取節點來向該P-GW發送該第一安全的資料傳輸量的單元，其中該核心網路實體、該P-GW和該存取節點是不同的網路實體。

22. 根據請求項21之設備，亦包括：

用於獲得基於該第一共用金鑰的一第三共用金鑰，以確保在該設備和一行動性管理實體（MME）之間發送的控制訊息傳遞安全的單元，其中該第三共用金鑰是由該設備和該

MME共用的，並且該P-GW、該MME和該存取節點是不同的網路實體。

23. 根據請求項22之設備，亦包括：

用於獲得基於該第三共用金鑰的一第四共用金鑰，以確保該設備和該存取節點之間的資料傳輸量以及該設備和該MME之間的控制訊息傳遞安全的單元，其中該第四共用金鑰是由該設備和該存取節點共用的；

用於基於該第四共用金鑰來確保該第一安全的資料傳輸量安全，以產生一第二安全的資料傳輸量的單元，其中該第一安全的資料傳輸量是封裝在該第二安全的資料傳輸量之中的；及

用於替代該第一安全的資料傳輸量，經由該存取節點向該P-GW發送該第二安全的資料傳輸量的單元，其中該P-GW、該MME和該存取節點是不同的網路實體。

24. 一種其上儲存有一或多個指令的非臨時性機器可讀儲存媒體，其中當該一或多個指令由至少一個處理器執行時，使得該至少一個處理器用於：

獲得一第一共用金鑰，其中該第一共用金鑰是由一設備和一核心網路實體共用的，其中該第一共用金鑰是基於一秘密共用金鑰獲得的，該秘密共用金鑰不是經由空中發送的；

獲得基於該第一共用金鑰的一第二共用金鑰，以確保使用者面資料傳輸量在該設備和一封包資料網路閘道（P-GW）

之間傳輸期間的安全，其中該第二共用金鑰是由該設備和該P-GW共用的；

基於該第二共用金鑰來確保資料傳輸量安全，以產生第一安全的資料傳輸量；及

經由一存取節點來向該P-GW發送該第一安全的資料傳輸量，其中該核心網路實體、該P-GW和該存取節點是不同的網路實體。

25. 根據請求項24之非臨時性機器可讀儲存媒體，其上儲存有一或多個進一步的指令，其中當該一或多個進一步的指令由該至少一個處理器執行時，使得該至少一個處理器用於：

獲得基於該第一共用金鑰的一第三共用金鑰，以確保在該設備和一行動性管理實體（MME）之間發送的控制訊息傳遞安全，其中該第三共用金鑰是由該設備和該MME共用的，並且該P-GW、該MME和該存取節點是不同的網路實體。

26. 根據請求項25之非臨時性機器可讀儲存媒體，其上儲存有一或多個進一步的指令，其中當該一或多個進一步的指令由該至少一個處理器執行時，使得該至少一個處理器用於：

獲得基於該第三共用金鑰的一第四共用金鑰，以確保該設備和該存取節點之間的資料傳輸量以及該設備和該MME之間的控制訊息傳遞安全，其中該第四共用金鑰是由該設備和該存取節點共用的；

基於該第四共用金鑰來確保該第一安全的資料傳輸量安

全，以產生一第二安全的資料傳輸量，其中該第一安全的資料傳輸量是封裝在該第二安全的資料傳輸量之中的；及

替代該第一安全的資料傳輸量，經由該存取節點向該P-GW發送該第二安全的資料傳輸量，其中該P-GW、該MME和該存取節點是不同的網路實體。