I745415

(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 I745415 B**

(45)公告日： 中華民國 110 (2021) 年 11 月 11 日

(21)申請案號：106127922 (22)申請日： 中華民國 106 (2017) 年 08 月 17 日

(51)Int. Cl.： ***H04W12/06 (2021.01)*** ***H04L9/28 (2006.01)***

H04L29/06 (2006.01)

(30)優先權：2016/09/19 美國 62/396,791

2017/04/17 美國 15/489,670

(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)；帕拉尼古德 艾納德 PALANIGOUNDER, ANAND (IN)；伊史考特 愛德利恩愛德華 ESCOTT, ADRIAN EDWARD (GB)

(74)代理人：李世章

(56)參考文獻：

US 2008/0313455A1 US 2016/0127897A1

US 2016/0127903A1 WO 2009/087006A1

審查人員：賴文能

申請專利範圍項數：42 項 圖式數：18 共 99 頁

(54)名稱

基於擴展認證協定（EAP）程序的執行來推導蜂巢網路的安全金鑰的技術

(57)摘要

描述了用於無線通訊的技術。一種用於使用者設備（UE）處的無線通訊的方法包括經由認證器與認證伺服器執行擴展認證協定（EAP）程序。該 EAP 程序至少部分基於在 UE 和認證伺服器之間交換的一組認證憑證。該方法亦包括：作為執行 EAP 程序的一部分，推導主通信期金鑰（MSK）和擴展主通信期金鑰（EMSK），該 MSK 和該 EMSK 至少部分基於認證憑證和第一組參數；決定與認證器相關聯的網路類型；及至少部分基於所決定的網路類型，與認證器執行至少一個認證程序。該至少一個認證程序基於 MSK 或 EMSK 與所決定的網路類型的關聯。

Techniques are described for wireless communication. A method for wireless communication at a user equipment (UE) includes performing an extensible authentication protocol (EAP) procedure with an authentication server via an authenticator. The EAP procedure is based at least in part on a set of authentication credentials exchanged between the UE and the authentication server. The method also includes deriving, as part of performing the EAP procedure, a master session key (MSK) and an extended master session key (EMSK) that are based at least in part on the authentication credentials and a first set of parameters; determining a network type associated with the authenticator; and performing, based at least in part on the determined network type, at least one authentication procedure with the authenticator. The at least one authentication procedure is based on an association of the MSK or the EMSK with the determined network type.

指定代表圖：

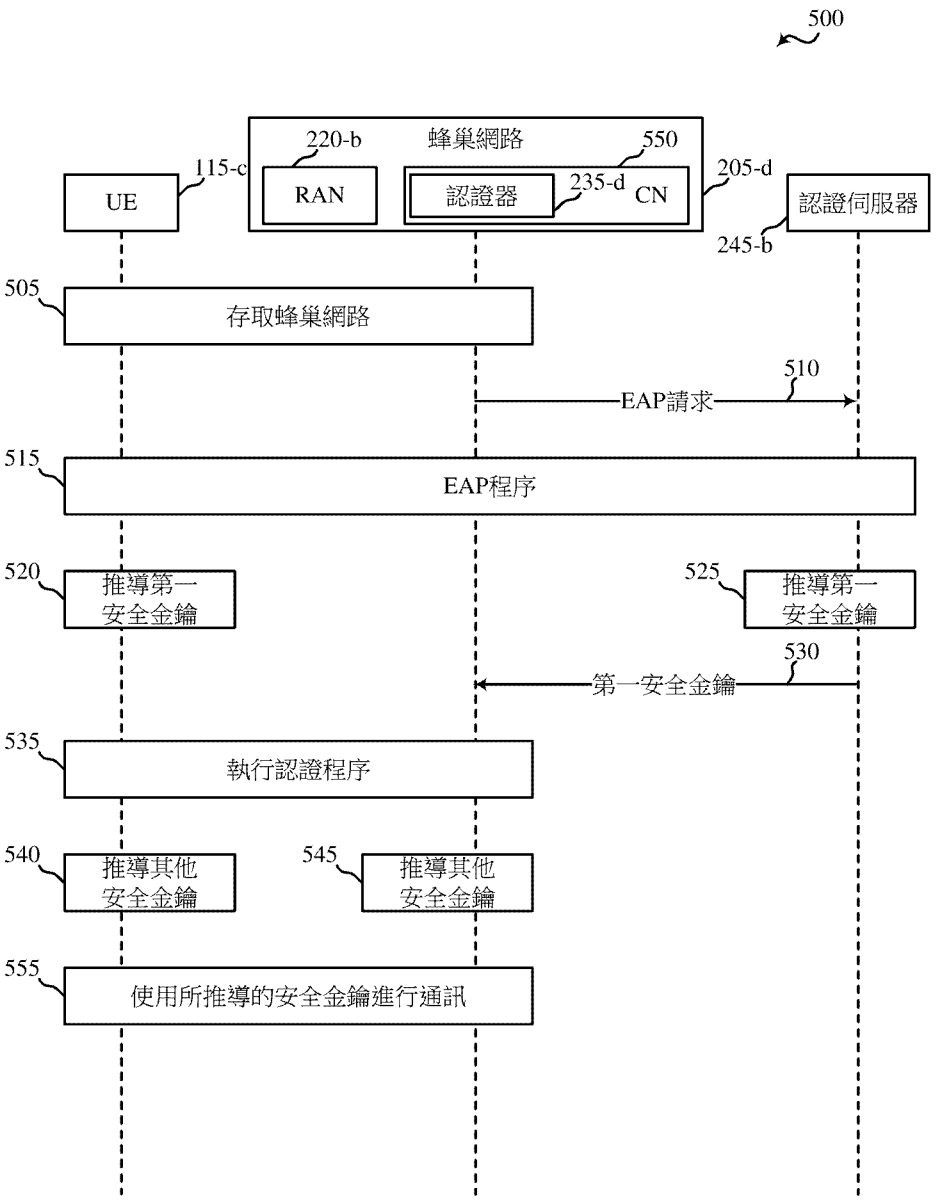

圖5

符號簡單說明：

115-c・・・UE

205-d・・・蜂巢網路

220-b・・・RAN

235-d・・・認證器

245-b・・・認證伺服器

500・・・訊息流

505・・・流程

510・・・流程

515・・・流程

520・・・流程

525・・・流程

530・・・流程

535・・・流程

540・・・流程

545・・・流程

550・・・流程

555・・・流程

專利案號：106127922

公告本

申請日：

I745415

IPC分類：

【發明摘要】

【中文發明名稱】基於擴展認證協定（EAP）程序的執行來推導蜂巢網路的安全金鑰的技術

【英文發明名稱】TECHNIQUES FOR DERIVING SECURITY KEYS FOR A CELLULAR NETWORK BASED ON PERFORMANCE OF AN EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) PROCEDURE

【中文】

描述了用於無線通訊的技術。一種用於使用者設備（UE）處的無線通訊的方法包括經由認證器與認證伺服器執行擴展認證協定（EAP）程序。該EAP程序至少部分基於在UE和認證伺服器之間交換的一組認證憑證。該方法亦包括：作為執行EAP程序的一部分，推導主通信期金鑰（MSK）和擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於認證憑證和第一組參數；決定與認證器相關聯的網路類型；及至少部分基於所決定的網路類型，與認證器執行至少一個認證程序。該至少一個認證程序基於MSK或EMSK與所決定的網路類型的關聯。

【英文】

Techniques are described for wireless communication. A method for wireless communication at a user equipment (UE) includes performing an extensible authentication protocol (EAP) procedure with an authentication server via an authenticator. The EAP procedure is based at least in part on a set of authentication credentials exchanged between the UE and the authentication server. The method also includes deriving, as part of performing the EAP procedure, a master session key

(MSK) and an extended master session key (EMSK) that are based at least in part on the authentication credentials and a first set of parameters; determining a network type associated with the authenticator; and performing, based at least in part on the determined network type, at least one authentication procedure with the authenticator. The at least one authentication procedure is based on an association of the MSK or the EMSK with the determined network type.

【指定代表圖】第（ 5 ）圖。

【代表圖之符號簡單說明】

115-c UE

205-d 蜂巢網路

220-b RAN

235-d 認證器

245-b 認證伺服器

500 訊息流

505 流程

510 流程

515 流程

520 流程

525 流程

530 流程

535 流程

540 流程

545 流程

550 流程

555 流 程

【特徵化學式】

無

【發明說明書】

【中文發明名稱】基於擴展認證協定（EAP）程序的執行來推導蜂巢網路的安全金鑰的技術

【英文發明名稱】TECHNIQUES FOR DERIVING SECURITY KEYS FOR A CELLULAR NETWORK BASED ON PERFORMANCE OF AN EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) PROCEDURE

【技術領域】

【0001】 本專利申請案主張享有由LEE等人於2017年4月17日提出申請的、名稱為「TECHNIQUES FOR DERIVING SECURITY KEYS FOR A CELLULAR NETWORK BASED ON PERFORMANCE OF AN EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) PROCEDURE」的美國專利申請案第15/489,670號，以及由LEE等人於2016年9月19日提出申請的、名稱為「TECHNIQUES FOR DERIVING SECURITY KEYS FOR A CELLULAR NETWORK BASED ON PERFORMANCE OF AN EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) PROCEDURE」的美國臨時專利申請案第62/396,791號的優先權，上述每個申請案被轉讓給本案的受讓人。

【0002】 本案內容例如係關於無線通訊系統，更具體地說，係關於用於基於擴展認證協定（EAP）程序的執行來推導蜂巢網路的安全金鑰的技術。

【先前技術】

【0003】 無線通訊系統被廣泛地部署以提供各種類型的通訊內容，例如語音、視訊、封包資料、訊息傳遞、廣播等等。這些系統可以是能夠經由共享可用系統資源（例如，時間、頻率和功率）來支援與多個使用者通訊的多工存取系統。這些多工存取系統的實例包括分碼多工存取（CDMA）系統、分時多工存取（TDMA）系統、分頻多工存取（FDMA）系統和正交分頻多工存取（OFDMA）系統。

【0004】 在一些實例中，無線多工存取通訊系統可以是或包括蜂巢網路。蜂巢網路可以包括多個網路存取設備，每個網路存取設備同時支援多個通訊設備（或者公知為使用者設備（UE））的通訊。在第四代（4G）網路、長期進化（LTE）網路或高級LTE（LTE-A）網路中，網路存取設備可以採取增強型節點B（eNB）的形式，每個eNB包括一組一或多個基地台的集合。在第五代（5G或下一代（NextGen））網路中，網路存取設備可以在與網路存取設備控制器（例如，存取節點控制器（ANC））的通訊中採取智慧無線電頭端（SRH）或gNodeB（gNB）的形式，其中與網路存取設備控制器通訊的一或多個網路存取設備的集合定義網路節點。eNB、gNB或網路節點可以在下行鏈路通道（例如，用於從eNB、gNB或網路節點到該UE的傳輸）和上行鏈路通道（例如，用於從UE到eNB、gNB或網路節點的傳輸）上與一組UE通訊。

【0005】 當UE存取蜂巢網路時，UE或蜂巢網路可以發起使UE能夠向蜂巢網路的認證器認證它自己，並且使認證器能夠向UE認證蜂巢網路的一或多個程序。在一些實例中，認證程序可以包括EAP程序，其中具有與認證認證器的安全連接的認證伺服器對UE進行認證；使UE能夠推導一或多個安全金鑰用於向認證器認證它自己；及推導在安全連接上發送給認證器的一或多個安全金鑰，以便使認證器能夠向UE認證蜂巢網路。

【發明內容】

【0006】 在一些情況下，蜂巢網路可以允許經由不同類型的存取網路存取該蜂巢網路，其中的一些存取網路可能或多或少容易受到攻擊，並且其中一些可能或多或少處於該蜂巢網路的服務供應商的控制下。例如，蜂巢網路可以允許經由蜂巢存取網路或非蜂巢存取網路（例如，無線區域網路（WLAN））存取該蜂巢網路。當與不同存取網路相關聯的認證器支援相同的EAP程序時，作為經由與蜂巢存取網路相關聯的認證器或與非蜂巢存取網路相關聯的認證器執行該EAP程序的結果，可以推導相同的主通信期金鑰（MSK）。因此，該相同的MSK或從其推導的相同安全金鑰可以被提供給與該蜂巢存取網路相關聯的認證器或與該非蜂巢存取網路相關聯的認證器。若非蜂巢存取網路被攻擊者損害，則該攻擊者對MSK或從其推導的安全金鑰的存取可以使該攻擊者能夠使用該非蜂巢存取網路向UE冒充該蜂巢存取網路，這會損害該UE及/

或運行在該UE上的應用的安全性。本案內容中描述的技術經由決定與認證器相關聯的網路類型和基於與該網路類型相關聯的EAP通信期金鑰（例如，MSK或擴展MSK（EMSK））的類型與該認證器執行認證程序（或推導該認證器的安全金鑰）來幫助減輕這種威脅。在一些實例中，當認證器與非蜂巢存取網路相關聯時，可以使用MSK，並且當認證器與蜂巢存取網路相關聯時可以使用EMSK。

【0007】 在一個實例中，描述了一種用於UE處的無線通訊的方法。該方法可以包括經由認證器與認證伺服器執行EAP程序。該EAP程序至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證。該方法亦可以包括作為執行該EAP程序的一部分，推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；及至少部分基於所決定的網路類型與該認證器執行至少一個認證程序。該至少一個認證程序可以基於該MSK或該EMSK與所決定的網路類型的關聯。

【0008】 在一個實例中，描述了一種用於UE處的無線通訊的裝置。該裝置可以包括用於經由認證器與認證伺服器執行EAP程序的單元。該EAP程序可以至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證。該裝置亦可以包括用於作為執行該EAP程序的一部分，推導MSK和EMSK的單元，該MSK和該EMSK至少部分基於

該認證憑證和第一組參數的；用於決定與該認證器相關聯的網路類型的單元；及用於與該認證器執行至少一個認證程序的單元。該至少一個認證程序可以基於該MSK或該EMSK與所決定的網路類型的關聯。

【0009】 在一個實例中，描述了一種用於UE處的無線通訊的另一裝置。該裝置可以包括處理器和與該處理器電子通訊的記憶體。該處理器和該記憶體可以被配置為經由認證器與認證伺服器執行EAP程序。該EAP程序可以至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證。該處理器和記憶體亦可以被配置為作為執行該EAP程序的一部分，推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；及至少部分基於所決定的網路類型與該認證器執行至少一個認證程序。該至少一個認證程序可以基於該MSK或該EMSK與所決定的網路類型的關聯。

【0010】 在一個實例中，描述了一種儲存用於UE處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體。該代碼可以由處理器執行以經由認證器與認證伺服器執行EAP程序。該EAP程序可以至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證。該代碼亦可以由該處理器執行以作為執行該EAP程序的一部分，推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；

及至少部分基於所決定的網路類型與該認證器執行至少一個認證程序。該至少一個認證程序可以基於該MSK或該EMSK與所決定的網路類型的關聯。

【0011】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，所決定的網路類型可以包括蜂巢網路類型，並且與該認證器執行該至少一個認證程序可以包括推導蜂巢網路的第一安全金鑰。該第一安全金鑰可以至少部分基於該EMSK和第二組參數。在一些實例中，該第二組參數可以包括：該蜂巢網路的辨識符、至少一個蜂巢網路特定參數、該UE和該蜂巢網路之間交換的至少一個參數或者它們的組合。

【0012】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，與該認證器執行該至少一個認證程序可以包括推導該蜂巢網路的網路節點的第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和第三組參數；及至少部分基於該第二安全金鑰經由該網路節點與該蜂巢網路通訊。在這些實例中的一些中，該第三組參數可以包括：該網路節點的辨識符、至少一個網路節點特定參數、該UE和該網路節點之間交換的至少一個參數或者它們的組合。

【0013】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0014】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0015】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，所決定的網路類型可以包括非蜂巢網路類型，並且與該認證器執行該至少一個認證程序可以包括推導非蜂巢網路的第一安全金鑰。該第一安全金鑰可以至少部分基於該MSK和第二組參數。

【0016】 在一個實例中，一種用於認證伺服器處的無線通訊的方法可以包括經由認證器與UE執行EAP程序。該EAP程序可以至少部分基於在該認證伺服器和該UE之間交換的一組認證憑證。該方法亦可以包括作為執行該EAP程序的一部分，推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；至少部分基於該MSK或該EMSK與該網路類型的關聯，並且至少部分基於第二組參數推導，所決定的網路類型的安全金鑰；及經由秘密頻道將該安全金鑰發送給該認證器。

【0017】 在一個實例中，描述了一種用於認證伺服器處的無線通訊的裝置。該裝置可以包括用於經由認證器與UE執行EAP程序的單元。該EAP程序可以至少部分基於在該認證伺服器和該UE之間交換的一組認證憑證。該裝置亦可以包括用於作為執行該EAP程序的一部分，推導

MSK和EMSK的單元，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；用於決定與該認證器相關聯的網路類型的單元；用於至少部分基於該MSK或該EMSK與該網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰的單元；及用於經由秘密頻道將該安全金鑰發送給該認證器的單元。

【0018】 在一個實例中，描述了另一種用於認證伺服器處的無線通訊的裝置。該裝置可以包括處理器和與該處理器電子通訊的記憶體。該處理器和記憶體可以被配置為經由認證器與UE執行EAP程序。該EAP程序可以至少部分基於在該認證伺服器和該UE之間交換的一組認證憑證。該處理器和該記憶體亦可以被配置為作為執行該EAP程序的一部分，推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；至少部分基於該MSK或該EMSK與該網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰；及經由秘密頻道將該安全金鑰發送給該認證器。

【0019】 在一個實例中，描述了一種儲存用於認證伺服器處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體。該代碼可以由處理器執行以經由認證器與UE執行EAP程序。該EAP程序可以至少部分基於在該認證伺服器和該UE之間交換的一組認證憑證。該代碼亦可以由該處理器執行以作為執行該EAP程序的一部分，推導

MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數；決定與該認證器相關聯的網路類型；至少部分基於該MSK或該EMSK與該網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰；及經由秘密頻道將該安全金鑰發送給該認證器。

【0020】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0021】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，所決定的網路類型可以包括蜂巢網路類型，並且該第二組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、該認證伺服器和該蜂巢網路之間交換的至少一個參數或者它們的組合。

【0022】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0023】 在一個實例中，描述了一種用於蜂巢網路處的無線通訊的方法。該方法可以包括從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK可以至少部分基於一組認證憑證和第二組參數。該認證憑證可以在EAP程序期間在UE和該認證伺

服器之間交換。該方法亦可以包括：至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【0024】 在一個實例中，描述了一種用於蜂巢網路處的無線通訊的裝置。該裝置可以包括用於從認證伺服器接收第一安全金鑰的單元，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK可以至少部分基於一組認證憑證和第二組參數。該認證憑證可以在EAP程序期間在UE和該認證伺服器之間交換。該裝置亦可以包括用於至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序的單元。

【0025】 在一個實例中，描述了另一種用於蜂巢網路處的無線通訊的裝置。該裝置可以包括處理器和與該處理器電子通訊的記憶體。該處理器和該記憶體可以被配置為從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK至少部分基於一組認證憑證和第二組參數。該認證憑證可以在EAP程序期間在UE和該認證伺服器之間交換。該處理器和記憶體亦可以被配置為至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【0026】 在一個實例中，描述了一種儲存用於蜂巢網路處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體。該代碼可由處理器執行以從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK至少部分基於一組認證憑證和第二組參數。

該認證憑證可以在EAP程序期間在UE和該認證伺服器之間交換。該代碼亦可執行用於至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【0027】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，與該UE執行該至少一個認證程序可以包括推導該蜂巢網路的網路節點的第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和第三組參數；及至少部分基於該第二安全金鑰經由該網路節點與該UE通訊。在一些實例中，該第三組參數可以包括：該網路節點的辨識符、至少一個網路節點特定參數、在該UE和該網路節點之間交換的至少一個參數或者它們的組合。

【0028】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該第二組參數可以包括：該蜂巢網路的辨識符、至少一個蜂巢網路特定參數、在該UE和該蜂巢網路之間交換的至少一個參數或者它們的組合。

【0029】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0030】 在上面描述的方法、裝置和非暫時性電腦可讀取媒體的一些實例中，該蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0031】 前面已經對根據本案內容的實例的技術和技術優點進行了相當廣泛的概述，以便可以更好地理解下面的詳細描述。下文將描述另外的技術和優點。揭示的構思和具體實例可以容易地被作為用於修改或設計用於執行本案內容的相同目的的其他結構的基礎。此類等同構造沒有脫離所附請求項的範疇。經由以下結合附圖時考慮的描述，將更好地理解被認為在它們的組織上和在操作方法二者上是本案揭示的構思的特性以及關聯的優點。各圖都僅是被提供用於說明和描述的目的，並不意欲作為請求項的限制的定義。

【圖式簡單說明】

【0032】 經由參照以下附圖可以實現對本發明的本質和優點的進一步的理解。在附圖中，類似的組件或功能可以具有相同的元件符號。此外，可以經由在元件符號後跟隨破折號和在類似組件當中進行區分的第二標記來區分相同類型的各種組件。若在本說明書中只使用了第一元件符號，則該描述可適用於具有相同的第一元件符號的類似組件中的任意一個，而不考慮第二元件符號。

【0033】 圖1示出根據本案內容的各個態樣的無線通訊系統的實例；

【0034】 圖2示出根據本案內容的各個態樣的無線通訊系統的實例；

【0035】 圖3示出根據本案內容的各個態樣的無線通訊系統的金鑰層級的實例。

【0036】 圖4示出根據本案內容的各個態樣的無線通訊系統的實例；

【0037】 圖5示出根據本案內容的各個態樣的在UE、蜂巢網路和認證伺服器之間的實例訊息流；

【0038】 圖6示出根據本案內容的各個態樣的UE的方塊圖；

【0039】 圖7示出根據本案內容的各個態樣的無線通訊管理器的方塊圖；

【0040】 圖8示出根據本案內容的各個態樣的無線通訊系統的示意圖；

【0041】 圖9示出根據本案內容的各個態樣的認證伺服器的方塊圖；

【0042】 圖10示出根據本案內容的各個態樣的認證伺服器的方塊圖；

【0043】 圖11示出根據本案內容的各個態樣的網路節點的方塊圖；

【0044】 圖12示出根據本案內容的各個態樣的通訊管理器的方塊圖；

【0045】 圖13示出根據本案內容的各個態樣的網路節點的示意圖；及

【0046】 圖14-18示出說明根據本案內容的各個態樣的無線通訊的方法的流程圖。

【實施方式】

【0047】 本案內容中描述的技術使UE能夠經由與不同類型的存取網路相關聯的認證器與認證伺服器執行EAP程序。在成功地經由認證器執行了EAP程序時，UE和認證伺服器可以至少部分基於與認證器相關聯的網路類型來推導認證器的安全金鑰。在一些實例中，UE和認證伺服器可以在認證器與非蜂巢存取網路相關聯時基於MSK來推導認證器的安全金鑰，並且可以在認證器與蜂巢存取網路相關聯時基於EMSK來推導認證器的安全金鑰。

【0048】 以下描述提供了實例，但並不限制申請專利範圍中闡述的範疇、適用性或實例。可以改變所論述的元素的功能和佈置而不脫離本案內容的精神和範疇。各個實例可以酌情省略、替代或者添加各種程序或組件。例如，可以按照與所描述順序不同的順序來執行所描述的方法，並且可以添加、省略或組合各個步驟。另外，可以將針對一些實例描述的特徵組合到一些其他的實例中。

【0049】 圖1示出根據本案內容的各個態樣的無線通訊系統100的實例。無線通訊系統100可以包括網路存取設備（例如，分散式網路存取設備、分散式單元、gNB、無線電頭端（RH）、SRH、傳輸/接收點（TRP）、邊緣節點、邊緣單元等等）105、UE 115、網路存取設備控制器（例如，集中式網路存取設備、中央節點、中央單元、存取節點控制器（ANC）等等）125和核心網路130。核心網路130可以提供使用者認證、存取授權、追蹤、網際網路協定（IP）連接和其他存取、路由或移動功能。

網路存取設備控制器125可以經由回載鏈路132（例如，S1、S2等等）與核心網路130互動，並且可以執行針對與UE 115的通訊的無線配置和排程。在各個實例中，網路存取設備控制器125可以直接地或間接地（例如，經由核心網路130）經由回載鏈路134（例如，X1、X2等等）相互通訊，回載鏈路134可以是有線或無線通訊鏈路。每個網路存取設備控制器125亦可以經由多個網路存取設備（例如，RH）105與多個UE 115通訊。在無線通訊系統100的替代配置中，網路存取設備控制器125的功能可以由網路存取設備105提供或者跨越網路節點（例如，存取節點、新無線電基地台（NR BS）等等）135的網路存取設備105分佈。在無線通訊系統100的另一個替代配置中，網路節點135可以由eNB替代，網路存取設備105可以用基地台替代，並且網路存取設備控制器125可以由基地台控制器替代（或者連結到核心網路130）。

【0050】 網路存取設備控制器125可以經由一或多個網路存取設備105與UE 115通訊，每個網路存取設備105具有用於與多個UE 115無線通訊的一或多個天線。每個網路節點135可以為相應地理覆蓋區域110提供通訊覆蓋，並且可以提供與一或多個網路存取設備105相關聯的一或多個遠端收發機。網路存取設備105可以執行LTE/LTE-A基地台的很多功能。在一些實例中，網路存取設備控制器125可以用分散式形式實現，在每個網路存取設備105中提供網路存取設備控制器125的一部分。網

路節點135的地理覆蓋區域110可以被劃分為只構成該覆蓋區域的一部分的扇區（未圖示），並且在一些實例中，網路節點135的地理覆蓋區域110可以經由與網路節點135相關聯的一組網路存取設備105的一組地理覆蓋區域構成（未圖示）。在一些實例中，網路存取設備105可以用另外的網路存取設備替代，例如基地台收發機、無線電基地台、存取點、無線電收發機、節點B、eNB、家庭節點B、家庭進化型節點B、gNB等等。無線通訊系統100可以包括不同類型（例如，巨集細胞及/或小型細胞網路存取設備）的網路存取設備105（或者基地台或其他網路存取設備）。網路存取設備105及/或網路節點135的地理覆蓋區域可以重疊。在一些實例中，不同網路存取設備105可以與不同無線電存取技術相關聯。

【0051】 在一些實例中，無線通訊系統100可以包括5G網路。在其他實例中，無線通訊系統100可以包括LTE/LTE-A網路。無線通訊系統100可以在一些情況下是異質網路，其中不同類型的網路存取設備105或網路節點135為各個地理區域提供覆蓋。例如，每個網路存取設備105或網路節點135可以為巨集細胞、小型細胞及/或其他類型的細胞提供通訊覆蓋。根據上下文，術語「細胞」可以用於描述基地台、RH、與基地台或RH相關聯的載波或分量載波、或者載波或基地台的覆蓋區域（例如，扇區等等）。

【0052】 巨集細胞可以覆蓋相對大的地理區域（例如，半徑為若干公里）並且可以允許具有與網路供應商的服務訂制的UE 115存取。小型細胞可以包括與巨集細胞相比較更低功率的RH或基地台，並且可以工作在與巨集細胞相同或不同的頻帶中。根據各個實例，小型細胞可以包括微微細胞、毫微微細胞和微細胞。微微細胞可以覆蓋相對較小的地理區域並且可以允許具有與網路供應商的服務訂制的UE 115不受限制的存取。毫微微細胞亦可以覆蓋相對小的地理區域（例如，家庭）並且可以提供具有與該毫微微細胞的關聯性的UE 115（例如，封閉用戶組（CSG）中的UE、家庭中的使用者的UE等等）的受限制的存取。巨集細胞的網路存取設備可以被稱為巨集網路存取設備。小型細胞的網路存取設備可以被稱為小型細胞網路存取設備、微微網路存取設備、毫微微網路存取設備或家用網路存取設備。網路存取設備可以支援一或多個（例如，兩個、三個、四個等等）細胞（例如，分量載波）。

【0053】 無線通訊系統100可以支援同步或非同步操作。對於同步操作，網路節點135或網路存取設備105可以具有相似的訊框定時，並且來自不同網路存取設備105的傳輸可以在時間上近似對準。對於非同步操作，網路節點135或網路存取設備105可以具有不同訊框定時，並且來自不同網路存取設備105的傳輸可以在時間上不對準。本案中描述的技術可以用於同步操作或非同步操作。

【0054】 可以容適各個揭示的實例中的一些實例的通訊網路可以是根據分層協定堆疊操作的基於封包的網路。在使用者平面中，承載或封包資料彙聚協定（PDCP）層處的通訊可以是基於IP的。無線鏈路控制（RLC）層可以在一些情況下執行封包分段和重組以經由邏輯通道進行通訊。媒體存取控制（MAC）層可以執行優先順序處理和邏輯通道向傳輸通道中的多工。MAC層亦可以使用混合ARQ（HARQ）來提供MAC層處的重傳以提高鏈路效率。在控制平面中，無線電資源控制（RRC）協定層可以提供UE 115和網路存取設備105、網路存取設備控制器125或支援使用者平面資料的無線電承載的核心網路130之間的RRC連接的建立、配置和維護。在實體（PHY）層處，傳輸通道可以映射到實體通道。

【0055】 UE 115可以遍佈整個無線通訊系統100，並且每個UE 115可以是靜止的或行動的。UE 115亦可以包括或由本發明所屬領域中具有通常知識者稱為行動站、用戶站、行動單元、用戶單元、無線單元、遠端單元、行動設備、無線設備、無線通訊設備、遠端設備、行動用戶站、存取終端、行動終端、無線終端、遠端終端機、手持機、使用者代理、行動服務客戶端、客戶端或一些其他合適的術語。UE 115可以是蜂巢式電話、個人數位助理（PDA）、無線數據機、無線通訊設備、手持設備、平板電腦、膝上型電腦、無線電話、無線區域迴路（WLL）站、萬物互聯（IoE）設備、機動車、電器或其他具有無

線通訊介面的電子設備。UE可以能夠與各種類型的網路節點135或網路存取設備105（包括小型細胞節點、中繼節點等等）通訊。UE亦可以能夠直接與其他UE通訊（例如，使用對等（P2P）協定）。

【0056】 無線通訊系統100中示出的通訊鏈路122可以包括從UE 115到網路存取設備105的上行鏈路（UL）通道，及/或從網路存取設備105到UE 115的下行鏈路（DL）通道。下行鏈路通道亦可以被稱為前向鏈路通道，而上行鏈路通道亦可以被稱為反向鏈路通道。

【0057】 每條通訊鏈路122可以包括一或多個載波，其中每個載波可以是由根據一或多個無線電存取技術調制的多個次載波或頻調（例如，不同頻率的波形信號）組成的信號。每個經調制的信號可以在不同次載波上發送並且可以攜帶控制資訊（例如，參考信號、控制通道等等）、管理負擔資訊、使用者資料等。通訊鏈路122可以使用分頻雙工（FDD）技術（例如，使用成對的頻譜資源）或分時雙工（TDD）技術（例如，使用未成對的頻譜資源）來發送雙向通訊。可以定義FDD的訊框結構（例如，訊框結構類型1）和TDD的訊框結構（例如，訊框結構類型2）。

【0058】 在無線通訊系統100的一些實例中，網路存取設備105及/或UE 115可以包括用於採用天線分集方案來提高網路存取設備105和UE 115之間的通訊品質和可靠性的多個天線。補充地或作為替代，網路存取設備105

及/或UE 115可以採用多輸入多輸出（MIMO）技術，其可以利用多路環境的優勢來發送攜帶相同或不同編碼資料的多個空間層。

【0059】 無線通訊系統100可以支援多個細胞或載波上的操作，一種可以被稱為載波聚合（CA）或多載波操作的特徵。載波亦可以被稱為分量載波（CC）、層、通道等等。術語「載波」、「分量載波」、「細胞」和「通道」可以在本案中互換使用。UE 115可以配置有多個下行鏈路CC和一或多個上行鏈路CC用於載波聚合。載波聚合可以與FDD分量載波和TDD分量載波二者一起使用。

【0060】 一或多個UE 115可以包括無線通訊管理器140。在一些實例中，無線通訊管理器140可以用於經由與核心網路130相關聯的認證器與認證伺服器執行EAP程序。如參考圖2所描述的，可以經由核心網路130存取認證伺服器。EAP程序可以至少部分基於UE和認證伺服器之間交換的一組認證憑證。無線通訊管理器140亦可以用於推導至少部分基於認證憑證和第一組參數的MSK和EMSK（共同地被稱為EAP方法或認證方法）（作為執行EAP程序的一部分）；決定認證器與蜂巢網路相關聯；及至少部分基於EMSK，與蜂巢網路執行至少一個認證程序。在一些實例中，無線通訊管理器140可以是參考圖6-8描述的無線通訊管理器的態樣的實例。

【0061】 圖2示出根據本案內容的各個態樣的無線通訊系統200的實例。無線通訊系統200可以包括UE

115-a的歸屬蜂巢網路205和由UE 115-a存取的蜂巢網路（亦即，被存取的蜂巢網路205-a）。

【0062】 歸屬蜂巢網路205可以包括第一認證器235（例如，提供歸屬安全錨定功能（H-SEAF）的伺服器或設備）和歸屬使用者平面閘道（H-UP-GW）210。本發明所屬領域中具有通常知識者應當領會的是，歸屬蜂巢網路205亦可以包括提供其他功能的其他伺服器或設備（未圖示）。被存取的蜂巢網路205-a可以包括第二認證器235-a（例如，提供存取SEAF（V-SEAF）的伺服器或設備）、被存取的UP-GW（V-UP-GW）210-a、被存取的蜂巢網路控制平面核心網路功能單元（V-CP-CN）215和無線電存取網路（RAN）220。在一些實例中，RAN 220可以包括參考圖1描述的網路節點135、網路存取設備105和網路存取設備控制器125中的一或多個。第一認證器235、H-UP-GW 210、第二認證器235-a、V-UP-GW 210-a和V-CP-CN 215可以是參考圖1描述的核心網路130的示例性組件。

【0063】 歸屬蜂巢網路205可以與認證伺服器245通訊（或可以提供認證伺服器245）。認證伺服器245可以提供認證伺服器功能單元（AUSF）。認證伺服器245可以存取及/或調用認證憑證庫和處理功能單元（ARPF）240。

【0064】 UE 115-a可以經由RAN 220的節點（例如，網路存取設備）連接到被存取的蜂巢網路205-a。圖

2假設UE 115-a在操作在漫遊模式中的同時存取被存取的蜂巢網路205-a。在非漫遊場景中，UE 115-a可以經由歸屬蜂巢網路205的RAN而不是被存取的蜂巢網路205-a存取歸屬蜂巢網路205（圖2中未圖示）。

【0065】 V-CP-CN 215可以包括或管理UE 115-a的行動性管理（MM）功能及/或通信期管理（SM）功能的一或多個態樣，以及維護相對應的安全性上下文。第二認證器235-a可以促進並管理由被存取的蜂巢網路205-a對UE 115-a的認證，以及可以維護可以從其推導後續安全金鑰的錨定通信期金鑰。當使用者平面安全性終止於V-UP-GW 210-a處時，V-UP-GW 210-a可以維護UE 115-a的使用者平面安全性上下文（例如，安全金鑰）。使用者平面安全性可以由RAN 220及/或V-UP-GW 210-a終止並且可以由網路配置。一般來講，UE 115-a可以維護與被存取的蜂巢網路205-a的每個節點的安全性上下文。

【0066】 在存取了被存取的蜂巢網路205-a時，第二認證器235-a可以促進由UE 115-a和認證伺服器245執行的EAP程序。第二認證器235-a可以經由（歸屬蜂巢網路205的）第一認證器235建立或維護用於與認證伺服器245執行EAP程序的秘密頻道。

【0067】 由UE 115-a和認證伺服器245執行的EAP程序可以至少部分基於UE 115-a和認證伺服器245之間交換的一組認證憑證。作為執行EAP程序的一部分，UE

115-a和認證伺服器245中的每一個可以推導MSK和EMSK。MSK和EMSK可以至少部分基於認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0068】 當EAP程序成功時（例如，當UE 115-a和認證伺服器245成功地相互認證時），認證伺服器245可以向第二認證器235-a發送通信期錨定金鑰（例如，第一安全金鑰）。根據本案內容中描述的技術，通信期錨定金鑰可以至少部分基於EMSK。通信期錨定金鑰亦可以至少部分基於第二組參數。第二組參數可以包括被存取的蜂巢網路205-a的辨識符、至少一個蜂巢網路特定參數、在UE 115-a和第二蜂巢網路205-a之間交換的至少一個參數或者它們的組合。

【0069】 UE 115-a可以獨立地推導通信期錨定金鑰。至少部分基於通信期錨定金鑰，UE 115-a和第二認證器235-a可以相互認證並推導另外的安全金鑰（例如，第二蜂巢網路205-a的其他節點或功能單元的安全金鑰），如圖3中所示。

【0070】 作為對圖2中示出的替代，提供H-SEAF和V-SEAF的伺服器或設備可以不假設在UE 115-a和認證伺服器245之間執行的EAP程序中的認證器的角色，相反，認證器可以與認證伺服器245（例如，提供AUSF的伺服器）搭配使用。在這些實例中，認證伺服器245可以

基於MSK或EMSK和第二組參數來推導H-SEAF或V-SEAF的通信期錨定金鑰，並且將通信期錨定金鑰發送給H-SEAF（在非漫遊場景中）或V-SEAF（在漫遊場景中）。

【0071】 圖3示出根據本案內容的各個態樣的無線通訊系統的金鑰層級300的實例。這一解決方案經由使用EMSK推導從EAP伺服器（例如，參考圖2描述的認證伺服器245）向下傳遞的金鑰（例如，KSEAF），來提供到針對一般EAP協定遞送給3GPP服務網路的金鑰的服務網路拘束。在一些實例中，金鑰層級300可以由參考圖1和2描述的無線通訊系統100和200使用。例如，UE及/或網路節點可以使用金鑰層級300來實現參考圖1和2描述的認證或安全性功能的一或多個態樣。

【0072】 金鑰層級300可以包括用作通用用戶辨識模組（USIM）和ARPF之間的安全性上下文的K根金鑰305。K根金鑰305可以用作執行EAP程序和推導金鑰310（例如，MSK和EMSK）以提供認證伺服器和UE之間（例如，參考圖2描述的認證伺服器245和UE 115-a之間）的安全性上下文的基礎。K根金鑰305可以用於執行基於共享金鑰的EAP程序，但是在執行基於證書的EAP程序時可以使用一或多個其他金鑰（例如，基於證書推導的金鑰）。EMSK可以被認證伺服器（例如，AUSF）和UE用於推導針對認證器（例如，針對參考圖2描述的第二認證器235-a）的K_{SEAF}錨定通信期金鑰315。由於

EMSK（而不是MSK）被用於推導K_{SEAF}，因此可以不需要將憑證的使用限制於3GPP存取。例如，當非3GPP實體基於EAP認證獲取MSK時，非3GPP實體無法推導K_{SEAF}，這是因為K_{SEAF}是從非3GPP實體所不知道的EMSK推導出的。K_{SEAF}錨定通信期金鑰315可以由認證器和UE維護。

【0073】 K_{SEAF}錨定通信期金鑰315可以被認證器用於推導K_{CP-CN}金鑰320和K_{UP-GW}金鑰325。K_{CP-CN}金鑰320可以由CP-CN功能單元（例如，參考圖2描述的V-CP-CN 215）和UE維護。K_{UP-GW}金鑰325可以由UP-GW功能單元（例如，參考圖2描述的V-UP-GW 210-a）和UE維護。K_{UP-GW}金鑰325可以被UP-GW用於確立$K_{UP-GWenc}$金鑰340和$K_{UP-GWint}$金鑰345。$K_{UP-GWenc}$金鑰340和$K_{UP-GWint}$金鑰345可以用於使用者平面封包的完整性保護和編碼。

【0074】 K_{CP-CN}金鑰320可以被CP-CN功能單元用於推導K_{NASenc}金鑰330、K_{NASint}金鑰335和$K_{AN/NH}$金鑰350。$K_{AN/NH}$金鑰350可以被存取點用於推導K_{UPint}金鑰355、K_{UPenc}金鑰360、K_{RRCint}金鑰365和K_{RRCenc}金鑰370，它們可以用於RRC和使用者平面封包的完整性保護和編碼。

【0075】 圖4示出根據本案內容的各個態樣的無線通訊系統400的實例。無線通訊系統400可以包括UE

115-b的歸屬蜂巢網路205-b和由UE 115-b存取的蜂巢網路（亦即，被存取的蜂巢網路205-c）。

【0076】 歸屬蜂巢網路205-b可以包括第一認證器235-b（例如，提供H-SEAF的伺服器或設備）和H-UP-GW 210-b。歸屬蜂巢網路205-b亦可以包括提供其他功能的其他伺服器或設備（未圖示）。被存取的蜂巢網路205-c可以包括第二認證器235-c（例如，提供V-SEAF的伺服器或設備）、V-UP-GW 210-c、V-CP-CN 215-a和RAN 220-a。在一些實例中，RAN 220-a可以包括參考圖1描述的網路節點135、網路存取設備105和網路存取設備控制器125中的一或多個。第一認證器235-b、H-UP-GW 210-b、第二認證器235-c、V-UP-GW 210-c和V-CP-CN 215-a可以是參考圖1描述的核心網路130的示例性組件。

【0077】 歸屬蜂巢網路205-b可以與認證伺服器245-a通訊（或者可以提供認證伺服器245-a）。認證伺服器245-a可以提供AUSF。認證伺服器245-a可以存取及/或調用ARPF 240-a。

【0078】 第一認證器235-b、H-UP-GW 210-b、第二認證器235-c、V-UP-GW 210-c、V-CP-CN 215-a、RAN 220-a、認證伺服器245-a和ARPF 240-a中的每一個可以是參考圖2描述的類似編號的組件、功能單元或節點的實例。

【0079】 圖4亦示出包括非蜂巢存取節點410（例如，WALN存取點（AP）或無線LAN控制器（WLC））的非蜂巢網路405。如圖所示，UE 115-b可以連接到RAN 220-a或非蜂巢存取節點410，並且在每種情況下，相同的認證伺服器245-a可以與UE 115-b執行EAP程序。當UE 115-b連接到RAN 220-a時，第二認證器235-c可以用作由UE 115-b和認證伺服器245-a執行的EAP程序中的認證器。當UE 115-b連接到非蜂巢存取節點410時，非蜂巢存取節點410可以用作由UE 115-b和認證伺服器245-a執行的EAP程序中的認證器。

【0080】 若UE 115-b和認證伺服器245-a二者皆能夠執行相同的EAP程序並推導相同的通信期錨定金鑰（例如，用於在UE 115-b和第二認證器235-c之間執行認證程序，或者用於在UE 115-b和非蜂巢存取節點410之間執行認證程序），包括非蜂巢存取節點410的攻擊者可以能夠從非蜂巢存取節點410獲得該通信期錨定金鑰並使用它來假扮被存取的蜂巢網路205-c或歸屬蜂巢網路205-b的節點。為了解決上面提到的問題，UE 115-b和認證伺服器245-a可以決定與認證器相關聯的網路類型（例如，與第二認證器235-c或非蜂巢存取節點410相關聯的網路的類型），並且決定要使用哪個金鑰（在MSK和EMSK之間）來推導通信期錨定金鑰（亦即，基於該網路類型推導通信期錨定金鑰）。在一些實例中，在認證器（例如，非蜂巢存取節點410）與非蜂巢存取網路（例如，

非蜂巢網路405）相關聯時可以使用MSK，並且在認證器（例如，第二認證器235-c）與蜂巢存取網路（例如，被存取的蜂巢網路205-c）相關聯時可以使用EMSK。另外，針對與蜂巢網路相關聯的認證器推導的通信期錨定金鑰可以至少部分基於與該蜂巢網路相關聯的一組參數來推導得到。例如，K_{SEAF}金鑰可以由UE 115-b和認證伺服器245-a基於金鑰推導公式（KDF）來推導得到

K_{SEAF}=KDF(EMSK, PLMN ID, CTX)

其中PLMN ID是與服務（例如，被存取的）蜂巢網路205-b相關聯的且在該EAP程序期間提供給認證伺服器245-a的公共陸地行動網辨識符，並且CTX是描述存取技術（例如，蜂巢網路存取，例如5G（NextGen）、4G、LTE/LTE-A或3G網路存取）的上下文。本發明所屬領域中具有通常知識者應當領會的是，K_{SEAF}亦可以至少部分基於其他合適的參數來推導得到。

【0081】 經由基於與認證器相關聯的網路類型來推導認證器的通信期錨定金鑰，一個網路類型的網路無法獲得另一個類型的網路的通信期錨定金鑰並且假扮不同網路類型的節點。因此，相同的EAP程序（或認證方法）可以用於不同類型的網路而不影響不同類型網路的安全性。

【0082】 圖5示出根據本案內容的各個態樣的UE 115-c、蜂巢網路205-d和認證伺服器245-b之間的實例訊息流500。UE 115-c可以是參考圖1、2和4描述的UE 115的態樣的實例。蜂巢網路205-d可以是參考圖2和4

描述的蜂巢網路205的實例，並且在一些情況下可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。認證伺服器245-b可以是參考圖2和4描述的認證伺服器245的態樣的實例。蜂巢網路205-d可以包括RAN 220-b和蜂巢CN 550。RAN 220-b和CN 550可以是參考圖2和4描述的RAN 220和CN的實例。在一些實例中，RAN 220-b可以包括參考圖1描述的網路節點135、網路存取設備105或網路存取設備控制器125中的一或多個。CN 550可以包括認證器235-d（例如，CN 550的節點），其可以是參考圖2和4描述的認證器235的態樣的實例。

【0083】 在505處，UE 115-c可以存取蜂巢網路205-d，並且UE 115-c或蜂巢網路205-d可以發起EAP程序。在一些實例中，UE 115-c可以經由RAN 220-b的網路存取設備（例如，網路節點）存取蜂巢網路205-d。RAN 220-b可以與CN 550通訊。CN 550內的認證器235-d可以促進EAP程序的執行。在蜂巢網路的替代配置中，認證器235-d可以是RAN 220-b的一部分或者搭配認證伺服器245-b一起使用。

【0084】 在510處，蜂巢網路205-d可以向認證伺服器245-b發送用於執行EAP程序的請求。在一些實例中，在510處發送的請求可以經由認證器235-d和認證伺服器245-b之間的秘密頻道進行發送（例如，該請求可以使

用Diameter協定（例如，使用Diameter封裝）在認證器235-d和認證伺服器245-b之間進行發送）。

【0085】 在515處，UE 115-c和認證伺服器245-b可以經由認證器235-d執行EAP程序，其中認證器235-d提供在UE 115-c和認證伺服器245-b之間發送的訊息的傳輸。EAP程序可以至少部分基於在UE 115-c和認證伺服器245-b之間交換的一組認證憑證。作為執行該EAP程序的一部分，UE 115-c和認證伺服器245-b中的每一個可以推導MSK和EMSK。MSK和EMSK可以至少部分基於認證憑證和第一組參數來推導得到。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0086】 在505、510或515處的操作之前、期間或之後，UE 115-c和認證伺服器245-b中的每一個可以決定認證器235-d與蜂巢網路（亦即，與蜂巢網路205-d）相關聯。

【0087】 在520和525處，UE 115-c和認證伺服器245-b中的每一個可以獨立地推導蜂巢網路205-d的第一安全金鑰。由於UE 115-c和認證伺服器245-b中的每一個決定認證器235-d與蜂巢網路205-d相關聯，因此，UE 115-c和認證伺服器245-b中的每一個可以至少部分基於該EMSK來推導第一安全金鑰。第一安全金鑰亦可以至少部分基於第二組參數來推導得到。在一些實例中，

第二組參數可以包括蜂巢網路205-d的辨識符、至少一個蜂巢網路特定參數、在UE 115-c或認證伺服器245-b和蜂巢網路205-c之間交換的至少一個參數或者它們的組合。

【0088】 在530處，認證伺服器245-b可以經由認證器235-d和認證伺服器245-b之間的秘密頻道向認證器235-d發送第一安全金鑰（例如，第一安全金鑰可以使用Diameter協定（例如，使用Diameter封裝）在認證伺服器245-b和認證器235-d之間進行發送）。

【0089】 在535處，UE 115-c和蜂巢網路205-d可以執行認證程序。在540和545處，在535處成功執行了認證程序時，UE 115-c和蜂巢網路205-d可以推導蜂巢網路205-d的一或多個網路節點的一或多個另外的安全金鑰（例如，第二安全金鑰）。在一些實例中，第二安全金鑰可以至少部分基於第一安全金鑰和第三組參數。在一些實例中，第三組參數可以包括該網路節點的辨識符、至少一個網路節點特定參數、UE 115-c和該網路節點之間交換的至少一個參數或者它們的組合。

【0090】 在555處，UE 115-c可以至少部分基於所推導的安全金鑰與蜂巢網路205-d通訊。

【0091】 圖6示出根據本案內容的各個態樣的UE 115-d的方塊圖600。UE 115-d可以是參考圖1、2、4和5描述的UE 115的態樣的實例。UE 115-d可以包括接收器610、無線通訊管理器620和發射器630。UE

115-d亦可以包括處理器。這些組件中的每一個可以相互通訊。

【0092】 接收器610可以接收信號或資訊，例如與各種通道（例如，控制通道、資料通道、廣播通道、多播通道、單播通道等等）相關聯的參考信號、控制資訊或使用者資料。所接收的信號和資訊可以由接收器610使用（例如，用於頻率/時間追蹤）或者被傳遞給UE 115-d的其他組件，包括無線通訊管理器620。接收器610可以是參考圖8描述的收發機825的態樣的實例。接收器610可以包括單個天線或複數個天線或與之相關聯。

【0093】 無線通訊管理器620可以用於管理UE 115-d的無線通訊的一或多個態樣。在一些實例中，無線通訊管理器620的一部分可以合併到接收器610或發射器630中或與之共享。無線通訊管理器620可以包括EAP管理器635、網路類型辨識器640和網路認證器645。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。

【0094】 如上參考圖5所描述的，EAP管理器635可以用於經由認證器與認證伺服器執行EAP程序。EAP程序可以至少部分基於UE和認證伺服器之間交換的一組認證憑證。如上參考圖5所描述的，作為執行EAP程序的一部分，EAP管理器635亦可以用於推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識

符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0095】 如上參考圖5所描述的，網路類型辨識器640可以用於決定與該認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。

【0096】 網路認證器645可以用於至少部分基於所決定的網路類型與該認證器執行至少一個認證程序。如上參考圖5所描述的，該至少一個認證程序可以基於該MSK或EMSK與所決定的網路類型的關聯。

【0097】 發射器630可以發送從UE 115-d的其他組件（包括無線通訊管理器620）接收的信號或資訊。該信號或資訊可以包括例如與各種通道（例如，控制通道、資料通道、廣播通道、多播通道、單播通道等等）相關聯的參考信號、控制資訊或使用者資料。在一些實例中，發射器630可以搭配接收器610在收發機中一起使用。發射器630可以是參考圖8描述的收發機825的態樣的實例。發射器630可以包括單個天線或複數個天線或與之相關聯。

【0098】 圖7示出根據本案內容的各個態樣的無線通訊管理器720的方塊圖700。無線通訊管理器720可以是參考圖6描述的無線通訊管理器620的態樣的實例。

【0099】 無線通訊管理器720可以包括EAP管理器635-a、網路類型辨識器640-a、網路認證器645-a和蜂巢網路通訊管理器715。EAP管理器635-a、網路類型辨

識器640-a和網路認證器645-a可以是參考圖6描述的EAP管理器635、網路類型辨識器640和網路認證器645的實例。網路認證器645-a可以包括網路金鑰推導器705和網路節點金鑰推導器710。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。

【0100】 如上參考圖5所描述的，EAP管理器635-a可以用於經由認證器與認證伺服器執行EAP程序。EAP程序可以至少部分基於在UE和認證伺服器之間交換的一組認證憑證。如上參考圖5所描述的，作為執行EAP程序的一部分，EAP管理器635-a亦可以用於推導MSK和EMSK，該MSK和該EMSK至少部分基於該認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0101】 如上參考圖5所描述的，網路類型辨識器640-a可以用於決定與認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。

【0102】 網路認證器645-a至少部分基於所決定的網路類型與該認證器執行至少一個認證程序。該至少一個認證程序可以基於該MSK或EMSK與所決定的網路類型的關聯。

【0103】 如上參考圖5所描述的，當所決定的網路類型包括蜂巢網路類型時，網路金鑰推導器705可以用於推導

蜂巢網路的第一安全金鑰。第一安全金鑰可以至少部分基於該EMSK和第二組參數。在一些實例中，第二組參數可以包括該蜂巢網路的辨識符、至少一個蜂巢網路特定參數、在該UE和蜂巢網路之間交換的至少一個參數或者它們的組合。當所決定的網路類型包括非蜂巢網路類型時，網路金鑰推導器705可以用於推導非蜂巢網路的第一安全金鑰。

【0104】 如上參考圖5所描述的，當所決定的網路類型包括蜂巢網路類型時，網路節點金鑰推導器710可以用於推導該蜂巢網路的網路節點的第二安全金鑰。第二安全金鑰可以至少部分基於第一安全金鑰和第三組參數。在一些實例中，第三組參數可以包括該網路節點的辨識符、至少一個網路節點特定參數、在UE和網路節點之間交換的至少一個參數或者它們的組合。

【0105】 如上參考圖5所描述的，蜂巢網路通訊管理器715可以用於至少部分基於第二安全金鑰經由該網路節點與該蜂巢網路通訊。

【0106】 圖8示出根據本案內容的各個態樣的無線通訊系統800的示意圖。無線通訊系統800可以包括UE 115-e，其可以是參考圖1、2和4-6描述的UE 115的態樣的實例。

【0107】 UE 115-e可以包括無線通訊管理器805、記憶體810、處理器820、收發機825和天線830。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由

一或多個匯流排）。無線通訊管理器805可以是參考圖6和7描述的無線通訊管理器620和720的態樣的實例。

【0108】 記憶體810可以包括隨機存取記憶體（RAM）或唯讀記憶體（ROM）。記憶體810可以儲存電腦可讀、電腦可執行軟體815，其包括指令，該等指令在被執行時使處理器820執行本案中描述的各種功能，包括與網路安全性和認證有關的功能。在一些情況下，軟體815可以不由處理器820直接執行，但是可以使處理器820（例如，在被編譯和執行時）執行本案中描述的功能。處理器820可以包括智慧硬體設備（例如，中央處理單元（CPU）、微控制器、特殊應用積體電路（ASIC）等等）。

【0109】 如本案中所描述的，收發機825可以經由一或多個天線或有線鏈路與一或多個網路雙向通訊。例如，收發機825可以與蜂巢網路205-e（或其一或多個節點）或另一個UE 115-f雙向通訊。收發機825可以包括數據機，其用於調制封包並將經調制封包提供給天線用於傳輸，以及解調從天線接收的封包。在一些情況下，UE 115-e可以包括單個天線830。然而，在一些情況下，UE 115-e可以具有一個以上的天線830，它們可以能夠同時發送或接收多個無線傳輸。

【0110】 圖9示出根據本案內容的各個態樣的認證伺服器245-c的方塊圖900。認證伺服器245-c可以是參考圖2、4和5描述的認證伺服器245的態樣的實例。認證伺服器245-c可以包括接收器910、認證管理器920和發射

器930。認證伺服器245-c亦可以包括處理器。這些組件中的每一個可以相互通訊。

【0111】 接收器910可以從各個網路節點(包括蜂巢網路、WLAN等等的節點)接收認證請求。接收器910亦可以經由網路節點從UE接收認證資訊。所接收的認證請求和認證資訊可以被傳遞給認證管理器920。接收器910可以是參考圖10描述的認證介面1025的態樣的實例。接收器910可以包括一或多個有線及/或無線介面。

【0112】 認證管理器920可以用於管理認證伺服器245-c的設備認證的一或多個態樣。在一些實例中，認證管理器920的一部分可以合併到接收器910或發射器930中或者與之共享。認證管理器920可以包括EAP管理器935、網路類型辨識器940、網路金鑰推導器945和網路金鑰安裝器950。這些組件中的每一個可以直接地或間接地相互通訊(例如，經由一或多個匯流排)。

【0113】 如上參考圖5所描述的，EAP管理器935可以用於經由認證器與UE執行EAP程序。EAP程序可以至少部分基於認證伺服器和UE之間交換的一組認證憑證。如上參考圖5所描述的，作為執行EAP程序的一部分，EAP管理器935亦可以用於推導MSK和EMSK，該MSK和該EMSK至少部分基於認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。

【0114】 如上參考圖5所描述的，網路類型辨識器940可以用於決定與認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。

【0115】 如上參考圖5所描述的，網路金鑰推導器945可以用於至少部分基於MSK或EMSK與該網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰。當所決定的網路類型包括蜂巢網路類型時，並且在一些實例中，第二組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、在認證伺服器和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0116】 如上參考圖5所描述的，網路金鑰安裝器950可以用於經由秘密頻道向認證器發送安全金鑰。

【0117】 發射器930可以發送從認證伺服器245-c的其他組件（包括認證管理器920）接收的認證回饋訊息和安全金鑰。發射器930可以是參考圖10描述的認證介面1025的態樣的實例。發射器930可以包括一或多個有線及/或無線介面。

【0118】 圖10示出根據本案內容的各個態樣的認證伺服器245-d的方塊圖1000。認證伺服器245-d可以是參考圖2、4、5和9描述的認證伺服器245的態樣的實例。

【0119】 認證伺服器245-d可以包括認證管理器1005、記憶體1010、處理器1020和認證介面1025。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。認證管理器1005可以是參考圖9描述的認證管理器920的態樣的實例。

【0120】 記憶體1010可以包括RAM或ROM。記憶體1010可以儲存電腦可讀、電腦可執行軟體1015，其包括指令，該等指令在被執行時使處理器1020執行本案中描述的各種功能，包括與網路安全性和認證有關的功能。在一些情況下，軟體1015可以不由處理器1020直接執行，但是可以使處理器1020（例如，在被編譯和執行時）執行本案中描述的功能。處理器1020可以包括智慧硬體設備（例如，CPU、微控制器、ASIC等等）。

【0121】 如本案中所描述的，認證介面1025可以經由一或多個天線或有線鏈路與一或多個網路、網路節點或UE雙向通訊。在一些實例中，認證介面1025可以用於與網路節點建立安全連接(例如，使用Radius或Diameter協定）並且經由該安全連接和網路節點與UE雙向通訊。

【0122】 圖11示出根據本案內容的各個態樣的網路節點1105的方塊圖1100。網路節點1105可以是參考圖2、4和5描述的網路節點的態樣的實例，並且在一些實例中，可以是參考圖2、4和5描述的認證器235的實例。網路節點1105可以包括接收器1110、通訊管理器1120和

發射器1130。網路節點1105亦可以包括處理器。這些組件中的每一個可以相互通訊。

【0123】 接收器1110可以從其他網路節點、從UE、從認證伺服器等接收信號或資訊。所接收的信號和資訊可以被傳遞給網路節點1105的其他組件，包括通訊管理器1120。接收器1110可以是參考圖13描述的認證介面1325的態樣的實例。接收器1110可以包括一或多個有線及/或無線介面。

【0124】 通訊管理器1120可以用於管理網路節點1105的無線通訊的一或多個態樣。在一些實例中，通訊管理器1120的一部分可以合併到接收器1110或發射器1130中或者與之共享。通訊管理器1120可以包括網路金鑰管理器1135和UE認證器1140。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。

【0125】 如上參考圖5所描述的，網路金鑰管理器1135可以用於從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。EMSK可以至少部分基於一組認證憑證和第二組參數。認證憑證可以在EAP程序期間在UE和認證伺服器之間交換。在一些實例中，第一組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、在UE和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，第二組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路

參數、至少一個UE參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0126】 如上參考圖5所描述的，UE認證器1140可以用於至少部分基於第一安全金鑰與UE執行至少一個認證程序。

【0127】 發射器1130可以發送從網路節點1105的其他組件（包括通訊管理器1120）接收的信號或資訊。發射器1130可以是參考圖13描述的認證介面1325的態樣的實例。接收器1110可以包括一或多個有線及/或無線介面。

【0128】 圖12示出根據本案內容的各個態樣的通訊管理器1220的方塊圖1200。通訊管理器1220可以是參考圖11描述的通訊管理器1120的態樣的實例。

【0129】 通訊管理器1220可以包括網路金鑰管理器1135-a、UE認證器1140-a和UE通訊管理器1210。網路金鑰管理器1135-a和UE認證器1140-a可以是參考圖11描述的網路金鑰管理器1135和UE認證器1140的實例。UE認證器1140-a可以包括網路節點金鑰推導器1205。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。

【0130】 如上參考圖5所描述的，網路金鑰管理器1135-a可以用於從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。EMSK

可以至少部分基於一組認證憑證和第二組參數。可以在EAP程序期間在UE和認證伺服器之間交換認證憑證。在一些實例中，第一組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、在UE和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，第二組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0131】 如上參考圖5所描述的，UE認證器140-a可以用於至少部分基於第一安全金鑰與UE執行至少一個認證程序。網路節點金鑰推導器1205可以用於與UE執行至少一個認證程序，可以包括推導蜂巢網路的網路節點的第二安全金鑰。第二安全金鑰可以至少部分基於第一安全金鑰和第三組參數。在一些實例中，第三組參數可以包括網路節點的辨識符、至少一個網路節點特定參數、在UE和網路節點之間交換的至少一個參數或者它們的組合。

【0132】 如上參考圖5所描述的，UE通訊管理器1210可以用於至少部分基於第二安全金鑰經由網路節點與UE通訊。

【0133】 圖13示出根據本案內容的各個態樣的網路節點1105-a的示意圖1300。網路節點1105-a可以是參考圖2、4、5和11描述的網路節點的態樣的實例。

【0134】 網路節點1105-a可以包括通訊管理器1305、記憶體1310、處理器1320和認證介面1325。這些組件中的每一個可以直接地或間接地相互通訊（例如，經由一或多個匯流排）。通訊管理器1305可以是參考圖11或12描述的通訊管理器的態樣的實例。

【0135】 記憶體1310可以包括RAM或ROM。記憶體1310可以儲存電腦可讀、電腦可執行軟體1315，其包括指令，該等指令在被執行時使處理器1320執行本案中描述的各種功能，包括與網路安全性和認證有關的功能。在一些情況下，軟體1315可以不直接由處理器1320執行，但是可以使處理器1320（例如，在被編譯和執行時）執行本案中描述的功能。處理器1320可以包括智慧硬體設備（例如，CPU、微控制器、ASIC等等）。

【0136】 如本案中所描述的，認證介面1325可以經由一或多個天線或有線鏈路與一或多個網路、網路節點或UE雙向通訊。在一些實例中，認證介面1325可以用於與認證伺服器建立安全連接（例如，使用Radius或Diameter協定）並且促進由UE和認證伺服器執行的EAP程序。

【0137】 圖14示出根據本案內容的各個態樣的用於無線通訊的方法1400的流程圖。如參考圖1-8所描述的，方法1400的操作可以由UE 115或其組件執行。在一些實例中，方法1400的操作可以由參考圖6-8描述的無線通訊管理器執行。在一些實例中，UE可以執行用於控制

該UE的功能組件執行下面描述的功能的代碼集。補充地或者作為替代，UE可以使用專用硬體來執行下面描述的功能的態樣。

【0138】 在方塊1405處，如上參考圖5所描述的，UE可以經由認證器與認證伺服器執行EAP程序。EAP程序可以至少部分基於在UE和認證伺服器之間交換的一組認證憑證。在某些實例中，可以使用參考圖6和7描述的EAP管理器635來執行方塊1405的操作。

【0139】 在方塊1410處，如上參考圖5所描述的，作為執行EAP程序的一部分，UE可以推導MSK和EMSK，該MSK和該EMSK至少部分基於認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在某些實例中，可以使用參考圖6和7描述的EAP管理器635來執行方塊1410的操作。

【0140】 在方塊1415處，如上參考圖5所描述的，UE可以決定與認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。在某些實例中，可以使用參考圖6和7描述的網路類型辨識器640來執行方塊1415的操作。

【0141】 在方塊1420處，UE可以至少部分基於所決定的網路類型與認證器執行至少一個認證程序。如上參考圖5所描述的，該至少一個認證程序可以至少部分基於MSK

或EMSK與所決定的網路類型的關聯。在某些實例中，可以使用參考圖6和7描述的網路認證器645來執行方塊1420的操作。

【0142】 圖15示出根據本案內容的各個態樣的用於無線通訊的方法1500的流程圖。如參考圖1-8所描述的，方法1500的操作可以由UE 115或其組件執行。在一些實例中，方法1500的操作可以由參考圖6-8描述的無線通訊管理器執行。在一些實例中，UE可以執行用於控制該UE的功能組件執行下面描述的功能的代碼集。補充地或者作為替代，UE可以使用專用硬體來執行下面描述的功能的態樣。

【0143】 在方塊1505處，如上參考圖5所描述的，UE可以經由認證器與認證伺服器執行EAP程序。該EAP程序可以至少部分基於在UE和認證伺服器之間交換的一組認證憑證。在某些實例中，可以使用參考圖6和7描述的EAP管理器635執行方塊1505的操作。

【0144】 在方塊1510處，如上參考圖5所描述的，作為執行EAP程序的一部分，UE可以推導MSK和EMSK，該MSK和該EMSK至少部分基於認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在某些實例中，可以使用參考圖6和7描述的EAP管理器635執行方塊1510的操作。

【0145】 在方塊1515處，如上參考圖5所描述的，UE可以決定與認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。在某些實例中，可以使用參考圖6和7描述的網路類型辨識器640執行方塊1515的操作。

【0146】 在方塊1520處，方法1500可以分支到方塊1525或1540，這取決於所決定的網路類型包括蜂巢網路類型還是非蜂巢網路類型。當所決定的網路類型包括蜂巢網路類型時，方法1500可以分支到方塊1525。當所決定的網路類型包括非蜂巢網路類型時，方法1500可以分支到方塊1540。在某些實例中，可以使用參考圖6和7描述的網路類型辨識器640來執行方塊1520的操作。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。

【0147】 若UE決定網路類型包括蜂巢網路類型，則在方塊1525和1530處，UE可以至少部分基於所決定的網路類型與認證器執行至少一個認證程序。該至少一個認證程序可以基於MSK或EMSK與所決定的網路類型的關聯。在方塊1525處，如上參考圖5所描述的，UE可以推導蜂巢網路的第一安全金鑰。第一安全金鑰可以至少部分基於EMSK和第二組參數。在一些實例中，第二組參數可以包括該蜂巢網路的辨識符、至少一個蜂巢網路特定參

數、在UE和蜂巢網路之間交換的至少一個參數或者它們的組合。在某些實例中，可以使用參考圖6和7描述的網路認證器645，或參考圖7所描述的網路金鑰推導器705來執行方塊1525的操作。

【0148】 在方塊1530處，如上參考圖5所描述的，UE可以推導蜂巢網路的網路節點的第二安全金鑰。第二安全金鑰可以至少部分基於第一安全金鑰和第三組參數。在一些實例中，第三組參數可以包括網路節點的辨識符、至少一個網路節點特定參數、在UE和網路節點之間交換的至少一個參數或者它們的組合。在某些實例中，可以使用參考圖6和7描述的網路認證器645，或參考圖7所描述的網路節點金鑰推導器710來執行方塊1530的操作。

【0149】 在方塊1535處，如上參考圖5所描述的，UE可以至少部分基於第二安全金鑰，經由網路節點與蜂巢網路通訊。在某些實例中，可以使用參考圖7描述的蜂巢網路通訊管理器715來執行方塊1530的操作。

【0150】 若UE決定網路類型包括非蜂巢網路，則在方塊1540處，UE可以推導非蜂巢網路的第一安全金鑰。第一安全金鑰可以至少部分基於MSK和第四組參數。在某些實例中，可以使用參考圖6和7描述的網路認證器645，或參考圖7所描述的網路金鑰推導器705來執行方塊1540的操作。

【0151】 圖16示出根據本案內容的各個態樣的用於無線通訊的方法1600的流程圖。如參考圖1-5、9和10所

描述的，方法1600的操作可以由認證伺服器或其組件執行。在一些實例中，方法1600的操作可以由參考圖9和10描述的認證管理器執行。在一些實例中，認證伺服器可以執行用於控制該認證伺服器的功能組件執行下面描述的功能的代碼集。補充地或者作為替代，認證伺服器可以使用專用硬體執行下面描述的功能的態樣。

【0152】 在方塊1605處，如上參考圖5所描述的，認證伺服器可以經由認證器與UE執行EAP程序。EAP程序可以至少部分基於在認證伺服器和UE之間交換的一組認證憑證。在某些實例中，可以使用參考圖9描述的EAP管理器935來執行方塊1605的操作。

【0153】 在方塊1610處，如上參考圖5所描述的，作為執行EAP程序的一部分，認證伺服器可以推導MSK和EMSK，該MSK和該EMSK至少部分基於認證憑證和第一組參數。在一些實例中，第一組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在某些實例中，可以使用參考圖9描述的EAP管理器935來執行方塊1610的操作。

【0154】 在方塊1615處，如上參考圖5所描述的，認證伺服器可以決定與認證器相關聯的網路類型。在一些實例中，所決定的網路類型可以包括蜂巢網路類型或非蜂巢網路類型（例如，WLAN類型）。在某些實例中，可以使用參考圖9描述的網路類型辨識器940來執行方塊1615的操作。

【0155】 在方塊1620處，如上參考圖5所描述的，認證伺服器可以至少部分基於MSK或EMSK與網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰。當所決定的網路類型包括蜂巢網路類型時，並且在一些實例中，第二組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、認證伺服器和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。在某些實例中，可以使用參考圖9描述的網路金鑰推導器945來執行方塊1620的操作。

【0156】 在方塊1625處，如上參考圖5所描述的，認證伺服器可以經由秘密頻道向認證器發送安全金鑰。在某些實例中，可以使用參考圖9描述的網路金鑰安裝器950來執行方塊1625的操作。

【0157】 圖17示出根據本案內容的各個態樣的用於無線通訊的方法1700的流程圖。如參考圖1-5和11-13所描述的，可以由蜂巢網路或其組件執行方法1700的操作。在一些實例中，可以由參考圖11-13描述的通訊管理器執行方法1700的操作。在一些實例中，蜂巢網路（或其一或多個節點）可以執行用於控制該蜂巢網路的功能組件執行下面描述的功能的代碼集。補充地或者作為替代，蜂巢網路（或其一或多個節點）可以使用專用硬體執行下面描述的功能的態樣。

【0158】 在方塊1705處，如上參考圖5所描述的，蜂巢網路可以從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK可以至少部分基於一組認證憑證和第二組參數。該認證憑證可以在EAP程序期間在UE和認證伺服器之間交換。在一些實例中，第一組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、UE和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，第二組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。在某些實例中，可以使用參考圖11描述的網路金鑰管理器1135來執行方塊1705的操作。

【0159】 在方塊1710處，如上參考圖5所描述的，蜂巢網路可以至少部分基於第一安全金鑰與UE執行至少一個認證程序。在某些實例中，可以使用參考圖11描述的UE認證器140來執行方塊1710的操作。

【0160】 圖18示出根據本案內容的各個態樣的用於無線通訊的方塊1800的流程圖。如參考圖1-5和11-13所描述的，可以由蜂巢網路或其組件執行方法1800的操作。在一些實例中，可以由參考圖11-13描述的通訊管理器執行方法1800的操作。在一些實例中，蜂巢網路（或其一或多個節點）可以執行用於控制該蜂巢網路的功能組

件執行下面描述的功能的代碼集。補充地或者作為替代，蜂巢網路（或其一或多個節點）可以使用專用硬體執行下面描述的功能的態樣。

【0161】 在方塊1805處，如上參考圖5所描述的，蜂巢網路可以從認證伺服器接收第一安全金鑰，該第一安全金鑰至少部分基於EMSK和第一組參數。該EMSK可以至少部分基於一組認證憑證和第二組參數。該認證憑證可以在EAP程序期間在UE和認證伺服器之間交換。在一些實例中，第一組參數可以包括蜂巢網路的辨識符、至少一個蜂巢網路特定參數、UE和蜂巢網路之間交換的至少一個參數或者它們的組合。在一些實例中，第二組參數可以包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的組合。在一些實例中，蜂巢網路可以包括以下各項中的至少一項：5G網路、4G網路、LTE網路、LTE-A網路、3G網路或者它們的組合。在某些實例中，可以使用參考圖11描述的網路金鑰管理器1135來執行方塊1805的操作。

【0162】 在方塊1810處，蜂巢網路可以至少部分基於第一安全金鑰與UE執行至少一個認證程序。如上參考圖5所描述的，與UE執行至少一個認證程序可以包括推導蜂巢網路的網路節點的第二安全金鑰。第二安全金鑰可以至少部分基於第一安全金鑰和第三組參數。在一些實例中，第三組參數可以包括網路節點的辨識符、至少一個網路節點特定參數、UE和網路節點之間交換的至少一個參

數或者它們的組合。在某些實例中，可以使用參考圖11描述的UE認證器140，或參考圖12描述的網路節點金鑰推導器1205來執行方塊1810的操作。

【0163】 在方塊1815處，如上參考圖5所描述的，蜂巢網路可以至少部分基於第二安全金鑰，經由網路節點與UE通訊。在某些實例中，可以使用參考圖12描述的UE通訊管理器1210來執行方塊1815的操作。

【0164】 應當注意的是，上面描述的方法說明了本案內容中描述的技術的可能實施方式。在一些實例中，方法的操作可以用不同循序執行或者包括不同操作。

【0165】 本案描述的技術可以用於各種無線通訊系統，例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其他系統。術語「系統」和「網路」通常互換使用。CDMA系統可以實現諸如CDMA 2000、通用陸地無線電存取（UTRA）等的無線電技術。CDMA 2000涵蓋IS-2000、IS-95和IS-856標準。IS-2000版本0和A可以被稱為CDMA 2000 1X、1X等等。IS-856（TIA-856）可以被稱為CDMA 2000 1xEV-DO、高速封包資料（HRPD）等。UTRA包括寬頻CDMA（W-CDMA）和CDMA的其他變型。TDMA系統可以實現諸如行動通訊全球系統（GSM）之類的無線電技術。OFDMA系統可以實現例如超行動寬頻（UMB）、進化型UTRA（E-UTRA）、IEEE 802.11（Wi-Fi）、IEEE 802.16（WiMAX）、IEEE 802.20、快閃

OFDMTM等的無線電技術。UTRA和E-UTRA是通用行動電信系統（UMTS）的一部分。3GPP LTE和LTE-A是使用E-UTRA的UMTS的新版本。在來自名為3GPP的組織的文件中描述了UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM。在來自名為「第3代合作夥伴項目2」（3GPP2）的組織的文件中描述了CDMA 2000和UMB。本案中描述的技術可以用於上面提及的系統和無線電技術以及其他系統和無線電技術，包括非授權頻寬或共享頻寬上的蜂巢（例如，LTE）通訊。然而，上面的描述以舉例為目的描述了LTE/LTE-A系統，並且在上面大部分描述中使用了LTE術語，但是這些技術可應用於LTE/LTE-A應用以外。

【0166】 上面結合附圖闡述的詳細描述描述了實例，但是不表示可以被實現或在請求項的範疇內的所有例子。術語「示例性」在本說明書中使用時意指「用作實例、實例或說明」，而不是「優選的」或「比其他實例更具優勢的」。出於提供對所描述技術的理解的目的，詳細描述包括具體細節。然而，在沒有這些具體細節的情況下，亦可以實踐這些技術。在一些實例中，公知的結構和裝置以方塊圖的形式示出，以便於避免使得所描述的實例的構思不清楚。

【0167】 資訊和信號可以使用各種不同的技術和方法中的任意一種來表示。例如，在貫穿上面的描述中可能提及的資料、指令、命令、資訊、信號、位元、符號和碼片

可以用電壓、電流、電磁波、磁場或粒子、光場或粒子或其任意組合來表示。

【0168】 利用被設計為執行本案所描述的功能的通用處理器、數位訊號處理器（DSP）、ASIC、FPGA或其他可程式設計邏輯裝置、個別閘門或者電晶體邏輯裝置、個別硬體組件或者其任意組合可以實現或執行結合本案揭示內容所描述的各種說明性方塊和組件。通用處理器可以是微處理器，或者，該處理器可以是任何傳統的處理器、控制器、微控制器或者狀態機。處理器亦可以被實現為計算設備的組合，例如，DSP和微處理器的組合、多個微處理器、結合DSP核心一或多個微處理器或者任何其他此類結構。

【0169】 本案描述的功能可以用硬體、由處理器執行的軟體、韌體或其任意組合來實現。若用由處理器執行的軟體實現，則可以將這些功能作為一或多個指令或代碼儲存在電腦可讀取媒體上或者經由電腦可讀取媒體來發送。其他實例和實施方式在本案內容和所附請求項的範疇和精神內。例如，由於軟體的本質，上面描述的功能可以使用由處理器執行的軟體、硬體、韌體、硬接線或其任意組合來實現。實現功能的組件亦可以實體地位於各種位置處，包括為分散式的，從而在不同的實體位置處實現部分功能。另外，如本案所使用的，包括在申請專利範圍中，術語「或者」當用於兩個或更多個項目的列表中時，意指其自身可以採用所列項目中的任何一個，或者可以採用所列

項目的兩個或更多個項目的任意組合。例如，若組合被描述為包含分量A、B及/或C，則該組合可以只包含A；只包含B；只包含C；聯合包含A和B；聯合包含A和C；聯合包含B和C或者聯合包含A、B和C。另外，如本案所使用的，包括在申請專利範圍中，項目列表（例如，以諸如「……中的至少一個」或「……中的一或多個」之類的措詞描述的項目列表）中所使用的「或者」指示分離的列表，從而例如「A、B或C中的至少一個」的列表指A或B或C或AB或AC或BC或ABC（亦即，A和B和C）。

【0170】 電腦可讀取媒體包括電腦儲存媒體和通訊媒體二者，其中通訊媒體包括便於從一個地方向另一個地方傳送電腦程式的任何媒體。儲存媒體可以是通用電腦或專用電腦能夠存取的任何可用媒體。經由舉例而非限制的方式，電腦可讀取媒體可以包括RAM、ROM、EEPROM、快閃記憶體、CD-ROM或其他光碟存放裝置、磁碟存放裝置或其他磁存放裝置、或者能夠用於攜帶或儲存具有指令或資料結構形式的期望的程式碼單元並能夠由通用電腦或專用電腦或通用處理器或專用處理器存取的任何其他媒體。另外，可以將任何連接適當地稱作電腦可讀取媒體。例如，若軟體是使用同軸電纜、光纖光纜、雙絞線、數位用戶線（DSL）或者諸如紅外線、無線電和微波之類的無線技術從網站、伺服器或其他遠端源發送的，則同軸電纜、光纖光纜、雙絞線、DSL或者諸如紅外線、無線電和微波之類的無線技術包括在媒體的定義中。如本案

所使用的，磁碟和光碟包括壓縮光碟（CD）、鐳射光碟、光碟、數位多功能光碟（DVD）、軟碟和藍光光碟，其中磁碟通常磁性地複製資料，而光碟則用鐳射來光學地複製資料。上面的組合亦應當被包括在電腦可讀取媒體的範疇之內。

【0171】 提供前面對揭示內容的描述以使本發明所屬領域中具有通常知識者能夠實施或使用本案內容。對本發明所屬領域中具有通常知識者而言，對本案內容的各種修改將是顯而易見的，並且可以將本案所定義的一般性原理應用於其他變型而不脫離本案內容的精神或範疇。因此，本案內容並不意欲要受限於本案描述的實例和設計，而是要符合與本案所揭示的原理和新穎性特徵相一致的最廣泛的範疇。

【符號說明】

【0172】

100 無線通訊系統

105 網路存取設備

110 地理覆蓋區域

115 UE

115-a UE

115-b UE

115-c UE

115-d UE

115-e UE

115-f UE

122 通訊鏈路

125 網路存取設備控制器

130 核心網路

132 回載鏈路

134 回載鏈路

135 網路節點

140 無線通訊管理器

205 歸屬蜂巢網路

205-a 蜂巢網路

205-b 蜂巢網路

205-c 蜂巢網路

205-d 蜂巢網路

205-e 蜂巢網路

210 歸屬使用者平面閘道（H-UP-GW）

210-a V-UP-GW

210-b H-UP-GW

210-c V-UP-GW

215 V-CP-CN

215-a V-CP-CN

220 RAN

220-a RAN

220-b RAN

235 第一認證器

235-a 第二認證器

235-b 第一認證器

235-c 第二認證器

235-d 認證器

240 認證憑證庫和處理功能單元（ARPF）

240-a 認證憑證庫和處理功能單元（ARPF）

245 認證伺服器

245-a 認證伺服器

245-b 認證伺服器

245-c 認證伺服器

245-d 認證伺服器

300 金鑰層級

305 K根金鑰

310 推導金鑰

315 K_{SEAF}錨定通信期金鑰

320 K_{CP-CN}金鑰

325 K_{UP-GW}金鑰

330 K_{NASenc}金鑰

335 K_{NASint}金鑰

340 $K_{UP-GWenc}$金鑰

345 $K_{UP-GWint}$金鑰

350 $K_{AN/NH}$金鑰

355 K_{UPint}金鑰

360 K_{UPenc}金鑰

365 K_{RRCint}金鑰

370 K_{RRCenc}金鑰

400 無線通訊系統

405 非蜂巢網路

410 非蜂巢存取節點

500 訊息流

505 流程

510 流程

515 流程

520 流程

525 流程

530 流程

535 流程

540 流程

545 流程

550 流程

555 流程

600 方塊圖

610 接收器

620 無線通訊管理器

630 發射器

635 EAP管理器

635-a EAP管理器

640 網路類型辨識器

640-a 網路類型辨識器

645 網路認證器

645-a 網路認證器

700 方塊圖

705 網路金鑰推導器

710 網路節點金鑰推導器

715 蜂巢網路通訊管理器

720 無線通訊管理器

800 無線通訊系統

805 無線通訊管理器

810 記憶體

815 電腦可執行軟體

820 處理器

825 收發機

830 天線

900 方塊圖

910 接收器

920 認證管理器

930 發射器

935 EAP管理器

940 網路類型辨識器

945 網路金鑰推導器

950 網路金鑰安裝器

1000 方塊圖

1005 認證管理器

1010 記憶體

1015 電腦可執行軟體

1020 處理器

1025 認證介面

1100 方塊圖

1105 網路節點

1105-a 網路節點

1110 接收器

1120 通訊管理器

1130 發射器

1135 網路金鑰管理器

1135-a 網路金鑰管理器

1140 UE認證器

1140-a UE認證器

1200 方塊圖

1205 網路節點金鑰推導器

1210 UE通訊管理器

1220 通訊管理器

1300 示意圖

1305 通訊管理器

1310 記憶體

1315 電腦可執行軟體

1320 處理器

1325 認證介面

1400 方法

1405 方塊

1410 方塊

1415 方塊

1420 方塊

1500 方法

1505 方塊

1510 方塊

1515 方塊

1520 方塊

1525 方塊

1530 方塊

1535 方塊

1540 方塊

1600 方法

1605 方塊

1610 方塊

1615 方塊

1620 方塊

1625 方塊

1700 方法

1705 方塊

1710 方塊

１８００　方塊

１８０５　方塊

１８１０　方塊

１８１５　方塊

【生物材料寄存】

【０１７３】　國內寄存資訊(請依寄存機構、日期、號碼順序註記)

無

【０１７４】　國外寄存資訊(請依寄存國家、機構、日期、號碼順序註記)

無

【發明申請專利範圍】

【第1項】 一種用於一使用者設備（UE）處的無線通訊的方法，包括以下步驟：

經由一認證器與一認證伺服器執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；及

至少部分基於該所決定的網路類型，與該認證器執行至少一個認證程序，該至少一個認證程序係基於該MSK或該EMSK與該所決定的網路類型的一關聯。

【第2項】 如請求項1之方法，其中該所決定的網路類型包括一蜂巢網路類型，並且與該認證器執行該至少一個認證程序包括以下步驟：

推導一蜂巢網路的一第一安全金鑰，該第一安全金鑰至少部分基於該EMSK和一第二組參數。

【第3項】 如請求項2之方法，其中該第二組參數包括：該蜂巢網路的一辨識符、至少一個蜂巢網路特定參數、該UE和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第4項】 如請求項2之方法，其中與該認證器執行該至少一個認證程序包括以下步驟：

推導該蜂巢網路的一網路節點的一第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和一第三組參數；及

至少部分基於該第二安全金鑰，經由該網路節點與該蜂巢網路通訊。

【第5項】 如請求項4之方法，其中該第三組參數包括：該網路節點的一辨識符、至少一個網路節點特定參數、該UE和該網路節點之間交換的至少一個參數或者它們的一組合。

【第6項】 如請求項1之方法，其中該MSK及該EMSK進一步至少部分地基於一第一組參數，該第一組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第7項】 如請求項2之方法，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第四代（4G）網路、一長期進化（LTE）網路、一高級LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第8項】 如請求項1之方法，其中該所決定的網路類型是一非蜂巢網路類型，並且與該認證器執行該至少一個認證程序包括以下步驟：

推導一非蜂巢網路的一第一安全金鑰，該第一安全金鑰至少部分基於該MSK和一第二組參數。

【第9項】 一種用於一使用者設備（UE）處的無線通訊的裝置，包括：

用於經由一認證器與一認證伺服器執行一擴展認證協定（EAP）程序的單元，該EAP程序至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證；

用於作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK）的單元，該MSK和該EMSK至少部分基於該認證憑證；

用於決定與該認證器相關聯的一網路類型的單元；及

用於至少部分基於該所決定的網路類型，與該認證器執行至少一個認證程序的單元，該至少一個認證程序係基於該MSK或該EMSK與該所決定的網路類型的一關聯。

【第10項】 一種用於一使用者設備（UE）處的無線通訊的裝置，包括：

一處理器；及

與該處理器電子通訊的記憶體；

其中該處理器和該記憶體被配置為：

經由一認證器與一認證伺服器執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；及

至少部分基於該所決定的網路類型，與該認證器執行至少一個認證程序，該至少一個認證程序係基於該MSK或該EMSK與該所決定的網路類型的一關聯。

【第11項】 如請求項10之裝置，其中該所決定的網路類型包括一蜂巢網路類型，並且與該認證器執行該至少一個認證程序包括被配置為執行以下操作的該處理器和該記憶體：

推導一蜂巢網路的一第一安全金鑰，該第一安全金鑰至少部分基於該EMSK和一第二組參數。

【第12項】 如請求項11之裝置，其中該第二組參數包括：該蜂巢網路的一辨識符、至少一個蜂巢網路特定

參數、該UE和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第13項】 如請求項11之裝置，其中與該認證器執行該至少一個認證程序包括被配置為執行以下操作的該處理器和該記憶體：

推導該蜂巢網路的一網路節點的一第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和一第三組參數；及

至少部分基於該第二安全金鑰，經由該網路節點與該蜂巢網路通訊。

【第14項】 如請求項13之裝置，其中該第三組參數包括：該網路節點的一辨識符、至少一個網路節點特定參數、該UE和該網路節點之間交換的至少一個參數或者它們的一組合。

【第15項】 如請求項10之裝置，其中該MSK及該EMSK進一步至少部分地基於一第一組參數，該第一組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第16項】 如請求項11之裝置，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第四代（4G）網路、一長期進化（LTE）網路、一高級

LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第17項】 如請求項10之裝置，其中該所決定的網路類型是一非蜂巢網路類型，並且與該認證器執行該至少一個認證程序包括：

推導一非蜂巢網路的一第一安全金鑰，該第一安全金鑰至少部分基於該MSK和一第二組參數。

【第18項】 一種儲存用於一使用者設備（UE）處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體，該代碼可由一處理器執行以進行以下操作：

經由一認證器與一認證伺服器執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於在該UE和該認證伺服器之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；及

至少部分基於該所決定的網路類型，與該認證器執行至少一個認證程序，該至少一個認證程序係基於該MSK或該EMSK與所決定的網路類型的一關聯。

【第19項】 一種用於一認證伺服器處的無線通訊的方法，包括以下步驟：

經由一認證器與一使用者設備（UE）執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於該認證伺服器和該UE之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；

至少部分基於該MSK或該EMSK與該網路類型的關聯，並且至少部分基於一第二組參數，推導該所決定的網路類型的一安全金鑰；及

經由秘密頻道將該安全金鑰發送給該認證器。

【第20項】 如請求項19之方法，其中該MSK及該EMSK進一步至少部分地基於一第一組參數，該第一組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第21項】 如請求項19之方法，其中該所決定的網路類型包括一蜂巢網路類型，並且該第二組參數包括：一蜂巢網路的一辨識符、至少一個蜂巢網路特定參數、該認證伺服器和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第22項】 如請求項21之方法，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第

四代（4G）網路、一長期進化（LTE）網路、一高級LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第23項】 一種用於一認證伺服器處的無線通訊的裝置，包括：

用於經由一認證器與一使用者設備（UE）執行一擴展認證協定（EAP）程序的單元，該EAP程序至少部分基於該認證伺服器和該UE之間交換的一組認證憑證；

用於作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK）的單元，該MSK和該EMSK至少部分基於該認證憑證；

用於決定與該認證器相關聯的一網路類型的單元；

用於至少部分基於該MSK或該EMSK與該所決定的網路類型的一關聯，並且至少部分基於一第二組參數，推導該所決定的網路類型的一安全金鑰的單元；及

用於經由一秘密頻道將該安全金鑰發送給該認證器的單元。

【第24項】 一種用於認證伺服器處的無線通訊的裝置，包括：

一處理器；及

與該處理器電子通訊的記憶體；

其中該處理器和該記憶體被配置為：

經由一認證器與一使用者設備（UE）執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於該認證伺服器和該UE之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；

至少部分基於該MSK或該EMSK與該所決定網路類型的一關聯，並且至少部分基於一第二組參數，推導該所決定的網路類型的一安全金鑰；及

經由一秘密頻道將該安全金鑰發送給該認證器。

【第25項】 如請求項24之裝置，其中該MSK及該EMSK進一步至少部分地基於一第一組參數，該第一組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第26項】 如請求項24之裝置，其中該所決定的網路類型包括一蜂巢網路類型，並且該第二組參數包括：一蜂巢網路的一辨識符、至少一個蜂巢網路特定參數、該認證伺服器和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第27項】 如請求項26之裝置，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第四代（4G）網路、一長期進化（LTE）網路、一高級LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第28項】 一種儲存用於一認證伺服器處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體，該代碼可由一處理器執行以進行以下操作：

經由一認證器與一使用者設備（UE）執行一擴展認證協定（EAP）程序，該EAP程序至少部分基於該認證伺服器和該UE之間交換的一組認證憑證；

作為執行該EAP程序的一部分，推導一主通信期金鑰（MSK）和一擴展主通信期金鑰（EMSK），該MSK和該EMSK至少部分基於該認證憑證；

決定與該認證器相關聯的一網路類型；

至少部分基於該MSK或該EMSK與該所決定的網路類型的一關聯，並且至少部分基於一第二組參數，推導該所決定的網路類型的一安全金鑰；及

經由一秘密頻道將該安全金鑰發送給該認證器。

【第29項】 一種用於一蜂巢網路處的無線通訊的方法，包括以下步驟：

從一認證伺服器接收一第一安全金鑰，該第一安全金鑰至少部分基於一擴展主通信期金鑰（EMSK）和一第一組參數，該EMSK至少部分基於一組認證憑證和一第二組參數，該認證憑證是在一擴展認證協定（EAP）程序期間在一使用者設備（UE）和該認證伺服器之間交換的；及

至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【第30項】 如請求項29之方法，其中與該UE執行該至少一個認證程序包括：

推導該蜂巢網路的一網路節點的一第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和一第三組參數；及

至少部分基於該第二安全金鑰，經由該網路節點與該UE通訊。

【第31項】 如請求項30之方法，其中該第三組參數包括：該網路節點的一辨識符、至少一個網路節點特定參數、該UE和該網路節點之間交換的至少一個參數或者它們的一組合。

【第32項】 如請求項29之方法，其中該第一組參數包括：該蜂巢網路的一辨識符、至少一個蜂巢網路特定

參數、該UE和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第33項】 如請求項29之方法，其中該第二組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第34項】 如請求項29之方法，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第四代（4G）網路、一長期進化（LTE）網路、一高級LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第35項】 一種用於一蜂巢網路處的無線通訊的裝置，包括：

用於從一認證伺服器接收一第一安全金鑰的單元，該第一安全金鑰至少部分基於一擴展主通信期金鑰（EMSK）和一第一組參數，該EMSK至少部分基於一組認證憑證和一第二組參數，該認證憑證是在一擴展認證協定（EAP）程序期間在一使用者設備（UE）和該認證伺服器之間交換的；及

用於至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序的單元。

【第36項】 一種用於蜂巢網路處的無線通訊的裝置，包括：

一處理器；以及

與該處理器電子通訊的記憶體；

其中該處理器和該記憶體被配置為：

從一認證伺服器接收一第一安全金鑰，該第一安全金鑰至少部分基於一擴展主通信期金鑰（EMSK）和一第一組參數，該EMSK至少部分基於一組認證憑證和一第二組參數，該認證憑證是在一擴展認證協定（EAP）程序期間在一使用者設備（UE）和該認證伺服器之間交換的；及

至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【第37項】 如請求項36之裝置，其中與該UE執行該至少一個認證程序包括被配置為執行以下操作的該處理器和該記憶體：

推導該蜂巢網路的一網路節點的一第二安全金鑰，該第二安全金鑰至少部分基於該第一安全金鑰和一第三組參數；及

至少部分基於該第二安全金鑰，經由該網路節點與該UE通訊。

【第38項】 如請求項37之裝置，其中該第三組參數包括：該網路節點的一辨識符、至少一個網路節點特定

參數、該UE和該網路節點之間交換的至少一個參數或者它們的一組合。

【第39項】 如請求項36之裝置，其中該第一組參數包括：該蜂巢網路的一辨識符、至少一個蜂巢網路特定參數、該UE和該蜂巢網路之間交換的至少一個參數或者它們的一組合。

【第40項】 如請求項36之裝置，其中該第二組參數包括：至少一個辨識符、至少一個亂數、至少一個網路參數、至少一個UE參數或者它們的一組合。

【第41項】 如請求項36之裝置，其中該蜂巢網路包括以下各項中的至少一項：一第五代（5G）網路、一第四代（4G）網路、一長期進化（LTE）網路、一高級LTE（LTE-A）網路、一第三代（3G）網路或者它們的一組合。

【第42項】 一種儲存用於一蜂巢網路處的無線通訊的電腦可執行代碼的非暫時性電腦可讀取媒體，該代碼可由一處理器執行以進行以下操作：

從一認證伺服器接收一第一安全金鑰，該第一安全金鑰至少部分基於一擴展主通信期金鑰（EMSK）和一第一組參數，該EMSK至少部分基於一組認證憑證和一第二組參數，該認證憑證是在一擴展認證協定（

EAP）程序期間在一使用者設備（UE）和該認證伺服器之間交換的；及

至少部分基於該第一安全金鑰，與該UE執行至少一個認證程序。

【發明圖式】

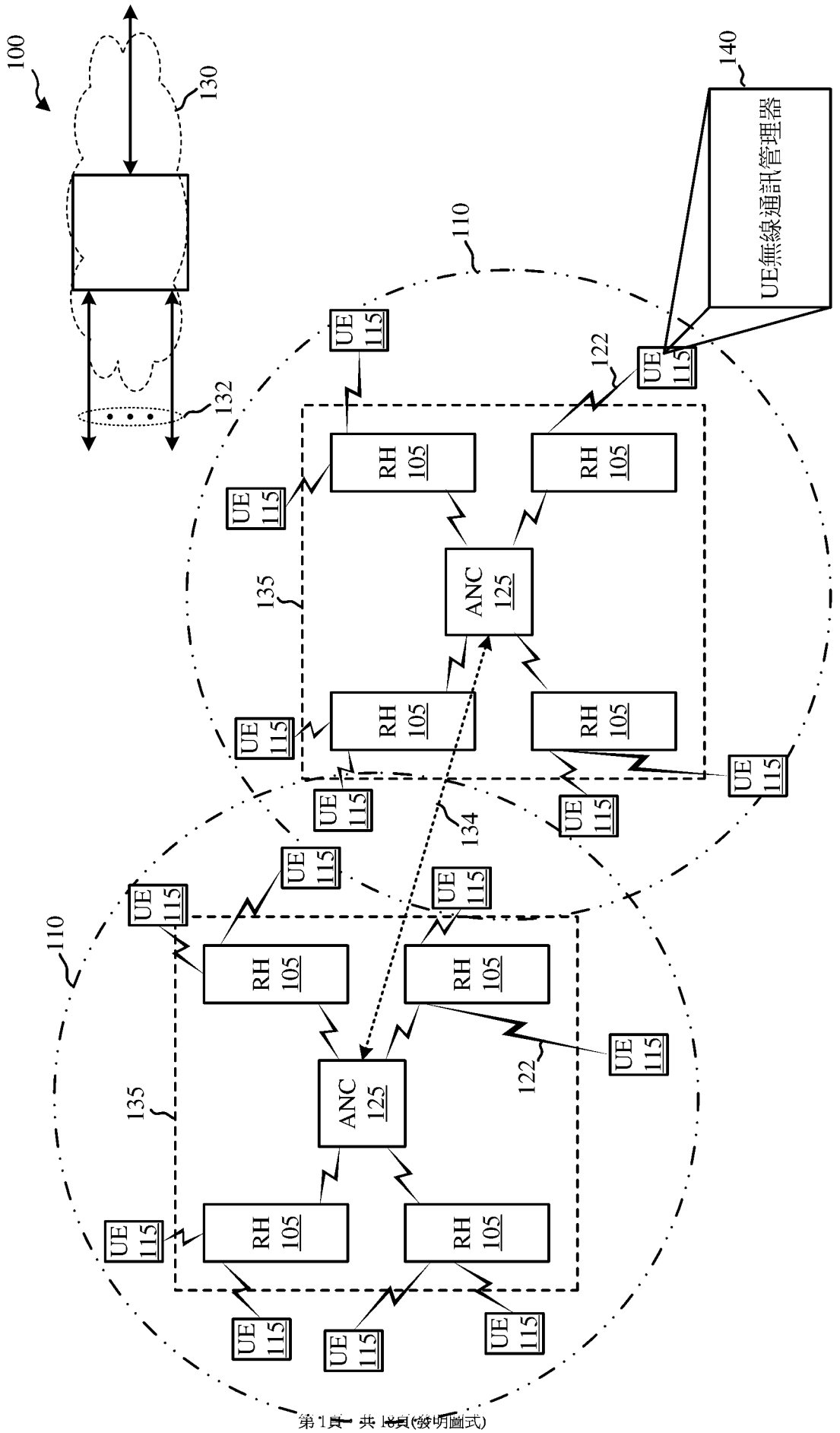

圖1

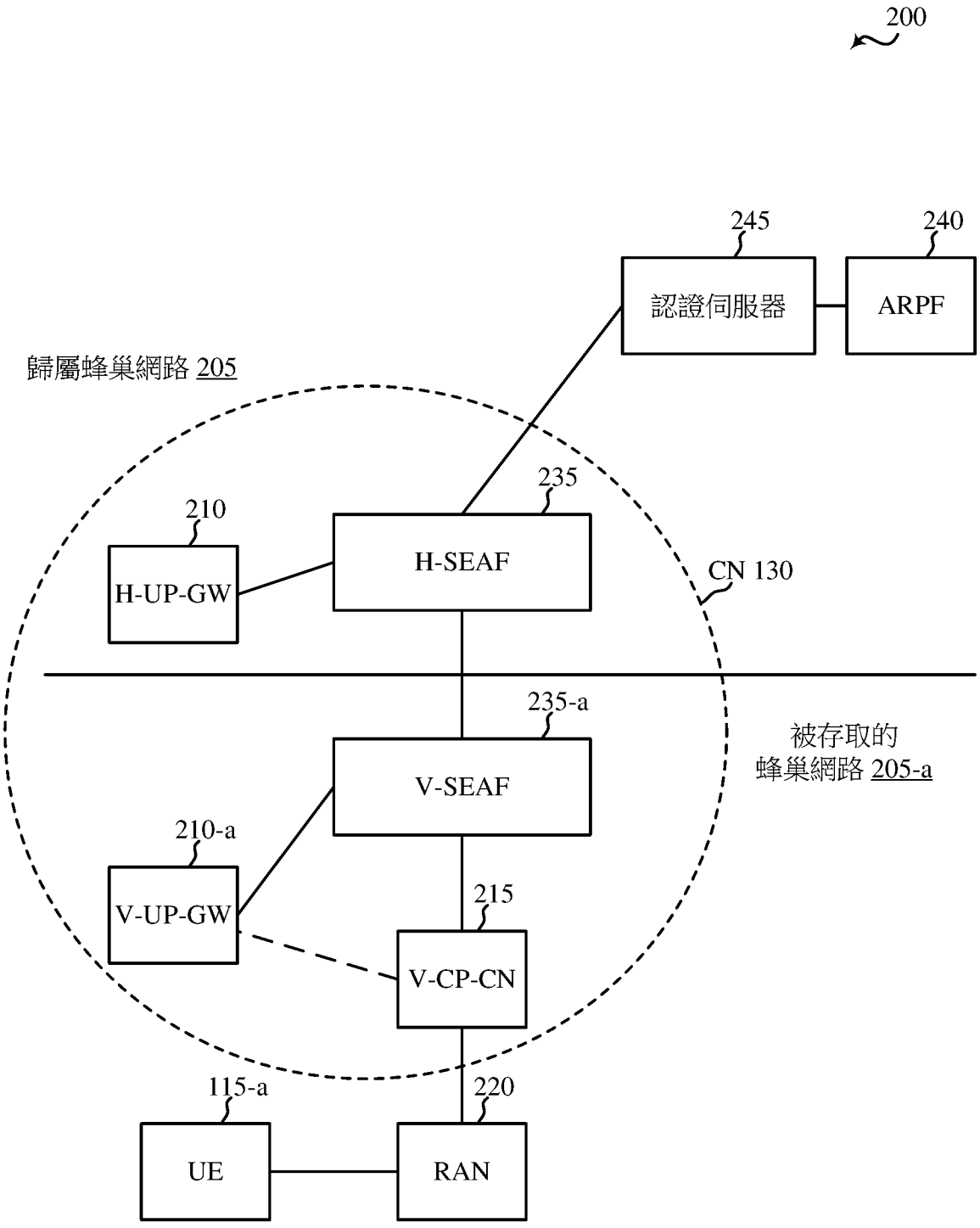
200
245
240
認證伺服器
ARPF
歸屬蜂巢網路 205
235
210
H-SEAF
H-UP-GW
CN 130
235-a
被存取的
蜂巢網路 205-a
V-SEAF
210-a
V-UP-GW
215
V-CP-CN
115-a
220
UE
RAN

圖2

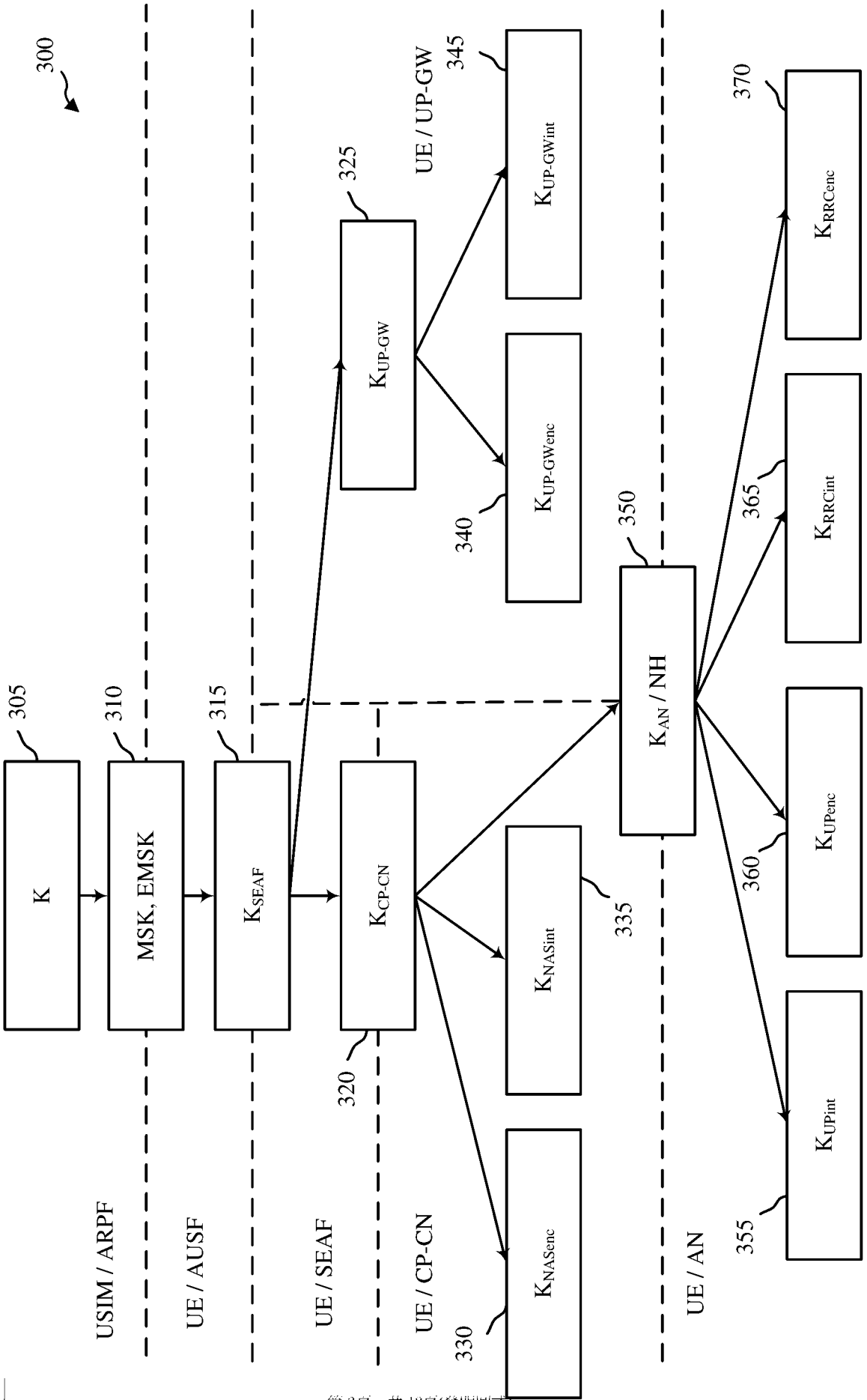
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
K
MSK, EMSK
K_{SEAF}
K_{CP-CN}
K_{UP-GW}
K_{NASenc}
K_{NASint}
$K_{UP-GWenc}$
$K_{UP-GWint}$
K_{AN} / NH
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}
USIM / ARPF
UE / AUSF
UE / SEAF
UE / CP-CN
UE / UP-GW
UE / AN

圖3

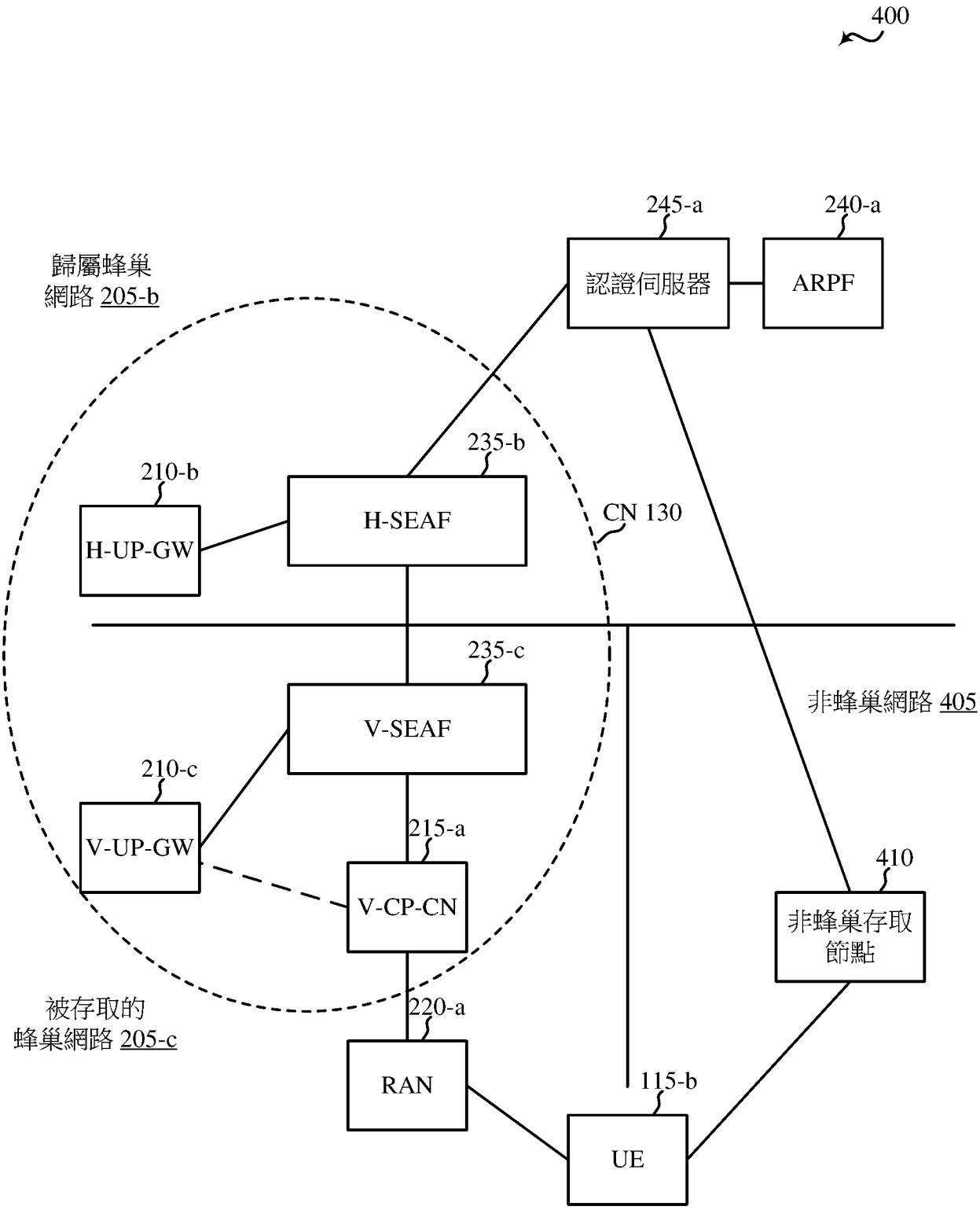
400
245-a
240-a
認證伺服器
ARPF
歸屬蜂巢
網路 205-b
235-b
210-b
H-SEAF
H-UP-GW
CN 130
235-c
V-SEAF
非蜂巢網路 405
210-c
V-UP-GW
215-a
410
V-CP-CN
非蜂巢存取
節點
被存取的
蜂巢網路 205-c
220-a
RAN
115-b
UE

圖4

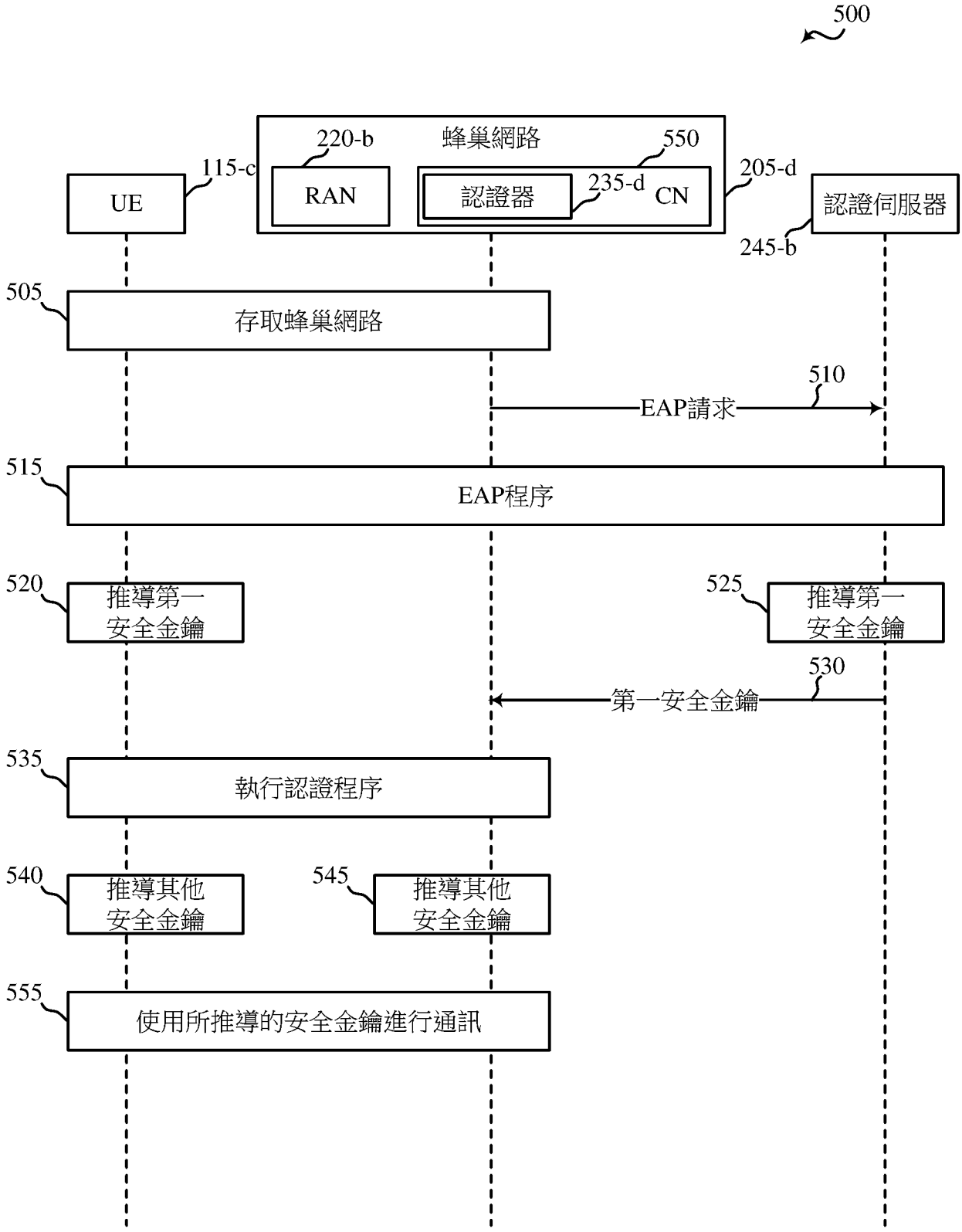
500
220-b
蜂巢網路
550
115-c
205-d
UE
RAN
認證器
235-d
CN
認證伺服器
245-b
505
存取蜂巢網路
510
EAP請求
515
EAP程序
520
推導第一
安全金鑰
525
推導第一
安全金鑰
530
第一安全金鑰
535
執行認證程序
540
推導其他
安全金鑰
545
推導其他
安全金鑰
555
使用所推導的安全金鑰進行通訊

圖5

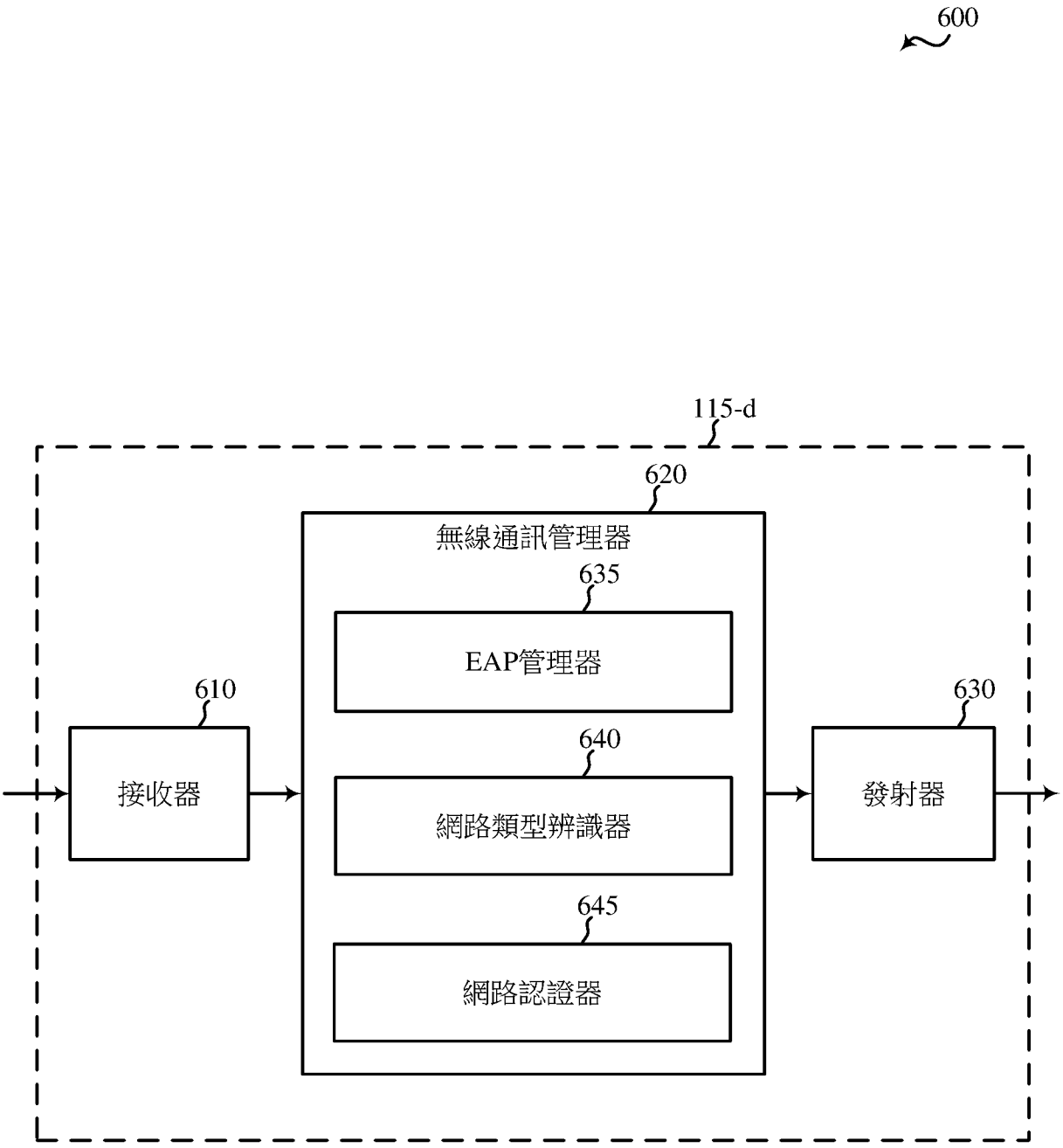
600
115-d
620
無線通訊管理器
635
EAP管理器
610
接收器
640
網路類型辨識器
630
發射器
645
網路認證器

圖6

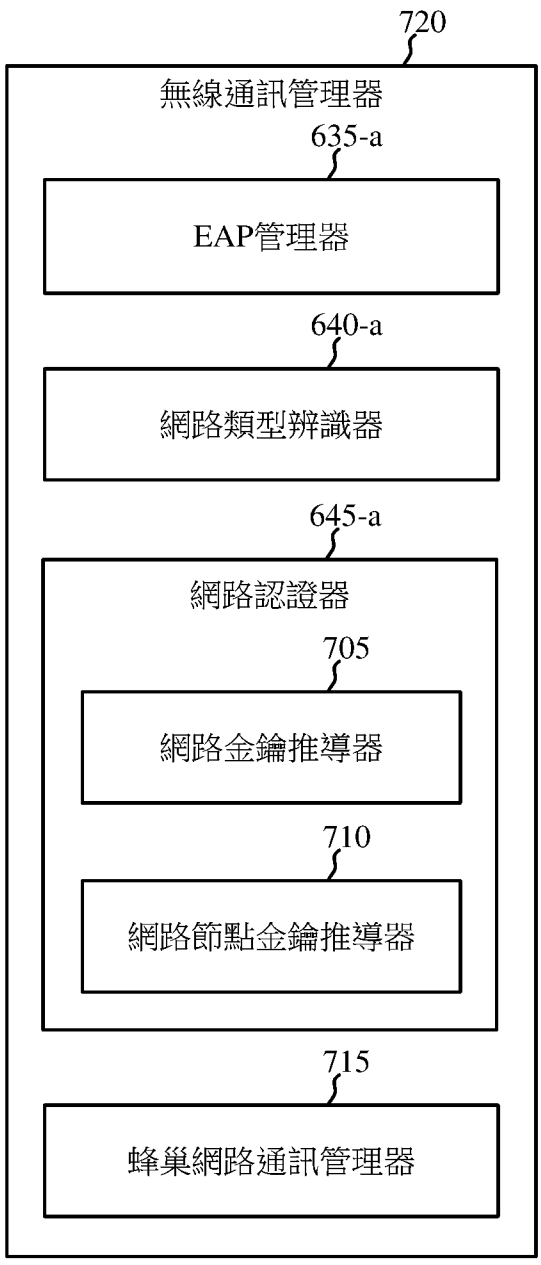
700
720
無線通訊管理器
635-a
EAP管理器
640-a
網路類型辨識器
645-a
網路認證器
705
網路金鑰推導器
710
網路節點金鑰推導器
715
蜂巢網路通訊管理器

圖7

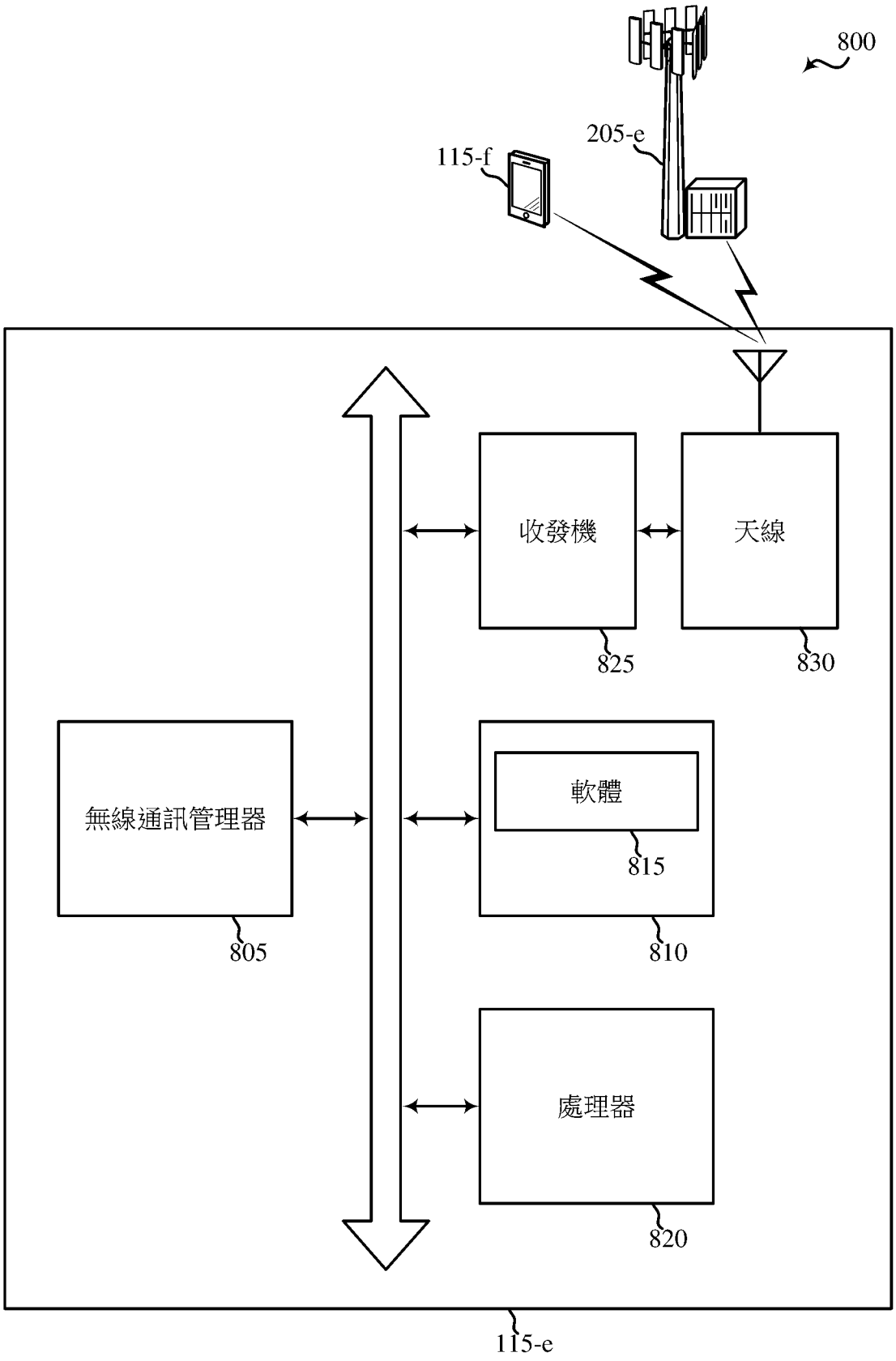
800
205-e
115-f
收發機
天線
825
830
無線通訊管理器
軟體
815
805
810
處理器
820
115-e

圖8

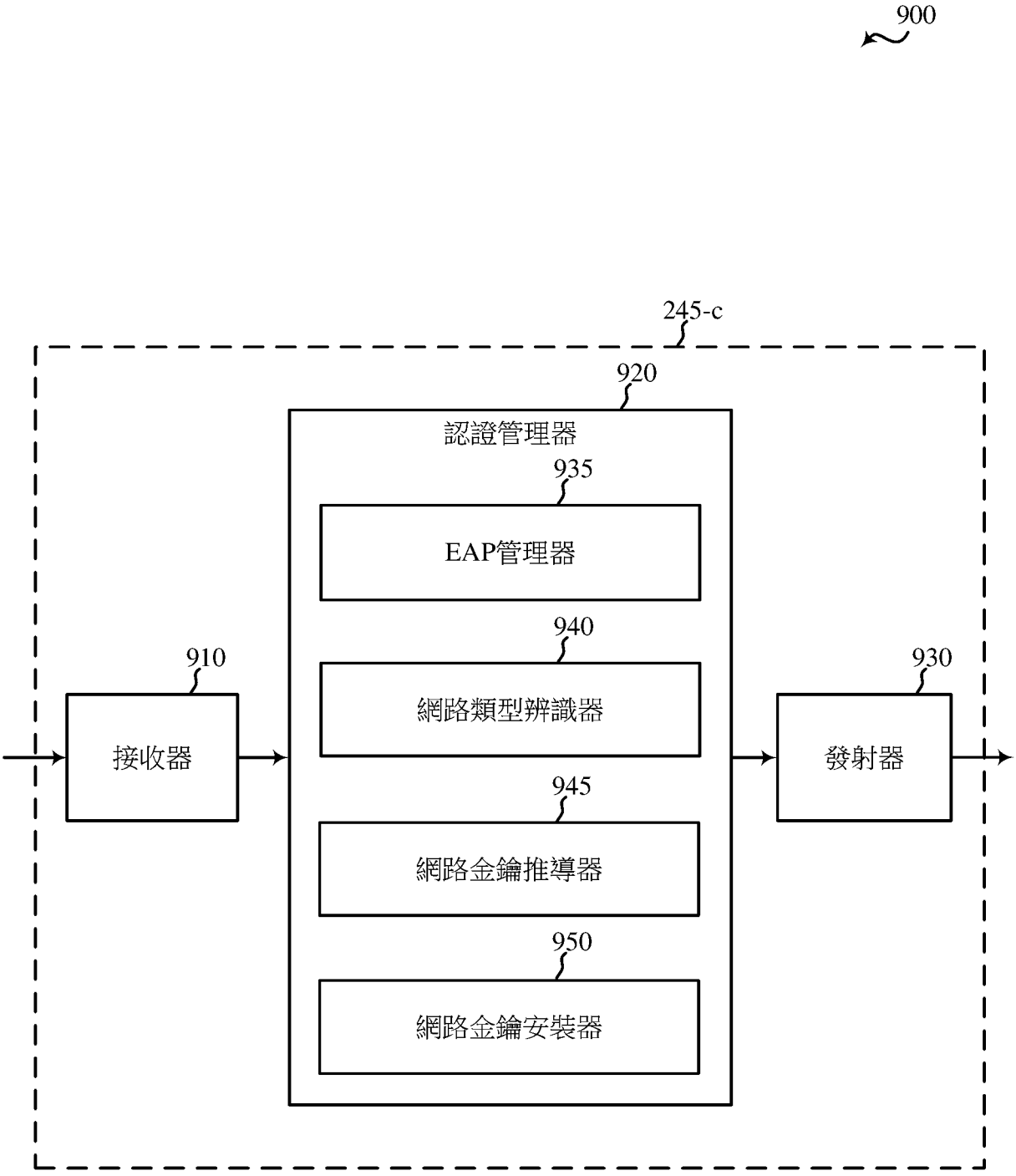
900
245-c
920
認證管理器
935
EAP管理器
940
網路類型辨識器
945
網路金鑰推導器
950
網路金鑰安裝器
910
接收器
930
發射器

圖9

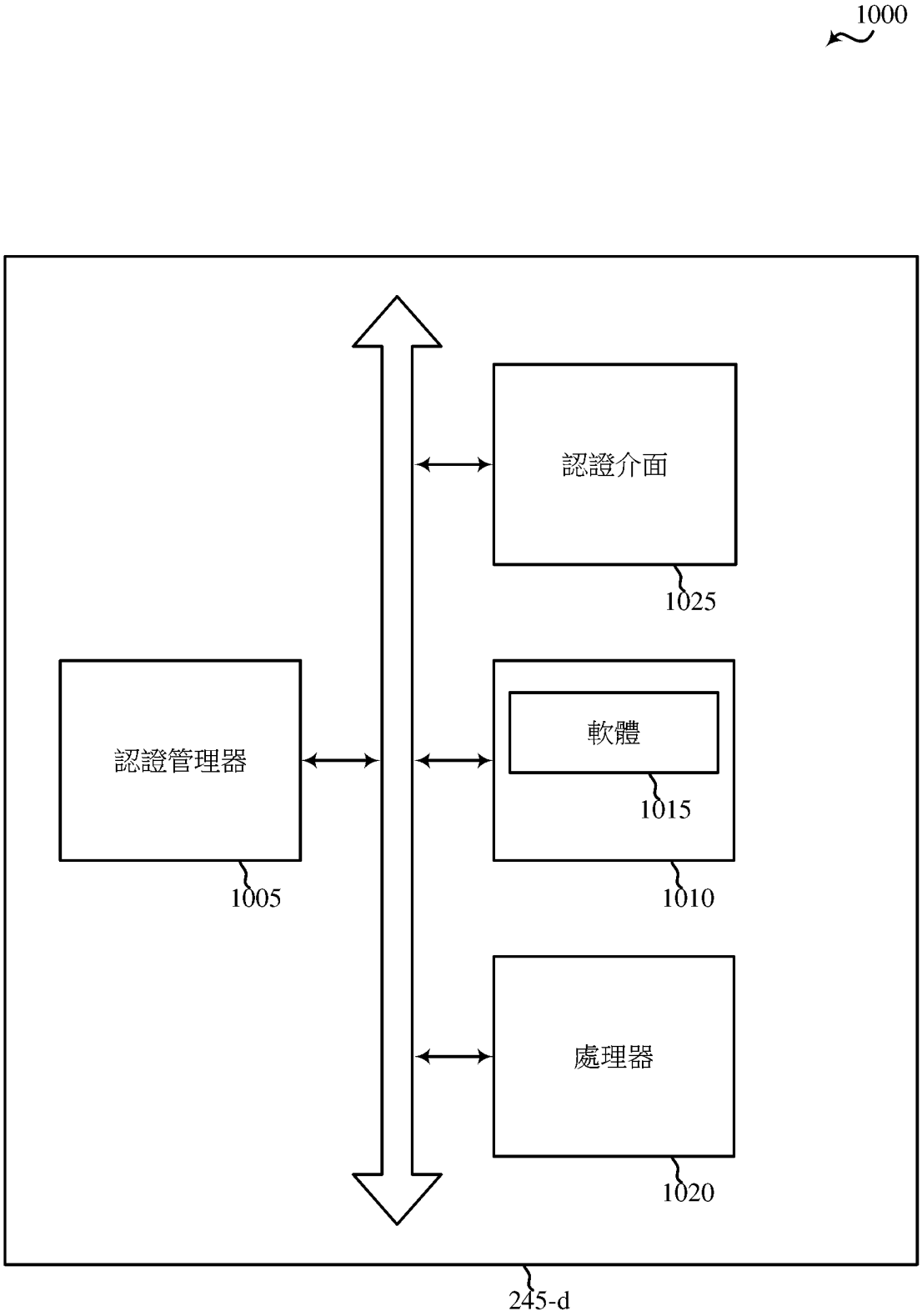

圖10

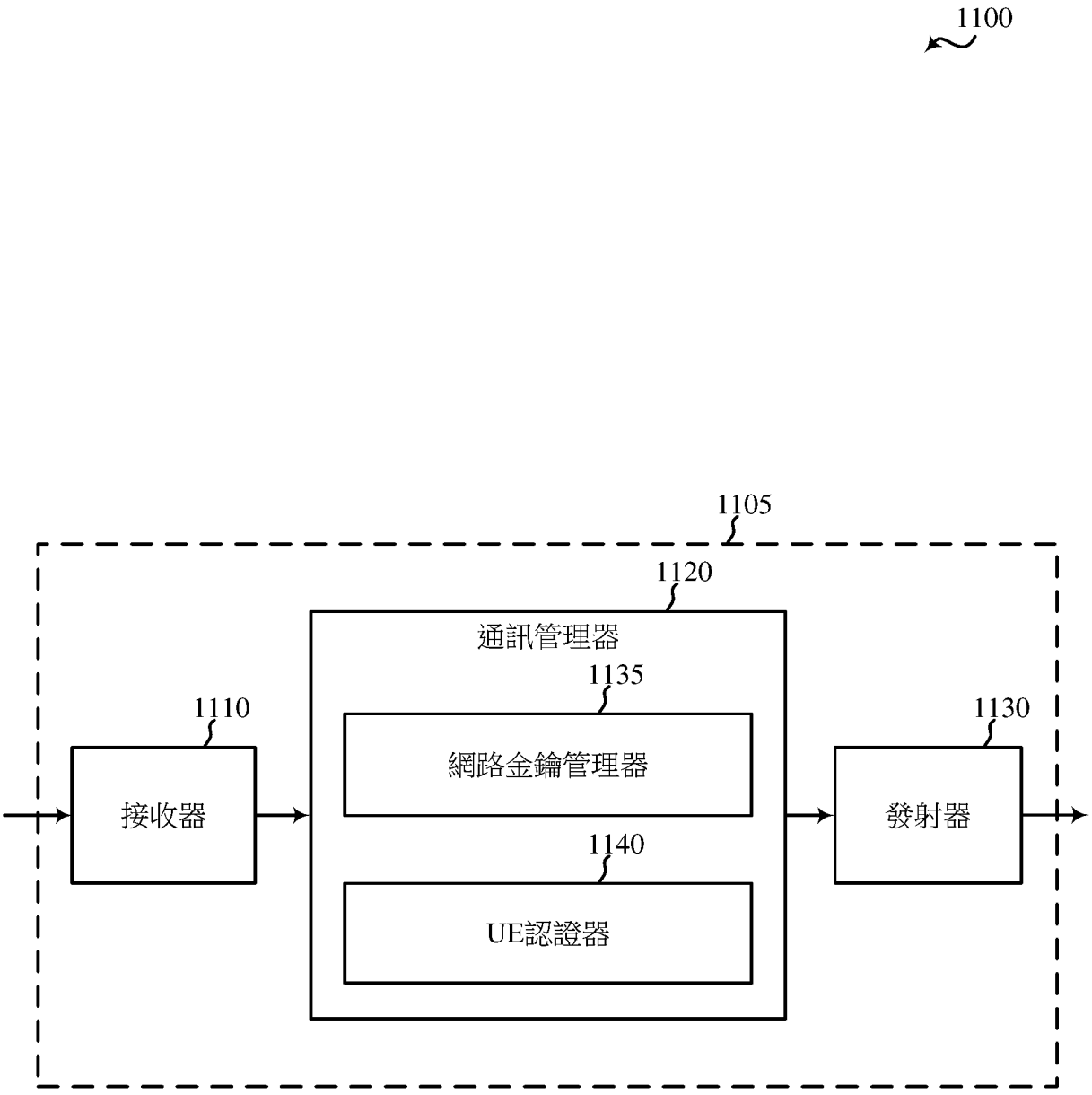
1100
1105
1120
通訊管理器
1135
網路金鑰管理器
1140
UE認證器
1110
接收器
1130
發射器

圖11

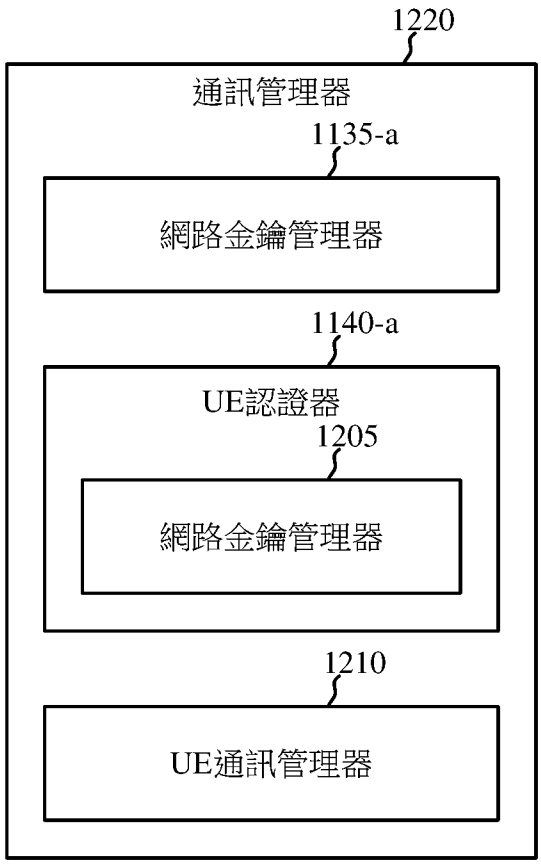
1200
1220
通訊管理器
1135-a
網路金鑰管理器
1140-a
UE認證器
1205
網路金鑰管理器
1210
UE通訊管理器

圖12

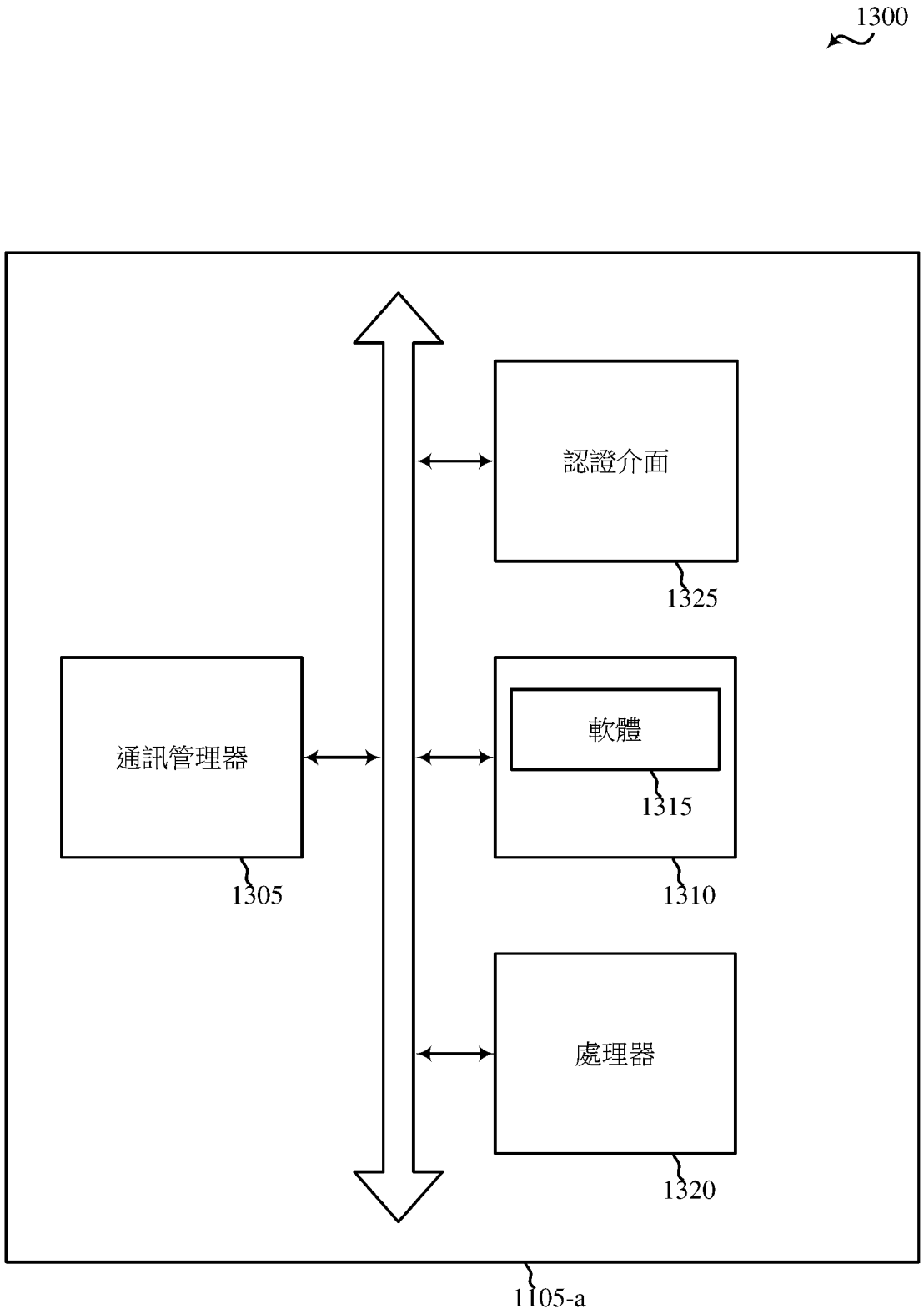

圖13

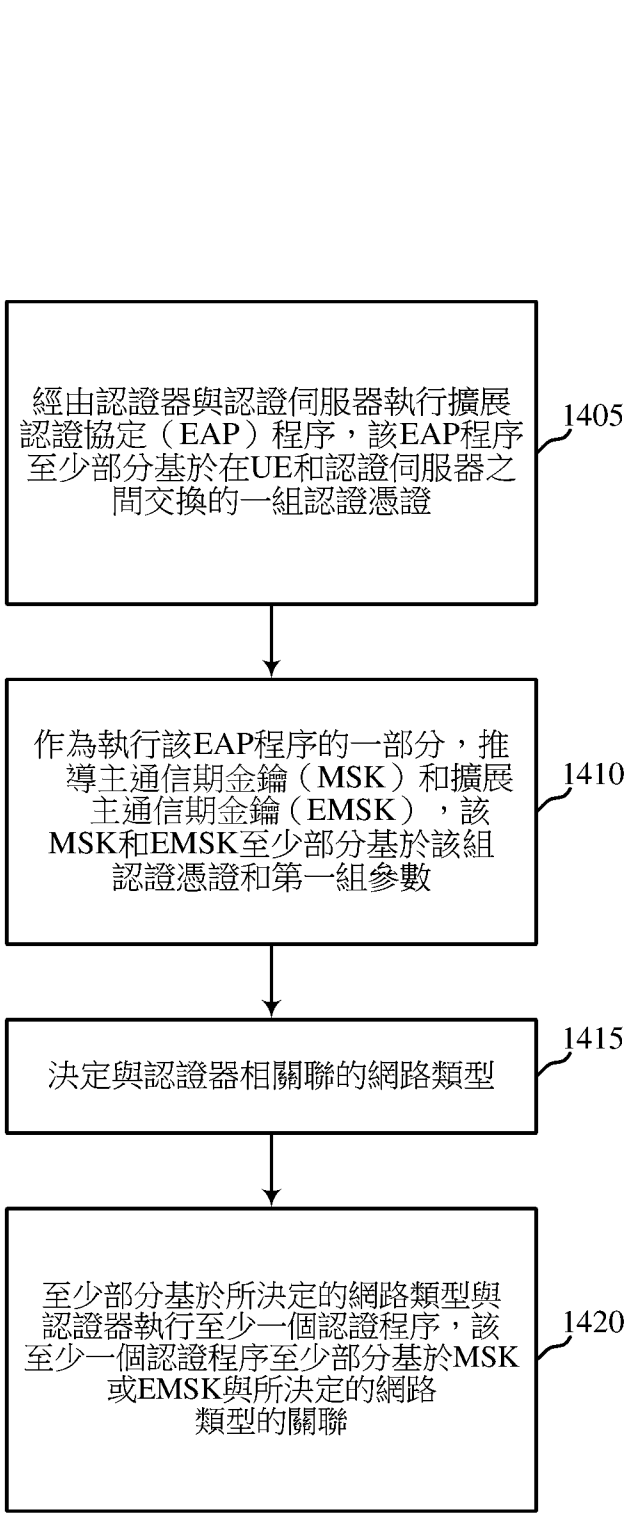
1400
經由認證器與認證伺服器執行擴展認證協定（EAP）程序，該EAP程序至少部分基於在UE和認證伺服器之間交換的一組認證憑證
1405
作為執行該EAP程序的一部分，推導主通信期金鑰（MSK）和擴展主通信期金鑰（EMSK），該MSK和EMSK至少部分基於該組認證憑證和第一組參數
1410
決定與認證器相關聯的網路類型
1415
至少部分基於所決定的網路類型與認證器執行至少一個認證程序，該至少一個認證程序至少部分基於MSK或EMSK與所決定的網路類型的關聯
1420

圖14

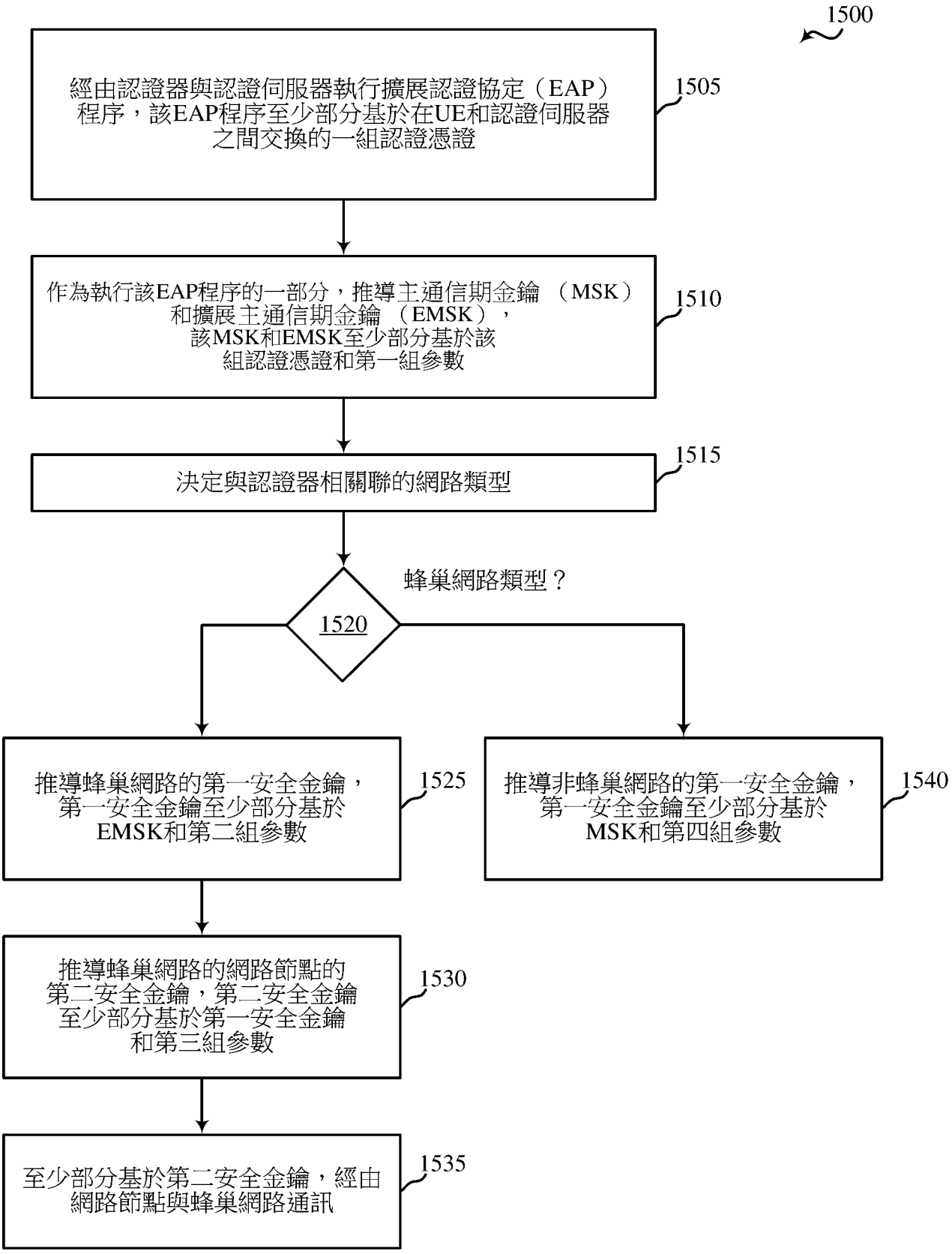
1500
經由認證器與認證伺服器執行擴展認證協定（EAP）程序，該EAP程序至少部分基於在UE和認證伺服器之間交換的一組認證憑證
1505
作為執行該EAP程序的一部分，推導主通信期金鑰 （MSK）和擴展主通信期金鑰 （EMSK），該MSK和EMSK至少部分基於該組認證憑證和第一組參數
1510
決定與認證器相關聯的網路類型
1515
蜂巢網路類型？
1520
推導蜂巢網路的第一安全金鑰，第一安全金鑰至少部分基於EMSK和第二組參數
1525
推導非蜂巢網路的第一安全金鑰，第一安全金鑰至少部分基於MSK和第四組參數
1540
推導蜂巢網路的網路節點的第二安全金鑰，第二安全金鑰至少部分基於第一安全金鑰和第三組參數
1530
至少部分基於第二安全金鑰，經由網路節點與蜂巢網路通訊
1535

圖15

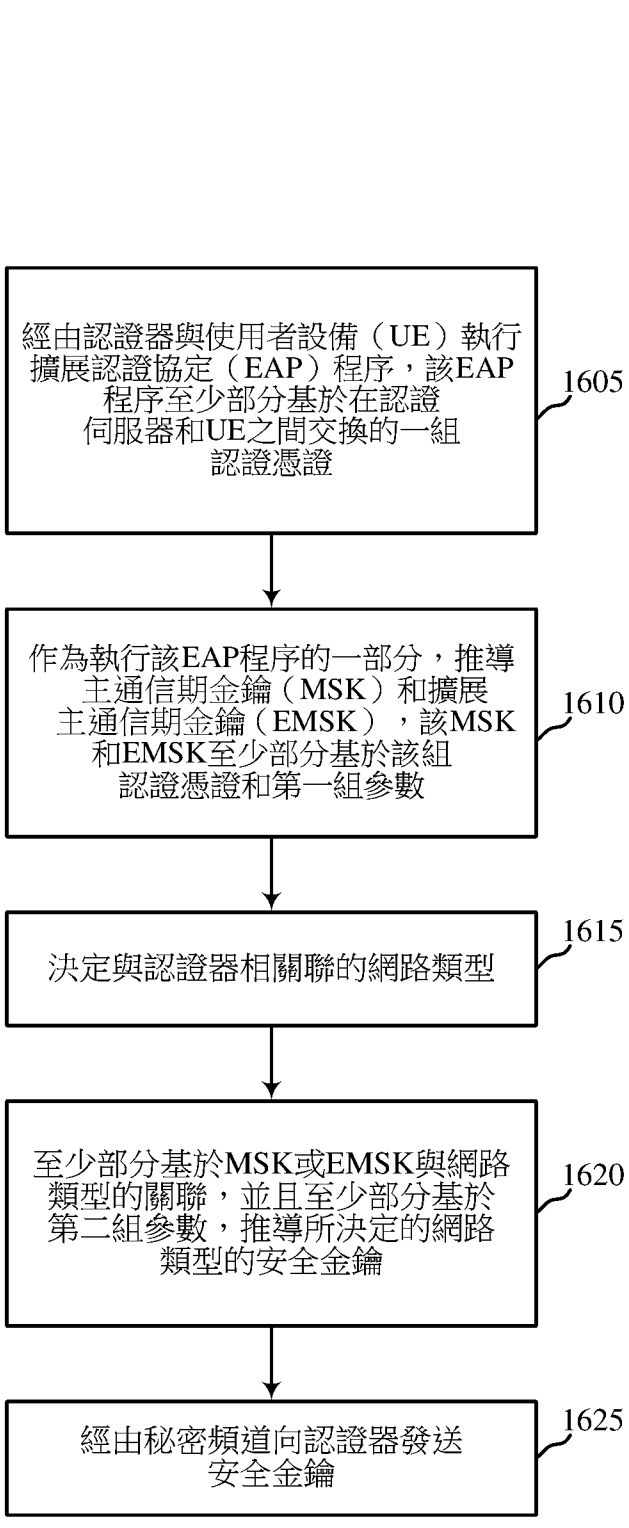
1600
經由認證器與使用者設備（UE）執行擴展認證協定（EAP）程序，該EAP程序至少部分基於在認證伺服器和UE之間交換的一組認證憑證
1605
作為執行該EAP程序的一部分，推導主通信期金鑰（MSK）和擴展主通信期金鑰（EMSK），該MSK和EMSK至少部分基於該組認證憑證和第一組參數
1610
決定與認證器相關聯的網路類型
1615
至少部分基於MSK或EMSK與網路類型的關聯，並且至少部分基於第二組參數，推導所決定的網路類型的安全金鑰
1620
經由秘密頻道向認證器發送安全金鑰
1625

圖16


1700
從認證伺服器接收至少部分基於擴展主通信期金鑰（EMSK）和第一組參數的第一安全金鑰，該EMSK可以至少部分基於一組認證憑證和第二組參數，該組認證憑證在擴展認證協定（EAP）程序期間在使用者設備（UE）和認證伺服器之間交換
1705
至少部分基於第一安全金鑰與UE執行至少一個認證程序
1710

圖17

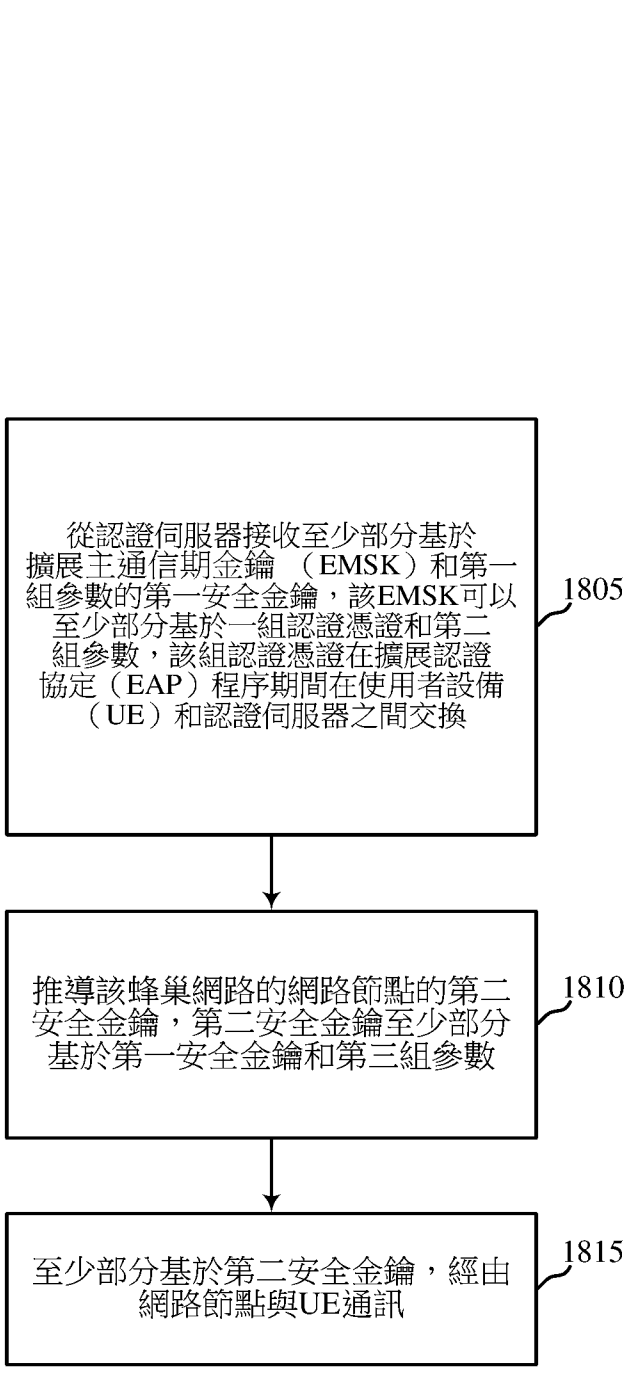
1800
從認證伺服器接收至少部分基於擴展主通信期金鑰 （EMSK）和第一組參數的第一安全金鑰，該EMSK可以至少部分基於一組認證憑證和第二組參數，該組認證憑證在擴展認證協定（EAP）程序期間在使用者設備（UE）和認證伺服器之間交換
1805
推導該蜂巢網路的網路節點的第二安全金鑰，第二安全金鑰至少部分基於第一安全金鑰和第三組參數
1810
至少部分基於第二安全金鑰，經由網路節點與UE通訊
1815

圖18