(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7008690号
(P7008690)

(45)発行日　令和4年1月25日(2022.1.25)

(24)登録日　令和4年1月13日(2022.1.13)

(51)国際特許分類			FI		
H04W	*12/04*	*(2021.01)*	H04W	12/04	
H04W	*12/06*	*(2021.01)*	H04W	12/06	
G09C	*1/00*	*(2006.01)*	G09C	1/00	640E
G06F	*21/44*	*(2013.01)*	G06F	21/44	

請求項の数　15　（全42頁）

(21)出願番号　特願2019-513988(P2019-513988)
(86)(22)出願日　平成29年8月17日(2017.8.17)
(65)公表番号　特表2019-533344(P2019-533344A)
(43)公表日　令和1年11月14日(2019.11.14)
(86)国際出願番号　PCT/US2017/047355
(87)国際公開番号　WO2018/052640
(87)国際公開日　平成30年3月22日(2018.3.22)
審査請求日　令和2年7月29日(2020.7.29)
(31)優先権主張番号　62/396,791
(32)優先日　平成28年9月19日(2016.9.19)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　15/489,670
(32)優先日　平成29年4月17日(2017.4.17)
最終頁に続く

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国 カリフォルニア ９２１２１ サン ディエゴ モアハウス ドライブ ５７７５
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100163522
弁理士　黒田 晋平
(72)発明者　ス・ボム・イ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　アナンド・パラニゴウンダー
アメリカ合衆国・カリフォルニア・９２
最終頁に続く

(54)【発明の名称】　拡張可能認証プロトコル（ＥＡＰ）手順の実施に基づいてセルラーネットワークに対するセキュリティ鍵を導出するための技法

(57)【特許請求の範囲】
【請求項１】
ユーザ機器(UE)におけるワイヤレス通信のための方法であって、
オーセンティケータを介して認証サーバを用いて拡張可能認証プロトコル(EAP)手順を実行するステップであって、前記EAP手順が、前記UEと前記認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも基づく、ステップと、
前記認証クレデンシャルおよびパラメータの第1のセットに少なくとも基づくマスタセッション鍵(MSK)および拡張マスタセッション鍵(EMSK)を、前記EAP手順を実行することの一部として導出するステップと、
前記オーセンティケータに関連付けられたネットワークタイプを決定するステップと、
前記オーセンティケータを用いて少なくとも1つの認証手順を、前記決定されたネットワークタイプに少なくとも基づいて実行するステップとを含み、前記少なくとも1つの認証手順が、前記MSKまたは前記EMSKと前記決定されたネットワークタイプとの関連に基づく、方法。
【請求項２】
前記決定されたネットワークタイプがセルラーネットワークタイプを含み、前記オーセンティケータを用いて前記少なくとも1つの認証手順を実行するステップが、
セルラーネットワークに対する第1のセキュリティ鍵を導出するステップを含み、前記第1のセキュリティ鍵が、前記EMSKおよびパラメータの第2のセットに少なくとも基づき、
前記パラメータの第2のセットが、前記セルラーネットワークの識別子、少なくとも1つの

セルラーネットワーク固有のパラメータ、前記UEと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、または、
前記オーセンティケータを用いて前記少なくとも1つの認証手順を実行するステップが、前記セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出するステップであって、前記第2のセキュリティ鍵が、前記第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも基づく、ステップと、
前記第2のセキュリティ鍵に少なくとも基づいて前記ネットワークノードを介して前記セルラーネットワークと通信するステップとを含み、
前記パラメータの第3のセットが、前記ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、前記UEと前記ネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、請求項1に記載の方法。
【請求項３】
前記パラメータの第1のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記オーセンティケータに関連付けられたセルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、または、
前記決定されたネットワークタイプが非セルラーネットワークタイプであり、前記オーセンティケータを用いて前記少なくとも1つの認証手順を実行するステップが、
非セルラーネットワークに対する第1のセキュリティ鍵を導出するステップを含み、前記第1のセキュリティ鍵が、前記MSKおよびパラメータの第2のセットに少なくとも基づく、請求項1に記載の方法。
【請求項４】
ユーザ機器(UE)におけるワイヤレス通信のための装置であって、
オーセンティケータを介して認証サーバを用いて拡張可能認証プロトコル(EAP)手順を実行するための手段であって、前記EAP手順が、前記UEと前記認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも基づく、手段と、
前記認証クレデンシャルおよびパラメータの第1のセットに少なくとも基づくマスタセッション鍵(MSK)および拡張マスタセッション鍵(EMSK)を、前記EAP手順を実行することの一部として導出するための手段と、
前記オーセンティケータに関連付けられたネットワークタイプを決定するための手段と、
前記オーセンティケータを用いて少なくとも1つの認証手順を、前記決定されたネットワークタイプに少なくとも基づいて実行するための手段とを含み、前記少なくとも1つの認証手順が、前記MSKまたは前記EMSKと前記決定されたネットワークタイプとの関連に基づく、装置。
【請求項５】
前記決定されたネットワークタイプがセルラーネットワークタイプを含み、前記少なくとも1つの認証手順を実行するための前記手段が、
セルラーネットワークに対する第1のセキュリティ鍵を導出するための手段を含み、前記第1のセキュリティ鍵が、前記EMSKおよびパラメータの第2のセットに少なくとも基づき、
前記パラメータの第2のセットが、前記セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、前記UEと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、または、
前記少なくとも1つの認証手順を実行するための前記手段が、
前記セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出するための手段であって、前記第2のセキュリティ鍵が、前記第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも基づく、手段と、

前記第2のセキュリティ鍵に少なくとも基づいて前記ネットワークノードを介して前記セルラーネットワークと通信するための手段とを含み、
前記パラメータの第3のセットが、前記ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、前記UEと前記ネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、請求項4に記載の装置。
【請求項６】
前記パラメータの第1のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記オーセンティケータに関連付けられたセルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、または、
前記決定されたネットワークタイプが非セルラーネットワークタイプであり、前記少なくとも1つの認証手順を実行するための前記手段が、
非セルラーネットワークに対する第1のセキュリティ鍵を導出するための手段を含み、前記第1のセキュリティ鍵が、前記MSKおよびパラメータの第2のセットに少なくとも基づく、請求項4に記載の装置。
【請求項７】
認証サーバにおけるワイヤレス通信のための方法であって、
オーセンティケータを介してユーザ機器(UE)を用いて拡張可能認証プロトコル(EAP)手順を実行するステップであって、前記EAP手順が、前記認証サーバと前記UEとの間で交換される認証クレデンシャルのセットに少なくとも基づく、ステップと、
前記認証クレデンシャルおよびパラメータの第1のセットに少なくとも基づくマスタセッション鍵(MSK)および拡張マスタセッション鍵(EMSK)を、前記EAP手順を実行することの一部として導出するステップと、
前記オーセンティケータに関連付けられたネットワークタイプを決定するステップと、
前記MSKまたは前記EMSKと前記ネットワークタイプとの関連に少なくとも基づいて、およびパラメータの第2のセットに少なくとも基づいて、前記決定されたネットワークタイプに対するセキュリティ鍵を導出するステップと、
前記セキュリティ鍵をセキュアなチャネルを介して前記オーセンティケータに送信するステップとを含む、方法。
【請求項８】
前記パラメータの第1のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記決定されたネットワークタイプがセルラーネットワークタイプを含み、前記パラメータの第2のセットが、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、前記認証サーバと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み、
前記セルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、請求項7に記載の方法。
【請求項９】
認証サーバにおけるワイヤレス通信のための装置であって、
オーセンティケータを介してユーザ機器(UE)を用いて拡張可能認証プロトコル(EAP)手順を実行するための手段であって、前記EAP手順が、前記認証サーバと前記UEとの間で交換される認証クレデンシャルのセットに少なくとも基づく、手段と、
前記認証クレデンシャルおよびパラメータの第1のセットに少なくとも基づくマスタセッ

ション鍵(MSK)および拡張マスタセッション鍵(EMSK)を、前記EAP手順を実行することの一部として導出するための手段と、
前記オーセンティケータに関連付けられたネットワークタイプを決定するための手段と、
前記MSKまたは前記EMSKと前記決定されたネットワークタイプとの関連に少なくとも基づいて、およびパラメータの第2のセットに少なくとも基づいて、前記決定されたネットワークタイプに対するセキュリティ鍵を導出するための手段と、
前記セキュリティ鍵をセキュアなチャネルを介して前記オーセンティケータに送信するための手段とを含む、装置。
【請求項１０】
前記パラメータの第1のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記決定されたネットワークタイプがセルラーネットワークタイプを含み、前記パラメータの第2のセットが、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、前記認証サーバと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、または、
セルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、請求項9に記載の装置。
【請求項１１】
セルラーネットワークにおけるワイヤレス通信のための方法であって、
拡張マスタセッション鍵(EMSK)およびパラメータの第1のセットに少なくとも基づいてかつ前記セルラーネットワークのネットワークタイプに対して導出された第1のセキュリティ鍵を、前記セルラーネットワークに関連付けられたオーセンティケータにおいて認証サーバから受信するステップであって、前記EMSKが認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも基づき、前記認証クレデンシャルが拡張可能認証プロトコル(EAP)手順の間にユーザ機器(UE)と前記認証サーバとの間で交換される、ステップと、
前記第1のセキュリティ鍵に少なくとも基づいて前記UEを用いて少なくとも1つの認証手順を、前記オーセンティケータによって実行するステップとを含む、方法。
【請求項１２】
前記UEを用いて前記少なくとも1つの認証手順を実行するステップが、
前記セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出するステップであって、前記第2のセキュリティ鍵が、前記第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも基づく、ステップと、
前記第2のセキュリティ鍵に少なくとも基づいて前記ネットワークノードを介して前記UEと通信するステップとを含み、
前記パラメータの第3のセットが、前記ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、前記UEと前記ネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、あるいは、
前記パラメータの第1のセットが、前記セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、前記UEと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、または、
前記パラメータの第2のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記セルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、請

求項11に記載の方法。
【請求項１３】
セルラーネットワークにおけるワイヤレス通信のための装置であって、
拡張マスタセッション鍵(EMSK)およびパラメータの第1のセットに少なくとも基づいてかつ前記セルラーネットワークのネットワークタイプに対して導出された第1のセキュリティ鍵を、前記セルラーネットワークに関連付けられたオーセンティケータにおいて認証サーバから受信するための手段であって、前記EMSKが認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも基づき、前記認証クレデンシャルが拡張可能認証プロトコル(EAP)手順の間にユーザ機器(UE)と前記認証サーバとの間で交換される、手段と、
前記第1のセキュリティ鍵に少なくとも基づいて前記UEを用いて少なくとも1つの認証手順を前記オーセンティケータにおいて実行するための手段とを含む、装置。
【請求項１４】
前記UEを用いて前記少なくとも1つの認証手順を実行するための前記手段が、
前記セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出するための手段であって、前記第2のセキュリティ鍵が、前記第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも基づく、手段と、
前記第2のセキュリティ鍵に少なくとも基づいて前記ネットワークノードを介して前記UEと通信するための手段とを含む、
前記パラメータの第3のセットが、前記ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、前記UEと前記ネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、あるいは、
前記パラメータの第1のセットが、前記セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、前記UEと前記セルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含む、または、
前記パラメータの第2のセットが、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含む、または、
前記セルラーネットワークが、第5世代(5G)ネットワーク、第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、LTE-Advanced(LTE-A)ネットワーク、第3世代(3G)ネットワーク、またはそれらの組合せのうちの少なくとも1つを含む、請求項13に記載の装置。
【請求項１５】
コンピュータ上で実行されると、請求項１～３、７、８、１１、または１２のいずれか一項に記載の方法を実行するためのコンピュータ実行可能コードを備えるコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
相互参照
本特許出願は、各々が本出願の譲受人に譲渡される、2017年4月17日に出願された「Techniques For Deriving Security Keys For A Cellular Network Based On Performance of an Extensible Authentication Protocol (EAP) Procedure」と題する、Leeらによる米国特許出願第15/489,670号、および2016年9月19日に出願された「Techniques For Deriving Security Keys For A Cellular Network Based On Performance of an Extensible Authentication Protocol (EAP) Procedure」と題する、Leeらによる米国仮特許出願第62/396,791号の優先権を主張する。
【０００２】
本開示は、たとえば、ワイヤレス通信システムに関し、より詳細には、拡張可能認証プロトコル(EAP)手順の実施に基づいてセルラーネットワークに対するセキュリティ鍵を導出

するための技法に関する。
【背景技術】
【０００３】
ワイヤレス通信システムは、音声、ビデオ、パケットデータ、メッセージング、ブロードキャストなどの、様々なタイプの通信コンテンツを提供するために広く展開されている。これらのシステムは、利用可能なシステムリソース(たとえば、時間、周波数、および電力)を共有することによって、複数のユーザとの通信をサポートすることが可能な多元接続システムであり得る。そのような多元接続システムの例は、符号分割多元接続(CDMA)システム、時分割多元接続(TDMA)システム、周波数分割多元接続(FDMA)システム、および直交周波数分割多元接続(OFDMA)システムを含む。
【０００４】
いくつかの例では、ワイヤレス多元接続通信システムは、セルラーネットワークであってもよく、またはそれを含んでもよい。セルラーネットワークは、各々がユーザ機器(UE)としても知られている複数の通信デバイスのための通信を同時にサポートする、いくつかのネットワークアクセスデバイスを含み得る。第4世代(4G)ネットワーク、ロングタームエボリューション(LTE)ネットワーク、またはLTE-Advanced(LTE-A)ネットワークでは、ネットワークアクセスデバイスは、拡張ノードB(eNB)の形態を取ってもよく、各eNBは1つまたは複数の基地局のセットを含む。第5世代(5GまたはNextGen)ネットワークでは、ネットワークアクセスデバイスは、ネットワークアクセスデバイスコントローラ(たとえば、アクセスノードコントローラ(ANC)と通信中のスマートレディオヘッド(SRH:smart radio heads)またはgノードB(gNB)の形態を取ってもよく、そこにおいて、ネットワークアクセスデバイスコントローラと通信中の1つまたは複数のネットワークアクセスデバイスのセットが、ネットワークノードを規定する。eNB、gNB、またはネットワークノードは、(たとえば、eNB、gNB、またはネットワークノードからUEへの送信用の)ダウンリンクチャネル上および(たとえば、UEからeNB、gNB、またはネットワークノードへの送信用の)アップリンクチャネル上でUEのセットと通信し得る。
【０００５】
UEがセルラーネットワークにアクセスするとき、UEまたはセルラーネットワークは、UEがそれ自体をセルラーネットワークのオーセンティケータに対して認証することを可能にし、オーセンティケータがセルラーネットワークをUEに対して認証することを可能にする、1つまたは複数の手順を開始し得る。いくつかの例では、認証手順はEAP手順を含んでもよく、オーセンティケータとのセキュアな接続を有する認証サーバは、UEを認証し、UEがそれ自体をオーセンティケータに対して認証するために1つまたは複数のセキュリティ鍵を導出することを可能にし、オーセンティケータがセルラーネットワークをUEに対して認証することを可能にするためにセキュアな接続を介してオーセンティケータに送信される1つまたは複数のセキュリティ鍵を導出する。
【発明の概要】
【課題を解決するための手段】
【０００６】
いくつかの場合には、セルラーネットワークは、異なるタイプのアクセスネットワークを介してセルラーネットワークへのアクセスを可能にしてもよく、アクセスネットワークのうちのいくつかは攻撃に対して多少は脆弱である場合があり、アクセスネットワークのうちのいくつかは多少はセルラーネットワークの事業者の制御下にある場合がある。たとえば、セルラーネットワークは、セルラーアクセスネットワークまたは非セルラーアクセスネットワーク(たとえば、ワイヤレスローカルエリアネットワーク(WLAN))を介してセルラーネットワークへのアクセスを可能にする場合がある。同じEAP手順が異なるアクセスネットワークに関連付けられたオーセンティケータによってサポートされるとき、同じマスタセッション鍵(MSK)が、セルラーアクセスネットワークに関連付けられたオーセンティケータまたは非セルラーアクセスネットワークに関連付けられたオーセンティケータを介してEAP手順を実行した結果として導出される場合がある。したがって、同じMSKまた

はMSKから導出される同じセキュリティ鍵が、セルラーアクセスネットワークに関連付けられたオーセンティケータまたは非セルラーアクセスネットワークに関連付けられたオーセンティケータに与えられる場合がある。非セルラーアクセスネットワークが攻撃者によって不正アクセスされた場合、MSKまたはMSKから導出されたセキュリティ鍵への攻撃者のアクセスは、攻撃者が、UEへのセルラーアクセスネットワークになりすますために非セルラーアクセスネットワークを使用することを可能にする場合があり、そのことが、UEおよび/またはUE上で動作しているアプリケーションのセキュリティを危うくする。本開示で説明する技法は、オーセンティケータに関連付けられたネットワークのタイプを決定すること、およびネットワークのタイプに関連付けられたEAPセッション鍵(たとえば、MSKまたは拡張MSK(EMSK))のタイプに基づいてオーセンティケータを用いて認証手順を実行すること(またはオーセンティケータに対するセキュリティ鍵を導出すること)によって、そのような脅威を緩和するのに役立つ。いくつかの例では、MSKは、オーセンティケータが非セルラーアクセスネットワークに関連付けられているときに使用されてもよく、EMSKは、オーセンティケータがセルラーアクセスネットワークに関連付けられているときに使用されてもよい。

【０００７】

一例では、UEにおけるワイヤレス通信のための方法が説明される。方法は、オーセンティケータを介して認証サーバを用いてEAP手順を実行するステップを含み得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。方法はまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するステップと、オーセンティケータに関連付けられたネットワークタイプを決定するステップと、オーセンティケータを用いて少なくとも1つの認証手順を、決定されたネットワークタイプに少なくとも部分的に基づいて実行するステップとを含み得る。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【０００８】

一例では、UEにおけるワイヤレス通信のための装置が説明される。装置は、オーセンティケータを介して認証サーバを用いてEAP手順を実行するための手段を含み得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。装置はまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するための手段と、オーセンティケータがセルラーネットワークに関連付けられていると決定するための手段と、オーセンティケータを用いて少なくとも1つの認証手順を実行するための手段とを含み得る。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【０００９】

一例では、UEにおけるワイヤレス通信のための別の装置が説明される。装置は、プロセッサと、プロセッサと電子通信しているメモリとを含み得る。プロセッサおよびメモリは、オーセンティケータを介して認証サーバを用いてEAP手順を実行するように構成され得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。プロセッサおよびメモリはまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出することと、オーセンティケータに関連付けられたネットワークタイプを決定することと、オーセンティケータを用いて少なくとも1つの認証手順を、決定されたネットワークタイプに少なくとも部分的に基づいて実行することとを行うように構成され得る。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【００１０】

一例では、UEにおけるワイヤレス通信のためのコンピュータ実行可能コードを記憶する非

一時的コンピュータ可読媒体が説明される。コードは、オーセンティケータを介して認証サーバを用いてEAP手順を実行することをプロセッサによって実行可能である。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。コードはまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出することと、オーセンティケータに関連付けられたネットワークタイプを決定することと、オーセンティケータを用いて少なくとも1つの認証手順を、決定されたネットワークタイプに少なくとも部分的に基づいて実行することとを行うことをプロセッサによって実行可能である。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【００１１】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、決定されたネットワークタイプはセルラーネットワークタイプを含んでもよく、オーセンティケータを用いて少なくとも1つの認証手順を実行することは、セルラーネットワークに対する第1のセキュリティ鍵を導出することを含み得る。第1のセキュリティ鍵は、EMSKおよびパラメータの第2のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第2のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００１２】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、オーセンティケータを用いて少なくとも1つの認証手順を実行することは、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出することであって、第2のセキュリティ鍵が第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づく、導出することと、第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してセルラーネットワークと通信することとを含み得る。これらの例のいくつかにおいて、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００１３】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００１４】

上記で説明した方法、装置、または非一時的コンピュータ可読媒体のいくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【００１５】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、決定されたネットワークタイプは非セルラーネットワークタイプを含んでもよく、オーセンティケータを用いて少なくとも1つの認証手順を実行することは、非セルラーネットワークに対する第1のセキュリティ鍵を導出することを含み得る。第1のセキュリティ鍵は、MSKおよびパラメータの第2のセットに少なくとも部分的に基づき得る。

【００１６】

一例では、認証サーバにおけるワイヤレス通信のための方法は、オーセンティケータを介してUEを用いてEAP手順を実行するステップを含み得る。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。方法はまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づ

くMSKおよびEMSKを、EAP手順を実行することの一部として導出するステップと、オーセンティケータに関連付けられたネットワークタイプを決定するステップと、MSKまたはEMSKとネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出するステップと、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信するステップとを含み得る。

【００１７】

一例では、認証サーバにおけるワイヤレス通信のための装置が説明される。装置は、オーセンティケータを介してUEを用いてEAP手順を実行するための手段を含み得る。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。装置はまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するための手段と、オーセンティケータに関連付けられたネットワークタイプを決定するための手段と、MSKまたはEMSKとネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出するための手段と、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信するための手段とを含み得る。

【００１８】

一例では、認証サーバにおけるワイヤレス通信のための別の装置が説明される。装置は、プロセッサと、プロセッサと電子通信しているメモリとを含み得る。プロセッサおよびメモリは、オーセンティケータを介してUEを用いてEAP手順を実行するように構成され得る。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。プロセッサおよびメモリはまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出することと、オーセンティケータに関連付けられたネットワークタイプを決定することと、MSKまたはEMSKと決定されたネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出することと、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信することとを行うように構成され得る。

【００１９】

一例では、認証サーバにおけるワイヤレス通信のためのコンピュータ実行可能コードを記憶する非一時的コンピュータ可読媒体が説明される。コードは、オーセンティケータを介してUEを用いてEAP手順を実行することをプロセッサによって実行可能である。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。コードはまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出することと、オーセンティケータに関連付けられたネットワークタイプを決定することと、MSKまたはEMSKと決定されたネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出することと、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信することとを行うことをプロセッサによって実行可能である。

【００２０】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００２１】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、

決定されたネットワークタイプはセルラーネットワークタイプを含んでもよく、パラメータの第2のセットはセルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、認証サーバとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００２２】

上記で説明した方法、装置、または非一時的コンピュータ可読媒体のいくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【００２３】

一例では、セルラーネットワークにおけるワイヤレス通信のための方法が説明される。方法は、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信するステップを含み得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。方法はまた、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行するステップを含み得る。

【００２４】

一例では、セルラーネットワークにおけるワイヤレス通信のための装置が説明される。装置は、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信するための手段を含み得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。装置はまた、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行するための手段を含み得る。

【００２５】

一例では、セルラーネットワークにおけるワイヤレス通信のための別の装置が説明される。装置は、プロセッサと、プロセッサと電子通信しているメモリとを含み得る。プロセッサおよびメモリは、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信するように構成され得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。プロセッサおよびメモリはまた、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行するように構成され得る。

【００２６】

一例では、セルラーネットワークにおけるワイヤレス通信のためのコンピュータ実行可能コードを記憶する非一時的コンピュータ可読媒体が説明される。コードは、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信することをプロセッサによって実行可能である。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。コードはまた、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行することを実行可能である。

【００２７】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、UEを用いて少なくとも1つの認証手順を実行することは、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出することであって、第2のセキュリティ鍵が第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づく、導出することと、第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してUEと通信することとを含み得る。いくつかの例では、パラメータの第3のセッ

トは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００２８】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、パラメータの第2のセットはセルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００２９】

上記で説明した方法、装置、および非一時的コンピュータ可読媒体のいくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００３０】

上記で説明した方法、装置、または非一時的コンピュータ可読媒体のいくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【００３１】

上記は、以下の発明を実施するための形態がより良く理解され得るように、本開示による例の技法および技術的利点をかなり広く概説している。追加の技法および利点が以下で説明される。開示する概念および具体例は、本開示の同じ目的を遂行するための他の構造を修正または設計するための基礎として容易に利用され得る。そのような均等な構成は、添付の特許請求の範囲から逸脱しない。本明細書で開示する概念の特性、それらの編成と動作方法の両方が、関連する利点とともに、添付の図に関して検討されると以下の説明からより良く理解されよう。図の各々は、例示および説明のために提供され、特許請求の範囲の限定の定義として提供されるものではない。

【００３２】

本発明の本質および利点のさらなる理解は、以下の図面を参照することによって実現され得る。添付の図面において、類似の構成要素または機能は、同じ参照符号を有することがある。さらに、同じタイプの様々な構成要素は、参照符号の後に、ダッシュと、類似の構成要素を区別する第2の符号とを続けることによって、区別されることがある。第1の参照符号のみが本明細書において使用される場合、説明は、第2の参照符号にかかわらず、同じ第1の参照符号を有する類似の構成要素のうちのいずれにも適用可能である。

【図面の簡単な説明】

【００３３】

【図１】本開示の様々な態様による、ワイヤレス通信システムの一例を示す図である。

【図２】本開示の様々な態様による、ワイヤレス通信システムの一例を示す図である。

【図３】本開示の様々な態様による、ワイヤレス通信システムに対する鍵階層構造の一例を示す図である。

【図４】本開示の様々な態様による、ワイヤレス通信システムの一例を示す図である。

【図５】本開示の様々な態様による、UEと、セルラーネットワークと、認証サーバとの間の例示的なメッセージフローを示す図である。

【図６】本開示の様々な態様による、UEのブロック図である。

【図７】本開示の様々な態様による、ワイヤレス通信マネージャのブロック図である。

【図８】本開示の様々な態様による、ワイヤレス通信システムの図である。

【図９】本開示の様々な態様による、認証サーバのブロック図である。

【図１０】本開示の様々な態様による、認証サーバのブロック図である。

【図１１】本開示の様々な態様による、ネットワークノードのブロック図である。

【図１２】本開示の様々な態様による、通信マネージャのブロック図である。

【図１３】本開示の様々な態様による、ネットワークノードの図である。
【図１４】本開示の様々な態様による、ワイヤレス通信のための方法を示すフローチャートである。
【図１５】本開示の様々な態様による、ワイヤレス通信のための方法を示すフローチャートである。
【図１６】本開示の様々な態様による、ワイヤレス通信のための方法を示すフローチャートである。
【図１７】本開示の様々な態様による、ワイヤレス通信のための方法を示すフローチャートである。
【図１８】本開示の様々な態様による、ワイヤレス通信のための方法を示すフローチャートである。
【発明を実施するための形態】
【００３４】
本開示で説明する技法は、UEが、異なるタイプのアクセスネットワークに関連付けられたオーセンティケータを介して認証サーバを用いてEAP手順を実行することを可能にする。オーセンティケータを介してEAP手順の実行が成功すると、UEおよび認証サーバは、オーセンティケータに関連付けられたネットワークのタイプに少なくとも部分的に基づいて、オーセンティケータのためのセキュリティ鍵を導出し得る。いくつかの例では、UEおよび認証サーバは、オーセンティケータが非セルラーアクセスネットワークに関連付けられているときにMSKに基づいてオーセンティケータに対するセキュリティ鍵を導出してもよく、オーセンティケータがセルラーアクセスネットワークに関連付けられているときにEMSKに基づいてオーセンティケータに対するセキュリティ鍵を導出してもよい。
【００３５】
以下の説明は例を提供するものであり、特許請求の範囲に記載される範囲、適用可能性、または例を限定するものではない。本開示の範囲から逸脱することなく、説明される要素の機能および構成に変更が加えられてよい。様々な例は、様々な手順または構成要素を適宜に省略してよく、置換してよく、または追加してよい。たとえば、説明される方法は、説明される順序とは異なる順序で実行されてよく、様々なステップが追加されてよく、省略されてよく、または組み合わされてよい。また、いくつかの例に関して説明する特徴が、いくつかの他の例では組み合わせられてよい。
【００３６】
図1は、本開示の様々な態様によるワイヤレス通信システム100の一例を示す。ワイヤレス通信システム100は、ネットワークアクセスデバイス(たとえば、分散ネットワークアクセスデバイス、分散ユニット、gNB、レディオヘッド(RH)、SRH、送信/受信ポイント(TRP)、エッジノード、エッジユニット、など)105、UE115、ネットワークアクセスデバイスコントローラ(たとえば、集中型ネットワークアクセスデバイス、中心ノード、中心ユニット、アクセスノードコントローラ(ANC)、など)125、およびコアネットワーク130を含み得る。コアネットワーク130は、ユーザ認証、アクセス許可、トラッキング、インターネットプロトコル(IP)接続、および他のアクセス機能、ルーティング機能、またはモビリティ機能を提供してもよい。ネットワークアクセスデバイスコントローラ125は、バックホールリンク132(たとえば、S1、S2など)を通じてコアネットワーク130とインターフェースすることができ、UE115との通信のために無線構成およびスケジューリングを実行することができる。様々な例では、ネットワークアクセスデバイスコントローラ125は、直接または間接的に(たとえば、コアネットワーク130を通じて)のいずれかで、有線またはワイヤレスの通信リンクであってよいバックホールリンク134(たとえば、X1、X2など)を介して互いに通信してよい。各ネットワークアクセスデバイスコントローラ125はまた、いくつかのネットワークアクセスデバイス(たとえば、RH)105を通していくつかのUE115と通信してもよい。ワイヤレス通信システム100の代替構成では、ネットワークアクセスデバイスコントローラ125の機能は、ネットワークアクセスデバイス105によって与えられてもよく、またはネットワークノード(たとえば、アクセスノード、新しい無線基地局

(NR BSなど)135のネットワークアクセスデバイス105にわたって分散されてもよい。ワイヤレス通信システム100の別の代替構成では、ネットワークノード135がeNBによって置き換えられてもよく、ネットワークアクセスデバイス105が基地局と置き換えられてもよく、ネットワークアクセスデバイスコントローラ125が基地局コントローラ(またはコアネットワーク130へのリンク)によって置き換えられてもよい。

【００３７】

ネットワークアクセスデバイスコントローラ125は、1つまたは複数のネットワークアクセスデバイス105を介してUE115と通信してもよく、各ネットワークアクセスデバイス105は、いくつかのUE115とワイヤレスに通信するために1つまたは複数のアンテナを有する。ネットワークノード135の各々は、それぞれの地理的カバレージエリア110の通信カバレージを提供してもよく、1つまたは複数のネットワークアクセスデバイス105に関連する1つまたは複数の遠隔トランシーバを提供してもよい。ネットワークアクセスデバイス105は、LTE/LTE-A基地局の機能のうちの多くを実行し得る。いくつかの例では、ネットワークアクセスデバイスコントローラ125は、分散された形態で実装されてもよく、ネットワークアクセスデバイスコントローラ125の一部は、各ネットワークアクセスデバイス105内に設けられる。ネットワークノード135に対する地理的カバレージエリア110は、カバレージエリア(図示せず)の一部のみを構成するセクタに分割されてもよく、いくつかの例では、ネットワークノード135に対する地理的カバレージエリア110は、ネットワークノード135(図示せず)に関連するネットワークアクセスデバイス105のセットに対する地理的カバレージエリアのセットから形成されてもよい。いくつかの例では、ネットワークアクセスデバイス105は、トランシーバ基地局、無線基地局、アクセスポイント、無線トランシーバ、ノードB、eNB、ホームノードB、ホームeノードB、gNBなどの、代替ネットワークアクセスデバイスと置き換えられてもよい。ワイヤレス通信システム100は、様々なタイプ(たとえば、マクロセルネットワークアクセスデバイスおよび/またはスモールセルネットワークアクセスデバイス)のネットワークアクセスデバイス105(または、基地局もしくは他のネットワークアクセスデバイス)を含み得る。ネットワークアクセスデバイス105および/またはネットワークノード135の地理的カバレージエリアは重複してもよい。いくつかの例では、異なるネットワークアクセスデバイス105は、異なる無線アクセス技術に関連してよい。

【００３８】

いくつかの例では、ワイヤレス通信システム100は、5Gネットワークを含み得る。他の例では、ワイヤレス通信システム100は、LTE/LTE-Aネットワークを含み得る。ワイヤレス通信システム100は、場合によっては、異なるタイプのネットワークアクセスデバイス105またはネットワークノード135が様々な地理的領域にカバレージを提供する異種ネットワークであり得る。たとえば、各ネットワークアクセスデバイス105またはネットワークノード135は、マクロセル、スモールセル、および/または他のタイプのセルに通信カバレージを提供し得る。「セル」という用語は、文脈に応じて、基地局、RH、基地局もしくはRHに関連付けられるキャリアもしくはコンポーネントキャリア、またはキャリアもしくは基地局のカバレージエリア(たとえば、セクタなど)を表すために使用され得る。

【００３９】

マクロセルは、比較的大きい地理的エリア(たとえば、半径数キロメートル)をカバーし得、ネットワークプロバイダのサービスに加入しているUE115によるアクセスを可能にし得る。スモールセルは、マクロセルと比較すると、低電力のRHまたは基地局を含むことがあり、マクロセルと同じまたは異なる周波数帯域で動作することがある。スモールセルは、様々な例によれば、ピコセル、フェムトセル、およびマイクロセルを含み得る。ピコセルは、比較的小さい地理的エリアをカバーし得、ネットワークプロバイダのサービスに加入しているUE115による無制限アクセスを可能にし得る。フェムトセルも、比較的小さい地理的エリア(たとえば、自宅)をカバーし得、フェムトセルとの関連性を有するUE115(たとえば、限定加入者グループ(CSG:closed subscriber group)の中のUE、自宅内のユーザのためのUEなど)による制限付きアクセスを提供し得る。マクロセル用のネットワーク

アクセスデバイスは、マクロネットワークアクセスデバイスと呼ばれることがある。スモールセル用のネットワークアクセスデバイスは、スモールセルネットワークアクセスデバイス、ピコネットワークアクセスデバイス、フェムトネットワークアクセスデバイス、またはホームネットワークアクセスデバイスと呼ばれることがある。ネットワークアクセスデバイスは、1つまたは複数の(たとえば、2つ、3つ、4つなどの)セル(たとえば、コンポーネントキャリア)をサポートしてもよい。

【００４０】

ワイヤレス通信システム100は、同期動作または非同期動作をサポートし得る。同期動作の場合、ネットワークノード135またはネットワークアクセスデバイス105は、同様のフレームタイミングを有してもよく、異なるネットワークアクセスデバイス105からの送信は、時間的にほぼ整合され得る。非同期動作の場合、ネットワークノード135またはネットワークアクセスデバイス105は、異なるフレームタイミングを有してもよく、異なるネットワークアクセスデバイス105からの送信は、時間的に整合されないことがある。本明細書で説明される技法は、同期動作または非同期動作のいずれかに使用されてよい。

【００４１】

開示する様々な例のうちのいくつかに適合し得る通信ネットワークは、階層化されたプロトコルスタックに従って動作するパケットベースネットワークであり得る。ユーザプレーンでは、ベアラまたはパケットデータコンバージェンスプロトコル(PDCP:Packet Data Convergence Protocol)レイヤにおける通信は、IPベースであってよい。無線リンク制御(RLC:Radio Link Control)レイヤは、場合によっては、論理チャネルを介して通信するために、パケットのセグメント化および再アセンブリを実行し得る。媒体アクセス制御(MAC)レイヤは、優先度処理、およびトランスポートチャネルへの論理チャネルの多重化を実行し得る。MACレイヤはまた、MACレイヤにおける再送信を行ってリンク効率を改善するために、ハイブリッドARQ(HARQ)を使用し得る。制御プレーンでは、無線リソース制御(RRC)プロトコルレイヤは、UE115と、ネットワークデバイス105、ネットワークアクセスデバイスコントローラ125、またはユーザプレーンデータのための無線ベアラをサポートするコアネットワーク130との間のRRC接続の確立、構成、および保守を行い得る。物理(PHY)レイヤにおいて、トランスポートチャネルは、物理チャネルにマッピングされ得る。

【００４２】

UE115は、ワイヤレス通信システム100全体にわたって分散され得、各UE115は固定またはモバイルであり得る。UE115は、移動局、加入者局、モバイルユニット、加入者ユニット、ワイヤレスユニット、リモートユニット、モバイルデバイス、ワイヤレスデバイス、ワイヤレス通信デバイス、リモートデバイス、モバイル加入者局、アクセス端末、モバイル端末、ワイヤレス端末、リモート端末、ハンドセット、ユーザエージェント、モバイルクライアント、クライアント、または何らかの他の好適な用語をも含むか、あるいはそのように当業者によって呼ばれることもある。UE115は、セルラーフォン、携帯情報端末(PDA)、ワイヤレスモデム、ワイヤレス通信デバイス、ハンドヘルドデバイス、タブレットコンピュータ、ラップトップコンピュータ、コードレスフォン、ワイヤレスローカルループ(WLL)局、インターネットオブエブリシング(IoE:Internet of Everything)デバイス、自動車、アプライアンス、またはワイヤレス通信インターフェースを有する他の電子デバイスであってよい。UEは、スモールセルノード、中継ノードなどを含む、様々なタイプのネットワークノード135またはネットワークアクセスデバイス105と通信することが可能であり得る。UEはまた、(たとえば、ピアツーピア(P2P:peer-to-peer)プロトコルを使用して)他のUEと直接通信できる場合がある。

【００４３】

ワイヤレス通信システム100に示す通信リンク122は、UE115からネットワークアクセスデバイス105へのアップリンク(UL)チャネル、および/またはネットワークアクセスデバイス105からUE115へのダウンリンク(DL)チャネルを含んでよい。ダウンリンクチャネルは、順方向リンクチャネルと呼ばれることもあり、アップリンクチャネルは、逆方向リン

クチャネルと呼ばれることもある。

【００４４】

各通信リンク122は、1つまたは複数のキャリアを含み得、ここで、各キャリアは、1つまたは複数の無線アクセス技術に従って変調された複数のサブキャリアまたはトーン(たとえば、異なる周波数の波形信号)から構成された信号であり得る。各被変調信号は、異なるサブキャリア上で送信されてよく、制御情報(たとえば、基準信号、制御チャネルなど)、オーバーヘッド情報、ユーザデータなどを搬送してよい。通信リンク122は、(たとえば、ペアにされたスペクトルリソースを使用する)周波数分割複信(FDD)技法、または(たとえば、ペアにされていないスペクトルリソースを使用する)時分割複信(TDD)技法を使用して、双方向通信を送信し得る。FDD用のフレーム構造(たとえば、フレーム構造タイプ1)およびTDD用のフレーム構造(たとえば、フレーム構造タイプ2)が規定され得る。

【００４５】

ワイヤレス通信システム100のいくつかの例では、ネットワークアクセスデバイス105および/またはUE115は、ネットワークアクセスデバイス105とUE115との間の通信品質および信頼性を改善するために、アンテナダイバーシティ方式を採用するための複数のアンテナを含み得る。追加または代替として、ネットワークアクセスデバイス105および/またはUE115は、マルチパス環境を利用して、同じかまたは異なるコード化データを搬送する複数の空間レイヤを送信し得る、多入力多出力(MIMO)技法を採用し得る。

【００４６】

ワイヤレス通信システム100は、複数のセル上またはキャリア上での動作、すなわち、キャリアアグリゲーション(CA:carrier aggregation)またはマルチキャリア動作と呼ばれることがある機能をサポートし得る。キャリアは、コンポーネントキャリア(CC:component carrier)、レイヤ、チャネルなどと呼ばれることもある。「キャリア」、「コンポーネントキャリア」、「セル」、および「チャネル」という用語は、本明細書で互換的に使用されることがある。ue115は、キャリアアグリゲーションのために、複数のダウンリンクCCと1つまたは複数のアップリンクCCとで構成され得る。キャリアアグリゲーションは、FDDコンポーネントキャリアとTDDコンポーネントキャリアの両方とともに使用され得る。

【００４７】

UE115のうちの1つまたは複数は、ワイヤレス通信マネージャ140を含み得る。いくつかの例では、ワイヤレス通信マネージャ140は、コアネットワーク130に関連付けられたオーセンティケータを介して認証サーバを用いてEAP手順を実行するために使用され得る。認証サーバは、図2に関して説明したコアネットワーク130を介してアクセスされ得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。ワイヤレス通信マネージャ140はまた、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順(EAP方法または認証方法と総称される)を実行することの一部として導出することと、オーセンティケータがセルラーネットワークに関連付けられていると決定することと、EMSKに少なくとも部分的に基づいてセルラーネットワークを用いて少なくとも1つの認証手順を実行することとを行うために使用され得る。いくつかの例では、ワイヤレス通信マネージャ140は、図6～図8に関して説明したワイヤレス通信マネージャの態様の一例であり得る。

【００４８】

図2は、本開示の様々な態様によるワイヤレス通信システム200の一例を示す。ワイヤレス通信システム200は、UE115-aのホームセルラーネットワーク205とUE115-aによって訪問されるセルラーネットワーク(すなわち、訪問先セルラーネットワーク205-a)とを含み得る。

【００４９】

ホームセルラーネットワーク205は、第1のオーセンティケータ235(たとえば、ホームセキュリティアンカー機能(H-SEAF)を与えるサーバまたはデバイス)と、ホームユーザプレ

ーンゲートウェイ(H-UP-GW)210とを含み得る。ホームセルラーネットワーク205はまた、他の機能(図示せず)を与える他のサーバまたはデバイスを含み得ることは、当業者には諒解されよう。訪問先セルラーネットワーク205-aは、第2のオーセンティケータ235-a(たとえば、訪問するSEAF(V-SEAF)を与えるサーバまたはデバイス)と、訪問先UP-GW(V-UP-GW)210-aと、訪問先セルラーネットワーク制御プレーンコアネットワーク機能(V-CP-CN)215と、無線アクセスネットワーク(RAN)220とを含み得る。いくつかの例では、RAN220は、図1に関して説明したネットワークノード135、ネットワークアクセスデバイス105、およびネットワークアクセスデバイスコントローラ125のうちの1つまたは複数を含み得る。第1のオーセンティケータ235、H-UP-GW210、第2のオーセンティケータ235-a、V-UP-GW210-a、およびV-CP-CN215は、図1に関して説明したコアネットワーク130の例示的な構成要素であり得る。

【００５０】

ホームセルラーネットワーク205は、認証サーバ245と通信中であり得る(または認証サーバ245を与え得る)。認証サーバ245は、認証サーバ機能(AUSF)を与え得る。認証サーバ245は、認証クレデンシャルリポジトリおよび処理機能(ARPF)240にアクセスしてもよく、および/またはARPF240を呼び出してもよい。

【００５１】

UE115-aは、RAN220のノード(たとえば、ネットワークアクセスデバイス)を介して訪問先セルラーネットワーク205-aに接続し得る。図2は、UE115-aが、ローミングモードで動作中に、訪問先セルラーネットワーク205-aにアクセスしたものと仮定する。非ローミングシナリオでは、UE115-aは、ホームセルラーネットワーク205のRANを介して、訪問先セルラーネットワーク205-aではなくホームセルラーネットワーク205にアクセスし得る(図2に示さず)。

【００５２】

V-CP-CN215は、対応するセキュリティコンテキストを維持するばかりでなく、UE115-aに対するモビリティ管理(ＭＭ)機能および/またはセッション管理(SM)機能の1つまたは複数の態様を含んでもよく、または管理してもよい。第2のオーセンティケータ235-aは、訪問先セルラーネットワーク205-aによってUE115-aの認証を促進および管理してもよく、後続のセキュリティ鍵が導出され得るアンカーセッション鍵を維持してもよい。V-UP-GW210-aは、ユーザプレーンセキュリティがV-UP-GW210-aにおいて終了するとき、UE115-aに対するユーザプレーンセキュリティコンテキスト(たとえば、セキュリティ鍵)を維持し得る。ユーザプレーンセキュリティは、RAN220および/またはV-UP-GW210-aによって終了されてもよく、ネットワークによって構成されてもよい。一般に、UE115-aは、訪問先セルラーネットワーク205-aの各ノードを用いてセキュリティコンテキストを維持し得る。

【００５３】

訪問先セルラーネットワーク205-aにアクセスすると、第2のオーセンティケータ235-aは、UE115-aおよび認証サーバ245によって実行されるEAP手順を促進し得る。第2のオーセンティケータ235-aは、認証サーバ245を用いてEAP手順を実行するためのセキュアなチャネルを、(ホームセルラーネットワーク205の)第1のオーセンティケータ235を介して確立または維持し得る。

【００５４】

UE115-aおよび認証サーバ245によって実行されるEAP手順は、UE115-aと認証サーバ245との間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。EAP手順を実行することの一部として、UE115-aおよび認証サーバ245はそれぞれ、MSKおよびEMSKを導出し得る。MSKおよびEMSKは、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００５５】

EAP手順が成功したとき(たとえば、UE115-aおよび認証サーバ245が首尾よく互いに認証したとき)、認証サーバ245は、セッションアンカー鍵(たとえば、第1のセキュリティ鍵)を第2のオーセンティケータ235-aに送信し得る。本開示で説明する技法によれば、セッションアンカー鍵は、EMSKに少なくとも部分的に基づき得る。セッションアンカー鍵はまた、パラメータの第2のセットに少なくとも部分的に基づき得る。パラメータの第2のセットは、訪問先セルラーネットワーク205-aの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UE115-aと第2のセルラーネットワーク205-aとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００５６】

UE115-aは、セッションアンカー鍵を単独で導出し得る。第2のセッションアンカー鍵に少なくとも部分的に基づいて、UE115-aおよび第2のオーセンティケータ235-aは、図3に示すように、互いに認証し、追加のセキュリティ鍵(たとえば、第2のセルラーネットワーク205-aの他のノードまたは機能に対するセキュリティ鍵)を導出し得る。

【００５７】

図2に示すものに対する代替において、H-SEAFおよびV-SEAFを与えるサーバまたはデバイスは、UE115-aと認証サーバ245との間で実行されるEAP手順においてオーセンティケータの役割を担うことはなく、代わりに、オーセンティケータは、認証サーバ245(たとえば、AUSFを与えるサーバ)と一緒に置かれてよい。これらの例では、認証サーバ245は、MSKまたはEMSKおよびパラメータの第2のセットに基づいてH-SEAFまたはV-SEAFに対するセッションアンカー鍵を導出し、セッションアンカー鍵を(非ローミングシナリオにおいて)H-SEAFに、または(ローミングシナリオにおいて)V-SEAFに送信し得る。

【００５８】

図3は、本開示の様々な態様による、ワイヤレス通信システムに対する鍵階層構造300の一例を示す。この解法は、EAPサーバ(たとえば、図2に関して説明した認証サーバ245)から伝えられる鍵(たとえば、K_{SEAF})を導出するためにEMSKを使用することによって一般的なEAPプロトコルに対する3GPPサービングネットワークに供給される鍵に結合するサービングネットワークを提供する。いくつかの例では、鍵階層構造300は、図1および図2に関して説明したワイヤレス通信システム100および200によって使用され得る。たとえば、UEおよび/またはネットワークノードは、図1および図2に関して説明した認証またはセキュリティ機能の1つまたは複数の態様を実装するために鍵階層構造300を使用し得る。

【００５９】

鍵階層構造300は、汎用加入者識別モジュール(USIM)とARPFとの間のセキュリティコンテキストとして使用されるKルート鍵305を含み得る。Kルート鍵305は、認証サーバとUEとの間(たとえば、図2に関して説明した認証サーバ245とUE115-aとの間)のセキュリティコンテキストを与えるためにEAP手順を実行して鍵310(たとえば、MSKおよびEMSK)を導出するためのベースとして使用され得る。Kルート鍵305は、共有鍵ベースのEAP手順を実行するために使用され得るが、1つまたは複数の他の鍵(たとえば、証明書に基づいて導出される鍵)は、証明書ベースのEAP手順を実行するときに使用され得る。EMSKは、オーセンティケータのために(たとえば、図2に関して説明した第2のオーセンティケータ235-aのために)K_{SEAF}アンカーセッション鍵315を導出するために認証サーバ(たとえば、AUSF)およびUEによって使用され得る。EMSK(MSKではない)はK_{SEAF}を導出するために使用されるので、3GPPアクセスに対するクレデンシャルの使用を制限する必要はない。たとえば、非3GPPエンティティがEAP認証に基づくMSKを取得するとき、K_{SEAF}は非3GPPエンティティに知られていないEMSKから導出されるので、非3GPPエンティティはK_{SEAF}を導出することはできない。K_{SEAF}アンカーセッション鍵315は、オーセンティケータおよびUEによって維持され得る。

【００６０】

K_{SEAF}アンカーセッション鍵315は、K_{CP-CN}鍵320およびK_{UP-GW}鍵325を導出するためにオーセンティケータによって使用され得る。K_{CP-CN}鍵320は、CP-CN機能(たとえば、図2に関して説明したV-CP-CN215)およびUEによって維持され得る。K_{UP-GW}鍵325

は、UP-GW機能(たとえば、図2に関して説明したV-UP-GW210-a)およびUEによって維持され得る。K_{UP-GW}鍵325は、$K_{UP-GWenc}$鍵340および$K_{UP-GWint}$鍵345を確立するためにUP-GWによって使用され得る。$K_{UP-GWenc}$鍵340および$K_{UP-GWint}$鍵345は、ユーザプレーンパケットの完全性保護および符号化のために使用され得る。

【００６１】

K_{CP-CN}鍵320は、K_{NASenc}鍵330、K_{NASint}鍵335、および$K_{AN/NH}$鍵350を導出するためにCP-CN機能によって使用され得る。$K_{AN/NH}$鍵350は、K_{UPint}鍵355、K_{UPenc}鍵360、K_{RRCint}鍵365、およびK_{RRCenc}鍵370を導出するためにアクセスノードによって使用され得、それらは、RRCおよびユーザプレーンパケットの完全性保護および符号化のために使用され得る。

【００６２】

図4は、本開示の様々な態様によるワイヤレス通信システム400の一例を示す。ワイヤレス通信システム400は、UE115-bのホームセルラーネットワーク205-bとUE115-bによって訪問されるセルラーネットワーク(すなわち、訪問先セルラーネットワーク205-c)とを含み得る。

【００６３】

ホームセルラーネットワーク205-bは、第1のオーセンティケータ235-b(たとえば、H-SEAFを与えるサーバまたはデバイス)とH-UP-GW210-bとを含み得る。ホームセルラーネットワーク205-bはまた、他の機能(図示せず)を与える他のサーバまたはデバイスを含み得る。訪問先セルラーネットワーク205-cは、第2のオーセンティケータ235-c(たとえば、V-SEAFを与えるサーバまたはデバイス)、V-UP-GW210-c、V-CP-CN215-a、およびRAN220-aを含み得る。いくつかの例では、RAN220-aは、図1に関して説明したネットワークノード135、ネットワークアクセスデバイス105、およびネットワークアクセスデバイスコントローラ125のうちの1つまたは複数を含み得る。第1のオーセンティケータ235-b、H-UP-GW210-b、第2のオーセンティケータ235-c、V-UP-GW210-c、およびV-CP-CN215-aは、図1に関して説明したコアネットワーク130の例示的な構成要素であり得る。

【００６４】

ホームセルラーネットワーク205-bは、認証サーバ245-aと通信中であり得る(または認証サーバ245-aを与え得る)。認証サーバ245-aは、AUSFを与え得る。認証サーバ245-aは、ARPF240-aにアクセスしてもよく、および/またはARPF240-aを呼び出してもよい。

【００６５】

第1のオーセンティケータ235-b、H-UP-GW210-b、第2のオーセンティケータ235-c、V-UP-GW210-c、V-CP-CN215-a、RAN220-a、認証サーバ245-a、およびARPF240-aは、図2に関して説明した、同様に番号付けられた構成要素、機能、またはノードの例であり得る。

【００６６】

図4はまた、非セルラーアクセスノード410(たとえば、WLANアクセスポイント(AP)またはワイヤレスLANコントローラ(WLC))を含む非セルラーネットワーク405を示す。図示のように、UE115-bは、RAN220-aまたは非セルラーアクセスノード410に接続されてもよく、各場合において、同じ認証サーバ245-aが、UE115-bを用いてEAP手順を実行し得る。UE115-bがRAN220-aに接続するとき、第2のオーセンティケータ235-cは、UE115-bおよび認証サーバ245-aによって実行されるEAP手順においてオーセンティケータとして役立ち得る。UE115-bが非セルラーアクセスノード410に接続するとき、非セルラーアクセスノード410は、UE115-bおよび認証サーバ245-aによって実行されるEAP手順においてオーセンティケータとして役立ち得る。

【００６７】

UE115-bおよび認証サーバ245-aがともに、同じEAP手順を実行することおよび(たとえば、UE115-bと第2のオーセンティケータ235-cとの間の認証手順を実行するため、またはUE115-bと非セルラーアクセスノード410との間の認証手順を実行するために)同じセッションアンカー鍵を導出することができる場合、非セルラーアクセスノード410を危う

くする攻撃者は、非セルラーアクセスノード410からセッションアンカー鍵を取得し、訪問先セルラーネットワーク205-cまたはホームセルラーネットワーク205-bのノードになりすますためにそのセッションアンカー鍵を使用することが可能になる場合がある。前述の問題を解決するために、UE115-bおよび認証サーバ245-aは、オーセンティケータに関連付けられたネットワークのタイプ(たとえば、第2のオーセンティケータ235-cまたは非セルラーアクセスノード410に関連付けられたネットワークのタイプ)を決定し、セッションアンカー鍵を導出する(すなわち、ネットワークのタイプに基づくセッションアンカー鍵を導出する)ために(MSKとEMSKとの間で)どの鍵を使用するかを決定し得る。いくつかの例では、MSKは、オーセンティケータ(たとえば、非セルラーアクセスノード410)が非セルラーアクセスネットワーク(たとえば、非セルラーネットワーク405)に関連付けられているときに使用されてもよく、EMSKは、オーセンティケータ(たとえば、第2のオーセンティケータ235-c)がセルラーアクセスネットワーク(たとえば、訪問先セルラーネットワーク205-c)に関連付けられているときに使用されてもよい。加えて、セルラーネットワークに関連付けられたオーセンティケータのために導出されるセッションアンカー鍵は、セルラーネットワークに関連付けられたパラメータのセットに少なくとも部分的に基づいて導出され得る。たとえば、K_{SEAF}鍵は、鍵導出式(KDF)

K_{SEAF}=KDF(EMSK、PLMN ID、CTX)

に基づいてUE115-bおよび認証サーバ245-aによって導出されてもよく、ここでPLMN IDは、サービング(たとえば、訪問先)セルラーネットワーク205-bに関連付けられたパブリックランドモバイルネットワーク識別子であり、EAP手順の間に認証サーバ245-aに供給され、CTXは、アクセス技術(たとえば、5G(NextGen)、4G、LTE/LTE-A、または3Gのネットワークアクセスなどのセルラーネットワークアクセス)を記述するコンテキスト(context)である。K_{SEAF}はまた、他の好適なパラメータに少なくとも部分的に基づいて導出され得ることは、当業者には諒解されよう。

【００６８】

オーセンティケータに関連付けられたネットワークのタイプに基づいてオーセンティケータのためのセッションアンカー鍵を導出することによって、一ネットワークタイプのネットワークは、別のタイプのネットワークのためのセッションアンカー鍵を取得すること、および異なるネットワークタイプのノードになりすますことができなくなる。それゆえ、同じEAP手順(または認証方法)が、異なるタイプのネットワークのセキュリティに影響を及ぼすことなく、異なるタイプのネットワークのために使用され得る。

【００６９】

図5は、本開示の様々な態様による、UE115-cと、セルラーネットワーク205-dと、認証サーバ245-bとの間の例示的なメッセージフロー500を示す。UE115-cは、図1、図2および図4に関して説明したUE115の態様の一例であってもよい。セルラーネットワーク205-dは、図2および図4に関して説明したセルラーネットワーク205の一例であってもよく、いくつかの場合には、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含んでもよい。認証サーバ245-bは、図2および図4に関して説明した認証サーバ245の態様の一例であってもよい。セルラーネットワーク205-dは、RAN220-bとセルラーCN550とを含み得る。RAN220-bおよびCN550は、図2および図4に関して説明したRAN220およびCNの例であり得る。いくつかの例では、RAN220-bは、図1に関して説明したネットワークノード135、ネットワークアクセスデバイス105、またはネットワークアクセスデバイスコントローラ125のうちの1つまたは複数を含み得る。CN550は、図2および図4に関して説明したオーセンティケータ235の態様の一例であり得る、オーセンティケータ235-d(たとえば、CN550のノード)を含み得る。

【００７０】

505において、UE115-cはセルラーネットワーク205-dにアクセスしてもよく、UE115-cまたはセルラーネットワーク205-dはEAP手順を開始してもよい。いくつかの例では、UE115-cは、RAN220-bのネットワークアクセスデバイス(たとえば、ネットワークノード)

を介してセルラーネットワーク205-dにアクセスし得る。RAN220-bは、CN550と通信中であり得る。CN550内部のオーセンティケータ235-dは、EAP手順の実施を促進し得る。セルラーネットワークの代替構成では、オーセンティケータ235-dは、RAN220-bの一部であってもよく、または認証サーバ245-bと一緒に置かれてもよい。

【００７１】

510において、セルラーネットワーク205-dは、EAP手順を実行するための要求を認証サーバ245-bに送信し得る。いくつかの例では、510において送信された要求は、オーセンティケータ235-dと認証サーバ245-bとの間のセキュアなチャネル上で送信され得る(たとえば、要求は、Diameterプロトコルを使用して(たとえば、Diameterカプセル化を使用して)オーセンティケータ235-dと認証サーバ245-bとの間で送信され得る)。

【００７２】

515において、UE115-cおよび認証サーバ245-bは、オーセンティケータ235-dを介してEAP手順を実行してもよく、オーセンティケータ235-dは、UE115-cと認証サーバ245-bとの間で送信されるメッセージに対するトランスポートを与える。EAP手順は、UE115-cと認証サーバ245-bとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。EAP手順を実行することの一部として、UE115-cおよび認証サーバ245-bの各々は、MSKおよびEMSKを導出し得る。MSKおよびEMSKは、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づいて導出され得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００７３】

505、510、または515における動作の前、途中、または後において、UE115-cおよび認証サーバ245-bはそれぞれ、オーセンティケータ235-dがセルラーネットワーク(すなわち、セルラーネットワーク205-d)に関連付けられたものと決定し得る。

【００７４】

520および525において、UE115-cおよび認証サーバ245-bの各々は、セルラーネットワーク205-dに対する第1のセキュリティ鍵を単独で導出し得る。なぜならば、UE115-cおよび認証サーバ245-bはそれぞれ、オーセンティケータ235-dがセルラーネットワーク205-dに関連付けられているものと決定し、UE115-cおよび認証サーバ245-bの各々は、EMSKに少なくとも部分的に基づいて第1のセキュリティ鍵を導出し得るからである。第1のセキュリティ鍵はまた、パラメータの第2のセットに少なくとも部分的に基づいて導出され得る。いくつかの例では、パラメータの第2のセットは、セルラーネットワーク205-dの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UE115-cもしくは認証サーバ245-bとセルラーネットワーク205-cとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００７５】

530において、認証サーバ245-bは、オーセンティケータ235-dと認証サーバ245-bとの間のセキュアなチャネルを介して第1のセキュリティ鍵をオーセンティケータ235-dに送信し得る(たとえば、第1のセキュリティ鍵は、Diameterプロトコルを使用して(たとえば、Diameterカプセル化を使用して)認証サーバ245-bとオーセンティケータ235-dとの間で送信され得る)。

【００７６】

535において、UE115-cおよびセルラーネットワーク205-dは、認証手順を実行し得る。540および545において、535における認証手順を首尾よく実行すると、UE115-cおよびセルラーネットワーク205-dは、セルラーネットワーク205-dの1つまたは複数のネットワークノードに対する1つまたは複数の追加のセキュリティ鍵(たとえば、第2のセキュリティ鍵)を導出し得る。いくつかの例では、第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワ

ークノード固有のパラメータ、UE115-cとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００７７】

555において、UE115-cは、導出されたセキュリティ鍵に少なくとも部分的に基づいてセルラーネットワーク205-dと通信し得る。

【００７８】

図6は、本開示の様々な態様による、UE115-dのブロック図600を示す。UE115-dは、図1、図2、図4および図5に関して説明したUE115の態様の一例であり得る。装置115-dは、受信機610、ワイヤレス通信マネージャ620、および送信機630を含み得る。UE115-dはまたプロセッサを含み得る。これらの構成要素の各々は、互いに通信していてよい。

【００７９】

受信機610は、様々なチャネル(たとえば、制御チャネル、データチャネル、ブロードキャストチャネル、マルチキャストチャネル、ユニキャストチャネルなど)に関連付けられた基準信号、制御情報、またはユーザデータなどの信号または情報を受信し得る。受信された信号および情報は、受信機610によって(たとえば、周波数/時間追跡のために)使用されてもよく、またはワイヤレス通信マネージャ620を含むUE115-dの他の構成要素に渡されてもよい。受信機610は、図8に関して説明するトランシーバ825の態様の一例であり得る。受信機610は、単一のアンテナもしくは複数のアンテナを含んでよく、またはそれに関連してよい。

【００８０】

ワイヤレス通信マネージャ620は、UE115-dに対するワイヤレス通信の1つまたは複数の態様を管理するために使用され得る。いくつかの例では、ワイヤレス通信マネージャ620の一部は、受信機610または送信機630の中に組み込まれてよく、またはそれらと共有されてよい。ワイヤレス通信マネージャ620は、EAPマネージャ635、ネットワークタイプ識別器640、およびネットワークオーセンティケータ645を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。

【００８１】

EAPマネージャ635は、図5に関して上記で説明したように、オーセンティケータを介して認証サーバを用いてEAP手順を実行するために使用され得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。EAPマネージャ635はまた、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するために使用され得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００８２】

ネットワークタイプ識別器640は、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定するために使用され得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。

【００８３】

ネットワークオーセンティケータ645は、決定されたネットワークタイプに少なくとも部分的に基づいて、オーセンティケータを用いて少なくとも1つの認証手順を実行するために使用され得る。少なくとも1つの認証手順は、図5に関して上記で説明したように、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【００８４】

送信機630は、ワイヤレス通信マネージャ620を含む、UE115-dの他の構成要素から受信された信号または情報を送信し得る。信号または情報は、たとえば、様々なチャネル(たと

えば、制御チャネル、データチャネル、ブロードキャストチャネル、マルチキャストチャネル、ユニキャストチャネルなど)に関連付けられた基準信号、制御情報、またはユーザデータを含み得る。いくつかの例では、送信機630は、トランシーバの中で受信機610と一緒に置かれてよい。送信機630は、図8に関して説明するトランシーバ825の態様の一例であり得る。送信機630は、単一のアンテナもしくは複数のアンテナを含んでよく、またはそれに関連してよい。

【００８５】

図7は、本開示の様々な態様による、ワイヤレス通信マネージャ720のブロック図700を示す。ワイヤレス通信マネージャ720は、図6に関して説明したワイヤレス通信マネージャ620の態様の一例であり得る。

【００８６】

ワイヤレス通信マネージャ720は、EAPマネージャ635-a、ネットワークタイプ識別器640-a、ネットワークオーセンティケータ645-a、およびセルラーネットワーク通信マネージャ715を含み得る。EAPマネージャ635-a、ネットワークタイプ識別器640-a、およびネットワークオーセンティケータ645-aは、図6に関して説明したEAPマネージャ635、ネットワークタイプ識別器640、およびネットワークオーセンティケータ645の例であり得る。ネットワークオーセンティケータ645-aは、ネットワーク鍵導出器(deriver)705およびネットワークノード鍵導出器710を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。

【００８７】

EAPマネージャ635-aは、図5に関して上記で説明したように、オーセンティケータを介して認証サーバを用いてEAP手順を実行するために使用され得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。EAPマネージャ635-aはまた、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するために使用され得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【００８８】

ネットワークタイプ識別器640-aは、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定するために使用され得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。

【００８９】

ネットワークオーセンティケータ645-aは、決定されたネットワークタイプに少なくとも部分的に基づいて、オーセンティケータを用いて少なくとも1つの認証手順を実行するために使用され得る。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。

【００９０】

決定されたネットワークタイプがセルラーネットワークタイプを含むとき、ネットワーク鍵導出器705は、図5に関して上記で説明したように、セルラーネットワークに対する第1のセキュリティ鍵を導出するために使用され得る。第1のセキュリティ鍵は、EMSKおよびパラメータの第2のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第2のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。決定されたネットワークタイプが非セルラーネットワークタイプを含むとき、ネットワーク鍵導出器705は、非セルラーネットワークに対する第1のセキュリティ鍵を導出するために使用され得る。

【００９１】

決定されたネットワークタイプがセルラーネットワークタイプを含むとき、ネットワークノード鍵導出器710は、図5に関して上記で説明したように、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出するために使用され得る。第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【００９２】

セルラーネットワーク通信マネージャ715は、図5に関して上記で説明したように、第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してセルラーネットワークと通信するために使用され得る。

【００９３】

図8は、本開示の様々な態様による、ワイヤレス通信システム800の図を示す。ワイヤレス通信システム800は、図1、図2および図4～図6に関して説明したUE115の態様の一例であり得るUE115-eを含み得る。

【００９４】

UE115-eは、ワイヤレス通信マネージャ805、メモリ810、プロセッサ820、トランシーバ825、およびアンテナ830を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。ワイヤレス通信マネージャ805は、図6および図7に関して説明したワイヤレス通信マネージャ620および720の態様の一例であり得る。

【００９５】

メモリ810は、ランダムアクセスメモリ(RAM)または読取り専用メモリ(ROM)を含み得る。メモリ810は、実行されると、プロセッサ820に、ネットワークセキュリティおよび認証に関する機能を含む、本明細書で説明する様々な機能を実行させる命令を含むコンピュータ可読、コンピュータ実行可能ソフトウェア815を記憶し得る。いくつかの場合、ソフトウェア815は、プロセッサ820によって直接実行可能ではないことがあるが、(たとえば、コンパイルされ、実行されると)本明細書で説明する機能をプロセッサ820に実行させ得る。プロセッサ820は、インテリジェントハードウェアデバイス(たとえば、中央処理装置(CPU)、マイクロコントローラ、特定用途向け集積回路(ASIC)など)を含み得る。

【００９６】

トランシーバ825は、本明細書で説明するように、1つまたは複数のアンテナまたは有線リンクを介して、1つまたは複数のネットワークと双方向に通信し得る。たとえば、トランシーバ825は、セルラーネットワーク205-e(またはそれの1つまたは複数のノード)または別のUE115-fと双方向に通信し得る。トランシーバ825は、パケットを変調し、変調されたパケットを送信のためにアンテナに供給するために、かつアンテナから受信されたパケットを復調するために、モデムを含み得る。いくつかの場合、UE115-eは、単一のアンテナ830を含み得る。しかしながら、いくつかの場合、UE115-eは、複数のワイヤレス送信を同時に送信または受信することが可能であり得る複数のアンテナ830を有し得る。

【００９７】

図9は、本開示の様々な態様による、認証サーバ245-cのブロック図900を示す。認証サーバ245-cは、図2、図4および図5に関して説明した認証サーバ245の態様の一例であってもよい。認証サーバ245-cは、受信機910と、通信マネージャ920と、送信機930とを含み得る。認証サーバ245-cはまた、プロセッサを含み得る。これらの構成要素の各々は、互いに通信していてよい。

【００９８】

受信機910は、セルラーネットワーク、WLANなどのノードを含む様々なネットワークノードから認証要求を受信し得る。受信機910はまた、ネットワークノードを介してUEから認証情報を受信し得る。受信された認証要求および認証情報は、認証マネージャ920に渡されてもよい。受信機910は、図10に関して説明する認証インターフェース1025の態様

の一例であってよい。受信機910は、1つまたは複数の有線および/またはワイヤレスのインターフェースを含み得る。

【００９９】

認証マネージャ920は、認証サーバ245-cに対するデバイス認証の1つまたは複数の態様を管理するために使用され得る。いくつかの例では、認証マネージャ920の一部は、受信機910または送信機930の中に組み込まれてよく、またはそれらと共有されてよい。認証マネージャ920は、EAPマネージャ935、ネットワークタイプ識別器940、ネットワーク鍵導出器945、およびネットワーク鍵インストーラ950を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。

【０１００】

EAPマネージャ935は、図5に関して上記で説明したように、オーセンティケータを介してUEを用いてEAP手順を実行するために使用され得る。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。EAPマネージャ935はまた、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出するために使用され得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。

【０１０１】

ネットワークタイプ識別器940は、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定するために使用され得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。

【０１０２】

ネットワーク鍵導出器945は、図5に関して上記で説明したように、MSKまたはEMSKとネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出するために使用され得る。決定されたネットワークタイプがセルラーネットワークタイプを含むとき、いくつかの例では、パラメータの第2のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、認証サーバとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【０１０３】

ネットワーク鍵インストーラ950は、図5に関して上記で説明したように、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信するために使用され得る。

【０１０４】

送信機930は、認証フィードバックメッセージと、認証マネージャ920を含む認証サーバ245-cの他の構成要素から受信されたセキュリティ鍵とを送信し得る。送信機930は、図10に関して説明する認証インターフェース1025の態様の一例であってよい。送信機930は、1つまたは複数の有線および/またはワイヤレスのインターフェースを含み得る。

【０１０５】

図10は、本開示の様々な態様による、認証サーバ245-dのブロック図1000を示す。認証サーバ245-dは、図2、図4、図5および図9に関して説明した認証サーバ245の態様の一例であってもよい。

【０１０６】

認証サーバ245-dは、認証マネージャ1005、メモリ1010、プロセッサ1020、および認

証インターフェース1025を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。認証マネージャ1005は、図9に関して説明した認証マネージャ920の態様の一例であってもよい。

【０１０７】

メモリ1010は、RAMまたはROMを含み得る。メモリ1010は、実行されると、プロセッサ1020に、ネットワークセキュリティおよび認証に関する機能を含む、本明細書で説明する様々な機能を実行させる命令を含むコンピュータ可読、コンピュータ実行可能ソフトウェア1015を記憶し得る。いくつかの場合、ソフトウェア1015は、プロセッサ1020によって直接実行可能ではないことがあるが、(たとえば、コンパイルされ、実行されると)本明細書で説明する機能をプロセッサ1020に実行させ得る。プロセッサ1020は、インテリジェントハードウェアデバイス(たとえば、CPU、マイクロコントローラ、ASICなど)を含み得る。

【０１０８】

認証インターフェース1025は、本明細書で説明するように、1つまたは複数のアンテナまたは有線リンクを介して、1つまたは複数のネットワーク、ネットワークノード、またはUEと双方向に通信し得る。いくつかの例では、認証インターフェース1025は、(たとえば、Radiusプロトコルまたは Diameterプロトコルを使用して)ネットワークノードとのセキュアな接続を確立するため、ならびにセキュアな接続およびネットワークノードを介してUEと双方向に通信するために使用され得る。

【０１０９】

図11は、本開示の様々な態様による、ネットワークノード1105のブロック図1100を示す。ネットワークノード1105は、図2、図4および図5に関して説明したネットワークノードの態様の一例であってもよく、いくつかの例では、図2、図4および図5に関して説明したオーセンティケータ235の一例であってもよい。ネットワークノード1105は、受信機1110と、通信マネージャ1120と、送信機1130とを含み得る。ネットワークノード1105はまた、プロセッサを含み得る。これらの構成要素の各々は、互いに通信していてよい。

【０１１０】

受信機1110は、他のネットワークノード、UE、認証サーバなどから信号または情報を受信し得る。受信された信号および情報は、通信マネージャ1120を含むネットワークノード1105の他の構成要素に渡されてよい。受信機1110は、図13に関して説明する認証インターフェース1325の態様の一例であってよい。受信機1110は、1つまたは複数の有線および/またはワイヤレスのインターフェースを含み得る。

【０１１１】

通信マネージャ1120は、ネットワークノード1105のためのワイヤレス通信の1つまたは複数の態様を管理するために使用され得る。いくつかの例では、通信マネージャ1120の一部は、受信機1110または送信機1130の中に組み込まれてよく、またはそれらと共有されてよい。通信マネージャ1120は、ネットワーク鍵マネージャ1135およびUEオーセンティケータ1140を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。

【０１１２】

ネットワーク鍵マネージャ1135は、図5に関して上記で説明したように、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信するために使用され得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。いくつかの例では、パラメータの第1のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、パラメータの第2のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメ

ータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【０１１３】

UEオーセンティケータ1140は、図5に関して上記で説明したように、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行するために使用され得る。

【０１１４】

送信機1130は、通信マネージャ1120を含むネットワークノード1105の他の構成要素から受信された信号または情報を送信し得る。送信機1130は、図13に関して説明する認証インターフェース1325の態様の一例であってよい。受信機1110は、1つまたは複数の有線および/またはワイヤレスのインターフェースを含み得る。

【０１１５】

図12は、本開示の様々な態様による、通信マネージャ1220のブロック図1200を示す。通信マネージャ1220は、図11に関して説明した通信マネージャ1120の態様の一例であり得る。

【０１１６】

通信マネージャ1220は、ネットワーク鍵マネージャ1135-a、UEオーセンティケータ1140-a、およびUE通信マネージャ1210を含み得る。ネットワーク鍵マネージャ1135-a、およびUEオーセンティケータ1140-aは、図11に関して説明したネットワーク鍵マネージャ1135およびUEオーセンティケータ1140の例であり得る。UEオーセンティケータ1140-aは、ネットワークノード鍵導出器1205を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。

【０１１７】

ネットワーク鍵マネージャ1135-aは、図5に関して上記で説明したように、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信するために使用され得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。いくつかの例では、パラメータの第1のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、パラメータの第2のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【０１１８】

UEオーセンティケータ1140-aは、図5に関して上記で説明したように、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行するために使用され得る。ネットワークノード鍵導出器1205は、少なくとも1つの認証手順を実行するために使用されてもよく、UEは、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出する。第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。

【０１１９】

UE通信マネージャ1210は、図5に関して上記で説明したように、第2のセキュリティ鍵に

少なくとも部分的に基づいてネットワークノードを介してUEと通信するために使用され得る。

【０１２０】

図13は、本開示の様々な態様による、ネットワークノード1105-aの図1300を示す。ネットワークノード1105-aは、図2、図4、図5および図11に関して説明したネットワークノードの態様の一例であってもよい。

【０１２１】

ネットワークノード1105-aは、通信マネージャ1305、メモリ1310、プロセッサ1320、および認証インターフェース1325を含み得る。これらの構成要素の各々は、(たとえば、1つまたは複数のバスを介して)直接または間接的に互いに通信し得る。通信マネージャ1305は、図11または図12に関して説明した通信マネージャの態様の一例であり得る。

【０１２２】

メモリ1310は、RAMまたはROMを含み得る。メモリ1310は、実行されると、プロセッサ1320に、ネットワークセキュリティおよび認証に関する機能を含む、本明細書で説明する様々な機能を実行させる命令を含むコンピュータ可読、コンピュータ実行可能ソフトウェア1315を記憶し得る。いくつかの場合、ソフトウェア1315は、プロセッサ1320によって直接実行可能ではないことがあるが、(たとえば、コンパイルされ、実行されると)本明細書で説明する機能をプロセッサ1320に実行させ得る。プロセッサ1320は、インテリジェントハードウェアデバイス(たとえば、CPU、マイクロコントローラ、ASICなど)を含み得る。

【０１２３】

認証インターフェース1325は、本明細書で説明するように、1つまたは複数のアンテナまたは有線リンクを介して、1つまたは複数のネットワーク、ネットワークノード、またはUEと双方向に通信し得る。いくつかの例では、認証インターフェース1325は、(たとえば、RadiusプロトコルまたはDiameterプロトコルを使用して)認証サーバとのセキュアな接続を確立するため、およびUEおよび認証サーバによって実行されるEAP手順を促進するために使用され得る。

【０１２４】

図14は、本開示の様々な態様による、ワイヤレス通信のための方法1400を示すフローチャートを示す。方法1400の動作は、図1～図8に関して説明したように、UE115またはそれの構成要素によって実行され得る。いくつかの例では、方法1400の動作は、図6～図8に関して説明したワイヤレス通信マネージャによって実行され得る。いくつかの例では、UEは、以下で説明する機能を実行するためにUEの機能要素を制御するためのコードのセットを実行し得る。追加または代替として、UEは、専用ハードウェアを使用して、以下で説明する機能の態様を実行し得る。

【０１２５】

ブロック1405において、UEは、図5に関して上記で説明したように、オーセンティケータを介して認証サーバを用いてEAP手順を実行し得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。いくつかの例では、ブロック1405の動作は、図6および図7に関して説明したEAPマネージャ635を使用して実行され得る。

【０１２６】

ブロック1410において、UEは、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出し得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1410の動作は、図6および図7に関して説明したEAPマネージャ635を使用して実行され得る。

【０１２７】

ブロック1415において、UEは、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定し得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。いくつかの例では、ブロック1415の動作は、図6および図7に関して説明したネットワークタイプ識別器640を使用して実行され得る。

【０１２８】

ブロック1420において、UEは、決定されたネットワークタイプに少なくとも部分的に基づいて、オーセンティケータを用いて少なくとも1つの認証手順を実行し得る。少なくとも1つの認証手順は、図5に関して上記で説明したように、MSKまたはEMSKと決定されたネットワークタイプとの関連に少なくとも部分的に基づき得る。いくつかの例では、ブロック1420の動作は、図6および図7に関して説明したネットワークオーセンティケータ645を使用して実行され得る。

【０１２９】

図15は、本開示の様々な態様による、ワイヤレス通信のための方法1500を示すフローチャートを示す。方法1500の動作は、図1～図8に関して説明したように、UE115またはそれの構成要素によって実行され得る。いくつかの例では、方法1500の動作は、図6～図8に関して説明したワイヤレス通信マネージャによって実行され得る。いくつかの例では、UEは、以下で説明する機能を実行するためにUEの機能要素を制御するためのコードのセットを実行し得る。追加または代替として、UEは、専用ハードウェアを使用して、以下で説明する機能の態様を実行し得る。

【０１３０】

ブロック1505において、UEは、図5に関して上記で説明したように、オーセンティケータを介して認証サーバを用いてEAP手順を実行し得る。EAP手順は、UEと認証サーバとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。いくつかの例では、ブロック1505の動作は、図6および図7に関して説明したEAPマネージャ635を使用して実行され得る。

【０１３１】

ブロック1510において、UEは、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出し得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1510の動作は、図6および図7に関して説明したEAPマネージャ635を使用して実行され得る。

【０１３２】

ブロック1515において、UEは、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定し得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。いくつかの例では、ブロック1515の動作は、図6および図7に関して説明したネットワークタイプ識別器640を使用して実行され得る。

【０１３３】

ブロック1520において、方法1500は、決定されたネットワークタイプがセルラーネットワークタイプを含むかまたは非セルラーネットワークタイプを含むかに応じて、ブロック1525かまたは1540に分岐し得る。決定されたネットワークタイプがセルラーネットワークタイプを含むとき、方法1500はブロック1525に分岐し得る。決定されたネットワークタイプが非セルラーネットワークタイプを含むとき、方法1500はブロック1540に分岐し得る。いくつかの例では、ブロック1520の動作は、図6および図7に関して説明したネットワークタイプ識別器640を使用して実行され得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。

【０１３４】
ネットワークタイプがセルラーネットワークタイプを含むものとUEが決定した場合、ブロック1525および1530において、UEは、決定されたネットワークタイプに少なくとも部分的に基づいて、オーセンティケータを用いて少なくとも1つの認証手順を実行し得る。少なくとも1つの認証手順は、MSKまたはEMSKと決定されたネットワークタイプとの関連に基づき得る。ブロック1525において、UEは、図5に関して上記で説明したように、セルラーネットワークに対する第1のセキュリティ鍵を導出し得る。第1のセキュリティ鍵は、EMSKおよびパラメータの第2のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第2のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1525の動作は、図6および図7に関して説明したネットワークオーセンティケータ645、または図7に関して説明したネットワーク鍵導出器705を使用して実行され得る。
【０１３５】
ブロック1530において、UEは、図5に関して上記で説明したように、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出し得る。第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1530の動作は、図6および図7に関して説明したネットワークオーセンティケータ645、または図7に関して説明したネットワークノード鍵導出器710を使用して実行され得る。
【０１３６】
ブロック1535において、UEは、図5に関して上記で説明したように、第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してセルラーネットワークと通信し得る。いくつかの例では、ブロック1530の動作は、図7に関して説明したセルラーネットワーク通信マネージャ715を使用して実施され得る。
【０１３７】
ネットワークタイプが非セルラーネットワークタイプを含むものとUEが決定した場合、ブロック1540において、UEは、非セルラーネットワークに対する第1のセキュリティ鍵を導出し得る。第1のセキュリティ鍵は、MSKおよびパラメータの第4のセットに少なくとも部分的に基づき得る。いくつかの例では、ブロック1540の動作は、図6および図7に関して説明したネットワークオーセンティケータ645、または図7に関して説明したネットワーク鍵導出器705を使用して実行され得る。
【０１３８】
図16は、本開示の様々な態様による、ワイヤレス通信のための方法1600を示すフローチャートを示す。方法1600の動作は、図1～図5、図9および図10に関して説明したように、認証サーバまたはその構成要素によって実行され得る。いくつかの例では、方法1600の動作は、図9および図10に関して説明した通信マネージャによって実行され得る。いくつかの例では、認証サーバは、以下で説明する機能を実行するように認証サーバの機能要素を制御するためのコードのセットを実行し得る。追加または代替として、認証サーバは、専用ハードウェアを使用して、以下で説明する機能の態様を実行し得る。
【０１３９】
ブロック1605において、認証サーバは、図5に関して上記で説明したように、オーセンティケータを介してUEを用いてEAP手順を実行し得る。EAP手順は、認証サーバとUEとの間で交換される認証クレデンシャルのセットに少なくとも部分的に基づき得る。いくつかの例では、ブロック1605の動作は、図9に関して説明したEAPマネージャ935を使用して実行され得る。
【０１４０】

ブロック1610において、認証サーバは、図5に関して上記で説明したように、認証クレデンシャルおよびパラメータの第1のセットに少なくとも部分的に基づくMSKおよびEMSKを、EAP手順を実行することの一部として導出し得る。いくつかの例では、パラメータの第1のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1610の動作は、図9に関して説明したEAPマネージャ935を使用して実行され得る。

【０１４１】

ブロック1615において、認証サーバは、図5に関して上記で説明したように、オーセンティケータに関連付けられたネットワークタイプを決定し得る。いくつかの例では、決定されたネットワークタイプは、セルラーネットワークタイプまたは非セルラーネットワークタイプ(たとえば、WLANタイプ)を含み得る。いくつかの例では、ブロック1615の動作は、図9に関して説明したネットワークタイプ識別器940を使用して実行され得る。

【０１４２】

ブロック1620において、認証サーバは、図5に関して上記で説明したように、MSKまたはEMSKとネットワークタイプとの関連に少なくとも部分的に基づいて、およびパラメータの第2のセットに少なくとも部分的に基づいて、決定されたネットワークタイプに対するセキュリティ鍵を導出し得る。決定されたネットワークタイプがセルラーネットワークタイプを含むとき、いくつかの例では、パラメータの第2のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、認証サーバとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。いくつかの例では、ブロック1620の動作は、図9に関して説明したネットワーク鍵導出器945を使用して実行され得る。

【０１４３】

ブロック1625において、認証サーバは、図5に関して上記で説明したように、セキュリティ鍵をセキュアなチャネルを介してオーセンティケータに送信し得る。いくつかの例では、ブロック1625の動作は、図9に関して説明したネットワーク鍵インストーラ950を使用して実行され得る。

【０１４４】

図17は、本開示の様々な態様による、ワイヤレス通信のための方法1700を示すフローチャートを示す。方法1700の動作は、図1～図5および図11～図13に関して説明したように、セルラーネットワークまたはそれの構成要素によって実行され得る。いくつかの例では、方法1700の動作は、図11～図13に関して説明した通信マネージャによって実行され得る。いくつかの例では、セルラーネットワーク(またはそれの1つまたは複数のノード)は、以下で説明する機能を実行するように、セルラーネットワークの機能要素を制御するためのコードのセットを実行し得る。追加または代替として、セルラーネットワーク(またはそれの1つまたは複数のノード)は、専用ハードウェアを使用して、以下で説明する機能の態様を実行し得る。

【０１４５】

ブロック1705において、セルラーネットワークは、図5に関して上記で説明したように、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信し得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。いくつかの例では、パラメータの第1のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、パラメータの第2のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメー

タ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。いくつかの例では、ブロック1705の動作は、図11に関して説明したネットワーク鍵マネージャ1135を使用して実行され得る。

【０１４６】

ブロック1710において、セルラーネットワークは、図5に関して上記で説明したように、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行し得る。いくつかの例では、ブロック1710の動作は、図11に関して説明したUEオーセンティケータ1140を使用して実行され得る。

【０１４７】

図18は、本開示の様々な態様による、ワイヤレス通信のための方法1800を示すフローチャートを示す。方法1800の動作は、図1～図5および図11～図13に関して説明したように、セルラーネットワークまたはその構成要素によって実行され得る。いくつかの例では、方法1800の動作は、図11～図13に関して説明した通信マネージャによって実行され得る。いくつかの例では、セルラーネットワーク(またはそれの1つまたは複数のノード)は、以下で説明する機能を実行するように、セルラーネットワークの機能要素を制御するためのコードのセットを実行し得る。追加または代替として、セルラーネットワーク(またはそれの1つまたは複数のノード)は、専用ハードウェアを使用して、以下で説明する機能の態様を実行し得る。

【０１４８】

ブロック1805において、セルラーネットワークは、図5に関して上記で説明したように、EMSKおよびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信し得る。EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき得る。認証クレデンシャルは、EAP手順の間にUEと認証サーバとの間で交換され得る。いくつかの例では、パラメータの第1のセットは、セルラーネットワークの識別子、少なくとも1つのセルラーネットワーク固有のパラメータ、UEとセルラーネットワークとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、パラメータの第2のセットは、少なくとも1つの識別子、少なくとも1つの乱数、少なくとも1つのネットワークパラメータ、少なくとも1つのUEパラメータ、またはそれらの組合せを含み得る。いくつかの例では、セルラーネットワークは、5Gネットワーク、4Gネットワーク、LTEネットワーク、LTE-Aネットワーク、3Gネットワーク、またはそれらの組合せのうちの少なくとも1つを含み得る。いくつかの例では、ブロック1805の動作は、図11に関して説明したネットワーク鍵マネージャ1135を使用して実行され得る。

【０１４９】

ブロック1810において、セルラーネットワークは、第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行し得る。UEを用いて少なくとも1つの認証手順を実行することは、図5に関して上記で説明したように、セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出することを含み得る。第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づき得る。いくつかの例では、パラメータの第3のセットは、ネットワークノードの識別子、少なくとも1つのネットワークノード固有のパラメータ、UEとネットワークノードとの間で交換される少なくとも1つのパラメータ、またはそれらの組合せを含み得る。いくつかの例では、ブロック1810の動作は、図11に関して説明したUEオーセンティケータ1140、または図12に関して説明したネットワークノード鍵導出器1205を使用して実行され得る。

【０１５０】

ブロック1815において、セルラーネットワークは、図5に関して上記で説明したように、第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してUEと通

信し得る。いくつかの例では、ブロック1815の動作は、図12に関して説明したUE通信マネージャ1210を使用して実行され得る。

【０１５１】

上記で説明した方法は、本開示で説明する技法の可能な実装形態を示すことに留意されたい。いくつかの例では、方法の動作は、異なる順序で実行されてもよく、または異なる動作を含んでもよい。

【０１５２】

本明細書で説明された技法は、CDMA、TDMA、FDMA、OFDMA、SC-FDMA、および他のシステムなどの様々なワイヤレス通信システムのために使用され得る。「システム」および「ネットワーク」という用語は、しばしば、互換的に使用される。CDMAシステムは、CDMA2000、ユニバーサル地上波無線アクセス(UTRA)などの無線技術を実装してよい。CDMA2000は、IS-2000規格、IS-95規格、およびIS-856規格を対象とする。IS-2000のリリース0およびAは、CDMA2000 1X、1Xなどと呼ばれることがある。IS-856(TIA-856)は、CDMA2000 1xEV-DO、High Rate Packet Data(HRPD)などと呼ばれることがある。UTRAは、広帯域CDMA(WCDMA(登録商標))、およびCDMAの他の変形を含む。TDMAシステムは、Global System for Mobile communications(GSM(登録商標))などの無線技術を実装し得る。OFDMAシステムは、ウルトラモバイルブロードバンド(UMB)、発展型UTRA(E-UTRA)、IEEE802.11(Wi-Fi)、IEEE802.16(WiMAX)、IEEE802.20、Flash-OFDM(商標)などの無線技術を実装してもよい。UTRAおよびE-UTRAは、ユニバーサルモバイルテレコミュニケーションシステム(UMTS)の一部である。3GPP LTEおよびLTE-Aは、E-UTRAを使用するUMTSの新しいリリースである。UTRA、E-UTRA、UMTS、LTE、LTE-A、およびGSM(登録商標)は、3GPPと称する団体からの文書に記載されている。CDMA2000およびUMBは、「第3世代パートナーシッププロジェクト2」(3GPP2)と称する団体からの文書に記載されている。本明細書で説明された技法は、免許不要帯域幅または共有帯域幅を介したセルラー(たとえば、LTE)通信を含む、上述のシステムおよび無線技術、ならびに他のシステムおよび無線技術のために使用され得る。しかしながら、上の説明は、例としてLTE/LTE-Aシステムを説明し、上の説明の大部分においてLTE用語が使用されるが、技法はLTE/LTE-A適用例以外に適用可能である。

【０１５３】

添付の図面に関して上記に記載した発明を実施するための形態は、例について説明しており、実装され得る例、または特許請求の範囲内にある例のすべてを表すとは限らない。この説明で使用される場合、「例」および「例示的」という用語は、「例、事例、または例示として機能すること」を意味し、「好ましい」または「他の例よりも有利である」ことを意味しない。発明を実施するための形態は、説明した技法の理解を与えるための具体的な詳細を含む。しかしながら、これらの技法は、これらの具体的な詳細を伴うことなく実践され得る。いくつかの事例では、説明した例の概念を不明瞭にすることを回避するために、よく知られている構造および装置がブロック図の形態で示される。

【０１５４】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表されてよい。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁気粒子、光場もしくは光粒子、またはそれらの任意の組合せによって表され得る。

【０１５５】

本開示に関して説明した様々な例示的なブロックおよび構成要素は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、ASIC、FPGAもしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明した機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行され得る。汎用プロセッサはマイクロプロセッサであってよいが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってよい。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば

、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成としても実装され得る。

【０１５６】

本明細書で説明した機能は、ハードウェア、プロセッサによって実行されるソフトウェア、ファームウェア、またはそれらの任意の組合せとして実装されてよい。プロセッサによって実行されるソフトウェアで実装される場合、機能は、1つもしくは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されてよく、あるいはコンピュータ可読媒体を介して送信されてよい。他の例および実装形態が、本開示および添付の特許請求の範囲内および趣旨内にある。たとえば、ソフトウェアの性質に起因して、上記で説明した機能は、プロセッサによって実行されるソフトウェア、ハードウェア、ファームウェア、ハードワイヤリング、またはこれらのうちのいずれかの組合せを使用して実装することができる。機能を実装する構成要素はまた、異なる物理的ロケーションにおいて機能の部分が実装されるように分散されることを含めて、様々な位置において物理的に配置されてよい。特許請求の範囲内を含む本明細書で使用される場合、「または」という用語は、2つ以上の項目の列挙において使用されるとき、列挙される項目のうちのいずれか1つが単独で採用され得ること、または列挙される項目のうちの2つ以上の任意の組合せが採用され得ることを意味する。たとえば、構成が、構成要素A、B、またはCを含むものとして説明される場合、その構成は、Aのみ、Bのみ、Cのみ、AとBとの組合せ、AとCとの組合せ、BとCとの組合せ、またはAとBとCとの組合せを含むことができる。また、特許請求の範囲内を含む本明細書で使用される場合、項目の列挙(たとえば、「のうちの少なくとも1つ」または「のうちの1つまたは複数」などの句で始まる項目の列挙)の中で使用される「または」は、たとえば、「A、B、またはCのうちの少なくとも1つ」という列挙が、AまたはBまたはCまたはABまたはACまたはBCまたはABC(すなわち、AおよびBおよびC)を意味するような、選言的列挙を示す。

【０１５７】

コンピュータ可読媒体は、コンピュータ記憶媒体と、ある場所から別の場所へのコンピュータプログラムの伝達を容易にする任意の媒体を含む通信媒体の両方を含む。記憶媒体は、汎用コンピュータまたは特殊目的コンピュータによってアクセスされ得る任意の使用可能な媒体とされ得る。限定ではなく例として、コンピュータ可読媒体は、RAM、ROM、EEPROM、フラッシュメモリ、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または、命令もしくはデータ構造の形で所望のプログラムコード手段を担持しまたは記憶するのに使用され得る、汎用コンピュータもしくは特殊目的コンピュータ、もしくは汎用プロセッサもしくは特殊目的プロセッサによってアクセスされ得る任意の他の媒体を含むことができる。また、任意の接続が、適正にコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用されるディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザーディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー(登録商標)ディスク(disk)、およびブルーレイディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、レーザーを用いてデータを光学的に再生する。上記のもの組合せも、コンピュータ可読媒体の範囲内に含まれる。

【０１５８】

本開示のこれまでの説明は、当業者が本開示を作成または使用できるように与えられる。本開示の様々な修正が当業者に容易に明らかとなり、本明細書で定義される一般原理は、本開示の範囲から逸脱することなく他の変形に適用され得る。したがって、本開示は、本

明細書で説明した例および設計に限定されるものではなく、本明細書で開示する原理および新規の技法と一致する最も広い範囲が与えられるべきである。

【符号の説明】

【０１５９】

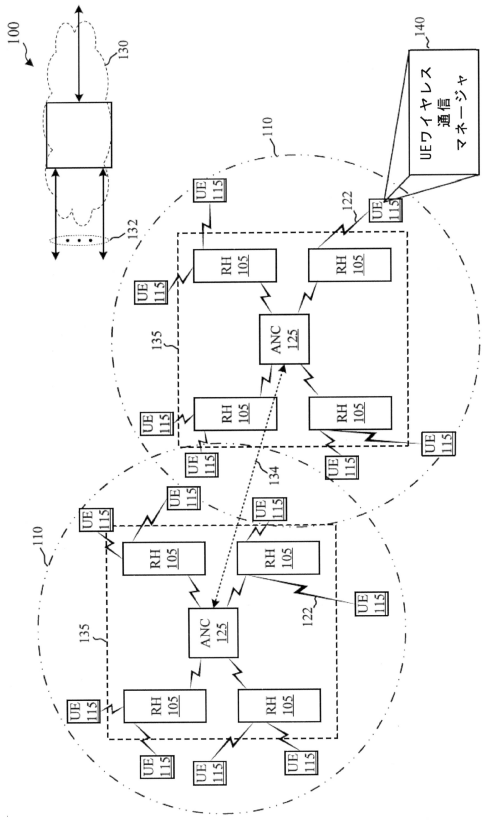
100 ワイヤレス通信システム
105 ネットワークアクセスデバイス
110 地理的カバレージエリア
115 ユーザ機器(UE)
115-a UE
115-b UE
115-c UE
115-d UE
115-e UE
115-f UE
122 通信リンク
125 ネットワークアクセスデバイスコントローラ
130 コアネットワーク
132 バックホールリンク
134 バックホールリンク
135 ネットワークノード
140 ワイヤレス通信マネージャ
200 ワイヤレス通信システム
205 ホームセルラーネットワーク
205-a 訪問先セルラーネットワーク
205-b ホームセルラーネットワーク
205-c 訪問先セルラーネットワーク
205-d セルラーネットワーク
205-e セルラーネットワーク
210 ホームユーザプレーンゲートウェイ(H-UP-GW)
210-a 訪問先ユーザプレーンゲートウェイ(V-UP-GW)
210-b H-UP-GW
210-c V-UP-GW
215 訪問先セルラーネットワーク制御プレーンコアネットワーク機能(V-CP-CN)
215-a V-CP-CN
220 無線アクセスネットワーク(RAN)
220-a RAN
220-b RAN
235 第1のオーセンティケータ
235-a 第2のオーセンティケータ
235-b 第1のオーセンティケータ
235-c 第2のオーセンティケータ
235-d オーセンティケータ
240 処理機能(ARPF)
240-a ARPF
245 認証サーバ
245-a 認証サーバ
245-b 認証サーバ
245-c 認証サーバ
245-d 認証サーバ
300 鍵階層構造

305 Kルート鍵
310 鍵
315 KSEAFアンカーセッション鍵
320 KCP-CN鍵
325 KUP-GW鍵325
330 KNASenc鍵
335 KNASint鍵
340 KUP-GWenc鍵
345 KUP-GWint鍵
350 KAN/NH鍵
355 KUPint鍵
360 KUPenc鍵
365 KRRCint鍵
370 KRRCenc鍵
400 ワイヤレス通信システム
405 非セルラーネットワーク
410 非セルラーアクセスノード
500 メッセージフロー
505 番号
510 番号
515 番号
520 番号
525 番号
530 番号
535 番号
540 番号
545 番号
550 番号
555 番号
600 ブロック図
610 受信機
620 ワイヤレス通信マネージャ
630 送信機
635 拡張可能認証プロトコル(EAP)マネージャ
635-a EAPマネージャ
640 ネットワークタイプ識別器
640-a ネットワークタイプ識別器
645 ネットワークオーセンティケータ
645-a ネットワークオーセンティケータ
700 ブロック図
705 ネットワーク鍵導出器
710 ネットワークノード鍵導出器
715 セルラーネットワーク通信マネージャ
720 ワイヤレス通信マネージャ
800 ワイヤレス通信システム
805 ワイヤレス通信マネージャ
810 メモリ
815 コンピュータ可読、コンピュータ実行可能ソフトウェア
820 プロセッサ
825 トランシーバ

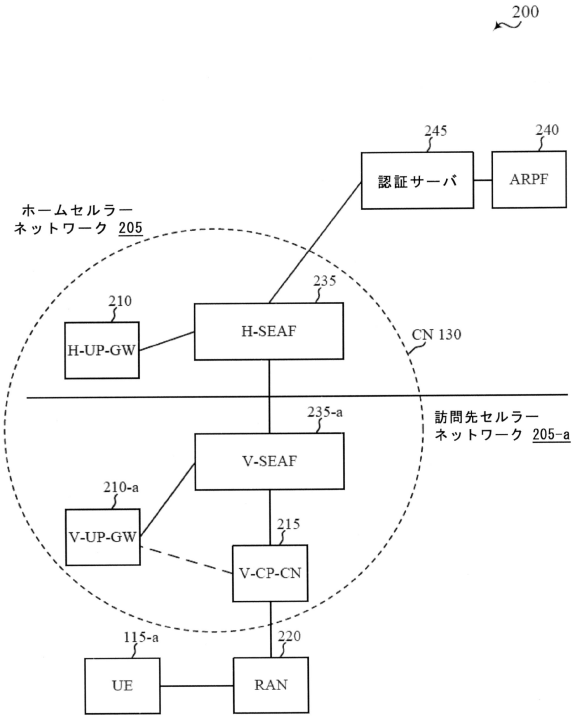
830 アンテナ
900 ブロック図
910 受信機
920 認証マネージャ
930 送信機
935 EAPマネージャ
940 ネットワークタイプ識別器
945 ネットワーク鍵導出器
950 ネットワーク鍵インストーラ
1000 ブロック図
1005 認証マネージャ
1010 メモリ
1015 コンピュータ可読、コンピュータ実行可能ソフトウェア
1020 プロセッサ
1025 認証インターフェース
1100 ブロック図
1105 ネットワークノード
1105-a ネットワークノード
1110 受信機
1120 通信マネージャ
1130 送信機
1135 ネットワーク鍵マネージャ
1135-a ネットワーク鍵マネージャ
1140 UEオーセンティケータ
1140-a UEオーセンティケータ
1200 ブロック図
1205 ネットワークノード鍵導出器
1210 UE通信マネージャ
1220 通信マネージャ
1300 図
1305 通信マネージャ
1310 メモリ
1315 コンピュータ可読、コンピュータ実行可能ソフトウェア
1320 プロセッサ
1325 認証インターフェース

【図面】

【図１】



【図２】



【図３】

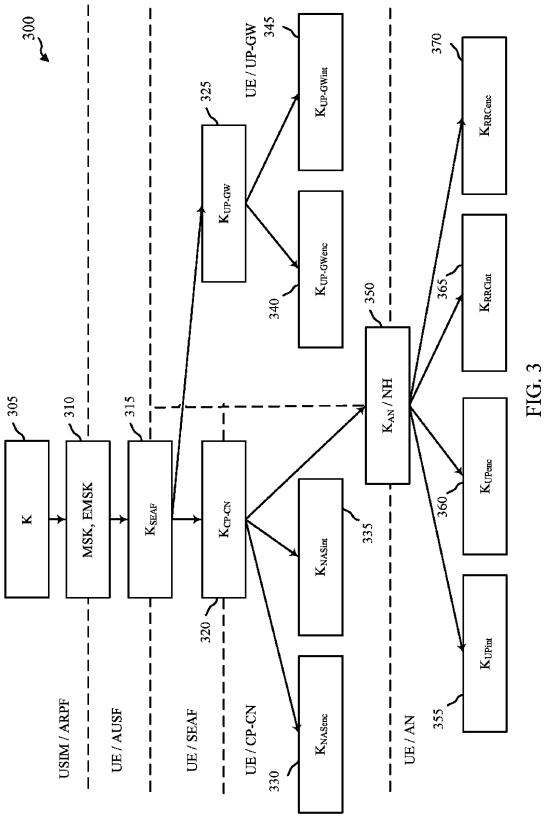
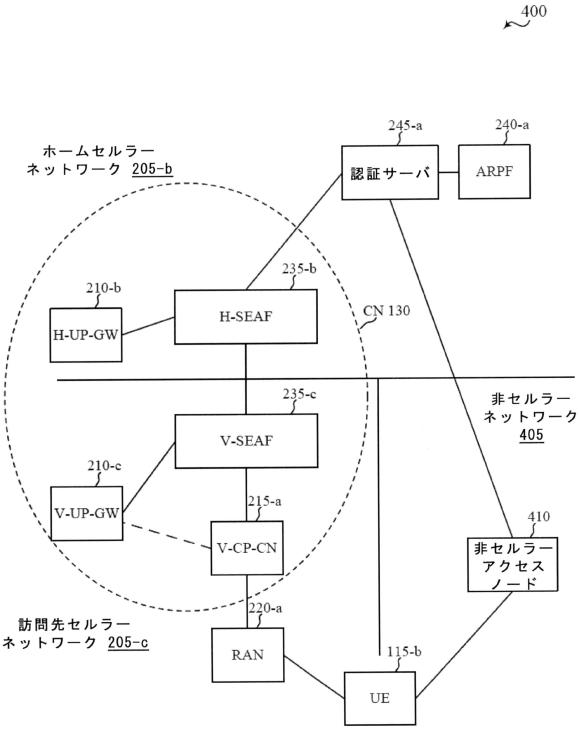
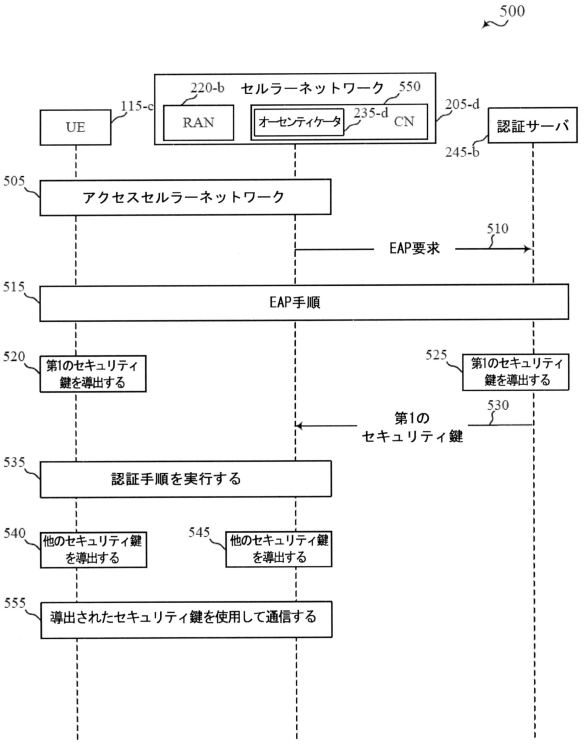


FIG. 3

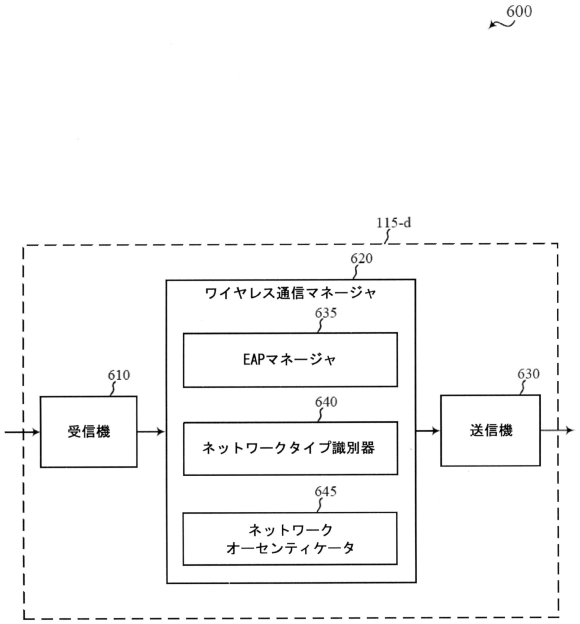
【図４】



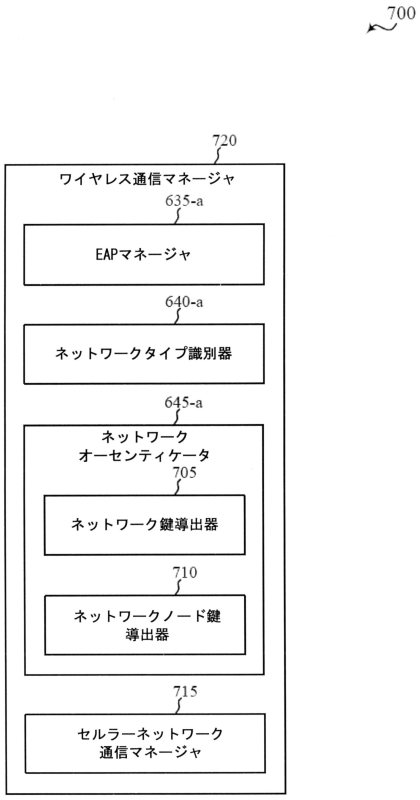
【図５】


500
220-b
セルラーネットワーク
550
115-c
UE
RAN
オーセンティケータ
235-d
CN
205-d
認証サーバ
245-b
505
アクセスセルラーネットワーク
510
EAP要求
515
EAP手順
520
第1のセキュリティ鍵を導出する
525
第1のセキュリティ鍵を導出する
530
第1のセキュリティ鍵
535
認証手順を実行する
540
他のセキュリティ鍵を導出する
545
他のセキュリティ鍵を導出する
555
導出されたセキュリティ鍵を使用して通信する

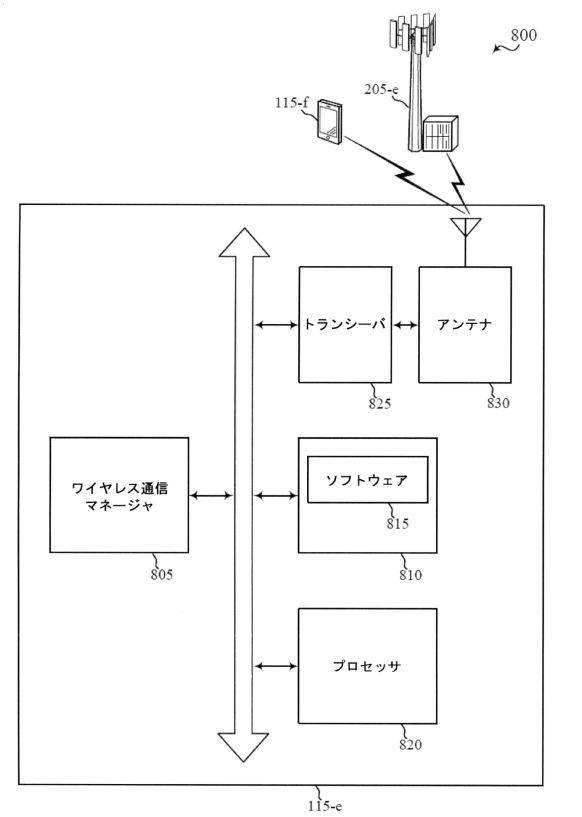
【図６】


600
115-d
620
ワイヤレス通信マネージャ
635
EAPマネージャ
610
受信機
630
送信機
640
ネットワークタイプ識別器
645
ネットワーク
オーセンティケータ

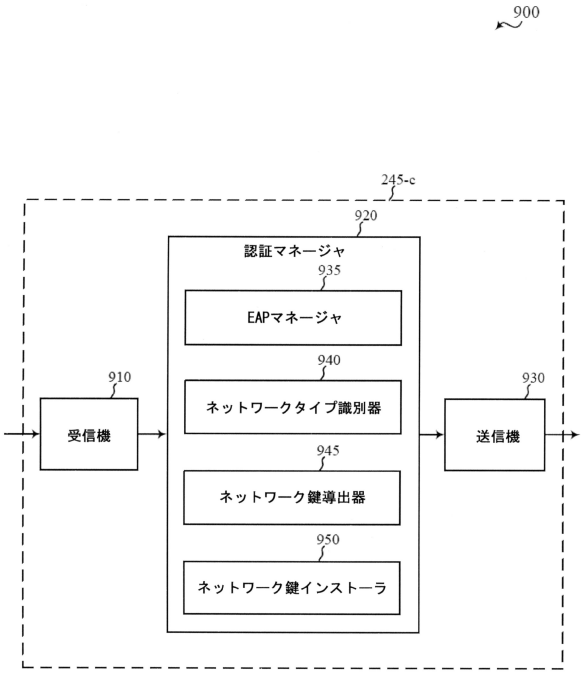
【図７】


700
720
ワイヤレス通信マネージャ
635-a
EAPマネージャ
640-a
ネットワークタイプ識別器
645-a
ネットワーク
オーセンティケータ
705
ネットワーク鍵導出器
710
ネットワークノード鍵
導出器
715
セルラーネットワーク
通信マネージャ

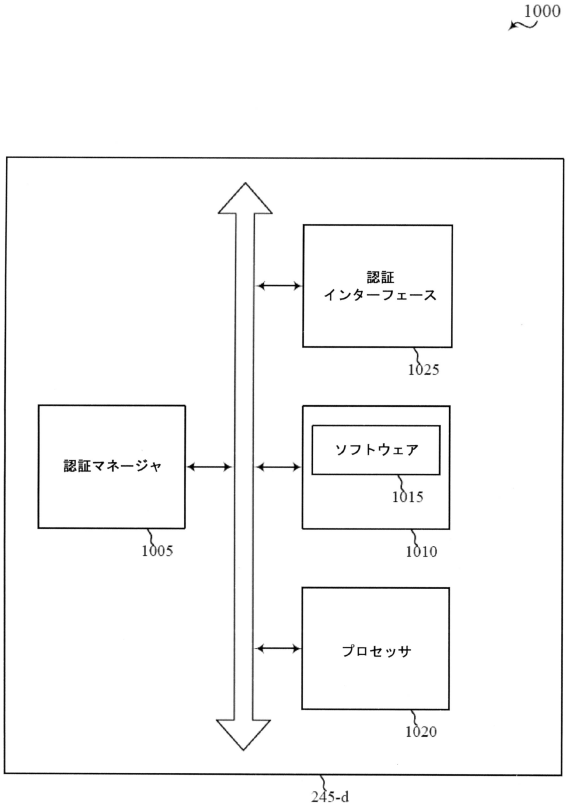
【図８】


800
115-f
205-e
トランシーバ
アンテナ
825
830
ワイヤレス通信
マネージャ
ソフトウェア
815
805
810
プロセッサ
820
115-e

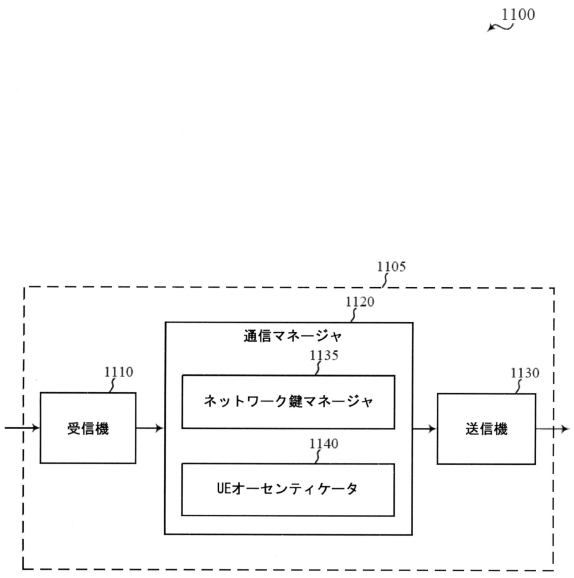
【図９】



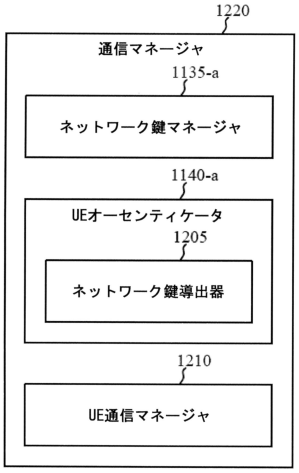
【図１０】



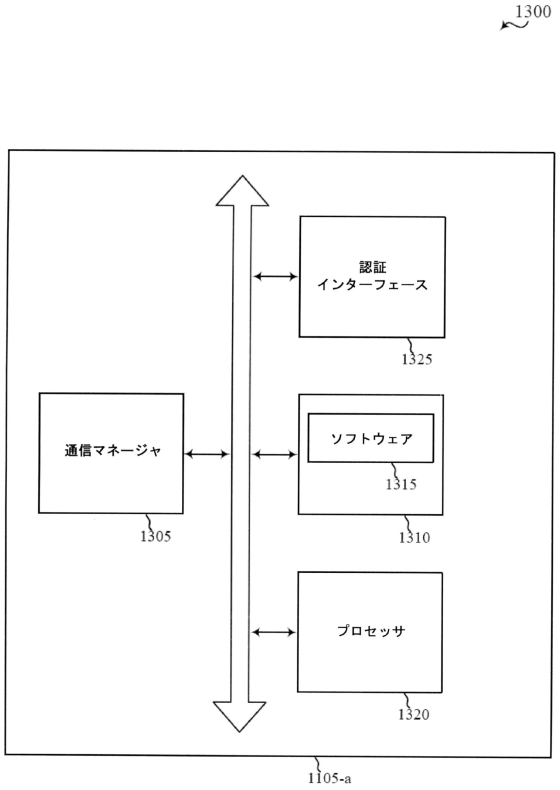
【図１１】



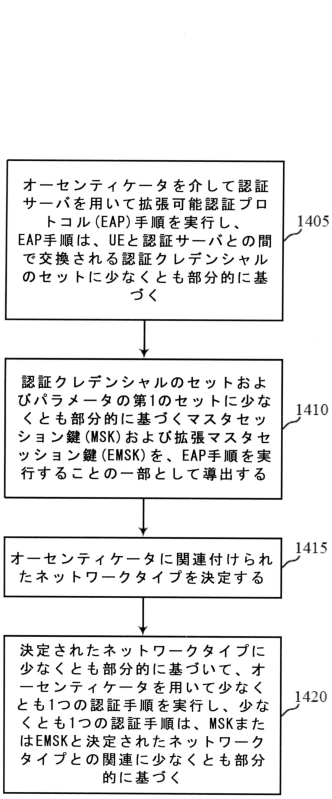
【図１２】



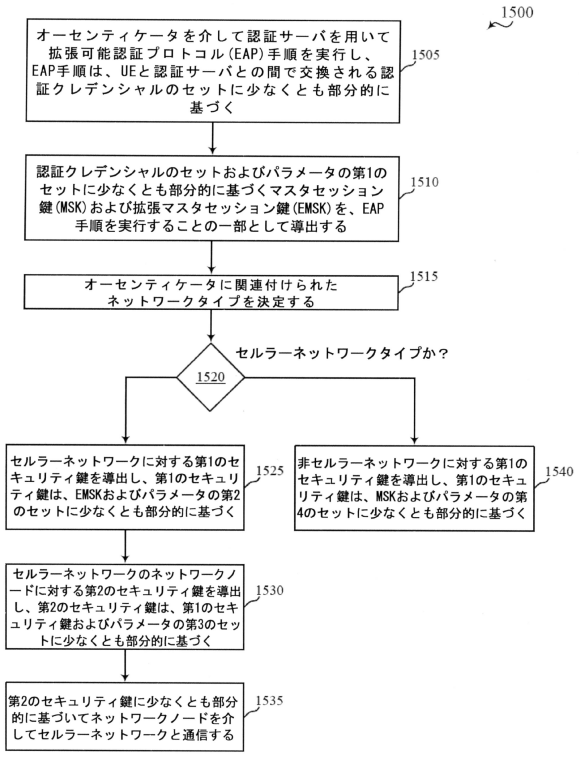
【図１３】



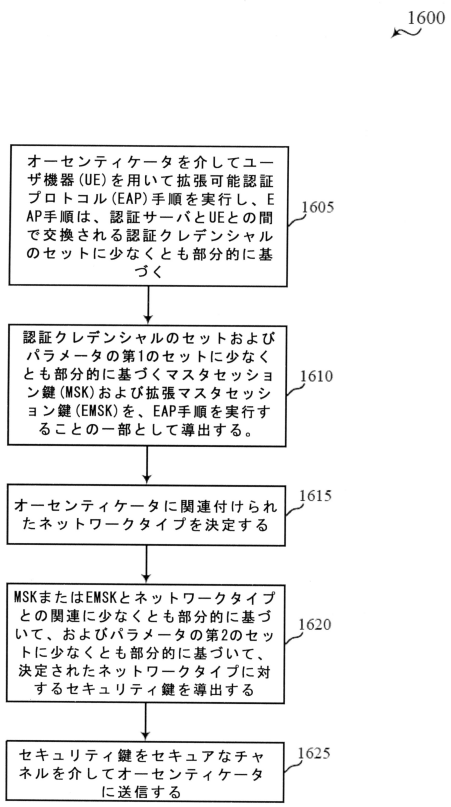
【図１４】



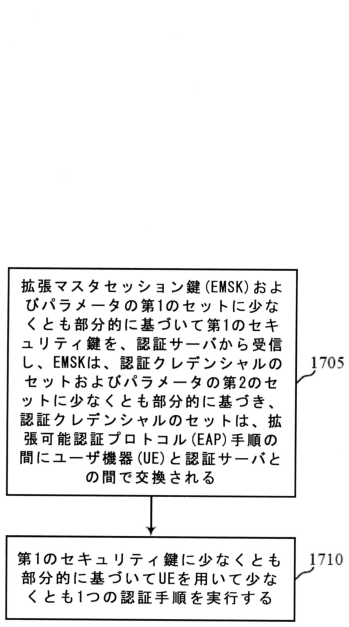
【図１５】



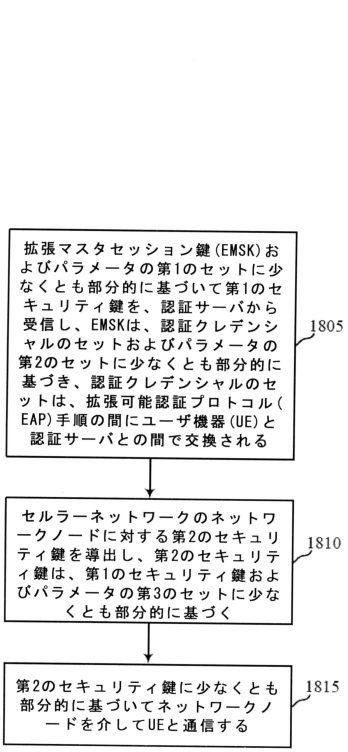
【図１６】



【図１７】


1700
拡張マスタセッション鍵(EMSK)およびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信し、EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき、認証クレデンシャルのセットは、拡張可能認証プロトコル(EAP)手順の間にユーザ機器(UE)と認証サーバとの間で交換される
1705
第1のセキュリティ鍵に少なくとも部分的に基づいてUEを用いて少なくとも1つの認証手順を実行する
1710

【図１８】


1800
拡張マスタセッション鍵(EMSK)およびパラメータの第1のセットに少なくとも部分的に基づいて第1のセキュリティ鍵を、認証サーバから受信し、EMSKは、認証クレデンシャルのセットおよびパラメータの第2のセットに少なくとも部分的に基づき、認証クレデンシャルのセットは、拡張可能認証プロトコル(EAP)手順の間にユーザ機器(UE)と認証サーバとの間で交換される
1805
セルラーネットワークのネットワークノードに対する第2のセキュリティ鍵を導出し、第2のセキュリティ鍵は、第1のセキュリティ鍵およびパラメータの第3のセットに少なくとも部分的に基づく
1810
第2のセキュリティ鍵に少なくとも部分的に基づいてネットワークノードを介してUEと通信する
1815

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　エイドリアン・エドワード・エスコット
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　田畑 利幸
(56)参考文献　国際公開第２０１６／０７３６０７（WO，Ａ１）
国際公開第２００９／０８７００６（WO，Ａ１）
特開２００５－０９４７５８（ＪＰ，Ａ）
特表２０１１－５０９００２（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　４／００－９９／００
Ｇ０９Ｃ　１／００－ ５／００
Ｈ０４Ｋ　１／００－ ３／００
Ｈ０４Ｌ　９／００－ ９／４０
Ｇ０６Ｆ　２１／００
Ｇ０６Ｆ　２１／３０－２１／４６
３ＧＰＰ ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４