(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6517696号
(P6517696)
(45)発行日　令和1年5月22日(2019.5.22)　(24)登録日　平成31年4月26日(2019.4.26)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673A
H04M 11/00 (2006.01)　　H04L 9/00 675B
　　H04M 11/00 302

請求項の数 15　(全 22 頁)

(21)出願番号　特願2015-545866(P2015-545866)
(86)(22)出願日　平成25年12月6日(2013.12.6)
(65)公表番号　特表2016-504844(P2016-504844A)
(43)公表日　平成28年2月12日(2016.2.12)
(86)国際出願番号　PCT/US2013/073522
(87)国際公開番号　WO2014/089403
(87)国際公開日　平成26年6月12日(2014.6.12)
審査請求日　平成28年11月18日(2016.11.18)
(31)優先権主張番号　13/706,849
(32)優先日　平成24年12月6日(2012.12.6)
(33)優先権主張国　米国(US)

(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　ミカエラ・ヴァンダーヴィーン
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

最終頁に続く

(54)【発明の名称】なりすましリスクに対してプライベート表現保護を提供するための方法および装置

(57)【特許請求の範囲】
【請求項１】
ユーザ機器(UE)によって実施される通信の方法であって、
前記UEにおいて、事前に認可された特定のUEのみにアクセスが限定されるプライベート表現を送信する旨の内部要求を受信するステップであって、前記内部要求が前記プライベート表現に関連付けられた表現コードへの参照を含む、ステップと、
表現検証マネージャ(EVM)によって、前記表現コードへの前記参照が以前に取得および記憶された表現コードに対応するかどうかを判断するステップと、
前記表現コードが前記記憶された表現コードに対応すると判断されると、前記プライベート表現を1つまたは複数の監視側UEへ送信するステップか、または
前記表現コードが前記記憶された表現コードに対応しないと判断されると、前記プライベート表現の前記1つまたは複数の監視側UEへの送信を禁止するステップと
を含む、方法。
【請求項２】
前記内部要求が前記UE上で実行されるアプリケーションから受信され、
前記アプリケーションの構成プロセスの一部として取得された前記表現コードは、前記表現コードのセキュアメモリストアに記憶される、
請求項1に記載の方法。
【請求項３】
前記セキュアメモリストアが、前記UEに関連付けられた不揮発性メモリ(NVM)である、

請求項2に記載の方法。
【請求項４】
前記表現コードに関連付けられたデバイス間(D2D)情報を送信するステップをさらに含む、請求項2に記載の方法。
【請求項５】
信頼できるサーバから前記表現コードを取得するステップと、
前記表現コードをセキュアメモリストアに記憶するステップと
をさらに含む、請求項1に記載の方法。
【請求項６】
前記EVMが前記UEのモデムに関連付けられる、請求項1に記載の方法。
【請求項７】
前記EVMが前記UEのアプリケーションインターフェースとモデムインターフェースとの間の中間レイヤとして構成される、請求項1に記載の方法。
【請求項８】
請求項1～7のいずれか一項に記載の方法を実施するための命令を含む、コンピュータプログラム。
【請求項９】
ワイヤレス通信のための装置であって、
1つまたは複数の監視側UEへ、事前に認可された特定のUEのみにアクセスが限定されるプライベート表現を送信する旨の内部要求を受信するための手段であって、前記内部要求が前記プライベート表現に関連付けられた表現コードへの参照を含む、手段と、
表現検証マネージャ(EVM)によって、前記表現コードへの前記参照が以前に取得および記憶された表現コードに対応するかどうかを判断するための手段と、
前記表現コードが前記記憶された表現コードに対応すると判断されると、前記プライベート表現を1つまたは複数の監視側UEへ送信するための手段か、または
前記表現コードが前記表現コードの前記記憶された表現コードに対応しないと判断されると、前記プライベート表現の前記1つまたは複数の監視側UEへの送信を禁止するための手段と
を備える、装置。
【請求項１０】
前記内部要求が前記装置上で実行されるアプリケーションから受信され、
前記アプリケーションの構成プロセスの一部として取得された前記表現コードは、前記表現コードのセキュアメモリストアに記憶される、
請求項9に記載の装置。
【請求項１１】
前記セキュアメモリストアが、前記装置に関連付けられた不揮発性メモリ(NVM)である、請求項10に記載の装置。
【請求項１２】
前記送信するための手段が、
前記表現コードに関連付けられたデバイス間(D2D)情報を送信するように構成される、
請求項10に記載の装置。
【請求項１３】
信頼できるサーバから前記表現コードを取得するための手段と、
前記表現コードをセキュアメモリストアに記憶するための手段と
をさらに備える、請求項9に記載の装置。
【請求項１４】
前記EVMが前記装置のモデムに関連付けられる、請求項9に記載の装置。
【請求項１５】
前記EVMが前記装置のアプリケーションインターフェースとモデムインターフェースとの間の中間レイヤとして構成される、請求項9に記載の装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は一般に通信システムに関し、より詳細には、ワイヤレス通信ベースのネットワークにおいてデバイス間(D2D)通信とともにプライベート表現を使用することに関する。
【背景技術】
【０００２】
ワイヤレス通信システムは、電話、ビデオ、データ、メッセージング、およびブロードキャストなど、様々な電気通信サービスを提供するために広く展開されている。通常のワイヤレス通信システムは、利用可能なシステムリソース(たとえば、帯域幅、送信電力)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技術を利用することができる。そのような多元接続技術の例には、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、直交周波数分割多元接続(OFDMA)システム、シングルキャリア周波数分割多元接続(SC-FDMA)システム、および時分割同期符号分割多元接続(TD-SCDMA)システムがある。
【０００３】
これらの多元接続技術は、異なるワイヤレスデバイスが自治体、国家、地域、さらには地球規模のレベルで通信するのを可能にする共通プロトコルを提供するために、様々な電気通信規格において採用されている。電気通信規格の一例は、ロングタームエボリューション(LTE)である。LTEは、第3世代パートナーシッププロジェクト(3GPP)によって公表されたUniversal Mobile Telecommunications System(UMTS)モバイル規格に対する拡張セットである。LTEは、スペクトル効率を改善することによってモバイルブロードバンドインターネットアクセスをよりよくサポートすること、コストを下げること、サービスを改善すること、新しいスペクトルを利用すること、および、ダウンリンク(DL)上のOFDMAとアップリンク(UL)上のSC-FDMAと多入力多出力(MIMO)アンテナ技術とを使用して他のオープン規格とよりよく統合することを行うように設計されている。LTEは、直接デバイス間(ピアツーピア)通信をサポートすることができる。
【０００４】
現在、多くのデバイス(たとえば、ユーザ機器(UE))が、セルラーネットワーク内で動作可能であり得る。D2D LTEプロトコルは、直接通信範囲内にあるUE間の通信を提供し得る。UEは表現を使用して、近接度認識アプリケーションによって駆動される様々な属性(ユーザ識別情報またはサービス識別情報、アプリケーション機能、位置など)を告知することができる。表現は、表現が告知側UEの範囲内の任意のUEにとってアクセス可能である場合にはパブリックとすることができ、または、事前に認可された特定のUEのみにアクセスが限定される場合にはプライベートとすることができる。プライベート表現を使用するとき、告知側UEは、近接しているときに、告知された表現にアクセスする/告知された表現を復号する許可が付与された1つまたは複数の監視側UEに、対応する表現コードを(たとえば、オフラインプロセスを介して)提供しておいてもよい。
【０００５】
しかしながら、ユーザセキュリティ違反は、プライベート表現なりすましリスクから生じ得る。たとえば、第1のユーザが第2のユーザに関連付けられた表現コードを知っている場合、第1のユーザは、第1のユーザのデバイスが第2のユーザの表現コードを用いてプライベート表現を告知する旨の要求を生成するアプリケーションを使用することによって、第2のユーザになりすますことができる。したがって、他者はだまされて第2のユーザが存在していると錯覚する可能性がある。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
D2D通信に対する需要が高まるにつれて、ワイヤレス通信ベースのネットワークにおいてプライベート表現識別子を保護するための方法/装置が必要とされている。

【課題を解決するための手段】
【０００７】
以下では、1つまたは複数の態様を基本的に理解してもらうために、そのような態様の簡略化された概要を提示する。この概要は、すべての企図された態様の包括的な概観ではなく、すべての態様の主要または重要な要素を識別するものでも、いずれかまたはすべての態様の範囲を定めるものでもない。その唯一の目的は、後で提示するより詳細な説明の導入として、1つまたは複数の態様のいくつかの概念を簡略化された形で提示することである。
【０００８】
1つまたは複数の態様およびその対応する開示によれば、様々な態様は、LTEベースのWWANにおいてプライベート表現保護を提供することに関して説明されている。一例では、UEは、プライベート表現および/または少なくともプライベート表現に関連付けられた表現コードへの参照を告知する旨の(たとえば、UE上で実行されるアプリケーションからの)要求を内部で受信し、表現コードへの参照および/または表現コードが表現コードの記憶されたインスタンスと一致するかどうかを判断するように装備される。一態様では、UEは、表現コードの記憶されたインスタンスが、要求とともに受信された表現コードに対応するときに、プライベート表現または表現コードのうちの少なくとも1つを告知するように装備され得る。別の態様では、UEは、記憶された表現コードが、要求とともに受信された表現コードに対応しないときに、プライベート表現に関連付けられたいかなる情報の告知も禁止するように装備され得る。
【０００９】
関係する態様によれば、ワイヤレス通信ネットワークにおいてプライベート表現保護を提供するための方法が提供される。方法は、少なくともプライベート表現を告知する旨の要求への参照を受信するステップを含むことができる。一態様では、要求は、プライベート表現に関連付けられた表現コードを含み得る。さらに、方法は、表現検証マネージャ(EVM: expression verification manager)によって、少なくとも表現コードへの参照が表現コードの以前に取得および記憶されたインスタンスに対応するかどうかを判断するステップを含むことができる。一態様では、方法は、表現コードが表現コードの記憶されたインスタンスに対応すると判断されると、プライベート表現または表現コードのうちの少なくとも1つを告知するステップを含み得る。追加または代替として、一態様では、方法は、表現コードが表現コードの記憶されたインスタンスに対応しないと判断されると、プライベート表現に関連付けられた情報の告知を禁止するステップを含み得る。
【００１０】
別の態様は、LTEベースのワイヤレス通信ネットワークにおいてプライベート表現保護を提供するように構成された通信装置に関する。通信装置は、少なくともプライベート表現への参照を告知する旨の要求を受信するための手段を含むことができる。一態様では、要求は、プライベート表現に関連付けられた表現コードを含み得る。さらに、通信装置は、表現検証マネージャ(EVM)によって、少なくとも表現コードへの参照が表現コードの以前に取得および記憶されたインスタンスに対応するかどうかを判断するための手段を含むことができる。一態様では、通信装置は、表現コードが表現コードの記憶されたインスタンスに対応すると判断されると、プライベート表現または表現コードのうちの少なくとも1つを告知するための手段を含むことができる。追加または代替として、一態様では、通信装置は、表現コードが表現コードの記憶されたインスタンスに対応しないと判断されると、プライベート表現に関連付けられた情報の告知を禁止するための手段を含むことができる。
【００１１】
別の態様は、通信装置に関する。装置は、プライベート表現を告知する旨の要求を受信するように構成された処理システムを含むことができる。一態様では、要求は、少なくともプライベート表現に関連付けられた表現コードへの参照を含み得る。さらに、処理システムは、表現検証マネージャ(EVM)によって、少なくとも表現コードへの参照が表現コー

ドの以前に取得および記憶されたインスタンスに対応するかどうかを判断するように構成され得る。一態様では、処理システムは、表現コードが表現コードの記憶されたインスタンスに対応すると判断されると、プライベート表現または表現コードのうちの少なくとも1つを告知するようにさらに構成され得る。追加または代替として、一態様では、処理システムは、表現コードが表現コードの記憶されたインスタンスに対応しないと判断されると、プライベート表現に関連付けられた情報の告知を禁止するようにさらに構成され得る。

【００１２】

さらに別の態様は、プライベート表現を告知する旨の要求を受信するためのコードを含むコンピュータ可読媒体を有することができるコンピュータプログラム製品に関する。一態様では、要求は、少なくともプライベート表現に関連付けられた表現コードへの参照を含み得る。さらに、コンピュータ可読媒体は、表現検証マネージャ(EVM)によって、少なくとも表現コードへの参照が表現コードの以前に取得および記憶されたインスタンスに対応するかどうかを判断するためのコードを含むことができる。一態様では、コンピュータ可読媒体は、表現コードが表現コードの記憶されたインスタンスに対応すると判断されると、プライベート表現または表現コードのうちの少なくとも1つを告知するためのコードを含むことができる。追加または代替として、一態様では、コンピュータ可読媒体は、表現コードが表現コードの記憶されたインスタンスに対応しないと判断されると、プライベート表現に関連付けられた情報の告知を禁止するためのコードを含むことができる。

【００１３】

上記の目的および関連する目的を達成するために、1つまたは複数の態様は、以下で十分に記載され、特許請求の範囲で具体的に指摘される特徴を含む。以下の説明および添付の図面は、1つまたは複数の態様のある特定の例示的な特徴を詳細に説明する。しかしながら、これらの特徴は、種々の態様の原理が利用される場合がある種々の方法のうちのいくつかを示すものにすぎず、この説明は、そのようなすべての態様、およびそれらの均等物を含むことを意図している。

【図面の簡単な説明】

【００１４】

【図１】ネットワークアーキテクチャの一例を示す図である。

【図２】アクセスネットワークの一例を示す図である。

【図３】LTEにおけるDLフレーム構造の一例を示す図である。

【図４】LTEにおけるULフレーム構造の一例を示す図である。

【図５】ユーザプレーンおよび制御プレーンの無線プロトコルアーキテクチャの一例を示す図である。

【図６】アクセスネットワーク中の発展型ノードBおよびユーザ機器の一例を示す図である。

【図７】デバイス間通信ネットワークを示す図である。

【図８】ワイヤレス通信の方法のフローチャートである。

【図９】例示的な装置における異なるモジュール/手段/構成要素間のデータフローを示す概念データフロー図である。

【図１０】処理システムを使用する装置のためのハードウェア実装の一例を示す図である。

【発明を実施するための形態】

【００１５】

添付の図面とともに以下で説明される詳細な説明は、様々な構成を説明するものであり、本明細書に記載された概念が実施され得る唯一の構成を表すものではない。詳細な説明は、様々な概念の完全な理解をもたらす目的で、具体的な詳細を含んでいる。しかし、これらの概念がこれらの具体的な詳細なしに実践され得ることが、当業者には明らかであろう。場合によっては、そのような概念を曖昧にするのを回避する目的で、周知の構造および構成要素がブロック図の形式で示される。

【００１６】
次に、電気通信システムのいくつかの態様を、様々な装置および方法を参照して提示する。これらの装置および方法は、以下の詳細な説明で説明され、様々なブロック、モジュール、構成要素、回路、ステップ、プロセス、アルゴリズムなど(「要素」と総称される)によって添付の図面に示される。これらの要素は、電子ハードウェア、コンピュータソフトウェア、またはそれらの任意の組合せを使用して実装され得る。そのような要素をハードウェアとして実装するか、ソフトウェアとして実装するかは、特定の適用例および全体的なシステムに課された設計制約に依存する。
【００１７】
例として、要素または要素の任意の部分または要素の任意の組合せを、1つまたは複数のプロセッサを含む「処理システム」で実装することができる。プロセッサの例として、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ(DSP)、フィールドプログラマブルゲートアレイ(FPGA)、プログラマブル論理デバイス(PLD)、状態機械、ゲート論理回路、個別ハードウェア回路、および本開示全体にわたって説明する様々な機能を実施するように構成された他の適切なハードウェアがある。処理システム内の1つまたは複数のプロセッサは、ソフトウェアを実行することができる。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語と呼ばれるか、または他の名称で呼ばれるかを問わず、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行可能ファイル、実行スレッド、手順、機能などを意味するよう広く解釈されるべきである。
【００１８】
したがって、1つまたは複数の例示的な実施形態では、説明される機能は、ハードウェア、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で実装され得る。ソフトウェアで実装される場合、機能は、1つまた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るか、または符号化され得る。コンピュータ可読媒体は、コンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、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、命令またはデータ構造の形態の所望のプログラムコードを搬送または記憶するために使用でき、かつコンピュータによってアクセスできる、任意の他の媒体を含み得る。本明細書で使用する場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(CD)、レーザーディスク（登録商標）、光ディスク、デジタル多用途ディスク(DVD)、フロッピー（登録商標）ディスク、およびブルーレイディスクを含み、ディスク(disk)は、通常、磁気的にデータを再生し、ディスク(disc)は、レーザーで光学的にデータを再生する。上記の組合せもコンピュータ可読媒体の範囲の中に含まれるべきである。
【００１９】
図1は、LTEネットワークアーキテクチャ100を示す図である。LTEネットワークアーキテクチャ100は、発展型パケットシステム(EPS)100と呼ばれることがある。EPS100は、1つまたは複数のユーザ機器(UE)102、発展型UMTS地上無線アクセスネットワーク(E-UTRAN)104、発展型パケットコア(EPC)110、ホーム加入者サーバ(HSS)120、およびオペレータのIPサービス122を含み得る。EPSは、他のアクセスネットワークと相互接続することができるが、簡単のために、それらのエンティティ/インターフェースは図示していない。図示のように、EPSはパケット交換サービスを提供するが、当業者なら容易に諒解するように、本開示の全体を通して提示する様々な概念は、回線交換サービスを提供するネットワークに拡張することができる。
【００２０】
E-UTRANは、発展型ノードB(eNB)106および他のeNB108を含む。eNB106は、UE102にユー

ザプレーンプロトコルおよび制御プレーンプロトコルの終端を提供する。eNB106は、バックホール(たとえばX2インターフェース)を介して他のeNB108に接続されてよい。eNB106は、基地局、トランシーバ基地局、無線基地局、無線トランシーバ、トランシーバ機能、基本サービスセット(BSS)、拡張サービスセット(ESS)と呼ばれるか、または他の何らかの適切な用語で呼ばれることもある。eNB106は、EPC110へのアクセスポイントをUE102に提供する。UE102の例としては、セルラーフォン、スマートフォン、セッション開始プロトコル(SIP)フォン、ラップトップ、携帯情報端末(PDA)、衛星無線、全地球測位システム、マルチメディアデバイス、ビデオデバイス、デジタルオーディオプレーヤ(たとえば、MP3プレーヤ)、カメラ、ゲームコンソール、または同様に機能する任意の他のデバイスが挙げられる。UE102は、当業者によって、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、クライアントと呼ばれるか、または他の何らかの適切な用語で呼ばれることもある。

【００２１】

eNB106は、S1インターフェースによってEPC110に接続される。EPC110は、モビリティ管理エンティティ(MME)112、他のMME114、サービングゲートウェイ116、およびパケットデータネットワーク(PDN)ゲートウェイ118を含む。MME112は、UE102とEPC110との間のシグナリングを処理する制御ノードである。概して、MME112は、ベアラおよび接続管理を行う。すべてのユーザIPパケットは、サービングゲートウェイ116を通して転送され、サービングゲートウェイ116自体は、PDNゲートウェイ118に接続される。PDNゲートウェイ118は、UE IPアドレス割振りならびに他の機能を提供する。PDNゲートウェイ118は、オペレータのIPサービス122に接続される。オペレータのIPサービス122は、インターネット、イントラネット、IPマルチメディアサブシステム(IMS)、およびPSストリーミングサービス(PSS)を含み得る。

【００２２】

図2は、LTEネットワークアーキテクチャにおけるアクセスネットワーク200の例を示す図である。この例では、アクセスネットワーク200は、いくつかのセルラー領域(セル)202に分割される。1つまたは複数の低電力クラスeNB208は、セル202のうちの1つまたは複数と重なるセルラー領域210を有することができる。低電力クラスeNB208は、フェムトセル(たとえば、ホームeNB(HeNB))、ピコセル、マイクロセル、またはリモートラジオヘッド(RRH)とすることができる。マクロeNB204は各々、それぞれのセル202に割り当てられ、セル202中のすべてのUE206、212にEPC110へのアクセスポイントを提供するように構成される。UE212のうちいくつかは、デバイス間通信中であってよい。アクセスネットワーク200のこの例では集中型コントローラはないが、代替構成では集中型コントローラが使用されてもよい。eNB204は、無線ベアラ制御、アドミッション制御、モビリティ制御、スケジューリング、セキュリティ、およびサービングゲートウェイ116への接続性を含めた、すべての無線関連機能を担う。

【００２３】

アクセスネットワーク200によって用いられる変調方式および多元接続方式は、導入されている特定の電気通信規格に応じて異なり得る。LTE適用例では、DL上ではOFDMが使用され、かつUL上ではSC-FDMAが使用されて、周波数分割複信(FDD)と時分割複信(TDD)の両方がサポートされる。当業者なら以下の詳細な説明から容易に諒解するように、本明細書で提示する様々な概念は、LTE適用例に好適である。しかし、これらの概念は、他の変調技法および多元接続技法を利用する他の電気通信規格に容易に拡張することができる。例として、これらの概念は、エボリューションデータオプティマイズド(EV-DO)またはウルトラモバイルブロードバンド(UMB)に拡張することができる。EV-DOおよびUMBは、CDMA2000規格ファミリの一部として第3世代パートナーシッププロジェクト2(3GPP2)によって公表されたエアインターフェース規格であり、CDMAを利用してブロードバンドインターネット

アクセスを移動局に提供する。これらの概念はまた、広帯域CDMA(W-CDMA)およびTD-SCDMAなどのCDMAの他の変形形態を採用するUniversal Terrestrial Radio Access(UTRA)、TDMAを採用するGlobal System for Mobile Communications(GSM（登録商標）)、ならびにOFDMAを採用するEvolved UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、およびFlash-OFDMに拡張され得る。UTRA、E-UTRA、UMTS、LTE、およびGSM（登録商標）は、3GPP団体による文書に記述されている。CDMA2000およびUMBは、3GPP2団体による文書に記述されている。実際の利用されるワイヤレス通信規格、および多元接続技術は、具体的な用途およびシステムに課される全体的な設計制約に依存する。

【００２４】

図3は、LTEにおけるDLフレーム構造の一例を示す図300である。フレーム(10ms)は、等しいサイズの10個のサブフレームに分割され得る。各サブフレームは、連続する2個のタイムスロットを含むことができる。リソースグリッドを使用して2つのタイムスロットを表すことができ、各タイムスロットはリソースブロックを含む。リソースグリッドは、複数のリソース要素に分割される。LTEでは、リソースブロックは、周波数領域における連続する12個のサブキャリアを含み、また、各OFDMシンボル中の通常のサイクリックプレフィックスの場合、時間領域における連続する7個のOFDMシンボルを含み、すなわち84個のリソース要素を含む。拡張サイクリックプレフィックスの場合、リソースブロックは、時間領域における連続する6つのOFDMシンボルを含み、72個のリソース要素を有する。物理DL制御チャネル(PDCCH)、物理DL共有チャネル(PDSCH)、および他のチャネルは、リソース要素にマップされ得る。

【００２５】

図4は、LTEにおけるULフレーム構造の一例を示す図400である。ULのための利用可能なリソースブロックは、データセクションと制御セクションとに区分され得る。制御セクションは、システム帯域幅の2つの端部に形成されてよく、構成可能なサイズを有し得る。制御セクションのリソースブロックは、制御情報の送信のためにUEに割り当てられ得る。データセクションは、制御セクションに含まれないすべてのリソースブロックを含み得る。このULフレーム構造により、データセクションは連続的なサブキャリアを含むことになり、これにより、単一のUEに、データセクション中の連続的なサブキャリアのすべてを割り当てることができる。

【００２６】

制御情報をeNBに送信するために、制御セクション中のリソースブロック410a、410bをUEに割り当てることができる。また、データをeNBに送信するために、データセクション中のリソースブロック420a、420bをUEに割り当てることができる。UEは、制御セクション中の割り当てられたリソースブロック上の物理UL制御チャネル(PUCCH)中で、制御情報を送信することができる。UEは、データセクション中の割り当てられたリソースブロック上の物理UL共有チャネル(PUSCH)中で、データのみ、またはデータと制御情報の両方を送信することができる。UL送信は、サブフレームの両方のスロットにまたがることができ、周波数にわたってホップすることができる。

【００２７】

1組のリソースブロックを使用して、初期システムアクセスを実施し、物理ランダムアクセスチャネル(PRACH)430中でUL同期を達成することができる。PRACH430は、ランダムシーケンスを搬送し、いかなるULデータ/シグナリングも搬送できない。各ランダムアクセスプリアンブルは、6個の連続するリソースブロックに対応する帯域幅を占有する。開始周波数は、ネットワークによって指定される。すなわち、ランダムアクセスプリアンブルの送信は、ある時間リソースおよび周波数リソースに制限される。周波数ホッピングは、PRACHにはない。PRACH試行は、単一のサブフレーム(1ms)中で、または少数の連続的なサブフレームのシーケンス中で搬送され、UEは、フレーム(10ms)ごとに単一のPRACH試行しか行うことができない。

【００２８】

図5は、LTEにおけるユーザプレーンおよび制御プレーンのための無線プロトコルアーキ

テクチャの一例を示す図500である。UE502およびeNBの無線プロトコルアーキテクチャは、レイヤ1、レイヤ2、およびレイヤ3という3つのレイヤで示される。データ/シグナリングの通信522は、3つのレイヤにわたってUE502とeNB504との間で発生する場合がある。レイヤ1(L1レイヤ)は、最下位レイヤであり、様々な物理レイヤ信号処理機能を実施する。本明細書では、L1レイヤは物理レイヤ506と呼ばれる。レイヤ2(L2レイヤ)508は、物理レイヤ506の上にあり、物理レイヤ506を介したUEとeNBとの間のリンクを担う。

【００２９】

ユーザプレーンでは、L2レイヤ508は、媒体アクセス制御(MAC)サブレイヤ510、無線リンク制御(RLC)サブレイヤ512、およびパケットデータコンバージェンスプロトコル(PDCP)サブレイヤ514を含み、これらは、ネットワーク側のeNBにおいて終端する。図示されていないが、UEは、L2レイヤ508の上にいくつかの上位レイヤを有することができ、これらは、ネットワーク側のPDNゲートウェイ118において終端するネットワークレイヤ(たとえば、IPレイヤ)と、接続の他端(たとえば、遠端UE、サーバなど)において終端するアプリケーションレイヤとを含む。

【００３０】

PDCPサブレイヤ514は、異なる無線ベアラと論理チャネルとの多重化を行う。PDCPサブレイヤ514は、無線送信のオーバーヘッドを低減するための上位レイヤのデータパケットのヘッダ圧縮、データパケットを暗号化することによるセキュリティ、およびeNB間のUEのハンドオーバのサポートも提供する。RLCサブレイヤ512は、上位レイヤのデータパケットのセグメント化および再アセンブリ、紛失したデータパケットの再送信、ならびに、ハイブリッド自動再送要求(HARQ)による順序の狂った受信を補償するためのデータパケットの並べ替えを行う。MACサブレイヤ510は、論理チャネルとトランスポートチャネルとの間の多重化を行う。MACサブレイヤ510はまた、1つのセルの中の様々な無線リソース(たとえば、リソースブロック)の複数のUEへの割振りを担う。MACサブレイヤ510はまた、HARQ動作も担う。

【００３１】

制御プレーンでは、UEおよびeNBの無線プロトコルアーキテクチャは、制御プレーンのヘッダ圧縮機能がないことを除いて、物理レイヤ506およびL2レイヤ508に関して実質的に同じである。制御プレーンはまた、レイヤ3(L3レイヤ)中に無線リソース制御(RRC)サブレイヤ516を含む。RRCサブレイヤ516は、無線リソース(すなわち、無線ベアラ)を取得すること、およびeNBとUE502との間のRRCシグナリングを使用して下位レイヤを構成することを担う。ユーザプレーンはまた、インターネットプロトコル(IP)サブレイヤ518およびアプリケーションサブレイヤ520を含む。IPサブレイヤ518およびアプリケーションサブレイヤ520は、eNB504とUE502との間のアプリケーションデータの通信をサポートすることに関与する。

【００３２】

図6は、アクセスネットワーク内のUE650と通信しているWANエンティティ(たとえば、eNB、MME、など)610のブロック図である。DLでは、コアネットワークからの上位層パケットが、コントローラ/プロセッサ675に与えられる。コントローラ/プロセッサ675は、L2レイヤの機能性を実装する。DLでは、コントローラ/プロセッサ675は、ヘッダ圧縮、暗号化、パケットのセグメント化および並べ替え、論理チャネルとトランスポートチャネルとの間の多重化、ならびに、様々な優先度メトリックに基づくUE650への無線リソース割振りを行う。コントローラ/プロセッサ675はまた、HARQ動作、紛失したパケットの再送、およびUE650へのシグナリングを担う。

【００３３】

送信(TX)プロセッサ616は、L1レイヤ(すなわち、物理レイヤ)のための様々な信号処理機能を実装する。これらの信号処理機能は、UE650における順方向誤り訂正(FEC)を容易にするための符号化およびインタリービングと、様々な変調方式(たとえば、2値位相シフトキーイング(BPSK)、直交位相シフトキーイング(QPSK)、M位相シフトキーイング(M-PSK)、M直交振幅変調(M-QAM))に基づく信号コンスタレーションへのマッピングとを含む。次い

で、符号化され変調されたシンボルは、並列ストリームに分割される。次いで、各ストリームは、OFDMサブキャリアにマッピングされ、時間および/または周波数領域で基準信号(たとえば、パイロット)と多重化され、次いで逆高速フーリエ変換(IFFT)を使用して一緒に結合されて、時間領域OFDMシンボルストリームを搬送する物理チャネルが生成される。OFDMストリームは、複数の空間ストリームを生成するために空間的にプリコーディングされる。チャネル推定器674からのチャネル推定値を、符号化変調方式の決定ならびに空間処理に使用することができる。チャネル推定値は、UE650によって送信される基準信号および/またはチャネル状態フィードバックから導出され得る。次いで、各空間ストリームは、別個の送信機618TXを介して異なるアンテナ620に提供される。各送信機618TXは、送信のためにそれぞれの空間ストリームでRFキャリアを変調する。

【００３４】

UE650において、各受信機654RXは、それぞれのアンテナ652を介して信号を受信する。各受信機654RXは、RFキャリア上に変調された情報を回復し、情報を受信(RX)プロセッサ656に与える。RXプロセッサ656は、L1レイヤの様々な信号処理機能を実装する。RXプロセッサ656は、情報に対して空間処理を実施して、UE650に向けられた空間ストリームがあればそれを回復する。複数の空間ストリームがUE650に向けられている場合、これらをRXプロセッサ656によって単一のOFDMシンボルストリームに結合することができる。次いで、RXプロセッサ656は、高速フーリエ変換(FFT)を使用して、OFDMシンボルストリームを時間領域から周波数領域に変換する。周波数領域信号は、OFDM信号の各サブキャリアについて別個のOFDMシンボルストリームを含む。各サブキャリア上のシンボル、および基準信号は、WANエンティティ610によって送信された最も可能性の高い信号コンスタレーションポイントを決定することによって、回復され復調される。これらの軟判定は、チャネル推定器658によって計算されるチャネル推定値に基づき得る。次いで、軟判定は復号されデインタリーブされて、物理チャネル上でWANエンティティ610によって元々送信されたデータおよび制御信号が回復される。次いで、データおよび制御信号は、コントローラ/プロセッサ659に与えられる。

【００３５】

コントローラ/プロセッサ659は、L2レイヤを実装する。コントローラ/プロセッサは、プログラムコードおよびデータを記憶するメモリ660に関連付けられ得る。メモリ660は、コンピュータ可読媒体と呼ばれることもある。ULにおいて、コントローラ/プロセッサ659は、トランスポートチャネルと論理チャネルとの間の逆多重化、パケットリアセンブリ、復号、ヘッダ圧縮、コアネットワークから上位レイヤパケットを回復するための制御信号処理を提供する。次いで、上位レイヤパケットはデータシンク662に与えられ、データシンク662は、L2レイヤの上のすべてのプロトコルレイヤを表す。様々な制御信号も、L3処理のためにデータシンク662に与えられ得る。コントローラ/プロセッサ659はまた、HARQ動作をサポートするために、肯定応答(ACK)および/または否定応答(NACK)プロトコルを使用した誤り検出を担う。

【００３６】

ULでは、データソース667を使用して、上位レイヤパケットがコントローラ/プロセッサ659に与えられる。データソース667は、L2レイヤの上のすべてのプロトコルレイヤを表す。WANエンティティ610によるDL送信に関して説明した機能性と同様に、コントローラ/プロセッサ659は、ヘッダ圧縮、暗号化、パケットのセグメント化および並べ替え、ならびに、WANエンティティ610による無線リソース割振りに基づく論理チャネルとトランスポートチャネルとの間の多重化を行うことによって、ユーザプレーンおよび制御プレーンのL2レイヤを実装する。コントローラ/プロセッサ659はまた、HARQ動作、紛失したパケットの再送、およびWANエンティティ610へのシグナリングを担う。

【００３７】

WANエンティティ610によって送信された基準信号またはフィードバックからチャネル推定器658によって導出されたチャネル推定値を、TXプロセッサ668によって使用して、適切な符号化変調方式を選択し、空間処理を容易にすることができる。TXプロセッサ668によ

って生成された空間ストリームは、別個の送信機654TXを介して、異なるアンテナ652に提供される。各送信機654TXは、送信のためにそれぞれの空間ストリームでRFキャリアを変調する。

【００３８】

UL送信は、WANエンティティ610において、UE650における受信機機能に関して説明した方法と同様の方法で処理される。各受信機618RXは、そのそれぞれのアンテナ620を通して信号を受信する。各受信機618RXは、RF搬送波上に変調された情報を回復し、この情報をRXプロセッサ670に与える。RXプロセッサ670は、L1レイヤを実装することができる。

【００３９】

コントローラ/プロセッサ675は、L2レイヤを実装する。コントローラ/プロセッサ675は、プログラムコードおよびデータを記憶するメモリ676に関連付けられ得る。メモリ676は、コンピュータ可読媒体と呼ばれることもある。ULでは、コントローラ/プロセッサ675は、トランスポートチャネルと論理チャネルとの間の逆多重化、パケット再アセンブリ、暗号化解除、ヘッダ圧縮解除、制御信号処理を行って、UE650からの上位レイヤパケットを回復する。コントローラ/プロセッサ675からの上位レイヤパケットは、コアネットワークに与えられ得る。コントローラ/プロセッサ675はまた、HARQ動作をサポートするために、ACKおよび/またはNACKプロトコルを使用した誤り検出を担う。

【００４０】

図7は、デバイス間通信システム700の図である。デバイス間通信システム700は、複数のワイヤレスデバイス702、704を含む。任意の態様では、デバイス間通信システム700は、ワイヤレスデバイス702、704のうちの1つまたは複数と通信するように動作可能なアプリケーションサーバ706も含み得る。

【００４１】

デバイス間通信システム700は、たとえば、ワイヤレスワイドエリアネットワーク(WWAN)など、セルラー通信システムと重なり得る。ワイヤレスデバイス702、704の中には、DL/UL WWANスペクトルおよび/または無許可スペクトル(たとえば、WiFi)を用いてデバイス間通信で互いに通信することができるものもあり、基地局と通信することができるものもあり、両方とも行えるものもある。別の態様では、WWANは、1つまたは複数のネットワークエンティティ(たとえば、MMEなど)を介して提供される接続性を通して協調通信環境を提供することができる複数の基地局を含み得る。

【００４２】

ワイヤレスデバイス702は、構成要素の中でも、アプリケーションプロセッサ720、表現検証マネージャ730、およびモデムプロセッサを含み得る。一態様では、アプリケーションプロセッサ720は、1つまたは複数のアプリケーション722を有効にするように構成され得る。そのような態様では、アプリケーション722は、1つまたは複数の他の認可されたピアデバイス(たとえば、ワイヤレスデバイス704)への告知のためのプライベート表現724を含み得る。図7に示すように、各プライベート表現は関連付けられた表現コード726を有し得る。表現コード726は、プライベート表現724にアクセスするのを支援するために、受信側ワイヤレスデバイスによって傍受され、使用され得る。さらに、表現コード726は、プライベート表現724において自己認証を支援するために使用され得る(たとえば、要求側アプリケーション722が表現コードが生成された/記憶されたデバイスに関連付けられていることを確認する)。

【００４３】

表現検証マネージャ730は、セキュアメモリストア732(たとえば、セキュア不揮発性メモリ)を含み得る。一態様では、表現検証マネージャ730は、アプリケーション722の構成/再構成プロセスの一部としてプライベート表現コードを生成し得る。たとえば、アプリケーション722のインストールの一部として、表現検証マネージャ730は、プライベート表現コードを生成し得る。一例では、表現検証マネージャ730は、アプリケーション722がプライベート表現に関連付けられたアクセス特性(たとえば、どのピアデバイス704がプライベート表現にアクセスするのを許可されるか)を変更するように再構成されると、更新され

たプライベート表現コードを生成し得る。一態様では、表現検証マネージャ730は、各アプリケーション722に関連付けられた複数のプライベート表現コードを生成し得る。別の態様では、セキュアメモリストア732は生成されたプライベート表現コードを安全に記憶し得る。図7は表現検証マネージャ730をアプリケーションプロセッサ720およびモデムプロセッサ740とは別個のモジュールとして示しているが、表現検証マネージャ730は、アプリケーションプロセッサ720、モデムプロセッサ740、またはそれらの任意の組合せに常駐し得る。さらに、一態様では、表現検証マネージャ730はアプリケーションプロセッサ720とモデムプロセッサ740との間のインターフェースとして働き得る。別の態様では、表現検証マネージャ730の第1の部分はモデムプロセッサ740に関連付けられ得、表現検証マネージャ730の第2の部分はアプリケーションプロセッサ720とモデムプロセッサ740との間の中間レイヤとして構成され得る。別の態様では、セキュアメモリストア732は他のデバイス704からの情報(たとえば、不明瞭なD2D情報712)を記憶し得る。そのような態様では、受信された情報はtime to live(TTL)値を有し得る。別の態様では、TTL値は局所的に生成され得る。モデムプロセッサ740は、1つまたは複数の無線アクセス技術(RAT)を使用して情報を受信および送信するように構成され得る。

【００４４】

アプリケーションサーバ706は、プライベート表現通信に関連付けられた情報を記憶するように構成され得る。一態様では、アプリケーションサーバ706は、プライベート表現コード726をワイヤレスデバイス(たとえば、702、704)上のアプリケーション722に配信するときに、ユーザ選択された関係に従い得る。一態様では、信頼できるアプリケーションサーバ706は、セキュアメモリストア732に記憶されるべき表現コード714を生成し得る。

【００４５】

動作上の態様では、アプリケーション722の構成/再構成プロセスの一部として、不明瞭なD2D情報モジュール736は、不明瞭なD2D情報712を生成する際にワイヤレスデバイス702を支援し得る。一態様では、不明瞭なD2D情報712は、認可されたワイヤレスデバイス704に直接送信され得る。別の態様では、不明瞭なD2D情報712は、プライベート表現ストア708に記憶し、1つまたは複数の認可されたワイヤレスデバイス704に通信するために、アプリケーションサーバ706に通信され得る。一態様では、不明瞭なD2D情報712は、プライベート表現724、表現コード726、アプリケーション722の名前、カウンタ、生成時刻、以前に生成された表現コード、有効期限、告知側ワイヤレスデバイス702の証明書などを含み得る。別の態様では、不明瞭なD2D情報712は、不明瞭なD2D情報712の真正性を示すデジタル署名で署名され得る。そのような態様では、デジタル署名は、事業者の署名付きの鍵、一時デバイス識別子、TTL値などを含み得る。

【００４６】

別の動作上の態様では、ワイヤレスデバイス702に関連付けられたアプリケーション722は、プライベート表現724が告知されることを要求し得る。そのような態様では、アプリケーション722は、プライベート表現724および関連付けられた表現コード726とともに要求を表現検証マネージャ730に送り得る。表現検証マネージャ730は、受信された表現コード726をセキュアメモリストア732に記憶されたプライベート表現コード734と比較するように構成され得る。表現コード726が記憶されたプライベート表現コード734と一致する場合、表現検証マネージャ730はモデムプロセッサ740がプライベート表現724を告知する710ことを可能にする。対照的に、表現コード726が記憶されたプライベート表現コード734と一致しない場合、表現検証マネージャ730はモデムプロセッサ740がプライベート表現724を告知する710ことを禁止する。

【００４７】

ワイヤレスデバイスは、代わりに、当業者によって、ユーザ機器(UE)、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、ワイヤレスノード、リモートユニット、モバイルデバイス、ワイヤレス通信デバイス、遠隔デバイス、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、遠隔端末、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

で呼ばれることもある。

【００４８】

以下で説明する例示的な方法および装置は、たとえばFlashLinQ、WiMedia、Bluetooth（登録商標）、ZigBee、またはIEEE802.11標準に基づくWi-Fiに基づくワイヤレスデバイス間通信システムなど、様々なワイヤレスデバイス間通信システムのうちの任意のものに適用可能である。説明を簡略化するために、例示的な方法および装置について、LTEのコンテキスト内で説明する。しかしながら、例示的な方法および装置は、より一般的には、様々な他のワイヤレスデバイス間通信システムに適用可能であることを、当業者であれば理解されよう。

【００４９】

図8および図11は、提示した主題の様々な態様による様々な方法を示している。説明を簡単にするために、方法について、一連の動作またはシーケンスステップとして図示および説明しているが、いくつかの動作は、本明細書で図示および説明したものと異なる順序で、かつ/または他の動作と同時に行うことができるため、請求する主題は、動作の順序によって限定されないことを理解し、諒解されたい。たとえば、方法は、代わりに、状態図においてなど、一連の相互に関係する状態またはイベントとして表すことができることを、当業者であれば理解し、諒解されよう。さらに、特許請求する主題に従って方法を実装するために、示したすべての行為が必要とされ得るわけではない。さらに、以下および本明細書の全体にわたって開示される方法を製造品に記憶して、そのような方法をコンピュータにトランスポートし、伝達するのを容易にすることができることをさらに諒解されたい。本明細書で使用される場合、製造品という用語は、任意のコンピュータ可読デバイス、キャリア、または媒体からアクセス可能なコンピュータプログラムを包含する。

【００５０】

図8は、ワイヤレス通信の第2の方法のフローチャート800である。この方法は、UEによって実施され得る。

【００５１】

任意の態様では、ブロック802において、UEはアプリケーションの構成プロセスの一部として表現コードおよび関連付けられたプライベート表現を生成し得る。一態様では、表現コードは、アクセス制御のために、たとえば、対応するプライベート表現へのアクセスを許可される人をフィルタリングするために使用され得る。たとえば、D2D対応アプリケーションが最初にインストールされる(および/またはデフレンド(de-friending)が行われる、たとえば、プライベート表現アクセス認可の取消し)とき、UEはプライベート表現とプライベート表現に関連付けられた表現コードの両方を生成し得る。一態様では、UEは、表現コードがオーバージエアで使用されるとき、プライベート表現を生成することなく表現コードを再生成し得る。

【００５２】

追加または代替として、任意の態様では、ブロック814において、UEは信頼できるサーバから安全に表現コードを受信し得る。

【００５３】

一態様では、ブロック804において、UEは生成された表現コードを記憶し得る。一態様では、表現コードは鍵ストアに記憶され得る。そのような態様では、鍵ストアは、データおよびコードのための保護された不揮発性物理メモリを含み得る。鍵ストアは、告知されたプライベート表現のためのローカル鍵(たとえば、コード)を維持し得る。別の任意の態様では、鍵ストアは、監視されたプライベート表現のためのリモート鍵を維持し、任意選択で検証する。そのような態様では、リモート鍵の検証は、たとえば、署名検証を使用することによって、リモートUEがこのUEにその表現を監視することを認可したことのチェックを含む。

【００５４】

任意の態様では、UEはまた、表現コードに関連付けられた不明瞭なD2D情報を送信し得る。そのような態様では、不明瞭なD2D情報は、別のUEおよび/または信頼できるアプリケ

ーションサーバに送信され得る。さらに、そのような態様では、不明瞭なD2D情報は、プライベート表現、表現コード、アプリケーションの名前、カウンタ、生成時刻、以前に生成された表現コード、有効期限、告知側UEの証明書などを含み得る。別の態様では、不明瞭なD2D情報は、不明瞭なD2D情報の真正性を示すデジタル署名で署名され得る。そのような態様では、デジタル署名は、事業者の署名付きの鍵、一時デバイス識別子、time to live(TTL)値などを含み得る。

【００５５】

ブロック808において、UEは、表現コード(および/または表現コードへの参照)を含み、関連付けられたプライベート表現の告知を要求する、アプリケーションからの要求を受信し得る。

【００５６】

ブロック810において、UEは、告知要求とともに含まれる表現コードが要求側アプリケーションの記憶された表現コードと一致するかどうかを判断し得る。一態様では、UEに関連付けられた表現検証マネージャ(EVM)が、この判断を行い得る。そのような態様では、EVMは、UEアプリケーションプロセッサ(高レベルオペレーティングシステム(HLOS)「サービス」の一部であるとき)、モデムプロセッサ、またはそれらの任意の組合せに常駐する信頼できるエンティティであり得る。さらに、一態様では、EVMはアプリケーションとUEのモデムプロセッサとの間のインターフェースとして働き得る。別の態様では、EVMの第1の部分はUEのモデムに関連付けられ得、EVMの第2の部分はUEのアプリケーションレイヤとモデムとの間の中間レイヤとして構成され得る。

【００５７】

ブロック810において、告知要求とともに含まれる表現コードが要求側アプリケーションの記憶された表現コードと一致するとUEが判断した場合、ブロック812において、UEはプライベート表現を告知し得る。

【００５８】

対照的に、ブロック810において、告知要求とともに含まれる表現コードが要求側アプリケーションの記憶された表現コードと一致しないとUEが判断した場合、ブロック814において、UEはプライベート表現の告知を禁止し得る。

【００５９】

図9は、例示的な装置902における異なるモジュール/手段/構成要素間のデータフローを示す概念データフロー図900である。装置はUEであり得る。

【００６０】

装置902は、アプリケーションからのプライベート表現922を告知する旨の要求920を受信し得るアプリケーション処理モジュール910を含む。一態様では、要求920は、表現コード916および/または表現コード916への参照を含み得る。一態様では、表現コード916は、アプリケーション構成モジュール906によって生成され、セキュアメモリモジュール908に記憶され得る。任意の態様では、表現コード916は、受信モジュール904を使用して、信頼できるアプリケーションサーバ706から受信され得る。装置902は、要求920とともに受信された表現コード916および/または表現コード916への参照をセキュアメモリモジュール908に記憶された表現コード916と比較するように構成され得るプライベート表現検証モジュール912をさらに含み得る。一態様では、プライベート表現検証モジュール912は、表現検証マネージャ730に関して説明したように実装され得る。表現コード916が一致する場合、プライベート表現検証モジュール912は、プライベート表現922を告知するように送信モジュール914を促す。対照的に、表現コード916が一致しない場合、プライベート表現検証モジュール912は、送信モジュール914がプライベート表現922を告知することを禁止する。別の態様では、アプリケーション構成モジュール906は、送信モジュール914を使用して送信するための、表現コードに関連付けられた不明瞭なD2D情報918を生成し得る。そのような態様では、不明瞭なD2D情報918は、別のUE(たとえば、UE704)および/または信頼できるアプリケーションサーバ706に送信され得る。さらに、そのような態様では、不明瞭なD2D情報918は、プライベート表現、表現コード、アプリケーションの名前、カウンタ、生

成時刻、以前に生成された表現コード、有効期限、告知側UEの証明書などを含み得る。別の態様では、不明瞭なD2D情報918は、不明瞭なD2D情報の真正性を示すデジタル署名で署名され得る。

【００６１】

装置は、上述した図8のフローチャート内のアルゴリズムのステップの各々を実施する追加のモジュールを含むことができる。そのため、上述した図8のフローチャート内の各ステップは、モジュールによって実施されてよく、装置は、これらのモジュールの1つまたは複数を含むことができる。モジュールは、特に、上記のプロセス/アルゴリズムを遂行するように構成されるか、上記のプロセス/アルゴリズムを実行するように構成されたプロセッサによって実施されるか、プロセッサによって実施するためにコンピュータ可読媒体内に記憶されるか、またはそれらのいくつかの組合せによる、1つまたは複数のハードウェア構成要素であってよい。

【００６２】

図10は、処理システム1014を使用する装置902'向けのハードウェア実装形態の一例を示す図1000である。処理システム1014は、バス1024によって全体的に表されるバスアーキテクチャで実装される場合がある。バス1024は、処理システム1014の特定の適用例および全体的な設計制約に応じて、任意の数の相互接続するバスおよびブリッジを含み得る。バス1024は、プロセッサ1004によって表される1つまたは複数のプロセッサおよび/またはハードウェアモジュール、モジュール804、806、808、810ならびにコンピュータ可読媒体1006を含む、様々な回路を互いにリンクさせる。バス1024は、タイミングソース、周辺機器、電圧調整器、および電力管理回路などの様々な他の回路をリンクすることもでき、これらの回路は当技術分野でよく知られており、したがってこれ以上は説明しない。

【００６３】

処理システム1014は、トランシーバ1010に結合され得る。トランシーバ1010は、1つまたは複数のアンテナ1020に結合される。トランシーバ1010は、送信媒体上の様々な他の装置と通信するための手段を提供する。処理システム1014は、コンピュータ可読媒体1006に結合されたプロセッサ1004を含む。プロセッサ1004は、コンピュータ可読媒体1006上に記憶されたソフトウェアの実行を含む、全般的な処理を担う。ソフトウェアは、プロセッサ1004によって実行されると、任意の特定の装置の上記で説明した様々な機能を処理システム1014に実施させる。コンピュータ可読媒体1006は、ソフトウェアを実行するとき、プロセッサ1004によって操作されるデータを記憶するために使用される場合もある。処理システムは、モジュール904、906、908、および910のうちの少なくとも1つをさらに含む。モジュールは、コンピュータ可読媒体1006に存在する/記憶される、プロセッサ1004で動作しているソフトウェアモジュール、プロセッサ1004に結合された1つもしくは複数のハードウェアモジュール、またはそれらの何らかの組合せとすることができる。処理システム1014は、UE650の構成要素であってよく、メモリ660、ならびに/または、TXプロセッサ668、RXプロセッサ656、およびコントローラ/プロセッサ659のうちの少なくとも1つを含み得る。

【００６４】

一構成では、ワイヤレス通信のための装置902/902'は、プライベート表現を告知する旨の、プライベート表現に関連付けられた表現コードを含む要求を受信するための手段、表現検証マネージャ(EVM)によって、表現コードが表現コードの以前に取得および記憶されたインスタンスに対応するかどうかを判断するための手段、表現コードが表現コードの記憶されたインスタンスに対応すると判断されると、プライベート表現または表現コードのうちの少なくとも1つを告知するための手段、および/または、表現コードが表現コードの記憶されたインスタンスに対応しないと判断されると、プライベート表現に関連付けられた情報の告知を禁止するための手段を含む。別の態様では、装置902/902'は、アプリケーションの構成プロセスの一部として表現コードのインスタンスを取得するための手段を含み得る。そのような態様では、装置902/902'は、表現コードのインスタンスをセキュアメモリストアに記憶するための手段を含み得る。別の態様では、装置902/902'は、表現コー

ドに関連付けられた不明瞭なD2D情報を送信するための手段を含み得る。別の態様では、装置902/902'は、不明瞭なD2D情報の真正性を示すデジタル署名を生成するための手段であって、不明瞭なD2D情報が生成されたデジタル署名とともに送信される、手段を含み得る。一態様では、装置902/902'は、信頼できるサーバから安全に表現コードのインスタンスを取得するための手段を含み得る。そのような態様では、装置902/902'は、表現コードのインスタンスをセキュアメモリストアに記憶するための手段を含み得る。前述の手段は、前述の手段によって列挙された機能を実施するように構成された、装置902、および/または装置902'の処理システム1014の、前述のモジュールのうちの1つまたは複数であり得る。上記で説明したように、処理システム1014は、TXプロセッサ668と、RXプロセッサ656と、コントローラ/プロセッサ659とを含み得る。したがって、一構成では、上記の手段は、上記の手段によって記載された機能を実施するように構成された、TXプロセッサ668と、RXプロセッサ656と、コントローラ/プロセッサ659とであり得る。

【００６５】

開示したプロセスにおけるステップの特定の順序または階層は、例示的な手法の一例であることを理解されたい。設計上の選好に基づいて、プロセスにおけるステップの特定の順序または階層は再構成可能であることを理解されたい。さらに、いくつかのステップを組み合わせるか、または省略することができる。添付の方法クレームは、様々なステップの要素を例示的な順序で提示したものであり、提示された特定の順序または階層に限定されるものではない。

【００６６】

「例示的な」という言葉は、例、事例、または例示として機能することを意味するように本明細書で使用される。「例示的」として本明細書で説明するいかなる態様または設計も、必ずしも他の態様または設計よりも好ましいまたは有利なものと解釈されるべきではない。加えて、本明細書で使用する場合、「のうちの少なくとも1つ」および/または項目のリスト「のうちの1つまたは複数」に言及する句は、個々のメンバーを含む、それらの項目の任意の組合せを指す。一例として、「a、b、またはcのうちの少なくとも1つ」は、a、b、c、a-b、a-c、b-c、およびa-b-cをカバーするものとする。

【００６７】

上記の説明は、本明細書で説明される様々な態様を当業者が実践できるようにするために与えられる。これらの態様への様々な変更は当業者には容易に明らかであり、本明細書で定義した一般的原理は他の態様に適用され得る。したがって、特許請求の範囲は本明細書で示す態様に限定されるよう意図されているわけではなく、文言通りの特許請求の範囲と整合するすべての範囲を許容するように意図されており、単数の要素への言及は、そのように明記されていない限り、「唯一無二の」ではなく、「1つまたは複数の」を意味するよう意図されている。別段に明記されていない限り、「いくつかの」という用語は1つまたは複数を指す。当業者に知られている、または後に知られるようになる、本開示全体にわたって説明する様々な態様の要素の構造的および機能的な均等物のすべては、参照により本明細書に明確に組み込まれ、特許請求の範囲によって包含されるように意図されている。その上、本明細書で開示する内容は、そのような開示が特許請求の範囲で明示的に記載されているかどうかにかかわらず、公に供することは意図されていない。いかなるクレーム要素も、要素が「ための手段(means for)」という語句を使用して明確に記載されていない限り、ミーンズプラスファンクションとして解釈されるべきではない。

【符号の説明】

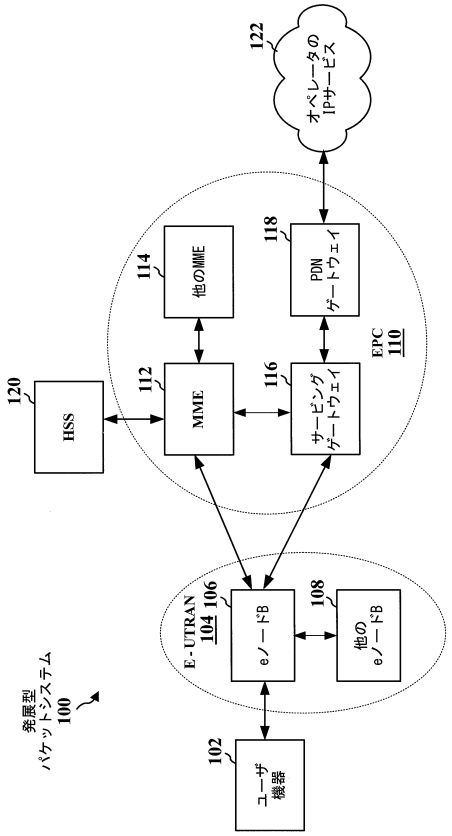
【００６８】

100 LTEネットワークアーキテクチャ、発展型パケットシステム(EPS)
102 ユーザ機器(UE)
104 発展型UMTS地上無線アクセスネットワーク(E-UTRAN)
106 発展型ノードB(eNB)
108 他のeNB
110 発展型パケットコア(EPC)

112 モビリティ管理エンティティ(MME)
114 他のMME
116 サービングゲートウェイ
118 パケットデータネットワーク(PDN)ゲートウェイ
120 ホーム加入者サーバ(HSS)
122 オペレータのIPサービス
200 アクセスネットワーク
202 セルラー領域(セル)
204 マクロeNB、eNB
206 UE
208 低電力クラスeNB
210 セルラー領域
212 UE
410a リソースブロック
410b リソースブロック
420a リソースブロック
420b リソースブロック
430 物理ランダムアクセスチャネル(PRACH)
502 UE
504 eNB
506 物理レイヤ
508 レイヤ2(L2レイヤ)
510 媒体アクセス制御(MAC)サブレイヤ
512 無線リンク制御(RLC)サブレイヤ
514 パケットデータコンバージェンスプロトコル(PDCP)サブレイヤ
516 無線リソース制御(RRC)サブレイヤ
518 インターネットプロトコル(IP)サブレイヤ
520 アプリケーションサブレイヤ
522 通信
610 WANエンティティ
616 送信(TX)プロセッサ
618RX 受信機
618TX 送信機
620 アンテナ
650 UE
652 アンテナ
654RX 受信機
654TX 送信機
656 受信(RX)プロセッサ
658 チャネル推定器
659 コントローラ/プロセッサ
660 メモリ
662 データシンク
667 データソース
668 TXプロセッサ
670 RXプロセッサ
674 チャネル推定器
675 コントローラ/プロセッサ
676 メモリ
700 デバイス間通信システム

702 ワイヤレスデバイス
704 ワイヤレスデバイス
706 アプリケーションサーバ
708 プライベート表現ストア
710 告知する
712 不明瞭なD2D情報
714 表現コード
720 アプリケーションプロセッサ
722 アプリケーション
724 プライベート表現
726 表現コード
730 表現検証マネージャ
732 セキュアメモリストア
734 プライベート表現コード
736 不明瞭なD2D情報モジュール
740 モデムプロセッサ
902 装置
902' 装置
904 受信モジュール、モジュール
906 アプリケーション構成モジュール、モジュール
908 セキュアメモリモジュール、モジュール
910 アプリケーション処理モジュール、モジュール
912 プライベート表現検証モジュール、モジュール
914 送信モジュール、モジュール
916 表現コード
918 不明瞭なD2D情報
920 要求
922 プライベート表現
1004 プロセッサ
1006 コンピュータ可読媒体
1010 トランシーバ
1014 処理システム
1020 アンテナ
1024 バス

【図１】



【図２】

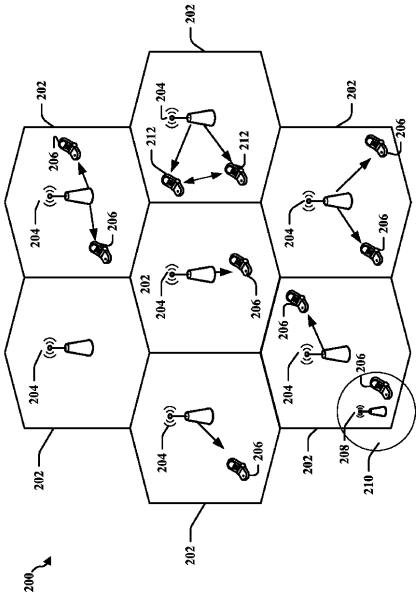
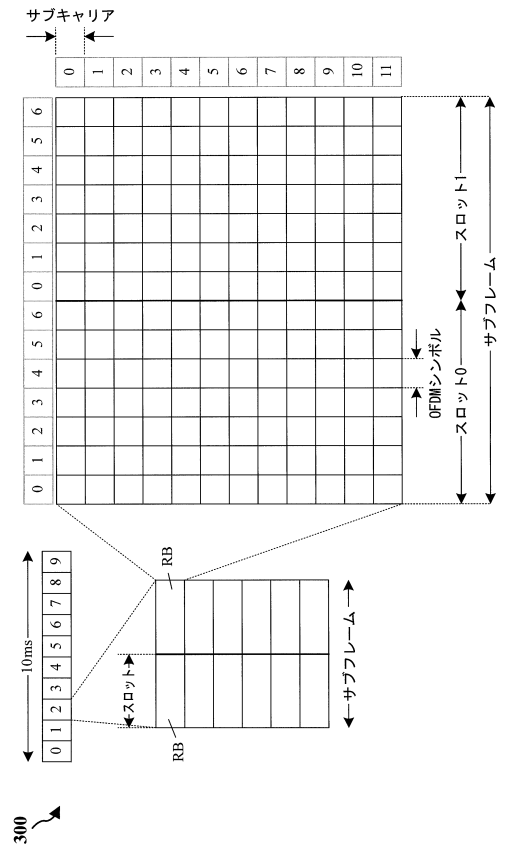
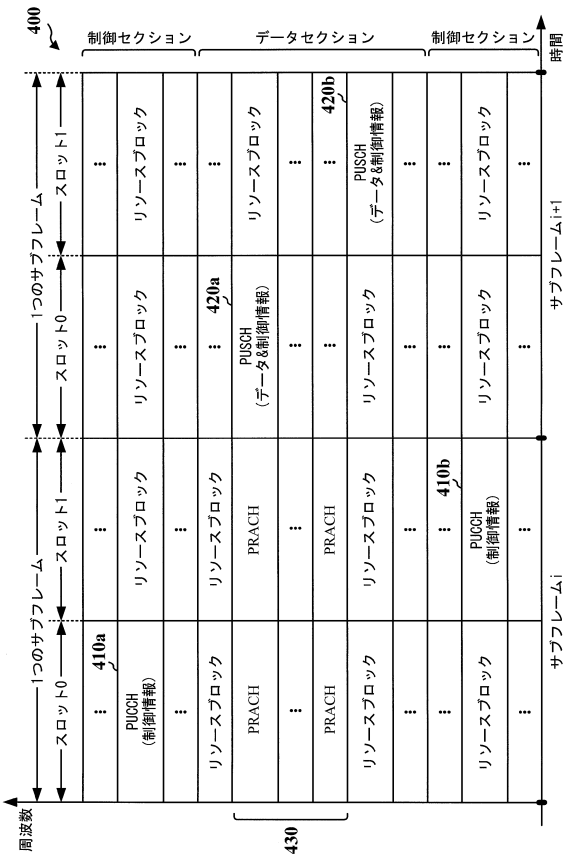


FIG. 2

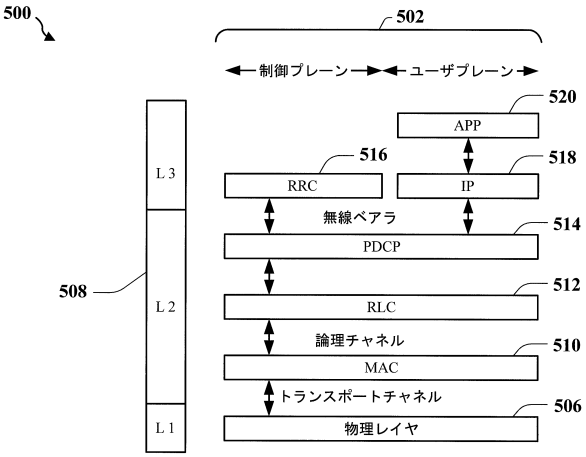
【図３】



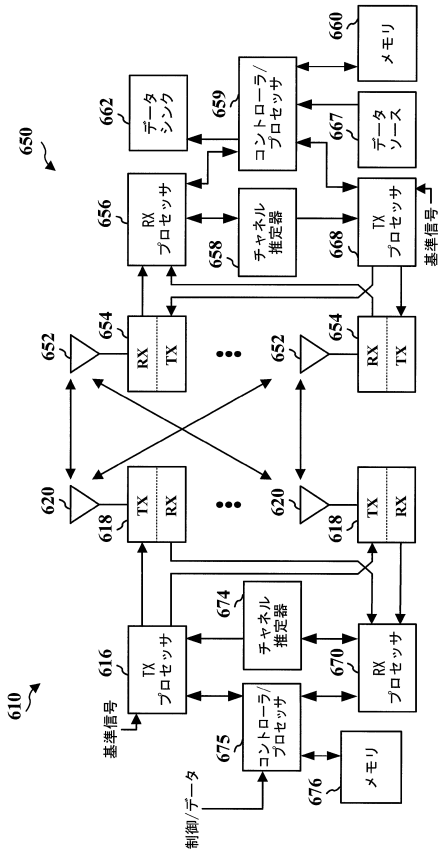
【図４】



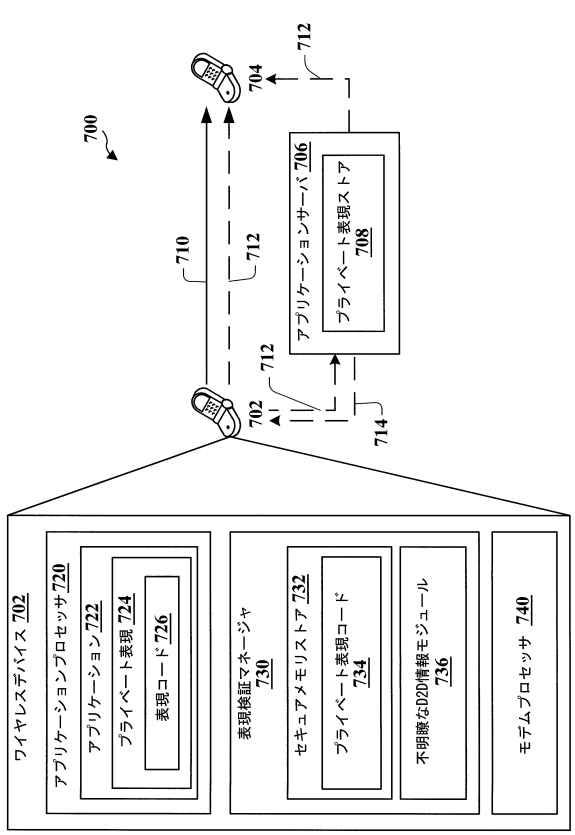
【図５】


500
502
制御プレーン
ユーザプレーン
520
APP
516
RRC
518
IP
無線ベアラ
514
PDCP
512
RLC
論理チャネル
510
MAC
トランスポートチャネル
506
物理レイヤ
L 3
L 2
L 1
508

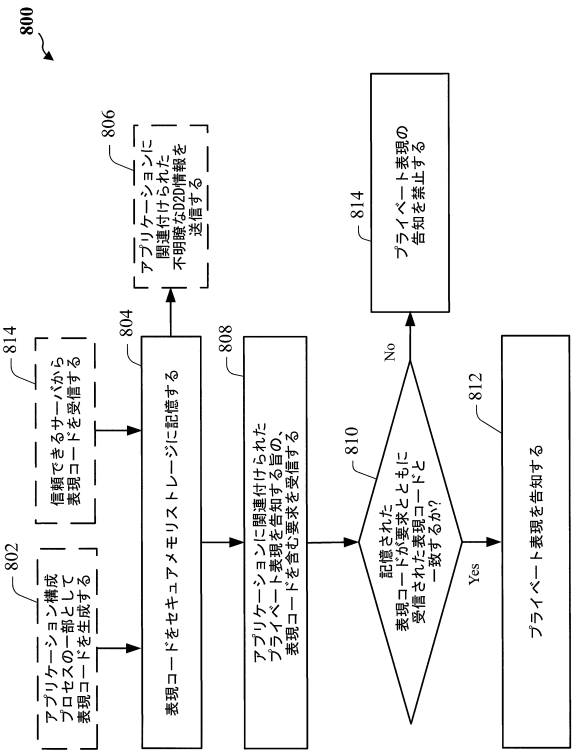
【図６】


650
610
660
メモリ
662
データシンク
659
コントローラ/プロセッサ
667
データソース
656
RXプロセッサ
658
チャネル推定器
668
TXプロセッサ
基準信号
652
654
RX
TX
620
618
674
670
616
675
676
制御/データ

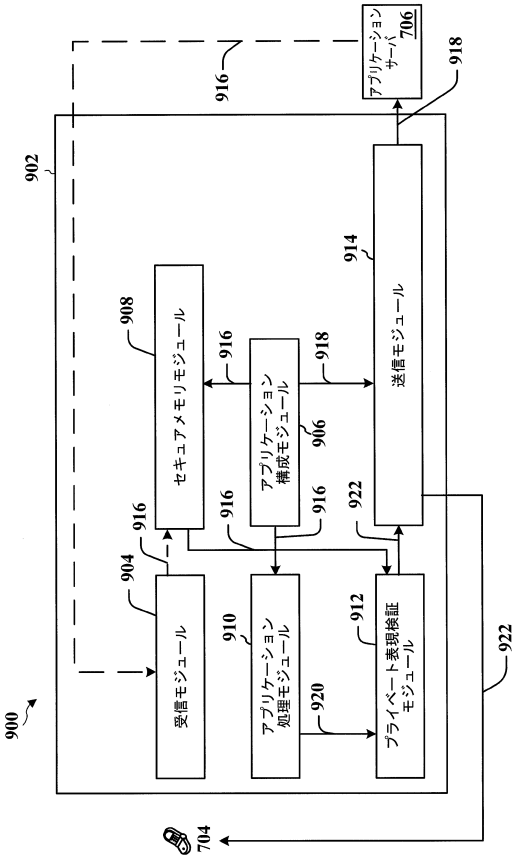
【図７】


700
704
712
710
アプリケーションサーバ 706
プライベート表現ストア 708
702
714
ワイヤレスデバイス 702
アプリケーションプロセッサ 720
アプリケーション 722
プライベート表現 724
表現コード 726
表現検証マネージャ 730
セキュアメモリストア 732
プライベート表現コード 734
不明瞭なD2D情報モジュール 736
モデムプロセッサ 740

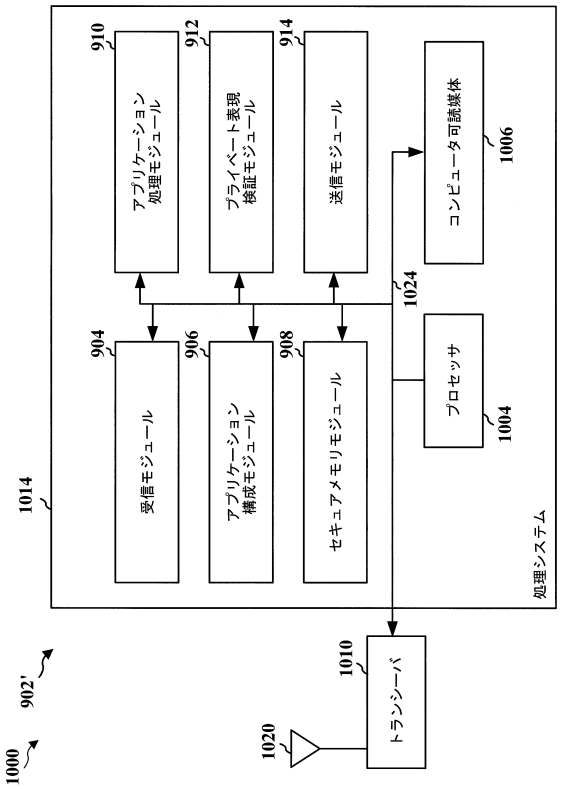
【図８】


800
802
アプリケーション構成プロセスの一部として表現コードを生成する
814
信頼できるサーバから表現コードを受信する
804
表現コードをセキュアメモリストレージに記憶する
806
アプリケーションに関連付けられた不明瞭なD2D情報を送信する
808
アプリケーションに関連付けられたプライベート表現を告知する旨の、表現コードを含む要求を受信する
810
記憶された表現コードが要求とともに受信された表現コードと一致するか?
No
Yes
814
プライベート表現の告知を禁止する
812
プライベート表現を告知する

【図９】


900
902
704
916
アプリケーション
サーバ
706
918
914
送信モジュール
908
セキュアメモリモジュール
916
アプリケーション
構成モジュール
906
904
受信モジュール
910
アプリケーション
処理モジュール
912
プライベート表現検証
モジュール
920
922

【図１０】


1000
902'
1014
処理システム
910
アプリケーション
処理モジュール
912
プライベート表現
検証モジュール
914
送信モジュール
1006
コンピュータ可読媒体
1024
904
受信モジュール
906
アプリケーション
構成モジュール
908
セキュアメモリモジュール
プロセッサ
1004
1010
トランシーバ
1020

フロントページの続き

(72)発明者　ヴィンセント・ディー・パーク
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　ゲオルギオス・チルチス
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　青木　重徳

(56)参考文献　特表２０１１－５２６４７２（ＪＰ，Ａ）
特開平１０－２２８４７６（ＪＰ，Ａ）
米国特許出願公開第２０１２／００６４８２８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｍ　１１／００