(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6759232号
(P6759232)
(45)発行日　令和2年9月23日(2020.9.23)　(24)登録日　令和2年9月4日(2020.9.4)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/32 (2006.01)　H04L 9/00 601E
H04L 9/00 675A
H04L 9/00 601B

請求項の数 18　(全 29 頁)

(21)出願番号　特願2017-549426(P2017-549426)
(86)(22)出願日　平成28年3月3日(2016.3.3)
(65)公表番号　特表2018-510578(P2018-510578A)
(43)公表日　平成30年4月12日(2018.4.12)
(86)国際出願番号　PCT/US2016/020545
(87)国際公開番号　WO2016/160256
(87)国際公開日　平成28年10月6日(2016.10.6)
審査請求日　平成31年2月14日(2019.2.14)
(31)優先権主張番号　62/140,331
(32)優先日　平成27年3月30日(2015.3.30)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/140,426
(32)優先日　平成27年3月30日(2015.3.30)
(33)優先権主張国・地域又は機関
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　アナンド・パラニガウンダー
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　金沢　史明

最終頁に続く

(54)【発明の名称】完全前方秘匿性を有する認証および鍵共有

(57)【特許請求の範囲】
【請求項１】
ユーザ機器とネットワークとの間の完全前方秘匿性(PFS)を有する認証および鍵共有プロトコルを提供するための方法であって、
前記ユーザ機器を用いてアタッチ要求を生成するステップと、
前記ネットワークから前記ユーザ機器を用いて、前記ネットワークによるPFSサポートの指示を含む認証トークンを受信するステップと、
前記ユーザ機器を用いて、前記ネットワークがPFSをサポートするかどうかを決定するステップと、
前記ユーザ機器を用いて、UE公開鍵値を前記ネットワークに送信するステップと、
前記ユーザ機器を用いて、前記ネットワークからネットワーク公開鍵値を受信するステップと、
前記ユーザ機器を用いて、前記ネットワーク公開鍵値とUE秘密鍵値に基づいて共有鍵値を決定するステップと、
前記ユーザ機器を用いて、結合された共有鍵値を作成するために、前記共有鍵値をセッション鍵値と結合するステップと、
前記ユーザ機器を用いて、前記ネットワークへの後続のトラフィックを保護するために、前記結合された共有鍵値を利用するステップと
を備える、方法。
【請求項２】

前記アタッチ要求が、前記ユーザ機器がPFSをサポートするという指示を含む、請求項1に記載の方法。

【請求項３】

前記ユーザ機器を用いてアタッチ要求を生成するステップが、サービス要求、トラッキングエリア要求、または位置更新要求のうちの1つを生成するステップを備える、請求項1に記載の方法。

【請求項４】

前記ユーザ機器を用いて、前記共有鍵値を前記セッション鍵値と結合するステップが、前記共有鍵値および/または前記セッション鍵値の暗号ハッシュを決定するステップを備える、請求項1に記載の方法。

【請求項５】

前記セッション鍵値がK_{ASME}である、請求項1に記載の方法。

【請求項６】

前記セッション鍵値が、暗号鍵(CK)または完全性鍵(IK)のうちの少なくとも1つである、請求項1に記載の方法。

【請求項７】

前記ネットワークに前記UE公開鍵値を送信するステップが、前記ユーザ機器を用いて、楕円曲線暗号を使用して一時的Diffie-Hellmanペアを生成するステップを含む、請求項1に記載の方法。

【請求項８】

前記ネットワークに前記UE公開鍵値を送信するステップが、前記ユーザ機器を用いて、有限体算術を使用して一時的Diffie-Hellmanペアを生成するステップを含む、請求項1に記載の方法。

【請求項９】

前記ユーザ機器が、前記ネットワークがPFSをサポートしていないと決定すると、前記ネットワークへの接続を拒否するステップを備える、請求項1に記載の方法。

【請求項１０】

前記認証トークンが、前記ネットワークがPFSをサポートすることを示すように構成された認証管理フィールド(AMF)ビット値を含む、請求項1に記載の方法。

【請求項１１】

ユーザ機器(UE)とネットワークとの間の完全前方秘匿性(PFS)を有する認証および鍵共有プロトコルを提供するための装置であって、

メモリと、

前記メモリに動作可能に結合され、

UEからアタッチ要求を受信することと、

ネットワークサポートインジケータを含む認証要求をネットワークリソースに送信することと、

前記ネットワークリソースから認証トークンを受信することであって、前記認証トークンが、ネットワークがPFSをサポートするという指示を含む、受信することと、

前記認証トークンを前記UEに送信することと、

UE公開鍵値を含む認証応答を受信することと、

前記認証応答が期待応答でない場合は前記アタッチ要求を拒否することと、

前記認証応答が前記期待応答である場合、

ネットワーク公開鍵値およびネットワーク秘密鍵値を取得することと、

前記ネットワーク秘密鍵値と前記UE公開鍵値とに基づいて共有鍵値を決定することと、

結合された共有鍵値を作成するために、前記共有鍵値をセッション鍵値に結合することと、

後続のネットワークトラフィックを保護するために、前記結合された共有鍵値を使用することと

を行うように構成された少なくとも1つのプロセッサと
を備える、装置。
【請求項１２】
前記認証トークンが、前記UEと前記ネットワークリソースとの間で完全性保護される、請求項11に記載の装置。
【請求項１３】
前記少なくとも1つのプロセッサが、アタッチ要求の代わりに、サービス要求、トラッキングエリア要求、または位置更新要求のうちの1つを受信することによって、前記UEから前記アタッチ要求を受信するように構成される、請求項11に記載の装置。
【請求項１４】
前記少なくとも1つのプロセッサが、前記共有鍵値と前記セッション鍵値の暗号ハッシュを決定するように構成される、請求項11に記載の装置。
【請求項１５】
前記セッション鍵値が、K_{ASME}、暗号鍵(CK)、または完全性鍵(IK)のうちの少なくとも1つである、請求項11に記載の装置。
【請求項１６】
前記共有鍵値が、楕円曲線暗号または有限体算術のうちの1つによって決定される、請求項11に記載の装置。
【請求項１７】
前記アタッチ要求が、前記UEがPFSをサポートするという指示を含む、請求項11に記載の装置。
【請求項１８】
前記認証トークンが、前記ネットワークがPFSをサポートすることを示すための認証管理フィールド(AMF)ビット値を含む、請求項11に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、2015年3月30日に出願された、米国仮出願第62/140,331号「Authentication and Key Agreement with Perfect Forward Secrecy」、2015年3月30日に出願された、米国仮出願第62/140,426号「Authentication and Key Agreement with Perfect Forward Secrecy」、および2015年8月13日に出願された、米国実用新案第14/825,988号「Authentication and Key Agreement with Perfect Forward Secrecy」の利益を主張し、これらの各々は本願の譲受人に譲渡されており、その内容はその全体が参照により本明細書に組み込まれる。
【背景技術】
【０００２】
一般に、ワイヤレス通信システムは、ネットワークと、ネットワークにアクセスしようとするデバイスとの間の認証手順を容易にすることができる。異なるネットワークは、異なる認証手順を有する場合がある。デバイスは、ネットワークへのアクセスを提供する前にデバイスを認証するために使用されるセキュリティ証明書を含み得る。いくつかのシステムでは、機密通信は、デバイス上のモジュールに記憶され、デバイスをホストネットワークに結合する、セキュリティ証明書を利用する場合がある。たとえば、広く使用されている認証および鍵共有(AKA:Authentication and Key Agreement)プロトコルは、デバイス(たとえば、取外し可能ユニバーサル加入者識別モジュール(USIM))とネットワーク(たとえば、ホーム加入者サーバ(HSS))との間で安全に共有される対称ルート鍵(K)に依存する。他のネットワークは、安全な交換を実現するために、他のタイプの暗号保証を提供することが可能であり得る。
【０００３】
AKAを使用する既存のワイヤレスネットワークにおいては、長期ルート鍵(たとえば、K)

が漏洩されると、過去のすべての通信の機密性が損なわれ得るというリスクがある。すなわち、攻撃者は、過去の暗号化された通信をキャプチャし、長期ルート鍵(K)が漏洩されるとそれを解読することができる。異なるレベルの暗号保証(たとえば、弱いものと強いもの)を提供することができるネットワークは、中間者攻撃に対して脆弱である可能性があり、強力な暗号保証がより弱い解決策にビッドダウン(bid down)され得るというリスクがある。

【発明の概要】

【課題を解決するための手段】

【０００４】

以下で、議論された技術の基本的な理解を提供するために、本開示のいくつかの態様を要約する。この概要は、本開示の企図する全特徴の広い全体像ではなく、本開示の全態様の鍵となる要素または重要な要素を特定する意図も、本開示の任意またはすべての態様の範囲を示す意図もない。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、本開示の1つまたは複数の態様のいくつかの概念を要約の形で提示することである。

【０００５】

本開示による、ユーザ機器とネットワークとの間の完全前方秘匿性(PFS:perfect forward secrecy)を有する認証および鍵共有プロトコルを提供するための方法の一例は、ユーザ機器を用いてアタッチ要求を生成するステップと、認証トークンがネットワークによるPFSサポートの指示を含むように、ユーザ機器を用いて認証トークンを受信するステップと、ユーザ機器を用いて、ネットワークがPFSをサポートすることを決定するステップと、ユーザ機器を用いて、UE公開鍵値をネットワークに提供するステップと、ユーザ機器を用いて、ネットワークからネットワーク公開鍵値を受信するステップと、ユーザ機器を用いて、ネットワーク公開鍵値とUE秘密鍵値に基づいて共有鍵値を決定するステップと、ユーザ機器を用いて、結合された共有鍵値を作成するために、共有鍵値をセッション鍵値と結合するステップと、ユーザ機器を用いて、後続のネットワークトラフィックを保護するために、結合された共有鍵値を利用するステップとを含む。

【０００６】

そのような方法の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。アタッチ要求は、ユーザ機器がPFSをサポートするという指示を含み得る。アタッチ要求を生成するステップは、サービス要求、トラッキングエリア要求、または位置更新要求のうちの1つを含み得る。共有鍵値をセッション鍵値と結合するステップは、共有鍵値とセッション鍵値の暗号ハッシュを決定するステップを含み得る。セッション鍵値は、K_{ASME}、暗号鍵(CK)、または完全性鍵(IK)であってもよい。ネットワークにUE公開鍵値を提供することは、楕円曲線暗号を使用して、または有限体算術を使用して、一時的Diffie-Hellmanペアを生成することを含み得る。ネットワークがPFSをサポートしていないと決定すると、ネットワークへの接続を拒否する。認証トークンは、ネットワークがPFSをサポートすることを示すために、1に設定された認証管理フィールド(AMF:authentication management field)ビット値を含み得る。

【０００７】

本開示による、ユーザ機器(UE)とネットワークとの間の完全前方秘匿性(PFS)を有する認証および鍵共有プロトコルを提供するための例示的な装置は、メモリと、メモリに動作可能に結合され、UEからアタッチ要求を受信することと、ネットワークサポートインジケータを含む認証要求をネットワークリソースに提供することと、認証トークンが、ネットワークがPFSをサポートするという指示を含むように、ネットワークリソースから認証トークンを受信することと、認証トークンをUEに提供することと、UE公開鍵値を含む認証応答を受信することと、認証応答が期待応答でない場合はアタッチ要求を拒否することと、認証応答が期待応答である場合、ネットワーク公開鍵値およびネットワーク秘密鍵値を取得することと、ネットワーク秘密鍵値とUE公開鍵値とに基づいて共有鍵値を決定することと、結合された共有鍵値を作成するために、共有鍵値をセッション鍵値に結合することと、後続のネットワークトラフィックを保護するために、結合された共有鍵値を使用するこ

ととを行うように構成された少なくとも1つのプロセッサとを含む。

【０００８】

そのような装置の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。認証トークンは、UEとネットワークリソースとの間で完全性保護され得る。UEから受信したアタッチ要求は、アタッチ要求の代わりに、サービス要求、トラッキングエリア要求、または位置更新要求のうちの1つを受信することを含み得る。共有鍵値とセッション鍵値の暗号ハッシュが決定され得る。セッション鍵値は、K_{ASME}、暗号鍵(CK)、または完全性鍵(IK)のうちの少なくとも1つであってもよい。共有鍵値は、楕円曲線暗号または有限体算術のうちの1つによって決定され得る。アタッチ要求は、UEがPFSをサポートするという指示を含み得る。認証トークンは、ネットワークがPFSをサポートすることを示すために、1に設定された認証管理フィールド(AMF)ビット値を含み得る。

【０００９】

本開示による強力なセキュリティプロトコルを有するシステムに対するビッドダウン攻撃(bid-down attack)を防止するための方法の一例は、ユーザ機器からアタッチ要求を受信するステップと、認証要求が、ネットワークが強力なセキュリティプロトコルをサポートするという指示を含むように、ホームネットワークに認証要求を送信するステップと、完全性保護されたトークンが、ネットワークが強力なセキュリティプロトコルをサポートすることを示すように構成された少なくとも1つのビットを含むように、ホームネットワークから完全性保護されたトークンを受信するステップと、完全性保護されたトークンをユーザ機器に送信するステップとを含む。

【００１０】

そのような方法の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。アタッチ要求は、ユーザ機器が強力なセキュリティプロトコルをサポートするという指示を含み得る。強力なセキュリティプロトコルは、完全前方秘匿性を有する認証および鍵共有プロトコルであり得る。認証要求は、ネットワークが強力なセキュリティプロトコルをサポートすることを示すために、情報要素として属性値ペア(AVP:Attribute Value Pairs)を有する直径プロトコルメッセージであり得る。完全性保護されたトークンは、ホームネットワークから受信された認証ベクトルに含まれ得る。少なくとも1つのビットは、認証管理フィールド(AMF)に含まれ得る。

【００１１】

本開示による強力なセキュリティプロトコルを有するシステムに対するビッドダウン攻撃を防止するための命令を備える、例示的な非一時的プロセッサ可読記憶媒体は、ユーザ機器からアタッチ要求を受信するためのコードと、認証要求が、ネットワークが強力なセキュリティプロトコルをサポートするという指示を含むように、ホームネットワークに認証要求を送信するためのコードと、完全性保護されたトークンが、ネットワークが強力なセキュリティプロトコルをサポートすることを示すように構成された少なくとも1つのビットを含むように、ホームネットワークから完全性保護されたトークンを受信するためのコードと、完全性保護されたトークンをユーザ機器に送信するためのコードとを含む。

【００１２】

そのような非一時的プロセッサ可読記憶媒体の実装形態は、以下の制限のうちの1つまたは複数を含み得る。アタッチ要求は、ユーザ機器が強力なセキュリティプロトコルをサポートするという指示を含み得る。強力なセキュリティプロトコルは、完全前方秘匿性を有する認証および鍵共有プロトコルであり得る。認証要求は、ネットワークが強力なセキュリティプロトコルをサポートすることを示すために、情報要素として属性値ペア(AVP)を有する直径プロトコルメッセージであり得る。完全性保護されたトークンは、ホームネットワークから受信された認証ベクトルに含まれ得る。少なくとも1つのビットは、認証管理フィールド(AMF)に含まれ得る。

【００１３】

本明細書に記載された項目および/または技法は、以下に挙げる能力、ならびに言及されていない他の能力のうちの1つまたは複数を提供することができる。モバイルデバイス

は、完全前方秘匿性をサポートすることを示すための指示をネットワークに提供することができる。ネットワークは、ネットワークが完全前方秘匿性をサポートすることを示すために、ホームネットワークに情報要素を提供することができる。完全性保護されたトークンは、ホームネットワークによって生成され、モバイルデバイスに転送され得る。完全性保護されたトークンは、ネットワークが完全前方秘匿性をサポートすることを示すために、情報要素を含み得る。モバイルデバイスおよびネットワークは、共有鍵を生成するために、Diffie-Hellman交換に参加することができる。共有鍵は、セッション鍵に結合するために使用され得る。後続のネットワークトラフィックを保護するために、結合されたセッション鍵が使用され得る。完全前方秘匿性を有する認証および鍵共有プロトコルが実現され得る。ネットワーク完全前方秘匿性を組み込んだ完全性保護されたトークンの使用によって、ビッドダウン攻撃の潜在的可能性が大幅に削減され得る。他の能力が提供されてよく、本開示に従ったすべての実装形態が、論じられる能力のすべてを提供しなければならないとは限らないことはもちろん、論じられる任意の特定の能力を提供しなければならないとも限らない。さらに、述べられたもの以外の手段によって、上で述べられた効果が達成されることが可能であることがあり、述べられた項目/技法は、述べられた効果を必ずしも生まないことがある。

【００１４】

本発明の他の態様、特徴、および実施形態は、添付の図面と併せて本発明の特定の例示的な実施形態の以下の説明を検討することにより、当業者には明らかになるであろう。本発明の特徴について、以下のいくつかの実施形態および図に対して説明する場合があるが、本発明のすべての実施形態は、本明細書で説明する有利な特徴のうちの1つまたは複数を含むことができる。言い換えれば、1つまたは複数の実施形態について、いくつかの有利な特徴を有するものとして説明する場合があるが、そのような特徴のうちの1つまたは複数は、本明細書で説明する本発明の様々な実施形態に従って使用される場合もある。同様に、例示的な実施形態について、デバイス、システム、または方法の実施形態として以下で説明する場合があるが、そのような例示的な実施形態は、様々なデバイス、システム、および方法において実装され得ることを理解されたい。

【図面の簡単な説明】

【００１５】

【図１】いくつかの態様/実施形態による、モバイルデバイスの一実施形態の構成要素のブロック図である。

【図２】いくつかの態様/実施形態による、例示的なワイヤレス通信システムのブロック図である。

【図３】いくつかの態様/実施形態による、図2のワイヤレス通信システムにおいて使用されるコンピュータシステムの一例のブロック図である。

【図４】3GPPロングタームエボリューション(LTE)認証手順の従来技術のコールフロー図である。

【図５】いくつかの態様/実施形態による、完全前方秘匿性(PFS)特性を有する例示的な認証手順のコールフロー図である。

【図６】完全前方秘匿性(PFS)特性を有する、別の例示的な認証手順のコールフロー図である。

【図７】いくつかの態様/実施形態による、モバイルデバイスとの安全な通信を提供するプロセスのブロックフロー図である。

【図８】いくつかの態様/実施形態による、ネットワークサーバとの安全な通信を提供するプロセスのブロックフロー図である。

【図９】いくつかの態様/実施形態による、強力なセキュリティプロトコルを有するシステムに対するビッドダウン攻撃を防止するためのプロセスのブロックフロー図である。

【発明を実施するための形態】

【００１６】

完全前方秘匿性(PFS)を有する認証および鍵共有(AKA)を提供するための技法が説明され

る。本明細書で使用されるように、長期鍵のうちの1つが将来漏洩された場合、長期鍵のセットから導出されたセッション鍵が漏洩されないことを確実にするために、完全前方秘匿性という用語は、鍵共有プロトコルの特性の暗号定義を指す。本明細書で使用される完全という用語は、障害または欠陥を完全に含まないか、または可能な限りそのような状態に近いものを意味するものではない。AKAは、現代のセルラーネットワーク(たとえば、GSM（登録商標）、UMTS、LTE、eHRPD)において広く使用されている認証および鍵共有プロトコルである。AKAは、3GPP TS 33.102に規定されている。AKAのセキュリティは、一般に、UE(たとえば、典型的にはUSIMに記憶される)とホームネットワーク内のサーバ(たとえば、ホーム加入者サーバ(HSS))との間で安全に共有される対称ルート鍵(K)に依存する。AKAは完全前方秘匿性(PFS)を提供しない。すなわち、AKAは、長期鍵(たとえば、K)が将来漏洩された場合、漏洩することができないセッション鍵を提供しない。議論されるように、一実施形態では、AKAの潜在的なセキュリティ欠陥は、PFS特性によって緩和され得る。たとえば、モバイルデバイスとネットワークサーバとの間で一時的Diffie-Hellman(DHE)交換が発生し得る。モバイルデバイスおよびネットワークサーバは、それぞれ、個々の秘密鍵値および公開鍵値を決定することができる。共有鍵を生成するために、公開鍵が交換され、それぞれの秘密鍵と組み合わされ得る。結果として得られた共有鍵は、認証ベクトル(たとえば、K_{ASME})内のベース鍵に結合され、ネットワーク内の通信を保護するために使用され得る。モバイルデバイスとネットワークサーバの両方がPFSをサポートすることを確実にするために、セキュアな認証情報要素が使用され得る。セキュアな認証ビットは、ビッドダウン攻撃(たとえば、中間者攻撃)を防止することができる。

【００１７】

図1を参照すると、本明細書に記載の様々な技法が利用され得るモバイルデバイス100が示されている。モバイルデバイス100はユーザ機器(UE)であり、様々なモバイル通信および/またはコンピューティングデバイスの機能を含むか、または実装することができ、例として、現在存在しているか、将来開発されるかにかかわらず、携帯情報端末(PDA)、スマートフォン、ラップトップ、デスクトップ、またはタブレットコンピュータなどのコンピューティングデバイス、自動車コンピューティングシステムなどを含むが、これらに限定されない。

【００１８】

モバイルデバイス100は、プロセッサ111(または、プロセッサコア)およびメモリ140を含む。モバイルデバイスは、任意で、公共バス101またはプライベートバス(図示せず)によってメモリ140に動作可能に接続された、信頼できる環境を含み得る。モバイルデバイス100はまた、ワイヤレスネットワークを介してワイヤレスアンテナ122を介してワイヤレス信号123を送受信するように構成された通信インターフェース120およびワイヤレストランシーバ121を含み得る。ワイヤレストランシーバ121は、バス101に接続されている。ここでは、モバイルデバイス100は、単一のワイヤレストランシーバ121を有するものとして示されている。しかしながら、モバイルデバイス100は、代わりに、Wi-Fi、CDMA、ワイドバンドCDMA(WCDMA（登録商標）)、ロングタームエボリューション(LTE)、Bluetooth（登録商標）近距離ワイヤレス通信技術などの複数の通信規格をサポートするために、複数のワイヤレストランシーバ121およびワイヤレスアンテナ122を有することができる。

【００１９】

通信インターフェース120および/またはワイヤレストランシーバ121は、複数のキャリア(異なる周波数の波形信号)上の動作をサポートすることができる。マルチキャリア送信機は、複数のキャリア上で同時に変調信号を送信することができる。各変調信号は、符号分割多元接続(CDMA)信号、時分割多元接続(TDMA)信号、直交周波数分割多元接続(OFDMA)信号、シングルキャリア周波数分割多元接続(SC-FDMA)信号などであり得る。各変調信号は、異なるキャリア上で送信されてもよく、パイロット、オーバーヘッド情報、データなどを搬送してもよい。

【００２０】

モバイルデバイス100はまた、SPSアンテナ158を介して(たとえば、SPS衛星から)衛星測

位システム(SPS)信号159を受信するユーザインターフェース150(たとえば、ディスプレイ、GUI)およびSPS受信機155を含み得る。SPS受信機155は、単一のグローバルナビゲーション衛星システム(GNSS)または複数のそのようなシステムと通信することができる。GNSSは、全地球測位システム(GPS)、Galileo、Glonass、Beidou(Compass)などを含み得るが、これらに限定されない。SPS衛星はまた、衛星、宇宙船(SV)などとも呼ばれる。SPS受信機155は、SPS信号159を全体的または部分的に処理し、モバイルデバイス100の位置を決定するためにこれらのSPS信号159を使用する。プロセッサ111、メモリ140、DSP 112、および/または特殊プロセッサ(図示せず)はまた、SPS受信機155とともに、SPS信号159を全体的または部分的に処理するために、および/またはモバイルデバイス100の位置を計算するために利用され得る。SPS信号159または他の位置信号からの情報の記憶は、メモリ140またはレジスタ(図示せず)を使用して実行される。1つだけのプロセッサ111、1つのDSP 112、および1つのメモリ140が図1に示されているが、これらの構成要素のうちのいずれか1つ、ペア、またはすべてがモバイルデバイス100によって使用され得る。モバイルデバイス100に関連付けられるプロセッサ111およびDSP 112は、バス101に接続される。

【００２１】

メモリ140は、機能を1つまたは複数の命令またはコードとして記憶する非一時的コンピュータ可読記憶媒体(または、媒体)を含むことができる。メモリ140を構成する媒体は、RAM、ROM、FLASH、ディスクドライブなどを含むが、これに限定されるものではない。一般に、メモリ140によって記憶された機能は、汎用プロセッサ111、専用プロセッサ、またはDSP 112によって実行される。したがって、メモリ140は、プロセッサ111および/またはDSP 112に、説明されている機能を実行させるように構成されたソフトウェア(プログラミングコード、命令など)を記憶する、プロセッサ可読メモリおよび/またはコンピュータ可読メモリである。あるいは、モバイルデバイス100の1つまたは複数の機能は、ハードウェアにおいて全体的または部分的に実行され得る。

【００２２】

モバイルデバイス100は、ビュー内の他の通信エンティティおよび/またはモバイルデバイス100にとって利用可能な情報に基づいて、様々な技法を使用して、関連付けられるシステム内のその現在の位置を推定することができる。たとえば、モバイルデバイス100は、1つまたは複数のワイヤレスローカルエリアネットワーク(LAN)、BLUETOOTH（登録商標）またはZIGBEE(登録商標)などの近距離ワイヤレス通信技術を利用するパーソナルエリアネットワーク(PAN)、SPS衛星、および/あるいは地図サーバまたはLCIサーバから取得された地図制約データに関連付けられるアクセスポイント(AP)から取得された情報を使用して、その位置を推定することができる。

【００２３】

次に図2を参照すると、例示的な通信システム200のブロック図が示されている。通信システム200は、LTE無線アクセス技術を使用して、UE 202(すなわち、モバイルデバイス100)と進化型ノードB(eNB) 204(たとえば、基地局、アクセスポイントなど)との間のワイヤレス無線通信を提供するロングタームエボリューション(LTE)無線アクセスネットワーク(RAN)を含み得る。図2のLTEネットワークは、他のネットワークが使用され得る場合にのみ例示的である。説明を簡単にするために、図2は、UE 202および1つのeNB 204を示すが、RANは、任意の数のUEおよび/またはeNBを含むことができる。eNB 204は、順方向リンクまたはダウンリンクチャネルを介してUE 202に情報を送信し、UE 202は、逆方向リンクまたはアップリンクチャネルを介してeNB 204に情報を送信することができる。図示されるように、RANは、これらに限定されないが、LTE、LTE-A、HSPA、CDMA、高速パケットデータ(HRPD)、進化型HRPD(eHRPD)、CDMA2000、GSM（登録商標）、GPRS、GSM（登録商標）進化(EDGE)のための強化されたデータレート、UMTSなどの、任意の適切なタイプの無線アクセス技術を利用することができる。

【００２４】

eNB 204は、課金(たとえば、サービスの利用料金など)、セキュリティ(たとえば、暗号化および完全性保護)、加入者管理、モビリティ管理、ベアラ管理、QoS処理、データフロ

ーのポリシー制御、および/または外部ネットワークとの相互接続を可能にするコアネットワークと通信することができる。RANおよびコアネットワークは、たとえば、S1インターフェースを介して通信することができる。コアネットワークは、サービングゲートウェイ(S-GW)210からの制御シグナリングのためのエンドポイントとなり得るモビリティ管理エンティティ(MME)206を含むことができる。MME 206は、モビリティ管理(たとえば、追跡)、認証、およびセキュリティなどの機能を提供することができる。MME 206は、S1インターフェースを介してRANと通信することができる。サービングゲートウェイ(S-GW)210は、コアネットワークをLTE RANに接続するユーザプレーンノードである。MME 206は、S11インターフェースを介してS-GW 210と通信するように構成され得る。MME 206およびS-GW 210は、ユーザ、ならびにRANから発信される、および/またはRANで終端する制御シグナリングのための単一のエンドポイントを提供するために、単一のノードとして構成され得る。ネットワークはまた、ポリシーおよび課金ルール機能(PCRF)212を含み得る。

【００２５】

通信システム200はまた、コアネットワーク(およびRAN)と外部ネットワークとの間の通信を容易にするパケットデータネットワーク(PDN)ゲートウェイ(GW)214を含み得る。PDN GW 214は、パケットフィルタリング、QoSポリシング、課金、IPアドレス割当て、およびトラフィックの外部ネットワークへのルーティングを提供することができる。一例では、S-GW 210およびPDN GW 214は、S5インターフェースを介して通信することができる。図2においては別々のノードとして示されているが、S-GW 210およびPDN GW 214は、たとえば、通信システム200内のユーザプレーンノードを削減するために単一のネットワークノードとして動作するように構成され得ることを理解されたい。通信システム200はまた、MME 206と通信することができるホーム加入者サービス(HSS)エンティティ208を含み得る。通信システム200はまた、互いに通信し、さらにPDN GW 214およびHSS 208とさらに通信するように構成された3GPP認証、認可および課金(AAA)サーバ/プロキシ、および3GPP2 AAAサーバ/プロキシ(図示せず)などの、他のネットワーク構成要素を含み得る。

【００２６】

通信システム200は、PDN GW 214を介して外部ネットワークと通信するように構成され得る。外部ネットワーク(図示せず)は、公衆交換電話網(PSTN)、IPマルチメディアサブシステム(IMS)、および/またはIPネットワークなどのネットワークを含み得るが、これらに限定されない。IPネットワークは、インターネット、ローカルエリアネットワーク、ワイドエリアネットワーク、イントラネットなどであり得る。図2は、ただ1つの可能な構成の一例であり、多くの他の構成および追加の構成要素が、以下に説明される様々な態様および実装形態に従って使用され得る。

【００２７】

図3に示されるコンピュータシステム300は、図2の要素の機能を少なくとも部分的に実装するために利用され得る。図3は、本明細書で説明されるような様々な他の実施形態によって提供される方法を実行することができ、および/またはモバイルデバイスまたは他のコンピュータシステムとして機能することができるコンピュータシステム300の一実施形態の概略図を提供する。たとえば、eNB 204、MME 206、HSS 208、S-GW 210、PCRF 212、およびPDN GW 214は、1つまたは複数のコンピュータシステム300で構成され得る。図3は、様々な構成要素の一般化された図を提供し、そのいずれか、またはすべてが適宜、利用され得る。したがって、図3は、個々のシステム要素をいかにして、比較的別々にまたは比較的十分に統合して実装し得るかを広く示している。

【００２８】

バス305を介して電気的に結合され得る(または、適宜他の方法で通信し得る)ハードウェア要素を備えるコンピュータシステム300が示される。ハードウェア要素は、これに限定されないが、1つまたは複数の汎用プロセッサおよび/あるいは1つまたは複数の専用プロセッサ(デジタル信号処理チップ、グラフィックス高速化プロセッサ、および/または同等物)を含む1つまたは複数のプロセッサ310と、これに限定されないが、マウス、キーボード、および/または同等物などを含むことができるが1つまたは複数の入力デバイス315

と、これに限定されないが、ディスプレイデバイス、プリンタ、および/または同等物を含むことができる1つまたは複数の出力デバイス320とを含み得る。プロセッサ310は、たとえば、インテリジェントハードウェアデバイス、たとえばインテル(登録商標)コーポレーションまたはAMD(登録商標)によって作成されたものなどの中央処理装置(CPU)、マイクロコントローラ、ASICなどを含むことができる。他のプロセッサタイプも利用することができる。

【００２９】

コンピュータシステム300は、これに限定されないが、ローカルおよび/またはネットワークアクセス可能なストレージを備え得る、1つまたは複数の非一時的ストレージデバイス325をさらに含む(および/または通信する)ことができ、および／または、これに限定されないが、プログラム可能、フラッシュ更新可能、および/または同様の、ディスクドライブ、ドライブアレイ、光ストレージデバイス、ランダムアクセスメモリ(「RAM」)および/または読出し専用メモリ(「ROM」)などのソリッドステートストレージデバイスを含むことができる。そのようなストレージデバイスは、これに限定されないが、様々なファイルシステム、データベース構造、および/または同等物などの、任意の適切なデータ記憶ストアを実現するように構成され得る。

【００３０】

コンピュータシステム300はまた、通信サブシステム330を含む場合があり、通信サブシステム330は、これに限定されないが、モデム、ネットワークカード(ワイヤレスまたはワイヤード)、赤外線通信デバイス、ワイヤレス通信デバイスおよび/またはチップセット(Bluetooth（登録商標）短距離ワイヤレス通信技術トランシーバ/デバイス、802.11デバイス、WiFiデバイス、WiMaxデバイス、セルラー通信設備など)、および/または同等物を含むことができる。通信サブシステム330は、ネットワーク(一例を挙げると、以下に説明するネットワークなど)、他のコンピュータシステム、および/または本明細書に記載された他の任意のデバイスとの間でデータを交換できるようにする場合がある。多くの実施形態では、コンピュータシステム300は、上記のような、RAMまたはROMデバイスを含むことができるワーキングメモリ335をさらに備える。

【００３１】

コンピュータシステム300はまた、オペレーティングシステム340、デバイスドライバ、実行可能ライブラリ、および/あるいは1つまたは複数のアプリケーションプログラム345などの他のコードを含む、ワーキングメモリ335内に現在配置するように示されているソフトウェア要素を備えることができ、他のコードは、様々な実施形態によって提供されるコンピュータプログラムを備えることができ、および/または本明細書で説明されるように、他の実施形態によって提供される方法を実装するように、および/またはシステムを構成するように設計され得る。単なる例として、本明細書で説明した1つまたは複数のプロセスは、コンピュータ(および/またはコンピュータ内のプロセッサ)によって実行可能なコードおよび/または命令として実装されてもよい。そのようなコードおよび/または命令は、説明される方法に従って1つまたは複数の動作を実行するために、汎用コンピュータ(または他のデバイス)を構成および/または適合させるために使用することができる。

【００３２】

これらの命令および/またはコードのセットは、上述したストレージデバイス325などのコンピュータ可読記憶媒体に記憶され得る。いくつかの場合において、記憶媒体はコンピュータシステム300などのコンピュータシステム内に組み込まれてよい。他の実施形態では、記憶媒体は、コンピュータシステムから分離されてよく(たとえば、コンパクトディスクなどの取外し可能媒体)、ならびに/あるいは記憶媒体を使用して記憶された命令/コードによる汎用コンピュータのプログラム、構成、および/または適合を行うことができるようにインストールパッケージで提供されてよい。これらの命令は、コンピュータシステム300によって実行可能である実行可能コードの形をとってよく、ならびに/あるいは(たとえば、一般に利用可能な様々なコンパイラ、インストールプログラム、圧縮/解凍ユーティリティなどのいずれかを使用して)コンピュータシステム300上でのコンパイルおよ

び/またはインストール時に実行可能コードの形をとるソースコードおよび/またはインストール可能コードの形をとってよい。

【００３３】

図4を参照すると、3GPPロングタームエボリューション(LTE)認証手順の従来技術のコールフロー図400が示されている。従来技術のコールフロー図400は、3GPP TS 33.401などの公表された標準に準拠している。コールフローに示されるメッセージは、コンピュータシステム間で電気的に送信される情報(たとえば、データフィールド)を表す。情報は、当技術分野で知られているデータタイプ(たとえば、バイナリ、数字、文字、varchar、日付など)であり得る。図400は、通信システム200によって使用され得るセキュリティ手順を表し、したがって、図400は、UE 202(たとえば、モバイルデバイス100)、ネットワーク402、およびホームネットワーク404を含む。ネットワーク402は、eNodeB(eNB) 204およびMME 206を含み得る。ホームネットワーク404は、少なくともHSS 208を含む。コールフロー図400は、ネットワーク上に認証情報を提供するための認証および鍵共有(AKA)手順を示す。UE 202は、国際移動局装置識別子(IMSI:International Mobile Station Equipment Identity)を含む非アクセス層(NAS)要求メッセージ410をMME 206に(たとえば、eNB 204を介して)送信する。MME 206は、ユーザ認証を実行するためにHSS 208から認証データを検索するように構成される。MME 206は、IMSI(たとえば、NASアタッチ要求メッセージ410に含まれる)およびネットワーク識別情報(SN_id)を含む認証情報要求メッセージ412をHSS 208に送信することができる。SN_idは、モバイル国コードおよびモバイルネットワークコードを含み得る。認証情報要求メッセージ412はまた、ネットワークタイプ(たとえば、E-UTRAN)および要求された認証ベクトル(AV)の数(図示せず)を示すデータフィールドを含み得る。HSS 208は、認証情報要求メッセージ412を受信し、1つまたは複数のAVを生成するように構成される。一例では、HSS 208は、認証センター(AuC)(図示せず)にAVを要求することができる。AVは、認証トークン(AUTN)、期待応答(XRES)、乱数(RAND)、およびキーアクセスセキュリ
ティ管理エンティティ(K_{ASME})を含む。K_{ASME}は、NASシグナリング保護とユーザプレーン保護のためのアクセス層(AS)およびNAS暗号化鍵と完全性鍵を生成するための基盤を形成する。AVは、認証情報応答メッセージ414においてMME 206に提供される。AKA(たとえば、UMTS、GSMA)を使用する他の3GPPネットワークにおいては、AVは、認証トークン(AUTN)、期待応答(XRES)、乱数(RAND)、暗号鍵(CK)、および完全性鍵(IK)を含む。CKとIKは、メッセージの暗号化と完全性保護のために使用される。

【００３４】

MME 206は、進化型パケットシステム(EPS)プロトコルを介してUE 202の認証を開始するように構成され得る。MME 206は、ホームネットワーク404から受信されたAUTNおよびRAND値、ならびに受信したK_{ASME}値に基づくNASキーセット識別子(KSI_{ASME})を含む、NAS認証要求メッセージ416を生成する。KSI_{ASME}は、UE 202およびMME 206に記憶される。UE 202は、(たとえば、AUTNが受け入れられ得るかどうかをチェックすることによって)AVの新鮮さを識別するように構成される。次いで、UE 202は、検証が受け入れられた場合(たとえば、AUTNが受け入れられた場合)に応答(RES)値を計算し得、次いで、RES値を含むNAS認証応答メッセージ418を送信する。検証が失敗した場合、UE 202は、失敗の理由を示すCAUSE値とともに認証失敗メッセージをMME 206に送信する。MME 206は、RES値とXRES値が等しいかどうかを決定するように構成される。それらが等しい場合、認証は成功である。それらが等しくない場合、MME 206は、さらなるアイデンティティ要求を開始するように、またはUE 202に向けて認証拒絶メッセージを送信するように構成され得る。

【００３５】

認証に成功すると、MME 206は、MME 206とUE 202との間の往復メッセージからなるNASセキュリティモードコマンド(SMC)手順を開始するように構成され得る。MME 206は、機密性および完全性アルゴリズムを含むNASセキュリティモードコマンド(SMC)メッセージ420を送信する。たとえば、NAS SMCメッセージ420は、再生されたUEセキュリティ能力、選択されたNASアルゴリズム、K_{ASME}を識別するためのKSI_{ASME}値、およびアイドルモビリティ

においてマッピングされたコンテキストを作成する場合の$NONCE_{UE}$および$NONCE_{MME}$値の両方を含み得る。NAS SMCメッセージ420は、メッセージ内のKSI_{ASME}値によって示されるK_{ASME}に基づいて、NAS完全性鍵を用いて完全性保護され得る(しかし、暗号化されない)。UE 202は、NAS SMCメッセージ420の完全性を検証するように構成される。これは、これらが攻撃者によって修正されなかったことを保証するために、MME 206によって送信されたUEセキュリティ機能がUE 202に記憶されたものと一致することを保証することと、KSI_{ASME}値によって示されるK_{ASME}に基づいて、示されたNAS完全性アルゴリズムおよびNAS完全性鍵を使用して完全性保護をチェックすることとを含み得る。NASセキュリティモードコマンドのチェックがパスする場合、UE 202は、NASセキュリティモード完了メッセージ422で応答するように構成される。UE 202は、NAS完全性保護および暗号化/解読を実行し、暗号化および完全性保護されたMME 206にNASセキュリティモード完了メッセージ422を送信するように構成される。MME 206は、NASセキュリティモードコマンドにおいて示される鍵およびアルゴリズムを使用して、NASセキュリティモード完了メッセージ422に対する完全性保護を解読し、チェックするように構成される。このセキュリティコンテキストを有するMMEにおけるNASダウンリンク暗号化は、NASセキュリティモード完了メッセージ422を受信した後に開始することができる。MME 206におけるNASアップリンク解読は、NAS SMCメッセージ420を送信した後に開始することができる。

【００３６】

NASセキュリティモード完了メッセージ422の受信に続いて、MME 206は、S1AP初期コンテキスト設定メッセージ424を送信することによって、eNB 204とMME 206との間のS1インターフェースを開始するように構成され得る。一般に、初期コンテキスト設定手順の目的は、E-UTRAN無線アクセスベアラ(E-RAB)コンテキスト、セキュリティ鍵、ハンドオーバ制限リスト、UE無線能力およびUEセキュリティ機能などを含む、必要な全体的初期UEコンテキストを確立することである。手順は、UEに関連付けられるシグナリングを使用する。S1AP初期コンテキスト設定メッセージ424は、トレース起動(Trace Activation)情報要素(IE)、ハンドオーバ制限リストIE(ローミング、エリアまたはアクセス制限を含み得る)、UE無線能力IE、RAT/周波数優先順位のための加入者プロファイルID IE、CSフォールバックインジケータIE、SRVCC動作可能IE、CSGメンバーシップステータスIE、登録LAI IE、UEにサービスするMMEを示すGUMMEI ID IE、MMEによって割り当てられたMME UE S1AP IDを示すMME UE S1AP ID2 IE、管理ベースのMDT許可IE、および、MMEで利用可能である場合、RAT/周波数優先順位の加入者プロファイルID IEを含み得る。eNBは、3GPP TS 25.331プロトコル仕様に記載されるものなどの、無線リソース制御(RRC)プロトコルを介してUE 202との安全な通信を開始するように構成され得る。eNBは、RRC SMCメッセージ426をUE 202に送信することができ、UE 202は、本明細書に記載されるように、RRCセキュリティモード完了メッセージ428を生成するように構成され得る。

【００３７】

さらに図2を参照して、図5を参照すると、完全前方秘匿性(PFS)を有する例示的な認証手順のコールフロー図500が示されている。図500は、通信システム200によって使用され得るセキュリティ手順を表し、したがって、図500は、UE 202(たとえば、モバイルデバイス100)、ネットワーク502、およびホームネットワーク504を含む。ネットワーク502は、eNodeB(eNB) 204およびMME 206を含み得る。ホームネットワーク504は、PFS特性を有するAKAをサポートすると想定されるHSS 208を少なくとも含む。コールフロー図500は、完全前方秘匿性(PFS)特性を追加することによって、図4において説明した認証および鍵共有(AKA)手順を改善する。図500における新しいまたは改善されたフィールド(たとえば、図4におけるコールフローと比較して)は、「PFS」プレフィックスでラベル付けされ、図500において下線付きで強調表示される。任意の要素はイタリック体で示される。図500における新しい計算手順(たとえば、段階)は、それぞれのプロセスボックスに示される。

【００３８】

UE 202は、PFS NASアタッチ要求510をMME 206に送信するように構成され得る。PFS NASアタッチ要求510は、識別情報(たとえば、IMSI)を含み、任意でUE PFS情報要素(IE)も含

み得る。UE PFS IEは、UE 202がPFS特性を有するAKAを処理することができることを示すためのブールデータビット、または任意のデータタイプであり得る。しかしながら、PFS特性を有するAKAを処理するUEの能力は、他の方法で(たとえば、他のメッセージ交換に存在する情報要素を介して)確立され得るため、UE PFS IEは任意である。MME 206は、要求を受信すると、ホームネットワーク504(たとえば、HSS 208)に認証ベクトルを要求するように構成される。MME 206は、UEセキュリティ情報(たとえば、IMSI)、ネットワークタイプ(たとえば、E-UTRAN)を示すデータフィールド、およびネットワーク502がPFS特性(たとえば、MME(SN)PFS情報要素)をサポートするという指示を含むPFS認証情報要求メッセージ512を生成する。PFS認証情報要求メッセージ512は、典型的には、情報要素として属性値ペア(AVP)を有する直径プロトコルメッセージである。MME(SN)PFS情報要素は、ブール値または他のデータ値であってもよく、ネットワーク502がPFS特性をサポートすることを示すために使用される。この指示は、中間者(MiM)攻撃を防止することを助けるために使用され得る。すなわち、PFS NASアタッチ要求510を傍受する悪意のある局は、MME(SN)PFS情報要素なしのPFS NASアタッチ要求メッセージをホームネットワーク504に単に転送し、UEにPFS特性なしのAKAプロトコルを使用させようとすることはできない。

【００３９】

HSS 208は、PFS認証情報要求メッセージ512を受信し、ネットワーク502がPFS特性をサポートするかどうかを決定するように構成される。PFSがサポートされている場合、段階526で、HSS 208は、認証トークン(AUTN)を生成するように構成される。この場合、認証トークン(AUTN)内の認証管理フィールド(AMF)内のフィールドは、ネットワーク502がPFS特性をサポートしていることを示すように設定される(たとえば、ブールビットが1に設定される)。これは、PFSビットと呼ばれ得る。ネットワーク502がPFS特性をサポートしない場合、PFSビットは、PFSがサポートされていないことを示すための値に設定され、標準的なAKAプロトコルが使用される(たとえば、ブールビットが0に設定される)。HSS 208は、認証ベクトル(AV)を含むPFS認証情報応答メッセージ514を生成する。PFS認証情報応答メッセージ514内のAVは、上述したPFSビット、(AUTN)、期待応答(XRES)値、乱数(RAND)値、および鍵アクセスセキュリティ管理エンティティ(K_{ASME})値を有する認証トークンを含む。

【００４０】

UE 202およびMME 206は、それぞれ段階521および段階524において、公開および秘密一時的Diffie-Hellman(DHE)鍵のそれぞれのペアを生成するように構成される。Diffie-Hellmanペアは、たとえば、楕円曲線暗号または有限体算術を使用して生成され得る。限定ではなく一例として、DHEのペアは、1977年9月6日に出願された、米国特許第4,200,770号「Cryptographic Apparatus and Method」に記載されているものであり得る。UE 202は、UE秘密鍵値($DHEpriKey_{UE}$)およびUE公開鍵値($DHEpubKey_{UE}$)を生成するように構成される。MME 206は、MME秘密鍵値($DHEpriKey_{MME}$)およびMME公開鍵値($DHEpubKey_{MME}$)を生成するように構成される。秘密鍵($DHEpriKey_{UE}$、$DHEpriKey_{MME}$)は、一般に、暗号的に安全な擬似乱数発生器(CSPRNG)を使用して生成されるが、それぞれのシステムにとって利用可能な他の機密(および、好ましくは非決定論的)情報が使用され得る。対応する公開鍵もそれぞれのシステムによって生成される。DHE鍵のペアは、潜在的なネットワーク攻撃(たとえば、DHE鍵の生成による処理遅延)の影響を低減するために、UE 202およびMME 206によって事前に選択され、生成(たとえば、事前計算)され得る。UEは、段階521の前の任意の時点にそのDHEペアを生成することができ、MMEは、段階530の前の任意の時点に、または段階530において、そのDHEペアを生成し得る点に留意されたい。

【００４１】

UE 202およびMME 206は、AKA認証手順中にそれらの公開鍵を交換するように構成され、それぞれが共有鍵(たとえばsharedDHEkey)を導出する。たとえば、MME 206は、HSS 208から受信したAUTNおよびRAND値、ならびに受信したK_{ASME}値に基づくNASキーセット識別子(KSI_{ASME})を含む、PFS NAS認証要求メッセージ516を生成する。段階528において、UE 202がPFS特性を処理することができる場合、UE 202は、AUTN値におけるPFSビットが、PFS特性がサポートされていることを示すかどうかを決定するように構成される。UE 202がPFS特

性をサポートするように構成されていない場合、メッセージ交換は標準的なAKA手順(たとえば、UEが、図4に記載されたNAS認証応答メッセージ418を送信する)の下で継続することができる。UE 202はまた、前述のように、AUTN値が新鮮であるかどうかを決定するように構成される。AUTN値が受け入れられ、PFSビットが設定されている場合、UE 202はRES値を計算し、RES値およびUE公開鍵値(すなわち$DHEpubKey_{UE}$)を含むPFS NAS認証応答メッセージ518をMME 206に提供する。AUTN値が受け入れられるが、PFSビットが設定されていない(たとえば、0の値)場合、UE 202は、PFS特性をサポートしないネットワークとの接続手順を中止することを決定してもよく、標準的なAKA手順に従ってRESを計算して送信してもよい(たとえば、UEが、図4に記載されたNAS認証応答メッセージ418を送信する)。AUTN検証が失敗した場合、UE 202は、失敗の理由を示すCAUSE値とともに認証失敗メッセージをMME 206に送信する。

【００４２】

PFS NAS認証応答メッセージ518を受信すると、段階530において、MME 206は、RES値がXRES値と等しいかどうかを決定し、受信したUE公開鍵(すなわち、$DHEpubKey_{UE}$)に基づいてDiffie-Hellman共有鍵(すなわちsharedDHEkey)を導出するように構成される。UEの認証に失敗した場合(すなわち、RES値がXRESに等しくない場合)、ネットワークはアタッチ要求を拒絶し得、高価な非対称暗号動作を実行する際に計算リソースが無駄にされることはないことが理解されるべきである。これは、悪意のあるUEによる、あらゆるサービス拒否攻撃の軽減に役立つ。次いで、共有鍵は、HSS 208から受信されたK_{ASME}値(たとえば、セッション鍵)に結合され、結合された鍵は、後続のすべてのNASトラフィックを保護するために使用される。たとえば、結合された鍵は、K'_{ASME}(たとえば、K_{ASME}-prime)として指定されてもよく、K_{ASME}の鍵導出関数(KDF)および共有鍵に基づいて生成されてもよい。すなわち、K'_{ASME}=KDF(K_{ASME}、sharedDHEkey)である。KDFは、暗号化ハッシュ関数(たとえば、SHA256、SHA512、SHA3など)であり得る。結果として得られたK'_{ASME}値は、後続のLTEセキュリティ手順においてK_{ASME}値として使用され得る。

【００４３】

MME 206はまた、MME公開鍵(すなわち、$DHEpubKey_{MME}$)、ならびに機密性および完全性アルゴリズムを含むPFS NAS SMCメッセージ520を送信する。たとえば、PFS NAS SMCメッセージ520は、再生されたUEセキュリティ能力、選択されたNASアルゴリズム、K_{ASME}を識別するためのKSI_{ASME}値、およびアイドルモビリティにおいてマッピングされたコンテキストを作成する場合の$NONCE_{UE}$および$NONCE_{MME}$値の両方を含み得る。PFS NAS SMCメッセージ520は、メッセージ内のKSI_{ASME}値によって示されるK_{ASME}に基づいて、NAS完全性鍵を用いて完全性保護され得る(しかし、暗号化されない)。UE 202は、PFS NAS SMCメッセージ520の完全性を検証するように構成される。これは、これらが攻撃者によって修正されなかったことを保証するために、MMEによって送信されたUEセキュリティ機能がUEに記憶されたものと一致することを保証することと、KSI_{ASME}値によって示されるK_{ASME}に基づいて、示されたNAS完全性アルゴリズムおよびNAS完全性鍵を使用して完全性保護をチェックすることとを含み得る。段階532において、UE 202は、MME公開鍵(たとえば$DHEpubKey_{MME}$)に基づいてDiffie-Hellman共有鍵(たとえば、sharedDHEkey)を導出するように構成される。次いで、sharedDHEkeyは、上述のようなK'_{ASME}を作成するために、K_{ASME}値に結合される(たとえば、KSI_{ASME}値によって識別されるように)。結果として得られたK'_{ASME}値は、後続のすべてのLTEセキュリティ手順においてK_{ASME}値として使用され得る。

【００４４】

PFS NAS SMCメッセージ520に基づくチェックがパスすると(すなわち、MMEによって送信されたUEセキュリティ能力がUEに記憶されたものと一致し、完全性保護が、KSI_{ASME}値によって示されるK_{ASME}に基づいて、示されたNAS完全性アルゴリズムおよびNAS完全性鍵を使用する)、UE 202は、PFS NASセキュリティモード完了メッセージ522で応答するように構成される。UE 202は、K'_{ASME}に基づいてNAS完全性保護および暗号化/解読を実行し、(たとえば、K'_{ASME}に基づいて)暗号化および完全性保護されたMME 206にPFS NASセキュリティモード完了メッセージ522を送信するように構成される。MME 206は、K'_{ASME}に基づく

鍵、およびPFS NAS SMCメッセージ520において示される他のアルゴリズムを使用して、PFS NASセキュリティモード完了メッセージ522に対する完全性保護を解読し、チェックするように構成される。

【００４５】

さらに図2、図4、および図5を参照して、図6を参照すると、完全前方秘匿性(PFS)を有する別の例示的な認証手順のコールフロー図600が示されている。図600は、通信システム200によって使用され得る代替のセキュリティ手順を表し、したがって、図600は、UE 202(たとえば、モバイルデバイス100)、ネットワーク602、およびホームネットワーク604を含む。ネットワーク602は、eNodeB(eNB) 204およびMME 206を含み得る。ホームネットワーク604は、PFS特性を有するAKAをサポートすると想定されるHSS 208を少なくとも含む。コールフロー図600は、完全前方秘匿性(PFS)特性を追加することによって、図4で説明した認証および鍵共有(AKA)手順を改善する。図600はまた、図5において前述されたメッセージのうちのいくつかを含む。たとえば、UE 202は、PFS NASアタッチ要求510をMME 206に送信するように構成され得る。MME 206は、要求を受信すると、ホームネットワーク604(たとえば、HSS 208)に認証ベクトルを要求するように構成される。MME 206は、PFS認証情報要求メッセージ512(たとえば、MME(SN)PFS情報要素を含む)を生成し、それをホームネットワーク604に提供する。ホームネットワーク604(たとえば、HSS 208)は、PFS認証情報要求メッセージ512を受信し、ネットワーク602がPFS特性をサポートするかどうかを決定するように構成される。PFSがサポートされている場合、段階526で、HSS 208は、図5において説明したPFSビットを含む認証トークン(AUTN)を生成するように構成される。ネットワーク602がPFS特性をサポートしない場合、PFSビットは、PFSがサポートされておらず、標準的なAKAプロトコルが使用されることを示すための値に設定される(たとえば、ブールビットが0に設定される)。HSS 208は、認証ベクトル(AV)を含むPFS認証情報応答メッセージ514を生成する。PFS認証情報応答メッセージ514内のAVは、上述したPFSビット、(AUTN)、期待応答(XRES)値、乱数(RAND)値、および鍵アクセスセキュリティ管理エンティティ(K_{ASME})値を有する認証トークンを含む。

【００４６】

UE 202およびMME 206は、それぞれ段階521および段階524において、公開および秘密一時的Diffie-Hellman(DHE)鍵のそれぞれのペアを生成するように構成される。UE 202は、UE秘密鍵値($DHEpriKey_{UE}$)およびUE公開鍵値($DHEpubKey_{UE}$)を生成するように構成される。MME 206は、MME秘密鍵値($DHEpriKey_{MME}$)およびMME公開鍵値($DHEpubKey_{MME}$)を生成するように構成される。秘密鍵($DHEpriKey_{UE}$、$DHEpriKey_{MME}$)は、一般に、暗号的に安全な擬似乱数発生器(CSPRNG)を使用して生成されるが、それぞれのシステムにとって利用可能な他の機密情報が使用され得る。対応する公開鍵は、それぞれのシステムによって同様の非決定論的な方法で生成され得る。DHE鍵のペアは、潜在的なネットワーク攻撃(たとえば、DHE鍵の生成による処理遅延)の影響を低減するために、UE 202およびMME 206によって事前に選択され、生成(たとえば、事前計算)され得る。MMEは、段階524の前の任意の時点にそのDHEペアを生成することができ、UEは、段階521の前の任意の時点にそのDHEペアを生成し得る点に留意されたい。

【００４７】

UE 202およびMME 206は、AKA認証手順中にそれらの公開鍵を交換するように構成され、それぞれが共有鍵(たとえばsharedDHEkey)を導出する。図5におけるPFS NAS認証要求メッセージ516とは対照的に、図6におけるコールフローでは、MME 206は、HSS 208から受信したAUTNおよびRAND値、受信したK_{ASME}値に基づくNASキーセット識別子(KSI_{ASME})、ならびにMME公開鍵(すなわち$DHEpubKey_{MME}$)を含むPFS NAS認証要求メッセージ616を生成する。段階628において、UE 202は、AUTN値におけるPFSビットが、PFS特性がサポートされていることを示すかどうかを決定し、PFS NAS認証要求メッセージ616内にMME公開鍵(すなわち、$DHEpubKey_{MME}$)が存在するかどうかを決定するように構成される。

【００４８】

UE 202はまた、前述のように、AUTN値が新鮮であるかどうかを決定するように構成され

る。AUTN値が受け入れられ、PFSビットが設定されている場合、次いでMME公開鍵(すなわち、$DHEpubKey_{MME}$)が存在する場合、UE 202はRES値を計算し、RES値およびUE公開鍵値(すなわち、$DHEpubKey_{UE}$)を含むPFS NAS認証応答メッセージ518をMME 206に提供する。AUTN値が受け入れられるが、PFSビットが設定されておらず(たとえば、0の値)、またMME公開鍵(すなわち、$DHEpubKey_{MME}$)が存在しない場合、UE 202は、PFS特性をサポートしないネットワークとの接続手順を中止することを決定してもよく、標準的なAKA手順に従ってRESを計算して送信してもよい(たとえば、UEが、図4に記載されたNAS認証応答メッセージ418を送信する)。UE 202は、PFSビットが設定されているが、MME公開鍵(すなわち、$DHEpubKey_{MME}$)が存在しない場合、またはAUTN検証が失敗した場合(たとえば、PFS値およびMME公開鍵の存在に関係なく)、UE 202は、認証失敗メッセージをMME 206に送信する。一例では、失敗メッセージは、失敗の理由を示すCAUSE値を含み得る。

【００４９】

段階530において、MME 206は、RES値がXRES値と等しいかどうかを決定し、次いで、受信したUE公開鍵(すなわち、PFS NAS認証応答メッセージ518における$DHEpubKey_{UE}$)に基づいてDiffie-Hellman共有鍵(すなわち、sharedDHEkey)を導出するように構成される。次いで、共有鍵は、HSS 208から受信されたK_{ASME}値に結合され、結合された鍵は、後続のすべてのNASトラフィックを保護するために使用される。たとえば、結合された鍵は、K'_{ASME}(たとえば、K_{ASME}-prime)として指定されてもよく、K_{ASME}の鍵導出関数(KDF)および共有鍵に基づいて生成されてもよい。すなわち、$K'_{ASME}=KDF(K_{ASME}$、sharedDHEkey)である。KDFは、暗号化ハッシュ関数(たとえば、SHA256、SHA512、SHA3など)であり得る。結果として得られたK'_{ASME}値は、LTEネットワークにおけるK_{ASME}値として使用され得る。段階632において、UE 202は、MME公開鍵(たとえば$DHEpubKey_{MME}$)に基づいてDiffie-Hellman共有鍵(たとえば、sharedDHEkey)を導出するように構成される。次いで、sharedDHEkeyは、上述のようなK'_{ASME}を作成するために、K_{ASME}値に結合される(たとえば、KSI_{ASME}値によって識別されるように)。結果として得られたK'_{ASME}値は、後続のLTEセキュリティ手順においてK_{ASME}値として使用され得る。

【００５０】

MME 206は機密性および完全性アルゴリズムを含むPFS NAS SMCメッセージ620を送信する。たとえば、PFS NAS SMCメッセージ620は、再生されたUEセキュリティ能力、選択されたNASアルゴリズム、およびアイドルモビリティにおいてマッピングされたコンテキストを作成する場合の$NONCE_{UE}$および$NONCE_{MME}$値の両方を含み得る。一実施形態では、PFS NAS SMCメッセージ620は、段階530において決定されたK'_{ASME}に基づいて、NAS完全性鍵を用いて完全性保護され得る(しかし、暗号化されない)。UE 202は、PFS NAS SMCメッセージ620の完全性を検証するように構成される。これは、これらが攻撃者によって修正されなかったことを保証するために、MMEによって送信されたUEセキュリティ機能がUEに記憶されたものと一致することを保証することと、段階632において導出されるK'_{ASME}に基づいて、示されたNAS完全性アルゴリズムおよびNAS完全性鍵を使用して完全性保護をチェックすることとを含み得る。

【００５１】

PFS NAS SMCメッセージ620に基づくチェックがパスする場合(たとえば、MMEによって送信されたUEセキュリティ能力が、UEに記憶されたものと一致し、完全性保護が、K'_{ASME}に基づいて、示されたNAS完全性アルゴリズムおよびNAS完全性鍵を使用する)、UE 202は、PFS NASセキュリティモード完了メッセージ522で応答するように構成される。UE 202は、K'_{ASME}に基づいてNAS完全性保護および暗号化/解読を実行し、暗号化および完全性保護されたMME 206にPFS NASセキュリティモード完了メッセージ522を送信するように構成される。MME 206は、K'_{ASME}に基づく鍵、およびPFS NAS SMCメッセージ620において示される他のアルゴリズムを使用して、PFS NASセキュリティモード完了メッセージ522に対する完全性保護を解読し、チェックするように構成される。

【００５２】

PFS特性に関連付けられるセキュリティ態様を含めることに加えて、図5および図6にお

いて提供されるコールフローの例は、ビッドダウン攻撃(たとえば、悪意のあるエンティティがメッセージ交換を変更する中間者攻撃)に対する保護を提供する。すなわち、コールフローは、中間者が「PFSを有するAKA」手順から「PFSを有しないAKA」手順にビッドダウンすることを防止する。加入者のホームネットワーク(たとえば、HSS 208)がPFSをサポートする場合、HSSがMME(たとえば、MME(SN)PFS情報要素)から受信した指示を理解していることが示唆され、AKA認証ベクトル(AV)生成の間に認証トークン(AUTN)内のAMFフィールド内のPFSビットを設定することができる。一般に、ネットワーク(たとえば、MME)がPFSをサポートする場合、AV要求の一部として、ホームネットワーク(たとえば、HSS)にそのPFSサポートを示す。この指示は、たとえUEがアタッチ要求においてPFSサポートを示さなくても、HSSに含まれる。HSSは、AUTN内のAMFビット(たとえば、PFSビット)を設定する。AUTNは、HSSとUEとの間で完全性保護される。PFSをサポートするUEは、PFSビットがAUTNに設定されているかどうかをチェックするように構成される。PFSビットが設定されているが、AKAがPFSなしで実行される場合、UEは認証を拒絶する。PFSをサポートしないUEは、ビットチェックを無視し得る。ネットワーク(たとえば、MME)がPFSをサポートしない(すなわち、PFSビットがAVにおいてゼロに設定されている)場合、UEがPFSなしでネットワークとの認証を継続するかどうかを決定するために、UEポリシーが呼び出され得る。

【００５３】

さらに図1～図6を参照して、図7を参照すると、モバイルデバイスとの安全な通信を提供するためのプロセス700は、図示される段階を含む。しかしながら、プロセス700は一例にすぎず、限定的ではない。プロセス700は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって変更され得る。たとえば、UE公開鍵およびUE秘密鍵は、事前に計算され得る。プロセス700は、通信システム200内のUE 202の一例でもあるモバイルデバイス100上で実行することができる。

【００５４】

段階702において、モバイルデバイス100内のプロセッサ111およびワイヤレストランシーバ121は、アタッチ要求を生成するように構成されている。一実施形態では、アタッチ要求はPFSサポートインジケータを含み得る。プロセッサ111およびワイヤレストランシーバ121は、アタッチ要求を生成するための手段である。アタッチ要求は、LTE、LTE-A、HSPA、CDMA、高速パケットデータ(HRPD)、進化型HRPD(eHRPD)、CDMA2000、GSM（登録商標）、GPRS、GSM（登録商標）進化(EDGE)のための強化されたデータレート、UMTSなどの、モバイルデバイス100と通信ネットワークとの間のワイヤレス通信であり得る。通信システムは、ネットワーク内のメッセージフローを保護するために、「PFSを有するAKA」プロトコルを利用することができる。アタッチ要求を生成することは、PFS NASアタッチ要求510を、モバイルデバイスからeNB 204を介してMME 206に送信することであり得る。PFSサポートアタッチ要求は、ブールビット、またはPFS NASアタッチ要求510内の任意のUE PFS情報要素などの任意のデータタイプを任意で含み得る。

【００５５】

段階704において、認証トークンがサービングセルによるPFSサポートの指示を含むように、モバイルデバイス100内のプロセッサ111およびワイヤレストランシーバ121は、認証トークンで認証要求を受信するように構成される。認証トークンの値は、ネットワークサポートインジケータ(たとえば、MME PFS)に少なくとも部分的に基づいている。すなわち、認証トークンは、ネットワークがPFSをサポートしているか否かを示すように構成される。たとえば、ネットワークによるPFSサポートの指示は、PFS認証情報応答メッセージ514内のAUTNフィールドであり得る。認証トークンは、ネットワークがPFS(たとえば、AUTN内のPFSビット)をサポートするという指示としてデータフィールド(たとえば、ビット、バイト)を含み得る。

【００５６】

段階706において、モバイルデバイス100内のプロセッサ111は、ネットワークが完全前方秘匿性(PFS)をサポートするかどうかを決定するように構成される。段階704において受信された認証トークンは、ネットワークがPFSをサポートするか否かを示すためにPFSビッ

ト(たとえば、AMFビット)を含み得る。ネットワークがPFSをサポートしていない(すなわち、PFSビットがゼロに等しい)場合、段階716において、モバイルデバイス100は、UE公開鍵値なしで認証応答を提供するように構成される。たとえば、図4を参照すると、認証応答は、NAS認証応答メッセージ418であり得る。段階718において、モバイルデバイス100は、図4に示されるような標準的なAKA認証手順を実行するように構成される。

【００５７】

モバイルデバイス100が、ネットワークがPFSをサポートしている(たとえば、AUTN内のPFSビットが1に等しい)とモバイルデバイス100が決定した場合、段階708において、モバイルデバイス100内のプロセッサ111がUE公開鍵値をネットワークに提供する(たとえば、認証応答において)ように構成される。プロセッサ111およびワイヤレストランシーバ121は、UE公開鍵値をネットワークに提供するための手段である。たとえば、プロセッサ111は、UE公開鍵値およびUE秘密鍵値を生成するように構成される。公開鍵および秘密鍵はDiffie-Hellmanペアとして生成される。プロセッサ111は、UE秘密鍵および公開鍵を生成するための手段である。プロセッサ111は、UE秘密鍵値として暗号的に安全な擬似乱数発生器(CSPRNG)を生成するように構成され得る。UE公開鍵値もまた、プロセッサ111によって非決定論的な方法で生成される。UE秘密鍵値および公開鍵値は、プロセス700の実行に先立って生成され、モバイルデバイス上のメモリに記憶され、必要に応じて取り出される。図5におけるLTEの例においては、モバイルデバイス100は、RES値およびUE公開鍵値(すなわち、$DHEpubKey_{UE}$)を含む、PFS NAS認証応答メッセージ518をMME 206に提供し得る。

【００５８】

段階710において、ワイヤレストランシーバ121およびモバイルデバイス内のプロセッサ111は、ネットワーク公開鍵値をネットワークから受信するように構成される。たとえば、モバイルデバイス100は、(たとえば、MME 206からeNB 204を介して)ネットワーク502からPFS NAS SMCメッセージ520を受信するように構成され得る。PFS NAS SMCメッセージ520は、ネットワーク公開鍵(たとえば$DHEpubKey_{MME}$)、ならびに機密性および完全性アルゴリズムを含み得る。

【００５９】

段階712において、モバイルデバイス100内のプロセッサ111は、ネットワーク公開鍵値およびUE秘密鍵値に基づいて共有鍵値を決定するように構成される。たとえば、プロセッサ111は、受信したネットワーク公開鍵値(すなわち、$DHEpubKey_{MME}$)および以前に生成されたUE秘密鍵値($DHEpriKey_{UE}$)に基づいて、Diffie-Hellman共有鍵(すなわちsharedDHEkey)を導出するように構成される。

【００６０】

段階714において、モバイルデバイス100内のプロセッサ111は、共有鍵値をセッション鍵値と結合し、後続のネットワークトラフィックを保護するために結合された共有鍵値を使用するように構成される。共有鍵値をセッション鍵値と結合することは、共有鍵値とセッション鍵値との連結(たとえば、SHA256(共有鍵、ルート鍵))に対して暗号ハッシュを実行することを含み得る。図5を参照すると、共有鍵値(すなわち、sharedDHEkey)がK_{ASME}値に結合されている。結果として得られた結合された共有鍵値はK'_{ASME}として指定され、K_{ASME}の鍵導出関数(KDF)および共有鍵に基づいて生成され得る。すなわち、$K'_{ASME}=KDF(K_{ASME}$、sharedDHEkey)である。KDFは、暗号化ハッシュ関数(たとえば、SHA256、SHA512、SHA3など)であり得る。結果として得られたK'_{ASME}値(すなわち、結合された共有鍵値)は、LTEネットワークにおけるK_{ASME}値として使用され得る。すなわち、後続のネットワークトラフィックを保護するために、結合されたセッション鍵が使用される。

【００６１】

さらに図1～図6を参照して、図8を参照すると、ネットワークサーバとの安全な通信を提供するためのプロセス800は、図示される段階を含む。しかしながら、プロセス800は一例にすぎず、限定的ではない。プロセス800は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって変更され得る。たとえば、ネットワーク公開鍵値および秘密鍵値は、あらかじめ計算され、メモリに記憶され、プロセス800に

よって必要に応じて取り出され得る。プロセス800は、通信システム200内のMME 206の一例でもあるコンピュータシステム300上で実行することができる。

【００６２】

段階802において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、UEからアタッチ要求を受信するように構成される。一例では、アタッチ要求は、任意のPFSサポートインジケータを含み得る。ネットワーク502は、アタッチ要求を受信するための手段としてコンピュータシステム300を含み得る。図5おけるLTEの例においては、ネットワーク502は、UE 202からPFS NASアタッチ要求510を受信する。PFS NASアタッチ要求は、識別情報(たとえば、IMSI)を含み、任意でUE PFS情報要素(IE)を含み得る。任意のUE PFS IEは、UE 202がPFS特性をサポートすることを示すように構成されたデータフィールド(たとえば、ブールビットまたは他の文字)である。PFS NASアタッチ要求510は、UE 202からMME 206に送信される。

【００６３】

段階804において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、ネットワークサポートインジケータを含む認証要求をネットワークリソースに提供するように構成される。標準的なAKA手順は、ホームネットワーク(たとえば、HSS)から認証ベクトルを要求するためにネットワーク(たとえば、MME)を必要とする。AKAプロトコルへのPFSの追加は、通信システム200上のセキュリティの強さを改善する。UEのホームネットワークがPFSをサポートしていると想定される。しかしながら、潜在的に多くの異なるネットワークがUEにとって利用可能であるので、UEが、PFSをサポートしないネットワークにアタッチすることが可能である。したがって、中間者は、要求された「PSFを有するAKA」プロトコルを「PSFを有しないAKA」プロトコルにビッドダウンしようと試みることも可能である。プロセス800は、ネットワークに、ホームネットワークへのPFSをサポートする能力を示すように要求することによって、このリスクを排除することができる。LTEの例においては、この指示は、ネットワークがPFS特性(たとえば、MME(SN)PFS情報要素)をサポートするという指示として、PFS認証情報要求メッセージ512に含まれる。認証要求は、典型的には、情報要素として属性値ペア(AVP)を有する直径プロトコルメッセージであるが、他のネットワークにおいては、ネットワークがPFS特性をサポートすることを示すために他のデータ値またはタイプが使用され得る。

【００６４】

段階808において、通信サブシステム330およびプロセッサ310は、認証トークンが、ネットワークがPFSをサポートするという指示を含むように、ネットワークリソースから認証トークンを受信するように構成される。段階804において提供された認証要求を受信することに応答して、ネットワークリソースは1つまたは複数の認証ベクトルで応答することができる。認証ベクトルは、ネットワークリソースとUEとの間で完全性保護された認証トークンを含む。認証トークンの値は、ネットワークサポートインジケータに少なくとも部分的に基づいている。すなわち、認証トークンは、ネットワーク(たとえば、段階804において認証要求を提供したネットワーク)がPFSをサポートしているか否かを示すように構成される。たとえば、認証トークンは、PFS認証情報応答メッセージ514内のAUTNフィールドであり得る。認証トークンは、ネットワークがPFS(たとえば、AUTN内のPFSビット)をサポートするという指示としてデータフィールド(たとえば、ビット、バイト)を含み得る。

【００６５】

段階810において、通信サブシステム330およびプロセッサ310は、認証トークンをUEに提供するように構成される。LTEの例においては、認証トークンは、RAT(たとえば、eNB 204)を介して提供され、PFS NAS認証要求メッセージ516、616のうちの1つ(すなわち、AUTN値)に含まれ得る。段階812において、ネットワークは、UE公開鍵値を含む認証応答を受信するように構成される。コンピュータ300内の通信サブシステム330は、認証応答を受信するための手段である。たとえば、認証応答は、RES値およびUE公開鍵値(すなわち、DHEpub Key_{UE})を含むPFS NAS認証応答メッセージ518であり得る。

【００６６】

段階814において、プロセッサ310は、段階812において受信された認証応答が期待応答であるかどうかを決定するように構成される。期待応答は、たとえば、応答値(たとえば、RES)が以前に記憶された期待応答値(たとえば、XRES)と等しいものである。LTEの例においては、RES値はPFS NAS認証応答メッセージ518に含まれ、XRES値はネットワークリソースから受信した認証ベクトルに含まれていた。プロセッサ310は、2つの値に対して論理比較演算を実行するように構成される。2つの値が一致しない場合、段階818においてUEのアタッチ要求が拒否される。

【００６７】

段階806において、コンピュータシステム300内のプロセッサ310は、ネットワーク公開鍵値およびネットワーク秘密鍵値を生成するように構成される。ネットワーク公開鍵および秘密鍵の値は、楕円曲線暗号を使用して生成されるDiffie-Hellmanペアであり得る。他の非決定論的な方法(たとえば、CSPRNGの結果)もまた、鍵を生成するために使用され得る。鍵の集まりは、プロセス800の実行前にあらかじめ生成され、メモリに記憶され得る。鍵のペアは、プロセス800によって必要に応じてメモリから取り出され得る。

【００６８】

段階816において、プロセッサ310は、ネットワーク秘密鍵値およびUE公開鍵値に基づいて共有鍵値を決定するように構成される。共有鍵値は、段階812において受信した、受信したUE公開鍵(すなわち、$DHEpubKey_{UE}$)、および段階806において生成したネットワーク秘密鍵に基づくDiffie-Hellman共有鍵(すなわちsharedDHEkey)である。

【００６９】

段階820において、プロセッサ310は、共有鍵値をセッション鍵値と結合するように構成され、後続のネットワークトラフィックを保護するために結合された共有鍵値が使用される。一般に、セッション鍵値は、UEとネットワークリソースとの間で共有される対称ルート鍵から導出される。AKA手順におけるセッション鍵の例は、K_{ASME}鍵値である。共有鍵値は、鍵導出関数(KDF)を介してセッション鍵値(たとえば、K_{ASME})に結合され得る。KDFは、暗号化ハッシュ関数(たとえば、SHA256、SHA512、SHA3など)であり得る。他の結合アルゴリズムも使用され得る。図5において説明されるLTEの例においては、結合された共有鍵はK'_{ASME}であり、これはKDF関数(たとえば、$K'_{ASME}=KDF(K_{ASME}$、sharedDHEkey))で生成される。結果として得られたK'_{ASME}値は、LTEネットワークにおける後続のトラフィックを保護するためにK_{ASME}値として使用され得る。

【００７０】

さらに図1～図6を参照して、図9を参照すると、強力なセキュリティプロトコルを有するシステムに対するビッドダウン攻撃を防止するためのプロセス900は、図示される段階を含む。しかしながら、プロセス900は一例にすぎず、限定的ではない。プロセス900は、たとえば、段階を追加、除去、再配置、結合、および/または同時に実行することによって変更され得る。プロセス900は、ネットワーク502内に含まれるコンピュータシステム300上で実行することができる。

【００７１】

段階902において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、ユーザ機器からアタッチ要求を受信するように構成される。ある例においては、強力なセキュリティプロトコルがPFS特性をサポートする。したがって、相対比較においては、PFSをサポートするAKA手順は、PFSをサポートしないAKA手順よりも強力である。LTEの例においては、UE 202は、PFS NASアタッチ要求510をコンピュータシステム300に送信するように構成される。

【００７２】

段階904において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、認証要求が、ネットワークが強力なセキュリティプロトコルをサポートするという指示を含むように、ホームネットワークに認証要求を送信するように構成される。一例では、コンピュータシステム300は、ホームネットワークに認証ベクトルを要求し、ユーザ機器に関連付けられるセキュリティ情報(たとえば、IMSI)を含む認証要求と、ネット

ワークタイプ(たとえば、E-UTRAN)を示すデータフィールドと、ネットワークが強力なセキュリティプロトコルをサポートするという指示とを生成するように構成される。PFS認証情報要求メッセージ512は、段階904において送信された認証要求の一例である。対応するMME(SN)PFS情報要素は、ネットワークが強力なセキュリティプロトコル(たとえば、PFSを有するAKA)をサポートするという指示の一例である。認証要求は、中間者(MiM)がPFSを有するAKAを標準的なAKAプロトコルにビッドダウンするのを防止するために役立つ。一例においては、段階902において受信されたアタッチ要求を傍受する可能性のあるMiM(たとえば、局)は、結果として得られる転送されるメッセージが、ネットワークが強力なセキュリティプロトコル(たとえば、PFSを有するAKA)をサポートしているという指示を含まないので、そのアタッチ要求をホームネットワークに単に転送することはできない。

【００７３】

段階906において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、完全性保護されたトークンが、ネットワークが強力なセキュリティプロトコルをサポートすることを示すように構成された少なくとも1つのビットを含むように、ホームネットワークから完全性保護されたトークンを受信するように構成される。完全性保護されたトークンは、ユーザ機器とホームネットワークとの間の完全性保護を提供する。LTEの例においては、認証トークンAUTNは完全性保護されたトークンである。AUTNにおいて、認証管理フィールド(AMF)内のフィールドは、ネットワークがPFS特性をサポートすることを示すように設定され得る(たとえば、ブールビットが1に設定される)。AUTN内のPFSビットは、ネットワークが強力なセキュリティプロトコルをサポートしていることを示すように構成された少なくとも1つのビットの一例である。たとえば、ネットワークが強力なセキュリティプロトコルをサポートする場合、PFSビットは、強力なセキュリティプロトコルがサポートされていることを示すための値に設定され得る(たとえば、PFSビットが1に設定される)。逆に、強力なセキュリティプロトコルがネットワークによってサポートされていない場合、PFSビットはゼロに設定され得る。

【００７４】

段階908において、コンピュータシステム300内の通信サブシステム330およびプロセッサ310は、完全性保護されたトークンをユーザ機器に送信するように構成される。ユーザ機器は、ネットワークが強力なセキュリティプロトコルをサポートしているかどうかを決定するために、完全性保護されたトークンから少なくとも1つのビットを解析するように構成され得る。図5において説明されるLTEの例においては、ユーザ機器は、AUTN値のPFSビットが、PFS特性がサポートされていることを示すかどうかを決定するように構成され得る。PFSビットが設定されている場合(および、他の認証値が有効である場合)、ユーザ機器はDiffie-Hellman公開鍵をネットワークに提供する。公開鍵は、比較的弱いセキュリティプロトコル(たとえば、PFSを有しないAKA)に必要とされない強力なセキュリティプロトコルの構成要素である。完全性保護されたトークン内のPFSビットが設定されていない場合(たとえば、0の値)、ユーザ機器は、より弱いセキュリティプロトコルに従って応答するように構成され得る。完全性保護されたトークンは、ユーザ機器とホームネットワークとの間の保護を提供するので、強力なセキュリティプロトコルは、中間者が完全性保護されたトークンの値を変更することができないため、弱いセキュリティプロトコルにビッドダウンすることができない。

【００７５】

PFS特性を有する認証手順は、図5および図6に示されるコールフローに限定されない。たとえば、モビリティシナリオにおいては、UEは、PFS NASアタッチ要求510の代わりに、サービス要求または位置エリア更新またはトラッキングエリア更新(TAU)要求メッセージを開始することができる。UEは、そのPFSサポートをこれらのメッセージ内で(たとえば、UE PFS IEを含むことによって)任意で示すことができる。したがって、MMEが変更した場合、またはMMEが新しいAKAを開始することを決定した場合、必要に応じてPFS特性を有する新しいAKAが実行され得る。さらに、PFS特性は、アクセス層(AS)セキュリティに実装され得る。K_{ASME}(および他のNASセキュリティ鍵)と同様に、eNBとUEとの間のPFS特性を有す

るASセキュリティ鍵を設定するために、上述の一時的DHE方法が使用され得る。K_{eNB}および他のASセキュリティ鍵は、K_{eNB}とUEとの間で導出されたsharedDHEkeyに結合され得る。たとえば、eNB 204およびUE 202は、それぞれのDiffie-Hellman公開鍵を交換し、PFS特性を有するASセキュリティ鍵を設定するために、RRCメッセージ交換(たとえばRRCConnectionSetupCompleteおよびRRCセキュリティモードコマンド)を使用してDHE公開鍵を交換することができる。このPFS特性の実装形態は、ASセキュリティ鍵を導出するために使用されるNASレベル鍵(たとえば、K_{ASME})が将来漏洩された場合、UEとeNBとの間の過去のオーバージエア(OTA)トラフィックの機密性が損なわれることを防止する。これは、UEがアイドルモードとアクティブモードとの間で遷移するとき、またはアイドルモードモビリティの間にUEが異なるeNBに移動するときに起こり得る。

【００７６】

特定の要望に応じて、大幅な変更が行われ得る。たとえば、カスタマイズされたハードウェアが使用される場合もあり、ならびに/あるいは、特定の要素が、ハードウェア、ソフトウェア(アプレットなどのポータブルソフトウェアを含む)、またはその両方で実現される場合がある。さらに、ネットワーク入力/出力デバイスなどの他のコンピューティングデバイスへの接続が利用される場合がある。

【００７７】

本開示による方法を実行するために、(コンピュータシステム300などの)コンピュータシステムが使用される場合がある。そのような方法の手順のうちのいくつか、または全部は、プロセッサ310が、ワーキングメモリ335に含まれる1つまたは複数の命令(オペレーティングシステム340および/またはアプリケーションプログラム345などの他のコードに組み込まれていてもよい)の1つまたは複数のシーケンスを実行することに応じてコンピュータシステム300によって実行され得る。そのような命令は、ストレージデバイス325のうちの1つまたは複数などの別のコンピュータ可読媒体からワーキングメモリ335に読み込まれ得る。単なる例として、ワーキングメモリ335に含まれる命令のシーケンスの実行は、プロセッサ310に、本明細書で説明する方法の1つまたは複数の手順を実行させる場合がある。

【００７８】

本明細書で使用される「機械可読媒体」および「コンピュータ可読媒体」という用語は、機械を特定の様式で動作させるデータを提供することに関与する任意の媒体を指す。モバイルデバイス100および/またはコンピュータシステム300を使用して実施される実施形態では、実行のためにプロセッサ111、310に命令/コードを提供することに様々なコンピュータ可読媒体が関与している可能性があり、ならびに/あるいは、そのような命令/コードを(たとえば、信号として)記憶および/または搬送するために使用されている可能性がある。多くの実施形態では、コンピュータ可読媒体は、物理的および/または有形の記憶媒体である。そのような媒体は、不揮発性媒体、揮発性媒体、および送信媒体を含む多くの形態をとることができるが、これらに限定されない。不揮発性媒体は、たとえば、ストレージデバイス140、325などの光ディスクおよび/または磁気ディスクを含む。揮発性媒体は、ワーキングメモリ140、335などの動的メモリを含むが、これに限定されない。送信媒体には、バス101、305を構成するワイヤ、ならびに通信サブシステム330の様々な構成要素(および/または、通信サブシステム330が他のデバイスとの通信を提供する媒体)を含む、同軸ケーブル、銅線および光ファイバを含むが、これに限定されない。したがって、送信媒体はまた、電波(電波および赤外線データ通信中に生成されるものなどの、無線、音響および/または光波を含むが、これに限定されない)の形態をとることができる。

【００７９】

物理的および/または有形のコンピュータ可読媒体の一般的な形態は、たとえば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープ、または他の任意の磁気媒体、CD-ROM、ブルーレイディスク、または他の任意の光媒体、パンチカード、紙テープ、孔のパターンを有する他の任意の物理的媒体、RAM、PROM、EPROM、フラッシュEPROM、他の任意のメモリチップまたはカートリッジ、後述する搬送波、あるいはコンピュ

ータが命令および/またはコードを読み取ることができる他の任意の媒体を含む。

【００８０】

様々な形態のコンピュータ可読媒体が、実行のために1つまたは複数の命令の1つまたは複数のシーケンスをプロセッサ111、310に搬送することに関与することができる。単なる例として、命令は、最初に、リモートコンピュータの磁気ディスクおよび/または光ディスク上で搬送され得る。リモートコンピュータは、命令をその動的メモリにロードし、その命令を、モバイルデバイス100および/またはコンピュータシステム300によって受信および/または実行される送信媒体を介して信号として送信することができる。電磁信号、音響信号、光信号等の形態であってもよいこれらの信号はすべて、本発明の様々な実施形態に従って命令が符号化され得る搬送波の例である。

【００８１】

上述の方法、システム、およびデバイスは、例である。様々な代替的な構成は、様々な手順または構成要素を適宜、省略、置換、または追加することができる。たとえば、代替方法では、段階は上記の説明とは異なる順番で実行されてよく、様々な段階が追加、省略、または組み合わされてよい。また、いくつかの構成に関して記載された特徴は、様々な他の構成内に組み合わされてよい。構成の様々な態様および要素は、同様の方法で組み合わされてよい。また、技術は徐々に発達しており、したがって、要素の多くは、例であり、本開示または特許請求の範囲を限定しない。

【００８２】

例示的な構成(実装形態を含む)の完全な理解を提供するために、本明細書において具体的な詳細が与えられる。しかしながら、構成は、これらの具体的な詳細なしに実践される場合がある。たとえば、よく知られている回路、プロセス、アルゴリズム、構造、および技法が、構成を不明瞭にすることを避けるために不必要な詳細なしに示されている。この説明は、例示的な構成のみを提供し、特許請求の範囲の範囲、適用可能性、または構成を限定しない。むしろ、構成の前述の説明は、説明された技法を実装するための実施可能要件(enabling description)を当業者に提供する。本開示の趣旨または範囲から逸脱することなしに、要素の機能および配置に様々な変更を加えることができる。

【００８３】

構成は、フロー図またはブロック図として描写されるプロセスとして記載されてよい。各々は動作について順次のプロセスとして説明する場合があるが、動作の多くは、並列に、または同時に実行することができる。さらに、動作の順序は、並べ替えられる場合がある。プロセスは、図に含まれていない追加のステップを有してもよい。さらに、方法の例は、ハードウェア、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、またはそれらの任意の組合せによって実装される場合がある。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコードで実装されるとき、必要なタスクを実行するプログラムコードまたはコードセグメントは、記憶媒体などの非一時的コンピュータ可読媒体に記憶される場合がある。プロセッサは、記述されたタスクを実行することができる。

【００８４】

特許請求の範囲を含む本明細書で使用されるように、「少なくとも1つ」の前に付された項目のリストにおいて使用される「または」は離接リストを指し、たとえば、「A、B、またはCの少なくとも1つ」は、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)、あるいは複数の特徴(たとえばAA、AAB、ABBCなど)を有する組合せを意味する。

【００８５】

特許請求の範囲を含む本明細書で使用されるように、特に明記されない限り、機能または動作が項目または条件に「基づいている」という記載は、機能または動作が記載された項目または条件に基づいており、記載された項目または条件に加えて1つまたは複数の項目および/または条件に基づき得ることを意味する。

【００８６】

いくつかの例示的な構成を説明してきたが、本開示の趣旨から逸脱することなしに、様々な修正、代替構成、および同等物が使用され得る。たとえば、上記の要素は、より大きなシステムの構成要素であってもよく、他の規則が本発明の適用より優先してもよく、本発明の適用を変更してもよい。また、上記要素が考慮される前、途中、または後に、いくつかのステップが行われてもよい。したがって、上記の説明は、特許請求の範囲を制限しない。

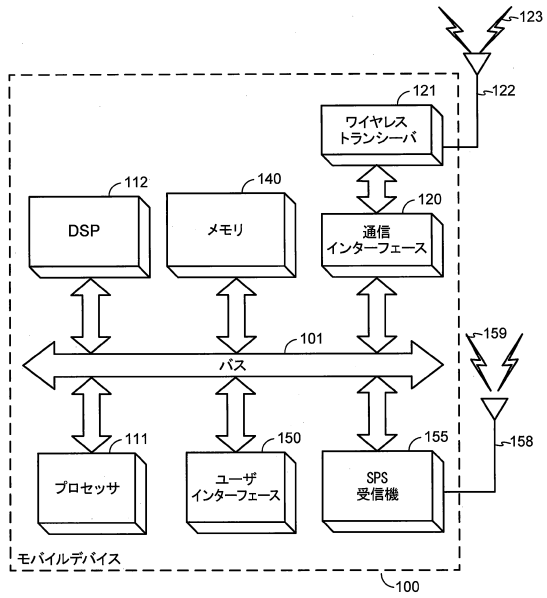
【符号の説明】

【００８７】

100 モバイルデバイス
101 公共バス
101 バス
111 プロセッサ
111 汎用プロセッサ
112 DSP
120 通信インターフェース
121 ワイヤレストランシーバ
122 ワイヤレスアンテナ
123 ワイヤレス信号
140 メモリ
150 ユーザインターフェース
155 SPS受信機
158 SPSアンテナ
159 衛星測位システム(SPS)信号
200 通信システム
202 UE
204 進化型ノードB(eNB)
206 モビリティ管理エンティティ(MME)
208 ホーム加入者サービス(HSS)エンティティ
210 サービングゲートウェイ(S-GW)
212 ポリシーおよび課金ルール機能(PCRF)
214 パケットデータネットワーク(PDN)ゲートウェイ(GW)
300 コンピュータシステム
305 バス
310 プロセッサ
315 入力デバイス
320 出力デバイス
325 ストレージデバイス
330 通信サブシステム
335 ワーキングメモリ
340 オペレーティングシステム
345 アプリケーションプログラム
400 コールフロー図
402 ネットワーク
404 ホームネットワーク
410 非アクセス層(NAS)要求メッセージ
410 NASアタッチ要求メッセージ
412 認証情報要求メッセージ
414 認証情報応答メッセージ
416 NAS認証要求メッセージ
418 NAS認証応答メッセージ

420 NASセキュリティモードコマンド(SMC)メッセージ
422 NASセキュリティモード完了メッセージ
424 S1AP初期コンテキスト設定メッセージ
426 RRC SMCメッセージ
428 RRCセキュリティモード完了メッセージ
500 コールフロー図
502 ネットワーク
504 ホームネットワーク
510 PFS NASアタッチ要求
512 PFS認証情報要求メッセージ
514 PFS認証情報応答メッセージ
516 PFS NAS認証要求メッセージ
518 PFS NAS認証応答メッセージ
520 PFS NAS SMCメッセージ
521 段階
522 PFS NASセキュリティモード完了メッセージ
524 段階
526 段階
528 段階
530 段階
532 段階
600 コールフロー図
602 ネットワーク
604 ホームネットワーク
616 PFS NAS認証要求メッセージ
620 PFS NAS SMCメッセージ
632 段階
700 プロセス
708 段階
718 段階
800 プロセス
900 プロセス
902 プロセス
904 段階
906 段階
908 段階

【図１】



【図２】

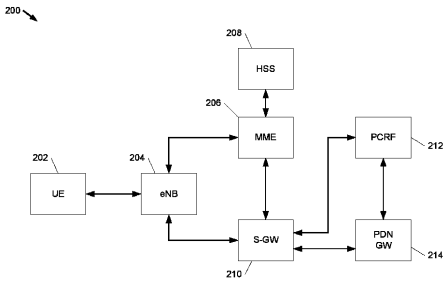
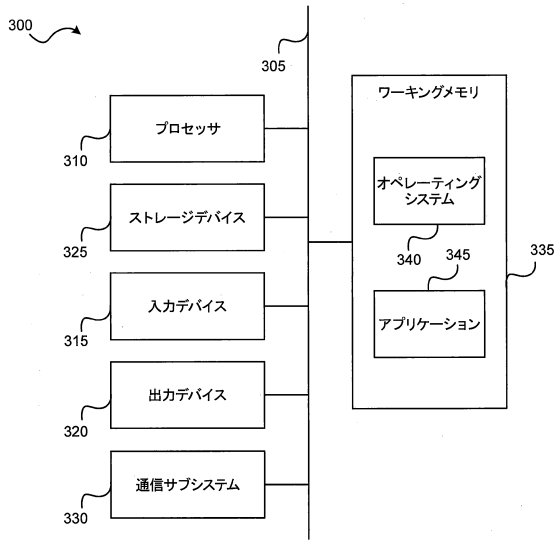
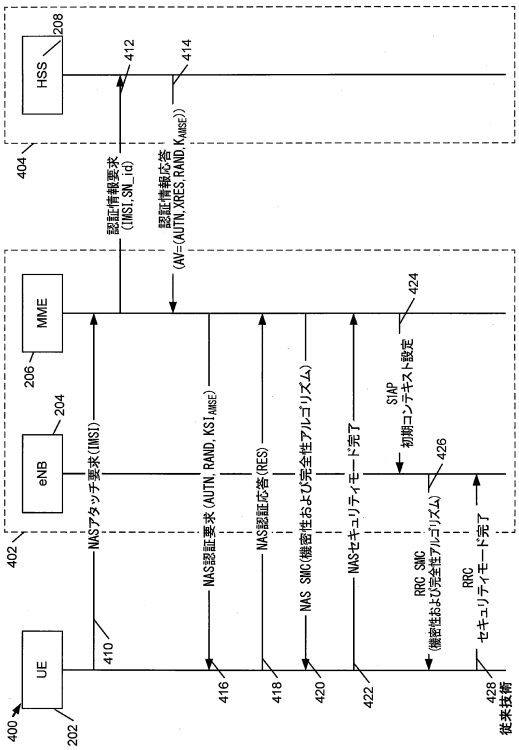


FIG. 2

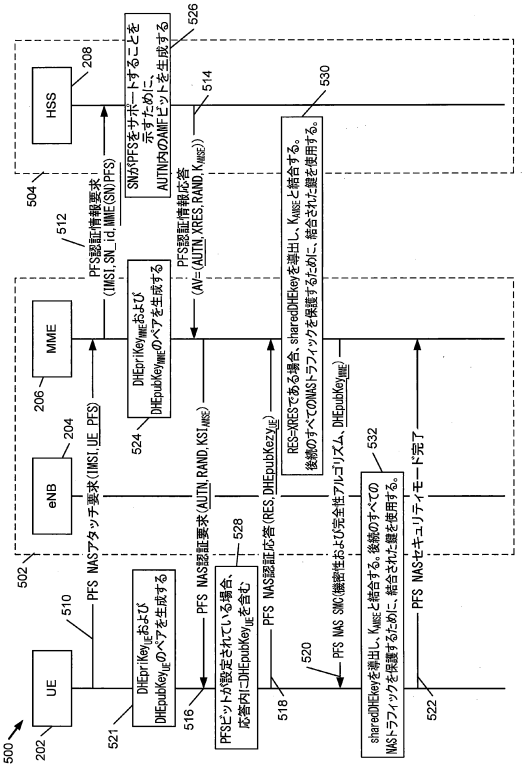
【図３】



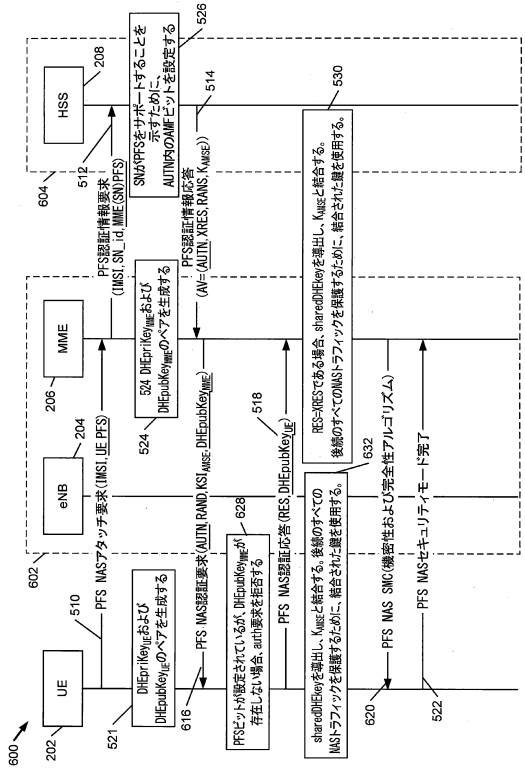
【図４】



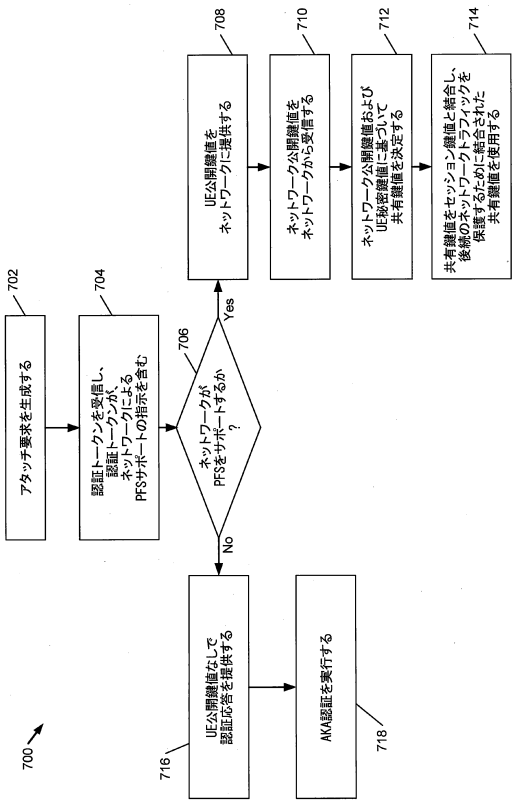
【図５】


500
UE
202
eNB
204
MME
206
HSS
208
502
504
510
512
514
516
518
520
522
524
526
528
530
532
PFS NASアタッチ要求(IMSI, UE PFS)
PFS認証情報要求 (IMSI, SN_id, MME(SN)PFS)
PFS認証情報応答 (AV=(AUTN, XRES, RAND, K_MME))
PFS NAS認証要求(AUTN, RAND, KSI_MME)
PFS NAS認証応答(RES, DHEpubKey_UE)
PFS NAS SMC(機密性および完全性アルゴリズム、DHEpubKey_MME)
PFS NASセキュリティモード完了
DHEpriKey_UEおよびDHEpubKey_UEのペアを生成する
DHEpriKey_MMEおよびDHEpubKey_MMEのペアを生成する
PFSビットが設定されている場合、応答内にDHEpubKey_UEを含む
RES=XRESである場合、sharedDHEkeyを導出し、K_NASEと結合する。後続のすべてのNASトラフィックを保護するために、結合された鍵を使用する。
sharedDHEkeyを導出し、K_NASEと結合する。後続のすべてのNASトラフィックを保護するために、結合された鍵を使用する。
SNがPFSをサポートすることを示すために、AUTN内のAMFビットを生成する

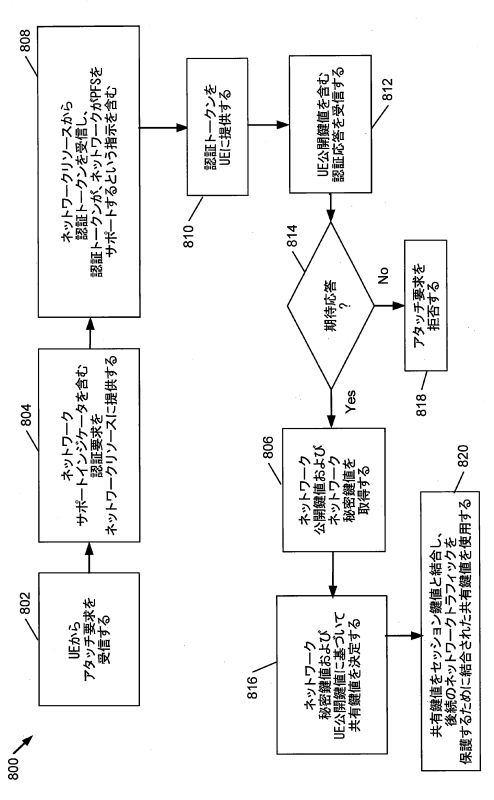
【図６】


600
UE
202
eNB
204
MME
206
HSS
208
602
604
510
512
514
518
520
522
524
526
528
530
532
PFS NASアタッチ要求(IMSI, UE PFS)
PFS認証情報要求 (IMSI, SN_id, MME(SN)PFS)
PFS認証情報応答 (AV=(AUTN, XRES, RAND, K_MME))
PFS NAS認証要求(AUTN, RAND, KSI_MME, DHEpubKey_MME)
PFS NAS認証応答(RES, DHEpubKey_UE)
PFS NAS SMC(機密性および完全性アルゴリズム)
PFS NASセキュリティモード完了
DHEpriKey_UEおよびDHEpubKey_UEのペアを生成する
524 DHEpriKey_MMEおよびDHEpubKey_MMEのペアを生成する
PFSビットが設定されているが、DHEpubKey_MMEが存在しない場合、auth要求を拒否する
RES=XRESである場合、sharedDHEkeyを導出し、K_NASEと結合する。後続のすべてのNASトラフィックを保護するために、結合された鍵を使用する。
sharedDHEkeyを導出し、K_NASEと結合する。後続のすべてのNASトラフィックを保護するために、結合された鍵を使用する。
SNがPFSをサポートすることを示すために、AUTN内のAMFビットを設定する

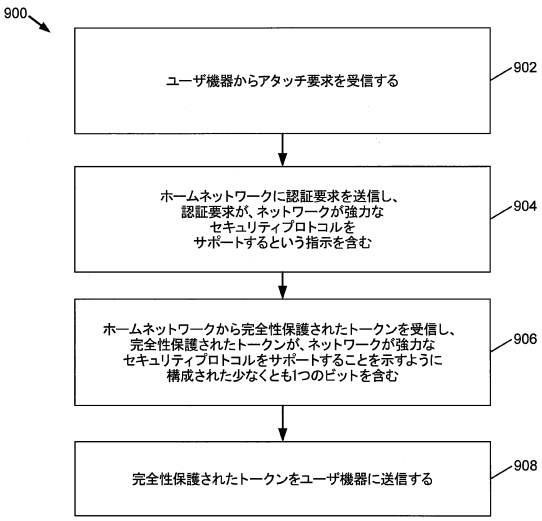
【図７】


700
702
アタッチ要求を生成する
704
認証トークンを受信し、認証トークンが、ネットワークによるPFSサポートの指示を含む
706
ネットワークがPFSをサポートするか？
Yes
No
708
UE公開鍵値をネットワークに提供する
710
ネットワーク公開鍵値をネットワークから受信する
712
ネットワーク公開鍵値およびUE秘密鍵値に基づいて共有鍵値を決定する
714
共有鍵値をセッション鍵値と結合し、後続のネットワークトラフィックを保護するために結合された共有鍵値を使用する
716
UE公開鍵値なしで認証応答を提供する
718
AKA認証を実行する

【図８】


800
802
UEから、アタッチ要求を受信する
804
ネットワーク、サポートインジケータを含む認証要求をネットワークリソースに提供する
806
ネットワーク公開鍵値およびネットワーク秘密鍵値を取得する
808
ネットワークリソースから認証トークンを受信し、認証トークンがネットワークがPFSをサポートするという指示を含む
810
認証トークンをUEに提供する
812
UE公開鍵値を含む認証応答を受信する
814
期待応答？
Yes
No
816
ネットワーク秘密鍵値およびUE公開鍵値に基づいて共有鍵値を決定する
818
アタッチ要求を拒否する
820
共有鍵値をセッション鍵値と結合し、後続のネットワークトラフィックを保護するために結合された共有鍵値を使用する

【図９】


900
ユーザ機器からアタッチ要求を受信する
902
ホームネットワークに認証要求を送信し、
認証要求が、ネットワークが強力な
セキュリティプロトコルを
サポートするという指示を含む
904
ホームネットワークから完全性保護されたトークンを受信し、
完全性保護されたトークンが、ネットワークが強力な
セキュリティプロトコルをサポートすることを示すように
構成された少なくとも1つのビットを含む
906
完全性保護されたトークンをユーザ機器に送信する
908

フロントページの続き

(31)優先権主張番号　14/825,988
(32)優先日　平成27年8月13日(2015.8.13)
(33)優先権主張国・地域又は機関
米国(US)

(56)参考文献　特表２０１４－５１１０７０（ＪＰ，Ａ）
特表２０１４－５２７３７９（ＪＰ，Ａ）
特開２０１２－２５３８１７（ＪＰ，Ａ）
特表２００８－５４７２４８（ＪＰ，Ａ）
特表２００９－５２７９５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｗ　１２／００－１２／１２