【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年9月10日(2020.9.10)

【公表番号】特表2019-533344(P2019-533344A)
【公表日】令和1年11月14日(2019.11.14)
【年通号数】公開・登録公報2019-046
【出願番号】特願2019-513988(P2019-513988)
【国際特許分類】
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　12/06　(2009.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　12/06
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０９Ｃ　1/00　６４０Ｅ
Ｇ０６Ｆ　21/44
Ｈ０４Ｌ　9/00　６０１Ｂ

【手続補正書】
【提出日】令和2年7月29日(2020.7.29)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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部分的に基づく、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部分的に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部分的に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部分的に基づき、

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部分的に基づく、ステップと、
前記第2のセキュリティ鍵に少なくとも部分的に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部分的に基づく、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部分的に基づく、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部分的に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部分的に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部分的に基づき、
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部分的に基づく、手段と、
前記第2のセキュリティ鍵に少なくとも部分的に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部分的に基づく、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部分的に基づく、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部分的に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、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部分的に基づく、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部分的に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、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部分的に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部分的に基づき、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部分的に基づいて前記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部分的に基づく、ステップと、
前記第2のセキュリティ鍵に少なくとも部分的に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部分的に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部分的に基づき、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部分的に基づいて前記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部分的に基づく、手段と、
前記第2のセキュリティ鍵に少なくとも部分的に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。