(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4763726号
(P4763726)
(45)発行日　平成23年8月31日(2011.8.31)　(24)登録日　平成23年6月17日(2011.6.17)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04W 12/06 (2009.01)　　H04Q 7/00 183

請求項の数 24　(全 21 頁)

(21)出願番号　特願2007-554262 (P2007-554262)
(86)(22)出願日　平成18年2月3日 (2006.2.3)
(65)公表番号　特表2008-530861 (P2008-530861A)
(43)公表日　平成20年8月7日 (2008.8.7)
(86)国際出願番号　PCT/US2006/003947
(87)国際公開番号　WO2006/084183
(87)国際公開日　平成18年8月10日 (2006.8.10)
審査請求日　平成19年9月6日 (2007.9.6)
(31)優先権主張番号　60/650,358
(32)優先日　平成17年2月4日 (2005.2.4)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/654,133
(32)優先日　平成17年2月18日 (2005.2.18)
(33)優先権主張国　米国 (US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】無線通信のための安全なブートストラッピング

(57)【特許請求の範囲】
【請求項１】
ネットワークアプリケーション機能と交信するためにレガシー移動端末を認証する方法であって、
ブートストラッピングサーバ機能において、第１のパラメータとしての第１の乱数、少なくとも部分的に前記第１の乱数に基づく公開鍵、並びに少なくとも部分的に前記第１の乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを生成することと、
前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて前記認証チャレンジの発信源を検証できる移動端末へ、認証チャレンジを送ることと、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む前記認証応答を前記ブートストラッピングサーバ機能において受信することと、
前記ブートストラッピングサーバ機能において第１のパラメータを、前記ブートストラッピングサーバ機能へ提供された第２の鍵に基づいて再計算することにより、前記認証応答が前記移動端末から発せられたかを検証することと、
前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記ブートストラッピングサーバ機能において相互認証鍵を生成することと、

を含む方法。
【請求項２】
前記加入者識別モジュールが、広域移動体通信システム（ＧＳＭ）の加入者識別モジュール（ＳＩＭ）またはＣＤＭＡ２０００認証モジュールのいずれか１つである請求項１に記載の方法。
【請求項３】
前記認証応答内の受信されたパラメータと前記ブートストラッピングサーバ機能によって再計算されるパラメータを比較することをさらに含み、双方のパラメータが同一である場合、前記認証応答が前記移動端末から発せられたと見なされる請求項１に記載の方法。
【請求項４】
前記ブートストラッピングサーバ機能と通信的に接続されたホームロケーションレジスタから前記プライベート鍵を得ることをさらに含む請求項１に記載の方法。
【請求項５】
前記プライベート鍵および前記プライベート鍵の複製が、前記移動端末の加入者識別モジュールおよび前記ブートストラッピングサーバ機能と通信的に接続されたネットワークデータベースとに知られている同一の安全なアルゴリズムおよび事前共有秘密鍵に基づいて生成される請求項１に記載の方法。
【請求項６】
前記ブートストラッピングサーバ機能に提供される前記プライベート鍵の複製が、前記移動端末外に格納された前記事前共有秘密鍵の複製および前記認証チャレンジ内の乱数に基づいて生成される請求項１に記載の方法。
【請求項７】
前記認証応答の前記第１のパラメータが、前記認証応答の発信源を検証するために前記ブートストラッピングサーバ機能によって用いられるメッセージ認証符号を含む請求項１に記載の方法。
【請求項８】
前記相互認証鍵を前記ブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送ってそれらの間の通信を安全にするために前記相互認証鍵を共有することをさらに含む、請求項１に記載の方法。
【請求項９】
無線移動端末と交信するための通信インターフェースと、
前記移動端末を認証するためにブートストラッピングサーバ機能を実施するように構成された処理回路とを含み、この機能を
前記通信インターフェースと接続され、ブートストラッピングサーバ機能において、第１のパラメータとしての第１の乱数、少なくとも部分的に前記第１の乱数に基づく公開鍵、並びに少なくとも部分的に前記第１の乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを生成することと、
前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて前記認証チャレンジの発信源を検証できる前記移動端末へ、前記認証チャレンジを送ることと、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む前記認証応答をブートストラッピングサーバ機能において受信することと、
前記ブートストラッピングサーバ機能において第１のパラメータを、前記ブートストラッピングサーバ機能へ提供された第２の鍵に基づいて再計算することにより、前記認証応答が前記移動端末から発せられたかを検証することと、
前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記ブートストラッピングサーバ機能において相互認証鍵を生成することとにより行う

ネットワーク装置。
【請求項１０】
前記加入者識別モジュールが広域移動体通信システム（ＧＳＭ）の加入者識別モジュール（ＳＩＭ）またはＣＤＭＡ２０００認証モジュールのいずれか１つである請求項９に記載のネットワーク装置。
【請求項１１】
前記処理回路が前記移動端末においてもプライベート鍵に基づいて計算される前記プライベート鍵の複製に基づいて、ブートストラッピングサーバ機能において相互認証鍵を計算することと、
前記移動端末およびネットワークアプリケーション機能が前記相互認証鍵を共有するように前記相互認証鍵を前記ブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送ることとによって、前記移動端末を認証するために前記ブートストラッピングサーバ機能を実施するように構成された請求項９に記載のネットワーク装置。
【請求項１２】
前記処理回路が、前記認証応答内の受信された前記第１のパラメータと前記ブートストラッピングサーバ機能によって計算される前記第１のパラメータとを比較することであって、双方の第１のパラメータが同一である場合、前記認証応答が前記移動端末から発せられていると見なす比較を行うことによって前記移動端末を認証するために、前記ブートストラッピングサーバ機能を実施するようにさらに構成された請求項９に記載のネットワーク装置。
【請求項１３】
レガシー移動端末を認証するためにブートストラッピングサーバ機能を実施するネットワーク装置であって、
ブートストラッピングサーバ機能において、第１のパラメータとしての第１の乱数、少なくとも部分的に前記第１の乱数に基づく公開鍵、並びに少なくとも部分的に前記第１の乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを生成する手段と、
前記認証チャレンジを前記移動端末に送るための手段と、ここで前記移動端末は前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて前記認証チャレンジの発信源を検証できる、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む前記認証応答をブートストラッピングサーバ機能において受信する手段と、
前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記ブートストラッピングサーバ機能において相互認証鍵を生成する手段と、
前記認証応答が前記移動端末から発せられたかどうかを決定するための手段とを含むネットワーク装置。
【請求項１４】
前記認証応答が前記移動端末から発せられたかどうかを決定するための手段が、前記認証応答の第１のパラメータを検証するために用いられる前記プライベート鍵の複製を含み、前記プライベート鍵の複製が前記事前共有秘密鍵および前記乱数並びに前記認証チャレンジおよび前記認証応答内で伝送される他のパラメータから導出される請求項１３に記載のネットワーク装置。
【請求項１５】
レガシー移動端末と交信するためにネットワークアプリケーション機能を認証する方法であって、
第１のパラメータとしての第１の乱数、少なくとも部分的に前記乱数に基づく公開鍵、並びに少なくとも部分的に前記乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを前記移動端末において受信することと、

前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記移動端末において相互認証鍵を生成することと、
前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて、前記ブートストラッピングサーバ機能において前記認証チャレンジが発生したかどうかを検証することと、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む認証応答を前記ブートストラッピングサーバ機能へ送ることを含む方法。

【請求項１６】
受信された前記認証チャレンジ内の乱数を受信することに対応して、前記加入者識別モジュールからの前記プライベート鍵を前記移動端末へ送ることをさらに含む請求項１５に記載の方法。

【請求項１７】
前記プライベート鍵が前記認証チャレンジおよび応答で伝送される付加的パラメータを用いて生成される請求項１６に記載の方法。

【請求項１８】
前記加入者識別モジュールが広域移動体通信システム（ＧＳＭ）の加入者識別モジュール（ＳＩＭ）またはＣＤＭＡ２０００認証モジュールのいずれか１つである請求項１５に記載の方法。

【請求項１９】
移動端末であって、
ブートストラッピングサーバ機能と交信するための無線通信インターフェースと、
レガシー通信プロトコルを動作させ、かつ前記ブートストラッピングサーバ機能によりチャレンジ応答プロトコルにおいて移動端末を認証するように構成された処理回路とを含み、処理回路が、
第１のパラメータとしての第１の乱数、少なくとも部分的に前記乱数に基づく公開鍵、並びに少なくとも部分的に前記乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを前記移動端末において乱数を含む認証チャレンジを受信し、
前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記移動端末において相互認証鍵を生成し、
前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて、前記認証チャレンジが前記ブートストラッピングサーバ機能から発したかどうかを検証し、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む認証応答を前記ブートストラッピングサーバ機能へ送る移動端末。

【請求項２０】
前記加入者識別モジュールは前記処理回路に接続され、事前共有秘密鍵およびアルゴリズムを格納するためのものである請求項１９に記載の移動端末。

【請求項２１】
前記加入者識別モジュールが、前記乱数、前記事前共有秘密鍵および前記アルゴリズムに基づいて前記プライベート鍵を生成する請求項２０に記載の移動端末。

【請求項２２】
前記加入者識別モジュールが、広域移動体無線システム（ＧＳＭ）のプロトコルに準拠する加入者識別モジュール（ＳＩＭ）である請求項２０に記載の移動端末。

【請求項２３】
前記事前共有秘密鍵は、前記無線端末がレガシー無線ネットワーク上で通信を確立可能とするために用いられる請求項１９に記載の移動端末。

【請求項２４】
レガシー移動端末であって、
第１のパラメータとしての第１の乱数、少なくとも部分的に前記乱数に基づく公開鍵、並びに少なくとも部分的に前記乱数、前記公開鍵、およびプライベート鍵に基づく署名を含む認証チャレンジを前記移動端末において受信するための手段と、
前記第１の乱数、前記第２の乱数、および前記プライベート鍵に少なくとも部分的に基づいて前記移動端末において相互認証鍵を生成するための手段と、
前記ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に用いて、前記認証チャレンジがブートストラッピングサーバ機能において発したかどうかを検証するための手段と、
前記移動端末の加入者識別モジュールに格納された事前共有秘密鍵および前記第１の乱数に少なくとも部分的に基づいて前記移動端末において生成された前記プライベート鍵の複製で計算された第２のパラメータおよび第２の乱数を含む認証応答を前記ブートストラッピングサーバ機能へ送るための手段と、を含むレガシー移動端末。
【発明の詳細な説明】
【技術分野】
【０００１】
米国特許法１１９条の下での優先権主張
本特許出願は、２００５年２月４日に出願された米国仮出願番号60/650,358、"Secure Bootstrapped Keys in GSM"（「ＧＳＭにおける安全なブートストラップした鍵」）および２００５年２月１８日に出願された米国仮出願番号60/654,133、"Secure Bootstrapping with CAVE"（「ＣＡＶＥによる安全なブートストラッピング」）に対する優先権を主張する。これらの仮出願はこの文書の譲受人に譲渡され、これによって、ここに参照として明白に組み込まれている。
【０００２】
発明の分野
本発明は一般に無線通信を安全にするためのシステムと方法に関する。より詳細には、本発明の１つの特徴は、レガシー無線の認証と鍵共有方法を利用することによりアプリケーションのセキュリティ鍵を提供するために、レガシーネットワーク認証方法をサポートする装置に対し新しい認証と鍵共有方式を提供する。
【背景技術】
【０００３】
無線通信のためのセルラ技術の１つの形式は、第２世代（２Ｇ）無線電信ネットワーク上で動作する広域移動体通信システム（ＧＳＭ）プロトコルで定義される。ＧＳＭは、２．５Ｇネットワークとしても知られる、ＧＳＭネットワークに対してインターネットコンテンツおよびパケットベースのデータサービスを提供する汎用パケット無線システム（ＧＰＲＳ）のようなより新しいネットワークによってさらに拡張される。ＧＳＭおよびＧＰＲＳは音声、インターネット閲覧、電子メール、およびマルチメディアデータを含む多くの形式の無線通信に用いられる。ＧＳＭは、そのようなシステム上で交信されるコンテンツを保護するために種々のセキュリティ方式を組み込む。サービスプロバイダもユーザも、それらの通信のプライバシーおよびそれらのデータ保護のために、これらのセキュリティ方式に頼る。また、サービスプロバイダは支払い請求のため、それらの加入者を認証するためにこれらのセキュリティ手段を用いる。これらのセキュリティ方式は通常、ネットワークに対してユーザ移動端末を認証することによって動作し、後続の伝送は暗号化されるかもしれない。しかし、ＧＳＭセキュリティ手段は、ＧＳＭセキュリティプロトコルの弱点のために、ネットワーク認証の不足、セキュリティプロトコルの再実行の可能性、およびＧＳＭ暗号化アルゴリズムの弱点から起こる不正な基地局の攻撃などのような第三者による攻撃を受けやすい。
【０００４】
これらのセキュリティの弱点は、第三世代（３Ｇ）無線通信規格における、セキュリテ

ィプロトコルの開発において検討された。特に、ユニバーサル移動電話システム（ＵＭＴＳ）のために開発された認証と鍵共有（ＡＫＡ）プロトコルは、ＧＳＭが影響を受けやすい不正基地局の攻撃を防止する一連番号およびメッセージ認証符号（ＭＡＣ）のような特徴を含む。したがって、ネットワーク認証のためにＵＭＴＳユーザサービス識別モジュール（ＵＳＩＭ）を用いる移動加入者は、ＧＳＭ加入者識別モジュール（ＳＩＭ）のユーザに対して加えられる攻撃の影響を受けにくい。

【０００５】

３Ｇ標準化団体は、例えば、第３世代パートナーシッププロジェクト文書３ＧＰＰ　３３．２２０汎用認証アーキテクチャ（ＧＡＡ）において、汎用ブートストラッピングアーキテクチャのために汎用認証アーキテクチャ（ＧＡＡ）を開発している。このアーキテクチャは、移動加入者のユーザ機器（ＵＥ）とブートストラッピングサーバ機能（ＢＳＦ）として知られている新しいサーバエンティティとの間の鍵を確立するために３Ｇ　ＡＫＡプロトコルに頼っている。これらの鍵から、ＢＳＦによって、さらなる複数の鍵が、ネットワークアプリケーション機能（ＮＡＦ）と適切なＵＥの間で共有されるセキュリティ鍵を確立する方法として種々のＮＡＦに対して導出され、提供されるかもしれない。

【０００６】

開発中の手法は、ＧＳＭなどの２Ｇまたはより初期のレガシーシステムに比較して固有のセキュリティが改良されたＵＭＴＳのユニバーサル加入者識別モジュール（ＵＳＩＭ）でサポートされるような３Ｇの認証と鍵共有法に頼っている。例えば、汎用認証アーキテクチャ（ＧＡＡ）および汎用ブートストラッピングアーキテクチャ（ＧＢＡ）は３Ｇネットワークに対して指定され、移動ユーザ機器とネットワークアプリケーションおよび／またはサービスを容易にするネットワークサーバとの間の安全な相互認証を提供するために、３Ｇ移動ネットワークのセキュリティインフラストラクチャ（すなわち、ＵＳＩＭベースのセキュリティ）を構築する。

【０００７】

しかし、これらの相互認証手法（例えば、ＧＡＡおよびＧＢＡ）は、例えばＧＳＭ認証と鍵共有（ＡＫＡ）プロトコルなどの、より以前に開発された（例えば、２Ｇ）通信システムでは利用可能でない。これらのＧＳＭプロトコルは再実行攻撃の影響を受けやすい。したがって攻撃側は鍵の再使用を強制し、鍵を暴露するためにいくつかの状況における弱点を利用し、これによりセキュリティを攻撃するかもしれない。したがって、再実行攻撃の影響を受けにくく、鍵が容易に暴露されないような方法で、ＧＳＭの認証と鍵共有からアプリケーションセキュリティ鍵をブートストラップするための方法が必要である。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

したがって、３Ｇネットワークに対して指定された汎用認証アーキテクチャ（ＧＡＡ）がレガシーシステム（例えば、２Ｇまたはそれ以前のシステム）をサポートするように拡張されるかもしれない手法を確立する必要がある。このことは、ＧＳＭの加入者または加入者識別モジュール（ＳＩＭ）を有する他の装置が、ＳＩＭをＵＭＴＳ　ＵＳＩＭで置き替える必要無しに、移動ネットワークアプリケーションおよび／またはサービスを利用するための鍵を供給されることを可能とするだろう。さらに、そのような方法はＧＳＭ認証自体の脆弱性に基づく弱点を汎用認証アーキテクチャに持ち込むべきでない。

【課題を解決するための手段】

【０００９】

アプリケーション-セキュリティ鍵をレガシー加入者識別モジュール（例えば３Ｇ　ＡＫＡ方式をサポートしないＧＳＭ　ＳＩＭおよびＣＤＭＡ２０００　Ｒ－ＵＩＭ）をサポートする移動端末と安全に共有するための相互認証方法が提供される。チャレンジ-応答の鍵交換はブートストラッピングサーバ機能（ＢＳＦ）と移動端末（ＭＴ）の間で実施される。ＢＳＦはホームロケーションレジスタ（ＨＬＲ）からこの移動端末に対応するネットワーク認証パラメータ（例えば、ＧＳＭ　ＲＡＮＤ、ＳＲＥＳ、Ｋｃ）を受信し、ＲＡ

ＮＤを含む認証チャレンジを生成し、それをサーバ認証された公開鍵方式の下で前記ＭＴへ送信する。この認証チャレンジは乱数、識別情報、タイムススタンプ、一連番号およびディフィー-ヘルマン公開鍵などの更なるパラメータを含むかもしれない。

【００１０】

ＭＴは、認証チャレンジを受信し、それがブートストラッピングサーバ証明書に基づいてＢＳＦから発しているかどうかを決定する。ＭＴは認証チャレンジ（例えば、乱数）および事前共有秘密鍵（例えば、ＧＳＭ　ＳＩＭにおける）から導出された鍵に基づいて認証チャレンジへの応答を構築する。すなわち、ＭＴ内のＳＩＭは、認証チャレンジで受信された乱数ＲＡＮＤおよびＳＩＭに格納された事前共有秘密鍵とに基づいてブートストラッピングサーバ機能によって用いられる秘密鍵（例えば、ＳＲＥＳおよびＫｃ）を導出することができる。認証応答は暗号化された乱数、識別情報、タイムスタンプ、一連番号、およびディフィー-ヘルマン公開鍵のようなさらなるパラメータを含むかもしれない。ＢＳＦは、認証応答を受信し、それがＭＴから発しているかどうかを決定する。チャレンジ-応答方式は、チャレンジの発信源を検証するための公開鍵方式および応答の発信源を検証するための事前共有秘密鍵を利用する。例えば、ＢＳＦは認証応答（例えばＲＡＮＤ、ＳＲＥＳ、および／または、Ｋｃを用いてまたはそれらに基づいてＨＬＲから求めた）内の１つ以上のパラメータを独立して再計算することができ、それにより認証応答内の受信された１つ以上のパラメータが同一であるかを検証する。

【００１１】

これらのメッセージが認証された場合、ＢＳＦおよびＭＴは、ＲＡＮＤ、ＳＲＥＳ、Ｋｃ、および／またはＢＳＦとＭＴの間で伝送されていたかもしれないさらなるパラメータに基づいてアプリケーションセキュリティ鍵を計算するかもしれない。鍵ＳＲＥＳおよびＫｃはＢＳＦおよびＭＴが独立に分かり、それらの間で伝送されない。アプリケーションセキュリティ鍵は、移動端末とネットワークアプリケーション機能がアプリケーションセキュリティ鍵を共有し、それらの間の安全な通信のためにそれらを用いることができるように、ブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送られるかもしれない。

【００１２】

ネットワークアプリケーション機能と交信するために、レガシー移動端末を認証するための方法が提供される。この方法は、（ａ）ブートストラッピングサーバ機能で認証チャレンジを生成すること、（ｂ）認証チャレンジを移動端末に送信することであって、移動端末がブートストラッピングサーバ機能に関連している予め得たブートストラッピングサーバ証明書に基づいて認証チャレンジの発信源を検証でき、（ｃ）移動端末で生成された第１の鍵で計算された第１のパラメータを含む認証応答をブートストラッピングサーバ機能において受信すること、（ｄ）ブートストラッピングサーバ機能に提供された第２の鍵に基づいて、ブートストラッピングサーバ機能において第１のパラメータを再計算することにより、認証応答が移動端末から発せられたかどうかを検証すること、（ｅ）認証応答内の受信された第１のパラメータとブートストラッピングサーバ機能によって再計算された第１のパラメータを比較することとを含む。双方の第１のパラメータが同一である場合、認証応答は、その移動端末から発せられたと見なされる。

【００１３】

第１の鍵は、移動端末に格納された広域移動体通信システム（ＧＳＭ）加入者識別モジュール（ＳＩＭ）またはＣＤＭＡ２０００認証モジュールのいずれかであるかもしれない加入者識別モジュールから得られるかもしれない。第２の鍵はブートストラッピングサーバ機能に通信的に接続されたホームロケーションレジスタから得られるかもしれない。第１および第２の鍵は、移動端末内の加入者識別モジュールおよびブートストラッピングサーバ機能に通信的に接続されたネットワークデータベースには既知の同一の安全性アルゴリズムおよび事前共有秘密鍵に基づいて生成されるかもしれない。認証チャレンジはパラメータとして乱数を含むかもしれない。また、移動端末の加入者識別モジュールに格納された乱数および事前共有秘密鍵は、認証応答内の第１のパラメータを計算するために用い

られる第１の鍵を生成するために、加入者識別モジュールにより用いられる。ブートストラッピングサーバ機能に提供された第２の鍵は、移動端末の外部に格納された事前共有秘密鍵および認証チャレンジ内の乱数とに基づいて生成されるかもしれない。認証応答の第１のパラメータは、第１の鍵で計算され、認証応答の発信源を検証するためにブートストラッピングサーバ機能によって用いられるメッセージ認証符号を含むかもしれない。

【００１４】

いくつかの実施態様において、第３の鍵がブートストラッピングサーバ機能において第２の鍵に基づいて生成されるかもしれない。第１のパラメータは、ブートストラッピングサーバ機能で第３の鍵を用いて再計算される。

【００１５】

さらに、本方法は、（ａ）ブートストラッピングサーバ機能において、移動端末によっても第１の鍵を用いて独立に計算される第２の鍵に基づいて第４の鍵を計算すること、および（ｂ）移動端末とネットワークアプリケーション機能がそれら間の通信を安全にするための第４の鍵を共有するために、第４の鍵をブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送信することをさらに含むかもしれない。

【００１６】

もう一つの特徴は、（ａ）無線移動端末と交信するための通信インターフェースと、（ｂ）通信インターフェースに接続され、移動端末を認証するためにブートストラッピングサーバ機能を実施するように構成された処理回路とを含むネットワーク装置を提供する。処理回路は、（ａ）乱数を含む認証チャレンジを生成すること、（ｂ）認証チャレンジを移動端末に送信することであって、移動端末がブートストラッピングサーバ機能に関連している予め得たブートストラッピングサーバ証明書に基づいて認証チャレンジの発信源を検証でき、（ｃ）乱数、事前共有秘密鍵およびアルゴリズムに基づいて第１の鍵により計算される第１のパラメータを含む認証応答を移動端末から受信することであって、前記事前共有秘密鍵およびアルゴリズムが移動端末内の加入者識別モジュールおよびブートストラッピングサーバ機能に通信的に接続されたネットワークデータベースに既知であり、（ｄ）ネットワークデータベースによりブートストラッピングサーバ機能に提供された第２の鍵に基づいて、ブートストラッピングサーバ機能において第２のパラメータを計算すること、（ｅ）第１のパラメータと第２のパラメータを比較することであって、第１および第２のパラメータが同一である場合、前記認証応答が移動端末から発せられたと見なされることとによって移動端末を認証するかもしれない。いくつかの実施態様において、加入者識別モジュールは広域移動体通信システム（ＧＳＭ）加入者識別モジュール（ＳＩＭ）またはＣＤＭＡ２０００認証モジュールのいずれか１つであるかもしれない。さらに、処理回路は、（ａ）ブートストラッピングサーバ機能において、移動端末によっても第１の鍵に基づいて計算される第４の鍵を第２の鍵に基づいて計算すること、（ｂ）移動端末とネットワークアプリケーション機能が第４の鍵を共有するために第４の鍵をブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送信することとによって移動端末を認証するためにブートストラッピングサーバ機能を実施するようにさらに構成されるかもしれない。処理回路は、認証応答内の受信された第１のパラメータと、ブートストラッピングサーバ機能によって計算された第１のパラメータとを比較して移動端末を認証するためにブートストラッピングサーバ機能を実施するようにさらに構成されるかもしれない。ここで２つの第１のパラメータが同一である場合、認証応答を移動端末から発せられたと見なす。

【００１７】

さらに別の態様は、ネットワークアプリケーション機能と交信するために、レガシー移動端末を認証するための方法を提供する。この方法は、（ａ）乱数を含む認証チャレンジを移動端末で受信すること、（ｂ）移動端末が、ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて、認証チャレンジがブートストラッピングサーバ機能で発せられたかどうかを検証すること、（ｃ）移動端末内のレガシー加入者識別モジュールによって生成された第１の鍵に基づいて認証応答を生成するこ

と、（ｄ）加入者識別モジュールからの第１の鍵を、認証チャレンジ内の受信された乱数を受信することに対応して、移動端末に提供することとを含む。本方法は、加入者識別モジュールにおいて乱数、事前共有秘密鍵およびアルゴリズムを用いて第１の鍵を生成することをさらに含むかもしれない。事前共有秘密鍵およびアルゴリズムは、両者とも加入者識別モジュールおよびブートストラッピングサーバ機能と通信的に接続されたネットワークデータベースに格納される。いくつかの実施態様において、第１の鍵は、認証チャレンジおよび応答で伝送される付加的パラメータを用いて生成されるかもしれない。

【００１８】

本方法は、移動端末において第１の鍵に基づいて第３の鍵を計算することをさらに含むかもしれない。第３の鍵は、ブートストラッピングサーバ機能においても、ネットワークデータベースによってブートストラッピングサーバ機能に提供された第２の鍵に基づいて独立に計算されるかもしれない。第３の鍵は、移動端末およびネットワークアプリケーション機能が第３の鍵を共有するために、ブートストラッピングサーバ機能から要求ネットワークアプリケーション機能へ送信される。

【００１９】

別の特徴は、（ａ）ブートストラッピングサーバ機能と交信するための無線通信インターフェース、（ｂ）事前共有秘密鍵およびアルゴリズムを格納するための加入者識別モジュール、（ｃ）レガシー通信プロトコルを動作させ、かつブートストラッピングサーバ機能を用いてチャレンジ-応答プロトコルにおいて移動端末を認証するように構成された処理回路とを含む移動端末を提供する。処理回路は、（ａ）乱数を含む認証チャレンジをブートストラッピングサーバ機能から受信すること、（ｂ）ブートストラッピングサーバ機能に関連する予め得たブートストラッピングサーバ証明書に基づいて認証チャレンジがブートストラッピングサーバ機能で発せられたかどうかを決定すること、（ｃ）乱数、事前共有秘密鍵およびアルゴリズムから生成される第１の鍵を用いて計算される第１のパラメータを含む認証応答を生成することとによって、動作するかもしれない。さらに、処理回路は、（ａ）第１の鍵および認証チャレンジおよび応答で伝送される他のパラメータに基づいて導出される第３の鍵を生成し、（ｂ）その第３の鍵を用いてメッセージ認証符号を生成するかもしれない。メッセージ認証符号はブートストラッピングサーバへの認証応答に含まれるかもしれない。加入者識別モジュールは乱数、事前共有秘密鍵およびアルゴリズムに基づく第１の鍵を生成するかもしれない。

【００２０】

加入者識別モジュールは広域移動体通信システム（ＧＳＭ）プロトコルに準拠する加入者識別モジュール（ＳＩＭ）であるかもしれない。また、事前共有秘密鍵は、移動端末がレガシー無線ネットワーク上で通信を確立することを可能にするためにも用いられるかもしれない。

【発明を実施するための最良の形態】

【００２１】

以下の記述において、実施例の十分な理解を提供するために特定の詳細が述べられる。しかし、通常の当業者は実施例がこれらの特定の詳細の範囲外で実行されるかもしれないことを理解するだろう。例えば、不必要な詳細によって実施例が不明瞭にならないように回路はブロック図で示されるかもしれない。他の例では、周知の回路、構造、および技術は実施例を不明瞭しないように詳細に示されないかもしれない。

【００２２】

また、実施例がフローチャート、フロー図、構造図、またはブロック図として表される処理として説明されるかもしれないことを注意する。フローチャートは動作を一連の処理として記述するかもしれないが、多くの動作は並列または同時に実行することができる。さらに、動作の順序は配列し直されるかもしれない。動作が完了すると、処理は終了する。処理は方法、機能、手順、サブルーチン、サブプログラムなどに対応するかもしれない。処理が機能に対応している場合、その終了は、機能の呼び出し機能または主機能へのリターンに対応している。

【００２３】
さらに、記憶媒体は、読み出し専用メモリー（ＲＯＭ）、ランダムアクセスメモリー（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリ装置および／または情報記憶用の機械読み出し可能な媒体を含む１つ以上のデータ記憶用装置を表すかもしれない。用語「機械読み出し可能媒体」は、可搬または固定記憶装置、光記憶装置、無線チャネル並びに命令および／またはデータを記憶、収納または持ち運びすることが可能な他の種々の媒体を非限定的に含む。
【００２４】
さらに、実施例はハードウェア、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、またはそれらの組み合わせで実施されるかもしれない。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施される場合、必要なタスクを実行するためのプログラムコードまたはコードセグメントは、記憶媒体または他の記憶装置のような機械読み出し可能な媒体に格納されるかもしれない。プロセッサは必要なタスクを実行するかもしれない。コードセグメントは手順、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造もしくはプログラム文の組み合わせを表すかもしれない。コードセグメントは、情報、データ、引数、パラメータ、または記憶内容を通過させおよび／または受信することにより、もう一つのコードセグメントまたはハードウェア回路と接続されるかもしれない。情報、引数、パラメータ、データ等は、メモリー共有、メッセージパッシング、トークンパッシング、ネットワーク伝送などを含む適切な手段で通過、転送または伝達されるかもしれない。
【００２５】
以下の記述において、一定の用語は、本発明の１つ以上の実施例の一定の特徴を説明するために用いられる。例えば、用語「移動端末」、「ユーザ機器」、「移動装置」、「無線装置」、および「無線移動装置」は携帯電話、ポケットベル、無線モデム、携帯情報端末（ＰＩＭ）、パームトップコンピュータ、ラップトップコンピュータ、および／または少なくとも部分的にセルラネットワークを介して通信するその他の移動通信／計算装置を指すために互換性を持って用いられる。用語「レガシー」は３Ｇより前の、３Ｇより前のプロトコルを動作させる、またはＧＳＭ準拠のＳＩＭもしくはＣＤＭＡ準拠の認証モジュールもしくはＭＮ-ＡＡＡ認証モジュールを用いるネットワーク、プロトコルおよび／または移動体装置を指すために用いられる。さらに、用語、加入者識別モジュールは、ＧＳＭ準拠の加入者識別モジュール（ＳＩＭ）、ＣＤＭＡ準拠の認証モジュールもしくはＭＮ-ＡＡＡ認証モジュール、または無線ネットワークに対して移動端末を識別するために移動端末に通常含まれる任意の他のモジュールを指すために用いられる。
【００２６】
１つの特徴は、レガシーシステムをサポートするために汎用認証アーキテクチャを拡張する方法を提供し、その結果、ＧＳＭ加入者識別モジュール（ＳＩＭ）を保持している加入者は、ＳＩＭを３Ｇ　ＵＭＴＳ準拠のユーザサービス識別モジュール（ＵＳＩＭ）と交換することなく移動アプリケーションにおいて使用するための鍵を供給されるかもしれない。
【００２７】
図１は１実施態様に従ってブートストラッピングサーバおよびレガシー移動端末が互いを相互認証できる通信システムを示すブロック図である。ＧＳＭ準拠の、または、ＣＤＭＡ２０００準拠の通信システムのようなネットワークアーキテクチャ１００は移動端末（ＭＴ）１０２、ホームロケーションレジスタ（ＨＬＲ）１０４、ブートストラッピングサーバ機能（ＢＳＦ）１０６、および少なくとも１つのネットワークアプリケーション機能（ＮＡＦ）１０８を含む。ＨＬＲ１０４とＢＳＦ１０６に対して、ネットワークアーキテクチャ１００のインフラストラクチャの一部である１つ以上のネットワーク装置および／またはサーバがホストとなるかもしれない。ＨＬＲ１０４は、加入者に属する各ＭＴ１０２に対する国際移動加入者識別番号（ＩＭＳＩ）を含む無線キャリアに対する移動加入者

情報を格納するデータベースを含む。ＩＭＳＩはネットワーク内のＭＴ１０２に関連する一意の数である。ＩＭＳＩはまた、各ＭＴ１０２の加入者識別モジュール（ＳＩＭ）にも格納され、ＭＴ１０２に関する情報を検索するためにネットワークＨＬＲへＭＴによって送られる。

【００２８】

ＭＴ１０２はネットワーク１００上で通信するために、予め定義されたプロトコル（例えば、３Ｇより前のプロトコル）を用いてサービスプロバイダに登録するかまたは接続するレガシー無線通信装置であるかもしれない。いくつかの実施態様において、サービスプロバイダによるこの登録プロセスは、事前共有秘密鍵（例えば、ＧＳＭ　ＳＩＭ、ＣＤＭＡ認証モジュール、または他のレガシーモジュールに格納されている）を用いてＭＴ１０２を認証することを含むかもしれない。例えば、ＭＴ１０２は、ＭＴ１０２が、ＧＳＭまたはＣＤＭ２０００ネットワークで動作できるように、および無線経由の通信のためのネットワークによって認証され得るように、ＧＳＭ準拠のＳＩＭ、またはＣＤＭＡ２０００準拠の認証モジュールを含むかもしれない。

【００２９】

ＭＴ１０２がネットワークを介した通信のためにサービスプロバイダによっていったん認証されると、本発明の１つの態様は、安全なネットワークアプリケーションを可能にするためにもう一つの認証の層を追加する。この付加的認証方式は基本的なネットワークベアラまたはベアラの認証方式とは別のものである。認証の付加的層は、ネットワークまたはベアラのセキュリティサービスとは独立している鍵を確立するためにＳＩＭまたは認証モジュール内の既存の鍵を、新しいプロトコルと共に用いる。この新しい認証方式は、ＭＴ１０２と特定のＮＡＦの間で共有され、ＢＳＦ１０６を経由してＮＡＦ１０８に分配される認証用または他の目的のための鍵を提供する。例えば、ＮＡＦ１０８はネットワーク化された装置で動作するアプリケーション、例えば商取引アプリケーションおよび／または、位置に基づくサービスであるかもしれない。

【００３０】

ＭＴ１０２がネットワークアプリケーションの使用を始める準備ができている場合、それは通信リンク１１０を通じてＮＡＦ１０８との接続を開始する。ＭＴとＮＡＦが適切な鍵をまだ共有していない場合、ＮＡＦ１０８はインターフェース１１２を通じてＢＳＦ１０６へ認証鍵を要求する。未だそうしていない場合、ＭＴ１０２とＢＳＦ１０６は、認証リンク１１４上でＭＴ１０２と鍵を共有する。

【００３１】

ディフィー-ヘルマンの鍵交換はＭＴ１０２とＢＳＦ１０６の間の鍵共有処理の一部として用いられるかもしれない。ディフィー-ヘルマンの鍵交換は、互いの知識を予め有していない二者が、安全でない通信チャネル上で共有秘密鍵を共同で確立することを可能とする暗号化プロトコルである。１つのアプリケーションにおいて、この共有秘密鍵は対称鍵暗号法を用いて後続の通信を暗号化するために用いることができる。

【００３２】

しかし、それだけでは従来のディフィー-ヘルマン鍵交換アルゴリズムは、このアルゴリズムのセキュリティを密かに攻撃する「中間者」の攻撃を受けやすい。これは、ＭＴ１０２とＮＡＦ１０８の間で商取引および／または秘密取引を実行するために、無線媒体上で情報が交換される場合に特に問題である。

【００３３】

本発明の１つの特徴は、ＢＳＦ１０６とＭＴ１０２が公開鍵または共有秘密鍵を、ＧＳＭおよび／またはＣＤＭＡ２０００固有の弱点に影響されにくい方法で共有することを可能とするプロトコルを提供する。特に、ＢＳＦ１０６を認証するために、ＭＴ１０２は最初に、ディジタル証明書を供給される。これは、ＢＳＦ１０６からＭＴ１０２への通信がディジタル署名されるかまたはサーバ認証されたチャンネルで伝達されることを可能とし、その結果、ＭＴ１０２が、認証処理の間に受信した鍵またはパラメータがＢＳＦ１０６から来るのであり、「中間者」または再実行攻撃を試みる別のエンティティから来るので

はないことを確認することを可能とする。したがって、本方法は３Ｇの汎用ブートストラッピングアーキテクチャの認証方式を、ネットワーク認証からそれら自身利益を得ないＵＭＴＳ　ＡＫＡ以外のプロトコルに拡張するために適用されるかもしれない。

【００３４】

図２は通信ネットワーク上で動作するブートストラッピングサーバ機能との相互認証を実行するように構成された移動端末（ＭＴ）２００を示すブロック図である。ＭＴ２００は無線ネットワークと交信するための通信インターフェース２０６と接続された処理回路２０２（例えば、プロセッサ）、および加入者識別モジュール（ＳＩＭ）カード２０４を含む。処理回路２０２は、図４、５、６、および７に示す方法の一部またはすべてを実行するように構成されるかもしれない。ＳＩＭ２０４は、秘密鍵Ｋｉ、ＧＳＭの認証と鍵共有アルゴリズム（すなわち、ＧＳＭ　Ａ３／Ａ８アルゴリズム）の実施を含むかもしれない。また、ＳＩＭ２０４は公開鍵または、ＢＳＦ１０６のプライベート鍵に対応する公開鍵のデジタルサーバ証明書を含むＭＴ１０２に挿入される。特に、ＳＩＭ２０４は、ＧＳＭネットワークで使用するために構成された標準的レガシースマートカードであるかもしれない。この公開鍵またはサーバ証明書はＲＳＡ公開鍵に対応するかもしれない。または、ディジタル署名を提供する他の公開鍵技術、例えばＤＳＡ（ディジタル署名アルゴリズム）、も用いられるかもしれない。また、ＢＳＦ１０６およびＭＴ１０２は、有限体の乗法部分群または楕円曲線にある一点のような、巡回群の予め定めた生成元Ｐを、ディフィー-ヘルマンの鍵交換を用いることができるように共有するかもしれない。代替的実施例において、ＭＴ２００はＳＩＭ２０４の代わりにＣＤＭＡ２０００準拠の認証モジュールを含むかもしれない。

【００３５】

図３は本発明の１つの態様に従って移動局（ＭＴ）を認証するためにブートストラッピングサーバ機能を実行するように構成されたネットワーク装置を示すブロック図である。ネットワーク装置３００は無線ネットワークと交信するための通信インターフェース３０６および記憶装置３０４に接続された処理回路３０２（例えば、プロセッサ）を含む。処理回路３０２は、ＭＴとディフィー-ヘルマンの鍵交換を実施するための鍵および／またはパラメータを保持する限り、ブートストラッピングサーバ機能を実行するように構成されるかもしれない。例えば、処理回路３０２は、図４、５、６、および７に示す方法の一部またはすべてを実行するように構成されるかもしれない。

【００３６】

図４に、１つの実施態様に従ってレガシーＳＩＭを有する移動端末とブートストラッピングサーバ機能とを相互認証するチャレンジ-応答方式を実行する方法を示す。このチャレンジ-応答方式はチャレンジの発信源を検証するための公開鍵方式および応答の発信源を検証するための事前共有秘密鍵を利用する。

【００３７】

ブートストラッピングサーバ機能（ＢＳＦ）は、認証チャレンジを生成し、サーバ認証された公開鍵方式の下で移動端末（ＭＴ）に送る（４０２）。認証チャレンジは、乱数（例えば、ＲＡＮＤ）を含むかもしれない。また、認証チャレンジは、ネットワークデータベースおよびＭＴ内の加入者識別モジュールに既知の事前共有秘密鍵（例えば、Ｋｉ）から導出される。例えば、事前共有秘密鍵Ｋｉおよび乱数（例えば、ＲＡＮＤ）は、認証チャレンジパラメータを生成するために用いる秘密鍵（例えば、ＳＲＥＳおよびＫｃ）を生成するために用いられるかもしれない。認証チャレンジは、タイムスタンプ、他の乱数、識別情報、ディフィー-ヘルマン公開鍵などの付加的パラメータも含むかもしれない。また認証チャレンジはディジタル署名されおよび／またはサーバ認証されたチャンネル上で送信される。

【００３８】

ＭＴは、認証チャレンジを受信し、それがブートストラッピングサーバ証明書に基づいてＢＳＦから発せられたかどうかを検証する（４０４）。そのようなブートストラッピングサーバ証明書（例えば公開鍵）は、設定時、オフラインで、および／または前の処理の

間にＭＴおよびＢＳＦへ供給されているかもしれない。ＭＴはＭＴ内の加入者識別モジュールによって導出される、および／または提供される鍵に基づいて認証チャレンジへの応答を構築する（４０６）。これらの秘密鍵は、認証チャレンジ内の受信された乱数および加入者識別モジュールに格納された事前共有秘密鍵とに基づいて加入者識別モジュールで生成されるかもしれない。例えば、認証チャレンジ内の受信された乱数（例えばＲＡＮＤ）およびＭＴの加入者識別モジュールに格納された事前共有秘密鍵（例えばＫｉ）は、認証応答パラメータを生成するために用いられる鍵（例えばＳＲＥＳおよびＫｃ）を生成するために用いられるかもしれない。さらに、いくつかの実施態様において、ＭＴは、付加的パラメータ（例えば、タイムスタンプ、他の乱数、識別情報、ディフィー-ヘルマン公開鍵）を用いて、認証応答を構築するために用いられる鍵を計算するかもしれない。

【００３９】

ＢＳＦは、認証チャレンジを受信し、それがブートストラッピングサーバ機能によって独立に得られた秘密鍵（例えば、ＳＲＥＳとＫｃ）に基づいてＭＴから発せられたかどうかを検証する（４０８）。例えば、ＢＳＦは、乱数ＲＡＮＤおよび事前共有秘密鍵（例えば、Ｋｉ）に基づいてネットワークデータベースによって生成される秘密鍵（例えば、ＳＲＥＳおよびＫｃ）を用いるかもしれない。したがって、ブートストラッピングサーバ証明書は、チャレンジの発信源を検証するためにＭＴによって用いられ、一方、鍵（例えば、ＳＲＥＳおよびＫｃ）は応答の発信源を検証するためにＢＳＦによって用いられる。これは、第三者による攻撃が行われないことを保証する。

【００４０】

鍵（例えば、ＳＲＥＳおよびＫｃ）の検証および独立した計算から、ＭＴおよびＢＳＦの共有鍵を計算することができる。ブートストラッピングサーバが、移動端末とネットワークアプリケーション機能の間の安全な通信を可能にするために、要求ネットワークアプリケーション機能に提供することができるアプリケーション鍵は、移動端末およびブートストラッピングサーバで生成されるかもしれない（４１０）。例えば、共有鍵または共有鍵から導出されたアプリケーション鍵は、ＢＳＦによって要求ネットワークアプリケーション機能（ＮＡＦ）へ送ることができ、その結果、ＮＡＦおよびＭＴはＮＡＦとＭＴとの間の通信を安全にするために用いることができる鍵を共有する。

【００４１】

図５に、本発明の１つの実施例に従ってブートストラッピングサーバ機能およびサーバ機能の認証を用いて移動端末を認証する方法を示す。この方法は、ネットワークアプリケーション機能が、ネットワークアプリケーショントランザクションを開始するに先立ち移動端末（ＭＴ）と鍵共有を望む場合に実施されるかもしれない。例えば、ＧＳＭの認証と鍵共有（ＡＫＡ）はチャレンジ-応答プロトコルに基づく。２つのアルゴリズムＡ３およびＡ８と同様に秘密鍵Ｋｉは、ネットワークホームロケーションレジスタ（ＨＬＲ）／認証センタ（ＡｕＣ）と同様にＭＴ内の加入者識別モジュール（ＳＩＭ）に格納される。ＳＩＭは、改竄防止となるように設計され、ユーザによって容易に読みだすことができない秘密データおよびアルゴリズムを含む。

【００４２】

鍵を求める要求が生成され、内部にレガシーＳＩＭを備えているＭＴからブートストラッピングサーバ機能（ＢＳＦ）へ送信される（５０２）。ＢＳＦはネットワークＨＬＲまたはＡｕＣからＭＴに対する認証情報を得る（５０４）。例えば、ＨＬＲ／ＡｕＣは、Ｋｉと共に、それぞれ３２ビットの出力ＳＲＥＳおよび６４ビットの出力Ｋｃを生ずるための２つのアルゴリズムＡ３およびＡ８への入力である１２８ビットのランダムなチャレンジＲＡＮＤを選択する。次に要求ＭＴのＳＩＭに対応する三個組（ＲＡＮＤ、ＳＲＥＳ、Ｋｃ）は要求ＭＴ内部のＳＩＭを認証するためにＢＳＦに提供される。ＢＳＦは次に乱数ＲＡＮＤ（ＨＬＲで生成される）および他のパラメータをチャレンジとしてＭＴに送る（５０６）。

【００４３】

ＭＴは、認証チャレンジがブートストラッピングサーバ証明書に基づいて、予想したＢ

ＳＦから発せられたかどうかを検証する（５０８）。例えば、この検証は、ＭＴにおいて供給されたＢＳＦの公開鍵またはデジタルサーバ証明書を用いて実行されるかもしれない。認証チャレンジが予想したＢＳＦから来ていない場合、処理は終了する。そうでなければ、チャレンジに対する認証応答はＭＴのＳＩＭによって提供された秘密鍵に基づいて構築される（５１０）。例えば、ＭＴは、事前共有秘密鍵Ｋｉおよび乱数ＲＡＮＤを用いてアルゴリズムＡ３およびＡ８によって１つ以上の秘密鍵（ＳＲＥＳとＫｃ）を計算するＳＩＭ（ＭＴ内）へ送る。次に、認証応答を構築するために秘密鍵ＳＲＥＳおよびＫｃをＭＴに送る。１つの実施態様において、メッセージ認証符号を計算するために、または認証応答の一部として送られる１つ以上のパラメータを導出もしくは暗号化するために、秘密鍵ＳＲＥＳおよびＫｃが用いられるかもしれない。

【００４４】

認証応答はＭＴからＢＳＦへ送られる（５１２）。次に、ＢＳＦは独立に得られた秘密鍵に基づいて認証応答の発信源を検証する（５１４）。例えば、ＨＬＲから得たＳＲＥＳとＫｃ（乱数ＲＡＮＤおよび事前共有秘密鍵Ｋｉに対応する三個組内）は、ＭＴからの認証応答における１つ以上のパラメータの有効性を確認するために用いられるかもしれない。例えば、ＢＳＦは、ＨＬＲから受信した乱数ＲＡＮＤ、ＳＲＥＳ、および／または、Ｋｃを用いてメッセージ認証符号（または、認証応答における他のパラメータ）を独立に計算するかもしれない。ＭＴとＢＳＦによって計算されたパラメータ（例えば、メッセージ認証符号）が合致する場合、認証応答の発信源が検証される。

【００４５】

代替的な実施態様において、ＭＴは１つ以上の秘密鍵（ＳＩＭから得られるＳＲＥＳおよびＫｃ）および他のパラメータ（認証チャレンジもしくは応答またはＳＩＭから得られる）を用いて第３の鍵を計算するかもしれない。この第３の鍵は、次に、認証応答を構築するために用いられる（例えば、メッセージ認証符号を計算する）。ＢＳＦは、ＭＴと同じ鍵および／またはパラメータが分かっているため、ＢＳＦも同じ鍵を計算するかもしれない。その結果、ＢＳＦは、認証応答がＭＴから発せられたかどうかを検証できる。

【００４６】

認証応答がいったん検証されると、ＢＳＦおよびＭＴは独立にＢＳＦとＭＴ双方に知られている１つ以上の鍵および／またはパラメータ（例えば、ＳＲＥＳ、Ｋｃおよび／または他のパラメータ）に基づいて共有鍵を計算する（５１６）。この共有鍵は、次に、ＭＴとＮＡＦの間の安全な通信またはトランザクションを確立するために、要求ＮＡＦへ提供することができる（５１８）。

【００４７】

ＭＴは公開鍵方式によってＢＳＦからの伝送を認証する。ＢＳＦはＭＴに乱数ＲＡＮＤを用いてチャレンジを送り、ＭＴからの伝送を認証するために、それが対応する秘密鍵ＳＲＥＳおよび／またはＫｃを所有することを確定する。このように、ＢＳＦおよびＭＴは、ブートストラッピングのために鍵を導出するかもしれない情報を共有するために相互に認証される。

【００４８】

図６に、１つの実施態様に従って、ネットワークアプリケーション機能に対して相互に安全に認証するために、ＧＳＭ準拠の移動端末６０８およびブートストラッピングサーバ機能６０４間でチャレンジ-応答プロトコルを実行する方法を示す。ＧＳＭの認証と鍵共有（ＡＫＡ）はチャレンジ応答プロトコルに基づく。レガシーＳＩＭに基づいてブートストラップするために、ＨＬＲ／ＡｕＣおよびＳＩＭは、既存の秘密鍵ＫｉおよびＧＳＭアルゴリズムＡ３およびＡ８に基づいて同様の計算を実行する。ＧＳＭプロトコルにおいて、秘密鍵Ｋｉ並びに認証アルゴリズムＡ３およびＡ８はネットワークＨＬＲ６０２と同様に、加入者識別モジュール（ＳＩＭ）スマートカードにも格納される。ＳＩＭ６０８は改竄防止となるように設計され、ユーザによって容易に読みだされないデータおよびアルゴリズムを含む。通常、秘密鍵Ｋｉおよび認証アルゴリズムＡ３およびＡ８は、ネットワークによる無線経由のサービスを確立するために用いられる。

【００４９】
一実施例において、認証鍵に対する要求は、ＭＴ６０６がＳＩＭ６０８から関連する国際移動加入者識別番号（ＩＭＳＩ）６００を検索し、それをブートストラッピングサーバ機能（ＢＳＦ）６０４に送ることによって開始されるかもしれない。ＢＳＦ６０４はＩＭＳＩ６００を、ＩＭＳＩ６００がネットワークに加入しているＭＴに属すかどうかを検証するかもしれないＨＬＲ６０２へ送る。ＨＬＲ６０２はＭＴ６０６内に加入者のＳＩＭが入っている加入者に対するサービスプロバイダによって動作されるかもしれない。ＨＬＲ６０２は、例えば、事前共有秘密鍵Ｋｉと共に１２８ビットのランダムなチャレンジＲＡＮＤを選択し、それらをそれぞれ署名された３２ビットの出力ＳＲＥＳおよび６４ビットの出力秘匿性鍵Ｋｃを生ずるための２つのアルゴリズムＡ３およびＡ８に対する入力として用いる。次に、ＨＬＲ６０２は、ＳＩＭ６０８の識別番号ＩＭＳＩ６００に対応する三個組（ＲＡＮＤ、ＳＲＥＳ、Ｋｃ）をＢＳＦ６０４へ送る。ＢＳＦ６０４は、ランダム秘密の指数ｘを生成し、ディフィー-ヘルマン公開鍵P^xを計算する。ここで、Ｐは予めＢＳＦ６０４およびＭＴ６０６の双方に供給された巡回群生成元である。巡回群は有限体の乗法群または楕円曲線の加法群のようなものである。次に、ＢＳＦ６０２はＭＴ６０６へ三個組（ＲＡＮＤ、P^x、ＳＩＧ）６１０を送る。ここで、ＳＩＧはＢＳＦ６０４のＲＳＡプライベート鍵を用いて計算されたディジタル署名である。メッセージ６１０は、トランザクション識別子のような他のサーバ認証されたパラメータを含むようにさらに機能強化されるかもしれない。

【００５０】
ＭＴ６０６は、三個組（ＲＡＮＤ、P^x、ＳＩＧ）６１０を受信し、ＳＩＧを検証するためにＢＳＦ６０４のディジタル証明書を用いる。ＭＴ６０６は、ＢＳＦ６０４から伝送されたデータを認証することができるようにディジタル証明書を供給されると仮定されている。データがＢＳＦで発せられたと見なされる場合、ＭＴ６０６は乱数ｙを生成し、P^yを計算する。また、ＭＴ６０６はＲＡＮＤ６１２をＳＩＭ６０８へ送る。ＳＩＭ６０８はＲＡＮＤおよびＫｉに基づいて生成される１組（ＳＲＥＳ、Ｋｃ）６１４をＭＴ６０６に返す。ＳＩＭ６０８が真正である場合、ＨＬＲ６０２によって生成したと同じＳＲＥＳおよびＫｃを生成するべきである。次にＭＴ６０６は、ＳＲＥＳおよびＫｃで鍵を掛けたP^yのメッセージ認証符号ＭＡＣを計算し、応答（P^y、ＭＡＣ）６１６をＢＳＦ６０４へ送る。この応答６１６は、トランザクション識別子のように、ＭＡＣが計算されるための他のパラメータを含むようにさらに機能強化されるかもしれない。

【００５１】
ＢＳＦ６０４は、P^yを受信し、ＨＬＲ６０２から認証用三個組で受信したＳＲＥＳとＫｃを用いてＭＡＣを検証する。このＭＡＣが正しい場合、ＢＳＦは、ＭＴ６０６が正しいＳＩＭ６０８を有していることを検証し、確認メッセージ６１８をＭＴ６０６へ送るかもしれない。

【００５２】
この実施例において、ＭＴ６０６およびＢＳＦ６０４は、このように相互認証されたディフィー-ヘルマンの鍵交換を実行し、それらがそれぞれ計算する鍵P^{xy}を共有する。次に、さらなる通信のための鍵は、例えば、ＭＴおよびＢＳＦ双方に知られている識別情報、ＲＡＮＤ、ＳＲＥＳ、およびＫｃのような更なる情報を含むP^{xy}のハッシュとして計算されるかもしれない。ＳＩＭ６０８ではなくＭＴ６０６内でディフィー-ヘルマンの計算が行われるか、または結果として得られる鍵が格納される場合には、この鍵P^{xy}および得られた共有鍵は、ＭＴからＳＩＭ６０８が外される場合、またはＭＴが異なるＳＩＭ６０８を用いて動作する場合には、削除されるべきである。

【００５３】
このプロトコルはＭＴ６０６がアルゴリズムＡ５／２をサポートしない場合には、ＧＳＭに起因する標準的弱点から保護することに注意のこと。Ａ５／２アルゴリズムは、ＧＳＭプロトコルにおいて上記プロトコルを密かに攻撃するかもしれないほぼ瞬時の中断を許している。しかし、Ａ５／２アルゴリズムは３ＧＰＰリリース６仕様において段階的に廃

止されることになる。

【００５４】

プロトコルの攻撃を試みる中間者はＳＩＧ故に最初のチャレンジ（ＲＡＮＤ、Ｐ、ＳＩＧ）を変えることができず、攻撃するものはそれ自身のP^zの挿入または異なるＲＡＮＤの使用ができないことにさらに注意のこと。これは、これらのメッセージを再実行しかできないかもしれないが、どんな再実行も、一時的ディフィー-ヘルマンを用いるのと同等であるため、それはＢＳＦになりすますことはできない。逆に、ＢＳＦが、用いられたＲＡＮＤがこのプロトコルの１つの使用から次の使用までフレッシュであることを保証し、かつ応答（P^y、ＭＡＣ）が短時間の間だけ受信されることを保証する場合、攻撃側には、通常のＧＳＭシナリオにおけるＲＡＮＤによるチャレンジを行い、鍵を導出するＡ５／１アルゴリズムを攻撃するような他の手段によって、ＳＲＥＳおよびＫｃを導出する機会がない。

【００５５】

図７に、１つの実施態様に従って、相互に安全に認証し、ネットワークアプリケーション機能（ＮＡＦ）に対する鍵を共有するために、ＧＳＭ準拠の加入者識別モジュール（ＳＩＭ）７０８をサポートするレガシー移動端末（ＭＴ）７０６とブートストラッピングサーバ機能（ＢＳＦ）７０４間でチャレンジ-応答プロトコルを実行する代替的方法を示す。図６の方法と同様に、認証鍵に対する要求は、その関連ＩＭＳＩ７００をＳＩＭ７０８からＢＳＦ７０４へ送るＭＴ７０６によって開始されるかもしれない。ＢＳＦ７０４は、ＩＭＳＩ７００を、ＩＭＳＩ７００がネットワークに加入するＭＴに属すかどうかを検証できるＨＬＲ７０２へ送る。次に、ＨＬＲ７０２はＳＩＭ７０８の識別番号ＩＭＳＩ７００に対応する三個組（ＲＡＮＤ、ＳＲＥＳ、Ｋｃ）を選択し、ＢＳＦ７０４へ送る。例えば、ＲＡＮＤは１２８ビットの乱数であるかもしれない。また、Ｋｉは事前共有秘密保全鍵Ｋｉであり、それらは、それぞれ署名した応答ＳＲＥＳ（例えば３２ビットの数）および秘匿性鍵Ｋｃ（例えば６４ビットの数）を生ずる２つのアルゴリズムＡ３およびＡ８に対する入力として用いられる。ＭＴ７０６は、ＢＳＦ７０４から伝送されたデータの認証を可能にする公開鍵またはディジタル証明書が供給されると仮定されている。

【００５６】

ＢＳＦ７０４はＨＬＲ７０２から三個組（ＲＡＮＤ、ＳＲＥＳ、Ｋｃ）を受信する。次にＢＳＦ７０４は、ＭＴ７０６がＢＳＦ７０４から受信したデータの送信源を認証することを可能にする公開鍵ベースの方式を用いてＲＡＮＤ（および、タイムスタンプ、シーケンス番号、ランダムシードまたは識別情報などの他のパラメータかもしれない）のディジタル署名ＳＩＧを計算する。ＢＳＦ７０４はＲＡＮＤおよびＳＩＧ７１０をＭＴ７０６へ送る。ＭＴ７０６は、（ＲＡＮＤ、ＳＩＧ）７１０を受信すると、ＢＳＦ７０４のディジタル証明書を用いてＳＩＧを検証する。データがＢＳＦ７０４からであると見なされる場合、ＭＴ７０６は、ＲＡＮＤ７１２をＳＩＭ７０８に送り、対応するパラメータＳＲＥＳおよびＫｃを検索する。すなわち、ＳＩＭ７０８は、事前共有秘密鍵ＫｉおよびＲＡＮＤを、供給されているＡ３およびＡ８アルゴリズムの入力として用いて、ＳＲＥＳとＫｃの組を生成する。次にＭＴ７０６は、公開鍵ベースの方式の下でＰＳＫを暗号化して、鍵ＰＳＫを生成し、メッセージ認証符号ＭＡＣをその結果に適用するかもしれない。タイムスタンプ、シーケンス番号、ランダムシードまたは識別情報のようなさらなるパラメータが応答に含まれるかもしれない。ＭＡＣは、入力パラメータとしてＫｃおよびＳＲＥＳを含むかもしれない機能またはアルゴリズム（ＭＴ７０６およびＢＳＦ７０４双方に既知）に基づくかもしれない。またＭＡＣはＭＴ７０６が正当なＳＩＭ７０８を処理することをＢＳＦ７０４に証明するために用いられる。データならびにＳＲＥＳおよびＫｃで鍵を掛けられたＭＡＣの公開鍵ベース暗号化の操作はいずれの順番でも実行されるかもしれないことに注意のこと。次に、ＭＴ７０６は（暗号化されたＰＳＫ、ＭＡＣ）７１６をＢＳＦ７０４に送る。ＢＳＦ７０４はＭＴ７０６が正しいＳＲＥＳおよびＫｃを有していることを、ＭＡＣを検証することにより検証する。ＭＡＣのこの検証は、ＭＡＣを再計算しそれをＭＴ７０６から受信したＭＡＣと比較するために、ＢＳＦ７０４によってＨＬＲ７０２か

ら受信されたＳＲＥＳおよびＫｃを用いてなされる。ＭＡＣが正しいと見なされる場合、ＰＳＫはＭＴ７０６およびＳＩＭ７０８から発せられていると見なされ、確認または肯定応答７１８がＭＴ７０６へ送られる。このように、このＰＳＫはＭＴ７０６およびＢＳＦ７０４の間で共有され、または更なる鍵導出がＰＳＫ、Ｋｃ、ＳＲＥＳ、識別情報、および場合によっては他のパラメータを用いてなされるかもしれない。

【００５７】

図６および７に示したＧＳＭベースの移動端末用のチャレンジ-応答方式は他の形式の移動端末でも実施されるかもしれない。例えば、本発明はＣＤＭＡ２０００準拠のネットワークおよび移動端末（ＭＴ）で使用できるかもしれない。そのような実施態様において、ＣＤＭＡ２０００準拠の移動端末は、ネットワークアプリケーションのセキュリティに用いることができる事前共有秘密鍵を共有するためのｃｄｍａ２０００認証モジュール、ＵＴＭまたはＲＵＩＭを含む。１実施例において、事前共有鍵は、認証されたディフィー-ヘルマンアルゴリズムを用いて生成される。ここで、ＢＳＦによって提供される公開パラメータP^xは公開鍵ディジタル署名方式（すなわち、ＭＴに既知のブートストラッピングサーバ証明書）によって認証される。一方ＭＴによって提供されたパラメータP^yは、ＣＡＶＥ（セルラ認証および音声暗号化アルゴリズム）からのＳＭＥＫＥＹ（信号メッセージ暗号化鍵）またはＭＮ-ＡＡＡ認証符号（移動ノード認証、許可および課金）のような要素で鍵を掛けられたメッセージ認証符号を加えることによって認証される。ＭＴは、ＢＳＦからのディジタル署名したメッセージおよび事前共有秘密鍵Ｋｉを認証できるようにする公開鍵またはディジタル証明書を供給されると仮定される。また認証符号識別番号ＩＭＳＩは認証符号モジュールおよびＨＬＲ双方に既知であると仮定される。

【００５８】

当業者は、この方法はベアラの認証がＣＡＶＥに基づいている環境に等しくに適用されることを理解するだろう。また本方法がこれらのブートストラッピング動作が全体に対称およびＲＳＡ操作を用いて実行されるかもしれず、またこれによりディフィー-ヘルマンおよびＲＳＡ双方のサポートを必要とするプロトコルより優れた実施を提供するかもしれないという利点を提供することを理解するだろう。

【００５９】

図１、２、および／または３に示す１つ以上の部品および機能は、本発明から逸脱することなく再配列および／または１つの部品に結合されるかまたは複数の部品で具体化されるかもしれない。また、付加的要素または部品が本発明から逸脱することなく加えられるかもしれない。図１、２、および／または３に示す機器、装置、および／または部品は、図４、５、６および／または、７に示す方法、特徴、またはステップを実行するように構成されるかもしれない。

【００６０】

上述の実施例は単に例であり、本発明を限定するように解釈されるべきでないことに注意するべきである。実施例の記述は例示的であるように意図されており、特許請求の範囲を限定するように意図されていない。そのように、本教示は他の形式の装置に容易に適用することができ、また多くの代替手段、変更、および変形は当業者に明らかだろう。

【図面の簡単な説明】

【００６１】

【図１】１実施態様に従ってブートストラッピングサーバおよびレガシー移動端末が互いに相互認証できる通信システムを示すブロック図。

【図２】１実施態様に従って通信ネットワーク上で動作するブートストラッピングサーバ機能と相互認証を実行するように構成された移動端末を示すブロック図。

【図３】１実施態様に従って移動局を認証するためにブートストラッピングサーバ機能を実行するように構成されたネットワーク装置を示すブロック図。

【図４】１実施態様に従ってレガシー移動端末とブートストラッピングサーバ機能を相互認証するチャレンジ-応答方式を実行する方法。

【図５】１実施態様に従ってブートストラッピングサーバ機能およびそのサーバ機能の認

証を用いて移動端末を認証する一般的方法。
【図６】１実施態様に従ってネットワークアプリケーション機能に対して相互に安全に認証するための、ＧＳＭ準拠の移動端末とブートストラッピングサーバ機能間でチャレンジ-応答プロトコルを実行する方法。
【図７】１実施態様に従ってネットワークアプリケーション機能に対して相互に安全に認証するための、ＧＳＭ準拠の移動端末とブートストラッピングサーバ機能間でチャレンジ-応答プロトコルを実行する代替的方法。

【図１】

図 1

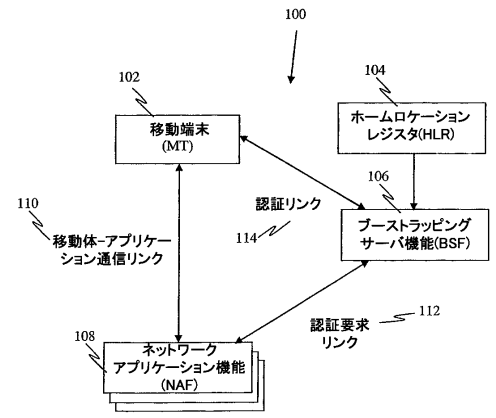

Figure 1

【図２】

図 2

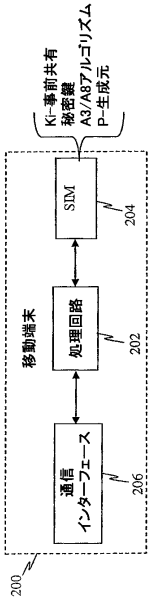

Figure 2

【図３】

図３

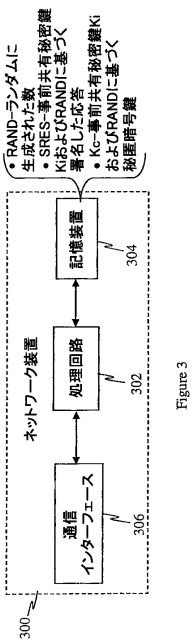

Figure 3

【図４】

図４

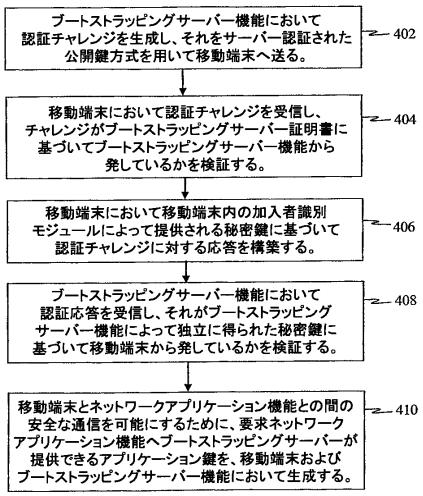

Figure 4

【図５】

図５

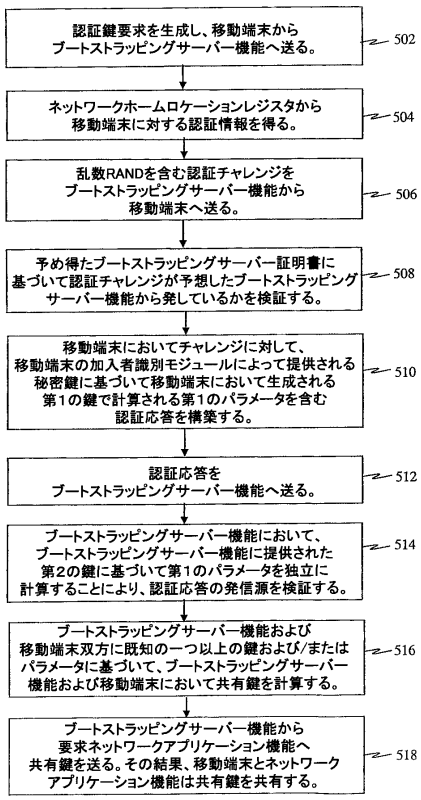

Figure 5

【図６】

図６

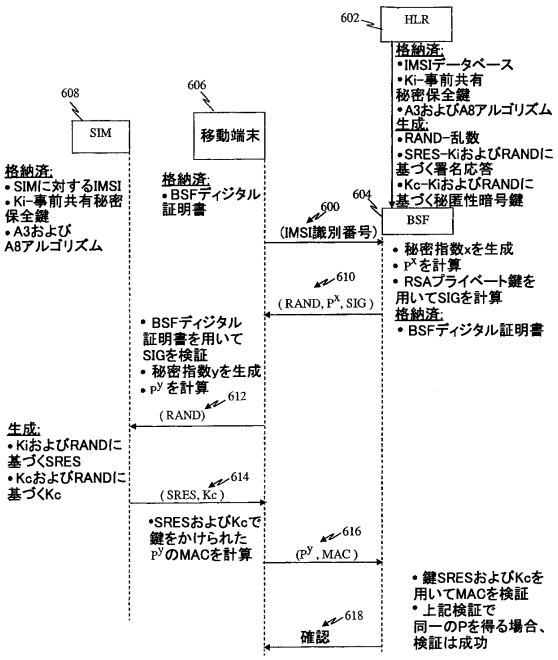

Figure 6

【図７】

図 7

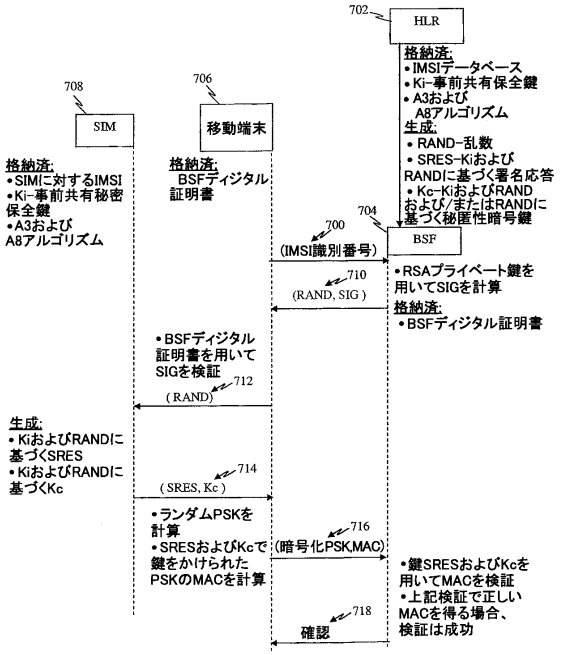

Figure 7

フロントページの続き

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(72)発明者 ローズ、グレゴリー・ゴードン
アメリカ合衆国、カリフォルニア州 ９２１１７、サン・ディエゴ、ノース・スター・ドライブ ３２３４
(72)発明者 センプル、ジェームズ
イギリス国、エスダブリュ７・５エヌユー、ロンドン・グレイター・ロンドン、クイーンズゲイト・プレイス ７、ナンバー４
(72)発明者 ナシールスキー、ジョン・ウォレイス
アメリカ合衆国、カリフォルニア州 ９２１２９、サン・ディエゴ、エルフォード・コート ８７１９

審査官 石田 信行

(56)参考文献 特表２００２－５１６５２１（ＪＰ，Ａ）
特表２００７－５２８６５０（ＪＰ，Ａ）
特表２００５－５１５７０１（ＪＰ，Ａ）
特開２００３－００５６４１（ＪＰ，Ａ）
特表平１１－５０５３８４（ＪＰ，Ａ）
特表平１０－５１０６９２（ＪＰ，Ａ）
特開平０７－１９３５６９（ＪＰ，Ａ）
3GPP TS 33.220 V1.1.0, ２００４年 2月 9日, P1-17

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
H04W 12/06