(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5036099号
(P5036099)
(45)発行日　平成24年9月26日(2012.9.26)　(24)登録日　平成24年7月13日(2012.7.13)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601B
H04B 7/26 (2006.01)　　H04B 7/26

請求項の数 13　(全 19 頁)

(21)出願番号　特願2001-19495(P2001-19495)
(22)出願日　平成13年1月29日(2001.1.29)
(65)公開番号　特開2001-251292(P2001-251292A)
(43)公開日　平成13年9月14日(2001.9.14)
審査請求日　平成19年12月21日(2007.12.21)
(31)優先権主張番号　09/500869
(32)優先日　平成12年2月9日(2000.2.9)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　596092698
アルカテル－ルーセント　ユーエスエー　インコーポレーテッド
アメリカ合衆国　０７９７４　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００－７００
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100106183
弁理士　吉澤　弘司

最終頁に続く

(54)【発明の名称】通信鍵を更新する方法

(57)【特許請求の範囲】
【請求項１】
通信システム（６５）と通信する装置（６４）に維持される通信鍵（ＳＳＤ）を更新する方法において、該装置（６４）は、
該装置（６４）に記憶された秘密値（Ａ－ＫＥＹ）を用いて新しい通信鍵（ＳＳＤ－ＮＥＷ）を生成するステップと、
該装置（６４）に記憶された該秘密値（Ａ－ＫＥＹ）を用いて更新鍵（ＳＳＤ－ＫＥＹ）を生成するステップと、
該更新鍵（ＳＳＤ－ＫＥＹ）を使用して署名値（ＡＵＴＨＢＳ）を生成するステップと、
ホーム通信システム（７０）から在圏通信システム（７１）に新しい通信鍵（ＳＳＤ－ＮＥＷ）を送信することなく該新しい通信鍵（ＳＳＤ－ＮＥＷ）をホーム通信システム（７０）にとどめておきながら、該通信システム（６５）の該ホーム通信システム（７０）から在圏通信システム（７１）で受信された更新鍵（ＳＳＤ－ＫＥＹ）を使用して該在圏通信システム（７１）によって生成され、該通信システム（６５）の該在圏通信システム（７１）から受信された署名値（ＡＵＴＨＢＳ）と、該装置（６４）において生成された該署名値（ＡＵＴＨＢＳ）とを比較するステップと、
該比較の結果に基づいて、該通信鍵（ＳＳＤ）を該新しい通信鍵（ＳＳＤ－ＮＥＷ）で更新するステップとを実行するように適合されていることを特徴とする、通信システム（６５）と通信する装置（６４）に維持される通信鍵（ＳＳＤ）を更新する方法。

【請求項２】
請求項１記載の方法において、該装置（６４）は、さらに、
更新シーケンス（ＲＡＮＤＳＳＤ）を受信するステップと、
該装置（６４）に記憶された秘密値（Ａ－ＫＥＹ）及び該シーケンス（ＲＡＮＤＳＳＤ）を用いて該新しい通信鍵（ＳＳＤ－ＮＥＷ）を生成するステップとを実行するように適合されていることを特徴とする方法。
【請求項３】
請求項２記載の方法において、該装置（６４）は、さらに、
チャレンジシーケンス（ＲＡＮＤＢＳ）を生成するステップと、
該チャレンジシーケンス（ＲＡＮＤＢＳ）を該在圏通信システム（７１）へ送信するステップと、
該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて該署名値（ＡＵＴＨＢＳ）を生成するステップと、
該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて該在圏通信システム（７１）によって生成された署名値（ＡＵＴＨＢＳ）を受信するステップと、
該署名値（ＡＵＴＨＢＳ）を、該在圏通信システム（７１）によって生成された該署名値（ＡＵＴＨＢＳ）と比較するステップとを実行するように適合されていることを特徴とする方法。
【請求項４】
請求項３記載の方法において、該装置（６４）は、さらに、
該更新シーケンス（ＲＡＮＤＳＳＤ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて第２署名値（ＡＵＴＨＳＳＤ）を生成するステップと、
該第２署名値（ＡＵＴＨＳＳＤ）を、該ホーム通信システム（７０）で生成された該シーケンス（ＲＡＮＤＳＳＤ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて該在圏通信システム（７１）によって生成された第２署名値（ＡＵＴＨＳＳＤ）と比較するために、該在圏通信システム（７１）へ送信するステップとを実行するように適合されていることを特徴とする方法。
【請求項５】
請求項３記載の方法において、
該署名値（ＡＵＴＨＢＳ）を生成するステップは、
該更新シーケンス（ＲＡＮＤＳＳＤ）、該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）の少なくとも一部を含む署名ストリングを形成するステップと、
少なくとも該署名ストリングから該署名値（ＡＵＴＨＢＳ）を生成するステップとを有することを特徴とする方法。
【請求項６】
請求項４記載の方法において、
該第２署名値（ＡＵＴＨＳＳＤ）を生成するステップは、
該更新シーケンス（ＲＡＮＤＳＳＤ）、該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）の少なくとも一部を含む第２署名ストリングを形成するステップと、
少なくとも該第２署名ストリングから該第２署名値（ＡＵＴＨＢＳ）を生成するステップとを有することを特徴とする方法。
【請求項７】
装置（６４）及び通信システム（６５）に維持される通信鍵（ＳＳＤ）を更新する方法において、在圏通信システム（７１）は、
ホーム通信システム（７０）から該在圏通信システム（７１）に新しい通信鍵（ＳＳＤ－ＮＥＷ）を送信することなく該新しい通信鍵（ＳＳＤ－ＮＥＷ）をホーム通信システム（７０）にとどめておきながら、該ホーム通信システム（７０）内に記憶され該装置（６

４）と関連している秘密値（Ａ－ＫＥＹ）を使用して該ホーム通信システム（７０）が求めた更新シーケンス（ＲＡＮＤＳＳＤ）と更新鍵（ＳＳＤ－ＫＥＹ）とを該ホーム通信システム（７０）から該在圏通信システム（７１）で受信するステップと、
秘密値（Ａ－ＫＥＹ）を用いて該装置（６４）で新しい通信鍵（ＳＳＤ－ＮＥＷ）を生成するために該装置（６４）のための該更新シーケンス（ＲＡＮＤＳＳＤ）を該在圏通信システム（７１）によって該装置（６４）へ送信するステップと、
該ホーム通信システム（７０）が求めた該更新鍵（ＳＳＤ－ＫＥＹ）を使用して該在圏通信システム（７１）で署名値（ＡＵＴＨＢＳ）を生成するステップと、
該装置（６４）が、該装置（６４）に記憶されている秘密値（Ａ－ＫＥＹ）を使用して該装置（６４）が生成した更新鍵（ＳＳＤ－ＫＥＹ）を用いて該装置（６４）で生成された署名値（ＡＵＴＨＢＳ）と比較するために、該在圏通信システム（７１）で生成された該署名値（ＡＵＴＨＢＳ）を該在圏通信装置（７１）によって該装置（６４）へ送信するステップと、
該比較の結果に応じて更新確認（７７）を受信するステップとを実行するように適合されていることを特徴とする、装置（６４）及び通信システム（６５）に維持される通信鍵（ＳＳＤ）を更新する方法。

【請求項８】
請求項７記載の方法において、該在圏通信システム（７１）は、さらに、
該装置（６４）からチャレンジシーケンス（ＲＡＮＤＢＳ）を受信するステップと、
該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて該署名値（ＡＵＴＨＢＳ）を生成するステップとを実行するように適合されていることを特徴とする方法。

【請求項９】
請求項８記載の方法において、該在圏通信システム（７１）は、さらに、
該更新シーケンス（ＲＡＮＤＳＳＤ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて第２署名値（ＡＵＴＨＳＳＤ）を生成するステップと、
該更新シーケンス（ＲＡＮＤＳＳＤ）及び該更新鍵（ＳＳＤ－ＫＥＹ）を用いて該装置（６４）で生成された第２署名値（ＡＵＴＨＳＳＤ）を受信するステップと、
該第２署名値（ＡＵＴＨＳＳＤ）を、該装置（６４）によって生成された第２署名値（ＡＵＴＨＳＳＤ）と比較するステップとを実行するように適合されていることを特徴とする方法。

【請求項１０】
請求項９記載の方法において、
該署名値（ＡＵＴＨＢＳ）を生成するステップは、
該更新シーケンス（ＲＡＮＤＳＳＤ）、該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）の少なくとも一部を含む署名ストリングを形成するステップと、
少なくとも該署名ストリングから該署名値（ＡＵＴＨＢＳ）を生成するステップとを有することを特徴とする方法。

【請求項１１】
請求項９記載の方法において、
該第２署名値（ＡＵＴＨＳＳＤ）を生成するステップは、
該更新シーケンス（ＲＡＮＤＳＳＤ）、該チャレンジシーケンス（ＲＡＮＤＢＳ）及び該更新鍵（ＳＳＤ－ＫＥＹ）の少なくとも一部を含む第２署名ストリングを形成するステップと、
少なくとも該第２署名ストリングから該第２署名値（ＡＵＴＨＢＳ）を生成するステップとを有することを特徴とする方法。

【請求項１２】
装置（６４）及び通信システム（６５）に維持される通信鍵（ＳＳＤ）を更新する方法において、ホーム通信システム（７０）は、

更新シーケンス（ＲＡＮＤＳＳＤ）を生成するステップと、
該ホーム通信システム（７０）に記憶された該装置（６４）に関連する秘密値（Ａ－ＫＥＹ）を用いて新しい通信鍵（ＳＳＤ－ＮＥＷ）を該ホーム通信システム（７０）によって生成するステップと、
該秘密値（Ａ－ＫＥＹ）を用いて更新鍵（ＳＳＤ－ＫＥＹ）を該ホーム通信システム（７０）によって生成するステップと、
該在圏通信システム（７１）が、該ホーム通信システム（７０）が求めた更新鍵（ＳＳＤ－ＫＥＹ）を使用して署名値（ＡＵＴＨＢＳ）を生成して、該装置（６４）に記憶されている秘密値（Ａ－ＫＥＹ）を使用して該装置（６４）で生成された更新鍵（ＳＳＤ－ＫＥＹ）を使用して該装置（６４）で生成された署名値（ＡＵＴＨＢＳ）との比較のために該在圏通信システム（７１）が生成した該署名値（ＡＵＴＨＢＳ）を該装置（６４）に送信するために、該ホーム通信システム（７０）から該在圏通信システム（７１）に該新しい通信鍵（ＳＳＤ－ＮＥＷ）を送信することなく該新しい通信鍵（ＳＳＤ－ＮＥＷ）を該ホーム通信システム（７０）にとどめておきながら、該ホーム通信システム（７０）から該在圏通信システム（７１）に該更新鍵（ＳＳＤ－ＫＥＹ）を送信するステップと、
該比較の結果に応じて、該通信鍵（ＳＳＤ）を該新しい通信鍵（ＳＳＤ－ＮＥＷ）で更新するステップとを実行するように適合されていることを特徴とする、装置（６４）及びホーム通信システム（７０）に維持される通信鍵（ＳＳＤ）を更新する方法。
【請求項１３】
装置（６４）及びホーム通信システム（７０）に維持される通信鍵（ＳＳＤ）を更新する方法において、
該装置（６４）が秘密値（Ａ－ＫＥＹ）を用いて該装置（６４）で新しい通信鍵（ＳＳＤ－ＮＥＷ）を生成するために、更新シーケンス（ＲＡＮＤＳＳＤ）を該ホーム通信システム（７０）から該装置（６４）で受信するステップと、
該装置（６４）に関連する秘密値（Ａ－ＫＥＹ）を用いて該ホーム通信システム（７０）で生成された更新鍵（ＳＳＤ－ＫＥＹ）を該ホーム通信システム（７０）から在圏通信システム（７１）で受信するステップと、
該ホーム通信システム（７０）が求めた該更新鍵（ＳＳＤ－ＫＥＹ）を使用して署名値（ＡＵＴＨＢＳ）を該在圏通信システム（７１）によって生成するステップと、
該更新鍵（ＳＳＤ－ＫＥＹ）を使用して署名値（ＡＵＴＨＢＳ）を該装置（６４）で生成するステップと、
該ホーム通信システム（７０）から該在圏通信システム（７１）に新しい通信鍵（ＳＳＤ－ＮＥＷ）を送信することなく該新しい鍵（ＳＳＤ－ＮＥＷ）を該ホーム通信システム（７０）にとどめておきながら、該在圏通信システム（７１）によって生成され該通信システム（６５）の該在圏通信システム（７１）から受信した署名値（ＡＵＴＨＢＳ）と該装置（６４）によって生成された署名値（ＡＵＴＨＢＳ）とを、該装置（６４）で比較するステップと、
該比較の結果を該装置（６４）から該ホーム通信システム（７０）へ送信するステップとを有することを特徴とする、装置（６４）及びホーム通信システム（７０）に維持される通信鍵（ＳＳＤ）を更新する方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、通信に関し、特に、通信当事者によって使用される鍵（キー）などの情報の更新に関する。
【０００２】
【従来の技術】
通常のワイヤレス通信システムは、ある地域内のワイヤレス装置にワイヤレス通信サービスを提供する。移動通信交換センタ（ＭＳＣ）は、とりわけ、ワイヤレス装置どうしの間の呼、および、ワイヤレス装置とワイヤライン（固定電話）装置との間の呼を確立し維持

する。このため、ＭＳＣは、その地域内のワイヤレス装置を公衆交換電話網と相互接続する。ＭＳＣによってサービスされる地域は、「セル」と呼ばれる空間的に相異なる領域に分けられる。各セルは、蜂の巣パターンの１個の六角形によって模式的に表されるが、実際には、各セルは、セルの周囲の地形に依存する不規則な形状を有する。通常、各セルは１個の基地局（ＢＳ）を有する。基地局は、そのセル内のワイヤレス装置と通信するために使用する無線機およびアンテナを有する。また、基地局は、その地域内のＭＳＣと通信するために使用する伝送装置を有する。

【０００３】

ＭＳＣは、信号網（シグナリングネットワーク）を使用する。信号網により、それぞれの地理的サービスエリア内のワイヤレス装置に関して、位置検証や、他の地理的サービスエリア内でローミングしているワイヤレス装置への呼配送のための情報の交換が可能となる。ワイヤレス装置がワイヤレス通信システムと通信しようとするとき、ワイヤレス通信システムは、そのワイヤレス装置がワイヤレス通信システムにアクセスするのを可能にする前に、そのワイヤレス装置の識別を認証あるいは確認する。図１に、通常のワイヤレス通信システム５の一部を示す。ワイヤレス通信システム５は、基地局１０を通じて、基地局１０に対応するセルやセクタのような地理的領域１２にワイヤレス通信サービスを提供する。まず、セル１２内のワイヤレス装置１４が、基地局１０に登録する（基地局１０との通信しようとする）とき、ワイヤレス装置１４がワイヤレス通信システムにアクセスすることが可能になる前に、ワイヤレス装置１４は認証される（ワイヤレス装置の識別が確認される）。ワイヤレス装置１４のホームネットワークあるいはホーム通信システムは、ワイヤレス装置１４が存在するセルラ地理的サービスエリアを構成するセルの集まりとすることが可能であり、通常、ワイヤレス通信サービスを提供するためにワイヤレス装置の所有者と契約しているサービスプロバイダによって制御されるネットワークである。ワイヤレス装置１４がそのホームネットワーク以外のネットワーク内にあるとき、そのネットワークを在圏通信ネットワーク（あるいは在圏通信システム）という。ワイヤレス装置１４が在圏通信システムで動作している場合、基地局１０によるワイヤレス装置の認証は、そのワイヤレス装置のホーム通信システムのホーム認証センタ１６との通信を伴う。ホーム認証センタ１６は、独立（スタンドアローン）のセンタであることも可能であり、あるいは、ホーム通信システムのＭＳＣ（ホームＭＳＣ）に接続、付属、統合あるいはこれと同じ場所に配置することも可能である。また、在圏認証センタ１８は、独立（スタンドアローン）のセンタであることも可能であり、あるいは、在圏通信システムのＭＳＣ（在圏ＭＳＣ）に接続、付属、統合あるいはこれと同じ場所に配置することも可能である。

【０００４】

図１の例では、ワイヤレス装置１４は、在圏通信システム内にある。その結果、ワイヤレス装置１４の認証は、ワイヤレス装置のホーム通信システムのホーム認証センタとの通信を伴う。ワイヤレス装置１４が在圏通信システムにアクセスしようとすると、基地局１０は、在圏通信システムの在圏認証センタ１８と通信する。在圏認証センタ１８は、ワイヤレス装置１４の電話番号のようなワイヤレス装置（端末）識別子から、ワイヤレス装置１４がホーム認証センタ１６を使用するシステムに登録していると判断する。次に、在圏認証センタ１８は、（例えばＩＳ－４１(TIA/EIA-41-D, "Cellular Radiotelecommunications Intersystem Operations", December 1997)で指定される標準の下で）信号網２０のようなネットワークを通じてホーム認証センタ１６と通信する。

【０００５】

次に、ホーム認証センタ１６は、ワイヤレス装置１４の登録エントリを有するホームロケーションレジスタ（ＨＬＲ）２２にアクセスする。ホームロケーションレジスタ２２は、ワイヤレス装置の電話番号のような識別子によってワイヤレス装置と関連づけられることが可能である。ホームロケーションレジスタ２２に保有される情報は、ワイヤレス装置と通信システムの間の通信の安全性（セキュリティ）を高めるために使用される共有秘密データ（ＳＳＤ：shared secret data）あるいは秘密鍵のような、認証鍵あるいは暗号化鍵を有することができ、あるいはそれを生成するために使用される。通常のワイヤレス通信

システムでは、ワイヤレス装置とワイヤレス通信システムの両方が、Ａ－ＫＥＹと呼ばれる秘密値を有する。ワイヤレス通信システムは、Ａ－ＫＥＹと、ランダムに生成されたシーケンス（列）ＲＡＮＤＳＳＤとを用いて、共有秘密データ（ＳＳＤ）値すなわち通信鍵を生成する。通信鍵ＳＳＤは、さまざまな機能を有する複数の通信鍵、例えば、認証鍵ＳＳＤ－Ａ（共有秘密データＡ）と暗号化鍵ＳＳＤ－Ｂ（共有秘密データＢ）、に分割することができる。ＳＳＤ－Ａ値は、認証手続きに使用され、ＳＳＤ－Ｂ値は、鍵生成および暗号化手続きに使用される。

【０００６】

在圏通信システムにアクセスしようとしているワイヤレス装置１４を認証するには、ホーム通信システムが、乱数列（チャレンジ）ＲＡＮＤのような情報を在圏通信システムに供給し、在圏通信システムは、乱数ＲＡＮＤをワイヤレス装置１４に送信して、ワイヤレス装置１４が、認証鍵（ＳＳＤ－Ａ）と乱数ＲＡＮＤを用いて導出した署名値ＡＵＴＨＲで応答することができるようにする。ホーム通信システムが在圏通信システムと通信鍵を共有しない場合、ワイヤレス装置によって生成される署名値ＡＵＴＨＲが、装置１４と同様にホーム通信システムで生成される署名値ＡＵＴＨＲと比較するために、ホーム通信システムへ送信される。これらの署名値が一致した場合、ワイヤレス装置１４は認証されたことになる。

【０００７】

ホーム認証センタ１６は、通信鍵値ＳＳＤを更新する必要があると判断した場合（例えばある判断基準により、ＳＳＤが漏洩された可能性があることが示された場合）、ワイヤレス装置１４に関連するＳＳＤ値を更新することができる。図２に、ワイヤレス装置とワイヤレス通信システムとの間での、ＩＳ－９５Ｂ(TIA/EIA-95-B, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Systems")で指定される標準によるＳＳＤ更新手続きを示す。ワイヤレス通信システムは、サービス基地局、在圏認証センタ、在圏ロケーションレジスタ。ホーム認証センタ、ホームロケーションレジスタ、在圏ＭＳＣあるいはホームＭＳＣを有することが可能である。

【０００８】

この例で鍵更新を開始するため、ホーム認証センタ１６は、更新シーケンスＲＡＮＤＳＳＤを作成する。ホーム認証センタ１６は、ＲＡＮＤＳＳＤ、Ａ－ＫＥＹおよびワイヤレス装置のＥＳＮを、ＳＳＤ生成手続き３０のような暗号化関数への入力として使用して、新しい鍵値（ＳＳＤ－ＮＥＷ）を生成する。ホーム認証センタは、在圏認証センタおよびサービス基地局を通じて、ＳＳＤ更新メッセージ３２のような更新メッセージでＲＡＮＤＳＳＤシーケンスをワイヤレス装置１４へ送る。ワイヤレス装置１４は、通信システムから受信したＲＡＮＤＳＳＤシーケンスを提供し、通信システムと同様にして新しい通信鍵を生成する。例えば、ワイヤレス装置１４は、ＲＡＮＤＳＳＤ、Ａ－ＫＥＹおよび電子シリアル番号（ＥＳＮ）（これらはワイヤレス装置に記憶される）を、ＳＳＤ鍵生成手続き３４のような暗号化関数に提供する。ＳＳＤ鍵生成手続き３４は、ＳＳＤ－ＮＥＷを生成し、これは、ＳＳＤ－Ａ－ＮＥＷとＳＳＤ－Ｂ－ＮＥＷに分割される。ＳＳＤ生成手続き３０および３４は、乱数ＲＡＮＤＳＳＤ、ＥＳＮおよび値Ａ－ＫＥＹを入力として使用するＣＡＶＥアルゴリズムを実装している。ＣＡＶＥアルゴリズムは、出力が与えられても関数への入力の決定ができない一方向性関数として当業者に周知である。

【０００９】

新しいＳＳＤ値を認証および暗号化手続きで使用することを受け入れる前に、ワイヤレス装置は、ＳＳＤ－ＮＥＷを検証することにより、通信システムを認証する。これを行うため、ワイヤレス装置は、ブロック３６で、乱数ＲＡＮＤＢＳチャレンジを生成する。ワイヤレス装置は、ＲＡＮＤＢＳおよびＳＳＤ－Ａ－ＮＥＷを、ＥＳＮや、国際移動局識別番号（ＩＭＳＩ：international mobile station identification number）から導出されるＡＵＴＨ＿ＤＡＴＡストリングのような付加データとともに、署名手続き３８のような暗号化関数に提供する。署名手続き３８は、署名値ＡＵＴＨＢＳを生成する。また、ワイヤレス装置は、ＲＡＮＤＢＳを、例えば基地局チャレンジ３７の一部として、ワイヤレス通

信システムにも送る。ワイヤレス通信システムは、署名手続き４０のような対応する暗号化関数を使用して、ワイヤレス装置からのＲＡＮＤＢＳと、ＳＳＤ生成手続き３０からのＳＳＤ－Ａ－ＮＥＷと、ＡＵＴＨＢＳを導出するためにワイヤレス装置により使用されるＥＳＮやＡＵＴＨ＿ＤＡＴＡのような付加データとを用いて、ＡＵＴＨＢＳを導出する。

【００１０】

ワイヤレス通信システムは、署名手続き４０によって生成されたＡＵＴＨＢＳ値を、例えば基地局チャレンジ確認命令４１で、ワイヤレス装置へ送る。ブロック４２で、ワイヤレス装置は、ワイヤレス装置で生成したＡＵＴＨＢＳ値を、システムから送信されたＡＵＴＨＢＳ値と比較する。この比較で一致した場合、ワイヤレス装置１４は、直接にＳＳＤ－ＮＥＷを検証したことにより、通信システムを認証したことになる。ワイヤレス装置１４は、ＳＳＤ－Ａ値をＳＳＤ－Ａ－ＮＥＷとし、ＳＳＤ－Ｂ値をＳＳＤ－Ｂ－ＮＥＷとする。その後、ワイヤレス装置は、ＳＳＤ更新の正常終了を示すＳＳＤ更新確認４３をホーム認証センタへ送る。ホーム認証センタは、ＳＳＤ更新確認を受信すると、ＳＳＤ－ＡおよびＳＳＤ－Ｂを、システムによって生成されたＳＳＤ－Ａ－ＮＥＷおよびＳＳＤ－Ｂ－ＮＥＷの値とする。

【００１１】

ＳＳＤ更新手続きの後、ワイヤレス通信システムは、通常、新しいＳＳＤ鍵値の正当性を確かめるために（例えば、ワイヤレスシステムが新しいＳＳＤ鍵を正しく計算したことを確かめるために）、ワイヤレス装置を認証する。ワイヤレス通信システムは、ランダムチャレンジＲＡＮＤＵのようなシーケンスを生成し、シーケンスＲＡＮＤＵを、例えば認証チャレンジメッセージ４４で、ワイヤレス装置へ送る。ワイヤレス装置１４は、認証チャレンジメッセージ４４を受信すると、シーケンスＲＡＮＤＵの少なくとも一部を、入力ＥＳＮ、ＡＵＴＨ＿ＤＡＴＡ、ＳＳＤ－Ａ、ならびに、ＲＡＮＤＵおよびＩＭＳＩから導出されるＲＡＮＤ＿ＣＨＡＬＬＥＮＧＥとともに、暗号化関数、例えば、認証署名手続き４６に提供する。認証署名手続き４６は、ＲＡＮＤ＿ＣＨＡＬＬＥＮＧＥ、ＥＳＮ、ＡＵＴＨ＿ＤＡＴＡおよびＳＳＤ－Ａを入力として使用したＣＡＶＥアルゴリズムの出力として、認証署名値ＡＵＴＨＵを生成する。ワイヤレス通信システムは、同様にして、認証署名手続き４８を使用して、認証署名値ＡＵＴＨＵを生成する。その後、ワイヤレス装置は、ワイヤレス装置が計算した値ＡＵＴＨＵをワイヤレス通信システムへ送信する。ワイヤレス通信システムは、ブロック５０で、システムが計算した値ＡＵＴＨＵを、ワイヤレス装置から受信したＡＵＴＨＵと比較する。これらの値が一致した場合、ワイヤレス通信システムは、新しいＳＳＤ値を検証したことになり、ワイヤレス装置は認証されたことになる。

【００１２】

ワイヤレス装置１４が在圏通信システム内にあり、ホーム通信システムが何らかの理由で新しい通信鍵ＳＳＤ－ＮＥＷを在圏通信システムと共有していない場合、在圏通信システムは、単に、ワイヤレス装置とホーム通信システムとの間の通信のための通路として作用する。このため、上記の鍵更新は、ワイヤレス装置が通信システムを認証するために、ホーム通信システムと在圏通信システムの間の大量の通信を必要とする。さらに、上記の方式における鍵更新の後には、ＳＳＤの正当性を確かめることにより通信システムの側からワイヤレス装置を認証するための、通信システムによるワイヤレス装置の別個の認証がある。この別個の認証は、ワイヤレス装置と通信システムの相互認証を提供しているが、在圏通信システムとホーム通信システムの間でさらに多くの通信が行われることになる。

【００１３】

例えば、図３Ａに、ＩＳ－４１シグナリング標準対応の在圏通信システム内でワイヤレス装置１４がどのように認証されるかを示す。ワイヤレス装置１４およびホーム通信システム６０はいずれも、Ａ－ＫＥＹという秘密値を保有する。ワイヤレス装置１４が、在圏システム６２へのアクセスを要求すると、在圏システム６２は、ホームシステム６０に対してデータを要求する。この例では、ワイヤレス装置１４に関連するホームロケーションレジスタ２２（図１）は、ワイヤレス装置の電話番号のような識別子を用いて検索される。

ワイヤレス装置１４のＨＬＲ２２は、秘密値すなわち鍵Ａ－ＫＥＹを記憶しており、これは、新しい通信鍵ＳＳＤ－ＮＥＷを生成するために使用される。ＳＳＤ－ＮＥＷは、少なくともシーケンスＲＡＮＤＳＳＤおよびＡ－ＫＥＹを入力として用いてＣＡＶＥアルゴリズムを実行することにより計算することができる。ＣＡＶＥアルゴリズムは当業者に周知であり、ＩＳ－４１標準で規定されている。

【００１４】

ホームシステム６０は、値ＲＡＮＤＳＳＤを在圏システムに転送し、在圏システムは、ＲＡＮＤＳＳＤ値をワイヤレス装置１４へ送信する。すると、ワイヤレス装置１４は、式ＳＳＤ－Ａ－ＮＥＷ，ＳＳＤ－Ｂ－ＮＥＷ＝$CAVE_{A\text{-}KEY}$（ＲＡＮＤＳＳＤ）で示されるように、ホームシステム６０により計算されたのと同様にしてＳＳＤを計算する。その後、ワイヤレス装置１４は、値ＲＡＮＤＢＳを在圏システム６２へ送り、在圏システム６２はこの値ＲＡＮＤＢＳをホームシステム６０へ送る。対応する暗号化関数を使用して、ホームシステム６０は、ワイヤレス装置１４からのＲＡＮＤＢＳを用いてＡＵＴＨＢＳを導出する。ホームシステム６０は、ＡＵＴＨＢＳ値を在圏システム６２へ送り、在圏システム６２はこのＡＵＴＨＢＳ値をワイヤレスシステム１４へ送る。ホームシステム６０へのＲＡＮＤＢＳの通信およびホームシステムからのＡＵＴＨＢＳの応答は、認証要求あるいは基地局チャレンジともいうトランザクションである。ワイヤレス装置１４は、ワイヤレス装置１４で生成したＡＵＴＨＢＳ値を、システムから送信されたＡＵＴＨＢＳ値と比較する。この比較で一致した場合、ワイヤレス装置は、ＳＳＤ－Ａ値をＳＳＤ－Ａ－ＮＥＷとし、ＳＳＤ－Ｂ値をＳＳＤ－Ｂ－ＮＥＷとする。その後、ワイヤレス装置は、在圏システム６２を通じて、ＳＳＤ更新の正常終了を示すＳＳＤ更新確認命令をホームシステム６０へ送る。ホームシステム６０からのＲＡＮＤＳＳＤの通信およびＳＳＤ更新確認の受信は、認証指令（ＡＵＴＨＤＩＲ）ともいうトランザクションである。ホームシステム６０は、ＳＳＤ更新確認命令を受信すると、ＳＳＤ－ＡおよびＳＳＤ－Ｂを、システムにより生成したＳＳＤ－Ａ－ＮＥＷおよびＳＳＤ－Ｂ－ＮＥＷ値とする。

【００１５】

その後、図３Ａの例では、ホームシステム６０は、乱数チャレンジＲＡＮＤＵをワイヤレス装置１４へ送ることによりワイヤレス装置１４に呼びかける第２認証指令ともいうものを開始する。ホームシステム６０は、値ＲＡＮＤＵを在圏システム６２へ送り、在圏システム６２はこの値ＲＡＮＤＵをワイヤレス装置１４へ送る。ワイヤレス装置１４およびホームシステム６０は両方とも、値ＡＵＴＨＵを計算する。ＡＵＴＨＵは、ＡＵＴＨＵ＝$CAVE_{SSD\text{-}A}$（ＲＡＮＤ）で示されるように、乱数ＲＡＮＤＵおよびＳＳＤ－Ａ値を入力とするＣＡＶＥアルゴリズムのような暗号化関数の出力に等しい。その後、ワイヤレス装置１４は、計算した値ＡＵＴＨＵを在圏システム６２へ送り、在圏システム６２は、ワイヤレス装置１４から受信したＡＵＴＨＵ値をホームシステム６０へ送る。ワイヤレス装置１４からの値ＡＵＴＨＵがホームシステム６０で計算したＡＵＴＨＵ値と一致した場合、新しいＳＳＤ値はホームシステム６０の側から検証され、ワイヤレス装置１４は認証されたことになり、在圏システムへのアクセスが許可される。

【００１６】

図３Ｂに、ホームシステムとワイヤレス装置の認証が実行される際のＳＳＤ鍵の更新を実行するための別の実装を示す。この実装では、ホームシステム６０は、値ＲＡＮＤＳＳＤを生成した後、式ＳＳＤ－Ａ－ＮＥＷ，ＳＳＤ－Ｂ－ＮＥＷ＝$CAVE_{A\text{-}KEY}$（ＲＡＮＤＳＳＤ）で示されるように、ＳＳＤ－Ａ－ＮＥＷを計算する。また、ホームシステムは、値ＲＡＮＤＵを生成することが可能であり、与えられたＳＳＤ－Ａ－ＮＥＷに対して、ホームシステム６０は、ＡＵＴＨＵを計算することも可能である。その後、ホームシステムは、ＲＡＮＤＳＳＤを、ＲＡＮＤＵおよびＡＵＴＨＵとともに、在圏システム６２へ送る。在圏システム６２は、ワイヤレス装置がＳＳＤ－Ａ－ＮＥＷを計算するために、ＲＡＮＤＳＳＤをワイヤレス装置１４へ転送する。すると、ワイヤレス装置１４は、値ＲＡＮＤＢＳを在圏システム６２へ送り、在圏システム６２はこの値ＲＡＮＤＢＳをホームシステム６０へ送る。ホームシステム６０は、対応する暗号化関数を使用して、ワイヤレス装置

１４からのＲＡＮＤＢＳを用いてＡＵＴＨＢＳを導出する。ホームシステム６０は、ＡＵＴＨＢＳ値を在圏システム６２へ送り、在圏システム６２はこのＡＵＴＨＢＳ値をワイヤレス装置１４へ送る。ワイヤレス装置１４は、ワイヤレス装置１４で生成したＡＵＴＨＢＳ値を、システムから送信されたＡＵＴＨＢＳ値と比較する。この比較で一致した場合、ワイヤレス装置は、ＳＳＤ－Ａ値をＳＳＤ－Ａ－ＮＥＷとし、ＳＳＤ－Ｂ値をＳＳＤ－Ｂ－ＮＥＷとする。

【００１７】

その後、ワイヤレス装置は、在圏システム６２を通じて、ＳＳＤ更新の正常終了を示すＳＳＤ更新確認命令をホームシステム６０へ送る。ホームシステム６０は、ＳＳＤ更新確認命令を受信すると、ＳＳＤ－ＡおよびＳＳＤ－Ｂを、システムにより生成したＳＳＤ－Ａ－ＮＥＷおよびＳＳＤ－Ｂ－ＮＥＷ値とする。ここで、ＲＡＮＤＵおよびＡＵＴＨＵはすでに在圏システム６２にあるため、在圏システム６２は、ＲＡＮＤＵをワイヤレス装置１４へ送る。ワイヤレス装置１４は、このＲＡＮＤＵ値を用いてＡＵＴＨＵを計算し、ＡＵＴＨＵを在圏システム６２へ送る。ワイヤレス装置１４からの値ＡＵＴＨＵがホームシステム６０で計算されたＡＵＴＨＵ値と一致した場合、在圏システム６２は、ＳＳＤ更新に関する認証報告をホームシステム６０へ送り、これに対してホームシステム６０は、確認応答（ＡＣＫ）信号で応答する。

【００１８】

【発明が解決しようとする課題】

上記のワイヤレス装置の鍵更新およびその後の認証は、ホームシステムと在圏システムの間で大量の通信を使用し、ホームシステムが通信鍵を保有する場合にシステム資源を消費する。

【００１９】

【課題を解決するための手段】

本発明は、更新鍵を用いて装置あるいは通信システムの認証を実行することにより、通信鍵を更新するシステムに関する。更新鍵を用いて認証を実行することによって、鍵更新システムは、通信鍵をホーム通信システムに維持しながら更新鍵を在圏通信システムへ送ることにより、ホーム通信システムと在圏通信システムとの間の通信を低減することができる。例えば、鍵更新を実行する際に、ホーム通信システムは、ホーム通信システムで生成されるシーケンスＲＡＮＤＳＳＤと、ホーム通信システムおよび装置に維持される秘密鍵Ａ－ＫＥＹを用いて、新しい認証鍵ＳＳＤ－Ａ－ＮＥＷのような通信鍵を生成する。また、ホーム通信システムは、同じくシーケンスＲＡＮＤＳＳＤおよび秘密鍵Ａ－ＫＥＹを用いて、更新鍵ＳＳＤ－ＫＥＹを生成する。ホーム通信システムは、更新鍵ＳＳＤ－ＫＥＹおよびシーケンスＲＡＮＤＳＳＤを在圏通信システムへ送り、在圏通信システムは、シーケンスＲＡＮＤＳＳＤを装置へ送る。装置は、ホーム通信システムと同様にして、新しい認証鍵ＳＳＤ－Ａ－ＮＥＷのような新しい通信鍵と、更新鍵ＳＳＤ－ＮＥＷとを生成する。在圏通信システムは更新鍵ＳＳＤ－ＫＥＹを有しているため、在圏認証システムは、在圏通信システムにある更新鍵を用いて署名値ＡＵＴＨＳＳＤあるいはＡＵＴＨＢＳを生成して、装置あるいは通信システムを認証することができる。

【００２０】

【発明の実施の形態】

本発明の原理による更新鍵を用いた鍵更新の実施例について以下で説明する。この実施例は、ワイヤレス装置のような装置と、ワイヤレス通信システムのような通信システムとの間の鍵更新手続きを改善する。例えば、通信システムは、ある判断基準によりＳＳＤが漏洩された可能性があることが示された場合やその他の理由（例えば、初期化する場合）により、共有秘密鍵（ＳＳＤ）のような通信鍵の更新を開始することができる。通信鍵は、装置と通信システムの間の通信の安全性を高めるために装置および通信システムによって使用される鍵である。通信鍵またはその一部は、認証鍵、暗号化鍵、鍵生成鍵、あるいは、通信の内容にディジタル署名するために使用される完全性(integrity)鍵とすることが可能である。通信鍵ＳＳＤは、認証鍵ＳＳＤ－Ａと暗号化鍵ＳＳＤ－Ｂのように、他の複

数の通信鍵へと分割することができる。ＳＳＤ－Ａは認証手続きで使用され、ＳＳＤ－Ｂは鍵生成（例えば、暗号鍵Ｋｃを生成する場合）や、暗号化手続きで使用される。鍵更新システムは、通信鍵を更新することによって、通信システムが装置の認証を実行する際に使用する認証鍵を更新する。通信システムは、更新鍵を使用するホーム通信システムや在圏通信システムを含むことが可能である。実施例では、更新鍵は、通信鍵に加えて更新手続きの一部として生成され、通信鍵の更新中の認証を実行するために使用される。実施態様に依存して、また、ワイヤレス装置が在圏通信システムに登録しているかそれともホーム通信システムに登録しているかに依存して、鍵更新システムおよびその各部分は、サービス基地局、在圏認証センタ、在圏ＭＳＣ、在圏ロケーションレジスタ、ホームロケーションレジスタ、ホームＭＳＣあるいはホーム認証センタのような、通信システムのさまざまな部分で実現することが可能である。

【００２１】

鍵更新を実行する際に、通信システムは、少なくとも装置の秘密値Ａ－ＫＥＹを用いて新しい通信鍵（例えば、新しい通信鍵ＳＳＤ－ＮＥＷあるいは新しい認証鍵ＳＳＤ－Ａ－ＮＥＷ）を生成する。本発明の特徴によれば、通信システムは、秘密値Ａ－ＫＥＹの少なくとも一部、あるいは、新しい通信鍵を生成する際に使用される情報の少なくとも一部を用いて、新しい通信鍵とは異なる更新鍵を生成する。装置は、更新鍵を用いて通信システムを認証し、あるいは、通信システムは、更新鍵を用いて装置を更新する。認証が実行された後、装置と通信システムは、新しい通信鍵で通信鍵を更新することにより、装置と通信システムの間の通信を続けることが可能となり、更新鍵は捨てることができる。こうして、更新鍵は、通信鍵の更新中の認証を実行するために使用される一時鍵として扱うことができる。

【００２２】

図４に、更新鍵ＳＳＤ－ＫＥＹを使用する鍵更新システムの実施例６３を示す。通信鍵ＳＳＤ（認証鍵ＳＳＤ－Ａと、暗号化鍵ＳＳＤ－Ｂ）は、装置６４が更新鍵を用いて通信システム６５を認証した後に更新される。装置６４および通信システム６５はそれぞれ、装置６４に関連する秘密値Ａ－ＫＥＹを有する。通信鍵ＳＳＤの更新を実行するとき、通信システムは、ＲＡＮＤＳＳＤシーケンスを作成し、これは装置６４に提供される。シーケンスＲＡＮＤＳＳＤは、乱数、ある周期で繰り返す擬似乱数、あるいは、受け取る値が前に受け取った値以下にならない単調増大カウンタの出力とすることが可能である。通信システム６５は、シーケンスＲＡＮＤＳＳＤおよび秘密鍵Ａ－ＫＥＹを入力として使用した暗号化関数６７（Ｆ０）の出力をとることにより、新しい通信鍵ＳＳＤ－ＮＥＷを計算する。また、通信システム６５は、シーケンスＲＡＮＤＳＳＤおよび秘密鍵Ａ－ＫＥＹを入力として使用した暗号化関数６８（Ｆ１）の出力をとることにより、更新鍵ＳＳＤ－ＫＥＹを計算する。

【００２３】

この実施例では、暗号化関数６７は、暗号化関数６８とは異なり、これにより、更新鍵ＳＳＤ－ＫＥＹは、新しい通信鍵ＳＳＤ－ＮＥＷとは異なるか、または、少なくとも、認証鍵ＳＳＤ－Ａ－ＮＥＷとは異なる。例えば、与えられた入力ＲＡＮＤＳＳＤおよびＡ－ＫＥＹに対して、暗号化関数６７および６８は、一方の出力が与えられても他方の出力は予測することができないような無関係な出力として、ＳＳＤ－ＫＥＹおよび新しい通信鍵ＳＳＤ－ＮＥＷを生成する。実施例に依存して、シーケンスＲＡＮＤＳＳＤおよびＡ－ＫＥＹのさまざまな部分を入力として使用して認証鍵とは異なる更新鍵を生成しながら、暗号化関数６７と６８とは同一とすることも異なることも可能である。実施例に依存して、鍵更新システムは、鍵生成手続き６７あるいは６８への追加入力（例えば、ＥＳＮやＩＭＳＩのようなワイヤレス装置や加入者に特徴的な値）を使用することも可能である。鍵生成手続き６７あるいは６８は、入力として乱数ＲＡＮＤＳＳＤおよび値Ａ－ＫＥＹを任意の追加入力とともに使用するＣＡＶＥアルゴリズムを実装する。ＣＡＶＥアルゴリズムは、一方向性関数として当業者に周知である。他の生成手続きも使用可能である。

【００２４】

通信システム６５は、更新シーケンスＲＡＮＤＳＳＤを装置６４へ送り、装置６４は、通信システム６５と同様にして新しい通信鍵ＳＳＤ－ＮＥＷおよび更新鍵ＳＳＤ－ＫＥＹを生成する。通信システム６５を認証するため、装置は、更新シーケンスＲＡＮＤＢＳを生成し、このシーケンスＲＡＮＤＢＳを通信システム６５へ送る。シーケンスＲＡＮＤＢＳは、乱数、ある周期で繰り返す擬似乱数、あるいは、受け取る値が前に受け取った値以下にならない単調増大カウンタの出力とすることが可能である。装置６４は、少なくとも、装置６４で生成したシーケンスＲＡＮＤＢＳおよび更新鍵を用いて、署名値ＡＵＴＨＢＳを生成する。ＡＵＴＨＢＳを生成するため、装置は、ＲＡＮＤＢＳおよびＳＳＤ－ＫＥＹを、ＲＡＮＤＳＳＤ、ＥＳＮあるいは国際移動局識別番号（ＩＭＳＩ）から導出されるＡＵＴＨ＿ＤＡＴＡストリングのような付加データとともに、署名手続き６９に提供する。実施例に依存して、署名手続き６９は、署名手続き６９へのさまざまな入力が使用可能な暗号化関数である。署名生成手続き６９は、入力として乱数ＲＡＮＤＢＳおよび更新鍵ＳＳＤ－ＫＥＹを任意の追加入力とともに使用するＣＡＶＥアルゴリズムを実行することができる。

【００２５】

鍵生成手続き６７および６８ならびに署名手続き６９は、ＣＡＶＥアルゴリズムやＳＨＡ－１のようなハッシュ関数あるいは任意の一方向性暗号化関数とすることが可能である。他の生成手続きも使用可能である。ハッシュ関数は、一方向性関数（出力が与えられた場合に入力を再生することが実現不可能な関数）として、入力から出力への多対一写像を生成する関数として、あるいは、入力よりも情報の少ない出力を生成する関数であって、これにより、出力が与えられた場合に入力を突きとめることが困難であるものとして特徴づけることができる。このような関数において、出力を入力の署名(signature)という。

【００２６】

通信システム６５は、通信システム６５で生成した更新鍵ＳＳＤ－ＫＥＹと、装置６４から受信したシーケンスＲＡＮＤＢＳとを署名生成手続き６９への入力として使用して、装置６４と同様にして署名値ＡＵＴＨＢＳを生成する。通信システム６５は、ＡＵＴＨＢＳを装置６４へ送る。装置６４は、通信システム６５から受信した署名値ＡＵＴＨＢＳを、装置６４で生成した署名値ＡＵＴＨＢＳと比較することにより、通信システム６５を認証する。装置６４は、この比較の結果を通信システム６５に通知する。装置６４が、更新鍵ＳＳＤ－ＫＥＹを用いて通信システムを認証した後、通信鍵は新しい通信鍵で更新され、更新鍵は捨てることができる。

【００２７】

図４の実施例では、通信システム６５は、さらに、ホーム通信システム７０および在圏通信システム７１を含むことが可能である。本発明のもう１つの特徴によれば、ホーム通信システム７０は、装置が通信鍵あるいは更新鍵を決定する際に使用する情報とともに、更新鍵ＳＳＤ－ＫＥＹを在圏通信システム７１へ送る。在圏通信システム７１および装置６４は、この更新鍵を用いて認証を実行することにより、ホーム通信システム７０と在圏通信システム７１の間の通信回数を低減することが可能となり、ホーム通信システム７０は、少なくとも鍵更新が完了するまで、在圏通信システム７１に新しい通信鍵を保持することができる。

【００２８】

この実施例では、ホーム通信システム７０は、少なくとも、ホーム通信システム７０に記憶されている装置６４に関連する更新シーケンスＲＡＮＤＳＳＤおよび秘密値Ａ－ＫＥＹまたはその一部を用いて、新しい通信鍵ＳＳＤ－ＮＥＷを生成する。また、ホーム通信システム７０は、上記の装置６４の場合と同様にして、少なくとも、更新シーケンスＲＡＮＤＳＳＤおよび秘密値Ａ－ＫＥＹまたはその一部を用いて、更新鍵を生成する。ホーム通信システム７０は、更新シーケンスＲＡＮＤＳＳＤおよび更新鍵ＳＳＤ－ＫＥＹを、更新指令７２で在圏通信システム７１へ送り、在圏通信システム７１は、メッセージ７３で、更新シーケンスＲＡＮＤＳＳＤを装置６４へ送る。装置６４で、新しい通信鍵ＳＳＤ－ＮＥＷ（この実施例では、通信鍵ＳＳＤ－Ａ－ＮＥＷおよびＳＳＤ－Ｂ－ＮＥＷを含む）お

よび更新鍵ＳＳＤ－ＫＥＹは、ホーム通信システム７０の場合と同様にして生成される。装置６４は、チャレンジシーケンスＲＡＮＤＢＳを生成し、更新鍵およびチャレンジシーケンスＲＡＮＤＢＳ（その一部を含む）を暗号化関数６９への入力として使用して署名値ＡＵＴＨＢＳを生成する。

【００２９】

装置６４は、チャレンジシーケンスＲＡＮＤＢＳをメッセージ７４で在圏通信システム７１へ送り、在圏通信システム７１は、少なくとも、更新鍵ＳＳＤ－ＫＥＹおよびシーケンスＲＡＮＤＢＳを暗号化関数６９への入力として使用して署名値ＡＵＴＨＢＳを生成する。ＡＵＴＨＢＳを生成するためにＲＡＮＤＢＳをホーム通信システム７０へ転送してホーム通信システム７０からＡＵＴＨＢＳを在圏通信システム７１へ送ってもらうのではなく、更新鍵ＳＳＤ－ＫＥＹを在圏通信システム７１へ送って在圏通信システム７１が装置６４と同様にして署名値ＡＵＴＨＢＳを生成することにより、通信回数を低減することができる。在圏通信システム７１は、メッセージ７６でＡＵＴＨＢＳを装置６４へ送る。装置６４は、在圏通信システム７１から受信した署名値ＡＵＴＨＢＳを、装置６４で生成した署名値ＡＵＴＨＢＳと比較することにより、通信システムを認証する。装置６４は、メッセージ７７で、この比較の結果を在圏通信システム７１に通知し、在圏通信システム７１は、メッセージあるいは認証報告７８で、この比較の結果をホーム通信システム７０に通知する。装置６４が更新鍵を用いて通信システムを認証した後、通信鍵ＳＳＤ（認証鍵ＳＳＤ－Ａを含む）は、新しい通信鍵ＳＳＤ－ＮＥＷ（新しい認証鍵ＳＳＤ－Ａ－ＮＥＷを含む）で更新される。このように、新しい認証鍵は在圏通信システム７１と共有されず、新しい認証鍵を用いて計算される署名値が認証で使用されることもない。ホーム通信システム７０は、新鍵ＳＳＤ－Ａのような通信鍵を在圏通信システム７１と共有することもしないことも可能であり、更新鍵は捨てることも捨てないことも可能である。

【００３０】

図５Ａに、本発明の特徴による鍵および署名値生成手続き８０を示す。この手続きでは、更新鍵ＳＳＤ－ＫＥＹを生成し、その更新鍵を用いて、鍵更新を実行する際に相互認証を行うために装置および通信システムによって使用される署名値ＡＵＴＨＳＳＤおよびＡＵＴＨＢＳを生成する。装置および通信システムはそれぞれ、装置に関連する秘密値Ａ－ＫＥＹを有する。通信鍵ＳＳＤ（認証鍵ＳＳＤ－Ａおよび暗号化鍵ＳＳＤ－Ｂを含む）のような通信鍵の更新を実行するとき、通信システムは、ＲＡＮＤＳＳＤシーケンスを作成し、これは装置に提供される。シーケンスＲＡＮＤＳＳＤは、乱数、ある周期で繰り返す擬似乱数、あるいは、受け取る値が前に受け取った値以下にならない単調増大カウンタの出力とすることが可能である。

【００３１】

通信システムは、シーケンスＲＡＮＤＳＳＤおよび秘密鍵Ａ－ＫＥＹを入力として使用した暗号化関数８２（Ｆ０）の出力をとることにより、新しい通信鍵ＳＳＤ－ＮＥＷを計算する。また、通信システムは、シーケンスＲＡＮＤＳＳＤおよび秘密鍵Ａ－ＫＥＹを入力として使用した暗号化関数８４（Ｆ１）の出力をとることにより、更新鍵ＳＳＤ－ＫＥＹを計算する。この実施例では、暗号化関数８２は、暗号化関数８４とは異なり、これにより、更新鍵ＳＳＤ－ＫＥＹは、新しい通信鍵ＳＳＤ－ＮＥＷとは異なるか、または、少なくとも、認証鍵ＳＳＤ－Ａ－ＮＥＷとは異なる。実施例に依存して、シーケンスＲＡＮＤＳＳＤおよびＡ－ＫＥＹのさまざまな部分を入力として使用して新しい通信鍵ＳＳＤ－ＮＥＷとは異なる更新鍵を生成しながら、暗号化関数８２と８４とは同一とすることも異なることも可能である。実施例に依存して、鍵更新システムは、鍵生成手続き８２あるいは８４への追加入力（例えば、ＥＳＮやＩＭＳＩのようなワイヤレス装置や加入者に特徴的な値）を使用することも可能である。鍵生成手続き８２あるいは８４は、入力として乱数ＲＡＮＤＳＳＤおよび値Ａ－ＫＥＹを任意の追加入力とともに使用するＣＡＶＥアルゴリズムを実装する。ＣＡＶＥアルゴリズムは、一方向性関数として当業者に周知である。他の生成手続きも使用可能である。

【００３２】

装置は、通信システムから、例えばＳＳＤ更新メッセージで、ＲＡＮＤＳＳＤを受信した後、通信システムと同様にして、新しい通信鍵ＳＳＤ－ＮＥＷおよび更新鍵ＳＳＤ－ＫＥＹを生成することができる。新しい通信鍵値（ＳＳＤ－ＮＥＷ）を生成した後、装置と通信システムは、更新鍵（ＳＳＤ－ＫＥＹ）を用いて認証を実行することができる。これを行うため、装置は、乱数チャレンジのような数あるいはシーケンスＲＡＮＤＢＳを生成する。シーケンスＲＡＮＤＢＳは、乱数、ある周期で繰り返す擬似乱数、あるいは、受け取る値が前に受け取った値以下にならない単調増大カウンタの出力とすることが可能である。装置が、例えばシーケンスＲＡＮＤＢＳから導出される署名値を用いて、通信システムを認証し、通信システムが、例えばシーケンスＲＡＮＤＳＳＤから導出される署名値を用いて、装置を認証する場合、通信システムと装置とは相互認証の関係になるが、必ずしもインターロックした（一方の認証ができなければ他方の認証もできない）相互認証とはならない。この実施例では、インターロック相互認証が、更新鍵を用いて実行される。その理由は、装置によって生成されるＲＡＮＤＢＳと、通信システムによって生成されるＲＡＮＤＳＳＤは両方とも、装置および通信システムによる認証で用いられるそれぞれの署名値ＡＵＴＨＳＳＤおよびＡＵＴＨＢＳを生成する際に使用されるからである。通信システムからのランダムシーケンス（ＲＡＮＤＳＳＤ）および装置からのランダムシーケンス（ＲＡＮＤＢＳ）を用いて相互認証に関わる署名値を生成することによって、装置および通信システムによる認証はインターロックするため、乱数チャレンジおよび対応する署名値が取得されても、それを繰り返し使用して装置あるいはシステムへの無権限のアクセスを取得するようなリプレイ攻撃を受けにくい。

【００３３】

実施例に依存して、更新鍵を用いて、装置と通信システムの間の単一の相互認証あるいはインターロック認証で、少なくとも１つの署名値を生成することが可能である。この実施例では、装置は、ＲＡＮＤＢＳ、ＲＡＮＤＳＳＤおよびＳＳＤ－ＫＥＹを、ＥＳＮや、国際移動局識別番号（ＩＭＳＩ）から導出されるＡＵＴＨ＿ＤＡＴＡストリングのような任意の付加データとともに、署名手続き８６に提供する。署名手続き８６は、署名値ＡＵＴＨＳＳＤを生成する。装置は、ＲＡＮＤＢＳ、ＲＡＮＤＳＳＤおよびＳＳＤ－ＫＥＹを、ＥＳＮや、国際移動局識別番号（ＩＭＳＩ）から導出されるＡＵＴＨ＿ＤＡＴＡストリングのような任意の付加データとともに、署名手続き８８に提供する。署名手続き８８は、署名値ＡＵＴＨＢＳを生成する。

【００３４】

実施例に依存して、値ＲＡＮＤＢＳ、ＲＡＮＤＳＳＤあるいはＳＳＤ－ＫＥＹまたはこれらから導出される値のさまざまな部分を入力として使用しながら、署名手続き８６および８８は、同一とすることも異なることも可能である。実施例に依存して、鍵更新システムは、署名手続き８６あるいは８８へのさまざまな入力を使用可能である。例えば、ＲＡＮＤＢＳを署名手続き８６への入力から除き、ＲＡＮＤＳＳＤを署名手続き８８への入力から除くことも可能である。この場合、相互認証はもはやインターロックしなくなる。署名生成手続き８６あるいは８８は、入力として乱数ＲＡＮＤＳＳＤ、ＲＡＮＤＢＳおよび更新鍵ＳＳＤ－ＫＥＹを任意の追加入力とともに使用するＣＡＶＥアルゴリズムを実装することが可能である。ＣＡＶＥアルゴリズムは、一方向性関数として当業者に周知である。他の生成手続きも使用可能である。

【００３５】

通信システムは、装置と同様にしてＡＵＴＨＳＳＤを決定する。この実施例では、通信システムは、装置からＲＡＮＤＢＳを受信し、装置と同様にして、更新鍵ＳＳＤ－ＫＥＹ、ＲＡＮＤＳＳＤおよびＲＡＮＤＢＳを用いてＡＵＴＨＳＳＤを生成する。ＡＵＴＨＳＳＤにより、通信システムは、装置で生成されたＡＵＴＨＳＳＤを受信し、装置で生成されたＡＵＴＨＳＳＤ値を通信システムで決定したＡＵＴＨＳＳＤ値と比較すれば、装置を認証することができる。また、通信システムは、更新鍵ＳＳＤ－ＫＥＹを用いて、装置と同様にしてＡＵＴＨＢＳを決定することが可能である。通信システムは、署名値ＡＵＴＨＢＳを装置へ送り、装置は、通信システムから受信した署名値ＡＵＴＨＢＳを装置で生成した

署名値ＡＵＴＨＢＳと比較することによって、通信システムを認証する。認証が成功した場合、装置と通信システムは、通信鍵ＳＳＤの値を新しい通信鍵ＳＳＤ－ＮＥＷの値とする。これにより、この実施例では、認証鍵ＳＳＤ－Ａは新しい認証鍵ＳＳＤ－Ａ－ＮＥＷで置き換えられる。前述のように、この実施例では、新しい値ＳＳＤは、ＳＳＤ－ＡとＳＳＤ－Ｂに分割可能である。ただし、ＳＳＤ－Ａは認証手続きで使用され、ＳＳＤ－Ｂは、鍵生成（例えば暗号鍵Ｋｃを生成する場合）や暗号化手続きで使用される。

【００３６】

新しい暗号化鍵ＳＳＤ－Ｂが与えられると、装置および通信システムは両方とも、暗号鍵Ｋｃの値を計算する。ただし、値Ｋｃは、$Kc = CAVE_{SSD\text{-}B}(RAND)$で示されるように、鍵入力として値ＳＳＤ－Ｂを使用するとともに、通信システムにより生成されたシーケンスＲＡＮＤのような追加情報を入力として使用した、ＣＡＶＥアルゴリズムの出力に等しい。この時点で、ワイヤレス装置と通信システムの間の通信が可能となり、暗号化されるべきメッセージと鍵Ｋｃを入力とする暗号化関数を用いて暗号化されることが可能となる。この暗号化関数は、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）およびＧＳＭ(global system mobile)方式で、それぞれの標準により規定される。

【００３７】

更新鍵を用いた鍵更新は、周期的に、あるいは、ワイヤレス通信システムがある判断基準に基づいて共有鍵ＳＳＤが漏洩されたと判断した場合、ワイヤレス装置がホーム通信システムや信頼できる在圏通信システムに戻った場合、Ａ－ＫＥＹが変更された場合、新たな加入（申込み）が設定されてＳＳＤ値が初期化された場合、あるいはその他の理由により、実行可能である。さらに、実施例に依存して、鍵生成手続き８２および８４ならびに署名手続き８６および８８への入力は、上記のものとは異なる値や上記のものに加えて別の値、あるいは、それらおよびその他の入力から導出される入力を含むことも可能である。例えば、ワイヤレス装置の電子シリアル番号（ＥＳＮ）、ワイヤレス装置の電話番号（ＭＩＮ１）あるいはワイヤレス装置のＩＭＳＩの少なくとも一部を、鍵生成および署名手続き８２、８４、８６および８８への入力として使用可能である。鍵生成手続き８２および８４ならびに署名手続き８６および８８は、ＣＡＶＥアルゴリズムあるいはＳＨＡ－１のようなハッシュ関数あるいは一方向性暗号化関数とすることが可能である。他の手続きも可能である。

【００３８】

実施例に依存して、更新鍵を用いた鍵更新のための通信は、ワイヤレス装置とホーム認証センタとの間でワイヤレス装置が在圏ネットワークにある場合には在圏認証センタを通じて）行うことが可能である。代替実施例では、更新鍵およびその一部を用いた鍵更新は、他の位置で実行することも可能である。

【００３９】

図５Ｂに、ホーム通信システムに新しい通信鍵ＳＳＤ－ＮＥＷを保持しながらホーム通信システムと在圏通信システムとの間の通信回数を低減した、更新鍵を用いて装置と通信システムの間の相互認証を実行する鍵更新システムの実施例を示す。例えば、ホーム通信システム９０は、シーケンスＲＡＮＤＳＳＤと更新鍵ＳＳＤ－ＫＥＹを生成し、更新指令９３の一部として在圏通信システム９２へ送る。在圏通信システム９２は、更新メッセージ９６で、シーケンスＲＡＮＤＳＳＤを装置９４へ送り、装置９４は、ＲＡＮＤＳＳＤを用いて更新鍵ＳＳＤ－ＫＥＹを生成する。装置９４は、シーケンスＲＡＮＤＢＳを生成し、更新鍵ＳＳＤ－ＫＥＹを用いて装置９４で生成した署名値ＡＵＴＨＳＳＤとともに、ＲＡＮＤＢＳを、ランダムチャレンジメッセージ９８で、在圏通信システム９２へ送る。在圏通信システム９２は、更新鍵ＳＳＤ－ＫＥＹを用いて、装置９４と同様にして署名値ＡＵＴＨＳＳＤを生成する。在圏通信システム９２は、装置９４から受信した署名値ＡＵＴＨＳＳＤを、在圏通信システム９２で生成した署名値ＡＵＴＨＳＳＤと比較することによって、装置９４を認証する。

【００４０】

新しい通信鍵ＳＳＤ－ＮＥＷをホーム通信システム９０に維持しながらホーム通信システ

ム９０と在圏通信システム９２との間の通信回数を低減するため、在圏通信システム９２は、装置９４と同様にして、シーケンスＲＡＮＤＢＳおよび更新鍵を用いて署名値ＡＵＴＨＢＳを生成する。このため、在圏通信システム９２は、シーケンスＲＡＮＤＢＳをホーム通信システム９０へ転送する必要がなく、また、ホーム通信システム９０が在圏通信システム９２へ署名値ＡＵＴＨＢＳを送る必要もない。在圏通信システム９２は、チャレンジ応答１００で、署名値ＡＵＴＨＢＳを装置９４へ送る。装置９４は、在圏通信システム９２から受信した署名値ＡＵＴＨＢＳを、装置９４で生成した署名値ＡＵＴＨＢＳと比較することによって、通信システムを認証する。

【００４１】

この比較で一致した場合、相互認証は完了し、装置９４は、メッセージ１０２で、更新の結果を在圏通信システム９２に通知する。在圏通信システム９２は、例えば認証報告の一部として、メッセージ１０２で、更新の結果をホーム通信システム９０に通知する。メッセージ１０２は、追加情報、例えば署名値ＡＵＴＨＳＳＤおよびＲＡＮＤＢＳのような相互認証プロセスで用いられるパラメータを含むことも可能であり、それにより、ホーム通信システムは、在圏通信システムが正しい更新をしたかどうかを判断することができる。更新および相互認証が成功した場合、装置９４は、通信鍵ＳＳＤ（ＳＳＤ－ＡおよびＳＳＤ－Ｂ）を新しい通信鍵ＳＳＤ－ＮＥＷ）ＳＳＤ－Ａ－ＮＥＷ，ＳＳＤ－Ｂ－ＮＥＷ）とする。鍵更新の後、更新鍵は捨てることができる。

【００４２】

上記の実施例に加えて、本発明の原理による鍵更新システムは、鍵生成および署名手続きへの入力パラメータを省略あるいは追加することも、上記のシステムの変形あるいは一部を使用することも可能である。例えば、上記では、鍵更新について、更新鍵を用いて装置と通信システムの相互認証を実行するものとして説明したが、この鍵更新は、更新鍵を用いて生成された署名値を比較することによる一方向性認証を実行することも可能である。

【００４３】

実施例に依存して、鍵生成および署名手続きのための入力は、異なるソースから装置、在圏通信システムあるいはホーム通信システムへ通信されることも可能である。例えば、ＥＳＮを署名手続きへの入力として使用し、在圏通信システムがＡＵＴＨＢＳおよびＡＵＴＨＳＳＤの計算を実行する場合、ＥＳＮは、ホーム通信システムから在圏通信システムへ送信されることが可能である。注意すべき点であるが、ＩＳ－４１に関して、在圏通信システムとホーム通信システムとの間の通信は通常、装置への発呼がなされるたびにではなく、ワイヤレス装置が在圏通信システムに登録するたびに実行される。また、ワイヤレス装置がホーム通信システムにあるときに同じ手続きを実行することも可能である。その場合、在圏通信システムではなくホーム通信システムが、装置と通信する。装置と通信システムとの間の通信は、サービス基地局を通る。

【００４４】

さらに、この鍵更新システムは、更新鍵を用いて通信鍵を更新して鍵更新における認証を実行するために、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡあるいはＧＳＭのようなさまざまな多元接続方式に基づく通信システムで使用可能である。例えば、本発明の鍵更新システムは、ＣＤＭＡ２０００スペクトラム拡散方式(CDMA 2000 Spread Spectrum Systems)のＴＩＡ／ＥＩＡ／ＩＳ－２０００標準で指定される標準、セルラ方式移動局・地上局間互換性仕様(Cellular System Mobile Station-Land Station Compatibility Specification)のＥＩＡ／ＴＩＡ／ＩＳ－５５３で指定される標準、セルラ方式デュアルモード移動局・基地局：ディジタル制御チャネル(Cellular System Dual Mode Mobile Station-Base Station : Digital Control Channel)のＩＳ－１３６で指定される標準、あるいはその他の標準のような、さまざまな標準の下で動作するシステムにおいて使用可能である。理解されるべき点であるが、さまざまな値、入力およびアーキテクチャブロックの異なる記法、用語および特徴づけも使用可能である。例えば、ホーム通信システムについて記述した機能は、ホーム認証センタ、ホームロケーションレジスタ（ＨＬＲ）あるいはホームＭＳＣでも実行可能であり、在圏通信システムの機能は、在圏認証センタ、在圏ロケーションレジスタ

あるいは在圏ＭＳＣでも実行可能である。理解されるべき点であるが、上記のアーキテクチャのシステムおよびその一部は、本発明の原理に従って当業者に理解されるように、装置内の処理回路において、通信システムの別の位置において、あるいは、特定用途向け集積回路、ソフトウェア駆動処理回路、ファームウェアまたはその他のディスクリート素子の構成において、実装あるいは統合することが可能である。

【００４５】

【発明の効果】

以上述べたごとく、本発明によれば、更新鍵を用いて認証を実行することによって、鍵更新システムは、通信鍵をホーム通信システムに維持しながら更新鍵を在圏通信システムへ送ることにより、ホーム通信システムと在圏通信システムとの間の通信を低減することができる。

【図面の簡単な説明】

【図１】本発明の原理による更新鍵を用いた鍵更新を使用可能なワイヤレス通信システムの概略図である。

【図２】ＩＳ－９５Ｂに基づいてワイヤレス装置とワイヤレス通信システムとの間で使用される、鍵更新と、別個の認証手続きを示す図である。

【図３】ＩＳ－４１準拠ネットワークのような通常のネットワークにおける更新プロセスのための、ワイヤレス装置と、在圏通信システムと、ホーム通信システムの間の通信を示す図である。

【図４】本発明の原理に従って、更新鍵を用いて通信システムを認証する鍵更新システムの実施例を示す図である。

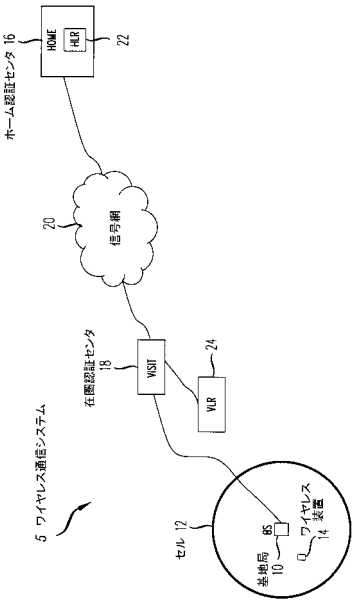
【図５】Ａは、本発明の原理に従って相互認証とともに鍵更新を実行する際の更新鍵および通信鍵を生成する方法を示す図である。Ｂは、本発明の原理に従って更新鍵を用いて相互認証を実行する鍵更新システムの実施例の流れ図である。

【符号の説明】

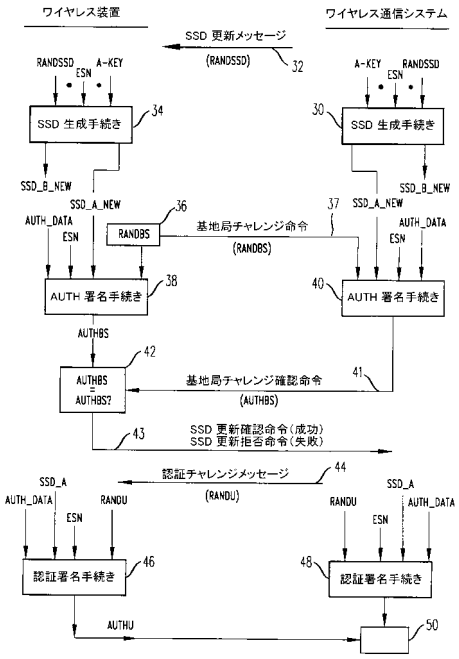
５　ワイヤレス通信システム
１０　基地局
１２　地理的領域（セル）
１４　ワイヤレス装置
１６　ホーム認証センタ
１８　在圏認証センタ
２０　信号網
２２　ホームロケーションレジスタ（ＨＬＲ）
２４　在圏ロケーションレジスタ（ＶＬＲ）
３０　ＳＳＤ生成手続き
３２　ＳＳＤ更新メッセージ
３４　ＳＳＤ生成手続き
３６　ＲＡＮＤＢＳ
３７　基地局チャレンジ
３８　署名手続き
４０　署名手続き
４１　基地局チャレンジ確認命令
４３　ＳＳＤ更新確認
４４　認証チャレンジメッセージ
４６　認証署名手続き
４８　認証署名手続き
６０　ホーム通信システム
６２　在圏通信システム
６３　鍵更新システム
６４　装置

６５　通信システム
６７　暗号化関数Ｆ０
６８　暗号化関数Ｆ１
６９　署名手続き
７０　ホーム通信システム
７１　在圏通信システム
７２　更新指令
７８　認証報告
８０　鍵および署名値生成手続き
８２　暗号化関数（Ｆ０）
８４　暗号化関数（Ｆ１）
８６　署名手続き
８８　署名手続き
９０　ホーム通信システム
９２　在圏通信システム
９３　更新指令
９４　装置
９６　更新メッセージ
９８　ランダムチャレンジメッセージ
１００　チャレンジ応答

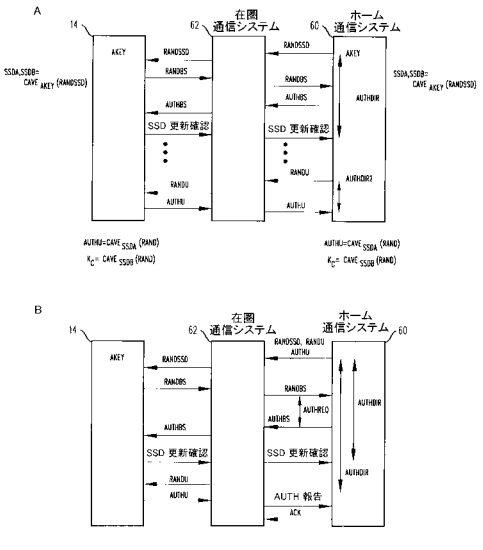
【図１】



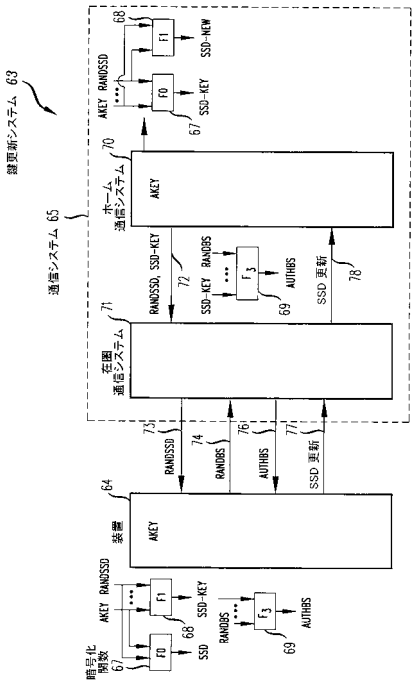
【図２】



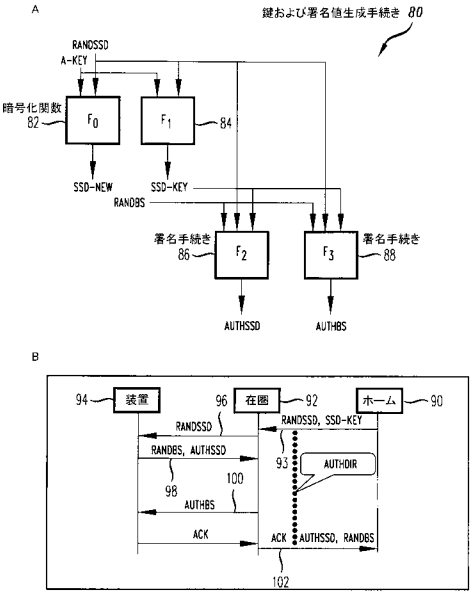
【図３】


A
在圏
通信システム
ホーム
通信システム
AKEY
RANDSSD
RANDBS
AUTHBS
SSD 更新確認
RANDU
AUTHU
AUTHDIR
AUTHDIR2
B
AUTH 報告
ACK

【図４】


鍵更新システム 63
通信システム 65
ホーム
通信システム
在圏
通信システム
装置
AKEY
RANDSSD
SSD-KEY
SSD-NEW
RANDBS
AUTHBS
SSD 更新
暗号化関数
SSD

【図５】


A
鍵および署名値生成手続き 80
RANDSSD
A-KEY
暗号化関数
SSD-NEW
SSD-KEY
RANDBS
署名手続き
AUTHSSD
AUTHBS
B
装置
在圏
ホーム
RANDSSD, SSD-KEY
AUTHDIR
ACK

フロントページの続き

(72)発明者 セミョン ビー、ミジコフスキー
アメリカ合衆国、０７７５１ ニュージャージー、モーガンビル、イエローナイフ ロード ２２７

審査官 中里 裕正

(56)参考文献 欧州特許出願公開第００９７７４５２（ＥＰ，Ａ１）
Cellular Radiotelecommunications Intersystem Operations, 3GPP2 N.S0005-0, Version 1.0, p.3-193 - 3-195, ＵＲＬ, http://www.3gpp2.org/public_html/specs/N.S0005-0_v1.0.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/08
H04B 7/26