(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3667576号
(P3667576)
(45)発行日　平成17年7月6日(2005.7.6)　(24)登録日　平成17年4月15日(2005.4.15)

(51)Int.Cl.[7]		F I		
H04L	9/32	H04L	9/00	675A
H04L	9/08	H04L	9/00	601C
H04Q	7/38	H04B	7/26	109R

請求項の数 11　(全 15 頁)

(21)出願番号　特願平11-319721
(22)出願日　平成11年11月10日(1999.11.10)
(62)分割の表示　特願平4-267809の分割
　原出願日　平成4年9月11日(1992.9.11)
(65)公開番号　特開2000-124898(P2000-124898A)
(43)公開日　平成12年4月28日(2000.4.28)
　審査請求日　平成11年11月10日(1999.11.10)
(31)優先権主張番号　759312
(32)優先日　平成3年9月13日(1991.9.13)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　１００１３－２４１２
ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　３２
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】通信チャネルを開設するための方法および移動機

(57)【特許請求の範囲】

【請求項１】

秘密コード列を保持する移動機によって実行される、基地局との通信チャネルを開設するための方法において、

ａ．基地局からディジタル乱数信号列を受信するステップと、

ｂ．前記ディジタル乱数信号列と、前記移動機を特徴づけるビット列と、少なくとも前記秘密コード列をハッシュすることにより導出されるキーとを含むストリングを生成するステップと、

ｃ．前記ストリングをハッシュしてハッシュストリングを生成するステップと、

ｄ．認証処理における比較のために前記ハッシュストリングを基地局へ送信するステップとを有することを特徴とする、通信チャネルを開設するための方法。

【請求項２】

開設される通信チャネルはワイヤレス通信チャネルであることを特徴とする請求項１に記載の方法。

【請求項３】

開設される通信チャネルはセルラ無線通信チャネルであることを特徴とする請求項１に記載の方法。

【請求項４】

移動機が基地局の管轄内に入ったことを判定するステップをさらに有することを特徴とする請求項１に記載の方法。

【請求項５】
前記ステップｄは、前記ストリングの少なくとも一部も送信することを特徴とする請求項１に記載の方法。
【請求項６】
前記移動機が発呼しようとするときに前記ステップａ～ｄの実行を開始させるステップをさらに有することを特徴とする請求項１に記載の方法。
【請求項７】
前記基地局が前記移動機を活性化させて着呼させようとするときに前記ステップａ～ｄの実行を開始させるステップをさらに有することを特徴とする請求項１に記載の方法。
【請求項８】
前記基地局が前記移動機を再認証しようとするときに前記ステップａ～ｄの実行を開始させるステップをさらに有することを特徴とする請求項１に記載の方法。
【請求項９】
秘密コード列を保持する移動機であって、前記移動機が、
基地局からディジタル乱数信号列を受信する手段と、
前記ディジタル乱数信号列と、前記移動機を特徴づけるビット列と、少なくとも前記秘密コード列をハッシュすることにより導出されるキーとを含むストリングを生成する手段と、
前記ストリングをハッシュしてハッシュストリングを生成する手段と、
認証処理における比較のために前記ハッシュストリングを基地局へ送信する送信手段とを有することを特徴とする移動機。
【請求項１０】
移動機が基地局の管轄内に入ったことを判定する手段をさらに有することを特徴とする請求項９に記載の移動機。
【請求項１１】
前記送信手段は、前記ストリングの少なくとも一部も送信することを特徴とする請求項９に記載の移動機。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】
本発明は、認証プロトコルに関し、特に、セルラ無線電話などの通信の妥当性を保証するためのプロトコルに関する。
【０００２】
【従来の技術】
米国における現在のセルラ電話配置のもとでは、セルラ電話加入者が呼を発すると、そのセルラ電話はサービス提供者に対し料金請求のために発呼者の識別番号を指示する。この情報は暗号化されない。詐欺者がうまい時刻に盗聴すると、その加入者の識別情報を取得することができる。
【０００３】
技術があれば、盗聴者が、与えられたセル内のすべてのセルラ周波数を自動的に走査して、そのような識別情報を検索することが可能である。その結果、セルラ電話サービスの侵害が横行する。また、音声信号の暗号化の欠如は、盗聴者に、会話の内容をさらす。要するに、セルラ電話技術において有効なセキュリティ手段に対する明らかな需要が存在し、認証およびプライバシーを保証するために暗号技術を使用することが示唆される。
【０００４】
セルラ電話技術に存在する一般的な種類の認証問題を解決するためにいくつかの標準的暗号化方法が存在するが、これらはそれぞれ実際上の問題を有することが分かっている。第１に、古典的なチャレンジ／応答プロトコルが、公開鍵暗号化アルゴリズムに基づいて使用される。この方法では、加入者の移動局には、ホームシステムによっても知られている秘密鍵が発行される。サーバシステムが加入者を認証しようとする場合、ホームシステム

に、与えられた加入者とともに使用するチャレンジおよび応答を問い合わせる。サーバシステムはホームシステムによって提供された応答と移動局によって提供された応答を比較し、それらが一致した場合、移動局は認証される。

【０００５】

この方法の問題点は、しばしばサーバシステムが呼設定の認証をするのに十分急速にホームシステムと接触することができないこと、または、ホームシステムのデータベースソフトウェアが加入者の秘密鍵を参照しチャレンジ／応答対を十分急速に作成することができないことである。

【０００６】

公開鍵暗号化は、認証問題を解決するための方法の他の標準的クラスを与える。一般的に、各移動局には、サービス提供者の公開鍵によって署名され、その移動局はサービス提供者の正当な顧客であることを宣言する、識別番号の「公開鍵証明書」が与えられる。さらに、各移動局には、正当な顧客であることを第三者（例えばサーバシステム）に対して証明するために、その証明書とともに使用することができるハッシュデータ（個人鍵）も与えられる。

【０００７】

例えば、サービス提供者がＲＳＡ鍵の対（Ｆ，Ｇ）を有するとする。Ｆは個人鍵、Ｇは公開鍵である。サービス提供者は、各移動局に自分のＲＳＡ鍵の対（Ｄ，Ｅ）を、Ｆ（Ｅ）（提供者の個人鍵Ｆを使用して移動局の公開鍵Ｅを暗号化したもの）とともに提供する。移動局は、サーバシステムに（Ｅ，Ｆ（Ｅ））を送ることによって同一性を主張する。サーバシステムはＧをＦ（Ｅ）に適用してＥを取得する。サーバシステムはチャレンジＸを生成し、移動局の公開鍵Ｅでそれを暗号化して移動局に送るＥ（Ｘ）を取得する。移動局は個人鍵ＤをＥ（Ｘ）に適用してＸを取得し、応答として正当なサーバに送り返す。

【０００８】

【発明が解決しようとする課題】

この方式のいくつかの変形は、他のものよりも計算量やデータ伝送量が少ないが、現在セルラ電話で使用される種類のハードウェアで１秒以下で効率的に実行可能な公開鍵認証方式はまだ存在しない。サーバシステムとホームシステムの間のネットワーク接続は、当面の認証には必要でないが、古典的方法の場合のように、古典的方法を排除した同じ時間制約が公開鍵方式をも排除する。

【０００９】

【課題を解決するための手段】

セルラ電話技術のセキュリティ需要は、共有秘密データフィールドによる配置によって満たされる。移動装置は、サービス提供者によってそれに割り当てられた秘密を保持し、その秘密から共有秘密データフィールドを生成する。サービス提供者もその共有秘密データフィールドを生成する。移動装置がベース局のセルに入ると、自分自身をベース局に認知させ、ハッシュ認証文字列をベース局に与える。ベース局は提供者に問い合わせ、その移動装置が正当な装置であると判定された場合、提供者はベース局に共有秘密データフィールドを提供する。その後、移動装置は、共有秘密データフィールドを使用して、移動装置とベース局の間で実行される認証プロセスの助けを借りて、ベース局と通信する。

【００１０】

この配置の１つの特徴は、異なるベース局は、提供者によって移動装置に組み込まれた秘密へのアクセス許可を有しないことである。また、移動装置との対話に成功したベース局のみが共有秘密データフィールドを有する。

【００１１】

他方、より多くの時間がかかる、秘密を使用する認証プロセスは、提供者が関わる場合にのみ起こるが、これは、移動装置が最初にセルに入るとき（または共有秘密データフィールドが損傷を受けた疑いがあるとき）であり、頻繁には起こらない。

【００１２】

本発明の原理によれば、移動装置とベース局の両方が、暗号鍵の対を作成するために共有

秘密データフィールドの一部を使用する。この対の第１暗号鍵は、移動装置によって音声を暗号化するために使用され、ベース局によって音声を復号するために使用される。対の第２暗号鍵は、ベース局によって音声を暗号化するために使用され、移動装置によって音声を復号するために使用される。

【００１３】

共有秘密データフィールドを作成するために使用されるのと同じハッシュ関数が、暗号鍵の対を作成するために使用される。

【００１４】

暗号化される制御メッセージは、自己反転暗号化プロセスに従う３つの連続した変換によって暗号化される。第１の変換では、暗号化するメッセージの各語に乱数が加算される。この乱数は、共有秘密データフィールドの一部からなるハッシュ文字列に関係し、この文字列は、共有秘密データフィールドを導出する際に使用されるハッシュ関数によってハッシュされるものである。

【００１５】

第２の変換では、制御メッセージ（第１変換によって変更されたもの）を構成する語の集合が前半と後半に分割され、前半が部分的に後半に基づいて変更される。第３の変換では、暗号化するメッセージ（第２変換によって変更されたもの）の各語から乱数が減算される。この場合も、この乱数は、共有秘密データフィールドの一部からなるハッシュ文字列に関係し、この文字列は、共有秘密データフィールドを導出する際に使用されるハッシュ関数によってハッシュされるものである。

【００１６】

【実施例】

移動セルラ電話配置においては、多くの移動電話、それよりもずっと少数のセルラ無線提供者（各提供者は１つ以上のベース局を有する）、および、１つ以上の交換ネットワーク提供者（コモンキャリア）が存在する。セルラ無線提供者およびコモンキャリアは、セルラ電話加入者がセルラおよび非セルラ電話加入者のいずれとも通信できるように協力する。

【００１７】

この配置を図１に示す。コモンキャリアＩおよびコモンキャリアＩＩが、交換機１０～１４からなる交換ネットワークを形成するために協力する。固定装置２０および２１は交換機１０に接続され、移動装置２２および２３は自由に移動し、ベース局３０～４０は交換機１０～１４に接続される。ベース局３０～３４は提供者１に属し、ベース局３５および３６は提供者２に属し、ベース局３７は提供者４に属し、ベース局３８～４０は提供者３に属する。説明のため、ベース局とは、１個以上の送信機があるセルと同義語とする。セルの集合体はセルラ地理サービスエリア（ＣＧＳＡ）を構成する（例えば、図１のベース局３０、３１、および３２）。

【００１８】

各移動装置は、その装置に固有の電子シリアル番号（ＥＳＮ）を有する。ＥＳＮ番号は、装置が製造される際にメーカーによって組み込まれ（例えば、読みだし専用メモリ内に）、変更不可能である。しかし、アクセスは可能である。

【００１９】

顧客が、所有またはリースしている移動装置に対するサービスアカウントの設定を要求すると、サービス提供者はその顧客に、電話番号（ＭＩＮ１指定）、エリアコード指定（ＭＩＮ２指定）および「秘密」（Ａキー）を割り当てる。ＭＩＮ１およびＭＩＮ２指定は提供者の所定のＣＧＳＡに付随し、図１の配置のすべてのベース局は、特定のＭＩＮ２およびＭＩＮ１の対が属するＣＧＳＡを識別することができる。Ａキーは、顧客の機器および提供者のＣＧＳＡプロセッサ（図１で明確には図示せず）のみに既知である。ＣＧＳＡプロセッサは装置のＥＳＮ、Ａキー、ＭＩＮ１およびＭＩＮ２指定ならびにサービス供給者が有することを所望する他の情報を保持する。

【００２０】

ＭＩＮ１およびＭＩＮ２指定ならびにＡキーが組み込まれると、顧客の装置は、ＣＧＳＡプロセッサがその移動装置に特殊な乱数シーケンス（ＲＡＮＤＳＳＤ）および「共有秘密データ」（ＳＳＤ）フィールドの作成の指令を送ると、サービスのために初期化される。ＣＧＳＡは、移動装置が存在するセルのベース局を通じて、ＲＡＮＤＳＳＤ、およびＳＳＤフィールド生成指令を送る。ＳＳＤフィールドの作成は図２のプロトコルに従う。

【００２１】

ちなみに、図１の配置では、各ベース局は、ある事前に割り当てられた周波数チャネル（同報バンド）でセル内の全装置に情報を同報する。さらに、各ベース局は、相互に同意した（一時的に）専用のチャネルを通じて各移動装置と双方向通信を維持する。ベース局と移動装置が通信チャネルについて同意する方法は本発明にとって重要ではないため、詳細な説明はしない。例えば、ある方法では、移動装置が全チャネルを走査し、空いたチャネルを選択する。続いて移動装置はベース局にそのＭＩＮ２およびＭＩＮ１指定を送り（平文形式でまたは公開鍵で暗号化して）、ベース局が認証プロセスを開始することを可能にする。いったん認証された通信が設定されれば、必要ならば、ベース局は移動局に対し他のチャネルに切り替えるよう指示する。

【００２２】

以下でさらに詳細に説明するように、本発明の移動電話システムで通話を設定し維持する際に、対話を通して認証プロセスが何回か実行される。従って、使用される認証プロセスは比較的に安全で簡単に実現できるものであるべきである。設計を単純化し実現化費用を低減するため、移動装置およびベース局はいずれも同じプロセスを使用すべきである。

【００２３】

多くの認証プロセスは、プロセスを実現するために、ハッシュ関数または一方向関数を使用する。ハッシュ関数は、「秘密」を署名に変換する多対一写像を実現する。以下で、簡単で、高速で、有効で、かつ柔軟なハッシュ関数の１つを説明する。これは本発明の認証プロセスに非常に適しているが、もちろん他のハッシュ関数も使用可能である。

【００２４】

［ジャンブルプロセス］

ジャンブルプロセスは、ｋ語の鍵ｘ（ｊ）の助けを借りて、ｄ個の「秘密」データｂ（ｉ）からなるブロックの「署名」を作成することができる。ただし、ｄ、ｉ、ｊ、およびｋは整数である。「署名」作成プロセスは、一度に１データ語ずつに対して実行される。説明のため、ジャンブルプロセスが作用する語は８ビット長（０～２５５の範囲を与える）とするが、他のワードサイズも使用可能である。

【００２５】

「秘密」データブロック長はのこぎり波関数で実現される。

$s_d(t) = t \quad (0 \leqq t \leqq d-1)$

$s_d(t) = 2d-2-t \quad (d \leqq t \leqq 2d-3)$

$s_d(t) = s_d(t+2d-2) \quad$ （すべてのｔに対して）

この関数は以下のプロセスで使用される。ただし、ｚ＝０およびｉ＝０から開始し、ｉは$0 \leqq i \leqq 6d-5$の範囲の順次増大する整数値である。

【００２６】

ａ）　$b(s_d(i))$は、$b(s_d(i)) = b(s_d(i)) + x(i_k) + SBOX(z) \mod 256$　によって更新される。ただし、

＊　$i_k = i \mod k$,　$SBOX(z) = y + [y/2048] \mod 256$

＊　$y = (z \# 16)(z+111)(z)$

＊　［ｙ／２０４８］はｙ／２０４８の整数部分であり、＃はビットごとの排他的ＯＲ関数を表す。

ｂ）　ｚは、$z = z + b(s_d(i)) \mod 256$　によって更新される。

【００２７】

このプロセスでは、データと鍵の実際の区別がないことに注意すべきである。従って、認証に使用される任意の文字列は、上記プロセスの鍵として使用される部分を有することが

できる。逆に、鍵と連結されたデータワードは、「認証文字列」とみなすことができる。また、各語ｂ（ｉ）（ただし０≦ｉ＜ｄ）は、一度に１語ずつ個別にハッシュされ、これはハッシュを「その場で」実行する。ハッシュプロセス自体には追加バッファは不要である。

【００２８】

上記のプロセスは、非常に基本的な従来のプロセッサで容易に実行可能である。その理由は、必要な演算は、（２０４８による除算を実行するための）シフト、（[]関数およびｍｏｄ２５６関数を実行するための）切り捨て、加算、乗算、およびビットごとの排他的ＯＲ関数である。

【００２９】

図２のＳＳＤフィールド初期化プロセスに戻って、ＲＡＮＤＳＳＤシーケンスおよび新たなＳＳＤフィールド作成の指令（図２の矢印１００）が移動局によって受信されると、新たなＳＳＤフィールドが図４に従って生成される。移動装置は、ＥＳＮ指定、Ａキー、およびＲＡＮＤＳＳＤシーケンスを連結して認証文字列を形成する。認証文字列は、ＳＳＤフィールドを出力する（上記の）ジャンブルブロック１０１に送られる。

【００３０】

ＳＳＤフィールドは２個のサブフィールドからなる。ＳＳＤ－Ａサブフィールドは、認証手続きをサポートするために使用される。ＳＳＤ－Ｂサブフィールドは音声プライバシー手続きおよびいくつかのシグナリングメッセージ（後で説明）の暗号化をサポートするために使用される。注意すべき点は、上記のようにして形成されたＳＳＤフィールドを再分割することによって、または、最初にＳＳＤフィールドを拡張することによって、さらに多くのＳＳＤサブフィールドを作成することも可能であることである。ＳＳＤフィールド内のビット数を増大させるには、より多くのデータビットから開始するだけでよい。以下の説明から分かるように、これは困難な条件ではない。

【００３１】

ホームＣＧＳＡプロセッサは、受信したＭＩＮ２およびＭＩＮ１指定が割り当てられた移動装置のＥＳＮおよびＡキーを知っている。ホームＣＧＳＡプロセッサはまた、送ったＲＡＮＤＳＳＤシーケンスも知っている。従って、ホームＣＧＳＡプロセッサは、移動装置のＳＳＤフィールド作成プロセスを繰り返すことができる位置にある。ＲＡＮＤＳＳＤ信号をＥＳＮ指定およびＡキーと連結することにより、上記のジャンブルプロセスによって、ＣＧＳＡプロセッサは新たなＳＳＤフィールドを作成し、それをＳＳＤ－ＡおよびＳＳＤ－Ｂサブフィールドに分割する。しかし、ホームＣＧＳＡプロセッサで作成されたＳＳＤフィールドは確認されなければならない。

【００３２】

図２に従って、作成されたＳＳＤフィールドの確認が移動装置によって開始される。ブロック１０２で、移動装置は乱数チャレンジシーケンス（ＲＡＮＤＢＳシーケンス）を生成し、サーバベース局（移動装置が位置するエリアをサービスするベース局）を通じてそれをホームＣＧＳＡプロセッサに送る。図５に従って、ホームＣＧＳＡプロセッサは、チャレンジＲＡＮＤＢＳシーケンス、移動装置のＥＳＮ、移動装置のＭＩＮ１指定、および新たに作成されたＳＳＤ－Ａを連結して、ジャンブルプロセスに送る認証文字列を形成する。

【００３３】

このとき、ジャンブルプロセスは、移動局に送るハッシュ認証信号ＡＵＴＨＢＳを作成する。移動局もまた、ＲＡＮＤＢＳシーケンス、そのＥＳＮ指定、そのＭＩＮ１指定および新たに作成されたＳＳＤ－Ａを連結してジャンブルプロセスに送る認証文字列を形成する。移動局は、そのジャンブルプロセスの結果を、ホームＣＧＳＡプロセッサから受信したハッシュ認証信号（ＡＵＴＨＢＳ）と比較する。比較ステップ（ブロック１０４）が一致を示した場合、移動局は、ＳＳＤフィールドの更新が成功したことを示す確認メッセージをホームＣＧＳＡプロセッサに送る。そうでない場合、移動局は一致比較の失敗を報告する。

【００３４】
移動局を初期化した後、ＳＳＤフィールドは、ホームＣＧＳＡプロセッサが新たなＳＳＤフィールドの作成を指示するまで有効である。その指示は、例えば、ＳＳＤフィールドが損傷を受けたと信ずる理由がある場合に起こり得る。このような場合、ホームＣＧＳＡプロセッサは他のＲＡＮＤＳＳＤシーケンスおよび新たなＳＳＤフィールドの作成の指令を移動装置に送る。
【００３５】
上記のように、セルラ電話技術では、各ベース局は、そのセル内のすべての移動装置のためにさまざまな情報信号を同報する。図１の管理方法によれば、ベース局によって同報される信号のうちの１つは乱数または擬似乱数シーケンス（ＲＡＮＤシーケンス）である。ＲＡＮＤシーケンスは、移動装置によって作成され送信される信号を乱数化するためにさまざまな認証プロセスによって使用される。もちろん、ＲＡＮＤシーケンスは、記録／再生攻撃を防ぐために周期的に変更しなければならない。ＲＡＮＤ信号の潜伏期を選択する１つの方法は、予想される平均通話時間よりも小さくとることである。その結果、移動装置は、一般的に、連続する通話に異なるＲＡＮＤ信号を使用することになる。
【００３６】
本発明の１つの目的によれば、移動装置は、セルに入ったことを検知するとすぐに認証可能なようにベース局に登録する。移動装置は、認証された場合にのみ、通話を開始すること、または、ベース局に対して移動装置への通話を指示することができる。
【００３７】
移動装置は、登録プロセスを開始すると、ベース局によって同報されたＲＡＮＤシーケンスを受信し、そのＭＩＮ１およびＭＩＮ２指定ならびにそのＥＳＮシーケンス（平文で）を、ハッシュ認証文字列とともに送信する。図６に従って、ハッシュ認証文字列は、ＲＡＮＤシーケンス、ＥＳＮシーケンス、ＭＩＮ１指定およびＳＳＤ－Ａサブフィールドを連結して認証文字列を形成し、その認証文字列をジャンブルプロセスに送ることによって導出される。ジャンブルプロセスの出力のハッシュ認証文字列は、ＥＳＮシーケンスとともにサーバベース局に送られる。
【００３８】
ある実施例では、移動装置によって使用されるＲＡＮＤシーケンスの全部または一部が（ＥＳＮシーケンスならびにＭＩＮ１およびＭＩＮ２指定とともに）サーバベース局にも送られる。その理由は、ハッシュ認証文字列がベース局に到達するときまでにＲＡＮＤ値が変化する可能性があるためである。
【００３９】
ベース局側では、サーバベース局は、ＲＡＮＤシーケンスを知っており（ベース局がそれを作成したため）、また、移動装置が確認したＥＳＮならびにＭＩＮ２およびＭＩＮ１指定をも知っている。しかし、サーバベース局は、移動装置のＳＳＤフィールドは知らない。それが（ＭＩＮ１およびＭＩＮ２指定から）知っているのは、移動装置のホームＣＧＳＡプロセッサの識別情報である。
【００４０】
その結果、認証プロセスは、移動装置のホームＣＧＳＡプロセッサへ、ＭＩＮ１指定、ＥＳＮシーケンス、移動装置が作成し送信したハッシュ認証文字列、およびサーバベース局が同報した（そして、移動装置が、作成したハッシュ認証文字列に組み込んだ）ＲＡＮＤシーケンスを送ることによって進行する。移動装置のＭＩＮ１指定およびＥＳＮシーケンスから、ホームＣＧＳＡプロセッサは、移動装置の識別情報、およびそれによって、移動装置のＳＳＤ－Ａサブフィールドを知る。
【００４１】
従って、移動装置がしたのと同じように認証文字列を作成し、それをジャンブルプロセス（図６）に送ることができる。移動装置のホームＣＧＳＡプロセッサによって作成されたハッシュ認証文字列が、移動装置で作成されサーバベース局によって提供されたハッシュ認証文字列と一致した場合、確認は成功と認められる。このような場合、ホームＣＧＳＡ

プロセッサはサーバベース局にその装置のＳＳＤフィールドを提供する。ちなみに、ＥＳＮ指定およびＳＳＤフィールドを安全に保持するため、ベース局とＣＧＳＡプロセッサの間の通信は暗号化形式で実行される。

【００４２】

上記のプロトコルでは、移動装置のＣＧＳＡプロセッサは、ハッシュ認証文字列の正当性の確認を試みる。確認が失敗した場合、ＣＧＳＡプロセッサは、サーバベース局に対し、移動装置は認証されなかったことを通知し、移動装置との接触が放棄されるか、または、移動装置に登録プロセスの再試行が指示されるべきであることを提案する。登録プロセスを再試行するためには、ホームＣＧＳＡプロセッサは、認証プロセスへの関与を続行するか、または、それをサーバベース局に委任することができる。

【００４３】

後者の場合、サーバベース局はホームＣＧＳＡプロセッサに対し移動装置のＥＳＮシーケンスおよびＭＩＮ１指定を通知し、ＣＧＳＡプロセッサは移動装置のＳＳＤフィールドおよびＳＳＤフィールドの作成に使用されたＲＡＮＤＳＳＤを応答する。ハッシュ認証文字列を作成し、それを移動装置によって送信されたハッシュ認証文字列と比較するという意味で、認証がサーバベース局によって実行される。続いて、ホームＣＧＳＡプロセスがサーバ局によって移動装置にＲＡＮＤＳＳＤを送信することなしに再試行指令が実行可能である。この「登録」プロトコルを図３に示す。

【００４４】

移動装置が（上記のプロセスによって）サーバベース局に「登録」されると、サーバベース局は移動装置のＥＳＮおよびＳＳＤフィールドを所有し、そのセルでの以後の認証プロセスは、次の１つの場合を除いてホームＣＧＳＡプロセッサの参照なしにサーバベース局で実行可能である。何らかの理由で、ＳＳＤフィールドを変更したい場合には、通信はホームＣＧＳＡプロセッサと移動装置の間で有効であり、サーバベース局はこの通信のための通路としてのみ作用する。その理由は、新たなＳＳＤフィールドの作成は秘密Ａキーへのアクセスを必要とし、ＣＧＳＡプロセッサによるＡキーへのアクセスは全く許されていないためである。

【００４５】

従って、新たなＳＳＤフィールドが作成され移動装置がホームＣＧＳＡのエリアに存在しない場合、次のことが起こる。

・　ホームＣＧＳＡプロセッサはＲＡＮＤＳＳＤシーケンスを作成し、そのＲＡＮＤＳＳＤシーケンスに基づいてＳＳＤフィールドを変更する。

・　ホームＣＧＳＡプロセッサはサーバベース局にＲＡＮＤＳＳＤシーケンスおよび新たに作成されたＳＳＤフィールドを提供する。

・　サーバベース局は、移動装置に対し、そのＳＳＤフィールドを変更するよう指示し、移動装置にＲＡＮＤＳＳＤシーケンスを提供する。

・　移動装置はＳＳＤフィールドを変更し、サーバベース局にチャレンジを送る。

・　サーバベース局は（上記の）ＡＵＴＨＢＳ文字列を作成し、それを移動装置に送る。

・　移動装置はＡＵＴＨＢＳ文字列を確認し、サーバベース局に対し、移動装置およびサーバベース局の両方が同一のＳＳＤフィールドを有することを通知する。

【００４６】

サーバベース局によって登録された後、移動装置は図７の認証プロセスとともに通話を開始することができる。通話開始シーケンスは、信号ＲＡＮＤ、ＥＳＮ、ＳＳＤ－Ａおよび少なくともいくつかの被呼者識別（電話）番号（図７のＭＩＮ３）を連結する。連結された信号は、サーバベース局によって確認可能なハッシュ認証シーケンスを生成するためにジャンブルプロセスに送られる。もちろん、サーバベース局での確認を可能にするためには、被呼者識別情報（および、以前のように、おそらくＲＡＮＤ信号の一部）はベース局によって受信可能な方法（例えば平文）で送信されなければならない。認証シーケンスが確認されると、ベース局は通話を処理し被呼者への接続を形成することが可能となる。

【００４７】

移動装置が「被呼者」である場合に移動装置に接続するためのプロトコルは図６の登録プロトコルに従う。すなわち、サーバベース局は、被呼移動局に対し、ＲＡＮＤシーケンス、ＥＳＮ指定、ＭＩＮ１指定およびＳＳＤ－Ａサブフィールドから作成された認証シーケンスを送信することを要求する。認証が実行されると、ベース局と被呼者移動装置の間には、被呼者移動装置が、通話を発信した移動装置（または固定装置）から発信されたデータを受信し、それにデータを送信するためのパスが設定される。

【００４８】

上記のすべての認証は、認証されるパケットすなわち文字列自体に関してのみ（確認されるという意味で）有効であることに注意すべきである。その他の場合にセキュリティを強化するためには、３つの異なる付加的なセキュリティ手段が使用可能である。それらは、音声暗号化、臨時の再認証、および制御メッセージ暗号化である。

【００４９】

［音声暗号化］

音声信号は、最初にそれをディジタル形式に変換することによって暗号化される。これはさまざまな従来の方法で実現可能であり、圧縮や誤り訂正符号を加えることもできる。ディジタル信号のビットはＫビットからなる連続するグループに分割され、各グループが暗号化される。特に、移動装置およびベース局の両方において、ＲＡＮＤシーケンス、ＥＳＮおよびＭＩＮ１指定、ならびにＳＳＤ－Ｂサブフィールドは連結されジャンブルプロセスに送られる。

【００５０】

ジャンブルプロセスは２Ｋビットを生成し、これらのビットはそれぞれＫビットからなるグループＡおよびＢに分割される。移動装置では、グループＡが出力音声を暗号化するために使用され、グループＢが入力音声を復号するために使用される。逆に、ベース局では、グループＡが入力音声を復号するために使用され、グループＢが出力音声を暗号化するために使用される。図８はこの音声暗号化および復号プロセスを示す。

【００５１】

［再認証］

ベース局の希望により、ベース局によってアクティブであると信じられている移動装置が、実際に、アクティブであると認定された移動装置であることを確認するために、再認証プロセスが開始される。これは、ベース局によって、移動装置に対し、図９に従ってハッシュ認証シーケンスの送信を要求することによって実現される。このような各要求とともに、ベース局は特殊な（ＲＡＮＤＵ）シーケンスを送信する。移動装置は、ＲＡＮＤＵシーケンス、移動装置のエリアコードＭＩＮ２指定、ＭＩＮ１指定およびＳＳＤ－Ａ指定を連結することによってハッシュ認証シーケンスを作成する。連結された文字列はジャンブルプロセスに送られ、生じたハッシュ認証文字列がベース局に送られる。ベース局は、この時点で、ハッシュ認証文字列が正当であることを確認することができる位置にある。

【００５２】

［制御メッセージ暗号系］

第３のセキュリティ手段は、制御メッセージのプライバシーの保証を取り扱う。設定された通話の間に、制御メッセージの送信を要求するさまざまな状況が生じることがある。ある場合は、制御メッセージは通話を発信した移動局またはベース局に重大な悪影響を与えることがある。このため、対話の進行中に送信されるある種の制御メッセージを（十分に）暗号化することが所望される。あるいは、選択されたメッセージ種の選択されたフィールドを暗号化することも可能である。これは、クレジットカード番号のような「データ」制御メッセージや、通話再定義制御メッセージを含む。これは制御メッセージ暗号系によって実現される。

【００５３】

制御メッセージ暗号系（ＣＭＣ）は以下の性質を有する対称鍵暗号系である。

１）　比較的安全である。

２）　８ビットコンピュータ上で効率的に動作する。

３）　自己反転的（すなわち、包合的）である。
【００５４】
ＣＭＣの暗号鍵は、次のようにして「秘密」（例えば、ＳＳＤ－Ｂサブフィールド）から導出される、２５６バイトの配列ＴＢＯＸ［ｚ］である。
１．　０≦ｚ＜２５６の範囲の各ｚに対し、ＴＢＯＸ［ｚ］＝ｚとおく。
２．　配列ＴＢＯＸ［ｚ］および秘密（ＳＳＤ－Ｂ）をジャンブルプロセスに送る。
これは、本質的に、（図８のビット数が２５６バイトではなく２Ｋバイトであることを除いては）図８の要素３０１、３０２および３０３で示されたものである。
【００５５】
鍵が導出されると、ＣＭＣが、制御メッセージを暗号化および復号するために使用可能となる。あるいは、鍵が使用されるたびごとに、鍵を「大急ぎで」導出することも可能である。ＣＭＣは複数バイトの可変長メッセージを暗号化する能力を有する。ＣＭＣの操作は自己反転的、逆数的、包合的である。すなわち、平文を生じるために暗号文に対してなされる操作と、暗号文を生じるために平文に対してなされる操作が、完全に同一である。包合的関数とは、自分自身の逆であるような関数である（例えば、ｘ＝１／ｘ′、ｘ′＝Ｔ（Ｔ（ｘ′））。従って、ＣＭＣ操作を２度実行すると、データは不変のままである。
【００５６】
以下の説明では、暗号化プロセス（および復号プロセス）に対し、平文（または暗号文）はデータバッファ内に存在し、ＣＭＣは、そのデータバッファの内容に対し、データバッファの最終内容が暗号文（または平文）を構成するように作用する、と仮定する。これは、図１０の要素５０２および５０４が１つの同一のレジスタでよいことを意味する。
【００５７】
ＣＭＣは３つの連続する段階からなり、それぞれデータバッファ内の各バイト列を変更する。ＣＭＣ全体およびＣＭＣの第２構成段階がいずれも包合的であることに注意すべきである。データバッファの長さががｄバイトであり、各バイトをｂ（ｉ）で表すとき、０≦ｉ＜ｄの範囲のｉに対し、
Ｉ．ＣＭＣの第１段階は次の通りである。
１．　変数ｚを０に初期化する。
２．　０≦ｉ＜ｄの範囲の連続する整数値ｉに対し、
ａ．　変数ｑを、ｑ＝ｚ＃（ｉの下位バイト）によって形成する。ただし、＃はビットごとのブール排他的ＯＲ演算子である。
ｂ．　変数ｋを、ｋ＝ＴＢＯＸ［ｑ］によって形成する。
ｃ．　ｂ（ｉ）を、ｂ（ｉ）＝ｂ（ｉ）＋ｋ　ｍｏｄ　２５６　と更新する。
ｄ．　ｚを、ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６　と更新する。
【００５８】
ＩＩ．　ＣＭＣの第２段階は包合的であり、次の通りである。
１．　０≦ｉ＜（ｄ－１）／２の範囲のｉのすべての値に対し、ｂ（ｉ）＝ｂ（ｉ）＃（ｂ（ｄ－１－ｉ）ＯＲ　１）　とする。ただし、ＯＲはビットごとのブールＯＲ演算子である。
ＩＩＩ．　ＣＭＣの最終段階は、第１段階の逆である復号である。
１．　変数ｚを０に初期化する。
２．　０≦ｉ＜ｄの範囲の連続する整数値ｉに対し、
ａ．　変数ｑを、ｑ＝ｚ＃（ｉの下位バイト）によって形成する。
ｂ．　変数ｋを、ｋ＝ＴＢＯＸ［ｑ］によって形成する。
ｃ．　ｚを、ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６　と更新する。
ｄ．　ｂ（ｉ）を、ｂ（ｉ）＝ｂ（ｉ）－ｋ　ｍｏｄ　２５６　と更新する。
【００５９】
選択された制御およびデータメッセージを暗号化および復号するために使用されるこれら３段階のプロセスを図１０に示す。１つの所望される実施例では、第１段階および第３段階はそれぞれ自己鍵暗号化および復号である。自己鍵系は、系の出力が以後の系の出力に

作用するために使用されるような時間変動系である。暗号および自己鍵系に関するこれ以上のことは、Ｗ．ディフィー、Ｍ．Ｅ．ヘルマン著「プライバシーと認証：暗号入門」Ｉ．Ｅ．Ｅ．Ｅ．会議録第６７巻第３号（１９７９年３月）を参照。

【００６０】

［移動装置機器］

図１１は、移動装置ハードウェアのブロック図である。これは、セルラ電話のキーパッド、受話器および装置の電源制御スイッチ（図示せず）を含む制御ブロック２００を有する。制御ブロック２００はプロセッサ２１０に接続される。プロセッサ２１０は、音声信号をディジタル表現に変換すること、誤り訂正符号を組み込むこと、出力ディジタル音声信号を暗号化すること、入力音声信号を復号すること、さまざまな制御メッセージを形成および暗号化（さらに復号）すること、などのような、移動装置の動作を制御する。

【００６１】

ブロック２１０は、信号の送受信に関連する回路の集合からなるブロック２２０に結合される。ブロック２００～２２０は、市販の移動電話装置によって現在実行されている機能を実行する（市販の装置は暗号化および復号は実行しないが）、基本的には従来のブロックである。これまで説明した認証および暗号化プロセスを実現するため、図１１の装置は、プロセッサ２１０に結合したいくつかのレジスタからなるブロック２４０と、同じくプロセッサ２１０に結合した「個性」モジュール２３０をも含む。モジュール２３０は、移動電話装置の物理的構造の一部でもよいし、ソケットインタフェースを通じて移動電話装置に結合した取り外し可能（かつはめ込み可能）なモジュールでもよい。これは、電磁パスすなわち接続を通じてプロセッサ２１０に結合してもよい。要するに、モジュール２３０は、例えば、「スマートカード」である。

【００６２】

モジュール２３０はジャンブルプロセッサ２３１およびプロセッサ２３１に付随するいくつかのレジスタからなる。あるいは、他の所望される実施例では、Ａキーのみがモジュール２３０内に存在する。Ａキー、ならびにＭＩＮ１およびＭＩＮ２指定を、ブロック２４０のレジスタではなく、モジュール２３０のレジスタに組み込む（そして保持する）ことからいくつかの利益が生じる。

【００６３】

生成されたＳＳＤフィールドをモジュール２３０のレジスタに格納することも有益である。さらに、プロセッサ２３１のプロセスを実行するために必要な作業レジスタをモジュール２３０のレジスタに含めることも有益である。これらの要素をモジュール２３０に含めることにより、ユーザは、それを異なる移動装置（例えば「拡張」移動装置）で使用し、重要な情報がモジュール外に格納されることがないようにするために、モジュールを携帯することができる。もちろん、移動装置は、モジュール２３０が装置の統合的かつ永続的部分であるように生産することも可能である。このような実施例では、ジャンブルプロセッサ２３１はプロセッサ２１０内に合併することができる。ブロック２４０は、装置のＥＳＮ指定および受信されるさまざまなＲＡＮＤシーケンスを格納する。

【００６４】

上記の説明はセルラ電話環境における加入者認証について述べられており、携帯用ポケット受話器に使用される個人通信ネットワークを含むものであるが、本発明の原理は、通信が十分に安全ではないと認識され、模写が潜在的問題であるような他の状況における利用可能性を有することは明らかである。これには例えばコンピュータネットワークが含まれる。

【００６５】

【発明の効果】

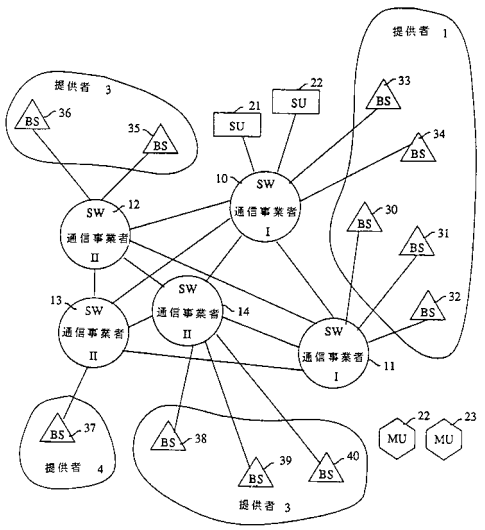
以上述べたごとく、本発明によれば、現在セルラ電話で使用される種類のハードウェアを使用して、高速で効率的に実行可能な公開鍵認証方式が与えられる。

【図面の簡単な説明】

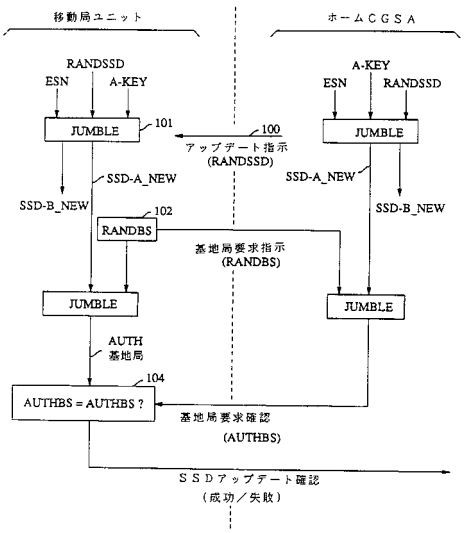
【図１】固定電話および移動電話の両方へサービスするために相互接続された、ネットワ

ーク提供者とセルラ無線提供者の配置図である。
【図２】共有秘密データフィールドの作成およびその確認を指示するプロセスを示す図である。
【図３】例えば移動装置が最初にベース局によってサービスされるセルに入った場合の、訪問先のベース局における登録プロセスを示す図である。
【図４】共有秘密データを作成するために連結されハッシュされた要素を示す図である。
【図５】確認シーケンスを作成するために連結されハッシュされた要素を示す図である。
【図６】移動装置が発信する際に、登録シーケンスを作成するために連結されハッシュされた要素を示す図である。
【図７】呼開始シーケンスを作成するために連結されハッシュされた要素を示す図である。
【図８】移動装置における音声暗号化および復号のプロセスを示す図である。
【図９】再認証シーケンスを作成するために連結されハッシュされた要素を示す図である。
【図１０】選択された制御およびデータメッセージを暗号化および復号するための３段プロセスを示す図である。
【図１１】移動装置のハードウェアのブロック図である。
【符号の説明】
１０～１４　交換機
２０、２１　固定装置
２２、２３　移動装置
３０～４０　ベース局
２００　制御ブロック
２１０　プロセッサ
２３１　ジャンブルプロセッサ

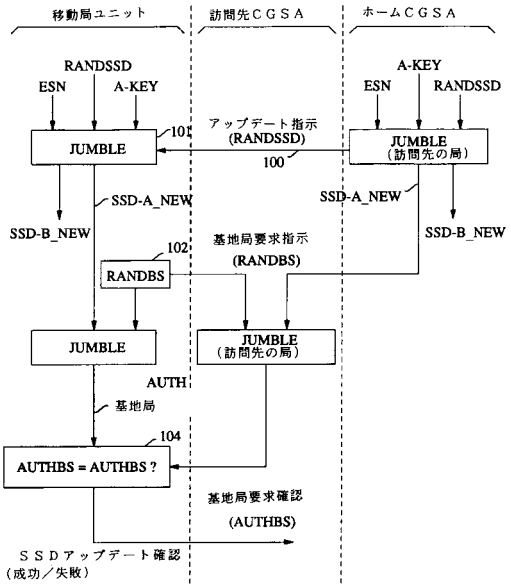
【図１】



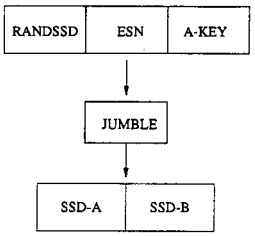
【図２】



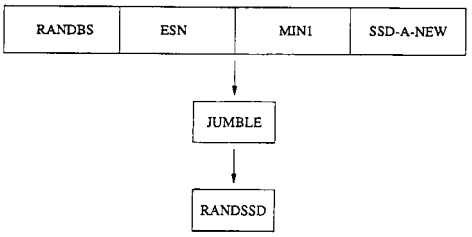
【図３】



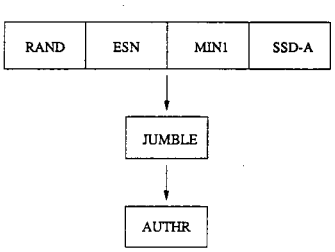
【図４】



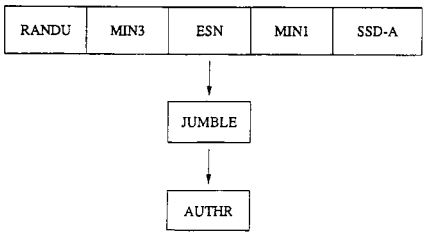
【図５】



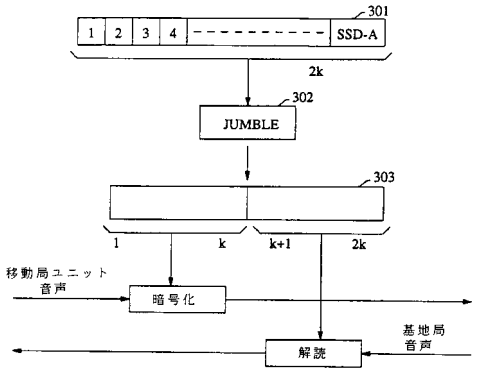
【図６】



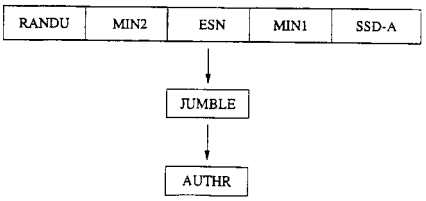
【図７】



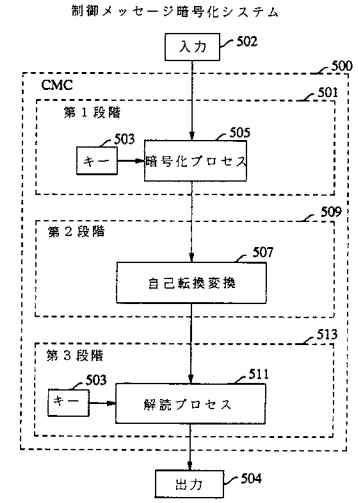
【図８】



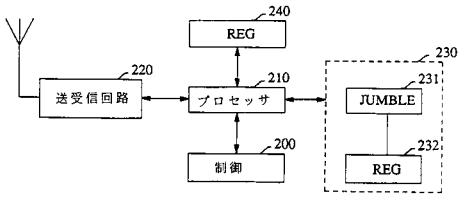
【図９】



【図１０】


制御メッセージ暗号化システム
入力
502
500
CMC
501
第１段階
503
キー
505
暗号化プロセス
509
第２段階
507
自己転換変換
513
第３段階
503
キー
511
解読プロセス
出力
504

【図１１】


240
REG
230
220
送受信回路
210
プロセッサ
231
JUMBLE
200
制御
232
REG

フロントページの続き

(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(72)発明者 ジェームス アレクサンダー リーズ サード
アメリカ合衆国 ０７９７４ ニュージャージー ニュープロヴィデンス、サウスゲート ロード １２７
(72)発明者 フィリップ アンドリュー トラヴァンティ
アメリカ合衆国 ０７９７４ ニュージャージー マーレーヒル、キャンドルウッド ドライヴ １５

審査官 青木 重徳

(56)参考文献 特開平０３－２０６７４４（ＪＰ，Ａ）
特開昭６４－１００５８６（ＪＰ，Ａ）
特開昭６３－７０６３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 9/32
H04L 9/08
H04Q 7/38