(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-509384
(P2005-509384A)
(43)公表日　平成17年4月7日(2005.4.7)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
H04Q 7/38	H04B	7/26	109S	5K067
	H04L	9/00	601E	

審査請求 未請求　予備審査請求 有　（全 15 頁）

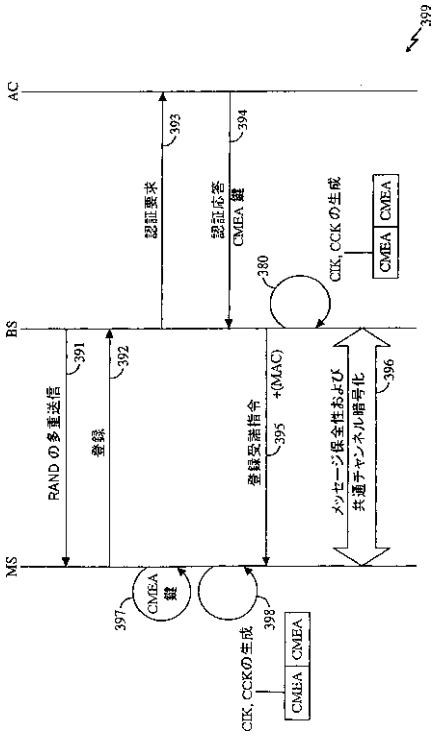
(21)出願番号　特願2003-543347 (P2003-543347)
(86)(22)出願日　平成14年10月31日 (2002.10.31)
(85)翻訳文提出日　平成16年5月6日 (2004.5.6)
(86)国際出願番号　PCT/US2002/035297
(87)国際公開番号　WO2003/041442
(87)国際公開日　平成15年5月15日 (2003.5.15)
(31)優先権主張番号　10/011,964
(32)優先日　平成13年11月5日 (2001.11.5)
(33)優先権主張国　米国 (US)

(71)出願人　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　100058479
弁理士　鈴江　武彦
(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　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】ＣＤＭＡ通信システムにおけるメッセージ保全性のための方法及び装置

(57)【要約】
【課題】移動局と基地局とがメッセージ保全性の実行を可能とすること。
【解決手段】通信システム１００において、この方法及び装置は、認証センタ１９８、又は認証センタ１９８と移動切換センタ１９９との間のインタフェース１９７の動作バージョンに関わらず、メッセージ保全性を提供する。この方法及び装置は、携帯メッセージ暗号アルゴリズム（ＣＭＥＡ）鍵を生成することと、移動局と基地局との間のメッセージ保全性のために、ＣＭＥＡ鍵に基づいて、ＣＭＥＡ鍵から導出される保全性鍵（ＣＩＫ）を生成することとを含んでいる。移動局は、登録メッセージを基地局に送信し、移動局が、基地局から、登録受諾指令または認証ベクトルの要素を受信したかに基づいて、基地局と通信している認証センタ１９８の動作バージョンを決定する。万が一、移動局が、基地局から有効な登録受諾指令を受信した場合には、ＣＩＫがＣＭＥＡ鍵に基づいて生成される。



【特許請求の範囲】
【請求項１】
通信システムにおける方法であって、
携帯メッセージ暗号アルゴリズム鍵を生成することと、
移動局と基地局との間のメッセージ保全性のために、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することと
を備えた方法。
【請求項２】
請求項１に記載の方法において、
前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することは、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成するために、前記携帯メッセージ暗号アルゴリズム鍵を二回繰り返すことを含む方法。
【請求項３】
請求項１に記載の方法において、
前記移動局と前記基地局とは、前記通信システムにおける逆方向及び順方向の通信のそれぞれについて、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することを、ローカルに実行する方法。
【請求項４】
通信システムにおける装置であって、
携帯メッセージ暗号アルゴリズム鍵を生成する手段と、
移動局と基地局との間のメッセージ保全性のために、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成する手段と
を備えた装置。
【請求項５】
請求項４に記載の装置において、
前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成する手段は、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成するために、前記携帯メッセージ暗号アルゴリズム鍵を二回繰り返す手段を含む装置。
【請求項６】
請求項４に記載の装置において、
前記移動局と前記基地局とは、逆方向及び順方向の通信のそれぞれについて、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することを、ローカルに実行する手段を含む装置。
【請求項７】
通信システムにおいて使用されるプロセッサであって、
携帯メッセージ暗号アルゴリズム鍵を生成する手段と、
前記通信システムにおける移動局と基地局との間のメッセージ保全性のために、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成する手段と
を備えたプロセッサ。
【請求項８】
請求項７に記載のプロセッサにおいて、
前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成する手段は、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成するために、前記携帯メッセージ暗号アルゴリズム鍵を二回繰り返す手段を含むプロセッサ。
【請求項９】
移動局における方法であって、

登録メッセージを基地局に送信することと、
前記移動局が、前記基地局から、登録受諾指令または認証ベクトルの要素を受信したかに基づいて、前記基地局と通信している認証センタの動作バージョンを決定することとを備えた方法。
【請求項１０】
請求項９に記載の方法において、
携帯メッセージ暗号アルゴリズム鍵を生成することと、
万が一、前記移動局が前記基地局から前記登録受諾指令を受信した場合には、前記移動局と前記基地局との間のメッセージ保全性のために、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することと
を更に備えた方法。
【請求項１１】
請求項１０に記載の方法において、
前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することは、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成するために、前記携帯メッセージ暗号アルゴリズム鍵を二回繰り返すことを含む方法。
【請求項１２】
請求項１０に記載の方法において、
前記移動局と前記基地局とは、前記通信システムにおける逆方向及び順方向の通信のそれぞれについて、前記携帯メッセージ暗号アルゴリズム鍵に基づいて、前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵を生成することを、ローカルに実行する方法。
【請求項１３】
請求項１０に記載の方法において、
前記携帯メッセージ暗号アルゴリズム鍵から導出される保全性鍵に基づいて、メッセージ認証コードを生成することと、
前記基地局の正当性を確認するために、前記移動局のための前記登録受諾指令の通信用に前記メッセージ認証コードを使用することと
を更に備えた方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に通信の分野に関し、特に携帯通信システムにおける通信に関する。
【背景技術】
【０００２】
コード分割多元接続（ＣＤＭＡ）通信システムは、初期の世代から更に発展した世代へと進化している。システムを更新する時に、システムの様々な操作に関連した１つ以上のパラメータが変わりうる。より進化したシステムにおける移動局もまた、新たなパラメータ内で動作するように更新される。初期の世代のシステムの１つは、本書で参考文献として組み込んでいるTIA/EIA-95A/B規格で定義されたパラメータに従って動作する。進化したシステムの１つは、本書で参考文献として組み込んでいるTIA/EIA-IS-2000-A規格に従って動作する。この特許出願の時期に、TIA/EIA-IS-2000-A規格の新たなバージョンの改訂がなされており、本書で参考文献として組み込んでいるTIA/EIA-IS-2000-B規格として発表される。この規格の写しは、http://www.3gpp2.orgのアドレスのWWWにアクセスすることによって、または、TIA, Standards and Technology Department, 2500 Wilson Boulevard, Arlington, Va. 22201, United States of Americaに手紙を書くことによって得られる。
【０００３】
通信システムは、多くの異なる構成要素を持っている。各構成要素の動作パラメータは

、対応する規格によって定義される。対応する規格の新たなバージョンに従って動作するように、新たなシステムは、ある構成要素を変更することによって部分的に更新される。提案されたTIA/EIA-IS-2000-B規格の指令及び本質的な特徴は、移動局と基地局との間の通信のメッセージ保全性を提供している。メッセージ保全性は、メッセージの送信者の正当性を保証する。メッセージ保全性を達成するために、認証および鍵合意（ＡＫＡ：Authentication and Key Agreement）処理が発展し、規格の関連セクションで定義されている。認証センタ（ＡＣ）は、システムで動作している移動局に関連する認証情報を管理する構成要素である。移動切換センタ（ＭＳＣ）とＡＣとの間のインタフェースの動作パラメータは、ＡＫＡ処理を実行するために、初期のバージョンからアップグレードされる必要がある。ＭＡＳ－ＡＣインタフェースアップグレードがないと、アップグレードされた移動局と、ＡＫＡ処理を実行することができる基地局とは、ＭＳＣ－ＡＣインタフェースを経由してＡＫＡ情報を運ぶためのシステムの欠如によって、このＡＫＡ処理を実際に実行することができない。その結果、メッセージ保全性は実行できない。このような条件は、基地局と移動局とが、ＭＳＣ－ＡＣインタフェースをアップグレードする前に、提案されたTIA/EIA-IS-2000-B規格にしたがって動作するようにアップグレードされた場合に深刻な展開問題となる。

【０００４】

この目的のために、より進化した世代の移動局と基地局とが、メッセージ保全性を実行することを可能とする方法及び装置に対する必要性がある。

【発明の開示】

【０００５】

通信システムでは、方法及び装置が、認証センタ、または認証センタと移動切換センタとの間のインタフェースの動作バージョンに関わらず、メッセージ保全性を提供する。この方法及び装置は、携帯メッセージ暗号化アルゴリズム（ＣＭＥＡ）鍵を生成することと、移動局と基地局との間のメッセージ保全性のためのＣＭＥＡ鍵に基づいてＣＭＥＡ鍵から導出される保全性鍵（ＣＩＫ）を生成することとを含んでいる。この移動局は、基地局へ登録メッセージを送信する。そして、この移動局が、基地局から、登録受諾指令又は認証ベクトルの要素を取得したかに基づいてこの基地局と通信している認証センタの動作バージョンを判定する。仮にこの移動局が基地局から有効な登録受諾指令を取得した場合には、ＣＭＥＡ鍵に基づいてＣＩＫが生成される。このＣＩＫは、ＣＭＥＡ鍵を２回繰り返すことによって生成される。この移動局と基地局とは、この通信システムにおける逆方向及び順方向通信のそれぞれのために、ＣＭＥＡ鍵に基づいてＣＩＫをローカルに生成する。

【発明を実施するための最良の形態】

【０００６】

本発明の特徴、目的、および利点は、全体を通じて同一のまたは類似の要素を示す同一参照符号を示す図面を用いた以下の詳細記載から更に明白になるであろう。

【０００７】

本発明の種々の実施例は、コード分割多元接続（ＣＤＭＡ）技術に従って動作する無線通信システムに組み込まれる。ＣＤＭＡ技術は、開示され、Telecommunication Industry Association（ＴＩＡ）及び他の規格組織によって発行された種々の規格に記載されている。図１は、本発明の様々な実施例を含んでいるコード分割多元接続（ＣＤＭＡ）通信システム規格のうちの何れかに従って動作することが可能な通信システム１００の一般的なブロック図である。通信システム１００は、音声、データ、またはその両方の通信のためのものでありうる。一般に、通信システム１００は、基地局１０１とデータネットワーク１０５とを含んでいる。この基地局１０１は、移動局１０２～１０４のような多くの移動局間、及び移動局１０２～１０４と公衆切換電話との間の通信リンクを提供する。本発明の主要な範囲と種々の利点から逸脱することなく、図１における移動局は、データ接続局と称され、基地局はデータ接続ネットワークと称される。基地局１０１は、基地局コントローラ及び基地トランシーバシステムのような多くの構成要素を含む。簡略化のために、

それら構成要素は図示してない。基地局１０１はまた、例えば基地局１６０のような他の基地局とも通信する。基地局１０１および基地局１６０に接続されたＭＳＣ１９９は、本通信システム１００の種々の動作局面を制御する。ＡＣ１９８は、システム１００に提供された認証サービスの管理を行うＭＳＣ１９９と通信しうる。ＡＣ１９８とＭＳＣ１９９との間のインタフェース１９７は、認証プロセスに関連した適切な情報の通信のための通信媒体を提供する。

【０００８】

基地局１０１は、そのカバー領域にある各移動局と、基地局１０１から送信された順方向リンク信号を経由して通信する。この移動局１０２～１０４に向けられた順方向リンク信号は合計され、順方向リンク信号１０６が形成される。順方向リンク信号１０６を受信する移動局１０２～１０４の各々は、順方向リンク信号１０６を復号し、ユーザに対する情報を抽出する。基地局１６０はまた、順方向リンク信号を経由して、そのカバー領域にある移動局と通信する。移動局１０２～１０４は、対応する逆方向リンクを経由して、基地局１０１および基地局１６０と通信する。各々の逆方向リンクは、例えば各移動局１０２～１０４のそれぞれに対する各逆方向リンク信号１０７～１０９のような逆方向リンク信号によって維持される。

【０００９】

図２は、受信ＣＤＭＡ信号の処理及び復調を行うために使用される受信機２００のブロック図を示す。受信機２００は、逆方向及び順方向リンク信号上の情報を復号するために使用されうる。受信されたサンプルは、ＲＡＭ２０４に格納される。受信サンプルは、無線周波数／中間周波数（ＲＦ／ＩＦ）システム２９０とアンテナシステム２９２によって生成される。ＲＦ／ＩＦシステム２９０とアンテナシステム２９２とは、多様化ゲインを受信するために、多数の信号を受信し、この受信した信号のＲＦ／ＩＦ処理を行う１つ以上の構成要素を含みうる。多数の受信信号は、異なる伝搬経路を通って伝搬された共通ソースからのものでありうる。アンテナシステム２９２は、ＲＦ信号を受信し、このＲＦ信号をＲＦ／ＩＦシステム２９０に渡す。ＲＦ／ＩＦシステム２９０は、あらゆる従来式ＲＦ／ＩＦ受信機でありうる。この受信されたＲＦ信号は、フィルタをかけられ、ダウンコンバートされ、デジタル化されることによって、基本帯域周波数におけるＲＸサンプルが形成される。このサンプルは、復調器（ｄｅｍｕｘ）２０２に供給される。ｄｅｍｕｘ２０２の出力は、サーチャユニット２０６とフィンガエレメント２０８との供給される。制御ユニット２１０は、そこに接続されている。結合器２１２は、復号器２１４をフィンガエレメント２０８に接続している。制御ユニット２１０は、ソフトウェアによって制御されるマイクロプロセッサでありうる。また、同一の集積回路か、または別個の集積回路に配置されうる。復号器２１４における復号機能は、ターボ復号器か、または任意の他の適切なアルゴリズムに従っている。

【００１０】

動作中、受信サンプルは、ｄｅｍｕｘ２０２に供給される。ｄｅｍｕｘ２０２は、このサンプルを、サーチャユニット２０６及びフィンガエレメント２０８に供給する。制御ユニット２１０は、フィンガエレメント２０８が、サーチャユニット２０６からの検索結果に基づいて、異なる時間オフセットにおいて受信信号の復調と逆拡散とを実行できるようにしている。この復調の結果は結合され、復号器２１４に渡される。復号器２１４は、このデータを復号し、デコードされたデータを出力する。この復号プロセスは、受信データを逆暗号化するためのプロセスを含む。チャンネルの逆拡散は、この受信サンプルを、ＰＮシーケンスの複素共役と、単一タイミング仮説において割り当てられたＷａｌｓｈ関数とによって積算し、この結果得られたサンプルをデジタル的にフィルタリングすることによって実行される。これには、集積ダンプアキュムレータ回路（図示せず）がしばしば用いられる。そのような技術は、当該技術分野では良く知られている。

【００１１】

図３は、逆方向および順方向リンク信号を送信するための送信機３００のブロック図を示す。送信のためのトラフィックチャンネルデータが、変調されるために変調器３０１に

入力される。この変調は、ＱＡＭ、ＰＳＫ、あるいはＢＰＳＫなどの良く知られた変調技術のうちの何れかに従いうる。データは、変調器３０１におけるデータ速度で符号化される。この変調器３０１への入力データは、メッセージ保全性を実行するためのデータを含む。このデータ速度は、データ速度／出力レベルセレクタ３０３によって選択される。逆方向リンク信号のために、このデータ速度選択は、受信基地局からのフィードバック情報に基づいている。従って、このデータ速度／出力レベルセレクタ３０３は、変調器３０１におけるデータ速度を選択する。変調器３０１の出力は、アンテナ３０４から送信されるために、ブロック３０２内の信号拡散動作／増幅を経る。また、パイロット信号がブロック３０７において生成される。このパイロット信号は、ブロック３０７において適切なレベルに増幅される。このパイロット信号の出力レベルは、受信基地局におけるチャンネル条件にしたがっている。このパイロット信号は、結合器３０８において、トラフィックチャンネル信号と結合される。この結合された信号は、増幅器３０９内で増幅され、アンテナ３０４から送信される。このアンテナ３０４は、アンテナアレイと、複数入力複数出力構成とを含むあらゆる数の組み合わせでありうる。データ速度／出力レベルセレクタ３０３はまた、フィードバック情報に従って、送信された信号の増幅レベルのための出力レベルを選択する。この選択されたデータ速度と出力レベルの組み合わせによって、送信されたデータの受信基地局における適切な復号が可能となる。

【００１２】

移動局１０２は、基地局１０１のカバー領域から、基地局１６０のカバー領域へとロームしうる。移動局は、基地局１０１および基地局１６０とのソフトハンドオフプロセスを経る。ハンドオフプロセスは一般に知られている。移動局１０２は、基地局１６０からの順方向リンク信号１６１を受信し、逆方向リンク信号１１７を送信することによって、通信サービスの使用を継続する。ＡＣ１９８は、移動局と、基地局１０１および基地局１６０のうちの何れかとの間の安全な通信のために暗号鍵を認証し、提供する。

【００１３】

図４のメッセージフロー３９９に示すように、本発明の種々の局面に従った認証及び暗号化のためのメッセージフローが示されている。このメッセージフロー３９９に含まれている基地局と移動局とは、提案されたTIA/EIA-IS-2000-B規格に従って動作している。この場合、ＡＣ１９８は、提案されたTIA/EIA-IS-2000-B規格における関連するセクションにしたがって動作するような更新がなされていない。ＡＣ１９８とＭＳＣ１９９との間のインタフェースは、TIA/EIA-IS-2000-Bで概説されているようなメッセージ保全性と暗号化の動作に対して適切であって、本書で参考文献として組み込まれているANSI-41規格に適合して動作するように更新されていない。この基地局は、ランダムアクセス番号（ＲＡＮＤ）メッセージ３９１を全ての移動局に多重送信する。移動局はＲＡＮＤを使って、登録メッセージ３９２を生成する。基地局は、登録メッセージによって運ばれた認証情報を、ＭＳＣ－ＡＣインタフェース１９７を経由して、認証要求メッセージ３９３によってＡＣ１９８に通信する。ＡＣ１９８は、認証要求メッセージ内の認証情報を、予期された値と比較し、移動局の認証を確認し、携帯メッセージ暗号化アルゴリズム鍵（ＣＭＥＡ鍵）３９４を運ぶ認証応答メッセージを生成する。このＣＭＥＡ鍵の生成によって、移動局と基地局との間の暗号通信が可能となる。移動局では、この内部メッセージ３９７によって、同一のＣＭＥＡ鍵も生成される。この移動局は、このローカルに生成されたＣＭＥＡ鍵に基づいて、内部メッセージ３９８によって、ＣＭＥＡ鍵から導出される暗号鍵（ＣＣＫ）をローカルに生成する。このＣＣＫは、暗号化のために使われる。またこの移動局は、本発明の実施例に従って、基地局とのメッセージ保全性を実行するためにＣＭＥＡ鍵から導出される保全性鍵（ＣＩＫ）を生成する。このＣＩＫは、ＣＭＥＡ鍵に基づいている。ＣＭＥＡ鍵は、本発明の実施例に従って、２回繰り返されることによってＣＩＫを生成する。基地局はまた、内部メッセージ３８０によってＣＣＫをローカルに生成する。基地局はまた、移動局とのメッセージ保全性のために、ＣＭＥＡ鍵に基づいて同一のＣＩＫを生成する。基地局は、認証応答メッセージ３９３に基づいて、登録受諾指令３９５を移動局に送信する。この登録受諾指令３９５は、メッセージ認証コード（ＭＡＣ）を含んでいる

。ＭＡＣの値は、基地局において生成されたＣＩＫに基づいている。この生成されたＣＩＫは、予め定義された関数に従ってＭＡＣを生成するために、プロセッサへの入力として使用される。それだけに、固有の生成されたＣＩＫに基づく移動局は、この登録受諾指令３９５を送信している基地局の正当性を確認することができる。このポイントの後に、移動局と基地局との間の共通通信３９６が、公知の暗号化アルゴリズムに従って、ＣＣＫを経由して暗号化される。更に、基地局と移動局との間の共通通信２９６は、基地局と移動局とにおいて生成されたＣＩＫに基づくメッセージ保全性チェックを含む。従って、メッセージ保全性機能は、ＡＣ１９８に、TIA/EIA-IS-2000A規格で定義された動作とは異なった動作を要求することなく、移動局と基地局との間の通信のために提供される。

【００１４】

図５のメッセージフロー４００には、認証および暗号化のためのメッセージフローが示されている。ここに示されている基地局と移動局とは、提案されたTIA/EIA-IS-2000-B規格にしたがって動作している。ＡＣ１９８は、TIA/EIA-IS-2000-B規格で定義された適切な規格にしたがって動作している。また、ＭＳＣ－ＡＣインタフェース１９７は、規格ANSI-41の適切なセクションに基づいて更新される。これによって、TIA/EIA-IS-2000-B規格で定義された認証パラメータの通信が可能となる。メッセージフロー４００は、移動局、基地局、およびＡＣ１９８との間で使用される。基地局は、ランダムアクセス番号（ＲＡＮＤ）メッセージ４２１を全ての移動局に多重送信する。移動局は、ＲＡＮＤを使って、登録メッセージ４０１を生成する。その後、基地局は、認証要求メッセージ４０８をＡＣ１９８に送る。その後、ＡＣ１９８は、認証要求メッセージ４０２を送る。メッセージ４０２は、TIA/EIA-IS-2000-Bに従って１セットの認証ベクトル（ＡＶ）を運ぶ。各ＡＶは、保全性鍵（ＩＫ）と暗号化鍵（ＣＫ）とを含む認証のために使用される多くの要素を含む。基地局は、認証ベクトルのうちの一つを選択し、この選択されたＡＶのうちのある要素を、認証要求メッセージ４０３上で移動局に送信する。このＡＶの要素は、ＡＣ１９８において保持されたルート鍵に基づいて生成される。同一のルート鍵はまた、移動局にも格納される。移動局は、通信されたＡＶ要素が、この格納されたルート鍵に基づいて生成されたＡＶ要素と一致するか否かを内部的にチェックする。仮に一致がなされている場合には、有効な移動局が、この基地局を認証していたことになる。このルート鍵と、この通信されたＡＶ要素とに基づいて、移動局は、内部メッセージ４０５を経由してＩＫとＣＫとを内部的に生成する。移動局はまた、この通信されたＡＶ要素に基づいてユーザ応答（ＲＥＳ）を生成する。移動局は、その後、このＲＥＳを、認証応答４０４によって、基地局へ送信する。基地局はまた、内部メッセージ４０６を経由してＩＫとＣＫとをローカルに生成する。基地局は、受信したＲＥＳを、予期されたＲＥＳと比較する。一致した場合には、有効な基地局が、移動局を認証していたことになる。この時に、この通信４０７は、TIA/EIA-IS-2000-Bにしたがってメッセージ保全化と暗号化を実行する。

【００１５】

本発明の種々の局面によって、この認証プロセスからの結果であるＣＭＥＡ鍵を、メッセージ保全を実行するための保全性鍵として使用することが可能となる。移動局は、ＡＣ１９８またはＭＳＣ－ＡＣインタフェース１９７の異なるバージョン以外に、提案されたTIA/EIA/IS-2000-B規格にしたがって動作する基地局を備えたシステムへローミングすることができるので、この移動局は、ＡＣ１９８またはＭＳＣ－ＡＣインタフェース１９７のバージョンがこのシステムに組み込まれているか否かを前もって知る方法を持っていない。更に詳しく言えば、万が一、提案されたTIA/EIA-IS-2000-B規格に従って動作している移動局と基地局とが通信システム１００で通信している一方、ＡＣ１９８が、TIA/EIA-IS-95-BまたはTIA/EIA-IS-2000-Aに従って動作しており、及び／又はＭＳＣ－ＡＣインタフェース１９７がTIA/EIA-IS-95-BまたはTIA/EIA-IS-2000-Aに適切なANSI-41に従って動作している場合には、メッセージ保全性機能の欠如によって、移動局は、基地局との如何なる通信も拒否する。従って、移動局は、複雑なことを追加することなく、ＡＣ１９８またはＭＳＣ－ＡＣインタフェース１９７のシステムに組み込まれているバージョンを区別する方法及び装置を必要とする。

【００１６】
図６に示すように、フローチャート６００は、ＡＣ１９８またはＭＳＣ－ＡＣインタフェース１９７のバージョンに関わらず、移動局がメッセージ保全性鍵を確立し、基地局との認証を実行することを可能にするアルゴリズムを示している。ステップ６０１では、移動局は、認証されているか、または認証されていない。ステップ６０２では、ＡＣ１９８がTIA/EIA-IS-95B又はTIA/EIA-IS-2000-Aに従って動作しているものと仮定すると、移動局は、登録メッセージ３９２を基地局に送信し、ＣＭＥＡ鍵を計算し、内部メッセージ３９７，３９８を経由してＣＩＫ，ＣＣＫを生成する。万が一、この移動局が、成功した認証プロセスを通っている場合には、この移動局は、認証の型式によってＣＩＫあるいはＩＫである保全性鍵を持つであろう。この場合、登録メッセージのメッセージ認証コード（ＭＡＣ）は、この登録メッセージに含まれている。このＭＡＣの存在によって基地局は、移動局とのローカルな認証を実行することが可能となる。これによって、ネットワークにおける認証に関連するトラフィックを低減する。移動局は、基地局からの登録受諾指令３９５を受信することを予定している。ステップ６０３では、移動局が、ＡＣ１９８またはＭＳＣ－ＡＣインタフェース１９７がTIA/EIA-IS-95B及びTIA/EIA-IS-2000-AまたはTIA/EIA-IS-2000-Bに従って動作しているか否かを判定する。TIA/EIA-IS-95B及びTIA/EIA-IS-2000-Aに従った認証は、２Ｇ認証と称される。TIA/EIA-IS-2000-Bに従った認証は３Ｇ認証と称される。移動局がモードに滞在する合計時間を制限するためにタイマが使用される。ステップ６０４において、このタイマが満了すると、このプロセスはステップ６０２において始まる。そして、万が一、移動局が、保全性鍵を持っていない場合には、移動局は、ステップ６０６へと直接移動する。移動局が、基地局からの登録受諾指令３９５を取得した場合には、ＡＣ１９８及びＭＳＣ－ＡＣインタフェース１９７は、２Ｇ認証手続きにしたがって動作する。ステップ６０５におけるプロセスは、ステップ６０６に進む。ステップ６０６では、基地局との共通チャンネル上における通信のためのメッセージ保全と暗号化とを実行するために、移動局が、生成されたＣＭＥＡ鍵を用いて、内部メッセージ３９７，３９８を経由してＣＩＫ，ＣＣＫを導く。仮に、移動局が、基地局から認証要求メッセージ４０３を受信した場合には、ＡＣ１９８とＭＳＣ－ＡＣインタフェース１９７は、３Ｇ認証手続きにしたがって動作する。そのため、ステップ６０５におけるプロセスフローは、ステップ６０７に進み、生成されたＣＭＥＡ鍵とあらゆる未決定のＣＩＫおよびＣＣＫを処分し、ＩＫとＣＫを生成する。ステップ６０７におけるプロセスは、１つ以上のステップを含みうる。ステップ６０８では、ＩＫとＣＫとが、内部メッセージ４０５を経由して生成される。ステップ６０９と６１０では、移動局があるモードに長い時間とどまることを阻止するタイマの使用とともに、基地局とともに、認証が確認される。ステップ６１１では、この移動局は、メッセージの保全と暗号化のために、ＩＫとＣＫとを確立している。ステップ６１２では、この移動局は、基地局に、メッセージの保全と暗号化のための１セットの正しいパラメータを保持する。このプロセスは、移動局が登録を実行することを要求される毎に繰り返される。

【００１７】
これらの知識によって、ここで開示された実施例に関連する様々に例示された論理ブロック、モジュール、回路、およびアルゴリズムステップが、電子工学ハードウェア、コンピュータソフトウェア、あるいはこれらの組み合わせとして適用されることが更に理解されよう。ハードウェアとソフトウェアとの相互互換性を明確に説明するために、様々に例示された部品、ブロック、モジュール、回路、およびステップが、それらの機能に関して一般的に記述された。それら機能がハードウェアとしてあるいはソフトウェアとして適用されているかは、特有の応用例および全体システムに課せられている設計条件による。熟練した技術者であれば、各特定のアプリケーションに応じて変更することによって上述した機能を実施しうる。しかしながら、この適用判断は、本発明の範囲から逸脱したものと解釈すべきではない。

【００１８】
様々に示された論理ブロック、モジュール、および上述された実施例に関連して記載さ

れた回路もまた実装され、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、アプリケーションに固有の集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）またはその他のプログラマブル論理デバイス、ディスクリートゲートあるいはトランジスタ論理、ディスクリートハードウェア部品、あるいは上述された機能を実現するために設計された何れかの組み合わせとともに実行されうる。汎用プロセッサとしてマイクロプロセッサを用いることが可能であるが、代わりに、従来技術によるプロセッサ、コントローラ、マイクロコントローラ、あるいは状態機器を用いることも可能である。プロセッサは、たとえばＤＳＰとマイクロプロセッサとの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアに接続された１つ以上のマイクロプロセッサ、またはその他の配置のような計算デバイスの組み合わせとして実装することも可能である。

【００１９】

ここで開示された実施例に関連して記述された方法やアルゴリズムのステップは、ハードウェアや、プロセッサによって実行されるソフトウェアモジュールや、これらの組み合わせによって直接的に具現化される。ソフトウェアモジュールは、ＲＡＭ、フラッシュメモリ、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、レジスタ、ハードディスク、リムーバブルディスク、ＣＤ－ＲＯＭ、あるいは当該技術分野で知られているその他の型式の記憶媒体に収納されうる。好適な記憶媒体は、プロセッサがそこから情報を読み取り、またそこに情報を書き込むことができるようにプロセッサに結合される。または、記憶媒体はプロセッサに不可欠となりうる。このプロセッサと記憶媒体は、ＡＳＩＣに収納することができる。ＡＳＩＣは、ユーザ端末内に収納することもできる。または、このプロセッサと記憶媒体が、ユーザ端末におけるディスクリートな部品として収納されることもある。

【００２０】

開示された実施例における上述の記載は、いかなる当業者であっても、本発明の活用または利用を可能とするようになされている。これらの実施例への様々な変形例もまた、当業者に対しては明らかであって、ここで定義された一般的な原理は、本発明の主旨または範囲を逸脱しない他の実施例にも適用されうる。このように、本発明は、上記で示された実施例に制限されるものではなく、ここで記載された原理と新規の特徴に一致した広い範囲に相当するものを意図している。

【図面の簡単な説明】

【００２１】

【図１】本発明の種々の実施例に従って動作することが可能な通信システムを示している。

【図２】データを受信し、受信したデータを本発明の種々の局面に従ったデータ速度で復号する通信システム受信機を示している。

【図３】データパケットを、本発明の種々の局面に従ってスケジュールされたデータ速度で送信する通信システム送信機を示している。

【図４】本発明の種々の局面に従った認証及び鍵起動処理を示す図である。

【図５】TIA/EIA-IS-2000-B規格に従った認証及び鍵起動処理を示す図である。

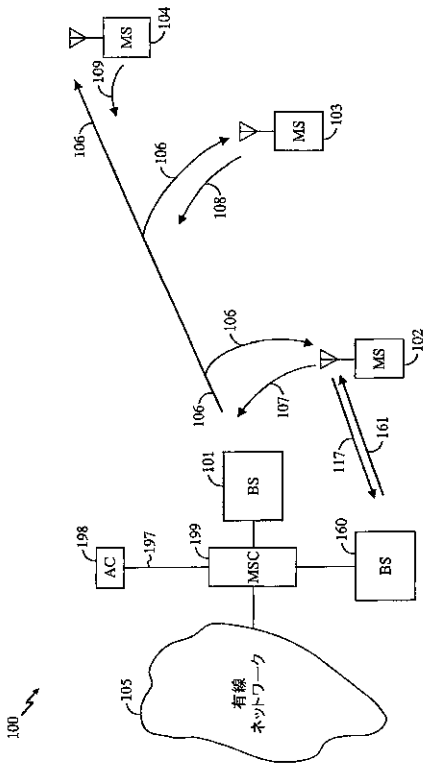
【図６】移動局が、本発明の種々の局面に従った通信システムのメッセージ保全性を実行するための処理フローを示している。

【符号の説明】

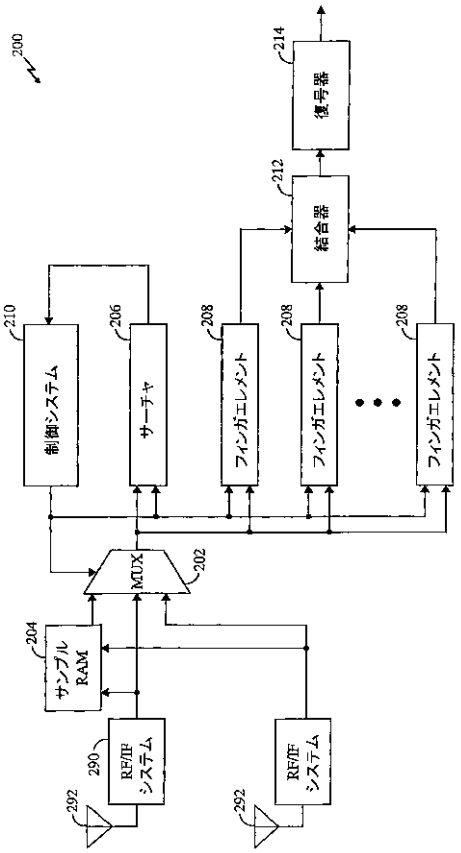
【００２２】

１００…通信システム、１０１…基地局、１０２～１０４…移動局、１０５…データネットワーク、１６０…基地局、１９７…インタフェース、１９８…認証センタ、１９９…移動切換センタ、２００…受信機、２０２…復調器、２０４…ＲＡＭ、２０６…サーチャユニット、２０８…フィンガエレメント、２１０…制御ユニット、２１２…結合器、２１４…復号器、２９０…中間周波数システム、２９２…アンテナシステム、２９６…共通通信、３００…送信機、３０１…変調器、３０３…出力レベルセレクタ、３０４…アンテナ、３０８…結合器、３０９…増幅器

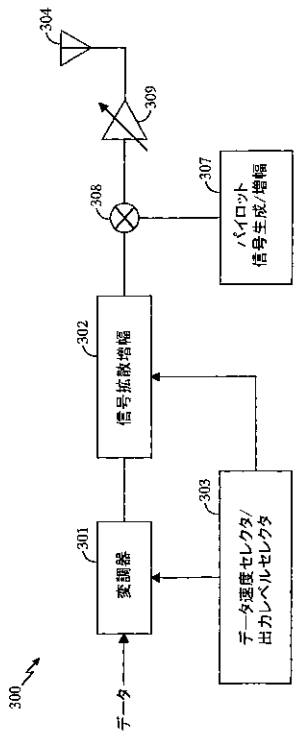
【図１】


MS
104
109
106
MS
103
108
106
106
MS
102
107
161
117
101
BS
198
AC
197
199
MSC
160
BS
105
有線
ネットワーク
100

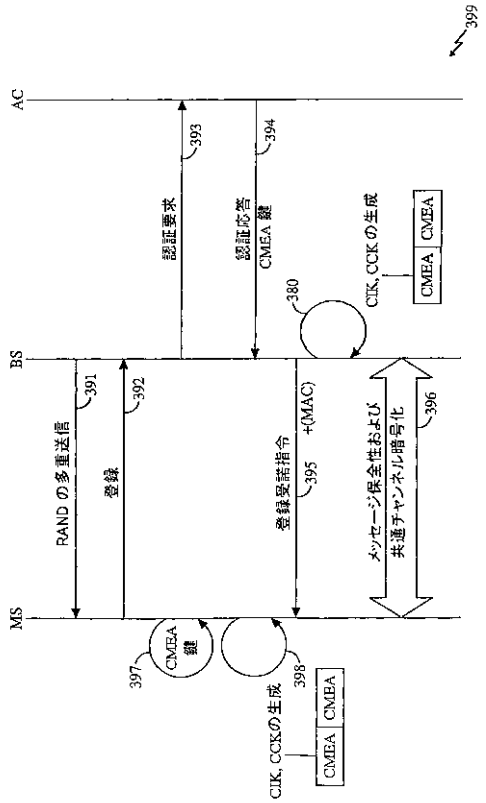
【図２】


200
214
復号器
212
結合器
210
制御システム
206
サーチャ
208
フィンガエレメント
208
フィンガエレメント
208
フィンガエレメント
202
MUX
204
サンプル
RAM
290
RF/IF
システム
292
292
RF/IF
システム

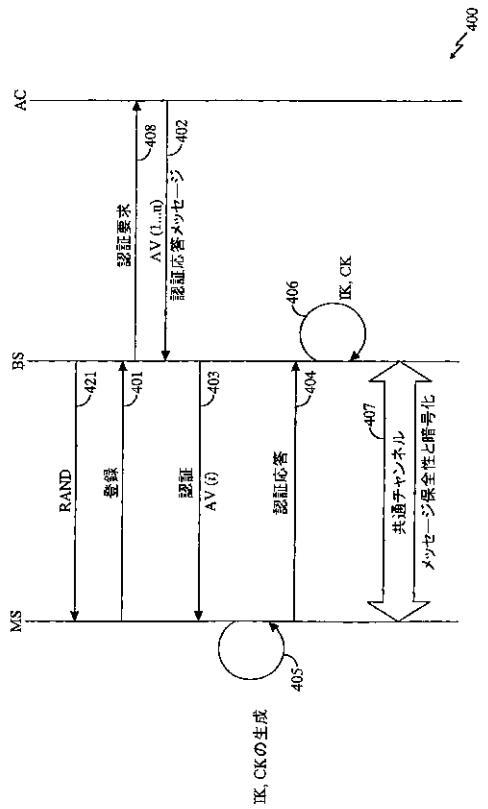
【図３】


304
309
308
307
パイロット
信号生成/増幅
302
信号拡散増幅
301
変調器
303
データ速度セレクタ/
出力レベルセレクタ
300
データ

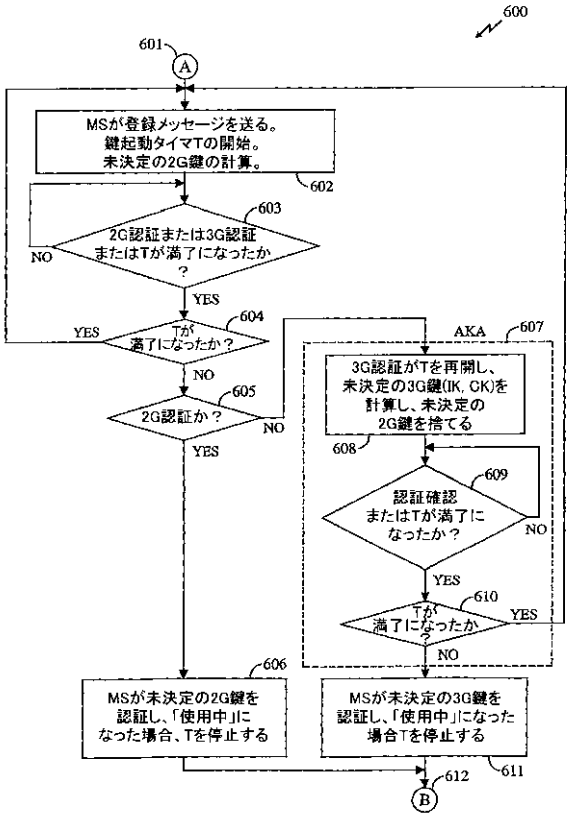
【図４】


399
AC
393
認証要求
394
認証応答
CMEA 鍵
CIK, CCKの生成
CMEA
CMEA
380
BS
391
RANDの多重送信
392
登録
登録受諾指令
395
+(MAC)
メッセージ保全性および
共通チャンネル暗号化
396
MS
397
CMEA
鍵
398
CIK, CCKの生成
CMEA
CMEA

【図５】


400
AC
BS
MS
408
402
認証要求
AV (1...n)
認証応答メッセージ
406
IK, CK
421
401
403
404
407
RAND
登録
認証
AV (i)
認証応答
共通チャンネル
メッセージ保全性と暗号化
405
IK, CKの生成

【図６】


600
601
A
MSが登録メッセージを送る。
鍵起動タイマTの開始。
未決定の2G鍵の計算。
602
603
2G認証またはは3G認証
またはTが満了になったか
？
NO
YES
604
Tが
満了になったか？
YES
NO
605
2G認証か？
NO
YES
AKA
607
3G認証がTを再開し、
未決定の3G鍵(IK, CK)を
計算し、未決定の
2G鍵を捨てる
608
609
認証確認
またはTが満了に
なったか？
NO
YES
610
Tが
満了になったか
？
YES
NO
606
MSが未決定の2G鍵を
認証し、「使用中」に
なった場合、Tを停止する
MSが未決定の3G鍵を
認証し、「使用中」になった
場合Tを停止する
611
612
B

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte l Application No
PCT/US 02/35297

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04L29/06 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 58081 A (NOKIA MOBILE PHONES LTD ;IMMONEN OLLI (FI)) 9 August 2001 (2001-08-09)	1,3,4,6, 7
A	page 3, line 14 -page 5, line 14 page 6, line 12 -page 8, line 25 page 11, line 14 -page 12, line 16 figures 2-7	9-13
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the generat state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2003	08/04/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Pacholec, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte: Application No
PCT/US 02/35297

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WAGNER D ET AL: "CRYPTANALYSIS OF THE CELLULAR MESSAGE ENCRYPTION ALGORITHM" ADVANCES IN CRYPTOLOGY - CRYPTO '97. SANTA BARBARA, AUG. 17 - 21, 1997, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 17, 17 August 1997 (1997-08-17), pages 526-537, XP000767552 ISBN: 3-540-63384-7 the whole document	1-13
A	WO 99 03246 A (LUCENT TECHNOLOGIES INC) 21 January 1999 (1999-01-21) page 3, line 16 -page 4, line 15 page 6, line 28 -page 7, line 27	1-13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int al Application No
PCT/US 02/35297

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0158081 A	09-08-2001	FI 20000203 A	02-08-2001
		AU 3180901 A	14-08-2001
		BR 0107925 A	10-12-2002
		CN 1397124 T	12-02-2003
		EP 1252739 A1	30-10-2002
		WO 0158081 A1	09-08-2001
WO 9903246 A	21-01-1999	WO 9903246 A2	21-01-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 クイック、ロイ・フランクリン・ジュニア
アメリカ合衆国、カリフォルニア州 ９２１０７、サン・ディエゴ、バルセロナ・ドライブ １１５０
(72)発明者 ホ、サイ・イウ・ダンカン
アメリカ合衆国、カリフォルニア州 ９２１２２、サン・ディエゴ、ナンバー・ディー１１７、フィオレ・テラス ５２２５

Ｆターム(参考) 5J104 AA01 AA16 AA32 EA04 EA15 EA16 EA17 EA18 JA03 MA05
NA02 NA37 PA01
5K067 AA30 BB04 BB21 DD51 EE02 EE10 HH24 HH36