(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4818345号
(P4818345)

(45)発行日　平成23年11月16日(2011.11.16)　(24)登録日　平成23年9月9日(2011.9.9)

(51)Int.Cl.		F I		
H04W 12/10	(2009.01)	H04Q	7/00	185
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 12/04	(2009.01)	H04Q	7/00	182
H04L 9/08	(2006.01)	H04L	9/00	601A
G09C 1/00	(2006.01)	H04L	9/00	601E

請求項の数 6　(全 9 頁)　最終頁に続く

(21)出願番号　特願2008-307854 (P2008-307854)
(22)出願日　平成20年12月2日 (2008.12.2)
(65)公開番号　特開2009-141958 (P2009-141958A)
(43)公開日　平成21年6月25日 (2009.6.25)
審査請求日　平成20年12月2日 (2008.12.2)
(31)優先権主張番号　60/992,675
(32)優先日　平成19年12月5日 (2007.12.5)
(33)優先権主張国　米国(US)

(73)特許権者　507334299
イノヴァティヴ　ソニック　リミテッド
Ｉｎｎｏｖａｔｉｖｅ　Ｓｏｎｉｃ　Ｌｉｍｉｔｅｄ
英国領ヴァージン諸島　トルトラ　ロード・タウン　オフショア・インコーポレイションズ・センター　ピー・オー・ボックス　９５７
Ｐ．Ｏ．Ｂｏｘ　９５７，　Ｏｆｆｓｈｏｒｅ　Ｉｎｃｏｒｐｏｒａｔｉｏｎｓ　Ｃｅｎｔｒｅ，　Ｒｏａｄ　Ｔｏｗｎ，　Ｔｏｒｔｏｌａ，　Ｂｒｉｔｉｓｈ　Ｖｉｒｇｉｎ　Ｉｓｌａｎｄｓ
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】セキュリティーキー変更を処理する方法及び通信装置

(57)【特許請求の範囲】

【請求項１】

無線通信システムのＵＥ（ユーザー端末）においてセキュリティーキー変更を処理する方法であって、

ハンドオーバープロセスで前記セキュリティーキー変更を起動し、前記ハンドオーバープロセスは、前記セキュリティーキー変更に、前記セキュリティーキー変更に対応するＡＫＡ（認証及びキー同意）プロセスが伴うかまたはＡＫＡプロセスが伴わないかを示し、

前記方法は、

前記ハンドオーバープロセスで前記セキュリティーキー変更を起動するためのハンドオーバーメッセージを受信する段階を含み、

前記ハンドオーバーメッセージは、前記セキュリティーキー変更に前記ＡＫＡプロセスが伴うかどうかを示す指示子を含む、セキュリティーキー変更の処理方法。

【請求項２】

前記方法は更に、

前記指示子に基づいて、前記セキュリティーキー変更に、対応するＡＫＡプロセスが伴うかどうかを判断する段階と、

前記セキュリティーキー変更に、対応するＡＫＡプロセスが伴った場合に、前記ＡＫＡプロセスに対応するベースキー（K_{ASME}）に基づいてＡＳ（アクセスセキュリティー）キーセットを生成する段階と、

前記セキュリティーキー変更に、対応するＡＫＡプロセスが伴わなかった場合に、前の

基地局キー（K_{eNB}）または前のベースキーに基づいて前記ＡＳキーセットを生成する段階と、を含み、

前記ＡＳキーセットはユーザープレーンキー（$K_{eNB-UP-enc}$）とＲＲＣキー（$K_{eNB-RRC-int}$）、（$K_{eNB-RRC-enc}$）を含む、請求項１に記載のセキュリティーキー変更の処理方法。

【請求項３】

前記ＵＥはＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態で動作する、請求項１又は請求項２に記載のセキュリティーキー変更の処理方法。

【請求項４】

無線通信システムにおいてセキュリティーキー変更を実行するための通信装置であって、

処理プロセスを実行するＣＰＵ（中央処理装置）と、

前記ＣＰＵに結合され、前記処理プロセスを実行するためのプログラムを記録する記憶装置と、を含み、

ハンドオーバープロセスで前記セキュリティーキー変更を起動し、前記ハンドオーバープロセスは、前記セキュリティーキー変更に、前記セキュリティーキー変更に対応するＡＫＡプロセスが伴うかまたはＡＫＡプロセスが伴わないかを示し、

前記処理プロセスは、前記ハンドオーバープロセスで前記セキュリティーキー変更を起動するためのハンドオーバーメッセージを受信する段階を含み、前記ハンドオーバーメッセージは、前記セキュリティーキー変更に前記ＡＫＡプロセスが伴うかどうかを示す指示子を含む、通信装置。

【請求項５】

前記処理プロセスは更に、

前記指示子に基づいて、前記セキュリティーキー変更に、対応するＡＫＡプロセスが伴うかどうかを判断する段階と、

前記セキュリティーキー変更にＡＫＡプロセスが伴った場合に、前記ＡＫＡプロセスに対応するベースキー（K_{ASME}）に基づいてＡＳキーセットを生成する段階と、

前記セキュリティーキー変更に、対応するＡＫＡプロセスが伴わなかった場合に、前の基地局キー（K_{eNB}）または前のベースキーに基づいて前記ＡＳキーセットを生成する段階と、を含み、

前記ＡＳキーセットはユーザープレーンキー（$K_{eNB-UP-enc}$）とＲＲＣキー（$K_{eNB-RRC-int}$）、（$K_{eNB-RRC-enc}$）を含む、請求項４に記載の通信装置。

【請求項６】

前記通信装置はＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態で動作する、請求項４又は請求項５に記載の通信装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は無線通信システムに用いられる方法及び装置に関し、特に無線通信システムにおいてセキュリティーキー変更を処理する方法及び装置に関する。

【背景技術】

【０００２】

第三世代移動通信技術は高スペクトル利用効率、高カバー率、優れた通話品質と高速の伝送を実現するとともに、ＱｏＳ（サービス品質）の確保、柔軟性のある双方向通信の実現、通話中断率の低減に大きく寄与する。

【０００３】

ユーザーデータかその他情報の傍受による被害を防止するために、従来の第三世代移動通信システムではセキュリティーモード制御プロセスで完全性保護（ｉｎｔｅｇｒｉｔｙ　ｐｒｏｔｅｃｔｉｏｎ）または暗号化保護を実行することで、データ伝送の安全性を確

保する。暗号化保護の動作は、暗号化アルゴリズムを利用し、暗号化保護に必要なキーストリームブロックを算出する。その後、送信端でキーストリームブロックと平文ブロックを暗号化して暗号文ブロックにさせ、受信端で送信端と同じキーストリームブロックを利用すれば、受信した暗号文ブロックを解読して平文ブロックを得ることができる。

【０００４】

第三世代移動通信システムにおける情報交換のセキュリティーは、３ＧＰＰ（第三世代パートナーシッププロジェクト）が制定したセキュリティー構造プロトコル仕様によって守られる。同仕様によれば、ネットワークとＵＥの間にセキュリティーキーの認証・生成を行い、データの機密性と安全性を確保するために、ＡＫＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ、認証及びキー同意）プロセスを設けている。言い換えれば、モバイル管理（ｍｏｂｉｌｅ ｍａｎａｇｅｍｅｎｔ）層でＡＫＡプロセスを実行した後、ＵＥには新しいセキュリティーキー（以下にキーと略する）が割り当てられる。

【０００５】

図１を参照する。図１はＬＴＥ（ｌｏｎｇ ｔｅｒｍ ｅｖｏｌｕｔｉｏｎ）無線通信システムに用いられるキーヒエラルキーを表す説明図である。種々のセキュリティーレベルに応じて、ＵＥは永久キー（ｐｅｒｍａｎｅｎｔ ｋｅｙ）Ｋと、暗号化キー（ｃｉｐｈｅｒｉｎｇ ｋｅｙ、ＣＫ）と、完全性キー（ｉｎｔｅｇｒｉｔｙ ｋｅｙ、ＩＫ）と、ベースキーK_{ASME}と、ＮＡＳ暗号化（ｎｏｎ－ａｃｃｅｓｓ ｓｔｒａｔｕｍ ｅｎｃｒｙｐｔｉｏｎ）キー$K_{(NAS,enc)}$と、基地局キーK_{eNB}とを含む。永久キーＫはＵＥ（ユーザー端末）のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）に保存されている。暗号化キーと完全性キーはＵＭＴＳ（Ｕｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍ）のＡＫＡに用いられ、ベースキーK_{ASME}はＵＥとＡＳＭＥ（Ａｃｃｅｓｓ Ｓｅｃｕｒｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｅｎｔｉｔｙ）の間に用いられる。また、ＮＡＳについて、ＮＡＳ暗号化キー$K_{(NAS,enc)}$とＮＡＳ完全性キー$K_{(NAS,int)}$はそれぞれＮＡＳメッセージの暗号化と完全性保護に用いられる。前記基地局キーK_{eNB}からでは、ユーザープレーンデータの暗号化、ＲＲＣ（無線リソース制御）完全性保護及びＲＲＣ暗号化にそれぞれ用いられるユーザープレーンキー$K_{eNB-UP-enc}$とＲＲＣ（無線リソース制御）キー$K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$が派生する。図１では、各セキュリティーキーの派生関係を示している。例えば、基地局キーK_{eNB}は、ベースキーK_{ASME}を基に特殊なアルゴリズムを利用して算出することができ、他も同様である。ＵＥがＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態で動作するとき、基地局キーK_{eNB}からではユーザープレーンキー$K_{eNB-UP-enc}$とＲＲＣキー$K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$が派生する。ＵＥがＲＲＣ＿ＩＤＬＥ状態またはＬＴＥ＿ＩＤＬＥ状態に切り替わると、基地局キーK_{eNB}、ユーザープレーンキー$K_{eNB-UP-enc}$、及びＲＲＣキー$K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$はｅＮＢ（基地局）から削除される。それ以外、ＵＥによるＡＫＡプロセスの完成後、図１に示すセキュリティーキーは、後続のセキュリティーキー変更の起動時にすべて更新される。

【０００６】

ＵＥがＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態で動作するとき、以下の状況が発生すれば、ｅＮＢはセキュリティーキー変更を実行してデータの機密性と安全性を確保する。

【０００７】

１．　ユーザープレーンまたはＲＲＣ暗号化／完全性保護に用いられるシーケンス番号が限られたビット長を有する場合、シーケンス番号の表示ビット数で表示できる値を超えると、シーケンス番号は初期値（０）に戻って初期値から累算する（ラップアラウンドと称する）。シーケンス番号がラップアラウンドする前に、データの機密性と安全性を確保するために、セキュリティーキーを更新しなければならない。

２．　ＵＥがＬＴＥ＿ＡＣＴＩＶＥ状態で長時間動作した場合、ユーザープレーンまたはＲＲＣ暗号化／完全性保護に用いられるシーケンス番号がまだラップアラウンドしていなくても、セキュリティーキーが解読されるのを避けるために、セキュリティーキーを更新しなければならない。
３．　ベースキーＫＡＳＭＥの寿命が所定の有効期間までくると、同じベースキーの長時間使用を避けるために、セキュリティーキーを更新しなければならない。
４．　ＵＥがＧＥＲＡＮ／ＵＴＲＡＮ（第二世代／第三世代）からＬＴＥに移動した場合、すなわちＲＡＴ間ハンドオーバーの完成後、数秒以内にセキュリティーキー更新を完成させなければならない。
【０００８】
以上の状況を分析して、状況１と状況２はＡＫＡプロセスを実行しなくてもよいが、状況３と状況４は、新たなＡＳ（アクセスセキュリティーキー）キーセットを生成するためにＡＫＡプロセスを実行しなければならない。状況１と状況２では、新しいユーザープレーンキーとＲＲＣキーは、本来の基地局キーからか、或いは本来のベースキーから得られた新しい基地局キーから算出できるため、セキュリティーキー変更時にはＡＫＡプロセスを実行しなくてもよい。
【０００９】
現在の仕様では、セキュリティーキー変更の起動方式を規定していない。可能な方法として、セル間ハンドオーバープロセスで、セキュリティーキー変更を起動することが考えられる。言い換えれば、ＵＥが所属するセルにおいて、ネットワークがセル間ハンドオーバープロセスを実行すれば、セキュリティーキー変更は同時に起動される。換言すると、ハンドオーバー前に本来のＡＳキーを使用し、ハンドオーバー後に新しいＡＳキーを使用することである。
【００１０】
従来の技術では、ＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態のセキュリティーキー変更は、ＡＫＡを伴うセキュリティーキー変更と、ＡＫＡを伴わないセキュリティーキー変更を含む。しかし、この２つの状況を取り扱う明確な規定は、現時点では存在していない。
【発明の開示】
【発明が解決しようとする課題】
【００１１】
本発明の主な目的は、セキュリティーキー変更を処理する方法及び通信装置を提供することにある。
【課題を解決するための手段】
【００１２】
本発明では、無線通信システムのＵＥ（ユーザー端末）においてセキュリティーキー変更を処理する方法を開示する。当該方法は、ＲＲＣ（無線リソース制御）プロセスでセキュリティーキー変更を起動し、当該ＲＲＣプロセスは、セキュリティーキー変更に、当該セキュリティーキー変更に対応するＡＫＡ（認証及びキー同意）プロセスが伴うかまたはＡＫＡプロセスが伴わないかを示す段階を含む。
【００１３】
本発明では更に、無線通信システムにおいてセキュリティーキー変更を実行するための通信装置を開示する。当該通信装置は、処理プロセスを実行するＣＰＵ（中央処理装置）と、前記ＣＰＵに結合され、前記処理プロセスを実行するためのプログラムを記録する記憶装置とを含む。前記処理プロセスは、ＲＲＣプロセスでセキュリティーキー変更を起動し、当該ＲＲＣプロセスは、セキュリティーキー変更に、当該セキュリティーキー変更に対応するＡＫＡプロセスが伴うかまたはＡＫＡプロセスが伴わないかを示す段階を含む。
【発明を実施するための最良の形態】
【００１４】
かかる方法及び装置の特徴を詳述するために、具体的な実施例を挙げ、図を参照にして

以下に説明する。

【００１５】

図２を参照する。図１は無線通信システム１０を表す説明図である。無線通信システム１０は望ましくはＬＴＥシステムであり、概してネットワークと複数のＵＥを含む。図２に示すネットワークとＵＥは無線通信システム１０の構造を説明するために用いるに過ぎない。実際、ネットワークは要求に応じて複数の基地局、ＲＮＣ（無線ネットワークコントローラー）を含みうる。ＵＥは携帯電話、コンピュータシステムなどの装置である。

【００１６】

図３を参照する。図３は無線通信装置１００のブロック図である。無線通信装置１００は図２に示すＵＥを実施する。説明を簡素化するために、図３では無線通信装置１００の入力装置１０２、出力装置１０４、制御回路１０６、ＣＰＵ（中央処理装置）１０８、記憶装置１１０、プログラム１１２及びトランシーバー１１４のみ示している。無線通信装置１００では、制御回路１０６はＣＰＵ１０８を用いて記憶装置１１０に記録されたプログラム１１２を実行し、無線通信装置１００の動作を制御し、入力装置１０２（例えばキーボード）でユーザーが入力した信号を受信し、出力装置１０４（スクリーン、スピーカーなど）で映像、音声などの信号を出力する。無線信号を受発信するトランシーバー１１４は受信した信号を制御回路１０６に送信し、または制御回路１０６による信号を無線で出力する。言い換えれば、通信プロトコルに当てはめれば、トランシーバー１１４は第一層の一部とみなされ、制御回路１０６は第二層と第三層の機能を実施する。

【００１７】

図４を参照する。図４は図３に示すプログラム１１２を表す説明図である。プログラム１１２はアプリケーション層２００と、第三層２０２と、第二層２０６とを含み、第一層２１８に接続されている。第三層２０２には、ＲＲＣプロセスを通して基地局またはＵＴＲＡＮとＲＲＣメッセージを交換し、ＲＲＣメッセージ内のＩＥ（情報要素）に基づいて第一層２１８と第二層２０６の動作を設定するためのＲＲＣエンティティー２２２が設けられている。また、ＲＲＣエンティティー２２２は無線通信装置１００をＲＲＣ＿ＩＤＬＥ状態またはＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態に切り替えることができる。

【００１８】

無線通信装置１００がＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態にある場合、本発明の実施例では、セキュリティーキー変更にＡＫＡプロセスが伴うかどうかを判断するためのセキュリティーキー変更処理プログラム２２０を前記プログラム１１２に設ける。図５を参照する。図５は本発明による方法４０のフローチャートである。下記方法４０は無線通信システムのＵＥにおけるセキュリティーキー変更の処理に用いられ、セキュリティーキー変更処理プログラム２２０としてコンパイルすることができる。

【００１９】

ステップ４００：開始。

ステップ４０２：ｅＮＢで起動されるＲＲＣプロセスで、セキュリティーキー変更を起動する。

ステップ４０４：前記ＲＲＣプロセスを利用し、前記セキュリティーキー変更と、当該セキュリティーキー変更に対応するＡＫＡプロセスの随伴関係を取得する。

ステップ４０６：終了。

【００２０】

以上のように、本発明の実施例ではＲＲＣプロセスでセキュリティーキー変更を起動し、更にＲＲＣプロセスで、セキュリティーキー変更に、それに対応するＡＫＡプロセスが伴うか伴わないかを指示する。望ましくは、ＵＥはＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態で作動するときに、ＲＲＣプロセスでｅＮＢからのＲＲＣメッセージを受信する。このＲＲＣメッセージは、セキュリティーキー変更にＡＫＡプロセスが伴うかどうかを指示する指示子を含む。

【００２１】

また望ましくは、アクセスセキュリティー（ＡＳ）キーセットはユーザープレーンキー

$K_{eNB-UP-enc}$とＲＲＣキー$K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$を含む。セキュリティーキー間の派生関係は前述を参照すればよく、ここで説明を省略する。指示子によりセキュリティーキー変更にＡＫＡプロセスが伴うと示されれば、前にＡＫＡプロセスが完成したと判明し、ＵＥで新しいＡＳキーセットを生成する。この新しいＡＳキーセットは、新しいベースキーに基づいて生成しなければならない。それに反して、指示子によりセキュリティーキー変更にＡＫＡプロセスが伴わないと示されれば、新しいＡＳキーセットは本来のベースキーK_{ASME}または基地局キーK_{eNB}に基づいて生成される。したがって、ＵＥはＲＲＣメッセージ内の指示子に基づいて、セキュリティーキー変更にＡＫＡが伴うかどうかを判断し、対応する新しいＡＳキーセットを生成する。

【００２２】

また、ＵＥが自ら状態指標を使用することもできる。この状態指標は、ＡＫＡプロセスに対応する新しいＡＳキーセットの起動状態を示す。ＡＫＡプロセスの実行時、状態指標を第一値に設定する。この第一値はＡＳキーセットが起動されていないことを示す。セキュリティーキー変更の起動後、状態指標を第二値に設定する。この第二値は、ＡＳキーセットが起動されたことを示す。例えば、状態指標を１ビットで表示すれば、ビット値０を起動済ＡＳキーセットがあることを示すものとし、ビット値１をＡＫＡプロセスにより新しいＡＳキーセットが生成されたがまだ起動されていないことを示すものとすることができる。この場合、新しいＡＳキーセットの起動後、ビット値は０に戻される。

【００２３】

また、ＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態またはＬＴＥ＿ＡＣＴＩＶＥ状態にあるＵＥで、ｅＮＢからセキュリティーキー変更起動用のＲＲＣメッセージを受信すれば、当該ＵＥは状態指標に基づいて、セキュリティーキー変更とＡＫＡプロセスの随伴関係を判断する。状態指標が第一値であればセキュリティーキー変更にＡＫＡプロセスが伴うと判断し、第二値であればセキュリティーキー変更にＡＫＡプロセスが伴わないと判断する。例えば、状態指標が０であれば、本来のベースキーまたは基地局キーにより新しいＡＳキーセットが生成されたことが判明し、ＵＥはセキュリティーキー変更にＡＫＡプロセスが伴わないと判断する。状態指標が１であれば、新しいＡＳキーセットが割り当てられたことが判明し、ＵＥはセキュリティーキー変更にＡＫＡプロセスが伴うと判断する。セキュリティーキー変更起動プロセスの終了後、状態指標を０に戻す。状態指標を０に戻すことは、ＡＫＡプロセスに対応する新しいＡＳキーセットが起動されたことを示す。

【００２４】

以上のように、ＵＥはセキュリティーキー変更にＡＫＡプロセスが伴うかどうかを判断し、それによって新しいＡＳキーセットに更新するかどうかを決める。

【００２５】

まとめて言えば、本発明の実施例ではＲＲＣプロセスでセキュリティーキー変更を起動する。ＵＥはセキュリティーキー変更にＡＫＡプロセスが伴うかどうかを判断し、それによって新しいＡＳキーセットに更新するかどうかを決める。

以上は本発明に好ましい実施例であって、本発明の実施の範囲を限定するものではない。よって、当業者のなし得る修正、もしくは変更であって、本発明の精神の下においてなされ、本発明に対して均等の効果を有するものは、いずれも本発明の特許請求の範囲に属するものとする。

【図面の簡単な説明】

【００２６】

【図１】ＬＴＥ無線通信システムに用いられるキーヒエラルキーを表す説明図である。

【図２】無線通信システムを表す説明図である。

【図３】無線通信装置のブロック図である。

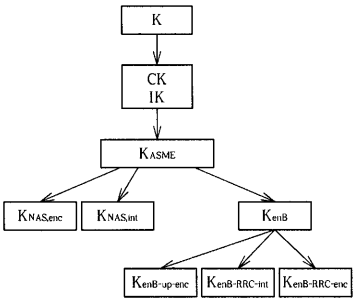
【図４】図３に示すプログラムを表す説明図である。

【図５】本発明による方法のフローチャートである。

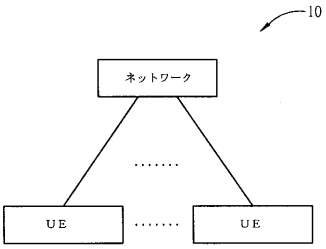
【符号の説明】

【００２７】
１０　無線通信システム
１００　無線通信装置
１０２　入力装置
１０４　出力装置
１０６　制御回路
１０８　ＣＰＵ
１１０　記憶装置
１１２　プログラム
１１４　トランシーバー
２００　アプリケーション層
２０２　第三層
２０６　第二層
２１８　第一層
２２０　キー変更処理プログラム
２２２　ＲＲＣエンティティー

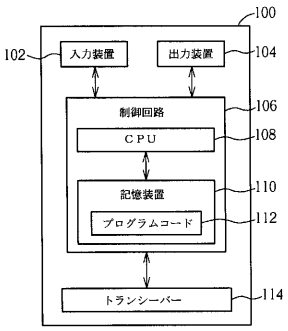
【図１】



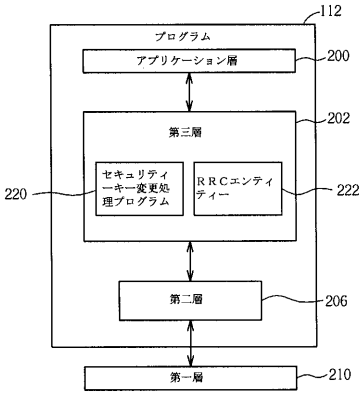
【図２】



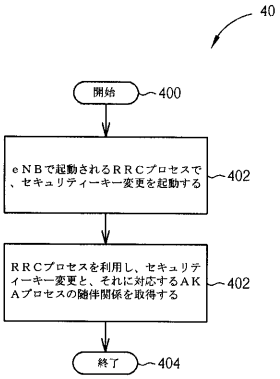
【図３】


100
102
入力装置
出力装置
104
制御回路
106
CPU
108
記憶装置
110
プログラムコード
112
トランシーバー
114

【図４】


112
プログラム
アプリケーション層
200
第三層
202
セキュリティーキー変更処理プログラム
220
RRCエンティティー
222
第二層
206
第一層
210

【図５】


40
開始
400
eNBで起動されるRRCプロセスで、セキュリティーキー変更を起動する
402
RRCプロセスを利用し、セキュリティーキー変更と、それに対応するAKAプロセスの随伴関係を取得する
402
終了
404

フロントページの続き

(51)Int.Cl. FI
G09C 1/00 630B

(74)代理人 100091214
弁理士 大貫 進介
(74)代理人 100107766
弁理士 伊東 忠重
(74)代理人 100104156
弁理士 龍華 明裕
(72)発明者 郭 豊旗
台灣台北市北投區立▲德▼路一五０號四樓

審査官 齋藤 哲

(56)参考文献 特開２００１－３３９３８６（ＪＰ，Ａ）
Huawei, Key Update in LTE-ACTIVE state, 3GPP TSG RAN WG3 Meeting #57bis, R3-071942, 3rd Generation Partnership Project, ２００７年１０月１１日, ＵＲＬ, http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_57bis/docs/R3-071942.zip

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ １／００－５／００
Ｈ０４Ｂ ７／２４－７／２６
Ｈ０４Ｋ １／００－３／００
Ｈ０４Ｌ ９／００－９／３８
Ｈ０４Ｗ ４／００－９９／００