(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-173261
(P2004-173261A)
(43)公開日　平成16年6月17日(2004.6.17)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	675A	5J104
H04Q	7/38	H04B	7/26	109R	5K067

審査請求 有　請求項の数 24　ＯＬ　（全 19 頁）

(21)出願番号　特願2003-376332(P2003-376332)
(22)出願日　平成15年11月5日(2003.11.5)
(31)優先権主張番号　2002-072008
(32)優先日　平成14年11月19日(2002.11.19)
(33)優先権主張国　韓国(KR)

(71)出願人　502032105
エルジー　エレクトロニクス　インコーポレイティド
大韓民国，ソウル　１５０－７２１，ヨンドゥンポ－ク，ヨイド－ドン，２０
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹
(72)発明者　オウ，　ミュン　ダエ
大韓民国　ソウル，　ガングセオ－ク，　ワゴク６ドン，　ハンヤン　アパートメント，　ナンバービー－２０２
最終頁に続く

(54)【発明の名称】移動通信システムの転送情報暗号化及び暗号化解除装置及びその方法

(57)【要約】
【課題】　移動通信システムの転送情報暗号化及び暗号化解除装置及びその方法を提供する。
【解決手段】　移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、ユーザ端末が転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの暗号化要求メッセージを受信し、それを承認するメッセージを前記端末に転送する承認段階と、前記端末がネットワークからの暗号化要求承認メッセージを受信し、それに応答するメッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、それに対応して情報転送中の暗号化準備が完了したというメッセージを端末に転送する完了段階とを含んでなる。
【選択図】　なし

【特許請求の範囲】
【請求項１】
移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、
前記端末とネットワーク間の情報転送中に暗号化を必要とすると、ユーザ端末が転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、
前記ネットワークが端末からの暗号化要求メッセージを受信し、それを承認するメッセージを前記端末に転送する承認段階と、
前記端末がネットワークからの暗号化要求承認メッセージを受信し、それに応答するメッセージをネットワークに転送する応答段階と、
前記ネットワークが端末からの暗号化承認応答メッセージを受信し、それに対応して情報転送中の暗号化準備が完了したというメッセージを端末に転送する完了段階とを含んでなることを特徴とする移動通信システムの転送情報暗号化方法。
【請求項２】
前記承認段階による承認メッセージ中にはＲＡＮＤ値が含まれていることを特徴とする請求項１記載の移動通信システムの転送情報暗号化方法。
【請求項３】
前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することができることを特徴とする請求項１記載の移動通信システムの転送情報暗号化方法。
【請求項４】
前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することができることを特徴とする請求項１記載の移動通信システムの転送情報暗号化方法。
【請求項５】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンテクストアクティベーション情報の少なくとも一つであることを特徴とする請求項１記載の移動通信システムの転送情報暗号化方法。
【請求項６】
移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、
前記端末とネットワーク間の情報転送中に暗号化を必要とすると、前記端末が転送情報に暗号化を要求する特定値を含ませてネットワークに転送する暗号化要求段階と、
前記ネットワークが端末からの前記特定値を基礎として情報暗号化準備過程に必要なキー値を算出した後、暗号化準備過程が完了したというメッセージを端末に転送する完了段階と、
前記暗号化準備完了後、端末とネットワークが情報転送中に暗号化を行う実行段階とを含んでなることを特徴とする移動通信システムの転送情報暗号化方法。
【請求項７】
前記暗号化要求段階の特定値はＲＡＮＤ番号値を用いることを特徴とする請求項６記載の移動通信システムの転送情報暗号化方法。
【請求項８】
前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することができることを特徴とする請求項６記載の移動通信システムの転送情報暗号化方法。
【請求項９】
前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することができることを特徴とする請求項６記載の移動通信システムの転送情報暗号化方法。
【請求項１０】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンテクストアクティベーション情報の少なくとも一つであることを特徴とする請求項６記載の移動通信システ

ムの転送情報暗号化方法。
【請求項１１】
移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、
前記端末がすべての転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、
前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていると、前記ＲＡＮＤ値を用いて暗号化に必要なキー（Ｋｃ）値を算出し、転送情報の暗号化準備を完了する第１完了段階と、
前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていないと、暗号化遂行可否に応じてＲＡＮＤ値を生成し、ＳＲＥＳ値を算出／格納し、暗号化準備が完了したという承認メッセージを端末に転送する第２完了段階と、
前記端末がネットワークからの暗号化準備完了メッセージを受信し、ＳＲＥＳ値が含まれた応答メッセージをネットワークに転送する応答段階と、
前記ネットワークが端末からの暗号化承認応答メッセージを受信し、ネットワークに格納されたＳＲＥＳ値と、端末からのＳＲＥＳ値とを比較して、同一か否かによって転送情報の暗号化可否を判断する判断段階とを含んでなることを特徴とする移動通信システムの転送情報暗号化方法。
【請求項１２】
前記第２完了段階の承認メッセージ中にはＲＡＮＤ値が含まれていることを特徴とする請求項１１記載の移動通信システムの転送方法暗号化方法。
【請求項１３】
前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することを特徴とする請求項１１の記載の移動通信システムの転送情報暗号化方法。
【請求項１４】
前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することを特徴とする請求項１１記載の移動通信システムの転送情報暗号化方法。
【請求項１５】
前記第２完了段階のネットワークが、端末からの転送中の暗号化要求メッセージ中にＲＡＮＤ値が含まれず、暗号化を行わない場合、転送情報に暗号化が行われないというメッセージを端末に転送する段階をさらに含むことを特徴とする請求項１１記載の移動通信システムの転送情報暗号化方法。
【請求項１６】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴とする請求項１１記載の移動通信システムの転送情報暗号化方法。
【請求項１７】
移動通信端末とネットワーク間に送受信される情報の暗号化を解除する方法において、
前記端末とネットワーク間の情報転送中の暗号化が不要ならば、ユーザ端末が転送情報の暗号化解除を要求するメッセージをネットワークに転送する暗号化解除要求段階と、
前記ネットワークが端末からの暗号化解除要求メッセージを受信し、それを承認する転送中の暗号化解除メッセージを前記端末に転送する暗号化解除承認段階とを含んでなることを特徴とする移動通信システムの転送情報暗号化解除方法。
【請求項１８】
前記暗号化解除要求段階では端末とネットワーク間に情報が転送される途中でも暗号化解除を要求することができることを特徴とする請求項１７記載の移動通信システムの転送情報暗号化解除方法。
【請求項１９】
前記暗号化解除要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化解除を要求することができることを特徴とする請求項１７記載の移動通信システムの

転送情報暗号化解除方法。
【請求項２０】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴とする請求項１７記載の移動通信システムの転送情報暗号化方法。
【請求項２１】
移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、
前記移動通信ネットワークに暗号化要求を転送する送信機と、
前記暗号化要求を受け、ネットワークに転送される情報を暗号化し、且つネットワークからの暗号化された情報を処理するプロセッサーとを含んでなることを特徴とする移動通信端末。
【請求項２２】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴とする請求項２１記載の移動通信端末。
【請求項２３】
移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、
前記移動通信端末からの暗号化要求を受信する受信機と、
前記暗号化要求に応答して、移動通信端末からの暗号化された情報を受信し、且つ移動通信端末に転送された情報を暗号化するプロセッサーとを含んでなることを特徴とする移動通信端末。
【請求項２４】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴とする請求項２３記載の移動通信端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動通信システムにおける情報転送時に、情報の暗号化及び暗号化解除を行う装置及びその方法に係り、特に、ＧＳＭまたはＣＤＭＡ移動通信システムにおいて、端末とネットワーク間で転送される情報の暗号化及び暗号化解除の時、その暗号化及び暗号化解除を移動通信端末で直接行うための移動通信システムの転送情報暗号化及び暗号化解除装置及びその方法に関する。
【背景技術】
【０００２】
現在、米国やヨーロッパーで２世代移動通信システムとして常用サービス中であるＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍｓ ｆｏｒ Ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎ）と、２．５世代移動通信システムとして常用サービス中であるＧＰＦＳ（Ｇｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ）の場合、ユーザ認証及び暗号化手続きを行っている。
【０００３】
前記ユーザ認証及び暗号化手続きというのは、移動通信端末の電源がＯＮになる度に端末は必ず端末使用を知らせるユーザの意思表現である登録手続きをネットワーク上で行う必要があるということを意味ずる。
【０００４】
前記登録手続きには、付加（Ａｔｔａｃｈ）登録手続きと位置地域アップデート（Ｌｏｃａｔｉｏｎ Ａｒｅａ Ｕｐｄａｔｅ）及び経路地域アップデート（Ｒｏｕｔｉｎｇ Ａｒｅａ Ｕｐｄａｔｅ）登録手続きなどがある。

【０００５】
前記登録手続きの過程中にネットワーク上で必要時にユーザ認証及び暗号化準備過程が行われる。
【０００６】
前記ユーザ認証及び暗号化準備過程をネットワーク上で行う場合、端末（ＭＳ：Ｍｏｂｉｌｅ　Ｓｔａｔｉｏｎ）がネットワークに登録を要求すると、ネットワークでは当該端末が認証端末であるか否かを確認する認証手続き（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）と、端末とネットワーク間の転送データの暗号化を行うか否かを判断する暗号化手続き（Ｃｉｐｈｅｒｉｎｇ）とを行う。
【０００７】
前記認証手続き及び暗号化手続きは、転送される無線音声や無線データが他人から盗聴及び悪用されるおそれを防止するための手続きである。
【０００８】
万一、端末とネットワーク間の暗号化手続きを経て暗号化を行うと、相互に転送されるデータは相互約束によって暗号化された状態で転送されることになる。
【０００９】
この暗号化を行うか否かは、次の２つの方法によって判断される。
【００１０】
第１、端末の電源が消えた後、ネットワークに登録する過程中に行われる。
【００１１】
第２、端末の特定サービスを所望する時点で行われる。
【００１２】
前記特定サービスには、音声通話のための音声コール（Ｖｏｉｃｅ　ｃａｌｌ）と、短文伝送のためのＳＭＳ（Ｓｈｏｒｔ　ｍｅｓｓａｇｅ　ｓｅｒｖｉｃｅ）、付加サービスのためのＳＳ（Ｓｕｐｐｌｅｍｅｎｔａｒｙ　Ｓｅｒｖｉｃｅ）、ＧＰＲＳパケット転送のためのＰＤＰコンテクストアクティベーション（Ｐａｃｋｅｔ　Ｄａｔａ　Ｐｒｏｔｏｃｏｌ　Ｃｏｎｔｅｘｔ　Ａｃｔｉｖａｔｉｏｎ）などが属する。
【００１３】
端末とネットワーク間のデータ転送過程が約束されていない場合、すなわち、ネットワーク登録時に暗号化と関連した手続きが行われなくデータが暗号化されずに転送される際にも、サービスが行われる時点でネットワークによって暗号化と関連した手続きが行われることができる。
【００１４】
これにより、端末とネットワークはこの時点から転送データを暗号化してから転送を行う。
【００１５】
上記のようなＧＳＭ移動通信端末の転送データ暗号化技術において、通常の概略的なシステム構成は、図１に示すとおりである。
【００１６】
同図に示すように、移動通信システムは、一般有線電話１７０またはコンピュータ１８０と接続するために、公衆電話交換網（ＰＳＴＮ）／総合情報通信網（ＩＳＤＮ）１６０に接続される移動通信交換局１５０と、前記移動通信交換局１５０に接続される多数の基地局制御器１３０，１４０と、前記基地局制御器１３０，１４０に接続される多数の基地局１１１，１２１と、前記基地局１１１，１２１に無線リンクを介して接続される多数の移動通信端末１１０，１２０とから構成される。
【００１７】
前記多数の基地局１１１，１２１は、多数の移動通信端末１１０，１２０と移動通信交換局１５０との間で無線リンクと有線リンクとに適した信号フォーマットに変換させる役割を果たし、前記移動通信端末１１０，１２０の送受信電界強度（電波受信強度）を測定して移動通信交換局１５０に提供する。

【００１８】
前記多数の基地局制御器１３０，１４０は、多数の基地局１１１，１２１の各要素別機能とセル運用者間の接続手段となり、多数の基地局運用の管理、基地局のハードウェアとソフトウェアのサービス状態の管理、コールトラフィックに対する資源の割り当てと構成、基地局運用に関する情報樹立、基地局運用、監視及び故障に関連した下部装置監視などの機能を行う。
【００１９】
前記移動通信交換局１５０は、多数の基地局制御器１３０，１４０及び多数の移動通信端末１１０，１２０に回線交換サービスを提供し、付加機能としてチャネル切換え（ｈａｎｄｏｆｆ）機能を有している。
【００２０】
このような移動通信システムでは、任意の端末ユーザが移動通信端末１１０，１２０を用いて電話を掛けるか受けると、多数の基地局１１１，１１２のいずれか一つの基地局と接続される。
【００２１】
図２は従来のＧＳＭ移動通信端末とネットワーク間で暗号化準備過程中に行われるメッセージの流れ図である。
【００２２】
ヨーロッパで常用化サービス中であるＧＳＭとＧＰＲＳの場合、移動通信端末の電源がＯＮになると、端末１０はネットワック２０に登録を要求する。
【００２３】
この際、移動通信端端末１０は登録要求メッセージ（Ａｔｔａｃｈ　Ｒｅｑｕｅｓｔ）２０１を無線で基地局に転送し、基地局は前記登録要求メッセージ２０１を基地局制御器を経て移動通信交換局に転送する。
【００２４】
前記ネットワーク２０は端末１０からの登録要求メッセージ２０１を受信し、暗号化を行うか否かを判断し、暗号化を行う場合、暗号化要求メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｑｕｅｓｔ）２０２を端末１０に転送する。
【００２５】
前記端末１０はネットワーク２０からの前記暗号化要求メッセージ２０２を受信し、これに対応して適切な暗号化承認応答メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｓｐｏｎｓｅ）２０３をネットワーク２０に転送する。
【００２６】
前記ネットワーク２０は端末１０からの前記暗号化承認応答メッセージ２０３を受信し、登録手続きが完了したという登録完了メッセージ（Ａｔｔａｃｈ　Ａｃｃｅｐｔ）２０４を前記端末１０に転送する。これで端末１０とネットワーク２０間の暗号化過程が完了する。
【００２７】
一方、前記ネットワーク２０の判断結果、暗号化を行わない場合、ネットワーク２０は暗号化メッセージを前記端末１０に転送しない。また、端末１０とネットワーク２０間のデータは暗号化されていない状態で転送が行われる。
【００２８】
図３は端末が音声コール（Ｖｏｉｃｅ　ｃａｌｌ）のために行う手続きについて示すメッセージの流れ図である。
【００２９】
前記端末１０が音声コールを行うために、ネットワーク２０にＣＭサービス要求メッセージ３０１を転送すると、ネットワーク２０は前記ＣＭサービス要求メッセージ３０１に暗号化を施すか否かを判断し、暗号化を施す場合、暗号化要求メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｑｕｅｓｔ）３０２を端末１０に

転送する。
【００３０】
ここで、前記ＣＭはＣｏｎｎｅｃｔｉｏｎ Ｍａｎａｇｅｍｅｎｔの略語である。
【００３１】
前記端末１０はネットワーク２０からの前記暗号化要求メッセージ３０２を受信し、これに対応して適切な暗号化承認応答メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｃｉｐｈｅｒｉｎｇ Ｒｅｓｐｏｎｓｅ）３０３をネットワーク２０に転送する。これで端末１０とネットワーク２０間の暗号化過程が完了する。
【００３２】
前記ネットワーク２０は端末１０からの前記暗号化承認応答メッセージ３０３を受信し、登録手続きが完了したというＣＭサービス登録完了メッセージ（ＣＭ Ｓｅｒｖｉｃｅ Ａｃｃｅｐｔ）３０４を前記端末１０に転送する。
【００３３】
次に、前記従来の過程を図４を参照して説明する。
【００３４】
ＧＳＭ方式の移動通信端末の電源がＯＮになり、待機状態４０１で端末はデータと関連した登録要求メッセージまたは音声コールと関連したＣＭサービス要求メッセージをネットワークに転送すると、前記ネットワークはこのメッセージを受信し４０２、暗号化を行うか否かを判断する４０３。
【００３５】
前記暗号化遂行可否の判断４０３結果、暗号化を行わない場合、暗号化を行わないという登録／ＣＭサービス完了メッセージを端末に転送し４０４、これで暗号化を行わない手続きが完了する４０５。
【００３６】
これにより、前記手続き後に転送されるすべてのデータは暗号化されていない状態で転送される。
【００３７】
前記暗号化遂行可否の判断４０３結果、暗号化を行う場合、ＲＡＮＤ（ＲＡＮＤｏｍ ｎｕｍｂｅｒ）値を生成し、ＳＲＥＳ（Ｓｉｇｎｅｄ Ｒｅｓｐｏｎｓｅ）値を算出／格納４０６した後、暗号化要求メッセージを端末に転送する４０７。
【００３８】
前記端末はネットワークからの前記暗号化要求メッセージを受信し、暗号化承認応答メッセージをネットワークに転送する。そうすると、前記ネットワークは端末からの前記暗号化承認応答メッセージを受信する４０８。
【００３９】
前記ネットワークは端末からの前記暗号化承認応答メッセージを受信し、ネットワークに格納されたＳＲＥＳ値と、前記端末からのＳＲＥＳ値とを比較して、両値が同一であるか否かを判断する４０９。
【００４０】
前記判断４０９結果、両値が同一でない場合、登録／ＣＭサービスをそれ以上使用できないという登録／ＣＭサービス不可メッセージを端末に転送し４１０、これで手続きが完了する４１１。
【００４１】
前記手続き完了４１１後には各種データの暗号化サービスが不可能となる。
【００４２】
前記判断４０９結果、両値が同一である場合、登録／ＣＭサービスを使用できるという登録／ＣＭサービス可能メッセージを端末に転送し４１２、手続きを完了する４１３。
【００４３】
前記手続き完了４１３後には各種転送データの暗号化サービスが可能となる。
【００４４】

以上で音声コール過程における暗号化動作がすべて完了する。

【００４５】

かかる従来の技術では、暗号化を行うか否かの判断が一方的にネットワークでのみ行われる。

【００４６】

よって、初期に暗号化手続きが行われない場合や特定のデータでない場合は、普通のデータ転送中にユーザが重要なデータの暗号化を所望しても、暗号化を行う方法が全くないという問題点がある。

【００４７】

このため、ユーザの重要なデータが外部から盗聴及び悪用されるおそれがある。

【００４８】

前記データだけでなく音声の場合にも暗号化されずに転送されてしまうので、ユーザの重要な情報がすべて他人に漏れてしまうという深刻な問題点がある。

【発明の開示】

【発明が解決しようとする課題】

【００４９】

したがって、本発明は、かかる従来の問題点を解決するためのもので、その目的は、移動通信システムにおいて、端末とネットワーク間で転送される情報の暗号化及び暗号化解除の時、その暗号化及び暗号化解除を移動通信ユーザ端末で直接行うための移動通信システムの転送情報暗号化及び暗号化解除装置及びその方法を提供することにある。

【課題を解決するための手段】

【００５０】

本発明の移動通信システムにおいて、端末とネットワーク間で転送される情報を暗号化するとき、それを移動通信端末で直接暗号化を行うが、この際、初期ネットワーク登録或いはサービス開示時点で端末とネットワーク間の暗号化過程が行われないことがある。

【００５１】

この場合、端末ユーザが自分の音声やデータの重要性によって特定時点からの暗号化を所望すると、前記端末ユーザは端末を用いて所定の暗号化手続きの進行をネットワークに要求する。

【００５２】

前記ネットワークは端末側からの特定時点暗号化要求を受信し、二つの方法によって所定の暗号化過程を行う。

【００５３】

第１、端末が暗号化準備過程の進行をネットワークに要求すると、通常の方法でネットワークによって暗号化過程が行われる。

【００５４】

第２、端末が暗号化を要求しながら特定値を含むメッセージをネットワークに転送すると、ネットワークはその特定値を基礎として暗号化準備過程に必要なキー値を算出した後、暗号化準備過程が完了したというメッセージを端末に転送し、この時点から端末とネットワークは暗号化を行い始める。

【００５５】

また、ユーザが重要データを転送完了し、それ以上暗号化を所望しない場合は、暗号化停止を要求するメッセージをネットワークに転送する。

【００５６】

そうすると、前記ネットワークはそれに対応する応答を端末に転送し、これにより端末とネットワーク間の暗号化過程はそれ以上行われない。

【００５７】

本発明は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、ユーザ端末が転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネ

ットワークが端末からの暗号化要求メッセージを受信し、それを承認するメッセージを前記端末に転送する承認段階と、前記端末がネットワークからの暗号化要求承認メッセージを受信し、それに応答するメッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、それに対応して情報転送中の暗号化準備が完了したというメッセージを端末に転送する完了段階とを含んでなる。

【００５８】

本発明は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、前記端末が転送情報に暗号化を要求する特定値を含ませてネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの前記特定値を基礎として情報暗号化準備過程に必要なキー値を算出した後、暗号化準備過程が完了したというメッセージを端末に転送する完了段階と、前記暗号化準備完了後、端末とネットワークが情報転送中に暗号化を行う実行段階とを含んでなる。

【００５９】

本発明は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末がすべての転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていると、前記ＲＡＮＤ値を用いて暗号化に必要なキー（Ｋｃ）値を算出し、転送情報の暗号化準備を完了する第１完了段階と、前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていないと、暗号化遂行可否に応じてＲＡＮＤ値を生成し、ＳＲＥＳ値を算出／格納し、暗号化準備が完了したという承認メッセージを端末に転送する第２完了段階と、前記端末がネットワークからの暗号化準備完了メッセージを受信し、ＳＲＥＳ値が含まれた応答メッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、ネットワークに格納されたＳＲＥＳ値と、端末からのＳＲＥＳ値とを比較して、同一か否かによって転送情報の暗号化可否を判断する判断段階とを含んでなる。

【００６０】

本発明は、移動通信端末とネットワーク間に送受信される情報の暗号化を解除する方法において、前記端末とネットワーク間の情報転送中の暗号化が不要ならば、ユーザ端末が転送情報の暗号化解除を要求するメッセージをネットワークに転送する暗号化解除要求段階と、前記ネットワークが端末からの暗号化解除要求メッセージを受信し、それを承認する転送中の暗号化解除メッセージを前記端末に転送する暗号化解除承認段階とを含んでなる。

【００６１】

本発明は、移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、前記移動通信ネットワークに暗号化要求を転送する送信機と、前記暗号化要求を受け、ネットワークに転送される情報を暗号化し、且つネットワークからの暗号化された情報を処理するプロセッサーとを含んでなる。

【００６２】

本発明は、移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、前記移動通信端末からの暗号化要求を受信する受信機と、前記暗号化要求に応答して、移動通信端末からの暗号化された情報を受信し、且つ移動通信端末に転送された情報を暗号化するプロセッサーとを含んでなる。

【００６３】

本発明による移動通信システムの転送情報暗号化方法は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、ユーザ端末が転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの暗号化要求メッセージを受信し、それを承認するメッセージを前記端末に転送する承認段階と、前記端末が

ネットワークからの暗号化要求承認メッセージを受信し、それに応答するメッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、それに対応して情報転送中の暗号化準備が完了したというメッセージを端末に転送する完了段階とを含んでなることを特徴とし、これにより上記目的を達成する。

【００６４】

前記承認段階による承認メッセージ中にはＲＡＮＤ値が含まれていることを特徴としてもよい。

【００６５】

前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することができることを特徴としてもよい。

【００６６】

前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することができることを特徴としてもよい。

【００６７】

前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンテクストアクティベーション情報の少なくとも一つであることを特徴としてもよい。

【００６８】

本発明による移動通信システムの転送情報暗号化方法は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、前記端末が転送情報に暗号化を要求する特定値を含ませてネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの前記特定値を基礎として情報暗号化準備過程に必要なキー値を算出した後、暗号化準備過程が完了したというメッセージを端末に転送する完了段階と、前記暗号化準備完了後、端末とネットワークが情報転送中に暗号化を行う実行段階とを含んでなることを特徴とし、これにより上記目的を達成する。

【００６９】

前記暗号化要求段階の特定値はＲＡＮＤ番号値を用いることを特徴としてもよい。

【００７０】

前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することができることを特徴としてもよい。

【００７１】

前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することができることを特徴としてもよい。

【００７２】

前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンテクストアクティベーション情報の少なくとも一つであることを特徴としてもよい。

【００７３】

本発明による移動通信システムの転送情報暗号化方法は、移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末がすべての転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていると、前記ＲＡＮＤ値を用いて暗号化に必要なキー（Ｋｃ）値を算出し、転送情報の暗号化準備を完了する第１完了段階と、前記ネットワークが端末からの前記暗号化要求メッセージを受信し、このメッセージ中にＲＡＮＤ値が含まれていないと、暗号化遂行可否に応じてＲＡＮＤ値を生成し、ＳＲＥＳ値を算出／格納し、暗号化準備が完了したという承認メッセージを端末に転送する第２完了段階と、前記端末がネットワークからの暗号化準備完了メッセージを受信し、ＳＲＥＳ値が含まれた応答メッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、ネットワークに格納されたＳＲＥＳ値と、端末からのＳＲＥＳ値とを比較して、同一か否かによって転送情報の暗号化可否を判断する判断段階とを含んでなることを特徴とし、こ

れにより上記目的を達成する。

【００７４】

前記第２完了段階の承認メッセージ中にはＲＡＮＤ値が含まれていることを特徴としてもよい。

【００７５】

前記暗号化要求段階では端末とネットワーク間に情報が転送される途中でも暗号化を要求することを特徴としてもよい。

【００７６】

前記暗号化要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化を要求することを特徴としてもよい。

【００７７】

前記第２完了段階のネットワークが、端末からの転送中の暗号化要求メッセージ中にＲＡＮＤ値が含まれず、暗号化を行わない場合、転送情報に暗号化が行われないというメッセージを端末に転送する段階をさらに含むことを特徴としてもよい。

【００７８】

前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴としてもよい。

【００７９】

本発明による移動通信システムの転送情報暗号化解除方法は、移動通信端末とネットワーク間に送受信される情報の暗号化を解除する方法において、前記端末とネットワーク間の情報転送中の暗号化が不要ならば、ユーザ端末が転送情報の暗号化解除を要求するメッセージをネットワークに転送する暗号化解除要求段階と、前記ネットワークが端末からの暗号化解除要求メッセージを受信し、それを承認する転送中の暗号化解除メッセージを前記端末に転送する暗号化解除承認段階とを含んでなることを特徴とし、これにより上記目的を達成する。

【００８０】

前記暗号化解除要求段階では端末とネットワーク間に情報が転送される途中でも暗号化解除を要求することができることを特徴としてもよい。

【００８１】

前記暗号化解除要求段階では端末とネットワーク間に転送される情報がない場合でも暗号化解除を要求することができることを特徴としてもよい。

【００８２】

前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴としてもよい。

【００８３】

本発明による移動通信端末は、移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、前記移動通信ネットワークに暗号化要求を転送する送信機と、前記暗号化要求を受け、ネットワークに転送される情報を暗号化し、且つネットワークからの暗号化された情報を処理するプロセッサーとを含んでなることを特徴とし、これにより上記目的を達成する。

【００８４】

前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴とし、これにより上記目的を達成する。

【００８５】

本発明による移動通信端末は、移動通信端末と移動通信ネットワーク間に送受信される情報を暗号化する装置において、前記移動通信端末からの暗号化要求を受信する受信機と、前記暗号化要求に応答して、移動通信端末からの暗号化された情報を受信し、且つ移動通信端末に転送された情報を暗号化するプロセッサーとを含んでなることを特徴とし、これにより上記目的を達成する。

【００８６】
前記情報は音声情報、データ、ＳＭＳ情報、ＳＳ情報及びＰＤＰコンタクストアクティベーション情報の少なくとも一つであることを特徴としてもよい。
【発明の効果】
【００８７】
本発明は、ＧＳＭ方式の移動通信端末においてユーザのデータ暗号化の手続きを改善することにより、ユーザのデータ転送の信頼性を高めることができる効果がある。のみならず暗号化準備過程の有無判断をネットワーウだけでなく端末でも行えるようにすることにより、端末ユーザがデータ転送を所望する時点から必要時にいつでもデータの暗号化及び暗号化解除を自由に行うことができ、これにより転送データの信頼性を向上させることができるという効果がある。
【発明を実施するための最良の形態】
【００８８】
以下、添付図を参照して本発明の好適な実施例を詳細に説明する。
【００８９】
図５は本発明の一実施例を示すＧＳＭ移動通信システムにおける暗号化準備過程を示す動作流れ図である。
【００９０】
以下、本発明で説明される実施例は、端末とネットワーク間でやり取りされるユーザデータを基準として説明するが、その他ユーザが転送するユーザ音声コール（Ｖｏｉｃｅ ｃａｌｌ）メッセージと、短文伝送のためのＳＭＳ（Ｓｈｏｒｔ ｍｅｓｓａｇｅ ｓｅｒｖｉｃｅ）、付加サービスのためのＳＳ（Ｓｕｐｐｌｅｍｅｎｔａｒｙ Ｓｅｒｖｉｃｅ）、ＧＰＲＳパケット転送のためのＰＤＰコンテクストアクティベーション（Ｐａｃｋｅｔ Ｄａｔａ Ｐｒｏｔｏｃｏｌ Ｃｏｎｔｅｘｔ Ａｃｔｉｖａｔｉｏｎ）などに適用することができる。
【００９１】
また、本発明で説明されるＧＳＭ移動通信システムとＧＳＭ移動通信端末は一つの実施例に過ぎないもので、ＧＤＭＡ移動通信システムとＣＤＭＡ移動通信端末などのあらゆる方式の移動通信システムと移動通信端末に幅広く適用することができる。
【００９２】
前記ユーザ音声コールメッセージの転送中の暗号化及び暗号化解除方法と、前記ユーザデータの転送中の暗号化及び暗号化解除方法とが同一であるので、そのうちユーザデータを基準として説明する。
【００９３】
前記図５において、ユーザが端末１０の電源をＯＮにすると、端末１０はネットワーク２０に登録を要求する。
【００９４】
前記移動通信端末１０は登録要求メッセージ（Ａｔｔａｃｈ Ｒｅｑｕｅｓｔ）５０１を無線でネットワーク２０の基地局１１１に転送し、基地局１１１は前記登録要求メッセージ５０１を基地局制御器１３０を経て移動通信交換局１５０に転送する。
【００９５】
前記ネットワーク２０は端末１０からの登録要求メッセージ５０１を受信し、暗号化を行うか否かを判断し、暗号化を行う場合、暗号化承認要求メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｃｉｐｈｅｒｉｎｇ Ｒｅｑｕｅｓｔ）５０２を端末１０に転送する。
【００９６】
前記端末１０はネットワーク２０からの前記暗号化承認要求メッセージ５０２を受信し、これに対応して適切な暗号化承認応答メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｃｉｐｈｅｒｉｎｇ Ｒｅｓｐｏｎｓｅ）５０３をネットワーク２０に転送する。
【００９７】

前記ネットワーク２０は端末１０からの前記暗号化承認応答メッセージ５０３を受信し、登録手続きが完了したという登録完了メッセージ（Ａｔｔａｃｈ　Ａｃｃｅｐｔ）５０４を前記端末１０に転送することにより、端末１０とネットワーク２０間の暗号化初期過程が完了する。

【００９８】

この際、前記ネットワーク２０の判断結果、暗号化を行わない場合、ネットワーク２０は暗号化メッセージを前記端末１０に転送しない。また、端末１０とネットワーク２０間のデータは暗号化されていない状態で普通の転送５０５が行われる。

【００９９】

前記端末１０とネットワーク２０間のデータの暗号化準備過程が初期登録手続きで行われず、データを転送する過程５０５で、ユーザが端末１０によるデータ転送中に暗号化を所望する場合、ユーザ端末１０はデータ転送中に暗号化を要求するメッセージ（Ａｃｔｉｖａｔｅ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｑｕｅｓｔ）５０６をネットワーク２０に転送する。

【０１００】

この際、前記データ転送中に暗号化を要求するメッセージ５０６は、その中に特定値（ＲＡＮＤ：　ＲＡＮＤｏｍ　ｎｕｍｂｅｒ）が含まれずにネットワーク２０に転送されてしまう。

【０１０１】

前記ネットワーク２０は端末１０からの前記データ転送中の暗号化要求メッセージ５０６を受信し、暗号化過程を行う。

【０１０２】

前記ネットワーク２０の暗号化準備過程が完了すると、ネットワーク２０は暗号化に必要な暗号化承認要求メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｑｕｅｓｔ）５０７を端末１０転送する。

【０１０３】

前記端末１０はネットワーク２０からの前記暗号化承認要求メッセージ５０７を受信し、これに対する応答として暗号化承認答メッセージ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｓｐｏｎｓｅ）５０８をネットワーク２０に転送する。

【０１０４】

前記端末１０が暗号化承認応答メッセージ５０８をネットワーク２０に転送すると、前記ネットワーク２０はデータ転送中の暗号化準備過程がすべて完了したというデータ転送中の暗号化準備完了メッセージ５０９を端末１０に転送することになり、これで暗号化準備過程に必要なすべての手続きが完了する。

【０１０５】

以上でデータ転送中の暗号化準備過程に必要なすべての手続きが完了すると、その後に転送されるすべてのデータは暗号化され転送される。

【０１０６】

図６では、前記端末１０からネットワーク２０へのデータ転送中に暗号化を要求するメッセージ６０１は、その中に特定値（ＲＡＮＤ：　ＲＡＮＤｏｍ　ｎｕｍｂｅｒ）が含まれてネットワーク２０に転送される。

【０１０７】

次いで、前記ネットワーク２は端末１０からの前記ＲＡＮＤ特定値を基礎として暗号化準備過程に必要なキー（Ｋｅｙ）値を生成し、その後暗号化準備過程が完了したというデータ転送中の暗号化準備完了メッセージ６０２を前記端末１０に転送する。

【０１０８】

前記データ転送中の暗号化準備完了メッセージ６０２の転送後には、端末１０とネットワーク２０間に転送されるすべてのデータは暗号化され転送される。

【０１０９】

ここで、前記端末１０がデータ転送中の暗号化要求メッセージを転送する時点は変わる

ことができ、端末１０とネットワーク間２０のデータ転送中に暗号化を要求することができ、また端末１０とネットワーク２０間の転送データがない場合にも暗号化を要求することができる。。

【０１１０】

また、端末１０とネットワーク２０間で暗号化が行われ暗号化済みデータが転送されている途中でも、端末ユーザがそれ以上暗号化転送を所望しない場合、図７に示すように端末ユーザは端末１０から、暗号化を停止するデータ転送中の暗号化解除要求メッセージ（Ｄｅａｃｔｉｖａｔｅ　Ｃｉｐｈｅｒｉｎｇ　Ｒｅｑｕｅｓｔ）７０１をネットワーク２０に転送する。

【０１１１】

前記端末からネットワークへの暗号化解除要求メッセージとは、端末から転送されるデータ中に暗号化解除用のメッセージが含まれていることを意味する。

【０１１２】

前記ネットワーク２０は端末１０からの前記データ転送中の暗号化解除要求メッセージ７０１を受信し、前記データ転送中の暗号化解除要求メッセージに相応するデータ転送中の暗号化解除準備完了メッセージ（Ｄｅａｃｔｉｖａｔｅ　Ｃｉｐｈｅｒｉｎｇ　Ｃｏｍｐｌｅｔｅ）７０２を端末１０に転送することにより、これまでの暗号化準備過程がすべて解除される。

【０１１３】

図８ａ及び図８ｂは、本発明のＧＳＭ移動通信システムにおける暗号化準備過程を示すフローチャートである。

【０１１４】

ＧＳＭ方式の移動通信端末が、待機状態またはデータ転送状態８０１でデータ転送中の暗号化要求メッセージをネットワークに転送すると，前記ネットワークは端末からの前記データ転送中の暗号化要求メッセージを受信し８０２、受信されたメッセージにＲＡＮＤ値が含まれているか否かを判断する８０３。

【０１１５】

本発明において、前記端末がデータ転送中の暗号化要求メッセージをネットワークに転送したということは、本発明の端末が既にＲＡＮＤ値を基準として暗号化のためのキー（ｋｃ）値を生成し終えることで、本発明の端末は暗号化準備が完了し、今度はネットワークが暗号化準備を完了する順番であるという意味である。

【０１１６】

したがって、本発明では転送中のデータの暗号化過程が端末によって主導されている。

【０１１７】

前記判断８０３の結果、受信された転送中の暗号化要求メッセージにＲＡＮＤ値が含まれていると、ＲＡＮＤ値を用いてデータ暗号化に必要なキー値を算出８０４する。その後、ネットワークが転送中の暗号化準備完了メッセージを端末に転送すると、前記端末は前記ネットワークからの前記転送中の暗号化準備完了メッセージを受信する８０５し、これで暗号化手続きが完了する８０６。

【０１１８】

前記暗号化手続きが完了した８０６後、転送されるすべてのデータは暗号化され転送される。

【０１１９】

前記判断８０３結果、受信された転送中の暗号化要求メッセージにＲＡＮＤ値が含まれていなければ、転送されるデータに暗号化を施すか否かを判断する８０７。

【０１２０】

前記判断８０３結果、転送されるデータに暗号化を施さない場合、データ転送中の暗号化不可メッセージを端末に転送し８０８、これで手続きが完了する８０９。

【０１２１】

前記暗号化不可手続きが完了した８０９後、転送されるすべてのデータは暗号化されず

に転送される。

【０１２２】

前記判断８０７結果、転送されるデータに暗号化を施す場合、ＲＡＮＤ（ＲＡＮＤｏｍ ｎｕｍｂｅｒ）値を生成してＳＲＥＳ（Ｓｉｇｎｅｄ Ｒｅｓｐｏｎｓｅ）値を算出／格納８１０した後、暗号化承認要求メッセージを端末に転送する８１１。この際、前記ＲＡＮＤ値を含ませて転送する。

【０１２３】

前記端末はネットワークからの前記暗号化承認要求メッセージを受信し、暗号化承認応答メッセージをネットワークに転送すると、前記ネットワークは端末からの暗号化承認応答メッセージを受信する８１２。

【０１２４】

ここには端末で算出したＳＲＥＳ値を含む。

【０１２５】

前記ネットワークは端末からの前記暗号化承認応答メッセージを受信し、ネットワークに格納されているＳＲＥＳ値と、前記端末からのＳＲＥＳ値とを比較した後、両値が同一であるか否かを判断する８１３。

【０１２６】

前記判断８１３結果、両値が同一でなければ、転送されるデータにそれ以上暗号を使用できないという転送中のデータ暗号化承認不可メッセージを端末に転送し８１４、これで手続きが完了する８１５。

【０１２７】

前記手続き完了８１５後には各種転送データの暗号化サービスが不可能となる。

【０１２８】

前記判断８１３結果、両値が同一であれば、転送されるデータが暗号化されるという転送中のデータ暗号化承認可能メッセージを端末に転送し８１６、これで手続きが完了する８１７。

【０１２９】

前記手続き完了８１７後には各種転送されるデータの暗号化サービスが可能となる。

【０１３０】

移動通信システムにおいて、端末とネットワーク間で転送される情報の暗号化及び暗号化解除の時、その暗号化及び暗号化解除を移動通信ユーザ端末で直接行うための移動通信システムの転送情報暗号化及び暗号化解除装置及びその方法を提供する。

【０１３１】

移動通信端末とネットワーク間に送受信される情報を暗号化する方法において、前記端末とネットワーク間の情報転送中に暗号化を必要とすると、ユーザ端末が転送情報の暗号化を要求するメッセージをネットワークに転送する暗号化要求段階と、前記ネットワークが端末からの暗号化要求メッセージを受信し、それを承認するメッセージを前記端末に転送する承認段階と、前記端末がネットワークからの暗号化要求承認メッセージを受信し、それに応答するメッセージをネットワークに転送する応答段階と、前記ネットワークが端末からの暗号化承認応答メッセージを受信し、それに対応して情報転送中の暗号化準備が完了したというメッセージを端末に転送する完了段階とを含んでなる。

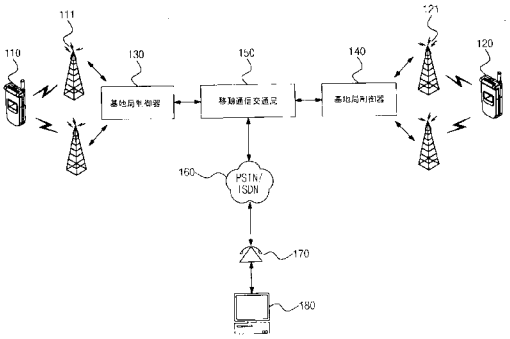
【０１３２】

以上のように、本発明の好ましい実施形態を用いて本発明を例示してきたが、本発明は、この実施形態に限定して解釈されるべきものではない。本発明は、特許請求の範囲によってのみその範囲が解釈されるべきであることが理解される。当業者は、本発明の具体的な好ましい実施形態の記載から、本発明の記載および技術常識に基づいて等価な範囲を実施することができることが理解される。本明細書において引用した特許、特許出願および文献は、その内容自体が具体的に本明細書に記載されているのと同様にその内容が本明細書に対する参考として援用されるべきであることが理解される。

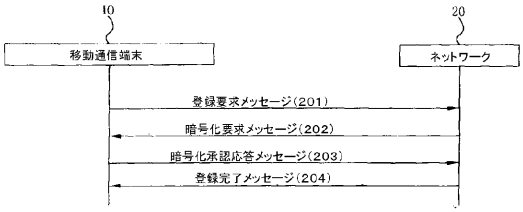
【図面の簡単な説明】

【０１３３】
【図１】ＧＳＭ移動通信端末の転送データ暗号化準備過程を示す通常の概略的なシステム構成図である。
【図２】従来のＧＳＭ移動通信端末とネットワーク間の暗号化準備過程中に行われるメッセージの流れ図である。
【図３】従来のＧＳＭ移動通信端末が音声コールを行うための手続きについて示すメッセージ流れ図である。
【図４】従来のＧＳＭ移動通信システムにおける暗号化準備過程を示すフローチャートである。
【図５】本発明のＧＳＭ移動通信システムにおける暗号化準備過程を示すシステム動作流れ図である。
【図６】本発明のＧＳＭ移動通信システムにおける特定キー値による暗号化準備過程を示すシステム動作流れ図である。
【図７】本発明のＧＳＭ移動通信システムにおける暗号化解除過程を示す動作流れ図である。
【図８ａ】本発明のＧＳＭ移動通信システムにおける暗号化準備過程を示すフローチャートである。
【図８ｂ】本発明のＧＳＭ移動通信システムにおける暗号化準備過程を示すフローチャートである。
【符号の説明】
【０１３４】
１１０　移動通信端末
１１１　基地局
１２０　移動通信端末
１２１　基地局
１３０　基地局制御器
１４０　基地局制御器
１５０　移動通信交換局
１６０　公衆電話交換網（ＰＳＴＮ）／総合情報通信網（ＩＳＤＮ）
１７０　一般有線電話
１８０　コンピュータ

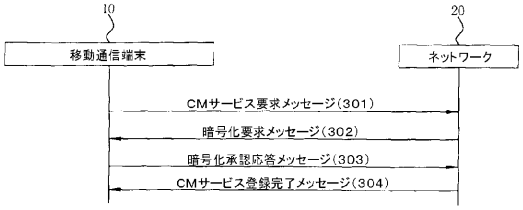
【図１】



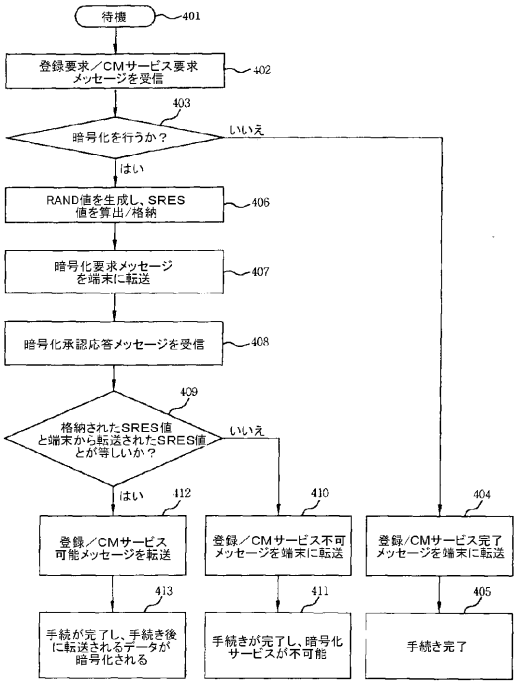
【図２】



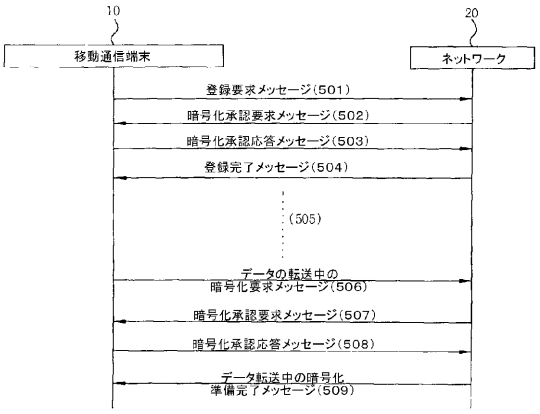
【図３】



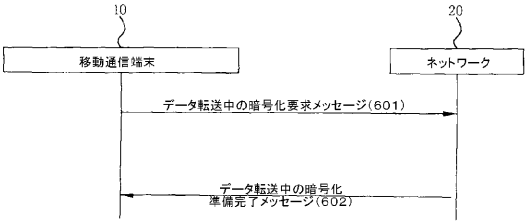
【図４】



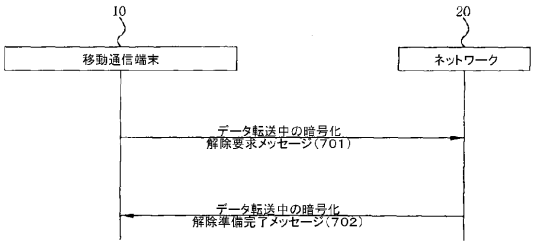
【図５】



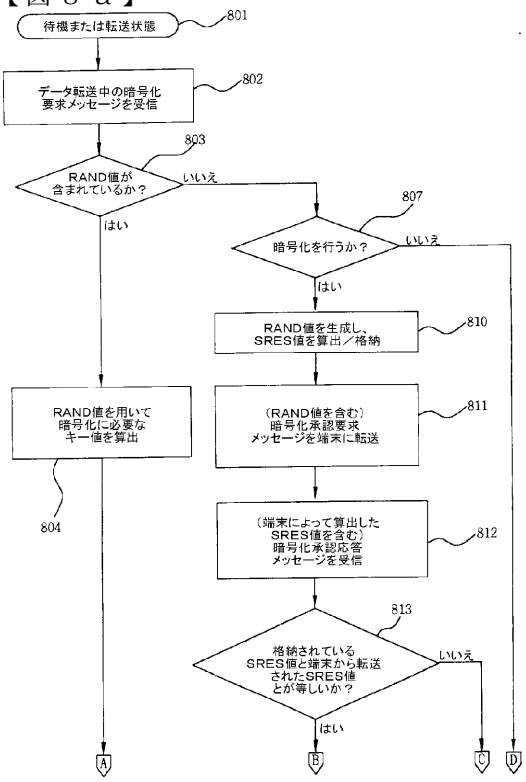
【図６】



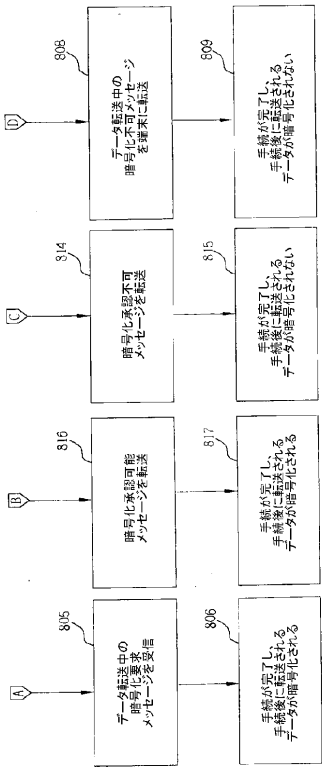
【図７】


10
20
移動通信端末
ネットワーク
データ転送中の暗号化
解除要求メッセージ(701)
データ転送中の暗号化
解除準備完了メッセージ(702)

【図８ａ】


待機または転送状態
801
データ転送中の暗号化
要求メッセージを受信
802
RAND値が
含まれているか？
803
いいえ
はい
暗号化を行うか？
807
いいえ
はい
RAND値を生成し、
SRES値を算出／格納
810
RAND値を用いて
暗号化に必要な
キー値を算出
804
(RAND値を含む)
暗号化承認要求
メッセージを端末に転送
811
(端末によって算出した
SRES値を含む)
暗号化承認応答
メッセージを受信
812
格納されている
SRES値と端末から転送
されたSRES値
とが等しいか？
813
いいえ
はい
A
B
C
D

【図８ｂ】


D
データ転送中の
暗号化不可メッセージ
を端末に転送
808
手続が完了し、
手続後に転送される
データが暗号化されない
809
C
暗号化承認不可
メッセージを転送
814
手続が完了し、
手続後に転送される
データが暗号化されない
815
B
暗号化承認可能
メッセージを転送
816
手続が完了し、
手続後に転送される
データが暗号化される
817
A
データ転送中の
暗号化要求
メッセージを受信
805
手続が完了し、
手続後に転送され
データが暗号化される
806

フロントページの続き

Ｆターム(参考) 5J104 AA01 AA16 AA32 AA33 BA02 EA01 EA04 EA15 JA03 MA05
NA02 PA01 PA07
5K067 AA30 AA32 DD24 DD51 EE02 EE10 EE16 EE23 HH22 HH23
HH24 HH36