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

特許第4002035号

(P4002035)

(45)発行日　平成19年10月31日(2007.10.31)　(24)登録日　平成19年8月24日(2007.8.24)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	630C
H04L	9/08	(2006.01)	H04L	9/00	601C
H04L	9/32	(2006.01)	H04L	9/00	675B
H04M	1/68	(2006.01)	H04M	1/68	
H04M	11/00	(2006.01)	H04M	11/00	303

請求項の数 7　(全 9 頁)

(21)出願番号　特願平11-214543
(22)出願日　平成11年7月29日(1999.7.29)
(65)公開番号　特開2000-83018(P2000-83018A)
(43)公開日　平成12年3月21日(2000.3.21)
審査請求日　平成12年10月12日(2000.10.12)
審判番号　不服2004-12119(P2004-12119/J1)
審判請求日　平成16年6月14日(2004.6.14)
(31)優先権主張番号　09/127766
(32)優先日　平成10年7月31日(1998.7.31)
(33)優先権主張国　米国(US)

(73)特許権者　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　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
(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】機密を要する情報を最初は機密化されてない通信を用いて伝送するための方法

(57)【特許請求の範囲】

【請求項１】

機密を要する情報を、無線通信システムの移動機に対して最初は機密化されてない通信を用いて伝送するための方法であって、

（ａ）前記移動機が、無線通信システムの網の公開キー（ＰＫｎｅｔ）と前記公開キーの証明を受信するステップ；

（ａ１）前記公開キーの証明に基づいて前記網の公開キーの正当性を検証することで、前記網を認証するステップ；

（ｂ）少なくとも第一の乱数と移動機情報とに前記公開キーを用いてキー付き暗号化を遂行することにより、暗号化結果を生成するステップ；

（ｃ）前記移動機から前記認証された網に前記暗号化結果を送信するステップとを含み、前記暗号化結果が前記移動機を認証するために用いられ、さらに；

（ｄ）認証された前記移動機と前記認証された網との間で第一と第二の通信チャネルを確立するステップとを含み、前記第一と第二の通信チャネルを通じた通信が暗号化され、さらに；

（ｅ）認証情報を前記第一の通信チャネルを通じて前記認証された網に送信するステップを含み、前記第一の通信チャネルが音声通信チャネルであり；および

（ｆ）前記第二の通信チャネルを通じて前記認証された網から機密を要する情報を受信するステップを含み、前記第二の通信チャネルは制御チャネルであることを特徴とする方法。

【請求項２】
前記移動機情報は、前記移動機に対する識別子であることを特徴とする請求項１の方法。
【請求項３】
前記ステップ（ｆ）が、前記機密を要する情報として、前記認証された網からルートキーを受信することを特徴とする請求項１の方法。
【請求項４】
前記ステップ（ｂ）の前に、さらに：
（ｈ）少なくとも前記第一の乱数を生成するステップを含むことを特徴とする請求項１の方法。
【請求項５】
無線通信システムの網からの機密を要する情報を最初は機密化されてない通信を用いて伝送するための方法であって、
（ａ）前記網の公開キー（ＰＫ$_{net}$）と前記公開キーの証明とを出力（送信）するステップ；および
（ｂ）無線通信システムの移動機が網を認証したときに、前記移動機からの暗号化結果を前記網が受信するステップとを含み、前記暗号化結果は、少なくとも第一の乱数と移動機情報とに前記網の前記公開キーを用いてキー付き暗号化を遂行することにより得られるものであり、さらに；
（ｃ）前記暗号化結果を解読することにより、前記第一の乱数と前記移動機情報とを得るステップ；
（ｄ）前記認証された網と前記移動機との間で第一と第二の通信チャネルを確立するステップを含み、前記移動機が前記移動機情報に基づいて認証され、前記第一と第二の通信チャネルを通じた通信が暗号化され、さらに；
（ｅ）前記第一の通信チャネルを通じて前記認証された移動機から認証情報を受信するステップを含み、前記第一の通信チャネルは音声チャネルであり；および
（ｆ）前記認証情報が許容できる場合、前記第一の乱数を用いて確立された第二の通信チャネルを通じて前記認証された移動機に機密を要する情報を伝送するステップを含み、前記第二の通信チャネルが制御チャネルであることを特徴とする方法。
【請求項６】
前記移動機情報は識別子であり、そして前記機密を要する情報がルートであり、前記方法はさらに、
（ｇ）前記ルートキーを前記移動機に対する前記識別子と関連づけるステップを含むことを特徴とする請求項５の方法。
【請求項７】
前記ステップ（ｆ）が、前記機密を要する情報としてルートキーを前記認証された移動機に送信することを特徴とする請求項５の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
機密を要する情報を最初は機密化されてない通信を用いて伝送するための方法
【０００２】
【従来の技術】
幾つかの最初は機密化されてない通信、例えば、空中通信（オーバーザーアエ通信）は、最初から機密化されている形式の通信、例えば、専用の通信チャネルより、通信の柔軟性および効率の面では優れる。ただし、不幸なことに、空中通信等の通信は、最初は機密化されてないために、アタッカによって２つのパーティ間の通信が中断され、被害を受けることがある。
【０００３】
無線通信システムにおいては、しばしば移動機とも呼ばれる移動機ユーザによって購入さ

れるハンドセットは、典型的には、サービスを起動するためには、網サービスプロバイダに持ち込み、長いキーおよびパラメータをそのハンドセットに入力することを必要とされる。網サービスプロバイダもその移動機に対して、長いキーおよびパラメータのコピーを維持し、これらをその移動機と関連づける。周知のように、これら長いキーおよびパラメータを用いることで、網と移動機の間で空中を通じて情報を機密に伝送することが可能となる。

【０００４】

別の方法においては、ユーザは、長いキーを安全な（機密）通信チャネル（例えば、地上回線や郵便）通じて受け取り、これらコードを手操作で移動機に入力する。

【０００５】

長いキーおよびパラメータを、空中を介してではなく、機密通信チャネルを通じて受け取る方法や、網サービスプロバイダに出向いて受け取る方法は、空中アタックに対しては安全である。ただし、これらの情報を安全（機密）に伝送するための方法は、移動機ユーザになんらかの負担および制約を課す。理想的には、移動機ユーザにとっては、ハンドセットを購入したときハンドセットを物理的にプロバイダの所に持ち込んだり、あるいは、移動機に手操作にて長いコードを入力することを必要とされることなく、直ちにサービスを得られることが望ましい。移動機を遠隔的に起動および準備する能力は北米無線標準の一部であり、“over the air service provisioning、OTAP）”（空中を通じてのサービスの準備）と呼ばれる。

【０００６】

現在、北米セルラ標準IS41-Cは、OTASP プロトコルを指定するが、このプロトコルにおいては、２パーティ間の機密キーを確立するために（つまり、機密情報を伝送するために）周知のDiffe-Hellman （DH）キー合意が用いられる。図１は、IS41-Cにおいて用いられるDHキー合意を、移動機と網との間の機密キーの確立に適用した場合について示す。すなわち、図１は、DHキー合意に従う網１０と移動機２０との間の通信を簡略的に示す。ここで用いられる網なる用語は、網サービスプロバイダによって運用される認証センタ、ホーム位置レジスタ、ビジティング（訪問）位置レジスタ、移動体交換センタ、および基地局を総称的に指す。

【０００７】

網１０は、乱数R_Nを生成し、（g^R_N mod p）を計算する。図１に示すように、網１０は、５１２ビットの素数ｐ、素数ｐによって生成されるグループ（群）のジェネレータ（生成プログラム）ｐ、および（g^R_N mod p）を移動機２０に送信する。次に、移動機２０は、乱数R_Mを生成し、（g^R_M mod p）を計算し、（g^R_M mod p）を網１０に送信する。

【０００８】

移動機２０は、網１０から受信された(g^R_N mod p)に乱数R_Mをべき乗することで(g^$R_M R_N$ mod p)を得、網１０は、移動機２０から受信された(g^R_N mod p)に乱数R_Nをべき乗することで(g^$R_M R_N$ mod p)を得る。移動機２０と網１０は両方とも同一の結果を得、この６４個の最下位ビットを用いて、Ａ－キーと呼ばれる長く生きるキーを確立する。このＡ－キーは、移動機２０と網１０との間の通信を機密化するために用いられる他のキーを生成するためのルートキーとして用いられる。

【０００９】

このDHキー交換と関連する一つの問題は、これが認証手続きを経ておらず、受マン－イン－ザ－ミドルアタックに弱いことである。例えば、移動機と網との２パーティ間の通信の例においては、アタッカは、最初に網１０のふりをし、次に、網１０に対して、移動機のふりをする。こうして、アタッカは、移動機２０と網１０との間でメッセージを中継する際に、Ａ－キーを選択し、これを知ることで、認証要件を満すことができる。加えて、DHキーの交換は、オフラインディクショナリアタックにも弱い。

【００１０】

最初は機密化されてない通信チャネルを用いて機密を要する情報を伝送するためのもう一

つのプロトコルとして、CFT（Carrol-Frankel-Tsiounis）キー分配プロトコルがある。このプロトコルの詳細に関しては、Carrolらによる論文“Efficient key distribution for slow computing devices:Achieving fast over the air activation for wireless systems”,IEEE Symposium on Security and Privacy,May 1998を参照されたい。このCFTキー分配プロトコルは、片方のパーティが証明機関（certificate authority、CA）の公開キーを所有していることを想定する。説明の目的で、このプロトコルを、以下に、網１０と移動機２０との間の空中通信の背景で詳細に説明する。

【００１１】

CA（証明機関）は、自身の特別なキーを維持する信頼のおける機関である。より詳細には、CAは、公開キーPK_{CA}および機密解読キーdk_{CA}を維持する。網サービスプロバイダは、例えば、CAに出向き、CAに対して、彼らの公開キーPK_{net}の署名をリクエストする。より詳細には、CAは、公開キーPK_{net}を他の情報と共にハッシュすることで、ENC_{dkCA}(h(PK_{net} + 他の情報）に等しい網に対する証明を生成する。ここで、これは、PK_{net}と他の情報のハッシュを、暗号化／解読アルゴリズムENCを、dk_{CA}を解読キーとして用いて解読することによって得られる。こうして、PK_{CA}についての知識を持つパーティは、この証明を暗号化することで、PK_{net}と他の情報のハッシュを得ることができる。この他の情報は、網がその公開キーと共に運ぶ（伝送する）ことを望む任意の他の情報を表す。

【００１２】

以下では、CFT キー（鍵）分配プロトコルについて図２との関連で説明する。図２は、簡潔さのために、CFT キー分配プロトコルに従う網１０と移動機２０との間の通信を簡略的に示す。図２に示すように、網１０は、最初に、その公開キーPK_{net}、他の情報、および証明を、移動機２０に送信する。移動機２０は、CAの公開キーPK_{CA}を用いて、公開キーPK_{net}＋証明からの他の情報の、ハッシュを得る。移動機は、網１０から平文にて受信される公開キーPK_{net}＋他の情報の、ハッシュも得る。

【００１３】

移動機２０は、次に、ハッシュの結果が証明から得られたそれと一致する場合は、その公開キーPK_{net}が正当であるものと認証する。公開キーPK_{net}の正当性を検証した後、移動機２０は、自身の中に用意されている乱数ジェネレータ（乱数生成プログラム）を用いて、第一の乱数を、セッションキー（SK）として生成し、第二の乱数APを、検証の目的で生成する。次に、移動機２０は、これらセッションキーSKと乱数APを、暗号化／解読アルゴリズムENC に従って、公開キーPK_{net}を用いて暗号化する。ENC_{PKnet}(SK、AP) なる表現はこの暗号化を表す。移動機２０は、次に、この暗号化の結果を網１０に送信する。

【００１４】

網１０は、移動機２０の出力を、公開キーPK_{net}と関連する解読キーdk_{net}を用いて復号（解読）することで、セッションキーSKおよび乱数APを得る。当業者においては理解できるように、機密のためには、網１０は、暗号解読キーdk_{net}を知っていることのみを要求される。次に、網１０は、Ａ－キー、つまり、上述のルートキー、および乱数APを、暗号化／解読アルゴリズムENC にて、セッションキーSKを用いて暗号化し、次に、暗号化の結果を移動機２０に返信する。

【００１５】

移動機２０は、セッションキーSKを用いて、網１０の出力を解読することで、Ａ－キーおよび乱数APを得る。移動機２０は、次に、網１０の出力から復号（解読）された乱数APが、最初に移動機２０から網１０に送信した乱数APと一致するか検証する。一致する場合は、移動機２０は、そのＡ－キーを、アタッカからではなく、網１０から来たものとして認証し、続いて、移動機２０は、最終的には、未認証ではあるが、このＡ－キーから導かれる（生成される）キーを用いて暗号化される音声通信が行なわれる任意の周知の通信プロトコル（例えば、IS41-C）を遂行する。この起動プロセスの次のステップとして、こうして暗号化された音声チャネルが移動機２０と網１０との間に確立され、網サービスプロバイダは、移動機ユーザから認証情報（例えば、課金の目的のクレジットカード情報）をリクエストする。この認証情報が受理された場合は、網１０は、移動機ユーザを認証し、以

降、サービスを提供する。

【００１６】

【発明が解決しようとする課題】

ただし、CFTプロトコルは、同一ハンドセットが、Ａ－キーを、OTASP（空中を通じてのサービスの準備のための呼）に対して反復して用いた場合は、安全（機密）でなくなる。具体的には、移動機が自身の通し番号（識別番号）を用いて、OPASP のために、網にアクセスするものと想定する。このとき、アタッカは、このアクセスをブロックし、乱数セッションキーSKおよび乱数APを傍受し、これらをブロックした移動機の識別番号を用いて網に送信する。網は、これに応答して暗号化されたＡ－キーを送り返す。すると、アタッカは、これを取り出し、接続を放棄する。こうして、アタッカは、その移動機に対するＡ－キーを手に入れる。本当の移動機が、再び、自身のセッションキーSKおよび乱数APを用いて網にアクセスすると、網は、再び、同一のキーを移動機からのセッションキーSKにて暗号化して移動機に送信する。この結果、移動機はＡ－キーを獲得する。その後、移動機が認証情報を暗号化された音声チャネルを用いて供給することでサービスの準備は完了する。ただし、不幸なことに、アタッカは、既に、Ａ－キーを手に入れており、後に、アタッカもこれを用いて偽の呼をかけることができる。

【００１７】

このアタックを阻止するための一つの方法として、網がOTASP呼が同一の移動機から発信された場合でも、各OTASP の試みに対して、異なるＡ－キーを生成する方法が考えられる。CFT プロトコルの作成者は、このことをインプリシット（陰的）に想定するが、ただし、キー分配プロトコルにはこのような制約を課されるべきではないため、これは、イクスプリシット（陽的）にすべきである。ただし、網にこの制約が追加された場合は、網は擬似乱数関数（pseudo-random function、PRF）を用いてＡ－キーを移動機に関連付けるスキームや、他の類似のスキームを遂行できなくなる。

【００１８】

第二に、CFT プロトコルでは、より穏やかな形式であるサービスの拒絶というアタックが可能となる。この形式のアタックでは、アタッカは、このプロトコル全体を通じて、移動機の本当のＩＤ番号の代わりに、別のｉｄ番号を用いる。この場合、プロトコルは成功するが、ただし、本当の移動機のｉｄ番号は起動されない。こうして、その後のユーザによるシステムへのアクセスの試みは拒絶される。このアタックは、通信に用いられる移動機のｉｄ番号が移動機から網に送信されるセッションキーSKおよび乱数APの公開キー暗号化の一部を構成しないために可能となる。

【００１９】

【課題を解決するための手段】

本発明による機密を要する情報を最初は機密化されてない通信を用いて伝送するための方法においては、第一のパーティは第二のパーティの公開キーを受信し、暗号化結果を生成する。この暗号化結果は、キー（鍵）付き暗号化を、少なくとも第一の乱数に関して前記公開キーを用いて遂行することで生成される。第一のパーティは、次に、この暗号化結果を第二のパーティに送信する。第二のパーティは、この暗号化結果を解読することで、前記第一の乱数を得る。次に、第一のパーティから、認証情報が前記第一の乱数を用いて確立された第一の暗号化され認証された通信チャネルを通じて第二のパーティに送信される。第二のパーティがこの認証情報を受理した場合は、さらに、第二のパーティから機密を要する情報が、前記第一の乱数を用いて確立された第二の暗号化され認証された通信チャネルを通じて第一のパーティに送信される。

【００２０】

無線産業に適用された場合は、無線システムの移動機が第一のパーティとなり、網が第二のパーティとなる。この用途においては、機密を要する情報として、ルートキー、例えば、Ａ－キーが伝送される。

【００２１】

従来のプロトコルとは異なり、本発明による方法は、機密を要する情報の伝送は、認証情

報が受理されるまでは許されない。さらに、第一のパーティの識別子に関してもキー（鍵）付き暗号化が遂行されるために、サービスの拒絶というアタックも防止できる。

【００２２】

【発明の実施の形態】

以下に本発明のより完全な理解を図るために、本発明を図面を用いて詳細に説明するが、これら図面中、類似する参照符号は対応するパーツを指す。

【００２３】

以下では、本発明による機密を要する情報を最初は機密化されてない通信を用いて伝送するための方法を、網１０と移動機２０の間のＡ－キーの空中通信に適用された場合について説明する。ただし、本発明は、（単に移動機と網との間の、単にＡ－キーの空中通信のみでなく）、任意のパーティ間での任意の情報の通信に適用できることに注意する。例えば、本発明による方法は、インターネットを通じてのパーティ間の通信にも適用できる。ただし、簡潔さの目的で、以下では、本発明による方法は、網１０と移動機２０との間でのＡ－キーの空中通信に適用された場合について説明される。

【００２４】

図３は、本発明によるプロトコルに従う網１０と移動機２０との間の通信を図解する。図３に示すように、網１０は、最初、その公開キーPK_{net}、他の情報、および証明を移動機２０に送信する。移動機２０は、CA（証明機関）の公開キーPK_{CA}を用いて、公開キーPK_{net}＋証明からの他の情報のハッシュを得る。より詳細には、CAによって用いられる暗号化／解読アルゴリズムおよびハッシングアルゴリズム、並びに、CAの公開キーが、移動機２０内に事前に格納されており、移動機２０は、この暗号化／解読アルゴリズムおよびCAの公開キーPK_{CA}を用いて、送信された証明を暗号化することで、公開キーPK_{net}と任意の他の情報のハッシュを得る。移動機２０は、さらに、ハッシングアルゴリズムを用いて、網１０から平文にて受信される公開キーPK_{net}＋証明からの他の情報のハッシュも得る。

【００２５】

移動機２０は、次に、前者のハッシュの結果が、証明から得られたそれと一致する場合は、その公開キーPK_{net}を、正当であるものと認証する。

【００２６】

公開キーPK_{net}の正当性を検証した後、移動機２０は、自身中に用意されている乱数ジェネレータ（乱数生成プログラム）を用いて、乱数を、セッションキー（SK）として生成する。次に、移動機２０は、周知の暗号化／解読アルゴリズムENCにて、このセッションキーSKおよび移動機２０の識別番号IDを公開キーPK_{net}を用いて暗号化し、この暗号化の結果を網１０に送信する。好ましくは、この暗号化／解読アルゴリズムENCは、周知のRSAアルゴリズムとされる。特に、改めて明記しない限り、この明細書において言及される全ての暗号化および解読（動作）は、このRASアルゴリズムに従って遂行されものと想定されるが、ただし、当業者においては理解できるように、他の暗号化／解読アルゴリズム、例えば、Rabinアルゴリズムを用いることも、あるいは、複数のアルゴリズムを用いることもできる。

【００２７】

網１０は、移動機２０の出力を、公開キーPK_{net}と関連する解読キーdk_{net}を用いて復号（解読）することで、セッションキーSKおよび移動機２０の識別番号IDを得る。次に、網１０は、このセッションキーSKをルートキー（Ａ－キー）として用い、任意の周知のプロトコル、例えば、IS41-Cにて、暗号化された音声チャネルを自身と移動機２０との間に確立する。さらに、この音声チャネルが任意の周知のメッセージ認証アルゴリズム、例えば、HMACアルゴリズムを用いてメッセージ認証（検証）される。

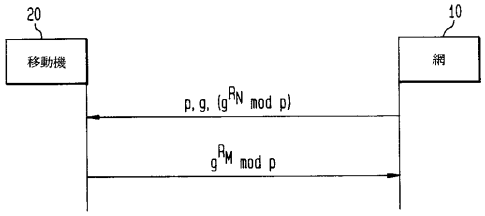
【００２８】

網サービスプロバイダは、この暗号化された音声チャネルを通じて、認証情報（例えば、課金の目的のクレジットカード情報）を移動機ユーザからリクエストする。この認証情報が受理された場合は、このプロトコルは継続される。ただし、この認証情報が受理されなかった場合は、このプロトコルは終端する。

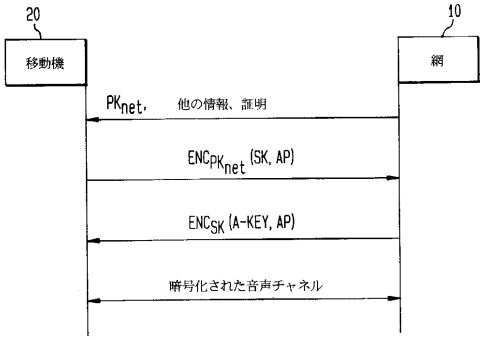
【００２９】
いったん認証プロトコルが受理されると、網は、移動機２０に向けて暗号化されメッセージ認証された制御チャネルを確立する。このチャネルの確立のためには、暗号化のための任意の周知のプロトコル、例えば、IS41-C、およびメッセージ認証のための任意の周知のプロトコル、例えば、HMACが用いられ、これらプロトコルにおいては、上述のセッションキーSKが、ルート、すなわち、Ａ－キーとして用いられる。
【００３０】
好ましくは、暗号化のために用いるプロトコル、例えば、IS41-Cプロトコルが、本発明と同一の発明者によって同時に出願された２つの特許出願、つまり、“ METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT（２パーティ認証およびキー合意のための方法）”、および“ METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INTIALLY UNSECURED COMMUNICATION（最初は機密化されてない通信を用いて機密を要する情報を伝送するための方法）”のいずれか一つに開示される認証（手続き）を遂行するように修正される。詳しくは、本発明の発明者によって同時に出願されたこれら二つの特許出願、つまり、“ METHOD FOR TWO PARTY AUTHENTICATION AND KEY AGREEMENT（２パーティ認証およびキー合意のための方法）”、および“ METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INTIALLY UNSECURED COMMUNICATION（最初は機密化されてない通信を用いて機密を要する情報を伝送するための方法）”の全内容を参照されたい。
【００３１】
別の方法として、認証され暗号化された音声チャネルと認証され暗号化された制御チャネルを別個に確立する代わりに、これら両方のチャネルを同時に確立することもできる。もう一つの代替として、認証情報を音声チャネルを通じて送信しないことも、さらにもう一つの代替として、同一の暗号化され認証された通信チャネルを用いて認証情報と機密を要する情報の両方を伝送することもできる。
【００３２】
次に、網１０は、こうして認証され、暗号化された制御チャネルを用いてＡ－キーを移動機２０に送信する。網１０は、さらに、このＡ－キーを移動機２０から受信されるIDを用いて移動機２０Ｓ関連づける。こうして、その後は、これと同一のＡ－キーが各OTASP の試みに対して発行される。次に、移動機２０と網１０との間の通信がこの新たに送信されたＡ－キーに基づいて再構成（リコンフィギュア）される。
【００３３】
CFT キー分配プロトコルとは異なり、本発明によるプロトコルの一つの実施例においては、網は、特定のＡ－キーを移動機と識別番号を用いて関連づける。このため、各OTASPに対してランダムに確立したＡ－キーを用いる必要はなくなる。さらに、本発明によるプロトコルは、Ａ－キーをユーザの認証情報が受信されるまでは確立しないた。このため、このプロトコルは、上述のマン－イン－ザ－ミドルアタックに対する対抗できる。さらに、移動機のｉｄも暗号化して網に送られ。このため、サービスの拒絶という形式のアタックを防止できる。
【００３４】
本発明がこうして説明されたが、明らかなように、本発明は、様々な修正された形態にて実現することもでき、これらバリエーションも、本発明の精神および範囲から逸脱するものと見做されるべきではなく、これら全ての修正が特許請求の範囲に含まれるものである。
【図面の簡単な説明】
【図１】 Diffe-Hellmanキー（鍵）合意に従う網と移動機との間の通信を示す図である。
【図２】 Carroll-Frankel-Tsiounis（CFT）キー分配プロトコルに従う網と移動機との間の通信を示す図である。
【図３】本発明のプロトコルに従う網と移動機との間の通信を示す図である。
【符号の説明】

１０　網
２０　移動機

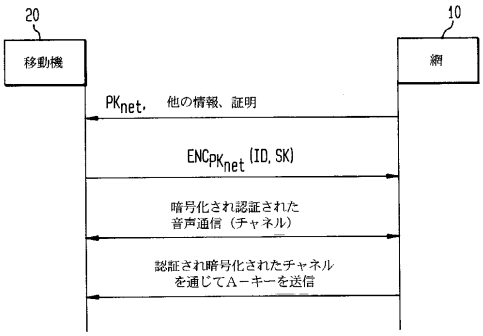
【図１】



【図２】



【図３】



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 サーヴァー パテル
アメリカ合衆国 ０７０４５ ニュージャーシィ，モンヴィル，ミラー レーン ３４

合議体
審判長 吉岡 浩
審判官 青木 重徳
審判官 相崎 裕恒

(56)参考文献 特開平６－１８８７７（ＪＰ，Ａ）
特開平４－５０５６９３（ＪＰ，Ａ）
Ｍｉｃｈａｅｌ Ｊ. Ｂｅｌｌｅｒ，“Ｐｒｉｖａｃｙ ａｎｄ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｎ ａ Ｐｏｒｔａｂｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｙｓｔｅｍ”，ＩＥＥＥ Ｊｏｕｒｎａｌ ｏｎ Ｓｅｌｅｃｔｅｄ Ａｒｅａｓ ｉｎ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ，Ａｕｇｕｓｔ １９９３，Ｖｏｌ. １１，Ｎｏ. ６，ｐ. ８２１－８２９

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08
G09C 1/00
H04M 1/68
H04M11/00