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

特許第4689830号
(P4689830)

(45)発行日　平成23年5月25日(2011.5.25)　(24)登録日　平成23年2月25日(2011.2.25)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/32 (2006.01)　H04L 9/00 675A
H04L 9/00 601A

請求項の数 21　(全 12 頁)

(21)出願番号　特願2000-578954 (P2000-578954)
(86)(22)出願日　平成11年10月19日 (1999.10.19)
(65)公表番号　特表2002-529013 (P2002-529013A)
(43)公表日　平成14年9月3日 (2002.9.3)
(86)国際出願番号　PCT/US1999/024522
(87)国際公開番号　WO2000/025475
(87)国際公開日　平成12年5月4日 (2000.5.4)
審査請求日　平成18年10月17日 (2006.10.17)
(31)優先権主張番号　09/178,192
(32)優先日　平成10年10月23日 (1998.10.23)
(33)優先権主張国　米国(US)

(73)特許権者　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　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100095441
弁理士　白根　俊郎

最終頁に続く

(54)【発明の名称】無線システムのための申し込み登録方法、装置、無線装置及びホームシステム

(57)【特許請求の範囲】
【請求項１】
無線端末に無線申し込みを登録するための方法であって、該方法は、
ａ）該無線端末にユーザ識別子及びパスワードを入力する；
ｂ）該無線端末で：
ｉ）公開／秘密キーペアを発生する；
ii）該パスワードを使用して、安全キー交換（ＳＫＥ）プロトコルに従って該無線端末の公開キーを暗号化し、それにより第１のＳＫＥメッセージを形成する；及び
iii)ホームシステムに該ユーザ識別子及び該第１のＳＫＥメッセージを送信する；
ｃ）該ホームシステムで：
ｉ）公開／秘密キーペアを発生する；
ii）該ユーザ識別子を使用して、該パスワードを決定する；
iii）該パスワードを使用して、ＳＫＥプロトコルに従って該ホームシステムの公開キーを暗号化し、それにより第２のＳＫＥメッセージを形成する；
iv）該無線端末に該第２のＳＫＥメッセージを送信する；
ｖ）該パスワードを使用して、該無線端末の公開キーを解読する；及び
vi）該ホームシステムの秘密キー及び該無線端末の公開キーを使用して、セッションキーを形成する；
ｄ）該無線端末で：
ｉ）該パスワードを使用して、該ホームシステムの公開キーを解読する；及び

ii）該無線端末の秘密キー及び該ホームシステムの公開キーを使用して、セッションキーを形成する；及び

e）該無線端末及び該ホームシステムの両方で、該セッションキーを使用して、該ホームシステムから該無線端末にバーチャルユーザ識別モジュール（ＶＵＩＭ）の全部または一部をダウンロードする、ことを具備し、

前記第１のＳＫＥメッセージを送信することは、該第１のＳＫＥメッセージを前記無線端末から中間サービングシステムに送信し、該第１のＳＫＥメッセージを該中間サービングシステムから前記ホームシステムに送信し、

前記第２のＳＫＥメッセージを送信することは、該第２のＳＫＥメッセージを前記ホームシステムから前記中間サービングシステムに送信し、該第２のＳＫＥメッセージを該中間サービングシステムから前記無線端末に送信し、

該中間サービングシステム内の該無線端末の次の認証における認証キーとして該セッションキーの第１の部分を使用し、次の制御信号送信における暗号化キーとして該セッションキーの第２の部分を使用する方法。

【請求項２】

該ユーザ識別子を送信する前にそれを暗号化する工程をさらに具備する、請求項１の方法。

【請求項３】

該第２のＳＫＥメッセージを該無線端末に送信する前に通信チャネルを開く工程をさらに具備する、請求項１の方法。

【請求項４】

請求項１の方法であって、

ａ）該公開／秘密キーペアがディッフィーヘルマン公開／秘密キーペアを具備し；及び

ｂ）該ＳＫＥメッセージがディッフィーヘルマン暗号化キー交換（ＤＨ－ＥＫＥ）メッセージを具備する：

請求項１の方法。

【請求項５】

下記を具備する請求項１の方法：

ａ）該パスワードを使用して、該無線端末の公開キーを暗号化する工程が次の該工程を具備する：

ｉ）該無線端末の公開キーを第１のランダム数で最初に連結し、それにより第１の連結された数を形成する；及び

ii）該パスワードを使用して、該第１の連結された数を暗号化する；及び

ｂ）該パスワードを使用して、該ホームシステムの公開キーを暗号化する工程は、次の該工程を具備する：

ｉ）該ホームシステムの公開キーを第２のランダム数で最初に連結し、それにより第２の連結された数を形成する；及び

ii）該パスワードを使用して、該第２の認証された数を暗号化する。

【請求項６】

無線端末に無線申し込みを登録するための装置であって、該装置は、

ａ）該無線端末にユーザ識別子及びパスワードを入力するための手段；

ｂ）該無線端末で：

ｉ）公開／秘密キーペアを発生するための手段；

ii）該パスワードを使用し、安全キー交換（ＳＫＥ）プロトコルに従って該無線端末の公開キーを暗号化し、それにより第１のＳＫＥメッセージを形成するための手段；及び

iii)ホームシステムに該ユーザ識別子及び該第１のＳＫＥメッセージを送信するための手段；

ｃ）該ホームシステムで：

ｉ）公開／秘密キーペアを発生するための手段；
ii）該ユーザ識別子を使用して、該パスワードを決定するための手段；
iii）該パスワードを使用し、ＳＫＥプロトコルに従って該ホームシステムの公開キーを暗号化し、それにより第２のＳＫＥメッセージを形成するための手段；
iv）該無線端末に該第２のＳＫＥメッセージを送信するための手段；
ｖ）該パスワードを使用して、該無線端末の公開キーを解読するための手段；及び
vi）該ホームシステムの秘密キー及び該無線端末の公開キーを使用して、セッションキーを形成するための手段；
ｄ）該無線端末で：
ｉ）該パスワードを使用して、該ホームシステムの公開キーを解読するための手段；及び
ii）該無線端末の秘密キー及び該ホームシステムの公開キーを使用して、セッションキーを形成するための手段；及び
ｅ）該無線端末及び該ホームシステムの両方で、該セッションキーを使用して、該ホームシステムから該無線端末にバーチャルユーザ識別モジュール（ＶＵＩＭ）の全部または一部をダウンロードするための手段を具備し、
前記第１のＳＫＥメッセージを送信するための手段は、
該第１のＳＫＥメッセージを前記無線端末から中間サービングシステムに送信するための手段と、
該第１のＳＫＥメッセージを該中間サービングシステムから前記ホームシステムに送信するための手段と、を具備し、
前記第２のＳＫＥメッセージを送信するための手段は、
該第２のＳＫＥメッセージを前記ホームシステムから前記中間サービングシステムに送信するための手段と、
該第２のＳＫＥメッセージを該中間サービングシステムから前記無線端末に送信するための手段と、を具備し、
該中間サービングシステム内の該無線端末の次の認証における認証キーとして該セッションキーの第１の部分を使用するための手段と、
次の制御信号送信における暗号化キーとして該セッションキーの第２の部分を使用するための手段とをさらに具備する装置。

【請求項７】
該ユーザ識別子を送信する前にそれを暗号化するための手段をさらに具備する、請求項６の装置。

【請求項８】
該第２のＳＫＥメッセージを該無線端末に送信する前に通信チャネルを開くための手段をさらに具備する、請求項６の装置。

【請求項９】
下記を具備する請求項６の装置：
ａ）該公開／秘密キーペアがディッフィー－ヘルマン公開／秘密キーペアを具備し；及び
ｂ）該ＳＫＥメッセージがディッフィー－ヘルマン暗号化キー交換（ＤＨ－ＥＫＥ）メッセージを具備する。

【請求項１０】
下記を具備する請求項６の装置：
ａ）該無線端末の公開キーを暗号化するために該パスワードを使用するための手段が次を具備する：
ｉ）該無線端末の公開キーを第１のランダム数で最初に連結し、それにより第１の連結された数を形成するための手段；及び
ii）該第１の連結された数を暗号化するために該パスワードを使用するための手段；及び

ｂ）該パスワードを使用して、該ホームシステムの公開キーを暗号化するための手段が次を具備する：

ｉ）該ホームシステムの公開キーを第２のランダム数で最初に連結し、それにより第２の連結された数を形成するための手段；及び

ii）該パスワードを使用して、該第２の連結された数を暗号化するための手段。

【請求項１１】

該無線端末内にユーザ識別子及びパスワードを受信するための手段と、

公開／秘密キーペアを発生するための手段と、

該パスワードを使用し、安全キー交換（ＳＫＥ）プロトコルに従って該無線端末の公開キーを暗号化し、それによりＳＫＥメッセージを形成するための手段と、

ホームシステムに該ユーザ識別子及び該ＳＫＥメッセージを送信するための手段と、

該ホームシステムから暗号化された公開キーを受信するための手段と、

該パスワードを使用して、該ホームシステムからの該暗号化された公開キーを解読するための手段と、

該無線端末の秘密キー及び該ホームシステムの公開キーを使用して、該セッションキーを形成するための手段と、

該セッションキーを使用して、該ホームシステムから該無線端末にバーチャルユーザ識別モジュール（ＶＵＩＭ）の全部または一部をダウンロードするための手段と、を具備し、

前記ＳＫＥメッセージを送信するための手段は、

該ＳＫＥメッセージを前記無線端末から中間サービングシステムに送信するための手段と、

該ＳＫＥメッセージを該中間サービングシステムから前記ホームシステムに送信するための手段と、を具備し、

該中間サービングシステム内の該無線端末の次の認証における認証キーとして該セッションキーの第１の部分を使用するための手段と、

次の制御信号送信における暗号化キーとして該セッションキーの第２の部分を使用するための手段とをさらに具備する無線端末。

【請求項１２】

該ユーザ識別子を送信する前にそれを暗号化するための手段をさらに具備する、請求項１１の端末。

【請求項１３】

該ユーザ識別子及び該ＳＫＥメッセージを送信する前に通信チャネルを開くための手段をさらに具備する、請求項１１の端末。

【請求項１４】

下記を具備する、請求項１１の端末：

ａ）該公開／秘密キーペアはディッフィーヘルマン公開／秘密キーペアを具備する；及び

ｂ）該ＳＫＥメッセージはディッフィーヘルマン暗号化キー交換（ＤＨ－ＥＫＥ）メッセージを具備する。

【請求項１５】

下記を具備する請求項１１の端末：

ａ）該パスワードを使用して、該無線端末の公開キーを暗号化するために構成された該端末の一部分が次を具備する：

ｉ）該無線端末の公開キーを第１のランダム数で最初に連結し、それにより第１の連結された数を形成するための手段；及び

ii）該第１の連結された数を暗号化するために該パスワードを使用するための手段；及び

ｂ）該パスワードを使用して、該ホームシステムの公開キーを暗号化するために構成された該端末の一部分は次を具備する：

ｉ）該ホームシステムの公開キーを第２のランダム数で最初に連結し、それにより第２の連結された数を形成するための手段；及び

ii）該パスワードを使用して、該第２の連結された数を暗号化するための手段。

【請求項１６】

公開／秘密キーペアを発生する手段と、

ユーザ識別子及び暗号化された公開キーを無線端末から受信する手段と、

ユーザ識別子を使用して、パスワードを決定する手段と、

該パスワードを使用して、安全キー交換（ＳＫＥ）プロトコルに従って該ホームシステムの公開キーを暗号化し、それによりＳＫＥメッセージを形成する手段と、

該ＳＫＥメッセージを送信する手段と、

該パスワードを使用して、該無線端末の公開キーを解読する手段と、

該ホームシステムの秘密キー及び該無線端末の公開キーを使用して、セッションキーを形成する手段と、

該セッションキーを使用して、該ホームシステムから該無線端末にバーチャルユーザ識別モジュール（ＶＵＩＭ）の全部または一部をダウンロードする手段と、を具備し、

前記ＳＫＥメッセージを送信するための手段は、

該ＳＫＥメッセージを前記ホームシステムから前記中間サービングシステムに送信するための手段と、

該第２のＳＫＥメッセージを該中間サービングシステムから前記無線端末に送信するための手段と、を具備し、

該中間サービングシステム内の該無線端末の次の認証における認証キーとして該セッションキーの第１の部分を使用するための手段と、

次の制御信号送信における暗号化キーとして該セッションキーの第２の部分を使用するための手段とをさらに具備するホームシステム。

【請求項１７】

該ユーザ識別子を受信する前に通信チャネルを開くための手段をさらに具備する、請求項１６のシステム。

【請求項１８】

下記を具備する、請求項１６のシステム：

ａ）該公開／秘密キーペアがディッフィー－ヘルマン公開／秘密キーペアを具備する；及び

ｂ）該ＳＫＥメッセージがディッフィー－ヘルマン暗号化キー交換（ＤＨ－ＥＫＥ）メッセージを具備する。

【請求項１９】

下記を具備する、請求項１６のシステム：

ａ）該パスワードを使用して、該無線端末の公開キーを暗号化するために構成された該端末の一部分が次を具備する：

ｉ）該無線端末の公開キーを第１のランダム数で最初に連結し、それにより第１の認証された数を形成するための手段；及び

ii）該パスワードを使用して、該第１の連結された数を暗号化するための手段；及び

ｂ）該パスワードを使用して、該ホームシステムの公開キーを暗号化するために構成された該端末の一部分が次を具備する：

ｉ）該ホームシステムの公開キーを第２のランダム数で最初に連結し、それにより第２の連結された数を形成するための手段；及び

ii）該パスワードを使用して、該第２の連結された数を暗号化するための手段。

【請求項２０】

請求項１の方法を実施する無線端末であって、前記無線端末は、初期の準備及び／または移動可能な申込みを安全に及び自動的に大気中で行うように構成されている無線端末。

【請求項２１】

請求項１の方法を実施するホームシステムであって、前記ホームシステムは、無線端末の初期の準備及び／または移動可能な申込みを安全に及び自動的に大気中で行うように構成されているホームシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は無線音声及びデータシステムに関し、そして特に加入者が彼の申し込み(subscription)を１つの無線端末から他に転送できるようにすることに関する。このように本発明は申し込み移動可能性(subscription portability)、時には個人移動性(personal mobility) とも言われる、を提供する。

【０００２】

【従来の技術】

無線端末（携帯電話，ラップトップ・コンピュータ等）は、その端末が、無線と有線の両方の、他の端末と通信するサービスを使用し得るようにするためには、、そのユーザーが無線通信サービスに加入することなしに、そのように使用されることはできない。これはサービスプロバイダが登録することを要求し、そして端末、すなわちそれを無線サービスにアクセスさせる識別と保護情報とを有する端末、をサービスしプログラムする資格がある(entitled)ものとして認める準備を順に要求する。

【０００３】

無線サービス工業では術語“登録(registration)”はいくつかの意味を持つ。ここでは術語“登録”は端末のユーザのアイデンティティ(identity)を確立するため及び無線サービスへのアクセスを許すために必要とされる情報の交換(exchange)を意味するであろう。

【０００４】

この登録は２つの事態において要求されるかもしれない。第１に、端末が初めに(originally)購入される時で、それは誰にも登録されない。この事態は初期準備(initial provisioning)として引用される。第２に、加入者が再登録、すなわち彼の申込みを１つの無線端末から他へ転送することを選ぶことができる。この再登録は、例えば、彼の携帯電話から彼のラップトップ・コンピュータへのもの、または彼の正規の携帯電話から彼が遠隔の都市への旅行中にちょうど借りた携帯電話へのものであるかもしれない。この再登録は予約可能な申込みとして引用される。

【０００５】

初期のアナログの進歩した移動電話システム（ＡＭＰＳ）では、準備は端末の分布サイトで熟練者により手動で行われる。これらのある従業員は、典型的には地上有線電話を通して、サービスプロバイダに端末を手動で登録する。従業員はサービスプロバイダが彼または彼女に使用可能とした秘密情報を使用して、キーパッドを介して端末に情報を入力(enter)し、そして申込み情報を端末内に永久に保存する。この取決め(arrangement) は、販売人が各小売店に広く訓練された従業員を持たねばならないので高価である。さらに、秘密情報をこれらの従業員が容易に使用可能であるので、過程が安全ではない。

【０００６】

初期の準備と移植可能な申込みとの両者を扱うための１つの代わりの手段は、ユーザ識別子モジュール(a user identification module)（ＵＩＭ）として知られる別々の取り外し可能な装置をユーザに供給することである。サービスプロバイダはＵＩＭをユーザに配布する前にそれにアイデンティティ及び安全情報を準備する。ユーザが端末にＵＩＭを挿入すると、端末はＵＩＭから必要なアイデンティティ情報を読み、それによりユーザの申込みのアイデンティティを獲得する。この手段は移動体用グローバルシステム（ＧＳＭ）において一般的である。ＵＩＭの挿入の後に端末を登録することは大気中送信工程であり、そしてモジュール，（独特の識別番号を有する）サービスプロバイダによって運用される基地局，及び（独特の電子連続番号(Electronic Serial Number)、すなわちＥＳＮを有する）無線端末自身の間の情報の３通りの移転(three-way transfer)を含む。

【０００７】

この第１の代わりの手段はまだ完全には満足されない。それはモジュールと無線端末との間の電子インターフェイスを必要とし、そしてこのインターフェイスは端末の費用を増す。さらに、インターフェイスはＵＩＭが着脱される時汚染を招き、必然的に繰り返し使用で信頼性を失うかもしれない。

【０００８】

第２の代わりの手段は初期準備を扱うが、しかし移動可能な申込みを扱わない。この第２の手段は、加入者が最初に新しい電話を購入するとき、ユーザはユーザのクレジットを決定することができ、そしてそれから大気中送信メッセージを使用して端末内に必要な申込み情報をプログラムすることができる顧客サービス代理人(representative)に到達するために特殊番号をダイヤルする。

【０００９】

この第２の代わりの手段は端末内にいかなる特殊インターフェイスも必要としないＵＩＭ手段を超える改良である。しかしながら、この第２の手段もまた、サービスプロバイダが大気中送信プログラミング装置を運用するために顧客サービスセンタに高度に熟練した人員をなお持たねばならないので、完全には満足されない。顧客サービス工程の高価な性質は、友人が彼に１～２日間貸した電話を加入者が再登録するのを妨げる。

【００１０】

本発明の目的は、初期の準備のための方法を供給することであり、そして準備と登録工程とを完了するために熟練した人員を必要としない、またはユーザが端末に物理的に挿入しなければならない取り外しのきく品目も必要としない移動可能な申込みの方法を供給することである。

【００１１】

ここに記述された手順は、加入者が彼または彼女の携帯無線申込み識別子，またはユーザ識別子(use identification)（従来型では、彼の国際移動ユーザ識別子，すなわちＩＭＵＩ）及びパスワード（従来型では、彼の個人識別番号，すなわちＰＩＮ）を無線端末に入力するのみを要求する。パスワードは、キーパッド内で番号をキーイングする(keying)とか、マイクロフォンに（適当な音声認識技術付きの）フレーズを言うとか、あるいは何か他の便利な方法のような、何か便利な方法で端末に記入されてもよい。無線端末はそれから大気中送信信号を使用してサービスプロバイダと連絡をとって必要な申込み情報を得ることができ、そしてサービスプロバイダはその後でこの無線端末をこの加入者に登録されているものとして認識するので、それ自身を自動的に再プログラム(reprogram) し－サービスプロバイダを再プログラムする。平均的加入者は暴力攻撃(brute-force attack)を妨げるために十分に長い（１２ディジット以上の）安全コードを記憶することができないので、パスワードはかなり短く－複数の銀行カードＰＩＮにおけるように、典型的には４乃至６ディジット－でなければならない。

【００１２】

パスワードは登録手順の間危険(compromise)から保護されねばならず、その逆に申込み情報はユーザ識別子及びパスワードを手に入れる不正なユーザによるコピー作成(cloning)にさらされるであろうことは明らかである。ベロヴィン(Bellovin)及びメリット(Merritt)の作業のような暗号作成法の最近の進歩は、下に引用したように、端末と無線ネットワークとの両者がパスワードを示さずに正しいパスワードを知ることを安全に確かめる技術を準備する。これらの技術はまた初期のパスワード確定に続いて交換された申込み情報の暗号化において使用され得る暗号化キーを確立するための手段を準備する。これらの技術の存在は、複数の取り外し可能なＵＩＭのためにも顧客サービスの調停(intervention)のためにも必要とせずに初期の準備及び移動可能な申込みのための登録をサポートすることを可能とする。

【００１３】

【課題を解決するための手段】

出願人は１つの無線端末から他へ本当に移動可能であり、そして短くて安全なパスワードを使用する申込み方法及び装置を開発した。

【００１４】
加入者が彼の申込み(subscription)に端末を登録したいときはいつでも、彼は彼のユーザ識別子（従来型では、彼の国際移動ユーザ識別子，すなわちＩＭＵＩ）及び彼のパスワード（従来型では、彼の個人識別番号，すなわちＰＩＮ）を無線端末に記入する。端末は公開／秘密キーペアを発生してそれを蓄積する。このキーペアはむしろディッフィーヘルマン（Ｄ－Ｈ）キーペア(key pair)である。それは公開キーをランダム(random)数で随意に連結し(concatenates)、そして（随意に連結された）番号をパスワードで暗号化する。いすれかの便利な安全キー交換(secure key exchange)（ＳＫＥ）法が使用されてよい。いくつかの適当なＳＫＥ法が下記に記述されている。トーマス・ウー（Ｔｈｏｍａｓ Ｗｕ），“安全な遠隔パスワード・プロトコル（Ｔｈｅ Ｓｅｃｕｒｅ Ｒｅｍｏｔｅ Ｐａｓｓｗｏｒｄ Ｐｒｏｔｏｃｏｌ）”議事録１９９８インターネット・ソサイティ・ネットワーク・アンド・ディストリビューテッド・システム・セキュリティ・シンポジューム，サンディエゴ，カリフォルニア，１９９８年3月，ｐｐ．９７－１１１，ｈｔｔｐ：／／ｊａｆａｒ．ｓｔａｎｆｏｒｄ．ｅｄｕ／ｓｒｐ／ｎｄｓｓ．ｈｔｍｌに、及びデーヴィッド・ピー・ジャブロン（Ｄａｖｉｄ Ｐ． Ｊａｂｌｏｎ）“強力パスワード－単なる認証されたキー交換（Ｓｔｒｏｎｇ Ｐａｓｓｗｏｒｄ－Ｏｎｌｙ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ）”ウエストボロのインテグリティ・サイエンス社，マサチューセッツ，ＵＳＡ．１９９７年3月2日，ｈｔｔｐ：／／ｗｏｒｌｄ．ｓｔｄ．ｃｏｍ／～ｄｐｊ／ｓｐｅｋｅ９７．ｈｔｍｌ，その開示は引用されてこの中に組み込まれる。ベロヴィン及びメリットのディッフィーヘルマン暗号化キー交換（ＤＨ－ＥＫＥ）法は特に適当であり、そして本発明の残りの説明はＤＨ－ＥＫＥを参照してなされる。ＩＥＥＥコンピュータ・ソサイエティ・シンポジューム・オン・リサーチ・イン・セキュリティ・アンド・プライバシー議事録のｐｐ７２－８４，１９９２年5月における、スティーヴン・Ｍ・ベロヴィン（Ｓｔｅｖｅｎ Ｍ．Ｂｅｌｌｏｖｉｎ）及びマイケル・メリット（Ｍｉｃｈａｅｌ Ｍｅｒｒｉｔｔ），“暗号化されたキー交換：辞書攻撃に備えて安全にするパスワード基準プロトコル（Ｅｎｃｒｙｐｔｅｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ：Ｐａｓｓｗｏｒｄ－Ｂａｓｅｄ Ｐｒｏｔｏｃｏｌｓ Ｓｅｃｕｒｅ Ａｇａｉｎｓｔ Ｄｉｃｔｉｏｎａｒｙ Ａｔｔａｃｋｓ）”を見よ、これの開示は引用されてこの中に組み込まれる。楕円カーブまたは指数群のいずれもこの方法とともに使用され得る。結果としての暗号化されたメッセージはＤＨ－ＥＫＥメッセージと呼ばれる。

【００１５】
端末はそれからローカル・サービング・システムと無線連絡をとって登録を頼む。このサービングシステムは加入者のホームシステムであってもよいが、しばしばそうではない。いずれにしても、端末及びホームシステムはそれぞれ他のアイデンティティについて、中間サービスシステムが無いか、１システムがあるのか、または数システムまでもがあるのかを確かめねばならない。この説明の残りは１中間システムを仮定するが、１つも扱わないかまたは数システムを扱うことに容易に変更される。すなわち、（たとえ）それらが通り過ぎねばならないものであっても、いかに多くの中間システムがあるかには無関係に、端末及びホームシステムは常にメッセージのソース及び目的先（またはその逆）になるであろう。

【００１６】
端末は、全ユーザ識別子かホームシステム(home system)を識別するのに必要十分なユーザ識別子かのいずれかを述べることにより、何が加入者のホームシステムであるかをサービング(serving)システムに知らせる。それはまたＤＨ－ＥＫＥメッセージも述べる。好ましくは、誰が登録を頼んでいるかの詳細(specifics) が明文(in the clear)で送られないので、サービングシステムは最初にそれのＤ－Ｈ公開キーを端末に供給する。また好ましくは、サービングシステムは登録処理を容易にするために端末とのチャネルを開く。

【００１７】
サービングシステムはパスワードでそれを暗号化するホームシステムにＤＨ－ＥＫＥメッセージを送る。パスワードはホームシステムと加入者にのみ知らされる。ホームシステム

はそれによって加入者の公開キーを回復する。ホームシステムはそれ自身のＤ－Ｈ公開／秘密キーペアを発生してそれを蓄積する。それはそれから新しく発生された公開キーをランダム数で連結し、その連結された数をＤＨ－ＥＫＥを使用してパスワードで暗号化し、そしてこの新しく発生されたＤＨ－ＥＫＥメッセージを端末に返送する。端末はパスワードでそれを解読してホームシステムの公開キーを回復する。

【００１８】

端末及びホームシステムは今それぞれそれ自身の秘密キーと他の公開キーとを入手しており、その両方はパスワードよりもはるかに大きい。このようにしてそれぞれは従前の方法を使用して共通のセッションキー(session key) を発生することができる。さらにそれぞれは端末内にバーチャル(virtual)ユーザ識別モジュール（ＶＵＩＭ）をダウンロードするために、すなわち、端末に挿入されている物理的ＵＩＭ（ＰＵＩＭ）から別の方法で得られるいくつかのまたはすべての情報を、大気中送信で、端末に供給するために、セッションキー(session key)を安全に使用することができる。

【００１９】

登録は今、あたかもＰＵＩＭが使用されたかのように、従前の様式で続けることができる。代案として、登録はダウンロード手順内に含まれてもよい。ＶＵＩＭ付きの端末は、ＰＵＩＭ付きの端末が後々まで取得しない何かを、すなわち（そして秘密のセッションキーを共有した）ホームシステムへの通信リンクを、すでに持っているので、これは可能である。

【００２０】

この方法の長所は公開キーが仮のものであり、そしてそれぞれ次の登録において取り替えられ得ることである。さらに各公開キーは本質的にランダム数であり、試みた暗号解読が成功したか否かの表示を一切準備しない。したがってオフラインの辞書攻撃(dictionary attack) は失敗する。辞書攻撃者が回復する唯一のものは可能な公開キーの収集であり、その誰も他のもののいずれかからそれを区別する何ものをも持たない。このようにパスワードの正しい推量(guess) を不正な推量から区別する何ものもない。従ってあとに続くはずの(follow-on) オンライン攻撃はパスワードの完全な辞書をなお使用するに違いなく、そしてそれゆえに失敗するであろう。

【００２１】

この長所はまた暗号キー自体(per se)としてよりもむしろ、キー交換手順における秘密キー(private key)として使用されているパスワードとして見られてよい。手順が暗号化キー交換よりもむしろ安全キー交換と呼ばれるのはこの理由のためである。端末及びホームシステムはパスワードもセッションキーも暗号化形式に交換する必要はない。重要なことは、端末がパスワードを知っておりそして共通のセッションキーを持っていることをホームシステムは保証されることである。また、端末がホームシステムにそれのアイデンティティを証明して(demonstrating) いる間、パスワードが盗聴者によって発見されないことも重要である。もしもパスワードが、暗号化形式にあっても、メッセージ内に含まれないならば、そのときは危険にさらされることはもっと難かしくなる。

【００２２】

【発明の実施の形態】

図１はＤＨ－ＥＫＥメッセージの交換１００を示す。ユーザ１０２はユーザ識別子及びパスワードを無線端末１０４に記入する。端末１０４はディッフィー－ヘルマン（Ｄ－Ｈ）秘密及び公開キーのペアを発生し、そしてそれらを蓄積する。随意に、端末１０４及びサービングシステム１０６の基地局はユーザ識別子を妨害から保護するため局部セッション暗号化キーＳＥＳＳ１０８を確立するために別の手順を実行する。端末１０４は暗号化の前にランダム数で随意に連結された、Ｄ－Ｈ公開キーを暗号化するためにパスワードを使用し、それから（随意に局部セッションキーの下で暗号化された）ユーザ識別子及び暗号化された公開キー、すなわち、第１のＤＨ－ＥＫＥメッセージ１１０を登録依頼中のサービングシステム１０６の基地局に送信する。この依頼はダウンロード手順を効率的に完了するために供された(dedicated) チャネル割り当てに終わる。

【００２３】
サービングシステム１０６は申込み登録を依頼してホームシステム１１２と連絡をとる。ホームシステム１１２は申込み記録内のパスワードを使用して無線端末の公開キー(public key)を解読する。ホームシステムはそれから、端末の公開キーとホームシステムの秘密キーとを使用して仮のセッションキーが得られる、秘密及び公開Ｄ－Ｈキーを創造する。ホームシステムはそれから、暗号化の前にランダム数を随意に連結し、申込み記録内に蓄積されたパスワードを使用して、それ自身の公開キーを暗号化し、そしてそれを第２のＤＨ－ＥＫＥメッセージ１１４の形式でサービングシステム１０６を経由して無線端末１０４に返す。無線端末１０４はホームシステムの公開キーを解読しそしてホームシステムの公開キーとそれ自身の秘密キーとを使用して、（たぶん）同じ仮のセッションキーを創造する。

【００２４】
図２はＤＨ－ＥＫＥ交換を続けなければならない認証手順２００を示す。無線端末１０４及びホームシステム１１２はそれぞれが同じキーを持つことを証明するためにこの手順を実行する。この認証は片務的(unilateral)（例えば、ホームシステム１１２が無線端末１０４を認証することだけを許す）か双務的(bilateral)かのどちらかである。双務的技術は３ステップを有する。第１に、無線端末１０４はランダム数C_Wを暗号化しそしてその暗号化された数Ｅ（C_W）２０２をホームシステム１１２に送る。第２に、ホームシステム１１２はそれ自身のランダム数C_Hを発生し、（C_W, C_H）を暗号化しそしてその暗号化された数Ｅ（C_W, C_H）２０４を無線端末１０４に送る。第３に、無線端末１０４はC_Hを暗号化しそしてその暗号化された数Ｅ（C_H）２０６をホームシステム１１２に送る。片務的手順は、例えば、第１のステップを省略し、そして第２ステップにおけるC_Wを第２の任意数により置き換える。

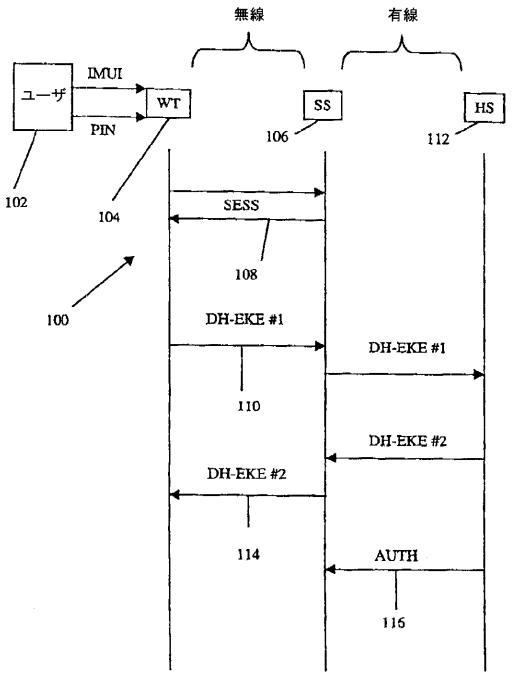
【００２５】
公開キーはパスワードによって暗号化され、そして認証はインターロック法(interlocked manner)において送られている３つの異なるものから成る。従ってマン・イン・ザ・ミドル(man-in-the-middle) 攻撃者はキーの不正受領を引き起こすことができず、そして分離対数(discrete logarithm)または楕円曲線群を壊さずに相互キーを知ることはできない。そのような破損はもしグループサイズが大きければ、一般に実行不可能(infeasible)と考えられる。

【００２６】
もしもホームシステム１１２が無線端末１０４のセッションキーを確かめるならば、それは申込み情報－すなわち、バーチャルＵＩＭ（ＶＵＩＭ）の全部または部分－をサービングシステム１０６に、大気中送信のためには暗号化形式及びサービングシステムによる使用のためには非暗号化形式の両形式で転送するであろう。セッションキー－または、少なくともそれの第１の部分－はサービングシステム１０６内の端末１０４の次の認証のための認証キーＡＵＴＨとしても役に立つ。これは、認証キーが各登録で創造され、従って登録から登録へ任意に変化するであろう、現行のセルラ認証手順を超える利点を有する。典型的にＤ－Ｈ交換は、認証のために必要とされるよりも大きい５１２ビットの出力を生ずる。結果として、セッションキーの残り、すなわち、それの第２の部分は次の制御信号送信のための従前の暗号化キーとして役に立ち得る。

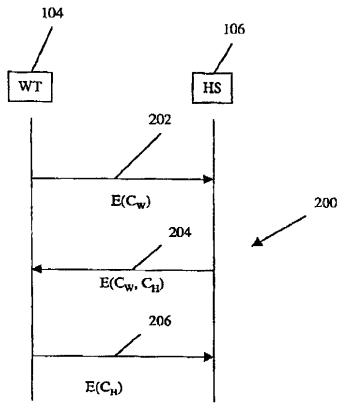
【００２７】
サービングシステム１０６は暗号化された申込みデータ－ＶＵＩＭ－を端末にダウンロードし、そしてビジタ・ロケーション・レジスタ（ＶＬＲ）に登録記入をさせる。ユーザは今電話を掛ける準備ができている。次のシステムアクセスのために、ユーザは既存のセルラ基準に記述されているように仮の移動ユーザ識別子（ＴＭＵＩ）を割り当てられることができる。呼ごとの暗号キーの発生は既存のセルラ基準に記述されている手順を使用している認証キーを使用して実行されることができる。言い換えれば、既存のセルラ基準におけるエアリンク安全手順は、ここに記述された方法を使用して認証キーの発生後の変更無しに使用することができる。

【００２８】
私の発明は工業における活用が可能であり、そして新しい無線端末に無線申込み(subscription)を登録することが望まれる時はいつでも製造及び使用され得る。分離されそして互いにばらばらにされて、ここに示された装置及び方法の個々の要素は完全に従来型であってもよく、私の発明としてクレームするものはこれらの組み合わせである。
【００２９】
私は装置及び方法の種々のモードを記述したが、私の発明の真の精神及び範囲はそれには制限されず、しかし次の請求範囲及びそれらと同等のも
のによってのみ制限され、そして私はそのような私の発明をクレームする。
【図面の簡単な説明】
【図１】　ＤＨ－ＥＫＥメッセージの交換を示す。
【図２】　認証手順を示す。
【符号の説明】
１００…ＤＨ－ＥＫＥメッセージの交換、１０４…無線端末、１０６…サービングシステム、１１２…ホームシステム、１０８…局部セッション暗号化キー、１１０…ディッフィー－ヘルマン暗号化キー交換メッセージ、１１４…ディッフィー－ヘルマン暗号化キー交換メッセージ、２００…認証手順、２０２…暗号化された数Ｅ、２０４…暗号化された数Ｅ、２０６…暗号化された数Ｅ

【図１】



【図２】



フロントページの続き

(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、デル・モンテ・アベニュー ４５０２

審査官 青木 重徳

(56)参考文献 特開平０８－２７４７６９（ＪＰ，Ａ）
特表平１１－５０１１７９（ＪＰ，Ａ）
特開昭５９－１５４８３７（ＪＰ，Ａ）
特開平０８－３２０８４７（ＪＰ，Ａ）
特開平０６－３４３１０８（ＪＰ，Ａ）
特開平０４－３４７９４９（ＪＰ，Ａ）
特開昭６０－２２３２４８（ＪＰ，Ａ）
David P. Jablon, “Strong Password-Only Authenticated Key Exchange”, ACM SIGCOMM Computer Communication Review, [online], １９９６年 9月２５日, Volume 26, Issue 5, p.5-26, [retrieved on 2010-03-11]. Retrieved from the Internet, ＵＲＬ, http://portal.acm.org/citation.cfm?id=242897
Steven M. Bellovin, Michael Merritt, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”, IEEE Computer Society Symposium on Research in Security and Privacy, [online], １９９２年 5月, p.72-84, [retrieved on 2010-03-11]. Retrieved from the Internet, ＵＲＬ, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=213269

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/08
H04L 9/32