(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3609436号
(P3609436)
(45)発行日　平成17年1月12日(2005.1.12)　(24)登録日　平成16年10月22日(2004.10.22)

(51)Int.Cl.[7]	F I
H04M 11/00	H04M 11/00 302
H04M 1/667	H04M 1/667
H04M 3/42	H04M 3/42 E

請求項の数 7　(全 14 頁)

(21)出願番号　特願平5-77290
(22)出願日　平成5年4月5日(1993.4.5)
(65)公開番号　特開平6-46162
(43)公開日　平成6年2月18日(1994.2.18)
審査請求日　平成11年8月27日(1999.8.27)
(31)優先権主張番号　863901
(32)優先日　平成4年4月6日(1992.4.6)
(33)優先権主張国　米国(US)

(73)特許権者　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ＆Ｔ　ＣＯＲＰ.
アメリカ合衆国　１００１３－２４１２
ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　３２
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100077919
弁理士　井上　義雄
(74)代理人　100085176
弁理士　加藤　伸晃

最終頁に続く

(54)【発明の名称】電話回線を介して使用する汎用認証装置

(57)【特許請求の範囲】
【請求項１】
認証装置であって、
認証情報を表す可聴信号を音声電話回線を介して自動的に送信する手段からなり、該回線は電話網を介して認証システムへ接続されており、そして該送信する手段は、該認証装置の利用者が電話機のスピーカを聞くことができる状態を維持しつつ、該認証装置の利用者が電話機のマイクロフォンに該送信する手段を保持することによって、該認証情報を表す可聴信号を該認証システムへ送信するものであり、更に、
該送信する手段に結合されている、キー入力された個人識別番号とは無関係に数字を発生する手段からなり、該数字が、時間的に変化する数量と該認証装置に固有のキーとから導出され、該数量が、該認証装置と該認証システムの内部に独立的に維持されており、該数字は、該認証装置の該利用者の同一性を認証し、そして該数字は、該認証装置を識別するデータからなるが、キー入力された個人識別データに基づくいかなるデータをも含んでいないものであり、更に、
個人識別番号を記録する手段と、
個人識別番号の入力のためのキーパッドと、
記録された個人識別番号と入力された個人識別番号との整合に応動して該認証装置を始動させる手段とからなることを特徴とする認証装置。
【請求項２】
請求項１に記載の認証装置であって、該電話機の該スピーカで受信した入力要求信号に応

動して該利用者が操作する、該認証装置の状態を変更させる制御キーをさらに備えることを特徴とする認証装置。
【請求項３】
請求項２に記載の認証装置において、該数字の送信を始めるために該制御キーが用いられることを特徴とする認証装置。
【請求項４】
請求項１に記載の認証装置であって、該認証装置を不動作にするキーをさらに備えることを特徴とする認証装置。
【請求項５】
請求項１に記載の認証装置であって、該認証装置の始動または利用後、所定の時間経過の後に、該認証装置を不動作とする計時手段をさらに備えることを特徴とする認証装置。
【請求項６】
請求項１に記載の認証装置であって、日及び時間を維持する時計手段をさらに備え、該独立的に維持される数量は日及び時間であることを特徴とする認証装置。
【請求項７】
請求項１に記載の認証装置において、該認証装置は、実質的にクレジットカードの大きさであり、付属物はないことを特徴とする認証装置。
【発明の詳細な説明】
【０００１】
【技術分野】
本発明は通信システムユーザの認証装置に関する。
【０００２】
問題
電話のコーリングカードの詐欺、会社のＰＢＸの詐欺による使用によって、現在顧客は１年１０億ドルを越える損害を受けている。典型的な構成においては、ＰＢＸへの発呼ではＰＢＸにアクセスするために８００番の番号を使う。その正当性は、起呼者に対して多桁のアクセスコードをダイヤルするように要求することによって確認され、もし正当であれば、起呼者に対してＰＢＸを通して第２ダイヤル音を与えることによってアクセスを許す。起呼者は次にＰＢＸ内の通常の利用者に対して拒否されない範囲で任意の出接続を設定できる。明らかに、８００番の番号とアクセスコードを知っている人ならだれでもＰＢＸに課金される呼を発することができる。より一般的には、現在のコーリングカードの装置は盗まれたカードの使用、あるいはコーリングカード番号を音声タップを通して盗聴したり、コーリングカード番号を目で見たりすることによって、広範な詐欺の対象になっている。
【０００３】
コンピュータのハッカーもそのコンピュータを使用して企業のＰＢＸにアクセスして、試行錯誤して正しいアクセスコードを見付ける活動を行なう。彼等はそのコードをＰＢＸの電話番号と共に再販者に売り付け、それがまた多数の詐欺ユーザに売り込む。これによって詐欺の範囲は大幅に広がる。より一般的には、通常の電話回線のユーザに対して、彼等に電話あるいは他のサービスの不当な請求が行なわれないようにするための安価で便利な方法が存在しないという問題がある。
【０００４】
解決
上述の問題はコーリングカードの使用を認証するために企業のＰＢＸによって使用するように任意の電話回線を通して使用できる本発明の原理に従った汎用認証（ＵＡ）装置を利用して、従来技術に対する進歩が達成され、解決される。この認証装置はそのユーザを認証する固有の信号を提供する。認証装置はコーリングカードの代りに使用されて質問応答型の認証方式を可能にし、問合わせのデータとそのデータに対する応答を生ずるのに使用されるハードウエアを装備している。いずれの場合にも、装置によって送られる認証メッセージ（応答）は連続した認証要求について異なっている。これはオーディオインタフェ

ース（トーンの発生と受話）を含み、これによって装置はトーン信号を使って電話機と直接交信でき、ユーザがコードを手でキーイングする必要がなくなる。

【０００５】

有利なことに、ＵＡは特別の電話機（移動電話、スマートカード電話その他）を必要としない。この装置はまた種々の他のサービス（バンキング等）用の電話回線を通した認証およびコンピュータシステムに対するリモート・ログインの認証を助けるのに使うことができる。このような装置を提供するための追加コストは極めて小さい（資格を持つユーザ当り数ドルの一時的コスト）。ユーザに関する限り、その装置の使い方はキャッシュディスペンサの使い方より複雑ではない。

【０００６】

【詳細な記述】

カード大の装置に問合せを応答に変換する関数を実現するための計算用ハードウエア、入力を与えるためのキーパッド、ＬＣＤディスプレイおよび加入者線を通して交換機に対して電話機から送信できるトーンの形式で入力を受信し、出力を提供するオーディオインタフェースが装備されている。問合せ（第１の数）を応答（第２の数の一部）に変換する関数を実現する目的は、時間的に変化する問合せに基づいて時間的に変化する応答を生ずることであり、これによって、あるときに問合せ－応答の組合せを盗んでもこれを後で使うことはできなくなる。これはまた、現在コーリングカードに存在する磁気バーを持っており、従ってコーリングカード用の機能を持つ特殊電話機を利用でき、また任意の他の電話機も利用できる。ランダムに選択した２人の異なるユーザに対して２つの異なる装置を提供しても、確実に応答を発生するのに異なる装置を使用できる。この装置はＡＴ＆Ｔのスマートカード（登録商標）や特殊電話機のみで使用できる他のスマートカードとは大幅に異なっている（これについては後に詳述する。）。時間的に変化する認証メッセージは異なる３種の方法で発生される。第１の方法はチャレンジ応答方式であり、これでは遠端のシステムで認証装置に対して乱数を与え、認証装置は適切な応答を計算して、システムに対して返送する。他の方法は関数に対する入力として時刻を与え、遠端のシステムに対して関数の出力と使用した時刻を送信する方法である。第３の方法は使用するごとに増分される計数値のような単調増加あるいは減少する関数を使用する。第１の方法について、次の節で詳述する。第２と第３の方法については後に簡単に説明する。

【０００７】

装置の使用法

企業のＰＢＸの認証にこの装置を使用する手順は次のとおりである。各々の合法的な利用者には個人識別番号（ＰＩＮ）が割当てられており、これはまた彼あるいは彼女の持つ特定の装置に関連する。認証を求める前に、ユーザはそのＰＩＮを汎用認証器（ＵＡ）と呼ぶ装置に与える。もしＰＩＮが正しければ、ＵＡは起動されて使用できるようになる。次にユーザは電話番号をダイヤルし、（もし必要なら、番号はＵＡに印刷しておいてよい。）認証を求める（これは現在企業のＰＢＸで行なっている。）。音声による応答でユーザに対して起動したＵＡを発呼電話機の受話器の近くに持ってゆき、受話器から入来トーンを受信するようにすることを指示する。次に認証システムは乱数を表わすトーンの集合を送信し、これはＵＡのオーディオインタフェースによって受信される。これが問合せ番号である。次にＵＡは問合せ番号に対する適切な応答として出力番号を発生し、ユーザに対してメッセージを与えて、ＵＡを送話機にあてて、伝送を開始するキーを押すように指示する。ＵＡはそれが生じた出力を表わすトーンの集合を送信する。システムは応答と内部で発生した出力を比較し、もし一致すれば、要求を認証する。この動作シナリオの全体を図１に示す。

【０００８】

ユーザにはオプションがある。現在でも利用できる認証装置のオプションはＵＡの番号を手でキーインし、応答をシステムに手でダイヤルして返送する方法である。この場合にはシステムからの音声による応答はユーザに対してＵＡに与えるべき乱数を指示する。ユーザによってこれがＵＡにキーインされると、ＵＡはそのディスプレイに対応する出力番号

を生ずる。これは（電話の２重音周波数（ＤＴＭＦ）があればそれを使って、あるいは音声認識システムがあれば音声を使って）ユーザによって与えられ、認証を求める。この代りに望ましくはユーザはＵＡに対して出力番号を表わすトーンを送信するように要求する。

【０００９】

この装置の高レベルの状態図を図２に示す。初期には、ＰＩＮの入力の後、装置はレディ（待機）状態になる。レディ状態では、特別の受信／送信キー（図３に示す縁ノッチ）をクリックすることによって装置は受信状態になる。受信状態で、装置は音声入力あるいはキー入力を受信する。８桁の入力の受信を完了すると、装置は計算状態になって応答を計算する。計算が完了すれば、装置は送信準備状態になり計算の完了を示す発光ダイオード（ＬＥＤ）をフラッシュする。送信レディ状態で、受信／送信キーをもう一度クリックすると、計算された応答に対応する音声出力を生じ、装置はレディ状態に戻る。装置はリセットバー（図３に示す）を使ってどの状態からでもリセット状態にすることができる。

【００１０】

外観と内部構造

図３はＵＡの外観を示している。装置の外観は通常の電話機を使って通信できるようにするためのオーディオインタフェースを有すること以外はスマートカードに似ている。キーパッドによってＰＩＮの入力と入力乱数の手動による入力（もし利用者が選択すれば）ができるようになる。ＬＣＤは入力された番号をディスプレイする。応答を計算したあとで、応答番号が表示される。計算が完了したことを表示するためにはＬＥＤがフラッシュする。縁の切込みにあるキーはオーディオ受信／送信を動作するもので、ユーザがＵＡを送話器あるいは受話器に密着させやすいようになっている。

【００１１】

装置についた磁気バーによってこれをコーリングカードリーダの付いた電話機でも利用できるようになる。この場合には、符号化された識別情報だけが送信され、認証の安全性は低下する。

【００１２】

装置の内部構造を図４に図示する。キーパッドからの入力は入力番号を入れるのにマニュアルモードを選ぶか、ＰＩＮを入れるときに行なわれる。操作によってはキーパッドからの入力はＰＩＮ入力レジスタあるいはＭＵＸのいずれかにゲートされる。ＰＩＮ入力レジスタの内容は記憶されたＰＩＮレジスタの内容と比較され、一致する場合には以降の動作のためにマイクロプロセッサの計算／テーブルルックアップユニットが（応答の生成のために）動作される。ユーザが（ノッチのキーを使って）トーン検出を動作したときには（受信器からの）受信されたトーンはビットに変換されてＭＵＸに送られる。ＭＵＸは入力を自動モード（音声インタフェースを通す）にするかあるいはマニュアルモード（キーパッドを通す）にするかを選択できるようにする。ＭＵＸによって選択された入力は入力シフトレジスタに入れられ、次に計算／テーブルルックアップ装置に与えられる。応答の計算が完了すると、応答は出力表示レジスタと出力シフトレジスタの両方に与えられる。出力表示レジスタによって応答出力をＬＣＤに表示できる。出力表示レジスタの内容はユーザがそれを動作したときに（縁のノッチのキーを２度目にクリックする）トーン発生器に与えられ、トーン発生器は出力を送信器で送信できるトーンに変換する。

【００１３】

図１は認証のシナリオのブロック図である。ユーザはＰＩＮを汎用認証器に与える（動作ブロック１０１）。これによって汎用認証器が使えるようになる。次にユーザは認証サービス用の電話番号を呼び出し、認証システムによって発生された一般的な乱数である入力番号を受信するために、ＵＡを電話機の受話器にあてる。認証システムに対して呼が設定され（矢印１０５）一般に交換機あるいはＰＢＸである認証システムはトーン信号によってＵＡに乱数を与える。このトーンはＵＡに対して送信され（矢印１０９）、電話の受話器を通して受信される。ＵＡは次に応答を計算し、加入者の送信器を経由して応答を送信する。この応答は認証システムに送信され（矢印１１３）、これはＵＡの応答を内部で発

生された番号と比較して、もし応答が正しければ（動作ブロック１１５）、要求を許可する。認証システムは次にユーザに対して認証の可否を返送し（矢印１１７）、そのあとでユーザは電話呼を発するか他の方法で認証の許可を利用する。この汎用認証器を使用して、ＵＡにトーンを与える代りにＵＡにキーボードで入力してもよく、ユーザに対して乱数を認証システムからの音声応答を通して与えてもよい。同様に、ユーザの電話機の２重トーン多周波（ＤＴＭＦ）キーボードを通して応答をキーインすることによって認証システムに対してユーザが応答を送信してもよい。さらに代替構成においては、ＵＡそのものが入力番号を与えてもよい。この構成では、ブロック１０７と矢印１０９は使用されず、ＵＡは入力番号を受信する代りに、ブロック１０３の内部で入力番号を発生する。この場合の応答は入力番号を含む必要があり、これによって認証システムはＵＡによって使用されたのと同一の入力番号から応答番号を認証することができる。

【００１４】

図２はＵＡの状態図である。静止状態２０１では、ユーザはＰＩＮ入力２０３を与える。これによってＵＡは状態２０４となり、ここで、ＵＡはＰＩＮ入力が正しいかどうかを確認する。もしＰＩＮが正しければ（矢印２０７）、ＵＡはレディ状態（２０９）となり、レディ信号を表示する。次にユーザは認証を要求する呼を発生し、ＵＡを電話機の受話器の近くに置き、ＵＡの縁のノッチのキーをクリックする（矢印２１１）。これによってＵＡは受信状態（２１３）になり、入力数字の番号が受信されたときにこれを表示する準備ができたことになる。ＵＡはすべての入力数字が受信されるまで受信状態を保ち、これによって誤って縁のノッチキーをクリックしてもＵＡが受信状態にある間は（矢印２１５）単に無視されることになる。入力数字が受信されると（矢印２１７）、ＵＡは計算状態（２１９）に入り、応答番号を計算する。この場合も縁のノッチキーのクリックが早すぎると（矢印２１１）、ＵＡが計算状態にある間は無視される。ＵＡが応答の計算を完了した後（矢印２２３）（これはユーザに対してＬＥＤのディスプレイのフラッシュで知らされる）、ＵＡは送信レディ状態（２２５）となる。ユーザは次にＵＡを電話のハンドセットの送話器の近くにおき、縁のノッチのキーを押し（矢印２２７）、応答出力を電話接続を通して認証システムに送信する。これによってＵＡはレディ状態（２０９）に戻る。何かの理由でユーザが任意の時にレディ状態に戻って、再開したいときには、これはリセットキーを操作してＵＡをレディ状態に戻すことができる（矢印２２９、２３１、２３３、２３５）。ＵＡはタイムアウト（矢印２３７）あるいは所定の回数のＵＡの使用（矢印２３９）の内の早い方で静止状態に戻る。

【００１５】

図３は汎用認証器３０１の外観図である。これは電話接続を通して信号を受信するマイクロフォンと、電話接続を通して信号を送信するスピーカを含む音声インタフェース３０３を有する。ＵＡ内部の計算ハードウエアはＵＡの外からは見えないので破線で示してある。ＵＡはまたキーボード３０７を持ち、これは１２個のＤＴＭＦキーとＵＡをリセットするリセットバー３０９を持つ。さらにＵＡによって受信されたり、発生された番号のＬＣＤディスプレイ３１１と、ＵＡの縁のノッチのキー３１１が図示されている。磁気コードバー３１５もまたＵＡの外側に付いていてＵＡを通常のクレジットカードリーダで読むこともできる。

【００１６】

図４はＵＡの内部のブロック図である。ブロック４０１はＵＡのキーパッドに接続された出力回路を表わし、キーパッドの番号に対応するディジタル信号を発生する。ゲート４０３はモード信号４０２によって制御されて、この場合にはキーパッド３０７からの出力信号のディジタル信号をシフトレジスタ４０５に与える。このレジスタの出力はマイクロプロセッサ４０７で比較される。マイクロプロセッサ４０７は概念的にプログラムメモリ４１０、計算メカニズム、状態コントローラ４１３、ＵＡがユーザに与えられるときにプリセットされる小容量のリードオンリメモリであるＰＩＮレジスタ４０９、ＰＩＮレジスタ４０９とシフトレジスタ４０５の出力を比較する比較器４１１に分けられている。レジスタ４０９はまた、ＵＡのシーケンス識別子とＵＡの秘密キーを記憶している。比較器４１

１の出力は計算メカニズムと状態コントローラ４１３によって利用されて、ＵＡをレディ状態にするかどうかを判定する。ＬＥＤ４１５はコントローラ４１３に接続されていてユーザに表示を示す。次に認証センタに対する接続をダイヤルしたあと、トーン検出器／トーン発生器４２３をマイクロフォン４２１からの入力信号を検出する（検出動作４２２）ように検出器を動作する。検出器動作信号４２２は縁のノッチキー３１３からの入力信号４２２を受信する状態制御器４１３から来る。トーン検出器の出力は次にマルチプレクサ４２７を経由してシフトレジスタ４３１に与えられ、その出力はマイクロプロセッサ４０７の計算メカニズムと状態制御器４１３に与えられる。これはストアドプログラム４１０によって制御される。計算メカニズム４１３は次に入力乱数、秘密キーおよびシーケンス識別子を使って出力を発生する。これはＵＡのシーケンス識別子とシフトレジスタ４３１から受信された入力に対応する出力を出力表示レジスタ４３３に与え、これはＬＣＤディスプレイ３１１を動作する。出力はまた出力シフトレジスタ４３５に与えられ、これはトーン検出／トーン発生器４２３のトーン発生器部の入力となる。トーン発生器は状態コントローラ４３７からの信号によって動作され、シフトレジスタ４３５の出力に基づいてトーンを発生し、そのトーンはスピーカ４３９に与えられて認証システムに送信される。リセットバー３０９は計算メカニズムと状態コントローラ４１３、それに出力ディスプレイとシフトレジスタ４３３にリセット信号４４０を送る。

【００１７】

図５は汎用認証器の動作の全体のブロック図である。円の中の番号は順次のステップを表わし、読者がプロセスの進行を追いやすくするために図に付けてある。破線の中の２つの主要なブロックは汎用認証器３０１と認証システム５０１であり、後者は交換機あるいはＰＢＸである。プロセスはユーザが認証を要求したときに開始する。（動作ブロック５０３）。（ユーザが先に正しいＰＩＮを入れてＵＡは既にレディ状態にあるものと仮定する。）認証の要求は認証システム５０１への接続のための番号をダイヤルすることによって実行される。動作の完了は矢印５０５によって表わされる。認証システムは８桁の入力番号を発生し（ブロック５０７）、この番号はトーンによってＵＡに送信される（矢印５０９）。ＵＡはユーザが認証を要求したハンドセットの受話器の近くに保持することによってそのトーンを受信する。入力番号が次に送られ、次にＵＡのトーン検出器から記憶装置５１５に送られ（矢印５１３）、入力番号を表わす数字を記憶する（代替の構成では入力番号をユーザがキーパッド３０７を使ってキーインしてもよい。）。これらの８桁の数字は次に計算ハードウエア５１９に与えられ（矢印５１７）、これは８桁の出力を発生する。これらの８桁の出力はＵＡの８桁の識別子と組合わされ（ブロック５２３）、計算ハードウエアの８桁の出力と、シーケンス識別子の８桁の出力から成る１６桁の出力を形成する。これはブロック５２５の１６桁に記憶されトーン発生器４２３からスピーカ４３９を経由して電話接続を通して認証システム５０１に送信される。これは受信されて１６桁の応答レジスタ５３１に記憶され、これは８桁のＵＡシーケンス識別子をブロック５３３に選択して、これらの桁を計算ハードウエアに送信する（矢印５３５）。この計算ハードウエアは次に入力番号とＵＡシーケンス識別子を使用して、ＵＡの計算ハードウエア５１９によって計算された８桁の出力を計算する。計算された出力は出力レジスタ５４５に送信され（矢印５４９）、ここで、これはブロック５３１に受信されて記憶された８桁の出力と比較される（矢印５４３）。もしそれが一致すれば、認証されたことになり、不一致であれば認証が否定される。認証／否定の信号５４７はユーザに返送され、交換機あるいはＰＢＸがユーザからの以降の呼を受理するか拒否するかが決められることになる。表１はＵＡの種々の要素の部品表である。

【００１８】

【表１】

項　　目	数量	部品番号
トーン検出／発生器	1	ＳＳＩ２０Ｃ９０
マイクロプロセッサ	1	ＭＣ６８０５
直列入力並列出力シフトレジスタ（PIN入力ﾚｼﾞｽﾀ・出力ｼﾌﾄﾚｼﾞｽﾀ用）	2	７４ＡＬＳ１６４
並列入力直列出力シフトレジスタ（入力シフトレジスタ用）	1	７４ＡＬＳ１６５
装置の寸法	1	長さ　3 3/8” 幅　2 1/8” (8.57×5.40 cm)

表　1

【００１９】
安全性
問合せ応答法による認証は単一パスワードあるいはコードよりすぐれていることが知られている（例えば、Ｗ．Ｊ．　Ｃａｅｌｌｉ（編）の情報化時代のコンピュータセキュリティ、頁２２３－２３４、エルスビア科学出版社、ＩＦＩＰ１９８９参照。）。問合せ応答法では、ユーザによって与えられる応答はシステムによって与えられた特定の問合せ（入力番号）についてのみ有効である。応答を不法にモニタして盗聴されても、システムによって与えられる問合せは次回はほとんど確実に異なっており、完全に別の応答が必要になるから、何も問題にならない。問合せを応答に写像するのに複雑な関数（あるいは大きな表あるいは関数と表の組合せ）を使うことによって、典型的にシステムのセキュリティを破そうとする試みに対して良い保護ができることになる。
【００２０】
第２の保証はＰＩＮ（通常４桁）を使うことである。これによってＰＩＮが分からなければ、ＵＡは詐欺には使えないことになる。またユーザはＰＩＮを離れた場所で（例えば公衆電話の遠くで）予め与えておくようにしてもよい。最後に一度ＰＩＮを入れても、ＵＡは有限の回数（例えば５回）、しかも有限な時間の間しか使うことができない。ＵＡを使い続けるにはＰＩＮをもう一度入れなければならない。これによって正しいＰＩＮを入れたＵＡが盗まれても、これは有限の回数しか使えないことになる。またもしユーザがＰＩＮを入力して続けてＵＡを使うのを忘れたときには、自動内部タイマによってある時間の後でＵＡは消去され、詐欺でＵＡを使うことができない。もちろんＵＡをなくしたときには、クレジットカードやコーリングカードと同様にただちにとどけ出ることが期待される。
【００２１】
最後に、多くの認証システムと同様に、この認証システムでも誤りの場合には制限された再試行のあとで接続を切断する。従って、遠端のシステムが正しくない応答を受けたときには、これは、ユーザが再試行できるように異なる入力を送る。再試行の制限回数を超えたときには、接続は切られる。接続の再設定にはもちろん電話網の通常の遅延が生ずる。
【００２２】
実装
実装は２つの部分から成る。交換機／ＰＢＸのソフトウエア／ハードウエアの問合せ応答の実装と、入力番号を与えたときに出力番号を決定するＵＡのプログラムの実装である。

交換機、ＰＢＸあるいは他の通信ネットワークの要素上に実装されるべき部分は入力乱数の選択、ＤＴＭＦの出力および／あるいはユーザに番号を中継するための音声応答、応答あるいはユーザによってキーインされた数字の受信、その応答とシステム自身の内部で発生された応答との比較である。応答の発生は内部調査されないようにするためにチップ中にパッケージされる。ＵＡの内部では応答の発生のために類似の機構を利用する。このメカニズムは計算アルゴリズム、テーブルルックアップのプロセスあるいはその両者の組合せである。

【００２３】

交換機／ＰＢＸの中での一致応答を発生するメカニズムはまた、関連する特定のＵＡの番号（ＩＤ）を考慮しなければならない。２つの異なるＵＡはほとんど確実に問合せ－応答の一致に異なる関数を使用する。ＵＡは出力応答中のそのＩＤ番号を指定する埋込まれた数字によってＩＤを知る。交換機／ＰＢＸはこのＩＤの助けによってＵＡによって与えられた応答をチェックするのに使用する適切な関数を決定する。

【００２４】

先に述べたように、問合せと応答の関数写像は異なるＵＡについては異なっているようにするべきである。これはＵＡの中である入力をある出力に写像する表を持つことによって容易に達成することができる。しかしこれには２つの重大な欠点が存在する。第１は入力の集合が制約されるためにセキュリティ上の兼ね合いが問題になること、第２はシステム側で多数のＵＡの表を蓄積するために極めて大量のメモリを必要とすることである。（概要の暗号アルゴリズムを使った）解決法は写像に共通のアルゴリズムを使用するが、各ユーザについて異なるキー入力を使用することによって各ユーザについてある程度アルゴリズムを変化することである。システムの中ではＵＡのシーケンスＩＤを使って表を参照してそのＵＡのキーを見付け、次にこれをアルゴリズムに与えてこれを特定のＵＡについて適切に修正して与えられた入力について適切な応答を計算することができる。ＵＡの中では詳細はもう少し簡単である。アルゴリズムの特定の部分だけを実装すればよい。これは全体的あるいは部分的に表駆動にすることができる。図５はＵＡおよび（初期問合せ番号とＵＡのシーケンスＩＤを共に８桁の長さと仮定した）交換機あるいはＰＢＸの問合せ応答システムに関連した全体図を示している（問合せ番号とシーケンスＩＤの各々に８桁を用いることによって充分な保護が可能になり、同時にキーインされるべき全体の応答の長さは１６桁になる。これは現在使用されているコーリングカードの符号（１４桁）と同等である。）。

【００２５】

他の装置および方式との比較

問合せ－応答方式はユーザが使用される関数を記憶すると考えられる高セキュリティのコンピュータシステムでは時として使用される。これに対して、公開キー暗号化およびディジタル署名のような認証方式で使用されるのに広く研究されている最もセキュリティの高い関数は、いわゆるトラップドア関数である。（リベスト，Ｒ．Ｌ．，シャミール，Ａ．，アデルマン，Ｌ．，ディジタル署名と公開キー暗号システム：コミュニケーションＡＣＭ２１，２（７８年２月）ｐｐ１２０－１２６）、（マークル，Ｒ．Ｃ，ヘルマン，Ｍ．Ｅ：情報の秘匿とトラップドアナップザックでの受信；ＩＥＥＥトランザクションオンインフォーメーションセオリ、２４，５（７８年９月）ｐｐ５２５－５３０）（ディフィー，Ｗ．，ヘルマン，Ｍ．Ｅ．，プライバシーと認証－暗号化入門、ＩＥＥＥプロシーディングス、６７，３（７９年３月）ｐｐ３９７－４２７）（ディプロト，Ａ．ナックザック問題の一般化に基づく公開キー暗号システム、ヨーロクリプト８５アブストラクト、リンツ、オーストリア８５年４月）。これらはキーの内の一部を公開にしなければならないときにはもちろん有用である。しかし、ここで考えている装置では各ユーザのキー（使用される関数）は秘密にしておくことができるから、秘密キー方式で充分であり、公開キー暗号化あるいはディジタル署名方式は必要ない。２つの良く知られた秘密キー方式として、ナショナルビューロオブスタンダードのデータ暗号標準（ＤＥＳ）アルゴリズム（ナショナルビューロオブスタンダード、コンピュータセキュリティのための暗号化ワークショッ

プレポート、２１－２２、１９７６年９月、ＮＢＳＩＲ７７－１２９１（１９７７年９月））と高速データ暗号化アルゴリズム（ＦＥＡＬ）（シマズ，Ａ，ミヤグチ，Ｓ．高速データ暗号化アルゴリズム－ＦＥＡＬ、ヨーロクリプト８７アブストラクト、アムステルダム（８７年４月）ｐｐＶＩＩ－１１）がある。しかしコーリングカードの詐欺の防止には暗号化で開発された超高度なセキュリティ機能は不要であり、単にたやすい犯罪を防止するのに充分な複雑さがあれば良いことになる。ＤＥＳアルゴリズムあるいはＤＥＳアルゴリズムに基づくもっと簡単なアルゴリズムをここで使用すれば良い。

【００２６】

認証と暗号化の方式はセルラ電話システムでも有用である。これはユーザを一義的に識別し、通信のセキュリティを保持し、移動無線通信における他の特殊なセキュリティに関する必要性を満足するために使用される。このような目的で、ある種のセルラ電話方式の標準（ＥＴＳＩ／ＴＣＧＳＭ標準、セクションＧＳＭ３．２０（ＥＴＳＩ／ＰＴ１２による発表）（９０年２月）ｐｐ４－２８）では通信における複雑な暗号化／認証方式を必須のものとしている。適切に装備されたディジタル伝送用のセルラ電話機はその動作のためにこのような方式を必要としている。これに対してここで提示した必要性は通常の電話からの認証のみであり、この必要性は単純な秘密キー方式で満足することができる。認証を実行するためにここで提案された装置（ＵＡ）は、どのような電話回線を通してでも使用でき、特別の電話機は必要とせず、比較的安価で使いやすいパッケージとして実装でき、この点で独創的である。

【００２７】

ここで提案しているＵＡは現在利用できる種々のスマートカードとは異なっている。スマートカードは代表的には銀行サービスで使用されるが、また多数の分野でも使用される。（チャウム，Ｄ．，シャウミュラビクル，Ｉ．（編）スマートカード２０００：ＩＣカードの将来、ノースホランド社１９８９）、（マクリンドル，Ｊ．，スマートカード、ＩＦＳ社（スプリンガーバーラグ刊）１９９０）、（ブライト，Ｒ．スマートカード：原理、実際、応用、エリスハーウッド社（ジョンワイリー）１９８８）。スマートカードは一般にマイクロプロセッサと適切な量のメモリを持ち、認証、トランザクションの記録、過去のトランザクションの再生、その他を実行できる。しかしスマートカードは（コンタクトがあるものでも、コンタクトがないものでも）電力を与えリモートシステム（バンキング他）との通信のための特別の読み取り装置を必要とする。いわゆる封入式の電池を持つアクティブカードでも読み取り装置あるいは少なくとも遠方のシステムと直接交信するデータインタフェースを持つ。これに対してＵＡは内蔵のトーン検出器とトーン発生器があるために通常の電話機を通して動作することができる。

【００２８】

ＵＡは湿気による破損を最小化するために封入された装置であり、電池も封入されている。低電力の表示によってユーザに対して電池が消耗し始めていることを知らせ、この場合にユーザーは代りのＵＡを要求できる。典型的にＵＡは通常のクレジットカードやコーリングカードのように２年おきに更新される。電池の電力はＵＡの予期される寿命の間続くものとして適切である。顧客によって与えられるＰＩＮは、ＵＡを顧客に渡す前にＲＯＭに焼き付けられる。ＵＡの番号、キーあるいは応答メッセージを制御するのに必要な情報もＵＡのＲＯＭに焼き付けられる。ひとつの有利な実装においては、プログラムもまたＲＯＭに焼き付けられる。また代りに電池が装備されるからＲＡＭに格納しても良い。

【００２９】

汎用認証装置の追加の利点は、これが典型的なユーザが持つコーリングカード他の多サービスカードを置換できることである。これはどのような種別のサービスの認証にも使用することができる。例えば、これはリモートログインができるコンピュータシステムのセキュリティを改善するのにも使用できる。合法的なユーザは時に変更しなければならないパスワードを与える代りに、認証装置を持つ。ＵＡは複雑な関数を使ってセキュリティの高い問合せ応答メカニズムを容易に実装することができる。ダイヤルすることによってシステムは問合せを送り、ログインするためにはユーザは適切な応答を返送しなければならな

い。これはこのようなシステムのログインのセキュリティを改善するための比較的安価で便利な方法である。これはユーザ側で特別の装置を必要としない。

【００３０】

所望のサービスの使用を認証するために、ＵＡを特定の動作モードに設定するために異なるサービスについて異なるコードを使用することができる。特定のサービスを使用するための認証を要求する電話番号を呼び、問合せ－応答のプロセスは先に述べたように実行される。ＵＡの実装および全体の構成は現在の技術で実行できる。

【００３１】

認証サービスは電話交換機（例えば、ＡＴ＆Ｔの５ＥＳＳ（登録商標）交換機）の付加機能として提供できる。このようなゲートキーパとして動作できる交換機を使って企業のＰＢＸを取扱うことができる。ＰＢＸにアクセスする発呼者の要求が認証されれば、発呼者はゲートキーパ交換機によってＰＢＸにアクセスすることが許可され、ＰＢＸは発呼者の要求を処理するか、ＰＢＸはアクセスを要求するユーザの繰返される認証によって塞がれることはない。また認証メカニズムのシステム側が電話網を通して一度利用できるようになれば、ＵＡを種々の目的で利用することが容易になる。電話網の所有会社（市内電話会社あるいは長距離電話会社）は、ＵＡと認証サービスの両方がネットワークにあれば、認証をエンドツーエンドのサービスとして提供することができる。この点においてはＵＡはスマートカードと競争になることはない。スマートカードは通常はここで提案しているＵＡより計算能力で強力であり融通性がある。これはまたより高価でそれを動作するには特殊端末が必要であるから制約がある。ＵＡの範囲は限定されているが（認証のみに使用）、どのような通常の音声電話機からでも使用でき、そのハードウエアは汎用でなく専用であるから安価である。この点で、プラスチックのコーリングカードの代りにＵＡを導入することは有効である。このような装置には明かな需要がある。スマートカードリーダ端末がもっと増加した時になれば、ＵＡをスマートカードに更新してもよい。

【００３２】

代替実装法

ＤＴＭＦを利用した標準のトーンを使用しないで、代りに音声信号を音声周波数の範囲にある２つの周波数で周波数シフトキーイングする（高周波と低周波）ことによって符号化して、もっと丈夫で安価な実装が可能になる。これは例えば入来発呼者識別のために使用される米国特許４，８２３，９５６に述べられている。この場合には、ＤＴＭＦトーン検出器／発生器（ＳＳＩ２０Ｃ９０）は不要になる。また入来音声を拾うためにカーボンマイクロフォンの代りに他の技術を使うこともできる。誘導コイルを用いた検出器（補聴器に使用しているものに類似）によって、マイクロフォンを必要とせずに（受話器からではなく）電話回線から直接に電気信号を拾うことができる。これは雑音環境で良好に動作する。同様に、通常の金属ダイアフラムのスピーカの代りに、出力音声を発生するにはピエゾ（圧電）効果音声発生器を使用できる。このようなピエゾ効果装置は金属ダイアフラムよりも物理的に丈夫でよりコンパクトである。これは安価でもある。遠端で周波数が高いか低いかを判定すればよいから音声出力に高忠実性の必要はない。従って、ピエゾ効果発生器は典型的に少数の周波数でしか使えないが充分である。

【００３３】

認証システムを使って認証を受けるにはユーザは２つの動作が要求される。ユーザはまず受信／送信キーをクリックして装置を受信機の近くに置き、入来音声信号を受信する。次に再びキーをクリックして装置を送話機の近くに置き出力音声信号を送信する。この方式を変更してユーザの動作回数を減らして、装置を使いやすくすることができる。

【００３４】

内部クロックと疑似ランダム信号発生器（疑似乱数シーケンス発生器のような）を追加して、装置はそれ自身で入力番号を発生するようにすることもできる。この場合には電話回線から入力音声信号を受信する必要はない。この場合にはユーザはただ装置を送話機の近くに置き、送信キーをクリックすればよい。内部クロックから取られる時刻が疑似乱数信号発生器に対する種として与えられ、この発生器の出力が認証装置に対する入力数字にな

る。装置はその内部時刻（年、月、日、時間、分）を計算／テーブルルックアップ関数からの出力数字と共に送信する。

【００３５】

遠端のシステムは装置からの時刻を受信し、まずそれが内部の時刻に近いか（スレショルド以内か）を確認する。もし装置の時刻がスレショルド内でなければ、遠端のシステム（ＰＢＸあるいは交換機）は認証を要求する前に装置のクロックを遠端のシステムのクロックと同期することを要求する。時刻の一致のチェックは詐欺者が時刻と出力数字の対を記録して、その対を再び使って詐欺的認証をしてしまうのを防止するものである。

【００３６】

もし装置の時刻が許容できるスレショルドの中に入っていれば、遠端のシステムは送信された時刻を使って認証の入力数字を作り、次に出力数字を得て受信された出力数字との一致をとる。一致が得られれば、認証が行なわれる。

【００３７】

他の代替法として、安全性は低いが、ＵＡで回数を記憶し、使用するたびに回数を進める方法がある。認証システムも回数を記憶している。ＵＡは回数と回数を変換したものの両方を認証システムに送信する。次に認証システムは変換を確認するが、送信された回数が最後に認証された値より大きいときにしか認証を受理しない。有利なことに、この構成によって有効な認証を盗んで単にこれを再利用することが防止され、また認証システムから乱数を受信する必要がなくなる。

【００３８】

ここでランダムあるいは疑似ランダム等の用語は、その数字が予測できないことを意味するが、乱数表に見られるようなテストに合格したものである必要はない。予測不可能性がその主要な性質である。

【００３９】

ここで述べたような音声通信インタフェースはＡＴ＆Ｔスマートカード（登録商標）のようなスマートカードにも使うことができる。このような通信モードでは特別な読み取り端末は必要ないから、音声インタフェースを持つスマートカードを通常の電話回線で使用することができる。情報の伝送はカードを送話器の近くに保持して受信／送信キーをクリックすることによって実行できる。同様に遠端からの情報はカードを受話器の近くに置き、受信／送信キーをクリックすることによって行なわれる。伝送誤りに対処するために、誤り検出／訂正符号を用いて音声信号を符号化できる。

【００４０】

上述の説明は本発明の有利な一実施例のためだけであることが理解されるであろう。本発明の精神と範囲を逸脱することなく、当業者には多くの他の構成を工夫することができる。従って本発明は添付の特許請求の範囲による規定によってのみ制限されるものである。

【図面の簡単な説明】

【図１】汎用認証のシナリオのブロック図である。

【図２】汎用認証の状態図である。

【図３】汎用認証装置の外観を示す図である。

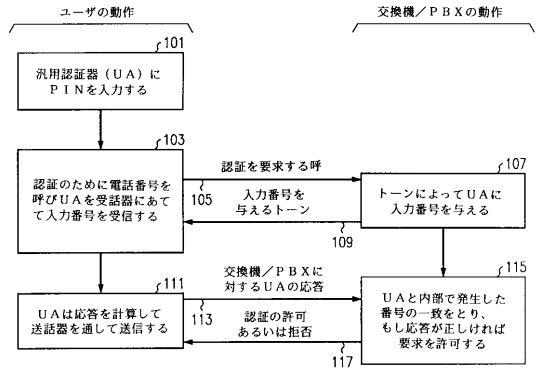
【図４】汎用認証装置の内部構造を示す図である。

【図５】汎用認証装置の動作の全体ブロック図である。

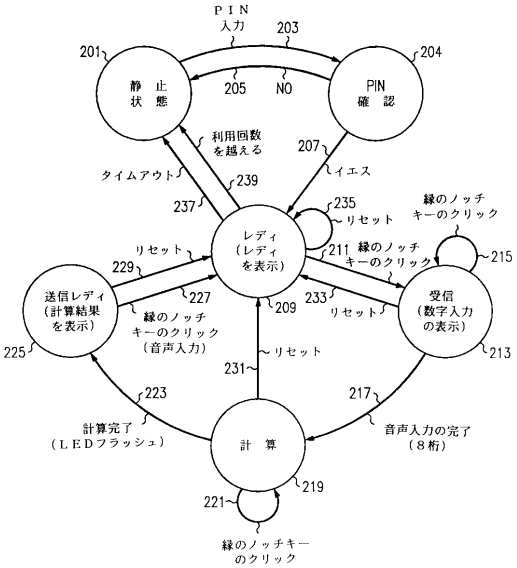
【符号の説明】

３０７　　キーパッド
３０９　　リセットバー
３１１　　ＬＣＤ表示器
３１３　　縁のノッチ　キー
４０７　　マイクロプロセッサ
４１０　　プログラムメモリ
４２１　　マイクロフォン
４３９　　スピーカ

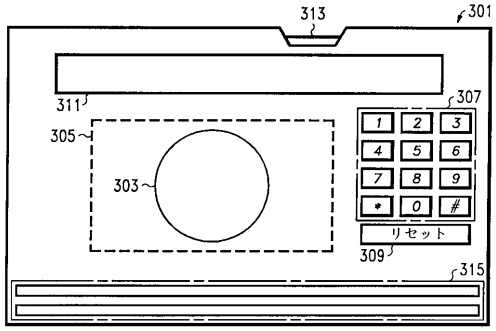
【図１】


ユーザの動作
交換機／ＰＢＸの動作
101
汎用認証器（ＵＡ）にＰＩＮを入力する
103
認証のために電話番号を呼びＵＡを受話器にあてて入力番号を受信する
認証を要求する呼
105
入力番号を与えるトーン
107
トーンによってＵＡに入力番号を与える
109
111
ＵＡは応答を計算して送話器を通して送信する
交換機／ＰＢＸに対するＵＡの応答
113
認証の許可あるいは拒否
115
ＵＡと内部で発生した番号の一致をとり、もし応答が正しければ要求を許可する
117

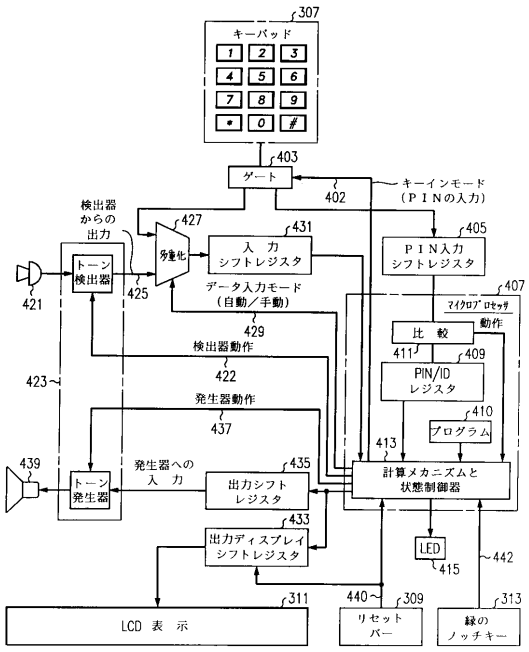
【図２】


ＰＩＮ入力
201
203
204
静止状態
205
NO
PIN確認
利用回数を越える
207
イエス
タイムアウト
239
237
235
リセット
緑のノッチキーのクリック
215
211
リセット
229
レディ（レディを表示）
送信レディ（計算結果を表示）
227
緑のノッチキーのクリック（音声入力）
209
233
リセット
受信（数字入力の表示）
213
225
リセット
231
223
217
計算完了（ＬＥＤフラッシュ）
計算
音声入力の完了（８桁）
219
221
緑のノッチキーのクリック

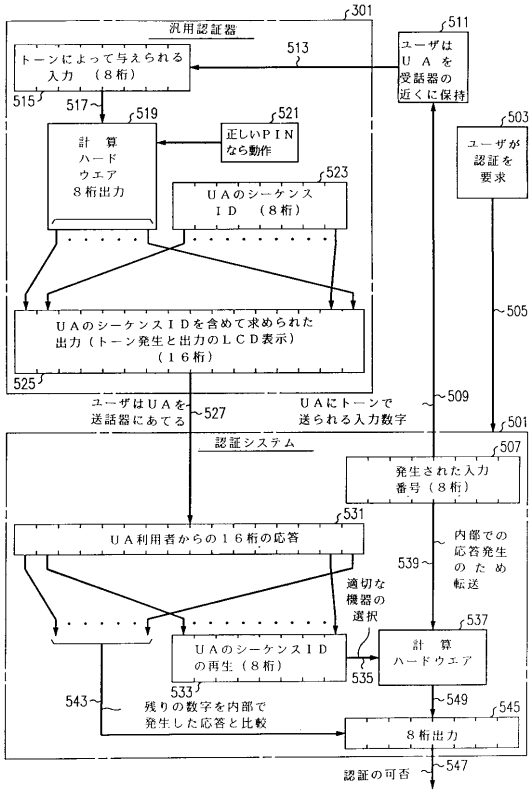
【図３】


313
301
311
307
305
303
1 2 3
4 5 6
7 8 9
* 0 #
リセット
309
315

【図４】


307
キーパッド
1 2 3
4 5 6
7 8 9
* 0 #
403
ゲート
402
キーインモード（ＰＩＮの入力）
検出器からの出力
427
多重化
431
入力シフトレジスタ
405
ＰＩＮ入力シフトレジスタ
421
トーン検出器
425
データ入力モード（自動／手動）
407
マイクロプロセッサ
429
検出器動作
比較
動作
411
409
PIN/IDレジスタ
423
422
発生器動作
410
プログラム
437
413
439
トーン発生器
発生器への入力
435
出力シフトレジスタ
計算メカニズムと状態制御器
433
出力ディスプレイシフトレジスタ
LED
415
442
440
309
313
311
LCD 表示
リセットバー
緑のノッチキー

【図５】


301
汎用認証器
トーンによって与えられる入力 （８桁）
513
511
ユーザはＵＡを受話器の近くに保持
515
517
519
計算ハードウエア８桁出力
521
正しいＰＩＮなら動作
503
ユーザが認証を要求
523
ＵＡのシーケンスＩＤ （８桁）
505
ＵＡのシーケンスＩＤを含めて求められた出力（トーン発生と出力のＬＣＤ表示）（１６桁）
525
ユーザはＵＡを送話器にあてる
527
ＵＡにトーンで送られる入力数字
509
501
認証システム
507
発生された入力番号（８桁）
531
ＵＡ利用者からの１６桁の応答
539
内部での応答発生のため転送
適切な機器の選択
537
計算ハードウエア
ＵＡのシーケンスＩＤの再生（８桁）
533
535
543
残りの数字を内部で発生した応答と比較
549
545
８桁出力
547
認証の可否

フロントページの続き

(72)発明者　アクテルザマン
アメリカ合衆国　６０５６５　イリノイズ，ネイパーヴィル，マークェット　アヴェニュー　１５８５
(72)発明者　アミタバ　ハツラ
アメリカ合衆国　０７７３３　ニュージャーシィ，ホルムデル，スプリング　ヴァレー　ドライヴ　２２

審査官　吉村　博之

(56)参考文献　特開昭６３－２６０３４３（ＪＰ，Ａ）
特表昭６１－５０２９９９（ＪＰ，Ａ）
特開昭６２－０４３９４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04M 11/00-11/10
H04M 1/66-1/67