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

特許第4221680号
(P4221680)

(45)発行日　平成21年2月12日(2009.2.12)　(24)登録日　平成20年11月28日(2008.11.28)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330G
G07F 7/10	(2006.01)	G07F	7/10	
H04L 9/32	(2006.01)	H04L	9/00	673E
		H04L	9/00	675A

請求項の数 7　(全 14 頁)

(21)出願番号　特願平11-521129
(86)(22)出願日　平成10年10月1日(1998.10.1)
(65)公表番号　特表2001-509295(P2001-509295A)
(43)公表日　平成13年7月10日(2001.7.10)
(86)国際出願番号　PCT/FR1998/002104
(87)国際公開番号　WO1999/018546
(87)国際公開日　平成11年4月15日(1999.4.15)
審査請求日　平成17年9月30日(2005.9.30)
(31)優先権主張番号　08/942,904
(32)優先日　平成9年10月2日(1997.10.2)
(33)優先権主張国　米国(US)

(73)特許権者　508166383
アクティブカール
フランス国　シュールセーヌ　エフ－９２１５０　アブニュ　デュ　ジェネラル　ドゴール　２４－２８
(74)代理人　100077861
弁理士　朝倉　勝三
(72)発明者　オードゥベール　イブ
アメリカ合衆国　カリフォルニア　９５０３２　ロス・ゲートス　フォレスター・ロード　２３７

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】スマートカードを使用した認証システム

(57)【特許請求の範囲】

【請求項１】

ユーザ用にカスタマイズされた少なくとも１つの第１のユニット（２；１０２；２０２；３０２）と、ある機能へのアクセスを制御する少なくとも１つの第２の検証ユニット（３；１０３；２０３；３０３）とを備えた、少なくとも１人の前記ユーザの前記機能へのアクセス制御のための認証システムであって、

前記第１のユニット（２；１０２；２０２；３０２）が、

時間の関数として変化する少なくとも第１の動的変数（Ｔ）を生成する第１の生成手段（１３；１１３；２１３；３１３）と、

前記第１のユニットにて生成された前記第１の動的変数（Ｔ）に依存した入力パラメータを使用して少なくとも１つの第１の暗号化アルゴリズムに従って前記第１のユニットに特有の第１のパスワード（Ａ）を生成するものであって、前記第１のパスワード（Ａ）を生成するための前記入力パラメータの１つが、前記第１の暗号化アルゴリズムにて使用される暗号化キー（Ｋｎ；Ｋ）である、第１の計算手段（２４，２５；１２４，１２５；２２５）と、

前記第１のパスワードを前記第２のユニットへ転送する手段（１０；３３）とを有し、

前記第２のユニット（３；１０３；２０３；３０３）が、

前記第１のユニットによってなされたアクセス又は認証要求に応答して前記第１のユニットに割り当てられた時間の関数として変化する第１の動的変数（Ｔａ）を生成する第２の生成手段（１８；１１８；２１８）と、

前記第２のユニットにて生成された前記第１の動的変数（Ｔａ）に依存した入力パラメータを使用して少なくとも１つの第２の暗号化アルゴリズムを介して第２のパスワード（Ａａ）を生成するものであって、前記第２のパスワード（Ａａ）を生成するのに使用される前記入力パラメータの１つが、前記第２の暗号化アルゴリズムにて使用される暗号化キー（Ｋｎａ；Ｋａ）である、第２の計算手段（２４ａ，２５ａ；１２４ａ，１２５ａ；２２５ａ）と、
前記第１及び第２のパスワード（Ａ，Ａａ）をそれぞれ比較する比較手段（３４；１３４；２３４）と、
前記第１及び第２のパスワード（Ａ，Ａａ）間に所定の一致がある場合に前記機能（１）へのアクセスの権限を与える手段（３４；１３４；２３４）とを有する、認証システムにおいて、
前記第１及び第２のユニットにそれぞれ与えられた前記第１及び第２の生成手段が、前記第１のユニットの前記第１の動的変数（Ｔ）と前記第２のユニットの前記第１の動的変数（Ｔａ）とを一斉にではあるが独立に生成し、
前記第１のユニットが、チップカード（４；１０４；２０４；３０４）とカードリーダ（５；１０５；２０５；３０５）とをさらに備え、
前記第１のユニット（２；１０２；２０２；３０２）の前記第１の動的変数（Ｔ）を生成する前記手段（１２，１３；１１３；２１３；３１２，３１３）が、チップカードの外側に配置され、前記第１のユニットの前記第１の動的変数（Ｔ）が、前記カードリーダによって前記チップカードへ転送され、
前記第１のユニット（２；１０２；３０２）及び前記第２のユニット（３；１０３；３０３）がそれぞれ、アクセス要求に先立って前記第１のユニットによってなされたアクセス要求の回数を含む関数に従って少なくとも第２の動的変数（Ｎｎ，Ｎｎａ）を生成する第３の生成手段（８；１０８）及び第４の生成手段（１９；１１９）を備え、
前記第１の計算手段が、前記第１のユニットの前記両動的変数（Ｔ，Ｎｎ）の処理のための前記チップカード（４；１０４；２０４；３０４）内の処理手段（２５；２２５）を備えていることを特徴とする認証システム。

【請求項２】
請求項１記載の認証システムにおいて、前記第１のユニット（２；１０２；３０２）及び前記第２のユニット（３；１０３；３０３）が、前記第１及び第２の動的変数（Ｔ，Ｔａ，Ｎｎ，Ｎｎａ）の少なくとも１つを含む関数に従って少なくとも第３の動的変数（Ｋｎ，Ｋｎａ）を生成するための第５の生成手段（２８；１２８）及び第６の生成手段（２８ａ；１２８ａ）を備え、前記第１の計算手段（２４，２５；１２４，１２５）及び前記第２の計算手段（２４ａ，２５ａ；１２４ａ，１２５ａ）が前記第１の動的変数（Ｔ，Ｔａ）、前記第２の動的変数（Ｎｎ，Ｎｎａ）及び前記第３の動的変数（Ｋｎ，Ｋｎａ）の関数とする前記第１のパスワード（Ａ）及び前記第２のパスワード（Ａａ）をそれぞれ生成することを特徴とする認証システム。

【請求項３】
請求項２記載の認証システムにおいて、前記第１のユニット（２；１０２；３０２）及び前記第２のユニット（３；１０３；３０３）が、前記第１の動的変数（Ｔ，Ｔａ）及び前記第２の動的変数（Ｎｎ，Ｎｎａ）の論理的組み合わせによって中間の動的変数を生成するための第３の計算手段（２４；１２４）及び第４の計算手段（２４ａ；１２４ａ）を備え、前記第１の計算手段（２５；１２５）及び前記第２の計算手段（２５ａ；１２５ａ）が前記中間の動的変数及び前記第３の動的変数（Ｋｎ，Ｋｎａ）の関数とする前記第１のパスワード（Ａ）及び前記第２のパスワード（Ａａ）をそれぞれ生成することを特徴とする認証システム。

【請求項４】
請求項３記載の認証システムにおいて、前記第３の計算手段（１２４）が、前記チップカード（１０４）内に配置されていることを特徴とする認証システム。

【請求項５】

請求項３記載の認証システムにおいて、前記第３の計算手段（２４）が、前記チップカード（４）の外に配置されていることを特徴とする認証システム。
【請求項６】
請求項２ないし５のいずれか１項に記載の認証システムにおいて、前記第２の動的変数（Ｎｎ，Ｎｎａ）が、アクセス要求に先立って前記第１のユニット（２；１０２；３０２）によってなされた前記アクセス要求の回数であり、前記第３の動的変数（Ｋｎ，Ｋｎａ）が、前記第２の動的変数（Ｎｎ，Ｎｎａ）及び前記第３の動的変数の前値の関数であることを特徴とする認証システム。
【請求項７】
請求項２ないし６のいずれか１項に記載の認証システムにおいて、前記第３の動的変数（Ｋｎ，Ｋｎａ）が、前記暗号化キーであることを特徴とする認証システム。
【発明の詳細な説明】
【０００１】
本発明は、個人及び／又はメッセージの認証のための電子システムに関し、特に、ある機能へのユーザのアクセスを制御して問題のシステムと関連された専門サービスユニットからユーザにサービス又は他の提供を条件付きで得ることを可能にさせる電子システムに関する。
【０００２】
さらに、本発明は、コンピュータ、より一般的には、正式且つ正当に権利が与えられている人に使用が予約されたコンピュータ化ネットワークへのアクセス制御あるいはコンピュータ化ネットワーク内で扱われるメッセージの認証のためのシステムに関する。
【０００３】
米国特許第４，７２０，８６０号は、パスワードを発生させるために静的変数と動的変数とを使用した認証システムを開示している。この特許において、成し遂げようとするすべてのトランザクションのときには、アクセス要求手続きの開始時にユーザによって認証ユニット（トークン）に固定コードが入力される。この固定コードは静的変数を構成している。また、トークンの中で第２の変数が生成され、その変数は時間の関数として、特に、固定コードがユーザによってトークンに入力された瞬間の関数として、動的に変化する。この静的及び動的の２つの変数は、次に、トークン内でパスワードを生成するためにインプリメントされた秘密の暗号化アルゴリズムの入力パラメータとして使用される。このパスワードはトークン上に表示され、ユーザはそれをテストサーバに転送するよう求められる。固定コードは、サーバにも転送され、このサーバは、原理的にはトークン内で使用されたものと同じ値を持つ動的変数とともに、同じ暗号化アルゴリズムを使用することによって、パスワードを計算する。このパスワードは、ユーザによってサーバに転送されたパスワードと比較され、一致した場合に、機能へのアクセスのための認証が与えられる。このようにして、このアクセス制御システムは静的変数を使用し、この静的変数から、動的変数も使用しながら暗号化アルゴリズムによりパスワードを計算する。
【０００４】
パスワードを生成するのに時間依存の動的変数を使った認証システムが、米国特許第３，８０６，８７４号、４，６０１，０１１号、４，８００，５９０号にも開示されている。
【０００５】
トークン及びサーバの両方にて独立に生成されたこの時間依存の動的変数とそれぞれの側で動的変数を生成するのに使用されるこれら２つの設備のクロックとは、一定の精度で同期されていなければならない。
【０００６】
本発明の目的は、不正に対して改善されたセキュリティを提案する認証システムを提供することである。本発明の他の目的は、少なくとも部分的に従来のハードウェア設備を使用しながら、動的パスワード、特に時間依存の動的パスワードを与える認証システムを提供することである。
【０００７】

従って、本発明は、ユーザ用にカスタマイズされた少なくとも１つの第１のユニットと、ある機能へのアクセスを制御する少なくとも１つの第２の検証ユニットとを備えた、少なくとも１人の前記ユーザの前記機能へのアクセス制御のための認証システムであって、
前記第１のユニットが、
時間の関数として変化する少なくとも第１の動的変数を生成する第１の生成手段と、
前記第１のユニットにて生成された前記第１の動的変数に依存した入力パラメータを使用して少なくとも１つの第１の暗号化アルゴリズムに従って前記第１のユニットに特有の第１のパスワードを生成するものであって、前記第１のパスワードを生成するための前記入力パラメータの１つが、前記第１の暗号化アルゴリズムにて使用される暗号化キーである、第１の計算手段と、
前記第１のパスワードを前記第２のユニットへ転送する手段とを有し、
前記第２のユニットが、
前記第１のユニットによってなされたアクセス又は認証要求に応答して前記第１のユニットに割り当てられた時間の関数として変化する第１の動的変数を生成する第２の生成手段と、
前記第２のユニットにて生成された前記第１の動的変数に依存した入力パラメータを使用して少なくとも１つの第２の暗号化アルゴリズムを介して第２のパスワードを生成するものであって、前記第２のパスワードを生成するのに使用される前記入力パラメータの１つが、前記第２の暗号化アルゴリズムにて使用される暗号化キーである、第２の計算手段と、
前記第１及び第２のパスワードをそれぞれ比較する比較手段と、
前記第１及び第２のパスワード間に所定の一致がある場合に前記機能へのアクセスの権限を与える手段とを有する、認証システムにおいて、
前記第１及び第２のユニットにそれぞれ与えられた前記第１及び第２の生成手段が、前記第１のユニットの前記第１の動的変数と前記第２のユニットの前記第１の動的変数とを一斉にではあるが独立に生成し、
前記第１のユニットが、チップカードとカードリーダとをさらに備え、
前記第１のユニットの前記第１の動的変数を生成する前記手段が、チップカードの外側に配置され、前記第１のユニットの前記第１の動的変数が、前記カードリーダによって前記チップカードへ転送され、
前記第１のユニット及び前記第２のユニットがそれぞれ、アクセス要求に先立って前記第１のユニットによってなされたアクセス要求の回数を含む関数に従って少なくとも第２の動的変数を生成する第３の生成手段及び第４の生成手段を備え、
前記第１の計算手段が、前記第１のユニットの前記両動的変数の処理のための前記チップカード内の処理手段を備えていることを特徴とする認証システムを提供している。

【０００８】

本発明のシステムは、データの暗号化に関して非常に高いレベルのセキュリティを与えるが自身では電源を持たないスマートカードのようなカードの利点を、時間依存の動的パスワードを与える認証システムの利点と結びつけている。

【０００９】

本発明の他の特徴及び利点は、単に一例として添付図面を参照して行う下記説明から明らかとなるであろう。

【００１０】

本発明の第１実施例による認証システムを非常に簡単化した図を図１に示す。
このシステムは、図１において、箱１で象徴化された機能への条件付きアクセスを認めるものとする。この用語“機能”は、非常に広い意味で捕えるべきである。これは、要求の公式化によって端末の検証を必要とする認証と、さらに、好ましくは、要求が合法かどうかを確かめるために機能に対してアクセスを要求する人の識別とを含む許可によってアクセスが条件付けされた、あらゆる機能を表している。

【００１１】

この機能は、任意の種類、例えば建物、コンピュータ化ネットワーク、あるいはコンピュータ、金銭上の取り引き（テレビショッピング、ホームバンキング、双方向テレビゲーム、ペイテレビ）などへのアクセスのための機能とすることができる。機能は、また、メッセージの認証を含むこともできる。

【００１２】

図１に示した第１実施例において、本発明によるシステムは少なくとも１つの第１の認証ユニット２と少なくとも１つの第２の検証ユニット３とを含んでいることがわかる。本発明による認証システムは多数の第１のユニットと１つ以上の第２のユニットとを含むことができ、いずれにしても、一般的には、第２のユニットの数は第１のユニットよりもかなり少ないことに注目されたい。従って、本発明は、ユニット２，３の数を何ら限定するものではない。

【００１３】

第１のユニット２は、スマートカード４、スマートカードリーダ５及びパーソナルコンピュータ（ＰＣ）のようなコンピュータ６を備え、このコンピュータ６には、スマートカードリーダ５がＲＳ－２３２Ｃ又はパラレルポートのような適当なインタフェースによってキーボード又はＰＣＭＣＩＡが接続される。

【００１４】

スマートカード４は、暗号化アルゴリズムＡＬＧＯを実行するよう正式にプログラムされたマイクロコントローラ７及び習慣的なＲＯＭメモリを備えている。このスマートカード４は、また、図１に、イベントカウンタの内容Ｎｎを記憶するレジスタ８及び秘密の動的キーＫｎを記憶するレジスタ９によって示したＥＥＰＲＯＭのようなプログラマブルメモリも備えている。

【００１５】

コンピュータ６は、例えばスマートカード４のユーザの個人識別番号ＰＩＮのような情報の入力を与えることを意図したキーボード１０を備えている。コンピュータ６は、また、ディスプレイスクリーン１１とカウンタ１３を増分させるクロック１２とを備え、そのカウンタ１３は時間を表す動的変数Ｔを与える。コンピュータ６は、また、図示しない通常のマイクロプロセッサ、メモリ、インタフェースなどを備えている。

【００１６】

第２のユニット３（以下サーバという）は、接続１４によってコンピュータ６と通信する。この通信は、適切な手段によって短距離又は長距離で行うことができる。その接続によって流す情報は、特にサーバ３にて管理を受ける必要のあるパスワード、及び、できればこのサーバによって認証及び演算されるべきデータである。

【００１７】

サーバ３は、特にさまざまな第１のユニット２によって公式化されたアクセス要求によりアドレス指定された機能１を条件付きで解除できるプロセッサ１５を備え、これら機能がサーバ３の内外で実施することができる。サーバ３は、一般的には多数の第１のユニット２と協働することに注目すべきである。このサーバ３は、また、各スマートカード４のための秘密の動的キーＫｎａを記憶するメモリ１６と、時間を表す動的変数Ｔｃを与えるカウンタ１８を増分させるクロック１７と、各スマートカード４のイベントカウンタの内容Ｎｎａを記憶するメモリ１９とを備えている。

【００１８】

図２は、機能へのアクセス要求が第１のユニット２のユーザによって公式化されたとき展開される各種演算の簡単化されたフローチャートを示す。図２は２つの部分に分けられており、一点鎖線Ｌより左の部分は第１のユニット２において実行される演算を表し、右側の部分はサーバ３において展開されるものを示している。

【００１９】

カード４は、特定のユーザに個人的に割り当てられるようカスタマイズされる。これは公開識別番号（ユーザＩＤ）を与え、及び／あるいは、この番号はその中に非暗号化されて登録され、その初期化のときにそこに割り当てることができる。これは、また、ユーザの

名前又はユーザに特有の任意の他の情報によって形成することができる。

【００２０】

サーバ３において、手続きを初期化するため、公開識別番号（ユーザＩＤ）は最初にサーバ１５へ転送されなければならない。この動作は各種方法で実施することができる。ユーザＩＤは、例えばカード４をリーダ５に挿入するやいなや直接に、又は、ユーザ自身によってコンピュータ６のキーパッド１０に入力した後に、コンピュータ６によってサーバ３へ転送することができる。

【００２１】

また、ユーザは、２０において、コンピュータ６のキーパッド１０にユーザの秘密の個人識別コード又はＰＩＮを打ち込むことによって自己の権利を入力しなければならない。カード４内の２１において、打ち込まれたコードは、カード４のメモリに格納されたＰＩＮコードに対して検証される。不一致の場合、アクセス要求は、２２において、カード４によりただちに拒否され、それらがすべて失敗に終わった場合の最終的な拒絶となる前に、ユーザはできる限りいくつかの試みを連続して行うであろう。

【００２２】

一方、ＰＩＮコードが入力され、メモリ内のＰＩＮコードと一致した場合は、２３において、プログラムはカード４内でパスワードを計算する演算をトリガする。

【００２３】

この計算は、秘密又は公開とすることができる暗号化アルゴリズム（ブロック２５）の助けを借りて暗号化することからなる。公開の場合、当業者にはＤＥＳ（Data Encryption Standard）として知られているアルゴリズムとすることができる。

【００２４】

問題のアルゴリズムは、この場合、３つの数で表される動的変数による入力パラメータを使用する。それらの１つは、スマートカード４のレジスタ８に格納されていてカード４によってなされたアクセス要求の回数を表す変数Ｎｎであり、他は、現在の時刻を表すものであってコンピュータ６内のカウンタ１３の位置に相当する変数Ｔである。これらの変数は、初期化のとき、開始値Ｎ０及び／又はＴ０にセットされ、それぞれはゼロに等しくする必要はなく、秘密であってもそうでなくてもよい。また、Ｎｎ及びＴは、パラメータとして、とりわけアクセス要求の回数、アクセス要求の回数の関数及び現在の時刻をそれぞれ含む所定の関数に従って変化する。

【００２５】

特に、図２において、第１のユニット２により、一度でも、キーパッド１０への秘密の個人識別番号又はＰＩＮの入力を通じてユーザが識別されたことがあると、パーソナルコンピュータ６はスマートカード４内のイベントカウンタ８の内容Ｎｎを読み取る。

【００２６】

変数Ｎｎ及びＴはそれぞれ３２ビットとすることができ、コンピュータ６の２４において、連結動作が行われ、これにより、全体で６４ビットの入力パラメータ又は質問を提示する。さもなければ、２４における演算は、Ｎｎ及びＴに関して実施されるインターリーブ、ハッシング、排他的倫理和、論理積などの演算のような任意の所定の処理又は組み合わせとすることができる。換言すれば、２４における演算は、これらに限定されるものではなく、実質的に無限数の可能なやり方の１つであって、Ｎｎ及びＴの組み合わせ又は処理から出力（例えば６４ビット）を生成するために実施される任意の演算とすることができる。

【００２７】

この質問は、コンピュータ６によってスマートカード４に入力され、２５において、スマートカード４のレジスタ９に格納された暗号化キーＫｎを使って実施されるアルゴリズムＡＬＧＯにより暗号化される。２５において実施されるアルゴリズムを定義する他の方法は、Ｎｎ，Ｔの現在の値の関数としてアルゴリズムがパスワードを生成すること、又は２４において、Ｎｎ及びＴを連結することによって生成される値を含むキーに従ってＫｎを暗号化することである。

【００２８】
カード４内の２５において実施される暗号化は、２６においてパスワードＡを生成し、２７においてコンピュータ６にＮｎを格納しているカード４のアクセス要求レジスタ８の位置を１単位だけ増分させるようにする。この増分数Ｎｎ＋１は、カード４の２８において、第３の動的変数又は秘密の暗号化キーの新しい値Ｋｎ＋１を計算するための演算に当てられる。さもなければ、ユニット２７の出力は、１以外の他の数によってレジスタ８の増分を行うことができ、すなわち、増分は、毎回２単位（又は任意の他の数）によってもよい。また、増分の単位の数はアクセス要求ごとに変えることもできる。もちろん、増分はサーバ３において実施されるものと同期が取られていなければならない。

【００２９】
図３には、この新しい値を計算するために２８において実施することができる演算の例を示している。これらの演算は、スマートカード４及びサーバ３の両方において一斉に実施される。まず、値Ｎｎ＋１及びＫｎは、２９において、論理結合演算、例えば排他的論理和による結合に当てられる。この結果の中間値Ｚは、３０において、２５において使用したものと同じとすることができる既知又は公開アルゴリズムによって暗号化される。この暗号化は、たとえ、任意の他の秘密キーＱ（ブロック３１）が使用されたとしても、好ましくは現在の動的変数Ｋｎの値とする暗号化キーによって実施することができる。

【００３０】
暗号化演算３０の結果は、暗号化キーの新しい値Ｋｎ＋１であり、これは次のアクセス要求の間、使用されることになるであろう。この値はレジスタ９に格納される。

【００３１】
３２において、コンピュータ６のスクリーン１１上に表示されたパスワードＡを得た後、ユーザはサーバ３と通信することが促される。注目すべきは、このパスワードは、暗号化演算の全体的な結果でも、あるいはそのほんの一部の、例えば３２ビットワードでもよい。通信（破線３３によって示した）は、例えばコンピュータ６のキーパッド１０にそのワードを入力することによって行うことができる。この通信は、また、モデムによる場合のように自動的に実施することができ、その場合、パスワードＡは、３０において、必ずしもユーザに示す必要はない。

【００３２】
公開識別番号（ユーザＩＤ）がサーバ３に入力されると、第１ユニット２と協調し、独自に生成された第１ユニット２の動的変数によって、プロセッサ１５のプログラムは、第１ユニットにおいて実行されたものと同じ計算動作を実行する。従って、これらの動作は、図２において、同じ符号に“ａ”を付した符号にて示してある。例えば、識別番号をサーバ３に転送することによるアクセス要求に応答して、サーバ３のメモリ１６及び１９から変数Ｋｎａ及びＮｎａが抽出される。メモリ１６及び１９は、サーバに協働を依頼するスマートカード４ごとに変数Ｋｎａ及びＮｎａを記憶している。

【００３３】
アクセス要求に応答して、変数Ｔｃもカウンタ１８から抽出される。もし、スマートカード４と一緒に使用されるコンピュータ６がすべて同じ値Ｔ０に初期化されなかった場合、コンピュータ６は、例えばユーザＩＤがサーバ３に転送されたときにサーバ３によって識別されなければならない。この識別に応答して、マイクロプロセッサ１５はメモリにおいてこのコンピュータのための時間変数Ｔの初期値Ｔ０を読み込み、Ｔ０及びＴｃからコンピュータ６の時間変数Ｔに等しい時間変数Ｔａを計算することになる。

【００３４】
その結果、サーバ３は、そのサイドで、且つ第１のユニット２で生成されてサーバ３に送られる動的変数なしで、パスワードＡａを生成する。このパスワードＡａはユーザによってサーバ３へ送られるパスワードＡと比較されることになるものである。スマートカード４が本物ならば、パスワードＡ及びＡａは、一致するはずであり、あるいは少なくとも指定された規則に従って合致するはずである。３４において実施されたテストが遂に肯定応答となると、１における機能が自由になる。逆の場合は、アクセスは３５において拒絶さ

れる。

【００３５】

注目すべきは、本発明によるシステムにおいて、動的変数の１つが上述のように時間又はその関数であるとき、コンピュータ６及びサーバ３の両方で使用されるクロックのドリフトに遭遇することになるので、いくつかの問題が発生する。この問題の有利な解決法はＷＯ９７／３６２６３に開示されている。

【００３６】

開示されている実施例によれば、１における機能が最終的には自由になる第１のユニット２の認証のプロセスは、３つの、すなわち１つは暗号化キーＫｎ（Ｋｎａ）、他は既になされたアクセス要求の回数Ｎｎ（Ｎｎａ）及び時間Ｔ（Ｔａ）（又はそれらの変数の所定の関数に従って計算された数）である、３つの動的変数によって実施される。

【００３７】

暗号化キーＫｎ（Ｋｎａ）は、それ自身、１つのアクセス要求から別なものに変化し、値Ｎｎ（Ｎｎａ）の関数として動的に変化していき、これと論理的に組み合わされ、暗号化されて、次のアクセス要求のときに使用される暗号化キーＫｎ＋１（Ｋａｎ＋１）を生じさせる。

【００３８】

本発明の変形例によれば、第１のユニット２からサーバ３へのデータの転送は、把握することができるので、これらのデータは、機能１を果たしながら、当然次のテスト３４で許可が下りる限り、処理することができる。

【００３９】

３６において、ユーザのアクセス要求を公式化する間に、ユーザはキーパッド１０によって第１のユニット２にデータを入力する。これらのデータは、３７において、２つの変数Ｎｎ及びＴの連結値によって論理的に組み合わされ、この結果は２５において実施される暗号化処理のための入力パラメータとして使用される。代案として、データは、また、２５における暗号化動作の結果と直接組み合わされてもよいし、あるいは、アルゴリズムモジュール２５に与えられる他のキーとすることもできる。本質的な視点は、２５の出力が転送されたデータの関数でなければならないことである。

【００４０】

このデータは、また、例えばコンピュータ６のキーパッド１０によって、又はリンク１４を介して自動的に、サーバ３へ送られる。

【００４１】

サーバ３において、３６ａにてこのように受信されたデータは、第１のユニット２と同様の方法にて処理される。具体的には、そのデータは，３７ａにおいて、Ｎｎａ及びＴａの連結値による論理演算３７ａを通じて組み合わされ、この結果は、２５ａにおける暗号化処理のための入力パラメータとなる。もしくはそのデータは、２５ａにおける暗号化演算の結果と組み合わされるか、又はアルゴリズムモジュール２５ａに与えられる他のキーとすることができる。このデータは、また、機能１を実行する機構にも暗号化されずに送られる。

【００４２】

このようにして、データの確実性は、それぞれそのデータを表す値の関数であるパスワードＡ及びＡａを比較することによって証明することができる。従って、機能１の実行も、両サイドで提示されたデータ間に不一致があれば、拒否によって阻止される。

【００４３】

ここで、各種変形例について説明する。これら変形例のいくつかは、例えば第１のユニット２における動作の改良に関して述べるが、第１のユニット２及びサーバ３は同一又は整合するパスワードＡ，Ａａを生成できなければいけないので、同様の改良はサーバ３にも適用されることは理解されよう。

【００４４】

機能２８（図２及び図３に示した）は、交互にＴの関数として変えることができる。また

、アルゴリズム３０は新しいＫｎが生成されるたびに変更することもできる。同様に、ユニット２５にて実施されるアルゴリズムも、パスワードが生成される度に変更することができる。例えば、モジュール２５，２５ａ及び３０，３０ａは、異なるパスワード生成動作に使用されるアルゴリズムを持った複数のアルゴリズムを格納することができる。機能２８ａ，アルゴリズム３０ａ及びアルゴリズム２５ａに関する同期変更は、サーバ３において実施されることになる。

【００４５】

加えて、機能２９（図３）は、排他的論理和演算以外に、論理積演算、あるいは他に任意の論理演算のような他の機能とすることができる。さらに、機能２９では、Ｋｎ又はＱによって暗号化されるために、Ｎｎ＋１がアルゴリズム３０に直接入力されるようなものを不要にすることができる。あるいは、Ｑは、２９において、Ｎｎ＋１と排他的論理和演算され、Ｋｎ又はＱは論理演算２９の出力を暗号化するためのキーとして使用される。

【００４６】

別の変形例は、図２の要素２６及び２７間に論理積ゲートを与えることができ、要素２６の出力はこの論理積ゲートへの１つの入力となり、サーバ３からの信号はこの論理積ゲートへの他の入力となり、サーバ３からのその信号は要素２６ａが出力を生成したときのみ生成されるようにしたことである。この方法において、カード４内のレジスタ８及びサーバ３内のレジスタ１９は、同期して増分されることになる。従って、ＮｎとＮｎａとの間に同期の損失はない。しかし、本発明の実際の適用においては、このようにサーバからカードに戻される通信は好ましくない。

【００４７】

他の変形例は、スマートカード４のメモリにデータ３６を格納できるようにしたことである。例えばデータ３６は、カード４が銀行カードである場合、取引残高、口座番号などを表すデータとすることができる。

【００４８】

機能２８及び２８ａにおけるＫｎの再導出に関し、このような再導出は次のように実施することができる。Ｋｎは各パスワード生成のために２回、例えばパスワード生成の前後に再導出することができる。また、Ｋｎはパスワード生成処理と並行して再導出されてもよく、換言すれば、モジュール２５及び２５ａの出力をそれぞれモジュール２７及び２７ａへ直接入力することによってパスワードを生成している間に、Ｋｎを再導出することができる。

【００４９】

また、さもなければ、Ｎｎ及びＴを直接アルゴリズムモジュール２５へ入力することもできる。また、データをＮｎ又はＴと直接に論理的組み合わせをすることができ、あるいはデータを２つに分けて、各部分をＮｎ又はＴの一方と論理的に組み合わせすることもできる。

【００５０】

図４は、第１実施例の別バージョンを示したもので、パーソナルコンピュータにて実施されるソフトウェアを簡単にし、パーソナルコンピュータとスマートカードとの間の情報交換を制限したものである。図４において、図２と同じ符号に１００を加えた符号は、対応する要素を示している。スマートカード１０４にないものは、時間変数を格納するクロックカウンタ１１３である。パスワードの生成に含まれる他のすべての機能は、スマートカード１０４にインプリメントされている。

【００５１】

テスト１２１において、第１のユニット１０２によってキーパッドに個人識別番号又はＰＩＮを入れることでユーザが一度でも確認されていると、パーソナルコンピュータ１０６は、カウンタ１１３に格納された変数Ｔをスマートカード１０４へ送る。１２４において、Ｎｎ及びＴは連結又は図２に関して説明したように処理され、カード１０４内に例えば６４ビットの入力パラメータ又は質問を生成する。この質問は、１２５において、レジスタ１０９に格納された暗号化キーＫｎを使って実施されるアルゴリズムＡＬＧＯにより暗

号化される。

【００５２】

１２５において実施される暗号化は、１２６において、パスワードＡを生成し、このパスワードＡは、１３２において、パーソナルコンピュータ１０６の画面にフォーマットされて表示される。このパスワードＡは、図２に関して説明したように、サーバ又は第２のユニット１０３に送られる。もちろん、パーソナルコンピュータ１０６がモデムによってパスワードＡを直接第２のユニット１０３へ送るならば、パスワードＡはユーザに対して表示させる必要はない。

【００５３】

１２５においてなされる暗号化は、１２７においてＮｎの値の増分を生じさせて、新しい値Ｎｎ＋１がスマートカード１０４のレジスタ１０８に格納される。この増分は、上述したように、１の増分又は他の種類の増分とすることができる。増分された番号Ｎｎ＋１は、１２８において、上述した計算動作を受けて、第３の動的変数又は秘密の暗号化キーのための新しい値を計算する。

【００５４】

図５に示した、第１実施例の単純化バージョンは、イベントカウンタ及びキー導出、すなわちＴ以外の他の動的変数、静的なキーＫｎを省略したものとすることができる。図５において、図２と同じ符号に２００を加えた符号は、対応する要素を示すのに使用している。イベントカウンタ及びキー導出は別として、図５の動作は、図２及び図４の動作と同様であり、詳述はしない。

【００５５】

図１ないし図５の第１実施例にて示したスマートカードリーダ５は、受動的又は“ダム（dumb）”スマートカードリーダである。すなわち、スマートカード４とパーソナルコンピュータ６との間で単にデータを転送するだけのものである。さもなければ、スマートカードリーダ５は、能動的又は“インテリジェント”スマートカードリーダとすることができ、且つ携帯型とすることができる。このような“インテリジェント”スマートカードリーダの使用を指向した本発明の第２実施例は、図６に示される。

【００５６】

図６に示したように、第１のユニット３０２において、“インテリジェント”スマートカードリーダ３０５は、第１実施例のスマートカード３０４を読み取り、第２のユニット１３，１０３，２０３の様にすることができる第２のユニット３０３による使用に適用される。スマートカードリーダ３０５は、キーボード１０、ディスプレイスクリーン１１、レジスタ１３及びクロック１２に相当するキーパッド３１０、ディスプレイスクリーン３１１、レジスタ３１３及びクロック３１２を備え、それ自身、電池３５０のような電源を含んでいる。そのようなスマートカードリーダは、図２のパーソナルコンピュータ６、又は図４及び図５のパーソナルコンピュータ１０６，２０６のそれぞれのために示した機能を実行することができる。

【００５７】

上述のように、スマートカードリーダ３０５は、Ｔを与えるように構成することができ、スマートカード３０４は、図４及び図５に関して説明したように、第１のユニット３０２の他の演算を実行するように構成することができる。

【００５８】

あるいは、スマートカードリーダ３０５は、図２のパーソナルコンピュータ６と同じ演算を実行するように構成することができ、スマートカード３０４は、第１のユニット３０２の他の演算を実行するように構成することができる。さもなければ、上述のように、時間変数Ｔは、パーソナルコンピュータ３０６によってスマートカードリーダ３０５に与えられるようにして、リーダ３０５におけるクロック３１２の必要性をなくすことができる。

【００５９】

第１のユニット２，１０２，２０２のような第１のユニットは、携帯情報端末（ＰＤＡ：Personal Digital Assistant）、セルラー方式電話又は他のタイプの電話のように、その

装置が、図２、図４又は図５に示したように、スマートカードを読み取って実施するようにハードウェア、ソフトウェア、又はそれらの両方において構成されている限り、ユーザが所有する任意の装置に与えることができる。

【００６０】

本発明は、アルゴリズム及びキーが格納され、インプリメントされている場合に現在の時間を表す動的変数Ｔを生成しないので、従来例と区別される。従来は、アルゴリズム及びキーが格納される場合にクロック生成が実施されるような具体例を開示している。本発明は、パーソナルコンピュータ又はインテリジェントカードリーダによってスマートカードの外側で発生され、スマートカードに転送されて、スマートカードに格納されたキーを使ってパスワードを生成するための時間変数に基づいている。これは、たとえ、カード内の電源がまったく必要なくなったとしても、スマートカードで利用できるハードウェア及びソフトウェアのセキュリティ機構の利点と静的なパスワードよりも安全な時間依存性の動的パスワードの利点とを結合するので、有利である。また、一般には安全でないパーソナルコンピュータ、携帯情報端末、セルラー方式電話機などのような広く流通されている電子装置を使用して、時間依存性の動的パスワードを与えるスマートカードと協働して安全性の高い認証システムを提供することができるので、有利である。

【００６１】

本発明は、ここに詳細に示して説明したものに限定されるものではなく、特に、上述実施例に限定されるものではないことは、当業者には理解されよう。本発明の範囲内において、多少の他の変形を成すことは可能である。また、開示した変形は、別々に組み合わせることもできる。

【図面の簡単な説明】

【００６２】

【図１】本発明の第１実施例による認証システムの概略図である。

【図２】認証要求が処理されたときの本発明によるシステムにおける動作の展開の原理を示すフローチャートである。

【図３】パスワードの計算に使用される暗号化キーを計算するモードのフローチャートを示す。

【図４】図２に示した演算の別バージョンを示す。

【図５】図１に示した第１実施例を単純にしたバージョンを使ったパスワード計算に伴う演算のフローチャートを示す。

【図６】本発明の第２実施例を表したブロック図を示す。

【図１】

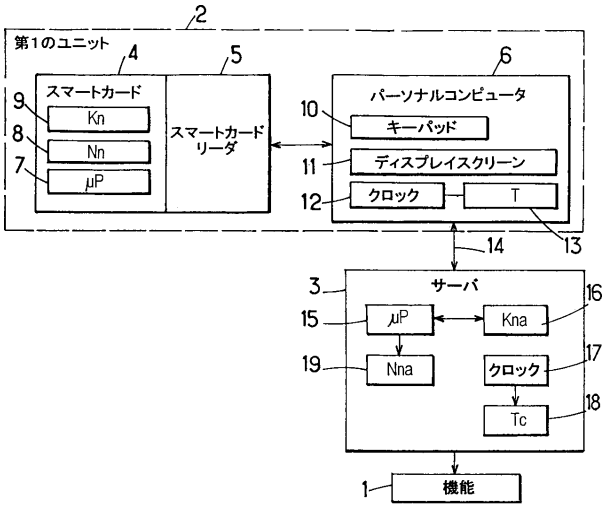


FIG.:1

【図３】

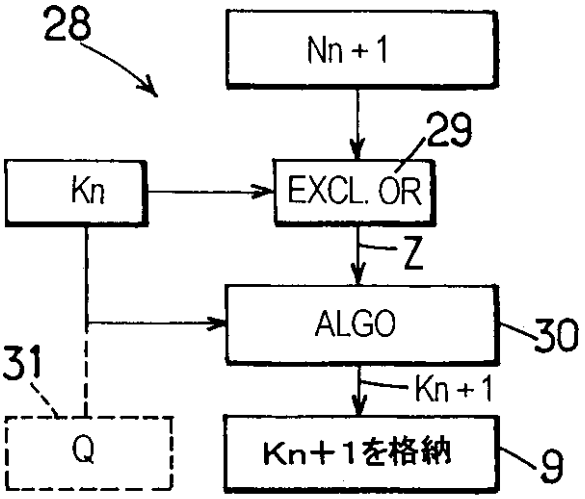
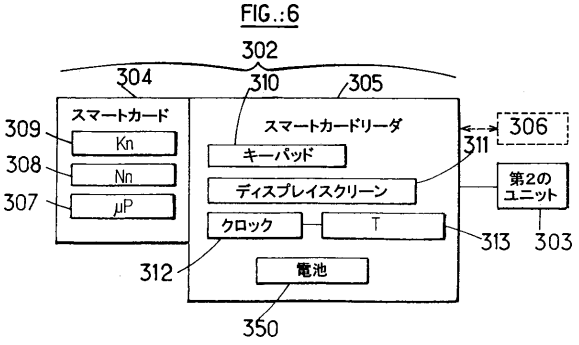


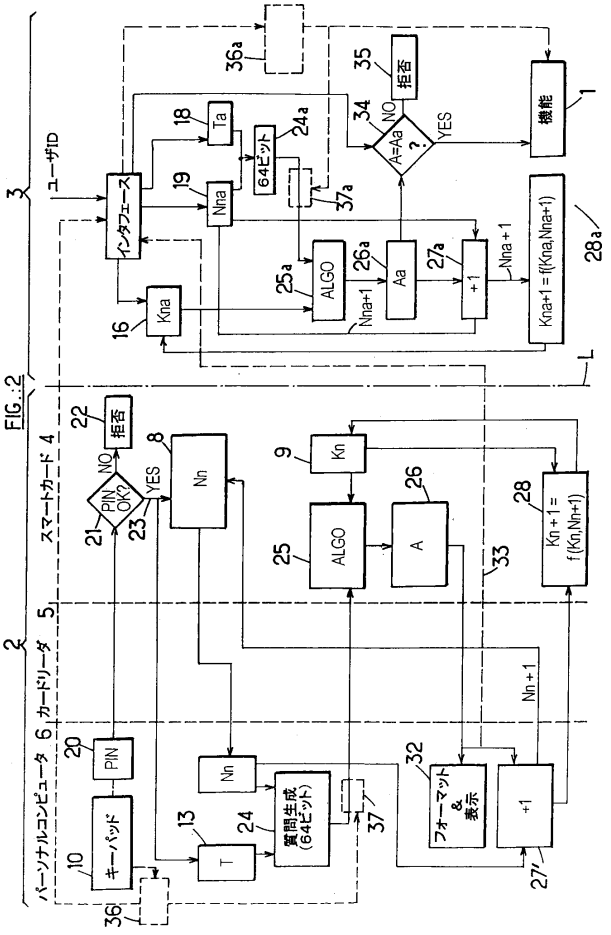
FIG.:3

【図６】

FIG.:6



【図２】



【図４】

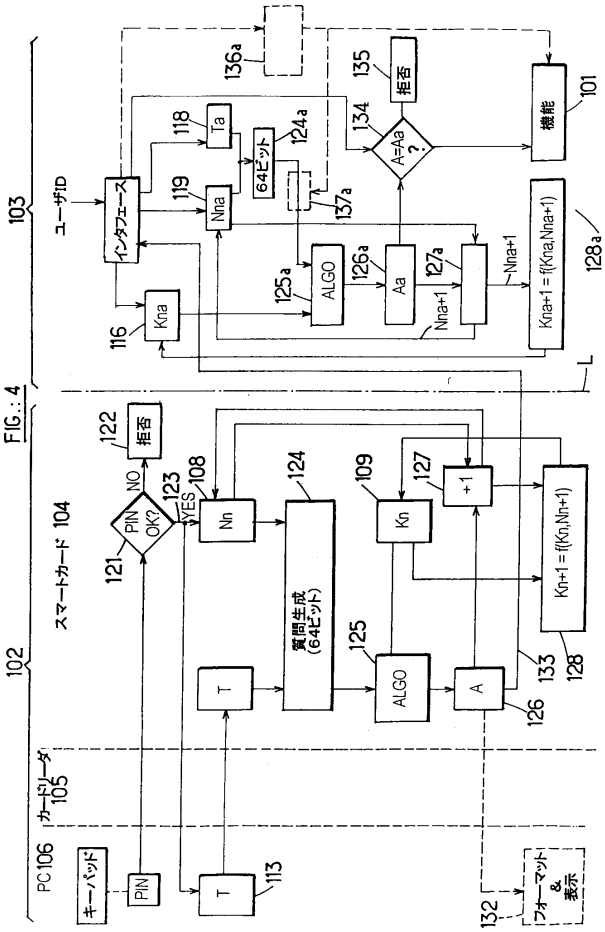


FIG.:4
102
103
スマートカード 104
カードリーダ 105
PC 106
ユーザID
インタフェース
Ta
Nna
64ビット
Kna
ALGO
Aa
Nna+1
Kna+1 = f(Kna,Nna+1)
A=Aa ?
拒否
機能
PIN
キーパッド
T
Nn
Kn
+1
Kn+1 = f(Kn,Nn+1)
A
PIN OK?
NO
YES
フォーマット & 表示

【図５】

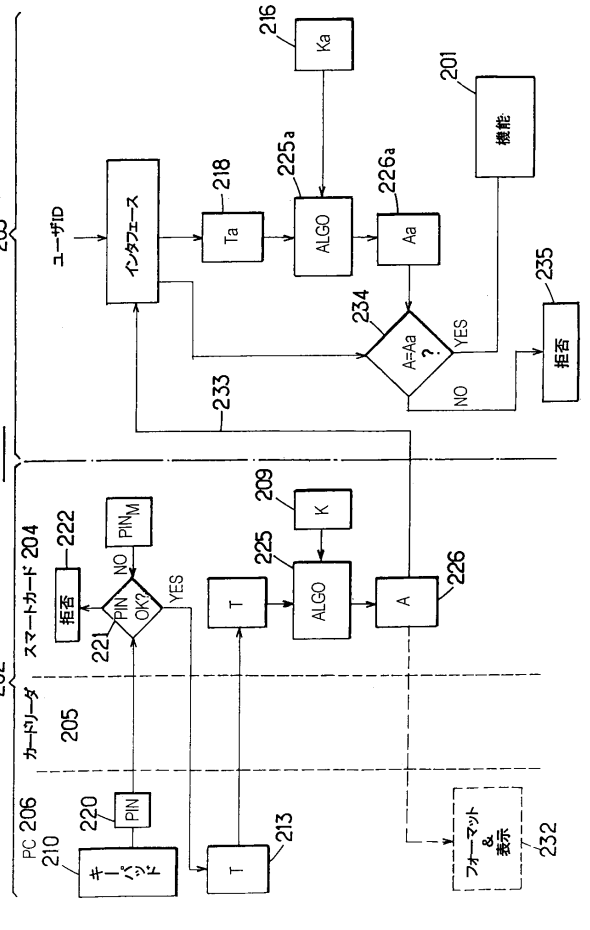


FIG.:5
202
203
スマートカード 204
カードリーダ 205
PC 206
ユーザID
インタフェース
Ta
ALGO
Aa
Ka
K
機能
A=Aa ?
YES
NO
拒否
PIN
PIN OK?
キーパッド
T
A
フォーマット & 表示

フロントページの続き

(56)参考文献 特開平０７－１０７０８６（ＪＰ，Ａ）
鈴木利則，スマートカードを用いた認証システムの開発とインターネットへの応用，情報処理学会研究報告 Ｖｏｌ．９５ Ｎｏ．１１５ IPSJ SIG Notes 95-OS-71，１９９５年１２月 １日，第95巻,第115号，p.25-p.30

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
G07F 7/10
H04L 9/32