(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-535903
(P2013-535903A)
(43)公表日　平成25年9月12日(2013.9.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	*(2006.01)*	H04L	9/00	675A	5J104
		H04L	9/00	673C	

審査請求 未請求　予備審査請求 未請求　（全 33 頁）

(21)出願番号	特願2013-520925 (P2013-520925)
(86)(22)出願日	平成23年7月18日 (2011.7.18)
(85)翻訳文提出日	平成25年3月19日 (2013.3.19)
(86)国際出願番号	PCT/AU2011/000904
(87)国際公開番号	WO2012/021918
(87)国際公開日	平成24年2月23日 (2012.2.23)
(31)優先権主張番号	2010903315
(32)優先日	平成22年7月23日 (2010.7.23)
(33)優先権主張国	オーストラリア(AU)

(71)出願人　307043108
エミュー　ホールディングス　ピーティワイ　リミテッド
オーストラリア国　３０００　ビクトリア州　メルボルン　バーク　ストリート　５５０　レベル　１９
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100111235
弁理士　原　裕子

最終頁に続く

(54)【発明の名称】暗号化装置及び方法

(57)【要約】
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するユーザ装置に入力される値を暗号化する方法が開示される。方法は、ユーザ装置がコード生成アルゴリズムを使用して認証キーを処理して、認証コードを生成するステップと、ユーザ装置が値確認コード生成アルゴリズムを使用して値を処理して、値確認コードを生成するステップとを含む。方法は、ユーザ装置が認証コード、値及び値確認コードを使用して、値を暗号化するメッセージを構築するステップを更に含み、メッセージは値を決定及び確認して、ユーザ装置及び／又はユーザを認証するために認証システムによって処理するために通信ネットワークを介して認証システムに伝達される。ユーザ装置に入力される値を認証システムに伝達し、且つ伝達された値を確認する方法、並びに関連するユーザ装置及び認証システムも開示される。

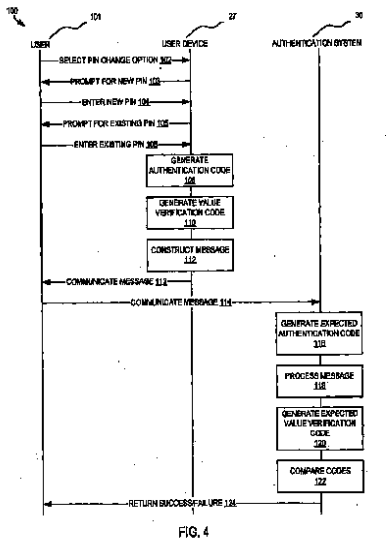

FIG. 4

【特許請求の範囲】
【請求項１】
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するユーザ装置に入力される値を暗号化する方法であって、
前記ユーザ装置が前記コード生成アルゴリズムを使用して前記認証キーを処理して、認証コードを生成するステップと、
前記ユーザ装置が前記値確認コード生成アルゴリズムを使用して前記値を処理して、値確認コードを生成するステップと、
前記ユーザ装置が前記認証コード、前記値及び前記値確認コードを使用して、前記値を暗号化するメッセージを構築するステップであって、前記メッセージは前記値を決定及び確認して、前記ユーザ装置及び／又は前記ユーザを認証するために前記認証システムによって処理するために通信ネットワークを介して認証システムに伝達されるステップと
を含む、方法。
【請求項２】
前記値確認コード生成アルゴリズムを使用して前記値を処理して値確認コードを生成するステップは、前記認証キー又は異なる秘密キーを処理することを更に含む、請求項１に記載の方法。
【請求項３】
前記認証コード、前記値及び前記値確認コードを使用して前記値を暗号化するメッセージを構築するステップは、少なくとも前記認証コード及び前記値を含む論理又は算術演算を実行することを含む、請求項１又は２に記載の方法。
【請求項４】
前記論理又は算術演算を実行することは、連結シーケンスを提供するために前記値及び値確認コードを連結すること、及びモジュラス演算を使用して前記認証コードを前記連結シーケンスに加算することを含む、請求項３に記載の方法。
【請求項５】
前記認証コード、前記値及び前記値確認コードは、Ｘ桁を含む数字の組からの数字のシーケンスを含み、前記モジュラス演算は、モジュラスＸ演算を含む、請求項４に記載の方法。
【請求項６】
前記認証コードは、ｎ桁シーケンスであり、前記値は、前記認証コードのシーケンス長よりも短いシーケンス長を有し、前記値確認コードは、前記認証コードのシーケンス長と前記値のシーケンス長との差に対応するシーケンス長を有する、請求項４又は５に記載の方法。
【請求項７】
前記認証コードの各数字は、前記連結シーケンスの各数字に別々に加算される、請求項６に記載の方法。
【請求項８】
前記コード生成アルゴリズムを使用して前記認証キーを処理して認証コードを生成するステップは、前記ユーザ装置のユーザによって入力されるPINを処理することを更に含む、請求項１～７の何れか１項に記載の方法。
【請求項９】
前記値確認コード生成アルゴリズムを使用して前記値を処理して値確認コードを生成するステップは、前記ユーザ装置のユーザによって入力されるPINを処理することを更に含む、請求項１～７の何れか１項に記載の方法。
【請求項１０】
前記値は、前記認証システムにおいて記憶される置換PINである、請求項１～９の何れか１項に記載の方法。
【請求項１１】
通信ネットワークを介して認証システムに伝達される値を確認する方法であって、前記

認証システムはユーザ装置と関係付けられる認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶しており、
前記認証システムがユーザ装置によって構築されるメッセージを受信するステップと、
前記認証システムが前記コード生成アルゴリズムを使用して前記認証キーを処理して、期待される認証コードを生成するステップと、
前記認証システムが前記期待される認証コードを使用して前記メッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
前記認証システムが前記値確認コード生成アルゴリズムを使用して前記受信した値を処理して、期待される値確認コードを生成するステップと、
前記認証システムが前記期待される値確認コードを前記受信した値確認コードと比較するステップと、
前記期待される値確認コードが前記受信した値確認コードと相関する場合に、前記受信した値を確認して、前記ユーザ装置及び／又は前記ユーザを認証するステップと
を含む、方法。
【請求項１２】
前記値確認コード生成アルゴリズムを使用して前記受信した値を処理して前記期待される値確認コードを生成するステップは、前記認証キー又は異なる秘密キーのいずれかを処理することを更に含む、請求項１１に記載の方法。
【請求項１３】
前記メッセージを処理するステップは、前記期待される認証コードを使用して論理又は算術演算を実行することを含む、請求項１１又は１２に記載の方法。
【請求項１４】
前記論理又は算術演算を実行することは、モジュラス演算を使用して前記メッセージの少なくとも一部から前記期待される認証コードを減算することを含む、請求項１３に記載の方法。
【請求項１５】
前記期待される認証コード及び前記メッセージは、Ｘ桁の組から選択される数字からなり、前記モジュラス演算は、モジュラスＸ演算を含む、請求項１４に記載の方法。
【請求項１６】
前記期待される認証コードの各数字は、前記メッセージの各数字から別々に減算される、請求項１５に記載の方法。
【請求項１７】
前記コード生成アルゴリズムを使用して前記認証キーを処理して期待される認証コードを生成するステップは、前記ユーザ装置と関係付けられ且つ前記認証システムに記憶されるPINを処理することを更に含む、請求項１１～１６の何れか１項に記載の方法。
【請求項１８】
前記値確認コード生成アルゴリズムを使用して前記受信した値を処理して期待される値確認コードを生成するステップは、前記ユーザ装置と関係付けられ且つ前記認証システムに記憶されるPINを処理することを更に含む、請求項１１～１６の何れか１項に記載の方法。
【請求項１９】
前記値は、前記認証システムにおいて記憶される、前記ユーザ装置と関係付けられる置換PINである、請求項１１～１８の何れか１項に記載の方法。
【請求項２０】
ユーザ装置に入力される値を通信ネットワークを介して認証システムに伝達する方法であって、前記ユーザ装置は、第１の認証キー、第１のコード生成アルゴリズム及び第１の値確認コード生成アルゴリズムを記憶し、前記認証システムは、第２の認証キー、第２のコード生成アルゴリズム及び第２の値確認コード生成アルゴリズムを記憶し、
前記ユーザ装置が前記第１のコード生成アルゴリズムを使用して前記第１の認証キーを処理して、認証コードを生成するステップと、

前記ユーザ装置が前記第１の値確認コード生成アルゴリズムを使用して前記値を処理して、値確認コードを生成するステップと、
前記ユーザ装置が前記認証コード、前記値及び前記値確認コードを使用して、前記値を暗号化するメッセージを構築するステップと、
前記メッセージを前記認証システムに伝達するステップと、
前記認証システムが前記メッセージを受信するステップと、
前記認証システムが前記第２のコード生成アルゴリズムを使用して前記第２の認証キーを処理して、期待される認証コードを生成するステップと、
前記認証システムが前記期待される認証コードを使用して前記メッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
前記認証システムが前記第２の値確認コード生成アルゴリズムを使用して前記受信した値を処理して、期待される値確認コードを生成するステップと、
前記認証システムが前記期待される値確認コードを前記受信した値確認コードと比較するステップと、
前記期待される値確認コードが前記受信した値確認コードと相関する場合に、前記受信した値を確認して、前記ユーザ装置及び／又は前記ユーザを認証するステップと
を含む、方法。
【請求項２１】
値を受信するための入力部と、
メッセージを出力するための出力部と、
プロセッサと、
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するメモリと、
前記プロセッサにアクセス可能なメモリに存在するソフトウェアであって、前記ユーザ装置に入力される値を暗号化する方法を実行するために前記プロセッサによって実行可能な一連の命令を含むソフトウェアと
を含むユーザ装置であって、前記方法は、
前記コード生成アルゴリズムを使用して前記認証キーを処理して、認証コードを生成するステップと、
前記値確認コード生成アルゴリズムを使用して前記値を処理して、値確認コードを生成するステップと、
前記認証コード、前記値及び前記値確認コードを使用して、前記値を暗号化するメッセージを構築するステップと、
前記メッセージを出力するステップであって、前記メッセージは前記値を決定及び確認して、前記ユーザ装置及び／又は前記ユーザを認証するために前記認証システムによって処理するために通信ネットワークを介して認証システムに伝達されるステップと
を含む、ユーザ装置。
【請求項２２】
前記出力は、ｎ桁ディスプレイであり、前記認証コードは、ｎ桁シーケンスであり、前記値は、前記認証コードのシーケンス長よりも短いシーケンス長を有し、前記値確認コードは、前記認証コードのシーケンス長と前記値のシーケンス長との差に対応するシーケンス長を有する、請求項２１に記載のユーザ装置。
【請求項２３】
前記出力は、ｎ桁ディスプレイであり、前記認証コード、前記値及び前記値確認コードの全ては、ｎ桁より短いシーケンス長を有する、請求項２１に記載のユーザ装置。
【請求項２４】
通信ポートと、
プロセッサと、
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するメモリと、

前記プロセッサにアクセス可能なメモリに存在するソフトウェアであって、方法を実行するために前記プロセッサによって実行可能な一連の命令を含むソフトウェアと
を含む認証システムであって、前記方法は、
メッセージを受信するステップと、
前記コード生成アルゴリズムを使用して前記認証キーを処理して、期待される認証コードを生成するステップと、
前記期待される認証コードを使用して前記メッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
前記値確認コード生成アルゴリズムを使用して前記受信した値を処理して、期待される値確認コードを生成するステップと、
前記期待される値確認コードを前記受信した値確認コードと比較するステップと、
前記期待される値確認コードが前記受信した値確認コードと相関する場合に、前記受信した値を確認して、前記ユーザ装置及び／又は前記ユーザを認証するステップと
を含む、認証システム。
【請求項２５】
請求項２１に記載のユーザ装置と、
請求項２４に記載の認証システムと
を含む、システム。
【請求項２６】
プロセッサ及びソフトウェアを記憶するための関連するメモリを含むユーザ装置で使用されるソフトウェアであって、請求項１～１０の何れか１項に記載の方法を実行するために前記プロセッサによって実行可能な一連の命令を含む、ソフトウェア。
【請求項２７】
プロセッサ及びソフトウェアを記憶するための関連するメモリを含む認証システムで使用されるソフトウェアであって、請求項11～19の何れか１項に記載の方法を実行するために前記プロセッサによって実行可能な一連の命令を含む、ソフトウェア。
【請求項２８】
請求項２６又は２７に記載のソフトウェアを保持する、コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、信頼できない又は安全でない通信ネットワーク上で通信するために、個人識別番号（personal identification number；PIN）等の値を暗号化する方法及び装置に関する。
【背景技術】
【０００２】
多くの電子認証システムにおいて、ユーザは、インターネットバンキング、オンラインショッピング、現金自動支払機、株式の取引、請求書の支払い、電子資金、電気通信サービス等のサービスへのアクセス、又は部屋若しくは車両へのアクセスの前に承認の証拠を提供することを要求される。承認の証拠は、ユーザがアクセスを許可される前に入力又はそれ以外で提供しなければならないパスワード若しくはPINの形式であってもよい。
【０００３】
ユーザは、悪意の第三者によって発見される可能性を少なくするために、自身のPINを秘密にして、それを定期的に変更するように忠告される。PINを変更する間の期間が長くなると、それが発見されて、サービス、部屋又は車両への非承認アクセスを得るために使用される可能性が高くなり得る。
【０００４】
通信ネットワーク上でPINを変更する方法の１つは、例えば、SSH（Secure Shell）プロトコルを使用して、セキュアトンネルを確立することを含み、ここで暗号化されていないデータは、ネットワーク上で暗号化されたトンネルを通じてサーバに伝送されてもよい。

しかしながら、この方法は、完全にプロセッサ集約型であり、トンネルを確立するのに通信リソースとオーバヘッドを必要とする。更に、セキュアトンネルは「介入者（man in the middle）」がPINを取得するのを防ぎ得るが、PINは、それにもかかわらずサーバによって検出されない「介入者」型攻撃により改ざん及び／又は干渉の影響を受けやすい。

【０００５】

要求される処理要件が少なく、「介入者」型攻撃の影響を受けにくいように、PIN等の値を伝達することが望ましいであろう。

【０００６】

背景技術の上記検討は、本発明の文脈を説明するために含まれている。参照された何れの文書又は他の素材も本明細書の請求項の何れか１つの優先日において刊行され、周知であり、又は慣用知識の一部であったと認められるべきではない。

【発明の概要】

【０００７】

一態様によれば、本発明は、認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するユーザ装置に入力される値を暗号化する方法であって、

ユーザ装置がコード生成アルゴリズムを使用して認証キーを処理して認証コードを生成するステップと、

ユーザ装置が値確認コード生成アルゴリズムを使用して値を処理して値確認コードを生成するステップと、

ユーザ装置が認証コード、値及び値確認コードを使用して値を暗号化するメッセージを構築するステップであって、メッセージは値を決定及び確認して、ユーザ装置及び／又はユーザを認証するために認証システムによって処理するために通信ネットワークを介して認証システムに伝達されるステップとを含む方法を提供する。

【０００８】

この方法は、セキュアトンネルを確立し及びそれを介して通信することと比較して、少ないプロセッサスループット又は通信リソース要求を使用して暗号化された値の通信を可能にし得る。暗号化されたデータパケット内の暗号化されていないデータを伝達する代わりに、本発明の実施形態では、データが暗号化されてもよく、この場合それは値である。少ないプロセッサスループットは、電力消費を減らして、低電力ユーザ装置での使用に特に適した方法を提供することが期待される。また、暗号化チャネルを使用してネットワーク上で非暗号化トラフィックを伝達するセキュアトンネルと異なり、本発明の実施形態は、信用できない又は安全でない通信チャネルを介して伝達される値を暗号化するメッセージを構築し得る。

【０００９】

本発明の実施形態は、「介入者（man in the middle）」型の攻撃の問題を解決し得る。例えば、攻撃者がメッセージを傍受した場合、値が攻撃者から隠されるだけでなく、攻撃者は認証システムへの伝送に確認可能な値を代用することもできないであろう。実際に、攻撃者が暗号化された値と関係付けられるメッセージの特定のビット又は要素の知識を持っていたとしても、値確認コードはメッセージによって暗号化される値から生成されるので、例えば、攻撃者が傍受したメッセージを改ざんすることによって異なる暗号化された値を代用して、これを認証システムに伝達しようした場合、攻撃者は、代用される値に対する有効な値確認コードを生成することができないであろう。

【００１０】

本発明の実施形態は、例えば、ユーザだけが知っているPINを含む値を伝達するメッセージを構築してもよい。例えば、ユーザが新たな又は代替のPINを選択する場合である。更に、メッセージは、ユーザ装置に対して一意の認証キーを処理することによって構築されるので、ユーザ装置及び／又はユーザを認証するための認証処理に使用可能な情報も含んでよい。言い換えれば、本発明の方法の実施形態は、値及び認証情報が認証システムによって導出され又は決定されるメッセージを構築してもよい。

【００１１】

ユーザ装置は、スマートカード、携帯電話、ハンドヘルドコンピュータ、ノートパッドコンピュータ、タブレットコンピュータ、デスクトップコンピュータ、PDA（personal digital assistant）、又は任意の他の適切な装置を含んでもよい。

【００１２】

値は、例えば、パスワード、PIN、クレジットカード番号、他の数字、文字列、文字、配列、データ構造、又は任意の他のデータを含んでもよい。値がPINである場合、PINは、既存のPIN（「古いPIN」）を置換するために認証システムに伝達される代替の又は新たなPIN（「新たなPIN」）を含んでもよい。ユーザは、新たなPINを選択してユーザ装置に入力してもよい。攻撃者がメッセージを傍受した場合、新たなPINは、攻撃者から隠されるであろう。更に、攻撃者が認証システムに代わりの代替PINを送信しようとした場合、攻撃者は、認証キーへのアクセス無しで代わりの代替PINを有効に暗号化することができないであろう。更に、攻撃者が認証システムに異なるメッセージを送信した場合、メッセージは無効な値確認コードを含むことになるので、新たなPINは認証システムで確認及び更新されないであろう。この点に関して、万一攻撃者が有効な値確認コードを推定したとしても、攻撃者は、認証キーを知らずに認証システムに記録された新たなPINを推定することができないであろう。

【００１３】

認証キーは、好ましくは、認証システムと共有される対称キー等の秘密キーである。認証キーは、例えば、256ビットバイナリコード等のシード、コード又はデータシーケンスを含んでもよい。認証キーは、固定又は静止キーであってもよく、又は、それは、認証コード生成アルゴリズムの反復ごとに又は場合によっては既定の期間の経過後に更新されるワンタイム使用可能キーを含んでもよい。

【００１４】

ユーザ装置は、適切な通信チャネルを介して認証システムにメッセージを伝達してもよく、又は、それは、別の手段を介して、例えば、通信ネットワークを介して認証システムに構築されたメッセージを伝達するように適合される通信端末等の、異なる装置にユーザがメッセージを入力することによって、認証システムに伝達される出力としてメッセージを構築してもよい。

【００１５】

ユーザ装置が認証システムにメッセージを伝達する実施形態では、ユーザ装置は、認証システムに直接に又は適切なデータ通信ネットワークを介して認証システムとデータ通信するネットワークノードを介して間接的に構築されたメッセージを伝達する有線及び／又は無線通信インターフェースを含んでもよい。

【００１６】

認証システムへの通信のための通信端末等の装置へのユーザ入力のためにユーザ装置がユーザにメッセージを出力する実施形態では、ユーザ装置は、有線及び／又は無線通信インターフェースを含む必要はないが、その代わりに、ユーザにメッセージを出力するためにディスプレイ等のユーザインターフェースを含んでもよい。例えば、適切なユーザインターフェースは、ディスプレイ（LED又はLCDディスプレイ等）又は音声出力インターフェースを含んでもよい。更に別の実施形態では、ユーザ装置は、ユーザにメッセージを出力するために第２のユーザ装置等の中間通信装置に構築されたメッセージを伝達して、それからユーザが認証システムに入力し、そうでなければ構築されたメッセージを伝達するための有線及び／又は無線通信インターフェースを含んでもよい。例として、ユーザ装置は、携帯電話、ハンドヘルドコンピュータ、ノートパッドコンピュータ、タブレットコンピュータ、デスクトップコンピュータ又はPDA（personal digital assistant）等の第２のユーザ装置へのSMS（short message service message）、Ｅメールメッセージ又はインスタントメッセージングサービス等の電子データ通信で、携帯電話等の第２のユーザ装置に構築されたメッセージを伝達するための電子データ通信インターフェースを含んでもよい。

【００１７】

上記の有線通信インターフェースに関して、適切な有線通信インターフェースは、例えば、USBインターフェース、IEEE802.3インターフェース、SPI（serial peripheral interface bus）インターフェース、又は接触型スマートカードインターフェース等を含んでもよい。他の適切な有線通信インターフェースが熟練した受信者には周知であろう。適切な無線通信インターフェースは、例えば、磁気ストライプインターフェース、光学インターフェース、IEEE802.11無線インターフェース、Bluetooth（登録商標）インターフェース、ZigBee（登録商標）インターフェース、無線USB、又は非接触型スマートカードインターフェース等を含んでもよい。他の適切な無線通信インターフェースが熟練した受信者には周知であろう。

【００１８】

認証コードを生成するためにコード生成アルゴリズムを使用して認証キーを処理することは、好ましくは、適切なハッシュ関数を認証キーに、場合によっては認証キー及び他のデータを伴う論理関数の結果に適用することによって、認証キーをｎ桁認証コードに変換する符号化処理を含む。適切なハッシュ関数は、例えば、MD5、SHA-1、SHA-224、SHA-256、SHA-384又はSHA-512を含んでもよい。理解されるように、ハッシュ関数は、この場合、認証キー又は認証キー及び他のデータを伴う論理演算の結果のいずれかである入力を変換して、固定長ハッシュ値出力を提供する。

【００１９】

コード生成アルゴリズムが認証キー及び他のデータを伴う論理演算の結果を入力として取るハッシュ関数を適用する場合、適切な論理演算は、例えば、XOR論理演算を含んでもよい。しかしながら、他の論理演算が使用されることも可能である。他のデータは、同期カウンタ値、及び／又は識別コード（古いPIN等）、及び／又はユーザ装置に関するモード情報等のデータ値を付加することによって形成されてもよい。同期カウンタ値は、認証処理後にユーザ装置及び認証システムにおいて新たな認証キーを生成又は更新するために認証システムにおける対応するカウンタと同期されるカウント値であってもよい。認証キーを伴う論理演算と共に他のデータ内に識別コードを含むことは、正しいユーザがユーザ装置を使用していることを確実にするのを支援してもよい。

【００２０】

一実施形態では、ユーザは、方法を実行するようにユーザ装置を起動するためにユーザ装置に古いPINを入力（input or enter）することを要求される。

【００２１】

値確認コードを生成するために値確認コード生成アルゴリズムを使用して値を処理することは、好ましくは、ユーザ装置のユーザによって入力（input or enter）される古いPIN等の、値に、場合によっては値及び他のデータを伴う論理演算の結果に適切なハッシュ関数を適用することによって、値をｍ桁値確認コードに変換する符号化処理を含む。従って、古いPINは、認証コード生成アルゴリズム及び値確認コード生成アルゴリズムに使用されてもよい。値確認コードを生成するために使用される論理演算は、認証キー又は実際に異なる秘密キーを伴ってもよい。従って、値確認コードの生成に古いPIN及び／又は認証キーを伴う実施形態は、値を確認して（認証キーを介して）ユーザ装置及び／又は（古いPINを介して）ユーザを認証するために認証システムによって処理され得る値確認コードを生成してもよい。従って、値確認コードによって、即ち、値を確認してユーザ装置及び／又はユーザを認証することによって、２つの目的が果たされてもよい。

【００２２】

値を暗号化するメッセージを構築するために認証コード、値及び値確認コードを使用することは、少なくとも認証コード及び値を含む論理又は算術演算を実行することを含んでもよい。しかしながら、一部の実施形態では、論理又は算術演算は、値確認コードを更に伴ってもよい。

【００２３】

論理又は算術演算は、値及び値確認コードを連結して値及び値確認コードを含む連結結果を形成し、それからモジュラス演算を使用して連結結果に認証コードを加算することを

含んでもよい。この場合、連結結果に認証コードを加算することによって、値及び値確認コードを暗号化するメッセージが構築される。

【００２４】

好ましくは、認証コード、値及び値確認コードは、可能なX桁の数字の組から個々の数字のシーケンスとしてそれぞれ形成される。これに関して、本明細書を通じて使用される場合に、「数字（digit）」という用語は、数字、文字又はシンボル等を示すものであることが理解されるべきである。数字が複数のバイナリビットを使用して表されてもよいことが理解されるであろう。例えば、「９」という数字は、バイナリで「1001」として表されてもよい。この例示では、数字は、「０」から「９」の１０個の数字の組から選択される「９」という数である。可能なX桁の数字の組は、ASCII文字セット（言い換えれば、異なる数字１２８個の数字の組）、拡張ASCII文字セット（言い換えれば、異なる数字２５５個の数字の組）、又はASCII文字のサブセットを含んでもよい。この場合、各数字は、８ビットバイナリシーケンス、又は２文字バイナリ化１０進シーケンスとして表されてもよい。

【００２５】

個々の数字のシーケンスが可能な数字Xの数字の組からの数字を含み、メッセージを構築するためにモジュラス演算が使用される実施形態では、モジュラス演算は、モジュラスX演算を使用してもよい。モジュラスX演算を使用することは、一意の可逆的（即ち、復号可能）メッセージが暗号化された値ごとに構築されることを確実にしてもよい。言い換えると、暗号化された値は、メッセージによって暗号化された値を回復又は再構築するために一意に復号可能であってもよい。従って、同じ認証コードを使用してメッセージを構築することによって暗号化される２つの異なる値は、異なる一意で可逆的な構築されたメッセージを生ずるであろう。

【００２６】

一実施形態では、構築されたメッセージは、N桁メッセージであるので、N桁の「長さ」を有する。認証コードは、構築されたメッセージのそれと同じ又はより短い長さを有してもよい。従って、例えば、認証コードは、ｎ＝Ｎであるｎ桁コードを含んでもよい。

【００２７】

好ましくは、値は、認証コードの長さよりも短い長さを有し、値確認コードは、値と値確認コードとの結合された長さが認証コードの長さに対応するように認証コードの長さと値の長さの差に対応する長さを有する。このようにして、適切な算術又は論理演算を選択することによって、構築されたメッセージは、認証コードの長さと対応する長さを有してもよく、また構築されたメッセージの各数字は、値又は値確認コードのいずれかの個々の数字を暗号化してもよい。例えば、認証コードがｎ桁の長さを有すると仮定すると、構築されたメッセージもｎ桁の長さを有してもよく、ｎ桁は値を暗号化するｉ桁及び値確認コードを暗号化するｍ桁を含んでおり、ｎ＝ｉ＋ｍである。この例示では、メッセージの長さが値及び値確認コードの結合された長さに対応しており、同じ桁数を有するので、認証コードにおける各数字は、値及び値確認コードを隠すメッセージを構築するための連結されたシーケンスの個々の数字と共に別個の算術演算（加算又は減算等）に関与してもよい。代替的に、メッセージは、認証コード、及び連結された値及び値確認コードを含む論理演算（XOR論理演算等）を実行することによって構築されてもよい。

【００２８】

別の代替では、値を暗号化するメッセージを構築するために認証コード、値及び値確認コードを使用することは、値を暗号化するために認証コード及び値のみを使用して、それからメッセージの構築を遂行するために値確認コードを暗号化された値に付加する論理又は算術演算を実行することを伴ってもよい。この代替では、値確認コードは暗号化されなくてもよい。この場合、論理又は算術演算を実行することは、例えば、認証コード及び値のみを伴うモジュラス算術演算を含む算術演算を含んでもよい。上記のように、認証コード及び値は、Ｘ桁を含む数字の組からの数字のシーケンスを含んでもよく、モジュラス演算は、モジュラスＸ演算を使用してもよい。この実施形態では、例えば、認証コードにお

ける各数字がモジュラス演算を使用して値の各数字に別々に加算されることで値を暗号化するメッセージを構築するように、認証コード及び値が同じ長さを有することが好ましい。この場合、値を暗号化するメッセージは、値を暗号化する部分及び値確認コードを含む非暗号化部分を含むであろう。

【００２９】

メッセージを構築する他の方法も可能である。例えば、認証コードを連結シーケンス又は値に加える代わりに、メッセージを構築することは、認証コードから連結シーケンス又は値のいずれかを減算すること又はその逆を伴ってもよい。加算又は減算の代わりに、メッセージは、認証コード、値及び値確認コード、又は認証コード及び値、又はこれらのバイナリ若しくは他の表現を伴うバイナリXOR演算（排他的OR）等の論理演算の結果として構築されてもよい。例えば、値及び値確認コードのバイナリ表現が連結されてもよく、結果として生ずる連結シーケンスがメッセージを構築するために認証コードのバイナリ表現でＸＯＲされてもよい。別の例示では、値のバイナリ表現は、論理結果を提供するためにバイナリXORを使用して認証コードのバイナリ表現と結合されて、値確認コードがその結果に付加されてもよい。例えば、異なる論理又は算術演算を使用してメッセージを構築する他の方法も可能であることが理解されるであろう。

【００３０】

認証システムによってメッセージを受信すると、認証システムは、メッセージを構築するためにユーザ装置によって使用されるのと同じ認証キー及びコード生成アルゴリズムを処理することによって期待される認証コードを生成する。次に、認証システムは、メッセージを構築するためにユーザ装置によって実行されたものに逆の論理及び／又は算術演算を適用することによってメッセージに含まれる値及び値確認コードを決定又は導出する。次に、認証システムは、メッセージから決定又は導出された値確認コードと比較される期待される値確認コードを生成するために同じ値確認コード生成アルゴリズムを使用して決定又は導出された値を処理する。導出された値確認コードが期待される値確認コードと一致する場合、これは、値を確認して、値を暗号化するために使用される認証コードが正確であったことを示すので、ユーザ装置及び／又はユーザを認証する。

【００３１】

また、一部の実施形態では、ユーザ装置及び／又はユーザを識別する情報は、メッセージの中で又はメッセージとは独立して認証システムに伝達されてもよい。例えば、認証システムが複数のユーザ装置を認証する場合、識別情報は、認証コードを生成するためにユーザ装置がどの認証キーを使用すべきであったかを決定するために使用されてもよい。

【００３２】

また、方法は、構築されたメッセージを認証システムに伝達する前に、ユーザ装置及び／又はユーザに対して認証システムを認証することを含んでもよい。このようにして、ユーザは、メッセージを認証サーバに伝達する前に認証システムの真正性を確認することが可能であってもよい。方法は、例えば、

ユーザ装置が、サーバ認証キーに基づいて応答生成アルゴリズムを使用して認証システムにおいて生成された認証応答を受信することであって、この応答はユーザ及び／又はユーザ装置から認証要求を受信することに応答して生成されること、

ユーザ装置が、同じ応答生成アルゴリズムを使用して、サーバ認証キーに基づいて期待される認証応答を生成すること、

ユーザ装置が、認証応答と期待される認証応答とを比較すること、及び

予測される認証応答が受信した認証応答と相関する場合に、暗号化のための値を入力するようにユーザを促すことを含んでもよい。

【００３３】

サーバ認証キーは、値を暗号化するために使用される認証キーと同じであってもよく、又はそれは異なるキーであってもよい。同様に、応答生成アルゴリズムは、コード生成アルゴリズムと同じであってもよく、又はそれは異なるアルゴリズムであってもよい。

【００３４】

別の態様によれば、本発明は、通信ネットワークを介して認証システムに伝達される値を確認する方法であって、認証システムはユーザ装置と関係付けられる認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶しており、
認証システムがユーザ装置によって構築されるメッセージを受信するステップと、
認証システムがコード生成アルゴリズムを使用して認証キーを処理して、期待される認証コードを生成するステップと、
認証システムが期待される認証コードを使用してメッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
認証システムが値確認コード生成アルゴリズムを使用して受信した値を処理して、期待される値確認コードを生成するステップと、
認証システムが期待される値確認コードを受信した値確認コードと比較するステップと、
期待される値確認コードが受信した値確認コードと相関する場合に、受信した値を確認して、ユーザ装置及び／又はユーザを認証するステップとを含む方法を提供する。

【００３５】
方法は、認証システムが単一のメッセージを処理することによって受信した値を確認してユーザ装置及び／又はユーザを認証することの双方を可能にしてもよい。

【００３６】
認証システムは、異なるユーザ装置と関係付けられる複数の認証キーを記憶してもよい。ラベル等の認証システムに送信される更なる情報が、どの認証キーがユーザ装置及び／又はユーザと関係付けられるべきかを決定するために使用されてもよい。例として、ラベルは、クレジットカード番号、アカウント番号、又はユーザ名等を含んでもよい。

【００３７】
値確認コード生成アルゴリズムを使用して受信した値を処理して期待される値確認コードを生成するステップは、認証キー又は異なる秘密キーのいずれかを処理することを更に含んでもよい。この場合、予想される値確認コードは、ユーザ装置が正確なキーを使用した場合に限り、受信した値確認コードと相関するであろう。従って、値確認コードは、２つの目的、即ち、値を確認すること及びユーザ装置及び／又はユーザを認証することを果たすであろう。この点で、期待される値確認コードと受信した値確認コードとの「相関」は、２つの値が同一であるか、期待される関係を有することを意味してもよい。

【００３８】
メッセージを処理することは、期待される認証コードを使用して論理又は算術演算を実行することを含んでもよい。論理又は算術演算を実行することは、モジュラス演算を使用してメッセージの少なくとも一部から期待される認証コードを減算することを含んでもよい。

【００３９】
認証コードは、メッセージ全体から減算されてもよく、又は値確認コードが暗号化されたPINに付加されている場合、値確認コードは、認証コードを減算する前にメッセージから除去（de-append）されてもよい。

【００４０】
期待される認証コード及びメッセージは、可能なＸ桁を含む数字の組から選択される数字からなってもよい。また、モジュラス演算は、モジュラスＸを使用してもよい。一実施形態では、期待される認証コードの各数字は、モジュラス演算を使用してメッセージの各数字から別個に減算されてもよい。

【００４１】
正しいユーザがユーザ装置を操作していることを確実にするために、コード生成アルゴリズムを使用して認証キーを処理して期待される認証コードを生成するステップは、ユーザ装置と関係付けられ且つ認証システムに記憶されるPINを処理することを更に含んでもよい。ユーザ装置の側において、正しい認証コードを生成するために、ユーザは、正しいPINを入力する必要があるであろう。

【００４２】
同様に、値確認コード生成アルゴリズムを使用して受信した値を処理して期待される値確認コードを生成するステップは、ユーザ装置と関係付けられ且つ認証システムに記憶されるPINを処理することを更に含んでもよい。同じPINが、コード生成アルゴリズム及び値確認コード生成アルゴリズムの双方に使用されてもよい。
【００４３】
上記のように、値は、認証システムにおける記憶のための、ユーザ装置と関係付けられる代替の又は新たなPINであってもよい。また、メッセージが伝達される前にユーザ装置が認証システムを認証できるように、方法は、メッセージを受信する前に、
認証システムが、ユーザ装置と関係付けられる認証要求を受信すること、
認証システムが、認証キーに基づいて応答生成アルゴリズムを使用して認証応答を生成すること、
認証システムが、認証応答を要求側に伝達することを含んでもよい。
【００４４】
要求側は、ユーザ装置又はネットワーク接続されたコンピュータ等の別の装置を含んでもよい。
【００４５】
本発明の実施形態の別の態様によれば、ユーザ装置に入力される値を通信ネットワークを介して認証システムに伝達する方法であって、ユーザ装置が、第１の認証キー、第１のコード生成アルゴリズム及び第１の値確認コード生成アルゴリズムを記憶し、認証システムが、第２の認証キー、第２のコード生成アルゴリズム及び第２の値確認コード生成アルゴリズムを記憶する方法が提供される。この方法は、
ユーザ装置が第１のコード生成アルゴリズムを使用して第１の認証キーを処理して、認証コードを生成するステップと、
ユーザ装置が第１の値確認コード生成アルゴリズムを使用して値を処理して、値確認コードを生成するステップと、
ユーザ装置が認証コード、値及び値確認コードを使用して、値を暗号化するメッセージを構築するステップと、
メッセージを認証システムに伝達するステップと、
認証システムがメッセージを受信するステップと、
認証システムが第２のコード生成アルゴリズムを使用して第２の認証キーを処理して、期待される認証コードを生成するステップと、
認証システムが期待される認証コードを使用してメッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
認証システムが第２の値確認コード生成アルゴリズムを使用して受信した値を処理して、期待される値確認コードを生成するステップと、
認証システムが期待される値確認コードを受信した値確認コードと比較するステップと、
期待される値確認コードが受信した値確認コードと相関する場合に、受信した値を確認して、ユーザ装置を認証するステップとを含む。
【００４６】
別の態様によれば、本発明は、
値を受信するための入力部と、
メッセージを出力するための出力部と、
プロセッサと、
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するメモリと、
プロセッサにアクセス可能なメモリに存在するソフトウェアであって、ユーザ装置に入力される値を暗号化する方法を実行するためにプロセッサによって実行可能な一連の命令を含むソフトウェアとを含むユーザ装置を提供する。この方法は、

コード生成アルゴリズムを使用して認証キーを処理して、認証コードを生成するステップと、
値確認コード生成アルゴリズムを使用して値を処理して、値確認コードを生成するステップと、
認証コード、値及び値確認コードを使用して、値を暗号化するメッセージを構築するステップと、
メッセージを出力するステップであって、メッセージは値を決定及び確認して、ユーザ装置を認証するために認証システムによって処理するために通信ネットワークを介して認証システムに伝達されるステップとを含む。

【００４７】

ソフトウェアは、上記の方法の任意のステップを更に実行してもよい。一実施形態では、ユーザ装置は、出力としてｎ桁ディスプレイを含むスマートカードを含む。この実施形態では、認証コードは、ｎ桁シーケンスであってもよく、値は、認証コードのシーケンス長よりも短いシーケンス長を有してもよく、値確認コードは、認証コードのシーケンス長と値のシーケンス長との差に対応するシーケンス長を有してもよい。この実施形態は、ディスプレイで全ての数字を使用しつつ、値を暗号化するのに必要とされる処理能力を低減させてもよい。認証コード、値及び値確認コードは、全てｎ桁より短いシーケンス長を有してもよい。

【００４８】

別の態様によれば、本発明は、
通信ポートと、
プロセッサと、
認証キー、コード生成アルゴリズム、及び値確認コード生成アルゴリズムを記憶するメモリと、
プロセッサにアクセス可能なメモリに存在するソフトウェアであって、方法を実行するためにプロセッサによって実行可能な一連の命令を含むソフトウェアとを含む認証システムを提供する。この方法は、
メッセージを受信するステップと、
コード生成アルゴリズムを使用して認証キーを処理して、期待される認証コードを生成するステップと、
期待される認証コードを使用してメッセージを処理して、受信した値及び受信した値確認コードを決定するステップと、
値確認コード生成アルゴリズムを使用して受信した値を処理して、期待される値確認コードを生成するステップと、
期待される値確認コードを受信した値確認コードと比較するステップと、
期待される値確認コードが受信した値確認コードと相関する場合に、受信した値を確認して、ユーザ装置及び／又はユーザを認証するステップとを含む。

【００４９】

ソフトウェアは、上記の方法の任意のステップを更に実行してもよい。また、本発明は、上記のユーザ装置及び認証システムを含むシステム、上記の方法の何れか１つを実行するためにプロセッサによって実行可能な一連の命令を含むソフトウェア自体、及びソフトウェアを含むコンピュータ可読媒体にまで及ぶ。

【００５０】

本発明の実施形態は、単に例示を目的として、添付の図面を参照して以下に説明されるであろう。図面の特殊性が上述した本発明の一般性に取って代わるものではないことが理解されるべきである。

【図面の簡単な説明】

【００５１】

【図１】本発明の実施形態による認証システム及びユーザ装置を含む例示的なネットワークの概略図である。

【図２】図１の認証システムの低レベルブロック図である。
【図３】図１のユーザ装置の低レベルブロック図である。
【図４】図３のユーザ装置において値を暗号化して、図２の認証システムにおいてその値を確認する方法の実施形態の流れ図である。
【図５】認証システムを認証する方法の実施形態の流れ図である。
【発明を実施するための形態】
【００５２】
（ネットワークの例）
本発明の実施形態は、図１に例が示されている通信ネットワーク上で実現され得る。図１に示されたネットワーク20は、１つ以上のユーザ装置及び１つ以上の認証システムを含む。この例示では、ユーザ装置は、パーソナルコンピュータ（ＰＣ）22及び24、スマートカード26及び27、並びにハンドヘルド装置28を含む。認証システムは、サーバ30及び32を含む。図示のように、ユーザ装置22から28及び認証システム30、32は、通信ネットワーク34を介して電子データ通信をサポートするために接続される。
【００５３】
ネットワーク34上のデータ伝送は、有線又は無線のデータ通信を含んでもよい。認証システム30及び32は、ネットワーク34、並びに各データベース36及び38等の１つ以上のデータベース上でのデータ伝送を容易にし得る。
【００５４】
本発明の実施形態は、MAN（metropolitan area network）、WAN（wide area network）、LAN（local area network）又は他のインターネット等の異なるネットワーク上で実現されてもよいことが理解されるであろう。また、一部の実施形態は完全にユーザ装置又は認証システムで行われ得るので、実施形態は、必ずしもネットワーク上で行われる必要はない。
【００５５】
（認証システムの例）
図２は、本発明の実施形態による認証システム30のブロック図を示す。認証システム30は、プロセッサ42、メモリ44、少なくとも１つの入力装置46、少なくとも１つの出力装置48、通信ポート50及び記憶装置54を含む。図示のように、認証システム30の構成要素は、バス、又はデータ、アドレス及び／若しくは制御バス等の一群のバス56を介して結合される。
【００５６】
プロセッサ42は、例えば、認証システム30内の異なる機能を処理するために１つ以上の処理装置を含んでもよい。メモリ44は、任意の適切なメモリ装置を含み、例えば、揮発性又は不揮発性、ソリッドステート記憶装置、磁気装置等を含んでもよい。メモリ44は、プロセッサ42によって実行されるコンピュータソフトウェアプログラム62を記憶する。
【００５７】
この実施形態では、メモリ44は、少なくとも１つの認証キー64も記憶する。多数の認証キーがメモリ44又はデータベース59に記憶されてもよく、各認証キーは異なるユーザ装置と関係付けられる。例えば、認証システム30が金融機関向けである場合、各認証キー64は、特定のアカウント、又はアカウント保持者と関係付けられてもよい。
【００５８】
代替的に、認証キー64は、認証システム30の外部に記憶されてもよく、通信ネットワーク34を介して認証システム30にアクセス可能であってもよい。
【００５９】
また、メモリ44は、認証コードを生成するためのコード生成アルゴリズム66、及び値確認コードを生成するための値確認コード生成アルゴリズム68を記憶する。こうしたアルゴリズム及び認証キーの更なる詳細が以下に与えられるであろう。
【００６０】
入力装置46は、入力データ58を受信し、例えば、キーボード、マウス又は他のポインタ

装置、トラックボール、ジョイスティック又はタッチスクリーン、マイクロホン、モデム又は無線データアダプタ等のデータ受信機又はアンテナ、データ収集カード等を含んでもよい。入力装置46は、入力データ58を入力するためにユーザによって操作可能であってもよい。又は、それは、別の入力データソースからデータを受信してもよい。

【００６１】

出力装置48は、出力データ60を作成又は生成する。出力装置48は、ディスプレイ装置、一組のオーディオスピーカ、プリンタ、ポート（例えば、USBポート）、周辺構成要素アダプタ、モデム又は無線ネットワークアダプタ等のデータ送信機又はアンテナ等を含んでもよい。

【００６２】

記憶装置54は、任意の形式のデータ又は情報記憶手段、例えば、揮発性又は不揮発性メモリ、ソリッドステート記憶装置、磁気装置を含み得る。ファイルシステム及びファイルが記憶装置54に記憶されてもよい。記憶装置54は、少なくとも１つのデータベース59を収容してもよい。

【００６３】

通信ポート50によって、認証システム30は、ネットワーク34等の有線又は無線ネットワークを介して他の装置と通信することができる。適切な通信ポートは、IEEE802.11型の無線インターフェース、GPRS（general packet radio service）互換インターフェース、WAP（wireless application protocol）互換インターフェース、Bluetooth（登録商標）インターフェース、光学インターフェース（IrDAインターフェース等）、ZigBeeインターフェース、USB（universal serial bus）インターフェース等、又はRFID（adio frequency identification）誘導型の通信インターフェースを使用してもよい。

【００６４】

使用時、認証システム30は、データが通信ポート50を介してデータベース59に記憶され及び／又はデータベース59から取得されることを可能にするように適合され得る。

【００６５】

認証システム30は、任意の形態の端末、サーバ処理システム、専用ハードウェア、コンピュータ、コンピュータシステム又はコンピュータ化装置、パーソナルコンピュータ（PC）、移動式又は携帯電話、移動式データ端末、携帯型コンピュータ、PDA（Personal Digital Assistant）、ページャ、スマートカード又は任意の他の種類の装置を含んでもよい。

【００６６】

（ユーザ装置の例）

図3は、本発明の実施形態によるユーザ装置27のブロック図を示す。図示のように、この例では、ユーザ装置27は、キーパッド70の形態の入力、ディスプレイ72の形態の出力、プロセッサ74、メモリ76及び電力供給78を含むスマートカードである。

【００６７】

この例では、キーパッド70は、０から９の数字、並びにユーザ装置27の動作の選択及び制御を行うための２つの追加ボタンを含む１２ボタン式キーパッドである。ユーザは、キーパッド70を使用してユーザ装置27にPIN等の値を入力してもよい。ディスプレイ72は、８桁英数字LCDディスプレイである。

【００６８】

プロセッサ74は、メモリ76に存在するコンピュータソフトウェアプログラム80を実行するためのマイクロプロセッサ又はマイクロコントローラである。適切なプロセッサ74の例は、6502、ARM、Motorola6800、Texas Instruments MSP430である。電力供給78は、プロセッサ74及びユーザ装置27の他の機能的要素に電源を供給するために、バッテリ又は誘導コイルを含んでもよい。

【００６９】

メモリ76は、プロセッサ74に搭載されたROM（read-only memory）（例えば、EPROM又はEEPROM）を含む。しかしながら、メモリ76は、プロセッサ74の外部にあることも可能であ

る。また、メモリ76は、プロセッサ74に作業メモリを提供するためのRAM（random access memory）を含んでもよい。メモリ76は、プロセッサ74によって実行されるコンピュータソフトウェアプログラム80を記憶する。

【００７０】

また、スマートカードは、クレジットカード又はデビットカードとして機能してもよく、カードと関係付けられる更なる情報を記憶するための磁気ストライプ、集積回路又は他の構成要素を含んでもよい。この情報は、認証システム30に転送するために適切な読み取り機によって読み取り可能であってもよい（図２を参照）。また、スマートカードは、認証システム30とデータ通信するために、上記の通信ポートを含んでもよい（図２を参照）。

【００７１】

ユーザ装置27の上記例示はスマートカードの形態であるが、更なる実施形態が他の形態で実装されることも勿論可能である。例えば、ユーザ装置は、携帯電話、PDA（personal digital assistant）、ラップトップコンピュータ、又はハンドヘルドコンピュータ等の適切な処理基盤が搭載された移動式装置を含んでもよい。同様に、ユーザ装置は、実行可能ソフトウェアプログラムによってプログラミングされるデスクトップコンピュータを含んでもよい。従って、ユーザ装置が多数の異なるハードウェア「プラットフォーム」を含み得ることが理解されるであろう。

【００７２】

ユーザ装置27のメモリ76は、認証キー82を記憶する。認証キー82は、電子データ交換サービス（例えば、オンラインバンキングサービス、株式の取引サービス又はオンラインショッピングサービス等）、コンピュータネットワークサービス（例えば、ネットワークログオンサービス）、通信サービス（例えば、Ｅメールサービス又はメッセージングサービス）、メンバーシップベースサービス（例えば、オンラインフォーラム、レンタカーサービス、又は健康サービス）、又はセキュリティサービス（例えば、ビルアクセスサービス）等の特定のサービスにアクセスするためのものであってもよい。

【００７３】

代替的に、認証キー82は、複数の異なるサービスへのアクセスを可能にしてもよい。一実施形態では、メモリ76は、各々が１つ又は複数の特定サービスにアクセスするための複数の認証キーを記憶してもよい。ユーザは、どの認証キーが使用されるべきかをユーザ装置27に示すために特定のサービスを選択することを要求されてもよい。

【００７４】

認証キー82は、ユーザ装置27と関係付けられるシード、コード又はデータシーケンス等の秘密キーである。この例示では、認証キー82は、ユーザ装置27のメモリ76に記憶された256ビットの共有キーである。認証キー82は、特定サービス向けに認証システム30のメモリ44に記憶された認証キー64と同じである。

【００７５】

また、メモリ76には２つのアルゴリズムが記憶される。これらは、認証システム30に記憶されたアルゴリズム66及び68と同じであるコード生成アルゴリズム84及び値確認コード生成アルゴリズム86を含む。適切なコード生成アルゴリズム84及び適切な値確認コード生成アルゴリズム86の例が以下に示される。

【００７６】

（例示的なコード生成アルゴリズム）

この例示におけるコード生成アルゴリズム66及び84は、

```
<STEP1> = ENCODE(
        <CODE LENGTH>, HASH(
                <MODE SECRET> XOR (
                        <MODE COUNTER> &
                        <MODE TYPE> &
```

<MODE INSTANCE> &
<PIN>
)
)
)

【００７７】

ここで、<STEP1>は認証コードであり、<CODE LENGTH>は生成される認証コードの長さであり、<MODE SECRET>は識別されたモードタイプのための認証キーであり、<MODE COUNTER>はユーザ装置と認証システムとの間で同期されるカウンタであり、<MODE TYPE>は、特定のモードタイプを表す数であり、<MODE INSTANCE>はモードのインスタンスであり、例えば、ユーザ装置が１つ以上の同じ<MODE TYPE>値を有する場合（例えば、２つのOTP（one-time-password）モード）、<PIN>はユーザ装置27又はユーザと関係付けられる既存のPIN（即ち、古いPIN）であり、XORは論理的排他ORであり、“＆”は追加を示す。

【００７８】

この例示では、コード生成アルゴリズム66、84は、（この例示では、新しいPINである）値を暗号化するために異なるアルゴリズムと関係付けられる異なる「モード」を使用してもよい。例えば、「モード」は、ワンタイムパスワードモード、両方向応答モード、又はユーザ入力データを考慮に入れるモードを含んでもよい。モードは、アクセスされているサービスに依存してもよく、認証システムで使用されるモード、そしてアルゴリズムと対応するであろう。コード生成アルゴリズム66、84は、単一のモードのみで動作することが可能であってもよく、この場合、モードパラメータのMODE TYPE及びMODE INSTANCEが省略されてもよい。

【００７９】

HASHは、任意の適切なハッシュ関数、例えば、MD5、SHA-1、SHA-224、SHA-256、SHA-384又はSHA-512であってもよい。この例では、ハッシュ関数はSHA-256関数である。また、ENCODEは、任意の符号化関数であってもよい。この例では、ENCODEは、以下の方程式を使用して、HASHの256ビットの結果（DATA）を<CODE LENGTH>の長さを有する認証コードに変換する。

Digit N = DATA[(48 + (N * 8))…(48 + ((N + 1) * 8) － 1)] MOD 10d

【００８０】

ここで、Ｎは０から（<CODE LENGTH> － 1）に等しく、DATAはこの例示ではSHA-256ハッシュ関数であるHASH関数の256ビットの結果である。勿論、上記方程式は限定的な例示であることは意図されておらず、HASHを符号化するための他の関数が使用されてもよいことが理解されるであろう。

【００８１】

以下の例示では、<CODE LENGTH> = 3であり、（１６進数の）256ビットHASHの結果が表１に示されている。

【表１】

Byte number															
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Byte Value															
DD	09	36	E7	7A	1C	88	5B	E4	70	2C	D4	67	0B	31	D5

Byte number															
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Byte Value															
EF	54	A4	07	12	C5	7D	72	45	23	CC	FA	0A	19	4F	92

【００８２】

ENCODE関数は、以下の方程式を使用して、HASHの256ビットの結果（DATA）を３桁（Digit 0, Digit 1, Digit 2)の長さを有する認証コードに変換する。

```
Digit 0 = Data[48..55] MOD 10d = 88h MOD 10d = 136d MOD 10d = 6
Digit 1 = Data[56..63] MOD 10d = 5Bh MOD 10d = 91d MOD 10d = 1
Digit 2 = Data[64..71] MOD 10d = E4h MOD 10d = 228d MOD 10d = 8
```

ENCODE、そして<STEP1>の結果は、３桁の値になるであろう。

```
<STEP1> = 618.
```

【００８３】

言い換えると、この例示では、認証コード＝618である。この場合、ENCODE関数は、ハッシュ関数HASHを適用することによって、256ビット認証キーをｎ桁の認証コードに変換する。これは、この例示では、３ビット認証コードである。３ビット認証コードは、２ビット値及び１ビット値確認コードを暗号化する３ビットメッセージ、又は３ビット値を暗号化するメッセージを構築するために使用されてもよい。

【００８４】

この例示では、カウンタ（MODE COUNTER）は、安全性を高めるためにユーザ装置27と認証システムとの間で同期されるカウント値である。例として、一方又は他方を認証するためにユーザ装置と認証システムとの間でメッセージが伝達されるたびに、カウンタがインクリメントされ、カウンタを使用して認証キーがインクリメントされることにより、新しい認証キーを生成する。カウンタは選択的である。代替的に、値が暗号化されるたびに同じ認証キーを使用することもできる。

【００８５】

（例示的な値確認コード生成アルゴリズム）

この例示における値確認コード（VVC）生成アルゴリズム68及び８６は、以下の通りである。

```
<VVC> = ENCODE(
                8 -   <PIN LENGTH>, HASH(
                <MODE SECRET> XOR (
                <MODE COUNTER> &
                <MODE TYPE> &
```

```
                    <MODE INSTANCE> &
                    <PIN> &
                    <SEPARATOR> &
                    <NEW PIN>
                    )
                )
        )
```

【００８６】

ここで、<PIN LENGTH>は暗号化されている値の長さであり、<MODE SECRET>、<MODE COUNTER>、<MODE TYPE>、<MODE INSTANCE>、<PIN>、HASH、ENCODE、XOR及び“＆”は上記の通りであり、<SEPARATOR>は定数であり、この場合は１６進数値“FE”であり、<NEW PIN>は暗号化されている値である。本例示では、セパレータは単にPIN（即ち、古いPIN）とNEW PINとを区分化する好都合な機構を提供するために含まれる。

【００８７】

上記の例は、認証コード及び値確認コードの各々を生成するための適切なアルゴリズムの２つの例示に過ぎず、他のアルゴリズムを使用することもできることが理解されるであろう。例えば、異なる又はより少ない変数がXORステップに含まれてもよく、PIN（即ち、古いPIN）を使用する必要がない。更に、ユーザ装置27が単一のモードで動作する場合、<MODE COUNTER>、<MODE TYPE>、<MODE INSTANCE>等の値は適用できないであろう。更に、アカウント番号等の他の情報、又は追加のユーザ入力値が使用されてもよい。

【００８８】

また、コード生成アルゴリズムで使用されるのとは異なる秘密キーが値確認コード生成アルゴリズムで使用されてもよく、又は実際には、値確認コード生成アルゴリズムは、秘密キーを全く使用せずに、別の手法を用いて値確認コードを生成してもよい。

【００８９】

（値の暗号化の例示）

図４は、本発明の実施形態によるユーザ装置27へ入力された値を暗号化する方法100を示す。この例示では、値は、認証システム30において記憶される代替PINである。

【００９０】

次に図３及び図４を参照すると、ステップ102において、ユーザ101は、ユーザ装置27のキーパッド70を使用してPIN変更選択肢を選択する。PIN変更選択肢の選択は、以下に記載されるように、ユーザ装置27が認証システム30を認証すること可能にするために、認証システム30によって生成される認証応答を入力することをユーザに要求してもよい。しかしながら、このステップは、伝達された値が何れの場合も暗号化されているので選択的である。

【００９１】

ステップ103では、ユーザ装置27は、代替PINを入力するようにユーザ101を促す。ステップ104では、ユーザ101は、代替の又は新たなPIN、例えば、代替の又は新たなPINを表す数字のシーケンス「9876」をキーパッド70に入力する。代替又は新たなPINが正確に入力されたことを確実にするために、ソフトウェア80は代替PINを再入力することをユーザに促してもよい。

【００９２】

次に、ソフトウェア80は、ステップ105で既存のPIN（即ち、古いPIN）を入力することをユーザ101に促して、ユーザはそれをステップ106で入力する。例えば、既存のPINは、数字のシーケンス“1234”であってもよい。

【００９３】

ステップ108では、ソフトウェア80は、認証コードを生成するためにコード生成アルゴリズム84を使用して認証キー82を処理する。　この例示では、以下の１６進数値が使用される。

<MODE SECRET> =
4B 50 13 07 66 4D CB 01 FF B6 B3 35 10 7B 42 E6 FC A6 B8 57 51 AE 72 7435
9E 69 79 15 35 5B 70

<CODE LENGTH> = 8
<MODE COUNTER> = 00 00 01
<MODE TYPE> = 13
<MODE INSTANCE> = 00
<PIN> = 31 32 33 34

【００９４】

この例示では、すでに記載したように、<MODE TYPE>, <MODE INSTANCE>, <MODE COUNTER>は選択的であって、コード生成アルゴリズムに含まれ得る追加データの例を提示するためにのみ含まれている。

【００９５】

また、この例示では、“1234”の値（この場合は既存のPINである）が１６進数形式のASCII表示に変換されることにも留意されたい。このようは手法は、例えば、英数字値（英数字のＰＩＮ等）、或いは非英数字値が使用されることを可能にする。

【００９６】

次に、この例示では、上記パラメータがコード生成アルゴリズム84によって以下のように処理される。

```
<STEP1> = ENCODE(
        <CODE LENGTH>, HASH(
                <MODE SECRET> XOR (
                        <MODE COUNTER> &
                        <MODE TYPE> &
                        <MODE INSTANCE> &
                        <PIN>
                        )
                )
        )

<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> & <PIN> =
00 00 01 13 00 31 32 33 34

<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> & <PIN> =
4B 50 12 14 66 7C F9 32
CB B6 B3 35 10 7B 42 E6
FC A6 B8 57 51 AE 72 74
35 9E 69 79 15 35 5B 70

HASH(<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> &
<MODE INSTANCE> & <PIN>)) =
9A 4B 42 FD 17 76 67 F8
54 9F 5B D2 07 BC 7B 77
B2 3D 6F 49 5D A9 F7 5C
F5 FF 86 C8 5C 97 F9 68

ENCODE(<LENGTH>, HASH(<MODE SECRET> XOR (<MODE COUNTER>
& <MODE TYPE> & <MODE INSTANCE> & <PIN>))) =
```

38491078

従って、認証コードは、ｎ桁コード（ここでｎ＝８）として生成される。

認証コード＝38491078

【００９７】

ステップ110では、ソフトウェア80は、値確認コードを生成するために値確認コード生成アルゴリズム86を使用して値を処理する。

【００９８】

<MODE SECRET>（即ち、認証キー）, <MODE COUNTER>, <MODE TYPE>, <MODE INSTANCE>及び<PIN>に対する値は上記のように与えられる。更に、以下の通りである。

```
<SEPARATOR> = FE
<NEW PIN> = 39 38 37 36
<PIN LENGTH> = 4
```

【００９９】

この例示では、再度、この例示で新たなPINである“9876”の値が、処理のために１６進数形式のASCII表示（即ち、“39 38 37 36”）に変換されている。次に、上記パラメータは、値確認コード生成アルゴリズム86によって以下のように処理される。

```
<VVC> = ENCODE(
        8 - <PIN LENGTH>, HASH(
                <MODE SECRET> XOR (
                        <MODE COUNTER> &
                        <MODE TYPE> &
                        <MODE INSTANCE> &
                        <PIN> &
                        <SEPARATOR> &
                        <NEW PIN>
                        )
                )
        )

<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> & <PIN> &
<SEPARATOR> & <NEW PIN> =
00 00 01 13 00 31 32 33 34 FE 39 38 37 36

<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> & <MODE
INSTANCE> & <PIN> & <SEPARATOR> & <NEW PIN>) =
4B 50 12 14 66 7C F9 32
CB 48 8A 0D 27 4D 42 E6
FC A6 B8 57 51 AE 72 74
35 9E 69 79 15 35 5B 70

HASH(<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> &
<MODE INSTANCE> & <PIN> & <SEPARATOR> & <NEW PIN>)) =
CF F4 47 C9 4C 36 CB 66
69 BA 3A B6 61 7C AD EE
B6 98 63 19 DA 2A 19 71
12 40 6D 08 C1 C3 45 18
```

ENCODE(4, HASH(<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> & <PIN> & <SEPARATOR> & <NEW PIN>))) = 3256

従って、値確認コードは、ｍ桁コード（ここでｍ＝4）として生成される。

Value Verification Code = 3256

【０１００】

ステップ112では、ソフトウェア80は、認証コード（38491078）、値（9876）及び値確認コード（3256）を使用して、値（9876）を暗号化するためのメッセージを構築する。この例示では、オペランドとして全ての３つの値を含む算術演算を使用してメッセージを構築する。この演算では、値及び値確認コードは連結シーケンス（98763256）を提供するために連結される。次に、モジュラス１０演算を使用して、連結シーケンスに認証コードが付加される。各数字は以下のように別個に付加される。

<MESSAGE> = <STEP1> ADD (<NEW PIN> & <VVC>)

【表２】

<STEP1> = 1.	3	8	4	9	1	0	7	8
<NEW PIN>	9	8	7	6				
<VVC>					3	2	5	6
<MESSAGE>	2	6	1	5	4	2	2	4

【０１０１】

ここで、ADDはモジュラス１０の加算演算である。

【０１０２】

この例では、値確認コード＜VVC＞が４桁値＜NEW PIN＞の末尾に連結されているが、値確認コードは、値の先頭に連結され、又は他の数字によって値から分離されることも可能であることに留意されたい。実際に、値確認コードは、認証コード<STEP 1>に付加されるのではなく、メッセージの末尾に付加され得る。

【０１０３】

また、この例示では、値確認コード<VVC>は、この例示では８桁である認証コード<STEP 1>の長さと、この例示では４桁である値<NEW PIN>の長さとの差に対応するシーケンス長を有するように選択される。従って、この例示では、値は４桁を含み、認証コードは８桁を含み、値確認コードは４桁を含む。同様に、値<NEW PIN>が６桁を含み且つ認証コードが８桁を含む場合は、値確認コード＜VVC＞は２桁を含んでもよい。連結値及び値確認コードと比較して認証コード<STEP 1>の桁数が異なってもよいことが理解されるであろう。しかしながら、認証コードは、値と少なくとも等しく、そうでなければ長さが値より長いことが望ましい。

【０１０４】

更に、この例は、認証コード、値及び値確認コードが１０桁（0，1，2，3，4，5，6，7，8 及び9）を含む数字の組から選択される数字のシーケンスからなるように、モジュラス１０加算を使用する。しかしながら、数字がＸ桁を含む数字の組から選択される場合、メッセージは、モジュラスＸ加算又は減算等のモジュラスＸ算術演算を使用して構築され

得る。

【０１０５】

次に、構築されたメッセージ（即ち、26154224）は、ステップ113では、ユーザ101に伝達又は出力され、メッセージは、ユーザ装置27の８桁ディスプレイ72上に表示するために出力されてもよい。メッセージ（26154224）は、値（9876）を決定及び確認して、ユーザ装置27及び／又はユーザ101を認証するために、認証システム30によって処理するために通信ネットワーク34を介して認証システム30に伝達するためのものである。

【０１０６】

ステップ114では、ユーザ101は、適切な手段によってメッセージを認証システム30に伝達する。ユーザがパーソナルコンピュータ24へのアクセスを有する場合、認証システム30にメッセージを伝達することは、ネットワーク34を介して認証システム30に送信するために、ユーザ101が手動でパーソナルコンピュータ24にメッセージを入力することを含んでもよい。他の代替では、ユーザ装置27は、ネットワーク接続されており（例えば、それが携帯電話又はPDAである場合）、更なるユーザ入力無しで認証システム30にメッセージを直接送信してもよい。更に他の代替では、メッセージは、現金自動支払機等の別の装置によってユーザ装置27（例えば、クレジットカード）から読み取られて、認証システム30に送信されてもよい。こうした代替では、ユーザ101は、メッセージの値を知る必要がない。

【０１０７】

メッセージと共に、ユーザ101（又はユーザ装置27）は、認証システム30に、クレジットカード番号、アカウント番号又はアカウント名等のユーザ装置27と関係付けられる追加の情報を伝達する。このような情報は、メッセージの伝達を要求するユーザ及び／又はカードを識別して、どの認証キー及びPINがユーザ装置27と関係付けられるかを決定するために使用されてもよい。しかしながら、追加の情報は、メッセージが伝達される前又は後のいずれかで提供されてもよいので、メッセージと共に伝達されることが不可欠ではない。

【０１０８】

（値の確認の例示）

この例示では、認証システム30は、通信ポート50を介してメッセージを受信する。認証システム30は、追加の情報を使用して、どの認証キー及びPINがユーザ装置27と関係付けられるかを決定し、また、値を確認してユーザ101及び／又はユーザ装置27を認証するために受信したメッセージを処理するためにこれらを取得する。

【０１０９】

ステップ116で、認証システム30におけるソフトウェア62は、期待される認証コード<STEP 1#>を生成するためにコード生成アルゴリズム66を使用して認証キー64を処理する。このアルゴリズムは、上記のようにユーザ装置27で行われたコード生成アルゴリズム84のステップを反復する。ユーザ装置27によって使用された認証キー82が認証システム30によって使用された認証キー64と同じあった場合、同じ認証コード（例えば、“ 38491078 ”）が取得されるはずである。次に、ステップ118では、受信した値<NEW PIN#>及び受信した値確認コード<VVC#>を導出するために期待される認証コード（例えば、“ 38491078 ”）を使用してメッセージ（例えば、“ 26154224 ”）を処理する。

【０１１０】

この例示では、メッセージの処理は、以下のようにメッセージを復号するためにモジュラス１０演算を使用してメッセージから期待される認証コードを減ずることを含む。

<NEW PIN#> & <VVC#> = <MESSAGE> SUBTRACT <STEP 1#>

【表３】

<MESSAGE>	2	6	1	5	4	2	2	4
<STEP 1#>	3	8	4	9	1	0	7	8
<NEW PIN#> & <VVC#>	9	8	7	6	3	2	5	6

【０１１１】

この例示では、メッセージを構築するためにユーザ装置27によって適用されるものに対する逆演算（即ち、モジュラス１０加算）であるので、モジュラス１０減算が使用される。

【０１１２】

上記例示では、<NEW PIN#>は認証システム30によってメッセージから導出される新たなPIN値であり、<VVC#>は導出された値確認コードであり、<STEP 1#>は認証システム30によって生成される期待される認証コードである。

【０１１３】

この例示では、期待される認証コード<STEP 1#>の各数字は、モジュラス１０演算を使用して受信したメッセージの各数字から別個に減算される。それによって、この場合、認証システム30は、受信した値の“9876”及び受信した値確認コードの“3256”を決定する。

【０１１４】

値及び値確認コードのシーケンス長はあらかじめ決めされていてもよく、その結果、認証システム30は、<NEW PIN#> & <VVC#>のどの数字が値の末尾と関係付けられるか及びどの数字が値確認と関係付けられるかを決定することができる。代替的に、長さは、様々な長さのＰＩＮを可能にするために、メッセージと共に認証システム30に伝達されてもよい。

【０１１５】

ステップ120では、認証システム30におけるソフトウェア62は、期待される値確認コード<VVC_EXP>を生成するために値確認コード生成アルゴリズム68を使用して受信した値“9876”を処理する。このアルゴリズムは、上記のようにユーザ装置27で行われた値確認コード生成アルゴリズム86のステップを反復する。メッセージが正確に送信されたとすれば、同じ値確認コード“3256”が取得されるはずである。ステップ122では、ソフトウェア62は、期待される値確認コード<VVC_EXP>を受信した値確認コード<VVC#>と比較する。２つのコードが相関する場合、認証システム30は、受信した値<VVC#>を確認して、ユーザ装置27及び／又はユーザ101を認証する。値確認コード<VVC#>が有効である場合、認証システム30は、メモリ44又はデータベース59に記憶された既存のPIN“1234”を置換PIN“9876”で置換し、それによってユーザ装置27と関係付けられるPINを更新するであろう。２つのコードが相関しなければ、PINは更新されない。ステップ124では、認証システム30は、PINが更新されたことをユーザ装置27に伝達する。

【０１１６】

（認証システムの認証の例）

上記の通り、PIN変更選択肢の選択は、認証システム30によって生成される認証応答を入力することをユーザ101に要求してもよい。このような認証応答の例は、次に図５を参照して説明されるであろう。既に記載されたように、この認証方法は選択的である。他の方法が、ユーザ装置27に対して認証システム30を認証するために使用されてもよい。又は、値が暗号化されて送信されるので、認証システム30は認証される必要が全くない。

【０１１７】

図５に示される方法128では、ステップ130において、ユーザは、認証システム30に認証要求を伝達する。認証要求は、ユーザ装置27、又はネットワーク接続コンピュータ若しく

は現金自動支払機等の別の装置を介して伝達されてもよい。ステップ132では、認証システム30におけるソフトウェア62は、例えば、バイナリ符号化１０進数加算を使用してカウンタをインクリメントし、以下のように新たなカウンタを使用して認証キーをインクリメントする。

```
<MODE COUNTER> = <MODE COUNTER> BCDADD 1

<MODE SECRET> = HASH(
        <MODE SECRET> XOR (
                <MODE COUNTER> &
                <MODE TYPE> &
                <MODE INSTANCE> &
        )
)
```

例えば、以下の通りである。

```
<MODE COUNTER> = 00 00 00
<MODE TYPE> = 10
<MODE INSTANCE> = 00
<MODE SECRET> =
D1 B9 1D 2C F8 2A 72 28
AA F6 6D 2C 3E 49 58 79
1E 78 C7 CE 53 81 DE 00
79 2F BD B6 C3 62 2F BB

<MODE COUNTER> = <MODE COUNTER> + 1 = 00 00 01

<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> =
00 00 01 10 00

<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> & <MODE
INSTANCE>) =
D1 B9 1C 3C F8 2A 72 28
AA F6 6D 2C 3E 49 58 79
1E 78 C7 CE 53 81 DE 00
79 2F BD B6 C3 62 2F BB

HASH(<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> &
<MODE INSTANCE)) =
23 FA 77 1B 48 2E 39 20
FF 18 23 F8 6B 98 BC C2
0C FA 0F CC 15 7E 69 78
D7 A1 8B CC A4 C3 B2 81 (新たな認証キー).
```

【０１１８】

ステップ134では、ソフトウェア62は、新たな認証キー64に基づく認証応答生成アルゴリズムを使用して認証応答を生成する。

```
        <AUTHENTICATION RESPONSE> = ENCODE(
        <AUTHENTICATION MESSAGE LENGTH> - 2, HASH(
```

```
                    <MODE SECRET> (
                            <MODE COUNTER> &
                            <MODE TYPE> &
                            <MODE INSTANCE> &
                    )
            )
            ) & <MODE COUNTER> MOD 100
```

ここで、<AUTHENTICATION MESSAGE LENGTH>は認証応答の長さである。

【０１１９】

例えば、以下の通りである。

```
<MODE COUNTER> & <MODE TYPE> & <MODE INSTANCE> =
00 00 01 10 00

<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> & <MODE
INSTANCE>) =
23 FA 76 0B 48 2E 39 20
FF 18 23 F8 6B 98 BC C2
0C FA 0F CC 15 7E 69 78
D7 A1 8B CC A4 C3 B2 81

HASH(<MODE SECRET> XOR (<MODE COUNTER> & <MODE TYPE> &
<MODE INSTANCE>)) =
AA 04 89 DD 6D D9 2C 0C
6D FF BE 8D 90 FC 3A CA
FD 49 CE 6D 4F E7 F0 C1
13 68 05 89 0A E8 88 F7

ENCODE(<LENGTH> - 2, HASH(<MODE SECRET> XOR (<MODE
COUNTER> & <MODE TYPE> & <MODE INSTANCE>)))
D1 = 2C MOD 10d = 44 MOD 10 = 4
D2 = 0C MOD 10d = 12 MOD 10 = 2
D3 = 6D MOD 10d = 109 MOD 10 = 9
D4 = FF MOD 10d = 255 MOD 10 = 5

ENCODE(<LENGTH> - 2, HASH(<MODE SECRET> XOR (<MODE
COUNTER> & <MODE TYPE> & <MODE INSTANCE>))) & <MODE
COUNTER> MOD 100 =
429501
```

【０１２０】

認証システム30は、例えば、認証要求を伝達するのに使用される同じ通信手段を介して、ステップ136でユーザ101に認証応答（“429501”）を伝達する。

【０１２１】

ステップ138では、ユーザ101は、認証応答を受信して、ユーザ装置27のキーパッド70に認証応答（“429501”）を入力する。ステップ140では、ユーザ装置27におけるソフトウェア80は、同じ認証応答生成アルゴリズムを使用して、同じ認証キー（MODE SECRET）に基づく期待される認証応答を生成する。これは、最初にカウンタ及びシークレットのコピーを作ることによって行われる。

```
<TMP MODE COUNTER> = <MODE COUNTER>
<TMP MODE SECRET> = <MODE SECRET>
```

【０１２２】

次に、ソフトウェア80は、以下のアルゴリズムを使用して(TMP MODE COUNTER MOD 10)が受信した認証応答の最後の２桁と等しくなるまで一時カウンタ(TMP MODE COUNTER)及び一時シークレット(TMP MODE SECRET)をインクリメントする。

```
while (<TMP MODE COUNTER> MOD 10 != <AUTHENTICATION
RESPONSE>.RIGHT(2))
        <TMP MODE COUNTER> = <TMP MODE COUNTER> BCDADD 1
                <TMP MODE SECRET> = HASH(
                <TMP MODE SECRET> XOR (
                        <TMP MODE COUNTER> &
                        <MODE TYPE> &
                        <MODE INSTANCE> &
                        )
                )
```

ソフトウェア80は、期待される認証応答を以下のように計算する。

```
<expected authentication response> =
        ENCODE(
                <authentication response LENGTH> - 2,
                HASH(
                        <TMP MODE SECRET> XOR (
                        <TMP MODE      COUNTER> & <MODE TYPE> &
                        <MODE INSTANCE>
                        )
                )
        ) & <TMP MODE COUNTER> MOD 100
```

【０１２３】

ソフトウェア80は、期待される認証応答を受信した認証応答と比較し、認証応答が受信した認証応答と相関する場合、認証システム30が認証されることを示す。これに応じて、ソフトウェア80は、ステップ142（ステップ103と等しい）で暗号化される値を入力することをユーザに促す。また、<MODE SECRET>及び<MODE COUNTER>は、一致する認証応答が見つかれば更新される。

```
<MODE COUNTER> = <TMP MODE COUNTER>
<MODE SECRET> = <TMP MODE SECRET>
```

【０１２４】

様々な変更、追加及び／又は修正が本発明の範囲から逸脱することなく既に記載された部分に対して行われてもよいこと、及び上記教示に照らして、本発明は、当業者によって理解される様々な方法でソフトウェア、ファームウェア及び／又はハードウェアに実装されてもよいことが理解されるべきである。

【０１２５】

本願は、１つ以上の将来の願書の優先権の基礎として利用されてもよく、任意のこのような将来の願書の請求項は本願に記載された何れか１つの特徴又は特徴の組み合わせを対象としてもよい。何れかのこのような将来の願書は、例示を目的として与えられ、何れかの将来の願書で請求項に記載され得ることに関して非限定的である１つ以上の以下の請求

項を含んでもよい。

【図１】

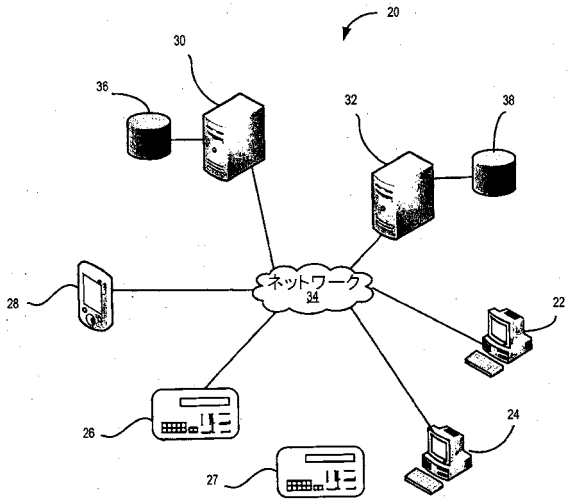

FIG. 1

【図２】

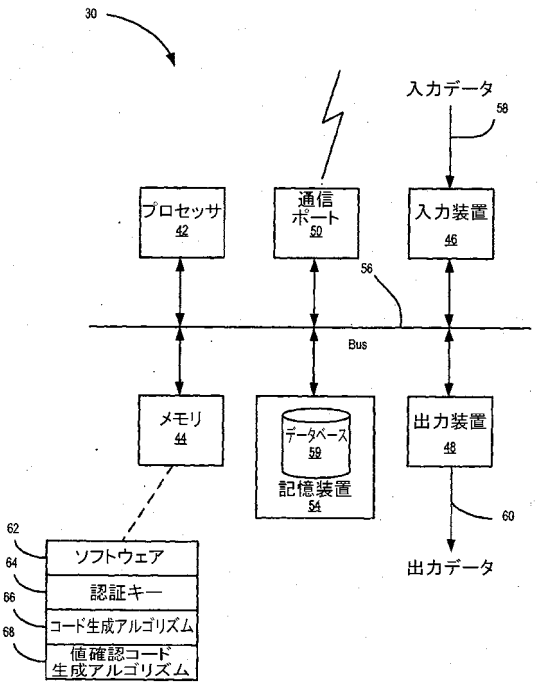

FIG. 2

【図３】

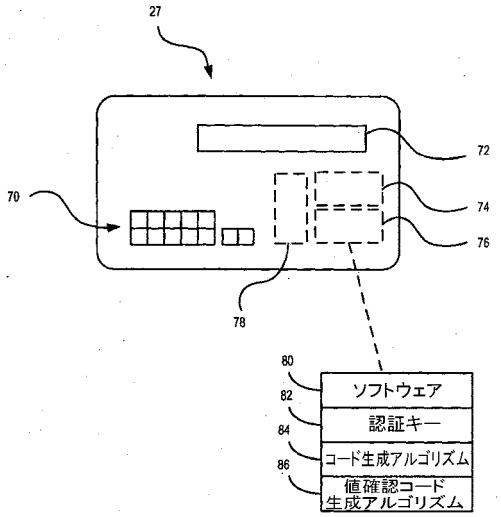

FIG. 3

【図４】

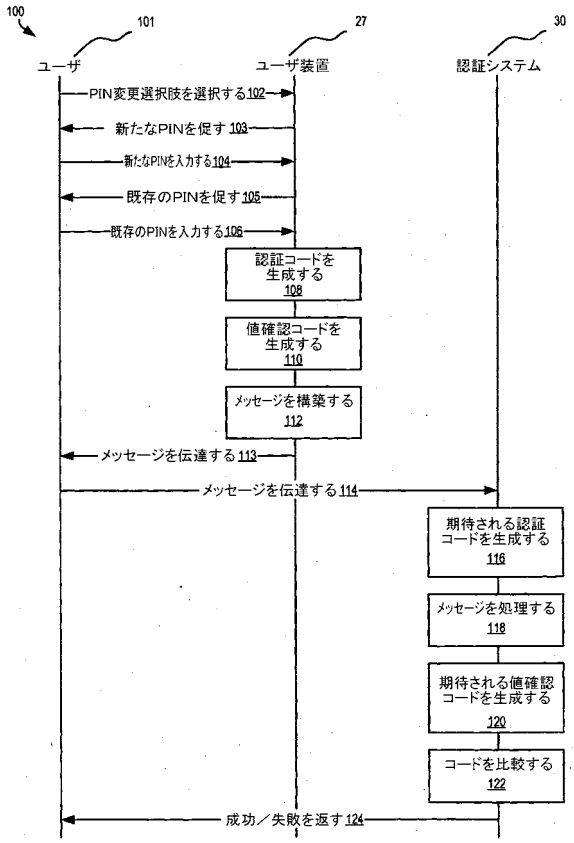

FIG. 4

【図５】

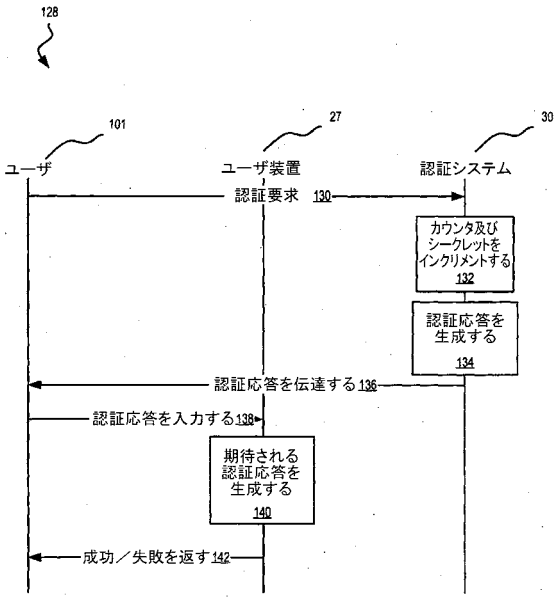

FIG. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2011/000904

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/14 (2006.01) ***H04L 9/28*** (2006.01) ***H04W 12/00*** (2009.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPI, EPODOC (key words used: Encrypt, secure, enter, device, mobile, PIN, value, authenticate, key, algorithm, communicate, message, replace and the like terms)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,373,559 A (KAUFMAN et al.) 13 December 1994 (abstract, column 3 lines 60 – 62, column 7 lines 6 – 33, column 9 lines 27 – 31)	1 – 28
Y	US 2003/0210788 A1 (BILLHARTZ et al.) 13 November 2003 (abstract, paragraph [0011])	1 – 28
A	US 2004/0083393 A1 (JORDAN et al.) 29 April 2004 (the abstract)	
A	US 2009/0320107 A1 (CORELLA) 24 December 2009 (the abstract)	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 November 2011	08 November 2011
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **KHALID AHMAD** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 3 9935 9634

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2011/000904

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/0104411 A1 (AGRAWAL et al.) 1 May 2008 (the abstract)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2011/000904

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5373559	US	5491752				
US	2003210788	AU	2003234521	BR	0309881	CA	2483880
		CN	1726670	EP	1508222	JP	2005525047
		US	6931132	US	2005185794	US	8014526
		WO	03096614				
US	2004083393	NONE					
US	2009320107	US	7975292				
US	2008104411	NONE					

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 レノン、 ジェイムズ エバン
オーストラリア国 ５０６１ サウス オーストラリア州 アンリー ビーチ アベニュー ６

Ｆターム(参考) 5J104 AA07 JA03 KA02 NA05 PA07