【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成26年9月4日(2014.9.4)

【公表番号】特表2013-535903(P2013-535903A)
【公表日】平成25年9月12日(2013.9.12)
【年通号数】公開・登録公報2013-050
【出願番号】特願2013-520925(P2013-520925)
【国際特許分類】
*Ｈ０４Ｌ　9/32　(2006.01)*
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｌ　9/00　６７３Ｃ

【手続補正書】
【提出日】平成26年7月18日(2014.7.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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み、又は
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９】
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１０】
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９に記載の方法。
【請求項１１】
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９又は１０に記載の方法。
【請求項１２】
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１１に記載の方法。
【請求項１３】
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１２に記載の方法。
【請求項１４】
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１３に記載の方法。
【請求項１５】
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み、又は
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９～１４の何れか１項に記載の方法。
【請求項１６】
前記値は、前記ユーザ装置と関係付けられる置換PINである、請求項１～１５の何れか１項に記載の方法。
【請求項１７】
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１８】
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し、又は
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１７に記載のユーザ装置。
【請求項１９】
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２０】
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１～１６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２１】
請求項２０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。