【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30年3月29日(2018.3.29)

【公表番号】特表2017-506850(P2017-506850A)
【公表日】平成29年3月9日(2017.3.9)
【年通号数】公開・登録公報2017-010
【出願番号】特願2016-553393(P2016-553393)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　9/10　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｌ　9/00　６２１Ａ

【手続補正書】
【提出日】平成30年2月13日(2018.2.13)
【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】
データを認証する方法であって、
公開鍵およびセッション鍵ＩＤの表記の複数の組み合わせを不揮発性メモリに記憶するステップを備え、
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせを記憶する前記ステップは、各セッション鍵ＩＤの表記を複数の電子ヒューズに記憶するステップを含み、
ペイロードと、前記ペイロードに付随する公開鍵、セッション鍵ＩＤおよび署名とを入力するステップとを含み、前記署名は、前記ペイロードと、前記付随の公開鍵および秘密鍵を含む鍵ペアのうち秘密鍵との関数であり、
プロセッサを用いて、前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記組み合わせから、および前記署名および前記ペイロードから、前記ペイロードが真正であるか否かを判断するステップと、
前記ペイロードが真正であるという判断に応答して、前記ペイロードの処理を実行するステップと、
前記ペイロードが真正ではないという判断に応答して、前記ペイロードの処理を無効化するステップと、
前記複数の組み合わせのうち１つの組み合わせ中の前記セッション鍵ＩＤの表記を記憶する前記複数の電子ヒューズのうち１つの電子ヒューズに電流を通さないようにすることによって、新規セッション鍵を形成するステップとを備える、方法。
【請求項２】
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせにそれぞれ関連付けられた複数の鍵状態を記憶するステップをさらに備え、各鍵状態は、関連付けられた組み合わせが有効であるか否かを示し、
前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断するステップは、

前記複数の組み合わせのうち１つの組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有するか否か、および前記１つの組み合わせに関連付けられた前記鍵状態から、前記１つの組み合わせが有効であるか否かを判断するステップと、
前記１つの組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有し且つ有効ではないという判断に応答して、前記ペイロードが真正ではないことを指示するステップとを備える、請求項１に記載の方法。
【請求項３】
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせにそれぞれ関連付けられた複数の鍵状態を記憶する前記ステップは、各鍵状態を１つ以上の電子ヒューズに記憶するステップを含む、請求項２に記載の方法。
【請求項４】
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせのうち、各公開鍵の表記は、公開鍵のハッシュ値であり、
前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断するステップは、
前記付随の公開鍵のハッシュ値を計算するステップと、
前記付随の公開鍵の前記ハッシュ値が、前記複数の組み合わせのうち１つの組み合わせの公開鍵の表記とマッチングするか否かを判定するステップと、
前記付随の公開鍵の前記ハッシュ値が前記複数の組み合わせの公開鍵の表記とマッチングしないという判断に応答して、前記ペイロードが真正ではないことを指示するステップとを含む、請求項１に記載の方法。
【請求項５】
前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断するステップは、
公開鍵およびセッション鍵ＩＤの前記複数の組み合わせのうち、前記付随の公開鍵の前記ハッシュ値とマッチングする前記公開鍵の表記を有する１つの組み合わせに対して、付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングするか否かを判断するステップと、
前記付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングするという判断に応答して、前記ペイロードが真正であることを指示するステップと、
前記付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングしないという判断に応答して、前記ペイロードが真正ではないことを指示するステップとを含む、請求項４に記載の方法。
【請求項６】
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせにそれぞれ関連付けられた複数の鍵状態を記憶するステップをさらに備え、各鍵状態は、関連付けられた組み合わせが有効であるか否かを示し、
前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断するステップは、
前記複数の組み合わせのうち１つの組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有するか否か、および前記組み合わせに関連付けられた前記鍵状態から、前記組み合わせが有効であるか否かを判断するステップと、
前記組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有し且つ有効ではないという判断に応答して、前記ペイロードが真正ではないことを指示するステップとを含み、
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせを記憶する前記ステップは、
各セッション鍵ＩＤの表記を複数の電子ヒューズに記憶するステップと、
前記複数の組み合わせのうち１つの組み合わせ中の前記セッション鍵ＩＤの表記を記憶

する前記複数の電子ヒューズのうち１つに電流を通さないようにすることによって、新規セッション鍵を形成するステップとを含む、請求項４に記載の方法。
【請求項７】
認証システムであって、
公開鍵およびセッション鍵ＩＤの表記の複数の組み合わせを記憶するように構成可能な不揮発性メモリを備え、前記不揮発性メモリは、公開鍵およびセッション鍵ＩＤの表記の前記組み合わせを記憶するための複数の電子ヒューズを含み、
前記不揮発性ストレージに連結されたプロセッサを備え、
前記プロセッサは、
ペイロードと、前記ペイロードに付随する公開鍵、セッション鍵ＩＤおよび署名とを入力するように構成され、前記署名は、前記ペイロードと、前記付随の公開鍵および秘密鍵を含む鍵ペアのうち秘密鍵との関数であり、
前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、および前記署名および前記ペイロードから、前記ペイロードが真正であるか否かを判断し、
前記ペイロードが真正であるという判断に応答して、前記ペイロードの処理を実行し、
前記ペイロードが真正ではないという判断に応答して、前記ペイロードの処理を無効化し、
前記複数の組み合わせのうち１つの組み合わせ中の前記セッション鍵ＩＤの表記を記憶する前記複数の電子ヒューズのうち１つに電流を通さないようにすることによって、新規セッション鍵を形成するように構成されている、システム。
【請求項８】
前記不揮発性メモリは、公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせにそれぞれ関連付けられた複数の鍵状態を記憶するストレージをさらに含み、各鍵状態は、関連付けられた組み合わせが有効であるか否かを示し、
プロセッサは、さらに、
前記複数の組み合わせのうち１つの組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有するか否か、および前記１つの組み合わせに関連付けられた前記鍵状態から、前記組み合わせが有効であるか否かを判断し、
前記１つの組み合わせが前記付随の公開鍵とマッチングする公開鍵の表記を有し且つ有効ではないという判断に応答して、前記ペイロードが真正ではないことを指示するように構成されている、請求項７に記載のシステム。
【請求項９】
前記不揮発性メモリは、前記複数の鍵状態を記憶するための複数の電子ヒューズを含む、請求項８に記載のシステム。
【請求項１０】
前記不揮発性メモリは、前記セッション鍵ＩＤの表記を記憶するための複数の電子ヒューズを含み、
前記プロセッサはさらに、前記複数の組み合わせのうち１つの組み合わせ中の前記セッション鍵ＩＤの表記を記憶する前記複数の電子ヒューズのうち１つに電流を通さないようにすることによって、新規セッション鍵を形成するように構成されている、請求項９に記載のシステム。
【請求項１１】
公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせのうち、各公開鍵の表記は、公開鍵のハッシュ値であり、
前記プロセッサは、前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断する際に、
前記付随の公開鍵のハッシュ値を計算し、
前記付随の公開鍵の前記ハッシュ値が、前記複数の組み合わせのうち１つの組み合わせ

の公開鍵の表記とマッチングするか否かを判定し、
前記付随の公開鍵の前記ハッシュ値が前記複数の組み合わせの公開鍵の表記とマッチングしないという判断に応答して、前記ペイロードが真正ではないことを指示するように構成されている、請求項８に記載のシステム。
【請求項１２】
前記プロセッサは、前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断する際に、
公開鍵およびセッション鍵ＩＤの前記複数の組み合わせのうち、前記付随の公開鍵の前記ハッシュ値とマッチングする前記公開鍵の表記を有する１つの組み合わせに対して、付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングするか否かを判断し、
前記付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングするという判断に応答して、前記ペイロードが真正であることを指示し、
前記付随のセッション鍵ＩＤ番号が前記１つの組み合わせの前記セッション鍵ＩＤ番号の表記とマッチングしないという判断に応答して、前記ペイロードが真正ではないことを指示するように構成されている、請求項１１に記載のシステム。
【請求項１３】
前記不揮発性メモリ内の公開鍵およびセッション鍵ＩＤの表記の前記複数の組み合わせのうち、各組み合わせは、公開鍵およびセッション鍵ＩＤのハッシュ値であり、
前記プロセッサは、前記付随の公開鍵およびセッション鍵ＩＤ並びに前記不揮発性メモリに記憶された前記複数の組み合わせから、前記ペイロードが真正であるか否かを判断する際に、
前記付随の公開鍵および前記セッション鍵ＩＤの第１ハッシュ値を計算し、
前記第１ハッシュ値が前記不揮発性メモリ内の前記ハッシュ値のいずれかとマッチングするか否かを判断し、
前記第１ハッシュ値が前記不揮発性メモリ内の前記ハッシュ値のいずれかとマッチングしないという判断に応答して、前記ペイロードが真正ではないことを指示するように構成されている、請求項８のシステム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正の内容】
【００２３】
復号された署名がハッシュ値とマッチングすることに応答して、比較関数１６４は、入力されたペイロードに付随するセッション鍵ＩＤ　１１０を、不揮発性メモリ１３２に記憶され且つハッシュ化された公開鍵１３４のいずれか１つとマッチングする鍵に関連付けられたセッション鍵ＩＤと比較する。セッション鍵ＩＤ　１１０がセッション鍵ＩＤ　１３６のいずれか１つとマッチングしないことに応答して、比較関数１６４は、ペイロードが真正ではないと指示し、システムは、ロックダウン関数１６２を用いて、システムの起動またはプログラム可能なロジックの構築を中止することによって、ペイロード１０６のさらなる処理を無効化する。セッション鍵ＩＤ　１１０がセッション鍵ＩＤ　１３６のいずれか１つとマッチングすることに応答して、システムは、ブートプログラムの実行および／またはプログラム可能なロジック１６８の構築などを続行することによって、ペイロード１０６の処理を可能にする。各セッション鍵ＩＤ　１３６および各公開鍵１３４の各組み合わせが単一のハッシュ値である実装において、比較関数１６４が必要とされず、比較関数１６０が肯定的な比較結果を発見した場合、処理関数１６８は、ブートプログラムの実行および／またはプログラム可能なロジック１６８の構築などを続行する。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】変更
【補正の内容】
【００３９】
計算されたハッシュ値が不揮発性メモリに記憶された公開鍵のハッシュ値のいずれかとマッチングする場合、プロセスは、判断ブロック４０６から判定ブロック４１０に進行し、関連する有効ビットの状態から、マッチングした公開鍵のハッシュ値が有効であるか否かをチェックする。マッチングした公開鍵のハッシュ値が有効ではない場合、ブロック４０８において、システムをロックダウンする。