(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7157107号
(P7157107)

(45)発行日　令和4年10月19日(2022.10.19)

(24)登録日　令和4年10月11日(2022.10.11)

(51)国際特許分類		FI		
H04L 9/32 (2006.01)		H04L	9/32	200A
G06F 21/44 (2013.01)		G06F	21/44	
G09C 1/00 (2006.01)		G09C	1/00	640E

請求項の数　5　（全9頁）

(21)出願番号　特願2020-119602(P2020-119602)
(22)出願日　令和2年7月13日(2020.7.13)
(62)分割の表示　特願2018-110814(P2018-110814)の分割
原出願日　平成25年8月30日(2013.8.30)
(65)公開番号　特開2020-174392(P2020-174392A)
(43)公開日　令和2年10月22日(2020.10.22)
審査請求日　令和2年8月9日(2020.8.9)
(31)優先権主張番号　61/695,155
(32)優先日　平成24年8月30日(2012.8.30)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　13/969,133
(32)優先日　平成25年8月16日(2013.8.16)
最終頁に続く

(73)特許権者　507107291
テキサス インスツルメンツ インコーポレイテッド
アメリカ合衆国 テキサス州 ７５２６５－５４７４ ダラス メイル ステイション ３９９９ ピーオーボックス ６５５４７４
(74)代理人　230129078
弁護士　佐藤 仁
(72)発明者　ジンメン ホウ
アメリカ合衆国 ７５０２５ テキサス州 プラノ、 チェリー クリーク ドライブ ７７００
審査官　青木 重徳

最終頁に続く

(54)【発明の名称】　一方向のキーフォブ及び車両ペアリング認証、保持、及び無効化

(57)【特許請求の範囲】

【請求項１】

キーフォブデバイスであって、

信号を送信するように構成されるトランスミッタと、

１２８ビットのキーフォブカウンタ値を提供するように構成されるキーフォブカウンタと、

前記１２８ビットのキーフォブカウンタ値と動作鍵とを格納するように構成されるメモリと、

前記トランスミッタと前記メモリとに結合されるプロセッサであって、

前記動作鍵を用いて前記１２８ビットのキーフォブカウンタ値の全てのビットを直接に暗号化することによって前記１２８ビットのキーフォブカウンタ値の動作鍵暗号化値を生成し、

前記動作鍵を用いて暗号化されていない前記１２８ビットのキーフォブカウンタ値の選択された数の最下位ビットと、前記１２８ビットのキーフォブカウンタ値の前記動作鍵暗号化値の幾つかの所定の数のビットと、制御ユニットによって実行されるべきコマンドであって無効化モードに入るための前記コマンドを識別するデータフィールドとを含むメッセージを送信する、

ように構成される、前記プロセッサと、

を含み、

前記無効化モードの間に動作するキーフォブの第１のセットに関連付けられる動作鍵が前

記制御ユニットに保持され、前記無効化モードの間に動作を実行しないキーフォブに関連付けられる動作鍵が前記制御ユニットから削除される、キーフォブデバイス。
【請求項２】
請求項１に記載のキーフォブデバイスであって、
前記選択された数の最下位ビットが前記１２８ビットのキーフォブカウンタ値の最下位の８ビットである、キーフォブデバイス。
【請求項３】
請求項１に記載のキーフォブデバイスであって、
前記プロセッサが、前記メッセージを送信する後に前記キーフォブカウンタを１増分するように更に構成される、キーフォブデバイス。
【請求項４】
請求項１に記載のキーフォブデバイスであって、
前記プロセッサが、前記トランスミッタに、無効化手順を開始するための無効化信号を送信させるように更に構成される、キーフォブデバイス。
【請求項５】
請求項１に記載のキーフォブデバイスであって、
前記キーフォブカウンタ値がＡＥＳ－１２８暗号に基づいて前記動作鍵により暗号化される、キーフォブデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、概して、セキュリティに向けられ、更に具体的には、キーフォブ車両動作鍵の認証、保持、及び無効化のための方法に向けられる。
【背景技術】
【０００２】
キーフォブは、車両ドアの開／閉及びロック／ロック解除などの周知のアクションを行うために、車両制御ユニットなどの制御ユニットとペアリングされ得る。キーフォブは、送信のみが可能であり得、これは、双方向通信ができないことに起因してキーフォブにより送られるコマンドを認証するために制御ユニットから送られるチャレンジメッセージを介して利用可能な承認プロセスを制限する。制御ユニットは、受け取ったコマンドの正当性を認証すること、及び、有効キーフォブからの以前の伝送の再生を含み、承認されていないコマンドをリジェクトすることが可能である必要がある。
【０００３】
時折、キーフォブが失われることがあり、又はキーフォブの持ち主が制御ユニットにアクセスすることが承認されなくなる可能性がある。この状況において、どのキーフォブがまだ有効であり、どれが無視されるべきかを、制御ユニットに識別させるプロセスがあるはずである。
【発明の概要】
【０００４】
説明される実施例は、制御ユニット認証、保持、及び無効化に対するキーフォブのための方法を提供する。初期ペアリングの後、キーフォブと車両制御ユニットは、秘密の動作鍵（ＯｐＫｅｙ）を共有する。認証では、キーフォブは識別子を送り、識別子は１２８ビットカウンタの８最下位（ｌｏｗｅｓｔ－ｏｒｄｅｒ）ビット、及び制御ユニットに対するカウンタのＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値の幾つかのビットであり得る。
【０００５】
１つ又は複数のキーフォブが車両制御ユニットなどの制御ユニットとペアリングされた後、各キーフォブは、制御ユニットと秘密裏に共有されるそれ自体のＯｐＫｅｙを有する。キーフォブは、制御ユニットが車両ドアのロック解除／ロック又は開／閉などの所定のアクションをとるため、共有されたＯｐＫｅｙの所有を制御ユニットに認証する必要がある。本発明は、送信可能であるが受信不能のキーフォブを介する場合でもこの問題を解決

する。また、本明細書に記載される実施例は、第三者が、以前に送信されたメッセージを再生することにより真正のキーフォブに成りすますことを防止する。また、キーフォブがなくなった後、そのＯｐＫｅｙが無効化され得る一方、残りの又は新たなキーフォブのＯｐＫｅｙが保持され得る。

【０００６】

ＯｐＫｅｙ無効化及び保持では、残りの又は新たなキーフォブが、認証メッセージを制御ユニットに送るように真正の制御ユニットユーザーによりプロンプトされる。制御ユニットはその後、ＯｐＫｅｙ保持及び無効化モードに入るようにプロンプトされる。続いて、残りの又は新たなキーフォブの各々が、認証メッセージを制御ユニットに送るようにユーザーによりプロンプトされる。制御ユニットは最終的に、ＯｐＫｅｙ保持及び無効化モードを出るようにプロンプトされ、それぞれ、ＯｐＫｅｙ保持及び無効化モードに入る直前及びその間に制御ユニットが有効認証メッセージを受け取ったキーフォブのＯｐＫｅｙのみを保持する。

【０００７】

このように本発明を一般的な用語で説明したので、ここで添付の図面を参照する。

【図面の簡単な説明】

【０００８】

【図１】キーフォブ及び制御ユニットの通常オペレーションを図示する。

【０００９】

【図２】一実施例においてキーフォブをディアクティベートするために用いることができる、キーフォブ保持及び無効化プロセスを図示する。

【００１０】

【図３】一実施例に従ったＯｐＫｅｙ認証を用いるキーフォブ及び制御ユニットの通常オペレーションを図示するフローチャートである。

【００１１】

【図４】ＯｐＫｅｙの保持及び無効化のためのプロセスを図示するフローチャートである。

【００１２】

【図５】一実施例に従った例示のキーフォブのブロック図である。

【００１３】

【図６】一実施例に従った例示の制御ユニットのブロック図である。

【発明を実施するための形態】

【００１４】

これ以降では、添付の図面を参照して本発明をより詳細に説明する。しかし、本発明は、多くの異なる形式において具現化され得、本明細書に記載の実施例に限定されると理解すべきではない。そうではなく、これらの実施例は、本開示が、行き届き、包括的であるように、そして、本発明の範囲が当業者に完全に理解されるように提供される。当業者であれば、本発明の種々の実施例を用いることが可能であり得る。

【００１５】

実施例は、送信可能であるが受信不能であるキーフォブに、秘密のＯｐＫｅｙのその所有を車両制御ユニットに認証させ得、一方で、第三者が、認証のためにキーフォブにより制御ユニットへ以前送られたメッセージを再生することによって真正のキーフォブに成りすますことを防止する。また、本発明により、真正の車両ユーザーは、失われた又は期限満了したキーフォブのＯｐＫｅｙを無効化し得るが、各残りの有効キーフォブのＯｐＫｅｙを保持し得る。

【００１６】

図１は、キーフォブ１０１及び制御ユニット１０２の通常オペレーションを図示する。初期ペアリングの後、キーフォブ１０１及び制御ユニット１０２は、秘密のＯｐＫｅｙを共有する。例えば、キーフォブ１０１及び制御ユニット１０２は、２０１３年８月１６日出願の同時係属中の米国特許出願、出願番号第１３／９６９，１５４号、発明の名称「一方向キーフォブ及び車両ペアリング」に開示されたシステム及び方法を用いてペアリング

され得、当該出願の開示は、全体として参照のためこの出願に組み込まれている。
【文献】米国特許出願番号第１３／９６９，１５４号
【００１７】
キーフォブ１０１及び制御ユニット１０２双方の間で共有されるＯｐＫｅｙに加えて、いずれのデバイスも１２８ビットカウンタ１０３、１０４を有する。他の実施例において、異なるサイズのカウンタが用いられ得る。通常オペレーションにおいて、キーフォブ１０１は、カウンタ１０３のＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値をつくる。キーフォブ１０１はその後、１２８ビットカウンタ１０３の８最下位ビット、及びカウンタ１０３のＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値の幾つかの所定のビットを制御ユニット１０２に送信する（１０５）。キーフォブは、各伝送の後そのカウンタ値を１増分し、１などの初期カウンタ値から開始する。メッセージ１０５自体の送信は、車両ドアのロック解除／ロックなど、キーフォブ１０１からのコマンドを表し得る。代替として、個別のコマンドデータフィールドが、キーフォブ１０１からの所望のコマンドを識別するためメッセージ１０５に含まれ得る。
【００１８】
メッセージ１０５を受信すると、制御ユニット１０２は、１２８ビットカウンタ１０４の８最下位ビットを設定するためキーフォブ１０１から受け取った８カウンタビットを用い、受け取った８ビットの値がカウンタ１０４の８最下位ビットの値より大きくない場合、カウンタ１０４の残りのビットの値を１増分する。また、制御ユニット１０２は、カウンタ１０４のＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値をつくる。制御ユニット１０２はその後、カウンタ１０４のそのＯｐＫｅｙ暗号化された値からの所定のビットを、カウンタ１０３のＯｐＫｅｙ暗号化された値を表すビットと比較する。制御ユニット１０２は、これらのビットが合致する場合、メッセージ１０５を及びそのためＯｐＫｅｙを認証する。
【００１９】
認証が失敗した場合、制御ユニット１０２は、カウンタ１０４をその変化の前の値に回復させる。
【００２０】
承認されていない又は偽のキーフォブ１０６が、ペアリングされることなくメッセージ１０７を制御ユニット１０２に送ろうと試みる場合、制御ユニット１０２はそのメッセージ１０７をリジェクトする。偽のキーフォブ１０６は、制御ユニット１０２のための有効ＯｐＫｅｙを有さない。また、偽のキーフォブ１０６は、有効メッセージのために用いる制御ユニット１０２のための適切なカウンタ値を知らない。
【００２１】
図２は、一実施例においてキーフォブをディアクティベートするために用いることができるキーフォブ保持及び無効化プロセスを図示する。この例では、３つのキーフォブ２０１～２０３が同じ制御ユニット２０４とペアリングされる。各ペアリングされたキーフォブ２０１～２０３は、制御ユニット２０４と共有される固有の秘密のＯｐＫｅｙ（ＯｐＫｅｙ１、ＯｐＫｅｙ２、ＯｐＫｅｙ３）を有する。また、各キーフォブ２０１～２０３は、それ自体のカウンタ２０５～２０７を有する。制御ユニット２０４は、各キーフォブ２０１～２０３に対し個別のカウンタ２０８～２１０を維持する。
【００２２】
キーフォブ２０３が失われたとき又は無効化される必要があるとき、ユーザーが下記工程を行い得る。第１に、ユーザーは、ＯｐＫｅｙ無効化モードに入るように制御ユニット２０４をプロンプトする。ＯｐＫｅｙ無効化モードは、残りのキーフォブ２０１、２０２からのメッセージにより、又は／及び制御ユニット２０４への何らかの他の入力により、トリガされ得る。
【００２３】
制御ユニット２０４がＯｐＫｅｙ無効化モードにある一方で、ユーザーは、各残りのキーフォブ２０１、２０２が制御ユニット２０４と通常オペレーションを行うようにプロン

プトする。例えば、各キーフォブ２０１、２０２は、そのＯｐＫｅｙから導出されるメッセージ１０５（図１）などのメッセージを制御ユニット２０４に送る。各残りのキーフォブ２０１、２０２がそのメッセージを送ったか又は制御ユニット２０４とオペレーションを行った後、ユーザーは、ＯｐＫｅｙ保持モードを出るように制御ユニットをプロンプトする。キーフォブ２０３は、失われたか又はもはや承認されないため、無効化モードの間メッセージを送らない。

【００２４】

制御ユニット２０４は、無効化モードを出る前に受け取ったＯｐＫｅｙのみを保持する。一実施例において、制御ユニット２０４は、無効化モードに入る前に受け取った最後のＯｐＫｅｙ、及び無効化モードの間受け取った全てのＯｐＫｅｙを保持する。他の実施例において、制御ユニット２０４は、無効化モードの間受け取ったＯｐＫｅｙのみを保持する。全ての他のＯｐＫｅｙ（例えば、ＯｐＫｅｙ３）は制御ユニット２０４により削除される。これにより、失くした又は承認されていないキーフォブが、無効化手順の後制御ユニット２０４と動作しないようにされる。

【００２５】

図３は、ＯｐＫｅｙ認証を用いるキーフォブ及び制御ユニットの通常オペレーションのためのプロセスを図示するフローチャートである。ステップ３０１において、キーフォブは、１２８ビットカウンタの８最下位ビットを読む。ステップ３０２において、キーフォブは、キーフォブカウンタのＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値を生成する。ステップ３０３において、キーフォブカウンタの８最下位ビット及びＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値からの幾つかの選択されたビットが制御ユニットに送られる。この情報は、キーフォブによる特定のコマンド又はリクエストに関連付けられ得る。

【００２６】

ステップ３０４において、制御ユニットは、キーフォブから受け取った８最下位ビットに基づいて制御ユニットカウンタを更新する。一実施例に従って、この更新は、制御ユニットカウンタの８最下位ビットを、キーフォブカウンタの受け取った８最下位ビットに設定することにより、及び、キーフォブカウンタの受け取ったビットの値が制御ユニットカウンタの対応するビットの値より大きくない場合に制御ユニットカウンタの残りのビットの値を１増分することにより成される。ステップ３０５において、制御ユニットは、更新された制御ユニットカウンタのＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値を生成する。制御ユニットは、制御ユニットカウンタのＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値の選択されたビットを、キーフォブから受け取ったキーフォブカウンタのＡＥＳ‐１２８、ＯｐＫｅｙ暗号化された値の選択されたビットと比較する。

【００２７】

選択されたビットが合致する場合、これは、両方のデバイスが同じＯｐＫｅｙ及びカウンタ値を用いたことを示しており、制御ユニットは、キーフォブからのコマンド又はリクエストを認証する。

【００２８】

図４は、ＯｐＫｅｙの保持及び無効化のためのプロセスを図示するフローチャートである。ステップ４０１において、残りの（即ち、失われていない）又は新たなキーフォブが通常オペレーションを完了した直後、ユーザーは、ＯｐＫｅｙ無効化モードに入るように制御ユニットをプロンプトする。ユーザーはその後、制御ユニットと通常オペレーションを行うように各残りの又は許可されたキーフォブをプロンプトする。通常オペレーションは、図１及び図３に図示するような送信、又はキーフォブにＯｐＫｅｙ暗号化された値を制御ユニットに送らせ得る任意のオペレーションに関与し得る。

【００２９】

ステップ４０３において、ユーザーは、残りの全ての又は許可されたキーフォブが通常オペレーションを完了した後、ＯｐＫｅｙ無効化モードを出るように制御ユニットをプロンプトする。例えば、ユーザーは、無効化モードを出るように「終了」ボタンをアクティブにし得、又は無効化モードは、一連の時間期間後終了し得る。

【００３０】
ステップ４０４において、制御ユニットは、ＯｐＫｅｙ無効化モードに入る前に動作した最後のキーフォブに関連付けられるＯｐＫｅｙと、無効化モードが終了する前に用いられたキーフォブに関連付けられる任意のＯｐＫｅｙとを除く全てのＯｐＫｅｙを削除する。失くした又は許可されていないキーフォブは、この短い無効化モード時間期間の間動作しない可能性が高いため、失くした又は許可されていないデバイスのためのＯｐＫｅｙは、制御ユニットから削除され得る。その結果、失くした及び許可されていないデバイスは、もはや制御ユニットとペアリングされず、コマンドを制御ユニットに送るためにもはや用いられ得ない。別の実施例において、無効化モードの間動作するキーフォブに関連付けられるＯｐＫｅｙのみが保持され、無効化モード期間の間オペレーションを実施しない全ての他のＯｐＫｅｙが削除される。
【００３１】
図５及び図６は、それぞれ、例示のキーフォブ５００及び制御ユニット６００のブロック図である。キーフォブ４００及び制御ユニット６００は各々、プロセッサ５０１、６０１、メモリ５０２、６０２、及びトランシーバ６０３又はトランスミッタ５０３を含む。デバイスのプロセッサ５０１、６０１は、カウンタを維持及び更新すること、ＯｐＫｅｙ暗号化された値を生成すること、及び、ペアリングされたデバイスからのＯｐＫｅｙのみが用いられることを認証するためにこのような値を比較することなどの、通常オペレーションを行うために用いられ得る。これらのプロセッサは、標準的なＣＰＵ、マイクロコントローラ、低電力デジタルシグナルプロセッサなどであり得、短時間に複雑な演算を実行することが可能であり得る。
【００３２】
デバイスのメモリ５０２、６０２は、ＯｐＫｅｙ、カウンタ値、暗号化された値、及び、キーフォブと制御ユニットとの間で交換される他のビットをストアするために用いられ得る。メモリは、フラッシュメモリ又はＥＥＰＲＯＭなどの不揮発性ストレージデバイスであり得る。
【００３３】
キーフォブトランスミッタ５０３及び制御ユニットトランシーバ６０３は、有線（図示せず）、ワイヤレス、又はその両方が可能であり得る。トランシーバ及びトランスミッタは、カウンタ値、ＯｐＫｅｙ暗号化されたデータ、及び、通常オペレーションの間及び無効化モードの間の他のビットを通信するためにデバイスにより用いられ得る。キーフォブにより、車両の又は他のデバイスの遠隔エントリ及び制御が可能となり、それらの伝送のために、Ｂｌｕｅｔｏｏｔｈ、ＬＦ、又はＵＨＦなどのワイヤレス技術を用い得る。キーフォブトランスミッタ５０３は、制御ユニット６００からの信号を送信のみ可能であり、受信はしない。
【００３４】
当業者であれば、本発明の特許請求の範囲内で、説明した例示の実施例に変形が成され得ること、及び多くの他の実施例が可能であることが分かるであろう。

【図面】

【図１】

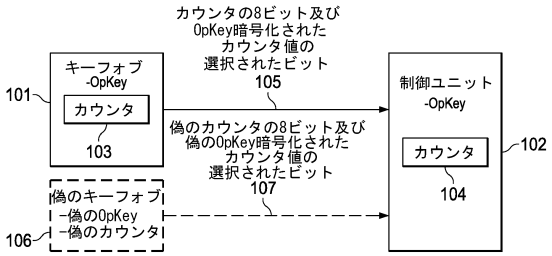

FIG. 1

【図２】

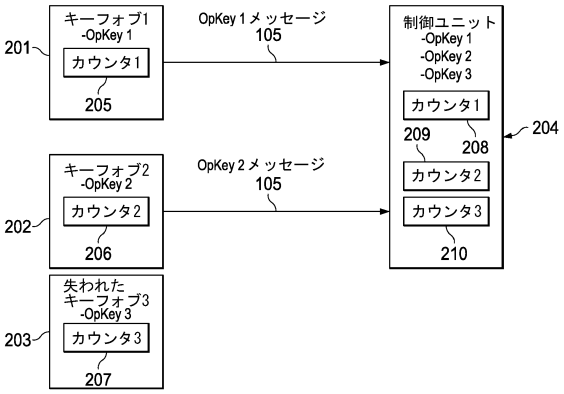

FIG. 2

【図３】

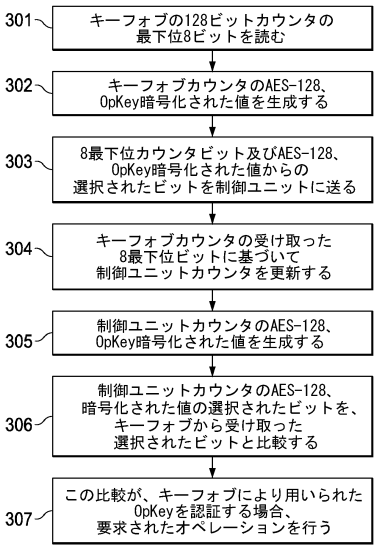

FIG. 3

【図４】

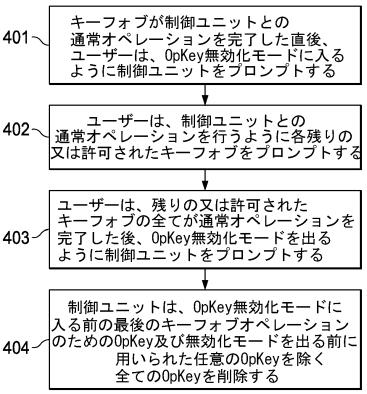

FIG. 4

【図５】

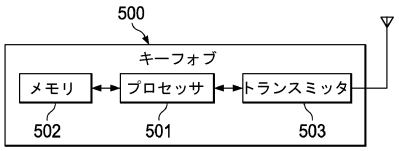

FIG. 5

【図６】

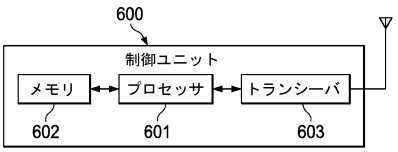

FIG. 6

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)

(56)参考文献
特開２００８－１９３５７５（ＪＰ，Ａ）
特開２００８－２６２２９９（ＪＰ，Ａ）
米国特許第０６７１８２４０（ＵＳ，Ｂ１）
米国特許出願公開第２０１０／００３９２１５（ＵＳ，Ａ１）
特開２０１０－１７９８３４（ＪＰ，Ａ）
特開２００８－０５０８８５（ＪＰ，Ａ）
米国特許出願公開第２００３／０１２９９４９（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０１２４３７４（ＵＳ，Ａ１）
米国特許第０６８２９３５７（ＵＳ，Ｂ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０９Ｃ　１／００
Ｇ０６Ｆ　２１／４４