

【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 28 年 9 月 15 日 (2016.9.15)

【公表番号】特表 2015-534322(P2015-534322A)

【公表日】平成 27 年 11 月 26 日 (2015.11.26)

【年通号数】公開・登録公報 2015-074

【出願番号】特願 2015-530107(P2015-530107)

【国際特許分類】

H 0 4 L 9/32 (2006.01)

【F I】

H 0 4 L 9/00 6 7 5 A

【手続補正書】

【提出日】平成 28 年 7 月 29 日 (2016.7.29)

【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】

キー FOB デバイスであって、
制御ユニットへ信号を送信するように構成されるトランスミッタと、
キー FOB カウンタと動作鍵 (O p K e y) とをストア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に結合されるプロセッサと、
を含み、
前記プロセッサが、
前記キー FOB カウンタの A E S - 1 2 8 O p K e y 暗号化された値を生成し、
前記キー FOB カウンタの所定の数の最下位ビットと前記キー FOB カウンタの前記 A
E S - 1 2 8 O p K e y 暗号化された値の所定の数のビットとを含むメッセージを前記
制御ユニットに送信し、
無効化手順に入るコマンドを前記制御ユニットに送信する、
ように構成される、キー FOB デバイス。

【請求項 2】

請求項 1 に記載のキー FOB デバイスであって、
前記キー FOB カウンタの前記所定の数の最下位ビットが 8 ビットである、キー FOB
デバイス。

【請求項 3】

請求項 1 に記載のキー FOB デバイスであって、
前記キー FOB カウンタが 1 2 8 ビットカウンタである、キー FOB デバイス。

【請求項 4】

請求項 1 に記載のキー FOB デバイスであって、
前記プロセッサが、前記メッセージを前記制御ユニットに送信した後に前記キー FOB
カウンタを 1 増分するように更に構成される、キー FOB デバイス。

【請求項 5】

請求項 1 に記載のキー FOB デバイスであって、
前記メッセージが、前記制御ユニットによって実行されるべきコマンドを識別するデー
タフィールドを更に含む、キー FOB デバイス。

【請求項 6】

制御ユニットデバイスであって、
キーフォブから信号を受信するように構成されるレシーバと、
制御ユニットカウンタと動作鍵 (OpKey) とをストアするように構成されるメモリと、
前記レシーバと前記メモリとに結合されるプロセッサと、
を含み、
前記プロセッサが、
キーフォブカウンタの AES - 128 OpKey 暗号化された値の所定の数のビットを含むメッセージを前記キーフォブから受け取り、
前記制御ユニットカウンタの AES - 128 OpKey 暗号化された値を生成し、
前記キーフォブカウンタの AES - 128 OpKey 暗号化された値の前記所定の数のビットが、前記制御ユニットカウンタの前記 AES - 128 OpKey 暗号化された値からの所定の数のビットと合致するか否かを認証し、
OpKey 無効化手順に入る、
ように、構成される、制御ユニットデバイス。

【請求項 7】

請求項 6 に記載の制御ユニットデバイスであって、
前記プロセッサが、
前記キーフォブカウンタの選ばれた数の最下位ビットを前記キーフォブから受け取り、
前記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前に、前記受け取ったビットと前記制御ユニットカウンタの対応するビットとに基づいて前記制御ユニットカウンタを更新する、
ように更に構成される、制御ユニットデバイス。

【請求項 8】

請求項 7 に記載の制御ユニットデバイスであって、
前記制御ユニットカウンタの前記選ばれた数の最下位ビットが 8 ビットである、制御ユニットデバイス。

【請求項 9】

請求項 6 に記載の制御ユニットデバイスであって、
前記プロセッサが、前記キーフォブカウンタの AES - 128 OpKey 暗号化された値の前記所定の数のビットが、前記制御ユニットカウンタの前記 AES - 128 OpKey 暗号化された値からの前記所定の数のビットと合致する場合に、制御オペレーションを開始するように更に構成される、制御ユニットデバイス。

【請求項 10】

請求項 6 に記載の制御ユニットデバイスであって、
前記制御ユニットカウンタが 128 ビットカウンタである、制御ユニットデバイス。

【請求項 11】

請求項 7 に記載の制御ユニットデバイスであって、
前記プロセッサが、前記キーフォブカウンタの AES - 128 OpKey 暗号化された値の前記所定の数のビットが、前記制御ユニットカウンタの前記 AES - 128 OpKey 暗号化された値からの前記所定の数のビットと合致することを認証することに失敗した後に前記制御ユニットカウンタを前記更新前の値に回復させるように更に構成される、制御ユニットデバイス。

【請求項 12】

請求項 6 に記載の制御ユニットデバイスであって、
前記メッセージが、前記制御ユニットによって実行されるべきコマンドを識別するデータフィールドを更に含む、制御ユニットデバイス。

【請求項 13】

請求項 6 に記載の制御ユニットであって、

前記プロセッサが、

OpKey無効化手順を開始するためのコマンドが検出されるときに、キーフォブから受信されるメッセージに関連付けられるOpKeyを記録し始め、

OpKey無効化手順を終わらせるためのコマンドが検出されるときに、キーフォブから受信されるメッセージに関連付けられるOpKeyの記録を終わらせる、
ように更に構成される、制御ユニットデバイス。

【請求項14】

請求項13に記載の制御ユニットであって、

前記プロセッサが、前記OpKey無効化手順を開始するための前記コマンドが検出されるときと前記OpKey無効化手順を終わらせるための前記コマンドが検出されるときとの間の期間の間に記録されていない任意のストアされたOpKeyを削除するように更に構成される、制御ユニットデバイス。

【請求項15】

請求項13に記載の制御ユニットであって、

前記プロセッサが更に、前記OpKey無効化手順を開始するための前記コマンドが検出されるときと前記OpKey無効化手順を終わらせるための前記コマンドが検出されるときとの間の期間の間に記録されていない、又は前記OpKey無効化手順を開始するための前記コマンドが検出される直前に記録されていない、任意のストアされたOpKeyを削除するように更に構成される、制御ユニットデバイス。

【請求項16】

制御ユニットにおいて保持されるべきキーフォブ動作鍵(OpKey)を選択するための方法であって、

OpKey無効化手順を開始するためのコマンドを前記制御ユニットにより受信することと、

キーフォブから受け取ったメッセージに関連付けられるOpKeyの記録を開始することと、

OpKey無効化手順を終わらせるためのコマンドを前記制御ユニットにより受信することと、

キーフォブから受け取ったメッセージに関連するOpKeyの記録を終わらせることと、

を含む、方法。

【請求項17】

請求項16に記載の方法であって、

前記OpKey無効化手順を開始するための前記コマンドが受信されるときと前記OpKey無効化手順を終わらせるための前記コマンドが受信されるときとの間の期間の間に記録されていない任意のストアされたOpKeyを削除することを更に含む、方法。

【請求項18】

請求項16に記載の方法であって、

前記OpKey無効化手順を開始するための前記コマンドが受信されるときと前記OpKey無効化手順を終わらせるための前記コマンドが受信されるときとの間の期間の間に記録されていない、又は前記OpKey無効化手順を開始するための前記コマンドが検出される直前に記録されていない、任意のストアされたOpKeyを削除することを更に含む、方法。