(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7008661号
(P7008661)

(45)発行日　令和4年1月25日(2022.1.25)

(24)登録日　令和4年1月13日(2022.1.13)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	２００Ｂ
Ｈ０４Ｌ　9/08　(2006.01)	Ｈ０４Ｌ	9/32	２００Ａ
Ｇ０９Ｃ　1/00　(2006.01)	Ｈ０４Ｌ	9/08	Ｃ
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０９Ｃ	1/00	６４０Ｅ
Ｂ６０Ｒ　16/02　(2006.01)	Ｇ０６Ｆ	21/44	

ＦＩ

請求項の数　8　（全20頁）　最終頁に続く

(21)出願番号　特願2019-102042(P2019-102042)
(22)出願日　令和1年5月31日(2019.5.31)
(65)公開番号　特開2020-198483(P2020-198483A)
(43)公開日　令和2年12月10日(2020.12.10)
審査請求日　令和3年3月29日(2021.3.29)

(73)特許権者　000005326
本田技研工業株式会社
東京都港区南青山二丁目１番１号
(74)代理人　100154380
弁理士　西村 隆一
(74)代理人　100081972
弁理士　吉田 豊
(72)発明者　大口 良輔
埼玉県和光市中央１丁目４番１号 株式会社本田技術研究所内
(72)発明者　沖 秀一
埼玉県和光市中央１丁目４番１号 株式会社本田技術研究所内
(72)発明者　天沼 佳幸
埼玉県和光市中央１丁目４番１号 株式
最終頁に続く

(54)【発明の名称】　認証システム

(57)【特許請求の範囲】

【請求項１】

車両に搭載される車両制御装置と、

前記車両制御装置と通信可能に接続され、前記車両制御装置の制御プログラムを更新する更新装置と、

前記更新装置と通信可能に接続され、前記更新装置の正当性を認証する認証サーバと、を備えた認証システムであって、

前記更新装置は、

第１乱数を生成する第１乱数生成部と、

所定の関数に、定数と、前記第１乱数生成部により生成された前記第１乱数と、を代入して第１値を生成し、前記認証サーバに送信する第１代入部と、を有し、

前記認証サーバは、所定の秘密鍵により、前記更新装置から送信された前記第１値の署名を生成して前記更新装置に送信する署名生成部を有し、

さらに前記更新装置は、

前記第１代入部により生成された前記第１値と、前記認証サーバから送信された前記署名と、を記憶する記憶部と、

前記車両制御装置に接続されると、前記記憶部に記憶された前記第１値と前記署名とを前記車両制御装置に転送する転送部と、を有し、

前記車両制御装置は、

前記秘密鍵に対応する所定の公開鍵により、前記更新装置から送信された前記署名が有効

であるか否かを検証する署名検証部と、
第２乱数を生成する第２乱数生成部と、
前記関数に、前記定数と、前記第２乱数生成部により生成された前記第２乱数と、を代入して第２値を生成し、前記更新装置に送信する第２代入部と、を有し、
前記第１代入部は、前記関数に、前記車両制御装置から送信された前記第２値と、前記第１乱数生成部により生成された前記第１乱数と、を代入して第３値を生成し、
前記第２代入部は、前記署名検証部により前記署名が有効であると確認されると、前記関数に、前記更新装置から送信された前記第１値と、前記第２乱数生成部により生成された前記第２乱数と、を代入して第４値を生成し、
さらに前記車両制御装置は、
前記第１代入部により生成された前記第３値と、前記第２代入部により生成された前記第４値と、が一致するか否かを判定し、一致すると判定すると、前記更新装置が前記認証サーバにより正当性が認証された更新装置であると判定する認証判定部と、
前記更新装置による前記制御プログラムの更新を許可する更新許可部と、を有することを特徴とする認証システム。
【請求項２】
請求項１に記載の認証システムにおいて、
前記車両制御装置は、前記更新装置が接続されると、第３乱数を生成して前記更新装置に送信する第３乱数生成部をさらに有し、
前記更新装置は、前記第１代入部により生成された前記第３値により、前記車両制御装置から送信された前記第３乱数を暗号化し、暗号化された第３乱数を前記車両制御装置に送信する暗号化部をさらに有し、
さらに前記車両制御装置は、前記第２代入部により生成された前記第４値により、前記更新装置から送信された前記暗号化された第３乱数を復号する復号部を有し、
前記認証判定部は、前記第３乱数生成部により生成された第３乱数と、前記復号部により復号された第３乱数と、が一致するか否かを判定し、一致すると判定すると、前記第１代入部により生成された前記第３値と、前記第２代入部により生成された前記第４値と、が一致すると判定することを特徴とする認証システム。
【請求項３】
請求項１に記載の認証システムにおいて、
前記車両制御装置は、前記更新装置が接続されると、第３乱数を生成して前記更新装置に送信する第３乱数生成部をさらに有し、
前記更新装置は、前記第１代入部により生成された前記第３値により、前記車両制御装置から送信された前記第３乱数を暗号化し、暗号化された第３乱数を前記車両制御装置に送信する第１暗号化部をさらに有し、
さらに前記車両制御装置は、前記第２代入部により生成された前記第４値により、前記第３乱数生成部により生成された前記第３乱数を暗号化する第２暗号化部を有し、
前記認証判定部は、前記更新装置から送信された暗号化された第３乱数と、前記第２暗号化部により暗号化された第３乱数と、が一致するか否かを判定し、一致すると判定すると、前記第１代入部により生成された前記第３値と、前記第２代入部により生成された前記第４値と、が一致すると判定することを特徴とする認証システム。
【請求項４】
請求項１に記載の認証システムにおいて、
前記車両制御装置は、前記更新装置が接続されると、第３乱数を生成して前記更新装置に送信する第３乱数生成部をさらに有し、
前記更新装置は、前記第１代入部により生成された前記第３値により、前記車両制御装置から送信された前記第３乱数のメッセージ認証コードを生成して前記車両制御装置に送信する第１メッセージ認証コード生成部をさらに有し、
さらに前記車両制御装置は、前記第２代入部により生成された前記第４値により、前記第３乱数生成部により生成された前記第３乱数のメッセージ認証コードを生成する第２メッ

セージ認証コード生成部を有し、
前記認証判定部は、前記更新装置から送信されたメッセージ認証コードと、前記第２メッセージ認証コード生成部により生成されたメッセージ認証コードと、が一致するか否かを判定し、一致すると判定すると、前記第１代入部により生成された前記第３値と、前記第２代入部により生成された前記第４値と、が一致すると判定することを特徴とする認証システム。
【請求項５】
請求項１に記載の認証システムにおいて、
前記車両制御装置は、前記更新装置が接続されると、第３乱数を生成する第３乱数生成部と、
前記第２代入部により生成された前記第４値により、前記第３乱数生成部により生成された第３乱数を暗号化し、暗号化された第３乱数を前記更新装置に送信する暗号化部と、をさらに有し、
前記更新装置は、前記第１代入部により生成された前記第３値により、前記車両制御装置から送信された前記暗号化された第３乱数を復号し、復号された第３乱数を前記車両制御装置に送信する復号部をさらに有し、
前記認証判定部は、前記第３乱数生成部により生成された第３乱数と、前記更新装置から送信された復号された第３乱数と、が一致するか否かを判定し、一致すると判定すると、前記第１代入部により生成された前記第３値と、前記第２代入部により生成された前記第４値と、が一致すると判定することを特徴とする認証システム。
【請求項６】
請求項１～５のいずれか１項に記載の認証システムにおいて、
前記署名は所定期間有効であることを特徴とする認証システム。
【請求項７】
請求項６に記載の認証システムにおいて、
前記署名生成部は、前記所定期間を設定することを特徴とする認証システム。
【請求項８】
請求項６または７に記載の認証システムにおいて、
前記署名は、前記所定期間内であっても、前記更新装置と前記認証サーバとが非接続状態から接続状態になると無効になることを特徴とする認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両の制御プログラムを更新する装置を認証する認証システムに関する。
【背景技術】
【０００２】
従来、車両のソフトウェアを更新するための装置の正当性を、認証サーバが認証するようにしたシステムが知られている。例えば特許文献１記載のシステムでは、ソフトウェアの更新用のコンピュータが構成証明データを認証サーバに送信し、認証サーバが構成証明データに基づいてそのコンピュータの正当性を確認して認証情報を生成することで、車両に搭載された機器が認証情報を確認してコンピュータとの接続を許可する。
【先行技術文献】
【特許文献】
【０００３】
特許文献１：特開２０１４－４８８００号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上記特許文献１記載の装置では、ソフトウェアの更新時においてコンピュータ（ソフトウェアの更新用の装置）が認証サーバと接続される必要があるため、ネット

ワーク圏外で車両のソフトウェアを更新することは難しい。
【課題を解決するための手段】
【０００５】
本発明の一態様である認証システムは、車両に搭載される車両制御装置と、車両制御装置と通信可能に接続され、車両制御装置の制御プログラムを更新する更新装置と、更新装置と通信可能に接続され、更新装置の正当性を認証する認証サーバと、を備える。更新装置は、第１乱数を生成する第１乱数生成部と、所定の関数に、定数と、第１乱数生成部により生成された第１乱数と、を代入して第１値を生成し、認証サーバに送信する第１代入部と、を有する。認証サーバは、所定の秘密鍵により、更新装置から送信された第１値の署名を生成して更新装置に送信する署名生成部を有する。さらに更新装置は、第１代入部により生成された第１値と、認証サーバから送信された署名と、を記憶する記憶部と、車両制御装置に接続されると、記憶部に記憶された第１値と署名とを車両制御装置に転送する転送部と、を有する。車両制御装置は、秘密鍵に対応する所定の公開鍵により、更新装置から送信された署名が有効であるか否かを検証する署名検証部と、第２乱数を生成する第２乱数生成部と、関数に、定数と、第２乱数生成部により生成された第２乱数と、を代入して第２値を生成し、更新装置に送信する第２代入部と、を有する。第１代入部は、関数に、車両制御装置から送信された第２値と、第１乱数生成部により生成された第１乱数と、を代入して第３値を生成する。第２代入部は、署名検証部により署名が有効であると確認されると、関数に、更新装置から送信された第１値と、第２乱数生成部により生成された第２乱数と、を代入して第４値を生成する。さらに車両制御装置は、第１代入部により生成された第３値と、第２代入部により生成された第４値と、が一致するか否かを判定し、一致すると判定すると、更新装置が認証サーバにより正当性が認証された更新装置であると判定する認証判定部と、更新装置による制御プログラムの更新を許可する更新許可部と、を有する。
【発明の効果】
【０００６】
本発明によれば、認証された機器によりネットワーク圏外において車両の制御プログラムを更新することができる。
【図面の簡単な説明】
【０００７】
【図１】本発明の実施形態に係る認証システムを概略的に示す図。
【図２】本発明の実施形態に係る認証システムの構成の一例を示すブロック図。
【図３】図２の認証システムにより実行される処理の一例を示すフローチャート。
【図４】図２の認証システムによる処理を説明する図。
【図５】本発明の第１の変形例に係る認証システムの構成を示すブロック図。
【図６】図５の認証システムにより実行される処理の一例を示すフローチャート。
【図７】図５の認証システムによる処理を説明する図。
【図８】本発明の第２の変形例に係る認証システムの構成を示すブロック図。
【図９】図５の認証システムにより実行される処理の一例を示すフローチャート。
【図１０】図５の認証システムによる処理を説明する図。
【図１１】本発明の第３の変形例に係る認証システムの構成を示すブロック図。
【図１２】図５の認証システムにより実行される処理の一例を示すフローチャート。
【図１３】図５の認証システムによる処理を説明する図。
【発明を実施するための形態】
【０００８】
以下、図１～図１３を参照して本発明の実施形態について説明する。図１は、本発明の実施形態に係る認証システム１００の構成を概略的に示す図である。認証システム１００は、車両に搭載されて車両の動作等を制御する車両制御装置１０と、車両制御装置１０に接続されて車両を制御するためのソフトウェアプログラム（車両制御プログラム）を更新する更新装置２０と、更新装置２０の正当性を認証する認証サーバ３０とを備える。車両制

御装置１０と更新装置２０とは、例えば、車両のＤＬＣ（Data Link Coupler）を介してＣＡＮ（Controller Area Network）通信等により有線接続される。更新装置２０と認証サーバ３０とは、インターネット網や携帯電話網などに代表される公衆無線通信網を含むネットワーク４を介して接続される。

【０００９】

車両メーカは、車両制御プログラムのアップデートや品質改善などの必要に応じ、販売店等を通じて更新用プログラムを配布する。販売店等では、来店した顧客の車両の車両制御装置１０に、更新用プログラムをダウンロードした更新装置２０を接続して、車両制御プログラムを更新する。車両制御装置１０は、悪意のある第三者によって不正なハードウェアやソフトウェアにより車両制御プログラムが書き換えられることを防止するため、車両メーカの認証サーバ３０により認証された更新装置２０による更新のみを許可する。車両制御プログラムの更新は、止むを得ずネットワーク４の圏外で行う場合もあるが、このような場合は更新装置２０が認証サーバ３０による認証を受けることが難しい。そこで、本発明の実施形態に係る認証システム１００は、ネットワーク圏外において不正アクセスを排除しつつ車両制御プログラムを更新するよう、以下のように構成する。

【００１０】

図２は、認証システム１００の構成の一例を概略的に示すブロック図である。図２に示すように、認証システム１００は、車両制御装置１０と、ＣＡＮ通信等により車両制御装置１０と接続可能な更新装置２０と、ネットワーク４を介して更新装置２０と接続可能な認証サーバ３０とを備える。

【００１１】

更新装置２０は、車両に接続して運転履歴等の車両情報を取得する診断機などの専用機器であり、使用ユーザに対して予め車両のメーカによりＩＤおよびパスワード等の認証情報が割り当てられ、専用のソフトウェアがインストールされる。更新装置２０は、ＣＰＵ等の演算部２１と、ＲＯＭ，ＲＡＭ，ハードディスク等の記憶部２２と、その他の周辺回路とを有するコンピュータを含んで構成され、通信部２３を介してネットワーク４に接続可能である。演算部２１は、機能的構成として、認証情報生成部２１０と、第１乱数生成部２１１と、代入部２１２と、転送部２１３と、コード暗号化部２１４とを有する。

【００１２】

車両制御プログラムの更新を行う更新装置２０と車両制御装置１０との間のデータ通信では、安全で高速な送受信を実現するため、データの暗号化と復号に同一の共通鍵を用いる共通鍵暗号化方式が用いられる。この場合、例えば、更新装置２０と車両制御装置１０との間で、離散対数問題を使用するディフィ・ヘルマン鍵共有アルゴリズムを用いた鍵交換を行うことにより、共通鍵を事前に共有することなく、互いに同一の共通鍵を生成して共有することができる。楕円曲線上の離散対数問題を使用する楕円曲線ディフィ・ヘルマン鍵共有アルゴリズムを用いてもよい。以下では、ディフィ・ヘルマン鍵共有アルゴリズムを用いて鍵交換を行う例を説明する。

【００１３】

認証情報生成部２１０は、ユーザからの認証要求が入力されると、更新装置２０の認証情報を生成し、ネットワーク４を介して認証サーバ３０に送信する。ネットワーク４の圏外で更新装置２０により車両制御プログラムの更新を行うユーザは、事前にネットワーク４の圏内で更新装置２０に認証要求を入力し、認証サーバ３０による認証を受ける。認証情報には、車両のメーカにより更新装置２０の使用ユーザに割り当てられたＩＤおよびパスワード等の識別情報が含まれる。認証サーバ３０は、更新装置２０から送信された認証情報を検証することで、更新装置２０のハードウェアの正当性を認証する。認証情報には、更新装置２０のソフトウェア構成を証明する構成証明情報を含めてもよい。この場合、認証サーバ３０は、更新装置２０から送信された構成証明情報を検証することで、更新装置２０のソフトウェアの正当性を認証する。

【００１４】

認証要求では有効期間を指定することができる。例えば、ネットワーク４の圏外で車両制

御プログラムの更新を行う予定の期間を有効期間として指定することができる。認証情報生成部２１０は、認証要求において指定された有効期間を認証情報とともに認証サーバ３０に送信する。

【００１５】

第１乱数生成部２１１は、ディフィ・ヘルマン鍵共有アルゴリズムにおける更新装置２０側の秘密鍵である第１乱数ａを生成する。第１乱数ａは、２以上の整数であり、認証要求時にランダムに生成される。

【００１６】

代入部２１２は、所定の関数Ｆに、予め設定された定数Ｇ（整数）と、第１乱数生成部２１１により生成された第１乱数ａとを代入して、鍵交換用の公開鍵である第１値Ａを生成する（式(i)，(ii)）。式(i)，(ii)中の値Ｎを巨大素数とすることで、鍵交換用の公開鍵（第１値Ａ）から秘密鍵（第１乱数ａ）を求めることが極めて困難となる。

Ｆ（ｘ，ｙ）＝ｘ＾ｙ　ｍｏｄ　Ｎ　　・・・(i)

Ａ＝Ｆ（Ｇ，ａ）＝Ｇ＾ａ　ｍｏｄ　Ｎ　　・・・(ii)

【００１７】

代入部２１２により生成された第１値Ａは、記憶部２２に記憶されるとともに、ネットワーク４を介して認証サーバ３０に送信される。このとき、認証要求において有効期間が指定されている場合は、その情報も認証サーバ３０に送信される。認証サーバ３０は、更新装置２０の正当性を認証することができた場合には、更新装置２０から送信された第１値Ａの署名を生成し、ネットワーク４を介して更新装置２０に送信する。認証サーバ３０から送信された署名は、記憶部２２に記憶される。

【００１８】

転送部２１３は、更新装置２０がＣＡＮ通信等により車両制御装置１０に有線接続されると、記憶部２２に記憶された第１値Ａと署名とを車両制御装置１０に転送する。車両制御装置１０は、更新装置２０から第１値Ａと署名とを受信すると、署名を検証し、署名の有効性が確認されると更新装置２０との鍵交換を許可する。鍵交換が許可されると、車両制御装置１は、更新装置２０側と同様に鍵交換用の公開鍵である第２値Ｂ（式(iii)）を生成して更新装置２０に送信するとともに、後述するチャレンジコードを生成して更新装置２０に送信する。

Ｂ＝Ｆ（Ｇ，ｂ）＝Ｇ＾ｂ　ｍｏｄ　Ｎ　　・・・(iii)

【００１９】

代入部２１２は、車両制御装置１０から公開鍵である第２値Ｂを受信すると、関数Ｆに、受信した第２値Ｂと、第１乱数生成部２１１により生成された第１乱数ａとを代入して、車両制御装置１０とのデータ通信で使用する共通鍵となる第３値Ｃを生成する（式(iv)）。さらに第３値を加工してもよい。この場合は、後述する第４値に対しても同様の加工を行う。代入部２１２により生成された第３値Ｃは、記憶部２２に記憶される。

Ｃ＝Ｆ（Ｂ，ａ）＝Ｂ＾ａ　ｍｏｄ　Ｎ　　・・・(iv)

【００２０】

コード暗号化部２１４は、代入部２１２により生成された共通鍵である第３値Ｃにより、車両制御装置１０から送信されたチャレンジコード（後述）を暗号化する。例えば、車両制御装置１０から送信されたチャレンジコードと代入部２１２により生成された第３値Ｃとを組み合わせ、周知のハッシュ関数を用いてハッシュ値に変換したレスポンスコードとして車両制御装置１０に送信する。

【００２１】

認証サーバ３０は、ＣＰＵ等の演算部３１と、ＲＯＭ，ＲＡＭ，ハードディスク等の記憶部３２と、その他の周辺回路とを有するコンピュータを含んで構成され、通信部３３を介してネットワーク４に接続可能である。演算部３１は、機能的構成として、更新装置認証部３１０と、署名生成部３１１とを有する。

【００２２】

記憶部３２には、公開鍵暗号化方式による秘密鍵が記憶される。秘密鍵に対応する公開鍵

は、車両制御装置１０の製造時に登録される。
【００２３】
更新装置認証部３１０は、更新装置２０から送信された認証情報を検証し、更新装置２０の正当性を認証する。例えば、更新装置２０から送信されたＩＤおよびパスワードが車両のメーカにより割り当てられたものであると確認されると更新装置２０のハードウェアの正当性を認証し、更新装置２０のソフトウェア構成が車両のメーカにより定められた専用のソフトウェアと同一であることが確認されると更新装置２０のソフトウェアの正当性を認証する。
【００２４】
署名生成部３１１は、更新装置認証部３１０により更新装置２０の正当性が認証されると、記憶部３２に記憶された秘密鍵により、更新装置２０から送信された第１値Ａの署名を生成する。すなわち、周知のハッシュ関数を用いて更新装置２０から送信された第１値Ａをハッシュ値に変換し、ハッシュ値を秘密鍵で暗号化して署名を生成し、ネットワーク４を介して更新装置２０に送信する。この場合、署名には有効期間が設定される。署名の有効期間は、所定期間（例えば、認証時点から２４時間）に設定されてもよく、更新装置２０から送信された有効期間に応じて設定されてもよい。署名の有効期間は、更新装置２０が認証サーバ３０の認証を受けた後、所定時間（例えば、１０分間）以上ネットワーク４の圏外に存在した後に、再度、更新装置２０がネットワーク４の圏内に入ると強制的に終了するように設定することもできる。これは、更新装置２０が認証サーバ３０の認証を受けた後、ネットワーク４の圏外にて所定の作業を終え、ネットワーク４の圏内の所定の場所へ戻されたことにより、残存する有効期間は不要と判断できるためである。
【００２５】
車両制御装置１０は、エンジン制御用ＥＣＵ、変速機制御用ＥＣＵ等、機能の異なる複数のＥＣＵからなる電子制御ユニットにより構成される。車両制御装置１０は、ＣＰＵ等の演算部１１と、ＲＯＭ，ＲＡＭ，ハードディスク等の記憶部１２と、その他の周辺回路とを有するコンピュータを含んで構成される。演算部１１は、機能的構成として、署名検証部１１０と、第２乱数生成部１１１と、代入部１１２と、コード生成部１１３と、コード復号部１１４と、認証判定部１１５と、更新許可部１１６とを有する。
【００２６】
記憶部１２には、認証サーバ３０に登録された秘密鍵に対応する公開鍵が記憶される。公開鍵暗号化方式では、互いに異なる一対の公開鍵および秘密鍵が生成され、各種情報データの送信側および受信側により事前共有される。公開鍵および秘密鍵の一方で暗号化された各種情報データは、公開鍵および秘密鍵の他方で復号される。例えば、認証サーバ３０の秘密鍵で暗号化された各種情報データは、車両制御装置１０の公開鍵で復号される。これにより、ネットワーク４を介して安全に各種情報データを送受信することができる。
【００２７】
署名検証部１１０は、記憶部１２に記憶された公開鍵により、更新装置２０から送信された署名が有効であるか否かを検証する。例えば、更新装置２０から送信された署名を公開鍵で復号してハッシュ値に戻すとともに、更新装置２０から送信された第１値Ａのハッシュ値を生成し、これらのハッシュ値が一致するか否かに基づいて署名の正当性を検証する。これにより、更新装置２０から送信された第１値Ａが認証サーバ３０により署名されたこと、および認証後に改ざんされていないことを確認することできる。署名検証部１１０は、現在時刻が署名の有効期間内であるか否かも確認する。署名検証部１１０は、署名の有効性が確認されると、更新装置２０との鍵交換を許可する。
【００２８】
第２乱数生成部１１１は、署名検証部１１０により鍵交換が許可されると、車両制御装置１０側の秘密鍵である第２乱数ｂ（２以上の整数）をランダムに生成する。
【００２９】
代入部１１２は、関数Ｆに、定数Ｇと、第２乱数生成部１１１により生成された第２乱数ｂとを代入して、車両制御装置１０側の公開鍵である第２値Ｂ（式(iii)）を生成し、ＣＡ

Ｎ通信等を介して更新装置２０に送信する。また、関数Ｆに、更新装置２０から送信された公開鍵である第１値Ａと、第２乱数生成部１１１により生成された第２乱数ｂとを代入して、更新装置２０とのデータ通信で使用する共通鍵となる第４値Ｄを生成する（式(v)）。さらに第４値を加工してもよい。この場合は、前述の第３値に対しても同様の加工を行う。代入部１１２により生成された第４値Ｄは、記憶部１２に記憶される。

Ｄ＝Ｆ（Ａ，ｂ）＝Ａ＾ｂ　ｍｏｄ　Ｎ　　・・・(v)

【００３０】

ここで、式(ii)～(v)より、車両制御装置１０側で生成された共通鍵である第４値Ｄは、更新装置２０側の秘密鍵である第１乱数ａが認証後に改ざんされていなければ、更新装置２０側で生成された共通鍵である第３値Ｃと同一の値となる（式(vi)）。

Ｄ＝Ａ＾ｂ　ｍｏｄ　Ｎ
＝（Ｇ＾ａ　ｍｏｄ　Ｎ）＾ｂ　ｍｏｄ　Ｎ
＝Ｇ＾ａｂ　ｍｏｄ　Ｎ
＝（Ｇ＾ｂ　ｍｏｄ　Ｎ）＾ａ　ｍｏｄ　Ｎ
＝Ｂ＾ａ　ｍｏｄ　Ｎ＝Ｃ　　・・・(vi)

【００３１】

認証システム１００では、車両制御装置１０側の共通鍵である第４値Ｄと更新装置２０側の共通鍵である第３値Ｃとが互いに同一の値であるか否かを判定することで、更新装置２０が認証サーバ３０により正当性を認証されたものであるか否かを判定する。これにより、ネットワーク４の圏外で車両制御装置１０側から更新装置２０が認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。

【００３２】

コード生成部１１３は、更新装置２０が接続されると、乱数からなるコードを生成し、チャレンジコードとして更新装置２０に送信する。チャレンジコードは、生成される度に不規則に変化する一種のワンタイムパスワードである。コード生成部１１３により生成されたコードは、記憶部１２に記憶される。更新装置２０は、車両制御装置１０から送信されたチャレンジコードを共通鍵（第３値Ｃ）で暗号化し、レスポンスコードとして車両制御装置１０に送信する。

【００３３】

コード復号部１１４は、記憶部１２に記憶された共通鍵（第４値Ｄ）により、更新装置２０から送信されたレスポンスコードを復号する。記憶部１２に記憶された車両制御装置１０側の共通鍵（第４値Ｄ）が更新装置２０側の共通鍵（第３値Ｃ）と同一の値であれば、更新装置２０側で暗号化されたコードは車両制御装置１０側で元のコードと同一の値に復号される。

【００３４】

認証判定部１１５は、コード復号部１１４により復号されたコードとコード生成部１１３により生成されたコードとが一致するか否かを判定し、一致すると判定すると、共通鍵である第３値Ｃと第４値Ｄとが互いに同一の値であると判定する。車両制御装置１０および更新装置２０の両者の共通鍵が同一の値であると判定されると、更新装置２０が認証サーバ３０により正当性を認証されたものであると判定される。

【００３５】

更新許可部１１６は、認証判定部１１５により更新装置２０が認証サーバ３０により正当性を認証されたものであると判定されると、更新装置２０による車両制御装置１０のセキュア領域へのアクセスおよび車両制御プログラムの更新を許可する。

【００３６】

図３は、認証システム１００により実行される処理の一例を示すフローチャートであり、予め記憶されたプログラムに従い、車両制御装置１０の演算部１１で実行される認証確認処理、更新装置２０の演算部２１で実行される認証要求処理、および認証サーバ３０の演算部３１で実行される認証処理の一例を示す。このフローチャートに示す処理は、例えば更新装置２０にユーザからの認証要求が入力されると開始される。

【００３７】
更新装置２０による認証要求処理では、まず、ステップＳ２００で、認証情報生成部２１０での処理により、更新装置２０の認証情報を生成して認証サーバ３０に送信する。次いでステップＳ２０１で、第１乱数生成部２１１での処理により第１乱数ａ（秘密鍵）を生成し、代入部２１２での処理により関数Ｆに定数Ｇと第１乱数ａとを代入して第１値Ａ（鍵交換用の公開鍵）を生成する。また、生成された第１値Ａを、認証要求において指定された有効期間とともに認証サーバ３０に送信する。
【００３８】
認証サーバ３０による認証処理では、ステップＳ３００，Ｓ３０１で、通信部３３を介して更新装置２０から送信された認証情報および第１値Ａをそれぞれ受信する。次いでステップＳ３０２で、更新装置認証部３１０での処理により、認証情報を検証して更新装置２０の正当性を認証する。ステップＳ３０２で更新装置２０の正当性が認証されると、ステップＳ３０３で、署名生成部３１１での処理により、事前共有された秘密鍵で第１値Ａのハッシュ値を暗号化して有効期間付きの署名を生成し、更新装置２０に送信する。ステップＳ３０２で更新装置２０の正当性が認証されない場合は、認証サーバ３０での認証処理を終了する。
【００３９】
更新装置２０では、ステップＳ２０２で通信部２３を介して認証サーバ３０から送信された有効期間付きの署名を受信すると、ステップＳ２０３で更新装置２０が車両制御装置１０に接続されるまで待機する。ステップＳ２０３で更新装置２０が車両制御装置１０に接続されると、ステップＳ２０４で、転送部２１３での処理により、記憶部２２に記憶された第１値Ａ（公開鍵）および有効期間付きの署名を車両制御装置１０に転送する。
【００４０】
車両制御装置１０による認証確認処理では、ステップＳ１００で、ＣＡＮ通信等を介して更新装置２０から送信された第１値Ａ（公開鍵）および有効期間付きの署名を受信する。次いでステップＳ１０１で、署名検証部１１０での処理により、事前共有された公開鍵で署名を復号してハッシュ値に戻すとともに第１値Ａのハッシュ値を生成し、これらが一致するか否かに基づいて署名の正当性を検証する。ステップＳ１０１で署名の正当性が確認されると、ステップＳ１０２で、現在時刻が署名の有効期間内であるか否かを判定する。ステップＳ１０１またはＳ１０２で否定されて署名の有効性が確認されない場合は、車両制御装置１０での認証確認処理を終了する。
【００４１】
ステップＳ１０１およびＳ１０２で肯定されて署名の有効性が確認されると、ステップＳ１０３で、第２乱数生成部１１１での処理により、第２乱数ｂ（秘密鍵）を生成する。また、代入部１１２での処理により、関数Ｆに定数Ｇと第２乱数ｂとを代入して第２値Ｂ（鍵交換用の公開鍵）を生成し、更新装置２０に送信する。次いでステップＳ１０４で、関数Ｆに、ステップＳ１００で受信された第１値Ａ（公開鍵）と、ステップＳ１０３で生成された第２乱数ｂ（秘密鍵）とを代入して第４値Ｄ（共通鍵）を生成する。次いでステップＳ１０５で、コード生成部１１３での処理により、乱数からなるコードを生成し、チャレンジコードとして更新装置２０に送信する。
【００４２】
更新装置２０では、ステップＳ２０５で、車両制御装置１０から送信された第２値Ｂを受信すると、ステップＳ２０６で、代入部２１２での処理により、第３値Ｃ（共通鍵）を生成する。すなわち、関数Ｆに、ステップＳ２０５で受信された第２値Ｂ（公開鍵）と、ステップＳ２０１で生成された第１乱数ａ（秘密鍵）とを代入して第３値Ｃ（共通鍵）を生成する。次いでステップＳ２０７で、車両制御装置１０から送信されたチャレンジコードを受信すると、ステップＳ２０８で、コード暗号化部２１４での処理により、第３値Ｃ（共通鍵）でチャレンジコードを暗号化し、レスポンスコードとして車両制御装置１０に送信する。
【００４３】

車両制御装置１０では、ステップＳ１０６で、更新装置２０から送信されたレスポンスコードを受信すると、コード復号部１１４での処理により、ステップＳ１０４で生成された第４値Ｄ（共通鍵）でレスポンスコードを復号する。次いでステップＳ１０７で、認証判定部１１５での処理により、ステップＳ１０６で復号されたコードがステップＳ１０５で生成されたコードと一致するか否かを判定する。ステップＳ１０７で肯定されるとステップＳ１０８に進み、否定されると車両制御装置１０での認証確認処理を終了する。ステップＳ１０８では、更新許可部１１６での処理により、更新装置２０による車両制御プログラムの更新を許可する。

【００４４】

図４は、認証システム１００による処理を説明する図である。図４を参照して本実施形態に係る認証システム１００の主要な動作についてより具体的に説明する。更新装置２０のユーザは、ネットワーク４（図１）の圏外において車両制御プログラムを更新する予定があるものとする。ユーザが事前にネットワーク４の圏内において更新装置２０のキーボード等の入力部を介して認証要求を入力すると、更新装置２０から認証サーバ３０に認証情報、鍵交換用の公開鍵およびユーザにより指定された有効期間が送信される（ステップＳ２００，Ｓ２０１）。認証サーバ３０は、受信した認証情報に基づいて更新装置２０の正当性を認証した場合、受信した公開鍵に有効期間付きで署名して更新装置２０に送信する（ステップＳ３００～Ｓ３０３）。ユーザは、更新装置２０のディスプレイ等の表示部を介して認証が成功したことを確認した後（ステップＳ２０２）、更新装置２０をネットワーク４の圏外へ持ち出すことができる。

【００４５】

ユーザがネットワーク４の圏外において更新装置２０を対象車両の車両制御装置１０に接続すると、更新装置２０から車両制御装置１０に更新装置２０の鍵交換用の公開鍵と有効期間付きの署名が転送される（ステップＳ２０３，Ｓ２０４）。車両制御装置１０は、受信した署名を検証し、署名が有効であれば、車両制御装置１０の鍵交換用の公開鍵とチャレンジコードを更新装置２０に送信する（ステップＳ１００～Ｓ１０３，Ｓ１０５）。更新装置２０は、車両制御装置１０の公開鍵から共通鍵を生成し、生成した共通鍵でチャレンジコードを暗号化してレスポンスコードとして車両制御装置１０に送信する（ステップＳ２０５～Ｓ２０８）。車両制御装置１０は、更新装置２０の公開鍵から共通鍵を生成し、生成した共通鍵でレスポンスコードを復号し、チャレンジコードと一致すれば更新装置２０による車両制御プログラムの更新を許可する（ステップＳ１０４，Ｓ１０６～Ｓ１０８）。同一の車両メーカの複数の車両に搭載された車両制御装置１０など、同一の秘密鍵に対応した公開鍵を保有する複数の車両制御装置１０については、有効期間内に順次、車両制御プログラムの更新を行うことができる（ステップＳ２０３～Ｓ２０８，Ｓ１００～Ｓ１０８）。

【００４６】

これにより、ネットワーク４の圏外で車両制御装置１０側から更新装置２０が認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。また、署名を検証した上で鍵交換を許可し、さらに鍵交換で生成された共通鍵の一致を検証することで、確実に不正アクセスを排除することができる。さらに、署名に有効期間を設定することで、更新装置２０が事前認証後に悪意のある第三者の手に渡って不正な車両制御プログラムに更新される可能性を低減することができる。このような可能性は、更新装置２０がネットワーク４の圏内に入ると有効期間が強制的に終了するように設定することで一層低減することができる。

【００４７】

本実施形態によれば以下のような作用効果を奏することができる。

（１）認証システム１００は、車両に搭載される車両制御装置１０と、車両制御装置１０と通信可能に接続され、車両制御装置１０の制御プログラムを更新する更新装置２０と、更新装置２０と通信可能に接続され、更新装置２０の正当性を認証する認証サーバ３０とを備える（図１、図２）。

【００４８】
更新装置２０は、第１乱数ａ（秘密鍵）を生成する第１乱数生成部２１１と、所定の関数Ｆに、定数Ｇと、第１乱数生成部２１１により生成された第１乱数ａとを代入して第１値Ａ（鍵交換用の公開鍵）を生成し、認証サーバ３０に送信する代入部２１２とを有する。認証サーバ３０は、所定の秘密鍵により、更新装置２０から送信された第１値Ａの署名を生成して更新装置２０に送信する署名生成部３１１を有する。さらに更新装置２０は、代入部２１２により生成された第１値Ａと、認証サーバ３０から送信された署名とを記憶する記憶部２２と、車両制御装置１０に接続されると、記憶部２２に記憶された第１値Ａと署名とを車両制御装置１０に転送する転送部２１３とを有する（図２）。
【００４９】
車両制御装置１０は、秘密鍵に対応する所定の公開鍵により、更新装置２０から送信された署名が有効であるか否かを検証する署名検証部１１０と、第２乱数ｂ（秘密鍵）を生成する第２乱数生成部１１１と、関数Ｆに、定数Ｇと、第２乱数生成部１１１により生成された第２乱数ｂとを代入して第２値Ｂ（鍵交換用の公開鍵）を生成し、更新装置２０に送信する代入部１１２とを有する（図２）。
【００５０】
代入部２１２は、関数Ｆに、車両制御装置１０から送信された第２値Ｂ（公開鍵）と、第１乱数生成部２１１により生成された第１乱数ａ（秘密鍵）とを代入して第３値Ｃ（共通鍵）を生成する。代入部１１２は、署名検証部１１０により署名が有効であると確認されると、関数Ｆに、更新装置２０から送信された第１値Ａ（公開鍵）と、第２乱数生成部１１１により生成された第２乱数ｂ（秘密鍵）とを代入して第４値Ｄ（共通鍵）を生成する。
【００５１】
さらに車両制御装置１０は、代入部２１２により生成された第３値Ｃと、代入部１１２により生成された第４値Ｄとが一致するか否かを判定し、一致すると判定すると、更新装置２０が認証サーバ３０により正当性が認証された更新装置であると判定する認証判定部１１５と、更新装置２０による制御プログラムの更新を許可する更新許可部１１６とを有する（図２）。
【００５２】
これにより、ネットワーク４の圏外で車両制御装置１０側から更新装置２０が認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。また、署名を検証した上で鍵交換を許可し、さらに鍵交換で生成された共通鍵の一致を検証することで、確実に不正アクセスを排除することができる。
【００５３】
（２）車両制御装置１０は、更新装置２０が接続されると、コードを生成して更新装置２０に送信するコード生成部１１３をさらに有する。更新装置２０は、代入部２１２により生成された第３値Ｃ（共通鍵）により、車両制御装置１０から送信されたコードを暗号化し、暗号化されたコードを車両制御装置１０に送信するコード暗号化部２１４をさらに有する。さらに車両制御装置１０は、代入部１１２により生成された第４値Ｄ（共通鍵）により、更新装置２０から送信された暗号化されたコードを復号するコード復号部１１４を有する（図２）。認証判定部１１５は、コード生成部１１３により生成されたコードと、コード復号部１１４により復号されたコードとが一致するか否かを判定し、一致すると判定すると、代入部２１２により生成された第３値Ｃと、代入部１１２により生成された第４値Ｄとが一致すると判定する。
【００５４】
このような構成により、鍵交換により生成された車両制御装置１０側の共通鍵と更新装置２０側の共通鍵とが一致するか否かを検証し、更新装置２０が認証サーバ３０により正当性を認証されたものであることを確認することができる。
【００５５】
（３）署名は所定期間有効である。署名に有効期間を設定することで、有効期間内に複数の車両制御装置１０の車両制御プログラムを更新することができる。また、更新装置２０

が事前認証後に悪意のある第三者の手に渡って不正な車両制御プログラムに更新される可能性を低減することができる。

【００５６】

（４）署名生成部３１１は、所定期間を設定する。例えば、更新装置２０を介して認証サーバ３０に送信されたユーザによる指定に応じて認証サーバ３０側で生成される署名に所定期間を設定する。この場合、例えば、更新装置２０のユーザが車両制御プログラムを更新する予定の日時に合わせて必要に応じて有効期間を指定できるため、更新装置２０が事前認証後に悪意のある第三者の手に渡って不正な車両制御プログラムに更新される可能性を一層低減することができる。

【００５７】

（５）署名は、所定期間内であっても、更新装置２０と認証サーバ３０とが非接続状態から接続状態になると無効になる。更新装置２０がネットワーク４圏内に入ると有効期間が強制的に終了するように設定することで、更新装置２０が事前認証後に悪意のある第三者の手に渡って不正な車両制御プログラムに更新される可能性をより一層低減することができる。

【００５８】

［第１の変形例］

上記の実施形態は、以下のように変形することができる。図５～図７は、それぞれ図２～図４に対応する第１の変形例である。なお、図５～図７において図２～図４と同一の箇所には同一の符号を付している。上記実施形態に係る認証システム１００と第１の変形例に係る認証システム１００Ａとは、鍵交換により生成された車両制御装置１０Ａ側の共通鍵と更新装置２０Ａ側の共通鍵とが一致するか否かを検証するための構成が異なる。すなわち、図５に示すように、認証システム１００Ａを構成する車両制御装置１０Ａは、コード復号部１１４（図２）に代えて、コード暗号化部１１７を有する。

【００５９】

図６に示すように、車両制御装置１０Ａのコード暗号化部１１７は、ステップＳ１０９において、ステップＳ１０５で生成されたコードをステップＳ１０４で生成された第４値Ｄ（共通鍵）で暗号化する。また、認証判定部１１５は、ステップＳ１０７において、ステップＳ１１０で更新装置２０Ａから受信したレスポンスコードがステップＳ１０９で暗号化されたコードと一致するか否かを判定する。

【００６０】

すなわち、図７に示すように、車両制御装置１０Ａ側で暗号化されたコードは、鍵交換により生成された同一の共通鍵により暗号化されていれば、更新装置２０Ａ側で暗号化されたコードと一致する。この場合、車両制御装置１０Ａ側の共通鍵（第４値Ｄ）で暗号化されたコードは、更新装置２０Ａ側の共通鍵（第３値Ｃ）で暗号化されたコード、すなわちレスポンスコードと一致する。認証システム１００Ａでは、これらのコードが一致するか否かを判定することで、更新装置２０Ａが認証サーバ３０により正当性を認証されたものであるか否かを判定する。これにより、第１の変形例に係る認証システム１００Ａにおいても、ネットワーク４の圏外で車両制御装置１０Ａ側から更新装置２０Ａが認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。また、署名を検証した上で鍵交換を許可し、さらに鍵交換で生成された共通鍵の一致を検証することで、確実に不正アクセスを排除することができる。

【００６１】

第１の変形例に係る認証システム１００Ａでは、更新装置２０Ａは、代入部２１２により生成された第３値Ｃにより、車両制御装置１０Ａから送信されたコードを暗号化し、暗号化されたコードを車両制御装置１０Ａに送信するコード暗号化部２１４を有する。車両制御装置１０Ａは、代入部１１２により生成された第４値Ｄにより、コード生成部１１３により生成されたコードを暗号化するコード暗号化部１１７を有する（図５）。認証判定部１１５は、更新装置２０Ａから送信された暗号化されたコードと、コード暗号化部１１７により暗号化されたコードとが一致するか否かを判定し、一致すると判定すると、代入部

２１２により生成された第３値Ｃと、代入部１１２により生成された第４値Ｄとが一致すると判定する。

【００６２】

このような構成により、第１の変形例に係る認証システム１００Ａにおいても、鍵交換により生成された車両制御装置１０Ａ側の共通鍵と更新装置２０Ａ側の共通鍵とが一致するか否かを検証し、更新装置２０Ａが認証サーバ３０により正当性を認証されたものであることを確認することができる。

【００６３】

［第２の変形例］

図８～図１０は、それぞれ図２～図４に対応する第２の変形例である。なお、図８～図１０において図２～図４と同一の箇所には同一の符号を付している。上記実施形態に係る認証システム１００と第２の変形例に係る認証システム１００Ｂとは、鍵交換により生成された車両制御装置１０Ｂ側の共通鍵と更新装置２０Ｂ側の共通鍵とが一致するか否かを検証するための構成が異なる。すなわち、図８に示すように、認証システム１００Ｂを構成する更新装置２０Ｂは、コード暗号化部２１４（図２）に代えて、ＭＡＣ生成部２１５を有し、車両制御装置１０Ｂは、コード復号部１１４（図２）に代えて、ＭＡＣ生成部１１８を有する。

【００６４】

図９に示すように、更新装置２０ＢのＭＡＣ生成部２１５は、ステップＳ２０９において、ステップＳ２０６で生成された第３値Ｃ（共通鍵）により、ステップＳ２０７で車両制御装置１０Ｂから受信したチャレンジコードのメッセージ認証コードであるＭＡＣ値を生成し、レスポンスコードとして車両制御装置１０Ｂに送信する。車両制御装置１０ＢのＭＡＣ生成部１１８は、ステップＳ１１１において、ステップＳ１０４で生成された第４値Ｄ（共通鍵）により、ステップＳ１０５で生成されたコードのＭＡＣ値を生成する。認証判定部１１５は、ステップＳ１１３において、ステップＳ１１２で更新装置２０Ｂから受信したレスポンスコードがステップＳ１１１で生成されたＭＡＣ値と一致するか否かを判定する。

【００６５】

すなわち、図１０に示すように、車両制御装置１０Ｂ側で生成されたＭＡＣ値は、鍵交換により生成された同一の共通鍵により生成されていれば、更新装置２０Ｂ側で生成されたＭＡＣ値と一致する。この場合、車両制御装置１０Ｂ側の共通鍵（第４値Ｄ）により生成されたＭＡＣ値は、更新装置２０Ｂ側の共通鍵（第３値Ｃ）により生成されたＭＡＣ値、すなわちレスポンスコードと一致する。認証システム１００Ｂでは、これらのＭＡＣ値が一致するか否かを判定することで、更新装置２０Ｂが認証サーバ３０により正当性を認証されたものであるか否かを判定する。これにより、第２の変形例に係る認証システム１００Ｂにおいても、ネットワーク４の圏外で車両制御装置１０Ｂ側から更新装置２０Ｂが認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。また、署名を検証した上で鍵交換を許可し、さらに鍵交換で生成された共通鍵の一致を検証することで、確実に不正アクセスを排除することができる。

【００６６】

第２の変形例に係る認証システム１００Ｂでは、更新装置２０Ｂは、代入部２１２により生成された第３値Ｃにより、車両制御装置１０Ｂから送信されたコードのＭＡＣ値を生成して車両制御装置１０Ｂに送信するＭＡＣ生成部２１５を有する。車両制御装置１０Ｂは、代入部１１２により生成された第４値Ｄにより、コード生成部１１３により生成されたコードのＭＡＣ値を生成するＭＡＣ生成部１１８を有する（図８）。認証判定部１１５は、更新装置２０Ｂから送信されたＭＡＣ値と、ＭＡＣ生成部１１８により生成されたＭＡＣ値とが一致するか否かを判定し、一致すると判定すると、代入部２１２により生成された第３値Ｃと、代入部１１２により生成された第４値Ｄとが一致すると判定する。

【００６７】

このような構成により、第２の変形例に係る認証システム１００Ｂにおいても、鍵交換に

より生成された車両制御装置１０Ｂ側の共通鍵と更新装置２０Ｂ側の共通鍵とが一致するか否かを検証し、更新装置２０Ｂが認証サーバ３０により正当性を認証されたものであることを確認することができる。

【００６８】

［第３の変形例］

図１１～図１３は、それぞれ図２～図４に対応する第３の変形例である。なお、図１１～図１３において図２～図４と同一の箇所には同一の符号を付している。上記実施形態に係る認証システム１００と第３の変形例に係る認証システム１００Ｃとは、鍵交換により生成された車両制御装置１０Ｃ側の共通鍵と更新装置２０Ｃ側の共通鍵とが一致するか否かを検証するための構成が異なる。すなわち、図１１に示すように、認証システム１００Ｃを構成する更新装置２０Ｃは、コード暗号化部２１４（図２）に代えて、コード復号部２１６を有し、車両制御装置１０Ｃは、コード復号部１１４（図２）に代えて、コード暗号化部１１７を有する。

【００６９】

図１２に示すように、車両制御装置１０Ｃのコード生成部１１３およびコード暗号化部１１７は、ステップＳ１１４において、乱数からなるコードを生成してステップＳ１０４で生成された第４値Ｄ（共通鍵）で暗号化し、チャレンジコードとして更新装置２０Ｃに送信する。更新装置２０Ｃのコード復号部２１６は、ステップＳ２１１において、ステップＳ２０６で生成された第３値Ｃ（共通鍵）により、ステップＳ２１０で車両制御装置１０Ｃから受信したチャレンジコードを復号し、レスポンスコードとして車両制御装置１０Ｃに送信する。車両制御装置１０Ｃの認証判定部１１５は、ステップＳ１０７において、ステップＳ１１５で更新装置２０Ｃから受信したレスポンスコードがステップＳ１１４で生成されたコードと一致するか否かを判定する。

【００７０】

すなわち、図１３に示すように、車両制御装置１０Ｃ側で生成されたコードは、鍵交換により生成された同一の共通鍵により暗号化および復号されていれば、更新装置２０Ｃ側で復号されたコードと一致する。この場合、車両制御装置１０Ｃ側で生成されたコードは、車両制御装置１０Ｃ側の共通鍵（第４値Ｄ）で暗号化され、更新装置２０Ｃ側の共通鍵（第３値Ｃ）で復号されたコード、すなわちレスポンスコードと一致する。認証システム１００Ｃでは、これらのコードが一致するか否かを判定することで、更新装置２０Ｃが認証サーバ３０により正当性を認証されたものであるか否かを判定する。これにより、第３の変形例に係る認証システム１００Ｃにおいても、ネットワーク４の圏外で車両制御装置１０Ｃ側から更新装置２０Ｃが認証サーバ３０により正当性を認証されたものであるか否かを確認することができる。また、署名を検証した上で鍵交換を許可し、さらに鍵交換で生成された共通鍵の一致を検証することで、確実に不正アクセスを排除することができる。

【００７１】

第３の変形例に係る認証システム１００Ｃでは、車両制御装置１０Ｃは、更新装置２０Ｃが接続されると、コードを生成するコード生成部１１３と、代入部１１２により生成された第４値Ｄにより、コード生成部１１３により生成されたコードを暗号化し、暗号化されたコードを更新装置２０Ｃに送信するコード暗号化部１１７とを有する。更新装置２０Ｃは、代入部２１２により生成された第３値Ｃにより、車両制御装置１０Ｃから送信された暗号化されたコードを復号し、復号されたコードを車両制御装置１０Ｃに送信するコード復号部２１６を有する（図１１）。認証判定部１１５は、コード生成部１１３により生成されたコードと、更新装置２０Ｃから送信された復号されたコードとが一致するか否かを判定し、一致すると判定すると、代入部２１２により生成された第３値Ｃと、代入部１１２により生成された第４値Ｄとが一致すると判定する。

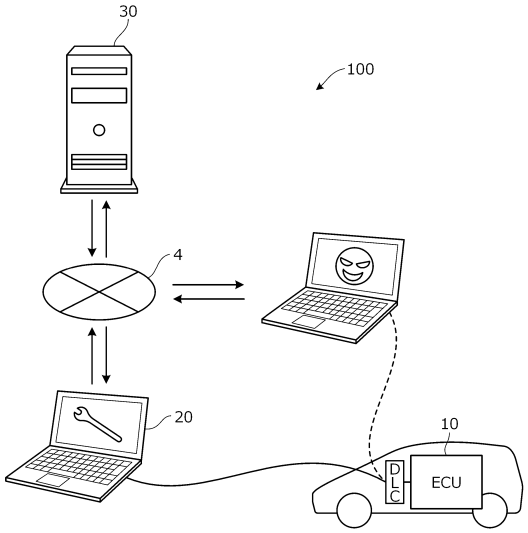
【００７２】

このような構成により、第３の変形例に係る認証システム１００Ｃにおいても、鍵交換により生成された車両制御装置１０Ｃ側の共通鍵と更新装置２０Ｃ側の共通鍵とが一致するか否かを検証し、更新装置２０Ｃが認証サーバ３０により正当性を認証されたものである

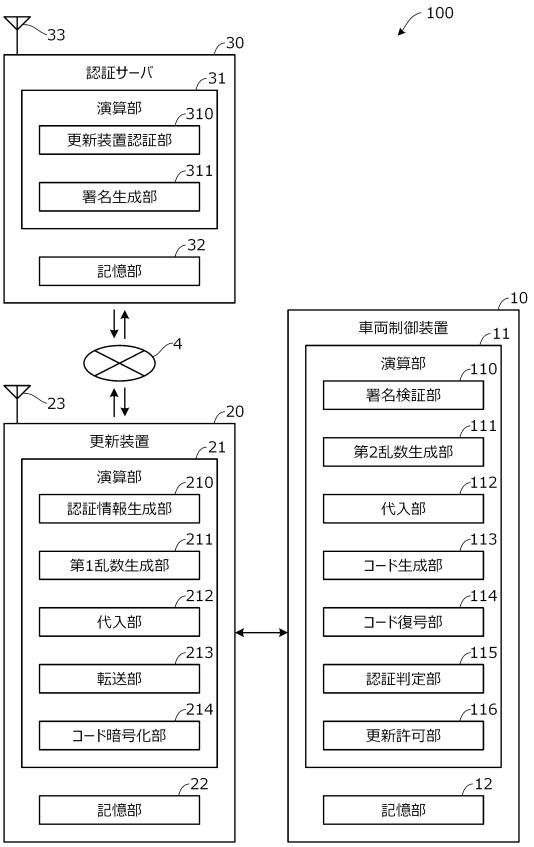
ことを確認することができる。
【００７３】
［他の変形例］
上記実施形態では、車両制御装置１０と更新装置２０とが車両のＤＬＣを介してＣＡＮ通信等により有線接続されるとしたが、車両制御装置と通信可能に接続され、車両制御装置の制御プログラムを更新する更新装置の構成はこのようなものに限らない。例えば、車両制御装置１０とＷｉ－Ｆｉ（Wireless Fidelity）（登録商標）、Bluetooth（登録商標）等の近接無線通信により通信可能に構成してもよい。
【００７４】
上記実施形態では、署名生成部３１１が有効期間を設定するようにしたが、署名を生成する署名生成部はこのようなものに限らない。署名の有効期間を設定しなくてもよい。また、署名の有効期間に加えてＧＰＳセンサにより取得可能な位置による有効範囲を設定してもよい。この場合、例えば、更新装置２０のユーザが車両制御プログラムを更新する予定のエリアに合わせて必要に応じて有効範囲を指定することができる。
【００７５】
以上の説明はあくまで一例であり、本発明の特徴を損なわない限り、上述した実施形態および変形例により本発明が限定されるものではない。上記実施形態と変形例の１つまたは複数を任意に組み合わせることも可能であり、変形例同士を組み合わせることも可能である。
【符号の説明】
【００７６】
４　ネットワーク、１０　車両制御装置、２０　更新装置、３０　認証サーバ、１１，２１，３１　演算部、１２，２２，３２　記憶部、２３，３３　通信部、１００　認証システム、１１０　署名検証部、１１１　第２乱数生成部、１１２，２１２　代入部、１１３　コード生成部、１１４，２１６　コード復号部、１１５　認証判定部、１１６　更新許可部、１１７，２１４　コード暗号化部、１１８，２１５　ＭＡＣ生成部、２１０　認証情報生成部、２１１　第１乱数生成部、２１３　転送部、３１０　更新装置認証部、３１１　署名生成部

【図面】

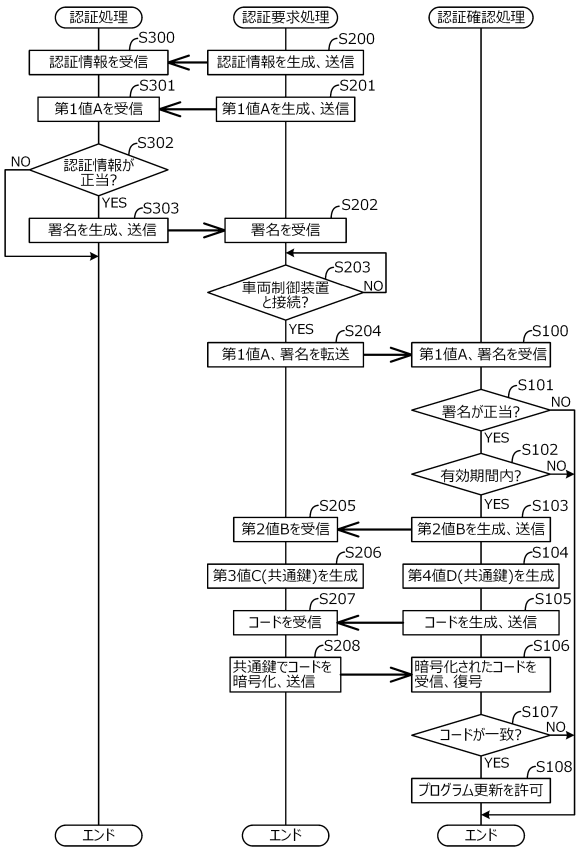
【図１】


30
100
4
20
10
DLC
ECU

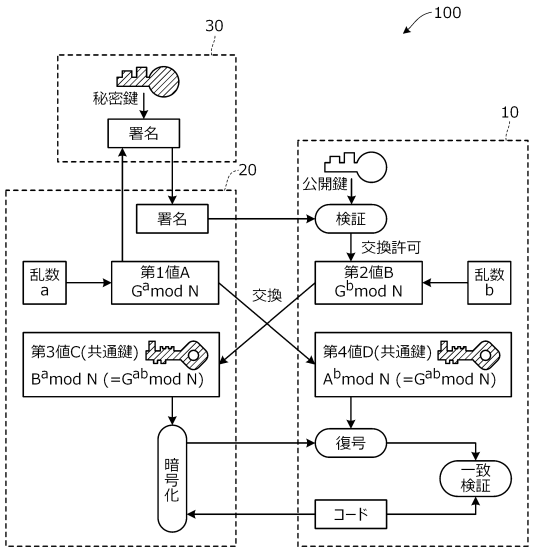
【図２】


100
33
30
認証サーバ
31
演算部
310
更新装置認証部
311
署名生成部
32
記憶部
10
車両制御装置
11
演算部
110
署名検証部
111
第2乱数生成部
112
代入部
113
コード生成部
114
コード復号部
115
認証判定部
116
更新許可部
12
記憶部
4
23
20
更新装置
21
演算部
210
認証情報生成部
211
第1乱数生成部
212
代入部
213
転送部
214
コード暗号化部
22
記憶部

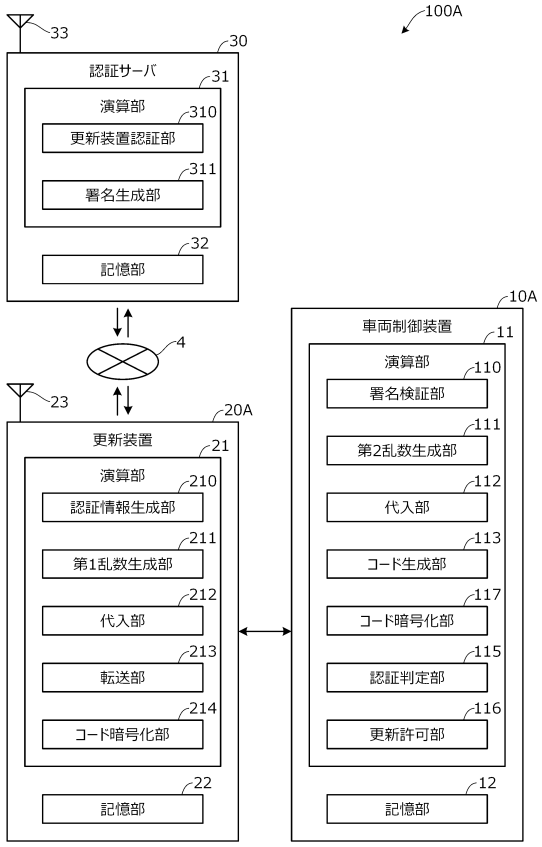
【図３】


認証処理
認証要求処理
認証確認処理
S300
認証情報を受信
S200
認証情報を生成、送信
S301
第1値Aを受信
S201
第1値Aを生成、送信
S302
認証情報が正当?
NO
YES
S303
署名を生成、送信
S202
署名を受信
S203
車両制御装置と接続?
NO
YES
S204
第1値A、署名を転送
S100
第1値A、署名を受信
S101
署名が正当?
NO
YES
S102
有効期間内?
NO
YES
S205
第2値Bを受信
S103
第2値Bを生成、送信
S206
第3値C(共通鍵)を生成
S104
第4値D(共通鍵)を生成
S207
コードを受信
S105
コードを生成、送信
S208
共通鍵でコードを暗号化、送信
S106
暗号化されたコードを受信、復号
S107
コードが一致?
NO
YES
S108
プログラム更新を許可
エンド
エンド
エンド

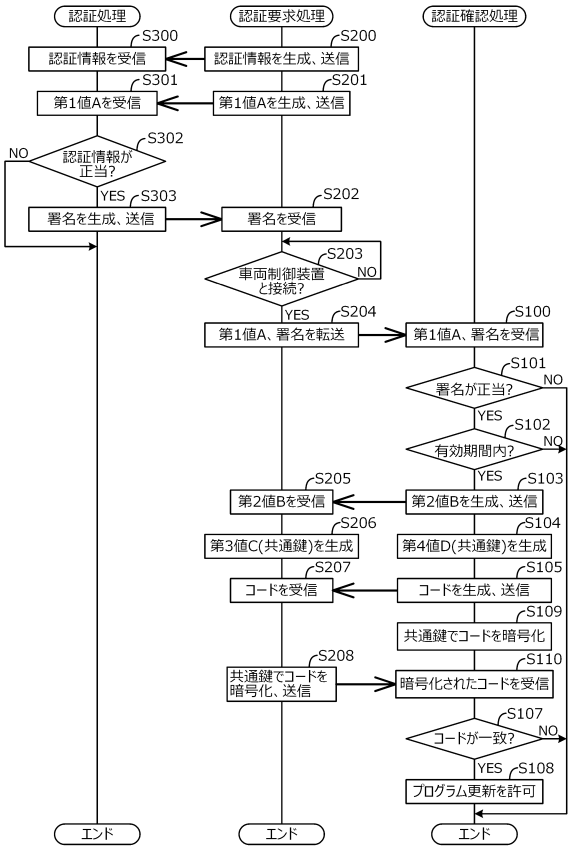
【図４】


100
30
秘密鍵
署名
10
20
公開鍵
署名
検証
交換許可
乱数 a
第1値A Gamod N
交換
第2値B Gbmod N
乱数 b
第3値C(共通鍵) Bamod N (=Gabmod N)
第4値D(共通鍵) Abmod N (=Gabmod N)
暗号化
復号
一致検証
コード

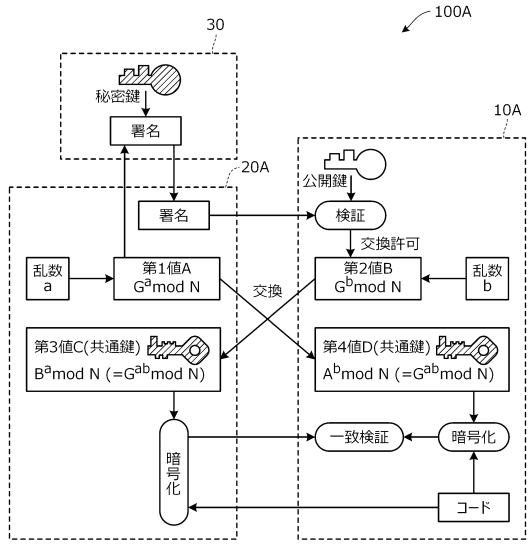
【図５】


100A
33
30
認証サーバ
31
演算部
310
更新装置認証部
311
署名生成部
32
記憶部
4
23
20A
更新装置
21
演算部
210
認証情報生成部
211
第1乱数生成部
212
代入部
213
転送部
214
コード暗号化部
22
記憶部
10A
車両制御装置
11
演算部
110
署名検証部
111
第2乱数生成部
112
代入部
113
コード生成部
117
コード暗号化部
115
認証判定部
116
更新許可部
12
記憶部

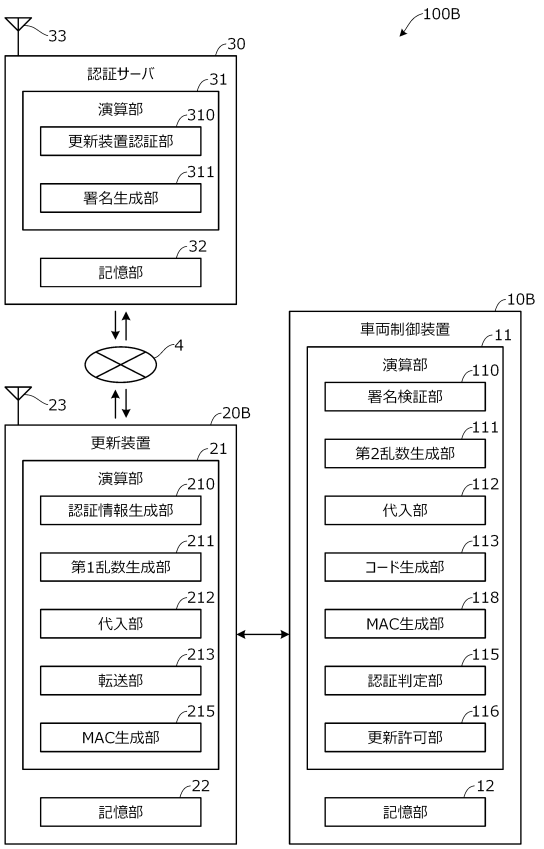
【図６】


認証処理
認証要求処理
認証確認処理
S300
認証情報を受信
S200
認証情報を生成、送信
S301
第1値Aを受信
S201
第1値Aを生成、送信
S302
認証情報が正当?
NO
YES
S303
署名を生成、送信
S202
署名を受信
S203
車両制御装置と接続?
NO
YES
S204
第1値A、署名を転送
S100
第1値A、署名を受信
S101
署名が正当?
NO
YES
S102
有効期間内?
NO
YES
S205
第2値Bを受信
S103
第2値Bを生成、送信
S206
第3値C(共通鍵)を生成
S104
第4値D(共通鍵)を生成
S207
コードを受信
S105
コードを生成、送信
S109
共通鍵でコードを暗号化
S208
共通鍵でコードを暗号化、送信
S110
暗号化されたコードを受信
S107
コードが一致?
NO
YES
S108
プログラム更新を許可
エンド
エンド
エンド

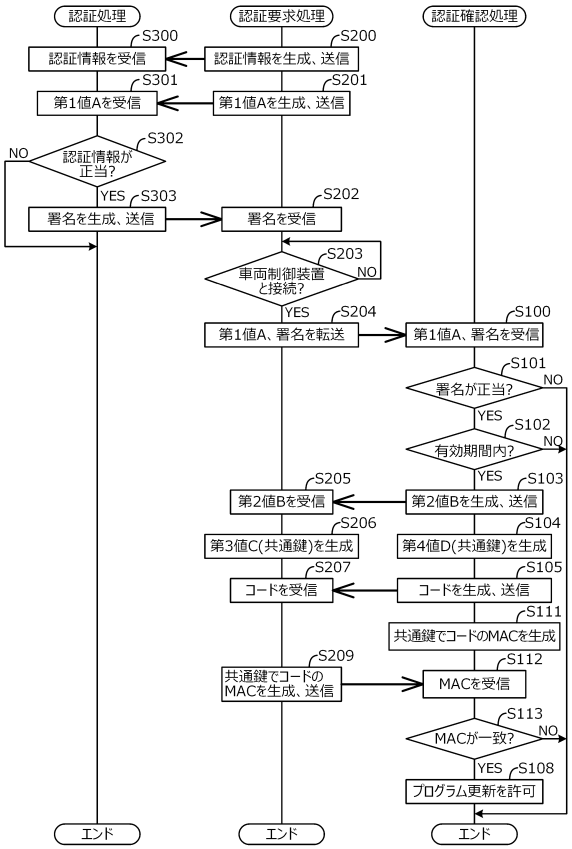
【図７】


100A
30
秘密鍵
署名
10A
20A
公開鍵
署名
検証
交換許可
乱数 a
第1値A Gamod N
交換
第2値B Gbmod N
乱数 b
第3値C(共通鍵) Bamod N (=Gabmod N)
第4値D(共通鍵) Abmod N (=Gabmod N)
暗号化
一致検証
暗号化
コード

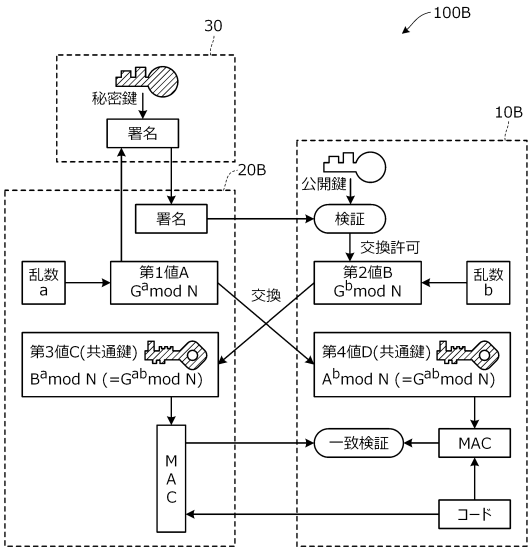
【図８】


100B
33
30
認証サーバ
31
演算部
310
更新装置認証部
311
署名生成部
32
記憶部
4
23
20B
更新装置
21
演算部
210
認証情報生成部
211
第1乱数生成部
212
代入部
213
転送部
215
MAC生成部
22
記憶部
10B
車両制御装置
11
演算部
110
署名検証部
111
第2乱数生成部
112
代入部
113
コード生成部
118
MAC生成部
115
認証判定部
116
更新許可部
12
記憶部

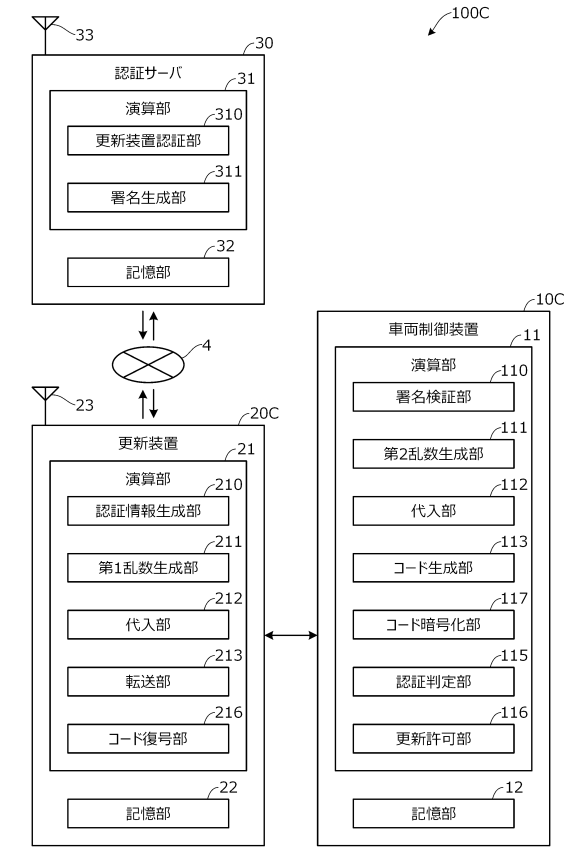
【図９】



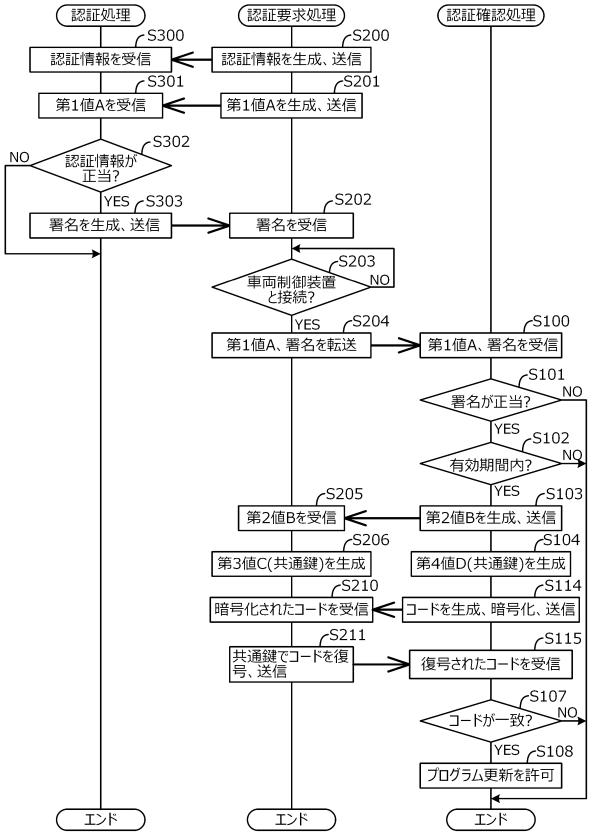
【図１０】



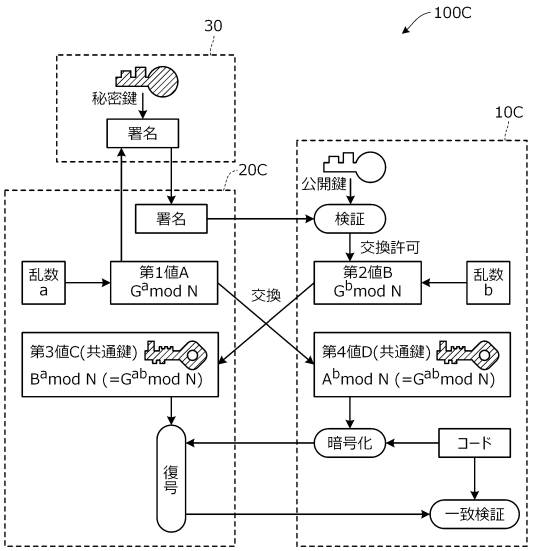
【図１１】



【図１２】



【図１３】


100C
30
秘密鍵
署名
10C
20C
公開鍵
署名
検証
交換許可
乱数
a
第1値A
Gamod N
交換
第2値B
Gbmod N
乱数
b
第3値C(共通鍵)
Bamod N (=Gabmod N)
第4値D(共通鍵)
Abmod N (=Gabmod N)
暗号化
コード
復号
一致検証

フロントページの続き

(51)国際特許分類　　ＦＩ
　　Ｂ６０Ｒ　16/02　６６０Ｕ

会社本田技術研究所内
審査官　行田 悦資

(56)参考文献　国際公開第２０１６／１５１９８７（WO，Ａ１）
特開２０１８－０４２２５６（ＪＰ，Ａ）
特開２０１２－１０４０４９（ＪＰ，Ａ）
特開２０１６－１８４８９２（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８
Ｇ０９Ｃ　１／００
Ｇ０６Ｆ　２１／４４
Ｂ６０Ｒ　１６／０２