(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年8月22日(22.08.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/159593 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2019/001320

(22) 国際出願日： 2019年1月17日(17.01.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2018-023447 2018年2月13日(13.02.2018) JP

(71) 出願人: 株式会社デンソー (**DENSO CORPORATION**) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP).

(72) 発明者: 米谷 昭(**KOMEDANI Akira**); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP).

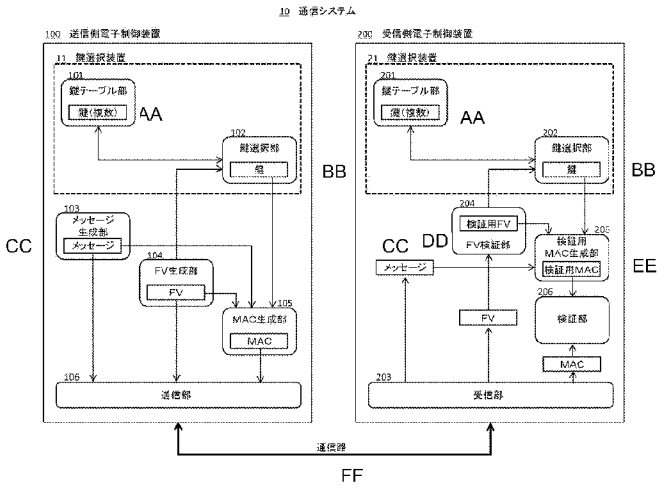
(74) 代理人: 藤江 和典, 外(**FUJIE Kazunori** et al.); 〒1690075 東京都新宿区高田馬場１－２９－２０ 安念ビル５階 桜こみち国際特許事務所 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** ELECTRONIC CONTROL DEVICE AND COMMUNICATION SYSTEM

(54) 発明の名称： 電子制御装置及び通信システム

[図1]



10 Communication system
11, 21 Key selection device
100 Transmission-side electronic control device
101, 201 Key table unit
102, 202 Key selection unit
103 Message generation unit
104 FV generation unit
105 MAC generation unit
106 Transmission unit
200 Reception-side electronic control device
203 Reception unit
204 FV verification unit
205 Verification MAC generation unit
206 Verification unit
AA Keys
BB Key
CC Message
DD Verification FV
EE Verification MAC
FF Communication path

(57) **Abstract:** This electronic control device is a transmission-side electronic control device (100) in a communication system (10) constituted of the transmission-side electronic control device (100), which transmits a message, and a reception-side electronic control device (200) that receives the message. The transmission-side electronic control device (100) is provided with: a key table unit (101) that has a plurality of keys; a key selection unit (102) that selects one key from the key table unit on the basis of synchronization information, which is information synchronized in communication between the transmission-side electronic control device and the reception-side electronic control device; a message generation unit (103) that generates the message; a MAC generation unit (105) that generates a message authentication code (MAC) by using the key selected by the key selection unit and the message; and a transmission unit (106) that assigns the message authentication code to the message and transmits the message.

WO 2019/159593 A1

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

(57) 要約:電子制御装置は、メッセージを送信する送信側電子制御装置(１００)及び前記メッセージを受信する受信側電子制御装置(２００)で構成される通信システム(１０)の前記送信側電子制御装置(１００)であって、複数の鍵を有する鍵テーブル部(１０１)と、当該送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部(１０２)と、前記メッセージを生成するメッセージ生成部(１０３)と、前記鍵選択部で選択された鍵及び前記メッセージを用いてメッセージ認証コード(ＭＡＣ)を生成するＭＡＣ生成部(１０５)と、前記メッセージに前記メッセージ認証コードを付与して送信する送信部(１０６)と、を備える。

明　細　書

発明の名称 ： 電子制御装置及び通信システム

関連出願の相互参照

[0001] 本出願は、２０１８年２月１３日に出願された日本特許出願番号２０１８－０２３４４７号に基づくもので、ここにその記載内容を援用する。

技術分野

[0002] 本出願は、電子制御装置（ＥＣＵ：Electric Control Unit）のセキュリティを確保するための暗号鍵の選択及び切替に関するものであり、主として車載の電子制御装置に用いるものである。

背景技術

[0003] 近年、自動車は駆動、制動に限らず、車内環境全般、あるいは通信などにも電子制御装置を用いた制御が用いられるようになってきている。また、運転そのものについても、運転者に対する運転サポートを行う安全運転支援システム、さらには運転者そのものが不要な自動運転システムの開発が活発になっている。これらの流れの中で、電子制御装置が接続された車内ネットワークのハッキングが大きな問題となる。一旦車内ネットワークがハッキングされると、自動車運転の安全性そのものが脅かされることとなり、通常のコンピュータのハッキングと異なり、直接人の生命や身体に危険が生じる可能性が極めて高い。そこで、車載向け電子制御装置のセキュリティに関する様々な技術が提案されている。

[0004] 電子制御装置間の通信では、メッセージの正真性（Integrity）、すなわち改ざんやなりすましをチェックするため、メッセージ認証コード（ＭＡＣ：Message Authentication Code）が用いられている。メッセージ認証コードの生成及びそのチェックを行うために、送信側電子制御装置及び受信側電子制御装置は、共通の鍵である共有鍵を用いている。そして、共有鍵を複数持ちこれを定期的に切り替えることによりメッセージの正真性が高まることから、複数の鍵を送信側と受信側で切り替える方法が提案されている。

先行技術文献

特許文献

[0005] 特許文献1：ＷＯ２０１５－１７０４５２号

特許文献2：特開２０１０－４４２０号

発明の概要

[0006] 特許文献１には、車両の状態が所定状態であることを条件として、更新フレームを送信することにより鍵を更新することが記載されている。また、特許文献２には、鍵管理サーバから複数の端末に対し、デバイス鍵更新命令を送信することにより一括して鍵を更新することが記載されている。

[0007] ここで、いずれの特許文献に記載の技術も、装置間の鍵を更新する際に専用の同期信号を送信している。しかし、ネットワークの輻輳が増加している場合や、送信側電子制御装置と受信側電子制御装置とが異なるバスドメインに存在する場合には、鍵の切り換え及びメッセージの送受信が順次行われず、受信側電子制御装置の鍵が切り替わる前に切り替え後の鍵を用いて認証されたメッセージが送信側電子制御装置から送られていることもある。あるいは、専用の同期信号を受信できずに鍵の切り換えに失敗する場合もある。このような場合、送信側の鍵と受信側の鍵とが異なるために、受信側電子制御装置では受信したメッセージの認証をＮＧと判定し破棄してしまう。

[0008] 発明者の詳細な検討の結果、特にＣＡＮ（Controller Area Network）等の車載ネットワークにおいては、車両を制御する制御情報が短周期で定期送信されていることから、安定的に車両を制御するためにも確実に鍵の切り換えを行う必要性が高いという課題を見出だした。

本開示の目的は、専用の同期信号を用いることなく送信側電子制御装置及び受信側電子制御装置の鍵を切り替えることで、専用の同期信号を用いた場合に起こりうる送受信間の鍵の切り換えタイミングのずれや鍵の切り換えの失敗を原因とした通信の不成立を低減することにある。

[0009] 本開示の一態様による電子制御装置は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通

信システムの前記送信側電子制御装置であって、複数の鍵を有する鍵テーブル部と、当該送信側電子制御装置と前記受信側電子制御装置との間で同期された情報である同期情報に基づき、前記鍵テーブルから一つの鍵を選択する鍵選択部と、前記メッセージを生成するメッセージ生成部と、前記鍵選択部で選択された鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成するＭＡＣ生成部と、前記メッセージに前記メッセージ認証コードを付与して送信する送信部と、を有する。

[0010] 本開示の他の態様による電子制御装置は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムの前記受信側電子制御装置であって、前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信する受信部と、複数の鍵を有する鍵テーブル部と、当該受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部と、前記鍵選択部で選択された鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成する検証用ＭＡＣ生成部と、前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する検証部と、を有する。

[0011] 本開示の他の態様による通信システムは、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムであって、前記送信側電子制御装置及び前記受信側電子制御装置はそれぞれ、複数の鍵を有する鍵テーブル部と、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部と、を有し、前記送信側電子制御装置は、前記メッセージを生成するメッセージ生成部と、前記鍵選択部で選択された鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成するＭＡＣ生成部と、前記メッセージに前記メッセージ認証コードを付与して送信する送信部と、を有し、前記受信側電子制御

装置は、前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信する受信部と、前記鍵選択部で選択された鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成する検証用ＭＡＣ生成部と、前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する検証部と、を有する。

[0012] 本開示の他の態様による鍵選択装置は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムで用いられる鍵選択装置であって、複数の鍵を有する鍵テーブル部と、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部と、前記鍵選択部で選択された前記一つの鍵を出力する出力部と、を有する。

[0013] 本開示の他の態様によるメッセージ送信方法は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムの前記送信側電子制御装置で実行されるメッセージ送信方法あって、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、前記メッセージを生成し、選択された前記一つの鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成し、前記メッセージに前記メッセージ認証コードを付与して送信する。

[0014] 本開示の他の態様によるメッセージ受信方法は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムの前記受信側電子制御装置で実行されるメッセージ受信方法であって、前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信し、前記受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの

鍵を選択し、選択された前記一つの鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成し、前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する。

[0015] 本開示の他の態様による鍵選択方法は、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムで用いられる鍵選択方法であって、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する前記鍵テーブル部から一つの鍵を選択し、選択された前記一つの鍵を出力する。

[0016] 本開示の他の態様によるコンピュータにて実行可能なメッセージ送信プログラムは、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムの前記送信側電子制御装置で実行されるメッセージ送信プログラムであって、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、前記メッセージを生成し、選択された前記一つの鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成し、前記メッセージに前記メッセージ認証コードを付与して送信すること、を有する。

[0017] 本開示の他の態様によるコンピュータにて実行可能なメッセージ受信プログラムは、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムの前記受信側電子制御装置で実行されるメッセージ受信プログラムであって、前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信し、前記受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、選択された前記一つの鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成し、前記メッセージ認証コードと前記検証用メッセージ認証コードの同

一性を検証すること、を有する。

[0018] 本開示の他の態様によるコンピュータにて実行可能な鍵選択プログラムは、メッセージを送信する送信側電子制御装置及び前記メッセージを受信する受信側電子制御装置で構成される通信システムで用いられる鍵選択プログラムであって、前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する前記鍵テーブル部から一つの鍵を選択し、選択された前記一つの鍵を出力すること、を有する。

[0019] 本開示の他の態様による電子制御装置は、暗号化メッセージを送信する送信側電子制御装置及び前記暗号化メッセージを受信する受信側電子制御装置で構成される通信システムの前記送信側電子制御装置であって、複数の鍵を有する鍵テーブル部と、当該送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部と、メッセージを生成するメッセージ生成部と、前記鍵選択部で選択された鍵及び前記メッセージを用いて前記暗号化メッセージを生成する暗号化部と、前記暗号化メッセージを送信する送信部と、を有する。

[0020] 本開示の他の態様による電子制御装置は、暗号化メッセージを送信する送信側電子制御装置及び前記暗号化メッセージを受信する受信側電子制御装置で構成される通信システムの前記受信側電子制御装置であって、前記暗号化メッセージを受信する受信部と、複数の鍵を有する鍵テーブル部と、当該受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部と、前記鍵選択部で選択された鍵を用いて前記暗号化メッセージを復号する復号部と、を有する。

[0021] 本開示の電子制御装置、通信システム、鍵選択装置、メッセージ送信方法、メッセージ受信方法、鍵選択方法、メッセージ送信プログラム、メッセージ受信プログラム、鍵選択プログラム（以下、まとめて電子制御装置等とす

る）によれば、専用の同期信号を用いた場合に起こりうる送受信間の鍵の切り換えタイミングのずれや鍵の切り換えの失敗を原因とした通信の不成立を低減することができる。

図面の簡単な説明

[0022] [図1]図１は、実施形態１の通信システム及び電子制御装置の構成を説明するブロック図であり、

[図2]図２は、実施形態１の通信システム及び電子制御装置の動作（メッセージ送信方法、メッセージ受信方法、メッセージ送信プログラム、メッセージ受信プログラム）を説明するフローチャートであり、

[図3]図３は、実施形態１の鍵選択装置の態様を説明するブロック図であり、

[図4]図４は、実施形態１の鍵選択部における鍵選択方法を説明する説明図であり、

[図5]図５は、実施形態２の通信システム及び電子制御装置の構成を説明するブロック図であり、

[図6]図６は、実施形態２の通信システム及び電子制御装置の動作（メッセージ送信方法、メッセージ受信方法、メッセージ送信プログラム、メッセージ受信プログラム）を説明するフローチャートであり、

[図7]図７は、実施形態３の通信システム及び電子制御装置の構成を説明するブロック図である。

発明を実施するための形態

[0023] 以下、本開示の実施形態について、図面を参照して説明する。

なお、本開示とは、以下の実施形態に限定されるものではない。また、少なくともダブルクォーテーション内の語句は、請求の範囲に記載された語句を意味し、同じく以下の実施形態に限定されるものではない。

請求の範囲の従属項に記載の構成及び方法、従属項に記載の構成及び方法に対応する実施形態の構成及び方法、並びに請求の範囲に記載がなく実施形態のみに記載の構成及び方法は、本発明においては任意の構成及び方法である。請求の範囲の記載が実施形態の記載よりも広い場合における実施形態に

記載の構成及び方法も、本発明の構成及び方法の例示であるという意味で、本発明においては任意の構成及び方法である。いずれの場合も、特許請求の範囲の独立項に記載することで、本発明の必須の構成及び方法となる。

実施形態に記載した効果は、本開示の例示としての実施形態の構成を有する場合の効果であり、必ずしも本開示が有する効果ではない。

複数の実施形態がある場合、各実施形態に開示の構成は各実施形態のみで閉じるものではなく、実施形態をまたいで組み合わせることが可能である。例えば一の実施形態に開示の構成を、他の実施形態に組み合わせても良い。また、複数の実施形態それぞれに開示の構成を集めて組み合わせても良い。

本開示に記載した課題は公知の課題ではなく、本発明者が独自に知見したものであり、本開示の構成及び方法と共に発明の進歩性を肯定する事実である。

[0024] なお、以下の実施形態は、主として自動車の車載用電子制御装置を例として説明するが、本開示は、請求の範囲で限定がない限り、車載用途以外の電子制御装置等を含むものである。

[0025] （実施形態１）

[0026] １．通信システムの構成

図１で示す通り、本実施形態の通信システム１０は、複数の電子制御装置、すなわちメッセージを送信する送信側電子制御装置１００、当該メッセージを受信する受信側電子制御装置２００、及びこれらを接続する通信路からなる。

[0027] ここで、本開示の“電子制御装置”とは、情報を取得又は処理することができ、かつ情報を他の装置との間で送信又は／及び受信できるものであればよく、車載用の電子制御装置の他、例えば、コンピュータ（パーソナルコンピュータ、組み込み型のマイクロコンピュータ等）、表示装置（テレビ、ナビゲーションシステム等）、記録再生装置（ＢＤ、ＤＶＤプレーヤー、ＳＤカードリーダー等）、通信装置（携帯電話、スマートフォン、タブレット、基地局等）、回路基板、半導体モジュール、半導体などが挙げられ、完成品

、半完成品、部品の形態のいずれも含むものである。

[0028] ２．送信側電子制御装置の構成

本実施形態の送信側電子制御装置１００は、鍵テーブル部１０１、鍵選択部１０２、メッセージ生成部１０３、ＦＶ生成部１０４、ＭＡＣ生成部１０５、送信部１０６を有する。

送信側電子制御装置１００、およびこれを構成する個々の機能ブロックは、専用又は汎用の中央演算処理装置、メモリ、バス、及びメモリに展開されて実行されるプログラムによって実現されてもよく、また半導体モジュールや回路基板をはじめとする専用のハードウェアで実現されてもよい。後述の受信側電子制御装置２００も同様である。

[0029] 鍵テーブル部１０１は、複数の鍵を有しており、例えばメモリで構成される。鍵は、通常の共通鍵を想定しているが、その他の鍵でもよく、またセッション鍵を用いてもよい。

[0030] 鍵選択部１０２は、後述のＦＶ生成部１０４で生成されたフレッシュネス値（ＦＶ：Freshness Value）（同期情報に相当）に基づき、鍵テーブル部１０１に保存された複数の鍵から一つの鍵を選択する。かかる選択は、予め定められた鍵選択ルールに従って行われる。鍵選択ルールは、例えばメモリに展開されてこれを実行することにより実現することができる。鍵選択方法の具体例は、後述する。選択された一つの鍵は、ＭＡＣ生成部１０５に出力される。

[0031] ここで、本開示の“基づき”とは、与えられる同期情報から最終的に一つの鍵を選択できればよく、その過程で必要な演算や処理を行う場合も含む。

また、本開示の“一つの鍵”とは、使用する、あるいは所定時間後次に使用を予定する一つの鍵を選択していればよく、これに加えて予備の鍵や次々回に使用を予定する鍵を選択している場合も当然含まれる。

[0032] なお、鍵テーブル部１０１及び鍵選択部１０２で、鍵選択装置１１を構成する。この場合、鍵選択装置１１の出力部から、選択された鍵がＭＡＣ生成部１０５に出力される。

[0033] メッセージ生成部１０３は、受信側電子制御装置２００に送信するメッセージを生成する。メッセージの具体例として、車両に搭載された車載用の電子制御装置の場合における車両を制御するための各種制御情報が挙げられる。制御情報については、実施形態２で説明する。車載用以外の電子制御装置の場合は、例えばセンサー等で検知した検出データ、テキストデータ、音声データ、画像データ等が挙げられる。

[0034] ＦＶ生成部１０４は、メッセージ生成部１０３で生成され後述の送信部１０６で送信されたメッセージの送信回数に応じてそれぞれフレッシュネス値を生成する。本実施形態では、フレッシュネス値のうち、カウンタを主として説明する。例えば、車載ネットワークであるＣＡＮの場合、生成された制御情報の種類に応じて付与されたＣＡＮＩＤ毎に、送信回数をカウントすることによりフレッシュネス値を生成する。例えば、ＣＡＮ＃１が付与された制御情報が４回送信された場合、ＣＡＮ＃１のフレッシュネス値は４となる。

[0035] ここで、本開示の“フレッシュネス値（ＦＶ）”とは、過去に使用された値かどうかを判別できる性質を有する値であり、例えばカウンタ、時間情報、ノンスを含む。カウンタとは、特定のメッセージが送信側電子制御装置から送信された回数、又は受信側電子制御装置で受信された回数を示す値であり、シーケンス番号も含む概念である。また、絶対的な値の他、例えばある基準を設けて当該基準からカウントした相対的な値も含む。

[0036] フレッシュネス値は、後述のように受信側電子制御装置２００でも、ＣＡＮＩＤ毎に受信回数をカウントすることにより生成される。したがって、送信側電子制御装置１００及び受信側電子制御装置２００でフレッシュネス値は同じ値をとることから、フレッシュネス値は送信側電子制御装置１００と受信側電子制御装置２００との通信において同期された情報である同期情報となる。

[0037] ここで、本開示の“同期された情報”とは、略同一時刻において送信側電子制御装置と受信側電子制御装置の双方で接することができる同一の情報の

他、異なる情報であってもその情報から同一の属性や同一の性質を導くことができる情報であればよい。また、情報単位で見た場合に、当該情報の全部の他、当該情報の一部であってもよい。さらに、情報の内容そのものを用いる場合の他、情報の属性や性質、例えば当該情報の送受信回数や所定条件下で当該情報を送受信したこと、等であってもよい。

[0038] ＭＡＣ生成部１０５は、鍵選択部１０２で選択された鍵、メッセージ生成部１０３で生成されたメッセージ、及びＦＶ生成部１０４で生成したフレッシュネス値を用いて、メッセージ認証コード（ＭＡＣ：Message Authentication Code）を生成する。例えば、メッセージにフレッシュネス値を挿入又は付加したデータに対し、選択された鍵を用いてＭＡＣアルゴリズムに基づき計算することによりメッセージ認証コードを生成する。

[0039] 送信部１０６は、メッセージ生成部１０３で生成されたメッセージにＦＶ生成部１０４で生成したフレッシュネス値を挿入又は付加したデータに、ＭＡＣ生成部１０５で生成したメッセージ認証コードを付与して送信する。送信先として特定の受信側電子制御装置２００を指定して送信してもよいが、送信先を指定せずにブロードキャストで送信してもよく、結果的に受信側電子制御装置２００で受信できるものであればよい。

[0040] ３．受信側電子制御装置の構成

本実施形態の受信側電子制御装置２００は、鍵テーブル部２０１、鍵選択部２０２、受信部２０３、ＦＶ検証部２０４、検証用ＭＡＣ生成部２０５、検証部２０６を有する。

[0041] 受信部２０３は、送信側電子制御装置１００から送信されたメッセージにフレッシュネス値を挿入又は付加したデータ、及びデータに付与されたメッセージ認証コードを受信する。

[0042] ＦＶ検証部２０４は、受信部２０３で受信したフレッシュネス値と、受信側電子制御装置２００で生成した検証用フレッシュネス値との同一性を検証する。検証用フレッシュネス値は、例えば車載ネットワークであるＣＡＮの場合、受信したメッセージに含まれる制御情報に付与されたＣＡＮＩＤ毎に

受信回数をカウントすることにより生成する。受信部２０３で受信したフレッシュネス値と検証用フレッシュネス値が一致すれば、検証用フレッシュネス値を後述の鍵選択部２０２及び検証用ＭＡＣ生成部２０５に出力する。一致しなければ、受信したデータを破棄する。

[0043] ＦＶ検証部２０４は、上述の動作に代えて、以下の動作を行ってもよい。検証用フレッシュネス値は、過去直近に受信したメッセージに含まれていたＣＡＮＩＤ毎に記録されているフレッシュネス値であり、ＦＶ検証部２０４は、受信部２０３で受信したフレッシュネス値が検証用フレッシュネス値よりも大きいかを検証する。大きければ、受信部２０３で受信したフレッシュネス値を新たな検証用フレッシュネス値として後述の鍵選択部２０２及び検証用ＭＡＣ生成部２０５に出力する。この場合は、受信回数をカウントするための構成を必要としないので、回路規模を小さくすることが可能である。

[0044] 鍵テーブル部２０１は、送信側電子制御装置１０１の鍵テーブル部１０１と同じ構成を有する。

[0045] 鍵選択部２０２は、送信側電子制御装置１００の鍵選択部１０２と同じ構成を有する。そして、鍵選択部２０２は、ＦＶ検証部２０４で生成された検証用フレッシュネス値（同期情報に相当）に基づき、鍵テーブル部２０１に保存された複数の鍵から一つの鍵を選択する。かかる選択は、鍵選択部１０２と同様の予め定められた鍵選択ルールに従って行われる。選択された一つの鍵は、検証用ＭＡＣ生成部２０５に出力される。

なお、送信側電子制御装置１００と同様、鍵テーブル部２０１及び鍵選択部２０２で、鍵選択装置２１を構成する。この場合、鍵選択装置２１の出力部から、選択された鍵が検証用ＭＡＣ生成部２０５に出力される。

[0046] 検証用ＭＡＣ生成部２０５は、鍵選択部２０２で選択された鍵、受信部２０３で受信したメッセージ、及びＦＶ検証部２０４から出力された検証用フレッシュネス値を用いて、検証用メッセージ認証コードを生成する。例えば、メッセージに検証用フレッシュネス値を挿入又は付加したデータに対し、選択された鍵を用いてＭＡＣアルゴリズムに基づき計算することにより検証

用メッセージ認証コードを生成する。

[0047] 検証部２０６は、受信部２０３で受信したメッセージ認証コードと検証用ＭＡＣ生成部２０５で生成した検証用メッセージ認証コードの同一性を検証する。メッセージ認証コードと検証用メッセージ認証コードが一致すれば、受信したメッセージの処理を行う。一致しなければ、受信したメッセージを破棄する。

[0048] なお、本実施形態では、メッセージにフレッシュネス値を挿入又は付加したデータを送信しているので、再生攻撃に対する耐性を上げることができる。しかし、必ずしもメッセージにフレッシュネス値を挿入又は付加する必要はない。フレッシュネス値の挿入又は付加がなくとも、送信側電子制御装置１００及び受信側電子制御装置２００がそれぞれ同じフレッシュネス値を生成することで同じ鍵を選択することができる。

[0049] 以上の本実施形態の送信側電子制御装置１００及び受信側電子制御装置２００によれば、本開示の上記効果を奏するとともに、フレッシュネス値を同期情報として利用しているので、従来のような専用の同期信号の送信を必要としないのはもちろん、フレッシュネス値自体を送信するか否かに関わらず、送信側電子制御装置１００及び受信側電子制御装置２００で同じ鍵を選択することができる。

[0050] ４．メッセージ送信方法、メッセージ受信方法、及び同方法を実行するプログラム

送信側電子制御装置１００で実行されるメッセージ送信方法、及び受信側電子制御装置２００で実行されるメッセージ受信方法を、図２を用いて説明する。

なお、図２の処理の順序は、ある処理が次の処理の前提条件となっていなければ、適宜入れ替えることが可能である。以下のいずれの実施形態においても同様である。

[0051] 送信側電子制御装置１００は、以下のステップを実行する。

同期情報であるフレッシュネス値を生成する（Ｓ１０１）

フレッシュネス値に基づき、鍵テーブル部１０１に保存された複数の鍵から一つの鍵を選択する（Ｓ１０２）。

受信側電子制御装置２００に送信するメッセージを生成する（Ｓ１０３）。

Ｓ１０２で選択した鍵、Ｓ１０３で生成したメッセージ、及びＳ１０１で生成したフレッシュネス値を用いて、メッセージ認証コードを生成する（Ｓ１０４）。

Ｓ１０３で生成したメッセージ、Ｓ１０１で生成したフレッシュネス値、からなるデータに、Ｓ１０４で生成したメッセージ認証コードを付与して送信する（Ｓ１０５）。

[0052] 受信側電子制御装置２００は、以下のステップを実行する。

送信側電子制御装置１００から送信されたメッセージ及びフレッシュネス値からなるデータ、及びデータに付与されたメッセージ認証コードを受信する（Ｓ２０１）。

Ｓ２０１で受信したフレッシュネス値と、受信側電子制御装置２００で生成した検証用フレッシュネス値とを比較（検証）する（Ｓ２０２）。一致又は条件を満たさなければ、受信したデータを破棄する（Ｓ２０３）。

Ｓ２０２で一致又は条件を満たせば、検証用フレッシュネス値に基づき、鍵テーブル部２０１に保存された複数の鍵から一つの鍵を選択する（Ｓ２０４）。

Ｓ２０４で選択された鍵、Ｓ２０１で受信したメッセージ、及び検証用フレッシュネス値を用いて検証用メッセージ認証コードを生成する（Ｓ２０５）。

Ｓ２０１で受信したメッセージ認証コードとＳ２０５で生成した検証用メッセージ認証コードの同一性を検証する（Ｓ２０６）。一致すれば、メッセージの処理を行う（Ｓ２０７）。一致しなければ、データを破棄する（Ｓ２０３）。

[0053] なお、これらの方法をコンピュータにて実行可能なプログラムの態様で実

現してもよい。

[0054] ここで、本開示の“コンピュータ”とは、少なくとも演算回路及びメモリを備えていればよく、汎用、専用等、その用途を問わない。また、パーソナルコンピュータ、サーバ、マイクロコンピュータ等、その形態も問わない。

[0055] 以上の本実施形態のメッセージ送信方法及びメッセージ受信方法によれば、本開示の上記効果を奏するとともに、メッセージ認証コードの検証に先立って、フレッシュネス値の検証を行っているので、メッセージの正真性を高めることができる。

[0056] ５．鍵選択装置、鍵選択方法、及び鍵選択プログラム

本実施形態では、図３（ａ）のように、鍵選択装置１１及び鍵選択装置２１を送信側電子制御装置１００及び受信側電子制御装置２００を構成する部品として構成した。この場合、鍵選択装置１１及び鍵選択装置２１は、例えば部品としての半導体モジュールや半導体として構成される。

[0057] しかし、図３（ｂ）のように、鍵選択装置１１及び鍵選択装置２２を独立した電子制御装置として構成し、メッセージ生成部１０３、ＦＶ生成部１０４、ＭＡＣ生成部１０５、及び送信部１０６からなるメッセージ送信装置１２、並びに、受信部２０３、ＦＶ検証部２０４、検証用ＭＡＣ生成部２０５、及び検証部２０６からなるメッセージ受信装置２２との間をそれぞれ接続して全体を送信側電子制御装置１００及び受信側電子制御装置２００としてもよい。この場合、鍵選択装置１１及び鍵選択装置２１は、部品としての半導体モジュールや半導体として構成することの他、完成品又は半完成品としての電子制御装置や回路基板として構成することができる。

[0058] あるいは、図３（ｃ）のように、鍵選択装置１１を、メッセージ送信装置１２及びメッセージ受信装置２２とで共有してもよい。この場合も、鍵選択装置１１は、部品、完成品又は半完成品として構成することが可能である。

[0059] なお、鍵選択装置１１及び鍵選択装置２１で実行される鍵選択方法は、コンピュータにて実行可能な鍵選択プログラムの態様で実現してもよい。

[0060] ここで、本開示の“鍵選択装置”とは、入力に応じて複数の鍵から一つの

鍵を選択できれば足り、その形態を問わない。すなわち、電子制御装置、回路基板、半導体モジュール、半導体などの、完成品、半完成品、部品の形態のいずれも含む。

[0061] なお、図３（ａ）（ｂ）（ｃ）は全て全体が通信システム１０となる。

また、図３（ｃ）のように、鍵テーブル部１０１と鍵選択部１０２からなる鍵選択装置１１を送信側と受信側で共有する場合、図３（ｃ）の鍵テーブル部１０１及び鍵選択部１０２は、送信側電子制御装置１００と受信側電子制御装置２００それぞれの鍵テーブル部１０１及び２０１、並びに鍵選択部１０２及び２０２として把握できる。

[0062] ６．鍵の選択方法（鍵選択ルール）

本実施形態では、鍵選択部１０２や鍵選択部２０２で鍵の選択に用いる同期情報としてフレッシュネス値を用いているが、鍵の選択方法（鍵選択ルール）についてさらに詳しく説明する。なお、本項では、鍵テーブルに含まれる鍵が２個（鍵１、鍵２）の場合を前提に説明するが、鍵の個数は２以上でもよい。

[0063] （１）カウンタ

図４（ａ）に、フレッシュネス値の一例であるカウンタの一例を示す。カウンタは８ビットからなる。そして、上位４ビットはイグニッションＯＮの回数をカウントし、下位４ビットは特定のＣＡＮＩＤを有するメッセージの送受信回数をカウントする。

[0064] 鍵選択ルールの一例として、カウンタの上位４ビットのうち最下位のビットが０の場合には鍵１を、１の場合には鍵２を選択する場合を考える。この場合は、イグニッションＯＮ毎に鍵を切り替えることができる。

他の例として、カウンタの上位４ビットのうち、最上位のビットが０の場合には鍵１を、１の場合には鍵２を選択する場合を考える。この場合は、イグニッションＯＮが８回実行される毎に鍵を切り替えることができる。

他の例として、カウンタの下位４ビットのうち、最上位のビットが０の場合には鍵１を、１の場合には鍵２を選択する場合を考える。この場合は、特

定のＣＡＮＩＤの送受信回数が８回実行される毎に鍵を切り替えることができる。

さらに、これらの例を組み合わせたり、複数のビットを用いてもよい。

この構成によれば、多様な鍵の切り換えのタイミングを設計することが可能となる。

[0065] あるいは、図４（ａ）のカウンタに代えて、図４（ｂ）のようなＣＡＮＩＤ毎のフレッシュネス値を用いてもよい。ここでは、制御情報の種類毎にＣＡＮＩＤが付与されているとする。

この構成によれば、ＣＡＮＩＤ毎に鍵選択ルールを設けることもできる。例えば、ＣＡＮ＃１が付与されたメッセージは最下位ビット、ＣＡＮ＃２が付与されたメッセージは最上位ビットの値に応じて鍵を切り替えるというルールが考えられる。このように、ＣＡＮＩＤ毎に鍵選択ルールを定めることにより、例えば電子制御装置が扱う制御情報の重要度に応じて鍵の切り換えタイミングを決めることができ、制御情報の重要度が高い程鍵の切り換えタイミングを早くすることが可能である。

[0066] このように、鍵選択部１０２や鍵選択部２０２は、フレッシュネス値を構成する特定のビットに基づき、鍵テーブル部１０１及び鍵テーブル部２０１から一つの鍵を選択する。

[0067] ここで、本開示の“特定のビット”とは、特定の一つのビットの他、特定の複数のビットも含む。例えば、上位２ビット、下位４ビット等が挙げられる。

[0068] （２）時間情報

同期情報として、フレッシュネス値の一例である、送信側電子制御装置及び受信側電子制御装置で生成される時間情報を用いてもよい。例えば、送信側電子制御装置１００及び受信側電子制御装置２００のタイマーを同期させ、各々の時間情報または送信側電子制御装置１００から送信される時間情報に基づき、鍵を切り替えてもよい。

[0069] ここで、本開示の“時間情報”とは、時間を示す情報であり、例えば時刻

やタイムスタンプ、基準時からの経過時間等が挙げられる。また時刻には、日や年の情報を含む場合、あるいは日や年の情報単独の場合も含む。

[0070] （３）ノンス

同期情報として、フレッシュネス値の一例である、ノンスを用いてもよい。ノンスとは、送信側電子制御装置１００から受信側電子制御装置２００に送信する使い捨てのランダムな値である。そして、例えばノンスの特定のビットに基づき、鍵を切り替えてもよい。

[0071] （実施形態２）

[0072] 図５は、本実施形態の通信システム３０を構成する送信側電子制御装置３００、及び受信側電子制御装置４００を示す。なお、実施形態１と同様の構成は同じ図番を用いている。なお、本実施形態の通信システム３０及びこれを構成する送信側電子制御装置３００及び受信側電子制御装置４００は、車両に搭載されていることを前提としている。

[0073] １．送信側電子制御装置の構成

本実施形態の送信側電子制御装置３００は、実施形態１の送信側電子制御装置１００と同様の構成を有する。その結果、各ブロックの機能は以下の通りとなる。

[0074] メッセージ生成部１０３は、メッセージとして車両を制御する制御情報を生成する。

また、鍵選択部３０２は、制御情報に基づき、鍵テーブル部１０１に保存された複数の鍵から一つの鍵を選択する。つまり、本実施形態では、車両を制御する制御情報が同期情報に該当する。

[0075] ここで、本開示の“車両を制御”とは、車両全体の挙動を制御する場合の他、車両を構成する部品（例えば、ドア、ミラー、エアバック、ワイパー等）を制御する場合、車両に搭載されている各種装置（エアコン、ナビゲーションシステム、オーディオプレーヤー等）を制御する場合も含む。

本開示の“制御情報”には、例えば、速度、ドアの開閉に関する情報、ミラー角度の調整に関する情報、シート位置の調整に関する情報、イグニッシ

ョンのＯＮ－ＯＦＦに関する情報、を含むが、これらに限定されない。

[0076] ＭＡＣ生成部３０５は、鍵選択部３０２で選択された鍵、メッセージ生成部１０３で生成された制御情報、及びＦＶ生成部１０４で生成したフレッシュネス値を用いて、を用いて、メッセージ認証コード（ＭＡＣ：Message Authentication Code）を生成する。

送信部３０６は、メッセージ生成部１０３で生成された制御情報にＦＶ生成部１０４で生成したフレッシュネス値を挿入又は付加したデータに、ＭＡＣ生成部３０５で生成したメッセージ認証コードを付与して送信する。

[0077] ２．受信側電子制御装置の構成

本実施形態の受信側電子制御装置４００は、実施形態１の受信側電子制御装置２００と同様の構成を有する。その結果、各ブロックの機能は以下の通りとなる。

[0078] 受信部４０３は、送信側電子制御装置１００から送信された制御情報にフレッシュネス値を挿入又は付加したデータ、及びデータに付与されたメッセージ認証コードを受信する。

鍵選択部４０２は、受信した制御情報に基づき、鍵テーブル部２０１に保存された複数の鍵から一つの鍵を選択する。

検証用ＭＡＣ生成部４０５は、鍵選択部４０２で選択された鍵、受信部４０３で受信した制御情報、及びＦＶ検証部２０４から出力された検証用フレッシュネス値を用いて、検証用メッセージ認証コードを生成する。

[0079] ３．メッセージ送信方法、メッセージ受信方法、及び同方法を実行するプログラム

送信側電子制御装置３００で実行されるメッセージ送信方法、及び受信側電子制御装置４００で実行されるメッセージ受信方法を、図６を用いて説明する。

[0080] 送信側電子制御装置３００は、以下のステップを実行する。

受信側電子制御装置４００に送信するメッセージである制御情報を生成する（Ｓ３０１）。

Ｓ３０１で生成した制御情報に基づき、鍵テーブル部１０１に保存された複数の鍵から一つの鍵を選択する（Ｓ３０２）。

Ｓ３０２で選択した鍵、Ｓ３０１で生成した制御情報、及びフレッシュネス値を用いて、メッセージ認証コードを生成する（Ｓ３０３）。

Ｓ３０１で生成した制御情報及びフレッシュネス値に、Ｓ３０３で生成したメッセージ認証コードを付与して送信する（Ｓ３０４）。

[0081] 受信側電子制御装置４００は、以下のステップを実行する。

送信側電子制御装置３００から送信された制御情報及びフレッシュネス値、並びに制御情報及びフレッシュネス値に付与されたメッセージ認証コードを受信する（Ｓ４０１）。

Ｓ４０１で受信したフレッシュネス値と、受信側電子制御装置４００で生成した検証用フレッシュネス値とを比較（検証）する（Ｓ４０２）。一致又は条件を満たさなければ、受信した制御情報を破棄する（Ｓ４０７）。

Ｓ４０２で一致又は条件を満たせば、制御情報に基づき、鍵テーブル部２０１に保存された複数の鍵から一つの鍵を選択する（Ｓ４０３）。

Ｓ４０３で選択された鍵、Ｓ４０１で受信した制御情報、及び検証用フレッシュネス値を用いて検証用メッセージ認証コードを生成する（Ｓ４０４）。

Ｓ４０１で受信したメッセージ認証コードとＳ４０４で生成した検証用メッセージ認証コードの同一性を検証する（Ｓ４０５）。一致すれば、制御情報の処理を行う（Ｓ４０６）。一致しなければ、制御情報を破棄する（Ｓ４０７）。

[0082] ４．鍵の選択方法（鍵選択ルール）

本実施形態では、鍵選択部３０２や鍵選択部４０２で鍵の選択に用いる同期情報として車両を制御する制御情報を用いているが、鍵の選択方法（鍵選択ルール）についてさらに詳しく説明する。なお、本項では、鍵テーブルに含まれる鍵が２個（鍵１、鍵２）の場合を前提に説明するが、鍵の個数は２以上でもよい。

[0083] （１）速度情報

鍵選択ルールの一例として、速度が一定以上となった場合には鍵１を、速度が一定以下となった場合には鍵２を選択するようにしてもよい。速度に応じて鍵を選択、変更するようにすることで、車両の危険性に応じた鍵の切り換えが可能となる。

[0084] （２）ドアの開閉情報

鍵選択ルールの一例として、ドアの開閉が所定回数毎に鍵１と鍵２を切り替えるようにしてもよい。ドアの開閉時は車両が停止しているので、車両が安全な状態、かつ車載ネットワークの輻輳が小さいときに鍵の切り換えを行うことが可能となる。

[0085] （３）ミラー調整情報、またはシートの位置調整情報

鍵選択ルールの一例として、ミラー調整が行われたとき、又はシートの位置調整が行われたときに、鍵１と鍵２を切り替えるようにしてもよい。これらが行われたときは運転者が変わった時である場合が多いので、事実上運転者毎に鍵を変更することが可能となる。

[0086] （４）その他

送信側電子制御装置３００から送信される制御情報の送信頻度に基づいて鍵を選択してもよい。

ここで、本開示の“送信頻度”とは、所定時間に送信される制御情報の頻度をいい、回数、周期、時間等で示されるものである。

[0087] 以上の本実施形態の送信側電子制御装置３００及び受信側電子制御装置４００によれば、本開示の上記効果を奏するとともに、制御情報を同期情報として利用しているので、従来のような専用の同期信号の送信を必要としないのはもちろん、車両の搭載された電子制御装置の通信方式を変更することなく、送信側電子制御装置３００及び受信側電子制御装置４００で同じ鍵を選択することができる。

[0088] （実施形態３）

[0089] 図７は、本実施形態の通信システム５０を構成する送信側電子制御装置５

００、及び受信側電子制御装置６００を示す。なお、実施形態１と同様の構成は同じ図番を用いている。実施形態１及び実施形態２ではメッセージ認証の例を開示し、メッセージ認証コード生成のために鍵を用いる例を示した。本実施形態では暗号化の例を開示し、送信するメッセージを暗号化及び暗号化メッセージを復号するために鍵を用いる例を示す。なお、実施形態１及び２に記載された事項は、当然適宜実施形態３と組み合わせることが可能である。

[0090] １．送信側電子制御装置の構成

本実施形態の送信側電子制御装置５００は、鍵テーブル部１０１、鍵選択部１０２、メッセージ生成部１０３、ノンス生成部５０１、暗号化部５０２、及び送信部１０６を有する。

[0091] ノンス生成部５０１は、使い捨てのランダムな値であるノンスを生成する。本実施形態では、ノンスが本開示の同期された情報である同期情報となるが、これに限られない。

[0092] 鍵選択部１０２は、ノンス生成部５０１で生成されたノンスに基づき、鍵テーブル部１０１に保存された複数の鍵から一つの鍵を選択する。

[0093] 暗号化部５０２は、鍵選択部１０２で選択された鍵を用いてメッセージ生成部１０３で生成されたメッセージを暗号化し、暗号化メッセージを生成する。暗号化の方法は任意である。なお、ノンスを含めたメッセージを暗号化してもよい。

[0094] 送信部１０６は、暗号化部５０２で生成した暗号化メッセージ、およびノンスを送信する。

[0095] ２．受信側電子制御装置の構成

本実施形態の受信側電子制御装置６００は、受信部２０３、鍵テーブル部２０１、鍵選択部２０２、復号部６０１を有する。

[0096] 鍵選択部２０２は、受信部２０３で受信したノンスに基づき、鍵テーブル部２０１に保存された複数の鍵から一つの鍵を選択する。

[0097] 復号部６０１は、鍵選択部２０２で選択された鍵を用いて暗号化メッセー

ジを復号し、メッセージを生成する。復号の方法も暗号化と同様任意である。なお、ノンスを含めたメッセージを復号してもよい。

[0098] 以上の本実施形態の送信側電子制御装置５００及び受信側電子制御装置６００によれば、本開示の上記効果を奏するとともに、メッセージの秘匿性を確保することができる。

[0099] （その他の実施形態）

[0100] 以上の実施形態では、二つの電子制御装置間に着目したが、これを３つ以上の電子制御装置に用いてもよい。例えば、ＥＣＵ１からＥＣＵ２及びＥＣＵ３にメッセージを送信する際、ＥＣＵ１及びＥＣＵ２の間では鍵選択ルール１及び鍵セットＡを用い、ＥＣＵ１及びＥＣＵ３の間では鍵選択ルール２及び鍵セットＢを用いるようにしてもよい。この構成によれば、受信側のＥＣＵ、あるいは送受信するメッセージの種類に応じて、鍵選択ルールや鍵セットを用いることが可能となる。

[0101] （総括）

[0102] 以上、本開示の各実施形態における電子制御装置等について説明した。

なお、本開示は、コンピュータに実行されるプログラムの形態でも実現できるが、専用や汎用のハードウェアにおける記憶領域（外部記憶装置（ハードディスク、ＵＳＢメモリ等）、内部記憶装置（ＲＡＭ，ＲＯＭ等））に格納されるプログラムは、記録媒体を介して、あるいは記録媒体を介さずにサーバから通信回線を経由して上述の専用又は汎用のハードウェア（コンピュータに相当）に提供することもできる。これにより、プログラムのアップグレードを通じて常に最新の機能を提供することができる。

産業上の利用可能性

[0103] 本開示の電子制御装置等は、各実施形態で自動車に搭載される電子制御装置を念頭に置いて説明したが、自動二輪車、船舶、鉄道、航空機等、移動する移動体全般に適用することが可能でありこれらを含むものである。また、移動体に限らず、コンピュータを包含する製品全般に適用可能である。

請求の範囲

[請求項1] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記送信側電子制御装置（１００）であって、

複数の鍵を有する鍵テーブル部（１０１）と、

当該送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部（１０２）と、

前記メッセージを生成するメッセージ生成部（１０３）と、

前記鍵選択部で選択された鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成するＭＡＣ生成部（１０５）と、

前記メッセージに前記メッセージ認証コードを付与して送信する送信部（１０６）と、

を有する電子制御装置（１００）。

[請求項2] 前記同期情報は、当該送信側電子制御装置及び前記受信側電子制御装置で生成されるフレッシュネス値（ＦＶ）である、

請求項１記載の電子制御装置（１００）。

[請求項3] 前記同期情報は、当該送信側電子制御装置及び前記受信側電子制御装置で生成される時間情報である、

請求項１又は２記載の電子制御装置（１００）。

[請求項4] 前記同期情報は、当該送信側電子制御装置から前記受信側電子制御装置に送信した使い捨てのランダムな値であるノンスである、

請求項１又は２記載の電子制御装置（１００）。

[請求項5] 車両に搭載された当該送信側電子制御装置であって、

前記同期情報は、前記車両を制御する制御情報である、

請求項１記載の電子制御装置（３００）。

[請求項6] 前記鍵選択部は、前記フレッシュネス値を構成する特定のビットに基づき、前記鍵テーブル部から一つの鍵を選択する、

請求項２記載の電子制御装置（１００）。

[請求項7] 前記鍵選択部は、当該送信側電子制御装置から送信される前記制御情報の送信頻度に基づき、前記鍵テーブル部から一つの鍵を選択する、

請求項５記載の電子制御装置（３００）。

[請求項8] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記受信側電子制御装置（２００）であって、

前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信する受信部（２０３）と、

複数の鍵を有する鍵テーブル部（２０１）と、

当該受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部（２０２）と、

前記鍵選択部で選択された鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成する検証用ＭＡＣ生成部（２０５）と、

前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する検証部（２０６）と、

を有する電子制御装置（２００）。

[請求項9] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）であって、

前記送信側電子制御装置及び前記受信側電子制御装置はそれぞれ、

複数の鍵を有する鍵テーブル部（１０１、２０１）と、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から

一つの鍵を選択する鍵選択部（１０２、２０２）と、

を有し、

前記送信側電子制御装置は、

前記メッセージを生成するメッセージ生成部（１０３）と、

前記鍵選択部で選択された鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成するＭＡＣ生成部（１０５）と、

前記メッセージに前記メッセージ認証コードを付与して送信する送信部（１０６）と、

を有し、

前記受信側電子制御装置は、

前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信する受信部（２０３）と、

前記鍵選択部で選択された鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成する検証用ＭＡＣ生成部（２０５）と、

前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する検証部（２０６）と、

を有する通信システム（１０）。

[請求項10] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）で用いられる鍵選択装置（１１、１２）であって、

複数の鍵を有する鍵テーブル部（１０１、１０２）と、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部（１０２、２０２）と、

前記鍵選択部で選択された前記一つの鍵を出力する出力部と、

を有する鍵選択装置（１１、１２）。

[請求項11] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記送信側電子制御装置（１００）で実行されるメッセージ送信方法あって、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、

前記メッセージを生成し、

選択された前記一つの鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成し、

前記メッセージに前記メッセージ認証コードを付与して送信する、

メッセージ送信方法。

[請求項12] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記受信側電子制御装置（２００）で実行されるメッセージ受信方法であって、

前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信し、

前記受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、

選択された前記一つの鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成し、

前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証する、

メッセージ受信方法。

[請求項13] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信シ

ステム（１０）で用いられる鍵選択方法であって、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する前記鍵テーブル部から一つの鍵を選択し、

選択された前記一つの鍵を出力する、

鍵選択方法。

[請求項14] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記送信側電子制御装置（１００）で実行されるメッセージ送信プログラムであって、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、

前記メッセージを生成し、

選択された前記一つの鍵及び前記メッセージを用いてメッセージ認証コード（ＭＡＣ）を生成し、

前記メッセージに前記メッセージ認証コードを付与して送信すること、

を有するコンピュータにて実行可能なメッセージ送信プログラム。

[請求項15] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）の前記受信側電子制御装置（２００）で実行されるメッセージ受信プログラムであって、

前記送信側電子制御装置から送信された前記メッセージ及び前記メッセージに付与されたメッセージ認証コード（ＭＡＣ）を受信し、

前記受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する鍵テーブル部から一つの鍵を選択し、

選択された前記一つの鍵及び前記メッセージを用いて検証用メッセージ認証コード（ＭＡＣ）を生成し、

前記メッセージ認証コードと前記検証用メッセージ認証コードの同一性を検証すること、

を有するコンピュータにて実行可能なメッセージ受信プログラム。

[請求項16] メッセージを送信する送信側電子制御装置（１００）及び前記メッセージを受信する受信側電子制御装置（２００）で構成される通信システム（１０）で用いられる鍵選択プログラムであって、

前記送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、複数の鍵を有する前記鍵テーブル部から一つの鍵を選択し、

選択された前記一つの鍵を出力することと、

を有するコンピュータにて実行可能な鍵選択プログラム。

[請求項17] 暗号化メッセージを送信する送信側電子制御装置（５００）及び前記暗号化メッセージを受信する受信側電子制御装置（６００）で構成される通信システム（５０）の前記送信側電子制御装置（５００）であって、

複数の鍵を有する鍵テーブル部（１０１）と、

当該送信側電子制御装置と前記受信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部（１０２）と、

メッセージを生成するメッセージ生成部（１０３）と、

前記鍵選択部で選択された鍵及び前記メッセージを用いて前記暗号化メッセージを生成する暗号化部（５０２）と、

前記暗号化メッセージを送信する送信部（１０６）と、

を有する電子制御装置（５００）。

[請求項18] 暗号化メッセージを送信する送信側電子制御装置（５００）及び前記暗号化メッセージを受信する受信側電子制御装置（６００）で構成

される通信システム（５０）の前記受信側電子制御装置（６００）であって、

前記暗号化メッセージを受信する受信部（２０３）と、

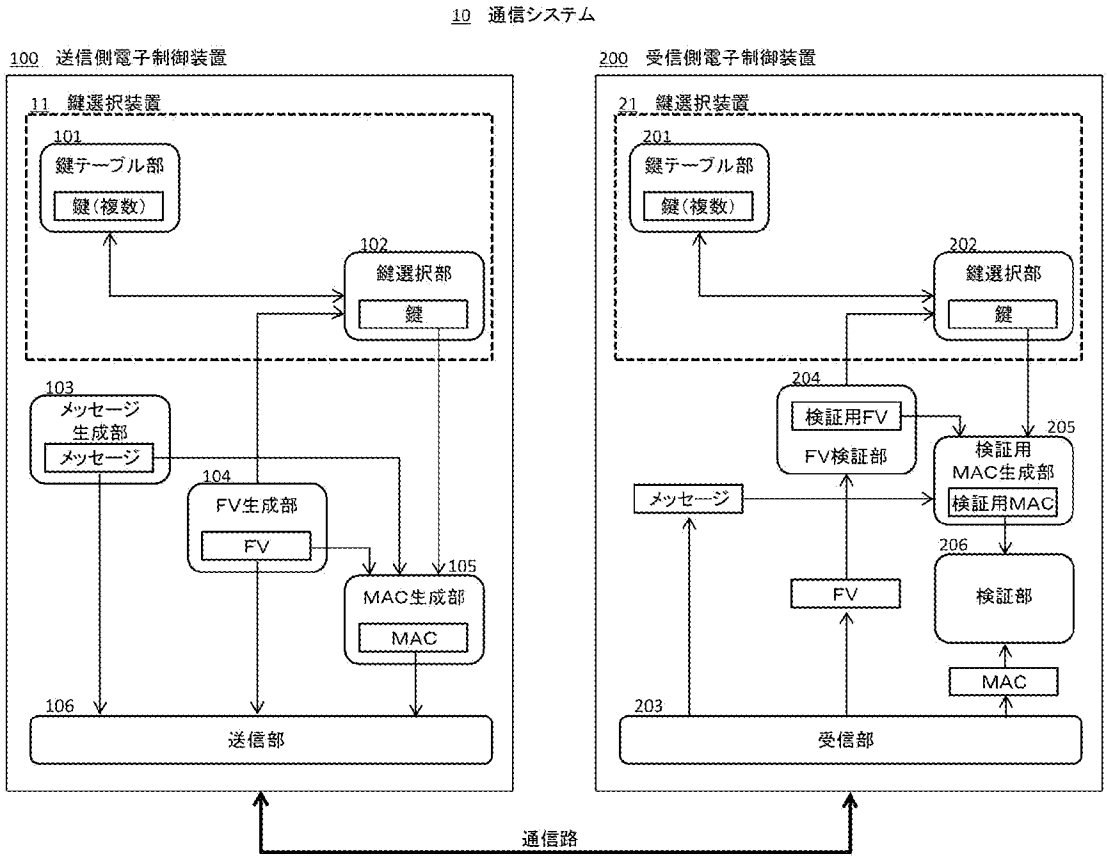
複数の鍵を有する鍵テーブル部（２０１）と、

当該受信側電子制御装置と前記送信側電子制御装置との通信において同期された情報である同期情報に基づき、前記鍵テーブル部から一つの鍵を選択する鍵選択部（２０２）と、

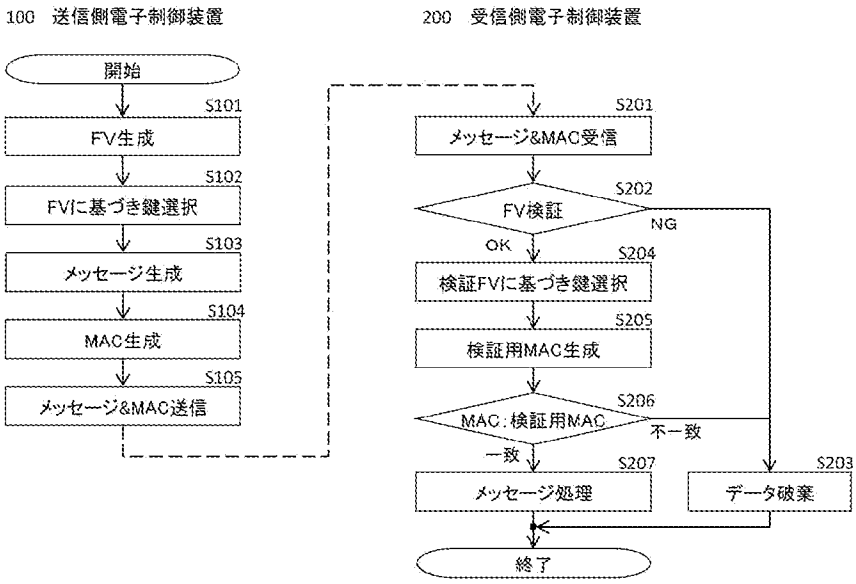
前記鍵選択部で選択された鍵を用いて前記暗号化メッセージを復号する復号部（６０２）と、

を有する電子制御装置（６００）。

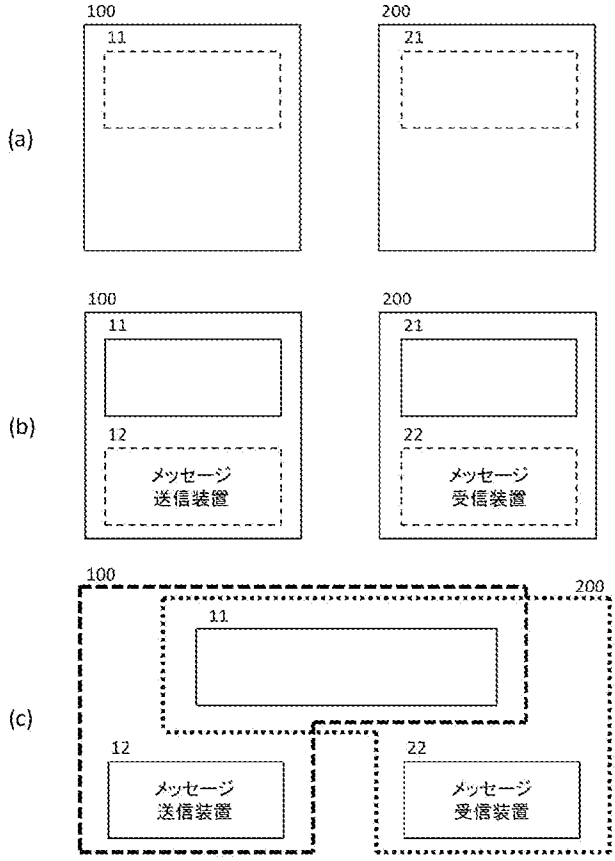
[図1]


10 通信システム
100 送信側電子制御装置
11 鍵選択装置
101
鍵テーブル部
鍵(複数)
102
鍵選択部
鍵
103
メッセージ
生成部
メッセージ
104
FV生成部
FV
105
MAC生成部
MAC
106
送信部
200 受信側電子制御装置
21 鍵選択装置
201
鍵テーブル部
鍵(複数)
202
鍵選択部
鍵
204
検証用FV
FV検証部
205
検証用
MAC生成部
検証用MAC
メッセージ
206
検証部
FV
MAC
203
受信部
通信路

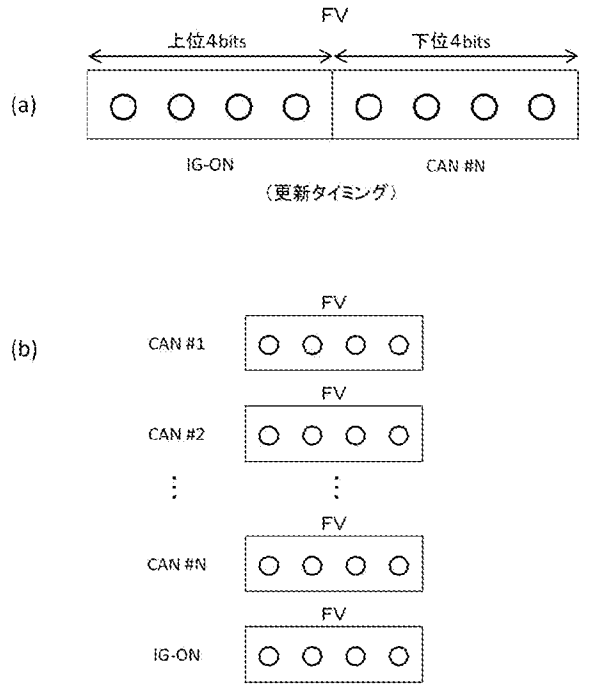
[図2]


100 送信側電子制御装置
開始
S101
FV生成
S102
FVに基づき鍵選択
S103
メッセージ生成
S104
MAC生成
S105
メッセージ&MAC送信
200 受信側電子制御装置
S201
メッセージ&MAC受信
S202
FV検証
NG
OK
S204
検証FVに基づき鍵選択
S205
検証用MAC生成
S206
MAC:検証用MAC
不一致
一致
S207
メッセージ処理
S203
データ破棄
終了

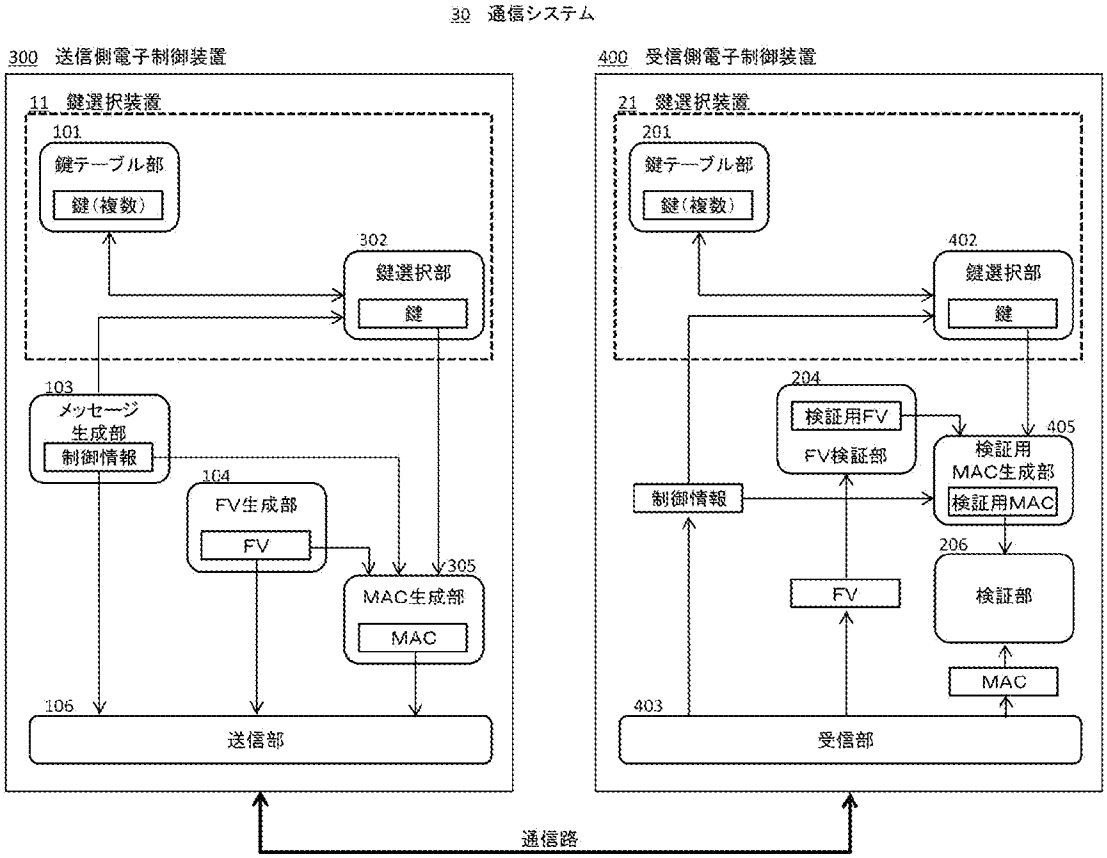
[図3]


(a)
100
11
200
21
(b)
100
11
12
メッセージ
送信装置
200
21
22
メッセージ
受信装置
(c)
100
200
11
12
メッセージ
送信装置
22
メッセージ
受信装置

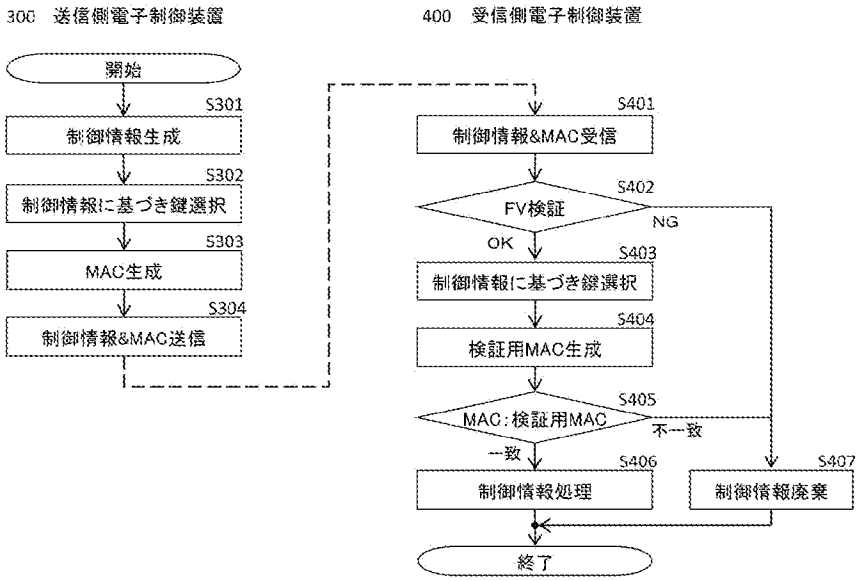
[図4]


(a)
FV
上位4bits
下位4bits
IG-ON
CAN #N
(更新タイミング)
(b)
FV
CAN #1
FV
CAN #2
FV
CAN #N
FV
IG-ON

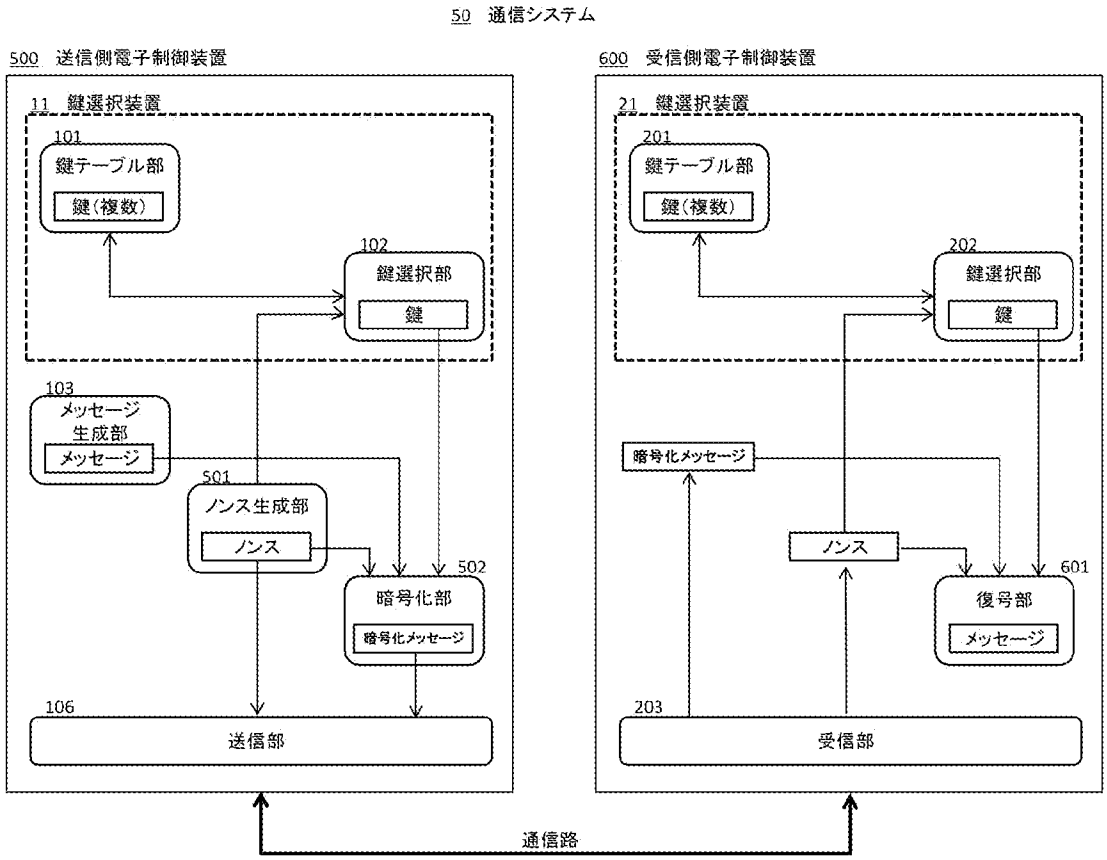
[図5]


30 通信システム
300 送信側電子制御装置
11 鍵選択装置
101
鍵テーブル部
鍵(複数)
302
鍵選択部
鍵
103
メッセージ生成部
制御情報
104
FV生成部
FV
305
MAC生成部
MAC
106
送信部
400 受信側電子制御装置
21 鍵選択装置
201
鍵テーブル部
鍵(複数)
402
鍵選択部
鍵
204
検証用FV
FV検証部
405
検証用MAC生成部
検証用MAC
制御情報
206
検証部
FV
MAC
403
受信部
通信路

[図6]


300 送信側電子制御装置
開始
S301
制御情報生成
S302
制御情報に基づき鍵選択
S303
MAC生成
S304
制御情報&MAC送信
400 受信側電子制御装置
S401
制御情報&MAC受信
S402
FV検証
NG
OK
S403
制御情報に基づき鍵選択
S404
検証用MAC生成
S405
MAC:検証用MAC
不一致
一致
S406
制御情報処理
S407
制御情報廃棄
終了

[図7]


50 通信システム
500 送信側電子制御装置
11 鍵選択装置
101
鍵テーブル部
鍵(複数)
102
鍵選択部
鍵
103
メッセージ
生成部
メッセージ
501
ノンス生成部
ノンス
502
暗号化部
暗号化メッセージ
106
送信部
600 受信側電子制御装置
21 鍵選択装置
201
鍵テーブル部
鍵(複数)
202
鍵選択部
鍵
暗号化メッセージ
ノンス
601
復号部
メッセージ
203
受信部
通信路

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/001320

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/14(2006.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl. H04L9/14, G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2017/0302452 A1 (GM GLOBAL TECHNOLOGY OPERATIONS LLC) 19 October 2017, paragraphs [0014]-[0024] & DE 102017107879 A & CN 107306269 A	1, 2, 5-16 3, 4, 17, 18
X Y	JP 2003-272285 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 26 September 2003, paragraphs [0119]-[0136] (Family: none)	17, 18 3
X Y	JP 6-98179 A (NEC CORP.) 08 April 1994, paragraphs [0008]-[0014] (Family: none)	17, 18 3
X Y	JP 2003-101528 A (NAGANO FUJITSU COMPONENT KK) 04 April 2003, paragraphs [0047]-[0053] (Family: none)	17, 18 3
X Y	WO 2011/145353 A1 (SANYO ELECTRIC CO., LTD.) 24 November 2011, paragraphs [0012]-[0051] & US 2013/0195272 A1, paragraphs [0038]-[0078] & CN 102484791 A	1, 2, 4, 6, 8-18 4, 17, 18

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 April 2019 (05.04.2019)	16 April 2019 (16.04.2019)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／００１３２０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14(2006.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14, G09C1/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	US 2017/0302452 A1 (GM GLOBAL TECHNOLOGY OPERATIONS LLC) 2017.10.19, 段落 0014－0024 & DE 102017107879 A & CN 107306269 A	1, 2, 5-16 3, 4, 17, 18
X Y	JP 2003-272285 A (松下電器産業株式会社) 2003.09.26, 段落 0119－0136 (ファミリーなし)	17, 18 3

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０５．０４．２０１９	国際調査報告の発送日 １６．０４．２０１９
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　６３０４ 行田　悦資 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	JP 6-98179 A (日本電気株式会社) 1994.04.08, 段落 0008－0014 (ファミリーなし)	17, 18 3
X Y	JP 2003-101528 A (長野富士通コンポーネント株式会社) 2003.04.04, 段落 0047－0053 (ファミリーなし)	17, 18 3
X Y	WO 2011/145353 A1 (三洋電機株式会社) 2011.11.24, 段落 0012－0051 & US 2013/0195272 A1, 段落 0038－0078 & CN 102484791 A	1, 2, 4, 6, 8-18 4, 17, 18