

(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
2020年10月15日(15.10.2020)



(10) 国際公開番号

WO 2020/209248 A1

(51) 国際特許分類:
G06F 21/44 (2013.01)

SEISAKUSHO) [JP/JP]; 〒4800195 愛知県丹羽郡大口町豊田三丁目260番地 Aichi (JP).

(21) 国際出願番号: PCT/JP2020/015654

(72) 発明者: 大橋 洋介(OHASHI, Yosuke); 〒4800195 愛知県丹羽郡大口町豊田三丁目260番地 株式会社東海理化電機製作所内 Aichi (JP). 古田 昌輝(FURUTA, Masateru); 〒4800195 愛知県丹羽郡大口町豊田三丁目260番地 株式会社東海理化電機製作所内 Aichi (JP).

(22) 国際出願日: 2020年4月7日(07.04.2020)

(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 2019-076299 2019年4月12日(12.04.2019) JP
特願 2020-052415 2020年3月24日(24.03.2020) JP

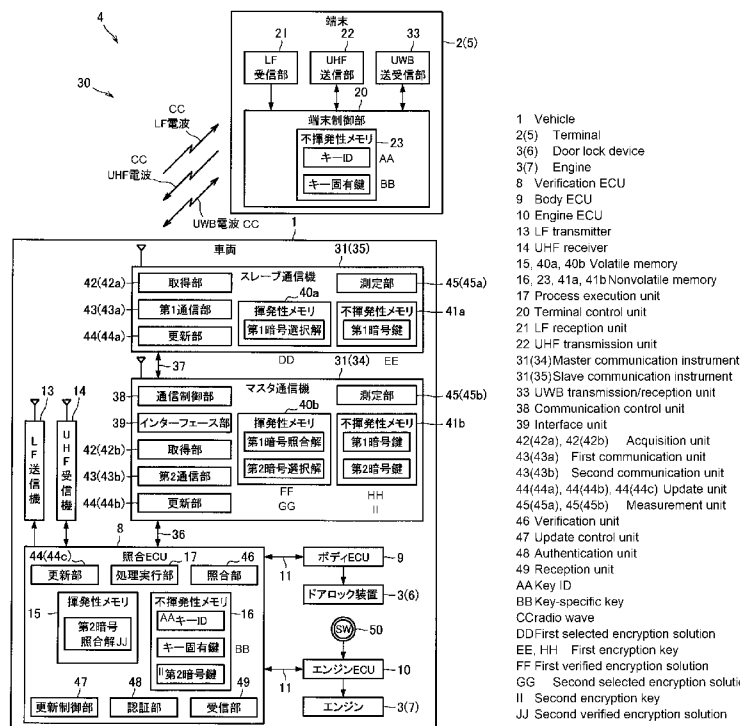
(74) 代理人: 伊藤 学, 外 (ITO, Manabu et al.); 〒1600023 東京都新宿区西新宿7-22-37 ストック西新宿413 協学国際特許事務所 Tokyo (JP).

(71) 出願人: 株式会社東海理化電機製作所(KABUSHIKI KAISHA TOKAI RIKI DENKI

(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,

(54) Title: COMMUNICATION SYSTEM AND COMMUNICATION INSTRUMENT

(54) 発明の名称: 通信システム及び通信機



(57) Abstract: [Problem] To provide a new and improved communication system and a communication instrument with which it is possible to quicken a timing from when communication with an external device is completed until when communication data corresponding to a communication result is outputted to another device. [Solution] Provided is a communication system comprising a communication instrument for transmitting a selected solution which is selected in accordance with the result of first communication with an external apparatus, and a control device for receiving the

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

selected solution from the communication instrument by second communication in which a communication partner with the communication instrument is different than in the first communication.

(57) 要約: 【課題】 外部装置との通信が完了してから、通信結果に対応する通信データを別の装置へ出力するまでのタイミングを早期化可能とした、新規かつ改良された通信システム、及び通信機を提供する。 【解決手段】 外部機器との第1通信の結果に応じて選択された選択解を送信する通信機と、前記第1通信とは前記通信機との通信相手が異なる第2通信により前記通信機から前記選択解を受信する制御装置と、を有する、通信システムが提供される。

明 細 書

発明の名称：通信システム及び通信機

技術分野

[0001] 本発明は、通信システム及び通信機に関する。

背景技術

[0002] 従来、通信機と外部機器との間で通信を行う通信システムがある（例えば、特許文献 1 参照）。例えば、通信機と外部機器との間の通信で導き出された結果を処理することによって生成された通信データを、通信機から別の装置に出力する場合がある。かかる場合、一般的には、通信機において結果が導き出された後に、結果が処理されて通信データが生成される。

先行技術文献

特許文献

[0003] 特許文献 1：特開 2012-036582 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、通信機において結果が導き出されてから通信データを生成すると、通信データの送信が完了するまでに時間がかかるという問題があった。

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、外部装置との通信が完了してから、通信結果に対応する通信データを別の装置へ出力するまでのタイミングを早期化可能とした、新規かつ改良された通信システム、及び通信機を提供することにある。

課題を解決するための手段

[0005] 上記課題を解決するために、本発明のある観点によれば、外部機器との第 1 通信の結果に応じて選択された選択解を送信する通信機と、前記第 1 通信とは前記通信機との通信相手が異なる第 2 通信により前記通信機から前記選択解を受信する制御装置と、を有する、通信システムが提供される。

[0006] また、上記課題を解決するために、本発明の別の観点によれば、外部機器

との第1通信の結果に応じて選択された選択解を取得する取得部と、前記第1通信とは通信相手が異なる第2通信により前記選択解を制御装置に送信する通信部と、を備える、通信機が提供される。

発明の効果

[0007] 以上説明したように本発明によれば、処理時間の増加を抑制可能な通信システム及び通信機が提供される。

図面の簡単な説明

[0008] [図1]通信システムの構成を示すブロック図である。

[図2]車両における通信機の配置を示す図である。

[図3]距離測定の手順を示す説明図である。

[図4] (a) 測定値が正当である場合の暗号選択解の送信を示す説明図であり、
(b) 測定値が正当でない場合の暗号選択解の送信を示す説明図であり、
(c) 第1暗号選択解が第1暗号照合解に一致しない場合における照合ECUへの通知例を示す説明図である。

[図5]照合ECUへの通知と、マスタ通信機における測定値の判定結果と、スレーブ通信機における測定値の判定結果との対応関係の例をまとめた表である。

[図6]スレーブ通信機と端末との間において通信エラーが生じた場合における照合ECUへの通知例を示す説明図である。

発明を実施するための形態

[0009] 以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0010] <1. 一実施形態>

以下、通信システム及び通信機の一実施形態について図1～図4を用いて説明する。

[0011] <<1. 1. 構成例>>

図 1 を用いて、本実施形態に係る通信システムの構成例について説明する。図 1 に示すように、本実施形態に係る通信システムは、電子キーシステム 4 を備える。電子キーシステム 4 は、無線を通じて端末 2 が正規のものか否かを確認することにより（端末 2 を認証することにより）車載装置 3 の作動可否を制御する。より具体的に、本例の電子キーシステム 4 は、車両 1 及び端末 2 のうち、一方によって認証に必要なキー ID（ID 情報）が送信され、当該キー ID が他方によって受信された場合に、当該他方によって受信されたキー ID と当該他方に登録されたキー ID とを照合する ID 照合（以下、「スマート照合」とも記載する。）を実行するスマート照合システムである。

[0012] 後にも説明するように、本例では、スマート照合が車両 1 において行われる場合を主に想定する。しかし、スマート照合は端末 2 において行われてもよい。また、スマート照合は、無線通信による端末 2 の認証の一例である。したがって、端末 2 の認証の手法はスマート照合に限定されない。電子キーシステム 4 によってスマート照合が実行される場合、図 1 に示すように、端末 2 は、電子キー 5 であることが望ましい。電子キー 5 は、例えば車両 1 との無線通信を通じたスマート照合に使用され、スマート照合に基づいて車載装置 3 の作動を実行するキー機能を有する。

[0013] （車両の各構成）

続いて、車両 1 の各構成について説明する。車両 1 は、車載装置 3 と、照合 ECU（Electronic Control Unit）8 と、ボディ ECU 9 と、エンジン ECU 10 と、LF（Low Frequency）送信機 13 と、UHF（Ultra High Frequency）受信機 14 と、通信機 31 とを備える。図 1 に示すように、車載装置 3 としては、車両ドアの施解錠を制御するドアロック装置 6 が例として挙げられる他、車両 1 のエンジン 7 が例として挙げられる。

[0014] 照合 ECU 8 は、揮発性メモリ 15 と、不揮発性メモリ 16 と、処理実行部 17 と、更新部 44c と、照合部 46 と、更新制御部 47 と、認証部 48 と、受信部 49 とを有する。認証部 48 は、スマート照合を実行し、スマー

ト照合によって端末2を認証する。照合ECU8の不揮発性メモリ16には、端末2に固有のキーIDと、キー固有鍵とが登録されている。キーID及びキー固有鍵は、スマート照合に使用される。揮発性メモリ15、処理実行部17、更新部44c、照合部46、更新制御部47及び受信部49については、後に詳細に説明する。

[0015] ボディECU9は、車載電装品の電源を管理する。例えば、ボディECU9は、車両ドアの施解錠を切り替えるドアロック装置6を制御する。また、エンジンECU10は、エンジン7を制御する。照合ECU8、ボディECU9、及び、エンジンECU10の間は、車両1の内部の通信線11を介して接続されている。通信線11を介した通信におけるプロトコルは、例えばCAN (Controller Area Network) であってもよいし、LIN (Local Interconnect Network) であってもよい。

[0016] LF送信機13は、車両1と端末2とのスマート照合の通信実行に際して、端末2へLF帯の電波を送信する。また、端末2によってLF帯の電波が受信され、端末2によってUHF帯の電波が送信されると、UHF受信機14は、端末2から送信されたUHF帯の電波を受信する。なお、LF送信機13は、例えば車両1の室外に位置する端末2に電波を送信する室外用のLF送信機と、車両1の室内に位置する端末2に電波を送信する室内用のLF送信機とを備えることが好ましい。通信機31については、後に詳細に説明する。

[0017] (端末の各構成)

続いて、端末2の各構成について説明する。端末2は、端末制御部20と、LF受信部21と、UHF送信部22と、UWB (Ultra Wide Band) 送受信部33とを備える。端末制御部20は、端末2を制御する。端末制御部20は、不揮発性メモリ23を備える。端末制御部20の不揮発性メモリ23には、端末2に固有のキーIDと、キー固有鍵とが登録されている。キーID及びキー固有鍵は、スマート照合に使用される。

[0018] LF受信部21は、車両1と端末2とのスマート照合の通信実行に際して

、車両 1 から送信された L F 電波を受信する。L F 受信部 2 1 によって車両 1 から送信された L F 電波が受信されると、U H F 送信部 2 2 は、車両 1 へ U H F 電波を送信する。U W B 送受信部 3 3 については、後に詳細に説明する。

[0019] (スマート照合)

続いて、スマート照合の流れを説明する。まず、車両 1 の L F 送信機 1 3 は、定期又は不定期にウェイク信号を L F 送信する。端末 2 は、L F 受信部 2 1 によってウェイク信号を受信すると、待機状態から起動し、U H F 送信部 2 2 によってアック信号を U H F 送信する。照合 E C U 8 は、U H F 受信機 1 4 によってウェイク信号に対するアック信号を端末 2 から受信すると、認証部 4 8 によってスマート照合を開始する。このとき、照合 E C U 8 の認証部 4 8 は、室外の端末 2 が室外用の L F 送信機 1 3 のウェイク信号を受信した場合には、室外の端末 2 と車両 1 との間の室外スマート照合を実行する。一方、照合 E C U 8 の認証部 4 8 は、室内の端末 2 が室内用の L F 送信機 1 3 のウェイク信号を受信した場合には、室内の端末 2 との間の室内スマート照合を実行する。

[0020] ここで、スマート照合には、端末 2 に登録されたキー I D とあらかじめ車両 1 に登録されたキー I D との一致を確認するキー I D 照合が含まれてもよいし、キー固有鍵を用いた要求応答認証が含まれてもよい。要求応答認証は、乱数である要求コードに対してキー固有鍵を使用した応答コードを車両 1 及び端末 2 の双方に演算させ、これら応答コードの一致を確認する認証である。本例では、照合 E C U 8 の認証部 4 8 が、キー I D 照合及び要求応答認証の両方が成立する場合、スマート照合を成立とする場合を主に想定する。

[0021] (距離測定システム)

図 1 に示すように、本実施形態に係る通信システムは、距離測定システム 3 0 を備える。以下、距離測定システム 3 0 について説明する。なお、距離測定システム 3 0 は、直接的には車両 1 及び端末 2 の間の距離に準じた測定値 V_m を測定する。しかし、説明を簡便にするため、以下では、距離測定シ

システム 30 が車両 1 及び端末 2 の間の距離を測定すると表現する場合もある。

[0022] ここで、車両 1 と端末 2 とが遠く離れている場合には、車両 1 と端末 2 との間の通信接続がされないため、スマート照合が成立しないのが通例である。しかし、車両 1 から遠く離れた端末 2 を中継器などにより車両 1 に通信接続してスマート照合を成立させてしまう不正行為がなされる場合がある。かかる不正行為への対策のため、距離測定システム 30 は、車両 1 及び端末 2 の間の距離に準じた測定値 V_m を測定する機能を備え、測定値 V_m の正当性からスマート照合の成立可否を決定する機能（不正通信検出機能）を備える。

[0023] 距離測定システム 30 は、端末 2 が備える、UWB 送受信部 33 と、車両 1 が備える、通信機 31 とによって主に実現される。UWB 送受信部 33 は、通信機 31 との間で距離測定のための通信を実行する。また、通信機 31 は、端末 2 との間で距離測定のための通信を実行する。本例では、車両 1 が複数の通信機 31（特に、マスタ通信機 34 とスレーブ通信機 35）を備える場合を主に想定する。しかし、車両 1 が備える通信機 31 の数は限定されない。

[0024] 本例では、マスタ通信機 34 は、通信線 36 を介して照合 ECU 8 に接続されている。スレーブ通信機 35 は、通信線 37 を介してマスタ通信機 34 と接続されている。通信線 36 及び通信線 37 を介して通信における通信プロトコルは、例えば LIN であってもよいし、CAN であってもよい。なお、通信線 36 には、UART (Universal Asynchronous Receiver Transmitter) などの通信インターフェースが用いられていてもよい。

[0025] マスタ通信機 34 は、通信制御部 38 と、インターフェース部 39 と、揮発性メモリ 40 b と、不揮発性メモリ 41 b と、取得部 42 b と、第 2 通信部 43 b と、更新部 44 b と、測定部 45 b とを備える。インターフェース部 39 は、照合 ECU 8 及びスレーブ通信機 35 それぞれと通信可能なインターフェースである。例えば、インターフェース部 39 は、スレーブ通信機

35に対して作動信号を出力する。通信制御部38は、スレーブ通信機35の作動を制御する。通信制御部38は、スレーブ通信機35が複数存在する場合などには、複数のスレーブ通信機35の作動順を設定したり、複数のスレーブ通信機35の一部を選択的に作動させたりする。揮発性メモリ40b、不揮発性メモリ41b、取得部42b、第2通信部43b、更新部44b及び測定部45bについては、後に詳細に説明する。

[0026] スレーブ通信機35は、揮発性メモリ40aと、不揮発性メモリ41aと、取得部42aと、第1通信部43aと、更新部44aと、測定部45aとを備える。揮発性メモリ40a、不揮発性メモリ41a、取得部42a、第1通信部43a、更新部44a及び測定部45aについては、後に詳細に説明する。

[0027] ここで、図2を参照しながら、通信機31の設置の一例について説明する。図2に示した例では、車両1の5箇所に通信機31が設置されている。通信機31のうち、マスタ通信機34は、車両1の室内に配置されることにより、車室内に測距用電波を送信する。測距用電波については、後に説明する。第1スレーブ通信機35aは、車両1の運転席前側の隅に配置されることにより、車両1前方及び運転席側に測距用電波を送信する。第2スレーブ通信機35bは、車両1の助手席前側の隅に配置されることにより、車両1前方及び助手席側に測距用電波を送信する。

[0028] 第3スレーブ通信機35cは、車両1の運転席後側の隅に配置されることにより、車両1後方及び運転席側に測距用電波を送信する。第4スレーブ通信機35dは、車両1の助手席後側の隅に配置されることにより、車両1後方及び助手席側に測距用電波を送信する。ただし、通信機31の設置は、かかる例に限定されない。

[0029] 図1に戻って説明を続ける。スレーブ通信機35の不揮発性メモリ41a、及び、マスタ通信機34の不揮発性メモリ41bは、第1暗号鍵をそれぞれ記憶している。すなわち、スレーブ通信機35が使用する第1暗号鍵と、マスタ通信機34が使用する第1暗号鍵とは、共通する暗号鍵である。さら

に、マスタ通信機 3 4 の不揮発性メモリ 4 1 b、及び、照合 E C U 8 の不揮発性メモリ 1 6 は、第 2 暗号鍵をそれぞれ記憶している。すなわち、マスタ通信機 3 4 が使用する第 2 暗号鍵と、照合 E C U 8 が使用する第 2 暗号鍵とは、共通する暗号鍵である。

[0030] 本例では、スレーブ通信機 3 5 の不揮発性メモリ 4 1 a、及び、マスタ通信機 3 4 の不揮発性メモリ 4 1 b それぞれが記憶する第 1 暗号鍵と、マスタ通信機 3 4 の不揮発性メモリ 4 1 b、及び、照合 E C U 8 の不揮発性メモリ 1 6 それぞれが記憶する第 2 暗号鍵とが、異なる場合を主に想定する。しかし、当該第 1 暗号鍵と、当該第 2 暗号鍵とは、同一であってもよい。なお、当該第 1 暗号鍵及び当該第 2 暗号鍵それぞれがどのように使用されるかは、後に詳細に説明する。

[0031] (距離測定のための通信)

続いて、距離測定のための通信および測定値の判定結果の通知について説明する。例えば、照合 E C U 8 から距離測定要求が出力されると、マスタ通信機 3 4 のインターフェース部 3 9 は、照合 E C U 8 から距離測定要求の入力を受け付ける。インターフェース部 3 9 によって距離測定要求の入力を受け付けられると、通信制御部 3 8 は、インターフェース部 3 9 を介して距離測定要求をスレーブ通信機 3 5 に出力する。なお、照合 E C U 8 から距離測定要求が出力されるタイミングは、スマート通信が確立したとき（例えば、車両 1 から送信されたウェイク信号に対し、端末 2 からのアック信号を車両 1 が受信したとき）であってもよいし、室外スマート照合又は室内スマート照合が成立したときであってもよい。

[0032] 通信機 3 1（マスタ通信機 3 4 及びスレーブ通信機 3 5）は、距離測定要求の入力を受け付けると、端末 2 との間で距離測定のための通信をそれぞれ開始する。

[0033] 続いて、距離測定のための通信について説明する。なお、本例では、距離測定のための通信に使用される電波（測距用電波及びその応答電波）が UWB 帯の電波を使用して行われる場合を主に想定する。そこで、以下では、距

離測定のための通信に使用される電波を「UWB電波S a」と記載する場合がある。しかし、距離測定のための通信に使用される電波は、UWB帯の電波に限定されない。

[0034] まず、距離測定のための通信においては、通信機3 1（すなわち、マスタ通信機3 4及びスレーブ通信機3 5）は、UWB電波S aを送信する。端末2のUWB送受信部3 3は、通信機3 1からUWB電波S aを受信すると、その応答としてUWB電波S aを返信する。そして、通信機3 1は、端末2から送信されたUWB電波S aを受信する。このとき、通信機3 1の測定部4 5（すなわち、マスタ通信機3 4の測定部4 5 b及びスレーブ通信機3 5の測定部4 5 a）は、通信機3 1及び端末2の間の距離に準じた測定値V m（距離に相当する測距値）を測定する。

[0035] より具体的には、通信機3 1の測定部4 5は、UWB電波S aの送信からその応答であるUWB電波S aの受信までの伝搬時間を計算し、この伝搬時間から通信機3 1及び端末2の間の距離に準じた測定値V m（距離に相当する測距値）を算出する。また、測定部4 5は、測定値V mが正当であるか否かを判定する。測定値V mが正当であるか否かは、例えば測定値V mが規定値V k未満であるか否かによって判定される。

[0036] （暗号鍵の更新）

上記のように、通信機3 1は、端末2との間で距離測定のための通信（第1通信）を行う。そして、通信機3 1は、距離測定のための通信の結果として測定値V mを得る。通信機3 1は、測定値V mが正当であるか否かを示す判定結果を得る。通信機3 1は、判定結果を、通信線を介した通信（第2通信）により照合E C U 8に送信する。例えば、スレーブ通信機3 5は、通信線3 7、マスタ通信機3 4及び通信線3 6を介して、判定結果を照合E C U 8に送信する。また、マスタ通信機3 4は、通信線3 6を介して、判定結果を照合E C U 8に送信する。なお、距離測定のための通信と通信線を介した通信とは、通信機3 1との通信相手が異なる。

[0037] 照合E C U 8は、通信線を介した通信により通信機3 1から判定結果を受

信する。照合E C U 8においては、判定結果に応じてスマート照合の照合結果を有効又は無効にする。

[0038] このとき、通信機3 1は、判定結果をそのまま照合E C U 8に送信するのではなく、判定結果を処理することによって通信データを生成し、通信データを照合E C U 8に送信する場合が想定される。かかる場合には、通信機3 1において結果が導き出されてから通信データが生成されると、通信データの送信が完了するまでに時間が掛かってしまう。そこで、本実施形態では、通信機3 1は、端末2との通信が完了してから、通信結果に対応する通信データを照合E C U 8に送信するまでのタイミングを早期化する。

[0039] なお、端末2は、通信機3 1と通信（第1通信）を行う外部機器の一例であり、距離測定のための通信は、通信機3 1と外部機器との間で行われる通信（第1通信）の一例であり、測定値V mは、通信機3 1と外部機器との間で行われる通信（第1通信）の結果の一例である。したがって、通信機3 1と通信（第1通信）を行う外部機器は、端末2に限定されないし、通信機3 1と外部機器との間で行われる通信（第1通信）は、距離測定のための通信に限定されないし、通信機3 1と外部機器との間で行われる通信（第1通信）の結果は、測定値V mに限定されない。

[0040] また、測定値V mが正当であるか否かを示す判定結果は、通信機3 1と外部機器との間で行われる通信（第1通信）の結果に対応する通信データの一例である。したがって、通信機3 1と外部機器との間で行われる通信（第1通信）の結果に対応する通信データは、測定値V mが正当であるか否かを示す判定結果に限定されない。例えば、通信機3 1と外部機器との間で行われる通信（第1通信）の結果に対応する通信データは、通信機3 1と外部機器との間で行われる通信（第1通信）に基づく何らかの判定結果（例えば、正常判定を示す結果または異常判定を示す結果など）であってもよい。

[0041] 照合E C U 8は、通信機3 1との間で通信線を介した通信（第2通信）を行う制御装置の一例であり、通信線を介した通信は、通信機3 1と制御装置との間で行われる通信（第2通信）の一例である。したがって、通信機3 1

との間で通信線を介した通信（第2通信）を行う制御装置は、照合E C U 8に限定されないし、通信機31と制御装置との間で行われる通信（第2通信）は、通信線を介した通信に限定されない。また、本例では、判定結果に対する処理の例として暗号鍵を用いた暗号化を想定する。しかし、判定結果に対する処理は、暗号鍵を用いた暗号化に限定されない。

[0042] 照合E C U 8の更新制御部47は、所定条件（以下、「鍵生成条件」とも言う。）が満たされた場合に、乱数 α 及び乱数 β を生成し、乱数 β を照合E C U 8の更新部44cに出力するとともに、乱数 α 及び乱数 β を、通信線36を介してマスタ通信機34に送信する。これによって、鍵生成条件が初めて満たされた場合には、乱数が初めて生成される。鍵生成条件が2回目以降に満たされた場合には、乱数が更新される。マスタ通信機34のインターフェース部39は、照合E C U 8から通信線36を介して乱数 α 及び乱数 β を受信すると、乱数 α 及び乱数 β を更新部44bに出力するとともに、通信線37を介して乱数 α をスレーブ通信機35に送信する。

[0043] スレーブ通信機35の更新部44aは、マスタ通信機34から通信線37を介して乱数 α が受信されると、乱数 α と第1暗号鍵とに基づいて第1暗号選択解を生成する。より詳細に、スレーブ通信機35の更新部44aは、第1暗号鍵を用いて乱数 α を暗号化することによって第1暗号選択解を生成する。ここでの乱数 α は、第1選択解に相当し得る。そして、更新部44aは、第1暗号選択解を初めて生成した場合には、生成した第1暗号選択解を揮発性メモリ40aに記憶させる。一方、更新部44aは、第1暗号選択解を2回目以降に生成した場合には、生成した第1暗号選択解によって揮発性メモリ40aに記憶されている第1暗号選択解を更新する。かかる構成によれば、第1暗号選択解のセキュリティ性が向上する。

[0044] 図1には、スレーブ通信機35の揮発性メモリ40aに記憶されている第1暗号選択解が示されている。ここで、第1暗号選択解の数は限定されないが、少なくとも判定結果の種類に対応する数の第1暗号選択解が揮発性メモリ40aに記憶される。本例では、判定結果が2種類であるため、2つの第

1 暗号選択解が揮発性メモリ 40 a に記憶される。すなわち、更新部 44 a は、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解、及び、測定値 V_m が正当ではないことを示す判定結果に対応する第 1 暗号選択解を、揮発性メモリ 40 a に記憶させる。判定結果は、1 種類であってもよいし、3 種類以上であってもよい。

[0045] マスタ通信機 34 の更新部 44 b は、インターフェース部 39 から乱数 α が入力されると、乱数 α と第 1 暗号鍵とに基づいて第 1 暗号照合解を生成する。より詳細に、マスタ通信機 34 の更新部 44 b は、第 1 暗号鍵を用いて乱数 α を暗号化することによって第 1 暗号照合解を生成する。ここでの乱数 α は、第 1 照合解に相当し得る。そして、更新部 44 b は、第 1 暗号照合解を初めて生成した場合には、生成した第 1 暗号照合解を揮発性メモリ 40 b に記憶させる。一方、更新部 44 b は、第 1 暗号照合解を 2 回目以降に生成した場合には、生成した第 1 暗号照合解によって揮発性メモリ 40 b に記憶されている第 1 暗号照合解を更新する。かかる構成によれば、第 1 暗号照合解のセキュリティ性が向上する。

[0046] 図 1 には、マスタ通信機 34 の揮発性メモリ 40 b に記憶されている第 1 暗号照合解が示されている。ここで、第 1 暗号照合解の数は限定されないが、少なくとも判定結果の種類に対応する数の第 1 暗号照合解が揮発性メモリ 40 b に記憶される。本例では、判定結果が 2 種類であるため、2 つの第 1 暗号照合解が揮発性メモリ 40 b に記憶される。すなわち、更新部 44 b は、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号照合解、及び、測定値 V_m が正当ではないことを示す判定結果に対応する第 1 暗号照合解を、揮発性メモリ 40 b に記憶させる。

[0047] また、マスタ通信機 34 の更新部 44 b は、インターフェース部 39 から乱数 β が入力されると、乱数 β と第 2 暗号鍵とに基づいて第 2 暗号選択解を生成する。より詳細に、マスタ通信機 34 の更新部 44 b は、第 2 暗号鍵を用いて乱数 β を暗号化することによって第 2 暗号選択解を生成する。ここでの乱数 β は、第 2 選択解に相当し得る。そして、更新部 44 b は、第 2 暗号

選択解を初めて生成した場合には、生成した第2暗号選択解を揮発性メモリ40bに記憶させる。一方、更新部44bは、第2暗号選択解を2回目以降に生成した場合には、生成した第2暗号選択解によって揮発性メモリ40bに記憶されている第2暗号選択解を更新する。かかる構成によれば、第2暗号選択解のセキュリティ性が向上する。

[0048] 図1には、マスタ通信機34の揮発性メモリ40bに記憶されている第2暗号選択解が示されている。ここで、第2暗号選択解の数は限定されないが、少なくとも判定結果の種類に対応する数の第2暗号選択解が揮発性メモリ40bに記憶される。本例では、判定結果が2種類であるため、2つの第2暗号選択解が揮発性メモリ40bに記憶される。すなわち、更新部44bは、測定値 V_m が正当であることを示す判定結果に対応する第2暗号選択解、及び、測定値 V_m が正当ではないことを示す判定結果に対応する第2暗号選択解を、揮発性メモリ40bに記憶させる。

[0049] 照合ECU8の更新部44cは、更新制御部47から乱数 β が入力されると、乱数 β と第2暗号鍵とに基づいて第2暗号照合解を生成する。より詳細に、照合ECU8の更新部44cは、第2暗号鍵を用いて乱数 β を暗号化することによって第2暗号照合解を生成する。ここでの乱数 β は、第2照合解に相当し得る。そして、更新部44cは、第2暗号照合解を初めて生成した場合には、生成した第2暗号照合解を揮発性メモリ15に記憶させる。一方、更新部44cは、第2暗号照合解を2回目以降に生成した場合には、生成した第2暗号照合解によって揮発性メモリ15に記憶されている第2暗号照合解を更新する。かかる構成によれば、第2暗号照合解のセキュリティ性が向上する。

[0050] 図1には、照合ECU8の揮発性メモリ15に記憶されている第2暗号照合解が示されている。ここで、第1暗号選択解の数は限定されないが、少なくとも判定結果の種類に対応する数の第2暗号照合解が揮発性メモリ15に記憶される。本例では、判定結果が2種類であるため、2つの第2暗号照合解が揮発性メモリ15に記憶される。すなわち、更新部44cは、測定値 V

mが正当であることを示す判定結果に対応する第2暗号照合解、及び、測定値 V_m が正当ではないことを示す判定結果に対応する第2暗号照合解を、揮発性メモリ15に記憶させる。

[0051] なお、解生成条件は、距離測定要求が照合ECU8から出力されるタイミングと同様に、スマート通信が確立したという条件（例えば、車両1から送信されたウェイク信号に対し、端末2からのアック信号を車両1が受信したという条件）であってもよいし、室外スマート照合又は室内スマート照合が成立したという条件であってもよい。すなわち、解生成条件は、端末2の認証のための通信が確立したという条件であってもよいし、端末2の認証の一部が成立したという条件であってもよい。

[0052] かかる構成によれば、端末2の認証が行われるたびに暗号選択解が更新されれば、暗号選択解のセキュリティ性が向上する。特に、端末2の認証が行われるときに距離測定のための通信が行われ、測定値 V_m が正当であるか否かが判定され、判定結果に対応する暗号選択解が照合ECU8に送信されるよう構成されている場合が想定される。かかる場合に、端末2の認証が行われるたびに暗号選択解が更新されれば、暗号選択解が照合ECU8に送信されるたびに暗号選択解が更新されることとなるため、暗号選択解のセキュリティ性がより向上する。

[0053] 本例では、解生成条件が、端末2の認証のための通信が確立したという条件である場合、かつ、照合ECU8からマスタ通信機34に対して出力される距離測定要求に、乱数 α 及び乱数 β が付される場合を主に想定する。しかし、距離測定要求に乱数 α 及び乱数 β が付されていなくてもよく、距離測定要求と乱数 α 及び乱数 β とは、別々に照合ECU8からマスタ通信機34に対して出力されてもよい。

[0054] 解生成条件は、かかる例に限定されない。例えば、解生成条件は、所定時間が経過したという条件を含んでもよい。かかる構成によれば、所定時間が経過した後も同じ暗号鍵が使用されてしまうことがなくなるため、暗号選択解のセキュリティ性が向上することが期待される。所定時間は、1度だけ到

来する時間であってもよいし、複数回到来する時間であってもよい。また、複数回到来する時間は、定期的に複数回到来する時間であってもよい。

[0055] あるいは、解生成条件は、端末2と通信機31との間で行われた共通の暗号鍵を使用した通信（暗号通信）の回数が所定回数に達したという条件を含んでもよい。かかる構成によれば、暗号通信の回数が所定回数に達した後も同じ暗号鍵が使用されてしまうことがなくなるため、暗号選択解のセキュリティ性が向上することが期待される。なお、端末2と通信機31との間で行われた暗号通信の回数は、例えば、端末2及び通信機31それぞれから照合ECU8に通知され、照合ECU8によって管理されていればよい。

[0056] また、本例では、更新制御部47によって乱数が生成される場合を想定する。しかし、更新制御部47によって生成されるデータは、乱数に限定されない。例えば、更新制御部47によって生成されるデータは、規則的に変化するデータであってもよい。すなわち、更新制御部47によって生成されるデータは、時間の経過とともに変化する情報であればよく、より望ましくは出力されるたびに変化する情報であるのがよい。また、本例では、セキュリティ性を向上させるため、乱数 α と乱数 β とが異なる値である場合を主に想定する。しかし、乱数 α と乱数 β とは同一の値であってもよい。

[0057] 以上のように、第1暗号選択解及び第1暗号照合解は、第1暗号鍵を用いた共通鍵暗号方式による暗号化に基づいて生成される。かかる構成によれば、通信の秘匿性が向上する。また、第1暗号鍵による暗号化の対象である第1選択解及び第1照合解が同じ値（上記例では、第1選択解及び第1照合解が共に乱数 α ）であれば、第1暗号選択解及び第1暗号照合解は、同じ値として生成される。かかる構成によれば、第1暗号選択解及び第1暗号照合解との照合は、双方が一致するか否かに基づいて容易に判定され得る。しかし、第1暗号選択解及び第1暗号照合解は、同じ値として生成されなくてもよく、第1暗号選択解及び第1暗号照合解の対応関係が把握されていれば、かかる対応関係に基づいて、第1暗号選択解及び第1暗号照合解との照合が行われ得る。

[0058] 同様に、第2暗号選択解及び第2暗号照合解は、第2暗号鍵を用いた共通鍵暗号方式による暗号化に基づいて生成される。かかる構成によれば、通信の秘匿性が向上する。また、また、第2暗号鍵による暗号化の対象である第2選択解及び第2照合解が同じ値（上記例では、第2選択解及び第2照合解が共に乱数 β ）であれば、第2暗号選択解及び第2暗号照合解は、同じ値として生成される。かかる構成によれば、第2暗号選択解及び第2暗号照合解との照合は、双方が一致するか否かに基づいて容易に判定され得る。しかし、第2暗号選択解及び第2暗号照合解は、同じ値として生成されなくてもよく、第2暗号選択解及び第2暗号照合解の対応関係が把握されていれば、かかる対応関係に基づいて、第2暗号選択解及び第2暗号照合解との照合が行われ得る。

[0059] （判定結果の通知）

通信機31は、測定値 V_m が正当であるか否かを示す判定結果に応じて選択された暗号選択解を照合ECU8に送信する。そして、照合ECU8は、通信機31から送信された暗号選択解を受信する。かかる構成によれば、通信機31と端末2との間の距離測定のための通信が完了する前から、判定結果に対応する暗号選択解が用意されている。したがって、かかる構成によれば、距離測定のための通信が完了してから、判定結果に対応する暗号選択解を照合ECU8へ出力するまでのタイミングを早期化することが可能となる。

[0060] 照合ECU8の照合部46は、受信した暗号選択解と当該暗号選択解に対応して用意された暗号照合解とを照合する。かかる構成によれば、受信した暗号選択解に対応する暗号照合解があらかじめ用意されている。したがって、かかる構成によれば、暗号選択解を受信してから、当該暗号選択解に適合する暗号照合解を得て当該暗号照合解に対応する判定結果を得るタイミングを早期化することが可能となる。

[0061] 本例では、スレーブ通信機35、及び、マスタ通信機34の双方によって、測定値 V_m が正当であるか否かを示す判定結果が送信される。

- [0062] まず、スレーブ通信機 3 5 の取得部 4 2 a は、測定部 4 5 a によって得られた判定結果に対応する第 1 暗号選択解を揮発性メモリ 4 0 a から取得し、第 1 通信部 4 3 a は、取得部 4 2 a によって取得された第 1 暗号選択解を、通信線 3 7 を介してマスタ通信機 3 4 に送信する。かかる構成によれば、判定結果に対応する第 1 暗号選択解があらかじめ用意されているため、判定結果が得られてから、当該判定結果に対応する第 1 暗号選択解を送信するまでの時間が短縮され得る。
- [0063] より詳細に、取得部 4 2 a は、測定部 4 5 a によって測定値 V_m が正当であることを示す判定結果が得られた場合、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解を揮発性メモリ 4 0 a から取得し、第 1 通信部 4 3 a は、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解を、通信線 3 7 を介してマスタ通信機 3 4 に送信する。かかる構成によれば、後にも説明するように、照合 ECU 8 によって測定値 V_m が正当であることを示す判定結果が得られる。
- [0064] 一方、取得部 4 2 a は、測定部 4 5 a によって測定値 V_m が正当ではないことを示す判定結果が得られた場合、測定値 V_m が正当ではないことを示す判定結果に対応する第 1 暗号選択解を揮発性メモリ 4 0 a から取得し、第 1 通信部 4 3 a は、測定値 V_m が正当ではないことを示す判定結果に対応する第 1 暗号選択解を、通信線 3 7 を介してマスタ通信機 3 4 に送信する。かかる構成によれば、後にも説明するように、照合 ECU 8 によって測定値 V_m が正当ではないことを示す判定結果が得られる。
- [0065] マスタ通信機 3 4 の取得部 4 2 b は、第 2 通信部 4 3 b によってスレーブ通信機 3 5 から通信線 3 7 を介して第 1 暗号選択解が受信されると、第 2 通信部 4 3 b によって受信された第 1 暗号選択解と揮発性メモリ 4 0 b に記憶された第 1 暗号照合解とを照合する。かかる構成によれば、第 1 暗号照合解があらかじめ用意されているため、第 1 暗号選択解を受信してから、当該第 1 暗号選択解に対応する第 1 暗号選択解を得るまでの時間が短縮され得る。
- [0066] 第 2 通信部 4 3 b は、取得部 4 2 b によって第 1 暗号選択解と適合する第

1 暗号照合解が揮発性メモリ 40b から取得された場合、取得部 42b によって取得された第 1 暗号照合解に対応する第 2 暗号選択解を、通信線 36 を介して照合 ECU8 に送信する。かかる構成によれば、第 1 暗号照合解に対応する第 2 暗号選択解があらかじめ用意されているため、第 1 暗号照合解を受信してから、当該第 1 暗号照合解に対応する第 2 暗号選択解を送信するまでの時間が短縮され得る。

[0067] より詳細に、第 2 通信部 43b は、取得部 42b によって第 1 暗号選択解と適合する第 1 暗号照合解として、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号照合解が揮発性メモリ 40b から取得された場合、測定値 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解を、通信線 36 を介して照合 ECU8 に送信する。かかる構成によれば、後にも説明するように、照合 ECU8 によって測定値 V_m が正当であることを示す判定結果が得られる。

[0068] 一方、第 2 通信部 43b は、取得部 42b によって第 1 暗号選択解と適合する第 1 暗号照合解として、測定値 V_m が正当ではないことを示す判定結果に対応する第 1 暗号照合解が揮発性メモリ 40b から取得された場合、測定値 V_m が正当ではないことを示す判定結果に対応する第 2 暗号選択解を、通信線 36 を介して照合 ECU8 に送信する。かかる構成によれば、後にも説明するように、照合 ECU8 によって測定値 V_m が正当ではないことを示す判定結果が得られる。

[0069] なお、第 2 通信部 43b によって受信された第 1 暗号選択解に適合する第 1 暗号照合解が取得部 42b によって揮発性メモリ 40b から取得されない場合も想定される。かかる場合には、第 2 通信部 43b は、通信線 36 を介して照合 ECU8 に対して何も送信しなくてもよい。あるいは、通信部 43b は、第 1 暗号照合解が取得されないことを示す情報を、通信線 36 を介して照合 ECU8 に対して送信してもよい。これによって、照合 ECU8 の受信部 49 によって第 1 暗号照合解が取得されないことを示す情報が受信されれば、照合 ECU8 の照合部 46 は、マスタ通信機 34 から第 2 暗号照合解

が受信されない状況が生じて、その状況がマスタ通信機 34 において第 1 暗号照合解が取得されないことが理由で生じたことを把握することができる。

[0070] さらに、マスタ通信機 34 の取得部 42b は、測定部 45b によって得られた判定結果に対応する第 2 暗号選択解を揮発性メモリ 40b から取得し、第 2 通信部 43b は、取得部 42b によって取得された第 2 暗号選択解を、通信線 36 を介して照合 ECU 8 に送信する。かかる構成によれば、判定結果に対応する第 2 暗号選択解があらかじめ用意されているため、判定結果が得られてから、当該判定結果に対応する第 2 暗号選択解を送信するまでの時間が短縮され得る。

[0071] より詳細に、取得部 42b は、測定部 45b によって測定値 V_m が正当であることを示す判定結果が得られた場合、測定値 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解を揮発性メモリ 40b から取得し、第 2 通信部 43b は、測定値 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解を、通信線 36 を介して照合 ECU 8 に送信する。かかる構成によれば、後にも説明するように、照合 ECU 8 によって測定値 V_m が正当であることを示す判定結果が得られる。

[0072] 一方、取得部 42b は、測定部 45b によって測定値 V_m が正当ではないことを示す判定結果が得られた場合、測定値 V_m が正当ではないことを示す判定結果に対応する第 2 暗号選択解を揮発性メモリ 40b から取得し、第 2 通信部 43b は、測定値 V_m が正当ではないことを示す判定結果に対応する第 2 暗号選択解を、通信線 36 を介して照合 ECU 8 に送信する。かかる構成によれば、後にも説明するように、照合 ECU 8 によって測定値 V_m が正当ではないことを示す判定結果が得られる。

[0073] 照合 ECU 8 の照合部 46 は、受信部 49 によってマスタ通信機 34 から通信線 36 を介して第 2 暗号選択解が受信された場合、受信部 49 によって受信された第 2 暗号選択解と揮発性メモリ 15 に記憶された第 2 暗号照合解とを照合する。かかる構成によれば、受信部 49 によって受信された第 2 暗

号選択解に対応する第2暗号照合解があらかじめ用意されている。したがって、かかる構成によれば、受信部49によって第2暗号選択解が受信されてから、当該第2暗号選択解に適合する第2暗号照合解を得て当該第2暗号照合解に対応する判定結果を得るタイミングを早期化することが可能となる。

[0074] 処理実行部17は、照合部46によって第2暗号選択解と適合する第2暗号照合解を揮発性メモリ15から取得した場合、取得した第2暗号照合解に対応する判定結果を得る。より詳細に、処理実行部17は、第2暗号選択解と適合する第2暗号照合解として、測定値 V_m が正当であることを示す判定結果に対応する第2暗号照合解を揮発性メモリ15から取得した場合、測定値 V_m が正当であることを示す判定結果を得る。一方、処理実行部17は、第2暗号選択解と適合する第2暗号照合解として、測定値 V_m が正当ではないことを示す判定結果に対応する第2暗号照合解を揮発性メモリ15から取得した場合、測定値 V_m が正当ではないことを示す判定結果を得る。

[0075] なお、照合部46によって第2暗号選択解と適合する第2暗号照合解が揮発性メモリ15から取得されない場合も想定される。かかる場合には、処理実行部17は、測定値 V_m が正当ではないことを示す判定結果を得ればよい（測定値 V_m が正当ではないと判定すればよい）。

[0076] 処理実行部17は、測定値 V_m が正当か否かを示す判定結果に基づいて、スマート照合の成立可否を決定する。例えば、処理実行部17は、少なくとも一つの通信機31から測定値 V_m が正当であることを示す判定結果が入力された場合、スマート照合の成立を有効にする。一方、処理実行部17は、いずれの通信機31からも測定値 V_m が正当であることを示す判定結果が入力されない場合、スマート照合の成立を無効にする。照合ECU8は、スマート照合の成立が有効にされた場合に、車載装置3の作動を許可又は実行する。

[0077] <<1. 2. 動作例>>

次に、図3及び図4を用いて、本実施形態の距離測定システム30の作用について説明する。

[0078] 図3に示すように、ステップS101において、照合ECU8は、マスタ通信機34へ距離測定要求を送信する。また、更新制御部47は、乱数 α 、 β を生成し、距離測定要求とともに乱数 α 、 β をマスタ通信機34へ送信する。このとき、更新部44cは、乱数 β 及び第2暗号鍵を用いて第2暗号照合解を更新する。上記したように、距離測定要求及び乱数 α 、 β は、例えばスマート通信が確立したとき（例えば、車両1から送信されたウェイク信号に対し、端末2からのアック信号を車両1が受信したとき）に送信されてもよいし、室外スマート照合又は室内スマート照合が成立したときに送信されてもよい。スマート通信が確立したとは、例えば車両1から送信されたウェイク信号に対し、端末2からのアック信号を車両1が受信したことである。さらに、上記したように、距離測定要求と乱数 α 、 β とは、別のタイミングに送信されてもよい。

[0079] ステップS102において、マスタ通信機34のインターフェース部39は、距離測定要求及び乱数 α 、 β を受信すると、マスタ通信機34の更新部44bは、乱数 α 及び第1暗号鍵を用いて第1暗号照合解を更新し、乱数 β 及び第2暗号鍵を用いて第2暗号選択解を更新する。また、マスタ通信機34の通信制御部38は、スレーブ通信機35a～35dの作動順を設定し、作動順に従ってスレーブ通信機35a～35dに、距離測定要求及び乱数 α を通知する。このように、距離測定要求の通知のタイミングをスレーブ通信機35a～35dの間で異ならせることによって、スレーブ通信機35a～35dの作動タイミングを異ならせることができる。

[0080] スレーブ通信機35a～35dそれぞれの更新部44aは、距離測定要求及び乱数 α の通知を受けると、乱数 α 及び第1暗号鍵を用いて第1暗号選択解を更新する。これにより、第1暗号選択解、第1暗号照合解、第2暗号選択解及び第2暗号照合解が、今回の通信でのみ有効なユニークな値に更新される。

[0081] 本例では、マスタ通信機34によって使用される第1暗号鍵とスレーブ通信機35によって使用される第1暗号鍵とは、共通の暗号鍵である。すなわ

ち、第1暗号選択解及び第1暗号照合解は、共通鍵暗号方式で暗号化される。また、第1暗号選択解の元になるデータ（すなわち、第1選択解）と、第1暗号照合解の元になるデータ（すなわち、第1照合解）とが同じ値（本例では、乱数 α ）である場合、第1暗号選択解及び第1暗号照合解は同じ値となる。

[0082] 同様に、本例では、マスタ通信機34によって使用される第2暗号鍵と照合ECU8によって使用される第2暗号鍵とは、共通の暗号鍵である。すなわち、第2暗号選択解及び第2暗号照合解は、共通鍵暗号方式で暗号化される。また、第2暗号選択解の元になるデータ（すなわち、第2選択解）と、第2暗号照合解の元になるデータ（すなわち、第2照合解）とが同じ値（本例では、乱数 β ）である場合、第2暗号選択解及び第2暗号照合解は同じ値となる。

[0083] ステップS103において、スレーブ通信機35a～35dそれぞれは、距離測定要求及び乱数 α の通知を受けると（すなわち、自身の作動タイミングになると）、端末2からのUWB電波Saを受信し、これに対する応答のUWB電波Saを端末2へ送信する。端末2のUWB送受信部33は、スレーブ通信機35a～35dそれぞれからの応答を受信すると、さらにUWB電波Saを送信する。スレーブ通信機35a～35dそれぞれの測定部45aは、応答のUWB電波Saを送信してから再びUWB電波Saを受信するまでの時間を計測する。そして、スレーブ通信機35a～35dそれぞれの測定部45aは、計測した時間から、自身と端末2との間の距離に準じた測定値Vmを算出する。

[0084] スレーブ通信機35a～35dそれぞれの測定部45aは、算出した測定値Vmの正当性を判定する。スレーブ通信機35a～35dそれぞれの測定部45aは、測定値Vmが規定値Vk未満の場合、車両1及び端末2の間の距離が正当であると判定する。一方、スレーブ通信機35a～35dそれぞれの測定部45aは、測定値Vmが規定値Vk以上の場合、車両1及び端末2の間の距離が正当ではないと判定する。

- [0085] 一方、マスタ通信機34は、自身の作動タイミングになると、距離測定要求の通知を行わず、自身が端末2からのUWB電波S aを受信し、これに対する応答のUWB電波S aを端末2へ送信する。端末2のUWB送受信部33は、マスタ通信機34からの応答を受信すると、さらにUWB電波S aを送信する。マスタ通信機34の測定部45bは、応答のUWB電波S aを送信してから再びUWB電波S aを受信するまでの時間を計測する。そして、マスタ通信機34の測定部45bは、計測した時間から、自身と端末2との間の距離に準じた測定値V mを算出する。
- [0086] マスタ通信機34の測定部45bは、算出した測定値V mの正当性を判定する。マスタ通信機34の測定部45bは、測定値V mが規定値V k未満の場合、車両1及び端末2の間の距離が正当であると判定する。一方、マスタ通信機34の測定部45bは、測定値V mが規定値V k以上の場合、車両1及び端末2の間の距離が正当ではないと判定する。
- [0087] ステップS 104において、スレーブ通信機35a～35dそれぞれの第1通信部43aは、測定部45aによって測定値V mが正当であるか否かを示す判定結果が得られると、当該判定結果に対応する第1暗号選択解をマスタ通信機34へ通知する。
- [0088] ステップS 105において、マスタ通信機34の第2通信部43bは、スレーブ通信機35a～35dそれぞれから、測定値V mが正当であるか否かを示す判定結果が通知されると、スレーブ通信機35a～35dそれぞれから通知された判定結果に対応する第2暗号選択解を照合ECU8に通知する。さらに、マスタ通信機34の第2通信部43bは、測定部45bによって測定値V mが正当であるか否かを示す判定結果が得られると、測定部45bによって得られた判定結果に対応する第2暗号選択解を照合ECU8に通知する。
- [0089] 続いて、図4(a)及び図4(b)を用いて、判定結果の通知の仕方について説明する。
- [0090] 図4(a)に示すように、スレーブ通信機35の測定部45aによって、

測定値 V_m が正当であると判定された場合、スレーブ通信機 35 の取得部 42 a は、揮発性メモリ 40 a から測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解 A を取得する。第 1 通信部 43 a は、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解 A をマスタ通信機 34 へ送信する。

[0091] マスタ通信機 34 の揮発性メモリ 40 b は、測定値 V_m が正当であることを示す判定結果に対応する、第 1 暗号照合解 A' 及び第 2 暗号選択解 C を記憶している。照合部 46 によって、スレーブ通信機 35 から入力された、測定値 V_m が正当であることを示す判定結果に対応する第 1 暗号選択解 A と、揮発性メモリ 40 b に登録された第 1 暗号照合解 A' とが一致することが確認されると、第 2 通信部 43 b は、第 1 暗号照合解 A' に対応する第 2 暗号選択解 C を、照合 ECU 8 へ送信する。

[0092] 照合 ECU 8 の揮発性メモリ 15 は、測定値 V_m が正当であることを示す判定結果に対応する、第 2 暗号照合解 C' を記憶している。照合部 46 によって、マスタ通信機 34 から入力された、測定値 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解 C と、揮発性メモリ 15 に登録された第 2 暗号照合解 C' とが一致することが確認されると、処理実行部 17 は、第 2 暗号照合解 C' に対応する判定結果、すなわち、測定値 V_m が正当であることを示す判定結果を得る。

[0093] なお、マスタ通信機 34 の測定部 45 b によって測定値 V_m が正当であると判定された場合も同様に、マスタ通信機 34 の取得部 42 b は、測定値 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解 C を揮発性メモリ 40 b から取得する。そして、第 2 通信部 43 b は、第 2 暗号選択解 C を照合 ECU 8 へ送信する。これによって、照合 ECU 8 においては、測定値 V_m が正当であることを示す判定結果が認識される。

[0094] 図 4 (b) に示すように、スレーブ通信機 35 の測定部 45 a によって、測定値 V_m が正当ではないと判定された場合、スレーブ通信機 35 の取得部 42 a は、揮発性メモリ 40 a から測定値 V_m が正当ではないことを示す判

定結果に対応する第1暗号選択解Bを取得する。第1通信部43aは、測定値Vmが正当ではないことを示す判定結果に対応する第1暗号選択解Bをマスタ通信機34へ送信する。

[0095] マスタ通信機34の揮発性メモリ40bは、測定値Vmが正当ではないことを示す判定結果に対応する、第1暗号照合解B'及び第2暗号選択解Dを記憶している。照合部46によって、スレーブ通信機35から入力された、測定値Vmが正当ではないことを示す判定結果に対応する第1暗号選択解Bと、揮発性メモリ40bに登録された第1暗号照合解B'とが一致することが確認されると、第2通信部43bは、第1暗号照合解B'に対応する第2暗号選択解Dを照合ECU8へ送信する。

[0096] 照合ECU8の揮発性メモリ15は、測定値Vmが正当であることを示す判定結果に対応する、第2暗号照合解D'を記憶している。照合部46によって、マスタ通信機34から入力された、揮発性メモリ15に登録された測定値Vmが正当ではないことを示す判定結果に対応する第2暗号選択解Dと、揮発性メモリ15に登録された第2暗号照合解D'とが一致することが確認されると、処理実行部17は、第2暗号照合解D'に対応する判定結果、すなわち、測定値Vmが正当ではないことを示す判定結果を得る。

[0097] なお、マスタ通信機34の測定部45bによって測定値Vmが正当ではないと判定された場合も同様に、マスタ通信機34の取得部42bは、測定値Vmが正当ではないことを示す判定結果に対応する第2暗号選択解Dを揮発性メモリ40bから取得する。そして、第2通信部43bは、第2暗号選択解Dを照合ECU8へ送信する。これによって、照合ECU8においては、測定値Vmが正当ではないことを示す判定結果が認識される。

[0098] また、マスタ通信機34の取得部42bにスレーブ通信機35から入力された第1暗号選択解が、揮発性メモリ40bに登録された第1暗号照合解A'、B'のどちらとも一致しない場合も想定される。かかる場合には、上記したように、第2通信部43bは、第2暗号選択解C、Dのいずれも照合ECU8へ送信しなくてよく、取得部42bによって第1暗号照合解が取得さ

れないことを示す情報を照合E C U 8へ送信するとよい。

[0099] 図4(c)に具体的な例を示す。図4(c)に示したように、マスタ通信機34の取得部42bにスレーブ通信機35から入力された第1暗号選択解Eが、揮発性メモリ40bに登録された第1暗号照合解A'、B'のどちらとも一致しない場合(図4(c)では「暗号解不一致」)も想定される。かかる場合には、上記したように、第2通信部43bは、スレーブ通信機35における測定値V_mの判定結果として取得部42bによって第1暗号照合解が取得されないことを示す情報(図4(c)では「暗号解不一致」)を照合E C U 8へ送信する。

[0100] これによって、照合E C U 8においては、スレーブ通信機35における測定値V_mの判定結果に対応する第1暗号照合解が取得されないことが認識される。なお、スレーブ通信機35における測定値V_mの判定結果に対応する第1暗号照合解が取得されない理由として、スレーブ通信機35に対する不正行為が行われていることなどが想定される。

[0101] 図5は、照合E C U 8への通知と、マスタ通信機34における測定値V_mの判定結果と、スレーブ通信機35における測定値V_mの判定結果との対応関係の例をまとめた表である。図5に示した例において、「OK」は、測定値V_mが正当であることを示し、「NG」は、測定値V_mが正当ではないことを示す。「暗号解不一致」は、その通信機31での測定値V_mの判定結果に対応する第1暗号照合解または第2暗号選択解が取得されないことを示す。

[0102] 図5の1~4行目に示したように、マスタ通信機34の第2通信部43bは、1つに集約された第2暗号選択解を照合E C U 8に通知してもよい。すなわち、スレーブ通信機35a~35dそれぞれから通知された判定結果と、マスタ通信機34の測定部45bによって得られた判定結果との少なくともいずれかが一つが、測定V_mが正当であることを示す場合が想定される。かかる場合には、マスタ通信機34の第2通信部43bは、測定V_mが正当であることを示す判定結果に対応する第2暗号選択解Cを照合E C U 8に通知

してもよい。

[0103] したがって、マスタ通信機 3 4 の第 2 通信部 4 3 b は、マスタ通信機 3 4 の測定部 4 5 b によって測定 V_m が正当であることを示す判定結果が得られた場合には、スレーブ通信機 3 5 a ~ 3 5 d それぞれから通知された判定結果が得られるのを待たずして、測定 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解 C を照合 E C U 8 に通知してもよい。

[0104] 一方、スレーブ通信機 3 5 a ~ 3 5 d それぞれから通知された判定結果と、マスタ通信機 3 4 の測定部 4 5 b によって得られた判定結果との全部が、測定 V_m が正当ではないことを示す場合が想定される。かかる場合には、マスタ通信機 3 4 の第 2 通信部 4 3 b は、測定 V_m が正当ではないことを示す判定結果に対応する第 2 暗号選択解 D を照合 E C U 8 に通知してもよい。

[0105] また、図 5 の 5 ~ 7 行目には、第 2 暗号選択解に加えて「暗号解不一致」がマスタ通信機 3 4 から照合 E C U 8 に通知される例が示されている。

[0106] 例えば、スレーブ通信機 3 5 a ~ 3 5 d それぞれから通知された判定結果と、マスタ通信機 3 4 の測定部 4 5 b によって得られた判定結果とのうち、少なくともいずれかが一つが、測定 V_m が正当であることを示す場合、かつ、少なくともいずれかが一つに対応する第 1 暗号照合解または第 2 暗号選択解が取得されない場合が想定される。かかる場合には、マスタ通信機 3 4 の第 2 通信部 4 3 b は、測定 V_m が正当であることを示す判定結果に対応する第 2 暗号選択解 C と「暗号解不一致（すなわち、第 1 暗号照合解または第 2 暗号選択解が取得されないことを示す情報）」とを照合 E C U 8 に通知してもよい（図 5 の 5 ~ 6 行目）。

[0107] 例えば、図 5 の 5 行目に示したように、スレーブ通信機 3 5 a ~ 3 5 d それぞれから通知された判定結果の少なくともいずれかが一つに対応する第 1 暗号照合解または第 2 暗号選択解が取得されない場合、かつ、マスタ通信機 3 4 の測定部 4 5 b によって得られた判定結果が、測定 V_m が正当であることを示す場合が想定される。かかる場合には、マスタ通信機 3 4 の第 2 通信部 4 3 b は、測定 V_m が正当であることを示す判定結果に対応する第 2 暗号選

択解Cと「暗号解不一致（すなわち、第1暗号照合解または第2暗号選択解が取得されないことを示す情報）」とを照合ECU8に通知してもよい。

[0108] 例えば、図5の6行目に示したように、スレーブ通信機35a～35dそれぞれから通知された判定結果が、測定Vmが正当であることを示す場合、かつ、マスタ通信機34の測定部45bによって得られた判定結果に対応する第2暗号選択解が取得されない場合が想定される。かかる場合には、マスタ通信機34の第2通信部43bは、測定Vmが正当であることを示す判定結果に対応する第2暗号選択解Cと「暗号解不一致（すなわち、第1暗号照合解または第2暗号選択解が取得されないことを示す情報）」とを照合ECU8に通知してもよい。

[0109] 例えば、図5の7行目に示したように、スレーブ通信機35a～35dそれぞれから通知された判定結果と、マスタ通信機34の測定部45bによって得られた判定結果との全部に対応する第1暗号照合解または第2暗号選択解が取得されない場合が想定される。かかる場合には、マスタ通信機34の第2通信部43bは、測定Vmが正当ではないことを示す判定結果に対応する第2暗号選択解Dと「暗号解不一致（すなわち、第1暗号照合解または第2暗号選択解が取得されないことを示す情報）」とを照合ECU8に通知してもよい。

[0110] また、スレーブ通信機35a～35dおよびマスタ通信機34それぞれと端末2との間の通信の少なくともいずれかにおいて通信エラーが生じたことが理由となり、その通信機と端末2との間において距離測定のための通信ができなくなる場合が想定される。かかる場合には、端末2と通信機31との間において通信エラーが生じたことを示す情報が、照合ECU8に通知されてもよい。

[0111] 図6に具体的な例を示す。図6に示したように、スレーブ通信機35と端末2との間において通信エラーが生じ、スレーブ通信機35と端末2との間において距離測定のための通信ができなくなる場合が想定される。かかる場合には、スレーブ通信機35の第1通信部43aは、スレーブ通信機35と

端末 2 との間において通信エラーが生じたことを示す情報を、マスタ通信機 3 4 に送信してもよい。そして、マスタ通信機 3 4 の第 2 通信部 4 3 b は、スレーブ通信機 3 5 と端末 2 との間において通信エラーが生じたことを示す情報を、照合 E C U 8 に送信してもよい。

[0112] 図 6 に示した例と同様に、マスタ通信機 3 4 と端末 2 との間において通信エラーが生じ、マスタ通信機 3 4 と端末 2 との間において距離測定のための通信ができなくなる場合が想定される。かかる場合には、マスタ通信機 3 4 の第 2 通信部 4 3 b は、マスタ通信機 3 4 と端末 2 との間において通信エラーが生じたことを示す情報を、照合 E C U 8 に送信してもよい。

[0113] また、照合 E C U 8 の照合部 4 6 によって、マスタ通信機 3 4 から入力された第 2 暗号選択解が、揮発性メモリ 1 5 に登録された第 2 暗号照合解 C'、D' のどちらとも一致しない場合も想定される。かかる場合には、上記したように、処理実行部 1 7 によって、測定値 V m が正当ではないと認識されればよい。このように、照合 E C U 8 において、測定値 V m が正当であると判定されるためには、正しい暗号選択解が必要となるため、セキュリティ性が向上され得る。

[0114] 図 3 に戻り、ステップ S 1 0 6 において、照合 E C U 8 の処理実行部 1 7 は、判定結果に基づいて、スマート照合の可否を判定する。例えば、処理実行部 1 7 は、少なくともいずれか一つの通信機 3 1 から入力された第 2 暗号選択解から、測定値 V m が正当であることを示す判定結果を得れば、スマート照合の照合結果を有効とする。一方、処理実行部 1 7 は、全ての通信機 3 1 から入力された第 2 暗号選択解から、測定値 V m が正当ではないことを示す判定結果を得れば、スマート照合の照合結果を無効とする。

[0115] なお、図 5 の 1 ~ 4 行目に示したように、1 つに集約された第 2 暗号選択解がマスタ通信機 3 4 から照合 E C U 8 に入力される場合も想定される。かかる場合には、照合 E C U 8 の処理実行部 1 7 は、マスタ通信機 3 4 から入力された第 2 暗号選択解から、測定値 V m が正当であることを示す判定結果を得れば、スマート照合の照合結果を有効とすればよい。一方、処理実行部

17は、マスタ通信機34から入力された第2暗号選択解から、測定値Vmが正当ではないことを示す判定結果を得れば、スマート照合の照合結果を無効とすればよい。

[0116] さらに、図5の5～7行目に示したように、第2暗号選択解に加えて「暗号解不一致」がマスタ通信機34から照合ECU8に通知される場合も想定される。かかる場合には、照合ECU8の処理実行部17は、マスタ通信機34から入力された第2暗号選択解から、測定値Vmが正当であることを示す判定結果を得た場合、スマート照合の照合結果を有効としてもよいし、（暗号解不一致であるため）無効としてもよい。一方、処理実行部17は、マスタ通信機34から入力された第2暗号選択解から、測定値Vmが正当ではないことを示す判定結果を得た場合、スマート照合の照合結果を無効とすればよい。

[0117] 例えば、照合ECU8は、室外の端末2とスマート照合（室外スマート照合）が成立し、かつ、処理実行部17がスマート照合の照合結果を有効とした場合、ボディECU9によるドアロック装置6の施錠作動を許可又は実行する。これによって、例えば、ドア施錠時に車外ドアハンドルがタッチ操作されると、車両ドアが解錠され、ドア解錠時に車外ドアハンドルのロックボタンが押し操作されると、車両ドアが施錠される。

[0118] 一方、照合ECU8は、室内の端末2とスマート照合（室内スマート照合）が成立し、かつ、処理実行部17がスマート照合の照合結果を有効とした場合、室内のエンジンスイッチ50による車両電源の遷移操作が許可される。これによって、ブレーキペダルを踏み込まれながらエンジンスイッチ50が操作されると、エンジン7が始動する。

[0119] 照合ECU8は、処理実行部17がスマート照合の照合結果を無効とした場合、スマート照合の成立の有無に拘わらず、車載装置3の作動を禁止する。これによって、例えば、中継器などを用いた不正通信によって車載装置3が作動されてしまうことが防止される。

[0120] <<1. 3. 効果>>

上記の実施形態によれば、外部機器との第1通信の結果に応じて選択された選択解を送信する通信機と、第1通信とは通信機との通信相手が異なる第2通信により通信機から選択解を受信する制御装置と、を有する、通信システムが提供される。かかる構成によれば、外部機器と通信機との間の通信が完了する前から、第1の通信の結果に対応する選択解が用意されている。したがって、かかる構成によれば、通信が完了してから、第1の通信の結果に対応する選択解を制御装置へ出力するまでのタイミングを早期化することが可能となる。

[0121] また、制御装置は、受信した選択解と選択解に対応して用意された照合解とを照合してよい。かかる構成によれば、受信した暗号選択解に対応する暗号照合解があらかじめ用意されている。したがって、かかる構成によれば、選択解を受信してから、当該選択解に適合する照合解を得て当該照合解に対応する判定結果を得るタイミングを早期化することが可能となる。

[0122] 通信機は、選択解を暗号化した暗号選択解を送信し、制御装置は、暗号選択解を受信し、暗号選択解と照合解を暗号化した暗号照合解とを照合してよい。かかる構成によれば、判定結果そのものではなく、暗号選択解及び暗号照合解が用いられるため、判定結果の秘匿性が向上する。また、暗号選択解及び暗号照合解は、共通鍵暗号方式による暗号化に基づいて生成されてよい。かかる構成によれば、通信の秘匿性が向上する。

[0123] 通信システムは、所定条件が満たされた場合に、選択解および照合解を更新する更新制御部を備え、通信機は、更新後の選択解と第1暗号鍵とに基づいて暗号選択解を更新し、制御装置は、更新後の照合解と第1暗号鍵と共通する暗号鍵である第2暗号鍵とに基づいて暗号照合解を更新してよい。かかる構成によれば、暗号選択解及び暗号照合解の秘匿性が向上する。

[0124] 通信機は、第1通信機と、第2通信機とを含み、第1通信機は、外部機器との第1通信の結果に応じた第1暗号選択解を第2通信機に送信する第1通信部を備え、第2通信機は、第1通信機から受信した第1暗号選択解と適合する第1暗号照合解が取得された場合に、第1暗号照合解に対応する第2暗

号選択解を制御装置に送信する第2通信部を備えてよい。かかる構成によれば、あらかじめ暗号選択鍵及び暗号照合解が用意されているため、処理時間の増加が抑制されつつ、通信の秘匿性が向上する。

[0125] 第2通信部は、正常判定に対応する第1暗号選択解を受信し、正常判定に対応する第1暗号選択解に適合する第1暗号照合解が取得された場合には、正常判定に対応する第2暗号選択解を制御装置に送信し、異常判定に対応する第1暗号選択解を受信し、異常判定に対応する第1暗号選択解に適合する第1暗号照合解が取得された場合には、異常判定に対応する第2暗号選択解を制御装置に送信してもよい。かかる構成によれば、あらかじめ暗号選択鍵及び暗号照合解が用意されているため、処理時間の増加が抑制されつつ、通信の秘匿性が向上する。第1暗号選択解と第2暗号選択解とが異なっていれば、判定結果の秘匿性がさらに向上する。

[0126] <<1. 4. 変形例>>

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

[0127] 例えば、本実施形態は、以下のように変更して実施することができる。本実施形態及び以下の変更例は、技術的に矛盾しない範囲で互いに組み合わせて実施することができる。

[0128] (暗号選択解及び暗号照合解に関する変形例)

上記例では、第2暗号選択解が、第1暗号選択解とは別の暗号鍵によって生成される場合を想定した。しかし、第2暗号選択解は、第1暗号選択解を共通鍵暗号方式によって暗号化したものでもよい。すなわち、マスタ通信機34において、スレーブ通信機35から受信した第1暗号選択解に対して、共通鍵暗号方式による暗号化処理が実行されることによって第2暗号選択解

が生成されてもよい。かかる構成によれば、スレーブ通信機 35 及びマスタ通信機 34 の間と、マスタ通信機 34 及び照合 ECU 8 の間とにおいて、送信される暗号選択解を異ならせることができる。これは、秘匿性の向上に寄与する。

[0129] 上記例では、マスタ通信機 34 から照合 ECU 8 に送信されるデータが、第 2 暗号選択解である場合を想定した。しかし、マスタ通信機 34 から照合 ECU 8 に送信されるデータは限定されない。例えば、マスタ通信機 34 から照合 ECU 8 に送信されるデータは、第 1 暗号選択解に応じて送信されるデータであればよい。

上記例では、暗号選択解及び暗号照合解の更新が、乱数 α 、 β と暗号鍵とを用いて行われる場合を想定した。しかし、暗号選択解及び暗号照合解の更新手法は、限定されない。例えば、暗号選択解及び暗号照合解の更新は、所定の演算式を用いた暗号選択解及び暗号照合解の再暗号化によって行われてもよい。

[0130] 上記例では、距離測定要求とともに乱数 α 、 β が送信される場合を想定した。しかし、乱数 α 、 β の送信タイミングは、特に限定されない。例えば、乱数 α 、 β は、距離測定要求よりも前に送信されてもよい。

[0131] 上記例では、乱数 α 、 β が、照合 ECU 8 から出力される場合を想定した。しかし、乱数 α 、 β は、照合 ECU 8 とは異なるブロックから出力されてもよい。例えば、乱数 α 、 β は、マスタ通信機 34 から出力されてもよいし、スレーブ通信機 35 から出力されてもよい。すなわち、乱数 α 、 β は、照合 ECU 8、マスタ通信機 34、及び、スレーブ通信機 35 のうち、少なくともいずれか一つから出力されて、照合 ECU 8、マスタ通信機 34、及び、スレーブ通信機 35 の間で共有されればよい。

[0132] 上記例では、第 1 暗号選択解及び第 2 暗号選択解が、別の乱数に基づいて生成される場合を想定した。しかし、第 1 暗号選択解及び第 2 暗号選択解は、同じ乱数に基づいて生成されてもよい。同様に、第 1 暗号照合解及び第 2 暗号照合解が、別の乱数に基づいて生成される場合を想定した。しかし、第

1 暗号照合解及び第2暗号照合解は、同じ乱数に基づいて生成されてもよい。

[0133] 上記例では、第1暗号選択解及び第2暗号選択解が、別の暗号鍵に基づいて生成される場合を想定した。しかし、第1暗号選択解及び第2暗号選択解は、同じ暗号鍵に基づいて生成されてもよい。同様に、第1暗号照合解及び第2暗号照合解が、別の暗号鍵に基づいて生成される場合を想定した。しかし、第1暗号照合解及び第2暗号照合解は、共通する暗号鍵に基づいて生成されてもよい。

[0134] 暗号選択解及び暗号照合解は、更新されなくてもよい。すなわち、更新部44は、省略されてもよい。

上記例では、すべてのスレーブ通信機35に同じ暗号選択解が登録される場合を想定した。しかし、スレーブ通信機35ごとに異なる暗号選択解が登録されていてもよい。

暗号鍵の登録方法は、特に限定されない。

暗号選択解及び暗号照合解を演算する演算式（アルゴリズム）は、特に限定されない。すなわち、暗号選択解及び暗号照合解の生成方法は、特に限定されない。

暗号選択解及び暗号照合解は、必須の要件ではなく、暗号化されていない選択解及び照合解が用いられてもよい。このとき、選択解及び照合解は、同じであってもよいし、異なってもよい。

[0135] （距離測定のための通信に関する変形例）

距離測定のための通信開始のトリガがどのようなトリガであるかに関わらず、距離測定のための通信が行われるタイミングは、スマート照合の前であってもよいし、スマート照合の後であってもよいし、スマート照合の途中でなくてもよい。例えば、距離測定のための通信がスマート照合の前又は途中で実行される場合に、処理実行部17によってスマート照合の成立が無効にされる場合があり得る。かかる場合には、処理実行部17は、スマート照合を途中で強制的に終了させてもよい。すなわち、処理実行部17は、スマー

ト照合の成立を無効にした場合に、スマート照合（スマート通信）を成立させない何らかの処理を行えばよい。

[0136] 上記例では、測定値 V_m が、スレーブ通信機 35 と端末 2 との間の電波の伝播時間から測定される場合を主に説明した。しかし、測定値 V_m を測定する手法は、かかる例に限定されない。例えば、測定値 V_m は、スレーブ通信機 35 及び端末 2 のうち、一方から送信された電波を他方が受信した場合、当該他方が電波の受信強度（RSSI : Received Signal Strength Indicator）を測定し、この受信強度から距離に準じた測定値を算出してもよい。このとき、通信機 31 及び端末 2 のいずれか一方は、UWB 電波 S_a の送信だけを行い、他方は、UWB 電波 S_a の受信だけを行ってもよい。

[0137] 上記例では、端末 2 が UWB 送受信部 33 を備える場合を想定した。しかし、端末 2 は、UWB 送受信部 33 を備えていなくてもよい。かかる場合には、通信機 31 は、端末 2 からの電波の反射波の受信結果に基づいて、測定値 V_m を求めればよい。

[0138] 上記例では、スレーブ通信機 35 の測定部 45a、及び、マスタ通信機 34 の測定部 45b によって測定値 V_m が測定される場合を主に説明した。このとき、測距用電波は、スレーブ通信機 35 及びマスタ通信機 34 それぞれから端末 2 に送信される。しかし、測定値 V_m は、スレーブ通信機 35 及びマスタ通信機 34 以外によって測定されてもよい。例えば、測定値 V_m は、端末 2 によって測定されてもよい。このとき、測距用電波は、端末 2 からスレーブ通信機 35 及びマスタ通信機 34 それぞれに送信されればよい。

[0139] 上記例では、端末 2 から UWB 電波 S_a が最初に送信される場合を想定した。しかし、通信機 31 から UWB 電波 S_a が最初に送信されてもよい。

[0140] 上記例では、スレーブ通信機 35 の測定部 45a によって測定値 V_m が測定される場合を主に説明した。このとき、測距用電波は、スレーブ通信機 35 から端末 2 に送信される。しかし、測定値 V_m は、スレーブ通信機 35 以外によって測定されてもよい。例えば、測定値 V_m は、端末 2 によって測定されてもよい。このとき、測距用電波は、端末 2 からスレーブ通信機 35 に

送信されればよい。

[0141] また、複数のチャネルそれぞれを使用して電波送信が行われてもよい。このとき、測定部45は、複数のチャネルそれぞれを使用して行われた電波送信の結果（伝播時間または受信強度）に基づいて、測定値 V_m を算出してもよい。

・距離測定のための通信（測距用電波及びその応答電波）の方式は、UWB電波S_aを使用した方式に限定されない。例えば、距離測定のための通信として、他の周波数の電波が使用されてもよい。一例として、距離測定のための通信として、ブルートゥース（登録商標）通信が使用されてもよい。

[0142] 端末2と通信機31との間で行われる第1通信は、距離測定のための通信に限定されない。例えば、第1通信は、情報を送受信する通信であればよい。

端末2と通信機31との間で行われる第1通信は、通信相手を認証する通信であってもよい。例えば、通信相手を認証する通信としては、距離測定のための通信、ID照合のための通信、及び生体情報を認証するための通信などが挙げられる。

[0143] 端末2と通信機31との間で行われる第1通信は、通信相手を操作するための通信であってもよい。例えば、通信相手を操作するための通信としては、メディアプレーヤーの選曲を行うための通信、ラジオ選局又は音量調整の操作を行うための通信、ナビゲーションシステムの操作を行うための通信、空調の操作を行うための通信、及び、エンジンの遷移を操作するための通信などが挙げられる。また、通信相手を操作するための通信には、通信の結果を基に、ライト点灯又は表示などによって、ユーザに対しておもてなしをする機能を有するものが含まれる。

[0144] （システムの各種変形例）

上記例では、複数の通信機31のうちマスタ通信機34だけが、直接的に照合ECU8に接続されている場合を想定した。しかし、複数の通信機31が、照合ECU8に接続されていてもよい。また、通信機31は、マスタ通

信機 3 4 及びスレーブ通信機 3 5 に分かれていなくてもよい。

- [0145] 車両 1 の L F 送信機 1 3 は、車両 1 の周囲に L F 電波（ウェイク信号）エリアを形成するように車両 1 に設けられてもよい。例えば、車両 1 の L F 送信機 1 3 は、運転席ドアの周囲、助手席ドアの周囲、バックドアの周囲、及び、室内に、L F 電波エリアを形成してもよい。

通信制御部 3 8 は、L F 送信機 1 3 によって形成された L F 電波エリアに基づき、通信機 3 1 の作動を制御してもよい。例えば、通信制御部 3 8 は、運転席ドアの周囲の L F 電波エリアに端末 2 が進入し、室外スマート照合が成立した場合、運転席に近い第 1 スレーブ通信機 3 5 a 及び第 3 スレーブ通信機 3 5 c のみを作動させ、残りを作動させなくてもよい。

- [0146] 上記例では、スマート照合の種類に関わらず、スマート照合が行われる場合に、距離測定のための通信が行われる場合を主に説明した。しかし、スマート照合が行われる場合であっても、スマート照合の種類に応じて、距離測定のための通信を行うか否かが制御されてもよい。例えば、室外スマート照合が行われる場合には、距離測定のための通信が行われず、室内スマート照合が行われる場合にのみ、距離測定の通信が行われてもよい。すなわち、通信制御部 3 8 は、車両 1 の外側に形成される L F 電波エリアでは、通信機 3 1 を作動せず、室内に形成される L F 電波エリアでは、通信機 3 1 を作動させてもよい。

- [0147] 上記例では、スマート照合の成立可否を決定する処理実行部 1 7 が照合 E C U 8 に設けられる場合を主に説明した。しかし、処理実行部 1 7 が設けられる位置は限定されない。例えば、処理実行部 1 7 は、マスタ通信機 3 4 に設けられてもよいし、スレーブ通信機 3 5 に設けられてもよいし、端末 2 に設けられてもよい。

上記例では、マスタ通信機 3 4 が、各通信機 3 1 によって得られた判定結果を照合 E C U 8 へ送信するばあいを想定した。このとき、マスタ通信機 3 4 は、各通信機 3 1 によって得られた判定結果を、別々のタイミングで照合 E C U 8 へ送信してもよいし、同じタイミングで照合 E C U 8 へまとめて送

信してもよい。

[0148] 上記例では、距離測定のための通信による結果として、測定値 V_m が正当であるか否かを示す判定結果がスレーブ通信機 35 からからマスタ通信機 34 へ送信される場合を想定した。しかし、距離測定のための通信による結果として、他の判定結果がスレーブ通信機 35 からからマスタ通信機 34 へ送信されてもよい。例えば、距離測定のための通信による結果として、測定値 V_m がどの程度であるかを示すレベルがスレーブ通信機 35 からからマスタ通信機 34 へ送信されてもよいし、処理実行部 17 がマスタ通信機 34 に設けられた場合などには、スマート照合の照合結果を有効にするか無効にするかがスレーブ通信機 35 からからマスタ通信機 34 へ送信されてもよい。

[0149] 上記例では、通信機 31 と端末 2 との距離に準じた測定値 V_m の正当性が、通信機 31 によって判定される場合を主に説明した。しかし、測定値 V_m の正当性は、端末 2 によって判定されてもよい。このとき、端末 2 は、測定値 V_m の正当性の判定結果を通信機 31 に通知すればよい。

[0150] 車両 1 及び端末 2 の間の各種通信に使用される電波の周波数及び通信方式は、種々の態様に変更され得る。

[0151] 上記例では、スマート照合システムにおいて、ウェイク信号が車両 1 から端末 2 に送信される場合を主に説明した。しかし、ウェイク信号は、端末 2 から車両 1 に送信されてもよい。

上記例では、端末 2 の正否の確認が、キー ID の照合及び要求応答認証によって行われる場合を主に説明した。しかし、端末 2 の正否を確認する方式は、かかる例に限定されない。例えば、端末 2 の正否を確認する方式は、端末 2 及び車両 1 が通信を通じて、端末 2 及び車両 1 が正規のペアであるか否かを確認することが可能な方式であればよい。

[0152] 上記例では、電子キーシステム 4 が、スマート照合を実行するスマート照合システムである場合を主に説明した。しかし、電子キーシステム 4 は、スマート照合システムに限定されない。例えば、電子キーシステム 4 は、端末 2 の正否を確認することが可能なシステムであればよい。あるいは、電子キ

ーシステム 4 は省略されてもよく、UWB 通信を用いて端末 2 の正否が確認されてもよい。

[0153] 上記例では、端末 2 が電子キー 5 である場合を主に説明した。しかし、端末 2 は電子キー 5 である場合に限定されない。例えば、端末 2 は、車両 1 との無線通信が実行可能な高機能携帯電話であってもよい。

[0154] 上記例では、通信機 3 1 及び照合 ECU 8（制御装置）が車両 1 に搭載される場合を想定した。しかし、通信機 3 1 及び照合 ECU 8（制御装置）は、車両 1 に搭載されることに限定されず、種々の機器又は装置に搭載されてもよい。

符号の説明

[0155] 1…車両、2…端末、3…車載装置、4…電子キーシステム、5…電子キー、15…揮発性メモリ、17…処理実行部、20…端末制御部、30…距離測定システム、31…通信機、45…測定部、33…UWB 送受信部、34…マスタ通信機、35…スレーブ通信機、38…通信制御部、39…インターフェース部、40a…揮発性メモリ、40b…揮発性メモリ、42…取得部、43…通信部、44…更新部、45…測定部、46…照合部、47…更新制御部、48…認証部、49…受信部。

請求の範囲

- [請求項1] 外部機器との第1通信の結果に応じて選択された選択解を送信する通信機と、
- 前記第1通信とは前記通信機との通信相手が異なる第2通信により前記通信機から前記選択解を受信する制御装置と、
- を有する、通信システム。
- [請求項2] 前記制御装置は、
- 受信した前記選択解と前記選択解に対応して用意された照合解とを照合する、
- 請求項1に記載の通信システム。
- [請求項3] 前記通信機は、前記選択解を暗号化した暗号選択解を送信し、
- 前記制御装置は、前記暗号選択解を受信し、前記暗号選択解と前記照合解を暗号化した暗号照合解とを照合する、
- 請求項2に記載の通信システム。
- [請求項4] 前記暗号選択解及び前記暗号照合解は、共通鍵暗号方式による暗号化に基づいて生成される、
- 請求項3に記載の通信システム。
- [請求項5] 前記通信システムは、
- 所定条件が満たされた場合に、前記選択解および前記照合解を更新する更新制御部を備え、
- 前記通信機は、更新後の前記選択解と第1暗号鍵とに基づいて前記暗号選択解を更新し、
- 前記制御装置は、更新後の前記照合解と前記第1暗号鍵と共通する暗号鍵である第2暗号鍵とに基づいて前記暗号照合解を更新する、
- 請求項4に記載の通信システム。
- [請求項6] 前記更新制御部は、前記外部機器の認証のための通信が確立した場合、前記外部機器の認証の一部が成立した場合、所定時間が経過した場合又は前記通信機と前記制御装置との間の暗号通信の回数が所定回

数に達した場合、前記所定条件を満たしたものと判定する、
請求項 5 に記載の通信システム。

[請求項7]

前記通信システムは、
複数の暗号選択解を記憶する第 1 記憶部と、
複数の暗号照合解を記憶する第 2 記憶部と、を有し、
前記通信機は、前記第 1 記憶部に記憶された前記複数の暗号選択解
から前記第 1 通信の結果に応じて選択された前記暗号選択解を送信し
、
前記制御装置は、前記通信機から受信した前記暗号選択解と前記第
2 記憶部に記憶された前記複数の暗号照合解とを照合する、
請求項 3 ～ 6 のいずれか一項に記載の通信システム。

[請求項8]

前記通信機は、
前記第 1 通信の結果が正常判定を示す場合、前記正常判定に対応す
る暗号選択解を前記制御装置に送信し、
前記第 1 通信の結果が異常判定を示す場合、前記異常判定に対応す
る暗号選択解を前記制御装置に送信する、
請求項 3 ～ 7 のいずれか一項に記載の通信システム。

[請求項9]

前記通信機は、第 1 通信機と、第 2 通信機とを含み、
前記第 1 通信機は、
前記外部機器との前記第 1 通信の結果に応じた第 1 暗号選択解を前
記第 2 通信機に送信する第 1 通信部を備え、
前記第 2 通信機は、
前記第 1 通信機から受信した前記第 1 暗号選択解と適合する第 1 暗
号照合解が取得された場合に、前記第 1 暗号照合解に対応する第 2 暗
号選択解を前記制御装置に送信する第 2 通信部を備える、
請求項 3 ～ 8 のいずれか一項に記載の通信システム。

[請求項10]

前記第 1 通信部は、
前記第 1 通信の結果が正常判定を示す場合、前記正常判定に対応す

る第1暗号選択解を前記第2通信機に送信し、

前記第1通信の結果が異常判定を示す場合、前記異常判定に対応する第1暗号選択解を前記第2通信機に送信する、

請求項9に記載の通信システム。

[請求項11]

前記第2通信部は、

前記正常判定に対応する第1暗号選択解を受信し、前記正常判定に対応する第1暗号選択解に適合する前記第1暗号照合解が取得された場合には、前記正常判定に対応する第2暗号選択解を前記制御装置に送信し、

前記異常判定に対応する第1暗号選択解を受信し、前記異常判定に対応する第1暗号選択解に適合する前記第1暗号照合解が取得された場合には、前記異常判定に対応する第2暗号選択解を前記制御装置に送信する、

請求項10に記載の通信システム。

[請求項12]

前記第2通信部は、

受信した第1暗号選択解に適合する第1暗号照合解が取得されない場合には、前記第1暗号照合解が取得されないことを示す情報を前記制御装置に送信する、

請求項9～11のいずれか一項に記載の通信システム。

[請求項13]

前記制御装置は、

前記第2暗号選択解を受信する受信部と、

前記第2暗号選択解と第2暗号照合解とを照合する照合部と、を備える、

請求項9～12のいずれか一項に記載の通信システム。

[請求項14]

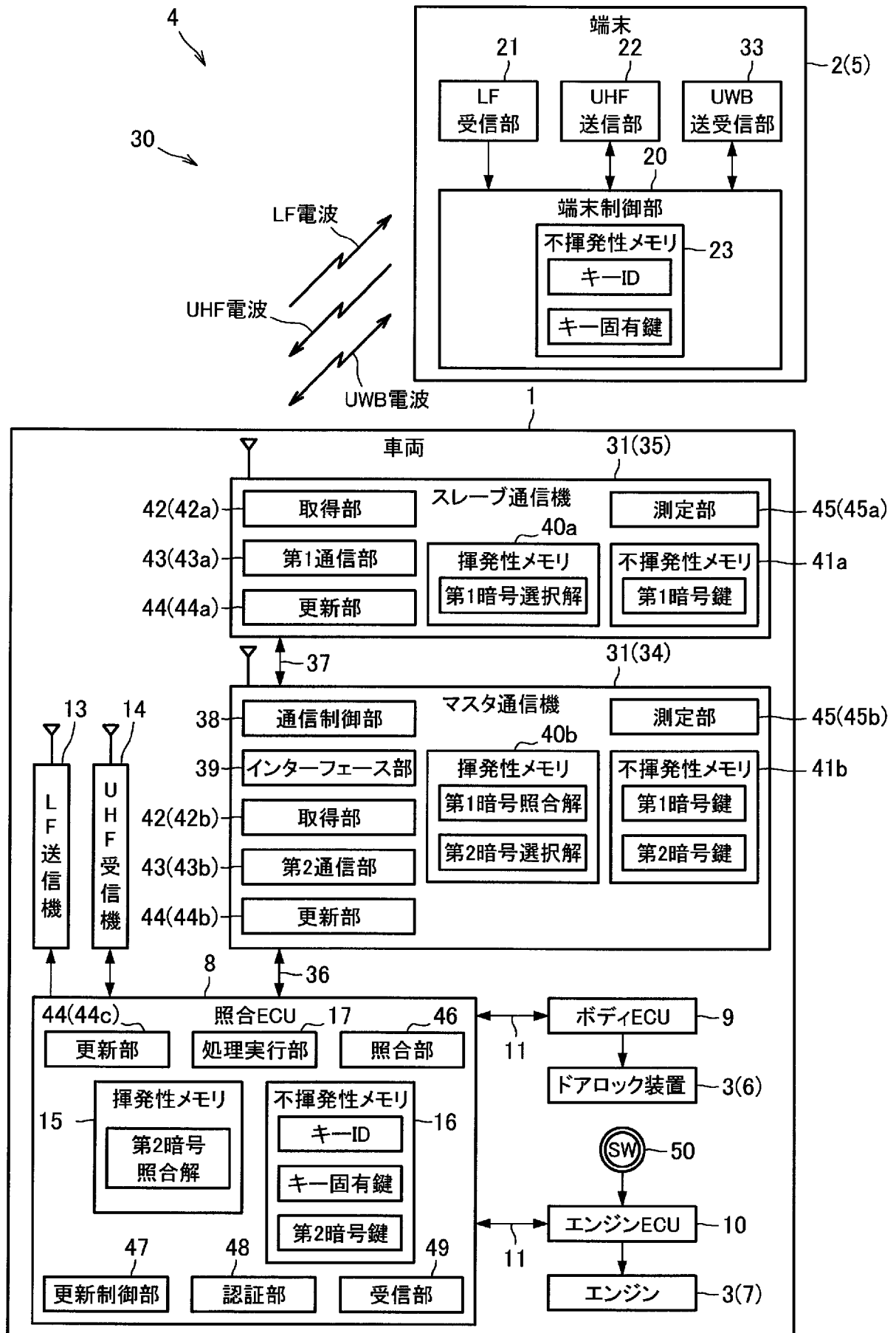
前記第1暗号選択解及び前記第1暗号照合解は、共通鍵暗号方式による第1暗号化に基づいて生成され、

前記第2暗号選択解及び前記第2暗号照合解は、共通鍵暗号方式による第2暗号化に基づいて生成される、

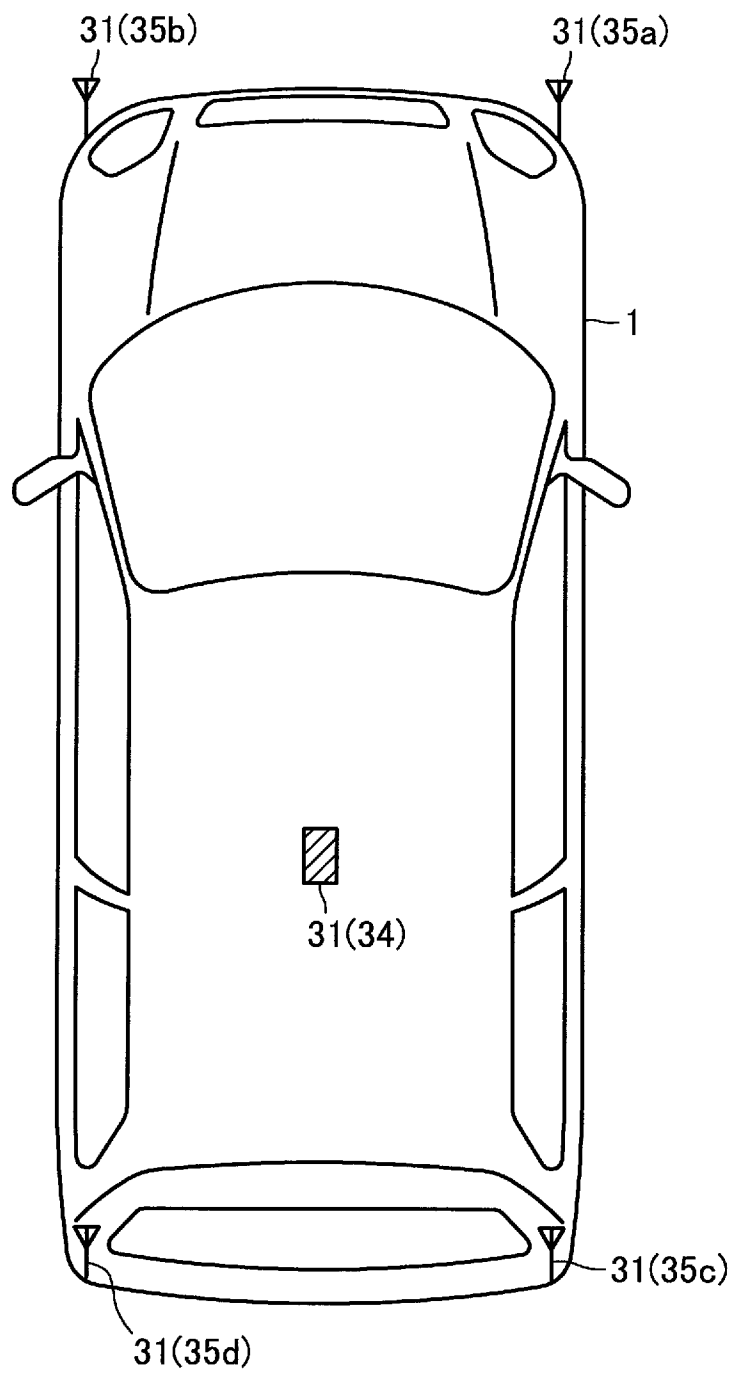
請求項 1 3 に記載の通信システム。

- [請求項15] 外部機器との第 1 通信の結果に応じて選択された選択解を取得する取得部と、
- 前記第 1 通信とは通信相手が異なる第 2 通信により前記選択解を制御装置に送信する通信部と、
- を備える、通信機。

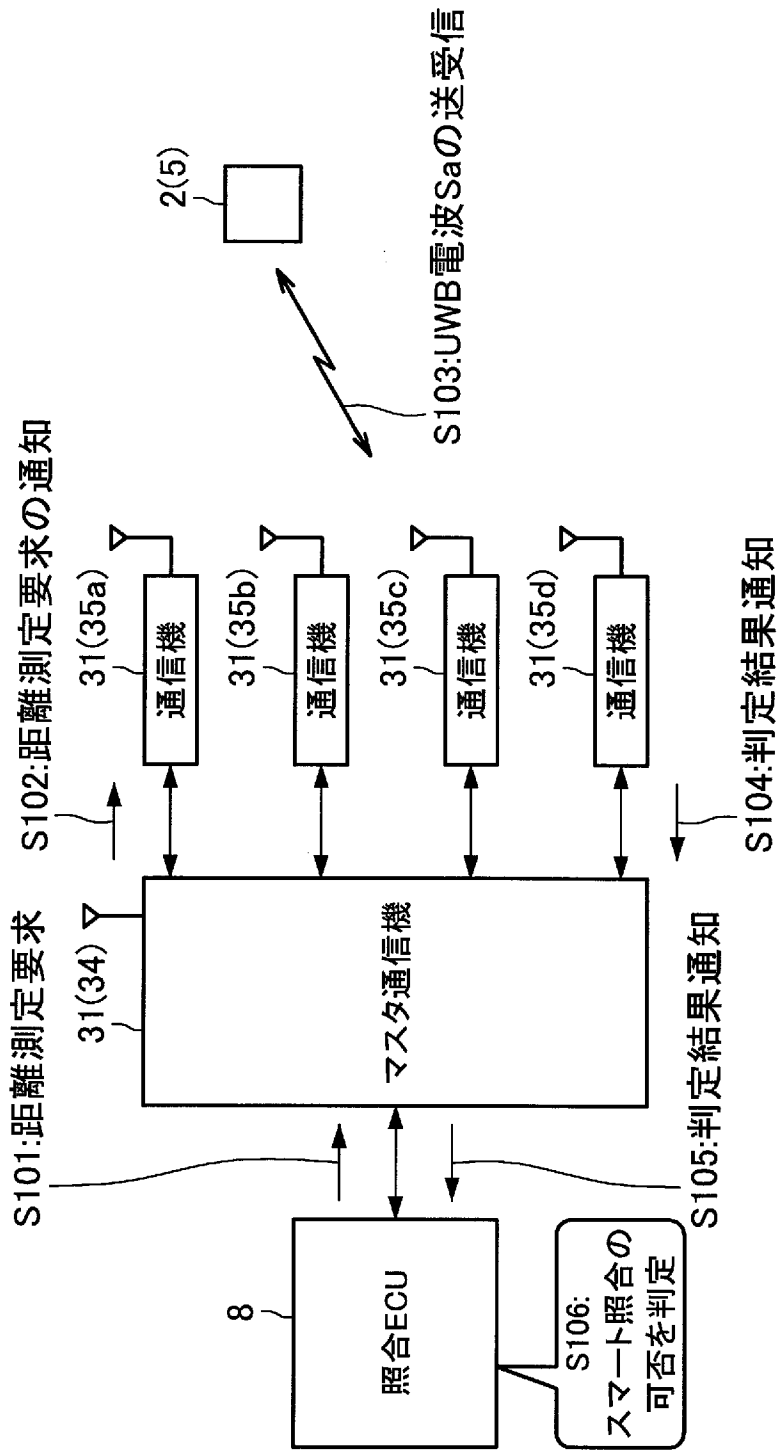
[図1]



[図2]

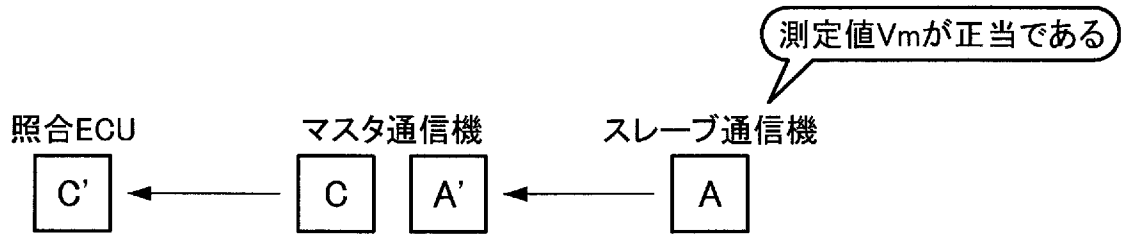


[図3]

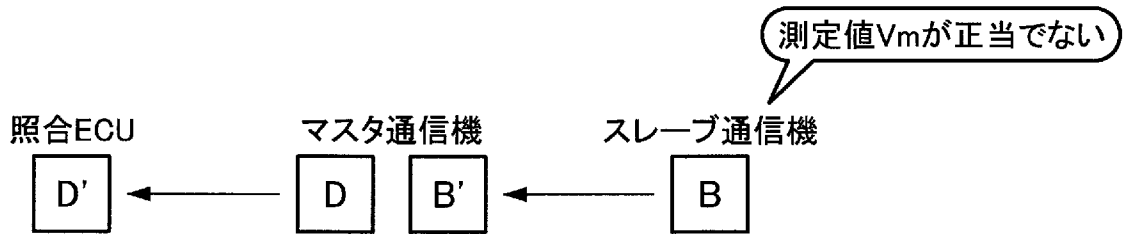


[図4]

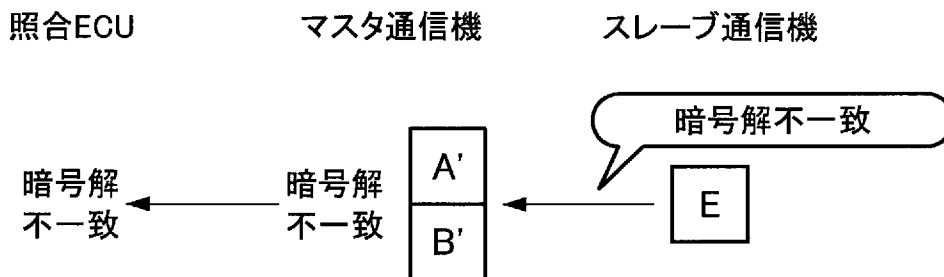
(a)



(b)



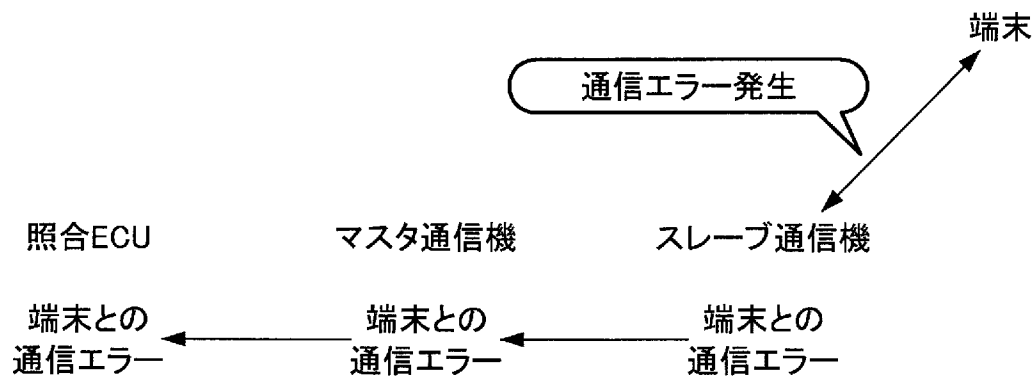
(c)



[図5]

行番号	照合ECUへの通知	マスタ通信機における 測定値の判定結果	スレーブ通信機における 測定値の判定結果
1	OK(第2暗号選択解C)	OK	OK
2		OK	NG
3		NG	OK
4	NG(第2暗号選択解D)	NG	NG
5	OK(第2暗号選択解C) + 暗号解不一致	OK	暗号解不一致
6		暗号解不一致	OK
7	NG(第2暗号選択解D) + 暗号解不一致	暗号解不一致	暗号解不一致

[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/015654

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44 (2013.01) i

FI: G06F21/44

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)

G06F21/44

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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	JP 2005-138633 A (TOKAIRIKA, CO., LTD.) 02.06.2005 (2005-06-02) paragraphs [0017]-[0028], [0049], fig. 1	1-3, 7, 9, 13, 15
Y	paragraphs [0017]-[0028], [0049], fig. 1	4-14
Y	JP 2010-11400 A (NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY) 14.01.2010 (2010-01-14) abstract, paragraphs [0026]-[0027]	4-14
Y	JP 2005-22491 A (HONDA MOTOR CO., LTD.) 27.01.2005 (2005-01-27) paragraphs [0030]-[0033], fig. 3-4	5-14
Y	JP 1997-277906 A (TOYOTA MOTOR CORP.) 28.10.1997 (1997-10-28) abstract	8-14



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

"I" 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

17 June 2020 (17.06.2020)

Date of mailing of the international search report

30 June 2020 (30.06.2020)

Name and mailing address of the ISA/

Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/015654

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2005-138633 A	02 Jun. 2005	US 2006/0152348 A1 paragraphs [0017]- [0039], fig. 1 KR 10-2006-0017484 A CN 1723142 A (Family: none)	
JP 2010-11400 A	14 Jan. 2010	(Family: none)	
JP 2005-22491 A	27 Jan. 2005	(Family: none)	
JP 1997-277906 A	28 Oct. 1997	US 6025653 A abstract DE 69735803 T	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/44(2013.01)i FI: G06F21/44		
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）） G06F21/44		
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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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	JP 2005-138633 A（株式会社東海理化電機製作所）02.06.2005（2005-06-02） 段落[0017]-[0028], [0049], 図1	1-3, 7, 9, 13, 15
Y	段落[0017]-[0028], [0049], 図1	4-14
Y	JP 2010-11400 A（独立行政法人産業技術総合研究所）14.01.2010（2010-01-14） 要約, 段落[0026]-[0027]	4-14
Y	JP 2005-22491 A（本田技研工業株式会社）27.01.2005（2005-01-27） 段落[0030]-[0033], 図3-4	5-14
Y	JP 1997-277906 A（トヨタ自動車株式会社）28.10.1997（1997-10-28） 要約	8-14
☐ 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、一般的な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抵触するものではなく、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 17.06.2020	国際調査報告の発送日 30.06.2020	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 上島 拓也 5S 6293 電話番号 03-3581-1101 内線 3546	

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/015654

引用文献			公表日	パテントファミリー文献	公表日
JP	2005-138633	A	02.06.2005	US 2006/0152348 A1 段落[0017]-[0039], 図1 KR 10-2006-0017484 A CN 1723142 A	
JP	2010-11400	A	14.01.2010	(ファミリーなし)	
JP	2005-22491	A	27.01.2005	(ファミリーなし)	
JP	1997-277906	A	28.10.1997	US 6025653 A 要約 DE 69735803 T	