(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5173891号
(P5173891)

(45)発行日　平成25年4月3日(2013.4.3)　(24)登録日　平成25年1月11日(2013.1.11)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
E05B 49/00	(2006.01)	E05B	49/00	J
B60R 25/01	(2013.01)	B60R	25/00	606
B60R 25/10	(2013.01)	B60R	25/10	617

請求項の数 4　(全 12 頁)

(21)出願番号　特願2009-48081(P2009-48081)
(22)出願日　平成21年3月2日(2009.3.2)
(65)公開番号　特開2010-206383(P2010-206383A)
(43)公開日　平成22年9月16日(2010.9.16)
審査請求日　平成23年8月8日(2011.8.8)

(73)特許権者　000003551
株式会社東海理化電機製作所
愛知県丹羽郡大口町豊田三丁目２６０番地
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　河村　大輔
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
(72)発明者　岩下　明暁
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

最終頁に続く

(54)【発明の名称】秘密鍵登録システム及び秘密鍵登録方法

(57)【特許請求の範囲】
【請求項１】
通信端末の製造時において書き込み器により前記通信端末に必要事項を書き込み、当該通信端末とその通信相手とを無線通信させて、該通信端末が持つ各種情報を前記通信相手に発信することにより、前記通信相手に必要事項を書き込んで登録作業を行う秘密鍵登録システムであって、
値が毎回変化する登録コードを前記書き込み器から前記通信端末に送るとともに、前記書き込み器において秘密鍵生成の一アルゴリズムである第１変換式により前記登録コードを演算して中間データを生成しつつ、当該中間データを前記通信端末に送り、前記通信端末において秘密鍵生成の他アルゴリズムである第２変換式により前記中間データを演算して、この演算結果を秘密鍵として前記通信端末に登録する通信端末側秘密鍵登録手段と、
前記通信端末が持つ前記登録コードを、無線通信を介して前記通信相手に発信し、前記通信相手において前記登録コード及び前記第１変換式による前記中間データの演算と、当該中間データ及び前記第２変換式による秘密鍵の演算とを行わせ、当該秘密鍵を前記通信相手に登録する通信相手側秘密鍵登録手段と
を備えたことを特徴とする秘密鍵登録システム。
【請求項２】
前記通信端末側秘密鍵登録手段は、前記通信端末が前記書き込み器から取得した前記中間データを、前記秘密鍵の演算後に消去することを特徴とする請求項１に記載の秘密鍵登録システム。

【請求項３】
前記第１変換式における前記アルゴリズムの計算量は、前記第２変換式における前記アルゴリズムの計算量がよりも大きく設定されていることを特徴とする請求項１又は２に記載の秘密鍵登録システム。
【請求項４】
通信端末の製造時において書き込み器により前記通信端末に必要事項を書き込み、当該通信端末とその通信相手とを無線通信させて、該通信端末が持つ各種情報を前記通信相手に発信することにより、前記通信相手に必要事項を書き込んで登録作業を行う秘密鍵登録方法であって、
前記通信端末への秘密鍵登録は、値が毎回変化する登録コードを前記書き込み器から前記通信端末に送るとともに、前記書き込み器において秘密鍵生成の一アルゴリズムである第１変換式により前記登録コードを演算して中間データを生成しつつ、当該中間データを前記通信端末に送り、前記通信端末において秘密鍵生成の他アルゴリズムである第２変換式により前記中間データを演算して、この演算結果を秘密鍵として前記通信端末に登録することにより行い、
前記通信相手への秘密鍵登録は、前記通信端末が持つ前記登録コードを、無線通信を介して前記通信相手に発信し、前記通信相手において前記登録コード及び前記第１変換式による前記中間データの演算と、当該中間データ及び前記第２変換式による秘密鍵の演算とを行わせ、当該秘密鍵を前記通信相手に登録することにより行うことを特徴とする秘密鍵登録方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号通信による通信が可能な通信端末とその通信相手とに、同通信の暗号鍵である秘密鍵を登録する際に使用する秘密鍵登録システム及び秘密鍵登録方法に関する。
【背景技術】
【０００２】
従来、多くの車両では、キーが持つ固有のキーコードを無線により発信する電子キーを車両キーとして用いる電子キーシステムが広く採用されている。この種の電子キーシステムの一種には、例えば電子キーでのボタン操作により遠隔操作によって車両ドアのドアロックを施解錠可能なワイヤレスドアロックシステムがある。また、電子キーシステムの他の種類には、車両から発信されるリクエストに応答して、電子キーがＩＤコードを自動で車両に返し、このＩＤコードのＩＤ照合が成立すれば、ドアロック施解錠やエンジン始動が許可又は実行されるキー操作フリーシステムもある。
【０００３】
この電子キーシステムでは、電子キーから発信されるＩＤコードがもし仮に傍受されても、簡単にＩＤコードが簡単に割り出されないようにするために、一般的には暗号通信（例えば、特許文献１等参照）が採用されている。この暗号通信には、暗号の一種として秘密鍵暗号（共通鍵暗号）が使用されている。秘密鍵暗号とは、送信側の暗号鍵と、受信側の復号鍵とが同じ鍵となっている暗号である。秘密鍵暗号には、鍵が送信と受信で同じ特性があることから、暗号及び復号の速度が速いという利点があり、車両の暗号通信において広く使用されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００４－３００８０３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、電子キーシステムに暗号通信を搭載する場合、この種の暗号通信では車両及

び電子キーの両方に秘密鍵が必要であるので、例えば製造段階や出荷段階等において、車両及び電子キーに秘密鍵を各々登録する必要がある。しかし、この秘密鍵登録の際に、もし仮に秘密鍵が盗聴されてしまうと、車両出荷後にこの秘密鍵を使用して不正にＩＤ照合が成立されてしまう可能性もあるので、これが車両盗難の問題に繋がる。このため、秘密鍵が盗み取られ難いセキュリティ性の高い暗号鍵の登録方式が必要であった。

【０００６】

本発明の目的は、秘密鍵の盗み取りを発生し難くすることができる秘密鍵登録システム及び秘密鍵登録方法を提供することにある。

【課題を解決するための手段】

【０００７】

前記問題点を解決するために、本発明では、通信端末の製造時において書き込み器により前記通信端末に必要事項を書き込み、当該通信端末とその通信相手とを無線通信させて、該通信端末が持つ各種情報を前記通信相手に発信することにより、前記通信相手に必要事項を書き込んで登録作業を行う秘密鍵登録システムであって、値が毎回変化する登録コードを前記書き込み器から前記通信端末に送るとともに、前記書き込み器において秘密鍵生成の一アルゴリズムである第１変換式により前記登録コードを演算して中間データを生成しつつ、当該中間データを前記通信端末に送り、前記通信端末において秘密鍵生成の他アルゴリズムである第２変換式により前記中間データを演算して、この演算結果を秘密鍵として前記通信端末に登録する通信端末側秘密鍵登録手段と、前記通信端末が持つ前記登録コードを、無線通信を介して前記通信相手に発信し、前記通信相手において前記登録コード及び前記第１変換式による前記中間データの演算と、当該中間データ及び前記第２変換式による秘密鍵の演算とを行わせ、当該秘密鍵を前記通信相手に登録する通信相手側秘密鍵登録手段とを備えたことを要旨とする。

【０００８】

この構成によれば、秘密鍵の生成には、登録コードを第１変換式で演算して中間データを求め、更にこの中間データを第２変換式で演算するというように、２つの変換式が必要となる。よって、例えば仮に書き込み器から第１変換式が盗み取られ、更に通信相手に秘密鍵を登録する際に、通信端末が発信する登録コードが盗聴されたとしても、盗難行為者の手元には第１変換式と登録コードしかないので、これらからでは秘密鍵を割り出すことができない。よって、秘密鍵の登録方式を、秘密鍵の盗難に対してセキュリティ性の高いものとすることが可能となる。

【０００９】

本発明では、前記通信端末側秘密鍵登録手段は、前記通信端末が前記書き込み器から取得した前記中間データを、前記秘密鍵の演算後に消去することを要旨とする。

この構成によれば、通信端末に秘密鍵が登録された後は、通信端末が書き込み器から取得した中間データは消去されるので、秘密鍵の登録後、通信端末には中間データが残ったままの状態とならない。よって、通信端末から中間データを盗み取るという不正行為が実行不可となるので、秘密鍵の盗難に対するセキュリティ性を、より高くすることが可能となる。

【００１０】

本発明では、前記第１変換式における前記アルゴリズムの計算量は、前記第２変換式における前記アルゴリズムの計算量がよりも大きく設定されていることを要旨とする。

この構成によれば、本構成のように書き込み器及び通信端末の各々に変換式を割り当てて、通信端末に秘密鍵を登録する際に必要な演算を２機器に亘るようにしても、通信端末側に乗せる変換式（アルゴリズム）は計算量が少ないもので済む。このため、通信端末に大きなメモリ容量を用意する必要がないので、通信端末のメモリを容量の大きいものに変更するなどの部品変更を生じ難くすることが可能となる。

【００１１】

本発明では、通信端末の製造時において書き込み器により前記通信端末に必要事項を書き込み、当該通信端末とその通信相手とを無線通信させて、該通信端末が持つ各種情報を

前記通信相手に発信することにより、前記通信相手に必要事項を書き込んで登録作業を行う秘密鍵登録方法であって、前記通信端末への秘密鍵登録は、値が毎回変化する登録コードを前記書き込み器から前記通信端末に送るとともに、前記書き込み器において秘密鍵生成の一アルゴリズムである第１変換式により前記登録コードを演算して中間データを生成しつつ、当該中間データを前記通信端末に送り、前記通信端末において秘密鍵生成の他アルゴリズムである第２変換式により前記中間データを演算して、この演算結果を秘密鍵として前記通信端末に登録することにより行い、前記通信相手への秘密鍵登録は、前記通信端末が持つ前記登録コードを、無線通信を介して前記通信相手に発信し、前記通信相手において前記登録コード及び前記第１変換式による前記中間データの演算と、当該中間データ及び前記第２変換式による秘密鍵の演算とを行わせ、当該秘密鍵を前記通信相手に登録することにより行うことを要旨とする。

【発明の効果】

【００１２】

本発明によれば、秘密鍵の盗み取りを発生し難くすることができる。

【図面の簡単な説明】

【００１３】

【図１】一実施形態における電子キーシステムの概略構成を示すブロック図。

【図２】秘密鍵登録システムのキー側の構成要素を示すブロック図。

【図３】対キー秘密鍵登録作業の実行手順を示すフローチャート。

【図４】秘密鍵登録システムの車両側の構成要素を示すブロック図。

【図５】対車両秘密鍵登録作業の実行手順を示すフローチャート。

【発明を実施するための形態】

【００１４】

以下、本発明を具体化した秘密鍵登録システム及び秘密鍵登録方法の一実施形態を図１～図５に従って説明する。

図１に示すように、車両１には、車両キーとして使用される電子キー２との間で無線通信によりキー照合を行って、このキー照合の成立を条件にドアロックの施解錠やエンジン始動等が許可又は実行される電子キーシステム３が設けられている。なお、電子キー２は、車両１との間で狭域無線通信が可能であって、電子キー２が固有に持つＩＤコードを無線通信により車両１に発信して、車両１にキー照合としてＩＤ照合を行わせることが可能なキーのことをいう。なお、車両１が通信相手に相当し、電子キー２が通信端末に相当する。

【００１５】

電子キーシステム３には、電子キー（通称、ワイヤレスキー）２をボタン操作することによって遠隔操作により車両ドアのドアロックを施錠又は解錠するワイヤレスドアロックシステムがある。この場合、車両１には、電子キー２とＩＤ照合を行う照合ＥＣＵ４と、車両１の電源系を管理するメインボディＥＣＵ５とが設けられ、これらＥＣＵ４，５が車内の一ネットワークであるバス６を介して接続されている。照合ＥＣＵ４には、ＵＨＦ（Ultra High Frequency）帯（約312MHz）の信号を受信可能な車両チューナ７が接続されている。また、メインボディＥＣＵ５には、ドアロックの施解錠を実行するときの駆動源としてドアロックモータ８が接続されている。

【００１６】

また、電子キー２には、電子キー２の各種動作を統括制御する通信制御部９が設けられている。この通信制御部９は、ＣＰＵ１０やメモリ１１等の各種デバイスを持ち、電子キー２が持つ固有のキーコードとしてＩＤコードがメモリ１１に登録されている。電子キー２には、車両ドアを遠隔操作により施錠するときに操作する施錠ボタン１２と、車両ドアを遠隔操作により解錠するときに操作する解錠ボタン１３とが設けられ、これらボタン１２，１３の操作有無が通信制御部９によって管理されている。また、通信制御部９には、ＵＨＦ帯の無線信号を発信可能なキー発信機１４が接続され、キー発信機１４の信号発信動作が通信制御部９によって管理されている。

【００１７】
例えば、施錠ボタン１２が操作されると、通信制御部９は、電子キー２のＩＤコードと、車両１にドアロック施錠の動作開始を要求する機能コード（施錠要求コード）とを含んだワイヤレス信号Ｓwlをキー発信機１４からＵＨＦ帯の信号で発信させて、狭域無線通信（ワイヤレス通信）を実行する。そして、照合ＥＣＵ４は、車両チューナ７でこのワイヤレス信号Ｓwlを受信すると、ワイヤレス信号Ｓwlに含まれるＩＤコードを、自身のメモリ１５に登録されたＩＤコードと照らし合わせてＩＤ照合（ワイヤレス照合）を行う。照合ＥＣＵ４は、ワイヤレス照合の成立を確認すると、続く施錠要求コードに従い、メインボディＥＣＵ５にドアロックの施錠動作を実行させる。
【００１８】
ワイヤレス通信には、電子キー２から発信されるワイヤレス信号Ｓwlを暗号化して車両１に送る暗号通信が使用されている。本例の暗号通信には、信号の送り手と受け手とで共通の暗号鍵を使用する秘密鍵暗号方式が採用されている。よって、電子キー２のメモリ１１と、車両１（照合ＥＣＵ４）のメモリ１５とには、同じ秘密鍵１６が登録されている。そして、電子キー２がワイヤレス信号Ｓwlを発信する際には、電子キー２の秘密鍵１６によって暗号化されたワイヤレス信号Ｓwlが発信され、車両１がこのワイヤレス信号Ｓwlを受信すると、車両１側の秘密鍵１６でワイヤレス信号Ｓwlが復号される。
【００１９】
次に、車両１及び電子キー２への秘密鍵１６の登録について、その詳細を図２～図５に従って説明する。
秘密鍵１６の登録に際して、作業者はまず先に電子キー２に秘密鍵１６を登録する作業（対キー秘密鍵登録作業）から実行する。この登録作業は、電子キー２の製造ライン上で実行されるものであって、図２に示す書き込み器１７が使用される。書き込み器１７は、製造ライン上の一工程を担う工作機械の一種であり、この書き込み器１７を統括管理するＣＰＵ（図示略）や、各種データを保持可能なメモリ１８を備える。書き込み器１７は、この登録作業時において製造ライン上を流れてくる電子キー２の通信制御部９のＩＣ（Integrated Circuit）に対し、自身の電気配線１９を介して各種データを有線により直に注入可能となっている。
【００２０】
書き込み器１７のメモリ１８には、秘密鍵１６の生成に必要な関数として第１変換式Ｆ１(ｘ)が登録されている。第１変換式Ｆ１(ｘ)は、自身１つのみでは秘密鍵１６を生成できるものではなく、他の変換式と協同して秘密鍵１６を生成するという、秘密鍵生成の一要素として働く位置付けの演算式である。第１変換式Ｆ１(ｘ)は、一種のアルゴリズムであって、その種類は特に問うものではない。
【００２１】
また、書き込み器１７には、毎回異なるコード列をとる登録コードＣcdを管理する登録コード処理部２０と、秘密鍵１６になる一段階前の鍵情報である中間データＤckを生成する中間データ生成部２１とが設けられている。登録コードＣcdは、製造される電子キー２に関連付けられたコードであって、１つひとつのキーを製造する度に異なる値で出力される。登録コード処理部２０は、自身が生成した登録コードＣcdを電子キー２及び中間データ生成部２１に送出する。中間データ生成部２１は、登録コード処理部２０から受け付けた登録コードＣcdを第１変換式Ｆ１(ｘ)により演算して中間データＤckを生成するとともに、この中間データＤckを電子キー２に送出する。なお、登録コード処理部２０、中間データ生成部２１が通信端末側秘密鍵登録手段を構成する。
【００２２】
電子キー２のメモリ１１には、秘密鍵１６の生成に必要な関数として第２変換式Ｆ２(ｘ)が登録されている。第２変換式Ｆ２(ｘ)は、第１変換式Ｆ１(ｘ)と同じく、自身１つのみでは秘密鍵１６を生成できるものではなく、第１変換式Ｆ１(ｘ)と協同して秘密鍵１６を生成する演算式である。これら変換式Ｆ１(ｘ)，Ｆ２(ｘ)は、電子キー２側の第２変換式Ｆ２(ｘ)よりも、書き込み器１７側の第１変換式Ｆ１(ｘ)の方が、秘密鍵１６を生成

する際の演算比重、即ち変換式の量（計算量）が大きく設定されている。なお、第２変換式Ｆ２(ｘ)も一種のアルゴリズムであって、その種類は特に問わない。

【００２３】

また、電子キー２には、書き込み器１７から受け付けた登録コードＣcdをメモリ１１に書き込む登録コード書込部２２と、書き込み器１７から受け付けた中間データDckを基に秘密鍵１６を生成するキー側秘密鍵生成部２３とが設けられている。キー側秘密鍵生成部２３は、書き込み器１７から受け付けた中間データDckを第２変換式Ｆ２(ｘ)により演算することで秘密鍵１６を生成するとともに、この秘密鍵１６を電子キー側の暗号鍵としてメモリ１１に登録する。なお、登録コード書込部２２、キー側秘密鍵生成部２３が通信端末側秘密鍵登録手段を構成する。

【００２４】

続いて、対キー秘密鍵登録作業の実行手順を図３を使用して説明すると、ステップ１００に示すように、書き込み器１７において登録作業開始スイッチの操作等の登録開始操作が行われた際、対キー秘密鍵登録作業の開始を電子キー２に要求する登録作業開始要求が、書き込み器１７から電子キー２に出力される。電子キー２は、書き込み器１７から登録作業開始要求を受け付けると、ステップ１０１に示すように、自身の動作モードが秘密鍵登録モードに入るとともに、秘密鍵１６の登録が可能な旨を応答通知として書き込み器１７に出力する。

【００２５】

登録コード処理部２０は、電子キー２から応答通知を受け付けると、ステップ１０２に示すように、登録コードＣcdを生成する。そして、登録コード処理部２０は、ステップ１０３に示すように、生成したこの登録コードＣcdを電子キー２に転送する。なお、この転送時、登録コード処理部２０は、生成した登録コードＣcdを、電子キー２のみならず中間データ生成部２１にも転送する。

【００２６】

登録コード書込部２２は、書き込み器１７から登録コードＣcdを受け付けると、ステップ１０４に示すように、この登録コードＣcdを電子キー２のメモリ１１に書き込んで登録（保持）する。そして、登録コード書込部２２は、登録コードＣcdの登録が完了したことを確認すると、ステップ１０５に示すように、登録完了通知を書き込み器１７に出力する。

【００２７】

中間データ生成部２１は、電子キー２から登録完了通知を受け付けると、ステップ１０６に示すように、登録コード処理部２０から取得した登録コードＣcdを第１変換式Ｆ１(ｘ)により演算して中間データDckを生成する。そして、中間データ生成部２１は、ステップ１０７に示すように、この中間データDckを電子キー２に転送する。

【００２８】

キー側秘密鍵生成部２３は、電子キー２から中間データDckを受け付けると、ステップ１０８に示すように、書き込み器１７から取得した中間データDckを第２変換式Ｆ２(ｘ)により演算して秘密鍵１６を生成する。そして、キー側秘密鍵生成部２３は、ステップ１０９に示すように、この秘密鍵１６を電子キー２のメモリ１１に書き込んで登録（保持）する。これにより、電子キー２のメモリ１１にキー側の秘密鍵１６が登録された状態となる。なお、このとき、キー側秘密鍵生成部２３は、秘密鍵１６の登録が完了したことを確認すると、書き込み器１７から取得した中間データDckを、自身のメモリ１１から消去する。

【００２９】

キー側秘密鍵生成部２３は、秘密鍵１６の登録が完了したことを確認すると、ステップ１１０に示すように、秘密鍵登録完了通知を書き込み器１７に出力しつつ、自身の対キー秘密鍵登録作業を終了する。書き込み器１７は、電子キー２から秘密鍵登録完了通知を取得すると、対キー秘密鍵登録作業を終了する。そして、製造ライン上において書き込み器１７に電子キー２が流れてくる度に、以上の秘密鍵登録作業が繰り返し実行され、電子キ

ー２が自動生産される。

【００３０】

続いて、図４に示すように、今度は車両１に秘密鍵１６に登録する作業（対車両秘密鍵登録作業）が実行される。この登録作業は、例えば車両１の出荷前に実行されるものであって、大量生産された電子キー２の中の特定のものを、車両１の専用キーとして設定する作業にもなっている。また、対車両秘密鍵登録作業は、電子キーシステム３の部品群（通信インフラ）を利用して行うものであって、電子キーシステム３の通信プロトコルに準じた無線通信に沿って、車両１への秘密鍵１６の登録が実行される。

【００３１】

本例の場合、電子キー２には、書き込み器１７から受け付けてメモリ１１に保持しておいた登録コードＣcdを、キー発信機１４から転送する登録コード転送部２４が設けられている。また、照合ＥＣＵ４のメモリ１５には、書き込み器１７が持っていたものと同様の第１変換式Ｆ１(ｘ)と、電子キー２が持っていたものと同様の第２変換式Ｆ２(ｘ)とが登録されている。また、照合ＥＣＵ４には、電子キー２から取得した登録コードＣcdと、メモリ１５に登録された第１変換式Ｆ１(ｘ)及び第２変換式Ｆ２(ｘ)とを用いて秘密鍵１６を生成する車両側秘密鍵生成部２５が設けられている。なお、登録コード転送部２４、車両側秘密鍵生成部２５が通信相手側秘密鍵登録手段を構成する。

【００３２】

続いて、対車両秘密鍵登録作業の実行手順を図５を使用して説明すると、ステップ２０に示すように、車両１において例えば種々の車載機器を操作するなどして対車両秘密鍵登録作業開始操作が実行されると、ステップ２０１に示すように、車両１（実際は照合ＥＣＵ４）の動作モードが秘密鍵登録モードに切り換わる。即ち、車両１に秘密鍵１６の登録が可能な状態となる。

【００３３】

そして、例えば電子キー２において施錠ボタン１２や解錠ボタン１３が所定の回数及び順序で操作されると、登録コード転送部２４は、ステップ２０２に示すように、電子キー２のメモリ１１に登録された登録コードＣcdを、キー発信機１４からＵＨＦ帯の信号で車両１に向けて発信させる。なお、このときの電子キー２は、登録コードＣcdの発信のために一時的に立ち上がり、発信動作が終了すると待機状態に戻る。

【００３４】

車両側秘密鍵生成部２５は、車両１が秘密鍵登録モードに入っているときに登録コードＣcdを車両チューナ７で受信すると、ステップ２０３に示すように、受信した登録コードＣcdを第１変換式Ｆ１(ｘ)により演算して中間データＤckを生成する。そして、車両側秘密鍵生成部２５は、ステップ２０４に示すように、生成した中間データＤckを第２変換式Ｆ２(ｘ)により演算して秘密鍵１６を生成する。その後、車両側秘密鍵生成部２５は、ステップ２０５に示すように、この秘密鍵１６を照合ＥＣＵ４のメモリ１５に書き込んで登録（保持）する。これにより、車両１のメモリ１５に車側の秘密鍵１６が登録された状態となる。

【００３５】

照合ＥＣＵ４は、メモリ１５に秘密鍵１６が登録されたことを確認すると、ステップ２０６に示すように、例えば車両１のハザードを数回点滅させたり、或いはホーンを数回鳴らしたりするなどして、秘密鍵登録が完了したことを作業者に通知する。以上により、電子キー２への秘密鍵１６の登録と、車両１への秘密鍵１６の登録との両方が完了した後、これらを組として市場に出荷する。

【００３６】

さて、本例においては、電子キー製造時に書き込み器１７に登録コードＣcdを電子キー２に乗せておき、車両１への秘密鍵１６の登録は、この電子キー２及び車両１の電子キーシステム３に準じた無線通信を電子キー２が車両１と行う際、電子キー２に乗せた登録コードＣcdを車両１に送り、車両１自身に秘密鍵１６を演算させて車両１に登録する。即ち、秘密鍵１６自体を電子キー２から車両１に無線通信により直に直接送って車両１に書き

込む方式は用いずに、車両１に自ら秘密鍵１６の演算を実行させる登録方式をとる。これは、秘密鍵１６を直に発信してしまうと、この秘密鍵１６が盗聴される可能性も否めないからである。

【００３７】

ところで、本例のような秘密鍵１６の登録方式を採用した場合、背景技術の問題点でも挙げたように、車両盗難の一行為として、例えば書き込み器１７の内容（即ち、第１変換式Ｆ１(ｘ)）を盗み取り、しかも車両１への秘密鍵登録時に、電子キー２から発信される登録コードＣcdを盗聴するという盗難行為が企てられることも想定される。しかし、この場合、盗難者の手元には、登録コードＣcd及び第１変換式Ｆ１(ｘ)しかなく、秘密鍵１６の演算に必要な第２変換式Ｆ２(ｘ)がないので、秘密鍵１６を割り出すことができない。よって、前述した盗難行為が企てられても秘密鍵１６がばれないので、秘密鍵１６の登録方式を秘密鍵１６の盗難に対して耐性の高いものとすることが可能となる。

【００３８】

本実施形態の構成によれば、以下に記載の効果を得ることができる。

（１）書き込み器１７に第１変換式Ｆ１(ｘ)を設けるとともに、電子キー２に第２変換式Ｆ２(ｘ)を設けることにより、これら２者の両方に変換式を用意し、登録コードＣcdから秘密鍵１６を求める演算作業を、これら書き込み器１７及び電子キー２の両方の機器に亘るようにした。よって、秘密鍵１６を演算するのに必要なパラメータが増えるので、もし仮に秘密鍵１６を盗難しようとした際には、これら全てのパラメータを用意しなくてはならなくなる。よって、秘密鍵１６の盗み取りを発生し難くすることができ、ひいては車両盗難に対するセキュリティ性も高くすることができる。

【００３９】

（２）電子キー２に秘密鍵１６が登録された後、電子キー２が書き込み器１７から取得した中間データＤckは電子キー２のメモリ１１から消去されるので、秘密鍵１６の登録完了後、電子キー２には中間データＤckが残ったままの状態とならない。よって、電子キー２から中間データＤckを入手するという不正行為が行われずに済むので、秘密鍵１６の盗難に対するセキュリティ性を、より高いものとすることができる。

【００４０】

（３）書き込み器１７だけでなく電子キー２にも変換式を持たせるに際して、電子キー２に乗せる第２変換式Ｆ２(ｘ)よりも、書き込み器１７に乗せる第１変換式Ｆ１(ｘ)の方を、計算量を多いものにした。このため、電子キー２に乗せる変換式は計算量が少ないもので済むので、電子キー２のメモリ１１を大きなメモリ容量を持つものに変更せずに済む。

【００４１】

なお、実施形態はこれまでに述べた構成に限らず、以下の態様に変更してもよい。

・　電子キーシステム３は、必ずしもワイヤレスドアロックシステムに限定されず、例えば車両１からのＩＤ返信要求に応答して電子キー２がＩＤコードを自動で返すキー操作フリーシステムとしてもよい。

【００４２】

・　秘密鍵暗号の種類は、DES（Data Encryption Standard）、FEAL（Fast data Encipherment ALgorithm）、MISTY（ミスティー）、IDEA（International Data Encryption Algorithm）など、種々のものが採用可能である。

【００４３】

・　電子キー２や車両１に登録されている変換式（第１変換式Ｆ１(ｘ)、第２変換式Ｆ２(ｘ)）は、登録作業後に消去されてもよい。

・　書き込み器１７は、電子キー２に登録コードＣcdや中間データＤckを必ずしも有線で送るものに限らず、これらを無線で送るものでもよい。

【００４４】

・　書き込み器１７は、生成した中間データＤckを電子キー２に送った後、これを自身から消去する動作をとってもよい。

・　電子キー２への秘密鍵１６の登録は、必ずしも電子キー製造時に実行されることに限定されず、例えば車両ディーラにおいて実行されてもよい。なお、登録タイミングが限定されないことは、車両１への秘密鍵１６の登録でも同様に言える。

【００４５】

・　対車両秘密鍵登録作業において、車両１を秘密鍵登録モードに入らせるトリガは、必ずしも車両機器を所定操作することに限定されない。例えば、コンピュータ等のツールを車両１に接続し、同ツールから指令を車両１に送って、車両１を秘密鍵登録モードに切り換えてもよい。

【００４６】

・　第１変換式Ｆ１(ｘ)及び第２変換式Ｆ２(ｘ)の計算量の重み付けは、第２変換式Ｆ２(ｘ)よりも第１変換式Ｆ１(ｘ)の計算量を多くすることに限らず、これを逆としてもよい。また、第１変換式Ｆ１(ｘ)及び第２変換式Ｆ２(ｘ)は、同じ計算量をとるものでもよい。

【００４７】

・　中間データＤckは、自身のみでは秘密鍵１６を満たすことができない仮秘密鍵の位置付けのデータとして定義する。

・　本例の秘密鍵１６登録方式は、車両１に適用されることに限らず、２機器が暗号通信を行うシステムであれば、特に限定されない。即ち、通信端末は、必ずしも電子キー２に限らず、どのような種の端末でもよいし、通信相手は、必ずしも車両１に限らず、端末との間で認証を行うものであれば、どのような種のものでもよい。

【００４８】

・　書き込み器１７、電子キー２、車両１の各々に設けた各処理部は、ＣＰＵが本例の秘密鍵登録用の制御プログラムを実行することで機能的に生成されるものであって、本例においてはこれらをブロック図で図示している。

【００４９】

次に、上記実施形態及び別例から把握できる技術的思想について、それらの効果とともに以下に追記する。

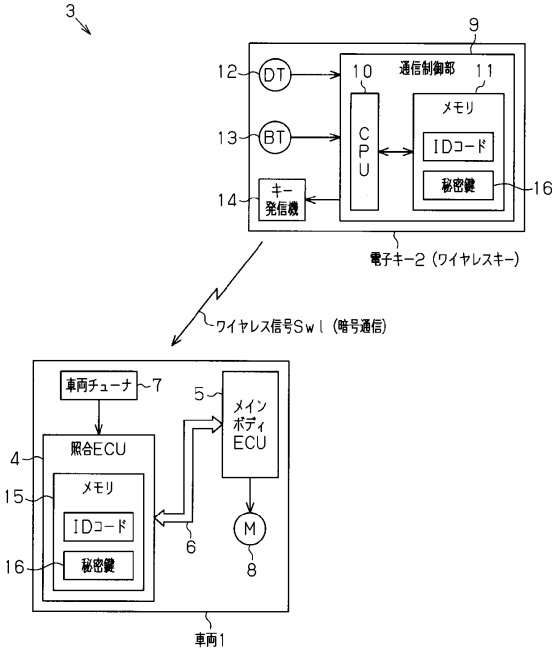
（１）請求項１～３のいずれかにおいて、前記通信相手を車両とし、前記通信端末を当該車両の電子キーとして、車両用の電子キーシステムに適用されている。この構成によれば、電子キー及び車両に登録される秘密鍵が盗難され難くなるので、車両が盗難に遭う可能性を低く抑えることが可能となる。

【符号の説明】

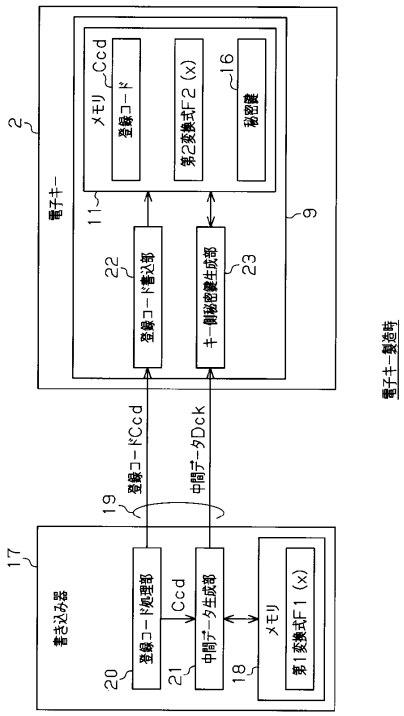
【００５０】

１…通信相手としての車両、２…通信端末としての電子キー、１６…秘密鍵、１７…書き込み器、２０…通信端末側秘密鍵登録手段を構成する登録コード処理部、２１…通信端末側秘密鍵登録手段を構成する中間データ生成部、２２…通信端末側秘密鍵登録手段を構成する登録コード書込部、２３…通信端末側秘密鍵登録手段を構成するキー側秘密鍵生成部、２４…通信相手側秘密鍵登録手段を構成する登録コード転送部、２５…通信相手側秘密鍵登録手段を構成する車両側秘密鍵生成部、Ｃcd…必要事項を構成する登録コード、Ｄck…必要事項を構成する中間データ、Ｆ１(ｘ)…第１変換式、Ｆ２(ｘ)…第２変換式。

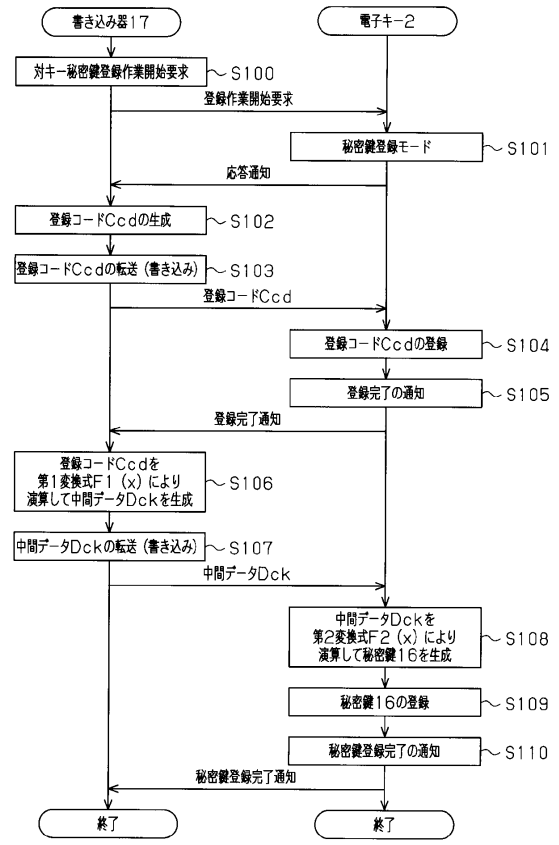
【図１】


3
9
12
DT
10
通信制御部
11
メモリ
13
BT
CPU
IDコード
秘密鍵
16
14
キー発信機
電子キー2（ワイヤレスキー）
ワイヤレス信号Swl（暗号通信）
車両チューナ
7
5
メインボディECU
照合ECU
4
メモリ
15
IDコード
秘密鍵
16
6
M
8
車両1

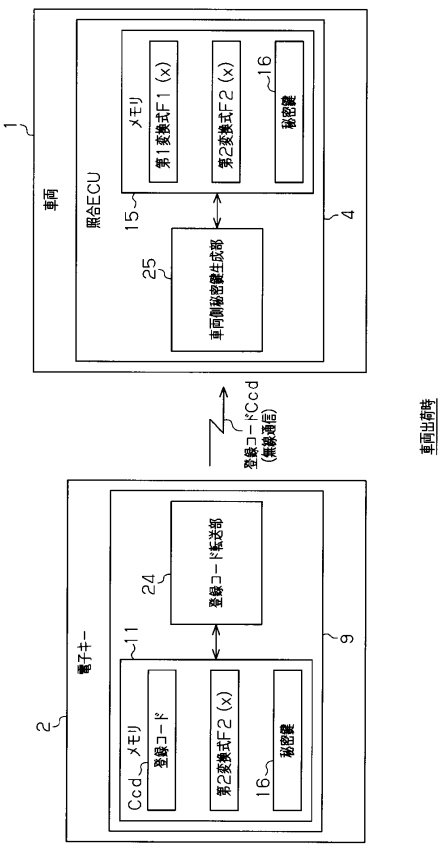
【図２】


2
電子キー
メモリ
Ccd
登録コード
第2変換式F2（x）
16
秘密鍵
11
9
22
登録コード書込部
キー側秘密鍵生成部
23
登録コードCcd
中間データDck
19
17
書き込み器
登録コード処理部
Ccd
中間データ生成部
メモリ
第1変換式F1（x）
20
21
18
電子キー製造時

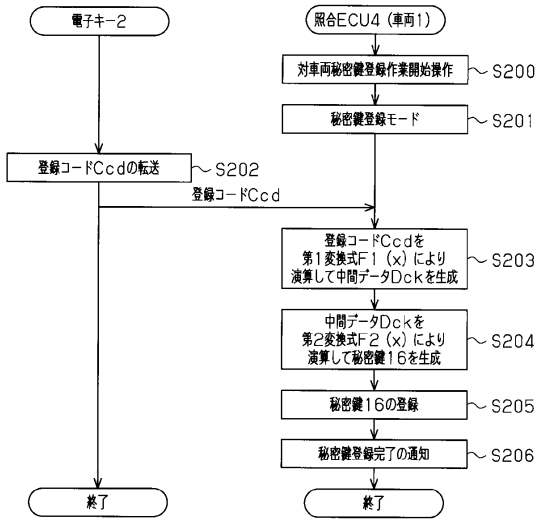
【図３】


書き込み器17
電子キー2
対キー秘密鍵登録作業開始要求
S100
登録作業開始要求
秘密鍵登録モード
S101
応答通知
登録コードCcdの生成
S102
登録コードCcdの転送（書き込み）
S103
登録コードCcd
登録コードCcdの登録
S104
登録完了の通知
S105
登録完了通知
登録コードCcdを第1変換式F1（x）により演算して中間データDckを生成
S106
中間データDckの転送（書き込み）
S107
中間データDck
中間データDckを第2変換式F2（x）により演算して秘密鍵16を生成
S108
秘密鍵16の登録
S109
秘密鍵登録完了の通知
S110
秘密鍵登録完了通知
終了
終了

【図４】


1
車両
照合ECU
メモリ
第1変換式F1（x）
第2変換式F2（x）
16
秘密鍵
15
4
25
車両側秘密鍵生成部
登録コードCcd（無線通信）
2
電子キー
11
登録コード送信部
24
9
Ccd
メモリ
登録コード
第2変換式F2（x）
16
秘密鍵
車両出荷時

【図５】


電子キー2
照合ECU4（車両1）
対車両秘密鍵登録作業開始操作
S200
秘密鍵登録モード
S201
登録コードCcdの転送
S202
登録コードCcd
登録コードCcdを
第1変換式F1（x）により
演算して中間データDckを生成
S203
中間データDckを
第2変換式F2（x）により
演算して秘密鍵16を生成
S204
秘密鍵16の登録
S205
秘密鍵登録完了の通知
S206
終了
終了

フロントページの続き

(72)発明者　岸本　耕平
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
(72)発明者　名和　佑記
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
(72)発明者　水野　善之
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
(72)発明者　水野　博光
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
(72)発明者　古賀　進一
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
(72)発明者　西田　耕太
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
(72)発明者　伊藤　智大
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
(72)発明者　河合　英樹
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

審査官　松平　英

(56)参考文献　特開２００１－２９５５２１（ＪＰ，Ａ）
特開２００６－７２４１４（ＪＰ，Ａ）
米国特許出願公開第２００６／０１０７０６８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２４
Ｂ６０Ｒ　２５／００
Ｂ６０Ｒ　２５／１０
Ｅ０５Ｂ　４９／００
Ｅ０５Ｂ　６５／００