(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3555345号
(P3555345)
(45)発行日　平成16年8月18日(2004.8.18)　(24)登録日　平成16年5月21日(2004.5.21)

(51)Int.Cl.[7]　F I
G07B 15/00　G07B 15/00　510
H04L 9/10　H04L 9/00　621A

請求項の数 4　(全 12 頁)

(21)出願番号　特願平8-210812
(22)出願日　平成8年8月9日(1996.8.9)
(65)公開番号　特開平10-55463
(43)公開日　平成10年2月24日(1998.2.24)
審査請求日　平成14年9月12日(2002.9.12)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　小林　健二
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所マルチメディアシステム開発本部内
(72)発明者　坂本　敏幸
神奈川県横浜市戸塚区吉田町２９２番地株式会社日立製作所マルチメディアシステム開発本部内

最終頁に続く

(54)【発明の名称】自動料金収受システムの車載機

(57)【特許請求の範囲】

【請求項１】

道路側に設置した路側機との間で料金支払いに関する収受情報を送受信して利用料金を徴収する自動料金収受システムに用いられる車載機において、

前記路側機と通信するための通信手段と、

前記収受情報を処理するための収受情報処理手段と、

前記通信手段から前記路側機に送信される前記収受情報処理手段の収受情報等の通信文を暗号化する暗号化手段と、

前記通信手段で受信された前記路側機からの暗号化された通信文を復号化する復号化手段と、

前記暗号化手段と前記復号化手段で使用する暗号鍵を保持する暗号鍵記憶手段と、

車載機に固有の識別情報を保持する識別情報記憶手段と、

前記通信手段から前記路側機に送信される前記識別情報記憶手段の識別情報を暗号化せずに送信させる識別制御手段とを有し、

少なくとも、前記暗号化手段と前記復号化手段と前記暗号鍵記憶手段と前記識別情報記憶手段と前記識別制御手段とを、一体に封止した半導体装置として構成したことを特徴とする自動料金収受システムの車載機。

【請求項２】

請求項１記載の自動料金収受システムの車載機において、前記識別情報は前記路側機との通信開始時に前記通信手段から前記路側機に送信されることを特徴とする自動料金収受シ

ステムの車載機。
【請求項３】
道路側に設置した路側機との間で料金支払いに関する収受情報を送受信して利用料金を徴収する自動料金収受システムに用いられる車載機において、
前記路側機と通信するための通信手段と、
前記収受情報を処理するための収受情報処理手段と、
前記通信手段から前記路側機に送信される前記収受情報処理手段の収受情報等の通信文を暗号化する暗号化手段と、
前記通信手段で受信された前記路側機からの暗号化された通信文を復号化する復号化手段と、
前記暗号化手段と前記復号化手段で使用する暗号鍵を保持する暗号鍵記憶手段と、
車載機に固有の識別情報を保持する識別情報記憶手段とを有し、
前記暗号化手段と前記復号化手段と前記暗号鍵記憶手段と前記識別情報記憶手段とを一つの集積回路として構成し、前記識別情報記憶手段の識別情報を暗号化せずに通信手段に送ることを特徴とする自動料金収受システムの車載機。
【請求項４】
請求項３記載の自動料金収受システムの車載機において、前記識別情報は前記路側機との通信開始時に前記通信手段から前記路側機に送信されることを特徴とする自動料金収受システムの車載機。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、有料道路を通行する車両と道路側に設置した路側機の間で利用料金の情報を通信しあうことで、自動的に利用料金を徴収する自動料金収受システムと、この通信ために車両に搭載される車載機に関する。
【０００２】
【従来の技術】
近年、有料道路を通行する車両から料金を自動的に徴収する、自動料金収受システムが研究されている。この技術は、車両に搭載した車載機と、道路側に設置された路側機との間で、電波などを使った路車間通信を行い、料金支払いに関する情報を交換して、料金を決済するものである。
【０００３】
具体的な決済の方法としては、たとえば、車載機に事前に現金と引き換えに相当額の残金情報を書き込み、料金徴収の際に路側機から車載機に利用料金の請求情報を送り、これに従い車載機が残金情報から利用金額を差し引くことが考えられている。
【０００４】
また、車両の通行した経路や車種によって料金を変えるには、経路や車種の情報を車載機から路側機に伝えることで対応することが考えられている。
【０００５】
【発明が解決しようとしている課題】
上記の自動料金収受システムでは、金銭に関する情報を通信で交換し、かつ、その内容に従って実際に料金を決済するので、通信内容を偽るなどの不正利用を防止する対策が必要である。この対策の一つとして通信内容を暗号化する事が考えられる。
【０００６】
路側機と車載機の間の通信を暗号化した場合、路側機は不特定多数の車載機が送信してくる暗号文を復号化できなければならない。このため、少なくとも暗号のアルゴリズムは自動料金収受システム全体で統一していなければならない。また、暗号に使う暗号鍵は、車載機ごとに別な物を持たせる方法や、自動料金収受システム全体で１つの鍵を持たせる方法などが考えられるが、いずれにしろ暗号鍵が漏洩しないように厳重に管理する必要がある。

【０００７】
一方、車載機の設計、製造は、自動料金収受システムの管理者が行うとは限らない。種々の車種に合わせてさまざまな形態の車載機を設計、製造することは、製造業者が実施した方が効率的だからである。
【０００８】
この場合、暗号アルゴリズムや暗号鍵に接する人間が増え、漏洩しないように管理する事が難しくなる。また製造業者から見ても、暗号アルゴリズムや暗号鍵の取り扱いに腐心するのは本意でないため、その内容を隠蔽したまま扱えることが好ましい。
【０００９】
本発明の目的は、車載機の設計、製造者と暗号鍵の管理者が異なる場合に、暗号鍵を隠蔽したまま、設計、製造することができる、自動料金収受システムの車載機を提供することである。
【００１０】
【課題を解決するための手段】
上記の課題を解決するために、収受情報の処理や車載機の表示などを制御する車載機制御手段と、路車間で通信する機能を持つ通信手段との間に、暗号化手段と復号化手段を設け、加えて暗号化と復号化に必要な暗号鍵の記憶手段を設け、前記の暗号化手段と前記復号化手段が直接読み込めるようにする。
【００１１】
前記暗号化手段と前記復号化手段が暗号鍵を直接読み込むので、前記暗号化手段、前記復号化手段を利用する前記車載機制御手段が、前記暗号鍵の転送やその内容を考慮する必要がない。
【００１２】
また暗号鍵の転送は、前記暗号鍵の記憶手段から前記暗号化手段と前記復号化手段の間だけに限られるので、暗号鍵の漏洩防止の管理がしやすくなる。また、車載機に固有の識別情報を保持する識別情報記憶手段と、前記識別情報記憶手段の内容を暗号化手段を通さずに通信手段に送る識別制御手段とを有し、少なくとも、前記暗号化手段と前記復号化手段と前記暗号鍵の記憶手段と前記識別情報記憶手段と前記識別制御手段とを、一体に封止した半導体装置として構成するようにする。
【００１３】
【発明の実施の形態】
以下に本発明による自動料金収受システムの車載機の１実施例を示す。図１はこの実施例の車載機のブロック図である。図１において１は車載機全体であり、２は路側機である。
【００１４】
車載機１は、路側機２と通信するためのアンテナ１１と、アンテナ１１に接続された路車間通信器１２と、料金収受の処理をする車載機制御器１４と、車載機制御器１４と路車間通信器１２の間にある暗号化装置１３とからなる。
【００１５】
暗号化装置１３は、その中に、暗号化器１３１と復号化器１３２と暗号鍵保存用メモリ１３３と識別情報保存用メモリ１３４と識別制御器１３５とスイッチ１３６を持つ。
【００１６】
車載機制御器１４は、その中に、車載機制御器１４全般を制御する主制御器１４１と、残金の情報を保存する残金情報保存用メモリ１４２と、車載機１が設置されている車両の車種などの情報を保存する車両情報保存用メモリ１４３と、車両が通過してきた経路を記録、保存する経路情報保存用メモリ１４４を持つ。
【００１７】
路側機２は、車載機１と通信するための路側機アンテナ２１と、路側機アンテナ２１に接続された路側機路車間通信器２２と、料金収受の通信を制御する路側機制御装置２４と、路側機路車間通信器２２と路側機制御装置２４の間にある路側機暗号化装置２３と、暗号鍵検索装置２５と、識別情報－暗号鍵対応表記憶手段２６を持つ。路側機２はその他に表

示装置などの構成要素を持つことができるが、本発明の本質に関係しないので図１に図示しない。

【００１８】

路車間通信器１２は、暗号化装置１３から通信器１２に渡された情報をアンテナ１１を通して路側機２に送信する。また、路側機２から送られた情報をアンテナ１１を通して受信し、暗号化装置１３に渡す。

【００１９】

暗号化器１３１は車載機制御器１４から送られた通信文を暗号化して路車間通信器１２に渡し、復号化器１３２は路車間通信器１２から暗号化された通信文を受け取って、復号化した後に車載機制御器１４に渡す。また、前記の暗号化と復号化の処理に使う暗号鍵を保存するための暗号鍵保存用メモリ１３３が、暗号化器１３１と復号化器１３２に接続されており、暗号化器１３１と復号化器１３２は暗号鍵を暗号鍵保存用メモリ１３３から得る。識別情報保存用メモリ１３４は車載機１台１台を識別する情報を内容として持ち、この情報と前記の暗号鍵は、自動料金収受システムの管理者によってあらかじめ識別情報保存用メモリ１３４と暗号鍵保存用メモリ１３３とにそれぞれ設定されている。また自動料金収受システムの管理者は、すべての車載機の識別情報と暗号鍵の対応関係を識別情報－暗号鍵対応表記憶手段２６に記録する。スイッチ１３６は、識別制御器１３５が制御することにより、路車間通信器１２への出力元を、暗号化器１３１と識別情報保存用メモリ１３４との間で切り替える。識別制御器１３５は路車間通信の開始時にスイッチ１３６を制御して、前記の識別情報保存用メモリ１３４の内容である識別情報を、暗号化せずに路車間通信器１２を通して路側機２に送る。

【００２０】

車載機１から送信された識別情報は、路側機アンテナ２１で受信され、路側機暗号化装置２３を通して路側機制御装置２４に送られる。路車間通信の開始時には、路側機暗号化装置２３は動作しておらず、識別情報はそのまま路側機制御装置２４に達する。

【００２１】

路側機制御装置２４は、識別情報が送られてくると、識別情報を暗号鍵検索装置２５に送る。暗号鍵検索装置２５は、送られた識別情報と、識別情報－暗号鍵対応表記憶手段２６の内容から、識別情報に対応する暗号鍵を検索し、路側機暗号化装置２３に設定する。ここで得られる暗号鍵は、自動料金収受システムの管理者が車載機１に設定したものと同じなので、路側機２は車載機１と同じ暗号鍵で暗号化、復号化することができるようになる。これ以後、車載機制御装置１４と路側機制御装置２４は、暗号化装置１３と路側機暗号化装置２３によって暗号化された、料金収受のための通信を始める。

【００２２】

車載機制御器１４の主制御器１４１は、料金収受の通信の際に、あらかじめ決められた手順で車種や経路の情報を路側機２に送る。また、主制御器１４１は、路側機２から確定した支払料金の情報を受け取ると、残金情報保存用メモリ１４２に保存された残金情報から差し引き、新しい残金情報を残金情報保存用メモリ１４２に書き込み、料金の決済をする。

【００２３】

以上に示した動作によって、路側機２と車載機制御装置１４は料金収受に関する情報を通信しあい、料金の決済をする。その間、車載機１に搭載された暗号化装置１３は通信文の暗号化と復号化の処理を行っているが、車載機制御器１４はその動作を制御しなくとも良い。特に、漏洩しないように管理する必要がある暗号鍵は暗号化装置１３から外に出ることがないため、漏洩防止の管理は暗号化装置１３に限定することができる。車載機制御器１４は漏洩防止の管理の対象に含めなくとも良いため、その設計や製造、配布が容易になる。

【００２４】

次に本発明による自動料金収受システムの車載機の別の実施例を示す。本実施例では先の実施例の構成と機能に加え、通信開始後、料金収受の情報を交換する前に、前記車載機と

前記路側機との間で相互認証を行ない、その制御、実行の機能を前記暗号化装置に持たせたのが特徴である。

【００２５】

図２はこの実施例の車載機のブロック図である。アンテナ１１と路車間通信器１２と車載機制御器１４の構成と動作は先の実施例と同じで有るため説明を省略する。路側機２は、構成は先の実施例と同じで有るが、路側機制御装置２７の動作を変更したため、その動作を暗号化器１３の動作とともに説明する。暗号化装置１３の構成と動作を以下に説明する。

【００２６】

暗号化装置１３は、暗号化器１３１と復号化器１３２と暗号鍵保存用メモリ１３３と識別情報保存用メモリ１３４と識別・認証制御器１３５と２つのスイッチ１３７と１３８を持つ。

【００２７】

暗号化器１３１は車載機制御器１４から送られた通信文を暗号化して路車間通信器１２に渡し、復号化器１３２は路車間通信器１２から暗号化された通信文を受け取って、復号化した後に車載機制御器１４に渡す。暗号化器１３１と復号化器１３２は、動作と非動作の状態を識別・認証制御器１３５により制御され、非動作の状態では入力された通信文を暗号化、復号化しないでそのまま出力する。また、前記の暗号化と復号化の処理に使う暗号鍵を保存するための暗号鍵保存用メモリ１３３が、暗号化器１３１と復号化器１３２に接続されており、暗号化器１３１と復号化器１３２は暗号鍵を暗号鍵保存用メモリ１３３から得る。識別情報保存用メモリ１３４は車載機１台１台を識別する情報を内容として持ち、この情報と前記の暗号鍵は、自動料金収受システムの管理者によってあらかじめ識別情報保存用メモリ１３４と暗号鍵保存用メモリ１３３とにそれぞれ設定されている。また自動料金収受システムの管理者は、すべての車載機の識別情報と暗号鍵の対応関係を識別情報－暗号鍵対応表記憶手段２６に記録する。

【００２８】

識別・認証制御器１３５は、路車間通信の開始時に識別情報を路側機２に送る機能と、あらかじめ定められた手順で路側機２と通信することにより車載機１と路側機２で相互認証する機能を持つ。

【００２９】

第１のスイッチ１３７は、識別・認証制御器１３５から制御することにより、暗号化器１３１への入力元を、車載機制御器１４と識別・認証制御器１３５との間で切り替える。第２のスイッチ１３８は、識別・認証制御器１３５から制御することにより、復号化器１３２からの出力先を、車載機制御器１４と識別・認証制御器１３５との間で切り替える。

【００３０】

次に、路車間通信開始時から、料金収受の情報を交換するまでの識別・認証制御器１３５と路側機制御器２７の動作を、図５と図６にそって説明する。図５は識別・認証制御器１３５の動作を表したフローチャートであり、図６は路側機制御器２７の動作を表したフローチャートである。

【００３１】

なお、これは識別、認証の手順の１実施例であり、その他にも識別、認証を実現する手順が存在する事は言うまでもない。

【００３２】

（１）識別・認証制御器１３５は、初期設定として暗号化器１３１、復号化器１３２を非動作状態にし、第１のスイッチ１３７と第２のスイッチ１３８を識別・認証制御器１３５側に切り替える。その後、路側機２からの通信開始要求が受信されていないかを監視する。

【００３３】

路側機制御装置２４は、初期設定として路側機暗号化装置２３を非動作状態にし、通信開始要求を車載機１に向けて継続的に発信する。同時に、車載機からの応答がないかを監視

する。
【００３４】
（２）車両が進行し、車載機１が路側機２と通信可能な範囲に入ると、路側機２の発信した通信開始要求は、路車間通信器１２、非動作状態の復号化器１３２、第２のスイッチ１３８を経由して識別・認証制御器１３５に入る。識別・認証制御器１３５は通信開始要求を受け取ると、識別情報を識別情報保存用メモリ１３４から読みだし、第１のスイッチ１３７、非動作状態の暗号化器１３１、路車間通信器１２を通して路側機２に送る。
【００３５】
この後、識別・認証制御器１３５は路側機２からの応答を監視する。
【００３６】
（３）車載機１から送信された識別情報は、路側機路車間通信器２２、非動作状態の路側機暗号化装置２３を経由して路側機制御装置２４に入る。路側機制御装置２４は、識別情報を受け取ると、暗号鍵検索装置２５に送る。暗号鍵検索装置２５は、受け取った識別情報に対応する暗号鍵を、識別情報－暗号鍵対応表記憶手段２６の中から検索し、路側機暗号化装置２３に設定する。ここで識別情報－暗号鍵対応表記憶手段２６の内容である識別情報－暗号鍵の対応関係は、自動料金収受システムの管理者が車載機に設定した識別情報と暗号鍵を記録したものなので、路側機暗号化装置２３に設定される暗号鍵は、車載機１の暗号化装置１３が使用する暗号鍵と同じものである。
【００３７】
次に、路側機制御装置２４は乱数Ｒ１を発生し、車載機１に向けて送信する。この後、路側機暗号化装置２３を動作状態にし、車載機からの応答を監視する。
【００３８】
（４）識別・認証制御器１３５は、路側機２から送られてきた乱数Ｒ１を受け取ると、暗号化器１３１、復号化器１３２を動作状態にする。次に、乱数Ｒ２を発生し、路側機２から送られてきた乱数Ｒ１に続けて路側機２に送信する。この際、暗号化器１３１が動作状態になっているため、通信内容は暗号化される。ここで暗号化された乱数Ｒ１とＲ２をｅ（Ｒ１｜Ｒ２）と表記する。この後、識別・認証制御器１３５は路側機２からの応答を監視する。
【００３９】
（５）車載機１から送られてきたｅ（Ｒ１｜Ｒ２）は、路側機２の暗号化装置２３を通過する際に復号化される。ここで復号化した結果をＲ１’と表記する。路側機２と車載機１の暗号鍵が一致するなら、Ｒ１’とＲ１は一致するが、もし路側機２と車載機１の暗号鍵が別のものならば、Ｒ１’とＲ１は一致しない。
【００４０】
路側機制御器２４は、Ｒ１’とＲ１が一致したならば、認証が正常に終了したとして次の処理に入るが、もし一致しない場合は（１）の初期状態に戻る。
【００４１】
次に路側機制御器２４は、乱数Ｒ２を車載機１に向けて返信する。乱数Ｒ２は、路側機暗号化装置２３で暗号化されて送信される。ここで暗号化した乱数Ｒ２をｅ（Ｒ２）と表記する。この後、路側機制御器２４は、車載機１からの次の通信を待って料金収受処理に入る。
【００４２】
（６）路側機２から送られたｅ（Ｒ２）は、復号化器１３２で復号化された後に識別・認証制御器１３５に入る。ここで、復号化した結果をＲ２’と表記する。
【００４３】
路側機２と車載機１側の暗号鍵が一致するなら、Ｒ２’とＲ２は一致するが、もし路側機２と車載機１の暗号鍵が別のものならば、Ｒ２’とＲ２は一致しない。識別・認証制御器１３５は、Ｒ２’とＲ２が一致すれば、認証が正常に終了したとして、第１のスイッチ１３７の入力元と第２のスイッチ１３８の出力先を、識別・認証制御器１３５から車載機制御器１４に切り替え、車載機制御器１４と路側機２が通信できるようにする。

【００４４】
もしＲ２’とＲ２が一致しなければ、認証できなかったものとして、（１）の初期状態に戻る。
【００４５】
上記のように車載機１と路側機２の両方で認証が正常に終われば、その後は車載機制御器１４と路側機２が通信しあって料金収受の処理を進めるが、もし認証が正常に終わらなければ料金収受の処理には入らない。
【００４６】
本実施例では、暗号化装置１３が路側機２と通信しあって相互認証を行なうので、車載機制御装置１４は最低限、料金収受の処理の機能を持つだけで良い。また相互認証の手順を秘密にしたい場合、相互認証の手順は識別・認証制御装置１３５の中に有るので、暗号鍵などの他の秘密にしたい情報とともに暗号化装置１３全体を管理することで、相互認証の手順が漏洩するのを防止することが容易になる。
【００４７】
次に本発明による自動料金収受システムの車載機のさらに別の実施例を示す。本実施例では先の実施例と同様に、前記車載機と前記路側機との間で相互認証を行なうが、その制御、実行の機能を前記主制御器に持たせたのが特徴である。
【００４８】
図３はこの実施例の車載機のブロック図である。本実施例は、暗号化装置１３と主制御器１４１の動作以外は先の実施例と同じで有るため、それ以外の部分の説明は省略する。
【００４９】
暗号化装置１３は、その中に、暗号化器１３１と復号化器１３２と暗号鍵保存用メモリ１３３と識別情報保存用メモリ１３４と識別制御器１３５とスイッチ１３６を持つ。
【００５０】
暗号化器１３１は車載機制御器１４から送られた通信文を暗号化して路車間通信器１２に渡し、復号化器１３２は路車間通信器１２から暗号化された通信文を受け取って、復号化した後に車載機制御器１４に渡す。暗号化器１３１と復号化器１３２は、動作と非動作の状態を主制御器１４１により制御され、非動作の状態では入力された通信文を暗号化、復号化しないでそのまま出力する。また、前記の暗号化と復号化の処理に使う暗号鍵を保存するための暗号鍵保存用メモリ１３３が、暗号化器１３１と復号化器１３２に接続されており、暗号化器１３１と復号化器１３２は暗号鍵を暗号鍵保存用メモリ１３３から得る。
【００５１】
識別情報保存用メモリ１３４は車載機１台１台を識別する情報を内容として持ち、この情報と前記の暗号鍵は、自動料金収受システムの管理者によってあらかじめ識別情報保存用メモリ１３４と暗号鍵保存用メモリ１３３とにそれぞれ設定されている。また自動料金収受システムの管理者は、すべての車載機の識別情報と暗号鍵の対応関係を識別情報－暗号鍵対応表記憶手段２６に記録する。
【００５２】
スイッチ１３６は、識別制御器１３５が制御することにより、路車間通信器１２への出力元を、暗号化器１３１と識別情報保存用メモリ１３４との間で切り替える。
【００５３】
識別制御器１３５は路車間通信の開始時にスイッチ１３６を制御して、前記の識別情報保存用メモリ１３４の内容である識別情報を、暗号化せずに路車間通信器１２を通して路側機２に送る。
【００５４】
本実施例では、主制御器１４１は料金収受の通信を制御する機能に加えて、相互認証の通信の手順を制御する機能を持つ。手順の詳細は先の実施例と同じであるため、説明を省略する。
【００５５】
本実施例によれば、例えば相互認証の手順としてＩＳＯ９７９８－２で定められた認証手

順を利用した場合、認証の途中から料金収受のための通信を同送することができ、通信回数を減らすことができる。

【００５６】

次に本発明による自動料金収受システムの車載機のさらに別の実施例を示す。本実施例では先の実施例の識別制御装置の機能を前記主制御器１４１に持たせたのが特徴である。

【００５７】

図４はこの実施例の車載機のブロック図である。本実施例は、暗号化装置１３の構成と主制御器１４１の動作以外は先の実施例と同じなので、それ以外の部分の説明は省略する。

【００５８】

暗号化装置１３は、その中に、暗号化器１３１と復号化器１３２と暗号鍵保存用メモリ１３３と識別情報保存用メモリ１３４とスイッチ１３６を持つ。

【００５９】

暗号化器１３１、復号化器１３２、暗号鍵保存用メモリ１３３の機能は先の実施例と同じであるため、説明を省略する。

【００６０】

識別情報保存用メモリ１３４は車載機１台１台を識別する情報を内容として持ち、この情報と前記の暗号鍵は、自動料金収受システムの管理者によってあらかじめ識別情報保存用メモリ１３４と暗号鍵保存用メモリ１３３とにそれぞれ設定されている。スイッチ１３６は、主制御器１４１が制御することにより、路車間通信器１２への出力元を、暗号化器１３１と識別情報保存用メモリ１３４との間で切り替える。

【００６１】

本実施例では、主制御器１４１は路車間通信の開始時にスイッチ１３６を制御して、前記の識別情報保存用メモリ１３４の内容である識別情報を、暗号化せずに路車間通信器１２を通して路側機２に送る。その後、主制御器１４１は路側機２との間で相互認証をするが、その手順の詳細は先の実施例と同じであるため、説明を省略する。本実施例によれば、暗号化装置１３の構成を簡単にすることができる。

【００６２】

【発明の効果】

本発明によれば、前記暗号鍵が、前記暗号化器と前記復号化器に直接渡されるので、前記暗号化装置を利用して通信を行う前記車載機制御装置は前記暗号鍵の転送を考慮しなくてもよい。また、前記暗号化装置の外部に前記暗号鍵が転送される事が無いので、前記暗号鍵の漏洩防止の管理がしやすくなる。特に、前記暗号化装置を１つの集積回路で実現すれば、内部の解析を物理的に困難にすることができる。

【００６３】

上記の暗号化装置を利用すれば、暗号鍵を隠蔽したまま、車載機の設計、製造をすることができる。

【００６４】

また料金収受の通信の前に認証を行う場合、前記暗号化装置に認証の手順を実行させ、認証を完了した後に前記車載機制御装置に通信経路を提供することで、前記車載機制御装置は認証の手順を考慮しなくてもよくなる。別な利点として、認証の手順や認証に必要な情報が前記暗号化装置内にあるため、認証の手順や認証に必要な情報の漏洩防止の管理がしやすい。

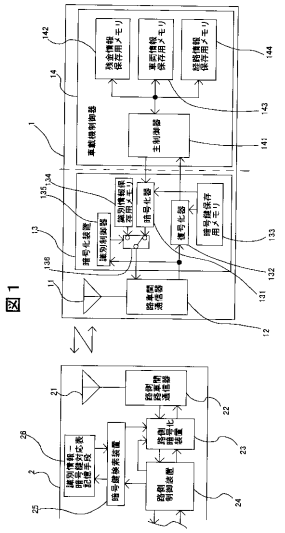
【００６５】

また認証の手順を前記車載機制御装置が制御する場合でも、認証に必要な情報を前記暗号化装置内に置くことで、前の例と同様に認証に必要な情報の漏洩防止の管理がしやすい。前の例にない利点として、例えばＩＳＯ９７９８－２で定められた認証手順を利用する場合、認証の途中から料金収受の通信文を同送することが可能なので、通信回数を減らすことができる。自動料金収受システムでは車両が高速に通信可能範囲を通過するので、通信回数が減ることは通信時間に余裕を持たせる上で非常に好ましい。

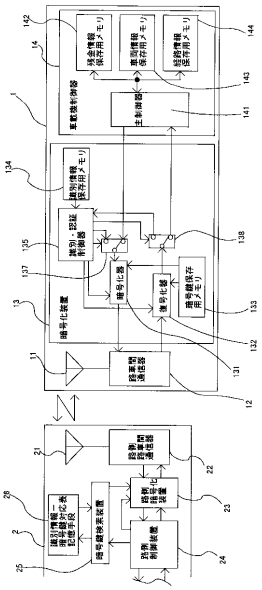
【図面の簡単な説明】

【図１】本発明による１実施例のブロック図
【図２】本発明による他の実施例のブロック図
【図３】本発明によるさらに他の実施例のブロック図
【図４】本発明によるさらに他の実施例のブロック図
【図５】図２の識別・認証制御器の動作を表したフローチャート
【図６】図２の路側機制御器の動作を表したフローチャート
【符号の説明】
１…車載機
１１…アンテナ
１２…路車間通信器
１３…暗号化装置
１３１…暗号化器
１３２…復号化器
１３３…暗号鍵保存用メモリ
１３４…識別情報保存用メモリ
１３５…識別制御器
１３６…スイッチ
１３７…第１のスイッチ
１３８…第２のスイッチ
１４…車載機制御装置
１４１…主制御器
１４２…残金情報保存用メモリ
１４３…車両情報保存用メモリ
１４４…経路情報保存用メモリ
２…路側機
２１…路側機アンテナ
２２…路側機路車間通信器
２３…路側機暗号化装置
２４…路側機制御装置
２５…暗号鍵検索装置
２６…認証情報－暗号鍵対応表記憶手段

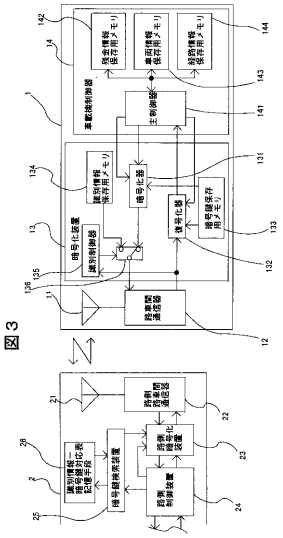
【図１】



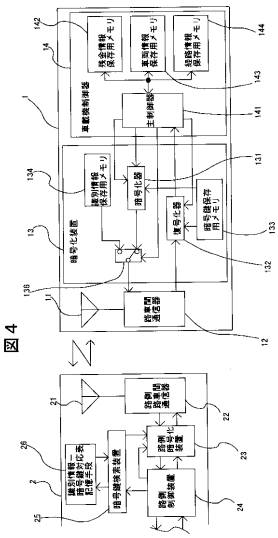
【図２】



【図３】

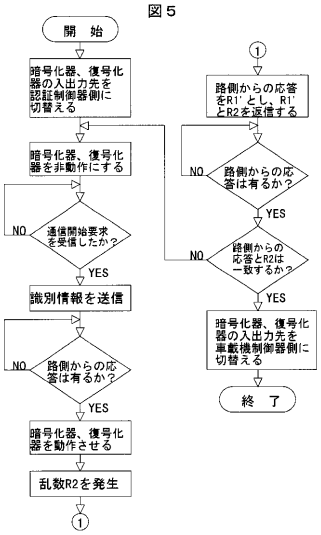


【図４】



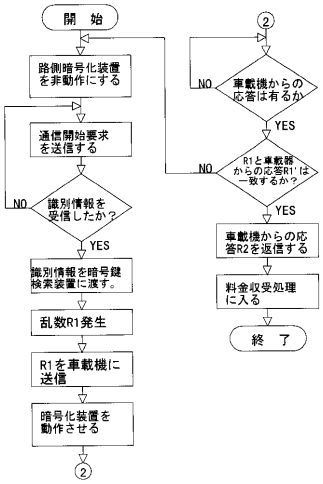
【図５】

図５


開　始
暗号化器、復号化器の入出力先を認証制御器側に切替える
暗号化器、復号化器を非動作にする
通信開始要求を受信したか？
NO
YES
識別情報を送信
路側からの応答は有るか？
NO
YES
暗号化器、復号化器を動作させる
乱数R2を発生
①
①
路側からの応答をR1'とし、R1'とR2を返信する
路側からの応答は有るか？
NO
YES
路側からの応答とR2は一致するか？
NO
YES
暗号化器、復号化器の入出力先を車載機制御器側に切替える
終　了

【図６】

図６


開　始
路側暗号化装置を非動作にする
通信開始要求を送信する
識別情報を受信したか？
NO
YES
識別情報を暗号鍵検索装置に渡す。
乱数R1発生
R1を車載機に送信
暗号化装置を動作させる
②
②
車載機からの応答は有るか
NO
YES
R1と車載器からの応答R1'は一致するか？
NO
YES
車載機からの応答R2を返信する
料金収受処理に入る
終　了

フロントページの続き

(72)発明者　田中　泰成
茨城県ひたちなか市大字高場２５２０番地株式会社日立製作所自動車機器事業部内

審査官　大山　広人

(56)参考文献　特開平０６－０６０２３７（ＪＰ，Ａ）
特開平０１－２３３８５１（ＪＰ，Ａ）
特開平０９－１１５０１９（ＪＰ，Ａ）
特開平０５－２１７０４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G07B 15/00
H04L 9/10