(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 696 31 010 T2** 2004.09.09

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 769 763 B1**
(21) Deutsches Aktenzeichen: **696 31 010.4**
(96) Europäisches Aktenzeichen: **96 116 816.8**
(96) Europäischer Anmeldetag: **18.10.1996**
(97) Erstveröffentlichung durch das EPA: **23.04.1997**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **10.12.2003**
(47) Veröffentlichungstag im Patentblatt: **09.09.2004**

(51) Int Cl.[7]: **G07B 15/00**

(30) Unionspriorität:
27121995 19.10.1995 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Denso Corp., Kariya, Aichi, JP

(74) Vertreter:
WINTER, BRANDL, FÜRNISS, HÜBNER, RÖSS, KAISER, POLTE, Partnerschaft, 85354 Freising

(72) Erfinder:
Maeda, Asako, Kariya-City, Aichi-pref. 448, JP;
Ando, Toshihide, Kariya-City, Aichi-pref. 448, JP;
Yoshida, Ichiro, Kariya-City, Aichi-pref. 448, JP

(54) Bezeichnung: **In einem Fahrzeug eingebaute Kommunikationsvorrichtung und Fahrzeugüberwachungssystem mit vorher verschlüsselten Daten zum hochzuverlässigen Kommunikationsbetrieb**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

QUERVERWEIS ZU VERWANDTER ANMELDUNG

[0001] Diese Anmeldung nimmt Bezug auf sich auf die Japanische Patentveröffentlichung Nr. JP 091150170 und beansprucht deren Priorität.

HINTERGRUND DER ERFINDUNG

1. Gebiet der Erfindung

[0002] Die vorliegende Erfindung bezieht sich auf eine an einem Fahrzeug angebrachte bzw. fahrzeuggebundene Kommunikationsvorrichtung, welche eine Datenkommunikation unter Verwendung verschlüsselter Daten mit einer entlang einer Straße bezüglich des Fahrzeugs angeordneten Straßenrandvorrichtung ausführt. Die vorliegende Erfindung bezieht sich auch auf ein diese fahrzeuggebundene Kommunikationsvorrichtung enthaltendes Fahrzeugfahrtüberwachungssystem zur Überwachung von Fahrzeugen, die in der Umgebung der Straßenrandvorrichtung umherfahren. Insbesondere bezieht sich die vorliegende Erfindung auf eine Vorrichtung zum Durchführen eines automatischen Einzugs einer Mautgebühr von einem Fahrzeug, welches entlang einer Mautstraße fährt.

2. Beschreibung des Stands der Technik

[0003] Ein Mautabrechnungssystem zum automatischen Einziehen einer Mautgebühr von einem entlang einer Mautstraße fahrenden Fahrzeug ist wohlbekannt. Dieses Mautabrechnungssystem enthält eine Kommunikationsvorrichtung (d. h., eine Straßenrandvorrichtung), die an einer Einfahrt oder einer Ausfahrt der Mautstraße installiert ist, und eine Kommunikationsvorrichtung (d. h., einer fahrzeuggebundenen Vorrichtung), die in einem entlang der Mautstraße fahrenden Fahrzeug installiert ist. Diese an einem Fahrzeug angebrachte bzw. fahrzeuggebundene Vorrichtung sendet in Reaktion auf eine Abfrage von seiten der Straßenrandvorrichtung Fahrzeuginsassendaten und Zahlungsverfahrensdaten. Dieses Mautabrechnungssystem führt einen automatischen Mautgebühreneinzug in der Straßenrandvorrichtung auf der Grundlage der von der fahrzeuggebundenen Vorrichtung gesendeten Daten durch.

[0004] Da in dem vorgenannten System persönliche Informationen wie etwa Mautabrechnungsdaten, Fahrzeugdaten, Insassendaten und dergleichen über eine Funkkommunikation zwischen der fahrzeuggebundenen Vorrichtung und der Straßenrandvorrichtung gesendet werden, gibt es indessen eine Möglichkeit, daß solche Daten durch Dritte abgefangen und mißbraucht werden. Wenn beispielsweise eine Kontokarte zum Entrichten der Mautgebühr verwendet wird, liegt eine Möglichkeit vor, daß Kontokarteninformationen abgefangen und mißbraucht werden.

[0005] Demgemäß schlägt, um die vorgenannten Probleme zu lösen, ein wohlbekannter Vorschlag, wie er in dem US-Patent Nr. 5,310,999 offenbart ist, beispielsweise die Ausführung einer Datenkommunikation zwischen der fahrzeuggebundenen Vorrichtung und der Straßenrandvorrichtung unter Verwendung verschlüsselter Daten, die durch Verschlüsseln der zu sendenden Daten erhalten werden, vor, so daß der Inhalt der Daten für einen Dritten, der solche Daten abfängt, unverständlich sein werden.

[0006] Da in dem oben vorgeschlagenen System ein bekanntes standardisiertes Verschlüsselungsprotokoll wie etwa der Algorithmus des Data Encryption Standard (DES) zum Durchführen des Lesens und Schreibens von Daten bezüglich einer IC-Karte oder dergleichen zum Verschlüsseln der Kommunikationsdaten verwendet wird, können indessen die Kommunikationsdaten zwischen der fahrzeuggebundenen Vorrichtung unter bestimmten Umständen vergleichsweise einfach entschlüsselt werden, nachdem solche Daten abgefangen und analysiert wurden. Auf diese Weise kann es Probleme bezüglich der Vertrauenswürdigkeit der Daten geben. Weil der DES-Algorithmus eine signifikante Zeitdauer benötigt, um den Datenverschlüsselungsvorgang durchzuführen, und weil es schwierig ist, diesen DES-Algorithmus zu beschleunigen, tritt auch das nachstehende Problem auf, wenn sich das Fahrzeug schnell bewegt und der DES-Algorithmus während Kommunikationsvorgängen zwischen der fahrzeuggebundenen Vorrichtung und der Straßenrandvorrichtung eine signifikante Zeitdauer zum Verschlüsseln der Sendedaten und Entschlüsseln der Empfangsdaten benötigt. Und zwar könnte die fahrzeuggebundene Vorrichtung, nachdem die fahrzeuggebundene Vorrichtung in den Kommunikationsbereich der Straßenrandvorrichtung eingetreten ist, einen Kommunikationsbereich der Straßenrandvorrichtung verlassen, bevor die Datenkommunikationsvorgänge beendet sind.

[0007] In dem zuvor beschriebenen Mautabrechnungssystem entschlüsselt die fahrzeuggebundene Vorrichtung zum Beispiel dann, wenn die fahrzeuggebundene Vorrichtung Daten (z. B. Mautabrechnungsdaten) in eine Kontokarte oder dergleichen schreibt und nach Vollendung dessen diese Daten verschlüsselt und die verschlüsselten Daten an die Straßenrandvorrichtung sendet, zuerst die von der Straßenrandvorrichtung aus ge-

sendeten Daten, um die Mautabrechnung durchzuführen, schreibt dann die Daten in die Kontokarte oder dergleichen auf der Grundlage solcher entschlüsselter Daten, verschlüsselt die sich ergebenden Daten und sendet das Verschlüsselungsergebnis an die Straßenrandvorrichtung. Das vorgenannte System benötigt jedoch eine signifikante Zeitdauer, um eine Entschlüsselung der Daten von der Straßenrandvorrichtung und eine Verschlüsselung der an die Straßenrandvorrichtung zu sendenden Daten durchzuführen. Unter der Annahme beispielsweise, daß die für jeweilige Verschlüsselungs- und Entschlüsselungsvorgänge benötigte Zeitdauer 30 ms beträgt und die Reisegeschwindigkeit des Fahrzeugs 120 km/h beträgt, bewegt sich das Fahrzeug jedes Mal, wenn die fahrzeuggebundene Vorrichtung einen Verschlüsselungs- und Entschlüsselungsvorgang durchführt, um einen Meter. Nachdem andererseits der Kommunikationsbereich der Straßenrandvorrichtung üblicherweise auf eine Größe festgelegt ist, die in etwa der Größe des Fahrzeugs entspricht, um zu vermeiden, daß eine Mehrzahl von Fahrzeugen gleichzeitig in diesen eintreten, wird der zurückgelegte Weg des Fahrzeugs innerhalb des Kommunikationsbereichs ein paar Meter oder so betragen. Da selbst bei einer einseitigen Kommunikation die Verschlüsselungs- und Entschlüsselungsvorgänge sowohl in der fahrzeuggebundenen Vorrichtung als auch der Straßenrandvorrichtung durchgeführt werden müssen, um eine normale Datenkommunikation zwischen diesen durchzuführen, kann auf einer Autobahn, auf der Fahrzeuge mit Geschwindigkeiten von etwa 120 km/h fahren, eine Datenkommunikation (zweiseitige Kommunikation) zwischen der Straßenrandvorrichtung und der fahrzeuggebundenen Kommunikation höchstens ein oder zwei Mal durchgeführt werden. Falls es mehr Kommunikationsvorgänge gibt, wird die fahrzeuggebundene Vorrichtung aus dem Kommunikationsbereich austreten, bevor die Kommunikationsvorgänge vollendet sind, und daher wird eine normale Datenkommunikation unmöglich.

[0008] Andererseits könnte man, um das vorgenannte Problem zu lösen, Geschwindigkeitsbeschränkungen vorschreiben oder eine Verschlüsselungsvorrichtung, welche den Verschlüsselungsvorgang in Übereinstimmung mit dem DES-Algorithmus durchführt, durch eine Vorrichtung ersetzen, welche einen Verschlüsselungsvorgang mit hoher Geschwindigkeit ermöglicht. Eine Beschränkung der Reisegeschwindigkeit des Fahrzeugs führt jedoch zu einer Verkehrsstauung und macht daher den Zweck eines automatischen Einzugs von Mautgebühren über eine Funkkommunikation, der darin besteht, eine Verkehrsstauung zu verringern, zunichte. Umgekehrt besteht ein Bedürfnis, teure Verschlüsselungsvorrichtungen zu verwenden, um die Verarbeitungsgeschwindigkeit der Verschlüsselungsvorrichtung schneller zu machen. Daher wird selbst dann, wenn solche teuren Vorrichtungen für die Straßenrandvorrichtung verwendet werden können, die Umsetzung eines Einbaus solcher teuren Vorrichtungen in die fahrzeuggebundene Vorrichtung schwierig sein, weil dies eine erhöhte Belastung für die Mautstraßenbenutzer bedeutet.

[0009] Des weiteren besteht eine andere Option zum Erhöhen der Verschlüsselungsgeschwindigkeit darin, einen Verschlüsselungsalgorithmus, der sich von dem DES-Algorithmus unterscheidet, beispielsweise einen Verschlüsselungsalgorithmus, der die Ausführung einer Verschlüsselung durch eine unter Verwendung von Hardware umgesetzte Pipeline-Verarbeitung ermöglicht, zu verwenden. In diesem Fall wird jedoch dann, wenn die Verschlüsselungsvorrichtung so konstruiert ist, daß sie eine Verschlüsselung nicht durch eine Software-Verarbeitung unter Verwendung einer CPU, sondern durch eine Pipeline-Verarbeitung unter Verwendung einer Sonderhardware durchführt, die Verschlüsselungsvorrichtung selbst teuer, und daher wird selbst dann, wenn es möglich ist, diese Konstruktion für die Straßenrandvorrichtung einzusetzen, schwierig sein, die gleiche Verschlüsselungsvorrichtung in der fahrzeuggebundenen Vorrichtung vorzusehen.

[0010] Die Druckschrift WO 95 10147 A offenbart einen automatischen Echtzeit-Autobahnmauteinzug von beweglichen Fahrzeugen in Übereinstimmung mit dem Oberbegriff von Anspruch 1. Demgemäß ist eine fahrzeuggebundene Kommunikationsvorrichtung vorgesehen, welche eine Ansteuerungseinrichtung zum Aufnehmen einer IC-Karte, eine Kryptographie-Einrichtung zum Verschlüsseln von an eine Straßenrandvorrichtung zu sendenden Sendedaten, und eine Kommunikationseinrichtung zum Durchführen von Kommunikationsvorgängen mit der Straßenrandvorrichtung aufweist. Eine kyptographische Verarbeitung wird nur in der IC-Karte und ihrer Schnittstelle durchgeführt. Daher wird die Sicherheit in einer Datenkommunikation durch die IC-Karte erreicht und hängt von in hohem Maße von der Robustheit des in der IC-Karte eingesetzten Kryptographie-Algorithmus ab.

[0011] Ferner offenbaren die Druckschriften GB-A-2 283 600, EP-A-0 401 192 und EP-A-0 613 108 Kommunikationssysteme einer verwandten Technologie.

ZUSAMMENFASSUNG DER ERFINDUNG

[0012] Angesichts der vorgenannten Probleme in dem Stand der Technik ist es ein Ziel der vorliegenden Erfindung, eine fahrzeuggebundene Kommunikationsvorrichtung zu schaffen, welche zu sendenden Daten wirksam verschlüsseln, eine Kommunikation in einem kleinen Kommunikationsbereich für eine kurze Zeitdauer durchführen und ein rechtswidriges Abfangen der Kommunikationsdaten und dergleichen verhindern kann. Die vorliegenden Erfindung ist auch darauf gerichtet, ein Fahrzeugüberwachungssystem wie etwa das vorgenannte Mautabrechnungssystem zu schaffen, welches diese fahrzeuggebundene Kommunikationsvorrichtung ver-

wendet.

[0013] Um die vorgenannten Aufgaben zu erfüllen, stellt ein Gesichtspunkt der vorliegenden Erfindung eine fahrzeuggebundene bzw. an einem Fahrzeug angebrachte Kommunikationsvorrichtung bereit, welche in einem Fahrzeug eingebaut ist und welche dazu dient, Kommunikationsvorgänge mit einer entlang einer Mautstraße installierten Straßenrandvorrichtung durchzuführen, wenn sich das Fahrzeug innerhalb des Kommunikationsbereichs der Straßenrandvorrichtung befindet. Die fahrzeuggebundene Kommunikationsvorrichtung weist eine Kryptographie-Einheit und eine Kommunikationseinheit auf. Die Kryptographie-Einheit verschlüsselt an die Straßenrandvorrichtung zu sendenden Sendedaten, bevor das Fahrzeug in den Kommunikationsbereich der Straßenrandvorrichtung eintritt. Die Kommunikationseinheit führt Kommunikationsvorgänge mit der Straßenrandvorrichtung durch Senden von durch die Kryptographie-Einheit verschlüsselten Sendedaten und durch Empfang von Empfangsdaten von der Straßenrandvorrichtung durch. Vorzugsweise entschlüsselt die Kryptographie-Einheit die Empfangsdaten, nachdem die Kommunikationseinheit Kommunikationsvorgänge mit der Straßenrandvorrichtung vollendet.

[0014] Auf diese Weise führt, nachdem eine signifikante Zeitdauer erforderlich ist, um die Sendedaten zu verschlüsseln und die Empfangsdaten zu entschlüsseln, die fahrzeuggebundene Kommunikationsvorrichtung gemäß der vorliegenden Erfindung diese Datenverschlüsselungs- und Entschlüsselungsvorgänge durch, wenn sie keine Kommunikationsvorgänge mit der Straßenrandvorrichtung durchführt. In anderen Worten, wenn die fahrzeuggebundenen Kommunikationsvorrichtung Kommunikationsvorgänge mit der Straßenrandvorrichtung durchführt, wird sie eine geringere Belastung erfahren. Daher kann die Dauer einer Kommunikation zwischen der fahrzeuggebundene Kommunikationsvorrichtung und der Straßenrandvorrichtung verkürzt werden, und zwischen diesen kann eine genaue Datenkommunikation durchgeführt werden, ohne den Fahrzeugen Geschwindigkeitsbeschränkungen aufzuerlegen oder eine teure kryptographische Vorrichtung zur Ausführung der Verschlüsselungs- und Entschlüsselungsvorgänge zu verwenden.

[0015] Vorzugsweise weist die fahrzeuggebundene Kommunikationsvorrichtung ferner eine Ansteuerungseinheit zum Aufnehmen einer vorbestimmte Kartendaten speichernden IC-Karte auf und weist die Kryptographie-Einheit einen Verschlüssler und einen Entschlüssler auf. Der Verschlüssler liest die Kartendaten von der IC-Karte, entschlüsselt die Kartendaten, um die Sendedaten zu generieren, und speichert die Sendedaten. Der Entschlüssler entschlüsselt die durch die Kommunikationseinheit empfangenen Empfangsdaten, um entschlüsselte Daten zu erhalten, und speichert ein Ergebnis des Kommunikationsvorgangs der Kommunikationseinheit auf der Grundlage der entschlüsselten Daten in der IC-Karte. Der Entschlüssler entschlüsselt die Empfangsdaten, nachdem die Kommunikationseinheit die Kommunikationsvorgänge mit der Straßenrandvorrichtung vollendet.

[0016] Auf diese Weise beginnt die Kommunikationseinheit dann, wenn das Fahrzeug in den Kommunikationsbereich der Straßenrandvorrichtung eintritt, eine Datenkommunikation mit der Straßenrandvorrichtung durch Senden durch den Verschlüssler verschlüsselter Daten durchzuführen. Dann entschlüsselt der Entschlüssler dann, wenn die Kommunikationseinheit die Datenkommunikation mit der Straßenrandvorrichtung beendet, die Empfangsdaten. Somit ist die fahrzeuggebundene Kommunikationsvorrichtung nicht mit einer Entschlüsselung der Empfangsdaten belastet, wenn sie mit der Straßenrandvorrichtung kommuniziert, und so kann die Kommunikationszeit zwischen der fahrzeuggebundene Kommunikationsvorrichtung und der Straßenrandvorrichtung verkürzt werden. Indessen wird die IC-Karte zum Speichern wenigstens eines Teil an die Straßenrandvorrichtung zu sendenden Daten wie etwa eines Identifikationscodes des Fahrers des Fahrzeugs, eine Bankkontonummer und dergleichen verwendet.

[0017] Im Übrigen könnte es in einem Mautabrechnungssystem ein Bedürfnis geben, das Kommunikationsergebnis in die IC-Karte zu schreiben und die Straßenrandvorrichtung von dem Ergebnis eines solchen zu informieren. Daher ist es hilfreich, wenn dieses Ergebnis im Voraus als die Sendedaten nach der Vollendung der Kommunikation zwischen der fahrzeuggebundene Kommunikationsvorrichtung und der Straßenrandvorrichtung verschlüsselt wird. Danach werden die verschlüsselten Daten an die Straßenrandvorrichtung gesendet, wenn das Fahrzeug in den nächsten Kommunikationsbereich der Straßenrandvorrichtung eintritt.

[0018] Vorzugsweise verschlüsselt der Entschlüssler das Ergebnis des Kommunikationsvorgangs, bevor er das Ergebnis in der IC-Karte speichert, und verwendet der Entschlüssler einen Kartendatenverschlüsselungsalgorithmus zum Verschlüsseln des Ergebnisses. Es muß hier erwähnt werden, daß sich der Kartendatenverschlüsselungsalgorithmus von einem Kommunikationsverschlüsselungsalgorithmus, der von dem Entschlüssler zum Entschlüsseln der Empfangsdaten und von dem Verschlüssler zum Verschlüsseln der Kartendaten verwendet wird, um die Sendedaten zu generieren, unterscheidet.

[0019] Das heißt, beim Schreiben von Daten in die IC-Karte werden solche Daten üblicherweise unter Verwendung des DES-Algorithmus oder dergleichen verschlüsselt, um ein Abfangen des Dateninhalts zu verhindern. Allerdings kann die Verwendung des gleichen Algorithmus zum Entschlüsseln der Empfangs- und Verschlüsseln der Sendedaten Probleme hinsichtlich der Datensicherheit aufwerfen, und daher wird es am besten sein, für diese Verschlüsselungsvorgänge unterschiedliche Algorithmen zu verwenden. Auf diese Weise können Daten sicher und geschützt zwischen der Straßenrandvorrichtung und der fahrzeuggebundene Kommu-

nikationsvorrichtung ausgetauscht werden.

[0020] Vorzugsweise ist die fahrzeuggebundene Kommunikationsvorrichtung mit einer Verifikationseinheit zum Ansteuern des Verschlüsslers und der IC-Karte, um einen gegenseitigen Verifikationsvorgang unter Verwendung vorbestimmter Verifikationsdaten durchzuführen, wenn die IC-Karte in die Ansteuerungseinheit eingesetzt wird und bevor der Verschlüssler die Sendedaten generiert, ausgestattet. Hierbei steuert die Verifikationseinheit auch den Verschlüssler an, um ein Ergebnis des gegenseitigen Verifikationsvorgangs in die Sendedaten einzuschließen.

[0021] In dem vorgenannten Mautabrechnungssystem oder dergleichen gibt es eine Möglichkeit, daß nicht nur die IC-Karte, sondern auch die fahrzeuggebundene Kommunikationsvorrichtung selbst gefälscht wird. Als eine Gegenmaßnahme hiergegen ist die Verifikationseinheit zum Ausführen einer gegenseitigen Verifikationsprozedur zwischen dem Verschlüssler und der IC-Karte vorgesehen. Nach Durchführen dieser Verifikationsprozedur werden die Verifikationsergebnisse in die an die Straßenrandvorrichtung zu sendenden Sendedaten eingebunden. Auf diese Weise wird der Straßenrandvorrichtung ein mögliches Problem in der fahrzeuggebundenen Kommunikationsvorrichtung zur Kenntnis gebracht.

[0022] Vorzugsweise weist der Kommunikationsverschlüsselungsalgorithmus eine höhere Verschlüsselungsgeschwindigkeit auf als der Kartendatenverschlüsselungsalgorithmus auf. Auf diese Weise kann die Kommunikationszeit zwischen der fahrzeuggebundenen Kommunikationsvorrichtung und der Straßenrandvorrichtung verkürzt werden. Demgemäß kann eine Datenkommunikation auch dann, wenn das Fahrzeug mit hoher Geschwindigkeit durch den Kommunikationsbereich der Straßenrandvorrichtung hindurchtritt, zuverlässiger ausgeführt werden.

[0023] Vorzugsweise weist die fahrzeuggebundene Vorrichtung eine Fehlerbestimmungseinheit zum Bestimmen eines Fehlers in Vorgängen der Kryptographie-Einheit und der Kommunikationseinheit und zum Hinzufügen von Fehlerdaten, die den bestimmten Fehler anzeigen, zu den Sendedaten auf. Auf diese Weise kann der Straßenrandvorrichtung ein Fehler in der fahrzeuggebundenen Vorrichtung zur Kenntnis gebracht werden, so daß diese Maßnahmen wie etwa ein Senden einer Nachricht an den Fahrer, das Fahrzeug anzuhalten, ein Lichtbild des Fahrzeugs zu erstellen oder dergleichen ergreifen kann.

[0024] Ein anderer Gesichtspunkt der vorliegenden Erfindung stellt ein Fahrzeugüberwachungssystem bereit, welches ein Fahrzeug, das sich entlang einer Mautstraße bewegt, überwacht und welches eine an einem Fahrzeug angebrachte bzw. fahrzeuggebundene Vorrichtung und eine Straßenrandvorrichtung aufweist. Die Straßenrandvorrichtung ist entlang der Mautstraße installiert, um Signale in Richtung eines vorbestimmten Kommunikationsbereichs auszusenden. Diese Straßenrandvorrichtung führt einen Kommunikationsvorgang mit der fahrzeuggebundenen Vorrichtung durch, wenn sich das Fahrzeug innerhalb des Kommunikationsbereichs befindet. Die fahrzeuggebundene Vorrichtung und die Straßenrandvorrichtung führen Kommunikationsvorgänge unter Verwendung von Kommunikationsdaten aus, welche einen verschlüsselten Teil und einen unverschlüsselten Teil aufweisen.

[0025] Auf diese Weise wird es mit den einen verschlüsselten Teil und einen unverschlüsselten Teil enthaltenden Kommunikationsdaten auch dann, wenn solche Daten abgefangen werden, schwieriger, die Kommunikationsdaten zu entziffern, und daher können zwischen der fahrzeuggebundenen Vorrichtung und der Straßenrandvorrichtung hoch zuverlässige Kommunikationsvorgänge durchgeführt werden.

[0026] Ein anderer Gesichtspunkt der vorliegenden Erfindung stellt ein Fahrzeugüberwachungssystem bereit, welches eine fahrzeuggebundenen Vorrichtung und eine Straßenrandvorrichtung aufweist. Die Straßenrandvorrichtung sendet für jedes vorbestimmte Zeitintervall ein Pilotsignal an den Kommunikationsbereich aus, wobei die Aussendung des Pilotsignals beendet wird, nachdem das Fahrzeug in den Kommunikationsbereich eintritt, führt einen Kommunikationsvorgang mit der fahrzeuggebundenen Vorrichtung durch Senden und Empfangen von Kommunikationsdaten an die und von der an einem Fahrzeug angebrachte Vorrichtung durch, während sich das Fahrzeug innerhalb des Kommunikationsbereichs befindet, und sendet ein Übertragungsvollendungssignal an die fahrzeuggebundene Vorrichtung, um eine Vollendung des Kommunikationsvorgangs anzuzeigen, und sendet nach Vollendung des Kommunikationsvorgangs mit der fahrzeuggebundenen Vorrichtung erneut das Pilotsignal aus. Die fahrzeuggebundene Vorrichtung stellt nach Empfang des Pilotsignals von der Straßenrandvorrichtung ein Pilotantwortsignal bereit und beginnt anschließend den Kommunikationsvorgang mit der Straßenrandvorrichtung. Diese fahrzeuggebundene Vorrichtung empfängt nach Vollendung des Kommunikationsvorgangs mit der Straßenrandvorrichtung das Übertragungsvollendungssignal von der Straßenrandvorrichtung. Die Straßenrandvorrichtung beendet nach Empfang des Pilotantwortsignals von der fahrzeuggebundenen Vorrichtung die Aussendung des Pilotsignals und nimmt nach Senden des Übertragungsvollendungssignals die Aussendung des Pilotsignals in vorbestimmten Zeitintervallen wieder auf.

[0027] Auf diese Weise kann, während eine Mehrzahl von Fahrzeugen vorliegen kann, die entlang der Mautstraße fahren, die Straßenrandvorrichtung nach Beenden von Kommunikationsvorgängen mit dem vorliegenden Fahrzeug rasch Kommunikationsvorgänge mit einer fahrzeuggebundenen Vorrichtung eines nächsten Fahrzeugs beginnen. Auf diese Weise kann die Straßenrandvorrichtung selbst dann, wenn Fahrzeuge nacheinander in ihren Kommunikationsbereich eintreten, korrekte Kommunikationsvorgänge durchführen.

[0028] Vorzugsweise sendet die Straßenrandvorrichtung nach Senden des Pilotsignals und der Kommunikationsdaten an die fahrzeuggebundene Vorrichtung für eine vorbestimmte Zeitdauer eine unmodulierte Trägerwelle an die fahrzeuggebundene Vorrichtung; generiert die fahrzeuggebundene Vorrichtung die Kommunikationsdaten durch Modulieren des Trägerwellensignals auf der Grundlage vorbestimmter Übertragungsinformationen und stellt die Kommunikationsdaten an die Straßenrandvorrichtung bereit; und sendet die fahrzeuggebundene Vorrichtung nach Vollendung des Kommunikationsvorgangs mit der Straßenrandvorrichtung ein Vollendungsanforderungssignal an die Straßenrandvorrichtung, sofern nicht die Straßenrandvorrichtung das Übertragungsvollendungssignal sendet.
[0029] Auf diese Weise können die fahrzeuggebundene Vorrichtung und die Straßenrandvorrichtung mit dem das Vollendungsanforderungssignal und das Übertragungsvollendungssignal verwendenden Kommunikationsvorgang prüfen, ob der Kommunikationsvorgang zwischen ihnen richtig vollendet wurde oder nicht.
[0030] Vorzugsweise ist die Straßenrandvorrichtung in entweder einer Einfahrt oder einer Ausfahrt der Mautstraße installiert. Die Straßenrandvorrichtung entschlüsselt während eines Kommunikationsvorgangs mit der fahrzeuggebundenen Vorrichtung die Mautzahlungsinformationen anzeigenden Kommunikationsdaten von der fahrzeuggebundenen Vorrichtung. Die Straßenrandvorrichtung führt einen Mautgebührenvorgang durch, um eine Mautgebühr von der fahrzeuggebundenen Vorrichtung auf der Grundlage der Mautzahlungsinformationen einzuziehen, verschlüsselt ein Ergebnis des Mautgebührenvorgangs und sendet das verschlüsselte Ergebnis an die fahrzeuggebundene Vorrichtung. Die fahrzeuggebundene Vorrichtung sendet während einer Kommunikation mit der Straßenrandvorrichtung die die Mautzahlungsinformationen anzeigenden Kommunikationsdaten. Zusätzlich empfängt die fahrzeuggebundene Vorrichtung das verschlüsselte Ergebnis des Mautgebührenvorgangs von der Straßenrandvorrichtung und entschlüsselt und speichert das Ergebnis. Es muß hier festgehalten werden, daß die fahrzeuggebundene Vorrichtung und die Straßenrandvorrichtung die Kommunikationsdaten unter Verwendung eines gemeinsamen Formats senden. Auf diese Weise können, da die fahrzeuggebundene Vorrichtung und die Straßenrandvorrichtung das gleiche Datenformat verwenden, Verschlüsselungsund Entschlüsselungsvorgänge in diesen Vorrichtungen effizient durchgeführt werden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0031] Zusätzliche Aufgaben und Vorteile der vorliegenden Erfindung werden aus der nachstehenden genauen Beschreibung bevorzugter Ausführungsformen hiervon leichter ersichtlich sein, wenn sie zusammen mit den begleitenden Zeichnungen genommen werden, in welchen:
[0032] **Fig.** 1 ein Blockdiagramm eines Mautstraßen-Mautabrechnungssystems gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung ist;
[0033] **Fig.** 2 ist ein Flußdiagramm ist, welches eine Kommunikationsschaltung einer fahrzeuggebundenen Vorrichtung gemäß der bevorzugten Ausführungsform darstellt;
[0034] **Fig.** 3 ein Diagramm ist, welches ein Format eines durch eine Straßenrandvorrichtung gemäß der bevorzugten Ausführungsform gesendeten Sendesignals darstellt;
[0035] **Fig.** 4 ein Flußdiagramm ist, welches eine durch die fahrzeuggebundene Vorrichtung dann, wenn eine IC-Karte in diese eingesetzt wird, ausgeführte Routine zeigt;
[0036] **Fig.** 5 ein Flußdiagramm ist, welches einen gegenseitigen Verifikationsprozeß zwischen einer IC-Karte und einem kryptographischen Modul der fahrzeuggebundenen Vorrichtung darstellt;
[0037] **Fig.** 6 ein Flußdiagramm ist, welches den durch eine in einem ersten Gerüst der Straßenrandvorrichtung vorgesehene Kommunikationsvorrichtung ausgeführten Kommunikationsprozeß darstellt;
[0038] **Fig.** 7 ein Diagramm ist, welches den Fluß einer Datenkommunikation zwischen der in dem ersten Gerüst vorgesehenen Kommunikationsvorrichtung und der fahrzeuggebundenen Vorrichtung darstellt;
[0039] **Fig.** 8 ein Flußdiagramm ist, welches einen durch die fahrzeuggebundene Vorrichtung ausgeführten ersten Gerüstdurchgangsprozeß darstellt;
[0040] **Fig.** 9 ein Flußdiagramm ist, welches einen durch eine in einem zweiten Gerüst der Straßenrandvorrichtung vorgesehene Kommunikationsvorrichtung ausgeführten Kommunikationsprozeß darstellt;
[0041] **Fig.** 10 ein Flußdiagramm ist, welches den Fluß von Daten zwischen der in dem zweiten Gerüst vorgesehenen Kommunikationsvorrichtung und der fahrzeuggebundenen Vorrichtung darstellt;
[0042] **Fig.** 11 ein Flußdiagramm ist, welches einen in der fahrzeuggebundenen Vorrichtung ausgeführten zweiten Gerüstdurchgangsprozeß darstellt; und
[0043] **Fig.** 12 ein Flußdiagramm ist, welches einen durch die fahrzeuggebundene Vorrichtung dann, wenn die IC-Karte aus ihrem Laufwerk entfernt wird, ausgeführten Prozeß darstellt.

GENAUE BESCHREIBUNG EINER DERZEIT BEVORZUGTEN BEISPIELHAFTEN AUSFÜHRUNGSFORM

[0044] Eine bevorzugte Ausführungsform der vorliegenden Erfindung ist nachstehend mit Bezug auf die begleitenden Zeichnungen beschrieben.

[0045] Zuerst ist **Fig.** 1 ein Blockdiagramm, welches den Gesamtaufbau eines Mautstraßen-Mautabrechnungssystems gemäß der vorliegenden Erfindung darstellt.

[0046] Wie in **Fig.** 1 dargestellt, beinhaltet das Mautstraßen-Mautabrechnungssystem gemäß der vorliegenden Erfindung eine fahrzeuggebundene Vorrichtung **10**, welche in einem Fahrzeug eingebaut ist, und eine Straßenrandvorrichtung **20**, welche in der Umgebung einer Einfahrt oder einer Ausfahrt einer Mautstraße installiert ist. Die Straßenrandvorrichtung **20** ist mit ersten und zweiten Gerüsten **30**, **40**, die in vorbestimmten Abständen entlang der Mautstraße in der Vorwärtsrichtung des Fahrzeugs aufgestellt sind, verbunden. Diese Gerüste **30**, **40** sind zwei erhöhte Plattformen, welche die eine Mehrzahl von Fahrstreifen aufweisende Mautstraße überqueren. Das erste Gerüst **30** und das zweite Gerüst **40** sind jeweils mit Transceivern **32**, **34**, ... und **42**, **44**, ... zur Durchführung einer Datenkommunikation mit jeder fahrzeuggebundenen Vorrichtung **10**, die in jedem entlang jedem Fahrstreifen der Straße fahrenden Fahrzeug eingebaut ist, ausgestattet.

[0047] Wenn das Fahrzeug durch Gerüste **30**, **40** hindurchfährt, führt die fahrzeuggebundene Vorrichtung **10** automatisch eine Datenkommunikation mit der Kommunikationsvorrichtung (d. h., einem Transceiver) des Kommunikationsbereichs durch, durch welchen das Fahrzeug hindurchtritt. Die fahrzeuggebundene Vorrichtung **10** beinhaltet ein IC-Karten-Laufwerk **12**, eine Kommunikationsschaltung **18**, welche eine Antenne **18a** aufweist und welche eine Funkkommunikation mit den Transceivern **32**, **24**, ..., **42**, **44**, ... durchführt, ein kryptographisches Modul (nachstehend als ein "Krypto-Modul" bezeichnet) **14** zum Verschlüsseln von Sendedaten und zum Entschlüsseln von Empfangsdaten sowie ein Steuergerät **16**, welches einen Mikroprozessor zum Steuern der vorgenannten Schaltungen beinhaltet. Das IC-Karten-Laufwerk **12** kann mit einer herausnehmbaren IC-Karte **2**, welche eine Kontokarte oder eine Guthabenkarte sein kann, zur Zahlung einer Mautgebühr versehen sein. Dieses IC-Karten-Laufwerk **12** führt Datenlese- und -schreibvorgänge an der IC-Karte durch.

[0048] Es sollte festgehalten werden, daß das Krypto-Modul **14** in die fahrzeuggebundenen Vorrichtung **10** eingebaut oder an dieser befestigt sein kann und dazu dient, den Verschlüsselungsalgorithmus oder die zur Verschlüsselung verwendeten Schlüsseldaten zu ändern. In anderen Worten, das Krypto-Modul **14** kann von der fahrzeuggebundenen Vorrichtung **10** abgenommen werden, um ihre Verschlüsselungs-Software umzuprogrammieren, oder kann innerhalb der fahrzeuggebundenen Vorrichtung **10** verbleiben, während sein Verschlüsselungsalgorithmus und die Schlüsseldaten geändert werden. Auf diese Weise ist es möglich, den Verschlüsselungsalgorithmus und die Schlüsseldaten des Krypto-Moduls **14** zu ändern.

[0049] Die Transceiver **32**, **34**, ..., die innerhalb des ersten Gerüsts **30** installiert sind, beinhalten nicht nur Antennen **32a**, **34a**, ... zum Durchführen einer Funkkommunikation mit der fahrzeuggebundenen Vorrichtung **10**, sondern auch kryptographische Einheiten (nachstehend als "Krypto-Einheiten" bezeichnet) **32b**, **34b**, ... zum Verschlüsseln von Sendedaten und Entschlüsseln von Empfangsdaten. Diese Transceiver **32**, **34** führen eine Datenkommunikation mit der fahrzeuggebundenen Vorrichtung **10** durch, während sie auch Daten verschlüsseln und entschlüsseln. Demgegenüber weisen die Transceiver **42**, **44**, ..., die innerhalb des zweiten Gerüsts **40** installiert sind, keine solchen Krypto-Einheiten auf und führen über ihre Antennen **42**, **44**, ... nur eine Datenkommunikation mit der fahrzeuggebundenen Vorrichtung **10** durch. Das heißt, die Transceiver **42**, **44**, ... liefern Sendedaten und empfangen Empfangsdaten in unveränderter Form an die Straßenrandvorrichtung **20** bzw. von dieser. Obwohl in **Fig.** 1 nicht gezeigt, muß festgehalten werden, daß in der gleichen Weise wie die fahrzeuggebundene Vorrichtung **10** jeder der Transceiver **32**, **34**, ... und **42**, **44**, ... mit einer Kommunikationsschaltung zum Durchführen von Sendevorgängen und einer Steuerungsvorrichtung, die einen Mikroprozessor enthält und deren Steuerungsprozesse eine Funkkommunikation mit der fahrzeuggebundenen Vorrichtung **10** und eine Datenübertragung mit der Straßenrandvorrichtung **20** überwachen, ausgerüstet ist.

[0050] Die Straßenrandvorrichtung **20** ist mit einem Paar von Gerüsten **30**, **40** ausgestattet. Die Straßenrandvorrichtung **20** beinhaltet auch Kommunikationssteuergeräte **22**, **24** zum Steuern der Kommunikationsvorgänge der Transceiver **32**, **34**, ... und **42**, **44**, ... und ein lokales Steuergerät **26**, welches einen Mikroprozessor enthält und welches eine Datenkommunikation mit den Transceivern **32**, **34**, ... und **42**, **44**, ... der Gerüste **30**, **40** über die Kommunikationssteuergeräte **22**, **24** durchführt, um den Einzug von Mautgebühren von einem fahrenden Fahrzeug zu steuern.

[0051] Des weiteren ist die Straßenrandvorrichtung **20** mit einer Mehrzahl von Kameras **52** verbunden, die in der Umgebung der Straße aufgebaut sind, um Lichtbilder umherfahrender Fahrzeuge anzufertigen. Wenn beispielsweise das System darin versagt, eine Mautgebühr von einem fahrenden Fahrzeug einzuziehen, steuert das lokale Steuergerät **26** die Kameras **52** durch ein Lichtbild-Steuergerät **28** an, um ein solches Fahrzeug abzulichten. Ferner ist das lokale Steuergerät **26** mit einem zentralen Steuergerät (Host-Rechner) **50** verbunden, welcher der Verwaltung der Mautgebühreneinzüge der Mautstraßen gewidmet ist. Das lokale Steuergerät **26** sendet Mautgebühreneinzugsergebnisse, Informationen über Fahrzeuge, von welchen Mautgebühren nicht richtig eingezogen wurden, und dergleichen an das Zentralsteuergerät **50**.

[0052] In dem Mautstraßen-Mautabrechnungssystem gemäß der vorliegenden Ausführungsform sendet üblicherweise jeder der Transceiver **32**, **34**, ... und **42**, **44**, ... der Straßenrandvorrichtung **20** ein Pilotsignal zum Aktivieren der fahrzeuggebundenen Vorrichtungen **10**, die in entlang den entsprechenden Fahrstreifen fahrenden Fahrzeugen eingebaut sind, in vorbestimmten Zeitintervallen. Wenn die fahrzeuggebundene Vorrichtung

10, die dieses Pilotsignal empfangen hat, ein Antwortsignal ausgesendet hat und die Transceiver **32**, **34**, ..., **42**, **44**, ... dieses Antwortsignal empfangen haben, führt die Straßenrandvorrichtung **2** eine Datenkommunikation mit der fahrzeuggebundenen Vorrichtung **10** aus, um eine Mautgebühr einzuziehen.

[0053] Andererseits wird die fahrzeuggebundene Vorrichtung **10** in einem Ruhezustand gehalten, um zum Beispiel ihren Energieverbrauch zu senken, bis sie das Pilotsignal von der Straßenrandvorrichtung **20** empfängt, und nach Empfang des Pilotsignals wird sie aktiviert, um ein Antwortsignal zu senden, und führt danach eine Datenkommunikation mit dem Transceiver der Straßenrandvorrichtung **20** aus, um Mautgebühren zu entrichten.

[0054] Ferner werden Datenkommunikationsvorgänge, die zwischen der Straßenrandvorrichtung **20** und der fahrzeuggebundenen Vorrichtung **10**, die oben erwähnt sind, durchgeführt werden, alle unter der Aufsicht der Straßenrandvorrichtung **20** ausgeführt. Das heißt, beispielsweise in der vorliegenden Ausführungsform ist, wie in **Fig.** 3 dargestellt, jeder der Transceiver **32**, **34**, ... und **42**, **44**, ... der Straßenrandvorrichtung **20** so angeordnet, daß er das Pilotsignal oder ein moduliertes Signal zur Datenkommunikation innerhalb einer vorbestimmten Sendezeitdauer T1 sendet und danach während einer anschließenden vorbestimmten Antwortzeitdauer T2 eines unmoduliertes Trägerwellensignal sendet. Die fahrzeuggebundene Vorrichtung **10** sendet ein Antwortsignal auf das Pilotsignal oder Datensignal durch Modulieren des Trägerwellensignals. Demgemäß ist die Kommunikationsschaltung **18** der fahrzeuggebundenen Vorrichtung **10** beispielsweise so aufgebaut, wie in **Fig.** 2 gezeigt.

[0055] Das heißt, wie in **Fig.** 2 gezeigt, ist die Antenne **18a** in der Kommunikationsschaltung **18** über einen Übertragungsweg **62** mit der Anode einer Diode **63** verbunden. Die Kathode der gleichen Diode **63** ist über einen Übertragungsweg **64** mit einem Oszillator **65** verbunden. Die Länge dieses Übertragungsweges **64** ist auf λ/4 festgelegt, wobei λ die Wellenlänge des von der Straßenrandvorrichtung **20** aus gesendeten Trägerwellensignals ist. Die Anode und die Kathode der Diode **63** sind jeweils über eine Spule **68** und einen Widerstand **69** bzw. über eine Spule **70** und einen Widerstand **71** mit Masse verbunden.

[0056] Ferner bildet die Spule **68** zusammen mit einem Kondensator **72**, der parallel zu dem Widerstand **69** geschaltet ist, einen Tiefpaßfilter, während die Spule **70** zusammen mit einem Kondensator **73**, der parallel zu dem Widerstand **71** geschaltet ist, eine Tiefpaßfilter bildet. Darüber hinaus bilden diese Tiefpaßfilter zusammen mit der Diode **63** eine Hüllkurvendetektorschaltung **80** zum Erfassen bzw. Demodulieren der Hüllkurve des Empfangssignals.

[0057] Indessen ist die Anode der Diode **63** über einen Widerstand **74** und einen Transistor Tr3 mit einer Stromquelle VDD verbunden, ist der Oszillator **65** über einen Transistor Tr1 mit der Stromquelle VDD verbunden, und ist ein Verbindungspunkt der Spule **70** und des Widerstands **71** über einen Widerstand Tr2 mit der Stromquelle VDD verbunden. Die Basen dieser Transistoren Tr1, Tr2 und Tr3 sind mit dem Steuergerät **16** verbunden.

[0058] Auf diese Weise wird in der Kommunikationsschaltung **18**, wenn jeder der Transistoren Tr1, Tr2 und Tr3 durch das Steuergerät **16** deaktiviert ist, die Hüllkurve des Sendesignals von der Straßenrandvorrichtung **20**, das von der Antenne **18a** empfangen wird, durch die Hüllkurvendetektorschaltung **80** demoduliert, und das resultierende demodulierte Signal S1 wird als das Empfangssignal dem Steuergerät **16** bereitgestellt. Das heißt, in diesem Zustand empfängt die Kommunikationsschaltung **18** ein moduliertes Signal, das von der Straßenrandvorrichtung **20** gesendet worden ist, innerhalb der in **Fig.** 3 dargestellten Zeitdauer T1. Die Kommunikationsschaltung **18** demoduliert die Hüllkurve diesem Empfangssignals und stellt das resultierende Signal S1 (ein binäres Signal) als Empfangsdaten dem Steuergerät **16** bereit.

[0059] Als nächstes wird, wenn die Transistoren Tr1 und Tr3 deaktiviert werden und nur der Transistor Tr2 aktiviert wird, nachdem eine Spannung einer Stromquelle an die Kathode der Diode **63** angelegt wird, die Diode **61** über den Widerstand **69** in Sperrichtung vorgespannt. Demgemäß kann die Diode **63** in diesem Fall das Empfangssignal nicht weiterleiten, und demzufolge wird das Empfangssignal aus der Antenne **18a** durch den Eingangsanschluß (die Anodenseite) der Diode **63** reflektiert.

[0060] Andererseits wird, wenn die Transistoren Tr1 und Tr2 deaktiviert werden und nur der Transistor Tr3 aktiviert wird, nachdem die Stromquellenspannung an die Anode der Diode **63** angelegt wird, die Diode **63** über die Widerstände **74**, **71** in Durchlaßrichtung vorgespannt. Demgemäß wird die Diode **63** in diesem Fall in einen Zustand gebracht, der einen bidirektionalen Durchgang des Empfangssignals ermöglicht. Demzufolge durchläuft das Empfangssignal aus der Antenne **18a** die Diode **63** und wird dem Übertragungsweg **64** zugeführt und wird dann durch einen Eingangsanschluß des Oszillators **65**, der eine unendlich große Eingangsimpedanz aufweist, reflektiert. Ferner durchläuft diese reflektierte Welle die Diode **63** in Sperrichtung und durchläuft den Übertragungsweg **62** und wird dann von der Antenne **18a** aus abgestrahlt. Des weiteren weist zu dieser Zeit, nachdem die effektive Länge des Übertragungsweges **64** λ/4 beträgt, das von der Antenne **18a** abgestrahlte Signal eine Phasendifferenz von π (180°) bezüglich des Signals, das reflektiert wird, wenn die Transistoren Tr1 und Tr3 deaktiviert werden und nur der Transistor Tr2 aktiviert wird.

[0061] Aus diesem Grund kann in der Kommunikationsschaltung **18** dann, wenn die Transistoren Tr2 und Tr3 innerhalb der in **Fig.** 3 dargestellten Sendezeitdauer T2, in welcher das unmodulierte Trägerwellensignal von

der Straßenrandvorrichtung **20** aus gesendet wird, abwechselnd aktiviert und deaktiviert werden, das Trägerwellensignal (unter Verwendung einer Phasenumtastung) phasenmoduliert und von der Antenne **18a** aus gesendet werden.

[0062] Das heißt, in der vorliegenden Ausführungsform aktiviert und deaktiviert das Steuergerät **16**, nachdem die Kommunikationsschaltung **18** das Sendesignal von der Straßenrandvorrichtung **20** innerhalb der in **Fig.** 3 dargestellten Zeitdauer T1 empfängt und das Wellenerfassungssignal S1 an das Steuergerät **16** liefert, die Transistoren Tr2 und Tr3 in Übereinstimmung mit zu sendenden Daten in Reaktion auf dieses Signal, um die Phase des Trägerwellensignals zu modulieren und das resultierende modulierte Signal von der Antenne **18a** aus zu senden und dadurch eine Datenkommunikation mit der Straßenrandvorrichtung **20** durchzuführen.

[0063] Es ist festzuhalten, daß der Oszillator **65** und der Transistor Tr1 vorgesehen sind, um eine Datenkommunikation mit der Straßenrandvorrichtung eines Systems, welches keine unmodulierten Trägerwellensignale sendet, ermöglicht. In diesem Fall führt das Steuergerät **16** dem Oszillator **65** Strom zu, indem es den Transistor Tr1 aktiviert, um hierdurch den Oszillator **65** anzusteuern, um das Trägerwellensignal zu generieren. Auch kann in diesem Zustand durch abwechselndes Aktivieren und Deaktivieren der Transistoren Tr2 und Tr3 in Übereinstimmung mit den zu sendenden Daten, Umschalten zwischen einer Übertragung des Trägerwellensignals von dem Oszillator **65** über die Antenne **18a** und Blockieren des Trägerwellensignals von dem Oszillator **65** und Verhindern einer Übertragung dieses Signals von der Antenne **18a** aus durchgeführt werden. Das heißt, durch Durchführen dieser Umschaltung wird das Signal, welches durch Durchführen einer Amplitudentastung (ASK) bezüglich des Trägerwellensignals von dem Oszillator **65** in Übereinstimmung mit den Sendedaten erhalten wird, von der Antenne **18a** aus gesendet.

[0064] Als nächstes wird nachstehend ein Datenübertragungsvorgang, der zwischen der fahrzeuggebundenen Vorrichtung **10** und der Straßenrandvorrichtung **20** des Mautstraßen-Mautabrechnungssystems der vorliegenden Erfindung ausgeführt wird, und eine Datenverarbeitung, welche in der fahrzeuggebundenen Vorrichtung **10** zur Ausführung dieser Datenkommunikation ausgeführt wird, erläutert werden. Allerdings muß hier festgehalten werden, daß die nachstehende Erläuterung Kommunikationsvorgänge zwischen der Straßenrandvorrichtung **20** und der fahrzeuggebundenen Vorrichtung **10** betrifft, die dann ausgeführt werden, wenn die zu entrichtende Mautgebühr an der Einfahrt oder der Ausfahrt der mit der Straßenrandvorrichtung **20** versehenden Mautstraße einheitlich ist. Auf diese Weise können sich diese Vorgänge von jenen, welche ausgeführt werden, wenn die Mautgebühr in Übereinstimmung mit der zurückgelegten Entfernung oder der gefahrenen Zeit festgelegt wird, unterscheiden.

[0065] Zuerst ist in der fahrzeuggebundenen Vorrichtung **10 Fig.** 4 ein Flußdiagramm, welches einen Datenprozeß (Kartenladeprozeß) zeigt, der von dem Steuergerät **16** dann ausgeführt wird, wenn die IC-Karte **2** in eine Einführungsöffnung (nicht gezeigt) des IC-Karten-Laufwerks **12** geladen wird, um die Sendedaten vorzubereiten. Es ist festzuhalten, daß, nachdem die fahrzeuggebundene Vorrichtung **10** normalerweise in einem Ruhezustand gehalten wird, wie zuvor erwähnt, dieser Datenprozeß gestartet wird, wenn das Laden der IC-Karte **2** durch einen in dem IC-Karten-Laufwerk **12** vorgesehenen Sensor erfaßt worden ist und das resultierende Erfassungssignal dem Steuergerät **16** bereitgestellt worden ist, um dasselbe zu aktivieren.

[0066] Wie in **Fig.** 4 dargestellt, führt, wenn dieser Prozeß gestartet wird, zuerst Schritt **110** einen Selbstdiagnosetest durch, um zu bestimmen, ob das Steuergerät **16** selbst normal arbeitet oder nicht, während Schritt **120** bestimmt, ob das Testergebnis normal ist. Falls das Testergebnis eine Anomalie anzeigt, bestimmt Schritt **120**, daß ein Diagnosefehler vorliegt, und so schreitet die Steuerung zu Schritt **280** fort, welcher später beschrieben wird. Umgekehrt geht die Steuerung dann, wenn das Testergebnis normal ist, zu Schritt **130**, welcher eine Batterieprüfung durchführt, indem die Spannung einer Batterie (nicht gezeigt), welche der fahrzeuggebundenen Vorrichtung **10** eine Stromquellenspannung zuführt, bestimmt wird. Es muß hier festgehalten werden, daß es zwei Arten von Batterien gibt, welche nämlich eine austauschbare Batterie und eine versiegelte Batterie sind, und daß die Batterieprüfung hier eine Prüfung der Spannung dieser zwei Batterien einschließt.

[0067] Als nächstes bestimmt Schritt **140**, ob der Spannungspegel der austauschbaren Batterie sehr niedrig ist, so daß sie ersetzt werden muß. Wenn Schritt **140** bestimmt, daß der Batterieaustausch erforderlich ist, sendet Schritt **150** eine Austauschnachricht diesbezüglich an eine Anzeige (nicht gezeigt), und danach wird das Steuergerät **16** in einen Ruhemodus gestellt. Nachdem Schritt **140** bestimmt, daß keine Notwendigkeit vorliegt, die Batterie zu ersetzen, bestimmt Schritt **160**, obwohl die Batteriespannung ausreicht, um Vorgänge des Steuergeräts **16** und der Kommunikationsschaltung **18** sicherzustellen, ob die Batteriespannung zum Betreiben des IC-Karten-Laufwerks **12**, des Krypto-Moduls **14** und dergleichen unzureichend ist (das heißt, Schritt **160** bestimmt, ob die Batteriespannung niedrig ist oder nicht). Wenn bestimmt wird, daß der Batteriespannungspegel niedrig ist, zeigt Schritt **170** den Batteriezustand wie etwa einen Spannungswert in der Anzeigeeinheit an, und danach geht, wenn ein Batterieproblem bestimmt ist, die Steuerung zu Schritt **280**, welcher später beschrieben wird. Wenn der Batteriespannungspegel normal ist, geht die Steuerung zu Schritt **180**.

[0068] Bezüglich dieser Batterieprüfung muß festgehalten werden, daß nach eine Bestimmung, daß ein Batterieaustausch erforderlich ist oder daß die Batteriespannung niedrig ist, eine Nachricht diesbezüglich in der Anzeigeeinheit angezeigt wird, so daß der Insasse des Fahrzeugs den Zeitpunkt zum Austausch der Batterie

aus dem Inhalt der Anzeigenachricht erkennen und die fahrzeuggebundene Vorrichtung durch Austausch der Batterie in ihren normalen Betriebszustand zurückbringen kann.

[0069] Als nächstes aktiviert Schritt **180** die IC-Karte **2** (Aktivierung und Rücksetzen) unter Verwendung des IC-Karten-Laufwerks **12**, um vorbestimmte Kartendaten von der IC-Karte **2** zu lesen und zu prüfen, ob die in das IC-Karten-Laufwerk **12** geladene IC-Karte **2** in der fahrzeuggebundenen Vorrichtung **10** verwendet werden kann (IC-Karten-Prüfung).

[0070] Auf der Grundlage des Ergebnisse der IC-Karten-Prüfung bestimmt Schritt **190**, ob die IC-Karte **2** in der fahrzeuggebundenen Vorrichtung **10** verwendet werden kann oder nicht. Falls die IC-Karte **2** nicht verwendet werden kann, bestimmt Schritt **190** einen IC-Karten-Fehler, und so schreitet die Steuerung zu Schritt **280** fort, der später beschrieben wird. Falls die IC-Karte **2** verwendet werden kann, geht die Steuerung zu Schritt **200**, welcher das Krypto-Modul **14** aktiviert und ansteuert, um eine gegenseitige Verifikation mit der IC-Karte **2** durchzuführen. Es ist festzuhalten, daß dieser gegenseitig Verifikationsvorgang gemäß dem in **Fig.** 5 dargestellten Prozeß, welcher später beschrieben wird, über die Verwendung in Übereinstimmung mit dem vorgenannten DES-Algorithmus generierter verschlüsselter Daten ausgeführt wird.

[0071] Als nächstes bestimmt Schritt **210**, ob das Ergebnis der gegenseitigen Verifikation zwischen dem Krypto-Modul **14** und der IC-Karte **2** positiv ist oder nicht. Falls das Ergebnis der gegenseitigen Verifikation negativ ist, bestimmt Schritt **210**, daß ein Verifikationsfehler vorliegt, und so geht die Steuerung zu dem später beschriebenen Schritt **280**. Falls das Ergebnis der gegenseitigen Verifikation positiv ist, schreitet die Steuerung zu Schritt **220** fort.

[0072] Schritt **220** bestimmt, ob die IC-Karte **2** eine Guthabenkarte ist, welche die Vorauszahlung der Mautgebühren anzeigt, oder eine Kontokarte, welche eine Bezahlung der Mautgebühren unter Verwendung eines vorbestimmten Bankkontos erlaubt. Falls die IC-Karte **2** eine Kontokarte ist, schreitet die Steuerung zu Schritt **230** (Prüfung der Kontokarte) fort, welcher Karteninformationen, d. h., Gültigkeitsdauer der Karte, Vorliegen/Nichtvorliegen einer Verwendungsgrenze der Art der fahrzeuggebundenen Vorrichtung, und dergleichen, von der IC-Karte **2** aufspürt und prüft. Auf der Grundlage des Ergebnisses der Prüfung der Kontokarte bestimmt der anschließende Schritt **250**, ob die Kontokarte verwendet werden kann oder nicht. Falls die Kontokarte nicht verwendet werden kann, bestimmt Schritt **250**, daß ein Kontokartenfehler aufgetreten ist, und so geht die Steuerung zu Schritt **280**, der später beschrieben wird. Umgekehrt schreitet die Steuerung zu Schritt **270** fort, wenn die Kontokarte verwendet werden kann.

[0073] Im übrigen dient, während erwähnt worden ist, daß die Kontokarte die Verwendungsgrenze der Art der fahrzeuggebundenen Vorrichtung als ihre Karteninformation speichern kann, diese Information zum Beschränken der Verwendung der Kontokarte nur auf bestimmte Arten einer fahrzeuggebundenen Vorrichtung, und zu diesem Zweck ist in der Kontokarte ein Identifikationscode gespeichert.

[0074] Falls andererseits die IC-Karte **2** eine Guthabenkarte ist, schreitet die Steuerung zu Schritt **240** (Prüfung der Guthabenkarte) fort, welcher Informationen in der Guthabenkarte wie etwa Gültigkeitsdauer, verbleibendes Guthaben, etc. ausliest und die Karteninformationen prüft. Auf der Grundlage des Kartenprüfergebnisses bestimmt der anschließende Schritt **260**, ob die Guthabenkarte verwendet werden kann oder nicht. Falls die Guthabenkarte nicht verwendet werden kann, bestimmt Schritt **260**, daß ein Guthabenkartenfehler aufgetreten ist, und so schreitet die Steuerung zu dem später beschriebenen Schritt **280** fort. Umgekehrt schreitet, falls die Guthabenkarte verwendet werden kann, die Steuerung zu Schritt **270** fort.

[0075] Schritt **270** führt einen Prozeß zum Abrufen eines Mautabrechnungsschlüssels Z, der beim Einziehen der Mautgebühr von der IC-Karte **2** verwendet wird, und Speichern der Einziehungsergebnisse (Datum/Zeit der Verwendung, verbleibendes Guthaben) in derselben IC-Karte **2** aus, und danach schreitet die Verarbeitung zu einem anschließenden Schritt **290** fort. Das heißt, die IC-Karte **2** verwendet verschlüsselte Daten zum Aktualisieren ihrer Daten, um ein leichtes Überschreiben der gespeicherten Daten zu verhindern. Hierbei veranlaßt das Steuergerät **16** in diesem Zustand die IC-Karte **2** dazu, einen Schlüssel Z (Mautabrechnungsschlüssel), der zum Erzeugen verschlüsselter Daten zur Aktualisierung der Kartendaten benötigt wird, zu erzeugen, liest und speichert diesen Schlüssel Z, und danach schreitet die Steuerung zu Schritt **290** fort. Es ist festzuhalten, daß der Mautabrechnungsschlüssel Z unter Verwendung des DES-Algorithmus durch Verschlüsseln von Karteninformationen wie etwa der Anzahl von Verarbeitungen und dergleichen auf der Grundlage eines speziellen IC-Kartenschlüssels (IC-Kartenschlüssels), welcher der IC-Karte **2** im Voraus zugewiesen wird, erzeugt wird.

[0076] Wenn andererseits irgend einer der Schritte **120**, **160**, **190**, **210**, **250** oder **260** einen Fehler in der fahrzeuggebundenen Vorrichtung **10** oder der IC-Karte **2** bestimmt, wird in Schritt **280** ein Fehlerstatusflag gesetzt, welches den Inhalt eines solchen Fehlers anzeigt, und danach schreitet die Verarbeitung zu Schritt **290** fort.

[0077] Als nächstes veranlaßt Schritt **290** das Krypto-Modul **14** dazu, einen Schlüssel (Kommunikationsschlüssel X1) zu erzeugen, welcher zum Verschlüsseln an die Straßenrandvorrichtung **20** zu sendender Daten verwendet werden wird, und Schritt **300** speichert einen solchen Kommunikationsschlüssel X1. Hier muß festgehalten werden, daß, wenn das Krypto-Modul **14** den Befehl zum Generieren des Kommunikationsschlüssels X1 von dem Steuergerät **16** empfängt, das Krypto-Modul **14** zuerst eine Zufallszahl R1 generiert und den Kommunikationsschlüssel X1 auf der Grundlage dieser Zufallszahl R1 und eines Kommunikationshauptschlüssels

einer Verschlüsselungsschlüsselzahl Kn, die unter mehreren Arten von Verschlüsselungsschlüsselzahlen ausgewählt wird, erzeugt. Ebenso wird hier zur Erzeugung dieses Kommunikationsschlüssels X1 ein Verschlüsselungsalgorithmus (nachstehend als ein FX-Algorithmus bezeichnet) verwendet, welcher im Vergleich mit dem DES-Algorithmus eine Verschlüsselung mit hoher Geschwindigkeit ermöglicht.

[0078] Hierbei ist zur Verwendung als der FX-Algorithmus ein Verschlüsselungsalgorithmus, der SAFER·K – 64 (Secure And Fast Encryption Routine of Length 64 bits) genannt wird, von J. L. Massey aus der Schweiz, oder FEAL (Fast Data Encipherment Algorithm) von H. Matsumoto von NTT, Japan, geeignet.

[0079] Nach Erzeugen des vorgenannten Kommunikationsschlüssels X1 liest Schritt **310** die Daten der fahrzeuggebundenen Vorrichtung (erste Lesedaten) RD1, welche an die Straßenrandvorrichtung **21** zu senden sind. Ein anschließender Schritt **320** stellt diese Daten dem Krypto-Modul **14** bereit, welches dazu veranlaßt wird, diese Daten RD1 unter Verwendung des vorgenannten Kommunikationsschlüssels X1 zu verschlüsseln. Es ist festzuhalten, daß auch für diese Verschlüsselungsverarbeitung der FX-Algorithmus verwendet wird.

[0080] Nachdem die ersten Lesedaten RD1 durch das Krypto-Modul **14** verschlüsselt worden sind, werden die verschlüsselten ersten Lesedaten <RD1> durch Schritt **330** als die an die Straßenrandvorrichtung **20** zu sendenden Sendedaten gespeichert. Dann informiert Schritt **340** die Insassen des Fahrzeugs von dem Zustand der Karte auf der Grundlage des in Schritt **280** gesetzten Fehlerstatus, Kartendaten aus der IC-Karte **2**, etc., und danach tritt das Steuergerät **16** in einen Ruhemodus ein.

[0081] Hierbei ist festzuhalten, daß dieser Vorgang eines Berichtens des Kartenzustands gleichzeitig mit einem Anzeigen von Nachrichten und dergleichen in der Anzeigevorrichtung durch Erzeugen von Tönen unter Verwendung eines Summers durchgeführt wird. Das heißt, durch Informieren des Insassen des Fahrzeugs über den Kartentyp, das verbleibende Guthaben der IC-Karte **2**, die Anomalie der Karte, etc. unter Verwendung sowohl optischer als auch akustischer Verfahren kann der Fahrzeuginsasse dazu veranlaßt werden, die Karte, die er zur Bezahlung der Mautgebühr verwendet, zu verifizieren, und kann dazu veranlaßt werden, die Karte auszutauschen, falls eine Anomalie vorliegt.

[0082] Auch enthalten zum Beispiel, wie in TABELLE 1 dargestellt, die ersten Lesedaten RD1, die als die Sendedaten gespeichert sind, einen Antwortcode für den Transceiver der Straßenrandvorrichtung **20**, einen Statuscode wie etwa Fehlerstatusdaten, welche den Betriebszustand der fahrzeuggebundenen Vorrichtung **10** repräsentieren, einen Gebührenzahlungsmodus, welcher ein Mautgebührenzahlungsverfahren etc. repräsentiert, einen Fahrzeugvorrichtungscode, welcher jeder fahrzeuggebundenen Vorrichtung eindeutig zugeordnet ist, eine Seriennummer CSN der IC-Karte **2**, Guthabendaten der IC-Karte **2**, ein exklusives ODER (CSN XOR CAN) der Seriennummer CSN der IC-Karte **2** und einer Anwendungsnummer CAN, welche den Typ der IC-Karte **2** repräsentiert, einen Transaktionszähler CTC, welcher die letzte Position zum Speichern der verarbeiteten Daten in der IC-Karte **2** repräsentiert, einen Zeiger, welcher den Typ des IC-Karten-Schlüssel, der zur Verschlüsselung der Kartendaten auf der IC-Karte **2** gemäß dem DES-Algorithmus verwendet wird, repräsentiert (Zeiger des verwendeten Schlüssels), etc. Unter diesen Datenelementen werden der Statuscode, der Gebührenzahlungsmodus, der Fahrzeugvorrichtungscode, die Seriennummer CSN und ein Teil der Guthabendaten verschlüsselt, während die verbleibenden Datenelemente unverändert in einem unverschlüsselten Zustand als die Sendedaten festgelegt und gespeichert werden.

TABELLE 1

KOMM.-SIGNALE 1. GERÜST	INHALT
1. PILOTSIGNAL (STRASSENRANDVORRICHTUNG)	PILOTSIGNAL ORTS-NR.
1. PILOTANTWORTSIGNAL (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE ZUFALLSZAHL R1 VERSCHLÜSSELUNGSSCHLÜSSELZAHL Kn
STRASSENRANDVERIFIKATIONS- NACHRICHT (STRASSENRANDVORRICHTUNG)	DATENABRUFBEFEHL ZUFALLSZAHL R3 VERSCHLÜSSELUNGSSCHLÜSSELZAHL KC
1. LESEDATEN (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE STATUSCODE* (FEHLERCODE) ZAHLUNGSMODUS* FAHRZEUGVORRICHTUNGSCODE* CSN* GUTHABEN* (TEILWEISE VERSCHLUESSELT) CSN XOR CAN CTC ZEIGER DES VERWENDETEN SCHLUESSELS
1. SCHREIBDATEN (STRASSENRANDVORRICHTUNG)	SCHREIBBEFEHL FAHRZEUGVORRICHTUNGSCODE** GESAMTMAUTGEBUEHR** ORTS-NR. (TEILWEISE VERSCHL.)** TRANSAKTIONSART DATUM ZEIT
ENDSIGNAL (FZ.-GEB. VORR.)	ANTWORTCODE
ENDBESTAETIGUNGSSIGNAL (STRASSENRANDVORRICHTUNG)	ENDBESTAETIGUNG

BEACHTE:

BEZEICHNET IN DER FAHRZEUGGEBUNDEN VORRICHTUNG VERSCHLUESSELTE DATEN
BEZEICHNET IN DER STRASSENRANDVORRICHTUNG VERSCHLUESSELTE DATEN

[0083] Als nächstes wird der gegenseitige Verifikationsprozeß von Schritt **200** zwischen der IC-Karte **2** und dem Krypto-Modul **14** ausgeführt, wie in **Fig.** 5 dargestellt. Es ist festzuhalten, daß in den Vorgängen der IC-Karte **2** und des Krypto-Moduls **14**, die nachstehend in Verbindung mit **Fig.** 5 erläutert werden, zum Generieren der verschiedenen Daten Funktionen verwendet werden, die auf dem DES-Algorithmus basieren.

[0084] Das heißt, wie in **Fig.** 5 dargestellt, veranlaßt das Steuergerät **16** dann, wenn diese gegenseitige Verifikation durchgeführt wird, zuerst die IC-Karte **2**, Kartendaten, welche die Seriennummer CSN, die Anwendungsnummer CAN, etc. enthalten, zu generieren (Schritt **3100**), und danach ruft das Steuergerät **16** solche Daten ab (Schritt **1100**). Das Steuergerät **16** sendet die abgerufenen Kartendaten (CSN, CAN) an das Krypto-Modul **14** und stellt einen Befehl zum Erzeugen einer Zufallszahl R an das Krypto-Modul **14** bereit (Schritt **1200**). Dann empfängt, nachdem das Krypto-Modul **14** eine Zufallszahl R in Übereinstimmung mit diesem Befehl erzeugt (Schritt **2100**), das Steuergerät **16** diese Zufallszahl R und stellt diese Zufallszahl R der IC-Karte

2 zusammen mit einem Befehl zum Erzeugen eines Verifikationsverschlüsselungsschlüssels Y bereit (Schritt **1300**).

[0085] Auf einen Empfang des Befehls zum Erzeugen des Verifikationsverschlüsselungsschlüssels Y hin ruft die IC-Karte **2** die Kartendaten aus der Speicherposition, die dem Transaktionszähler CTC entspricht, ab, und verschlüsselt unter Verwendung eines Verschlüsselungschlüssels, der sich unter den vorgenannten voreingestellten IC-Karten-Schlüsseln befindet, diese Kartendaten, um den Verifikationsverschlüsselungsschlüssel Y zu erzeugen (Schritt **3200**). Darüber hinaus verschlüsselt die IC-Karte **2** unter Verwendung dieses Verifikationsverschlüsselungsschlüssels Y die Zufallszahl R (Schritt **3300**).

[0086] Wenn die Zufallszahl R wie oben erwähnt in der IC-Karte **2** verschlüsselt worden ist, liest das Steuergerät **16** diese verschlüsselten Daten <R> und die Kartendaten, die für die Erzeugung des Verifikationsverschlüsselungsschlüssels Y verwendet worden sind, und stellt dem Krypto-Modul **14** einen Befehl zum Erzeugen eines Verifikationsverschlüsselungsschlüssels Y zusammen mit diesen Daten bereit (Schritt **1400**).

[0087] Dann bestimmt das Krypto-Modul **14** das exklusive ODER (CSN XOR CAN) der Seriennummer CSN und der Anwendungsnummer CAS der IC-Karte **2** und erzeugt unter Verwendung dieser exklusiven ODER-Daten und eines vorgeschriebenen Hauptschlüssels einen Verifikationsschlüssel, der der IC-Karte **2** eigentümlich ist. Dann erzeugt das Krypto-Modul unter Verwendung dieses Verschlüsselungschlüssels und der Kartendaten den Verifikationsverschlüsselungsschlüssel Y (Schritt **2200**) und verschlüsselt die Zufallszahl R (Schritt **2300**) unter Verwendung dieses Verschlüsselungschlüssels Y. Dann vergleicht das Krypto-Modul **14** die verschlüsselten Daten <R>' der Zufallszahl R, welche es verschlüsselt hat, mit den verschlüsselten Daten <R> der Zufallszahl R, die in der IC-Karte **2** verschlüsselt worden sind (Schritt **2400**). Falls beide verschlüsselten Daten zusammenpassen, bestimmt das Krypto-Modul **14**, daß die in den IC-Karten-Laufwerk **12** geladene IC-Karte **2** normal ist (Schritt **2500**). Es ist festzuhalten, daß, falls beide verschlüsselten Daten nicht zusammenpassen, das Steuergerät **16** bestimmt, daß ein Verifikationsfehler vorliegt, und so schreitet die Steuerung zu dem Prozeß von Schritt **280** fort.

[0088] Auf eine Vollendung der vorgenannten Verifikation der IC-Karte **2** auf der Seite des Krypto-Moduls **14** hin fordert das Steuergerät **16** das Krypto-Modul **14** auf, die auf der Seite der IC-Karte **2** zur Verifikation des Krypto-Moduls **14** verwendeten Verifikationsdaten zu generieren (Schritt **1500**). Demgemäß erzeugt das Krypto-Modul **14** einen von der IC-Karte **2**. besessenen Krypto-Modul-Verschlüsselungschlüssel SC durch Verwenden des exklusiven ODERs (CSN XOR CAN) der Seriennummer CSN und der Anwendungsnummer CAN der IC-Karte **2** und einen vorgeschriebenen IC-Karten-Schlüssel. Darüber hinaus verschlüsselt das Krypto-Modul **14** diesen Schlüssel SC durch Verwenden des Verifikationsverschlüsselungsschlüssels Y, der in Schritt **220** generiert worden ist, um dadurch die Verifikationsdaten SC' zu erzeugen (Schritt **2600**).

[0089] Wenn dann die Verifikationsdaten SC' wie zuvor erwähnt erzeugt sind, liest das Steuergerät **16** diese Verifikationsdaten SC' und sendet sie zusammen mit einem Befehl zum Ausführen einer Verifikation an die IC-Karte **2** (Schritt **1600**). Dann entschlüsselt die IC-Karte **2** die empfangenen Verifikationsdaten SC' unter Verwendung des Verifikationsverschlüsselungsschlüssels Y, der in Schritt **3200** erzeugt worden ist, und bestimmt, ob die entschlüsselten Verifikationsdaten SC' (=SC) mit dem von ihr besessenen Schlüssel zusammenpassen (Schritt **3400**). Wenn die Verifikationsdaten SC', SC zusammenpassen, bestimmt die IC-Karte **2**, daß das Krypto-Modul **14** (in anderen Worten, die fahrzeuggebundene Vorrichtung **10**) der mit der IC-Karte **2** geladenen fahrzeuggebundenen Vorrichtung **10** normal ist (Schritt **3500**). Wenn die Seite der IC-Karte **2** ebenfalls verifiziert, daß das Krypto-Modul **14** normal ist, bestimmt das Steuergerät **16**, daß die gegenseitige Verifikation erfolgreich durchgeführt worden ist (Schritt **1700**), und die Steuerung schreitet dann von Schritt **210** zu Schritt **220** fort. Umgekehrt bestimmt das Steuergerät **16** dann, wenn das Krypto-Modul **14** durch die Seite der IC-Karte **2** nicht positiv verifiziert wird, daß diese Fehlanpassung ein Verifikationsfehler ist, und die Steuerung schreitet zu Schritt **280** fort.

[0090] Als nächstes ist **Fig.** 6 ein Flußdiagramm, welches den jeweils in Transceivern **32**, **34**, die in dem ersten Gerüst **30** der Straßenrandvorrichtung **20** vorgesehen sind, ausgeführten Kommunikationsprozeß darstellt. Es ist festzuhalten, daß die nachstehende Erläuterung unter der Annahme erstellt wurde, daß der nachstehende Kommunikationsprozeß durch den Transceiver **32** ausgeführt wird.

[0091] Wie in **Fig.** 6 dargestellt, wird in Schritt **4100** ein erstes Pilotsignal zum Aktivieren der in einem Ruhezustand gehaltenen fahrzeuggebundenen Vorrichtung **10** gesendet. Danach bestimmt Schritt **4200** während Sendens eines Trägerwellensignals, welches durch die fahrzeuggebundene Vorrichtung **10** beim Rücksenden eines Antwortsignals während der Zeitdauer T2 verwendet werden wird, ob durch die Antenne **32a** ein erstes Pilotantwortsignal empfangen worden ist oder nicht. Wenn kein ersten Pilotantwortsignal empfangen wird, kehrt die Steuerung erneut zu Schritt **4100** zurück, welcher das erste Pilotsignal erneut sendet. Auf diese Weise sendet der Transceiver **32** das erste Pilotsignal für jede vorgeschriebene Zeitdauer t.

[0092] Das heißt, wenn sich ein Fahrzeug der Umgebung des ersten Gerüsts **30** nähert und in den Kommunikationsbereich des dem Fahrstreifen, auf welchem das Fahrzeug fährt, entsprechenden Transceivers **32** eintritt, empfängt die in dem Fahrzeug eingebaute fahrzeuggebundene Vorrichtung **10** das erste Pilotsignal von dem Transceiver **32** und wird aus ihrem Ruhezustand heraus aktiviert. Dann sendet, wie in **Fig.** 7 dargestellt,

die fahrzeuggebundene Vorrichtung **10** in Reaktion auf dieses erste Pilotsignal das erste Pilotantwortsignal zurück. Daher sendet der Transceiver **32** in Schritten **4100** und **4200** das erste Pilotsignal in periodischer Weise, um hierdurch zu bestimmen, ob das erste Pilotantwortsignal während dieses periodischen Sendevorgangs empfangen worden ist. Auf diese Weise wartet der Transceiver **32** weiterhin auf den Eintritt des Fahrzeugs in seinen eigenen Kommunikationsbereich.

[0093] Im übrigen beinhaltet, wie in TABELLE 1 dargestellt, das durch jeden der Transceiver **32**, **34** des ersten Gerüsts **30** gesendete erste Pilotsignal das Pilotsignal zum Starten der fahrzeuggebundenen Vorrichtung **10** und eine Ortszahl, die den Transceiver angibt, von welchem aus das Signal gesendet wurde. Das erste Pilotantwortsignal, das von der fahrzeuggebundenen Vorrichtung **10** in Reaktion auf das erste Pilotsignal gesendet wird, enthält einen Antwortcode, eine Zufallszahl R1, welche die Grundlage des zum Erzeugen der ersten Lesedaten verwendeten Kommunikationsschlüssels X1 bildet, und die Schlüsselzahl (Verschlüsselungschlüsselzahl) Kn des Kommunikationshauptschlüssels.

[0094] Wenn das von der fahrzeuggebundenen Vorrichtung **10** in Reaktion auf das erste Pilotsignal gesendete erste Pilotantwortsignal empfangen wird, geht die Steuerung zu Schritt **4300**, welcher der Krypto-Einheit **32b** die Zufallszahl R1 und die Verschlüsselungschlüsselzahl Kn, die in dem ersten Pilotantwortsignal enthalten ist, und einen Befehl zum Erzeugen des Kommunikationsschlüssels X1 bereitstellt.

[0095] Dann verwendet die Krypto-Einheit **32b** auf der Grundlage der empfangenen Zufallszahl R1 und der Verschlüsselungschlüsselzahl Kn den FX-Algorithmus, um den durch die fahrzeuggebundene Vorrichtung **10** bei der Erzeugung der ersten Lesedaten <RD1> verwendeten Kommunikationsschlüssel X1 zu erzeugen. Die Krypto-Einheit **32b** erzeugt auch eine Zufallszahl R3, welche die Grundlage eines Kommunikationsschlüssels X2 bildet, der durch die fahrzeuggebundene Vorrichtung **10** bei der Verschlüsselung der nächsten Sendedaten (zweiten Lesedaten) verwendet werden wird, und eine Schlüsselzahl eines Kommunikationshauptschlüssels (Verschlüsselungschlüsselzahl) Kc.

[0096] Schritt **4400** ruft die Zufallszahl R3 und die Verschlüsselungschlüsselzahl Kc ab und sendet eine Straßenrandvorrichtungsverifikationsnachricht (siehe TABELLE 1), welche diese Werte sowie einen Auslesebefehl der ersten Lesedaten enthält, wie in **Fig.** 7 gezeigt.

[0097] Indessen sendet, wie zuvor erwähnt, der Transceiver **32** bei der Übertragung dieser Straßenrandvorrichtungsverifikationsnachricht anschließend während der vorgeschriebenen Zeitdauer T2 ein unmoduliertes Trägersignal. Wie in **Fig.** 7 dargestellt, sendet der Transceiver **432** auch die Straßenrandvorrichtungsverifikationsnachricht, erste Schreibdaten und ein Endbestätigungssignal (später beschrieben), etc. für jede vorbestimmte Zeitdauer t in gleicher Weise wie bei der Übertragung des ersten Pilotsignals während regulären Betriebs.

[0098] Als nächstes empfängt Schritt **4500** bei der Übertragung der Straßenrandvorrichtungsverifikationsnachricht an die fahrzeuggebundene Vorrichtung **10**, wie zuvor erwähnt, nachdem die fahrzeuggebundene Vorrichtung **10** die ersten Lesedaten <RD1>, die im Voraus erzeugt worden sind, wenn die IC-Karte **2** hierin geladen wird, zurücksendet, die ersten Lesedaten <RD1>, bis die Trägerwellensendezeitdauer T2 verstreicht. Dann bestimmt Schritt **4600**, wenn die Trägerwellensendezeitdauer T2 verstreicht, ob die ersten Lesedaten <RD1> während dieser Sendezeitdauer empfangen worden sind, um zu prüfen, ob ein Kommunikationsfehler aufgetreten ist.

[0099] Falls ein Kommunikationsfehler aufgetreten ist, wird ein Fehlerstatuscode gesetzt, und hiernach wird dieser Prozeß vorübergehend beendet. Falls kein Kommunikationsfehler vorliegt, schreitet die Operation zu Schritt **4700** fort, welcher der Krypto-Einheit **32b** einen Befehl zum Entschlüsseln der empfangenen ersten Lesedaten <RD1> bereitstellt. Auf den Empfang der Anforderung zum Entschlüsseln der ersten Lesedaten <RD1> hin entschlüsselt die Krypto-Einheit **32b** die ersten Lesedaten <RD1> in Übereinstimmung mit dem FX-Algorithmus unter Verwendung des Kommunikationsschlüssels X1, der auf der Grundlage der Zufallszahl R1 und der Kommunikationsverschlüsselungschlüsselzahl Kc zuvor erzeugt worden ist. Auf diese Weise liest Schritt **4800**, nachdem Schritt **4700** den Befehl zur Entschlüsselung der ersten Lesedaten <RD1> generiert, die entschlüsselten Daten RD1.

[0100] Schritt **4900** bestimmt auf der Grundlage eines Statuscodes in diesen entschlüsselten Daten RD1, ob in den entschlüsselten ersten Lesedaten RD1 ein Fehler vorliegt. Falls ein Datenfehler vorliegt, schreitet die Steuerung zu Schritt **5400** fort. Falls in den ersten Lesedaten RD1 kein Fehler vorliegt, schreitet die Steuerung zu Schritt **5000** fort.

[0101] Schritt **5000** bestimmt gemäß den ersten Lesedaten RD1, ob die IC-Karte **2** in der fahrzeuggebundenen Vorrichtung **10** eine Guthabenkarte oder eine Kontokarte ist. Falls die IC-Karte **2** eine Kontokarte ist, schreitet die Steuerung zu Schritt **5100** fort, welcher auf der Grundlage beispielsweise des Fahrzeugvorrichtungscodes einen Fahrzeugtyp bestimmt, und die Mautgebühr wird in Übereinstimmung mit dem Fahrzeugtyp berechnet, und anschließend geht die Steuerung zu Schritt **5500**. Falls die IC-Karte **2** andererseits eine Guthabenkarte ist, schreitet der Vorgang zu Schritt **5200** fort, welcher den Fahrzeugtyp beispielsweise auf der Grundlage des Fahrzeugvorrichtungscodes bestimmt, und die Mautgebühr wird in Übereinstimmung mit dem Fahrzeugtyp berechnet. Der anschließende Schritt **5300** bestimmt aus dem Guthaben der Guthabenkarte, ob

die Mautgebühr bezahlt werden kann oder nicht. Wenn Schritt **5300** bestimmt, daß das Guthaben auf der Guthabenkarte zur Entrichtung der Mautgebühr ausreicht, schreitet die Steuerung dann zu Schritt **5500** fort. Wenn Schritt **5300** andererseits bestimmt, daß das Guthaben auf der Guthabenkarte zur Entrichtung der Mautgebühr nicht ausreicht, geht die Steuerung zu Schritt **5400**.

[0102] Indessen führt Schritt **5400**, falls ein Fehler in den entschlüsselten ersten Lesedaten RD1 vorliegt oder falls aus der IC-Karte **2** (insbesondere der Guthabenkarte) keine Mautgebühr eingezogen werden kann, eine Fehlerverarbeitung zur Übertragung von Fehlerdaten diesbezüglich auf die Seite der fahrzeuggebundenen Vorrichtung **10** und auch zum Setzen eines Fehlerstatuscodes durch. Auf eine Vollendung dieser Fehlerverarbeitung hin schreitet die Operation zu Schritt **5900** fort.

[0103] Als nächstes generiert Schritt **5500** erste Schreibdaten WD1 zum Einzug der Mautgebühr von der Seite der fahrzeuggebundenen Vorrichtung **10** und stellt die Daten der Krypto-Einheit **32b** bereit, und so steuert der Transceiver **32** die Krypto-Einheit **32b** an, um die ersten Schreibdaten WD1 zu verschlüsseln. Nachdem die Krypto-Einheit **32b** die ersten Schreibdaten WD1 verschlüsselt, ruft der Transceiver **32** diese verschlüsselten ersten Schreibdaten <WD1> ab und sendet sie an die fahrzeuggebundene Vorrichtung **10**, wie in **Fig.** 7 gezeigt. Es ist festzuhalten, daß der Transceiver **32** während dieser Übertragung nach Senden des den ersten Schreibdaten <WD1> entsprechenden modulierten Signals während der vorgeschriebenen Zeitdauer T2 auch ein unmoduliertes Trägerwellensignal sendet.

[0104] Hierbei enthalten, wie in TABELLE 1 dargestellt, die ersten Schreibdaten WD1 zum Beispiel den Schreibbefehl zum Speichern des Zahlungsergebnisses der Mautgebühr in die IC-Karte **2** auf der Seite der fahrzeuggebundenen Vorrichtung **10**, den Fahrzeugvorrichtungscode, die Gesamtsumme der Mautgebühren, die Ortsnummer des Transceivers **32**, den Transaktionstyp, der den Typ eines Gebühreneinzugs (d. h., einen Pauschalgebühreneinzug, einen gemäß der zurückgelegten Strecke variierenden Gebühreneinzug, oder einen zeitabhängigen Gebühreneinzug) wiedergibt, und das Datum und die Zeit.

[0105] Unter diesen Datenelementen werden der Fahrzeugvorrichtungscode, die Gesamtsumme der Mautgebühren und ein Teil der Ortsnummer jeweils verschlüsselt, und die verbleibenden Datenelemente werden als unverschlüsselte reguläre Sendedaten unberührt belassen (erste Schreibdaten <WD1>).

[0106] Des weiteren führt die Krypto-Einheit **32b** beim Verschlüsseln dieser ersten Schreibdaten WD1 ihre Verschlüsselungsverarbeitung in Übereinstimmung mit dem FX-Algorithmus unter Verwendung des zuvor generierten Kommunikationsschlüssels X1 durch. Das heißt, nachdem die Krypto-Einheit **32b** (auch die Krypto-Einheit **34b**) anders als das Krypto-Modul **14** auf der Seite der fahrzeuggebundenen Vorrichtung **10** nur zur Kommunikation mit der fahrzeuggebundenen Vorrichtung **10** verwendet wird, führt die Krypto-Einheit **32b** die Erzeugung der Schlüssel wie auch die Verschlüsselung und Entschlüsselung der Daten durch Verwendung nur des FX-Algorithmus durch, welcher der Kommunikationsverschlüsselungsalgorithmus ist.

[0107] Als nächstes sendet die fahrzeuggebundene Vorrichtung **10** nach Empfang der gesendeten ersten Schreibdaten <WD1> ein Endsignal, das den Antwortcode diesbezüglich enthält, wie in **Fig.** 7 dargestellt. Daher führt der Transceiver **32** nach Senden der ersten Schreibdaten <WD1> die Endsignalempfangsverarbeitung (Schritt **5700**) während der vorgeschriebenen Zeitdauer T2 aus. Nach Verstreichen der vorgeschriebenen Zeitdauer T2 bestimmt Schritt **5800**, ob das Endsignal empfangen worden ist, um das Vorliegen oder Nichtvorliegen eines Kommunikationsfehlers zu prüfen. Falls ein Kommunikationsfehler vorliegt, setzt der Transceiver **32** den Fehlerstatuscode und beendet hiernach diesen Prozeß. Falls kein Kommunikationsfehler vorliegt, schreitet die Steuerung zu Schritt **5900** fort.

[0108] Schritt **5900** stellt dem in dem Hauptteil der Straßenrandvorrichtung **20** eingebauten lokalen Steuergerät **26** die vorgenannten entschlüsselten ersten Lesedaten RD1, einen Fehlerstatus, der in dem Fehlerprozeß (in Schritt **5400**) gesetzt worden ist, etc. bereit. Der anschließende Schritt **6000** sendet ein Endbestätigungssignal an die fahrzeuggebundene Vorrichtung **10**. Dieses Endbestätigungssignal dient als ein Kommunikationsvollendungssignal, um die fahrzeuggebundene Vorrichtung **10** über die Vollendung der Datenkommunikation zu informieren, und das erste Pilotsignal (siehe **Fig.** 7), und hiernach endet dieser Prozeß.

[0109] Indessen wird, wie zuvor erwähnt, nach dem Endbestätigungssignal das erste Pilotsignal gesendet, um die in dem Fahrzeug, welches als nächstes in den Kommunikationsbereich eingetreten ist, geladene fahrzeuggebundene Vorrichtung **10** schnell zu aktivieren. Durch diesen Sendevorgang ist es möglich, die Verzögerungen beim Aktivieren der fahrzeuggebundenen Vorrichtung **10** zu vermeiden und so eine kürzere Kommunikationszeit bereitzustellen.

[0110] Des weiteren bestimmt der Transceiver **32** nach Senden des ersten Pilotsignals in Schritt **6000** durch Durchführung eines Bestimmungsprozesses (nicht gezeigt) ähnlich dem von Schritt **4200**, ob das erste Pilotantwortsignal durch die fahrzeuggebundene Vorrichtung **10** in Reaktion auf das erste Pilotsignal gesendet worden ist. Nach Empfang des ersten Pilotantwortsignals schreitet die Steuerung zu Schritt **4200** fort, und eine Kommunikation mit der fahrzeuggebundenen Vorrichtung, welche dieses erste Pilotantwortsignal gesendet hat, wird begonnen. Wenn das erste Pilotantwortsignal nicht empfangen wird, schreitet die Steuerung zu Schritt **4100** fort, wodurch der Vorgang zu dem normalen Betrieb eines Sendens des ersten Pilotsignals für jede vorgeschriebenen Zeitdauer t [ms] zurückkehrt.

[0111] Als nächstes ist **Fig.** 8 ein Flußdiagramm, welches den durch die fahrzeuggebundene Vorrichtung **10** nach Empfang des ersten Pilotsignals von den in dem ersten Gerüst **30** vorgesehenen Transceivern **32**, **34**, ... und nach Ausführen der Kommunikationsverarbeitung mit dem Transceiver, der das erste Pilotsignal gesendet hat, ausgeführten Datenprozeß (ersten Gerüstduruchgangsprozeß), der auf die vorgenannte Prozedur folgt.

[0112] Wie in **Fig.** 8 gezeigt, aktiviert die Kommunikationsschaltung **18** in der fahrzeuggebundenen Vorrichtung **10** das Steuergerät **16** nach einem Empfang des ersten Pilotsignals von dem Transceiver des ersten Gerüsts **30**, z. B. dem Transceiver **32**. Dann führt Schritt **6100** einen Kommunikationsprozeß zur Durchführung einer Datenkommunikation mit dem Transceiver **32** über die Kommunikationsschaltung **18** aus. Auf Empfang der erste Schreibdaten <WD1> von dem Transceiver **32** hin sendet das Steuergerät **16** das Endsignal über die Kommunikationsschaltung **18**, beendet die Kommunikationsverarbeitung (Schritt **6100**) und führt den ersten Gerüstdurchgangsprozeß von Schritt **6200** und nachfolgender Schritte aus.

[0113] Schritt **6200** bestimmt, ob die Kommunikationsschaltung **18** das Endbestätigungssignal von dem Transceiver **32** empfangen hat. Falls das Steuergerät **16** das Endbestätigungssignal noch nicht empfangen hat, schreitet die Steuerung zu Schritt **6300** fort, in welchem das Steuergerät **16** über die Kommunikationsschaltung **18** ein Befehlssignal zur Anforderung der Übertragung des Endbestätigungssignals unter Verwendung des unmodulierten Trägerwellensignals, das dem ersten Pilotsignal oder einem Sendesignal an die fahrzeuggebundene Vorrichtung **10** nachfolgt und das durch den Transceiver **32** für jede vorbestimmte Zeitdauer t gesendet wird, sendet.

[0114] Ebenso bestimmt der anschließende Schritt **6400**, ob das Sendesignal wie etwa das erste Pilotsignal von dem Transceiver **32** durch die Kommunikationsschaltung **18** empfangen worden ist; in anderen Worten, das Steuergerät **16** bestimmt, ob das Fahrzeug den Kommunikationsbereich des Transceivers **32** verlassen hat oder nicht. Falls sich das Fahrzeug noch immer innerhalb des Kommunikationsbereichs befindet, schreitet die Steuerung erneut zu Schritt **6200** fort, welcher bestimmt, ob der Transceiver **32** das Endbestätigungssignal in Reaktion auf das vorgenannte Anforderungssignal gesendet hat.

[0115] Falls kein Endbestätigungssignal empfangen worden ist, schreitet die Steuerung erneut zu Schritt **6300** fort. Danach werden Schritte **6200** bis **6400** wiederholt, bis das Fahrzeug aus dem Kommunikationsbereich des Transceivers **32** austritt oder das Endbestätigungssignal empfangen wird.

[0116] Das heißt, falls das Endbestätigungssignal beim Passieren des ersten Gerüsts **30** nach Vollendung einer Kommunikation mit dem Transceiver **32** nicht empfangen werden kann, sendet das Steuergerät **16** das Endbestätigungssignal-Anforderungssignal an den Transceiver **32**, um denselben Transceiver **32** anzuweisen, das Endbestätigungssignal erneut zu senden.

[0117] Daher kann auf der Seite der fahrzeuggebundenen Vorrichtung **10** das Steuergerät **16** die Vollendung der Kommunikation mit dem Transceiver **32** zuverlässig verifizieren. Selbst wenn kein Endbestätigungssignal empfangen wird, kann das Steuergerät **16** über den Transceiver **32** die Straßenrandvorrichtung **20** über diesen Punkt informieren. Dies ermöglicht eine gegenseitige Verifikation eines Kommunikationsfehlers zwischen diesen.

[0118] Wenn das Steuergerät **16** das Endbestätigungssignal empfängt oder das Fahrzeug die Kommunikationsbereiche der Transceiver **32**, **34**, ... des ersten Gerüsts verläßt, geht die Steuerung zu Schritt **6500**, welcher einen Befehl an das Krypto-Modul **14** generiert, um die von der Straßenrandvorrichtung **20** empfangenen ersten Schreibdaten <WD1> zu entschlüsseln. Dann liest, nachdem das Krypto-Modul **14** die ersten Schreibdaten <WD1> in Übereinstimmung mit dem FX-Algorithmus unter Verwendung des Kommunikationsschlüssels X1 entschlüsselt, der anschließende Schritt **6600** die entschlüsselten ersten Schreibdaten WD1 aus und verifiziert die Straßenrandvorrichtung **20** (genauer, den Transceiver, der die ersten Schreibdaten WD1 gesendet hat) auf der Grundlage des Fahrzeugvorrichtungscodes, der in den ersten Schreibdaten WD1 enthalten ist, und des Fahrzeugvorrichtungscodes der fahrzeuggebundenen Vorrichtung **10**.

[0119] Schritt **6700** bestimmt, ob das Verifikationsergebnis von Schritt **6600** für die Straßenrandvorrichtung **20** positiv ist oder nicht. Falls die zwei Fahrzeugvorrichtungscodes nicht zusammenpassen und Schritt **6700** demzufolge bestimmt, daß die Straßenrandvorrichtung nicht positiv verifiziert werden kann, setzt Schritt **6800** einen Fehlerstatuscode diesbezüglich, und dann tritt das Steuergerät **16** in einen Ruhemodus ein. Falls Schritt **6700** die positive Verifikation der Straßenrandvorrichtung **20** bestimmt, wenn beide Fahrzeugvorrichtungscodes zusammenpassen, schreitet die Steuerung zu Schritt **6900** fort.

[0120] Wenn Schritt **6900** die Zufallszahl R3 und die Verschlüsselungschlüsselzahl Kc, die während der vorherigen Datenkommunikation von der Seite der Straßenrandvorrichtung **20** empfangen wird, an das Krypto-Modul **14** sendet, wird das Krypto-Modul **14** von dem Steuergerät **16** angesteuert, um den für die nächste Datenkommunikation verwendeten Kommunikationsschlüssel X2 zu erzeugen, und ändert den Kommunikationsschlüssel von X1 zu X2. Es ist festzuhalten, daß nach Empfang der Zufallszahl R3 und der Verschlüsselungschlüsselzahl Kc das Krypto-Modul **1** den Kommunikationsschlüssel X2 in Übereinstimmung mit dem FX-Algorithmus unter Verwendung der Daten und des Kommunikationshauptschlüssels, der der Zufallszahl R3 und der Verschlüsselungschlüsselzahl Kc entspricht, generiert.

[0121] Wenn der Kommunikationsschlüssel von X1 zu X2 geändert ist, wie zuvor erwähnt, bestimmt Schritt

7000 den Typ der IC-Karte **2**. Falls die IC-Karte **2** eine Guthabenkarte ist, bestimmt Schritt **7100**, ob die Guthabenkarte ein ausreichendes Guthaben zur Entrichtung der Mautgebühr aufweist. Falls das Guthaben nicht ausreicht, setzt Schritt **7200** die Mautgebührensumme auf Null, und die Steuerung geht zu Schritt **7300**. Falls das Guthaben zur Entrichtung der Mautgebühr ausreicht, geht die Steuerung zu Schritt **7300**.

[0122] Schritt **7300** führt einen Mautabrechnungsprozeß zum Abziehen der Mautgebühr von der IC-Karte **2**, die eine Guthabenkarte ist, durch und Schritt **7400** bestimmt, ob die Mautgebühr richtig von der Guthabenkarte abgezogen worden ist. Falls die Mautgebühr nicht von der Guthabenkarte abgezogen werden kann, das heißt, falls das Guthaben in der Guthabenkarte nicht ausreicht oder die normale Ausführung des Mautabrechnungsprozesses fehlgeschlagen ist, geht die Steuerung zu Schritt **7500**, welcher ein Fehlerstatusflag setzt, und danach tritt das Steuergerät **16** in einen Ruhemodus ein. Umgekehrt schreitet, falls die Mautgebühr erfolgreich und richtig abgezogen worden ist, die Steuerung zu Schritt **7800** fort.

[0123] Des weiteren schreitet, wenn Schritt **7000** bestimmt, daß die IC-Karte **2** eine Kontokarte ist, die Steuerung zu Schritt **7600** fort, welcher die Kontodaten für die Entrichtung der Mautgebühr unter Verwendung der Kontokarte ausliest, und dann geht die Steuerung zu Schritt **7700**, welcher bestimmt, ob die abgerufenen Kontodaten richtig sind oder nicht. Wenn die Kontodaten nicht richtig sind, tritt das Steuergerät **16** in einen Ruhemodus ein, und wenn die Kontodaten richtig sind, schreitet die Steuerung zu Schritt **7800** fort.

[0124] Als nächstes stellt Schritt **7800** dem Krypto-Modul **14** die Fahrzeugvorrichtungsdaten (zweite Lesedaten) RD2 bereit, welche als nächstes an die Straßenrandvorrichtung **20** gesendet werden werden, und steuert das Krypto-Modul **14** an, um diese zweiten Lesedaten RD2 unter Verwendung des durch Schritt **6900** zu X2 geänderten Kommunikationsschlüssels zu verschlüsseln. Es ist festzuhalten, daß für diesen Verschlüsselungsvorgang erneut der FX-Algorithmus verwendet wird. Nach Verschlüsselung der zweiten Lesedaten RD2 durch das Krypto-Modul **14** speichert Schritt **7900** die verschlüsselten Daten <RD2> als die nächsten Sendedaten, und Schritt **8000** speichert Zahlungsdaten, z. B. Datum, Zeit und Ort, bei welchen die Mautgebühr entrichtet worden ist, in der IC-Karte **2**, um die Kartendaten zu aktualisieren. Schritt **8100** liest die aktualisierten Kartendaten und speichert die aktualisierten Daten, und danach tritt das Steuergerät **16** in einen Ruhemodus ein.

[0125] Hierbei werden der Mautabrechnungsprozeß (Schritt **7300**) zum Abziehen der Mautgebühr von der Guthabenkarte und der Kartendatenaktualisierungsprozeß (Schritt **800**) zum Aktualisieren der Daten der IC-Karte übrigens unter Verwendung der Daten ausgeführt, die in Übereinstimmung mit dem DES-Algorithmus unter Verwendung des vorgenannten Mautabrechnungsschlüssels Z, der im Voraus gespeichert wird, verschlüsselt worden sind.

[0126] Indessen enthalten beispielsweise, wie in TABELLE 2 gezeigt, die in Schritt **7800** verschlüsselten und in Schritt **7900** als die Sendedaten gespeicherten Lesedaten RD2 den Antwortcode für die Kommunikationsvorrichtung der Straßenrandvorrichtung **20**, Kontokarten-Dateidaten (Kontodaten, etc.) in dem Fall, daß die IC-Karte **2** eine Kontokarte ist, einen Statuscode wie etwa einen Fehlerstatuscode, der den Betriebszustand der Seite der fahrzeuggebundenen Vorrichtung **10** anzeigt, ein Zahlungsverfahren, ein Einzugsergebnis der Mautgebühr, einen Fahrzeugvorrichtungscode, eine Anwendungsnummer CAN der IC-Karte **2**, die Zufallszahl R3, Mautgebühreneinzugsverifikationdaten zur Bestätigung, daß der Mautgebühreneinzug auf der Seite der fahrzeuggebundenen Vorrichtung **10** durchgeführt worden ist, und dergleichen. Unter diesen Datenelementen werden der Antwortcode und ein Teil der Kontokarten-Dateidaten unverändert in ihrem unmodulierten Normalzustand belassen, während alle verbleibenden Datenelemente verschlüsselt werden.

[0127] Während die zweiten Lesedaten RD2 in Übereinstimmung mit dem FX-Algorithmus in der gleichen Weise wie jener der ersten Lesedaten RD1 verschlüsselt werden, muß hier festgehalten werden, daß unter den Datenelementen der zweiten Lesedaten RD2 die Mautgebühreinzugsverifikationsdaten bereits auf der Seite der IC-Karte **2** in Übereinstimmung mit dem DES-Algorithmus unter Verwendung des IC-Karten-Schlüssels verschlüsselt werden und diese Verifikationsdaten daher zweimal verschlüsselt werden, indem sie während der Sendezeit unter Verwendung des FX-Algorithmus weiter verschlüsselt werden.

[0128] Als nächstes ist **Fig.** 10 ein Flußdiagramm, welches den in den Transceivern **42**, **44**, ..., die in dem zweiten Gerüst **40** der Straßenrandvorrichtung **20** vorgesehen sind, ausgeführten Kommunikationsprozeß darstellt. Es ist festzuhalten, daß in der nachstehenden Erläuterung angenommen wird, daß dieser Prozeß durch den Transceiver **42** ausgeführt wird.

[0129] Wie in **Fig.** 9 dargestellt, überträgt Schritt **9100** wie in dem Fall der Transceiver **32**, **34**, ... des ersten Gerüsts **30** das zweite Pilotsignal zum Starten der fahrzeuggebundenen Vorrichtung **10**, die sich in einem Ruhemodus befindet. Während Sendens des Trägerwellensignals, das durch die fahrzeuggebundene Vorrichtung **10** zum Senden des Antwortsignals verwendet werden wird, während der vorgeschriebenen Zeitdauer T2 bestimmt Schritt **9200**, ob das zweite Pilotantwortsignal durch die Antenne **42a** empfangen worden ist oder nicht. Während kein zweites Pilotantwortsignal empfangen wird, fährt der Transceiver **42** fort, für jede vorbestimmte Zeitdauer t [ms] das zweite Pilotsignal in einer solchen Weise zu senden, daß die Steuerung zum Senden des zweiten Pilotsignals erneut zu Schritt **9100** zurückkehrt.

TABELLE 2

KOMM.-SIGNALE 2. GERÜST	INHALT
2. PILOTSIGNAL (STRASSENRANDVORRICHTUNG)	2. PILOTSIGNAL ORTS-NR.
2. PILOTANTWORTSIGNAL (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE ZAHLUNGSMODUSDATEN
DATENABRUFSIGNAL (FAHRZEUGGEB. VORRICHTUNG)	DATENABRUFBEFEHL
2. LESEDATEN (STRASSENRANDVORRICHTUNG)	ANTWORTCODE KONTOKARTENDATEI* (TEILVERSCHLÜSSELT) STATUSCODE* ZAHLUNGSMODUS* GEBUEHRENEINZUGSERGEBNIS* FAHRZEUGVORRICHTUNGSCODE* CSN* ZUFALLSZAHL R3* MAUTEINZUGSBESTAETIGUNGSDATEN*
2. SCHREIBDATEN (STRASSENRANDVORRICHTUNG)	SCHREIBBEFEHL ANZEIGEBEFEHL ANZEIGENACHRICHT
ENDSIGNAL (FZ.-GEB. VORR.)	ANTWORTCODE
ENDBESTAETIGUNGSSIGNAL (STRASSENRANDVORRICHTUNG)	ENDBESTAETIGUNG

BEACHTE:

BEZEICHNET IN DER FAHRZEUGGEBUNDENEN VORRICHTUNG VERSCHLUESSELTE DATEN

[0130] Wenn die fahrzeuggebundene Vorrichtung **10** das zweite Pilotsignal empfängt und aus dem Ruhezustand heraus aktiviert wird, sendet sie in Reaktion auf dieses zweite Pilotsignal das zweite Pilotantwortsignal, wie in **Fig.** 10 dargestellt. Dann schreitet die Steuerung nach Empfang dieses Antwortsignals zu Schritt **9300** fort, welcher den Typ der in der fahrzeuggebundenen Vorrichtung **10** geladenen IC-Karte **2** auf der Grundlage des Pilotantwortsignals bestimmt. Das heißt, nachdem die fahrzeuggebundene Vorrichtung **10** so eingerichtet ist, daß sie die den Antwortcode repräsentierenden Zahlungsmodusdaten und das Gebühreneinzugsverfahren als das zweite Pilotantwortsignal (siehe TABELLE 2) nach Empfang des zweiten Pilotsignals sendet, bestimmt der Transceiver **42** aus diesen Zahlungsmodusdaten, ob die IC-Karte **2** auf der Seite der fahrzeuggebundenen Vorrichtung **10** eine Kontokarte oder eine Guthabenkarte ist.

[0131] Falls die IC-Karte **2** eine Guthabenkarte ist, schreitet die Steuerung zu Schritt **9500** fort. Falls die IC-Karte **2** eine Kontokarte ist, stellt Schritt **9400** dem lokalen Steuergerät **26** des Hauptteils der Straßenrandvorrichtung **20** einen Befehl zum Suchen einer Anzeigenachricht bereit, um eine an die fahrzeuggebundene Vorrichtung **10** zu sendende Anzeigenachricht zu suchen, und danach schreitet die Steuerung zu Schritt **9500** fort. Es ist festzuhalten, daß das lokale Steuergerät **26** auf einen Empfang dieses Befehls zum Suchen einer Anzeigenachricht hin den Verwendungszustand der Kontokarte etc. sucht, um dadurch die an die Seite der fahrzeuggebundenen Vorrichtung **10** zu sendende Anzeigenachricht zu erzeugen, und diese an den Transceiver **42** überträgt (siehe **Fig.** 10).

[0132] Als nächstes sendet Schritt **9500** ein Datenleseanforderungssignal an die fahrzeuggebundene Vorrichtung **10**, um die Übertragung der zweiten Lesedaten <RD2> anzufordern, und danach führt Schritt **9600**

einen Prozeß aus, um während Sendens des unmodulierten Trägerwellensignals während der vorgeschriebenen Zeitdauer T2 auf den Empfang der zweiten Lesedaten <RD2> von der fahrzeuggebundenen Vorrichtung **10** zu warten. Wenn die vorgeschriebene Zeitdauer T2 verstrichen ist, bestimmt Schritt **9700** das Auftreten oder Nichtauftreten eines Kommunikationsfehlers durch Bestimmen, ob Schritt **9500** in seinem Empfang der zweiten Lesedaten <RD2> erfolgreich war. Wenn ein Kommunikationsfehler vorliegt, setzt der Transceiver **42** einen Fehlerstatuscode, und dann endet dieser Prozeß vorerst.

[0133] Wenn die fahrzeuggebundene Vorrichtung **10** andererseits in Reaktion auf das Datenlesesignal, das durch Schritt **9500** übertragen worden ist, die zweiten Lesedaten <RD2> sendet, schreitet die Steuerung zu Schritt **9800** fort, welcher zweite Schreibdaten WD2 generiert und dieselben Daten der fahrzeuggebundenen Vorrichtung **10** bereitstellt. Wie in TABELLE 2 gezeigt, enthalten die zweiten Schreibdaten WD2 Schreib/Anzeigebefehle zum Ansteuern der fahrzeuggebundenen Vorrichtung **10**, um Informationen zur Anzeige, daß die zweiten Lesedaten <RD2> durch das zweite Gerüst **40** empfangen worden sind, die Anzeigenachricht, die in dem lokalen Steuergerät **26** abgerufen und erzeugt wird, wenn die IC-Karte **2** eine Kontokarte ist, oder dergleichen zu speichern und anzuzeigen.

[0134] Nachdem die fahrzeuggebundene Vorrichtung **10** nach Empfang der zweiten Schreibdaten WD2 das aus dem Antwortcode bestehende Endsignal sendet, wie in **Fig.** 10 dargestellt, führt Schritt **9900** die Empfangsverarbeitung aus, in welcher er während Sendens des unmodulierten Trägerwellensignals während der vorgeschriebenen Zeitdauer T2 auf die Übertragung des Endsignals von der fahrzeuggebundenen Vorrichtung **10** wartet. Wenn die vorgeschriebene Zeitdauer T2 verstreicht, bestimmt Schritt **10000** das Vorliegen eines Kommunikationsfehlers durch Bestimmen, ob Schritt **9900** im Empfang des Endsignals erfolgreich war.

[0135] Wenn ein Kommunikationsfehler vorliegt, setzt der Transceiver **42** ein Fehlerstatusflag, und dann endet dieser Prozeß. Fall kein Kommunikationsfehler vorliegt, sendet Schritt **10100** die Fahrzeugvorrichtungsdaten, nämlich die von der fahrzeuggebundenen Vorrichtung **10** empfangenen zweiten Lesedaten <RD2>, an das lokale Steuergerät **26**, und der anschließende Schritt **10200** sendet das Endbestätigungssignal und das zweite Pilotsignal (siehe **Fig.** 11) an die fahrzeuggebundene Vorrichtung **10**, und dann endet dieser Prozeß.

[0136] Im Übrigen führt der Transceiver **42**, nachdem Schritt **10200** das zweite Pilotsignal gesendet hat, wie in dem Fall der durch die Transceiver **32**, **34** des ersten Gerüsts **30** eine Bestimmungsverarbeitung (nicht gezeigt) ähnlich dem Schritt **9200** zum Bestimmen, ob von der fahrzeuggebundenen Vorrichtung **10** in Reaktion auf das zweite Pilotsignal das zweite Pilotantwortsignal gesendet worden ist. Wenn der Transceiver **42** das zweite Pilotantwortsignal empfängt, schreitet die Steuerung zu Schritt **9300** fort. Wenn der Transceiver **42** darin versagt, das zweite Pilotantwortsignal zu empfangen, schreitet die Steuerung zu Schritt **9100** fort.

[0137] Des weiteren sind die durch Schritt **10100** an das lokale Steuergerät **26** gesendeten zweiten Lesedaten <RD2> verschlüsselte Daten, die in Übereinstimmung mit dem FX-Algorithmus verschlüsselt worden sind, und die darin enthaltenen Gebühreneinzugsverifikationsdaten sind solche, die in Übereinstimmung mit dem DES-Algorithmus weiter verschlüsselt worden sind. Daher werden die Gebühreneinzugsverifikationsdaten unter Verwendung des eingebauten Verschlüsslers des lokalen Steuergeräts **26** entschlüsselt. Wenn die Gebühreneinzugsverifikationsdaten, die unter Verwendung des FX-Algorithmus entschlüsselt worden sind, unter Verwendung des DES-Algorithmus weiter entschlüsselt werden, bestimmt das lokale Steuergerät **26** den durch die IC-Karte **2** während der Verschlüsselung der Gebühreneinzugsverifikationsdaten verwendeten Verschlüsselungschlüssel in der folgenden Weise und verwendet diesen Verschlüsselungschlüssel, um die Gebühreneinzugsverifikationsdaten zu entschlüsseln. Das lokale Steuergerät **26** bestimmt den der in der fahrzeuggebundenen Vorrichtung **10** geladenen IC-Karte **2** eigentümlichen IC-Karten-Schlüssel unter Verwendung des Zeigers des Schlüssels in den ersten Lesedaten RD1 von der fahrzeuggebundenen Vorrichtung **10** und generiert anschließend den Entschlüsselungsschlüssel.

[0138] Wenn die fahrzeuggebundene Vorrichtung **10** nach Empfang des zweiten Pilotsignals von den Transceivern **42**, **44**, ... des zweiten Gerüsts **40** aktiv wird und dieselbe fahrzeuggebundene Vorrichtung **10** eine Kommunikation mit dem Transceiver, der das zweite Pilotsignal gesendet hat, auf der Grundlage der vorgenannten Prozedur durchführt, führt das Steuergerät **16** der fahrzeuggebundenen Vorrichtung **10** eine Datenverarbeitungsprozedur (Durchgangsverarbeitung des zweiten Gerüsts **40**) aus, welche durch das Flußdiagramm von **Fig.** 11 gezeigt ist.

[0139] Wenn Schritt **11100** die zweiten Schreibdaten WD2 über eine Datenkommunikation mit den Transceivern **42**, **44**, ... des zweiten Gerüsts **40** empfängt und das Endsignal sendet, um dadurch die Datenkommunikation zu beenden, bestimmt Schritt **11200**, wie in **Fig.** 11 dargestellt, in gleicher Weise wie während der Zeit einer Vollendung der Kommunikation mit dem ersten Gerüst **30**, ob das Endbestätigungssignal empfangen worden ist oder nicht. Falls das Endbestätigungssignal nicht empfangen worden ist, sendet Schritt **11300** ein Endbestätigungssignalsendeanforderungssignal durch Ausnutzen des unmodulierten Trägerwellensignals, welches der Transceiver **42**, **44**, ... gesendet hat. Des weiteren bestimmt Schritt **11400**, ob das Fahrzeug den Kommunikationsbereich des zweiten Gerüsts **40** verlassen hat. Falls sich das Fahrzeug noch immer innerhalb dieses Kommunikationsbereichs befindet, schreitet die Steuerung zu Schritt **11200** fort. Nach Beendigung der Kommunikationsverarbeitung von Schritt **11100** werden die Schritte **11200** und **11400** wiederholt ausgeführt,

bis das Fahrzeug den Kommunikationsbereich des zweiten Gerüsts **40** verläßt oder das Steuergerät **16** in seinem Empfang des Endbestätigungssignals erfolgreich ist.

[0140] Wenn das Endbestätigungssignal empfangen wird oder wenn das Fahrzeug den Kommunikationsbereich des zweiten Gerüsts **40** verlassen hat, schreitet die Steuerung zu Schritt **11500** fort, welcher das Krypto-Modul **14** dazu veranlaßt, erneut den Kommunikationsschlüssel X1 zum Verschlüsseln der Sendedaten zu erzeugen, wie in dem Fall des zuvor erwähnten Schritts **290**, und Schritt **11600** speichert diesen Kommunikationsschlüssel X1. Schritt **11700** liest die Fahrzeugvorrichtungsdaten (ersten Lesedaten) RD1, die als nächstes an die Straßenrandvorrichtung **20** zu senden sind, und veranlaßt das Krypto-Modul **14** dazu, solche Daten unter Verwendung des Kommunikationsschlüssels X1 zu verschlüsseln, während Schritt **11800** die verschlüsselten ersten Lesedaten <RD1> speichert. Es ist festzuhalten, daß die Prozedur zum Erzeugen des Kommunikationsschlüssels X1 und der Verschlüsselungsvorgang der ersten Lesedaten RD1 in dem Krypto-Modul **14** vollständig die gleichen sind wie jene, die ausgeführt werden, wenn die IC-Karte in das IC-Karten-Laufwerk **12** geladen wird. Der einzige Unterschied zwischen diesen besteht darin, daß unter den Fahrzeugvorrichtungsdatenelementen, die in den ersten Lesedaten RD1 enthalten sind, der Inhalt des Datenelements bezüglich der IC-Karte **2** auf den geladenen Inhalt geändert wird, der durch Schritt **8100** gespeichert wird.

[0141] Wenn die zuvor verschlüsselten ersten Lesedaten <RD1> gespeichert sind, prüft Schritt **11900** den Zustand der fahrzeuggebundenen Vorrichtung **10** auf der Grundlage beispielsweise des Fehlerstatusflags, welches gesetzt ist, wenn ein Fehler vorliegt. Falls ein Fehler vorliegt, schreitet die Steuerung zu Schritt **11300** fort, welcher den Insassen unter Verwendung eines Summers oder dergleichen über den Fehler informiert. Falls kein Fehler vorliegt, schreitet die Steuerung zu Schritt **11200** fort, welcher den Insassen des Fahrzeugs unter Verwendung eines Summers und einer Anzeigevorrichtung über den Zustand der Karte informiert. Dann tritt das Steuergerät **16** in einen Ruhemodus ein. Es ist festzuhalten, daß der angezeigte Inhalt des Zustands der Karte beispielsweise das Guthaben der Karte ist, falls die IC-Karte **2** eine Guthabenkarte ist. Falls die IC-Karte **2** eine Kontokarte ist, sind die Inhalte der Anzeige beispielsweise der verwendete Betrag und die Nachricht, die in den zweiten Schreibdaten <WD2> enthalten sind.

[0142] Als nächstes ist **Fig.** 12 ein Flußdiagramm, welches den Datenprozeß (Kartenentfernungsprozeß) zeigt, der durch das Steuergerät ausgeführt wird, wenn die IC-Karte **2** aus dem IC-Karten-Laufwerk **12** der fahrzeuggebundenen Vorrichtung **10** entfernt wird. Es ist festzuhalten, daß dieser Prozeß begonnen wird, wenn die Entfernung der IC-Karte **2** durch einen in dem IC-Karten-Laufwerk **12** vorgesehenen Sensor erfaßt worden ist und das resultierende Erfassungssignal dem Steuergerät **16** bereitgestellt worden ist, um dasselbe Steuergerät **16** zu aktivieren.

[0143] Wenn dieser Prozeß begonnen wird, setzt, wie in **Fig.** 12 dargestellt, Schritt **12100** zuerst ein Fehlerstatusflag, welches angibt, daß die IC-Karte **2** entfernt worden ist und daß die fahrzeuggebundene Vorrichtung **10** keine Karte zur Entrichtung der Mautgebühr aufweist.

[0144] Ein nachfolgender Schritt **12200** liest die Fahrzeugvorrichtungsdaten nach Setzen des Fehlerstatusflags, um den Inhalt der ersten Lesedaten nach Verschlüsselung <RD1> zu aktualisieren, um dem Fehlerstatusflag zu entsprechen. Dann stellt Schritt **12200** dem Krypto-Modul **14** die Fahrzeugvorrichtungsdaten bereit, um dasselbe anzusteuern, um die verschlüsselten ersten Lesedaten <RD1> zu generieren.

[0145] Wenn die ersten Lesedaten <RD1> durch das Krypto-Modul **14** erzeugt werden, aktualisiert Schritt **12300** die ersten Lesedaten <RD1> als die Sendedaten, welche als nächstes an die Straßenrandvorrichtung **20** gesendet werden, und nachdem Schritt **12400** den Verwendungszustand der extrahierten IC-Karte **2** etc. anzeigt, tritt das Steuergerät **16** in einen Ruhemodus ein.

[0146] Wie oben erläutert, ist in dem Mautstraßen-Mautabrechnungssystem gemäß der vorliegenden Ausführungsform die Zeit, zu welcher die fahrzeuggebundene Vorrichtung **10** die Verschlüsselung der Sendedaten und die Entschlüsselung der Empfangsdaten durchführt, die Zeit, zu welcher die IC-Karte **2** zur Entrichtung der Gebühr in das IC-Karten-Laufwerk **12** geladen wird, das Zeitintervall von der Vollendung der Kommunikationsprozeduren zwischen dem Steuergerät **16** und den in dem ersten Gerüst **30** der Straßenrandvorrichtung **20** vorgesehenen Transceivern **32**, **34**, ... bis zu dem Eintritt des Fahrzeugs in den Kommunikationsbereich der in dem zweiten Gerüst **40** vorgesehenen Transceiver **42**, **44**, ..., nach der Vollendung von Kommunikationen mit dem zweiten Gerüst **40**, und die Zeit, zu welcher die IC-Karte **2** aus dem IC-Karten-Laufwerk **12** entfernt wird. Das heißt, das Steuergerät **16** führt während der Kommunikation mit jedem der Transceiver **32**, **34**, ... und **42**, **44**, ... der Straßenrandvorrichtung **20** weder eine Verschlüsselung noch eine Entschlüsselung durch. Ebenso führt das Steuergerät **16** auch bezüglich des Lesens der Karteninformationen von der IC-Karte **2** und des Aktualisierens der Kartendaten während einer Kommunikation mit jedem der Transceiver **32**, **34**, ... und **42**, **44**, ... der Seite der Straßenrandvorrichtung **20** keine Verschlüsselungs- und Entschlüsselungsvorgänge durch.

[0147] Auf diese Weise ist es möglich, die Verarbeitungszeit, die durch die fahrzeuggebundene Vorrichtung **10** während einer Datenkommunikation mit der Straßenrandvorrichtung **20** verbraucht wird, drastisch zu reduzieren, und daher kann die zur Ausführung der Datenkommunikation benötigte Zeitdauer reduziert werden. Diese ermöglicht eine fehlerfreie Ausführung einer Datenkommunikation für eine kurze Zeitdauer ohne Begrenzung der Reisegeschwindigkeit des Fahrzeugs oder Änderung des Krypto-Moduls **14** in ein teures, wel-

ches die Ausführung einer Hochgeschwindigkeitsverarbeitung ermöglicht.

[0148] Des weiteren führt die fahrzeuggebundene Vorrichtung **10** dann, wenn die IC-Karte **2** in das IC-Karten-Laufwerk **12** geladen worden ist, die gegenseitige Verifikationsprozedur zwischen der IC-Karte **2** und dem Krypto-Modul **14** aus und sendet die Statusinformationen (Fehlerstatus), welcher das Ergebnis dieser Verifikationsprozedur repräsentiert, als ein Element der Fahrzeugvorrichtungsdaten an die Straßenrandvorrichtung **20**. Daher ist es in dem Fall, daß die IC-Karte **2** oder die fahrzeuggebundene Vorrichtung **10** selbst gefälscht sind, möglich, diese Information in der Straßenrandvorrichtung **20** zu erfahren. Demgemäß ist es möglich, eine Täuschung des Fahrzeuginsassen zu kontrollieren, und somit kann ein Gebühreneinzug richtig durchgeführt werden.

[0149] Des weiteren werden, während Daten unter Verwendung des allgemein in der Technologie eingesetzten DES-Algorithmus verschlüsselt werden, wenn eine solche gegenseitig Verifikation oder ein Schreiben der Daten in die IC-Karte **2** durchgeführt werden, Daten während einer Kommunikation zwischen der fahrzeuggebundenen Vorrichtung **10** und der Straßenrandvorrichtung **20** in Übereinstimmung mit dem FX-Algorithmus verschlüsselt, der sich von dem DES-Algorithmus unterscheidet und der eine Verschlüsselung mit höherer Geschwindigkeit als dieser erlaubt.

[0150] Aus diesem Grund ist es möglich, in Transceivern **32**, **34**, ..., die in dem ersten Gerüst **30** vorgesehen sind, die während einer Datenkommunikation zur Durchführung der Verschlüsselung der Sendedaten und Entschlüsselung der Empfangsdaten benötigte Zeitdauer zu verkürzen, und somit kann eine Datenkommunikation bei höheren Geschwindigkeiten und höheren Genauigkeitsniveaus durchgeführt werden. Auch kann, falls der zuvor erwähnte, "SAFER·K – 64" oder "FEAL" genannte Verschlüsselungsalgorithmus als der FX-Algorithmus verwendet wird, die Verschlüsselungseinheit vergleichsweise preiswert durch eine Hardware-Konstruktion implementiert werden. Auf diese Weise kann die zur Durchführung des Verschlüsselungsvorgangs benötigte Zeitdauer verkürzt werden, und daher ist die Verwendung eines solchen Verschlüsselungsalgorithmus sehr effizient.

[0151] Des weiteren wird, wie zuvor erwähnt, in der vorliegenden Ausführungsform der FX-Algorithmus, der sich von dem allgemein verwendeten DES-Algorithmus unterscheidet, für die Datenkommunikation zwischen der fahrzeuggebundenen Vorrichtung **10** und der Straßenrandvorrichtung **20** verwendet. Aus diesem Grund wird es selbst dann, wenn das Kommunikationssignal abgefangen wird, schwierig sein, dasselbe Signal zu entschlüsseln. Zusätzlich werden in der vorliegenden Ausführungsform beim Verschlüsseln der Sendedaten nicht die gesamten Daten verschlüsselt, sondern ein Teil hiervon in einer herkömmlichen unverschlüsselten Weise unverändert belassen, und ferner werden die Kommunikationsschlüssel (X1, X2) jeweils auf der Grundlage der Verwendung der Zufallszahl, die jedes Mal, wenn sie verwendet wird, generiert wird, aktualisiert. Auf diese Weise werden die Daten schwieriger zu entschlüsseln. Dies ermöglicht die weitere Erhöhung der Kommunikationssicherheit.

[0152] Des weiteren kann, nachdem die Kommunikationsschlüssel X1 und X2 sowohl in der fahrzeuggebundenen Vorrichtung **10** als auch der Kommunikationsvorrichtung der Straßenrandvorrichtung **20** festgelegt werden, selbst dann, wenn der Fahrzeuginsasse versucht, durch Verwendung eines Senders, der ein durch Kopieren des Sendesignals von der autorisierten fahrzeuggebundenen Vorrichtung **10** erhaltenes Signal generiert, eine Entrichtung von Mautgebühren vorzutäuschen, dieser rechtswidrige Vorgang in der Straßenrandvorrichtung **20** zuverlässig erkannt werden, und somit kann die Kommunikationssicherheit erhöht werden.

[0153] Andererseits werden in der vorliegenden Ausführungsform Fehler wie etwa das Ergebnis der zuvor erwähnten gegenseitigen Verifikation, die auf der Seite der fahrzeuggebundenen Vorrichtung **10** aufgetreten sind, alle als Fehler auf die Seite der Straßenrandvorrichtung **20** übertragen. Auch wird, wenn ein Fehler durch die Straßenrandvorrichtung **20** erkannt wird, eine Information bezüglich des Vorliegens des Fehlers ebenso an die fahrzeuggebundene Vorrichtung **10** übertragen. Daher können sowohl die fahrzeuggebundene Vorrichtung **10** als auch die Straßenrandvorrichtung **20** von dem Fehler Kenntnis nehmen, und somit können beide dieser Vorrichtungen **10**, **20** Gegenmaßnahmen gegen diesen Fehler ergreifen.

[0154] Obwohl die vorliegende Erfindung in Verbindung mit einer bevorzugten Ausführungsform hiervon mit Bezug auf die begleitenden Zeichnungen vollständig beschrieben worden ist, ist festzuhalten, daß dem Fachmann vielfältige Änderungen und Modifikationen ersichtlich sein werden.

[0155] Beispielsweise muß nicht erwähnt werden, daß, während die oben beschriebene Ausführungsform den Fall darstellt, in welchem die Straßenrandvorrichtung **20** an der Einfahrt oder Ausfahrt der Mautstraße über eine Datenkommunikation mit der fahrzeuggebundenen Vorrichtung **10** die einheitliche Mautgebühr, die in Abhängigkeit mit dem Fahrzeugtyp variiert, aber bezüglich der zurückgelegten Strecke und der Fahrtzeit einheitlich ist, empfängt, die vorliegende Erfindung auch auf ein Mautstraßeri-Mautabrechnungssystem angewendet werden kann, bei welchem die Mautgebühr in Übereinstimmung mit der zurückgelegten Strecke oder der Fahrtzeit festgelegt wird.

[0156] In diesem Fall kann, um den Einzug der Mautgebühr an der Ausfahrt der Mautstraße in Übereinstimmung mit der zurückgelegten Strecke oder der Fahrtzeit zu ermöglichen, ein Einfahrtgerüst, das wie in dem Fall des ersten Gerüsts **30** konstruiert ist, an der Einfahrt der Mautstraße vorgesehen sein. Ein solches Ein-

fahrtgerüst kann die Übertragung und den Empfang der Signale, die wie in TABELLE 3 aufgebaut sind, zwischen der in dem Fahrzeug, welches es passiert, eingebauten fahrzeuggebundenen Vorrichtung **10** durchführen. Ferner können ein erstes Ausfahrtgerüst und ein zweites Ausfahrtgerüst, die in der gleichen Weise wie der des ersten Gerüsts **30** und des zweiten Gerüsts **40** konstruiert sind, in der Ausfahrt der Mautstraße zur Durchführung der Übertragung und des Empfangs der Signale, deren Formate in TABELLEN 4 und 2 dargestellt sind und welche in Verbindung mit der vorgenannten Ausführungsform erläutert sind, mit der in dem Fahrzeug, das sie passiert, eingebauten fahrzeuggebundenen Vorrichtung **10** vorgesehen sein, um Mautgebühren einzuziehen.

TABELLE 3

KOMM.-SIGNALE EINFAHRTGERÜST	INHALT
EINFAHRTPILOTSIGNAL (STRASSENRANDVORRICHTUNG)	PILOTSIGNAL ORTS-NR.
EINFAHRTPILOTANTWORTSIGNAL (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE ZUFALLSZAHL R1 VERSCHLÜSSELUNGSSCHLÜSSELZAHL Kn
DATENABRUFSIGNAL (FAHRZEUGGEBUNDENE VORR.)	DATENABRUFBEFEHL
EINFAHRTLESEDATEN (STRASSENRANDVORRICHTUNG)	ANTWORTCODE STATUSCODE* ZAHLUNGSMODUS* FAHRZEUGVORRICHTUNGSCODE*
EINFAHRTSCHREIBDATEN (STRASSENRANDVORRICHTUNG)	SCHREIBBEFEHL FAHRZEUGVORRICHTUNGSCODE** ORTS-NR. (TEILWEISE VERSCHL.)** TRANSAKTIONSART DATUM DER EINFAHRT ZEIT DER EINFAHRT
ENDSIGNAL (FZ.-GEB. VORR.)	ANTWORTCODE
ENDBESTAETIGUNGSSIGNAL (STRASSENRANDVORRICHTUNG)	ENDBESTAETIGUNG

BEACHTE:

BEZEICHNET IN DER FAHRZEUGGEBUNDEN VORRICHTUNG VERSCHLUESSELTE DATEN
BEZEICHNET IN DER STRASSENRANDVORRICHTUNG VERSCHLUESSELTE DATEN

[0157] Das heißt, wie in TABELLE 3 dargestellt, können die Einfahrtlesedaten, welche den Antwortcode, den Statuscode, den Gebühreneinzugsmodus, den Fahrzeugvorrichtungscode etc. enthalten, im Voraus in der fahrzeuggebundene Vorrichtung **10** generiert, verschlüsselt und gespeichert werden. Wenn dann das Fahrzeug in den Kommunikationsbereich der in dem Einfahrtgerüst vorgesehenen Kommunikationsvorrichtung eintritt, wird die Seite der fahrzeuggebundenen Vorrichtung **10** durch das Einfahrtpilotsignal, das periodisch gesendet wird, aktiviert und sendet das Einfahrtpilotantwortsignal, das wie in dem Fall des ersten Pilotsignals (siehe TABELLE 1) in der zuvor beschriebenen Ausführungsform aufgebaut ist. Wenn dann die Kommunikationsvorrichtung des Einfahrtgerüsts das Datenlesesignal sendet, sendet die fahrzeuggebundene Vorrichtung **10** die Einfahrtlesedaten. Nach ihrem Empfang der Einfahrtlesedaten ist die Kommunikationsvorrichtung des Einfahrtgerüsts andererseits so aufgebaut, daß es die Einfahrtschreibdaten, die einen Aufbau aufweisen, der durch Entfernen der berechneten Geldsumme aus dem Aufbau der ersten Schreibdaten (siehe TABELLE 1) in der vorgenannten Ausführungsform erhalten werden kann, sendet. Danach führen die Kommunikationsvor-

richtung und die fahrzeuggebundene Vorrichtung eine Übertragung und einen Empfang des Endsignals und des Endbestätigungssignals durch, um den Datenkommunikationsvorgang zu vollenden.

[0158] Nachdem das Fahrzeug das Einfahrtgerüst passiert hat, wie vorstehend erwähnt, werden des weiteren, wie in TABELLE 4 (nachstehend beschrieben) dargestellt, die Einfahrtdaten, welche den Antwortcode, den Fahrzeugvorrichtungscode, die Einfahrtortsnummer, das Einfahrtdatum, die Einfahrtzeit, etc. aufweisen, und die ersten Lesedaten, die aufgebaut sind wie in dem Fall der ersten Lesedaten in der vorgenannten Ausführungsform, in der fahrzeuggebundenen Vorrichtung **10** erzeugt, verschlüsselt und gespeichert als die Daten, die zu übertragen sind, wenn es das erste Ausfahrtgerüst passiert. Wenn das Fahrzeug dann in den Kommunikationsbereich der in dem ersten Ausfahrtgerüst vorgesehenen Kommunikationsvorrichtung eingetreten ist, wird die fahrzeuggebundene Vorrichtung **10** durch das erste Pilotsignal, das von dieser Kommunikationsvorrichtung aus periodisch gesendet wird, aktiviert und sendet das erste Pilotantwortsignal, das aufgebaut ist wie in dem Fall des Einfahrtpilotantwortsignals. Danach empfängt die fahrzeuggebundene Vorrichtung **10** die von der Kommunikationsvorrichtung des ersten Ausfahrtgerüsts gesendete Verifikationsnachricht der Straßenrandvorrichtung, welche den Antwortcode, die Zufallszahl R3 und die Verschlüsselungschlüsselzahl Kc enthält, und sendet die Einfahrtdaten. Ferner empfängt die fahrzeuggebundene Vorrichtung das danach von der Kommunikationsvorrichtung der Straßenrandvorrichtung gesendete Datenauslesesignal und sendet die ersten Lesedaten. Andererseits sendet die Kommunikationsvorrichtung des ersten Ausfahrtgerüsts auf einen Empfang dieser ersten Lesedaten hin die ersten Schreibdaten, die durch Hinzufügen der eine verstrichene Fahrtzeit nach Passieren des Einfahrtgerüsts oder die Ausfahrtnummer enthaltenden Mautabrechnungsdaten zu den ersten Schreibdaten der vorgenannten Ausführungsform vorbereitet worden sind. Danach werden zwischen der fahrzeuggebundenen Vorrichtung und dem Ausfahrtgerüst die Übertragung und der Empfang des Endsignals und des Endbestätigungssignals durchgeführt, um die Datenkommunikation zu vollenden.

[0159] Des weiteren werden, nachdem das Fahrzeug das erste Ausfahrtgerüst passiert, wie in TABELLE 2 gezeigt, Daten, die die gleichen sind wie die zweiten Lesedaten der vorgenannten Ausführungsform, in der fahrzeuggebundenen Vorrichtung **10** erzeugt, verschlüsselt und gespeichert. Wenn das Fahrzeug dann in den Kommunikationsbereich der in dem zweiten Ausfahrtgerüst vorgesehenen Kommunikationsvorrichtung eintritt, führt die fahrzeuggebundene Vorrichtung **10** eine Datenkommunikation, die die gleiche ist wie die, wenn die Seite der fahrzeuggebundenen Vorrichtung **10** das zweite Gerüst **40** der vorgenannten Ausführungsform passiert, mit der fahrzeuggebundene Vorrichtung **10** durch und schreibt hiernach die Kommunikationsergebnisse in die IC-Karte **2**.

[0160] Auf diese Weise ist es unter Verwendung der vorgenannten Konstruktionen möglich, den automatischen Einzug der Mautgebühren von der IC-Karte **2** in beiden Systemen, in welchen die Mautgebühr in Übereinstimmung mit der zurückgelegten Strecke festgelegt wird, und dem System, in welchem die Mautgebühr in Übereinstimmung mit der Fahrtzeit festgelegt wird, durchzuführen. Des weiteren besteht der einzige Unterschied zwischen dem System, in welchem die Mautgebühr in Übereinstimmung mit der Fahrtstrecke festgelegt wird, und dem System, in welchem die Mautgebühr in Übereinstimmung mit der Fahrtzeit festgelegt wird, in Bezug auf das Festlegen der Mautgebührendaten in den in TABELLE 4 dargestellten ersten Schreibdaten auf entweder die gefahrene Zeit oder die Ausfahrtnummer, aus welcher die zurückgelegte Strecke bekannt ist. Der Aufbau der zwischen der fahrzeuggebundenen Vorrichtung und der Straßenrandvorrichtung übertragenen und empfangenen Daten und Muster von Sende- und Empfangsvorgängen sind für beide Systeme vollkommen gleich. Hieraus ergibt sich, daß die fahrzeuggebundene Vorrichtung **10** für beide Systeme verwendet werden kann.

[0161] Solche Änderungen und Modifikationen sollen als innerhalb des Schutzumfangs der vorliegenden Erfindung, wie er durch die beigefügten Ansprüche definiert ist, liegend verstanden werden.

TABELLE 4

KOMM.-SIGNALE 1. AUSFAHRTGERÜST	INHALT
1. PILOTSIGNAL (STRASSENRANDVORRICHTUNG)	PILOTSIGNAL ORTS-NR.
1. PILOTANTWORTSIGNAL (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE ZUFALLSZAHL R1 VERSCHLÜSSELUNGSSCHLÜSSELZAHL Kn
STRASSENRANDVORRICHTUNGS- VERIFIKATIONSNACHRICHT (STRASSENRANDVORRICHTUNG)	ANTWORTCODE ZUFALLSZAHL R3 VERSCHLÜSSELUNGSSCHLÜSSELZAHL KC
EINFAHRTDATEN (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE FAHRZEUGVORRICHTUNGSCODE* EINFAHRTNUMMER* DATUM DES EINFAHRENS ZEIT DES EINFAHRENS
DATENABRUF (FZ.-GEB. V.)	DATENABRUFBEFEHL
ERSTE LESEDATEN (FAHRZEUGGEB. VORRICHTUNG)	ANTWORTCODE STATUSCODE* ZAHLUNGSMODUS* FAHRZEUGVORRICHTUNGSCODE* CSN* GUTHABEN (TEILVERSCHLÜSSELT)* CSN XOR CAN CTC ZEIGER ZU VERWENDENDEN SCHLUESSELS
ERSTE SCHREIBDATEN (STRASSENRANDVORRICHTUNG)	SCHREIBBEFEHL FAHRZEUGVORRICHTUNGSCODE** GESAMTGEBUEHR** ORTS-NR. (TEILVERSCHLUESSELT)** TRANSAKTIONSART DATUM ZEIT ABRECHNUNGSDATEN (ZEIT ODER AUSFAHRTNUMMER)
ENDSIGNAL (FZ.-GEB. VORR.)	ANTWORTCODE
ENDBESTAETIGUNGSSIGNAL (STRASSENRANDVORRICHTUNG)	ENDBESTAETIGUNG

BEACHTE:

BEZEICHNET IN DER FAHRZEUGGEBUNDEN VORRICHTUNG VERSCHLUESSELTE DATEN
BEZEICHNET IN DER STRASSENRANDVORRICHTUNG VERSCHLUESSELTE DATEN

Patentansprüche

1. Eine an einem Fahrzeug angebrachte Kommunikationsvorrichtung (**10**), welche in einem Fahrzeug montiert ist und welche zum Durchführen von Kommunikationsvorgängen mit einer entlang einer Straße montierten Straßenrandvorrichtung (**20**), wenn sich das Fahrzeug innerhalb eines Kommunikationsbereichs der Straßenrandvorrichtung (**20**) befindet, vorgesehen ist, wobei die an einem Fahrzeug angebrachte Kommunikationsvorrichtung (**10**) aufweist:
eine Ansteuerungseinrichtung (**12**) zum Aufnehmen einer IC-Karte (**2**), welche vorbestimmte Kartendaten speichert;
eine kryptographische Einrichtung (**14**) zum Verschlüsseln von zu der Straßenrandvorrichtung (**20**) zu übertragenden Übertragungsdaten, bevor das Fahrzeug in den Kommunikationsbereich der Straßenrandvorrichtung (**20**) eintritt, wobei die Übertragungsdaten die Kartendaten beinhalten; und
eine Kommunikationseinrichtung (**18**) zum Durchführen der Kommunikationsvorgänge mit der Straßenrandvorrichtung (**20**) durch Übertragen der durch die kryptographische Einrichtung (**14**) verschlüsselten Übertragungsdaten an die Straßenrandeinrichtung (**20**) und durch Empfangen von Empfangsdaten von der Straßenrandvorrichtung (**20**), wenn sich das Fahrzeug innerhalb des Kommunikationsbereichs der Straßenrandvor-

richtung (**20**) befindet,
wobei die kryptographische Einrichtung eine Verschlüsselungseinheit (**14**) und eine Entschlüsselungseinheit (**14**) beinhaltet, wobei
die Verschlüsselungseinheit (**14**) die Kartendaten der IC-Karte (**2**) unter Verwendung der Ansteuerungseinrichtung (**12**) liest, die Kartendaten durch Verwenden eines Kommunikationsverschlüsselungsalgorithmus verschlüsselt, um die Übertragungsdaten zu erzeugen, und die Übertragungsdaten speichert, und
die Entschlüsselungseinheit (**14**) die durch die Kommunikationseinrichtung (**18**) empfangenen Empfangsdaten durch Verwenden des Kommunikationsverschlüsselungsalgorithmus entschlüsselt, um entschlüsselte Daten zu erhalten, und ein Ergebnis des Kommunikationsvorgangs der Kommunikationseinrichtung (**18**) auf der Grundlage der entschlüsselten Daten über die Ansteuerungseinrichtung (**12**) in der IC-Karte speichert,
dadurch gekennzeichnet, daß
die Entschlüsselungseinheit (**14**) vor einem Speichern des Ergebnisses in der IC-Karte (**2**) ferner das Ergebnis des Kommunikationsvorgangs durch Verwenden eines Kartendatenverschlüsselungsalgorithmus verschlüsselt, wobei der Kommunikationsverschlüsselungsalgorithmus eine höhere Verarbeitungsgeschwindigkeit als der Kartendatenverschlüsselungsalgorithmus aufweist.

2. Eine an einem Fahrzeug angebrachte Kommunikationsvorrichtung (**10**) gemäß Anspruch 1, wobei die kryptographische Einrichtung (**14**) ferner zum Entschlüsseln der durch die Kommunikationseinrichtung (**18**) von der Straßenrandvorrichtung (**20**) empfangenen Empfangsdaten, nachdem die Kommunikationseinrichtung (**18**) die Kommunikationsvorgänge mit der Straßenrandvorrichtung (**20**) fertigstellt, vorgesehen ist.

3. Eine auf einem Fahrzeug angebrachte Kommunikationsvorrichtung (**10**) gemäß Anspruch 2, wobei die Kommunikationsvorrichtung (**10**) weiter aufweist:
eine Verifikationseinrichtung (**16**) zum Ansteuern der Verschlüsselungseinheit (**14**) der kryptographischen Einrichtung (**14**) und der IC-Karte (**2**), um einen gegenseitigen Verifikationsvorgang unter Verwendung vorbestimmter Verifikationsdaten durchzuführen, wenn die IC-Karte (**2**) innerhalb der Ansteuerungseinrichtung (**12**) eingesetzt ist und bevor die Verschlüsselungseinheit (**14**) die Übertragungsdaten erzeugt, wobei die Verifikationseinrichtung (**16**) ferner zum Ansteuern der Verschlüsselungseinheit (**14**) der kryptographischen Einrichtung (**14**) vorgesehen ist, um ein Ergebnis des gegenseitigen Verifikationsvorgangs in den Übertragungsdaten einzuschließen.

4. Eine an einem Fahrzeug angebrachte Kommunikationsvorrichtung (**10**) gemäß einem der Ansprüche 1 bis 3, wobei die Kommunikationsvorrichtugn (**10**) weiter aufweist:
eine Fehlerbestimmungseinrichtung (**16**) zum Bestimmen eines Fehlers in Vorgängen der kryptographischen Einrichtung (**14**), der Kommunikationseinrichtung (**18**), der Ansteuerungseinrichtung (**12**), der IC-Karte (**2**) und der Verifikationseinrichtung (**16**) sowie zum Hinzufügen von Fehlerdaten, welche den bestimmten Fehler anzeigen, zu den Übertragungsdaten.

Es folgen 11 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

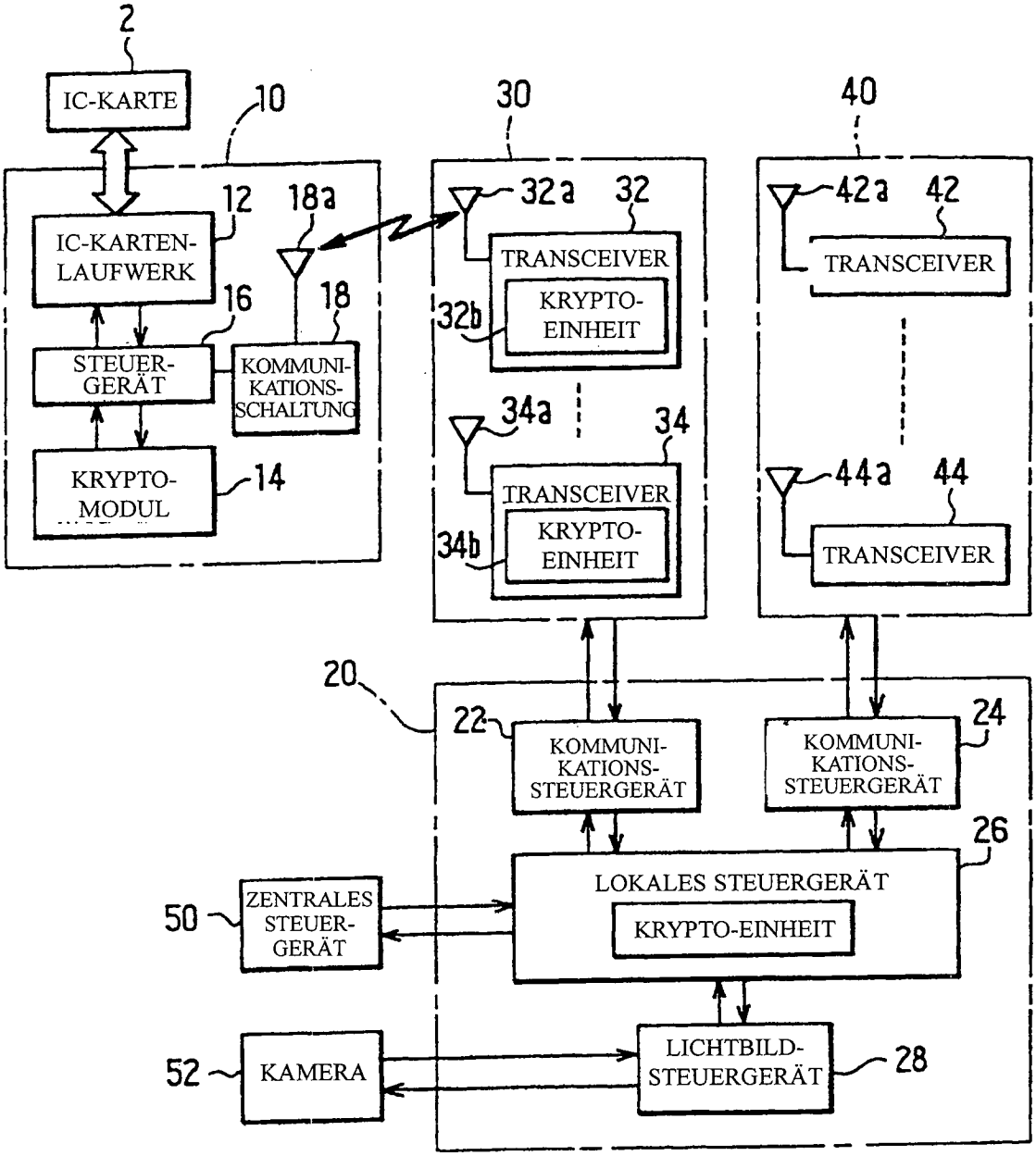


FIG. 2

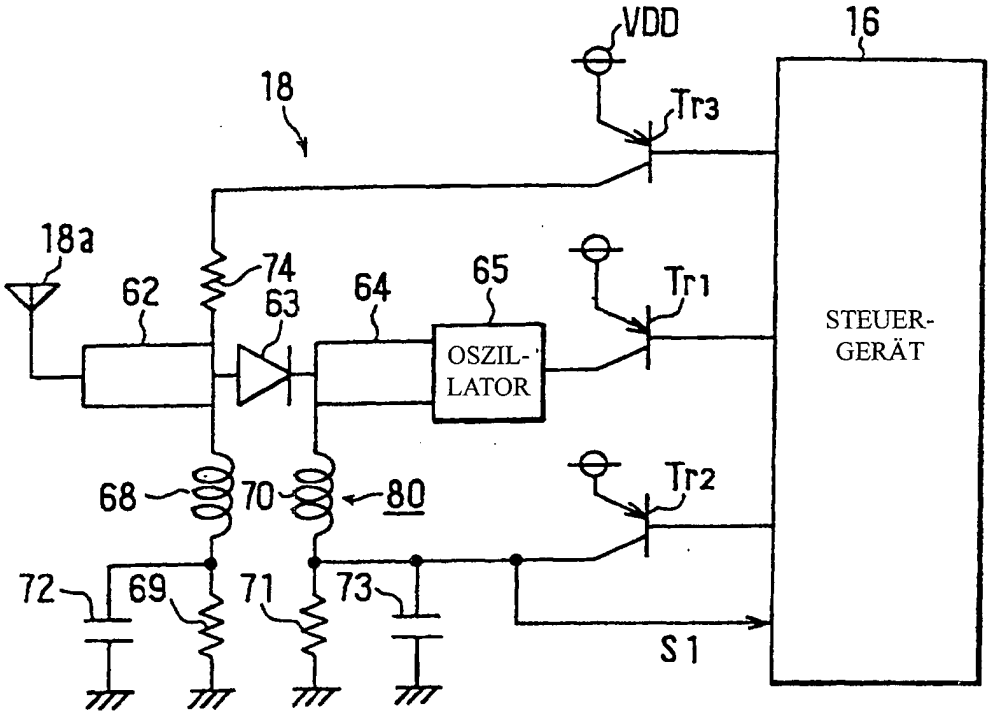

VDD
16
18
Tr3
18a
74
62
63
64
65
Tr1
STEUER-
GERÄT
OSZIL-
LATOR
68
70
80
Tr2
72
69
71
73
S1

FIG. 3

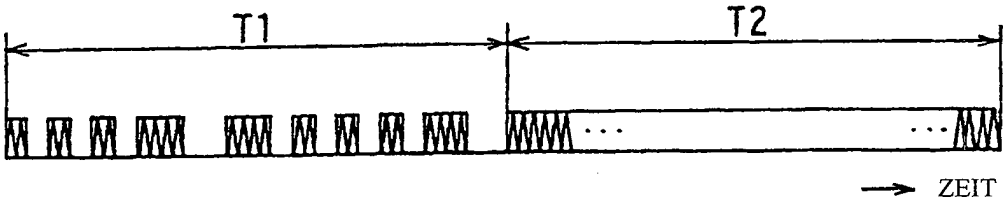

T1
T2
ZEIT

FIG. 4

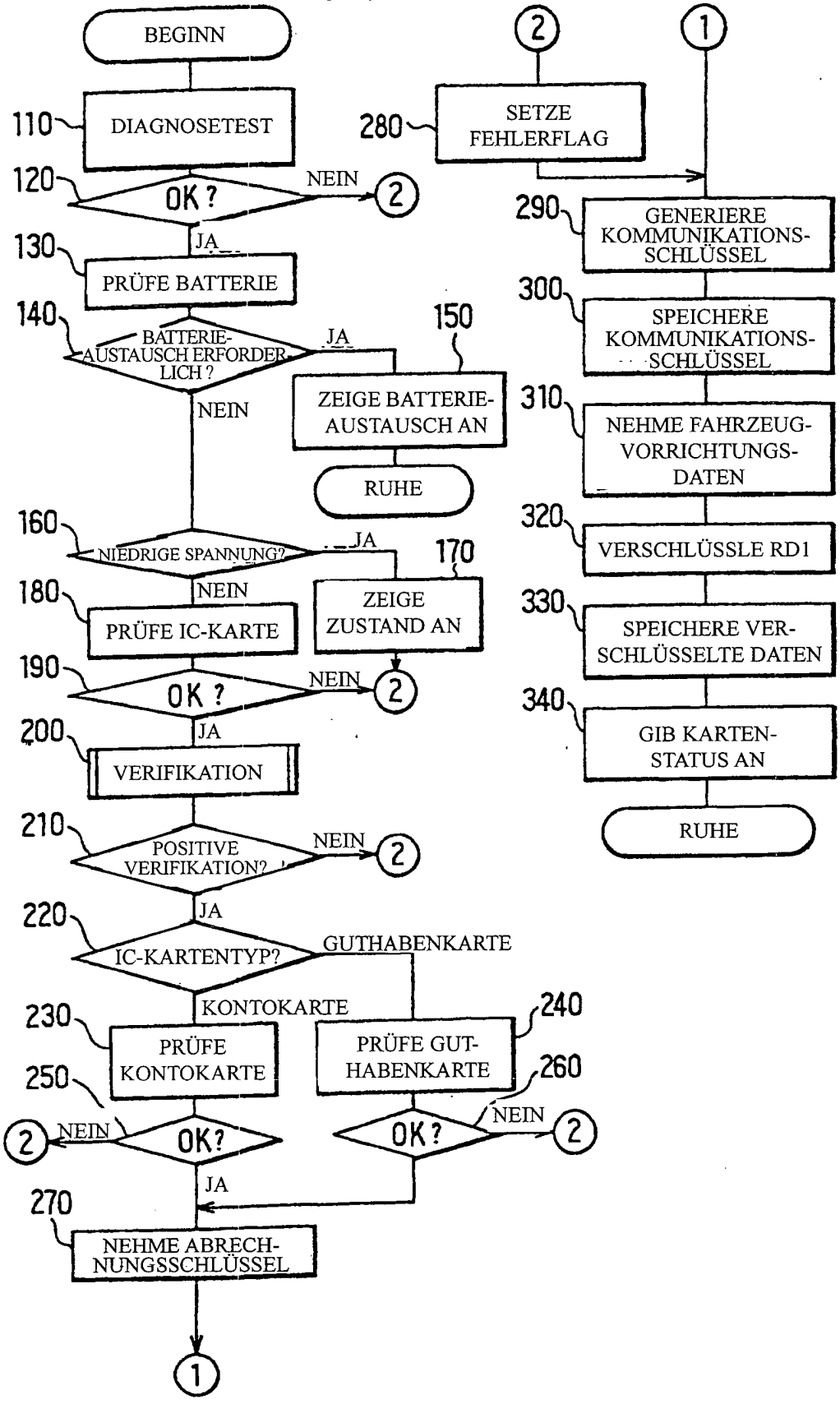

BEGINN
110
DIAGNOSETEST
120
OK ?
NEIN
2
JA
130
PRÜFE BATTERIE
140
BATTERIE-AUSTAUSCH ERFORDERLICH ?
JA
150
ZEIGE BATTERIE-AUSTAUSCH AN
RUHE
NEIN
160
NIEDRIGE SPANNUNG?
JA
170
ZEIGE ZUSTAND AN
NEIN
180
PRÜFE IC-KARTE
190
OK ?
NEIN
2
JA
200
VERIFIKATION
210
POSITIVE VERIFIKATION?
NEIN
2
JA
220
IC-KARTENTYP?
GUTHABENKARTE
KONTOKARTE
230
PRÜFE KONTOKARTE
240
PRÜFE GUT-HABENKARTE
250
260
2
NEIN
OK?
OK?
NEIN
2
JA
270
NEHME ABRECH-NUNGSSCHLÜSSEL
1
2
SETZE FEHLERFLAG
280
1
290
GENERIERE KOMMUNIKATIONS-SCHLÜSSEL
300
SPEICHERE KOMMUNIKATIONS-SCHLÜSSEL
310
NEHME FAHRZEUG-VORRICHTUNGS-DATEN
320
VERSCHLÜSSLE RD1
330
SPEICHERE VER-SCHLÜSSELTE DATEN
340
GIB KARTEN-STATUS AN
RUHE

FIG. 5

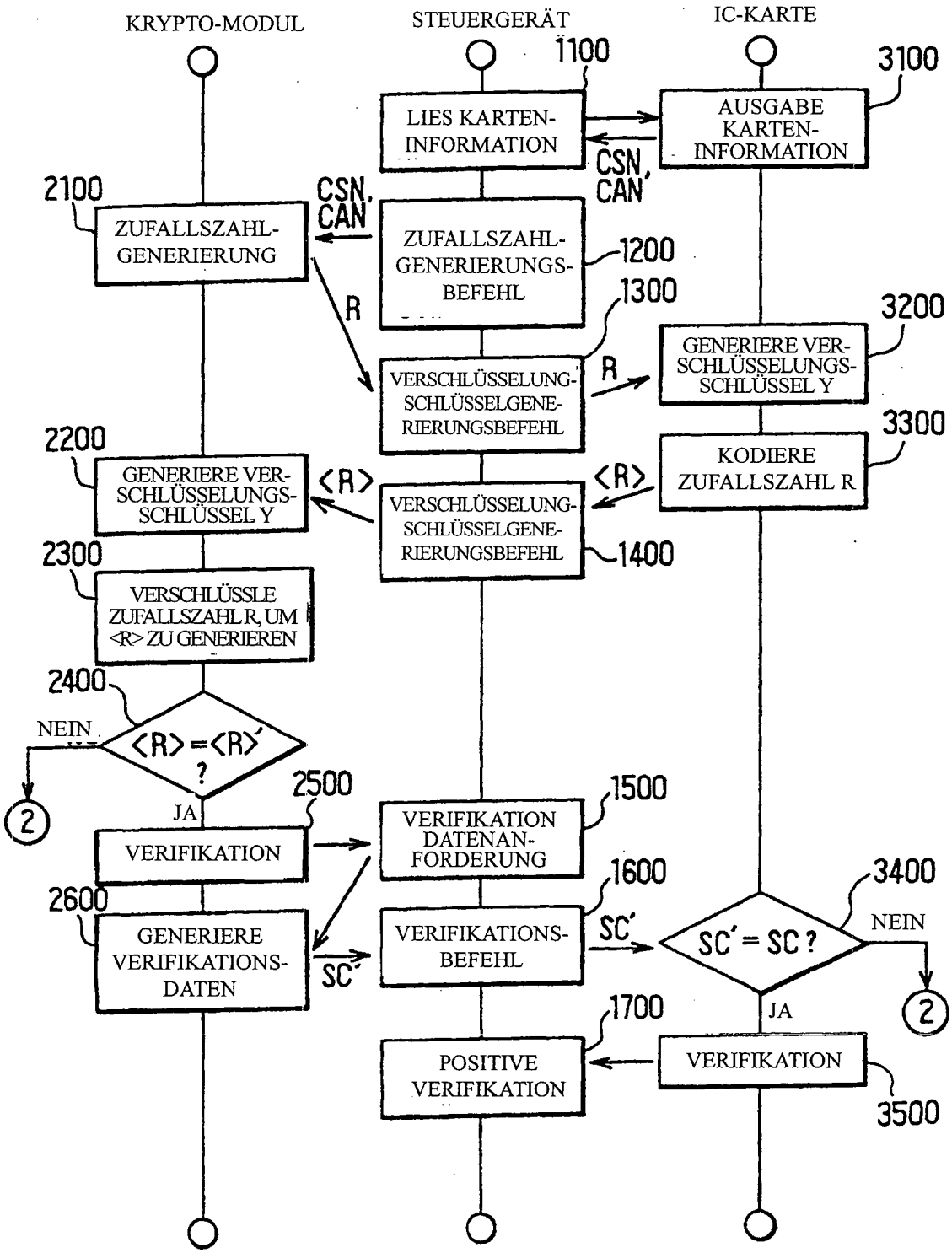

KRYPTO-MODUL
STEUERGERÄT
IC-KARTE
1100
3100
LIES KARTEN-INFORMATION
AUSGABE KARTEN-INFORMATION
CSN, CAN
CSN, CAN
2100
ZUFALLSZAHL-GENERIERUNG
ZUFALLSZAHL-GENERIERUNGS-BEFEHL
1200
R
1300
3200
VERSCHLÜSSELUNG-SCHLÜSSELGENE-RIERUNGSBEFEHL
R
GENERIERE VER-SCHLÜSSELUNGS-SCHLÜSSEL Y
2200
3300
GENERIERE VER-SCHLÜSSELUNGS-SCHLÜSSEL Y
<R>
<R>
KODIERE ZUFALLSZAHL R
VERSCHLÜSSELUNG-SCHLÜSSELGENE-RIERUNGSBEFEHL
1400
2300
VERSCHLÜSSLE ZUFALLSZAHL R, UM <R> ZU GENERIEREN
2400
NEIN
<R> = <R>' ?
2
JA
2500
1500
VERIFIKATION
VERIFIKATION DATENAN-FORDERUNG
1600
3400
2600
GENERIERE VERIFIKATIONS-DATEN
SC'
VERIFIKATIONS-BEFEHL
SC'
SC' = SC ?
NEIN
2
JA
1700
POSITIVE VERIFIKATION
VERIFIKATION
3500

FIG. 6

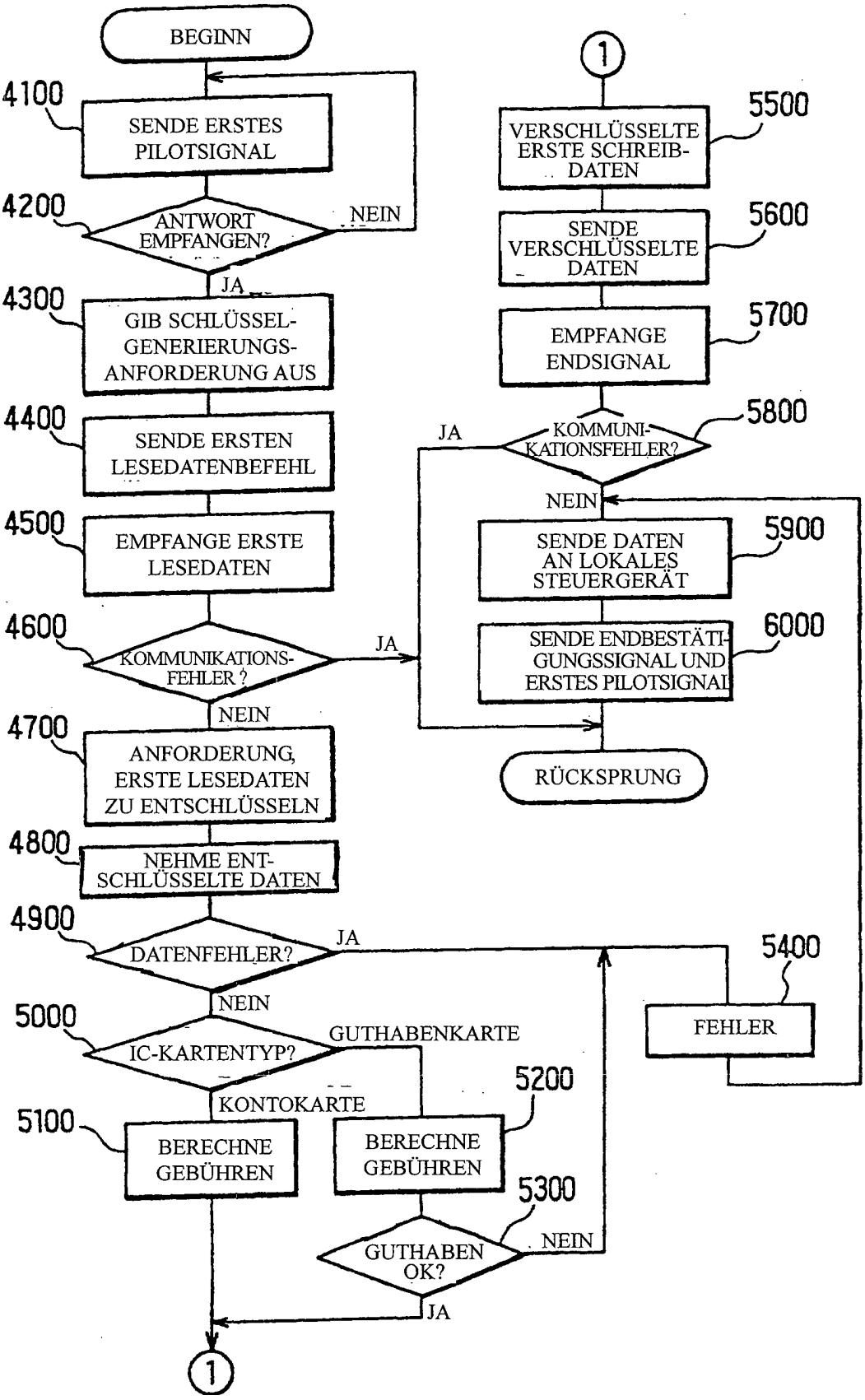

BEGINN
4100
SENDE ERSTES PILOTSIGNAL
4200
ANTWORT EMPFANGEN?
NEIN
JA
4300
GIB SCHLÜSSEL-GENERIERUNGS-ANFORDERUNG AUS
4400
SENDE ERSTEN LESEDATENBEFEHL
4500
EMPFANGE ERSTE LESEDATEN
4600
KOMMUNIKATIONS-FEHLER?
JA
NEIN
4700
ANFORDERUNG, ERSTE LESEDATEN ZU ENTSCHLÜSSELN
4800
NEHME ENT-SCHLÜSSELTE DATEN
4900
DATENFEHLER?
JA
NEIN
5000
IC-KARTENTYP?
GUTHABENKARTE
KONTOKARTE
5100
BERECHNE GEBÜHREN
5200
BERECHNE GEBÜHREN
5300
GUTHABEN OK?
NEIN
JA
1
1
5500
VERSCHLÜSSELTE ERSTE SCHREIB-DATEN
5600
SENDE VERSCHLÜSSELTE DATEN
5700
EMPFANGE ENDSIGNAL
5800
KOMMUNI-KATIONSFEHLER?
JA
NEIN
5900
SENDE DATEN AN LOKALES STEUERGERÄT
6000
SENDE ENDBESTÄTI-GUNGSSIGNAL UND ERSTES PILOTSIGNAL
RÜCKSPRUNG
5400
FEHLER

FIG. 7

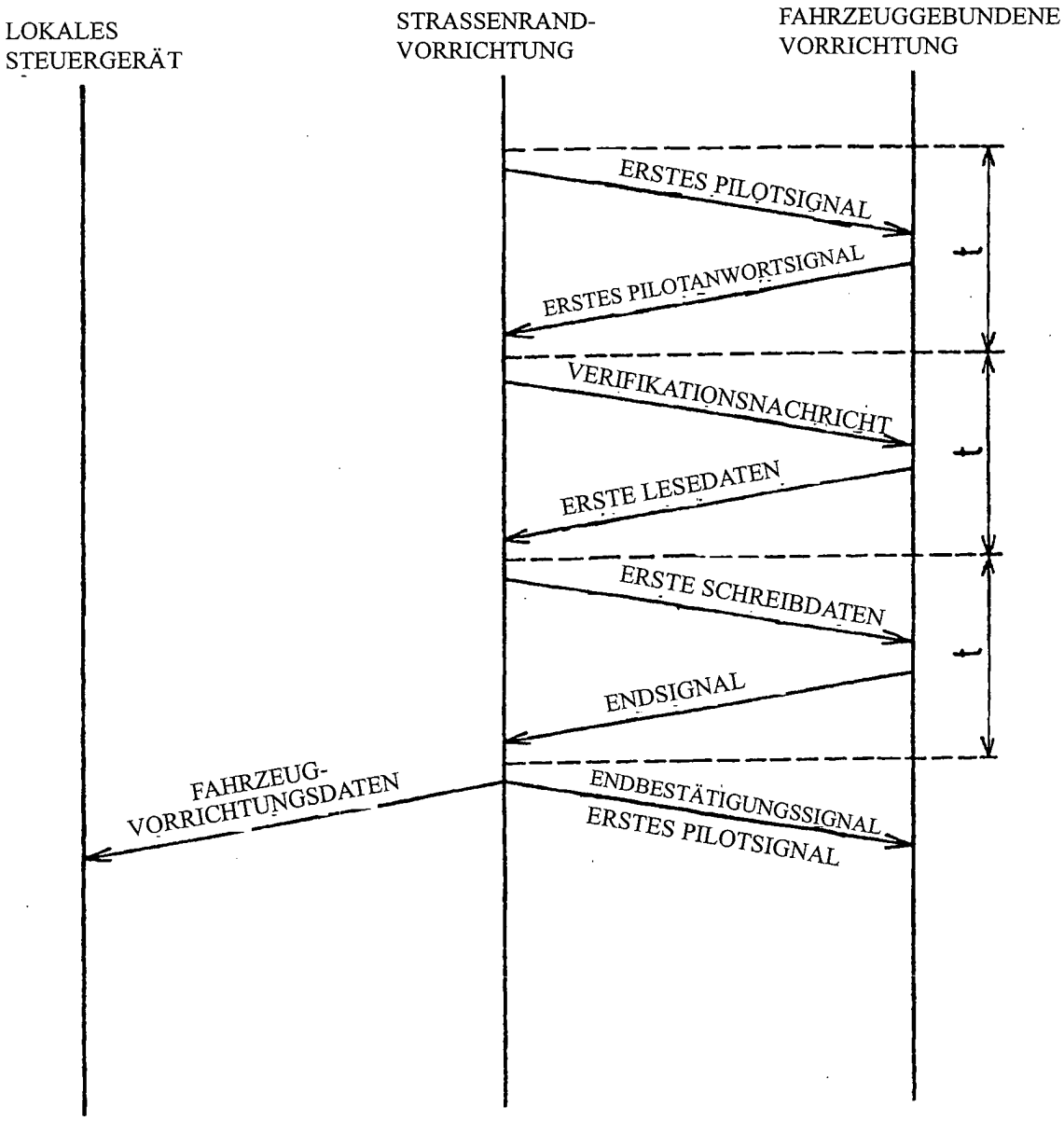

LOKALES STEUERGERÄT
STRASSENRAND-VORRICHTUNG
FAHRZEUGGEBUNDENE VORRICHTUNG
ERSTES PILOTSIGNAL
ERSTES PILOTANWORTSIGNAL
VERIFIKATIONSNACHRICHT
ERSTE LESEDATEN
ERSTE SCHREIBDATEN
ENDSIGNAL
FAHRZEUG-VORRICHTUNGSDATEN
ENDBESTÄTIGUNGSSIGNAL
ERSTES PILOTSIGNAL

FIG. 8

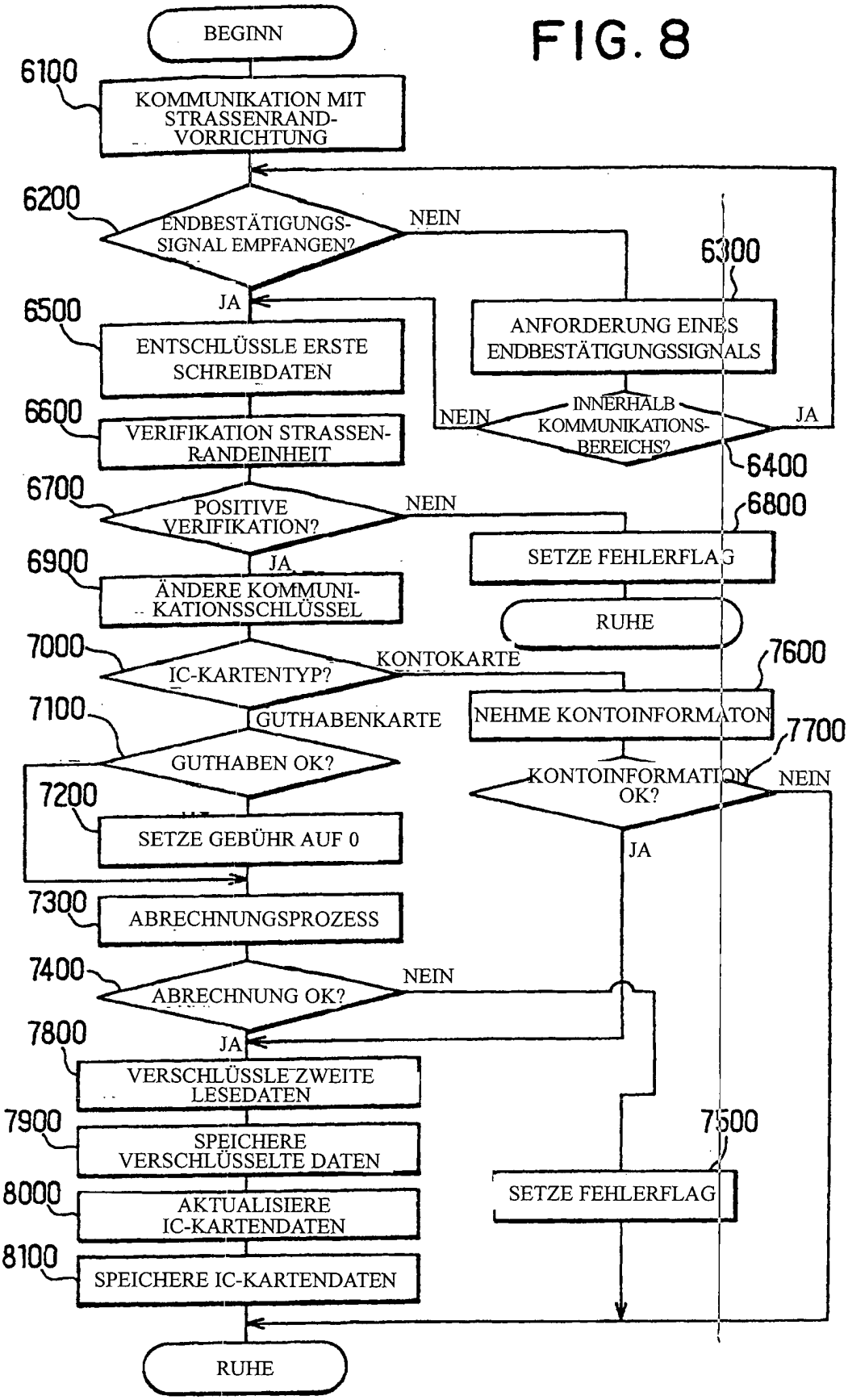

BEGINN
6100
KOMMUNIKATION MIT STRASSENRAND-VORRICHTUNG
6200
ENDBESTÄTIGUNGS-SIGNAL EMPFANGEN?
NEIN
JA
6300
ANFORDERUNG EINES ENDBESTÄTIGUNGSSIGNALS
INNERHALB KOMMUNIKATIONS-BEREICHS?
NEIN
JA
6400
6500
ENTSCHLÜSSLE ERSTE SCHREIBDATEN
6600
VERIFIKATION STRASSEN-RANDEINHEIT
6700
POSITIVE VERIFIKATION?
NEIN
6800
SETZE FEHLERFLAG
RUHE
JA
6900
ÄNDERE KOMMUNI-KATIONSSCHLÜSSEL
7000
IC-KARTENTYP?
KONTOKARTE
7600
NEHME KONTOINFORMATON
7700
KONTOINFORMATION OK?
NEIN
JA
GUTHABENKARTE
7100
GUTHABEN OK?
7200
SETZE GEBÜHR AUF 0
7300
ABRECHNUNGSPROZESS
7400
ABRECHNUNG OK?
NEIN
JA
7800
VERSCHLÜSSLE ZWEITE LESEDATEN
7900
SPEICHERE VERSCHLÜSSELTE DATEN
8000
AKTUALISIERE IC-KARTENDATEN
8100
SPEICHERE IC-KARTENDATEN
7500
SETZE FEHLERFLAG
RUHE

FIG. 9

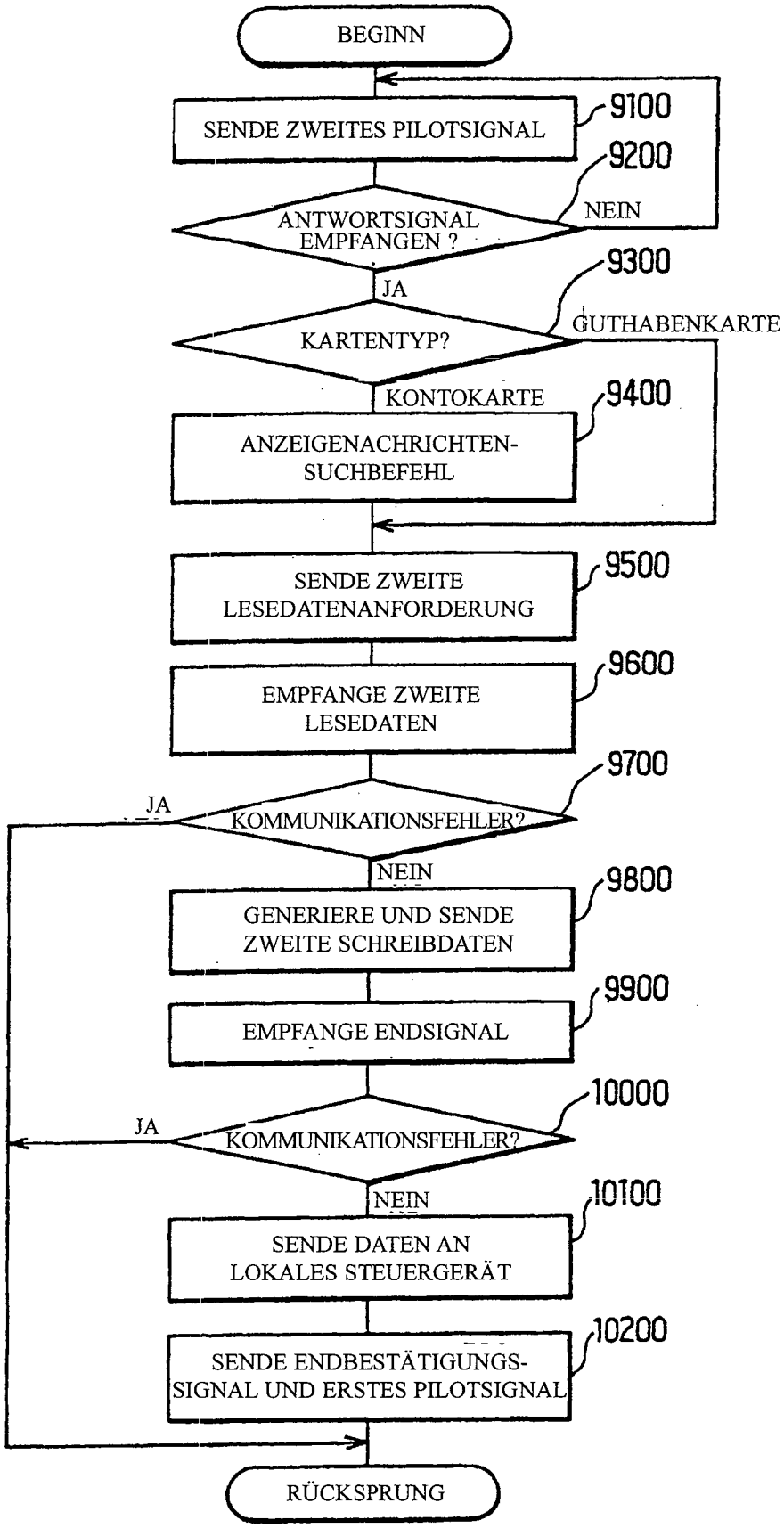

BEGINN
SENDE ZWEITES PILOTSIGNAL
9100
9200
ANTWORTSIGNAL EMPFANGEN ?
NEIN
JA
9300
KARTENTYP?
GUTHABENKARTE
KONTOKARTE
9400
ANZEIGENACHRICHTEN-SUCHBEFEHL
SENDE ZWEITE LESEDATENANFORDERUNG
9500
EMPFANGE ZWEITE LESEDATEN
9600
9700
JA
KOMMUNIKATIONSFEHLER?
NEIN
GENERIERE UND SENDE ZWEITE SCHREIBDATEN
9800
EMPFANGE ENDSIGNAL
9900
10000
JA
KOMMUNIKATIONSFEHLER?
NEIN
10100
SENDE DATEN AN LOKALES STEUERGERÄT
10200
SENDE ENDBESTÄTIGUNGS-SIGNAL UND ERSTES PILOTSIGNAL
RÜCKSPRUNG

FIG. 10

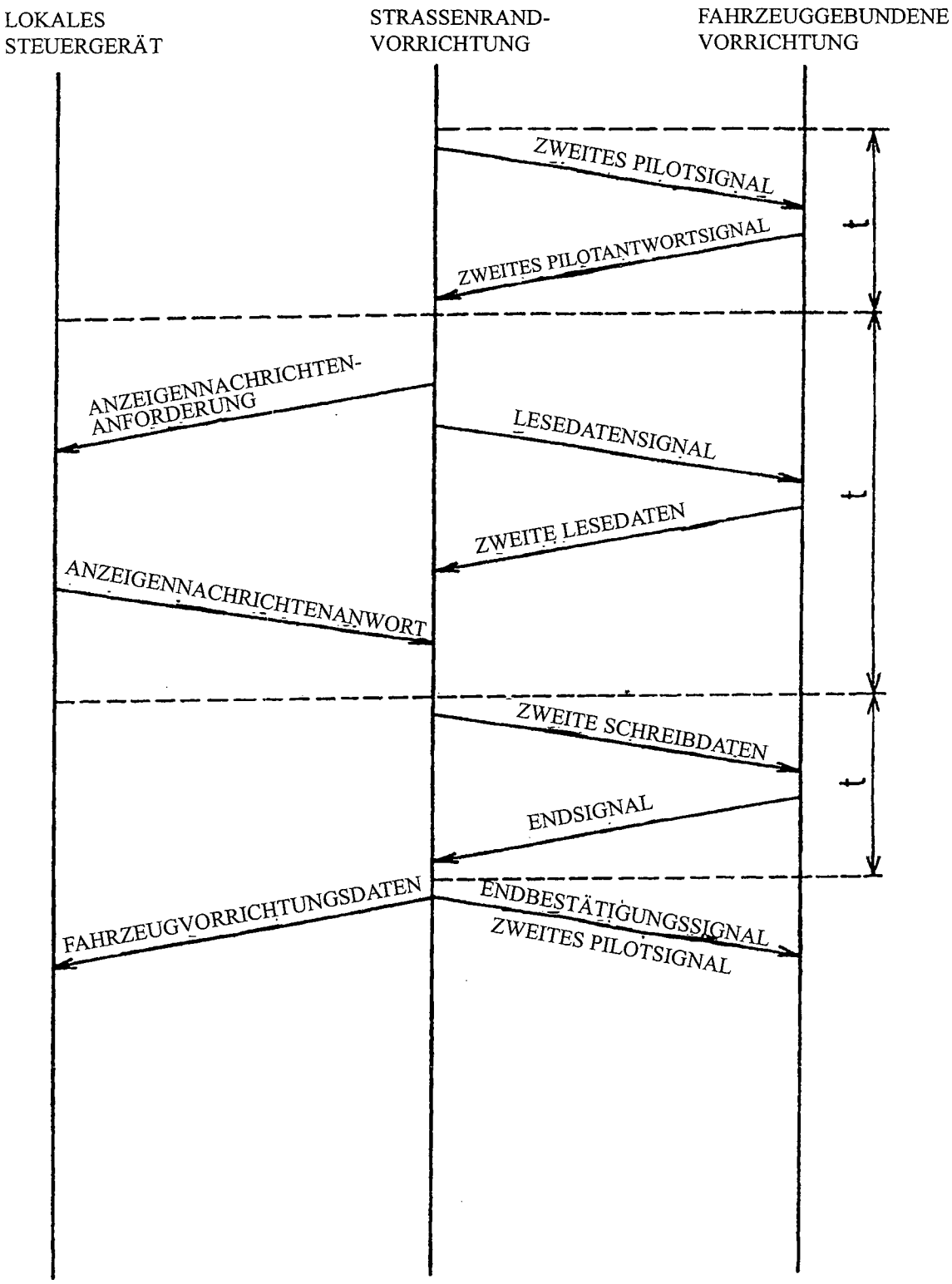

LOKALES STEUERGERÄT
STRASSENRAND-VORRICHTUNG
FAHRZEUGGEBUNDENE VORRICHTUNG
ZWEITES PILOTSIGNAL
ZWEITES PILOTANTWORTSIGNAL
t
ANZEIGENNACHRICHTEN-ANFORDERUNG
LESEDATENSIGNAL
ZWEITE LESEDATEN
t
ANZEIGENNACHRICHTENANWORT
ZWEITE SCHREIBDATEN
ENDSIGNAL
t
FAHRZEUGVORRICHTUNGSDATEN
ENDBESTÄTIGUNGSSIGNAL
ZWEITES PILOTSIGNAL

FIG. 11

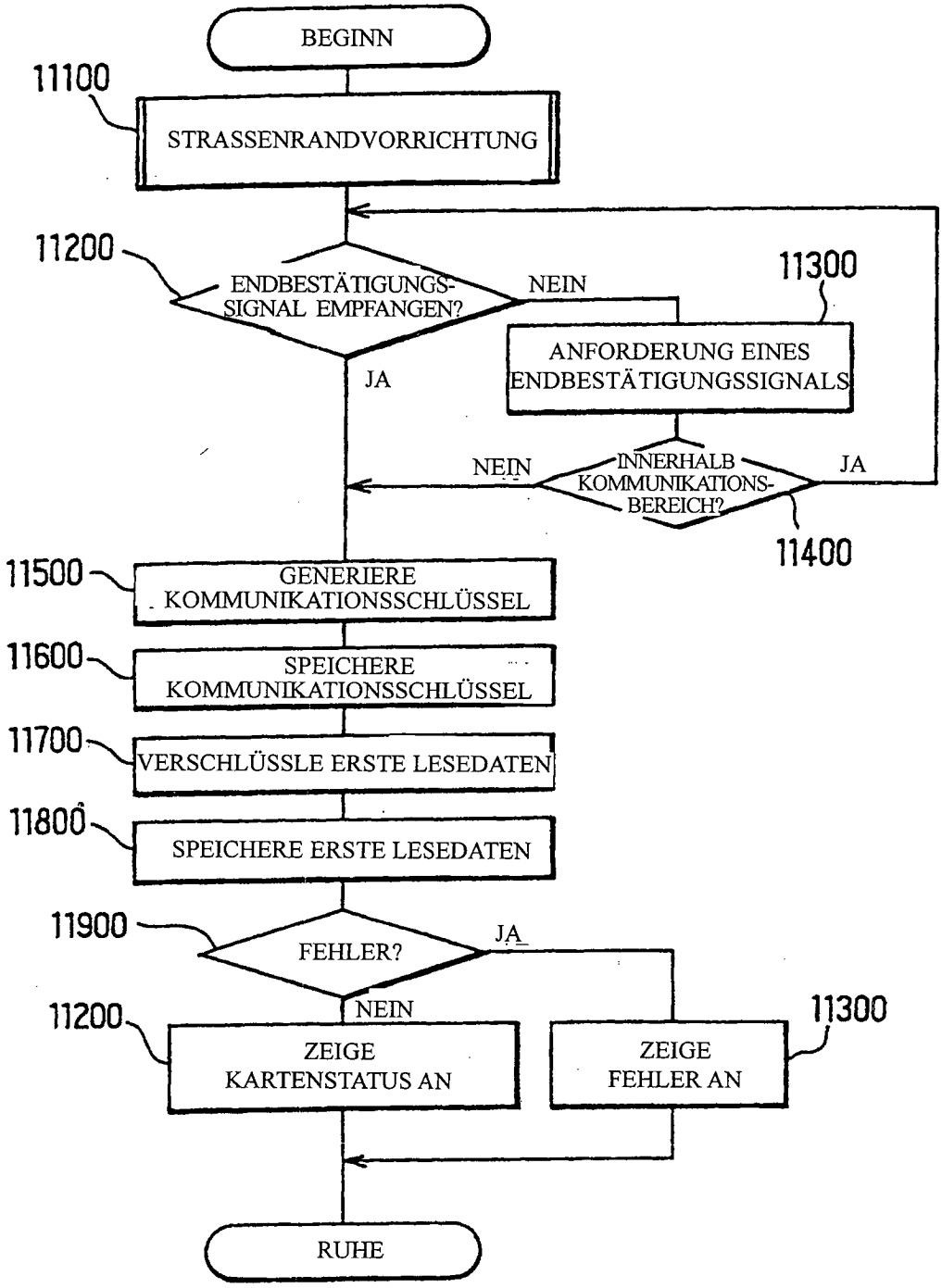
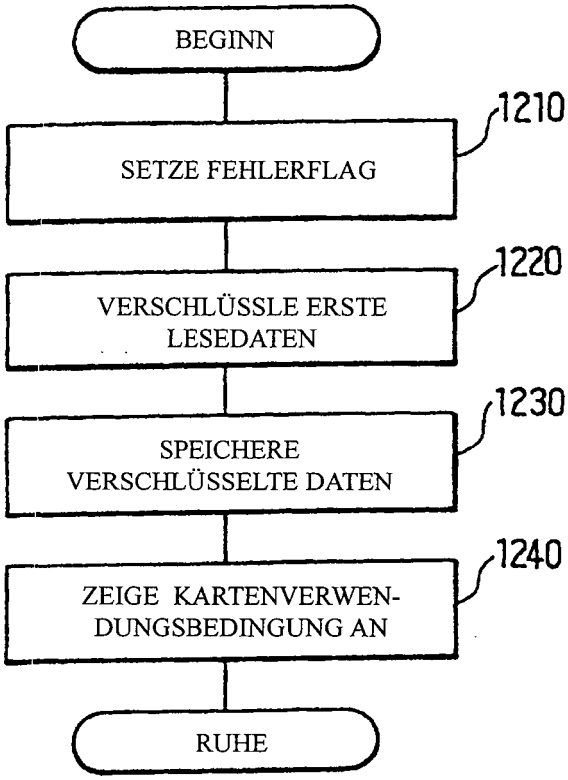

BEGINN
11100
STRASSENRANDVORRICHTUNG
11200
ENDBESTÄTIGUNGS-SIGNAL EMPFANGEN?
NEIN
11300
ANFORDERUNG EINES ENDBESTÄTIGUNGSSIGNALS
JA
NEIN
INNERHALB KOMMUNIKATIONS-BEREICH?
JA
11400
11500
GENERIERE KOMMUNIKATIONSSCHLÜSSEL
11600
SPEICHERE KOMMUNIKATIONSSCHLÜSSEL
11700
VERSCHLÜSSLE ERSTE LESEDATEN
11800
SPEICHERE ERSTE LESEDATEN
11900
FEHLER?
JA
NEIN
11200
ZEIGE KARTENSTATUS AN
ZEIGE FEHLER AN
11300
RUHE

FIG. 12


BEGINN
1210
SETZE FEHLERFLAG
1220
VERSCHLÜSSLE ERSTE LESEDATEN
1230
SPEICHERE VERSCHLÜSSELTE DATEN
1240
ZEIGE KARTENVERWENDUNGSBEDINGUNG AN
RUHE