



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
20.10.2010 Patentblatt 2010/42

(51) Int Cl.:
G07C 9/00 (2006.01)

(21) Anmeldenummer: **10158623.8**

(22) Anmeldetag: **31.03.2010**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Benannte Erstreckungsstaaten:
AL BA ME RS

(71) Anmelder: **Huf Hülsbeck & Fürst GmbH & Co. KG**
42551 Velbert (DE)

(72) Erfinder: **Ziller, Boris**
40885 Ratingen (DE)

(74) Vertreter: **Zenz**
Patent- und Rechtsanwälte
Rüttenscheider Strasse 2
45128 Essen (DE)

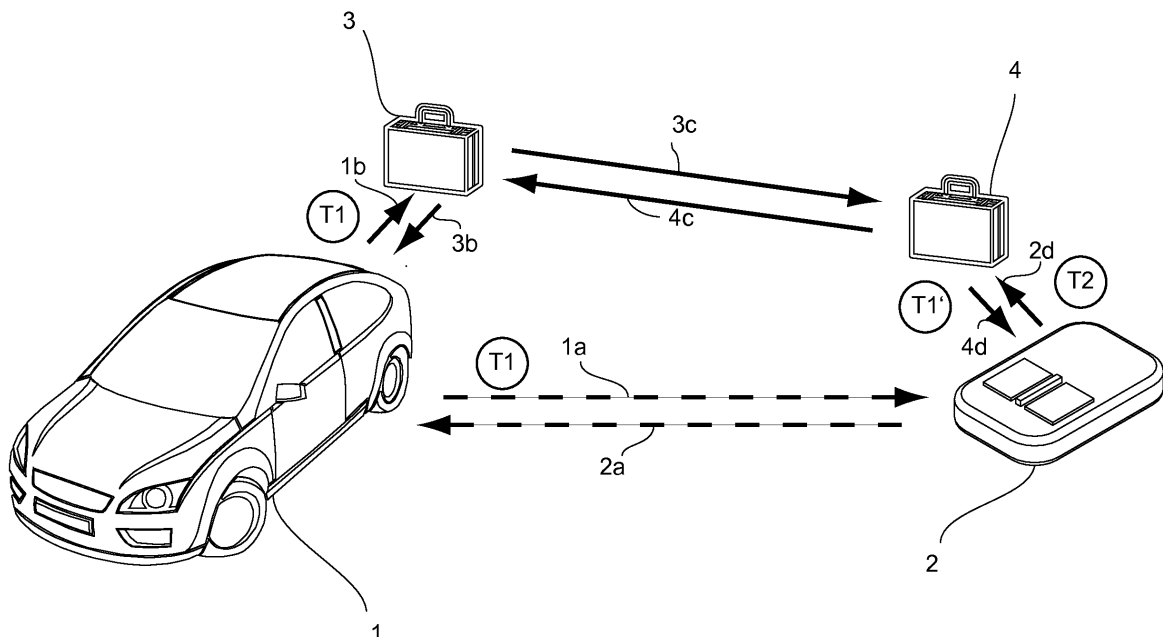
(30) Priorität: **16.04.2009 DE 102009002448**

(54) **Verfahren zur Sicherung einer Keyless-Entry-Kommunikation für Kraftfahrzeuge**

(57) Ein Verfahren zur Kontrolle der Zugangsberechtigung für ein Kraftfahrzeug. Mit einer fahrzeugseitigen Wechseltung wird ein Funksignal ausgesendet und ein vom Benutzer mitgeführter ID-Geber empfängt das Funksignal und überprüft es mit einer Auswerteschaltung. Bei erfolgreicher Überprüfung wird von dem ID-Geber ein hochfrequentes Freigabesignal ausgesendet und fahrzeugseitig empfangen.

Die Wechseltung steuert einen Schwingkreis derart an, dass die Einschwingdauer des Schwingkreises in Abhängigkeit von einem zufällig generierten Parameter variiert wird, wobei die Stromversorgung des Schwingkreises in Abhängigkeit von dem Parameter kontrolliert wird. Eine erwartete Systemlaufzeit wird mit realen Systemlaufzeit bestimmt und zur Verhinderung von Funkstreckenverlängerungen in die Auswertung einbezogen.

Fig. 1



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Verbesserung der Sicherheit einer Zugriffskontrolle für Keyless-Entry-Systeme bei Kraftfahrzeugen.

[0002] Derartige Keyless-Entry-Einrichtungen bieten Benutzern von Kraftfahrzeugen die Möglichkeit, ohne eine mechanische Schließbetätigung eines Türschlosses, den Zugriff auf ein Kraftfahrzeug zu erhalten. Der Benutzer führt dazu üblicherweise einen sogenannten ID-Geber mit sich, welcher in eine Funkkommunikation mit den Systemen des Kraftfahrzeugs tritt. Auslösendes Ereignis für die Aufnahme einer solchen Funkkommunikation ist eine Annäherung des Benutzers an das Kraftfahrzeug, z.B. die Annäherung der Hand an den Türgriffbereich. Bei Erfassung eines solchen Ereignisses sendet eine fahrzeugseitige Weckeinrichtung bzw. Weckschaltung ein Weck-Funksignal aus, welches ein vom Benutzer mitgeführter ID-Geber empfängt. Das Weck-Funksignal wird seitens des ID-Gebers durch eine Schaltung ausgewertet, insbesondere wird überprüft, ob das Weck-Funksignal von einem Kraftfahrzeug stammt, welchem der ID-Geber zugeordnet ist. Dies kann anhand einer im Weck-Funksignal codierten Nachricht überprüft werden. Im Falle einer erfolgreichen Überprüfung im ID-Geber, sendet dieser ein hochfrequentes Freigabe-Funksignal aus, welches fahrzeugseitig empfangen und decodiert wird. In Abhängigkeit von dem Signal und ggf. nach weiteren Überprüfungen des Signals erfolgt eine fahrzeugseitige Freigabe der Schließeinrichtung, so dass ein Zugriff des Benutzers erfolgen kann. Eine derartige Kommunikation läuft äußerst rasch ab, so dass der zugreifende Benutzer üblicherweise davon keine Kenntnis nimmt, sofern die Zugriffsberechtigung erfolgreich überprüft wird. Das Türschloss ist üblicherweise bereits freigegeben, sobald der Benutzer tatsächlich darauf zugreift.

[0003] Es gibt jedoch Angriffe auf derartige Kommunikationen, die als Relay-Station-Attacken bezeichnet werden. Üblicherweise soll nur Zugriff auf ein Fahrzeug gewährt werden, wenn der Träger des ID-Gebers sich in der Nähe des Fahrzeugs aufhält. Während die Funkstrecke zwischen ID-Geber und Kraftfahrzeug dazu üblicherweise auf einige Meter beschränkt ist, wird bei diesen Attacken die Funkstrecke künstlich und gezielt verlängert. Bei einer derartigen Funkstreckenverlängerung wird das Wecksignal vom Fahrzeug von einer ersten Verlängerungsstation empfangen und an eine zweite Station, die sich in der Nähe des ID-Gebers befindet, gesendet. Auf diese Weise kann ein Unberechtigter Zugriff auf das Fahrzeug erlangen, wenn er sich in Fahrzeugnähe aufhält und die zweite Funkstation in der Nähe des ID-Gebers aufhält.

[0004] Aus der EP 06117688 ist ein Verfahren bekannt, welches die Sicherheit derartiger Kommunikationsprotokolle verbessern soll.

[0005] Es besteht jedoch weiter der Bedarf, die Keyless-Entry-Systeme in ihre Sicherheit gegen derartige

Verlängerungen der Funkstrecken zu schützen.

[0006] Aufgabe der Erfindung ist es daher, ein verbessertes System zur Sicherung von Keyless-Entry-Systemen bereitzustellen.

5 **[0007]** Die Aufgabe wird erfindungsgemäß gelöst durch ein Verfahren zur Kontrolle der Zugangsberechtigung für ein Kraftfahrzeug mit den Merkmalen des Patentanspruchs 1.

10 **[0008]** Gemäß der Erfindung wird durch die Weckschaltung zur Erzeugung des Weck-Funksignals ein Schwingkreis unter Kontrolle der Stromversorgung des Schwingkreises derart angesteuert, dass die Einschwingdauer des Schwingkreises variierbar ist. Die Einschwingdauer wird dabei in Abhängigkeit von einem zufällig generierten Parameter variiert, was durch Kontrolle der Stromversorgung geschieht. Dazu wird beispielsweise der Duty-Cycle bzw. Tastgrad variiert.

15 **[0009]** Die Einschwingdauer des Schwingkreises kann zwischen einem minimalen, in der Praxis realisierbaren Wert und einem maximalen Wert variiert werden. Durch die Verlängerung der Einschwingdauer wird bewusst und gezielt eine Zeitkomponente in die Abfolge der Funkkommunikationen eingebracht, welche der Kontrolle der fahrzeugseitigen Schaltungen unterliegt.

20 **[0010]** In einer nicht-korruptierten Funkverbindung (ohne böswillige Funkstreckenverlängerung) setzt sich die Systemlaufzeit, also die Zeit vom Start der Aussendung des Wecksignals bis zum Empfang des Freigabe-signals, aus mehreren Komponenten zusammen. Während einer Zeit T1 schwingt der Schwingkreis unter Ansteuerung der Weckschaltung ein, bis die Ansprechschwelle des empfangenden ID-Gebers erreicht wurde, und sendet sein Wecksignal an den ID-Geber aus. Der ID-Geber empfängt dieses Signal, überprüft den darin codierten Informationsgehalt (z.B. ein sogenanntes Wake-up-pattern) und sendet ein hochfrequentes Antwortsignal an das Fahrzeug zurück, wobei für den Empfang und die Überprüfung eine Zeitkomponente T2 zu berücksichtigen ist. Fahrzeugseitig wird das hochfrequente Freigabesignal empfangen, überprüft und ein Freigabesignal an die mechanische Sperreinrichtung des Türschlosses gesendet, wobei eine Zeitkomponente T3 hinzukommt.

30 **[0011]** Eine derartige erwartete Systemlaufzeit wird erfindungsgemäß in Abhängigkeit von dem generierten Zufallsparameter zunächst berechnet. Aus dieser berechneten Systemlaufzeit ergibt sich ein Zeitfenster, innerhalb dessen bei einer unkorruptierten Verbindung ohne verlängerte Funkstrecke eine Rückmeldung zur Freigabe des Türschlosses erwartet wird.

35 **[0012]** Die tatsächlich benötigte Zeitdauer für die Aussendung des Funksignals und bis zum Erhalt des Freigabesignals, also die reale Systemlaufzeit, wird gemessen und gegenüber der erwarteten Systemlaufzeit abgeglichen. Falls die Zeitdauer um mehr als einen vorgegebenen Wert von der erwarteten Systemlaufzeit abweicht, wird eine Freigabe der Schließeinrichtung unterbunden.

40 **[0013]** Der Erfindung liegt die Erkenntnis zugrunde,

dass im Falle einer Funkstreckenverlängerung das ausgesendete Wecksignal in Abhängigkeit von dem zufällig erzeugten Parameter erzeugt wurde und daher eine gezielt beeinflusste Zeitkomponente enthält. Bei Verlängerung der Funkstrecke taucht diese Verlängerungskomponente der Zeit jedoch ein zweites Mal auf, nämlich bei der Verlängerung der Funkstrecke zum ID-Geber. Dort wird das Wecksignal mit einem weiteren Schwingkreis neu erzeugt und an den ID-Geber weitergeleitet. Die Zeitkomponente ist dann zweimal in der Systemlaufzeit enthalten und die gesamte Systemlaufzeit stimmt dann nicht mehr mit der erwarteten Systemlaufzeit überein. Das Antwortsignal wird also nicht innerhalb des Zeitfensters erhalten, welches für den Erhalt berechnet wurde. Kern der Erfindung ist daher die bewusste und künstliche Variation der Einschwingdauer der Weckschaltung und der Abgleich der erwarteten Systemlaufzeit mit der tatsächlichen Systemlaufzeit.

[0014] Grundsätzlich ist dieses Konzept für verschiedene Frequenzen des Wecksignals geeignet, insbesondere für Systeme mit einer Sendefrequenz von 20 kHz, aber auch für Systeme mit einer Sendefrequenz von 125 kHz.

[0015] Wesentlich ist, dass ein fahrzeugseitig bekannter Zeitanteil in die Systemlaufzeit bewusst eingebracht wird, so dass die Systemlaufzeit bei jedem Kommunikationsvorgang zur Verifikation der Zugriffsberechtigung ein anderer ist. Eine verlängerte Funkstrecke kann sich auf eine derartige verschiedene Zeitverzögerung von Fall zu Fall nicht einstellen. Grundsätzlich kann statt eines zufällig generierten Parameters auch eine fahrzeugseitig nach anderem Schema vorgegebene Verzögerung erzielt werden. Dadurch kann verhindert werden, dass aufgrund eines Zufalls die Verzögerungen in aufeinanderfolgenden Schließvorgängen zu ähnlich sind.

[0016] Um die Einschwingzeit des Schwingkreises zu beeinflussen, kann der Tastgrad der Stromversorgung beeinflusst werden. Es sind jedoch auch andere Möglichkeiten zur Veränderung des Einschwingverhaltens einsetzbar.

[0017] In einer Weiterbildung der Erfindung wird der Parameter, der die Verzögerung des Einschwingverhaltens bestimmt, an den ID-Geber gesendet. Alternativ kann auch ein aus dem Parameter erzeugter Wert von der Weckschaltung an den ID-Geber gesendet werden. Der ID-Geber erhält dann Informationen über die Einschwingdauer und kann seinerzeit eine Verifikation der Konsistenz verschiedener vorliegender Daten vornehmen. Beispielsweise können sogenannte RSSI-Daten, also für die Feldstärke bzw. Empfangsqualität repräsentative Daten verwendet werden, um die Entfernungsabhängigkeit des ID-Gebers von dem Fahrzeug zu bestimmen und mit in die Auswertung der Daten einzubeziehen.

[0018] In einer weiteren Ausführungsform der Erfindung wird die Kommunikation zwischen ID-Geber und fahrzeugseitigen Einrichtungen in mehreren Abschnitten durchgeführt.

[0019] Gemäß dieser Ausführungsform der Erfindung

wird zunächst eine Nachricht von der Weckschaltung im Fahrzeug an den ID-Geber gesendet. In Abhängigkeit von der gesendeten Nachricht kann der ID-Geber seine Ansprechschwelle für das nachfolgende Wecksignal einstellen. Auf diese Weise kann die Sicherheit des Verfahrens weiter erhöht werden.

[0020] In einer weiteren Ausführungsform ist die Weck-Schaltung derart ausgelegt, dass diese auf verschiedenen Frequenzen senden kann. Dazu können beispielsweise verschiedene Kanäle bei z.B. bei 20 kHz, 22 kHz und 24 kHz vorgesehen werden. Auf diesen Kanälen kann das Wecksignal gesendet werden. Der jeweils nächste verwendete Kanal kann in einer Nachricht codiert werden, und von der Weck-Schaltung an den ID-Geber übermittelt werden. Dieser kann dann bei der nachfolgenden Kommunikation anhand der empfangenen Frequenz diese mit dem Kanal laut zuvor übermittelter Nachricht abgleichen und so die Sicherheit des Authentifizierungsverfahrens weiter erhöhen.

[0021] Die Erfindung wird nun anhand eines Ausführungsbeispiels näher erläutert.

[0022] Figur 1 zeigt in schematischer Ansicht die Anordnung der Komponenten bei der Anwendung des erfindungsgemäßen Verfahrens gemäß einem ersten Ausführungsbeispiel.

[0023] In Figur 1 ist ein Fahrzeug 1 gezeigt, welches über eine schlüssellose Zugangsberechtigungskontrolle verfügt. Ein ID-Geber 2 wird von einem Benutzer mitgeführt und kann eine Funkkommunikation mit dem Fahrzeug 1 ausführen, um die Legitimation für einen Zugriff auf das Fahrzeug 1 zu überprüfen. Bei Annäherung eines Benutzers an das Fahrzeug 1, insbesondere bei Annäherung eines Körperteils des Benutzers an einen Fahrzeuggriff, wird eine Funkkommunikation 1a, 2a von dem Fahrzeug 1 mit dem ID-Geber 2 initiiert, in deren Verlauf die Legitimation des zugreifenden Benutzers überprüft wird. Insbesondere wird überprüft, ob die im ID-Geber gespeicherte Kennung im Fahrzeug als zugriffsberechtigte Kennung hinterlegt ist.

[0024] Die übliche und unkorruptierte Funkkommunikationsstrecke zwischen Fahrzeug 1 und ID-Geber 2 beträgt im Maximalfall einige Meter. Es soll sichergestellt werden, dass auf das Fahrzeug nicht zugegriffen werden kann, wenn sich der Benutzer mit dem legitimierenden ID-Geber übermäßig weit vom Fahrzeug entfernt aufhält, insbesondere außer Sichtweite.

[0025] Die Relay-Station-Attacke wird ausgeführt, indem die Funkstrecke zwischen Fahrzeug 1 und ID-Geber 2 künstlich verlängert wird, so dass die Funkkommunikation zwischen Fahrzeug und ID-Geber stattfindet, obwohl der Abstand zwischen Fahrzeug 1 und ID-Geber 2 eigentlich so groß ist, dass die Funkkommunikation aufgrund der Sendeleistung nicht möglich sein sollte. Dazu wird ein unberechtigter Angreifer sich in die Nähe des Fahrzeugs 1 begeben und mit einer Einrichtung 3, die z. B. in einem Koffer verborgen sein kann, einen Zugriffsversuch auf das Fahrzeug starten. Eine Gegenstation 4 befindet sich bei einem weiteren Angreifer in der Nähe

des berechtigten Benutzers mit dem ID-Geber 2. Das Fahrzeug sendet seine an die ID-Geber 2 gerichtete Kommunikation 1b aus, die von der Einrichtung 3 empfangen und über eine weitere Funkstrecke 3c an die Einrichtung 4 geleitet wird. Diese übermittelt in Nachricht 4d die empfangene Nachricht wiederum an den ID-Geber 2, welcher sie als Nachricht von dem Fahrzeug 1 auffasst und seine Legitimationsprüfung und -antwort absendet. Die Rückantwort 2d vom ID-Geber 2 an das Fahrzeug 1 läuft wiederum (4c, 3b) über die Stationen 4 und 3.

[0026] Erfindungsgemäß weist die fahrzeugseitige Kommunikationseinrichtung einen Schwingkreis auf, welcher beim Beginnen der Kommunikationsanfrage zum Einschwingen gebracht wird. Die Einschwingzeit, die der Schwingkreis zum Erreichen der Ansprechschwelle des ID-Gebers benötigt, wird fahrzeugseitig beeinflusst, indem der Duty-Cycle bzw. Tastgrad vorgegeben wird. Auf diese Weise kann die Verzögerung des Einschwingvorgangs gezielt beeinflusst werden. Gemäß der Erfindung sind Verzögerungen zwischen 1 und mehreren 10 ms möglich. Die Einschwingzeit wird in Abhängigkeit von einem fahrzeugseitig generierten Zufallsparameter eingestellt. Dieser Zufallsparameter kann mit anderen Fahrzeugsystemen gekoppelt sein, um aus irgendeiner sensorisch bestimmten Fahrzeuggröße eine Pseudozufallszahl generieren zu können. Dazu kommen alle im Fahrzeug vorliegenden Daten in Frage, z.B. Kilometerstand, Batteriespannung, Reifendruck oder sonstige Größen.

[0027] Eine derartig generierte Pseudozufallszahl liefert Werte, die von einem Angreifer nicht nachvollziehbar oder vorhersehbar sind.

[0028] Wird das erfindungsgemäße Verfahren gestartet, so wird fahrzeugseitig eine Verzögerung bestimmt, um die die natürliche Einschwingzeit des Schwingkreises verlängert wird. Über den Tastgrad der Versorgung des Schwingkreises wird die Einschwingzeit dementsprechend beeinflusst, so dass nach einer Anstiegszeit T1 die Ansprechschwelle der Kommunikation mit dem ID-Geber erreicht ist (in der Figur sind die Nachrichten 1a und 1b mit diesem Zeitfaktor behaftet). Befindet sich der ID-Geber in der Nähe des Fahrzeugs (Nachricht 1a), liegt also ein berechtigter Zugriff vor, so erfolgt die Antwort des ID-Gebers nach Auswertung und Überprüfung der Nachricht unmittelbar bzw. mit geringer Verzögerung T2. Die Antwort des ID-Gebers wird im Hochfrequenzbereich an die fahrzeugseitige Kommunikationseinrichtung übermittelt, so dass die gesamte Systemlaufzeit einem akzeptablen Zeitfenster um die Einschwingzeit des Kondensators plus die Zeit T2 für die Auswertung im ID-Geber 2 und die hochfrequente Rückantwort benötigt. Ist beispielsweise eine bewusste Verzögerung T1 von 5 ms eingestellt, so wird das akzeptierte Zeitfenster für eine Antwort des ID-Gebers beispielsweise zwischen 5 und 5,5 ms betragen. Außerhalb dieses Zeitfensters eingehende Antworten des ID-Gebers werden ignoriert und führen nicht zu einer Freigabe des Fahrzeugs 1.

[0029] Für die Kommunikation mit dem ID-Geber wird

fahrzeugseitig eine Wecknachricht 10 mit 20 kHz generiert. Der ID-Geber empfängt diese Nachricht 10, wertet sie aus und sendet ein hochfrequentes Antwortsignal 11 zurück. Da für die Hochfrequenzkommunikation wesentlich weniger Zeit benötigt wird, ist das Zeitfenster entsprechend eng um die vorgegebene Einschwingzeit anzuordnen.

[0030] Bei einem unberechtigten Zugriffsversuch empfängt die Einrichtung 3 die Nachricht 1b des Fahrzeugs 1. Die Einrichtung 3 übermittelt die empfangene Nachricht im Hochfrequenzbereich an die Einrichtung 4, hierzu wird regelmässig eine kaum relevante Zeitspanne benötigt. Bei der Übertragung 4d von der Station 4 und den ID-Geber 2, welche im niedrigeren Frequenzbereich stattfinden muss, tritt nun allerdings wiederum die vorgegebene Einschwingzeit T1' auf, die fahrzeugseitig in Abhängigkeit von einem Zufallsparameter vorgegeben wurde, da die Kondensatoren des Systems beim Aufstarten nicht geladen sind. Die zeitverzögerte Nachricht 1b wird dementsprechend mit etwa verdoppelter Verzögerung als Nachricht 4d an den ID-Geber 2 weitergeleitet.

[0031] Der fahrzeugseitig bewusst eingebrachte Zeitverzögerungsfaktor liegt demnach zweimal im System vor, so dass die Antwort 2d des ID-Gebers 2 an das Fahrzeug 1 verzögert gesendet wird. Nun fällt die Antwortnachricht des ID-Gebers 2 nicht in das zuvor kalkulierte Zeitfenster, und daher wird der Zugriff das Fahrzeug verwehrt.

[0032] Im Rahmen der Erfindung sind verschiedene Abwandlungen möglich. Insbesondere sind vielfältige Arten möglich, den Zeitverzögerungsparameter zu bestimmen. Dieser kann zufällig bestimmt werden, oder aus fahrzeugseitigen Parametern abgeleitet werden. Es ist wesentlich, dass die Erfindung mit üblichen, meist schon ohnehin vorhandenen Mitteln realisiert werden kann, da insbesondere die Einschwingzeit des Schwingkreises über den Duty-Cycle im Steuergerät eingestellt werden kann, so dass keine wesentlichen baulichen Veränderungen erforderlich sind.

Patentansprüche

1. Verfahren zur Kontrolle der Zugangsberechtigung für ein Kraftfahrzeug, wobei mittels einer fahrzeugseitigen Weckschaltung ein Weck-Funksignal ausgesendet wird, wobei ein von einem Benutzer des Kraftfahrzeugs mitgeführter ID-Geber das Weck-Funksignal empfängt und mittels einer Auswerteschaltung überprüft, wobei im Falle einer erfolgreichen Überprüfung von dem ID-Geber ein hochfrequentes Freigabe-Funksignal ausgesendet wird, wobei eine fahrzeugseitige Steuereinrichtung das Freigabe-Funksignal empfängt und in Abhängigkeit von dem Signal eine Freigabe einer fahrzeugseitigen Schließeinrichtung bewirkt,

dadurch gekennzeichnet, dass

durch die Weckschaltung zur Erzeugung des Weck-Funksignals ein Schwingkreis derart angesteuert wird, dass die Einschwingdauer des Schwingkreises in Abhängigkeit von einem zufällig generierten Parameter variiert wird, wobei die Stromversorgung des Schwingkreises in Abhängigkeit von dem Parameter kontrolliert wird,
eine erwartete Systemlaufzeit in Abhängigkeit von dem generierten Parameter bestimmt wird, und
die Zeitdauer von der Ansteuerung des Schwingkreises bis zum Empfang des Freigabe-Signals in der Steuereinrichtung gemessen und mit der erwarteten Systemlaufzeit verglichen wird,
wobei
dann, wenn die Zeitdauer um mehr als einen vorgegebenen Wert von der erwarteten Systemlaufzeit abweicht, eine Freigabe der Schließeinrichtung unterbunden wird.

5

10

15

20

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der Parameter oder ein aus dem Parameter erzeugter Wert von der Weckschaltung an den ID-Geber gesendet wird.

25

3. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** vor der Übermittlung des Wecksignals eine Nachricht von der Weckschaltung an den ID-Geber gesendet wird, wobei der ID-Geber in Abhängigkeit von der Nachricht seine Ansprechschwelle für das Wecksignal einstellt.

30

35

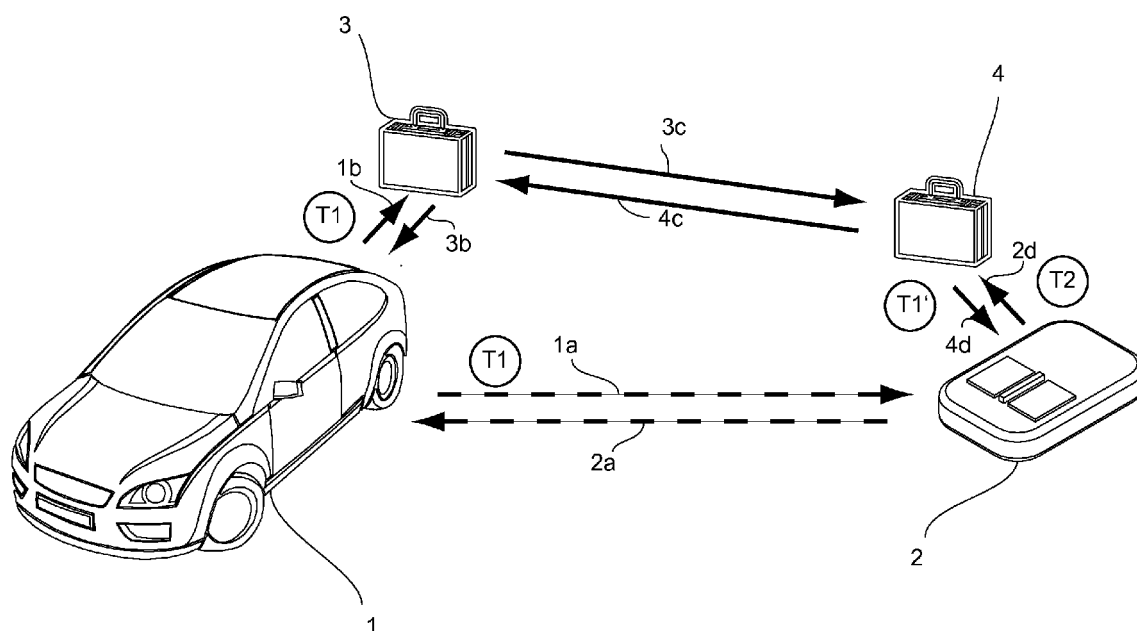
40

45

50

55

Fig. 1



IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- EP 06117688 A [0004]