



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 0 596 343 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
07.03.2001 Patentblatt 2001/10

(51) Int Cl.7: **E05B 49/00**

(21) Anmeldenummer: **93117117.7**

(22) Anmeldetag: **22.10.1993**

(54) **Verfahren zur Zuordnung eines mit einem Sender ausgestatteten Kraftfahrzeugschlüssels zu einem Empfänger einer Steuereinrichtung eines Kraftfahrzeugs**

Method for allocating a motor vehicle key equipped with a sender to a receiver of a control device of a motor vehicle

Procédé d'allocation d'une clé de véhicule à moteur avec un émetteur à un récepteur d'un dispositif de contrôle d'un véhicule à moteur

(84) Benannte Vertragsstaaten:
DE FR GB IT NL SE

(30) Priorität: **31.10.1992 DE 4236863**

(43) Veröffentlichungstag der Anmeldung:
11.05.1994 Patentblatt 1994/19

(73) Patentinhaber: **Mannesmann VDO AG
60326 Frankfurt (DE)**

(72) Erfinder: **Ranzenberger, Ralf
D-55278 Uelversheim (DE)**

(74) Vertreter: **Klein, Thomas, Dipl.-Ing.
Kruppstrasse 105
60388 Frankfurt (DE)**

(56) Entgegenhaltungen:
**EP-A- 0 372 285 WO-A-90/15211
WO-A-91/18169 DE-A- 4 201 568
FR-A- 2 566 823**

EP 0 596 343 B1

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).

Beschreibung

[0001] Die Erfindung bezieht sich auf ein Verfahren zur Zuordnung eines mit einem Sender für die drahtlose Übertragung verschlüsselter Funktionsbefehle ausgestatteten Kraftfahrzeugschlüssels zu einem Empfänger einer Steuereinrichtung für die Zentralverriegelung und Diebstahlsicherung eines Kraftfahrzeuges.

[0002] Zur Fernbedienung von Türschlössern an Kraftfahrzeugen werden Schlüssel benutzt, in die ein Sender zur drahtlosen Übertragung von verschlüsselten Funktionsbefehlen eingebaut ist. Im Kraftfahrzeug ist ein Empfänger angeordnet, der die übermittelten Daten entschlüsseln und in Steuersignale umwandeln kann. Zum Schutz gegen unbefugte Benutzung hat man bereits vorgeschlagen, die Codierung laufend zu verändern (DE-OS 34 06746 und 35 29 882). Dabei ist es aber erforderlich, daß die Übertragung in beiden Richtungen erfolgt und daß dem Sender zusätzlich ein Empfänger und dem Empfänger zusätzlich ein Sender zugeordnet werden muß. Diese Verfahren sind aber trotz des hohen Aufwandes gegen Mißbrauch noch nicht ausreichend gesichert, weil man sich aus mehreren abgehörten codierten Funktionsbefehlen das Codierschema ableiten und dann unbefugt, aber zerstörungsfrei Zugang zu einem Fahrzeug verschaffen kann. Dieser Nachteil kann vermieden werden, wenn stets ein bestimmter Bruchteil des Datentelegramms von der Übertragung ausgespart bleibt und wenn die Übertragung nur in einer Richtung erfolgt.

[0003] Dazu ist es aber erforderlich, daß zusammengehörige Sender und Empfänger bei Inbetriebnahme von übereinstimmenden Daten ausgehen, die für ein bestimmtes System Schlüssel + Sender/Schloß + Empfänger charakteristisch sind und eine Unterscheidung von allen anderen Systemen der gleichen Serie oder Baugruppe erlauben. Mit anderen Worten, jedes System muß einerseits individualisiert und andererseits synchronisiert werden.

[0004] Dieser Vorgang bereitet an sich keine Schwierigkeiten, ist aber mit einem erheblichen Aufwand an Dokumentation und Kennzeichnung verbunden, weil die Sender und Empfänger in der Regel bei einem anderen Hersteller gefertigt werden als die Schlüssel und Schlösser und weil schließlich die Endmontage des Systems an einem dritten Platz erfolgt. Über den gesamten Fertigungsweg muß sichergestellt werden, daß dem Kunden ein Fahrzeug ausgehändigt wird, bei dem die Schlüssel mechanisch zum Schloß passen und bei dem Sender und Empfänger die gleichen Ausgangsdaten abgespeichert haben.

[0005] Es ist daher schon vorgeschlagen worden (vgl. Patentanmeldung P 42 01 568.5) einen fertigen Sender in einen Schlüsselrohling einzusetzen und durch die Eingabe von Kenndaten elektronisch zu individualisieren, den Schlüsselrohling einem Schloßrohling zuzuordnen und beide Teile zueinander passend mechanisch zu individualisieren sowie für Transport- und Mon-

tagezwecke unverlierbar miteinander zu verbinden, einen fertigen Empfänger und ein mechanisch individualisiertes Schloß bestimmungsgemäß einzubauen und schließlich den mit dem Schloß eingebauten Empfänger durch den Sender des zugehörigen Schlüssels zu individualisieren und gleichzeitig mit dem Sender zu synchronisieren, indem die Kenndaten des Senders auf den Empfänger übertragen werden.

[0006] Bei diesem Verfahren entfällt zwar jeglicher Dokumentations- und Kennzeichnungsaufwand, es ist aber nicht sichergestellt, daß im Schlüssel gespeicherte Kenndaten auf dem Fertigungsweg versehentlich auf den Empfänger eines Schlosses übertragen werden, das mechanisch nicht zu dem Schlüssel paßt. Dadurch fallen mechanische und elektronische Individualisierung und Synchronisierung auseinander und das betroffene Schlüssel-Schloß-System ist nicht brauchbar. Außerdem besteht die Gefahr, daß die im Schlüssel gespeicherten Kenndaten während des Herstellungsprozesses unbefugt gesendet, ausgelesen und später mißbräuchlich benutzt werden.

[0007] Es besteht somit die Aufgabe, das bekannte Verfahren so weiterzubilden, daß die vorstehenden Nachteile nicht mehr auftreten können.

[0008] Die Aufgabe wird durch die Merkmale des Patentanspruchs 1 gelöst.

[0009] Das erfindungsgemäße Verfahren unterscheidet sich von dem Verfahren gemäß Patentanmeldung P 42 01 568.5 dadurch, daß der Schlüssel erst am Ende des Herstellungsprozesses, d. h. unmittelbar vor der Auslieferung des Fahrzeugs, mit den Kenndaten versehen wird, zu einem Zeitpunkt also, wenn eine Verwechslung von Schlüssel und Schloß sowie ein unbefugtes Betätigen des Senders zur Ermittlung der Kenndaten praktisch ausgeschlossen ist.

[0010] Die Individualisierung des Schlüssels erfolgt dabei nach einem nicht einsehbaren Programm, so daß die Kenndaten nicht einmal von der Person, die den Schlüssel in das Kenndatenprogrammiergerät einlegt, ermittelt werden können. Damit ist die Geheimhaltung der Kenndatenübertragung optimal gewährleistet.

[0011] Vorteilhafte Ausgestaltungen des Erfindungsgedankens sind in den Unteransprüchen 2 bis 6 beschrieben.

[0012] Weitere Einzelheiten werden anhand des in Figuren dargestellten Ausführungsbeispiels erläutert.

Fig. 1 Blockschaubild einer Anordnung zur Durchführung des erfindungsgemäßen Verfahrens

Fig. 2 Ablaufplan des erfindungsgemäßen Verfahrens.

[0013] Fig. 1 zeigt ein Blockschaubild mit einem Kenndatenerzeuger 1, einem Kenndaten-Programmiergerät 2 und einem Schlüssel 3. Als Kenndatenerzeuger 1 wird dabei vorteilhafterweise ein Fertigungsrechner eingesetzt. Dieser enthält einen Mikroprozessor mit

Pseudo-Zufallsgenerator und Datenspeicher sowie eine Schnittstelle. Nach einem bestimmten Ablaufplan (Figur 2) werden damit die Festcode- und Wechselcode-Daten sowie alle veränderlichen Steuerbefehle erstellt, die für den Sendebetrieb des Schlüssels 3 notwendig sind. Dabei kann der Pseudo-Zufallsgenerator sowohl schaltungstechnisch wie auch softwaremäßig realisiert werden. Der Ablaufplan sorgt nicht nur dafür, daß für jeden Schlüssel individuelle Kenndaten erstellt werden, sondern auch für internen Kontrollen, die zum fehlerfreien Ablauf der Kenndaten-Erzeugung und ihre Übertragung erforderlich sind.

[0014] Vom Kenndatenerzeuger 1 werden die Kenndaten an das Kenndatenprogrammiergerät 2 übergeben, wobei durch Rücklesen jeweils überprüft wird, ob bei der Datenübergabe Fehler aufgetreten sind. Das Kenndatenprogrammiergerät 2 enthält ebenfalls einen Mikroprozessor mit Datenspeicher, eine Schnittstelle zum Kenndatenerzeuger 1 und eine Schlüsselaufnahme mit einer Schnittstelle für den Schlüssel 3 in Form von Kontakten.

[0015] Der Schlüssel 3 ist mit einem Mikroprozessor, einem Arbeitsspeicher, einem nichtflüchtigen Speicher, einem Pseudo-Zufallsgenerator, einem Sender, einer Batterie, einer Betätigungseinrichtung in Form von Tasten und einer Schnittstelle mit Eingangskontakten ausgerüstet.

[0016] Zur Übertragung der Kenndaten in den Datenspeicher des Schlüssel 3 wird der Schlüssel 3 automatisch oder manuell in die Schlüsselaufnahme des Kenndatenprogrammiergeräts 2 eingelegt, wobei die Eingangskontakte des Schlüssels mit den Kontakten des Programmiergeräts 2 verbunden werden. Um dem Schlüssel 3 die notwendigen Kenndaten zu übermitteln, wird sein Mikroprozessor in einem Resetmodus gehalten und die notwendige Spannungsversorgung angelegt. Danach wird das Übertragungsprogramm gestartet und der Schlüssel 3 mit den Kenndaten programmiert. Auch hier wird durch Rücklesen kontrolliert, ob die in den nichtflüchtigen Speicher des Schlüssel 3 übertragenen Kenndaten mit dem für den bestimmten Schlüssel vorgesehenen Datensatz im Programmiergerät 2 übereinstimmt. Abhängig vom Ergebnis dieses Vergleichs wird eine entsprechende Rückmeldung an das Programmiergerät 2 abgesetzt. Bei einer Fehlermeldung wird der Programmiervorgang wiederholt. Erst danach wird der Schlüssel zur Entnahme freigegeben.

[0017] In einem weiteren Vorgang kann danach der für den Empfänger im Kraftfahrzeug bestimmte Teil des im Schlüssel gespeicherten Kenndatensatzes durch eine besondere Betätigung drahtlos übertragen werden. Der im Kraftfahrzeug angeordnete Empfänger entschlüsselt die übermittelten Daten und wandelt sie in die entsprechenden Steuersignale um.

Patentansprüche

1. Verfahren zur Zuordnung eines mit einem Sender für die drahtlose Übertragung verschlüsselter Funktionsbefehle ausgestatteten Kraftfahrzeugschlüssels zu einem Empfänger einer Steuereinrichtung für die Zentralverriegelung und Diebstahlsicherung eines Kraftfahrzeuges, bei welchem am Ende des Herstellungsprozesses des Kraftfahrzeuges von einem Kenndatenerzeuger nach einem bestimmten Algorithmus unter Einschaltung eines Pseudo-Zufallsgenerators erstmalig individuelle, für den Sendebetrieb des Kraftfahrzeugschlüssels notwendige Kenndaten generiert und zuerst in ein den Kraftfahrzeugschlüssel aufnehmendes Kenndatenprogrammiergerät eingespeist und anschließend von diesem zur Individualisierung des Kraftfahrzeugschlüssels an diesen weitergegeben werden und danach die für den Empfänger bestimmten Teile der im Schlüssel gespeicherten Kenndaten an den Empfänger drahtlos übertragen werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Übertragung der Kenndaten durch Zurücklesen kontrolliert wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß für jeden Schlüssel ein eigener Satz an Kenndaten generiert wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Kenndaten Festcode- und Wechselcode-Anteile sowie Steuerbefehle enthalten.

Claims

1. Method for associating a motor vehicle key which has a transmitter for the wireless transmission of encrypted function instructions with a receiver in a control device for the central locking system and anti-theft system of a motor vehicle, in which, at the end of the production process for the motor vehicle, a characteristic data generator uses a particular algorithm to generate, for the first time, individual characteristic data required for the motor vehicle key's transmission mode, by connecting a pseudo-random generator, and first to feed it into a characteristic data programming unit holding the motor vehicle key and then to pass it on from this characteristic data programming unit to the motor vehicle key for individualization purposes, and those parts of the characteristic data stored in the key which are intended for the receiver are then wirelessly transmitted to the receiver.
2. Method according to Claim 1, characterized in that

the transmission of the characteristic data is checked by reading back.

3. Method according to Claim 1 or 2, characterized in that a dedicated set of characteristic data is generated for each key. 5
4. Method according to one of Claims 1 to 3, characterized in that the characteristic data contains fixed code elements and alternating code elements and also control instructions. 10

Revendications

1. Procédé pour affecter une clé de véhicule automobile équipée d'un émetteur pour la transmission sans fil d'instructions de fonctionnement codées à un récepteur d'un dispositif de commande pour le verrouillage central et la sécurité antivol d'un véhicule automobile, avec lequel des données d'identification nécessaires pour le fonctionnement en émission de la clé du véhicule automobile sont générées pour la première fois individuellement à la fin du processus de fabrication du véhicule automobile par un générateur de données d'identification selon un algorithme donné en activant un générateur pseudo-aléatoire et tout d'abord mémorisées dans un programmeur de données d'identification recevant la clé du véhicule automobile et ensuite retransmises à partir du programmeur à la clé du véhicule automobile afin de personnaliser celle-ci, et les parties déterminées des données d'identification mémorisées dans la clé et destinées au récepteur sont ensuite transmises sans fil au récepteur. 15
20
25
30
35
2. Procédé selon la revendication 1, caractérisé en ce que la transmission des données d'identification est contrôlée par relecture. 40
3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'un jeu de données d'identification propre est généré pour chaque clé.
4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que les données d'identification contiennent des parties en code fixe et en code variable ainsi que des instructions de commande. 45

50

55

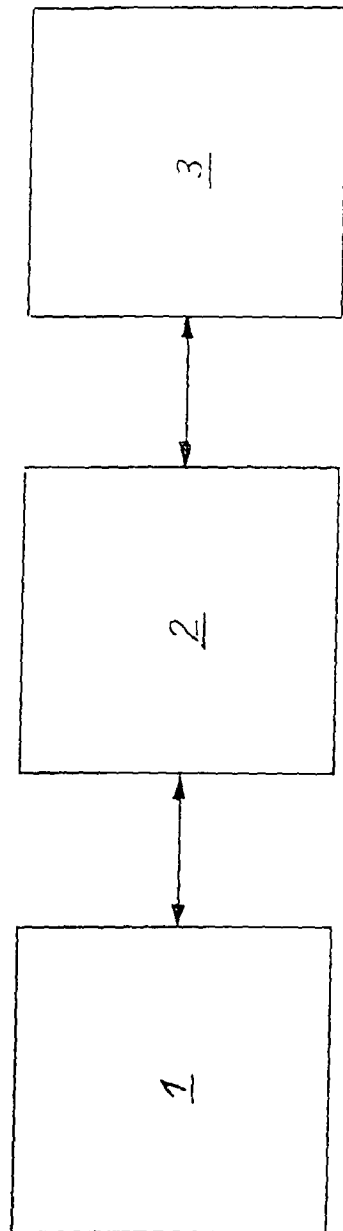
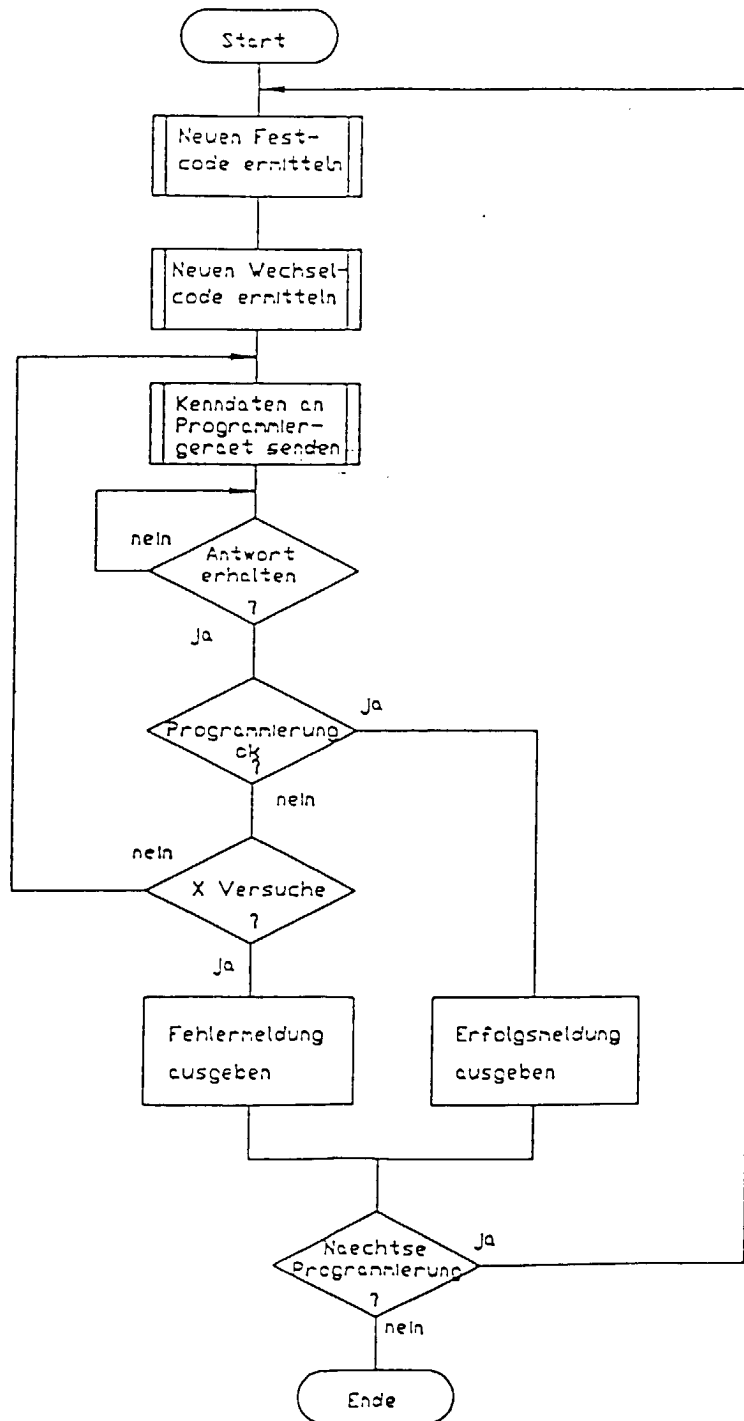


Fig. 1



Figur 2