(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 596 343 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **93117117.7**

(51) Int. Cl.5: **E05B 49/00**

(22) Anmeldetag: **22.10.93**

(30) Priorität: **31.10.92 DE 4236863**

(43) Veröffentlichungstag der Anmeldung:
11.05.94 Patentblatt 94/19

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

(71) Anmelder: **VDO Adolf Schindling AG**
Gräfstrasse 103
D-60487 Frankfurt(DE)

(72) Erfinder: **Ranzenberger, Ralf**
Ulfridstrasse 15
D-55278 Uelversheim(DE)

(74) Vertreter: **Klein, Thomas, Dipl.-Ing. (FH)**
Sodener Strasse 9
D-65824 Schwalbach/Ts. (DE)

(54) Verfahren zur Eingabe von Kenndaten in den Mikroprozessor eines Kraftfahrzeugschlüssels.

(57) Zur Eingabe von Kenndaten in den Mikroprozessor eines mit einem Sender ausgestatteten Kraftfahrzeugschlüssels (3) für die drahtlose Übertragung verschlüsselter Funktionsbefehle auf den Empfänger einer Steuereinrichtung für die Zentralverriegelung und Diebstahlsicherung eines Kraftfahrzeugs wird ein Verfahren vorgeschlagen, das dadurch gekennzeichnet, ist, daß die von einem Kenndatenerzeuger (1) nach einem bestimmten Algorithmus unter Einschaltung eines Pseudo-Zufallsgenerators generierten Kenndaten zuerst in ein Kenndatenprogrammiergerät (2) eingespeist und von diesem an den Kraftfahrzeugschlüssel (3) weitergegeben werden.

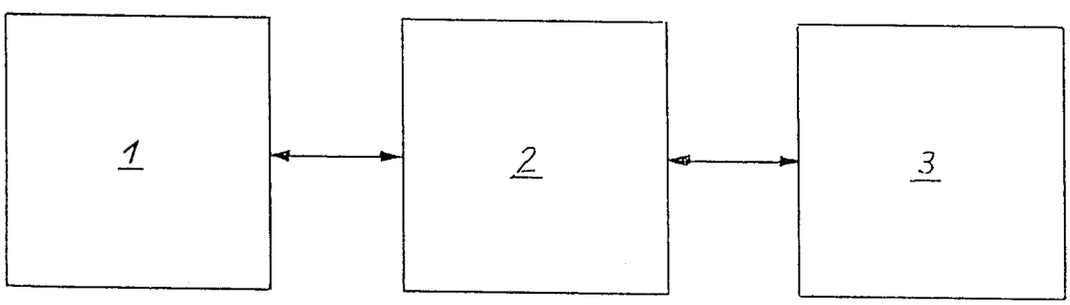


Fig. 1

EP 0 596 343 A1

Die Erfindung bezieht sich auf ein Verfahren zur Eingabe von Kenndaten in den Mikroprozessor eines mit einem Sender ausgestatteten Kraftfahrzeugschlüssels für die drahtlose Übertragung verschlüsselter Funktionsbefehle auf den Empfänger einer Steuereinrichtung für die Zentralverriegelung und Diebstahlsicherung eines Kraftfahrzeugs sowie auf eine Vorrichtung zur Durchführung des Verfahrens und einem nach dem verfahren hergestellten Schlüssel.

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 06 746 und 35 29 882). Dabei ist es aber erforderlich, daS 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.

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.

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.

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 Montagezwecke 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.

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.

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

Zur Lösung dieser Aufgabe wird vorgeschlagen, die von einem Kenndatenerzeuger nach einem bestimmten Algorithmus unter Einschaltung eines Pseudo-Zufallsgenerators generierten Kenndaten zuerst in ein Kenndatenprogrammiergerät einzuspeisen und anschließend von diesem an den Kraftfahrzeugschlüssel weiterzugeben.

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 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.

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.

Vorteilhafte Ausgestaltungen des Erfindungsgedankens sind in den Unteransprüchen 2 bis 9 beschrieben.

Weitere Einzelheiten werden anhand des in den Figuren dargestellten Ausführungsbeispiels erläutert.

Fig. 1 Blockschaltbild einer Anordnung zur Durchführung des erfindungsgemäßen Verfahrens,

Fig. 2 Ablaufplan des erfindungsgemäßen Verfahrens.

Fig. 1 zeigt ein Blockschaltbild 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.

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.

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.

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.

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 Eingabe von Kenndaten in den Mikroprozessor eines mit einem Sender ausgestatteten Kraftfahrzeugschlüssels für die drahtlose Übertragung verschlüsselter Funktionsbefehle auf den Empfänger einer Steuereinrichtung für die Zentralverriegelung und Diebstahlsicherung eines Kraftfahrzeugs, dadurch gekennzeichnet, daß die von einem Kenndatenerzeuger nach einem bestimmten Algorithmus unter Einschaltung eines Pseudo-Zufallsgenerators generierten Kenndaten zuerst in ein Kenndatenprogrammiergerät eingespeist und anschließend von diesem an den Kraftfahrzeugschlüssel weitergegeben 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.

5. Vorrichtung zur Durchführung des Verfahrens nach den Ansprüchen 1 bis 4, gekennzeichnet durch einen Kenndatenerzeuger mit Mikroprozessor, Speicher, Pseudo-Zufallsgenerator und Schnittstelle sowie durch ein Programmiergerät mit Mikroprozessor, Speicher, Schlüsselaufnahme und Schnittstelle mit Ausgangskontakten.

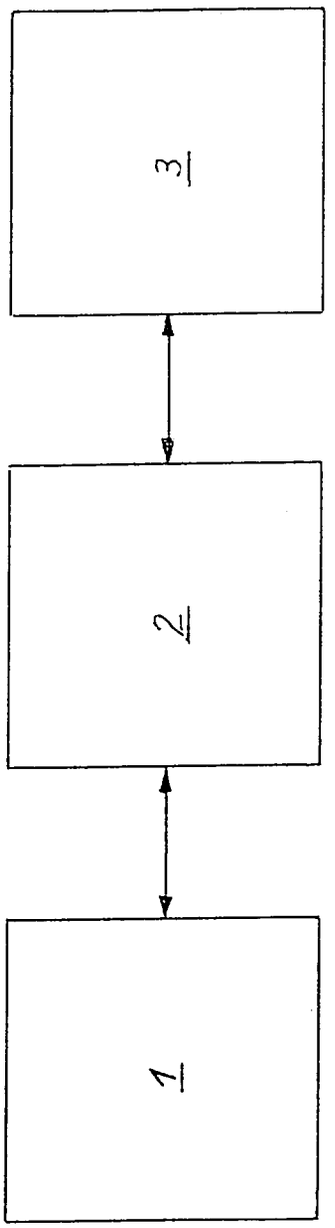
6. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, daß noch eine Transporteinrichtung vorgesehen ist, mit der die als Schüttgut vorliegenden Schlüssel vereinzelt und in die Schlüsselaufnahme eingelegt werden können.

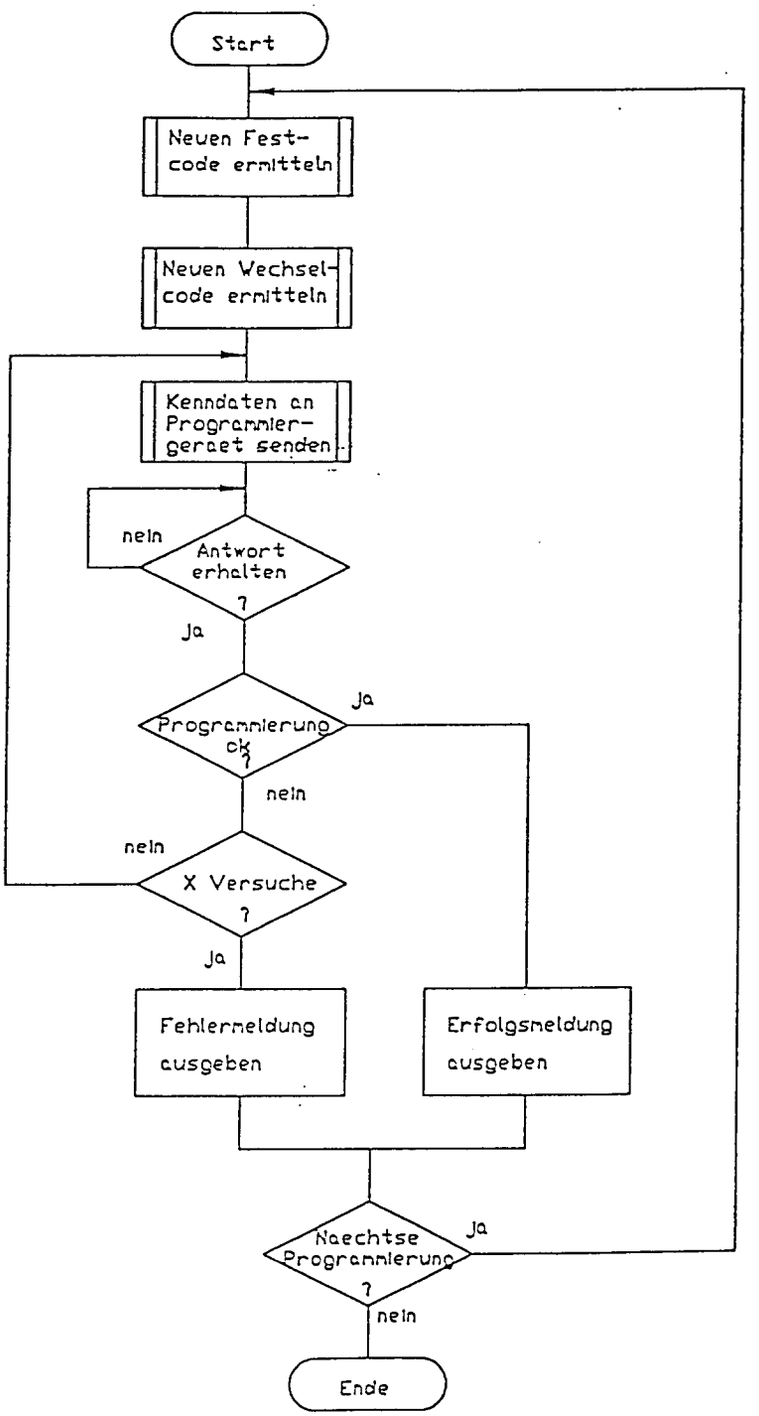
7. Schlüssel für Anwendung des Verfahrens nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, daß er einen Mikroprozessor, einen Arbeitsspeicher, einen nichtflüchtigen Speicher, einen Pseudo-Zufallsgenerator, einen Sender, eine Batterie, eine Betätigungseinrichtung und eine Schnittstelle mit Eingangskontakten aufweist.

8. Schlüssel nach Anspruch 7, dadurch gekennzeichnet, daß die Betätigungseinrichtung aus wenigstens 2 Tastern besteht.

9. Schlüssel nach Anspruch 8, dadurch gekennzeichnet, daß er außerdem eine Strom-aus-Sicherheitsschaltung enthält.

Fig. 1




Start
Neuen Fest-code ermitteln
Neuen Wechsel-code ermitteln
Kenndaten an Programmier-geraet senden
nein
Antwort erhalten ?
Ja
Programmierung ok ?
Ja
nein
nein
X Versuche ?
Ja
Fehlermeldung ausgeben
Erfolgsmeldung ausgeben
Naechtse Programmierung ?
Ja
nein
Ende

Figur 2

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 93 11 7117

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.5)
A	WO-A-91 18169 (HYATT) * Seite 4, Zeile 19 - Seite 5, Zeile 5 * * Seite 6, Zeile 12 - Zeile 24 * * Seite 7, Zeile 15 - Seite 9, Zeile 4; Abbildungen 1A,1B,4,7 *	1	E05B49/00
A	---	3,5,7,9	
A	EP-A-0 372 285 (DELTA ELETTRONICA) * Spalte 2, Zeile 47 - Spalte 3, Zeile 35; Abbildungen 1,2 *	1,4,7	
A	---		
A	WO-A-90 15211 (HARRIS,SHAW)		
A	---		
A,D, P	FR-A-2 566 823 (BLAIZE)	1	

	DE-A-42 01 568 (BALTES,WIESER,ULLRICH) * Spalte 1, Zeile 1 - Spalte 2, Zeile 45 *		

RECHERCHIERTE SACHGEBIETE (Int.Cl.5)
E05B

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	27. Januar 1994	Herbelet, J.C.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)