

12 **EUROPÄISCHE PATENTANMELDUNG**

21 Anmeldenummer: **90100689.0**

51 Int. Cl.<sup>5</sup>: **E05B 49/00, E05B 65/36**

22 Anmeldetag: **13.01.90**

Geänderte Patentansprüche gemäss Regel 86 (2) EPÜ.

30 Priorität: **24.02.89 DE 3905651**

43 Veröffentlichungstag der Anmeldung: **05.09.90 Patentblatt 90/36**

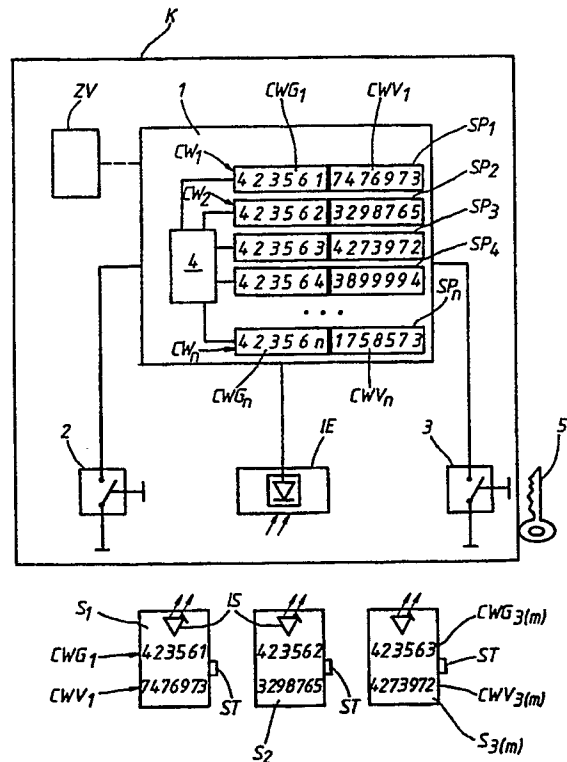
84 Benannte Vertragsstaaten: **ES FR GB IT SE**

71 Anmelder: **DAIMLER-BENZ AKTIENGESELLSCHAFT**  
**Mercedesstrasse 136**  
**D-7000 Stuttgart 60(DE)**

72 Erfinder: **Lindmayer, Martin**  
**Rosenstrasse 1**  
**D-7030 Böblingen 4(DE)**  
 Erfinder: **Claar, Klaus**  
**Sommerhofenstrasse 108**  
**D-7032 Sindelfingen(DE)**

54 **Verfahren zur Sicherung von Codeworten eines Fernwirksystems und Fernwirksystem mit durch Codeworte übertragbarem Code.**

57 Die Sicherheit eines auf drahtloser Codeübertragung mittels eines oder mehrerer unabhängiger Sender auf einen Empfänger beruhenden und für beliebige Objekte, insbesondere für zentral verriegelbare Kraftfahrzeuge, verwendbaren Fernwirksystems wird gesteigert, indem ein unveränderlicher Codeanteil, der bei jeder Codeübertragung zusammen mit einem gemäß einem vorgegebenen Algorithmus variablen Codeanteil übertragen wird, objektspezifisch sowohl in jedem Sender als auch in dem objektfesten Empfänger abgelegt wird. Ein Synchronisiervorgang zwischen einem Sender und dem Empfänger, der ohnehin nur abhängig von einer mechanischen Schlüsselrestriktion durchführbar ist, ist dann nur möglich, wenn der individuelle objektspezifische Codeanteil des jeweiligen Senders im Empfänger gespeichert und abrufbar ist.



EP 0 385 070 A1

## Verfahren zur Sicherung von Codeworten eines Fernwirksystems und Fernwirksystem mit durch Codeworte übertragbarem Code

Die Erfindung bezieht sich auf ein Verfahren zur Sicherung von Codeworten eines Fernwirksystems mit den Merkmalen des Oberbegriffs des Patentanspruchs 1 und auf ein Fernwirksystem nach dem Oberbegriff des Patentanspruchs 6, das insbesondere zur Durchführung des Verfahrens geeignet ist. Ein gattungsgemäßes Verfahren kann aus der Arbeitsweise eines insbesondere für Zentralverriegelungsanlagen von Kraftfahrzeugen vorgesehenen bekannten Fernwirksystems (DE 36 36 822 C1) hergeleitet werden.

Die drahtlos übertragenen Codeworte dieses Fernwirksystems werden gegen unbefugte Aufzeichnung und Benutzung geschützt, indem ein nach einem vorgegebenen Algorithmus veränderbarer Anteil jedes als aktuell betrachteten Codewortes im Empfänger und im zuletzt verwendeten Sender synchron fortgeschaltet wird. Der Algorithmus stützt sich auf ein sowohl im Empfänger als auch im Sender in EEPROMs gespeichertes, normalerweise unveränderliches Urcodewort ("Key-Code-Wort").

Aufgrund der gewählten Zusammensetzung jedes Codewortes und des verwendeten Algorithmus, der nur in eine Richtung fortschreitet, kann ein einmal verwendetes Codewort identisch erst nach einer sehr großen Zeitspanne bzw. nach einer sehr großen Anzahl von Fortschaltungen wiederkehren. Die unbefugte Wiederverwendung eines widerrechtlich aufgezeichneten Codewortes ist dadurch praktisch ausgeschlossen.

Neben seinem algorithmisch veränderbaren Anteil kann jedes Codewort des gattungsbildenden Fernwirksystems ferner sogenannte Systembits enthalten, die für verschiedene Unterscheidungen - z. B. Schlüsseltypen (Haupt-/ Nebenschlüssel), Automarke, Schlüsselssystem, aktuell steuerbare Funktion etc. - herangezogen werden können. Diese Systembits sind nach einer Variante des bekannten Systems von der algorithmischen Veränderung ausgenommen. Ein oder mehrere Systembit(s) kann/können aber gleichwohl vom Benutzer des Senders willkürlich - mittels zusätzlich zur Sendetaste am Sender vorgesehener Schalter - verändert werden, um die durch den Sender steuerbare bzw. auslösbare Funktion ohne Einflußnahme auf den Fortschaltealgorithmus zu verändern. Der Empfänger kann bei geöffneter Tür des Fahrzeugs mittels eines elektrischen Schalters manuell auf eine "Lernphase" umgeschaltet werden. In dieser wird das Key-Code-Wort des Empfängers neu programmiert, und zwar notwendigerweise einschließlich der erwähnten Systembits, indem das als nächstes von einem beliebigen, zum allgemei-

nen System passenden Sender zum Empfänger übertragene Codewort neu eingespeichert wird. Dieses neue Urcodewort wird dann als das bei jeder folgenden Codewort - Übertragung der Fortschaltung nach dem vorgegebenen Algorithmus unterliegende akzeptiert und gespeichert.

Ein in einem vorhandenen Sender gespeichertes Codewort kann durch Herausnehmen der Batterie aus dem Sender vollständig zurückgesetzt werden. Danach kann wieder der oben beschriebene "Lernvorgang" des Empfängers - mit dem Sender mit rückgesetztem Code - durchgeführt werden. Dies wird vor allem zur Abkürzung der Synchronisierung empfohlen, wenn die Codeworte in Sender und Empfänger einmal unterschiedlich weit fortgeschaltet worden sind.

Natürlich kann auch ein Unbefugter durch vorübergehende Entnahme der Batterie aus dem in seinem Besitz befindlichen Sender den beschriebenen Rücksetzvorgang im Sender durchführen.

Es ist auch ein Fernwirksystem einer Zentralverriegelungsanlage bekannt (DE 32 44 049 C2), welches in einer Ausführungsform mit mehreren Sendern eine von Sender zu Sender unterschiedliche Menge von Codeworten zur Verfügung stellt.

Da auch die Codeworte dieses Fernwirksystems algorithmisch fortgeschaltet werden, müssen Vorkehrungen getroffen werden, welche die Codefortschaltung in Abhängigkeit von dem verwendeten Sender auf den diesem individuell zugeteilten begrenzten Codewortvorrat begrenzen, um unnötigen Nachsynchronisierungsaufwand bei wechselnder Senderverwendung zu vermeiden.

Zu diesem Zweck sind jedem Sender unterschiedliche Kennungen zugeteilt, die bei Betätigung des jeweiligen Senders primär ausstrahlbar sind. Eine dem Empfänger nachgeschaltete Decodiereinrichtung ist zur Verarbeitung der von Sender zu Sender unterschiedlichen Menge von Codeworten mit mehreren, der Anzahl der Sender entsprechenden Decodierkanälen ausgerüstet, welche durch die Senderkennungen einschaltbar sind.

Über die Art dieser Senderkennungen wird in der letztgenannten Patentschrift keinerlei Aussage getroffen. Sie sind funktionell den willkürlich änderbaren Systembits des gattungsbildenden Fernwirksystems gleichzusetzen, welche ja ebenfalls - wie bereits erwähnt - unter anderem zur Kennzeichnung von Schlüsseltypen, die unterschiedliche Schließfunktionen haben, herangezogen werden können.

Die Erfindung hat die Aufgabe, ein Verfahren anzugeben, mit dem Codeworte eines Fernwirksystems noch besser geschützt werden können und

das gattungsgemäße Fernwirksystem so auszubilden, daß das erfindungsgemäße Verfahren damit durchgeführt werden kann, wobei mehrere gleichberechtigte Sender nebeneinander verwendbar sein sollen. Diese Aufgabe wird mit den kennzeichnenden Merkmalen des Verfahrensanspruchs 1 und des Vorrichtungsanspruchs 6 erfindungsgemäß gelöst.

Gemäß der Erfindung wird zum einen dem jeweiligen Objekt mindestens ein objektspezifischer und unveränderlicher Grundanteil aller - d. h. durch die algorithmische Fortschaltung erzeugbaren - Codeworte zugewiesen. Da durch elektronische Codierung mit verhältnismäßig geringem Aufwand nahezu beliebig viele Variationen eines Codewortanteils erstellt werden können, ist es möglich, jedem Objekt, d. h. auch jedem Kraftfahrzeug einer Typenbaureihe, einen eigenen, nirgends wiederkehrenden objektspezifischen Code zuzuweisen. Zum anderen wird auch jedem zum Objekt gehörenden Sender ein unveränderlicher Grundanteil aller Codeworte zugewiesen. Dieser kann für alle Sender gleich sein und braucht dann nur einmal im Objekt abgelegt zu werden.

Es ist zwar bekannt (DE 33 09 802 C2), die Anpassung standardisierter Sensoren (für Tankfüllung, Temperaturen etc.) an die individuellen Verhältnisse in einem bestimmten Kraftfahrzeug mit Hilfe eines ROM zu vereinfachen, welches fahrzeugspezifische Signalumsetzungskennlinien enthält und diese den zwischen den Sensoren und deren Anzeigeinstrumenten vorgesehenen Signal-Umsetzanordnungen aufprägt. Ein Hinweis auf die erfindungsgemäße Aufteilung der Codeworte eines Fernwirksystems kann der genannten Patentschrift aber nicht entnommen werden.

Zusätzliche Gattungsmerkmale der Unteransprüche sind ebenfalls aus der gattungsbildenden DE 36 36 822 C1 bekannt bzw. herleitbar. Die kennzeichnenden Merkmale der Unteransprüche 2 bis 5 offenbaren vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens, während die kennzeichnenden Merkmale der Unteransprüche 7 bis 13 das erfindungsgemäße Fernwirksystem nach Anspruch 6 vorteilhaft weiterbilden.

In bevorzugter Ausführung wird jedem Sender des Fernwirksystems ein individueller unveränderlicher Grundanteil aller Codeworte zugewiesen. Dieser ist folglich objekt **und** senderspezifisch. In dieser Ausführungsform muß im Objekt bzw. Empfänger ein Gesamtvorrat **aller** individuellen Grundanteile abgelegt werden, der mindestens der Anzahl der zu unabhängiger paralleler Verwendung mitgelieferten Sender entspricht.

Die permanente Speicherung der objektspezifischen Anteile muß jedem Schreibzugriff entzogen sein, kann also z. B. in ROMs vorliegen. Sie kann in geeigneter Weise mit der nur temporären Spei-

cherung der veränderbaren Anteile verknüpft sein oder aber in vollständig, d. h. auch physikalisch getrennten Speichern vorliegen.

Dies hat den Vorteil, daß im Gegensatz zum Stand der Technik nicht mehr jeder beliebige, im Ersatzteilhandel erhältliche Sender zur Einspeicherung eines neuen aktuellen Codewortes in den Empfänger verwendet werden kann, auch wenn ein Sender-RESET durchgeführt und die mechanische Sicherung überwunden wurde. Denn die objektspezifischen, unveränderlichen Anteile der Codeworte werden zwar immer übertragen und vorab auf Übereinstimmung geprüft, können aber unter keinen Umständen Veränderungen der entsprechenden permanenten Speicherinhalte im Objekt bzw. Empfänger bewirken.

Es liegt auf der Hand, daß der Verkauf von Ersatzsendern für ein solches System wesentlich besser überwacht und Mißbrauch noch stärker erschwert werden kann. Ein Austausch der einmal zugewiesenen objektspezifischen Grundanteile ist nur durch Austausch der Steuereinrichtung bzw. der Speicher möglich.

Zusätzlich können auch noch benutzerspezifische Anteile in den Grundanteilen enthalten sein, die bei Senderbetätigung dem Empfänger bzw. dem Objekt bereits vorab gewisse Benutzerdaten mitteilen. An sich sind derartige benutzerspezifische Codeanteile bereits bekannt; sie wirken sich bei der kraftfahrzeugtechnischen Anwendung eines Fernwirksystems z. B. auf einstellbare Fahrzeugbauteile wie Sitze oder Rückblickspiegel aus.

Unbefugte Benutzung des Fernwirksystems mit einem abhanden gekommenen Sender kann sehr wirksam abgewehrt werden, wenn jeder Codewort-Grundanteil, der einem

- zum einen bereits wenigstens einmal benutzen und

- zum anderen bei einem Einlesevorgang **nicht** benutzten Sender zugeteilt ist, automatisch entwertet - d. h. gesperrt oder gelöscht - wird. Diese automatische Sicherungsfunktion kann von verschiedenen Bedingungen abhängig gemacht werden:

- Die wenigstens einmalige Benutzung des Senders, dessen Codewort-Grundanteil gesperrt werden soll, kann z. B. durch Registrierung eines Codewortfortschaltvorgangs in dem zugordneten veränderbaren Anteil desselben Codewortes erfaßt werden.

- Die Sicherungsfunktion kann grundsätzlich bei der endgültigen Bestätigung eines mit mehreren Sendern vorgenommenen Einlesevorgangs ausgeführt werden.

- Sie kann in Abhängigkeit von der Reihenfolge des Einlesens ausgeführt werden, z. B. dann, wenn während des Einlesevorgangs eine bestimmte Reihenfolge nicht eingehalten werden kann, weil ein

Sender fehlt.

Hierbei ist es sinnvoll, wenn der Gesamtvorrat der im Objekt abgelegten Codewort - Grundanteile etwas größer als die Anzahl der gelieferten Sender ist. Neu zu beschaffenden Sendern für das Fernwirksystem kann dann ein weiterer, noch nicht benutzter Codewort - Grundanteil aus dem Gesamtvorrat zugewiesen werden.

Ein Ausführungsbeispiel eines erfindungsgemäßen Fernwirksystems ist in der Zeichnung dargestellt und wird im folgenden näher beschrieben.

Die einzige **Figur** zeigt stark schematisiert die für die Erfindung wesentlichen Bestandteile des Fernwirksystems.

Sie stellt ferner die Aufteilung der in den Sendern und dem Objekt bzw. Empfänger gespeicherten Codeworte in einen festen Grundanteil und einen algorithmisch veränderbaren Anteil anschaulich dar.

In einer Steuereinrichtung 1, die in einem zu schützenden Objekt, z. B. einem Kraftfahrzeug K, angeordnet ist, ist in n Speicherplätzen SP<sub>1</sub> bis SP<sub>n</sub> eine Gesamtmenge von n Codeworten CW<sub>1</sub> bis CW<sub>n</sub> abgelegt. Sie entspricht mindestens einer Anzahl m von zugehörigen Sendern S<sub>1</sub> bis S<sub>m</sub>, die für das jeweilige Objekt zu parallelem, unabhängigen Gebrauch -z. B. durch verschiedene Personen - geliefert werden sollen. Die Anzahl m der Sender S<sub>1</sub> bis S<sub>m</sub> kann kleiner oder gleich n sein. In der gewählten Darstellung ist m = 3.

Jedes Codewort CW<sub>1</sub> bis CW<sub>n</sub> besteht

- aus einem festen Grundanteil CWG<sub>1</sub>, CWG<sub>2</sub> etc., der objekt- und senderspezifisch ist und nicht verändert werden kann, also z. B. in ROMs abgelegt ist, und

- aus einem veränderbaren Anteil CWV<sub>1</sub>, CWV<sub>2</sub> etc., der in bekannter Weise nach einem beliebigen Algorithmus veränderbar ist.

Letzterer ist für die Erfindung nicht wesentlich und wird daher hier nicht näher erläutert.

Die Speicherplätze SP... sind der Klarheit halber für die unveränderlichen Grundanteile und die veränderbaren Anteile einheitlich dargestellt, können aber durchaus verschiedene Strukturen haben, insbesondere auch physikalisch voneinander getrennt sein.

Die Codeworte CW... sind hier anschaulich als Folgen dezimaler Ziffern dargestellt; es versteht sich von selbst, daß die Art des verwendeten Codes und ebenso die Art der Übertragung der Codeworte zwischen Sendern und Empfänger für das Wesen der Erfindung vollkommen unerheblich ist. Es sind beliebige Code- bzw. Übertragungsarten (Infrarot, Ultraschall, Funk) verwendbar.

Ersichtlich weichen auch die veränderbaren Anteile CWV... der Codeworte voneinander ab; da diese durch die Steuereinrichtung 1 jeweils nach einer Codeübertragung unabhängig von den übrigen ver-

änderbaren Anteilen algorithmisch fortgeschaltet werden, können allenfalls zufällig einmal in zwei oder mehreren Codeworten gleiche veränderbare Anteile CWV... auftreten. Diese Codeworte unterscheiden sich dann natürlich immer noch durch ihre Grundanteile CWG... .

Jeder Sender S<sub>1</sub> bis S<sub>3</sub> enthält in bekannter Weise ein Code - Übertragungsorgan, hier eine Infrarot-Diode IS, das durch Betätigung einer Sendetaste ST zur Übertragung des im jeweiligen Sender gespeicherten aktuellen Codewortes CW... aktivierbar ist. Ersichtlich stimmen die aktuellen Codeworte CW<sub>1</sub> bis CW<sub>3</sub> der Sender S<sub>1</sub> bis S<sub>3</sub> mit denen in den Speicherplätzen SP<sub>1</sub> bis SP<sub>3</sub> der Steuereinrichtung 1 vollständig überein.

Ein Infrarotempfänger IE des Kraftfahrzeuges K leitet jedes empfangene Codewort CW... in bekannter Weise an die Steuereinrichtung weiter, wo es vor dem Ausführen irgendeiner durch Sender S... steuerbaren Funktion - also z. B. Entriegelung oder Verriegelung des Fahrzeugs durch eine symbolisch angedeutete, an die Steuereinrichtung 1 angeschlossene Zentralverriegelung ZV - mit den in den Speicherplätzen SP... gespeicherten Codeworten CW... auf vollständige Übereinstimmung verglichen wird.

Wurde vollständige Übereinstimmung festgestellt, so wird im Ausführungsbeispiel das Fahrzeug K in Ausführung einer gesteuerten Funktion "Entriegelung" zentral entriegelt. Die Steuereinrichtung 1 reagiert natürlich nicht auf Codeworte eines fremden oder desynchronisierten Senders. Es versteht sich, daß auch mehr als nur ein Empfänger IE vorgesehen werden kann; es bleibt aber bei einer zentralen Steuereinrichtung.

Eine ebenfalls der Steuereinrichtung 1 zugeordnete Rücksetztaste 2 ist im geschützten Bereich des Objekts, z. B. im Fahrgastraum des Kraftfahrzeuges K, vorgesehen. Sie ist also nur bei entschertem Objekt (= offener Tür) zugänglich. Mittels dieser Rücksetztaste 2 können **alle** veränderbaren Anteile CWV<sub>1...n</sub> der Codeworte CW<sub>1...n</sub> in den Speichern SP<sub>1...n</sub> der Steuereinrichtung 1 unabhängig von einer Senderbetätigung auf definierte Anfangszustände -die untereinander ebenfalls verschieden sein können -zurückgesetzt werden. Durch dieses Rücksetzen kann der Fahrzeugeigner bei Verlust eines Senders unverzüglich verhindern, daß Unbefugte den abhanden gekommenen Sender zur Steuerung der ihm zugewiesenen Funktion verwenden können. Die aktuellen Codeworte in den Sendern werden dabei natürlich nicht rückgesetzt.

Ausgehend von diesem Rücksetzzustand der veränderbaren Anteile CWV<sub>1...n</sub> müssen die Speicherinhalte der Steuereinrichtung 1 mit den entsprechenden Speicherinhalten der noch beim Fahrzeugeigner vorhandenen Sender S... wieder synchronisiert werden, um deren weitere Benutzbarkeit

zu gewährleisten. Dazu muß eine neu einlesende Codeübertragung von jedem dieser Sender zum Empfänger durchgeführt werden. Als solche wird beispielsweise jede erste mit je einem Sender nach einem Rücksetzvorgang vorgenommene Codeübertragung betrachtet.

Mittels der objekt- und senderspezifischen Codewort-Grundanteile CWG... wird dabei stets

- das eingelesene Codewort darauf überprüft, ob wenigstens ein "passender" Grundanteil CWG... übertragen wird, und

- der jeweils neu eingelesene veränderbare Anteil CWV..., der im einlesenden Sender S... aktuell ist, zu dem im Objekt abgelegten Grundanteil eindeutig zugeordnet.

Jedes neu eingelesene Codewort muß dann vor der endgültig wirksamen Abspeicherung seines veränderbaren Anteils CWV... in einen Speicherplatz SP... mittels eines weiteren der Steuereinrichtung 1 zugeordneten Schalters 3, der eine Quittiereinrichtung darstellt, bestätigt werden.

Der Schalter 3 kann nur betätigt werden, wenn ein passender mechanischer Schlüssel 5 vorhanden ist. Dieser Schlüssel 5 steht hier symbolisch für die zugehörige mechanisch codierte Einrichtung zur Betätigung des Schalters 3. Dieser kann z. B. - in an sich bekannter Weise - in einen nicht dargestellten Schließzylinder einer Tür oder eines Zünd-/Lenkschlösses integriert sein und darin direkt mittels des Schlüssels 5 betätigt werden.

Aus der zusätzlichen mechanischen Sicherung jedes Einlesevorgangs resultiert der Vorteil, daß unbefugte Resynchronisierung der Steuereinrichtung 1 bzw. des Empfängers mit dem verlorenen Sender bereits durch Austausch der mechanischen Schlösser des Kraftfahrzeugs K verhindert werden kann.

Durch eine Entwerteeinrichtung 4 - die z. B. eine Lesesperre für Speicherplätze SP einschalten oder eine Löschung des jeweiligen Speicherinhalts steuern kann - ist es unter den bereits erwähnten bestimmten Bedingungen möglich, auch die unveränderlichen Grundanteile CWG... oder die vollständigen Codeworte CW... zu entwerten, die abhanden gekommenen Sendern zugewiesen waren. Die Entwerteeinrichtung 4 wird z. B. durch abschließende Betätigung des Schalters 3 aktiviert.

### Ansprüche

1. Verfahren zur Sicherung von zur Steuerung von Funktionen übertragbaren Codeworten eines Fernwirksystems

- insbesondere für eine Kraftfahrzeug - Zentralverriegelungsanlage -
- bei welchem
- jedes von einem Sender zu einem Empfänger zu

übertragende Codewort aus einem nach Maßgabe eines vorgegebenen Algorithmus veränderbaren Anteil und einem diesem Algorithmus nicht unterworfenen Grundanteil besteht,

- welche beiden Anteile immer gemeinsam übertragen werden und vor Ausführung irgendeiner Funktion mit entsprechenden Anteilen wenigstens eines im Objekt gespeicherten Codewortes auf vollständige Übereinstimmung geprüft werden,

**gekennzeichnet durch**

Zuweisung wenigstens eines übereinstimmenden unveränderlichen objektspezifischen Grundanteils jedes Codewortes sowohl zu dem Objekt als auch zu jedem Sender.

2. Verfahren nach Anspruch 1,

**gekennzeichnet durch**

Zuweisung einer mindestens einer vorgesehenen Anzahl von nebeneinander in dem Fernwirksystem verwendbaren Sendern entsprechenden Gesamtmenge unveränderlicher, jeweils objekt- und senderspezifischer Codewort - Grundanteile zum Objekt und

Zuweisung genau eines unveränderlichen Grundanteils aus dieser Gesamtmenge zu jedem der vorgesehenen Sender.

3. Verfahren nach Anspruch 2,

**gekennzeichnet durch**

unabhängige algorithmische Veränderung der veränderbaren Codewort - Anteile für jedes Codewort.

4. Verfahren nach Anspruch 1, 2 oder 3,

bei welchem wenigstens der veränderbare Anteil des wenigstens einen im Objekt gespeicherten Codewortes mittels eines Senders neu einlesbar ist,

**gekennzeichnet durch**

Prüfung des Grundanteils des von dem Sender beim Einlesen übertragenen Codewortes auf vollständige Übereinstimmung mit einem im Objekt abgelegten Codewort - Grundanteil vor wirksamem Einlesen nur des veränderbaren Codewort - Anteils.

5. Verfahren nach Anspruch 2 und 4,

bei welchem der einem Sender zugeteilte und dem Algorithmus nicht unterworfenen Grundanteil eines Codewortes im Objekt wenigstens entwertbar ist,

**gekennzeichnet durch**

automatische Entwertung des einem der bereits wenigstens einmal unter Fortschaltung des veränderbaren Codewort - Anteils benutzten vorgesehenen Sender zugeteilten Codewort - Grundanteils bei Nichtverwendung dieses Senders beim Einlesevorgang.

6. Fernwirksystem mit auf physikalischem Wege

- von wenigstens einem beweglichen Sender
- zu einem in einem ortsfesten oder beweglichen Objekt angeordneten Empfänger
- zur Steuerung von Funktionen von dem Empfänger nachgeschalteten Einrichtungen, insbesondere von Schließfunktionen einer Kraftfahrzeug - Zentral-

verriegelungsanlage,  
durch Codeworte übertragbarem Code,  
in welchem Fernwirksystem

- jedes Codewort aus einem nach Maßgabe eines vorgegebenen Algorithmus veränderbaren Anteil und einem diesem Algorithmus nicht unterworfenen Grundanteil besteht,
- welche Anteile bei jeder Betätigung einer Sendetaste des Senders gemeinsam übertragen werden und vor Ausführung irgendeiner Funktion mit den entsprechenden Anteilen wenigstens eines im Objekt gespeicherten Codewortes auf vollständige Übereinstimmung geprüft werden, insbesondere zur Durchführung des Verfahrens nach Anspruch 2,

**gekennzeichnet durch**

- eine Anzahl von n Speicherplätzen (SP<sub>1</sub> bis SP<sub>n</sub>) im Objekt (K) zur unveränderbaren Speicherung von diesem individuell zugewiesenen objekt- und senderspezifischen, untereinander verschiedenen Grundanteilen (CWG<sub>1</sub> bis CWG<sub>n</sub>) und
- einen festen Speicherplatz für genau einen Grundanteil (CWG<sub>1</sub>, CWG<sub>2</sub> etc.) aus dieser Gesamtmenge in jedem von m Sendern (S<sub>1</sub>, S<sub>2</sub> etc. bis S<sub>m</sub>).

7. Fernwirksystem nach Anspruch 6,  
mit einer Steuereinrichtung, welche

- zur synchronen Fortschaltung des veränderbaren Anteils eines im Empfänger und im Sender zum Zeitpunkt der Codeübertragung übereinstimmend wenigstens temporär gespeicherten aktuellen Codewortes nach jeder Codeübertragung gemäß dem vorgegebenen Algorithmus im Sender und im Empfänger und
- zur Sperrung des Fernwirksystems wenigstens gegen in der näheren Vergangenheit von dem jeweiligen Sender bereits übertragene Codeworte vorgesehen ist,

**gekennzeichnet durch**

voneinander unabhängige algorithmische Fortschaltung der mit je einem Grundanteil (CWG<sub>1</sub>, CWG<sub>2</sub> etc.) ein Codewort (CW<sub>1</sub>, CW<sub>2</sub> etc.) bildenden veränderbaren Anteile (CWV<sub>1</sub>, CWV<sub>2</sub> etc.).

8. Fernwirksystem nach Anspruch 6 oder 7,  
- mit wenigstens einer am Objekt vorgesehenen mechanisch codierten Schließeinrichtung, welche als Zugangsberechtigung (Schlüsselrestriktion) im Zusammenhang mit jeder willkürlichen Veränderung und Neusynchronisation eines aktuellen Codewortes in Sender und Empfänger durch einen mechanisch codierten Schlüssel betätigt werden muß, wobei wenigstens der veränderbare Anteil eines Codewortes in einem Lernzustand des Empfängers aus einem Sender in einen Speicher des Objekts zur Wiederherstellung der Synchronisierung von Sender und Empfänger einlesbar ist,

**gekennzeichnet durch**

- eine der Steuereinrichtung (1) zugeordnete Ein-

richtung (2) zum willkürlichen, senderunabhängigen Rücksetzen nur der veränderbaren Anteile (CWV<sub>1</sub>, CWV<sub>2</sub> bis CWV<sub>n</sub>) aller in den Speicherplätzen (SP) des Objekts (K) abgelegten Codeworte (CW<sub>1</sub>, CW<sub>2</sub> bis CW<sub>n</sub>) auf bestimmte Anfangszustände,  
- auch im Lernzustand des Empfängers (IE) bzw. der Steuereinrichtung (1) wirksame Überprüfung des Grundanteils (CWG...) jedes von einem Sender (S...) zum Empfänger (IE) übertragenen Codeworts (CW...) und  
- eine durch eine zur Steuerung der Steuereinrichtung (1) vorgesehene mechanisch codierte Einrichtung (5) betätigbare Quittiereinrichtung (3) zur Bestätigung eines durch einen Sender (S...) nach dem willkürlichen, senderunabhängigen Rücksetzen der veränderbaren Teile aller Codeworte (CW<sub>1</sub>, CW<sub>2</sub> bis CW<sub>n</sub>) bewirkten Codewort - Einlesevorgangs.

9. Fernwirksystem nach Anspruch 6,

**gekennzeichnet durch**

benutzerspezifische Anteile des jedem Sender (S...) zugewiesenen Codewort - Grundanteils (CWG...).

10. Fernwirksystem nach Anspruch 6,

**gekennzeichnet durch**

Speicherung der objektspezifischen Grundanteile (CWG...) in ROMs.

11. Fernwirksystem nach Anspruch 6,

**gekennzeichnet durch**

physikalisch voneinander getrennte Speicher zur jeweiligen Speicherung der objektspezifischen Grundanteile (CWG...) und der veränderbaren Anteile (CWV...).

12. Fernwirksystem nach Anspruch 6,

**gekennzeichnet durch**

eine von der Anzahl n der im Objekt (K) abgelegten Codeworte (CW<sub>1</sub> bis C<sub>n</sub>) nach unten abweichende Anzahl von Sendern (S<sub>1</sub> bis S<sub>m</sub>).

13. Fernwirksystem nach Anspruch 8,

**gekennzeichnet durch**

eine Entwerteinrichtung (4) zur Entwertung wenigstens der in Speicherplätzen (SP<sub>1</sub> bis SP<sub>n</sub>) des Objekts (K) abgelegten Codewort - Grundanteile (CWG...) im Zusammenhang mit einem Codewort - Einlesevorgang in Abhängigkeit von vorgegebenen Bedingungen.

Geänderte Patentansprüche gemäß Regel 86(2) EPÜ.

1. Verfahren zur Verbesserung des Schutzes von Codeworten eines Fernwirksystems gegen unbefugte Benutzung, welche Codeworte

- zur Steuerung von Funktionen - insbesondere einer Kraftfahrzeug - Zentralverriegelungsanlage - von einem Sender zu einem Empfänger berührungslos übertragbar sind,
- jeweils aus einem nach Maßgabe eines vorgegebenen Algorithmus veränderbaren Anteil

und einem diesem Algorithmus nicht unterworfenen Grundteil bestehen,

- welche beiden Anteile immer gemeinsam übertragen werden und vor Ausführung irgendeiner Funktion auf vollständige Übereinstimmung mit entsprechenden Anteilen wenigstens eines im Objekt gespeicherten Codewortes geprüft werden, **gekennzeichnet durch**

Zuweisung wenigstens eines übereinstimmenden unveränderlichen, jedem Schreibzugriff entzogenen objektspezifischen Grundanteils jedes Codewortes sowohl zu dem Objekt als auch zu jedem Sender.

5

10

15

20

25

30

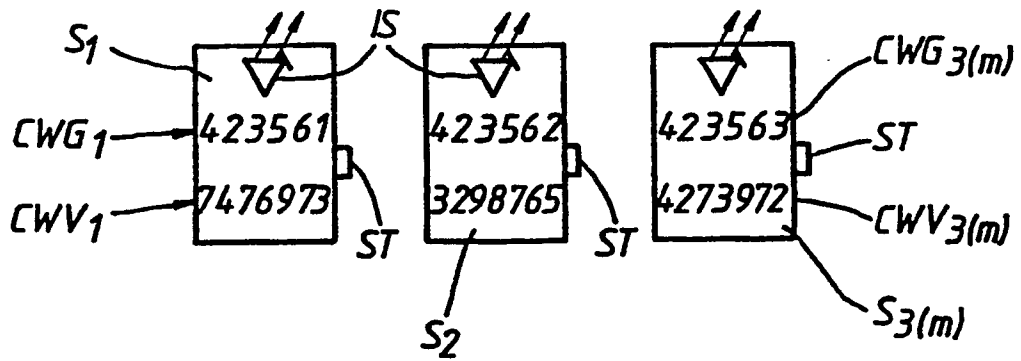
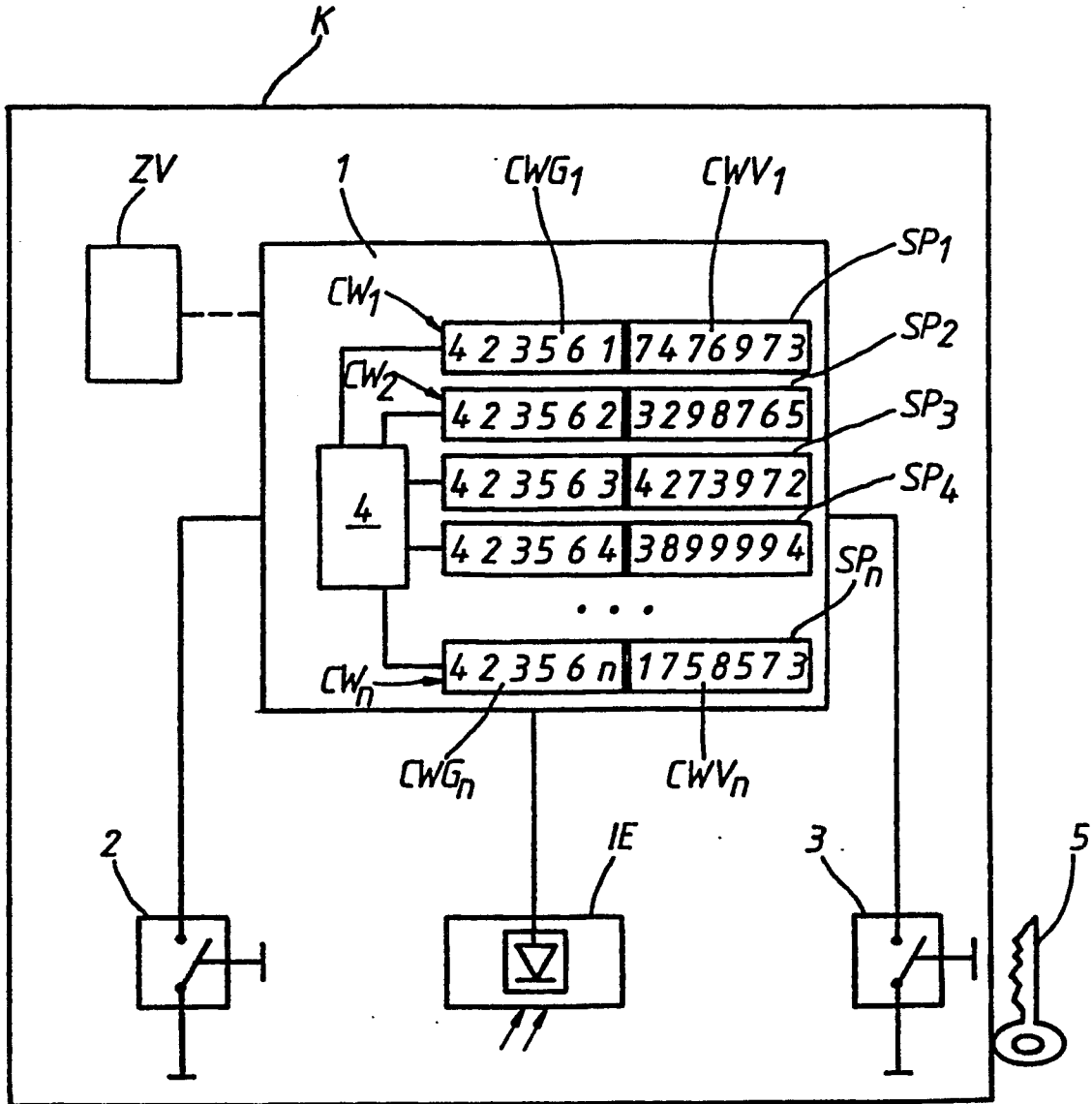
35

40

45

50

55





EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
X	EP-A-0244332 (SOUR) * Seite 2, Zeile 11 - Seite 5, Zeile 20; Figur *	1-4, 6, 7, 9, 11	E05B49/00 E05B65/36
Y		10	
A		8, 12	
Y	GB-A-2051442 (HOWARD) * Ansprüche 1, 2 *	10	
A, D	DE-C-3636822 (WILHELM RUF KG) * Spalte 4, Zeile 67 - Spalte 9, Zeile 64; Figur 1A *	1, 6, 8	
			RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
			E05B G08C
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort DEN HAAG		Abschlußdatum der Recherche 22. MAI 1990	Prüfer WANZEELE R. J.
KATEGORIE DER GENANNTEN DOKUMENTE		F : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument I : aus andern Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	
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			

1